CLIを使用したCatalyst 1300スイッチでの認可変更の基本設定

目的

この記事の目的は、コマンドラインインターフェイス(CLI)を使用して、Catalyst 1300スイッチの認可変更(CoA)機能の基本設定を実行する方法を示すことです。

該当するデバイスとソフトウェアバージョン

- Catalyst 1300 スイッチ | 4.1.3.36

はじめに

認可変更(CoA)はRADIUSプロトコルの拡張機能で、認証された後で認証、認可、アカウンティング(AAA)またはdot1xユーザセッションのプロパティを変更できます。AAAでユーザまたはグループのポリシーが変更されると、管理者はCisco Identity Services Engine(ISE)などのAAAサーバからRADIUS CoAパケットを送信して、認証を再初期化し、新しいポリシーを適用できます。

Cisco Identity Services Engine(ISE)は、完全な機能を備えたネットワークベースのアクセスコントロールおよびポリシー適用エンジンです。セキュリティの分析と適用、RADIUSおよびTACACSサービス、ポリシー配布などを提供します。Cisco ISEは現在、Catalyst 1300スイッチで唯一サポートされているCoAダイナミック認可クライアントです。詳細については、『ISE管理者ガイド』を参照してください。

CoAのサポートは、ファームウェアバージョン4.1.3.36でCatalyst 1300スイッチに追加されました。これには、ユーザの接続解除と、ユーザセッションに適用できる認可の変更のサポートが含まれます。このデバイスは、次のCoAアクションをサポートしています。

- セッションの切断
- ホストポートのCoAコマンドを無効にする
- Bounce host port CoAコマンド
- Reauthenticate host CoAコマンド

この記事では、CLIを使用したCatalyst 1300スイッチでの基本的なCoA設定コマンドについて説明します。手順は、ユーザの設定と要件によって異なります。

目次

- CLIを使用した基本的なCoA設定
- CoA設定のその他のコマンド
- 特権EXECモードのCLIコマンド

CLIを使用した基本的なCoA設定

RADIUSサーバとRADIUSアカウンティングの設定

RADIUSサーバを設定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

手順 1

radius-server keyコマンドを使用して、デバイスとRADIUSデーモン間のRADIUS通信に対する認証キーを設定します。

```
radius-server key
```

手順 2

RADIUSサーバホストを設定するには、radius-server hostコマンドを使用します。

```
radius-server host key priority 1 usage dot1.x
```

- IPアドレスはISEサーバのIPアドレスです。
- key <key-string>：デバイスとRADIUSサーバ間のすべてのRADIUS通信に対して、認証キーと暗号キーを指定します。このキーは、RADIUSデーモンで使用される暗号化と一致する必要があります。
- Priority：サーバが使用される順序を指定します。0が最高の優先順位です。(範囲：0 ~ 65535)
- usage dot1.x:802.1xポート認証にRADIUSサーバを使用するように指定します。

手順 3

```
aaa accounting dot1x start-stop group radius
```

動的承認サーバの設定

手順 1

グローバルコンフィギュレーションモードから、次のコマンドを実行して、CoAコンフィギュレーションモードに入ります。

```
aaa server radius dynamic-author
```

手順 2

デバイスとCoAクライアント間で共有されるRADIUSキー（範囲：0 ~ 128文字）を設定するには、ダイナミック認可ローカルサーバコンフィギュレーションモードでコマンドserver-key <key-string>を使用します。CoA要求で提供されるキーは、このキーと一致する必要があります。

```
server-key
```

> Note:
> ISEの場合、キー文字列は、RADIUSの設定時にRADIUSサーバのキー文字列に指定したものと同じキー文字列になります。

手順 3

CoAクライアントホストのIPアドレスを入力します。IPアドレスには、IPv4、IPv6、またはIPv6zアドレスを使用できます。

```
client
```

手順 4

```
Exit
```

802.1xの設定

802.1Xをグローバルに有効にするには、dot1x system-auth-controlコマンドを使用します。

```
dot1x system-auth-control
```

