重新映像AMP私有雲PC3000並還原備份

目錄

簡介
必要條件
需求
採用元件
設定
驗證
疑難排解

簡介

本文描述如何將高級惡意軟體防護(AMP)私有雲硬體裝置重新映像到出廠狀態，然後還原備份。如果只想將裝置恢復為出廠狀態，請跳過步驟8並按照常規安裝操作。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco AMP私有雲PC3000
- 通過思科整合管理控制器(CIMC)訪問基於核心的虛擬機器(KVM)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科進階惡意軟體防護私有雲PC3000 3.1.1
- 用於訪問KVM控制檯的鉻瀏覽器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1.登入CIMC。開啟KVM控制檯。

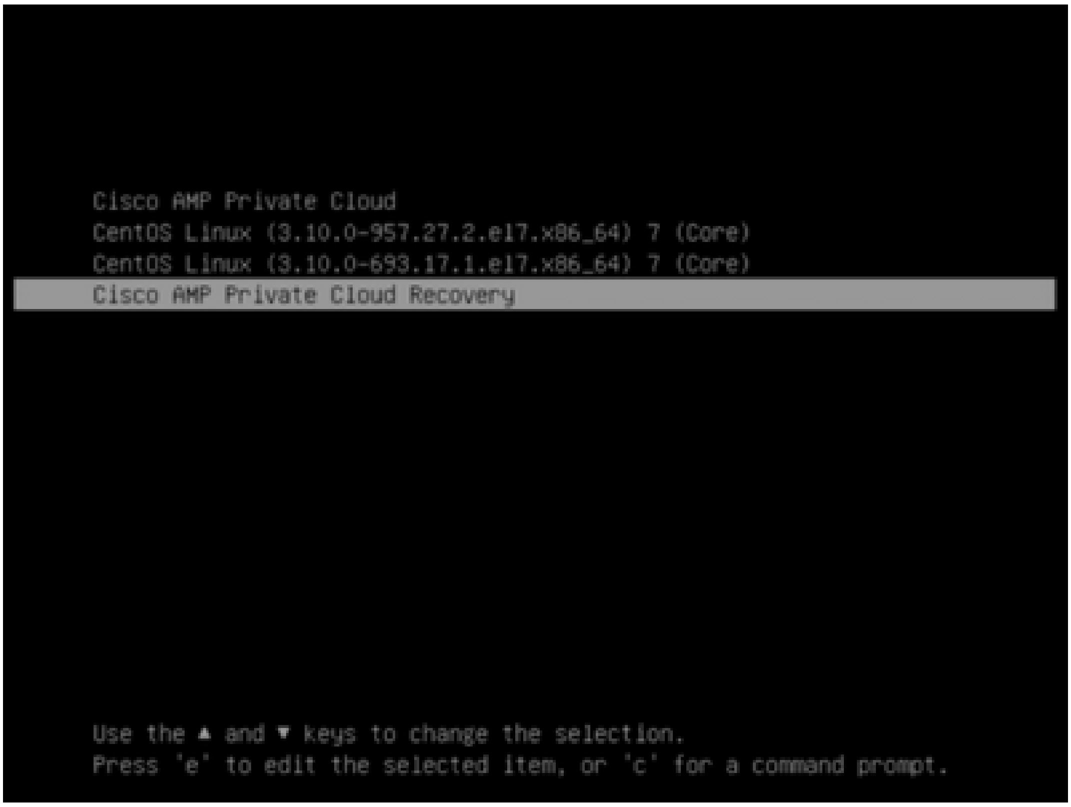
確保在瀏覽器中為該頁面啟用彈出視窗。

步驟2.重新載入裝置。

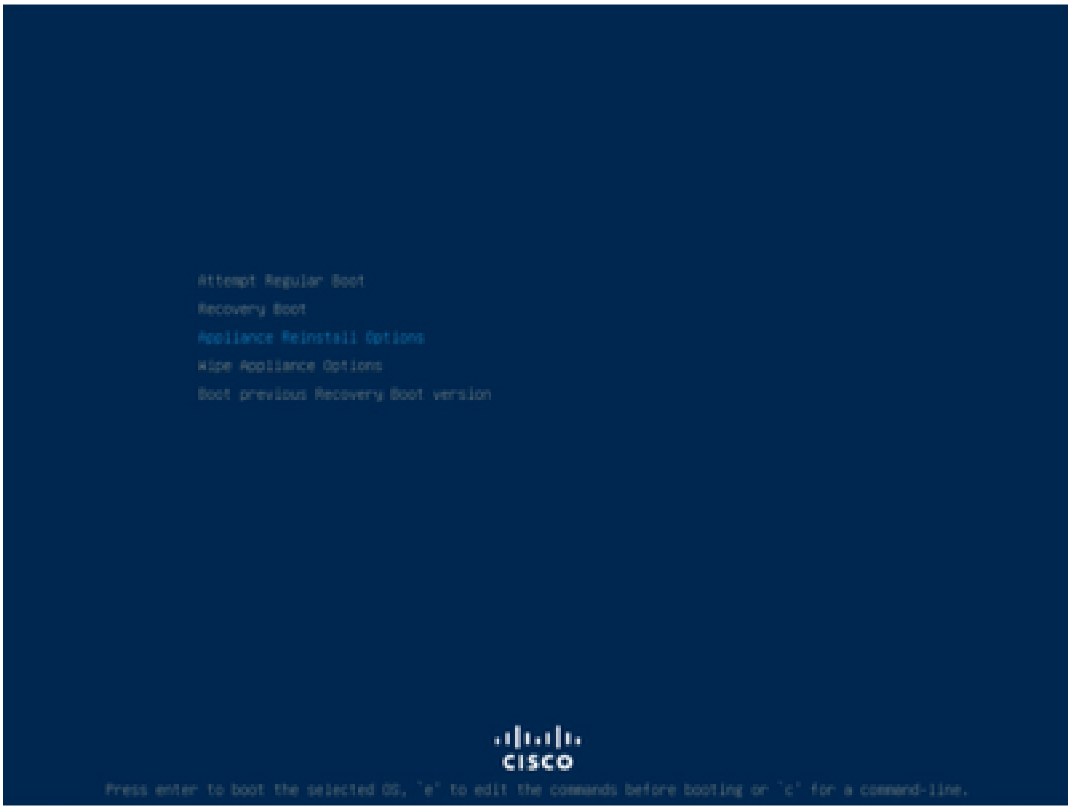
您可以通過管理門戶、安全外殼(SSH)或CIMC KVM重新啟動裝置。

步驟3.基本輸入輸出系統(BIOS)加電自檢(POST)完成後，GNU GR和Unified Bootloader(GRUB)選單顯示：

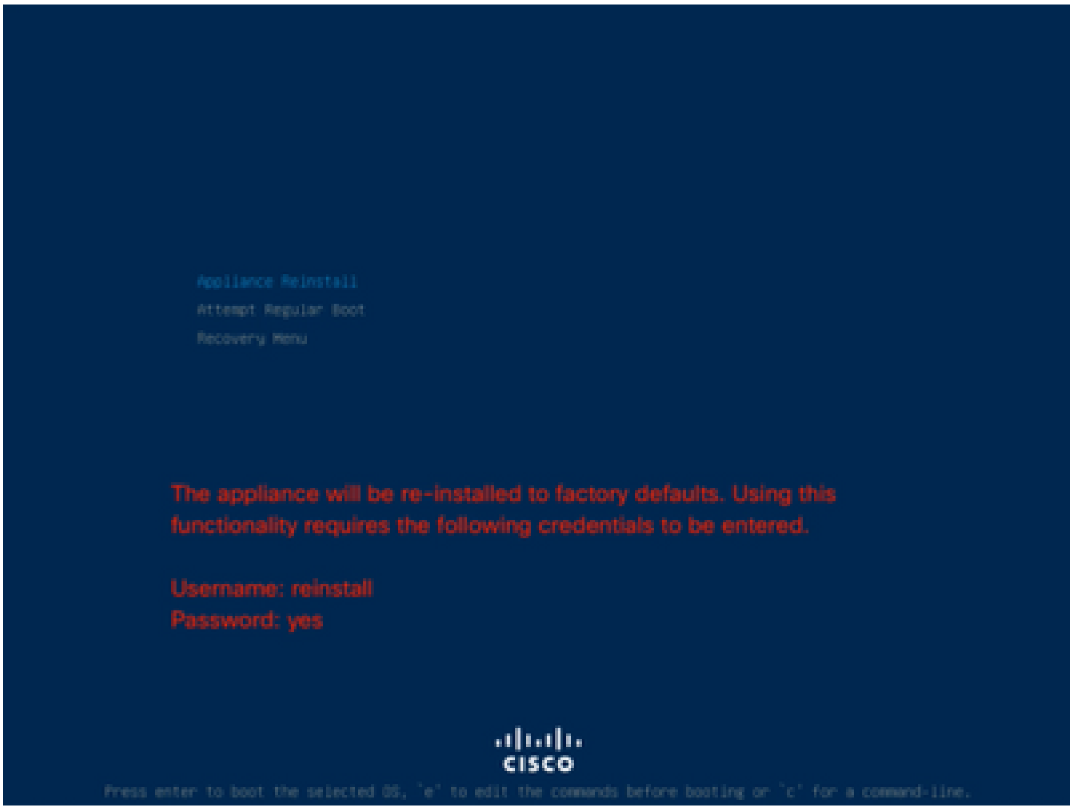
選擇Cisco AMP Private Cloud Recovery > Appliance Reinstall Options > Appliance Reinstall。



```
Cisco AMP Private Cloud
CentOS Linux (3.10.0-957.27.2.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-693.17.1.el7.x86_64) 7 (Core)
Cisco AMP Private Cloud Recovery

Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```



```
Attempt Regular Boot
Recovery Boot
Appliance Reinstall Options
Wipe Appliance Options
Boot previous Recovery Boot version

Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
```



The appliance will be re-installed to factory defaults. Using this functionality requires the following credentials to be entered.

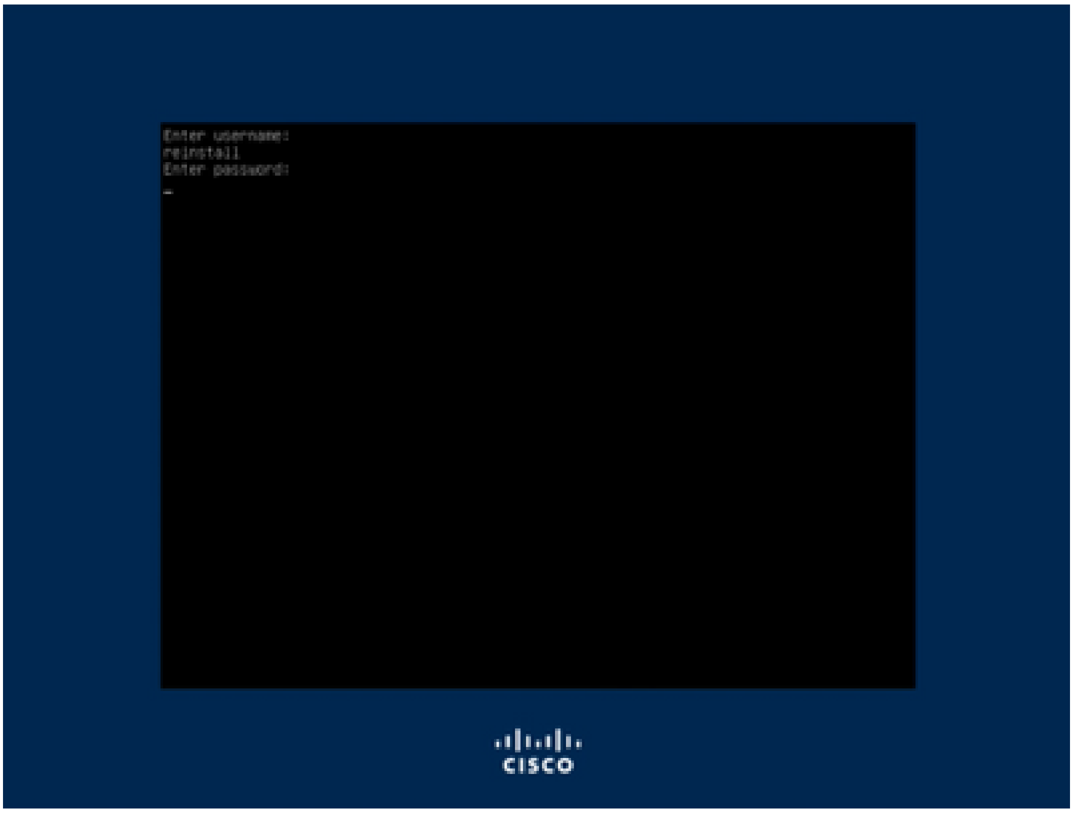
Username: reinstall
Password: yes

Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

步驟4.輸入使用者名稱和密碼。

使用者名稱:**重新安裝**

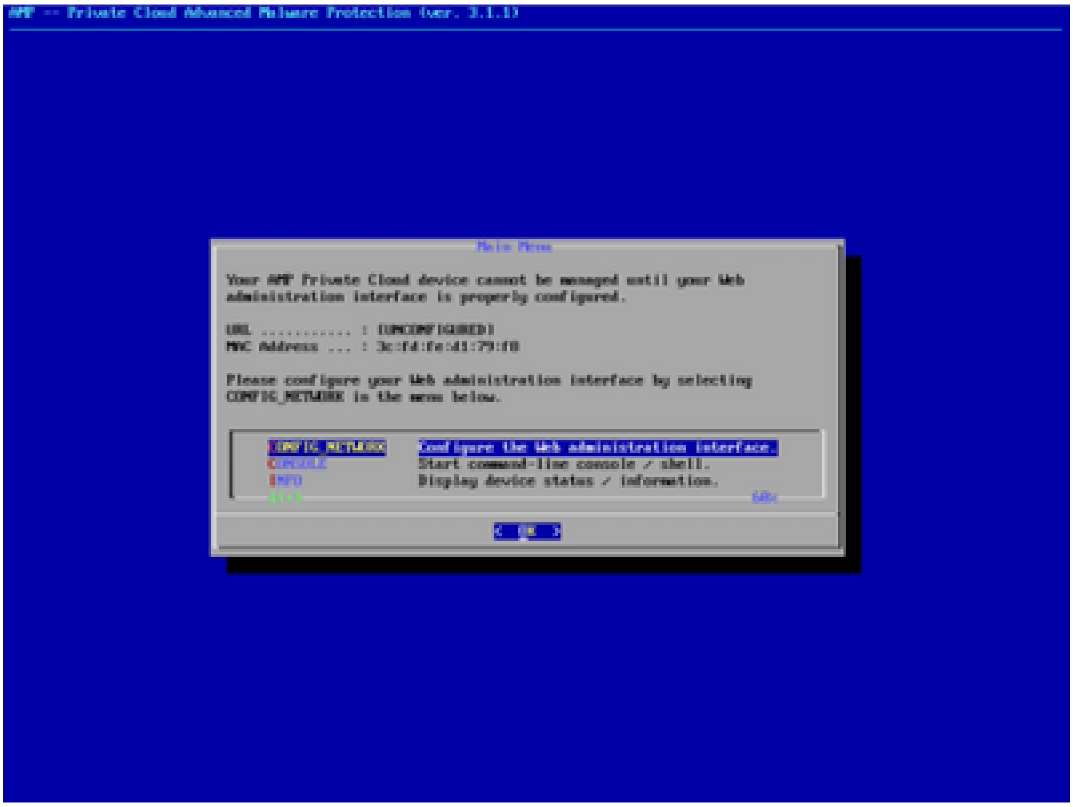
密碼：**是**



