

# Nexus Switch der Serie 7000 - Problem mit Remote-Benutzerauthentifizierung über SSH mit einem TACACS-Konto

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Symptome](#)

[Bedingungen](#)

[Fehlerbehebung](#)

[Lösung](#)

[Bestätigung](#)

[Problemumgehungen](#)

[Gelöste Versionen](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument beschreibt die erforderlichen Schritte, um eine Fehlerbehebung durchzuführen und sicherzustellen, dass ein Cisco Nexus Switch der Serie 7000 von dem bekannten Softwarefehler [Cisco Bug-ID CSCud02139](#) betroffen ist.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Nexus Switches der Serie 7000
- Cisco Nexus-Betriebssystem (NX-OS), Versionen 5.2(5) bis 5.2(7)
- Cisco NX-OS, Versionen 6.0(1) bis 6.1(3)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Problem

### Symptome

Benutzer können sich nicht remote bei einem Nexus Switch der Serie 7000 mit Virtual Device Context (VDC) mit TACACS-Authentifizierung anmelden.

Zusätzlich werden die folgenden Meldungen in den Protokollen angezeigt:

```
n7k-vdc-1# show log last 200 | grep TACACS
2013 May 13 17:17:31 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:17:46 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:06 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:12 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:16 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:20:26 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:20:39 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:21:50 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:22:09 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
n7k-vdc-1#
```

### Bedingungen

Dieses Problem tritt auf Switches der Serie Nexus 7000 auf, auf denen Cisco NX-OS-Versionen zwischen 5.2(5) und 5.2(7) sowie zwischen 6.0.1 und 6.1(3) ausgeführt werden.

Der VDC muss die TACACS-Authentifizierung verwenden, wie im folgenden Beispiel gezeigt:

```
n7k-vdc-1# show run tacacs+

!Command: show running-config tacacs+
!Time: Mon May 13 17:20:57 2013

version 6.1(2)
```

```
feature tacacs+

ip tacacs source-interface mgmt0
tacacs-server timeout 30
tacacs-server host 192.0.2.9 key 7 "keypassword"
aaa group server tacacs+ default
server 192.0.2.9
use-vrf management
```

```
n7k-vdc-1# show run aaa
```

```
!Command: show running-config aaa
!Time: Mon May 13 17:21:30 2013
```

```
version 6.1(2)
aaa authentication login default group default
aaa authorization config-commands default group default
aaa authorization commands default group default
aaa accounting default group default
no aaa user default-role
aaa authentication login error-enable
tacacs-server directed-request
```

## Fehlerbehebung

### 1. TACACS-Serverstatus bestätigen

Vergewissern Sie sich, dass der Nexus Switch der Serie 7000 erfolgreich Pings an den TACACS-Server über das richtige Virtual Routing and Forwarding (VRF) senden kann. Bestätigen Sie, dass der TACACS-Server Benutzer auf anderen Geräten weiterhin erfolgreich authentifiziert.

### 2. Überprüfen der AAA-Fehlerprotokolle (Authentication, Authorization, and Accounting)

Verwenden Sie diesen Befehl, um die AAA-Prozessfehlerprotokolle zu überprüfen:

```
n7k-vdc-1# show system internal aaa event-history errors
```

```
1) Event:E_DEBUG, length:54, at 786852 usecs after Mon May 13 17:22:09 2013
[102] All Configured methods failed for default:default
```

```
2) Event:E_DEBUG, length:53, at 786796 usecs after Mon May 13 17:22:09 2013
[102] protocol TACACS failed with server group default
```

```
3) Event:E_DEBUG, length:54, at 379206 usecs after Mon May 13 17:22:09 2013
[102] All Configured methods failed for default:default
```

```
4) Event:E_DEBUG, length:53, at 379172 usecs after Mon May 13 17:22:09 2013
[102] protocol TACACS failed with server group default
```

```
5) Event:E_DEBUG, length:54, at 89083 usecs after Mon May 13 17:21:51 2013
[102] All Configured methods failed for default:default
```

```
6) Event:E_DEBUG, length:53, at 89051 usecs after Mon May 13 17:21:51 2013
[102] protocol TACACS failed with server group default
```

