



show d ~ show e

- [show data-plane quick-reload status](#) (2 ページ)
- [show ddns update interface](#) (4 ページ)
- [show ddns update method](#) (7 ページ)
- [show debug](#) (9 ページ)
- [show dhcpd](#) (14 ページ)
- [show dhcprelay state](#) (16 ページ)
- [show dhcprelay statistics](#) (17 ページ)
- [show diameter](#) (19 ページ)
- [show disk](#) (20 ページ)
- [show dns](#) (22 ページ)
- [show dns-hosts](#) (25 ページ)
- [show dynamic-filter data](#) (27 ページ)
- [show dynamic-filter dns-snoop](#) (30 ページ)
- [show dynamic-filter reports infected-hosts](#) (33 ページ)
- [show dynamic-filter reports top](#) (37 ページ)
- [show dynamic-filter statistics](#) (41 ページ)
- [show dynamic-filter updater-client](#) (45 ページ)
- [show eigrp events](#) (48 ページ)
- [show eigrp interfaces](#) (51 ページ)
- [show eigrp neighbors](#) (53 ページ)
- [show eigrp topology](#) (57 ページ)
- [show eigrp traffic](#) (61 ページ)
- [show environment](#) (63 ページ)
- [show event manager](#) (70 ページ)

show data-plane quick-reload status

データプレーンのリロードの状態を表示するには、特権 EXEC モードで **show data-plane quick-reload status** コマンドを使用します。

show data-plane quick-reload status

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|----------------------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーションモード | ・対応 | ・対応 | ・対応 | ・対応 | — |

コマンド履歴

リリー 変更内容
ス

9.20(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

このコマンドは、現在のコンテキストのデータパスのクイックリロードステータスを表示します。

例

次に、データプレーンのクイックリロードが有効になっている場合の **show data-plane quick-reload status** コマンドの出力例を示します。

```
ciscoasa# show data-plane quick-reload status
data-plane reloaded!
```

次に、データプレーンのクイックリロードが無効になっている場合の **show data-plane quick-reload status** コマンドの出力例を示します。

```
ciscoasa# show data-plane quick-reload status
device reloaded
```

関連コマンド

| コマンド | 説明 |
|--------------------------------|--------------------------|
| data-plane quick-reload | データプレーンのクイックリロードを有効にします。 |

show ddns update interface

ASA インターフェイスに割り当てられた DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを使用します。

show ddns update interface [*interface-name*]

構文の説明

interface-name (任意) ネットワークインターフェイスの名前。

コマンド デフォルト

interface-name スtringを省略すると、各インターフェイスに割り当てられている DDNS 方式が表示されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

7.2(1) このコマンドが追加されました。

9.15(1) Web 更新方式の場合、このコマンドの出力には、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。

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。

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name      Update Destination
  ddns-2                  not available
ciscoasa#
```

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。

```
ciscoasa# 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 : asal.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。

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available

Last Update Not attempted
```

関連コマンド

| コマンド | 説明 |
|--------------------------|---|
| ddns | 標準の DDNS 更新方式タイプを指定します。 |
| ddns update | DDNS 方式をインターフェイスに関連付けます。 |
| ddns update method | DDNS 更新方式を作成します。 |
| interval maximum | DNS 要求の更新間隔を設定します。 |
| show ddns update method | 設定済みの各 DDNS 方式のタイプと間隔を表示します。DDNS 更新を実行する DHCP サーバー。 |
| 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。 |

| コマンド | 説明 |
|------------------------|-------------------------------------|
| web update-type | 更新するアドレスタイプ (IPv4 または IPv6) を指定します。 |
| web update-url | DDNS 更新方式を Web に設定し、更新 URL を設定します。 |

show ddns update method

実行コンフィギュレーションの DDNS 更新方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

show ddns update method [*method-name*]

構文の説明

method-name (任意) 設定済み DDNS 更新方式の名前。

コマンド デフォルト

method-name スtring を省略すると、設定されているすべての DDNS 更新方式が表示されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容

7.2(1) このコマンドが追加されました。

9.15(1) Web 更新方式の出力が追加されました。

9.18(1) Web 更新方式の出力は、設定された参照 ID を表示するように拡張されました。

例

次に、**ddns-2** という名前の DDNS 方式を表示する例を示します。

```
ciscoasa(config)# 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
ciscoasa(config)#
```

次の例は、Web 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method web1
Dynamic DNS Update Method: web1
Dynamic DNS updated via HTTP(s) protocols
URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<>h&myip=<a>
```

```
Update type configured: ipv4
Configured reference-identity name: dyndns
Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
```

| 関連コマンド | コマンド | 説明 |
|--------|-----------------------------------|--|
| | ddns | 作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。 |
| | ddns update | ASA インターフェイスをダイナミック DNS (DDNS) 更新方式または DDNS 更新ホスト名に関連付けます。 |
| | ddns update method | DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。 |
| | show ddns update interface | 設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。 |
| | 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 *command* について、*command* に続く *keywords* は、関連する **debug** コマンドによりサポートされる *keywords* と同一です。

コマンドデフォルト

このコマンドには、デフォルト設定がありません。

コマンドモード

次の表は、このコマンドを入力できるモードを示しています。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | • 対応 |

コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

8.0(2) 使用可能なコマンド値のリストに **eigrp** キーワードが追加されました。

8.4(1) 使用可能なコマンド値のリストに **route** キーワードが追加されました。

9.2(1) 使用可能なコマンド値のリストに **event manager** キーワードが追加されました。

9.5(2) デバッグの永続的な設定が含まれるように、出力が変更されました。

9.5(2) フィルタ条件セットに基づいたフィルタリングによってデバッグログを表示する機能が追加されました。

使用上のガイドライン

各 *command* について、*command* に続く *keywords* は、関連する **debug** コマンドによりサポートされる *keywords* と同一です。サポートされている構文については、関連する **debug** コマンドを参照してください。



(注) 各 *command* を使用できるかどうかは、該当する **debug** コマンドをサポートするコマンドモードによって異なります。

有効な *command* 値は次のとおりです。

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**
- **debug eigrp parser**
- **dhcpc**
- **dhcpd**
- **dhcrelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **event manager**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**

