Cisco FXOS CLI コンフィギュレーション ガイド 1.1(1)

初版：2015 年 07 月 16 日

最終更新：2015 年 09 月 28 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: オンラインのみ

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

目 次

Firepower 9300 の概要 1

Firepower 9300 セキュリティ アプライアンスについて 1

コマンドライン インターフェイス（CLI）の概要 3

管理対象オブジェクト 3

コマンド モード 4

オブジェクト コマンド 5

コマンドの実行 7

コマンド履歴 7

保留コマンドのコミット、廃棄、および表示 7

CLI に関するオンラインヘルプ 8

CLI セッション制限 8

使用する前に 9

タスク フロー 9

初期設定 10

FXOS CLI へのアクセス 12

ライセンス管理 15

スマート ソフトウェア ライセンスについて 15

Firepower 9300 上のセキュリティ モジュールのスマート ソフトウェア ライセンス 15

Smart Software Manager とアカウント 16

仮想アカウントごとに管理されるライセンスとデバイス 16

デバイス登録とトークン 16

License Authority との定期通信 17

コンプライアンス違反状態 17

Smart Call Home インフラストラクチャ 17

スマート ソフトウェア ライセンスの前提条件 17

スマート ソフトウェア ライセンスのデフォルト 18

スマート ソフトウェア ライセンスの設定 18

（任意）HTTP プロキシの設定 18
Firepower 9300 の License Authority への登録 19
スマート ソフトウェア ライセンスのモニタリング 20
スマート ソフトウェア ライセンスの履歴 21
User Management 23
User Accounts 23
デフォルト ユーザ ロール 25
ローカル認証されたユーザのパスワード プロファイル 26
デフォルト認証サービスの選択 27
リモート ユーザのロール ポリシーの設定 28
ローカル認証されたユーザへのパスワード強度チェックの有効化 29
変更間隔のパスワード変更の最大数の設定 30
パスワードの変更禁止間隔の設定 31
パスワード履歴カウントの設定 31
ローカル ユーザ アカウントの作成 32
ローカル ユーザ アカウントの削除 34
ローカル ユーザ アカウントのアクティブ化または非アクティブ化 34
ローカル認証されたユーザのパスワード履歴のクリア 35
Image Management 37
イメージ管理について 37
Cisco.com からのイメージのダウンロード 38
Firepower eXtensible Operating System ソフトウェア イメージの Firepower アプライアンス へのダウンロード 38
Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード 39
論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード 40
論理デバイスのイメージ バージョンの更新 42
Platform Settings 45
管理 IP アドレスの変更 45
日時の設定 47
タイム ゾーンの設定 47
NTP サーバの追加 49
NTP サーバの削除 49

手動での日付と時刻の設定 50
SSH の設定 51
Telnet の設定 51
SNMP の設定 52
SNMP について 52
SNMP 通知 53
SNMP セキュリティ レベルおよび権限 54
SNMP セキュリティ モデルとレベルのサポートされている組み合わせ 54
SNMPv3 セキュリティ機能 55
SNMP サポート 55
SNMP のイネーブル化および SNMP プロパティの設定 56
SNMP トラップの作成 57
SNMP トラップの削除 58
SNMPv3 ユーザの作成 59
SNMPv3 ユーザの削除 60
HTTPS ポートの変更 60
AAA の設定 61
AAA について 61
LDAP プロバイダーの設定 62
LDAP プロバイダーのプロパティの設定 62
LDAP プロバイダーの作成 63
LDAP プロバイダーの削除 66
RADIUS プロバイダーの設定 67
RADIUS プロバイダーのプロパティの設定 67
RADIUS プロバイダーの作成 67
RADIUS プロバイダーの削除 69
TACACS+ プロバイダーの設定 69
TACACS+ プロバイダーのプロパティの設定 69
TACACS+ プロバイダーの作成 70
TACACS+ プロバイダーの削除 71
Syslog の設定 71
DNS サーバの設定 73

インターフェイス管理 77
Firepower 9300 インターフェイスについて 77
インターフェイス プロパティの編集 78
ポート チャネルの作成 78
ブレークアウト ケーブルの設定 80
論理デバイス 81
論理デバイスについて 81
スタンドアロン ASA 論理デバイスの作成 82
クラスタの導入 84
クラスタリングについて 84
マスターおよびスレーブ ユニットの役割 85
クラスタ制御リンク 85
管理インターフェイス 85
クラスタリングのガイドライン 86
クラスタリングのデフォルト 86
ASA クラスタリングの設定 86
クラスタリングの履歴 89
セキュリティ モジュールのコンソールへの接続 89

第 1 章

Firepower 9300 の概要

- Firepower 9300 セキュリティ アプライアンスについて，1 ページ

Firepower 9300 セキュリティ アプライアンスについて

Cisco Firepower 9300 セキュリティ アプライアンスは、ネットワークおよびコンテンツ向けセキュリティ ソリューションの次世代プラットフォームです。 Firepower 9300 は、シスコ アプリケーション セントリック インフラストラクチャ（ACI）セキュリティ ソリューションの一部として、拡張性、一貫した管理、およびシンプルな管理を実現できるよう構築されており、小回りの効くオープンでセキュアなプラットフォームを提供します。

Firepower 9300 は次の機能を提供します。

- モジュラ シャーシ ベースのセキュリティ システム：高性能で柔軟な入出力構成と、優れた拡張性が提供されます。
- Firepower Chassis Manager：グラフィカル ユーザ インターフェイスでは、現在のシャーシの状態に関する無駄のない視覚表示と、シャーシ機能の簡素化された設定が提供されます。
- FXOS CLI：機能の設定、シャーシ ステータスのモニタ、高度なトラブルシューティング機能へのアクセスを可能にする、コマンドベースのインターフェイスを提供します。
- FXOS REST API：プログラムによるシャーシの設定および管理を可能にします。

第 2 章

コマンドラインインターフェイス（CLI）の概要

- 管理対象オブジェクト，3 ページ
- コマンド モード，4 ページ
- オブジェクト コマンド，5 ページ
- コマンドの実行，7 ページ
- コマンド履歴，7 ページ
- 保留コマンドのコミット、廃棄、および表示，7 ページ
- CLI に関するオンラインヘルプ，8 ページ
- CLI セッション制限，8 ページ

管理対象オブジェクト

Firepower eXtensible Operating System は、管理対象オブジェクト モデルを使用します。このモデルにおける管理対象オブジェクトは、管理可能な物理エンティティまたは論理エンティティの抽象です。 たとえば、シャーシ、セキュリティ モジュール、ネットワーク モジュール、ポート、およびプロセッサは管理対象オブジェクトとして表される物理エンティティです。ライセンス、ユーザ ロール、プラットフォーム ポリシーは管理対象オブジェクトとして表される論理エンティティです。

管理対象オブジェクトには関連付けられている設定可能なプロパティが複数存在する場合があります。

コマンド モード

CLI のコマンド モードは階層構造になっており、EXEC モードがこの階層の最高レベルとなります。 高いレベルのモードは、低いレベルのモードに分岐します。 高いレベルのモードから 1 つ低いレベルのモードに移動するには、**create**、**enter**、および **scope** コマンドを使用します。また、モード階層で 1 つ高いレベルに移動するには、**exit** コマンドを使用します。

（注） コマンド モードの大半は管理対象オブジェクトに関連付けられているため、あるオブジェクトと関連付けられているモードにアクセスできるようにするには、まず、そのオブジェクトを作成する必要があります。 アクセスするモードに対する管理対象オブジェクトを作成するには、**create** および **enter** コマンドを使用します。 **scope** コマンドは、管理対象オブジェクトを作成するものではありません。すでに管理対象オブジェクトが存在するモードにアクセスすることのみ可能です。

各モードには、そのモードで入力できるコマンドのセットが含まれています。 各モードで使用できるほとんどのコマンドは、関連付けられた管理対象オブジェクトに関係しています。

各モードの CLI プロンプトには、モード階層における現在のモードまでのフルパスが表示されます。 これにより、コマンドモード階層での現在位置がわかりやすくなります。また、階層内を移動する必要がある場合には、非常に便利な機能です。

次の表に、主要なコマンド モード、各モードへのアクセスに使用するコマンド、および各モードに関連付けられている CLI プロンプトを示します。

表 *1*：主要なコマンド モードとプロンプト

モード名	アクセスに使用するコマンド	モード プロンプト
EXEC	任意のモードから **top** コマンド	#
アダプタ	EXEC モードで **scope adapter** コマンド	/adapter #
ケーブル配線	EXEC モードから **scope cabling** コマンド	/cabling #
シャーシ	EXEC モードから **scope chassis** コマンド	/chassis #
イーサネット サーバ	EXEC モードで **scope eth-server** コマンド	/eth-server #
イーサネット アップリンク	EXEC モードで **scope eth-uplink** コマンド	/eth-uplink #

モード名	アクセスに使用するコマンド	モード プロンプト
ファブリック インターコネクト	EXEC モードで **scope fabric-interconnect** コマンド	/fabric-interconnect #
ファームウェア	EXEC モードで **scope firmware** コマンド	/firmware #
ホスト イーサネット インターフェイス	EXEC モードで **scope host-eth-if** コマンド	/host-eth-if #
ライセンス	EXEC モードから **scope license** コマンド	/license #
モニタリング	EXEC モードで **scope monitoring** コマンド	/monitoring #
組織	EXEC モードで **scope org** コマンド	/org #
セキュリティ	EXEC モードで **scope security** コマンド	/security #
サーバ	EXEC モードで **scope server** コマンド	/server #
サービス プロファイル	EXEC モードで **scope service-profile** コマンド	/service-profile #
ssa	EXEC モードから **scope ssa** コマンド	/ssa #
システム	EXEC モードで **scope system** コマンド	/system #
仮想 HBA	EXEC モードで **scope vhba** コマンド	/vhba #
仮想 NIC	EXEC モードで **scope vnic** コマンド	/vnic #

オブジェクト コマンド

オブジェクト管理用に 4 つの一般的なコマンドがあります。

- **create***object*
- **delete***object*
- **enter***object*
- **scope***object*

scope コマンドは、永続的オブジェクトであるか、ユーザ インスタンス化オブジェクトであるかに関わらず、すべての管理対象オブジェクトで使用できます。 その他のコマンドを使用して、ユーザ インスタンス化オブジェクトを作成および管理できます。 すべての **create***object* コマンドには、対応する **delete***object* コマンドおよび **enter***object* コマンドが存在します。

ユーザ インスタンス化オブジェクトの管理では、次の表に説明するように、これらのコマンドの動作はオブジェクトが存在するかどうかによって異なります。

表 *2*：オブジェクトが存在しない場合のコマンドの動作

コマンド	動作
create*object*	オブジェクトが作成され、該当する場合、そのコンフィギュレーション モードが開始されます。
delete*object*	エラー メッセージが生成されます。
enter*object*	オブジェクトが作成され、該当する場合、そのコンフィギュレーション モードが開始されます。
scope*object*	エラー メッセージが生成されます。

表 *3*：オブジェクトが存在する場合のコマンドの動作

コマンド	動作
create*object*	エラー メッセージが生成されます。
delete*object*	オブジェクトが削除されます。
enter*object*	該当する場合、オブジェクトのコンフィギュレーション モードが開始されます。
scope*object*	オブジェクトのコンフィギュレーション モードが開始されます。

コマンドの実行

任意のモードで Tab キーを使用すると、コマンドを実行できます。 コマンド名の一部を入力して Tab を押すと、コマンド全体が表示されるか、または別のキーワードを選択するか引数値を入力する必要があるところまで表示されます。

コマンド履歴

CLI では、現在のセッションで使用したすべてのコマンドが保存されます。 上矢印キーまたは下矢印キーを使用すると、これまでに使用したコマンドを 1 つずつ表示できます。 上矢印キーを押すと履歴内の直前のコマンドが、下矢印キーを押すと履歴内の次のコマンドが表示されます。 履歴の最後に到達すると、下矢印キーを押しても次のコマンドが表示されなくなります。

履歴内のすべてのコマンドは、履歴を 1 つずつ表示して目的のコマンドを再度呼び出し、Enter を押すだけでもう一度実行することができます。 このコマンドは手動で入力したように表示されます。 また、コマンドを再度呼び出した後、Enter を押す前にコマンドを変更することもできます。

