



トラブルシューティング

- [パケットキャプチャ](#) (1 ページ)
- [ネットワーク接続のテスト](#) (10 ページ)
- [管理インターフェイスのステータスのトラブルシューティング](#) (12 ページ)
- [ポート チャネル ステータスの確認](#) (13 ページ)
- [ソフトウェア障害からの回復](#) (15 ページ)
- [破損ファイル システムの回復](#) (20 ページ)
- [管理者パスワードが不明な場合における工場出荷時のデフォルト設定の復元](#) (31 ページ)
- [トラブルシューティング ログ ファイルの生成](#) (33 ページ)
- [モジュールのコアダンプの有効化](#) (36 ページ)
- [シリアル番号の確認 Firepower 4100/9300 シャーシ](#) (37 ページ)
- [RAID 仮想ドライブの再構築](#) (37 ページ)
- [SSD を使用している場合の問題の特定](#) (39 ページ)

パケットキャプチャ

パケット キャプチャ ツールは、接続と設定の問題のデバッグや、Firepower 4100/9300 シャーシを通過するトラフィックフローの理解に使用できる価値ある資産です。パケットキャプチャ ツールを使用すると、Firepower 4100/9300 シャーシの特定のインターフェイスを通過するトラフィックについてログを記録できます。

複数のパケット キャプチャ セッションを作成でき、各セッションで複数のインターフェイスのトラフィックをキャプチャできます。パケットキャプチャセッションに含まれる各インターフェイス用に、個別のパケット キャプチャ (PCAP) ファイルが作成されます。

バックプレーンポート マッピング

Firepower 4100/9300 シャーシでは、内部バックプレーン ポートに次のマッピング ポートを使用します。

セキュリティ モジュール	ポート マッピング	説明
セキュリティ モジュール 1/セキュリティ エンジン	Ethernet1/9	Internal-Data0/0
セキュリティ モジュール 1/セキュリティ エンジン	Ethernet1/10	Internal-Data0/1
セキュリティ モジュール 2	Ethernet1/11	Internal-Data0/0
セキュリティ モジュール 2	Ethernet1/12	Internal-Data0/1
セキュリティ モジュール 3	Ethernet1/13	Internal-Data0/0
セキュリティ モジュール 3	Ethernet1/14	Internal-Data0/1

パケットキャプチャの注意事項および制限事項

パケットキャプチャ ツールには、次の制限事項があります。

- キャプチャできるのは最大 100 Mbps までです。
- パケットキャプチャセッションの使用に使用可能な十分な記憶域がなくても、パケットキャプチャセッションを作成できます。パケットキャプチャセッションを開始する前に、使用可能な十分な記憶域があることを確認する必要があります。
- シングル幅の 4x100Gbps または 2x100Gbps ネットワークモジュール（それぞれ部品番号 FPR-NM-4X100G および FPR-NM-2X100G）でのパケットキャプチャセッションの場合、モジュールの `adminstate` が `off` に設定されると、キャプチャセッションが自動的に無効になり、「Oper State Reason: Unknown Error」というメッセージが生成されます。モジュールの `adminstate` を再度 `on` に設定してから、キャプチャセッションを再起動する必要があります。

他のすべてのネットワークモジュールでは、モジュールの `adminstate` が変更されてもパケットキャプチャセッションが継続されます。

- 複数のアクティブなパケットキャプチャセッションはサポートされません。
- 内部スイッチの入力の段階でのみキャプチャされます。
- 内部スイッチが認識できないパケット（セキュリティグループタグ、ネットワークサービスヘッダーパケットなど）にはフィルタの効果がありません。
- 1 つ以上の親で複数のサブインターフェイスを使用する場合でも、セッションごとに 1 つのサブインターフェイスのパケットのみをキャプチャできます。
- EtherChannel 全体または EtherChannel のサブインターフェイスのパケットをキャプチャできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバインターフェイスごとにパケットをキャプチャできます。親インターフェイス

ではなくサブインターフェイスを割り当てる場合は、メンバインターフェイス上のパケットをキャプチャすることはできません。

- キャプチャセッションがアクティブな間は、PCAP ファイルをコピーしたり、エクスポートできません。
- パケットキャプチャセッションを削除すると、そのセッションに関連するすべてのパケットキャプチャファイルも削除されます。

パケット キャプチャ セッションの作成または編集

手順

ステップ 1 パケット キャプチャ モードを開始します。

```
Firepower-chassis # scope packet-capture
```

ステップ 2 フィルタを作成します。[パケット キャプチャのためのフィルタの設定 \(6 ページ\)](#) を参照してください。

パケット キャプチャセッションに含まれるインターフェイスのいずれかにフィルタを適用できます。

ステップ 3 パケット キャプチャセッションを作成または編集するには、次の操作を行います。

```
Firepower-chassis /packet-capture # enter session session_name
```

ステップ 4 このパケット キャプチャセッションに使用するバッファ サイズを指定します。

```
Firepower-chassis /packet-capture/session* # set session-memory-usage session_size_in_megabytes
```

指定するバッファ サイズは 1 ~ 2048 MB にする必要があります。

ステップ 5 このパケット キャプチャセッションでキャプチャするパケットの長さを指定します。

```
Firepower-chassis /packet-capture/session* # set session-pcap-snaplength session_snap_length_in_bytes
```

スナップの指定長は、64 ~ 9006 バイトの範囲内にする必要があります。セッションスナップ長を設定しない場合のデフォルトのキャプチャ長は、1518 バイトです。

ステップ 6 このパケット キャプチャセッションに含める必要がある物理ソース ポートを指定します。

複数のポートからキャプチャしたり、物理ポートやアプリケーションポートの両方から同じパケットキャプチャセッション中に取得することができます。別のパケットキャプチャファイルがセッションに含まれる各ポート用に作成されます。EtherChannel 全体のパケットをキャプチャすることはできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバー インターフェイスごとにパケットをキャプチャできます。親 EtherChannel ではなくサブインターフェイスを割り当てる場合は、メンバインターフェイス上のパケットをキャプチャすることはできません。

(注) パケットキャプチャセッションからポートを削除するには、次に示すコマンドで **create** の代わりに **delete** を使用します。

a) 物理ポートを指定します。

```
Firepower-chassis /packet-capture/session* # create {phy-port | phy-aggr-port} port_id
```

