

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[手順説明](#)

[TACACS+ CLI の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Nexus 4000 シリーズ スイッチに Terminal Access Controller Access Control System (TACACS+) を設定する方法を説明します。Nexus 4000 シリーズでの TACACS+ 認証は、Cisco Catalyst スイッチの場合と少し異なります。

前提条件

要件

次の項目に関する知識があることが推奨されます。 [Cisco Nexus 7000 シリーズ NX-OS Fundamentals コマンド](#)。

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 Nexus 4005I スイッチ
- Cisco Secure Access Control Server (ACS) 5.x

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。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

この項の設定例では、1 台の Nexus 4005I スイッチと 1 台の TACACS+ サーバを設定する方法を説明します。

手順説明

Nexus スイッチおよび TACACS+ サーバを設定するには、次の手順を実行します。

1. TACACS+ プロトコル機能を有効にします。ACS サーバの IP アドレスに事前共有キーが設定されている必要があります。ACS サーバが複数存在する場合は、両方のホストを設定する必要があります。
2. AAA の概念および AAA サーバグループを有効にします。この設定例では、AAA グループの名前は「ACS」です。

TACACS+ CLI の設定

```
ASA
!--- Enable TACACS+ on the device.feature tacacs+
tacacs-server host 10.0.0.1 key 7 Ciscotacacs-server
host 10.0.0.2 key 7 Ciscotacacs-server directed-
request!--- Provide the name of your ACS server.aaa
group server tacacs+ ACS!--- Mention the IP address of
the tacacs-servers !--- referred to in the "tacacs-
server host" command.server 10.0.0.1 server 10.0.0.2!---
Telnet and ssh sessions.aaa authentication login default
group ACS local !--- Console sessions.aaa authentication
login console group ACS local !--- Accounting
command.aaa accounting default group ACS
```

注ACS サーバでは、Nexus 4000 シリーズと ACS サーバの間の認証に同じ事前共有キー「Cisco」を使用してください。

注TACACS+ サーバが停止している場合は、ユーザ名およびパスワードをスイッチに設定することにより、ローカル認証にフォールバックできます。

Nexus オペレーティングシステムでは、特権レベルという概念の代わりにロールという概念を使用します。デフォルトでは、*network-operator* ロールが割り当てられます。ユーザにフル権限を付与するには、ユーザに *network-admin* ロールを割り当てる必要があります。TACACS+ の場合は、元の値 *roles="roleA"* の TACACS カスタム属性を渡します。完全なアクセス権を持つユーザについては、次の設定を使用します。 `cisco-av-pair*shell: roles= " Admin`

```
!--- Enable TACACS+ on the device.feature tacacs+ tacacs-server host 10.0.0.1 key 7 Ciscotacacs-
server host 10.0.0.2 key 7 Ciscotacacs-server directed-request!--- Provide the name of your ACS
server.aaa group server tacacs+ ACS!--- Mention the IP address of the tacacs-servers !---
referred to in the "tacacs-server host" command.server 10.0.0.1 server 10.0.0.2!--- Telnet and
ssh sessions.aaa authentication login default group ACS local !--- Console sessions.aaa
authentication login console group ACS local !--- Accounting command.aaa accounting default
group ACS!--- Enable TACACS+ on the device.feature tacacs+ tacacs-server host 10.0.0.1 key 7
Ciscotacacs-server host 10.0.0.2 key 7 Ciscotacacs-server directed-request!--- Provide the name
of your ACS server.aaa group server tacacs+ ACS!--- Mention the IP address of the tacacs-servers
!--- referred to in the "tacacs-server host" command.server 10.0.0.1 server 10.0.0.2!--- Telnet
and ssh sessions.aaa authentication login default group ACS local !--- Console sessions.aaa
authentication login console group ACS local !--- Accounting command.aaa accounting default
group ACS
```

確認

TACACS+ サーバの設定を確認するには、この項のコマンドを使用します。

- `tacacs` サーバを示して下さいか。TACACS+ サーバコンフィギュレーションを表示します。
- `show aaa authentication [login {error-enable | mschap}]`か。設定された認証情報を表示する。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の `show` コマンドがサポートされています。OIT を使用して、`show` コマンド出力の解析を表示できます。

トラブルシューティング

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

- [AAA の設定](#)
- [TACACS+ の設定](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)