Platform Settings

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、[NTP] ページを使用します。 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。

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 [Platform Settings] > [NTP] を選択します。

ステップ 2 [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。

ステップ 3 [Set Time Source] で [Use NTP Server] をクリックし、使用する NTP サーバの IP アドレスまたはホスト名を [NTP Server] フィールドに入力します。

ステップ 4 [Save（保存）] をクリックします。
指定した NTP サーバが 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。

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 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。

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（保存）] 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　[Platform Settings] > [SSH] 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　[Save（保存）] 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 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 *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	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。
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 [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。
[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	Firepower シャーシが SNMP ホストに送信するトラップ メッセージに含める、デフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 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。
[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（保存）] 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 • informs

名前	説明
[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（保存）] 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）、および -（ハイフン）も指定できます。

名前	説明
[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（保存）] 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 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（保存）] 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。

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 [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（保存）] 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（保存）] 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 [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（保存）] 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（保存）] 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（保存）] 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（保存）] 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（保存）] 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（保存）] 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（保存）] 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（保存）] をクリックします。