

# Le serveur lame B460 M4 échoue à la découverte après un remplacement de carte mère

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Fond](#)

[Problèmes de détection](#)

[Échec de la détection à 3 % - Incompatibilité du micrologiciel](#)

[Solution](#)

[Échec de la détection à 5 % - incompatibilité du micrologiciel du contrôleur de carte](#)

[Solution](#)

[Échec de la découverte à 7 % - Incompatibilité du processeur](#)

[Solution](#)

## Introduction

Ce document décrit deux échecs de détection possibles qui peuvent se produire lors du remplacement d'une carte mère B460 M4 et de leurs solutions respectives.

## Conditions préalables

### Conditions requises

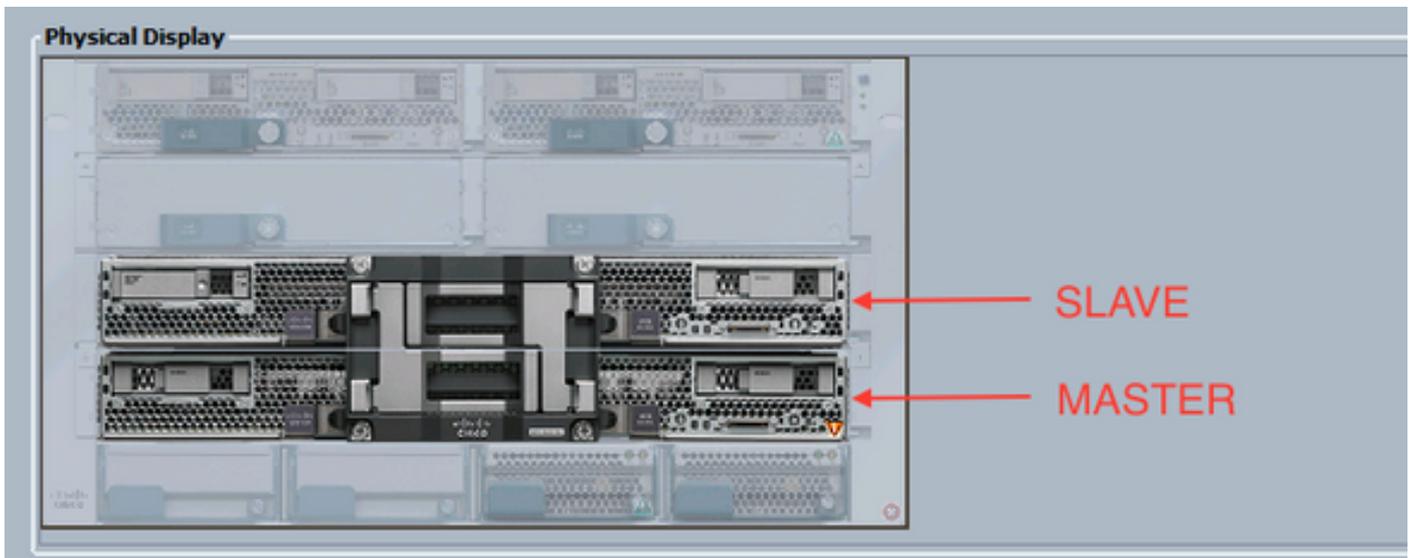
Ce document suppose des connaissances sur UCS B460 M4 et UCS Manager (UCSM).

### Components Used

- Serveur lame B460 M4
- UCS Manager
- Microprogramme 2.2(3b)

## Fond

Le serveur B460 M4 se compose de deux modules lame M4 évolutifs (B260 M4) et d'un connecteur évolutif qui relie les deux modules lames et leur permet de fonctionner comme un seul serveur. Le module lame situé en bas est le " maître " et le module lame situé en haut est l'esclave " . "

