运行UCSM运行状况和升级前检查工具

目录

简介

本文档介绍运行统一计算系统管理器(UCSM)运行状况和升级前检查工具的过程。

先决条件

要求

思科建议您在系统上安装Python 3.6或更高版本。

注意：如果您正在运行Windows操作系统，则可以安装Python并配置环境路径。

注意：请勿为Python问题/无法运行的脚本打开TAC支持请求。请参阅CLI命令部分以手动识别问题并根据识别的问题打开TAC支持请求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

UCSM检查工具是一个实用程序，用于对UCSM执行主动自检，以确保其稳定性和恢复能力。它可帮助自动执行UCS系统的运行状况和升级前检查列表，以在UCS基础设施升级和维护操作发生时节省时间。

注意：请始终下载并使用工具的最新版本。由于该工具经常增强，因此当您使用较旧版本时，它可能会遗漏重要的检查。

注意：此脚本是尽最大努力、免费使用的脚本。但是，它无法识别所有问题。

适用场合

- 在UCS基础设施升级之前
- 维护活动前后的UCS运行状况检查
- 当您与Cisco TAC合作时
- 随时主动进行运行状况检查

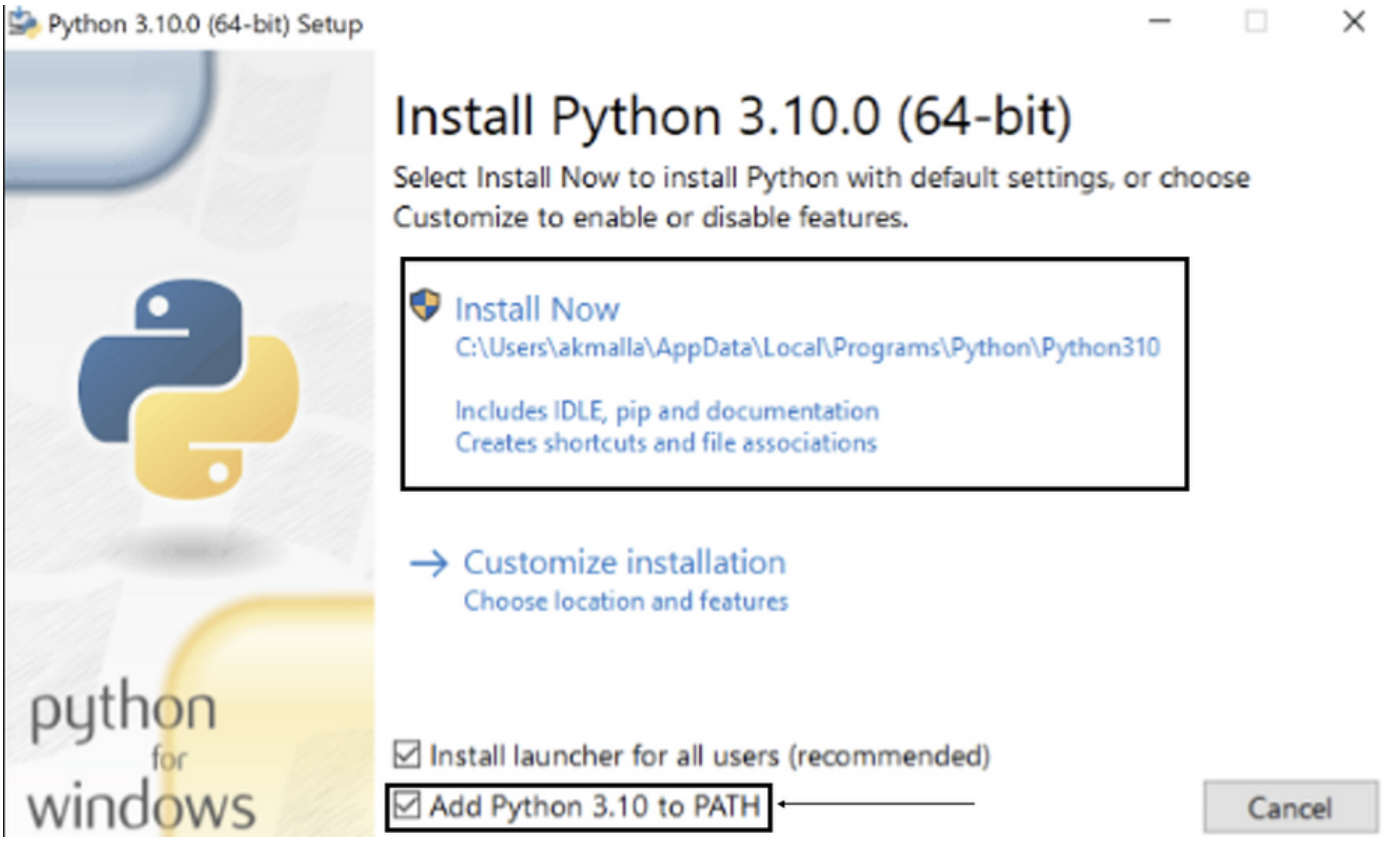
操作方法

Windows操作系统

步骤1:从Python下载下载最新版本的Python

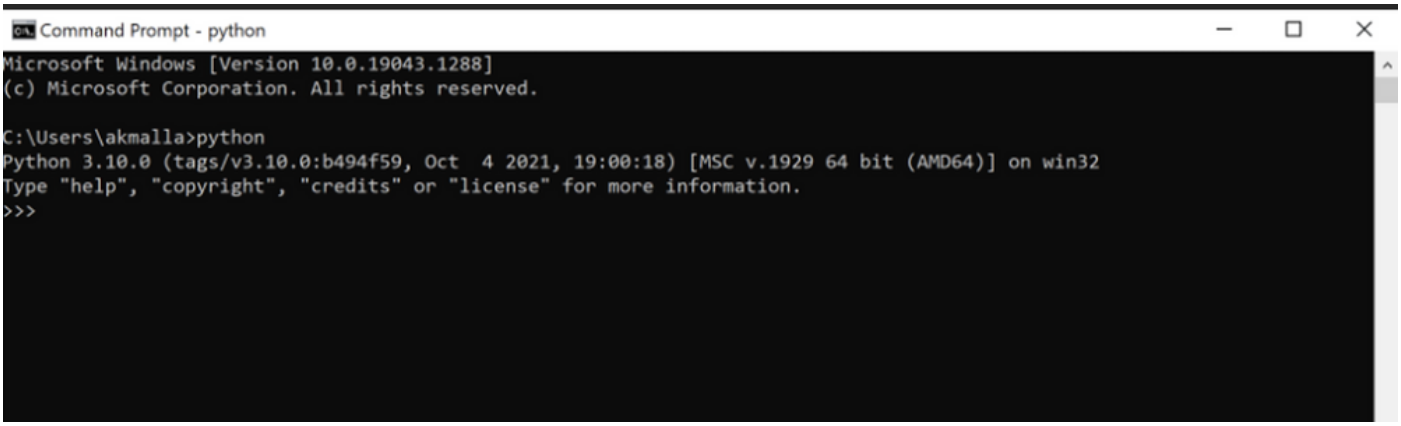
第二步：使用正常的安装过程并单击Install Now（推荐的安装程序）下载安装程序。

