

UCSM Health and Pre-Upgrade Check Toolの実行

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[使用するケース](#)

[使用方法](#)

[Windows OS](#)

[MacOS](#)

[実行される出力/チェックについて](#)

[UCSM HealthCheckによって実行されるチェック](#)

[サンプルUCSMツールの出力番号](#)

[ツール出力の分析 – 次のステップ](#)

[CLIコマンド](#)

はじめに


このドキュメントでは、Unified Computing System Manager(UCSM)の健全性とアップグレード前のチェックツールを実行するプロセスについて説明します。

前提条件

要件

システムにPython 3.6以降をインストールすることをお勧めします。

 注:Windows OSを実行している場合は、Pythonをインストールして環境パスを設定できません。

 注:Pythonの問題やスクリプトの実行に失敗した場合は、TACケースを開かないでください。問題を手動で特定し、特定された問題ごとにTACケースをオープンするには、「CLIコマンド」セクションを参照してください


使用するコンポーネント


このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

UCSM Check Toolは、UCSMの安定性と復元力を確保するためにUCSMのプロアクティブなセルフチェックを実行するユーティリティです。UCSシステムの健全性チェックとアップグレード前のチェックのリストを自動化し、UCSインフラストラクチャのアップグレードやメンテナンス作業にかかる時間を節約します。

 注：常に最新バージョンのツールをダウンロードして使用してください。このツールは頻繁に拡張されるため、古いバージョンを使用すると、重要なチェックを見逃す可能性があります。

 注：このスクリプトはベストエフォート型で、自由に使用でき、考えられるすべての問題を特定することはできません。

使用するケース


- UCSインフラストラクチャのアップグレード前
- メンテナンスアクティビティの前後のUCSヘルスチェック
- Cisco TACとの連携
- 予防的なヘルスチェック

