show b ～ show cq

show backup-package

Cisco ISA 3000 のバックアップパッケージのステータスとサマリー情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show backup-package** コマンドを使用します。

show backup-package { **status** { **backup | restore** } **| summary** }

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

構文の説明

backup | restore	表示する **status** 情報のタイプを指定します。
status	バックアップ操作または復元操作のいずれかのモード、ロケーション、パスフレーズ、最新の時刻情報を表示します。
summary	バックアップ操作と復元操作の両方のステータス情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	この コマンドが追加されました。

使用上のガイドライン

show backup-package コマンドはグローバル コンフィギュレーション モードでも使用可能です。

例

次に、バックアップパッケージのサマリー統計情報を表示する例を示します。

```
ciscoasa# show backup-package summary
 backup mode      : auto
 backup location  : disk3:
```

```
backup passphrase: cisco
last backup time : Mar 23 2014 22:05:52
restore mode      : auto
restore location  : disk3:
restore passphrase: cisco
Last restore time : Mar 24 2014 05:07:32
```

show bfd drops

BFDでドロップされたパケットの数を表示するには、グローバルコンフィギュレーションモードで show bfd drops コマンドを使用します。

show bfd drops

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

このコマンドにデフォルトの動作または値はありません。

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	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD でドロップされたパケットを表示する例を示します。

```
ciscoasa# show bfd drops
BFD Drop Statistics
                        IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL             0    0    0      0
BFD Not Configured      0    0    0      0
No BFD Adjacency        0    0    0      0
Invalid Header Bits     0    0    0      0
Invalid Discriminator   0    0    0      0
Session AdminDown       0    0    0      0
Authen invalid BFD ver  0    0    0      0
Authen invalid len      0    0    0      0
Authen invalid seq      0    0    0      0
Authen failed           0    0    0      0
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。

コマンド	説明
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFDテンプレートを設定し、BFDコンフィギュレーションモードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd map

設定済みの BFD マップを表示するには、グローバル コンフィギュレーション モードで show bfd map コマンドを使用します。

show bfd map

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

このコマンドにデフォルトの動作または値はありません。

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	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップを表示する例を示します。

```
ciscoasa# show bfd map
Destination: 40.40.40.2/24
 Source: 50.50.50.2/24
 Template: mh
 Authentication(Type): sha-1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。

コマンド	説明
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFDテンプレートを設定し、BFDコンフィギュレーションモードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd neighbors

既存の BFD 隣接関係の詳細なリストを表示するには、グローバル コンフィギュレーション モードで show bfd neighbors コマンドを使用します。

show bfd neighbors [**client** { **bgp** } | **details** | **interface** *interface-name* | **ipv4** *ip-address* | **ipv6** *ipv6-address* | **multihop-ipv4** *ip-address* | **multihop-ipv6** *ipv6-address*]

構文の説明

クライアント	（オプション）特定のクライアントのネイバーを表示します。
bgp	（オプション）BGP クライアントを表示します。
details	（オプション）各ネイバーのすべての BFD プロトコル パラメータおよびタイマーを表示します。
interface interface-name	（オプション）指定されたインターフェイスのネイバーを表示します。
ipv4 ip-address	（オプション）指定されたシングルホップ IP ネイバーを表示します。
ipv6 ipv6-address	（オプション）指定されたシングルホップ IPv6 ネイバーを表示します。
multihop-ipv4 ip-address	（オプション）指定されたマルチホップ IP ネイバーを表示します。
multihop-ipv6 ipv6-address	（オプション）指定されたマルチホップ IPv6 ネイバーを表示します。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、BFD 問題をトラブルシューティングできます。

例

次に、BFD ネイバーを表示する例を示します。

```
ciscoasa# show bfd neighbors
OurAddr     NeighAddr    LD/RD  RH     Holdown(mult)     State Int
172.16.10.1 172.16.10.2  1/6    1      260 (3 )          Up    Fa0/1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFDテンプレートを設定し、BFDコンフィギュレーションモードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd summary

BFD のサマリー情報を表示するには、グローバル コンフィギュレーション モードで show bfd summary コマンドを使用します。

show bfd summary［ **client | host | session** ］

構文の説明

クライアント	（オプション）クライアントの BFD サマリーを表示します。
ホスト	（オプション）セッションの BFD サマリーを表示します。
session	（オプション）プロトコルの BFD サマリーを表示します。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、BFD、BFD クライアント、または BFD セッションのサマリー情報を表示できます。BFD クライアントがピアとのセッションを開始すると、BFD は定期的に BFD 制御パケットをピアに送信します。次のセッションの状態に関する情報が、このコマンドの出力に含まれます。

- Up：別の BFD インターフェイスが BFD 制御パケットに確認応答すると、セッションはアップ状態に移行します。
- Down：データ パスで障害が生じ、BFD が設定された時間内に制御パケットを受信しない場合は、セッションとデータ パスがダウンとして宣言されます。セッションがダウンした場合は、BFD クライアントがトラフィックを再ルーティングするために必要なアクションを実行できるように、BFD が BFD クライアントに通知します。

例

次に、BFD サマリーを表示する例を示します。

```
ciscoasa# show bfd summary

         Session         Up      Down
Total    1               1       0
ciscoasa# show bfd summary session
Protocol                  Session     Up  Down
IPV4                      1     1     0
Total                     1     1     0
ciscoasa# show bfd summary client
Client                    Session      Up     Down
BGP                       1       1    0
EIGRP                     1       1    0
Total                     2       2    0
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップBFDテンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFDテンプレートを設定し、BFDコンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGPが登録され、BFDから転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。

show bgp

Border Gateway Protocol（BGP）ルーティングテーブル内のエントリを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp コマンドを使用します。

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath | multipaths | subnets**] | **bestpath | multipaths**] | **all | prefix-list name | pending-prefixes | route-map** *name*]]

構文の説明

ip-address	（オプション）AS パス アクセス リスト名を指定します。
mask	（オプション）指定したネットワークの一部であるホストをフィルタリングまたは照合するためのマスク。
longer-prefixes	（オプション）指定したルートと、より限定的なすべてのルートを表示します。
injected	（オプション）BGP ルーティング テーブルに注入された、より限定的なプレフィックスを表示します。
shorter-prefixes	（オプション）指定したルートと、より限定的でないすべてのルートを表示します。
length	（オプション）プレフィックス長。この引数の値は、0 ～ 32 の数値です。
bestpath	（オプション）このプレフィックスの最適パスを表示します。
multipaths	（オプション）このプレフィックスのマルチパスを表示します。
subnets	（オプション）指定したプレフィックスのサブネット ルートを表示します。
all	（オプション）BGP ルーティング テーブルのすべてのアドレス ファミリ情報を表示します。
prefix-list name	（オプション）指定したプレフィックス リストに基づいて出力をフィルタリングします。
pending-prefixes	（オプション）BGP ルーティング テーブルからの削除が保留されているプレフィックスを表示します。
route-map name	（オプション）指定したルート マップに基づいて出力をフィルタリングします。

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、ユーザー EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

show bgp コマンドは、BGP ルーティングテーブルの内容を表示するために使用します。出力は、特定のプレフィックスのエントリ、特定のプレフィックス長のエントリ、および、プレフィックスリスト、ルートマップ、または条件付きアドバタイズメントを介して注入されたプレフィックスのエントリを表示するようにフィルタリングできます。

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、CiscoIOS XE Release 2.4、およびそれ以降のリリースでは、シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドに続けて、clear bgp * コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

例

次に、BGP ルーティング テーブルの出力例を示します。

```
Router# show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

表 1 : show bgp のフィールド に、各フィールドの説明を示します。

表 *1 : show bgp* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 • s：テーブルエントリが抑制されます。 • d：テーブルエントリがダンプニングされています。 • h：テーブルエントリの履歴です。 • *：テーブルエントリが有効です。 • >：テーブルエントリがそのネットワークで使用するための最良エントリです。 • i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。 • r：テーブルエントリは RIB 障害です。 • S：テーブルエントリは失効しています。 • m：テーブルエントリには、そのネットワークで使用するためのマルチパスが含まれています。 • b：テーブルエントリには、そのネットワークで使用するためのバックアップ パスが含まれています。 • x：テーブル エントリには、ネットワークで使用するための最適外部ルートが含まれています。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 • i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 • e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 • ?：パスの発信元はクリアされません。通常、これはIGPからBGPに再配信されるルータです。

フィールド	説明
Network	ネットワークエンティティの IP アドレス
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システムメトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システム フィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。
(stale)	指定した自律システムの次のパスがグレースフル リスタート プロセス中に「stale」とマークされたことを示します。

例

show bgp（4 バイト自律システム番号）：例

次に、BGP ルーティングテーブルの出力例を示します。[Path] フィールドの下に 4 バイト自律システム番号（65536 と 65550）が表示されます。この例では、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、Cisco IOS XE Release 2.4 またはそれ以降のリリースが必要です。

```
RouterB# show bgp
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show bgp ip-address：例

次に、BGP ルーティングテーブルの 192.168.1.0 エントリに関する情報の出力例を示します。

```
Router# show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
```

```
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

次に、BGP ルーティングテーブルの 10.3.3.3 255.255.255.255 エントリに関する情報の出力例を示します。

```
Router# show bgp 10.3.3.3 255.255.255.255
BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

表 2 : show bgp（4 バイト自律システム番号）のフィールド に、各フィールドの説明を示します。

表 *2 : show bgp*（*4* バイト自律システム番号）のフィールド

フィールド	説明
BGP routing table entry fo	ルーティング テーブル エントリの IP アドレスまたはネットワーク番号。
version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
Paths	使用可能なパスの数、およびインストールされた最適パスの数。最適パスが IP ルーティングテーブルに登録されている場合、この行に「Default-IP-Routing-Table」と表示されます。
Multipath	このフィールドは、マルチパス ロードシェアリングがイネーブルの場合に表示されます。このフィールドは、マルチパスが iBGP と eBGP のどちらであるかを示します。
Advertised to update-groups	アドバタイズメントが処理される各アップデートグループの数。

フィールド	説明
Origin	エントリの作成元。送信元はIGP、EGP、incompleteのいずれかになります。この行には、設定されたメトリック（メトリックが設定されていない場合は0）、ローカルプリファレンス値（100がデフォルト）、およびルートのステータスとタイプ（内部、外部、マルチパス、最適）が表示されます。
Extended Community	このフィールドは、ルートが拡張コミュニティ属性を伝送する場合に表示されます。この行には、属性コードが表示されます。拡張コミュニティに関する情報は後続の行に表示されます。

例

show bgp all：例

次に、allキーワードを指定したshow bgpコマンドの出力例を示します。設定されたすべてのアドレス ファミリに関する情報が表示されます。

```
Router# show bgp all
For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

show bgp longer-prefixes：例

次に、longer-prefixes キーワードを指定した show bgp コマンドの出力例を示します。

```
Router# show bgp 10.92.0.0 255.255.0.0 longer-prefixes
BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                           0 109 108 ?
```

```
*> 10.92.1.0         10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.11.0        10.92.72.30       42482         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.14.0        10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.15.0        10.92.72.30        8696         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.16.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.17.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.18.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.19.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
```

show bgp shorter-prefixes：例

次に、shorter-prefixes キーワードを指定した show bgp コマンドの出力例を示します。8 ビット プレフィックス長を指定しています。

```
Router# show bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0         10.0.0.2                              0 ?
*                     10.0.0.2                0             0 200 ?
```

show bgp prefix-list：例

次に、prefix-list キーワードを指定した show bgp コマンドの出力例を示します。

```
Router# show bgp prefix-list ROUTE
BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                0              0 200 ?
```

show bgp route-map：例

次に、route-map キーワードを指定した show bgp コマンドの出力例を示します。

```
Router# show bgp route-map LEARNED_PATH
BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                0              0 200 ?
```

show bgp all community

特定の Border Gateway Protocol（BGP）コミュニティに属するすべてのアドレスファミリのルートを表示するには、ユーザー EXEC モードまたは特権 EXEC コンフィギュレーション モードで show bgp all community コマンドを使用します。

show bgp all community [*community-number....* [*community-number*]] [**local-as**] [**no-advertise**] [**no-export**] [**exact-match**]

構文の説明

community-number.	（オプション）指定したコミュニティ番号に関連するルートを表示します。 複数のコミュニティ番号を指定できます。範囲は 1 ～ 4294967295 または AA:NN（自律システム:コミュニティ番号（2 バイトの番号））です。
local-as	（オプション）ローカル自律システム外に送信されないルートだけを表示します（ウェルノウン コミュニティ）。
no-advertise	（オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。
no-export	（オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。
exact-match	（オプション）指定した BGP コミュニティ リストと正確に一致するルートだけを表示します。 （注） コマンドのキーワードの可用性はコマンド モードによって異なります。exact-match キーワードは、ユーザー EXEC モードでは使用できません。

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、ユーザー 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
9.2(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

ユーザーは、local-as、no-advertise、no-export の各キーワードを任意の順序で入力できます。bgp all community コマンドを使用する場合、数値のコミュニティはウェルノウンコミュニティの前に入力してください。

たとえば、次の文字列は無効です。

```
ciscoasa# show bgp all community local-as 111:12345
```

代わりに、次の文字列を使用します。

```
ciscoasa# show bgp all community 111:12345 local-as
```

例

次に、show bgp all community コマンドの出力例を示します。ここでは、1、2345、6789012 の各コミュニティを指定しています。

```
ciscoasa# show bgp all community 1 2345 6789012 no-advertise local-as no-export exact-match
For address family: IPv4 Unicast
BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network    Next Hop            Metric LocPrf Weight  Path
*> 10.0.3.0/24       10.0.0.4                               0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                 0             0 4 ?
*> 10.12.34.0/24     10.0.0.6                 0             0 6 ?
```

表 26 : show blocks のフィールド に、各フィールドの説明を示します。

表 3 : show bgp all community のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	BGP コミュニティを表示するように設定されたルータのルータ ID。ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリは抑制されています。d：テーブルエントリはダンプニングされています。h：テーブルエントリは履歴です。*：テーブルエントリは有効です。>：テーブルエントリはそのネットワークで使用するための最良エントリです。i：テーブルエントリは内部 BGP セッションを介して学習されています。
Origin codes	エントリの作成元を示します。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイプロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。e：外部ゲートウェイプロトコル（EGP）から発信されたエントリ。?：パスの発信元は不明です。通常、これは、IGP から BGP に再配布されたルートです。
Network	ネットワーク エンティティのネットワーク アドレスおよびネットワーク マスク。アドレスのタイプは、アドレス ファミリによって異なります。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。アドレスのタイプは、アドレス ファミリによって異なります。
Metric	相互自律システム メトリック。このフィールドはあまり使用されません。
LocPrf	set local-preference コマンドで設定されたローカルプリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。

show bgp all neighbors

すべてのアドレスファミリのネイバーへの Border Gateway Protocol（BGP）接続に関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp all neighbors コマンドを使用します。

show bgp all neighbors ［ *ip-address* ］［ **advertised-routes | paths** ［ *reg-exp* ］ **| policy** ［ **detail** ］ **| received prefix-filter | received-routes | routes** ］

構文の説明

ip-address	（任意）ネイバーの IP アドレスです。この引数を省略すると、すべてのネイバーに関する情報が表示されます。
advertised-routes	（オプション）ネイバーにアドバタイズされたすべてのルートを表示します。
paths reg-exp	（オプション）指定したネイバーから学習した自律システムパスを表示します。オプションの正規表現を使用して、出力をフィルタ処理できます。
ポリシー	（オプション）アドレスファミリごとに、ネイバーに適用されるポリシーを表示します。
detail	（オプション）ルート マップ、プレフィックス リスト、コミュニティ リスト、アクセス コントロール リスト（ACL）、自律システム パス フィルタ リストなどの詳細なポリシー情報を表示します。
received prefix-filter	（オプション）指定したネイバーから送信されたプレフィックス リスト（アウトバウンド ルート フィルタ（ORF））を表示します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
routes	（オプション）受信され、受け入れられるすべてのルートを表示します。このキーワードが入力されたときに表示される出力は、received-routes キーワードによって表示される出力のサブセットです。

コマンド デフォルト

このコマンドの出力には、すべてのネイバーの情報が表示されます。

コマンド 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、ユーザー 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
9.2(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

IPv4 などのアドレスファミリに固有のネイバーセッションの BGP および TCP 接続情報を表示するには、show bgp all neighbors コマンドを使用します。

例

次に、show bgp all neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp all neighbors
For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
```

```
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent:4445 (retransmit: 5), with data: 4445, total data bytes;244128
```

表 4 : show bgp all neighbor のフィールド に、各フィールドの説明を示します。

表 *4 : show bgp all neighbor* のフィールド

フィールド	説明
For address family	後続のフィールドが参照するアドレスファミリ。
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。
remote AS	ネイバーの自律システム番号。
external link	外部ボーダー ゲートウェイ プロトコル（eBGP）peerP。
BGP version	リモート ルータとの通信に使用される BGP バージョン。
remote router ID	ネイバーの IP アドレス。
BGP state	この BGP 接続の状態。
up for	ベースとなる TCP 接続が存在している時間（hh:mm:ss 形式）。
Last read	BGP がこのネイバーから最後にメッセージを受信してからの時間（hh:mm:ss 形式）。
hold time	BGP がメッセージを受信せずにこのネイバーとセッションを維持した時間（秒数）。
keepalive interval	キープアライブ メッセージがこのネイバーに転送される間隔（秒数）。
Message statistics	メッセージ タイプごとにまとめられた統計。
InQ depth is	入力キュー内のメッセージ数。
OutQ depth is	出力キュー内のメッセージ数。
Sent	送信されたメッセージの合計数。
Rcvd	受信されたメッセージの合計数。
Opens	送受信されたオープンメッセージ数。
Notifications	送受信された通知（エラー）メッセージ数。
Updates	送受信されたアップデートメッセージ数。

フィールド	説明
Keepalives	送受信されたキープアライブメッセージ数。
Route Refresh	送受信されたルートリフレッシュ要求メッセージ数。
Total	送受信されたメッセージの合計数。
Default minimum time between...	アドバタイズメント送信の間の時間（秒数）。
Connections established	TCP および BGP 接続が正常に確立した回数。
dropped	有効セッションに障害が発生したか停止した回数。
Last reset	このピアリングセッションが最後にリセットされてからの時間（hh:mm:ss 形式）。リセットがこの行に表示された理由。
External BGP neighbor may be...	BGP 存続可能時間（TTL）セキュリティ チェックがイネーブルであることを示します。ローカルピアとリモートピアをまたぐことができるホップの最大数がこの行に表示されます。
Connection state	BGP ピアの接続ステータス。
Local host、Local	ローカル BGP スピーカーの IP アドレスとポート番号。
Foreign host, Foreign port	ネイバーアドレスと BGP 宛先ポート番号。
Enqueued packets for retransmit:	TCP によって再送信のためにキューに格納されたパケット。
Event Timers	TCP イベントタイマー。起動およびウェイクアップのカウンタが提供されます（期限切れタイマー）。
Retrans	パケットを再送信した回数。
TimeWait	再送信タイマーが期限切れになるまで待機する時間。
AckHold	確認応答ホールドタイマー
SendWnd	伝送（送信）ウィンドウ。
KeepAlive	キープアライブパケットの数。
GiveUp	確認応答がないためにパケットがドロップされた回数。
PmtuAger	パス MTU ディスカバリタイマー。
DeadWait	デッドセグメントの有効期限タイマー。
iss:	初期パケット送信シーケンス番号。

フィールド	説明
snduna:	確認応答された最後の送信シーケンス番号。
sndnxt:	次に送信されるパケットのシーケンス番号。
sndwnd:	リモート ホストの TCP ウィンドウ サイズ。
irs:	初期パケット受信シーケンス番号。
rcvnxt:	ローカルに確認応答された最後の受信シーケンス番号。
rcvwnd:	ローカルホストの TCP ウィンドウサイズ。
delrcvwnd:	遅延受信ウィンドウ：ローカル ホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT:	計算されたスムーズ ラウンドトリップ タイムアウト。
RTTO:	ラウンドトリップ タイムアウト。
RTV:	ラウンドトリップ時間の差異。
KRTT:	新しいラウンドトリップ タイムアウト（Karn アルゴリズムを使用）。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT:	記録された最小ラウンドトリップ タイムアウト（計算に使用される組み込み値）。
maxRTT:	記録された最大ラウンドトリップ タイムアウト。
ACK hold	ローカル ホストが追加データを伝送（ピギーバック）するために確認応答を遅らせる時間の長さ。
IP Precedence value	BGP パケットの IP プレシデンス。
Datagrams	ネイバーから受信したアップデートパケットの数。
Rcvd:	受信パケット数。
with data	データとともに送信されたアップデートパケットの数。
total data bytes	受信データの合計量（バイト）。
Sent	送信されたアップデートパケットの数。
with data	データとともに受信したアップデート パケットの数。