```
Enter username:
reinstall
Enter password:
_
```

步驟5.開始重新映像，重新載入後您將看到初始選單。

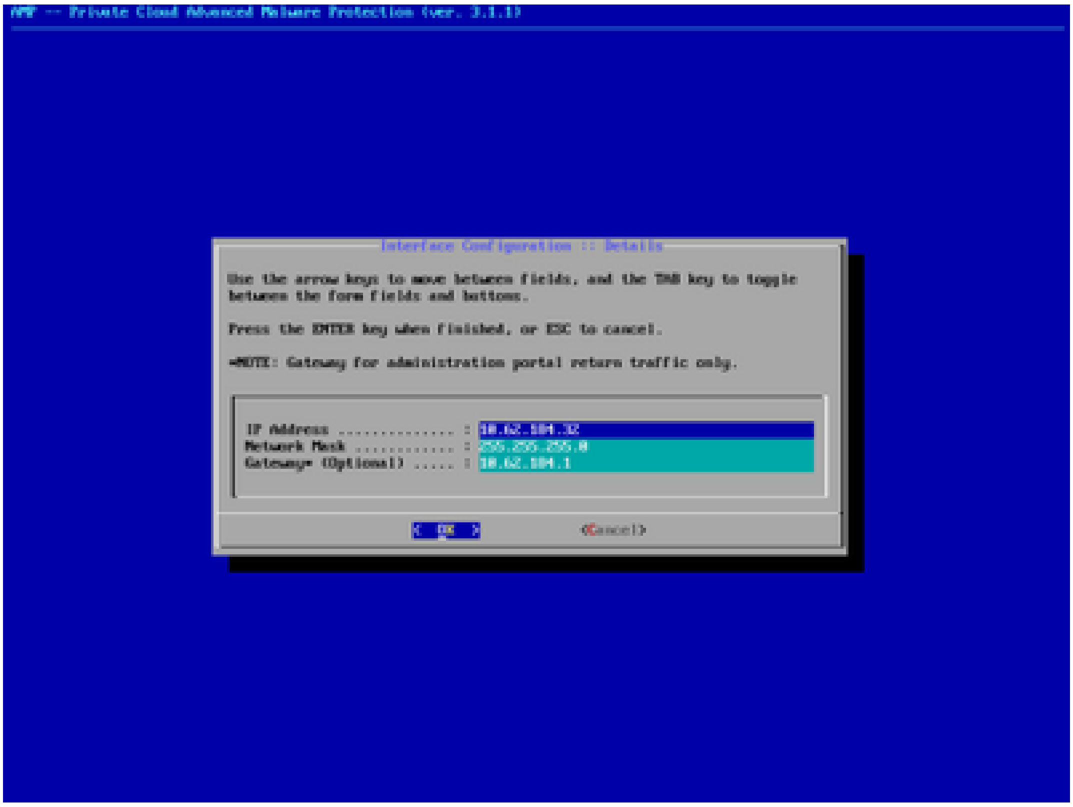
```
[   11.737938] usbcore: registered new interface driver usbserial_generic
[   11.744818] usbserial: USB Serial support registered for generic
[   11.753899] i8042: PNP: No PS/2 controller found. Probing ports directly.
[   11.905287] usb 1-6: new high-speed USB device number 2 using xhci_hcd
[   12.118200] usb 1-6: New USB device found, idVendor=2a4b, idProduct=0400
[   12.123103] usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[   12.130530] usb 1-6: Product: Emulex Pilot4 HighSpeed HUB
[   12.136513] usb 1-6: Manufacturer: Emulex Communications
[   12.140912] usb 1-6: SerialNumber: 0xBADDEFACE
[   12.146133] hub 1-6:1.0: USB hub found
[   12.150658] hub 1-6:1.0: 7 ports detected
[   12.267537] usb 1-7: new high-speed USB device number 3 using xhci_hcd
[   12.297535] i8042: Can't read CTR while initializing i8042
[   12.302622] i8042: probe of i8042 failed with error -5
[   12.306905] mousedev: PS/2 mouse device common for all mice
[   12.311260] rtc_cmos 00:00: RTC can wake from S4
[   12.316427] rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0
[   12.320010] rtc_cmos 00:00: alarms up to one month, y3k, 114 bytes nvram, hpet ir
[   12.325435] intel_pstate: Intel P-state driver initializing
[   12.332225] intel_pstate: HWP enabled
[   12.379200] cpuidle: using governor menu
[   12.344827] EFI Variables Facility v0.08 2004-May-17
[   12.370265] tsc: Refined TSC clocksource calibration: 2593.906 MHz
[   12.384179] Switched to clocksource tsc
[   12.405792] hidraw: raw HID events driver (C) Jiri Kosina
[   12.409874] usbhid: USB HID core driver
[   12.411948] usb 1-7: New USB device found, idVendor=0424, idProduct=6570
[   12.411952] usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
[   12.411955] usb 1-7: Product: USB2.0 Hub
[   12.413574] hub 1-7:1.0: USB hub found
[   12.413942] hub 1-7:1.0: 4 ports detected
[   12.441224] Detected 1 PCC Subspaces
[   12.445423] Registering PCC driver as Mailbox controller
[   12.451900] drop_monitor: Initializing network drop monitor service
[   12.456276] TCP: cubic registered
[   12.462456] Initializing XFRM netlink socket
[   12.466662] NET: Registered protocol family 10
[   12.472626] NET: Registered protocol family 17
[   12.472840] usb 1-6.1: new high-speed USB device number 4 using xhci_hcd
[   12.481900] mpls_gso: MPLS GSO support
[   12.491395] intel_rdt: Intel RDT MB allocation detected
[   12.505676] microcode: sig=0x50654, pf=0x80, revision=0x200004d
[   12.513400] microcode: Microcode Update Driver: v2.01 <tigran@aivazian.fsnet.co.uk>, Peter Oruba
```



```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.1.1)

Your AMP Private Cloud device cannot be managed until your Web
administration interface is properly configured.

