



show isakmp ipsec-over-tcp stats コマンド～ show mroute コマンド

show isakmp ipsec-over-tcp stats

IPsec over TCP の実行時統計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 または特権 EXEC モードで **show isakmp ipsec-over tcp stats** コマンドを使用します。

show isakmp ipsec-over-tcp stats

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
ASA v(1)	show isakmp ipsec-over-tcp stats コマンドが追加されました。
7.2(1)	show isakmp ipsec-over-tcp stats コマンドは廃止されました。 show crypto isakmp ipsec-over-tcp stats コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures
- Checksum errors
- Internal errors

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show isakmp ipsec-over-tcp stats
Global IPsec over TCP Statistics
-----
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モード または特権 EXEC モードで **show isakmp sa** コマンドを使用します。

show isakmp sa [detail]

構文の説明

detail SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	show isakmp sa コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。 show crypto isakmp sa コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth  Lifetime
1 209.165.200.225 User  Resp No    AM_Active 3des  SHA  preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth  Lifetime
2 209.165.200.226 User  Resp No    AM_ACTIVE 3des  SHA  preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth  Lifetime
3 209.165.200.227 User  Resp No    AM_ACTIVE 3des  SHA  preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth  Lifetime
4 209.165.200.228 User  Resp No    AM_ACTIVE 3des  SHA  preshrd 86400

ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

実行時統計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 モードまたは特権 EXEC モードで **show isakmp stats** コマンドを使用します。

show isakmp stats

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
ASAv(1)	show isakmp stats コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。 show crypto isakmp stats コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

各カウンタは、関連する cikePhase1GW カウンタにマッピングします。これらのカウンタの詳細については、「[CISCO-IPSEC-FLOW-MONITOR-MIB.my](#)」を参照してください。

- Active/Standby Tunnels : cikePhase1GWActiveTunnels
- Previous Tunnels : cikePhase1GWPreviousTunnels
- In Octets : cikePhase1GWInOctets
- In Packets : cikePhase1GWInPkts
- In Drop Packets : cikePhase1GWInDropPkts
- In Notifys : cikePhase1GWInNotifys
- In P2 Exchanges : cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids : cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects : cikePhase1GWInP2ExchgRejects

- In P2 Sa Delete Requests : cikePhase1GWInP2SaDelRequests
- Out Octets : cikePhase1GWOutOctets
- Out Packets : cikePhase1GWOutPkts
- Out Drop Packets : cikePhase1GWOutDropPkts
- Out Notifys : cikePhase1GWOutNotifys
- Out P2 Exchanges : cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids : cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects : cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests : cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels : cikePhase1GWInitTunnels
- Initiator Fails : cikePhase1GWInitTunnelFails
- Responder Fails : cikePhase1GWRespTunnelFails
- System Capacity Fails : cikePhase1GWSysCapFails
- Auth Fails : cikePhase1GWAauthFails
- Decrypt Fails : cikePhase1GWDecryptFails
- Hash Valid Fails : cikePhase1GWHashValidFails
- No Sa Fails : cikePhase1GWNoSaFails

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails

- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isis database

IS-IS リンクステート データベースを表示するには、特権 EXEC モードで **show isis database** コマンドを使用します。

```
show isis database [{detail | verbose} [ip [unicast] | ipv6 [unicast]] [topology base]]
[level-1 | level-2]
```

構文の説明

level-1	(任意) レベル 1 の IS-IS リンクステート データベースを示します。
level-2	(任意) レベル 2 の IS-IS リンクステート データベースを示します。
ip	(オプション) IPv4 アドレスファミリの IS-IS リンクステート データベースを表示します。
ipv6	(オプション) IPv6 アドレスファミリの IS-IS リンクステート データベースを表示します。
detail	(任意) 各リンクステート パケット (LSP) のコンテンツを表示します。
verbose	(オプション) IS-IS データベースに関する追加情報を表示します。
topology base	(オプション) MTR トポロジを表示します。
unicast	(オプション) ユニキャスト アドレス ファミリを表示します。

コマンドデフォルト

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IS-IS リンクステート データベースを表示します。

例

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

```
ciscoasa# show isis database

IS-IS Level-1 Link State Database:
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00              0xea19d300   0x3d0d        674           0/0/0
routerA.00-00        0x1b541556   0xa349        928           0/0/0
c3.00-00              0x9257c979   0x9952        759           0/0/0
c2.00-00              *0xef11e977   0x3188        489           0/0/0
c2.01-00              *0xa8333f03   0xd6ea        829           0/0/0
IS-IS Level-2 Link State Database:
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00              0x63871f24   0xaba2        526           0/0/0
routerA.00-00        0x0d540b55   0x81d7        472           0/0/0
routerA.00-01        0xffffffff01  0xe20b        677           0/0/0
c3.00-00              0x002e5434   0xb20a        487           0/0/0
c2.00-00              *0x74fd1227   0xbb0f        742           0/0/0
c2.01-00              *0x7ee72c1a   0xb506        968           0/0/0
```

表 9-1 show isis database のフィールド

フィールド	説明
LSPID	<p>LSP の ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。</p> <p>次のオクテットは疑似ノード ID です。このバイトが非ゼロの場合、LSP はシステムからのリンクを記述します。ゼロの場合は、LSP は、いわゆる非疑似ノード LSP です。このメカニズムは、Open Shortest Path First (OSPF) プロトコルのルータ リンクステート アドバタイズメント (LSA) に類似しています。LSP は、送信元ルータの状態を記述します。</p> <p>各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。</p> <p>最後のオクテットは LSP 番号です。単一の LSP に収容可能な量を超えるデータがある場合は、LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク (*) は、その LSP が、このコマンドの送信元のシステムによって生成されたことを示します。</p>
LSP Seq Num	他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。
LSP Checksum	LSP パケットのチェックサム。
LSP Holdtime	LSP が有効である時間(秒単位)。LSP Holdtime がゼロである場合は、LSP がページされて、すべてのルータのリンクステート データベース (LSDB) から削除されていることを示します。この値は、ページされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。
ATT	Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 だけのルータ、および他のレベル 2 ルータとの接続を失ったレベル 1-2 ルータは、Attach ビットを使用して最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルトルートを示します。

表 9-1 show isis database のフィールド(続き)

フィールド	説明
P	P ビット。中継システムが修復可能なエリアパーティションであるかどうかを検出します。シスコおよび他のベンダーは、エリアパーティション修復をサポートしません。
OL	過負荷ビット。IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。

次に、**show isis database detail** コマンドの出力例を示します。出力に示されるように、**show isis database** コマンドで表示される情報に加えて、**show isis database detail** コマンドにより各 LSP のコンテンツが表示されます。

```
ciscoasa# show isis database detail

IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00       0xea19d301   0x3b0e        1189          0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:      10 IP 10.22.22.0 255.255.255.0
  Metric:      10 IS c2.01
routerA.00-00  0x1b541556   0xa349        642          0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:      10 IP 10.22.22.0 255.255.255.0
  Metric:      10 IS c2.01
```

表 9-2 show isis database detail のフィールド

フィールド	説明
Area Address	ルータから到達可能なエリアアドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリアアドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリアアドレスになります。
メトリック	送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先(IP アドレス、エンドシステム [ES]、または CLNS プレフィックス)に到達するコスト用のメトリック。

次に、**show isis database detail** コマンドの、別の出力例を示します。この LSP は、レベル 2 LSP です。エリアアドレス 39.0001 は、ルータが存在するエリアのアドレスです。

```
ciscoasa# show isis database 12 detail

IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00       0x63871f25   0xa9a3        1076          0/0/0
  Area Address: 49.0001
```

```

NLPID:          0xcc
Hostname: c1
IP Address:    10.22.22.1
Metric:       10 IS c2.01
routerA.00-00  0x0d540b56    0x7fd8                941                0/0/0
Area Address:  49.0001
NLPID:          0xcc
Hostname: routerA
IP Address:    10.22.22.5
Metric:       10 IS c2.01
Metric:       0 IP-External 1.1.1.0 255.255.255.0
Metric:       0 IP-External 2.1.1.0 255.255.255.0
Metric:       0 IP-External 2.2.2.0 255.255.255.0
Metric:       0 IP-External 3.1.1.0 255.255.255.0

```

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

```

ciscoasa# show isis database verbose

IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00       *0xea19d301  0x3b0e        644            0/0/0
Area Address:  49.0001
NLPID:          0xcc
Hostname: c1
IP Address:    22.22.22.1
Metric:       10 IP 22.22.22.0 255.255.255.0
Metric:       10 IS c2.01
routerA.00-00  0x1b541557  0xa14a        783            0/0/0
Area Address:  49.0001
NLPID:          0xcc
Hostname: routerA
IP Address:    22.22.22.5
Metric:       10 IP 22.22.22.0 255.255.255.0
Metric:       10 IS c2.01

```

表 9-3 **show isis database verbose** のフィールド

フィールド	説明
LSPID	<p>リンクステート パケット (LSP) ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。</p> <p>次のオクテットは疑似ノード ID です。このバイトがゼロの場合は、LSP はシステムからのリンクを記述します。ゼロでない場合は、LSP は非疑似ノード LSP です。これは、Open Shortest Path First (OSPF) のルータ LSA と類似しており、LSP は送信元ルータの状態を記述します。各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。</p> <p>最後のオクテットは LSP 番号です。すべてのデータが単一の LSP に収容できない場合は、その LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク (*) は、このコマンドを送信したシステムが LSP を生成したことを示します。</p>
LSP Seq Num	他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。
LSP Checksum	LSP パケットのチェックサム。

表 9-3 show isis database verbose のフィールド(続き)

フィールド	説明
LSP Holdtime	LSP が有効である時間(秒単位)。LSP Holdtime がゼロである場合は、LSP がページされて、すべてのルータのリンクステート データベース (LSDB) から削除されていることを示します。この値は、ページされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。
ATT	Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 ルータは、Attach ビットを使用して、最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルト ルートを設定します。
P	P ビット。このビットは、IS がエリア パーティションを修復できるかどうかを検出します。シスコおよび他のベンダーは、エリア パーティション修復をサポートしません。
OL	過負荷ビット。このビットは、IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに、中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。
Area Address	ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。
NLPID	ネットワーク層プロトコル ID。
Hostname	ノードのホスト名。
ルータ ID	ノードのトラフィック エンジニアリング ルータ ID。
IP Address	インターフェイスの IPv4 アドレス。
メトリック	発信元ルータとアドバタイズされるネイバー間の隣接のコストの IS-IS メトリック、またはアドバタイズするルータからアドバタイズされる宛先までにかかるコストのメトリック (IP アドレス、エンドシステム (ES)、またはコネクションレス型ネットワーク サービス (CLNS) のプレフィックスを指定できます)。
アフィニティ	フラッドされているリンク属性フラグ。
Physical BW	リンクの帯域幅容量(ビット/秒)。
Reservable BW	このリンクの予約可能帯域幅。
BW Unreserved	予約可能帯域幅。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される(受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をバージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステータスを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
pre-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis hostname

IS-IS ルータのルータ名とシステム ID のマッピング テーブル エントリを表示するには、特権 EXEC モードで **show isis hostname** コマンドを使用します。

show isis hostname

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS ルーティング ドメインでは、各ルータはシステム ID により表されます。システム ID は、IS-IS ルータごと構成されている Network Entity Title (NET) の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されているルータのシステム ID が 0023.0003.000a であるとして、ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、ルータ名とシステム ID のマッピング テーブルに含まれるエントリが表示されます。

no hostname dynamic コマンドを入力してダイナミック ホスト名機能が無効にされていない場合は、マッピングはダイナミック ホスト マッピング テーブルで構成されます。

例

次に、ciscoASA のホスト名を変更し、NET 49.0001.0050.0500.5005.00 を ciscoASA に割り当てる例を示します。

```
ciscoasa(config)# hostname ciscoASA
ciscoASA(config)# router isis
ciscoASA(config-router)# net 49.0001.0050.0500.5005.00
ciscoASA(config-router)# hostname dynamic
ciscoASA(config-router)#
```

show isis hostname コマンドを入力すると、ダイナミック ホスト マッピング テーブルが表示されます。ダイナミック ホスト マッピング テーブルは、ciscoASA、c2、c3 および routerA という名前のローカル ルータの、ルータ名とシステム ID のマッピング テーブル エントリを表示します。このテーブルは、c3 がレベル-1 ルータであり、そのホスト名がレベル-1 (L1) リンクステート プロトコル (LSP) によりアドバタイズされることも示します。c2 はレベル-2 ルータであり、そのホスト名は L2 LSP によりアドバタイズされます。ASA ciscoASA のレベルの下に表示される * 記号は、これが、ASA のルータ名とシステム ID のマッピング情報であることを示します。

```
ciscoASA# show isis hostname

Level System ID      Dynamic Hostname (c1)
  * 0050.0500.5005   ciscoASA
  1 0050.0500.5007   c3
  2 0050.0500.5006   routerA
  2 0050.0500.5008   c2
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される (受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される (受信ではなく) IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。

コマンド	説明
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティングプロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手动アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティングプロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイプライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis lsp-log

新しい LSP をトリガーしたインターフェイスの、レベル 1 およびレベル 2 の IS-IS リンクステート パケット (LSP) ログを表示するには、特権 EXEC モードで **show isis lsp-log** コマンドを使用します。

show isis lsp-log

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS リンクステート パケット (LSP) のログを表示します。

例

次に、**show isis lsp-log** コマンドの出力例を示します。

```
ciscoasa# show isis lsp-log
```

```

Level 1 LSP log
When      Count      Interface      Triggers
04:16:47      1      subint      CONFIG NEWADJ DIS
03:52:42      2      subint      NEWADJ DIS
03:52:12      1      subint      ATTACHFLAG
03:31:41      1      subint      IPUP
03:30:08      2      subint      CONFIG
03:29:38      1      subint      DELADJ
03:09:07      1      subint      DIS ES
02:34:37      2      subint      NEWADJ
02:34:07      1      subint      NEWADJ DIS

```

```

Level 2 LSP log
When      Count      Interface      Triggers
03:09:27  1           subint        CONFIG NEWADJ
03:09:22  1           subint        NEWADJ
02:34:57  2           subint        DIS
02:34:50  1           subint        IPUP
02:34:27  1           subint        CONFIG DELADJ
02:13:57  1           subint        DELADJ
02:13:52  1           subint        NEWADJ
01:35:58  2           subint        IPIA
01:35:51  1           subint        AREASET IPIA
    
```

表 9-4 `show isis lsp-log` のフィールド

フィールド	説明
When	LSP が生成されてからの経過時間。
Count	このときに発生したイベントの数。
インターフェイス	LSP を再び生成したインターフェイス。
Triggers	<p>LSP のフラッドをトリガーしたイベント。次のような、LSP に可能なトリガー。</p> <ul style="list-style-type: none"> • AREASET: アクティブ エリア セットが変更されました。 • ATTACHFLAG: Attach ビットの状態が変更されました。 • CLEAR: ある形式の手動の clear コマンドが送信されました。 • CONFIG: 任意のコンフィギュレーションが変更されました。 • DELADJ: 隣接関係がダウンしました。 • DIS: DIS が変更されたか、または疑似ノードが変更されました。 • ES: エンドシステムの隣接関係が変更されました。 • HIPPIY: LSPDB 過負荷ビットの状態が変更されました。 • IF_DOWN: 新しい LSP が必要です。 • IP_DEF_ORIG: 元のデフォルト情報が変更されました。 • IPDOWN: 直接接続されている IP プレフィックスがダウンしました。 • IP_EXTERNAL: 再配布された IP ルートが現れたか、または失われました。 • IPIA: エリア間 IP ルートが現れたか、または失われました。 • IPUP: 直接接続されている IP プレフィックスが起動しました。 • NEWADJ: 新しい隣接関係が現れました。 • REDIST: 再配信されたレベル-2 CLNS ルートが変更されました。 • RRR_INFO: RRR 帯域幅リソース情報。

関連コマンド

コマンド	説明
<code>advertise passive-only</code>	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
<code>area-password</code>	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。

コマンド	説明
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される(受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。

コマンド	説明
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis neighbors

IS-IS ネイバーに関する情報を表示するには、特権 EXEC モードで **show isis neighbors** コマンドを使用します。

show isis neighbors [detail]

構文の説明

detail (任意)IS-IS ネイバーの詳細情報を表示します。

コマンドデフォルト

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

show isis neighbors コマンドは、接続されている IS-IS ルータに関する簡潔な情報を表示するために使用されます。**detail** キーワードを入力すると、さらに詳細な情報が表示されます。

例

show isis neighbors command を入力して、IS-IS ネイバーの routerA に関する情報を表示します。

