プラットフォーム設定

日時の設定

日付と時刻を手動で設定したり、現在のシステム時刻を表示するには、下記で説明する [NTP] ページの システムのネットワーク タイム プロトコル（NTP）を設定します。

NTP の設定は、Firepower 4100/9300 シャーシとシャーシにインストールされている論理デバイス間で自動的に同期されます。

（注）

Firepower 4100/9300 シャーシに Firepower Threat Defense を導入すると、スマート ライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように Firepower 4100/9300 シャーシに NTP を設定する必要があります。Firepower 4100/9300 シャーシと Firepower Management Center に同じ NTP サーバを使用する必要があります。

NTP を使用すると、[Current Time] タブの全体的な同期ステータスを表示できます。または、[Time Synchronization] タブの [NTP Server] テーブルの [Server Status] フィールドを見ると、設定済みの各 NTP サーバの同期ステータスを表示できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

設定された日付と時刻の表示

手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Current Time] タブをクリックします。
システムは、デバイスに設定された日付、時刻、タイム ゾーンを表示します。

NTP を使用している場合、[Current Time] タブに総合的な同期ステータスを表示することもできます。設定済みの各 NTP サーバの同期ステータスは、[Time Synchronization] タブにある NTP サーバ テーブルの [Server Status] フィールドを見て確認できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

タイム ゾーンの設定

手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Current Time] タブをクリックします。

ステップ 3 [Time Zone] ドロップダウン リストから、Firepower シャーシの適切なタイム ゾーンを選択します。

NTP を使用した日付と時刻の設定

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。最大 4 台の NTP サーバを設定できます。

手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Time Synchronization] タブをクリックします。

ステップ 3 [Set Time Source] で、[Use NTP Server] をクリックします。

ステップ 4 使用する NTP サーバ（最大 4 台）ごとに、それぞれの IP アドレスまたはホスト名を [NTP Server] フィールドに入力し、[Add] をクリックします。

ステップ 5 [Save] をクリックします。
Firepower シャーシが、指定した NTP サーバ情報で設定されます。

各サーバの同期ステータスは、NTP サーバ テーブルの [Server Status] フィールドを見て確認できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

（注） システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

NTP サーバの削除

手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Time Synchronization] タブをクリックします。

ステップ 3 削除する各 NTP サーバに対して、NTP サーバ テーブルでそのサーバの [Delete] アイコンをクリックします。

ステップ 4 [Save] をクリックします。

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。

手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Time Synchronization] タブをクリックします。

ステップ 3 [Set Time Source] で [Set Time Manually] をクリックします。

ステップ 4 [Date] ドロップダウン リストをクリックしてカレンダーを表示し、カレンダーで使用できるコントロールを使って日付を設定します。

ステップ 5 時、分、および AM/PM のそれぞれのドロップダウン リストを使用して時間を指定します。

ヒント [Get System Time] をクリックすると、Firepower Chassis Manager への接続に使用しているシステムの設定に合わせて日付と時刻を設定することができます。

ステップ 6 [Save] をクリックします。
指定した日付と時刻が Firepower シャーシに設定されます。

（注） システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効または無効にする方法、および FXOS シャーシを SSH クライアントとして有効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 [Platform Settings] > [SSH] > [SSH Server] を選択します。

ステップ 2 Firepower シャーシへの SSH アクセスを有効化するには、[Enable SSH] チェックボックスをオンにします。SSH アクセスをディセーブルにするには、[Enable SSH] チェックボックスをオフにします。

ステップ 3 サーバの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

（注） コモン クライテリアでは 3des-cbc がサポートされていません。FXOS シャーシでコモン クライテリア モードが有効な場合、暗号化アルゴリズムとして 3des-cbc を使用することはできません。

ステップ 4 サーバの [Key Exchange Algorithm] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換は署名とホスト キーを組み合わせてホスト認証を提供します。この

キー交換方式により、明示的なサーバ認証が可能となります。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 5 サーバの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 6 サーバの [Host Key] について、RSA キー ペアのモジュラス サイズを入力します。
モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

ステップ 7 サーバの [Volume Rekey Limit] に、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 8 サーバの [Time Rekey Limit] について、FXOS がセッションを切断するまでに SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 9 [Save] をクリックします。

ステップ 10 [SSH Client] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。

ステップ 11 [Strict Host Keycheck] について、[enable]、[disable]、または [prompt] を選択して、SSH ホスト キー チェックを制御します。