- http-map
- icmp
- igmp
- ipv6 eigrp
- ipv6 eigrp neighbor
- ipv6 eigrp notifications
- ipv6 eigrp summary
- ils
- imagemgr
- ipsec-over-tcp
- ipv6
- iua-proxy
- kerberos
- ldap
- mfib
- mgcp
- mmp
- mrib
- ntdomain
- ntp
- ospf
- parser
- pim
- pix
- pptp
- radius
- rip
- route
- rtsp
- sdi
- sequence
- sfr

- sip
- skinny
- smtp
- sqlnet
- ssh
- ssl
- sunrpc
- tacacs
- timestamps
- vpn-sessiondb
- webvpn
- xdmcp
- xml

例

show debug コマンドを使用して、すべてのデバッグ コンフィギュレーション、特定の機能のデバッグ コンフィギュレーション、および機能の一部に対するデバッグ コンフィギュレーションを表示できます。

次のコマンドでは、認証、アカウントिंग、およびフラッシュメモリのデバッグをイネーブルにします。

```
ciscoasa# debug aaa authentication
debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

関連コマンド

| コマンド | 説明 |
|--------------|-------------------------------|
| debug | すべての debug コマンドを表示します。 |

show dhcpd

DHCP のバインディング情報、状態情報、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **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。 |
| <i>IP_address</i> | 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 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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

7.0(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

オプションの IP アドレスを **show dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけが表示されます。

show dhcpd binding | state | statistics コマンドはグローバル コンフィギュレーション モードでも使用可能です。

例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
ciscoasa# 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。

```
ciscoasa# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
ciscoasa# 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

| コマンド | 説明 |
|----------------------------------|--------------------------------------|
| clear configure dhcpd | すべての DHCP サーバー設定を削除します。 |
| 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。 |
| dhcpd lease | クライアントに付与される DHCP 情報のリースの長さを定義します。 |
| 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 state

DHCP リレーエージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

show dhcprelay state

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

7.0(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

このコマンドは、現在のコンテキストおよび各インターフェイスについての DHCP リレーエージェントの状態情報を表示します。

例

次に、**show dhcprelay state** コマンドの出力例を示します。

```
ciscoasa# 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
```

関連コマンド

| コマンド | 説明 |
|--------------------------------------|--------------------------------------|
| show dhcpd | DHCP サーバーの統計情報と状態情報を表示します。 |
| show dhcprelay statistics | DHCP リレー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。 |

show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

show dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

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。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容

7.0(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

show dhcprelay statistics コマンドの出力は、**clear dhcprelay statistics** コマンドを入力するまで増加します。

例

次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
ciscoasa# 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
ciscoasa#
```

関連コマンド

| コマンド | 説明 |
|--------------------------------------|---------------------------------------|
| clear configure dhcprelay | DHCP リレー エージェントの設定をすべて削除します。 |
| 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。 |
| debug dhcprelay | DHCP リレー エージェントのデバッグ情報を表示します。 |
| show dhcprelay state | DHCP リレー エージェントの状態を表示します。 |
| 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。 |

show diameter

各 Diameter 接続の状態情報を表示するには、特権 EXEC モードで **show diameter** コマンドを使用します。

show diameter

構文の説明

このコマンドには引数またはキーワードはありません。

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。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

9.5(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

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。

例

次に、**show diameter** コマンドの出力例を示します。

```
ciscoasa# 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

| コマンド | 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。 |
| inspect diameter | Diameter トラフィックを検査します。 |

show disk

ASA のフラッシュメモリの内容だけを表示するには、特権 EXEC モードで **show disk** コマンドを使用します。

show disk [0 | 1] [filesystem | all] controller

構文の説明

0 | 1 内部フラッシュメモリ (0、デフォルト) または外部フラッシュメモリ (1) を指定します。

all フラッシュメモリの内容とファイルシステム情報を表示します。

コントローラ フラッシュコントローラのモデル番号を指定します。

filesystem 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、このコマンドは内部フラッシュメモリを示します。

コマンドモード

次の表は、このコマンドを入力できるモードを示しています。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

コマンド履歴

リリリー 変更内容
ス

7.0(1) このコマンドが追加されました。

例

次に、**show disk** コマンドの出力例を示します。

```
ciscoasa# show disk
-#- --length-- -----date/time----- path
 11 1301      Feb 21 2005 18:01:34 test.cfg
 12 1949      Feb 21 2005 20:13:36 test1.cfg
 13 2551      Jan 06 2005 10:07:36 test2.cfg
 14 609223    Jan 21 2005 07:14:18 test3.cfg
 15 1619      Jul 16 2004 16:06:48 test4.cfg
 16 3184      Aug 03 2004 07:07:00 old_running.cfg
 17 4787      Mar 04 2005 12:32:18 test5.cfg
 20 1792      Jan 21 2005 07:29:24 test6.cfg
 21 7765184   Mar 07 2005 19:38:30 test7.cfg
 22 1674      Nov 11 2004 02:47:52 test8.cfg
```

```

23 1863      Jan 21 2005 07:29:18 test9.cfg
24 1197      Jan 19 2005 08:17:48 test10.cfg
25 608554    Jan 13 2005 06:20:54 backupconfig.cfg
26 5124096   Feb 20 2005 08:49:28 cdisk1
27 5124096   Mar 01 2005 17:59:56 cdisk2
28 2074      Jan 13 2005 08:13:26 test11.cfg
29 5124096   Mar 07 2005 19:56:58 cdisk3
30 1276      Jan 28 2005 08:31:58 lead
31 7756788   Feb 24 2005 12:59:46 asdmfile.dbg
32 7579792   Mar 08 2005 11:06:56 asdmfile1.dbg
33 7764344   Mar 04 2005 12:17:46 asdmfile2.dbg
34 5124096   Feb 24 2005 11:50:50 cdisk4
35 15322     Mar 04 2005 12:30:24 hs_err.log
10170368 bytes available (52711424 bytes used)