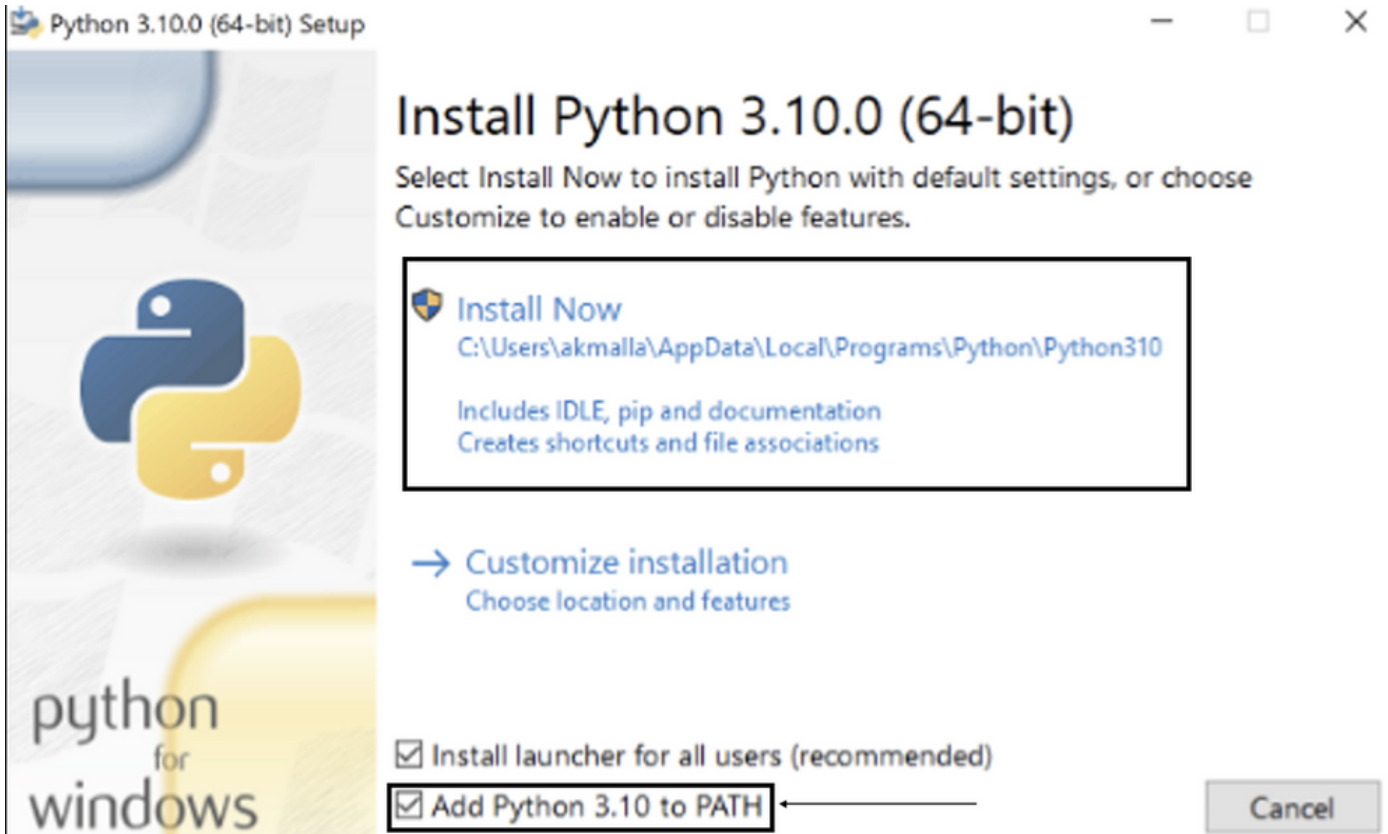
使用方法

Windows OS

ステップ 1： [Pythonダウンロード](#) から最新バージョンのPythonをダウンロードする

ステップ 2： 通常のインストールプロセスを使用し、Install Now (推奨) をクリックしてセットアップをダウンロードします。

 注： Add Python to PATHにチェックマークが付いていることを確認してください。



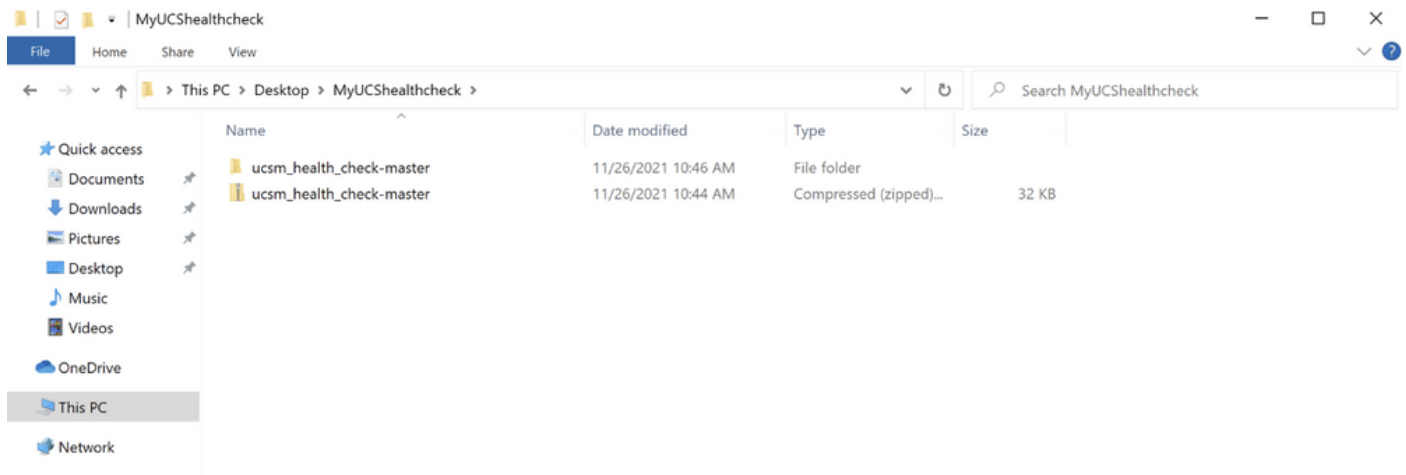
ステップ 3 : システム上でPythonがインストールされているディレクトリに移動します。

