

CPS에서 서브스크립션 변경 후 PPPoE 세션의 비종료 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[문제 재현 단계](#)

[COA와 관련하여 주목해야 할 주요 사항 및 그 중단](#)

[솔루션](#)

소개

이 문서에서는 CPS(Cisco Policy Suite) over Radius 프로토콜에서 서브스크립션 변경 후 PPPoE 세션의 비종료 문제를 해결하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 리눅스
- CPS
- RADIUS 프로토콜

Cisco에서는 다음 권한 액세스를 권장합니다.

- CPS CLI에 대한 루트 액세스
- CPS GUI에 대한 "qns-svn" 사용자 액세스(정책 작성기 및 제어 센터)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CPS 13.1
- UCS-B

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다.

배경 정보

CPS는 PPPoE(Point-to-Point Protocol over Ethernet) 가입자를 지원하기 위해 AAA(Authentication, Authorization, and Accounting) 서버/클라이언트 모델로 작동하도록 설계되었습니다. CPS는 ASR9K 또는 ASR1K 디바이스와 상호 작용하여 PPPoE 세션을 관리합니다.

문제

PPPoE 세션은 외부 프로비저닝 시스템에서 SOAP(Simple Object Access Protocol) API(Application Programming Interface) 요청을 통해 CPS에서 새 서브스크립션을 선택한 후 연결을 끊고 다시 연결하지 않습니다.

CPS는 COA(Change of Action) 요청을 생성하여 ASR9K 디바이스로 전송할 수 있지만 이러한 요청은 ASR9K 디바이스에서 "No response Timeout Error(응답 시간 초과 오류 없음)"로 시간 초과됩니다.

다음은 샘플 오류 메시지입니다.

```
dc1-1b01 dc1-1b01 2021-09-28 21:26:13,331 [pool-2-thread-1] ERROR
c.b.p.r.jms.PolicyActionJmsReceiver - Error executing RemoteAction. Returning Error Message
response
com.broadhop.exception.BroadhopException: Timeout: No Response from RADIUS Server
    at com.broadhop.radius.impl.actions.AsynchCoARequest.execute(AsynchCoARequest.java:213)
~[com.broadhop.radius.service_13.0.1.r150127.jar:na]
    at
com.broadhop.utilities.policy.remote.RemoteActionStub.execute(RemoteActionStub.java:62)
~[com.broadhop.utility_13.0.0.release.jar:na]
    at
com.broadhop.policy.remote.jms.PolicyActionJmsReceiver$RemoteActionExecutor.run(PolicyActionJmsReceiver.java:98) ~[com.broadhop.policy.remote.jms_13.0.0.release.jar:na]
    at
com.broadhop.utilities.policy.async.PolicyRemoteAsyncActionRunnable.run(PolicyRemoteAsyncActionRunnable.java:24) [com.broadhop.utility_13.0.0.release.jar:na]
    at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511) [na:1.8.0_72]
    at java.util.concurrent.FutureTask.run(FutureTask.java:266) [na:1.8.0_72]
    at
com.broadhop.utilities.policy.async.AsyncPolicyActionExecutionManager$GenericThread.run(AsyncPolicyActionExecutionManager.java:301) [com.broadhop.utility_13.0.0.release.jar:na]
Caused by: net.jradius.exception.TimeoutException: Timeout: No Response from RADIUS Server
    at net.jradius.client.RadiusClientTransport.sendReceive(RadiusClientTransport.java:112)
~[na:na]
    at net.jradius.client.RadiusClient.changeOfAuth(RadiusClient.java:383) ~[na:na]
    at com.broadhop.radius.impl.actions.AsynchCoARequest.execute(AsynchCoARequest.java:205)
~[com.broadhop.radius.service_13.0.1.r150127.jar:na]
... 6 common frames omitted
```

문제 재현 단계

1단계. ASR9K 또는 ASR1K 디바이스에서 PPPoE 세션을 시작하고 Control Center를 통해 CPS에서 해당 세션이 표시되는지 확인합니다.

2단계. 가입자와 연결된 서비스 구독을 업데이트하는 SOAP API 요청을 시작합니다.

The image shows a Wireshark capture of a SOAP API request. The packet list pane shows three packets: a TCP ACK (No. 2665), an HTTP POST (No. 2666), and a TCP ACK (No. 2667). The packet details pane for packet 2666 shows the following structure:

- Frame 2666: 1348 bytes on wire (10784 bits), 1348 bytes captured (10784 bits)
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 10.210.226.1, Dst: 10.210.226.2
- Transmission Control Protocol, Src Port: 32928, Dst Port: 8080, Seq: 2897, Ack: 1, Len: 1280
- [2 Reassembled TCP Segments (4176 bytes): #2665(2896), #2666(1280)]
- Hypertext Transfer Protocol
- eXtensible Markup Language
 - <?xml
 - <SOAP-ENV:Envelope
 - xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 - xmlns:ns1="http://broadhop.com/unifiedapi/soap/types">
 - <SOAP-ENV:Body>
 - <ns1:UpdateSubscriberRequest>
 - <ns1:subscriber>
 - <ns1:id>
 - <ns1:name>
 - <ns1:credential>
 - <ns1:status>
 - <ns1:avp>
 - <ns1:avp>
 - <ns1:avp>
 - <ns1:version>
 - <ns1:subAccount>
 - <ns1:subAccount>
 - </ns1:subscriber>
 - </ns1:UpdateSubscriberRequest>
 - </SOAP-ENV:Body>
 - </SOAP-ENV:Envelope>

3단계. CPS는 ASR9K 또는 ASR1K에 대한 COA 요청을 시작합니다. CPS에서 동일한 COA의 중복 요청을 사용하여 동일한 리q를 재시도하는 것을 확인할 수 있습니다.

