Prime Network ciscoConfigManEvent Trap Flood

TAC **Document ID: 117695**

Contributed by Thomas Maneri, Cisco TAC Engineer.
Jul 01, 2014

Contents

Introduction

This document describes the cause, repercussions, and solution to a problem where you receive a flood of ***Cisco Configuration management event notification*** (ciscoConfigManEvent) traps in the Cisco Prime Network.

Problem

Network devices might be configured in such a way that when a ***show run*** or ***conf t*** command is entered on a device, the device sends out a ***ciscoConfigManEvent*** trap. If the device is monitored by Cisco Prime Network, you can view these traps in the Trap tab of the Event Vision as ***Cisco Configuration management event notification*** events.

A flood of these traps occurs because Cisco Prime Network executes a ***show run interface <interface id>*** command to the devices for every interface defined within the device. This occurs every polling cycle, which is every 15 minutes by default. The majority of customers now experience a flood of these types of events. Large service providers can have a high number of interfaces on each device, and it is common to see several thousands of these events within the Cisco Prime Network every minute.

This causes many side effects, such as:

- The Database (DB) becomes full, and the temporary space runs out.
- Customers experience slow GUI performance due to the large number of events in the DB.
- There is a high number of *orphan* events in the DB (events that are not associated with a ticket and are not archived).
- There is slower trap and Virtual Network Element (VNE) processing due to the the large number of events.

Solution

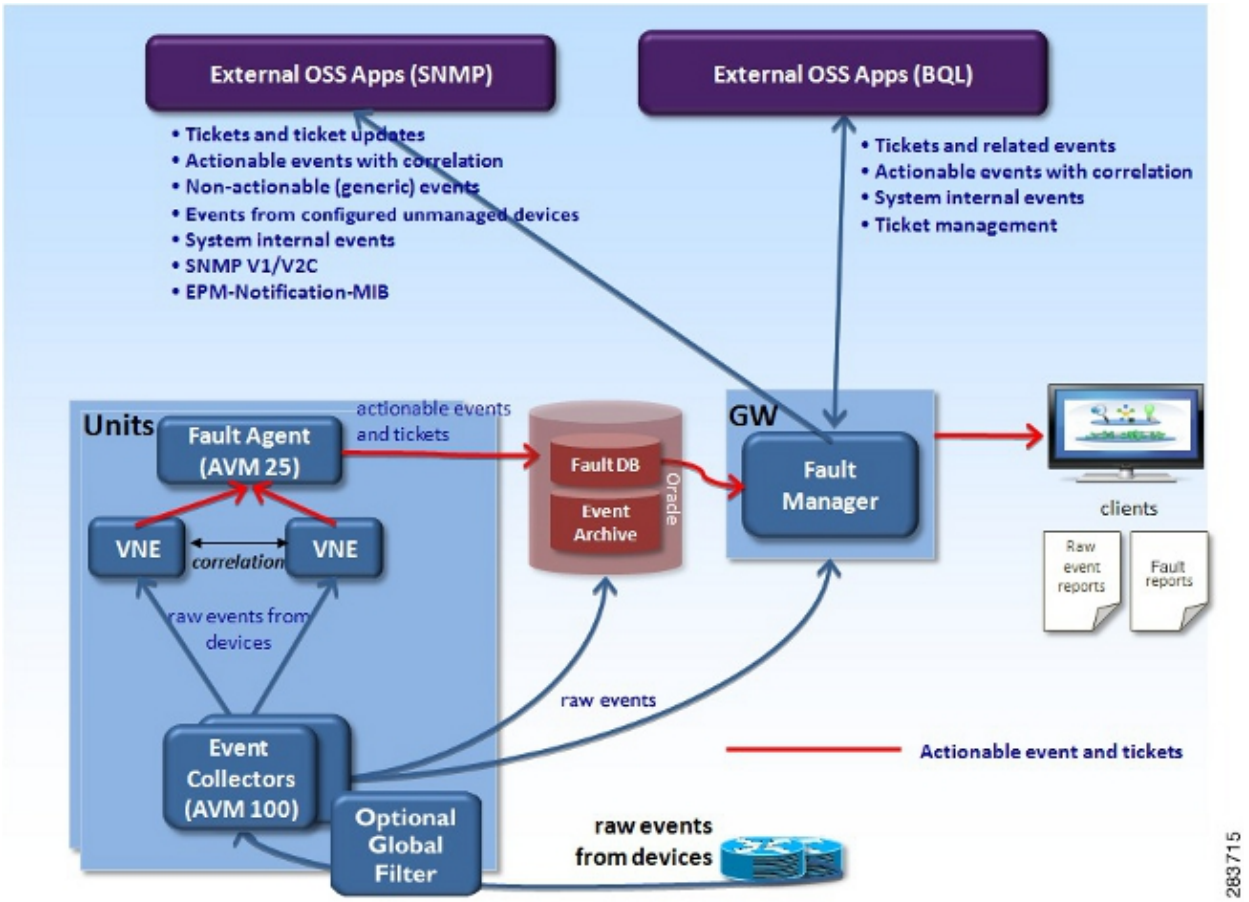
The best solution for this problem is to change the configuration of the network devices so that they do not send these types of traps to the Prime Network server. However, this is not practical in some large service provider systems. This section provides a workaround for this problem. The goal of this workaround is to filter the traps as soon as they reach the Event Collector (AVM 100).

Note: For Cisco Prime Network Versions 4.0 and later, refer to the Cisco Prime Network Administrator Guide, 4.0 in order to obtain a solution to this problem. The workaround that is described in this document is for all Active Network Abstraction (ANA) versions as well as all Cisco Prime Network Versions 3.11 and

earlier.

Caution: If you enable the ***ciscoConfigManEvent*** trap filter, then the ***ciscoConfigManEvent*** traps are not saved to the Event Archive; therefore, they are not available for reports.

Normally, traps are filtered at the VNE level after they are written into the Event Persistence (EP) DB (commonly known as the Event Archive). In order to prevent this processing, an Optional Global Filter is required:



Enter these commands as the ANA or Prime Network user from the ~/Main directory in order to filter this type of trap as soon as it enters into the system:

```
./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"
```

Enter these commands in order to disable the previous commands:

```
./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
```

Note: Some customers have the devices configured so that each trap is sent encapsulated into a syslog. If this is the case, you must add a rule on the syslog processor for those also.

Updated: Jul 01, 2014 Document ID: 117695