フィールド	説明
total data bytes	送信データの合計量（バイト）。

show bgp cidr-only

Classless Inter-Domain Routing（CIDR）を使用したルートを表示するには、EXEC モードで show bgp cidr-only コマンドを使用します。

show bgp cidr-only

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 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
9.2(1)	このコマンドが追加されました。

例

次に、show bgp cidr-only コマンドの出力例をします。

```
 ciscoasa# show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

表 5 : show bgp cidr-only のフィールドに、各フィールドの説明を示します。

表 *5 : show bgp cidr-only* のフィールド

フィールド	説明
BGP table version is 220	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp community

指定したBGPコミュニティに属するルートを表示するには、EXECモードでshow bgp communityコマンドを使用します。

show bgp community *community-number* [**exact**]

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
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの show bgp community コマンドの出力例を示します。

```
ciscoasa# show bgp community 111:12345 local-as
 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2            0             0 222 ?
 *> 10.0.0.0         10.43.222.2            0             0 222 ?
 *> 10.43.0.0        10.43.222.2            0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2            0             0 222 ?
 *  10.43.222.0/24   10.43.222.2            0             0 222 i
 *> 172.17.240.0/21  10.43.222.2            0             0 222 ?
 *> 192.168.212.0    10.43.222.2            0             0 222 i
 *> 172.31.1.0       10.43.222.2            0             0 222 ?
```

表 6 : show bgp community のフィールドに、各フィールドの説明を示します。

表 *6 : show bgp community* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp community-list

Border Gateway Protocol（BGP）コミュニティリストで許可されたルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp community-list コマンドを使用します。

show bgp community-list { *community-list-number* | *community-list-name* [**exact-match**] }

構文の説明

community-list-number	1 ～ 500 の範囲の標準または拡張コミュニティリスト番号。
community-list-name	コミュニティ リストの名前。コミュニティ リストの名前は、standard または expanded になります。
exact-match	（オプション）完全一致を持つルートだけを表示します。

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、ユーザー 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
9.2(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

このコマンドを使用する場合は、引数を指定する必要があります。exact-match キーワードは任意です。

例

次に、特権 EXEC モードでの show bgp community-list コマンドの出力例を示します。

```
ciscoasa# show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
```

```
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1             0    100      0 1800 174 ?
*>i                 10.0.16.1             0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1             0    100      0 1800 701 i
*>i                 10.0.16.1             0    100      0 1800 701 i
*                   10.92.72.24                         0 1878 704 701 i
```

表 7 : show bgp community-list のフィールド に、各フィールドの説明を示します。

表 *7 : show bgp community-list* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。

フィールド	説明
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp filter-list

指定したフィルタリストと一致するルートを表示するには、EXEC モードで show bgp filter-list コマンドを使用します。

show bgp filter-list *access-list-name*

構文の説明

access-list-name	自律システム パス アクセス リストの名前。

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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの show bgp filter-list コマンドの出力例を示します。

```
ciscoasa# show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

表 8 : show bgp filter-list のフィールド に、各フィールドの説明を示します。

表 *8 : show bgp filter-list* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp injected-paths

Border Gateway Protocol（BGP）ルーティングテーブルに注入されたすべてのパスを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp injected-paths コマンドを使用します。

show bgp injected-paths

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 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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、EXEC モードでの show bgp injected-paths コマンドの出力例を示します。

```
ciscoasa# show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

表 9 : show bgp injected-path のフィールド に、各フィールドの説明を示します。

表 *9 : show bgp injected-path* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv4

IP バージョン 4（IPv4）Border Gateway Protocol（BGP）ルーティングテーブル内のエントリを表示するには、特権 EXEC モードで show bgp ipv4 コマンドを使用します。

show bgp ipv4

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 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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、show bgp ipv4 unicast コマンドの出力例を示します。

```
ciscoasa# show bgp ipv4 unicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

次に、show bgp ipv4 multicast コマンドの出力例を示します。

```
Router# show bgp ipv4 multicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

show bgp ipv4 に、各フィールドの説明を示します。

表 *10 : show bgp ipv4* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6

IPv6 Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp ipv6 コマンドを使用します。

show bgp ipv6 unicast [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。
ipv6-prefix	（オプション）IPv6 ネットワーク番号。IPv6 BGP ルーティング テーブル内の特定のネットワークを表示するために入力します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/prefix-length	（オプション）IPv6プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
longer-prefixes	（オプション）ルートと、より限定的なルートを表示します。
labels	（オプション）アドレス ファミリごとに、このネイバーに適用されるポリシーを表示します。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

次に、show bgp ipv6 コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

次に、show bgp ipv4 multicast コマンドの出力例を示します。

```
Router# show bgp ipv4 multicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network            Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                           0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   3FFE:C00:E:9::2                        0 1251 1930 559 i
*                   3FFE:3600::A                           0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                           0 293 1275 559 i
*                   3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

表 10 : show bgp ipv4 のフィールド に、各フィールドの説明を示します。

表 *11 : show bgp ipv6* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。

フィールド	説明
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

次に、show bgp ipv6 コマンドの出力例を示します。ここでは、プレフィックス 3FFE:500::/24 に関する情報を示しています。

```
ciscoasa# show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
```

```
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
ciscoasa# show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv6 community

IPv6 Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp ipv6community コマンドを使用します。

show bgp ipv6 unicast community [*community-number*] [**exact-match**] [**local-as | no-advertise | no-export**]

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。
community-number	（オプション）有効な値は 1 ～ 4294967295 のコミュニティ番号、または AA:NN（自律システムのコミュニティ番号:2 バイトの番号）です。
exact-match	（オプション）完全一致を持つルートだけを表示します。
local-as	（オプション）ローカル自律システム外に送信されないルートだけを表示します（ウェルノウン コミュニティ）。
no-advertise	（オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。
no-export	（オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 community コマンドの出力は show ip bgp community コマンドと類似しています。

コミュニティは、set community ルート マップ コンフィギュレーション コマンドを使用して設定します。数値のコミュニティはウェルノウン コミュニティの前に入力する必要があります。たとえば、次の文字列は無効です。

```
ciscoasa# show ipv6 bgp unicast community local-as 111:12345
```

代わりに、次の文字列を使用します。

```
ciscoasa# show ipv6 bgp unicast community 111:12345 local-as
```

例

次に、show bgp ipv6 community コマンドの出力例を示します。

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
       Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64      ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80     ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                            0 2 ?
*>                       ::                                         0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64      ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64       2000:0:0:3::2                            0 2 3 i
*> 2010::/64                ::                                       0 32768 ?
*> 2020::/64                ::                                       0 32768 ?
*> 2030::/64                ::                                       0 32768 ?
*> 2040::/64                ::                                       0 32768 ?
*> 2050::/64                ::                                       0 32768 ?
```

表 *12 : show bgp ipv6 community* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 community-list

IPv6 Border Gateway Protocol（BGP）コミュニティ リストで許可されたルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp ipv6 community-list コマンドを使用します。

show bgp ipv6 unicast community-list { *number* | *name* } [**exact-match**]

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。
number	1 ～ 199 の範囲のコミュニティ リスト番号。
name	コミュニティ リストの名前。
exact-match	（オプション）完全一致を持つルートだけを表示します。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast community-list コマンドの出力は show ip bgp community-list コマンドと類似しています。

例

次に、コミュニティリスト番号 3 に対する show ipv6 bgp community-list コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64      2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80    2001:0DB8:0:3::1                         0 1 i
```

```
*> 2001:0DB8:0:2::1/64      ::                                    0 32768 i
*> 2001:0DB8:0:2:1::/80     ::                                    0 32768 ?
* 2001:0DB8:0:3::2/64       2001:0DB8:0:3::1                         0 1 ?
*>                        ::                                  0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                    0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                         0 1 ?
```

次の表で、この出力に表示される重要なフィールドについて説明します。

表 *13 : show bgp ipv6 community-list* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。

フィールド	説明
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 filter-list

指定した IPv6 フィルタ リストと一致するルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp ipv6 filter-list コマンドを使用します。

show bgp ipv6 unicast filter-list *access-list-number*

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。
>*access-list-number*	IPv6 自律システム パス アクセス リストの数。1 ～ 199 の範囲の数を指定できます。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 filter-list コマンドの出力は show ip bgp filter-list コマンドと類似しています。

次に例を示します。

次に、IPv6 自律システム パス アクセス リスト番号 1 に対する show bgp ipv6 filter-list コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast filter-list 1
BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network             Next Hop                            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
```

```
*                           2001:0DB8:0:4::2                        0 2 1 ?
*> 2001:0DB8:0:6::1/64      ::                                        32768  i
*> 2030::/64                2001:0DB8:0:4::2                        0 1
*> 2040::/64                2001:0DB8:0:4::2                        0 2 1 ?
*> 2050::/64                2001:0DB8:0:4::2                        0 2 1 ?
Table below describes the significant fields shown in the display.
```

表 *14 : show bgp ipv6 community-list* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。

フィールド	説明
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 inconsistent-as

送信元に一貫性のない複数の自律システムを含む IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp ipv6 inconsistent-as を使用します。

show bgp ipv6 unicast inconsistent-as

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast inconsistent-as コマンドの出力は show ip bgp inconsistent-as コマンドと類似しています。

例

次に、show bgp ipv6 inconsistent-as コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast inconsistent-as
BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                       0 1251 4270 10318 ?
*                   3FFE:3600::A                          0 3462 6175 ?
*                   3FFE:700:20:1::11                     0 293 6175 ?表 15 : show bgp
 ipv6 community-list のフィールド below describes the significant fields shown in the
display.
```

表 *15 : show bgp ipv6 community-list* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 neighbors

ネイバーへの IPv6 Border Gateway Protocol（BGP）接続に関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 neighbors** コマンドを使用します。

show bgp ipv6 unicast neighbors [*ipv6-address*] [**received-routes | routes | advertised-routes | paths** *regular-expression*]

構文の説明

unicast	*IPv6* ユニキャスト アドレス プレフィックスを指定します。
ipv6-address	（オプション）IPv6 BGP スピーキング ネイバーのアドレス。この引数を省略した場合、すべての IPv6 ネイバーが表示されます。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
ルート	（オプション）受信され、受け入れられるすべてのルートを表示します。これは **received-routes** キーワードの出力のサブセットです。
advertised-routes	（オプション）ネイバーにアドバタイズされているネットワーキング デバイスのすべてのルートを表示します。
paths *regular-expression*	（オプション）受信したパスの照合に使用される正規表現。

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、ユーザー 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
9.3(2)	This **command was added.**

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast neighbors** コマンドの出力は **show ip bgp neighbors** コマンドと類似しています。

例

次に、**show bgp ipv6 neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *16 : show bgp ipv6 community-list* のフィールド

フィールド	説明
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。ネイバーがルータと同じ自律システム内にある場合、これらの間のリンクは内部となり、そうでない場合は外部リンクと見なされます。
remote AS	ネイバーの自律システム。
internal link	このピアが内部ボーダー ゲートウェイ プロトコル（iBGP）ピアであることを示します。
BGP version	リモート ルータとの通信に使用される BGP バージョン。ネイバーのルータ ID（IP アドレス）も指定されます。
remote router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
BGP state	この BGP 接続の内部ステート。
up for	ベースとなる TCP 接続が存在している時間。
Last read	BGP がこのネイバーから最後にメッセージを読み取った時間。
hold time	ピアからのメッセージ間の最大経過時間。
keepalive interval	TCP 接続が維持されていることを確認できるように、キープアライブ パケットを送信する時間間隔。
Neighbor capabilities	このネイバーからアドバタイズされ受信される BGP 機能。
Route refresh	ルート リフレッシュ機能を使用してネイバーがダイナミック ソフト リセットをサポートすることを示します。
Address family IPv6 Unicast	BGP ピアが IPv6 到達可能性情報を交換していることを示します。
Received	このピアから受信した、キープアライブを含む BGP メッセージの合計数。
通知	ピアから受信したエラー メッセージの数。
Sent	このピアに送信された、キープアライブを含む BGP メッセージの合計数。
通知	ルータがこのピアに送信したエラー メッセージの数。
advertisement runs	最小アドバタイズメント間隔の値。
For address family	後続のフィールドが参照するアドレスファミリ。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
neighbor version	送信済みのプレフィックスおよびこのネイバーに送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。
Route refresh request	このネイバーで送受信されるルート リフレッシュ要求の数。.
Community attribute（出力例になし）	neighbor send-community コマンドがこのネイバー用に設定されている場合に表示されます。.
Inbound path policy（出力例になし）	インバウンドフィルタリストまたはルートマップが設定されているかどうかを示します。
Outbound path policy（出力例になし）	アウトバウンド フィルタ リスト、ルート マップ、または抑制マップが設定されているかどうかを示します。
bgp-in（出力例になし）	IPv6ユニキャストアドレス ファミリのインバウンドアップデート プレフィックス フィルタ リストの名前。
aggregate（出力例になし）	IPv6 ユニキャスト アドレス ファミリのアウトバウンド アップデート プレフィックス フィルタ リストの名前。
uni-out（出力例になし）	IPv6 ユニキャスト アドレス ファミリのアウトバウンド ルートマップの名前。
accepted prefixes	受け入れられたプレフィックスの数。
Prefix advertised	アドバタイズされたプレフィックスの数。
suppressed	抑制されたプレフィックスの数。
withdrawn	取り消されたプレフィックスの数。
history paths（出力例になし）	履歴を記憶するために保持されるパス エントリの数。
Connections established	ルータが TCP 接続を確立し、2 つのピアが相互に BGP 通信を行うことに同意した回数。
dropped	良好な接続に失敗したか、ダウンした回数。
Last reset	このピアリング セッションが最後にリセットされてからの経過時間（時:分:秒形式）。
Connection state	BGP ピアの状態。

フィールド	説明
unread input bytes	処理待ちのパケットのバイト数。
Local host、Local port	ローカル ルータおよびポートのピア アドレス。
Foreign host, Foreign port	ネイバーのピア アドレス。
Event Timers	各タイマーの開始とウェイク アップの回数を表示する表。
snduna	ローカル ホストが送信したものの、確認応答を受信していない最後の送信シーケンス番号。
sndnxt	ローカル ホストが次に送信するシーケンス番号。
sndwnd	リモート ホストの TCP ウィンドウ サイズ。
irs	最初の受信シーケンス番号。
rcvnxt	ローカル ホストが確認応答した最後の受信シーケンス番号。
rcvwnd	ローカル ホストの TCP ウィンドウ サイズ。
delrecvwnd	遅延受信ウィンドウ：ローカル ホストによって接続から読み取られ、ホストがリモート ホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT	計算されたスムーズラウンドトリップ タイムアウト（ミリ秒単位）。
RTTO	ラウンドトリップ タイムアウト（ミリ秒単位）。
RTV	ラウンドトリップ時間の差異（ミリ秒単位）。
KRTT	Karn アルゴリズムを使用した新しいラウンドトリップ タイムアウト（ミリ秒単位）。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT	計算に組み込み値を使用して記録された最小ラウンドトリップ タイムアウト（ミリ秒単位）。
maxRTT	記録された最大ラウンドトリップタイムアウト（ミリ秒単位）。
ACK hold	データを「ピギーバックする」ためにローカル ホストが確認応答を遅延させる時間（ミリ秒単位）。
Flags	BGP パケットの IP プレシデンス。
Datagrams: Rcvd	ネイバーから受信したアップデート パケットの数。

フィールド	説明
with data	データとともに受信したアップデート パケットの数。
total data bytes	データのバイト総数。
Sent	送信されたアップデートパケットの数。
with data	データとともに送信されたアップデート パケットの数。
total data bytes	データのバイト総数。

次に、**advertised-routes** キーワードを指定した **show bgp ipv6 neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

b

次に、**routes** キーワードを指定した **show bgp ipv6 neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
Table below describes the significant fields shown in the display.
```

表 17 : show bgp ipv6 neighbors advertised-routes と routes のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

次に、**paths** キーワードを指定した **show bgp ipv6 neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
The table below describes the significant fields shown in the display.
```

show bgp ipv6 neighbors paths のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

次に、**show bgp ipv6 neighbors** コマンドの出力例を示します。ここでは、IPv6 アドレス 2000:0:0:4::2 の受信ルートを示しています。

```
ciscoasa# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
Network               Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                        0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                        0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                        0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                        0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                        0 2 ?
```

show bgp ipv6 paths

データベース内のすべての IPv6 Border Gateway Protocol（BGP）パスを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 paths** コマンドを使用します。

show bgp ipv6 unicast paths *regular-expression*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
regular-expression	データベース内の受信パスの照合に使用される正規表現。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast paths** コマンドの出力は **show ip bgp paths** コマンドと類似しています。

例

次に、**show bgp ipv6 paths** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
```

```
0x6132245C   46        1      0 6346 8664 4927 i
Table below describes the significant fields shown in the display.
```

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

show bgp ipv6 prefix-list

プレフィックスリストに一致するルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 prefix-list** コマンドを使用します。

show bgp ipv6 unicast prefix-list *name*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
name	指定したプレフィックス リスト。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

指定するプレフィックス リストは、IPv4 プレフィックス リストと同様の形式の IPv6 プレフィックス リストである必要があります。

例

```
The following is sample output from the show bgp ipv6 prefix-list
command:
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
Table below describes the significant fields shown in the display.
```

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 quote-regexp

自律システム パスの正規表現に一致する IPv6 Border Gateway Protocol（BGP）ルートを引用符で囲まれた文字列として表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 quote-regexp** コマンドを使用します。

show bgp ipv6 unicast quote-regexp 正規表現

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
正規表現	BGP 自律システム パスと一致させるために使用される正規表現。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast quote-regexp** コマンドの出力は **show ip bgp quote-regexp** コマンドと類似しています。

例

次に、**show bgp ipv6 quote-regexp** コマンドの出力例を示します。ここでは、33 で始まるパスまたは 293 を含むパスを示しています。

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
```

```
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
* 3FFE:C00:E:F::2                        0 6389 1849 293 1275
Table below describes the significant fields shown in the display.
```

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 regexp

自律システム パスの正規表現に一致する IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 regexp** コマンドを使用します。

show bgp ipv6 unicast regexp *regular-expression*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
regular-expression	BGP 自律システム パスと一致させるために使用される正規表現。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast regexp** コマンドの出力は **show ip bgp regexp** コマンドと類似しています。

例

次に、**show bgp ipv6 regexp** コマンドの出力例を示します。ここでは、33 で始まるパスまたは 293 を含むパスを示しています。

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
```

```
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
Table below describes the significant fields shown in the display.
```

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 route-map

ルーティング テーブルへの登録に失敗した IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 route-map** コマンドを使用します。

show bgp ipv6 unicast route-map *name*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
name	照合のために指定したルート マップ。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

次に、rmap という名前のルートマップに対する **show bgp ipv6 route-map** コマンドの出力例を示します。

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1         0    100     50 ?
*>i543::/64         2001:0DB8:101::1         0    100     50 ?
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 summary

すべての IPv6 Border Gateway Protocol（BGP）接続のステータスを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show bgp ipv6 summary** コマンドを使用します。

show bgp ipv6 unicast summary

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。

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、ユーザー 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
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast summary** コマンドの出力は **show ip bgp summary** コマンドと類似しています。

例

次に、**show bgp ipv6 summary** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP device identifier	ネットワーキング デバイスの IP アドレス。
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。

フィールド	説明
main routing table version	メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。
Neighbor	ネイバーの IPv6 アドレス。
V	ネイバーに通知される BGP バージョン番号。
AS	Autonomous System
MsgRcvd	ネイバーから受信された BGP メッセージ。
MsgSent	ネイバーに送信された BGP メッセージ。
TblVer	ネイバーに送信された BGP データベースの最後のバージョン。
InQ	処理を待機しているネイバーからのメッセージの数。
OutQ	ネイバーへの送信を待機しているメッセージの数。
Up/Down	BGP セッションが確立状態となったか、確立されていない場合は現在の状態になった時間の長さ。
State/PfxRcd	BGP セッションの現在の状態/デバイスがネイバーから受信したプレフィックスの数。最大数（**neighbor maximum-prefix** コマンドで設定）に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルになります。 アイドル ステータスの（管理者）エントリは、接続が **neighbor shutdown** コマンドを使用してシャットダウンされたことを示します。

show bgp neighbors

ネイバーへの Border Gateway Protocol（BGP）接続および TCP 接続に関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp neighbors コマンドを使用します。

show bgp neighbors ［ **slow** | *ip-address* ［ **advertised-routes | | paths** ［ *reg-exp* **| policy** ［ **detail** ］ | **received prefix-filter | received-routes | routes** ］］