```
ciscoasa# show isis neighbors
```

```
System Id      Type Interface  IP Address      State Holdtime Circuit Id
routerA        L1  subint       22.22.22.5     UP    21           c2.01
routerA        L2  subint       22.22.22.5     UP    22           c2.01
c2             L1  subint       22.22.22.3     UP    9            9          c2.01
c2             L2  subint       22.22.22.3     UP    9            9          c2.01
```

show isis neighbors detail コマンドを入力して、IS-IS ネイバーの routerA に関する詳細情報を表示します。

```
ciscoasa# show isis neighbors detail
```

```
System Id      Type Interface  IP Address      State Holdtime Circuit Id
routerA        L1  subint       22.22.22.5     UP    23           c2.01
Area Address(es): 49.0001
```

```

SNPA:          0025.8407.f2b0
State Changed: 00:03:03
LAN Priority:   64
Format: Phase V
Remote TID:    0
Local TID:     0
Interface name: subint
routerA        L2    subint        22.22.22.5        UP    22                c2.01
Area Address(es): 49.0001
SNPA:          0025.8407.f2b0
State Changed: 00:03:03
LAN Priority:   64
Format: Phase V
Remote TID:    0
Local TID:     0
Interface name: subint
    
```

表 9-5 *show isis neighbors* のフィールド

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
タイプ	レベルのタイプ。 IS-IS ネイバーがレベル 1、レベル-1-2、またはレベル 2 のルータのいずれであるかを示します。
インターフェイス	システムが学習されたインターフェイス。
IP Address	ネイバー ルータの IP アドレス。
状態	IS-IS ネイバーの状態がアップかダウンか示します。
Holdtime	リンクステート パケット (LSP) のホールド時間。 LSP が有効である時間 (秒単位)。
Circuit Id	IS-IS 近接ルータがどのようにローカル ルータに接続されているかを示す、 IS-IS 近接ルータのポート ロケーション。
Area Address(es)	ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。
State Changed	状態が変化しました。
LAN Priority	LAN のプライオリティ。
Remote TID	近接ルータ トポロジの ID。
Local TID	ローカル ルータ トポロジの ID。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアダプタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される(受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をバージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
pre-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis rib

特定のルートのパス、または IP ローカルルーティング情報ベース (RIB) に格納されているメジャー ネットワーク下での全ルートのパスを表示するには、特権 EXEC モードで **show isis rib** コマンドを使用します。

```
show isis [* | ip [unicast] | ipv6 [unicast]] rib [redistribution [level-1 | level-2]] [network_ip [mask]]
```

構文の説明

*	(オプション)すべての IS-IS アドレス ファミリを表示します。
ip	(オプション)IPv4 アドレス ファミリを表示します。
ipv6	(オプション)IPv6 アドレス ファミリを表示します。
level-1	(オプション)レベル 1 再配布 RIB を表示します。
level-2	(オプション)レベル 2 再配布 RIB を表示します。
network_ip [mask]	(オプション)ネットワークの RIB 情報を表示します。
再配布	(オプション)IS-IS IP 再配布 RIB 情報を表示します。
unicast	(オプション)ユニキャスト アドレス ファミリを表示します。

コマンドデフォルト

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IP グローバル RIB 内に存在する IP プレフィックス アップデートが、IS-IS ローカル RIB 内で更新されたことを確認するには、**show isis rib** コマンドを入力します。

例

次に、IS-IS ローカル RIB 内に格納されたすべてのルートを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib

IPv4 local RIB for IS-IS process

IPv4 unicast topology base (TID 0, TOPOID 0x2) = = = = =
10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスが 10.3.2.0 のメジャー ネットワーク 10.0.0.0 下の全ルータを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPv4 unicast topology base (TID 0, TOPOID 0x2) = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレス マスクが 10.3.2.0 255.255.255.0 の ネットワーク下の全ルータを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPv4 unicast topology base (TID 0, TOPOID 0x2) = = = = =
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される(受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をバージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
pre-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis spf-log

ルータがフル最短パス優先(SPF)計算を実行した頻度と理由を表示するには、特権 EXEC モードで **show isis spf-log** コマンドを使用します。

```
show isis [* | ip [unicast] | ipv6 [unicast]] spf-log
```

構文の説明

*	(オプション)すべての IS-IS アドレス ファミリを表示します。
ip	(オプション)IPv4 アドレス ファミリを表示します。
ipv6	(オプション)IPv6 アドレス ファミリを表示します。
unicast	(オプション)ユニキャストアドレス ファミリを表示します。

コマンドデフォルト

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ルータがフル最短パス優先(SPF)計算を実行した頻度と理由を表示します。

例

次に、**show isis ipv6 spf-log** コマンドの出力例を示します。

```
ciscoasa# show isis ipv6 spf-log
```

```
TID 0 level 1 SPF log
  When   Duration  Nodes  Count  First trigger LSP  Triggers
00:15:46  3124      40     1      milles.00-00  TLVCODE
00:15:24  3216      41     5      milles.00-00  TLVCODE NEWLSP
00:15:19  3096      41     1      deurze.00-00  TLVCODE
00:14:54  3004      41     2      milles.00-00  ATTACHFLAG LSPHEADER
00:14:49  3384      41     1      milles.00-01  TLVCODE
00:14:23  2932      41     3      milles.00-00  TLVCODE
00:05:18  3140      41     1                          PERIODIC
```

```

00:03:54 3144 41 1 milles.01-00 TLVCODE
00:03:49 2908 41 1 milles.01-00 TLVCODE
00:03:28 3148 41 3 bakel.00-00 TLVCODE TLVCONTENT
00:03:15 3054 41 1 milles.00-00 TLVCODE
00:02:53 2958 41 1 mortel.00-00 TLVCODE
00:02:48 3632 41 2 milles.00-00 NEWADJ TLVCODE
00:02:23 2988 41 1 milles.00-01 TLVCODE
00:02:18 3016 41 1 gemert.00-00 TLVCODE
00:02:14 2932 41 1 bakel.00-00 TLVCONTENT
00:02:09 2988 41 2 bakel.00-00 TLVCONTENT
00:01:54 3228 41 1 milles.00-00 TLVCODE
00:01:38 3120 41 3 rips.03-00 TLVCONTENT

```

表 9-6 show isis spf-log のフィールド

フィールド	説明
When	今からどれくらい前(時間:分:秒)にフル SPF 計算が発生したか。直近 20 回分の発生内容が記録されます。
持続時間	今回の SPF 実行を完了させるために必要なミリ秒数。経過時間は実経過時間であり、CPU 時間ではありません。
ノード	今回の SPF 実行で計算されるトポロジを生成するルータおよび疑似ノード(LAN)の数。
Count	今回の SPF 実行をトリガーしたイベントの数。トポロジが変更されると、複数のリンクステートパケット(LSP)が短時間で受信されます。ルータは、フル SPF を実行するまでに 5 秒待機し、すべての新しい情報を保持できるようにします。この数は、ルータがフル SPF を実行するまで 5 秒待機する間に発生した(新しい LSP の受信のような)イベントの数を意味します。
First trigger LSP	新しい LSP の到着でフル SPF 計算がトリガーされると、常にルータは LSP ID を保存します。LSP ID は、エリア内でルーティングが不安定である原因の手掛かりを提供できます。複数の LSP が 1 つの SPF を実行すると、最後に受信された LSP の LSP ID だけが記憶されます。
Triggers	フル SPF 計算をトリガーしたすべての理由のリスト。トリガーに関する次の表を参照してください。

表 9-7 spf-log Triggers

Trigger	説明
ATTACHFLAG	このルータは、レベル 2 バックボーンに接続されているか、または、レベル 2 バックボーンとの接続を失ったばかりです。
ADMINDIST	このルータの IS-IS プロセスに、別のアドミニストレーティブ ディスタンスが設定されました。
AREASET	このエリアの学習されたエリア アドレスの設定が変更されました。
BACKUPOVFL	IP プレフィックスが失われました。ルータはそのプレフィックスに到達するために別の方法があることを知っていますが、そのバックアップルートは保存していません。別のルートを見つける唯一の方法は、フル SPF の実行です。
DBCHANGED	このルータで、clear isis * コマンドが発行されました。

表 9-7 *spf-log Triggers (続き)*

Trigger	説明
IPBACKUP	IP ルートが失われましたが、これは IS-IS を介してではなく、優れたアドミニストレーティブ ディスタンスを持つ別のプロトコルを介して学習されました。IS-IS はフル SPF を実行し、失われた IP プレフィックスまでの IS-IS ルートをインストールします。
IPQUERY	このルータで、clear ip route コマンドが発行されました。
LSPEXPIRED	リンクステート データベース (LSDB) 内のいくつかの LSP の期限が切れましました。
LSPHEADER	LSP ヘッダー内の ATT/P/OL ビットまたは IS タイプが変更されました。
NEWADJ	このルータが、別のルータとの新しい隣接関係を作成しました。
NEWAREA	このルータに、新しいエリアが (Network Entity Title [NET] を介して) 設定されました。
NEWLEVEL	このルータに、(IS タイプを介して) 新しいレベルが設定されました。
NEWLSP	トポロジ内に新しいルータまたは疑似ノードが現れました。
NEWMETRIC	このルータのインターフェイスに、新しいメトリックが設定されました。
NEWSYSID	このルータに、(NET を介して) 新しいシステム ID が設定されました。
PERIODIC	ルータは通常、15 秒ごとの間隔でフル SPF 計算を実行します。
RTCLEARED	このルータで、clear clns route コマンドが発行されました。
TLVCODE	TLV コードの不一致であり、最新バージョンの LSP に異なる TLV が含まれていることを示します。
TLVCONTENT	TLV のコンテンツが変更されました。これは通常、エリア内で隣接関係がアップまたはダウンしたことを示します。「First trigger LSP」カラムは、不安定な状態が発生した可能性のある場所を示します。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される (受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。

コマンド	説明
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。

コマンド	説明
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis topology

すべてのエリア内の接続された全ルータのリストを表示するには、特権 EXEC モードで **show isis topology** コマンドを使用します。

show isis [* | **ip** [unicast] | **ipv6** [unicast]] **topology** [level-1 | level-2]

構文の説明

*	(オプション)すべての IS-IS アドレス ファミリを表示します。
ip	(オプション)IPv4 アドレス ファミリを表示します。
ipv6	(オプション)IPv6 アドレス ファミリを表示します。
level-1	(オプション)エリア内のすべてのレベル 1 ルータへのパスを表示します。
level-2	(オプション)ドメイン内のすべてのレベル 2 ルータへのパスを表示します。
unicast	(オプション)ユニキャスト アドレス ファミリを表示します。

コマンドデフォルト

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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

show isis topology コマンドを使用すると、すべてのエリア内の全ルータの存在およびルータ間の接続状態を確認できます。

例

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

```
ciscoasa# show isis topology

IS-IS TID 0 paths to level-1 routers
System Id      Metric      Next-Hop      Interface      SNPA
-----
cisco1         --
routerA        10          routerA       subint         0025.8407.f2b0
```

```

c3                10
c2                10                c2                subint
c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id        Metric    Next-Hop        Interface    SNPA
cisco1          --
routerA         10                routerA        subint        0025.8407.f2b0
c3              10
c2              10                c2                subint
c08c.60e6.986f

```

表 9-8 `show isis topology` のフィールド

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
メトリック	送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先 (IP アドレス、エンドシステム [ES]、または CLNS プレフィックス) に到達するコスト用のメトリック。
Next-Hop	ネクスト ホップ ルータのアドレス。
インターフェイス	システムが学習されたインターフェイス。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。

関連コマンド

コマンド	説明
<code>advertise passive-only</code>	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
<code>area-password</code>	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
<code>authentication mode</code>	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
<code>authentication send-only</code>	グローバルな IS-IS インスタンスでは、送信される (受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
<code>clear isis</code>	IS-IS データ構造をクリアします。
<code>default-information originate</code>	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
<code>distance</code>	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
<code>domain-password</code>	IS-IS ドメイン認証パスワードを設定します。
<code>fast-flood</code>	IS-IS LSP がフルになるように設定します。
<code>hello padding</code>	IS-IS hello をフル MTU サイズに設定します。
<code>hostname dynamic</code>	IS-IS ダイナミック ホスト名機能を有効にします。
<code>ignore-lsp-errors</code>	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパーズするのではなく無視するように ASA を設定します。
<code>isis adjacency-filter</code>	IS-IS 隣接関係の確立をフィルタ処理します。

コマンド	説明
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。

コマンド	説明
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show kernel

デバッグに使用できる Linux brctl ユーティリティが提供する情報を表示するには、特権 EXEC モードで **show kernel** コマンドを使用します。

show kernel [process | bridge | cgroup-controller | ifconfig | module]

構文の説明

bridge	タップのブリッジを表示します。
cgroup-controller	cgroup-controller の統計情報を表示します。
ifconfig	タップおよびブリッジ インターフェイスの統計情報を表示します。
module	インストールおよび実行されているモジュールを表示します。
process	ASA で実行されているアクティブなカーネル プロセスの現在のステータスを表示します。

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
8.0(2)	このコマンドが追加されました。
8.4(1)	cgroup-controller キーワードが追加されました。
8.6(1)	ifconfig 、 module 、および bridge キーワードが追加されました。

使用上のガイドライン

このコマンドは、カーネルで実行されるさまざまなプロセスの統計情報を表示します。

例

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

```
ciscoasa# show kernel process
```

```
PID  PPID  PRI  NI      VSIZE      RSS      WCHAN  STAT  RUNTIME  COMMAND
  1     0   16   0     991232     268  3725684979  S      78  init
  2     1   34  19         0         0  3725694381  S         0  ksoftirqd/0
  3     1   10  -5         0         0  3725736671  S         0  events/0
  4     1   20  -5         0         0  3725736671  S         0  khelper
```

```

 5   1  20 -5      0      0 3725736671   S      0 kthread
 7   5  10 -5      0      0 3725736671   S      0 kblockd/0
 8   5  20 -5      0      0 3726794334   S      0 kseriod
66   5  20  0      0      0 3725811768   S      0 pdflush
67   5  15  0      0      0 3725811768   S      0 pdflush
68   1  15  0      0      0 3725824451   S      2 kswapd0
69   5  20 -5      0      0 3725736671   S      0 aio/0
171  1  16  0      991232    80 3725684979   S      0 init
172 171  19  0      983040   268 3725684979   S      0 rcS
201 172  21  0     1351680   344 3725712932   S      0 lina_monitor
202 201  16  0 1017602048 899932 3725716348   S     212 lina
203 202  16  0 1017602048 899932      0   S      0 lina
204 203  15  0 1017602048 899932      0   S      0 lina
205 203  15  0 1017602048 899932 3725712932   S      6 lina
206 203  25  0 1017602048 899932      0   R 13069390 lina
ciscoasa#

```

表 9-9 に、各フィールドの説明を示します。

表 9-9 `show kernel process` のフィールド

フィールド	説明
PID	プロセス ID。
PPID	親プロセス ID。
PRI	プロセスのプライオリティ。
NI	プライオリティの計算に使用されるナイス値。値は 19(最大ナイス値)～-19(最小ナイス値)の範囲です。
VSIZE	仮想メモリのサイズ(バイト単位)。
RSS	プロセスの Resident Set Size(KB 単位)。
WCHAN	プロセスが待機しているチャンネル。
STAT	プロセスの状態。 <ul style="list-style-type: none"> • R:実行中 • S:割り込み可能な待機状態でスリープ中 • D:割り込み不可能なディスク スリープで待機中 • Z:ゾンビ • T:トレースまたは停止(信号による) • P:ページング
RUNTIME	プロセスがユーザモードまたはカーネルモードでスケジュールされている jiffy の数。実行時間は utime と stime の合計です。
COMMAND	プロセス名。

次に、`show kernel module` コマンドの出力例を示します。

