

Esegui strumento di verifica dello stato e pre-aggiornamento UCSM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Scenari d'uso](#)

[Modalità d'uso](#)

[Sistema operativo Windows](#)

[MacOS](#)

[Uscite/controlli eseguiti](#)

[Controlli eseguiti dal controllo di prevenzione sullo stato UCSM](#)

[Numero di output dello strumento UCSM di esempio](#)

[Analisi output strumento - Passaggi successivi](#)

[Comandi CLI](#)

Introduzione

Questo documento descrive il processo di esecuzione dello strumento di verifica dello stato e pre-aggiornamento di Unified Computing System Manager (UCSM).

Prerequisiti

Requisiti

Cisco consiglia di installare Python 3.6 o versioni successive.



Nota: se si esegue il sistema operativo Windows, è possibile installare e configurare il percorso di ambiente tramite Python.



Nota: non aprire una richiesta TAC per problemi/errori di esecuzione dello script Python. Fare riferimento alla sezione dei comandi CLI per identificare manualmente il problema e aprire la richiesta TAC per ciascun problema identificato.


Componenti usati


Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

UCSM Check Tool è un'utilità per eseguire autocontrolli proattivi su UCSM al fine di garantirne la stabilità e la resilienza. Consente di automatizzare un elenco di controlli di integrità e pre-aggiornamento sui sistemi UCS per risparmiare tempo quando vengono eseguite le operazioni di aggiornamento e manutenzione dell'infrastruttura UCS.

 Nota: scarica e usa sempre la versione più recente dello strumento. Poiché lo strumento viene migliorato frequentemente, quando si utilizza una versione precedente, è possibile che non vengano eseguiti controlli importanti.

 Nota: si tratta di uno script molto utile e di facile utilizzo. Tuttavia, non è in grado di identificare tutti i problemi.

Scenari d'uso

- Prima degli aggiornamenti dell'infrastruttura UCS
- Controllo dello stato di UCS prima e dopo l'attività di manutenzione
- Quando si lavora con Cisco TAC
- Controllo proattivo in qualsiasi momento

