



show p ~ show r

- [show packet tracer](#) (3 ページ)
- [show packet-statistics](#) (5 ページ)
- [show pager](#) (8 ページ)
- [show path-monitoring](#) (9 ページ)
- [show password encryption](#) (11 ページ)
- [show perfmon](#) (12 ページ)
- [show phone-proxy](#) (廃止予定) (14 ページ)
- [show pim bsr-router](#) (16 ページ)
- [show pim df](#) (17 ページ)
- [show pim group-map](#) (19 ページ)
- [show pim interface](#) (21 ページ)
- [show pim join-prune statistic](#) (23 ページ)
- [show pim neighbor](#) (25 ページ)
- [show pim range-list](#) (27 ページ)
- [show pim topology](#) (29 ページ)
- [show pim topology reserved](#) (31 ページ)
- [show pim topology route-count](#) (33 ページ)
- [show pim traffic](#) (34 ページ)
- [show pim tunnel](#) (36 ページ)
- [show policy-list](#) (38 ページ)
- [show policy-route](#) (40 ページ)
- [show port-channel](#) (41 ページ)
- [show port-channel load-balance](#) (46 ページ)
- [show power inline](#) (49 ページ)
- [show prefix-list](#) (52 ページ)
- [show priority-queue](#) (54 ページ)
- [show processes](#) (56 ページ)
- [show ptp](#) (61 ページ)
- [show quota management-session](#) (63 ページ)

- [show raid](#) (65 ページ)
- [show reload](#) (70 ページ)
- [show resource allocation](#) (71 ページ)
- [show resource types](#) (75 ページ)
- [show resource usage](#) (77 ページ)
- [show rest-api agent](#) (82 ページ)
- [show rip database](#) (84 ページ)
- [show rollback-status](#) (86 ページ)
- [show route](#) (91 ページ)
- [show running-config](#) (97 ページ)

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
ユーザー EXEC または 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
	9.17.1	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。

```
ciscoasa# 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

コマンド	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情報を表示するには、**show packet-statistics** コマンドを使用します。

show packet-statistics *interface_id* [**brief**]

構文の説明

interface_id 統計情報が表示されているインターフェイス ID。

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
ユーザー EXEC または 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
9.18(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 packet-statistics コマンドは、オペレーティングシステムの複数ソース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、次のコマンドの出力を統合します。

- FXOS :
 - **show portmanager counters ethernet**
 - **show queuing interface ethernet**
 - **show portmanager counters internal**
 - **show queuing interface internal**
 - **show portmanager switch counters packet-trace**
- FPGA : **show npu-accel statistics**
- ASA :
 - **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。

例

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

```
ciscoasa# show packet-statistics Ethernet 1/1
===== show portmanager counters Ethernet 1 1 =====
Good Octets Received : 66882
Bad Octets Received : 0
MAC Transmit Error : 0
...
===== show queuing interface Ethernet 1 1 =====
Queue Traffic-type Scheduler-type oper-bandwidth Destination
-----
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
...
===== show portmanager counters Internal 1 1 =====
Good Octets Received : 3770
Bad Octets Received : 0
MAC Transmit Error : 0
...
===== show queuing interface Internal 1 1 =====
Queue Traffic-type Scheduler-type oper-bandwidth Destination
-----
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
...
===== show portmanager switch counters packet-trace =====
Counter Source port- 0/0 Destination port- 0/0
-----
goodOctetsRcv --- ---
badOctetsRcv --- ---
Ingress counters
gtBrgInFrames 5 5
gtBrgVlanIngFilterDisc 0 0
...
===== show npu-accel statistics =====
module: kc50-pcie, pipe: 0
-----
reg_pcie_rcv_reg_access_rd_tlp_cnt = 1312987327
reg_pcie_rcv_reg_access_wr_tlp_cnt = 227526828
...
===== show interface detail =====
Interface Ethernet1/1 "", is admin down, line protocol is down
```

```
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Auto-Duplex, Auto-Speed
Available but not configured via nameif
MAC address f87a.410e.5994, MTU not set
...
...
===== show asp drop =====
Frame drop:
Slowpath security checks failed (sp-security-failed) 18
FP L2 rule drop (l2_acl) 118
Interface is down (interface-down) 11
Last clearing: Never
```

show pager

インターフェイスのデフォルトルートまたはスタティックルートを表示するには、特権 EXEC モードで **show pager** コマンドを使用します。

show pager

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	• 対応

コマンド履歴

リリー 変更内容
ス

4.0(1) このコマンドが追加されました。

例

次に、**show pager** コマンドの出力例を示します。

```
ciscoasa(config)# show pager
pager lines 0
```

関連コマンド

コマンド	説明
clear configure pager	Telnetセッションで「---More---」プロンプトまでに表示されるよう設定されている行数を実行コンフィギュレーションから削除します。
show running-config pager	実行コンフィギュレーションに Telnet セッションで「---More---」プロンプトまでに表示されるよう設定されている行数を表示します。
terminal pager	Telnetセッションで「---More---」プロンプトまでに表示する行数を設定します。このコマンドは実行コンフィギュレーションに保存されません。

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
9.18(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。

```
ciscoasa# 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。

```
ciscoasa#
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

コマンド	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 password encryption

パスワード暗号化のコンフィギュレーション設定を表示するには、特権 EXEC モードで **show password encryption** コマンドを使用します。

show password encryption

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
ス

8.3(1) このコマンドが追加されました。

8.4(1) ユーザー コンテキストに show password encryption が追加されました。

使用上のガイドライン

キーが **write memory** コマンドを使用して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。

```
ciscoasa# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

関連コマンド

コマンド	説明
password encryption aes	パスワードの暗号化をイネーブルにします。
key config-key password-encrypt	暗号キーを生成するために使用されるパスフレーズを設定します。

show perfmon

ASA のパフォーマンスに関する情報を表示するには、特権 EXEC モードで **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 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) このコマンドのサポートが ASA に追加されました。

7.2(1) **detail** キーワードが追加されました。

使用上のガイドライン

このコマンドの出力は、Telnet セッションには表示されません。

perfmon コマンドでは、指定した間隔でパフォーマンス統計情報が連続的に表示されます。show perfmon コマンドを使用すると、すぐに情報を表示できます。



(注) ASA では、現在および平均のカウンタ数を正確な値で計算して表示するのに時間がかかります。現在の値に対する Perfmon の統計更新間隔のデフォルト値は 120 秒です。平均カウンタは、最後に **clear perfmon** が実行されたときから、またはデバイスを起動してからコマンドが使用されなかったときの値の平均に基づいて計算されます。

例

次に、**show perfmon** コマンドの出力例を示します。

```
ciscoasa(config)# show perfmon
```

```
Context: my_context
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
WebSns Req         0/s        0/s
TCP Fixup           0/s        0/s
TCP Intercept      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
```

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

```
ciscoasa(config)# 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

コマンド	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 phone-proxy (廃止予定)

phone-proxy 固有の情報を表示するには、グローバル コンフィギュレーション モードで **show phone-proxy** コマンドを使用します。

show phone-proxy [**media-sessions** [**detail**] | **signaling-sessions** [**detail**] | **secure-phones**]

構文の説明

detail	詳細情報を表示します。
media-sessions	電話プロキシによって保存されている、対応するメディア セッションを表示します。また、メディアセッションが確立されているインターフェイスに設定されているメディアターミネーションアドレスを表示します。
secure-phones	データベースに格納されているセキュア モードに対応した電話を表示します。
signaling-sessions	電話プロキシに保存されている、対応するシグナリングセッションを表示します。

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	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
8.2(1)	コマンドが更新され、 media-sessions キーワードを指定しても、メディアセッションが確立されているインターフェイスに設定されたメディアターミネーションアドレスが表示されるようになりました。
9.4(1)	このコマンドは、すべての phone-proxy モードコマンドとともに廃止されました。

例

次に、**show phone proxy** コマンドを使用して電話プロキシ固有の情報を表示する例を示します。

