

Ejecutar la herramienta de comprobación de estado y actualización previa de UCSM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Cuándo se debe utilizar](#)

[Cómo usarla](#)

[SO Windows](#)

[MacOS](#)

[Comprender las salidas/comprobaciones realizadas](#)

[Comprobaciones realizadas por la comprobación de estado de UCSM](#)

[Número de salida de la herramienta UCSM de ejemplo](#)

[Analizar la salida de la herramienta: siguientes pasos](#)

[Comandos CLI](#)

Introducción

Este documento describe el proceso para ejecutar la herramienta de comprobación de estado y actualización previa de Unified Computing System Manager (UCSM).

Prerequisites

Requirements

Cisco recomienda que tenga instalado Python 3.6 o posterior en el sistema.

Nota: Si está ejecutando el sistema operativo Windows, puede tener instalado Python y configurado el trayecto del Entorno.

Nota: No abra un caso TAC para problemas de Python/fallo al ejecutar el script. Consulte la sección de comandos de CLI para identificar manualmente el problema y abrir un caso de TAC por problema identificado

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La herramienta de comprobación de UCSM es una utilidad para realizar autocomprobaciones proactivas en UCSM con el fin de garantizar su estabilidad y resistencia. Ayuda a automatizar una lista de comprobaciones de estado y previas a la actualización de los sistemas UCS para ahorrar tiempo a la hora de llevar a cabo las operaciones de mantenimiento y actualización de la infraestructura de UCS.

Nota: descargue y utilice siempre la última versión de la herramienta. Dado que la herramienta se mejora con frecuencia, cuando se utiliza una versión anterior, puede pasar por alto comprobaciones importantes.

Nota: este script es un esfuerzo máximo, de uso gratuito y no puede identificar todos los problemas posibles.

Cuándo se debe utilizar

- Antes de actualizar la infraestructura UCS
- Comprobación del estado de UCS antes y después de la actividad de mantenimiento
- Cuando trabaja con Cisco TAC
- Comprobación de estado proactiva en cualquier momento

Cómo usarla

SO Windows

Paso 1. Descargar la última versión de Python desde [Python Descargas](#)

Paso 2. Utilice el proceso de instalación normal y haga clic en **Install Now** (el proceso recomendado) para descargar la configuración.

Nota: Asegúrese de marcar **Add Python to PATH**.

Python 3.10.0 (64-bit) Setup



python
for
windows

Install Python 3.10.0 (64-bit)

Select Install Now to install Python with default settings. Customize to enable or disable features.



Install Now

C:\Users\akmalla\AppData\Local\Programs\Python\Python310

Includes IDLE, pip and documentation
Creates shortcuts and file associations



Customize installation

Choose location and features

Install launcher for all users (recommended)

Add Python 3.10 to PATH

Paso 3. Navegue hasta el directorio en el que Python se instaló en el sistema.

Paso 4. Abra el símbolo del sistema y escriba el comando **Python** para verificar la instalación de python.