```

次に、**show disk filesystems** コマンドの出力例を示します。

```

ciscoasa# show disk filesystems
***** Flash Card Geometry/Format Info *****
COMPACT FLASH CARD GEOMETRY
  Number of Heads:          4
  Number of Cylinders       978
  Sectors per Cylinder     32
  Sector Size               512
  Total Sectors             125184
COMPACT FLASH CARD FORMAT
  Number of FAT Sectors     61
  Sectors Per Cluster      8
  Number of Clusters       15352
  Number of Data Sectors   122976
  Base Root Sector         123
  Base FAT Sector          1
  Base Data Sector         155

```

次に、**show disk controller** コマンドの出力例を示します。

```

ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA

```

関連コマンド

| コマンド | 説明 |
|------------|------------------|
| dir | ディレクトリの内容を表示します。 |

show dns

完全修飾ドメイン名 (FQDN) ホストの現在の解決済み DNS アドレスと信頼できる DNS 送信元の設定を表示するには、特権 EXEC モードで **show dns** コマンドを使用します。

show dns [*host fqdn_name* | **ip-cache** [*count*] | **trusted-source** [*detail*]]

構文の説明

hostfqdn_name (オプション) 情報を表示する対象を指定した完全修飾ドメイン名 (FQDN) のみに制限します。

ip-cache [*count*] (オプション) ネットワークサービス オブジェクト ドメインの指定用に DNS 応答をスヌーピングして作成された IP キャッシュの内容を表示します。キャッシュ内のアイテム数のみを表示する場合は **count** キーワードを含めます。

trusted-source [*detail*] (オプション) ネットワークサービス オブジェクト ドメインの解決用にスヌーピングされる信頼できる DNS サーバーの設定を表示します。信頼できるすべての DNS サーバーの 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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリー 変更内容
ス

7.0(1) このコマンドが追加されました。

9.17(1) パラメータなしで **show dns** コマンドを実行した場合に **show dns-hosts** コマンドと同じ情報が提供されるようになりました。また、**ip-cache** キーワードと **trusted-source** キーワードが追加されました。

例

次に、**show dns** コマンドの出力例を示します。いずれの FQDN ホストもアクティブ化されていない場合、このコマンドによる出力はありません。

```
ciscoasa# 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。

```
ciscoasa# show dns host www.example.com
Name: www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 00:00:36
Address: 10.1.1.2 TTL 00:01:01
```

9.17(1) 以降では、このコマンドをパラメータなしで実行すると **show dns-hosts** コマンドと同じ情報が表示され、ネットワークサービスオブジェクトドメインの解決に使用される信頼できる DNS 送信元と IP キャッシュに関する情報も含まれます。

```
ciscoasa# show dns
Host                Flags      Age Type  Address(es)
sngdc01-ucs-dcz01n-gslb1- (temp, OK) 0    IP    173.39.112.230
alln01-ucs-dcz03n-gslb1-s (temp, OK) 0    IP    173.37.151.38
rcdn9-ucs-dcz05n-gslb1-sn (temp, OK) 0    IP    72.163.7.198
aer01-ucs-dcz01n-gslb1-sn (temp, OK) 0    IP    173.38.213.70
rtp5-ucs-dcz01n-gslb1-sni (temp, OK) 0    IP    64.101.37.118
mtv5-ucs-dcz06n-gslb1-sni (temp, OK) 0    IP    173.36.225.38
www.cisco.com        (temp, OK) 0    IP    72.163.4.161
  origin-www.cisco.com
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
  DNS Server Configured: 72.163.47.11: management : N/A
  DNS Server Configured: 173.37.137.85: management : N/A
  DNS Server Configured: 173.37.142.73: management : N/A
DNS snooping IP cache: 0 in use, 0 most used
Address                Idle(sec) Timeout(sec) Hit-count      Branch(es)
```

関連コマンド

| コマンド | 説明 |
|--------------------------|---|
| clear dns-hosts | DNS キャッシュをクリアします。 |
| clear ip-cache | ネットワークサービス オブジェクト ドメインの指定用に DNS 応答をスヌーピングして作成されたキャッシュをクリアします。 |
| dns domain-lookup | ASA によるネームルックアップの実行をイネーブルにします。 |

| コマンド | 説明 |
|---------------------------|-----------------------|
| dns name-server | DNS サーバー アドレスを設定します。 |
| dns trusted-source | 信頼できる DNS サーバーを識別します。 |

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **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

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
7.0(1) このコマンドが追加されました。

例

次に、**show dns-hosts** コマンドの出力例を示します。

```
ciscoasa# 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
```

関連コマンド

| コマンド | 説明 |
|--------------------------|--|
| clear dns-hosts | DNS キャッシュをクリアします。 |
| dns domain-lookup | ASA によるネームルックアップの実行をイネーブルにします。 |
| dns name-server | DNS サーバー アドレスを設定します。 |
| dns retries | ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数を指定します。 |

| コマンド | 説明 |
|--------------------|----------------------------------|
| dns timeout | 次の DNS サーバーを試行するまでに待機する時間を指定します。 |

表 11 に、各フィールドの説明を示します。

表 1 : *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。 <ul style="list-style-type: none"> • 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。ASA は、72 時間の無活動後にこのエントリを削除します。 • 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。 • OK : このエントリは有効です。 • ?? : このエントリは疑わしいため、再検証が必要です。 • 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。 |
| Address(es) | IP アドレス。 |

関連コマンド

| コマンド | 説明 |
|--------------------------|--|
| clear dns-hosts | DNS キャッシュをクリアします。 |
| dns domain-lookup | ASA によるネームルックアップの実行をイネーブルにします。 |
| dns name-server | DNS サーバー アドレスを設定します。 |
| dns retries | ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数を指定します。 |
| dns timeout | 次の DNS サーバーを試行するまでに待機する時間を指定します。 |

show dynamic-filter data

ボットネットトラフィックフィルタダイナミックデータベースに関する情報（ダイナミックデータベースの最終ダウンロード日、データベースのバージョン情報、データベース内のエントリ数、10個のサンプルエントリなど）を表示するには、特権 EXEC モードで **show dynamic-filter data** コマンドを使用します。

show dynamic-filter data

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|----------------------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

コマンド履歴

リリース 変更内容
8.2(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

ダイナミックデータベース情報を表示するには、最初に **dynamic-filter use-database** コマンドと **dynamic-filter updater-client enable** コマンドを使用して、データベースの使用とダウンロードをイネーブルにします。

例

次に、**show dynamic-filter data** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter data
Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
  cisco.example, cisco.invalid, bad.example.com
  bad.example.net, bad.example.org, bad.cisco.example
  bad.cisco.ivalid
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
```

```
Dynamic data: 0 domain names , 1080 IPv4 addresses
Local data: 0 domain names , 0 IPv4 addresses
```