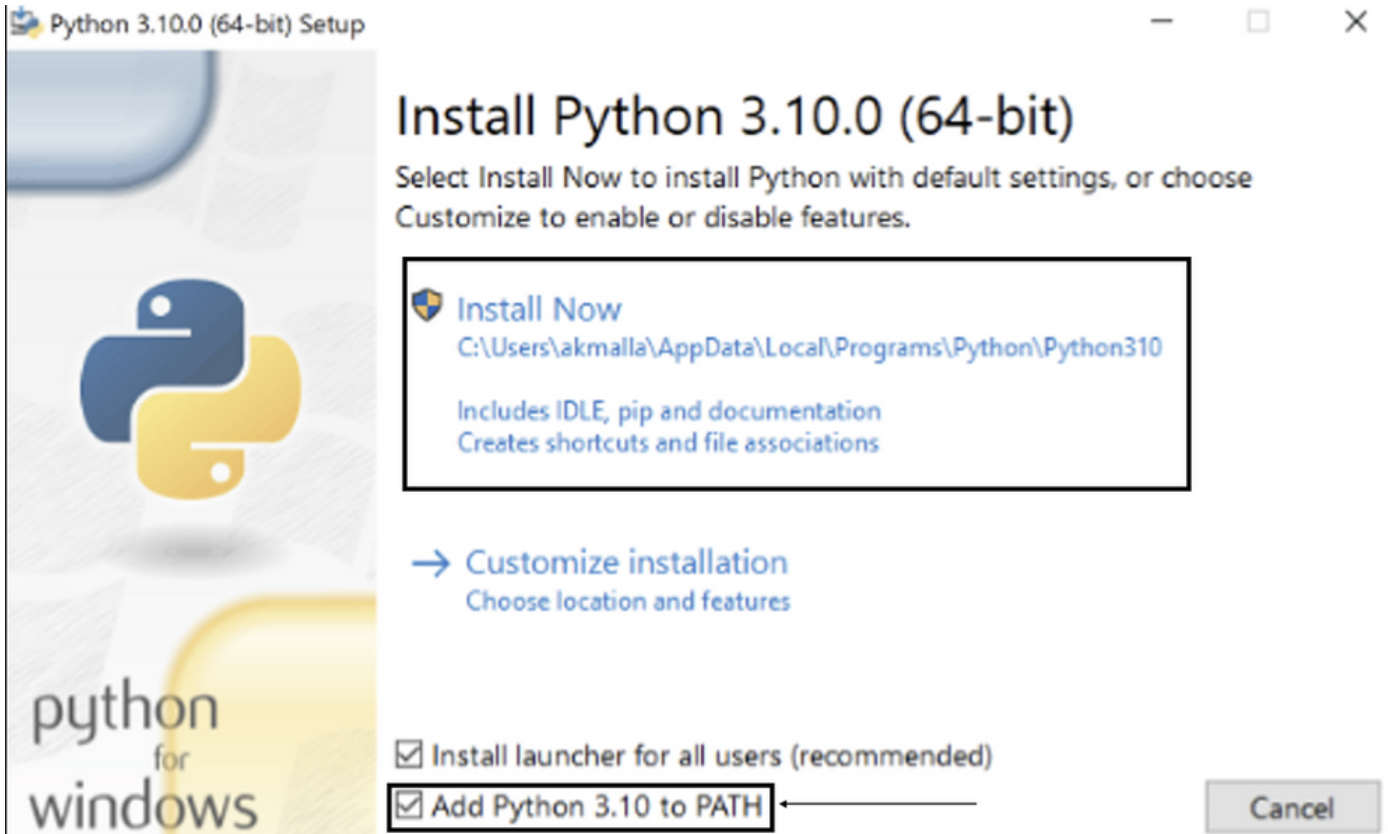
Modalità d'uso

Sistema operativo Windows

Passaggio 1. Scarica l'ultima versione di Python da [Python Downloads](#)

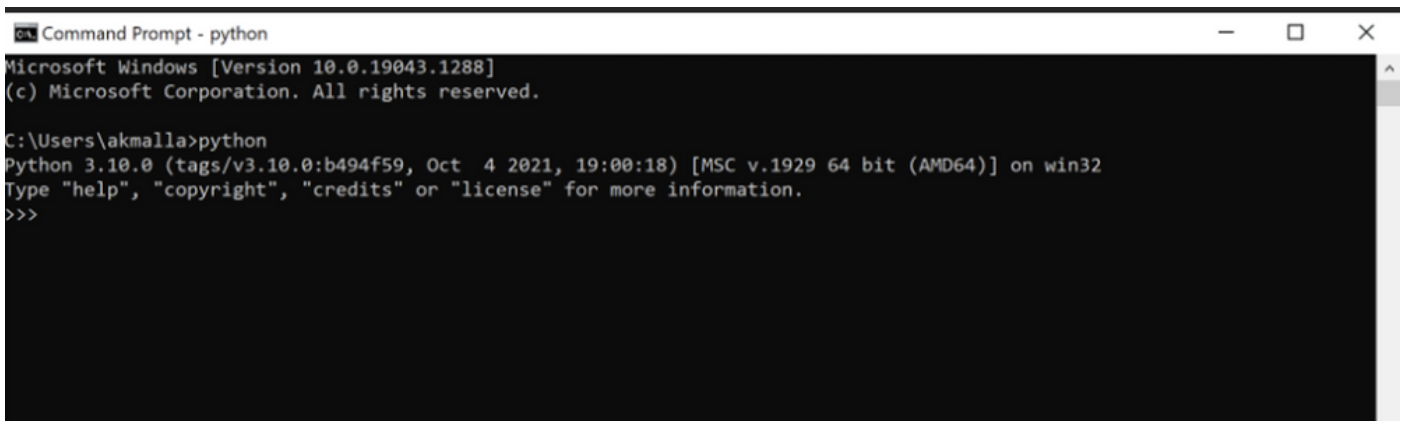
Passaggio 2. Utilizzare la normale procedura di installazione e fare clic su Installa ora (quella consigliata) per scaricare l'installazione.