例 :

```
Firepower-chassis /packet-capture/session* # create phy-port Ethernet1/1
Firepower-chassis /packet-capture/session/phy-port* #
```

b) サブインターフェイスのパケットをキャプチャします。

```
Firepower-chassis /packet-capture/session/phy-port* # set subinterface id
```

1つ以上の親で複数のサブインターフェイスを使用する場合でも、キャプチャセッションごとに1つのサブインターフェイスのパケットのみをキャプチャできます。Etherchannelのサブインターフェイスはサポートされていません。親インターフェイスをインスタンスにも割り当てる場合、親インターフェイスまたはサブインターフェイスのいずれかを選択できます。両方を選択することはできません。

例 :

```
Firepower-chassis /packet-capture/session/phy-port* # set subinterface 100
Firepower-chassis /packet-capture/session/phy-port* #
```

c) コンテナインスタンスの場合、コンテナインスタンス名を指定します。

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier instance_name
```

例 :

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/phy-port* #
```

d) アプリケーションタイプを指定します。

```
Firepower-chassis /packet-capture/session/phy-port* # set app name
```

例 :

```
Firepower-chassis /packet-capture/session/phy-port* # set app ftd
Firepower-chassis /packet-capture/session/phy-port* #
```

e) (任意) 目的のフィルタを適用します。

```
Firepower-chassis /packet-capture/session/phy-port* # set {source-filter} filtername
```

(注) ポートからフィルタを削除するには、**set source-filter ""** を使用します。

f) 必要に応じて上記のステップを繰り返して必要なポートをすべて追加します。

ステップ7 このパケットキャプチャセッションに含める必要があるアプリケーションソースポートを指定します。

複数のポートからキャプチャしたり、物理ポートやアプリケーションポートの両方から同じパケットキャプチャセッション中に取得することができます。別のパケットキャプチャファイラがセッションに含まれる各ポート用に作成されます。

(注) パケットキャプチャセッションからポートを削除するには、次に示すコマンドで **create** の代わりに **delete** を使用します。

a) アプリケーションポートを指定します。

```
Firepower-chassis /packet-capture/session* # create app_port module_slot link_name interface_name app_name
```

構文の説明

module_slot	アプリケーションがインストールされているセキュリティモジュール。
link_name	インターフェイスを指すユーザー記述名 (link1、inside_port1 など)。
interface_name	パケットをキャプチャする必要があるアプリケーションに接続されているインターフェイス (Ethernet1/1、Ethernet2/2 など)。
app_name	モジュールにインストールされているアプリケーション (ftd、asa)。

b) コンテナインスタンスの場合、コンテナインスタンス名を指定します。

```
Firepower-chassis /packet-capture/session/app-port* # set app-identifier instance_name
```

例 :

```
Firepower-chassis /packet-capture/session/app-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/app-port* #
```

構文の説明

instance_name	パケットキャプチャが必要なアプリケーションインスタンスの名前 (native、container など)。
----------------------	---

c) (任意) 目的のフィルタを適用します。

```
Firepower-chassis /packet-capture/session/phy-port* # set {source-filter} filtername
```

構文の説明

filtername	「create filter」コマンドによる packet-capture 範囲のフィルタ名。
-------------------	---

(注) ポートからフィルタを削除するには、**set source-filter ""** を使用します。

d) 必要に応じて上記のステップを繰り返して必要なアプリケーションポートをすべて追加します。

ステップ8 パケットキャプチャセッションをすぐに開始するには、次の操作を行います。

```
Firepower-chassis /packet-capture/session* # enable
```

新しく作成したパケットキャプチャセッションはデフォルトでは無効になっています。セッションを明示的に有効にすると、変更がコミットされたときにパケットキャプチャセッションがアクティブになります。別のセッションがすでにアクティブになっている場合、セッションを有効にするとエラーが生成されます。このセッションを有効にする前に、すでにアクティブなパケットキャプチャセッションを無効にする必要があります。

ステップ9 トランザクションをシステム設定にコミットします。

```
Firepower-chassis /packet-capture/session* # commit-buffer
```

パケットキャプチャセッションを有効にすると、システムはパケットのキャプチャを開始します。セッションからPCAPファイルをダウンロードする前に、キャプチャを停止する必要があります。

例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create session asalinside
Firepower-chassis packet-capture/session # set session-memory-usage 256
Firepower-chassis packet-capture/session* # create phy-port Ethernet3/1
Firepower-chassis packet-capture/session* # create phy-aggr-port Ethernet2/1/1
Firepower-chassis packet-capture/session* # create app-port 1 link1 Ethernet 1/1 asa
Firepower-chassis packet-capture/session* # exit
Firepower-chassis packet-capture* # create filter interfacelvlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcIP 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcPort 80
Firepower-chassis packet-capture/filter* # set destIP 10.10.10.10
Firepower-chassis packet-capture/filter* # set destPort 5050
Firepower-chassis packet-capture/filter* # exit
Firepower-chassis packet-capture/session* # scope phy-port Ethernet3/1
Firepower-chassis packet-capture/session/phy-port* # set src-filter interfacelvlan100
Firepower-chassis packet-capture/session/phy-port* # exit
Firepower-chassis packet-capture/session* # scope app-port 1 link1 Ethernet1/1 asa
Firepower-chassis packet-capture/session/app-port* # set src-filter interfacelvlan100
Firepower-chassis packet-capture/session/app-port* # exit
Firepower-chassis packet-capture/session* # enable
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

パケットキャプチャのためのフィルタの設定

パケットキャプチャセッションに含まれるトラフィックを制限するためにフィルタを作成できます。パケットキャプチャセッションの作成中にどのインターフェイスが特定のフィルタを使用するかを選択できます。



(注) 現在実行中のパケット キャプチャ セッションに適用されているフィルタを変更または削除する場合、そのセッションを無効にしてから再度有効にするまでは実行されません。

手順

ステップ 1 パケット キャプチャ モードを開始します。

```
Firepower-chassis # scope packet-capture
```

ステップ 2 新しいソフトウェア キャプチャ フィルタを作成するには、次の操作を行います。

```
Firepower-chassis /packet-capture # create filter filter_name
```

既存のパケット キャプチャ フィルタを編集するには、次の操作を行います。

```
Firepower-chassis /packet-capture # enter filter filter_name
```

既存のパケット キャプチャ フィルタを削除するには、次の操作を行います。

```
Firepower-chassis /packet-capture # delete filter filter_name
```

ステップ 3 1 つ以上のフィルタ プロパティを設定することによってフィルタの詳細を指定します。

```
Firepower-chassis /packet-capture/filter* # set <filterprop filterprop_value
```

