Disparadores de ThreshDNSLookupFailure da armadilha de SNMP no nó à espera SRP quando a conexão SRP saltar

Índice

Introdução

Este artigo descreve o disparador falso aparente da armadilha de ThreshDNSLookupFailure quando um salto da conexão do protocolo de redundância do serviço (SRP) ocorre em um nó do apoio SRP. O Domain Name Service da infraestrutura (DNS) é usado na vária rede da evolução dos Nós a longo prazo (LTE) indiretamente como parte do processo de configuração de chamada. Em um gateway da rede dos dados do pacote (PGW) pode ser usado para resolver todos os nomes de domínio totalmente qualificados (FQDNs) retornados na autenticação S6b, assim como para resolver FQDNs especificada como pares nas várias configurações do valor-limite do diâmetro. Se os intervalos DNS (falhas) ocorrem em um nó de ativo que processa atendimentos, a seguir este pode negativamente afetar configurações de chamada segundo que componentes confiam no DNS que funciona corretamente.

Problema

Começar em StarOS v15 lá é um limiar configurável para medir a taxa da falha de DNS da infraestrutura. No caso onde o PGW é executado com recuperação da sessão dos Inter-chassis (ICSR), há a probabilidade que se a conexão SRP entre ambos os Nós vai para baixo seja qual for a razão, e o nó à espera de seguimento entra no estado ativo pendente (mas não inteiramente ativo porque o outro nó permanece inteiramente active SRP que não supõe nenhuma outra edição), a seguir o alarme associado/armadilha DNS é provocada. Isto é porque no estado ativo pendente, o nó tenta estabelecer as várias conexões do diâmetro para as várias relações do diâmetro no contexto do ingresso na preparação potencialmente de se transformar inteiramente active SRP. Se a configuração para ALGUMAS das conexões do diâmetro é baseada na especificação espreita na configuração do valor-limite que são FQDNs em vez dos endereços IP de Um ou Mais Servidores Cisco ICM NT, a seguir aqueles pares precisam de ser resolvidos através do DNS com A (IPv4) ou o AAAA (IPv6) pergunta. Desde que o nó está no estado ativo pendente, tais perguntas TODAS FALHAM porque as respostas aos pedidos serão distribuídas ao nó de ativo (que deixará cair as respostas), que conduz à taxa de falha 100% que causa por sua vez o alarme/armadilha a ser provocado. Quando este for comportamento esperado nesta encenação, o resultado potencial é um bilhete aberto do cliente em relação ao significado do alarme.

Está aqui um exemplo de tal alarme onde o diâmetro Rf é configurado com FQDNs e exige consequentemente o DNS resolver. É mostrado um FQDN que precise de 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 vai abaixo do por qualquer motivo (externo aos pares de Nós PGW e à razão não importante para fins deste exemplo) para os minutos 7+, e os disparadores de ThreshDNSLookupFailure da armadilha de 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%
```

Estão aqui o alarme e o log 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 a falha de 100% para as perguntas preliminares e secundárias AAAA DNS que tentam resolver pares Rf do diâmetro:

%time	%dns-central-AAAA-atmpts%	%dns-preliminar-NS-AAAA-atmpts%	%dns-preliminar-NS-AAAA-fails%	%dns-preliminar-NS-pergunta-timeouts%	%dns-secundário-NS-AAAA-atmpts%	%dns-secundário-NS-AAAA-fails%	%dns-secundár NS-pergu 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

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

Estes armadilha/alarme pode ser ignorada e cancelado desde que o nó não é verdadeiramente active SRP e manipulação de nenhum tráfego. Note a taxa de falha no exemplo acima é muito mais baixos do que o 100% e o erro previstos CSCuu60841 tem fixado agora que edição em uma liberação futura de modo que sempre o relatório 100%.

cancele o alarme proeminente

OU

Apenas claro que alarme particular:

cancele o id> do <alarm identificação do alarme

Uma outra torção desta edição pode ocorrer recentemente em um chassi à espera SRP depois que um switchover SRP ocorreu. O alarme deve ser ignorado nessa encenação igualmente desde que o chassi é apoio SRP e as falhas de DNS são consequentemente irrelevantes.

Finalmente, vai sem dizer que a causa para este alarme precisa de ser investigada imediatamente verdadeiramente em um SRP PGW ativo, porque o subscritor ou o impacto de fatura ocorrerão provavelmente segundo que tipos de FQDNs estão tentando ser resolvidos.