

Risolvere i problemi relativi alla non interruzione della sessione PPPoE dopo una modifica della sottoscrizione in CPS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Fasi di riproduzione problemi](#)

[Punti principali da rilevare riguardo al Cacao e ai suoi ritiri](#)

[Soluzione](#)

Introduzione

In questo documento viene descritta la procedura per risolvere i problemi di non interruzione delle sessioni PPPoE dopo una modifica della sottoscrizione in Cisco Policy Suite (CPS) su protocollo Radius.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Linux
- CPS
- Protocollo Radius

Cisco consiglia di disporre dei privilegi di accesso:

- accesso root alla CLI di CPS
- Accesso utente "qns-svn" alle interfacce utente CPS (Policy Builder e Control Center)

Componenti usati

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

- CPS 13.1

- UCS-B

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.

Premesse

CPS è progettato come modello server/client AAA (Authentication, Authorization, and Accounting) per supportare gli abbonati PPPoE (Point-to-Point over Ethernet). CPS interagisce con i dispositivi ASR9K o ASR1K per gestire le sessioni PPPoE.

Problema

Le sessioni PPPoE non si disconnettono e non si riconnettono dopo una nuova selezione di sottoscrizioni in CPS tramite una richiesta API (Application Programming Interface) SOAP (Simple Object Access Protocol) da un sistema di provisioning esterno.

L'osservazione è che CPS è in grado di generare la richiesta di modifica dell'azione (COA) e di inviarla al dispositivo ASR9K, ma queste richieste hanno un timeout da parte del dispositivo ASR9K con "No response Timeout Error" (Nessun errore di timeout di risposta).

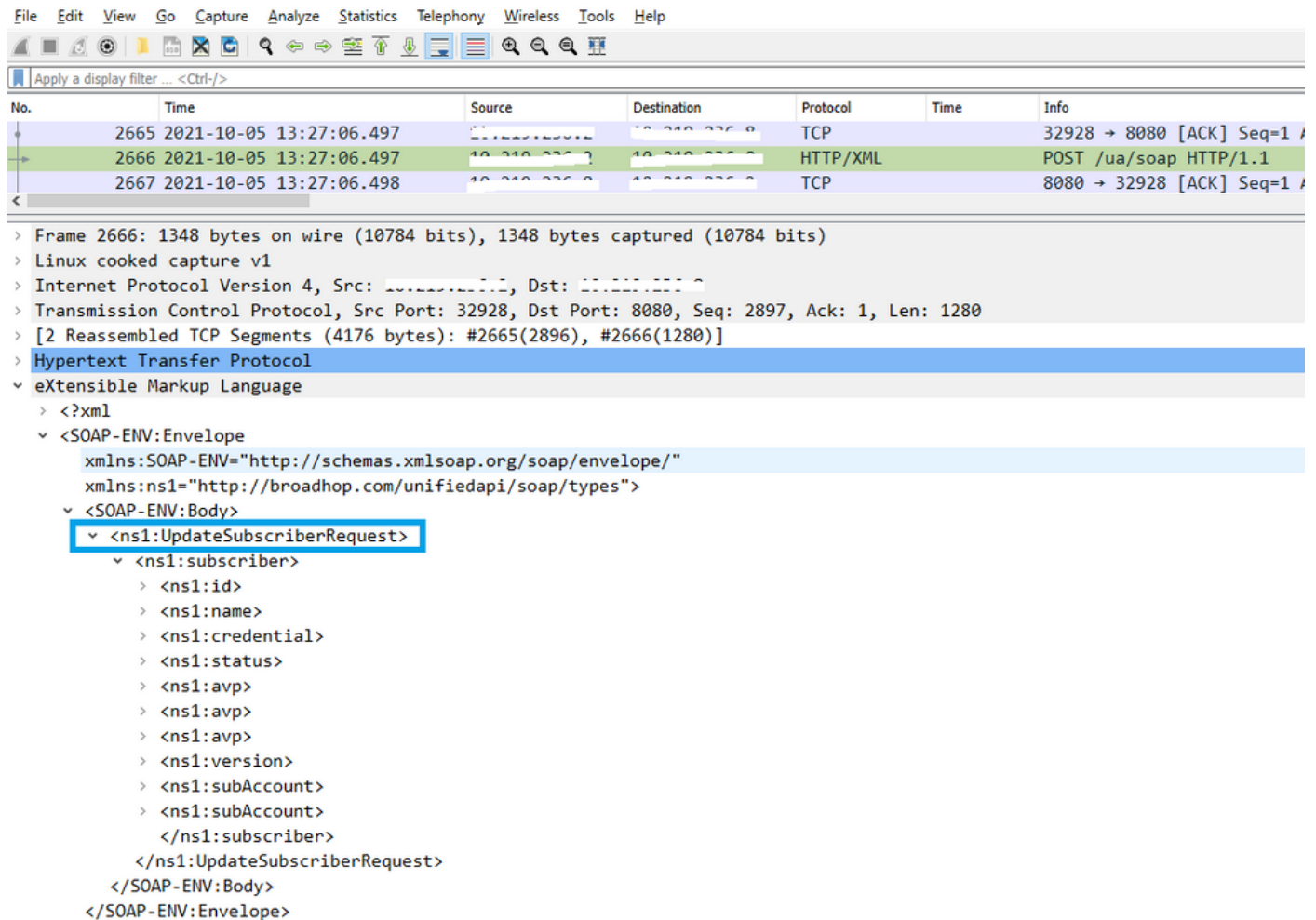
Di seguito è riportato un esempio di messaggio di errore:

```
dc1-lb01 dc1-lb01 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$RemoteActionExecutor.run(PolicyActionJmsR
eceiver.java:98) ~[com.broadhop.policy.remote.jms_13.0.0.release.jar:na]
    at
com.broadhop.utilities.policy.async.PolicyRemoteAsyncActionRunnable.run(PolicyRemoteAsyncActionR
unnable.java:24) [com.broadhop.utility_13.0.0.release.jar:na]
    at java.util.concurrent.Executors$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$GenericThead.run(AsyncPoli
cyActionExecutionManager.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
```