(注) IPv4 または IPv6 アドレスを使用してフィルタリングできますが、同じパケット キャプチャ セッションでの両方によるフィルタリングはできません。

表 1: サポートされるフィルタ プロパティ

ivlan	内部 VLAN ID (ポート入力時のパケットの VLAN)
ovlan	外部 VLAN ID (Firepower 4100/9300 シャーシによって追加された VLAN)
srcip	送信元 IP アドレス (IPv4)
destip	宛先 IP アドレス (IPv4)
srcipv6	送信元 IP アドレス (IPv6)
destipv6	宛先 IP アドレス (IPv6)
srcport	送信元ポート番号
destport	宛先ポート番号
プロトコル	IP プロトコル (IANA によって定義される 10 進形式のプロトコル値)

ethertype	イーサネットプロトコルタイプ (IANA によって定義される 10 進形式のイーサネットプロトコルタイプ値。たとえば、IPv4=2048、IPv6=34525、ARP=2054、SGT=35081)
srcmac	送信元 MAC アドレス
destmac	宛先 MAC アドレス

例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create filter interfacelvlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcip 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcport 80
Firepower-chassis packet-capture/filter* # set destip 10.10.10.10
Firepower-chassis packet-capture/filter* # set destport 5050
Firepower-chassis packet-capture/filter* # commit-buffer
```

パケットキャプチャセッションの開始および停止

手順

ステップ 1 パケットキャプチャモードを開始します。

```
Firepower-chassis # scope packet-capture
```

ステップ 2 停止または開始するパケットキャプチャセッションの範囲を入力します。

```
Firepower-chassis /packet-capture # enter session session_name
```

ステップ 3 パケットキャプチャセッションを開始するには、次の操作を行います。

```
Firepower-chassis /packet-capture/session* # enable [append | overwrite]
```

(注) 別のセッションの実行中は、パケットキャプチャセッションを開始できません。

パケットキャプチャセッションの実行中は、トラフィックをキャプチャするにつれて個々の PCAP ファイルのファイルサイズが増加します。バッファのサイズ制限に達すると、システムがパケットの廃棄を開始し、廃棄カウントフィールドの値が増加します。

ステップ 4 パケットキャプチャセッションを停止するには、次の操作を行います。

```
Firepower-chassis /packet-capture/session* # disable
```

ステップ 5 トランザクションをシステム設定にコミットします。

```
Firepower-chassis /packet-capture/session* # commit-buffer
```


パケットキャプチャセッションを有効にすると、セッションに含まれるインターフェイスのPCAPファイルがトラフィックの収集を開始します。セッションがセッションデータを上書きするように設定されている場合、既存のPCAPデータは消去されます。そうでない場合、データは（もしあれば）既存のファイルに追加されます。

例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # scope session asalinside
Firepower-chassis packet-capture/session # enable append
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

パケットキャプチャファイルのダウンロード

セッションからローカルコンピュータにパケットキャプチャ（PCAP）ファイルをダウンロードできます。これでネットワークパケットアナライザを使用して分析できるようになります。

PCAP ファイルは `workspace://packet-capture` ディレクトリに保存されており、以下の命名規則を使用します。

```
workspace://packet-capture/session-<id>/<session-name>-<interface-name>.pcap
```

手順

Firepower 4100/9300 シャーシから PCAP ファイルをコピーするには、次の操作を行います。

(注) セッションから PCAP ファイルをダウンロードする前にパケットキャプチャセッションを停止する必要があります。

- a) ローカル管理に接続します。

```
Firepower-chassis # connect localmgmt
```

- b) PCAP ファイルをコピーします。

```
# copy pcap_file copy_destination
```

例

```
Firepower-chassis# connect localmgmt
# copy workspace:/packet-capture/session-1/test-ethernet-1-1-0.pcap
scp://user@10.10.10.1:/workspace/
```

パケットキャプチャセッションの削除

個々のパケットキャプチャセッションは、現在実行していなければ削除できます。非アクティブパケットキャプチャセッションは、いずれも削除できます。

手順

ステップ1 パケットキャプチャモードを開始します。

```
Firepower-chassis # scope packet-capture
```

ステップ2 特定のパケットキャプチャセッションを削除するには、次の手順を実行します。

```
Firepower-chassis /packet-capture # delete session session_name
```

ステップ3 すべての非アクティブパケットキャプチャセッションを削除するには、次のようにします。

```
Firepower-chassis /packet-capture # delete-all-sessions
```

ステップ4 トランザクションをシステム設定にコミットします。

```
Firepower-chassis /packet-capture* # commit-buffer
```

例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # delete session asalinside
Firepower-chassis packet-capture* # commit-buffer
Firepower-chassis packet-capture #
```

ネットワーク接続のテスト

始める前に

基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名またはIPv4アドレスを使ってpingを実行するには、**ping** コマンドを使用します。ネットワーク上の別のデバイスのホスト名またはIPv6アドレスを使ってpingを実行するには、**ping6** コマンドを使用します。

ネットワーク上の別のデバイスに至るルートを、そのホスト名またはIPv4アドレスを使ってトレースするには、**tracert** コマンドを使用します。ネットワーク上の別のデバイスに至るルートを、そのホスト名またはIPv6アドレスを使ってトレースするには、**tracert6** コマンドを使用します。

- **ping** コマンドおよび **ping6** コマンドは、`local-mgmt` モードで使用可能です。
- **ping** コマンドは `module` モードでも使用できます。

- **traceroute** コマンドおよび **traceroute6** コマンドは、local-mgmt モードで使用可能です。
- **traceroute** コマンドは module モードでも使用できます。

手順

ステップ 1 次のコマンドのいずれか 1 つを入力することにより、local-mgmt モードまたは module モードに接続します。

- **connect local-mgmt**
- **connect module *module-ID* {console | telnet}**

例：

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

ステップ 2 基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名または IPv4 アドレスを使って ping を実行します。

ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

例：

この例は、ネットワーク上の別のデバイスに対して ping 接続を 12 回実行する方法を示しています。

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

ステップ 3 ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv4 アドレスを使ってトレースします。

traceroute {*hostname* | *IPv4_address*}

例：

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

FP9300-A(local-mgmt)#
```

ステップ4 (任意) local-mgmt モードを終了して最上位モードに戻るには、**exit** を入力します。

管理インターフェイスのステータスのトラブルシューティング

初期化時や設定時に、何らかの理由（Chassis Manager にアクセスできないなど）で管理インターフェイスが起動しないと思われる場合は、local-mgmt シェルで **show mgmt-port** コマンドを使用して、管理インターフェイスのステータスを確認します。



(注) fxos シェルで **show interface brief** コマンドを使用しないでください。現在、このコマンドでは、誤った情報が表示されます。

手順

ステップ1 次のコマンドを入力することにより、local-mgmt モードに接続します。

• **connect local-mgmt**

例：

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

ステップ2 **show mgmt-port** コマンドを使用して管理インターフェイスのステータスを確認します。

例：

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

RX bytes:1648941394 (1.5 GiB) TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#

show mgmt-ip-debug コマンドを使用することもできますが、インターフェイス設定情報の広範なリストが生成されます。

ポート チャネル ステータスの確認

現在定義されているポート チャネルのステータスを判別するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して /eth-uplink/fabric モードを開始します。

- **scope eth-uplink**
- **scope fabric {a | b}**

例：

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

ステップ 2 現在のポート チャネルとそれぞれの管理状態および動作状態のリストを表示するには、**show port-channel** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric # show port-channel
```

```
Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State      State Reason
  -----
  10
ed Failed          Port-channel10 Data          Enabl
          No operational members
  11
ed Failed          Port-channel11 Data          Enabl
          No operational members
  12
led Admin Down    Port-channel12 Data          Disab
          Administratively down
  48
ed Up              Port-channel48 Cluster        Enabl

FP9300-A /eth-uplink/fabric #
```

ステップ 3 個々のポート チャネルとポートに関する情報を表示するには、次のコマンドを入力して /port-channel モードを開始します。

• **scope port-channel ID**

例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, 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 lines removed for brevity --->

```
FP9300-A (fxos)#
```

ステップ4 指定したポートチャネルのステータス情報を表示するには、**show** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State             State Reason
  -----
  10                        Port-channel10 Data          Enabl
ed      Failed                    No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

ステップ5 ポートチャネルのメンバポートのステータス情報を表示するには、**show member-port** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
  Port Name          Membership      Oper State      State Reas
on
  -----
  Ethernet2/3        Suspended      Failed          Suspended
  Ethernet2/4        Suspended      Failed          Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

ポートチャネルは、論理デバイスに割り当てられるまでは表示されないことに注意してください。ポートチャネルが論理デバイスから削除された場合や論理デバイスが削除された場合は、ポートチャネルが一時停止状態に戻ります。

ステップ6 追加のポートチャネルおよびLACP情報を表示するには、次のコマンドを入力することにより、/eth-uplink/fabric/port-channel モードを終了して fxos モードに入ります。

• **top**

• connect fxos

例：

ステップ7 現在のポート チャンネルのサマリー情報を表示するには、**show port-channel summary** コマンドを入力します。

例：

```

FP9300-A(fxos)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
10   Po10 (SD)        Eth       LACP      Eth2/3(s)  Eth2/4(s)
11   Po11 (SD)        Eth       LACP      Eth2/1(s)  Eth2/2(s)
12   Po12 (SD)        Eth       LACP      Eth1/4(D)  Eth1/5(D)
48   Po48 (SU)        Eth       LACP      Eth1/1(P)  Eth1/2(P)

```

fxos モードでは、さらに **show port-channel** コマンドおよび **show lacp** コマンドも使用できます。これらのコマンドを使用すると、容量、トラフィック、カウンタ、使用状況など、さまざまなポート チャンネルおよび LACP 情報を表示することができます。

次のタスク

ポートチャンネルの作成方法については、[EtherChannel \(ポートチャンネル\) の追加](#)を参照してください。

ソフトウェア障害からの回復

始める前に

システムが正常にブートできないソフトウェア障害が発生した場合は、以下の手順を実行して、ソフトウェアの新規バージョンをブートできます。このプロセスを実行するには、キックスタートイメージをTFTPブートし、新規システムとマネージャイメージをダウンロードし、新規イメージを使用してブートする必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300 : <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 シリーズ <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

リカバリ イメージには、3つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64の現在のリカバリ イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

手順

ステップ1 ROMMON にアクセスします。

- a) コンソール ポートに接続します。
- b) システムをリブートします。

システムはロードを開始し、そのプロセス中にカウントダウン タイマーを表示します。

- c) カウントダウン中に **Esc** キーを押すと、ROMMON モードに入ります。

例 :

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

ステップ2 キックスタート イメージを TFTP ブートします。

- a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) キックスタートイメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

(注) キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタートイメージとの間の対応を示す情報は、Cisco.com のソフトウェアダウンロードページにあります。

- c) ブートコマンドを使用して、ROMMON からイメージをブートします。

```
boot tftp://<IP address>/<path to image>
```

(注) さらに、Firepower 4100/9300 シャーシのフロントパネルにある USB スロットに挿入した FAT32 フォーマットの USB メディアデバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例：

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
```

```

NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.

```

ステップ3 Firepower4100/9300 シャーシに直前にロードしたキックスタートイメージと一致するリカバリシステムとマネージャ イメージをダウンロードします。

- a) リカバリ システムとマネージャ イメージをダウンロードするには、管理IPアドレスとゲートウェイを設定する必要があります。これらのイメージは、USBを使用してダウンロードすることはできません。

```

switch(boot) # config terminal
switch(boot) (config) # interface mgmt 0
switch(boot) (config-if) # ip address <ip address> <netmask>
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway <gateway>
switch(boot) (config) # exit

```

- b) リカバリ システムとマネージャ イメージを、リモートサーバからブートフラッシュにコピーします。

switch(boot)# **copy URL bootflash:**

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname/path/image_name**

例 :

```

switch(boot) # copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:

```

```

switch(boot) # copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:

```

- c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、nuova-sim-mgmt-nsg.0.1.0.001.bin からマネージャ イメージへの symlink を作成します。この

リンクは、ロードするマネージャ イメージをロードメカニズムに指示します。symlink 名は、ロードしようとしているイメージに関係なく、常に `nuova-sim-mgmt-nsg.0.1.0.001.bin` とする必要があります。