関連コマンド

| コマンド | 説明 |
|--|--|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタ コンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNS スヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。 |
| dns server-group | ASA の DNS サーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミック データベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミック データベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |
| dynamic-filter enable | アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |

| コマンド | 説明 |
|---|---|
| dynamic-filter updater-client enable | ダイナミック データベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミック データベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィック フィルタのホワイトリストを編集します。 |
| inspect dns dynamic-filter-snoop | DNSインスペクションとボットネットトラフィック フィルタ スヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィック フィルタ ルールを表示します。 |
| show dynamic-filter data | ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。 |
| show dynamic-filter reports | 上位10個のボットネットサイト、ポート、および感染したホストに関するレポートを生成します。 |
| show dynamic-filter statistics | ボットネットトラフィック フィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。 |
| show dynamic-filter updater-client | サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。 |
| show running-config dynamic-filter | ボットネットトラフィック フィルタの実行コンフィギュレーションを表示します。 |

show dynamic-filter dns-snoop

ボットネットトラフィックフィルタのDNSスヌーピングサマリー（または実際のIPアドレスと名前）を表示するには、特権 EXEC モードで **show dynamic-filter dns-snoop** コマンドを使用します。

show dynamic-filter dns-snoop [detail]

構文の説明

detail （任意）DNS 応答からスヌーピングされた IP アドレスと名前を表示します。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|--------------------------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュ レーション | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリー 変更内容
ス

8.2(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

この出力には、ブラックリストに一致する名前だけでなく、すべての検査済み DNS データが含まれます。スタティック エントリの DNS データは含まれません。

DNS スヌーピングデータを消去するには、**clear dynamic-filter dns-snoop** コマンドを入力します。

例

次に、**show dynamic-filter dns-snoop** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter dns-snoop
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrsrc address buckets
```

次に、**show dynamic-filter dns-snoop detail** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter dns-snoop detail
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrsrc address buckets
DNS reverse Cache Information:
```

```
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
[www3.example.com] cat=2, ttl=3
[www.bad.example.com] cat=2, ttl=3
[www.example.com] cat=2, ttl=3
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
[cisco.example] cat=2, ttl=73
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
[cisco.invalid] cat=2, ttl=2
```

関連コマンド

| コマンド | 説明 |
|--|--|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタのコンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNSスヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。 |
| dns server-group | ASA の DNS サーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |

| コマンド | 説明 |
|---|--|
| dynamic-filter enable | アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |
| dynamic-filter updater-client enable | ダイナミック データベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミック データベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィックフィルタのホワイトリストを編集します。 |
| inspect dns dynamic-filter-snoop | DNS インスペクションとボットネットトラフィックフィルタスヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィック フィルタルールを表示します。 |
| show dynamic-filter data | ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。 |
| show dynamic-filter reports | 上位10個のボットネットサイト、ポート、および感染したホストに関するレポートを生成します。 |
| show dynamic-filter statistics | ボットネットトラフィックフィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。 |
| show dynamic-filter updater-client | サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。 |
| show running-config dynamic-filter | ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。 |

show dynamic-filter reports infected-hosts

ボットネット トラフィック フィルタで分類された、感染したホストのレポートを生成するには、特権 EXEC モードで **show dynamic-filter reports infected-hosts** コマンドを使用します。

show dynamic-filter reports infected-hosts [**max-connections** | **latest-active** | **highest-threat** | **subnet ip_address netmask** | **all**]

構文の説明

| | |
|----------------------------------|--|
| all | バッファに格納されている感染したホストの情報をすべて表示します。この表示には、数千ものエントリが含まれることがあります。CLI ではなく、ASDM を使用して PDF を生成できます。 |
| highest-threat | 脅威レベルが最高のマルウェア サイトに接続する 20 個のホストを表示します。 |
| latest-active | 最近アクティビティを行った 20 個のホストを表示します。各ホストについて、アクセスした 5 件のマルウェア サイトに関する詳細情報が表示されます。 |
| max-connections | 接続数が最も多い感染ホストを 20 個表示します。 |
| subnet ip_address netmask | 指定されたサブネット内のホストを最大 20 個表示します。 |

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

8.2(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

これらのレポートには、感染ホストの詳細な履歴が含まれ、感染ホスト、閲覧したマルウェア サイト、およびマルウェア ポートを示します。

レポートデータを消去するには、**clear dynamic-filter reports infected-hosts** コマンドを入力します。

例

次に、**show dynamic-filter reports infected hosts all** コマンドの出力例を示します。

```
ciscoasa#
          show
          dynamic-filter
          reports
          infected-hosts
          all

Total 2 infected-hosts in buffer

Host (interface)                Latest malicious conn time, filter action  Conn
logged, dropped

=====

192.168.1.4 (internal)          15:39:40 UTC Sep 17 2009, dropped
      3          3

Malware-sites connected to (not ordered)

Site                Latest conn port, time, filter action  Conn logged, dropped
Threat-level Category

-----

10.73.210.27 (bad.example.com)  80, 15:39:31 UTC Sep 17 2009, dropped    2    2
very-high Malware

10.65.2.119 (bad2.example.com)  0, 15:39:40 UTC Sep 17 2009, dropped    1    1
very-high admin-added

=====

192.168.1.2 (internal)          15:39:01 UTC Sep 17 2009, dropped
      5          5

Malware-sites connected to (not ordered)

Site                Latest conn port, time, filter action  Conn logged, dropped
Threat-level Category

-----

10.131.36.158 (bad.example.com)  0, 15:37:46 UTC Sep 17 2009, dropped    1    1
very-high admin-added

10.65.2.119 (bad2.example.com)  0, 15:37:53 UTC Sep 17 2009, dropped    1    1
very-high admin-added

20.73.210.27 (bad3.example.com)  80, 15:39:01 UTC Sep 17 2009, dropped    3    3
very-high Malware

=====
```