構文の説明

slow	（オプション）ダイナミックに設定された低速ピアに関する情報を表示します。
ip-address	（オプション）IPv4 ネイバーに関する情報を表示します。この引数を省略すると、すべてのネイバーに関する情報が表示されます。
advertised-routes	（オプション）ネイバーにアドバタイズされたすべてのルートを表示します。
paths reg-exp	（オプション）指定したネイバーから学習した自律システムパスを表示します。オプションの正規表現を使用して、出力をフィルタ処理できます。
ポリシー	（オプション）アドレス ファミリごとに、このネイバーに適用されるポリシーを表示します。
detail	（オプション）ルート マップ、プレフィックス リスト、コミュニティ リスト、アクセス コントロール リスト（ACL）、自律システム パス フィルタ リストなどの詳細なポリシー情報を表示します。
received prefix-filter	（オプション）指定したネイバーから送信されたプレフィックス リスト（アウトバウンド ルート フィルタ（ORF））を表示します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
routes	（オプション）受信され、受け入れられるすべてのルートを表示します。このキーワードが入力されたときに表示される出力は、received-routes キーワードによって表示される出力のサブセットです。

コマンド デフォルト

このコマンドの出力には、すべてのネイバーの情報が表示されます。

コマンド 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、ユーザー 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
9.2(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

ネイバーセッションの BGP および TCP 接続情報を表示するには、show bgp neighbors コマンドを使用します。BGPの場合、これには詳細なネイバー属性、機能、パス、およびプレフィックス情報が含まれています。TCP の場合、これには BGP ネイバー セッション確立およびメンテナンスに関連した統計が含まれています。

アドバタイズされ、取り消されたプレフィックスの数に基づいて、プレフィックスアクティビティが表示されます。ポリシー拒否には、アドバタイズされたものの、その後、出力に表示されている機能または属性に基づいて無視されたルートの数が表示されます。

シスコが採用している4バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドに続けて、clear bgp * コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

例

出力例は、show bgp neighbors コマンドで使用できるさまざまなキーワードによって異なります。以降のセクションでは、さまざまなキーワードの使用例を示します。

show bgp neighbors：例

次に、10.108.50.2 の BGP ネイバーの出力例を示します。このネイバーは、内部 BGP（iBGP）ピアです。ルート更新とグレースフル リスタート機能をサポートしています。

```
ciscoasa# show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
```

```
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

次の表で、この出力に表示される重要なフィールドを説明します。アスタリスク文字（*）の後ろにあるフィールドは、カウンタが非ゼロ値の場合だけ表示されます。

表 10 : show bgp ipv4 のフィールド に、各フィールドの説明を示します。

表 *18 : show bgp ipv4* のフィールド

フィールド	説明
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。
remote AS	ネイバーの自律システム番号。
local AS 300 no-prepend（出力には表示されない）	ローカルの自律システム番号が受信された外部ルートの先頭に付加されていないことを確認します。この出力は、自律システムを移行しているときのローカル自律システムの非表示をサポートします。
internal link	iBGP ネイバーの場合「internal link」と表示されます。外部 BGP（eBGP）ネイバーの場合は「external link」と表示されます。
BGP version	リモート ルータとの通信に使用される BGP バージョン。
remote router ID	ネイバーの IP アドレス。
BGP state	セッション ネゴシエーションの有限状態マシン（FSM）ステージ。
up for	ベースとなる TCP 接続が存在している時間（hhmmss 形式）。
Last read	BGP がこのネイバーから最後にメッセージを受信してからの時間（hhmmss 形式）。
last write	BGP がこのネイバーに最後にメッセージを送信してからの時間（hhmmss 形式）。
hold time	BGP がメッセージを受信せずにこのネイバーとセッションを維持した時間（秒数）。
keepalive interval	キープアライブ メッセージがこのネイバーに転送される間隔（秒数）。
Neighbor capabilities	このネイバーからアドバタイズされ受信される BGP 機能。2 つのルータ間で機能が正常に交換されている場合、「advertised and received」が表示されます。
Route Refresh	ルート リフレッシュ機能のステータス。
Graceful Restart Capability	グレースフル リスタート機能のステータス。
Address family IPv4 Unicast	このネイバーの IP Version 4 ユニキャスト固有プロパティ。
Message statistics	メッセージ タイプごとにまとめられた統計。

フィールド	説明
InQ depth is	入力キュー内のメッセージ数。
OutQ depth is	出力キュー内のメッセージ数。
Sent	送信されたメッセージの合計数。
Received	受信されたメッセージの合計数。
Opens	送受信されたオープンメッセージ数。
通知	送受信された通知（エラー）メッセージ数。
Updates	送受信されたアップデートメッセージ数。
Keepalives	送受信されたキープアライブメッセージ数。
Route Refresh	送受信されたルートリフレッシュ要求メッセージ数。
Total	送受信されたメッセージの合計数。
Default minimum time between...	アドバタイズメント送信の間の時間（秒数）。
For address family:	後続のフィールドが参照するアドレスファミリ。
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
neighbor version	送信済みのプレフィックスおよび送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。
update-group	このアドレスファミリのアップデートグループメンバーの数。
Prefix activity	このアドレスファミリのプレフィックス統計。
Prefixes current	このアドレスファミリに対して受け入れられるプレフィックス数。
Prefixes total	受信されたプレフィックスの合計数。
Implicit Withdraw	プレフィックスが取り消されて再アドバタイズされた回数。
Explicit Withdraw	フィージブルでなくなったため、プレフィックスが取り消された回数。
Used as bestpath	最適パスとしてインストールされた受信プレフィックス数。
Used as multipath	マルチパスとしてインストールされた受信プレフィックス数。

フィールド	説明
* Saved（ソフト再構成）	ソフト再構成をサポートするネイバーで実行されたソフトリセットの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
* History paths	このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
* Invalid paths	無効なパスの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
Local Policy Denied Prefixes	ローカルポリシー設定が原因で拒否されたプレフィックス。カウンタは、インバウンドおよびアウトバウンドのポリシー拒否ごとに更新されます。この見出しの下のフィールドは、カウンタの値がゼロ以外である場合にだけ表示されます。
* route-map	インバウンドおよびアウトバウンドのルートマップポリシー拒否を表示します。
* filter-list	インバウンドおよびアウトバウンドのフィルタリストポリシー拒否を表示します。
* prefix-list	インバウンドおよびアウトバウンドのプレフィックスリストポリシー拒否を表示します。
* AS_PATH too long	アウトバウンドの AS パス長ポリシー拒否を表示します。
* AS_PATH loop	アウトバウンドの AS パス ループ ポリシー拒否を表示します。
* AS_PATH confed info	アウトバウンド コンフェデレーション ポリシー拒否を表示します。
* AS_PATH contains AS 0	自律システム（AS）0 のアウトバウンド拒否を表示します。
* NEXT_HOP Martian	アウトバウンドの Martian 拒否を表示します。
* NEXT_HOP non-local	アウトバウンドの非ローカル ネクスト ホップ拒否を表示します。
* NEXT_HOP is us	アウトバウンドのネクストホップ自身の拒否を表示します。
* CLUSTER_LIST loop	アウトバウンドのクラスタリスト ループ拒否を表示します。
* ORIGINATOR loop	ローカルで発信されたルートのアウトバウンド拒否を表示します。
* unsuppress-map	抑制マップによるインバウンド拒否を表示します。
* advertise-map	アドバタイズ マップによるインバウンド拒否を表示します。

フィールド	説明
* Well-known Community	ウェルノウンコミュニティのインバウンド拒否を表示します。
* SOO loop	site-of-origin によるインバウンド拒否を表示します。
* Bestpath from this peer	最適パスがローカルルータから提供されたことによるインバウンド拒否を表示します。
* Suppressed due to dampening	ネイバーまたはリンクがダンプニング状態であることによるインバウンド拒否を表示します。
* Bestpath from iBGP peer	最適パスが iBGP ネイバーから提供されたことによるインバウンド拒否を表示します。
* Incorrect RIB for CE	CEルータのRIBエラーによるインバウンド拒否を表示します。
* BGP distribute-list	配布リストによるインバウンド拒否を表示します。
Number of NLRIs...	アップデート内のネットワーク層到達可能性属性の数。
Connections established	TCP および BGP 接続が正常に確立した回数。
dropped	有効セッションに障害が発生したか停止した回数。
Last reset	このピアリング セッションが最後にリセットされてからの時間。リセットがこの行に表示された理由。
External BGP neighbor may be...（出力には表示されない）	BGP TTL セキュリティ チェックがイネーブルであることを示します。ローカルピアとリモートピアをまたぐことができるホップの最大数がこの行に表示されます。
Connection state	BGP ピアの接続ステータス。
Connection is ECN Disabled	明示的輻輳通知のステータス（イネーブルまたはディセーブル）。
Local host: 10.108.50.1, Local port: 179	ローカルBGPスピーカーのIPアドレス。BGPポート番号179。
Foreign host: 10.108.50.2, Foreign port: 42698	ネイバーアドレスと BGP 宛先ポート番号。
Enqueued packets for retransmit:	TCP によって再送信のためにキューに格納されたパケット。
Event Timers	TCPイベントタイマー。起動およびウェイクアップのカウンタが提供されます（期限切れタイマー）。
Retrans	パケットを再送信した回数。
TimeWait	再送信タイマーが期限切れになるまで待機する時間。

フィールド	説明
AckHold	確認応答ホールドタイマー
SendWnd	伝送（送信）ウィンドウ。
KeepAlive	キープアライブパケットの数。
GiveUp	確認応答がないためにパケットがドロップされた回数。
PmtuAger	パス MTU ディスカバリ タイマー。
DeadWait	デッドセグメントの有効期限タイマー。
iss:	初期パケット送信シーケンス番号。
snduna	確認応答されなかった最後の送信シーケンス番号。
sndnxt:	次に送信されるパケットのシーケンス番号。
sndwnd:	リモートネイバーの TCP ウィンドウ サイズ。
irs:	初期パケット受信シーケンス番号。
rcvnxt:	ローカルに確認応答された最後の受信シーケンス番号。
rcvwnd:	ローカルホストの TCP ウィンドウサイズ。
delrcvwnd:	遅延受信ウィンドウ：ローカルホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT:	計算されたスムーズ ラウンドトリップ タイムアウト。
RTTO:	ラウンドトリップ タイムアウト。
RTV:	ラウンドトリップ時間の差異。
KRTT:	新しいラウンドトリップ タイムアウト（Karn アルゴリズムを使用）。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT:	記録された最小ラウンドトリップ タイムアウト（計算に使用される組み込み値）。
maxRTT:	記録された最大ラウンドトリップ タイムアウト。
ACK hold:	ローカルホストが追加データを伝送（ピギーバック）するために確認応答を遅らせる時間の長さ。

フィールド	説明
IP Precedence value:	BGP パケットの IP プレシデンス。
Datagrams	ネイバーから受信したアップデートパケットの数。
Rcvd:	受信パケット数。
with data	データとともに送信されたアップデートパケットの数。
total data bytes	受信データの合計量（バイト）。
Sent	送信されたアップデートパケットの数。
Second Congestion	輻輳による再送信に要した秒数。
Datagrams: Rcvd	ネイバーから受信したアップデートパケットの数。
out of order:	シーケンスを外れて受信したパケットの数。
with data	データとともに受信したアップデート パケットの数。
Last reset	このピアリングセッションが最後にリセットされてからの経過時間。
unread input bytes	処理待ちのパケットのバイト数。
retransmit	再送信されたパケット数。
fastretransmit	再送信タイマーが期限切れになる前に、順序が不正なセグメントのために再送信された重複する確認応答の数。
partialack	部分的な確認応答（後続の確認応答がない、またはそれ以前の送信）のために再送信された回数。

show bgp neighbors advertised-routes：例

次に、172.16.232.178 ネイバーのみにアドバタイズされたルートを表示する例を示します。

```
ciscoasa# show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

表 19 : show bgp neighbors advertised routes のフィールド に、各フィールドの説明を示します。

表 *19 : show bgp neighbors advertised routes* のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバーにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	設定済の local-preference route-map コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、network ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

例

show bgp neighbors paths：例

次に、paths キーワードを指定した show bgp neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp neighbors 172.29.232.178 paths ^10
Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

表 20 : show bgp neighbors paths のフィールド に、各フィールドの説明を示します。

表 *20 : show bgp neighbors paths* のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
パス	そのルートの自律システム パスと、そのルートの発信元コード。

例

show bgp neighbors received prefix-filter：例

次の例は、10.0.0.0 ネットワークのすべてのルートをフィルタリングするプレフィックス リストが 192.168.20.72 ネイバーから受信されたことを示しています。

```
ciscoasa# show bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

表 21 : show bgp neighbors received prefix filter のフィールド に、各フィールドの説明を示します。

表 *21 : show bgp neighbors received prefix filter* のフィールド

フィールド	説明
Address family	プレフィックスフィルタが受信されるアドレスファミリモード。
ip prefix-list	指定したネイバーから送信されたプレフィックスリスト。

例

show bgp neighbors policy：例

次の出力例に表示されているのは、192.168.1.2 にあるネイバーに適用されたポリシーです。ネイバー デバイスで設定されたポリシーが表示されます。

```
ciscoasa# show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

show bgp neighbors：例

次に、show bgp neighbors コマンドの出力例を示します。ここでは、BGP TCP パス最大伝送ユニット（MTU）ディスカバリが 172.16.1.2 にある BGP ネイバーに対して有効になっていることを確認しています。

```
ciscoasa# show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

次に、show bgp neighbors コマンドの出力の一部を示します。ここでは、192.168.3.2 にある外部 BGP ピアに対する BGP グレースフルリスタート機能のステータスを確認し

ています。グレースフル リスタートは、この BGP ピアに対してディセーブルである と示されています。

```
ciscoasa# show bgp neighbors 192.168.3.2
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

show bgp paths

データベース内のすべての BGP パスを表示するには、EXEC モードで show bgp paths コマンドを使用します。

show bgp paths
Cisco 10000 Series Router
show bgp paths *regexp*

構文の説明

regexp	BGP 自律システム パスと一致する正規表現。

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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの show bgp paths コマンドの出力例を示します。

```
ciscoasa# show bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

表 22 : show bgp paths のフィールド に、各フィールドの説明を示します。

表 *22 : show bgp paths* のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Hash	パスが格納されているハッシュ バケット。

フィールド	説明
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

show bgp policy-list

設定されたポリシーリストとポリシーリストエントリに関する情報を表示するには、ユーザー EXEC モードで show bgp policy-list コマンドを使用します。

show bgp policy-list [*policy-list-name*]

構文の説明

policy-list-name	（オプション）この引数を使用して指定したポリシー リストに関する情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、show bgp policy-list コマンドの出力例を示します。このコマンドの出力には、ポリシー リスト名と設定された match 句が表示されます。次の出力例は、表示される出力に類似しています。

```
ciscoasa# show bgp policy-list
policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show bgp prefix-list

プレフィックスリストまたはプレフィックス リスト エントリに関する情報を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp prefix-list コマンドを使用します。

show bgp prefix-list [**detail | summary**] [*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer|first-match**]]]

構文の説明

detail | summary	（オプション）すべてのプレフィックス リストに関する詳細情報または要約情報を表示します。
first-match	（任意）指定した network/length と一致する、指定したプレフィックスリストの最初のエントリを表示します。
longer	（任意）指定した network/length と一致するか、またはより限定的な、プレフィックスリストのすべてのエントリを表示します。
network/length	（オプション）このネットワーク アドレスおよびネットマスク長（ビット単位）を使用する、指定したプレフィックス リストのすべてのエントリを表示します。
prefix-list-name	（オプション）特定のプレフィックス リストのエントリを表示します。
seq sequence-number	（オプション）指定したプレフィックス リストに指定したシーケンス番号があるプレフィックス リスト エントリだけを表示します。

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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、show bgp prefix-list コマンドの出力例を示します。ここでは、test という名前のプレフィックスリストの詳細を示しています。

```
ciscoasa# show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

自律システム パスの正規表現と一致するルートを表示するには、EXEC モードで show bgp regexp コマンドを使用します。

show bgp regexp *regexp*

構文の説明

regexp	BGP 自律システム パスと一致する正規表現。 自律システム番号の形式の詳細については、router bgp コマンドの説明を参照してください。

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、ユーザー 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
9.2(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

シスコが採用している4バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドに続けて、clear bgp * コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

円滑に移行するには、4 バイト自律システム番号を使用して指定されている自律システム内にあるすべてのBGPスピーカーで、4バイト自律システム番号をサポートするようアップグレードすることを推奨します。

例

次に、特権 EXEC モードでの show bgp regexp コマンドの出力例を示します。

```
Router# show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

bgp asnotation dot コマンドを設定すると、4 バイト自律システムパスの正規表現マッチング形式が asdot 表記形式に変更されます。4 バイト自律システム番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト自律システム番号だけがマッチングされます。1 つ目の例では、show bgp regexp コマンドは、asplain 形式で表された 4 バイト自律システム番号を使用して設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの自律システムパスに関する情報が asdot 表記法を使って表示されます。

（注） asdot 表記法では、シスコの正規表現で特殊文字であるピリオドを使用します。特殊な意味を削除するには、ピリオドの前にバックスラッシュを使用します。

```
Router# show bgp regexp ^65536$
Router# show bgp regexp ^1\.0$
BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

次に、bgp asnotation dot コマンドを入力した後の show bgp regexp コマンドの出力例を示します。ここでは、4 バイト自律システム番号を表示しています。

（注） asdot 表記法では、シスコの正規表現で特殊文字であるピリオドを使用します。特殊な意味を削除するには、ピリオドの前にバックスラッシュを使用します。

```
Router# show bgp regexp ^1\.14$
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

show bgp replication

Border Gateway Protocol（BGP）アップデートグループのアップデート複製統計情報を表示するには、EXEC モードで show bgp replication コマンドを使用します。

show bgp replication [*index-group* | *ip-address*]

構文の説明

index-group	（オプション）アップデート グループのアップデート複製統計情報を対応するインデックス番号とともに表示します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。
ip-address	（オプション）このネイバーのアップデート複製統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC、ユーザー 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
9.2(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

このコマンドの出力には、BGP アップデート グループ複製統計情報が表示されます。

アウトバウンドポリシーが変更された場合、ルータは、3 分間のタイマー期限が切れた後で、アウトバウンド ソフト リセットをトリガーすることにより、自動的にアップデート グループ メンバーシップを再計算し、変更を適用します。この動作は、ネットワーク オペレータがミスを犯した場合に、コンフィギュレーションを変更する時間を与えるように設計されています。タイマー期限が切れる前に、アウトバウンド ソフト リセットを手動で有効にするには、clearbgpip-addresssoft out コマンドを入力します。

例

次の show bgp replication コマンドの出力例には、すべてのネイバーのアップデート グループの複製情報が表示されます。

```
ciscoasa# show bgp replication
BGP Total Messages Formatted/Enqueued : 0/0
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
```

```
         2 internal        2        10.4.9.5        0        0      0      0
The following sample output from the show bgp replication command shows update-group
statistics for the 10.4.9.5 neighbor:
Router# show bgp replication 10.4.9.5
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2        10.4.9.5        0        0      0      0
```

表 23 : show bgp replication のフィールド に、各フィールドの説明を示します。

表 *23 : show bgp replication* のフィールド

フィールド	説明
Index	アップデート グループのインデックス番号。
タイプ	ピアのタイプ（内部または外部）。
Members	ダイナミック アップデート ピア グループ内のメンバーの数。
Leader	ダイナミック アップデート ピア グループの最初のメンバー。

show bgp rib-failure

ルーティング情報ベース（RIB）テーブルへの登録に失敗した Border Gateway Protocol（BGP）ルートを表示するには、特権 EXEC モードで show bgp rib-failure コマンドを使用します。

show bgp rib-failure

構文の説明

このコマンドにはキーワードまたは引数はありません。

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、ユーザー 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
9.2(1)	このコマンドが追加されました。

例

次に、show bgp rib-failure コマンドの出力例を示します。

```
ciscoasa# show bgp rib-failure
Network           Next Hop                    RIB-failure   RIB-NH Matches
10.1.15.0/24      10.1.35.5          Higher admin distance             n/a
10.1.16.0/24      10.1.15.1          Higher admin distance             n/a
```

表 24 : show bgp rib-failure のフィールド に、各フィールドの説明を示します。

表 *24 : show bgp rib-failure* のフィールド

フィールド	説明
ネットワーク	ネットワーク エンティティの IP アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。

フィールド	説明
RIB-failure	RIB 失敗の原因。アドミニストレイティブ ディスタンスが高いということは、スタティック ルートなど優れた（低い）アドミニストレーティブ ディスタンスを持つルートが IP ルーティング テーブルにすでにあることを意味します。
RIB-NH Matches	より高いアドミニストレイティブディスタンスが RIB-failure 列に表示され、使用されるアドレスファミリに対して bgp suppress-inactive が設定されている場合にだけ適用されるルートステータス。次の 3 種類があります。 • [Yes]：RIB のルートに BGP ルートと同じネクスト ホップがあるか、またはネクスト ホップが BGP ネクスト ホップと同じ隣接に再帰することを意味します。 • [No]：RIB のネクスト ホップが BGP ルートのネクスト ホップとは別に再帰することを意味します。 • [n/a]：使用されるアドレスファミリに対して bgp suppress-inactive が設定されないことを意味します。

show bgp summary

すべての Border Gateway Protocol（BGP）接続のステータスを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp summary コマンドを使用します。

show bgp summary

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、ユーザー 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
9.2(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 bgp summary コマンドは、BGP ネイバーへのすべての接続について BGP パス、プレフィックス、および属性情報を表示するために使用します。

