Nexus 4005I での TACACS+ の設定例

内容

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

次の項目に関する専門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いています。

- 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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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。

手順ごとの説明

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 Cisco tacacs-server host 10.0.0.2 key 7 Cisco tacacs-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：Nexus 4000シリーズとACSサーバ間の認証には、ACSサーバで同じ事前共有キー「Cisco」を使用します。

注：TACACS+サーバがダウンしている場合は、スイッチでユーザ名とパスワードを設定することで、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、ユーザがログインするときに属性を割り当てるように TACACS サーバを設定する必要があります。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="network-admin"`

`cisco-av-pair*shell:roles="network-admin"(The * makes it optional)`

`shell:roles="network-admin"`

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。

- **show tacacs-server**：TACACS+ サーバ設定が表示されます。
- **show aaa authentication [login {error-enable | mschap}]**：設定されている認証情報を表示します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

トラブルシュート

現在、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