安裝和配置安全終端虛擬私有雲

目錄

簡介

本文檔介紹並重點介紹如何在ESXi環境中的伺服器上成功部署虛擬私有雲(VPC)。 有關快速入門手冊、部署策略、權利指南、控制檯和管理員使用手冊等其他文檔，請訪問本網站文檔

作者：Roman Valenta，思科TAC工程師。

必要條件

要求:

VMware ESX 5或更高版本

- 雲代理理模式（僅限）：128 GB RAM、8個CPU核心（2個CPU，每個推薦有4個核心）、1 TB的VMware資料儲存區最小可用磁碟空間
- 驅動器型別：空隙模式需要SSD，建議使用代理
- RAID型別：一個RAID 10組（條帶化映象）
- 最低VMware資料儲存區大小：2 TB
- RAID 10組(4K)的最小資料儲存隨機讀取數：60K IOPS
- RAID 10組(4K)的最小資料儲存隨機寫入數：30K IOPS

思科建議您瞭解以下主題：

- 有關如何使用證書的基本知識。
- 有關如何在DNS伺服器（Windows或Linux）下設定DNS的基本知識
- 在VMWare ESXi中安裝開放式虛擬裝置(OVA)模板

在本實驗中使用：

VMware ESX 6.5

- 雲代理模式（僅限）：48 GB RAM、8個CPU核心（建議使用2個CPU和4個核心）、1 TB的VMware資料儲存區最小可用磁碟空間
- 驅動器型別：SATA
- RAID型別：一個RAID 1
- 最低VMware資料儲存區大小：1 TB
- MobaXterm 20.2（多終端程式，類似PuTTY）
- Cygwin64（用於下載AirGap更新）

此外

- 使用openSSL或XCA建立的憑證
- DNS伺服器（Linux或Windows）我的實驗室使用Windows Server 2016和CentOS-8
- 用於測試終端的Windows VM
- 授權

如果記憶體低於48GB，則3.2+ VPC上的RAM將不可用。

注意：私有雲OVA建立驅動器分割槽，因此無需在VMWare.伺服器中指定這些分割槽，該伺服器會解析乾淨的介面主機名。

有關版本特定的硬體要求的詳細資訊，請參閱VPC裝置產品手冊。

注意：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。

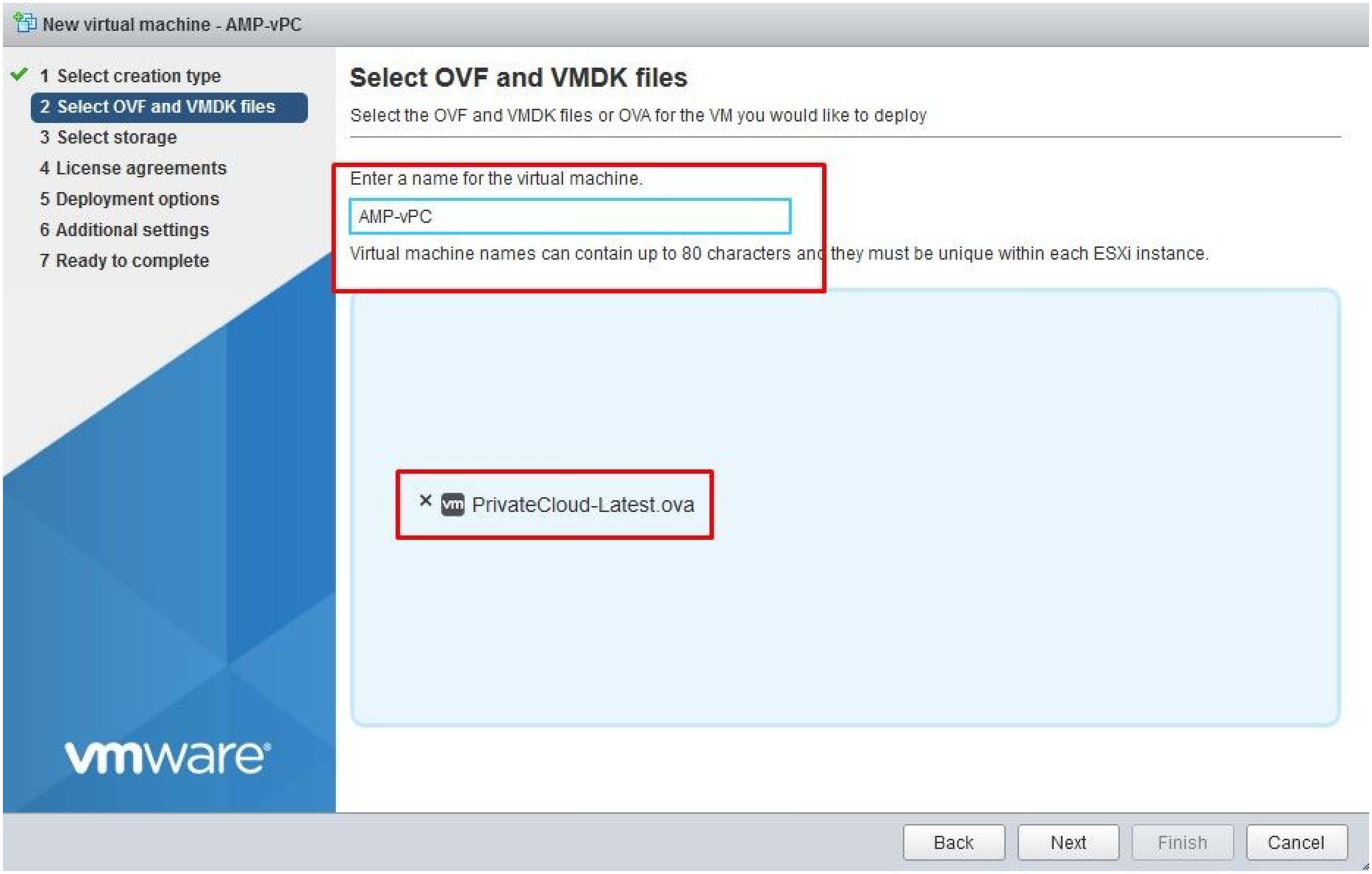
VPC部署

選擇電子交付或權利電子郵件中提供的URL。下載OVA檔案並繼續安裝

VM安裝

第1步：

導覽至File > Deploy OVF Template，以開啟Deploy OVF Template嚮導，如下圖所示。



New virtual machine - AMP-vPC

Select OVF and VMDK files

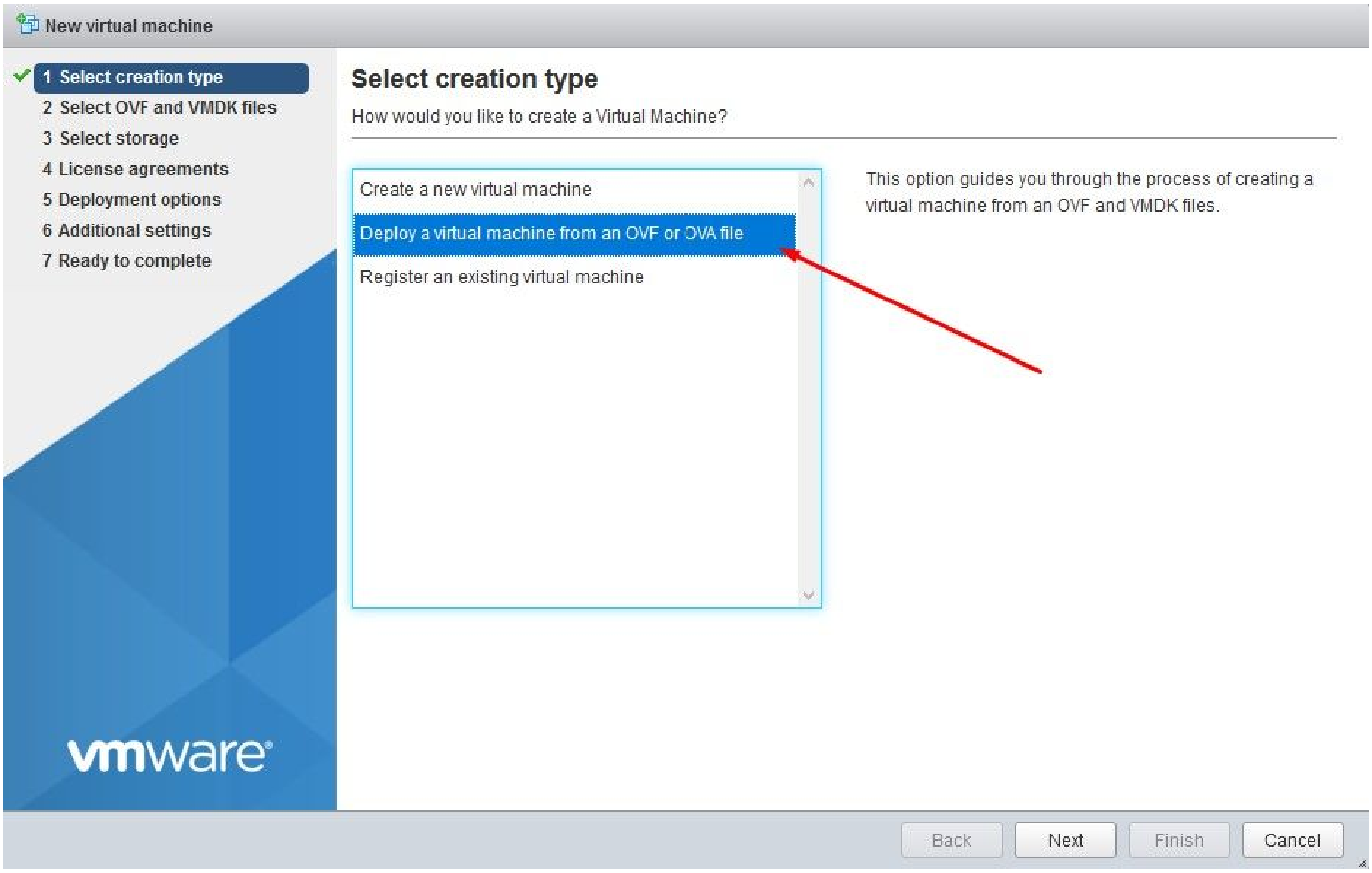
Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

AMP-vPC

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× PrivateCloud-Latest.ova



New virtual machine

Select creation type

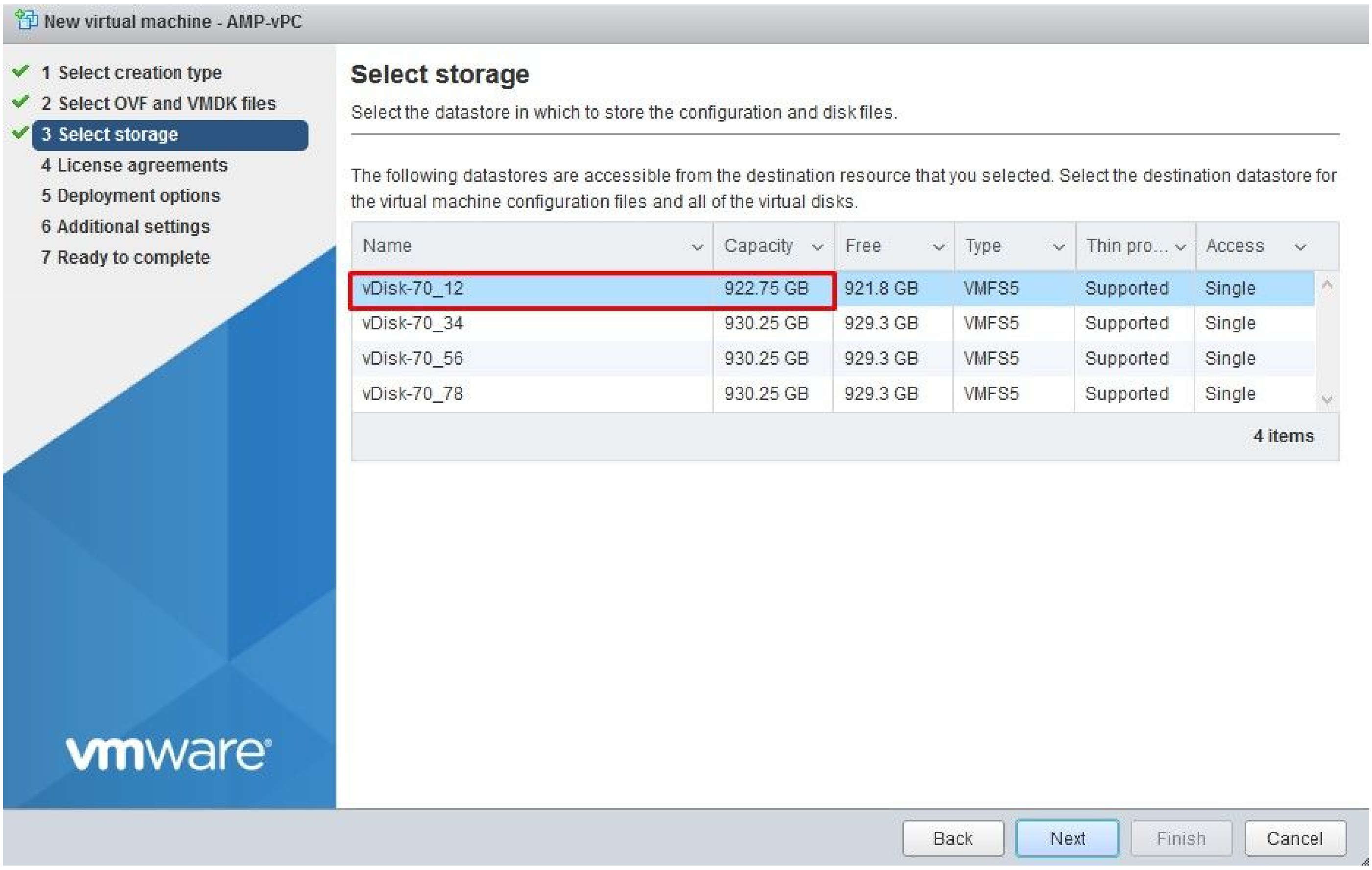
How would you like to create a Virtual Machine?

Create a new virtual machine

Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.



New virtual machine - AMP-vPC

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

Select storage

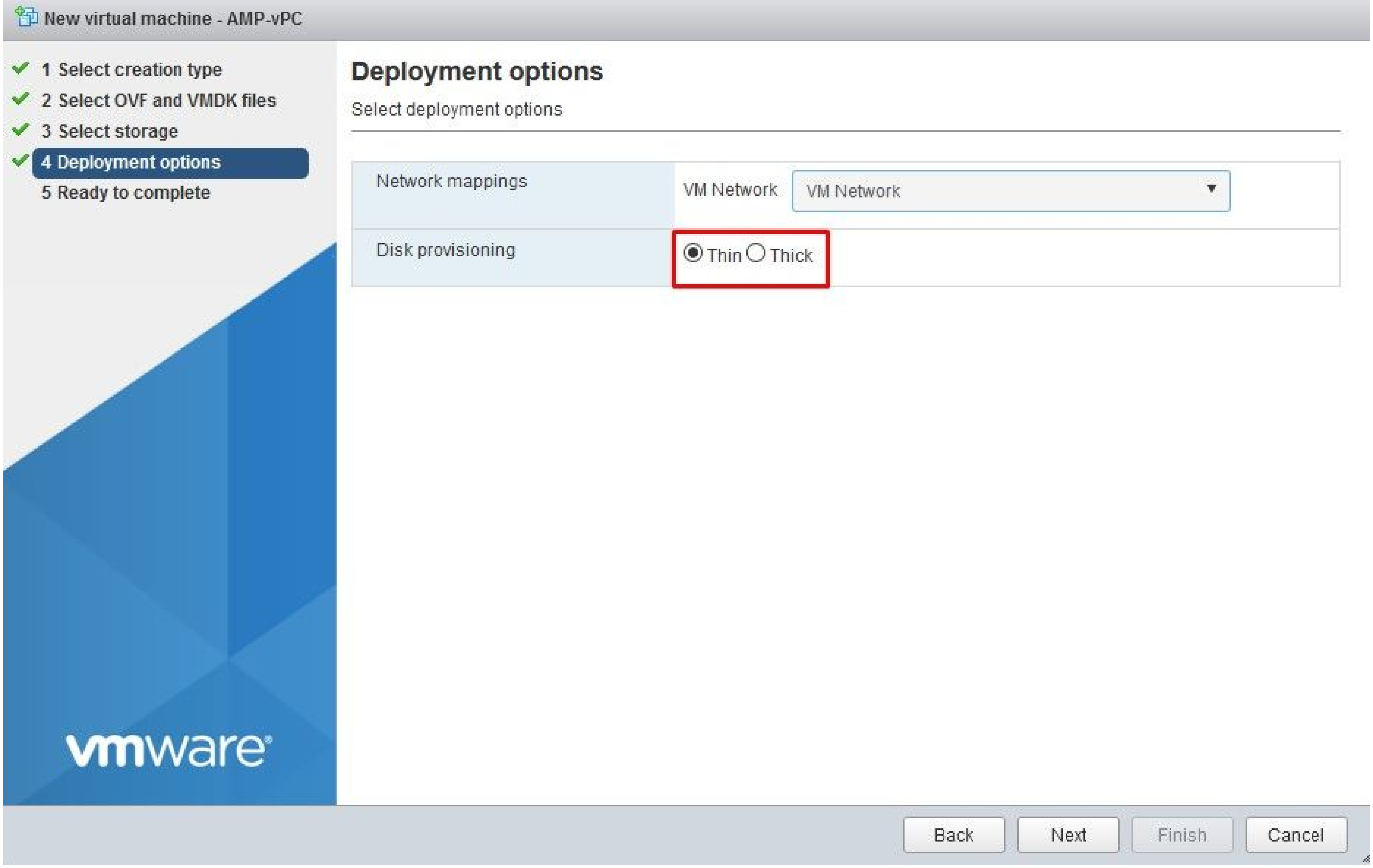
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	Supported	Single
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	Supported	Single

4 items

注意:Thick Provisioning在建立磁碟時保留空間。如果選擇此選項，則效能會比精簡配置更高。但是，這不是強制性的。現在在Next上選擇，如下圖所示。



New virtual machine - AMP-vPC

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 Deployment options
5 Ready to complete

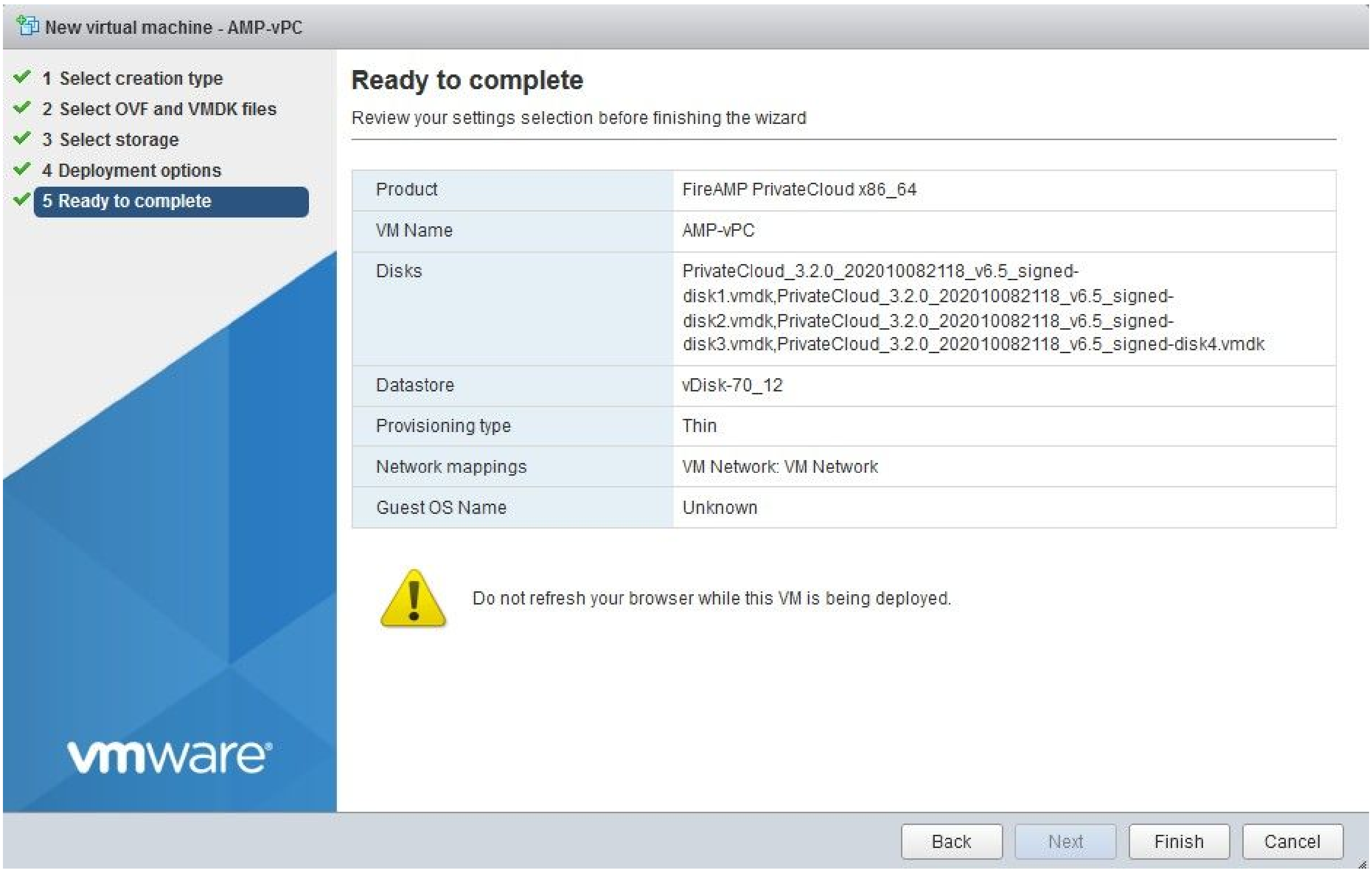
Deployment options

Select deployment options

Network mappings	VM Network	VM Network ▼
Disk provisioning	● Thin ○ Thick	

步驟 2:

選擇瀏覽……以選擇OVA檔案，然後在下一步上選擇。您會注意到OVF模板詳細資訊頁面上的預設OVA引數，如下圖所示。選擇下一步。



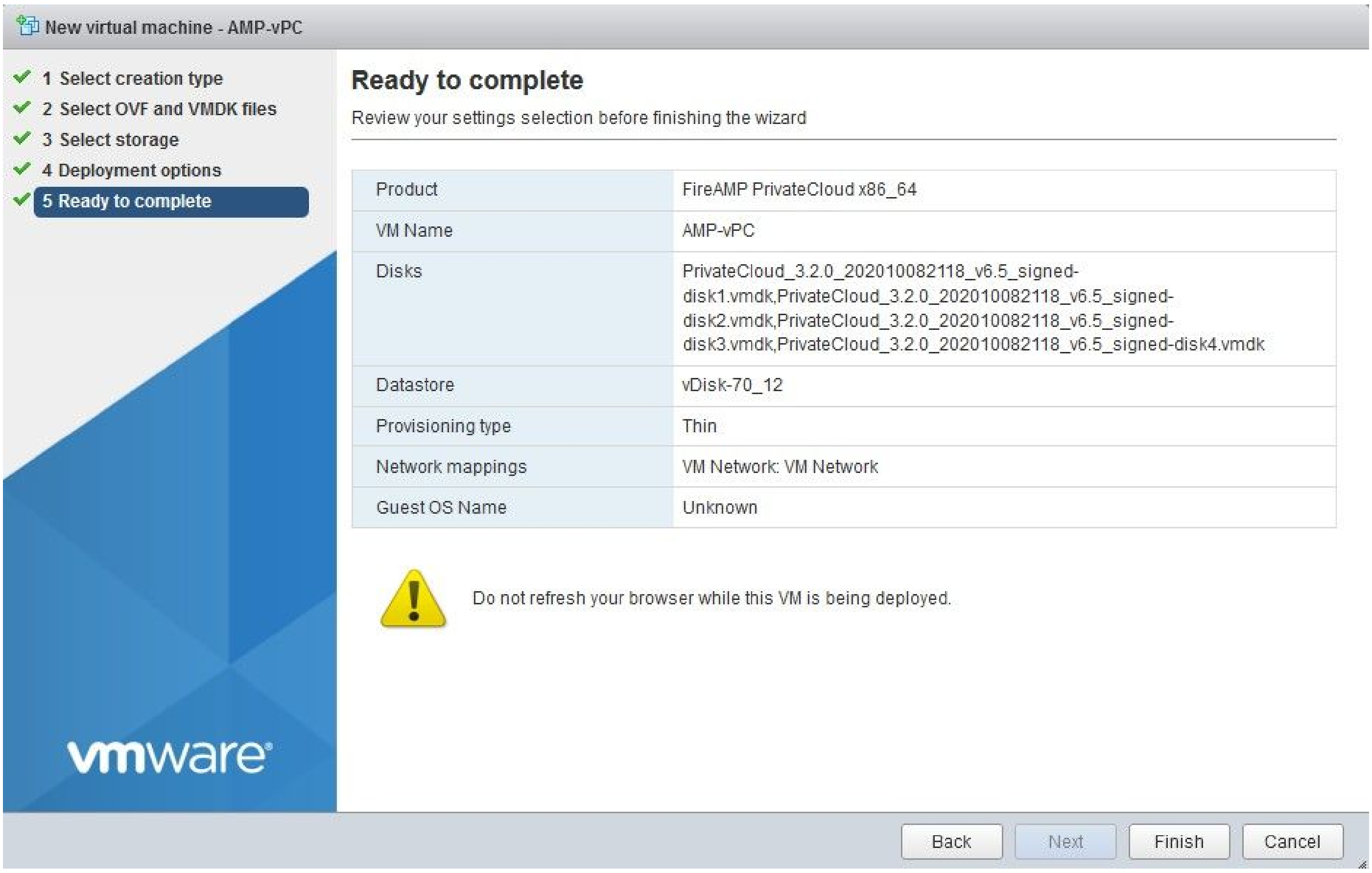
Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

初始管理介面設定



New virtual machine - AMP-vPC

Ready to complete

Review your settings selection before finishing the wizard

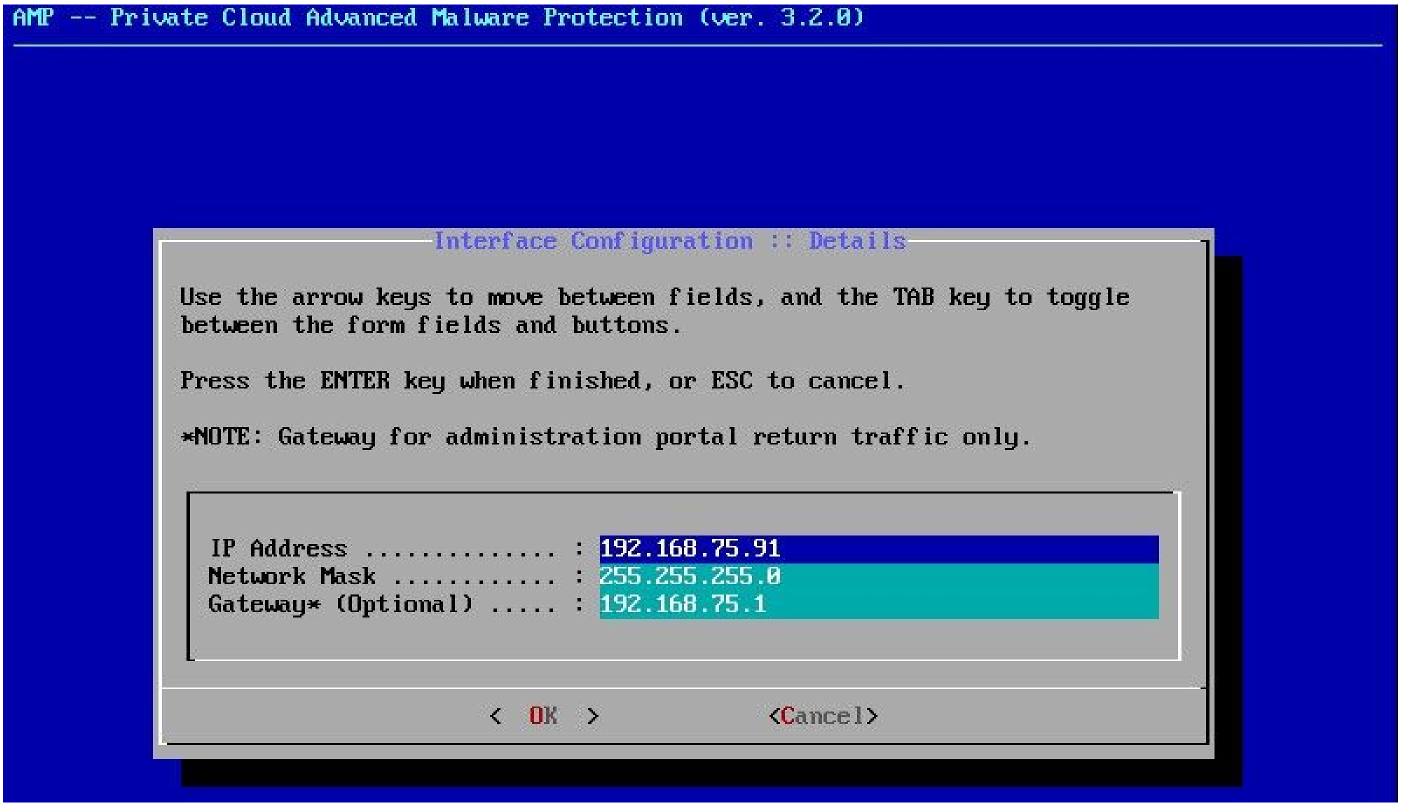
Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

VM啟動後，您通過VM控制檯執行初始配置。

步驟 1:

您可能注意到，URL顯示[UNCONFIGURED]（如果介面沒有從DHCP伺服器接收IP地址）。請注意，此介面是Management介面。這不是Production接口。

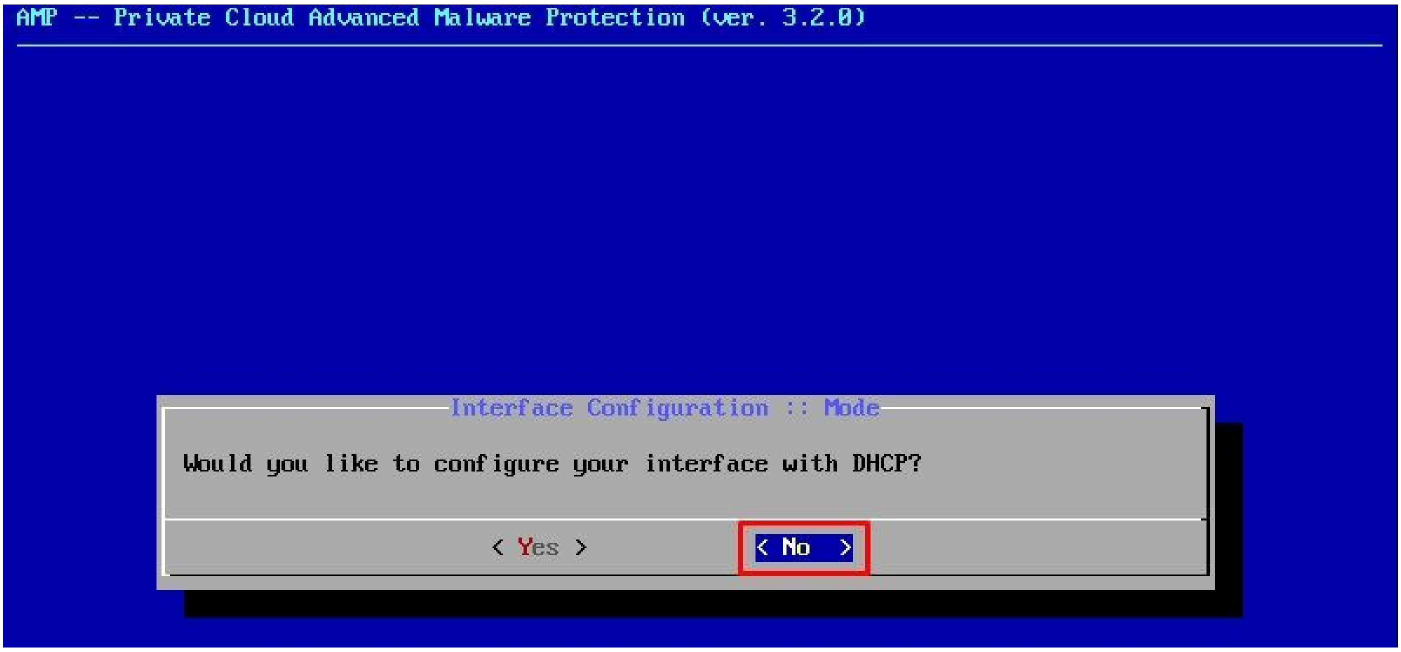


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

              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 ............... : 192.168.75.91
    Network Mask ............. : 255.255.255.0
    Gateway* (Optional) ...... : 192.168.75.1

                  <  OK  >              <Cancel>
```

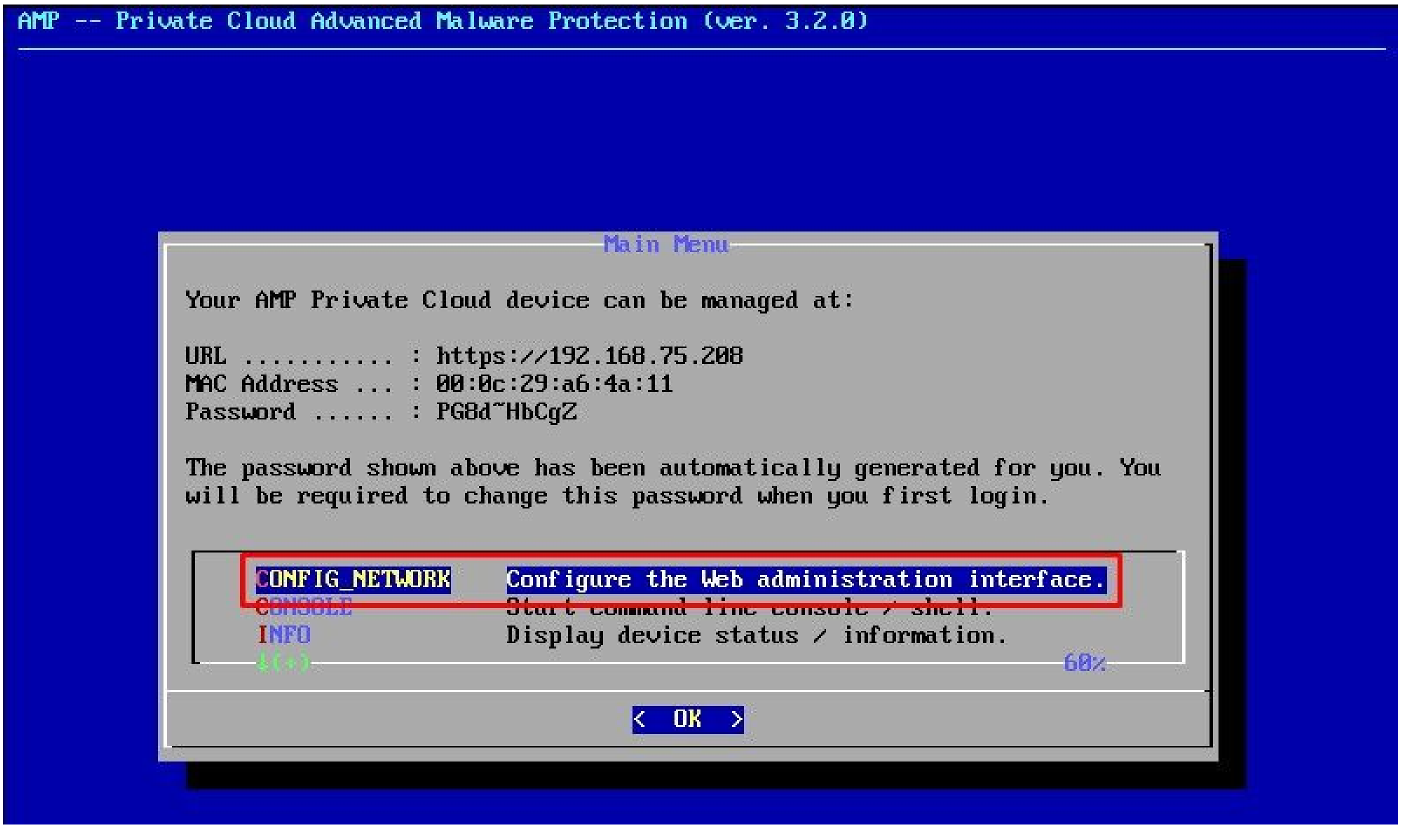
步驟 2:

您可以瀏覽Tab、Enter和Arrow鍵。

導航到CONFIG_NETWORK，然後選擇鍵盤上的Enter鍵，開始配置安全終端私有雲的管理IP地址。如果不希望使用DHCP，請選擇No並選擇Enter鍵。

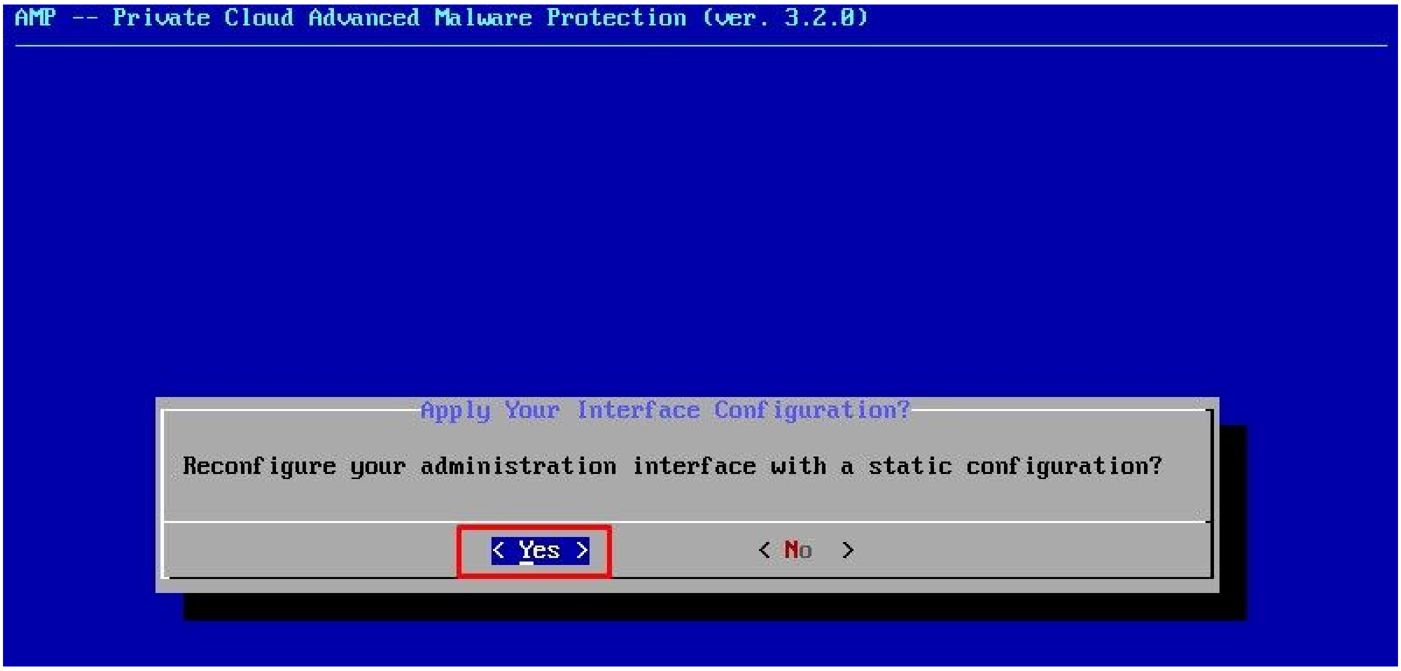


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Interface Configuration :: Mode

Would you like to configure your interface with DHCP?

        < Yes >        < No  >
```



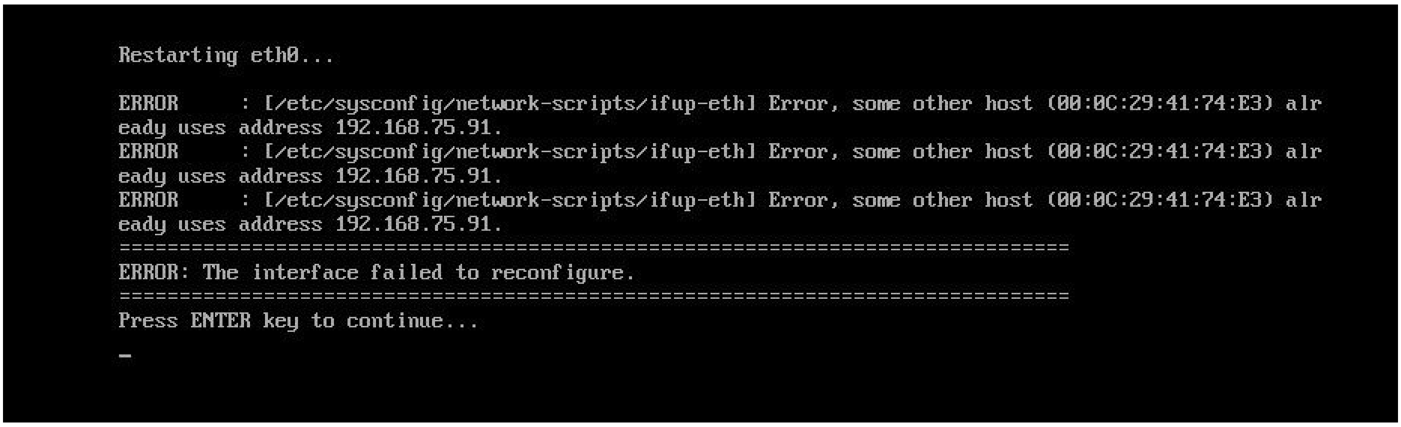
```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Main Menu

Your AMP Private Cloud device can be managed at:

URL ........... : https://192.168.75.208
MAC Address ... : 00:0c:29:a6:4a:11
Password ...... : PG8d~HbCgZ

The password shown above has been automatically generated for you. You
will be required to change this password when you first login.

    CONFIG_NETWORK    Configure the Web administration interface.
    CONSOLE           Start command line console / shell.
    INFO              Display device status / information.
    ↓(+)                                                     60%

                     <  OK  >
```

在出現的視窗中，選擇Yes，然後選擇Enter鍵。

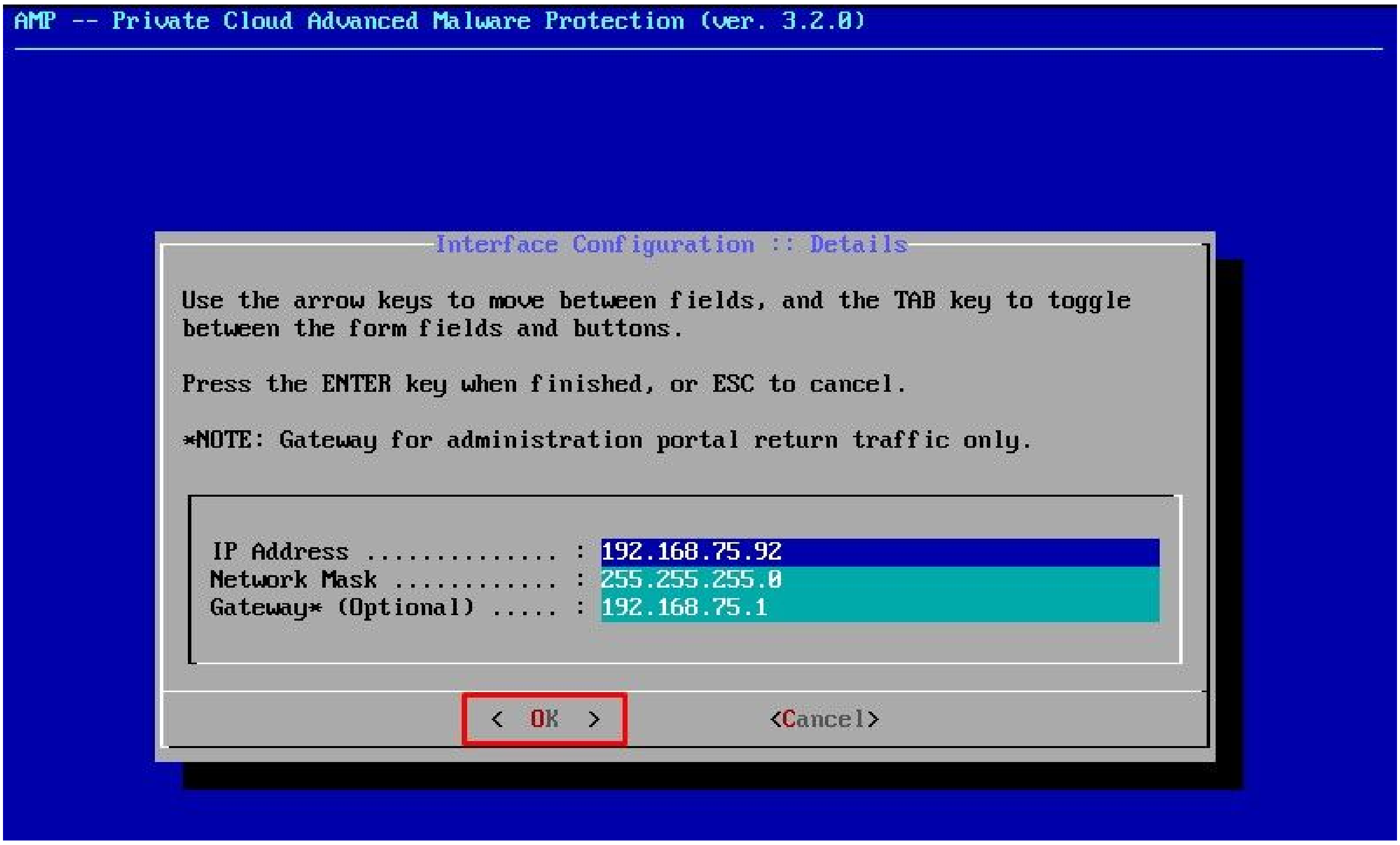


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Apply Your Interface Configuration?

Reconfigure your administration interface with a static configuration?

< Yes >          < No  >
```

如果IP已在使用中，您將使用此錯誤日誌進行處理。只需返回並選擇獨一無二且未使用的產品。



```
Restarting eth0...

ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
==============================================================================
ERROR: The interface failed to reconfigure.
==============================================================================
Press ENTER key to continue...
_
```



AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Interface Configuration :: Details

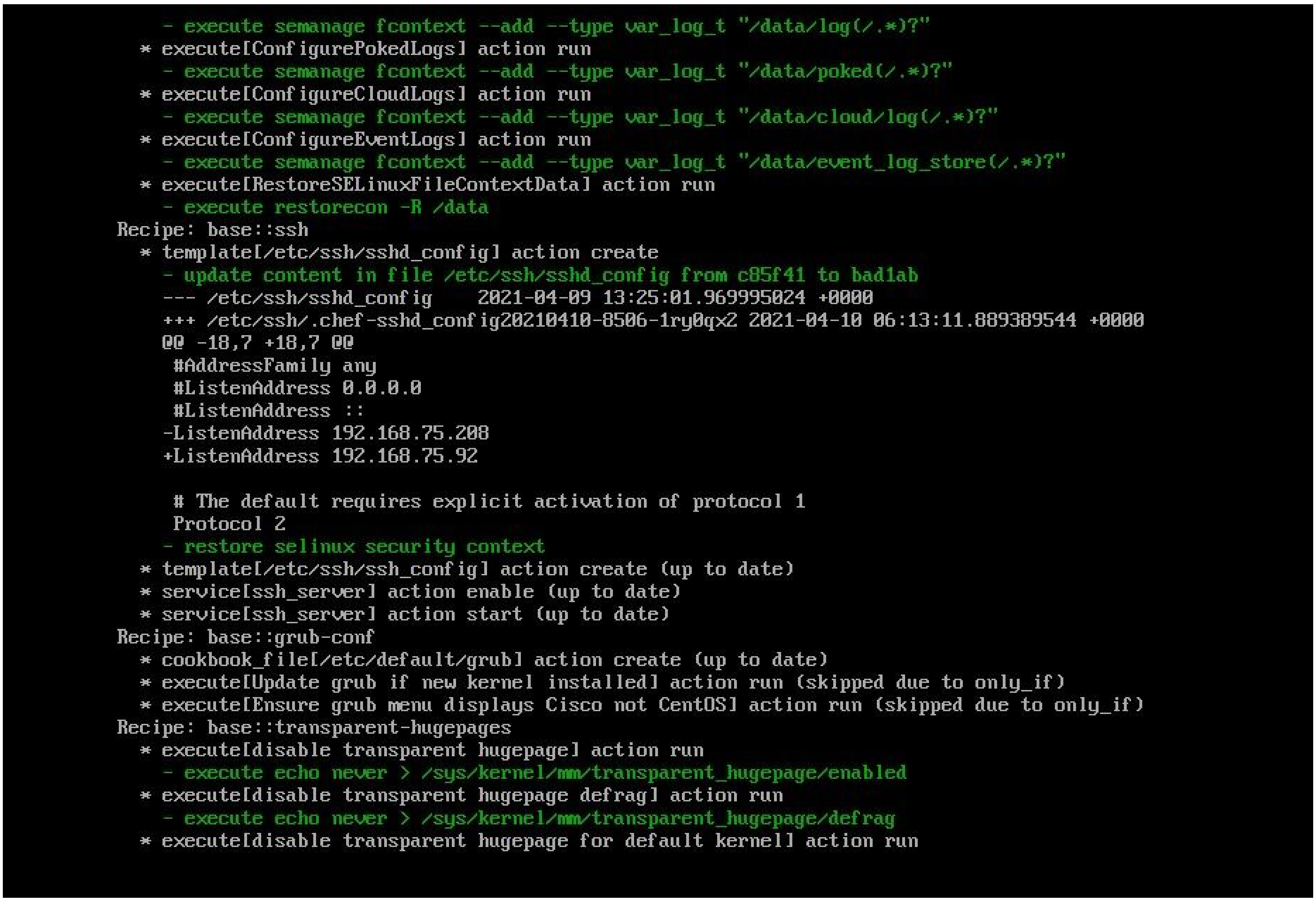
Use the arrow keys to move between fields, and the TAB key to toggle between the form fields and buttons.

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

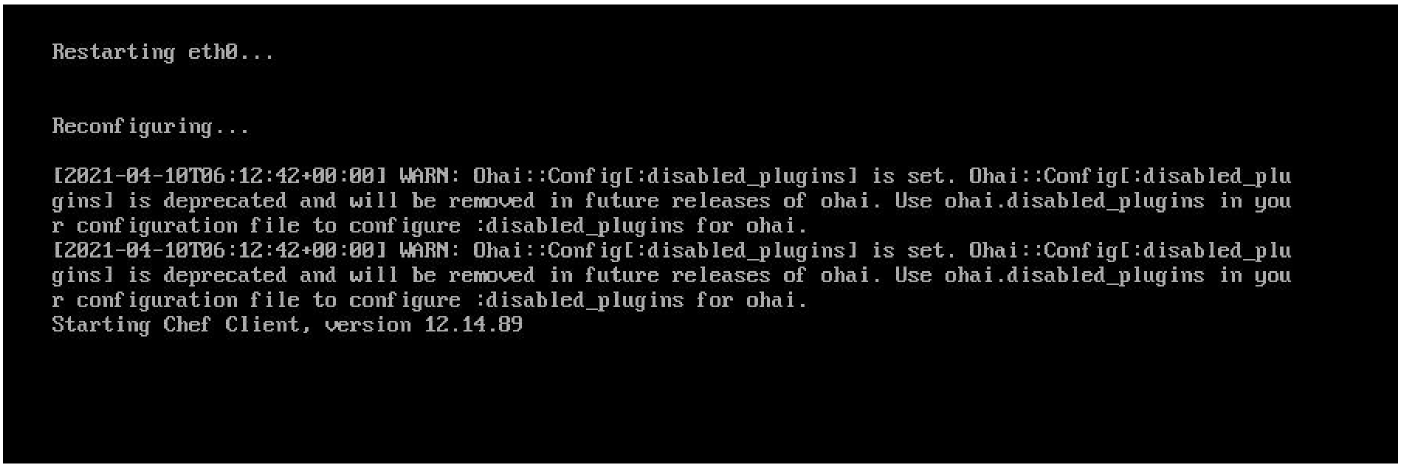
*NOTE: Gateway for administration portal return traffic only.

IP Address .... : 192.168.75.92
Network Mask .... : 255.255.255.0
Gateway* (Optional) ..... : 192.168.75.1

如果一切順利，您會看到如下所示的輸出



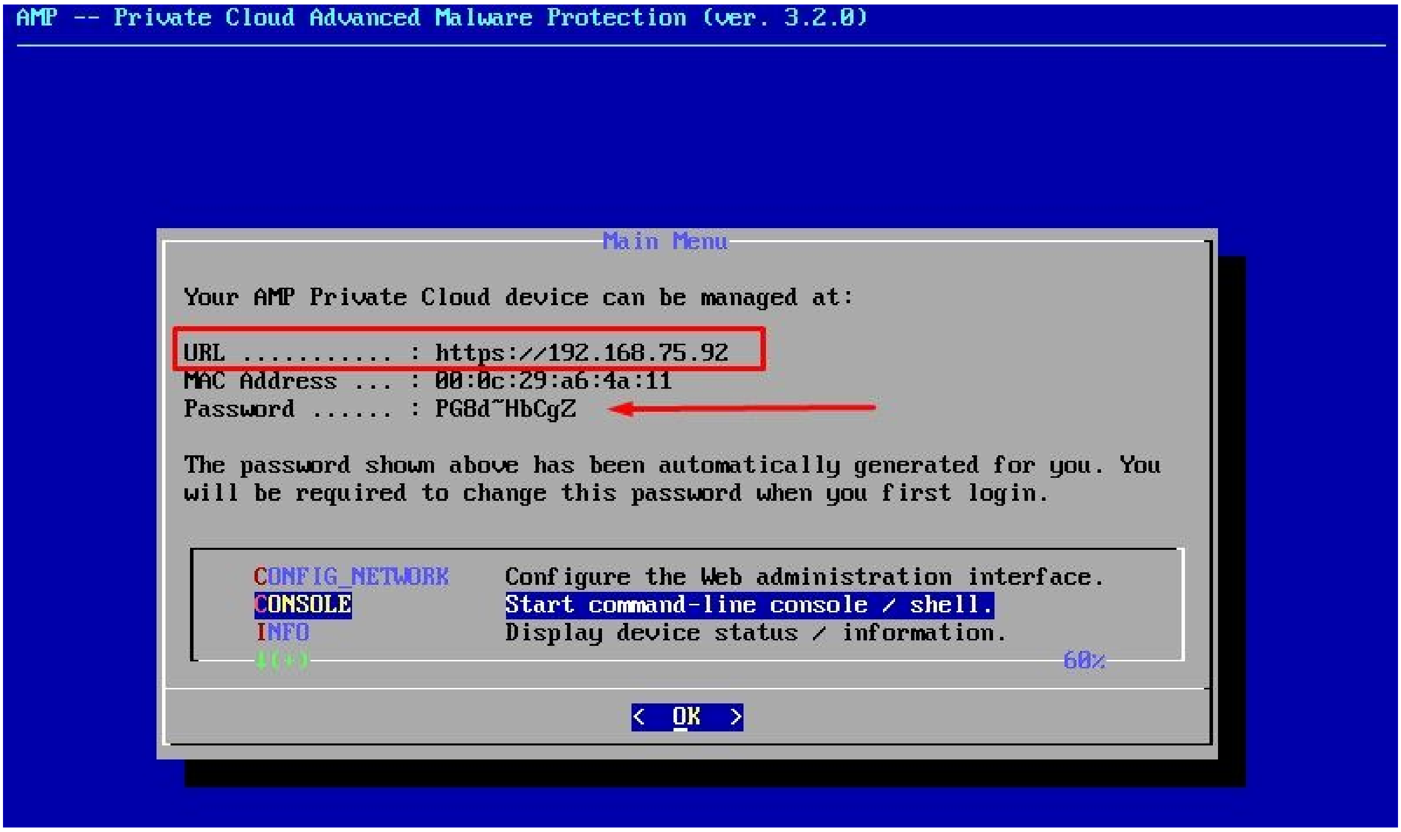
```
    - execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
  * execute[ConfigurePokedLogs] action run
    - execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
  * execute[ConfigureCloudLogs] action run
    - execute semanage fcontext --add --type var_log_t "/data/cloud/log(/.*)?"
  * execute[ConfigureEventLogs] action run
    - execute semanage fcontext --add --type var_log_t "/data/event_log_store(/.*)?"
  * execute[RestoreSELinuxFileContextData] action run
    - execute restorecon -R /data
Recipe: base::ssh
  * template[/etc/ssh/sshd_config] action create
    - update content in file /etc/ssh/sshd_config from c85f41 to bad1ab
    --- /etc/ssh/sshd_config    2021-04-09 13:25:01.969995024 +0000
    +++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.889389544 +0000
    @@ -18,7 +18,7 @@
     #AddressFamily any
     #ListenAddress 0.0.0.0
     #ListenAddress ::
    -ListenAddress 192.168.75.208
    +ListenAddress 192.168.75.92

     # The default requires explicit activation of protocol 1
     Protocol 2
    - restore selinux security context
  * template[/etc/ssh/ssh_config] action create (up to date)
  * service[ssh_server] action enable (up to date)
  * service[ssh_server] action start (up to date)
Recipe: base::grub-conf
  * cookbook_file[/etc/default/grub] action create (up to date)
  * execute[Update grub if new kernel installed] action run (skipped due to only_if)
  * execute[Ensure grub menu displays Cisco not CentOS] action run (skipped due to only_if)
Recipe: base::transparent-hugepages
  * execute[disable transparent hugepage] action run
    - execute echo never > /sys/kernel/mm/transparent_hugepage/enabled
  * execute[disable transparent hugepage defrag] action run
    - execute echo never > /sys/kernel/mm/transparent_hugepage/defrag
  * execute[disable transparent hugepage for default kernel] action run
```



```
Restarting eth0...


Reconfiguring...

[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plu
gins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in you
r configuration file to configure :disabled_plugins for ohai.
[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plu
gins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in you
r configuration file to configure :disabled_plugins for ohai.
Starting Chef Client, version 12.14.89
```

步驟 3:

等待藍色畫面再次彈出您的新靜態IP。另請注意一次性密碼。記下筆記，然後開啟瀏覽器。



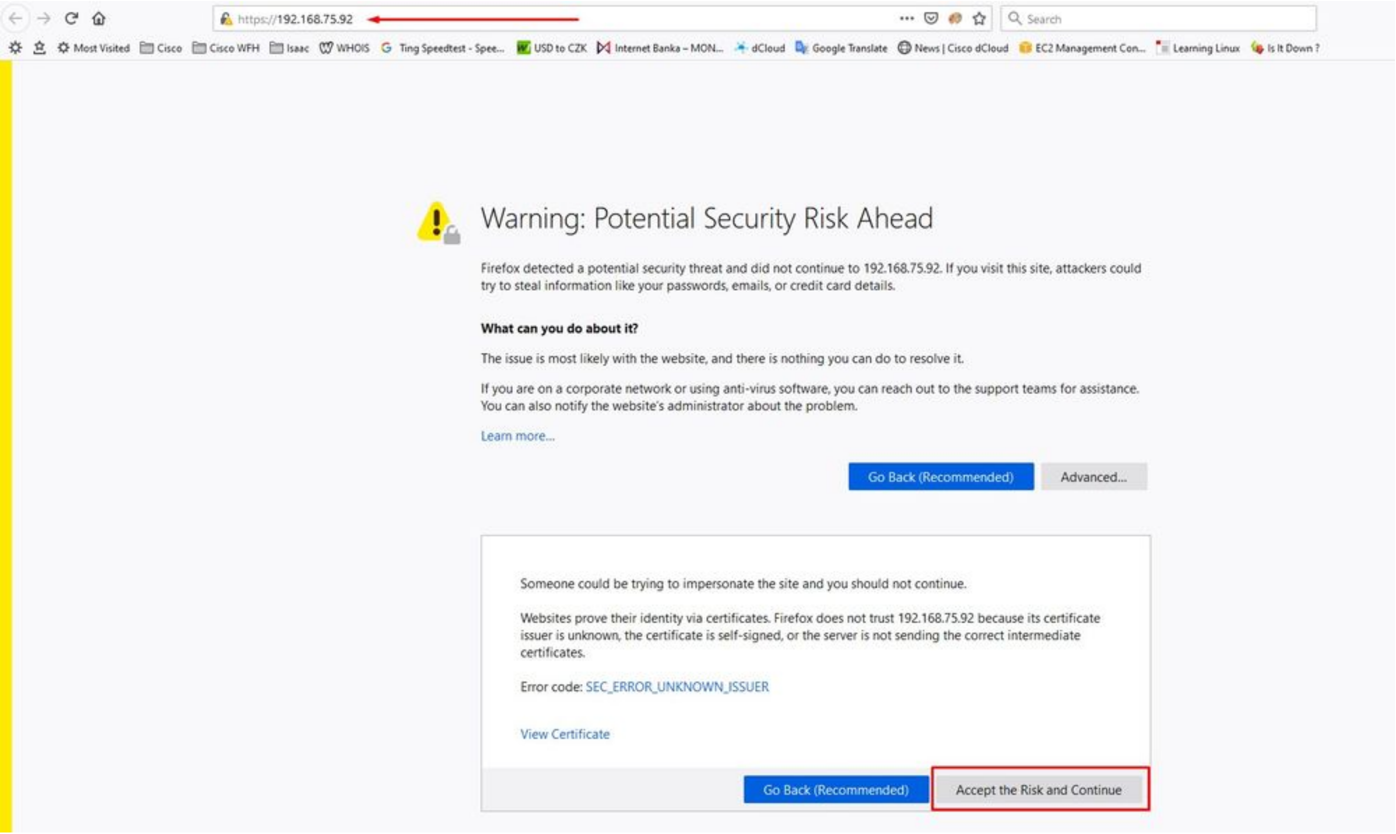
```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

                              Main Menu

 Your AMP Private Cloud device can be managed at:

 URL ........... : https://192.168.75.92
 MAC Address ... : 00:0c:29:a6:4a:11
 Password ...... : PG8d~HbCgZ

 The password shown above has been automatically generated for you. You
 will be required to change this password when you first login.

     CONFIG_NETWORK     Configure the Web administration interface.
     CONSOLE            Start command-line console / shell.
     INFO               Display device status / information.
     ↓(+)                                                   60%

