セキュリティ モジュール/エンジン管理

FXOS セキュリティ モジュール/セキュリティ エンジンについて

FXOS CLI を使用して、セキュリティ モジュール/エンジン の次の機能を実行できます。

- [デコミッション（Decommission）]（セキュリティモジュールのみ）：セキュリティモジュールを使用停止にすると、セキュリティモジュールはメンテナンスモードに設定されます。また、特定の障害状態を修正するために、セキュリティモジュールをデコミッションしてから確認応答することもできます。セキュリティモジュールの使用停止 （2 ページ）を参照してください。
- [確認応答（Acknowledge）]：新たにインストールされたセキュリティモジュールをオンラインにします。セキュリティモジュール/エンジンの確認応答 （3 ページ）を参照してください。
- [電源の再投入（Power Cycle）]：セキュリティ モジュール/エンジンを再起動します。セキュリティモジュール/エンジンの電源オン/オフ （3 ページ）を参照してください。
- [再初期化（Reinitialize）]：セキュリティモジュール/エンジンのハードディスクを再フォーマットし、導入済みのすべてのアプリケーションや設定をセキュリティ モジュール/エンジンから削除し、システムを再起動します。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合は、再初期化が完了すると、FXOSはアプリケーション ソフトウェアをインストールし、論理デバイスを再度導入し、アプリケーションを自動的に起

動します。セキュリティ モジュール/エンジンの最初期化 （4 ページ）を参照してください。

警告 セキュリティ モジュール/エンジンのすべてのアプリケーションデータが再初期化時に削除されます。セキュリティ モジュール/エンジンを再初期化する前に、すべてのアプリケーションデータをバックアップしておいてください。

- [電源オフ/オン（Power off/on）]：セキュリティ モジュール/エンジンの電源状態を切り替えます。セキュリティモジュール/エンジンの電源オン/オフ （3 ページ） を参照してください。

セキュリティモジュールの使用停止

セキュリティ モジュールを使用停止にすると、セキュリティ モジュール オブジェクトが設定から削除され、そのセキュリティモジュールは管理対象外になります。セキュリティモジュール上で実行していた論理デバイスやソフトウェアは非アクティブになります。

セキュリティ モジュールの使用を一時的に中止する場合に、セキュリティ モジュールを使用停止にできます。

（注） **delete decommissioned** コマンドを使用してモジュールを削除するには、その前に、モジュールを使用停止にする必要があります。

手順

ステップ 1 モジュールを使用停止にするには、**decommission server** コマンドを入力します。

decommission server {*ID* | *chassis-id/blade-id*}

使用停止にするモジュールをホストしているデバイスの種類によって、モジュールはモジュールIDで識別されるか（4100シリーズ）、シャーシ番号とモジュール番号で識別されます（9300デバイス）。

例：

```
FP9300-A# decommission server 1/2
FP9300-A* #
```

ステップ 2 **commit-buffer** コマンドを入力して変更をコミットします。

使用停止にされたモジュールの一覧を表示するには、**show server decommissioned** コマンドを使用します。

セキュリティモジュール/エンジンの確認応答

新しいセキュリティモジュールがシャーシに取り付けられた後、または既存のモジュールが異なる製品ID（PID）を持つモジュールで交換された後、セキュリティモジュールを確認応答してからでなければ、そのモジュールを使用することはできません。

セキュリティ モジュールのステータスが [mismatch] または [token mismatch] として示されている場合、スロットに取り付けたセキュリティモジュールのデータが、そのスロットに以前インストールされたデータと一致していないことを意味します。セキュリティモジュールに既存のデータがあり、新しいスロットでそのデータを使用する（つまり、そのセキュリティモジュールは不注意で誤ったスロットに取り付けられたのではない）場合は、論理デバイスを展開する前に、セキュリティ モジュールを再初期化する必要があります。

手順

ステップ 1 シャーシ モードに入ります。

```
scope chassis
```

ステップ 2 交換しないモジュールを使用停止にして物理的に取り外した後、またはモジュールを同じタイプではない（つまり、異なる PID を持つ）別のモジュールと交換した後、**acknowledge slot** コマンドを入力します。

```
acknowledge slot
```

例：

```
FP9300-A# scope chassis
FP9300-A /chassis # acknowledge slot 2
FP9300-A /chassis* #
```