Command Prompt - python

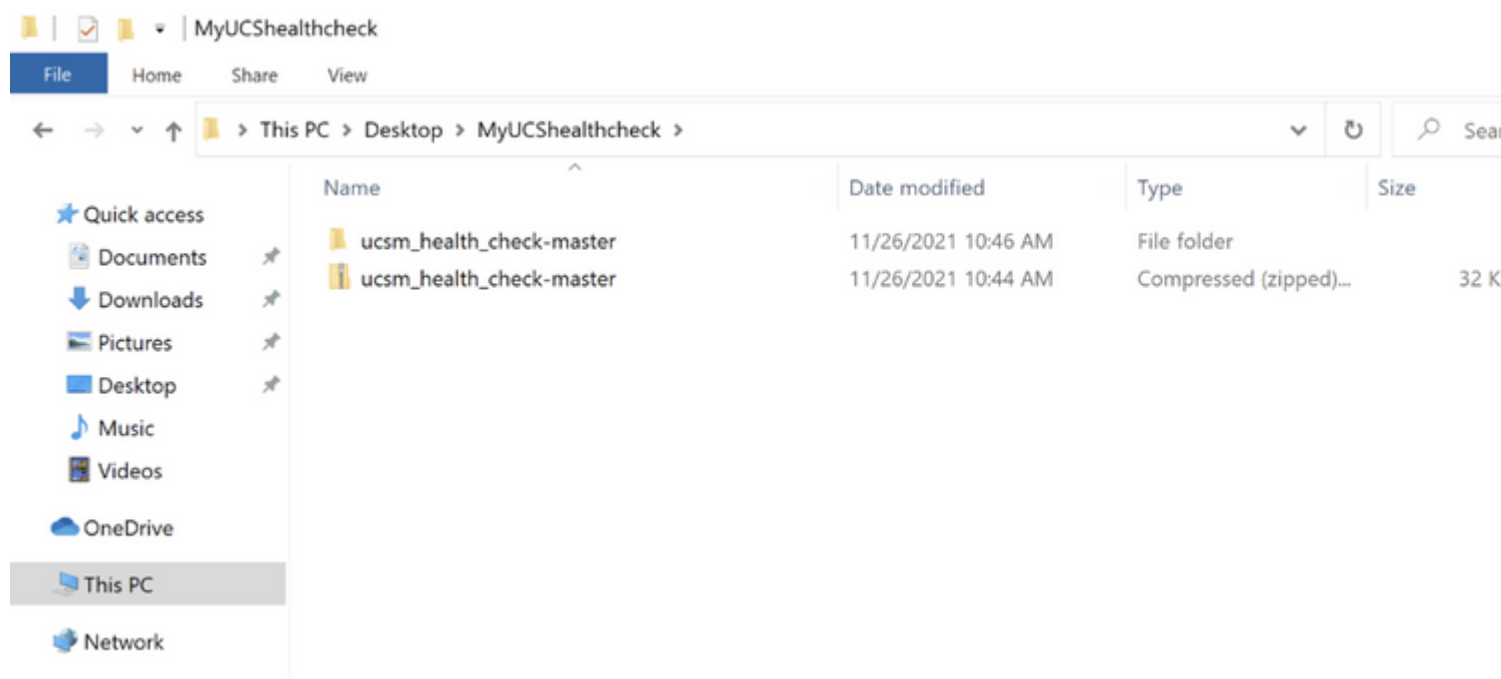
```
Microsoft Windows [Version 10.0.19043.1288]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\akmalla>python
```

```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct 4 2021, 19:00:18) [MSC v.1929 64 bit (AMD64)] on  
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>>
```

Paso 5. Descargue la última versión del script de comprobación de estado desde [aquí](#) y guárdelo en una carpeta. Ahora, extraiga el archivo comprimido, como se muestra en la imagen.



Paso 6. **Descargue** y **guarde** los registros de asistencia técnica de UCSM más recientes en la carpeta creada, como se muestra en la imagen. Haga clic en este enlace para buscar los pasos para descargar el paquete de registro de UCSM; [Generación de soporte técnico de UCSM](#).

Paso 7. Abra CMD y cd en la carpeta donde se encuentra UCSMTool.py y ejecute **UCSMTool.py** como se muestra en la imagen.

C:\> Select Command Prompt - UCSMTool.py

```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\[redacted]>cd akash
```

```
C:\Users\[redacted]>cd ucsm_health_check-mast
```

```
C:\Users\[redacted]\ucsm_health_check-master>
```

```
UCS Health Check Tool 1.1
```

```
Enter the UCSM file path: █
```

Paso 8. Introduzca la ruta del archivo en el que se encuentra el archivo de asistencia técnica de UCSM y seleccione la **opción deseada**.

