Executar a ferramenta de verificação de integridade e pré-atualização do UCSM

Contents

Introduction

Este documento descreve o processo para executar a ferramenta de verificação de integridade e pré-atualização do Unified Computing System Manager (UCSM).

Prerequisites

Requirements

A Cisco recomenda que você tenha o Python 3.6 ou posterior instalado no sistema.

> **Observação**: se você estiver executando o sistema operacional Windows, poderá ter o Python instalado e configurado o caminho Ambiente.

> **Observação**: não abra um caso TAC para problemas Python/Falha na execução do script. Consulte a seção de comandos CLI para identificar manualmente o problema e abrir o caso do TAC por problema identificado

---

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Ferramenta de Verificação UCSM é um utilitário para executar autoverificações proativas no UCSM para garantir sua estabilidade e resiliência. Ele ajuda a automatizar uma lista de verificações de integridade e pré-atualização em sistemas UCS para economizar tempo quando as operações de atualização e manutenção da infraestrutura do UCS ocorrem.

> **Observação**: sempre baixe e use a versão mais recente da ferramenta. Como a ferramenta é aprimorada com frequência, quando você usa uma versão mais antiga, ela pode perder verificações importantes.

> **Observação**: este script é um melhor esforço, gratuito e não pode identificar todos os problemas possíveis.

Quando usar

- Antes das atualizações de infraestrutura do UCS
- Verificação de integridade do UCS antes e depois da atividade de manutenção
- Quando você trabalha com o Cisco TAC
- Verificação de integridade proativa a qualquer momento