                              < OK >
```

通過Web GUI進行vPC的初始配置

步驟 1:

開啟Web瀏覽器並導航到裝置的管理IP地址。當安全終結點私有雲最初生成其自己的HTTPS證書時，您可能會收到證書錯誤，如下圖所示。將瀏覽器配置為信任安全終端私有雲的自簽名HTTPS證書。

在瀏覽器中，鍵入您之前配置的STATIC IP。



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.75.92. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

Someone could be trying to impersonate the site and you should not continue.

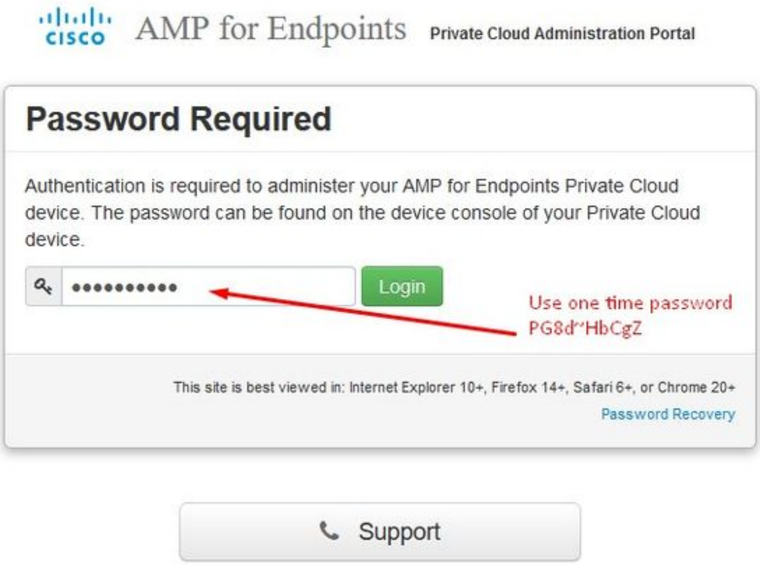
Websites prove their identity via certificates. Firefox does not trust 192.168.75.92 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

步驟 2:

登入後，您需要重置密碼。在Old Password欄位中使用控制檯中的初始密碼。在New Password（新密碼）欄位中使用您的新密碼。在「新密碼」欄位中重新輸入新密碼。在「更改密碼」上選擇。



AMP for Endpoints Private Cloud Administration Portal

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.

Use one time password
PG8d'`HbCgZ

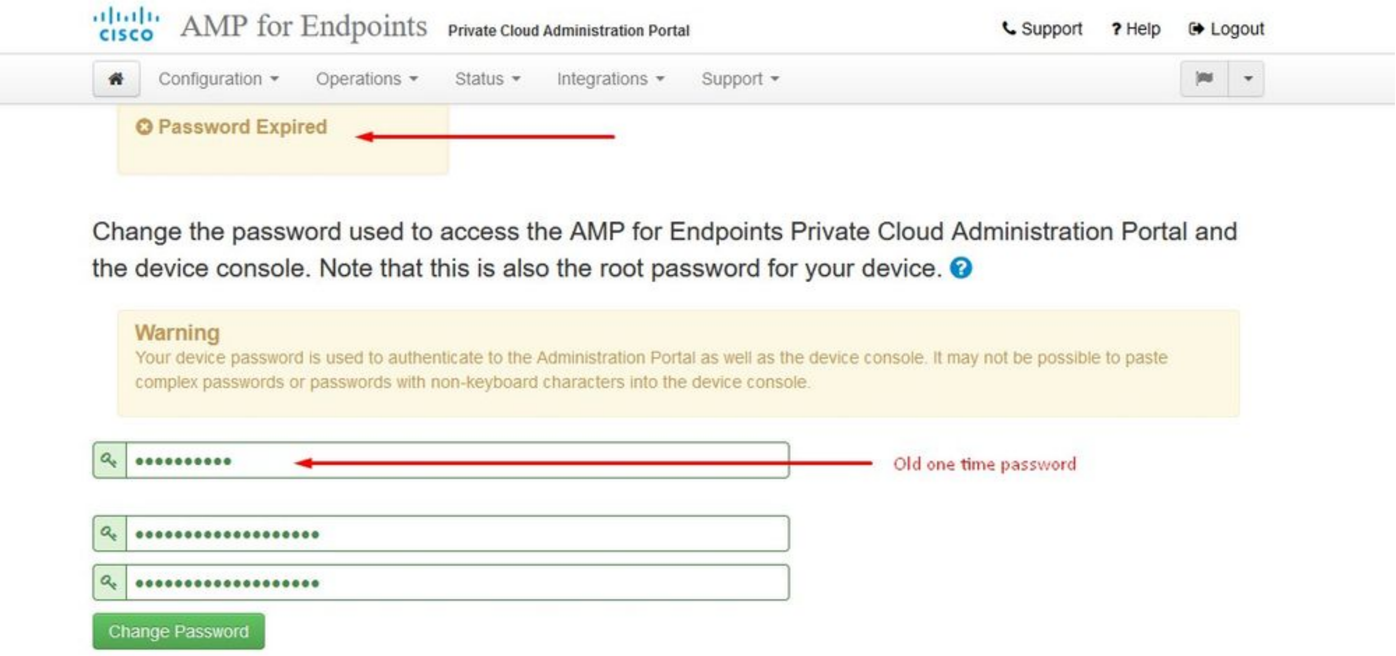
This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

Password Recovery

步驟 3:

登入後，您需要重置密碼。在Old Password欄位中使用控制檯中的初始密碼。在New

Password（新密碼）欄位中使用您的新密碼。在「新密碼」欄位中重新輸入新密碼。在「更改密碼」上選擇。



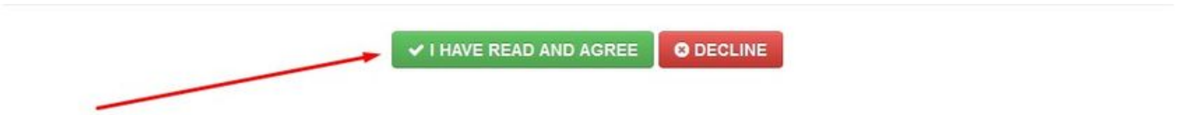
Password Expired

Change the password used to access the AMP for Endpoints Private Cloud Administration Portal and the device console. Note that this is also the root password for your device.

Warning
Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the device console.

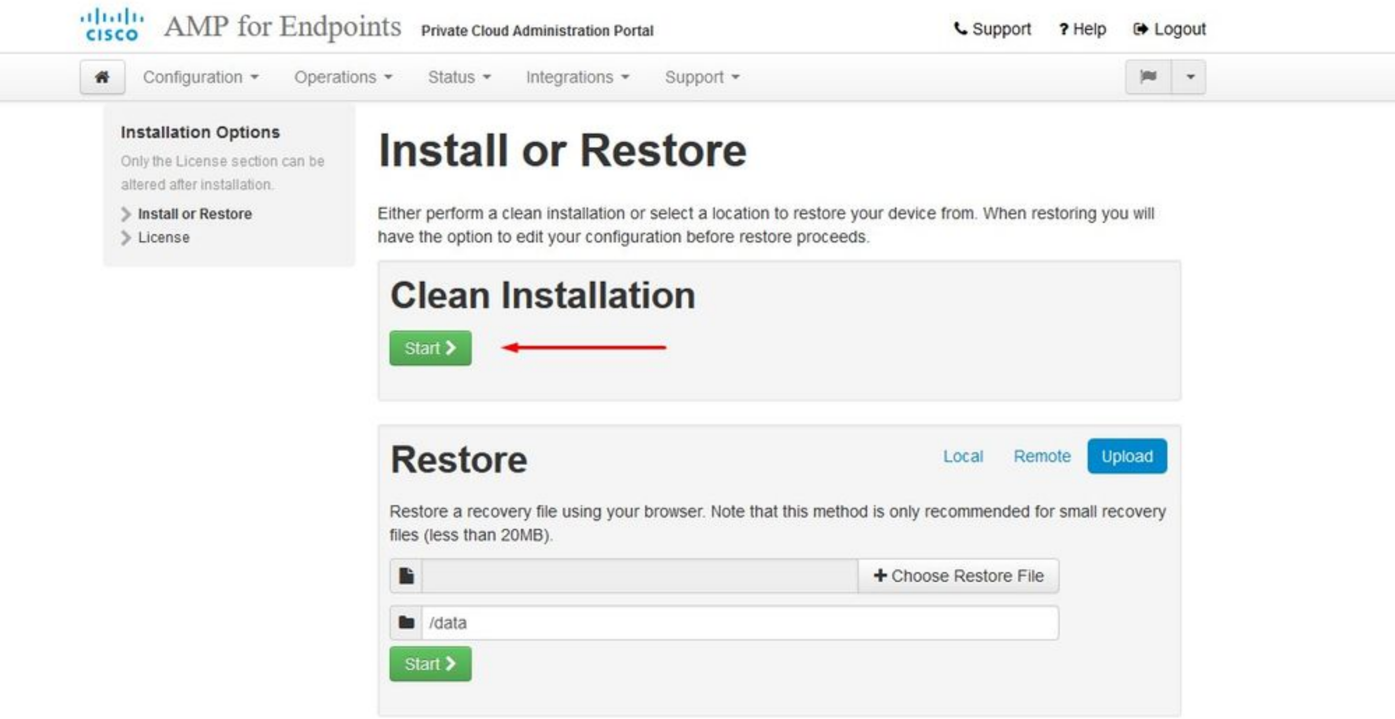
步驟 4:

在下一頁上，向下滾動到底部以接受許可協定。選擇「我已閱讀並同意」。



步驟 5:

接受協定後，您將看到安裝螢幕，如下圖所示。如果要從備份還原，可以在此處進行還原，但是本指南將繼續使用全新安裝選項。在Clean Installation部分中選擇Start。



Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License

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.

Clean Installation

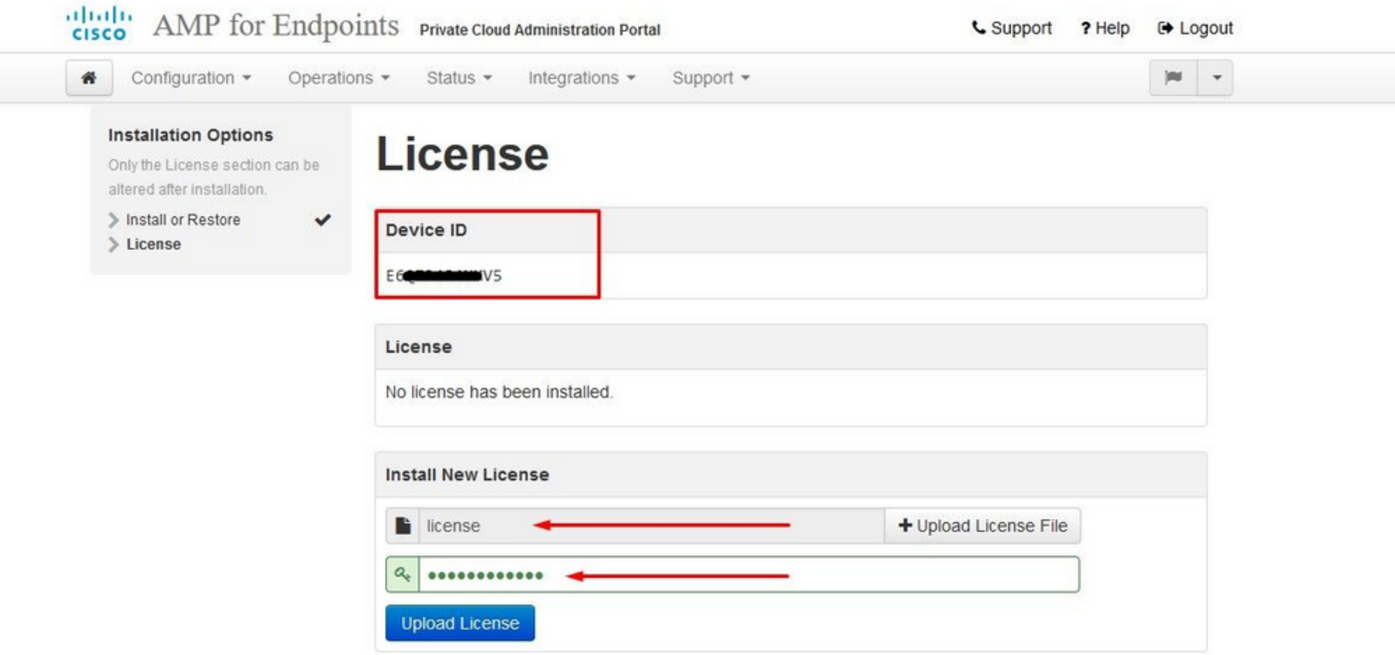
Restore

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

/data

步驟 6:

你首先需要的是前進的許可證。購買產品時您將收到許可證和密碼。選擇on +Upload License File。選擇許可證檔案並輸入密碼短語。在Upload License上選擇。如果上傳失敗，請檢查密碼是否正確。如果上傳成功，則會顯示一個包含有效許可證資訊的螢幕。選擇Next。 如果仍然無法安裝許可證，請聯絡Cisco技術支援。



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License

License

Device ID

E6[redacted]V5

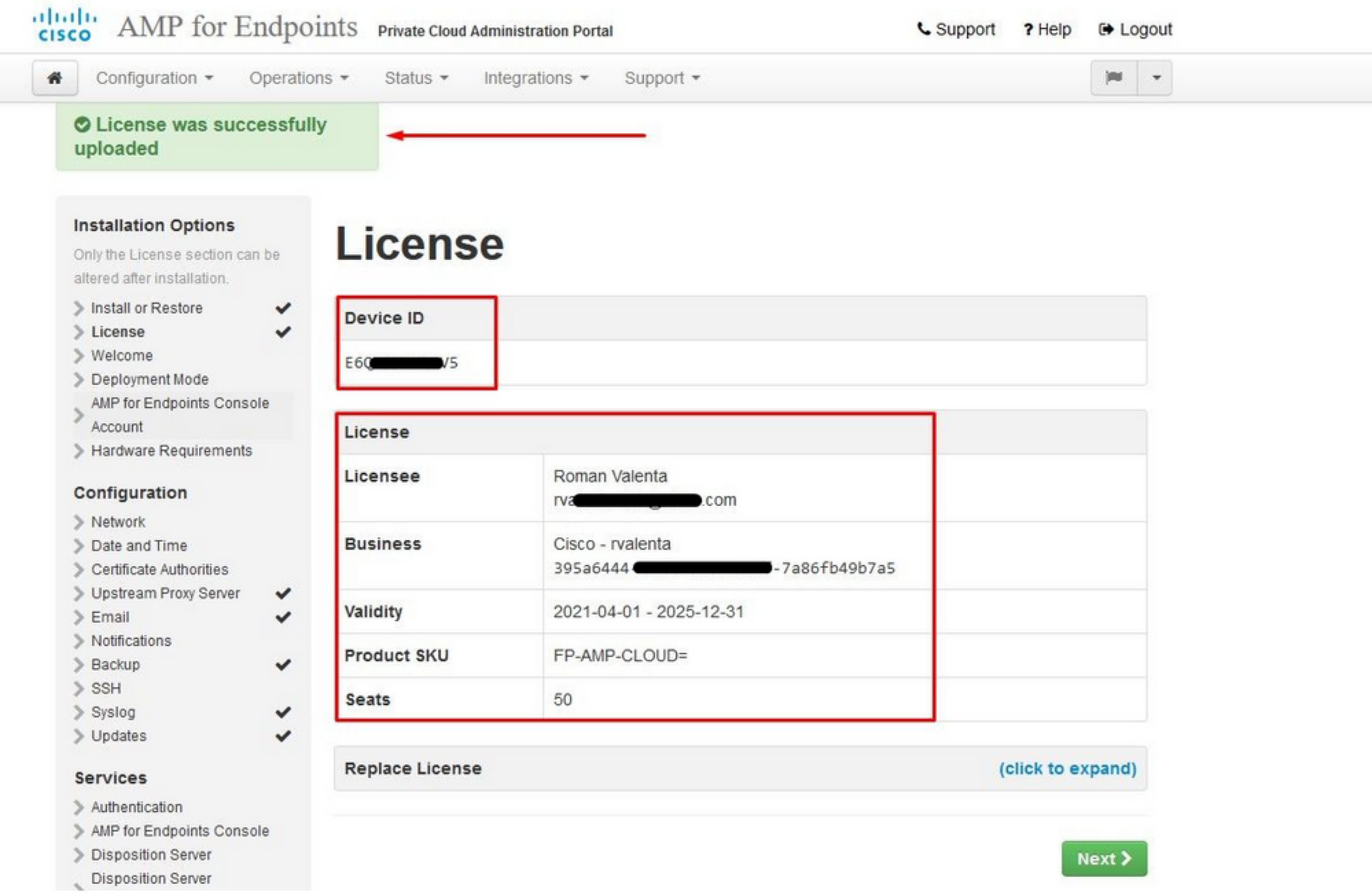
License

No license has been installed.

Install New License

license

•••••••••••••



License was successfully uploaded

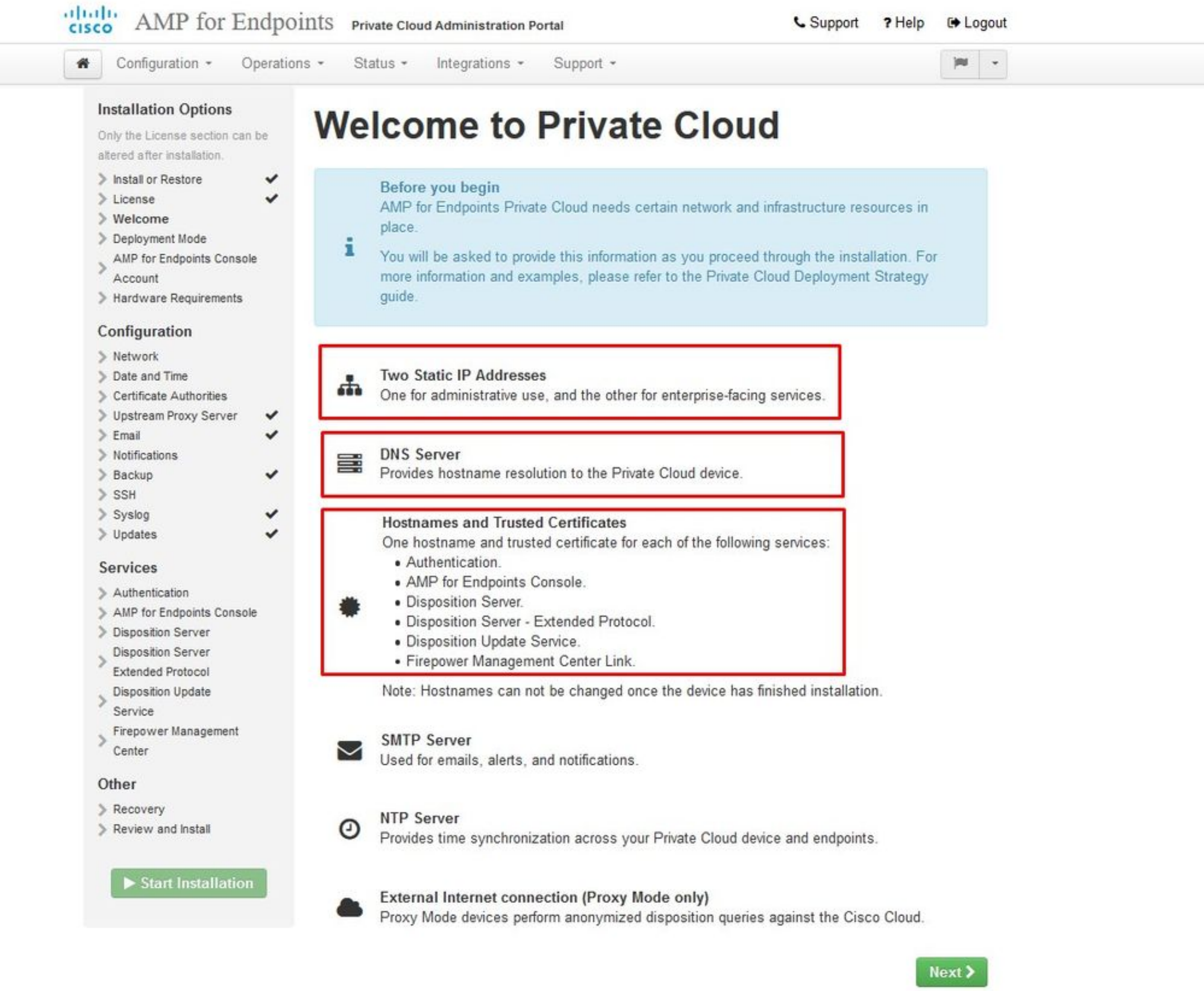
License

Device ID
E60[redacted]V5

License	
Licensee	Roman Valenta rva[redacted].com
Business	Cisco - rvalenta 395a6444[redacted]-7a86fb49b7a5
Validity	2021-04-01 - 2025-12-31
Product SKU	FP-AMP-CLOUD=
Seats	50

步驟 7:

您將收到歡迎頁面，如圖所示。此頁顯示配置私有雲之前必須擁有的資訊。請仔細閱讀要求。選擇Next以啟動安裝前配置。



Welcome to Private Cloud

Before you begin
AMP for Endpoints Private Cloud needs certain network and infrastructure resources in place.

You will be asked to provide this information as you proceed through the installation. For more information and examples, please refer to the Private Cloud Deployment Strategy guide.

Two Static IP Addresses
One for administrative use, and the other for enterprise-facing services.

DNS Server
Provides hostname resolution to the Private Cloud device.

Hostnames and Trusted Certificates
One hostname and trusted certificate for each of the following services:
- Authentication.
- AMP for Endpoints Console.
- Disposition Server.
- Disposition Server - Extended Protocol.
- Disposition Update Service.
- Firepower Management Center Link.

Note: Hostnames can not be changed once the device has finished installation.

SMTP Server
Used for emails, alerts, and notifications.

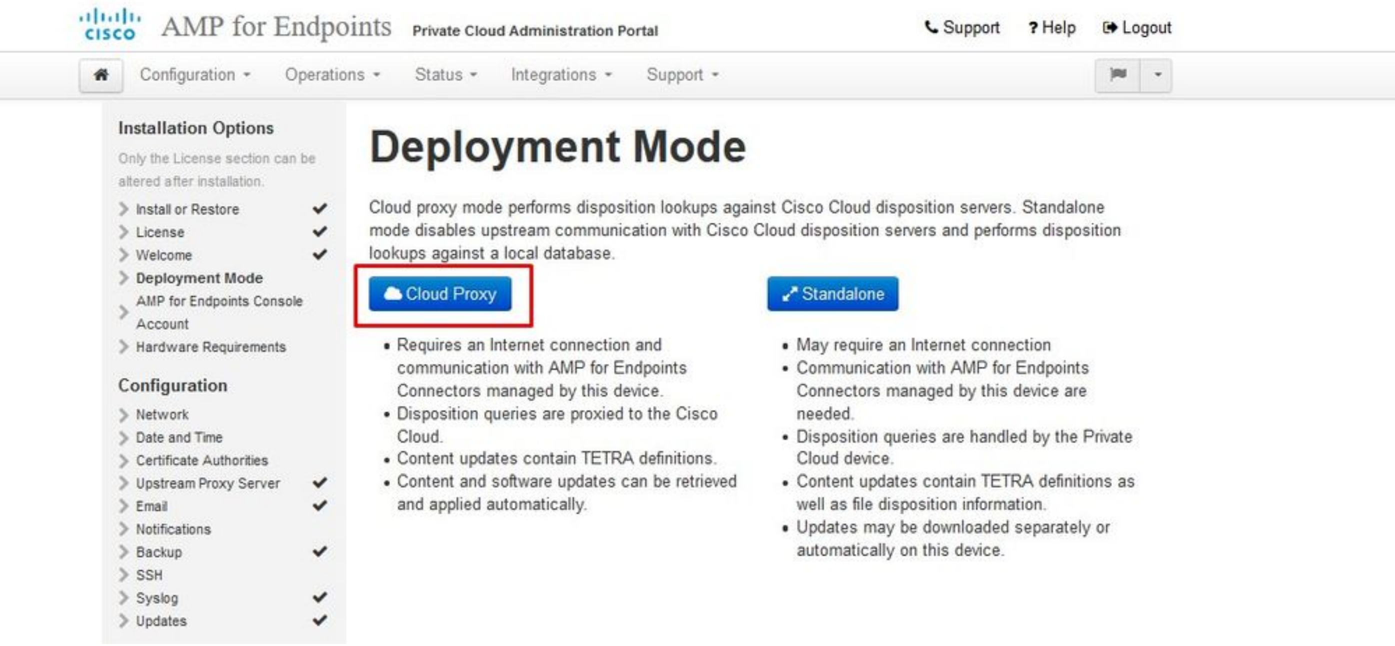
NTP Server
Provides time synchronization across your Private Cloud device and endpoints.

External Internet connection (Proxy Mode only)
Proxy Mode devices perform anonymized disposition queries against the Cisco Cloud.

組態

步驟 1:

註意：請注意，在下一組幻燈片中，我們包含一些獨佔內容，如圖所示，這些內容僅是AIR GAP模式所獨有的，這些內容將被括起來並標籤為AIRGAP ONLY



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode
- AMP for Endpoints Console Account
- Hardware Requirements

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Email ✓
- Notifications
- Backup ✓
- SSH
- Syslog ✓
- Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

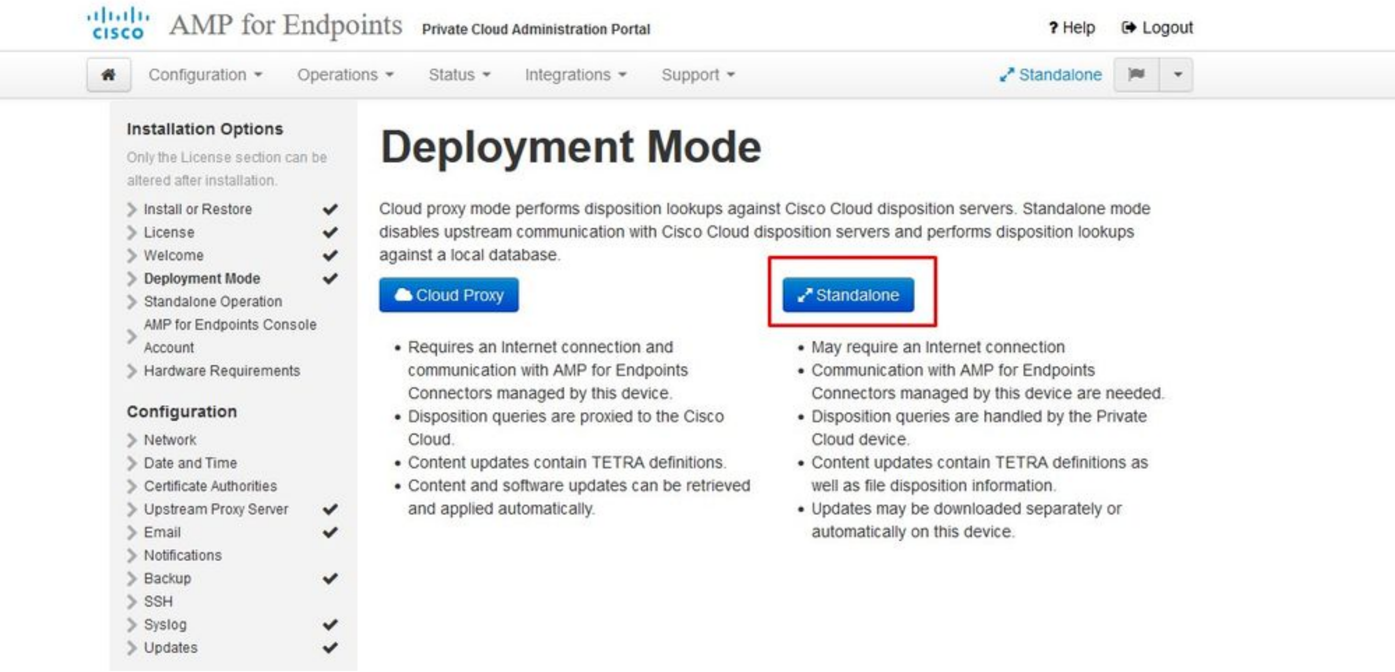
Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require 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.

︾︾ AIRGAP ONLY ︾︾



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- Standalone Operation
- AMP for Endpoints Console Account
- Hardware Requirements

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Email ✓
- Notifications
- Backup ✓
- SSH
- Syslog ✓
- Updates ✓

Deployment Mode

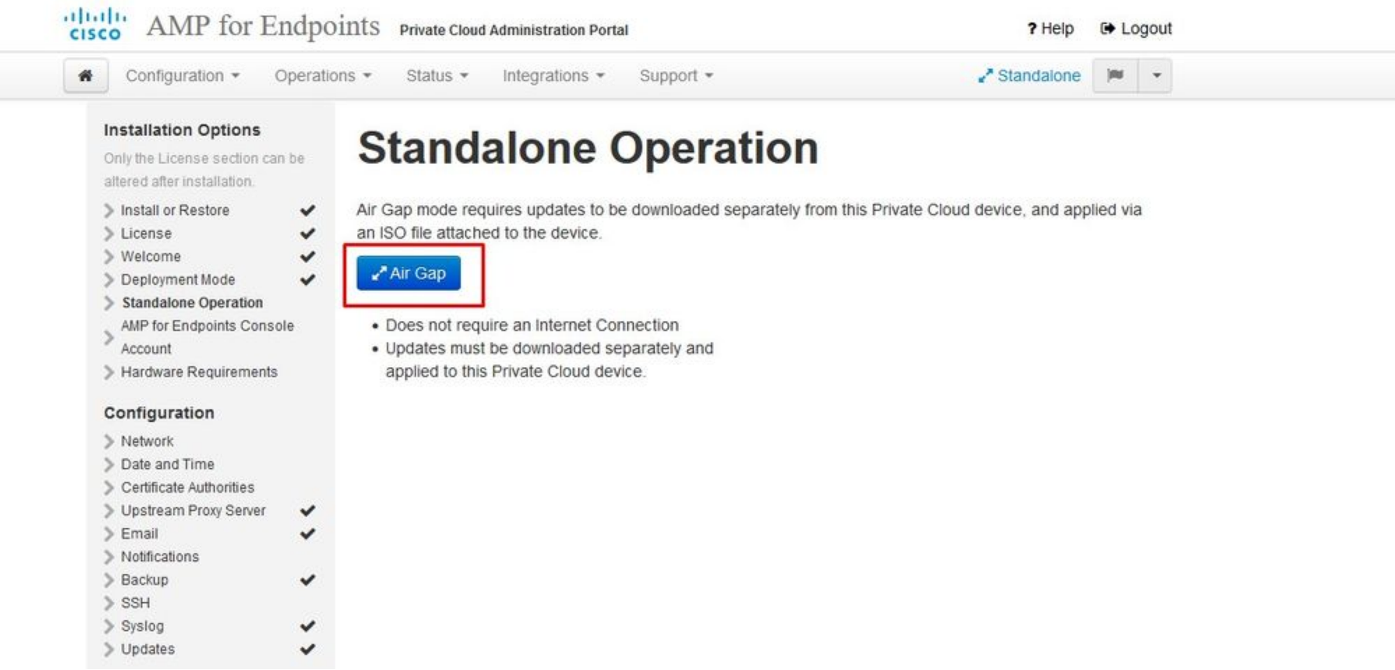
Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require 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.



Standalone Operation

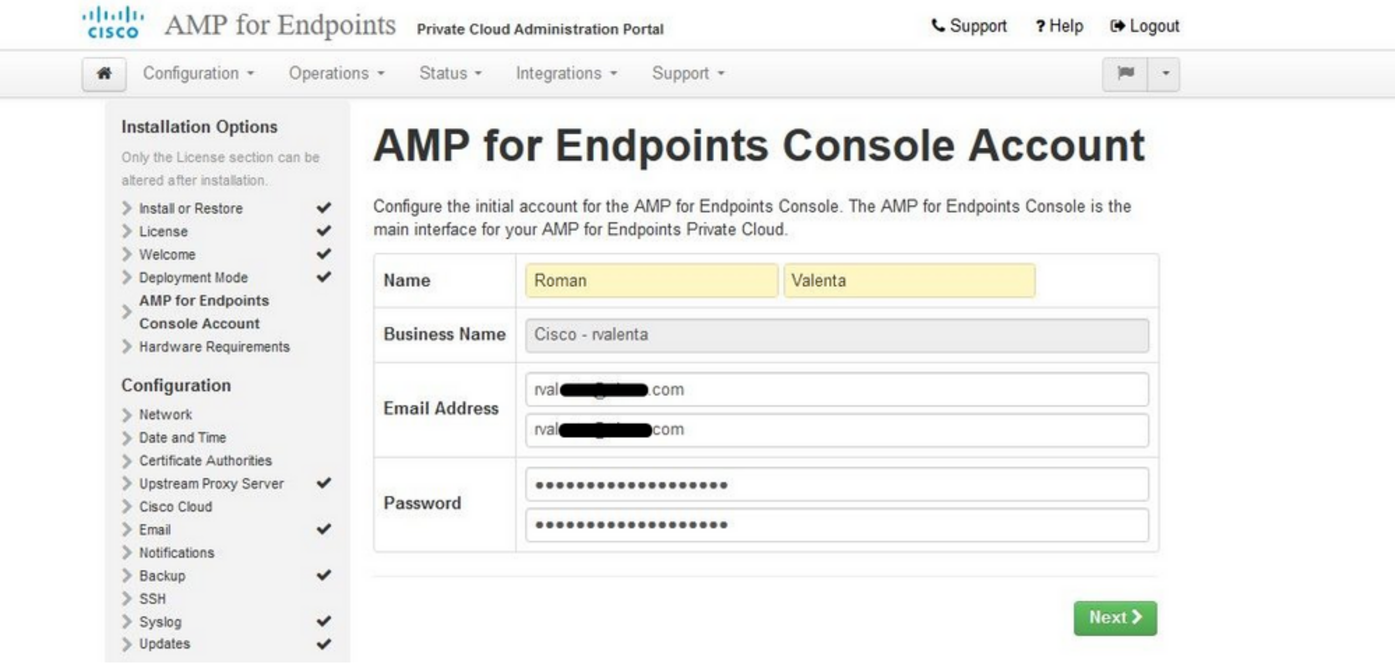
Air Gap mode requires updates to be downloaded separately from this Private Cloud device, and applied via an ISO file attached to the device.

- Does not require an Internet Connection
- Updates must be downloaded separately and applied to this Private Cloud device.

僅︽︽︽AIRGAP ︽

步驟 2:

導航到Secure Endpoint Console Account頁。控制檯使用管理使用者來建立策略、電腦組並新增其他使用者。輸入控制檯帳戶的名稱、電子郵件地址和密碼。選擇Next。



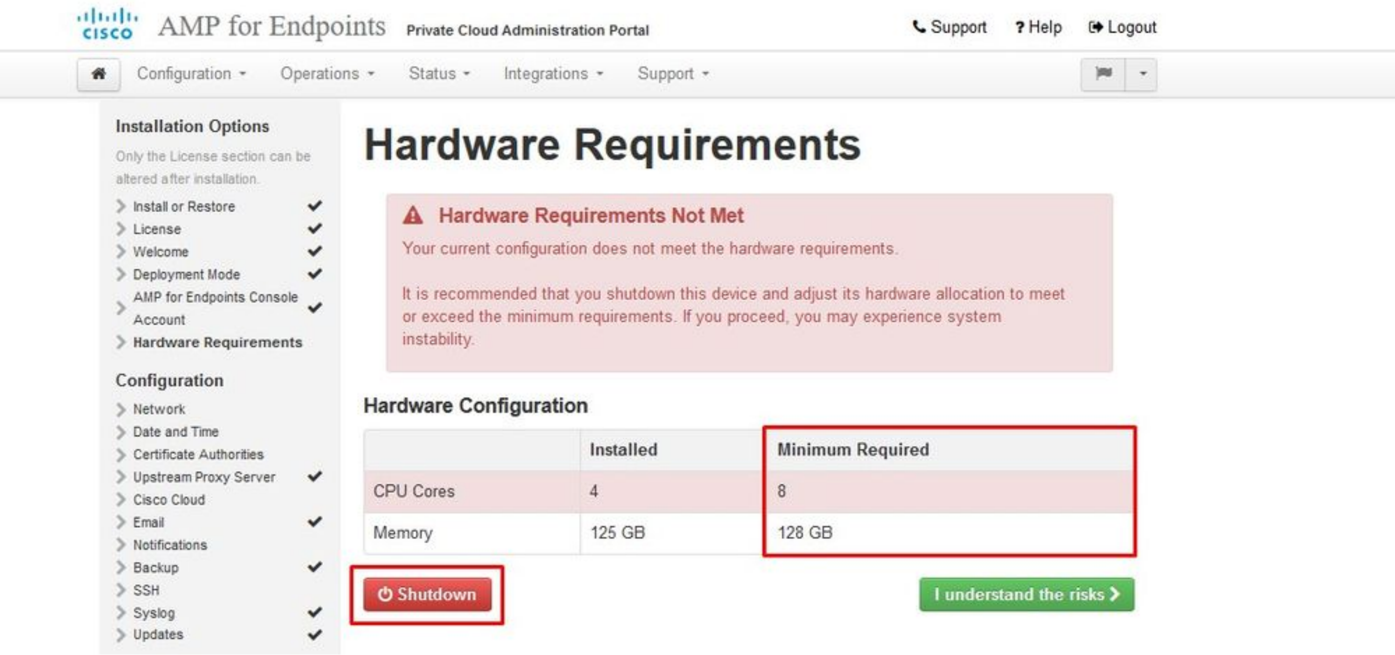
AMP for Endpoints Console Account

Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

Name	Roman Valenta
Business Name	Cisco - rvalenta
Email Address	rval[redacted].com rval[redacted]com
Password	••••••••••••••••••• •••••••••••••••••••

如果您在從OVA檔案部署時遇到此問題，則有兩個選擇：稍後繼續並修復此問題，或者關閉以便部署虛擬機器並進行相應調整。重新啟動後，繼續原來的位置。

註：這已在OVA檔案中修復，用於3.5.2版，該版本使用128GB RAM和8CPU核心正確載入



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Cisco Cloud
- Email ✓
- Notifications
- Backup ✓
- SSH
- Syslog ✓
- Updates ✓

Hardware Requirements

Hardware Requirements Not Met

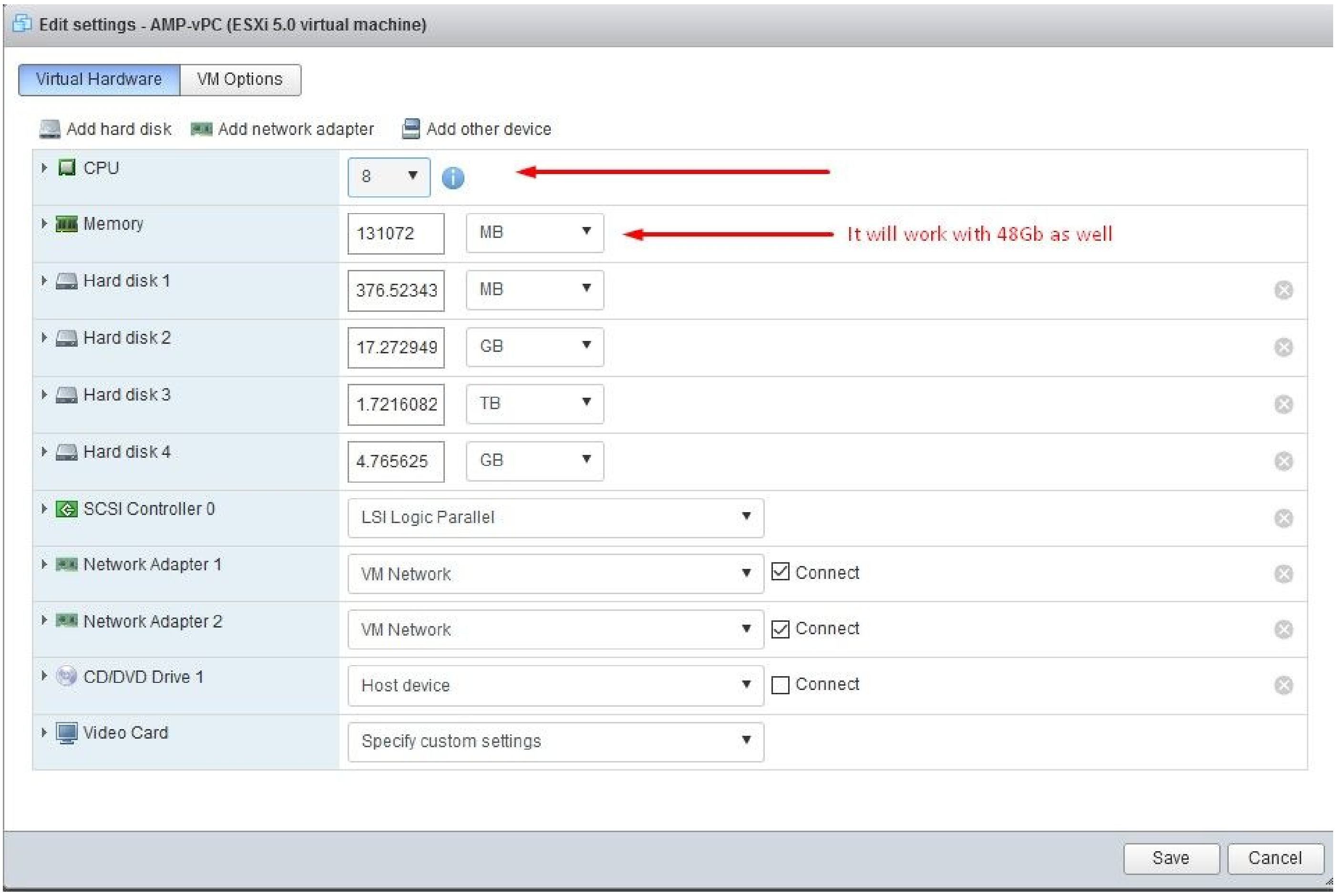
Your current configuration does not meet the hardware requirements.

It is recommended that you shutdown this device and adjust its hardware allocation to meet or exceed the minimum requirements. If you proceed, you may experience system instability.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	4	8
Memory	125 GB	128 GB

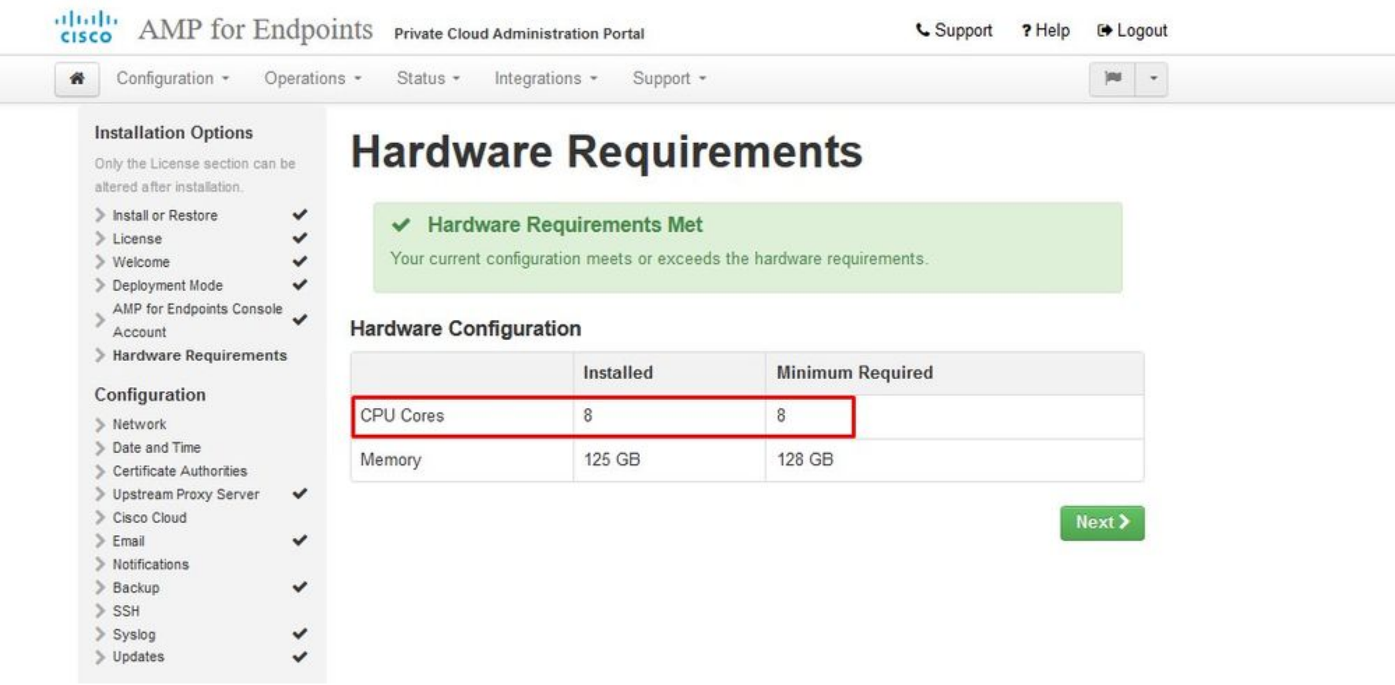
注意：僅使用推薦值，除非用於實驗



Edit settings - AMP-vPC (ESXi 5.0 virtual machine)

CPU	8	
Memory	131072 MB	It will work with 48Gb as well
Hard disk 1	376.52343 MB	
Hard disk 2	17.272949 GB	
Hard disk 3	1.7216082 TB	
Hard disk 4	4.765625 GB	
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	VM Network	☑ Connect
Network Adapter 2	VM Network	☑ Connect
CD/DVD Drive 1	Host device	□ Connect
Video Card	Specify custom settings	

重新引導後，我們繼續原來的位置。



Hardware Requirements

✓ Hardware Requirements Met

Your current configuration meets or exceeds the hardware requirements.

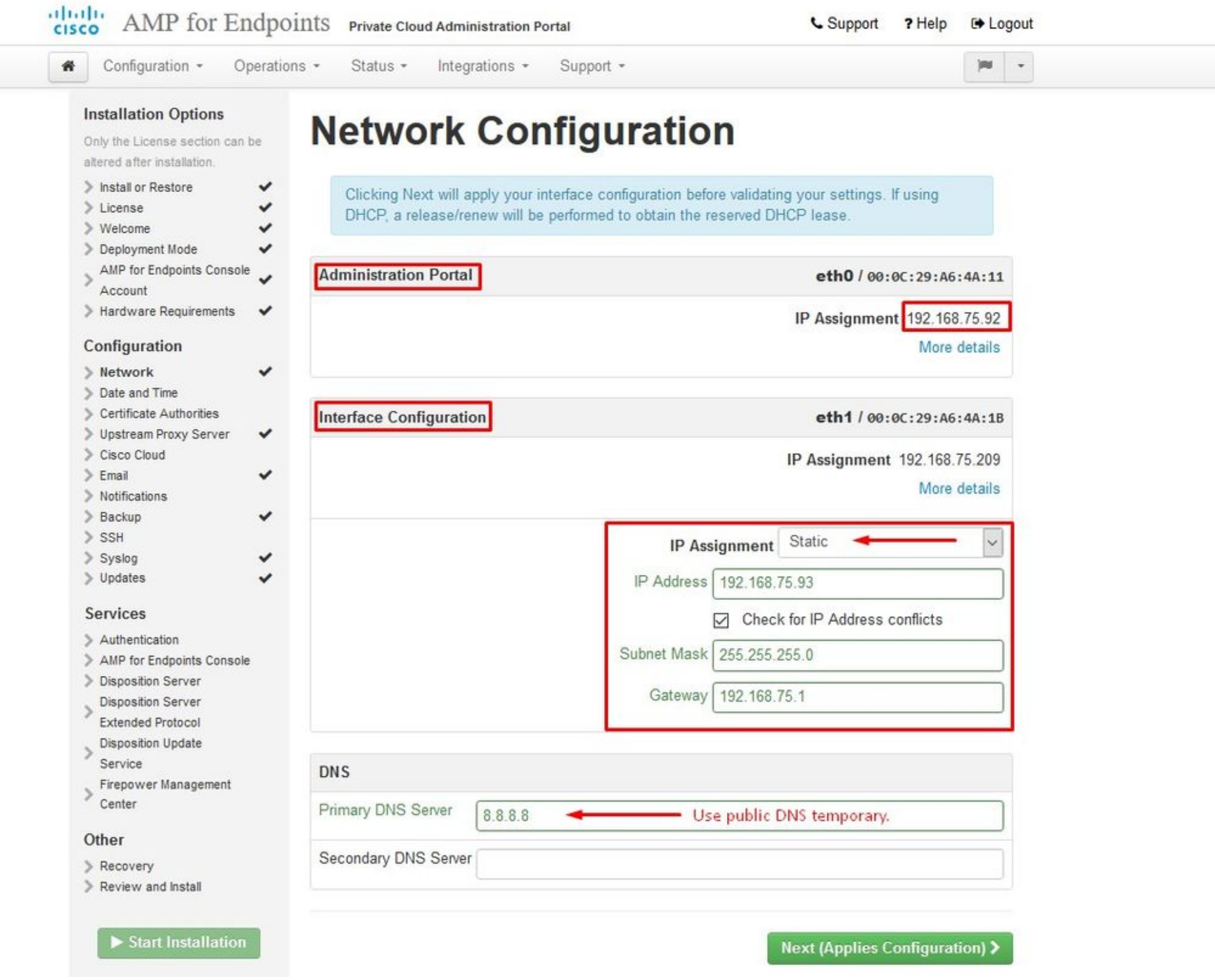
Hardware Configuration

	Installed	Minimum Required
CPU Cores	8	8
Memory	125 GB	128 GB

確保也使用靜態IP配置ETH1。

注意：除非您已為介面建立了MAC地址保留，否則永遠不能將裝置配置為使用DHCP。如果介面的IP地址發生更改，則可能會導致所部署的安全端點聯結器出現嚴重問題。如果未配置DNS伺服器，您可以使用公共DNS臨時服務器完成安裝。

步驟 3:



Network Configuration

Clicking Next will apply your interface configuration before validating your settings. If using DHCP, a release/renew will be performed to obtain the reserved DHCP lease.

Administration Portal — eth0 / 00:0C:29:A6:4A:11

IP Assignment 192.168.75.92

More details

Interface Configuration — eth1 / 00:0C:29:A6:4A:1B

IP Assignment 192.168.75.209

More details

IP Assignment: Static

IP Address: 192.168.75.93

☑ Check for IP Address conflicts

Subnet Mask: 255.255.255.0

Gateway: 192.168.75.1

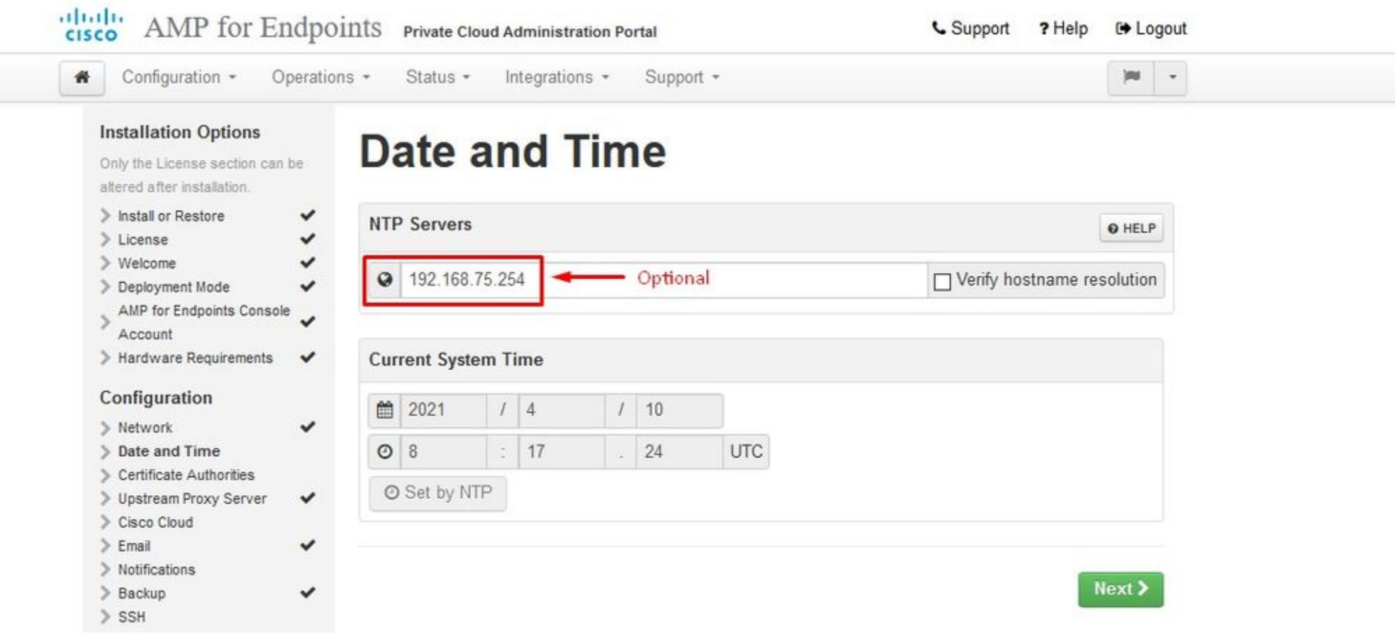
DNS

Primary DNS Server: 8.8.8.8 — Use public DNS temporary.

Secondary DNS Server:

步驟 4:

您將看到「日期和時間」頁面。輸入要用於日期和時間同步的一個或多個NTP伺服器的地址。您可以使用內部或外部NTP伺服器，並指定多個逗號或空格分隔清單。將時間與瀏覽器同步，或從裝置控制檯運行amp-ctl ntpdate以強制與NTP伺服器進行即時時間同步。選擇Next。



AMP for Endpoints Private Cloud Administration Portal

Support | ? Help | Logout

Configuration ▾ | Operations ▾ | Status ▾ | Integrations ▾ | Support ▾

Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements ✓

Configuration

- Network ✓
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Cisco Cloud
- Email ✓
- Notifications
- Backup ✓
- SSH

Date and Time

NTP Servers — HELP

192.168.75.254 ← Optional

□ Verify hostname resolution

Current System Time

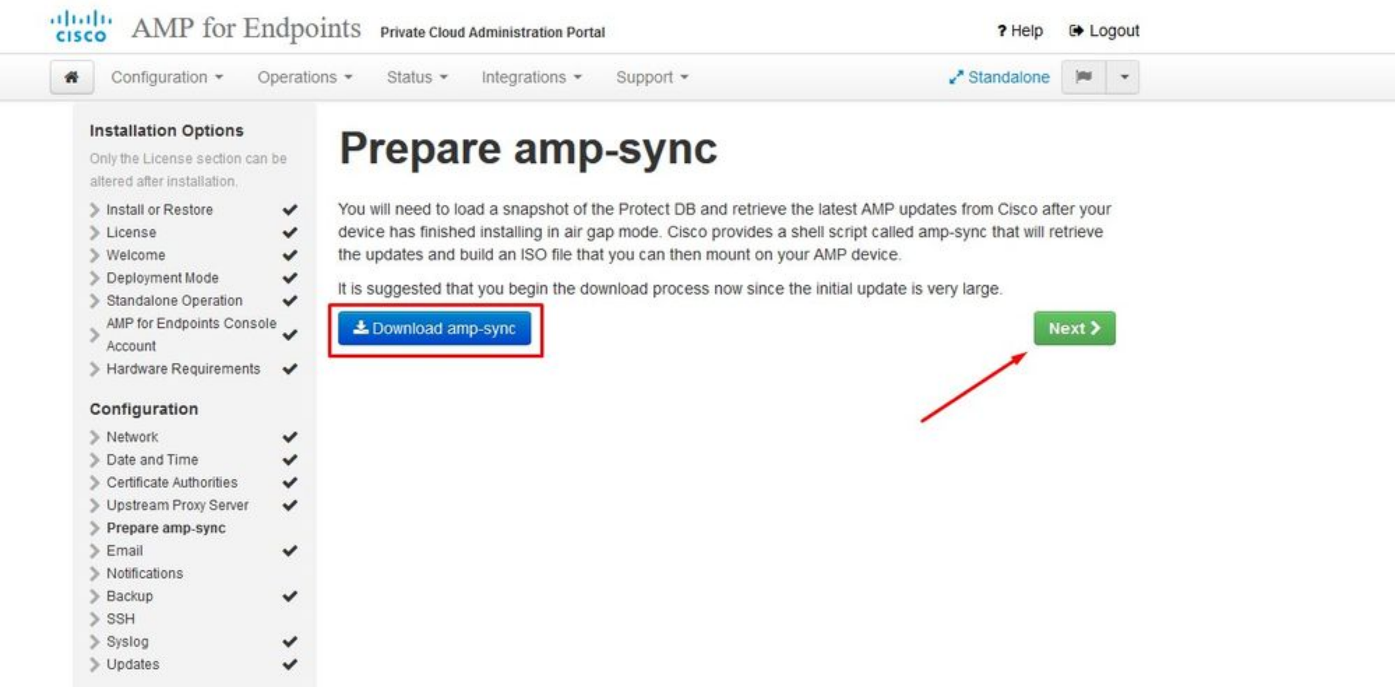
2021 / 4 / 10

8 : 17 . 24 UTC

Set by NTP

Next >

︾︾AIRGAP ONLY︾︾



AMP for Endpoints Private Cloud Administration Portal

? Help | Logout

Configuration ▾ | Operations ▾ | Status ▾ | Integrations ▾ | Support ▾ | Standalone

Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- Standalone Operation ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements ✓

Configuration

- Network ✓
- Date and Time ✓
- Certificate Authorities ✓
- Upstream Proxy Server ✓
- Prepare amp-sync
- Email ✓
- Notifications
- Backup ✓
- SSH
- Syslog ✓
- Updates ✓

Prepare amp-sync

You will need to load a snapshot of the Protect DB and retrieve the latest AMP updates from Cisco after your device has finished installing in air gap mode. Cisco provides a shell script called amp-sync that will retrieve the updates and build an ISO file that you can then mount on your AMP device.

It is suggested that you begin the download process now since the initial update is very large.

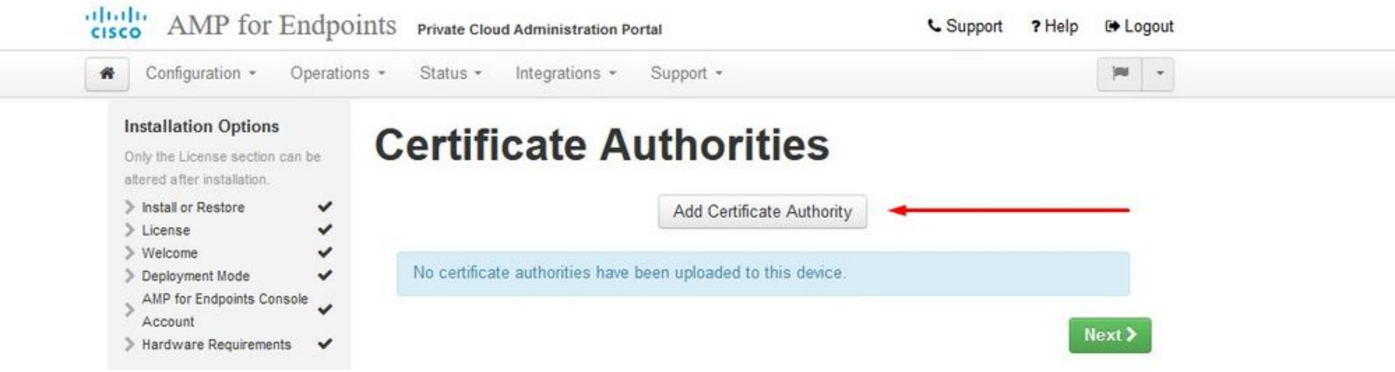
Download amp-sync

Next >

僅︽︽︽AIRGAP︽

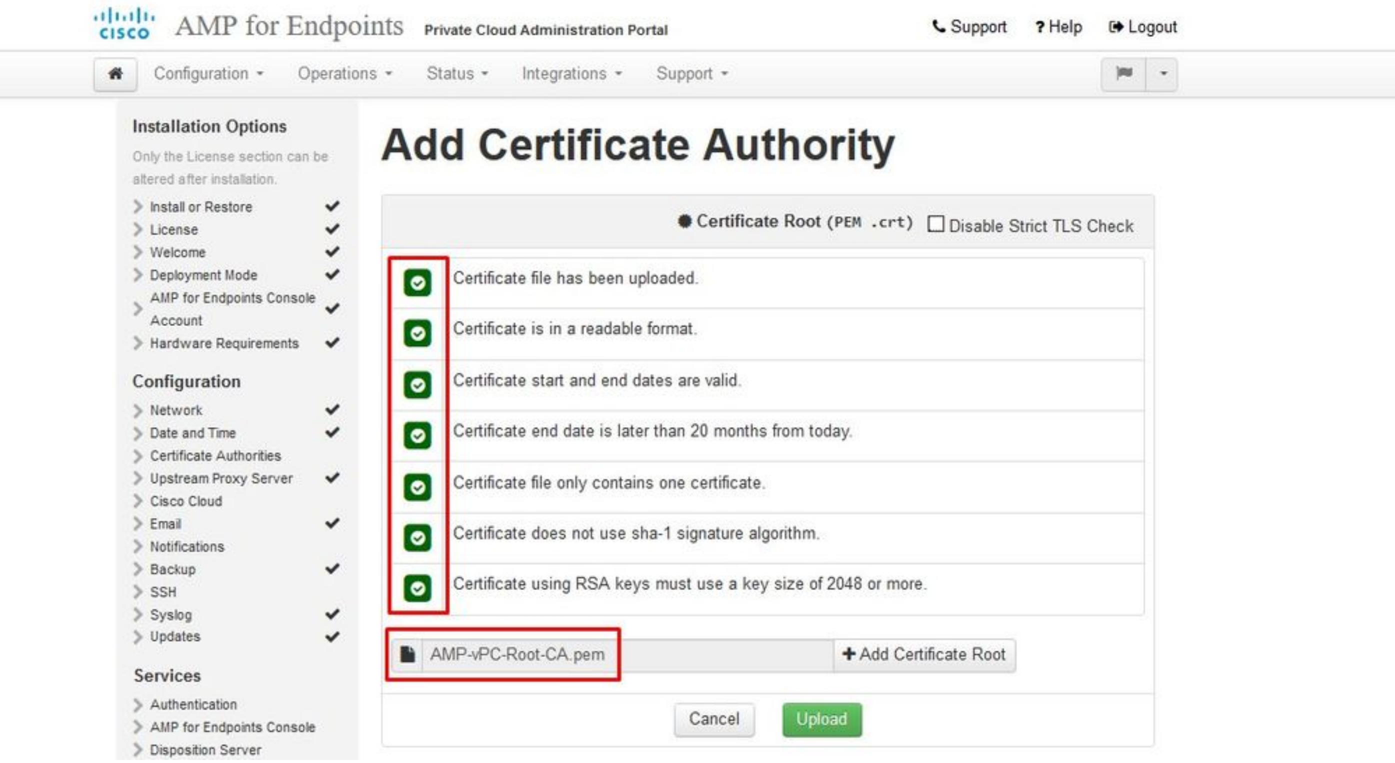
步驟 5:

您將看到「Certificate Authorities」頁面，如下圖所示。在Add Certificate Authority上選擇以新增根證書。


AMP for Endpoints Private Cloud Administration Portal
Support
? Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore ✓
License ✓
Welcome ✓
Deployment Mode ✓
AMP for Endpoints Console Account ✓
Hardware Requirements ✓
Add Certificate Authority
Next

Certificate Authorities

No certificate authorities have been uploaded to this device.



Add Certificate Authority

● Certificate Root (PEM .crt) □ Disable Strict TLS Check

✓ Certificate file has been uploaded.

✓ Certificate is in a readable format.

✓ Certificate start and end dates are valid.

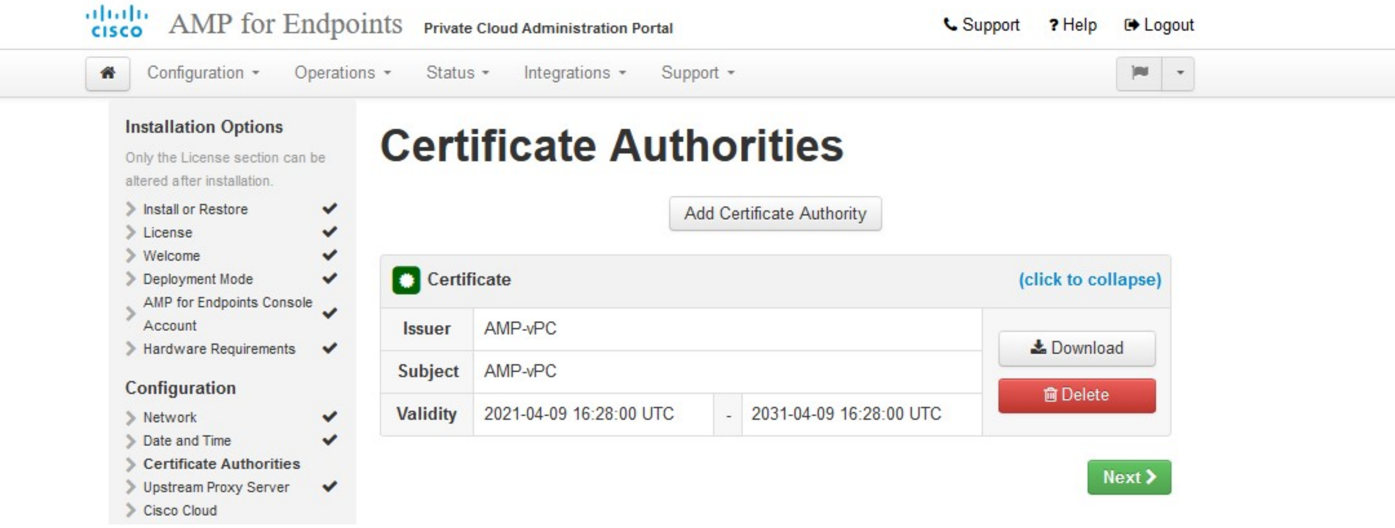
✓ Certificate end date is later than 20 months from today.

✓ Certificate file only contains one certificate.

✓ Certificate does not use sha-1 signature algorithm.

✓ Certificate using RSA keys must use a key size of 2048 or more.

AMP-vPC-Root-CA.pem



Certificate Authorities

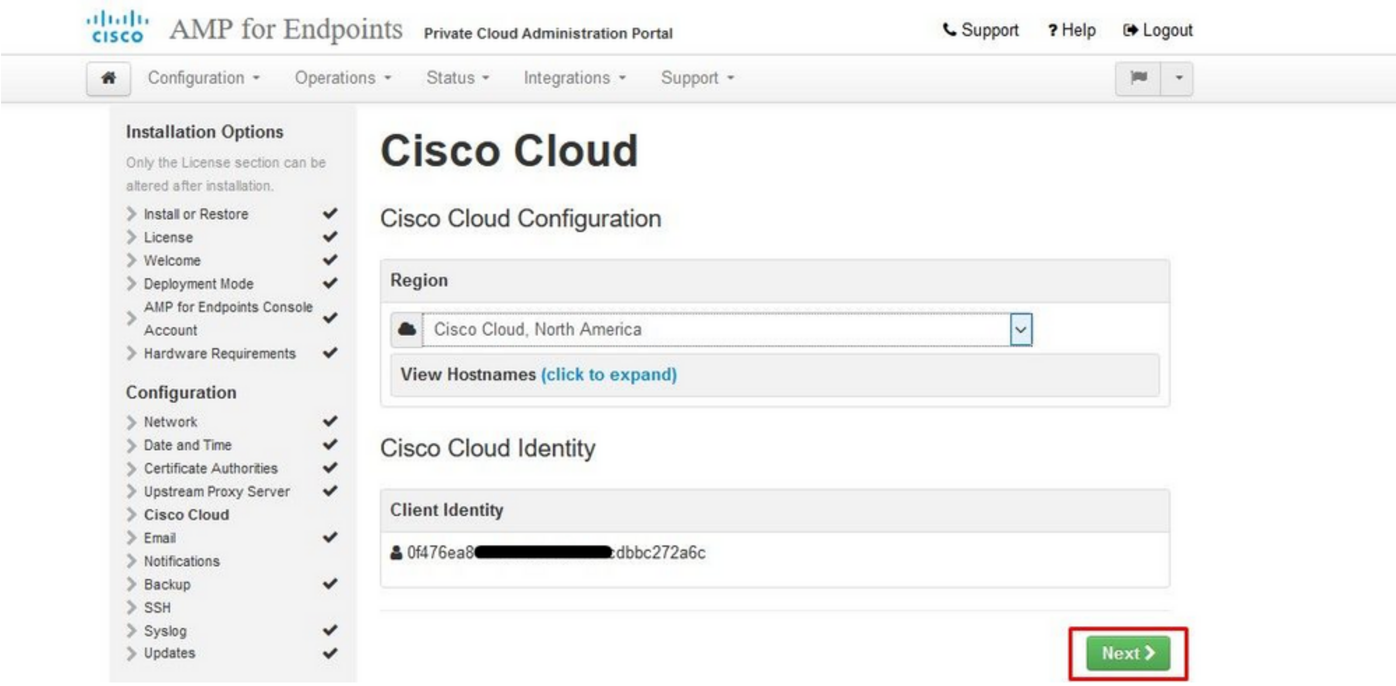
Certificate

Issuer	AMP-vPC		
Subject	AMP-vPC		
Validity	2021-04-09 16:28:00 UTC	-	2031-04-09 16:28:00 UTC

步驟 6:

下一步是設定Cisco Cloud頁面，如下圖所示。選擇適當的思科雲區域。如果需要為安全終結點私有雲裝置建立防火牆例外，以便與思科雲進行通訊以查詢檔案和更新裝置，請展開檢視主機名。選擇

Next。



Cisco Cloud

Cisco Cloud Configuration

Region: Cisco Cloud, North America

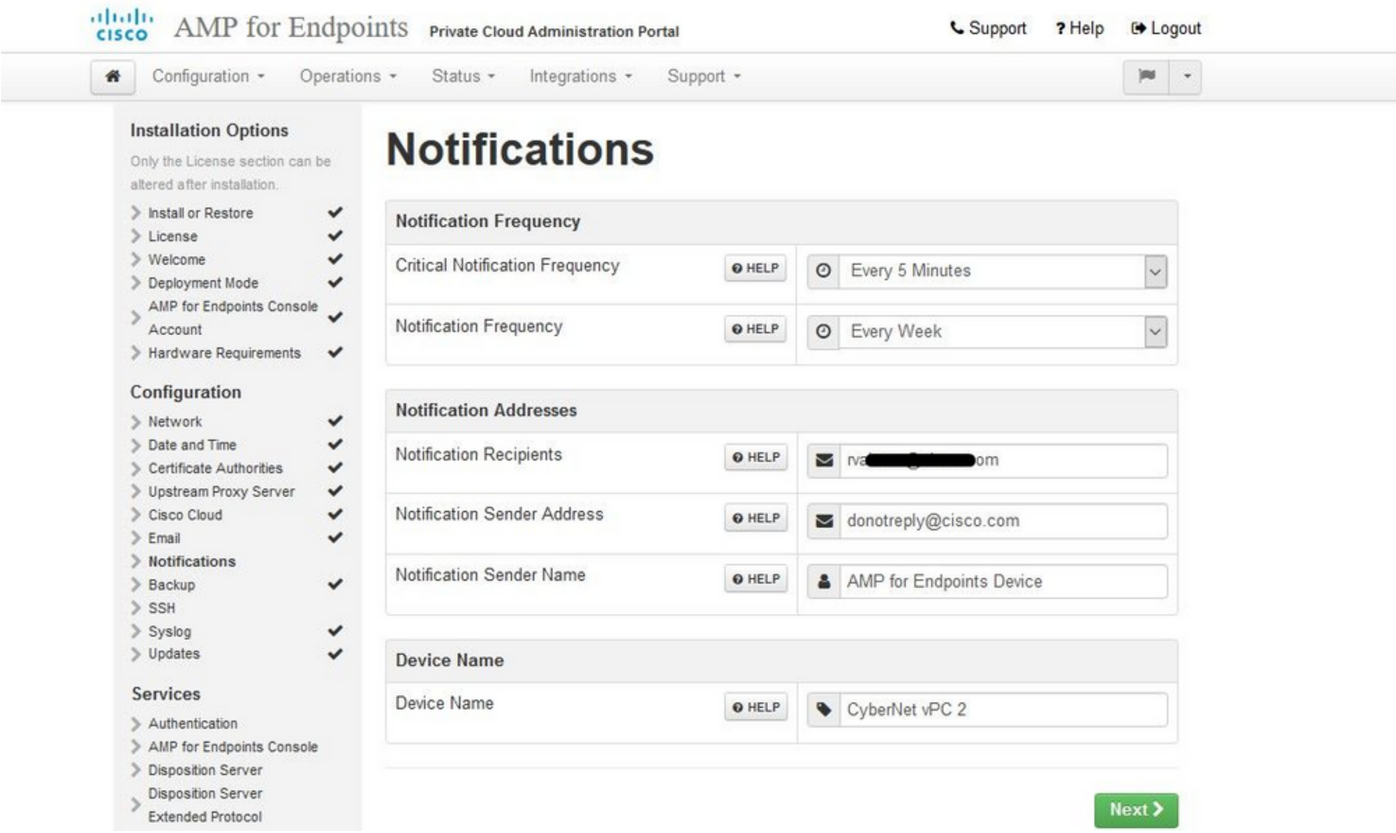
View Hostnames (click to expand)

Cisco Cloud Identity

Client Identity: 0f476ea8[redacted]dbbc272a6c

步驟 7:

導覽至通知頁面，如下圖所示。選擇關鍵通知和定期通知的頻率。輸入要接收安全終端裝置警報通知的電子郵件地址。您可以使用電子郵件別名，也可以通過逗號分隔清單指定多個地址。您還可以指定裝置使用的發件人姓名和電子郵件地址。這些通知與安全終結點控制檯訂閱不同。如果您有多個安全終端私有雲裝置，您還可以指定唯一的裝置名稱。選擇Next。



Notifications

Notification Frequency

Critical Notification Frequency: Every 5 Minutes

Notification Frequency: Every Week

Notification Addresses

Notification Recipients: rva[redacted]om

Notification Sender Address: donotreply@cisco.com

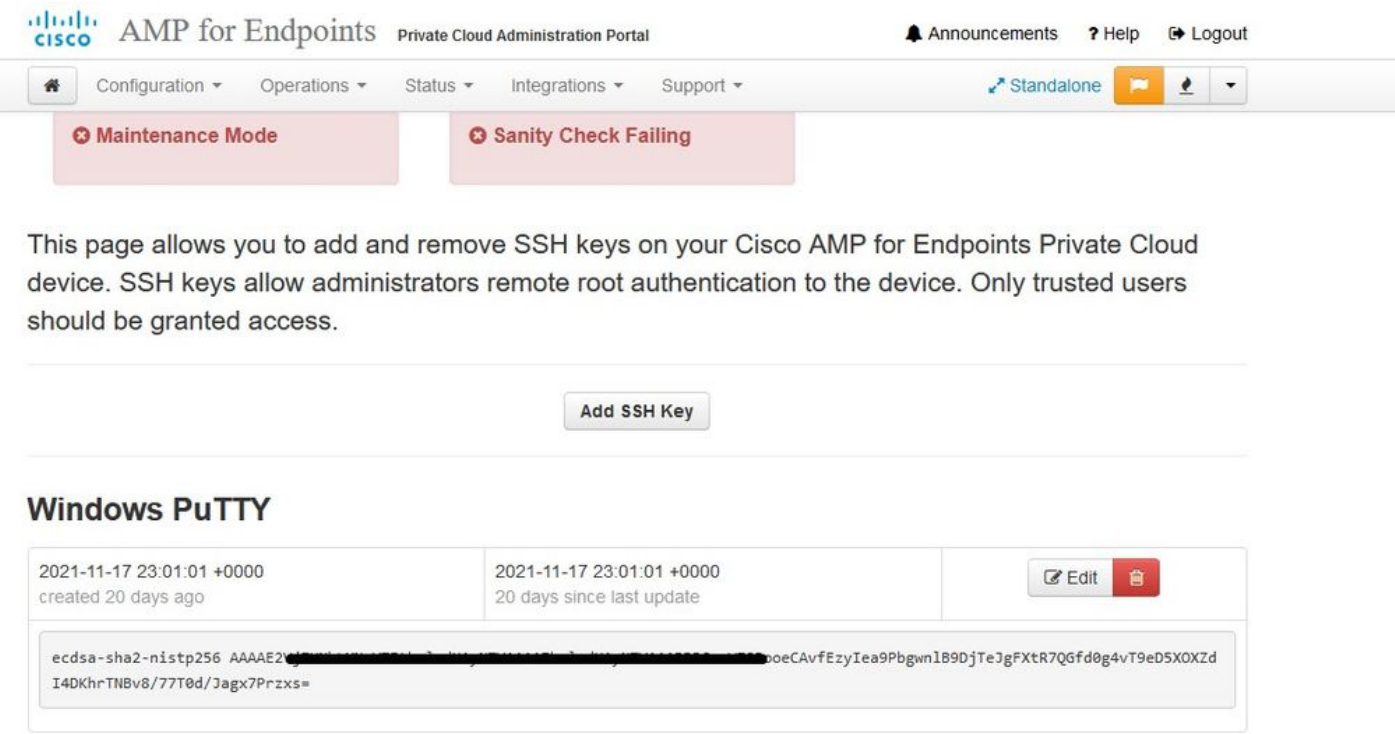
Notification Sender Name: AMP for Endpoints Device

Device Name

Device Name: CyberNet vPC 2

步驟 8:

接下來，導航到SSH Keys頁面，如下圖所示。選擇Add SSH Key以輸入您要新增到裝置的所有公鑰。SSH金鑰允許您通過具有根使用者許可權的遠端shell訪問裝置。只能向受信任的使用者授予訪問許可權。您的私有雲裝置需要OpenSSH格式的RSA金鑰。您可以稍後通過管理門戶中的Configuration > SSH新增更多SSH金鑰。選擇Next。



This page allows you to add and remove SSH keys on your Cisco AMP for Endpoints Private Cloud device. SSH keys allow administrators remote root authentication to the device. Only trusted users should be granted access.

Windows PuTTY

2021-11-17 23:01:01 +0000 created 20 days ago	2021-11-17 23:01:01 +0000 20 days since last update	Edit

