安装和配置安全终端虚拟私有云

目录

简介

先决条件

VPC部署

VM安装

初始管理接口设置

通过Web GUI对vPC进行初始配置

配置

服务

AirGap更新软件包

问题#1 - Data Store的房间耗尽

问题#2 — 旧更新

基本故障排除

问题#1 - FQDN和DNS服务器

问题#2 — 根CA的问题

简介

本文档介绍并重点介绍如何在ESXi环境中的服务器上成功部署虚拟私有云(VPC)。 有关快速入门指南、部署策略、授权指南、控制台和管理员用户指南等其他文档，请访问本网站文档

作者：Roman Valenta，Cisco TAC工程师。

先决条件

要求:

VMware ESX 5或更高版本

- 云代理模式（仅限）：128 GB RAM，8个CPU核心（建议使用2个CPU和4个核心），VMware Datastore的最小可用磁盘空间为1 TB
- 驱动器类型：空隙模式所需的SSD，建议用于代理
- RAID类型：一个RAID 10组（带区镜像）
- 最低VMware Datastore规模：2 TB
- RAID 10组(4K)的最小数据存储随机读取数：60K IOPS
- RAID 10组(4K)的最小数据存储随机写入数：30K IOPS

Cisco 建议您了解以下主题：

- 有关如何使用证书的基本知识。
- 有关如何在DNS服务器（Windows或Linux）下设置DNS的基本知识
- 在VMWare ESXi中安装开放式虚拟设备(OVA)模板

在本实验中用到：

VMware ESX 6.5

- 云代理模式（仅限）：48 GB RAM，8个CPU核心（建议使用2个CPU和4个核心），VMware Datastore上的最小可用磁盘空间为1 TB
- 驱动器类型：SATA
- RAID类型：一个RAID 1
- 最低VMware Datastore规模：1 TB
- MobaXterm 20.2（类似于PuTTY的多终端程序）
- Cygwin64（用于下载AirGap更新）

此外

- 使用openSSL或XCA创建的证书
- DNS服务器（Linux或Windows）我的实验室使用Windows Server 2016和CentOS-8
- 用于测试终端的Windows VM
- 许可证

如果内存低于48GB RAM，那么版本3.2+ VPC将无法使用。

注意：私有云OVA创建驱动器分区，因此无需在VMWare.服务器中指定这些分区，该服务器解析干净的接口主机名。

有关特定于版本的硬件要求的详细信息，请参阅VPC设备产品手册。

注：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

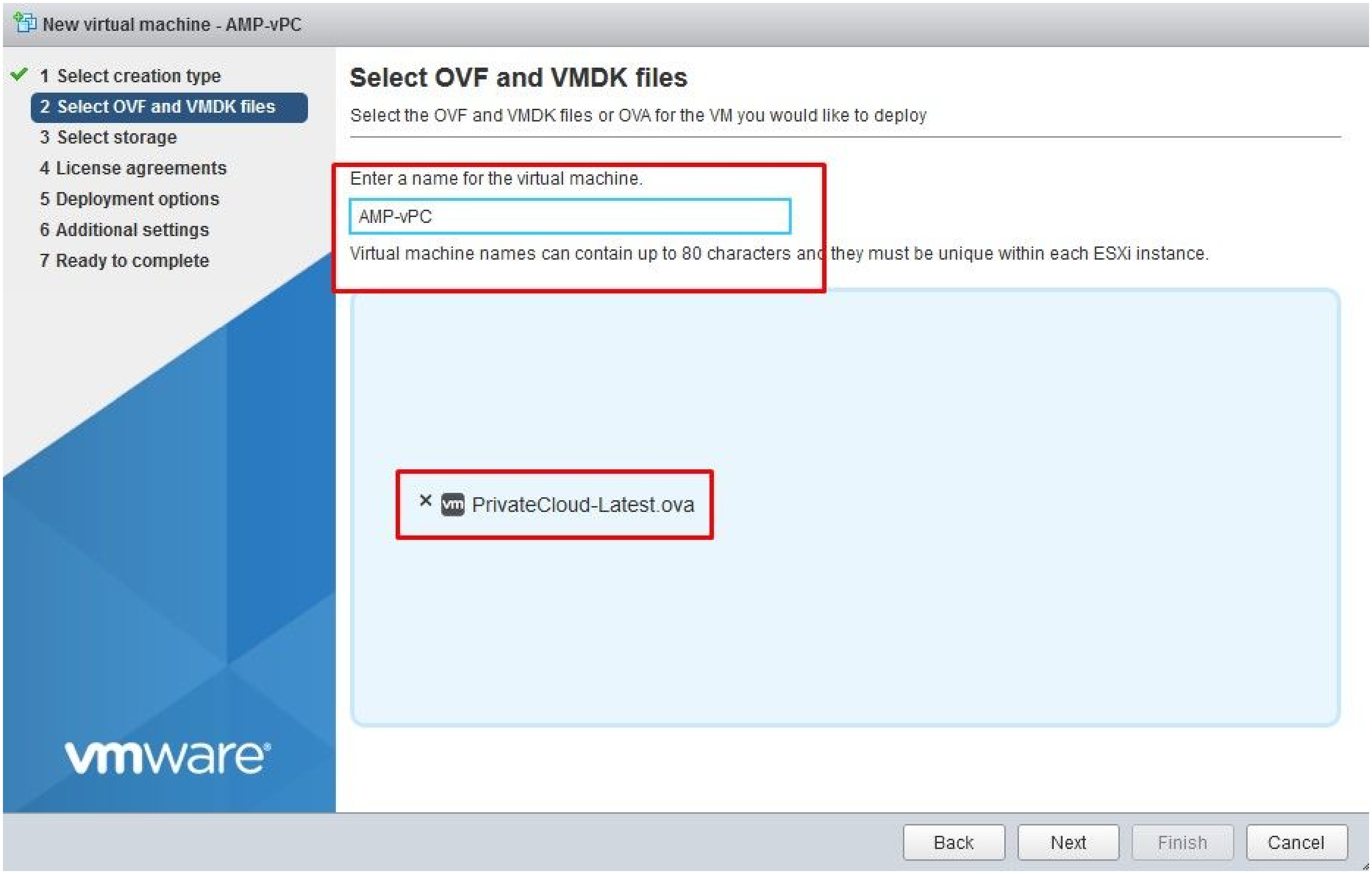
VPC部署

选择eDelivery或授权邮件中提供的URL。下载OVA文件并继续安装

VM安装

步骤1:

导航到文件>部署OVF模板以打开部署OVF模板向导，如图所示。



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 OVF and VMDK files

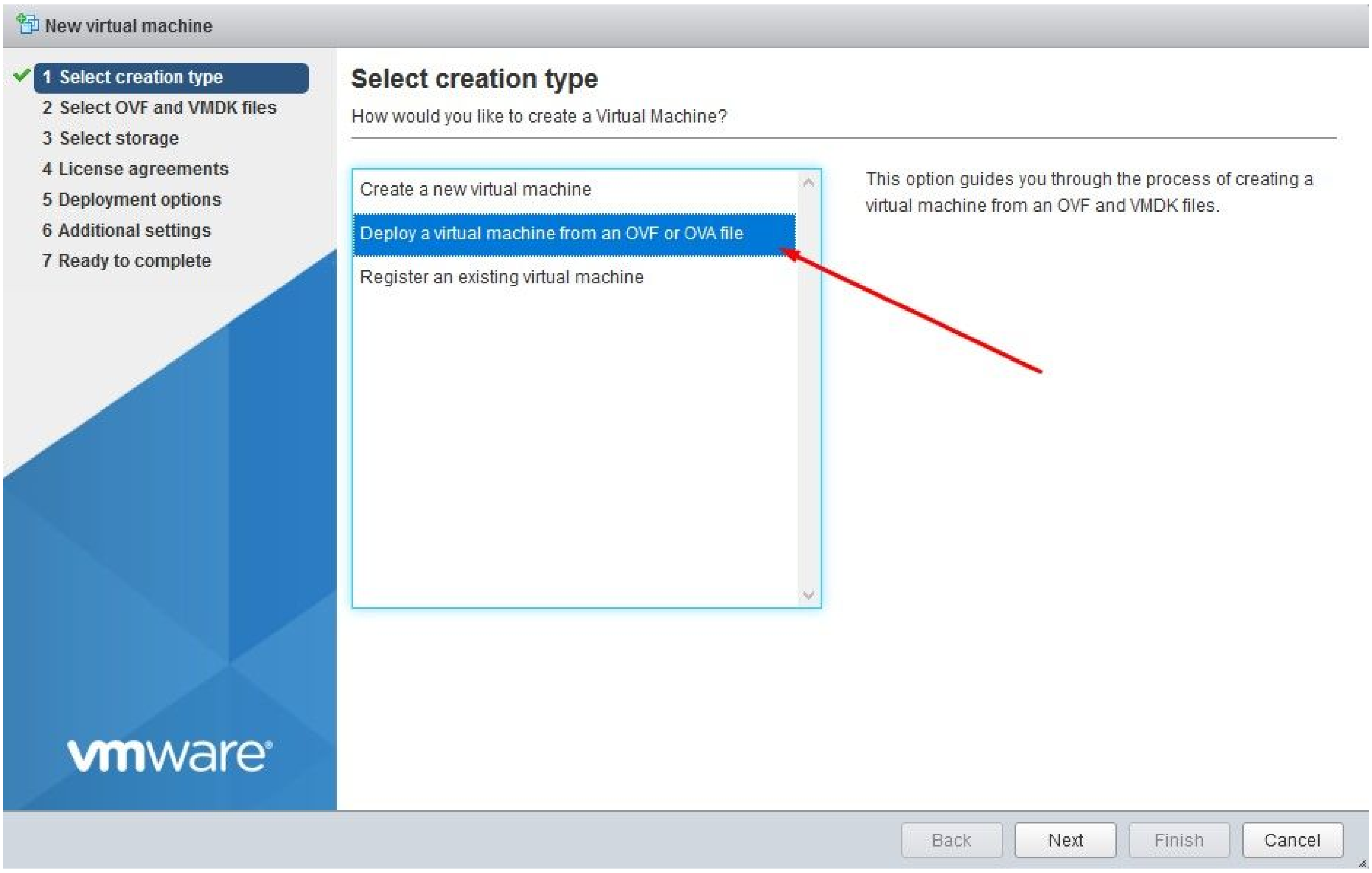
Select the OVF and VMDK files or OVA for the VM you would like to deploy

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

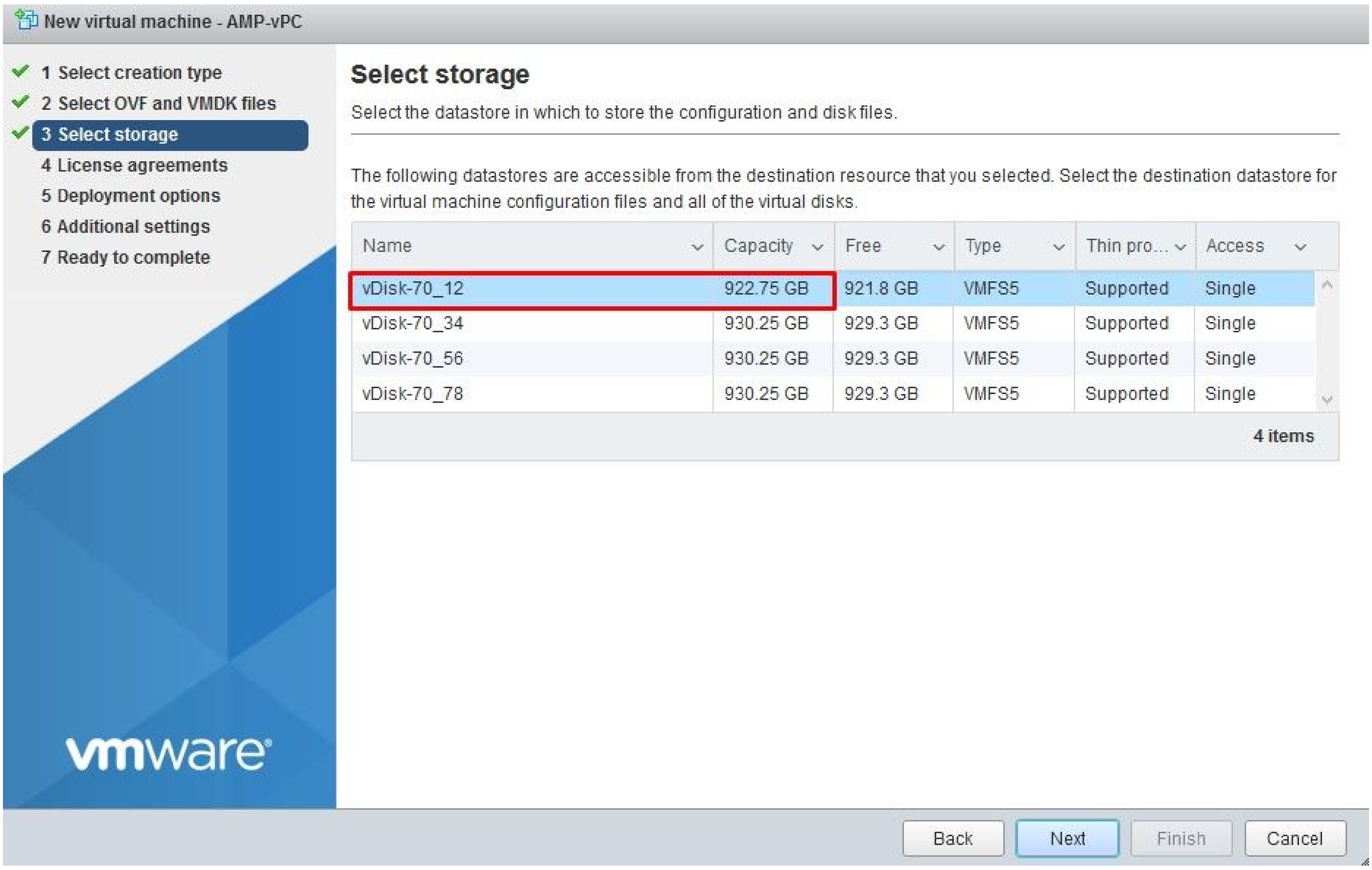
✓ 1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

Select 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

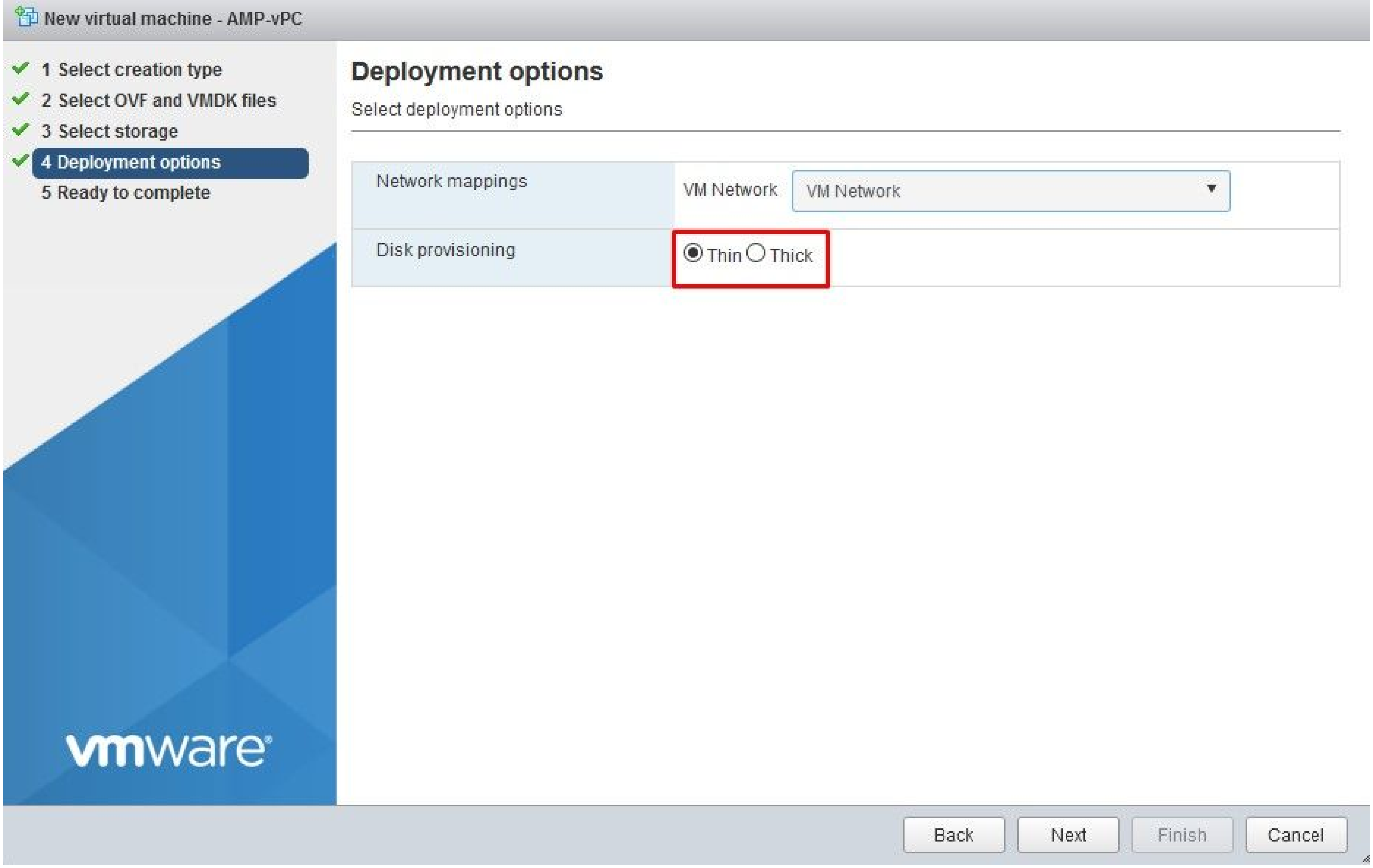
Select the datastore in which to store the configuration and disk files.