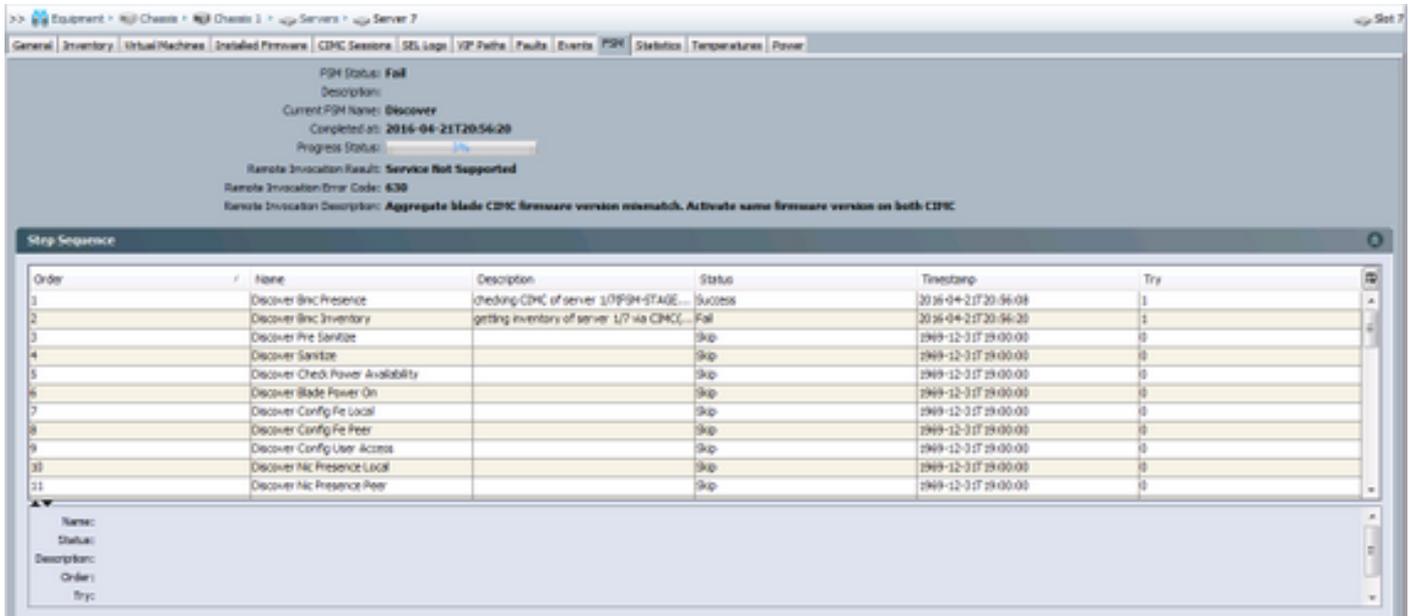


## Problèmes de détection

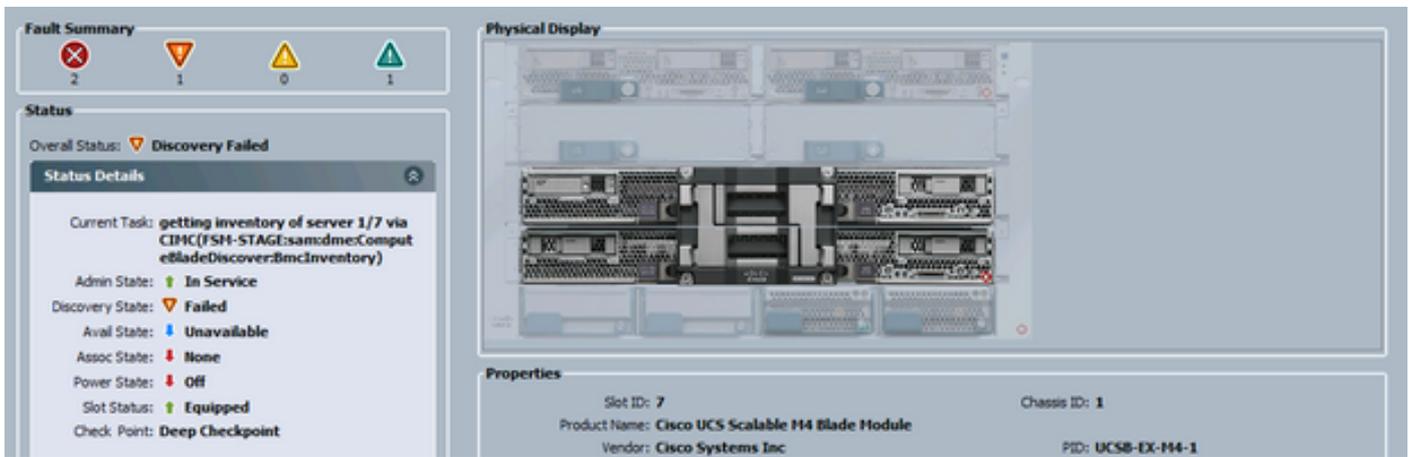
### Échec de la détection à 3 % - Incompatibilité du micrologiciel