```
ecdsa-sha2-nistp256 AAAAE2V[redacted]poeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7QGfd0g4vT9eD5XOXZd
I4DKhrTNBv8/77T0d/Jagx7Przxs=
```

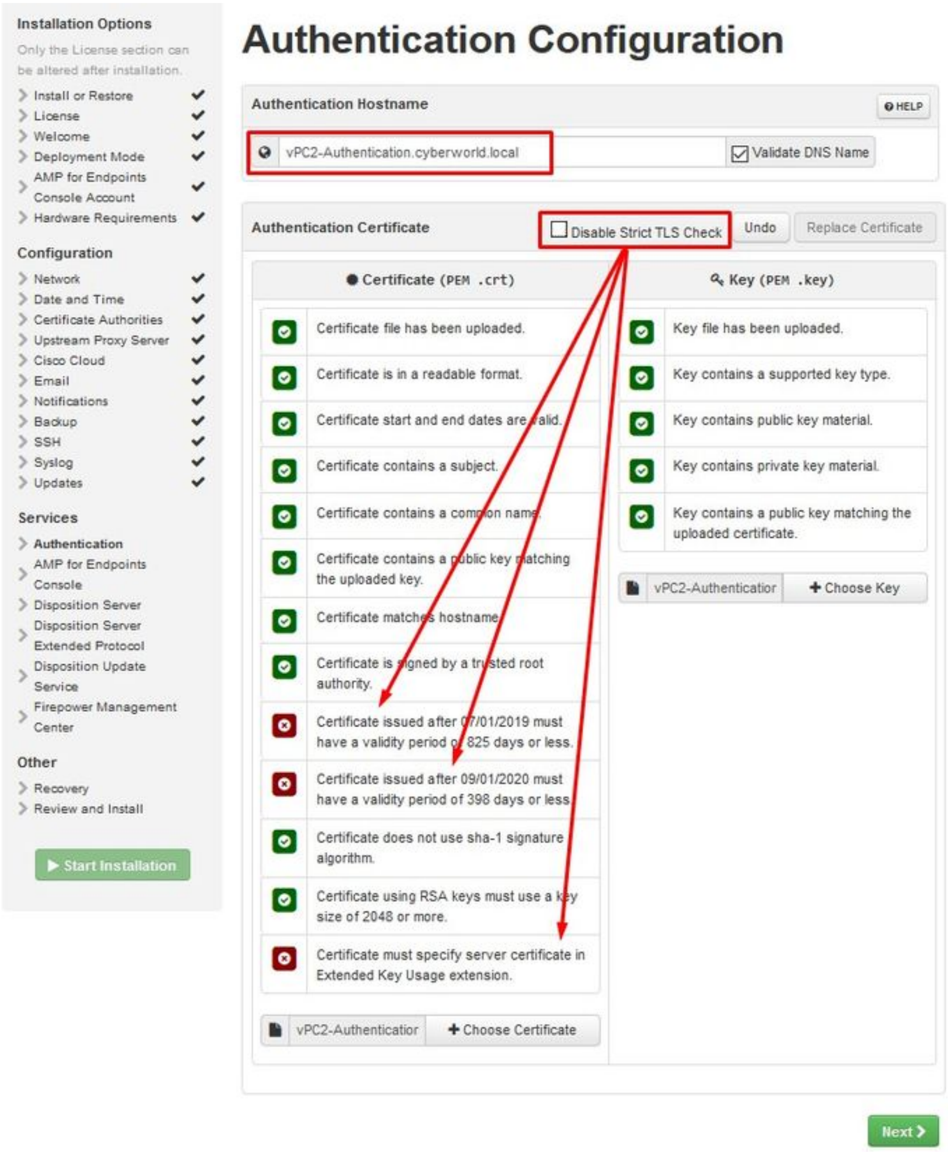
接下來您會看到Services部分。在接下來的頁面中，您需要為這些裝置服務分配主機名並上傳適當的證書和金鑰對。在接下來的幾張幻燈片中，我們可以看到6個證書中一個的配置。

服務

步驟 1:

在配置過程中，您可能會遇到這些錯誤。

您可能會注意到的第一個「錯誤」會以3個箭頭突出顯示。要跳過此步驟，只需取消選中「禁用嚴格TLS檢查」



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✔
- License ✔
- Welcome ✔
- Deployment Mode ✔
- AMP for Endpoints Console Account ✔
- Hardware Requirements ✔

Configuration

- Network ✔
- Date and Time ✔
- Certificate Authorities ✔
- Upstream Proxy Server ✔
- Cisco Cloud ✔
- Email ✔
- Notifications ✔
- Backup ✔
- SSH ✔
- Syslog ✔
- Updates ✔

Services

- Authentication
- AMP for Endpoints Console
- Disposition Server
- Disposition Server Extended Protocol
- Disposition Update Service
- Firepower Management Center

Other

- Recovery
- Review and Install

Authentication Configuration

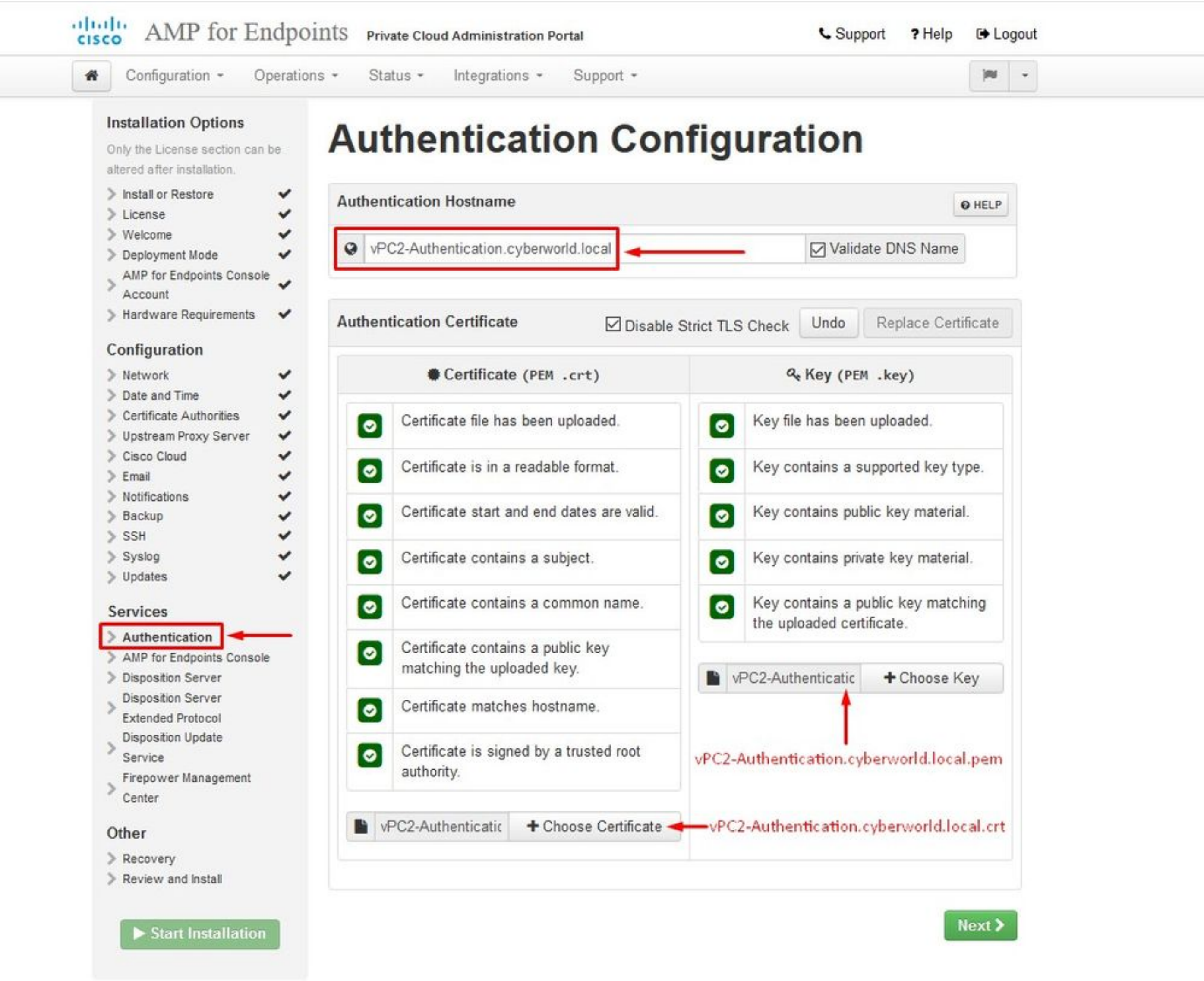
Authentication Hostname

vPC2-Authentication.cyberworld.local ☑ Validate DNS Name

Authentication Certificate ☐ Disable Strict TLS Check

Certificate (PEM .crt)	Key (PEM .key)
✓ Certificate file has been uploaded.	✓ Key file has been uploaded.
✓ Certificate is in a readable format.	✓ Key contains a supported key type.
✓ Certificate start and end dates are valid.	✓ Key contains public key material.
✓ Certificate contains a subject.	✓ Key contains private key material.
✓ Certificate contains a common name.	✓ Key contains a public key matching the uploaded certificate.
✓ Certificate contains a public key matching the uploaded key.	
✓ Certificate matches hostname.	
✓ Certificate is signed by a trusted root authority.	
✗ Certificate issued after 07/01/2019 must have a validity period of 825 days or less.	
✗ Certificate issued after 09/01/2020 must have a validity period of 398 days or less.	
✓ Certificate does not use sha-1 signature algorithm.	
✓ Certificate using RSA keys must use a key size of 2048 or more.	
✗ Certificate must specify server certificate in Extended Key Usage extension.	
vPC2-Authenticatior + Choose Certificate	vPC2-Authenticatior + Choose Key

沒有嚴格TLS檢查



Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local ☑ Validate DNS Name

Authentication Certificate ☑ Disable Strict TLS Check

Certificate (PEM .crt)	Key (PEM .key)
✓ Certificate file has been uploaded.	✓ Key file has been uploaded.
✓ Certificate is in a readable format.	✓ Key contains a supported key type.
✓ Certificate start and end dates are valid.	✓ Key contains public key material.
✓ Certificate contains a subject.	✓ Key contains private key material.
✓ Certificate contains a common name.	✓ Key contains a public key matching the uploaded certificate.
✓ Certificate contains a public key matching the uploaded key.	
✓ Certificate matches hostname.	
✓ Certificate is signed by a trusted root authority.	

vPC2-Authenticatic + Choose Certificate ← vPC2-Authentication.cyberworld.local.crt

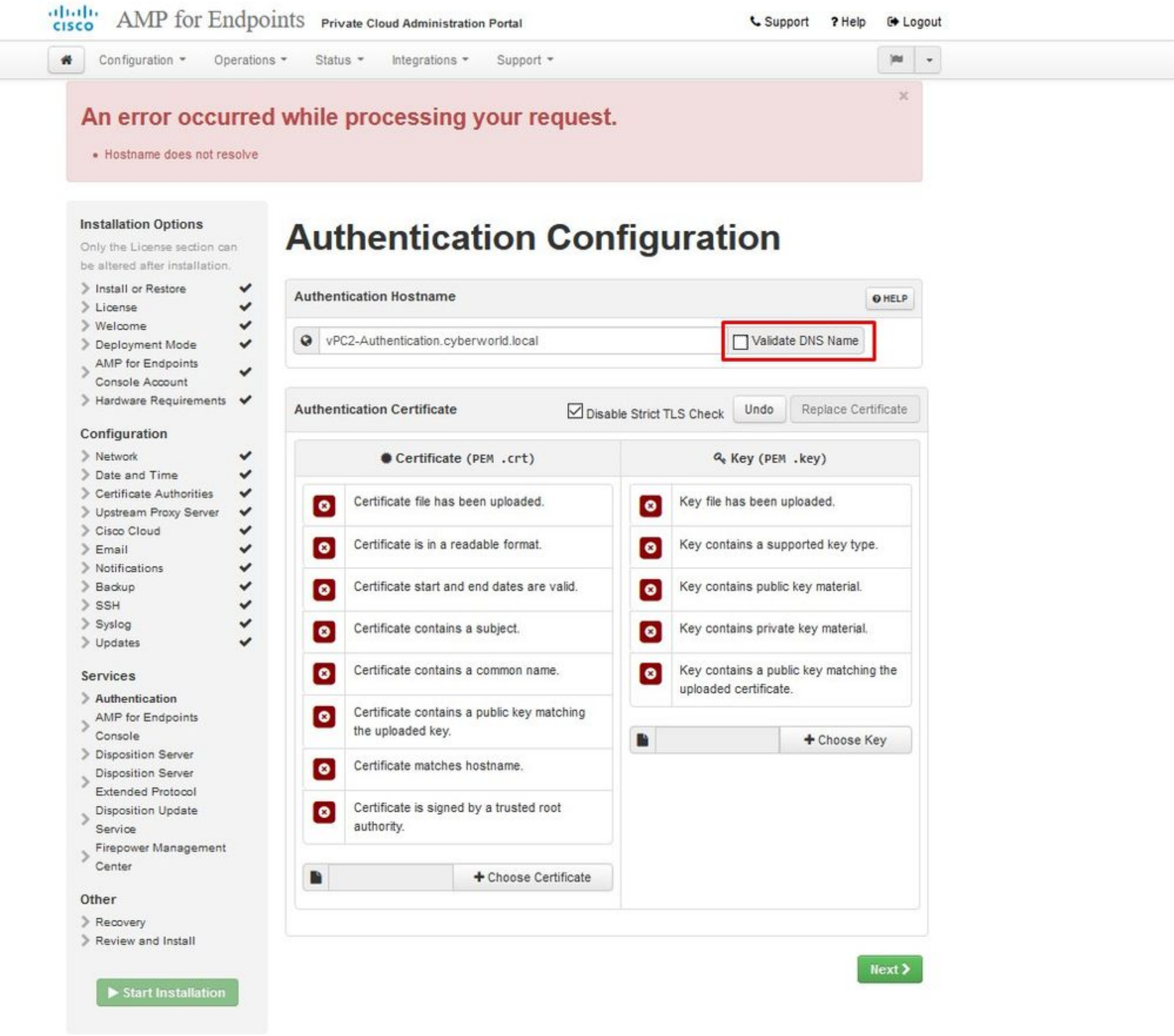
vPC2-Authenticatic + Choose Key ↑ vPC2-Authentication.cyberworld.local.pem

步驟 2:

如果您未選中「Validate DNS Name」，則會出現下一個錯誤。你有兩個選擇。

#1：取消選中驗證DNS複選標籤

#2：返回到DNS伺服器並配置其餘主機記錄。



An error occurred while processing your request.

- Hostname does not resolve

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local □ Validate DNS Name

Authentication Certificate ☑ Disable Strict TLS Check

● Certificate (PEM .crt)

☒ Certificate file has been uploaded.
☒ Certificate is in a readable format.
☒ Certificate start and end dates are valid.
☒ Certificate contains a subject.
☒ Certificate contains a common name.
☒ Certificate contains a public key matching the uploaded key.
☒ Certificate matches hostname.
☒ Certificate is signed by a trusted root authority.

Key (PEM .key)

☒ Key file has been uploaded.
☒ Key contains a supported key type.
☒ Key contains public key material.
☒ Key contains private key material.
☒ Key contains a public key matching the uploaded certificate.

現在，對剩餘的證書再重複相同進程五次。

驗證

— 身份驗證服務可在私有雲的未來版本中使用，以處理使用者身份驗證。

安全終端主控台

— 控制檯是安全終結點管理員可以訪問安全終結點控制檯的DNS名稱，安全終結點聯結器可接收新的策略和更新。

處置伺服器

— 處置伺服器是安全終結點聯結器傳送和檢索雲查詢資訊的DNS名稱。

Disposition Server — 擴展協定

— 處置伺服器 — 擴展協定是較新的安全端點聯結器傳送和檢索雲查詢資訊的DNS名稱。

處置更新服務

— 將Cisco Threat Grid裝置連結到私有雲裝置時，會使用Disposition Update Service。Threat Grid裝置用於從安全終端控制檯傳送要分析的檔案，而Threat Grid使用Disposition Update Service在檔案分析後更新其處置情況(清除或惡意)。

Firepower管理中心

- Firepower管理中心連結可將Cisco Firepower管理中心(FMC)裝置連結到您的私有雲裝置。這允許您在FMC控制面板中顯示安全終結點資料。有關FMC與安全端點整合的詳細資訊，請參閱您的FMC文檔。

⚠ 注意：一旦裝置完成安裝，就無法更改主機名。

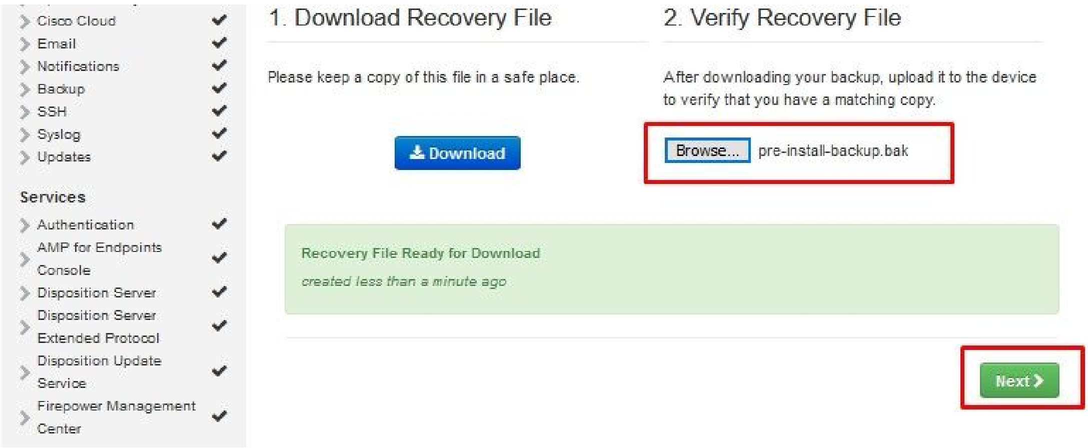
記下所需的主機名。您需要為安全終端私有雲建立六條唯一的DNS A記錄。每個記錄都指向虛擬私有雲控制檯介面(eth1)的相同IP地址，並且必須由私有雲和安全終端進行解析。

步驟 3:

在下載下一頁上，然後驗證Recovery File。

您將看到「Recovery（恢復）」頁面，如下圖所示。開始安裝之前，您必須下載並驗證配置的備份。恢復檔案包含所有配置以及伺服器金鑰。如果丟失恢復檔案，您將無法恢復配置，並且必須重新安裝所有Secure Endpoint聯結器。如果沒有原始金鑰，您必須使用新金鑰重新配置整個私有雲基礎設施。恢復檔案包含與opadmin門戶相關的所有配置。備份檔案包含恢復檔案的內容以及任何儀表板門戶資料（如事件、聯結器歷史記錄等）。如果只想恢復opadmin而不恢復事件資料和所有資料，則可以使用恢復檔案。如果從備份檔案還原，則會還原opadmin和儀表板門戶資料。

選擇「Download」，將備份儲存到本地電腦。下載檔案後，選擇Choose File上傳備份檔案並驗證其未損毀。選擇下一步以驗證檔案並繼續。


1. Download Recovery File

Please keep a copy of this file in a safe place.

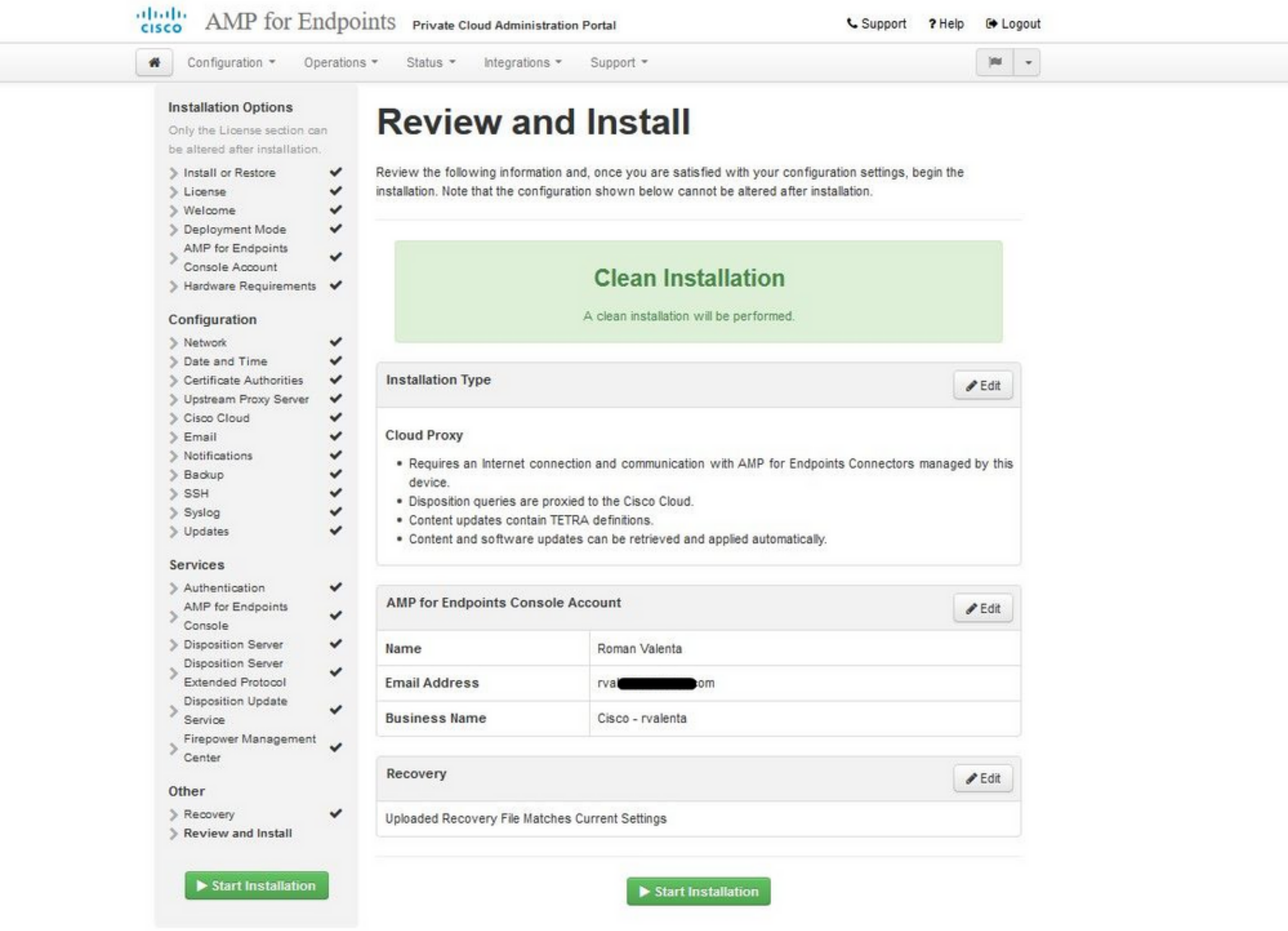
2. Verify Recovery File

After downloading your backup, upload it to the device to verify that you have a matching copy.

Browse... pre-install-backup.bak

Recovery File Ready for Download
created less than a minute ago

Cisco Cloud ✓
Email ✓
Notifications ✓
Backup ✓
SSH ✓
Syslog ✓
Updates ✓
Services
Authentication ✓
AMP for Endpoints Console ✓
Disposition Server ✓
Disposition Server Extended Protocol ✓
Disposition Update Service ✓
Firepower Management Center ✓
Download
Next



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements ✓

Configuration

- Network ✓
- Date and Time ✓
- Certificate Authorities ✓
- Upstream Proxy Server ✓
- Cisco Cloud ✓
- Email ✓
- Notifications ✓
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Services

- Authentication ✓
- AMP for Endpoints Console ✓
- Disposition Server ✓
- Disposition Server Extended Protocol ✓
- Disposition Update Service ✓
- Firepower Management Center ✓

Other

- Recovery ✓
- Review and Install

▶ Start Installation

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.

Clean Installation

A clean installation will be performed.

Installation Type Edit

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

AMP for Endpoints Console Account Edit

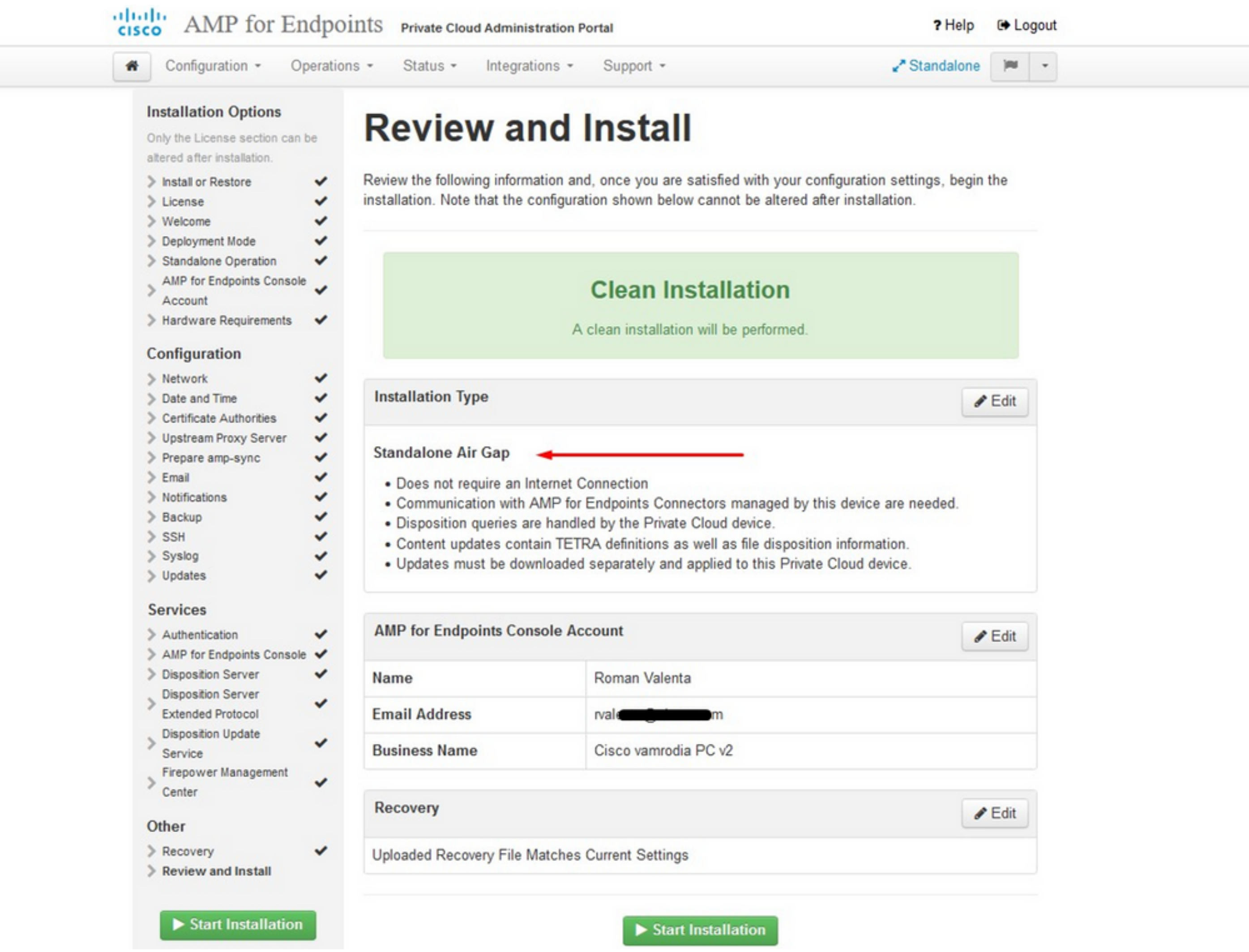
Name	Roman Valenta
Email Address	rva[redacted]om
Business Name	Cisco - rvalenta

Recovery Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

︾ ︾ AIRGAP ONLY ︾ ︾



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- Standalone Operation ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements ✓

Configuration

- Network ✓
- Date and Time ✓
- Certificate Authorities ✓
- Upstream Proxy Server ✓
- Prepare amp-sync ✓
- Email ✓
- Notifications ✓
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Services

- Authentication ✓
- AMP for Endpoints Console ✓
- Disposition Server ✓
- Disposition Server Extended Protocol ✓
- Disposition Update Service ✓
- Firepower Management Center ✓

Other

- Recovery ✓
- **Review and Install**

▶ Start Installation

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.

Clean Installation

A clean installation will be performed.

Installation Type Edit

Standalone Air Gap

- Does not require 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 must be downloaded separately and applied to this Private Cloud device.

AMP for Endpoints Console Account Edit

Name	Roman Valenta
Email Address	rval[redacted]m
Business Name	Cisco vamrodia PC v2

Recovery Edit

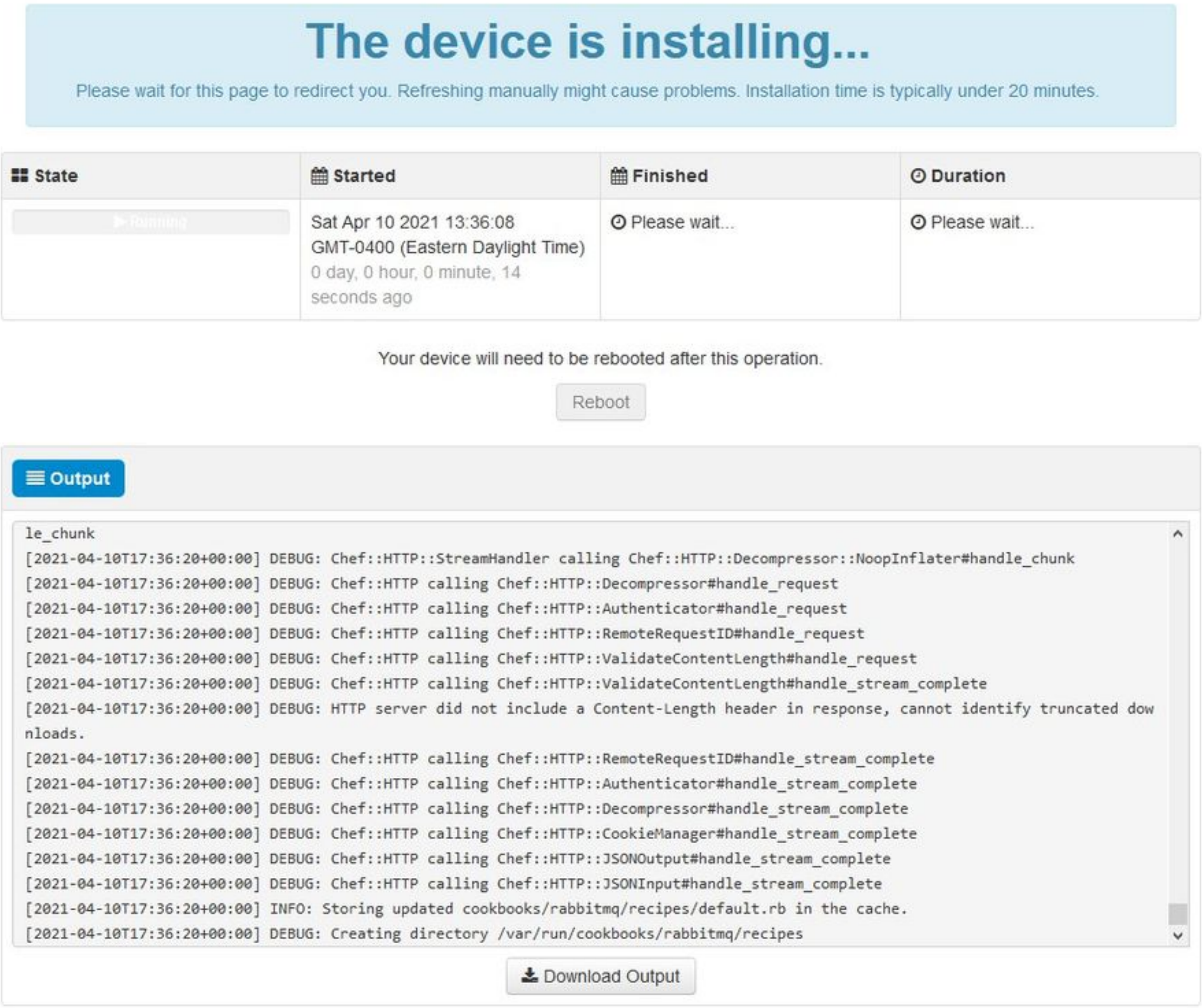
Uploaded Recovery File Matches Current Settings

▶ Start Installation

僅︽︽︽AIRGAP ︽

你看見類似這樣的輸入......

⚠ 注意：當您處於此頁上時，不要刷新，因為它可能會導致問題。



The device is installing...

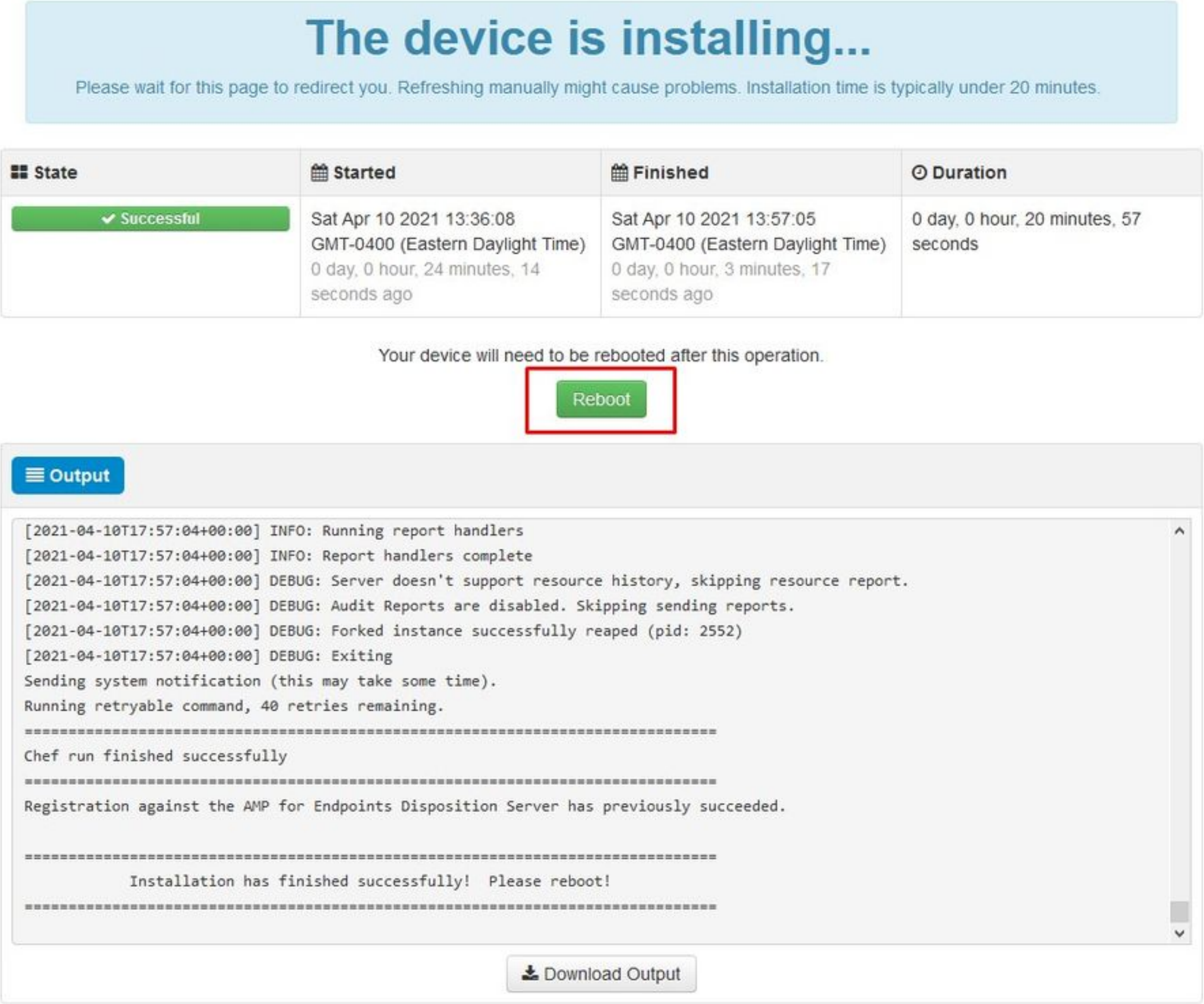
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 14 seconds ago	Please wait...	Please wait...

Your device will need to be rebooted after this operation.

```
le_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP::StreamHandler calling Chef::HTTP::Decompressor::NoopInflater#handle_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: HTTP server did not include a Content-Length header in response, cannot identify truncated dow
nloads.
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::CookieManager#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONOutput#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONInput#handle_stream_complete
[2021-04-10T17:36:20+00:00] INFO: Storing updated cookbooks/rabbitmq/recipes/default.rb in the cache.
[2021-04-10T17:36:20+00:00] DEBUG: Creating directory /var/run/cookbooks/rabbitmq/recipes
```

安裝完成後，按重新啟動按鈕



The device is installing...

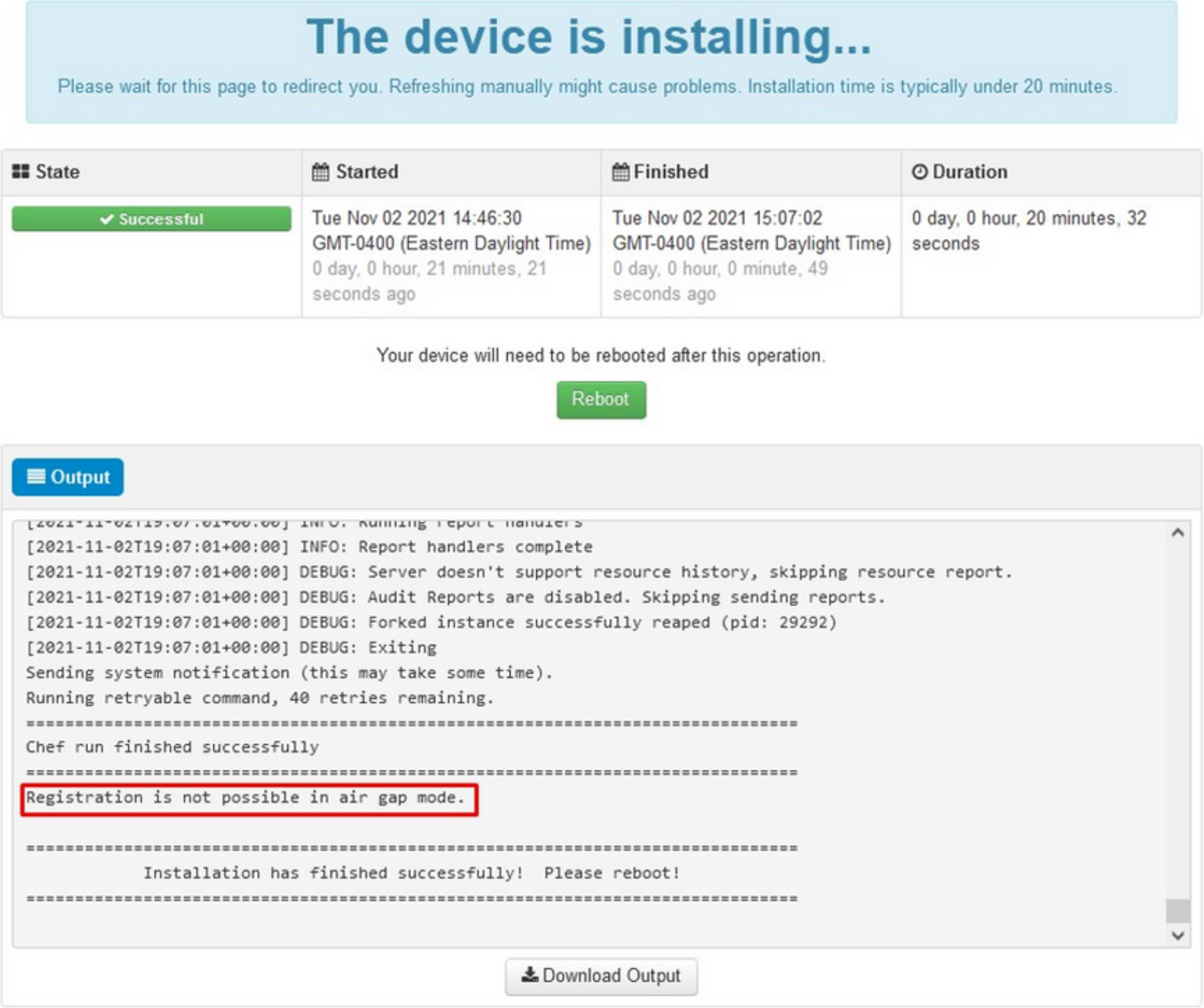
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 24 minutes, 14 seconds ago	Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 3 minutes, 17 seconds ago	0 day, 0 hour, 20 minutes, 57 seconds

Your device will need to be rebooted after this operation.

```
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
================================================================================
Chef run finished successfully
================================================================================
Registration against the AMP for Endpoints Disposition Server has previously succeeded.