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:厚调配在创建磁盘时保留空间。如果选择此选项，则可以提高调配精简的性能。但是，这不是强制性的。现在选择Next，如图所示。



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

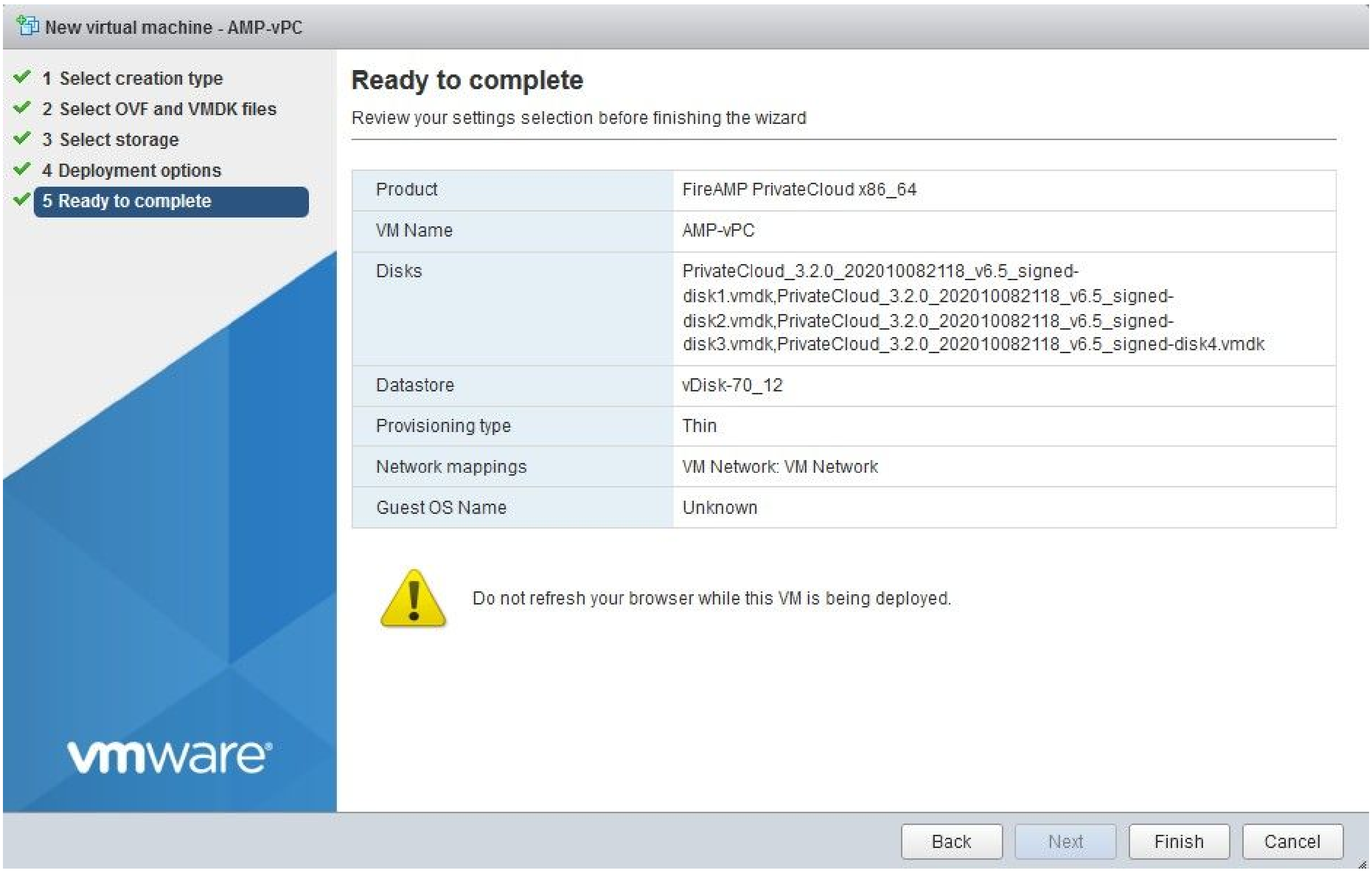
Deployment options

Select deployment options

Network mappings	VM Network: VM Network ▾
Disk provisioning	● Thin ○ Thick

步骤 2：

选择Browse...以选择OVA文件，然后在Next中选择。您注意到OVF模板详细信息页面上的默认OVA参数，如图所示。选择下一步。



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

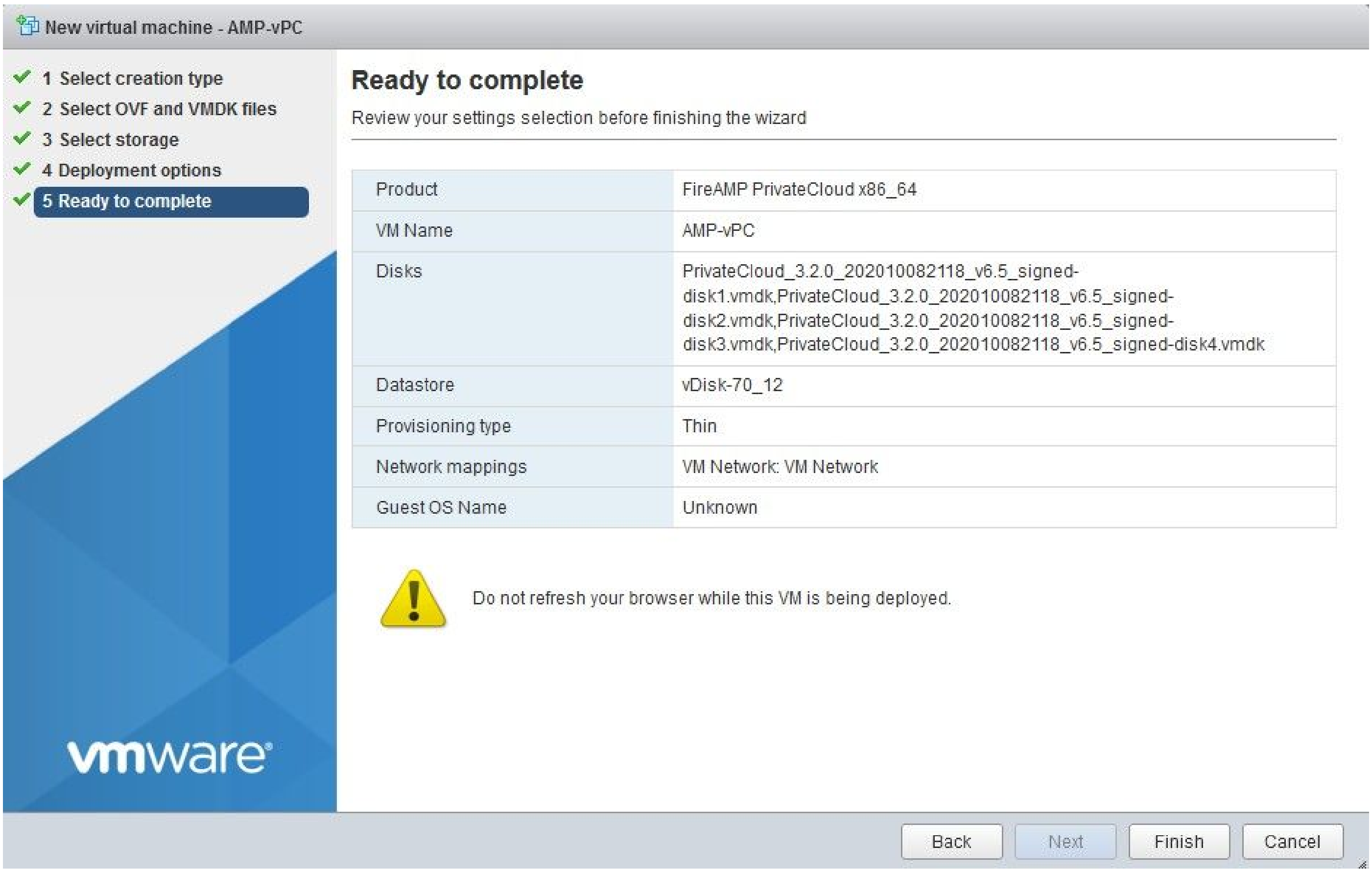
Ready to complete

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.

初始管理接口设置


New virtual machine - AMP-vPC

Ready to complete

Review your settings selection before finishing the wizard

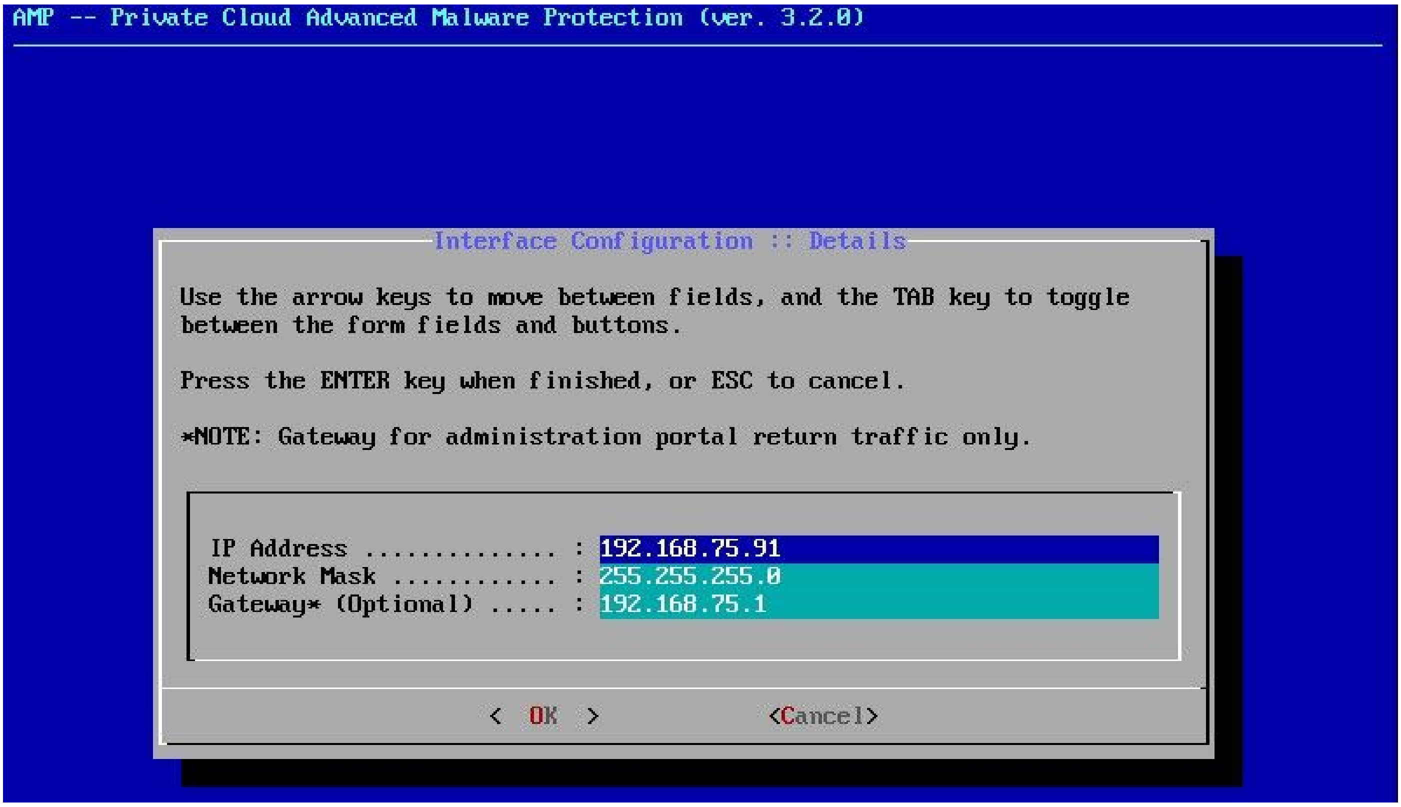
Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning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

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

在VM启动后，通过VM控制台执行初始配置。

步骤 1：

您可能注意到，如果接口未从DHCP服务器接收IP地址，则URL显示[UNCONFIGURED]。请注意，此接口是Management接口。这不是Production接口。

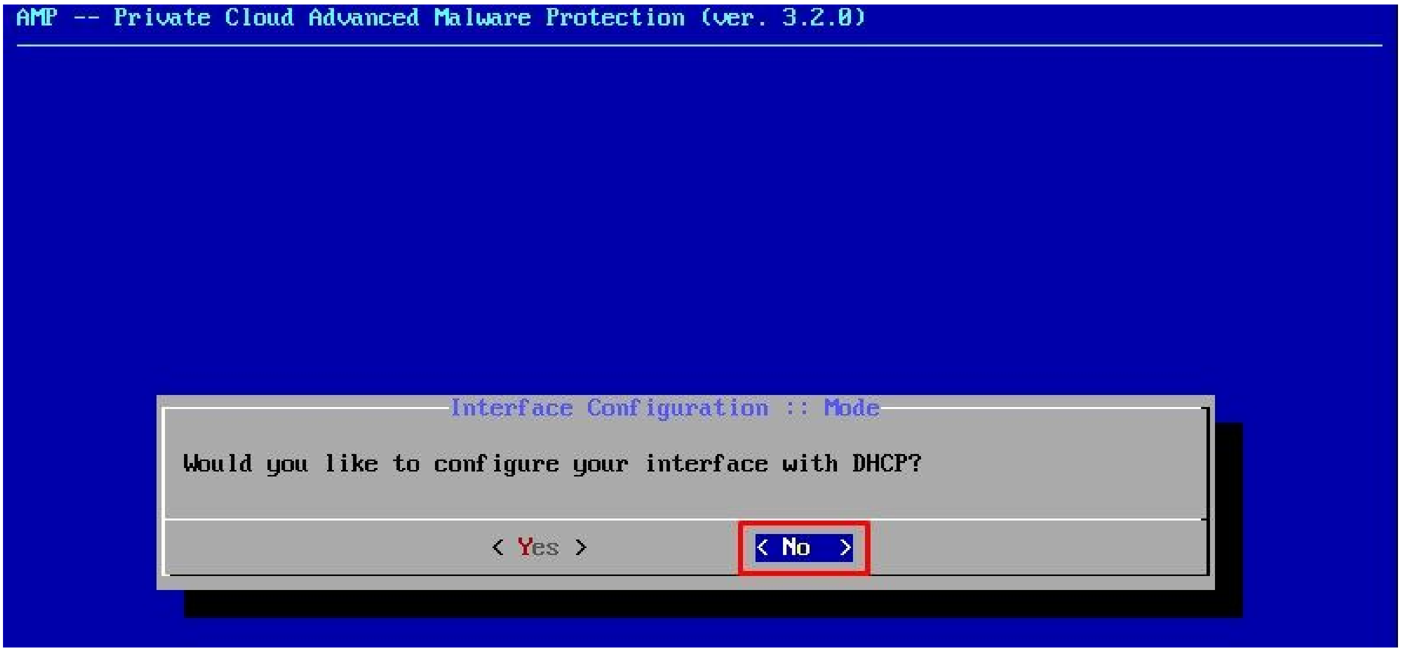


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

            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>
```

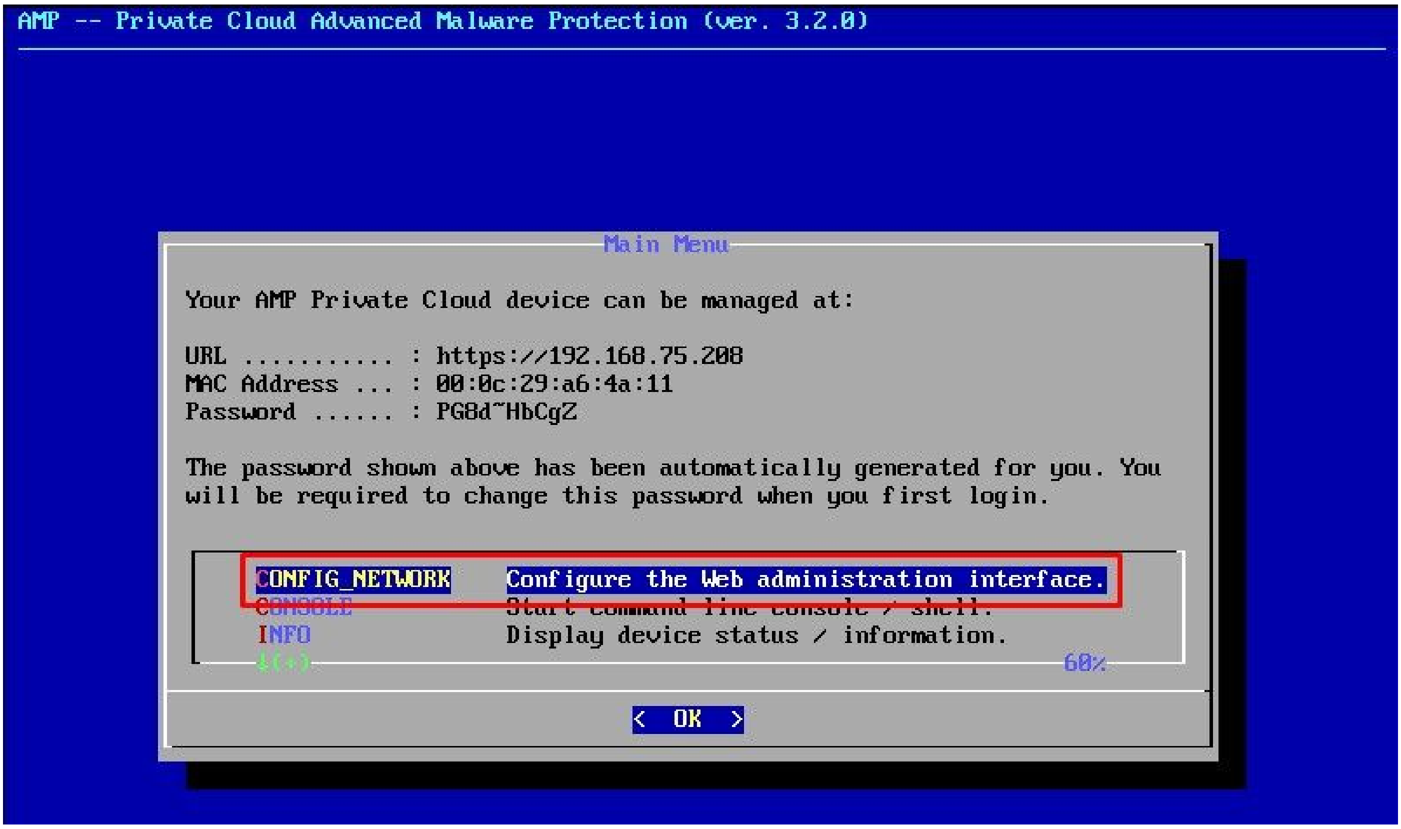
步骤 2：

可以通过Tab、Enter和箭头键进行导航。

导航到CONFIG_NETWORK，然后选择键盘上的Enter键，开始配置安全终端私有云的管理IP地址。如果不想使用DHCP，请选择No并选择Enter 键。

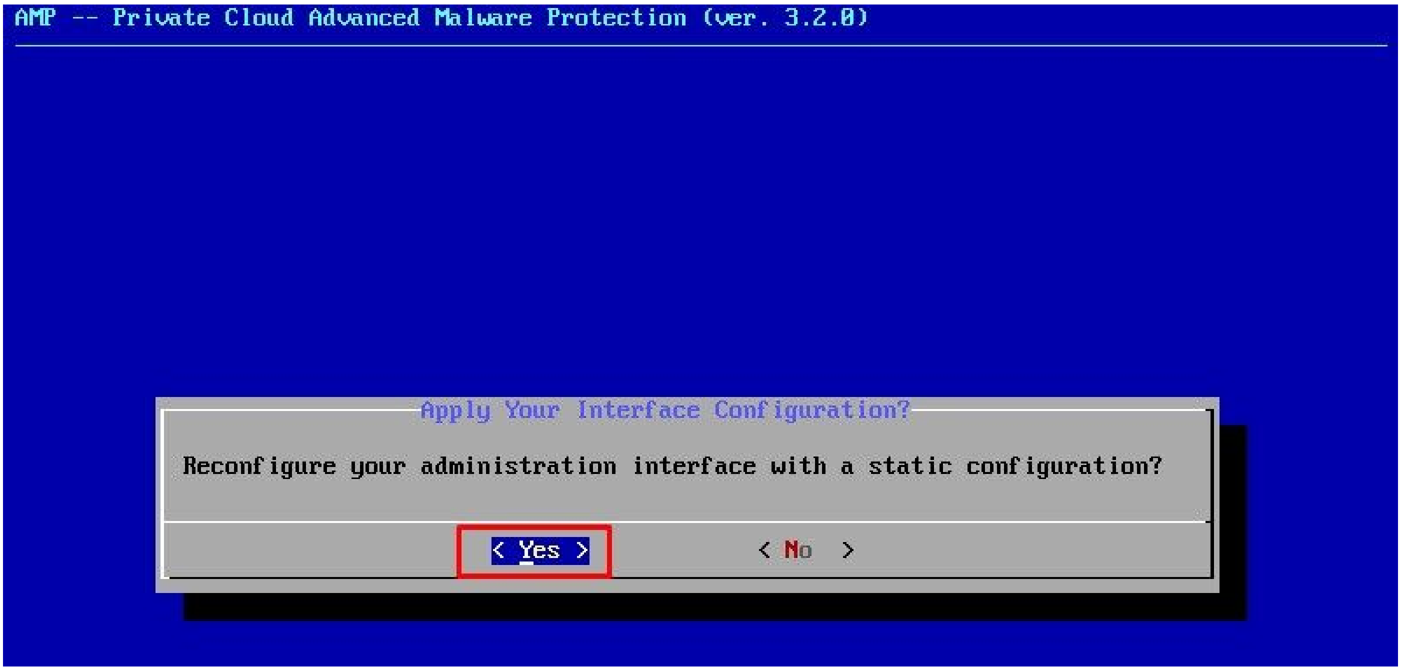


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

              Interface Configuration :: Mode

  Would you like to configure your interface with DHCP?

              < Yes >             < No  >
```



