

# Nexus 7000 Series Switch Probleem met externe gebruikersverificatie via SSH met een TACACS-account

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Symptomen](#)

[Voorwaarden](#)

[Problemen oplossen](#)

[Oplossing](#)

[Bevestiging](#)

[Voorwendselen](#)

[Opgeloste versies](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document bevat de stappen die nodig zijn om problemen op te lossen en te bevestigen dat een Cisco Nexus 7000 Series switch is beïnvloed door het bekende softwarestoornis [Cisco bug-id CSC02139](#).

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Nexus 7000 Series Switches

- Cisco Nexus Operating System (NX-OS) versies 5.2(5) tot en met 5.2(7) Inclusief
- Cisco NX-OS versies 6.0(1) tot en met 6.1(3) inclusief

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Probleem

### Symptomen

Gebruikers kunnen niet op afstand inloggen op een Nexus 7000 Series switch Virtual Device Context (VDC) met TACACS-verificatie.

Bovendien, worden deze berichten gezien in de logboeken:

```
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#
```

### Voorwaarden

Dit probleem wordt aangetroffen op Nexus 7000 Series switches waarop Cisco NX-OS-versies tussen 5.2(5) en 5.2(7) en tussen 6.0.1 en 6.1(3) worden uitgevoerd.

De VDC moet Tacacs-verificatie gebruiken, zoals dit voorbeeld:

```
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
```

## Problemen oplossen

### 1. De status van de TACACS-server bevestigen

Bevestig dat de Nexus 7000 Series switch met succes de TACACS-server kan pingen via de juiste virtuele routing en doorsturen (VRF). Bevestig dat de TACACS-server nog steeds met succes gebruikers op andere apparaten authenticceert.

### 2. Controleer de foutenlogs van het verificatie-, autorisatie- en accounting (AAA) proces

Gebruik deze opdracht om de logboeken met AAA-procesfouten te controleren:

```
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. Controleer de foutenlogboeken in het TACACS+-proces

Gebruik deze opdracht om de foutlogboeken van het TACACS+-proces te controleren:

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. Debug TACACS+ verificatieaanvragen

Zet het zuiveren voor de verzoeken van de Verificatie TACACS+ aan.AAA-debugging voert deze logboeken uit:

```

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. Voer een pakketvastlegging op de TACACS-server uit

Een pakketopname op de TACACS-server toont aan dat er geen pakketten uit de VDC komen.

## 6. Voer een Ethalyzer Capture uit op de Nexus 7000 Series Switch

Een Ethalyzer-opname laat zien dat er geen pakketten naar de TACACS-server vertrekken.

## 7. Controleer de lopende processen op de VDC

Het `cpu` sorteercommando `show` toont 33 exemplaren (32 niet meer actief) van het TACACSD proces.

```

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
```

## Oplossing

De VDC stuit op het bekende softwaredefect Cisco bug-id [CSC02139](#).

Het TACACSD-proces spaait kinderprocessen die vastzitten. Dit bereikt een maximum van 32 processen, en het is niet in staat om nog meer te kweken om de authenticatie te overgaan.

## Bevestiging

1. Bevestig dat er 33 gevallen van TACACSD zijn. U kunt de opdracht **show proc cpu sortering** gebruiken | **grep -c 'tacacsd'** om de gevallen te tellen.
2. Voer een ethanalyzer op en bevestig dat het verzoek de Nexus 7000 Series switch niet verlaat.
3. Overeenkomen met de vorige logberichten.

## Voorwendselen

Er zijn drie mogelijkheden. Verwijder alle TACACS-configuratie en verwijder en lees de optie en de configuratie. Een andere optie is om een supervisor switchover uit te voeren. Of je kunt de VDC opnieuw laden.

## Opgeloste versies

- NX-OS-versies 5.2(9) en Later in de 5.2-trein
- NX-OS-versies 6.1(3) en later in de 6.1-trein

## Gerelateerde informatie

- [Cisco Bug Toolkit - Cisco bug-id CSCud02139](#)
- [Technisch overzicht van virtuele apparaatcontexten](#)
- [Ethanalyzer: Cisco NX-OS-software, ingebouwd pakketvastlegging hulpprogramma](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.