Mensagens TPM C460 M4 nos registros SEL

Contents

Introduction

A intenção deste documento é resolver o problema observado em relação aos eventos SEL (System Event Logs, registros de eventos do sistema) relacionados ao TPM (Trusted Platform Module) em alguns servidores C460 M4. Um pequeno número de servidores C460 M4 SPARE verá um evento SEL crítico relacionado à presença de TPM logo fora da fábrica. As instruções abaixo o ajudarão a resolver os servidores afetados por esse problema.

Problema

Sistemas com impacto potencial:

Cerca de 614 sistemas C460 M4 sobressalentes (enviados entre 2 de junho de 2014 e 13 de abril de 2016).

Visibilidade/impacto do cliente:

Os clientes podem ver um evento SEL crítico semelhante ao abaixo nos servidores recebidos da fábrica.


Event Log

<<Newest <Newer Log Entries 1 to 2 (2) Older> Oldest>>

Time (UTC)	Severity	
2016-04-13 11:16:17	Critical	TPM_FAULT_STATUS: Add-in Card sensor, Predictive Failure asserted

NÃO há impacto operacional no servidor, mas a mensagem pode levar a uma preocupação desnecessária, resultando em uma chamada para o TAC. Isso tem a ver com o modo como os TPMs eram manipulados na fabricação. Os sistemas C460 M4 mantêm um valor "em cache" para a presença de TPM, indicando se um TPM já foi instalado no servidor - cada servidor tem um TPM instalado durante o teste. O C460 M4 também rastreia a precisão atual do TPM e, como todos os servidores solicitados como peças sobressalentes são enviados sem um TPM, o sistema dispara um alarme pensando que o módulo que foi instalado foi removido.

Solução

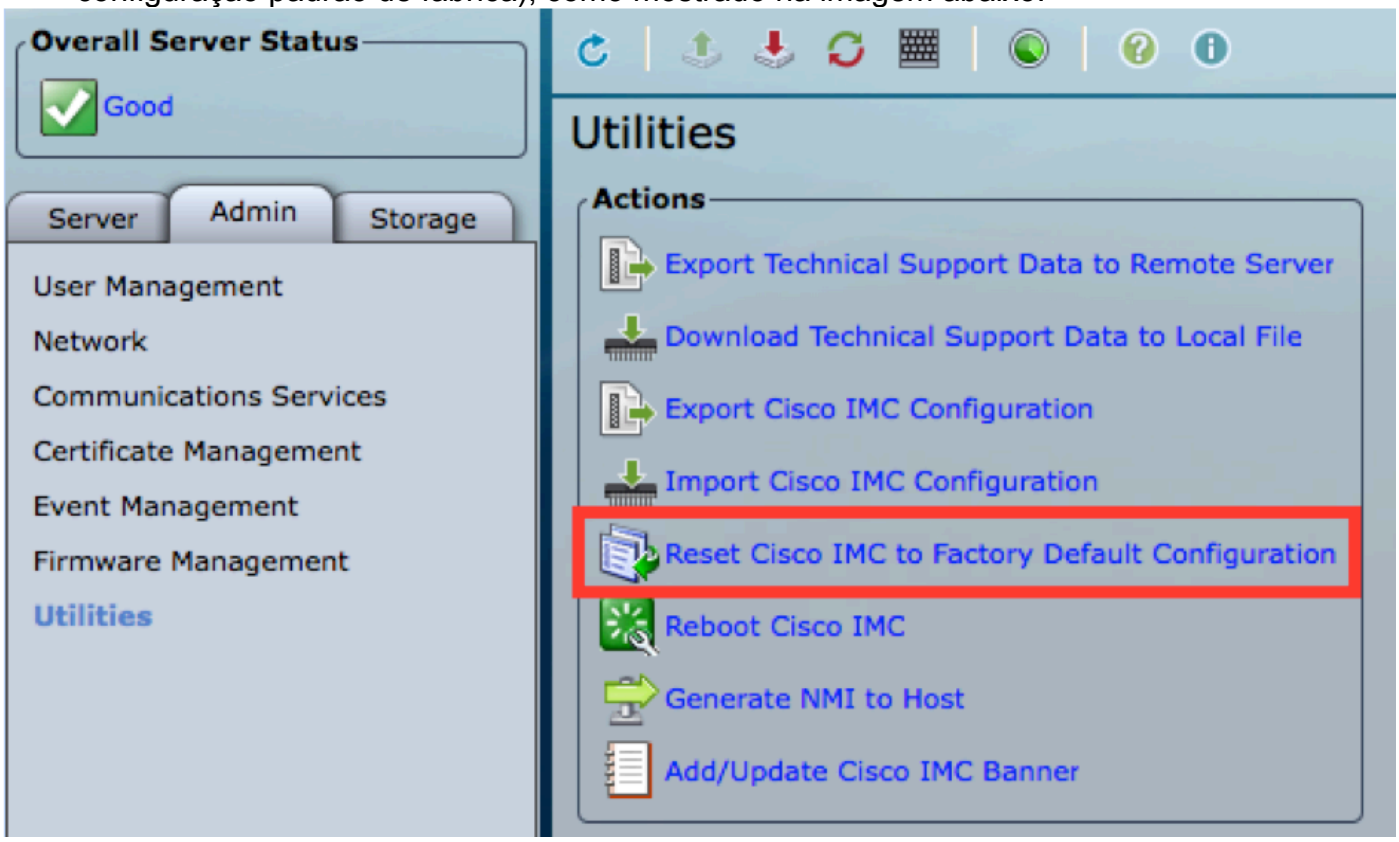
A área de trabalho abaixo permitirá que você aborde rapidamente esse evento SEL caso deseje remover as mensagens. O trabalho envolve redefinir o Integrated Management Controller (IMC) para as configurações padrão de fábrica, limpando qualquer valor de presença de TPM em cache.