保留コマンドのコミット、廃棄、および表示

CLI でコンフィギュレーション コマンドを入力する場合は、**commit-buffer** コマンドを入力するまで、そのコマンドは適用されません。 コミットされるまで、コンフィギュレーション コマンドは保留状態となります。**discard-buffer** コマンドを入力して廃棄できます。

複数のコマンド モードで保留中の変更を積み重ね、単一の **commit-buffer** コマンドによりまとめて適用できます。 任意のコマンド モードで **show configuration pending** コマンドを入力すると、保留中のコマンドが表示されます。

（注） 複数のコマンドをまとめてコミットするのは、アトミック操作ではありません。 失敗したコマンドがあっても、成功したコマンドは適用されます。 失敗したコマンドはエラー メッセージで報告されます。

コマンドが保留中の場合、コマンド プロンプトの前にアスタリスク（*）が表示されます。 アスタリスクは、**commit-buffer** コマンドを入力すると消去されます。

次に、プロンプトがコマンド エントリのプロセス中に変わる例を示します。

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

CLI に関するオンラインヘルプ

いつでも ? 文字を入力して、コマンド構文の現在の状態で使用可能なオプションを表示することができます。

プロンプトに何も入力しなかった場合、? と入力すると、現在のモードで使用できるコマンドがすべて表示されます。コマンドの一部を入力した後に ? と入力すると、コマンド構文の現在位置で使用できるキーワードと引数がすべて表示されます。

CLI セッション制限

Firepower eXtensible Operating System は、同時にアクティブにできる CLI セッションの数を合計で 32 セッションに制限します。 この値は設定可能です。

第 3 章

使用する前に

- タスク フロー，9 ページ
- 初期設定，10 ページ
- FXOS CLI へのアクセス，12 ページ

タスク フロー

次の手順では、Firepower アプライアンスの設定時に実行する必要がある基本的なタスクを示します。

手順

ステップ 1 Firepower アプライアンス ハードウェアを設定します（『Cisco Firepower 9300 Hardware Installation Guide』を参照）。

ステップ 2 初期設定を完了します（初期設定，（10 ページ）を参照）。

ステップ 3 日付と時刻を設定します（日時の設定，（47 ページ）を参照）。

ステップ 4 DNS サーバを設定します（DNS サーバの設定，（73 ページ）を参照）。

ステップ 5 製品ライセンスを登録します（ライセンス管理，（15 ページ）を参照）。

ステップ 6 ユーザを設定します（User Management，（23 ページ）を参照）。

ステップ 7 必要に応じてソフトウェア アップデートを実行します（Image Management，（37 ページ）を参照）。

ステップ 8 追加のプラットフォーム設定を行います（Platform Settings，（45 ページ）を参照）。

ステップ 9 インターフェイスを設定します（インターフェイス管理，（77 ページ）を参照）。

ステップ 10 論理デバイスを作成します（論理デバイス，（81 ページ）を参照）。

初期設定

システムの設定と管理に Firepower Chassis Manager または FXOS CLI を使用するには、まず、コンソール ポートを介してアクセスした FXOS CLI を使用して初期設定タスクを実行する必要があります。 FXOS CLI を使用して Firepower アプライアンスに初めてアクセスすると、システムの設定に使用できるセットアップ ウィザードが表示されます。

システム設定を既存のバックアップ ファイルから復元するか、セットアップ ウィザードを実行してシステムを手動でセットアップするか、選択できます。 システムを復元する場合は、バックアップ ファイルが、管理ネットワークから到達可能な場所に存在する必要があります。

Firepower アプライアンスの単一の管理ポートには、1 つのみの IPv4 アドレス、ゲートウェイ、サブネット マスク、または 1 つのみの IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを指定する必要があります。 管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

はじめる前に

1. Firepower アプライアンスの次の物理接続を確認します。
   - コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
   - 1 Gbps イーサネット管理ポートが外部ハブ、スイッチ、またはルータに接続されている。

   詳細については、『Cisco Firepower 9300 Hardware Installation Guide』を参照してください。
2. コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。
   - 9600 ボー
   - 8 データ ビット
   - パリティなし
   - 1 ストップ ビット

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 Firepower アプライアンスの電源を入れます。
Firepower アプライアンスが起動すると、電源投入時セルフテスト メッセージが表示されます。

ステップ 3 未設定のシステムが起動すると、セットアップ ウィザードでシステム設定に必要な次の情報の入力を求められます。

- セットアップ モード（フル システム バックアップからの復元または初期セットアップ）

- 強力なパスワードの適用ポリシー（強力なパスワードのガイドラインについては、User Accounts, （23 ページ）を参照）
- admin パスワード
- システム名
- 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- DNS サーバの IPv4 または IPv6 アドレス
- デフォルトのドメイン名

ステップ 4 設定の要約を確認し、設定を保存および適用する場合は yes を入力し、セットアップ ウィザードをやり直して設定を変更する場合は no を入力します。
セットアップ ウィザードのやり直しを選択した場合は、以前に入力した値がカッコ内に表示されます。 以前に入力した値をそのまま使用する場合は、Enter を押します。

次の例では、IPv4 管理アドレスを使用して設定します。

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IP address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforce Strong Password=no
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  IPv6 value=0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

次の例では、IPv6 管理アドレスを使用して設定します。

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address :  2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
```

```
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

FXOS CLI へのアクセス

FXOS CLIには、コンソール ポートに繋いだ端末を使って接続します。 コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

また、FXOS CLI への接続には SSH と Telnet を使用することもできます。 Firepower eXtensible Operating System では、同時に最大 8 つの SSH 接続がサポートされます。 SSH で接続するには、Firepower アプライアンス のホスト名または IP アドレスが必要になります。

次のいずれかの構文例を使用して SSH、Telnet または Putty でログインします。

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **sshucs-***auth-domain\\username@{UCSM-ip-address|UCMS-ipv6-address}*

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -lucs-***auth-domain\\username {UCSM-ip-address| UCSM-ipv6-address| UCSM-host-name}*

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** *{UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name}* **-lucs-***auth-domain\\username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **sshucs-***auth-domain\\username@{UCSM-ip-address|UCSM-ipv6-address}*

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

Linux 端末からは以下の Telnet を使用します。

（注） Telnet はデフォルトでディセーブルです。 Telnet を有効化する手順については、Telnet の設定,（51 ページ）を参照してください。

- **telnetucs-***UCSM-host-name* **ucs-***auth-domain\username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnetucs-**{*UCSM-ip-address*|*UCSM-ipv6-address*}*ucs-auth-domain\username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントから：

- Login as: **ucs-***auth-domain\username*

```
Login as: ucs-example\jsmith
```

（注） デフォルトの認証がローカルに設定され、コンソール認証が LDAP に設定されている場合は、ucs-local\admin（admin はローカル アカウント名）を使用して Putty クライアントからファブリック インターコネクトにログインできます。

第 4 章

ライセンス管理

シスコ スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。 各ユニットのライセンス キーを管理しなくても、簡単にデバイスを導入したり導入を終了したりできます。 スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

- スマート ソフトウェア ライセンスについて，15 ページ
- スマート ソフトウェア ライセンスの前提条件，17 ページ
- スマート ソフトウェア ライセンスのデフォルト，18 ページ
- スマート ソフトウェア ライセンスの設定，18 ページ
- スマート ソフトウェア ライセンスのモニタリング，20 ページ
- スマート ソフトウェア ライセンスの履歴，21 ページ

スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

Firepower 9300 上のセキュリティ モジュールのスマート ソフトウェア ライセンス

Firepower 9300 上の セキュリティ モジュールの場合、スマート ソフトウェア ライセンス設定は Firepower 9300 スーパーバイザとセキュリティ モジュールの間で分割されます。

- Firepower 9300：License Authority との通信に使用するパラメータなど、スーパーバイザのすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。 Firepower 9300 自体の動作にライセンスは必要ありません。
- セキュリティモジュール：セキュリティ モジュールのすべてのライセンス資格を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

http://tools.cisco.com/rhodui/index

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。 Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスター アカウントの下の [Default Virtual Account] に割り当てられます。 アカウント管理者は、必要に応じて追加の仮想アカウントを作成できます。たとえば、地域、部署、子会社用のアカウントを作成できます。 複数の仮想アカウントを使用すると、大量のライセンスおよびデバイスをより簡単に管理できます。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。アカウントに割り当てられたライセンスを使用できるのは、その仮想アカウントのデバイスのみです。 追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。 仮想アカウント間でデバイスを移行することもできます。

シャーシ内のセキュリティ モジュールには独自のライセンスが必要なため、Firepower 9300 シャーシのみをデバイスとして登録します。 たとえば3つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

デバイス登録とトークン

各仮想アカウントに対して登録トークンを作成できます。 このトークンはデフォルトで 30 日間有効です。 各デバイスの導入時または既存のデバイスの登録時に、このトークン ID と権限付与レベルを入力します。 既存のトークンの有効期限が切れた場合は、新しいトークンを作成できます。

（注） デバイス登録は、セキュリティ モジュールではなく、Firepower 9300 スーパーバイザで設定されます。

導入後、または手動で既存のデバイスにこれらのパラメータを設定した後、起動時にデバイスを Cisco License Authority に登録します。 デバイスをトークンに登録すると、デバイスと License Authority との間の通信に使用する ID 証明書がライセンス機関から発行されます。 この証明書は 6 ヵ月ごとに更新されますが、1 年間有効です。

License Authority との定期通信

デバイスは 30 日ごとに License Authority と通信します。 Smart Software Manager に変更を行う場合、デバイスの認証を更新して変更をすぐに反映させることができます。 またはスケジュール設定されたデバイスの通信を待つこともできます。

必要に応じて、HTTP プロキシを設定できます。 少なくとも 90 日ごとに、デバイスが直接または HTTP プロキシ経由でインターネットにアクセスする必要があります。 通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。 90 日が経過する前に License Authority に連絡してください。

（注） オフライン ライセンスはサポートされていません。

コンプライアンス違反状態

デバイスは次の状況でコンプライアンス違反になる可能性があります。

- 過剰使用：デバイスが利用不可のライセンスを使用した場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れた場合。
- 通信の欠如：デバイスが Licensing Authority にアクセスできず再認証されない場合。

90 日間の再認証試行後、デバイスはアプリケーションに応じた方法で制限されます。

Smart Call Home インフラストラクチャ

デフォルトでは、Licensing Authority の URL を指定する Smart Call Home プロファイルがコンフィギュレーションに存在します。 このプロファイルは削除できません。 ライセンス プロファイルの設定可能なオプションは Licensing Authority の宛先アドレス URL のみであることに注意してください。 Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。

スマート ソフトウェア ライセンスの前提条件

- Cisco Smart Software Manager でマスター アカウントを作成します。

  http://tools.cisco.com/rhodui/index

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。 Smart Software Manager では、組織のマスター アカウントを作成できます。

- Cisco Software Central から 1 つ以上のライセンスを購入します。

- デバイスが Licensing Authority と通信できるように、デバイスからのインターネット アクセスまたは HTTP プロキシ アクセスを確認します。 オフライン ライセンスはサポートされていません。
- デバイスがライセンス認証局サーバの名前を解決できるように、DNS サーバを設定します。 DNS サーバの設定, （73 ページ）を参照してください。
- デバイスのクロックを設定します。 日時の設定, （47 ページ）を参照してください。

スマート ソフトウェア ライセンスのデフォルト

Firepower 9300 のデフォルト設定には、Licensing Authority の URL を指定する、「SLProf」という Smart Call Home プロファイルが含まれます。

```
scope monitoring
  scope callhome
    scope profile SLProf
      scope destination SLDest
        set address https://tools.cisco.com/its/service/oddce/services/DDCEService
```

スマート ソフトウェア ライセンスの設定

Cisco License Authority と通信するため、必要に応じて HTTP プロキシを設定できます。 License Authority に登録するには、スマート ソフトウェア ライセンス アカウントから取得した Firepower 9300 の登録トークン ID を入力する必要があります。

手順

ステップ 1 （任意）HTTP プロキシの設定, （18 ページ）.

ステップ 2 Firepower 9300 の License Authority への登録, （19 ページ）.