URL ............ : [UNCONFIGURED]
MAC Address .... : 3c:fd:fe:d1:79:f8

Please configure your Web administration interface by selecting
CONFIG_NETWORK in the menu below.
```

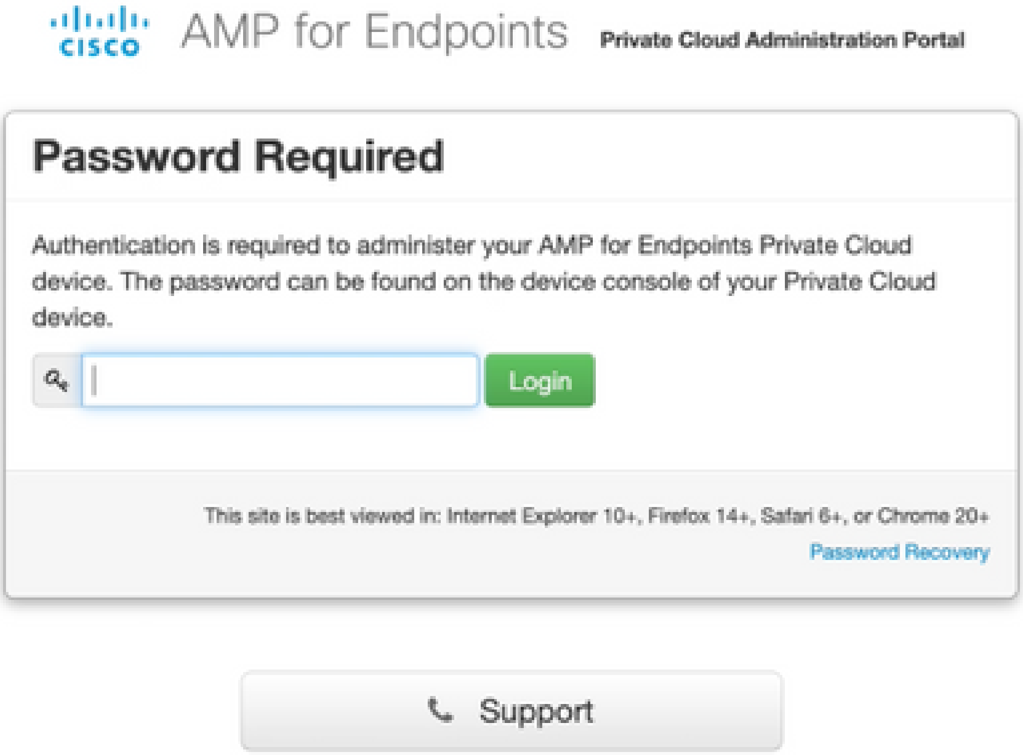
Main Menu
CONFIG_NETWORK   Configure the Web administration interface.
CONSOLE   Start command-line console / shell.
INFO   Display device status / information.
v(+)
68%
< OK >

步驟6.在CONFIG_NETWORK子選單中配置網路。



```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.1.1)

Interface Configuration :: Details

Use the arrow keys to move between fields, and the TAB key to toggle
between the form fields and buttons.

Press the ENTER key when finished, or ESC to cancel.

*NOTE: Gateway for administration portal return traffic only.

