

# El servidor blade B460 M4 falla en la detección después de la sustitución de una placa base

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Problemas de detección](#)

[La detección falla al 3% - Discordancia del firmware](#)

[Solución](#)

[La detección falla al 5% - Discordancia del firmware del controlador de la placa](#)

[Solución](#)

[La detección falla al 7% - Discordancia de la CPU](#)

[Solución](#)

## Introducción

Este documento describe dos posibles fallas de detección que pueden ocurrir cuando se reemplaza una placa base B460 M4 y sus respectivas soluciones.

## Prerequisites

## Requirements

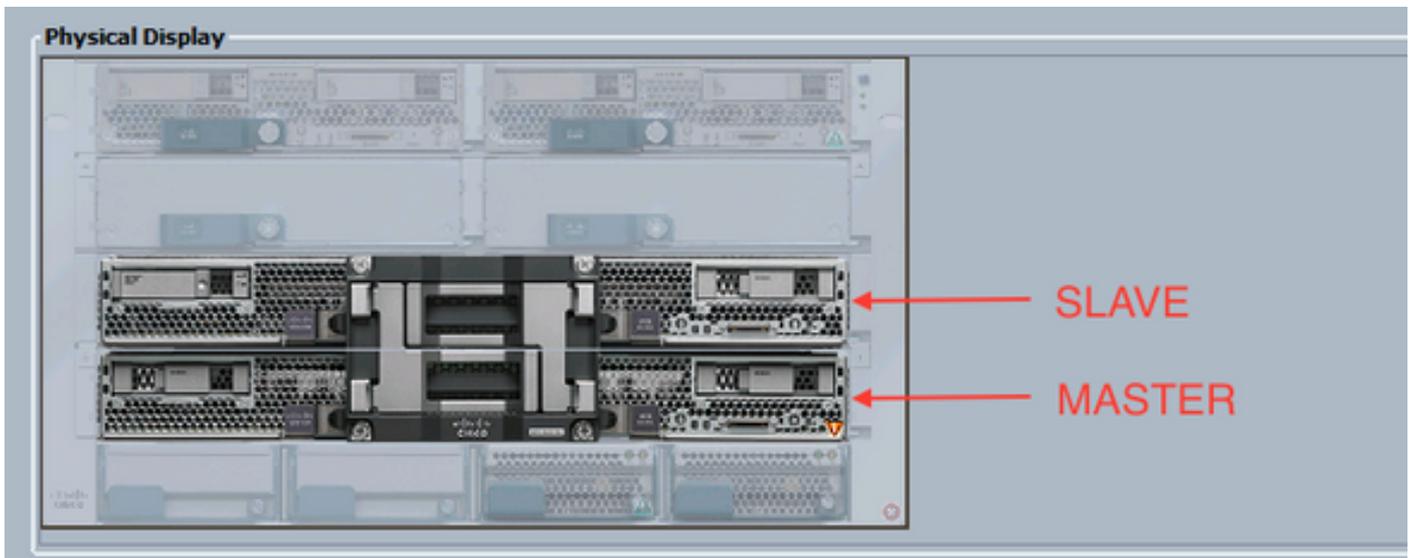
Este documento asume el conocimiento de UCS B460 M4 y UCS Manager (UCSM).

## Componentes Utilizados

- Servidor blade B460 M4
- UCS Manager
- Firmware 2.2(3b)

## Background

El servidor B460 M4 consta de dos módulos de servidor blade M4 escalables (B260 M4) y un conector de escalabilidad que conecta los dos módulos de servidor blade y les permite funcionar como un único servidor. El módulo blade de la parte inferior es el "maestro" y el módulo blade de la parte superior es el "esclavo".



## Problemas de detección

### La detección falla al 3% - Discordancia del firmware

En este escenario de falla, la detección falla en un 3% con la **discordancia de la versión del firmware Remote Invocation Description Aggregate blade CIMC. Active la misma versión de firmware en ambos CIMC** como se muestra en la siguiente figura. Esto puede ocurrir debido a que la placa base o el módulo blade de reemplazo tienen un firmware diferente al del servidor B460 M4 anterior.

