

Konfigurieren von TACACS+ auf Catalyst 1900 und 2820

Inhalt

[Einführung](#)

[Bevor Sie beginnen](#)

[Konventionen](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Zugehörige Informationen](#)

Einführung

Die Software-Version Catalyst 1900/2820 8.x Enterprise Edition unterstützt TACACS+ (nicht XTACACS). Die Einstellungen für TACACS+- oder CiscoSecure-Serverbenutzer für die Authentifizierung sind mit denen für Router-Benutzer identisch. Dieser technische Tipp beschreibt die Konfiguration für Catalyst 1900 und 2820.

Hinweis: Die Failover-Funktion für die Switches 1900 und 2820 wird anders implementiert als für andere Cisco Geräte. Wenn der TACACS+-Server nicht erreichbar ist, können die lokalen Passwörter verwendet werden oder es ist keine Authentifizierung erforderlich (je nach Konfiguration des Switches). Wenn der TACACS+-Server erreichbar ist, der TACACS+-Daemon jedoch nicht verfügbar ist, werden keine lokalen Passwörter und kein Failover auf eine Authentifizierung verwendet (d. h. Sie werden vom Switch ausgeschlossen).

Hinweis: HTTP-Webverbindungen werden immer mit dem lokalen Kennwort authentifiziert (nicht tacacs+). Die Verwendung von Menüoptionen ist bei aktiviertem TACACS+ ungültig. TACACS+ wird für die Befehlszeilenschnittstellenauthentifizierung verwendet.

[Bevor Sie beginnen](#)

[Konventionen](#)

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

[Voraussetzungen](#)

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

[Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konfigurationsschritte

1. Aktivieren Sie über die Befehlszeilenschnittstelle (CLI) die TACACS+-Authentifizierung für die Anmeldung mit dem folgenden Befehl. **Anmeldetaktiken**
2. Verwenden Sie den folgenden Befehl, um dem Switch mitzuteilen, wo sich der Server befindet. **tacacs-server host 1.1.1**
3. Verwenden Sie den folgenden Befehl, um dem Switch mitzuteilen, welchen gemeinsamen Schlüssel er verwendet. **tacacs-server key cisco**
4. Wählen Sie eine der beiden Optionen unten aus. Verwenden Sie den folgenden Befehl, um dem Switch das Kennwort mitzuteilen, das verwendet werden soll, wenn der TACACS+-Server nicht erreichbar ist. **Aktivieren von Kennwort Level 1 Cisco** Verwenden Sie den folgenden Befehl, um den Switch anzuweisen, das lokale Kennwort zu verwenden, wenn der TACACS+-Server nicht erreichbar ist. **tacacs-server last-resort-Kennwort** Verwenden Sie den folgenden Befehl, um den Switch anzuweisen, Benutzer ohne Kennwort einzugeben, wenn der TACACS+-Server nicht erreichbar ist. **tacacs-server Last-Resort-Erfolg** Bevor Sie den Switch beenden, müssen Sie mithilfe von Telnet von einer anderen Sitzung zum Switch wechseln und sicherstellen, dass Sie TACACS+ verwenden können. Stellen Sie vor dem Verlassen des Switches sicher, dass der Server nicht erreichbar ist, ohne TACACS+ verwenden zu müssen. Die übrigen Schritte sind optional.
5. Verwenden Sie den folgenden Befehl, um die TACACS+-Authentifizierung für den Aktivierungsmodus zu aktivieren. **Nutzungstaktiken aktivieren Hinweis:** Dieser Schritt ist nur erforderlich, wenn Benutzer über den TACACS+-Server authentifiziert werden sollen. Es muss auch ein Aktivierungseintrag im Server vorhanden sein, damit dies funktioniert.
6. Verwenden Sie den folgenden Befehl, um die lokale Authentifizierung für den Aktivierungsmodus zu aktivieren, wenn der TACACS+-Server nicht erreichbar ist. **Aktivieren Sie die Kennwortstufe 15 Cisco** Dieses Passwort ist nur gültig, wenn tacacs-server last-resort password ebenfalls konfiguriert ist.
7. Mithilfe des nachstehenden Befehls können Sie die Anzahl der zulässigen Anmeldeversuche auf dem TACACS+-Server konfigurieren. **tacacs-server-Testnummer**
8. Verwenden Sie den folgenden Befehl, um das Zeitüberschreitungsintervall festzulegen, in dem der Serverdaemon reagieren muss (dies ist optional, kann aber in einem langsamen Netzwerk erforderlich sein). **tacacs-server timeout N**

Zugehörige Informationen

- [Technischer Support - Cisco Systems](#)