プレフィックスは、IP アドレスとネットワーク マスクです。これはネットワーク全体、ネットワークのサブセット、または単一のホストルートを表すことができます。パスは、所定の宛先へのルートです。デフォルトでは、BGP は宛先ごとに 1 つのパスだけをインストールします。マルチパス ルートが設定されている場合、BGP は各マルチパス ルートにパス エントリをインストールし、1 つのマルチパス ルートにのみ最適パスとマークされます。

BGP 属性とキャッシュ エントリは個別にも組み合わせても表示され、これは最適パス選択プロセスに影響を与えます。この出力のフィールドは、関連する BGP 機能が設定されているか、または属性が受信されたときに表示されます。メモリ使用量はバイト単位で表示されます。

シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドに続けて、clear bgp * コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

例

次に、特権 EXEC モードでの show bgp summary コマンドの出力例を示します。

```
Router# show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

表 25 : show bgp summary のフィールド に、各フィールドの説明を示します。

表 *25 : show bgp summary* のフィールド

フィールド	説明
BGP router identifier	優先度とアベイラビリティの順序で、bgp router-id コマンドによって指定されたルータ ID、ループバックアドレス、または最上位 IP アドレス。
BGP table version	BGP データベースの内部バージョン番号。
main routing table version	メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。
...network entries	BGP データベースの一意のプレフィックス エントリの数。
...using ... bytes of memory	同じ行のパス、プレフィックス、または属性のエントリのために消費されているメモリ量（バイト単位）。
...path entries using	BGP データベースのパス エントリの数。単一のパス エントリだけが特定の宛先にインストールされます。マルチパス ルートが設定されている場合、マルチパス ルートごとにパス エントリがインストールされます。
...multipath network entries using	特定の宛先にインストールされているマルチパスエントリの数。
* ...BGP path/bestpath attribute entries using	パスが最適パスとして選択されている一意の BGP 属性の組み合わせの数。
* ...BGP rrinfo entries using	ORIGINATOR 属性と CLUSTER_LIST 属性の一意の組み合わせの数。

フィールド	説明
...BGP AS-PATH entries using	一意の AS_PATH エントリの数。
...BGP community entries using	BGP コミュニティ属性の一意の組み合わせの数。
*...BGP extended community entries using	拡張コミュニティ属性の一意の組み合わせの数。
BGP route-map cache entries using	BGP ルート マップの match 句と set 句の組み合わせの数。値が 0 の場合、ルート キャッシュが空であることを示します。
...BGP filter-list cache entries using	AS パス アクセス リストの permit ステートメントまたは deny ステートメントに一致するフィルタ リスト エントリの数。値が 0 の場合、フィルタ リスト キャッシュが空であることを示します。
BGP advertise-bit cache entries using	（Cisco IOS Release 12.4(11)T 以降のリリースだけ）アドバタイズされたビットフィールドエントリの数および関連するメモリ使用量。ビットフィールド エントリは、プレフィックスがピアにアドバタイズされるときに生成される情報（1 ビット）を表します。アドバタイズされたビット キャッシュは、必要に応じてダイナミックに作成されます。
...received paths for inbound soft reconfiguration	インバウンド ソフト再構成のために受信され保存されるパスの数。
BGP using...	BGPプロセスによって使用されるメモリの総量（バイト単位）。
Dampening enabled...	BGP ダンプニングがイネーブルであることを示します。この行には、累積ペナルティを伝送するパスの数およびダンプニングされたパスの数が表示されます。
BGP activity...	パスまたはプレフィックスに対してメモリが割り当てられたか、または解放された回数を表示します。
Neighbor	ネイバーの IP アドレス。
V	ネイバーに通知される BGP バージョン番号。
AS	自律システム（AS）番号。
MsgRcvd	ネイバーから受信されたメッセージ数。
MsgSent	ネイバーに送信されたメッセージ数。
TblVer	ネイバーに送信された BGP データベースの最終バージョン。
InQ	ネイバーで処理するためにキューに格納されたメッセージ数。

フィールド	説明
OutQ	ネイバーに送信するために、キューに格納されたメッセージ数。
Up/Down	BGP セッションが確立状態となったか、確立状態ではない場合は現在の状態になった時間の長さ。
State/PfxRcd	BGP セッションの現在の状態と、ネイバーまたはピア グループから受信されたプレフィックスの数。最大数（neighbor maximum-prefix コマンドで設定）に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルに設定されます。 アイドル ステータスの（管理者）エントリは、接続が neighbor shutdown コマンドを使用してシャットダウンされたことを示します。

例

show bgp summary コマンドの次の出力は、BGP ネイバー 192.168.3.2 がダイナミックに作成され、この受信範囲グループであるグループ 192 のメンバーであることを示します。この出力は、IP プレフィックス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲グループに定義されることも示します。Cisco IOS リリース 12.2(33)SXH 以降のリリースでは、BGP ダイナミックネイバー機能により、ピアグループ（受信範囲グループ）に関連付けられたサブネット範囲を使用してBGPネイバーピアのダイナミックな作成をサポートする機能が追加されました。

```
ciscoasa# show bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

show bgp summary コマンドの次の出力は、4 バイトの異なる自律システム番号（65536 および 65550）の 2 つの BGP ネイバー（192.168.1.2 および 192.168.3.2）を示しています。ローカルな自律システム 65538 は、4 バイト自律システム番号でもあり、その番号はデフォルトの asplain 形式で表示されます。

```
Router# show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

show bgp summary コマンドの次の出力は同じ 2 つの BGP ネイバーを示していますが、4 バイト自律システム番号は asdot 表記法の形式で表示されます。表示形式を変更するには、ルータ コンフィギュレーション モードで bgp asnotation dot コマンドを設定する必要があります。

```
Router# show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24      0
```

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

```
ciscoasa> show bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

show bgp system-config

ユーザーコンテキストでシステムコンテキストのbgpの実行コンフィギュレーションを表示するには、ユーザー EXEC モードまたは特権 EXEC モードで show bgp system-config コマンドを使用します。

show bgp system-config

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 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、ユーザー EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、引数またはキーワードを指定せずにユーザー コンテキストでだけ使用できます。このコマンドは、システム コンテキストによってユーザー コンテキストに対して適用される実行コンフィギュレーションを確認する場合に役立つことがあります。

例

次の出力例は、show bgp system-config コマンドをユーザー EXEC モードで入力すると表示される出力に類似しています。

```
ciscoasa/c1(config)# show bgp system-config
router bgp 1
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 no bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
 address-family ipv4 unicast
  bgp scan-time 0
```

```
 bgp nexthop trigger enable
 bgp nexthop trigger delay 5
exit-address-family
```

show blocks

パケットバッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [**core | export-failed | interface**] [{ **address** *hex* **| all | assigned | free | old | pool** *size* [**summary**]} [**diagnostics | dump | header | packet] | queue history |** [**exhaustion snapshot | history** [**list**] [*1-MAX_NUM_SNAPSHOT* | *index*] [**detail**]] [**depleted** *size*]

構文の説明

address *hex*	（任意）このアドレスに対応するブロックを 16 進数形式で表示します。
all	（任意）すべてのブロックを表示します。
assigned	（任意）割り当て済みでアプリケーションによって使用されているブロックを表示します。
core	（任意）コア固有のバッファを表示します。
depleted	（任意）指定されたブロックサイズに対して枯渇したブロックの詳細を表示します。有効なサイズは、0、4、80、256、1550、2560、2048、4096、8192、9344、16384、および 65536/65664 です。
detail	（任意）一意のキュー タイプごとに最初のブロックの一部（128 バイト）を表示します。
dump *。	（任意）ヘッダーとパケットの情報を含め、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（任意）ブロックの診断を表示します。
exhaustion snapshot	（オプション）取得されたスナップショットの最後の x 番号（x は現時点では 10）および最後のスナップショットのタイムスタンプを出力します。スナップショットが取得された後、5 分以上経過しないと別のスナップショットは取得されません。
export-failed	（任意）システムバッファ エクスポートの失敗カウンタを表示します。
free	（任意）使用可能なブロックを表示します。
header	（任意）ブロックのヘッダーを表示します。

history *1-MAX_NUM_SNAPSHOT* **history** *index* **history list**	**history** オプションは、最近のスナップショットと履歴内のすべてのスナップショットを表示します。 **history list** オプションは、履歴内のスナップショットの要約を表示します。 **history** *index* オプションは、履歴内のスナップショットのインデックスを表示します。 **history** *1-MAX_NUM_SNAPSHOT* オプションは、履歴内の 1 つのスナップショットだけを表示します。
interface	（任意）インターフェイスに付加されているバッファを表示します。
old *	（任意）1 分よりも前に割り当てられたブロックを表示します。
packet	（任意）ブロックのヘッダーおよびパケットの内容を表示します。
pool *size* *	（任意）特定のサイズのブロックを表示します。
queue history	（任意）ASA がブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。
summary	（任意）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

*これらのコマンドがスクリプトに統合され、短い間隔で実行されると、システムが過負荷になる可能性があります。そのため、これらのコマンドは、システムのキャパシティが負荷に耐えるものであることを確認してから使用してください。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。
8.0(2)	dupb ブロックは、4 バイト ブロックではなく長さが 0 のブロックを使用するようになりました。0 バイト ブロック用の 1 行が追加されました。
9.1(5)	**exhaustion snapshot** 、 **history list** 、 **history** *index*、 および **history** *1-MAX_NUM_SNAPSHOT* の各オプションが追加されました。
9.14(1)	**depleted** キーワードがコマンドに追加され、枯渇したブロックの詳細が表示されました。
9.16(2)	失敗数を含むようにこのコマンドの出力が拡張されました。

使用上のガイドライン

show blocks コマンドは、ASA が過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックが ASA 経由で伝送されている限り、メモリがいっぱいになっている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが伝送されているかどうかを確認できます。トラフィックが伝送されておらず、かつメモリがいっぱいになっている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の高基準値に関する、システム全体の情報およびコンテキスト固有の情報が含まれます。

出力の説明については、「例」を参照してください。

例

次に、シングルモードでの **show blocks** コマンドの出力例を示します。

```
ciscoasa# show blocks
  SIZE    MAX    LOW    CNT    FAILED
     0    100     99    100       0
     4   1600   1598   1599       0
    80    400    398    399       0
   256   3600   3540   3542       0
  1550   4716   3177   3184       0
 16384     10     10     10       0
  2048   1000   1000   1000       0
```

表 26 : show blocks のフィールドに、各フィールドの説明を示します。

表 *26 : show blocks* のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。

フィールド	説明
0	dupb ブロックで使用されます。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。またこのサイズのブロックは、通常、パケットをドライバに送信するコードなどで使用されます。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。
256	ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブな ASA は、パケットを生成してスタンバイ ASA に送信し、変換と接続のテーブルを更新します。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイ ASA に対して更新されなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイトブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、ASA の処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態を ASA が維持できない問題が発生します。 ASA から送信される syslog メッセージも 256 バイトブロックを使用しますが、256 バイトブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバーに記録していないことを確認してください。この情報は、ASA コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することを推奨します。
1550	ASA で処理するイーサネットパケットを格納するために使用されます。 パケットは、ASA インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。ASA は、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを発信インターフェイス上の出力キューに配置します。ASA がトラフィック負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT 列に示されます）。CNT 列が 0 の場合、ASA はより多くのブロックを割り当てようとします。このコマンドを実行すると、1550 バイト ブロックの最大数を 8192 より大きくすることができます。使用可能なブロックがなくなった場合、ASA はパケットをドロップします。

フィールド	説明
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御の更新に使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、ブロックの最大数は変化しません。例外は 256 バイト ブロックおよび 1550 バイト ブロックで、ASA は必要に応じてより多くのブロックをダイナミックに作成できます。このコマンドを実行すると、1550 バイト ブロックの最大数を 8192 より大きくすることができます。
LOW	低基準値。この数は、ASA の電源がオンになった時点、またはブロックが（**clear blocks** コマンドで）最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。 （注） この値を MAX にリセットするには、ASA をリブートする必要があります。
CNT	特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。
FAILED	ブロックサイズのメモリカウントが完全に使い果たされると（LOW で CNT 値がゼロ）、対応する FAILED 列は、その後受信した同じブロックサイズの割り当て要求の数で増加します。最終的に、メモリ領域が解放されると、割り当てに現在使用可能なブロックが増加し、FAILED 列の値が減少します。ただし、CNT と FAILED の値が増加した場合は、問題があることを示しているため解決する必要があります。

例

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

```
ciscoasa# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified
...
    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 27 : show blocks all のフィールド に、各フィールドの説明を示します。

表 *27 : show blocks all* のフィールド

フィールド	説明
ブロック（Block）	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。alloc、get、put、free の 4 つのいずれかです。
場所	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

例

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。マルチコンテキストモードでは、出力に、コンテキストによって現在使用されているブロックの数（INUSE）とコンテキストによって使用されているブロックの基準値（HIGH）に関する情報が含まれます。

```
ciscoasa/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

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

```
ciscoasa# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
```

```
      1     1 put                                   contexta
      1     1 put                                   contexta
      1     1 put                                   contextb
      1     1 put                                   contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb
Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                   contexta
     15     1 put                                   contexta
      1     1 put                                   contexta
      1     1 put                                   contextb
      1     1 put                                   contextc
...
```

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

```
ciscoasa# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                   contexta
     15     1 put                                   contexta
      1     1 put                                   contexta
      1     1 put                                   contextb
      1     1 put                                   contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                                   contexta
      1     1 put                                   contexta
      1     1 put                                   contexta
      1     1 put                                   contextb
      1     1 put                                   contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...
total_count: total buffers in this class
```

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

```
ciscoasa# show blocks pool 1550 summary
Class 3, size 1550
================================================
         total_count=1531    miss_count=0
Alloc_pc         valid_cnt       invalid_cnt
0x3b0a18         00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b         00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000
================================================
         total_count=9716    miss_count=0
Freed_pc         valid_cnt       invalid_cnt
0x9a81f3         00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326         00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2         00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue    valid_cnt       invalid_cnt
0x3b0a18         00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b         00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000
================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

次に、 **show blocks exhaustion history list** コマンドの出力例を示します。

```
ciscoasa# show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

表 28 : show blocks pool summary のフィールド に、各フィールドの説明を示します。

表 *28 : show blocks pool summary* のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリでレポートされなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。

フィールド	説明
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されて内容が無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

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

```
ciscoasa# show blocks depleted 8192

Block Class: 8,   Class Size: 8192,   Count: 100

1 Depletion created at 11:47:48 UTC Feb 17 2022

First Snapshot Details:

 Block             allocd_by          freed_by            alloccnt    dup_cnt  timestamp
    oper location

0x00007f117bd5f9c0 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd5d300 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd5ac40 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd58580 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd55ec0 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd53800 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd51140 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd4ea80 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd4c3c0 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b

0x00007f117bd49d00 0x0000560e84d1236b 0x0000560e822144e4     1           0     246610
        alloc 0x0000560e84d1236b
```

```
0x00007f117bd47640 0x0000560e84d1236b 0x0000560e822144e4     1          0      246610
        alloc 0x0000560e84d1236b

0x00007f117bd44f80 0x0000560e84d1236b 0x0000560e822144e4     1          0      246610
        alloc 0x0000560e84d1236b

0x00007f117bd428c0 0x0000560e84d1236b 0x0000560e822144e4     1          0      246610
        alloc 0x0000560e84d1236b

0x00007f117bd40200 0x0000560e84d1236b 0x0000560e822144e4     1          0      246610
        alloc 0x0000560e84d1236b

0x00007f117bd3db40 0x0000560e84d1236b 0x0000560e822144e4     1          0      246620
        alloc 0x0000560e84d1236b

0x00007f117bd3b480 0x0000560e84d1236b 0x0000560e822144e4     1          0      246620
        alloc 0x0000560e84d1236b

<--- More --->

0x00007f117bc85a40 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc83380 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc80cc0 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc7e600 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc7bf40 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc79880 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

<--- More --->

. . . . .
. . . . .

0x00007f117bc771c0 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc74b00 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc72440 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b

0x00007f117bc6fd80 0x0000560e84d1236b 0x0000560e822144e4     1          0      263390
        alloc 0x0000560e84d1236b
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられるメモリを増やします。
clear blocks	システム バッファの統計情報をクリアします。

コマンド	説明
show conn	アクティブな接続を表示します。

show bootvar

ブートファイルとコンフィギュレーションのプロパティを表示するには、特権EXECモードで **show bootvar** コマンドを使用します。

show bootvar

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定します。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ **boot system** コマンドと **boot config** コマンドで設定します。

例

BOOT 変数は disk0:/f1_image を保持しています。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:/f1_backupimage です。この値は、BOOT 変数が **boot system** コマンドで変更されているものの、実行コンフィギュレーションがまだ **write memory** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:/f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブートローダは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:1/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションを指します。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、**boot config** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、**boot config** コマンドで変更して、**write memory** コマンドで保存できます。

次に、**show bootvar** コマンドの出力例を示します。

```
ciscoasa# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show bridge-group

割り当てられたインターフェイス、MAC アドレス、IP アドレスなどブリッジグループ情報を表示するには、特権 EXEC モードで **show bridge-group** コマンドを使用します。

show bridge-group *bridge_group_number*

構文の説明

bridge_group_number ブリッジグループ番号を 1 ～ 100 の整数で指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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。
9.7(1)	ルーテッドモードでの Integrated Routing and Bridging のサポートが追加されました。

例

次に、IPv4 アドレスを指定した **show bridge-group** コマンドの出力例を示します。

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

次に、IPv4 アドレスと IPv6 アドレスを指定した **show bridge-group** コマンドの出力例を示します。

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
```

```
   2000:101::1, subnet is 2000:101::/64
   2000:102::1, subnet is 2000:102::/64
Static mac-address entries: 0
Dynamic mac-address entries: 2
```

関連コマンド

コマンド	説明
bridge-group	トランスペアレントファイアウォールインターフェイスをブリッジ グループにグループ化します。
clear configure interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定します。
interface bvi	ブリッジ仮想インターフェイスを作成します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
show running-config interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションを表示します。

show call-home

設定した Call Home 情報を表示するには、特権 EXEC モードで **show call-home** コマンドを使用します。

[**cluster exec**] **show call-home** [**alert-group | detail | events | mail-server | status | profile** { *profile_name* | **all** } | **statistics**]

構文の説明

alert-group	（任意）使用可能なアラート グループを表示します。
cluster exec	（任意）クラスタリング環境では、あるユニットで **show call-home** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
detail	（任意）Call Home コンフィギュレーションの詳細を表示します。
events	（任意）現在の検出されたイベントを表示します。
mail-server status	（任意）Call Home メール サーバーのステータス情報を表示します。
profile *profile _name* **all**	（任意）すべての既存プロファイルのコンフィギュレーション情報を表示します。
statistics	（任意）Call Home の統計情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。
9.1(3)	**show cluster history** コマンドおよび **show cluster info** コマンドの出力を含めるために、Smart Call Home メッセージの新しいタイプが追加されました。

例

次に、設定された Call Home 設定を表示する show call-home コマンドの出力例を示します。

```
ciscoasa# show call-homeCurrent Smart Call-Home settings:Smart Call-Home feature :
enableSmart Call-Home message's from address: from@example.comSmart Call-Home message's
 reply-to address: reply-to@example.comcontact person's email address:
example@example.comcontact person's phone: 111-222-3333street address: 1234 Any Street,
 Any city, Any state, 12345customer ID: ExampleCorpcontract ID: X123456789site ID:
SantaClaraMail-server[1]: Address: smtp.example.com Priority: 1Mail-server[2]: Address:
 192.168.0.1 Priority: 10Rate-limit: 60 message(s) per minute
Available alert groups:Keyword                 State
------------------------ -------
Syslog Enable
diagnostic Enableenvironmental Enableinventory Enableconfiguration Enablefirewall
Enabletroubleshooting Enablereport Enable
Profiles:Profile Name: CiscoTAC-1Profile Name: prof1Profile Name: prof2
```

次に、Call Home コンフィギュレーション情報の詳細を表示する show call-home detail コマンドの出力例を示します。