```

ciscoasa# show kernel module

Module          Size  Used by  Tainted: P
cpp_base        861808  2
kvm_intel       44104   8
kvm             174304  1 kvm_intel
msrif           4180    0
tscsync        3852    0

```

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

```
ciscoasa# show kernel ifconfig

br0      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:43 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.255.255.255
         UP LOOPBACK RUNNING  MTU:16436  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0     Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
         inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:148 errors:0 dropped:0 overruns:0 frame:0
         TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1     Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:259 errors:0 dropped:0 overruns:0 frame:0
         TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2     Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3     Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:187 errors:0 dropped:0 overruns:0 frame:0
         TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4     Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

関連コマンド

コマンド	説明
show module	ASA にインストールされているモジュールに関する情報を表示します。

show kernel bridge

デバッグに使用できる各ポート上で学習された Linux ブリッジ、それらのメンバー ポート、および MAC アドレスを表示するには、特権 EXEC モードで **show kernel bridge** コマンドを使用します。

show kernel bridge [*mac-address bridge name*]

構文の説明

<i>bridge name</i>	ブリッジの名前を表示します。
<i>mac-address</i>	各ポートに関連付けられた MAC アドレスを表示します。

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
8.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、デバッグに使用できる各ポート上で学習された Linux ブリッジ、それらのメンバー ポート、および MAC アドレス(リモート MAC アドレスを含む)を表示します。

例

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

```
ciscoasa# show kernel bridge

bridge name      bridge id          STP enabled interfaces
br0              8000.0e3cd8a8909f no                tap1
                                                         tap3
br1              8000.26d29f51a490 no                tap2
                                                         tap4
                                                         tap5hostname#
```

次に、**show kernel bridge mac-address** コマンドの出力例を示します。

```
ciscoasa# show kernel bridge mac-address br1
```

```
port no    mac addr      is local?  ageing timer
 1   00:21:d8:cb:dc:f7   no          12.93
 3   00:22:bd:d8:7d:da   no          12.93
 2   26:d2:9f:51:a4:90   yes         0.00
 1   4e:a4:e0:73:1f:ab   yes         0.00
 3   52:04:38:3d:79:c0   yes         0.00
```

関連コマンド

コマンド	説明
show kernel	ASA にインストールされているモジュールに関する情報を表示します。

show lacp

EtherChannel LACP 情報(トラフィック統計情報、システム ID、およびネイバーの詳細など)を表示するには、特権 EXEC モードで次のコマンドを入力します。

```
show lacp {[channel_group_number]} {counters | internal | neighbor} | sys-id
```

構文の説明

<i>channel_group_number</i>	(オプション)EtherChannel チャンネル グループ番号を 1 ~ 48 の範囲で指定して、このチャンネル グループに関する情報だけを表示します。
counters	送受信された LACPDU 数およびマーカー数のカウンタを表示します。
internal	内部情報を表示します。
neighbor	ネイバー情報を表示します。
sys-id	LACP システム ID を表示します。

コマンドデフォルト

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。

例

次に、**show lacp sys-id** コマンドの出力例を示します。

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

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

```
ciscoasa# show lacp counters
```

```

          LACPDU      Marker      Marker Response      LACPDU
Port      Sent   Recv      Sent   Recv      Sent   Recv      Pkts Err
-----
Channel group: 1
Gi3/1      736   728        0     0         0     0         0
Gi3/2      739   730        0     0         0     0         0
Gi3/3      739   732        0     0         0     0         0

```

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

```
ciscoasa# show lacp internal

Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State      LACP port  Admin   Oper   Port      Port
-----  -
Port      Flags  State      Priority   Key     Key     Number    State
-----  -
Gi3/1    SA     bndl       32768     0x1    0x1    0x302     0x3d
Gi3/2    SA     bndl       32768     0x1    0x1    0x303     0x3d
Gi3/3    SA     bndl       32768     0x1    0x1    0x304     0x3d
```

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

```
ciscoasa# show lacp neighbor

Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
Port      Partner Partner  LACP Partner  Partner  Partner  Partner  Partner
-----  -
Port      Flags  State      Port Priority Admin Key Oper Key Port Number Port State
-----  -
Gi3/1    SA     bndl       32768     0x0    0x1    0x306     0x3d
Gi3/2    SA     bndl       32768     0x0    0x1    0x303     0x3d
Gi3/3    SA     bndl       32768     0x0    0x1    0x302     0x3d
```

関連コマンド

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 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 lacp cluster

cLACP システムの MAC および ID を表示するには、特権 EXEC モードで **show lacp cluster** コマンドを使用します。

show lacp cluster {system-mac | system-id}

構文の説明

system-mac	システム ID と、それが自動生成されたのか手動入力されたのかを表示します。
system-id	システム ID およびプライオリティを表示します。

コマンドデフォルト

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
9.0(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

clacp system-mac コマンドを使用して cLACP システムの ID およびプライオリティを設定します。

例

次に、**show lacp cluster system-mac** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

次に、**show lacp cluster system-id** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5      ,a300.010a.010a
```

関連コマンド

コマンド	説明
clacp system-mac	cLACP システムの ID およびプライオリティを設定します。

show license

スマート ライセンスのステータスを表示するには、特権 EXEC モードで **show license** コマンドを使用します。



(注)

この機能は、ASA v だけでサポートされています。

show license [all | entitlement | cert | pool | registration | features

構文の説明

all	スマート ライセンスの状態、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、権限付与ステータス、ライセンス証明書情報、およびスマート エージェント タスクのスケジュールを表示します。
entitlement	使用中の各権限、ハンドル(整数 ID など)、数、タグ、強制モード(適合、非適合など)、バージョン、および権限が要求されたタイミングに関する詳細情報を表示します。
cert	ID 証明書の内容、発行日、および有効期限を表示します。
プール	このデバイスが割り当てられる権限付与プールを表示します。
登録	現在のスマート ライセンスの登録ステータスを表示します。
機能	現在のライセンスを表示します。

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。

	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
コマンドモード					
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
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

show activation-key コマンドは、**show license features** コマンドと同じ出力を提供します。

例

次に、基本ライセンスのみ(現在のライセンス権限なし)の ASA の例を示します。

Serial Number: 9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

```

Licensed features for this platform:
Maximum Physical Interfaces      : 10           perpetual
Maximum VLANs                   : 50           perpetual
Inside Hosts                    : Unlimited   perpetual
Failover                        : Active/Standby perpetual
Encryption-DES                  : Enabled     perpetual
Encryption-3DES-AES             : Enabled     perpetual
Security Contexts               : 0           perpetual
GTP/GPRS                        : Disabled    perpetual
AnyConnect Premium Peers        : 2           perpetual
AnyConnect Essentials           : Disabled    perpetual
Other VPN Peers                 : 250         perpetual
Total VPN Peers                 : 250         perpetual
Shared License                  : Disabled    perpetual
AnyConnect for Mobile           : Disabled    perpetual
AnyConnect for Cisco VPN Phone  : Disabled    perpetual
Advanced Endpoint Assessment    : Disabled    perpetual
UC Phone Proxy Sessions         : 2           perpetual
Total UC Proxy Sessions         : 2           perpetual
Botnet Traffic Filter           : Enabled     perpetual
Intercompany Media Engine       : Disabled    perpetual
Cluster                         : Disabled    perpetual
    
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマートライセンス設定をクリアします。
feature tier	スマートライセンスの機能層を設定します。
http-proxy	スマートライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマートライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show running-config license	スマートライセンスの設定を表示します。
throughput level	スマートライセンスのスループットレベルを設定します。

show lisp eid

ASA EID テーブルを表示するには、特権 EXEC モードで **show lisp eid** コマンドを使用します。

```
show lisp eid [site-id id]
```

構文の説明

site-id id 特定のサイトの EID のみを表示します。

コマンドデフォルト

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	トランスプレセント	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
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は EID と サイト ID を 相関付ける EID テーブルを維持します。テーブルを表示するには、**show lisp eid** コマンドを使用します。

クラスター フロー モビリティの LISP インспекションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスターリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスター メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスター フロー モビリティには複数の相互に関連する設定が含まれています。

1. (オプション)ホストまたはサーバの IP アドレスに基づく検査される EID の限定:最初のホップ ルータは、ASA クラスターが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスターに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスターが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスターに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。

2. LISP トラフィックのインスペクション: ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID と サイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー: ビジネス クリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID: ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定: クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラス のトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、**show lisp eid** コマンドの出力例を示します。

```
ciscoasa# show lisp eid
LISP EID      Site ID
10.44.33.105  2
10.44.33.201  2
192.168.11.1  4
192.168.11.2  4
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

show local-host

ローカルホストのネットワーク状態を表示するには、特権 EXEC モードで **show local-host** を使用します。

```
show local-host [hostname | ip_address] [detail] [brief] [all] [connection {sctp | tcp | udp |
embryonic} start[-end]] [zone [zone-name]]
```

構文の説明

all	(廃止)ASA に接続するローカルホストと、ASA から接続するローカルホストが含まれます。
brief	(オプション)ローカルホストに関する簡潔な情報を表示します。
connection {sctp tcp udp embryonic} start[-end]	(廃止)番号と接続のタイプに基づいて、初期、TCP、UDP、または SCTP のフィルタを適用します。 <i>start</i> の数値は、そのタイプの最小接続数を示します。 <i>-end</i> の数値を含めると、10-100 などの範囲を指定できます。これらのフィルタは個別に使用することも、組み合わせて使用することもできます。
detail	(任意)アクティブな xlate およびネットワーク接続の詳細情報を含めた、ローカルホスト情報の詳細なネットワーク状態を表示します。
<i>hostname ip_address</i>	(オプション)ローカルホスト名または IPv4/IPv6 アドレスを指定します。
zone [zone_name]	(オプション)ゾーンごとにローカルホストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	ホスト制限があるモデルでは、このコマンドにより、外部インターフェイスと見なされるインターフェイスが表示されるようになりました。
7.2(4)	新しい2つのオプション、 connection と brief が show local-host コマンドに追加され、出力が内部ホストの接続数でフィルタリングされるようになりました。
9.1(2)	テレメトリベースのアラートとしてシスコに Smart Call Home 情報を送信するコマンドが、 show local-host コマンドから show local-host include interface コマンドに変更されました。これは、インターフェイスアドレス情報を提供します。

リリース	変更内容
9.3(2)	zone キーワードが追加されました。
9.5(2)	表示が変更され、アスタリスク(*)でバックアップ ポートのブロックが示されるようになりました。
9.5(2)	SCTP 接続が出力に追加されました。 connection sctp キーワードが追加されました。
9.14(1)	接続フィルタのキーワード:初期、TCP、UDP、または SCTP は廃止されました。

使用上のガイドライン

show local-host コマンドを使用すると、ローカル ホストのネットワーク状態を表示できます。ローカル ホストは、トラフィックを ASA に送信するか、またはトラフィックを通じて転送する任意のホストに対して作成されます。

このコマンドを使用すると、ローカル ホストの変換スロットおよび接続スロットを表示できます。変換情報には、ホストに割り当てられた **PAT** ポートのブロックが含まれます。

ホスト制限のあるモデルの場合、ルーテッド モードで、内部のホスト(ワーク ゾーンとホーム ゾーン)は、外部(インターネット ゾーン)と通信するときのみ制限値にカウントされます。インターネット ホストは制限値にカウントされません。ワークとホームの間のトラフィックを開始するホストも、制限値にカウントされません。デフォルト ルートに関連付けられたインターフェイスは、インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイス上のホストが制限値にカウントされます。トランスペアレント モードでは、ホスト数が最小のインターフェイスがホスト制限値にカウントされます。

廃止されたオプション

このコマンドでは、接続の制限数も表示されます。接続制限が設定されていない場合、値として 0 が表示され、制限は適用されません。

TCP 代行受信が設定されている場合に、**SYN** 攻撃が発生すると、**show local-host** コマンド出力では、代行受信された接続の数が使用回数に計上されます。このフィールドは通常、完全なオープン接続のみを表示します。

show local-host コマンド出力では、スタティック接続を使用するホストに対して最大初期接続の制限値(**TCP** 代行受信の水準点)が設定されている場合に、**TCP embryonic count to host counter** が使用されます。このカウンタは、他のホストからこのホストに向かう初期接続の合計を示します。この合計が設定された最大制限値を超過すると、このホストへの新規接続に **TCP** 代行受信が適用されます。

例

次に、**show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host

Interface mgmt: 2 active, 2 maximum active
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
```

```
TCP intercept watermark = unlimited
UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active,
Interface outside: 0 active, 0 maximum active
Interface any: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限がある ASA での **show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限がある ASA での **show local-host** コマンドの出力例を示します。ただし、デフォルトルートがない場合、ホスト制限はすべてのインターフェイスに適用されます。デフォルトルート インターフェイスは、デフォルト ルートまたはルートが使用するインターフェイスがダウンしている場合は検出できないことがあります。

```
ciscoasa# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface clin: 1 active, 1 maximum active
Interface clout: 0 active, 0 maximum active
```

次に、ホスト制限がない ASA での **show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host
Licensed host limit: Unlimited

Interface clin: 1 active, 1 maximum active
Interface clout: 0 active, 0 maximum active
```

次の例では、特定のホストに関する情報に続けて、そのホストの詳細情報を示しています。

```
ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active

ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
```

```
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
```

Xlate:

```
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri
```

Conn:

```
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active
```

関連コマンド

コマンド	説明
clear local-host	(廃止) show local-host コマンドによって表示されるローカルホストからのネットワーク接続を解放します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show logging

バッファ内のログまたはその他のロギング設定を表示するには、特権 EXEC モードで **show logging** コマンドを使用します。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting** | **flow-export-syslogs**]

構文の説明

all	(任意)すべての syslog メッセージ ID と、有効か無効かを表示します。
asdm	(任意)ASDM ロギング バッファの内容を表示します。
flow-export-syslogs	(オプション)NetFlow に送信されるメッセージと、それらがイネーブルかディセーブルかを表示します。
message	(任意)デフォルト以外のレベルにあるメッセージを表示します。メッセージ レベルを設定するには、 logging message コマンドを参照してください。
queue	(任意)syslog メッセージ キューを表示します。
設定	(任意)ロギング設定を表示します。ロギング バッファは表示されません。
<i>syslog_id</i>	(任意)表示するメッセージ番号を指定します。

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
7.0(1)	このコマンドが追加されました。
8.0(2)	syslog サーバが SSL/TLS 接続を使用するように設定されているかどうかを示します。
8.1(1)	flow-export-syslogs キーワードが追加されました。
8.4(1)	show logging コマンドでは、監査ブロックの現在の状態に関するエントリが出力に含まれます。
9.7(1)	このコマンドの出力には、IPv6 アドレスで設定された syslog サーバが含まれています。

使用上のガイドライン

logging buffered コマンドを使用している場合、キーワードなしの **show logging** コマンドからは、現在のメッセージバッファと現在の設定が表示されます。

show logging queue コマンドを使用すると、次の情報を表示できます。

- キュー内のメッセージ数
- キュー内に記録されたメッセージの最大数
- 処理に利用できるブロックメモリがなかったために廃棄されたメッセージ数
- トラップおよび他の **syslog** メッセージごとに別々のキュー



