clf - cz

cluster disable

ユニットでクラスタリングを無効にするには、**cluster disable** コマンドを使用します。

cluster disable

コマンド履歴

リリース	変更内容
6.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、クラスタからクラスタユニットを手動で削除できます。このコマンドではクラスタリング設定は変更されないため、後で **cluster enable** コマンドを使用してクラスタに再追加できます。

例

次に、ユニットのクラスタリングを無効にする例を示します。

```
> cluster disable
```

関連コマンド

Command	説明
cluster enable	クラスタリングをイネーブルにします。
cluster master unit	新しいユニットをクラスタのマスターユニットとして設定します。
cluster remove unit	ユニットをクラスタから削除します。
show cluster info	クラスタ情報を表示します。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。

cluster enable

ユニットでクラスタリングを有効にするには、**cluster enable** コマンドを使用します。

cluster enable

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

最初にイネーブルにしたユニットについては、マスターユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバーであるため、そのユニットがマスターユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

例

次に、ユニットでクラスタリングを有効にする例を示します。

```
> cluster enable
```

関連コマンド

Command	説明
cluster disable	クラスタリングをディセーブルにします。
cluster master unit	新しいユニットをクラスタのマスターユニットとして設定します。
cluster remove unit	ユニットをクラスタから削除します。
show cluster info	クラスタ情報を表示します。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。

cluster exec

クラスタ内のすべてのユニット、または特定のメンバーに対してコマンドを実行するには、**cluster exec** コマンドを使用します。

cluster exec ［**unit** *unit_name*］ *command*

構文の説明

unit *unit_name*	（オプション）特定のユニットに対してコマンドを実行します。メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。
command	実行するコマンドを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバーにコピーするには、マスター ユニットで次のコマンドを入力します。

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャファイル名には、capture1_device1.pcap、capture1_device2.pcap などのようにユニット名が自動的に付加されます、この例では、device1 と device2 がクラスタユニット名です。

次の例では、**cluster exec show port-channel** summary コマンドの出力に、クラスタの各メンバーの EtherChannel 情報が表示されています。

```
> cluster exec show port-channel summary
primary(LOCAL):**********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
```

```
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

関連コマンド

Command	説明
cluster enable	ユニットでクラスタリングを有効にします。
cluster master unit	新しいユニットをクラスタのマスターユニットとして設定します。
cluster remove unit	ユニットをクラスタから削除します。
show cluster info	クラスタ情報を表示します。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。

cluster exec clear rule hits

クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットするには、**cluster exec clear rule hits** コマンドを使用します。

cluster exec clear rule hits ［*id*］

構文の説明

id	（オプション）ルールの ID。この引数を含めると、指定したルールのルールヒット情報のみがクリアされます。 ルール ID を識別するには、**show access-list** コマンドを使用します。ただし、このコマンドの出力にすべてのルールが表示されているわけではありません。次の URL で REST API GET 操作をトリガーすると、すべてのルールとルールの ID を確認できます。 • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

コマンド デフォルト

ルール ID を指定しない場合、すべてのルールのルールヒット情報がクリアされ、ゼロにリセットされます。

（注） このアクションは元に戻せないため、このコマンドの使用には注意が必要です。

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。

使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

例

すべてのルールヒット情報をクリアする例を次に示します。

```
> cluster exec clear rule hits
```

関連コマンド

Command	説明
show cluster rule hits	クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。
cluster exec show rule hits	クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。
show rule hits	アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。
clear rule hits	アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。

cluster exec show rule hits

クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示するには、**cluster exec show rule hits** コマンドを使用します。

cluster exec show rule hits ［*id* | **raw** | **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*］

構文の説明

id	（オプション）ルールの ID。この引数を含めると、表示される情報は指定されたルールに限定されます。 ルール ID を識別するには、**show access-list** コマンドを使用します。ただし、このコマンドの出力にすべてのルールが表示されているわけではありません。次の URL で REST API GET 操作をトリガーすると、すべてのルールとルールの ID を確認できます。 • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
raw	（任意）.csv 形式でルールヒット情報を表示します。
gt *#hit-count*	（任意）ヒットカウントが #hit-count より大きいすべてのルールを表示します。
lt *#hit-count*	（任意）ヒットカウントが #hit-count より小さいすべてのルールを表示します。
range *#hit-count1 #hit-count2*	（任意）#hit-count1 と #hit-count2 の間のヒットカウントを持つすべてのルールを表示します。

コマンド デフォルト

ルール ID を指定しない場合、すべてのルールのルールヒット情報が表示されます。

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。

使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

例

次に、クラスタの各ノードからのルールヒット情報を分離形式で表示する例を示します。

```
> cluster exec show rule hits
unit-1-1(LOCAL):*******************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019

268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019


unit-1-3:*************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435264            1                   06:54:43 Mar 8 2019     06:54:43 Mar 8 2019

268435265            1                   06:54:57 Mar 8 2019     06:54:57 Mar 8 2019


unit-1-2:*************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019

268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
```

関連コマンド

Command	説明
cluster exec clear rule hits	クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。
show cluster rule hits	クラスタのすべてのノードからアクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を集約形式で表示します。
show rule hits	アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。
clear rule hits	アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。

cluster master unit

新しいユニットをデバイスクラスタのマスターユニットとして設定するには、**cluster master unit** コマンドを使用します。

cluster master unit *unit_name*

構文の説明

unit_name	新しいマスター ユニットとなるローカル ユニット名を指定します。メンバー名を表示するには、**cluster master unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

メイン クラスタ IP アドレスへの再接続が必要になります。

例

次に、新しいマスターユニットとして **device2** を設定する例を示します。

```
> cluster master unit device2
```

関連コマンド

Command	説明
cluster enable	ユニットでクラスタリングを有効にします。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。
cluster remove unit	ユニットをクラスタから削除します。
show cluster info	クラスタ情報を表示します。

cluster remove unit

クラスタからユニットを削除するには、**cluster remove unit** コマンドを使用します。

cluster remove unit *unit_name*

構文の説明

unit_name	クラスタから削除するローカルユニット名を指定します。メンバー名を表示するには、**cluster remove unit ?** または **show cluster info** コマンドを入力します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

例

次に、ユニット名を確認してから、device2 をクラスタから削除する例を示します。

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

関連コマンド

Command	説明
cluster enable	ユニットでクラスタリングを有効にします。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。
cluster master unit	新しいユニットをクラスタのマスターユニットとして設定します。
show cluster info	クラスタ情報を表示します。

cluster reset-interface-mode

クラスタリングを無効にした後でクラスタユニットをスタンドアロンモードに変換するには、**cluster reset-interface-mode** コマンドを使用します。

cluster reset-interface-mode

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

cluster disable コマンドを使用して、最初にクラスタリングを無効にする必要があります。この **cluster reset-interface-mode** コマンドは 脅威に対する防御 の設定をクリアし、論理デバイスを再起動します。4100 シリーズの FXOS では、論理デバイスもスタンドアロンタイプのデバイスに変換されます。ブートストラップ設定とインターフェイスの割り当ては維持されます。

例

次に、クラスタリングを無効にしてから、クラスタリング設定を削除する例を示します。

```
> cluster disable
> cluster reset-interface-mode

Broadcast message from root@firepower (Tue Apr 27 18:36:12 2021):

The system is going down for reboot NOW!
```

関連コマンド

Command	説明
cluster enable	ユニットでクラスタリングを有効にします。
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。
cluster master unit	新しいユニットをクラスタのマスターユニットとして設定します。
show cluster info	クラスタ情報を表示します。

configure cert-update auto-update

脅威に対する防御デバイスでのCA証明書の自動更新を有効または無効にするには、**configure cert-update auto-update** コマンドを使用します。

configure cert-update auto-update { **enable** | **disable** }

構文の説明

enable	CA 証明書の自動更新を有効にします。
disable	CA 証明書の自動更新を無効にします。

コマンド履歴

リリース	変更内容
7.0.5	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、バージョン 7.0.5 をインストールまたは 脅威に対する防御 をアップグレードすると、CA 証明書が自動的に更新されます。この機能を無効にするには、**disable** キーワードを使用します。CA バンドルの自動更新を再度有効にするには、**enable** キーワードを使用します。CA 証明書の自動更新を有効にすると、更新プロセスはシステムで定義された時刻に毎日実行されます。

例

次に、**configure cert-update auto-update** コマンドの出力例を示します。

```
> configure cert-update auto-update disable
Autoupdate is disabled
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

関連コマンド

Command	説明
show cert-update	CA 証明書の自動更新のステータスを表示します。
configure cert-update run-now	CA 証明書の更新をすぐに試します。
configure cert-update test	シスコのサーバーからの最新のCA証明書を使用して接続チェックを実行します。

configure cert-update run-now

CA 証明書の自動更新をすぐに実行するには、**configure cert-update run-now** コマンドを使用します。

configure cert-update run-now [**force**]

構文の説明

force	接続チェックが失敗した場合でも、CA 証明書の更新を実行します。

コマンド履歴

リリース	変更内容
7.0.5	このコマンドが導入されました。

使用上のガイドライン

CA 証明書をすぐに更新する場合は、**configure cert-update run-now** を使用します。ただし、シスコのサーバーのうちの 1 つでも SSL 接続チェックが失敗した場合、プロセスは終了します。接続に失敗しても更新を続行するには、**force** キーワードを使用します。たとえば、ローカル CA バンドルには、スマートライセンス、AMP 登録、ThreatGrid サービスなどのいくつかのシスコ サービスにアクセスするための証明書があり、シスコのスマートライセンスサービスへの接続に失敗した場合も、**configure cert-update run-now force** コマンドを使用すると、証明書の更新プロセスが実行されます。

（注） IPv6 のみの展開では、一部のシスコのサーバーが IPv6 をサポートしていないため、CA 証明書の自動更新が失敗することがあります。このような場合は、**configure cert-update run-now force** コマンドを使用して CA 証明書を強制的に更新します。

例

次に、接続チェックが失敗した場合の **configure cert-update run-now** コマンドの出力例を示します。

```
> configure cert-update run-now
Certs failed some connection checks.
```

次に、接続チェックが成功し、ローカル CA バンドルが更新された場合の **configure cert-update run-now** コマンドの出力例を示します。

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

次に、**configure cert-update run-now force** コマンドの出力例を示します。

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

関連コマンド

Command	説明
configure cert-update auto-update	毎日の CA 証明書の自動更新を有効または無効にします。
show cert-update	CA 証明書の自動更新のステータスを表示します。
configure cert-update test	シスコのサーバーからの最新のCA証明書を使用して接続チェックを実行します。

configure cert-update test

ローカルシステムの CA 証明書が最新であることを確認し、古い場合は、新しい CA バンドルを使用してサーバーへの SSL 接続をテストするには、**configure cert-update test** コマンドを使用します。

configure cert-update test

コマンド履歴

リリース	変更内容
7.0.5	このコマンドが導入されました。

使用上のガイドライン

この **configure cert-update test** コマンドは、ローカルシステムの CA バンドルを（シスコのサーバーからの）最新の CA バンドルと比較します。CA バンドルが最新の場合はチェックは実行されず、次の例のセクションに示すようにテスト結果が表示されます。CA バンドルが古い場合、ダウンロードされた CA バンドルに対して接続チェックが実行され、次の例のセクションに示すように結果が表示されます。

例

次に、ローカル CA バンドルが最新の場合の **configure cert-update test** コマンドからの出力例を示します。

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

次に、ローカル CA バンドルが古く、ダウンロードしたバンドルの接続チェックが失敗した場合の **configure cert-update test** コマンドの出力例を示します。

```
> configure cert-update test
Test failed, not able to fully connect.
```

次に、ローカル CA バンドルが古く、ダウンロードされたバンドルの接続チェックが成功した場合、または CA バンドルがすでに最新の場合の **configure cert-update test** コマンドからの出力の例を示します。

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

関連コマンド

Command	説明
configure cert-update auto-update	毎日の CA 証明書の自動更新を有効または無効にします。
show cert-update	CA 証明書の自動更新のステータスを表示します。
configure cert-update run-now	CA 証明書の更新をすぐに試します。

configure coredump packet-engine

パケットエンジンのコアダンプ生成を有効または無効にするには、**configure coredump packet-engine** コマンドを使用します。

configure coredump packet-engine {**enable** | **disable**}

構文の説明

disable	パケットエンジンのコアダンプ生成を無効にします。
enable	パケットエンジンのコアダンプ生成を有効にします。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

パケットエンジンのコアダンプ生成は、デフォルトで有効になっています。

このコマンドは、Firepower 2100 シリーズのみで使用できます。サポートされていないプラットフォームでこのコマンドを入力すると、次のメッセージが返されます。

```
This command is not available on this platform.
```

例

次の例では、パケットエンジンのコアダンプ生成を無効にします。

```
> configure coredump packet-engine disable
```

関連コマンド

Command	説明
show coredump	パケットエンジンのコアダンプ生成の設定を表示します。

configure disable-https-access

HTTPS アクセスリストをクリアし、すべての IP アドレスからの HTTPS 接続の試行を拒否するようにデバイスを設定するには、**configure disable-https-access** コマンドを使用します。

configure disable-https-access

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバイスへの HTTPS アクセスを無効にします。ローカルマネージャである Device Manager を使用する場合は、HTTPS アクセスが必要です。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次に、任意のアドレスからの HTTPS 接続を拒否するようにデバイスを設定する例を示します。

```
> configure disable-https-access
```

関連コマンド

Command	説明
configure https-access-list	指定した IP アドレスからの HTTPS 接続を受け入れるようにデバイスを設定します。
show https-access-list	現在の HTTPS アクセスリストを表示します。

configure disable-ssh-access

SSH アクセスリストをクリアし、すべての IP アドレスからの SSH 接続の試行を拒否するようにデバイスを設定するには、**configure disable-ssh-access** コマンドを使用します。

configure disable-ssh-access

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

デバイスへの SSH アクセスを無効にするには、このコマンドを使用します。これにより、コンソールポート経由以外の CLI アクセスが防止されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次に、任意のアドレスからの SSH 接続を拒否するようにデバイスを設定する例を示します。

```
> configure disable-ssh-access
```