```
ciscoasa
(config)#
show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address      Port  MAC                Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c    0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663    0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804    0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8    0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69    0:05:00 0:00:04
ciscoasa
(config)#
```

次に、**show phone proxy** コマンドを使用して、データベースに保存されている、セキュアモードに対応した電話を表示します。

```
ciscoasa
(config)#
show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used
Interface/IP Address      MAC                Timeout  Idle
-----
outside:69.181.112.219    001e.7ac4.da9c    0:05:00 0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00 0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00 0:00:09
ciscoasa
(config)#
```

次に、**show phone proxy** コマンドを使用して、正常に完了したコールの出力と、メディアセッションが確立されているインターフェイスに設定されたメディアターミネーションアドレスを表示する例を示します。

```
ciscoasa
(config)#
show phone-proxy media-sessions

Media-session: 128.106.254.3/1168 refcnt 6
<---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
<---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

関連コマンド

コマンド	説明
debug phone-proxy	電話プロキシインスタンスからのデバッグメッセージを表示します。
phone proxy	Phone Proxy インスタンスを設定します。

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

構文の説明

引数または変数はありません。

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
ユーザー EXEC または 特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

9.5(2) このコマンドが追加されました。

例

次に、show pim bsr-router コマンドの出力例を示します。

```
ciscoasa# 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、ユーザー EXEC モードまたは特権 EXEC モードで **show pim df** コマンドを使用します。

show pim df [**winner**] [*rp_address* / *if_name*]

構文の説明

rp_address 次のいずれか 1 つを指定できます。

- RP の名前。ドメインネームシステム (DNS) の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。
- 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。

if_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
ユーザー EXEC または特権 EXEC	• 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、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。

```
ciscoasa# 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/プロトコル マッピング テーブルを表示するには、特権 EXEC モードで **show pim group-map** コマンドを使用します。

show pim group-map [**info-source**] [*group*]

構文の説明

<i>group</i>	(任意) 次のいずれかを指定できます。 <ul style="list-style-type: none"> マルチキャストグループの名前。DNS の hosts テーブルに定義されているものか、ドメインの ipv4 host コマンドで定義したものです。 マルチキャストグループの 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。
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	—	—

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。
9.5(2)	このコマンドは変更され、 rp-timers 変数が組み込まれました。

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、ASA 上でさまざまなクライアントから学習されます。

ASA 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。

pim rp-address コマンドで複数の RP を設定した場合は、適切なグループ範囲が対応する RP とともに表示されます。グループに選択した RP を表示するには、**show pim group-map** コマンドでグループアドレスまたは名前を指定します。

例

次に、**show pim group-map** コマンドの出力例を示します。

```
ciscoasa# 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。

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。
pim rp-address	PIM ランデブー ポイント (RP) のアドレスを設定します。

show pim interface

PIMに関するインターフェイス固有の情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim interface** コマンドを使用します。

show pim interface [*if_name* | **state-off** | **state-on**]

構文の説明

if_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 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
ユーザー EXEC または 特権 EXEC	• 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。

使用上のガイドライン

ASA の PIM 実装は、ASA 自体を PIM ネイバーと見なします。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。

```
ciscoasa# show pim interface inside
Address   Interface   Ver/   Nbr   Query   DR   DR
          Interface   Mode   Count Intvl   Prior
172.16.1.4 inside   v2/S   2     100 ms  1     172.16.1.4
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

show pim join-prune statistic

PIMの加入とプルーンに関する集約的な統計情報を表示するには、ユーザー EXEC モードと特権 EXEC モードで **show pim join-prune statistics** コマンドを使用します。

show pim join-prune statistics [*if_name*]

構文の説明

if_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、加入とプルーンに関する統計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
ユーザー EXEC または 特権 EXEC	• 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。

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。

```
ciscoasa# show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface      Transmitted      Received
               0 / 0 / 0        0 / 0 / 0
   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

コマンド	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、ユーザー EXEC モードまたは特権 EXEC モードで **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
ユーザー EXEC または 特権 EXEC	• 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、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。

ASA の PIM 実装は、ASA 自体を PIM ネイバーと見なします。したがって、ASA 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。ASA 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。

```

ciscoasa# 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

```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

show pim range-list

PIM の範囲リストの情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim range-list** コマンドを使用します。

show pim range-list [*rp_address*]

構文の説明

rp_address 次のいずれか 1 つを指定できます。

- RP の名前。ドメインネームシステム (DNS) の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。
- 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
ユーザー EXEC または 特権 EXEC	• 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。

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。

```
ciscoasa# 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

コマンド	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 トポロジテーブルの情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology [*group*] [*source*]

構文の説明

group (任意) 次のいずれかを指定できます。

- マルチキャストグループの名前。DNS の **hosts** テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。
- マルチキャストグループの 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。

source (任意) 次のいずれかを指定できます。

- マルチキャスト送信元の名前。DNS の **hosts** テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。
- マルチキャスト送信元の 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
ユーザー EXEC または 特権 EXEC	• 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。

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。

```
ciscoasa# 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
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルを表示します。
show pim topology 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。

show pim topology reserved

予約済みグループに関するPIMトポロジテーブルの情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim topology reserved** コマンドを使用します。

show pim topology reserved

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
ユーザー EXEC または 特権 EXEC	• 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。

例

次に、**show pim topology reserved** コマンドの出力例を示します。

```
ciscoasa# 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
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジテーブルを表示します。

show pim topology route-count

PIM トポロジテーブルのエントリの数を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim topology route-count** コマンドを使用します。

show pim topology route-count [detail]

構文の説明

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。

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
ユーザー EXEC または 特権 EXEC	• 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。

使用上のガイドライン

このコマンドは、PIM トポロジテーブルのエントリの数を表示します。エントリに関する詳細な情報を表示するには、**show pim topology** コマンドを使用します。

例

次に、**show pim topology route-count** コマンドの出力例を示します。

```
ciscoasa# 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

コマンド	説明
show pim topology	PIM トポロジテーブルを表示します。

show pim traffic

PIMトラフィックのカウンタを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show pim traffic** コマンドを使用します。

show pim traffic

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
ユーザー EXEC または 特権 EXEC	• 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

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。

```
ciscoasa# 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

コマンド	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、ユーザーEXECモードまたは特権EXECモードで **show pim tunnel** コマンドを使用します。

show pim tunnel [*if_name*]

構文の説明

if_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
ユーザーEXECまたは特権EXEC	• 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。

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、送信元最初のホップDR ルータから 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。

```
ciscoasa# show pim tunnel
Interface      RP Address Source Address
Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

関連コマンド

コマンド	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のエントリに関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **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 デフォルト

ポリシー リストの名前を指定しない場合、このコマンドはすべてのポリシー リストを表示します。

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
ユーザー EXEC または 特権 EXEC	• 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。

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。

```
ciscoasa# 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
```

関連コマンド

コマンド	説明
policy-list	ポリシーリストを設定します。

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、ユーザー EXEC モードまたは特権 EXEC モードで **show policy-route** コマンドを使用します。

show policy-route

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
ユーザー EXEC または 特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.4(1) このコマンドが追加されました。

例

次に、**show policy-list** コマンドの出力例を示します。

```
ciscoasa# show policy-route

Interface          Route map
GigabitEthernet0/0 equal-access
```

関連コマンド

コマンド	説明
policy-route	ポリシーベースルーティングを設定します。

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、特権 EXEC モードで **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。
<i>channel_group_number</i>	(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

8.4(1) このコマンドが追加されました。

例

次に、**show port-channel** コマンドの出力例を示します。

```
ciscoasa# 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。

```

ciscoasa# 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。

```

ciscoasa# 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 LACPDU     F - Device is sending fast LACPDU.
      A - Device is in active mode.          P - Device is in passive mode.
Local information:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/1	SA	bndl	32768	0x1	0x1	0x302	0x3d

```

Partner's information:

```

Port	Flags	Partner State	LACP Partner Port	Partner Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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 LACPDU     F - Device is sending fast LACPDU.
      A - Device is in active mode.          P - Device is in passive mode.
Local information:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/2	SA	bndl	32768	0x1	0x1	0x303	0x3d

```

Partner's information:

```

Port	Flags	Partner State	LACP Partner Port	Partner Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/3	SA	bndl	32768	0x1	0x1	0x304	0x3d

```

Partner's information:

```

Port	Flags	State	Partner Port	Partner Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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。

```

ciscoasa# 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:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/1	SA	bndl	32768	0x1	0x1	0x302	0x3d

```

Partner's information:

```

Port	Flags	State	Partner Port	Partner Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/2	SA	bndl	32768	0x1	0x1	0x303	0x3d

```

Partner's information:

```

Port	Flags	State	Partner Port	Partner Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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 LACPDU      F - Device is sending fast LACPDU.
        A - Device is in active mode.          P - Device is in passive mode.
Local information:

```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi3/3	SA	bndl	32768	0x1	0x1	0x304	0x3d

```

Partner's information:

```

Port	Partner Flags	Partner State	LACP Partner Port Priority	Partner Admin Key	Partner Oper Key	Partner Port Number	Partner 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。

```

ciscoasa# show port-channel protocol
Channel-group listing:
-----
Group: 1
-----
Protocol: LACP

```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャンネルグループで許可されるアクティブインターフェイスの最大数を指定します。
lacp port-priority	チャンネルグループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャンネルインターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
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	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ンネルの情報も表示します。

コマンド	説明
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、特権 EXEC モードでこの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 | vlan-only number } parameters ]
```

構文の説明

channel_group_number EtherChannel チャンネル 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 (オプション) パケットの VLAN ID を指定します。

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。

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
8.4(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

デフォルトでは、ASA 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。アルゴリズムを変更するには、**port-channel load-balance** コマンドを参照してください。

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 14port 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。

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# show port-channel 1 load-balance hash-result 14port source 5
Would select GigabitEthernet3/2 of Port-channell based on algorithm src-dst-ip
```

関連コマンド	コマンド	説明
	channel-group	EtherChannel にインターフェイスを追加します。
	interface port-channel	EtherChannel を設定します。
	lacp max-bundle	チャンネルグループで許可されるアクティブ インターフェイスの最大数を指定します。
	lacp port-priority	チャンネルグループの物理インターフェイスのプライオリティを設定します。
	lacp system-priority	LACP システム プライオリティを設定します。
	port-channel load-balance	ロード バランシング アルゴリズムを設定します。
	port-channel min-bundle	ポートチャンネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
	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ンネルの情報も表示します。
	show port-channel load-balance	ポートチャン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 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、ユーザー EXEC モードで **show power inline** コマンドを使用します。

show power inline



(注) Firepower 1010 および ASA 5505 でのみサポートされています。

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
ユーザー 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。

9.13(1) Firepower 1010 のサポートが追加されました。

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と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。ASA 5505 では、イーサネット 0/6 および 0/7 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。

```
ciscoasa# 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

```

次に、ASA 5505 での **show power inline** コマンドの出力例を示します。

```

ciscoasa# show power inline
Interface      Power   Device
-----
Ethernet0/0    n/a    n/a
Ethernet0/1    n/a    n/a
Ethernet0/2    n/a    n/a
Ethernet0/3    n/a    n/a
Ethernet0/4    n/a    n/a
Ethernet0/5    n/a    n/a
Ethernet0/6    On     Cisco
Ethernet0/7    Off    n/a

```

表 11-1 に、各フィールドの説明を示します。

表 1: 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)	ASA 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まれます。
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。
デバイス	(ASA 5505) 給電されるデバイスのタイプを表示します。Cisco または IEEE のいずれかです。デバイスが給電されていない場合、値は n/a です。デバイスの給電が Cisco の場合、ディスプレイには Cisco と表示されます。IEEE は、デバイスの給電が IEEE 802.3af 準拠であることを示します。
クラス	(Firepower 1010) 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)	(Firepower 1010) 使用中の電流を表示します。
電圧 (V)	(Firepower 1010) 使用中の電圧を表示します。

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
clear interface	show interface コマンドのカウンタをクリアします。

コマンド	説明
interface	インターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
power inline	PoE を有効または無効にします。
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 prefix-list

設定されたプレフィックスリストに関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show prefix-list** コマンドを使用します。

```
show prefix-list [ summary | detail ] [ policy_list_name [ seq sequence_number | network/length [ longer | first-match ] ] ]
```

構文の説明

<i>policy_list_name</i>	(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。
summary	(オプション) 要約された追加統計情報を表示します。
detail	(オプション) 要約された追加統計情報と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。
<i>network/length</i> [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。

次のキーワードを追加することで、一致条件を変更できます。

- **longer** : 指定された *network/length* と一致するか、または (より限定的な) 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。
- **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 デフォルト

プレフィックスリストの名前を指定しない場合、このコマンドはすべてのプレフィックスリストを表示します。他のキーワードを含めない場合、出力にはプレフィックスリストのエントリだけが表示されます。

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
ユーザー EXEC または 特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(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

ルート マップとポリシー リストの一致基準としてルーティングでプレフィックス リストを使用します。

例

次に、**show prefix-list** コマンドの出力例を示します。

```
ciscoasa# show prefix-list

prefix-list prefix_1: 1 entries
  seq 1 permit 2.0.0.0/8
```

次に、要約された出力の例を示します。

```
ciscoasa# show prefix-list summary

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:  Description: FirstPrefixList
  count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
```

次に、詳細な出力の例を示します。

```
ciscoasa# show prefix-list detail

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:  Description: FirstPrefixList
  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

コマンド	説明
prefix-list	プレフィックスリストを設定します。

show priority-queue

インターフェイスのプライオリティキューの構成または統計情報を表示するには、特権 EXEC モードで **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 デフォルト

インターフェイス名を省略した場合は、すべての設定済みインターフェイスについての構成またはプライオリティ キュー統計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
ス

7.0(1) このコマンドが追加されました。

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。

```
ciscoasa# 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
ciscoasa#

```

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。

```

ciscoasa# 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
ciscoasa#

```

関連コマンド

コマンド	説明
clear configure priority-queue	指定されたインターフェイスからプライオリティキューコンフィギュレーションを削除します。
clear priority-queue statistics	プライオリティキューの統計カウンタをクリアします。
priority-queue	インターフェイスにプライオリティキューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティキューコンフィギュレーションを表示します。

show processes

ASA 上で動作しているプロセスのリストを表示するには、特権 EXEC モードで **show processes** コマンドを使用します。

show processes [**cpu-usage** [[**non-zero**] [**sorted**]] [**cpu-hog** | **memory** | **internals**]

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。

コマンド デフォルト

デフォルトで、このコマンドは ASA で実行されているプロセスを表示します。

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
7.0(1)	このコマンドが追加されました。
7.0(4)	ランタイム値が拡張され、1 ミリ秒以内の精度で表示されるようになりました。
7.2(1)	出力が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。
8.0(1)	cpu-usage キーワードが追加されました。
9.2(1)	出力が拡張され、CPU 占有検出情報が表示されるようになりました。

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、ASA 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	Stack Pointer	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。
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、ASA 上で ASA の 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 processes** 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。

ASA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ASA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、CPUの使用率がゼロではないプロセスのリストを表示する例を示します。この例では、ASA 5555 プラットフォームが、パケット処理といくつかのコントロールプレーンプロセスに2つのDATAPATHスレッドを使用しています。この出力では情報が統合されています。DATAPATHスレッドの命名法は<thread-name>-<core-id>-<process-id>です。そのため、show processの出力から、2332と2333というプロセスIDを持ち、論理コア0と1で実行されている、2つのデータパススレッドがあることが分かります。これらの割合が高い場合は、マシンの負荷を軽減する方法を検討してください。たとえば、VPNを実行している場合は、スプリットトンネリングまたはVPNロードバランシングを検討してください。

