プラットフォームの設定

日付と時刻の設定

日付と時刻を手動で設定したり、NTP サーバを設定したりするには、NTP pageを使用します。シャーシに設定した日付と時刻は、論理デバイスを含めて、シャーシ内の他のコンポーネントと同期されます。

NTP サーバ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。

手順

ステップ 1 [プラットフォーム設定（Platform Settings）] > [NTP] を選択します。

ステップ 2 Firepower のシャーシに適切なタイムゾーンを [タイムゾーン（Time Zone）] ドロップダウン リストから選択します。

ステップ 3 [時刻源を設定（Set Time Source）] で、[NTP サーバを使用（Use NTP Server）] をクリックし、[NTP サーバ（NTP Server）] フィールドで使用する NTP サーバの IP アドレスまたはホスト名を入力します。

ステップ 4 [保存（Save）] をクリックします。
Firepower のシャーシが指定した NTP サーバで設定されます。

（注） システム時刻を 10 分以上変更するとログアウトされます。そのため、Firepower Chassis Manager に再度ログインする必要があります。

手動での日付と時刻の設定

ここでは、Firepower のシャーシで日付と時刻を手動で設定する方法ついて説明します。

手順

ステップ 1 [プラットフォーム設定（Platform Settings）] > [NTP] を選択します。

ステップ 2 Firepower のシャーシに適切なタイムゾーンを [タイムゾーン（Time Zone）] ドロップダウン リストから選択します。

ステップ 3 [時刻源の設定（Set Time Source）] で、[時刻を手動で設定（Set Time Manually）] をクリックします。

ステップ 4 [日付（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、そのカレンダーで使用可能なコントロールを使用して日付を設定します。

ステップ 5 対応するドロップダウン リストを使用して、時刻を時間、分、および AM/PM で指定します。

ヒント [システム時刻を取得（Get System Time）] をクリックすると、Firepower Chassis Manager への接続に使用するシステムの設定に一致する日付と時刻を設定できます。

ステップ 6 [保存（Save）] をクリックします。
Firepower のシャーシが指定した日付と時刻で設定されます。

（注） システム時刻を 10 分以上変更するとログアウトされます。そのため、Firepower Chassis Manager に再度ログインする必要があります。

SSH の設定

次に、Firepower のシャーシへの SSH アクセスを有効または無効にする手順を示します。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 [プラットフォーム設定（Platform Settings）] > [SSH] を選択します。

ステップ 2 Firepower のシャーシへの SSH アクセスを有効にするには、[SSH を有効化（Enable SSH）] チェックボックスをオンにします。SSH アクセスを無効にするには、[SSH を有効化（Enable SSH）] チェックボックスをオフにします。

ステップ 3 [保存（Save）] をクリックします。

Telnet の設定

次に、Firepower のシャーシへの Telnet アクセスを有効または無効にする手順を示します。Telnet はデフォルトで無効になっています。

（注） 現在、Telnet は CLI を使用してのみ設定できます。

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 モードに入ります。
Firepower-chassis /system #**scope services**

ステップ 3 Firepower のシャーシへの 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 のシャーシへの 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 のシャーシへの Telnet アクセスを拒否するには、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の設定に対して確定します。
Firepower /system/services # **commit-buffer**

