

Inundação ciscoConfigManEvent da armadilha da rede principal

Índice

[Introdução](#)

[Problema](#)

[Solução](#)

Introdução

Este documento descreve a causa, as repercussões, e a solução a um problema onde você receba uma inundação de armadilhas ([ciscoConfigManEvent](#)) da **notificação de evento do Gerenciamento de configuração Cisco na rede da prima de Cisco**.

Problema

Os dispositivos de rede puderam ser configurados de tal maneira que quando uma **corrida** ou um **comando conf t da mostra** são inscritos em um dispositivo, o dispositivo manda uma armadilha **ciscoConfigManEvent**. Se o dispositivo é monitorado pela rede da prima de Cisco, você pode ver estas armadilhas na aba da armadilha da visão do evento como eventos da **notificação de evento do Gerenciamento de configuração Cisco**.

Uma inundação destas armadilhas ocorre porque a rede principal de Cisco executa um comando **do id> do <interface da relação da corrida da mostra aos** dispositivos para cada relação definida dentro do dispositivo. Isto ocorre cada ciclo de polling, que é cada 15 minutos à revelia. A maioria dos clientes experimenta agora uma inundação destes tipos de eventos. Os grandes provedores de serviços podem ter um alto número de relações em cada dispositivo, e é comum ver diversos milhares destes eventos dentro da rede da prima de Cisco cada minuto.

Isto causa muitos efeitos secundários, como:

- O base de dados (DB) torna-se completamente, e o espaço temporário é executado para fora.
- Os clientes experimentam o desempenho devido lento GUI ao número grande de eventos no DB.
- Há um alto número de eventos *órfãos no DB* (os eventos que não são associados com um bilhete e não são arquivados).
- Há um processamento mais lento do elemento da armadilha e de rede virtual (VNE) devido o ao número grande de eventos.