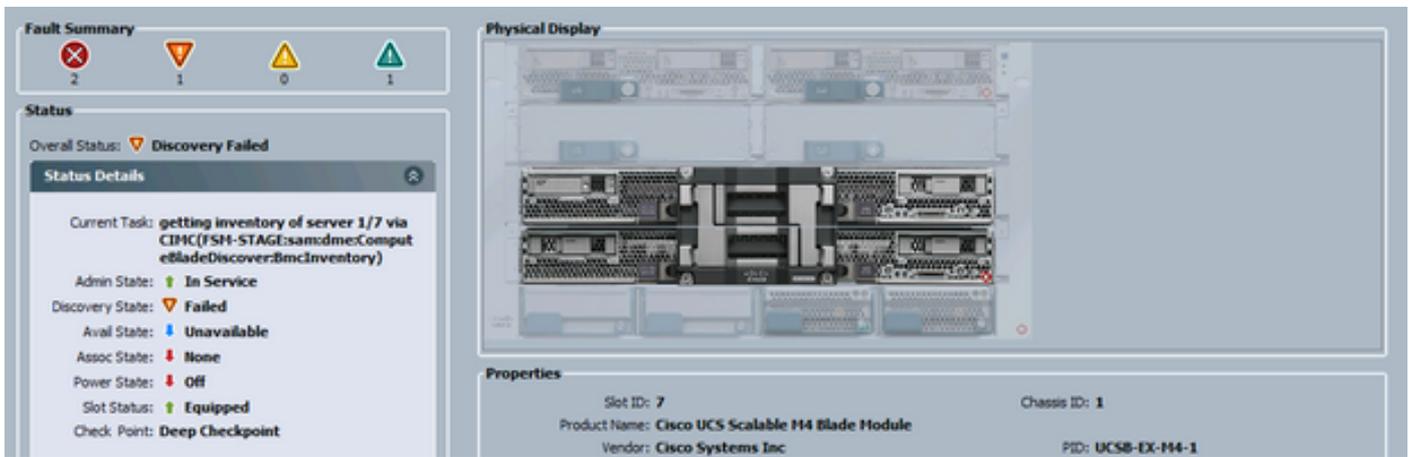
**Nota:** El siguiente ejemplo muestra una discordancia en el firmware CIMC, pero el mismo proceso se aplica a firmware CIMC, BIOS y controlador de placa no coincidentes.

The screenshot shows a management console interface. At the top, it displays 'PSM Status: Fail' and 'Description: Discover'. Below this, it shows 'Current PSM Name: Discover', 'Completed at: 2016-04-21T20:56:20', and 'Progress Status: 1%'. A red bar indicates the progress. Below the progress bar, it says 'Remote Invocation Result: Service Not Supported' and 'Remote Invocation Error Code: 630'. The error description is 'Aggregate blade CIMC firmware version mismatch. Activate same firmware version on both CIMC'.

Below the error message is a 'Stop Sequence' table with the following data:

Order	Name	Description	Status	Timestamp	Try
1	Discover Bmc Presence	checking CIMC of server 1/7 via STAGE...	Success	2016-04-21T20:56:00	1
2	Discover Bmc Inventory	getting inventory of server 1/7 via CIMC...	Fail	2016-04-21T20:56:20	1
3	Discover Pre Initialize		Skip	2016-12-31T19:00:00	0
4	Discover Sanitize		Skip	2016-12-31T19:00:00	0
5	Discover Check Power Availability		Skip	2016-12-31T19:00:00	0
6	Discover Blade Power On		Skip	2016-12-31T19:00:00	0
7	Discover Config Fe Local		Skip	2016-12-31T19:00:00	0
8	Discover Config Fe Peer		Skip	2016-12-31T19:00:00	0
9	Discover Config User Access		Skip	2016-12-31T19:00:00	0
10	Discover Mc Presence Local		Skip	2016-12-31T19:00:00	0
11	Discover Mc Presence Peer		Skip	2016-12-31T19:00:00	0

El estado general será **Discovery Failed** como se muestra en la siguiente figura.



El firmware no coincidente se puede comprobar desde la línea de comandos (CLI), como se muestra a continuación. En el resultado siguiente, el primer CIMC es el maestro y el segundo es el esclavo.

```
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:
```

