show aa ～ show asr

show aaa kerberos

Kerberos サービス情報を表示するには、特権 EXEC モードで **show aaa kerberos** コマンドを使用します。

show aaa kerberos [**username** *user*] | **keytab**]

構文の説明

keytab	Kerberos キータブファイルに関する情報を表示します。
username ユーザー	指定されたユーザーのチケットを表示します。

コマンド デフォルト

キーワードを指定しない場合、すべてのユーザーのチケットが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

ASA にキャッシュされたすべての Kerberos チケットを表示するには、キーワードを指定せずに **show aaa kerberos** コマンドを使用します。特定のユーザーの Kerberos チケットを表示するには、**username** キーワードを追加します。キータブファイルに関する情報を表示するには、**keytab** キーワードを使用する必要があります。

例

次に、**show aaa kerberos** コマンドの使用例を示します。

```
ciscoasa
(config)# show aaa kerberos
Default Principal      Valid Starting    Expires    Service Principalkcduser@example.com
       06/29/10 17:33:00     06/30/10 17:33:00
asa$/mycompany.com@example.comkcduser@example.com       06/29/10 17:33:00     06/30/10
17:33:00    http/owa.mycompany.com@example.com
```

次に、Kerberos キータブファイルに関する情報を表示する例を示します。

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
```

関連コマンド

コマンド	説明
aaa kerberos import-keytab	Kerberos キー発行局（KDC）からエクスポートした Kerberos キータブファイルをインポートします。
clear aaa kerberos	キャッシュされた Kerberos チケットをクリアします。
show running-config aaa-server	AAA サーバーの設定を表示します。

show aaa local user

現在ロックされているユーザー名のリストを表示するか、またはユーザー名の詳細を表示するには、グローバル コンフィギュレーション モードで **aaa local user** コマンドを使用します。

show aaa local user [**locked**]

構文の説明

locked	（任意）現在ロックされているユーザー名のリストを表示します。

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
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
7.0(1)	このコマンドが追加されました。
9.17(1)	**Expired** と **New-User** の列を追加しました。

使用上のガイドライン

オプションのキーワード **locked** を省略すると、ASA によって、すべての AAA ローカルユーザーの失敗試行およびロックアウトステータスの詳細が表示されます。

このコマンドは、ロックアウトされているユーザーのステータスだけに影響します。

ユーザーは 10 分後にロックが解除されます。ただし、再度ログインに成功するまでは、このコマンドの出力には、10 分以上経過してもユーザーがロックされていると表示されます。

例

次に、**show aaa** コマンドを使用して、すべてのユーザー名のロックアウトステータスを表示する例を示します。

次に、制限を 5 回に設定した後に **show aaa local user** コマンドを使用して、すべての AAA ローカルユーザーの失敗した認証試行回数およびロックアウトステータスの詳細を表示する例を示します。

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
```

```
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                   6      N            N           Y           cas
    -                   2      N            Y           N           sam
    -                   1      N            Y           N           dean
    -                   4      N            N           N           admin
ciscoasa(config)#
```

次に、制限を 5 回に設定した後に **lockout** キーワードを指定して **show aaa local user** コマンドを使用し、ロックアウトされている AAA ローカルユーザーのみの失敗した認証試行回数およびロックアウトステータスの詳細を表示する例を示します。

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                   6      N            N           Y           cas
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザーが何回誤ったパスワードを入力するとロック アウトされるかを示す最大回数を設定します。
clear aaa local user fail-attempts	ロックアウト ステータスを変更しないで、失敗試行回数を 0 にリセットします。
clear aaa local user lockout	指定したユーザーまたはすべてのユーザーのロックアウト ステータスをクリアして、それらのユーザーの失敗試行カウンタを 0 に設定します。

show aaa login-history

ログイン履歴を表示するには、特権 EXEC モードで **show aaa login-history** コマンドを使用します。

show aaa login-history [**user** *name*]

構文の説明

user *name*	（オプション）特定のユーザーのログイン履歴を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

デフォルトでは、1 つ以上の CLI 管理方式（SSH、Telnet、シリアルコンソール）でローカル AAA 認証をイネーブルにした場合、ASA はローカルデータベースのユーザー名または AAA サーバーからのユーザー名を保存します。ログイン履歴を表示するには、**show aaa login-history** コマンドを使用します。履歴存続期間を設定するには、 **aaa authentication login-history** コマンドを参照してください。

