

TACACS+ in Nexus 4005I - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurationen](#)

[Schrittweise Anleitung](#)

[CLI-Konfiguration von TACACS+](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie das Terminal Access Controller Access Control System (TACACS+) in einem Nexus Switch der Serie 4000 konfiguriert wird. Die TACACS+-Authentifizierung unterscheidet sich in der Nexus Serie 4000 geringfügig von der eines Cisco Catalyst Switches.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in diesem Bereich zu verfügen: [Befehle zu den Grundlagen der Cisco Nexus Serie 7000 NX-OS](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Nexus 4005I-Switch
- Cisco Secure Access Control Server (ACS) 5.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

Konfigurationen

Im Konfigurationsbeispiel in diesem Abschnitt wird die Konfiguration eines Nexus 4005I-Switches und eines TACACS+-Servers beschrieben.

Schrittweise Anleitung

Gehen Sie wie folgt vor, um den Nexus-Switch und den TACACS+-Server zu konfigurieren:

1. Aktivieren Sie die TACACS+-Protokollfunktion. Die IP-Adresse des ACS-Servers muss mit dem vorinstallierten Schlüssel konfiguriert werden. Wenn es mehr als einen ACS-Server gibt, müssen beide Hosts konfiguriert werden.
2. Aktivieren Sie das AAA-Konzept und die AAA-Servergruppe. In diesem Konfigurationsbeispiel lautet der Name der AAA-Gruppe "ACS".

CLI-Konfiguration von TACACS+

```
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
```

Hinweis: Verwenden Sie für die Authentifizierung zwischen dem Nexus 4000 und dem ACS-Server denselben vorinstallierten Schlüssel "Cisco" im ACS-Server.

Hinweis: Wenn der TACACS+-Server ausgefallen ist, können Sie die lokale Authentifizierung wiederherstellen, indem Sie den Benutzernamen und das Kennwort im Switch konfigurieren.

Das Nexus-Betriebssystem verwendet nicht das Konzept der *Berechtigungsebenen*, sondern verwendet *Rollen*. Standardmäßig werden Sie in die Rolle *Netzwerkoperator* eingefügt. Wenn ein Benutzer volle Berechtigungen erhalten soll, müssen Sie diese in die *Netzwerk-Admin*-Rolle eintragen und Sie müssen den TACACS-Server so konfigurieren, dass bei der Anmeldung ein Attribut gedrückt wird. Für TACACS+ übergeben Sie ein benutzerdefiniertes TACACS-Attribut mit dem Wert "roleA" zurück. Für einen Benutzer mit vollem Zugriff verwenden Sie: `cisco-av-pair*shell:roles="network-admin"`

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

```
shell:roles="network-admin"
```

Überprüfen

Verwenden Sie die Befehle in diesem Abschnitt, um die TACACS+-Serverkonfiguration zu überprüfen:

- **show tacacs-server**: Zeigt die TACACS+-Serverkonfiguration an.
- **show aa authentication [login {error-enable} | mschap]**: Zeigt konfigurierte Authentifizierungsinformationen an.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurieren von AAA](#)
- [Konfigurieren von TACACS+](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)