

UCSM 상태 및 업그레이드 전 확인 툴 실행

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[사용 시기](#)

[사용 방법](#)

[윈도우 OS](#)

[MacOS](#)

[수행되는 출력/확인 이해](#)

[UCSM HealthCheck에서 수행한 검사](#)

[샘플 UCSM 툴 출력 번호](#)

[툴 출력 분석 - 다음 단계](#)

[CLI 명령](#)

소개


이 문서에서는 UCSM(Unified Computing System Manager) 상태 및 업그레이드 전 확인 도구를 실행하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

시스템에 Python 3.6 이상을 설치하는 것이 좋습니다.

 참고: Windows OS를 실행 중인 경우 Python을 설치하고 환경 경로를 구성할 수 있습니다.

 참고: Python 문제/스크립트가 실행되지 않은 경우 TAC 케이스를 열지 마십시오. CLI 명령 섹션을 참조하여 문제를 수동으로 식별하고 식별된 문제별로 TAC 케이스를 엽니다


사용되는 구성 요소


이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

UCSM Check Tool은 UCSM에서 사전 활성 자체 검사를 수행하여 안정성과 복원력을 보장하는 유틸리티입니다. UCS 시스템의 상태 및 업그레이드 전 확인 목록을 자동화하여 UCS 인프라 업그레이드 및 유지 보수 작업이 발생할 때 시간을 절약할 수 있습니다.

 참고: 항상 최신 버전의 툴을 다운로드하여 사용하십시오. 이 도구는 자주 향상되므로 이전 버전을 사용할 때 중요한 검사를 놓칠 수 있습니다.

 참고: 이 스크립트는 사용 가능한 최선의 방법이며 모든 가능한 문제를 식별할 수 없습니다.

사용 시기

- UCS 인프라 업그레이드 전
- UCS 상태 유지 관리 활동 전후 확인
- Cisco TAC과 협력할 경우
- 언제든지 사전 대응적 상태 확인

