

Contenu

[Introduction](#)

[Problème](#)

[Systèmes potentiellement affectés :](#)

[Visibilité/incidence de client :](#)

[Solution](#)

[Travail autour des options :](#)

[Travail autour de 1 - Remettez à l'état initial l'IMC aux paramètres d'usine](#)

[Travail autour de 2 - Remise à l'état initial à Factory Defaults par l'intermédiaire IMC du CLI](#)

Introduction

L'intention de ce document est d'aborder la question vue concernant des événements relatifs de confiance des journaux d'événements de système du module de plate-forme (TPM) (SEL) sur des serveurs certain C460 M4. Un nombre restreint de serveurs de PIÈCE DE RECHANGE C460 M4 verront un événement essentiel SEL lié au juste de présence TPM hors de l'usine. Les instructions ci-dessous vous aideront à résoudre des serveurs affectés par cette question.

Problème

Systèmes potentiellement affectés :

Environ 614 systèmes SUPPLÉMENTAIRES C460 M4 (expédiés entre le 2 juin 2014, et le 13 avril 2016.)

Visibilité/incidence de client :

Les clients peuvent voir un événement essentiel SEL semblable à celui ci-dessous sur des serveurs reçus de l'usine.



The screenshot shows an 'Event Log' window with a table of log entries. The table has three columns: 'Time (UTC)', 'Severity', and a description of the event. The entry shown is dated 2016-04-13 11:16:17, has a 'Critical' severity, and the message is 'TPM_FAULT_STATUS: Add-in Card sensor, Predictive Failure asserted'.

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

Il n'y a AUCUNE incidence opérationnelle au serveur, mais le message peut mener au souci unecessary ayant pour résultat un appel au TAC. Ceci doit faire avec la manière que le TPM handed à la fabrication. Les systèmes C460 M4 gardent une valeur « cachée » pour la présence TPM, indiquant si un TPM était était jamais installé dans le serveur - chaque serveur a un TPM installé pendant le test. Le C460 M4 dépiste également le precense en cours du TPM, et puisque tous les serveurs commandés en tant que pièces de rechange se transportent sans TPM, le système déclenche une alarme pensant que le module qui a été par le passé installé a été retiré.