```
switch(boot)# copy bootflash:<manager-image>  
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例：

```
switch(boot)# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
  
switch(boot) (config)# interface mgmt 0  
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0  
switch(boot) (config-if)# no shutdown  
switch(boot) (config-if)# exit  
switch(boot) (config)# ip default-gateway 10.0.0.1  
switch(boot) (config)# exit  
switch(boot)# copy  
tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA  
bootflash:  
Trying to connect to tftp server.....  
Connection to server Established. Copying Started.....  
/  
TFTP get operation was successful  
Copy complete, now saving to disk (please wait)..  
  
switch(boot)# copy  
tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA  
bootflash:  
Trying to connect to tftp server.....  
Connection to server Established. Copying Started.....  
/  
TFTP get operation was successful  
Copy complete, now saving to disk (please wait)..  
  
switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA  
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin  
  
Copy complete, now saving to disk (please wait)..  
  
switch(boot)#
```

ステップ 4 直前にダウンロードしたシステム イメージをロードします。

```
switch(boot)# load bootflash:<system-image>
```

例：

```
switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA  
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA  
  
Manager image digital signature verification successful  
...  
System is coming up ... Please wait ...  
  
Cisco FPR Series Security Appliance
```

FP9300-A login:

ステップ5 リカバリ イメージがロードされたら、以下のコマンドを入力して、システムが旧イメージをロードしないようにします。

(注) この手順は、リカバリ イメージのロードの直後に実行する必要があります。

```
FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility
issue.
FP9300-A /org/fw-platform-pack* # commit-buffer
```

ステップ6 Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードしてインストールします。詳細については、[イメージ管理](#)を参照してください。

例 :

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
    Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

破損ファイルシステムの回復

始める前に

スーパーバイザのオンボードフラッシュが破損し、システムが正常に開始できなくなった場合は、次の手順を使用してシステムを回復できます。このプロセスを実行するには、キックスタートイメージをTFTPブートし、フラッシュを再フォーマットし、新規システムとマネージャイメージをダウンロードし、新規イメージを使用してブートする必要があります。



(注) この手順には、システムフラッシュの再フォーマットが含まれています。その結果、回復後にはシステムを完全に再設定する必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300 : <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 シリーズ <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

リカバリ イメージには、3つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64 の回復イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

手順

ステップ 1 ROMMON にアクセスします。

- a) コンソールポートに接続します。
- b) システムをリブートします。

システムはロードを開始し、そのプロセス中にカウントダウン タイマーを表示します。

- c) カウントダウン中に **Esc** キーを押すと、ROMMON モードに入ります。

例 :

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

ステップ 2 キックスタート イメージを TFTP ブートします。

- a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) キックスタートイメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

(注) キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタートイメージとの間の対応を示す情報は、Cisco.com のソフトウェアダウンロードページにあります。

- c) ブートコマンドを使用して、ROMMON からイメージをブートします。

```
boot tftp://<IP address>/<path to image>
```

(注) さらに、Firepower 4100/9300 シャーシのフロントパネルにある USB スロットに挿入した USB メディア デバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例：

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
```

```

SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.

```

ステップ3 キックスタートイメージをロードしたら、**init system** コマンドを使用してフラッシュを再フォーマットします。

init system コマンドを実行すると、システムにダウンロードされているすべてのソフトウェアイメージやシステムのすべての設定を含め、フラッシュの内容は消去されます。コマンドが完了するまで約 20 ～ 30 分かかります。

例：

```

switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.

Do you want to continue? (y/n) [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done

```

ステップ4 リカバリ イメージを Firepower 4100/9300 シャーシへダウンロードします。

- a) リカバリ イメージをダウンロードするには、管理 IP アドレスとゲートウェイを設定する必要があります。これらのイメージは、USB を使用してダウンロードすることはできません。

```
switch(boot) # config terminal
switch(boot) (config) # interface mgmt 0
switch(boot) (config-if) # ip address <ip address> <netmask>
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway <gateway>
switch(boot) (config) # exit
```

- b) リモートサーバからブートフラッシュに3つすべてのリカバリイメージをコピーします。

```
switch(boot)# copy URL bootflash:
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname/path/image_name**

例 :

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
```

bootflash:

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
```

bootflash:

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
```

bootflash:

- c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、`nuova-sim-mgmt-nsg.0.1.0.001.bin` からマネージャイメージへの symlink を作成します。このリンクは、ロードするマネージャイメージをロードメカニズムに指示します。symlink 名は、ロードしようとしているイメージに関係なく、常に `nuova-sim-mgmt-nsg.0.1.0.001.bin` とする必要があります。

```
switch(boot) # copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例 :

```
switch(boot) # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(boot) (config) # interface mgmt 0
switch(boot) (config-if) # ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway 10.0.0.1
switch(boot) (config) # exit
switch(boot) # copy
```



```

tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#

```

ステップ5 スイッチをリロードします。

```
switch(boot)# reload
```

例：

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.
```

```
!! Rommon image verified successfully !!
```

```

Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb
```

```
autoboot: Can not find autoboot file 'menu.lst.local'
Or can not find correct boot string !!
```

```
rommon 1 >
```

ステップ 6 キックスタート イメージおよびシステム イメージからブートします。

```
rommon 1 > boot <kickstart-image> <system-image>
```

(注) システム イメージのロード中に、ライセンス マネージャのエラー メッセージが表示されることがあります。このようなメッセージは無視して構いません。

例：

```
rommon 1 > dir
Directory of: bootflash:\
```

```
01/01/12 12:33a <DIR>          4,096 .
01/01/12 12:33a <DIR>          4,096 ..
01/01/12 12:16a <DIR>         16,384 lost+found
01/01/12 12:27a              34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a              330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a              250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a              330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
    4 File(s) 946,269,798 bytes
    3 Dir(s)
```

```
rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
```

```
!! Kickstart Image verified successfully !!
```

```
Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
```

```
INIT: version 2.86 booting
```

```
POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA
```

```
Manager image digital signature verification successful
```

```
...
```

```
System is coming up ... Please wait ...
nohup: appending output to `nohup.out'
```

```
---- Basic System Configuration Dialog ----
```

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system. To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

You have chosen to setup a new Security Appliance. Continue? (y/n):

ステップ7 イメージのロードが完了すると、システムにより初期構成設定を入力するように求められます。詳細については、[コンソールポートを使用した初期設定](#)を参照してください。

ステップ8 Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードします。詳細については、[イメージ管理](#)を参照してください。

例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
  Tftp      192.168.1.2          0
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

ステップ9 以前の手順でダウンロードしたプラットフォーム バンドル イメージをインストールします。
(注) インストールプロセスには通常 15 ～ 20 分かかります。

a) auto-install モードにします。