注意：确保选中Add Python to PATH。

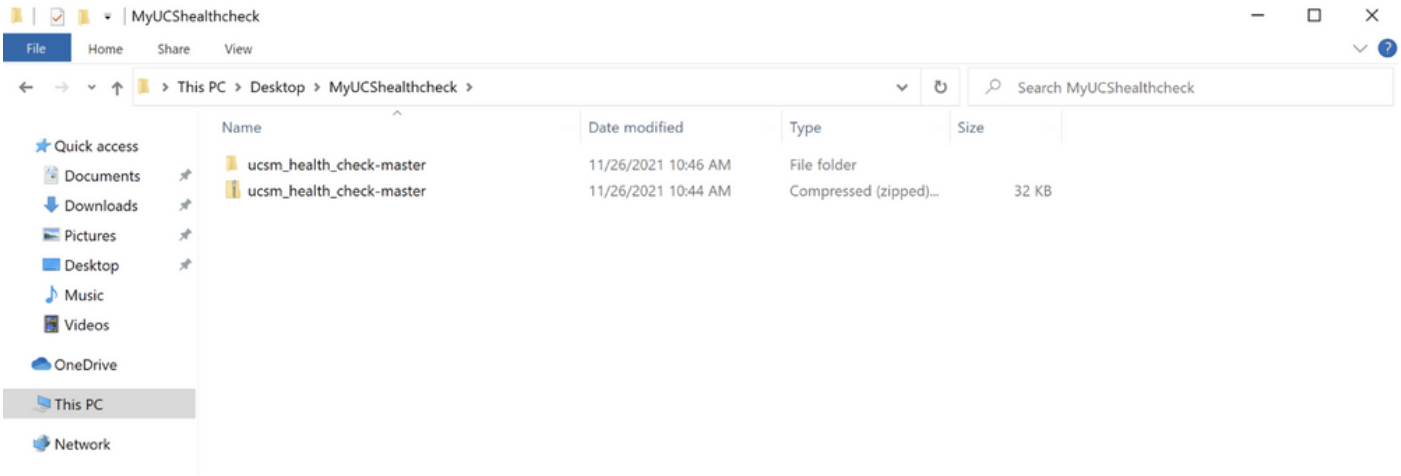


第三步：导航到系统上安装Python的目录。

第四步：打开命令提示符并键入命令Python以验证Python安装。