関連コマンド

Command	説明
configure ssh-access-list	指定した IP アドレスからの SSH 接続を受け入れるようにデバイスを設定します。
show ssh-access-list	現在の SSH アクセスリストを表示します。

configure firewall

ファイアウォールモードをトランスペアレントモードまたはルーテッドモードに設定するには、**configure firewall** コマンドを使用します。

configure firewall {**routed** | **transparent**}

構文の説明

routed	ファイアウォール モードをルーテッド ファイアウォール モードに設定します。
transparent	ファイアウォール モードをトランスペアレント ファイアウォールに設定します。

コマンド デフォルト

デフォルトでは、デバイスはルーテッドモードです。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、デバイスによってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。

（注） Device Manager を使用している場合、トランスペアレント ファイアウォール モードに切り替えることはできません。ローカルマネージャを使用していて、トランスペアレントモードに変換する場合は、まず **configure manager delete** を使用してマネージャを削除し、トランスペアレントモードに変換してから、**configure manager add** を使用して Management Center を指定する必要があります。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
> configure firewall transparent
```

関連コマンド

Command	説明
show running-config	実行コンフィギュレーションを表示します。
show firewall	ファイアウォール モードを表示します。

configure flow-offload

このコマンドは、特定のフロー（つまり、トラフィック）をハードウェアで処理することで、それらのフローの加速を有効または無効にします。フロー処理をハードウェアにオフロードすると、パフォーマンスが向上するため、デフォルトで有効になっています。

ダイナミック フロー オフロードは、Firepower 4100/9300 シャーシの 脅威に対する防御 でサポートされます。ダイナミック フロー オフロードでは、ハードウェアにオフロードされるトラフィックを選択できます。これは、脅威に対する防御 デバイスのソフトウェアや CPU で処理されないことを意味します。

configure flow-offload dynamic whitelist {enable | disable}

構文の説明

dynamic whitelist enable	ダイナミックオフロードを有効にします。
dynamic whitelist disable	ダイナミックオフロードを無効にします。

コマンド デフォルト

デフォルトでは、イネーブルです。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

ダイナミック フロー オフロードのサポートと制限については、『*Management Center Configuration Guide*』の共通ルール特性に関する章を参照してください。

例

次に、動的オフロードの無効化の例を示します。

```
> configure flow-offload dynamic whitelist disable
```

次に、動的オフロードの有効化の例を示します。

```
> configure flow-offload dynamic whitelist enable
```

関連コマンド

コマンド	説明
show flow-offload	ダイナミック フロー オフロード カウンタ、統計情報、および情報を表示します。
clear flow-offload	ダイナミック フロー オフロードのフロー、カウンタ、または統計をクリアします。

configure high-availability

デバイス間のハイアベイラビリティ設定（フェールオーバー）を無効化、一時停止、または再開するには、**configure high-availability** コマンドを使用します。

configure high-availability {**disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**]}

構文の説明

clear-interfaces	（任意）ハイアベイラビリティが無効化または一時停止されると、インターフェイス設定をクリアします。
disable	このデバイスとそのピア間のハイアベイラビリティ関係を解除します。 このオプションは、ローカルで管理されているデバイスでは使用できません。代わりに Device Manager を使用します。誤って無効化コマンドを使用した場合は、続けて BreakHAStatus リソースを使用して脅威に対する防御 API コールを実行し、アクションを完了する必要があります。
resume	このデバイスとそのピアの間で一時的に中断されたハイアベイラビリティ設定を再開します。ユニットは、ピア ユニットとアクティブ/スタンバイ ステータスをネゴシエートします。無効にした設定は再開できません。
suspend	このデバイスとそのピア間のハイアベイラビリティ設定を一時的に停止します。後で設定を再開できます。 アクティブ装置からハイ アベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

2つのデバイススタックをハイアベイラビリティペアとして設定できます。これはフェールオーバー設定とも呼ばれ、ペアの一方のデバイスに障害が発生した場合、もう一方のデバイスが引き継ぎます。

何らかの理由でデバイスマネージャの設定を更新できない場合は、**configure high-availability** コマンドを使用してハイアベイラビリティペアを管理できます。たとえば、ハイアベイラビリティペアに到達できない場合は、**configure high-availability disable** を使用して両方のハイアベイラビリティピアからフェールオーバー設定を削除できます。

フェールオーバー設定を一時的に停止して、後で再開することもできます。ユニットでHAを一時的に停止することは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイ ユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。
- スタンバイデバイスのソフトウェアアップグレードをインストール中のフェールオーバーを防ぎたい場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムでHA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

（注） ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

例

次の例は、ハイアベイラビリティ設定を一時的に停止してから再開する方法を示しています。

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
```

```
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

関連コマンド

Command	説明
show failover	フェールオーバー（ハイアベイラビリティ）設定を示します。
show high-availability config	フェールオーバー（ハイアベイラビリティ）設定を示します。**show failover** と同じ出力を提供します。

configure https-access-list

指定したIPアドレスからのHTTPS接続を受け入れるようにデバイスを設定するには、**configure https-access-list** コマンドを使用します。

configure https-access-list *address_list*

構文の説明

address_list	ホストまたはネットワークのIPアドレスのカンマ区切りリスト（IPv4 Classless Inter-Domain Routing（CIDR）表記またはIPv6プレフィックス長表記）。たとえば、10.100.10.0/24または2001:DB8::/96のように表記します。 すべてのIPv4ホストを指定するには、「0.0.0.0/0」と入力します。すべてのIPv6ホストを指定するには、「::/0」のように指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

サポートされているすべてのホストまたはネットワークを1つのコマンドに含める必要があります。このコマンドで指定されたアドレスは、HTTPSアクセスリストの現在の内容を上書きします。

HTTPSアクセスを許可するだけでは、ユーザーはローカルマネージャにログインできません。設定ソフトウェアへのアクセスは、ユーザー名とパスワードによって制御されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次の例では、任意のIPv4またはIPv6アドレスからのHTTPS接続を受け入れるようにデバイスを設定します。

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

関連コマンド

Command	説明
configure disable-https-access	HTTPSアクセスリストをクリアします。

Command	説明
show https-access-list	HTTPS アクセスリストを表示します。

configure identity-subnet-filter

ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外するには **configure identity-subnet-filter** コマンドを使用します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

configure identity-subnet-filter { **add** | **remove** } *subnet*

構文の説明

add	指定したサブネットを除外したサブネットのリストに追加します。
remove	指定したサブネットを除外したサブネットのリストから削除します。
subnet	追加または除外するサブネットを指定します。

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。

例

次の例では、管理インターフェイスの静的 IPv6 アドレスを設定します。

```
> configure identity-subnet-filter 192.0.2.0/24
```

関連コマンド

Command	説明
show identity-subnet-filter	ユーザーと IP、および SGT と IP のマッピングから現在除外されているサブネットを表示します。

configure inspection

デフォルトのアプリケーションプロトコル検査エンジンを有効または無効にするには、**configure inspection** コマンドを使用します。

configure inspection *protocol* {**enable** | **disable**}

構文の説明

disable	検査エンジンを無効にします。
enable	検査エンジンを有効にします。
protocol	有効または無効にする検査プロトコル。オプションのリストについては、「使用上のガイドライン」を参照してください。

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

使用上のガイドライン

デフォルトの検査エンジンは、シスコテクニカルサポートの指示がある場合、または関連するトラフィックタイプがネットワーク上で発生しないことが確実な場合にのみ無効にしてください。たとえば、検査対象のポートですべてのトラフィックをブロックする場合、そのポートの検査は安全に無効化できます。これらの検査は、すべてのデータインターフェイスに適用されます。

これらの検査エンジンは、Snort インスペクションとは別のものです。これらのエンジンは、次のサービスを提供します。

- ピンホールの作成：一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザーはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケットデータ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。NAT の制限については、デバイス（Management Center または Device Manager）の設定に使用するマネージャの設定ガイドの「NAT」の章を参照してください。
- プロトコルの強制：一部のインスペクションでは、検査対象プロトコルにある程度の RFC への準拠が強制されます。

次の検査エンジンは、無効にした後で有効にできます。現在有効になっている検査エンジンを確認するには、**show running-config policy-map** コマンドを使用し、**inspect** コマンドを探しま

す。各検査のデフォルトパラメータの詳細を表示するには、**show running-config all policy-map** コマンドを使用します。

- **dcerpc**：（TCP ポート 135）。分散型コンピューティング環境/リモートプロシージャコール。DCERPC 検査エンジンは、Endpoint Mapper（EPM）とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 通信を検査します。DCERPC に基づく Microsoft リモートプロシージャ コール（MSRPC）は、Microsoft 分散クライアントおよびサーバー アプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバー上のプログラムをリモートで実行できるようにします。検査は、ピンホールの作成および NAT サービスを提供します。

- **dns**：（UDP ポート 53）。Domain Name System（ドメイン ネーム システム）。DNS は UDP ポート 53 で検査されます。検査は、NAT サービスとプロトコルの適用を提供します。NAT ルールで NAT の書き換えオプションを使用するには、この検査エンジンを有効にする必要があります。NAT の書き換えは、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）間で NAT を実行するときに頻繁に必要になります。

- **esmtp**：（TCP ポート 25）。Extended Simple Mail Transfer Protocol。ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファ オーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、送受信者およびメール中継のブロックも行います。検査中に適用される制御の詳細については、**show running-config all policy-map** コマンドを使用し、「policy-map type inspect esmtp _default_esmtp_map」行および後続のパラメータを探して確認してください。

  ESMTP アプリケーションインスペクションは、ユーザーが使用できるコマンドとサーバーが返送するメッセージを制御し、その数を減らします。また、NAT サービスとプロトコル準拠を提供します。ESMTP インスペクションは、次の 3 つの主要なタスクを実行します。

  - SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。サポートされるコマンドは次のとおりです。

    拡張 SMTP：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY。

    SMTP（RFC 821）：DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。

  - SMTP コマンド応答シーケンスをモニターします。

  - 監査証跡を生成します。Syslog 監査記録 108002 は、メールアドレスに埋め込まれた無効な文字が置き換えられた場合に生成されます。詳細については、RFC 821 を参照してください。

- **ftp**：（TCP ポート 21）。File Transfer Protocol（ファイル転送プロトコル）。検査は、ピンホールおよび NAT サービスを提供します。

- **h323_h225**：（TCP ポート 1720、UDP ポート 1718）。H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。また、ステートトラッキングとフィルタリングを実行します。H.323 イン

スペクションは、Cisco CallManager などの H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。デバイスは、H.323 v3 機能の同一コールシグナリングチャネルでの複数コールを含めて、H.323 をバージョン 6 までサポートします。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

- **h323_ras**：（UDP ポート 1718 ー 1719）。**h323_h225**についての説明を参照してください。この検査は、RAS シグナリング用です。
- **icmp**：（ICMP トラフィックのみ）。ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP 検査エンジンを使用しない場合、ICMP にデバイスの通過を許可しない（アクセスコントロールルールでブロックする）ことをお勧めします。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。検査は、NAT サービスも提供します。
- **icmp_error**：（ICMP トラフィックのみ）。ICMP エラーインスペクションを有効にすると、デバイスは NAT の設定に基づいて、ICMP エラーメッセージを送信する中間ホップ用の変換セッションを作成します。デバイスは、変換後の IP アドレスでパケットを上書きします。これは、デバイスを通過するトレースルートに意味のある情報を提供するために必要です。
- **ip-options**：（RSVP トラフィックのみ）。IP オプションインスペクションは、パケットヘッダーの [IP Options] フィールドの内容に基づいて許可する IP パケットを制御します。Router Alert オプションが設定されているパケットは許可されます。その他のオプションが設定されているパケットはドロップされます。
- **netbios**：（UDP 送信元ポート 137、138）。NetBIOS Name Server over IP。NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス（NBNS）パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。
- **rsh**：（TCP ポート 514）。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバーへの TCP 接続を使用します。クライアントとサーバーは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ピンホールを開き、ネゴシエートされたポート番号の NAT をサポートします。

- **rtsp**：（TCP ポート 554）。Real-time Streaming Protocol。RTSP 検査エンジンを使用することにより、デバイスはRTSPパケットを通過させることができます。RTSPは、RealAudio、RealNetworks、Apple QuickTime、RealPlayer、およびCisco IP/TV 接続によって使用されます。RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。デバイスは、RFC 2326 に準拠して TCP だけをサポートします。このTCP制御チャネルは、クライアント上で設定されているトランスポートモードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。サポートされているRDTトランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

- **sqlnet**：（TCPポート1521）。インスペクション エンジンは、SQL*Net バージョン1および2をサポートしていますが、形式は Transparent Network Substrate（TNS）のみです。インスペクションでは、表形式データ ストリーム（TDS）形式をサポートしていません。SQL*Netメッセージは、埋め込まれたアドレスとポートについてスキャンされ、必要に応じて NAT の書き換えが適用されます。

  SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Netインスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを65000から約16000に減らすため、データ転送の問題が発生します。

- **sip**：（TCP/UDP ポート 5060）。セッション開始プロトコル。SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。SIPアプリケーション インスペクションでは、メッセージヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。

- **skinny**：（TCP ポート 2000）。Skinny Client Control Protocol（SCCP）。SCCP（Skinny）アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

- **sunrpc**：（TCP/UDP ポート 111）。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバー上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート111でポートマッパープロセス（通常はrpcbind）に照会します。

  クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバーに送信します。サーバーが応答すると、デバイスはこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

- **tftp**：（UDP ポート 69）。Trivial File Transfer Protocol。インスペクション エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を

検査し、必要に応じてダイナミックに接続と変換を作成し、TFTPクライアントとサーバーの間のファイル転送を許可します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。TFTP サーバーだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバーの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバーからのエラー通知があると、セカンダリ チャネルは閉じます。TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

- **xdmcp**：（UDP ポート 177）。X Display Manager Control Protocol。XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。XWindows セッションを正常にネゴシエートして開始するために、デバイスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。TCP ポート経由の戻り接続を許可するには、アクセスコントロールルールを使用します。

  XWindows セッション中、マネージャはウェルノウンポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。**setenv DISPLAY Xserver:***n*、ここで n はディスプレイ番号です。

  XDMCP が使用されている場合、デバイスが必要に応じて NAT を実行できる IP アドレスを使用して、ディスプレイがネゴシエートされます。XDCMP インスペクションでは、PAT はサポートされません。

例

次に、現在のインスペクション設定を表示し、XDMCP インスペクションを無効にする例を示します。検査エンジンは有効化または無効化できますが、デフォルトの動作を変更することはできません。たとえば、次の出力は、DNS/TCP インスペクションが無効になっていることを示しています。**configure inspection** コマンドを使用して、DNS インスペクションを TCP トラフィックに適用するように設定することはできません。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
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 ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
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 sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
!
```