- [enable]：FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。 FXOS CLI でシステム スコープまたはサービス スコープの enter ssh-host コマンドを使用して、手動でホストを追加する必要があります。
- prompt：シャーシにまだ保存されていないホストキーを許可または拒否するように求められます。
- disable：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

ステップ 12 クライアントの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

（注） コモン クライテリアでは 3des-cbc がサポートされていません。FXOS シャーシでコモン クライテリア モードが有効な場合、暗号化アルゴリズムとして 3des-cbc を使用することはできません。

ステップ 13 クライアントの [Key Exchange Algorithm] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換は署名とホスト キーを組み合わせてホスト認証を提供します。

このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 14 クライアントの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 15 クライアントの [Volume Rekey Limit] に、FXOS がセッションを切断する前にその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 16 クライアントの [Time Rekey Limit] について、FXOS がセッションを切断するまでに SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 17 [Save] をクリックします。

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

Firepower シャーシに簡易ネットワーク管理プロトコル（SNMP）を設定するには、[SNMP] ページを使用します。詳細については、次のトピックを参照してください。

SNMP の概要

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、選択したセキュリティ レベルと結合され、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を表示するために必要な特権を決定します。権限レベルは、メッセージが開示されないよう保護または認証の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、セキュリティ モデルが設定されているか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 *1* : ***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	未対応	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	未対応	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	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	なし	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 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 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] チェックボックス	SNMP が有効化かディセーブルか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。

名前	説明
[Port] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。
[Community/Username] フィールド	SNMP v1 および v2 のポーリングに使用するコミュニティ文字列。 このフィールドはSNMP v3には適用されないことに注意してください。 1～32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは public です。 [Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ることに注意してください。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。
[System Administrator Name] フィールド	SNMP 実装の担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 510 文字の英数字文字列を入力します。

ステップ 3 [Save] をクリックします。

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 [Platform Settings] > [SNMP] を選択します。
ステップ 2 [SNMP Traps] 領域で、[Add] をクリックします。
ステップ 3 [Add SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[Community/Username] フィールド	Firepower シャーシが SNMP ホストに送信するトラップに含める SNMP v1 または v2 コミュニティ名あるいは SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1～32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	Firepower シャーシが SNMP ホストとのトラップの通信に使用するポート。 1 ～ 65535 の整数を入力します。
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • V1 • V2 • V3
[Type] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 • Traps • nforms
[v3 Privilege] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

ステップ 4 [OK] をクリックして、[Add SNMP Trap] ダイアログボックスを閉じます。

ステップ 5 [Save] をクリックします。

SNMP トラップの削除

手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Traps] 領域で、削除するトラップに対応するテーブルの行の [Delete] アイコンをクリックします。

SNMPv3 ユーザの作成

手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Users] 領域で、[Add] をクリックします。

ステップ 3 [Add SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。
[Auth Type] フィールド	許可タイプ：[SHA]。
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。
[Password] フィールド	このユーザのパスワード。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Privacy Password] フィールド	このユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 4 [OK] をクリックして、[Add SNMP User] ダイアログボックスを閉じます。

ステップ 5 [Save] をクリックします。

SNMPv3 ユーザの削除

手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Users] 領域で、削除するユーザに対応するテーブルの行の [Delete] アイコンをクリックします。

HTTPS の設定

ここでは、Firepower 4100/9300 シャーシ で HTTPS を設定する方法を説明します。

（注） Firepower Chassis Manager または FXOS CLI を使用して HTTPS ポートを変更できます。他の HTTPS の設定はすべて、FXOS CLI を使用してのみ設定できます。

証明書、キー リング、トラスト ポイント

HTTPS は、公開キー インフラストラクチャ（PKI）を使用してクライアントのブラウザと Firepower 4100/9300 シャーシなどの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。一般的に、短いキーよりも長いキーの方がセキュアになります。FXOS では、最初に 2048 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキー ペアと独自の自己署名証明書を生成できます。リモート ユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、FXOS にはデフォルトのキー リングからの公開キーを含む組み込み用自己署名証明書が含まれます。

トラスト ポイント

FXOS に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース（つまり、トラスト ポイント）からサードパーティ証明書を取得し、インストールできます。サードパーティ証明書は、発行元トラスト ポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラストチェーンの一部となるトラストアンカーのいずれか）によって署名されます。新しい証明書を取得するには、FXOS で証明書要求を生成し、トラスト ポイントに要求を送信する必要があります。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