```
ciscoasa# show call-home detailDescription: Show smart call-home configuration in
detail.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:
Current Smart Call-Home settings:Smart Call-Home feature: enableSmart Call-Home message's
 from address: from@example.example.comSmart Call-Home message's reply-to address:
reply-to@example.example.comcontact person's email address: abc@example.comcontact
person's phone: 111-222-3333street address: 1234 Any Street, Any city, Any state,
12345customer ID: 111111contract ID: 123123site ID: SantaClaraMail-server[1]: Address:
example.example.com Priority: 1Mail-server[2]: Address: example.example.com Priority:
10Rate-limit: 60 message(s) per minute
Available alert groups:Keyword State------------------------ -------syslog Enablediagnostic
 Enableenvironmental Enableinventory Enableconfiguration Enablefirewall
Enabletroubleshooting Enablereport Enable
Profiles:
Profile Name: CiscoTAC-1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
 Limit: 3145728 BytesEmail address(es): anstage@cisco.comHTTP address(es):
https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity------------------------ ------------inventory n/a
Profile Name: prof1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
Limit: 3145728 BytesEmail address(es): example@example.comHTTP address(es):
https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a

Profile Name: prof2Profile status: ACTIVE Preferred Message Format: short-textMessage
Size Limit: 1048576 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a
```

次に、使用可能な Call Home イベントを表示する show call-home events コマンドの出力例を示します。

```
ciscoasa# show call-home eventsDescription: Show current detected events.Supported Modes:
 single mode and system context in multi mode, routed/transparent.Output:Active event
list:Event client alert-group severity active
```

```
(sec)------------------------------------------------------------------Configuration
Client configuration none 5Inventory inventory none 15
```

次に、使用可能な Call Home メール サーバーのステータスを表示する show call-home mail-server status コマンドの出力例を示します。

```
ciscoasa# show call-home mail-server statusDescription: Show smart call-home configuration,
 status, and statistics.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:Mail-server[1]: Address: example.example.com Priority: 1
[Available]Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

次に、使用可能なアラート グループを表示する show call-home alert-group コマンドの出力例を示します。

```
ciscoasa# show call-home alert-groupDescription: Show smart call-home alert-group
states.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:Available alert groups:Keyword State-----------------------
-------syslog Enablediagnostic Enableenvironmental Enableinventory Enableconfiguration
Enablefirewall Enabletroubleshooting Enablereport Enable
```

次に、show call-home profile profile-name | all コマンドの出力例と、すべての定義済みプロファイルおよびユーザー定義プロファイルに関する情報を示します。

```
ciscoasa# show call-home profile {profile-name
 | all}Description: Show smart call-home profile configuration.Supported Modes: single
mode and system context in multi mode, routed/transparent.Output:Profiles:
Profile Name: CiscoTAC-1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
 Limit: 3145728 BytesEmail address(es): anstage@cisco.comHTTP address(es):
https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity----------------------- ------------inventory n/a
Profile Name: prof1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
Limit: 3145728 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity----------------------- ------------configuration n/ainventory n/a

Profile Name: prof2Profile status: ACTIVE Preferred Message Format: short-textMessage
Size Limit: 1048576 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity----------------------- ------------configuration n/ainventory n/a
```

次に、Call Home の統計情報を表示する show call-home statistics コマンドの出力例を示します。

```
ciscoasa# show call-home statisticsDescription: Show smart call-home statistics.Supported
 Modes: single mode and system context in multi mode, routed/transparent.Output:Message
 Types Total Email HTTP-------------------- ---------------- ----------------
----------------Total Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1Tx Failed 5 4 1inventory 3 2 1configuration 2 2 0
Event Types Total-------------------- ----------------Total Detected 2inventory
1configuration 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

次に、Call Home の統計情報を表示する show call-home status コマンドの出力例を示します。

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.Supported Modes:
 single mode and system context in multi mode, routed/transparent.Output:Mail-server[1]:
 Address: kafan-lnx-01.cisco.com Priority: 1 [Available]Mail-server[2]: Address:
kafan-lnx-02.cisco.com Priority: 10 [Not Available]37. ciscoasa# show call-home events
Description: Show current detected events.Supported Modes: single mode and system context
 in multi mode, routed/transparent.Output:Active event list:Event client alert-group
severity active
(sec)-------------------------------------------------------------------Configuration
Client configuration none 5Inventory inventory none 15
```

次に、クラスタの Call Home の統計情報を表示する **cluster exec show call-home statistics** コマンドの出力例を示します。

```
ciscoasa(config)# cluster exec show call-home statistics
A(LOCAL):**********************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  3                3                0
                test                  3                3                0
 Total In-Delivering                  0                0                0
      Total In-Queue                  0                0                0
Total Dropped                         8                8                0
           Tx Failed                  8                8                0
       configuration                  2                2                0
                test                  6                6                0
Event Types             Total
--------------------   ----------------
      Total Detected                10
       configuration                 1
                test                 9
 Total In-Processing                 0
      Total In-Queue                 0
Total Dropped                        0
Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00
B:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0
 Total In-Delivering                  0                0                0
      Total In-Queue                  0                0                0
Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0
Event Types             Total
--------------------   ----------------
      Total Detected                 2
       configuration                 1
                test                 1
 Total In-Processing                 0
      Total In-Queue                 0
Total Dropped                        0
Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00
C:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  0                0                0
 Total In-Delivering                  0                0                0
```

```
      Total In-Queue                  0                 0                 0
Total Dropped                         2                 2                 0
          Tx Failed                   2                 2                 0
       configuration                  2                 2                 0
Event Types             Total
-------------------   ----------------
      Total Detected                  1
       configuration                  1
 Total In-Processing                  0
      Total In-Queue                  0
Total Dropped                         0
Last call-home message sent time: n/a
D:************************************************************************
Message Types           Total            Email             HTTP
-------------------   ---------------- ---------------- ----------------
       Total Success                  1                 1                 0
                test                  1                 1                 0
 Total In-Delivering                  0                 0                 0
      Total In-Queue                  0                 0                 0
Total Dropped                         2                 2                 0
          Tx Failed                   2                 2                 0
       configuration                  2                 2                 0
Event Types             Total
-------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1
 Total In-Processing                  0
      Total In-Queue                  0
Total Dropped                         0
Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。

show call-home registered-module status

登録されたモジュールのステータスを表示するには、特権 EXEC モードで **show call-home** registered-module status コマンドを使用します。

show call-home registered-module status [**all**]

（注） [**all**] オプションは、システム コンテキスト モードでのみ有効です。

構文の説明

all コンテキスト単位ではなく、デバイスに基づいてモジュール ステータスを表示します。マルチコンテキストモードでは、少なくとも 1 つのコンテキストでモジュールがイネーブルにされている場合、「**all**」オプションが含まれていれば、イネーブルにされていると表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

例

次に、**show call-home** registered-module status **all** の出力例を示します。

```
Output:
Module Name  Status
------------------------------------ --------------------Smart Call-Home
enabledFailover Standby/Active
```

関連コマンド

コマンド	説明
call-home	Call Home コンフィギュレーション モードを開始します。

コマンド	説明
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。

show capture

オプションを指定しない場合のキャプチャのコンフィギュレーションを表示するには、特権 EXEC モードで **show capture** コマンドを使用します。

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*] [**trace**]

構文の説明

access-list *access_list_name*	（任意）特定のアクセスリスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
capture_name	（オプション）パケット キャプチャの名前を指定します。
cluster exec	（任意）クラスタリング環境では、あるユニットで **show capture** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
count *number*	（任意）指定されたデータのパケット数を表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する ISAKMP データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。
detail	（任意）各パケットについて、プロトコル情報を追加表示します。
dump	（オプション）データ リンク経由で転送されたパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。
trace	各パケットの拡張トレース情報を表示します。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 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。
8.4(2)	IDS の出力に詳細情報が追加されました。
9.0(1)	**cluster exec** オプションが追加されました。
9.2(1)	出力で **vpn-user** ドメイン名が **filter-aaa** に変更されました。
9.3(1)	SGT およびイーサネット タギングの出力が追加されました。
9.10(1)	GRE の IP 復号化および IPinIP カプセル化のサポートが追加されました。
9.13(1)	asp-drop のキャプチャタイプ向けの show capture が拡張され、drop のロケーションの詳細が含まれるようになりました。
9.20(2)	物理ポートの show capture の詳細にドロップ設定（disable または mac-filter）が表示されます。

使用上のガイドライン

capture_name を指定した場合は、そのキャプチャのキャプチャバッファの内容が表示されます。

dump キーワードを指定しても、MAC 情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。通常、このコマンドは、ICMP、UDP、および TCP プロトコルの IP デコードをサポートします。バージョン 9.10（1）から、このコマンドは、ICMP、UDP、および TCP についての GRE および IPinIP カプセル化の IP デコード出力の表示をサポートするように拡張されています。

表 29 : パケット キャプチャの出力形式 で角カッコに囲まれている出力は、 **detail** キーワードを指定した場合に表示されます。

表 *29* : パケット キャプチャの出力形式

パケット タイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
『ARP』	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr* . *src-port dest-addr* . *dst-port* : [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr* . *src-port* d *est-addr* . *dst-port* : *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*

パケット タイプ	キャプチャの出力形式
IP/GRE	**ICMP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *ip-source > ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **UDP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **TCP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/IPinIP	**ICMP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: ip-source > ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **UDP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **TCP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr* : *ip-protocol ip-length*
その他	*HH:MM:SS.ms ether-hdr* : *hex-dump*

使用上のガイドライン

ASA が不正な形式の TCP ヘッダー付きのパケットを受信し、*invalid-tcp-hdr-length* という ASP ドロップ理由のためにそのパケットをドロップした場合、そのパケットを受信したインターフェイスでは **show capture** コマンドの出力にパケットが表示されません。

バージョン 9.13(1) 以降、show capture の出力が拡張され、トラブルシューティングを容易にするために、asp-drop のキャプチャタイプが表示されたときにドロップ位置情報が含まれるようになりました。ASP ドロップ カウンタを使用したトラブルシューティングでは、同じ理由による ASP ドロップがさまざまな場所で使用されている場合は特に、ドロップの正確な位置は不明です。この情報は、ドロップの根本原因を特定する上で重要です。この拡張機能を使用すると、ビルド ターゲット、ASA リリース番号、ハードウェア モデル、および ASLR メモリ テキスト領域などの ASP ドロップの詳細が表示されます（ドロップの位置のデコードが容易になります）。

例

次に、キャプチャのコンフィギュレーションを表示する例を示します。

```
ciscoasa(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次に、ARP キャプチャによってキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

次に、クラスタリング環境の 1 つのユニットでキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

次に、クラスタリング環境のすべてのユニットでキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# cluster exec
            show capture
mycapture (LOCAL):------------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
yourcapture:------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

次に、次のコマンドを入力した後でクラスタリング環境のクラスタ制御リンクでキャプチャされたパケットの例を示します。

```
ciscoasa (config)# capture a interface cluster
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet 0/0
ciscoasa(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

次に、SGT とイーサネット タギングがインターフェイスでイネーブルになっている場合にキャプチャされたパケットの例を示します。

```
ciscoasa(config)# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

SGT とイーサネットタギングがインターフェイスでイネーブルの場合、インターフェイスは引き続きタグ付きパケットまたはタグなしパケットを受信できます。この例は、出力に INLINE-TAG 36 があるタグ付きパケット用です。同じインターフェイスがタグなしパケットを受信した場合も、出力は変わりません（つまり、「INLINE-TAG 36」エントリは出力に含まれません）。

次に、パケットトレーサによって生成される GRE、IPinIP、およびその他のパケット、およびインターフェイス内の後続のキャプチャ出力の例を示します。

GRE パケット：

```
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

IPinIP パケット：

```
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

通常の tcp/udp/icmp パケット：

```
packet-tracer input inside tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside icmp 1.1.1.1 8 0 2.2.2.2


ciscoasa(config)# show capture inside
12:10:37.523746       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80: S
2145492151:2145492151(0) win 8192
12:10:37.623624       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:10:37.714471       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1 > 2.2.2.2 icmp: echo request
12:10:37.806690       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80: S
1501131661:1501131661(0) win 8192
12:10:37.897673      31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80:  udp
 0
12:10:41.974604       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1 > 2.2.2.2 icmp: echo
request
12:16:14.957225       1.1.1.1.1234 > 2.2.2.2.80: S 2091733697:2091733697(0) win 8192
12:16:15.023909       1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:16:15.090449       1.1.1.1 > 2.2.2.2 icmp: echo request
```

（注） GRE および IPinIP パケットは、TCP/UDP/ICMP デコード機能を使用してデコードされ、内部パケットを表示します。

次の例は、このコマンドの出力に対する機能拡張を示しています。ドロップする場所のプログラムカウンタまたは現在の指示（後で復号化）、ビルドターゲット、ASA の

リリース番号、ハードウェアモデル、およびASLRメモリのテキスト領域がキャプチャされて表示され、ドロップする場所の復号化を容易にします。

```
ciscoasa(config)# capture gtp_drop type asp-drop inspect-gtp
ciscoasa(config)# show capture gtp_drop [trace]
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983      192.168.108.12.41245 > 171.70.168.183.2123:  udp 27 Drop-reason:
 (inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow (NA)/NA

ciscoasa(config)# show capture gtp_drop trace detail
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983 0050.56b0.bd99 5057.a884.2beb 0x0800 Length: 69
192.168.108.12.41245 > 171.70.168.183.2123:  [udp sum ok] udp 27 (ttl 64, id 53384)
Drop-reason: (inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow
 (NA)/NA
```

次に、mac-filter ドロップを有効にしてキャプチャされたパケットの例を示します。

```
ciscoasa(config)# show capture test detail
Packet Capture info
Name:test
Session: 3
Admin State: disabled
OperState:down
OperState Reason: Session_Admin_Shut
Config Success:yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session PcapSnap Len: 1518
Error Code:0
Drop Count:0
Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id: 1
Port Id: 1
Pcapfile:/mnt/disk0/packet-capture/sess-3-test-ethernet-1-1-0.
pcapPcapsize:0
Drop:mac-filter
Filter:test-1-1
Packet Capture Filter Info
Name:test-1-1
Protocol:0
Ivlan: 0
Ovlan: 3178
SrcIp:0.0.0.0
DestIp: 0.0.0.0
SrcIpv6:::
DestIpv6: ::
SrcMAC: 00:00:00:00:00:00
DestMAC:00:00:00:00:00:00
SrcPort:0
```

```
DestPort: 0
Ethertype: 0
Total Physical breakout ports involved in Packet Capture: 0
0 packet captured on disk using switch capture
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバーにコピーします。

show chardrop

シリアルコンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、**show chardrop** コマンドの出力例を示します。

```
ciscoasa# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

show checkheaps

checkheaps に関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

show checkheaps

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show checkheaps** コマンドの出力例を示します。

```
ciscoasa# show checkheaps
Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	checkheap の確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

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

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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 checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 4 つのグループの 16 進数を表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは show checksum コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（ASA のフラッシュパーティションからの読み込み、またはフラッシュパーティションへの書き込み時）。「.」は、ASA が操作ですでに占有されているが、「ハングアップ」しているわけではないことを示します。このメッセージは、「system processing, please wait」メッセージに似ています。

例

次に、コンフィギュレーションまたはチェックサムを表示する例を示します。

```
ciscoasa(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの出力は、主に内部開発用であり、お客様には無意味な内容です。

例

次に、チャンクに関する統計情報を表示する例を示します。

```
ciscoasa# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed
 34
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルトクラスを表示するには、名前として **default** と入力します。

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
7.2(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show class default
Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。

show clns

IS-IS の Connectionless Network Service（CLNS）情報を表示するには、特権 EXEC モードで **show clns** コマンドを使用します。

show clns { **filter-set | interface** [*interface_name*] | **is-neighbors** [*interface_name*] [**detail**] | **neighbors** [**areas**] [*interface_name*] [**detail**] | **protocol** [ドメイン] | **traffic** [**since** { **bootup | show** }] }

構文の説明

areas	（オプション）CLNS マルチエリア隣接関係を表示します。
bootup	ブートアップ以降の CLNS プロトコル統計情報を表示します。
detail	（オプション）中継システムに関連付けられたエリアを表示します。そうでない場合は、サマリー表示が提供されます。
domain	（オプション）CLNS ドメインのルーティング プロトコル プロセス情報を表示します。
filter-set	CLNS フィルタ セットを表示します。
interface	CLNS インターフェイスのステータスと設定を表示します。
interface_name	（任意）インターフェイス名を指定します。
is-neighbors	IS ネイバー隣接関係を表示します。ネイバー エントリは、配置されているエリアに応じてソートされます。
neighbors	エンド システム（ES）、中継システム（IS）、およびマルチトポロジ統合 Intermediate System-to-Intermediate System（M-ISIS）ネイバーを表示します。
protocol	CLNS ルーティング プロトコル プロセス情報を表示します。少なくとも 2 つのルーティングプロセス、レベル 1 およびレベル 2 が常に存在し、さらに多い場合もあります。
show	この **show** コマンドを最後に使用した以降の CLNS プロトコル統計情報を表示します。
since	（任意）ブートアップ以降、またはこの **show** コマンドを最後に使用した以降のいずれかの CLNS プロトコル統計情報を表示します。
traffic	このルータが認識した CLNS パケットをリストします。

コマンド 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 の CLNS 情報を表示します。

例

以下の出力では、フィルタ セットが次のコマンドで定義されたものと仮定しています。

```
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0005..
.
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0023...

ciscoasa(config)# clns filter-set LOCAL 49.0003...
```

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

```
ciscoasa# show clns filter-set
CLNS filter set US-OR-NORDUNET
      permit 47.0005...
      permit 47.0023...
CLNS filter set LOCAL
      permit 49.0003...
```

次に、トークンリングおよびシリアルインターフェイスの情報を含める **show clns interface** コマンドの出力例を示します。

```
ciscoasa# show clns interface
GigabitEthernet0/1 is up, line protocol is up
  Checksums enabled, MTU 1500
  ERPDUs enabled, min. interval 10 msec.
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 0 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 3
    Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 3
```

```
Next IS-IS LAN Level-1 Hello in 1 seconds
Next IS-IS LAN Level-2 Hello in 1 seconds
```

表 *30 : show clns interface* のフィールド

フィールド	説明
GigabitEthernet0/1 is up, line protocol is up	インターフェイスがアップで、ライン プロトコルがアップであることを示します。
Checksums enabled	イネーブルまたはディセーブルにできます。
MTU	最大伝送単位（MTU）の後ろにある数字は、このインターフェイスのパケットに対する最大伝送サイズです。
ERPDUs	Error Protocol Data Unit（ERPDU）の生成に関する情報を表示します。イネーブルまたはディセーブルにできます。イネーブルの場合、指定された間隔よりも頻繁に送信されません。
RDPDUs	Redirect Protocol Data Unit（RDPDU）の生成に関する情報を表示します。イネーブルまたはディセーブルにできます。イネーブルの場合、指定された間隔よりも頻繁に送信されません。アドレス マスクがイネーブルの場合、リダイレクトがアドレス マスクで送信されます。
Congestion Experienced	CLNS がいつ輻輳検出ビットをオンにするのかを示します。デフォルトは、キュー内に 4 パケットを超えるパケットがある場合にこのビットがオンになります。
DEC compatibility mode	Digital Equipment Corporation（DEC）互換がイネーブルかどうかを示します。
Next ESH/ISH	次のエンド システム（ES）hello または中継システム（IS）helloがいつこのインターフェイスに送信されたかを示します。
Routing Protocol	このインターフェイスが属するエリアをリストします。通常、インターフェイスは 1 つのエリアのみに存在します。
Circuit Type	インターフェイスがローカル ルーティング（レベル 1）、エリア ルーティング（レベル 2）、またはローカルおよびエリア ルーティング（レベル 1-2）に対して設定されているかどうかを示します。

フィールド	説明
Interface number、local circuit ID、Level-1 Metric、DR ID、Level-1 IPv6 Metric、Number of active level-1 adjacencies、Level-2 Metric、DR ID、Level-2 IPv6 Metric、Number of active level-2 adjacencies、Next IS-IS LAN Level-1、Next IS-IS LAN Level-2	最後の一連のフィールドは、Intermediate System-to-Intermediate System（IS-IS）に関する情報を表示します。IS-IS に対して、レベル 1 およびレベル 2 メトリック、プロパティ、回線 ID、およびアクティブ レベル 1 およびレベル 2 隣接関係数が指定されます。
BFD enabled	BFD がインターフェイスでイネーブルです。

次に、 **show clns is-neighbors** コマンドの出力例を示します。

```
ciscoasa# show clns is-neighbors
System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
```

表 *31 : show clns is-neighbors* のフィールド

フィールド	説明
System Id	システムの ID 値。
インターフェイス	ルータが検出されるインターフェイス。
状態	隣接状態。Up および Init が状態です。show clns neighbors の説明を参照してください。
タイプ	L1、L2、および L1L2 タイプの隣接。 **show clns neighbors** の説明を参照してください。
プライオリティ	関連ネイバーがアドバタイズしている IS-IS プライオリティ。インターフェイスの指定 IS-IS ルータに対して最もプライオリティの高いネイバーが選ばれます。
Circuit Id	指定 IS-IS ルータの何がインターフェイス用であるかのネイバーの認識。
書式	ネイバーがフェーズ V（OSI）隣接またはフェーズ IV（DECnet）隣接のいずれであるかを示します。

次に、 **show clns is-neighbors detail** コマンドの出力例を示します。