Fasi di riproduzione problemi

Passaggio 1. Avviare sessioni PPPoE da dispositivi ASR9K o ASR1K, accertarsi di visualizzare tali sessioni in CPS tramite Control Center.

Passaggio 2. Avviare una richiesta API SOAP per aggiornare la sottoscrizione dei servizi associati al sottoscrittore.



The screenshot shows the Wireshark interface with a packet capture of a SOAP 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 selected packet (No. 2666) is expanded to show the following structure:

```
> Frame 2666: 1348 bytes on wire (10784 bits), 1348 bytes captured (10784 bits) on 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.210.226.2, 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
v eXtensible Markup Language
  > <?xml
  v <SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:ns1="http://broadhop.com/unifiedapi/soap/types">
  v <SOAP-ENV:Body>
    v <ns1:UpdateSubscriberRequest>
      v <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>
```

Passaggio 3. CPS avvia le richieste COA verso ASR9K o ASR1K. È possibile osservare che CPS esegue un nuovo tentativo della stessa richiesta con la richiesta duplicata dello stesso COA.

No.	Time	Source	Destination	Protocol	Time	Info
2675	2021-10-05 13:27:06.516	10.10.10.10	10.10.10.10	RADIUS		CoA-Request id=77
2757	2021-10-05 13:27:09.519	10.10.10.10	10.10.10.10	RADIUS		CoA-Request id=77, Duplicate Request
2899	2021-10-05 13:27:12.522	10.10.10.10	10.10.10.10	RADIUS		CoA-Request id=77, Duplicate Request
2985	2021-10-05 13:27:15.524	10.10.10.10	10.10.10.10	RADIUS		CoA-Request id=77, Duplicate Request


```

> Frame 2675: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.10
> 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=...