キー リングの作成

FXOS は、デフォルト キー リングを含め、最大 8 個のキー リングをサポートします。

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 キー リングを作成し、名前を付けます。
Firepower-chassis # **createkeyring** *keyring-name*

ステップ 3 SSL キーのビット長を設定します。
Firepower-chassis # **setmodulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}

ステップ 4 トランザクションをコミットします。
Firepower-chassis # **commit-buffer**

次の例は、1024 ビットのキー サイズのキー リングを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

次の作業

このキー リングの証明書要求を作成します。

デフォルト キー リングの再生成

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

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 デフォルト キー リングでキー リング セキュリティ モードに入ります。
Firepower-chassis /security # **scopekeyring default**

ステップ 3 デフォルト キー リングを再生成します。
Firepower-chassis /security/keyring # **setregenerate yes**

ステップ 4 トランザクションをコミットします。
Firepower-chassis # **commit-buffer**

次に、デフォルト キー リングを再生成する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

キー リングの証明書要求の作成

基本オプション付きのキー リングの証明書要求の作成

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 キー リングのコンフィギュレーション モードに入ります。
Firepower-chassis /security # **scope keyring** *keyring-name*

ステップ 3 指定された IPv4 または IPv6 アドレス、またはファブリック インターコネクトの名前を使用して証明書要求を作成します。証明書要求のパスワードを入力するように求められます。
Firepower-chassis /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}

ステップ 4 トランザクションをコミットします。
Firepower-chassis /security/keyring/certreq # **commit-buffer**

ステップ 5 コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。
Firepower-chassis /security/keyring # **show certreq**

次の例では、基本オプション付きのキーリングについてIPv4アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

次の作業

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キー リングの証明書を取得するため、証明書要求を含むファイルをトラスト アンカーまたは認証局に送信します。
- トラスト ポイントを作成し、トラスト アンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

詳細オプション付きのキー リングの証明書要求の作成

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 キー リングのコンフィギュレーション モードに入ります。
Firepower-chassis /security # **scope keyring** *keyring-name*

ステップ 3 証明書要求を作成します。
Firepower-chassis /security/keyring # **createcertreq**

ステップ 4 会社が存在している国の国コードを指定します。
Firepower-chassis /security/keyring/certreq* # **set country** *country name*

ステップ 5 要求に関連付けられたドメイン ネーム サーバ（DNS）アドレスを指定します。
Firepower-chassis /security/keyring/certreq* # **set dns** *DNS Name*

ステップ 6 証明書要求に関連付けられた電子メール アドレスを指定します。
Firepower-chassis /security/keyring/certreq* # **set e-mail** *E-mail name*

ステップ 7 Firepower 4100/9300 シャーシの IP アドレスを指定します。
Firepower-chassis /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }

ステップ 8 証明書を要求している会社の本社が存在する市または町を指定します。
Firepower-chassis /security/keyring/certreq* # **set locality** *locality name (eg, city)*

ステップ 9 証明書を要求している組織を指定します。
Firepower-chassis /security/keyring/certreq* # **set org-name** *organization name*

ステップ 10 組織ユニットを指定します。
Firepower-chassis /security/keyring/certreq* # **set org-unit-name** *organizational unit name*

ステップ 11 証明書要求に関するオプションのパスワードを指定します。
Firepower-chassis /security/keyring/certreq* # **set password** *certificate request password*

ステップ 12 証明書を要求している会社の本社が存在する州または行政区分を指定します。
Firepower-chassis /security/keyring/certreq* # **set state** *state, province or county*

ステップ 13 Firepower 4100/9300 シャーシ の完全修飾ドメイン名を指定します。
Firepower-chassis /security/keyring/certreq* # **set subject-name** *certificate request name*

ステップ 14 トランザクションをコミットします。
Firepower-chassis /security/keyring/certreq # **commit-buffer**

ステップ 15 コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。
Firepower-chassis /security/keyring # **show certreq**