The image shows a Wireshark capture of RADIUS CoA-Request packets. The packet list pane shows four packets, all with the same source and destination IP addresses (10.210.226.1 to 10.210.226.2) and the same protocol (RADIUS). The packet details pane for packet 2675 shows the following structure:

- Frame 2675: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 10.210.226.1, Dst: 10.210.226.2
- User Datagram Protocol, Src Port: 34761, Dst Port: 1700
- RADIUS Protocol
 - Code: CoA-Request (43)
 - Packet identifier: 0x4d (77)
 - Length: 90
 - Authenticator: dfdbe5861de70c1a39d5b0fb9350b1d0
 - Attribute Value Pairs
 - AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
 - AVP: t=Acct-Session-Id(44) l=10 val=0477a980
 - AVP: t=User-Name(1) l=19 val=...

참고: 첫 번째 패킷은 피어 디바이스(ASR9K)에서 승인되지 않으므로 CPS의 내부 로직에서는 재시도 메커니즘을 트리거하고 중복 요청을 보냅니다.

4단계. CPS는 첫 번째 세션 COA 요청 및 재시도에 대한 응답이 없으므로 다른 모든 세션 업데이트 작업을 삭제합니다.

이를 통해 PPPoE 세션이 ASR9K에서 여전히 활성 상태이고 세션 새로 고침을 위해 CPS에 세션 연결 끊기 요청이 전송되지 않았음을 확인할 수 있습니다. CPS는 COA 요청과 관련하여 ASR9K의 계정 중지 요청을 예상합니다.

COA와 관련하여 주목해야 할 주요 사항 및 그 중단

1. CPS는 데이터베이스에 있는 특정 가입자에 대한 모든 세션에 대한 COA 요청을 시작합니다.
2. CPS에서 특정 COA 요청에 대해 ACK 또는 NACK를 수신하지 않으면 정책 작성기의 컨피그레이션에 따라 재시도 메커니즘을 시작합니다.
3. 재시도 횟수 및 재시도 사이의 기간은 구성 가능합니다.

The screenshot shows the configuration interface for a Generic RADIUS Device Pool. The 'General Selection' tab is active. The configuration includes:

- Name:** default
- Description:** (empty)
- Default Shared Secret:** (empty)
- Default CoA Shared Secret:** (empty)
- * CoA Port:** 1700
- * CoA Retries:** 3
- * CoA Timeout Seconds:** 3
- Correlation Key:** AccountSessionId
- * Access Request Guard Timer (Milliseconds):** 0
- Coa Disconnect Template:** (empty)
- Disconnect Template:** (empty)
- Proxy Access Accept Filter:** (empty)
- Dup Check With Framed Ip
- Dup Check With Mac Address
- Radius Network Session Correlation
- Control Session Lifecycle

샘플 재시도 컨피그레이션

이션

솔루션

이 문제를 해결하려면 ASR9K로 추가 분석을 확장해야 하며, COA 요청 및 재시도에 대해 CPS에 다시 응답하지 않는 이유를 찾아야 합니다.

스니퍼 추적에서 CPS의 로드 밸런서(LB01)가 <IP-1>에서 COA를 소스 하고 기본 경로인 eth1을 통해 패킷을 라우팅하는 것을 확인할 수 있습니다.

다른 로드 밸런서(LB02)는 <IP-2>에서 COA를 제공하며 eth2를 통해 특정 경로를 사용합니다.

ASR9K에는 COA가 <IP-1>에서 오는 경우에만 ACL(Access List)이 수락됩니다.

따라서 CPS의 LB01에 있는 경로 테이블을 수정하여 적절한 소스 IP로 COA를 전송해야 합니다(즉, 특정 경로를 통해 <IP-2>).

서브스크립션 변경에 대한 엔드 투 엔드 RADIUS 트랜잭션의 성공적인 결과를 확인할 수 있으며, 필요한 수정 사항을 CPS LB 경로 테이블에 게시할 수 있습니다.

(radius.User_Name == " ") || (frame.number == 3444)

No.	Time	Source	Destination	Protocol	Time	Info
2934	2021-10-05 13:27:06.517	10.10.10.1	10.10.10.1	RADIUS		CoA-Request id=101
2939	2021-10-05 13:27:06.788	10.10.10.1	10.10.10.5	RADIUS		Accounting-Request id=234
2989	2021-10-05 13:27:09.047	10.10.10.1	10.10.10.1	RADIUS		CoA-Request id=102
2990	2021-10-05 13:27:09.056	10.10.10.1	10.10.10.5	RADIUS		CoA-NAK id=102
3384	2021-10-05 13:27:30.193	10.10.10.1	10.10.10.5	RADIUS		Access-Request id=145
3443	2021-10-05 13:27:33.666	10.10.10.1	10.10.10.5	RADIUS		Accounting-Request id=167
3444	2021-10-05 13:27:33.673	10.10.10.5	10.10.10.1	RADIUS		Accounting-Response id=167