関連コマンド

Command	説明
show running-config policy-map	インスペクション設定を含む、サービスポリシーのポリシーマップを表示します。
show service-policy	インスペクションの統計情報を含むサービスポリシー統計情報を表示します。

configure log-events-to-ramdisk

RAM ディスクへの接続イベントのロギングを有効または無効にして、システムパフォーマンスを向上させ、ソリッドステートドライブ（SSD）への接続イベントの書き込みに伴うディスクの消耗を減らすには、**configure log-events-to-ramdisk** コマンドを使用します。

configure log-events-to-ramdisk {**enable** | **disable**}

構文の説明

enable	RAM ディスクへの接続イベントロギングを有効にします。
disable	RAM ディスクへの接続イベントロギングを無効にします。接続イベントは SSD に記録されます。

コマンド デフォルト

この機能をサポートするプラットフォームでは、デフォルトで有効になっています。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

接続イベントを記録するために使用する RAM ディスクと物理 SSD を切り替えるには、このコマンドを使用します。有効にすると、接続イベントは RAM ディスクに記録されます。無効にすると、接続イベントは SSD に記録されます。停電が発生すると、RAM ディスクに記録された接続イベントは失われます。

このコマンドは、すべてのデバイスタイプで使用できるわけではありません。サポートされていないプラットフォームでこのコマンドを入力すると、次のメッセージが返されます。

```
This command is not available on this platform.
```

例

次に、RAM ディスクへのロギングを無効にする例を示します。

```
> configure log-events-to-ramdisk disable
```

関連コマンド

Command	説明
show log-events-to-disk	現在のロギングステータスを表示します。
show disk-manager	システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

configure manager add

Management Center または CDO、あるいはその両方からの接続、またはそれに対する接続を開始するようにデバイスを設定するには、**configure manager add** コマンドを使用します。

⚠

注意 リモートマネージャを追加すると、設定が工場出荷時のデフォルトにリセットされます。

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

構文の説明

hostname	Management Center のホスト名を指定します。
IPv4_address	Management Center の IPv4 アドレスを指定します。
IPv6_address	Management Center の IPv6 アドレスを指定します。
display_name	**show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。 • *hostname* | *IP_address*（**DONTRESOLVE** キーワードを使用しない場合） • **manager-***timestamp*
DONTRESOLVE	Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。このデバイスを Management Center に追加する場合は、デバイスの IP アドレスと *nat_id* の両方を必ず指定してください。接続の片側で IP アドレスを指定し、両側で同じ一意の NAT ID を指定する必要があります。
regkey	デバイスを Management Center へ登録するのに必要な、英数字の一意の登録キーを指定します。英数字とハイフン（-）を使用できます。
nat_id	一方が IP アドレスを指定しない場合に、Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。Management Center で同じ NAT ID を指定します。管理にデータインターフェイスを使用する場合は、登録用に脅威に対する防御 と Management Center の両方で NAT ID を指定する必要があります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.2	複数のマネージャに対するサポート（プライマリクラウド配信型 Management Center（CDO）と分析専用のオンプレミス Management Center）が追加されました。

使用上のガイドライン

デバイスを Management Center に登録するには、一意の英数字登録キーが常に必要です。

通常は、両方の IP アドレスが必要となります。つまり、Management Center でデバイスの IP アドレスを指定し、デバイスで Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Management Center の IP アドレスがわからない場合は、IP アドレスまたはホスト名の代わりに **DONTRESOLVE** キーワードを使用します。

（注） 管理にデータインターフェイスを使用する場合は、登録用に 脅威に対する防御と Management Center の両方で NAT ID を指定する必要があります。

IPv4 を使用して登録した Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから Management Center で再登録する必要があります。

Management Center からローカルの Device Manager に変更するには、**configure manager delete** コマンドを使用してから **configure manager local** コマンドを使用します。

（注） デバイスをある Management Center から別のものに移動したり、ローカルマネージャに変更したりする前に、現在の Management Center から削除してください。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

関連コマンド

Command	説明
configure manager delete	管理側 Management Center を削除します。
configure manager edit	管理側 Management Center を編集します。
configure manager local	ローカルマネージャを設定します。
show managers	現在のマネージャを表示します。

configure manager delete

現在のマネージャを無効にして、ノーマネージャモードを開始するには、**configure manager delete** コマンドを使用します。

⚠

注意 マネージャを削除すると、脅威に対する防御 設定が工場出荷時の初期状態にリセットされます。ただし、管理ブートストラップ設定は維持されます。

configure manager delete *identifier*

構文の説明

identifier	複数のマネージャが定義されている場合は、識別子（UUID ともいう。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.3	高可用性モードのチェックが追加されました。
7.2	複数のマネージャが設定されている場合に備えて、*identifier* 変数が追加されました。

使用上のガイドライン

現在のデバイスマネージャを削除するには、このコマンドを使用します。デバイスはノーマネージャモードになり、リモートマネージャ（Management Center）を追加したり、ローカルマネージャ（Device Manager ）を使用したりすることができるようになります。このコマンドは、ローカル管理とリモート管理を切り替えるときや、リモートマネージャがアクティブでなくなったときに使用します。

デバイスが高可用性用に設定されている場合は、まず、デバイスマネージャ(可能な場合)または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

このコマンドの動作は、現在のマネージャによって異なります。

- Remote：Management Center に到達できません。Management Center がまだ 脅威に対する防御 と通信している場合は、最初に Management Center のインベントリからデバイスを削除します。その後、このコマンドを使用できます。
- Local：制限なし。すぐにノーマネージャモードに移行します。

例

次の例では、現在のマネージャを削除して、ノーマネージャモードを開始します。

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

関連コマンド

Command	説明
configure manager add	デバイスの管理側 Management Center を設定します。
configure manager local	ローカルマネージャを設定します。
show managers	現在のマネージャを表示します。

configure manager edit

脅威に対する防御 設定の Management Center IP アドレスを編集するには、**configure manager edit** コマンドを使用します。

configure manager edit *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

構文の説明

identifier	Management Center の識別子（UUID）を指定します。**show managers** コマンドを使用して識別子を表示するか（7.2 以降）、Management Center CLI **show version** コマンドから UUID を取得します。
hostname {*ip_address* | *hostname*}	ホスト名/IPアドレスを変更します。
displayname *display_name*	表示名を変更します。

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。
7.2	**hostname** キーワードと **displayname** キーワードが追加されました。

使用上のガイドライン

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。**sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

例

Management Center UUID は Management Center を明確に識別します。たとえば、Management Center 高可用性の場合は、脅威に対する防御 デバイスでアクティブな Management Center を指定する必要があります。

識別子を表示するには、**show managers** コマンドを入力します。

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

UUID を取得したら、脅威に対する防御 デバイスの IP アドレスを編集できます。次に例を示します。

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 10.10.5.1
```

関連コマンド

Command	説明
configure manager delete	管理側 Management Center を削除します。
configure manager add	Management Center を設定します。
show managers	現在のマネージャを表示します。

configure manager local

ローカルマネージャである Device Manager を使用するようにデバイスを設定するには、**configure manager local** コマンドを使用します。

configure manager local

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、ローカルマネージャである Device Manager を有効にします。個別の Management Center を使用しない場合は、ローカルマネージャを使用します。ローカルマネージャを有効にすると、**http://***management_ip_address* でブラウザを使用して Device Manager を開くことができます。

（注） システムがデータベースを再初期化する必要があるため、コマンドの完了に最大 4 ー 6 分かかります。Please be patient.

ローカルマネージャは、6.5 以降のほとんどのプラットフォームで使用できます。使用しているプラットフォームで使用できない場合は、**configure manager add** コマンドを使用してリモートマネージャを設定します。

追加の制限事項

- ローカルマネージャに切り替える前に、デバイスを No Manager モードにする必要があります。No Manager モードを開始するには、**configure manager delete** コマンドを使用します。現在のマネージャを確認するには、**show managers** コマンドを使用します。
- デバイスはトランスペアレント ファイアウォール モードでは動作できません（**configure firewall** コマンドを参照）。ローカルマネージャはルーテッドモードのみをサポートします。

例

次に、ローカルマネージャを設定する例を示します。

```
> configure manager local
```

関連コマンド

Command	説明
configure manager add	デバイスの管理側 Management Center を設定します。

Command	説明
configure manager delete	管理側 Management Center を削除します。
show managers	現在のマネージャを表示します。

configure mini-coredump

ミニコアダンプの生成を有効または無効にするには、**configure mini-coredump** コマンドを使用します。

configure mini-coredump { **enable** | **disable** }

構文の説明

enable	ミニコアダンプの生成を有効にします。
disable	ミニコアダンプの生成を無効にします。

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ミニコアダンプの生成はデフォルトで有効になっています。

Snort 3 プロセスは、そのマルチスレッドの性質により、巨大なコアファイルをダンプします。これらのダンプは、ハードディスクに書き込まれるまでに時間がかかります。コアが書き込まれて新しいプロセスが開始されるまで、Snort のトラフィック検査は中断されます。ミニコアダンプを作成すると、時間の遅延が回避されます。ミニコアダンプには、デバッグに役立つスタックとメモリ値の重要な詳細が含まれています。

例

次に、ミニコアダンプの生成を無効にする例を示します。

```
> configure mini-coredump disable
```

関連コマンド

Command	説明
show mini-coredump status	ミニコアダンプの生成の設定を表示します。

configure network dns searchdomains

DNS 検索ドメインのリストを設定するには、**configure network dns searchdomains** コマンドを使用します。

configure network dns searchdomains ［*dnslist*］

構文の説明

dnslist	DNS 検索ドメインのカンマ区切りリストを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

DNS検索ドメインの現在のリストを新しいリストに置き換えるには、このコマンドを使用します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次の例では、新しい検索ドメインリストを設定し、完全修飾ホスト名ではないホスト名で ping を実行します。

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

関連コマンド

Command	説明
configure network dns servers	DNS サーバーを設定します。
show dns system	管理インターフェイスの現在の DNS 設定を表示します。

configure network dns servers

管理インターフェイスの DNS サーバーを設定するには、**configure network dns servers** コマンドを使用します。

configure nework dns servers ［*dnslist*］

構文の説明

dnslist	DNS サーバーのカンマ区切りリストを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

DNSサーバーの現在のリストを新しいリストに置き換えるには、このコマンドを使用します。これらのサーバーは管理インターフェイスでのみ使用されます。データインターフェイスを通過するコマンドの完全修飾ドメイン名を解決することはできません。

バージョン 6.3 以降、ローカル管理デバイス限定で、データインターフェイスおよび管理インターフェイスが同じ DNS グループを使用している場合、そのグループがマネージャからの次の展開時に更新されます。これは、データインターフェイスで使用されている DNS グループにも変更が適用されることを意味します。管理インターフェイスの変更はすぐに反映されます。すべての DNS 変更は、このコマンドを使用するのではなく、ローカルマネージャから行うことを推奨します。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次に、管理インターフェイスの DNS サーバーを設定する例を示します。

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

関連コマンド

Command	説明
configure network dns searchdomains	DNS 検索ドメインを設定します。
show dns system	管理インターフェイスの現在の DNS 設定を表示します。

configure network hostname

デバイスの管理インターフェイスのホスト名を設定するには、**configure network hostname** コマンドを使用します。

configure network hostname *name*

構文の説明

name	新しいホスト名を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

システムホスト名は複数の場所で定義されます。マネージャからホスト名を更新すると、システムはすべてのプロセスでホスト名を同期します。Device Manager （ローカルマネージャ）を使用しているときにこのコマンドを使用する場合は、すべてのシステムプロセスで同じ名前が使用されるように、Device Manager から変更を展開して更新を完了する必要があります。

例

次の例では、ホスト名を sfrocks に設定します。

```
> configure network hostname sfrocks
```

関連コマンド

Command	説明
show network	管理インターフェイスの設定を表示します。

configure network http-proxy

管理インターフェイスの HTTP プロキシを設定するには、**configure network http-proxy** コマンドを使用します。

configure network http-proxy

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	このコマンドは、ローカル管理システムで機能するようになりました。

使用上のガイドライン

このコマンドを使用して、デバイスのHTTPプロキシアドレスを設定します。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシのユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

例

次に、管理インターフェイスのHTTPプロキシを設定する例を示します。この例では、認証が設定されます。入力したパスワードは CLI に表示されません。

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

関連コマンド

Command	説明
configure network http-proxy-disable	HTTP プロキシ設定を無効化します。
show network	管理インターフェイスの設定を表示します。

configure network http-proxy-disable

管理インターフェイスの HTTP プロキシを削除するには、**configure network http-proxy-disable** コマンドを使用します。

configure network http-proxy-disable

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、管理インターフェイスの HTTP プロキシを削除する例を示します。

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Enabled
HTTP Proxy                  : 10.100.10.10
Port                        : 80
Authentication              : Enabled
Username                    : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Disabled
Authentication              : Disabled
```