ステップ 4 : コマンドプロンプトを開き、コマンドPythonを入力してPythonのインストールを確認します。

```
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 win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

ステップ 5 : [ここ](#)から最新バージョンのヘルスチェックスクリプトをダウンロードし、フォルダに保存します。次に、図に示すように、圧縮ファイルを抽出します。



手順 6：次の図に示すように、最新のUCSMテクニカルサポートログをダウンロードし、作成したフォルダに保存します。このリンクをクリックして、UCSMログバンドルのダウンロード手順を確認してください。[UCSMテクニカルサポートの生成。](#)

手順 7：CMDを開き、UCSMTTool.pyが存在するフォルダに移動して、図に示すようにUCSMTTool.pyを実行します。

```
Select Command Prompt - UCSMTTool.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>UCSMTTool.py

UCS Health Check Tool 1.1

Enter the UCSM file path: |
```

ステップ 8：UCSMテクニカルサポートファイルがあるファイルパスを入力し、必要なオプションを選択します。


1. UCSMヘルスチェック
2. アップグレード前のチェック


```
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

ステップ 1 : MacOSには、デフォルトのPythonがインストールされた状態で付属しています。次に示すように、インストールされているPythonのバージョンを確認します。

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

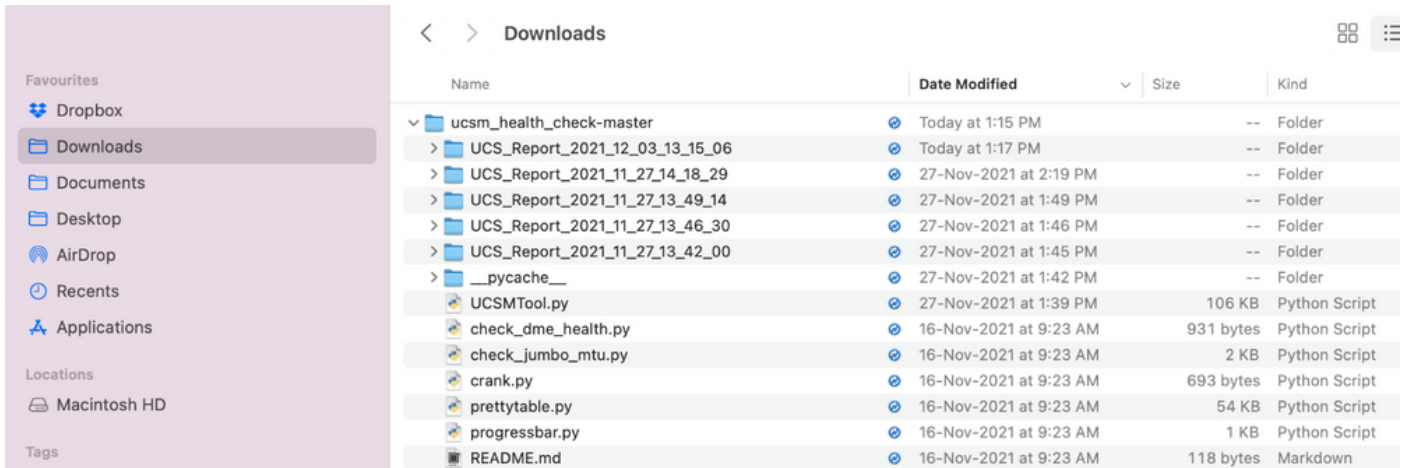
 注: Pythonのバージョンが3.6より古い場合は、3.6以降のリリースにアップグレードしてください。