ASDM のログインは履歴に保存されません。

ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。

ログインの履歴データは、リロードされると保持されなくなります。

例

次に、ログイン履歴を表示する例を示します。

```
ciscoasa(config)# show aaa login-history
Login history for user:                              cisco
Logins in last   1 days:                             45
Last successful login:                               14:07:28 UTC Aug 21 2018 from
10.86.190.50
Failures since last login:                           0
Last failed login:                                   None
Privilege level:                                     14
Privilege level changed from 11 to 14 at:            14:07:30 UTC Aug 21 2018
```

関連コマンド

コマンド	説明
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。
password-history	直前の **username** パスワードを保存します。ユーザーはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザーを設定します。

show aaa sdi node-secrets

システムにインストールされている SDI ノードシークレットファイルに関する情報を表示するには、特権 EXEC モードで **show aaa sdi node-secrets** コマンドを使用します。

show aaa sdi node-secrets

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	—

使用上のガイドライン

show aaa sdi node-secrets コマンドを使用すると、ノードシークレットファイルがシステムにインストールされている RSA SecurID サーバーのリストが表示されます。ノードシークレットファイルは RSA Authentication Manager からエクスポートされ、 **aaa sdi import-node-secret** コマンドを使用してシステムにアップロードされます。ノードシークレットファイルを削除するには、 **clear aaa sdi node-secret** コマンドを使用します。

例

次に、システムにノードシークレットファイルがインストールされている SecurID サーバーを表示する例を示します。

```
ciscoasa
#
show aaa sdi node-secrets

Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.cisco.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa
#
```

関連コマンド

コマンド	説明
aaa sdi import-node-secret	RSA Authentication Manager からエクスポートされたノードシークレットファイルをインポートします。
clear aaa sdi node-secret	ノードシークレットファイルを削除します。

show aaa-server

AAA サーバーの AAA サーバー統計情報を表示するには、特権 EXEC モードで **show aaa-server** コマンドを使用します。

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

構文の説明

LOCAL	（任意）ローカル ユーザー データベースの統計情報を表示します。
groupname	（任意）グループ内のサーバーの統計情報を表示します。
host *hostname*	（任意）グループ内の特定のサーバーの統計情報を表示します。
protocol *protocol*	（オプション）以下からプロトコルを指定して、サーバーの統計情報を表示します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

コマンド デフォルト

デフォルトで、すべての AAA サーバー統計情報が表示されます。

コマンド 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
7.1(1)	http-form プロトコルが追加されました。
8.0(2)	**aaa-server active** コマンドまたは **fail** コマンドを使用して手動でステータスが変更されたかどうかがサーバーステータスに表示されるようになりました。

例

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

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

次の表に、 **show aaa-server** コマンド出力のフィールドの説明を示します。

フィールド	説明
Server Group	**aaa-server** コマンドによって指定されたサーバーグループ名。
[サーバー プロトコル（Server Protocol）]	**aaa-server** コマンドによって指定されたサーバーグループのサーバープロトコル。
Server Address	AAA サーバーの IP アドレス。
Server port	ASA および AAA サーバーによって使用される通信ポート。RADIUS 認証ポートは、 **authentication-port** コマンドを使用して指定できます。RADIUS アカウンティングポートは、 **accounting-port** コマンドを使用して指定できます。非 RADIUS サーバーでは、ポートは **server-port** コマンドによって設定されます。

フィールド	説明
Server status	サーバーのステータス。次のいずれかの値が表示されます。 • ACTIVE：ASA はこの AAA サーバーと通信します。 • FAILED：ASA はこの AAA サーバーと通信できません。この状態になったサーバーは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。 ステータスの後に「(admin initiated)」と表示されている場合、このサーバーは、 **aaa-server active** コマンドまたは **fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。 最終トランザクション日時を次の形式で示します。 **Last transaction (** {**success** | **failure** }**)** **at** *time timezone date* ASA がサーバーと通信したことがない場合は、次のメッセージが表示されます。 **Last transaction at Unknown**
Number of pending requests	現在進行中の要求数。
Average round trip time	サーバーとのトランザクションを完了するまでにかかる平均時間。
Number of authentication requests	ASA によって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。
Number of authorization requests	認可要求数。この値は、コマンド認可、コンピュータを通過するトラフィック（TACACS+ サーバーの場合）の認可、トンネルグループでイネーブルにされた WebVPN および IPsec 認可機能が原因の認可要求を指します。タイムアウト後の再送信は、この値には含まれません。
Number of accounting requests	アカウンティング要求数。タイムアウト後の再送信は、この値には含まれません。
Number of retransmissions	内部タイムアウト後にメッセージが再送信された回数。この値は、Kerberos および RADIUS サーバー（UDP）にのみ適用されます。