(注) ゼロは、設定するキューサイズとして許容される数値であり、最大許容キューサイズを示します。設定されたキューサイズが 0 の場合は、**show logging queue** コマンドの出力に実際のキューサイズが示されます。

例

次に、**show logging** コマンドの出力例を示します。

```
ciscoasa(config)# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: enabled
  Standby logging: disabled
  Debug-trace logging: disabled
  Console logging: level informational, 3962 messages logged
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level informational, facility 20, 20549 messages logged
    Logging to inside 10.2.5.3 tcp/50001 connected
  Permit-hostdown state
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging: disabled
```



(注) *state* の有効な値は、enabled、disabled、disabled-blocking、および disabled-not blocking です。

次に、セキュア syslog サーバが設定された **show logging** コマンドの出力例を示します。

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
ciscoasa(config)# show logging
Syslog logging: disabled
  Facility:
  Timestamp logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: level debugging, 135 messages logged
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: list show _syslog, facility, 20, 21 messages logged
    Logging to inside 10.0.0.1 tcp/1500 SECURE
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging disabled
```

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

```
ciscoasa(config)# show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

次に、**show logging message all** コマンドの出力例を示します。

```
ciscoasa(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

次に、NetFlow に送信されるメッセージと、それらがイネーブルかディセーブルかを表示する例を示します。

```
ciscoasa# show logging flow-export-syslogs
Syslog ID      Type              Status
302013         Flow Created     Enabled
302015         Flow Created     Enabled
302017         Flow Created     Enabled
302020         Flow Created     Enabled
302014         Flow Deleted     Enabled
302016         Flow Deleted     Enabled
302018         Flow Deleted     Enabled
302021         Flow Deleted     Enabled
106015         Flow Denied      Enabled
106023         Flow Denied      Enabled
313001         Flow Denied      Enabled
313008         Flow Denied      Enabled
710003         Flow Denied      Enabled
106100         Flow Created/Denied Enabled
```

関連コマンド

コマンド	説明
logging asdm	ASDM へのロギングをイネーブルにします。
logging buffered	バッファへのロギングをイネーブルにします。
logging flow-export-syslogs	NetFlow データに関連付けられている syslog メッセージをイネーブルまたはディセーブルにします。
logging host	syslog サーバを定義します。
logging message	メッセージ レベルを設定するか、またはメッセージをディセーブルにします。
logging queue	ロギング キューを設定します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

show mac-address-table [*interface_name* | **count** | **static** | **vtep-mapping**]

構文の説明

count	(任意) ダイナミックおよびスタティック エントリの合計数を一覧します。
<i>interface_name</i>	(任意) MAC アドレス テーブル エントリを表示するインターフェイス名を指定します。
静的	(任意) スタティック エントリのみを一覧します。
vtep-mapping	(オプション) リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル (MAC アドレス テーブル) を表示します。

デフォルト

インターフェイスを指定しない場合、すべてのインターフェイス MAC アドレス エントリが表示されます。

コマンドモード

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。
9.4(1)	vtep-mapping キーワードが追加されました。
9.7(1)	ルーテッド モードのサポートが追加されました。

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table
interface      mac address      type      Time Left
-----
outside        0009.7cbe.2100  static    -
inside         0010.7cbe.6101  static    -
inside         0009.7cbe.5101  dynamic   10
```

次に、内部インターフェイスの **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table inside
interface      mac address      type      Time Left
-----
inside         0010.7cbe.6101   static    -
inside         0009.7cbe.5101   dynamic   10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table count
Static      mac-address bridges (curr/max): 0/65535
Dynamic     mac-address bridges (curr/max): 103/65535
```

show mac-address-table vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show mac-address-table vtep-mapping
interface      mac address      type      Age(min)  bridge-group  VTEP
-----
vni-outside    00ff.9200.0000   dynamic   5          1             10.9.1.3
vni-inside     0041.9f00.0000   dynamic   5          1             10.9.1.3
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォールモードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show mac-learn

各インターフェイスに対して MAC ラーニングがイネーブルかディセーブルかを表示するには、特権 EXEC モードで **show mac-learn** を使用します。

show mac-learn

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	ルーテッドモードのサポートが追加されました。

使用上のガイドライン

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、システムは対応するエントリを MAC アドレス テーブルに追加します。インターフェイスごとに MAC ラーニングをディセーブルにすることができます。

例

次に、**show mac-learn** コマンドの出力例を示します。

```
ciscoasa# show mac-learn
no mac-learn flood
interface                               mac learn
-----
outside                                  enabled
inside1_2                                enabled
inside1_3                                enabled
inside1_4                                enabled
inside1_5                                enabled
inside1_6                                enabled
inside1_7                                enabled
inside1_8                                enabled
diagnostic                               enabled
inside                                    enabled
```

関連コマンド

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show management-access

管理アクセスに設定された内部インターフェイスの名前を表示するには、特権 EXEC モードで show management-access コマンドを使用します。

show management-access

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。

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。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます(インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます)。

例

次に、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する例を示します。

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	ASA の管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show-map-domain

マッピングアドレスおよびポート (MAP) ドメインを表示するには、特権 EXEC モードで **show map-domain** コマンドを使用します。

show map-domain

デフォルト

デフォルト設定はありません。

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 モード。	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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 map-domain コマンドによって MAP コンフィギュレーションが表示されます (**show running-config map-domain** と同様) が、同時にドメイン設定が有効かどうかとも示されます。

例

次の例には、2 つのドメイン (1 と 2) があります。この出力では、MAP ドメイン 2 が不完全なためにアクティブではないことが説明されています。

```
ciscoasa(config)# show map-domain

MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート (MAP) ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート (MAP) ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

show memory

物理メモリの最大量、およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示するには、特権 EXEC モードで **show memory** コマンドを使用します。

show memory [detail]

構文の説明

detail (任意) 空きメモリおよび割り当て済みシステム メモリの詳細ビューを表示します。

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 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。
9.2(1)	ASA v をサポートするために、仮想マシン (VM) の統計情報が出力に追加されました。
9.3(2)	内部メモリ マネージャが show memory detail コマンドの標準 <code>glibc</code> ライブラリに置き換えられました。

使用上のガイドライン

show memory コマンドで、物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示できます。メモリは必要に応じて割り当てられます。

SNMP を使用して **show memory** コマンドから情報を表示することもできます。

show memory detail の出力を **show memory binsize** コマンドとともに使用して、メモリ リークをデバッグできます。

show memory detail コマンド出力は、要約、DMA メモリ、ヒープ メモリの 3 つのセクションに分割できます。要約には、メモリ全体の割り当てが表示されます。DMA にリンクしていないメモリ、または予約されていないメモリは、ヒープと見なされます。Free memory の値は、ヒープ内の未使用メモリです。Used memory の値は、割り当て済みのメモリの合計を示します。ヒープ割り当ての明細は、出力の後半で表示されます。予約メモリおよび DMA 予約メモリは、別のシステムプロセスおよび主に VPN サービスによって使用されます。

Free memory は、Heapcache Pool、Global Shared Pool、および System の 3 つの部分に分かれています。Heapcache Pool と Global Shared Pool は、glibc ヒープで利用可能なメモリの空き容量です。System は、基盤となるシステムから割り当てることができる使用可能なメモリです。ASA で使用可能な Free memory の総容量は、Heapcache Pool、Global Shared Pool、および System の合計です。

Used memory は Heapcache Pool、Global Shared Pool、Reserved、および System Overhead の 4 つの部分に分かれています。Heapcache Pool と Global Shared Pool プールは、glibc ヒープの Used memory の容量です。予約メモリ (DMA) は、DMA のプールに予約されているメモリ量です。System オーバーヘッドは、さまざまな実行プロセスの glibc オーバーヘッドおよびプロセスオーバーヘッドです。

- メモリは、起動時に DMA とヒープキャッシュ用に予約されます。
- 最初に、ヒープメモリはヒープキャッシュから割り当てられ、その後にヒープキャッシュがなくなると、グローバル共有プールから割り当てられます。
- グローバル共有プールでは、必要に応じてシステムからメモリが渡されます。メモリが解放されて返せるようになるたびに、システムに返します。
- 空きヒープメモリの合計は、ヒープキャッシュとグローバル共有プールのメモリ容量に、システムの空きメモリ容量を加えたものです。

割り当てられたメモリの統計情報の合計(バイト)列に表示される値は、**show memory detail** コマンド出力の実際の値(MEMPOOL_GLOBAL_SHARED POOL STATS)ではありません。



(注)

バージョン 9.3(2) より前は、すべてのシステムメモリ (DMA プール用を除き) が MEMPOOL_GLOBAL_SHARED の一部として表示されます。つまり、すべての割り当て可能な空きメモリが、MEMPOOL_GLOBAL_SHARED にありました。バージョン 9.3(2) では、MEMPOOL_GLOBAL_SHARED は、ブートアップ時にすべてのシステムメモリを取得しませんが、必要なときは常に、基盤となるオペレーティングシステムにメモリを要求します。同様に、大量のメモリが解放されたときは、システムにメモリが返されます。その結果、MEMPOOL_GLOBAL_SHARED のサイズは需要に応じて増減されて表示されます。割り当てを高速化するため、最小空きメモリ量は、MEMPOOL_GLOBAL_SHARED に残されます。

出力は、サイズ 49,152 のブロックが空きプールに割り当てられてから戻され、別のサイズ 131,072 のブロックが割り当てられていることを示します。この場合、空きメモリは $131,072 - 49,152 = 81,920$ バイト単位で減少しますが、実際は 100,000 バイトずつ減少します(空きメモリの行を参照)。

ciscoasa# **show memory detail**

```
Free memory heap:                1193358928 bytes (13%)
Free memory system:             6596267951 bytes (74%)
Used memory:
  Allocated memory in use:      464188448 bytes ( 5%)
  Reserved memory (DMA):        513802240 bytes ( 6%)
  Memory overhead:              202659216 bytes ( 2%)
-----
Total memory:                    8970276783 bytes (100%)

Least free memory:              7963442431 bytes (89%)
Most used memory:               1006834352 bytes (11%)
MEMPOOL_HEAPCACHE_0 POOL STATS:

Non-mmapped bytes allocated =   1541406720
Number of free chunks          =                633
Number of mmapped regions     =                0
```

```

Mmapped bytes allocated      =          0
Max memory footprint         = 1541406720
Keepcost                     = 1190961440
Max contiguous free mem      = 1190961440
Allocated memory in use     = 348047792
Free memory                   = 1193358928

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
32	177	5664
48	204	9792
64	161	10304
80	3	240
96	1	96**
112	2	224
160	5	800
192	1	192
208	1	208
224	1	224
240	1	240
256	13	4064
384	2	864
512	3	1648
1024	1	1296
12288	1	13792
24576	2	57424
32768	1	43824
65536	1	65616
262144	1	322672
1572864	1	1843712
1190961440	1	1190961440*

* - top most releasable chunk.

** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
80	1637	130960
96	13898	1334208
112	3422	383264
128	1910	244480
144	3677	529488
160	463	74080
176	856	150656
192	357	68544
208	350	72800
224	370	82880
240	337	80880
256	2293	587008
384	596	228864
512	657	336384
768	504	387072
1024	449	459776
1536	1217	1869312
2048	376	770048
3072	137	420864
4096	652	2670592

6144	73	448512
8192	212	1736704
12288	643	7901184
16384	598	9797632
24576	31	761856
32768	77	2523136
49152	31	1523712
65536	200	13107200
98304	30	2949120
131072	20	2621440
196608	28	5505024
262144	14	3670016
393216	23	9043968
524288	5	2621440
786432	9	7077888
1048576	11	11534336
1572864	10	15728640
2097152	5	10485760
3145728	3	9437184
4194304	3	12582912
6291456	1	6291456
8388608	1	8388608
12582912	7	88080384

MEMPOOL_DMA POOL STATS:

```

Non-mmapped bytes allocated = 513802240
Number of free chunks      = 153
Number of mmapped regions  = 0
Mmapped bytes allocated    = 0
Max memory footprint       = 513802240
Keepcost                   = 190724944
Max contiguous free mem    = 190724944
Allocated memory in use   = 322994736
Free memory                = 190807504
    
```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
48	30	1440
96	1	96**
112	28	3136
160	1	160
208	1	208
224	1	224
240	2	480
256	1	288
384	19	9104
512	65	40656
768	1	800
1024	2	2608
190724944	1	190724944*

- * - top most releasable chunk.
- ** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
--------------------------	-------	------------------

160	1	160
240	92	22080
256	2	512
512	2	1024
1024	163	166912
2048	5	10240
8192	1	8192
12288	18	221184
16384	1	16384
32768	38	1245184
49152	1	49152
65536	1	65536
131072	4	524288
196608	3	589824
262144	8	2097152
393216	6	2359296
524288	2	1048576
786432	1	786432
1048576	11	11534336
1572864	7	11010048
3145728	8	25165824
6291456	5	31457280
8388608	1	8388608
12582912	7	88080384

MEMPOOL_GLOBAL_SHARED POOL STATS:

```

Non-mmapped bytes allocated = 135168
Number of free chunks = 4
Number of mmapped regions = 0
Mmapped bytes allocated = 0
Max memory footprint = 0
Keepcost = 51616
Max contiguous free mem = 51616
Allocated memory in use = 4064
Free memory = 131104

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
432	1	432
40960	1	50848

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
96	1	96
112	1	112
160	1	160
208	3	624

Summary for all pools:

```

Non-mmapped bytes allocated = 2055344128
Number of free chunks = 790
Number of mmapped regions = 0
Mmapped bytes allocated = 0
Max memory footprint = 2055208960
Keepcost = 1381738000

```

```
Allocated memory in use    =    671046592
Free memory                =    1384297536
```

次の出力では、131,072 の代わりにサイズ 149,0327 のブロックが割り当てられたことを確認します。

```
ciscoasa# show memory binsize 131072
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7f739a97db9f, size = 1490327 , count = 9
pc = 0x7f7399be30a0, size = 309008  , count = 2
pc = 0x7f7399be31f4, size = 1255704 , count = 9
MEMPOOL_DMA pool bin stats:
pc = 0x7f73984ba38d, size = 323486  , count = 2
pc = 0x7f73984b8e55, size = 320286  , count = 2
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

show memory detail コマンドの出力に合計バイト数の概算が示されるのは仕様によるものです。これには次の 2 つの理由があります。

- 各フラグメントサイズに対して、すべてのフラグメントの合計を取得する必要があると、単一のフラグメントサイズの割り当て数が非常に多くなることで、パフォーマンスに影響する可能性があり、かつ、正確な値を取得するには、数千ものチャンクを実行することが必要になります。
- 各 **binsize** に対して、二重にリンクされた割り当てリスト全体を確認する必要があり、割り当ては多数存在する可能性があります。この場合、CPU を長期間占有できないため、割り当てを定期的に停止する必要があります。割り当てを再開した後、他のプロセスがメモリを割り当てまたは割り当て解除したことによって、メモリ状態が変化している可能性があります。このため、合計バイト列には、実際の値ではなく近似値が示されます。

例

次に、**show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      3208100250 bytes (72%)
Used memory:     1247711232 bytes (28%)
-----
Total memory:    4455811482 bytes (100%)
```

注: **Free memory** は、システムの空きメモリです。さらに、ASA プロセス内部のメモリ プールで使用可能なメモリを追加できる可能性があります。この情報を表示するには、**show memory detail** コマンドを使用します。ただし、CPU の占有や、ロード時のパケット損失が発生する可能性があるため慎重に使用してください。

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

```
ciscoasa# show memory detail
Heap Memory:
  Free Memory:
    Heapcache Pool:          447109376 bytes ( 10% )
    Global Shared Pool:      131152 bytes ( 0% )
    System:                  3208100250 bytes ( 72% )
  Used Memory:
    Heapcache Pool:          257533696 bytes ( 6% )
    Global Shared Pool:      4016 bytes ( 0% )
    Reserved (Size of DMA Pool): 234881024 bytes ( 5% )
    System Overhead:         308051968 bytes ( 7% )
-----
Total Memory:              4455811482 bytes ( 100% )
```

Warning: The information reported here is computationally expensive to determine, and may result in CPU hogs and performance impact.

