トラブルシューティング

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。
- 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 **[ツール（Tools）]** > **[パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 次のいずれかを実行します。

- パケット キャプチャ セッションを作成するには、[キャプチャ セッション（Capture Session）] ボタンをクリックします。
- 既存のパケット キャプチャ セッションを編集するには、そのセッションの [Edit] ボタンをクリックします。

ウィンドウの左側では、特定のアプリケーション インスタンスを選択し、そのインスタンスの表記を表示します。この表示は、パケットをキャプチャするインターフェイスを選択するために使用されます。ウィンドウの右側にパケット キャプチャ セッションを定義するためのフィールドが含まれています。

ステップ 3 ドロップダウン メニューから**インターフェイスを選択します**。

ステップ 4 トラフィックをキャプチャするインターフェイスをクリックします。選択したインターフェイスにチェック マークを表示します。

ステップ 5 サブインターフェイスの場合、[Subinterface selection] 列でサブインターフェイスを表示する親インターフェイスの左にあるアイコンをクリックします。列内のサブインターフェイスをクリックします。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。

複数のサブインターフェイスの場合、アイコンのラベルは **Subinterfaces(n)** になり、単一のサブインターフェイスの場合、ラベルはサブインターフェイス ID になります。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。親が割り当てられていない場合は、グレー表示されます。Etherchannel のサブインターフェイスはサポートされていません。

ステップ 6 論理デバイスからバックプレーン ポート上で送信されるトラフィックをキャプチャするには、次の操作を行います。

a) アプリケーション インスタンスを示すボックスをクリックします。

[Capture On]、[Application Port]、および [Application Capture Direction] フィールドは、[Configure Packet Capture Session] ウィンドウの右側で利用可能になります。

b) トラフィックをキャプチャするバックプレーン ポートを選択するか、[Capture On] ドロップダウン リストから [All Backplane Ports] を選択します。

ステップ 7 [Session Name] フィールドにパケット キャプチャ セッションの名前を入力します。

ステップ 8 [Buffer Size] リストからあらかじめ定義された値の 1 つを選択するか、[Custom in MB] を選択してから目的のバッファ サイズを入力して、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。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 9 [Snap Length] フィールドに、キャプチャするパケットの長さを指定します。有効値は 64 ～ 9006 バイトです。デフォルトのスナップ長は 1518 バイトです。

ステップ 10 このパケット キャプチャ セッションを実行したときに、既存の PCAP ファイルを上書きするか、または PCAP ファイルにデータを追加するかを指定します。

ステップ 11 アプリケーション インスタンスと特定のインターフェイス間のトラフィックをキャプチャするには、次の操作を行います。

a) 論理デバイスを表すボックスをクリックします。

b) [Capture On] ドロップダウン リストから、アプリケーション タイプ（[asa] など）を選択します。

c) 受信または送信トラフィックをキャプチャする [Application Port] を選択します。

d) 論理デバイスから指定したインターフェイスに向かうトラフィックのみキャプチャするには、[Application Capture Direction] の横にある [Egress Packets] オプションをクリックします。

（注） [Egress Packets] を選択すると、トラフィックは選択したバックプレーンポートでのみキャプチャされます。選択した場合でも、物理ポートではトラフィックはキャプチャされません。

e) 指定したインターフェイスで送信または受信するトラフィックをキャプチャするには、[Application Capture Direction] の横にある [All Packets] オプションをクリックします。

ステップ 12 キャプチャしたトラフィックをフィルタリングするには、次の手順を実行します。

a) [キャプチャ フィルタ（Capture Filter）] フィールドの [フィルタの適用（Apply Filters）] オプションをクリックします。

フィルタを設定するための一連のフィールドが示されます。

b) フィルタを作成する必要がある場合、[フィルタの作成（Create Filter）] をクリックします。

[パケット フィルタの作成（Create Packet Filter）] ダイアログボックスが表示されます。詳細については、パケット キャプチャのためのフィルタの設定 （5 ページ）を参照してください。

c) [適用（Apply）] ドロップダウン リストから、使用するフィルタを選択します。

d) [適用先（To）] ドロップダウン リストから、フィルタを適用するインターフェイスを選択します。

e) 追加のフィルタを適用するには、[別のフィルタの適用（Apply Another Filter）] をクリックしてから上記の追加のフィルタを適用するステップを繰り返します。

ステップ 13 次のいずれかを実行します。

- このパケット キャプチャ セッションを保存してすぐ実行するには、[保存して実行（Save and Run）] ボタンをクリックします。このオプションは、他のパケット キャプチャ セッションが現在実行されていない場合のみ使用できます。

- このパケットキャプチャセッションを後で実行できるように保存するには、[保存（Save）] ボタンをクリックします。

[キャプチャ セッション（Capture Session）] タブに作成された他のセッションとともにセッションが一覧表示されます。[保存して実行（Save and Run）] を選択した場合、パケット キャプチャ セッションは、パケットをキャプチャします。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。

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 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 次のいずれかを実行します。

- フィルタを作成するには、[フィルタの追加（Add Filter）] ボタンをクリックします。
- 既存のフィルタを編集するには、そのフィルタの [編集（Edit）] ボタンをクリックします。