フィールド	説明
Number of accepts	成功した認証要求数。
Number of rejects	拒否された要求数。この値には、エラー状態、および実際にクレデンシャルがAAAサーバーから拒否された場合の両方が含まれます。
Number of challenges	最初にユーザー名とパスワードの情報を受信した後に、AAA サーバーがユーザーに対して追加の情報を要求した回数。
Number of malformed responses	該当なし。将来的な使用のために予約されています。
Number of bad authenticators	次のいずれかが発生した回数。 • RADIUSパケットの「authenticator」ストリングが破損している（まれなケース）。 • ASAの共有秘密キーとRADIUSサーバーの共有秘密キーが一致しない。この問題を修正するには、正しいサーバーキーを入力します。 この値は、RADIUS にのみ適用されます。
Number of timeouts	ASA が、AAA サーバーが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。
Number of unrecognized responses	認識できない応答またはサポートしていない応答を ASA が AAA サーバーから受信した回数。たとえば、サーバーからのRADIUSパケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバーからのRADIUS 応答パケットが破損していることを意味していますが、まれなケースです。

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバー グループ内のすべてのサーバー、または特定のサーバーの統計情報を表示します。
clear aaa-server statistics	AAA サーバー統計情報をクリアします。

show access-list

アクセスリストのヒットカウンタおよびタイムスタンプ値を表示するには、特権EXECモードで **show access-list** コマンドを使用します。

show access-list [*id* [*ip_address* | **brief** | **numeric**] | **element-count**]

構文の説明

brief	（任意）アクセス リスト ID、ヒット カウント、および最終ルール ヒットのタイムスタンプをすべて 16 進形式で表示します。
id	（オプション）既存のアクセス リストの ID のカウンタを表示します。
ip_address	（オプション）指定したアクセスリスト内の送信元IPアドレスまたはホスト名のカウンタを表示します。
numeric	（任意）ACL名を指定すると、ポートが名前ではなく数値で表示されます。たとえば、www ではなく 80 と表示されます。
element-count	（任意）システムで定義されているすべてのアクセスリストのアクセスコントロール エントリの総数を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	**brief** キーワードのサポートが追加されました。
8.3(1)	ACL タイムスタンプを表示するための ACE 表示パターンが変更されました。
9.14(1)	**numeric** および **element-count** キーワードが追加されました。
9.17(1)	システムコンテキストのサポートが追加され、すべてのコンテキストで設定されているすべてのアクセスリストの要素カウントが表示されるようになりました。さらに、オブジェクトグループ検索が有効になっている場合、要素カウントの出力にオブジェクトグループの内訳も含まれます。

使用上のガイドライン

brief キーワードを指定して、アクセス リスト ヒット カウント、ID、およびタイムスタンプ情報を 16 進形式で表示できます。16 進形式で表示されるコンフィギュレーション ID は、3 列に表示され、Syslog 106023 および 106100 で使用されるものと同じ ID です。

アクセス リストが最近変更された場合、リストは出力から除外されます。この場合は、メッセージにそのことが示されます。

（注） 出力には、ACL に含まれる要素の数が表示されます。この番号は、必ずしも ACL 内のアクセス コントロール エントリ (ACE) の数と同じではありません。たとえば、アドレス範囲をもつネットワーク オブジェクトを使用する場合、システムは追加の要素を作成することがありますが、これらの追加要素は出力に含まれません。

クラスタリングのガイドライン

ASA クラスタリングを使用する場合、トラフィックが単一のユニットにより受信された場合でも、クラスタリングのダイレクタ ロジックにより、その他のユニットは ACL のヒット カウントを示す場合があります。これは予期された動作です。クライアントから直接パケットを受信しなかったユニットは、所有者要求に応じてクラスタ制御リンクを介して転送されたパケットを受信することがあるため、ユニットはパケットを受信ユニットに戻す前に ACL をチェックすることがあります。このため、トラフィックがユニットを通過しなかった場合でも ACL ヒット カウントが増分されます。