関連コマンド

Command	説明
configure network http-proxy	HTTP プロキシを設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にするには、**configure network ipv4 delete** コマンドを使用します。

configure network ipv4 delete ［*management_interface*］

構文の説明

management_ interface	管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

デバイスの管理インターフェイスの IPv4 設定を無効にするには、このコマンドを使用します。削除した IP アドレスに接続すると、デバイスへの接続が失われます。IPv4 アドレスを削除する前に、IPv6 アドレスが設定されていることを確認します。

IPv4 アドレスを変更するために設定を削除する必要はありません。IPv4 アドレッシングを維持しつつ、アドレスのみを変更する場合は、**configure network ipv4 manual** コマンドか **configure network ipv4 dhcp** コマンドを使用します。

例

次の例では、IPv4 アドレス設定を削除します。

```
> configure network ipv4 delete
```

関連コマンド

Command	説明
configure network ipv4 dhcp	DHCP サーバーからアドレスを取得するように IPv4 を設定します。
configure network ipv4 manual	静的 IP アドレスを使用して IPv4 を手動で設定します。

Command	説明
show network	管理インターフェイスの設定を表示します。

configure network ipv4 dhcp

DHCP サーバーから IPv4 アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv4 dhcp** コマンドを使用します。

configure network ipv4 dhcp ［*management_interface*］

構文の説明

management_ interface	管理インターフェイスを指定します。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバイスの管理インターフェイスが DHCP サーバーから IPv4 設定を受信するように指定します。管理インターフェイスはDHCPサーバーと通信して、設定情報を取得します。

（注） **configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定している場合、管理インターフェイスのDHCPを使用することはできないため、IP アドレスを手動で設定する必要があります。これは、**data-interfaces** である必要があるデフォルトルートがDHCPサーバーから受信したルートで上書きされる可能性があるためです。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。

例

次の例では、DHCP を使用して IPv4 アドレスを取得するように管理インターフェイスを設定する方法を示します。

```
> configure network ipv4 dhcp
```

関連コマンド

Command	説明
configure network ipv4 delete	IPv4 ネットワーキングを無効にします。
configure network ipv4 manual	IPv4 を手動で設定します。

Command	説明
show network	管理インターフェイスの設定を表示します。

configure network ipv4 dhcp-dp-route

管理インターフェイスのデフォルト IP アドレス、ネットワークマスク、およびゲートウェイを復元するには、**configure network ipv4 dhcp-dp-route** コマンドを使用します。このコマンドでは、DNS サーバーなどの他のネットワーク設定は変更されません。

（注） このコマンドは、Secure Firewall Threat Defense Virtual（Threat Defense Virtual）、Firepower 4100/9300、または ISA 3000 ではサポートされていません。

configure network ipv4 dhcp-dp-route

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

いずれかのバージョンの IP アドレスを指定しなかった場合でも、このコマンドの IPv4 バージョンと IPv6 バージョンの両方を入力して、設定を工場出荷時のデフォルトに復元する必要があります。

例

次の例では、管理インターフェイスのデフォルト設定を復元します。

```
> configure network ipv4 dhcp-dp-route
Creating /etc/sf/sftunnel.conf with header line
Set up management0 as DHCP ipv4 client with the default route through data interfaces.
>
```

関連コマンド

Command	説明
configure network ipv4 delete	IPv4 ネットワーキングを無効にします。
configure network ipv4 dhcp	DHCP 経由で IPv4 を設定します。
configure network ipv4 manual	IPv4 を手動で設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv4 dhcp-server-disable

管理インターフェイスで DHCP サーバーを無効にするには、**configure network ipv4 dhcp-server-disable** コマンドを使用します。

configure network ipv4 dhcp-server-disable

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

使用上のガイドライン

管理インターフェイスにアクティブなDHCPサーバーがある場合は、それを無効にできます。無効になっている場合、管理ネットワーク上のクライアントに静的アドレスを設定するか、ネットワーク上の別のデバイスをDHCPサーバーサービスを提供するデバイスとして設定する必要があります。

DHCPを使用してアドレスを取得するように管理IPアドレスを変更すると、DHCPサーバーは（有効な場合）自動的に無効になります。

例

次の例は、DHCP サーバーが有効になっているかどうかを確認してから、無効にする方法を示しています。

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

関連コマンド

Command	説明
configure network ipv4 dhcp-server-enable	管理インターフェイスの DHCP サーバーを有効にします。
show dhcp-server	管理インターフェイスの DHCP サーバーのステータスを表示します。

configure network ipv4 dhcp-server-enable

管理インターフェイスでオプションの DHCP サーバーを有効にするには、**configure network ipv4 dhcp-server-enable** コマンドを使用します。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

構文の説明

start_ip_address *end_ip_address*	DHCP アドレスプールの開始および終了 IPv4 アドレスを指定します。管理インターフェイスは、DHCP クライアント要求を受信すると、このプールからアドレスを提供します。プールは、管理 IPv4 アドレスと同じサブネットにある必要があります。 DHCP アドレスプールにネットワークアドレス、管理アドレス、またはブロードキャストアドレスを含めないでください。

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

使用上のガイドライン

管理インターフェイスの手動（静的）IPv4 アドレスを設定する場合は、管理ネットワーク上のエンドポイントにアドレスを提供するように DHCP サーバーを設定できます。

サーバーを有効にする前に、管理ネットワーク上に他の DHCP サーバーがないことを確認します。ネットワークごとに最大 1 台の DHCP サーバーを設定できます。1 台を超えると、予測できない結果が生じることがあります。

（注） このコマンドは、Threat Defense Virtual デバイスではサポートされません。

例

次に、DHCP サーバーを設定し、そのステータスを表示する例を示します。

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

関連コマンド

Command	説明
configure network ipv4 dhcp-server-disable	管理インターフェイスの DHCP サーバーを無効にします。

Command	説明
show dhcp-server	管理インターフェイスの DHCP サーバーのステータスを表示します。

configure network ipv4 manual

管理インターフェイスで静的 IPv4 アドレスを設定するには、**configure network ipv4 manual** コマンドを使用します。

configure network ipv4 manual *ipaddr netmask gw* ［*management_interface*］

構文の説明

ipaddr	IP アドレスを指定します。
netmask	サブネット マスクを指定します。
gw	デフォルトゲートウェイの IPv4 アドレスを指定します。 管理ネットワーク上の明示的なゲートウェイではなく、ゲートウェイとしてデバイス上のデータインターフェイスを使用する **data-interfaces** を指定するオプションがあります。管理用物理インターフェイスを別の管理ネットワークに接続したくない場合は、データインターフェイスを使用します。Management Center データインターフェイスの管理については、**configure network management-data-interface** コマンドを参照してください。 このコマンド内の gw は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として gw を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスとともに使用するように gw を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。
management_ interface	管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

リリース	変更内容
6.2	ゲートウェイの **data-interfaces** キーワードが追加されました。
6.7	**data-interfaces** キーワードがデータインターフェイスでの Management Center 管理に使用できるようになりました。

使用上のガイドライン

configure network management-data-interface コマンドを使用して Management Center アクセス用のデータインターフェイスを設定する場合は、手動 IP アドレス（IPv4 または IPv6）を設定する必要があります。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。data-interfaces である必要があるデフォルトルートは、DHCPサーバーから受信したルートで上書きされる可能性があるため、DHCP（デフォルト）は使用できません。

例

次の例では、管理インターフェイスで静的 IPv4 アドレスを設定します。

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

関連コマンド

Command	説明
configure network ipv4 delete	IPv4 ネットワーキングを無効にします。
configure network ipv4 dhcp	DHCP 経由で IPv4 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にするには、**configure network ipv4 delete** コマンドを使用します。

configure network ipv6 delete ［*management_interface*］

構文の説明

management_ interface	管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバイスの管理インターフェイスの IPv6 設定を無効にします。削除する IP アドレスに接続している場合、デバイスへの接続が失われます。IPv6 アドレスを削除する前に、IPv4 アドレスが設定されていることを確認します。

IPv6 アドレスを変更するために設定を削除する必要はありません。IPv6 アドレッシングを維持しつつ、アドレスのみを変更する場合は、**configure network ipv6** {**manual** | **dhcp** | **router**} コマンドを使用します。

例

次の例では、IPv6 アドレス設定を削除します。

```
> configure network ipv6 delete
```

関連コマンド

Command	説明
configure network ipv6 dhcp	DHCP 経由で IPv6 を設定します。
configure network ipv6 manual	IPv6 を手動で設定します。

Command	説明
configure network ipv6 router	ルータ経由で IPv6 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 destination-unreachable

管理インターフェイスで IPv6 を使用しているときに ICMPv6 宛先到達不能パケットを有効または無効にするには、**configure network ipv6 destination-unreachable** コマンドを使用します。

configure network ipv6 destination-unreachable {**enable** | **disable**}

構文の説明

enable	宛先到達不能パケットを有効にします。この設定は、デフォルトです。
disable	宛先到達不能パケットを無効にします。

コマンド デフォルト

デフォルトでは、イネーブルです。

コマンド履歴

リリース	変更内容
6.4.0	コマンドが追加されました。

使用上のガイドライン

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

例

次に、宛先到達不能メッセージを無効にする例を示します。

```
> configure network ipv6 destination-unreachable disable
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 echo-reply	エコー応答パケットを有効または無効にします。
configure network ipv6 manual	IPv6 を手動で設定します。
configure network ipv6 router	ルータ経由で IPv6 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 dhcp

DHCP サーバーから IPv6 アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv6 dhcp** コマンドを使用します。

configure network ipv6 dhcp ［*management_interface*］

構文の説明

management_ interface	管理インターフェイスを指定します。DHCPはデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバイスの管理インターフェイスが DHCP サーバーから IPv6 設定を受信するように指定します。管理インターフェイスはDHCPサーバーと通信して、設定情報を取得します。

（注） **configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定している場合、管理インターフェイスのDHCPを使用することはできないため、IP アドレスを手動で設定する必要があります。これは、**data-interfaces** である必要があるデフォルトルートがDHCPサーバーから受信したルートで上書きされる可能性があるためです。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。

例

次の例では、DHCP を使用して IPv6 アドレスを取得するように管理インターフェイスを設定する方法を示します。

```
> configure network ipv6 dhcp
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 manual	IPv6 を手動で設定します。

Command	説明
configure network ipv6 router	ルータ経由で IPv6 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 dhcp-dp-route

管理インターフェイスのデフォルト IP アドレス、ネットワークマスク、およびゲートウェイを復元するには、**configure network ipv6 dhcp-dp-route** コマンドを使用します。このコマンドでは、DNS サーバーなどの他のネットワーク設定は変更されません。

（注） このコマンドは、Threat Defense Virtual、Firepower 4100/9300、または ISA 3000 ではサポートされていません。

configure network ipv6 dhcp-dp-route

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

いずれかのバージョンの IP アドレスを指定しなかった場合でも、このコマンドの IPv4 バージョンと IPv6 バージョンの両方を入力して、設定を工場出荷時のデフォルトに復元する必要があります。

例

次の例では、管理インターフェイスのデフォルト設定を復元します。

```
> configure network ipv6 dhcp-dp-route
Set up management0 as DHCP ipv6 client with the default route through data interfaces.
>
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 dhcp	DHCP 経由で IPv6 を設定します。
configure network ipv6 manual	IPv6 を手動で設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 echo-reply

管理インターフェイスで IPv6 を使用しているときに ICMPv6 エコー応答パケットを有効または無効にするには、**configure network ipv6 echo-reply** コマンドを使用します。

configure network ipv6 echo-reply {**enable** | **disable**}

構文の説明

enable	エコー応答パケットを有効にします。この設定は、デフォルトです。
disable	エコー応答パケットを無効にします。

コマンド デフォルト

デフォルトでは、イネーブルです。

コマンド履歴

リリース	変更内容
6.4.0	コマンドが追加されました。

使用上のガイドライン

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例

次の例では、エコー応答メッセージを無効にします。

```
> configure network ipv6 echo-reply disable
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 destination-unreachable	宛先到達不能パケットを有効または無効にします。
configure network ipv6 manual	IPv6 を手動で設定します。
configure network ipv6 router	ルータ経由で IPv6 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 manual

管理インターフェイスで静的 IPv6 アドレスを設定するには、**configure network ipv6 manual** コマンドを使用します。

configure network ipv6 manual *ip6addr ip6prefix* ［*ip6gw*］［*management_interface*］

構文の説明

ip6addr	IP アドレスを指定します。
ip6prefix	プレフィックス長を指定します。
ip6gw	デフォルトゲートウェイの IPv6 アドレスを指定します。 管理ネットワーク上の明示的なゲートウェイではなく、ゲートウェイとしてデバイス上のデータインターフェイスを使用する **data-interfaces** を指定するオプションがあります。管理用物理インターフェイスを別の管理ネットワークに接続したくない場合は、データインターフェイスを使用します。Management Center データインターフェイスの管理については、**configure network management-data-interface** コマンドを参照してください。 このコマンド内の ip6gw は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として ip6gw を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスとともに使用するように ip6gw を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。
management_ interface	管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.2	ゲートウェイの **data-interfaces** キーワードが追加されました。
6.7	**data-interfaces** キーワードがデータインターフェイスでの Management Center 管理に使用できるようになりました。

使用上のガイドライン

configure network management-data-interface コマンドを使用して Management Center アクセス用のデータインターフェイスを設定する場合は、手動 IP アドレス（IPv4 または IPv6）を設定する必要があります。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。data-interfaces である必要があるデフォルトルートは、DHCP サーバーから受信したルートで上書きされる可能性があるため、DHCP（デフォルト）は使用できません。