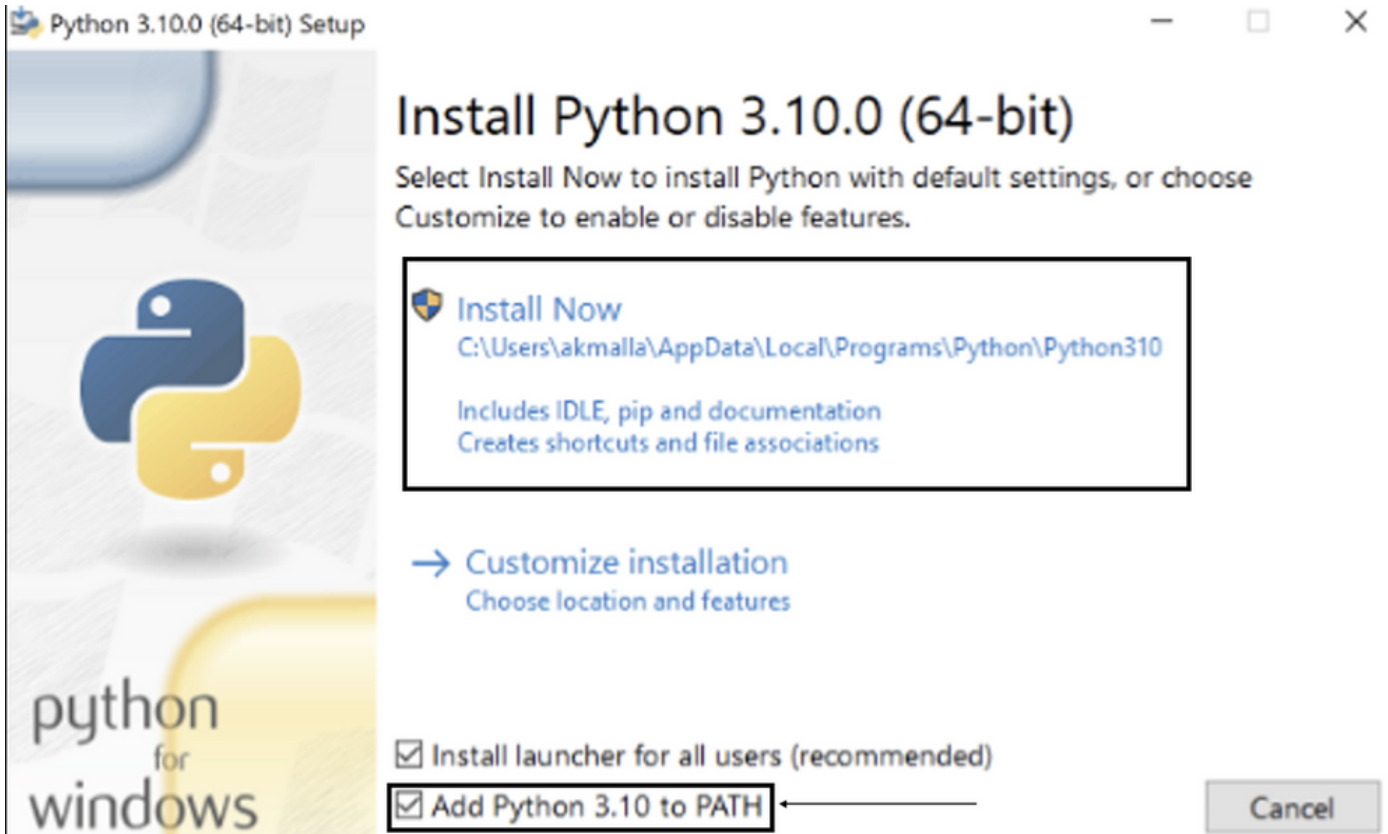
사용 방법

윈도우 OS

1단계. Python Downloads(Python 다운로드)에서 최신 버전의 [Python 다운로드](#)

2단계. 일반적인 설치 프로세스를 사용하고 Install Now(지금 설치)(권장)를 클릭하여 설치를 다운로드합니다.

 참고: Add Python to PATH(PATH에 Python 추가)를 선택해야 합니다.

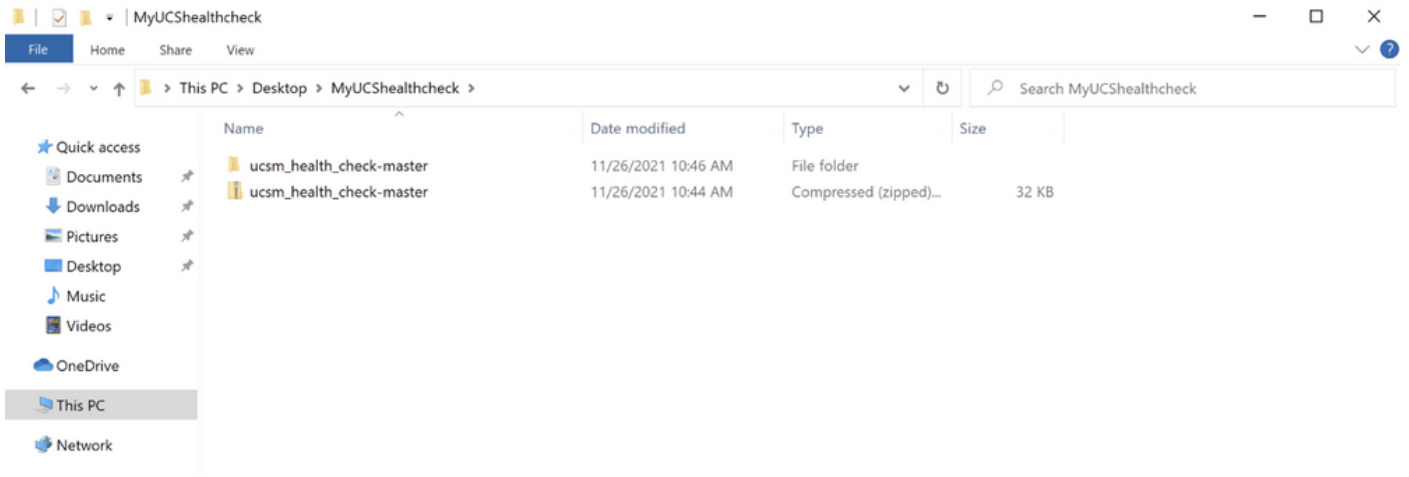


3단계. 시스템에 Python이 설치된 디렉토리로 이동합니다.

4단계. 명령 프롬프트를 열고 Python 명령을 입력하여 python 설치를 확인합니다.



5단계. [여기서](#) 최신 버전의 상태 확인 스크립트를 다운로드하여 폴더에 저장합니다. 이제 이미지에 표시된 대로 압축 파일을 추출합니다.