（任意）HTTP プロキシの設定

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。 このプロキシは、一般に Smart Call Home にも使用されます。

手順

ステップ 1 HTTP プロキシを有効化します。
scope monitoring scope callhome set http-proxy-server-enable on

例：

```
scope monitoring
  scope call-home
    set http-proxy-server-enable on
```

ステップ 2 プロキシ URL を設定します。
set http-proxy-server-url*ip_address*

例：

```
set http-proxy-server-url 10.1.1.1
```

ステップ 3 ポートを設定します。
set http-proxy-server-port*port*

例：

```
set http-proxy-server-port 443
```

ステップ 4 バッファをコミットします。
commit-buffer

Firepower 9300 の License Authority への登録

License Authority に Firepower 9300 を登録すると、Firepower 9300 と License Authority の間の通信に使用する ID 証明書が発行されます。 また、Firepower 9300 が該当する仮想アカウントに割り当てられます。 通常、この手順は 1 回で済みます。 ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、Firepower 9300 の再登録が必要になります。

手順

ステップ 1 Smart Software Manager で、この Firepower 9300 を追加する仮想アカウントの登録トークンを要求してコピーします。

ステップ 2 Firepower 9300 の登録トークンを入力します。
scope license register idtoken *id-token*

例：

```
scope license
  register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
g3R3dvemRD%0AY29NQT0%3D%0A
```

ステップ 3 後からデバイスの登録を解除するには、次を入力します。

deregister

Firepower 9300 の登録を解除すると、アカウントからデバイスが削除され、 デバイスのすべてのライセンス資格と証明書が削除されます。 登録を解除することで、ライセンスを新しい Firepower 9300 に利用することもできます。 あるいは、Smart Software Manager からデバイスを削除できます。

ステップ 4 ID 証明書を更新し、すべてのセキュリティ モジュールの資格を更新するには、次を入力します。
scope licdebug renew

デフォルトでは、ID 証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

スマート ソフトウェア ライセンスのモニタリング

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **show license all**

  スマート ソフトウェア ライセンスの状態、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、権限付与ステータス、ライセンス証明書情報、およびスマート エージェント タスクのスケジュールを表示します。

- **show license status**
- **show license techsupport**

スマート ソフトウェア ライセンスの履歴

機能名	プラットフォーム リリース	説明
Firepower 9300 のシスコ スマート ソフトウェア ライセンス	1.1(1)	スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを管理することができます。 スマート ライセンスは特定のシリアル番号に関連付けられません。 各ユニットのライセンス キーを管理しなくても、簡単にデバイスを導入したり導入を終了したりできます。 スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 スマート ソフトウェア ライセンス設定は、Firepower 9300 スーパバイザとセキュリティ モジュールの間で分割されます。 次のコマンドが導入されました。**deregister**、**register idtoken**、**renew**、**scope callhome**、**scope destination**、**scope licdebug**、**scope license**、**scope monitoring**、**scope profile**、**set address**、**set http-proxy-server-enable on**、**set http-proxy-server-url**、**set http-proxy-server-port**、**show license all**、**show license status**、**show license techsupport**

第 5 章

User Management

- User Accounts，23 ページ
- デフォルト ユーザ ロール，25 ページ
- ローカル認証されたユーザのパスワード プロファイル，26 ページ
- デフォルト認証サービスの選択，27 ページ
- リモート ユーザのロール ポリシーの設定，28 ページ
- ローカル認証されたユーザへのパスワード強度チェックの有効化，29 ページ
- 変更間隔のパスワード変更の最大数の設定，30 ページ
- パスワードの変更禁止間隔の設定，31 ページ
- パスワード履歴カウントの設定，31 ページ
- ローカル ユーザ アカウントの作成，32 ページ
- ローカル ユーザ アカウントの削除，34 ページ
- ローカル ユーザ アカウントのアクティブ化または非アクティブ化，34 ページ
- ローカル認証されたユーザのパスワード履歴のクリア，35 ページ

User Accounts

ユーザ アカウントは、システムにアクセスするために使用されます。 最大 48 個のローカル ユーザ アカウントを設定できます。 各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

管理者アカウント

管理者アカウントはデフォルト ユーザ アカウントで、変更や削除はできません。 このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられていま

す。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。 管理者アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザ アカウントは、シャーシによって直接認証され、admin 権限か AAA 権限を持つユーザが有効または無効にできます。 ローカル ユーザ アカウントが無効になっている場合、ユーザはログインできません。無効化されたローカル ユーザ アカウントの設定の詳細はデータベースから削除されません。 無効ローカル ユーザ アカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存のコンフィギュレーションで再びアクティブになります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ で認証されたユーザ アカウントです。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。 ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。

ユーザ名に関するガイドライン

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID としても使用されます。ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は一意である必要があります。

- ログイン ID は、英文字で開始する必要があります。 数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワードに関するガイドライン

ローカル認証された各ユーザ アカウントにパスワードが必要です。 admin 権限または AAA 権限を持つユーザは、ユーザ パスワードのパスワード強度チェックを実行するようにシステムを設定できます。 パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。 ローカル認証されたユーザのパスワード強度チェックを有効化した場合、Firepower eXtensible Operating System は次の要件を満たしていないパスワードをすべて拒否します。

- 8 ～ 80 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- password123 のような 3 つの連続する数字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントの場合は空白にしない。

デフォルト ユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。 デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、ローカル認証されたすべてのユーザのパスワード履歴やパスワード変更間隔プロパティが含まれます。 ローカル認証されたユーザのそれぞれに異なるパスワードプロファイルを指定することはできません。

Password History Count

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。 このプロパティが設定されている場合、Firepower シャーシは、ローカル認証されたユーザが以前に使用したパスワードを最大 15 個まで保存します。 パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になる前に、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用する必要があります。 たとえば、パスワード履歴カウントを 8 に設定した場合、ローカル認証されたユーザは最初のパスワードを 9 番目のパスワードが期限切れになった後まで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。 この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザについてパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更回数を制限することができます。 次の表で、パスワード変更間隔の 2 つの設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更不許可	このオプションでは、ローカル認証されたユーザは、パスワードの変更後、指定された時間内にはパスワードを変更できません。 1 ～ 745 時間の変更禁止間隔を指定できます。 デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが 48 時間の間パスワードを変更できないようにする場合、次のように設定します。 • [Change During Interval] をディセーブルに • [No Change Interval] を 48 に
変更間隔内のパスワード変更許可	このオプションは、ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。 デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に 1 回まで変更できるようにする場合、次のように設定します。 • [Change During Interval] をイネーブルに • [Change Count] を 1 に • [Change Interval] を 24 に

デフォルト認証サービスの選択

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scope security**

ステップ 2 デフォルト認証セキュリティ モードを開始します。
Firepower-chassis /security # **scopedefault-auth**

ステップ 3 デフォルト認証を指定します。
Firepower-chassis /security/default-auth # **set realm***auth-type*

auth-type は、次のキーワードのいずれかです。

- **ldap**：LDAP 認証を指定します
- **local**：ローカル認証を指定します
- **none**：ローカル ユーザはパスワードを指定せずにログインできます
- **radius**：RADIUS 認証を指定します

- **tacacs**：TACACS+ 認証を指定します

ステップ 4 （任意） 関連付けられたプロバイダー グループを指定します（存在する場合）。
Firepower-chassis /security/default-auth # **set auth-server-group***auth-serv-group-name*

ステップ 5 （任意） このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。
Firepower-chassis /security/default-auth # **set refresh-period***seconds*

60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。

この時間制限を超えると、Firepower eXtensible Operating System は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。

ステップ 6 （任意） 最後の更新要求から Firepower eXtensible Operating System が Web セッションが終了したと見なすまでの最大経過時間を指定します。
Firepower-chassis /security/default-auth # **set session-timeout***seconds*

60 ～ 172800 の整数を指定します。 デフォルト値は 7200 秒です。

（注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、**セッションの更新**時間および**セッションのタイムアウト**時間を増やすことを検討してください。

ステップ 7 （任意） 認証方式をレルムの二要素認証に設定します。
Firepower-chassis /security/default-auth # **set use-2-factor yes**

（注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。

ステップ 8 トランザクションをシステム設定にコミットします。
commit-buffer

次の例では、デフォルトの認証を RADIUS に設定し、デフォルトの認証プロバイダー グループを provider1 に設定し、二要素認証をイネーブルにし、更新間隔を 7200 秒（2 時間）に設定し、セッションのタイムアウト間隔を 28800 秒（8 時間）に設定し、二要素認証をイネーブルにします。そして、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 7200
Firepower-chassis /security/default-auth* # set session-timeout 28800
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

リモート ユーザのロール ポリシーの設定

デフォルトでは、LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Firepower Chassis Manager または FXOS CLI にログインするすべてのユーザに読み取り専用アクセ

ス権が付与されます。セキュリティ上の理由から、確立されたユーザ ロールに一致するユーザにアクセスを制限することが望ましい場合があります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

ユーザがログインを試みたときに、リモート認証プロバイダーが認証情報を含むユーザ ロールを提供しないと、ユーザは読み取り専用ユーザ ロールでログインすることができます。

これはデフォルトの動作です。

no-login

ユーザがログインを試みたときに、リモート認証プロバイダーが認証情報を含むユーザ ロールを提供しないと、アクセスは拒否されます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 Firepower Chassis Manager および FXOS CLI へのユーザ アクセスをユーザ ロールに基づいて制限するかどうかを指定します。
Firepower-chassis /security # **set remote-user default-role** {**assign-default-role** | **no-login**}

ステップ 3 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 /security # **commit-buffer**

次の例では、リモートユーザのロールポリシーを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # set remote-user default-role no-login
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

ローカル認証されたユーザへのパスワード強度チェックの有効化

パスワード強度チェックが有効化になっている場合、Firepower eXtensible Operating System では、強力なパスワードのガイドラインを満たしていないパスワードを選択できません（パスワードに関するガイドライン，（25 ページ）を参照）。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 パスワード強度チェックを有効化するかディセーブルにするかを指定します。
Firepower-chassis /security # **set enforce-strong-password** {**yes** | **no**}

次に、パスワード強度チェックをイネーブルにする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

変更間隔のパスワード変更の最大数の設定

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 パスワード プロファイル セキュリティ モードを開始します。
Firepower-chassis /security # **scope password-profile**

ステップ 3 ローカル認証されたユーザが指定した時間内にパスワードを変更できる回数を制限します。
Firepower-chassis /security/password-profile # **set change-during-interval enable**

ステップ 4 ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数を指定します。
Firepower-chassis /security/password-profile # **set change-count** *pass-change-num*

この値は、0 ～ 10 から自由に設定できます。

ステップ 5 [Change Count] フィールドで指定したパスワード変更回数が適用される最大時間数を指定します。
Firepower-chassis /security/password-profile # **set change-interval** *num-of-hours*

この値は、1 ～ 745 時間から自由に設定できます。

たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。

ステップ 6 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 /security/password-profile # **commit-buffer**

次の例は、change during interval オプションをイネーブルにし、変更回数を 5 回、変更間隔を 72 時間に設定し、トランザクションをコミットします。

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Firepower-chassis /security/password-profile* # set change-count 5
Firepower-chassis /security/password-profile* # set change-interval 72
```

```
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

パスワードの変更禁止間隔の設定

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 パスワード プロファイル セキュリティ モードを開始します。
Firepower-chassis /security # **scope password-profile**

ステップ 3 間隔中の変更機能をディセーブルにします。
Firepower-chassis /security/password-profile # **set change-during-interval disable**

ステップ 4 ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数を指定します。
Firepower-chassis /security/password-profile # **set no-change-interval** *min-num-hours*

この値は、1 ～ 745 時間から自由に設定できます。

この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合、無視されます。

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 /security/password-profile # **commit-buffer**

次に、間隔中の変更オプションをディセーブルにし、変更禁止間隔を72時間に設定し、トランザクションをコミットする例を示します。

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

パスワード履歴カウントの設定

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 パスワード プロファイル セキュリティ モードを開始します。
Firepower-chassis /security # **scope password-profile**

ステップ 3 ローカル認証されたユーザが、以前に使用したパスワードを再利用できるようになるまでに、作成する必要がある一意のパスワードの数を指定します
Firepower-chassis /security/password-profile # **set history-count** *num-of-passwords*

この値は、0 ～ 15 から自由に設定できます。

デフォルトでは、[History Count] フィールドは 0 に設定されます。これは、履歴カウントをディセーブルにし、ユーザはいつでも前に使用されたパスワードを再使用できます。

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 /security/password-profile # **commit-buffer**

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set history-count 5
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

ローカル ユーザ アカウントの作成

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 ユーザ アカウントを作成します。
Firepower-chassis /security # **create local-user** *local-user-name*