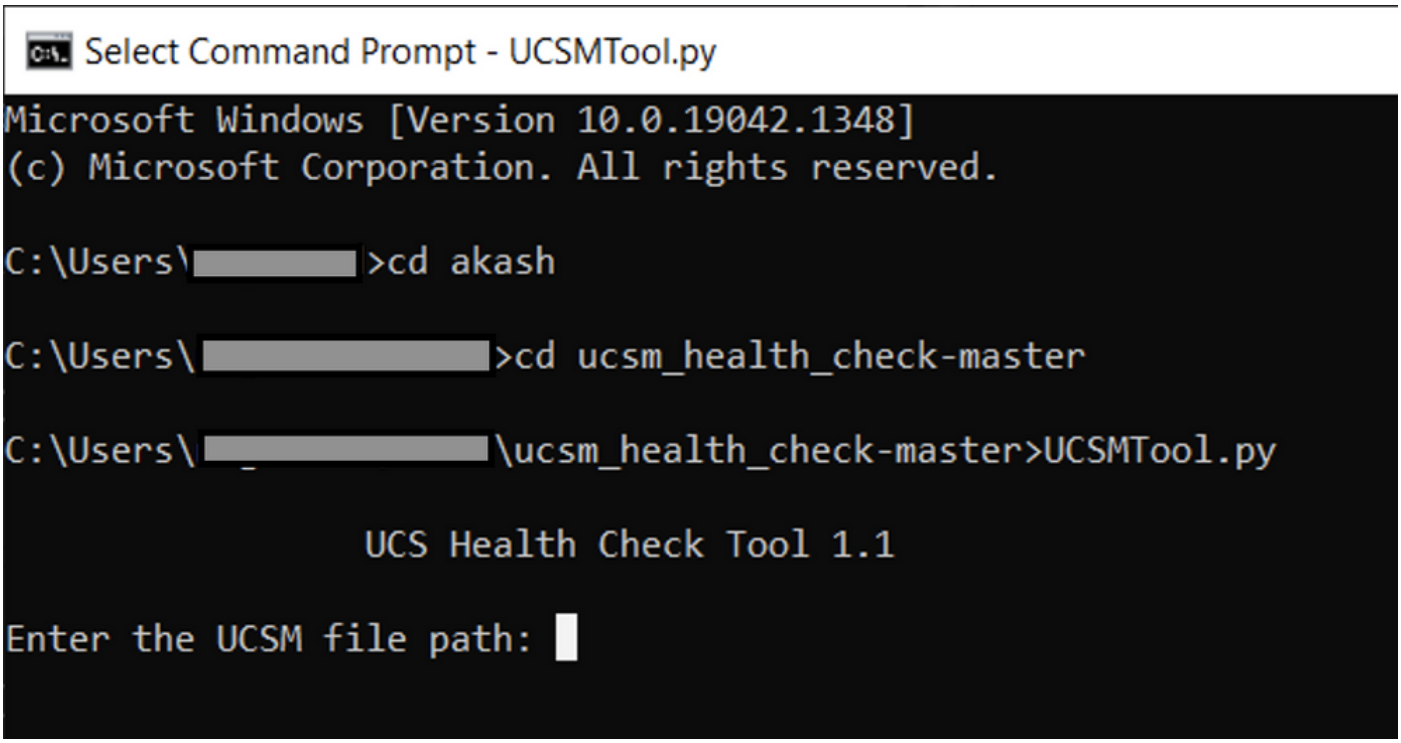


第五步：从此处下载最新版本的运行状况检查脚本，并将其保存到文件夹。现在，提取压缩文件，如图所示。



第六步：下载并保存最新的UCSM技术支持日志到创建的文件夹，如图所示。点击此链接可查找下载UCSM日志捆绑包的步骤：[生成UCSM技术支持。]

