

# SNMP陷阱在SRP暂挂节点的ThreshDNSLookupFailure触发，当SRP连接重新启动

## 目录

[简介](#)

[问题](#)

[解决方案](#)

[相关的思科支持社区讨论](#)

## 简介

此条款描述ThreshDNSLookupFailure陷阱的明显的错误触发，当服务冗余协议(SRP)时连接跳动在SRP待机节点发生。基础设施域名服务器(DNS)在间接多种节点演变(LTE)作为呼叫建立过程一部分，网络从长远来看使用。在信息包数据网络网关(PGW)上它在多种直径终端配置里可以用于解决在S6b验证(FQDN)返回的所有完全合格的域名，以及解决作为对等体指定的FQDN。如果DNS超时(失败)在处理呼叫的活动节点出现，则这能根据什么组件负影响呼叫建立依靠正常运行的DNS。

## 问题

开始在StarOS那里v15是测量基础设施DNS故障率的可配置阈值。在PGW实现与机箱之间会话恢复的案件中(ICSR)，有的可能性，如果两节点之间的SRP连接无论什么原因断开，并且接着而来的暂挂节点进入待定活动状态(但是不完全激活，因为另一个节点充分地不依然是假设其他问题)的SRP激活，然后相关的DNS报警/陷阱被触发。这是因为在待定活动状态，节点在充分潜在变为SRP激活的准备的入口上下文尝试建立多种直径接口的多种直径连接。如果是FQDN而不是IP地址直径连接的ANY的配置根据指定在终端配置里并列，则那些对等体需要通过有A (IPv4)或AAAA (IPv6)查询的DNS被解决。因为节点在待定活动状态，这样查询所有FAIL，因为对请求的答复将路由对将下降答复)的活动节点(导致100%故障率反过来导致将被触发的报警/陷阱。当这是在此方案时的预料之中的行为，可能导致是关于报警的意义的一张打开的客户票。

这是直径Rf配置与FQDN并且要求DNS解决这样报警的示例。显示需要由DNS解决的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
```

由于某种原因SRP连接沿着走(对对的外部PGW节点和原因不重要为此示例)为7+分钟和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%
```

这是报警和相关的日志：

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

```
Severity Object          Timestamp                Alarm ID
-----
Alarm Details
-----
Minor      VPN XGWin              Tuesday November 25 09:00:00      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确认尝试主要的和附属AAAA DNS的查询的100%失败解决直径Rf对等体：

%time %	%dns中央印 制厂 aaaaatmpts %	%dns主要的 NS aaaaatmpts%	%dns主要的 NS aaaafails%	%dns主要的 NS查询 timeouts%	%dns第二 NS aaaaatmpts %	%dns第二NS aaaafails%	%dns第二 NS查询 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
08:54:00	18412	17250	1162	1162	1162	1152	1152

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

## 解决方案

此陷阱/报警，因为节点真不是SRP活跃和不处理任何流量，可以忽略和清除。比预计100%和bug CSCuu60841当前修复在以后的版本的注释在以上示例的故障率是更低的该问题，以便总是报告100%。

### 清除未清的报警

或者

清楚特殊请警报：

### 清除报警id <alarm id>

在SRP切换发生了之后，此问题另一电线绞在一个SRP暂挂机箱能最近发生。在该方案应该也忽略报警，因为机箱是SRP待机因此，并且DNS失败是毫不相关的。

最后，不言而喻此报警的起因在—SRP活动PGW需要真立即调查的那，因为用户或发单的影响根据尝试解决什么类型的FQDN可能将发生。