當SRP連線退回時，在SRP備用節點上觸發SNMP陷阱閾值DNSLookupFailure

目錄

簡介

本文描述當服務冗餘協定(SRP)連線在SRP備用節點上發生反彈時，ThreshDNSLookupFailure陷阱的明顯錯誤觸發。基礎架構網域名稱服務(DNS)間接用於長期演化(LTE)網路中的各個節點，作為通話設定程式的一部分。在資料包資料網路網關(PGW)上，它可用於解析S6b身份驗證中返回的任何完全限定域名(FQDN)，以及解析在各種Diameter端點配置中指定為對等體的FQDN。如果在處理呼叫的活動節點上發生DNS超時（故障），則可能會對呼叫設定產生負面影響，具體取決於哪些元件依賴DNS正常工作。

問題

從StarOS v15開始，有一個可配置的閾值來測量基礎架構DNS故障率。在使用Inter-Chassis Session Recovery(ICSR)實施PGW的情況下，如果兩個節點之間的SRP連線因任何原因而關閉，並且隨後的備用節點進入掛起的啟用狀態（但並非完全啟用，因為另一個節點保持完全的SRP啟用，假設沒有其他問題），則觸發關聯的DNS警報/陷阱。這是因為處於待定的活動狀態時，節點會嘗試為入口上下文中的各種直徑介面建立各種直徑連線，為可能變為完全的SRP活動做準備。如果任一直徑連線的配置基於在終端配置中指定屬於FQDN而不是IP地址的對等體，則需要使用A(IPv4)或AAAA(IPv6)查詢通過DNS解析這些對等體。由於節點處於掛起的活動狀態，此類查詢全部失敗，因為對請求的響應將路由到活動節點（這將丟棄響應），這會導致100%的故障率，進而導致觸發警報/陷阱。雖然這是此場景中的預期行為，但潛在結果是有關警報重要性的已開啟客戶票證。

以下是此類警報的示例，其中Diameter Rf配置了FQDN，因此需要DNS解析。 顯示的是需要由DNS解析的FQDN。

```
   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
```

SRP連線由於某種原因（PGW節點對外部以及對於本示例而言不重要的原因）關閉7分鐘，並觸發SNMP陷阱ThreshDNSLookupFailure。

```
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%
```

以下是警報和相關日誌：

```
[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]>.
```

批次統計資料確認嘗試解析Diameter Rf對等體的主要和輔助AAAA DNS查詢出現100%故障：

%time %	%dns-central-aaaa-atmpts%	%dns-primary-ns-aaaa-atmpts%	%dns-primary-ns-aaaa-fails%	%dns-primary-ns-query-timeouts%	%dns-secondary-ns-aaaa-atmpts%	%dns-secondary-ns-aaaa-fails%	%dns-secondar 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
08:38:00	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
08:54:0	18412	17250	1162	1162	1162	1152	1152

0 08:56:00	18412	17250	1162	1162	1162	1152	1152

解決方案

此陷阱/警報可以忽略和清除，因為節點不是真正的SRP活動，也不處理任何流量。請注意，上述範例中的失敗率遠低於預期的100%，錯誤CSCuu60841現在已在未來版本中修正了此問題，因此它始終會報告100%。

清除未完成的警報

或

要清除這個特別的警報：

clear alarm id <alarm id>

在SRP切換發生後，新SRP備用機箱上可能會發生此問題的另一個扭曲。在這種情況下，應忽略警報，因為機箱為SRP備用，因此DNS故障不相關。

最後，不言而喻，需要在真正的SRP活動PGW上立即調查此警報的原因，因為根據嘗試解決的FQDN型別，可能會發生訂閱者或計費影響。