ステップ 3 設定をコミットします。

```
commit-buffer
```

セキュリティモジュール/エンジンの電源オン/オフ

セキュリティ モジュール/エンジンの電源の再投入を行うには、次の手順に従います。

手順

ステップ 1 /service-profile モードを開始します。

scope service-profile server {*chassis_id*>/*blade_id*}

例：

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile #
```

ステップ 2 次のいずれかの **cycle** コマンドを入力します。

- **cycle cycle-immediate**：直ちにモジュールの電源の再投入を行います。
- **cycle cycle-wait**：システムはモジュールで実行中のアプリケーションがシャットダウンするまで最大 5 分待ってから、モジュールの電源の再投入を行います。

例：

```
FP9300-A /org/service-profile # cycle cycle-wait
FP9300-A /org/service-profile* #
```

ステップ 3 バッファをコミットしてモジュールの電源の再投入を行います。

commit-buffer

セキュリティ モジュール/エンジンの最初期化

セキュリティ モジュール/エンジン を再初期化すると、セキュリティ モジュール/エンジン のハードディスクがフォーマットされ、インストールされているすべてのアプリケーションインスタンス、設定、およびデータが削除されます。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合、再初期化が完了すると、FXOSはアプリケーション ソフトウェアを再インストールし、論理デバイスを再導入して、アプリケーションを自動的に起動します。

⚠

注意 セキュリティ モジュール/エンジンのすべてのアプリケーション データが再初期化時に削除されます。Back up all application data before reinitializing a セキュリティ モジュール/エンジン.

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

ステップ 2 目的のモジュールでスロット モードを開始します。

scope slot {*slot_id*}

例：

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot #
```

ステップ 3 **reinitialize** コマンドを入力します。

例：

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
Warning: Reinitializing blade takes a few minutes. All the application data on blade
will get lost. Please backup application running config files before commit-buffer.
FP9300-A /ssa/slot* #
```

ステップ 4 必要に応じて、アプリケーションのコンフィギュレーション ファイルをバックアップします。

ステップ 5 モジュールを再初期化するためのバッファをコミットします。

commit-buffer

モジュールが再起動し、そのモジュール上のすべてのデータが削除されます。このプロセスには数分かかることがあります。

ステップ 6 **show detail** コマンドを使用すると、再フォーマット化操作の進行状態、再フォーマット化の結果（成功または失敗）、さらに操作が失敗した場合はエラー コードを確認することができます。

ネットワークモジュールの確認応答

新しいネットワークモジュールがシャーシに取り付けられた後、または既存のモジュールが異なる製品ID（PID）を持つモジュールで交換された後、ネットワークモジュールを確認応答してからでなければ、そのモジュールを使用することはできません。

手順

ステップ 1 `scope fabric-interconnect` モードを開始します。

scope fabric-interconnect

ステップ 2 新しいモジュールをインストールした後、またはモジュールを同じタイプではない（つまり、異なるPIDを持つ）別のネットワークモジュールと交換した後、**acknowledge** コマンドを入力します。

```
acknowledge
```

例：

```
FPR1 /fabric-interconnect # acknowledge
  fault  Fault
  slot   Card Config Slot Id  <======
```

ステップ 3 挿入されたスロットを確認するには、**acknowledge slot** を入力します。

```
acknowledge slot
```

例：

```
FPR1 /fabric-interconnect # acknowledg slot 2
  0-4294967295  Slot Id
```

ステップ 4 設定をコミットします。

```
commit-buffer
```

ネットワーク モジュールのオフラインまたはオンラインの切り替え

CLI コマンドを使ってネットワーク モジュールをオフラインにしたりオンラインに戻したりするには、次の手順を実行します。この方法は、モジュールのオンライン挿入や削除（OIR）を実行する場合などに使用されます。

（注）

- ネットワーク モジュールを取り外して交換する場合は、お使いのデバイスに該当するインストール ガイドの中で、メンテナンスとアップグレードの章にある指示に従ってください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.htmlを参照してください。
- 8 ポート1G 銅線 FTW ネットワークモジュール（FPR-8X1G-F FTW）でネットワークモジュールのオンライン挿入および取り外し（OIR）を実行する場合は、この手順を使用してカードをオンラインにするまで、ネットワークモジュールの LED が消灯していることを確認してください。LED は最初にオレンジ色で点滅します。ネットワークモジュールが検出されてアプリケーションがオンラインになると緑色に変わります。

（注） FTWネットワークモジュールを取り外してからスロットに対して確認応答すると、ネットワーク モジュール ポートは 脅威に対する防御 の論理デバイスから削除されます。この場合、ネットワークモジュールを再挿入する前に、Management Center を使用してハードウェアのバイパスインラインセット構成を削除する必要があります。ネットワークモジュールを挿入し直すと、次のことを行う必要があります：

- シャーシマネージャ またはFXOS コマンドライン インターフェイス（CLI）を使用して、ネットワーク モジュール ポートを管理用オンライン状態として設定します。
- 脅威に対する防御 論理デバイスにネットワーク モジュール ポートを追加し、Management Center を使用してポートを再設定します。

スロットに対して確認応答せずにネットワークモジュールを取り外すと、インラインセット構成は保持され、Management Center ではポートがダウン状態と表示されます。ネットワークモジュールを再挿入すると、以前の設定が復元されます。

ハードウェアバイパスのインラインセットの詳細については、「ハードウェア バイパス ペア」を参照してください

手順

ステップ 1 次のコマンドを使用して /fabric-interconnect モードに入った後、オフラインにする対象のモジュールの /card モードに入ります。