 Nota: assicurarsi di selezionare Aggiungi Python a PATH.

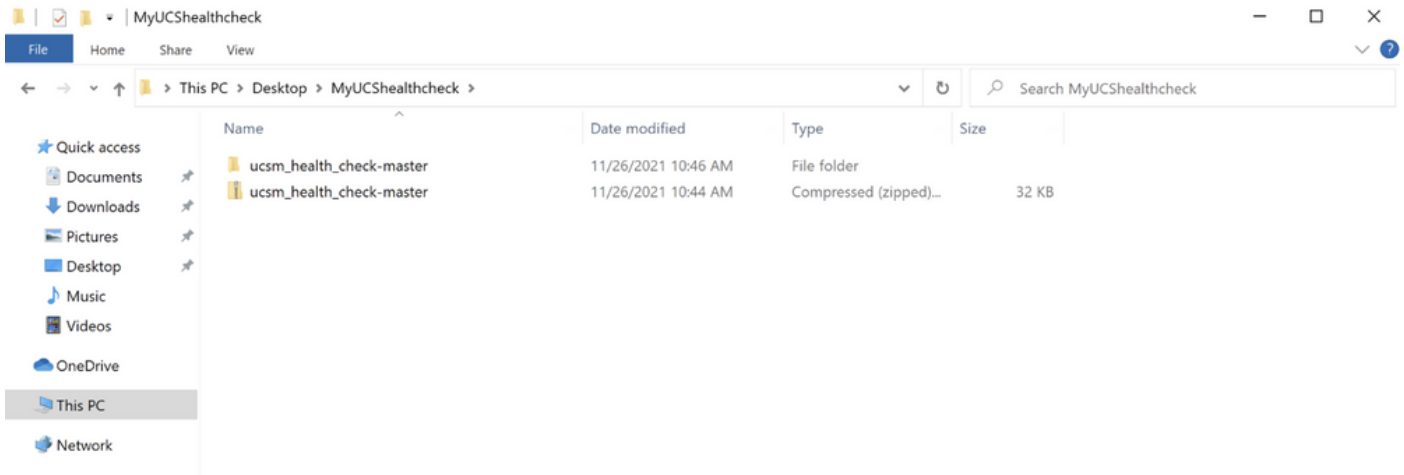


Passaggio 3. Passare alla directory in cui Python è stato installato sul sistema.

Passaggio 4. Aprire il prompt dei comandi e digitare il comando Python per verificare l'installazione di Python.



Passaggio 5. Scaricare la versione più recente dello script di controllo dello stato da [qui](#) e salvarla in una cartella. A questo punto, estrarre il file compresso, come mostrato nell'immagine.



Passaggio 6. Scaricare e salvare i log più recenti del supporto tecnico UCSM nella cartella creata, come mostrato nell'immagine. Fare clic su questo collegamento per trovare la procedura per scaricare il bundle di log UCSM: [Generazione del supporto tecnico UCSM](#).

Passaggio 7. Aprire CMD e cd nella cartella in cui si trova UCSMTool.py ed eseguire UCSMTool.py, come mostrato nell'immagine.

```
Select Command Prompt - UCSMTool.py
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\██████████>cd akash

C:\Users\██████████>cd ucsm_health_check-master

C:\Users\██████████\ucsm_health_check-master>UCSMTool.py

          UCS Health Check Tool 1.1

Enter the UCSM file path: █
```

Passaggio 8. Immettere il percorso del file di supporto tecnico UCSM e selezionare l'opzione desiderata.

