当SRP连接退回时，SNMP陷阱ThreshDNSLookupFailure在SRP备用节点上触发

目录

简介

本文描述当服务冗余协议(SRP)连接在SRP备用节点上发生退回时，ThreshDNSLookupFailure陷阱的明显错误触发。基础设施域名服务(DNS)在长期演进(LTE)网络中的不同节点间接用作呼叫建立过程的一部分。在数据包数据网络网关(PGW)上，它可用于解析在S6b身份验证中返回的任何完全限定域名(FQDN)，以及解析在各种Diameter终端配置中指定为对等体的FQDN。如果主用节点处理呼叫时发生DNS超时（故障），则这可能会对呼叫设置产生负面影响，具体取决于哪些组件依赖于DNS正常运行。

问题

从StarOS v15开始，有一个可配置的阈值来衡量基础设施DNS故障率。在使用机箱间会话恢复(ICSR)实施PGW时，如果两个节点之间的SRP连接因任何原因断开，随后的备用节点进入挂起的活动状态(但由于其他节点保持完全SRP活动状态（假设没有其他问题），则触发关联的DNS警报/陷阱。这是因为处于挂起活动状态时，节点会尝试在入口环境中为各种直径接口建立各种直径连接，以备可能成为完全SRP活动状态。如果ANY的直径连接配置基于在终端配置中指定FQDN而不是IP地址的对等体，则需要通过DNS和A(IPv4)或AAA(IPv6)查询解析这些对等体。由于节点处于挂起活动状态，因此此类查询ALL FAIL，因为对请求的响应将路由到活动节点（这将丢弃响应），这会导致100%的故障率，进而导致触发警报/陷阱。虽然这是此场景中的预期行为，但潜在结果是打开了有关警报重要性的客户票证。

以下是此类警报的示例，其中Diameter Rf配置了FQDN，因此需要DNS才能解析。 图中所示为需要由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连接因某种原因（对PGW节点对外部以及本示例中不重要的原因）中断7+分钟，并且SNMP陷阱ThreshDNSLookupFailure触发。

```
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%
```

以下是警报和关联日志：

```
[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]>.
```

批量统计数据确认，尝试解析Diameter Rf对等体的主AAAA和辅助AAAA DNS查询100%失败：

%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

解决方案

此陷阱/警报可以忽略和清除，因为节点不是真正的SRP活动状态，并且不处理任何流量。请注意，上例中的故障率远低于预期的100%,Bug CSCuu60841现在已在将来的版本中修复该问题，因此它将始终报告100%。

未清除警报

或者

要清除这个特定的警报：

clear alarm id <alarm id>

发生SRP切换后，新SRP备用机箱上可能会发生此问题的另一个转折。在该场景中，也应忽略警报，因为机箱是SRP备用，因此DNS故障不相关。

最后，不言而喻，此警报的原因需要在真正的SRP活动PGW上立即调查，因为用户或计费影响可能会发生，具体取决于尝试解决的FQDN类型。