認証、認可、アカウンティングの設定

AAA 認証サーバの設定

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

認証の順序について

AAA ポリシーでは、認証サーバにオプションで設定できるフェールオーバー機能を指定できます。2 つのフェールオーバー機能は、別々に、または組み合わせて、使用できます。

- 認証フェールオーバー
- 到達不能フェールオーバー

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「認証フェールオーバーについて」

認証フェールオーバーについて

認証フェールオーバー機能を使用すると、ユーザ ログイン認証のために、ローカル データベースに加え、オプションでリモート RADIUS サーバを使用できるようになります。この項の手順では、認証が解決される順序が設定されます。次のシステムを使用するよう、認証を設定できます。

- ローカル データベースのみ
- リモート サーバのみ
- 最初にローカル データベース、次にリモート サーバ
- 最初にリモート サーバ、次にローカル データベース

ローカル認証とリモート認証の両方を使用する場合、リモート RADIUS AAA サーバから取得されるユーザ属性を、同じユーザ名のローカル ユーザ データベースで見つかった属性にマージするかどうかも、設定できます。

（注） 認証フェールオーバー機能には、次の制限があります。

- RADIUS サーバでの認証は、GUI または CLI インターフェイスへのアクセス時にのみ使用可能で、ユーザ ID およびパスワードのみが必要です。自動受付インターフェイスは、ユーザに依存しないため、認証は不要です。
- ログイン情報は、ローカル システムとリモート サーバとの間では同期がとられません。したがって、次のとおりになります。
  - パスワードの期限切れなどのセキュリティ機能は、Cisco Unified SIP Proxy と RADIUS サーバで別々に設定する必要があります。
  - パスワードの期限切れまたはアカウントのロックアウトなどのセキュリティ イベントが、RADIUS サーバで発生した場合、Cisco Unified SIP Proxy ユーザに対しては、プロンプトは表示されません。
  - パスワードの期限切れまたはアカウントのロックアウトなどのセキュリティ イベントが、Cisco Unified SIP Proxy で発生した場合、RADIUS サーバのユーザに対しては、プロンプトは表示されません。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「到達不能フェールオーバーについて」

到達不能フェールオーバーについて

到達不能フェールオーバー機能は、RADIUS サーバでのみ使用されます。この機能を使用すると、RADIUS サーバへのアクセスに使用できる最大 2 つまでのアドレスを設定できます。

Cisco Unified SIP Proxy によって、RADIUS サーバでユーザの認証が試行されると、RADIUS サーバが、ユーザの認証に到達できないか、失敗したかを通知するメッセージが、ユーザに送信されます。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る

- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「認証シーケンスの例」

認証シーケンスの例

この例では、認証は、まず、リモート サーバによって実行され、次に、ローカル データベースによって実行されます。また、2 つのアドレスが、リモート RADIUS サーバに対して設定されます。

イベントのこのシーケンスは、次の例の認証中に発生する可能性があります。

1. Cisco Unified SIP Proxy では、まず、リモート RADIUS サーバへの通信が試行されます。
2. 1 台目の RADIUS サーバで、応答がないか、ユーザの認証クレデンシャルが受け付けられない場合、Cisco Unified SIP Proxy では、2 台目のリモート RADIUS サーバへの通信が試行されます。
3. 2 台目の RADIUS サーバで、応答がないか、ユーザの認証クレデンシャルが受け付けられない場合、ユーザは該当するエラー メッセージを受信し、Cisco Unified SIP Proxy では、ローカル データベースへの通信が試行されます。
4. ローカル データベースで、ユーザの認証クレデンシャルが受け付けられない場合、ユーザはエラー メッセージを受信します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「AAA 認証サーバの接続パラメータの設定」

AAA 認証サーバの接続パラメータの設定

手順

ステップ 1 [Configure] > [AAA] > [Authentication] を選択します。

[Configure AAA Authentication] ページが表示されます。

ステップ 2 プライマリ サーバの適切なフィールドに、次の情報を入力し、オプションで、セカンダリ サーバの適切なフィールドにも入力します。

- 認証順序
- ログイン再試行の回数
- ログイン タイムアウトの長さ
- ホスト名
- ポート
- パスワード

ステップ 3 [Apply] をクリックします。

ステップ 4 [OK] をクリックして、変更を保存します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る