1. Controllo dello stato UCSM
2. Controllo pre-aggiornamento

```
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

Passaggio 1. MacOS viene fornito con Python predefinito installato, verificare la versione Python installata come mostrato:

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

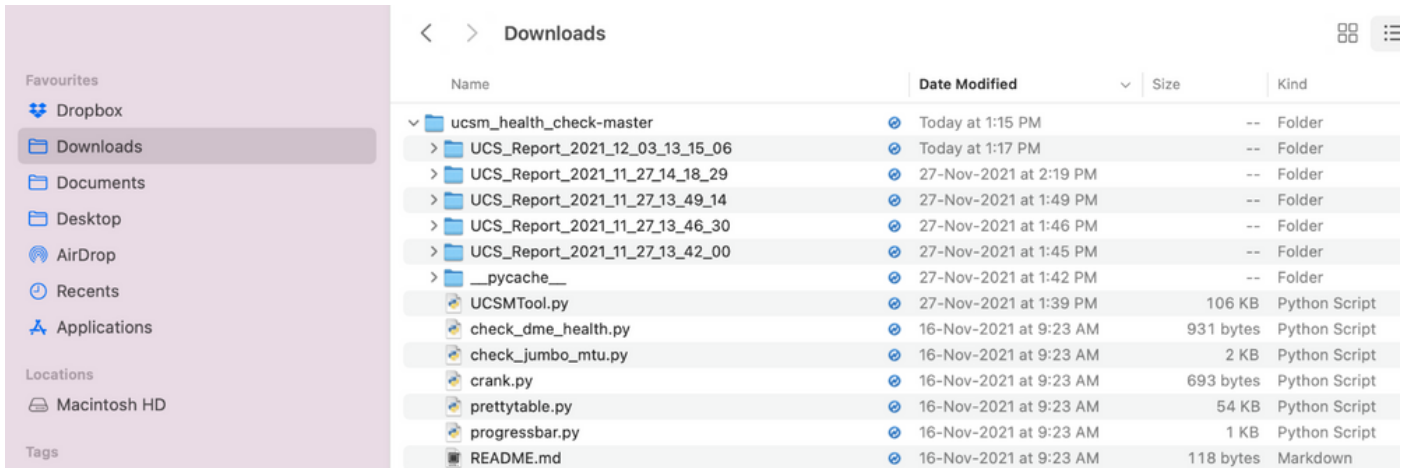
 Nota: se la versione Python è inferiore alla 3.6, aggiornare alla versione 3.6 e successive.

 Nota: se la versione Python è 3.6 o successiva, passare al punto 5. In caso contrario, passare al punto 2.

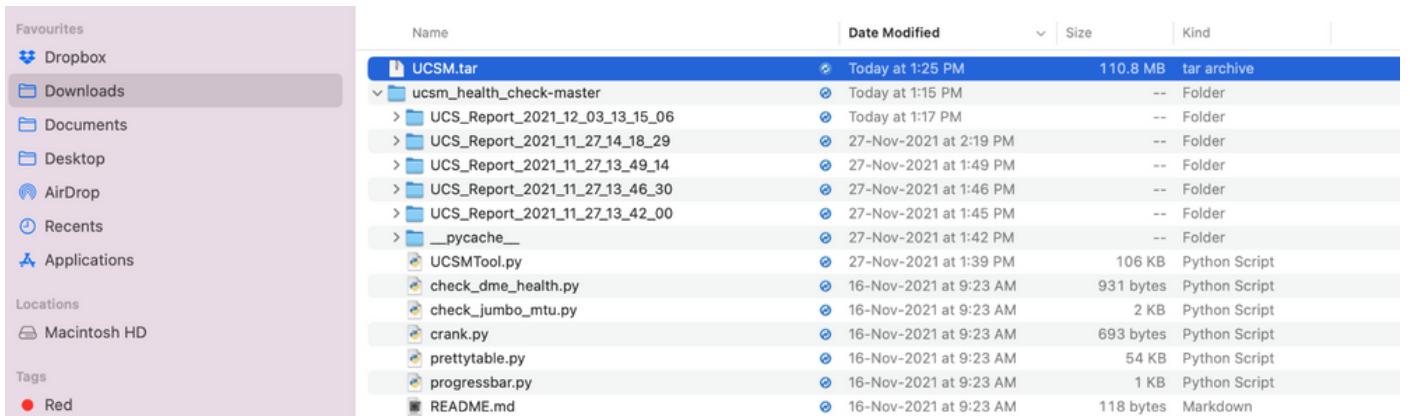
Passaggio 2. Scaricare l'ultima versione di Python dal sito <https://www.python.org/downloads/macos/>.

Passaggio 3. Utilizzare il normale processo di installazione per completare/aggiornare l'installazione Python.

Passaggio 4. Scaricare la versione più recente dello script di controllo dello stato da [qui](#) e salvarla in una cartella. A questo punto, estrarre il file compresso, come mostrato nell'immagine:



Passaggio 5. Scaricare e salvare i log più recenti del supporto tecnico UCSM nella cartella creata, come mostrato in questa immagine. Fare clic sul collegamento per trovare la procedura per scaricare il bundle di log UCSM: [Generazione del supporto tecnico UCSM](#).



Passaggio 6. Aprire il terminale, individuare la directory in cui è stato scaricato lo script di verifica dello stato, eseguire `python UCSMTTool.py` o `python3 UCSMTTool.py` come mostrato:.