 注: Pythonバージョンが3.6以降の場合はステップ5に進み、それ以外の場合はステップ2に進みます。

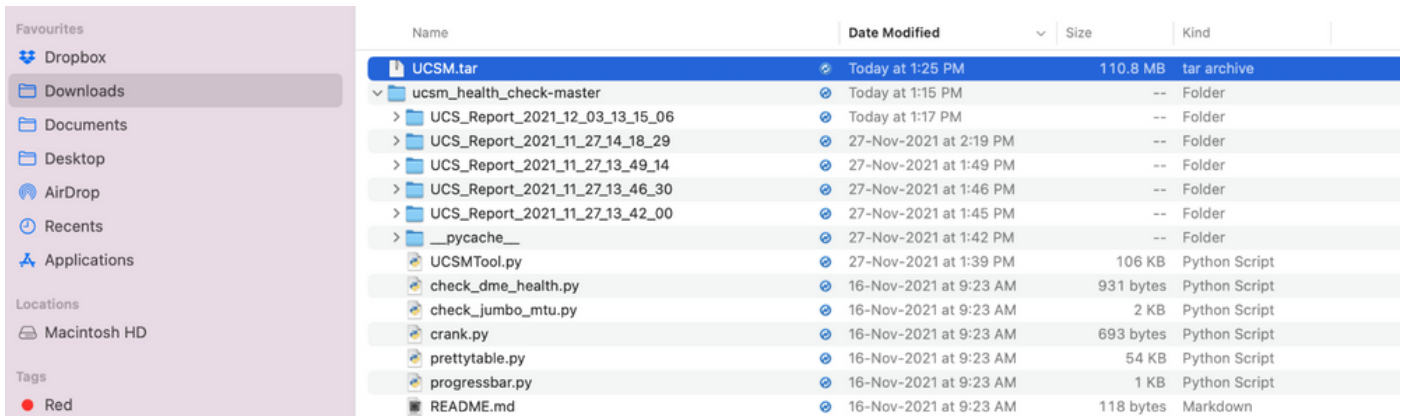
ステップ 2 : <https://www.python.org/downloads/macos/>から最新バージョンのPythonをダウンロードします。

ステップ 3 : 通常のインストールプロセスを使用して、Pythonのインストールを完了またはアップグレードします。

ステップ 4 : [ここ](#)からヘルスチェックスクリプトの最新バージョンをダウンロードし、フォルダに保存します。次の図に示すように、圧縮ファイルを抽出します。



ステップ 5：次の図に示すように、最新のUCSMテクニカルサポートログをダウンロードし、作成したフォルダに保存します。リンクをクリックして、UCSMログバンドルをダウンロードする手順を確認してください。[UCSMテクニカルサポートの生成。](#)



手順 6：端末を開き、ヘルスチェックスクリプトをダウンロードしたディレクトリを参照し、次に示すようにpython UCSMTool.pyまたはpython3UCSMTool.pyを実行します。

```
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
```

手順 7：UCSMテクニカルサポートファイルがあるファイルパスを入力し、スクリプトを実行する目的のオプションを選択します。

1. UCSMヘルスチェック
2. アップグレード前の確認

```
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
```

実行される出力/チェックについて

UCSM HealthCheckによって実行されるチェック

次のチェックは、UCSM-Healthchecktoolで実行されます。

UCSM HAクラスタ State : ファブリックインターコネクットのクラスタ状態を表示します。

PMONプロセス State : Cisco UCS Managerのすべてのプロセスの状態を表示します。

ファイル・システムのマウント : マウント・テーブルを表示します。

/var/ sysmgr sizeの問題を確認します。 /var/ sysmgrの使用状況を確認します。

/var/tmpのサイズの問題を確認します:/var/ tmpが使用されているかどうかを確認します。

6296 FI unresponsive after a power cycle, HW revision update:ファブリックインターコネクットモジュールとそのハードウェアリビジョン番号を確認します。

Faults with Severity Major or Severity Critical:UCS Managerにメジャーまたはクリティカルアラートがあるかどうかを報告します。

Check Backup Available:UCS Managerでバックアップが使用可能かどうかを確認します。

キーリング証明書 オン: キーリングが期限切れであるか、または有効であるかを確認します。

Safeshut回避策が必要かどうか:FIモデルとそのバージョンを確認して、shafeshut回避策が必要かどうかを確認します。

Cisco UCS Managerリリース 4.xの非推奨ハードウェア:Cisco UCS Manager 4.xリリースの非推奨ハードウェアを確認します。

3.1.x以降で見つかった非推奨のハードウェア:Cisco UCS Manager 3.xリリースで非推奨のハードウェアがないかどうかを確認します。

空白のMRAID12Gフィールドが原因で発生するB200M4のリポートをチェックします。B200M4サーバのMRAID12G RAIDコントローラのS/Nが空白かどうかをチェックします。