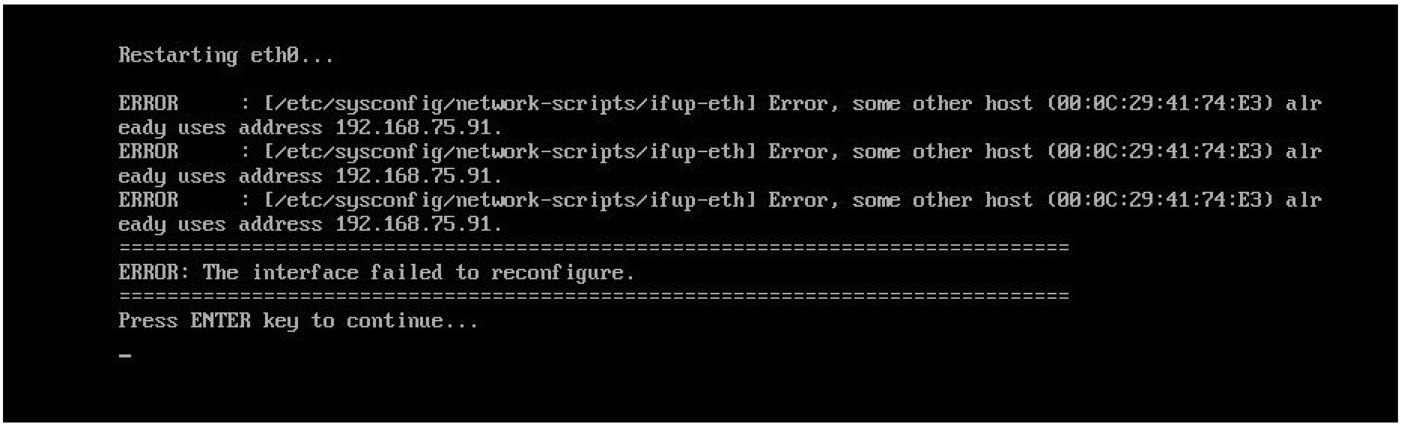
```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

                         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 >
```

在出现的窗口中，选择Yes，然后选择Enter键。

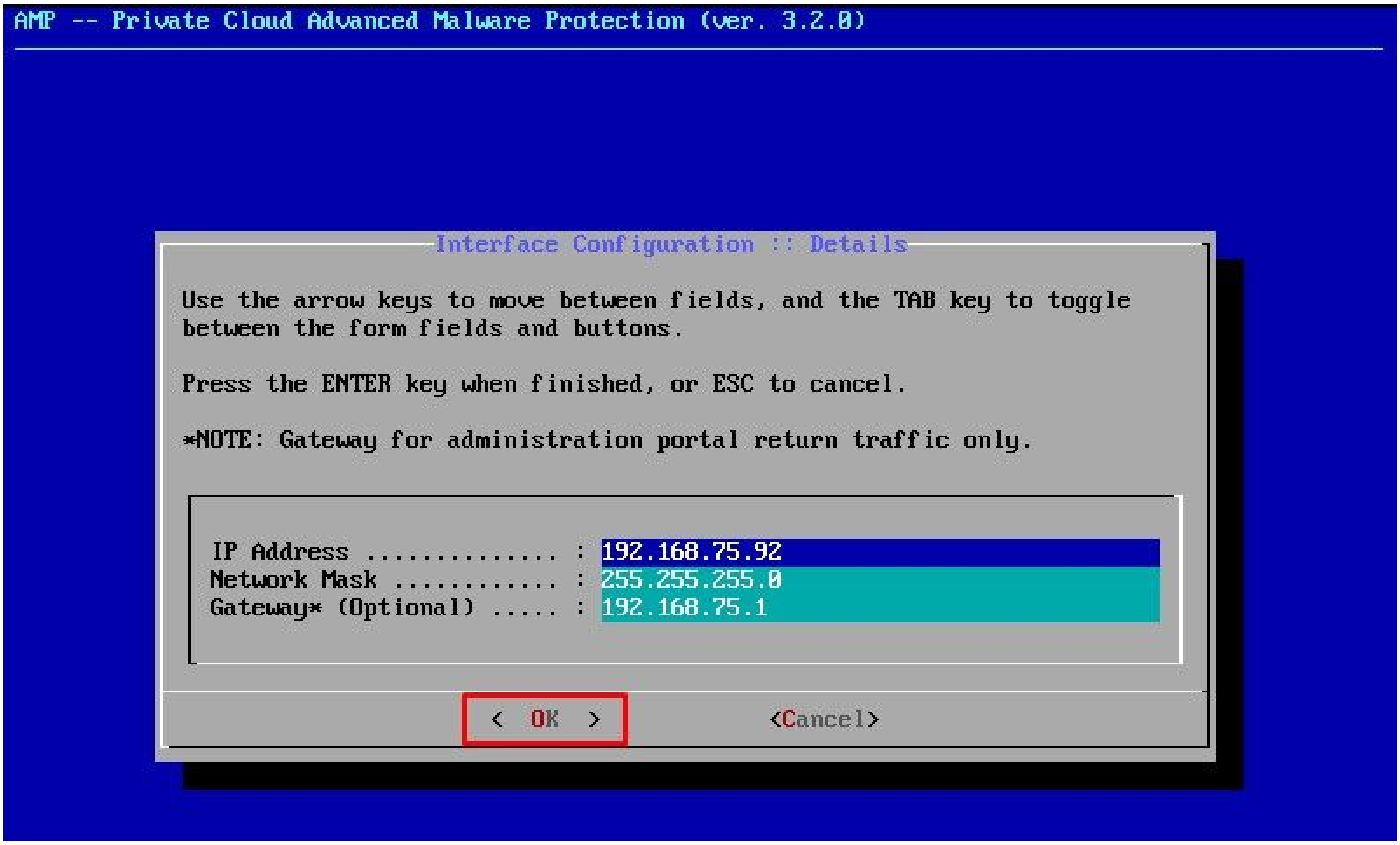


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Apply Your Interface Configuration?

Reconfigure your administration interface with a static configuration?
```

如果IP已在使用中，您将使用此错误日志进行处理。只需返回并选择独一无二且未使用的产品。

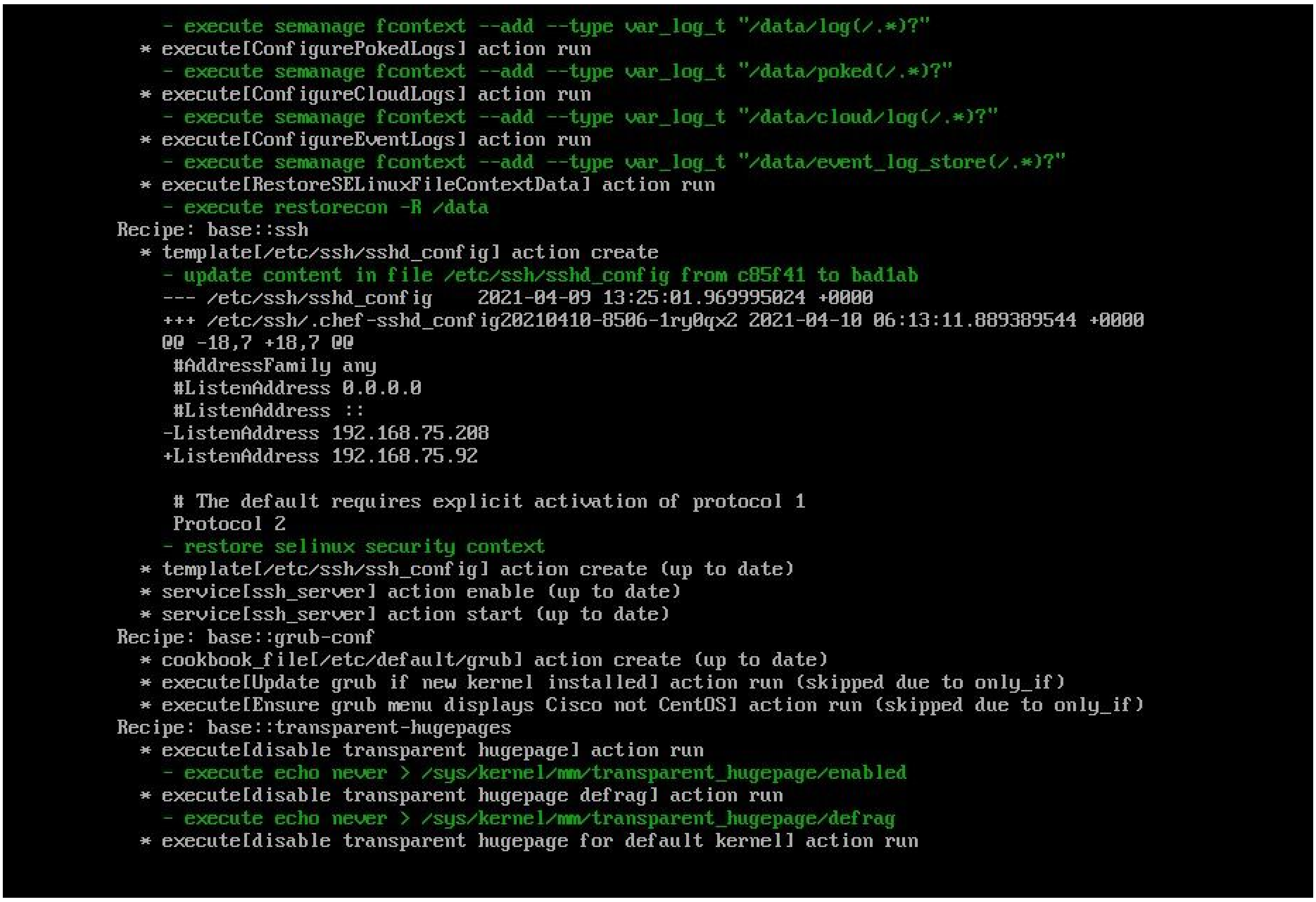


```
Restarting eth0...

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...
_
```

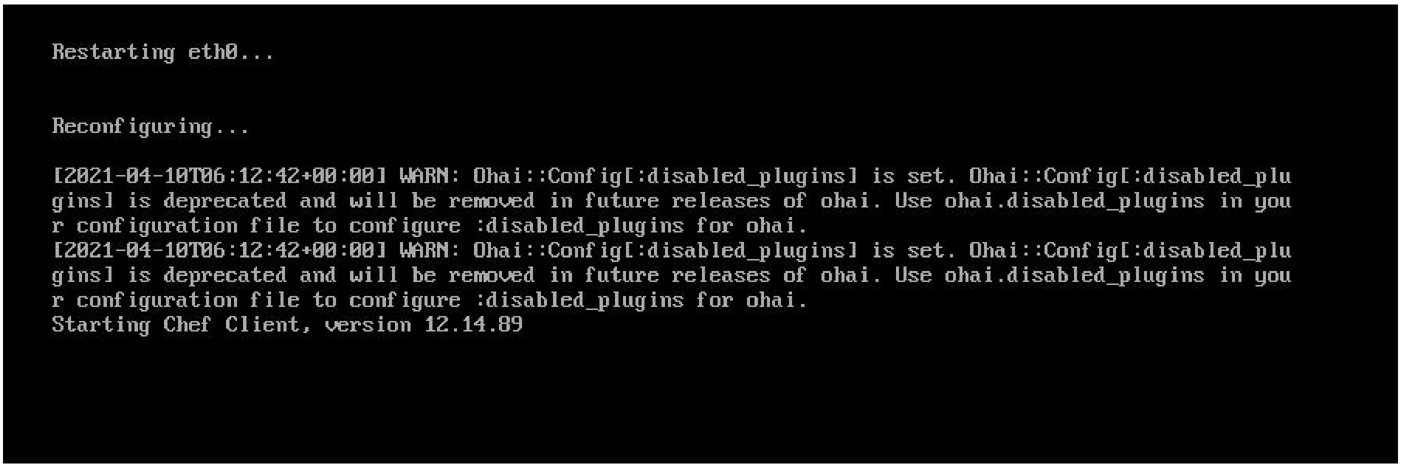