例

次の例では、管理インターフェイスの静的 IPv6 アドレスを設定します。

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 dhcp	DHCP 経由で IPv6 を設定します。
configure network ipv6 router	ルータ経由で IPv6 を設定します。
show network	管理インターフェイスの設定を表示します。

configure network ipv6 router

ステートレス自動設定を使用してルータからIPv6アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv6 router** コマンドを使用します。

configure network ipv6 router ［*management_interface*］

構文の説明

management_ interface	管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバイスの管理インターフェイスがルータから IPv6 の設定を受信するように指定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

例

次に、ステートレス自動設定を使用してルータからIPv6アドレスを受信するように管理インターフェイスを設定する例を示します。

```
> configure network ipv6 router
```

関連コマンド

Command	説明
configure network ipv6 delete	IPv6 ネットワーキングを無効にします。
configure network ipv6 dhcp	DHCP 経由で IPv6 を設定します。
configure network ipv6 manual	IPv6 を手動で設定します。

Command	説明
show network	管理インターフェイスの設定を表示します。

configure network management-data-interface

管理インターフェイスの代わりにデータインターフェイスを Management Center の管理用に設定するには、**configure network management-data-interface** コマンドを使用します。

configure network managament-data-interface [{ **ipv4** { **dhcp** | [**manual** *ip_address netmask*] [**default-gw** *gateway_ip*] } | **ipv6** { **manual** *ip_address prefix*] [**default-gw** *gateway_ip*] } | **ddns update-url** **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>** | **nameif** *name* | **client** *ip_address mask-or-prefix* | } **interface** *id* | **disable**]

構文の説明

ipv4	IP アドレスに IPv4 を指定します。
ipv6	IP アドレスに IPv6 を指定します。
dhcp	IPv4 アドレスの DHCP を指定します。
manual *ip_address netmask-or-prefix*	手動 IP アドレスとネットマスクまたはプレフィックスを指定します。
default-gw *gateway_ip*	デフォルトゲートウェイのアドレスを指定します。CLI でセカンダリインターフェイスを編集する場合、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。このインターフェイスのスタティックルートは Management Center でしか編集できません。
ddns update-url [illegible]	DDNS Web タイプ更新 URL を指定します。DDNS プロバイダーから提供されたユーザー名とパスワードを指定します。正しいパスについては、DDNS プロバイダーに確認してください。 疑問符（?）文字を入力する前に、キーボードの Ctrl キーと v キーを一緒に押します。これにより、? がソフトウェアでヘルプ照会と解釈されなくなり、? を入力できます。 これらのキーワードは引数のように見えますが、URL の最後にこのテキストをそのまま入力する必要があります。脅威に対する防御は、DDNS 更新を送信するときに、<h> と <a> フィールドを自動的にホスト名と IP アドレスに置き換えます。
nameif *name*	インターフェイス名を設定します。
client *ip_address*	特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。引数を指定せずに **configure network managament-data-interface** コマンドを入力した場合、このキーワードはウィザードの一部ではないことに注意してください。

interface *id*	Management Center 管理アクセスに使用するデータインターフェイス ID を指定します。Management Center アクセスには、データインターフェイス 1 つのみを指定できます。
disable	データインターフェイスで Management Center 管理アクセスを無効にします。

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。
7.3	Management Center にセカンダリ管理インターフェイスを追加した後は、このコマンドを使用して CLI でその設定の一部を編集できます。

使用上のガイドライン

最初にこのコマンドを設定するときに引数を指定しない場合は、データインターフェイスの基本的なネットワーク設定を行うためのウィザードが表示されます。

（注） このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要が生じる場合があります。SSH の詳細な使用方法については、次を参照してください。

Management Center でセカンダリ管理インターフェイスを設定する場合、このコマンドを使用して編集できます。CLI でセカンダリインターフェイスを手動で追加することはできません。Management Center を使用する必要があります。

このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは DHCP を使用できません。初期セットアップ時に IP アドレスを手動で設定しなかった場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して設定できるようになりました。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- データインターフェイスからの Management Center アクセスには、次の制限があります。
  - マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
  - このインターフェイスは管理専用にできません。
  - ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
  - PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。

- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。

- 脅威に対する防御 を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後で Management Center アクセスインターフェイス設定を変更できますが、脅威に対する防御 または Management Center が管理接続による再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、脅威に対する防御 には以前の展開を復元する **configure policy rollback** コマンドが含まれます。
- DDNS サーバー更新の URL を設定すると、脅威に対する防御 は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、脅威に対する防御 は HTTPS 接続の DDNS サーバー証明書を検証できます。脅威に対する防御 は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

  Management Center では、この 脅威に対する防御 に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に 脅威に対する防御 を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む 脅威に対する防御 に後でプ

ラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と 脅威に対する防御 を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、脅威に対する防御設定と一致するように、DNS サーバーを含むすべての設定を Management Center で手動で設定する必要があります。

- 管理インターフェイスは、脅威に対する防御 を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例

次に、DHCP を使用して Ethernet1/1 を Management Center 管理インターフェイスとして設定する例を示します。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

次に、手動 IP アドレスを使用して Ethernet1/1 を Management Center 管理インターフェイスとして設定する例を示します。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

関連コマンド

Command	説明
configure network ipv4 manual	手動IPv4 IPアドレスを使用して管理インターフェイスを設定します。
configure network ipv6 manual	手動IPv6 IPアドレスを使用して管理インターフェイスを設定します。
configure policy rollback	管理接続が中断された場合に、以前の展開を復元します。
show network	管理インターフェイスの設定を表示します。

configure network management-interface

Firepower 4100 または 9300 シリーズ デバイスでイベントと管理トラフィックを分離するために複数の管理インターフェイスを設定するには、**configure network management-interface** コマンドを使用します。脅威に対する防御 では、Firepower 4100 シリーズと 9300 シリーズのデバイスでのみ複数の管理インターフェイスが使用できます。このコマンドを使用して、Management Center 通信に使用する MTU ポートと TCP ポートを設定することもできます。

configure network management-interface { [**disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel**] *interface_id*] | **tcpport** *number* | **mtu-event-channel** [*bytes*] | **mtu-management-channel** [*bytes*] }

構文の説明

disable	指定した管理インターフェイスを無効にします。
disable-event-channel	指定したインターフェイスのイベント トラフィック チャネルを無効にします。
disable-management-channel	指定したインターフェイスの管理チャネルを無効にします。
enable	指定した管理インターフェイスを有効にします。
enable-event-channel	指定したインターフェイスのイベント トラフィック チャネルを有効にします。
enable-management-channel	指定したインターフェイスの管理チャネルを有効にします。
interface_id	有効または無効にする管理インターフェイスを指定します（**management0** または **management1**）。management0 および management1 は、物理インターフェイス ID に関係のない、これらのインターフェイスの内部名です。
tcpport *number*	Management Center との通信に使用する TCP ポートを設定します。デフォルトは 8305 です。デフォルトを変更する場合は、SSH（22）または HTTPS（443）ポートを指定しないでください。数値を 1024 以上（65535 まで）の高い範囲に維持します。このコマンドは、**configure network management-port** コマンドと同等です。
mtu-event-channel [*bytes*]	イベントインターフェイスの MTU を、IPv4 を有効にした場合は 64 ー 9000、IPv6 を有効にした場合は 1280 ー 9000 の間で設定します（バイト単位）。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。このコマンドは、**configure network mtu** コマンドと同等です。

mtu-management-channel [*bytes*]	管理インターフェイスの MTU を、IPv4 を有効にした場合は 64 ー 1500、IPv6 を有効にした場合は 1280 ー 1500 の間で設定します（バイト単位）。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。このコマンドは、**configure network mtu** コマンドと同等です。 （注） MTU を非常に低い値に設定すると、Device Manager のパフォーマンスに影響を及ぼす可能性があります。

コマンド デフォルト

management0 インターフェイスが有効になり、イベントトラフィックと管理トラフィックの両方に使用されます。 management1 は無効です。

デフォルトの TCP ポートは 8305 です。

デフォルトの MTU は管理インターフェイスでもイベントインターフェイスでも 1500 です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが追加されました。

使用上のガイドライン

デバイスを管理する場合、Management Center 管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベントトラフィックを処理することもできます（Management Center Web インターフェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは 1 つだけ設定できます。イベントトラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

Firepower 4100 シリーズと 9300 シリーズのデバイスでは、論理デバイスに割り当てる mgmt タイプのインターフェイスは、脅威に対する防御 アプリケーションでデフォルトの management0 インターフェイスとして指定されます。このインターフェイスには、デフォルトで管理チャンネルとイベントチャンネルの両方が含まれています。Management Center で別のイベントインターフェイスを設定した場合は、Firepower 4100 または 9300 デバイスで、脅威に対する防御論理デバイスに eventing-type インターフェイスを割り当てることで分離を活用することができます。このインターフェイスは、management1 インターフェイスとして指定されます。可能であれば、デバイス イベント インターフェイスと Management Center イベント インターフェイスの間で、イベント トラフィックが送信されます。イベント ネットワークがダウンすると、イベント トラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別

個のイベントインターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。必要に応じて、管理インターフェイスのイベントを無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

イベントインターフェイスを論理デバイスに割り当てても、このインターフェイスは有効になっておらず、ネットワーク設定も設定されていません。脅威に対する防御 CLI にアクセスし、**configure network management-interface** コマンドを使用して有効にする必要があります。次に、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して管理インターフェイスのアドレスを設定します。

例

次の例では、management1 を有効にし、管理チャネルを無効にします。デフォルトでは、両方のチャネルが有効になっています。

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

次の例では、Management Center との通信に使用するポートを変更します。

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

次の例では、イベントインターフェイスの MTU を 9000 に設定します。

```
> configure network management-interface mtu-event-channel 9000
MTU set successfully to 9000 from 1500 for management1
Refreshing Network Config...
Interface management1 speed is set to '10000baseT/Full'
>
```

次の例では、CLI プロンプトを使用して、管理インターフェイスの MTU を 1400 に設定します。

```
> configure network management-interface mtu-management-channel
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

関連コマンド

Command	説明
configure network mtu	管理インターフェイスまたはイベントインターフェイスの MTU を設定します。
configure network static-routes ipv4/ipv6	管理インターフェイスのスタティックルートを設定します。
show network	管理インターフェイスの設定を表示します。

configure network management-port

Management Center との通信に使用する TCP ポートを設定するには、**configure network management-port** コマンドを使用します。

configure network management-port *number*

構文の説明

number	Management Center との通信に使用する TCP ポートを設定します。デフォルトは 8305 です。デフォルトを変更する場合は、SSH（22）または HTTPS（443）ポートを指定しないでください。数値を 1024 以上（65535 まで）の高い範囲に維持します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

Management Center への管理接続に使用するポートを変更するには、このコマンドを使用します。このコマンドを使用しても、ローカルマネージャである Device Manager で使用されるポートが変更されることはありません。このコマンドは、**configure network management-interface tcpport** コマンドと同等です。両方のコマンドを使用する必要はありません。

例

次の例では、Management Center との通信に使用するポートを変更します。

```
> configure network management-port 8306
Management port changed to 8306.
```

関連コマンド

Command	説明
configure network ipv4	管理インターフェイスの IPv4 アドレスを設定します。
configure network ipv6	管理インターフェイスの IPv6 アドレスを設定します。
show network	管理インターフェイスの設定を表示します。

configure network mtu

管理インターフェイスまたはイベントインターフェイスの MTU を設定するには、**configure network mtu** コマンドを使用します。

configure network mtu ［ *interface_id* ］ ［ *bytes* ］

構文の説明

bytes	（任意）MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64ー1500、IPv6 を有効にした場合は 1280ー1500 の値を指定できます。 イベントインターフェイスでは、IPv4 を有効にした場合は 64ー9000、IPv6 を有効にした場合は 1280ー9000 です。 IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。 （注） MTU を非常に低い値に設定すると、Device Manager のパフォーマンスに影響を及ぼす可能性があります。
interface_id	（任意）MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID（management0、management1、br1、eth0など）を表示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。

コマンド デフォルト

デフォルトの MTU は管理インターフェイスでもイベントインターフェイスでも 1500 です。

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**configure network management-interface mtu-event-channel** および **configure network management-interface mtu-management-channel** コマンドと同等です。両方のコマンドを使用する必要はありません。

例

次の例では、イベントインターフェイス management1 の MTU を 8192 に設定します。

```
> configure network mtu 8192 management1
MTU set successfully to 8192 from 1500 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
```

>

次の例では、CLI プロンプトを使用して、管理インターフェイスの MTU を 1400 に設定します。

```
> configure network mtu
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

関連コマンド

Command	説明
configure network ipv4	管理インターフェイスの IPv4 アドレスを設定します。
configure network ipv6	管理インターフェイスの IPv6 アドレスを設定します。
configure network management-interface	管理インターフェイスまたはイベントインターフェイスの MTU を設定します。
show network	管理インターフェイスの設定を表示します。

configure network speed

管理インターフェイスまたはデータインターフェイスの速度を設定するには、**configure network speed** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

configure network speed { *speed* | **sfp-detect** [*interface_id*]

構文の説明

interface_id	（任意）速度を設定するインターフェイス ID を指定します。デフォルトは management0 です。
sfp-detect	インストールされている SFP モジュールの速度を検出し、適切な速度を使用します。この設定は、デフォルトです。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。
speed	特定の速度に速度を設定します。使用できる速度は、インターフェイスによって異なります。

コマンド デフォルト

デフォルトの速度は **sfp-detect** です。

コマンド履歴

リリース	変更内容
7.1	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

SFP 機能に関係なく、速度を特定の速度に設定する場合を除き、デフォルトの **sfp-detect** を使用することをお勧めします。

例

次に、管理インターフェイスである management0 の速度を 1gbps に設定する例を示します。

```
> configure network speed 1gbps
```