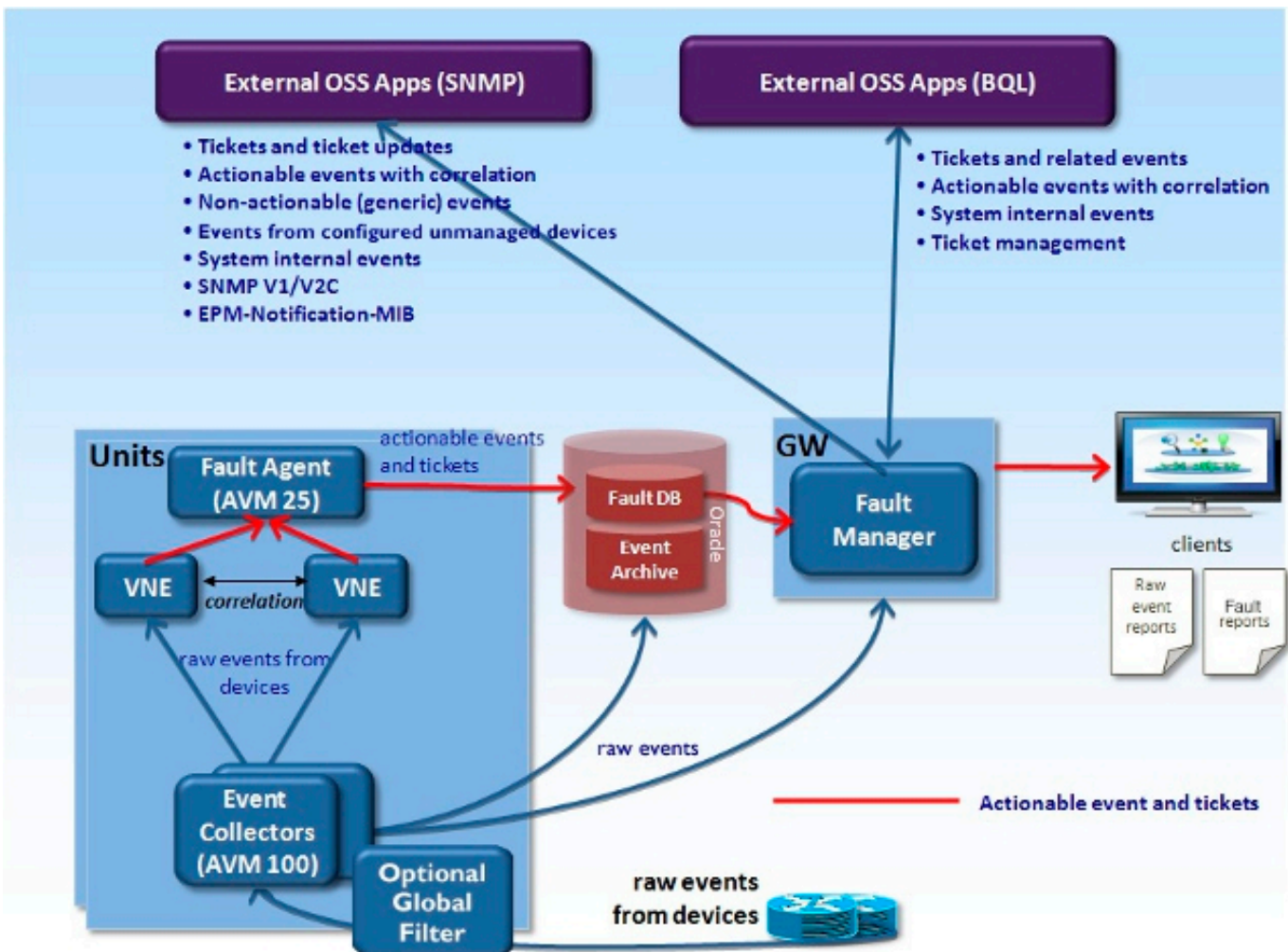
Solução

A melhor solução para este problema é mudar a configuração dos dispositivos de rede de modo que não enviem estes tipos de armadilhas ao servidor de rede principal. Contudo, isto não é prático em alguns grandes sistemas do provedor de serviços. Esta seção fornece uma ação alternativa para este problema. O objetivo desta ação alternativa é filtrar as armadilhas assim que alcançarem o coletor do evento (AVM 100).

Nota: Para as versões de rede 4.0 da prima de Cisco e mais atrasado, refira o [guia de administrador de rede da prima de Cisco, 4.0](#) a fim obter uma solução a este problema. A ação alternativa que é descrita neste documento é para todas as versões da abstração da rede ativa (ANA) assim como todas as versões de rede 3.11 da prima de Cisco e mais adiantado.

Cuidado: Se você permite o filtro **ciscoConfigManEvent** da armadilha, a seguir as armadilhas **ciscoConfigManEvent** não salvar ao arquivo do evento; conseqüentemente, não estão disponíveis para relatórios.

Normalmente, as armadilhas estão filtradas a nível VNE depois que estão escritas na persistência do evento (EP) DB (conhecida geralmente como o arquivo do evento). A fim impedir este processamento, um filtro global opcional é exigido:



Incorpore estes comandos como a ANA ou o usuário de rede principal do diretório ~/Main a fim

filtrar este tipo de armadilha assim que participar no sistema:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/enable true
```

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/classcom.sheer.metrocentral.  
framework.instrumentation.trap.matcher.RawEventSnmpMatcher
```

```
./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/matcher-conf
```

```
./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/matcher-conf/rule-1
```

```
./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/matcher-conf/rule-1/varbinds
```

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/matcher-conf/rule-1/varbinds  
/varbind-1 ".1.3.6.1.6.3.1.1.4.1={o}.1.3.6.1.4.1.9.9.43.2.0.1"
```

Incorpore estes comandos a fim desabilitar os comandos precedentes:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/enable false
```

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/class com.sheer.metrocentral.  
framework.instrumentation.trap.matcher.ExcludeAllMatcher
```

```
./runRegTool.sh -gs 127.0.0.1 remove 0.0.0.0 site/trap/agents/trap/processors  
/snmp-processors/snmp-processor4/matcher/matcher-conf
```

Nota: Alguns clientes têm os dispositivos configurados de modo que cada armadilha seja enviada encapsulada em um Syslog. Se este é o caso, você deve adicionar uma regra no processador do Syslog para aqueles igualmente.