```
MacBook-Pro:~ gakumari$ cd Downloads
MacBook-Pro:Downloads gakumari$ cd ucsm_health_check-master/
MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/python3 UCSMTTool.py
```

Passaggio 7. Immettere il percorso del file di supporto tecnico UCSM e scegliere l'opzione desiderata per eseguire lo script.

1. Controllo dello stato UCSM
2. Verifica pre-aggiornamento

```
MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/python3 UCSMTool.py
```

```
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
```

Uscite/controlli eseguiti

Controlli eseguiti dal controllo di prevenzione sullo stato UCSM

Questi controlli vengono eseguiti da UCSM-Healthchecktool:

Stato cluster UCSM HA: visualizza lo stato del cluster delle interconnessioni dell'infrastruttura.

PMON Process State: visualizza lo stato di tutti i processi in Cisco UCS Manager.

Montaggio file system: visualizza la tabella di montaggio.

Verificare il problema relativo alle dimensioni di /var/sysmgr: controlla gli utilizzi di /var/sysmgr.

Verifica la presenza di un problema relativo alle dimensioni di /var/tmp: verifica se vengono utilizzati/var/tmp.

6296 FI non risponde dopo un ciclo di alimentazione, aggiornamento revisione hardware: verificare il modulo Fabric interconnect e il relativo numero di revisione hardware.

Errori con livello di gravità maggiore o critico: segnala se si dispone di un avviso grave o critico in UCS Manager.

Controlla backup disponibile: verificare se il backup è disponibile in UCS Manager.

Controllo certificato keyring: verificare se il keyring è scaduto o valido.

Soluzione di sicurezza necessaria o no: verificare se è necessaria o meno una soluzione di sicurezza verificando il modello FI e la relativa versione.

Hardware deprecato in Cisco UCS Manager versione 4.x: verificare la presenza di hardware deprecato in Cisco UCS Manager versione 4.x.

Trovato hardware deprecato per la versione 3.1.x in avanti: verificare la presenza di hardware deprecato in Cisco UCS Manager 3.x Release

Controllare il riavvio B200M4 a causa di campi vuoti MRAID12G: verificare se il server B200M4

dispone di un S/N vuoto del controller RAID MRAID12G.

UCS 3.1 La modifica dell'allocazione massima dell'alimentazione causa un errore di rilevamento del blade: verifica i criteri di alimentazione configurati in UCS Manager.

Esistenza del codice di errore del danneggiamento bootflash F1219: verificare l'esistenza di un danneggiamento bootflash.

Verificare che httpd non venga avviato quando viene eliminato il keyring predefinito: verificare se il keyring predefinito è stato eliminato.

Gli FI di 3a GENERAZIONE hanno stati del file system non puliti-"Stato del file system: pulito con errori": verificare la presenza di errori del file system.

Verifica installazione automatica server alla versione 4.0(4b): impossibile attivare il controller SAS: verificare la versione del firmware dell'host e la versione di SAS Expander

Verificare che l'aggiornamento del firmware della serie C rimanga a lungo in fase di "esecuzione di un inventario del server" PNU OS Inventory: Verifica il modello del server e la relativa versione per identificare se si è verificato questo problema.

Controllare il dominio di autenticazione UCSM che utilizza un punto o un trattino: verificare se il nome del dominio di autenticazione è configurato con un punto o un trattino.

Errore di autenticazione locale o fallback: verificare la presenza di un metodo di autenticazione configurato per un particolare modello FI e verificarne anche la versione.