### 3. Überprüfen der Fehlerprotokolle des TACACS+-Prozesses

Verwenden Sie diesen Befehl, um die Fehlerprotokolle des TACACS+-Prozesses zu überprüfen:

```
n7k-vdc-1# show system internal tacacs+ event-history errors
```

```
1) Event:E_DEBUG, length:88, at 786728 usecs after Mon May 13 17:22:09 2013
[100] switch_tac_server: Unreachable servers case .setting error code for
aaa session 0

2) Event:E_DEBUG, length:77, at 786726 usecs after Mon May 13 17:22:09 2013
[100] switch_tac_server: no more server in the server group for
aaa session 0

3) Event:E_DEBUG, length:103, at 786680 usecs after Mon May 13 17:22:09 2013
[100] connect_tac_server: non blocking connect failed, switching server for
aaa session id(0) rtvalue(3)

4) Event:E_DEBUG, length:97, at 786677 usecs after Mon May 13 17:22:09 2013
[100] non_blocking_connect(171): getaddrinfo(DNS cache fail) with retcode:-1
for server:192.0.2.9

5) Event:E_DEBUG, length:62, at 786337 usecs after Mon May 13 17:22:09 2013
[100] tplus_encrypt(655):key is configured for this aaa session.

6) Event:E_DEBUG, length:95, at 786287 usecs after Mon May 13 17:22:09 2013
[100] tplus_make_acct_request(1343):Not calling the name-resolution routine
as rem_addr is empty

7) Event:E_DEBUG, length:63, at 786285 usecs after Mon May 13 17:22:09 2013
[100] tplus_make_acct_request(1308):Accounting userdata&colon;console0

8) Event:E_DEBUG, length:63, at 786266 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:Global source-interface mgmt0

9) Event:E_DEBUG, length:48, at 785842 usecs after Mon May 13 17:22:09 2013
[100] is_intf_up_with_valid_ip(1129):Port is up.

10) Event:E_DEBUG, length:57, at 785812 usecs after Mon May 13 17:22:09 2013
[100] is_intf_up_with_valid_ip(1126):Proper IOD is found.

11) Event:E_DEBUG, length:52, at 785799 usecs after Mon May 13 17:22:09 2013
[100] Exiting function: get_if_index_from_global_conf

12) Event:E_DEBUG, length:66, at 785797 usecs after Mon May 13 17:22:09 2013
[100] Function get_if_index_from_global_conf: found interface mgmt0

13) Event:E_DEBUG, length:53, at 785783 usecs after Mon May 13 17:22:09 2013
[100] Entering function: get_if_index_from_global_conf

14) Event:E_DEBUG, length:68, at 785781 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:Falling to globally configured one

15) Event:E_DEBUG, length:79, at 785779 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:No source-interface configured for this group
```

### 4. Debuggen von TACACS+-Authentifizierungsanforderungen

Aktivieren Sie das Debuggen für TACACS+-Authentifizierungsanforderungen. Beim AAA-Debugging werden folgende Protokolle ausgegeben:

```
n7k-vdc-1# debug tacacs+ aaa-request
n7k-vdc-1# show logging logfile last 5
2013 May 13 18:20:26.077572 tacacs: tplus_encrypt(655):key is configured
for this aaa session.
2013 May 13 18:20:26.077918 tacacs: non_blocking_connect(171): getaddrinfo
DNS cache fail) with retcode:-1 for server:192.0.2.9
2013 May 13 18:20:26.077938 tacacs: connect_tac_server: non blocking connect
failed, switching server for aaa session id(0) rtvalue(3)
2013 May 13 18:20:26.077978 tacacs: switch_tac_server: no more server in the
server group for aaa session 0
2013 May 13 18:20:26.077993 tacacs: switch_tac_server: Unreachable servers
case .setting error code for aaa session 0
```

## 5. Durchführen einer Paketerfassung auf dem TACACS-Server

Eine Paketerfassung auf dem TACACS-Server zeigt, dass keine Pakete vom VDC eingehen.