認証と認可の動作を制御するポリシーの指定

手順

ステップ 1 [Configure] > [AAA] > [Authorization] を選択します。

[Configure AAA Authorization] ページが表示されます。

ステップ 2 リモート AAA サーバの属性を、ローカル データベースの属性とマージするかどうかを、選択するか、選択を解除します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [OK] をクリックして、変更を保存します。

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

AAA アカウンティング サーバの設定

- 「概要」
- 「AAA アカウンティング イベント ロギング」
- 「AAA アカウンティング サーバとイベント ロギングの設定」

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

概要

最大で 2 台の AAA アカウンティング サーバを設定できます。アカウンティング サーバを 2 台設定すると、自動フェールオーバー機能を使用できます。1 台目のサーバが到達不能の場合、アカウンティング情報が 2 台目のサーバに送信されます。両方のアカウンティング サーバが到達不能の場合、サーバが使用可能になるまで、アカウンティング レコードがキャッシュ保存されます。キャッシュがいっぱいになるまでにサーバに到達できない場合、最も古いアカウンティング パケットがドロップされ、新しいパケットのための容量が確保されます。

AAA アカウンティング サーバの設定は、AAA 認証サーバの設定から完全に独立しているため、AAA アカウンティング サーバは、AAA 認証サーバと同じマシンまたは異なるマシンに設定できます。

Syslog サーバを使用する場合、AAA 設定には影響を受けず、既存のユーザ インターフェイスが使用し続けられます。RADIUS サーバから Syslog サーバに AAA アカウンティング情報が送信される場合、記録される前に 1 つの文字列に正規化されます。Syslog サーバが定義されていない場合、Cisco Unity Express でローカルに実行されている Syslog サーバによって、AAA アカウンティング ログが記録されます。

（注） RADIUS サーバのみがサポートされます。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る
- 次の項目：「AAA アカウンティング イベント ロギング」

AAA アカウンティング イベント ロギング

AAA アカウンティング ログには、次の操作を簡単に実行できる情報が含まれています。

- 設定の変更を監査する。
- セキュリティを管理する。
- 正確にリソースを割り当てる。
- リソースの使用を課金する必要があるかどうかを決定する。

AAA アカウンティングを設定し、次のタイプのイベントのログを記録することができます。

ログ名	説明
login	ログインが必要な場合のすべての形式のシステム アクセス。
logout	ログアウト前にログインが必要な場合のすべての形式のシステム アクセス。
login-fail	ログインが必要な場合のすべての形式のシステム アクセスの、失敗したログイン試行。
config-commands	任意のインターフェイスを使用してシステム設定に行われた変更。
exec-commands	任意のインターフェイスを使用して EXEC モードで入力されたすべてのコマンド。
system-startup	システムのソフトウェア バージョン、インストールされているライセンス、インストールされているパッケージ、インストールされている言語などに関する情報が含まれる、システムの起動。
system-shutdown	システムのソフトウェア バージョン、インストールされているライセンス、インストールされているパッケージ、インストールされている言語などに関する情報が含まれる、システムのシャットダウン。

実行されるアクションのタイプ固有の情報に加え、次の情報を示すアカウンティング ログも示されます。

- アクションを認可したユーザ
- アクションが実行された時刻
- アカウンティング レコードがサーバに送信された時刻

（注） スタートアップ コンフィギュレーションのシステム電源投入時の再実行中には、アカウント ロギングは実行されません。システムの起動時には、startup-config コマンドは記録されません。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る
- 次の項目：「AAA アカウンティング サーバとイベント ロギングの設定」

AAA アカウンティング サーバとイベント ロギングの設定

この手順を使用して、アカウンティング サーバへのログインに使用される情報を設定します。

手順

ステップ 1 [Configure] > [AAA] > [Accounting] を選択します。

[Configure AAA Accounting] ページが表示されます。

ステップ 2 適切なフィールドに、次の情報を入力します。

- アカウンティングがイネーブルか
- ログイン再試行の回数
- ログイン タイムアウトの長さ（秒単位）
- プライマリ サーバのサーバ IP アドレスまたは DNS 名
- プライマリ サーバに使用されるポート番号
- プライマリ サーバのパスワード
- セカンダリ サーバのサーバ IP アドレスまたは DNS 名
- セカンダリ サーバに使用されるポート番号
- セカンダリ サーバのパスワード

ステップ 3 ログに含めるログ イベントを選択し、含めないイベントの選択を解除します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [OK] をクリックして、変更を保存します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る