ステップ 3 ローカル ユーザ アカウントを有効化するかディセーブルにするかを指定します。
Firepower-chassis /security/local-user # **set account-status** {**active**| **inactive**}

ステップ 4 ユーザ アカウントのパスワードを設定します。
Firepower-chassis /security/local-user # **set password**

パスワードを入力します。*password*

パスワードを確認します。*password*

ステップ 5 （任意） ユーザの名を指定します。
Firepower-chassis /security/local-user # **set firstname** *first-name*

ステップ 6 （任意） ユーザの姓を指定します。
Firepower-chassis /security/local-user # **set lastname** *last-name*

ステップ 7 （任意） ユーザ アカウントが期限切れになる日付を指定します。 *month* 引数は、月の英名の最初の 3 文字です。
Firepower-chassis /security/local-user # **set expiration** *month day-of-month year*

（注） ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。 ただし、アカウントの有効期限を使用可能な最も遅い日付に設定することは可能です。

ステップ 8 （任意） ユーザの電子メール アドレスを指定します。
Firepower-chassis /security/local-user # **set email** *email-addr*

ステップ 9 （任意） ユーザの電話番号を指定します。
Firepower-chassis /security/local-user # **set phone** *phone-num*

ステップ 10 （任意） パスワードレス アクセス用の SSH キーを指定します。
Firepower-chassis /security/local-user # **set sshkey** *ssh-key*

ステップ 11 トランザクションをコミットします。
Firepower-chassis security/local-user # **commit-buffer**

次の例は、kikipopo という名前のユーザ アカウントを作成し、ユーザ アカウントをイネーブルにし、foo12345 にパスワードを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

次の例は、lincey という名前のユーザアカウントを作成し、ユーザアカウントをイネーブルにし、パスワードレス アクセス用の OpenSSH キーを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

次の例は、jforlenz という名前のユーザ アカウントを作成し、ユーザ アカウントをイネーブルにし、パスワードレスアクセス用のセキュア SSH キーを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

ローカル ユーザ アカウントの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 ローカルユーザ アカウントを削除します。
Firepower-chassis /security # **delete local-user***local-user-name*

ステップ 3 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 /security #**commit-buffer**

次に、foo というユーザ アカウントを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

ローカルユーザアカウントのアクティブ化または非アクティブ化

ローカル ユーザ アカウントをアクティブ化または非アクティブ化できるのは、admin 権限または AAA 権限を持つユーザのみです。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 アクティブ化または非アクティブ化するユーザに対してローカルユーザセキュリティモードを開始します。
Firepower-chassis /security # **scope local-user***local-user-name*

ステップ 3 ローカル ユーザ アカウントをアクティブ化するか非アクティブ化するかを指定します。
Firepower-chassis /security/local-user # **set account-status** {**active** | **inactive**}

（注） admin ユーザ アカウントは常にアクティブに設定されます。 変更はできません。

次に、accounting というローカル ユーザ アカウントをイネーブルにする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope local-user accounting
Firepower-chassis /security/local-user # set account-status active
```

ローカル認証されたユーザのパスワード履歴のクリア

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis # **scopesecurity**

ステップ 2 指定したユーザ アカウントに対してローカル ユーザ セキュリティ モードを開始します。
Firepower-chassis /security # **scope local-user** *user-name*

ステップ 3 指定したユーザ アカウントのパスワード履歴をクリアします。
Firepower-chassis /security/local-user # **clear password-history**

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 /security/local-user # **commit-buffer**

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

第 6 章

Image Management

- イメージ管理について，37 ページ
- Cisco.com からのイメージのダウンロード，38 ページ
- Firepower eXtensible Operating System ソフトウェア イメージの Firepower アプライアンス へのダウンロード，38 ページ
- Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード，39 ページ
- 論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード，40 ページ
- 論理デバイスのイメージ バージョンの更新，42 ページ

イメージ管理について

Firepower アプライアンスが使用するイメージには、次の 2 つの基本タイプがあります。

（注） すべてのイメージに対して、セキュアブートによるデジタル署名と検証が行われます。 イメージを少しでも変更すると検証エラーが発生するため、変更しないでください。

- プラットフォーム バンドル：Firepower プラットフォーム バンドルは、Firepower Supervisor および Firepower セキュリティ モジュールで動作する、複数の独立したイメージの集まりです。 プラットフォーム バンドルは、Firepower eXtensible Operating System のソフトウェア パッケージです。
- アプリケーション：アプリケーションイメージは、Firepower アプライアンスのセキュリティ モジュールに導入するソフトウェア イメージです。 アプリケーション イメージは、Cisco Secure Package ファイル（CSP）として提供されます。これは、論理デバイス作成時にセキュリティ モジュールに展開されるまで（または以降の論理デバイス作成に備えて）スーパーバイザに保存されます。 リリース 1.1.1 で使用できるアプリケーション イメージは ASA ASA

用のものに限られています。Firepower Supervisor には、同じアプリケーションイメージタイプについて複数のバージョンを保存することができます。

Cisco.com からのイメージのダウンロード

はじめる前に

Cisco.com アカウントが必要です。

手順

ステップ 1 Web ブラウザを使用して、http://www.cisco.com/go/firepower9300-software にアクセスします。
Firepower アプライアンスのソフトウェア ダウンロード ページがブラウザに表示されます。

ステップ 2 該当するソフトウェア イメージを見つけて、ローカル コンピュータにダウンロードします。

Firepower eXtensible Operating System ソフトウェア イメージの Firepower アプライアンス へのダウンロード

FTP、SCP、SFTP、または TFTP を使用して、FXOS ソフトウェア イメージを Firepower アプライアンス にコピーできます。

はじめる前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

- イメージのコピー元であるサーバの IP アドレスおよび認証クレデンシャル
- FXOS イメージ ファイルの完全修飾名

手順

ステップ 1 ファームウェア モードを開始します。
Firepower-chassis # **scopefirmware**

ステップ 2 FXOS ソフトウェア イメージをダウンロードします。
Firepower-chassis /firmware # **download image** *URL*

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*
- **scp**:// *username@hostname* / *path*

- **sftp**:// *username@hostname* / *path*
- **tftp**:// *hostname* : *port-num* / *path*

ステップ 3 ダウンロード プロセスをモニタする場合：
Firepower-chassis /firmware # **show package** *image_name* **detail**

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
    File Name: fxos-k9.1.1.1.119.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 5120
    State: Downloading
    Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード

はじめる前に

プラットフォーム バンドルのソフトウェア イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロード, （38 ページ）を参照）、そのイメージを Firepower アプライアンスに（ダウンロード）します（論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード, （40 ページ）を参照）。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 組織モードを開始します。
Firepower-chassis# **scopeorg**

ステップ 3 デフォルト プラットフォーム パック モードを開始します。
Firepower-chassis /org # **scopefw-platform-packdefault**

ステップ 4 デフォルト プラットフォーム バンドルをインストールするバージョンに設定します。
Firepower-chassis /org/fw-platform-pack # **setplatform-bundle-version***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。

ステップ 5 変更をコミットし、アップグレード プロセスを開始します。

commit-buffer

Firepower eXtensible Operating System は、バンドルを展開してコンポーネントをアップグレードおよびリロードします。

ステップ 6 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。

a) **scopefirmware** を入力します。
b) **scopeauto-install** を入力します。
c) **showfsmstatusexpand** を入力します。

論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード

FTP、SCP、SFTP、または TFTP を使用して、論理デバイス ソフトウェア イメージを Firepower アプライアンス にコピーできます。

はじめる前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

- イメージのコピー元であるサーバの IP アドレスおよび認証クレデンシャル
- ソフトウェア イメージ ファイルの完全修飾名

手順

ステップ 1 セキュリティ サービス モードを開始します。
Firepower-chassis # **scopessa**

ステップ 2 アプリケーション ソフトウェア モードを開始します。
Firepower-chassis /ssa # **scopeapp-software**

ステップ 3 論理デバイス ソフトウェア イメージをダウンロードします。
Firepower-chassis /ssa/app-software # **download image** *URL*

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*
- **scp**://*username@hostname/path*
- **sftp**://*username@hostname/path*
- **tftp**://*hostname*:*port-num/path*

ステップ 4 ダウンロード プロセスをモニタする場合：

Firepower-chassis /ssa/app-software # **show download-task**

ステップ 5 ダウンロードしたアプリケーションを表示する場合：
Firepower-chassis /ssa/app-software # **up**
Firepower-chassis /ssa # **show app**

ステップ 6 特定のアプリケーションの詳細を表示する場合：
Firepower-chassis /ssa # **scope app** *application_type image_version*
Firepower-chassis /ssa/app # **show expand**

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                        Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes

    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application

    Net Mgmt Bootstrap Key for the Application:
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------- ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1
```

```
        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

論理デバイスのイメージ バージョンの更新

はじめる前に

論理デバイスに使用するアプリケーションイメージをCisco.comからダウンロードして（Cisco.comからのイメージのダウンロード，（38 ページ）を参照）、そのイメージをFirepower アプライアンスに（ダウンロード）します（論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード，（40 ページ）を参照）。

手順

ステップ 1 セキュリティ サービス モードを開始します。
Firepower-chassis # **scopessa**

ステップ 2 スコープを更新するセキュリティ モジュールに設定します。
Firepower-chassis /ssa # **scopeslot***slot_number*

ステップ 3 スコープを更新するアプリケーションに設定します。
Firepower-chassis /ssa/slot # **scopeapp-instance***app_template*

ステップ 4 スタートアップ バージョンを更新するバージョンに設定します。
Firepower-chassis /ssa/slot/app-instance # **setstartup-version***version_number*

ステップ 5 設定をコミットします。
commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

次の例では、セキュリティモジュール1で動作するASAのソフトウェアイメージを更新します。show コマンドを使用すると、更新ステータスを表示できます。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa
Firepower-chassis /ssa/slot/app-instance # set startup-version 9.4.1.65
Firepower-chassis /ssa/slot/app-instance* # show configuration pending
 enter app-instance asa
+    set startup-version 9.4.1.65
 exit
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance # show
```

```
Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Updating          9.4.1.41        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
Firepower-chassis /ssa/slot/app-instance # show

Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Online            9.4.1.65        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
```

第 7 章

Platform Settings

- 管理 IP アドレスの変更，45 ページ
- 日時の設定，47 ページ
- SSH の設定，51 ページ
- Telnet の設定，51 ページ
- SNMP の設定，52 ページ
- HTTPS ポートの変更，60 ページ
- AAA の設定，61 ページ
- Syslog の設定，71 ページ
- DNS サーバの設定，73 ページ

管理 IP アドレスの変更

はじめる前に

Firepower アプライアンスの管理 IP アドレスを変更するには、次の手順を使用します。

（注） 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

手順

ステップ 1 IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。
Firepower-chassis# **scopefabric-interconnecta**

b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect # **show**

c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect #
setout-of-bandip*ip_address***netmask***network_mask***gw***gateway_ip_address*

d) 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 /fabric-interconnect* # **commit-buffer**

ステップ 2 IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。
Firepower-chassis# **scopefabric-interconnecta**

b) 管理 IPv6 設定のスコープを設定します。
Firepower-chassis /fabric-interconnect # **scopeipv6-config**

c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect/ipv6-config #
setout-of-bandipv6*ipv6_address***ipv6-prefix***prefix_length***ipv6-gw***gateway_address*

e) 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 /fabric-interconnect/ipv6-config* # **commit-buffer**

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                        Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    2001::8998                          64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
```

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

日時の設定

手動で日時を設定するか、NTP サーバを設定するには、（以下に説明する CLI コマンド）を使用します。シャーシに設定した時刻とタイムゾーンが、論理デバイスを含むシャーシ内の他のコンポーネントと同期されます。

タイム ゾーンの設定

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 タイム ゾーンを設定します。
Firepower-chassis /system/services # **settimezone**

この時点で、大陸、国、およびタイム ゾーン領域に対応する番号を入力するように求められます。プロンプトごとに適切な情報を入力します。

ロケーション情報の指定を完了すると、プロンプトが表示され、正しいタイム ゾーン情報が設定されているか確認するよう求められます。確認する場合は 1（yes）を入力し、操作をキャンセルする場合は 2（no）を入力します。

ステップ 4 設定されたタイム ゾーンを表示する場合：
Firepower-chassis /system/services # **top**
Firepower-chassis# **show timezone**

次に、太平洋標準時領域にタイム ゾーンを設定し、トランザクションをコミットし、設定したタイム ゾーンを表示する例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
```

```
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2015.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2015.
Is the above information OK?
1) Yes
2) No
#? 1
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services # top
Firepower-chassis# show timezone
Timezone: America/Los_Angeles (Pacific Time)
Firepower-chassis#
```