```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

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
```

如果一切顺利，您会看到如下输出



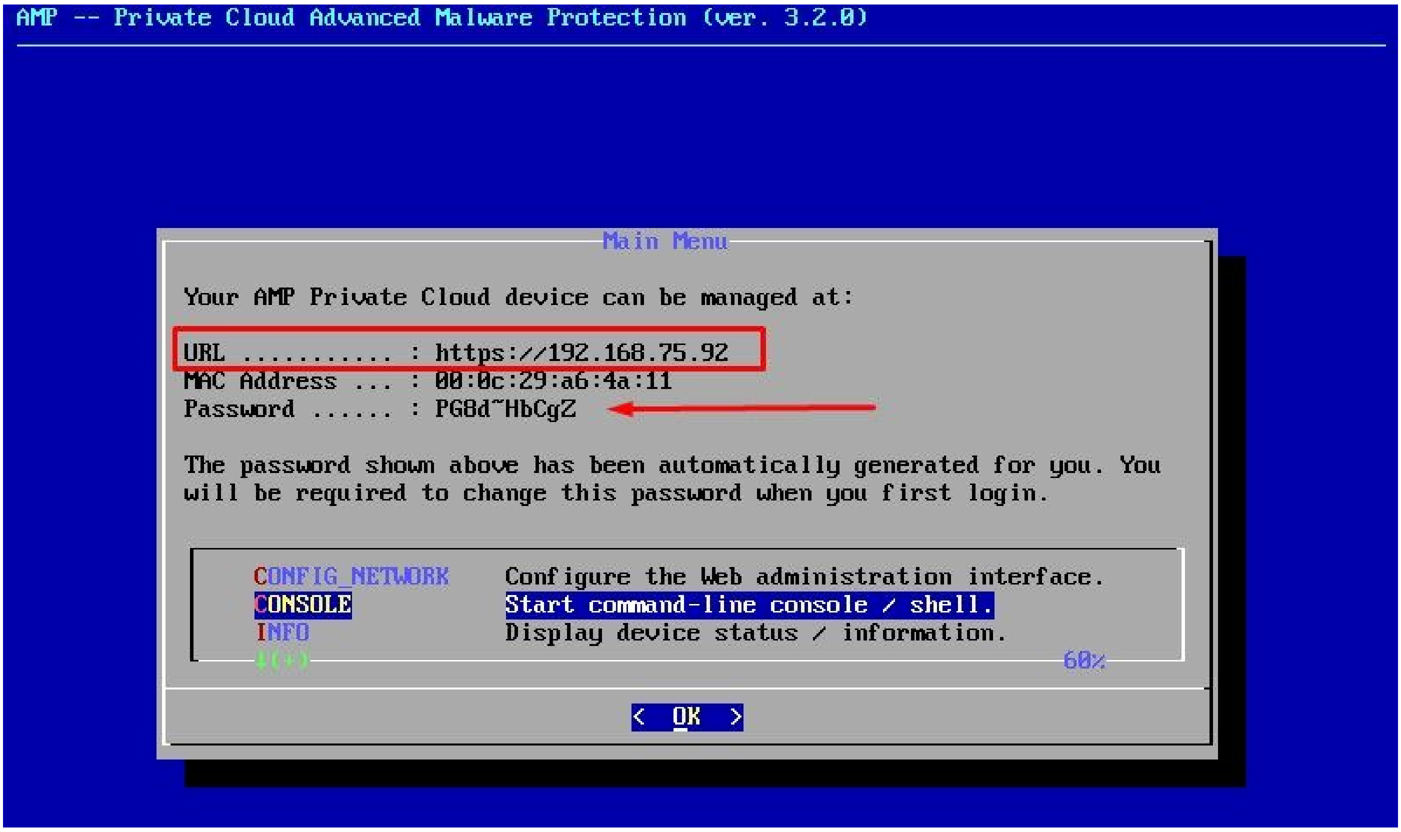
```
      - execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
    * execute[ConfigurePokedLogs] action run
      - execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
    * execute[ConfigureCloudLogs] action run
      - execute semanage fcontext --add --type var_log_t "/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
```

步骤 3：

等到蓝色屏幕再次弹出您的新静态IP。另请注意一次性密码。请记下笔记，然后打开我们的浏览器。



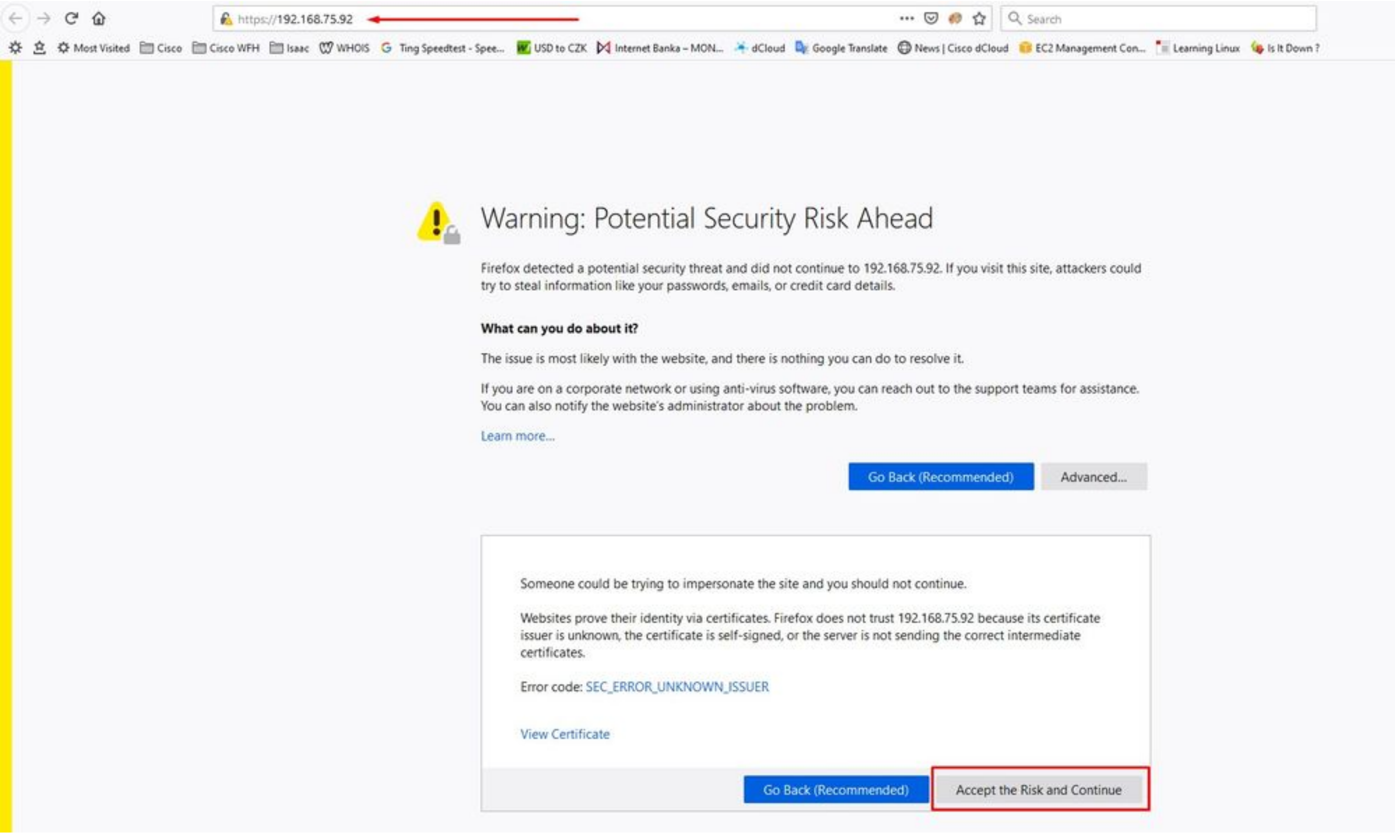
```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