IP Address ............... : 10.62.104.32
Network Mask ............. : 255.255.255.0
Gateway* (Optional) ...... : 10.62.104.1
```

步驟7.使用步驟5中的密碼登入AMP OPadmin門戶。

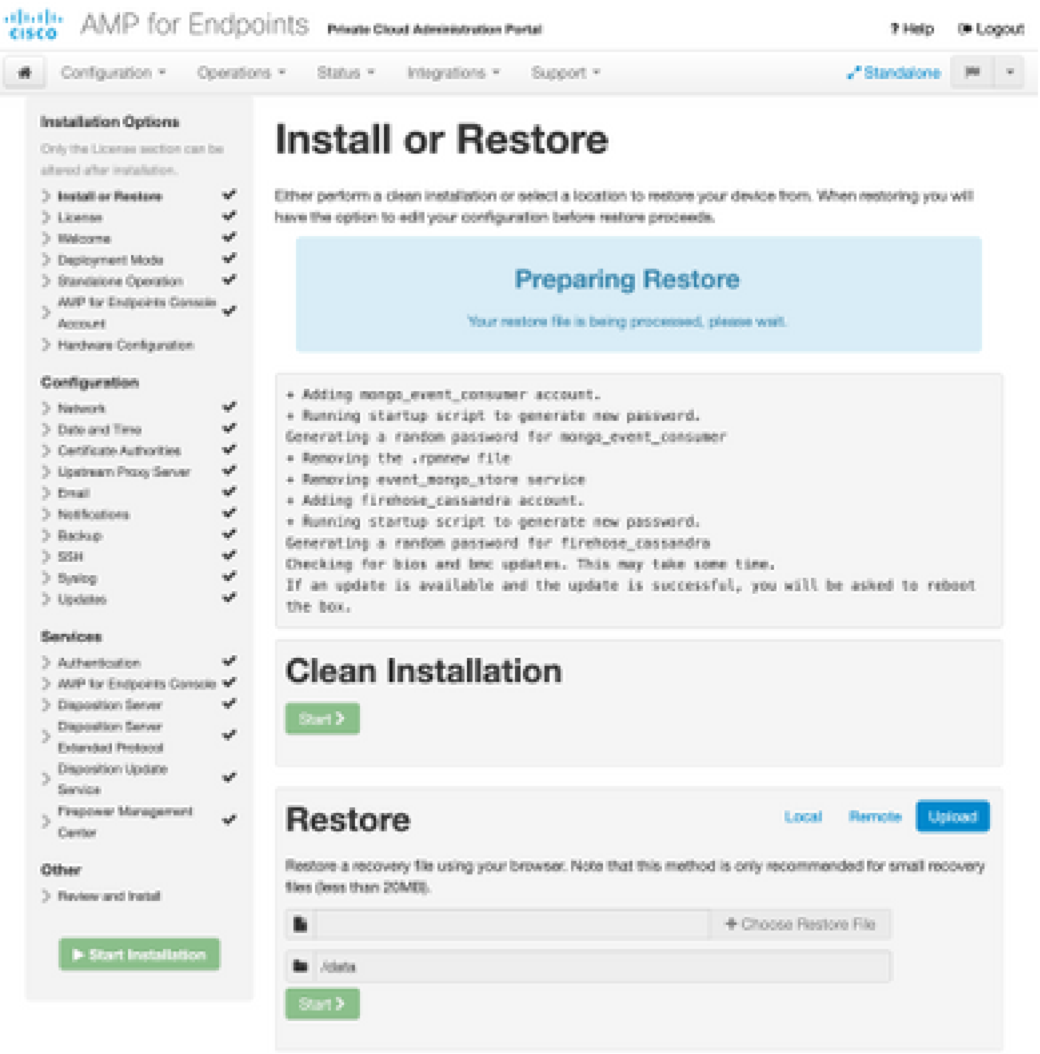


Password Required

Authentication is required to administer your AMP for Endpoints Private Cloud device. The password can be found on the device console of your Private Cloud device.

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

步驟8.使用SFTP或SCP將備份從遠端伺服器下載到/data/。



Only the License section can be altered after installation.

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Preparing Restore

Your restore file is being processed, please wait.

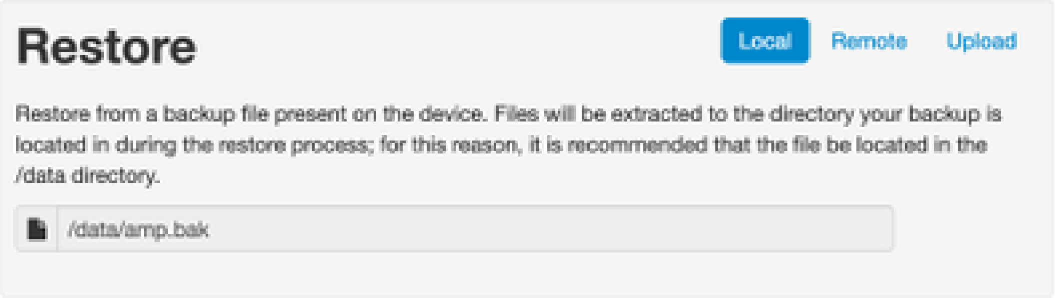
```
• Adding mongo_event_consumer account.
• Running startup script to generate new password.