Dans ce scénario d'échec, la découverte échoue à 3 % avec une **incompatibilité de version du microprogramme CIMC Remote Invocation Description Aggregate Blade**. **Activez la même version de microprogramme sur les deux modules CIMC** comme indiqué dans la figure ci-dessous. Cela peut se produire en raison du fait que la carte mère de remplacement ou le module lame possède un microprogramme différent de celui du serveur B460 M4 préexistant.

**Note:** L'exemple ci-dessous montre une non-correspondance dans le micrologiciel CIMC, mais le même processus s'applique aux micrologiciels CIMC, BIOS et contrôleur de carte qui ne correspondent pas.



L'état général sera **Échec de la découverte** comme indiqué dans la figure ci-dessous.



Vous pouvez vérifier le micrologiciel inadapté à partir de la ligne de commande (CLI), comme indiqué ci-dessous. Dans le résultat ci-dessous, le premier CIMC est le maître et le second est l'esclave.

```
UCS-A# show system firmware expand detail
```

```
Server 7:
```

```
  CIMC:
```

```
    Running-Vers: 2.2(3b)
    Package-Vers:
    Update-Status: Ready
    Activate-Status:
    Startup-Vers:
    Backup-Vers: 2.2(3a)
    Bootloader-Vers: 2.2(3b).33
```

```
  CIMC:
```

```
    Running-Vers: 2.2(3a)
    Package-Vers:
    Update-Status: Ready
    Activate-Status:
    Startup-Vers:
    Backup-Vers: 2.2(3b)
    Bootloader-Vers: 2.2(3a).33
```

```
  CIMC:
```

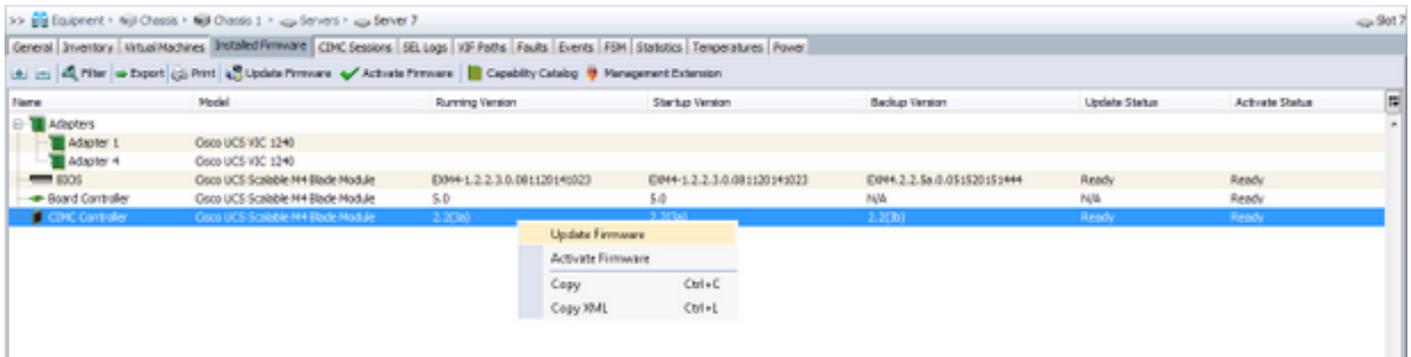
```
    Running-Vers: 2.2(3b)
    Package-Vers: 2.2(3b)B
    Update-Status: Ready
    Activate-Status: Ready
    Startup-Vers: 2.2(3b)
    Backup-Vers: 2.2(3b)
    Bootloader-Vers: 2.2(3b).33
```