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

︾︾ AIRGAP ONLY ︾︾



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 Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 21 minutes, 21 seconds ago	Tue Nov 02 2021 15:07:02 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 49 seconds ago	0 day, 0 hour, 20 minutes, 32 seconds

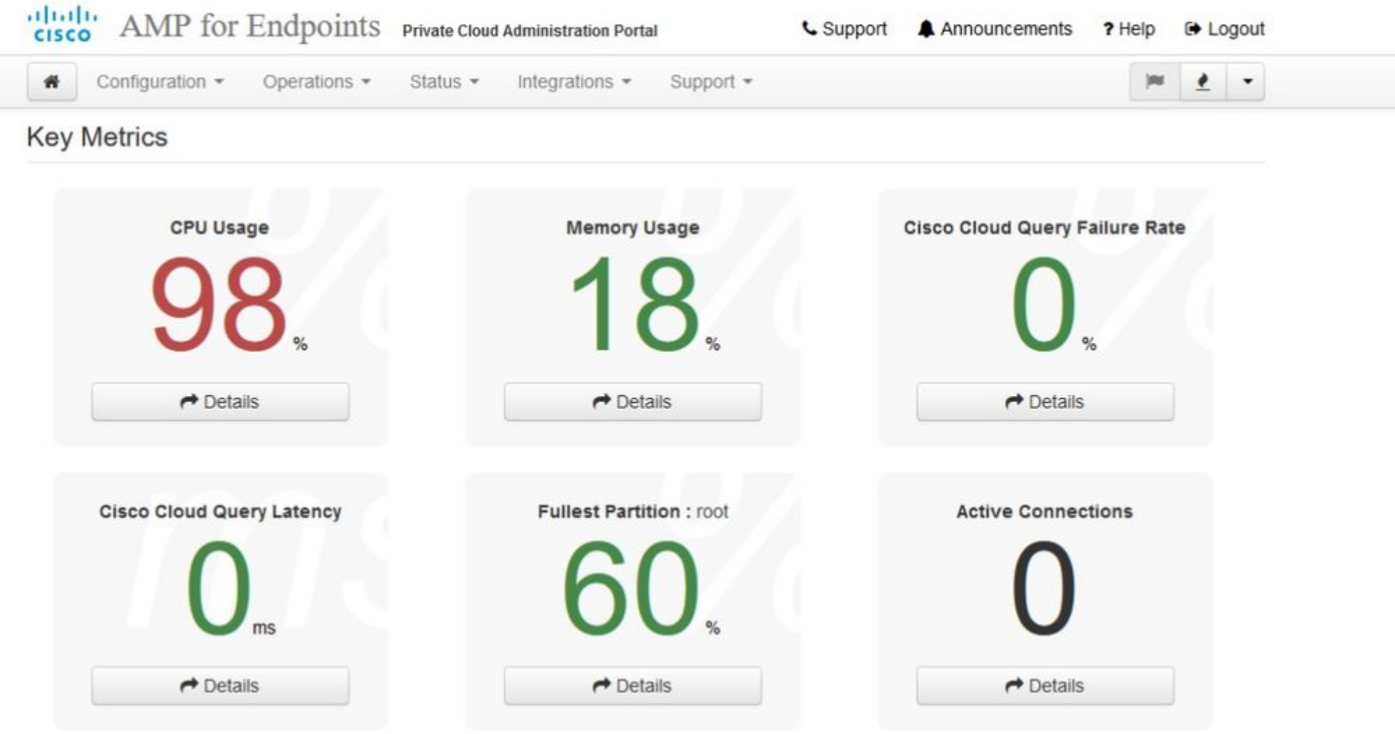
Your device will need to be rebooted after this operation.

```
[2021-11-02T19:07:01+00:00] INFO: Running report handlers
[2021-11-02T19:07:01+00:00] INFO: Report handlers complete
[2021-11-02T19:07:01+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-11-02T19:07:01+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-11-02T19:07:01+00:00] DEBUG: Forked instance successfully reaped (pid: 29292)
[2021-11-02T19:07:01+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
================================================================================
Chef run finished successfully
================================================================================
Registration is not possible in air gap mode.

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

僅︽︽︽AIRGAP ︽

裝置完全啟動後，下次使用管理員介面登入時，您會看到此儀表板。 您可能會注意到開始時的CPU使用率較高，但如果您用幾分鐘時間，CPU使用率會降低。

從此處導航至安全終端控制檯。點選旗幟旁邊右角看起來像是火的小圖示。



Key Metrics

CPU Usage 98 %

Memory Usage 18 %

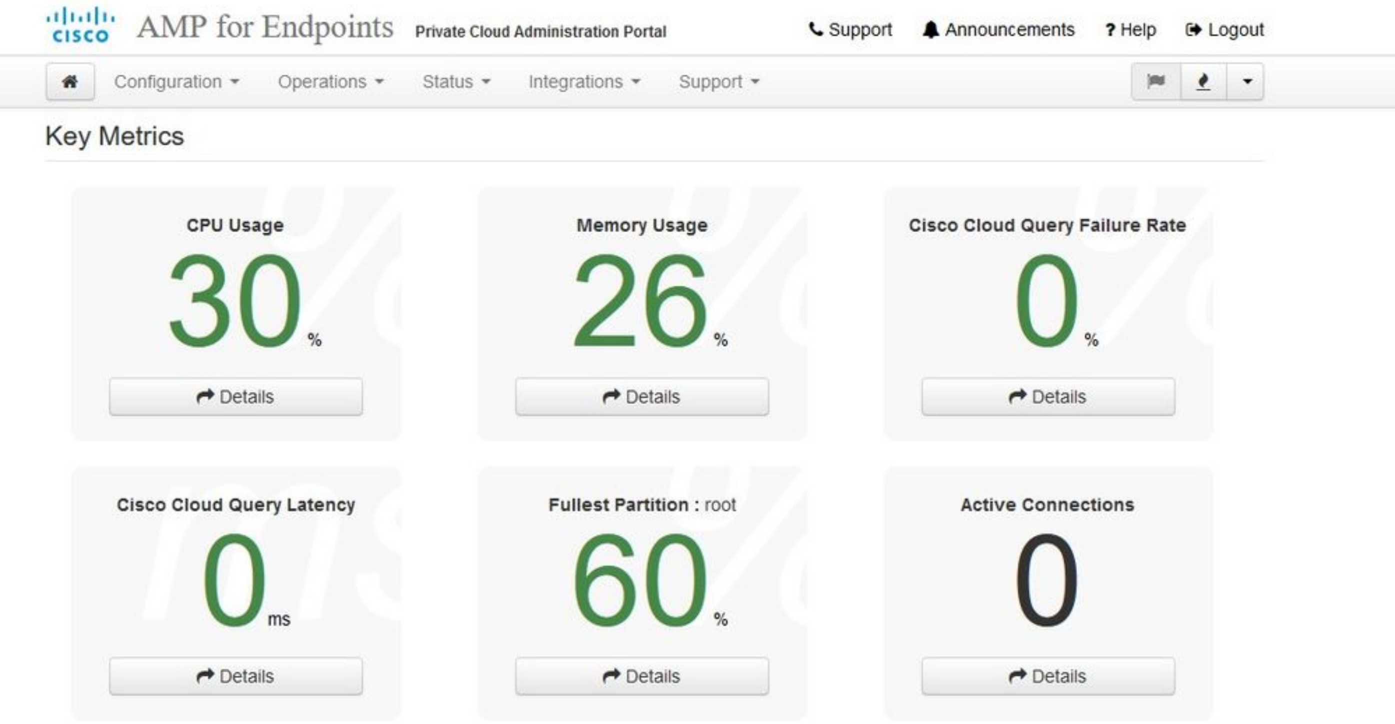
Cisco Cloud Query Failure Rate 0 %

Cisco Cloud Query Latency 0 ms

Fullest Partition : root 60 %

Active Connections 0

幾分鐘後……



Key Metrics

CPU Usage 30 %

Memory Usage 26 %

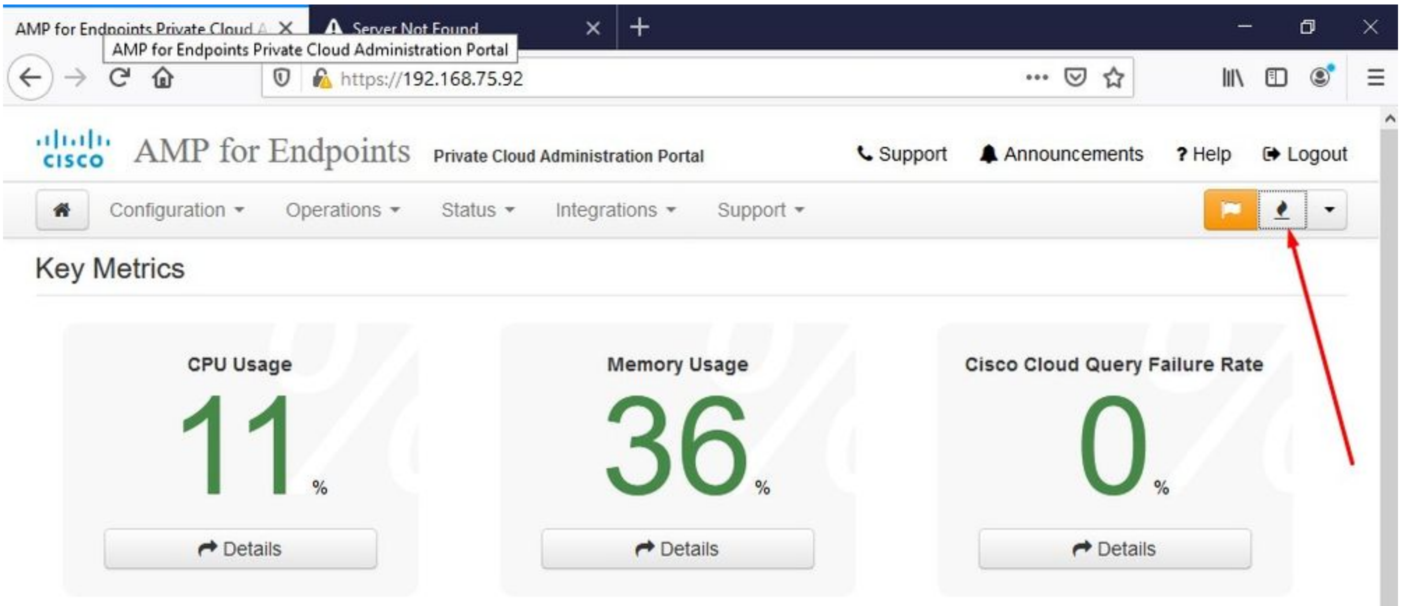
Cisco Cloud Query Failure Rate 0 %

Cisco Cloud Query Latency 0 ms

Fullest Partition : root 60 %

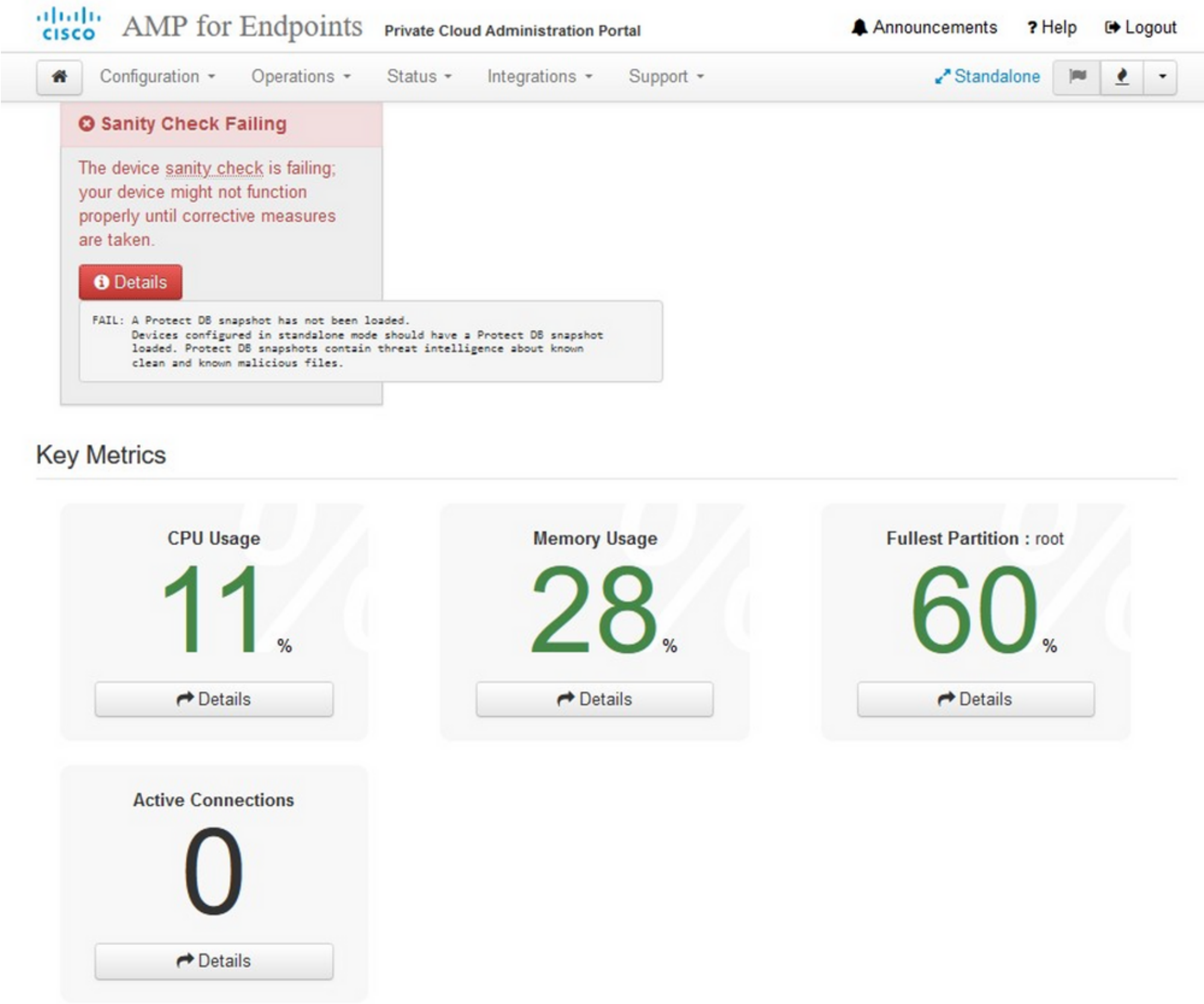
Active Connections 0

從此處導航至安全終端控制檯。點選旗幟旁邊右角看起來像是火的小圖示。



︾︾ AIRGAP ONLY ︾︾

如您所見，由於DB Protect Snapshot（資料庫保護快照）、客戶端定義、DFC和Tetra等原因，我們未通過健全性檢查。這必須通過通過下載的ISO檔案離線更新完成，該檔案之前通過amp-sync準備並上傳到VM或儲存在NFS位置。



Sanity Check Failing

The device sanity check is failing; your device might not function properly until corrective measures are taken.

```
FAIL: A Protect DB snapshot has not been loaded.
      Devices configured in standalone mode should have a Protect DB snapshot
      loaded. Protect DB snapshots contain threat intelligence about known
      clean and known malicious files.
```

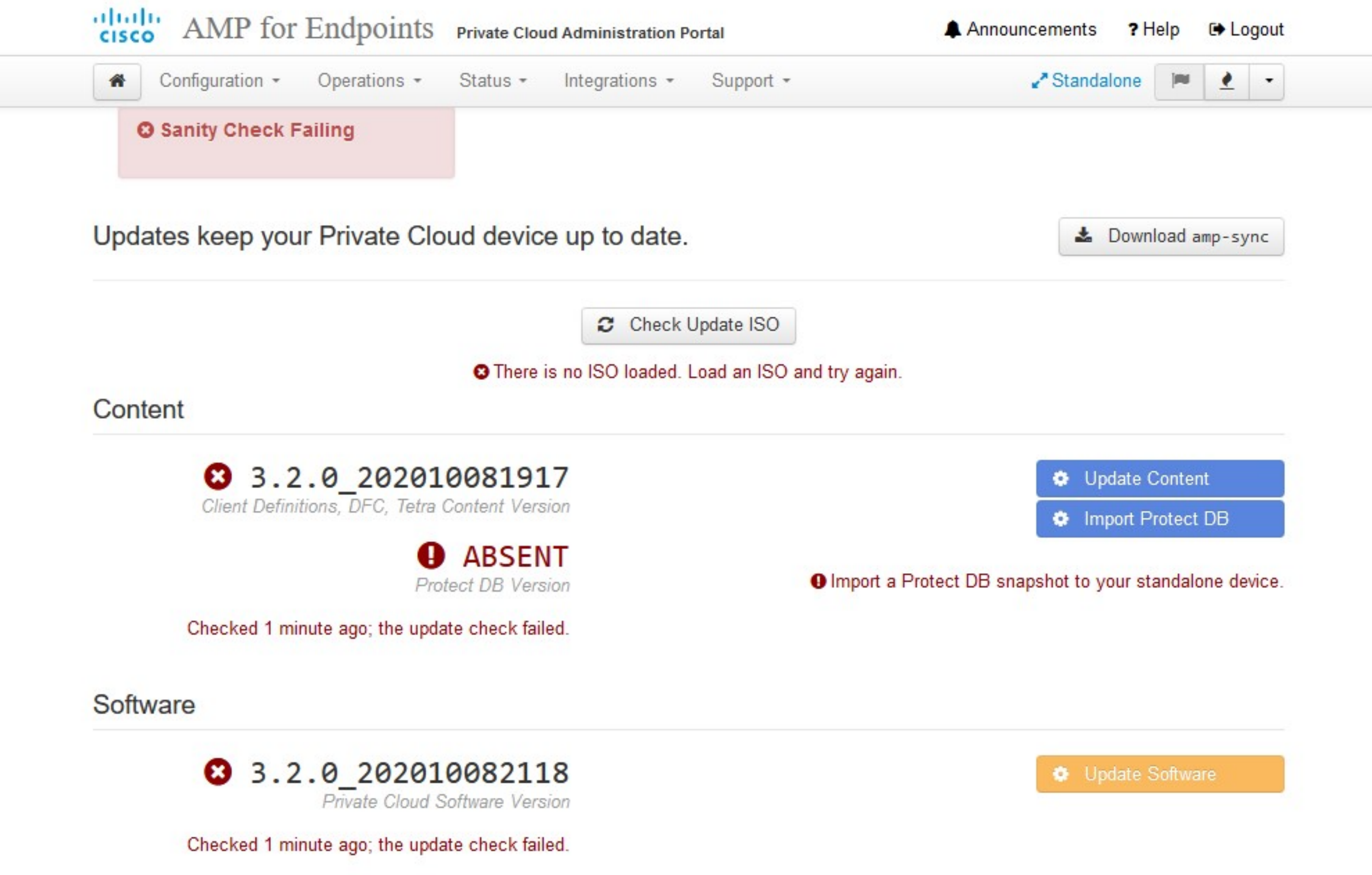
Key Metrics

CPU Usage: 11 %

Memory Usage: 28 %

Fullest Partition : root: 60 %

Active Connections: 0



Sanity Check Failing

Updates keep your Private Cloud device up to date.

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

Checked 1 minute ago; the update check failed.

Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

Checked 1 minute ago; the update check failed.

AirGap更新包

我們第一次必須使用此命令來接收Protect DB

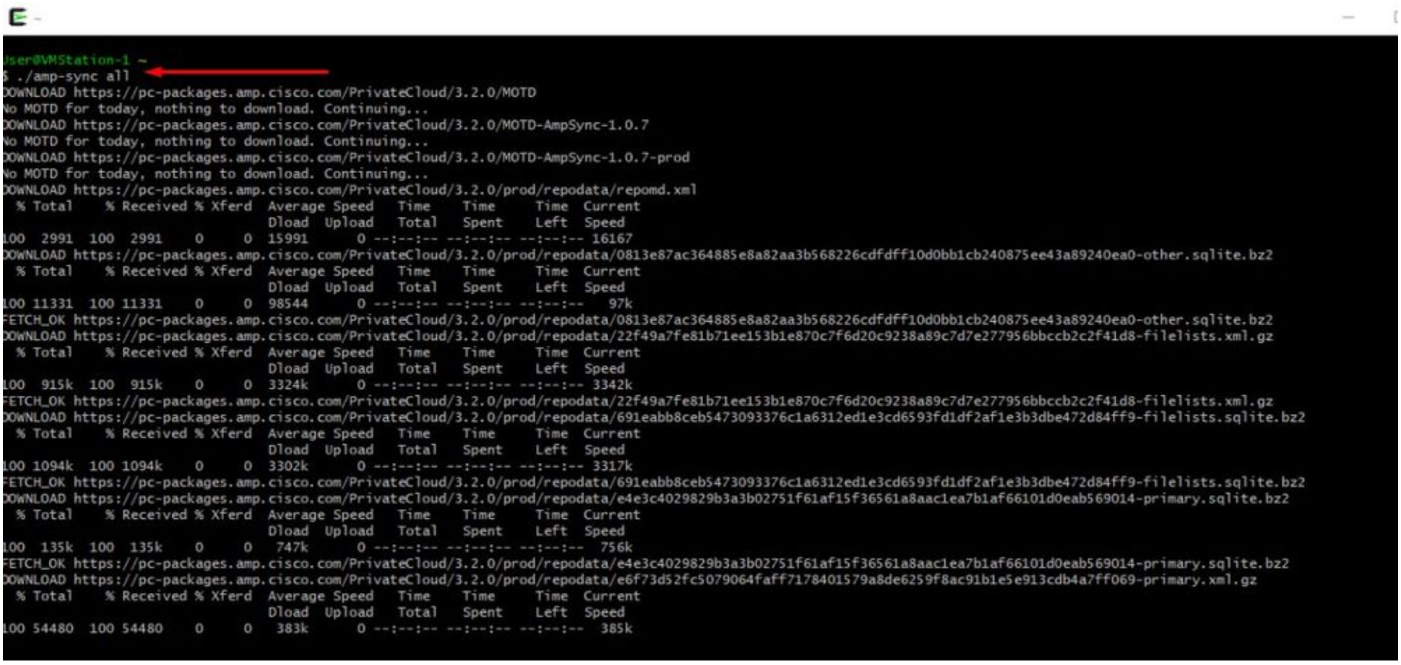
```
./amp-sync all
```

注意：通過此命令下載所有軟體包，然後驗證可能需要超過24小時。取決於速度和鏈路品質。對於使用1Gig光纖的情況，最終需要近25小時才能完成。部分原因還在於，此下載直接來自AWS，因此被限制。 最後請注意，此下載量相當大。就我而言，下載的檔案是323GB。

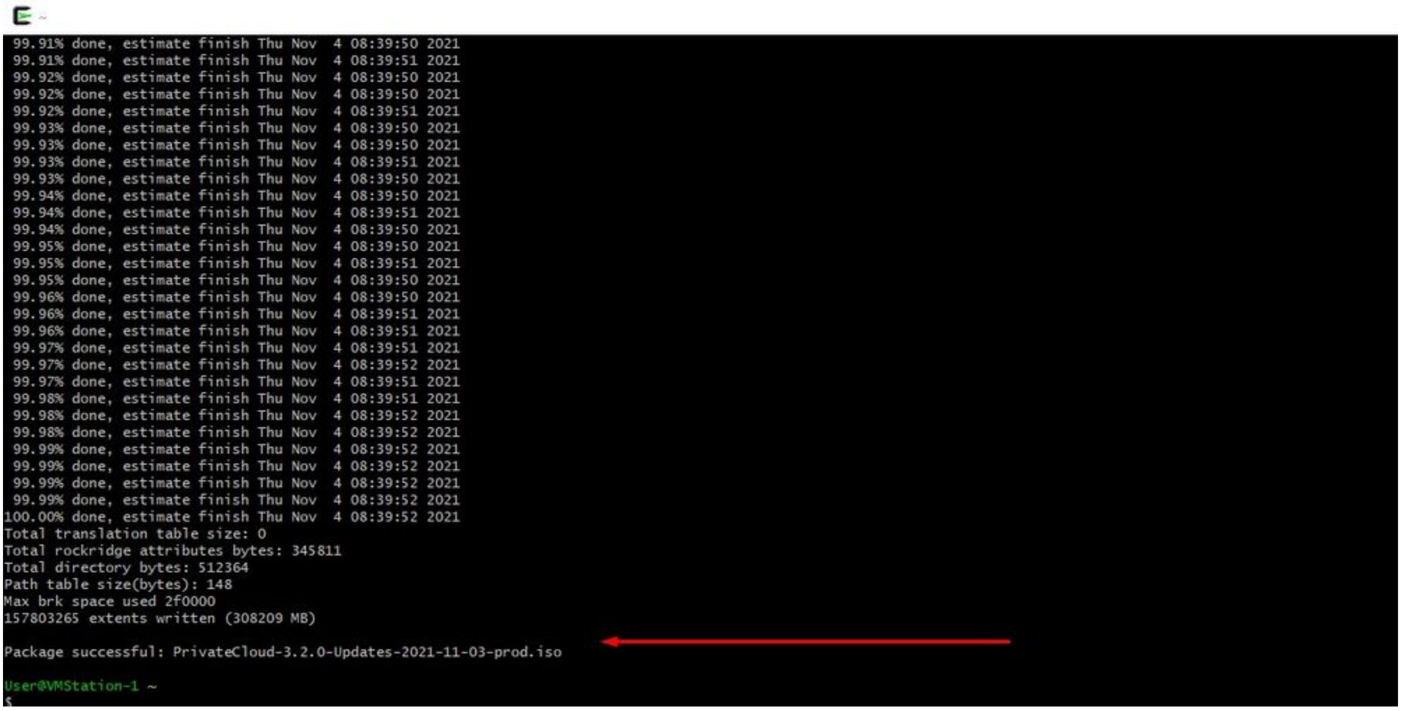
在本示例中，我們使用CygWin64

1.下載並安裝x64版本的Cygwin。
2.運行setup-x86_64.exe並完成安裝過程，選擇所有預設值。
3.選擇下載映象。
4.選擇要安裝的程式包：
全部 — >淨值 — >捲曲
全部 — >實用程式 — > genisoimage
全部 — >實用程式 — > xmlstarlet

* VPC 3.8.x up - > xorriso

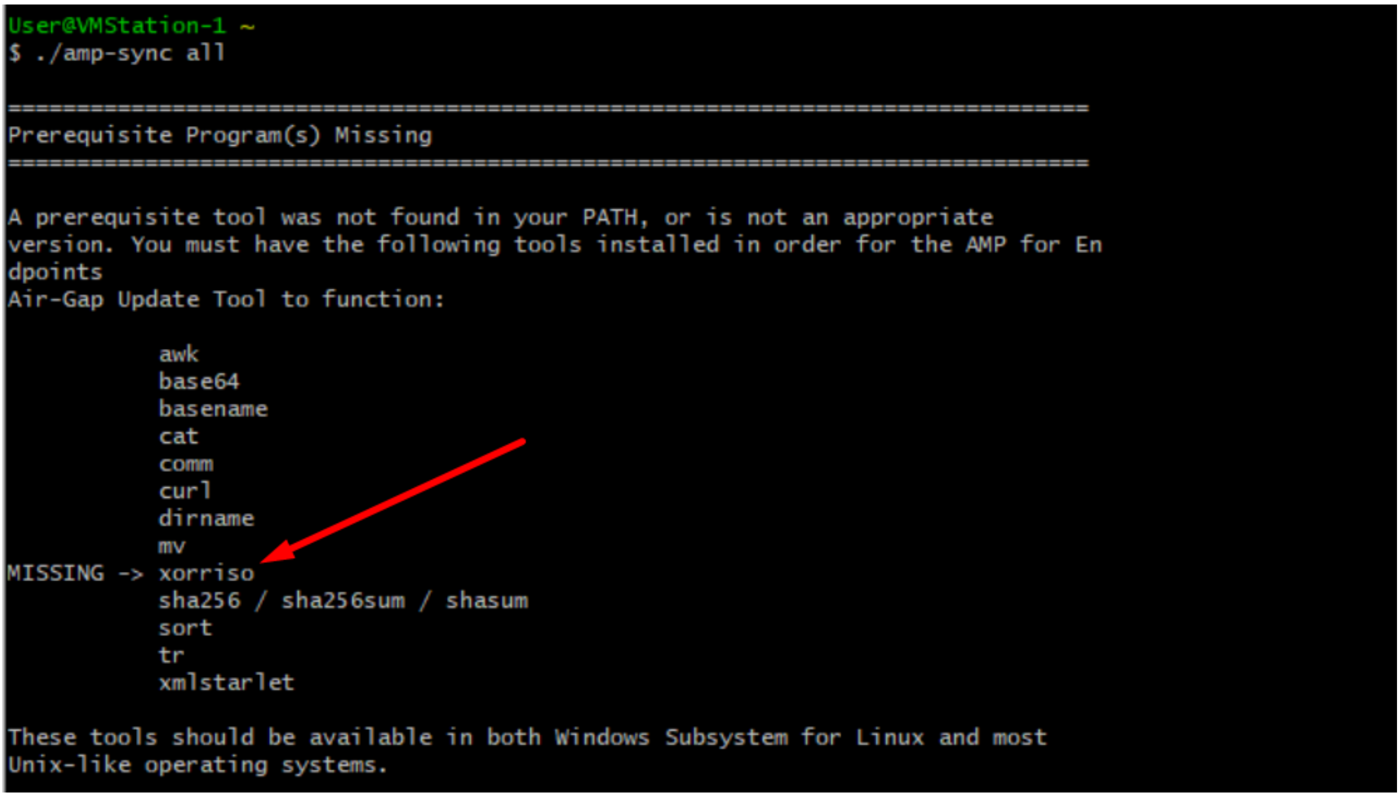


```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2991  100  2991    0     0  15991      0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11331  100 11331    0     0  98544      0 --:--:-- --:--:-- --:--:--   97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  915k  100  915k    0     0  3324k      0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1094k  100 1094k    0     0  3302k      0 --:--:-- --:--:-- --:--:-- 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  135k  100  135k    0     0   747k      0 --:--:-- --:--:-- --:--:--  756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 54480  100 54480    0     0   383k      0 --:--:-- --:--:-- --:--:--  385k
```



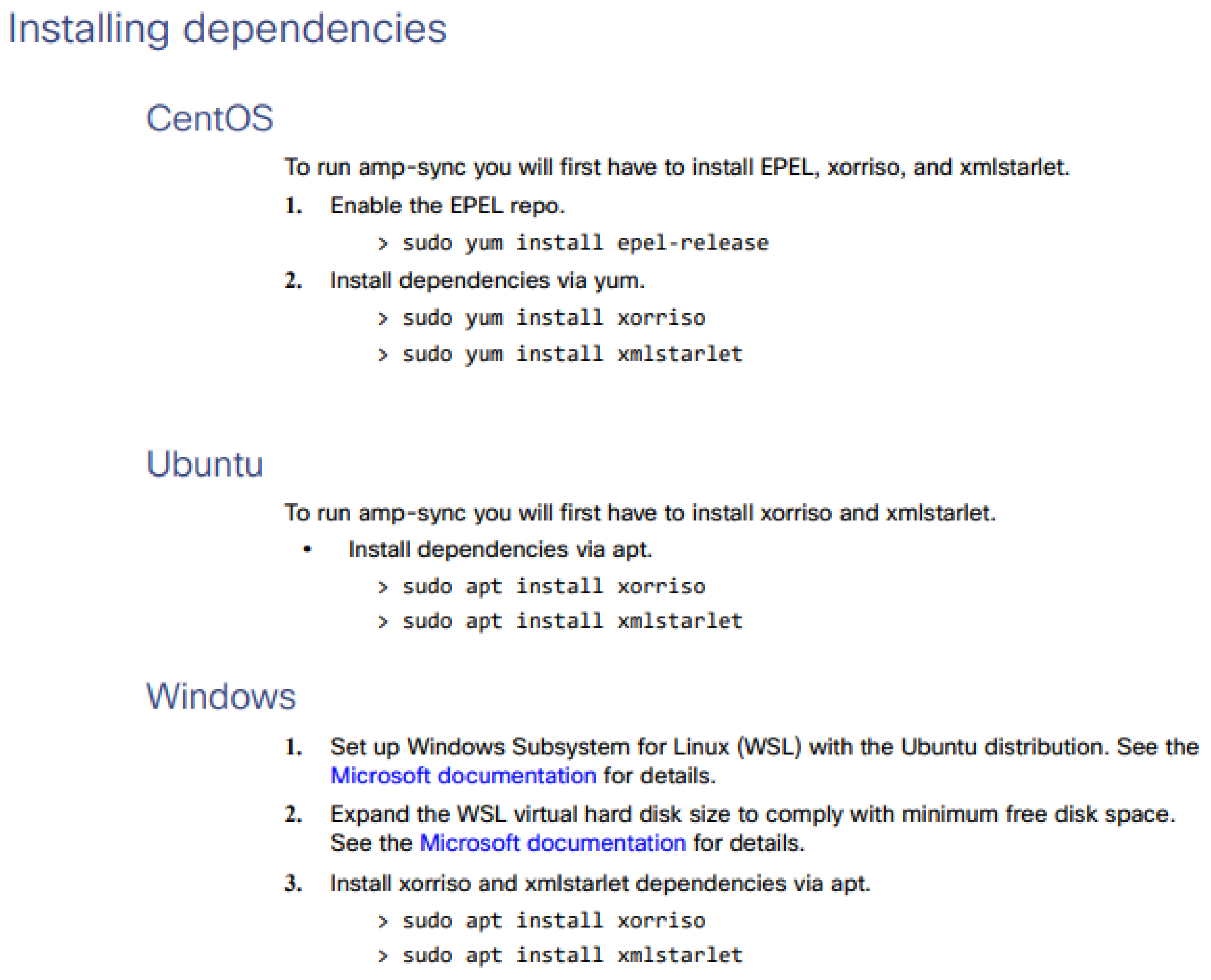
```
 99.91% done, estimate finish Thu Nov  4 08:39:50 2021
 99.91% done, estimate finish Thu Nov  4 08:39:51 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:51 2021
 99.93% done, estimate finish Thu Nov  4 08:39:50 2021
 99.93% done, estimate finish Thu Nov  4 08:39:50 2021
 99.93% done, estimate finish Thu Nov  4 08:39:51 2021
 99.93% done, estimate finish Thu Nov  4 08:39:50 2021
 99.94% done, estimate finish Thu Nov  4 08:39:50 2021
 99.94% done, estimate finish Thu Nov  4 08:39:51 2021
 99.94% done, estimate finish Thu Nov  4 08:39:50 2021
 99.95% done, estimate finish Thu Nov  4 08:39:50 2021
 99.95% done, estimate finish Thu Nov  4 08:39:51 2021
 99.95% done, estimate finish Thu Nov  4 08:39:50 2021
 99.96% done, estimate finish Thu Nov  4 08:39:50 2021
 99.96% done, estimate finish Thu Nov  4 08:39:51 2021
 99.96% done, estimate finish Thu Nov  4 08:39:51 2021
 99.97% done, estimate finish Thu Nov  4 08:39:51 2021
 99.97% done, estimate finish Thu Nov  4 08:39:52 2021
 99.97% done, estimate finish Thu Nov  4 08:39:51 2021
 99.98% done, estimate finish Thu Nov  4 08:39:51 2021
 99.98% done, estimate finish Thu Nov  4 08:39:52 2021
 99.98% done, estimate finish Thu Nov  4 08:39:52 2021
 99.99% done, estimate finish Thu Nov  4 08:39:52 2021
 99.99% done, estimate finish Thu Nov  4 08:39:52 2021
 99.99% done, estimate finish Thu Nov  4 08:39:52 2021
 99.99% done, estimate finish Thu Nov  4 08:39:52 2021
100.00% done, estimate finish Thu Nov  4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)

Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso

User@VMStation-1 ~
$
```

注意：在最新更新的VPC 3.8.x中，如果使用CygWin64作為主要下載工具，您可能會遇到下面描述的問題。



```
User@VMStation-1 ~
$ ./amp-sync all

================================================================================
Prerequisite Program(s) Missing
================================================================================

A prerequisite tool was not found in your PATH, or is not an appropriate
version. You must have the following tools installed in order for the AMP for En
dpoints
Air-Gap Update Tool to function:

           awk
           base64
           basename
           cat
           comm
           curl
           dirname
           mv
MISSING -> xorriso
           sha256 / sha256sum / shasum
           sort
           tr
           xmlstarlet

These tools should be available in both Windows Subsystem for Linux and most
Unix-like operating systems.
```

發行說明第#58頁。您可以看到，現在需要使用「xorriso」。我們將ISO的格式更改為ISO 9660，該依賴關係是將影象轉換為正確的格式，以便完成更新。遺憾的是，CygWin64沒有在其任何內建資料庫中提供xorriso。然而，對於那些仍希望使用CygWin64的企業，有辦法克服這個問題。



Installing dependencies

CentOS

To run amp-sync you will first have to install EPEL, xorriso, and xmlstarlet.

1. Enable the EPEL repo.

```
> sudo yum install epel-release
```

2. Install dependencies via yum.

```
> sudo yum install xorriso
> sudo yum install xmlstarlet
```

Ubuntu

To run amp-sync you will first have to install xorriso and xmlstarlet.

- Install dependencies via apt.

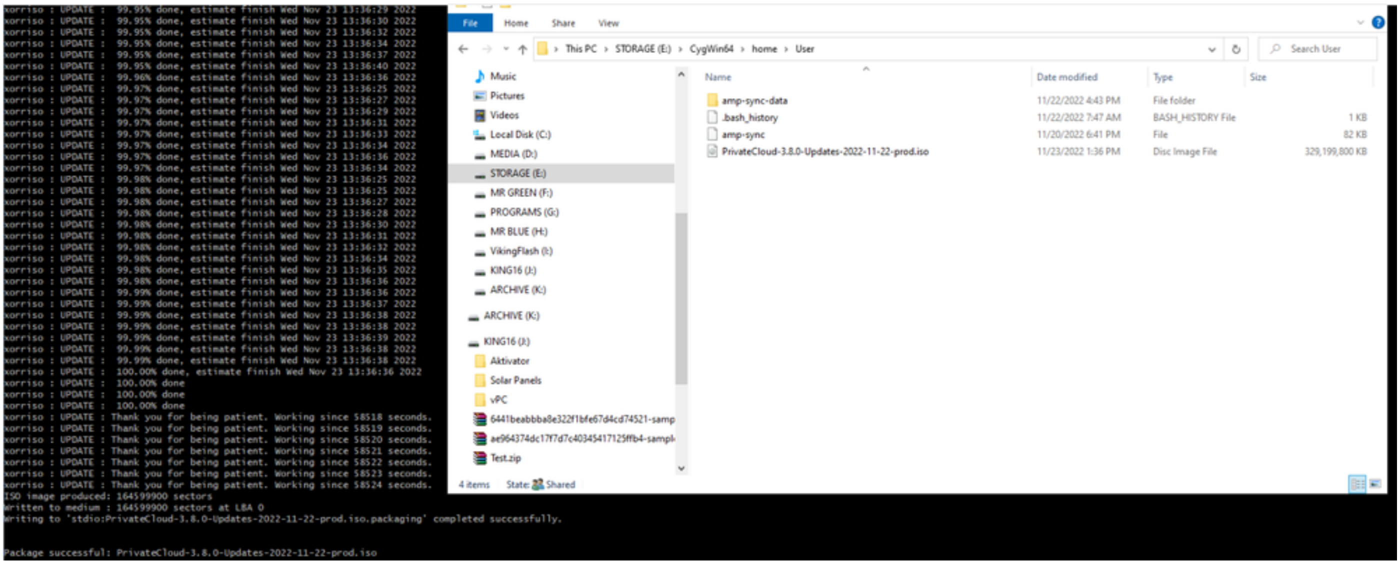
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

Windows

1. Set up Windows Subsystem for Linux (WSL) with the Ubuntu distribution. See the Microsoft documentation for details.
2. Expand the WSL virtual hard disk size to comply with minimum free disk space. See the Microsoft documentation for details.
3. Install xorriso and xmlstarlet dependencies via apt.

```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

要能夠再次使用CygWin，您必須從GitHub儲存庫手動下載xorriso。 開啟瀏覽器並鍵入<Latest xorriso.exe 1.5.2 pre-build for Windows>它應該作為名為<PeyTy/xorriso-exe-for-windows - GitHub>的第一個連結進入該GitHub頁面，然後下載位於zip檔案中的<xorriso-exe-for-windows-master.zip>檔案，該檔案位於名為<xorriso.exe>的其他幾個檔案中，請複製該檔案並將其貼上到本地Cyg的<CygWin64\binzip>路徑Win安裝。請嘗試再次運行<amp-sync>命令。您不會再看到錯誤訊息以及下載開始和完成，如圖所示。



```
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:29 2022
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:30 2022
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:32 2022
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:34 2022
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:37 2022
xorriso : UPDATE :  99.95% done, estimate finish Wed Nov 23 13:36:40 2022
xorriso : UPDATE :  99.96% done, estimate finish Wed Nov 23 13:36:36 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:25 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:27 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:29 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:31 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:33 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:34 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:36 2022
xorriso : UPDATE :  99.97% done, estimate finish Wed Nov 23 13:36:34 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:25 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:25 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:27 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:28 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:30 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:31 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:32 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:34 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:35 2022
xorriso : UPDATE :  99.98% done, estimate finish Wed Nov 23 13:36:36 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:36 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:37 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:38 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:38 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:39 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:38 2022
xorriso : UPDATE :  99.99% done, estimate finish Wed Nov 23 13:36:38 2022
xorriso : UPDATE :  100.00% done, estimate finish Wed Nov 23 13:36:36 2022
xorriso : UPDATE :  100.00% done
xorriso : UPDATE :  100.00% done
xorriso : UPDATE :  100.00% done
xorriso : UPDATE : Thank you for being patient. Working since 58518 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58519 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58520 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58521 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58522 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58523 seconds.
xorriso : UPDATE : Thank you for being patient. Working since 58524 seconds.
ISO image produced: 164599900 sectors
Written to medium : 164599900 sectors at LBA 0
Writing to 'stdio:PrivateCloud-3.8.0-Updates-2022-11-22-prod.iso.packaging' completed successfully.


Package successful: PrivateCloud-3.8.0-Updates-2022-11-22-prod.iso
```

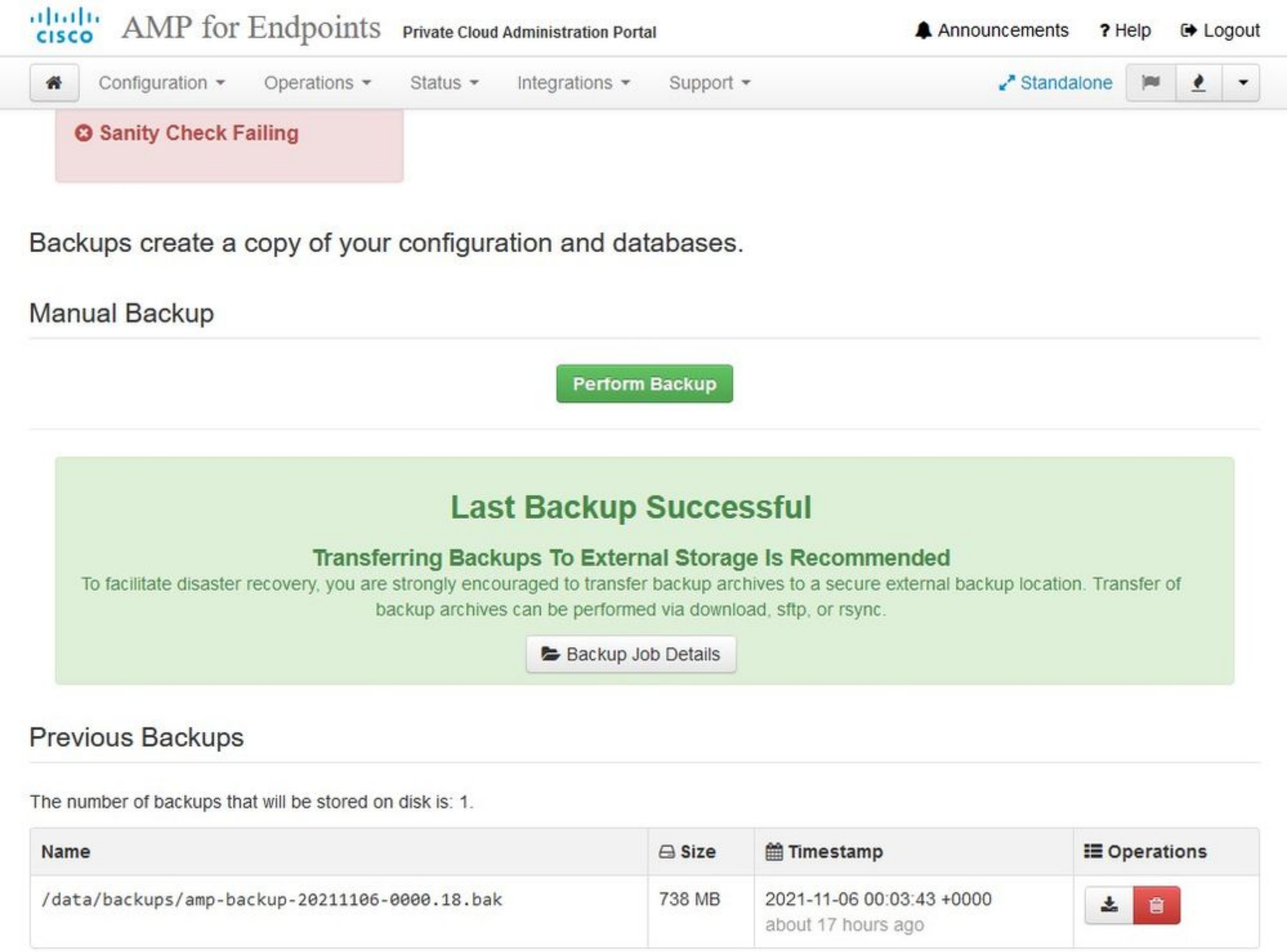
Name	Date modified	Type	Size
amp-sync-data	11/22/2022 4:43 PM	File folder	
.bash_history	11/22/2022 7:47 AM	BASH_HISTORY File	1 KB
amp-sync	11/20/2022 6:41 PM	File	82 KB
PrivateCloud-3.8.0-Updates-2022-11-22-prod.iso	11/23/2022 1:36 PM	Disc Image File	329,199,800 KB

在Airgap模式下執行當前(本例中)3.2.0 VPC的備份。

您可以從CLI使用此命令

```
rpm -qa | grep Pri
```

或者，也可以導航到操作>備份，如圖所示，並在該位置執行備份。



Sanity Check Failing

Backups create a copy of your configuration and databases.

Manual Backup

Last Backup Successful

Transferring Backups To External Storage Is Recommended

To facilitate disaster recovery, you are strongly encouraged to transfer backup archives to a secure external backup location. Transfer of backup archives can be performed via download, sftp, or rsync.

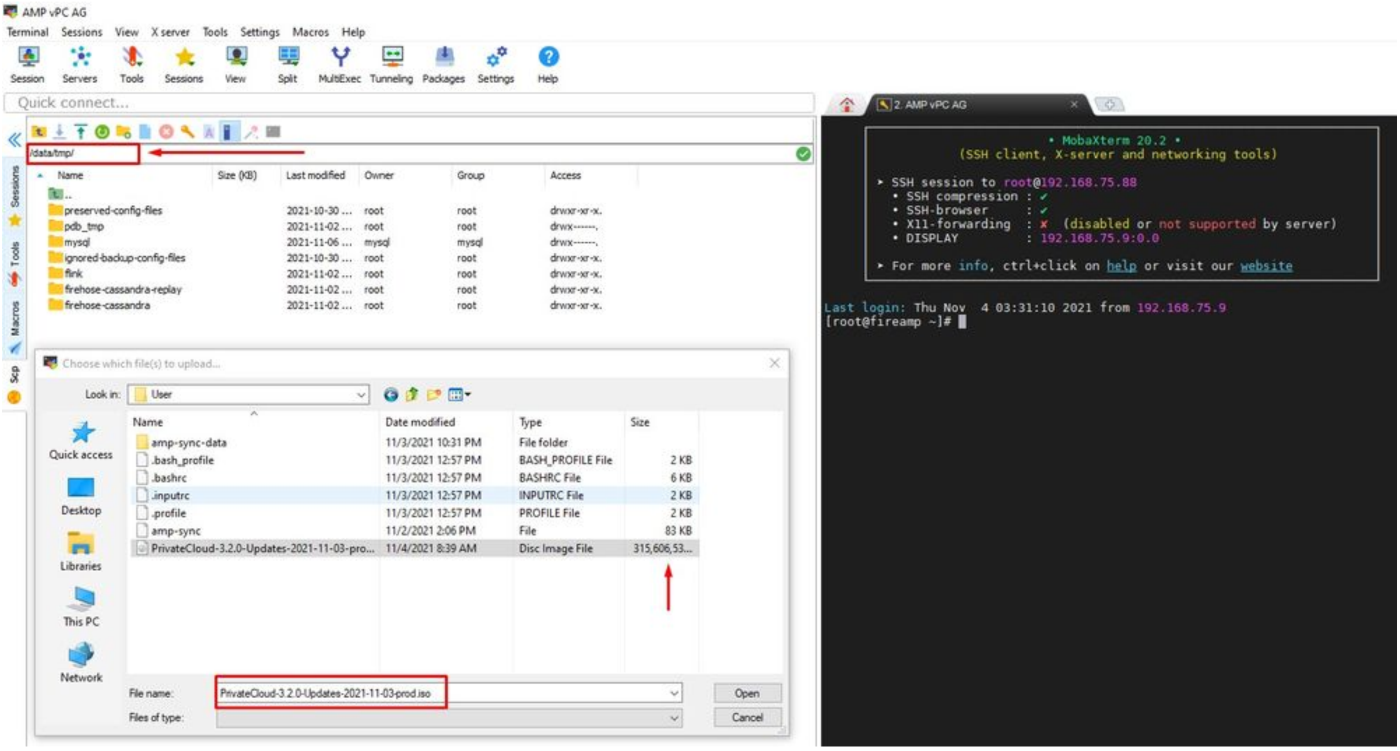
Previous Backups

The number of backups that will be stored on disk is: 1.

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20211106-0000.18.bak	738 MB	2021-11-06 00:03:43 +0000 about 17 hours ago	

將通過amp-sync生成的最新ISO傳輸到VPC。根據您的速度，這可能需要花費幾個小時。在本案中，移交時間超過16小時

```
/data/tmp
```


AMP vPC AG
Terminal Sessions View X server Tools Settings Macros Help
Session Servers Tools Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
Sessions Tools Macros Sftp
2. AMP vPC AG
Choose which file(s) to upload...
Look in: User
Quick access
Desktop
Libraries
This PC
Network
Open
Cancel

/data/tmp/

Name	Size (KB)	Last modified	Owner	Group	Access
..					
preserved-config-files		2021-10-30 ...	root	root	drwxr-xr-x.
pdb_tmp		2021-11-02 ...	root	root	drwx------.
mysql		2021-11-06 ...	mysql	mysql	drwx------.
ignored-backup-config-files		2021-10-30 ...	root	root	drwxr-xr-x.
flink		2021-11-02 ...	root	root	drwxr-xr-x.
firehose-cassandra-replay		2021-11-02 ...	root	root	drwxr-xr-x.
firehose-cassandra		2021-11-02 ...	root	root	drwxr-xr-x.

Name	Date modified	Type	Size
amp-sync-data	11/3/2021 10:31 PM	File folder	
.bash_profile	11/3/2021 12:57 PM	BASH_PROFILE File	2 KB
.bashrc	11/3/2021 12:57 PM	BASHRC File	6 KB
.inputrc	11/3/2021 12:57 PM	INPUTRC File	2 KB
.profile	11/3/2021 12:57 PM	PROFILE File	2 KB
amp-sync	11/2/2021 2:06 PM	File	83 KB
PrivateCloud-3.2.0-Updates-2021-11-03-pro...	11/4/2021 8:39 AM	Disc Image File	315,606,53...