```

Nota: Il primo pacchetto non viene riconosciuto dal dispositivo peer (ASR9K), quindi la logica interna in CPS attiva un meccanismo di ripetizione e invia richieste duplicate.

Passaggio 4. L'osservazione è che CPS interrompe tutte le altre azioni di aggiornamento della sessione, in quanto non è disponibile alcuna risposta per la prima richiesta di COA della sessione e i relativi tentativi.

In questo modo è possibile verificare che la sessione PPPoE è ancora attiva in ASR9K e che non è stata inviata alcuna richiesta di disconnessione della sessione a CPS per l'aggiornamento della sessione. CPS prevede una richiesta di interruzione dell'accounting da ASR9K in relazione alla richiesta COA.

Punti principali da rilevare riguardo al Cacao e ai suoi ritiri

1. CPS avvia le richieste COA per tutte le sessioni attive/esistenti nel relativo database per un determinato sottoscrittore.
2. Se CPS non riceve ACK o NACK per una particolare richiesta COA, avvia un meccanismo di ripetizione dei tentativi in base alla configurazione nel generatore di criteri.
3. È possibile configurare il numero di tentativi e la durata tra tentativi.

Generic RADIUS Device Pool General Selection

*Name default	Description
Default Shared Secret 	Default CoA Shared Secret
*CoA Port 1700	*CoA Retries 3
*CoA Timeout Seconds 3	Correlation Key AccountSessionId
*Access Request Guard Timer (Milliseconds) 0	Coa Disconnect Template select clear
Disconnect Template select clear	Proxy Access Accept Filter select clear
<input type="checkbox"/> Dup Check With Framed Ip	<input type="checkbox"/> Dup Check With Mac Address
<input type="checkbox"/> Radius Network Session Correlation	<input checked="" type="checkbox"/> Control Session Lifecycle

Configurazione dei

tentativi di esempio

Soluzione

Per risolvere questo problema, è necessario estendere ulteriormente l'analisi verso ASR9K e scoprire il motivo per cui non è stata inviata una risposta a CPS per la richiesta COA e i relativi tentativi.

Nelle tracce dello sniffer potete vedere che il load balancer (LB01) di CPS origina il COA da <IP-1> e instrada i pacchetti su eth1, che è la route predefinita.

L'altro Load Balancer (LB02) genera il COA da <IP-2> e utilizza un percorso specifico tramite eth2.

ASR9K ha l'elenco degli accessi (ACL) per accettare il certificato di autenticità solo se proviene da <IP-2>, non da <IP-1>.

È quindi necessario correggere la tabella di routing in LB01 di CPS per inviare il COA con l'indirizzo IP di origine corretto, ovvero <IP-2> tramite un percorso specifico.

In questa schermata è possibile visualizzare la transazione RADIUS end-to-end riuscita per una modifica alla sottoscrizione e la successiva correzione necessaria alla tabella di route di CPS LB.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Time	Info
2934	2021-10-05 13:27:06.517	10.110.100.5	10.110.100.1	RADIUS		CoA-Request id=101
2939	2021-10-05 13:27:06.788	10.110.100.5	10.110.100.1	RADIUS		Accounting-Request id=234
2989	2021-10-05 13:27:09.047	10.110.100.5	10.110.100.1	RADIUS		CoA-Request id=102
2990	2021-10-05 13:27:09.056	10.110.100.5	10.110.100.1	RADIUS		CoA-NAK id=102
3384	2021-10-05 13:27:30.193	10.110.100.1	10.110.100.5	RADIUS		Access-Request id=145
3443	2021-10-05 13:27:33.666	10.110.100.1	10.110.100.5	RADIUS		Accounting-Request id=167
3444	2021-10-05 13:27:33.673	10.110.100.5	10.110.100.1	RADIUS		Accounting-Response id=167