```
Firepower-chassis /firmware # scope auto-install
```

b) FXOS プラットフォーム バンドルをインストールします。

```
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
```

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です (たとえば、2.1(1.73))。

c) システムは、まずインストールするソフトウェアパッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェアパッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

- d) インストールの続行を確定するには**yes**を、インストールをキャンセルするには**no**を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

- e) アップグレードプロセスをモニタするには、次の手順を実行します。

- **scope firmware** を入力します。
- **scope auto-install** を入力します。
- **show fsm status expand** を入力します。

例：

```
TB10 /firmware/auto-install # show fsm status expand
FSM Status:
Affected Object: sys/fw-system/fsm
Current FSM: Deploy
Status: In Progress
Completion Time:
Progress (%): 98

FSM Stage:
Order  Stage Name                Status      Try
-----
1      DeployWaitForDeploy          Success     0
2      DeployResolveDistributableNames  Skip        0
3      DeployResolveDistributable      Skip        0
4      DeployResolveImages            Skip        0
5      DeployValidatePlatformPack      Success     1
6      DeployDebundlePort             Success     0
7      DeployPollDebundlePort          Success     1
8      DeployActivateUCSM              Success     0
9      DeployPollActivateOfUCSM        Success     0
10     DeployActivateMgmtExt           Skip        0
11     DeployPollActivateOfMgmtExt      Skip        0
12     DeployUpdateIOM                 Skip        0
13     DeployPollUpdateOfIOM           Skip        0
14     DeployActivateIOM               Skip        0
15     DeployPollActivateOfIOM         Skip        0
16     DeployActivateRemoteFI          Skip        0
17     DeployPollActivateOfRemoteFI    Skip        0
18     DeployWaitForUserAck            Skip        0
19     DeployActivateLocalFI           Success     0
20     DeployPollActivateOfLocalFI     In Progress 1
```

(注) ステージのステータスが「進行中」から「スキップ」または「成功」に変わるまで、次のステップに進まないでください。

ステップ 10 インストールしたプラットフォーム バンドル イメージがシステムの回復に使用するイメージに対応している場合は、将来的にシステムのロード時で使用できるようにキックスタートイメージおよびシステムイメージを手動で有効にする必要があります。回復イメージとして同じイメージを使用しているプラットフォーム バンドルをインストールする場合、自動アクティベーションは発生しません。

- a) **fabric-interconnect a** のスコープを設定します。

```
FP9300-A# scope fabric-interconnect a
```

- b) 実行中のカーネルバージョンと実行中のシステムバージョンを表示するには、**show version** コマンドを使用します。イメージをアクティブにするには、次の文字列を使用します。

```
FP9300-A /fabric-interconnect # show version
```

(注) Startup-Kern-Vers および Startup-Sys-Vers がすでに設定され、Running-Kern-Vers および Running-Sys-Vers と一致する場合は、イメージを有効にする必要はなく、手順 11 に進みます。

- c) 次のコマンドを入力して、イメージをアクティブにします。

```
FP9300-A /fabric-interconnect # activate firmware
kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

(注) サーバのステータスは「失敗したディスク (Disk Failed)」に変更される場合があります。このメッセージには注意を払う必要はなく、手順を続行できます。

- d) スタートアップバージョンが正しく設定されていることを確認し、イメージのアクティブ化ステータスをモニタするには、**show version** コマンドを使用します。

重要 ステータスが「アクティブにしています (Activating)」から「実行可能 (Ready)」に変わるまで、次のステップには進まないでください。

```
FP9300-A /fabric-interconnect # show version
```

例 :

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers:
  Startup-Sys-Vers:
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
```

```

Act-Kern-Status: Activating
Act-Sys-Status: Activating
Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

```

ステップ 11 システムを再起動します。

例：

```

FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #

```

システムは Firepower 4100/9300 シャーシの電源を最終的にオフにしてから再起動する前に、各セキュリティ モジュール/エンジンの電源をオフにします。このプロセスには約 5～10 分かかります。

ステップ 12 システムのステータスをモニタします。サーバのステータスは「検出 (Discovery)」から「構成 (Config)」、最終的には「OK」へと変わります。

例：

```

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Discovery In Progress
1/2 Equipped Discovery In Progress
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Config Complete
1/2 Equipped Config Complete
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Ok Complete
1/3 Empty

```

総合的なステータスが「OK」になれば、システムは回復したことになります。引き続き、セキュリティ アプライアンス (ライセンス設定を含む) を再設定し、論理デバイスがあれば再作成する必要があります。詳細については、次を参照してください。

- Firepower 9300 のクイック スタート ガイド [英語] : <http://www.cisco.com/go/firepower9300-quick>
- Firepower 9300 のコンフィギュレーション ガイド [英語] : <http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 シリーズのクイック スタート ガイド [英語] : <http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 シリーズのコンフィギュレーションガイド [英語] : <http://www.cisco.com/go/firepower4100-config>

管理者パスワードが不明な場合における工場出荷時のデフォルト設定の復元

この手順により Firepower4100/9300 シャーシシステムがデフォルト設定に戻ります。管理者パスワードも含まれます。管理者パスワードが不明な場合、次の手順を使用してデバイスの設定をリセットします。この手順では、インストールされている論理デバイスも消去されます。



(注) この手順では、Firepower 4100/9300 シャーシのコンソールにアクセスする必要があります。

手順

ステップ 1 付属のコンソールケーブルを使用して PC をコンソールポートに接続します。ターミナルエミュレータを回線速度 9600 ボー、データビット 8、パリティなし、ストップビット 1、フロー制御なしに設定して、コンソールに接続します。詳細については、『[Cisco Firepower 9300 ハードウェア設置ガイド](#)』を参照してください。

ステップ 2 デバイスの電源を入れます。次のようなプロンプトが表示されたら、ESC キーを押してブートを中断します。

例 :

```
!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
```

```
MAC Address: 00:00:00:00:00:00

find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
rommon 1 >
```

ステップ3 キックスタートイメージとシステムイメージの名前をメモします。

例：

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

ステップ4 キックスタートイメージをロードします。

[rommon 1] > [kickstart_image]boot

例：

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab-302: No such file or directory (use -n flag to
override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, 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. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

ステップ5 config ターミナルモードを開始します。

switch(boot) # **config terminal**

例：

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ6 パスワードを再設定し、変更を確認します。

switch(boot) (config) # **admin-password erase**

(注) この手順を実行すると、すべての設定が消去され、システムがデフォルト設定に戻ります。

例：


