SNMP-trap: ThreshDNSLookupError triggers op SRP-stand-by knooppunt wanneer SRP-verbinding wordt gestart

Inhoud

Inleiding

Dit artikel beschrijft de klaarblijkelijke valse trigger van de val van ThreshDNSLookupFailwanneer een de verbinding van het Protocol (SRP) op een standby knooppunt van SRP plaatsvindt. Infrastructuur Domain Name Service (DNS) wordt indirect op verschillende knooppunten in het LTE-netwerk (Long Term Evolution) gebruikt als onderdeel van het proces van Call Setup. Op een Packet Data Network Gateway (PGW) kan worden gebruikt om alle FQDN-namen (FQDN's) met volledige kwalificatie op te lossen die zijn teruggebracht in S6b-verificatie, evenals om FQDN's op te lossen die als peers zijn gespecificeerd in de verschillende configuraties van Diameter-eindpunt. Als DNS time-outs (defecten) optreden op een actieve knooppunt verwerkingsvraag, kan dit een negatieve invloed hebben op de aanroepen, afhankelijk van de onderdelen die afhankelijk zijn van de DNS-werking.

Probleem

Met ingang van StarOS v15 is er een configureerbare drempel om de mate van DNS-storing in de infrastructuur te meten. In het geval waarin de PGW wordt geïmplementeerd met sessieherstel tussen chassis (ICSR), is er de waarschijnlijkheid dat als de SRP-verbinding tussen beide knooppunten om welke reden dan ook daalt en het daaropvolgende Standby-knooppunt in hangende actieve toestand terechtkomt (maar niet volledig actief omdat het andere knooppunt volledig SRP actief blijft, zonder andere problemen), dan wordt het bijbehorende DNS-alarm/-val geactiveerd. Dit komt doordat in hangende actieve staat, het knooppunt probeert de verschillende diameterverbindingen voor de verschillende diameterinterfaces in de ingerichte context tot stand te brengen om potentieel SRP actief te worden. Als de configuratie voor een of meer van de diameterverbindingen is gebaseerd op het specificeren van peers in de endpointconfiguratie die FQDNs zijn in plaats van IP-adressen, moeten deze peers via DNS met A (IPv4) of AAA (IPv6) vragen worden opgelost. Aangezien het knooppunt zich in actieve toestand bevindt, kunnen dergelijke vragen ALLE FAIL-bestanden worden beantwoord omdat de reacties op de aanvragen naar het actieve knooppunt worden gestuurd (waardoor de reacties worden verlaagd). Dit levert een percentage van 100% op, wat op zijn beurt leidt tot het alarm/de val. Terwijl dit verwacht gedrag in dit scenario is, is het potentiële resultaat een open cliëntitel met betrekking tot het belang van het alarm.

Hier is een voorbeeld van zo een alarm waar Diameter Rf met FQDNs wordt gevormd en daarom vereist DNS om op te lossen. Shown is een FQDN dat door DNS moet worden opgelost.

```
   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
```

De SRP-verbinding wordt om de een of andere reden (extern aan het paar PGW-knooppunten en de reden niet belangrijk voor de doeleinden van dit voorbeeld) voor 7+ minuten ingedrukt, en de SNMP-trap ThreshDNSLookupFailtriggers.

```
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%
```

Dit is het alarm en het bijbehorende logboek:

```
[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 bevestigt 100% mislukking voor Primaire en Secundaire AAA DNS vragen om Diameter Rf peers op te lossen:

%tijd%	%dns-as-a-atmpts%	%dns-primair-n-aaaa-atmpts%	%dns-primaire-aaaa-mislukking%	%dns-primaire-n-query-timeouts%	%dns-secondaire-n-aa-atmpts%	%dns-secondair-aaaa-mislukking%	%dns-secondair query-timeouts%
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

Oplossing

Deze val/alarm kan worden genegeerd en gewist aangezien het knooppunt niet echt SRP actief is en geen verkeer verwerkt. Merk op dat het mislukkingspercentage in het bovenstaande voorbeeld veel lager is dan de verwachte 100% en bug CSCuu60841 heeft dat probleem nu in een toekomstige release opgelost, zodat het altijd 100% zal rapporteren.

klaar alarm

OF

U kunt dat specifieke alarm alleen verwijderen:

helder alarm <alarm>

Een andere twist van deze kwestie kan op een nieuw SRP Standby chassis voorkomen nadat een SRP-omschakeling heeft plaatsgevonden. Het alarm moet in dat scenario ook worden genegeerd, aangezien het chassis SRP Standby is en DNS-fouten daarom irrelevant zijn.

Tot slot spreekt het vanzelf dat de oorzaak van dit alarm onmiddellijk moet worden onderzocht op een waarlijk actief PGW van SRP, aangezien een impact op abonnees of facturering waarschijnlijk zal plaatsvinden afhankelijk van welke typen FQDN's proberen te worden opgelost.