

# Déclencheurs de ThreshDNSLookupFailure de déROUTement SNMP sur le noeud de réserve SRP quand la connexion SRP rebondit

## Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

## Introduction

Cet article décrit le déclencheur faux apparent du déROUTement de ThreshDNSLookupFailure quand un rebond de connexion de Protocol de Redondance de service (SRP) se produit sur un noeud de standby SRP. Le domain name service d'infrastructure (DN) est utilisé sur le divers réseau de l'évolution de Noeuds à long terme (LTE) indirectement en tant qu'élément du processus d'établissement d'appel. Sur une passerelle de réseau de données de paquets (PGW) il peut être utilisé pour résoudre tous les noms de domaine complet (FQDN) retournés dans l'authentification S6b, aussi bien que pour résoudre des FQDN spécifiés comme pairs dans les diverses configurations de point final de diamètre. Si les délais d'attente de DN (pannes) se produisent sur un noeud actif traitant des appels, alors ceci peut négativement affecter des établissements d'appel selon quels composants se fondent sur les DN fonctionnant correctement.

## Problème

Commencer dans StarOS v15 il y a un seuil configurable pour mesurer le taux d'échec de DN d'infrastructure. Dans le cas où le PGW est mis en application avec la reprise de session d'Inter-châssis (ICSR), il y a la probabilité qui si la connexion SRP entre les deux Noeuds descend pour quelque raison que ce soit, et le noeud de réserve suivant entre dans l'état active en suspens (mais pas entièrement actif parce que l'autre noeud demeure entièrement active SRP n'assumant aucune autre question), alors l'alarme/déROUTement associés de DN est déclenchée. C'est parce que dans l'état active en suspens, les tentatives de noeud d'établir les diverses connexions de diamètre pour le divers diamètre relie dans le contexte d'entrée en préparation de devenir potentiellement entièrement active SRP. Si la configuration pour les connexions l'un des de diamètre est basée sur spécifier scrute dans la configuration de point final qui sont des FQDN au lieu des adresses IP, alors ces pairs doivent être résolus par l'intermédiaire des DN avec A (ipv4) ou AAAA (IPv6) questionne. Puisque le noeud est dans l'état active en suspens, de telles requêtes TOUTES ÉCHOUENT parce que les réponses aux demandes seront conduites au noeud actif (qui relâchera les réponses), qui a comme conséquence le taux d'échec 100% qui entraîne consécutivement l'alarme/déROUTement à déclencher. Tandis que c'est comportement prévu dans ce scénario, le résultat potentiel est un ticket ouvert de client concernant l'importance de l'alarme.

Voici un exemple d'une telle alarme où le diamètre rf est configuré avec des FQDN et exige donc des DN de le résoudre. Affiché est un FQDN qui doit être résolu par des DN.

```
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 descend pour quelque raison (externe aux paires de Noeuds PGW et à la raison non importante aux fins de cet exemple) pour les minutes 7+, et les déclencheurs de ThreshDNSLookupFailure de déroutement SNMP.

```
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 log 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 la panne de 100% pour des requêtes DNS primaires et secondaires AAAA tentant de résoudre des pairs du diamètre rf :

%time %	%dns-central-aaaa-atmpts%	%dns-primaire-NS-aaaa-atmpts%	%dns-primaire-NS-aaaa-fails%	%dns-primaire-NS-requête-timeouts%	%dns-secondaire-NS-aaaa-atmpts%	%dns-secondaire-NS-aaaa-fails%	%dns-secondaire-NS-requête-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

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

Ces déroutement/alarme peut être ignoré et effacé puisque le noeud n'est pas véritable en activité SRP et en ne manipulant pas en trafiquez. Notez le taux d'échec dans l'exemple ci-dessus est beaucoup inférieur que le 100% et la bogue prévus CSCuu60841 a maintenant réparé cette question dans une version future de sorte qu'elle toujours l'état 100%.

**effacez l'alarme exceptionnelle**

OU

Juste clair qu'alarme particulière :

**effacez l'id> de <alarm d'id d'alarme**

Une autre torsade de cette question peut se produire sur nouvellement un châssis de réserve SRP après qu'un basculement SRP ait eu lieu. L'alarme devrait être ignorée dans ce scénario également puisque le châssis est standby SRP et des pannes de DN sont donc inutiles.

En conclusion, il va de soi que la cause pour cette alarme doit être immédiatement étudiée sur vraiment un SRP PGW actif, car l'abonné ou l'incidence de affichage se produira vraisemblablement selon quels types de FQDN tentent d'être résolus.