6단계. 이미지와 같이 최신 UCSM 기술 지원 로그를 다운로드하여 생성된 폴더에 저장합니다. 이 링크를 클릭하면 UCSM 로그 번들 다운로드 단계, UCSM [기술 지원 생성 단계를 확인할 수 있습니다.](#)

7단계. UCSMTool.py가 있는 폴더로 CMD 및 cd를 열고 이미지에 표시된 대로 UCSMTool.py를 실행합니다.

```
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: |
```

8단계. UCSM 기술 지원 파일이 있는 파일 경로를 입력하고 원하는 옵션을 선택합니다.


1. UCSM 상태 확인
2. 업그레이드 전 확인


```
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

1단계. MacOS는 기본 python이 설치된 상태로 제공되며, 다음과 같이 설치된 python 버전을 확인합니다.

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

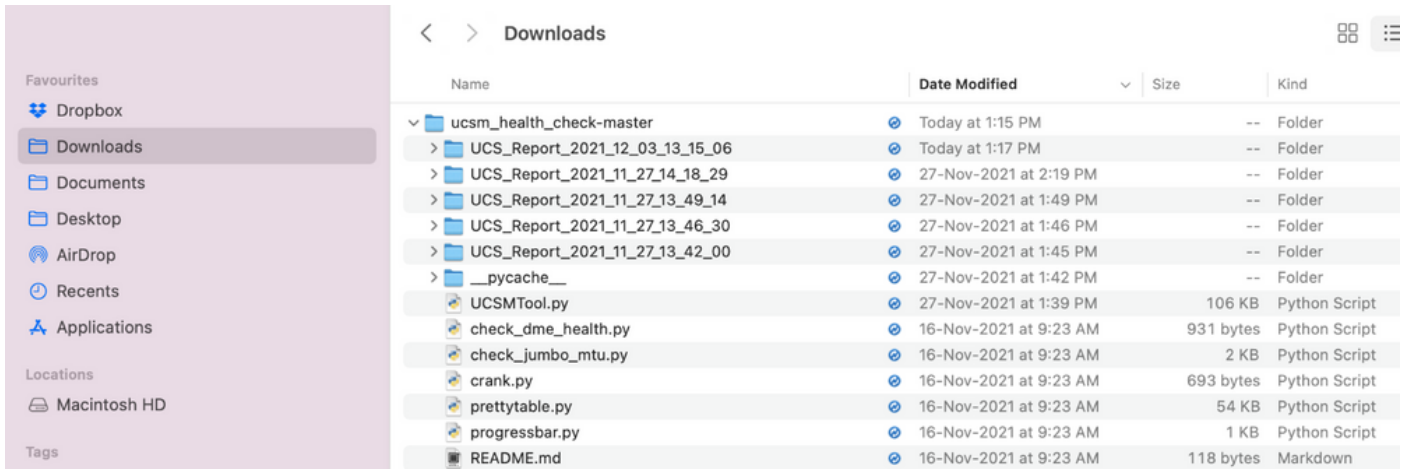
 참고: python 버전이 3.6보다 낮은 경우 3.6 이상 릴리스로 업그레이드하십시오.

 참고: python 버전이 3.6 이상이면 5단계로, 그렇지 않으면 2단계로 이동합니다.

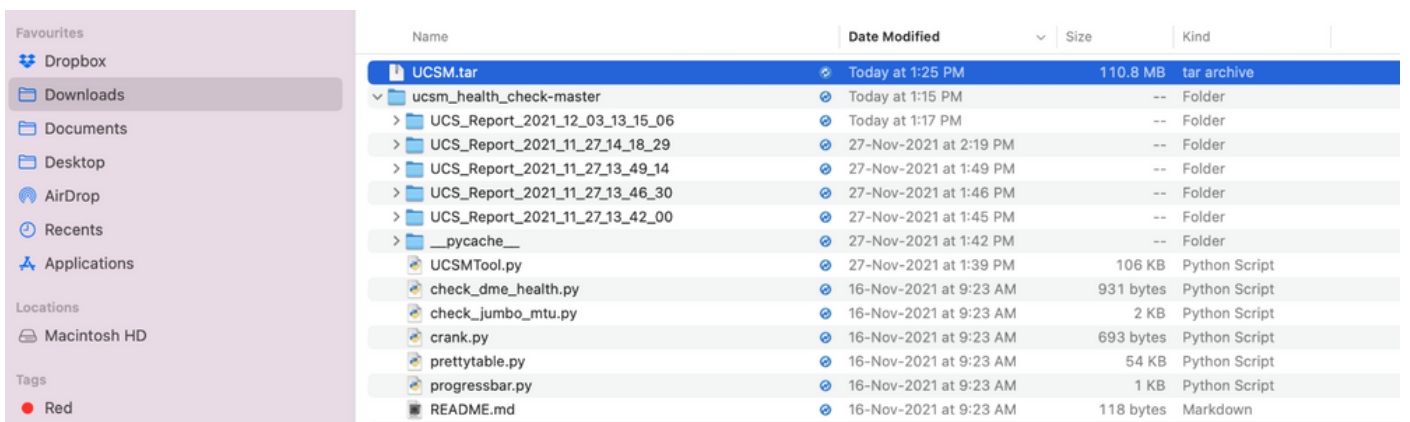
2단계. <https://www.python.org/downloads/macos/>에서 Python의 최신 버전을 [다운로드하십시오](#).

3단계. 일반적인 설치 프로세스를 사용하여 python 설치를 완료/업그레이드합니다.

4단계. [여기서](#) 상태 확인 스크립트의 최신 버전을 다운로드하여 폴더에 저장합니다. 이제 이 이미지에 표시된 대로 압축 파일을 추출합니다.



5단계. 이 이미지에 표시된 것처럼 최신 UCSM 기술 지원 로그를 다운로드하여 생성된 폴더에 저장합니다. 링크를 클릭하여 UCSM 로그 번들 다운로드 단계, UCSM [기술 지원 생성 단계를 찾습니다.](#)



6단계. 터미널을 열고 상태 확인 스크립트가 다운로드된 디렉토리로 이동한 다음 여기와 같이 python UCSMTool.py 또는 python3UCSMTool.py를 실행합니다.