1. Comprobación de estado de UCSM
2. Comprobación previa a la actualización

```
C:\[redacted]\Akash\ucsm_health_check-master>UCSMTool.py

UCS Health Check Tool 1.1

Enter the UCSM file path: \Akash\ucsm

Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1
Invalid file path: \Akash\ucsm

C:\[redacted]\Akash\ucsm_health_check-master>UCSMTool.py

UCS Health Check Tool 1.1

Enter the UCSM file path: C:\[redacted]\Akash\UCSM.tar

Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1

Log Extraction: [#####] COMPLETED
```

MacOS

Paso 1. MacOS viene con el Python predeterminado instalado, verifique la versión de Python instalada como se muestra aquí:

```
[MacBook-Pro:~ gakumari$ python --version
Python 2.7.16
[MacBook-Pro:~ gakumari$
[MacBook-Pro:~ gakumari$ python3 --version
Python 3.9.9
```

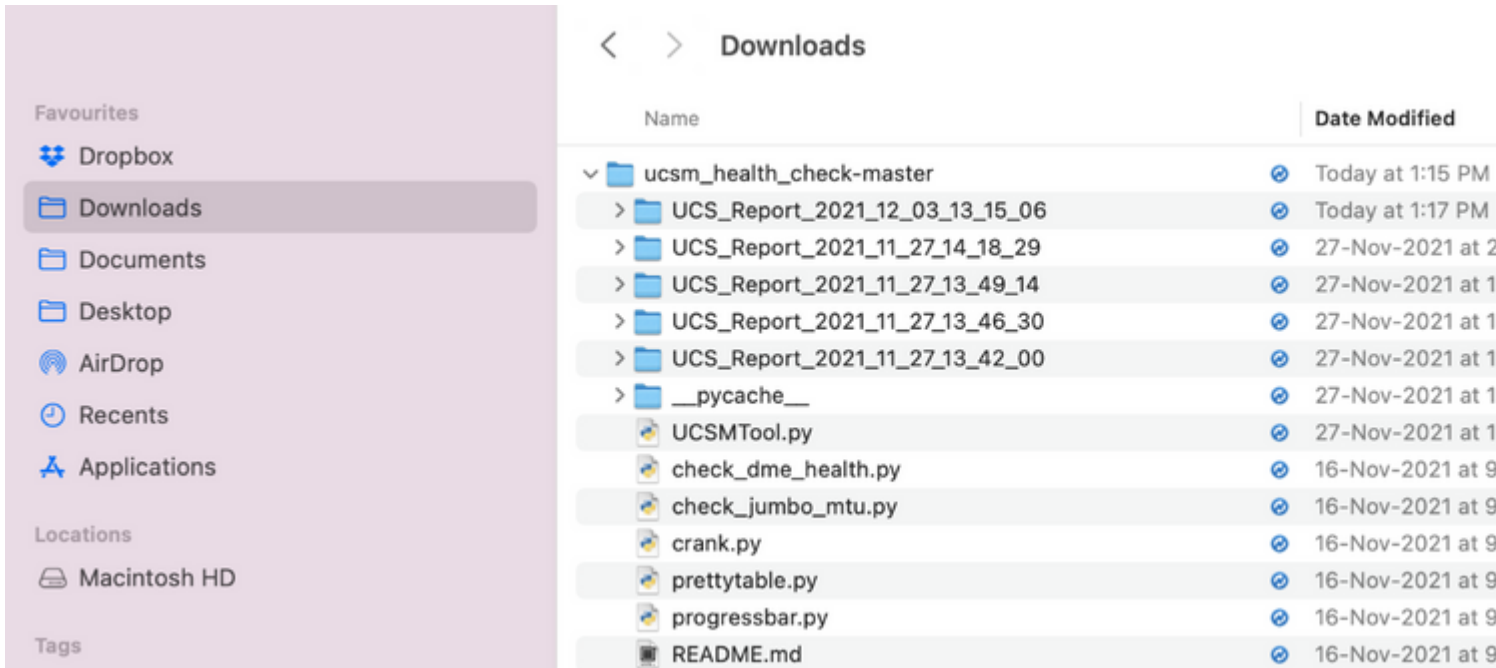
Nota: En caso de que la versión de Python sea inferior a la 3.6, actualice a la versión 3.6 y posteriores.