例

次に、16 進形式で指定されたアクセス ポリシー（ヒット カウントがゼロではない ACE）に関する簡単な情報の例を示します。最初の 2 列には、ID が 16 進形式で表示され、3 番めの列にはヒット カウントがリストされ、4 番めの列には、タイムスタンプ値が 16 進形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。タイムスタンプ値は、最終ヒットの時刻を報告します。ヒット カウントがゼロの場合、情報は表示されません。

次に、 **show access-list** コマンドの出力例を示します。これは、「IN」方向の outside インターフェイスに適用される、アクセスリスト名「test」を示します。

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

次に、 **object-group-search** グループがイネーブルになっていない場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
```

```
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

次に、**object-group-search** グループがイネーブルになっている場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
 BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21
 44ae5901 00000001 4a68aa7e
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158
 44ae5901 00000001 4a68aaa9
```

次に、**show access-list** コマンドの出力例を示します。これは、ACL 最適化がイネーブルになっている、「IN」方向の outside インターフェイスに適用される、アクセスリスト名「test」を示します。

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
```

```
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
ssh (hitcnt=1) 0x3666f922
```

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660
 44ae5901 00000001 4a68ab51
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922
 44ae5901 00000001 4a68ab66
```

次に、システムで定義されているすべてのアクセスリストのアクセスコントロールエントリの総数である要素カウントの例を示します。アクセスグループとして割り当てられているアクセスリストの場合、アクセスをグローバルに、またはインターフェイス上で制御するために、 **object-group-search access-control** コマンドを使用してオブジェクトグループ検索をイネーブルにすることで、要素カウントを減らすことができます。オブジェクトグループ検索をイネーブルにすると、ネットワークオブジェクトがアクセスコントロールエントリで使用されます。それ以外の場合、オブジェクトはそのオブジェクトに含まれる個々の IP アドレスに展開され、送信元/宛先アドレスのペアごとに個別のエントリが書き込まれます。したがって、5 つの IP アドレスを持つ送信元ネットワークオブジェクトと 6 つのアドレスを持つ宛先オブジェクトを使用する単一のルールは、1 つではなく 30 の要素（5 x 6 エントリ）に展開されます。要素カウントが多いほど、アクセスリストが大きくなり、パフォーマンスに影響を与える可能性が高くなります。

```
asa(config)# show access-list element-count

Total number of access-list elements: 33934
```

9.17(1) 以降では、オブジェクトグループ検索を有効にしている場合、ルールに含まれるオブジェクトグループの数（OBJGRP）、送信元オブジェクト（SRC OBJ）と宛先オブジェクト（DST OBJ）の数、および追加されたグループと削除されたグループの数に関する追加情報が提供されます。

```
ciscoasa/act/ciscoasactx001(config)# show access-list element-count
Total number of access-list elements: 892

OBJGRP     SRC OG     DST OG     ADD OG     DEL OG
842        842        842        842        0
```

マルチコンテキストモードでは、システムコンテキストで element-count キーワードを使用すると、すべてのコンテキストに統計が適用され、システム全体のカウントの要約が表示されます。オブジェクトグループ検索が有効な場合、アクセス コントロール エントリ（ACE）の総数、オブジェクト（OBJGRP）の数、および送信元（SRC）と宛先（DST）のオブジェクトグループの数が含まれます。オブジェクトグループ検索が無効な場合、オブジェクトカウントは常に 0 になります。次に、オブジェクトグループ検索を有効にしている場合のシステムコンテキストの例を示します。

```
ciscoasa/act(config)# show access-list element-count

Context Name            ACE        OBJGRP     SRC OG     DST OG
system                  0          0          0          0
admin                   0          0          0          0
ciscoasactx001          892        842        842        842
ciscoasactx002          312        298        298        298
ciscoasactx003          398        306        306        306
ciscoasactx004          162        132        132        132
ciscoasactx005          1280       583        583        583
ciscoasactx006          352        345        345        345
ciscoasactx007          353        351        351        351
ciscoasactx008          348        346        346        346
ciscoasactx009          433        420        420        420
ciscoasactx010          342        340        340        340
ciscoasactx011          363        361        361        361
ciscoasactx012          409        406        406        406
ciscoasactx013          381        373        373        373
ciscoasactx014          332        330        330        330
ciscoasactx015          465        374        374        374
ciscoasactx016          444        316        316        316
ciscoasactx017          284        268        268        268
sciscoasactx018         8837       0          0          0
ciscoasactx019          467        412        412        412
ciscoasactx020          934        527        527        527
ciscoasactx021          415        401        401        401
ciscoasactx022          676        562        562        562
ciscoasactx023          1208       1099       1099       1099
ciscoasactx024          350        322        322        322
ciscoasactx025          638        252        252        252
ciscoasactx026          318        304        304        304
ciscoasactx027          359        308        308        308
ciscoasactx028          1249       1087       1087       1087
ciscoasactx029          451        326        326        326
ciscoasactx030          377        315        315        315
ciscoasactx031          445        418        418        418
ciscoasactx032          347        309        309        309
ciscoasactx033          583        317        317        317
ciscoasactx034          340        311        311        311
ciscoasactx035          350        301        301        301