```
ciscoasa# sh processes cpu-usage non-zero
Hardware: ASA5555
Cisco Adaptive Security Appliance Software Version 9.9(2)56
ASLR enabled, text region 7f83f20fe000-7f83f65ea5cc
PC Thread 5Sec 1Min 5Min Process
0x00007f83f49338b5 0x00002aaac9ead080 0.0% 0.2% 0.2% vpnfol_thread_timer
0x00007f83f4722e18 0x00002aaac9eddbe0 0.1% 0.0% 0.0% UserFromCert Thread
0x00007f83f4722e18 0x00002aaac9eae9e0 0.7% 0.4% 0.4% Unicorn Proxy Thread
0x00007f83f465b6ec 0x00002aaac9ece1c0 0.4% 0.4% 0.4% Logger
0x00007f83f4272a53 0x00002aaac9ec3b00 0.1% 0.1% 0.1% Crypto CA
0x00007f83f2f97df9 0x00002aaac9ebcaa0 0.2% 0.2% 0.2% CP Processing
0x00007f83f52277ed 0x00002aaac9ed1480 0.0% 0.1% 0.0% Checkheaps
0x00007f83f42c8c83 0x00002aaac9ec3760 0.1% 0.0% 0.0% CERT API
0x00007f83f347b722 0x00002aaac9eb7740 0.1% 0.1% 0.1% ARP Thread
- - 37.1% 36.8% 36.3% DATAPATH-0-2332
- - 37.2% 36.8% 36.3% DATAPATH-1-2333
```

次に、ASA上で実行されているプロセスのリストを表示する例を示します。

```
ciscoasa# show processes
PC SP STATE Runtime SBASE Stack Process
Hsi 00102aa0 0a63f288 0089b068 117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068 10 0a64140c 3824/4096 FragDBG
Hwe 004257c8 0a7cacd4 0082dfd8 0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0 20 0a7cb474 3560/4096 dbgtrace
<--- More --->
- - - 638515 - - scheduler
- - - 2625389 - - total
```

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。

```
ciscoasa# show proc cpu-usage non-zero
PC Thread 5Sec 1Min 5Min Process
0818af8e d482f92c 0.1% 0.1% 0.1% Dispatch Unit
```

```
08bae136    d48180f0    0.1%    0.0%    0.2%    ssh
-----
```

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。

```
ciscoasa# show processes cpu-hog
Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
Sample count: 10000 Threshold: 10ms
Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
Sample count: 10000 Threshold: 10ms
The remainder of the CPU hog traceback follows:
Process: DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
LASTHOG At: 15:42:21 UTC Jan 6 2014
PC: 0x0000000000000000 (suspend)
Call stack: 0x000000000041c98c 0x000000000041cc99 0x0000000000069b0f0
0x000000000013619af 0x0000000000136cbbd 0x00000000001372203
0x000007ffffeab2f3a
Interrupt based hog #1
Hog #1, traceback #1, at: 15:41:16 UTC Jan 6 2014, hog 20 ms
PC: 0x0000000000eb616b
Call stack: 0x0000000001360281 0x000007ffffeaba5f0 0x0000000000ebcf71
0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x00000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x000000000013619af
Hog #1, traceback #2, at: 15:41:16 UTC Jan 6 2014, hog 21 ms
PC: 0x0000000000e8fc41
Call stack: 0x0000000001360281 0x000007ffffeaba5f0 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x00000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x000000000013619af 0x0000000000136cbbd
0x00000000001372203 0x000007ffffeab2f3a
Interrupt based hog #2
Hog #2, traceback #1, at: 15:41:36 UTC Jan 6 2014, hog 9 ms
PC: 0x0000000000eb6167
Call stack: 0x0000000001360281 0x000007ffffeaba5f0 0x0000000000ebcf71
0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x00000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x000000000013619af
Interrupt based hog #3
Hog #3, traceback #1, at: 15:42:21 UTC Jan 6 2014, hog 2 ms
PC: 0x000000000068a223
Call stack: 0x0000000001360281 0x000007ffffeaba5f0 0x000000000069bbba
0x000000000069b0a4 0x000000000013619af 0x0000000000136cbbd
0x00000000001372203 0x000007ffffeab2f3a
```

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。

```
ciscoasa# show processes memory
-----
Allocs Allocated Frees Freed Process
(bytes) (bytes)
-----
23512 13471545 6 180 *System Main*
0 0 0 0 lu_rx
2 8324 16 19488 vpnlb_thread
```

次に、各プロセスの内部詳細を表示する例を示します。

```
ciscoasa# show processes internals
```

```

Invoked Giveups Process
1 0 block_diag
19108445 19108445 Dispatch Unit
1 0 CF OIR
1 0 Reload Control Thread
1 0 aaa
2 0 CMGR Server Process
1 0 CMGR Timer Process
2 0 dbgtrace
69 0 557mcfix
19108019 19108018 557poll
2 0 557statspoll
1 0 Chunk Manager
135 0 PIX Garbage Collector
6 0 route_process
1 0 IP Address Assign
1 0 QoS Support Module
1 0 Client Update Task
8973 8968 Checkheaps
6 0 Session Manager
237 235 uauth
(other lines deleted for brevity)

```

関連コマンド

コマンド	説明
show cpu	CPU使用状況の情報を表示します。

show ptp

さまざまなPTP統計情報とクロック関連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 ptp** コマンドを使用します。

show ptp { **clock** | **internal-info** | **port** [*interface-name*] }



(注) このコマンドは、Cisco ISA 3000 アプライアンスにのみ適用されます。

構文の説明

clock	PTP クロックのプロパティを表示します。
internal-info	ポート固有のカウンタなど、PTP の内部情報を表示します。
port	PTP 対応のすべてのインターフェイスの PTP ポート情報を表示します。
<i>interface-name</i>	指定されたインターフェイスの PTP ポート情報を表示します。

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	—	—

コマンド履歴

リリース 変更内容

9.7(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 ptp port コマンドにオプションのインターフェイス ID を含めると、そのインターフェイスのポート情報のみが表示されます。

show ptp clock | **port** | **internal-info** 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、PTP クロック プロパティを表示する例を示します。

```
ciscoasa# 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。

```
ciscoasa# 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 management-session

現在の管理セッションの統計情報を表示するには、特権 EXEC モードで **show quota management-session** コマンドを使用します。

show quota management-session [**ssh** | **telnet** | **http** | **username user**]

構文の説明

ssh	SSH セッションを示します。
telnet	Telnet セッションを示します。
http	HTTP セッションを示します。
username user	特定のユーザーのセッションを表示します。

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

9.1(2) このコマンドが追加されました。

9.12(1) このコマンドは、**quota management-session** コマンドがコンテキストごとにクォータをサポートするようになったため、コンテキスト内でのみ使用可能になりました。**ssh**、**telnet**、**http**、および **username** キーワードが追加されました。表示出力にはプロトコルごとのセッション数が表示されるようになりました。

使用上のガイドライン

このコマンドは、アクティブな管理セッションをタイプ別に表示します。

例

次に、現在の管理セッションの統計情報を表示する例を示します。