NTP サーバの追加

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 指定したホスト名、IPv4 または IPv6 アドレスの NTP サーバを使用するようにシステムを設定します。
Firepower-chassis /system/services # **createntp-server***{hostname | ip-addr | ip6-addr}*

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 /system/services # **commit-buffer**

次の例では、IP アドレス 192.168.200.101 を持つ NTP サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IPv6 アドレス 4001::6 を持つ NTP サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

NTP サーバの削除

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 指定したホスト名、IPv4 または IPv6 アドレスの NTP サーバを削除します。
Firepower-chassis /system/services # **deletentp-server***{hostname | ip-addr | ip6-addr}*

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 /system/services # **commit-buffer**

次に、IP アドレス 192.168.200.101 の NTP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次に、IPv6 アドレス 4001::6 の NTP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

手動での日付と時刻の設定

ここでは、Firepower シャーシで日付と時刻を手動で設定する方法について説明します。 システム クロックの変更はただちに反映されます。

（注） システム クロックが NTP サーバと同期中である場合は、日付と時刻を手動で設定することはできません。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 システム クロックを設定します。
Firepower-chassis /system/services # **set clock** *month day year hour min sec*

month には、月の英名の最初の 3 文字を使用します。 時間は 24 時間形式で入力する必要があります。午後 7 時は 19 になります。

システム クロックの変更はただちに反映されます。バッファをコミットする必要はありません。

次に、システム クロックを設定する例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set clock jun 24 2015 15 27 00
Firepower-chassis /system/services #
```

SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効化またはディセーブルにする方法について説明します。 SSH はデフォルトでイネーブルになります。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 Firepower シャーシへの SSH アクセスを設定するには、次のいずれかを実行します。

- Firepower シャーシへの SSH アクセスを許可するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **enable ssh-server**

- Firepower シャーシへの SSH アクセスを禁止するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **disable ssh-server**

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 /system/services # **commit-buffer**

次の例では、Firepower シャーシへの SSH アクセスを有効化し、トランザクションをコミットします。

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # enable ssh-server
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Telnet の設定

次の手順では、Firepower シャーシへの Telnet アクセスを有効化またはディセーブルにする方法について説明します。 Telnet はデフォルトでディセーブルです。

（注） 現在は、CLI を使用した Telnet 設定のみ可能です。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 Firepower シャーシへの Telnet アクセスを設定するには、次のいずれかを実行します。

- Firepower シャーシへの Telnet アクセスを許可するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **enable telnet-server**

- Firepower シャーシへの Telnet アクセスを禁止するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **disable telnet-server**

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 /system/services # **commit-buffer**

次に、Telnet を有効にし、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

SNMP の設定

ここでは、Firepower シャーシに簡易ネットワーク管理プロトコル（SNMP）を設定する方法について説明します。 詳細については、次のトピックを参照してください。

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーションレイヤ プロトコルです。 SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- SNMP エージェント：Firepower シャーシ内のソフトウェア コンポーネントで、Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに送信します。 Firepower シャーシには、エージェントと一連の MIB が含まれています。 SNMP エージェントを有効化にしてマネージャとエージェント間のリレーションシップを作成するには、Firepower Chassis Manager または FXOS CLI で SNMP を有効化して設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。 SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。 SNMP は次のように定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。 これらの通知では、要求を SNMP マネージャから送信する必要はありません。 通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Firepower シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。 SNMP マネージャはトラップ受信時に確認応答を送信せず、Firepower シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。 インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。 Firepower シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、およびSNMPv3はそれぞれ別のセキュリティモデルを表します。 セキュリティモデルは選択されたセキュリティ レベルと組み合わされ、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージの表示に必要な権限を決定します。 権限レベルは、開示されないようメッセージを保護する必要があるか、またはメッセージを認証する必要があるかどうかを決定します。 サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。 SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。 セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。 セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *4*： *SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	[Username]	No	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-SHA	No	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。 SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。 SNMPv3 ユーザベース セキュリティ モデル（USM） は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

MIB のサポート

Firepower シャーシは MIB への読み取り専用アクセスをサポートします。

SNMPv3 ユーザの認証プロトコル

Firepower シャーシは、SNMPv3 ユーザの HMAC-SHA-96（SHA）認証プロトコルをサポートします。

SNMPv3 ユーザの AES プライバシー プロトコル

Firepower シャーシは、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。 AES-128 の設定を有効化して、SNMPv3 ユーザのプライバシー パスワードを含めると、Firepower シャーシはそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。 AES のプライバシー パスワードは最小で 8 文字です。 パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP のイネーブル化および SNMP プロパティの設定

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP を有効化します。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 SNMP コミュニティ モードを開始します。
Firepower-chassis /monitoring # **set snmp community**

set snmp community コマンドを入力すると、SNMP コミュニティの入力を求められます。

ステップ 4 SNMP コミュニティを指定します。 パスワードとしてコミュニティ名を使用します。 コミュニティ名は、最大 32 文字の英数字で指定できます。
Firepower-chassis /monitoring # **Enter a snmp community:***community-name*

ステップ 5 SNMP 担当者のシステムの連絡先を指定します。 システムの連絡先名（電子メール アドレスや、名前と電話番号など）は、最大 255 文字の英数字で指定できます。
Firepower-chassis /monitoring # **set snmp syscontact***system-contact-name*

ステップ 6 SNMP エージェント（サーバ）が実行されるホストの場所を指定します。 システム ロケーション名は、最大 512 文字の英数字で指定できます。
Firepower-chassis /monitoring # **set snmp syslocation***system-location-name*

ステップ 7 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 /monitoring # **commit-buffer**

次に、SNMP をイネーブルにし、SnmpCommSystem2 という名前の SNMP コミュニティを設定し、contactperson という名前のシステム連絡先を設定し、systemlocation という名前の連絡先ロケーションを設定し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
Firepower-chassis /monitoring* # set snmp syscontact contactperson1
Firepower-chassis /monitoring* # set snmp syslocation systemlocation
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

次の作業

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP をイネーブルにします。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 指定したホスト名、IPv4 アドレス、または IPv6 アドレスで SNMP トラップを作成します。
Firepower-chassis /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}

ステップ 4 SNMP トラップに使用する SNMP コミュニティ名を指定します。
Firepower-chassis /monitoring/snmp-trap # **set community** *community-name*

ステップ 5 SNMP トラップに使用するポートを指定します。
Firepower-chassis /monitoring/snmp-trap # **set port***port-num*

ステップ 6 トラップに使用する SNMP のバージョンとモデルを指定します。
Firepower-chassis /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}

ステップ 7 （任意） 送信するトラップのタイプを指定します。
Firepower-chassis /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}

ここに表示される値は次のとおりです。

- バージョンで v2c または v3 を選択した場合は **traps**。
- バージョンで v2c を選択した場合は **informs**。

（注） バージョンで v2c を選択した場合にのみインフォーム通知を送信できます。

ステップ 8 （任意） バージョンで v3 を選択した場合は、トラップに関連付ける権限を指定します。
Firepower-chassis /monitoring/snmp-trap # **set v3privilege** {**auth** | **noauth** | **priv**}

ここに表示される値は次のとおりです。

- [auth]：認証されますが、暗号化されません
- [noauth]：認証も暗号化も行われません
- [priv]：認証と暗号化が行われます

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 /monitoring/snmp-trap # **commit-buffer**

次の例は、SNMP をイネーブルにし、IPv4 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem2 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 192.168.100.112
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem2
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

次の例は、SNMP をイネーブルにし、IPv6 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem3 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 2001::1
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem3
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

SNMP トラップの削除

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 指定したホスト名または IP アドレスの SNMP トラップを削除します。
Firepower-chassis /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}

ステップ 3 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 /monitoring # **commit-buffer**

次に、IP アドレス 192.168.100.112 で SNMP トラップを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-trap 192.168.100.112
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

SNMPv3 ユーザの作成

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP を有効化します。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 指定した SNMPv3 ユーザを作成します。
Firepower-chassis /monitoring # **create snmp-user***user-name*

create snmp-user コマンドを入力すると、パスワードの入力を促すプロンプトが表示されます。

ステップ 4 AES-128 暗号化の使用を有効化またはディセーブルにします。
Firepower-chassis /monitoring/snmp-user # **set aes-128** {**no** | **yes**}

デフォルトでは、AES-128 暗号化はディセーブルになっています。

ステップ 5 ユーザ プライバシー パスワードを指定します。
Firepower-chassis /monitoring/snmp-user # **set priv-password**

set priv-password コマンドを入力すると、プライバシー パスワードの入力と確認を促すプロンプトが表示されます。

ステップ 6 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 /monitoring/snmp-user # **commit-buffer**

次の例では、SNMP を有効化し、snmp-user14 という名前の SNMPv3 ユーザを作成し、AES-128 暗号化を有効化し、パスワードおよびプライバシー パスワードを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-user snmp-user14
Password:
Firepower-chassis /monitoring/snmp-user* # set aes-128 yes
Firepower-chassis /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
```

```
Firepower-chassis /monitoring/snmp-user* # commit-buffer
Firepower-chassis /monitoring/snmp-user #
```

SNMPv3 ユーザの削除

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 指定した SNMPv3 ユーザを削除します。
Firepower-chassis /monitoring # **delete snmp-user***user-name*

ステップ 3 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 /monitoring # **commit-buffer**

次に、snmp user14 という名前の SNMPv3 ユーザを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-user snmp-user14
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

HTTPS ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。 HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 HTTPS 接続に使用するポートを指定します。
Firepower-chassis /system/services # **sethttpsport***port-number*

port-number には 1 ～ 65535 の整数を指定します。 HTTPS は、デフォルトでポート 443 で有効化になります。

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 /system/services # **commit-buffer**

HTTPS ポートを変更すると、現在のすべての HTTPS セッションが閉じられます。 ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

<*chassis_mgmt_ip_address*> は、初期設定時に入力した Firepower シャーシの IP アドレスまたはホスト名で、<*chassis_mgmt_port*> は設定が完了した HTTPS ポートです。

次の例では、HTTPS ポート番号を 443 に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set https port 444
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

AAA の設定

ここでは、認証、認可、アカウンティングについて説明します。 詳細については、次のトピックを参照してください。

AAA について

AAA は、コンピュータ リソースへのアクセスの制御、ポリシーの適用、使用状況の評価することでサービスの課金に必要な情報を提供する、一連のサービスです。 これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。 AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。 クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。 クレデンシャルが一致しない場合、認証は失敗し、ネットワーク アクセスは拒否されます。

Firepower アプライアンスでは、次のセッションを含むシャーシへの管理接続を認証するように設定することができます。

- HTTPS
- SSH
- シリアル コンソール

認証

認可はポリシーを使用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。 ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

Accounting

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。そこには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。 アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティ プランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。 認可では必ず、ユーザの認証が最初に済んでいる必要があります。 アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス コントロールに使用されるネットワーク サーバです。 認証は、ユーザを識別します。 認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。 アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

ローカル データベースのサポート

Firepower シャーシは、ユーザ プロファイルを取り込むことができるローカル データベースを維持します。 AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。 個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザ アカウントを作成します。 このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 指定した属性を含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set attribute** *attribute*

ステップ 4 指定した識別名を含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set basedn** *distinguished-name*

ステップ 5 指定したフィルタを含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set filter** *filter*

ステップ 6 システムがサーバをダウン状態として通知する前に、LDAP サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/ldap # **set timeout** *seconds*

ステップ 7 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 /security/ldap # **commit-buffer**

次の例では、LDAP 属性を CiscoAvPair に、ベース識別名を「DC=cisco-firepower-aaa3,DC=qalab,DC=com」に、フィルタを sAMAccountName=$userid に、タイムアウト間隔を 5 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # set attribute CiscoAvPair
Firepower-chassis /security/ldap* # set basedn "DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap* # set filter sAMAccountName=$userid
Firepower-chassis /security/ldap* # set timeout 5
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

（注） ユーザ ログインは LDAP ユーザーの userdn が 255 文字を超えると失敗します。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の LDAP プロバイダーがサポートされます。