関連コマンド

Command	説明
configure network ipv4	管理インターフェイスの IPv4 アドレスを設定します。

Command	説明
configure network ipv6	管理インターフェイスの IPv6 アドレスを設定します。
configure network management-interface	管理インターフェイスまたはイベントインターフェイスの MTU を設定します。
show network	管理インターフェイスの設定を表示します。

configure network static-routes

スタティックルートを追加または削除するには、**configure network static-routes** コマンドを使用します。

configure network static-routes {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

構文の説明

add	管理インターフェイスのスタティックルートを追加します。
delete	管理インターフェイスのスタティックルートを削除します。削除するルートを選択するように求められます。
interface	管理インターフェイスの ID。モデルの管理インターフェイス ID を表示するには、**show network** コマンドを使用します。
ipv4	IPv4 管理アドレスのスタティックルートを追加または削除します。
ipv6	IPv6 管理アドレスのスタティックルートを追加または削除します。
destination	追加または削除する宛先 IP アドレス（必要に応じて IPv4 形式または IPv6 形式）。たとえば、10.100.10.10 または 2001:db8::201 のように表示されます。
netmask_or_prefix	IPv4 のネットワークアドレスマスク、または IPv6 のプレフィックス。IPv4 ネットマスクは、ドット付き 10 進形式にする必要があります（255.255.255.0 など）。IPv6 プレフィックスは、96 などの標準プレフィックス番号です。
gateway	追加または削除するゲートウェイアドレス（必要に応じて IPv4 形式または IPv6 形式）。

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

使用上のガイドライン

configure network management-interface コマンドを使用してイベント専用インターフェイスを設定する際、そのインターフェイスが管理インターフェイスとは別のネットワーク上に存在する場合は、スタティックルートを設定する必要があります。スタティックルートは、through-the-box トラフィック（データインターフェイス上のトラフィック）には影響しません。スタティックルートがない場合、すべての管理トラフィックは、デフォルト管理インターフェイスのゲートウェイとして指定されたデフォルトルートを使用します。通常、単一の管理インターフェイスを使用する場合、またはイベント専用インターフェイスが同じネットワーク上にある場合、スタティックルートは必要ありません。

（注） デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト管理インターフェイスに対して **configure network ipv4** コマンドまたは **ipv6** コマンドを使用する場合は、デフォルト ルート ゲートウェイの IP アドレスしか変更できません。

例

次の例では、**10.115.24.0** の宛先アドレス、**255.255.255.0** のネットワークアドレスマスク、および **10.115.9.2** のゲートウェイアドレスを使用して、管理インターフェイス **management1** の IPv4 スタティックルートを追加します。

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

次の例では、**2001:db8::201** の宛先アドレス、**64** の IPv6 プレフィックス長、および **2001:db8::3657** のゲートウェイアドレスを使用して、管理インターフェイス **management1** の IPv6 スタティックルートを追加します。

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

次の例は、スタティックルートを削除する方法を示しています。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    management1
Destination:  10.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

関連コマンド

Command	説明
configure network management-interface	複数の管理インターフェイスを設定します。
configure network static-routes ipv4	管理インターフェイスの IPv4 スタティックルートを追加または削除します。

Command	説明
show network-static-routes	管理インターフェイス用に設定されたスタティックルートを表示します。

configure password

現在ログインしているユーザーアカウントのパスワードを変更するには、**configure password** コマンドを使用します。

configure password

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、現在のユーザーはCLIでパスワードを変更できます。コマンドを発行すると、CLIは現在の（古い）パスワードを入力するようユーザーに要求し、その後で新しいパスワードを2回入力するよう要求します。

例

次の例では、現在のユーザーアカウントのパスワードを変更します。

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

関連コマンド

Command	説明
configure user add	CLI アクセス用のユーザーアカウントを追加します。

configure policy rollback

脅威に対する防御 の設定 last-deployed に展開した設定にロールバックするには、**configure policy rollback** コマンドを使用します。

configure policy rollback

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。
7.2	ロールバックは高可用性でサポートされています。

使用上のガイドライン

Management Center の管理に 脅威に対する防御 でデータインターフェイスを使用し（**configure network management-data-interface** を参照）、ネットワーク接続に影響する Management Center からの設定変更を展開する場合、脅威に対する防御 の設定を last-deployed 設定にロールバックするため、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ 脅威に対する防御 でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは Management Center 7.2 以降は高可用性でサポートされています。
- ロールバックは、クラスタリング展開ではサポートされていません。
- ロールバックは、Management Center で設定できる設定にのみ影響します。たとえば、ロールバックは、脅威に対する防御 CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

ロールバック後、脅威に対する防御 はロールバックが正常に完了したことを Management Center に通知します。Management Center では、設定がロールバックされたことを示すバナーが展開画面に表示されます。

ロールバックが失敗した場合、一般的な展開の問題について https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html を参照して

ください。場合によっては、Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center 設定の問題を解決して、Management Center から再展開できます。

例

次に、最後に展開された設定をロールバックする例を示します。

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

関連コマンド

Command	説明
configure network management-data-interface	Management Center 管理用のデータインターフェイスを設定します。

configure raid

RAID 内で SSD を管理するには、**configure raid** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

configure raid ｛ **add** ｜ **remove** ｜ **remove-secure** ｝ **local-disk** ｛ **1** ｜ **2** ｝ ［ *psid* ］

構文の説明

add	SSD を RAID に追加します。新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。
psid	以前に別のシステムで使用されていて、まだロックされている SSD を追加する場合は、*psid* と入力します。*psid* は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。
remove	SSD を RAID から取り外し、データをそのまま保持します。
remove-secure	SSD を RAID から取り外し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。
local-disk ｛**1** ｜ **2**｝	SSD（disk1 または disk2）を指定します。

コマンド デフォルト

SSD が 2 つある場合、起動時に RAID が形成されます。

コマンド履歴

リリース	変更内容
7.1	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

ファイアウォールの電源が入っている状態で Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

例

次に、RAID から disk2 が削除され、安全に消去される例を示します。

```
> configure raid remove-secure local-disk 2
```

関連コマンド

Command	説明
show raid	RAID ステータスを表示します。
show ssd	SSD ステータスを表示します。

configure snort

Snort 検査エンジンの高度な動作を設定するには、**configure snort** コマンドを使用します。

configure snort preserve-connection {**enable** | **disable**}

構文の説明

preserve-connection {**enable** | **disable**}	Snort プロセスがダウンした場合に、ルーテッドインターフェイスとトランスペアレントインターフェイスで既存の TCP/UDP 接続を維持するかどうかを指定します。このオプションはデフォルトでは有効になっていますが、無効化できます。コマンドを有効にした場合、すでに許可されている接続は確立されたままですが、Snort が再び使用可能になるまで新しい接続を確立できません。無効化した場合、Snort がダウンすると、新規または既存のすべての接続がドロップされます。 ICMP ping などの非 TCP/UDP 接続は維持されません。 現在の設定を表示するには、**show running-config snort** コマンドを使用します。実行コンフィギュレーション全体を表示する場合、**snort preserve-connection** コマンドの **no** 形式を使用すると、この機能が無効であることが示されます。

コマンド履歴

リリース	変更内容
6.2.0.2、6.2.3	このコマンドが導入されました。ただし、**preserve-connection disable** は Device Manager（ローカル管理）ではサポートされていないため、設定を展開するたびに接続の維持が再度有効になります。 このコマンドは、脅威に対する防御 または Management Center でバージョン 6.2.1、6.2.2、6.2.2.x、または 6.2.0.2 以前のバージョンが実行されている場合には使用できません。この場合、コマンドが無効になっているかのようにデバイスが動作するため、Snort がダウンするとすべての新規および既存の接続がドロップされます。

使用上のガイドライン

preserve-connection を有効にすると、Snort がダウンしても、既存の接続は確立されたままになります。Snort が使用可能になると、これらの確立された接続は Snort 検査をバイパスし続けます。Snort 検査が必要な新しい接続は、Snort が再び使用可能になるまでドロップされます。

例

次の例では、**preserve-connection** を無効化します。

```
> configure snort preserve-connection disable
```

関連コマンド

コマンド	説明
show conn	接続を表示します。
show conn detail	接続の詳細に Snort 検査情報を含めます。
show conn detail long	長い形式の接続の詳細に Snort 検査情報を含めます。

configure ssh-access-list

指定した IP アドレスからの SSH 接続を受け入れるようにデバイスを設定するには、**configure ssh-access-list** コマンドを使用します。

configure ssh-access-list *address_list*

構文の説明

address_list	ホストまたはネットワークの IP アドレスのカンマ区切りリスト（IPv4 Classless Inter-Domain Routing（CIDR）表記または IPv6 プレフィックス長表記）。たとえば、10.100.10.0/24 または 2001:DB8::/96 のように表記します。 すべての IPv4 ホストを指定するには、「0.0.0.0/0」と入力します。すべての IPv6 ホストを指定するには、「::/0」のように指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

サポートされているすべてのホストまたはネットワークを 1 つのコマンドに含める必要があります。このコマンドで指定したアドレスで、SSH アクセスリストの現在の内容が上書きされます。

SSH アクセスを許可するだけでは、ユーザーはローカルマネージャにログインできません。設定ソフトウェアへのアクセスは、ユーザー名とパスワードによって制御されます。

現在 CLI にログインしている IP アドレスを除外すると、接続が切断されます。CLI に再度アクセスするには、IP アドレスを変更する必要があります。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

例

次の例では、任意の IPv4 または IPv6 アドレスからの SSH 接続を受け入れるようにデバイスを設定します。

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

関連コマンド

Command	説明
configure disable-ssh-access	SSH アクセスリストをクリアします。
show ssh-access-list	SSH アクセスリストを表示します。

configure ssl-protocol

クライアントがデバイスへの HTTPS 接続で使用できる SSL プロトコルを設定するには、ローカルマネージャを使用するときに **configure ssl-protocol** コマンドを使用します。

configure ssl-protocol {*protocol_list* | **default**}

構文の説明

default	デフォルトの SSL プロトコルリストを有効にします。**TLSv1.1**、**TLSv1.2**。
protocol_list	次のいずれかのプロトコルを指定するカンマ区切りリスト。**TLSv1**、**TLSv1.1**、**TLSv1.2**、**SSLv3**。

コマンド デフォルト

デフォルト設定は **TLSv1.1**、**TLSv1.2** です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、クライアントがデバイスへの HTTPS Web アクセスに使用できるプロトコルを設定します。これは、ローカルマネージャである Device Manager で使用されます。リモートマネージャでは使用できません。

（注） このコマンドを使用して、デバイスとの通信に現在使用しているプロトコルを無効にすると、接続が失われます。

例

次の例では、HTTPS 接続のすべての SSL プロトコルを受け入れるようにデバイスを設定します。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

関連コマンド

Command	説明
show ssl-protocol	現在設定されている SSL プロトコルを表示します。

configure tcp-randomization

TCP シーケンス番号のランダム化を無効にするには、**configure tcp-randomization** コマンドを使用します。

configure tcp-randomization {**enable** | **disable**}

構文の説明

enable	着信パケットと発信パケットの TCP シーケンス番号をランダムに変更して、攻撃者が次のパケットのシーケンス番号を予測できないようにします。
disable	着信パケットと発信パケットの TCP シーケンス番号を変更しないでください。

コマンド デフォルト

シーケンス番号のランダム化は、デフォルトで有効になっています。

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

使用上のガイドライン

個々の TCP 接続には 2 つの初期シーケンス番号（ISN）があり、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバーで生成されます。脅威に対する防御デバイスは、着信と発信の両方向で通過する TCP SYN の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化をディセーブルにすることができます。たとえば、連続番号が付いた TCP パケットに依存するソフトウェアテストツール、ソフトウェア製品、またはハードウェアデバイスを使用しているとします。TCP ランダム化設定を変更すると、デバイス上のすべてのインターフェイスとすべてのトラフィックに影響します。特定のインターフェイスまたはトラフィッククラスを指定して変更することはできません。

TCP シーケンス番号のランダム化は、ランダム化による特定の問題が発生した場合にのみ無効にする必要があります。

（注） Device Manager を使用している場合は、TCP シーケンス番号のランダム化を無効にできますが、Device Manager から設定を展開するたびに、この機能は再度有効になります。TCP シーケンス番号のランダム化を無効のままにしておく場合は、展開が完了するたびにコマンドを再入力する必要があります。

例

次の例では、TCP シーケンス番号のランダム化が無効になります。

```
> configure tcp-randomization disable
```

TCP シーケンス番号のランダム化が現在有効かそれとも無効かを確認するには、**set connection random-sequence-number disable** コマンドの実行コンフィギュレーションを調べます。このコマンドは global_policy ポリシーマップに含まれるため、**show running-config policy-map** コマンドを使用して設定の表示を制限できます。**set connection random-sequence-number** コマンドが設定に表示されない場合は、TCP シーケンス番号のランダム化が有効になっています。

たとえば、次の例では TCP シーケンス番号のランダム化が無効になっています（関連するコマンドが強調表示されています）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
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 sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class tcp
  set connection random-sequence-number disable
!
```

次の例では、**set connection random-sequence-number** コマンドが global_policy ポリシーマップに含まれていないため、TCP シーケンス番号のランダム化が有効になっていることがわかります。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
```

```
  no tcp-inspection
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 sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
```

configure unlock_time

失敗したログインの最大数を超えたためにユーザーアカウントがロックされた後、自動的にロック解除されるまでの時間を設定するには、**configure unlock_time** コマンドを使用します。このコマンドは、CC/UCAPL コンプライアンスモードのみで動作します。

configure unlock_time *number*

構文の説明

number	ロック解除時間を分単位で指定します。値の範囲は 1 ー 9999 です。

コマンド デフォルト

CC/UCAPL モードで実行している場合、デフォルトのロック解除時間は 30 分です。

CC/UCAPL モードで実行していない場合、ユーザーアカウントは、**configure user unlock** コマンドを使用してロック解除するまでロックされたままになります。自動ロック解除時間は設定できません。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