UCSM 3.1最大電力割り当ての変更により、ブレード検出が失敗する：UCS Managerで設定された電力ポリシーを確認する。

ブートフラッシュ破損の存在の障害コードF1219:ブートフラッシュ破損の存在を確認します。

デフォルトのキーリングが削除されたときにhttpdが起動に失敗するかどうかを確認します：デフォルトのキーリングが削除されているかどうかを確認します。

第3世代FIのファイルシステム状態がクリーンでない - 「ファイルシステムの状態：エラーでクリーン」：ファイルシステムエラーを確認します。

4.0(4b)へのサーバの自動インストールがSASコントローラのアクティブ化に失敗するか確認する:ホストファームウェアのバージョンとSASエクスパンダのバージョンを確認します

Cシリーズファームウェアのアップグレードの確認が「サーバのインベントリの実行」で長時間続くPNU OSインベントリ:サーバモデルとそのバージョンを確認して、この問題が発生しているかどうかを特定します。

ピリオドまたはハイフンを使用するUCSM認証ドメインの確認:認証ドメイン名にピリオドまたはハイフンが設定されているかどうかを確認します。

ローカルまたはフォールバック認証の失敗:特定のFIモデルに対して設定されている認証方式を確認し、そのバージョンも確認します。

UCSMとUCS Central間のヘルスチェック:UCSManagerがUCS Centralに登録されているかどうかを確認します。

LANおよびSANピングループ：クラスタ内のLAN/SANピン接続の設定を確認し、アップグレードまたはMWアクティビティの前に設定を確認するために強調表示します。

UCSMに存在する保留中のアクティビティの確認：UCS Managerドメインに保留中のアクティビティがあるかどうかを確認します。

IOMのヘルスチェック:IOMジュール全体の健全性をチェックします。

UCSMで使用可能なコアファイルの確認：コアファイルが60日以内に見つかるかどうかを確認します。

分離L2の設定ミスの可能性：分離L2が設定されている場合に、設定ミスがないかどうかを確認します。

VIC 1400および6400のリンクフラップの問題：この不具合に存在する状態を確認します

ファームウェアのアップデート中に2304 IOMが切断して再接続することを確認します。ファブリックインターコネクトとIOMジュールのモデルを確認し、潜在的な問題があるかどうかを特定します。

DMEヘルスチェック : Data Management Engine(DME)データベースの健全性を確認します。

FI上のインターフェイスの起動およびFlogiマッチングの数 : インターフェイスの数とflogiのセッションを確認します。

ジャンボまたは標準MTUの確認 : MTUの設定を確認します。

サンプルUCSMツールの出力番号

```
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.

ツール出力の分析 – 次のステップ

- このツールは、UCSシステムで手動コマンドを実行するプロセスを自動化します。
- ツールが実行される場合 OK また次のメリットがあります 合格/見つかりません すべてのテストに適用されますUCSシステムは、スクリプトが実行したすべてのチェックに適しています。
- このツールが FAIL/見つかりません 一部のチェックが正常に実行されない場合は、CLIコマンド (ここにリストされています) を使用して、スクリプト「Manually」で実行される UCSシステム/ファブリックインターコネクト上の同じチェックを実行できます。
- このツールでは、古い、新しい、オープンな、または解決された注意事項はチェックされません。そのため、アップグレードまたはメンテナンスを行う前に、UCSリリースノートとアップグレードガイドを確認することを強くお勧めします。

 ヒント:UCS環境の一般的なヘルスチェックのために、Cisco TACはこのサービスを提供しません。シスコのCX Customer Delivery Team (旧称Advanced Services) には、バグスクラブリスク分析が用意されています。このタイプのサービスが必要な場合は、営業/アカウントチームにお問い合わせください。

CLI コマンド

両方のファブリックインターコネクトへの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.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。