次に、Telnet を有効にし、トランザクションを確定する例を示します。

```
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

[SNMP] ページを使用して、Firepower のシャーシ上に Simple Network Management Protocol（SNMP）を設定します。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 のデータを維持し、必要に応じてそのデータを SNMP マネージャに報告する Firepower シャーシ内のソフトウェア コンポーネント。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にし、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 を有効にし、設定します。
- 管理情報ベース：SNMP エージェントの一連の管理対象オブジェクト。

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 のシャーシは、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 の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 のシャーシが 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 モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

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、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 *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	なし	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	なし	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（Username）]	なし	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	なし	HMAC セキュア ハッシュ アルゴリズム（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、またはプロセスに情報の利用や開示が行えないようにします。

SNMP サポート

Firepower のシャーシは、SNMP に次のサポートを提供します。

MIB のサポート

Firepower のシャーシは、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 のシャーシは、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 のシャーシは、SNMPv3 メッセージ暗号化用プライバシー 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 の設定を有効にして、SNMPv3 ユーザ用のプライバシー パスワードを含めると、Firepower の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 priv パスワードは、8 文字以上にします。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 の有効化と SNMP プロパティの設定

手順

ステップ 1 [プラットフォーム設定（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
[管理状態（Admin State）] チェックボックス	SNMP を有効にするか無効にするか。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
[ポート（Port）] フィールド	Firepower のシャーシが 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。
[コミュニティ/ユーザ名（Community/Username）] フィールド	Firepower のシャーシが SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティの名前、あるいは SNMP v3 のユーザ名。 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。
[システム管理者名（System Administrator Name）] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレスまたは名前と電話番号など、最大 255 文字の文字列を入力します。
[ロケーション（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 文字の英数字を入力します。

ステップ 3 [保存（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 [プラットフォーム設定（Platform Settings）] > [SNMP] を選択します。

ステップ 2 [SNMP トラップ（SNMP Traps）] 領域で、[追加（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 の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。

名前	説明
[コミュニティ/ユーザ名（Community/Username）] フィールド	Firepower のシャーシ がトラップを SNMP ホストに送信するときに含める SNMP v1 または v2c のコミュニティ名または SNMP v3 のユーザ名。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。
[ポート（Port）] フィールド	Firepower のシャーシがトラップのために SNMP ホストと通信するポート。 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
[タイプ（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 • Informs
[v3 特権（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。 • [認証（Auth）]：認証あり、暗号化なし • [認証なし（Noauth）]：認証なし、暗号化なし • [秘密（Priv）]：認証あり、暗号化あり

ステップ 4 [OK] をクリックして [SNMP トラップの追加（Add SNMP Trap）] ダイアログボックスを閉じます。

ステップ 5 [保存（Save）] をクリックします。

SNMP トラップの削除

手順

ステップ 1 [プラットフォーム設定（Platform Settings）] > [SNMP] を選択します。

ステップ 2 [SNMP トラップ（SNMP Traps）] 領域で、削除するトラップに対応するテーブルの行にある [削除（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 [プラットフォーム設定（Platform Settings）] > [SNMP] を選択します。

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

ステップ 3 [SNMP ユーザの追加（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（Description）]
[名前（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）、および -（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。
[パスワード（Password）] フィールド	このユーザのパスワード。
[パスワードの確認（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 [SNMP ユーザの追加（Add SNMP User）] ダイアログボックスを閉じます。

ステップ 5 [保存（Save）] をクリックします。

SNMPv3 ユーザの削除

手順

ステップ 1 [プラットフォーム設定（Platform Settings）] > [SNMP] を選択します。

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

HTTPS ポートの変更

デフォルトでは、HTTPS サービスはポート 443 で有効になっています。HTTPS を無効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 [プラットフォーム設定（Platform Settings）] > [HTTPS] を選択します。

ステップ 2 [ポート（Port）] フィールドに、HTTPS 接続に使用するポートを入力します。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 [保存（Save）] をクリックします。
Firepower のシャーシが指定した HTTPS ポートで設定されます。

HTTPS ポートを変更した後に、現在のすべての HTTPS セッションが閉じられます。ユーザは、次に示すように新しいポートを使用して Firepower Chassis Manager にログインし直す必要があります。

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

ここで、<*chassis_mgmt_ip_address*> は初期設定時に入力した Firepower のシャーシの IP アドレスまたはホスト名、<*chassis_mgmt_port*> は直前に設定した HTTPS ポートです。

AAA の設定