## 6. Ethalyzer-Erfassung für Nexus-Switch der Serie 7000

Eine Erfassung durch Ethalyzer zeigt, dass keine Pakete an den TACACS-Server ausgehen.

## 7. Überprüfen der ausgeführten Prozesse im VDC

Der Befehl **show proc cpu sort** zeigt 33 Instanzen (32 nicht mehr funktionsfähig) des ausgeführten TACACSD-Prozesses an.

```
n7k-vdc-1# show proc cpu sort | include tacacs
1538 16 16 1014 0.0% tacacsd
1855 16 10 1625 0.0% tacacsd
2163 16 10 1678 0.0% tacacsd
2339 15 23 676 0.0% tacacsd
3820 15 10 1595 0.0% tacacsd
3934 16 13 1272 0.0% tacacsd
4416 25 8 3211 0.0% tacacsd
4470 16 23 734 0.0% tacacsd
5577 26 12 2191 0.0% tacacsd
6592 969767 14589069 66 0.0% tacacs
6934 16 13 1297 0.0% tacacsd
8878 16 13 1252 0.0% tacacsd
8979 16 12 1345 0.0% tacacsd
10153 26 11 2453 0.0% tacacsd
10202 15 8 1888 0.0% tacacsd
10331 26 11 2368 0.0% tacacsd
10482 16 14 1190 0.0% tacacsd
14148 15 11 1433 0.0% tacacsd
14385 14 10 1496 0.0% tacacsd
14402 15 9 1775 0.0% tacacsd
20678 16 9 1785 0.0% tacacsd
20836 16 13 1246 0.0% tacacsd
21257 15 13 1212 0.0% tacacsd
```

```
21617 15 9 1749 0.0% tacacsd
22159 15 12 1328 0.0% tacacsd
23776 15 12 1320 0.0% tacacsd
24017 25 9 2788 0.0% tacacsd
29496 15 8 1990 0.0% tacacsd
29972 15 11 1368 0.0% tacacsd
30111 25 9 2847 0.0% tacacsd
30204 15 9 1721 0.0% tacacsd
30409 16 13 1254 0.0% tacacsd
32410 15 8 1876 0.0% tacacsd
```

## Lösung

Der VDC erkennt den bekannten Softwarefehler: Cisco Bug-ID: [CSCud02139](#).

Der TACACSD-Prozess erzeugt untergeordnete Prozesse, die hängen bleiben. Dies erreicht maximal 32 Prozesse, und es kann nicht mehr gelauncht werden, um die Authentifizierung zu bestehen.

## Bestätigung

1. Bestätigen Sie, dass es 33 Instanzen von TACACSD gibt. Sie können den Befehl **show proc cpu sort | grep -c 'tacacsd'**, um die Instanzen zu zählen.
2. Erfassen Sie den Ethalyzer, und stellen Sie sicher, dass die Anfrage den Nexus Switch der Serie 7000 nicht verlässt.
3. Ordnen Sie die vorherigen Protokollmeldungen zu.

## Problemumgehungen

Es gibt drei Möglichkeiten. Entfernen Sie alle TACACS-Konfigurationen, und entfernen Sie die Funktion sowie die Konfiguration, und lesen Sie sie. Eine weitere Option besteht darin, einen Supervisor-Switchover durchzuführen. Sie können den VDC auch neu laden.

## Gelöste Versionen

- NX-OS Version 5.2(9) und höher im 5.2 Train
- NX-OS Version 6.1(3) und höher im Zug 6.1

## Zugehörige Informationen

- [Cisco Bug-Toolkit - Cisco Bug-ID CSCud02139](#)
- [Technische Übersicht zu Virtual Device Contexts](#)
- [Ethalyzer: Integriertes Dienstprogramm zur Paketerfassung der Cisco NX-OS-Software](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.