```
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 UCSMTool.py
```

7단계. UCSM 기술 지원 파일이 있는 파일 경로를 입력하고 원하는 옵션을 선택하여 스크립트를 실행합니다.

1. UCSM 상태 확인
2. 업그레이드 전 확인

```
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
```

수행되는 출력/확인 이해

UCSM HealthCheck에서 수행한 검사

이러한 확인은 UCSM-Healthchecktool에서 수행합니다.

UCSM HA 클러스터 상태: Fabric Interconnect의 클러스터 상태를 표시합니다.

PMON 프로세스 상태: Cisco UCS Manager의 모든 프로세스 상태를 표시합니다.

파일 시스템 마운트: 마운트 테이블을 표시합니다.

/var/sysmgr 크기 문제 확인: /var/ sysmgr 사용 확인

/var/tmp 크기 문제 확인: /var/tmp가 사용되는지 확인합니다.

6296 FI가 전원 사이클 후 응답하지 않는 경우 HW 수정 버전 업데이트: Fabric Interconnect 모듈 및 해당 HW 수정 번호를 확인합니다.

Faults with Severity Major or or Severity Critical(심각도 주요 또는 심각도 중요 오류): UCS Manager에서 Major(주요) 또는 Critical(중요) 경고가 있는 경우 보고합니다.

사용 가능한 백업 확인: UCS Manager에서 백업을 사용할 수 있는지 확인합니다.

키 링 인증서 확인: 키가 만료되었거나 유효한지 확인하십시오.

Safeshut Workarout Needed or Not(필요한 해결 방법): FI 모델 및 해당 버전을 확인하여 Shafshut 해결 방법이 필요한지 여부를 확인합니다.

Cisco UCS Manager 릴리스 4.x에서 사용되지 않는 하드웨어: Cisco UCS Manager 4.x 릴리스에서 사용되지 않는 하드웨어가 있는지 확인하십시오.

3.1.x 이상의 사용되지 않는 하드웨어 발견: Cisco UCS Manager 3.x 릴리스에서 사용되지 않는 하드웨어가 있는지 확인

빈 MRAID12G 필드로 인해 B200M4가 재부팅되는지 확인: B200M4 서버에 MRAID12G RAID 컨트롤러의 빈 S/N이 있는지 확인합니다.

UCSM 3.1 최대 전력 할당 변경으로 인해 블레이드 검색 실패: UCS Manager에 구성된 전력 정책을 확인합니다.

bootflash 손상 결함 코드 F1219 존재: bootflash 손상이 있는지 확인합니다.

기본 키가 삭제될 때 httpd가 시작되지 않았는지 확인: 기본 키가 삭제되었는지 확인합니다.

3세대 FI에 잘못된 파일 시스템 상태가 있습니다.-"파일 시스템 상태: 오류가 있는 정상": 파일 시스템 오류를 확인하십시오.

4.0(4b)에 대한 서버 자동 설치 확인 실패 SAS 컨트롤러 활성화: 호스트 펌웨어 버전 및 SAS 익스팬더 버전을 확인합니다.

C-Series 펌웨어 업그레이드가 "서버 인벤토리 수행" PNU OS 인벤토리에서 오래 유지되는지 확인: 서버 모델 및 해당 버전을 확인하여 이 문제가 발생했는지 확인합니다.

Check UCSM Authentication Domain that uses a Period or Hyphen(마침표 또는 하이픈을 사용하는 UCSM 인증 도메인 확인): 인증 도메인 이름이 마침표 또는 하이픈 문자로 구성되어 있는지 확인합니다.

로컬 또는 풀백 인증 실패: 특정 FI 모델에 대해 구성된 인증 방법을 확인하고 해당 버전도 확인합니다.

UCSM과 UCS Central 간의 상태 확인: UCSManager가 UCS Central에 등록되어 있는지 확인

