O SNMP trap ThreshDNSLookupFailure dispara no nó de reserva SRP quando a conexão SRP é devolvida

Contents

Introduction

Este artigo descreve o falso disparador aparente da armadilha ThreshDNSLookupFailure quando uma devolução de conexão do Service Redundancy Protocol (SRP) ocorre em um nó de standby SRP. O serviço de nome de domínio de infraestrutura (DNS) é usado em vários nós na rede de evolução a longo prazo (LTE) indiretamente como parte do processo de configuração de chamada. Em um Gateway de Rede de Dados de Pacotes (PGW - Packet Data Network Gateway), ele pode ser usado para resolver qualquer FQDN (Fully Qualified Domain Names, nomes de domínio totalmente qualificados) retornados na autenticação S6b, bem como para resolver FQDNs especificados como pares nas várias configurações de ponto de extremidade de Diâmetro. Se os tempos limites (falhas) de DNS ocorrerem em um nó ativo processando chamadas, isso pode afetar negativamente as configurações de chamadas, dependendo de quais componentes dependem do DNS funcionando corretamente.

Problema

A partir do StarOS v15, há um limite configurável para medir a taxa de falha de DNS da infraestrutura. No caso em que o PGW é implementado com o ICSR (Inter-Chassis Session Recovery, recuperação de sessão entre chassis), há a probabilidade de que, se a conexão SRP entre ambos os nós ficar inativa por qualquer motivo, e o nó de standby subsequente entrar no estado Ativo pendente (mas não totalmente ativo porque o outro nó permanece totalmente ativo, assumindo que não há outros problemas), o alarme/interceptação de DNS associado é acionado. Isso ocorre porque, no estado ativo pendente, o nó tenta estabelecer as várias conexões de diâmetro para as várias interfaces de diâmetro no contexto de ingresso em preparação para se tornar totalmente ativo de SRP. Se a configuração para QUALQUER uma das conexões de diâmetro for baseada na especificação de peers na configuração de ponto final que são FQDNs em vez de endereços IP, então esses peers precisam ser resolvidos via DNS com consultas A (IPv4) ou AAAA (IPv6). Como o nó está no estado ativo pendente, tais consultas TODAS FALHAM porque as respostas às solicitações serão roteadas para o nó ativo (que descartará as respostas), o que resulta em uma taxa de falha de 100% que, por sua vez, faz com que o alarme/interceptação seja disparado. Embora esse seja um comportamento esperado nesse cenário, o resultado potencial é um tíquete de cliente aberto em relação ao significado do alarme.

Aqui está um exemplo de um alarme desse tipo em que o Diameter Rf é configurado com FQDNs e, portanto, exige que o DNS seja resolvido. Mostrado é um FQDN que precisa ser resolvido pelo

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
```

A conexão SRP é desativada por algum motivo (externa ao par de nós PGW e o motivo não é importante para os fins deste exemplo) por mais de 7 minutos e a interceptação SNMP ThreshDNSLookupFailure é acionada.

```
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%
```

Aqui está o alarme e o registro associado:

```
[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 confirma falha de 100% para consultas AAA DNS Primário e Secundário que tentam resolver peers de Rf de Diâmetro:

%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-failed%	%dns-secondar query-timeouts%
08:32:00	16108	16098	10	10	10	0	0
08:34:00	16108	16098	10	10	10	0	0
08:36:0	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
08:56:00	18412	17250	1162	1162	1162	1152	1152

Solução

Essa armadilha/alarme pode ser ignorada e apagada, pois o nó não é realmente SRP ativo e não está tratando nenhum tráfego. Observe que a taxa de falha no exemplo acima é muito menor que a esperada de 100% e o bug CSCuu60841 já corrigiu esse problema em uma versão futura para que ele sempre reporte 100%.

alarme livre

OU

Para apagar esse alarme específico:

clear alarm id <alarm id>

Outra reviravolta desse problema pode ocorrer em um chassi de standby SRP recém-criado após um switchover SRP. O alarme também deve ser ignorado nesse cenário, pois o chassi é o SRP Standby e as falhas de DNS são, portanto, irrelevantes.

Por fim, é evidente que a causa desse alarme precisa ser investigada imediatamente em um PGW realmente ativo de SRP, pois o impacto sobre o assinante ou a cobrança provavelmente ocorrerá dependendo dos tipos de FQDNs que estão tentando ser resolvidos.