Inondation ciscoConfigManEvent de déroutement de réseau principal

Contenu

Introduction

Ce document décrit la cause, les répercussions, et la solution à un problème où vous recevez une pléthore de déroutements (ciscoConfigManEvent) de **notification d'événement de gestion de la configuration de Cisco** dans le réseau de perfection de Cisco.

Problème

Des périphériques de réseau pourraient être configurés de telle manière que quand une **exposition fonctionnent** ou commande du **conf t** est écrit sur un périphérique, le périphérique envoie un déroutement **ciscoConfigManEvent**. Si le périphérique est surveillé par le réseau de perfection de Cisco, vous pouvez visualiser ces déroutements dans l'onglet de déroutement de la vision d'événement en tant qu'événements de **notification d'événement de gestion de la configuration de Cisco**.

Une pléthore de ces déroutements se produit parce que le réseau principal de Cisco exécute une commande d'**id> de <interface d'interface de passage d'exposition aux** périphériques pour chaque interface définie dans le périphérique. Ceci se produit chaque cycle de sondage, qui est toutes les 15 minutes par défaut. La majorité de clients éprouvent maintenant une pléthore de ces types d'événements. Les grands fournisseurs de services peuvent avoir un nombre élevé d'interfaces sur chaque périphérique, et il est commun pour voir plusieurs milliers de ces événements dans le réseau de perfection de Cisco chaque minute.

Ceci entraîne beaucoup d'effets secondaires, comme :

- La base de données (DB) devient complètement, et l'espace provisoire s'épuise.
- Les clients éprouvent la représentation lente GUI due au grand nombre d'événements dans le DB.
- Il y a un nombre élevé d'événements *orphelins* dans le DB (les événements qui ne sont pas associés avec un ticket et ne sont pas archivés).
- Il y a traitement de l'élément de déroutement plus lent et de réseau virtuel (VNE) dû au grand nombre d'événements.

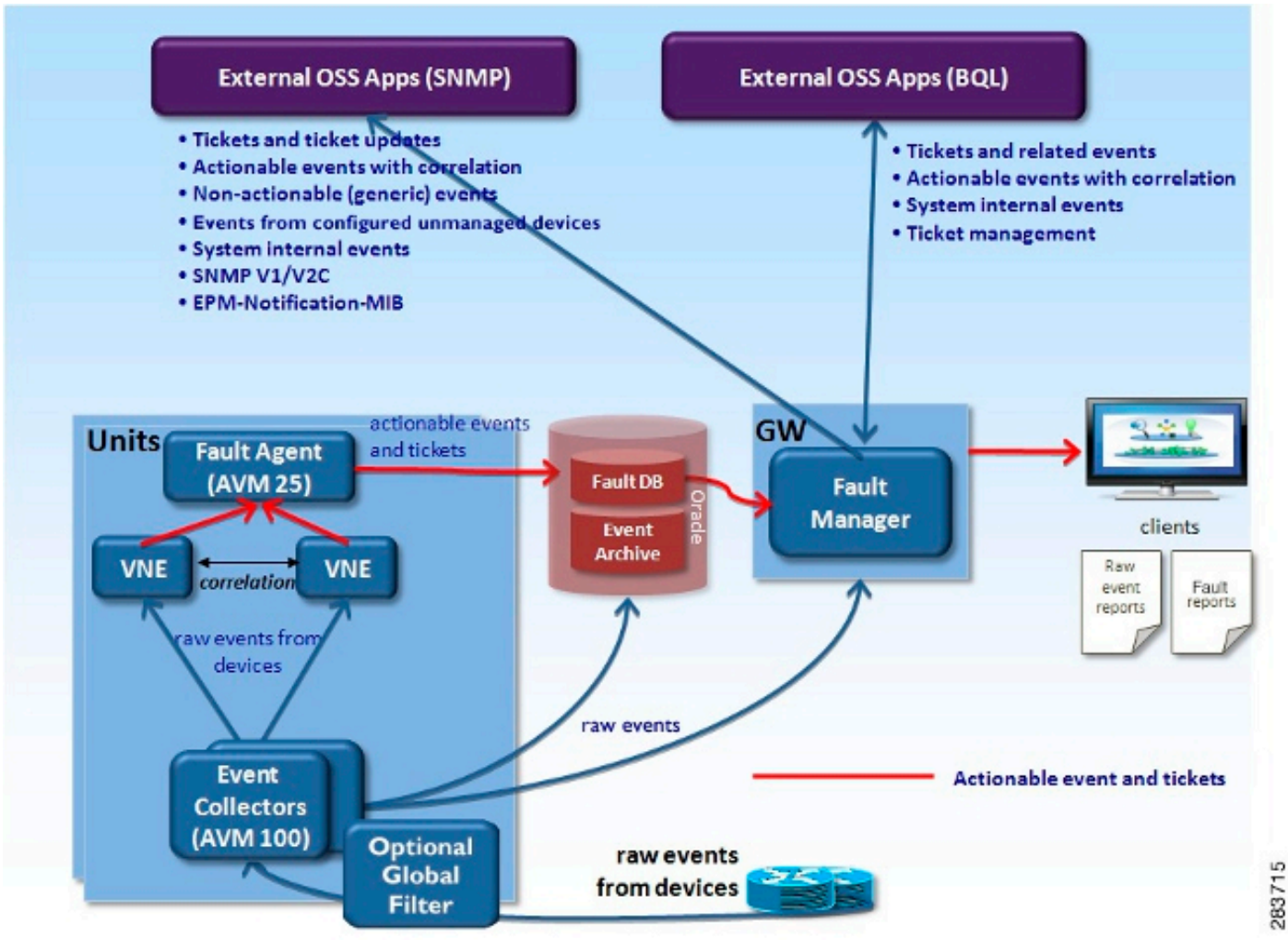
Solution

La meilleure solution pour ce problème est de changer la configuration des périphériques de réseau de sorte qu'ils n'envoient pas ces types de déroutements au serveur de réseau principal. Cependant, ce n'est pas pratique dans quelques grands systèmes de fournisseur de services. Cette section fournit un contournement pour ce problème. Le but de ce contournement est de filtrer les déroutements dès qu'ils atteindront le collecteur d'événement (AVM 100).

> Remarque: Pour des versions 4.0 et ultérieures de réseau de perfection de Cisco, référez-vous au guide d'administrateur réseau de perfection de Cisco, 4.0 afin d'obtenir une solution à ce problème. Le workaround qui est décrit dans ce document est pour toutes les versions actives d'abstraction de réseau (ANA) aussi bien que toutes les versions 3.11 et antérieures de réseau de perfection de Cisco.

> **Attention** : Si vous activez le filtre **ciscoConfigManEvent de** déroutement, alors les déroutements **ciscoConfigManEvent** ne sont pas enregistrés aux archives d'événement ; donc, ils ne sont pas disponibles pour des états.

Normalement, des déroutements sont filtrés au niveau VNE après qu'ils soient écrits dans le DB de la persistance d'événement (PE) (généralement connu sous le nom d'archives d'événement). Afin d'empêcher ce traitement, un filtre global facultatif est exigé :



Sélectionnez ces commandes en tant qu'ANA ou utilisateur du réseau principal à partir du

répertoire ~/Main afin de filtrer ce type de déroutement dès qu'il entrera dans le système :

```
./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"
```

Sélectionnez ces commandes afin de désactiver les commandes précédentes :

```
./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
```

> Remarque: Quelques clients font configurer les périphériques de sorte que chaque déroutement soit envoyé encapsulé dans un Syslog. Si c'est le cas, vous devez ajouter une règle sur le processeur de Syslog pour ceux également.