CC/UCAPL コンプライアンスモードで実行している場合は、ロックアウトされたユーザーのグローバルロック解除時間を設定できます。設定された時間が経過すると、ユーザーアカウントの最大ログイン試行失敗回数を超えた特定のユーザーのアカウントはロック解除され、ユーザーは再試行できるようになります。ログイン試行の失敗が許可される最大回数を設定するには、**configure user maxfailedlogins** コマンドを使用します。

ロック解除時間を設定した場合でも、**configure user unlock** コマンドを使用してユーザーアカウントをいつでもロック解除できます。ユーザーは、ロック解除時間が経過するまで待つ必要はありません。

例

次の例では、ロック解除時間を 60 分に設定します。

```
> configure unlock_time 60
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user maxfailedlogins	ユーザーがログインで失敗できる最大回数を設定します。
configure user unlock	指定したユーザーのアカウントのロックを解除します。

Command	説明
show user	ユーザーアカウントを表示します。

configure user access

既存ユーザーのアクセス認証レベルを変更するには、**configure user access** コマンドを使用します。

configure user access ユーザー名 {**basic** | **config**}

構文の説明

username	既存ユーザーの名前を指定します。
basic	ユーザーに基本的なアクセス権を付与します。ユーザーはコンフィギュレーション コマンドを入力することはできません。
config	ユーザーにコンフィギュレーション アクセス権を付与します。すべてのコマンドの管理者権限がユーザーに与えられます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ユーザーアカウントを作成するときに、ユーザーのアクセス権を指定します。**configure user access** コマンドを使用して、指定したユーザーのアクセスレベルを変更します。このコマンドは、該当ユーザーが次にログインするときに有効になります。

例

次の例では、ユーザー jdoe のアクセス権を Basic に変更します。

```
> configure user access jdoe basic
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
show user	ユーザーアカウントとアクセス権を表示します。

configure user add

CLIアクセス用の新しいユーザーアカウントを作成するには、**configure user add** コマンドを使用します。

configure user add ユーザー名 {**basic** | **config**}

構文の説明

username	既存ユーザーの名前を指定します。
basic	ユーザーに基本的なアクセス権を付与します。ユーザーはコンフィギュレーション コマンドを入力することはできません。
config	ユーザーにコンフィギュレーション アクセス権を付与します。すべてのコマンドの管理者権限がユーザーに与えられます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

指定した名前、アクセスレベル、およびパスワードで新しいユーザーを作成するには、このコマンドを使用します。このコマンドは、パスワードを要求するコマンドプロンプトを表示します。他のすべてのアカウントプロパティは、デフォルトのプロパティで設定されます。

例

次の例では、config アクセス権を使用して、joecool という名前のユーザ アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

関連コマンド

Command	説明
configure user access	ユーザーアクセスレベルを設定します。
configure user aging	ユーザーパスワードのエージングを設定します。
configure user delete	指定したユーザーを削除します。
configure user disable	指定したユーザーを無効にします。

Command	説明
configure user enable	指定したユーザーを有効にします。
configure user forcereset	指定したユーザーのパスワードを強制的にリセットします。
configure user maxfailedlogins	指定したユーザーのログイン失敗の最大回数を設定します。
configure user password	指定したユーザーのパスワードを設定します。
configure user strengthcheck	指定したユーザーのパスワードの強度チェック要件を設定します。
configure user unlock	指定したユーザーのアカウントのロックを解除します。
show user	ユーザーアカウントを表示します。

configure user aging

ユーザーのパスワードの有効期限を設定するには、**configure user aging** コマンドを使用します。

configure user aging *username max_days warn_days* ［ *grace_period* ］

構文の説明

username	ユーザーの名前を指定します。管理者ユーザーのエージング設定は変更できません。
max_days	パスワードの最大有効日数を指定します。有効範囲は1～9999です。
warn_days	パスワードの有効期限が切れる前に、ユーザーによるパスワード変更が猶予される日数を指定します。有効範囲は 1 ー 9999 ですが、最大日数未満にする必要があります。
grace_period	（任意、FXOS プラットフォームのみ。）パスワードの有効期限が切れた後、ユーザーが引き続きパスワードを変更できる日数を指定します。FXOS 以外のプラットフォームでは、パラメータは受け入れられますが、**show user** 出力には猶予期間が無効であることが示されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.0	*grace_period* パラメータが追加されました。

例

次に、ユーザーのパスワードを 100日後に期限切れになるように設定し、パスワードの有効期限の 30 日前にユーザーに警告を開始する例を示します。show user の出力で、[Exp]列と [Warn] 列の数値を確認します。

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

次に、パスワードを 180 日後に期限切れになるように設定し、期限切れになる 7 日前にユーザーへの警告を開始し、7 日の猶予期間を含める例を示します。

```
> configure user aging joeuser 180 7 7
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
```

```
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No
5
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user forcereset	指定したユーザーのパスワードを強制的にリセットします。
configure user password	指定したユーザーのパスワードを設定します。
show user	ユーザーアカウントを表示します。

configure user delete

ユーザーアカウントを削除するには、**configure user delete** コマンドを使用します。

configure user delete ユーザー名

構文の説明

username	ユーザーの名前を指定します。admin ユーザーは削除できません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次の例では、ユーザーアカウントを削除します。

```
> configure user delete jdoe
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user disable	ユーザーアカウントを削除せずに無効にします。
show user	ユーザーアカウントを表示します。

configure user disable

ユーザーアカウントを削除せずに無効にするには、**configure user disable** コマンドを使用します。

configure user disable ユーザー名

構文の説明

username	ユーザーの名前を指定します。**admin** ユーザーを無効にすることはできません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ユーザーアカウントを削除せずに無効にするには、このコマンドを使用します。無効なユーザーはログインできません。無効なユーザーアカウントを再度有効にするには、**configure user enable** コマンドを使用します。

例

次の例では、ユーザーアカウントを無効にします。

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user delete	指定したユーザーを削除します。
configure user enable	指定したユーザーを有効にします。
configure user unlock	指定したユーザーのアカウントのロックを解除します。
show user	ユーザーアカウントを表示します。

configure user enable

以前に無効にしたユーザーを有効にするには、**configure user enable** コマンドを使用します。

configure user enable ユーザー名

構文の説明

username	ユーザーの名前を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ユーザーを有効にしてログインを許可するには、このコマンドを使用します。

例

次の例では、無効なユーザーアカウントを有効にします。**show user**[Enabled] 列が変更されたことに注意してください。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user disable	指定したユーザーを無効にします。
configure user forcereset	指定したユーザーのパスワードを強制的にリセットします。
configure user unlock	指定したユーザーのアカウントのロックを解除します。
show user	ユーザーアカウントを表示します。

configure user forcereset

ユーザーが次にログインするときにパスワードの変更を強制するには、**configure user forcereset** コマンドを使用します。

configure user forcereset ユーザー名

構文の説明

username	ユーザーの名前を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ユーザーが次にログインするときにパスワードの変更を強制するには、このコマンドを使用します。ユーザーがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

例

次の例では、ユーザーが次にログインするときにパスワードのリセットを強制します。

```
> configure user forcereset jdoe
```

関連コマンド

Command	説明
configure user password	指定したユーザーのパスワードを設定します。
configure user strengthcheck	指定したユーザーのパスワードの強度チェック要件を設定します。
show user	ユーザーアカウントを表示します。

configure user maxfailedlogins

ユーザーの連続ログイン失敗回数の最大数を設定するには、**configure user maxfailedlogins** コマンドを使用します。

configure user maxfailedlogins *username number*

構文の説明

username	ユーザーの名前を指定します。
number	連続ログイン失敗回数の最大数を 1 ー 9999 の範囲で指定します。

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。ただし、新しいアカウントの作成時は、連続ログイン失敗回数のデフォルトの最大数は 5 です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.2.2	CC/UCAPL コンプライアンスモードで実行している場合は、**admin** ユーザーのログイン試行失敗回数の最大数も設定できます。

使用上のガイドライン

このコマンドを使用して、指定したユーザーのアカウントがロックされるまでの連続ログイン失敗回数の最大数を設定します。ユーザーアカウントがロックされた場合は、**configure user unlock** コマンドを使用してロックを解除します。

例

次の例では、連続ログイン失敗回数の最大数を 3 に設定します。

```
> configure user maxfailedlogins jdoe 3
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user password	指定したユーザーのパスワードを設定します。
configure user unlock	指定したユーザーのアカウントのロックを解除します。
show user	ユーザーアカウントを表示します。

configure user minpasswdlen

ユーザーパスワードの最小長を指定するには、**configure user minpasswdlen** コマンドを使用します。

configure user minpasswdlen *username number*

構文の説明

username	ユーザーの名前を指定します。
number	パスワードの最小長を 1 ～ 127 の間で指定します。

コマンド デフォルト

パスワードの最小長はありません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.2.2	**admin** ユーザーのパスワードの最小長を設定できるようになりました。

使用上のガイドライン

指定したユーザーのパスワードの最小長を設定するには、このコマンドを使用します。ユーザーアカウントの現在のパスワードの入力が求められます。最小長が現在のパスワードの長さよりも長い場合は、新しいパスワードを設定するように求められます。

例

次の例では、パスワードの最小長を8文字に設定します。この例では、現在のパスワードが新しい最小長よりも短いため、新しいパスワードを設定する必要があります。

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
show user	ユーザーアカウントを表示します。

configure user password

別のユーザーアカウントのパスワードを指定するには、**configure user password** コマンドを使用します。

configure user password ユーザー名

構文の説明

username	ユーザーの名前を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

指定したユーザーのパスワードを設定するには、このコマンドを使用します。このコマンドでは、ユーザーのパスワードを入力するよう要求されます。自分のパスワードを変更するには、このコマンドの代わりに **configure password** コマンドを使用します。

例

次の例では、別のユーザーのアカウントにパスワードを設定します。パスワードは入力時に非表示となります。

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

関連コマンド

Command	説明
configure password	現在ログインしているユーザーのパスワードを変更します。
configure user add	新しいユーザーを追加します。
configure user aging	ユーザーパスワードのエージングを設定します。
configure user forcereset	指定したユーザーのパスワードを強制的にリセットします。
configure user maxfailedlogins	指定したユーザーのログイン失敗の最大回数を設定します。
configure user strengthcheck	指定したユーザーのパスワードの強度チェック要件を設定します。
show user	ユーザーアカウントを表示します。

configure user strengthcheck

ユーザーのパスワードに対する強度の要件を有効または無効にするには、**configure user strengthcheck** コマンドを使用します。

configure user strengthcheck ユーザー名 {**enable** | **disable**}

構文の説明

username	ユーザーの名前を指定します。
enable	指定したユーザーのパスワードの要件を設定します。
disable	指定したユーザーのパスワードの要件を削除します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、パスワードの変更時にユーザーに対して特定のパスワード基準を満たすように要求する、強度チェックを有効または無効にします。ユーザーパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザーが次にログインしたときにこの要件が自動的に有効になります。

例

次の例では、ユーザーアカウントの強度チェックを有効にします。

```
> configure user strengthcheck jdoe enable
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user forcereset	指定したユーザーのパスワードを強制的にリセットします。
configure user maxfailedlogins	指定したユーザーのログイン失敗の最大回数を設定します。
configure user password	指定したユーザーのパスワードを設定します。
configure user unlock	指定したユーザーのアカウントのロックを解除します。
show user	ユーザーアカウントを表示します。

configure user unlock

ログイン失敗の最大数を超過したユーザーアカウントのロックを解除するには、**configure user unlock** コマンドを使用します。

configure user unlock ユーザー名

構文の説明

username	ユーザーの名前を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次の例では、ユーザーアカウントのロックを解除します。

```
> configure user unlock jdoe
```

関連コマンド

Command	説明
configure user add	新しいユーザーを追加します。
configure user maxfailedlogins	指定したユーザーのログイン失敗の最大回数を設定します。
show user	ユーザーアカウントを表示します。

conn data-rate

負荷の大きいデータを渡すデバイス上の接続を表示するには、**conn data-rate** コマンドを使用します。このコマンドには、フローごとのデータレートが既存の接続情報とともに表示されます。データレート別に接続の収集を無効にするには、このコマンドの **no** 形式を使用します。

conn data-rate

no conn data-rate

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

conn data-rate コマンドは、デバイスの全体的な負荷の最も大きな部分を占めている可能性のある接続やユーザーを特定する際に特に役立ちます。

有効にすると、**conn data-rate** 機能によって、すべての接続に関する次の 2 つの統計情報が追跡されます。

- 接続の順方向および逆方向の現在の（1 秒）データレート。
- 接続の順方向および逆方向の最大（1 秒）データレート。

例

次の例では、接続データレート収集を有効にする方法、この機能が有効になっていることを確認する方法、およびデータレートを表示する方法を示します。

```
> conn data-rate
> show conn data-rate
Connection data rate tracking is currently enabled.
Use 'show conn detail' to see the data rates of active connections.

> show conn detail

TCP outside: 198.51.100.1/46994 NP Identity Ifc: 203.0.113.1/22,
flags UOB , idle 0s, uptime 9m24s, timeout 1h0m, bytes 68627
Initiator: 198.51.100.1, Responder: 203.0.113.1
data-rate forward/reverse
current rate: 1194/0 bytes/sec <-----------------current data rate for forward/reverse
flows
max rate: 2520/0 bytes/sec <----------------max data rate for forward/reverse flows
time since last max 0:08:54/NA <----------------time since last max data rate for
forward/reverse flows
```

関連コマンド

Command	説明
show conn data-rate	接続データレートトラッキングの現在の状態を表示します。

Command	説明
show conn detail	データレート値によってフィルタ処理された接続を表示します。
clear conn data-rate	現在の最大データレート値をクリアします。

connect fxos

FXOS Service Manager CLI モードを開始するには、**connect fxos** コマンドを使用します。

connect fxos

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

FXOS は、Firepower 2100、4100、および 9300 シリーズ デバイスの基盤となるソフトウェアです。

例

次に、脅威に対する防御 CLI で起動したときに FXOS CLI を開始する例を示します。? と入力し、FXOS で使用可能なコマンドを確認します。

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

(...remaining copyrights omitted...)