Solution

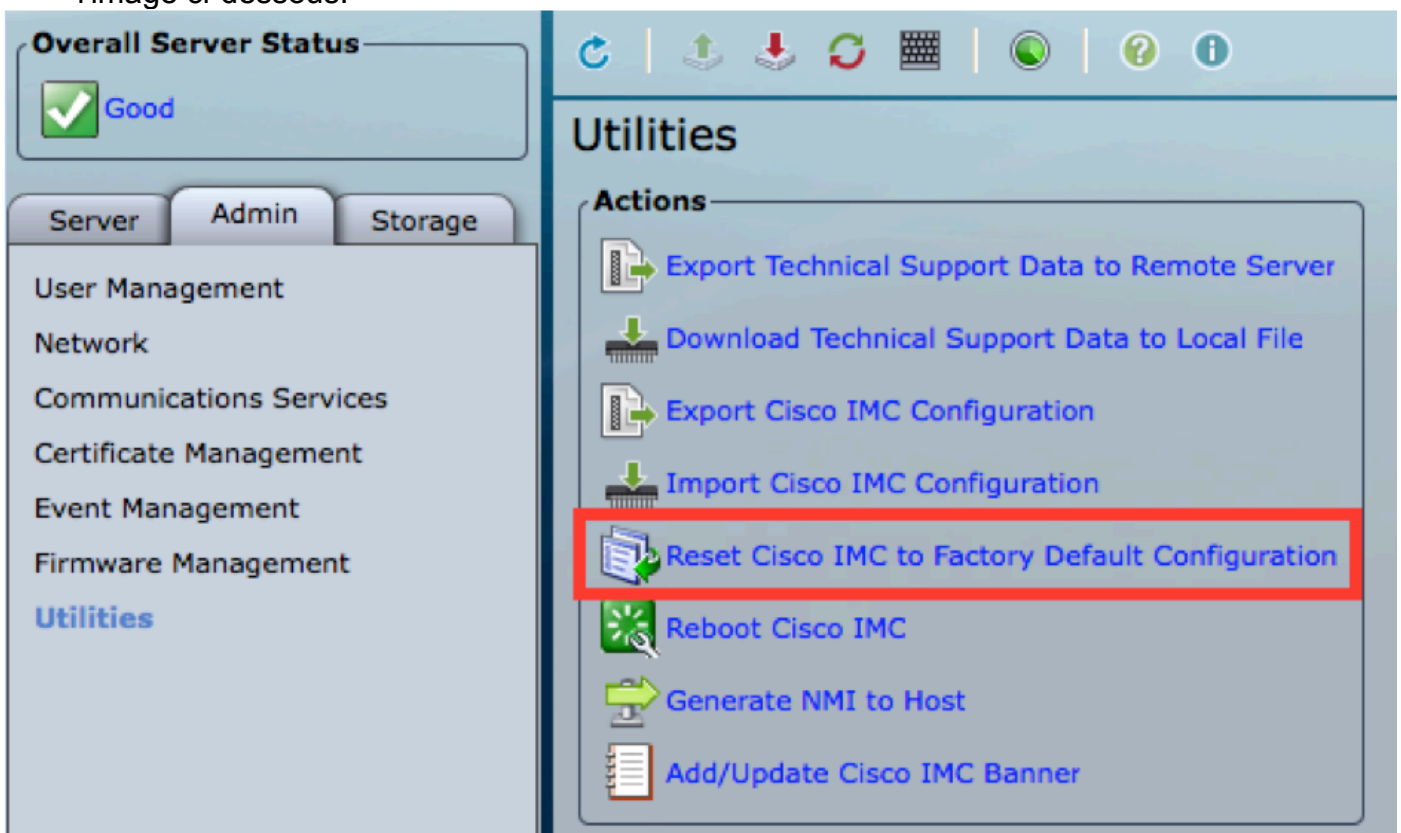
Le travail-around ci-dessous te permettra pour adresser rapidement cet événement SEL si vous souhaitez retirer les messages. Le travail-around implique de remettre à l'état initial le Contrôleur de gestion intégré (IMC) aux paramètres d'usine, effaçant n'importe quelle valeur cachée de présence TPM.

Travail autour des options :

Travail autour de 1 - Remettez à l'état initial l'IMC aux paramètres d'usine

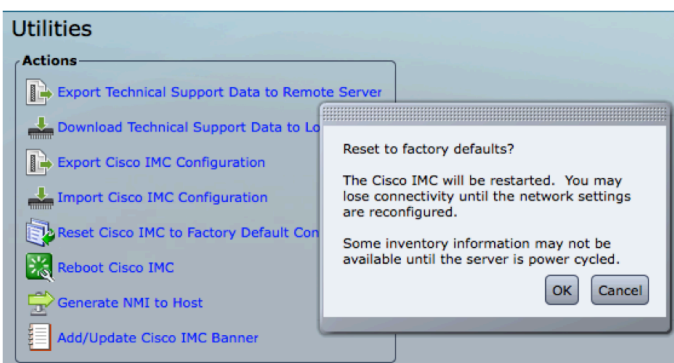
Repos à Factory Defaults par l'intermédiaire IMC de WebUI

1. Indiquez un navigateur l'IP IMC, procédure de connexion, et naviguez vers l'admin --> onglet d'utilitaires
2. Cliquez sur la « remise Cisco IMC à la configuration d'usine » suivant les indications de l'image ci-dessous.



3. Vous serez incité avec une case d'afficher. Cliquez sur OK pour poursuivre.

Remarque: L'IMC remettra à l'état initial complètement et vous devrez modifier toutes les configurations. Veuillez enregistrer n'importe quelles informations avant la remise.



Travail autour de 2 - Remise à l'état initial à Factory Defaults par l'intermédiaire IMC du CLI

1. SSH à l'IP IMC utilisant les qualifications de l'utilisateur.
2. Introduisez les commandes suivantes comme affiché ci-dessous :
 - a. portée cimc
 - b. usine-par défaut

```
[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. Écrivez « y » pour continuer.

Remarque: L'IMC remettra à l'état initial complètement et vous devrez modifier toutes les configurations.

Veillez enregistrer n'importe quelles informations avant la remise.