ここでは、認証、許可、および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を制御するための一連のサービスで、ポリシーを適用し、使用状況を評価し、サービスの課金に必要な情報を提供します。これらのプロセスは、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と見なされています。

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、ユーザのクレデンシャルとデータベースに保存されている他のユーザ クレデンシャルとを比較します。クレデンシャルが一致した場合は、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は、認証は失敗し、ネットワーク アクセスは拒否されます。

シャーシへの管理接続を認証するように Firepower アプライアンス を設定できます。これには、次のセッションが含まれます。

- HTTPS
- SSH
- シリアル コンソール

承認

許可はポリシーを適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許可される可能性があります。

アカウンティング

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。これには、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、許可、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、許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。許可では必ず、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、認証および許可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス制御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。許可は、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装します。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 のシャーシは、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。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、許可、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は、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これらのうち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 [プラットフォーム設定（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 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[タイムアウト（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。
[属性（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。

名前	説明
[ベース DN（Base DN）] フィールド	リモートユーザがログインして、システムがユーザ名に基づいてユーザの DN を取得しようとするときに、サーバが検索を開始する必要がある場合の、LDAP 階層内の特定の識別名。ベース DN は、最大 255 文字から CN= $userid の長さを差し引いた長さに設定することができます。ここで、$userid は、LDAP 認証を使用して Firepower のシャーシへアクセスしようとしているリモート ユーザの識別に使用されます。 このプロパティは必須です。このタブでベース DN を指定しない場合は、定義する LDAP プロバイダーごとにベース DN を指定する必要があります。
[フィルタ（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は、定義する LDAP プロバイダーごとにフィルタを指定する必要があります。

ステップ 4 [保存（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 プロバイダーをサポートします。

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 [プラットフォーム設定（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 プロバイダー（LDAP Providers）] 領域で、[追加（Add）] をクリックします。

b) [LDAP プロバイダーの追加（ADD LDAP Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[ホスト名/FDQN（または IP アドレス）（Hostname/FDQN (or IP Address)）] フィールド	LDAP プロバイダーが存在するホスト名または 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 文字の ASCII 文字です。
[ベース DN（Base DN）] フィールド	リモートユーザがログインして、システムがユーザ名に基づいてユーザの DN を取得しようとするときに、サーバが検索を開始する必要がある場合の、LDAP階層内の特定の識別名。ベース DN は、最大 255 文字から CN= $userid の長さを差し引いた長さに設定することができます。ここで、$userid は、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI へアクセスしようとしているリモート ユーザの識別に使用されます。 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。
[ポート（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。
[SSLの有効化（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。

名前	説明
[フィルタ（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。
[属性（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	[バインド DN（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）は使用できません。
[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。
[タイムアウト（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 プロバイダーや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 [LDAP プロバイダーの追加（Add LDAP Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

LDAP プロバイダーの削除

手順

ステップ 1 [プラットフォーム設定（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 プロバイダー（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にある [削除（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は、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これらのうち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 [プラットフォーム設定（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 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[タイムアウト（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 [保存（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 プロバイダーをサポートします。

手順

ステップ 1 [プラットフォーム設定（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 追加する各 RADIUS プロバイダーに、次の手順を実行します。

a) [RADIUS プロバイダー（RADIUS Providers）] 領域で、[追加（Add）] をクリックします。

b) [RADIUS プロバイダーの追加（ADD RADIUS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[ホスト名/FDQN（または IP アドレス）（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。
[タイムアウト（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。

名前	説明
[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。値を指定しなければ、Firepower Chassis Manager は [RADIUS] タブで指定した値を使用します。

