Logger Restart Generates Old SNMP Traps

Document ID: 91626

Contents

Introduction

This document describes out of date Simple Network Management Protocol (SNMP) trap messages in a Cisco Unified Intelligent Contact Management (ICM) Enterprise environment and provides two possible methods to prevent these informational messages from being reported.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ICM Enterprise
- An understanding of SNMP

Components Used

This document is not restricted to specific software and hardware versions.

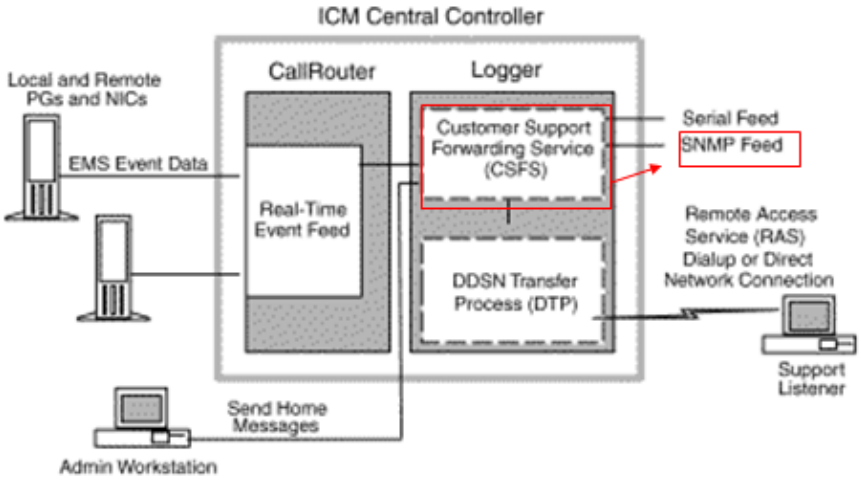
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The ICM's Logger collects events and messages from all components of the system. The Logger passes this information to the Customer Support Forwarding Service (CSFS) process that receives events, filters them and holds them in memory on the Logger as Figure 1 shows. The SNMP feed is an optional ICM feature that allows you to receive an event feed through an SNMP compliant interface (TCP/IP). When you use the SNMP feed, you can configure it to send the SNMP traps to the desired management client.

Figure 1 CSFS Feed



Problem

By design, after you restart one logger in a duplexed environment, or if one logger bounces, out of date SNMP traps might be generated and displayed in the configured SNMP management station(s). When the CSFS process is started as part of the Logger, it receives an event (alarm) to be reported to the remote client (via SNMP, Syslog or the Remote Monitoring Service [RMS]) and it saves a copy of the event in memory, called a base record. In a duplexed, fault tolerant environment, when the CSFS process on one side goes down and then restarts, it receives all outstanding base records from the other side and forwards them to the management client.

Solutions

This section describes the possible methods you can use to prevent out−dated SNMP information from being reported. Solution 1 shows you how to purge out−dated SNMP information from the logger and Solution 2 shows you how to suppress or filter out−dated SNMP information from the management client.

Solution 1

Purge the base records. In order to do this, stop the Loggers on both sides simultaneously and then restart them. This process purges all out of date SNMP traps from the CSFS process.

Note: This procedure should be done during a maintenance window or during low−route impact times.

1. Stop Logger B.
2. Stop Logger A.
3. Start Logger A.
4. Start Logger B.

Solution 2

An alternative solution is to have the customer's management client filter alarms that are older than a certain duration, for example, one week. Each trap that the SNMP service sends to the customer's second party application (such as HP OpenView) contains a timestamp of when the actual event occurs. Customers can then configure their third party application to disregard alarms with a time stamp older than a particular number of days or weeks. It is important to note that the Cisco Contact Center Technical Assistance Center (TAC) does not assist in the configuration of the particular third party application that the customer chooses to use to manage these events / traps.

Related Information

- **Cisco Unified Intelligent Contact Management Enterprise Support Documentation**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 10, 2007 Document ID: 91626