

Micrologiciel FPGA de point de terminaison sécurisé sur interconnexions de fabric UCS 6400

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Session SSH](#)

[Interface utilisateur Web d'UCS Manager](#)

Introduction

Ce document décrit comment activer la FPGA (Field-Programmable Gate Array) sécurisée sur les interconnexions de fabric 6400.

Problème

Dans les mises à niveau d'Unified Computing System Manager (UCS Manager) vers la version 4.1(3) ou ultérieure sur les IF 6400 (4e génération), les clients voient cette erreur majeure :



The screenshot shows the UCS Manager interface with a fault message. The top navigation bar includes the UCS logo, fault code F2023, ID 1494523, affected object sys/switch-A/fw-secure-fpga, cause unsecured-fpga, timestamp 2021-04-08T04:00:46Z, and the fault description Endpoint FPGA firmware Unse... Below the navigation bar, the 'Details' section is visible, divided into 'Summary' and 'Properties'.

Summary		Properties	
Severity	: Major/Pinned	Affected object	: sys/switch-A/fw-secure-fpga
Last Transition	: 2021-04-08T04:00:46Z	Description	: Endpoint FPGA firmware Unsecured.
Actions		ID	: 1494523
Acknowledge Fault		Cause	: unsecured-fpga
		Type	: management
		Created at	: 2021-04-08T04:00:46Z
		Code	: F2023
		Number of Occurrences	: 1
		Original severity	: Major
		Previous severity	: Major
		Highest severity	: Major

Description: Endpoint FPGA firmware Unsecured.

Fault Code: F2023

Il s'agit d'une nouvelle fonctionnalité en réponse à une vulnérabilité de démarrage sécurisée connue où des régions dorées de la FPGA pourraient avoir du code injecté ou modifié, ce qui en fait annule le démarrage sécurisé.

Solution

Ce message est attendu lorsque vous effectuez une mise à niveau vers la version 4.1(3) ou ultérieure sur les FI de la gamme 6400. Il peut se produire uniquement sur une ou les deux FI, et dépend du code avec lequel elles ont été livrées à l'origine.

Il n'y a pas de risque pour la production autre que la réduction de la sécurité. Cette opération peut

être retardée jusqu'à la prochaine fenêtre de maintenance planifiée.

La FPGA peut être sécurisée et l'erreur effacée par ces étapes via une session SSH ou dans l'interface utilisateur graphique d'UCS Manager.

Note: Cela nécessitera un redémarrage de chaque FI. Il est recommandé de le faire dans une fenêtre de service.

Session SSH

1. Ouvrez une session SSH sur le domaine. L'adresse IP du cluster ou l'adresse IP de l'IF fonctionne.

```
UCS-A# scope fabric-interconnect a  
UCS-A /fabric-interconnect# activate secure-fpga  
UCS-A/fabric-interconnect*# commit-buffer
```

Note: L'IF redémarre après un court délai. Ne redémarrez pas manuellement l'IF !