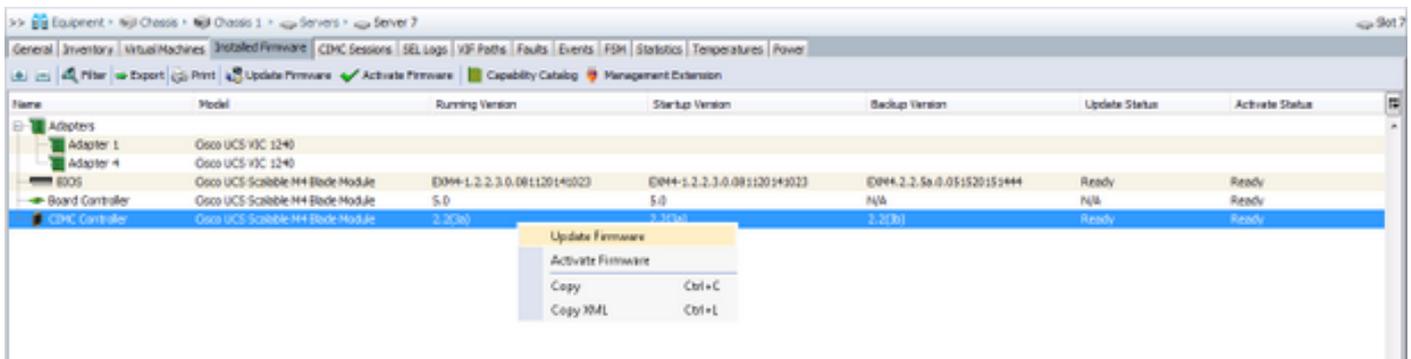
```
Running-Vers: 2.2(3b)
Package-Vers: 2.2(3b)B
Update-Status: Ready
Activate-Status: Ready
Startup-Vers: 2.2(3b)
Backup-Vers: 2.2(3b)
Bootloader-Vers: 2.2(3b).33
```

## Solución

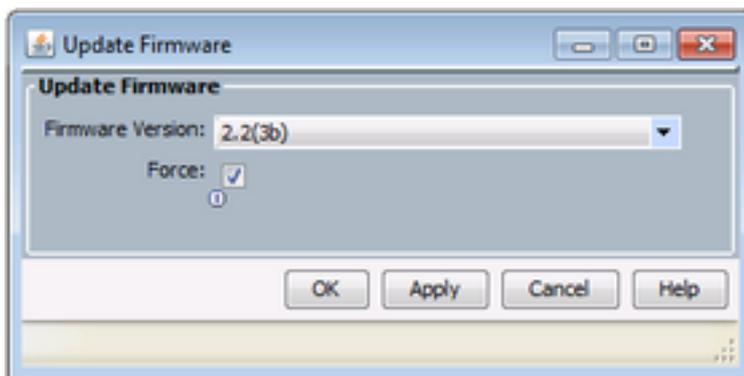
Para recuperarse de esto, siga estos pasos.

1) Vaya a Equipo > Chasis > Chasis # > **Servidores** > **Servidor #** > Firmware Instalado.

2) Haga clic con el botón derecho del ratón en el componente que debe actualizarse (por ejemplo, BIOS, controlador CIMC) y seleccione **Actualizar firmware**. En este ejemplo, el controlador CIMC se actualizará a 2.2(3b).



3) Seleccione el firmware correcto, la casilla **Force** y haga clic en **Apply**.



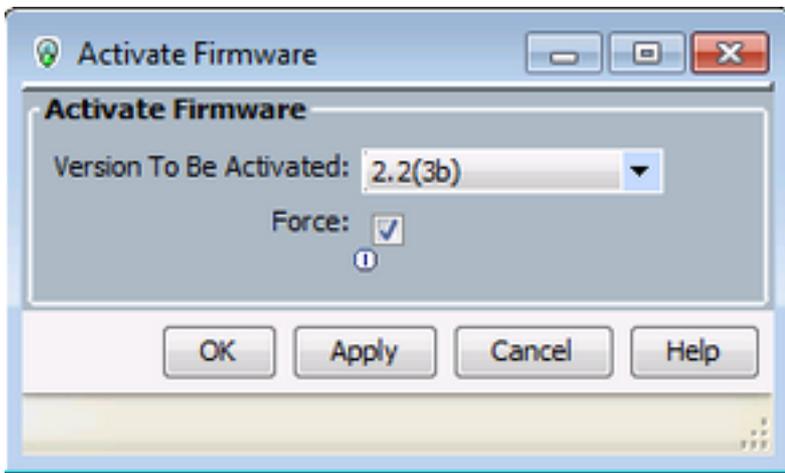
**Consejo:** Si no está claro qué versión debe seleccionarse del menú desplegable, el administrador del servidor puede navegar hasta **Equipo > Administración del firmware > Paquetes**, expandir ucs-k9-bundle-b-series.VERSIÓN .B.bin y buscar "ucs-EXM4". Habrá tres componentes: BIOS (BIOS), brdprog (controlador de la placa) y cimc (controlador CIMC).