MEMPOOL_HEAPCACHE_0 POOL STATS:

```

Non-mmapped bytes allocated = 704643072
Number of free chunks      = 309
Number of mmapped regions  = 0
Mmapped bytes allocated   = 0
Max memory footprint      = 704643072
Keepcost                  = 446723584
Max contiguous free mem    = 446723584
Allocated memory in use   = 257533696
Free memory                = 447109376

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
32	91	2912
48	116	5568
64	83	5312
96	1	96**
96	3	288
112	1	112
160	2	320
224	2	448
240	1	240
256	2	544
384	1	384
512	2	1392
768	2	1904
32768	1	44704
446723584	1	446723584*

* - top most releasable chunk.

** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
80	937	74960
96	10758	1032768
112	2051	229712
128	898	114944
144	2887	415728
160	290	46400
176	300	52800
192	164	31488
208	246	51168
224	183	40992
240	208	49920
256	1396	357376
384	474	182016
512	305	156160
768	322	247296
1024	240	245760
1536	321	493056
2048	171	350208

3072	45	138240
4096	259	1060864
6144	47	288768
8192	174	1425408
12288	94	1155072
16384	571	9355264
24576	17	417792
32768	51	1671168
49152	16	786432
65536	121	7929856
98304	14	1376256
131072	9	1179648
196608	19	3735552
262144	12	3145728
393216	15	5898240
524288	2	1048576
786432	9	7077888
1048576	12	12582912
1572864	5	7864320
2097152	3	6291456
3145728	2	6291456
4194304	4	16777216
6291456	3	18874368
8388608	1	8388608
12582912	3	37748736

MEMPOOL_DMA POOL STATS:

```

Non-mmapped bytes allocated = 234881024
Number of free chunks       = 162
Number of mmapped regions   = 0
Mmapped bytes allocated     = 0
Max memory footprint        = 234881024
Keepcost                    = 90103152
Max contiguous free mem     = 90103152
Allocated memory in use    = 144701888
Free memory                 = 90179136

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
96	1	96**
112	1	112
256	64	20480
384	32	15360
512	64	39936
90103152	1	90103152*

* - top most releasable chunk.

** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
160	2	320
256	2	512
512	1	512
1024	160	163840
2048	5	10240

8192	1	8192
12288	18	221184
16384	1	16384
32768	37	1212416
49152	2	98304
65536	1	65536
131072	4	524288
196608	2	393216
262144	4	1048576
393216	2	786432
524288	2	1048576
786432	1	786432
1048576	3	3145728
1572864	2	3145728
3145728	3	9437184
6291456	2	12582912
12582912	3	37748736

MEMPOOL_GLOBAL_SHARED POOL STATS:

```

Non-mmapped bytes allocated =      135168
Number of free chunks       =           4
Number of mmapped regions   =           0
Mmapped bytes allocated     =           0
Max memory footprint        =           0
Keepcost                    =      96368
Max contiguous free mem     =      96368
Allocated memory in use     =       4016
Free memory                  =     131152

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
448	1	448
20480	1	23296

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
96	1	96
112	1	112
160	1	160
192	3	576

Summary for all pools:

```

Non-mmapped bytes allocated =     939659264
Number of free chunks       =           475
Number of mmapped regions   =           0
Mmapped bytes allocated     =           0
Max memory footprint        =     939524096
Keepcost                    =     536923104
Allocated memory in use     =     402239600
Free memory                  =     537419664

```

On 5585:

=====

```

ciscoasa# show memory
Free memory:      4544618496 bytes (73%)

```

```
Used memory:      1714343936 bytes (27%)
-----
Total memory:    6258962432 bytes (100%)
```

Note: Free memory is the free system memory. Additional memory may be available from memory pools internal to the ASA process. Use 'show memory detail' to see this information, but use it with care since it may cause CPU hogs and packet loss under load.

```
ciscoasa# show memory detail
```

```
Heap Memory:
Free Memory:
  Global Shared Pool:      283589104 bytes ( 5% )
  System:                  4544618496 bytes ( 73% )
Used Memory:
  Global Shared Pool:      41813520 bytes ( 1% )
  Reserved (Size of DMA Pool): 445095936 bytes ( 7% )
  System Overhead:        943845376 bytes ( 15% )
-----
Total Memory:              6258962432 bytes ( 100% )
```

Warning: The information reported here is computationally expensive to determine, and may result in CPU hogs and performance impact.

```
-----
MEMPOOL_DMA POOL STATS:
```

```
Non-mmapped bytes allocated = 445095936
Number of free chunks       = 161
Number of mmapped regions   = 0
Mmapped bytes allocated     = 0
Max memory footprint        = 445095936
Keepcost                    = 250149264
Max contiguous free mem     = 250149264
Allocated memory in use     = 194871536
Free memory                  = 250224400
```

```
----- fragmented memory statistics -----
```

fragment size (bytes)	count	total (bytes)
64	1	64
96	1	96**
112	1	112
256	63	20192
384	32	15360
512	63	39312
250149264	1	250149264*

* - top most releasable chunk.

** - contiguous memory on top of heap.

```
----- allocated memory statistics -----
```

fragment size (bytes)	count	total (bytes)
80	1	80
144	1	144
160	2	320
256	2	512

512	1	512
1024	160	163840
2048	5	10240
8192	5	40960
12288	27	331776
16384	1	16384
32768	39	1277952
49152	1	49152
65536	1	65536
98304	4	393216
131072	4	524288
196608	1	196608
262144	3	786432
393216	2	786432
524288	2	1048576
786432	5	3932160
1048576	3	3145728
1572864	2	3145728
3145728	4	12582912
12582912	4	50331648

MEMPOOL_GLOBAL_SHARED POOL STATS:

```

Non-mmapped bytes allocated = 43286528
Number of free chunks = 474
Number of mmapped regions = 156
Mmapped bytes allocated = 282116096
Max memory footprint = 0
Keepcost = 11200
Max contiguous free mem = 132816
Allocated memory in use = 41813520
Free memory = 1473008

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
32	135	4320
48	203	9744
64	38	2432
80	2	160
80	20	1600
96	3	288
96	3	288
112	90	10080
112	10	1120
128	20	2560
144	1	144
240	1	240
384	1	384
400	1	400
448	1	448
480	1	480
544	1	544
560	6	3360
656	1	656
816	1	816
832	1	832
880	1	880
1088	3	3360
1664	1	1680
3136	1	3280
3584	1	3776

```

      8704          1          8704
    24576          1        25728
    40960          1        50064

```

```
----- allocated memory statistics -----
```

fragment size (bytes)	count	total (bytes)
64	354	22656
80	1234	98720
96	12337	1184352
112	1202	134624
128	970	124160
144	2777	399888
160	435	69600
176	155	27280
192	323	62016
208	250	52000
224	86	19264
240	388	93120
256	1478	378368
384	304	116736
512	304	155648
768	314	241152
1024	410	419840
1536	1188	1824768
2048	136	278528
3072	42	129024
4096	814	3334144
6144	56	344064
8192	174	1425408
12288	123	1511424
16384	584	9568256
24576	30	737280
32768	60	1966080
49152	30	1474560
65536	139	9109504
98304	25	2457600
131072	19	2490368
196608	32	6291456
262144	18	4718592
393216	29	11403264
524288	7	3670016
786432	8	6291456
1048576	13	13631488
1572864	11	17301504
2097152	6	12582912
3145728	2	6291456
4194304	4	16777216
8388608	1	8388608
12582912	6	75497472

```
Summary for all pools:
```

```

Non-mmapped bytes allocated = 488382464
Number of free chunks       =          635
Number of mmapped regions   =              0
Mmapped bytes allocated     = 282116096
Max memory footprint        = 445095936
Keepcost                    = 250160464
Allocated memory in use     = 236685056
Free memory                  = 251697408

```

次に、**jumbo-frame reservation** コマンドをイネーブルにして **write memory** コマンドと **reload** コマンドを発行した後の、ASA 5525 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      3208100250 bytes (72%)
Used memory:      1247711232 bytes (28%)
-----
Total memory:     4455811482 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5525 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      3208100250 bytes (72%)
Used memory:      1247711232 bytes (28%)
-----
Total memory:     4455811482 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにした後の、ASA 5515 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      3276619472 bytes (76%)
Used memory:      1018347824 bytes (24%)
-----
Total memory:     4294967296 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5515 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      3481145472 bytes (81%)
Used memory:      813821824 bytes (19%)
-----
Total memory:     4294967296 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにした後の、ASA 5585 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      8883297824 bytes (69%)
Used memory:      4001604064 bytes (31%)
-----
Total memory:     12884901888 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5585 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      9872205104 bytes (77%)
Used memory:      3012696784 bytes (23%)
-----
Total memory:     12884901888 bytes (100%)
```

次に、**jumbo-frame** コマンドをサポートしていない ASA 5520 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      206128232 bytes (38%)
Used memory:      330742680 bytes (62%)
-----
Total memory:     536870912 bytes (100%)
```

次に、**jumbo-frame** コマンドをサポートしていない ASA 5505 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:      48457848 bytes (18%)
Used memory:      219977608 bytes (82%)
-----
Total memory:     268435456 bytes (100%)
```

次に、ASA v で **show memory** コマンドの出力例を示します。

```
Free memory:      2694133440 bytes (63%)
Used memory:      1600833856 bytes (37%)
-----
Total memory:     4294967296 bytes (100%)
```

```
Virtual platform memory
-----
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory api

システムに登録されている malloc スタック API を表示するには、特権 EXEC モードで **show memory api** コマンドを使用します。

show memory api

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、システムに登録されている malloc スタック API を表示します。メモリ デバッグ機能(つまり、delay-free-poisoner、メモリ トラッカー、またはメモリ プロファイラ)がオンになっている場合、API が **show memory api** の出力に表示されます。

例

次に、**show memory api** コマンドの出力例を示します。

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory app-cache

アプリケーションによるメモリ使用状況を確認するには、特権 EXEC モードで **show memory app-cache** コマンドを使用します。

show memory app-cache [**threat-detection** | **host** | **flow** | **tcb** | **http** | **access-list** | **tcb-ibs**] [**detail**]

構文の説明 show

access-list	(オプション)アクセスリストのアプリケーション レベル メモリ キャッシュを表示します。
detail	(任意)空きメモリおよび割り当て済みシステム メモリの詳細ビューを表示します。
flow	(オプション)フローのアプリケーション レベル メモリ キャッシュを表示します。
ホスト	(オプション)ホストのアプリケーション レベル メモリ キャッシュを表示します。
http	(オプション)HTTP のアプリケーション レベル メモリ キャッシュを表示します。
tcb	(オプション)TCB のアプリケーション レベル メモリ キャッシュを表示します。
tcb-ips	(オプション)TCB-IPS のアプリケーション レベル メモリ キャッシュを表示します。
threat-detection	(オプション)脅威検出のアプリケーション レベル メモリ キャッシュを表示します。

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 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
8.0(1)	このコマンドが追加されました。
8.1(1)	access-list および http オプションが追加されました。
9.10(1)	tcb-ips オプションが追加されました。

使用上のガイドライン

このコマンドを使用して、アプリケーションによるメモリ使用状況を確認できます。

例

次に、**show memory app-cache threat-detection** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache threat-detection
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

次に、**show memory app-cache threat-detection detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

次に、**show memory app-cache host detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

次に、**show memory app-cache flow detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

次に、**show memory app-cache access-list detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
```

```

NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0

```

```

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768

```

次に、**show memory app-cache http detail** コマンドの出力例を示します。

```

ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0

```

```

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0

```

次に、**show memory app-cache tcb detail** コマンドの出力例を示します。

```

ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936

```

```

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000

```

次に、**show memory app-cache tcb-ips detail** コマンドの出力例を示します。

```

ha-asa5512a(config)# show memory app-cache tcb-ips detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB IPS Core 00      625 0 0 0 0
LIMIT      COUNT      ALLOC      FAILED    BYTES USED
TOTAL      625          0 0 0      0

```

```

ha-asa5512a(config)# show memory app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
[...]
SNP TCB IPS Core 00 625 0 0 0 0
SNP TCB IPS Total 625 0 0 0 0

```

```

[...]

```

```

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 61972 149 188 0      50212

```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。

show memory appcache-threshold

memory appcache-threshold のステータスとヒット カウントを表示するには、特権 EXEC モードで **show memory appcache-threshold** コマンドを使用します。

show memory appcache-threshold

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。

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		
	ルーター	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
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

管理対象アプリケーションのヒット カウントとメモリ割り当てしきい値のステータスを表示するには、**show memory appcache-threshold** コマンドを使用します。

例

次に、管理対象アプリケーションの memory appcache threshold のステータスを表示する例を示します。

```
ciscoasa# show memory appcache-threshold
      CACHE NAME  STATUS  THRESHOLD  HIT COUNT
      SNP Conn Core 00  ENABLED      85           5

ciscoasa# show memory appcache-threshold
      CACHE NAME  STATUS  THRESHOLD  HIT COUNT
      SNP Conn Core 00  DISABLED      85           5
```

表 9-10 `show memory appcache-threshold` のフィールド

フィールド	説明
Cache Name	管理対象のアプリケーション キャッシュの名前。ASA 9.10.1 リリースでは、SNP Conn Core 00 アプリケーションのキャッシュ タイプのみが管理されます。
Status(ステータス)	このアプリケーション キャッシュ タイプの <code>appcache-threshold</code> 機能が有効か無効かを示します。
Threshold	このアプリケーション キャッシュ タイプのしきい値。たとえば、「85」はシステムメモリの 85% が使用されていることを意味します。
Hit Count	カウンタが最後にクリアされてからこのしきい値にヒットした回数。

関連コマンド

コマンド	説明
<code>memory appcache-threshold enable</code>	特定のメモリしきい値に達した後のアプリケーション キャッシュの割り当てを制限するには、 <code>memory appcache-threshold</code> を有効にします。
<code>clear memory appcache-threshold</code>	<code>memory appcache-threshold</code> のヒットカウントをクリアします。

show memory binsize

特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示するには、特権 EXEC モードで **show memory binsize** コマンドを使用します。

show memory binsize *size*

構文の説明

<i>size</i>	特定のバイナリ サイズのチャンク(メモリ ブロック)を表示します。バイナリ サイズは show memory detail コマンド出力の「fragment size」列から取得されます。
-------------	---

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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この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、バイナリ サイズ 500 に割り当てられたチャンクについての要約情報を表示する例を示します。

```
ciscoasa# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

関連コマンド

コマンド	説明
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。

show memory caller-address

ASA で設定されたアドレス範囲を表示するには、特権 EXEC モードで **show memory caller-address** コマンドを使用します。

show memory caller-address

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

アドレス範囲を **show memory-caller address** コマンドで表示する前に、**memory caller-address** コマンドで設定する必要があります。

例

次に、**memory caller-address** コマンドでアドレス範囲を設定する方法、および **show memory-caller address** コマンドの出力結果の例を示します。

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464
```

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

アドレス範囲が **show memory-caller address** コマンドを入力する前に設定されていなかった場合、アドレスは表示されません。

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
```

関連コマンド

コマンド	説明
memory caller-address	発信元 PC のメモリ ブロックを設定します。

show memory delayed-free-poisoner

memory delayed-free-poisoner キューの使用状況の要約を表示するには、特権 EXEC モードで **show memory delayed-free-poisoner** コマンドを使用します。

show memory delayed-free-poisoner

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。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドを使用して、キューおよび統計情報をクリアします。