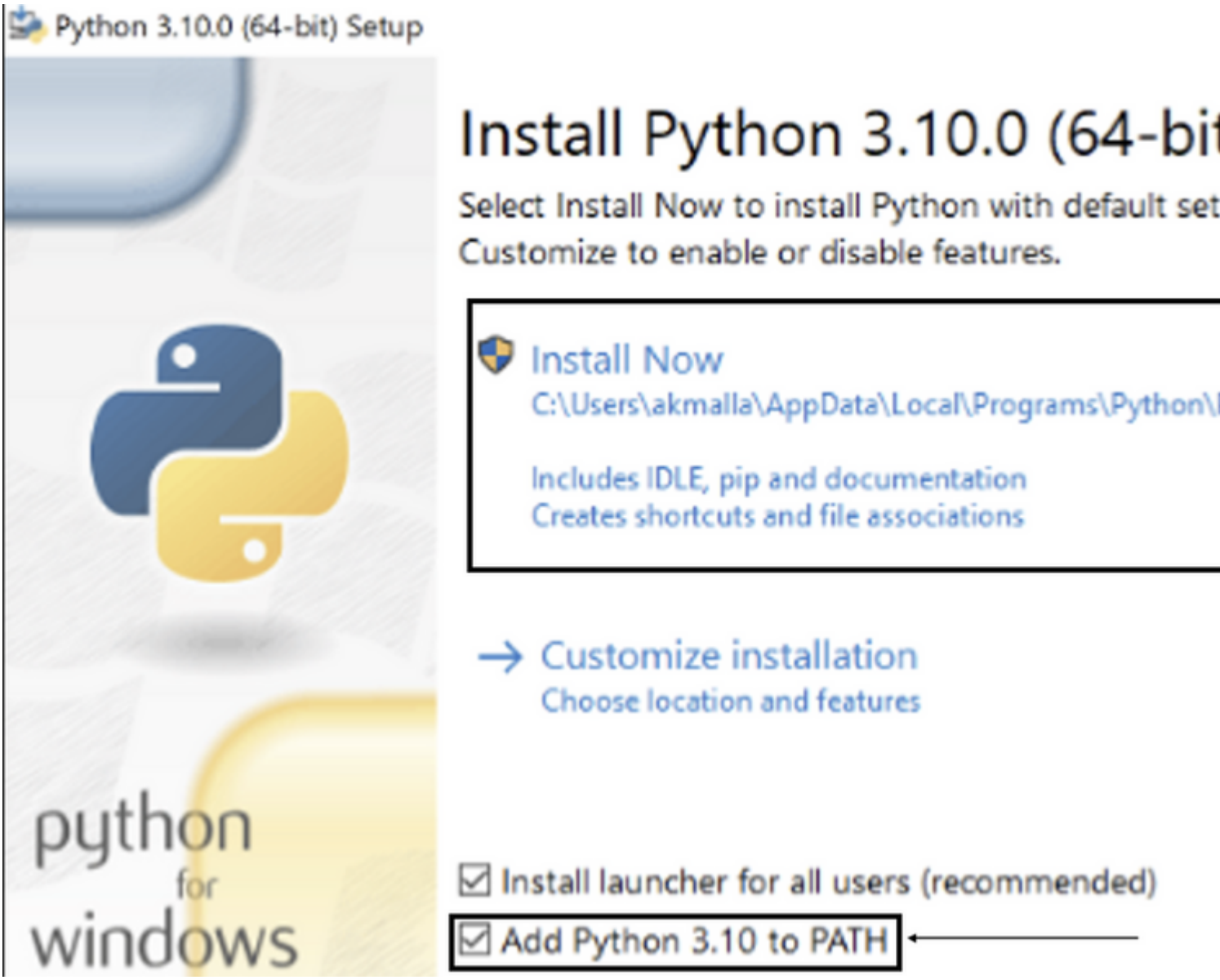
How to Use

SO Windows

Etapa 1. Baixe a versão mais recente do Python em Downloads Python

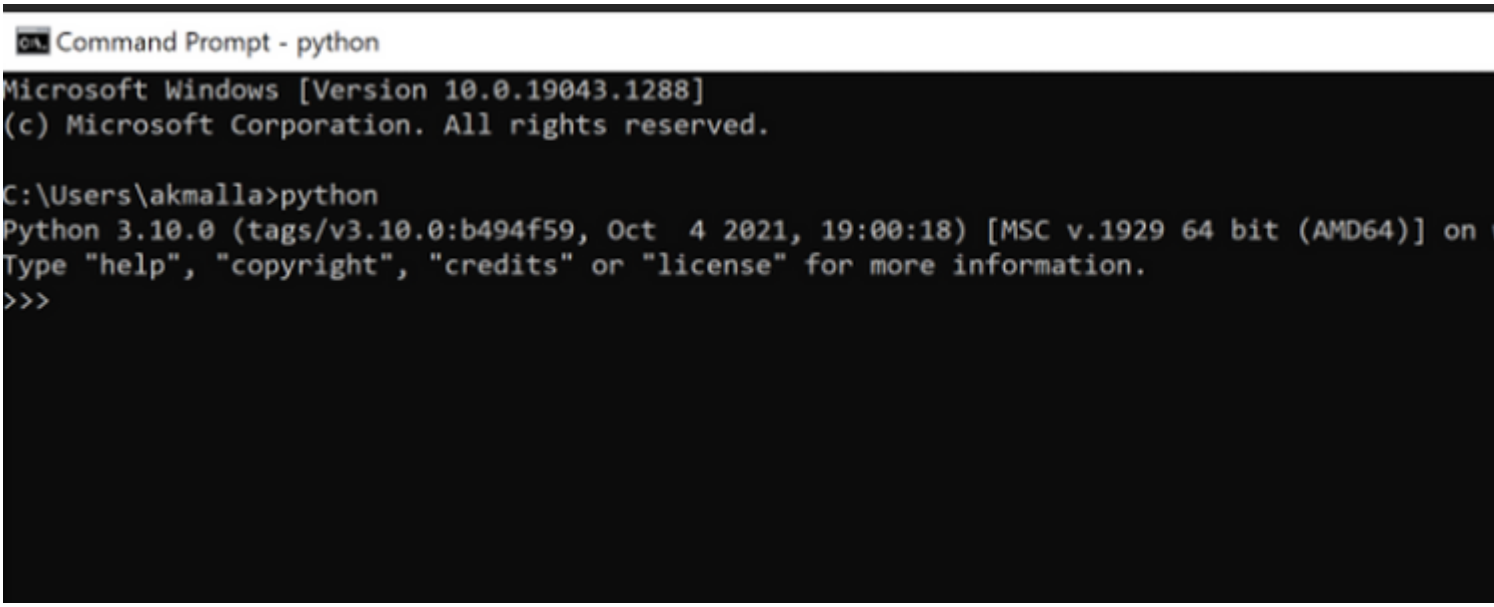
Etapa 2. Use o processo de instalação normal e clique em **Instalar agora** (o recomendado) para baixar a configuração.

> **Observação**: certifique-se de marcar **Add Python to PATH**.