Verifica dello stato tra UCS Manager e UCS Central: verifica della registrazione di UCS Manager con UCS Central

Gruppi di pin LAN e SAN: controllare la configurazione del pin LAN/SAN nel cluster ed evidenziarla per rivedere la configurazione prima dell'aggiornamento/di qualsiasi attività MW

Controllo delle attività in sospeso presenti in UCS Manager in corso. Verificare se sono presenti attività in sospeso nel dominio di UCS Manager.

Controllo stato per IOM: verifica dello stato complessivo dei moduli di I/O.

File di base disponibili in UCSM Verifica: verifica della presenza di eventuali file di base entro 60 giorni.

Possibile configurazione errata di L2 indipendente: verificare l'eventuale presenza di configurazioni errate nel caso in cui l'opzione L2 indipendente sia configurata.

Problema di link flap VIC 1400 e 6400: verificare le condizioni presenti nel problema

Controllare la disconnessione e la riconnessione degli IOM 2304 durante l'aggiornamento del firmware: verificare il modello del modulo Fabric Interconnect e IO e identificare eventuali problemi potenziali.

Controllo integrità DME: verificare lo stato del database DME (Data Management Engine).

Numero di interfacce attive e di corrispondenza floppy su FI: verificare il numero di interfacce e la sessione del floppy

Controllo MTU jumbo o standard: identificare la configurazione MTU.

Numero di output dello strumento UCSM di esempio

```
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:
```

S/No	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 fa
8	Check Backup Available	No Backup	Please ensure Refer this li http://go2.ci
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 re Refer this li http://go2.ci

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 i
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 Tru Eth up Port Flogi Count Secondary: FC Port Tru 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:


- a. Review firmware release notes
- b. Review compatibility
- c. Upload required images
- d. 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.

Analisi output strumento - Passaggi successivi

- Lo strumento automatizza il processo di esecuzione dei comandi manuali sui sistemi UCS.
- Se lo strumento viene eseguito correttamente e fornisce PASS/NOT FOUND per tutti i test. Il sistema UCS è adatto per tutti i controlli eseguiti dallo script.
- Nelle situazioni in cui lo strumento FAIL/FOUND su alcuni controlli o non viene eseguito correttamente, è possibile utilizzare i comandi CLI (elencati qui) per eseguire sugli interconnettori UCS System/Fabric gli stessi controlli eseguiti manualmente dallo script.
- Lo strumento NON verifica la presenza di avvertenze vecchie/nuove/aperte/risolte e pertanto si consiglia di esaminare le note sulla versione e le guide all'aggiornamento UCS prima di qualsiasi attività di aggiornamento o manutenzione.

 Suggerimento: per un controllo generale dello stato dell'ambiente UCS, Cisco TAC non fornisce questo servizio. Il team CX Customer Delivery di Cisco (in precedenza Advanced Services) dispone di un'analisi dei rischi e degli errori che offre. Per questo tipo di servizio, contattare il team vendite/account.

Comandi CLI

SSH su entrambe le interconnessioni fabric:

```
# 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 et

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.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).