Threshh trap SNMPtrigger DNSLookupFailure sul nodo di standby SRP quando la connessione SRP viene interrotta

Sommario

Introduzione

In questo articolo viene descritto l'apparente trigger falso della trap ThreshDNSLookupFailure quando si verifica un rimbalzo della connessione del protocollo di ridondanza del servizio (SRP) su un nodo in standby SRP. Il servizio DNS (Domain Name Service) dell'infrastruttura viene utilizzato indirettamente su vari nodi della rete LTE (Long Term Evolution) come parte del processo di configurazione della chiamata. In un Packet Data Network Gateway (PGW) può essere utilizzato per risolvere qualsiasi nome di dominio completo (FQDN) restituito nell'autenticazione S6b, nonché per risolvere i nomi di dominio completi specificati come peer nelle varie configurazioni degli endpoint con diametro. Se si verificano timeout (errori) DNS in un nodo attivo durante l'elaborazione delle chiamate, ciò può influire negativamente sulle impostazioni delle chiamate a seconda dei componenti che dipendono dal corretto funzionamento del DNS.

Problema

A partire da StarOS v15 è presente una soglia configurabile per misurare la frequenza degli errori DNS dell'infrastruttura. Nel caso in cui il PGW sia implementato con il ripristino della sessione tra chassis (ICSR), è probabile che se la connessione SRP tra entrambi i nodi si interrompe per qualsiasi motivo e il nodo Standby che ne deriva passa allo stato Attivo in sospeso (ma non completamente attivo perché l'altro nodo rimane completamente SRP attivo presupponendo che non vi siano altri problemi), viene attivato l'allarme/trap DNS associato. Questo perché nello stato attivo in sospeso, il nodo tenta di stabilire le varie connessioni di diametro per le varie interfacce di diametro nel contesto in entrata in preparazione di diventare potenzialmente completamente attivo SRP. Se la configurazione di ANY per le connessioni con diametro si basa sulla specifica di peer nella configurazione dell'endpoint che sono FQDN anziché indirizzi IP, è necessario risolvere tali peer tramite DNS con query A (IPv4) o AAAA (IPv6). Poiché lo stato attivo del nodo è in sospeso, le query ALL hanno esito negativo perché le risposte alle richieste verranno instradate al nodo attivo (che eliminerà le risposte), con una percentuale di errore del 100% che a sua volta determina l'attivazione dell'allarme/trap. Anche se questo è il comportamento previsto in questo scenario, il risultato potenziale è un biglietto del cliente aperto riguardo al significato dell'allarme.

Di seguito è riportato un esempio di tale allarme in cui Diameter Rf è configurato con FQDN e pertanto richiede la risoluzione del DNS. Viene mostrato un FQDN che deve essere risolto da DNS.

```
   diameter endpoint PGW-RF
      origin realm cisco.com
      use-proxy
      origin host test.Rf.cisco.com address 2001:5555:200:1001:240:200::
      peer test-0.cisco.COM realm cisco.COM fqdn lte-test-0.txsl.cisco.com
send-dpr-before-disconnect disconnect-cause 2
```

La connessione SRP si interrompe per qualche motivo (esterno alla coppia di nodi PGW e il motivo non importante ai fini di questo esempio) per oltre 7 minuti e i trigger Trap ThreshDNSLookupFailure del protocollo SNMP.

```
Tue Nov 25 08:43:42 2014 Internal trap notification 1037 (SRPConnDown)
vpn SRP ipaddr 10.211.220.100 rtmod 3 Tue Nov 25 08:43:42 2014 Internal trap notification 120
(SRPActive)
vpn SRP ipaddr 10.211.208.165 rtmod 3 Tue Nov 25 08:51:14 2014 Internal trap notification 1038
(SRPConnUp)
vpn SRP ipaddr 10.211.220.100 rtmod 3 Tue Nov 25 08:51:14 2014 Internal trap notification 121
(SRPStandby)
vpn SRP ipaddr 10.211.208.165 rtmod 9 Tue Nov 25 09:00:08 2014 Internal trap notification 480
(ThreshDnsLookupFailure)
context "XGWin" threshold 5% measured value 12%
```

Ecco l'allarme e il log associato:

```
[local]XGW> show alarm outstanding verbose

Severity Object          Timestamp                          Alarm ID
-------- ----------      ---------------------------------- ------------------
  Alarm Details
------------------------------------------------------------------------------
Minor    VPN XGWin       Tuesday November 25 09:00:0        3611583935317278720
<111:dns-lookup-failure> has reached or exceeded the configured threshold <5%>,
the measured value is <12%>. It is detected at <Context [XGWin]>.

2014-Nov-25+09:00:08.939 [alarmctrl 65201 info]
[5/0/6050 <evlogd:0> alarmctrl.c:192] [context: XGWin, contextID: 6] [software internal system
critical-info syslog] Alarm condition: id 321eec7445180000 (Minor):
<111:dns-lookup-failure> has reached
 or exceeded the configured threshold <5%>, the measured value is <12%>.
It is detected at <Context [XGWin]>.
```

Bulkstats conferma un errore del 100% per le query DNS AAAA primarie e secondarie che tentano di risolvere i peer Diameter Rf:

%tempo%	%dns-central-aaaa-atmpts%	%dns-primary-ns-aaaa-atmpts%	%dns-primary-ns-aaaa-fail%	%dns-primary-ns-query-timeout%	%dns-secondary-ns-aaaa-atmpts%	%dns-secondary-ns-aaaa-fail%	%timeout query-ns-secondar
08:32:00	16108	16098	10	10	10	0	0
08:34:00	16108	16098	10	10	10	0	0
08:36:00	16108	16098	10	10	10	0	0
08:38:0	16108	16098	10	10	10	0	0

08:40:00	16108	16098	10	10	10	0	0
08:42:00	16108	16098	10	10	10	0	0
08:44:00	16236	16162	74	74	74	64	64
08:46:00	16828	16466	362	362	362	352	352
08:48:00	17436	16770	666	666	666	656	656
08:50:00	18012	17058	954	954	954	944	944
08:52:00	18412	17250	1162	1162	1162	1152	1152
08:54:00	18412	17250	1162	1162	1162	1152	1152
08:56:00	18412	17250	1162	1162	1162	1152	1152

Soluzione

Questa trap/allarme può essere ignorata e cancellata poiché il nodo non è realmente SRP attivo e non gestisce alcun traffico. Si noti che la percentuale di errori nell'esempio riportato sopra è molto inferiore al 100% previsto e che il bug CSCuu60841 ha ora risolto il problema in una versione futura in modo che venga sempre segnalato il 100%.

segnale di allarme

O

Per cancellare quell'allarme:

clear alarm id <id allarme>

Èpossibile che si verifichi un'altra variante del problema sul nuovo chassis di standby SRP dopo il passaggio al nuovo sistema. L'allarme deve essere ignorato anche in questo scenario, poiché lo chassis è in modalità standby SRP e i guasti DNS sono pertanto irrilevanti.

Infine, è ovvio che la causa di questo allarme deve essere immediatamente investigata su un PGW realmente SRP attivo, in quanto l'impatto degli abbonati o della fatturazione si verificherà probabilmente a seconda dei tipi di FQDN che stanno tentando di risolvere.