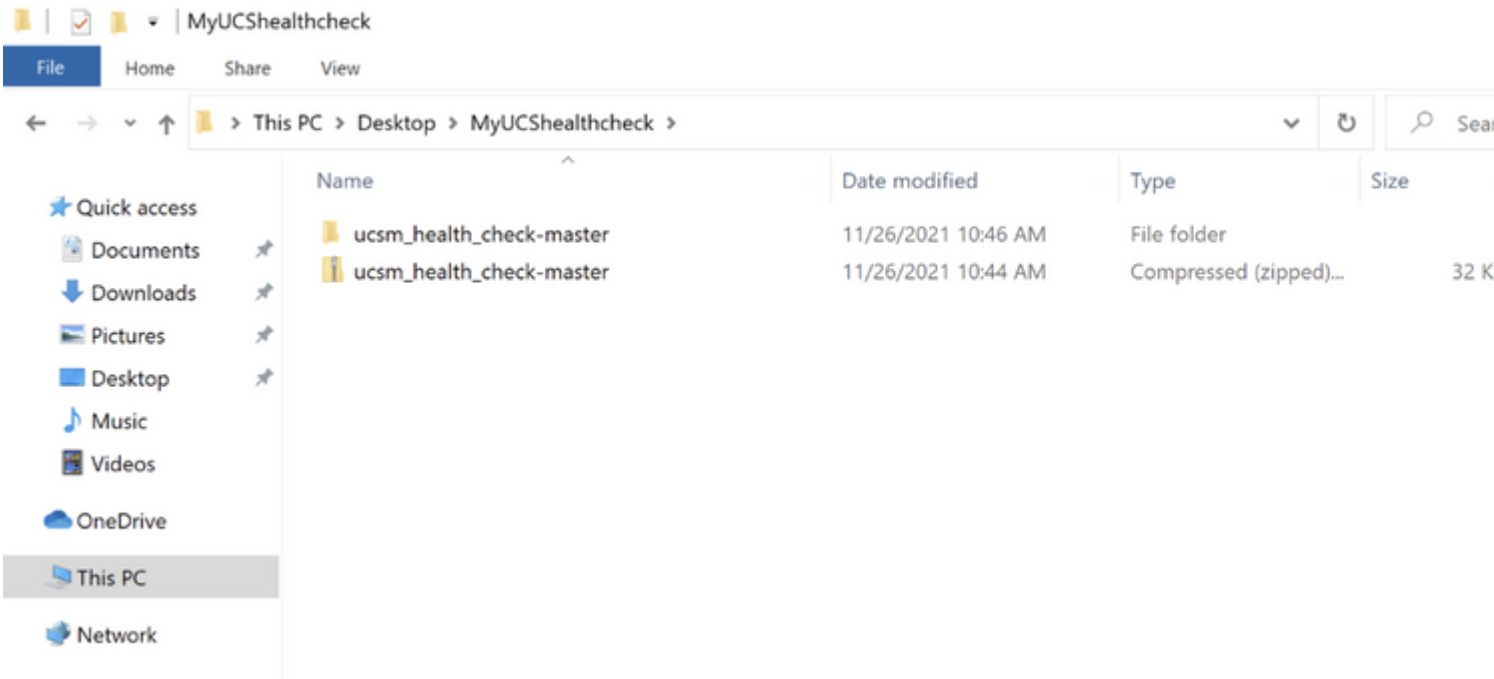


Etapa 3. Navegue até o diretório em que o Python foi instalado no sistema.

Etapa 4. Abra o prompt de comando e digite o comando **Python** para verificar a instalação do python.