Generating a random password for mongo_event_consumer
• Removing the .rpmnew file
• Removing event_mongo_store service
• Adding firehose_cassandra account.
• Running startup script to generate new password.
Generating a random password for firehose_cassandra
Checking for bios and bmc updates. This may take some time.
If an update is available and the update is successful, you will be asked to reboot
the box.
```

Clean Installation

Restore

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

/data

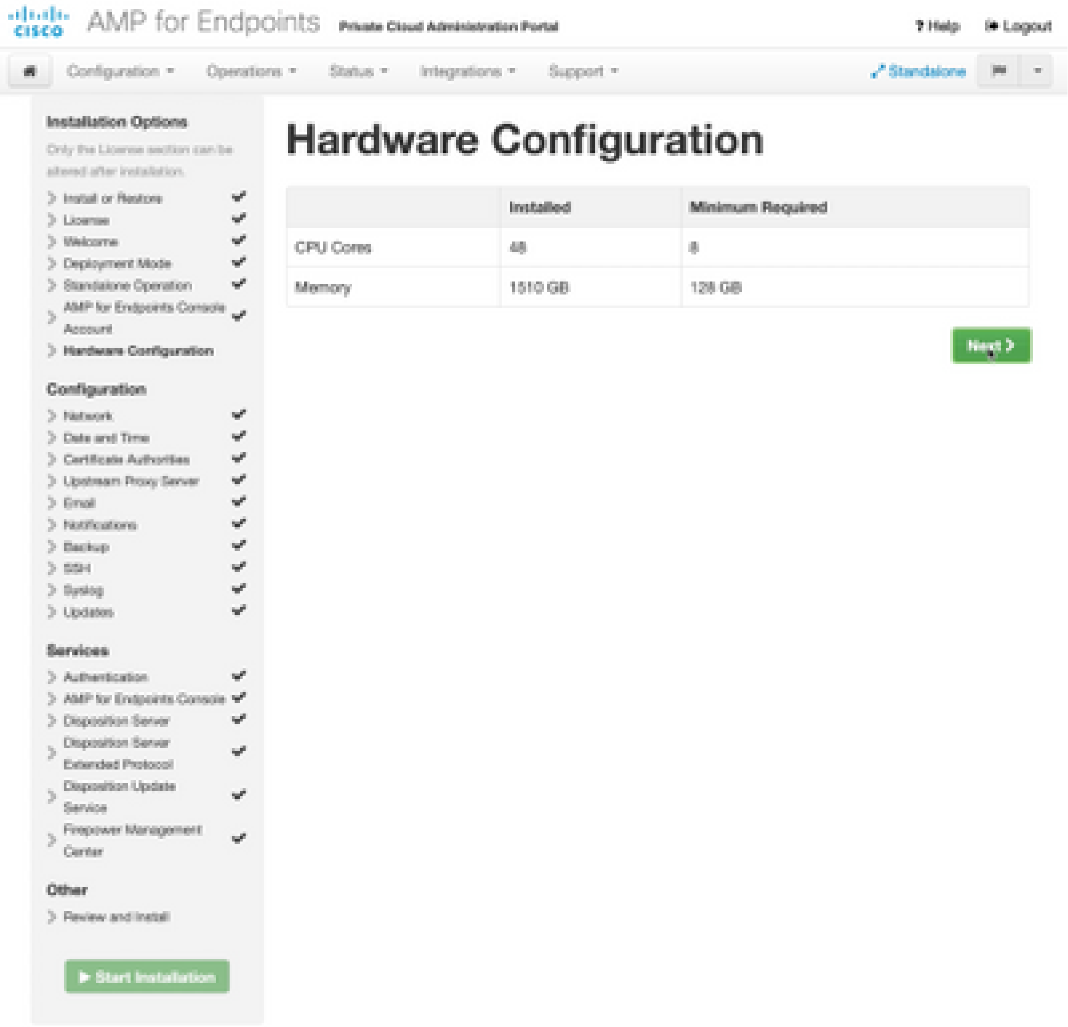


Restore

Restore from a backup file present on the device. Files will be extracted to the directory your backup is located in during the restore process; for this reason, it is recommended that the file be located in the /data directory.