Last clearing of the infected-hosts report: Never

関連コマンド

| コマンド | 説明 |
|--|--|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタコンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNSスヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASAがDNSサーバーにDNS要求を送信できるようにします。 |
| dns server-group | ASAのDNSサーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |
| dynamic-filter enable | アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |

| コマンド | 説明 |
|---|---|
| dynamic-filter updater-client enable | ダイナミック データベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミック データベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィックフィルタのホワイトリストを編集します。 |
| inspect dns dynamic-filter-snoop | DNS インスペクションとボットネットトラフィック フィルタ スヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィック フィルタ ルールを表示します。 |
| show dynamic-filter data | ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10個のサンプルエントリなど、ダイナミック データベースに関する情報を表示します。 |
| show dynamic-filter dns-snoop | ボットネットトラフィック フィルタの DNS スヌーピングの概要を表示します。 detail キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。 |
| show dynamic-filter statistics | ボットネットトラフィックフィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。 |
| show dynamic-filter updater-client | サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。 |
| show running-config dynamic-filter | ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。 |

show dynamic-filter reports top

ボットネット トラフィック フィルタによって分類された、上位 10 件のマルウェアサイト、ポート、および感染ホストのレポートを生成するには、特権 EXEC モードで **show dynamic-filter reports top** コマンドを使用します。

show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]

構文の説明

malware-ports (任意) 上位 10 件のマルウェアサイトのレポートを表示します。

malware-sites (任意) 上位 10 件のマルウェアポートのレポートを表示します。

infected-hosts (任意) 上位 10 件の感染ホストのレポートを表示します。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

8.2(1) このコマンドが追加されました。

8.2(2) **botnet-sites** および **botnet-ports** キーワードが **malware-sites** および **malware-ports** に変更されました。malware-sites レポートには、ドロップした接続数と、各サイトの脅威レベルおよびカテゴリが含まれています。最終クリアタイムスタンプが追加されました。脅威イベントについては、シビラティ（重大度）レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

このレポートはデータのスナップショットで、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。

レポートデータを消去するには、**clear dynamic-filter reports top** コマンドを入力します。

例

次に、**show dynamic-filter reports top malware-sites** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter reports top malware-sites
```

```

Site
-----
Connections logged dropped Threat Level Category
-----
bad1.example.com (10.67.22.34) 11 0 2 Botnet
bad2.example.com (209.165.200.225) 8 8 3 Virus
bad1.cisco.example (10.131.36.158) 6 6 3 Virus
bad2.cisco.example (209.165.201.1) 2 2 3 Trojan
horrible.example.net (10.232.224.2) 2 2 3 Botnet
nono.example.org (209.165.202.130) 1 1 3 Virus
Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009

```

次に、**show dynamic-filter reports top malware-ports** コマンドの出力例を示します。

```

ciscoasa# show dynamic-filter reports top malware-ports
Port
-----
Connections logged
-----
tcp 1000 617
tcp 2001 472
tcp 23 22
tcp 1001 19
udp 2000 17
udp 2001 17
tcp 8080 9
tcp 80 3
tcp >8192 2
Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009

```

次に、**show dynamic-filter reports top infected-hosts** コマンドの出力例を示します。