[パケットフィルタの作成または編集（Create or Edit Packet Filter）] ダイアログボックスが表示されます。

ステップ 3 [フィルタ名（Filter Name）] フィールドにパケット キャプチャ フィルタの名前を入力します。

ステップ 4 特定のプロトコルをフィルタリングするには、[プロトコル（Protocol）] リストから選択するか、または [カスタム（Custom）] を選択して目的のプロトコルを入力します。カスタム プロトコルは 10 進形式（0 ～ 255）の IANA によって定義されたプロトコルである必要があります。

ステップ 5 特定の EtherType をフィルタリングするには、[EtherType] リストから選択するか、または [カスタム（Custom）] を選択して目的の EtherType を入力します。カスタム EhterType は 10 進形

式の IANA によって定義された EtherType である必要があります（たとえば、IPv4＝2048、IPv6 = 34525、ARP = 2054、SGT = 35081）。

ステップ 6 内部 VLAN（ポートに入力する時の VLAN ID）または外部 VLAN（Firepower 4100/9300 シャーシによって追加された VLAN ID）に基づいてトラフィックをフィルタリングするには、指定されたフィールドに VLAN ID を入力します。

ステップ 7 特定の送信元または宛先のトラフィックをフィルタリングするには、IP アドレスとポートを入力するか、または特定の送信元または宛先フィールドに MAC アドレスを入力します。

（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。

ステップ 8 [保存（Save）] をクリックしてフィルタを保存します。

[フィルタ リスト（Filter List）] タブに他の作成されたフィルタとともにフィルタがリスト表示されます。

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 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 パケット キャプチャ セッションを開始するには、そのセッションの [セッションの有効化（Enable Session）] ボタンをクリックし、次に確認のために [はい（Yes）] をクリックします。

（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。

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。

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 3 パケット キャプチャ セッションを停止するには、そのセッションの [セッションの無効化（Disable Session）] ボタンをクリックし、次に確認のために [はい（Yes）] をクリックします。

セッションが無効になった後、PCAP ファイルをダウンロードできます（パケット キャプチャ ファイルのダウンロード （7 ページ）を参照）。

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。

手順

ステップ 1 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 パケット キャプチャ セッションから特定のインターフェイスの PCAP ファイルをダウンロードするには、そのインターフェイスに対応する [ダウンロード（Download）] ボタンをクリックします。

（注） パケット キャプチャ セッションの実行中は PCAP ファイルをダウンロードできません。

ブラウザによって、指定した PCAP ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するように求められます。

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 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

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、そのセッションの対応する [削除（Delete）] ボタンをクリックします。

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、パケット キャプチャ セッションのリストの上にある [すべてのセッションの削除（Delete All Sessions）] ボタンをクリックします。

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、**traceroute** 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、**traceroute6** 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              Port-channel10   Data               Enabl
ed     Failed           No operational members
    11              Port-channel11   Data               Enabl
ed     Failed           No operational members
    12              Port-channel12   Data               Disab
led    Admin Down       Administratively down
    48              Port-channel48   Cluster            Enabl
ed     Up

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 チャネルの作成方法については、EtherChannel（ポート チャネル）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) カウントタウン中に **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 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) カウントタウン中に **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
Copright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59:59.99 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
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                 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 #
```

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。

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。

Firepower eXtensible Operating System 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。

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Firepower4100/9300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 Firepower 4100/9300 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。

（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 **[Tools]** > **[Troubleshooting Logs]** を選択します。

ステップ 2 生成するログ ファイルのタイプをドロップダウン リストから選択します。

- [シャーシ（Chassis）]：シャーシハードウェアの問題やスーパーバイザやサービスマネージャを含むソフトウェアの問題のトラブルシューティングに使用するログファイルを生成します。
- [Module <#>]：セキュリティモジュール/エンジンの問題のトラブルシューティングに使用するログ ファイルを生成します。

ステップ 3 [Generate Log] をクリックします。

ステップ 4 [Yes] をクリックして、ログ ファイルを生成することを確認します。

ログ ファイルが生成されます。このプロセスには、時間がかかる場合があります。ログ ファイルの生成中は、黄色のステータス メッセージが表示されます。ログ ファイルの生成をキャンセルするには、ステータス メッセージの [Abort Job] をクリックします。ログファイルが生成されると、ステータスメッセージが緑色に変わり、ジョブが正常に完了したことが示されます。

ステップ 5 生成されたログ ファイルをダウンロードするには、[Download Files] リスト内のログ ファイルに移動して、[Download] をクリックします。ログ ファイルは、techsupportフォルダに保存されます。

（注） 新しく生成されたファイルを [Download files] リストに表示するには、必要に応じて [Refresh] をクリックする必要があります。

ステップ 6 生成されたログ ファイルを削除するには、[Download Files] リスト内のログ ファイルに移動して、[Delete] をクリックします。

Firepower モジュールのコアダンプの有効化

Firepower 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 Firepower 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.
```

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有効にするには、**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 **[概要（Overview）]** > **[インベントリ（Inventory）]** > **[すべて（All）]** を選択します。

この表には、シャーシにインストールされているコンポーネントのリストと、それらのコンポーネントの関連情報が記載されています。

ステップ 2 [シリアル（serial）] 列のシャーシのシリアル番号を探します。

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