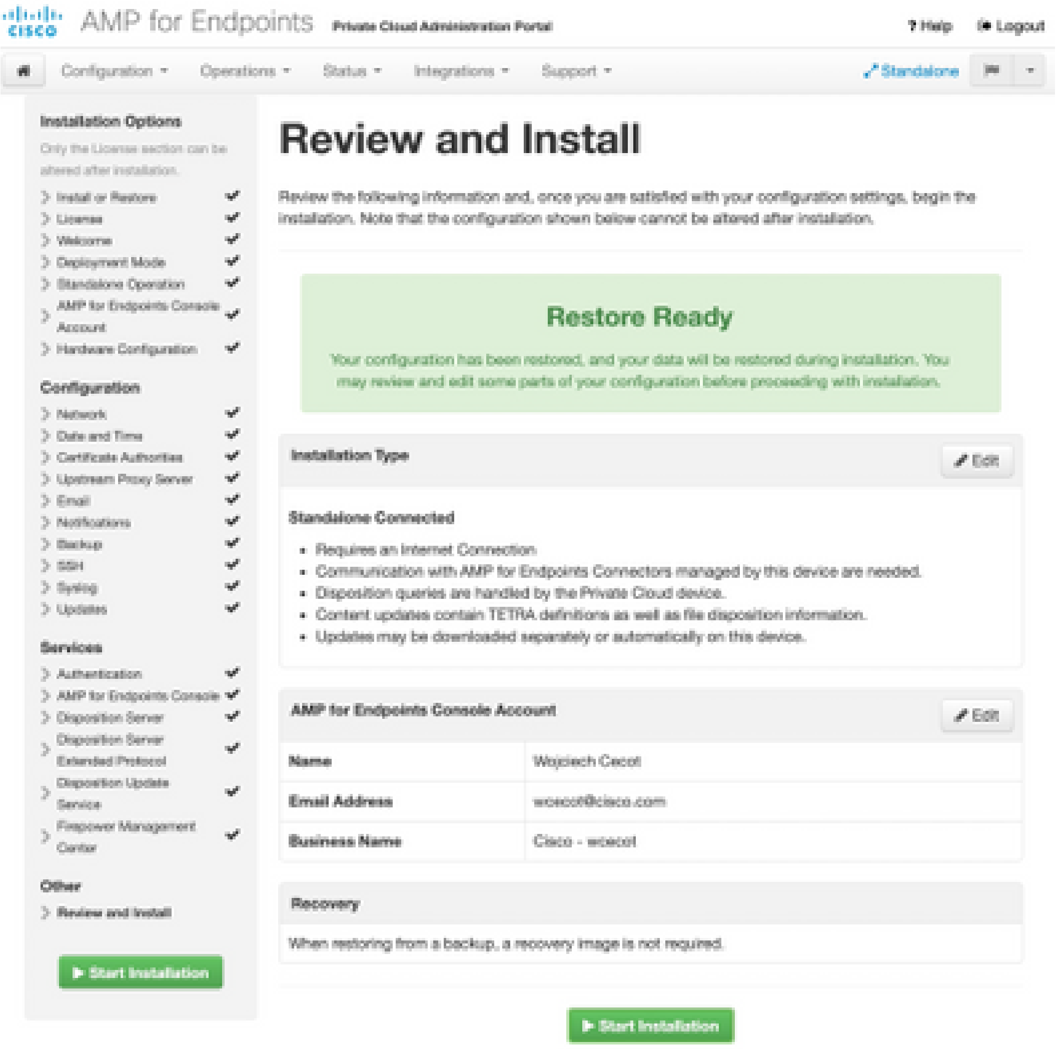
/data/amp.bak

步驟9.確認硬體配置，按一下**下一步>開始安裝**。



Hardware Configuration

	Installed	Minimum Required
CPU Cores	48	8
Memory	1510 GB	128 GB



Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type Edit

Standalone Connected

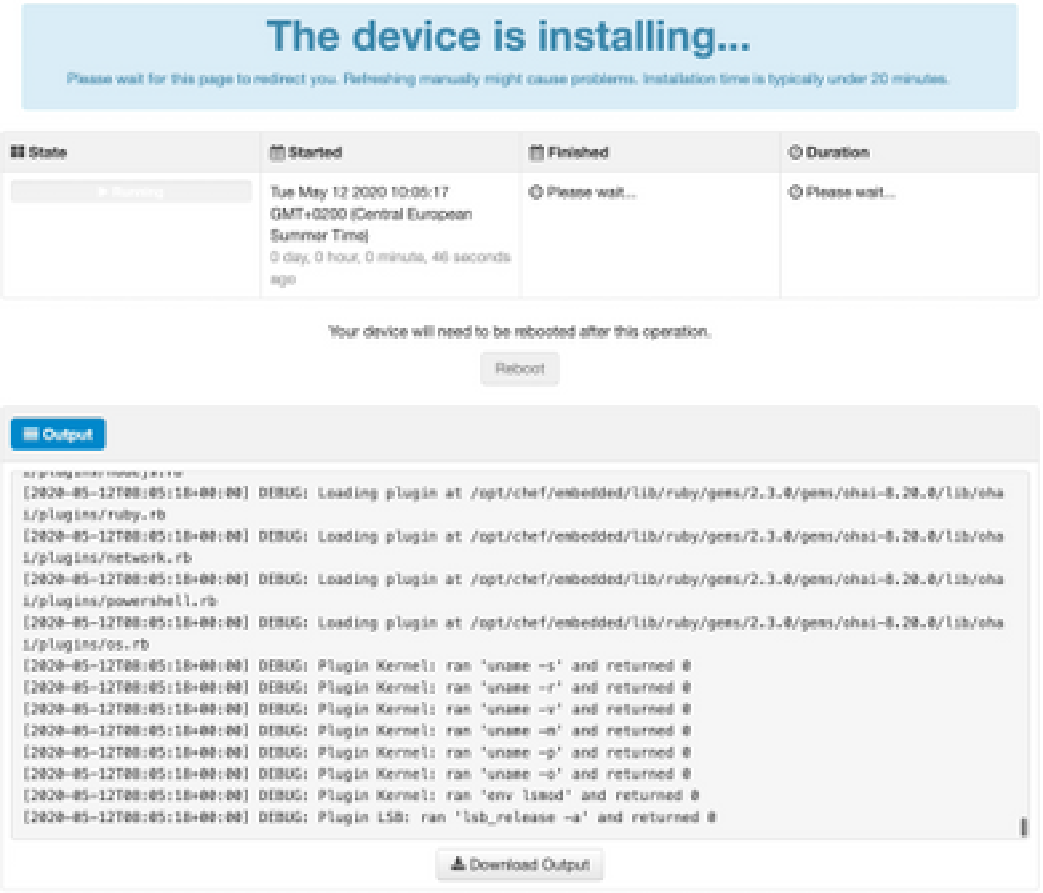
- Requires an Internet Connection.
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

AMP for Endpoints Console Account Edit

Name	Wojciech Cecot
Email Address	wcecot@cisco.com
Business Name	Cisco - wcecot

Recovery

When restoring from a backup, a recovery image is not required.



The device is installing...

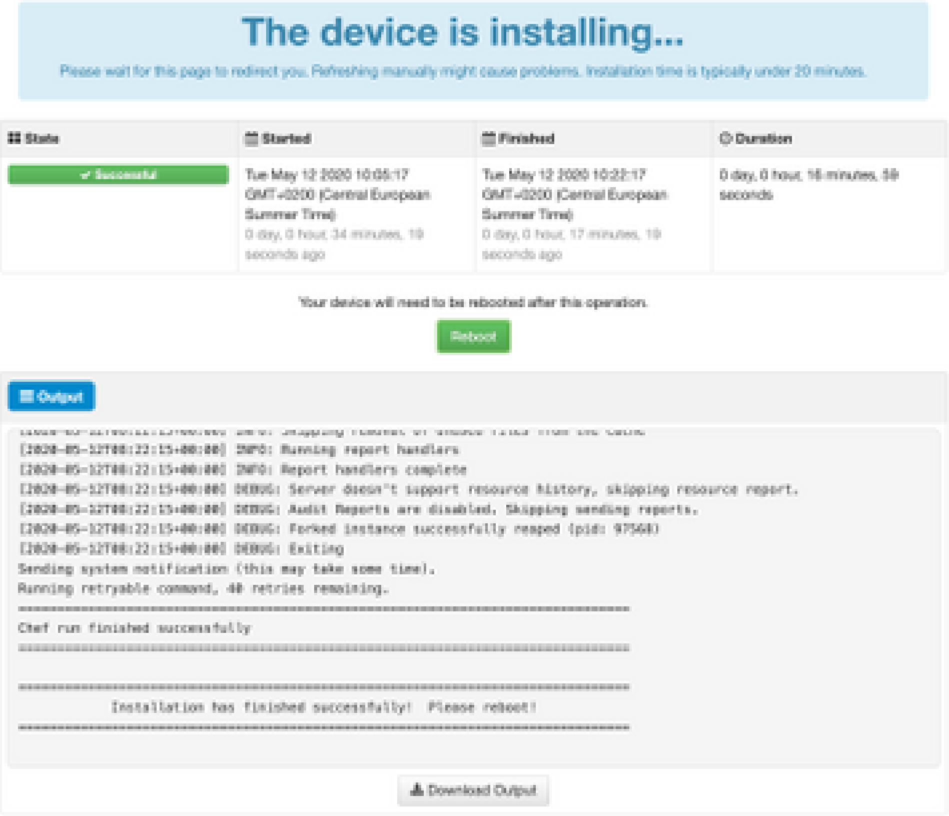
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 46 seconds ago	Please wait...	Please wait...

Your device will need to be rebooted after this operation.

