TACACS 계정이 있는 SSH를 통한 원격 사용자 인증의 Nexus 7000 Series 스위치 문제

목차

소개

이 문서에서는 Cisco Nexus 7000 Series 스위치가 알려진 소프트웨어 결함 Cisco 버그 ID CSCud02139의 영향을 받는지 확인하고 문제를 해결하는 데 필요한 단계를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Nexus 7000 Series Switch
- Cisco Nexus 운영 체제(NX-OS) 버전 5.2(5) - 5.2(7)(포함)
- Cisco NX-OS 버전 6.0(1) - 6.1(3)(포함)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

증상

사용자는 TACACS 인증을 통해 Nexus 7000 Series 스위치 VDC(Virtual Device Context)에 원격으로 로그인할 수 없습니다.

또한 다음 메시지가 로그에 표시됩니다.

```
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#
```

조건

이 문제는 Cisco NX-OS 버전을 실행하는 Nexus 7000 Series 스위치에서 5.2(5)와 5.2(7) 사이, 그리고 6.0.1과 6.1(3) 사이에서 발생합니다.

VDC는 다음 예와 같이 TACACS 인증을 사용해야 합니다.

```
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
```

문제 해결

1. TACACS 서버 상태 확인

   Nexus 7000 Series 스위치가 올바른 VRF(Virtual Routing and Forwarding)를 통해 TACACS 서버에 성공적으로 ping할 수 있는지 확인합니다.TACACS 서버가 여전히 다른 디바이스의 사용자를 성공적으로 인증하는지 확인합니다.
2. AAA(Authentication, Authorization, and Accounting) 프로세스 오류 로그 확인

   AAA 프로세스 오류 로그를 확인하려면 다음 명령을 사용합니다.

```
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+ 프로세스 오류 로그 확인

   TACACS+ 프로세스 오류 로그를 확인하려면 다음 명령을 사용합니다.

```
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. TACACS+ 인증 요청 디버그

TACACS+ 인증 요청에 대한 디버깅을 켭니다.AAA 디버깅은 다음 로그를 출력합니다.

```
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 서버에서 패킷 캡처 수행**

   TACACS 서버의 패킷 캡처에서는 VDC에서 패킷이 도착하지 않음을 보여줍니다.

6. **Nexus 7000 Series 스위치에서 Ethanalyzer 캡처 수행**

   Ethanalyzer 캡처는 패킷이 TACACS 서버로 이그레스(egress)되지 않음을 보여줍니다.

7. **VDC에서 실행 중인 프로세스를 확인합니다.**

   show **proc cpu sort** 명령은 실행 중인 TACACSD 프로세스의 33개 인스턴스(32개의 존재하지 않음)를 표시합니다.

```
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
```

솔루션

VDC에 알려진 소프트웨어 결함 Cisco 버그 ID CSCud02139가 있습니다.

TACACCSD 프로세스는 중단되는 하위 프로세스를 생성합니다. 이 프로세스는 최대 32개 프로세스에 도달하며 인증을 통과하기 위해 더 이상 실행할 수 없습니다.

확인

1. 33개의 TACACSD 인스턴스가 있는지 확인합니다. **show proc cpu sort** 명령을 사용할 수 있습니다 **| grep -c 'tacacsd'**를 사용하여 인스턴스를 계산합니다.
2. ethanalyzer 캡처를 수행하고 요청이 Nexus 7000 Series 스위치에서 나가지 않는지 확인합니다.
3. 이전 로그 메시지와 일치시킵니다.

해결 방법

세 가지 가능성이 있습니다. 모든 TACACS 컨피그레이션을 제거하고, 기능 및 컨피그레이션을 제거한 후 읽습니다. 또 다른 옵션은 수퍼바이저 전환을 수행하는 것입니다. 또는 VDC를 다시 로드할 수 있습니다.

해결된 버전

- NX-OS 버전 5.2(9) 이상(5.2 열차)
- NX-OS 버전 6.1(3) 이상(6.1 열차)

관련 정보

- Cisco 버그 툴킷 - Cisco 버그 ID CSCud02139
- 가상 장치 컨텍스트의 기술 개요
- Ethanalyzer: Cisco NX-OS Software 내장형 패킷 캡처 유틸리티
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.