SNMP trap ThreshDNSLookupFailure desencadena en el nodo en espera SRP cuando rebota la conexión SRP

Contenido

Introducción

En este artículo se describe el aparente disparador falso de la trampa ThreshDNSLookupFailure cuando se produce un rebote de conexión del protocolo de redundancia de servicio (SRP) en un nodo en espera de SRP. El servicio de nombres de dominio de infraestructura (DNS) se utiliza indirectamente en varios nodos de la red de evolución a largo plazo (LTE) como parte del proceso de configuración de llamadas. En una puerta de enlace de red de datos de paquetes (PGW), se puede utilizar para resolver cualquier nombre de dominio completamente calificado (FQDN) devuelto en la autenticación S6b, así como para resolver los FQDN especificados como pares en las diversas configuraciones de punto final de diámetro. Si se producen tiempos de espera (fallos) de DNS en llamadas de procesamiento de nodos activos, esto puede afectar negativamente a la configuración de llamadas dependiendo de los componentes en los que se confía el funcionamiento correcto del DNS.

Problema

A partir de StarOS v15, existe un umbral configurable para medir la tasa de fallos DNS de la infraestructura. En el caso de que el PGW se implemente con la recuperación de sesiones entre chasis (ICSR), es probable que si la conexión SRP entre ambos nodos se desactiva por la razón que sea, y el nodo en espera subsiguiente entra en estado Activo pendiente (pero no completamente activo porque el otro nodo permanece totalmente activo suponiendo que no haya otros problemas), se activa la alarma/trampa DNS asociada. Esto se debe a que, en el estado activo pendiente, el nodo intenta establecer las diversas conexiones de diámetro para las diversas interfaces de diámetro en el contexto de ingreso como preparación para convertirse potencialmente en un SRP activo. Si la configuración para CUALQUIERA de las conexiones de diámetro se basa en la especificación de peers en la configuración de punto final que son FQDN en lugar de direcciones IP, estos peers deben resolverse a través de las consultas DNS con A (IPv4) o AAAA (IPv6). Dado que el nodo está en estado activo pendiente, estas consultas FALLAN TODOS porque las respuestas a las solicitudes se enrutarán al nodo activo (que descartará las respuestas), lo que da como resultado una tasa de falla del 100% que, a su vez, hace que se active la alarma/trampa. Si bien se espera que esto ocurra en esta situación, el resultado potencial es un ticket abierto del cliente con respecto a la importancia de la alarma.

Este es un ejemplo de una alarma en la que Diámetro Rf se configura con FQDN y, por lo tanto, requiere que DNS se resuelva. Se muestra un FQDN que necesita ser resuelto por 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 conexión SRP deja de funcionar por algún motivo (externa al par de nodos PGW y el motivo no importante para los fines de este ejemplo) durante más de 7 minutos, y se activan los desencadenadores SNMP trap ThreshDNSLookupFailure.

```
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%
```

Aquí está la alarma y el registro asociado:

```
[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 una falla del 100% en las consultas de DNS AAAA principal y secundario que intentan resolver pares de Rf de diámetro:

%time %	%dns-central-aaaa-atmpts%	%dns-primary-ns-aaaa-atmpts%	%dns-primary-ns-aaa-failure%	%dns-primary-ns-query-timeouts%	%dns-secondary-ns-aaaa-atmpts%	%dns-secondary-ns-aaa-failure%	%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

Solución

Esta trampa/alarma se puede ignorar y borrar ya que el nodo no está realmente activo en SRP y no maneja tráfico alguno. Observe que la tasa de fallas en el ejemplo anterior es mucho menor que la esperada 100% y el error CSCuu60841 ha corregido ese problema en una futura versión para que siempre informe 100%.

clear alarm extraordinario

O

Para aclarar esa alarma en particular:

clear alarm id <alarm id>

Otro giro de este problema puede ocurrir en un nuevo chasis SRP Standby después de que se haya producido un switchover SRP. La alarma también debe ignorarse en ese escenario, ya que el chasis es SRP Standby y, por lo tanto, las fallas de DNS son irrelevantes.

Por último, huelga decir que la causa de esta alarma debe investigarse inmediatamente en un PGW realmente activo de SRP, ya que el impacto del suscriptor o de la facturación probablemente ocurra dependiendo de qué tipos de FQDN están intentando resolverse.