Catalyst 3550 シリーズ スイッチ上の 802.1x 有線認証と ACS バージョン 4.2 の設定例

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[スイッチ設定例](#)
[ACS の設定](#)
[確認](#)
[トラブルシューティング](#)

概要

この資料は Cisco Access Control Server（ACS）バージョン 4.2 を基本的な IEEE 802.1x 設定例および配線された認証に Remote Access Dial In User Service（RADIUS）プロトコルに与えたものです。

前提条件

要件

シスコでは次を推奨しています。

- ACS とスイッチ間の IP到達性を確認して下さい。
- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート 1645 および 1646 が ACS とスイッチ間で開いていることを確認して下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Catalyst 3550 シリーズ スイッチ
- Cisco Secure ACS バージョン 4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

スイッチ設定例

1. RADIUSサーバおよび事前共有キーを定義するために、このコマンドを入力して下さい:
   ```
   Switch(config)# radius-server host 192.168.1.3  key  cisco123
   ```

2. 802.1X 機能性を有効に するために、このコマンドを入力して下さい:
   ```
   Switch(config)# dot1x system-auth-control
   ```

3. グローバルにイネーブル 認証、許可、アカウンティング（AAA）および RADIUS認証および許可は、これらのコマンドを入力します:
   注: これは RADIUSサーバからの属性を渡す必要がある場合必要です; さもなければ、それをスキップできます。

   ```
   Switch(config)# aaa new-model
   Switch(config)# aaa authentication dot1x default group radius
   awitch(Config)# aaa authorization network default group radius
   Switch(Config)# aaa accounting dot1x default start-stop group radius

   Switch(config-if)# switchport mode acces
   Switch(config-if)# switchport access vlan <vlan>
   Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
   Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
   Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
   Switch(config-if)# dot1x timeout quiet-period <seconds to wait after failed attempt>
   Switch(config-if)# dot1x timeout tx-period <time to resubmit request>
   ```

ACS 設定

1. スイッチを ACS の AAA クライアントとして追加するために、**Network Configuration > Add エントリ AAA クライアント**にナビゲート し、この情報を入力して下さい:
   IP Address： *<IP>*共有秘密： *<key>*認証するを使用して: Radius（6.0）Cisco IOS ®/PIX

2. 認証を設定し、**システム構成**に **> グローバル な 認証 セットアップ** ナビゲート し、**割り当て MS-CHAP バージョン 2 認証** チェックボックスがチェックされることを確認するために設定するため:

3. ユーザを設定するために、メニューで『User Setup』 をクリック し、これらのステップを完了して下さい:
   ユーザ情報を入力して下さい: ネットワーク Admin *<username>*。『Add/Edit』 をクリックして下さい。**本名を**入力して下さい: ネットワーク Admin *<descriptive name>*。**説明を**追加

して下さい: *<your choice>*。**パスワード認証を**選択して下さい: ACS 内部データベース。**パスワードを**入力して下さい: ..... *<password>*。**パスワードを**確認して下さい: *<password>*。[Submit] をクリックします。

確認

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

設定がきちんと機能することを確認するためにこれらのコマンドを入力して下さい:

- **dot1x を示して下さい**
- **dot1x 要約を表示して下さい**
- **dot1x インターフェイスを示して下さい**
- **show authentication セッション インターフェイス *<interface>***
- **show authentication インターフェイス *<interface>***

```
Switch(config)# show dot1x
_____________________________________________________
Sysauthcontrol Enabled
Dot1x Protocol Version 3
_____________________________________________________
Switch(config)# show dot1x summary
_____________________________________________________
Interface PAE Client Status
_____________________________________________________
Fa0/4 AUTH
_____________________________________________________
Switch(config)# show dot1x interface fa0/4 detail
_____________________________________________________
Dot1x Info for FastEthernet0/4
_____________________________________________________
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

トラブルシューティング

このセクションは設定をトラブルシューティングするために使用できる debug コマンドを提供します。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- dot1x をすべてデバッグして下さい
- debug authentication すべて
- debug radius（デバッグ レベルで半径の情報を提供します）
- debug aaa authentication（認証のためのデバッグ）
- debug aaa authorization（許可のためのデバッグ）