```
ciscoasa# show clns is-neighbors detail
System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
```

```
  Uptime: 00:12:49
  NSF capable
  Interface name: inside
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 00:12:50
  NSF capable
  Interface name: inside
```

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

```
ciscoasa# show clns neighbors detail
System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          26   L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002        inside      000c.2906.491c      Up          27   L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

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

```
ciscoasa# show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          29   L1L2
CSR7002        inside      000c.2906.491c      Up          27   L1L2
```

表 *32 : show clns 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。
インターフェイス	システムの学習元インターフェイス名。
SNPA	サブネットワーク接続点。これはデータ リンク アドレスです。
状態	ES、IS、または M-ISIS の状態。 • Init：システムは IS で、IS-IS hello メッセージを待機しています。IS-IS は、ネイバーを隣接関係にないと見なします。 • Up：ES または IS が到達可能であると確信しています。
Holdtime	この隣接関係エントリがタイムアウトするまでの秒数。

フィールド	説明
タイプ	隣接関係のタイプ。表示される可能性のある値は次のとおりです。 • ES：エンドシステム隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。 • IS：ルータ隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。 • M-ISIS：ルータ隣接関係が、マルチトポロジ IS-IS プロトコルを介して検出されました。 • L1：レベル 1 ルーティングのみのルータ隣接関係。 • L1L2：レベル 1 およびレベル 2 ルーティングのルータ隣接関係。 • L2：レベル 2 のみのルータ隣接関係。
Protocol	隣接関係が学習されたプロトコル。有効なプロトコル ソースは、ES-IS、IS-IS、ISO IGRP、Static、DECnet、および M-ISIS です。

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

```
ciscoasa# show clns protocol
IS-IS Router
  System Id: 0050.0500.5008.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        outside - IP
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

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

```
ciscoasa# show clns traffic
CLNS:  Time since last clear: never
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0 , bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments:  Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
       Sent 0 requests, 0 replies
```

```
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
Tunneling dropped (rcvd) IP/IPV6:  0
ISO-IGRP: Querys (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP: Router Hellos: (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0
IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos     (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0
```

表 *33 : show clns traffic* のフィールド

フィールド	説明
CLNS & ESIS Output	このルータが送信したパケットの合計数。
入力	このルータが受信したパケットの合計数。
CLNS Local	このルータによって生成されたパケット数をリストします。
Forward	このルータが転送したパケット数をリストします。
CLNS Discards	CLNS が廃棄したパケットとその廃棄理由をリストします。
CLNS Options	CLNS パケット内で見つかったオプションをリストします。
CLNS Segments	セグメント化されたパケットの数と、パケットをセグメント化できなかったことによって発生した障害数をリストします。
CLNS Broadcasts	送受信された CLNS ブロードキャストの数をリストします。
Echos	受信されたエコー要求パケットとエコー応答パケットの数をリストします。このフィールドの後ろの行には、送信されたエコー要求パケットとエコー応答パケットの数をリストします。
ESIS (sent/rcvd)	送受信されたエンド システム Hello（ESH）、中継システム Hello（ISH）、およびリダイレクトの数をリストします。

フィールド	説明
ISO IGRP	送受信された ISO Interior Gateway Routing Protocol（IGRP）のクエリーおよび更新の数を表示します。
Router Hellos	送受信された ISO IGRP ルータ hello パケットの数を表示します。
IS-IS: Level-1 hellos (sent/rcvd)	送受信されたレベル 1 IS-IS hello パケットの数を表示します。
IS-IS: Level-2 hellos (sent/rcvd)	送受信されたレベル 2 の IS-IS hello パケットの数を表示します。
IS-IS: PTP hellos (sent/rcvd)	シリアル リンクを通して送受信されたポイントツーポイントの IS-IS hello パケットの数を表示します。
IS-IS: Level-1 LSPs (sent/rcvd)	送受信されたレベル 1 のリンクステート プロトコル データ ユニット（PDU）の数を表示します。
IS-IS: Level-2 LSPs (sent/rcvd)	送受信されたレベル 2 のリンクステート PDU の数を表示します。
IS-IS: Level-1 CSNPs (sent/rcvd)	送受信されたレベル 1 Complete Sequence Number Packet（CSNP）の数を表示します。
IS-IS: Level-2 CSNPs (sent/rcvd)	送受信されたレベル 2 の CSNP の数を表示します。
IS-IS: Level-1 PSNPs (sent/rcvd)	送受信されたレベル 1 Partial Sequence Number Packet（PSNP）の数を表示します。
IS-IS: Level-2 PSNPs (sent/rcvd)	送受信されたレベル 2 の PSNP の数を表示します。
IS-IS: Level-1 DR Elections	レベル 1 の指定ルータの選定が行われた回数を表示します。
IS-IS: Level-2 DR Elections	レベル 2 の指定ルータの選定が行われた回数を表示します。
IS-IS: Level-1 SPF Calculations	レベル 1 の最短パス優先（SPF）ツリーが計算された回数を表示します。
IS-IS: Level-2 SPF Calculations	レベル 2 の SPF ツリーが計算された回数を表示します。

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。

コマンド	説明
authentication key	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。

コマンド	説明
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 isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
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 clock

ASA に時刻を表示するには、ユーザー EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

構文の説明

detail （任意）クロック ソース（NTP またはユーザー コンフィギュレーション）と現在の夏時間設定（存在する場合）を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー EXEC	• 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 clock** コマンドの出力例を示します。

```
ciscoasa# show clock
12:35:45.205 EDT Tue Jul 27 2004
```

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

```
ciscoasa# show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	ASA のクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。

コマンド	説明
clock timezone	時間帯を設定します。
ntp server	NTP サーバーを指定します。
show ntp status	NTPアソシエーションのステータスを表示します。

show cluster

クラスタ全体の集約データまたはその他の情報を表示するには、特権 EXEC モードで **show cluster** コマンドを使用します。

show cluster [**chassis**] { **access-list** [*acl_name*] | **conn** [**count**] | **context** [*context_name*] | **cpu** [**usage**] **interface-mode | memory | resource | service-policy | traffic | xlate count** }

構文の説明

access-list [*acl_name*]	アクセス ポリシーのヒット カウンタを示します。特定の ACL のカウンタを表示するには、*acl_name* と入力します。
chassis	Firepower 9300 ASA セキュリティ モジュールについて、シャーシのクラスタ情報を表示します。
conn [**count**]	使用中の接続の、すべてのユニットでの合計数を表示します。 **count** キーワードを入力すると、接続数だけが表示されます。
context [*context_name*]	マルチコンテキストモードでのセキュリティコンテキストごとの使用状況を表示します。
cpu [**usage**]	CPU の使用率情報を表示します。
interface-mode	クラスタ インターフェイス モードを表示します（spanned または individual）。
memory	システム メモリ使用率などの情報を表示します。
resource usage	システム リソースと使用状況を表示します。
service-policy	MPF サービス ポリシー統計情報を表示します。
traffic	トラフィック統計情報を表示します。
xlate count	現在の変換情報を表示します。

コマンド 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。
9.4(1)	**service-policy** キーワードが追加されました。
9.4(1.152)	**chassis** キーワードが追加されました。
9.9(1)	**context** キーワードが追加されました。

使用上のガイドライン

show cluster info コマンドおよび **show cluster user-identity** コマンドも参照してください。

例

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

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13 (hitcnt=0,
 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44 (hitcnt=0,
 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
```

```
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):*************************************************************
  100 in use, 100 most used
  cl1:*********************************************************************
  100 in use, 100 most used
```

関連コマンド

コマンド	説明
show cluster info	クラスタ情報を表示します。
show cluster user-identity	クラスタ ユーザー ID 情報および統計情報を表示します。

show cluster history

クラスタのイベント履歴を表示するには、特権 EXEC モードで **show cluster history** コマンドを使用します。

show cluster history ［ **brief** ］［ **latest** ［ *number* ］ ］［ **reverse** ］［ **time** ［ *year month day* ］ *hh* **:** *mm* **:** *ss* ］

構文の説明

brief	一般イベントを除くクラスタ履歴を表示します。
latest [*number*]	最新のイベントを表示します。デフォルトでは、最新の 512 のイベントが表示されます。*number* を指定することでイベントの数を 1 ー 512 に制限できます。
reverse	イベントを逆の順序で表示します。
time [*year month day*] *hh*:*mm*:*ss*	指定された日時より前のイベントを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド 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。
9.14(1)	出力が拡張され、トラブルシューティングの詳細が表示されるようになりました。
9.16(1)	**brief**、**latest**、**reverse**、**time** キーワードが追加されました。
9.19(1)	コマンド出力は、**Master** と **Slave** から **Control_Node** と **Data_Node** に変更されました。

使用上のガイドライン

次に、 **show cluster history time** コマンドの出力例を示します。

```
asa1(cfg-cluster)# show cluster history time august 26 10:10:05
```

```
================================================================================
From State            To State              Reason
================================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI


10:10:01 UTC Aug 26 2020
ELECTION              ONCALL                Event: Cluster unit A state is CONTROL_NODE


10:10:02 UTC Aug 26 2020
ONCALL                DATA_NODE_COLD            Data Node proceeds with configuration
sync


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done
```

次に、 **show cluster history brief** コマンドの出力例を示します。

```
asa1(cfg-cluster)# show cluster history brief
================================================================================
From State            To State              Reason
================================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI



10:10:02 UTC Aug 26 2020
ONCALL                DATA_NODE_COLD            Data Node proceeds with configuration
sync


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
```

```
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done
```

次に、 **show cluster history latest** コマンドの出力例を示します。

```
asa1(cfg-cluster)# show cluster history latest 3
==========================================================================
From State             To State               Reason
==========================================================================

10:10:05 UTC Aug 26 2020
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done
```

関連コマンド

コマンド	説明
show cluster	クラスタ全体の集約データおよびその他の情報を表示します。
show cluster info	クラスタ情報を表示します。
show cluster user-identity	クラスタ ユーザー ID 情報および統計情報を表示します。

show cluster info

クラスタ情報を表示するには、特権 EXEC モードで **show cluster info** コマンドを使用します。

show cluster info ［ **auto-join** ｜ **clients** ｜ **conn-distribution** ｜ **counters** ｜ **flow-mobility** ｜ **goid** ［ *options* ］ ｜ **health** ［ **details** ］ ｜ **incompatible-config** ｜ **instance-type** ｜ **loadbalance** ｜ **load-monitor** ｜ **old-members** ｜ **packet-distribution** ｜ **trace** ［ オプション ］ ｜ **transport** ｛ **asp** ｜ **cp** ［ **detail** ］｝ ｜ **unit-join-acceleration incompatible-config** ］

構文の説明

auto-join	（オプション）一定時間遅延した後にクラスタノードがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ノードが永続的に無効になっている場合、またはノードがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。
clients	（オプション）登録クライアントのバージョンを表示します。
conn-distribution	（オプション）クラスタ内の接続分布を表示します。
flow-mobility counters	（オプション）EID の移動やフローオーナーの移動に関する情報を表示します。
goid [*options*]	（オプション）グローバル オブジェクト ID データベースを示します。次のオプションがあります。 classmap conn-set hwidb idfw-domain idfw-group interface policymap virtual-context
health [**details**]	（オプション）ヘルス モニタリング情報を表示します。details キーワードは、ハートビート メッセージの失敗数を表示します。
incompatible-config	（オプション）現在の実行コンフィギュレーションのクラスタリングと互換性のないコマンドを表示します。このコマンドは、クラスタリングをイネーブルにする前に役立ちます。
instance-type	（オプション）ASA 仮想 のクラスタノードごとの CPU コアと RAM を表示します。

loadbalance	（オプション）ロード バランシング情報を表示します。
load-monitor	（オプション）クラスタノードのトラフィック負荷をモニターします。これには、合計接続数、CPUとメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのノードが負荷を処理できる場合は、ノードのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、**load-monitor** コマンドを使用してデフォルトで有効になっています。
old-members	（オプション）クラスタの以前のノードを表示します。
packet-distribution	（オプション）クラスタのパケット分布を表示します。
trace [*options*]	（オプション）クラスタリング制御モジュール イベント トレースを表示します。次のオプションがあります。 • **latest** [*number*]：最新の *number* のイベントを表示します。number は 1 ～ 2147483647 の範囲です。デフォルトではすべてが表示されます。 • **level** *level*：レベル別にイベントをフィルタ処理します。レベルは、次のいずれかです。 **all** 、 **critical** 、 **debug** 、 **informational** 、または **warning** 。 • **module** *module*：モジュール別にイベントをフィルタ処理します。モジュールは、次のいずれかです。 **ccp** 、 **datapath** 、 **fsm** 、 **general** 、 **hc** 、 **license** 、 **rpc** 、 **or transport** 。 • **time** {[*month day*] [*hh* **:** *mm* **:** *ss*]}：指定した時刻または日付より前のイベントを表示します。
transport { **asp** | **cp** [**detail**]}	（オプション）次のトランスポート関連の統計情報を表示します。 • **asp** ：データプレーンのトランスポート統計情報。 • **cp** ：コントロールプレーンのトランスポート統計情報。 **detail** キーワードを入力すると、クラスタで信頼性の高いトランスポートプロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケットドロップの問題を特定できます。
unit-join-acceleration incompatible-config	（オプション）**unit join-acceleration** コマンドが有効になっている場合（デフォルト）、一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがノードに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。 **show cluster info unit-join-acceleration incompatible-config** コマンドを使用して、互換性のない設定を表示します。

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。
9.3(1)	**show cluster info health** コマンドの改善されたモジュールのサポートが追加されました。
9.5(1)	サイト ID 情報が出力に追加されました。
9.5(2)	**flow-mobility counters** キーワードが追加されました。
9.8(1)	**health details** キーワードが追加されました。
9.9(2)	**auto-join** キーワードが追加されました。
9.9(2)	**transport cp** の **detail** キーワードが追加されました。
9.13(1)	**load-monitor** キーワードと **unit-join-acceleration incompatible-config** キーワードが追加されました。
9.17(1)	**instance-type** キーワードが ASA 仮想 に追加され、ASA 仮想 の情報が **show cluster info** の出力に追加されました。
9.19(1)	コマンド出力は、**Master** と **Slave** から **Control_Node** と **Data_Node** に変更されました。

使用上のガイドライン

オプションを指定しない場合、**show cluster info** コマンドはクラスタの名前とステータス、クラスタノード、ノードの状態など、一般的なクラスタ情報を表示します。

clear cluster info コマンドを使用して、統計情報をクリアします。

show cluster コマンドおよび **show cluster user-identity** コマンドも参照してください。

例

次に、ハードウェア プラットフォームについての **show cluster info** コマンドの出力例を示します。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

次に、ASA 仮想 に対する **show cluster info** コマンドの出力例を示します。

```
Cluster ASAv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "A" in state CONTROL_NODE
        ID        : 0
        Version   : 9.17(1)79
        Serial No.: 9A3GVQ1EL7W
        CCL IP    : 10.1.1.24
        CCL MAC   : 0050.56a8.7d4f
        Module    : ASAv
        Resource  : 2 cores / 4096 MB RAM
        Last join : 16:27:46 UTC Feb 18 2021
        Last leave: N/A
Other members in the cluster:
    Unit "B" in state DATA_NODE
        ID        : 1
        Version   : 9.17(1)79
        Serial No.: 9ACE28176EE
        CCL IP    : 10.1.1.25
        CCL MAC   : 0050.56a8.883e
```

```
        Module    : ASAv
        Resource  : 2 cores / 4096 MB RAM
        Last join : 20:29:25 UTC Feb 19 2021
        Last leave: 16:31:46 UTC Feb 19 2021
```

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

```
ciscoasa(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's
confirmation upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

次に、 **show cluster info trace** コマンドの出力例を示します。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

次に、ASA 5500-X での **show cluster info health** コマンドの出力例を示します。

```
ciscoasa# show cluster info health
Member ID to name mapping:
  0 - A   1 - B(myself)
                          0        1
GigabitEthernet0/0        up       up
Management0/0             up       up
ips (policy off)          up       None
sfr (policy off)          None     up
Unit overall              healthy   healthy
Cluster overall           healthy
```

上記の出力には、ASA IPS（ips）と ASA FirePOWER（sfr）の両方のモジュールが表示されます。モジュールごとに ASA は「policy on」または「policy off」を使用してサービスポリシーが設定されたかどうかを示します。次に例を示します。

```
class-map sfr-class
match sfr-traffic
policy-map sfr-policy
class sfr-class
sfr inline fail-close
service-policy sfr interface inside
```

上記の設定により、ASA FirePOWER モジュール（「sfr」）は「policy on」と表示されます。あるモジュールが、あるクラスタノードでは「up」、他のノードでは「down」または「None」になっている場合、そのモジュールが down となっているノードはクラスタから除外されます。ただし、サービスポリシーが設定されていない場合、クラスタノードはクラスタから除外されません。モジュールステータスは、モジュールが実行中である場合にのみ関連します。

次に、ASA 5585-X での **show cluster info health** コマンドの出力例を示します。

```
ciscoasa# show cluster info health
spyker-13# sh clu info heal
Member ID to name mapping:
  0 - A(myself) 1 - B
                      0 1
GigabitEthernet0/0      upup
SSM Card (policy off)   upup
Unit overall            healthyhealth
Cluster overall         healthyhealth
```

サービス ポリシーにモジュールを設定した場合は、出力に「policy on」と表示されます。サービス ポリシーを設定しない場合は、モジュールがシャーシに存在しても、出力に「policy off」と表示されます。

次に、 **show cluster info flow-mobility counters** コマンドの出力例を示します。

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

次に、 **show cluster info auto-join** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Control Node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

show cluster info transport cp detail コマンドについては、次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
```

```
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1
Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent
This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0
This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256
This unit as a receiver of unicast messages
-----------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303
Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0
    total:                   0
    current:                 0
    high watermark:          0
    delivered:               0
    deliver failures:        0
```

```
    buffer full drops:       0
    message truncate drops:  0
    gate close ref count:    0
    num of supported clients:45
MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0
MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%
Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0
MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%
```

```
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

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

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
   1           0            0            13             27
```

次に、 **show cluster info unit-join-acceleration incompatible-config** コマンドの出力例を示します。

ciscoasa# show cluster info unit-join-acceleration incompatible-config

INFO: Clustering is not compatible with following commands. User must manually remove them to activate the cluster unit join-acceleration feature.