はじめる前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザ アカウントを作成します。 このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 LDAP サーバ インスタンスを作成し、セキュリティ LDAP サーバ モードを開始します。
Firepower-chassis /security/ldap # **create server***server-name*

SSL が有効化の場合、*server-name* は、通常 IP アドレスまたは FQDN となり、LDAP サーバのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。 IP アドレスが指定されていない場合は、DNS サーバを設定する必要があります。

ステップ 4 （任意） ユーザ ロールとロケールの値を保管する LDAP 属性を設定します。
Firepower-chassis /security/ldap/server # **set attribute***attr-name*

このプロパティは、常に、名前と値のペアで指定されます。 システムは、ユーザ レコードで、この属性名と一致する値を検索します。

デフォルトの属性が LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 5 （任意） リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名を設定します。
Firepower-chassis /security/ldap/server # **set basedn***basedn-name*

ベース DN の長さは、最大 255 文字から CN=username の長さを引いた長さに設定することができます。 username により、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI にアクセスしようとするリモート ユーザが識別されます。

デフォルトのベース DN が LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 6 （任意） ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）を設定します。
Firepower-chassis /security/ldap/server # **set binddn***binddn-name*

サポートされるストリングの最大長は 255 文字（ASCII）です。

ステップ 7 （任意） LDAP 検索を、定義されたフィルタと一致するユーザ名に制限します。
Firepower-chassis /security/ldap/server # **set filter***filter-value*

デフォルトのフィルタが LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 8 バインド DN に指定した LDAP データベース アカウントのパスワードを指定します。

Firepower-chassis /security/ldap/server # **set password**

標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。

パスワードを設定するには、**set password** コマンドを入力してから **Enter** キーを押し、プロンプトでキー値を入力します。

ステップ 9 （任意） Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序を指定します。
Firepower-chassis /security/ldap/server # **set order***order-num*

ステップ 10 （任意） LDAP サーバとの通信に使用するポートを指定します。 標準ポート番号は 389 です。
Firepower-chassis /security/ldap/server # **set port***port-num*

ステップ 11 LDAP サーバと通信するときの暗号化の使用を有効化またはディセーブルにします。
Firepower-chassis /security/ldap/server # **set ssl** {**yes**|**no**}

オプションは次のとおりです。

- **yes**：暗号化が必要です。 暗号化をネゴシエートできない場合は、接続に失敗します。
- **no**：暗号化はディセーブルです。 認証情報はクリア テキストとして送信されます。

LDAP では STARTTLS が使用されます。 これにより、ポート 389 を使用した暗号化通信が可能になります。

ステップ 12 LDAP データベースへの問い合わせがタイム アウトするまでの秒数を指定します。
Firepower-chassis /security/ldap/server # **set timeout***timeout-num*

1～60秒の整数を入力するか、0（ゼロ）を入力してLDAPプロバイダーに対して指定したグローバル タイムアウト値を使用します。 デフォルトは 30 秒です。

ステップ 13 LDAP プロバイダーまたはサーバの詳細を提供するベンダーを指定します。
Firepower-chassis /security/ldap/server # **set vendor***{ms-ad | openldap}*

オプションは次のとおりです。

- **ms-ad**：LDAP プロバイダーは Microsoft Active Directory です。
- **openldap**：LDAP プロバイダーは Microsoft Active Directory ではありません。

ステップ 14 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 /security/ldap/server # **commit-buffer**

次の例では、10.193.169.246 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 10.193.169.246
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
```

```
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 2
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 30
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

次の例では、12:31:71:1231:45b1:0011:011:900 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 1
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 45
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

LDAP プロバイダーの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 指定したサーバを削除します。
Firepower-chassis /security/ldap # **delete server** *serv-name*

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 /security/ldap # **commit-buffer**

次に、ldap1 という名前の LDAP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # delete server ldap1
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。 個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope radius**

ステップ 3 （任意） サーバをダウン状態として通知する前に RADIUS サーバとの通信を再試行する回数を指定します。
Firepower-chassis /security/radius # **set retries** *retry-num*

ステップ 4 （任意） システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/radius # **set timeout** *seconds*

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 /security/radius # **commit-buffer**

次の例は、RADIUS リトライを 4 に設定し、タイムアウト間隔を 30 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # set retries 4
Firepower-chassis /security/radius* # set timeout 30
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の RADIUS プロバイダーがサポートされます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope radius**

ステップ 3 RADIUS サーバ インスタンスを作成し、セキュリティ RADIUS サーバ モードを開始します。
Firepower-chassis /security/radius # **create server***server-name*

ステップ 4 （任意） RADIUS サーバとの通信に使用するポートを指定します。
Firepower-chassis /security/radius/server # **set authport***authport-num*

ステップ 5 RADIUS サーバ キーを設定します。
Firepower-chassis /security/radius/server # **set key**

キー値を設定するには、**set key** コマンドを入力してから Enter キーを押し、プロンプトでキー値を入力します。

ステップ 6 （任意） このサーバが試行される順序を指定します。
Firepower-chassis /security/radius/server # **set order** *order-num*

ステップ 7 （任意） サーバをダウン状態として通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
Firepower-chassis /security/radius/server # **set retries** *retry-num*

ステップ 8 システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を指定します。
Firepower-chassis /security/radius/server # **set timeout** *seconds*

ヒント RADIUS プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。

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 /security/radius/server # **commit-buffer**

次の例は、radiusserv7 という名前のサーバインスタンスを作成し、認証ポートを 5858 に設定し、キーを radiuskey321 に設定し、順序を 2 に設定し、再試行回数を 4 回に設定し、タイムアウトを 30 に設定し、二要素認証をイネーブルにし、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # create server radiusserv7
Firepower-chassis /security/radius/server* # set authport 5858
Firepower-chassis /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
Firepower-chassis /security/radius/server* # set order 2
Firepower-chassis /security/radius/server* # set retries 4
Firepower-chassis /security/radius/server* # set timeout 30
Firepower-chassis /security/radius/server* # commit-buffer
Firepower-chassis /security/radius/server #
```

RADIUS プロバイダーの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope RADIUS**

ステップ 3 指定したサーバを削除します。
Firepower-chassis /security/radius # **delete server** *serv-name*

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 /security/radius # **commit-buffer**

次の例は、radius1 という RADIUS サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # delete server radius1
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。 個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3 （任意） システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/tacacs # **set timeout** *seconds*

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 /security/tacacs # **commit-buffer**

次の例は、TACACS+ タイムアウト間隔を 45 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # set timeout 45
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の TACACS+ プロバイダーがサポートされます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3 TACACS+ サーバ インスタンスを作成し、TACACS+ サーバ モードを開始します。
Firepower-chassis /security/tacacs # **create server** *server-name*

ステップ 4 TACACS+ サーバ キーを指定します。
Firepower-chassis /security/tacacs/server # **set key**

キー値を設定するには、**set key** コマンドを入力してから Enter キーを押し、プロンプトでキー値を入力します。

ステップ 5 （任意） このサーバが試行される順序を指定します。
Firepower-chassis /security/tacacs/server # **set order***order-num*

ステップ 6 システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を指定します。
Firepower-chassis /security/tacacs/server # **set timeout***seconds*

ヒント TACACS+ プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。

ステップ 7 （任意） TACACS+ サーバとの通信に使用するポートを指定します。
Firepower-chassis /security/tacacs/server # **set port***port-num*

ステップ 8 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 /security/tacacs/server # **commit-buffer**

次の例は、tacacsserv680 という名前のサーバ インスタンスを作成し、キーを tacacskey321 に設定し、順序を 4 に設定し、認証ポートを 5859 に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # create server tacacsserv680
Firepower-chassis /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
Firepower-chassis /security/tacacs/server* # set order 4
Firepower-chassis /security/tacacs/server* # set port 5859
Firepower-chassis /security/tacacs/server* # commit-buffer
Firepower-chassis /security/tacacs/server #
```

TACACS+ プロバイダーの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3 指定したサーバを削除します。
Firepower-chassis /security/tacacs # **delete server** *serv-name*

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 /security/tacacs # **commit-buffer**

次の例では、tacacs1 という TACACS+ サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # delete server tacacs1
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

Syslog の設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。 中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。 syslog サービスは、シンプルコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。 この形式のロギングは、保護された長期的な保存場所をログに提供します。 ログは、ルーチントラブルシューティングおよびインシデント処理の両方で役立ちます。

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 コンソールへの syslog の送信を有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog console**

ステップ 3 （任意） 表示するメッセージの最低レベルを選択します。 syslog がイネーブルの場合、システムはそのレベル以上のメッセージをコンソールに表示します。 レベル オプションは緊急性の降順で一覧表示されます。 デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}

ステップ 4 オペレーティング システムによる syslog 情報のモニタリングを有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog monitor**

ステップ 5 （任意） 表示するメッセージの最低レベルを選択します。 モニタの状態がイネーブルの場合、システムはそのレベル以上のメッセージを表示します。 レベル オプションは緊急性の降順で一覧表示されます。 デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

（注） Critical より下のレベルのメッセージは、**terminal monitor** コマンドを入力した場合にのみ端末モニタに表示されます。

ステップ 6 syslog ファイルへの syslog 情報の書き込みを有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog file**

ステップ 7 メッセージが記録されるファイルの名前を指定します。 ファイル名は 16 文字まで入力できます。
Firepower-chassis /monitoring # **set syslog file name***filename*

ステップ 8 （任意） ファイルに保存するメッセージの最低レベルを選択します。 ファイルの状態がイネーブルの場合、システムはそのレベル以上のメッセージを syslog ファイルに保存します。 レベル オプションは緊急性の降順で一覧表示されます。 デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

ステップ 9 （任意） 最新のメッセージで最も古いメッセージが上書きされる前の最大ファイル サイズ（バイト単位）を指定します。 有効な範囲は 4096 ～ 4194304 バイトです。
Firepower-chassis /monitoring # **set syslog file size***filesize*

ステップ 10 最大 3 台の外部 syslog サーバへの syslog メッセージの送信を設定します。

a) 最大 3 台の外部 syslog サーバへの syslog メッセージの送信を有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}

b) （任意） 外部ログに保存するメッセージの最低レベルを選択します。 remote-destination がイネーブルにされると、システムはそのレベル以上を外部サーバに送信します。 レベル オプションは緊急性の降順で一覧表示されます。 デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level**{**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

c) 指定したリモート syslog サーバのホスト名または IP アドレスを指定します。 ホスト名は 256 文字まで入力できます。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname***hostname*

d) （任意） 指定したリモート syslog サーバに送信される syslog メッセージに含まれるファシリティ レベルを指定します。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}

ステップ 11 ローカル送信元を設定します。 有効化またはディセーブルにするローカル送信元ごとに、次のコマンドを入力します。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}

次のいずれかになります。

- audits：すべての監査ログ イベントのロギングを有効化またはディセーブルにします。
- events：すべてのシステム イベントのロギングを有効化またはディセーブルにします。
- faults：すべてのシステム障害のロギングを有効化またはディセーブルにします。

ステップ 12 トランザクションをコミットします。
Firepower-chassis /monitoring # **commit-buffer**

次の例は、ローカル ファイルの syslog メッセージのストレージをイネーブルにし、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # disable syslog console
Firepower-chassis /monitoring* # disable syslog monitor
Firepower-chassis /monitoring* # enable syslog file
Firepower-chassis /monitoring* # set syslog file name SysMsgsFirepower
Firepower-chassis /monitoring* # set syslog file level notifications
Firepower-chassis /monitoring* # set syslog file size 4194304
Firepower-chassis /monitoring* # disable syslog remote-destination server-1
Firepower-chassis /monitoring* # disable syslog remote-destination server-2
Firepower-chassis /monitoring* # disable syslog remote-destination server-3
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。 たとえば、DNS サーバを設定していないと、Firepower シャーシで設定を行うときに、

www.cisco.com などの名前を使用できません。 サーバの IP アドレスを使用する必要があり、IPv4 または IPv6 アドレスのいずれかを使用できます。 最大 4 台の DNS サーバを設定できます。

（注） 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 DNS サーバを作成または削除するには、次の該当するコマンドを入力します。