```
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/oha
i/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/oha
i/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/oha
i/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/oha
i/plugins/os.rb
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -s' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -r' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -v' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -m' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -p' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -o' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'env lsmod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0
```

步驟10.成功還原後需要重新啟動。



The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 34 minutes, 19 seconds ago	Tue May 12 2020 10:22:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 17 minutes, 19 seconds ago	0 day, 0 hour, 16 minutes, 59 seconds

Your device will need to be rebooted after this operation.

```
[2020-05-12T08:22:15+00:00] INFO: Skipping removal of unused files from the cache
[2020-05-12T08:22:15+00:00] INFO: Running report handlers
[2020-05-12T08:22:15+00:00] INFO: Report handlers complete
[2020-05-12T08:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T08:22:15+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2020-05-12T08:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T08:22:15+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
================================================================================
Chef run finished successfully
================================================================================


================================================================================
            Installation has finished successfully!  Please reboot!
================================================================================
```

驗證

重新引導裝置後，檢查兩個入口是否工作正常。嘗試在Web瀏覽器中開啟OPadmin和控制檯門戶。兩個入口都需要幾分鐘才能被訪問。

疑難排解

在備份還原過程中，OPadmin和控制檯門戶的密碼與以前相同。否則，您需要使用在嚮導中設定的內容。