次の例では、詳細オプション付きのキーリングについてIPv4アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* #  set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bgl-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #
```

次の作業

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キー リングの証明書を取得するため、証明書要求を含むファイルをトラスト アンカーまたは認証局に送信します。
- トラスト ポイントを作成し、トラスト アンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

トラスト ポイントの作成

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 トラストポイントを作成します。
Firepower-chassis /security # **createtrustpoint** *name*

ステップ 3 このトラスト ポイントの証明書情報を指定します。
Firepower-chassis /security/trustpoint # **setcertchain** [*certchain*]

コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラスト ポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、ENDOFBUF と入力して終了します。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ 4 トランザクションをコミットします。
Firepower-chassis /security/trustpoint # **commit-buffer**

次の例は、トラスト ポイントを作成し、トラスト ポイントに証明書を提供します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

次の作業

トラスト アンカーまたは認証局からキー リング証明書を取得し、キー リングにインポートします。

キー リングへの証明書のインポート

はじめる前に

- キー リング証明書の証明書チェーンを含むトラスト ポイントを設定します。
- トラスト アンカーまたは認証局からキー リング証明書を取得します。

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 証明書を受け取るキー リングでコンフィギュレーション モードに入ります。
Firepower-chassis /security # **scopekeyring** *keyring-name*

ステップ 3 キー リング証明書の取得元のトラスト アンカーまたは認証局に対しトラスト ポイントを指定します。
Firepower-chassis /security/keyring # **settrustpoint** *name*

ステップ 4 キー リング証明書を入力してアップロードするためのダイアログを起動します。
Firepower-chassis /security/keyring # **setcert**

プロンプトで、トラスト アンカーまたは認証局から受け取った証明書のテキストを貼り付けます。証明書の次の行に ENDOFBUF と入力して、証明書の入力を完了します。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ 5 トランザクションをコミットします。
Firepower-chassis /security/keyring # **commit-buffer**

次に、トラストポイントを指定し、証明書をキー リングにインポートする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

次の作業

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

注意 HTTPS で使用するポートとキー リングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

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 サービスを有効にします。
Firepower-chassis /system/services # **enable https**

ステップ 4 （任意） HTTPS 接続で使用されるポートを指定します。
Firepower-chassis /system/services # **set https port** *port-num*

ステップ 5 （任意） HTTPS に対して作成したキー リングの名前を指定します。
Firepower-chassis /system/services # **set https keyring** *keyring-name*

ステップ 6 （任意） ドメインで使用される暗号スイート セキュリティのレベルを指定します。
Firepower-chassis /system/services # **set https cipher-suite-mode** *cipher-suite-mode*

cipher-suite-mode には、以下のいずれかのキーワードを指定できます。

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom**：ユーザ定義の暗号スイート仕様の文字列を指定できます。

ステップ 7 （任意） **cipher-suite-mode** が **custom** に設定されている場合は、ドメインに対してカスタム レベルの暗号スイート セキュリティを指定します。
Firepower-chassis /system/services # **set https cipher-suite** *cipher-suite-spec-string*

cipher-suite-spec-string は最大 256 文字で構成できます。これは OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。!（感嘆符）、+（プラス記号）、-（ハイフン）、および :（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite を参照してください。

たとえば、FXOS がデフォルトとして使用する中強度仕様の文字列は次のようになります：
ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

（注） このオプションは、**cipher-suite-mode** が [custom]**custom**以外に設定されている場合は無視されます。

ステップ 8 （任意） 証明書失効リスト検査を、有効または無効にします。
setrevoke-policy *{ relaxed | strict }*

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

次の例では、HTTPS をイネーブルにし、ポート番号を 443 に設定し、キー リング名を kring7984 に設定し、暗号スイートのセキュリティ レベルを [high] 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 # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

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 [Platform Settings] > [HTTPS] を選択します。

ステップ 2 HTTPS 接続に使用するポートを [Port] フィールドに入力します。1 ～ 65535 の整数を指定します。このサービスは、デフォルトでポート 443 でイネーブルになります。

ステップ 3 [Save] をクリックします。
指定した HTTPS ポートが Firepower シャーシに設定されます。

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。

キーリングの削除

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 名前付きのキー リングを削除します。
Firepower-chassis /security # **deletekeyring** *name*

ステップ 3 トランザクションをコミットします。
Firepower-chassis /security # **commit-buffer**

次の例では、キー リングを削除します。

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

トラスト ポイントの削除

はじめる前に

トラスト ポイントがキー リングによって使用されていないことを確認してください。

手順

ステップ 1 セキュリティ モードに入ります。
Firepower-chassis# **scopesecurity**

ステップ 2 指定したトラスト ポイントを削除します。
Firepower-chassis /security # **deletetrustpoint** *name*

ステップ 3 トランザクションをコミットします。