- 指定した IPv4 または IPv6 アドレスの DNS サーバを使用するようにシステムを設定する場合：

  Firepower-chassis /system/services # **createdns***{ip-addr | ip6-addr}*

- 指定した IPv4 または IPv6 アドレスの DNS サーバを削除する場合：

  Firepower-chassis /system/services # **deletedns***{ip-addr | ip6-addr}*

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 /system/services # **commit-buffer**

次の例では、IPv4 アドレス 192.168.200.105 を持つ DNS サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IPv6 アドレス 2001:db8::22:F376:FF3B:AB3F を持つ DNS サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IP アドレス 192.168.200.105 を持つ DNS サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

第 8 章

インターフェイス管理

- Firepower 9300 インターフェイスについて，77 ページ
- インターフェイス プロパティの編集，78 ページ
- ポート チャネルの作成，78 ページ
- ブレークアウト ケーブルの設定，80 ページ

Firepower 9300 インターフェイスについて

Firepower 9300 は単一のインターフェイスだけでなく、EtherChannel（ポートチャネル）インターフェイスもサポートします。 EtherChannel インターフェイスには、同じタイプのメンバー インターフェイスを最大 16 個含めることができます。

各インターフェイスは、次のいずれかのタイプになります。

- [Data]（デフォルト）：データ インターフェイスはセキュリティ モジュール間で共有できません。
- [Management]：管理インターフェイスはセキュリティ モジュール間で共有できます。 各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。
- [Cluster]：クラスタ化された論理デバイスに使用する特別なインターフェイス タイプです。 このタイプは、ユニット間のクラスタ通信用にクラスタ制御リンクに自動的に割り当てられます。 デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。 クラスタ制御リンク用に別のポートチャネルを使用する場合は、クラスタを導入する前に、別のポートチャネルにクラスタ タイプを割り当てることができます。

インターフェイス プロパティの編集

手順

ステップ 1 インターフェイス モードを開始します。
scopeeth-uplink
scope fabric a

ステップ 2 インターフェイスをイネーブルにします。
enterinterface*interface_id*

イネーブル化

ステップ 3 （任意）インターフェイス タイプを設定します。
setport-type {**data** | **mgmt** | **cluster**}

例：

```
9300 /eth-uplink/fabric/interface # set port-type mgmt
```

data キーワードがデフォルトのタイプです。 **cluster** キーワードは選択しないでください。

ステップ 4 （任意）インターフェイス速度を設定します。
setspeed {**10gbps** | **1gbps**}

例：

```
9300 /eth-uplink/fabric/interface* # set speed 1gbps
```

ステップ 5 設定をコミットします。
commit-buffer

ポート チャネルの作成

EtherChannel（別名ポートチャネル）は、同じタイプの最大 16 のメンバ インターフェイスを含めることができます。

はじめる前に

Firepower アプライアンスは、Active Link Aggregation Control Protocol（LACP）モードの EtherChannel のみをサポートします。 最適な互換性を得るために、接続スイッチ ポートをアクティブ モードに設定することを推奨します。

手順

ステップ 1 インターフェイス モードを開始します。
scopeeth-uplink
scope fabric a

ステップ 2 ポートチャネルを作成します。
createport-channel*id*
イネーブル化

ステップ 3 メンバ インターフェイスを割り当てます。
createmember-port*interface_id*

例：

```
9300 /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
9300 /eth-uplink/fabric/port-channel/member-port* # exit
9300 /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
9300 /eth-uplink/fabric/port-channel/member-port* # exit
9300 /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
9300 /eth-uplink/fabric/port-channel/member-port* # exit
9300 /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
9300 /eth-uplink/fabric/port-channel/member-port* # exit
```

ステップ 4 （任意）インターフェイス タイプを設定します。
setport-type {**data** | **mgmt** | **cluster**}

例：

```
9300 /eth-uplink/fabric/port-channel # set port-type mgmt
```

data キーワードがデフォルトのタイプです。 デフォルトの代わりにこのポートチャネルをクラスタ制御リンクとして使用する場合以外は、**cluster** キーワードを選択しないでください。

ステップ 5 （任意）ポートチャネルのすべてのメンバのインターフェイス速度を設定します。
setspeed {**10gbps** | **1gbps**}

例：

```
9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
```

ステップ 6 設定をコミットします。
commit-buffer

ブレークアウト ケーブルの設定

次の手順では、Firepower シャーシで使用するブレークアウト ケーブルを設定する方法を示します。 ブレークアウト ケーブルを使用すれば、1 つの 40 Gbps ポートの代わりに 4 つの 10 Gbps ポートを利用できます。

手順

ステップ 1 新しいブレークアウトを作成するには、次のコマンドを使用します。

a) ケーブル接続モードを開始します。
scopecabling
scope fabric a

b) ブレークアウトを作成します。
createbreakout*epm_slotport*

例：

```
9300 /cabling/fabric/ # create breakout 2 1
```

c) 設定をコミットします。
commit-buffer

これにより自動リブートが実行されます。 複数のブレークアウトを設定する場合、commit-buffer コマンドを発行する前にそれらすべてを作成する必要があります。

ステップ 2 ブレークアウト ポートの有効化および設定を行うには、次のコマンドを使用します。

a) インターフェイス モードを開始します。
scopeeth-uplink

scopefabrica

scopeaggr-interface*epm_slotport*

b) インターフェイス速度およびポート タイプを設定するには、**set** コマンドを使用します。
インターフェイスの管理状態を設定するには、**enable** または **disable** コマンドを使用します。

c) 設定をコミットします。
commit-buffer

第 9 章

論理デバイス

- 論理デバイスについて，81 ページ
- スタンドアロン ASA 論理デバイスの作成，82 ページ
- クラスタの導入，84 ページ
- セキュリティ モジュールのコンソールへの接続，89 ページ

論理デバイスについて

論理デバイスを作成すると、Firepower アプライアンス スーパーバイザは指定されたバージョンのソフトウェアをダウンロードし、指定されたセキュリティ モジュール（クラスタの場合は、Firepower シャーシにインストールされたすべてのセキュリティ モジュール）にブートストラップコンフィギュレーションと管理インターフェイスの設定をプッシュすることで論理デバイスを展開します。

論理デバイスは次の 2 つのタイプのいずれかを作成できます。

（注） 作成できる論理デバイスのタイプは、どちらか一方のみです。 つまり、3 つのセキュリティ モジュールがインストールされている場合でも、1 つのセキュリティ モジュールでスタンドアロン論理デバイスを作成し、残り 2 つの論理デバイスを使用してクラスタを作成する、といったことはできません。

- スタンドアロン：Firepower シャーシに取り付けた各セキュリティ モジュールに、スタンドアロン論理デバイスを作成できます。
- クラスタ：ここで作成できるクラスタでは、Firepower シャーシにインストールされているすべてのセキュリティ モジュールが 1 つの論理デバイスとしてグループ化されます。 クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

スタンドアロン ASA 論理デバイスの作成

クラスタを設定していない場合は、Firepower シャーシに取り付けた各セキュリティ モジュールにスタンドアロン論理デバイスを作成できます。 クラスタを設定している場合は、スタンドアロンデバイスを設定する前に、クラスタを削除する必要があります。

はじめる前に

- 論理デバイスに使用するセキュリティ モジュールに、すでに論理デバイスが設定されている場合は、まず既存の論理デバイスを削除してください（論理デバイスの削除を参照）。
- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロード, （38 ページ）を参照）、そのイメージを Firepower アプライアンスに（ダウンロード）します（論理デバイス ソフトウェア イメージの Firepower アプライアンス へのダウンロード, （40 ページ）を参照）。
- 論理デバイスで使用する管理インターフェイスを設定します。

手順

ステップ 1 セキュリティ サービス モードを開始します。
Firepower# **scopessa**

ステップ 2 論理デバイスを作成します。
Firepower /ssa # **createlogical-device***device_name***asa***slot_id***standalone**

ステップ 3 論理デバイスの説明を入力します。
Firepower /ssa/logical-device* # **setdescription***"logical device description"*

ステップ 4 管理およびデータ インターフェイスを論理デバイスに割り当てます。
Firepower /ssa/logical-device* # **createexternal-port-link***nameinterface_name***asa**
Firepower-chassis /ssa/logical-device/external-port-link* # **exit**

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。
Firepower /ssa/logical-device* # **createmgmt-bootstrapasa**

b) 有効化パスワードを作成します。
Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-key-secretPASSWORD**

c) パスワード値を設定します。
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **setvalue**
Value: *password*

d) パスワード設定スコープを終了します。
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **exit**

e) 管理 IP アドレスを設定します。
Firepower /ssa/logical-device/mgmt-bootstrap* # **createipv4***slot_id***default**

f) ゲートウェイ アドレスを設定します。
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setgateway***gateway_address*

g) IP アドレスとマスクを設定します。
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setip***ip_address***mask***network_mask*

h) 管理 IP 設定スコープを終了します。
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **exit**

i) 管理ブートストラップ設定スコープを終了します。
Firepower /ssa/logical-device/mgmt-bootstrap* # **exit**

ステップ 6 設定をコミットします。
commit-buffer

トランザクションをシステムの設定にコミットします。

例

```
Firepower# scope ssa
Firepower /ssa # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # set description "logical device description"
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: <password>
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 1.1.1.254
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 1.1.1.1 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* # show configuration pending
+enter logical-device MyDevice1 asa 1 standalone
+    enter external-port-link inside Ethernet1/1 asa
+        set decorator ""
+        set description "inside link"
+    exit
+    enter external-port-link management Ethernet1/7 asa
+        set decorator ""
+        set description "management link"
+    exit
+    enter external-port-link outside Ethernet1/2 asa
+        set decorator ""
+        set description "external link"
+    exit
+    enter mgmt-bootstrap asa
+        enter bootstrap-key-secret PASSWORD
+            set value
+        exit
+        enter ipv4 1 default
+            set gateway 1.1.1.254
+            set ip 1.1.1.1 mask 255.255.255.0
+        exit
```

```
+    exit
+    set description "logical device description"
+exit
Firepower /ssa/logical-device* # commit-buffer
```

クラスタの導入

クラスタリングを利用すると、シャーシのすべてのセキュリティ モジュールを 1 つの論理デバイスとしてグループ化できます。 クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供すると同時に、複数デバイスの高いスループットおよび冗長性を実現します。クラスタリングは、ASA セキュリティ モジュールに対してのみ利用できます。

（注） Firepower 9300 は複数のシャーシにまたがる（シャーシ間）クラスタをサポートしません。シャーシ内クラスタリングのみがサポートされます。

クラスタリングについて

クラスタは、1 つのユニットとして機能する複数のセキュリティ モジュールから構成されます。Firepower 9300 にクラスタを導入すると、以下の処理が実行されます。

- セキュリティ モジュール間の通信のため、クラスタ制御リンクを作成します。 このリンクは、Firepower 9300 のクラスタ通信用バックプレーンを使用します。
- すべてのセキュリティ モジュールに、アプリケーション内でクラスタ ブートストラップ構成を作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各セキュリティ モジュールに対して、最小限のブートストラップ構成が Firepower 9300 スーパーバイザからプッシュされます。 クラスタリング環境をカスタマイズする場合、ブートストラップ コンフィギュレーションの一部は、セキュリティ モジュール内でユーザが設定できます。
- スパンされた EtherChannel として、クラスタにデータ インターフェイスを割り当てます。

  Firepower 9300 スーパーバイザは、スパンされた EtherChannel のトラフィックをすべてのセキュリティ モジュール間で負荷分散を行います。

  （注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。
- すべてのセキュリティ モジュールで共有する個別の管理インターフェイスを割り当てます。

クラスタリングの詳細と、クラスタリングがセキュリティモジュール レベルで動作する仕組みについては、セキュリティ モジュール アプリケーションのクラスタリングの章を参照してください。 ここでは、クラスタリングの概念と実装について詳しく説明します。

マスターおよびスレーブ ユニットの役割

クラスタ内のメンバの 1 つがマスター ユニットです。 マスター ユニットは自動的に決定されます。 他のすべてのメンバはスレーブ ユニットです。

すべてのコンフィギュレーション作業は、マスター ユニット上のみで実行する必要があります。 コンフィギュレーションは、スレーブ ユニットに複製されます。

クラスタ制御リンク

クラスタ制御リンクは、メンバインターフェイスを使用せずに、48 番のポートチャネルインターフェイスを使用して自動的に作成されます。 このクラスタ タイプの EtherChannel では、シャーシ内クラスタリングのクラスタ通信に Firepower 9300 のバックプレーンを使用します。 その後、シャーシ間クラスタリングがサポートされると、外部接続用としてこの EtherChannel にメンバーインターフェイスを追加できるようになります。 48 番のポートチャネル インターフェイスを使用しない場合は、代わりにクラスタ タイプの EtherChannel を事前設定することで、クラスタ制御リンクとして使用できます。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