kp-fpr2100-2#
```

次に、（**connect ftd** FXOS コマンドを使用して）最初に FXOS CLI から 脅威に対する防御 CLI を開始した場合の動作の例を示します。

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```

copy

フラッシュメモリに、またはフラッシュメモリからファイルをコピーするには、**copy** コマンドを使用します。

copy [**/noconfirm** | **/noverify**] [*interface_name*] { **/pcap capture:/** [*buffer_name*] | *src_url* | **running-config** | **startup-config** } *dest_url*

構文の説明

/noverify	（オプション）開発キー署名済みイメージをコピーするときに署名検証をスキップします。
/noconfirm	（オプション）確認のプロンプトを表示しないでファイルをコピーします。
interface_name	（任意）ファイルをコピーするインターフェイス名を指定します。インターフェイスを指定しない場合、脅威に対する防御 はデータルーティングテーブルを確認します。データルーティングテーブルの一部ではない**管理**インターフェイスまたはその他の管理専用インターフェイスを使用するには、このオプションを使用して指定する必要があります。
/pcap capture:/ [*buffer_name*]	指定したバッファから **capture** コマンドの raw パケットキャプチャダンプをコピーします。
running-config	システム メモリに格納されている実行コンフィギュレーションを指定します。
startup-config	フラッシュ メモリに格納されているスタートアップ コンフィギュレーションを指定します。スタートアップコンフィギュレーションは、フラッシュメモリ内の隠しファイルになっています。

src-url

dest-url

コピー元のファイル（コピーするファイル）とコピー先のファイル（コピーで作成するファイル）を指定します。2つのリモートロケーション間でコピーすることはできないため、コピー元のファイルがローカルの場合に、コピー先のファイルはローカルまたはリモートになります。コピー元のファイルがリモートの場合、コピー先のファイルはローカルである必要があります。ファイルの場所には次の URL シンタックスを使用します。

- **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
- **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。
- **smb:/**[[*path/*]*filename*]：サーバー メッセージブロック、UNIX サーバーのローカル ファイル システムを示します。
- **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。
- **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*]
- **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：SCP サーバーを示します。**;int=***interface* オプションを指定すると、ルートルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュアコピー（SCP）サーバーに接続するようになります。
- **system:/**[[*path/*]*filename*]：システムメモリを表します。
- **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：TFTP サーバーを示します。パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。
- **cluster_trace:** ：cluster_trace ファイルシステムを示します。

コマンド履歴

リリース	変更内容
7.1	インターフェイスを指定しない場合、脅威に対する防御はデータルーティングテーブルを確認します。管理ルーティングテーブルへのフォールバックはありません。以前は、デフォルトのルックアップは、データルーティングテーブルへのフォールバックを備えた管理ルーティングテーブルでした。管理インターフェイスと診断インターフェイスの統合により、管理ルーティングテーブルは自動的に使用されなくなりました。使用する場合は、管理インターフェイスを指定する必要があります。
6.1	このコマンドが導入されました。

使用上のガイドライン

クラスタ全体のキャプチャを実行後、マスターユニットで次のコマンドを入力して、クラスタ内のすべてのユニットから同じキャプチャ ファイルを TFTP サーバーに同時にコピーできます。

cluster exec copy /noconfirm /pcap capture:*cap_name* **tftp://***location***/***path***/***filename***.pcap**

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。ここで、A および B はクラスタ ユニット名です。

（注） ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

例

次に、インストールログのコピーを作成する例を示します。

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

次に、システム実行スペースでファイルをディスクから TFTP サーバーにコピーする例を示します。

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

次に、実行コンフィギュレーションを TFTP サーバーにコピーする例を示します。

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

次に、開発キー署名済みイメージを検証せずにコピーする例を示します。

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

関連コマンド

Command	説明
write net	実行コンフィギュレーションを TFTP サーバーにコピーします。

cpu hog granular-detection

リアルタイムの占有検出を行い、短期間での CPU 占有しきい値を設定するには、**cpu hog granular-detection** コマンドを使用します。

cpu hog granular-detection ［**count** *number*］［**threshold** *value*］

構文の説明

count *number*	実行されるコード実行割り込みの数を指定します。値は 1 ～ 10000000 です。デフォルト値および推奨値は 1000 です。
threshold *value*	範囲は 1 ～ 100 です。設定されていない場合はデフォルトが使用されます。デフォルトはプラットフォームによって異なります。

コマンド デフォルト

デフォルトの **count** は 1000 です。デフォルトの **threshold** は、プラットフォームによって異なります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

cpu hog granular-detection コマンドでは、現在のコード実行に 10 ミリ秒ごとに割り込み、割り込みの総数がカウントされます。割り込みによって CPU 占有がチェックされます。存在する場合は、ログに記録されます。このコマンドによって、データ パスでの CPU 占有検出の精度が低下します。

各スケジューラ ベースの占有は、最大 5 つの割り込みベースの占有エントリに関連付けられます。各エントリには最大 3 つのトレースバックが含まれる場合があります。割り込みベースの占有は上書きできません。空き領域がない場合は、新しい占有が廃棄されます。スケジューラ ベースの占有は、LRU ポリシーに従って引き続き再利用され、関連付けられている割り込みベースの占有はそのときにクリアされます。

例

次に、CPU 占有検出をトリガーする例を示します。

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

関連コマンド

Command	説明
show processes cpu-hog	CPU を占有しているプロセスを表示します。
clear process cpu-hog	CPU を占有しているプロセスをクリアします。

cpu profile activate

CPU プロファイリングを開始するには、**cpu profile activate** コマンドを使用します。

cpu profile activate ［*n_samples* ［**sample-process** *process_name*］［**trigger cpu-usage** *cpu%* ［*process_name*］］］

構文の説明

n_samples	サンプル数 *n* を保存するためのメモリを割り当てます。有効値は 1 ～ 100,000 です。
sample-process *process_name*	特定のプロセスのみをサンプリングします。
trigger cpu-usage *cpu%* [*process_name*]	グローバルな CPU 使用率である 5 秒を超えるまでプロファイラを開始しないようにし、CPU 使用率がこの値を下回った場合はプロファイラを停止します。 プロセス名を指定すると、プロセスの 5 秒間の CPU 使用率がトリガーとして使用されます。

コマンド デフォルト

n_samples のデフォルト値は 1000 です。

cpu% のデフォルト値は 0 です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

CPU プロファイラは、CPU 使用率が高いプロセスの特定に役立ちます。CPU のプロファイリングでは、タイマー割り込みが発生したときに CPU で動作していたプロセスのアドレスをキャプチャします。このプロファイリングは、CPU の負荷に関係なく、10 ミリ秒ごとに発生します。たとえば、5000 のサンプルを取得する場合、プロファイリングが完了するまで正確に 50 秒かかります。CPU プロファイラが使用する CPU 時間が比較的少ない場合は、サンプルの収集に時間がかかります。CPU プロファイル レコードは、別のバッファでサンプリングされます。

show cpu profile コマンドを **cpu profile activate** コマンドとともに使用して、ユーザーが収集できる情報、および TAC が CPU の問題のトラブルシューティングに使用できる情報を表示します。**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.
```

例

次の例では、プロファイラをアクティブ化して、デフォルトである1000個のサンプルを格納するように指示します。次に、**show cpu profile** コマンドは、プロファイリングが進行中であることを示します。いくらかの時間が経過してから、次の**show cpu profile** コマンドは、プロファイリングが完了したことを示します。最後に、**show cpu profile dump** コマンドを使用して結果を取得します。出力をコピーし、シスコテクニカルサポートに提出します。完全な出力を得るには、SSH セッションをログに記録する必要があります。

```
> 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.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 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.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

関連コマンド

Command	説明
show cpu profile	CPU プロファイリングの進行状況を表示します。
show cpu profile dump	プロファイリングに関して、完了していない結果または完了した結果を表示します。

cpu profile dump

CPU プロファイリングの結果をテキストファイルに保存するには、**cpu profile dump** コマンドを使用します。

cpu profile dump *dest_url*

構文の説明

dest_url	• **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。いずれのオプションも使用できます。 • **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。 • **smb:/**[[*path/*]*filename*]：UNIX サーバーのローカルファイルシステムを示します。サーバー メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク システムで使用されます。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。 • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバーに接続するようになります。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。 • **cluster:**：クラスタファイルシステムを示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

CPU profile dump コマンドは、CPU プロファイラの出力を、指定されたテキストファイルに 16 進数形式で書き込みます。

例

次に、最新の CPU プロファイルダンプを cpudump.txt という名前のファイルに保存する例を示します。

```
> cpu profile dump disk0:/cpudump.txt
```

関連コマンド

Command	説明
show cpu profile dump	プロファイリングに関して、完了していない結果または完了した結果を表示します。

crashinfo force

デバイスを強制的にクラッシュさせるには、**crashinfo force** コマンドを使用します。

crashinfo force /noconfirm {**page-fault** | **watchdog** | **process** *process_ID*}

構文の説明

page-fault	ページフォールトを利用して、デバイスを強制的にクラッシュさせます。
watchdog	ウォッチドッグを利用して、デバイスを強制的にクラッシュさせます。
process *process_ID*	process_ID で指定されたプロセスを強制的にクラッシュさせます。プロセス ID を表示するには、**show kernel process** コマンドを使用します。

コマンド デフォルト

デフォルトでは、デバイスはフラッシュメモリにクラッシュ情報ファイルを保存します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュを、**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュと区別できません。これは、これらのコマンドによって実際にクラッシュが発生しているためです。デバイスは、クラッシュのダンプが完了するとリロードします。

注意：実稼働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはデバイスをクラッシュさせて、強制的にリロードを実行します。

例

次に、ページフォールトにより強制的にクラッシュを実行する例を示します。

```
> crashinfo force /noconfirm page-fault
```

関連コマンド

Command	説明
clear crashinfo	クラッシュ情報ファイルの内容をクリアします。
crashinfo test	デバイスでフラッシュメモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo test

フラッシュメモリのファイルにクラッシュ情報を保存するデバイスの機能をテストするには、**crashinfo test** コマンドを使用します。

crashinfo test

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

crashinfo test コマンドを入力してもデバイスはクラッシュしません。フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

例

次に、クラッシュ情報ファイル テストの出力例を示します。

```
> crashinfo test
```

関連コマンド

Command	説明
clear crashinfo	クラッシュ情報ファイルの内容をクリアします。
crashinfo force	デバイスを強制的にクラッシュさせます。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crypto ca trustpool export

PKI trustpool を構成する証明書をエクスポートするには、**crypto ca trustpool export** コマンドを使用します。

crypto ca trustpool export *filename*

構文の説明

filename	エクスポートされた trustpool 証明書を保存するファイル。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、アクティブな trustpool の内容全体を、指定されたファイルパスに pem コード形式でコピーします。

例

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

関連コマンド

Command	説明
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
crypto ca trustpool remove	1 つの証明書を PKI trustpool から削除します。
show crypto ca trustpool	PKI trustpool を表示します。

crypto ca trustpool import

PKI trustpool を構成する証明書をインポートするには、**crypto ca trustpool import** コマンドを使用します。

crypto ca trustpool import ［**clean**］ **url** *url* **noconfirm** ［**signature-required**］
crypto ca trustpool import ［**clean**］ **default noconfirm**

構文の説明

clean	インポート前にダウンロードされたすべての trustpool 証明書を削除します。
default	デバイスのデフォルトの信頼できる CA リストに戻します。
noconfirm	すべてのインタラクティブ プロンプトを抑制します。
signature-required	署名されたファイルのみを受け入れることを指定します。**signature-required** キーワードが含まれている場合に、シグネチャが存在しないかまたは確認できないと、インポートが失敗します。

url *url*	インポートする trustpool ファイルの場所を指定します。 • **disk0:/**[[*path/*]*filename*]：内部フラッシュメモリを示します。 • **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。 • **smb:/**[[*path/*]*filename*]：UNIX サーバーのローカルファイルシステムを示します。サーバー メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク システムで使用されます。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。 • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバーに接続するようになります。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、trustpool バンドルを cisco.com からダウンロードするときに、ファイルのシグネチャを検証できます。バンドルを他のソースからダウンロードする場合や、シグネチャをサポートしていない形式でダウンロードする場合は、有効なシグネチャは必須ではありません。ユーザーにはシグネチャのステータスが通知され、バンドルを受け入れるかどうかを選択できます。

表示される可能性のあるインタラクティブな警告は、次のとおりです。

- 無効なシグネチャを持つシスコ バンドル形式
- シスコ以外のバンドル形式
- 有効なシグネチャを持つシスコ バンドル形式

（注） ファイルのシグネチャを確認できない場合は、その他の方法によって正規のファイルであることを確認していない限り、証明書をインストールしないでください。

例

次に、デフォルトの trustpool を復元する例を示します。

```
> crypto ca trustpool import clean default noconfirm
```

関連コマンド

Command	説明
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool remove	1 つの証明書を PKI trustpool から削除します。
show crypto ca trustpool	PKI trustpool を表示します。

crypto ca trustpool remove

PKI trustpool から指定した 1 つの証明書を削除するには、**crypto ca trustpool remove** コマンドを使用します。

crypto ca trustpool remove *cert_fingerprint* ［**noconfirm**］

構文の説明

cert_fingerprint	証明書フィンガープリントは 16 進数です。
noconfirm	すべてのインタラクティブプロンプトを抑制するには、このキーワードを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、証明書を削除する例を示します。

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

関連コマンド

Command	説明
clear crypto ca trustpool	trustpool からすべての証明書を削除します。
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
show crypto ca trustpool	PKI trustpool を表示します。

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