```
ciscoasa# show quota management-session
#Sessions          ConnectionType      Username
1                   SSH                 cisco
2                   TELNET             cisco
1                   SSH                 cisco1
```

関連コマンド

コマンド	説明
show running-config quota management-session	管理セッションクォータの現在の値を表示します。
quota management-session	デバイスで同時に実行できる ASDM、SSH、および Telnet セッションの数を設定します。

show raid

システムのハードドライブの RAID ステータスに関する情報を表示するには、特権 EXEC モードで **show raid** コマンドを使用します。

show raid

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	• 対応

コマンド履歴

リリース 変更内容
ス

9.1(1) このコマンドが追加されました。

9.17(1) Cisco Secure Firewall 3100 のサポートが追加されました。

使用上のガイドライン

一部のハードウェアモデルは、2つの内部ハードドライブをサポートします。たとえば、ASA 5545-X および 5555-X は最大2つのソリッドステートドライブをサポートします。2つのドライブが存在する場合、それらのドライブは RAID-1 設定で自動的にフォーマットされます。この構造は、デバイスをリロードするたびに再構築されます。RAID 設定に関する情報を表示するには、**show raid** コマンドを使用できます。



(注) デバイスのモデルが RAID をサポートしていない場合、**show raid** コマンドを入力すると無効なコマンドによるエラーメッセージが表示される場合があります。

例

次の表示例は、Cisco Secure Firewall 3100 の RAID にある2つの SSD を示しています。

```
> 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:

```

次に、アクティブで稼働中のハードドライブデバイスが1つある ASA デバイスが、State、Active Devices、および Working Devices の各行に表示される例を示します。また、最後のテーブルに示すように、2番目のデバイスが「removed」の状態であることも出力に示されます。つまり、2番目のドライブは取り付けられていなかったか、または2番目のドライブが実際に取り外されているかのいずれかです。

```
ciscoasa# show raid

/dev/md0:
  Version : 1.2
  Creation Time : Mon Mar  6 09:04:14 2017
  Raid Level : raid1
  Array Size : 124969216 (119.18 GiB 127.97 GB)
  Used Dev Size : 124969216 (119.18 GiB 127.97 GB)
  Raid Devices : 2
  Total Devices : 1
  Persistence : Superblock is persistent
  Intent Bitmap : Internal
  Update Time : Tue Mar 21 14:03:27 2017
  State : active, degraded
  Active Devices : 1
  Working Devices : 1
  Failed Devices : 0
  Spare Devices : 0
  Name : ciscoasa:0 (local to host ciscoasa)
  UUID : e8f90a6b:20433f38:e8b86378:6fd52057
  Events : 454610
  Number  Major  Minor  RaidDevice State
    0         8        0         0      active sync  /dev/sda
    1         0        0         1      removed
```

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
ID	アレイ コンポーネントの ID (例 : /dev/md0)。
Version	Superblock (RAID メタ データ) のフォーマット。
Creation Time	このコンポーネントが設定された日時。
RAID レベル	RAID レベル。RAID1 はミラーリング構成です。
Array Size	すべてのコンポーネントのデバイスで使用可能な合計記憶域 (バイト、ギガバイト、ギガバイト)。
Used Dev Size	各デバイスで合計容量に影響する記憶域の容量 (バイト、ギガバイト、ギガバイト)。これは最小のデバイスまたはパーティションによって決まります。大きいデバイスには未使用のスペースがある場合があります。
RAID Devices	スペア、不足、障害が発生したデバイスを含む完全なアレイのメンバデバイスの合計数。
Total Devices	使用可能な機能デバイスの数。

フィールド	説明
Persistence	Superblock がアレイのすべてのコンポーネントのデバイスに特定の位置に書き込まれること持続性 Superblock (アレイが作成されたときのデフォルト) は、Superblock がアレイのすべてのコンポーネントデバイスで特定の位置に書き込まれることを意味します。その後、RAID 設定は関連ディスクから直接読み取ることができます。
Update Time	アレイのステータスが変更された時刻。ステータス変更には、アクティブ化、障害などが含まれます。
状態	<p>RAID の現在のステータス。最初のステータスは、アレイが完全に動作している場合は active、アレイがアクティブでも保留中の書き込み操作がない場合は clean が示されます。</p> <p>表示される可能性のあるステータスは次のとおりです。</p> <ul style="list-style-type: none"> • resyncing, active : システムが新しく、現在 RAID 構造を構築しています。必要な構造の構築に 90 分以上かかる場合があります。完了率を示す出力の Rebuild Status 行を探します。 • (clean または active) , degraded, recovering : RAID 構造が正常に構築されました。 • (clean または active) , degraded : 1 つのハードドライブが機能していません。壊れているか、または見つからないかのいずれかです。2 つのドライブを使用する場合は、壊れているか、または見つからないドライブを交換します。 • (clean または active) , degraded, recovering : ハードドライブの取り付けまたは交換後にシステムが RAID 構造を再構築しています。
Active Devices	アレイの現在の機能デバイスの数。予備のデバイスは含まれていません。
Working Devices	アレイの使用可能な (障害のない) デバイスの総数。つまり、アクティブデバイスと予備のデバイス。
Failed Devices	アレイの障害の発生したデバイス。
Spare Devices	現在アレイに割り当てられている予備のデバイスの数。アレイのメンバーが見つからない場合は、使用可能なスペアをアクティブメンバーとしてアレイ内に構築する必要があります。ただし、システムがアレイへのスペアの追加に失敗した場合、ドライブもスペアとしてマークされます。
UUID	128 ビットの 16 進数汎用一意識別子 (UUID) はアレイの Superblock に格納されています。この番号は、ランダムに生成され、RAID を一意にタグ付けするために使用されます。すべてのコンポーネントデバイスがこの ID を共有します

フィールド	説明
Event	アレイのイベントカウンタ。Superblockが更新されるたびに増分されます。
Component table	<p>コンポーネントディスクの番号は0から始まります。メジャー番号は通常、デバイスタイプに対応し、マイナー番号は、そのグループ内の特定のデバイスのIDです。たとえば、「Major 8」はSCSIディスクを示します。</p> <p>RAID デバイスの各コンポーネントと、コンポーネントの現在のステータスのリストがここに表示されます。健全なディスクは、active sync 状態になっています。</p>

show reload

ASA のリロードのステータスを表示するには、特権 EXEC モードで **show reload** コマンドを使用します。

show reload

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	トランスパ 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 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

このコマンドには使用上のガイドラインがありません。

例

次に、リロードが 4 月 20 日、土曜日の午前 0 時（夜の 12 時）にスケジューリングされている例を示します。

```
ciscoasa# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

関連コマンド

コマン ド	説明
reload	コンフィギュレーションをリブートおよびリロードします。

show resource allocation

すべてのクラスとクラスメンバーにまたがってリソースごとにリソース割り当てを表示するには、特権 EXEC モードで **show resource allocation** コマンドを使用します。

show resource allocation [detail]

構文の説明

detail 追加情報を表示します。

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
ス

7.2(1) このコマンドが追加されました。

9.0(1) 新規リソースクラス **routes** が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。

新しいリソース タイプ **vpn other** と **vpn burst other** が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

使用上のガイドライン

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際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。

例

次に、**show resource allocation** コマンドの出力例を示します。ディスプレイには、各リソースの合計割り当て値が、絶対値および使用可能なシステムリソースのパーセンテージとして表示されます。

```
ciscoasa# show resource allocation
Resource          Total          % of Avail
Conns [rate]      35000          N/A
Inspects [rate]   35000          N/A
Syslogs [rate]    10500          N/A
Conns             305000         30.50%
```

```

Hosts                78842                N/A
SSH                  35                 35.00%
Telnet               35                 35.00%
Routes               25000              0.00%
Xlates              91749              N/A
Other VPN Sessions   20                 2.66%
Other VPN Burst     20                 2.66%
All                  unlimited

```

表 11-2 に、各フィールドの説明を示します。

表 2: *show resource allocation* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは1秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASAはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	使用できる場合は、すべてのコンテキストで割り当てられるシステムリソース総量のパーセンテージ。リソースにシステム制限がない場合、このカラムにはN/Aと表示されます。