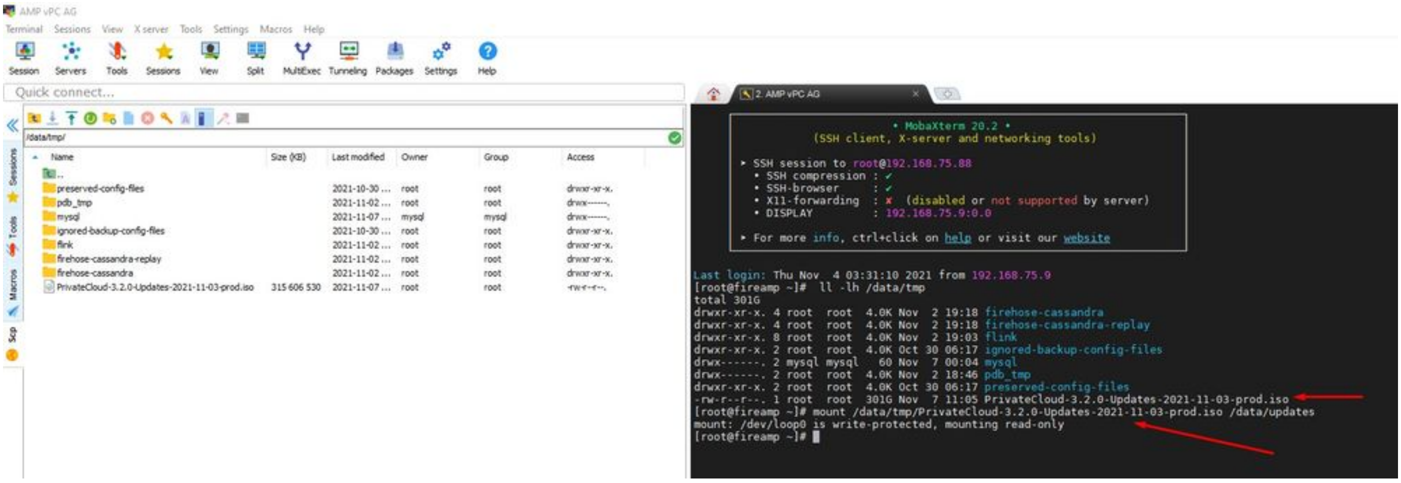
File name: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso

Files of type:

```
                    • MobaXterm 20.2 •
          (SSH client, X-server and networking tools)

 ➤ SSH session to root@192.168.75.88
   • SSH compression : ✓
   • SSH-browser     : ✓
   • X11-forwarding  : ✘  (disabled or not supported by server)
   • DISPLAY         : 192.168.75.9:0.0

 ➤ For more info, ctrl+click on help or visit our website

Last login: Thu Nov  4 03:31:10 2021 from 192.168.75.9
[root@fireamp ~]# 
```

上載完成後，裝載ISO

```
mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/
```

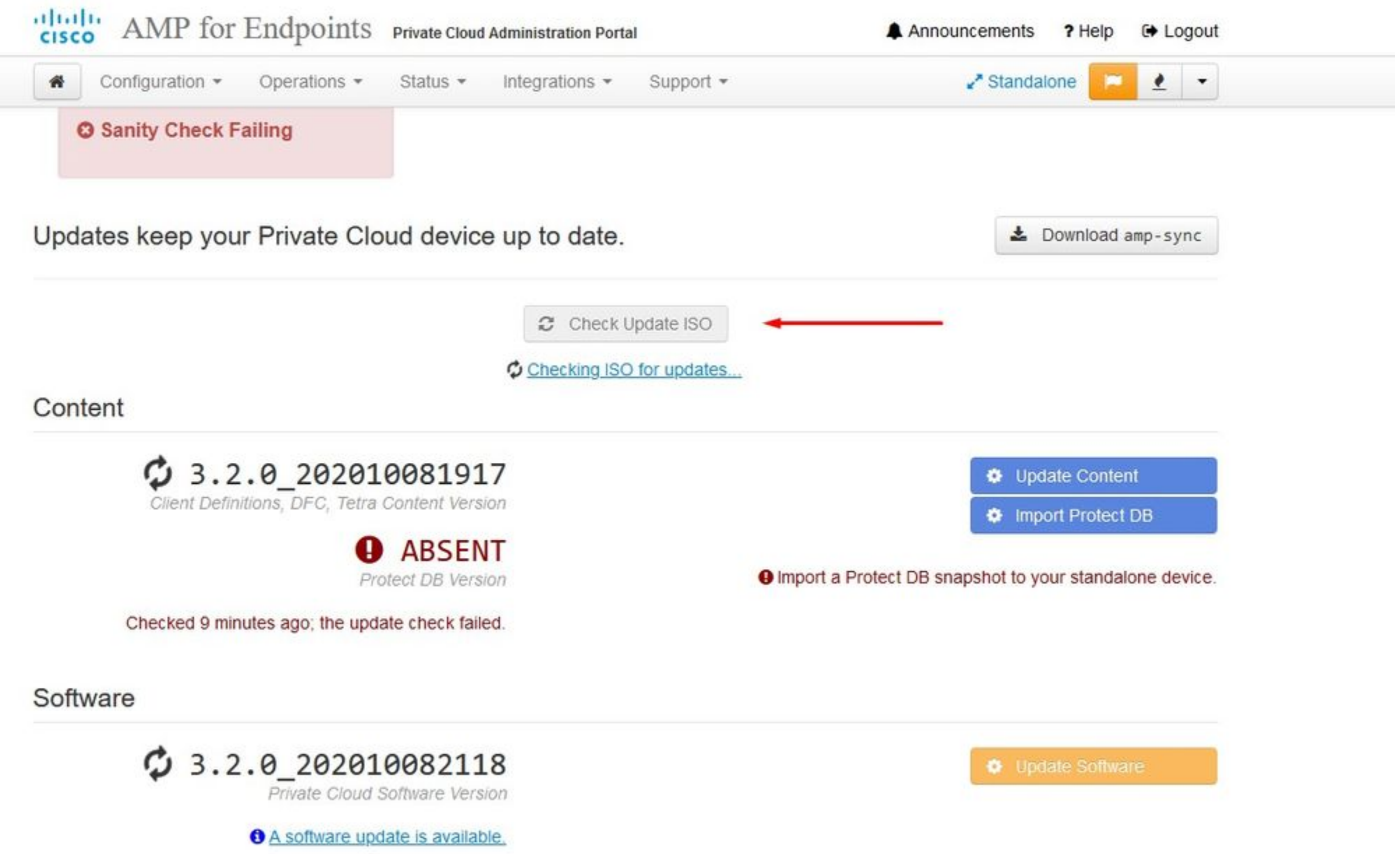

AMP vPC AG
Terminal Sessions View X server Tools Settings Macros Help
Session Servers Tools Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
Sessions Tools Macros Sftp
2. AMP vPC AG

/data/tmp/

Name	Size (KB)	Last modified	Owner	Group	Access
..					
preserved-config-files		2021-10-30 ...	root	root	drwxr-xr-x.
pdb_tmp		2021-11-02 ...	root	root	drwx------.
mysql		2021-11-07 ...	mysql	mysql	drwx------.
ignored-backup-config-files		2021-10-30 ...	root	root	drwxr-xr-x.
flink		2021-11-02 ...	root	root	drwxr-xr-x.
firehose-cassandra-replay		2021-11-02 ...	root	root	drwxr-xr-x.
firehose-cassandra		2021-11-02 ...	root	root	drwxr-xr-x.
PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso	315 606 530	2021-11-07 ...	root	root	-rw-r--r--.

```
                    • MobaXterm 20.2 •
          (SSH client, X-server and networking tools)

 ➤ SSH session to root@192.168.75.88
   • SSH compression : ✓
   • SSH-browser     : ✓
   • X11-forwarding  : ✘  (disabled or not supported by server)
   • DISPLAY         : 192.168.75.9:0.0

 ➤ For more info, ctrl+click on help or visit our website

Last login: Thu Nov  4 03:31:10 2021 from 192.168.75.9
[root@fireamp ~]#  ll -lh /data/tmp
total 301G
drwxr-xr-x. 4 root  root  4.0K Nov  2 19:18 firehose-cassandra
drwxr-xr-x. 4 root  root  4.0K Nov  2 19:18 firehose-cassandra-replay
drwxr-xr-x. 8 root  root  4.0K Nov  2 19:03 flink
drwxr-xr-x. 2 root  root  4.0K Oct 30 06:17 ignored-backup-config-files
drwx------. 2 mysql mysql   60 Nov  7 00:04 mysql
drwx------. 2 root  root  4.0K Nov  2 18:46 pdb_tmp
drwxr-xr-x. 2 root  root  4.0K Oct 30 06:17 preserved-config-files
-rw-r--r--. 1 root  root  301G Nov  7 11:05 PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso
[root@fireamp ~]# mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates
mount: /dev/loop0 is write-protected, mounting read-only
[root@fireamp ~]# 
```

導航到opdamin UI以執行更新 操作>更新裝置>選擇檢查更新ISO。



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Checking ISO for updates...

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

Checked 9 minutes ago; the update check failed.

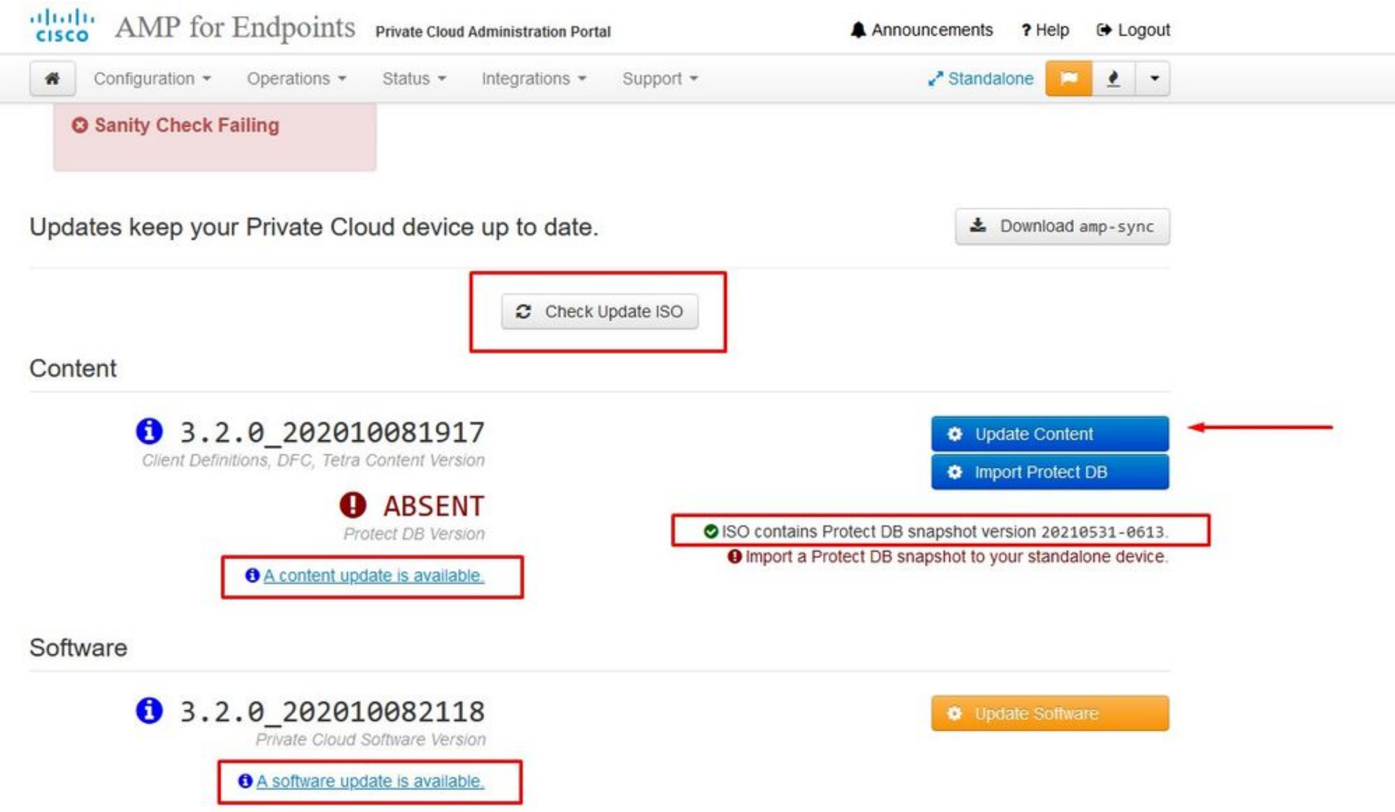
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

在本例中，我首先繼續更新內容



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

A content update is available.

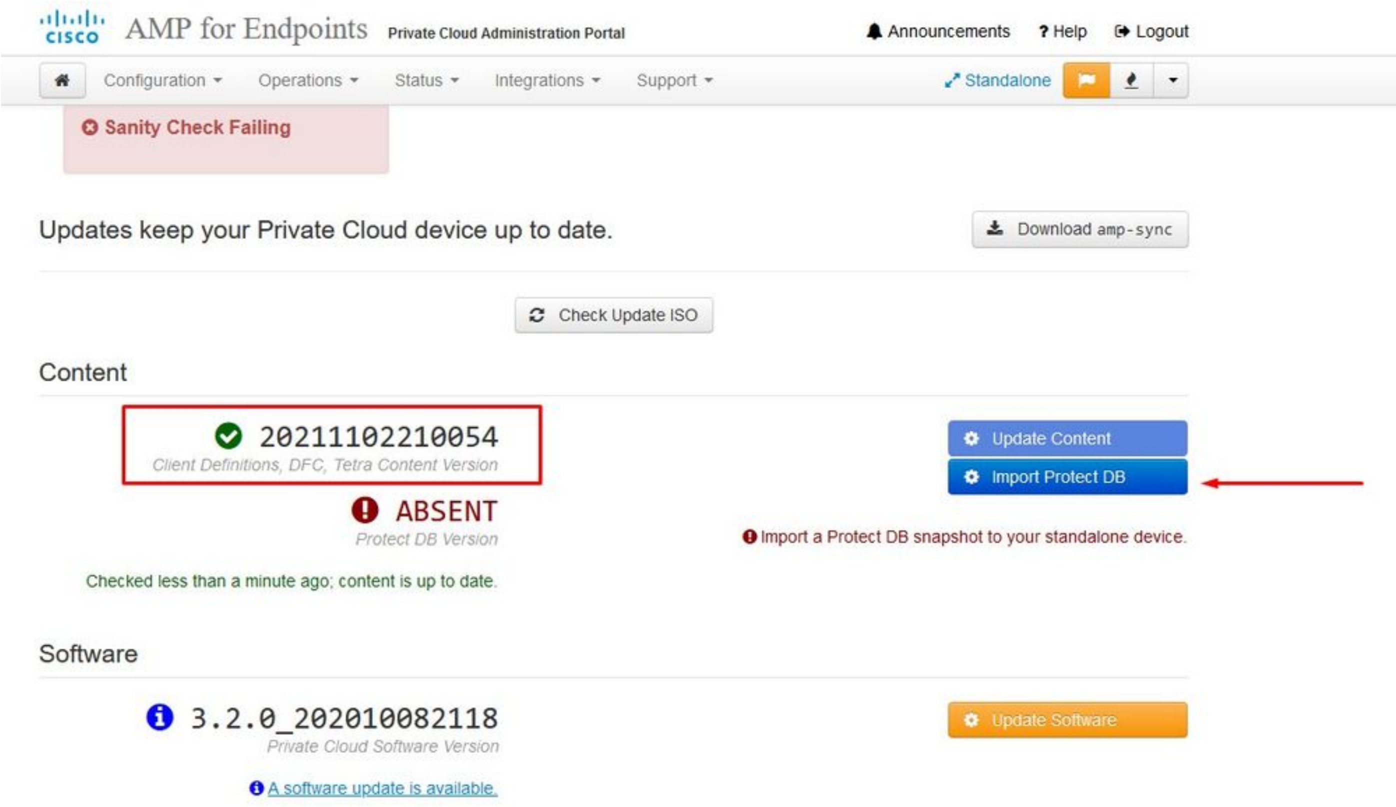
ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

然後選擇Import Protect DB。



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Content

✓ 20211102210054
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

Checked less than a minute ago; content is up to date.

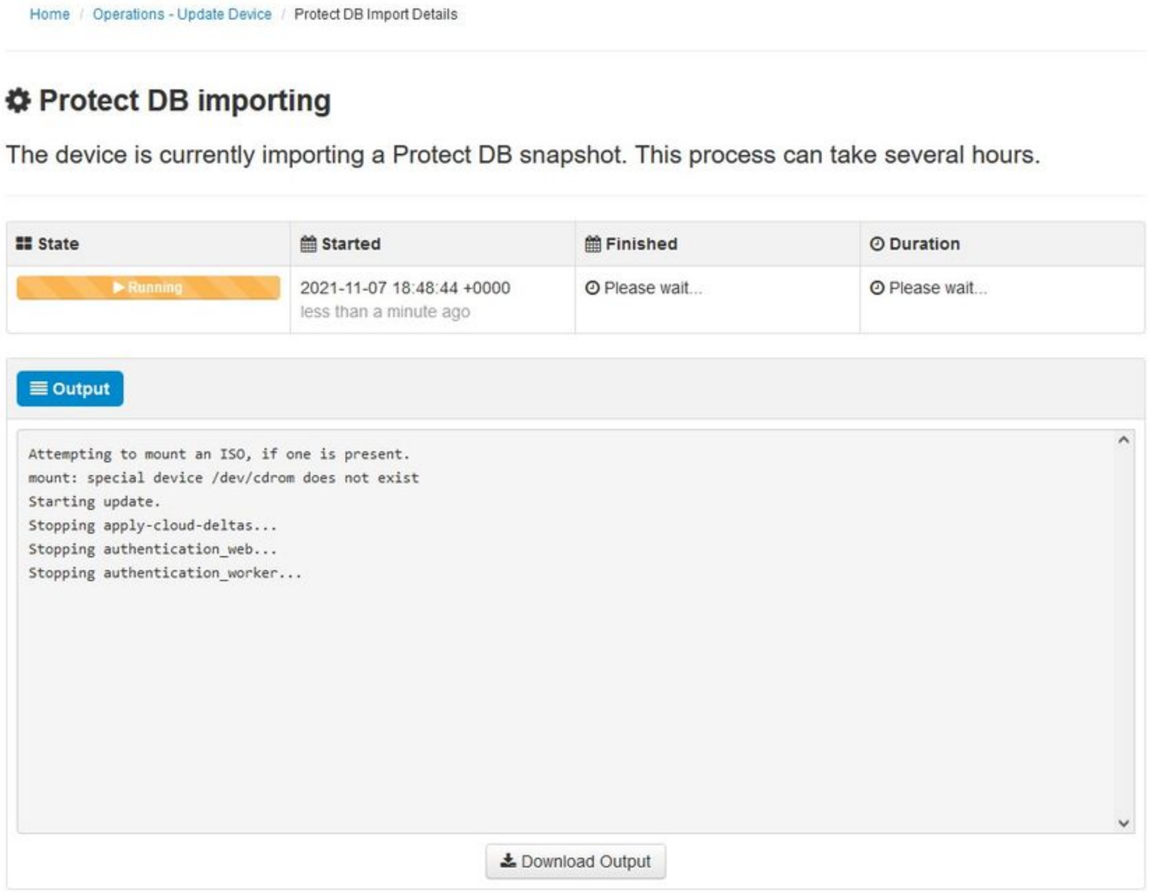
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

您可以看到，這是另一個很長的過程，需要很長時間才能完成。

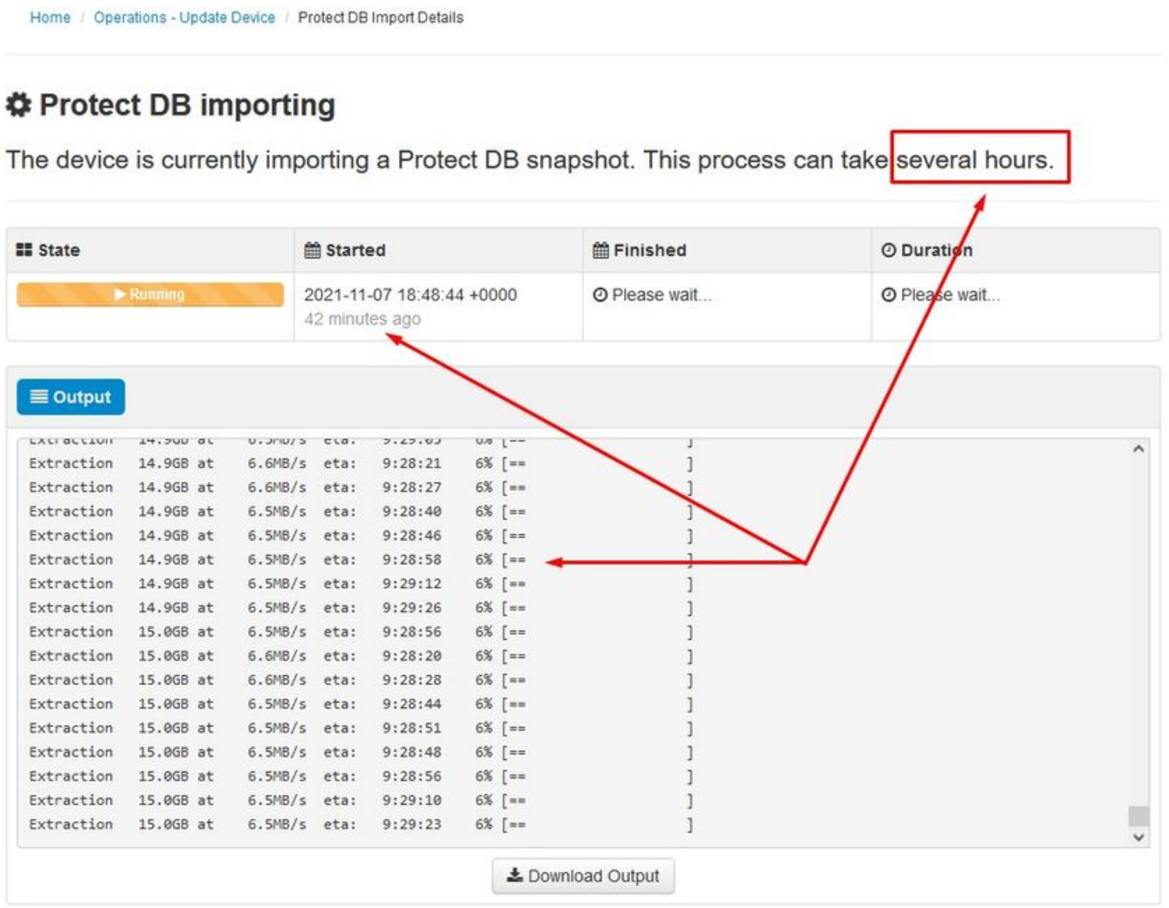

Home / Operations - Update Device / Protect DB Import Details
Output
Download Output

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-07 18:48:44 +0000 less than a minute ago	Please wait...	Please wait...

```
Attempting to mount an ISO, if one is present.
mount: special device /dev/cdrom does not exist
Starting update.
Stopping apply-cloud-deltas...
Stopping authentication_web...
Stopping authentication_worker...
```

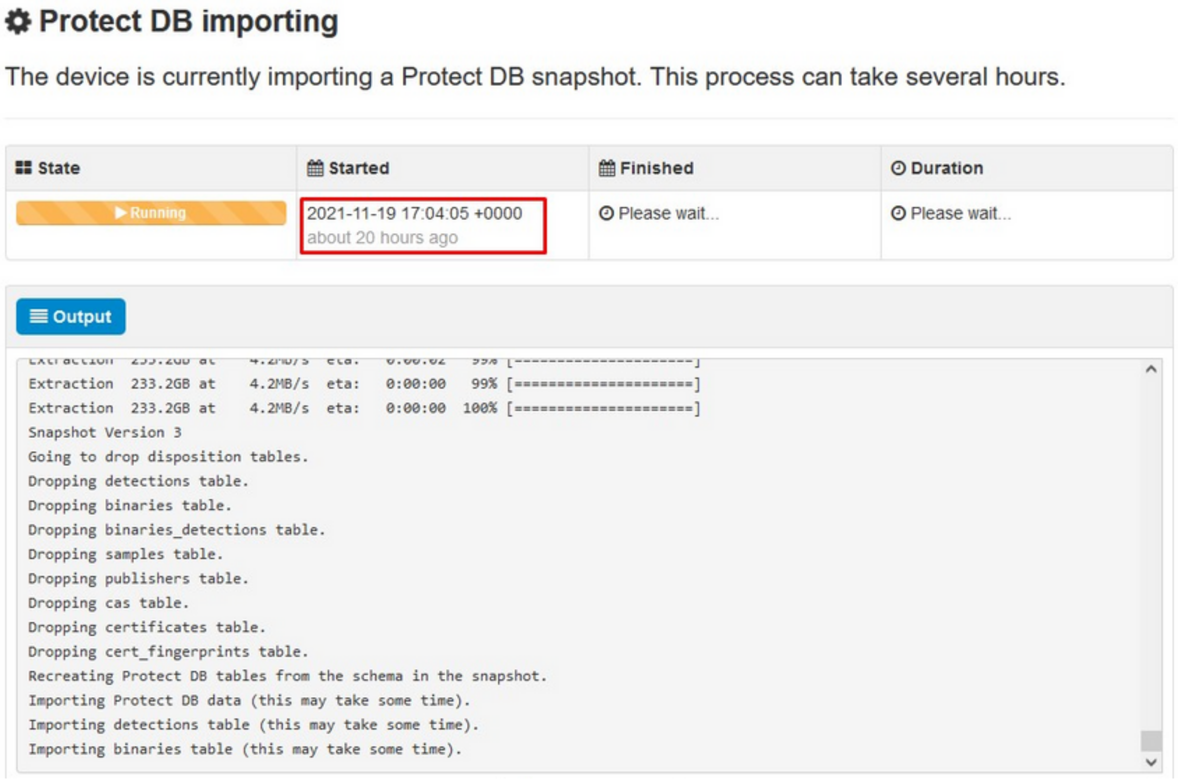

Home / Operations - Update Device / Protect DB Import Details
Output
Download Output

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-07 18:48:44 +0000 42 minutes ago	Please wait...	Please wait...

```
Extraction   14.9GB at    6.5MB/s  eta:   9:29:05    6% [==                    ]
Extraction   14.9GB at    6.6MB/s  eta:   9:28:21    6% [==                    ]
Extraction   14.9GB at    6.6MB/s  eta:   9:28:27    6% [==                    ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:40    6% [==                    ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:46    6% [==                    ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:58    6% [==                    ]
Extraction   14.9GB at    6.5MB/s  eta:   9:29:12    6% [==                    ]
Extraction   14.9GB at    6.5MB/s  eta:   9:29:26    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:56    6% [==                    ]
Extraction   15.0GB at    6.6MB/s  eta:   9:28:20    6% [==                    ]
Extraction   15.0GB at    6.6MB/s  eta:   9:28:28    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:44    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:51    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:48    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:56    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:29:10    6% [==                    ]
Extraction   15.0GB at    6.5MB/s  eta:   9:29:23    6% [==                    ]
```



Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

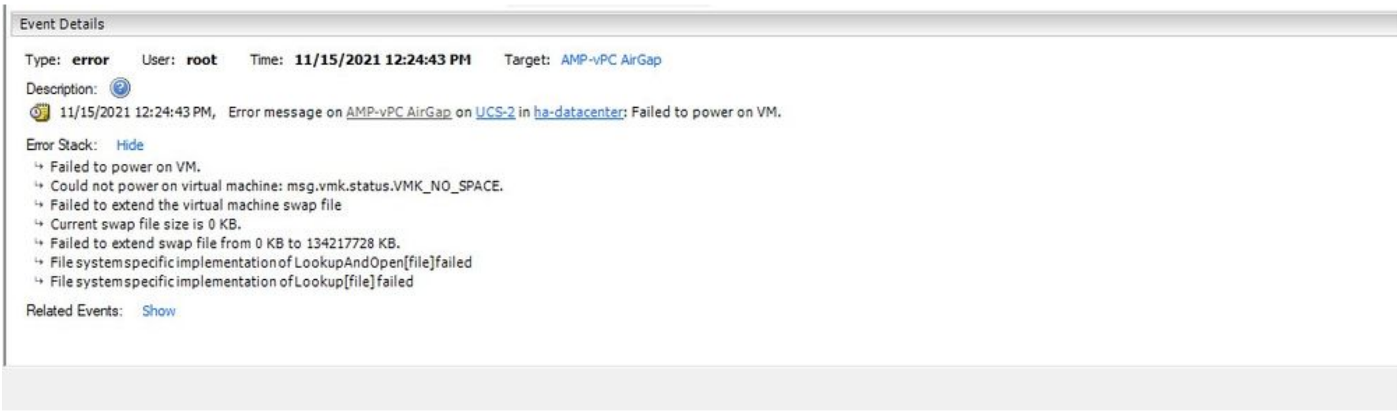
State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...	Please wait...

```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:02   99% [======================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   99% [======================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00  100% [======================]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

問題#1 — 資料儲存中的房間已耗盡

在這裡，您可以找到兩個問題。由於3.5.2版之前的vPC無法安裝外部NFS儲存，因此您必須將更新ISO檔案上傳到/data/temp目錄。就我的情況而言，由於我的資料儲存區只有1TB，所以我用完了房間，虛擬機器崩潰了。換句話說，您至少需要2 TB的資料儲存空間才能成功部署低於3.5.2版的AirGap VPC

以下影象來自ESXi伺服器，它顯示了當您嘗試啟動VM時HDD上不再有可用空間的錯誤。通過將128 GB RAM臨時切換到64 GB，我可以從此錯誤中恢復。然後我又重新開始了。另外請記住，如果您將此VM配置為瘦客戶端，則瘦客戶端部署的缺點是磁碟大小可以增大，但即使您釋放一些空間，磁碟大小也不會縮小。換句話說，假設您將300GB的檔案上傳到vPC的目錄，然後將其刪除。ESXi中的磁碟仍然顯示硬碟上減少了300 GB的空間



Event Details

Type: **error** User: **root** Time: **11/15/2021 12:24:43 PM** Target: AMP-vPC AirGap

Description:

11/15/2021 12:24:43 PM, Error message on AMP-vPC AirGap on UCS-2 in ha-datacenter: Failed to power on VM.

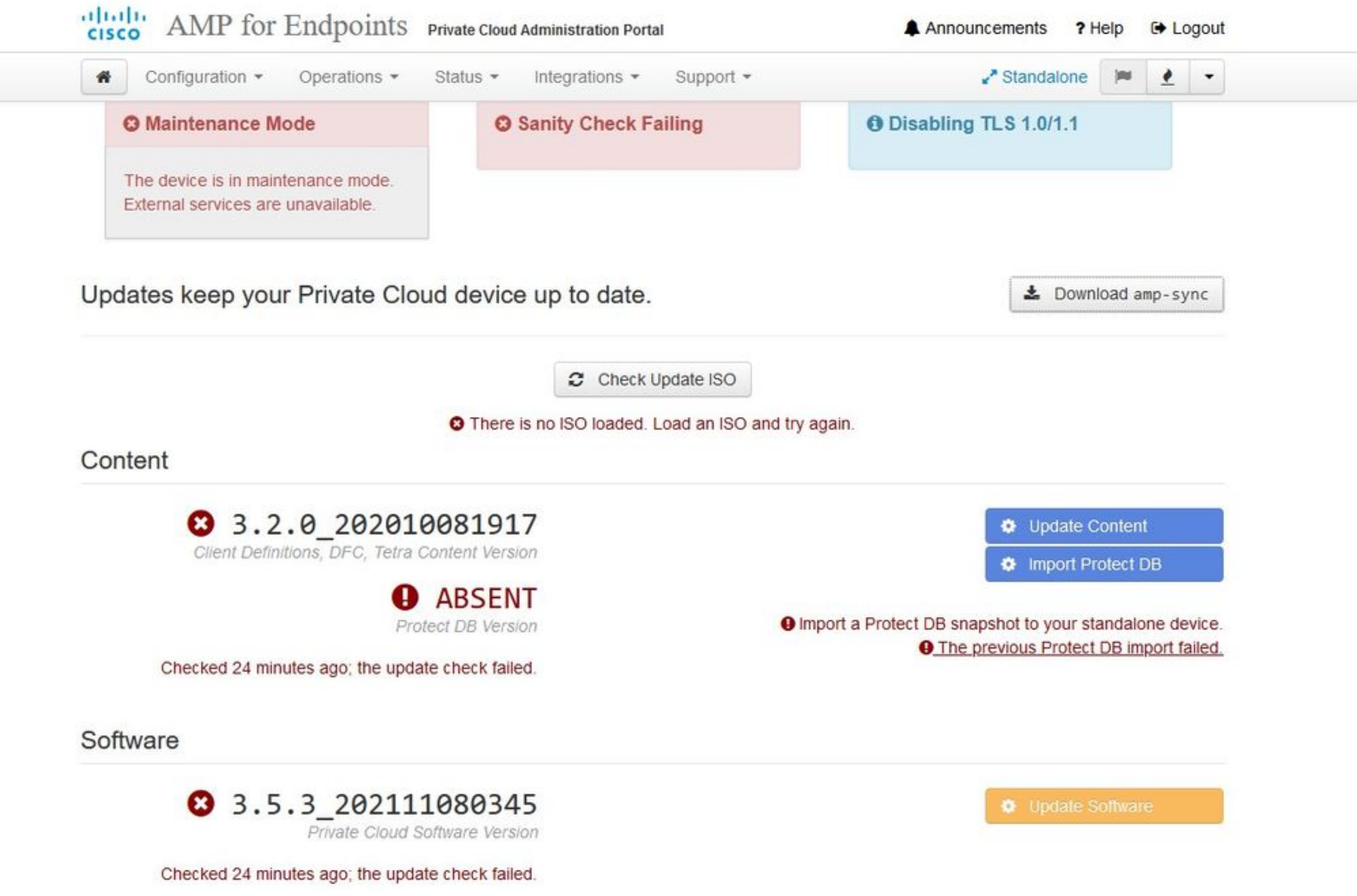
Error Stack: Hide

```
↳ Failed to power on VM.
↳ Could not power on virtual machine: msg.vmk.status.VMK_NO_SPACE.
↳ Failed to extend the virtual machine swap file
↳ Current swap file size is 0 KB.
↳ Failed to extend swap file from 0 KB to 134217728 KB.
↳ File system specific implementation of LookupAndOpen[file] failed
↳ File system specific implementation of Lookup[file] failed
```

Related Events: Show

問題#2 — 舊更新

第2^{個問題}是，如果您先運行軟體更新，就像我在第2^{次}試用時所做的那樣，從3.2.0開始，我最終使用VPC升級到3.5.2。因此，我不得不下載全新的ISO更新檔案，因為3.2.0版本因我不再使用原始3.2.0版本而變得無效。



Maintenance Mode

The device is in maintenance mode. External services are unavailable.

Sanity Check Failing

Disabling TLS 1.0/1.1

Updates keep your Private Cloud device up to date.

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

Checked 24 minutes ago; the update check failed.

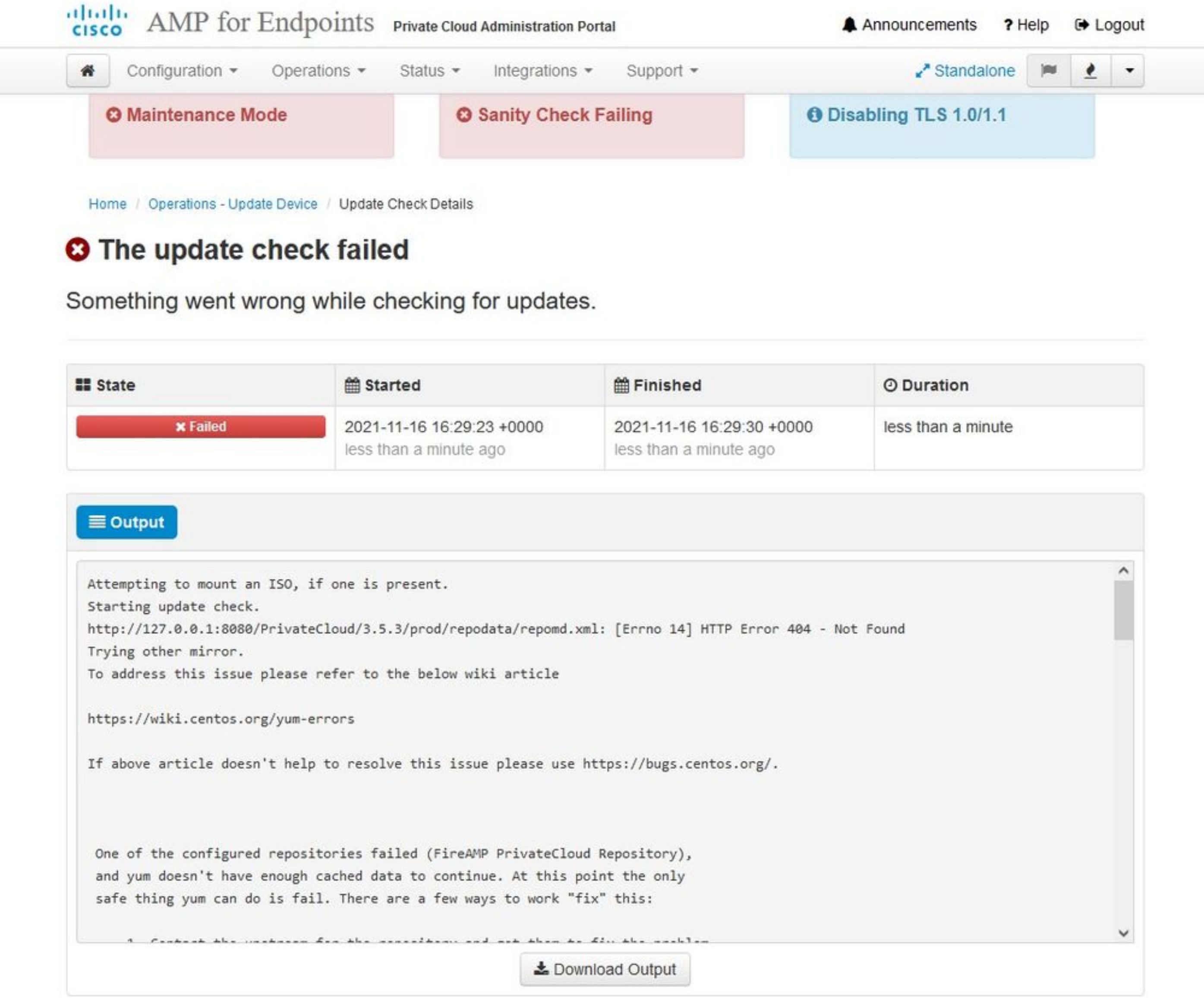
Import a Protect DB snapshot to your standalone device.
The previous Protect DB import failed.

Software

3.5.3_202111080345
Private Cloud Software Version

Checked 24 minutes ago; the update check failed.

如果您嘗試再次裝載ISO更新檔案，將會看到此錯誤。



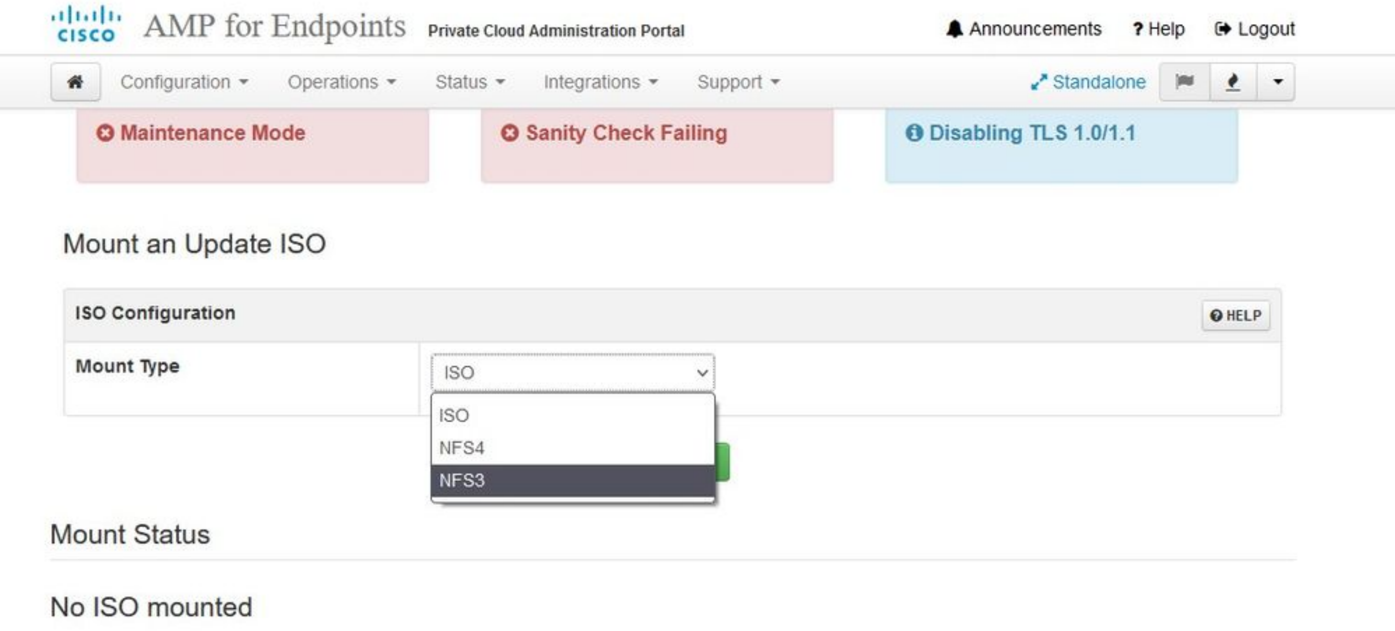
The update check failed

Something went wrong while checking for updates.

State	Started	Finished	Duration
✖ Failed	2021-11-16 16:29:23 +0000 less than a minute ago	2021-11-16 16:29:30 +0000 less than a minute ago	less than a minute

```
Attempting to mount an ISO, if one is present.
Starting update check.
http://127.0.0.1:8080/PrivateCloud/3.5.3/prod/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below wiki article

https://wiki.centos.org/yum-errors

If above article doesn't help to resolve this issue please use https://bugs.centos.org/.



 One of the configured repositories failed (FireAMP PrivateCloud Repository),
 and yum doesn't have enough cached data to continue. At this point the only
 safe thing yum can do is fail. There are a few ways to work "fix" this:

     1. Contact the upstream for the repository and get them to fix the problem.
```

此圖片顯示了如何將更新映像裝載到VPC的替代方法。在3.5.x版中，您可以使用遠端位置（如NFS儲存）與VPC共用更新檔案。



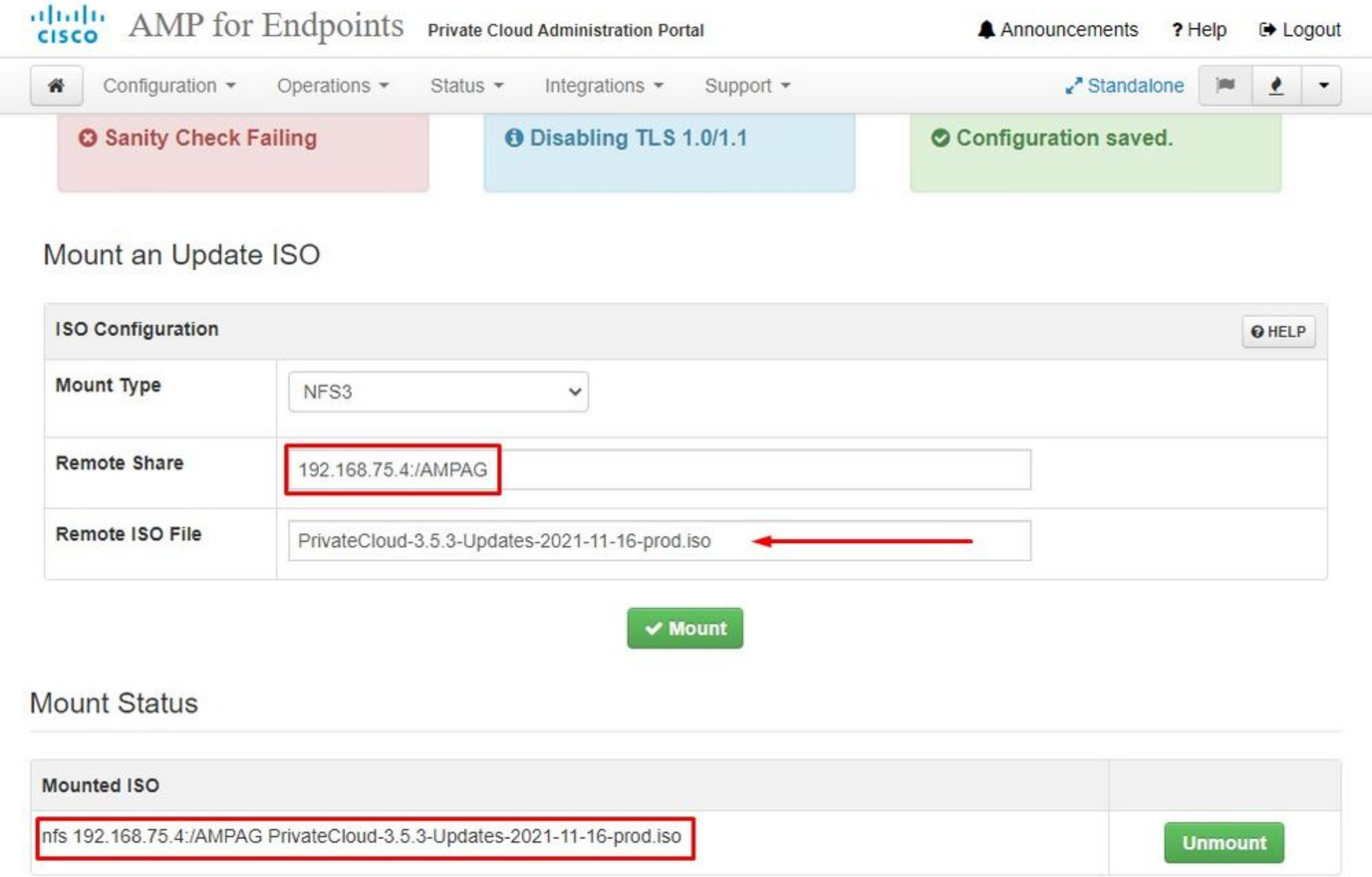
Mount an Update ISO

ISO Configuration

Mount Type: ISO

Mount Status

No ISO mounted



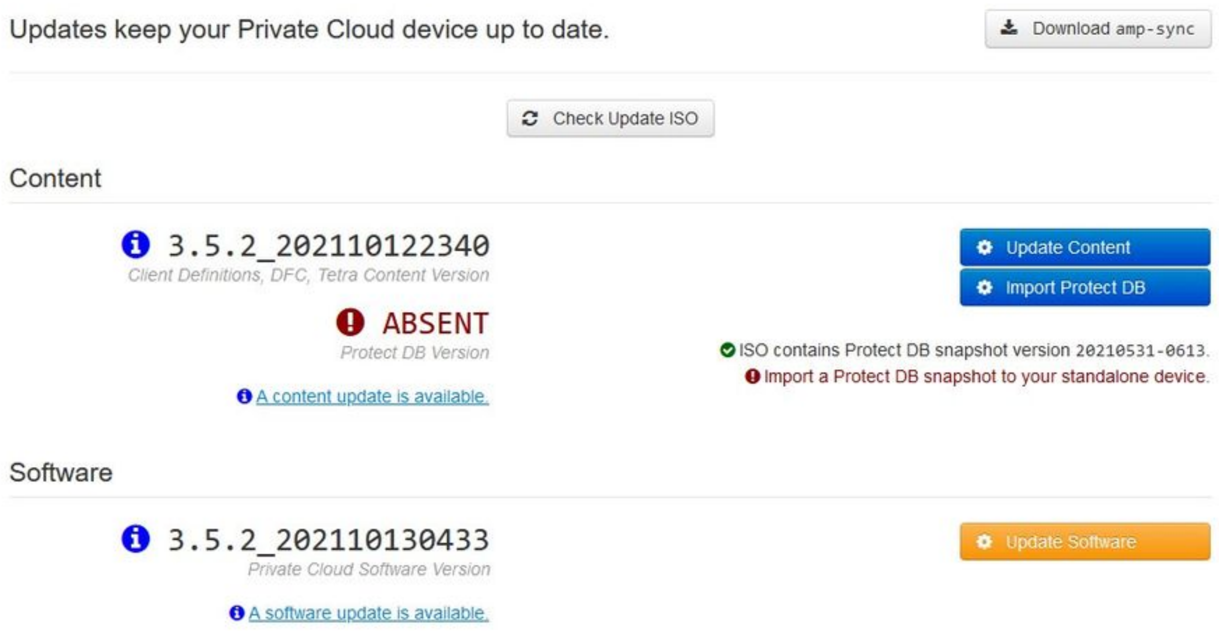
Mount an Update ISO

ISO Configuration

Mount Type	NFS3
Remote Share	192.168.75.4:/AMPAG
Remote ISO File	PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Mount Status

Mounted ISO	
nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso	Unmount



Updates keep your Private Cloud device up to date.

Content

3.5.2_202110122340
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

A content update is available.

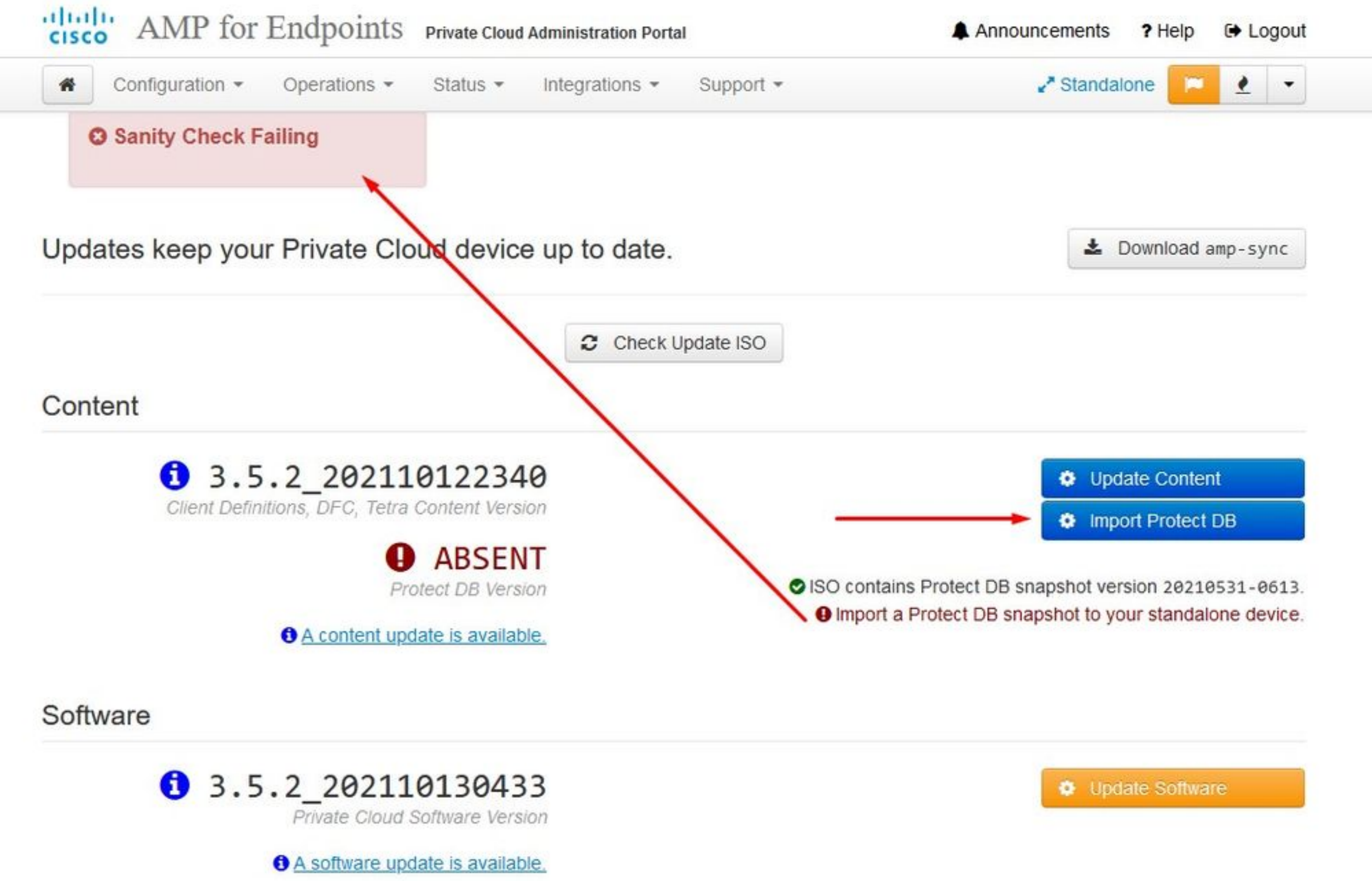
ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.5.2_202110130433
Private Cloud Software Version

A software update is available.

Sanity Check Failing與Protect DB not currently available on the VPC（保護當前在VPC上不可用的資料庫）有關



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Content

3.5.2_202110122340
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

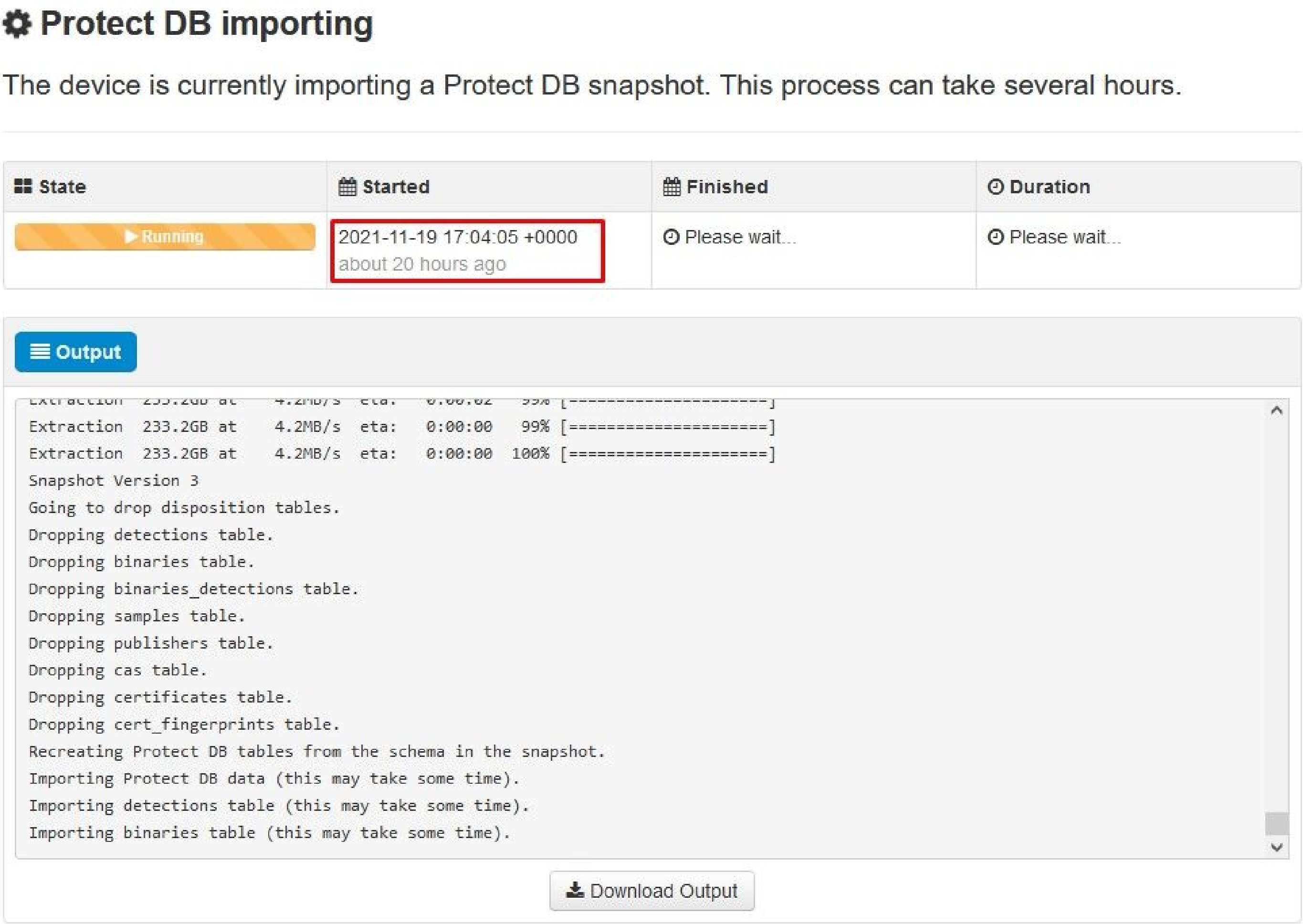
A content update is available.

ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.5.2_202110130433
Private Cloud Software Version

A software update is available.

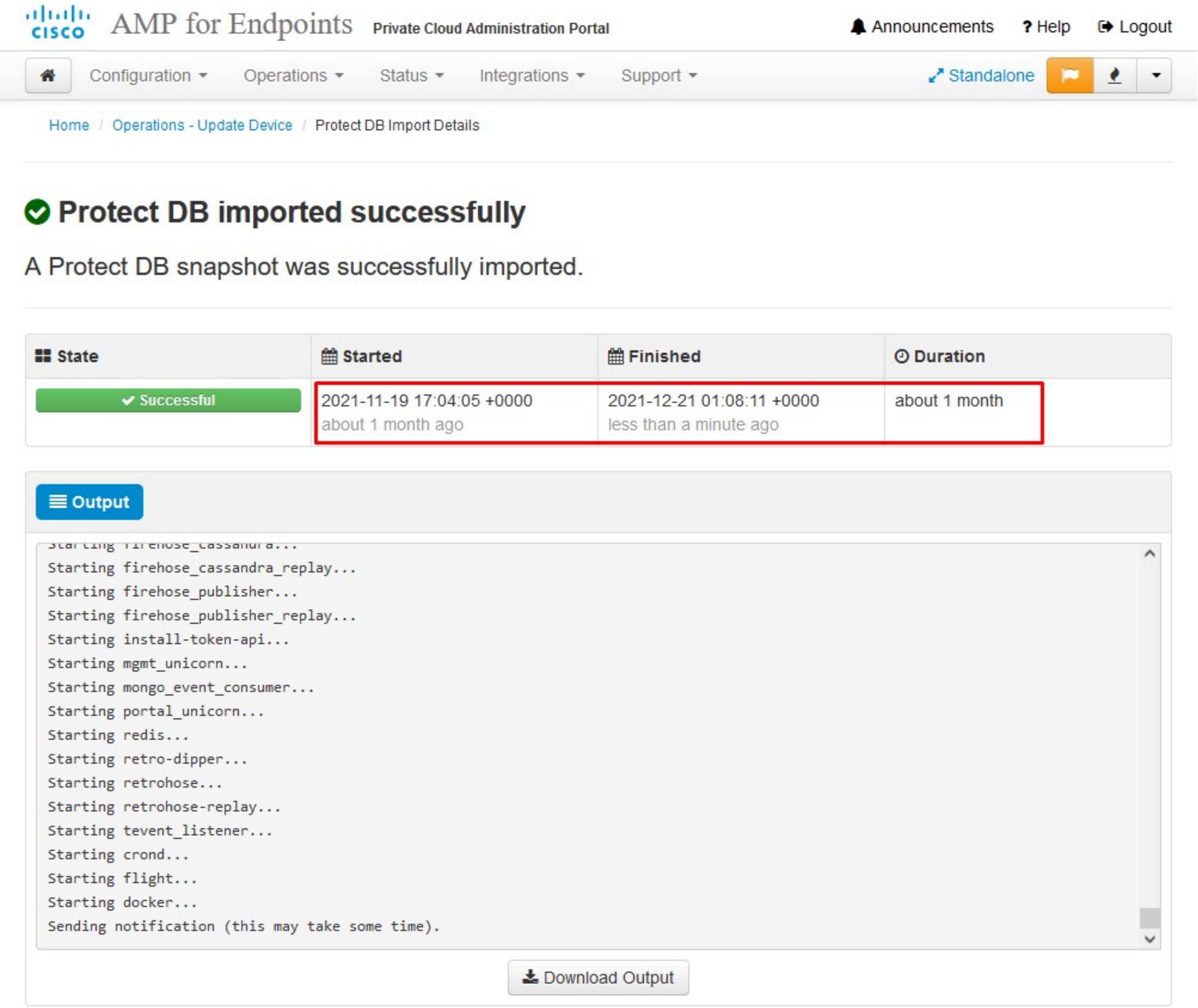


Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...	Please wait...

```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:02   99% [=====================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   99% [=====================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00  100% [=====================]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```



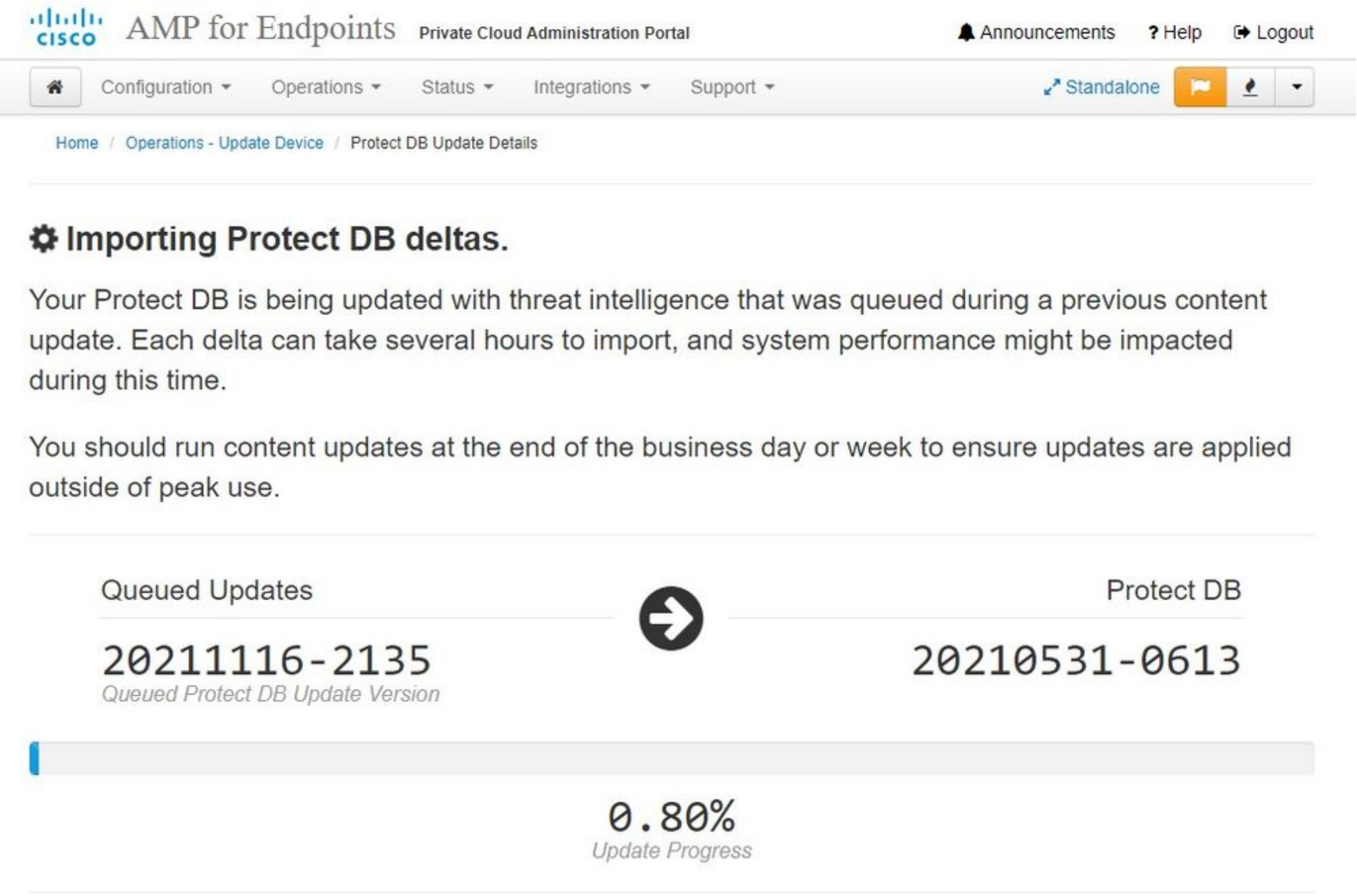
Protect DB imported successfully

A Protect DB snapshot was successfully imported.

State	Started	Finished	Duration
✓ Successful	2021-11-19 17:04:05 +0000 about 1 month ago	2021-12-21 01:08:11 +0000 less than a minute ago	about 1 month

```
Starting firehose_cassandra...
Starting firehose_cassandra_replay...
Starting firehose_publisher...
Starting firehose_publisher_replay...
Starting install-token-api...
Starting mgmt_unicorn...
Starting mongo_event_consumer...
Starting portal_unicorn...
Starting redis...
Starting retro-dipper...
Starting retrohose...
Starting retrohose-replay...
Starting tevent_listener...
Starting crond...
Starting flight...
Starting docker...
Sending notification (this may take some time).
```

下一次更新自動啟動



Importing Protect DB deltas.

Your Protect DB is being updated with threat intelligence that was queued during a previous content update. Each delta can take several hours to import, and system performance might be impacted during this time.

You should run content updates at the end of the business day or week to ensure updates are applied outside of peak use.

Queued Updates

20211116-2135

Queued Protect DB Update Version

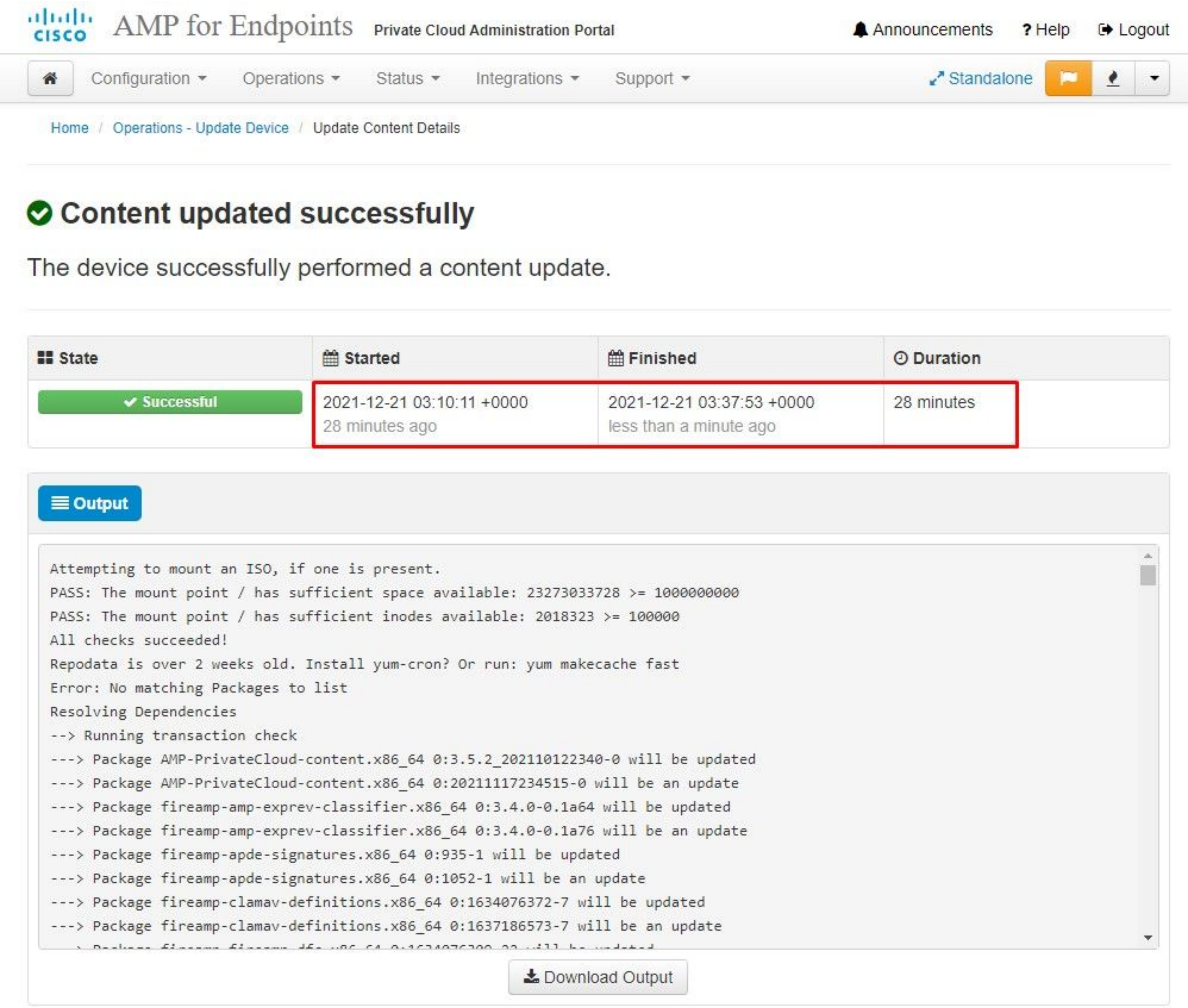
Protect DB

20210531-0613

0.80%

Update Progress

在匯入保護資料庫這一非常漫長的過程之後，您可以移動並更新客戶端定義和軟體，這大約需要花費3小時以上的時間。



Content updated successfully

The device successfully performed a content update.

State	Started	Finished	Duration
✓ Successful	2021-12-21 03:10:11 +0000 28 minutes ago	2021-12-21 03:37:53 +0000 less than a minute ago	28 minutes

```
Attempting to mount an ISO, if one is present.
PASS: The mount point / has sufficient space available: 23273033728 >= 1000000000
PASS: The mount point / has sufficient inodes available: 2018323 >= 100000
All checks succeeded!
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
---> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
---> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
---> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
---> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
---> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
---> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
---> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
---> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
---> Package fireamp-fireamp-dfc.x86_64 0:1634076300-22 will be updated
```

最後，請注意，此過程將花費很長時間。

對於VPC裝置，請訪問包含如何更新HW裝置、裝載ISO檔案以及從USB引導的其他方法的TZ。

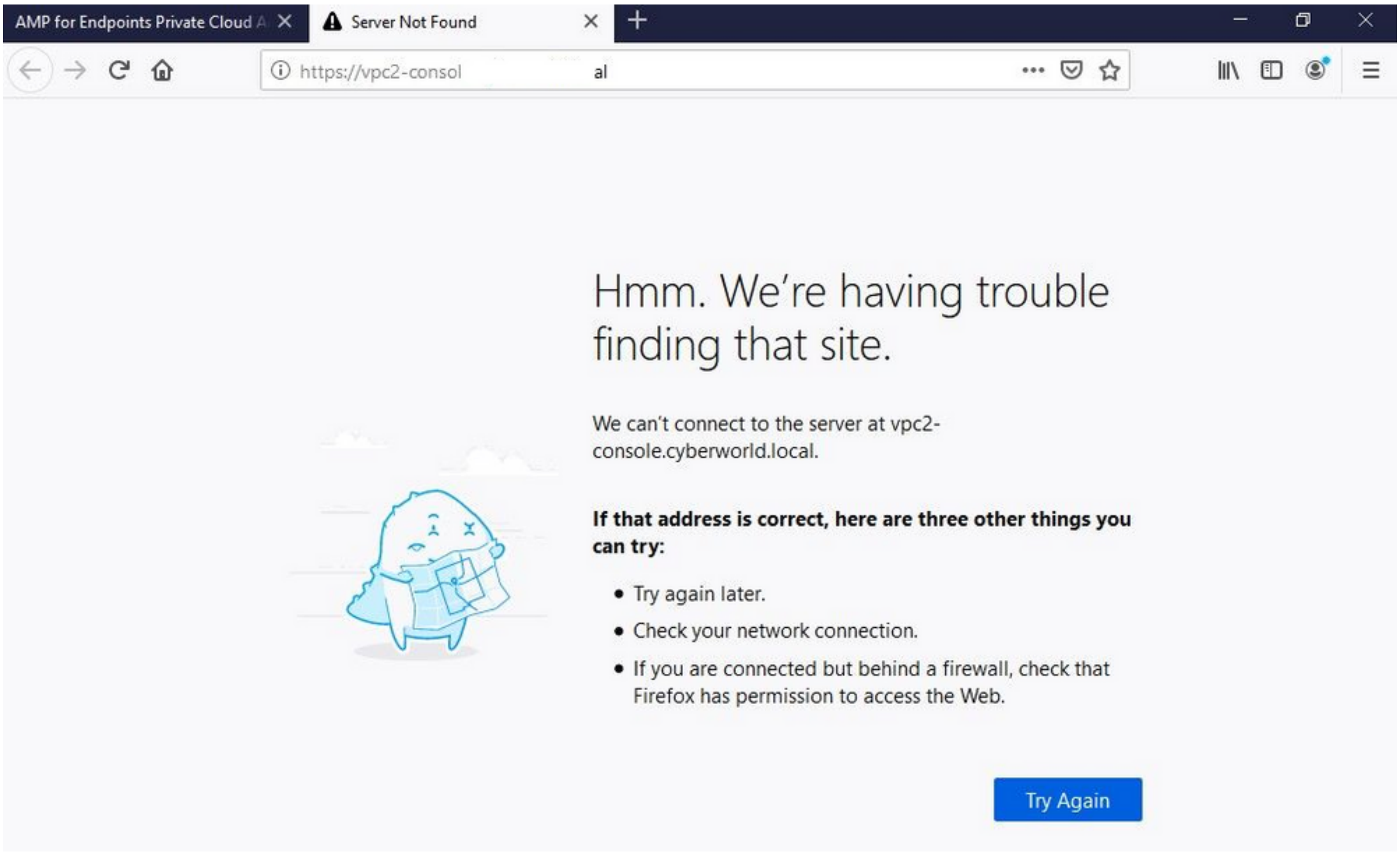
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

僅︽︽︽AIRGAP ︽

基本故障排除

問題#1理 — FQDN和DNS伺服器

第一個可能遇到的問題是您的DNS伺服器未建立，並且所有FQDN均未正確記錄和解析。當您嘗試通過安全終結點「fire」圖示導航到安全終結點控制檯時，問題可能如下所示。 如果只使用IP地址，則可以使用它，但無法下載聯結器。你可以從下面的第三張圖片看到。


AMP for Endpoints Private Cloud A
Server Not Found
https://vpc2-consol   al
Try Again

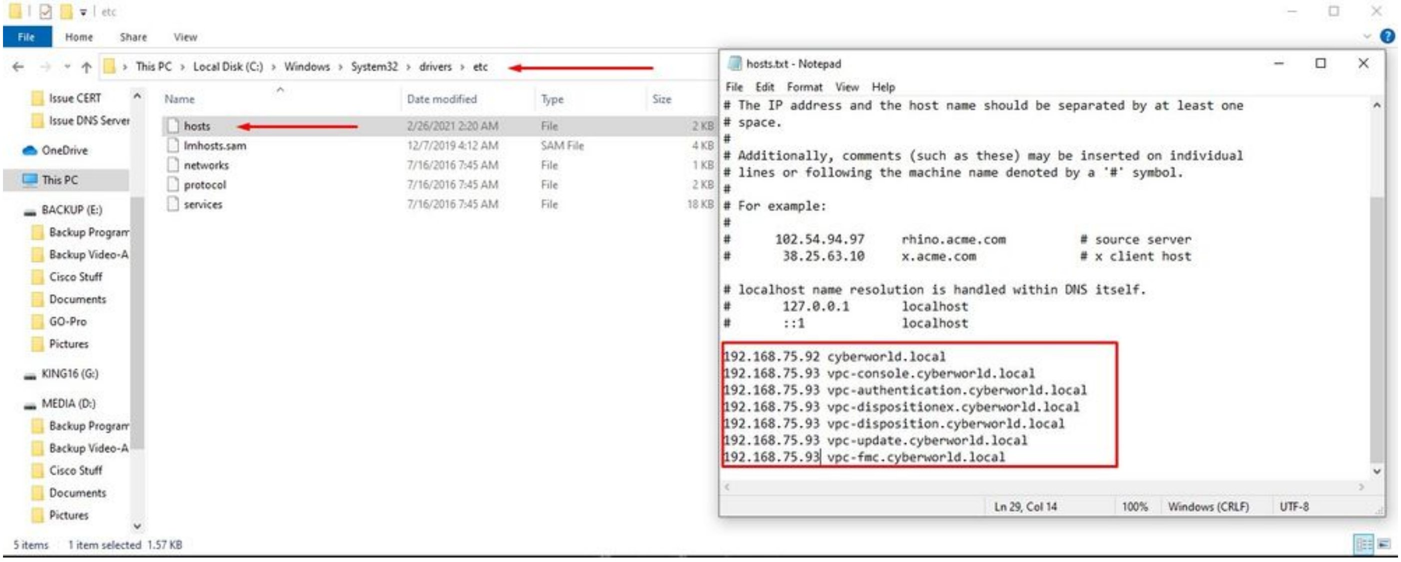
Hmm. We're having trouble finding that site.

We can't connect to the server at vpc2-console.cyberworld.local.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

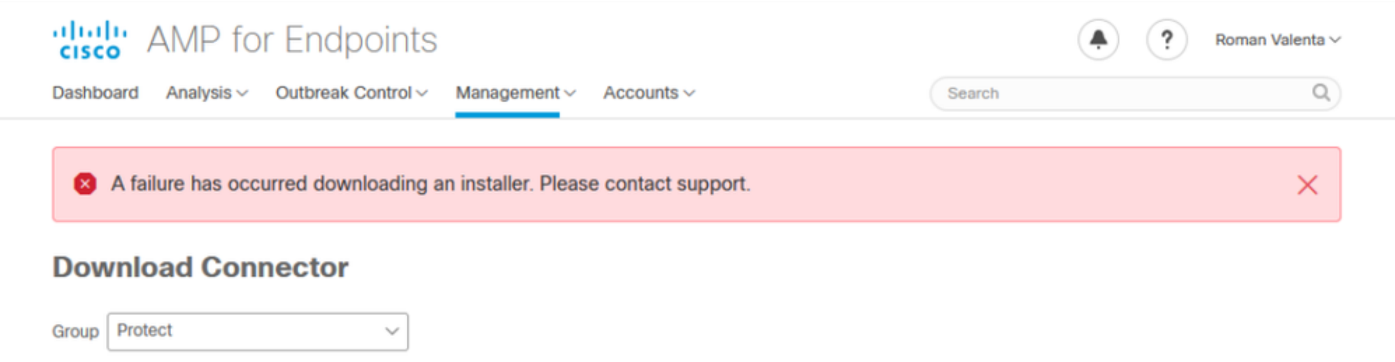
如果在本地電腦上修改了HOSTS檔案（如圖所示），可以解決此問題，但最終會出現錯誤。



Name	Date modified	Type	Size
hosts	2/26/2021 2:20 AM	File	2 KB
lmhosts.sam	12/7/2019 4:12 AM	SAM File	4 KB
networks	7/16/2016 7:45 AM	File	1 KB
protocol	7/16/2016 7:45 AM	File	2 KB
services	7/16/2016 7:45 AM	File	18 KB

```
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.75.92 cyberworld.local
192.168.75.93 vpc-console.cyberworld.local
192.168.75.93 vpc-authentication.cyberworld.local
192.168.75.93 vpc-dispositionex.cyberworld.local
192.168.75.93 vpc-disposition.cyberworld.local
192.168.75.93 vpc-update.cyberworld.local
192.168.75.93 vpc-fmc.cyberworld.local
```

嘗試下載安全終結點聯結器安裝程式時收到此錯誤。



A failure has occurred downloading an installer. Please contact support.

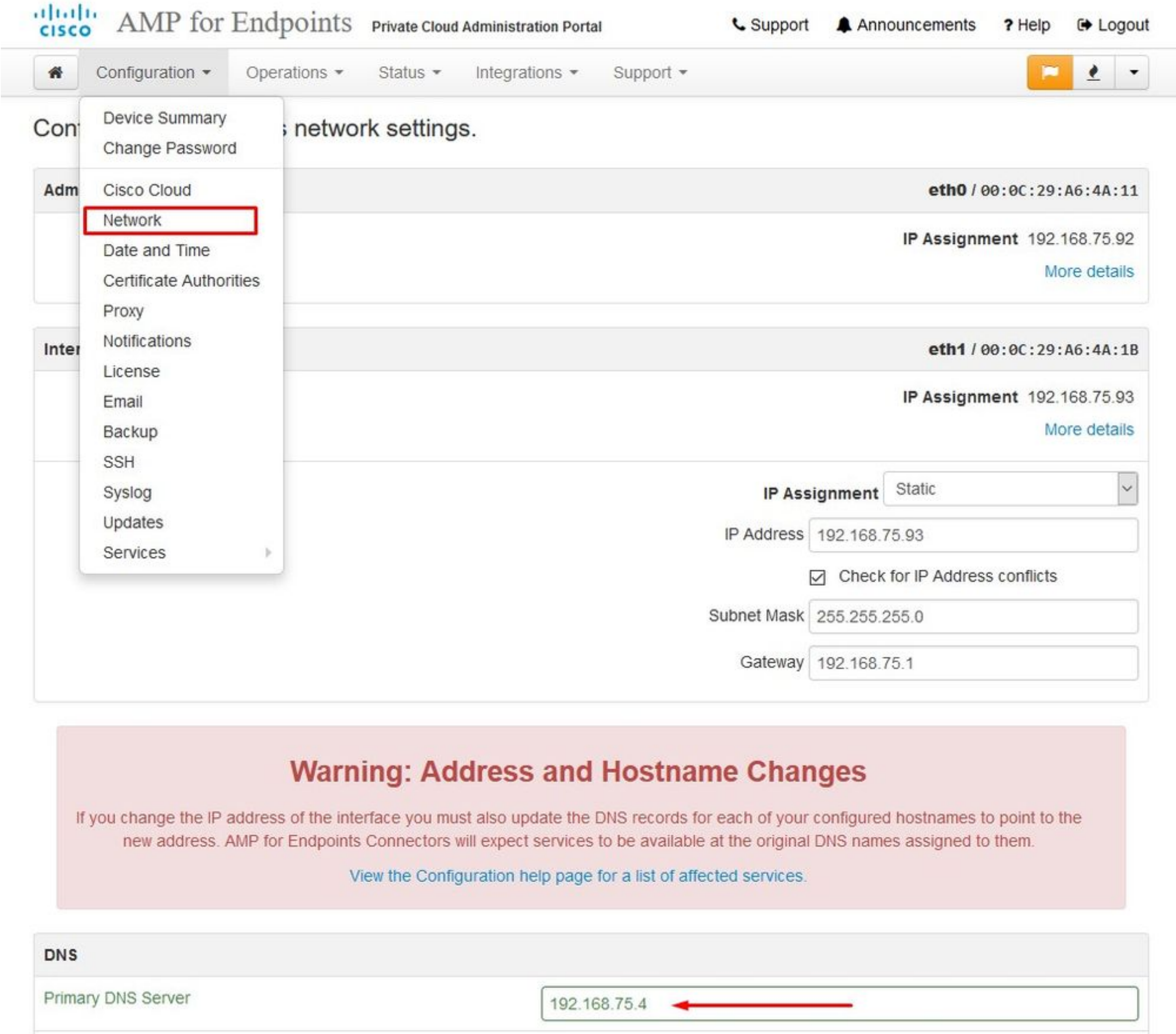
Download Connector

Group: Protect

經過一些故障排除後，唯一正確的解決方案是設定DNS伺服器。

```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0
================================================================================
Server:         8.8.8.x
Address:        8.8.8.x#53

** server can't find vPC-Console.cyberworld.local: NXDOMAIN
```

在DNS伺服器中記錄所有FQDN並將虛擬私有雲中的記錄從公共DNS更改為DNS伺服器後，一切都將按照預期開始工作。



Con… network settings.

Adm… **eth0** / 00:0C:29:A6:4A:11

IP Assignment 192.168.75.92

Inter… **eth1** / 00:0C:29:A6:4A:1B

IP Assignment 192.168.75.93

IP Assignment Static

IP Address 192.168.75.93

☑ Check for IP Address conflicts

Subnet Mask 255.255.255.0

Gateway 192.168.75.1

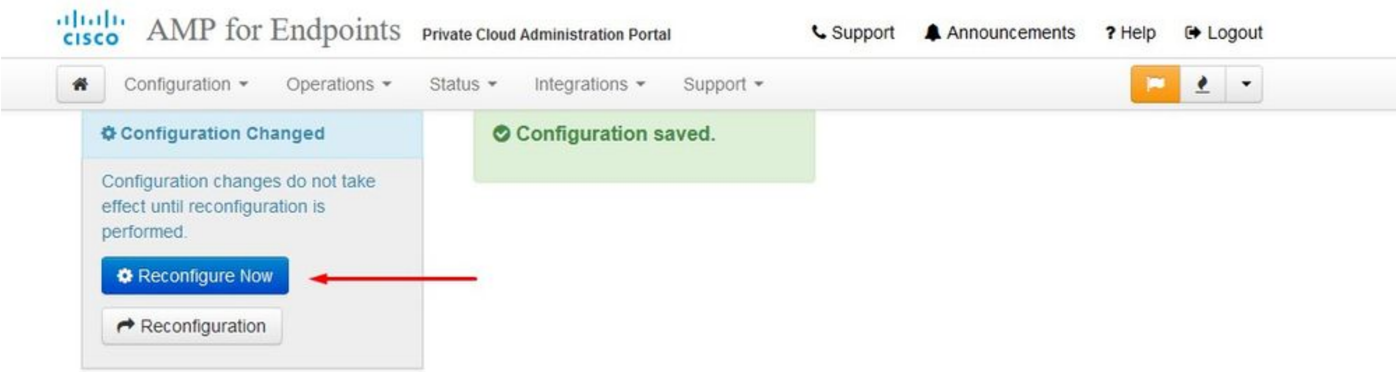
Warning: Address and Hostname Changes

If you change the IP address of the interface you must also update the DNS records for each of your configured hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.

View the Configuration help page for a list of affected services.

DNS

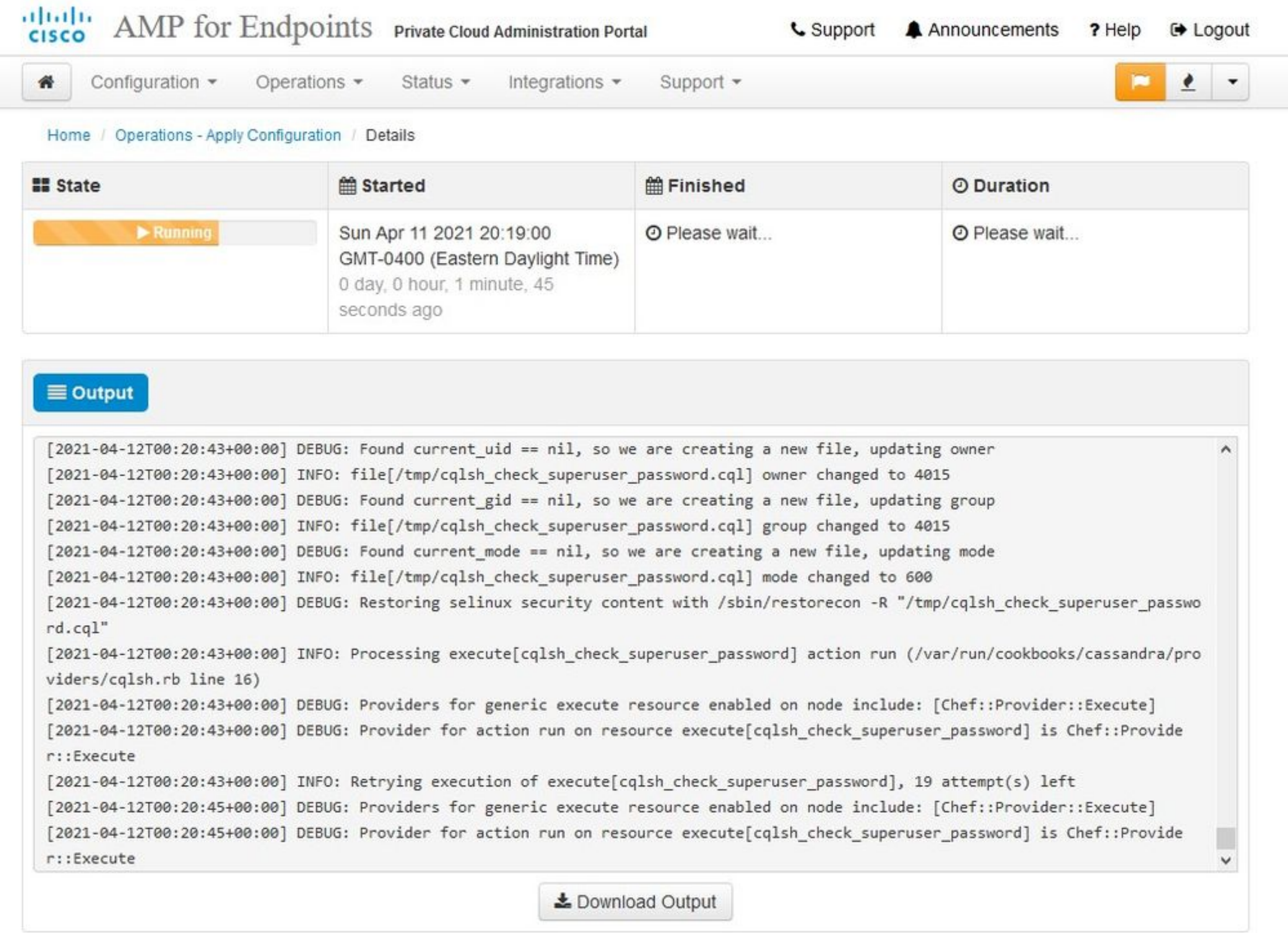
Primary DNS Server 192.168.75.4



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

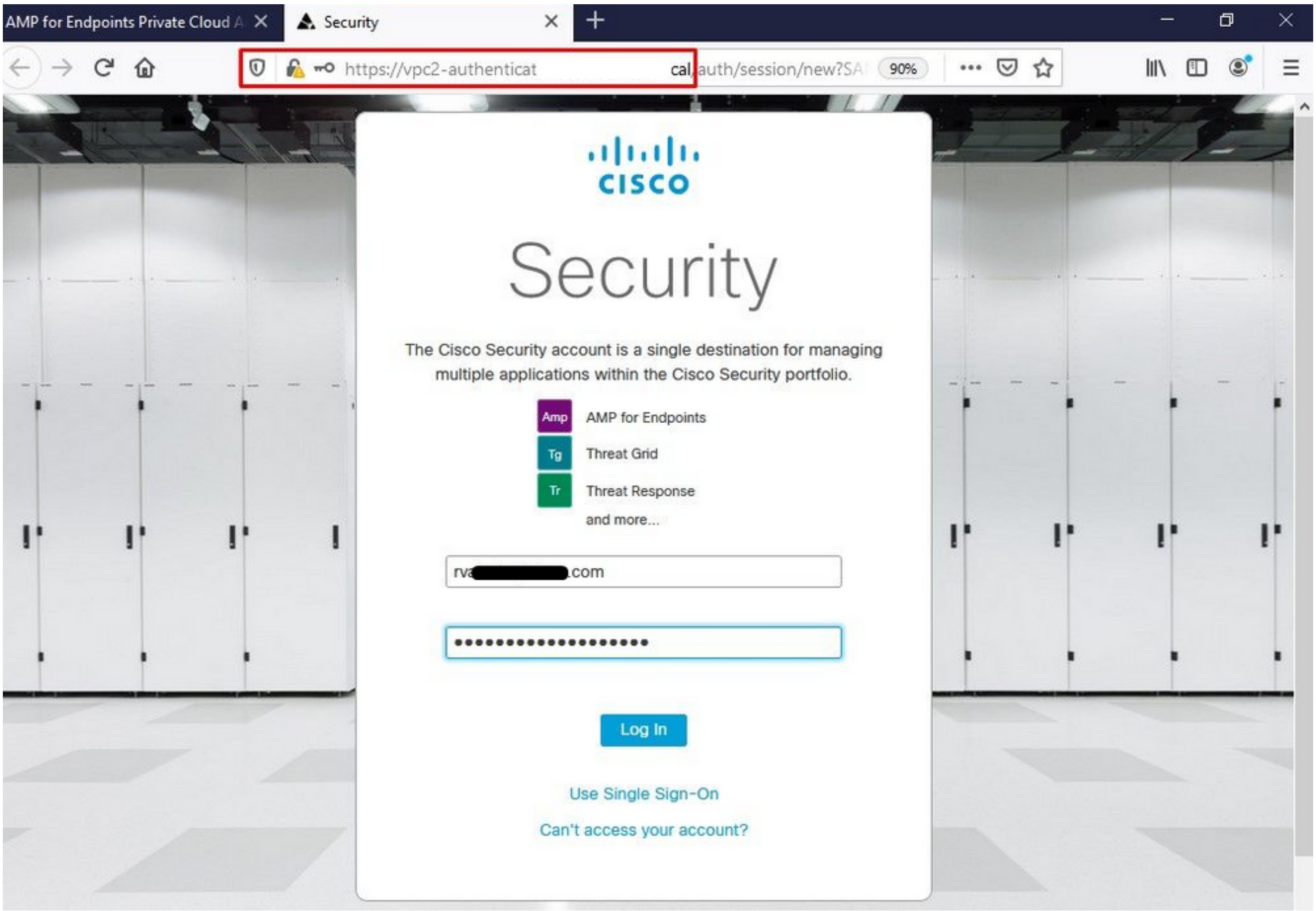
Configuration saved.



State	Started	Finished	Duration
▶ Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

```
[2021-04-12T00:20:43+00:00] DEBUG: Found current_uid == nil, so we are creating a new file, updating owner
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] owner changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_gid == nil, so we are creating a new file, updating group
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] group changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_mode == nil, so we are creating a new file, updating mode
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] mode changed to 600
[2021-04-12T00:20:43+00:00] DEBUG: Restoring selinux security content with /sbin/restorecon -R "/tmp/cqlsh_check_superuser_passwo
rd.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/run/cookbooks/cassandra/pro
viders/cqlsh.rb line 16)
[2021-04-12T00:20:43+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:43+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
[2021-04-12T00:20:43+00:00] INFO: Retrying execution of execute[cqlsh_check_superuser_password], 19 attempt(s) left
[2021-04-12T00:20:45+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:45+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
```

此時，您可以登入並下載聯結器



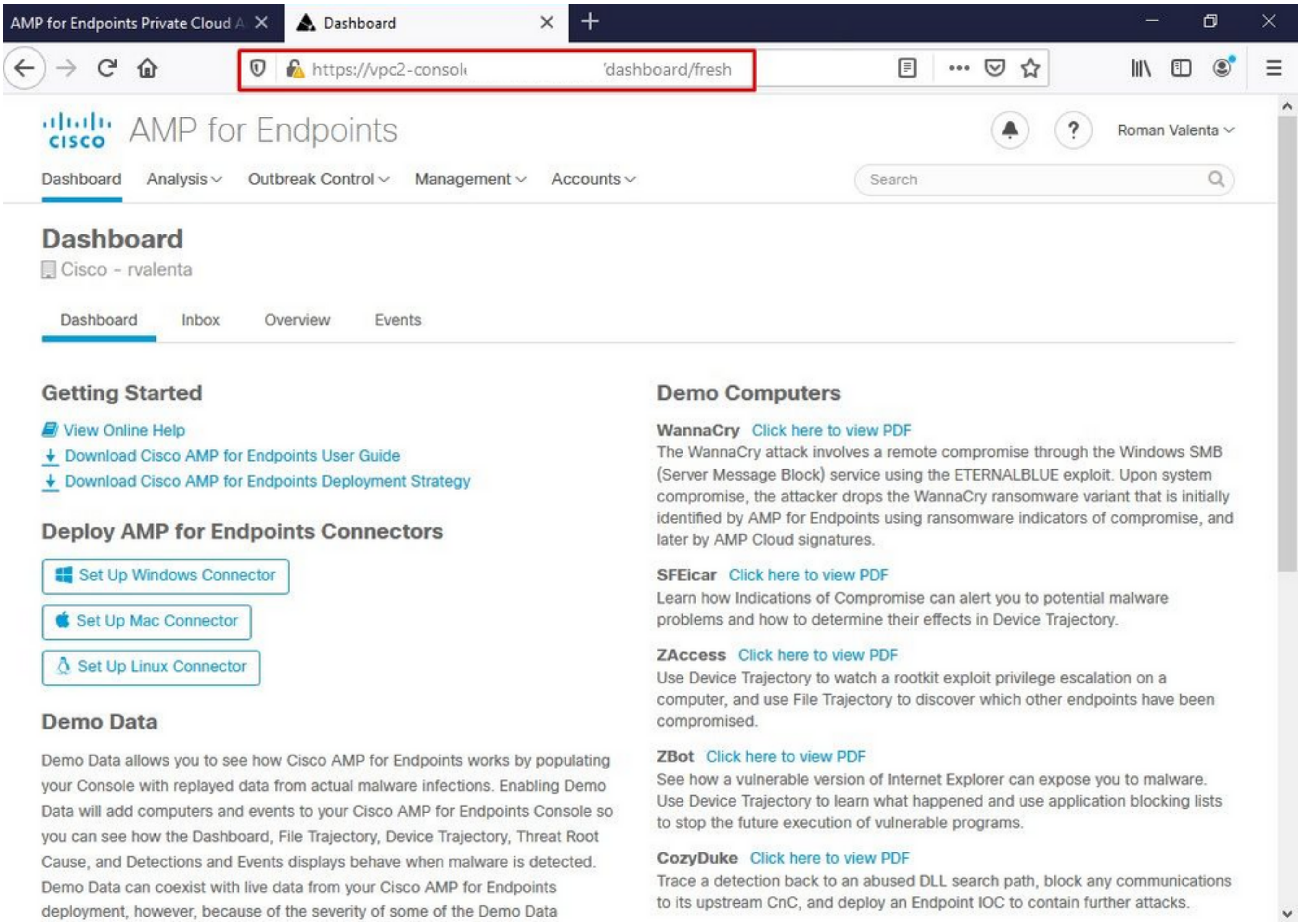
The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

rva[redacted].com

••••••••••••••••••••

您將獲得適用於您環境的初始安全終結點策略嚮導。它將引導您選擇您使用的防病毒產品（如果有）、代理以及要部署的策略型別。選擇適當的「設定......」按鈕取決於聯結器的作業系統。

您將看到「現有安全產品」頁面，如下圖所示。選擇您使用的安全產品。它會自動生成適用的排除項，以防止您的終端出現效能問題。選擇Next。



Dashboard

Cisco - rvalenta

Getting Started

View Online Help

Download Cisco AMP for Endpoints User Guide

Download Cisco AMP for Endpoints Deployment Strategy

Deploy AMP for Endpoints Connectors

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by populating your Console with replayed data from actual malware infections. Enabling Demo Data will add computers and events to your Cisco AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, and Detections and Events displays behave when malware is detected. Demo Data can coexist with live data from your Cisco AMP for Endpoints deployment, however, because of the severity of some of the Demo Data

Demo Computers

WannaCry Click here to view PDF
The WannaCry attack involves a remote compromise through the Windows SMB (Server Message Block) service using the ETERNALBLUE exploit. Upon system compromise, the attacker drops the WannaCry ransomware variant that is initially identified by AMP for Endpoints using ransomware indicators of compromise, and later by AMP Cloud signatures.