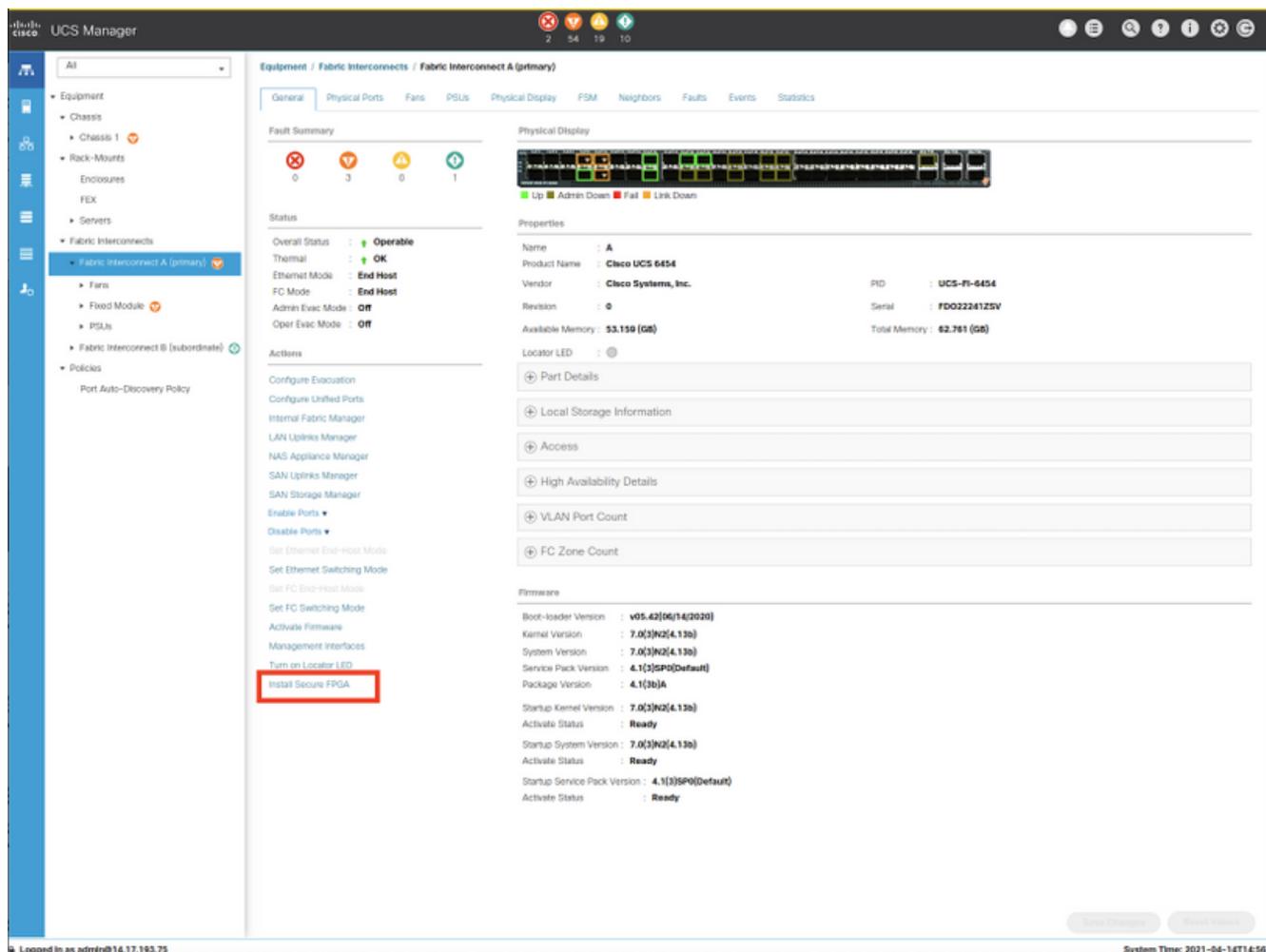
2. Répétez ce processus sur l'IF B.

```
UCS-B# top  
UCS-B# scope fabric-interconnect b  
UCS-B /fabric-interconnect# activate secure-fpga  
UCS-B/fabric-interconnect*# commit-buffer
```

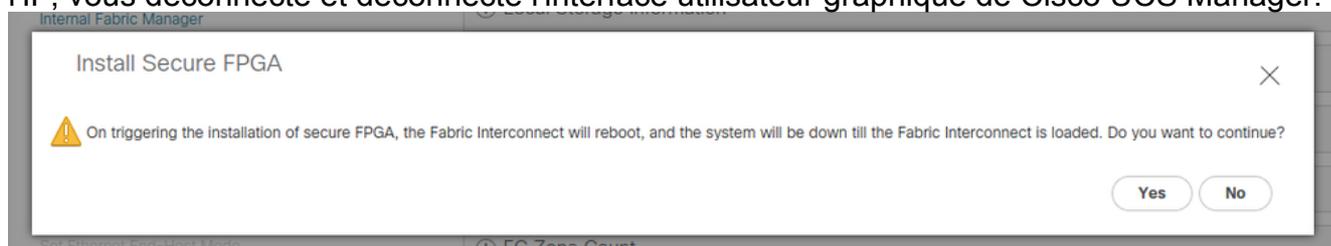
Note: L'IF redémarre après un court délai. Ne redémarrez pas manuellement l'IF ! L'erreur non sécurisée du microprogramme FPGA du point de terminaison doit maintenant être à l'état effacé.

Interface utilisateur Web d'UCS Manager

1. Dans le volet de navigation, sélectionnez **Équipement > Interconnexions de fabric > Fabric_Interconnect_Name**.
2. Dans le volet Travail, cliquez sur l'onglet **Général**.
3. Dans la zone Actions de l'onglet Général, cliquez sur **Installer Secure FPGA**.



4. Dans la boîte de dialogue, cliquez sur **OK**.
5. Cliquez sur **Oui** dans le message d'avertissement pour que Cisco UCS Manager redémarre l'IF, vous déconnecte et déconnecte l'interface utilisateur graphique de Cisco UCS Manager.



Note: L'IF redémarre après un court délai. Ne redémarrez pas manuellement l'IF ! Si vous ne voyez pas l'option Installer Secure FPGA, videz le cache de votre navigateur ou utilisez une session de navigation privée.

Pour plus d'informations sur la mise à niveau de Secure FPGA, reportez-vous aux [Notes de version de Cisco UCS Manager, version 4.1](#).