

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[症状](#)

[条件](#)

[トラブルシューティング](#)

[解決策](#)

[確認](#)

[回避策](#)

[解決済みバージョン](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Nexus 7000 シリーズ スイッチの問題をトラブルシューティングし、その原因が既知のソフトウェア欠陥である [Cisco Bug ID CSCud02139](#) であることを確認するために必要な手順について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Nexus 7000 シリーズ スイッチ
- Cisco Nexus オペレーティング システム (NX-OS) バージョン 5.2(5) から 5.2(7) まで
- Cisco NX-OS バージョン 6.0(1) から 6.1(3) まで

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

問題

症状

ユーザが Nexus 7000 シリーズ スイッチ仮想デバイス コンテキスト (VDC) に TACACS 認証でリモート ログインできない。

さらに、ログには以下のメッセージが記録される。

```
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#
```

条件

この問題は、Cisco NX-OS の 5.2(5) から 5.2(7) までのバージョンならびに 6.0.1 から 6.1(3) までのバージョンを実行している Nexus 7000 シリーズ スイッチで発生します。

以下に、VDC が使用しなければならない TACACS 認証の例を示します。

```
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
```

トラブルシューティング

1. TACACS サーバのステータスを確認する

Nexus 7000 シリーズ スイッチが、正しい Virtual Routing and Forwarding (VRF) を介して TACACS サーバを正常に ping できることを確認します。TACACS サーバが引き続き他のデバイス上のユーザを正常に認証できることを確認します。

2. 認証、認可、およびアカウントिंग (AAA) プロセスのエラー ログを確認する

以下のコマンドを使用して、AAA プロセスのエラー ログを確認します。

```
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. TACACS+ プロセスのエラー ログを確認する

以下のコマンドを使用して、TACACS+ プロセスのエラー ログを確認します。

```
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: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. TACACS+ 認証要求をデバッグする

TACACS+ 認証要求のデバッグをオンにします。AAA デバッグにより、以下のログが出力されます。

```
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. TACACS サーバ上でパケット キャプチャを実行する

TACACS サーバ上でのパケット キャプチャにより、VDC から到着するパケットがないこと

が表示されます。

6. Nexus 7000 シリーズ スイッチ上で Ethalyzer キャプチャを実行する

Ethalyzer キャプチャにより、TACACS サーバに送信されるパケットがないことが示されます。

7. VDC で実行中のプロセスを確認する

`show proc cpu sort` コマンドにより、実行中の TACACSD プロセスの 33 のインスタンスが表示されます (そのうち、32 のインスタンスは機能していません)。

```
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
```

解決策

VDC で、既知のソフトウェア欠陥である Cisco Bug ID [CSCud02139](#) が発生しています。

TACACSD プロセスが生成している子プロセスが溜まっています。そのようなプロセスの数が 32 に達すると、認証を行うための子プロセスをそれ以上生成できなくなります。

確認

1. TACACSD のインスタンス数が 33 であることを確認します。コマンド `show proc cpu sort | grep -c 'tacacsd'` を使用すると、インスタンスをカウントできます。
2. Ethalyzer キャプチャを実行し、要求が Nexus 7000 シリーズ スイッチから先に渡されないことを確認します。
3. 前のログ メッセージと照合します。

回避策

3 つの方法があります。TACACS コンフィギュレーションを完全に削除し、この機能とコンフィギュレーションを追加し直します。別のオプションとしては、スーパーバイザ スイッチオーバーを実行する方法もあります。あるいは、VDC をリロードすることもできます。

解決済みバージョン

- 5.2 トレインの NX-OS Versions 5.2(9) 以降
- 6.1 トレインの NX-OS Versions 6.1(3) 以降

関連情報

- [Cisco Bug Toolkit - Cisco Bug ID CSCud02139](#)
- [仮想デバイス コンテキストの技術概要](#)
- [Ethalyzer : Cisco NX-OS ソフトウェアの組み込みパケット キャプチャ ユーティリティ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)