 Total access-list elements in all Context: 25894
```

関連コマンド

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show activation-key

永続ライセンス、アクティブな時間ベースのライセンス、および永続ライセンスとアクティブな時間ベースのライセンスの組み合わせである実行ライセンスを表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。フェールオーバー ユニットでは、このコマンドによって、プライマリおよびセカンダリ ユニットの結合キーである、「フェールオーバー クラスタ」ライセンスも表示されます。

show activation-key［ **detail** ］

構文の説明

detail	非アクティブな時間ベース ライセンスを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	**detail** キーワードが追加されました。
8.2(1)	出力が変更されて、追加のライセンス情報が含まれるようになりました。
8.3(1)	出力に、機能で使用されるのが永続キーまたは時間ベース キーのいずれであるか、および使用中の時間ベース キーの期間が含まれるようになりました。インストールされているすべての時間ベース キー（アクティブと非アクティブの両方）も表示されます。
8.4(1)	ペイロード暗号化機能のないモデルのサポートが追加されました。

使用上のガイドライン

一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。<xref> に、リロードが必要なライセンスを示します。

表 *1:* 永続ライセンスのリロード要件

モデル	リロードが必要なライセンスアクション
すべてのモデル	暗号化ライセンスのダウングレード
ASA 仮想	vCPU ライセンスのダウングレード

リロードが必要な場合は、 **show activation-key** 出力は次のようになります。

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN およびユニファイド コミュニケーション ライセンスはリストに示されません。

例

例 2-1： **show activation-key** コマンドのスタンドアロンユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベースライセンスの組み合わせ）、およびアクティブな各時間ベースライセンスを示す、スタンドアロンユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key
Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual
This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
```

```
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

例 2-2：**show activation-key detail** のスタンドアロンユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベースライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベースライセンス（アクティブおよび非アクティブ）を示す、スタンドアロンユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail
Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5505 Security Plus license.
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual
```

```
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

例 2-3：**show activation-key detail** に対するフェールオーバーペアのプライマリユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail
Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
```

```
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Enabled        perpetual
Security Contexts               : 12             perpetual
GTP/GPRS                        : Enabled        perpetual
AnyConnect Premium Peers        : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 4              perpetual
            Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter           : Enabled        33 days
Intercompany Media Engine       : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces     : Unlimited      perpetual
Maximum VLANs                   : 150            perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Disabled       perpetual
Security Contexts               : 2              perpetual
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days
Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days
0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

例 2-4：show activation-key detail に対するフェールオーバーペアのセカンダリユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。

- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASAで実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail
Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
            Security Contexts              : 10             perpetual
            GTP/GPRS                       : Enabled        perpetual
            AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
            Total UC Proxy Sessions        : 4              perpetual
            Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
```

```
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
The flash permanent activation key is the SAME as the running permanent key.
```

例 2-5：show activation-key に対する、ライセンスがない ASA 仮想 のスタンドアロンユニット出力

展開した 1 つの vCPU ASA 仮想 の次の出力は、空白のアクティベーション キー、ライセンスなしの状態、1 つの vCPU ライセンスをインストールするメッセージを示しています。

（注） このコマンド出力には「This platform has an ASA 仮想 VPN Premium license.」が表示されます。このメッセージは、ASA仮想がペイロード暗号化を実行できることを示しており、ASA 仮想 の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:
Licensed features for this platform:
Virtual CPUs                   : 0              perpetual
Maximum Physical Interfaces    : 10             perpetual
Maximum VLANs                  : 50             perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
Encryption-DES                 : Enabled        perpetual
Encryption-3DES-AES            : Enabled        perpetual
Security Contexts              : 0              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers       : 2              perpetual
AnyConnect Essentials          : Disabled       perpetual
Other VPN Peers                : 250            perpetual
Total VPN Peers                : 250            perpetual
Shared License                 : Disabled       perpetual
AnyConnect for Mobile          : Disabled       perpetual
AnyConnect for Cisco VPN Phone : Disabled       perpetual
```

