AAA Authentication Login Default Local Group TACACS+コマンドについて

内容

概要

このドキュメントでは、Cisco IOS®デバイスでの**aaa authentication login default local group tacacs+**コマンドの動作について説明します。

前提条件

要件

シスコでは、次のことを推奨しています。

- デバイスで**aaa new-model**が有効になっている。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

> **注**：このセクションで使用されているコマンドの詳細を調べるには、Ciscoツールカタログにある[Cisco CLI Analyzer](#)を使用してください。シスコの内部ツールおよび情報にアクセスできるのは、登録されたシスコユーザのみです。

デバイスで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設定します。

```
aaa new-model
aaa authentication login default local group tacacs+
```
~だけで aaa new model ローカル認証が設定されている場合は、すべての回線とインターフェイス(コンソール回線**line con 0**を除く)に適用されます。

この場合、AAA方式リストは、デバイスのすべての回線のすべてのログイン試行に適用されます。最初のローカルデータベースがチェックされ、必要に応じてTerminal Access Controller Access Control System(TACACS)サーバが試行されます。

```
username cisco privilege 15 password 0 cisco
```
ローカルユーザーデータベース：

```
tacacs-server host 10.20.220.141
tacacs-server key cisco
```
これで、TACACSサーバが設定されました。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. テスト対象のデバイスで**Debug TACACS**および**Debug AAA Authentication**を有効にします。

```
RUT#show debug
General OS:
  TACACS access control debugging is on
   AAA Authentication debugging is on
```
2. デバイスでtelnetを実行します。

```
RUT#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/1            10.197.235.96   YES DHCP   up                    up
Loopback0                  192.168.1.2     YES manual up                    up

RUT#telnet 192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification

Username: cisco
*Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
*Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list 'default'
Password:

RUT>
```
ユーザ名ciscoがローカルで見つかったため、TACACSサーバに到達しようとしなかったことがわかります。

ここで、ボックスでローカルに設定されていないクレデンシャルを使用しようとすると、次のようになります。

```
RUT#telnet 192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification

Username:
*Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f
*Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list 'default'
Username: cisco1
*Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing
*Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31
*Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)
*Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141
*Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet
% Authentication failed
```

TACACSサーバ10.20.220.141に到達しようとしていることがわかります。これは予期されるデフォルトの動作です。TACACSサーバにユーザ名「cisco1」が設定されていないため、「Authentication failed」と表示されます。

デバイスの設定にデフォルトグループtacacs+ localのAAA認証ログがある場合、最初の設定はTACACSです。TACACSに到達できるが、設定されているユーザがいない場合、TACACSはフォールバックせず、ローカルデータベースで検索を試みます。メッセージ「Authentication failed」が表示されます。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- アクセスサーバでの基本的なAAAの設定
- シスコテクニカルサポートおよびダウンロード

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。