Содержание

Введение

Когда сильный удар соединения Сервисного протокола резервирования (SRP) происходит на резервном узле SRP, эта статья описывает очевидный ложный триггер trap-сообщения ThreshDNSLookupFailure. Сервис имен Домена инфраструктуры (DNS) используется на различных узлах в долгосрочной перспективе сеть Evolution (LTE) косвенно как часть процесса настройки вызова. В Пакетной сети передачи данных шлюз (PGW) это может использоваться, чтобы решить, что любые Полные доменные имена (FQDNs) возвратились на аутентификации S6b, а также решить FQDNs, заданный как узлы в различных конфигурациях оконечной точки Диаметра. Если таймауты DNS (сбои) происходят на активном узле, обрабатывающем вызовы, то это может негативно влиять на настройки вызова в зависимости от того, какие компоненты полагаются на DNS, функционирующий должным образом.

Проблема

При начале в StarOS v15 существует настраиваемое пороговое значение для измерения скорости Ошибки DNS инфраструктуры. В случае, где PGW внедрен с Восстановлением сеанса межшасси (ICSR), существует вероятность, что, если соединение SRP между обоими узлами выключается по любой причине, и следующий Резервный узел входит в Активное состояние в состоянии ожидания (но не полностью активный, потому что другой узел остается полностью SRP активное принятие никаких других проблем), тогда связанный сигнал тревоги/trap-сообщение DNS инициирован. Это вызвано тем, что в активном состоянии в состоянии ожидания, узел пытается установить различные соединения диаметра для различных интерфейсов диаметра во входном контексте в подготовке потенциального становления полностью активным SRP. Если конфигурация для ANY соединений диаметра основывается на определении узлов в конфигурации оконечной точки, которые являются FQDNs вместо IP-адресов, то те узлы должны быть решены через DNS с (IPv4) или AAAA (IPv6) запросы. Так как узел находится в активном состоянии в состоянии ожидания, такие запросы СБОЙ ALL, потому что ответы на запросы будут маршрутизироваться к активному узлу (который отбросит ответы), который приводит к 100%-й интенсивности отказов, которая в свою очередь заставляет сигнал тревоги/trap-сообщение быть инициированным. В то время как это - нормальное поведение в этом сценарии, потенциальным результатом является открытый билет клиента относительно значения сигнала тревоги.

Вот пример такого сигнала тревоги, где Диаметр, Rf настроен с FQDNs и поэтому требует, чтобы решил DNS. Показанный FQDN, который должен быть решен DNS.

Соединение SRP выключается по некоторым причинам (внешний к паре узлов PGW и причины, не важной в целях данного примера) для 7 + минуты и trap-сообщение SNMP триггеры ThreshDNSLookupFailure.

```
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%
```

Вот сигнал тревоги и привязанный журнал:

```
[local]XGW> show alarm outstanding verboseSeverity Object          Timestamp
Alarm ID-------- ----------      -------------------------------- ------------------  Alarm
Details--------------------------------------------------------------------------------Minor
VPN XGWin       Tuesday November 25 09:00:0        361158393531727872O<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 подтверждает 100%-й сбой для Основных и Вторичных запросов DNS AAAA, пытающихся решить Диаметр узлы Rf:

% %time	% %dns-central-aaaa-atmpts	% %dns-primary-ns-aaaa-atmpts	% %dns-primary-ns-aaaa-fails	% %dns-primary-ns-query-timeouts	% %dns-secondary-ns-aaaa-atmpts	% %dns-secondary-ns-aaaa-fails	% %dns-secondar query-tim
8:32:00	16108	16098	10	10	10	0	0
8:34:00	16108	16098	10	10	10	0	0
8:36:00	16108	16098	10	10	10	0	0
8:38:00	16108	16098	10	10	10	0	0
8:40:00	16108	16098	10	10	10	0	0
8:42:00	16108	16098	10	10	10	0	0
8:44:00	16236	16162	74	74	74	64	64
8:46:00	16828	16466	362	362	362	352	352
8:48:00	17436	16770	666	666	666	656	656
8:50:00	18012	17058	954	954	954	944	944
8:52:00	18412	17250	1162	1162	1162	1152	1152
8:54:00	18412	17250	1162	1162	1162	1152	1152
8:56:00	18412	17250	1162	1162	1162	1152	1152

Решение

Это trap-сообщение/сигнал тревоги может быть проигнорировано и очищено, так как узлом не является действительно активный SRP и не обрабатывающий никакой трафик. Обратите внимание, что интенсивность отказов в приведенном выше примере намного ниже, чем ожидаемые 100% и дефект, CSCuu60841 теперь устранил ту проблему в будущем выпуске так, чтобы это всегда сообщило о 100%.

очистите выдающийся сигнал тревоги

Или

Просто очистить ту особую тревогу:

очистите сигнальный идентификатор <сигнальный идентификатор>

Другое скручивание этой проблемы может произойти на недавно Резервное шасси SRP после того, как переключатель SRP имел место. Сигнал тревоги должен быть проигнорирован в том сценарии также, так как шасси является Резервом SRP, и Ошибки DNS поэтому не важны.

Наконец, это само собой разумеется, что причина для этого сигнала тревоги должна быть сразу исследована на действительно SRP активный PGW, поскольку абонент или тарифицирующий влияние, вероятно, произойдет в зависимости от того, какие типы FQDNs пытаются быть решенными.