Firepower-chassis /security # **commit-buffer**

次に、トラスト ポイントを削除する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

HTTPS の無効化

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 サービスを無効にします。
Firepower-chassis /system/services # **disable https**

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、HTTPS をディセーブルにし、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 /system/services # disable https
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 4100/9300 シャーシ 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

認可

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	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。 1 ～ 60 秒の整数を入力します。デフォルト値は 30 秒です。このプロパティは必須です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。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。
[Base DN] フィールド	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。ベース DN の長さは、最大 255 文字から CN=$userid の長さを引いた長さに設定することができます。$userid により、LDAP 認証を使用して Firepower シャーシ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。 このプロパティは必須です。このタブでベース DN を指定しない場合、定義する LDAP プロバイダーごとに 1 つずつ指定する必要があります。
[Filter] フィールド	LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。 このプロパティは必須です。このタブでフィルタを指定しない場合、定義する LDAP プロバイダーごとに 1 つずつ指定する必要があります。

ステップ 4 [Save] をクリックします。

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 追加する LDAP プロバイダーごとに、次の手順を実行します。

a) [LDAP Providers] 領域で、[Add] をクリックします。

b) [Add LDAP Provider] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Hostname/FDQN (or IP Address)] フィールド	LDAP プロバイダーのホスト名または IP アドレス。SSL がイネーブルの場合、このフィールドは、LDAP データベース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。
[Order] フィールド	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。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、lowest-available または 0（ゼロ）を入力します。
[Bind DN] フィールド	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）。 サポートされるストリングの最大長は 255 文字（ASCII）です。

名前	説明
[Base DN] フィールド	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。ベース DN の長さは、最大 255 文字から CN=$userid の長さを引いた長さに設定することができます。$userid 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] タブで設定されていない場合は、この値が必要です。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリア テキストで送信されます。 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。
[Filter] フィールド	LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。 デフォルトのフィルタが [LDAP] タブで設定されていない場合は、この値が必要です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。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] タブで設定されていない場合は、この値が必要です。
[Key] フィールド	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。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。
[Confirm Key] フィールド	確認のための LDAP データベース パスワードの再入力。

名前	説明
[Timeout] フィールド	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。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [LDAP] タブで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。
[Vendor] フィールド	この選択により、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が識別されます。 • LDAP プロバイダーが Microsoft Active Directory の場合は、[MS AD] を選択します。 • LDAP プロバイダーが Microsoft Active Directory でない場合は、[Open LDAP] を選択します。 デフォルトは [Open LDAP] です。

c）[OK] をクリックして、[Add LDAP Provider] ダイアログボックスを閉じます。

ステップ 4 [Save] をクリックします。

ステップ 5 （任意）証明書失効リスト検査を有効にします。
Firepower-chassis /security/ldap/server # **set revoke-policy** *{strict | relaxed}*

（注） この設定は、SSL 接続が使用可能である場合にのみ有効です。

LDAP プロバイダーの削除

手順

ステップ 1 [Platform Settings] > [AAA] を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 [LDAP Providers] 領域で、削除する LDAP プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	RADIUS 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。 1 ～ 60 秒の整数を入力します。デフォルト値は 5 秒です。 このプロパティは必須です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。

ステップ 4 [Save] をクリックします。

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 追加する RADIUS プロバイダーごとに、次の手順を実行します。

a) [RADIUS Providers] 領域で、[Add] をクリックします。

b) [Add RADIUS Provider] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Hostname/FDQN (or IP Address)] フィールド	RADIUS プロバイダーが存在する場所のホスト名または IP アドレス。
[Order] フィールド	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。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、lowest-available または 0（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Authorization Port] フィールド	Firepower Chassis Manager または FXOS CLI が RADIUS データベースと通信するために使用されるポート。有効な範囲は 1 ～ 65535 です。標準ポート番号は 1700 です。