## Solution

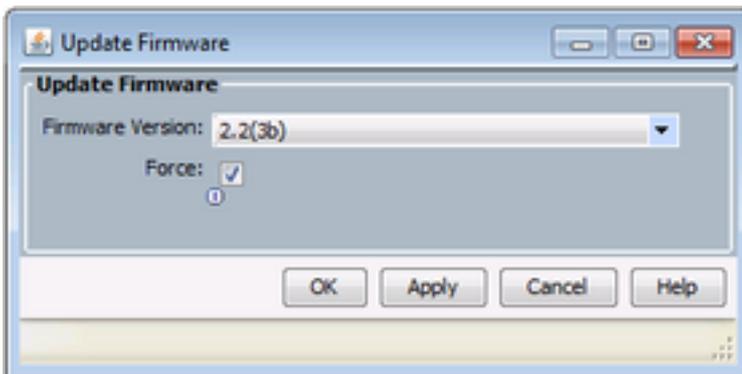
Afin de récupérer de ceci, suivez les étapes ci-dessous.

1) Accédez à Équipement > Châssis > Châssis # > **Serveurs** > **Serveur #** > **Microprogramme installé.**

2) Cliquez avec le bouton droit sur le composant qui doit être mis à jour (par exemple BIOS, contrôleur CIMC) et sélectionnez **Mettre à jour le micrologiciel.** Dans cet exemple, le contrôleur CIMC sera mis à jour en 2.2(3b).



3) Sélectionnez le micrologiciel correct, la case **Forcer** et cliquez sur **Appliquer**.



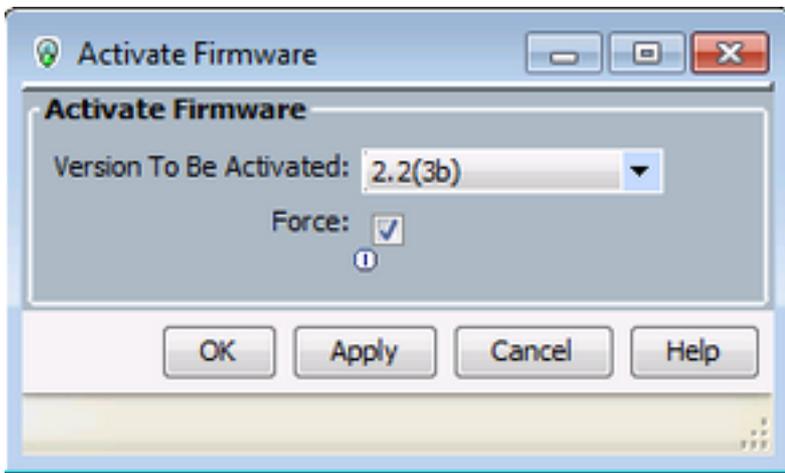
**Astuce** : S'il n'est pas clair quelle version doit être sélectionnée dans la liste déroulante, l'administrateur du serveur peut accéder à **Equipment > Firmware Management > Packages**, développer ucs-k9-bundle-b-series. *VERSION*.B.bin et rechercher « ucs-EXM4 ». Il y aura trois composants : bios (BIOS), brdprog (contrôleur de carte) et cimc (contrôleur CIMC).

**Astuce** : Étant donné que le microprogramme du contrôleur de carte ne peut pas être rétrogradé, si la carte mère de remplacement est fournie avec une version du microprogramme du contrôleur de carte qui n'est présente dans aucun des packages de la gamme de lames présents dans le domaine, l'administrateur réseau peut télécharger un package de la gamme de lames qui contient la version du microprogramme du contrôleur de carte nécessaire. Afin de vérifier quel package de série de lames contient le micrologiciel nécessaire, consultez le document *Contenu de l'offre groupée de version pour Cisco UCS Manager*.

4) Surveillez l'onglet Firmware installé et attendez que les colonnes **Update Status** et **Activate Status** passent à **Ready** et que la colonne **Backup Version** change pour le micrologiciel correct.

**Conseil** : l'administrateur du serveur peut surveiller l'état de la mise à jour à partir de **Equipment > Chassis > Chassis # > Servers > Server # > Inventory tab > CIMC tab > Update Status**

5) Cliquez avec le bouton droit de la souris sur ce même composant et sélectionnez **Activer le micrologiciel**. Sélectionnez à nouveau le micrologiciel correct, la case **Forcer** et cliquez sur **Appliquer**.



6) La colonne *Activate Status* de l'onglet **Installed Firmware** changera d'état et finira par revenir à *Ready*.