```

ciscoasa# show dynamic-filter reports top infected-hosts
Host
-----
Connections logged
-----
10.10.10.51 (inside) 1190
10.12.10.10 (inside) 10
10.10.11.10 (inside) 5
Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009

```

関連コマンド

| コマンド | 説明 |
|--|--|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタ コンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNS スヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。 |

| コマンド | 説明 |
|---|--|
| dns server-group | ASA の DNS サーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |
| dynamic-filter enable | アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |
| dynamic-filter updater-client enable | ダイナミックデータベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミックデータベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィックフィルタのホワイトリストを編集します。 |
| inspect dns dynamic-filter-snoop | DNS インспекションとボットネットトラフィックフィルタスヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィックフィルタルールを表示します。 |
| show dynamic-filter data | ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。 |

| コマンド | 説明 |
|---|--|
| show dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNSスヌーピングの概要を表示します。 detail キーワードを指定した場合は、実際のIPアドレスおよび名前を表示します。 |
| show dynamic-filter statistics | ボットネットトラフィックフィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。 |
| show dynamic-filter updater-client | サーバーのIPアドレス、ASAが次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。 |
| show running-config dynamic-filter | ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。 |

show dynamic-filter statistics

ポットネットトラフィックフィルタを使用して、ホワイトリスト、ブラックリスト、およびグレイリストとして分類された接続の数を表示するには、特権 EXEC モードで **show dynamic-filter statistics** コマンドを使用します。

show dynamic-filter statistics [*interface name*] [*detail*]

構文の説明

detail (任意) 各脅威レベルで分類またはドロップされたパケットの数を表示します。

interface name (任意) 特定の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

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容

8.2(1) このコマンドが追加されました。

8.2(2) 各脅威レベルで分類またはドロップされたパケット数を表示するための **detail** キーワードが追加されました。脅威イベントについては、シビラティ（重大度）レベルが警告から通知に変更されました。脅威イベントは5分ごとにトリガーできます。

使用上のガイドライン

グレイリストには、複数のドメイン名に関連付けられているが、これらすべてのドメイン名がブラックリストに記載されているわけではないアドレスが含まれます。

統計情報をクリアするには、**clear dynamic-filter statistics** コマンドを入力します。

例

次に、**show dynamic-filter statistics** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
Total conns classified 11, ingress 11, egress 0
Total whitelist classified 0, ingress 0, egress 0
```

```
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
Total conns classified 1182, ingress 1182, egress 0
Total whitelist classified 3, ingress 3, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

次に、**show dynamic-filter statistics interface outside detail** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
Total conns classified 2108, ingress 2108, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 1, dropped 1, ingress 0, egress 0
  Threat level 5 classified 1, dropped 1, ingress 0, egress 0
  Threat level 4 classified 0, dropped 0, ingress 0, egress 0
  ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
  Threat level 5 classified 6, dropped 6, ingress 4, egress 2
  Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

関連コマンド

| コマンド | 説明 |
|--|--|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタ コンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNS スヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。 |
| dns server-group | ASA の DNS サーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |

| コマンド | 説明 |
|---|---|
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |
| dynamic-filter enable | アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |
| dynamic-filter updater-client enable | ダイナミックデータベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミックデータベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィックフィルタのホワイトリストを編集します。 |
| inspect dns dynamic-filter-snoop | DNSインスペクションとボットネットトラフィックフィルタスヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィックフィルタルールを表示します。 |
| show dynamic-filter data | ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。 |
| show dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNSスヌーピングの概要を表示します。 detail キーワードを指定した場合は、実際のIPアドレスおよび名前を表示します。 |
| show dynamic-filter reports | 上位10個のボットネットサイト、ポート、および感染したホストに関するレポートを生成します。 |
| show dynamic-filter updater-client | サーバーのIPアドレス、ASAが次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。 |

| コマンド | 説明 |
|---------------------------------------|---------------------------------------|
| show running-config dynamic-filter | ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。 |

show dynamic-filter updater-client

ボットネットトラフィックフィルタのアップデータサーバーに関する情報（サーバーの IP アドレス、ASA がサーバーに接続する次のタイミング、インストールされているデータベースのバージョンなど）を表示するには、特権 EXEC モードで **show dynamic-filter updater-client** コマンドを使用します。

show dynamic-filter updater-client

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|----------------------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

コマンド履歴

リリース 変更内容

8.2(1) このコマンドが追加されました。

例

次に、**show dynamic-filter updater-client** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter updater-client
Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

関連コマンド

| コマンド | 説明 |
|----------------|----------------------------------|
| address | IP アドレスをブラックリストまたはホワイトリストに追加します。 |

| コマンド | 説明 |
|---|--|
| clear configure dynamic-filter | 実行ボットネットトラフィックフィルタコンフィギュレーションをクリアします。 |
| clear dynamic-filter dns-snoop | ボットネットトラフィックフィルタのDNSスヌーピングデータをクリアします。 |
| clear dynamic-filter reports | ボットネットトラフィックフィルタのレポートデータをクリアします。 |
| clear dynamic-filter statistics | ボットネットトラフィックフィルタの統計情報をクリアします。 |
| dns domain-lookup | サポートされているコマンドに対してネームルックアップを実行するために、ASAがDNSサーバーにDNS要求を送信できるようにします。 |
| dns server-group | ASAのDNSサーバーを指定します。 |
| dynamic-filter ambiguous-is-black | グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。 |
| dynamic-filter blacklist | ボットネットトラフィックフィルタのブラックリストを編集します。 |
| dynamic-filter database fetch | ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。 |
| dynamic-filter database find | ドメイン名またはIPアドレスをダイナミックデータベースから検索します。 |
| dynamic-filter database purge | ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。 |
| dynamic-filter drop blacklist | ブラックリストに登録されているトラフィックを自動でドロップします。 |
| dynamic-filter enable | アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。 |
| dynamic-filter updater-client enable | ダイナミックデータベースのダウンロードをイネーブルにします。 |
| dynamic-filter use-database | ダイナミックデータベースの使用をイネーブルにします。 |
| dynamic-filter whitelist | ボットネットトラフィックフィルタのホワイトリストを編集します。 |

| コマンド | 説明 |
|---|--|
| inspect dns dynamic-filter-snoop | DNS インスペクションとボットネットトラフィックフィルタスヌーピングをイネーブルにします。 |
| name | ブラックリストまたはホワイトリストに名前を追加します。 |
| show asp table dynamic-filter | 高速セキュリティパスにインストールされているボットネットトラフィック フィルタルールを表示します。 |
| show dynamic-filter data | ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。 |
| show dynamic-filter dns-snoop | ボットネットトラフィック フィルタの DNS スヌーピングの概要を表示します。 detail キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。 |
| show dynamic-filter reports | 上位 10 個のボットネットサイト、ポート、および感染したホストに関するレポートを生成します。 |
| show dynamic-filter statistics | ボットネットトラフィック フィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。 |
| show running-config dynamic-filter | ボットネットトラフィック フィルタの実行コンフィギュレーションを表示します。 |

show eigrp events

EIGRP イベントログを表示するには、特権 EXEC モードで **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

| | |
|------------------|--|
| <i>as-number</i> | (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。ASA 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。 |
| <i>end</i> | (任意) 出力されるエントリを、インデックス番号 <i>start</i> で開始され、インデックス番号 <i>end</i> で終了するエントリに限定します。 |
| <i>start</i> | (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、 <i>end</i> 引数で指定されたイベントで終了します。有効な値は、1 ~ 4294967295 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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容

8.0(2) このコマンドが追加されました。

9.0(1) マルチコンテキスト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

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。ネイバー変更イベントのロギングは、**no eigrp log-neighbor-changes** コマンドを使用してディセーブルにできます。ネイバー警告イベントのロギングは、**no eigrp log-neighbor-warnings** コマンドを使用してディセーブルにできます。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。

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# 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

| コマンド | 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。 |

| コマンド | 説明 |
|------------------------------------|----------------------------|
| eigrp log-neighbor-changes | ネイバー変更イベントのロギングをイネーブルにします。 |
| eigrp log-neighbor-warnings | ネイバー警告イベントのロギングをイネーブルにします。 |

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、特権 EXEC モードで **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

| | |
|------------------|--|
| <i>as-number</i> | (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。ASA 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。 |
| <i>if-name</i> | (任意) nameif コマンドで指定された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。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容

8.0(2) このコマンドが追加されました。

9.0(1) マルチコンテキスト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

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。