Nota: Si la versión de Python es 3.6 o posterior, vaya directamente al paso 5; de lo contrario, vaya directamente al paso 2.

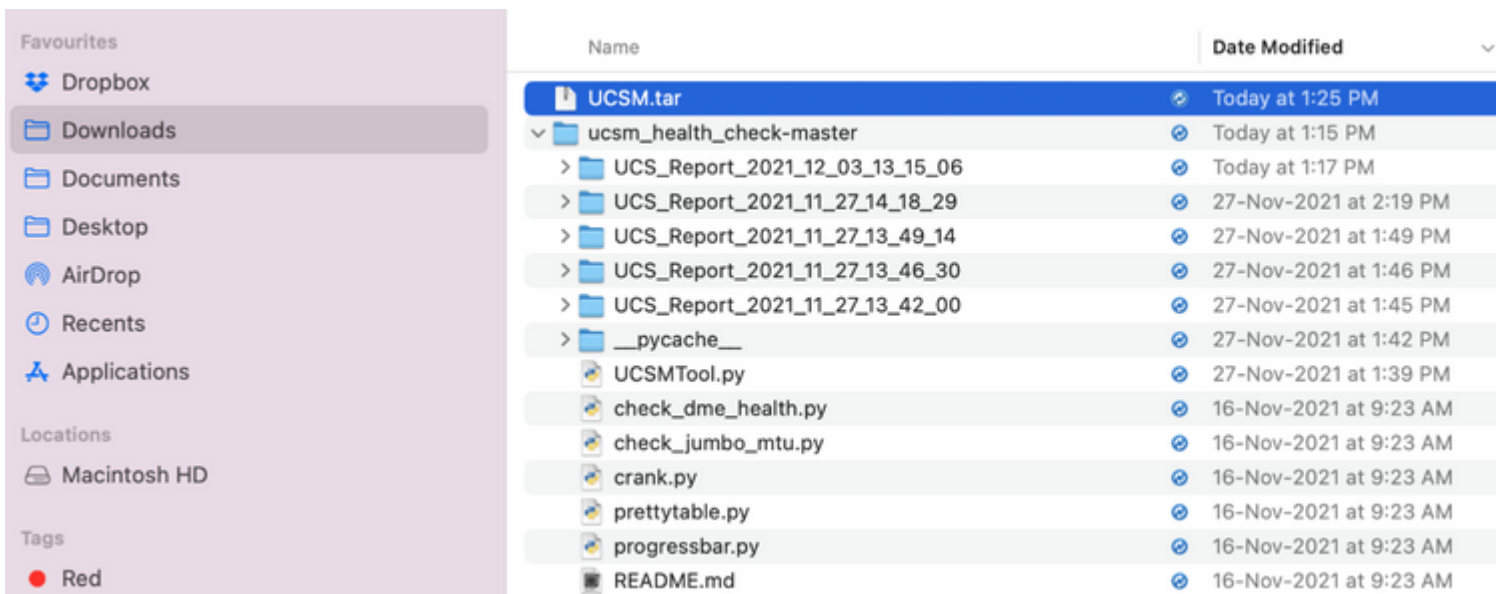
Paso 2. Descargue la última versión de Python desde <https://www.python.org/downloads/macos/>.

Paso 3. Utilice el proceso de instalación normal para completar/actualizar la instalación de Python.

Paso 4. **Descargue** desde [aquí](#) la última versión del script de comprobación de estado y **guárdelo** en una carpeta. Ahora, extraiga el archivo comprimido, como se muestra en esta imagen.



Paso 5. **Descargue y guarde** los registros de asistencia técnica de UCSM más recientes en la carpeta creada, como se muestra en esta imagen. Haga clic en el enlace para buscar los pasos para descargar el paquete de registro de UCSM; [Generación de soporte técnico de UCSM](#).