步骤 7.打开CMD和cd并转到UCSMTool.py所在的文件夹，然后运行UCSMTool.py（如图所示）。



步骤 8输入UCSM技术支持文件所在的文件路径，然后选择desired 选项。

1. UCSM运行状况检查

2. 升级前检查

```
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

步骤1:MacOS随附已安装默认Python，请验证已安装的Python版本，如下所示：

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

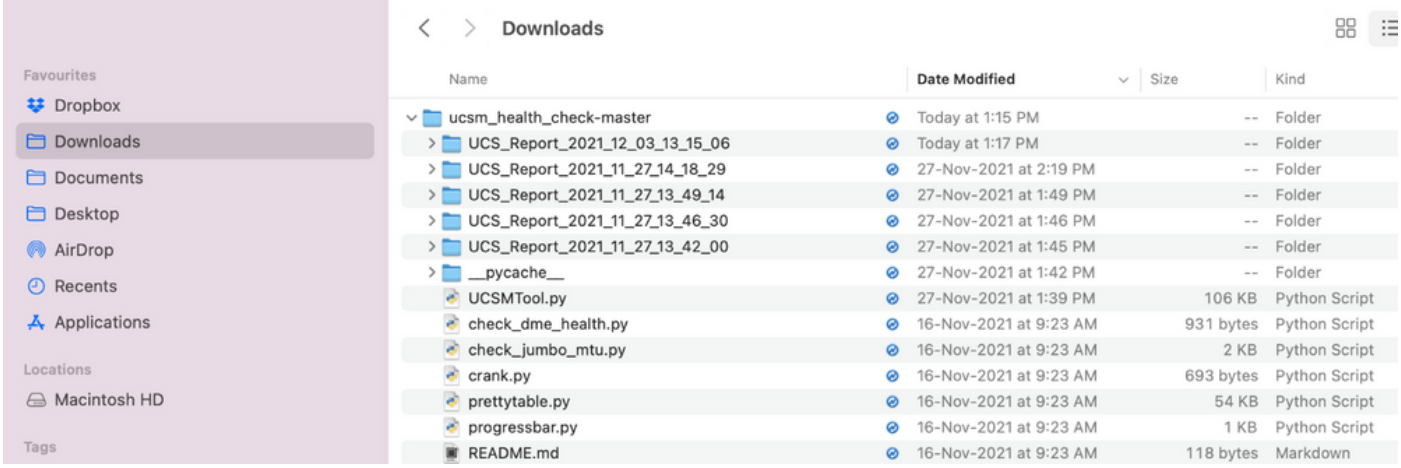
注意：如果Python版本低于3.6，请升级到3.6及更高版本。

注意：如果Python版本是3.6或更高版本，请跳到第5步，否则跳到第2步。

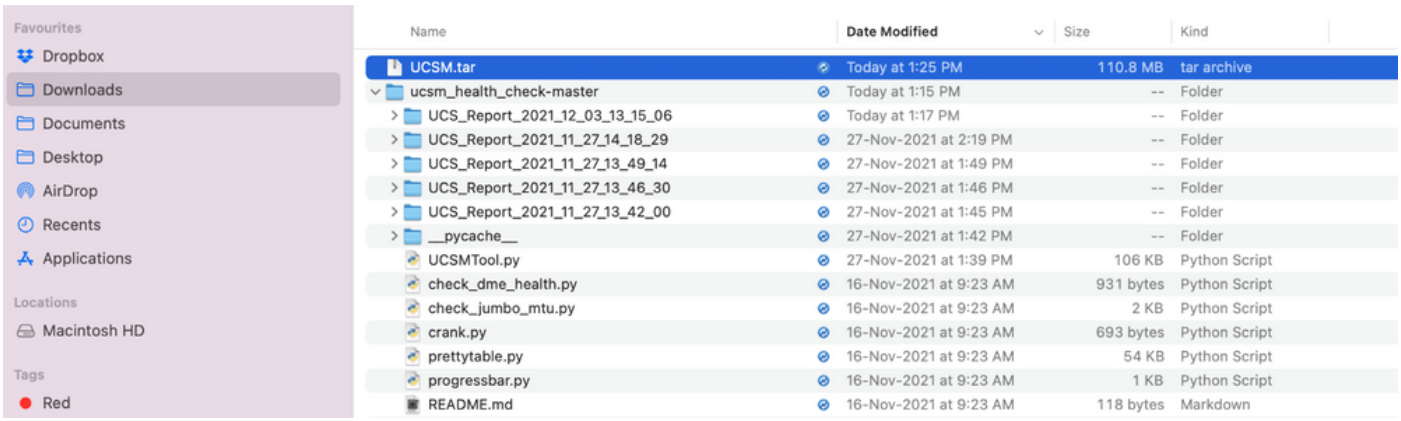
第二步：从https://www.python.org/downloads/macos/下载最新版本的Python。

第三步：使用正常安装过程完成/升级Python安装。

第四步：从此处下载运行状况检查脚本的最新版本并保存到文件夹。现在，提取压缩文件，如下图所示：



第五步：下载并保存最新的UCSM技术支持日志到创建的文件夹，如此图中所示。点击链接以查找下载UCSM日志捆绑包的步骤：[生成UCSM技术支持。]



第六步：打开终端，浏览到已下载运行状况检查脚本的目录，运行python UCSMTool.py或python3UCSMTool.py，如下所示：

```
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
```

步骤 7.输入UCSM技术支持文件所在的文件路径，然后选择desired option运行脚本。

1. UCSM运行状况检查

2. 升级前检查