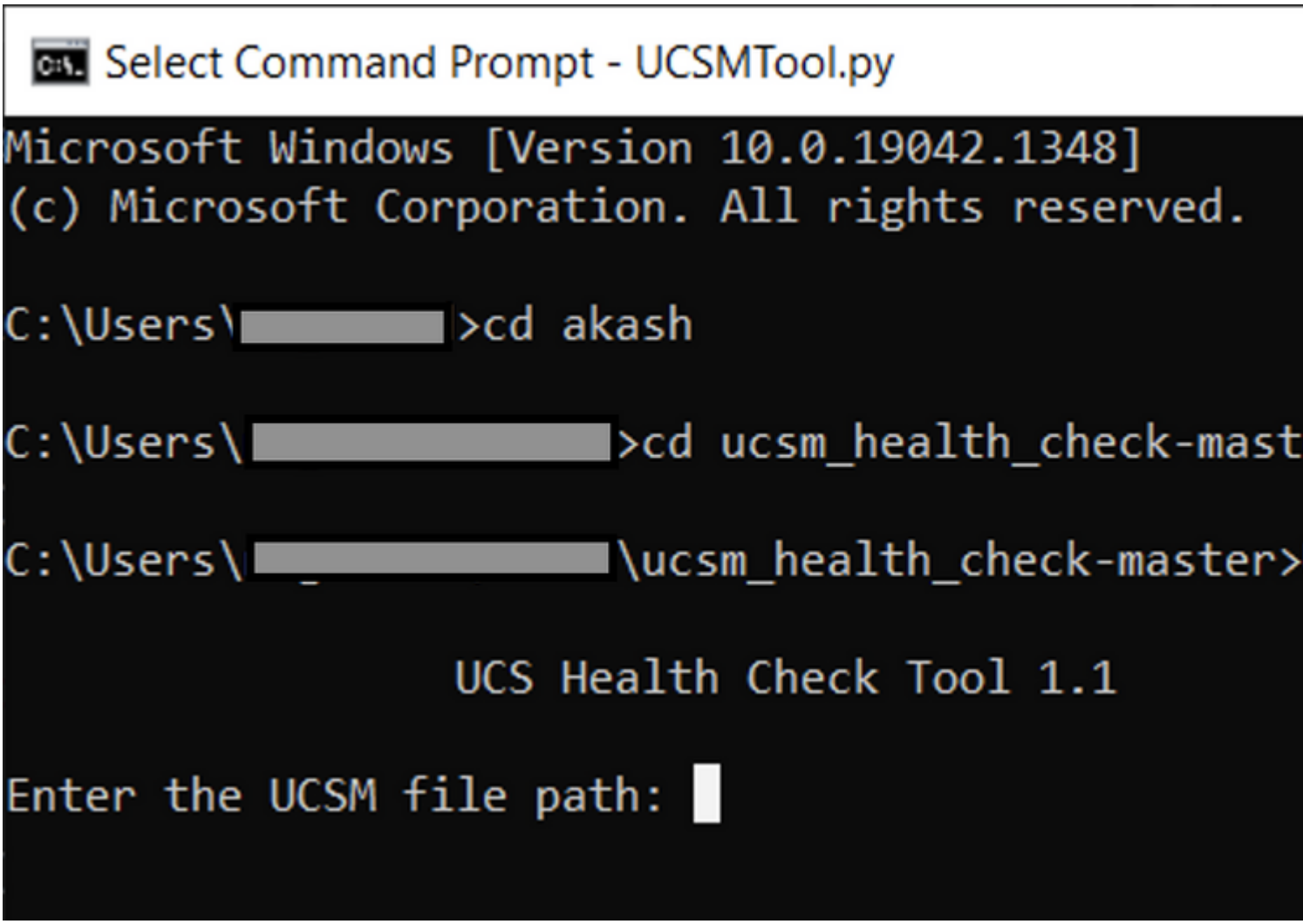


Etapa 5. Faça o download da versão mais recente do script de verificação de integridade aqui e salve-o em uma pasta. Agora, extraia o arquivo compactado, como mostrado na imagem.



Etapa 6. **Baixe** e **salve** os logs de suporte técnico do UCSM mais recentes na pasta criada, como mostrado na imagem. Clique neste link para encontrar as etapas de download do pacote de log do UCSM; Geração de suporte técnico do UCSM.

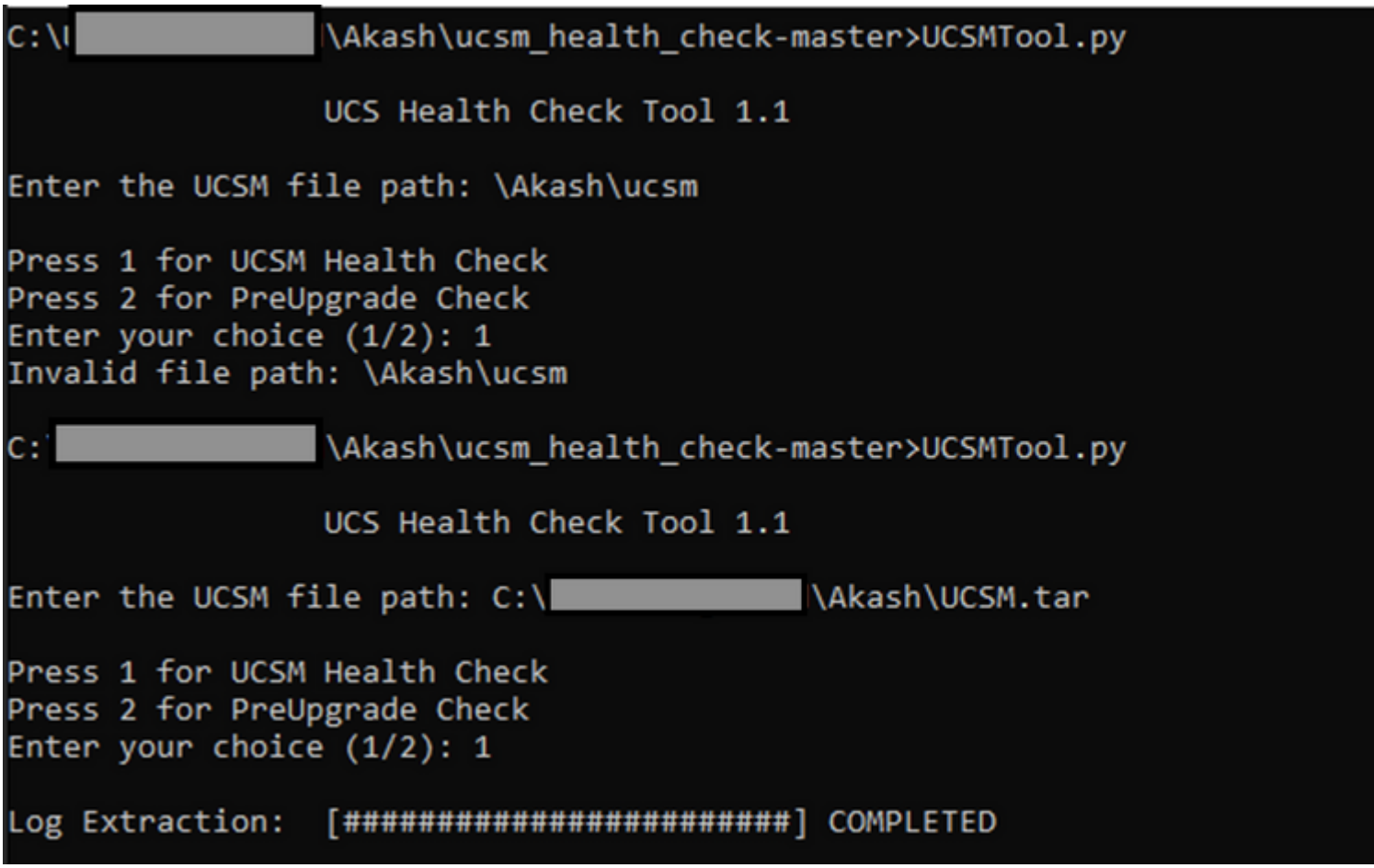
Passo 7. Abra o CMD e o cd na pasta onde está localizado o UCSMTool.py e execute o **UCSMTool.py** como mostrado na imagem.