LAN 및 SAN 핀 그룹: 클러스터의 lan/san 피닝 컨피그레이션을 확인하고 업그레이드/MW 활동 전에 컨피그레이션을 검토하도록 강조 표시합니다

UCSM에 보류 중인 활동 확인: UCS Manager 도메인에 보류 중인 활동이 있는지 확인합니다.

Health Check for IOM: IO 모듈의 전반적인 상태를 확인합니다.

UCSM에서 사용 가능한 코어 파일 확인: 60일 내에 코어 파일이 있는지 확인합니다.

디스조인트 L2 잠재적 컨피그레이션 오류: 디스조인트 L2가 구성된 경우 잘못된 컨피그레이션이 있는지 확인합니다.

VIC 1400 및 6400 Link Flap 문제: 이 결함에 있는 상태 확인

펌웨어 업데이트 중 2304 IOM 연결 끊기 및 재연결 확인: Fabric Interconnect 및 IO 모듈 모델을 확인하고 잠재적인 문제가 있는지 확인합니다.

DME 상태 확인: DME(Data Management Engine) 데이터베이스의 상태를 확인합니다.

FI에서 인터페이스 작동 및 Flogi 일치 수: 인터페이스 및 flogi 세션 수를 확인합니다.

점보 또는 표준 MTU 확인: MTU 컨피그레이션을 식별합니다.

샘플 UCSM 톨 출력 번호

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:	Not Found	

	clean with errors"		
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:


- Review firmware release notes
- Review compatibility
- Upload required images
- Generate/Review UCSM show tech
- Determine vulnerable upgrade bugs and complete pro-active workaround
- Verify FI HA and UCSM PMON status
- Generate all configuration and full state backups (right before upgrade)
- Verify data path is ready (right before upgrade)
- Disable call home (right before upgrade)

NOTE:

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

툴 출력 분석 - 다음 단계

- 이 도구는 UCS 시스템에서 수동 명령을 실행하는 프로세스를 자동화합니다.
- 도구가 실행되는 경우 확인 및 통과/찾을 수 없음 모든 테스트에서 UCS 시스템은 스크립트가 수행한 모든 검사에 적합합니다.
- 툴이 실패/찾음 일부 검사 시 또는 정상적으로 실행되지 않을 경우 CLI 명령(여기에 나열됨)을 사용하여 UCS 시스템/패브릭 인터커넥트에 대해 스크립트에서 수동으로 수행한 것과 동일한 검사를 수행할 수 있습니다.
- 이 툴에서는 이전/새/열기/해결된 주의 사항을 확인하지 않으므로 업그레이드 또는 유지 관리 활동 전에 UCS 릴리스 정보 및 업그레이드 가이드를 검토하는 것이 좋습니다.

 **팁:** UCS 환경의 일반적인 상태 점검을 위해 Cisco TAC에서는 이 서비스를 제공하지 않습니다. Cisco의 CX Customer Delivery Team(이전의 Advanced Services)은 버그 스크립/위험 분석을 제공합니다. 이러한 유형의 서비스가 필요한 경우 세일즈/어카운트 팀에 문의하십시오.

CLI 명령

두 Fabric Interconnect에 대한 SSH:

```
# 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.
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.