7) L'état *général* de l'onglet **Général** passe à *Inaccessible* pendant le redémarrage du serveur. Il doit ensuite passer à *Discovery* et passer par le processus de découverte.

#### Échec de la détection à 5 % - incompatibilité du micrologiciel du contrôleur de carte

**Avis :** Dans ce scénario d'échec, la découverte échoue à 5 % avec une **incompatibilité de version du microprogramme du contrôleur de carte lame *Remote Invocation DescriptionAggregate***. **Activez la même version du micrologiciel sur les deux contrôleurs de carte**, comme le montre la figure ci-dessous. Cela peut se produire en raison du fait que la carte mère de remplacement ou le module lame possède un microprogramme différent de celui du serveur B460 M4 préexistant.



Vous pouvez vérifier le micrologiciel inadapté à partir de la ligne de commande (CLI), comme indiqué ci-dessous. Dans le résultat ci-dessous, le premier contrôleur de carte est le maître et le second est l'esclave.

```
srini-2gfi-96-b-A /chassis/server # show firmware board controller detail
Server 2/7:
  Board Controller:
    Running-Vers: 2.0    <<<<
    Package-Vers: 2.2(7.156)B
    Activate-Status: Ready
  Board Controller: ( Master)
    Running-Vers: 2.0    <<<<
    Package-Vers:
    Activate-Status:
  Board Controller: ( Slave)
    Running-Vers: 1.0    <<<<
    Package-Vers:
    Activate-Status:
```

#### Solution

Pour récupérer, procédez comme suit :

- Étape 1 Dans le volet de navigation, cliquez sur l'onglet Équipement.
- Étape 2 Dans l'onglet Équipement, cliquez sur le noeud Équipement.
- Étape 3 Dans le volet de travail, cliquez sur l'onglet Firmware Management.  
Dans l'onglet Installed Firmware, cliquez sur Activate Firmware.  
L'interface utilisateur de Cisco UCS Manager ouvre la boîte de dialogue Activer le micrologiciel et vérifie les versions du micrologiciel pour tous les terminaux du domaine Cisco UCS.  
Cette étape peut prendre quelques minutes, selon le nombre de châssis et de serveurs
- Étape 4 Dans la liste déroulante Filtre de la barre de menus de la boîte de dialogue Activer le micrologiciel, sélectionnez Contrôleur de carte.  
L'interface utilisateur graphique de Cisco UCS Manager affiche tous les serveurs disposant de contrôleurs de carte dans la boîte de dialogue Activer le micrologiciel.
- Étape 5 Pour le contrôleur de carte, vous voulez mettre à jour, sélectionnez la version maximale/la plus grande dans la liste déroulante Version de démarrage. (Remarque: les déclassements ne sont pas possibles ; toujours sélectionner la version la plus élevée à activer)
- Étape 6 Click OK.  
(Facultatif)Vous pouvez également utiliser l'option Forcer l'activation du contrôleur de carte mère pour mettre à jour la version du micrologiciel lorsque vous mettez à niveau des processeurs avec différentes architectures. Par exemple, lorsque vous effectuez une mise à niveau de Sandy Bridge vers des processeurs Ivy Bridge.
- Étape 7
- Étape 8

#### **Échec de la découverte à 7 % - Incompatibilité du processeur**

Dans ce scénario d'échec, la détection échoue à 7 % avec *Remote Invocation Description Pre-boot Hardware config fail* - Examinez les résultats de **POST/diagnostic** comme indiqué dans la figure ci-dessous.

>> Equipment > Chassis > Chassis 1 > Servers > Server 7 Slot 7

General Inventory Virtual Machines Installed Firmware CIMC Sessions SEL Logs VIF Paths Faults Events FSM Statistics Temperatures Power

FSM Status: **Fail**  
 Description:  
 Current FSM Name: **Discover**  
 Completed at: **2016-04-22T02:03:29**  
 Progress Status: **7%**  
 Remote Invocation Result: **Intermittent Error**  
 Remote Invocation Error Code: **ERR-insufficiently-equipped**  
 Remote Invocation Description: **Pre-boot Hardware config failure - Look at POST/diagnostic results**