Etapa 8. Insira o caminho do arquivo onde o arquivo de suporte técnico do UCSM está localizado e escolha a **opção desejada**.

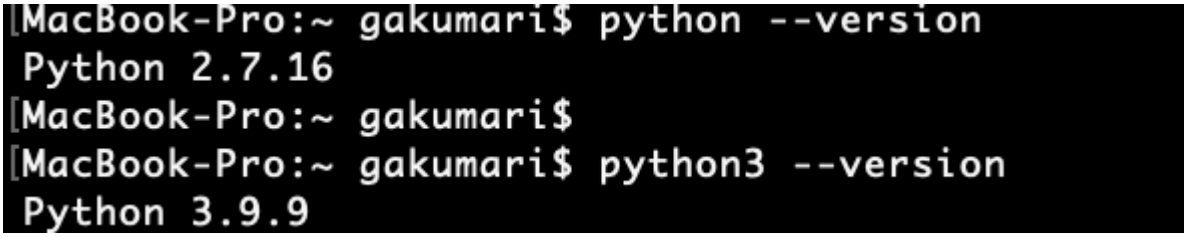
1. Verificação de integridade do UCSM

2. Verificação de Pré-Atualização



MacOS

Etapa 1. O MacOS vem com o python padrão instalado, verifique a versão do python instalada como mostrado aqui:



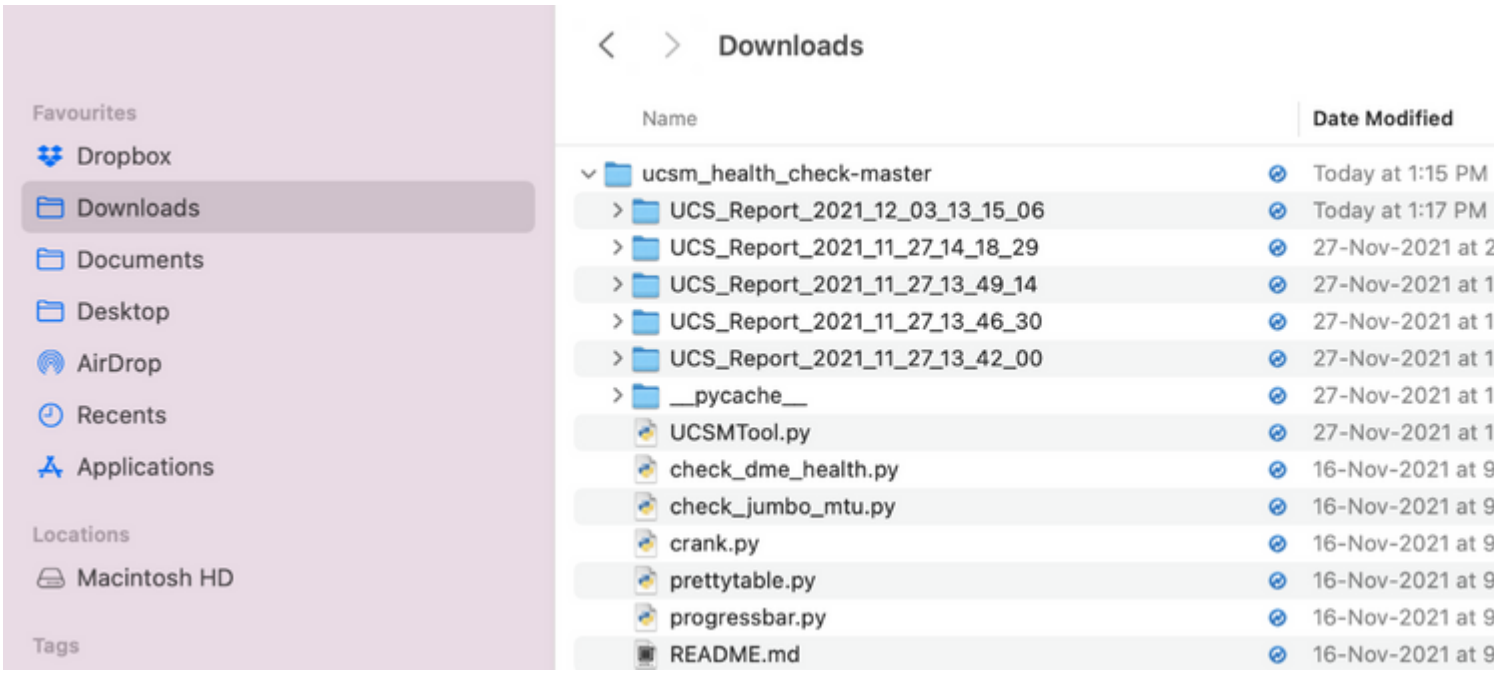
Observação: caso a versão do python seja inferior à 3.6, atualize para a 3.6 e versões posteriores.