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.
```

通过Web GUI进行vPC的初始配置

步骤 1：

打开Web浏览器并导航到设备的管理IP地址。当安全终端私有云最初生成自己的HTTPS证书时，您可能会收到证书错误，如图所示。将浏览器配置为信任安全终端私有云的自签HTTPS证书。

在浏览器中键入您之前配置的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.

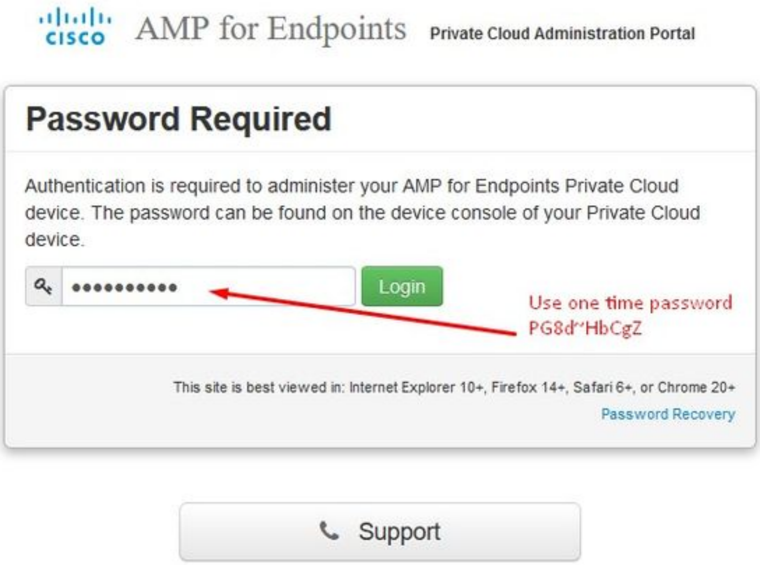
Websites prove their identity via certificates. Firefox does not trust 192.168.75.92 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

步骤 2：

登录后，您需要重置密码。在Old Password字段中使用控制台中的初始密码。在New Password（新密码）字段中使用您的新密码。在“新密码”字段中重新输入新密码。在“更改密码”中选择。



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

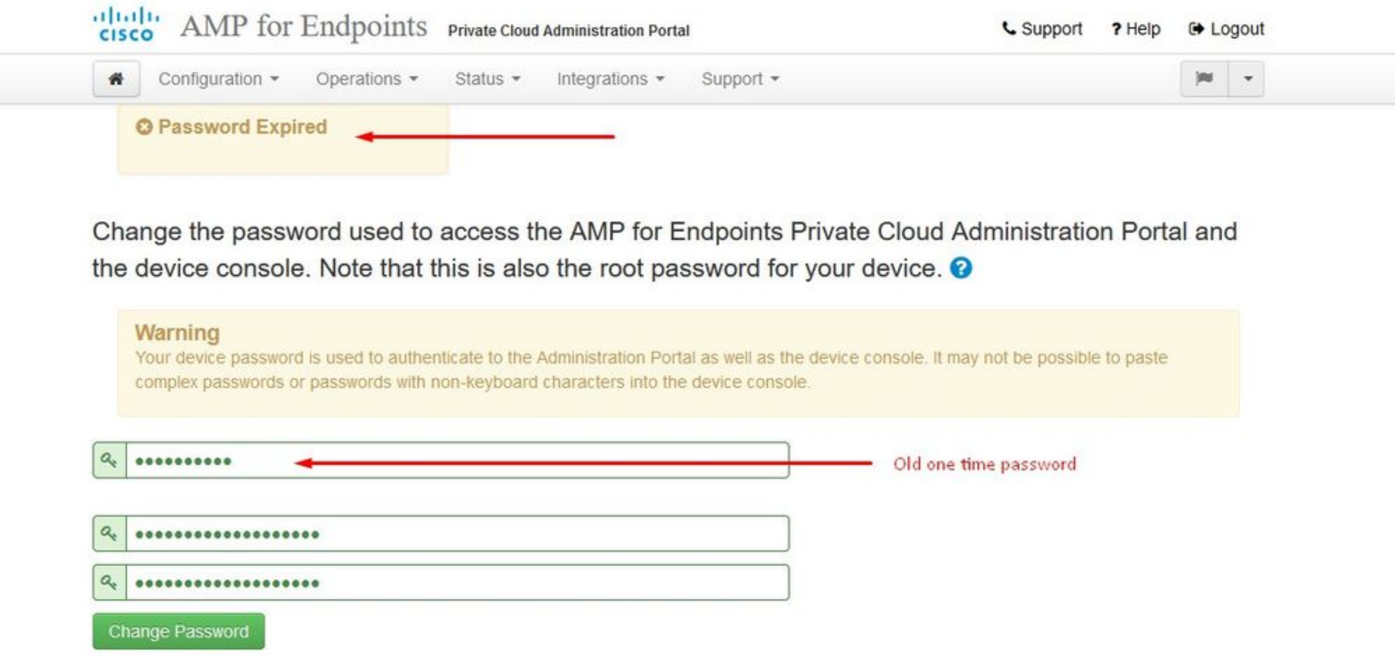
This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

Password Recovery

步骤 3：

登录后，您需要重置密码。在Old Password字段中使用控制台中的初始密码。在New

Password（新密码）字段中使用您的新密码。在“新密码”字段中重新输入新密码。在“更改密码”中选择。

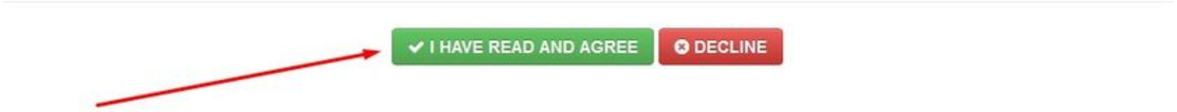


Change the password used to access the AMP for Endpoints Private Cloud Administration Portal and the device console. Note that this is also the root password for your device.

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.

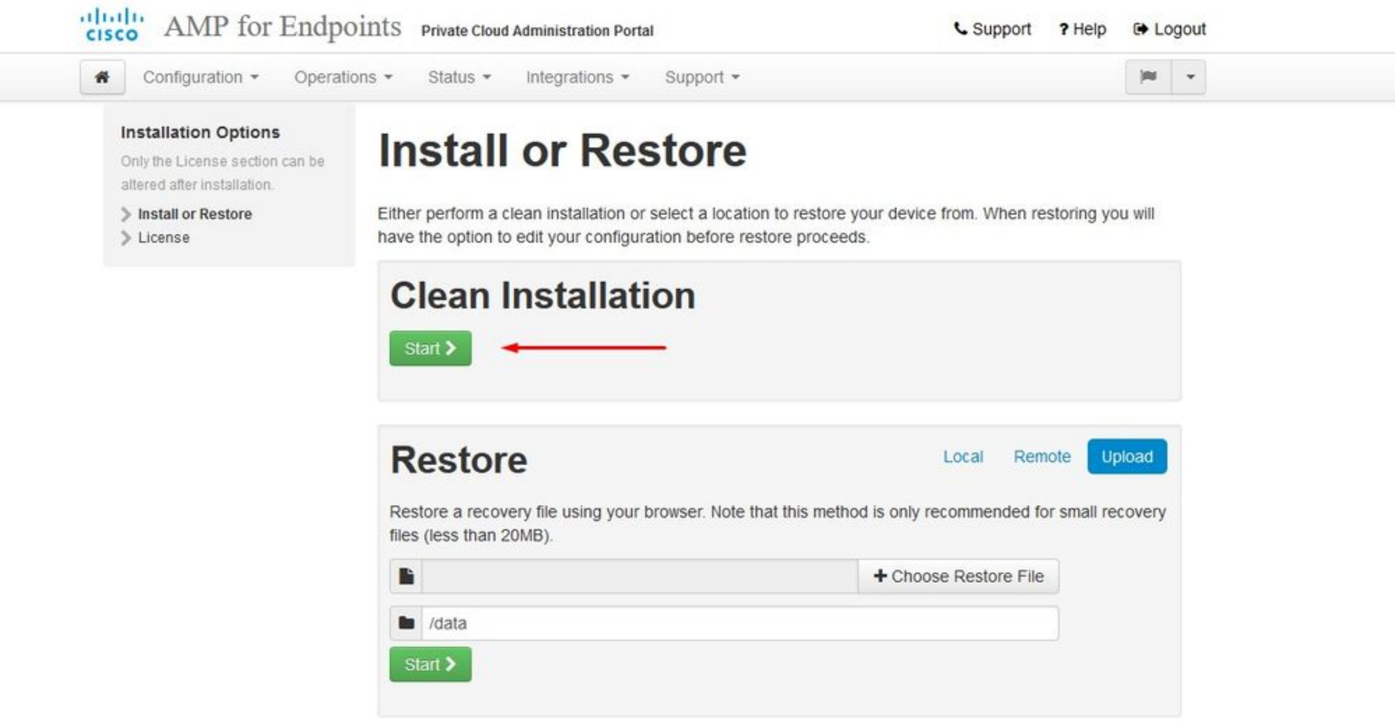
步骤 4：

在下一页上，向下滚动到底部，接受许可协议。选择“我已阅读并同意”(on I have read and agree)。



步骤 5：

接受协议后，您会看到安装屏幕，如图所示。如果您想从备份恢复，可以在此处进行恢复，但本指南将继续使用Clean Installation选项。在Clean Installation部分中选择Start。



Only the License section can be altered after installation.

Install or Restore

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

Clean Installation

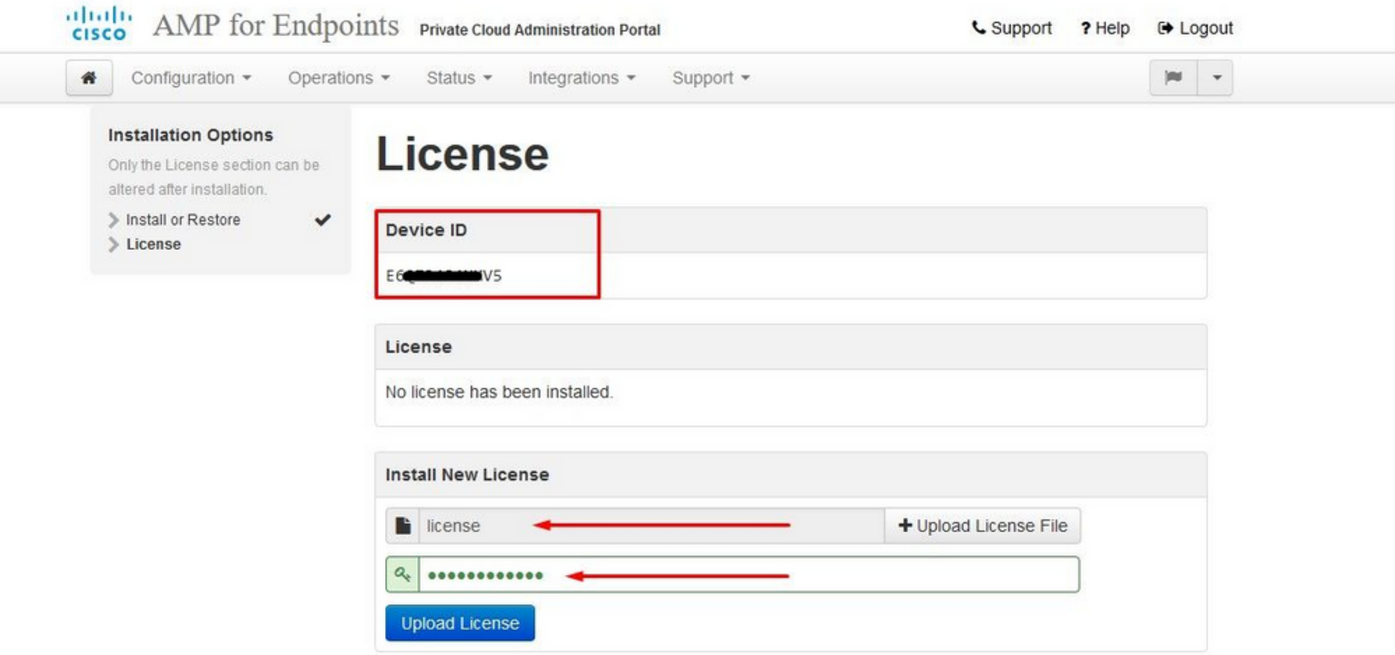
Restore

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

/data

步骤 6：

你需要的第一件事就是获得许可证，甚至可以继续前进。购买产品时，您将收到许可证和密码。选择on +Upload License File。选择许可证文件并输入密码。选择Upload License。如果上传失败，请检查密码是否正确。如果上传成功，将显示包含有效许可证信息的屏幕。选择“下一步”。 如果仍然无法安装许可证，请与Cisco技术支持联系。



Only the License section can be altered after installation.

License

Device ID

E6[redacted]V5

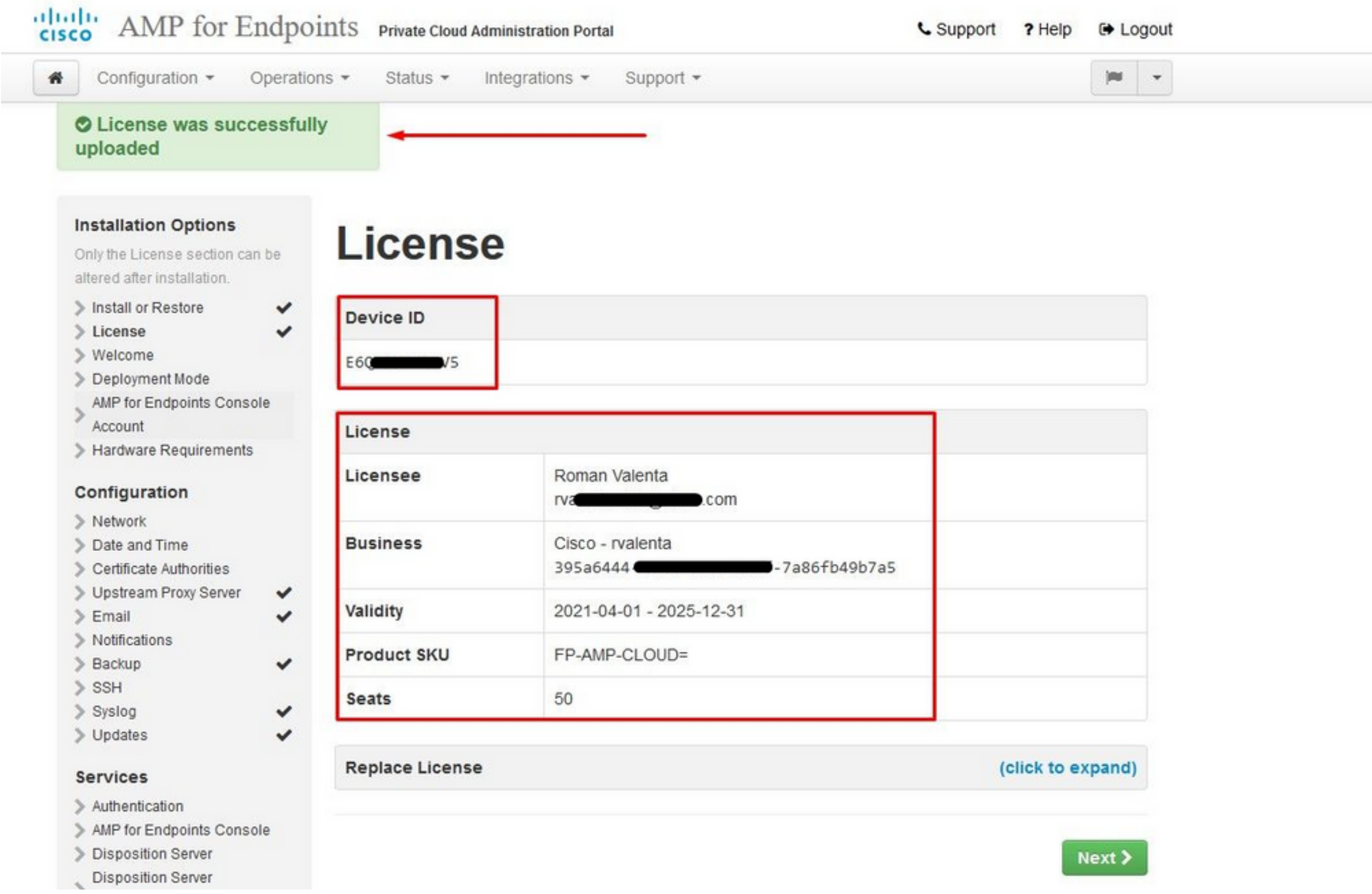
License

No license has been installed.

Install New License

license

•••••••••••••



License was successfully uploaded

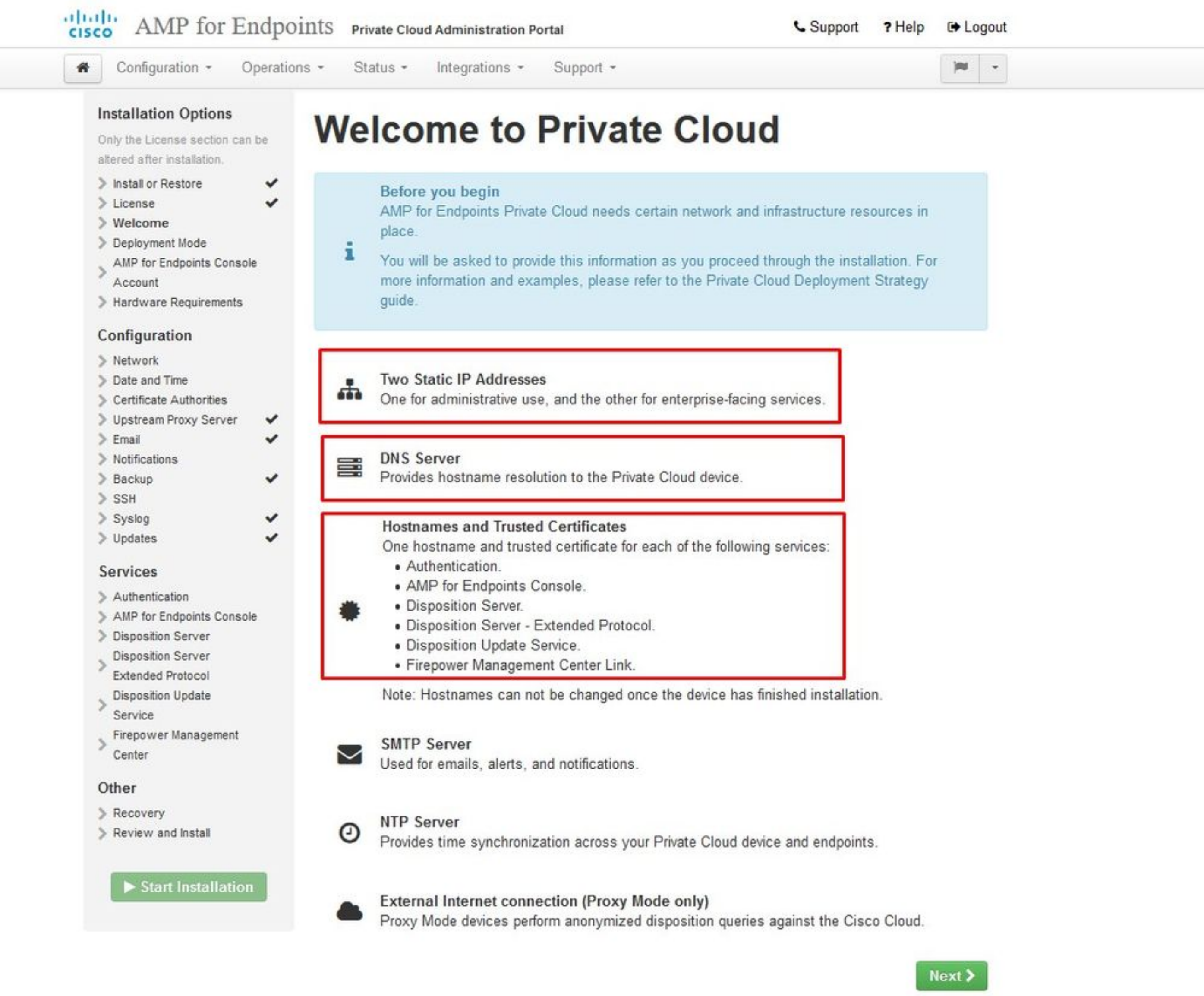
License

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

步骤 7：

您将收到欢迎页面，如图所示。此页显示配置私有云之前必须拥有的信息。仔细阅读要求。选择Next以启动安装前配置。



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.

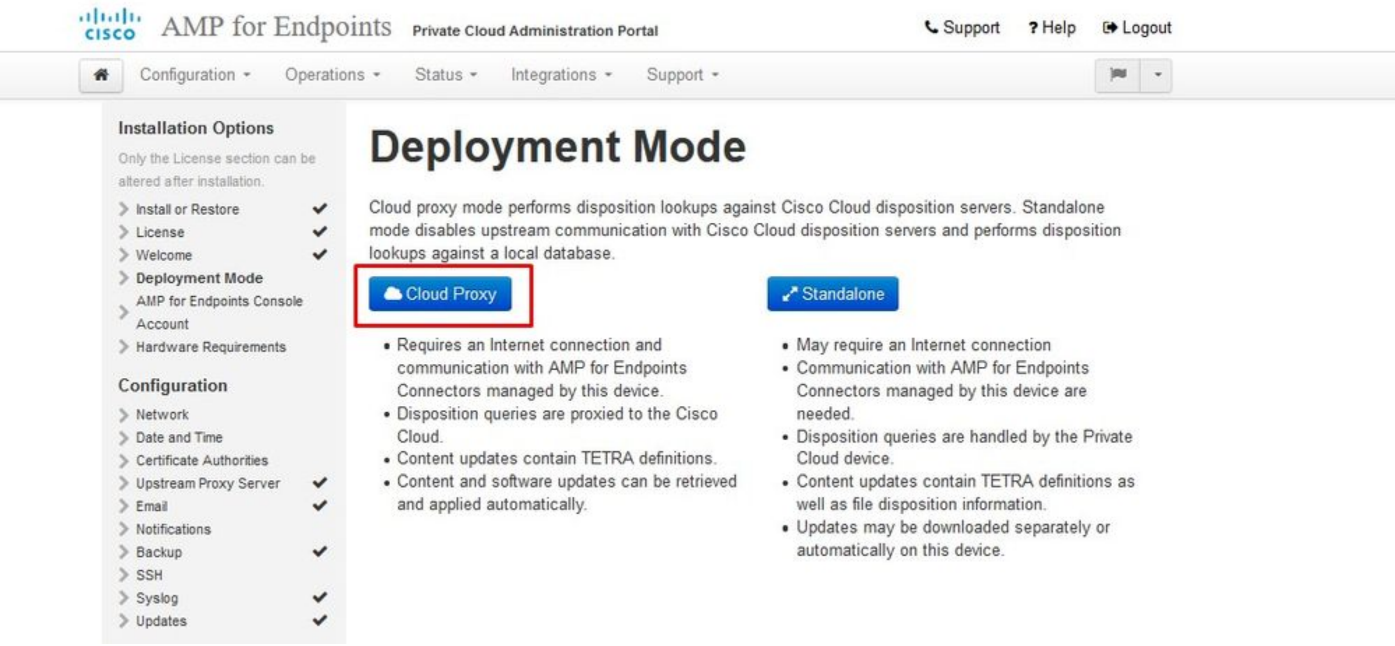
NTP Server
Provides time synchronization across your Private Cloud device and endpoints.

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

配置

步骤 1：

注意：请注意，在下一组幻灯片中，我们包含一些独占内容（如图所示），这些内容仅是AIR GAP模式所独有的，应将其括起来并标记为AIRGAP ONLY



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.

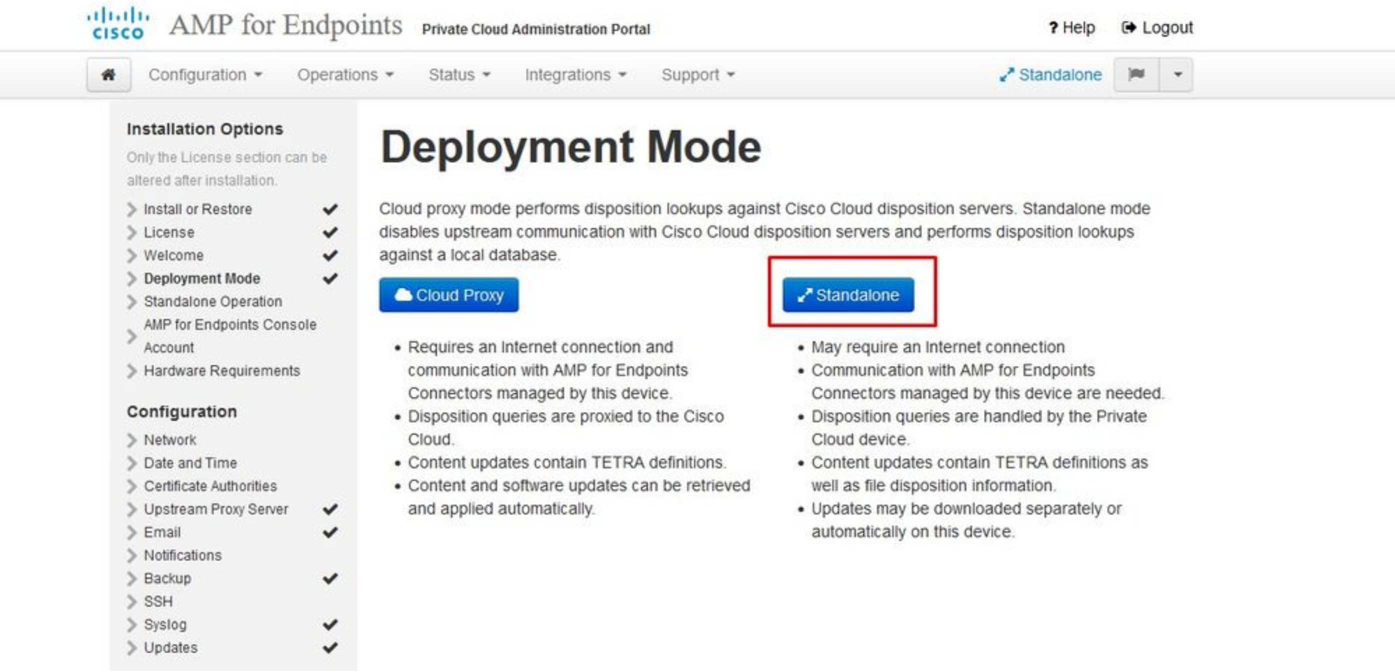
Cloud Proxy

- 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 ︾︾



Deployment Mode

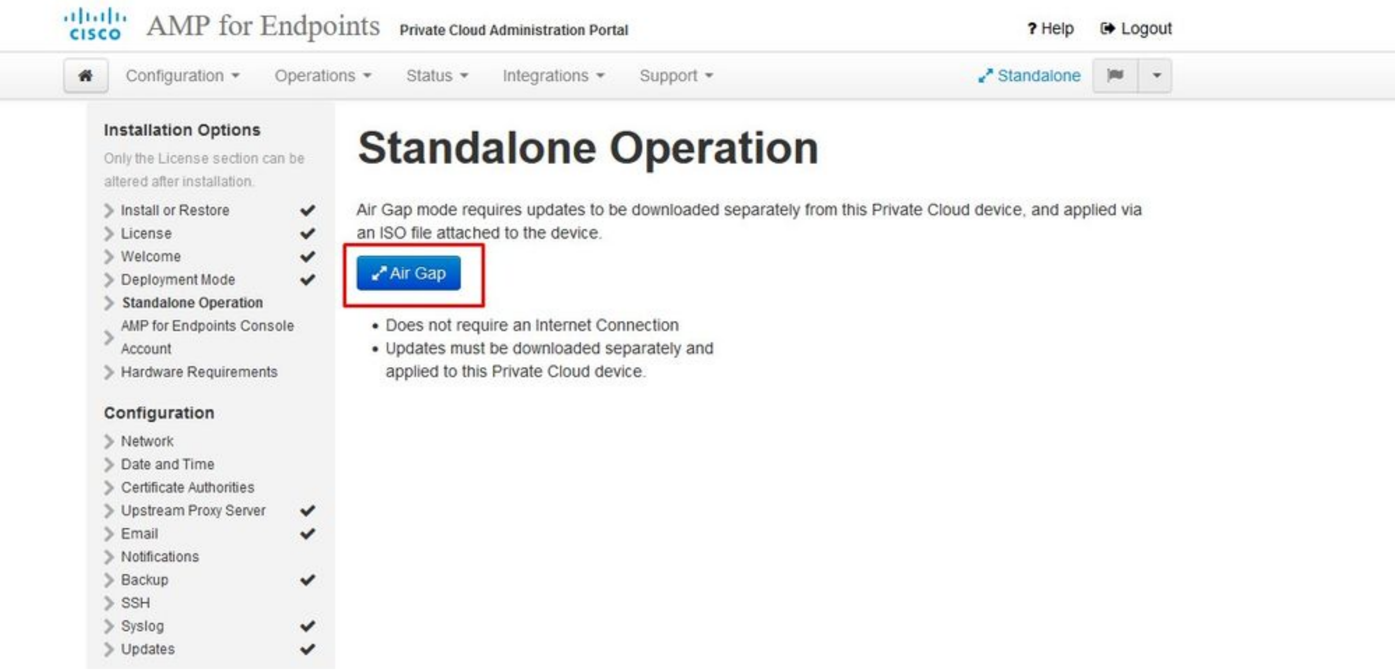
Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

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

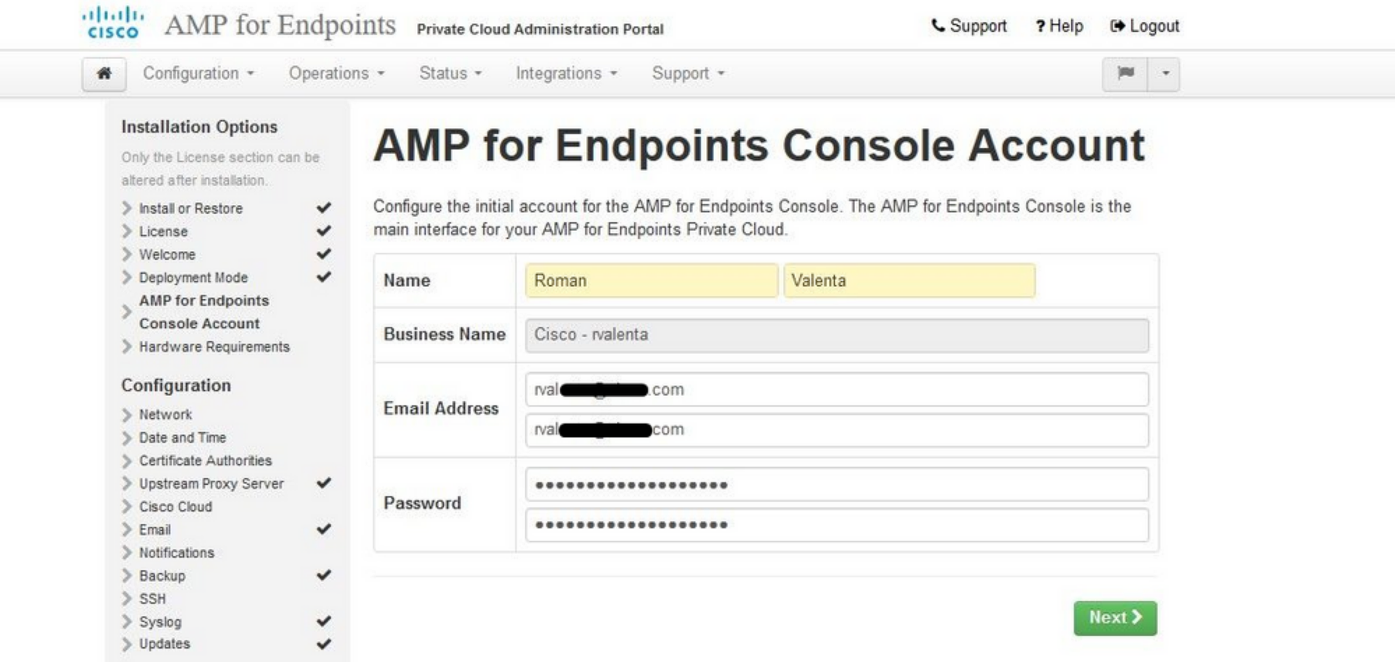
Air Gap mode requires updates to be downloaded separately from this Private Cloud device, and applied via an ISO file attached to the device.

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

仅︽︽AIRGAP︽︽

步骤 2：

导航到Secure Endpoint Console Account页面。管理用户用于控制台，以创建策略、计算机组并添加其他用户。输入控制台帐户的名称、电子邮件地址和密码。选择Next。



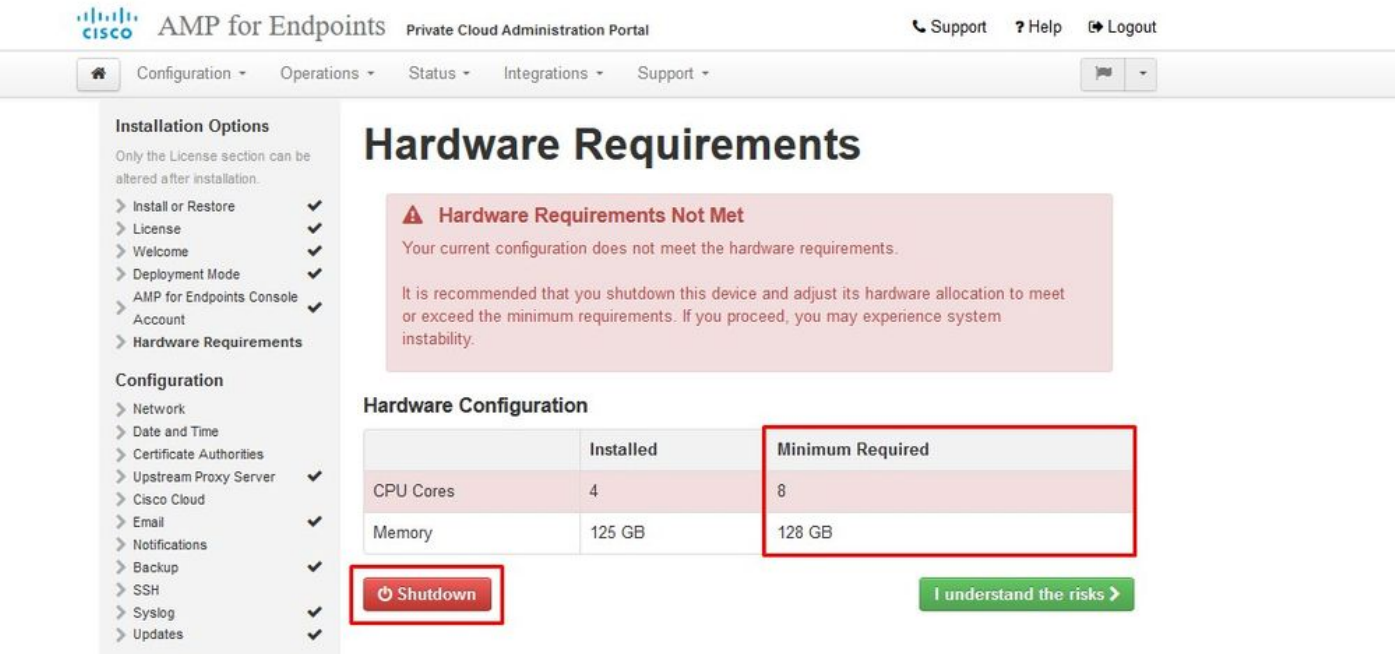
AMP for Endpoints Console Account

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	•••••••••••••••••••• ••••••••••••••••••••	

如果在从OVA文件部署时解决此问题，则您有两种选择：稍后继续并修复此问题，或者关闭以部署到已部署的虚拟机并相应地调整。重新启动后，继续您离开的位置。

注：这已在OVA文件中修复，适用于版本3.5.2，使用128GB RAM和8CPU核心正确加载