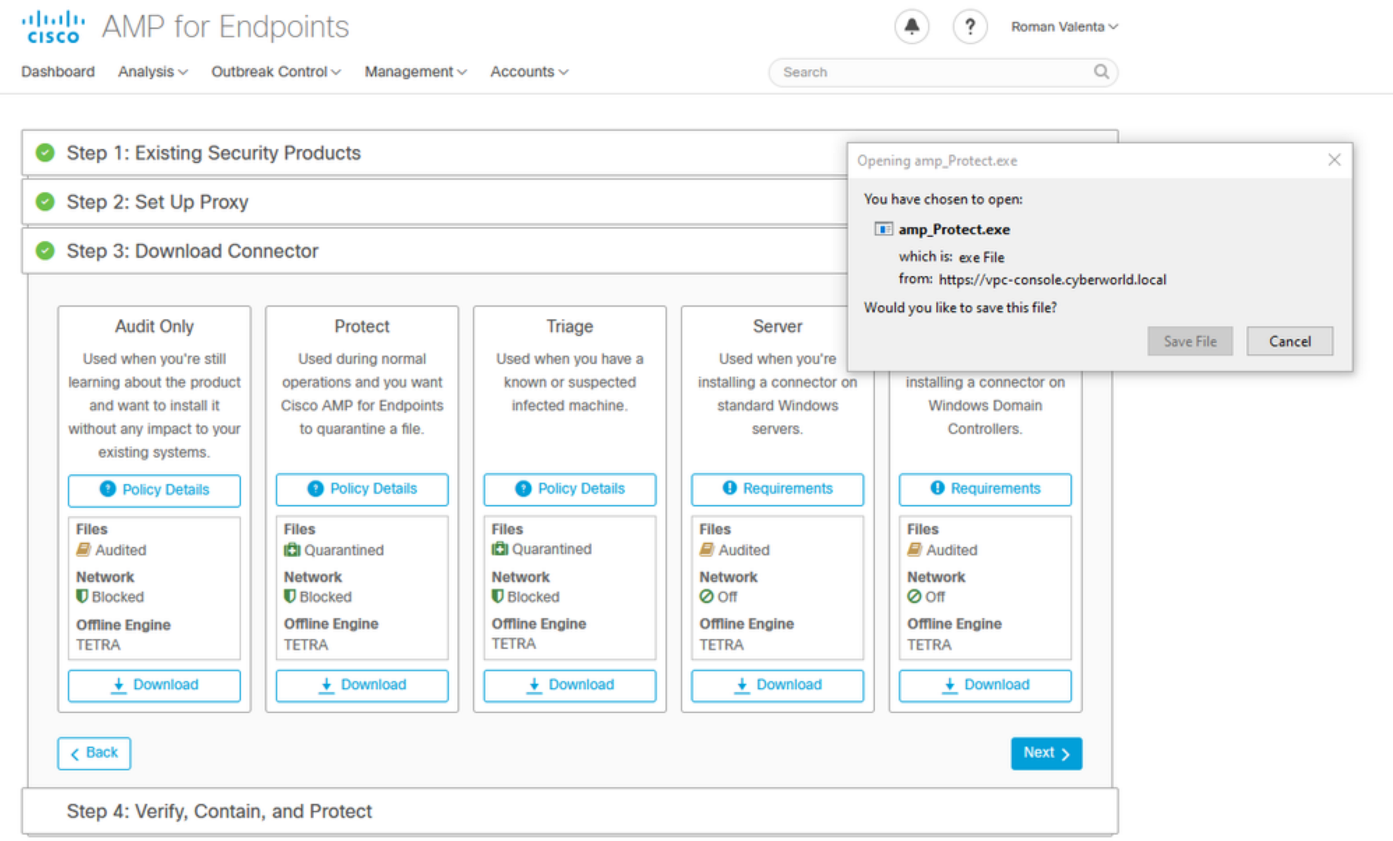
SFEicar Click here to view PDF
Learn how Indications of Compromise can alert you to potential malware problems and how to determine their effects in Device Trajectory.

ZAccess Click here to view PDF
Use Device Trajectory to watch a rootkit exploit privilege escalation on a computer, and use File Trajectory to discover which other endpoints have been compromised.

ZBot Click here to view PDF
See how a vulnerable version of Internet Explorer can expose you to malware. Use Device Trajectory to learn what happened and use application blocking lists to stop the future execution of vulnerable programs.

CozyDuke Click here to view PDF
Trace a detection back to an abused DLL search path, block any communications to its upstream CnC, and deploy an Endpoint IOC to contain further attacks.

下載聯結器。



Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

Audit Only	Protect	Triage	Server	
Used when you're still learning about the product and want to install it without any impact to your existing systems.	Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.	Used when you have a known or suspected infected machine.	Used when you're installing a connector on standard Windows servers.	installing a connector on Windows Domain Controllers.
Policy Details	Policy Details	Policy Details	Requirements	Requirements
Files Audited **Network** Blocked **Offline Engine** TETRA	**Files** Quarantined **Network** Blocked **Offline Engine** TETRA	**Files** Quarantined **Network** Blocked **Offline Engine** TETRA	**Files** Audited **Network** ⊘ Off **Offline Engine** TETRA	**Files** Audited **Network** ⊘ Off **Offline Engine** TETRA
Download	Download	Download	Download	Download

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

amp_Protect.exe

which is: exe File

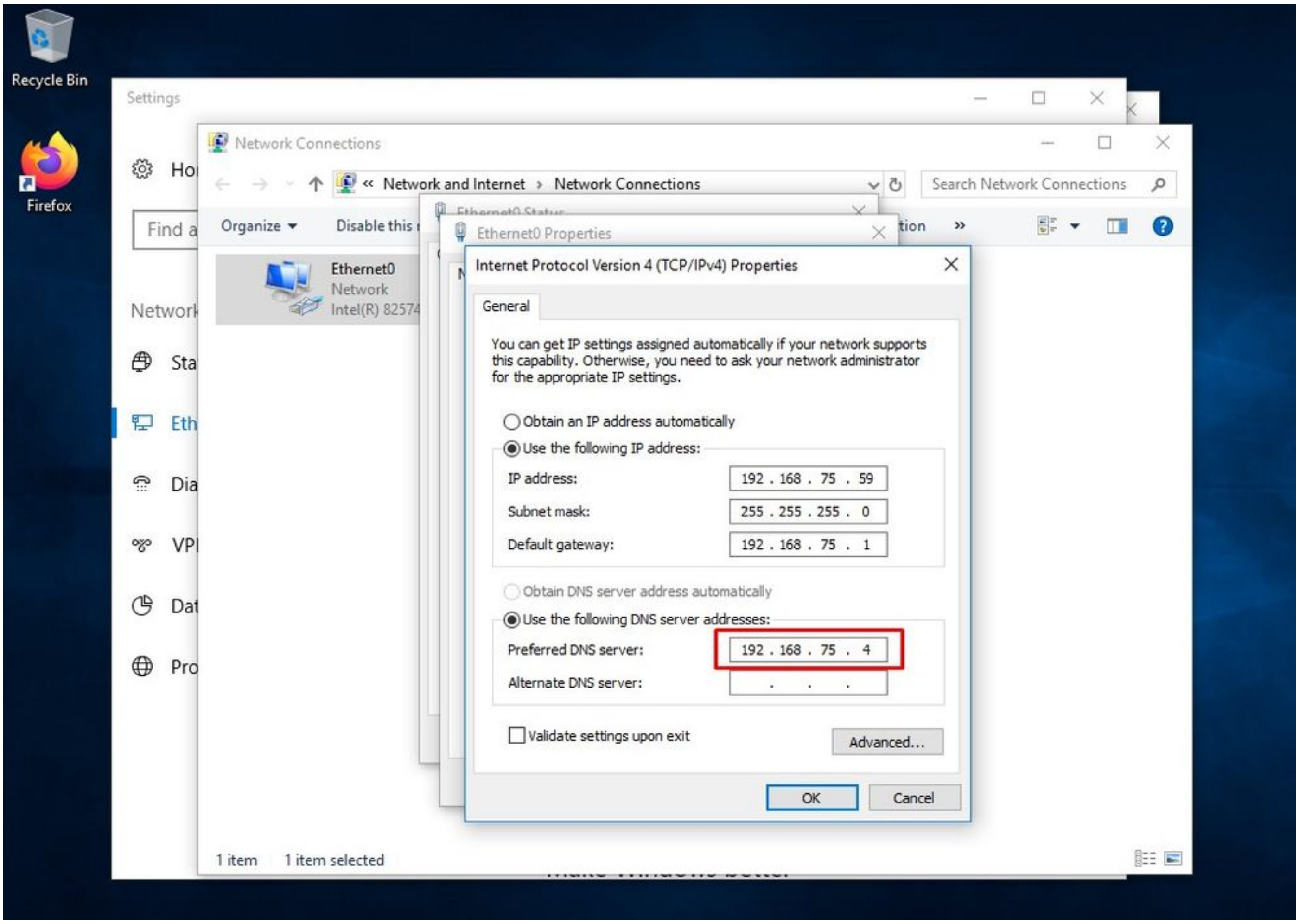
from: https://vpc-console.cyberworld.local

Would you like to save this file?

Save File　Cancel

問題#2 — 根CA問題

如果您使用自己的內部證書，則可能面臨的下一個問題是，在初始安裝後，聯結器可能會顯示為「已斷開連線」。



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 75 . 59

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 75 . 1

○ Obtain DNS server address automatically

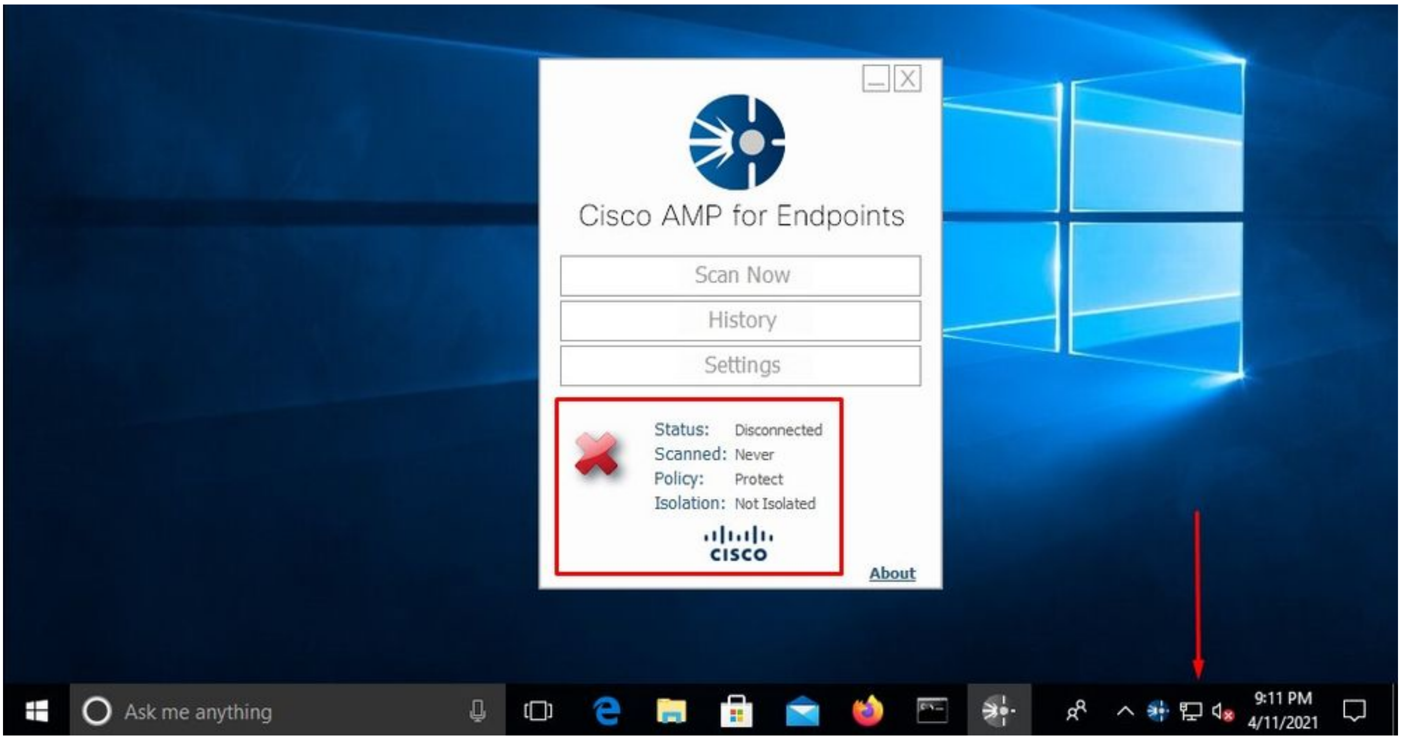
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 75 . 4

Alternate DNS server: . . .

□ Validate settings upon exit

安裝聯結器後，安全端點會被視為已斷開連線。運行診斷捆綁包並檢視日誌，您可以確定問題。



Cisco AMP for Endpoints

Status: Disconnected

Scanned: Never

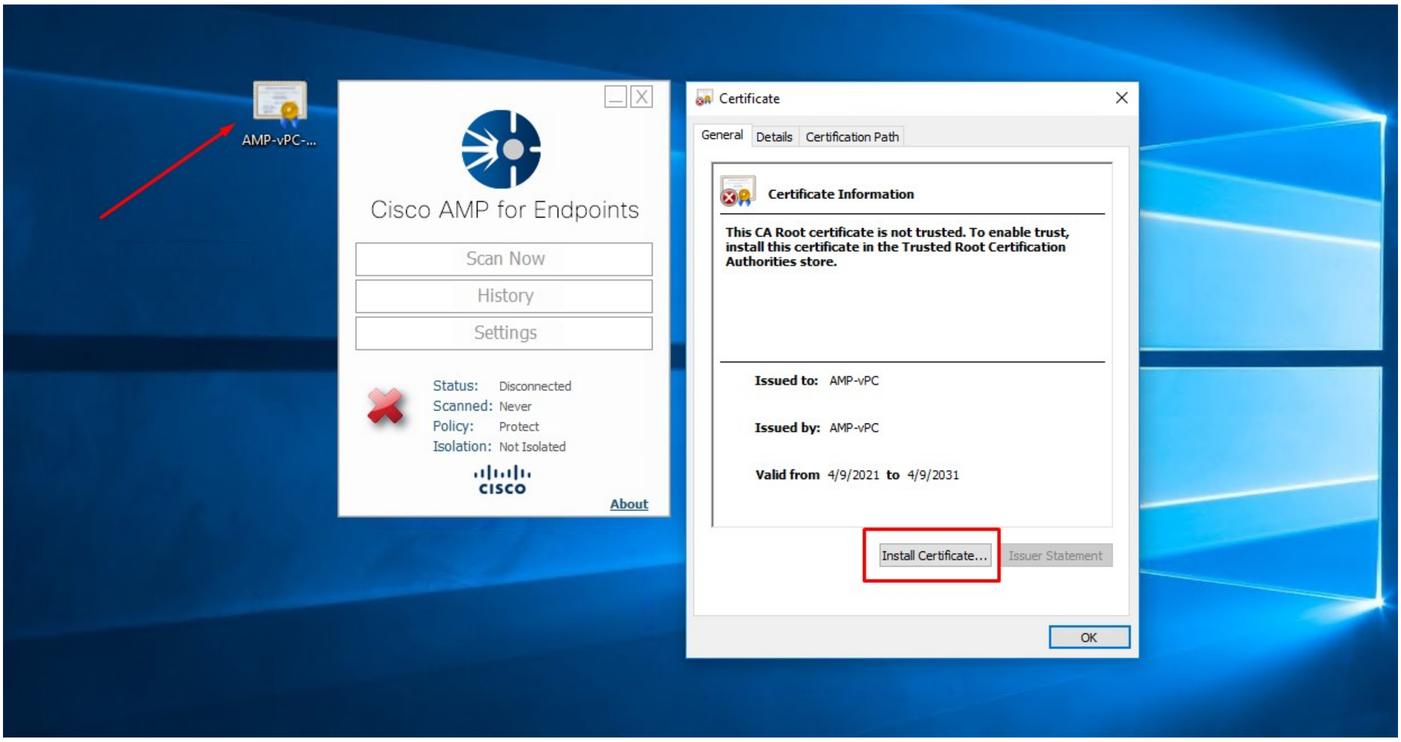
Policy: Protect

Isolation: Not Isolated

根據從診斷捆綁包中收集到的輸出，您可以看到根CA錯誤

```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

將根CA上傳到受信任的根CA儲存並重新啟動安全端點服務之後。一切如預期般開始運轉。



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

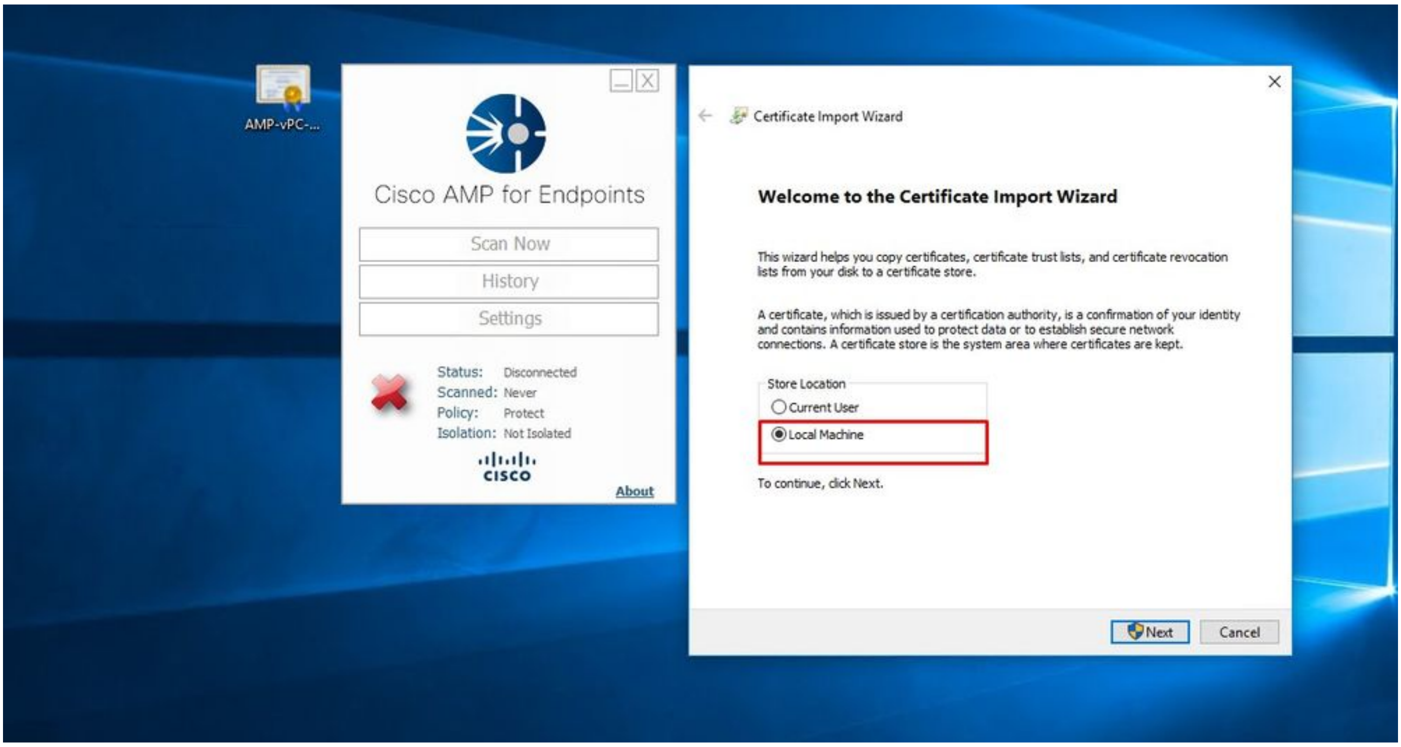
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: AMP-vPC

Issued by: AMP-vPC

Valid from 4/9/2021 to 4/9/2031



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

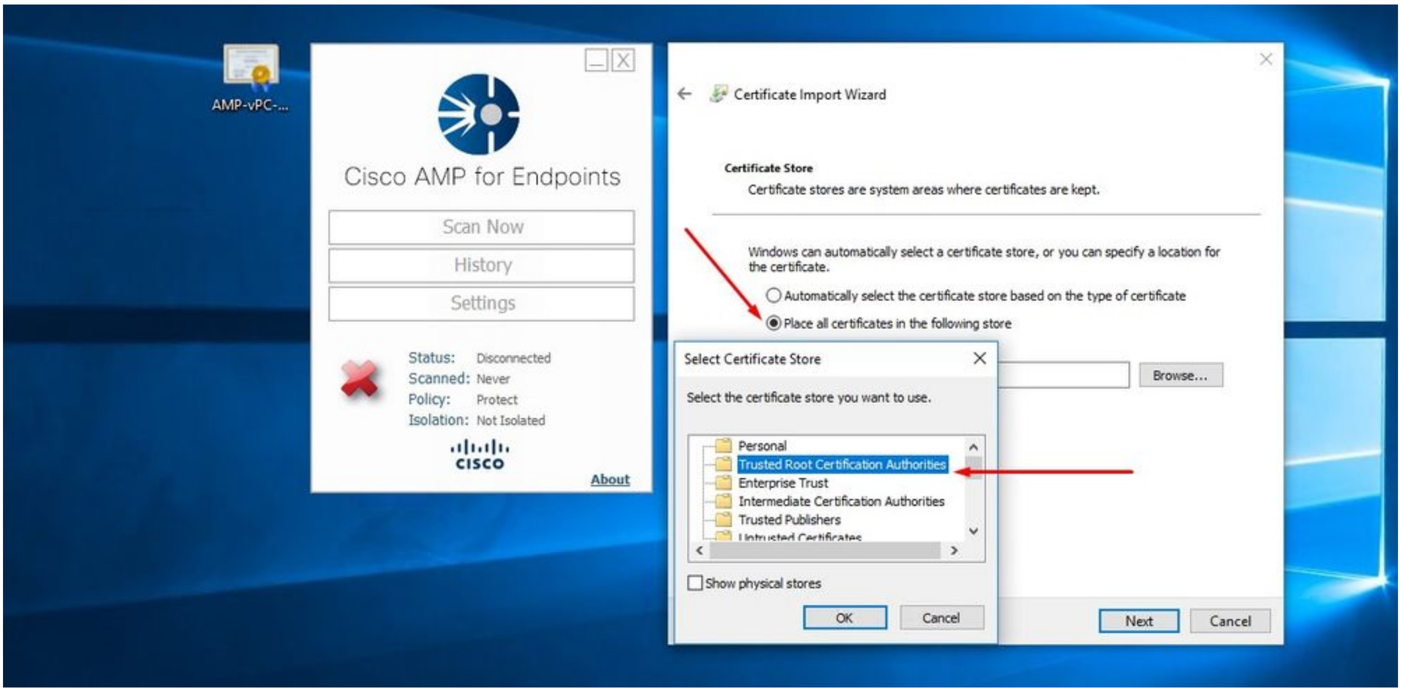
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

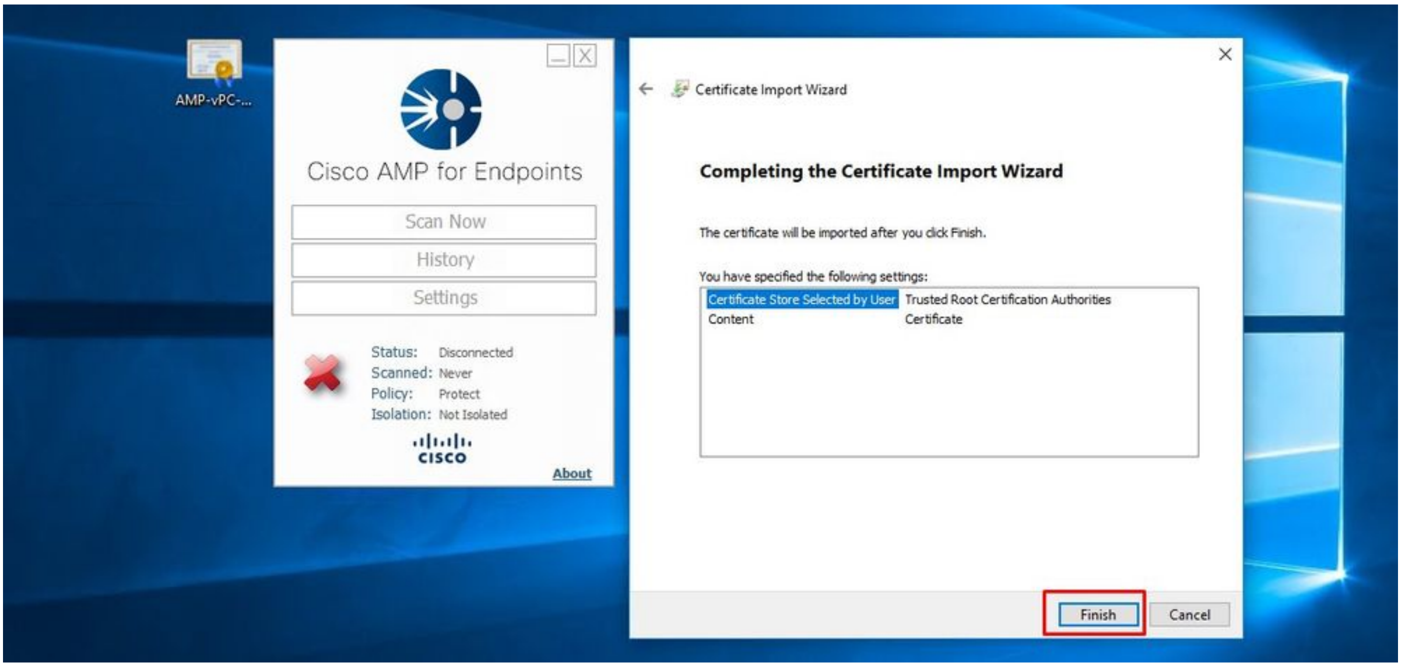
● Place all certificates in the following store

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

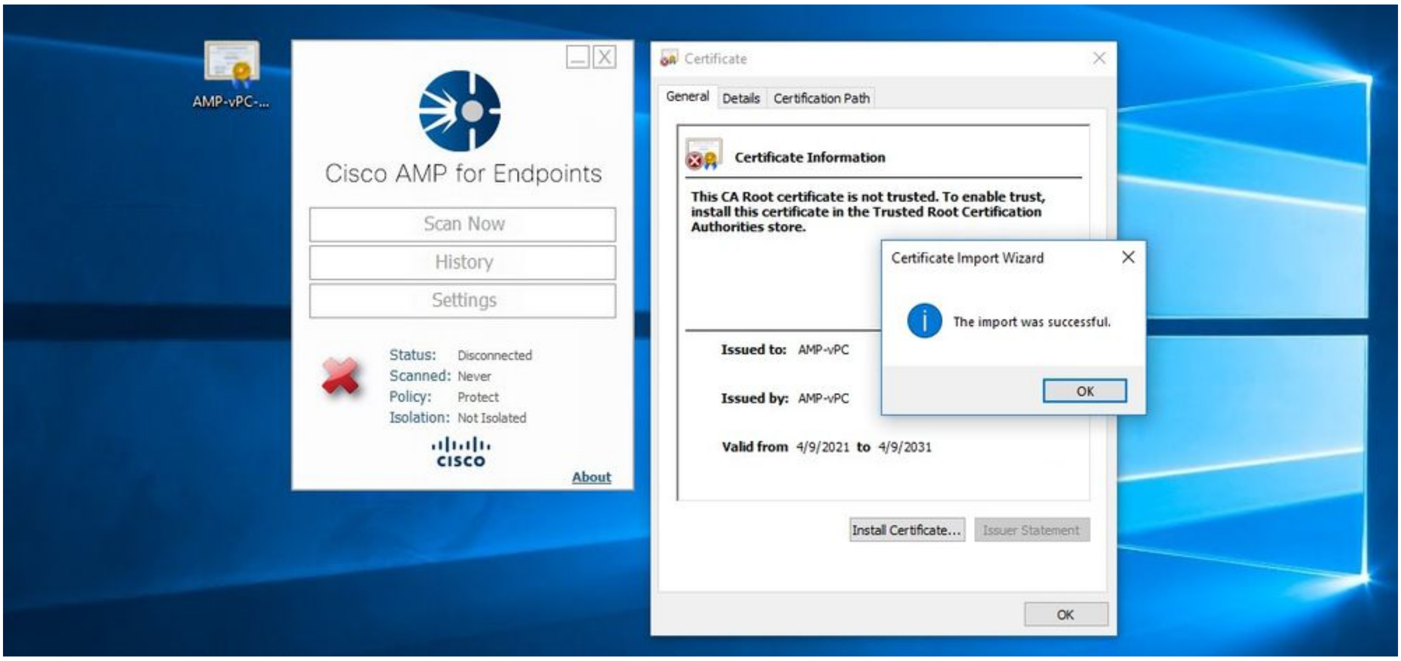
Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

Certificate Information

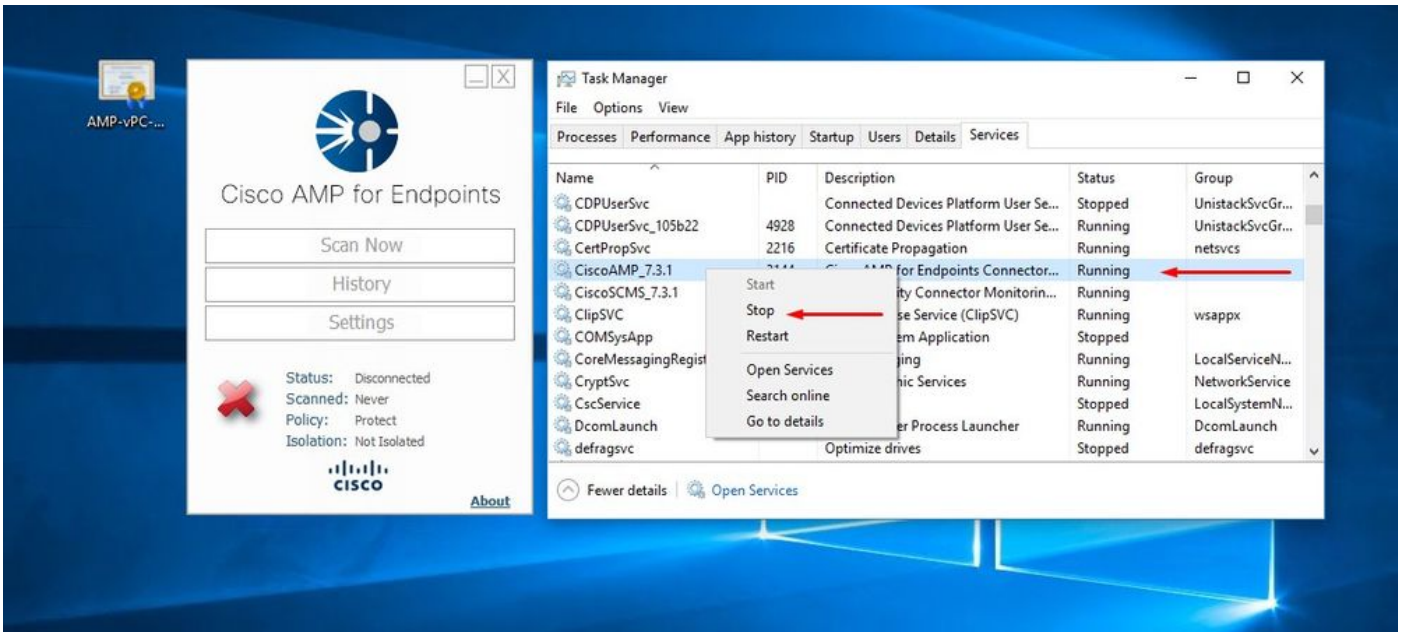
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: AMP-vPC

Issued by: AMP-vPC

Valid from 4/9/2021 to 4/9/2031

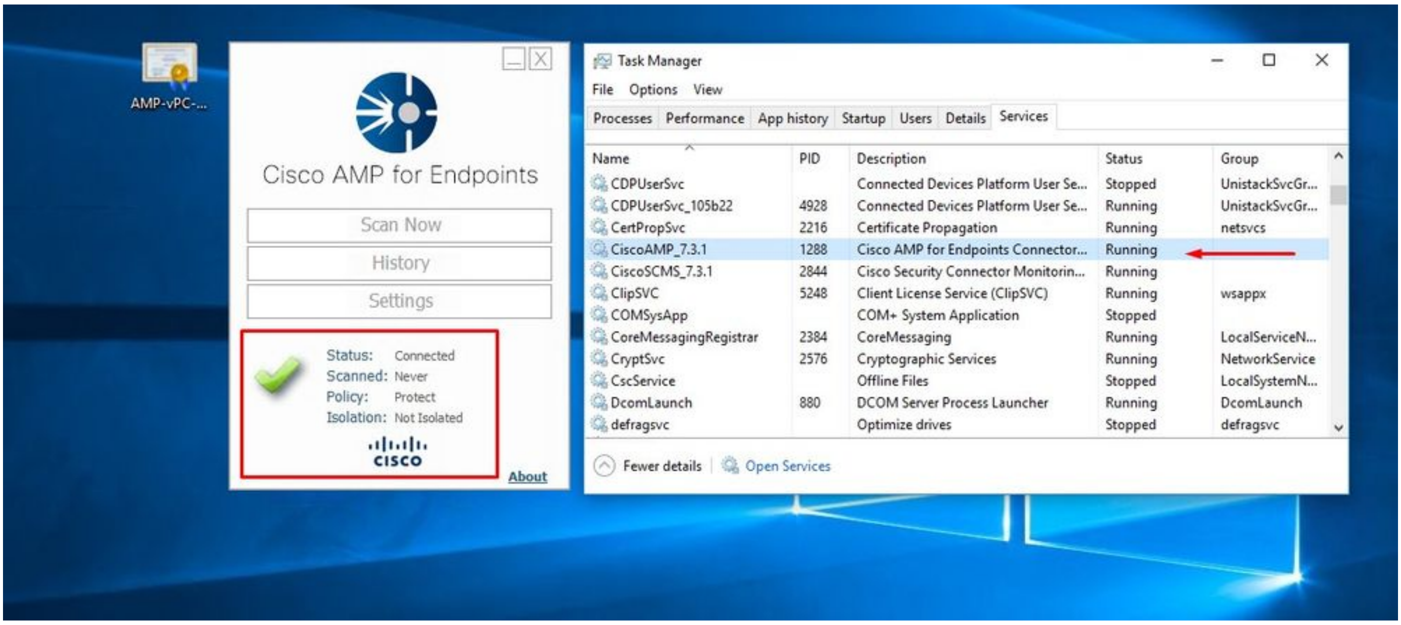
The import was successful.



Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

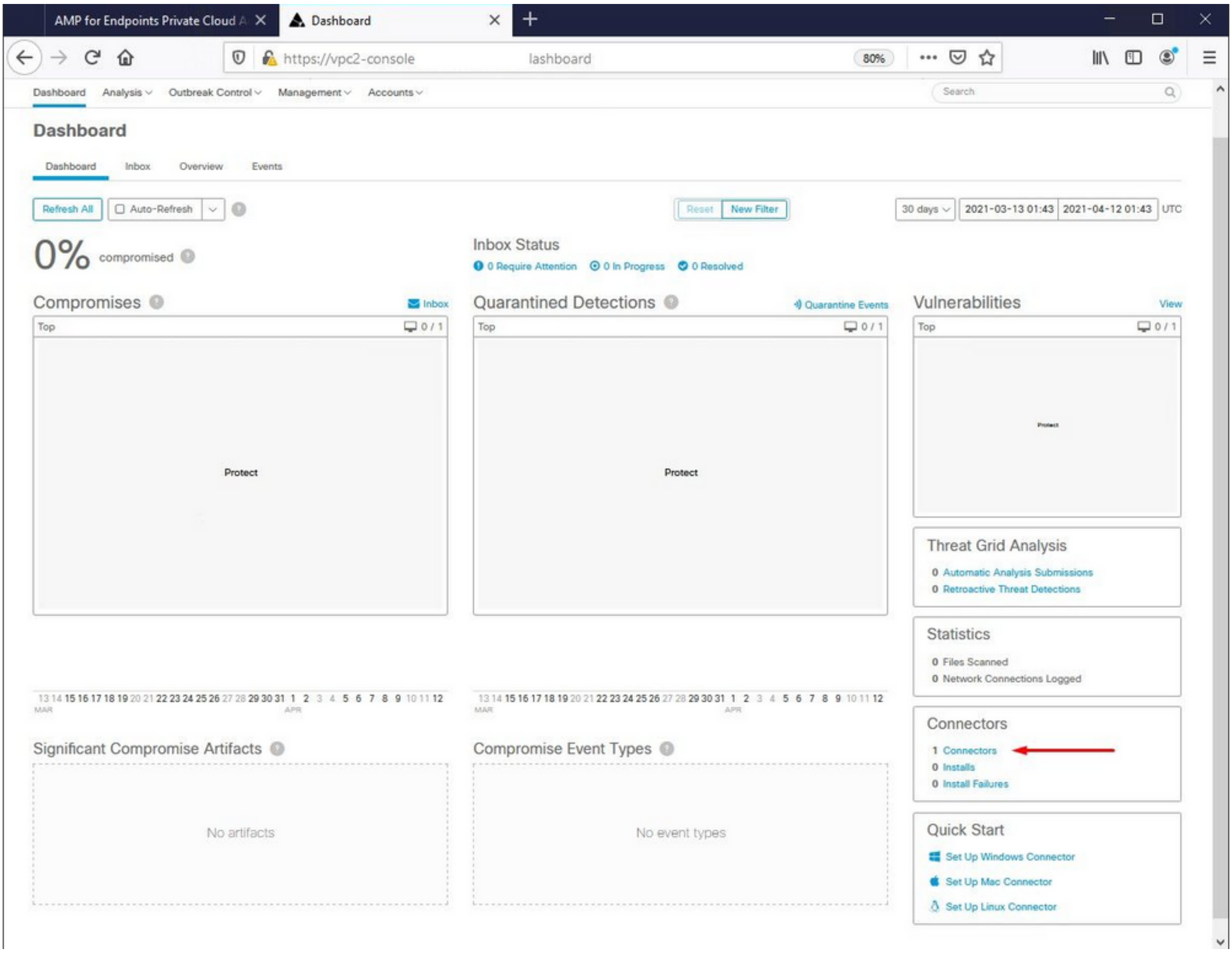
Name	PID	Description	Status	Group
CDPUserSvc		Connected Devices Platform User Se...	Stopped	UnistackSvcGr...
CDPUserSvc_105b22	4928	Connected Devices Platform User Se...	Running	UnistackSvcGr...
CertPropSvc	2216	Certificate Propagation	Running	netsvcs
CiscoAMP_7.3.1	[illegible]	[illegible] for Endpoints Connector...	Running	
CiscoSCMS_7.3.1		ity Connector Monitorin...	Running	
ClipSVC		se Service (ClipSVC)	Running	wsappx
COMSysApp		em Application	Stopped	
CoreMessagingRegist		ing	Running	LocalServiceN...
CryptSvc		ic Services	Running	NetworkService
CscService			Stopped	LocalSystemN...
DcomLaunch		er Process Launcher	Running	DcomLaunch
defragsvc		Optimize drives	Stopped	defragsvc

退回後，安全終端服務聯結器將如預期一樣聯機。



Status: Connected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

Name	PID	Description	Status	Group
CDPUserSvc		Connected Devices Platform User Se...	Stopped	UnistackSvcGr...
CDPUserSvc_105b22	4928	Connected Devices Platform User Se...	Running	UnistackSvcGr...
CertPropSvc	2216	Certificate Propagation	Running	netsvcs
CiscoAMP_7.3.1	1288	Cisco AMP for Endpoints Connector...	Running	
CiscoSCMS_7.3.1	2844	Cisco Security Connector Monitorin...	Running	
ClipSVC	5248	Client License Service (ClipSVC)	Running	wsappx
COMSysApp		COM+ System Application	Stopped	
CoreMessagingRegistrar	2384	CoreMessaging	Running	LocalServiceN...
CryptSvc	2576	Cryptographic Services	Running	NetworkService
CscService		Offline Files	Stopped	LocalSystemN...
DcomLaunch	880	DCOM Server Process Launcher	Running	DcomLaunch
defragsvc		Optimize drives	Stopped	defragsvc



0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Compromises

Quarantined Detections

Vulnerabilities

Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
0 Installs
0 Install Failures

Quick Start

Set Up Windows Connector
Set Up Mac Connector
Set Up Linux Connector

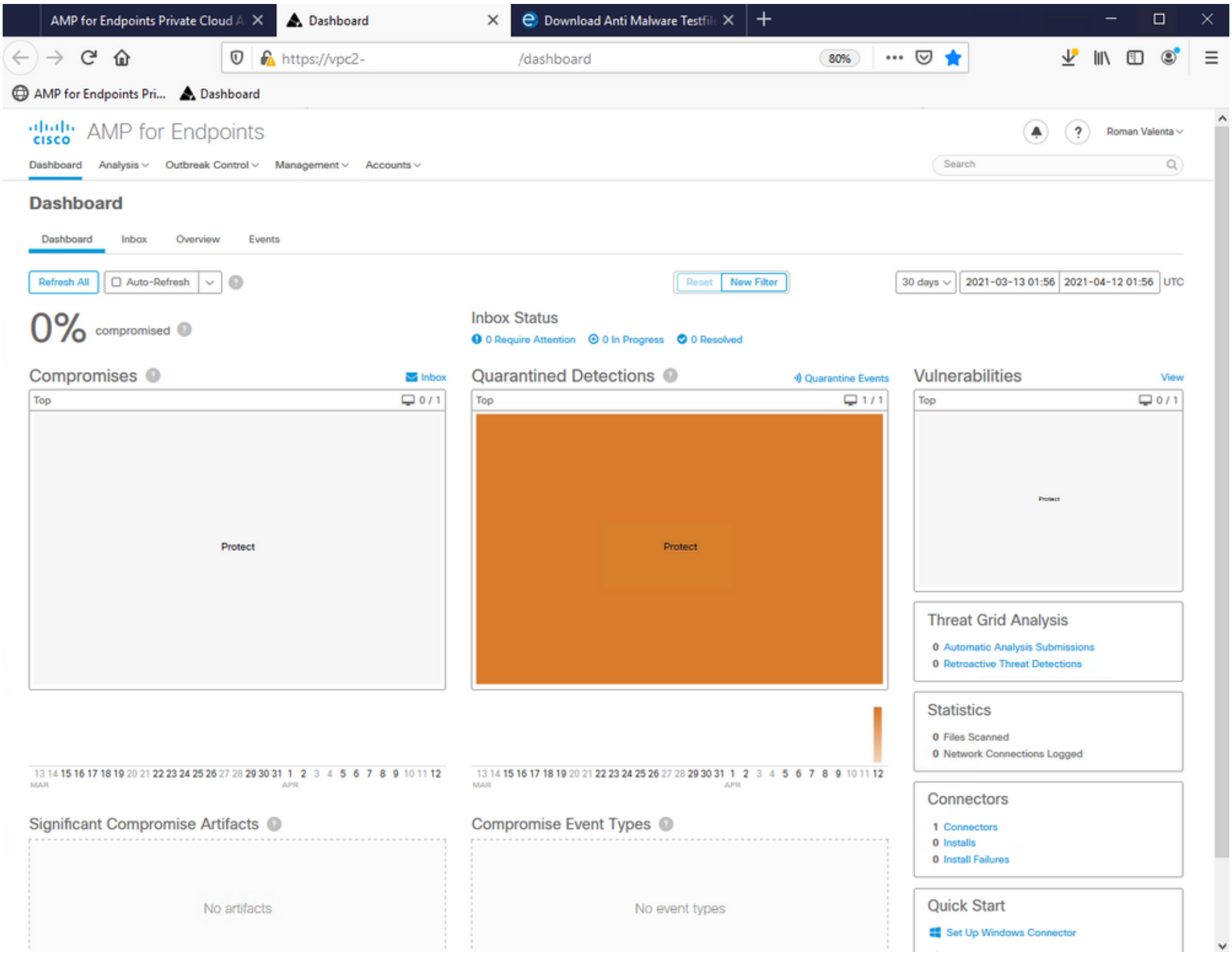
Significant Compromise Artifacts

No artifacts

Compromise Event Types

No event types

經測試的惡意活動



Dashboard

30 days 2021-03-13 01:56 2021-04-12 01:56 UTC

0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Compromises 0 / 1

Quarantined Detections 1 / 1

Vulnerabilities 0 / 1

Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
0 Installs
0 Install Failures

Quick Start

Set Up Windows Connector

Significant Compromise Artifacts

No artifacts

Compromise Event Types

No event types

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。