Observação: se a versão python for 3.6 ou posterior, vá para a Etapa 5; caso contrário, vá para a Etapa 2.

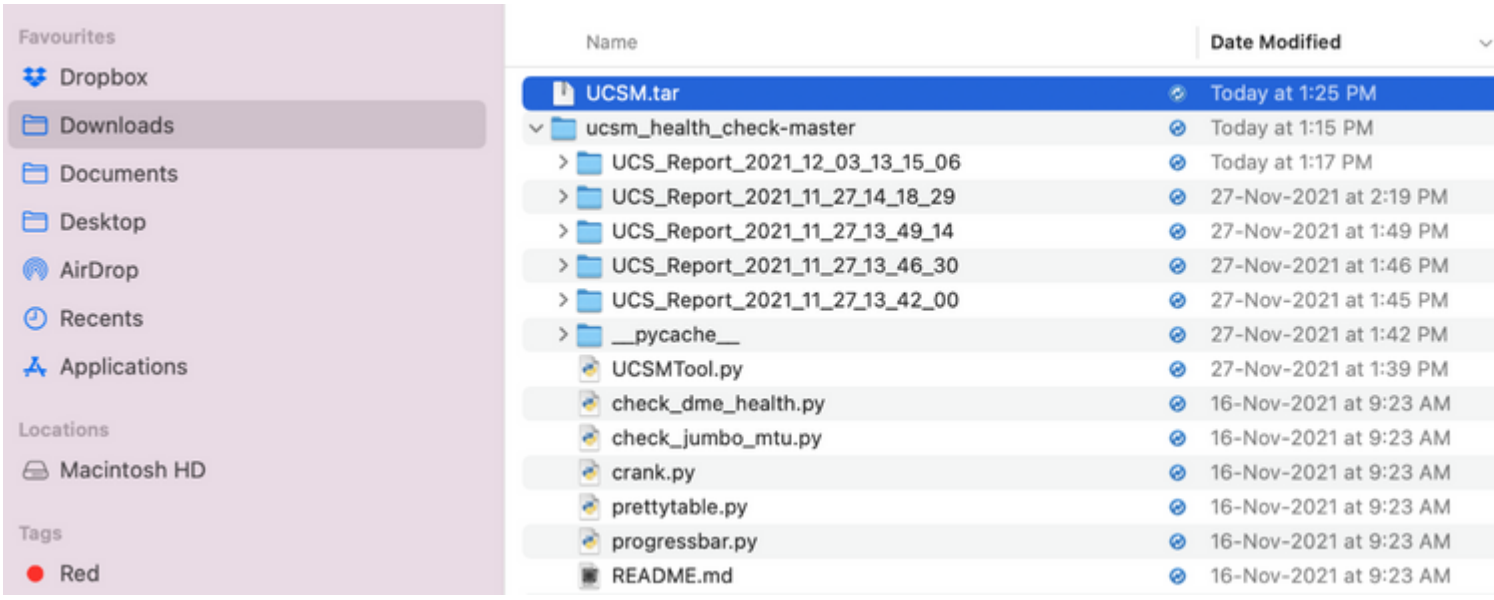
Etapa 2. Faça o download da versão mais recente do Python em https://www.python.org/downloads/macos/.

Etapa 3. Use o processo de instalação normal para concluir/atualizar a instalação do Python.

Etapa 4. **Baixe** a versão mais recente do script de verificação de integridade aqui e **salve**-o em uma pasta. Agora, extraia o arquivo compactado, como mostrado nesta imagem.



Etapa 5. **Baixe** e **salve** os logs de suporte técnico do UCSM mais recentes na pasta criada, como mostrado nesta imagem. Clique no link para encontrar as etapas de download do pacote de log do UCSM; [Geração de suporte técnico do UCSM.]