```
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

例 2-6：show activation-key に対する、vCPU 標準ライセンスを 4 つ所有する ASA 仮想 のスタンドアロンユニット出力

（注） このコマンド出力には「This platform has an ASA 仮想 VPN Premium license.」が表示されます。このメッセージは、ASA 仮想がペイロード暗号化を実行できることを示しており、ASA 仮想 の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key

Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
```

例 2-7：show activation-key に対する、vCPU Premium ライセンスを 4 つ所有する ASA 仮想 のスタンドアロンユニット出力

（注） このコマンド出力には「This platform has an ASA 仮想 VPN Premium license.」が表示されます。このメッセージは、ASA 仮想がペイロード暗号化を実行できることを示しており、ASA 仮想 の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

例 2-8：show activation-key に対する、フェールオーバーペアでの ASA サービスモジュールのプライマリユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key
```

```
erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a

Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

例 2-9：show activation-key に対する、フェールオーバーペアでの ASA サービスモジュールのセカンダリユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail
Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
```

```
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
```

例 2-10：クラスタでの show activation-key の出力

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
```

```
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 The flash permanent activation key is the SAME as the running permanent key.
Serial Number:  JMX1232L11M
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Running Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited  perpetual
Maximum VLANs                : 50         perpetual
Inside Hosts                 : Unlimited  perpetual
Failover                     : Disabled   perpetual
VPN-DES                      : Enabled    perpetual
VPN-3DES-AES                 : Enabled    perpetual
Security Contexts            : 0          perpetual
GTP/GPRS                     : Disabled   perpetual
SSL VPN Peers                : 2          perpetual
Total VPN Peers              : 250        perpetual
Shared License               : Disabled   perpetual
AnyConnect for Mobile        : Disabled   perpetual
AnyConnect for Linksys phone : Disabled   perpetual
AnyConnect Essentials        : Enabled    perpetual
Advanced Endpoint Assessment : Disabled   perpetual
UC Phone Proxy Sessions      : 12         62 days
Total UC Proxy Sessions      : 12         62 days
Botnet Traffic Filter        : Enabled    646 days

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
SSL VPN Peers           : 100         108 days
```

関連コマンド

コマンド	説明
activation-key	アクティベーションキーを変更します。

show ad-groups

Active Directory サーバーにリストされているグループを表示するには、特権 EXEC モードで **show ad-groups** コマンドを使用します。

show ad-groups *name*［ **filter** *string* ］

構文の説明

name	問い合わせる Active Directory サーバー グループの名前。
string	検索するグループ名の全体または一部を指定する、引用符で囲んだ問い合わせに含めるストリング。

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 モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは、グループの取得に LDAP プロトコルを使用する Active Directory サーバーに対してのみ適用されます。このコマンドを使用して、ダイナミック アクセス ポリシー AAA 選択基準に使用できる AD グループを表示します。

LDAP 属性タイプが LDAP の場合、ASA がサーバーからの応答を待機するデフォルト時間は 10 秒です。aaa-server ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用し、時間を調整できます。

（注） Active Directory サーバーに数多くのグループが含まれている場合は、サーバーが応答パケットに格納できるデータ量の制限に基づいて **show ad-groups command** の出力が切り捨てられることがあります。この問題を回避するには、 **filter** オプションを使用して、サーバーからレポートされるグループ数を減らします。

例