```
zone sf200 passive
```

次に、ASA 仮想 クラスタに対する show cluster info instance-type コマンドの出力例を示します。

```
ciscoasa# show cluster info instance-type
      Unit            Module Type     CPU Cores            RAM (MB)
      A                   ASAv           2                  4096
      B                   ASAv           2                  4096
```

関連コマンド

コマンド	説明
show cluster	クラスタ全体の集約データを表示します。
show cluster user-identity	クラスタ ユーザー ID 情報および統計情報を表示します。

show cluster user-identity

クラスタ全体のユーザーID情報と統計情報を表示するには、特権EXECモードで **show cluster user-identity** コマンドを使用します。

show cluster user-identity [**statistics** [**user** *name* | **user-group** *group_name*] | **user** [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** { **domain** *name* | **user-group** *group_name*] [**list** [*detail*]] }

構文の説明

active	アクティブなIP/ユーザーマッピングがあるユーザーを表示します。
all	ユーザー データベース内のすべてのユーザーを表示します。
domain *name*	ドメインのユーザー情報を表示します。
inactive	非アクティブな IP/ユーザー マッピングがあるユーザーを表示します。
list [*detail*]	ユーザーのリストを表示します。
statistics	クラスタ ユーザー ID 統計情報を表示します。
user	ユーザー データベースを表示します。
user *name*	特定のユーザーの情報を表示します。
user-group *group_name*	特定のグループの各ユーザーの情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

show cluster info コマンドおよび **show cluster** コマンドも参照してください。

例

次に、<< **command** >> コマンドの出力例を示します。

関連コマンド

コマンド	説明
show cluster	クラスタ全体の集約データを表示します。
show cluster info	クラスタ情報を表示します。

show cluster vpn-sessiondb distribution

クラスタ全体でアクティブおよびバックアップセッションがどのように分散しているかを表示するには、特権 EXEC モードでこのコマンドを実行します。

show cluster vpn-sessiondb distribution

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
9.9(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 show コマンドを使用すると、各メンバーで **show vpn-sessiondb summary** を実行する必要なく、セッションのクイックビューが提供されます。

各行には、メンバー ID、メンバー名、アクティブ セッション数、およびバックアップ セッションが存在するメンバーが含まれています。

例

たとえば、show cluster vpn-sessiondb distribution が以下のように出力された場合を考えます。

Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)

Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)

Member 2 (unit-1-2): active: 0

これは、次のように解釈できます。

- メンバー 0 には 209 のアクティブ セッションがあり、111 のセッションはメンバー 1 にバックアップされ、98 のセッションはメンバー 2 にバックアップされます。
- メンバー 1 には 204 のアクティブ セッションがあり、108 のセッションはメンバー 0 にバックアップされ、96 のセッションはメンバー 2 にバックアップされます。
- メンバー 2 にはアクティブ セッションがないため、クラスタ メンバーはこのノードのセッションをバックアップしていません。

関連コマンド

コマンド	説明
cluster redistribute vpn-sessiondb	分散型 VPN クラスタのアクティブな VPN セッションを再配布します。

show compression

ASA の圧縮統計情報を表示するには、特権 EXEC モードで **show compression** コマンドを使用します。

show compression［ **all | anyconnect-ssl | http-comp** ］

コマンド デフォルト

このコマンドにデフォルトの動作はありません。

構文の説明

all	すべての圧縮統計情報（anyconect-ssl、http comp）を表示
anyconnect-ssl	AnyConnect SSL 圧縮統計情報を表示します。
http-comp	HTTP-COMP 圧縮統計情報を表示

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

Show compression allでは次のタイプの統計情報が表示されます。

```
Compression AnyConnect Client Sessions              0
Compressed Frames                                   0
Compressed Data In (bytes)                          0
Compressed Data Out (bytes)                         0
Expanded Frames                                     0
Compression Errors                                  0
Compression Resets                                  0
Compression Output Buf Too Small                    0
Compression Ratio                                   0
Decompressed Frames                                 0
Decompressed Data In                                0
Decompressed Data Out                               0
```

```
Decompression CRC Errors                          0
Decompression Errors                              0
Decompression Resets                              0
Decompression Ratio                               0
Block Allocation Failures                         0
Compression Skip Percent                         0%
Time Spent Compressing (peak)                 0.0%
Time Spent Decompressing (peak)               0.0%
Number of http bytes in                           0
Number of http gzipped bytes out                  0
```

関連コマンド

コマンド	説明
圧縮	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。

show configuration

ASA でフラッシュメモリに保存されているコンフィギュレーションを表示するには、特権 EXEC モードで **show configuration** コマンドを使用します。

show configuration

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。

使用上のガイドライン

show configuration コマンドは、ASA のフラッシュメモリに保存されているコンフィギュレーションを表示します。**show running-config** コマンドとは異なり、**show configuration** コマンドの実行ではそれほど多くの CPU リソースが使用されません。

ASA のメモリ内のアクティブなコンフィギュレーション（保存されているコンフィギュレーションの変更など）を表示するには、**show running-config** コマンドを使用します。

例

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

```
ciscoasa# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
```

```
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
```

```
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

関連コマンド

コマンド	説明
configure	ターミナルからASAを設定します。

show configuration session

現在のコンフィギュレーションセッションおよびセッション内での変更を表示するには、特権 EXEC モードで **show configuration session** コマンドを使用します。

show configuration session [*session_name*]

構文の説明

session_name	既存のコンフィギュレーション セッションの名前。このパラメータを省略した場合、既存のすべてのセッションが表示されます。

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
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL およびそのオブジェクトの編集用に独立したセッションを作成する **configure session** コマンドとともに使用します。このコマンドは、セッション名と、そのセッションで行われたすべてのコンフィギュレーション変更を表示します。

コミット済みとして示されているセッションについて、変更が想定どおりに機能していないと判断した場合は、そのセッションを開いて、その変更を取り消すことができます。

例

次に、すべての使用可能なセッションの例を示します。

```
ciscoasa# show configuration session

config-session abc (un-committed)
 access-list abc permit ip any any
 access-list abc permit tcp any any

config-session abc2 (un-committed)
 object network test
 host 1.1.1.1
```

```
 object network test2
 host 2.2.2.2

ciscoasa#
```

関連コマンド

コマンド	説明
clear configuration session	コンフィギュレーション セッションとその内容を削除します。
clear session	コンフィギュレーション セッションの内容をクリアするか、そのアクセス フラグをリセットします。
configure session	セッションを作成するか、開きます。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show conn [**count** | [**all**] [**detail** [**data-rate-filter** { **lt | eq | gt** } *value*]] [**long**] [**state** *state_type*] [**protocol** { **tcp | udp | sctp** }] [**scansafe**] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]]
[**user-identity | user** [*domain_nickname* \ ] *user_name* **| user-group** [*domain_nickname* \ \ ] *user_group_name*] | **security-group**] [**zone** *zone_name* [**zone** *zone_name*] [**...**]] [**data-rate**]

構文の説明

address	（任意）指定した送信元 IP アドレスまたは宛先 IP アドレスとの接続を表示します。
all	（任意）通過トラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（任意）アクティブな接続の数を表示します。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、IP アドレスをダッシュ（-）で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、ポート番号をダッシュ（-）で区切ります。次に例を示します。 `1000-2000`
detail	（任意）変換タイプとインターフェイスの情報を含め、接続の詳細を表示します。
data-rate-filter { **lt	eq**	**gt** } *value*	（オプション）データレート値（1秒あたりのバイト数）に基づいてフィルタリングされた接続を表示します。次に例を示します。 `data-rate-filter gt 123`
long	（任意）接続をロング フォーマットで表示します。
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定した送信元ポートまたは宛先ポートとの接続を表示します。

protocol { **tcp** | **udp** | **sctp** }	（任意）接続プロトコルを指定します。
scansafe	（オプション）クラウド Web セキュリティ サーバーに転送される接続を表示します。
security-group	（オプション）表示されるすべての接続が指定したセキュリティ グループに属することを指定します。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、IP アドレスをダッシュ（-）で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、ポート番号をダッシュ（-）で区切ります。次に例を示します。 `1000-2000`
state *state_type*	（任意）接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、<xref> を参照してください。
user [*domain_nickname* \ ] *user_name*	（オプション）表示されるすべての接続が指定したユーザーに属することを指定します。 *domain_nickname* 引数が含まれていない場合、ASA はデフォルトドメインのユーザーに関する情報を表示します。
user-group [*domain_nickname* \\ ] *user_group_name*	（オプション）表示されるすべての接続が指定したユーザー グループに属することを指定します。 *domain_nickname* 引数が含まれていない場合、ASA はデフォルトドメインのユーザーグループに関する情報を表示します。
user-identity	（オプション）ASA がアイデンティティ ファイアウォール機能に対するすべての接続を表示することを指定します。接続を表示する場合、ASA は一致するユーザーを識別するとそのユーザー名と IP アドレスを表示します。同様に、ASA は一致するホストを識別するとそのホスト名と IP アドレスを表示します。
zone [*zone_name*]	（オプション）ゾーンの接続を表示します。 **long** キーワードと **detail** キーワードは、接続が構築されたプライマリインターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。
data-rate	（オプション）データレート トラッキング ステータスが有効になっているか無効になっているかを表示します。

コマンド デフォルト

デフォルトでは、すべての通過接続が表示されます。デバイスへの管理接続も表示するには、**all** キーワードを使用する必要があります。

コマンド 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(8)/7.2(4)/8.0(4)	「ローカル」と「外部」ではなく、送信元と宛先の概念を使用するように、構文が簡易化されました。新しい構文では、送信元アドレスが入力された最初のアドレスで、宛先が 2 番目のアドレスです。以前の構文では、**foreign** や **fport** などのキーワードを使用して宛先アドレスおよびポートを設定していました。
7.2(5)/8.0(5)/8.1(2)/8.2(4)/8.3(2)	**tcp_embryonic** 状態タイプが追加されました。このタイプは、i フラグを伴うすべての TCP 接続（不完全接続）を表示します。UDP の i フラグ接続は表示されません。
8.2(1)	TCP ステート バイパスに b フラグが追加されました。
8.4(2)	アイデンティティ ファイアウォールをサポートするために、**user-identity** 、 **user** 、および **user-group** キーワードが追加されました。
9.0(1)	クラスタリングのサポートが追加されました。 **scansafe** キーワードと **security-group** キーワードが追加されました。
9.3(2)	**zone** キーワードが追加されました。
9.5(2)	LISP フロー モビリティの対象となるトラフィックに L フラグが追加されました。
9.5(2)	Diameter 接続に、詳細な出力の Q フラグが追加されました。**protocol sctp** キーワードが追加されました。オフロードされたフローに、詳細な出力の o フラグが追加されました。
9.6(2)	STUN 接続に、詳細な出力の u フラグが追加されました。M3UA 接続に v フラグが追加されました。
9.7(1)	クラスタ ディレクタ ローカリゼーションの使用時にスタブ フローがローカル ディレクタ YI か、またはローカル バックアップ yI であることを示すため、I フラグが追加されました。

リリース	変更内容
9.9(1)	detail 出力の最後に位置する VPN スタブは、そのクラスタのロールに加えて、接続が VPN 暗号化スタブ フローのロールを果たしていることを示します。
9.13(1)	デッド接続検出（DCD）イニシエータ/レスポンダプローブカウントが、DCD 対応接続に関する **show conn detail** の出力に追加されました。
9.14(1)	接続データレートトラッキング ステータスが追加されました。 ユーザー指定のデータレート値によって接続をフィルタ処理するために、**show conn detail** コマンドに **data-rate-filter** キーワードが追加されました。
9.16(1)	マルチキャストデータ接続エントリは出力に表示されなくなりました。このエントリは **show local-host** の出力に移動しました。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続および UDP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注） ASA で第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

表 34 : 接続状態のタイプ に、**show conn state** コマンドを使用して指定できる接続タイプを示します。複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。

表 *34* : 接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続

キーワード	表示される接続タイプ
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ インスペクション エンジン接続
tcp_embryonic	TCP 初期接続
vpn_orphan	孤立した VPN トンネル フロー

使用上のガイドライン

detail オプションを使用すると、表 34 : 接続状態のタイプ に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。また、VPN スタブは、このコマンドの出力の最後に表示され、そのクラスタのロールに加えて、接続が VPN 暗号化スタブ フローのロールを果たしていることを示します。VPN スタブは非対称 VPN トラフィックのシナリオまたはハブ n スポークのシナリオで、クリア テキストのパケットを暗号化するために使用されます。

表 *35* : 接続フラグ

Flag	説明
a	SYN に対する外部 ACK を待機
A	SYN に対する内部 ACK を待機
b	TCP ステート バイパス
B	外部からの初期 SYN
C	コンピュータ テレフォニー インターフェイス クイック バッファ エンコーディング（CTIQBE）メディア接続。

Flag	説明
d	dump
D	DNS
E	外部バック接続。これは、内部ホストから開始されている必要があるセカンダリ データ接続です。たとえば、内部クライアントがPASVコマンドを発行し、外部サーバーが受け入れた後、ASA は FTP を使用してこのフラグが設定された外部バック接続を事前割り当てします。内部クライアントがサーバーに接続しようとすると、ASA はこの接続試行を拒否します。外部サーバーだけが事前割り当て済みのセカンダリ接続を使用できます。
f	内部 FIN
F	外部 FIN
g	メディア ゲートウェイ コントロール プロトコル（MGCP）接続
G	接続がグループの一部[1]
h	H.225
H	H.323
i	不完全な TCP 接続または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
l	ローカル ディレクタ/バックアップ スタブ フロー
L	LISP フロー モビリティの対象となるトラフィック
m	SIP メディア接続
M	SMTP データ
o	オフロードされたフロー。
O	発信データ
p	複製（未使用）

Flag	説明
P	内部バック接続。これは、内部ホストから開始されている必要があるセカンダリ データ接続です。たとえば、内部クライアントがPORTコマンドを発行し、外部サーバーが受け入れた後、ASA は FTP を使用してこのフラグが設定された内部バック接続を事前割り当てします。外部サーバーがクライアントに接続しようとすると、ASA はこの接続試行を拒否します。内部クライアントだけが事前割り当て済みのセカンダリ接続を使用できます。
q	SQL*Net データ
Q	Diameter 接続
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC[2]
s	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続[3]
T	SIP 接続[4]
u	STUN 接続
U	up
v	M3UA 接続
V	VPN の孤立
w	Firepower 9300 でのシャーシ間クラスタリングの場合、別のシャーシ上のバックアップオーナーでのフローを識別します。
W	WAAS
X	CSC SSM などのサービスモジュールによって検査されます。
y	クラスタリングの場合、バックアップ オーナー フローを識別します。
Y	クラスタリングの場合、ディレクタ フローを識別します。
z	クラスタリングの場合、フォワーダ フローを識別します。
Z	クラウド Web セキュリティ

[1] G フラグは、接続がグループの一部であることを示します。制御接続および関連するすべてのセカンダリ接続を指定するために、GRE および FTP Strict 検査によって設定されます。制御接続が切断されると、関連するすべてのセカンダリ接続も切断されます。
[2] show conn コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
[3] UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
[4] UDP 接続の場合、値 T は、timeout sip コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。

（注） DNS サーバーを使用する接続の場合、 **show conn** コマンドの出力で、接続の送信元ポートが *DNS* サーバーの *IP* アドレス に置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は app_id で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答が ASA を通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドルタイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注） **timeout conn** コマンドで定義した非アクティブ期間（デフォルトは 1:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグエントリも表示されなくなります。

LAN-to-LAN トンネルまたはネットワーク拡張モード トンネルがドロップし、回復しない場合は、孤立したトンネル フローが数多く発生します。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。 **show conn** コマンドの出力では、このような孤立したフローを **V** フラグで示します。

次の TCP 接続方向性フラグが同じセキュリティレベルのインターフェイス間の接続に適用された場合（ **same-security permit** コマンドを参照）、同じセキュリティレベルのインターフェイスでは「内部」または「外部」がないため、フラグの方向は無関係となります。ASA は、これらのフラグを同じセキュリティレベルの接続で使用する必要があるため、ASA が、他の接続の特性に基づいて 1 つのフラグを別のフラグより優先して選択することがあります（たとえば、f 対 F）が、選択された方向性は無視する必要があります。

- B：外部からの初期 SYN
- a：SYN に対する外部 ACK を待機
- A：SYN に対する内部 ACK を待機

- f：内部 FIN
- F：外部 FIN
- s：外部 SYN を待機
- S：内部 SYN を待機

特定の接続に関する情報を表示するには、**security-group** キーワードを入力し、接続元と接続先の両方でセキュリティ グループ テーブル値またはセキュリティグループ名を指定します。ASA は、指定のセキュリティ グループ テーブル値またはセキュリティグループ名に一致する接続を表示します。

送信元および宛先のセキュリティグループテーブル値または送信元および宛先のセキュリティグループ名を指定せずに **security-group** キーワードを指定すると、ASA はすべての SXP 接続のデータを表示します。

ASA は、接続データを *security_group_name* (*SGT_value*) の形式で表示するか、またはセキュリティグループ名が不明な場合は単に *SGT_value* として表示します。

（注） スタブ接続が低速パスを通過しないため、セキュリティ グループ データはスタブ接続には使用できません。スタブ接続には、接続の所有者にパケットを転送するために必要な情報だけが保持されます。

単一のセキュリティグループの名前を指定して、クラスタ内のすべての接続を表示できます。たとえば、次の例では、クラスタのすべてのユニットのセキュリティ グループ mktg に一致する接続が表示されます。

```
ciscoasa# show cluster conn security-group name mktg
```

接続データレートトラッキング機能の現在の状態（有効または無効）を表示するには、**data-rate** キーワードを使用します。 **data-rate filte** r キーワードを使用して、データレート値（1 秒あたりのバイト数）を基に接続をフィルタ処理します。接続データをフィルタリングするには、比較演算子（より小さい、等しい、より大きい）を使用します。出力には、順方向と逆方向の両方のフローについて、アクティブな接続と 2 つのデータレート値（瞬時（1 秒）および最大データレート値）が表示されます。

例

複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。次に、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示する例を示します。

```
ciscoasa# show conn state up,rpc,h323,sip
```

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

```
ciscoasa# show conn count
54 in use, 123 most used
```

次に、**show conn** コマンドの出力例を示します。次に、内部ホスト 10.1.1.15 から 10.10.49.10 の外部 Telnet サーバーへの TCP セッション接続の例を示します。B フラグが存在しないため、接続は内部から開始されています。「U」、「I」および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示します。

```
ciscoasa# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags
UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes
0, flags Ti
```

次に、**show conn**コマンドの出力例を示します。接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
ciscoasa# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

次に、**show conn detail** コマンドの出力例を示します。次に、外部ホスト 10.10.49.10 から内部ホスト 10.1.1.15 への UDP 接続の例を示します。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
ciscoasa# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
```

```
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
Cluster units to ID mappings:
  ID 0: asa1
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

次に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
ciscoasa# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
ciscoasa# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
 UOVB
```

クラスタリングの場合、接続フローをトラブルシュートするには、最初にすべてのユニットの接続を一覧表示します。一覧表示するには、マスターユニットで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3つのすべてのASAでの172.18.124.187:22から192.168.103.131:44727へのSSH接続が表示されています。ASA1にはzフラグがあり、この接続のフォワーダであることを表しています。ASA3にはYフラグがあり、この接続のディレクタであることを表しています。ASA2には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットはASA2の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットはASA1およびASA3の外部インターフェイスに入り、クラスタ制御リンクを介してASA2に転送され、次にASA2の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags z
ASA2:**************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags UIO
ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

ASA2での **show conn detail** の出力は、最新のフォワーダがASA1であったことを示しています。

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 1 in use, 61 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
```

```
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
Cluster units to ID mappings:
  ID 0: asa1
  ID 1: asa2
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
 0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

次に、アイデンティティ ファイアウォール機能の接続を表示する例を示します。

```
ciscoasa# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00,
bytes 10, flags -
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags -
...
ciscoasa# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags -
```

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

```
ciscoasa# show conn long zone zone-inside zone zone-outside
TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

detail キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828, cluster sent/rcvd bytes
 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

次の例では、接続データレートトラッキング機能のステータスを表示する方法について示します。

```
ciscoasa# show conn data-rate
Connection data rate tracking is currently enabled.
```

次の例では、指定したデータレートに基づいて接続をフィルタリングする方法について示します。

```
ciscoasa# show conn detail data-rate-filter ?
eq  Enter this keyword to show conns with data-rate equal to specified value
gt   Enter this keyword to show conns with data-rate greater than specified
       value
lt    Enter this keyword to show conns with data-rate less than specified value
ciscoasa# show conn detail data-rate-filter gt ?
<0-4294967295>  Specify the data rate value in bytes per second
ciscoasa# show conn detail data-rate-filter gt 123 | grep max rate
    max rate:     3223223/399628 bytes/sec
    max rate:     3500123/403260 bytes/sec
```

関連コマンド

コマンド	説明
clear conn	接続をクリアします。
clear conn data-rate	保存されている現在の最大データレートをクリアします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show console-output** コマンドの出力例を示します。コンソール出力がない場合、次のメッセージが表示されます。

```
ciscoasa# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
console timeout	ASA に対するコンソール接続のアイドルタイムアウトを設定します。
show running-config console timeout	ASA に対するコンソール接続のアイドルタイムアウトを表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | **detail** | **count**]

構文の説明

count	（任意）設定済みコンテキストの数を表示します。
detail	（任意）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（任意）コンテキスト名を設定します。名前を指定しない場合、ASA はすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

コマンド デフォルト

システム実行スペースでは、名前を指定しない場合、ASA はすべてのコンテキストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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。
8.0(2)	割り当てられた IPS 仮想センサーについての情報が追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、 **show context** コマンドの出力例を示します。この例では、3 つのコンテキストが表示されています。

```
ciscoasa# show context
Context Name      Interfaces                  URL
```

```
*admin            GigabitEthernet0/1.100        flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200        flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 36 : show context のフィールド に、各フィールドの説明を示します。

表 *36 : show context* のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
インターフェイス	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

例

次に、システム実行スペースでの **show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail
Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1
Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2
Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257
Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 37 : コンテキストの状態 に、各フィールドの説明を示します。

表 *37 :* コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
状態メッセージ：	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。
Has been created, but initial ACL rules not complete	ASA はコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、下位セキュリティ レベルから上位セキュリティ レベルへのトラフィック送信を禁止したり、アプリケーション インスペクションおよびその他のパラメータをイネーブルにします。このセキュリティポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックが ASA をいっさい通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだ ASA がコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、 **config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、 **config-url** コマンドを再度入力します。または、ブランクの実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、ASA がコンテキスト ID を新しいコンテキストに再利用するか、セキュリティアプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。

