Il riavvio del logger genera trap SNMP obsolete

Sommario

Introduzione

Questo documento descrive i messaggi trap SNMP (Simple Network Management Protocol) non aggiornati in un ambiente Enterprise Cisco Unified Intelligent Contact Management (ICM) e fornisce due possibili metodi per impedire la segnalazione di questi messaggi informativi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ICM Enterprise
- Conoscenza del protocollo SNMP

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

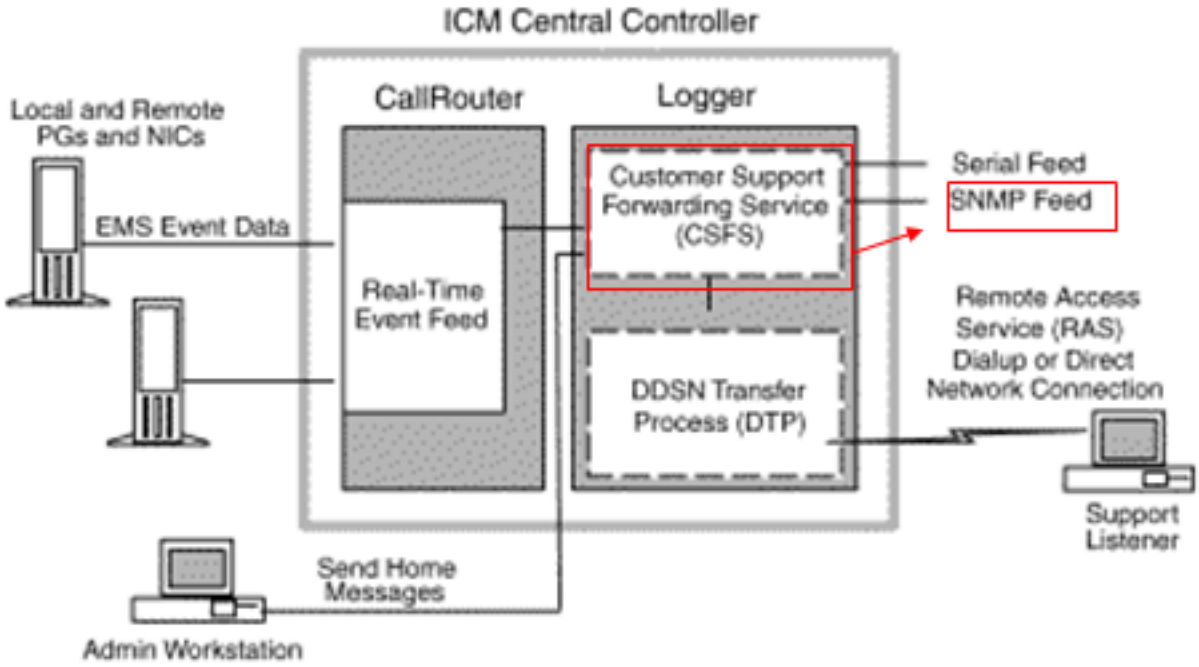
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il logger dell'ICM raccoglie eventi e messaggi da tutti i componenti del sistema. Il Logger trasmette queste informazioni al processo CSFS (Customer Support Forwarding Service) che riceve gli eventi, li filtra e li conserva in memoria sul Logger, come mostrato nella Figura 1. Il feed SNMP è una funzione ICM opzionale che consente di ricevere un feed di eventi tramite un'interfaccia conforme a SNMP (TCP/IP). Quando si utilizza il feed SNMP, è possibile configurarlo in modo da inviare le trap SNMP al client di gestione desiderato.

Figura 1 - Avanzamento CSFS



Problema

In base alla progettazione, dopo il riavvio di un logger in un ambiente duplex o se un registratore rimbalza, è possibile che nelle stazioni di gestione SNMP configurate vengano generate e visualizzate trap SNMP non aggiornate. Quando il processo CSFS viene avviato come parte del Logger, riceve un evento (allarme) da segnalare al client remoto (tramite SNMP, Syslog o il Servizio di monitoraggio remoto [RMS]) e salva in memoria una copia dell'evento, chiamata record di base. In un ambiente duplex a tolleranza di errore, quando il processo CSFS su un lato si interrompe e quindi si riavvia, riceve tutti i record di base in sospeso dall'altro lato e li inoltra al client di gestione.

Soluzioni

In questa sezione vengono descritti i possibili metodi da utilizzare per impedire la segnalazione di informazioni SNMP obsolete. La soluzione 1 mostra come eliminare le informazioni SNMP obsolete dal logger e la soluzione 2 mostra come eliminare o filtrare le informazioni SNMP obsolete dal client di gestione.

Soluzione 1

Eliminare i record di base. A tale scopo, arrestare i logger su entrambi i lati simultaneamente e quindi riavviarli. Questo processo elimina tutte le trap SNMP non aggiornate dal processo CSFS.

Nota: questa procedura deve essere eseguita durante un intervento di manutenzione o durante i

tempi di impatto del percorso ridotto.

1. Arrestare il logger B.
2. Arrestare Il Logger A.
3. Avviare il logger A.
4. Avviare il logger B.

Soluzione 2

Una soluzione alternativa consiste nel filtrare gli allarmi del client di gestione del cliente più vecchi di una determinata durata, ad esempio una settimana. Ogni trap inviata dal servizio SNMP all'applicazione di seconda parte del cliente (ad esempio HP OpenView) contiene un indicatore orario del momento in cui si verifica l'evento effettivo. I clienti possono quindi configurare l'applicazione di terze parti in modo da ignorare gli allarmi con un indicatore di data e ora antecedente a un determinato numero di giorni o settimane. È importante notare che il Cisco Contact Center Technical Assistance Center (TAC) non assiste il cliente nella configurazione della particolare applicazione di terze parti che sceglie di utilizzare per gestire questi eventi/trap.

Informazioni correlate

- Documentazione di supporto Enterprise per Cisco Unified Intelligent Contact Management
- Documentazione e supporto tecnico – Cisco Systems