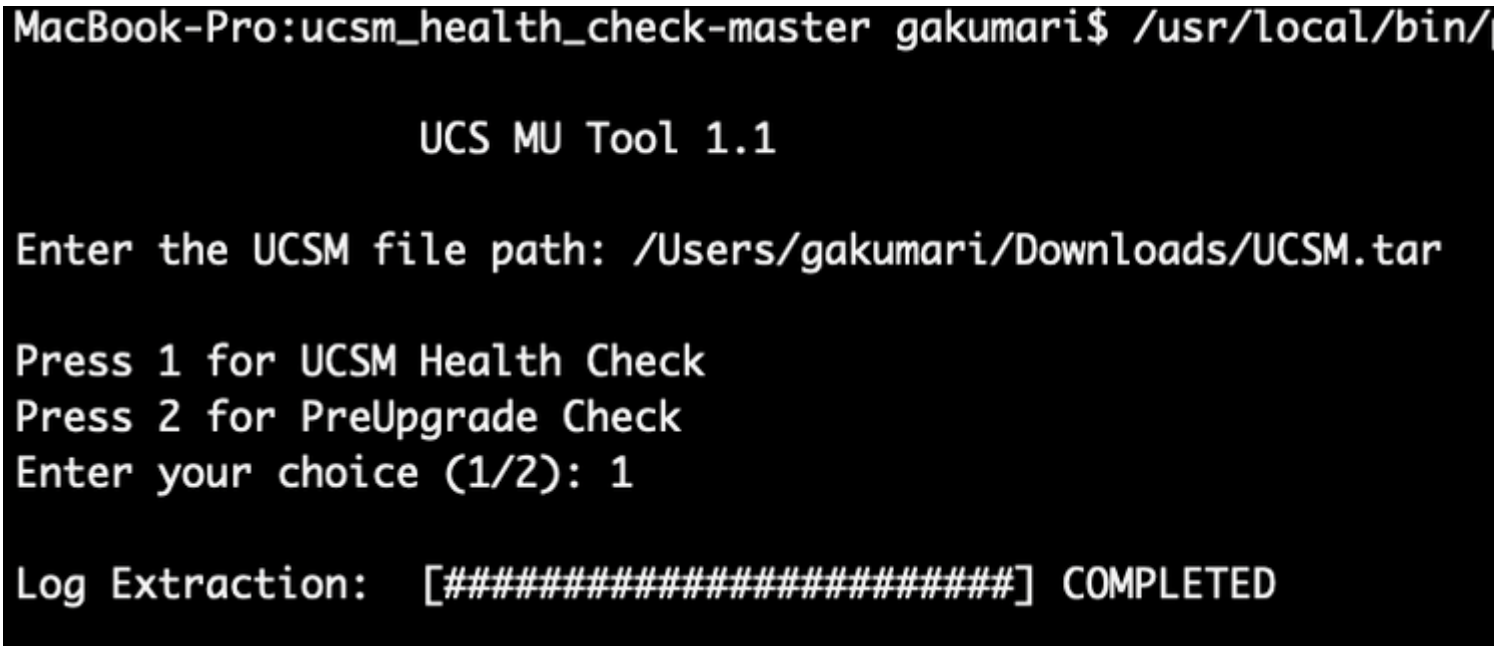
Etapa 6. Abra o terminal, navegue até o diretório onde você fez o download do script de verificação de integridade, execute **python UCSMTool.py** ou **python3UCSMTool.py** como mostrado aqui.

```
[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
```

Passo 7. Insira o caminho do arquivo onde o arquivo de suporte técnico do UCSM está localizado e escolha a **opção desejada** para executar o script.

1. Verificação de integridade do UCSM

2. Verificação de pré-atualização



Entender Saídas/Verificações Executadas

Verificações Executadas pela Verificação de Integridade do UCSM

Essas verificações são realizadas por UCSM-Healthchecktool:

Cluster UCSM HA Estado: Exibe o estado do cluster das interconexões em malha.

Processo PMON Estado: Exibe o estado de todos os processos no Cisco UCS Manager.

Montagem do Sistema de Arquivos: Exibe a tabela de montagem.

Verifique o problema /var/ sysmgr size: Verifica os usos de **/var/ sysmgr.**

Verifique o problema /var/ tmp size: Verifica se **/var/** tmp **usa.**

6296 FI sem resposta após um ciclo de energia, atualização de revisão de HW: Verificar o módulo de interconexão de estrutura e seu número de revisão de HW.

Falhas com severidade maior ou severidade crítica: relata se você tiver algum alerta grave ou crítico no UCS Manager.

Verificar backup disponível: verifique se o backup está disponível no UCS Manager.

Certificado do porta-chaves Verificar: Verifique se o chaveiro expirou ou é válido.

Safeshut Workaround Needed or Not: Verifique se a solução alternativa do shafeshut é necessária ou não, verificando o modelo FI e sua versão.