例

次に、**show memory delayed-free-poisoner** コマンドの出力例を示します。

```
ciscoasa# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
  3335600: memory held in queue
  6095: current queue count
  0: elements dequeued
  3: frees ignored by size
  1530: frees ignored by locking
  27: successful validate runs
  0: aborted validate runs
01:09:36: local time of last validate
```

表 9-11 に、**show memory delayed-free-poisoner** コマンド出力での重要なフィールドの説明を示します。

表 9-11 **show memory delayed-free-poisoner** コマンド出力の説明

フィールド	説明
memory held in queue	delayed free-memory poisoner ツール キューに保留されたメモリ。 delayed free-memory poisoner ツールがイネーブルになっていない場合、このようなメモリは、通常、 show memory 出力では「空き」容量になります。
current queue count	キューにある要素の数。
elements dequeued	キューから削除された要素の数。この数は、システム内の空きメモリだったメモリの大部分またはすべてが最終的にキューに保持されることになった場合に増加し始めます。
frees ignored by size	要求が小さすぎて必要なトラッキング情報を保持できなかったため、キューに配置されなかった解放要求の数。
frees ignored by locking	複数のアプリケーションがメモリを使用しているため、キューに配置されずに、ツールによって代行受信された解放要求の数。最後にメモリを解放してシステムに戻したアプリケーションが、このメモリ領域をキューに割り当てます。
successful validate runs	clear memory delayed-free-poisoner コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、キューの内容が(自動的に、または memory delayed-free-poisoner validate コマンドによって)検証された回数。
aborted validate runs	clear memory delayed-free-poisoner コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、複数のタスク(定期的な実行または CLI からの検証要求)が同時にキューを使用しようとしたため、キューの内容をチェックする要求が中止された回数。
local time of last validate	最後の検証の実行が完了したときのローカル システム時刻。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。

show memory logging

ロギング用のメモリ使用状況を表示するには、特権 EXEC モードで **show memory logging** コマンドを使用します。

```
show memory logging [brief | wrap | include [address] [caller] [operator] [size] [process] [time]
                    [context]]
```

構文の説明

address	(オプション)アドレス情報を表示します。
brief	(オプション)要約されたメモリ使用状況のロギングを表示します。
caller	(オプション)発信者情報を表示します。
コンテキスト	(オプション)仮想コンテキスト情報を表示します。
include	<p>指定したフィールドのみを出力に含めます。任意の順序でフィールドを指定できますが、必ず次の順序で表示されます。</p> <ol style="list-style-type: none"> 1. プロセス 2. 時刻 3. コンテキスト(シングル モード以外) 4. 処理(free/malloc/など) 5. アドレス 6. サイズ 7. 発信者 <p>出力形式は、次のとおりです。</p> <pre>process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0XXXXXXXXXX size=XX @ XXXXXXXXXXXX XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX</pre> <p>最大 4 つの発信者アドレスが表示されます。例に示すように、処理の種類(番号)が出力に列挙されます。</p>
operator	(オプション)オペレータ情報を表示します。
process	(オプション)プロセス情報を表示します。
size	(オプション)サイズ情報を表示します。
time	(オプション)時間情報を表示します。
wrap	(オプション)メモリ使用状況のロギングのラップされたデータを表示します。これらの重複するデータが表示されたり保存されたりしないように、重複するデータは、このコマンドの入力後に消去されます。

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
	9.4(1)	このコマンドが導入されました。

使用上のガイドライン **show memory logging** コマンドは、ログのメモリ割り当てとメモリ使用状況を表示し、ユーザがメモリ ロギング ラップ イベントに対処できるようにします。

例 次に、ASA での **show memory logging** コマンドの出力例を示します。

```
ciscoasa# show memory logging

Number of free                6
Number of calloc              0
Number of malloc              8
Number of realloc-new         0
Number of realloc-free       0
Number of realloc-null        0
Number of realloc-same        0
Number of calloc-fail         0
Number of malloc-fail         0
Number of realloc-fail        0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfff9a

0x000000000bfff606 process=[CMGR Server Process] time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bfff3d8
0x000000000bfff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098 0x000000000182c08d
```

```

0x00000000182c262 process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b 0x000000000182c08d

0x00000000182c262 process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x00000000182cc8a process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x000000000bfe9a

0x000000000bfff606 process=[CMGR Server Process] time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x000000000bfff3d8
0x000000000bfff606 0x00000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x000000001834188 0x00000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x000000000443455 0x0000000001318f5b

```

次に、ASA での **show memory logging include process operation size** コマンドの出力例を示します。

```

ciscoasa# show memory logging include process operation size
Number of free                6
Number of calloc              0
Number of malloc              8
Number of realloc-new         0
Number of realloc-free       0
Number of realloc-null       0
Number of realloc-same       0
Number of calloc-fail        0
Number of malloc-fail        0
Number of realloc-fail       0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72
process=
[CMGR Server Process] oper=[malloc] size=16 process=[CMGR Server Process] oper=[malloc]
size=512 process=[CMGR Server Process] oper=[free] size=512 process=[CMGR Server Process]
oper=[malloc] size=40 process=[CMGR Server Process] oper=[free] size=16 process=[CMGR
Server
Process] oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR
Server Process] oper=[malloc] size=512 process=[CMGR Server Process] oper=[free] size=512
process=[CMGR Server Process] oper=[malloc] size=40 process=[ci/console] oper=[malloc]
size=72
process=[ci/console] oper=[free] size=72

```

次に、ASA での **show memory logging brief** コマンドの出力例を示します。

```

ciscoasa# show memory logging brief
Number of free                6
Number of calloc              0
Number of malloc              8
Number of realloc-new         0
Number of realloc-free       0
Number of realloc-null       0
Number of realloc-same       0
Number of calloc-fail        0

```

```
Number of malloc-fail          0
Number of realloc-fail        0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory profile

ASA のメモリ使用率(プロファイリング)に関する情報を表示するには、特権 EXEC モードで **show memory profile** コマンドを使用します。

show memory profile [peak] [detail | collated | status]

構文の説明

collated	(任意)表示されるメモリ情報を整形します。
detail	(任意)メモリの詳細情報を表示します。
peak	(オプション)「使用中」のバッファではなく、ピーク キャプチャ バッファを表示します。
status	(任意)メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show memory profile コマンドを使用して、メモリ使用状況レベルとメモリ リークをトラブルシューティングします。プロファイリングが停止されている場合でも、プロファイル バッファの内容を表示できます。プロファイリングを開始すると、バッファは自動的にクリアされます。



(注)

メモリ プロファイリングをイネーブルにすると、ASA のパフォーマンスが一時的に低下する場合があります。

例

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

```
ciscoasa# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail コマンドの出力は、6つのデータ列と1つのヘッダー列に区分され、左揃えで表示されています。ヘッダー列には、先頭のデータ列に対応するメモリバケットのアドレスが表示されます(16進数)。データ自体は、バケットアドレスにあるテキストまたはコードが保持しているバイト数です。データカラム内のピリオド(.)は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケットアドレスを表しています。たとえば、最初の行の先頭のデータカラムのアドレスバケットは `0x001069e0` です。最初の行の2番目のデータカラムのアドレスバケットは `0x001069e4` で、以降も同様に増分していきます。通常は、ヘッダーカラムにあるアドレスが次のバケットアドレスです。これは、前の行の最後のデータカラムのアドレスに増分値を加算したものです。使用状況が含まれない行は表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダーカラムに3個のピリオド(...)で示されます。

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

```
ciscoasa# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . .
<snip>
```

次に、**show memory profile collated** コマンドの出力例を示します。

```
ciscoasa# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

次に、**show memory profile peak** コマンドの出力例を示します。このコマンドでは、ピーク キャプチャバッファを表示します。

```
ciscoasa# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次に、**show memory profile peak detail** コマンドの出力例を示します。このコマンドでは、ピークキャプチャバッファと、対応するバケットアドレスにあるテキスト/コードが保持しているバイト数を表示します。

```
ciscoasa# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

次に、**show memory profile status** コマンドの出力例を示します。このコマンドでは、メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。

```
ciscoasa# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8 (00000004)
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況(メモリ プロファイリング)のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。

show memory region

プロセス マップを表示するには、特権 EXEC モードで **show memory region** コマンドを使用します。

show memory region

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。

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		
	ルールテッド	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。

使用上のガイドラ イン

show memory region コマンドを使用すると、プロセス メモリ マップを表示できます。

例

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

```
ciscoasa# show memory region
ASLR enabled, text region 7f7397701000-7f739bc186c4

Address          Perm Offset  Dev  Inode          Pathname
7f7391a06000-7f7391d09000 rw-p 00000000 00:00 0             [stack:2161]
7f7391d2a000-7f739212e000 rw-p 00000000 00:00 0             [stack:2157]
7f7392530000-7f7392631000 rw-p 00000000 00:00 0             [stack:2156]
7f7392647000-7f7392849000 rw-p 00000000 00:00 0             [stack:2154]
7f7392895000-7f7392897000 r-xp 00000000 00:01 989          /lib64/libutil-2.18.so
7f7392897000-7f7392a96000 ---p 00002000 00:01 989          /lib64/libutil-2.18.so
7f7392a96000-7f7392a97000 r--p 00001000 00:01 989          /lib64/libutil-2.18.so
7f7392a97000-7f7392a98000 rw-p 00002000 00:01 989          /lib64/libutil-2.18.so
7f7392a98000-7f7392c9a000 r-xp 00000000 00:01 2923         /usr/lib64/libcrypto.so.1.0.0
7f7392c9a000-7f7392e99000 ---p 00202000 00:01 2923         /usr/lib64/libcrypto.so.1.0.0
7f7392e99000-7f7392ec3000 rw-p 00201000 00:01 2923         /usr/lib64/libcrypto.so.1.0.0
7f7392ec7000-7f7392f28000 r-xp 00000000 00:01 3114         /usr/lib64/libssl.so.1.0.0
7f7392f28000-7f7393127000 ---p 00061000 00:01 3114         /usr/lib64/libssl.so.1.0.0
```

```

7f7393127000-7f7393132000 rw-p 00060000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7393132000-7f739316a000 r-xp 00000000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739316a000-7f739336a000 ---p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336a000-7f739336c000 rw-p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336c000-7f73933ca000 r-xp 00000000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73933ca000-7f73935ca000 ---p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ca000-7f73935ce000 rw-p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ce000-7f7393606000 r-xp 00000000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393606000-7f7393805000 ---p 00038000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393805000-7f7393809000 rw-p 00037000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f739380a000-7f7393811000 r-xp 00000000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393811000-7f7393a11000 ---p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a11000-7f7393a12000 rw-p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a12000-7f7393b94000 r-xp 00000000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393b94000-7f7393d94000 ---p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393d94000-7f7393dd3000 rw-p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393de1000-7f7393df6000 r-xp 00000000 00:01 948 /lib64/libz.so.1.2.8
7f7393df6000-7f7393ff5000 ---p 00015000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff5000-7f7393ff6000 rw-p 00014000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff6000-7f739419a000 r-xp 00000000 00:01 961 /lib64/libc-2.18.so
7f739419a000-7f7394399000 ---p 001a4000 00:01 961 /lib64/libc-2.18.so
7f7394399000-7f739439d000 r--p 001a3000 00:01 961 /lib64/libc-2.18.so
7f739439d000-7f739439f000 rw-p 001a7000 00:01 961 /lib64/libc-2.18.so
7f73943a3000-7f73943b8000 r-xp 00000000 00:01 949 /lib64/libgcc_s.so.1
7f73943b8000-7f73945b8000 ---p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b8000-7f73945b9000 rw-p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b9000-7f73946bb000 r-xp 00000000 00:01 999 /lib64/libm-2.18.so
7f73946bb000-7f73948ba000 ---p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948ba000-7f73948bb000 r--p 00101000 00:01 999 /lib64/libm-2.18.so
7f73948bb000-7f73948bc000 rw-p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948bc000-7f73948be000 r-xp 00000000 00:01 3641 /asa/lib/libplatcap.so
7f73948be000-7f7394abd000 ---p 00002000 00:01 3641 /asa/lib/libplatcap.so
7f7394abd000-7f7394ac5000 rw-p 00001000 00:01 3641 /asa/lib/libplatcap.so
7f7394ac5000-7f7394b12000 r-xp 00000000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394b12000-7f7394d12000 ---p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d12000-7f7394d14000 rw-p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d14000-7f7394e3d000 r-xp 00000000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f7394e3d000-7f739503d000 ---p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503d000-7f739503f000 rw-p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503f000-7f73950ce000 r-xp 00000000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73950ce000-7f73952ce000 ---p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952ce000-7f73952d9000 rw-p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952d9000-7f73952e9000 r-xp 00000000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73952e9000-7f73954e8000 ---p 00010000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e8000-7f73954e9000 rw-p 0000f000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e9000-7f739551b000 r-xp 00000000 00:01 3629 /asa/lib/libmsglyr.so
7f739551b000-7f739571b000 ---p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f739571b000-7f7395720000 rw-p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f7395720000-7f739576c000 r-xp 00000000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739576c000-7f739596c000 ---p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739596c000-7f7395970000 rw-p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f7395970000-7f7395ac0000 r-xp 00000000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ac0000-7f7395cc0000 ---p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395cc0000-7f7395cca000 rw-p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ccb000-7f7395ceb000 r-xp 00000000 00:01 3628 /asa/lib/libpdtts.so
7f7395ceb000-7f7395eea000 ---p 00020000 00:01 3628 /asa/lib/libpdtts.so
7f7395eea000-7f7395eec000 rw-p 0001f000 00:01 3628 /asa/lib/libpdtts.so
7f7395eec000-7f7395eff000 r-xp 00000000 00:01 2057 /lib64/libresolv-2.18.so

```

```

7f7395eff000-7f73960ff000 ---p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f73960ff000-7f7396100000 r--p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f7396100000-7f7396101000 rw-p 00014000 00:01 2057 /lib64/libresolv-2.18.so
7f7396103000-7f7396110000 r-xp 00000000 00:01 955 /lib64/libudev.so.0.13.1
7f7396110000-7f739630f000 ---p 0000d000 00:01 955 /lib64/libudev.so.0.13.1
7f739630f000-7f7396310000 rw-p 0000c000 00:01 955 /lib64/libudev.so.0.13.1
7f7396310000-7f7396322000 r-xp 00000000 00:01 964 /lib64/libcgroup.so.1.0.38
7f7396322000-7f7396521000 ---p 00012000 00:01 964 /lib64/libcgroup.so.1.0.38
7f7396521000-7f7396523000 rw-p 00011000 00:01 964 /lib64/libcgroup.so.1.0.38
7f739677d000-7f7396784000 r-xp 00000000 00:01 2067 /lib64/librt-2.18.so
7f7396784000-7f7396983000 ---p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396983000-7f7396984000 r--p 00006000 00:01 2067 /lib64/librt-2.18.so
7f7396984000-7f7396985000 rw-p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396985000-7f7396988000 r-xp 00000000 00:01 2060 /lib64/libdl-2.18.so
7f7396988000-7f7396b87000 ---p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b87000-7f7396b88000 r--p 00002000 00:01 2060 /lib64/libdl-2.18.so
7f7396b88000-7f7396b89000 rw-p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b89000-7f7396ba2000 r-xp 00000000 00:01 1001 /lib64/libpthread-2.18.so
7f7396ba2000-7f7396da1000 ---p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da1000-7f7396da2000 r--p 00018000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da2000-7f7396da3000 rw-p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da7000-7f7396dce000 r-xp 00000000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396dce000-7f7396ecd000 ---p 00027000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396ecd000-7f7396fd0000 rw-p 00026000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396fd0000-7f73970b6000 r-xp 00000000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73970b6000-7f73972b5000 ---p 000e6000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972b5000-7f73972bd000 r--p 000e5000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972bd000-7f73972bf000 rw-p 000ed000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972d4000-7f73972de000 r-xp 00000000 00:01 3174 /usr/lib64/libnuma.so.1
7f73972de000-7f73974dd000 ---p 0000a000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974dd000-7f73974de000 rw-p 00009000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974de000-7f73974fe000 r-xp 00000000 00:01 950 /lib64/ld-2.18.so
7f73976fe000-7f73976ff000 r--p 00020000 00:01 950 /lib64/ld-2.18.so
7f73976ff000-7f7397700000 rw-p 00021000 00:01 950 /lib64/ld-2.18.so
7f7397701000-7f739bc19000 r-xp 00000000 00:01 3650 /asa/bin/lina
7f739be18000-7f739cc16000 rw-p 04517000 00:01 3650 /asa/bin/lina
7ffffe1fc000-7ffffe21d000 rw-p 00000000 00:00 0 [stack]
7ffffe2f1000-7ffffe2f3000 r-xp 00000000 00:00 0 [vdso]

