Fehlerbehebung: CSS und TACACS+

Inhalt

Einführung

Das TACACS+-Protokoll (Terminal Access Controller Access Control System) ermöglicht die Zugriffskontrolle für Router, Network Access Server (NAS) oder andere Geräte über einen oder mehrere Daemon-Server. Er verschlüsselt den gesamten Datenverkehr zwischen NAS und Daemon mithilfe von TCP-Kommunikation für eine zuverlässige Bereitstellung.

Dieses Dokument enthält Informationen zur Fehlerbehebung für den Content Services Switch (CSS) und TACACS+. Sie können den CSS als Client eines TACACS+-Servers konfigurieren und eine Methode für die Authentifizierung von Benutzern sowie für die Autorisierung und Abrechnung von Konfigurations- und Nicht-Konfigurationsbefehlen bereitstellen. Diese Funktion ist in WebNS 5.03 verfügbar.

Hinweis: Weitere Informationen finden Sie unter Konfigurieren des CSS als Client eines TACACS+-Servers.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

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

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Problem

Wenn Sie versuchen, sich bei einem TACACS+-Benutzer beim CSS anzumelden, funktioniert die Anmeldung nicht.

Befehle für Projektmappe und Debuggen

Wenn die TACACS+-Authentifizierung mit einem CSS nicht funktioniert, ist das Problem normalerweise entweder ein Konfigurationsproblem auf dem CSS oder dem TACACS+-Server. Zunächst müssen Sie prüfen, ob Sie den CSS als Client eines TACACS+-Servers konfiguriert haben.

Wenn Sie diese Option aktiviert haben, können Sie auf dem CSS weitere Protokollierungen verwenden, um das Problem zu ermitteln. Führen Sie diese Schritte aus, um die Protokollierung zu aktivieren.

Wechseln Sie auf dem CSS in den Debugmodus.

```
CSS# llama
CSS(debug)# mask tac 0x3
CSS(debug)# exit
CSS# configure
CSS(config)# logging subsystem security level debug-7
CSS(config)# logging subsystem netman level info-6
CSS(config)# exit
CSS# logon
!--- This logs messages to the screen.
```

Führen Sie folgende Befehle aus, um die Protokollierung zu deaktivieren:

```
CSS# llama
CSS(debug)# mask tac 0x0
CSS(debug)# exit
CSS# no logon
```

Diese Meldungen können angezeigt werden:

```
SEP 10 08:30:10 5/1 99 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0c
SEP 10 08:30:10 5/1 100 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:30:10 5/1 101 SECURITY-7: Security Manager sending error 7 reply to
ller 20201c00
```

Diese Meldungen weisen darauf hin, dass der CSS versucht, mit dem TACACS+-Server zu kommunizieren, der TACACS+-Server jedoch den CSS ablehnt. `Fehler 7` bedeutet, dass der im CSS eingegebene TACACS+-Schlüssel nicht mit dem Schlüssel auf dem TACACS+-Server übereinstimmt.

Bei erfolgreicher Anmeldung über einen TACACS+-Server wird diese Meldung angezeigt (beachten Sie, dass die `erfolgreiche 0`-Antwort gesendet wurde):

```
SEP 10 08:31:46 5/1 107 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0d
SEP 10 08:31:46 5/1 108 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:31:47 5/1 109 SECURITY-7: Security Manager sending success 0 reply to
caller 20201c00

SEP 10 08:31:47 5/1 110 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x2020
4b0d
```

Häufige Fehler

Der häufigste Fehler, wenn Sie einen CSS für die Arbeit mit einem TACACS+-Server einrichten, ist eigentlich sehr einfach. Dieser Befehl teilt dem CSS mit, welcher Schlüssel für die Kommunikation mit dem TACACS+-Server verwendet werden soll:

```
CSS(config)# tacacs-server key system enterkeyhere
```

Bei diesem Schlüssel kann es sich um einen Klartext oder einen DES-verschlüsselten Schlüssel handeln. Der Klartext-Schlüssel wird DES-verschlüsselt, bevor der Schlüssel in die aktuelle Konfiguration eingefügt wird. Um einen klaren Text zu verfassen, geben Sie ihn in Anführungszeichen. Verwenden Sie keine Anführungszeichen, um DES zu verschlüsseln. Es ist wichtig zu wissen, ob der TACACS+-Schlüssel DES-verschlüsselt ist oder ob der Schlüssel ein eindeutiger Text ist. Nachdem Sie den Befehl ausgegeben haben, ordnen Sie den Schlüssel des CSS dem Schlüssel zu, den der TACACS+-Server verwendet.

Zugehörige Informationen

- Konfigurieren des CSS als Client eines TACACS+-Servers
- Konfigurieren von TACACS+ und Extended TACACS+
- Technischer Support und Dokumentation - Cisco Systems