# SNMP déroute les déclencheurs ThreshDNSLookupFailure sur le noeud de secours SRP lorsque la connexion SRP rebondit

## Contenu



## Introduction

Cet article décrit le faux déclencheur apparent du déroutement ThreshDNSLookupFailure lorsqu'une connexion SRP (Service Redundancy Protocol) rebondit sur un noeud de secours SRP. Le service DNS (Infrastructure Domain Name Service) est utilisé indirectement sur divers noeuds du réseau LTE (Long Term Evolution) dans le cadre du processus de configuration des appels. Sur une passerelle de réseau de données de paquets (PGW), il peut être utilisé pour résoudre tous les noms de domaine complets (FQDN) retournés dans l'authentification S6b, ainsi que pour résoudre les noms de domaine complets spécifiés comme homologues dans les différentes configurations de terminaux de diamètre. Si des délais d'attente DNS (défaillances) surviennent sur un noeud actif qui traite des appels, cela peut avoir une incidence négative sur les configurations d'appels selon les composants qui dépendent du bon fonctionnement du DNS.

## Problème

Àpartir de StarOS v15, il existe un seuil configurable pour mesurer le taux de défaillance DNS de l'infrastructure. Dans le cas où le PGW est mis en oeuvre avec l'ICSR (Inter-Chassis Session Recovery), il est probable que si la connexion SRP entre les deux noeuds tombe en panne pour une raison quelconque et que le noeud de secours suivant passe en état Actif en attente (mais pas totalement actif parce que l'autre noeud reste complètement actif SRP en supposant qu'aucun autre problème ne se produise), alors l'alarme/déroutement DNS associé est déclenché. En effet, dans l'état actif en attente, le noeud tente d'établir les différentes connexions de diamètre pour les différentes interfaces de diamètre dans le contexte d'entrée, en préparation de devenir potentiellement complètement actif SRP. Si la configuration de N'IMPORTE QUELLE connexion de diamètre est basée sur la spécification d'homologues dans la configuration de point d'extrémité qui sont des noms de domaine complet au lieu d'adresses IP, ces homologues doivent être résolus via DNS avec des requêtes A (IPv4) ou AAAA (IPv6). Comme le noeud est en attente d'activation, de telles requêtes TOUTES ÉCHEC car les réponses aux requêtes seront acheminées vers le noeud actif (qui abandonnera les réponses), ce qui entraîne un taux d'échec de 100 %, ce qui déclenche à son tour l'alarme/déroutement. Bien que ce comportement soit attendu dans ce scénario, le résultat potentiel est un ticket client ouvert concernant la signification de l'alarme.

Voici un exemple d'alarme de ce type où Diameter Rf est configuré avec des FQDN et nécessite donc la résolution DNS.  Il s'agit d'un nom de domaine complet qui doit être résolu par le DNS.

```
   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
```

La connexion SRP s'arrête pour une raison quelconque (externe à la paire de noeuds PGW et la raison n'est pas importante aux fins de cet exemple) pendant plus de 7 minutes, et le déroutement SNMP ThreshDNSLookupFailure se déclenche.

```
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%
```

Voici l'alarme et le journal associé :

```
[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 confirme une défaillance à 100 % pour les requêtes DNS AAAA principales et secondaires qui tentent de résoudre les homologues Rf Diameter :

| %time% | %dns-central-aaaa-atmpts% | %dns-primary-ns-aaaa-atmpts% | %dns-primary-ns-aaaa-fail% | %dns-primary-ns-query-timeouts% | %dns-secondary-ns-aaaa-atmpts% | %dns-secondary-ns-aaaa-fail% | %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 |
| 08:38:0 | 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 |

# Solution

Ce déroutement/alarme peut être ignoré et effacé car le noeud n'est pas vraiment actif SRP et ne gère aucun trafic. Notez que le taux d'échec dans l'exemple ci-dessus est beaucoup plus faible que le 100% attendu et le bogue CSCuu60841 a maintenant résolu ce problème dans une version future de sorte qu'il va toujours signaler 100%.

**clear alarme en cours**

OU

Pour effacer cette alarme particulière :

**clear alert id <id d'alarme>**

Une autre torsion de ce problème peut survenir sur un nouveau châssis de secours SRP après une commutation SRP. L'alarme doit également être ignorée dans ce scénario, car le châssis est en veille SRP et les défaillances DNS ne sont donc pas pertinentes.

Enfin, il va sans dire que la cause de cette alarme doit être immédiatement étudiée sur un PGW réellement actif SRP, car l'impact sur l'abonné ou la facturation se produira probablement en fonction des types de FQDN qui tentent d'être résolus.