```
scope fabric-interconnect a
scope card ID
```

ステップ 2 **show detail** コマンドを使用すると、このカードに関する、現在のステータスなどの情報を表示することができます。

ステップ 3 モジュールをオフラインにするには、次のコマンドを入力します。

```
set adminstate offline
```

ステップ 4 **commit-buffer** コマンドを入力して、設定の変更内容を保存します。

再度 **show detail** コマンドを使用すると、モジュールがオフラインであることを確認できます。

ステップ 5 ネットワーク モジュールをオンラインに戻すには、次のコマンドを入力します。

```
set adminstate online
commit-buffer
```

例

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
```

```
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Offline
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Offline
    Power State: Off
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card #
```

ブレードのヘルスモニタリング

指定した回数の予期しないアプリケーションの再起動がブレードで検出されると、セキュリティモジュールまたはエンジンでフェールセーフが実行されます。これにより、冗長なHAまたはクラスタデプロイメントでさらなる副作用を引き起こす可能性のある無限のブートループ状態を防止します。

ブレードプラットフォームは定期的にヘルスチェックを実行し、MIOに報告します。ブレードが障害状態の場合、障害とエラーのメッセージが通知されます。

スロットのステータスを表示するには、`show detail` CLI を使用します。

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show detail
Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Fault
```

```
    Disk Format State: Ok
    Disk Format Status:
    Clear Log Data: Available
 Error Msg: Security Module is in failsafe mode. Applications are blocked from starting
 in this mode. Connect to security module for troubleshooting or to disable failsafe
mode. The app-instance can also be deleted. Security Module: 1. Application:
cisco-asa.99.1.20.52.
```

トラブルシューティングとデバッギング

FXOS CLI からブレード設定を監視、構成、およびリセットできます。

`show fault` および `show events` を使用して、セキュリティモジュールを監視します。

```
Firepower /ssa/slot # show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F1546    2017-08-19T12:11:18.036    801162 Security Module 1 is in failed
state. Error: Security Module is in failsafe mode. Applications are blocked from starting
 in this mode. Connect to security module for troubleshooting or to disable failsafe
mode. The app-instance can also be deleted. Security Module: 1. Application:
cisco-asa.99.1.20.52.
```

```
Firepower /ssa/slot # show event
Creation Time               ID       Code     Description
----------------------- -------- -------- -----------
2017-08-19T12:11:18.037    801163 E4197940 Slot 1 is in failed state. Error:Security
Module is in failsafe mode. Applications are blocked from starting in this mode. Connect
 to security module for troubleshooting or to disable failsafe mode. The app-instance
can also be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.
```

次の CLI を使用して、セキュリティモジュールを設定します。

```
Firepower-module> config ?
    syslog           => Configure syslog parameters for remote server and port
    vnic             => Configure specified VNIC
    memory           => Configure memory monitor
    disk             => Configure disk monitor
    process          => Configure process cpu monitor
    maxRestart       => Configure maximum restarts CSP. 0 shall mean Disable Restart.
Default 8
    restartTimeInter => Configure time in seconds to block all CSPs from starting if
server restarts maxRestart in this interval. Default 3600
    restartCounters  => To reset the restart_count
```

- `config maxRestart`：プロセスマネージャがサービスの開始を停止する前に、サービス/CSP によってブレードが再起動される回数。デフォルト値は 8 です。値が 0（ゼロ）に設定されると、この機能は無効になります。
- `config restartTimeInterval`：アプリが maxRestart で設定した回数以上再起動した場合に、アプリケーションが再起動しない時間間隔。デフォルト値は 3600 秒です。
- `show maxRestart`：現在のカウンタおよび設定された値を表示します。
- `config restartCounters reset`：再起動カウンタを 0 にリセットします。

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