```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況(メモリ プロファイリング)のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。

show memory top-usage

show memory detail コマンドから割り当てられたフラグメント サイズの上位いくつかを表示するには、特権 EXEC モードで **show memory top-usage** コマンドを使用します。

show memory top-usage [num]

構文の説明

num (オプション) リストにバイナリ サイズの数を表示します。有効な値は 1 ~ 64 です。

デフォルト

num のデフォルトは 10 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

リリース	変更内容
8.4(6)	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 memory detail コマンドから割り当てられたフラグメント サイズの上位いくつかを表示するには、**show memory top-usage** コマンドを使用します。

このコマンドは、クラスタリングを使用しません。クラスタリングがイネーブルの場合にクラスタリングをディセーブルにする必要はありません。

例

次に、**show memory top-usage** コマンドの出力例を示します。

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:
```

```
----- allocated memory statistics -----
```

fragment size (bytes)	count	total (bytes)
1572864	9	14155776
12582912	1	12582912
6291456	1	6291456

```

----- Binsize PC top usage -----
Binsize: 1572864                total (bytes): 14155776
pc = 0x805a870, size = 16422399 , count = 9

Binsize: 12582912              total (bytes): 12582912
pc = 0x805a870, size = 12960071 , count = 1

Binsize: 6291456                total (bytes): 6291456
pc = 0x9828a6c, size = 7962695  , count = 1

MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----
fragment size      count      total
  (bytes)                (bytes)
-----
    12582912           1      12582912
    2097152            6      12582912
    65536              181     11862016

----- Binsize PC top usage -----
Binsize: 12582912              total (bytes): 12582912
pc = 0x8249763, size = 37748736 , count = 1

Binsize: 2097152              total (bytes): 12582912
pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1

Binsize: 65536                total (bytes): 11862016
pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1

```

関連コマンド
コマンド**説明****show memory tracking**

現在収集されているすべての情報を表示します。

show memory tracking

ツールによって追跡される、現在割り当て済みのメモリを表示するには、特権 EXEC モードで **show memory tracking** コマンドを実行します。

show memory tracking [address | dump | detail]

構文の説明

address	(任意)アドレスごとのメモリのトラッキングを表示します。
detail	(オプション)内部メモリのトラッキング状態を表示します。
dump	(オプション)メモリのトラッキングアドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

show memory tracking コマンドを使用して、ツールにより追跡されている、現在割り当て済みのメモリを表示します。

例

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

```
ciscoasa# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

次に、**show memory tracking address** コマンドの出力例を示します。

```
ciscoasa# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

```
memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2
```

次に、**show memory tracking dump** コマンドの出力例を示します。

```
ciscoasa# show memory tracking dump
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c | .....
a893aee0: 0c | .....
a893aef0: 0c | .....
a893af00: 0c | .....
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。

show memory utilization

Show memory utilization コマンドを使用して、ASA に設定されているリロードしきい値の制限とクラッシュ情報を表示します。

show memory-utilization [reload-threshold]

構文の説明

reload-threshold	設定されているシステムメモリのリロードしきい値の制限、および、システムのリロードの前にクラッシュ情報が保存されているかどうかを表示します。
-------------------------	---

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	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

リロードしきい値が設定されているかどうかを確認するには、**show memory utilization** コマンドを使用します。設定されている場合は、しきい値の制限と、リロードが設定される前にクラッシュ情報を保存するオプションを選択するかどうかを確認できます。

例

次に、ASA 上にメモリ使用状況機能を設定する例を示します。

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is not configured.
```

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 93%
Crashinfo Generation: yes
```

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 90%
Crashinfo Generation: no
```

show memory webvpn

WebVPN のメモリ使用状況の統計情報を生成するには、特権 EXEC モードで **show memory webvpn** コマンドを使用します。

```
show memory webvpn [allobjects | blocks | dumpstate [cache | disk0 | disk1 | flash | ftp | system
| tftp] | pools | profile [clear | dump | start | stop] | usedobjects {{begin | exclude | grep |
include} line line}}
```

構文の説明

allobjects	プール、ブロック、すべての使用済みオブジェクトおよび解放済みオブジェクトについて、WebVPN メモリ使用量の詳細を表示します。
begin	一致する行から開始します。
blocks	メモリ ブロックについて、WebVPN メモリ使用量の詳細を表示します。
cache	WebVPN メモリ キャッシュ状態のダンプのファイル名を指定します。
clear	WebVPN メモリ プロファイルをクリアします。
disk0	WebVPN メモリ disk0 状態のダンプのファイル名を指定します。
disk1	WebVPN メモリ disk1 状態のダンプのファイル名を指定します。
dump	WebVPN メモリ プロファイルをファイルに出力します。
dumpstate	WebVPN メモリ状態をファイルに出力します。
exclude	一致する行を除外します。
flash	WebVPN メモリ フラッシュ状態のダンプのファイル名を指定します。
ftp	WebVPN メモリ FTP 状態のダンプのファイル名を指定します。
grep	一致する行を含めるか、または除外します。
include	一致する行を含めます。
line	一致する行を特定します。
<i>line</i>	一致する行を指定します。
プール	メモリ プールについて、WebVPN メモリ使用量の詳細を表示します。
プロファイル	WebVPN メモリ プロファイルを収集して、ファイルに出力します。
system	WebVPN メモリ システム状態のダンプのファイル名を指定します。
start	WebVPN メモリ プロファイルの収集を開始します。
stop	WebVPN メモリ プロファイルの収集を停止します。
tftp	WebVPN メモリ TFTP 状態のダンプのファイル名を指定します。
usedobjects	使用済みオブジェクトについて、WebVPN メモリ使用量の詳細を表示します。

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	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
webvpn 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
7.1(1)	このコマンドが追加されました。

例

次に、**show memory webvpn allobjects** コマンドの出力例を示します。

```
ciscoasa# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init!/!prep!/!f2ca!/!dstr!/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

関連コマンド

コマンド	説明
memory-size	WebVPN が使用できる ASA のメモリ量を設定します。

show mfib

転送エントリおよびインターフェイスの観点から MFIB を表示するには、特権 EXEC モードで **show mfib** コマンドを使用します。

show mfib [*group* [*source*]] [**verbose**] [**cluster**]

構文の説明

クラスタ	(オプション)MFIB のエポック番号と現在のタイマー値を表示します。
<i>group</i>	(オプション)マルチキャスト グループの IP アドレスを表示します。
<i>source</i>	(オプション)マルチキャスト ルートの送信元の IP アドレスを表示します。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。
verbose	(任意)エントリに関する追加情報を表示します。

デフォルト

任意の引数を指定しないと、すべてのグループの情報が表示されます。

コマンドモード

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 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
7.0(1)	このコマンドが追加されました。
9.0(1)	cluster キーワードが追加されました。ASA 5580 および 5585-X にのみ適用されます。

例

次に、**show mfib** コマンドの出力例を示します。

```
ciscoasa# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib verbose	転送エントリおよびインターフェイスに関する詳細情報を表示します。

show mfib active

アクティブなマルチキャスト送信元を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib active** コマンドを使用します。

show mfib [*group*] **active** [*kbps*]

構文の説明

<i>group</i>	(任意)マルチキャスト グループの IP アドレスです。
<i>kbps</i>	(任意)この値以上のマルチキャスト ストリームのみに表示を制限します。

このコマンドには引数またはキーワードはありません。

デフォルト

kbps のデフォルト値は 4 です。*group* を指定しない場合、すべてのグループが表示されます。

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 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
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show mfib active コマンドの出力では、PPS のレートに正または負の数値が表示されます。ASA が負の数値を表示するのは、RPF パケットが失敗した場合か、ルータが発信インターフェイス (OIF) リストを使用して RPF パケットをモニタしている場合です。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

例

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

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
  Source: 192.168.28.69 (mbone.ipd.anl.gov)
    Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
```

```
Group: 224.2.201.241, ACM 97
Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
```

```
Group: 224.2.207.215, ACM 97
Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

関連コマンド

コマンド	説明
show mroute active	アクティブなマルチキャスト ストリームを表示します。

show mfib count

MFIB ルートとパケット数データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib count** コマンドを使用します。

show mfib [group [source]] count

構文の説明

<i>group</i>	(任意) マルチキャスト グループの IP アドレスです。
<i>source</i>	(任意) マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

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 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
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、パケットのドロップに関する統計情報を表示します。

例

次に、**show mfib count** コマンドの出力例を示します。

```
ciscoasa# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

関連コマンド

コマンド	説明
clear mfib counters	MFIB ルータ パケット カウンタをクリアします。
show mroute count	マルチキャスト ルート カウンタを表示します。

show mfib interface

MFIB プロセスに関係しているインターフェイスの packets 統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib interface** コマンドを使用します。

show mfib interface [*interface*]

構文の説明

interface (任意) インターフェイス名。指定されたインターフェイスのみに表示を制限します。

デフォルト

すべての MFIB インターフェイスの情報が表示されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザ 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
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show mfib interface
IP Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running
MFIB interface      status      CEF-based output
                   [configured,available]
Ethernet0           up          [no, no]
Ethernet1           up          [no, no]
Ethernet2           up          [no, no]
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib reserved

予約済みグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib reserved** コマンドを使用します。

show mfib reserved [count | verbose | active [kpbs]]

構文の説明

active	(任意)アクティブなマルチキャスト送信元を表示します。
count	(任意)パケットおよびルートの数に関するデータを表示します。
<i>kpbs</i>	(オプション)この値以上のアクティブなマルチキャスト送信元に表示を制限します。
verbose	(任意)追加情報を表示します。

デフォルト

kpbs のデフォルト値は 4 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
ユーザ 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
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、224.0.0.0 ~ 224.0.0.225 の範囲の MFIB エントリを表示します。

例

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

```
ciscoasa# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
Forwarding: 0/0/0/0, Other: 0/0/0
```

```
(* ,224.0.0.0/24) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
(* ,224.0.0.1) Flags:
  Forwarding: 0/0/0/0, Other: 0/0/0
  outside Flags: IC
  dmz Flags: IC
  inside Flags: IC
```

関連コマンド

コマンド	説明
show mfib active	アクティブなマルチキャスト ストリームを表示します。

show mfib status

MFIB の全般的なコンフィギュレーションと動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib status** コマンドを使用します。

show mfib status

構文の説明 このコマンドには引数またはキーワードはありません。

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 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
	7.0(1)	このコマンドが追加されました。

例 次に、**show mfib status** コマンドの出力例を示します。

```
ciscoasa# show mfib status
IP Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running
```

関連コマンド	コマンド	説明
	show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib summary

MFIB のエントリとインターフェイスの数に関する要約情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib summary** コマンドを使用します。

show mfib summary

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。

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 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
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show mfib summary
IPv6 MFIB summary:

 54      total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

 17      total MFIB interfaces
```

関連コマンド

コマンド	説明
show mroute summary	マルチキャストルーティング テーブルの要約情報を表示します。

show mfib verbose

転送エントリとインターフェイスに関する詳細情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib verbose** コマンドを使用します。

show mfib verbose

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。

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 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
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show mfib summary	MFIB のエントリとインターフェイスの数に関する要約情報を表示します。

show mgcp

MGCP のコンフィギュレーションとセッション情報を表示するには、特権 EXEC モードで **show mgcp** コマンドを使用します。

show mgcp {commands | sessions} [detail]

構文の説明

コマンド	コマンド キュー内の MGCP コマンドの数を表示します。
detail	(任意)各コマンド(またはセッション)に関する追加情報を出力に表示します。
sessions	既存の MGCP セッションの数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド(またはセッション)に関する追加情報を出力に含めます。

例

次に、**show mgcp** コマンド オプションの例を示します。

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#
```

```
ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
  Gateway IP | host-pc-2
  Transaction ID | 2052
  Endpoint name | aaln/1
  Call ID | 9876543210abcdef
```

```

Connection ID |
Media IP | 192.168.5.7
Media port | 6058
ciscoasa#

ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#

ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
Gateway IP | host-pc-2
Call ID | 9876543210abcdef
Connection ID | 6789af54c9
Endpoint name | aaln/1
Media lcl port 6166
Media rmt IP | 192.168.5.7
Media rmt port 6058
ciscoasa#

```

関連コマンド

コマンド	説明
class-map	セキュリティアクションを適用するトラフィック クラスを定義します。
debug mgcp	MGCP のデバッグ情報をイネーブルにします。
inspect mgcp	MGCP アプリケーション インспекションをイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。

show mmp

既存の MMP セッションに関する情報を表示するには、特権 EXEC モードで **show mmp** コマンドを使用します。

show mmp [*address*]

構文の説明	<i>address</i>	MMP クライアント/サーバの IP アドレスを指定します。
-------	----------------	--------------------------------

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
	8.0(4)	このコマンドが追加されました。

例 次に、既存の MMP セッションに関する情報を表示する **show mmp** コマンドの使用例を示します。

```
ciscoasa# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

関連コマンド	コマンド	説明
	debug mmp	MMP 検査イベントを表示します。
	inspect mmp	MMP インспекション エンジンを設定します。
	show debug mmp	MMP インспекション モジュールの現在のデバッグ設定を表示します。

show mode

実行中のソフトウェア イメージ、およびフラッシュ メモリ内の任意のイメージのためのセキュリティ コンテキスト モードを表示するには、特権 EXEC モードで **show mode** コマンドを使用します。

show mode

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。

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。

例

次に、**show mode** コマンドの出力例を示します。次に、現在のモードと、実行されていないイメージ「image.bin」のモードの例を示します。

```
ciscoasa# show mode flash:/image.bin
Firewall mode: multiple
```

モードは、マルチまたはシングルのいずれかです。

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
mode	コンテキスト モードをシングルまたはマルチに設定します。

show module

ASA にインストールされているモジュールに関する情報を表示するには、ユーザ EXEC モードで **show module** コマンドを使用します。

show module [*id* | **all**] [**details** | **recover** | **log** [**console**]

構文の説明

all	(デフォルト)すべてのモジュールの情報を表示します。
console	(オプション)モジュールのコンソール ログ情報を表示します。
details	(オプション)モジュールのリモート管理設定などの追加情報を表示します。
<i>id</i>	モジュール ID を指定します。ハードウェア モジュールの場合、 0 (ASA の場合)または 1 (インストールされたモジュールの場合)のいずれかのスロット番号を指定します。ソフトウェア モジュールの場合、次の名前のいずれかを指定します。 <ul style="list-style-type: none"> • sfr: ASA FirePOWER モジュール。 • ips: IPS モジュール • cxsc: ASA CX モジュール
ログ	(オプション)モジュールのログ情報を表示します。
recover	(オプション) hw-module または sw-module module recover コマンドの設定を表示します。

デフォルト

デフォルトでは、すべてのモジュールの情報が表示されます。

コマンドモード

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		
	ルータッド	トランスペ アレント	シングル	マルチ コンテキ スト ¹	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

1. **show module recover** コマンドは、システム実行スペースでのみ使用できます。

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。
7.1(1)	このコマンドは、より多くの詳細情報を出力するように変更されました。
8.2(1)	SSC に関する情報が出力に含まれています。
8.2(5)	ASA 5585-X と、ASA 5585-X 上の IPS SSP のサポートに関する情報が追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。

リリース	変更内容
8.6(1)	ASA 5512-X ~ ASA 5555-X では、 log および console キーワードが追加されました。さらに、 ips のデバイス ID が追加されました。
9.1(1)	ASA CX ソフトウェア モジュールのサポートが、 cxsc モジュール ID の追加によって追加されました。
9.2(1)	sfr キーワードを含め、ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、ASA にインストールされているモジュールに関する情報を表示します。ASA 自体もディスプレイにモジュールとして表示されます(スロット 0)。

例

次に、**show module** コマンドの出力例を示します。モジュール 0 はベース デバイス。モジュール 1 は CSC SSM です。