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

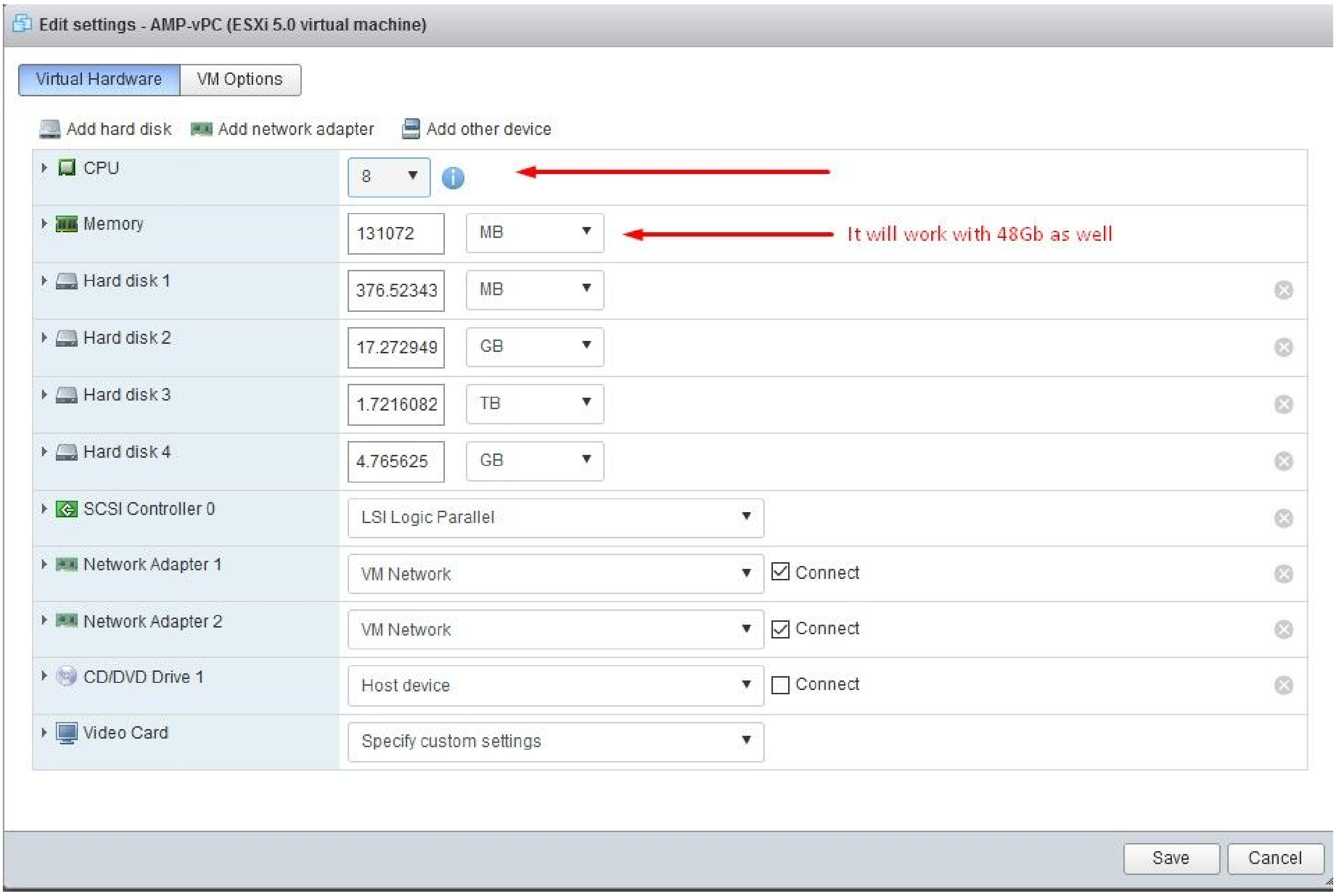
Your current configuration does not meet the hardware requirements.

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

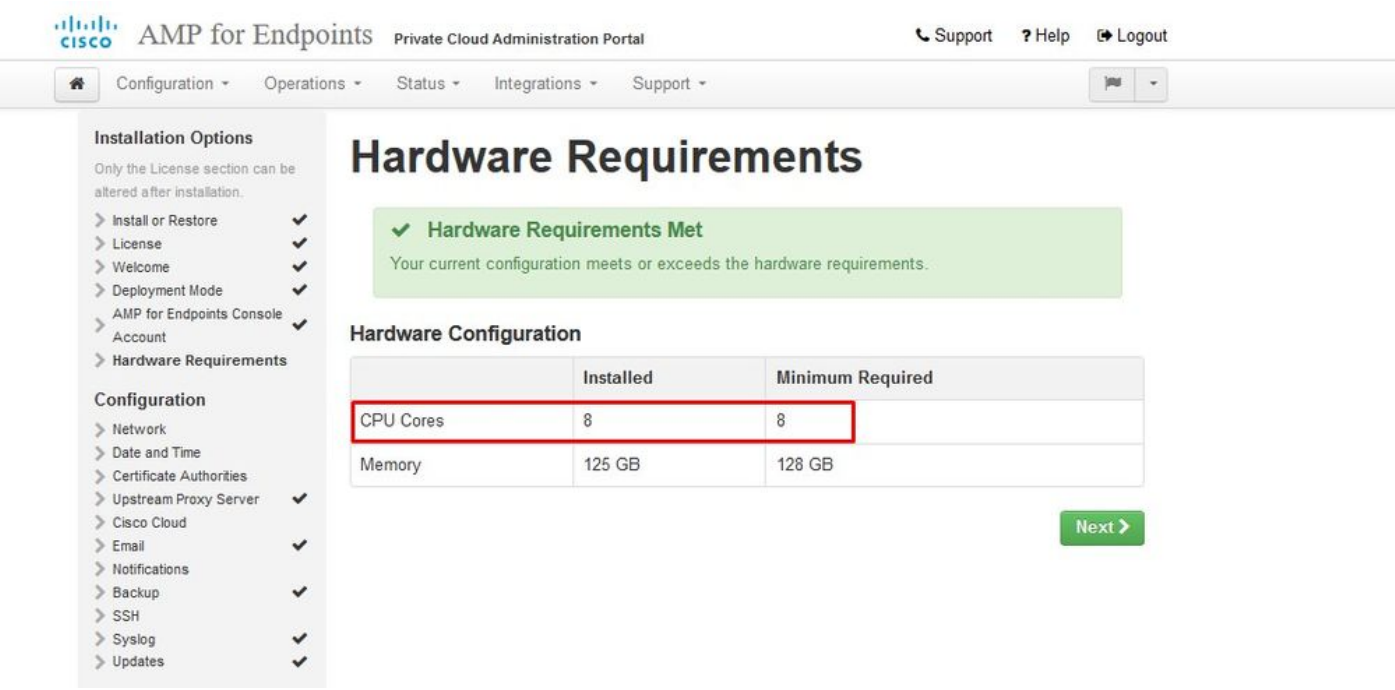
注：除非用于实验，否则请仅使用建议值



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		

重新启动后，我们继续原来的位置。



Hardware Requirements

✓ Hardware Requirements Met

Your current configuration meets or exceeds the hardware requirements.

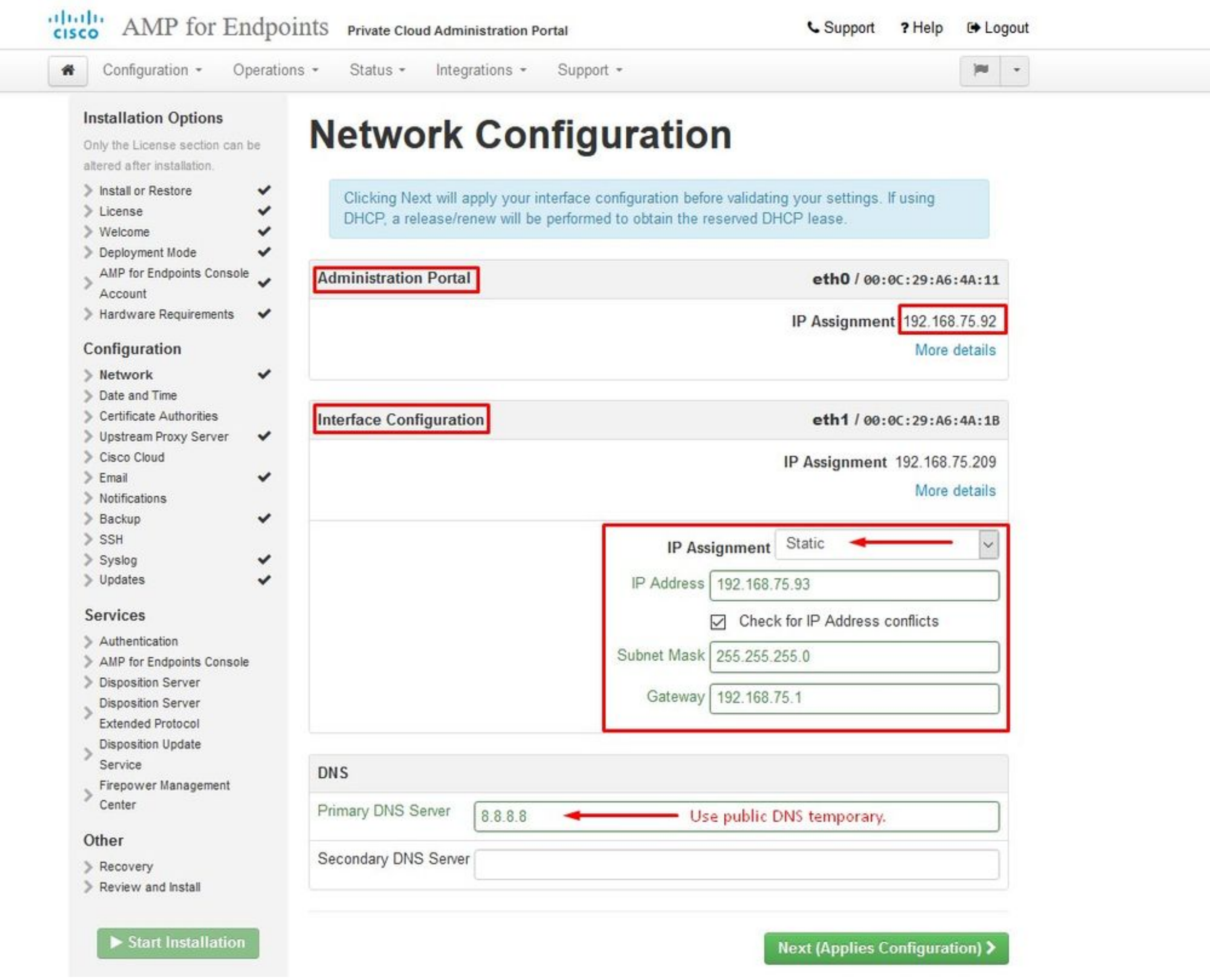
Hardware Configuration

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

确保也为ETH1配置静态IP。

注意：除非您已为接口创建MAC地址预留，否则切勿将设备配置为使用DHCP。如果接口的IP地址发生更改，则可能导致已部署的安全终端连接器出现严重问题。如果未配置DNS服务器，您可以使用公共DNS临时功能完成安装。

步骤 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

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

IP Assignment 192.168.75.209

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

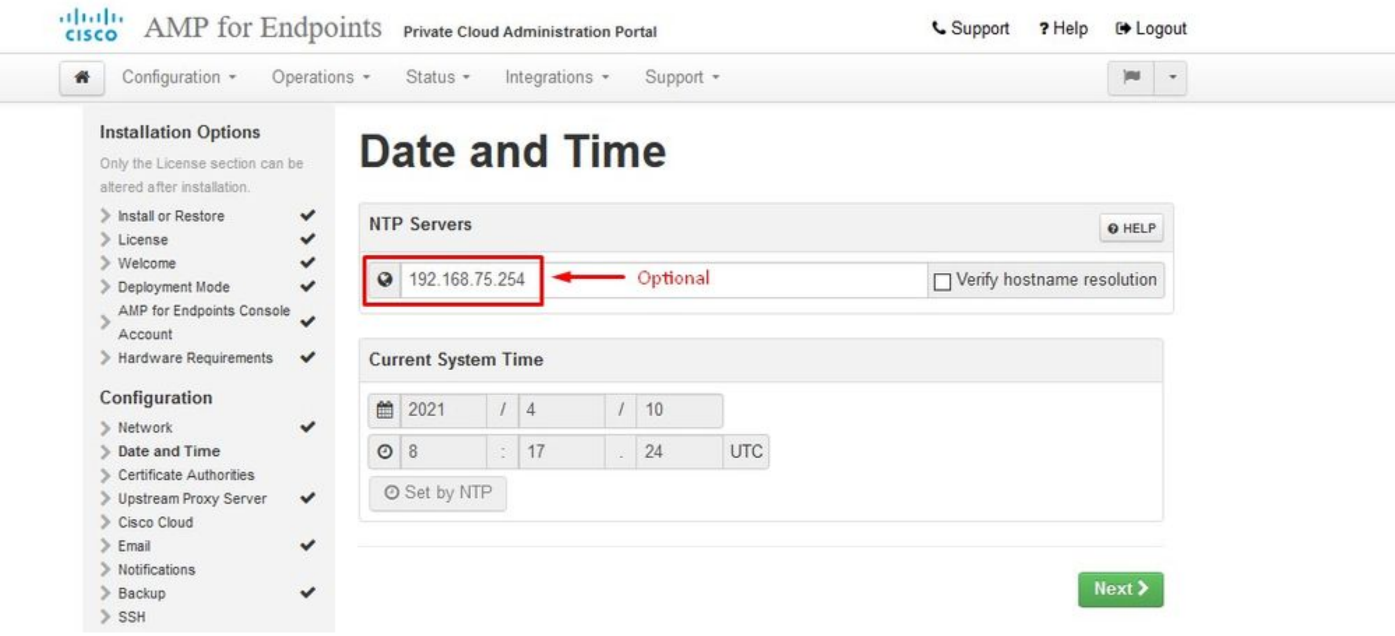
DNS

Primary DNS Server: 8.8.8.8 — Use public DNS temporary.

Secondary DNS Server:

步骤 4：

您将看到“日期和时间”页面。输入要用于日期和时间同步的一个或多个NTP服务器的地址。您可以使用内部或外部NTP服务器，并指定多个以逗号或空格分隔的列表。将时间与浏览器同步，或从设备控制台运行amp-ctl ntpdate以强制与NTP服务器进行即时时间同步。选择“下一步”。



Date and Time

NTP Servers

192.168.75.254

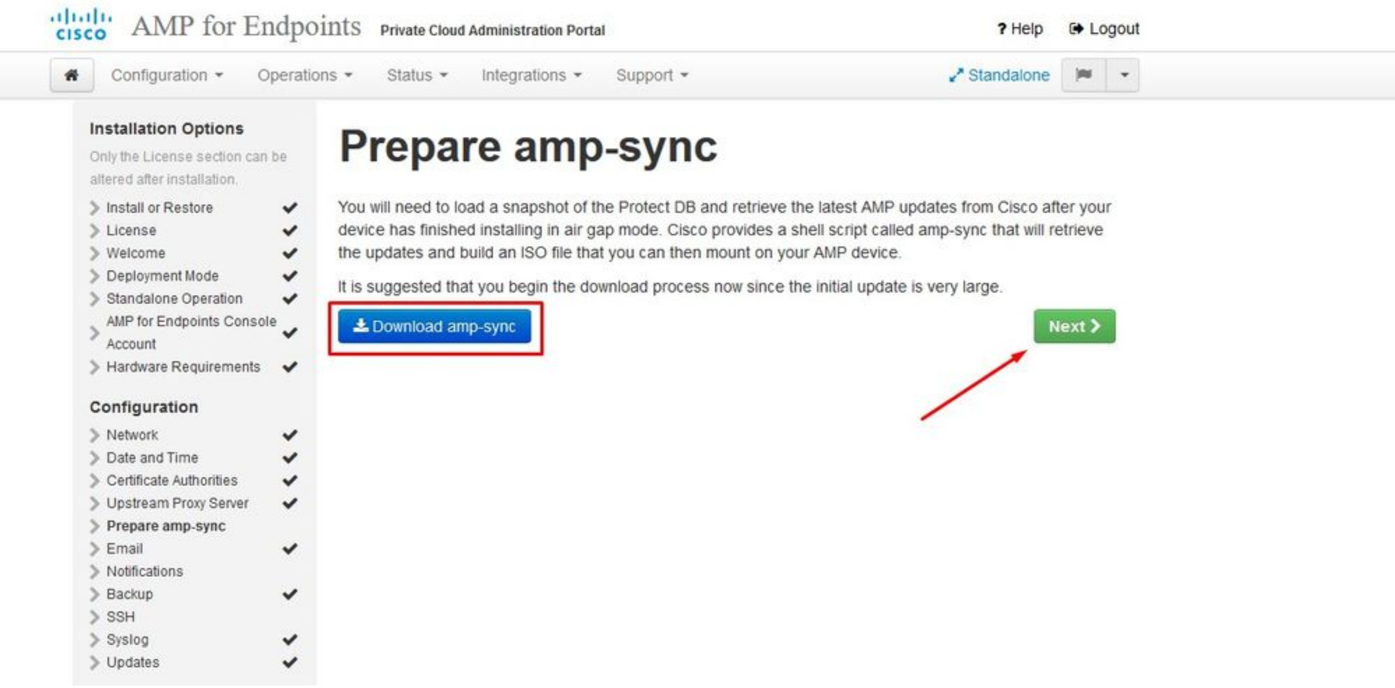
□ Verify hostname resolution

Current System Time

2021 / 4 / 10

8 : 17 . 24 UTC

︾︾ AIRGAP ONLY ︾︾



Prepare amp-sync

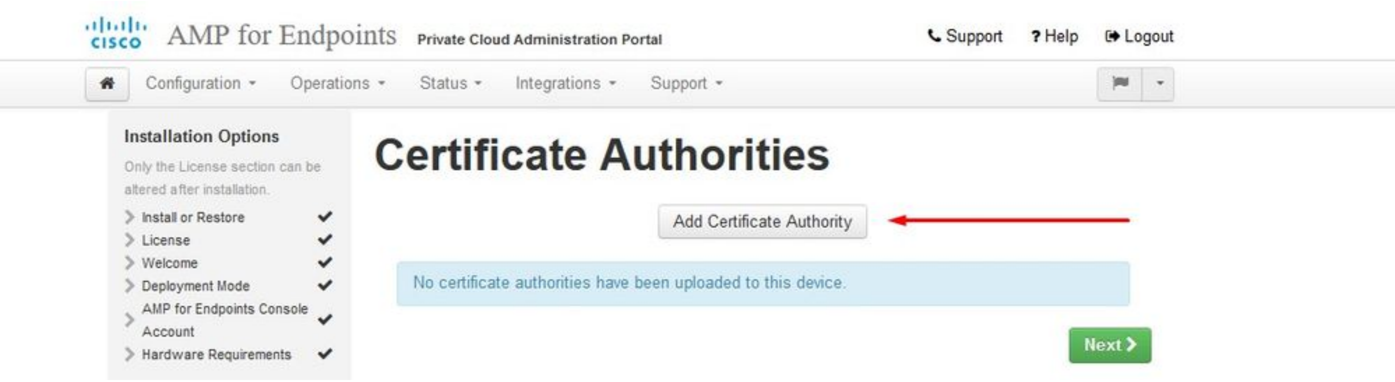
You will need to load a snapshot of the Protect DB and retrieve the latest AMP updates from Cisco after your device has finished installing in air gap mode. Cisco provides a shell script called amp-sync that will retrieve the updates and build an ISO file that you can then mount on your AMP device.

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

仅︽︽AIRGAP︽︽

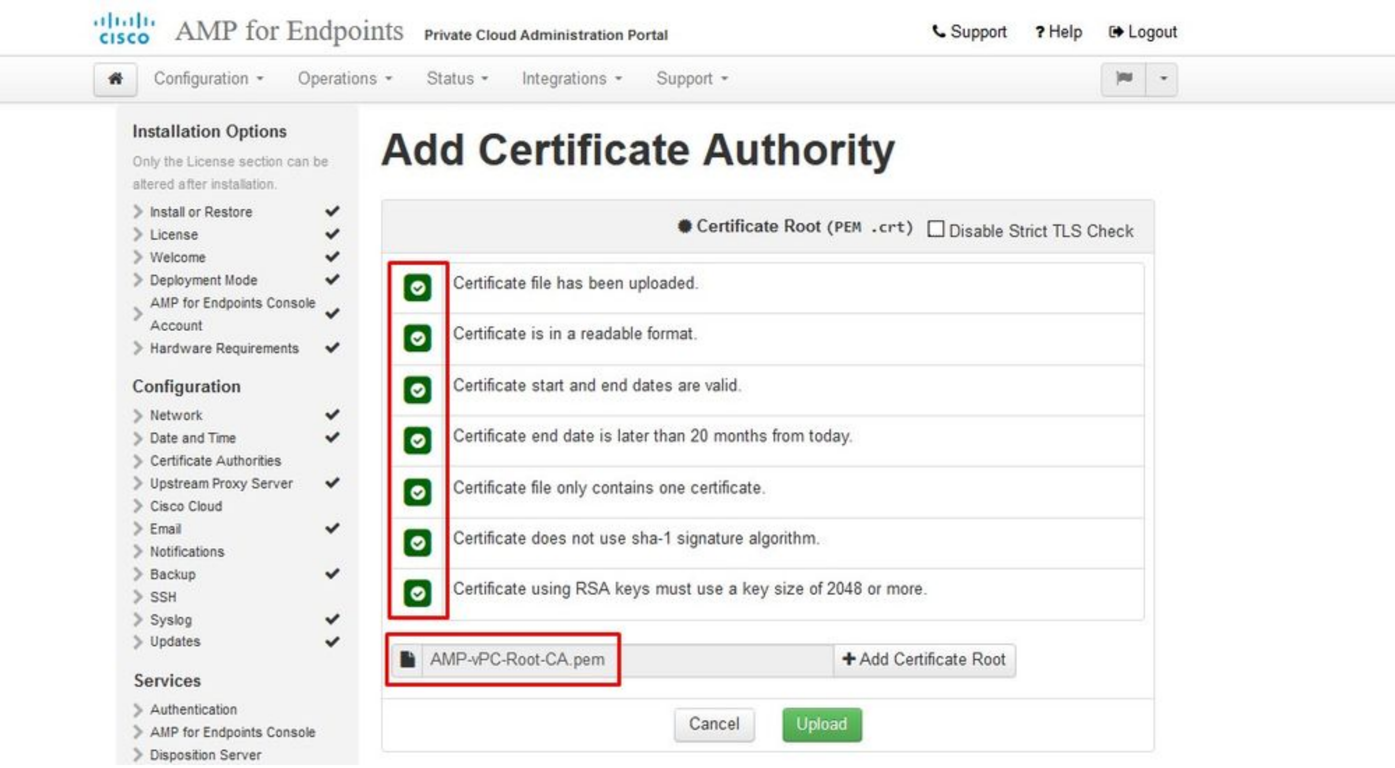
步骤 5：

您将看到Certificate Authorities页面，如图所示。选择on Add Certificate Authority以添加根证书。



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.

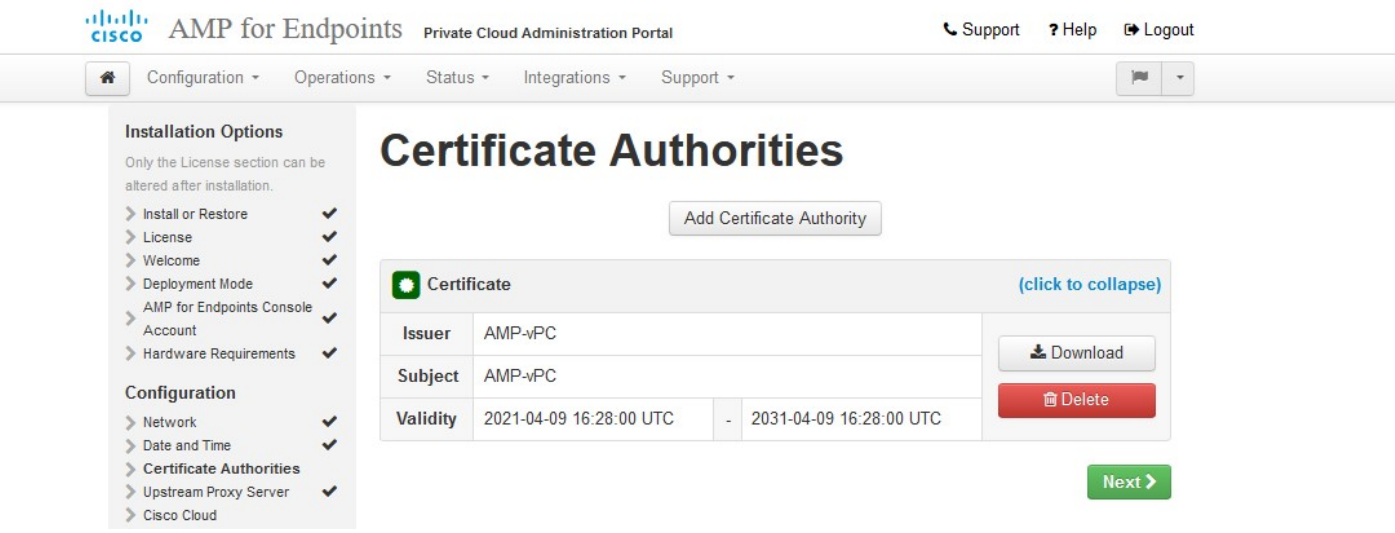
✓ Certificate end date is later than 20 months from today.

✓ 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

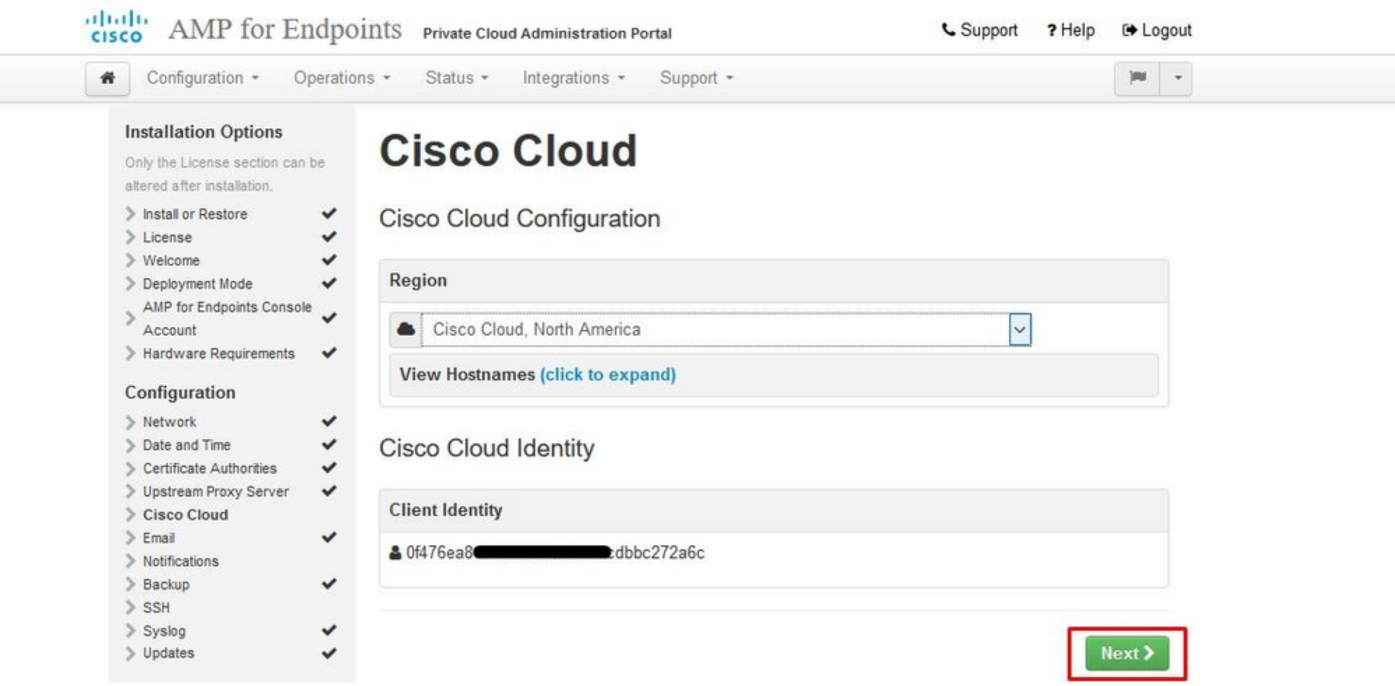
Certificate

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

步骤 6：

下一步是配置思科云页面，如图所示。选择适当的思科云区域。如果需要为安全终端私有云设备创建防火墙例外以与思科云进行通信以进行文件查找和设备更新，请展开View Hostnames。选择

Next。



Cisco Cloud

Cisco Cloud Configuration

Region: Cisco Cloud, North America

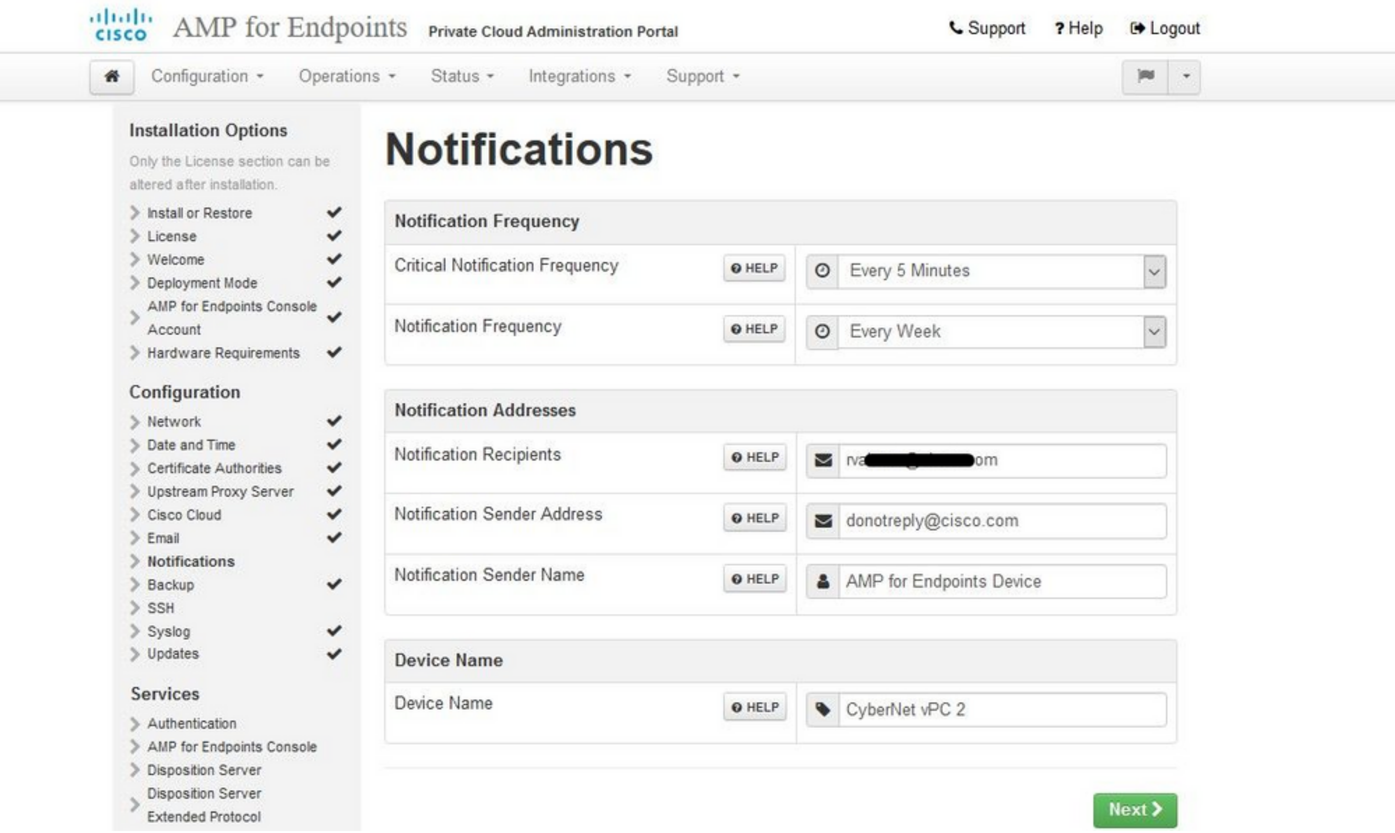
View Hostnames (click to expand)

Cisco Cloud Identity

Client Identity: 0f476ea8[redacted]dbbc272a6c

步骤 7：

导航至通知页面，如图所示。选择关键通知和定期通知的频率。输入要接收安全终端设备警报通知的邮件地址。您可以使用邮件别名，或通过逗号分隔列表指定多个地址。您还可以指定设备使用的发件人姓名和邮件地址。这些通知与安全终端控制台订阅不同。如果您有多个安全终端私有云设备，您还可以指定唯一的设备名称。选择“下一步”。



Notifications

Notification Frequency

Critical Notification Frequency	Every 5 Minutes
Notification Frequency	Every Week

Notification Addresses

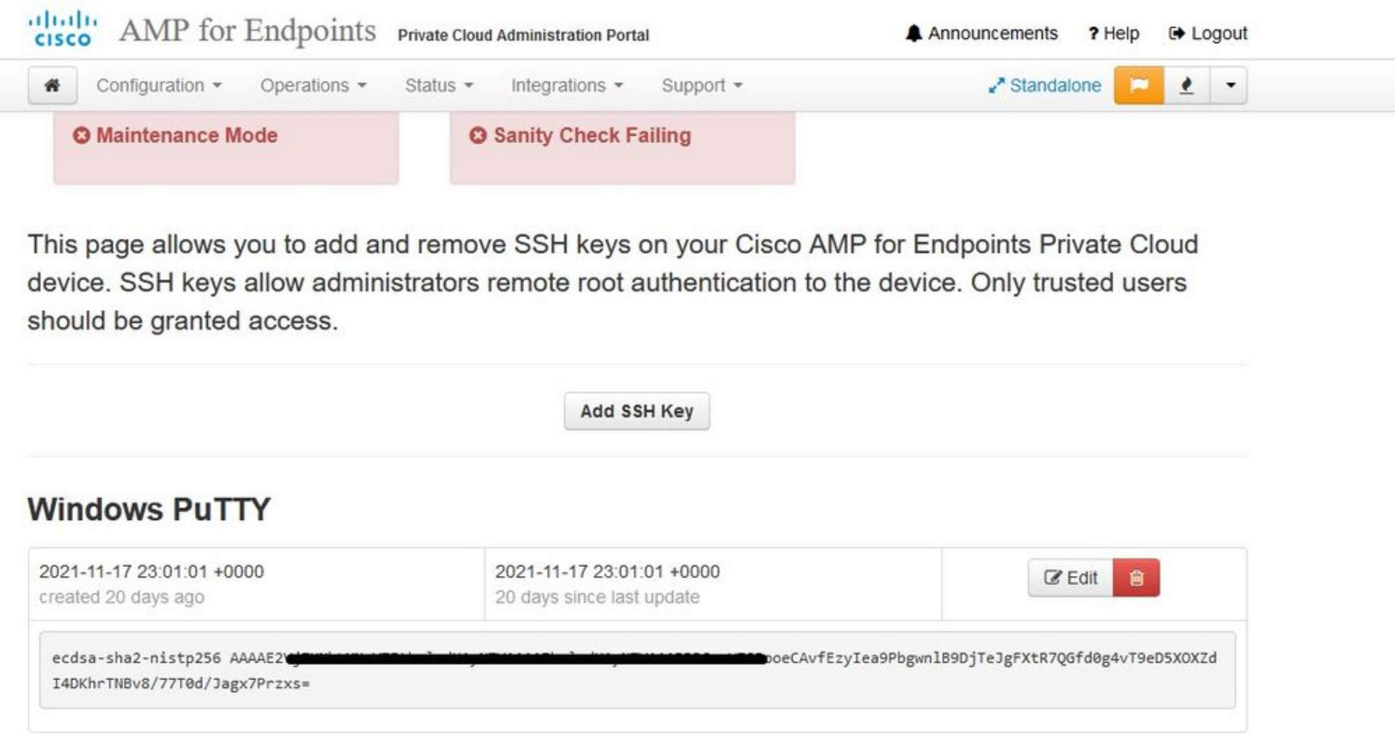
Notification Recipients	rva[redacted]om
Notification Sender Address	donotreply@cisco.com
Notification Sender Name	AMP for Endpoints Device

Device Name

Device Name	CyberNet vPC 2

步骤 8::

接下来，导航至SSH Keys页面，如图所示。选择on Add SSH Key以输入要添加到设备的所有公钥。SSH密钥允许您通过具有根权限的远程外壳访问设备。只有受信任的用户才能被授予访问权限。您的私有云设备需要OpenSSH格式的RSA密钥。您稍后可以通过Administration Portal中的Configuration > SSH添加更多SSH密钥。选择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]oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7QGfd0g4vT9eD5XOXZd
I4DKhrTNBv8/77T0d/Jagx7Przxs=
```