フィールド	説明
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、ASA がコンテキスト ID を新しいコンテキストに再利用するか、セキュリティアプライアンスを再起動するまでメモリに保持されます。
Real Interfaces	このコンテキストに割り当てられたインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはインターフェイスの実際の名前です。
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Real IPS Sensors	AIP SSM をインストールしている場合に、コンテキストに割り当てられる IPS 仮想センサー。センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはセンサーの実際の名前です。
Mapped IPS Sensors	センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。センサー名をマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

例

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

```
ciscoasa# show context count
Total active contexts: 2
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
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。

show controller

存在するすべてのインターフェイスについて、コントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

構文の説明

bridge	（オプション）ASA 5585-X の PCI ブリッジ固有の情報を表示します。
bridge-id	（オプション）ASA 5585-X の一意の各 PCI ブリッジ ID を表示します。
detail	（任意）コントローラの詳細を表示します。
pci	（オプション）ASA 5585-X の PCI コンフィギュレーション領域の先頭 256 バイトとともに PCI デバイスの要約を表示します。
physical_interface	（任意）インターフェイス ID を指定します。
port-num	（オプション）ASA 5585-X 適応型 ASA の各 PCI ブリッジ内の一意のポート番号を表示します。
slot	（オプション）ASA 5580 の PCI-e バスおよびスロットの情報のみを表示します。

コマンド デフォルト

インターフェイスを指定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 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。
8.0(2)	このコマンドは ASA 5505 のみではなく、すべてのプラットフォームに適用されるようになりました。 **detail** キーワードが追加されました。
8.1(1)	ASA 5580 用に **slot** キーワードが追加されました。

リリース	変更内容
8.2(5)	IPS SSP がインストールされた ASA 5585-X 用に **pci** 、 **bridge** 、*bridge-id*、*port-num* の各オプションが追加されました。また、すべての ASA モデル用に、ポーズフレームを送信して 1 ギガビット イーサネット インターフェイスでのフロー制御を可能にするためのサポートが追加されました。
8.6(1)	ASA とソフトウェアモジュール間の制御トラフィックに使用される ASA 5512-X から ASA 5555-X Internal-Control0/0 までのインターフェイス用と、ASA とソフトウェアモジュールへのデータトラフィックに使用される Internal-Data0/1 インターフェイス用に、 **detail** キーワ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

このコマンドは、内部的不具合やカスタマーにより発見された不具合を調査するときに、Cisco TAC がコントローラについての有用なデバッグ情報を収集するために役立ちます。実際の出力は、モデルとイーサネット コントローラによって異なります。このコマンドは、IPS SSP がインストールされている ASA 5585-X の対象となるすべての PCI ブリッジに関する情報も表示します。ASA サービスモジュールの場合、 **show controller** コマンドの出力に PCIe スロット情報は表示されません。

例

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

```
ciscoasa# show controller
Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
     Global Registers:
         Control:       0x0482
-------------------------------------------------------------------------
Number of VLANs: 1
-------------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
-------------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-------------------------------------------------------------------------
....
Ethernet0/6:
```

```
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00
...
Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                          0xe0004000 = 0x00000000
    ctrl_status                  0xe0004004 = 0x5501064a
    irq_src                      0xe0004008 = 0x00000000
    irq_msk                      0xe000400c = 0x00000000
    irq_hw_err_src               0xe0004010 = 0x00000000
    irq_hw_err_msk               0xe0004014 = 0x00001000
    bmu_cs_rxq                   0xe0004060 = 0x002aaa80
    bmu_cs_stxq                  0xe0004068 = 0x01155540
    bmu_cs_atxq                  0xe000406c = 0x012aaa80
   Bank 2: MAC address registers:

....
```

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

```
ciscoasa# show controller gigabitethernet0/0 detail
GigabitEthernet0/0:
   Intel i82546GB revision 03
     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
```

```
    TX Inter Packet Gap:        0xf8260410 = 0x00602008
    RX Filter Cntlr:            0xf8260150 = 0x00000000
    RX Chksum:                  0xf8265000 = 0x00000300
RX Descriptor Registers:
    RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
    RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
    RX Descriptor 0 Length:     0xf8262808 = 0x00001000
    RX Descriptor 0 Head:       0xf8262810 = 0x00000000
    RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
    RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
    RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
    RX Descriptor 1 Length:     0xf8260140 = 0x00000000
    RX Descriptor 1 Head:       0xf8260148 = 0x00000000
    RX Descriptor 1 Tail:       0xf8260150 = 0x00000000
TX Descriptor Registers:
    TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
    TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
    TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
    TX Descriptor 0 Length:     0xf8263808 = 0x00001000
    TX Descriptor 0 Head:       0xf8263810 = 0x00000000
    TX Descriptor 0 Tail:       0xf8263818 = 0x00000000
RX Address Array:
    Ethernet Address 0:         0012.d948.ef58
    Ethernet Address 1:         Not Valid!
    Ethernet Address 2:         Not Valid!
    Ethernet Address 3:         Not Valid!
    Ethernet Address 4:         Not Valid!
    Ethernet Address 5:         Not Valid!
    Ethernet Address 6:         Not Valid!
    Ethernet Address 7:         Not Valid!
    Ethernet Address 8:         Not Valid!
    Ethernet Address 9:         Not Valid!
    Ethernet Address a:         Not Valid!
    Ethernet Address b:         Not Valid!
    Ethernet Address c:         Not Valid!
    Ethernet Address d:         Not Valid!
    Ethernet Address e:         Not Valid!
    Ethernet Address f:         Not Valid!
PHY Registers:
    Phy Control:                0x1140
    Phy Status:                 0x7969
    Phy ID 1:                   0x0141
    Phy ID 2:                   0x0c25
    Phy Autoneg Advertise:      0x01e1
    Phy Link Partner Ability:   0x41e1
    Phy Autoneg Expansion:      0x0007
    Phy Next Page TX:           0x2801
    Phy Link Partnr Next Page:  0x0000
    Phy 1000T Control:          0x0200
    Phy 1000T Status:           0x4000
    Phy Extended Status:        0x3000
Detailed Output - RX Descriptor Ring:
rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
```

.....

次に、ASA 5512-X から ASA 5555-X までの内部インターフェイスに対する **show controller detail** コマンドの出力例を示します。

```
ciscoasa# show controller detail
Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0
Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap2
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0
```

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

```
Slot  Card Description                              PCI-e Bandwidth Cap.
----  ----------------                             ----------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x4, Card: x8
4.    ASA 5580 4 port GE Copper Interface Card       Bus: x4, Card: x4
5.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x8, Card: x8
6.    ASA 5580 4 port GE Fiber Interface Card        Bus: x4, Card: x4
7.    empty                                          Bus: x8
8.    empty                                          Bus: x8
```

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

```
ciscoasa# show controller
            pci
PCI Evaluation Log:
  ------------------------------------------------------------------------------
    Empty
```

```
PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
-------------------------------------------------------------------------------
  PCI Configuration Space (hex):
  0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
  0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
  0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
  0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
  0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
  0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
  0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
  0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
  0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  Link Capabilities: x4, Gen1
  Link Status: x4, Gen1
```

以下は、ASA 仮想 からの例です。この場合、rx_dropped_packets は、パケットが ASA 仮想 に入る前に VM レベルでドロップされていることを示します（多くの場合、帯域幅不足が原因）。考えられる原因の一つは、VM が処理できる範囲を超えた VM 宛てのトラフィックのブラスト/バーストが存在することです。

```
ciscoasa# show controller TenGigabitEthernet 0/2

TenGigabitEthernet0/2:
   DPDK Statistics
                 rx_good_packets : 13186640462
                 tx_good_packets : 3225386
                   rx_good_bytes : 12526548356100
                   tx_good_bytes : 383943970
                       rx_errors : 0
                       tx_errors : 0
       rx_mbuf_allocation_errors : 0
                    rx_q0packets : 0
                      rx_q0bytes : 0
                     rx_q0errors : 0
                    tx_q0packets : 0
                      tx_q0bytes : 0
                        rx_bytes : 12526548273860
             rx_unicast_packets : 13186630349
           rx_multicast_packets : 10025
           rx_broadcast_packets : 0
             rx_dropped_packets : 15357499
     rx_unknown_protocol_packets : 0
                        tx_bytes : 383943970
             tx_unicast_packets : 3224181
           tx_multicast_packets : 1205
           tx_broadcast_packets : 0
             tx_dropped_packets : 0
               tx_error_packets : 0
```

関連コマンド

コマンド	説明
show interface	インターフェイス統計情報を表示します。

コマンド	説明
show tech-support	Cisco TAC による問題の診断を可能にするような情報を表示します。

show coredump filesystem

コアダンプ ファイル システムの内容を表示するには、show coredump filesystem コマンドを入力します。

show coredump filesystem

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

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コアダンプ ファイル システムの内容を表示します。

例

次に、show coredump filesystem コマンドを入力して、最近生成された任意のコアダンプの内容を表示する例を示します。

```
ciscoasa(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

関連コマンド

コマンド	説明
coredump enable	コアダンプ機能をイネーブルにします。

コマンド	説明
clear configure coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
clear coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
show coredump log	コアダンプ ログを表示します。

show coredump log

コアダンプログの内容を新しい順に表示するには、**show coredump log** コマンドを入力します。コアダンプログの内容を古い順に表示するには、**show coredump log reverse** コマンドを入力します。

show coredump log
show coredump log [**reverse**]

構文の説明

reverse	最も古いコアダンプログを表示します。

コマンド デフォルト

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コアダンプログの内容を表示します。ログは、現在ディスク上にあるものを反映しています。

例

次に、これらのコマンドの出力例を示します。

```
ciscoasa(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
 file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
 file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

（注） 新しいコアダンプ用の領域を確保するため、古いコアダンプ ファイルは削除されます。これは、コアダンプファイルシステムがいっぱいになり、現在のコアダンプ用の領域が必要になった場合に、ASA によって自動的に行われます。このため、クラッシュが発生してコアダンプが上書きされないように、できるだけ早くコアダンプをアーカイブすることが不可欠となります。

ciscoasa(config)# show coredump log reverse

```
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
 file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
 file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

関連コマンド

コマンド	説明
coredump enable	コアダンプ機能をイネーブルにします。
clear configure coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
clear coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
show coredump filesystem	コアダンプ ファイル システムの内容を表示します。

show counters

プロトコルスタックカウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [**all** | **context** *context-name* | **summary** | `top` *N*] [**detail**] [**protocol** *protocol_name* [**:** *counter_name*]] [**threshold** *N*]

構文の説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

show counters summary detail threshold 1

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。
9.2(1)	イベント マネージャのカウンタが追加されました。

リリース	変更内容
9.13(1)	Firepower 1000 および 2100 のアプライアンスモードに新しいカウンタ「HTTPERR」が追加されました。これは、FXOS への HTTP 要求メッセージタイムアウトの数を表します。
9.12(1)	ACL 検索レベル用に新しいカウンタが 5 つ追加されました。 • OBJGRP_SEARCH_THRESHOLD（検索数 10000 のしきい値超過） • OBJGRP_SEARCH_THRESHOLD_LEVEL4（検索数 7500 ～ 10000） • OBJGRP_SEARCH_THRESHOLD_LEVEL3（検索数 5000 ～ 7500） • OBJGRP_SEARCH_THRESHOLD_LEVEL2（検索数 2500 ～ 5000） • OBJGRP_SEARCH_THRESHOLD_LEVEL1（検索数 1 ～ 2500）

例

次に、すべてのカウンタを表示する例を示します。

```
ciscoasa#

show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf
ciscoasa# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
UAUTH        IPV6_UNSUPPORTED     27   Summary
IDFW         HIT_USER_LIMIT        2   Summary
```

次に、カウンタの要約を表示する例を示します。

```
ciscoasa#

show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

次に、コンテキストのカウンタを表示する例を示します。

```
ciscoasa# show counters context single_vf
Protocol     Counter           Value   Context
```

```
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

次に、イベント マネージャのカウンタを表示する例を示します。

```
ciscoasa# show counters protocol eem
Protocol     Counter           Value   Context
EEM          SYSLOG            22      Summary
EEM          COMMANDS          6       Summary
EEM          FILES             3       Summary
```

次に、ACL 検索レベルのカウンタを表示する方法の例を示します。

```
ciscoasa# show counters
Protocol     Counter
Value   Context
ACL          OBJGRP_SEARCH_THRESHOLD                                  1582   Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL4                    534    Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL3                    524    Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL2                    307    Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL1                    216    Summary
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで show cpu コマンドを使用します。

［ **cluster exec** ］**show cpu** ［ **usage** *core-id* **| profile | dump | detailed** ］

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

［ **cluster exec** ］**show cpu** ［ **usage** ］［ **context** { **all** | *context_name* }］

構文の説明

all	すべてのコンテキストを表示することを指定します。
cluster exec	（任意）クラスタリング環境では、あるユニットで **show cpu** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
context	1 つのコンテキストを表示することを指定します。
context_name	表示するコンテキストの名前を指定します。
core-id	プロセッサ コアの数を指定します。
detailed	（オプション）CPU の内部使用に関する詳細な情報を表示します。
dump	（オプション）TTY にダンプ プロファイリング データを表示します。
profile	（オプション）CPU プロファイリング データを表示します。
usage	（任意）CPU 使用状況を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために、*core-id* オプションが追加されました。
9.1(2)	**show cpu profile** コマンドと **show cpu profile dump** コマンドの出力が更新されました。
9.2(1)	仮想プラットフォームの CPU 使用状況が ASA 仮想 の出力に追加されました。

使用上のガイドライン

CPU 使用状況は、5 秒ごとの負荷の近似値を使用し、この概算値をさらに以降の 2 つの移動平均に適用することによって算出されます。

show cpu コマンドを使用すると、プロセス関連の負荷を検出できます（つまり、**show process** コマンドを、シングルモードとマルチコンテキストモードのシステム コンフィギュレーションの両方で実行した場合に表示される項目の代わりに、アクティビティを表示できます）。

さらに、マルチコンテキストモードでは、プロセス関連負荷を分散するよう、設定されたすべてのコンテキストで消費される CPU に要求できます。このためには、各コンテキストに変更して **show cpu** コマンドを入力するか、**show cpu context** コマンドを入力します。

プロセス関連の負荷は、最も近い整数に丸められますが、コンテキスト関連の負荷の場合は精度を表す 10 進数が 1 つ追加されます。たとえば、**show cpu** コマンドをシステムコンテキストから入力すると、**show cpu context system** コマンドを入力した場合とは異なる数値が示されます。前者は **show cpu context all** コマンドで表示される要約とほぼ同じですが、後者はその要約の一部にすぎません。

show cpu profile dump コマンドを **cpu profile activate** コマンドとともに使用して、CPU 問題のトラブルシューティング時に TAC が使用する情報を収集できます。**show cpu profile dump** コマンドの出力は、16 進形式で表示されます。

CPU プロファイラが開始条件の発生を待機している場合、**show cpu profile** コマンドは次の出力を表示します。

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

ASA 仮想 に関して、次のライセンス ガイドラインに注意してください。

- 許可される vCPU の数は、インストールされている vCPU プラットフォーム ライセンスによって決定されます。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数と一致する場合、状態は Compliant になります。

- ライセンス vCPU の数が、プロビジョニングされた vCPU の数を下回る場合、状態は Noncompliant: Over-provisioned になります。
- ライセンス vCPU の数が、プロビジョニングされた vCPU の数を超える場合、状態は Compliant: Under-provisioned になります。

- メモリ制限は、プロビジョニングされた vCPU の数によって決定されます。
  - プロビジョニングされたメモリが上限にある場合、状態は Compliant になります。
  - プロビジョニングされたメモリが上限を超える場合、状態は Noncompliant: Over-provisioned になります。
  - プロビジョニングされたメモリが上限を下回る場合、状態は Compliant: Under-provisioned になります。

- 周波数予約制限は、プロビジョニングされた vCPU の数によって決定されます。
  - 周波数予約メモリが必要最低限（1000 MHz）以上である場合、状態は Compliant になります。
  - 周波数予約メモリが必要最低限（1000 MHz）未満である場合、状態は Compliant: Under-provisioned になります。

たとえば、次の出力は、ライセンスが適用されていないことを示します。許可される vCPU の数はライセンスされた数を示し、Noncompliant: Over-provisioned は、製品がライセンスされたリソースよりも多いリソースを使用して実行されていることを示しています。

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

復号化する場合は、この情報をコピーし、TAC に提供します。

（注） ASA が FXOS シャーシで実行されている場合、 **show cpu** コマンドの出力に表示される CPU コアの数が、Firepower 4100 プラットフォームや 9300（FXOS ベース）プラットフォームなど、一部のプラットフォームの **show version** コマンドの出力に表示される数よりも少ないことがあります。

動的なハイパースレッディングのサポートの導入により、Firepower 4100 プラットフォームおよび 9300 プラットフォームでの **show cpu** コマンドの出力が変更されました。トラフィックのスループットが低い場合、 **show cpu [detailed | core | external]** CLI の出力は、スタンドアロンの ASA 出力に表示されるものと異なります。CPU ハイパースレッディング機能がディセーブルになっている場合、CPU コアの使用状況出力の後半部分は低くなります。ASA トラフィックのスループットがしきい値の上限を超えている場合、CPU ハイパースレッディング機能をイ

ネーブルにすると **show cpu** コマンドがスタンドアロンの ASA と同じ出力を表示するようになります。

例

次に、CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次に、CPU の使用状況に関する情報を表示する例を示します。カッコ内に示されているように、コアごとの情報は（データパスの使用量+コントロールプレーンの使用量）の合計であることに注意してください。

```
ciscoasa# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

（注） 「Current control point elapsed versus the maximum control point elapsed for」という文は、コントロール ポイントの現在の負荷が、定義された期間内に検出された最大負荷と比較されることを意味します。これは絶対値ではなく比率です。5 秒間隔に対して 99% という数値は、コントロール ポイントの現在の負荷が、その 5 秒間隔における最大負荷の 99% であることを意味します。負荷が常に増加し続ける場合、負荷は常に 100% になります。ただし、最大絶対値が定義されていないため、実際の CPU には引き続き多くの空き容量がある可能性があります。この数値は、そのコアに関する「コントロールプレーンの使用量」の数値の合計ではないことに注意してください。

次に、マルチ モードでシステム コンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次に、すべてのコンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次に、「one」というコンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

次の例では、プロファイラをアクティブ化して、1000 個のサンプルを格納するように指示します。

```
ciscoasa# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

次に、プロファイリングのステータス（in-progress および completed）の例を示します。

```
ciscoasa# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
ciscoasa# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2
Process virtual address map:
---------------------------
...
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

次に、ASA 仮想 の CPU 使用状況の例を示します。

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
Virtual platform CPU resources
------------------------------
Number of vCPUs              :     2
Number of allowed vCPUs      :     2
vCPU Status                  :  Compliant
Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  4000 MHz
Maximum allowed              :  56000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :   136 MHz
```

次に、ASA 仮想 の CPU 使用状況の詳細の例を示します。

```
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.2 (0.2 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.1 (0.0 + 0.1)  0.0 (0.0 + 0.0)
Current control point elapsed versus the maximum control point elapsed for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%
CPU utilization of external processes for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
     5 seconds = 0.1%; 1 minute: 0.1%; 5 minutes: 0.1%
```

```
Virtual platform CPU resources
------------------------------
Number of vCPUs               :     4
Number of allowed vCPUs       :     4
vCPU Status                   :  Compliant
Frequency Reservation         :  1000 MHz
Minimum required              :  1000 MHz
Frequency Limit               :  20000 MHz
Maximum allowed               :  20000 MHz
Frequency Status              :  Compliant
Average Usage (30 seconds)    :    99 MHz
```

ASA バージョン 9.6.1 以降、コントロールポイント（CP）の処理用に 2 つまたは 4 つのコアが選択され、使用可能なすべてのコアに CP が広がらないよう実行できるコア CP の数を制限します。トラフィック負荷がない場合でも、CP 処理用に選択されたコアは CPU ピンニングに一定の負荷がかかります。また、データパス（DP）スレッドをチェックするために各コアで DP をポーリングします。この負荷は **show cpu core** 出力には含まれていますが、 **show cpu detail** 出力では除外されています。これは、show cpu detail によって CP および DP の負荷がチェックされるためです。

（注） Cisco Secure Firewall 4200 シリーズ デバイスでは、コア 0 はコントロールポイント専用となり、他のコアはデータパスプロセスの実行に使用されます。

例

次の例に、 **show cpu core** および **show cpu detail** コマンドの出力に含まれるさまざまな CPU 使用率値（Core 0 および Core 2）を示します。

```
ciscoasa(config)# show cpu core
Core 5 sec 1 min 5 min
Core 0 18.0% 18.0% 18.0%
Core 1 0.0% 0.0% 0.0%
Core 2 18.6% 18.5% 18.6%
Core 3 0.0% 0.0% 0.0%
ciscoasa(config)# show cpu detail
Break down of per-core data path versus control point cpu usage:
Core 5 sec 1 min 5 min
Core 0 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
Core 1 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
Core 2 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
Core 3 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPUプロファイリングをアクティベートします。

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