```
ciscoasa# show module
Mod Card Type                               Model                               Serial No.
-----
 0 ASA 5520 Adaptive Security Appliance     ASA5520                             P3000000034
 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20                           0

Mod MAC Address Range                       Hw Version   Fw Version   Sw Version
-----
 0 000b.fcf8.c30d to 000b.fcf8.c311        1.0          1.0(10)0    7.1(0)5
 1 000b.fcf8.012c to 000b.fcf8.012c        1.0          1.0(10)0    CSC SSM 5.0 (Build#1187)

Mod SSM Application Name                   SSM Application Version
-----
 1 CSC SSM scan services are not
 1 CSC SSM                                  5.0 (Build#1187)

Mod Status      Data Plane Status   Compatibility
-----
 0 Up Sys        Not Applicable
 1 Up            Up
```

次の表に、出力に表示される各フィールドを示します。

表 9-12 **show module** の出力フィールド

フィールド	説明
Mod	モジュール番号、0 または 1。
ポート	ポート番号。
Card Type	モジュール 0 に表示されるデバイスの場合、タイプはプラットフォームモデルです。モジュール 1 の SSM の場合、タイプは SSM タイプです。
モデル	このモジュールのモデル番号。
Serial No.	シリアル番号。
MAC Address Range	この SSM、またはデバイス、組み込みインターフェイスの MAC アドレス範囲。
Hw Version	ハードウェアのバージョン。
Fw Version	ファームウェアのバージョン。

表 9-12 `show module` の出力フィールド(続き)

フィールド	説明
Sw Version	ソフトウェアのバージョン。
SSM Application Name	SSM で実行されているアプリケーションの名前。
SSM Application Version	SSM で実行されているアプリケーションのバージョン。
Status (ステータス)	モジュール 0 のデバイスの場合、ステータスは Up Sys です。モジュール 1 の SSM のステータスは、次のいずれかです。 <ul style="list-style-type: none"> • Initializing: SSM が検出され、デバイスによってコントロール通信が初期化されます。 • Up: SSM がデバイスによる初期化を完了しました。 • Unresponsive: この SSM との通信中にデバイスでエラーが発生しました。 • Reloading: SSM がリロード中です。 • Shutting Down: SSM をシャットダウンしています。 • Down: SSM がシャットダウンされました。 • Recover: SSM が回復イメージをダウンロードしようとしています。 • No Image Present: IPS ソフトウェアがインストールされていません。
Data Plane Status	データ プレーンの現在の状態。
互換性	残りのデバイスに関連した SSM の互換性。
スロット	物理スロット番号(デュアル SSP モードでのみ有効)。

show module details コマンドの出力は、インストールされているモジュールによって異なります。たとえば、CSC SSM の出力には CSC SSM ソフトウェアのコンポーネントに関するフィールドが含まれます。

次に、**show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:                ASA-SSM-20
Hardware version:     V1.0
Serial Number:        12345678
Firmware version:     1.0(7)2
Software version:     4.1(1.1)S47(0.1)
MAC Address Range:    000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:    Up
Status:                Up
Mgmt IP addr:         10.89.147.13
Mgmt web ports:       443
Mgmt TLS enabled:     true
```

次の表に、出力の追加フィールドを示します。

表 9-13 *show module details* の追加出力フィールド

フィールド	説明
DC address (表示なし)	(ASA FirePOWER のみ)。モジュールを管理する Firepower Management Center のアドレス。
Mgmt IP addr	モジュールの管理インターフェイスの IP アドレスを表示します。
Mgmt Network Mask (表示なし)	管理アドレスのサブネット マスクを表示します。
Mgmt Gateway (表示なし)	管理アドレスのゲートウェイ。
Mgmt web ports	モジュールの管理インターフェイスに設定されたポートを表示します。
Mgmt TLS enabled	モジュールの管理インターフェイスの接続に対して Transport Layer Security がイネーブルであるかどうか(True または False)を表示します。

ソフトウェア モジュールを設定できるモデルの場合、**show module** コマンドは可能なすべてのモジュールを表示します。ステータス情報は、これらの 1 つがインストールされているかどうかを表示します。

```
ciscoasa# show module
```

```
Mod  Card Type                               Model                               Serial No.
-----
  0  ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt  ASA5555                             FCH1714J6HP
ips  Unknown                                  N/A                                  FCH1714J6HP
cxsc Unknown                                  N/A                                  FCH1714J6HP
sfr  FirePOWER Services Software Module     ASA5555                             FCH1714J6HP
```

```
Mod  MAC Address Range                       Hw Version  Fw Version  Sw Version
-----
  0  bc16.6520.1dcd to bc16.6520.1dd6  1.0         2.1(9)8    100.8(66)11
ips  bc16.6520.1dcb to bc16.6520.1dcb  N/A         N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A         N/A
sfr  bc16.6520.1dcb to bc16.6520.1dcb  N/A         N/A         5.3.1-100
```

```
Mod  SSM Application Name                     Status           SSM Application Version
-----
ips  Unknown                                  No Image Present Not Applicable
cxsc Unknown                                  No Image Present Not Applicable
sfr  ASA FirePOWER                             Up              5.3.1-100
```

```
Mod  Status           Data Plane Status  Compatibility
-----
  0  Up Sys          Not Applicable
ips  Unresponsive    Not Applicable
cxsc Unresponsive    Not Applicable
sfr  Up              Up
```

```
Mod  License Name  License Status  Time Remaining
-----
ips  IPS Module   Enabled        172 days
```

次に、**show module 1 recover** コマンドの出力例を示します。

```
ciscoasa# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:          tftp://10.21.18.1/ids-oldimg
Port IP Address:    10.1.2.10
Port Mask :         255.255.255.0
Gateway IP Address: 10.1.2.254
```

次に、SSC がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc:
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                   209.165.202.158/32
                   209.165.200.254/24
Mgmt Vlan: 20
```

次に、ASA 5585-X に IPS SSP がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: V1.0
Serial Number: 12345678
Firmware version: 1.0(7)2
Software version: 4.1(1.1)S47(0.1)
MAC Address Range: 000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status: Up
Status: Up
Mgmt IP addr: 10.89.147.13
Mgmt web ports: 443
Mgmt TLS enabled: true
```

次に、ASA 5585-X に CXSC SSP がインストールされているときの **show module all** コマンドの出力例を示します。

```
ciscoasa# show module all
```

Mod	Card Type	Model	Serial No.
0	ASA 5585-X Security Services Processor-10 wi	ASA5585-SSP-10	JAF1504CBRM
1	ASA 5585-X CXSC Security Services Processor-1	ASA5585-SSP-IPS10	JAF1510BLSE

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
0	ASA 5585-X Security Services Processor-10 wi	ASA5585-SSP-10	JAF1504CBRM	
1	ASA 5585-X CXSC Security Services Processor-1	ASA5585-SSP-IPS10	JAF1510BLSE	

```

-----
 0 5475.d05b.1d54 to 5475.d05b.1d5f 1.0          2.0(7)0      100.7(14)13
 1 5475.d05b.248c to 5475.d05b.2497 1.0          0.0(0)0      1.0

Mod SSM Application Name          Status          SSM Application Version
-----
 1 CXSC Security Module           Up              1.0

Mod Status          Data Plane Status  Compatibility
-----
 0 Up Sys           Not Applicable
 1 Up               Up

```

次に、ASA 5585-X に CXSC SSP がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```

ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version: 1.0
Serial Number: 123456789
Firmware version: 1.0(9)0
Software version: CXSC Security Module Version 1.0
App. name: CXSC Security Module
App. version: Version 1.0
Data plane Status: Up
Status: Up
HTTP Service: Up
Activated: Yes
Mgmt IP addr: 100.0.1.4
Mgmt web port: 8443

```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブートプロセスに関するデバッグメッセージを表示します。
hw-module module recover	回復イメージを TFTP サーバからロードして、モジュールを回復します。
hw-module module reset	モジュールをシャットダウンし、ハードウェアリセットを実行します。
hw-module module reload	モジュールソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーションデータを失わずに電源を切るための準備として、モジュールソフトウェアを閉じます。
sw-module	ソフトウェアモジュールを設定します。

show monitor-interface

フェールオーバーのためにモニタ対象にするインターフェイスの情報を表示するには、特権 EXEC モードで **show monitor-interface** コマンドを使用します。

show monitor-interface

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。

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。
8.2(2)	IPv6 アドレスが出力に追加されました。

使用上のガイドライン

インターフェイスには複数の IPv6 アドレスを設定できるため、**show monitor-interface** コマンドではリンクローカルアドレスのみが表示されます。IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- **Unknown**: 初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- **Normal**: インターフェイスはトラフィックを受信しています。
- **Normal (Waiting)**: インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
- **Testing**: ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- **Link Down**: インターフェイスまたは VLAN は管理のためにダウンしています。

- **No Link**: インターフェイスの物理リンクがダウンしています。
- **Failed**: インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

例

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

```
ciscoasa# show monitor-interface
```

```
This host: Primary - Active
    Interface outside (10.86.94.88): Normal (Waiting)
    Interface management (192.168.1.1): Normal (Waiting)
    Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
Other host: Secondary - Failed
    Interface outside (0.0.0.0): Unknown (Waiting)
    Interface management (0.0.0.0): Unknown (Waiting)
    Interface failif (0.0.0.0): Unknown (Waiting)
```

関連コマンド

コマンド	説明
monitor-interface	特定のインターフェイスでのヘルス モニタリングをイネーブルにします。

show mrib client

MRIB クライアント接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib client** コマンドを使用します。

show mrib client [**filter**] [**name client_name**]

構文の説明

filter	(任意) クライアント フィルタを表示します。各クライアントが所有する MRIB フラグと、各クライアントに関連するフラグに関する情報を表示するために使用します。
name client_name	(任意) PIM または IGMP など、MRIB のクライアントとして動作するマルチキャストルーティングプロトコルの名前。

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 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
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

filter オプションを使用して、さまざまな MRIB クライアントが登録されているルートおよびインターフェイス レベル フラグの変更を表示します。このコマンド オプションからは、MRIB クライアントが所有するフラグも表示されます。

例

次に、**filter** キーワードを使用した **show mrib client** コマンドの出力例を示します。

```
ciscoasa# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
```

```

groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All

```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルのエントリを表示します。

show mrib route

MRIB テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib route** コマンドを使用します。

```
show mrib route [[source | *] [group[/prefix-length]]]
```

構文の説明

*	(任意) 共有ツリー エントリを表示します。
<i>/prefix-length</i>	(任意)MRIB ルートのプレフィックス長。プレフィックス(アドレスのネットワーク部分)を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
<i>group</i>	(任意) グループの IP アドレスまたは名前。
<i>source</i>	(任意) ルート送信元の IP アドレスまたは名前。

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 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
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

MFIB テーブルには、MRIB から更新されるエントリとフラグのサブセットが保持されます。フラグは、マルチキャスト パケットの転送ルールのセットに従って、転送およびシグナリングの動作を決定します。

インターフェイスとフラグのリストに加えて、各ルート エントリにはさまざまなカウンタが表示されます。バイト数は、転送されたバイトの合計数です。パケット数は、このエントリについて受信されたパケット数です。**show mfib count** コマンドは、ルートとは無関係にグローバルなカウンタを表示します。

例

次に、**show mrib route** コマンドの出力例を示します。

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
             C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
                NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
                II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
    Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
    POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
    POS0/3/0/0 Flags: F NS LI
    Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
    POS0/3/0/0 Flags: F NS
    Decapstunnel0 Flags: A
```

関連コマンド

コマンド	説明
show mfib count	MFIB テーブルのルートとパケット数データを表示します。
show mrib route summary	MRIB テーブル エントリの要約を表示します。

show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、特権 EXEC モードで **show mroute** コマンドを使用します。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

構文の説明

active rate	(任意) アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定された <i>rate</i> 以上で送信を実行している送信元です。 <i>rate</i> が指定されていない場合、アクティブな送信元は 4 kbps 以上のレートで送信を実行している送信元です。
count	(任意) グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。
group	(任意) DNS ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。
pruned	(任意) プルーニングされたルートを表示します。
reserved	(任意) 予約済みグループを表示します。
<i>source</i>	(任意) 送信元のホスト名または IP アドレス。
summary	(任意) マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。

デフォルト

rate 引数を指定しない場合、デフォルトでは 4 Kbps になります。

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。

使用上のガイドライン

show mroute コマンドは、マルチキャストルーティングの内容を表示します。ASA は、PIM プロトコル メッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して、マルチキャストルーティングテーブルにデータを入力します。アスタリスク(*) は、すべての送信元アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャストグループアドレスを示します。(S,G) エントリを作成する場合、ソフトウェアはユニキャストルーティングテーブル内で(RPF を経由して)見つかった宛先グループへの最適パスを使用します。

実行コンフィギュレーションに含まれている **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**show mroute** コマンドの出力例を示します。

```
ciscoasa(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute の出力には、次のフィールドが含まれています。

- **Flags:** エントリに関する情報を提供します。
 - **D (Dense):** エントリはデンス モードで動作しています。
 - **S (Sparse):** エントリはスパース モードで動作しています。
 - **B (Bidir Group):** マルチキャスト グループが双方向モードで動作していることを示します。
 - **s (SSM Group):** マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
 - **C (Connected):** マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
 - **L (Local):** ASA 自体が、マルチキャスト グループのメンバーです。グループは、(設定済みのグループに対する) **igmp join-group** コマンドによってローカルに加入されています。
 - **I (Received Source Specific Host Report):** (S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。

- **P (Pruned)**: ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウストリーム メンバーが送信元に加入できるようにします。
- **R (RP-bit set)**: (S,G) エントリが RP をポイントしていることを示します。
- **F (Register flag)**: ソフトウェアがマルチキャスト送信元に登録されていることを示します。
- **T (SPT-bit set)**: パケットが最短パス送信元ツリーで受信されていることを示します。
- **J (Join SPT)**: (*, G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します(デフォルトの SPT しきい値設定は 0 kbps です)。J - Join 最短パス ツリー (SPT) フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、ASA は送信元ツリーに加入します。

(S, G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、ASA は送信元ツリー上のトラフィック速度をモニタします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとします。



(注) ASA は共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*, G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

グループにデフォルトの SPT しきい値 (0 Kbps) が使用されている場合、(*, G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、ASA は最短パス送信元ツリーにただちに切り替えます。

- **Timers:Uptime/Expires**: Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間 (時間、分、秒) をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間 (時間、分、秒) をインターフェイスごとに示します。
- **Interface state**: 着信インターフェイスまたは発信インターフェイスの状態を示します。
 - **Interface**: 着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。
 - **State**: アクセス リストまたは Time to Live (TTL) しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。
- **(* , 239.1.1.40) と (* , 239.2.2.1)**: IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク (*) は、すべての送信元を意味します。
- **RP**: RP のアドレス。スパス モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 224.0.0.0 です。
- **Incoming interface**: 送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- **RPF nbr**: 送信元に対するアップストリーム ルータの IP アドレス。
- **Outgoing interface list**: パケット転送時に使用されるインターフェイス。

関連コマンド

コマンド	説明
clear configure mroute	実行コンフィギュレーションから mroute コマンドを削除します。
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	設定されているマルチキャスト ルートを表示します。