Paso 6. Abra el terminal, busque el directorio donde tiene descargada la secuencia de comandos de comprobación de estado, ejecute **python UCSMTool.py** o **python3UCSMTool.py** como se muestra aquí.

```

[MacBook-Pro:~ gakumari$ cd Downloads
[MacBook-Pro:Downloads gakumari$ cd ucsm_health_check-master/
[MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/py

```

Paso 7. Introduzca la ruta del archivo en el que se encuentra el archivo de asistencia técnica de UCSM y seleccione la **opción deseada** para ejecutar la secuencia de comandos.

1. Comprobación de estado de UCSM

2. Comprobación previa a la actualización

```
MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/
UCS MU Tool 1.1
Enter the UCSM file path: /Users/gakumari/Downloads/UCSM.tar
Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1
Log Extraction: [#####] COMPLETED
```

Comprender las salidas/comprobaciones realizadas

Comprobaciones realizadas por la comprobación de estado de UCSM

Estas comprobaciones las realiza UCSM-Healthchecktool:

Clúster UCSM HA Estado: Muestra el estado del clúster de las fabric interconectadas.

Proceso PMON Estado: Muestra el estado de todos los procesos de Cisco UCS Manager.

Montaje del sistema de archivos: muestra la tabla de montaje.

Verifique el problema de tamaño de /var/ sysmgr: Verifica los usos de /var/ sysmgr.

Verifique el tamaño de /var/ tmp: Verifica si /var/ tmp utiliza.

6296 FI no responde después de un ciclo de alimentación, actualización de revisión de hardware: Módulo de interconexión de estructura de verificación y su número de revisión de hardware.

Fallos con gravedad mayor o crítica: informa si tiene alguna alerta mayor o crítica en UCS Manager.

Comprobar copia de seguridad disponible: compruebe si la copia de seguridad está disponible en UCS Manager.

Certificado de llavero Comprobar: Compruebe si el anillo de claves ha caducado o es válido.

Solución alternativa de seguridad necesaria o no: verifique si se necesita o no una solución alternativa de seguridad mediante la verificación del modelo de FI y su versión.

Hardware obsoleto en Cisco UCS Manager versión 4.x: busque hardware obsoleto en Cisco UCS Manager versión 4.x.

Se ha encontrado hardware obsoleto para 3.1.x en adelante: compruebe si hay hardware obsoleto en Cisco UCS Manager versión 3.x

Compruebe si B200M4 se ha reiniciado debido a campos MRAID12G en blanco: compruebe si el servidor B200M4 tiene un S/N en blanco de la controladora RAID MRAID12G.

El cambio de UCSM 3.1 en la asignación de potencia máxima provoca un fallo en la detección de blades: verifica la política de alimentación configurada en UCS Manager.

Existencia de error de corrupción de bootflash código F1219: Verifique la existencia de corrupción de bootflash.

Compruebe si httpd no se inicia cuando se elimina el anillo de claves predeterminado: compruebe si se elimina el anillo de claves predeterminado.

Los FI de 3ª GENERACIÓN tienen estados de sistema de archivos no limpios-"Estado del sistema de archivos: limpiar con errores": Comprobar si hay errores en el sistema de archivos.

Comprobar si la instalación automática del servidor en la versión 4.0(4b) no activa la controladora SAS: compruebe la versión del firmware del host y la versión del amplificador SAS

Verifique que la actualización del firmware de la serie C se mantenga durante mucho tiempo en el proceso de "realizar un inventario del servidor" PNU OS Inventory: verifica el modelo del servidor y su versión para identificar si se da este problema.

Verifique el dominio de autenticación de UCSM que utiliza un punto o un guión: Verifique si el nombre del dominio de autenticación está configurado con un punto o caracteres de guión.