```
ciscoasa# show ad-groups LDAP-AD17
          Server Group    LDAP-AD17

          Group list retrieved successfully

          Number of Active Directory Groups       46

          Account Operators

          Administrators

          APP-SSL-VPN CIO Users

          Backup Operators

          Cert Publishers

          CERTSVC_DCOM_ACCESS

          Cisco-Eng

          DHCP Administrators

          DHCP Users

          Distributed COM Users

          DnsAdmins

          DnsUpdateProxy

          Doctors

          Domain Admins

          Domain Computers

          Domain Controllers

          Domain Guests

          Domain Users

          Employees

          Engineering

          Engineering1

          Engineering2

          Enterprise Admins

          Group Policy Creator Owners

          Guests

          HelpServicesGroup
```

次に、同じコマンドで **filter** オプションを使用した例を示します。

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter “Eng”
.

Server Group    LDAP-AD17

Group list retrieved successfully

Number of Active Directory Groups       4

Cisco-Eng

Engineering

Engineering1

Engineering2
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバーが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
group-search-timeout	グループのリストについて Active Directory サーバーからの応答を ASA が待機する時間を調整します。

show admin-context

現在管理コンテキストとして割り当てられているコンテキスト名を表示するには、特権EXECモードで **show admin-context** コマンドを使用します。

show admin-context

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 モード	• 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 admin-context** コマンドの出力例を示します。次の例では、「admin」という名前で、フラッシュのルートディレクトリに保存されている管理コンテキストが表示されています。

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

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。
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。
clear configure context	すべてのコンテキストを削除します。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

show alarm settings

ISA 3000 で各タイプのアラームの構成を表示するには、ユーザー EXEC モードで **show alarm settings** コマンドを使用します。

show alarm settings

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

例

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

```
ciscoasa> show alarm settings

Power Supply
         Alarm                  Disabled
         Relay                  Disabled
         Notifies               Disabled
         Syslog                 Disabled
Temperature-Primary
         Alarm                  Enabled
         Thresholds             MAX: 92C                MIN: -40C
         Relay                  Enabled
         Notifies               Enabled
         Syslog                 Enabled
Temperature-Secondary
         Alarm                  Disabled
         Threshold
         Relay                  Disabled
         Notifies               Disabled
         Syslog                 Disabled
Input-Alarm 1
         Alarm                  Enabled
```

```
        Relay                   Disabled
        Notifies                Disabled
        Syslog                  Enabled
Input-Alarm 2
        Alarm                   Enabled
        Relay                   Disabled
        Notifies                Disabled
        Syslog                  Enabled
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

show arp

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

show arp

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(8)/7.2(4)/8.0(4)	ダイナミック ARP の期間経過が表示に追加されました。

使用上のガイドライン

表示出力には、ダイナミック、スタティック、およびプロキシARPエントリが表示されます。ダイナミック ARPエントリには、ARPエントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARPエントリにはダッシュ（-）が、プロキシARPエントリには「alias」という状態が含まれています。

例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。

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

show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、特権 EXEC モードで **show arp-inspection** コマンドを使用します。

show arp-inspection

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。
9.7(1)	ルーテッドモードのサポートが追加されました。

例

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

```
ciscoasa# show arp-inspection
interface                arp-inspection         miss
-----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。

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

show arp rate-limit

ARP レート制限設定を表示するには、特権 EXEC モードで **show arp rate-limit** コマンドを使用します。

show arp rate-limit

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
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

arp rate-limit 設定を表示するには、このコマンドを使用します。

例

次に、毎秒 10000 として ARP レートを表示する例を示します。