管理インターフェイス

クラスタに管理タイプのインターフェイスを割り当てることができます。 このインターフェイスはスパンド EtherChannel ではなく、特別な個別インターフェイスです。 管理インターフェイスによって各ユニットに直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。 アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカル アドレスを使用できるようにします。 このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。 ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在のマスターユニットに関連付けられています。 個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

クラスタリングのガイドライン

- 冗長性を持たせるため、EtherChannel を VSS または vPC に接続することを推奨します。
- 一部のシャーシ セキュリティ モジュールをクラスタ化して、別のセキュリティ モジュールをスタンドアロン モードで実行することはできません。すべてのセキュリティ モジュールをクラスタに含める必要があります。

クラスタリングのデフォルト

他のクラスタ タイプのインターフェイスが定義されていない場合、クラスタ制御リンクは 48 番のポートチャネルを使用します。

ASA クラスタリングの設定

Firepower 9300 スーパーバイザから簡単にクラスタを導入できます。 すべての初期設定が各ユニットに自動的に生成されます。

手順

ステップ 1 クラスタを導入する前に、少なくとも 1 つのデータ タイプのインターフェイスまたは EtherChannel（別名ポート チャネル）を設定します。 ポート チャネルの作成, （78 ページ）を参照してください。
導入後にクラスタにデータ インターフェイスを追加することもできます。

ステップ 2 管理タイプのインターフェイスまたは EtherChannel を追加します。 ポート チャネルの作成, （78 ページ）またはインターフェイス プロパティの編集, （78 ページ）を参照してください。

ステップ 3 クラスタを作成します。
scope ssa
enter logical-device *device_name* **asa "1,2,3" clustered**

device_name は、Firepower 9300 スーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタ名ではありません。 まだハードウェアをインストールしていなくても、3 つのセキュリティ モジュールすべてを指定する必要があります。

ステップ 4 クラスタ パラメータを設定します。
enter cluster-bootstrap

ステップ 5 セキュリティ モジュール設定のクラスタ グループ名を設定します。
set service-type*cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

ステップ 6 クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

ステップ 7 （任意）管理 IP アドレス情報を設定します。
この情報は、セキュリティ モジュール設定で管理インターフェイスを設定するために使用されます。

a) ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタ ユニットに割り当てられます。
set ipv4 pool *start_ip end_ip*

set ipv6 pool *start_ip end_ip*

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。 クラスタを拡張する予定の場合は、アドレスを増やします。 現在のマスター ユニットに属する仮想 IP アドレス（メイン クラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

b) 管理インターフェイスのメイン クラスタ IP アドレスを設定します。
set virtual ipv4 *ip_address* **mask** *mask*

set virtual ipv6 *ip_address* **prefix-length** *prefix*

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

c) ネットワーク ゲートウェイ アドレスを入力します。
set ipv4 gateway *ip_address*

set ipv6 gateway *ip_address*

ステップ 8 シャーシ ID を設定します。
set chassis-id*id*

ステップ 9 クラスタ制御リンクの制御トラフィックの認証キーを設定します。
set key*secret*

共有秘密は、1 ～ 63 文字の ASCII 文字列です。 共有秘密は、キーを生成するために使用されます。 このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 10 クラスタ ブートストラップ モードを終了します。
exit

ステップ 11 クラスタに管理およびデータ インターフェイスを割り当てます。
enter external-port-link*9300_interface_id asa_interface_id***asa**
exit

例：

```
enter external-port-link Port-channel1 Port-channel1 asa
  exit
```

```
enter external-port-link Port-channel2 Port-channel2 asa
  exit
enter external-port-link Port-channel3 Port-channel3 asa
  exit
```

ステップ 12 設定をコミットします。
commit-buffer

Firepower 9300 スーパーバイザは、デフォルトのセキュリティ モジュール ソフトウェア バージョンをダウンロードし、各セキュリティ モジュールにクラスタ ブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを導入します。

ステップ 13 セキュリティ モジュールに接続してクラスタリング設定をカスタマイズします。

例

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    exit
  exit
commit buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key f@rscape
      set mode spanned-etherchannel
```

```
    set service-type cluster1
    set virtual ipv4 10.1.1.1 mask 255.255.255.0
    set virtual ipv6 2001:DB8::1 prefix-length 64
    exit
  enter external-port-link Port-channel1 Port-channel1 asa
    exit
  enter external-port-link Port-channel1 Port-channel2 asa
    exit
  enter external-port-link Port-channel1 Port-channel3 asa
    exit
  enter external-port-link Port-channel1 Port-channel4 asa
    exit
  commit-buffer
```

クラスタリングの履歴

機能名	プラットフォームリリース	機能情報
Cisco ASA のシャーシ内クラスタリング	1.1(1)	Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できます。 次のコマンドが導入されました。**enter cluster-bootstrap**、**enter logical-device clustered**、**set chassis-id**、**set ipv4 gateway**、**set ipv4 pool**、**set ipv6 gateway**、**set ipv6 pool**、**set key**、**set mode spanned-etherchannel**、**set port-type cluster**、**set service-type**、**set virtual ipv4**、**set virtual ipv6**

セキュリティ モジュールのコンソールへの接続

次の手順を使用してセキュリティ モジュールのコンソールに接続します。

（注） コンソールへのアクセスで問題が発生する場合は、別の SSH クライアントを試すか、SSH クライアントを新しいバージョンにアップグレードすることを推奨します。

手順

ステップ 1 セキュリティ モジュールのコンソールに接続するには、次の手順を実行します。

a) FXOS CLI からセキュリティ モジュールに接続します。
Firepower-chassis # **connectmodule***slot_number***console**

セキュリティ モジュールに初めて接続すると、FXOS モジュール CLI にアクセスします。

b) モジュール OS に接続するには、を入力します。
Firepower-module1>**connect asa**

FXOS CLI のスーパーバイザ レベルからセキュリティ モジュールへの以降の接続では、モジュール OS に直接アクセスします。

ステップ 2 （任意） Ctrl+A+D キーを押し、モジュール OS コンソールを終了して FXOS モジュール CLI に移動します。
トラブルシューティングのために FXOS モジュール CLI にアクセスする場合があります。

ステップ 3 FXOS CLI のスーパーバイザ レベルに戻ります。

a) セキュリティ モジュール コンソールを終了するには、~ を入力します。
Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。
telnet>**quit**

例

次の例では、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパーバイザ レベルに戻ります。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

索 引

A

AAA 62, 63, 66, 67, 69, 70, 71
- LDAP プロバイダー 62, 63, 66
- RADIUS プロバイダー 67, 69
- TACACS+ プロバイダー 69, 70, 71

asa 42, 82, 86, 89
- イメージ バージョンの更新 42
- クラスタ化の作成 86
- クラスタの作成 86
- スタンドアロン ASA 論理デバイスの作成 82
- 接続 89
- 接続の終了 89

ASA イメージ 37, 38, 40
- Cisco.com からのダウンロード 38
- Firepower 9300 へのダウンロード 40
- 概要 37

authNoPriv 54
authPriv 54

C

call home 18
- HTTP プロキシの設定 18

Cisco Secure Package 37, 38, 40
- Cisco.com からのダウンロード 38
- Firepower 9300 へのダウンロード 40
- 概要 37

CLI。参照先： コマンドライン インターフェイス
CLI セッション制限 8
CSP。参照先： Cisco Secure Package

D

DNS 73

F

Firepower 9300 1
- 概要 1

Firepower eXtensible OS 39
- プラットフォーム バンドルのアップグレード 39

Firepower シャーシ 10
- 初期設定 10

Firepower プラットフォーム バンドル 37, 38, 39
- Cisco.com からのダウンロード 38
- Firepower 9300 へのダウンロード 38
- アップグレード 39
- 概要 37

H

HTTPS 60
- ポートの変更 60

HTTP プロキシ 18
- 設定 18

L

LDAP 62, 63, 66
LDAP プロバイダー 63, 66
- 削除 66
- 作成 63

license authority 19

N

noAuthNoPriv 54
NTP 47, 49
- 削除 49
- 設定 47
- 追加 49

R

RADIUS 67, 69
RADIUS プロバイダー 67, 69
　削除 69
　作成 67

S

smart call home 18
　HTTP プロキシの設定 18
SNMP 52, 53, 54, 55, 56, 57, 58, 59, 60
　イネーブル化 56
　概要 52
　権限 54
　community 56
　サポート 52, 55
　セキュリティ レベル 54
　通知 53
　トラップ 57, 58
　　削除 58
　　作成 57
　バージョン 3 のセキュリティ機能 55
　users 59, 60
　　削除 60
　　作成 59
SNMPv3 55
　セキュリティ機能 55
SSH 51
　設定 51
syslog 71
　リモート宛先の設定 71
　ローカル宛先の設定 71
　ローカル送信元の設定 71

T

TACACS+ 69, 70, 71
TACACS+ プロバイダー 70, 71
　削除 71
　作成 70
Telnet 51
　設定 51

あ

アカウント 26, 30, 31, 35
　ローカル認証された 26, 30, 31, 35

い

イネーブル化 56
　SNMP 56
イメージ 37, 38, 39, 40
　Cisco.com からのダウンロード 38
　Firepower 9300 へのダウンロード 38, 40
　Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード 39
　管理 37
イメージ バージョン 42
　更新 42
インターフェイス 78
　設定 78
　プロパティ 78
informs 53
　概要 53

お

オブジェクト コマンド 5

か

管理 IP アドレス[かんりIPあどれす] 45
　変更 45
管理対象オブジェクト 3

く

クラスタ 84, 86
　概要 84
　作成 86
　作成時のデフォルト 86

こ

高レベルのタスク リスト 9

コマンド 7
history 7
コマンド モード 4
コマンドライン インターフェイス 12
アクセス 12
コマンドライン インターフェイスへのアクセス 12
コミュニティ、SNMP 56

し

time 50
手動設定 50
system 10
初期設定 10
chassis 10
初期設定 10
初期設定 10

た

タイムゾーン 47, 50
設定 47, 50
タスク フロー 9

つ

通信サービス 56
SNMP 56

と

トラップ 53, 57, 58
概要 53
削除 58
作成 57

に

日時 47
設定 47
認証 27
デフォルト 27

は

パスワード 26, 29
強度チェック 29
変更間隔 26
履歴カウント 26
パスワード強度の適用 29
パスワード プロファイル 26, 30, 31, 35
概要 26
パスワード履歴カウント 31
パスワード履歴のクリア 35
変更間隔 30
変更禁止間隔 31

ひ

date 50
手動設定 50

ふ

プラットフォーム バンドル 37, 38, 39
Cisco.com からのダウンロード 38
Firepower 9300 へのダウンロード 38
アップグレード 39
概要 37
ブレークアウト ケーブル 80
設定 80
ブレークアウト ポート 80
プロファイル 26
password 26

ほ

ポート チャネル 78
設定 78
ポリシー 28
リモート ユーザのロール 28
保留コマンド 7

ゆ

users 8, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 59, 60
CLI セッション制限 8
SNMP 59, 60

users *(続き)*
アクティブ化 **34**
管理 **23**
削除 **34**
作成 **32**
デフォルト認証 **27**
デフォルト ロール **25**
パスワード強度チェック **29**
非アクティブ化 **34**
リモート、ロール ポリシー **28**
ローカル認証された **26, 30, 31, 35**
ユーザ アカウント **26, 30, 31, 35**
パスワード プロファイル **26, 30, 31, 35**

ら

license **19**
registering **19**
ライセンスの登録 **19**

り

リモート ユーザのロール ポリシー **28**
履歴、パスワード **26**

ろ

ローカル認証されたユーザ **26, 30, 31, 35**
パスワード プロファイル **26**
パスワード履歴カウント **31**
パスワード履歴のクリア **35**
変更間隔 **30**
変更禁止間隔 **31**
論理デバイス **42, 81, 82, 86, 89**
イメージ バージョンの更新 **42**
クラスタの作成 **86**
スタンドアロンの作成 **82**
接続 **89**
接続の終了 **89**
説明 **81**
論理デバイス接続の終了 **89**
論理デバイスへの接続 **89**