Hardware preterido no Cisco UCS Manager Release **4.x: Verifique se há qualquer Hardware preterido no Cisco UCS Manager Release 4.x.**

HW preterido encontrado para 3.1.x **em diante: Verifique se há hardware preterido na versão do Cisco UCS Manager 3.x**

Verifique a reinicialização do B200M4 devido a campos em branco de MRAID12G: verifique se o servidor B200M4 tem um S/N em branco da controladora RAID MRAID12G.

Alteração do UCSM 3.1 na alocação máxima de energia causa falha na descoberta de blade: Verifica a política de energia configurada no UCS Manager.

Existência do código de falha de corrupção do flash de inicialização F1219: Verifique a existência de corrupção do flash de inicialização.

Check for httpd fail to start when the default keyring is deleted: Verifique se o keyring padrão foi excluído.

Os FIs de 3ª GERAÇÃO têm estados de sistema de arquivos não limpos-"Estado do sistema de arquivos: limpar com erros": verifique se há erros no sistema de arquivos.

Verifique se Server AutoInstall to 4.0(4b) Fails to Ativate **SAS Controller: Verifique a versão do firmware do host e a versão do expansor de SAS**

Verifique se a atualização do firmware C-Series permanece longa no processo "executar um inventário do servidor" Inventário do SO PNU: Ele verifica o modelo do servidor e sua versão para identificar se você encontrou esse problema.

Verifique o domínio de autenticação UCSM que usa um ponto ou hífen: Verifique se o nome do domínio de autenticação está configurado com um ponto ou hífen.

Falha de autenticação local ou de fallback: verifique o método de autenticação configurado para um modelo de FI específico e também a sua versão.

Verificação de integridade entre UCSM e UCS central: Verifique se o UCSManager está registrado no UCS Central

Grupos de pinos de LAN e SAN: verifique a configuração de pinos de lan/san no cluster e destaque para revisar sua configuração antes da atualização/qualquer atividade de MW

Verificando atividades pendentes presentes no UCSM: verifique se há atividades pendentes no domínio do UCS Manager.

Verificação de integridade para IOM: verifique a integridade geral dos Módulos de E/S.

Arquivos principais disponíveis na **verificação UCSM:** verifique se algum arquivo principal foi encontrado dentro de 60 dias.

Configuração incorreta potencial de L2 disjunta: verifique se há alguma configuração incorreta caso a L2 disjunta esteja configurada.

Problema de Link Flap VIC 1400 e 6400: Verifique as condições presentes neste defeito

Verifique se os IOMs 2304 se desconectam e se reconectam durante a atualização do firmware: verifique o modelo de interconexão de estrutura e módulo de E/S e identifique se há algum problema em potencial.

Verificação de integridade do DME: verifique a integridade do banco de dados do Mecanismo de Gerenciamento de Dados (DME).

Número de Interface ativa e Correspondência de Flogi no FI: Verificar o número de interfaces e a sessão de flogi

Verificação de MTU Jumbo ou Padrão: identifique a configuração de MTU.

Número de Saída da Ferramenta UCSM de Exemplo

```
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 fau
+------+-------------------------------------------------------------------------+------------+---------------
| 8    | Check Backup Available                                                  | No Backup  | Please ensure
|      |                                                                         |            | Refer this lin
|      |                                                                         |            | http://go2.cis
+------+-------------------------------------------------------------------------+------------+---------------
| 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 rel
|      |                                                                         |            | Refer this lin
|      |                                                                         |            | http://go2.cis
+------+-------------------------------------------------------------------------+------------+---------------
| 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          | Not Found  |
```

	failure		
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:
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.
```

Analisar saída da ferramenta - Próximas etapas

- A ferramenta automatiza o processo de execução de comandos manuais em sistemas UCS.
- Se a ferramenta for executada **OK** e dá **APROVADO/NÃO ENCONTRADO** em todos os testes. O sistema UCS é bom para todas as verificações que o script executou.
- Em situações em que a ferramenta **FALHA/ENCONTRADO** em algumas verificações ou se o não for executado com êxito, você poderá usar os comandos CLI (listados aqui) para executar as mesmas verificações na interconexão de estrutura/sistema UCS que foram feitas pelo script Manualmente.
- A ferramenta NÃO verifica se há avisos antigos/novos/abertos/resolvidos e, portanto, é altamente recomendável revisar as Notas de versão e Guias de atualização do UCS antes de qualquer atividade de atualização ou manutenção.

> **Dica**: para uma verificação de integridade geral do seu ambiente UCS, o Cisco TAC não fornece esse serviço. A equipe de entrega ao cliente do CX da Cisco (conhecida anteriormente como Serviços avançados) tem uma análise de risco/depuração de bugs que ela oferece. Se você precisar desse tipo de serviço, entre em contato com sua equipe de vendas/contas.

Comandos CLI

SSH para ambas as interconexões em malha:

```
# 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 â€“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.
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.