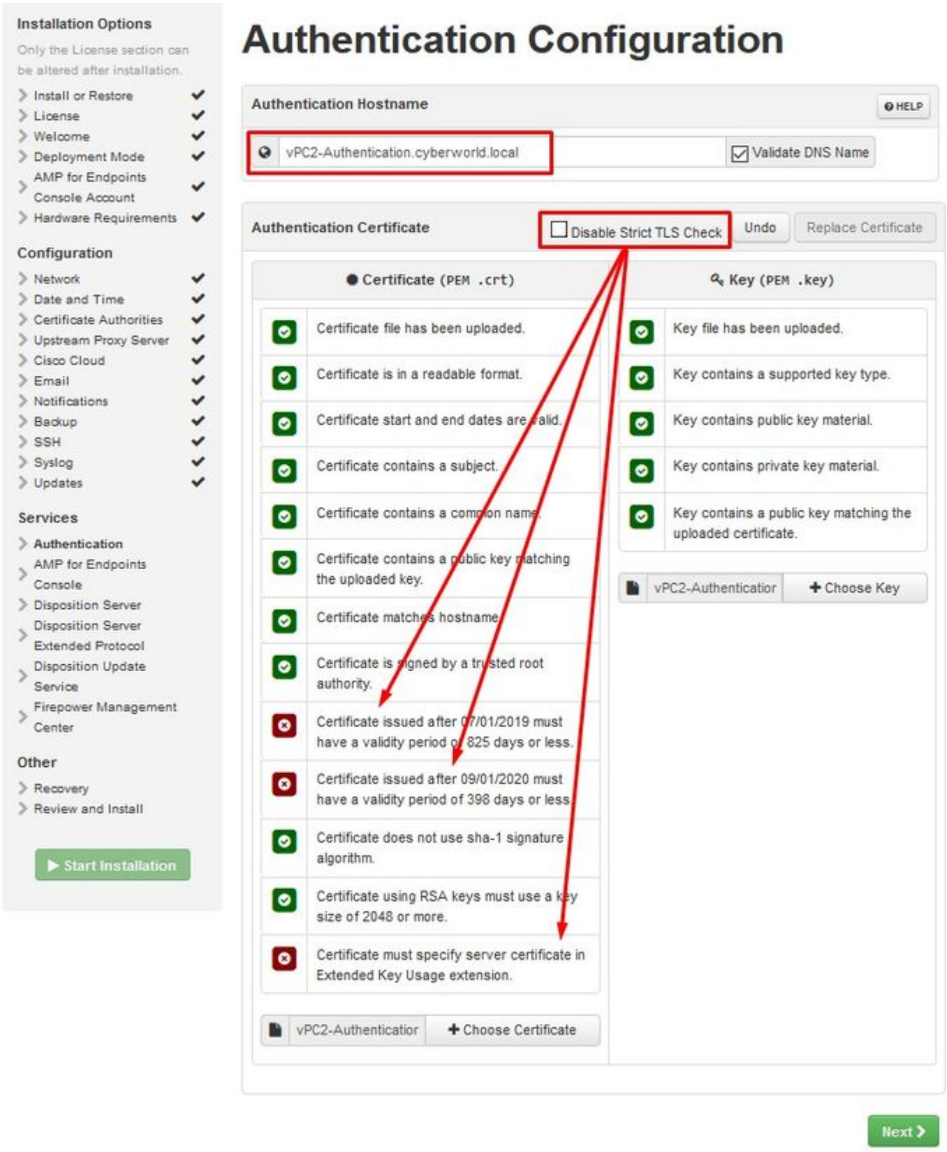
接下来，您将看到“服务”部分。在接下来的页面中，您需要为这些设备服务分配主机名并上传适当的证书和密钥对。在接下来的几张幻灯片中，我们可以看到6个证书中的一个的配置。