```
ciscoasa# show eigrp interfaces
EIGRP-IPv4 interfaces for process 100
Interface      Peers    Xmit Queue Un/Reliable  Mean   Pacing Time  Multicast  Pending
                Un/Reliable  SRTT   Un/Reliable  SRTT   Un/Reliable  Flow Timer  Routes
mgmt            0         0/0      0            0      11/434       0          0
outside        1         0/0      337          0      0/10         0          0
inside         1         0/0      10           10     1/63        103         0
```

表 6-2 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 2: *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 | ASA 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。 |

関連コマンド

| コマンド | 説明 |
|----------------|---|
| network | EIGRP ルーティングプロセスに参加するネットワークおよびインターフェイスを定義します。 |

show eigrp neighbors

EIGRP ネイバーテーブルを表示するには、特権 EXEC モードで **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。ASA 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) **nameif** コマンドで指定された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) **neighbor** コマンドを使用してスタティックに定義された 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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリース 変更内容
ス

8.0(2) このコマンドが追加されました。

9.0(1) マルチコンテキスト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

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。

```
ciscoasa# 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
```

表 6-2 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 3: **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 | ASA 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。 |
| 保留時間 (Holdtime) | ASA 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。 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。 この値が 0 に達すると、ASA は、ネイバーを到達不能と見なします。 |
| Uptime | ASA 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 | ASA 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、ASA 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、ASA 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。

```
ciscoasa# show eigrp neighbors static
EIGRP-IPv4 neighbors for process 100
Static Address      Interface
192.168.1.5         management
```

表 6-4 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 4: `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 | ASA 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。 |

例

次に、`show eigrp neighbors detail` コマンドの出力例を示します。

```
ciscoasa# 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
```

表 5: `show ip eigrp neighbors details` のフィールドの説明 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 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 | ASA 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 |
|--------------------|---|
| 保留時間 (Holdtime) | ASA 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。 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。 この値が0に達すると、ASA は、ネイバーを到達不能と見なします。 |
| Uptime | ASA 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、ASA 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、ASA 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 | ASA 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)。 |

関連コマンド

| コマンド | 説明 |
|------------------------------|----------------------------|
| clear eigrp neighbors | EIGRP ネイバー テーブルをクリアします。 |
| debug eigrp neighbors | EIGRP ネイバーデバッグメッセージを表示します。 |
| debug ip eigrp | EIGRP パケットデバッグメッセージを表示します。 |

show eigrp topology

EIGRP トポロジテーブルを表示するには、特権 EXEC モードで **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。 |
| <i>as-number</i> | (任意) EIGRP プロセスの自律システム番号を指定します。ASA 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。 |
| <i>ip-addr</i> | (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。 |
| <i>mask</i> | (オプション) <i>ip-addr</i> 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。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリー 変更内容
ス

8.0(2) このコマンドが追加されました。

リリース 変更内容
ス

9.0(1) マルチコンテキスト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 `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。

コマンド履歴

```
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
```

表 6-6 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 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 <i>n</i> 個（ <i>n</i> 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。 |
| (<i>cost /adv_cost</i>) | 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 番目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。 |
| <i>interface</i> | 情報の学習元のインターフェイス。 |

コマンド履歴

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。

```
ciscoasa# 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。

```
ciscoasa# 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

| コマンド | 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

送受信された EIGRP パケットの数を表示するには、特権 EXEC モードで **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。ASA 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。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | — | • 対応 | • 対応 | — |

コマンド履歴

リリー 変更内容
ス

8.0(2) このコマンドが追加されました。

9.0(1) マルチコンテキスト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

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。

```
ciscoasa# 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
```

表 6-4 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 7: 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 |
| 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。 |

関連コマンド

| コマンド | 説明 |
|-----------------------------|---------------------------------|
| debug eigrp packets | 送受信された EIGRP パケットのデバッグ情報を表示します。 |
| debug eigrp transmit | 送信された EIGRP メッセージのデバッグ情報を表示します。 |

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、特権 EXEC モードで **show environment** コマンドを使用します。

show environment [**alarm-contact** | **driver** | **fans** | **power-consumption** | **power-supply** | **temperature**] [**chassis** | **cpu** | **voltage**]

| 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。 |
| | chassis | (任意) 温度表示をシャーシに限定します。 |
| | cpu | (任意) 温度表示をプロセッサに限定します。 |
| | driver | <p>(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。</p> <ul style="list-style-type: none"> • RUNNING : ドライバは動作中です。 • STOPPED : エラーが原因でドライバが停止しています。 |
| | fans | <p>(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。</p> <ul style="list-style-type: none"> • OK : ファンは正常に動作中です。 • Failed : ファンが故障しているため交換が必要です。 <p>デュアルファンモジュールを取り外す際に、ファンの実際のステータスを表示するには、show environment basic および show environment expand FXOS コマンドを使用します。</p> |
| | power-consumption | (オプション) PoE インターフェイスの電力消費量を表示します。 |

power-supply

(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。

- **OK** : 電源は正常に動作中です。
- **Failed** : 電源が故障しているため交換が必要です。
- **Not Present** : 指定された電源が設置されていません。

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。

- **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。
- **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。
- **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。

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。ステータスは次のいずれかになります。

- **OK** : 温度は通常の動作範囲内にあります。
- **Critical** : 温度は通常の動作範囲外です。

voltage

(任意) CPU 電圧チャンネル 1 ~ 24 の値を表示します。動作ステータスは除きます。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

コマンド履歴

リリース 変更内容

8.1(1) このコマンドが追加されました。

8.4(2) ASA 5585-X SSP の出力が追加されました。さらに、デュアル SSP インストールのサポートが追加されました。

8.4.4(1) ASA 5515-X、ASA 5525-X、5545-X、および ASA 5555-X で表示される電源温度が、出力で変更されました。

8.6(1) ASA 5545-X および ASA 5555-X の CPU 電圧レギュレータ温度イベントの出力が追加されました。電源入力ステータスの出力が追加されました。電圧センサーの出力が追加されました。

9.7(1) ISA 3000 用に **alarm-contact** キーワードが追加されました。

9.13(1) Firepower 1010 PoE インターフェイスに **power-consumption** 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。



(注) デュアル SSP インストールの場合、冷却ファンおよび電源の出力は、シャーシマスターのセンサーによってのみ示されます。

例

次に、**show environment** コマンドの一般的な出力例を示します。