例

次に、**show resource allocation detail** コマンドの出力例を示します。

```

ciscoasa# show resource allocation detail
Resource Origin:
  A Value was derived from the resource 'all'
  C Value set in the definition of this class
  D Value set in default class
Resource Class Mmbrs Origin Limit Total Total %
Conns [rate] default all CA unlimited
gold 1 C 34000 34000 N/A
silver 1 CA 17000 17000 N/A
bronze 0 CA 8500
All Contexts: 3 51000 N/A
Inspects [rate] default all CA unlimited
gold 1 DA unlimited
silver 1 CA 10000 10000 N/A
bronze 0 CA 5000
All Contexts: 3 10000 N/A
Syslogs [rate] default all CA unlimited
gold 1 C 6000 6000 N/A
silver 1 CA 3000 3000 N/A
bronze 0 CA 1500
All Contexts: 3 9000 N/A
Conns default all CA unlimited
gold 1 C 200000 200000 20.00%
silver 1 CA 100000 100000 10.00%
bronze 0 CA 50000
All Contexts: 3 300000 30.00%
Hosts default all CA unlimited

```

	gold	1	DA	unlimited			
	silver	1	CA	26214	26214	N/A	
	bronze	0	CA	13107			
	All Contexts:	3			26214	N/A	
SSH	default	all	C	5			
	gold	1	D	5	5	5.00%	
	silver	1	CA	10	10	10.00%	
	bronze	0	CA	5			
	All Contexts:	3			20	20.00%	
Telnet	default	all	C	5			
	gold	1	D	5	5	5.00%	
	silver	1	CA	10	10	10.00%	
	bronze	0	CA	5			
	All Contexts:	3			20	20.00%	
Routes	default	all	C	unlimited			N/A
	gold	1	D	unlimited	5		N/A
	silver	1	CA	10	10		N/A
	bronze	0	CA	5			N/A
	All Contexts:	3			20		N/A
Xlates	default	all	CA	unlimited			
	gold	1	DA	unlimited			
	silver	1	CA	23040	23040		N/A
	bronze	0	CA	11520			
	All Contexts:	3			23040		N/A
mac-addresses	default	all	C	65535			
	gold	1	D	65535	65535	100.00%	
	silver	1	CA	6553	6553	9.99%	
	bronze	0	CA	3276			
	All Contexts:	3			137623	209.99%	

表 11-3 に、各フィールドの説明を示します。

表 3: show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
クラス	デフォルトクラスを含む、各クラスの名前。 すべてのコンテキストフィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 <ul style="list-style-type: none"> • A : この制限を個々のリソースとしてではなく、all オプションを使用して設定します。 • C : この制限はメンバー クラスから生成されます。 • D : この制限はメンバークラスでは定義されたのではなく、デフォルトクラスから生成されました。デフォルトクラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「C」または「D」を「A」に組み合わせることができます。

フィールド	説明
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、ASAはこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは1秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	使用できる場合、クラス内のすべてのコンテキストにわたって割り当てられるシステムリソースの合計数のパーセンテージ。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムにはN/Aと表示されます。

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。
show resource types	制限を設定できるリソースタイプを表示します。
show resource usage	ASA のリソース使用状況を表示します。

show resource types

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

show resource types

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	• 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。

7.2(1) このコマンドは、コンテキストごとに管理できる追加のリソースタイプを表示するように変更されました。

9.0(1) 新規リソース クラス **routes** が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。

新しいリソース タイプ **vpn other** と **vpn burst other** が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

例

次に、リソース タイプの例を示します。

```
ciscoasa# show resource types
Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec
Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM           ASDM Connections
  SSH            SSH Sessions
  Telnet         Telnet Sessions
```

```

Xlates           XLATE Objects
Routes           Routing Table Entries
Other-vpn        Other VPN licenses
Other-vpn-burst Allowable burst for Other VPN licenses
All              All Resources

```

関連コマンド

コマンド	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。
context	セキュリティ コンテキストを追加します。
show resource usage	ASA のリソース使用状況を表示します。

show resource usage

またはマルチモードの各コンテキストのリソース使用状況を表示するには、特権EXECモードで **show resource usage** コマンドを使用します。

```
show resource usage [ context context_name | top n | all | summary | system | detail ] [ resource
{ [ rate ] resource_name | all } ] [ counter counter_name [ count_threshold ] ]
```

構文の説明

context <i>context_name</i>	(マルチモードのみ) 統計情報を表示するコンテキストの名前を指定します。すべてのコンテキストを対象にするには、 all を指定します。ASAは、各コンテキストのリソース使用状況を一覧表示します。
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。 (注) 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 <i>counter_name</i>	次のカウンタタイプの数を表示します。 <ul style="list-style-type: none"> • 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。 • 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。 • 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。 • 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 特定のリソースの使用状況を表示します。すべてのリソースを対象にするには、**all** (デフォルト) 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。

リソースには、次のタイプがあります。

- **asdm** : ASDM 管理セッション。
- **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)。
- **inspects** : アプリケーション インспекション。
- **hosts** : ASA 経由で接続可能なホスト。
- **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。
- **routes** : ルーティング テーブル エントリ。
- **ssh** : SSH セッション。
- **syslogs** : システム ログ メッセージ。
- **telnet** : Telnet セッション。
- (マルチモードのみ) **VPN Other** : サイト間 VPN セッション。
- (マルチモードのみ) **VPN Burst Other** : サイト間 VPN バーストセッション。
- **xlates** : NAT 変換。

summary (マルチモードのみ) すべてのコンテキストの合算使用状況を表示します。

system (マルチモードのみ) すべてのコンテキストの合算使用状況を表示します。ただし、コンテキストの合算制限値ではなくシステムのリソース制限値を表示します。

top n (マルチモードのみ) 指定したリソースの上位 *n* 人のユーザーのコンテキストを表示します。このオプションでは、**resource all** ではなく、リソースの種類を1つ指定する必要があります。

コマンド デフォルト

マルチコンテキストモードでは、デフォルトコンテキストは **all** です。すべてのコンテキストのリソース使用状況が表示されます。シングルモードの場合、コンテキスト名は無視され、出力では「context」は「System」として表示されます。

デフォルトのリソース名は、**all** です。すべてのリソースタイプが表示されます。

デフォルトのカウント名は、**all** です。すべての統計情報が表示されます。

デフォルトのカウントしきい値は **1** です。

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	• 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。

7.2(1) コンテキストごとにリソースを制限できるため、このコマンドでは拒否されたリソースが表示されます。

9.0(1) 新規リソース クラス **routes** が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。

新しいリソース タイプ **vpn other** と **vpn burst other** が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、**admin** コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin
Resource          Current      Peak      Limit      Denied  Context
Telnet            1            1         5          0      admin
Conns             44           55        N/A        0      admin
Hosts             45           56        N/A        0      admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary
Resource          Current      Peak      Limit      Denied  Context
Syslogs [rate]   1743        2132     12000 (U)  0      Summary
Conns            584         763     100000 (S)  0      Summary
Xlates          8526        8966     93400      0      Summary
Hosts           254         254     262144     0      Summary
Conns [rate]    270         535     42200      1704   Summary
Inspects [rate] 270         535     100000 (S)  0      Summary
Other VPN Sessions 0           10       10         740   Summary
```

```

Other VPN Burst          0          10          10          730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.

```

次に、**show resource usage system** コマンドの出力例を示します。ここでは、すべてのコンテキストのリソース使用状況が表示されますが、合算のコンテキスト制限値ではなくシステム制限値が表示されています。

```

ciscoasa# show resource usage system
Resource          Current      Peak        Limit      Denied  Context
Telnet            3           5           100        0       System
SSH               5           7           100        0       System
Conns             40          55          N/A        0       System
Hosts            44          56          N/A        0       System

```

次に、**show resource usage detail counter all 0** コマンドの出力例を示します。このコマンドは、ユーザーが管理できるリソースだけでなく、すべてのリソースを表示します。

