Contenido

Introducción

Este artículo describe el activador falso evidente del desvío de ThreshDNSLookupFailure cuando una despedida de la conexión del Redundancy Protocol del servicio (SRP) ocurre en un nodo del recurso seguro SRP. Utilizan al servicio de nombre del dominio de la infraestructura (DNS) en la diversa red de la evolución de los Nodos a largo plazo (LTE) indirectamente como parte del proceso de configuración de llamada. En un gateway de la red de los datos del paquete (PGW) puede ser utilizado para resolver cualquier nombre de dominio completamente calificado (FQDN) vuelto en la autenticación S6b, así como para resolver los FQDN especificada como pares en las diversas configuraciones del punto final del diámetro. Si los descansos DNS (errores) ocurren en un nodo activo que procesa las llamadas, después éste puede afectar negativamente a las configuraciones de la llamada dependiendo de qué componentes confían en el DNS que funciona correctamente.

Problema

El comenzar en StarOS v15 allí es un umbral configurable para medir la tarifa del error de DNS de la infraestructura. En el caso donde el PGW se implementa con la recuperación de la sesión del Inter-chasis (ICSR), hay la probabilidad se acciona que si la conexión SRP entre ambos Nodos va abajo para cualquier razón, y el nodo espera de seguimiento entra el estado activo pendiente (pero no completamente activo porque el otro nodo sigue siendo completamente active SRP si se asume que ningún otro problema), después la alarma asociada/desvío DNS. Esto es porque en el estado activo pendiente, el nodo intenta establecer las diversas conexiones del diámetro para las diversas interfaces del diámetro en el contexto del ingreso en la preparación potencialmente de convertirse en completamente active SRP. Si la configuración para las conexiones unas de los del diámetro se basa en especificar mira en la configuración del punto final que son FQDN en vez de los IP Addresses, después esos pares necesitan ser resueltos vía el DNS con A (IPv4) o el AAAA (IPv6) pregunta. Puesto que el nodo está en el estado activo pendiente, tales interrogaciones TODAS FALLAN porque las respuestas a las peticiones serán ruteadas al nodo activo (que caerá las respuestas), que da lugar a la tasa de fallas 100% que a su vez causa la alarma/el desvío que se accionarán. Mientras que ésta es conducta esperada en este escenario, el resultado potencial es un boleto abierto del cliente con respecto a la significación de la alarma.

Aquí está un ejemplo de tal alarma donde el diámetro Rf se configura con los FQDN y por lo tanto requiere el DNS resolver. Se muestra un FQDN que necesita ser resuelto por el DNS.

La conexión SRP va abajo del por alguna razón (externo a los pares de Nodos PGW y la razón no importante con el propósito de este ejemplo) para los minutos 7+, y los activadores de ThreshDNSLookupFailure del SNMP trap.

```
Tue Nov 25 08:43:42 2014 Internal trap notification 1037 (SRPConnDown)
vpn SRP ipaddr 10.211.220.100 rtmod 3Tue Nov 25 08:43:42 2014 Internal trap notification 120
```

```
(SRPActive)
vpn SRP ipaddr 10.211.208.165 rtmod 3Tue Nov 25 08:51:14 2014 Internal trap notification 1038
(SRPConnUp)
vpn SRP ipaddr 10.211.220.100 rtmod 3Tue Nov 25 08:51:14 2014 Internal trap notification 121
(SRPStandby)
vpn SRP ipaddr 10.211.208.165 rtmod 9Tue 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 verboseSeverity 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 el error del 100% para las interrogaciones primarias y secundarias AAAA DNS que intentan resolver a los pares Rf del diámetro:

el %time %	%dns-central-AAAA-atmpts%	%dns-primario-NS-AAAA-atmpts%	%dns-primario-NS-AAAA-fails%	%dns-primario-NS-interrogación-timeouts%	%dns-secundario-NS-AAAA-atmpts%	%dns-secundario-NS-AAAA-fails%	%dns-secundar NS-interroga 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
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

Este desvío/alarma puede ser ignorado y ser borrado puesto que el nodo no es verdad active SRP y manipulación de ningún tráfico. Observe la tasa de fallas en el ejemplo anterior es mucho más bajos que el 100% y el bug previstos CSCuu60841 ahora ha reparado ese problema en una futura versión de modo que siempre el informe el 100%.

borre la alarma excepcional

O

Para apenas claro que alarma determinada:

borre el id> del <alarm identificación de la alarma

Otra torsión de este problema puede ocurrir en nuevamente un chasis espera SRP después de que haya ocurrido un intercambio SRP. La alarma se debe ignorar en ese escenario también puesto que el chasis es recurso seguro SRP y los errores de DNS son por lo tanto inútiles.

Finalmente, es evidente que la causa para esta alarma necesita ser investigada inmediatamente en verdad un SRP PGW activo, pues el suscriptor o el impacto que carga en cuenta ocurrirá probablemente dependiendo de qué tipos de FQDN están intentando ser resueltos.