[Timeout] フィールド	RADIUS 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。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [RADIUS] タブで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 5 秒です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。 必要に応じて、0 ～ 5 の整数を入力します。値を指定しない場合、Firepower Chassis Manager は [RADIUS] タブに指定した値を使用します。

c) [OK] をクリックして、[Add RADIUS Provider] ダイアログボックスを閉じます。

ステップ 4 [Save] をクリックします。

RADIUS プロバイダーの削除

手順

ステップ 1 [Platform Settings] > [AAA] を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 [RADIUS Providers] 領域で、削除する RADIUS プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 5 秒です。 このプロパティは必須です。

ステップ 4 [Save] をクリックします。

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 [Platform Settings] > [AAA] を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 追加する TACACS+ プロバイダーごとに、次の手順を実行します。

a) [TACACS Providers] 領域で、[Add] をクリックします。

b) [Add TACACS Provider] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Hostname/FDQN (or IP Address)] フィールド	TACACS+ プロバイダーが存在する場所のホスト名または IP アドレス。
[Order] フィールド	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。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、lowest-available または 0（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が TACACS+ データベースと通信するために使用するポート。 1 ～ 65535 の整数を入力します。デフォルト ポートは 49 です。
[Timeout] フィールド	タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [TACACS+] タブで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 5 秒です。

c) [OK] をクリックして、[Add TACACS Provider] ダイアログボックスを閉じます。

ステップ 4 [Save] をクリックします。

TACACS+ プロバイダーの削除

手順

ステップ 1 [Platform Settings] > [AAA] を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 [TACACS Providers] 領域で、削除する TACACS+ プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。

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 [Platform Settings] > [Syslog] を選択します。

ステップ 2 ローカル宛先を設定します。

a) [Local Destinations] タブをクリックします。

b) [Local Destinations] タブで、次のフィールドに値を入力します。

名前	説明
[Console] セクション	

名前	説明
[Admin State] フィールド	Firepower シャーシでコンソールに syslog メッセージが表示されるかどうか。 syslog メッセージをログに追加するだけでなく、コンソールにも表示する場合は、[Enable] チェックボックスをオンにします。[Enable] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、コンソールには表示されません。
[Level] フィールド	[Console - Admin State] の [Enable] チェックボックスをオンにした場合は、コンソールに表示するメッセージの最も低いレベルを選択します。Firepower シャーシのコンソールにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • Emergencies • Alerts • Critical
[Monitor] セクション	
[Admin State] フィールド	Firepower シャーシでモニタに syslog メッセージが表示されるかどうか。 syslog メッセージをログに追加するだけでなく、モニタにも表示する場合は、[Enable] チェックボックスをオンにします。[Enable] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、モニタには表示されません。
[Level] ドロップダウン リスト	[Monitor - Admin State] の [Enable] チェックボックスをオンにした場合は、モニタに表示するメッセージの最も低いレベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • Emergencies • Alerts • Critical • エラー • Warnings • Notifications • Information • Debugging

c) [Save] をクリックします。

ステップ 3 リモート宛先を設定します。

a) [Remote Destinations] タブをクリックします。

b) [Remote Destinations] タブで、Firepower シャーシによって生成されたメッセージを保存できる最大 3 つの外部ログについて、次のフィールドに入力します。
syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

名前	説明
[Admin State] フィールド	syslog メッセージをリモート ログ ファイルに保存する場合は、[Enable] チェックボックスをオンにします。
[Level] ドロップダウン リスト	システムに保存するメッセージの最も低いレベルを選択します。リモート ファイルにそのレベル以上のメッセージが保存されます。次のいずれかになります。 • Emergencies • Alerts • Critical • エラー • Warnings • Notifications • Information • Debugging
[Hostname/IP Address] フィールド	リモート ログ ファイルが存在するホスト名または IP アドレス。 （注） IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

名前	説明
[Facility] ドロップダウン リスト	ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。次のいずれかになります。 • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7

c) [Save] をクリックします。

ステップ 4 ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) [Local Sources] タブで、次のフィールドに値を入力します。

名前	説明
[Faults Admin State] フィールド	システム障害ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム障害をログに記録します。
[Audits Admin State] フィールド	監査ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべての監査ログ イベントをログに記録します。
[Events Admin State] フィールド	システム イベント ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム イベントをログに記録します。

c) [Save] をクリックします。

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 [Platform Settings] > [DNS] を選択します。

ステップ 2 [Enable DNS Server] チェックボックスをオンにします。

ステップ 3 追加する DNS サーバ（最大 4 台）ごとに、それぞれの IP アドレスを [DNS Server] フィールドに入力し、[Add] をクリックします。

ステップ 4 [Save] をクリックします。