```
switch boot (config) # admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n) [n] y
```

ステップ 7 config ターミナルモードを開始します。

```
switch boot (config) # exit
```

ステップ 8 この手順のステップ 3 でメモしたシステムイメージをロードし、[初期設定](#) タスクフローを使用してシステムを最初から設定します。

```
switch boot # load system_image
```

例：

```
switch boot # load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

```
Uncompressing system image:
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

トラブルシューティング ログ ファイルの生成

必要に応じて、トラブルシューティングに利用するため、または Cisco TAC へ送信するためのログ ファイルを生成できます。

手順

ステップ 1 ローカル管理モードに接続します。

```
Firepower# connect local-mgmt
```

ステップ 2 (省略可能) 次のコマンドを入力します：

```
Firepower(local-mgmt)# show tech-support ?
```

コマンド出力には、トラブルシューティング ファイルを生成できるコンポーネントが表示されます。

例：

```
chassis  Chassis
fprm     Firepower Platform Management
module   Security Module
```

ステップ 3 トラブルシューティング ファイルを生成するには、次のコマンドを実行します：

```
Firepower(local-mgmt)# show tech-support <component keyword>
```

トラブルシューティング ファイルを生成するコンポーネントに必須のキーワードが指定されていることを確認してください。たとえば、**module** キーワードを指定すると、セキュリティモジュールのトラブルシューティング ファイルが生成されます。

トラブルシューティングファイルを生成するコンポーネントに必須のキーワードが指定されていることを確認してください。たとえば、**fprm** キーワードを指定するとプラットフォーム管理用のトラブルシューティング ファイルが生成されます。

表 2: コマンドの例とコンポーネント

コンポーネント	コマンドの例
シャーシ	Firepower (local-mgmt)# show tech-support chassis 1
Firepower プラットフォーム管理	この fprm オプションは、バージョン 2.8(1) で廃止され、使用できなくなりました。
セキュリティモジュール	Firepower (local-mgmt)# show tech-support module 1

例 :

```
Firepower(local-mgmt)# show tech-support chassis 1 detail

The show tech support file will be located at
/workspace/techsupport/20191105041703_firepower-9300_BC1_all.tar

Initiating tech-support information task on FABRIC A ...

Initiating tech-support information task on Chassis 1 Fabric Extender 1 ...
Initiating tech-support information task on Chassis 1 CIMC 1 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/1 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/1 ...
Initiating tech-support information task on Chassis 1 CIMC 2 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/2 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/2 ...
Completed initiating tech-support subsystem tasks (Total: 8)
Waiting (Timeout: 900 Elapsed: 30) for completion of subsystem tasks (1/8).
Waiting (Timeout: 900 Elapsed: 50) for completion of subsystem tasks (2/8).
Waiting (Timeout: 900 Elapsed: 70) for completion of subsystem tasks (5/8).
Waiting (Timeout: 900 Elapsed: 90) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 110) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 130) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 150) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 170) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 190) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 210) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 230) for completion of subsystem tasks (7/8).
--More--
The detailed tech-support information is located at workspace:///techsupport/201--More--
91105041703_firepower-9300_BC1_all.tar
```

同様に、セキュリティモジュールからトラブルシューティングファイルを生成することもできます。

トラブルシューティングファイルが生成されると、そのファイルはワークスペース内で表示できます。

ステップ 4 次のコマンドを実行して、ファイルが生成されているかどうかを確認します。

```
dir workspace:/techsupport
```

例 :

```
1 34426880 Mar 05 13:10:05 2019 20190305130133_firepower-9300_FPRM.tar
1 56995840 Aug 27 05:30:37 2019 20190827052331_firepower-9300_FPRM.tar
1 56842240 Aug 27 12:42:42 2019 20190827123535_firepower-9300_FPRM.tar
1 87623680 Sep 17 06:27:57 2019 20190917062046_firepower-9300_FPRM.tar
1 87756800 Sep 17 10:22:38 2019 20190917101527_firepower-9300_FPRM.tar
1 152627200 Nov 05 04:30:10 2019 20191105041703_firepower-9300_BC1_all.tar
```

```
Usage for workspace://
3999125504 bytes total
476835840 bytes used
3317436416 bytes free
```

(注) 3つすべてのパラメータ (fprm、chassis、module) を使用してファイルを適切に生成した場合は、**/techsupport** ディレクトリ内に表示されます。

ステップ 5 次のコマンドを実行します。

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> ?

出力には、FXOSからローカルコンピュータへのトラブルシューティングファイルのコピーを可能にする、サポートされているプロトコルが示されています。サポートされているプロトコルのいずれかを使用できます。

例 :

```
Firepower(local-mgmt)# copy workspace:/techsupport/
20191105041703_firepower-9300_BC1_all.tar ?
ftp:          Dest File URI
http:         Dest File URI
https:        Dest File URI
scp:          Dest File URI
sftp:         Dest File URI
tftp:         Dest File URI
usbdrive:     Dest File URI
volatile:     Dest File URI
workspace:    Dest File URI
```

FXOS からコンピュータにファイルをコピーする前に、次の前提条件が満たされていることを確認してください :

- ローカルコンピュータ上のファイアウォールは、必要なポートを介して着信接続を受け入れます。たとえば、セキュアシェルを介してファイルをコピーする場合、コンピュータは、ポート 22 などの関連ポートからの接続を許可する必要があります。
- ファイルのコピーを許可するには、コンピュータがセキュアコピー (SCP) サービスまたはサポートされているプロトコルのいずれかを実行している必要があります。インターネット上では、さまざまな SSH または SCP サーバソフトウェアを見つけることができます。ただし、シスコでは、特定の SCP サーバのインストールと設定のサポートは提供していません。

ステップ 6 ファイルをコピーするには、次のコマンドを実行します。

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> <supported file transfer protocol>://<username>@<destination IP address>

例 :

```
firepower-9300(local-mgmt)# copy workspace:/techsupport/  
20191105041703_firepower-9300_BC1_all.tar scp:/xyz@192.0.2.1
```

モジュールのコアダンプの有効化

モジュールでコアダンプを有効にすると、システムクラッシュが発生した場合のトラブルシューティングに役立つ可能性があり、必要に応じて Cisco TAC に送信できます。

手順

ステップ 1 目的のモジュールに接続します。次に例を示します。

```
Firepower# connect module 1 console
```

ステップ 2 (任意) 次のコマンドを入力して、現在のコアダンプステータスを表示します。