c) [OK] をクリックして [RADIUS プロバイダーの追加（Add RADIUS Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（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 [プラットフォーム設定（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 プロバイダー（LDAP 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にある [削除（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は、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これらのうち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 [プラットフォーム設定（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 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[タイムアウト（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 [保存（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+ プロバイダーをサポートします。

手順

ステップ 1 [プラットフォーム設定（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 追加する各 TACACS+ プロバイダーに、次の手順を実行します。

a) [TACACS プロバイダー（TACACS Providers）] 領域で、[追加（Add）] をクリックします。

b) [TACACS プロバイダーの追加（ADD TACACS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[ホスト名/FDQN（または IP アドレス）（Hostname/FDQN (or IP Address)）] フィールド	TACACS+ プロバイダーが存在するホスト名または 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。

名前	説明
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[ポート（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されるポート。 1 ～ 65535 の整数を入力します。デフォルトのポートは 49 です。
[タイムアウト（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 [TACACS プロバイダーの追加（Add TACACS Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（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 [プラットフォーム設定（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 プロバイダー（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にある [削除（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 syslog サーバへのロギングは、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、ルーチンの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 [プラットフォーム設定（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) [ローカル宛先（Local Destinations）] タブをクリックします。

b) [ローカル宛先（Local Destinations）] タブで、次のフィールドに入力します。

名前	説明
[Console] セクション	
[Admin State] フィールド	Firepower のシャーシがコンソールに syslog メッセージを表示するかどうかを指定します。 ログに追加するとともに、コンソールに syslog メッセージを表示する場合は、[有効（Enable)] チェックボックスをオンにします。[有効（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、コンソールに表示されません。
[レベル（Level）] フィールド	[コンソール（Consle）] > [管理状態（Admin State）] で [有効（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最低のメッセージレベルを選択します。Firepower のシャーシはコンソールにそのレベル以上のメッセージを表示します。次のいずれかになります。 • 緊急事態（Emergencies） • アラート（Alerts） • クリティカル（Critical）
[Monitor] セクション	
[Admin State] フィールド	Firepower のシャーシがモニタに syslog メッセージを表示するかどうかを指定します。 syslog メッセージをログに追加するとともに、モニタに表示する場合は、[有効（Enable)] チェックボックスをオンにします。[有効（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、モニタに表示されません。

名前	説明
[レベル（Level）] ドロップダウン リスト	[モニタ（Monitor）] > [管理状態（Admin State）] で [有効（Enable）]チェックボックスをオンにした場合は、モニタに表示する最低のメッセージ 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。 • 緊急事態（Emergencies） • アラート（Alerts） • クリティカル（Critical） • エラー（Errors） • 警告（Warnings） • 通知（Notifications） • 情報（Information） • デバッグ（Debugging）

c) [保存（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) [リモート宛先（Remote Destinations）] タブをクリックします。

b) [リモート宛先（Remote Destinations）] 領域で、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 個の外部ログの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によって、外部 syslog サーバのディスク領域に応じてメッセージをアーカイブでき、保存後は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	リモート ログ ファイルに syslog メッセージを保存する場合は、[有効（Enable)] チェックボックスをオンにします。

名前	説明
[レベル（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。 • 緊急事態（Emergencies） • アラート（Alerts） • クリティカル（Critical） • エラー（Errors） • 警告（Warnings） • 通知（Notifications） • 情報（Information） • デバッグ（Debugging）
[ホスト名/IPアドレス（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。
[ファシリティ（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) [保存（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) [ローカル送信元（Local Sources）] タブをクリックします。

b) [ローカル送信元（Local Sources）] タブで、次のフィールドに入力します。

名前	説明
[障害管理状態（Faults Admin State）] フィールド	システム障害のロギングが有効かどうかを指定します。[有効（Enable）] チェックボックスをオンにすると、Firepower のシャーシはすべてのシステム障害をログに記録します。
[監査管理状態（Audits Admin State）] フィールド	監査ロギングが有効かどうかを指定します。[有効（Enable）] チェックボックスをオンにすると、Firepower の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。
[イベント管理状態（Events Admin State）] フィールド	システム イベントのロギングが有効かどうかを指定します。[有効（Enable）] チェックボックスをオンにすると、Firepower の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) [保存（Save）] をクリックします。

DNS サーバの設定

システムがIPアドレスへのホスト名の解決を必要とする場合、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 シャーシに関する設定を行うときに、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ます。これには、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は、3 台の DNS サーバをランダムに検索します。

手順

ステップ 1 [プラットフォーム設定（Platform Settings）] > [DNS] を選択します。

ステップ 2 [DNS サーバを有効にする（Enable Edge Server）] チェックボックスをオンにします。

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

ステップ 4 [保存（Save）] をクリックします。