```

ciscoasa# show resource usage detail counter all 0
Resource          Current      Peak        Limit      Denied  Context
memory           1012028     1538428    unlimited  0       admin
chunk:aaa        0           0           unlimited  0       admin
chunk:aaa_queue  0           0           unlimited  0       admin
chunk:acct       0           0           unlimited  0       admin
chunk:channels   25          39          unlimited  0       admin
chunk:CIFS       0           0           unlimited  0       admin
chunk:conn       0           0           unlimited  0       admin
chunk:crypto-conn 0           0           unlimited  0       admin
chunk:dbgtrace   1           2           unlimited  0       admin
chunk:dhcpd-radix 0           0           unlimited  0       admin
chunk:dhcp-relay-r 0           0           unlimited  0       admin
chunk:dhcp-lease-s 0           0           unlimited  0       admin
chunk:dnat       0           0           unlimited  0       admin
chunk:ether      0           0           unlimited  0       admin
chunk:est        0           0           unlimited  0       admin
...
Telnet           0           0           5          0       admin
SSH              1           1           5          0       admin
ASDM             0           1           5          0       admin
Syslogs [rate]  0           68          unlimited  0       admin
aaa rate        0           0           unlimited  0       admin
url filter rate  0           0           unlimited  0       admin
Conns           1           6           unlimited  0       admin
Xlates          0           0           unlimited  0       admin
tcp conns       0           0           unlimited  0       admin
Hosts           2           3           unlimited  0       admin
Other VPN Sessions 0           10          750        740     admin
Other VPN Burst  0           10          750        730     admin
udp conns       0           0           unlimited  0       admin
smtp-fixups     0           0           unlimited  0       admin
Conns [rate]    0           7           unlimited  0       admin
establisheds    0           0           unlimited  0       admin
pps             0           0           unlimited  0       admin
syslog rate     0           0           unlimited  0       admin
bps             0           0           unlimited  0       admin
Fixups [rate]   0           0           unlimited  0       admin
non tcp/udp conns 0           0           unlimited  0       admin
tcp-intercepts  0           0           unlimited  0       admin
globals         0           0           unlimited  0       admin
np-statics      0           0           unlimited  0       admin
statics         0           0           unlimited  0       admin

```

```

nats                0          0 unlimited          0 admin
ace-rules            0          0 N/A                0 admin
aaa-user-aces       0          0 N/A                0 admin
filter-rules        0          0 N/A                0 admin
est-rules           0          0 N/A                0 admin
aaa-rules           0          0 N/A                0 admin
console-access-rul  0          0 N/A                0 admin
policy-nat-rules    0          0 N/A                0 admin
fixup-rules         0          0 N/A                0 admin
aaa-uxlates         0          0 unlimited          0 admin
CP-Traffic:IP       0          0 unlimited          0 admin
CP-Traffic:ARP      0          0 unlimited          0 admin
CP-Traffic:Fixup    0          0 unlimited          0 admin
CP-Traffic:NPCP     0          0 unlimited          0 admin
CP-Traffic:Unknown  0          0 unlimited          0 admin

```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
clear resource usage	リソース使用状況の統計情報をクリアします。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。
show resource types	リソース タイプのリストを表示します。

show rest-api agent

REST API エージェントが現在イネーブルになっているかどうかを判断するには、特権 EXEC モードで **show rest-api agent** コマンドを使用します。

show rest-api agent



(注) このコマンドは、ASA 仮想のすべてのバージョン、ASA 5585-X、およびすべての ASA 5500-X シリーズ（ASA 5506-X と ASA 5508-X を除く）のデバイスでサポートされます。

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

9.3(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、REST API エージェントが現在イネーブルになっているかどうかを判断するために使用します。

例

この例は、REST API エージェントがイネーブルになっていることを示しています。

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

エージェントがディセーブルになっている場合に表示されるメッセージは、「REST API agent is currently disabled.」です。

関連コマンド

コマンド	説明
rest-api	REST API パッケージを確認してインストールします。REST API エージェントをイネーブルにします。
show version	REST API エージェントがイネーブルになっている場合、そのバージョン番号が show version 出力に含まれます。

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、特権 EXEC モードで **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 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	—	—

コマンド履歴

リリー 変更内容
ス

7.2(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

RIP ルーティング関連の **show** コマンドは、ASA 上で特権 EXEC モードで使用できます。RIP 関連の **show** コマンドを使用する場合に RIP コンフィギュレーションモードである必要はありません。

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。ルーティングテーブルにルーティングプロトコルデータベースから値を挿入する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

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

```
ciscoasa# 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。

```
Router# 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
```

関連コマンド

コマンド	説明
router rip	RIP ルーティングをイネーブルにし、グローバル RIP ルーティング パラメータを設定します。

show rollback-status

Cisco Security Manager がロールバック要求を ASA に送信すると、Cisco Security Manager から ASA への管理接続がリセットされます。ロールバック ジョブの結果を Cisco Security Manager に送信することはできません。**show rollback-status** を使用して、ASA を照会するとき Cisco Security Manager にロールバックジョブのステータスを表示します。

show rollback-status [*context_name*]

構文の説明

context_name ロールバック ジョブが適用されるコンテキストの名前。シングルモードの場合、これは適用されません。

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
設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース 変更内容
ス

9.6(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 rollback-status を使用して、ロールバックジョブのステータス、開始時刻、終了時刻、およびロールバックジョブが適用されているコンテキスト名を表示します。

例

次に、シングルモードで入力されたすべてのコンテキストのロールバック ステータスを表示する例を示します。

1. Cisco Security Manager からのロールバック要求が受信される前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. ASA で最初のロールバック要求を受信すると、ジョブが完了する前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
```

```
Status      : In Progress
Start Time  : 13:00:12 UTC May 11 2017
End Time    : N/A
```

3. ロールバック ジョブが完了したときは、次の状態です。

```
ciscoasa(config)# sh rollback-status
Status      : Succeeded
Start Time  : 13:00:12 UTC May 11 2017
End Time    : 13:00:14 UTC May 11 2017
```

4. ロールバックが失敗した場合、出力は次のようになります。

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Failed
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

5. ロールバックが失敗し、スタートアップ コンフィギュレーションに戻ると、次の状態です。

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Reverted ( Roll back failed, startup config applied )
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

次の例は、マルチモードで `system/admin` コンテキストから入力されたロールバック ステータスを示しています。

1. ロールバックを ASA に展開する前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. システム コンテキストのロールバックが開始された時点では、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : In Progress
Start Time  : 16:55:35 UTC May 11 2017
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
```

```
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

3. システム コンテキストのロールバックが完了した時点では、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

4. コマンドでコンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa(config)# sh rollback-status system
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
ciscoasa(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

次の例は、マルチモードで **admin/user** コンテキストから入力されたロールバック ステータスを示しています。

1. コンテキスト名が指定されていない場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

2. コンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

3. 誤ったコンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status ad
Context ad does not exist.
```

4. コンテキスト名が現在のコンテキストと一致しない場合は、次のようになります。

```
ciscoasa/admin(config)# sh rollback-status ctx1
Context ctx1 does not match current context.
```

ASA がスレーブまたはスタンバイ装置として動作している場合は、警告メッセージが表示されます。

1. スレーブから show コマンドが発行されると、出力は次のようになります。

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Slave.
```

2. スタンバイから show コマンドが発行されると、出力は次のようになります。

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Standby.
```

次の表で出力エントリの詳細について説明します。

出力	説明
Context Name	ロールバック ジョブが適用されるコンテキストの名前。シングル モードの場合、これは表示されません。
Status (ステータス)	最新のロールバック ジョブのステータス。次のいずれかになります。 <ul style="list-style-type: none"> • [None] : このコンテキストにロールバック ジョブは導入されていません。 • [In Progress] : ASA が Cisco Security Manager からロールバック 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。 • [revert] : Cisco Security Manager から送信された設定へのロールバックが失敗し、ASA に保存されているスタートアップ設定へのロールバックがトリガーされ、この復元アクションが正常に完了し、ASA は現在スタートアップ設定で実行されています。 • [Failed] : ロールバックはエラーが発生して完了しました。
Start Time	直近のロールバック ジョブの開始時刻。ASA でロールバック ジョブを受信するたびに、このフィールドは ASA の現在の時刻で更新されます。ステータスは [In Progress] として更新されます。ロールバックが None 状態の場合、[N/A] が表示されます。