ポートでの802.1xの設定

手順 1

インターフェイスコンフィギュレーションを入力し、interface GigabitEthernet<インターフェイスID>コマンドを使用して、インターフェイスIDを選択します。

```
interface gi1/0/1
```

手順 2

ポート許可状態の手動制御を有効にするには、dot1x port-controlコマンドを使用します。Autoモードは、デバイスとクライアント間の802.1X認証交換に基づいて、ポートで802.1X認証を有効にし、ポートを承認済みまたは未承認の状態に移行させます。

```
dot1x port-control auto
```

手順 3

すべての802.1X対応ポートまたは指定した802.1X対応ポートの再認証を手動で開始するには、特権EXECモードでdot1x re-authenticateコマンドを使用します。

```
dot1x re-authenticate gi1/0/1
```

手順 4

ポートセキュリティラーニングモードを設定するには、ポートセキュリティモードインターフェイス（イーサネット、ポートチャネル）コンフィギュレーションモードコマンドを使用します。セキュアなdelete-on-resetパラメータは、delete-on-reset time-of-liveを備えたセキュアMACアドレスを限定的に学習するセキュアモードです。

```
port security mode secure delete-on-reset
```

手順 5

インターフェイスの設定を終了するには、次のように入力します。

```
exit
```

CoA設定のその他のコマンド

設定と設定に基づいて使用できる他のCoAコマンドの一部を次に示します。

- attribute event-timestamp drop-packet：このコマンドは、Packet of Disconnect(PoD)要求またはevent-timestamp属性を含まないCoA要求を廃棄するようにデバイスを設定するために、ダイナミック認可ローカルサーバコンフィギュレーションモードで使用されます。

```
attribute event-timestamp drop-packet
```

- authenticationコマンドbounce-port ignore:RADIUS認可変更(CoA)バウンスポートコマンドを無視するようにデバイスを設定するには、グローバルコンフィギュレーションモードで authentication command bounce-port ignoreコマンドを使用します。

```
authentication command bounce-port ignore
```

- authenticationコマンドdisable-port ignore:RADIUS CoA disable-portコマンドを無視するようにデバイスを設定するには、グローバルコンフィギュレーションモードでこのコマンドを使用します

。

```
authentication command disable-port ignore
```

- domain delimiter <character>：受信したPoDおよびCoA要求のユーザ名ドメイン区切り記号を設定するには、動的認可ローカルサーバ設定モードでdomain delimiterコマンドを使用します。

```
domain delimiter $
```

この例では、$文字がデリミタとして設定されています。

- domain stripping [right-to-left]：受信したPoDおよびCoA要求のユーザ名ドメインの削除を有効にし、動作を定義するには、dynamic authorization local server設定モードでdomain strippingコマンドを使用します。

```
domain stripping right-to-left
```

- ignore server-key：このコマンドは、CoAサーバキーを無視するようにデバイスを設定するために、ダイナミック認可ローカルサーバコンフィギュレーションモードで使用されます。

```
ignore server-key
```

特権EXECモードのCLIコマンド

特権EXECモードから、認証されたクライアントに対してshowコマンドを実行し、クライアントカウンタをクリアして、ダイナミック認可サーバ設定を表示できます。

- show aaa clientsコマンドを使用して、AAA(CoA)クライアントの統計情報を表示します。

```
show aaa clients
```

- CoA設定を表示するには、show aaa server radius dynamic-authorコマンドを使用します。

```
show aaa server radius dynamic-author
```

- clear aaa countersは、aaa clientsカウンタのクリアに使用できます

```
clear aaa clients counters
```

結論

これで、CLIを使用したCatalyst 1300スイッチでの基本的な認可変更(CoA)設定が完了しました。

Catalyst 1300スイッチのCLIコマンドについての詳細は、『Cisco Catalyst 1300スイッチ

シリーズCLIガイド』を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。