Error de autenticación local o de reserva: verifique el método de autenticación configurado para un modelo de FI determinado y verifique también su versión.

Comprobación de estado entre UCSM y UCS central: Compruebe si UCSManager está registrado con UCS Central

Grupos de pines LAN y SAN: verifique la configuración de pines LAN/SAN en su clúster y resalte para revisar su configuración antes de la actualización/cualquier actividad MW

Comprobación de las actividades pendientes presentes en UCSM: compruebe si hay actividades pendientes en el dominio de UCS Manager.

Comprobación del estado de IOM: Compruebe el estado general de los módulos de IOM.

Archivos de núcleo disponibles en la comprobación de UCSM: compruebe si se encuentra algún archivo de núcleo en un plazo de 60 días.

Posible configuración errónea de L2 desconectada: verifique si existe alguna configuración incorrecta en caso de que se configure la configuración de L2 desconectada.

Problema de inestabilidad de link de VIC 1400 y 6400: Verifique las condiciones presentes en este defecto

Verifique que los IOM 2304 se desconecten y se vuelvan a conectar durante la actualización del firmware: verifique el modelo de módulo de E/S e interconexión del fabric e identifique si existe algún problema potencial.

Comprobación del estado de DME: compruebe el estado de la base de datos de Data Management Engine (DME).

Número de interfaz activa y coincidencia de indicadores en FI: verifique el número de interfaces y la

sesión de indicadores dinámicos

Comprobación de MTU Jumbo o Estándar: Identifique la configuración de MTU.

Número de salida de la herramienta UCSM de ejemplo

```
afrahmad@AFRAHMAD-M-C3RS ucsm_health_check-master $ python UCSMTool.py
```

```
UCS Health Check Tool 1.1
```

```
Enter the UCSM file path: /Users/afrahmad/Desktop/20190328180425_fabric-5410-1k08_UCSM.tar
```

```
Press 1 for UCSM Health Check
```

```
Press 2 for PreUpgrade Check
```

```
Enter your choice (1/2): 2
```

```
Enter the UCS Target Version [Ex:4.1(1x)]: 4.2(1i)
```

```
Log Extraction: [#####] COMPLETED
```

```
UCSM Version: 3.2(3h)A
```

```
Target Version: 4.2(1i)
```

```
Upgrade Path: 3.2(3) ==> 4.2(1i)
```

```
Summary Result:
```

SlNo	Name	Status	Comments
1	UCSM HA Cluster State	PASS	
2	PMON Process State	PASS	
3	File System Mount	PASS	
4	Check for /var/sysmgr size issue	Not Found	
5	Check for /var/tmp size issue	Not Found	
6	6296 FI unresponsive after power cycle, HW revision update	Not Found	
7	Faults with Severity Major or Severity Critical	Found	Review the faults
8	Check Backup Available	No Backup	Please ensure backup is available. Refer this link: http://go2.cisco.com
9	Keyring Cert Check	PASS	
10	Safeshut Workaround Needed or Not	Not Needed	
11	Deprecated Hardware in Cisco UCS Manager Release 4.x	Found	Review the release notes. Refer this link: http://go2.cisco.com
12	Deprecated HW found for 3.1.x onwards	Not Found	
13	Check for B200M4 reboot due to blank MRAID12G fields	Found	Contact TAC