Opções de solução alternativa:

Trabalhe em torno de 1 - Redefina o IMC para as configurações padrão de fábrica

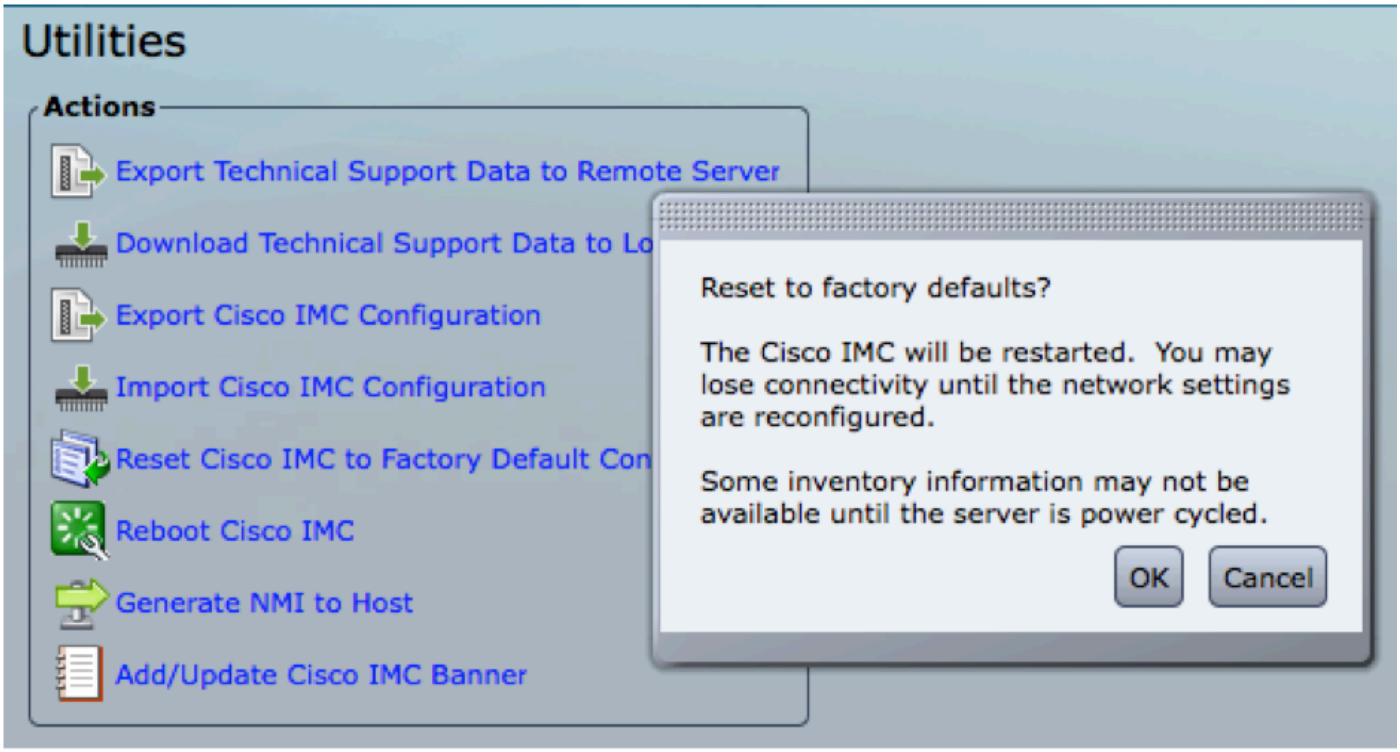
Restante para padrões de fábrica via IMC WebUI

1. Aponte um navegador para o IP IMC, faça login e navegue até a guia Admin —> Utilities (Utilitários)
2. Clique em "Reset Cisco IMC to Fatory Default Configuration" (Redefinir o Cisco IMC para a configuração padrão de fábrica), como mostrado na imagem abaixo.



3. Você receberá uma caixa pop-up. Clique em OK para continuar.

Note: *O IMC será redefinido completamente e você precisará redefinir todas as configurações. Registre todas as informações antes da redefinição.*



Trabalhe em torno de 2 - Redefinição dos padrões de fábrica via IMC CLI

1. SSH para o IP IMC usando as credenciais do usuário.
2. Digite os seguintes comandos conforme mostrado abaixo:
   a. scope cimc

   b. padrão de fábrica

```
C240-FCH1825V2M3# scope cimc
C240-FCH1825V2M3 /cimc # factory-default
This operation will reset the Cisco IMC configuration to factory default.
All your configuration will be lost. Some inventory information may
not be available until the server is powered on or power cycled.
Continue?[y|N]
```

3. Digite "y" para continuar.

Note: *O IMC será redefinido completamente e você precisará redefinir todas as configurações.*

Registre todas as informações antes da redefinição.