```
Firepower-module1> show coredump detail
```

このコマンドの出力には、コアダンプ圧縮が有効かどうかといった、現在のコアダンプステータス情報が表示されます。

例：

```
Firepower-module1>show coredump detail  
Configured status: ENABLED.  
ASA Coredump: ENABLED.  
Bootup status: ENABLED.  
Compress during crash: DISABLED.
```

(注) このコマンドは、アプライアンスで ASA 論理デバイスを実行している場合にのみ使用でき、アプライアンスで Firepower Threat Defense 論理デバイスを実行している場合には使用できません。

ステップ 3 `config coredump` コマンドを使用して、コアダンプを有効または無効にし、クラッシュ時のコアダンプ圧縮を有効または無効にします。

- クラッシュ時のコアダンプの作成を有効にするには、`config coredump enable` を使用します。
- クラッシュ時のコアダンプの作成を無効にするには、`config coredump disable` を使用します。
- コアダンプの圧縮を有効にするには、`config coredump compress enable` を使用します。
- コアダンプの圧縮を無効にするには、`config coredump compress disable` を使用します。

例：

```
Firepower-module1>config coredump enable  
Coredump enabled successfully.  
ASA coredump enabled, do 'config coredump disableAsa' to disable
```

```
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure. Are you sure? (y/n):
y
Firepower-module1>
```

(注) コアダンプファイルはディスク容量を消費します。容量が少なくなり、圧縮が有効になっていない場合は、コアダンプが有効になっていても、コアダンプファイルが保存されないことがあります。

シリアル番号の確認 Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシとそのシリアル番号の詳細を確認できます。Firepower 4100/9300 シャーシのシリアル番号は、論理デバイスのシリアル番号とは異なるので注意してください。

手順

ステップ1 シャーシの範囲を入力します。

scope chassis

例：

```
Firepower# scope chassis
Firepower /chassis #
```

ステップ2 インベントリ詳細の表示：

show inventory

例：

```
Firepower /chassis # show inventory
```

出力には、シリアル番号とその他の詳細が表示されます。

Chassis	PID	Vendor	Serial (SN)	HW Revision
1	FPR-C9300-AC	Cisco Systems Inc	JMX1950196H	0

RAID 仮想ドライブの再構築

RAID（独立ディスクの冗長アレイ）とは、優れたパフォーマンスとフォールトトレランス機能を提供する複数の独立した物理ドライブのアレイ（グループ）です。ドライブグループは、物理ドライブのグループです。これらのドライブは、仮想ドライブと呼ばれるパーティションで管理されます。

RAID ドライブ グループでは、単一ドライブのストレージシステムに比べてデータ ストレージの信頼性と耐障害性が高まります。ドライブの障害によるデータの損失は、失われたデータを残りのドライブから再構築することで防ぐことができます。RAID は、I/O パフォーマンスを向上させるとともに、ストレージサブシステムの信頼性を向上させます。

RAID ドライブのいずれかが故障するかオフラインになると、RAID 仮想ドライブは劣化状態と見なされます。以下の手順を使用して、RAID 仮想ドライブが劣化状態かどうかを確認し、必要に応じて、ローカルディスク設定保護ポリシーを一時的に **no** に設定して再構築してください。



(注) ローカルディスク設定保護ポリシーを **no** に設定すると、ディスク上のすべてのデータが破棄されます。

手順

ステップ 1 RAID ドライブのステータスを確認します。

1. シャーシ モードに入ります。
scope chassis
2. サーバモードに入ります。
scope server 1
3. RAID コントローラに入ります。
scope raid-controller 1 sas
4. 仮想ドライブを表示します。

show virtual-drive

RAID 仮想ドライブが劣化状態である場合は、動作状態が **Degraded** と表示されます。次に例を示します。

```
Virtual Drive:
  ID: 0
  Block Size: 512
  Blocks: 3123046400
  Size (MB): 1524925
  Operability: Degraded
  Presence: Equipped
```

ステップ 2 RAID ドライブを再構築するために、ローカルディスク設定ポリシー保護を **no** に設定します。この手順を完了するとディスク上のすべてのデータが破棄されることに注意してください。

1. 組織の範囲を入力します。
scope org
2. ローカルディスク設定ポリシーの範囲を入力します。

scope local-disk-config-policy ssp-default

3. 保護を no に設定します。

set protect no

4. 設定をコミットします。

commit-buffer

ステップ 3 RAID ドライブが再構築されるまで待ちます。RAID 再構築ステータスを確認します。

scope chassis 1

show server

RAID ドライブが正常に再構築されると、スロットの全体的なステータスが **Ok** と表示されま
す。次に例を示します。

例：

Server:

Slot	Overall Status	Service Profile
1	Ok	ssp-sprof-1

ステップ 4 RAID ドライブが正常に再構築されたら、ローカルディスク設定ポリシー保護を yes に戻しま
す。

1. 組織の範囲を入力します。

scope org

2. ローカルディスク設定ポリシーの範囲を入力します。

scope local-disk-config-policy ssp-default

3. 保護を no に設定します。

set protect yes

4. 設定をコミットします。

commit-buffer

SSD を使用している場合の問題の特定

デバイスに搭載されている SSD に関して、情報を収集し、考えられる問題を特定するには、
以下の手順を使用します。SSD の問題の症状の例として、データ管理エンジン (DME) プロセ
スの起動に失敗することがあります。



- (注) 新しい SSD を挿入すると、ブレード BIOS 検出後にインベントリに基本情報（タイプ、モデル、SN など）のみが入力されます。ローカルディスクデータは、SSP-OS アップグレードの完了時にのみ、インベントリに入力されます。SSP-OS のアップグレードの状態がまだ「更新中」の場合、インベントリにはローカルディスクのエントリが表示されず、SSD の接続に関する障害メッセージも表示されません。

以下の手順に示されているログファイルの出力が SSD に関する問題を示している場合は、TAC にお問い合わせください (<https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html> を参照)。

手順

ステップ 1 FXOS コマンドシェルに接続します。

```
connect fxos
```

ステップ 2 nvram ログファイルを表示します。

```
show logging nvram
```

エラー出力の例：

```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
block - inode=14, block=6
```

ステップ 3 ログファイルを表示します。

```
show logging logfile
```

エラー出力の例：

```
2020 Oct 21 21:11:25 (none) kernel: [28118744.718445] EXT3-fs error (device sda4):
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```


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。