14	UCSM 3.1 Change in max power allocation causes blade discovery failure	Not Found	
15	Existence of bootflash corruption fault code F1219	Not Found	
16	Check for httpd fail to start when default keyring is deleted	Not Found	
17	3rd GEN FIs has unclean file system states-"Filesystem state: clean with errors"	Not Found	
18	Check for Server Auto-Install to 4.0(4b) Fails to Activate SAS Controller	Not Found	
19	Check for C-Series firmware upgrade stays long in process "perform inventory of server" PNU OS Inventory	Not Found	
20	Check UCSM Authentication Domain using a Period or Hyphen	Not Found	
21	Local or fallback Authentication failure	Not Found	
22	Health check between UCSM and UCS central	Not Found	UCS Manager is
23	LAN and SAN Pin Groups	Not Found	
24	Checking Pending Activities Present in UCSM	Not Found	
25	Health Check for IOM	PASS	
26	Core Files available in UCSM Check	Not Found	No core files
27	Disjoint L2 potential misconfiguration	Not Found	
28	VIC 1400 and 6400 Link Flap Issue	Not Found	
29	Check 2304 IOMs disconnect and re-connect during firmware update step	Not Found	
30	Number of Interface up and Flogi Matching on FI	---	Primary: FC Port Trun Eth up Port: Flogi Count: Secondary: FC Port Trun Eth up Port: Flogi Count:
31	Jumbo or Standard MTU Check	NOT_FOUND	

Faults with Severity Major:

F0207: Adapter ether host interface 3/3/1/2 link state: down
F0207: Adapter ether host interface 3/3/1/4 link state: down
F0207: Adapter ether host interface 3/3/1/3 link state: down
F0283: ether VIF 1153 on server 3 / 3 of switch B down, reason: Admin config change
F0479: Virtual interface 1153 link state is down

We would recommend Customers should complete the below prior to an upgrade:

- Review firmware release notes
- Review compatibility
- Upload required images
- Generate/Review UCSM show tech

- e. Determine vulnerable upgrade bugs and complete pro-active workaround
- f. Verify FI HA and UCSM PMON status
- g. Generate all configuration and full state backups (right before upgrade)
- h. Verify data path is ready (right before upgrade)
- i. Disable call home (right before upgrade)

NOTE:

- a. All reports and logs will be saved in the same location from where the script was executed.
- b. Please visit the Summary Report/ Main Report to view all the Major and Critical Fault alerts.

Analizar la salida de la herramienta: siguientes pasos

- La herramienta automatiza el proceso de ejecución de comandos manuales en los sistemas UCS.
- Si la herramienta se ejecuta **OK** y ofrece **APROBADO/NO ENCONTRADO** en todas las pruebas. El sistema UCS es bueno para todas las comprobaciones que ha realizado el script.
- En situaciones donde la herramienta **FRACASAR/ENCONTRADO** en algunas comprobaciones o si no se ejecuta correctamente, puede utilizar los comandos de CLI (enumerados aquí) para realizar las mismas comprobaciones en UCS System/Fabric Interconnect que las realizadas en la secuencia de comandos Manualmente.
- La herramienta **NO** comprueba si hay advertencias antiguas/nuevas/abiertas/resueltas y, por tanto, se recomienda revisar las notas de la versión de UCS y las guías de actualización antes de llevar a cabo cualquier actividad de actualización o mantenimiento.

Consejo: Para realizar una comprobación general del estado de su entorno UCS, Cisco TAC no proporciona este servicio. El equipo de atención al cliente de Cisco CX (anteriormente conocido como Advanced Services) dispone de un análisis de riesgos/depuración de errores que ofrece. Si necesita este tipo de servicio, póngase en contacto con el equipo comercial/de cuentas.

Comandos CLI

SSH a ambos Fabric Interconnects:

```
# show cluster extended-state, verify HA status is ready.

# connect local-mgmt ; # show pmon state, Verify the services are in running status.

# connect nxos ; # show system internal flash, Verify free size in /var/sysmgr and /var/tmp

# connect nxos ; # show module, verify HW revision number for 6296 fabric interconnects.

# show fault detail | include F1219, verify this fault code for bootflash corruption

# show iom health status, displays health of IOM

# show server status, verify the status of server.

# scope monitoring; # scope sysdebug; # show cores , verify if there are any core files.

# scope security; # scope keyring default; #show detail, verify details for default keyring, expiry etc

# connect nxos; # show int br | grep -v down | wc -l, verify the number of active Ethernet interfaces
```

scope security; # show authentication, review the authentication type.

connect nxos; # show flogi database, review the flogi database.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).