```
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
```

了解执行的输出/检查

由UCSM运行状况检查执行的检查

这些检查由UCSM-Healthchecktool执行：

UCSM HA集群状态：显示交换矩阵互联的集群状态。

PMON进程状态：显示Cisco UCS Manager中所有进程的状态。

文件系统装载：显示装载表。

检查/var/sysmgr大小问题：检查/var/sysmgr使用情况。

检查/var/tmp大小问题：检查/var/ tmp使用情况。

6296 在重新通电后无响应，硬件修订版更新：验证交换矩阵互联模块及其硬件修订版号。

严重程度为严重程度为严重程度为严重程度为严重程度的故障：如果UCS Manager中有任何严重或严重程度为严重程度的警报，则进行报告。

选中Backup Available：验证UCS Manager中是否有备份。

密钥环证书检查：检查密钥环是否过期或有效。

Safeshut解决方法是否需要或不需要：通过验证FI模型及其版本来检查是否需要或不需要shafeshut解决方法。

Cisco UCS Manager版本4.x中已弃用的硬件：检查Cisco UCS Manager 4.x版本中是否有已弃用的硬件。

发现用于3.1.x及后续版本的已弃用硬件：在Cisco UCS Manager 3.x版本中检查是否有任何已弃用的硬件

检查B200M4是否由于空白MRAID12G字段而重新启动：检查B200M4服务器是否具有空白MRAID12G RAID控制器序列号。

UCSM 3.1最大功率分配更改会导致刀片发现故障：验证UCS Manager中配置的电源策略。

bootflash损坏故障代码F1219存在：检查bootflash损坏是否存在。

检查httpd在删除默认密钥环时是否无法启动：检查是否删除了默认密钥环。

第3代FI具有不干净的文件系统状态-“文件系统状态：清理出错”：检查文件系统错误。

检查4.0(4b)服务器自动安装是否无法激活SAS控制器：验证主机固件版本和SAS扩展器版本

检查C系列固件升级是否持续很长时间“执行服务器资产”PNU操作系统资产：它会验证服务器型号及其版本，以确定您是否遇到此问题。

检查使用句点或连字符的UCSM身份验证域：验证是否使用句点或连字符配置身份验证域名。

本地或回退身份验证失败：检查为特定FI型号配置的身份验证方法，并验证其版本。

UCSM和UCS中心之间的运行状况检查：验证UCSManager是否已在UCS中心注册

LAN和SAN引脚组：检查集群中的lan/san pinning配置，突出显示以在升级前/任何MW活动之前检查配置

检查UCSM中存在的挂起活动：验证UCS Manager域中是否存在任何挂起活动。

IOM运行状况检查：检查IO模块的整体运行状况。

UCSM中可用的核心文件检查：验证在60天内是否找到了任何核心文件。

分离L2潜在配置错误：在配置分离L2的情况下，验证是否存在任何配置错误。

VIC 1400和6400链路抖动问题：检查是否存在此缺陷的情况

在固件更新期间检查2304 IOM断开连接并重新连接：验证交换矩阵互联和IO模块型号并确定是否存在任何潜在问题。

DME运行状况检查：验证数据管理引擎(DME)数据库的运行状况。

FI上接口启用和Flogi匹配的数量：验证接口和Flogi会话的数量

超巨型或标准MTU检查：确定MTU配置。

UCSM工具输出编号示例

```
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 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  | Not Found  |
|      | step                                                              |            |
+------+-------------------------------------------------------------------+------------+--------------
| 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.
```

分析工具输出-后续步骤

- 该工具自动执行在UCS系统上运行手动命令的流程。
- 如果工具运行OK并在所有测试中显示PASS/NOT FOUND。UCS系统适用于脚本执行的所有

检查。
- 如果工具FAIL/FOUND 执行某些检查或未成功运行，则可以使用CLI命令（此处列出）对UCS系统/交换矩阵互联执行与脚本中手动执行的检查相同的检查。
- 此工具不检查任何旧/新/开放/解决的警告，因此强烈建议您在升级或维护活动之前查看UCS发行版本注释和升级指南。


提示：要对UCS环境执行常规运行状况检查，思科TAC不提供此服务。思科的CX客户交付团队（以前称为“高级服务”）提供漏洞清除/风险分析。如果您需要此类服务，请与您的销售/客户团队联系。

CLI命令

到两个交换矩阵互联的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.
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。