```
ciscoasa# show arp rate-limit
arp rate-limit 10000
```

関連コマンド

コマンド	説明
arp rate-limit	ARP レート制限を設定します。

show arp statistics

ARP 統計情報を表示するには、特権 EXEC モードで show arp statistics コマンドを使用します。

show arp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 2 に、各フィールドの説明を示します。

***表 2 : show arp statistics* のフィールド**

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。

フィールド	説明
Maximum queued blocks	IPアドレスの解決を待機している間にARPモジュールにキューイングされた最大ブロック数。
Queued blocks	現在ARPモジュールにキューイングされているブロック数。
Interface collision ARPs received	すべてのASAインターフェイスで受信された、ASAインターフェイスの IP アドレスと同じ IP アドレスからの ARP パケット数。
ARP-defense gratuitous ARPs sent	ARP-Defense メカニズムの一環として ASA によって送信された Gratuitous ARP の数。
Total ARP retries	最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。
Unresolved hosts	現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。
Maximum unresolved hosts	最後にクリアされた後、または ASA の起動後に、ARP モジュールに存在した未解決ホストの最大数。

関連コマンド

コマンド	説明
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアして、値をゼロにリセットします。
show arp	ARP テーブルを表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp vtep-mapping

リモートセグメントドメインにある IP アドレスの VNI インターフェイスでキャッシュされた MAC アドレスとリモート VTEP IP アドレスを表示するには、特権 EXEC モードで **show arp vtep-mapping** コマンドを使用します。

show arp vtep-mapping

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
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、

ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

例

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

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MAC アドレス テーブル）を表示します。

コマンド	説明
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこのNVEインターフェイスに関連付けられているピアVTEP IPアドレスを表示します。
show vni vlan-mapping	VNIセグメントIDと、VLANインターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDPポートを設定します。デフォルトでは、VTEP送信元インターフェイスはUDPポート4789へのVXLANトラフィックを受け入れます。

show asdm history

ASDM 履歴バッファの内容を表示するには、特権 EXEC モードで **show asdm history** コマンドを使用します。

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

構文の説明

asdmclient	（任意）ASDM クライアント用にフォーマットされた ASDM 履歴データを表示します。
feature *feature*	（任意）履歴表示を指定した機能に制限します。 *feature* 引数には、次の値を指定できます。 • **all** ：すべての機能の履歴を表示します（デフォルト）。 • **blocks** ：システムバッファの履歴を表示します。 • **cpu** ：CPU 使用状況の履歴を表示します。 • **failover** ：フェールオーバーの履歴を表示します。 • **ids** ：IDS の履歴を表示します。 • **interface** *if_name* ：指定したインターフェイスの履歴を表示します。 *if_name* 引数は、 **nameif** コマンドで指定したインターフェイスの名前です。 • **memory** ：メモリ使用状況の履歴を表示します。 • **perfmon** ：パフォーマンス履歴を表示します。 • **sas** ：セキュリティ アソシエーションの履歴を表示します。 • **tunnels** ：トンネルの履歴を表示します。 • **xlates** ：変換スロット履歴を表示します。
snapshot	（任意）最後の ASDM 履歴データ ポイントのみを表示します。
view *timeframe*	（任意）履歴の表示を指定した期間に制限します。 *timeframe* 引数には、次の値を指定できます。 • **all** ：履歴バッファ内のすべての内容（デフォルト）。 • **12h** ：12 時間 • **5d** ：5 日 • **60m** ：60 分 • **10m** ：10 分

コマンド デフォルト

引数またはキーワードを指定しない場合は、すべての機能のすべての履歴情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、 **show pdm history** コマンドから **show asdm history** コマンドに変更されました。

使用上のガイドライン

show asdm history コマンドは、ASDM 履歴バッファの内容を表示します。ASDM 履歴情報を表示する前に、 **asdm history enable** コマンドを使用して、ASDM 履歴トラッキングをイネーブルにする必要があります。

例

次に、 **show asdm history** コマンドの出力例を示します。このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。

```
ciscoasa# show asdm history view 10m feature interface outside
Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

次に、**show asdm history** コマンドの出力例を示します。前の例と同様に、このコマンドでは、直近の10分間に収集された外部インターフェイスのデータに出力が制限されています。ただし、この例では、出力はASDMクライアント用にフォーマットされています。

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient
MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
...
```

次に、**show asdm history** コマンドで **snapshot** キーワードを指定した場合の出力例を示します。

```
ciscoasa# show asdm history view 10m snapshot
Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
```

```
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
```

```
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
```

```
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

関連コマンド

コマンド	説明
asdm history enable	ASDM 履歴トラッキングをイネーブルにします。

show asdm image

現在の ASDM ソフトウェア イメージ ファイルを表示するには、特権 EXEC モードで **asdm image** コマンドを使用します。

show asdm image

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)	このコマンドは、**show pdm image** コマンドから **show asdm image** コマンドに変更されました。

例

次に、**show asdm image** コマンドの出力例を示します。

```
ciscoasa# show asdm image
Device Manager image file, flash:/ASDM
```

関連コマンド

コマンド	説明
asdm image	現在の ASDM イメージファイルを指定します。

show asdm log_sessions

アクティブな ASDM ロギングセッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm log_sessions** コマンドを使用します。

show asdm log_sessions

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

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギングセッションを使用して、ASA から Syslog メッセージを取得します。各 ASDM ロギング セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect log_session** コマンドで使用して、指定したセッションを終了できます。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギングセッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

例

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

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect log_session	アクティブなASDMロギングセッションを終了します。

show asdm sessions

アクティブな ASDM セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm sessions** コマンドを使用します。

show asdm sessions

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)	このコマンドは、**show pdm sessions** コマンドから **show asdm sessions** コマンドに変更されました。

使用上のガイドライン

アクティブな各 ASDM セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect** コマンドで使用して、指定したセッションを終了できます。

例

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

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect	アクティブなASDMセッションを終了します。

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。