# Problema dello switch Nexus serie 7000 con autenticazione utente remota tramite SSH con un account TACACS

## Sommario



## Introduzione

In questo documento viene descritto come risolvere i problemi e verificare che uno switch Cisco Nexus serie 7000 sia interessato dal difetto software Cisco ID bug CSCud02139.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Nexus serie 7000 Switch

- Sistema operativo Cisco Nexus (NX-OS) versioni da 5.2(5) a 5.2(7) incluse
- Cisco NX-OS versioni da 6.0(1) a 6.1(3) incluse

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Problema

## Sintomi

Gli utenti non possono accedere in remoto a uno switch Nexus serie 7000 Virtual Device Context (VDC) con autenticazione TACACS.

Inoltre, questi messaggi vengono visualizzati nei log:

```
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#
```

## Condizioni

Questo problema si verifica sugli switch Nexus serie 7000 con Cisco NX-OS versione 5.2(5) e 5.2(7), nonché tra la 6.0.1 e la 6.1(3).

Il VDC deve utilizzare l'autenticazione TACACS, come nell'esempio seguente:

```
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
```

## Risoluzione dei problemi

1. Confermare lo stato del server TACACS

   Confermare che lo switch Nexus serie 7000 sia in grado di eseguire correttamente il ping sul server TACACS tramite il VRF (Virtual Routing and Forwarding) corretto.Confermare che il server TACACS autentica comunque correttamente gli utenti su altri dispositivi.
2. Controllare i log degli errori del processo di autenticazione, autorizzazione e accounting (AAA)

   Per controllare i log degli errori del processo AAA, usare questo comando:

   ```
   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. Controllare i log degli errori di elaborazione TACACS+

Utilizzare questo comando per controllare i log degli errori di processo TACACS+:

```
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 delle richieste di autenticazione TACACS+**

Attiva debug per richieste di autenticazione TACACS+.Il debug AAA genera i seguenti log:

```
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. **Acquisizione di pacchetti sul server TACACS**

   Un'operazione di acquisizione sul server TACACS mostra che il VDC non invia pacchetti.

6. **Eseguire un'acquisizione con etanalyzer sullo switch Nexus serie 7000**

   L'acquisizione di Ethanalyzer indica che nessun pacchetto viene inviato al server TACACS.

7. **Controllare i processi in esecuzione sul controller di dominio virtuale**

   Il comando **show proc cpu sort** mostra 33 istanze (32 inattive) del processo TACACSD in esecuzione.

```
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
```

# Soluzione

Il VDC rileva il difetto software noto. ID bug Cisco CSCud02139.

Il processo TACACSD genera processi secondari che rimangono bloccati. In questo modo si raggiunge un massimo di 32 processi e non è più possibile generare codice per superare l'autenticazione.

## Conferma

1. Confermare la presenza di 33 istanze di TACACSD. È possibile utilizzare il comando **show proc cpu sort | grep -c 'tacacsd'** per contare le istanze.
2. Eseguire un'acquisizione con etanalyzer e verificare che la richiesta non lasci lo switch Nexus serie 7000.
3. Corrispondono ai messaggi di registro precedenti.

## Soluzioni

Ci sono tre possibilità. Rimuovere tutta la configurazione TACACS, quindi rimuovere e leggere la funzionalità e la configurazione. Un'altra opzione è quella di eseguire il cambio del supervisore. In alternativa, è possibile ricaricare il VDC.

## Versioni risolte

- NX-OS versione 5.2(9) e successive nel treno 5.2
- NX-OS versione 6.1(3) e successive nel treno 6.1

# Informazioni correlate

- Cisco Bug Toolkit - ID bug Cisco CSCud02139
- Panoramica tecnica dei contesti dei dispositivi virtuali
- Ethanalyzer: Utilità di acquisizione pacchetti integrata del software Cisco NX-OS
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).