**Consejo:** Dado que el firmware del controlador de la placa no se puede degradar, si la placa madre de reemplazo incluye una versión de firmware del controlador de la placa que no está presente en ninguno de los paquetes de la serie de servidores blade presentes en el dominio, el administrador de la red puede descargar un paquete de la serie de servidores blade que contiene el firmware de la versión del controlador de la placa necesario. Para verificar qué paquete de la serie de servidores blade contiene el firmware necesario, revise el *documento Contenido del paquete de lanzamiento para Cisco UCS Manager*.

4) Supervise la pestaña Firmware instalado y espere hasta que las columnas **Update Status** y **Activate Status** cambien a **Ready** y la columna Backup Version cambie al firmware correcto.

**Consejo:** El administrador del servidor puede supervisar el estado de actualización desde **Equipo > Chasis > Chasis # > Servidores > Servidor # > Ficha Inventario > Ficha CIMC > Estado de actualización**

5) Haga clic con el botón derecho del ratón en este mismo componente y seleccione **Activar firmware**. Una vez más, seleccione el firmware correcto, la casilla **Force** y haga clic en **Apply**.



6) La columna *Activar estado* de la ficha **Firmware instalado** cambiará de estado y, finalmente, volverá a *Preparado*.

7) El *estado general* de la ficha **General** cambiará a **Inaccesible** mientras el servidor se reinicia. Luego debería cambiar a *Discovery* y pasar por el proceso de descubrimiento.

#### La detección falla al 5% - Discordancia del firmware del controlador de la placa

**Aviso:** En este escenario de falla, la detección falla en un 5% con la **descripción *Remote Invocation Error de versión del firmware del controlador de placa blade agregado. Active la misma versión de firmware en ambos controladores de placa como se muestra en la siguiente figura.*** Esto puede ocurrir debido a que la placa base o el módulo blade de reemplazo tienen un firmware diferente al del servidor B460 M4 anterior.



El firmware no coincidente se puede comprobar desde la línea de comandos (CLI), como se muestra a continuación. En el resultado siguiente, el primer controlador de la Junta es el maestro y el segundo es el esclavo.

```
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:
```

#### Solución

Para recuperarse, siga estos pasos

- Paso 1 En el panel de navegación, haga clic en la ficha Equipo.
- Paso 2 En la ficha Equipo, haga clic en el nodo Equipo.
- Paso 3 En el panel Trabajo, haga clic en la ficha Administración del firmware.  
En la ficha Installed Firmware (Firmware instalado), haga clic en Activate Firmware (Activar firmware).
- Paso 4 La GUI de Cisco UCS Manager abre el cuadro de diálogo Activar firmware y verifica las versiones de firmware para todos los terminales del dominio Cisco UCS. Este paso puede tardar unos minutos, dependiendo del número de chasis y servidores  
En la lista desplegable Filtro de la barra de menús del cuadro de diálogo Activar firmware, seleccione Controlador de placa.
- Paso 5 La GUI de Cisco UCS Manager muestra todos los servidores que tienen controladores de placa en el cuadro de diálogo Activar firmware.  
Para el controlador de placa, desea actualizar, seleccione la versión máxima/más grande de la lista desplegable Versión de inicio. (Nota: las rebajas no son posibles; siempre seleccione la versión más alta que desea activar)
- Paso 6 Click OK.
- Paso 7 (Opcional) También puede utilizar la opción Force Board Controller Activation (Forzar activación del controlador de placa) para actualizar la versión del firmware cuando actualiza las CPU con arquitecturas diferentes. Por ejemplo, cuando se actualiza de Sandy Bridge a CPU Ivy Bridge.
- Paso 8

#### **La detección falla al 7% - Discordancia de la CPU**

En este escenario de falla, la detección falla en un 7% con la **falla de configuración del hardware** *Remote Invocation Description Pre-boot* - Observe los **resultados POST/diagnóstico** como se muestra en la siguiente figura.

>> Equipment > Chassis > Chassis 1 > Servers > Server 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

El estado general en la ficha **General** será **Compute Failed**.

>> Equipment > Chassis > Chassis 1 > Servers > Server 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

Los resultados POST se pueden verificar haciendo clic en **Ver resultados de publicación** en **Acciones** en la pestaña **General**. La siguiente figura muestra que el problema se debe a una discordancia de la CPU.

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

### Solución

Si el hardware coincide entre los dos módulos blade, esto podría deberse a la información almacenada en caché en el servidor. Existe una solicitud de mejora ([CSCuv27099](#)) para borrar la información almacenada en caché de UCS Manager (UCSM). El administrador del servidor también puede ponerse en contacto con el Cisco Technical Assistance Center (TAC) para obtener una solución temporal.