SNMP-Trap ThreshDNSLookupFailure-Trigger auf dem SRP-Standby-Knoten, wenn die SRP-Verbindungsbounzen auftreten

Inhalt

[Einführung](#)
[Problem](#)
[Lösung](#)
[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Artikel wird der scheinbare falsche Auslöser des ThreshDNSLookupFailure-Traps beschrieben, wenn ein SRP-Verbindungsbounce (Service Redundancy Protocol) auf einem SRP-Standby-Knoten auftritt. Infrastructure Domain Name Service (DNS) wird indirekt im Rahmen des Anrufeinrichtungsprozesses auf verschiedenen Knoten im LTE-Netzwerk (Long Term Evolution) verwendet. Auf einem Packet Data Network Gateway (PGW) kann es verwendet werden, um alle vollständig qualifizierten Domänennamen (FQDNs), die in der S6b-Authentifizierung zurückgegeben werden, aufzulösen und um FQDNs aufzulösen, die in den verschiedenen Diameter-Endpunktkonfigurationen als Peers angegeben wurden. Wenn DNS-Timeouts (Ausfälle) bei Anrufen zur Verarbeitung eines aktiven Knotens auftreten, kann sich dies negativ auf die Anrufeinrichtung auswirken, je nachdem, welche Komponenten davon abhängig sind, dass der DNS ordnungsgemäß funktioniert.

Problem

Ab StarOS v15 gibt es einen konfigurierbaren Grenzwert zur Messung der DNS-Fehlerrate der Infrastruktur. Wenn der PGW mit der Inter-Chassis Session Recovery (ICSR) implementiert wird, besteht die Wahrscheinlichkeit, dass die SRP-Verbindung zwischen beiden Knoten aus irgendeinem Grund ausfällt und der darauf folgende Standby-Knoten in den ausstehenden Aktiv-Zustand wechselt (aber nicht vollständig aktiv, da der andere Knoten voll aktiv bleibt, vorausgesetzt, dass keine anderen Probleme auftreten), dann wird der zugehörige DNS-Alarm/Trap ausgelöst. Dies liegt daran, dass der Knoten im ausstehenden aktiven Zustand versucht, die verschiedenen Durchmesser Verbindungen für die verschiedenen Durchmesser Schnittstellen im Eingangs-Kontext herzustellen, um eine potenzielle vollständige SRP-Aktivität vorzubereiten. Wenn die Konfiguration für EINE der Verbindungen mit Durchmesser auf der Angabe von Peers in der Endpunktkonfiguration basiert, die FQDNs anstelle von IP-Adressen sind, müssen diese Peers über DNS mit A (IPv4)- oder AAAA (IPv6)-Abfragen aufgelöst werden. Da sich der Knoten im ausstehenden aktiven Zustand befindet, werden ALLE FAIL-Anfragen abgefragt, da die Antworten auf die Anfragen an den aktiven Knoten weitergeleitet werden (der die Antworten verwirft), was zu einer Fehlerrate von 100 % führt, die wiederum die Alarmierung/das Trap auslöst. Dieses Verhalten ist in diesem Szenario zwar zu erwarten, aber das potenzielle Ergebnis ist ein geöffnetes Kundenticket bezüglich der Bedeutung des Alarms.

Hier ein Beispiel für einen solchen Alarm, bei dem Diameter Rf mit FQDNs konfiguriert ist und

daher DNS aufgelöst werden muss. Angezeigt ist ein FQDN, der durch DNS aufgelöst werden muss.

```
   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
```

Die SRP-Verbindung wird aus irgendeinem Grund (außerhalb des PGW-Knotenpaars und des für die Zwecke dieses Beispiels unwichtigen Grundes) für mindestens 7 Minuten unterbrochen, und der SNMP-Trap ThreshDNSLookupFailure-Trigger.

```
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%
```

Der Alarm und das zugehörige Protokoll sind wie folgt:

```
[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 bestätigen einen 100%igen Ausfall für primäre und sekundäre AAAA-DNS-Abfragen, die versuchen, Durchmesser-Rf-Peers zu lösen:

%Uhrzeit%	%dns-central-aaa-atmpts%	%dns-primary-ns-aaa-atmpts%	%dns-primary-ns-aaa-failure%	%dns-primary-ns-query-timeouts%	%dns-second-ns-aaa-atmpts%	%dns-second-ns-aaa-fail%	%dns-sec ns-query- timeouts%
08:32:00 Uhr	16108	16.098	10	10	10	0	0
08:34:00 Uhr	16108	16.098	10	10	10	0	0

08:36:00 Uhr	16108	16.098	10	10	10	0	0
08:38:00 Uhr	16108	16.098	10	10	10	0	0
08:40:00 Uhr	16108	16.098	10	10	10	0	0
08:42:00 Uhr	16108	16.098	10	10	10	0	0
08:44:00 Uhr	16236	16162	74	74	74	64	64
08:46:00 Uhr	16828	16466	362	362	362	352	352
08:48:00 Uhr	17436	16770	666	666	666	656	656
08:50:00 Uhr	18.012	17058	954	954	954	944	944
08:52:00 Uhr	18412	17250	1162	1162	1162	1152	1152
08:54:00 Uhr	18412	17250	1162	1162	1162	1152	1152
08:56:00 Uhr	18412	17250	1162	1162	1162	1152	1152

Lösung

Dieser Trap/Alarm kann ignoriert und gelöscht werden, da der Knoten nicht wirklich aktiv ist und keinen Datenverkehr verarbeitet. Beachten Sie, dass die Fehlerrate im obigen Beispiel viel niedriger ist als die erwarteten 100% und der Fehler CSCuu60841 hat dieses Problem jetzt in einer zukünftigen Version behoben, sodass es immer 100% melden wird.

Alarm ausstehend

ODER

So löschen Sie diesen Alarm:

clear alarm ID <Alarm-ID>

Ein weiterer Fehler kann bei einem neu eingerichteten SRP Standby-Chassis auftreten, nachdem ein SRP-Switchover durchgeführt wurde. Der Alarm sollte in diesem Szenario ebenfalls ignoriert werden, da das Chassis SRP Standby ist und DNS-Fehler daher irrelevant sind.

Schließlich muss die Ursache für diesen Alarm auf einem wirklich aktiven SRP-PGW sofort untersucht werden, da die Auswirkungen auf Abonnenten und Abrechnung wahrscheinlich davon abhängen, welche FQDNs versucht zu lösen.