出力	説明
End Time	ロールバック ジョブが完了した時刻。ジョブがエラーなしで完了した場合、[Status] は [Succeeded] として更新されます。ロールバック中に復元アクションが実行され、復元が正常に完了した場合、ステータスは [Reverted] として更新されます。復元に失敗した場合、ステータスは [Failed] として更新されます。[None] または [In Progress] 状態のロールバックの場合は、[N/A] が表示されます。

show route

ルーティングテーブルを表示するには、特権 EXEC モードで **show route** コマンドを使用します。

このコマンドで使用できるパラメータは、デバイス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）によって異なります。これは、シンタックスの説明に示されています。

```
show route [ management-only [ interface_name ] ] [ cluster | failover | hostname | ip_address
[ mask ] [ longer-prefixes ] | domain-name hostname_or_ip_address | bgp [ as_number ] |
connected | eigrp [ process_id ] | isis | isis | ospf [ process_id ] | rip | static | summary | zone ]
```

構文の説明

bgp <i>as_number</i>	(ルーテッド) 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。 <i>as_number</i> 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	(ルーテッド) 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	(ルーテッド、トランスペアレント) 接続されているルートを表示します。
domain-name <i>hostname_or_ip_address</i>	(ルーテッド、トランスペアレント) 指定された宛先ホスト名へのルートを表示します。ホスト名の解決を機能させるには、DNS を設定する必要があります。このキーワードで IP アドレスを使用することもできます。
eigrp <i>process_id</i>	(ルーテッド) EIGRP ルートを表示します。
failover	(ルーテッド) フェールオーバーが発生し、スタンバイユニットがアクティブユニットになった後の、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。
hostname	(ルーテッド、トランスペアレント) 指定された宛先ホスト名へのルートを表示します。ホスト名の解決を機能させるには、DNS を設定する必要があります。
interface_name	(ルーテッド、トランスペアレント) 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 <i>mask</i>	(ルーテッド、トランスペアレント) 指定した宛先へのルートを表示します。

isis	(ルーテッド) IS-IS ルートを表示します。
longer-prefixes	(ルーテッド、トランスペアレント) 指定された <i>ip_address/mask</i> ペアに一致するルートのみを表示します。
management-only	(ルーテッド、トランスペアレント) IPv4 管理ルーティングテーブル内のルートを表示します。
isis	(ルーテッド) IS-IS ルートを表示します。
ospf process_id	(ルーテッド) OSPF ルートを表示します。
rip	(ルーテッド) RIP ルートを表示します。
static	(ルーテッド、トランスペアレント) スタティック ルートを表示します。
summary	(ルーテッド、トランスペアレント) ルーティングテーブルの現在の状態を表示します。
zone	(ルーテッド、トランスペアレント) 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 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	• 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。

8.0(2) **eigrp** キーワードが追加されました。

8.4(1) **failover** キーワードが追加されました。出力には、RIB エポック番号 (シーケンス番号)、現在のタイマー値、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) が表示されます。

リリース	変更内容
9.0(1)	cluster キーワードが追加されました。ダイナミック ルーティング プロトコル (EIGRP、OSPF、および RIP) に適用され、ASA 5580 および 5585-X でのみ使用できます。
9.2(1)	bgp キーワードが追加されました。
9.2(1)	このコマンドでは、ローカルホストルートが、 connected ルートとともに表示されるようになりました。表示されるルートのプロトコルまたはタイプを示す新しいコード (L、I、E、su、および+) が追加されました。
9.3(2)	zone キーワードが追加されました。
9.5(1)	管理ルーティング テーブル機能のサポートが追加されました。
9.6(1)	isis キーワードが追加されました。
9.6(1)	isis キーワードが追加されました。
9.20(2)	domain-name 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。



- (注) ASA で対応する機能が設定されていない場合、**clustering** および **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、ASA 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、ASA 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。



- (注) Cisco IOS で **show ip route** コマンドを使用する場合、**longer-prefix** キーワードを使用できます。Cisco IOS でこのキーワードを使用すると、ルートは、指定したネットワークとマスクのペアが一致したときのみ表示されます。ASA では、**longer-prefix** キーワードは **show route** コマンドのデフォルトの動作です。したがって、CLI でキーワードを追加する必要はありません。このため、**ip** を入力してもルートは表示されません。スーパーネットルートを取得するには、マスク値を IP アドレスとともに渡す必要があります。

例

次に、**show route** コマンドの出力例を示します。

```
ciscoasa# 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, 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、管理コンテキストにおける ASA 5555 での **show route** コマンドの出力例を示します。この出力には、個々のユーザー認証用に VPN ハードウェアクライアントで使用される内部ループバック アドレスが表示されます。

```
ciscoasa/admin(config)# 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, 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    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

次に、**show route bgp** コマンドの出力例を示します。

```
ciscoasa# show route bgp
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
       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
Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

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。

```
ciscoasa(config)# 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, 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。

```
ciscoasa(cfg-cluster)# 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, 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。

```
ciscoasa# 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          0          0            0          408
Total          2          2          0            264       1272
```

show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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
Gateway of last resort is not set
S   192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outsidel
C   192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C   172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S   10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O   10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O   10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside

```

次に、**show route isis** コマンドの出力例を示します。

```

ciscoasa# show route isis
Routing Table:
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
       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
Gateway of last resort is not set
i L2   1.1.1.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2   2.2.2.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2   3.3.3.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2   4.4.4.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2   5.5.5.0 255.255.255.0 [115/10] via 22.22.22.5, subint

```

show running-config

ASA 上で現在実行されているコンフィギュレーションを表示するには、特権 EXEC モードで **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 ヘルプを参照してください。

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	• 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。

8.3(1) 暗号化されたパスワードが出力に追加されました。

9.7(1) このコマンドの出力も、IPv6 アドレスで設定された syslog サーバーを表示します。

9.13(1)

- テレメトリ設定の詳細が出力に含まれています。
- 新しいコマンド：設定されたブロックサイズ値（デフォルト値を除く）を表示する **fttp blocksize** が追加されました。

使用上のガイドライン

show running-config コマンドは、ASA 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。

ASA のフラッシュメモリに保存されたコンフィギュレーションを表示するには、**show configuration** コマンドを使用します。

show running-config コマンドの出力では、パスワードの暗号化が有効か無効かに応じて、パスワードが暗号化、マスク、またはクリアテキストの状態が表示されます。



(注) このコマンドを使用して ASA への接続または設定を行った後は、コンフィギュレーションに ASDM コマンドが表示されます。

ASA リリース 9.3 でディセーブルに変更された **error-recovery disable** のデフォルトです。そのため、WebVPN error recovery がデフォルト値の場合、**show running-config** コマンドは *error-recovery disable* を CLI に表示するようになりました。問題のトラブルシューティング時にシスコのテクニカル アシスタンス センターからの指示がない限り、これはディセーブルのままにしておくことを推奨します。

ASA 9.13(1) 以降、このコマンドの出力にはテレメトリの詳細が含まれていました。show running-config コマンドには、テレメトリサービスのデフォルト以外の設定 (**no service telemetry**) のみが表示されます。all コマンドを使用すると、デフォルトのテレメトリサービス設定も一緒に表示されます。

例

次に、**show running-config** コマンドの出力例を示します。

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
```

```
shutdown
no nameif
security-level 0
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
```

```

inspect ctiqbe
inspect cuseeme
inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end

```

次に、**show running-config access-group** コマンドの出力例を示します。

```

ciscoasa# show running-config access-group
access-group 100 in interface outside

```

次に、**show running-config arp** コマンドの出力例を示します。

```

ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893

```

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。

```

ciscoasa# 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。

```

ciscoasa# 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

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
show configuration	スタートアップ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。