**Step Sequence**

Order	Name	Description	Status	Timestamp
1	Discover Bmc Presence	checking CIMC of server 1/7(FSM-STAGE:sam:dme:ComputeBladeDiscover:BmcPresence)	Success	2016-04-22T02:03:07
2	Discover Bmc Inventory	getting inventory of server 1/7 via CIMC(FSM-STAGE:sam:dme:ComputeBladeDiscover:BmcInventory)	Success	2016-04-22T02:03:26
3	Discover Pre Sanitize	Preparing to check hardware configuration server 1/7(FSM-STAGE:sam:dme:ComputeBladeDiscover:PreSan...	Success	2016-04-22T02:03:29
4	Discover Sanitize	Checking hardware configuration server 1/7(FSM-STAGE:sam:dme:ComputeBladeDiscover:Sanitize)	Fail	2016-04-22T02:03:29
5	Discover Check Power Availability		Skip	1969-12-31T19:00:00
6	Discover Blade Power On		Skip	1969-12-31T19:00:00
7	Discover Config Fe Local		Skip	1969-12-31T19:00:00
8	Discover Config Fe Peer		Skip	1969-12-31T19:00:00
9	Discover Config User Access		Skip	1969-12-31T19:00:00
10	Discover Nic Presence Local		Skip	1969-12-31T19:00:00

Name:  
 Status:  
 Description:  
 Order:  
 Try:  
 Timestamp:

Save Changes Reset Values

L'état général de l'onglet Général sera Échec du calcul.

>> Equipment > Chassis > Chassis 1 > Servers > Server 7 Slot 7

General Inventory Virtual Machines Installed Firmware CIMC Sessions SEL Logs VIF Paths Faults Events FSM Statistics Temperatures Power

**Fault Summary**  
 3 Critical, 3 Warning, 0 Error, 1 Info

**Status**  
 Overall Status: **Compute Failed**

**Status Details**

Current Task: **Checking hardware configuration server 1/7(FSM-STAGE:sam:dme:ComputeBladeDiscover:Sanitize)**

Configuration Error: **compute-post-failure**

Admin State: **In Service**  
 Discovery State: **Failed**  
 Avail State: **Unavailable**  
 Assoc State: **None**  
 Power State: **Off**  
 Slot Status: **Equipped**  
 Check Point: **Deep Checkpoint**

**Actions**

- Create Service Profile
- Associate Service Profile
- Get Desired Power State
- Boot Server

**Physical Display**

**Properties**

Slot ID: 7 Chassis ID: 1  
 Product Name: **Cisco UCS Scalable M4 Blade Module**  
 Vendor: **Cisco Systems Inc** PID: **UCSB-EX-M4-1**  
 Revision: 0 Serial:  
 Name:  
 User Label:  
 UUID: 00000000-0000-0000-0000-000000000000  
 Service Profile:  
 Health LED: **Critical** Oper Qualifier Reason: **WILL\_BOOT\_FAULT:Sensor Failure Asserted**

**Health and Locator LED Details**

Save Changes Reset Values

Vous pouvez vérifier les résultats du POST en cliquant sur **Afficher les résultats du post** sous **Actions** dans l'onglet **Général**. La figure ci-dessous montre que le problème est dû à une non-correspondance du processeur.

POST Results

Filter Export Print

Affected object	ID	Type	Code	Created at	Severity	Description
sys/chassis-1/blade-7	4860	server: Cisco Systems Inc UCSB-EX-M4-1	POST-4860	2016-04-22T01:55:07	Critical	CPU Mismatch

**Details**

General

ID: 4860 Local ID: 259  
Type: server: Cisco Systems Inc UCSB-EX-M4-1 Code: POST-4860  
Created: 2016-04-22T01:55:07 Severity: Critical  
Recoverable: Non Recoverable Recoverable Action: Install matching CPU  
Description: CPU Mismatch

OK Apply Cancel Help

### Solution

Si le matériel correspond entre les deux modules lames, cela peut être dû aux informations mises en cache sur le serveur. Une demande d'amélioration ([CSCuv27099](https://support.cisco.com/servlet/JSP?url=//_jsp/docs/getDoc.do?name=tc&tid=CSCuv27099)) existe pour effacer les informations mises en cache d'UCS Manager (UCSM). L'administrateur du serveur peut également contacter le centre d'assistance technique Cisco (TAC) pour obtenir une solution de contournement.