```
ciscoasa# 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。

```

ciscoasa# 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、ASA 5555-X の場合の **show environment** コマンドの出力例を示します。

```

ciscoasa# show environment
Cooling Fans:
-----
Chassis Fans:
-----
Power Supplies:
-----
Left Slot (PS0): 9728 RPM - OK
Right Slot (PS1): 0 RPM - OK
Power Supplies:
-----
Left Slot (PS0): Present
Right Slot (PS1): Present

Power Input:
-----
Left Slot (PS0): OK
Right Slot (PS1): Failure Detected
Temperature:
-----
Left Slot (PS0): 29 C - OK
Right Slot (PS1): N/A
Processors:
-----
Processor 1: 81.0 C - OK
Chassis:
-----
Ambient 1: 39.0 C - OK (Chassis Back Temperature)
Ambient 2: 32.0 C - OK (Chassis Front Temperature)
Ambient 3: 47.0 C - OK (Chassis Back Left Temperature)
Power Supplies:
-----
Left Slot (PS0): 33 C - OK
Right Slot (PS1): -128 C - OK

```

次に、デュアル SSP インストールの ASA 5585-X シャーシマスターの場合の **show environment** コマンドの出力例を示します。

```

ciscoasa(config)# show environment
Cooling Fans:
-----
Power Supplies:
-----
Left Slot (PS0): 7000 RPM - OK (Fan Module Fan)
Right Slot (PS1): 6900 RPM - OK (Power Supply Fan)
Power Supplies:
-----
Power Supply Unit Redundancy: N/A
Power Supplies:
-----

```

```

Left Slot (PS0): 64 C - OK (Fan Module Temperature)
Right Slot (PS1): 64 C - OK (Power Supply Temperature)
Power Supplies:
-----
Left Slot (PS0): 7000 RPM - OK (Fan Module Fan)
Right Slot (PS1): 6900 RPM - OK (Power Supply Fan)
Temperature:
-----
Processors:
-----
Processor 1: 48.0 C - OK (CPU1 Core Temperature)
Processor 2: 47.0 C - OK (CPU2 Core Temperature)
Chassis:
-----
Ambient 1: 25.5 C - OK (Chassis Front Temperature)
Ambient 2: 37.5 C - OK (Chassis Back Temperature)
Ambient 3: 31.50 C - OK (CPU1 Back Temperature)
Ambient 4: 27.75 C - OK (CPU1 Front Temperature)
Ambient 5: 38.25 C - OK (CPU2 Back Temperature)
Ambient 6: 34.0 C - OK (CPU2 Front Temperature)
Power Supplies:
-----
Left Slot (PS0): 64 C - OK (Fan Module Temperature)
Right Slot (PS1): 64 C - OK (Power Supply Temperature)
Voltage:
-----
Channel 1: 3.310 V - (3.3V (U142 VX1))
Channel 2: 1.492 V - (1.5V (U142 VX2))
Channel 3: 1.053 V - (1.05V (U142 VX3))
Channel 4: 3.328 V - (3.3V_STDBY (U142 VP1))
Channel 5: 11.675 V - (12V (U142 VP2))
Channel 6: 4.921 V - (5.0V (U142 VP3))
Channel 7: 6.713 V - (7.0V (U142 VP4))
Channel 8: 9.763 V - (IBV (U142 VH))
Channel 9: 1.048 V - (1.05VB (U209 VX2))
Channel 10: 1.209 V - (1.2V (U209 VX3))
Channel 11: 1.109 V - (1.1V (U209 VX4))
Channel 12: 0.999 V - (1.0V (U209 VX5))
Channel 13: 3.324 V - (3.3V STDBY (U209 VP1))
Channel 14: 2.504 V - (2.5V (U209 VP2))
Channel 15: 1.799 V - (1.8V (U209 VP3))
Channel 16: 1.899 V - (1.9V (U209 VP4))
Channel 17: 9.763 V - (IBV (U209 VH))
Channel 18: 2.048 V - (VTT CPU0 (U83 VX2))
Channel 19: 2.048 V - (VTT CPU1 (U83 VX3))
Channel 20: 2.048 V - (VCC CPU0 (U83 VX4))
Channel 21: 2.048 V - (VCC CPU1 (U83 VX5))
Channel 22: 1.516 V - (1.5VA (U83 VP1))
Channel 23: 1.515 V - (1.5VB (U83 VP2))
Channel 24: 8.937 V - (IBV (U83 VH))

```

CPU 電圧レギュレータ温度イベントにより ASA がシャットダウンされた場合は、次の警告メッセージが表示されます。

```

WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the
max thermal operating temperature. The chassis and CPU need to be inspected immediately
for ventilation issues.

```

詳細については、syslog メッセージガイドの syslog メッセージ 735024 を参照してください。

次に、`ssh show environment alarm-contact` コマンドの出力例を示します。

```

ciscoasa> 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

```

次に、ドライバエラー統計情報の例を示します。

```

Driver Error Statistics:
-----
I2C I/O Errors      : 0
GPIO Errors         : 0
Ioctl Null Ptr Errors : 0
Poll Errors         : 0
Invalid Ioctl Errors : 0
PECI Errors         : 3
Unknown Errors      : 0

```

PECI エラーは、CPU 温度データの取得時に問題が発生していることを示します。エラーカウント数は、温度データの取得に失敗した回数です。

関連コマンド

| コマンド | 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 relay | 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 event manager

設定された各イベント マネージャ アプレットに関する情報を表示するには、特権 EXEC モードで **show event manager** コマンドを使用します。

show event manager

構文の説明

このコマンドには引数またはキーワードはありません。

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 モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|-------------------|-------------|-----------|--------------|--------|------|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

例

次に、**show event manager** コマンドの出力例を示します。

```
ciscoasa# show event manager
event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

関連コマンド

| コマンド | 説明 |
|--|----------------------------------|
| show running-config event manager | イベント マネージャ の実行コンフィギュレーションを表示します。 |

翻訳について

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