服务

步骤 1：

在配置过程中，您可能会遇到这些错误。

您可能会注意到的第一个“错误”以3个箭头突出显示。要绕过此检查，只需取消选中“Disable Strict TLS Check”



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

Authentication Configuration

Authentication Hostname — HELP

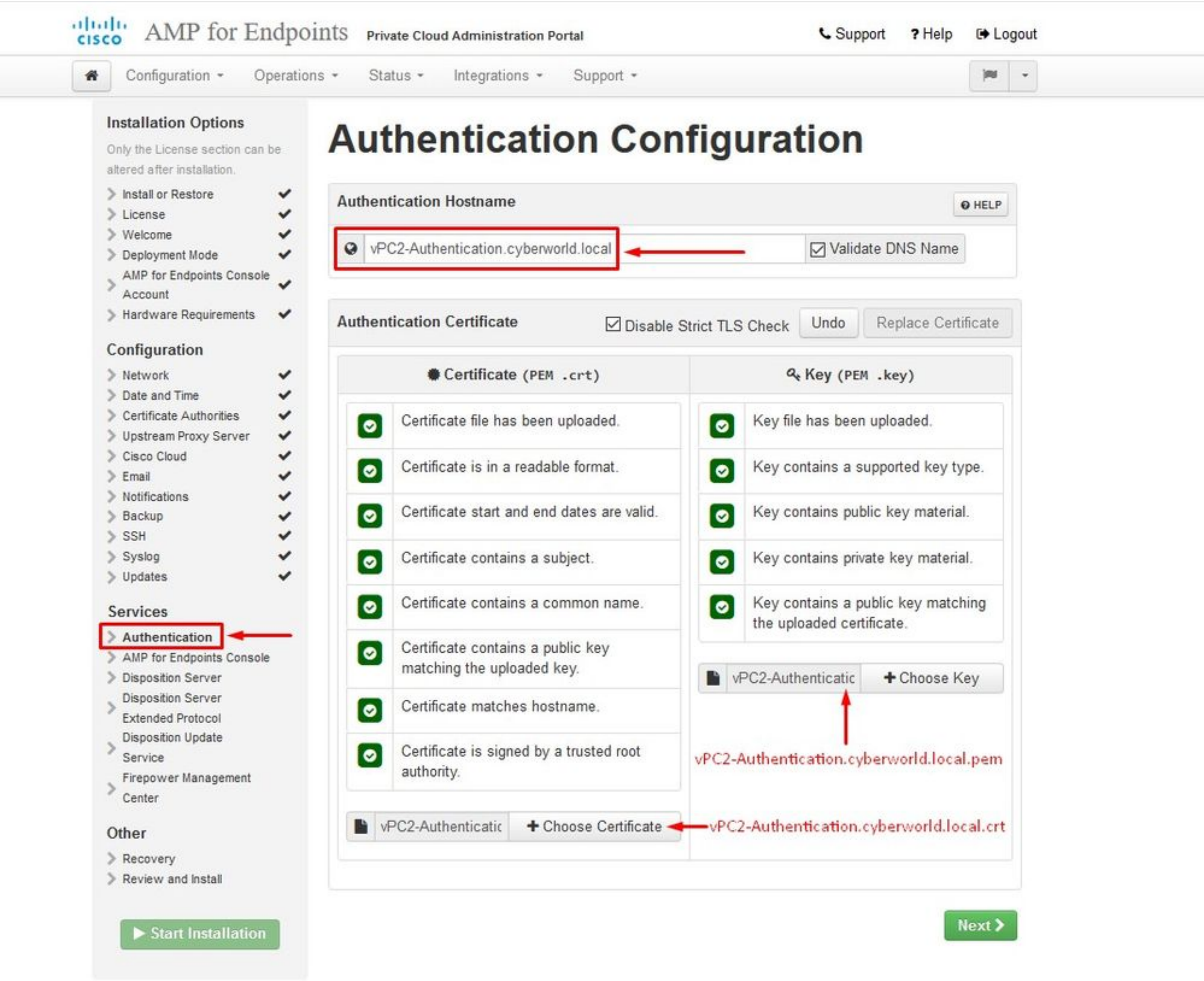
vPC2-Authentication.cyberworld.local — ☑ Validate DNS Name

Authentication Certificate — □ Disable Strict TLS Check — Undo — Replace Certificate

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.	vPC2-Authenticatior — + Choose 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	

Next >

不使用严格TLS检查



Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local ☑ Validate DNS Name

Authentication Certificate ☑ Disable Strict TLS Check Undo Replace Certificate

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.	vPC2-Authenticatic + Choose Key
✓ Certificate matches hostname.	
✓ Certificate is signed by a trusted root authority.	
vPC2-Authenticatic + Choose Certificate	

vPC2-Authentication.cyberworld.local.pem

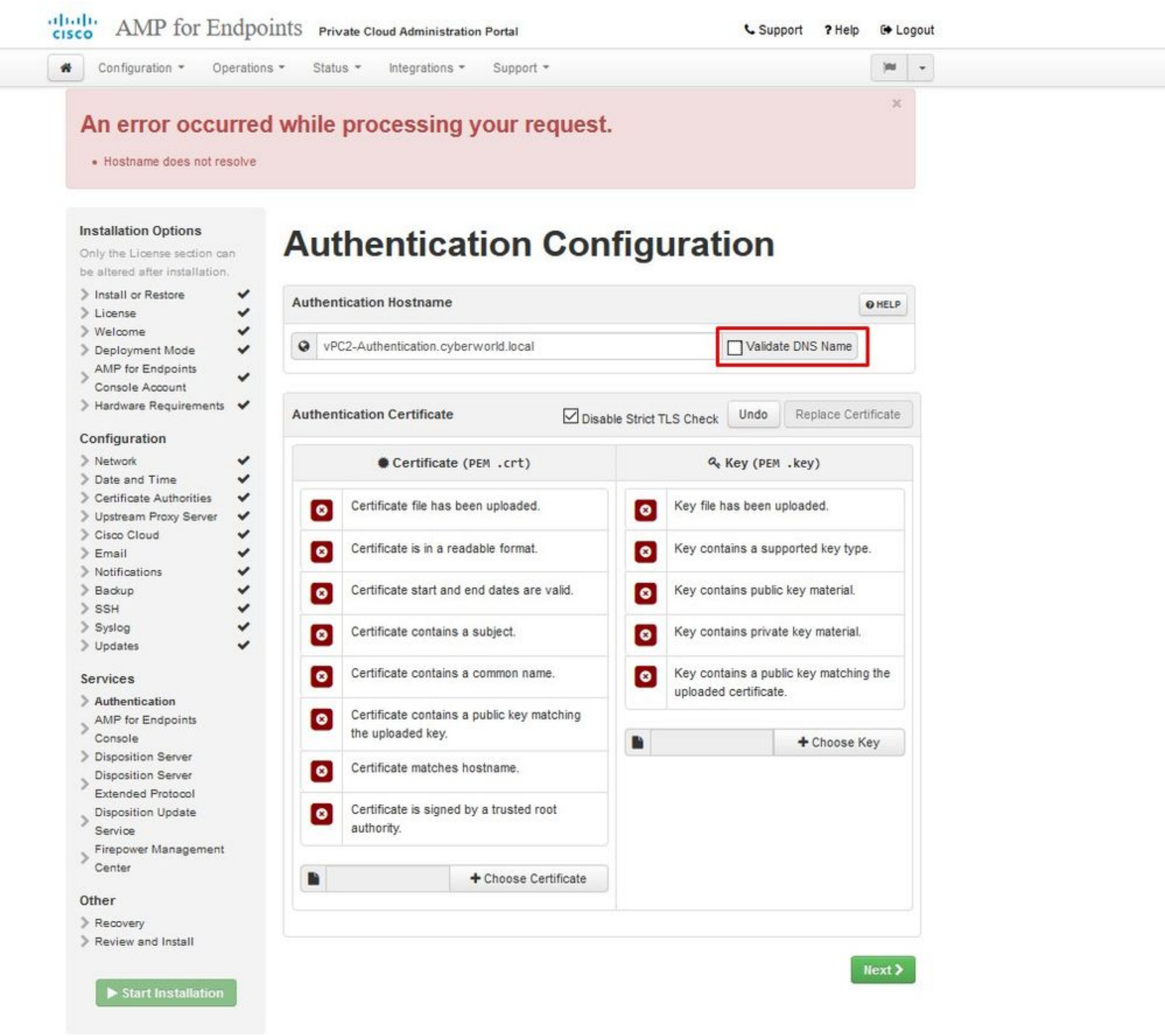
vPC2-Authentication.cyberworld.local.crt

步骤 2：

如果您未选中“Validate DNS Name”，则会出现下一个错误。这里有两个选择。

#1：取消选中Validate DNS复选标记

#2：返回到DNS服务器并配置其余主机记录。



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)	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.	

现在，对其余证书重复相同过程五次。

身份验证

— 身份验证服务可用于未来版本的私有云，以处理用户身份验证。

安全终端控制台

— 控制台是安全终端管理员可访问安全终端控制台的DNS名称，安全终端连接器可接收新策略和更新。

处置服务器

- Disposition Server是安全终端连接器发送和检索云查找信息的DNS名称。

Disposition Server — 扩展协议

— 处置服务器 — 扩展协议是较新的安全终端连接器发送和检索云查找信息的DNS名称。

处置更新服务

— 将Cisco Threat Grid设备链接到私有云设备时，使用处置更新服务。Threat Grid设备用于从安全终端控制台发送要分析的文件，而Threat Grid使用Disposition Update Service在文件分析后更新其处置情况(安全或恶意的)。

Firepower 管理中心

- Firepower管理中心链接可将Cisco Firepower管理中心(FMC)设备链接到私有云设备。这允许您在FMC控制面板中显示安全终端数据。有关FMC与安全终端集成的详细信息，请参阅您的FMC文档。

⚠ 注意：一旦设备完成安装，就无法更改主机名。

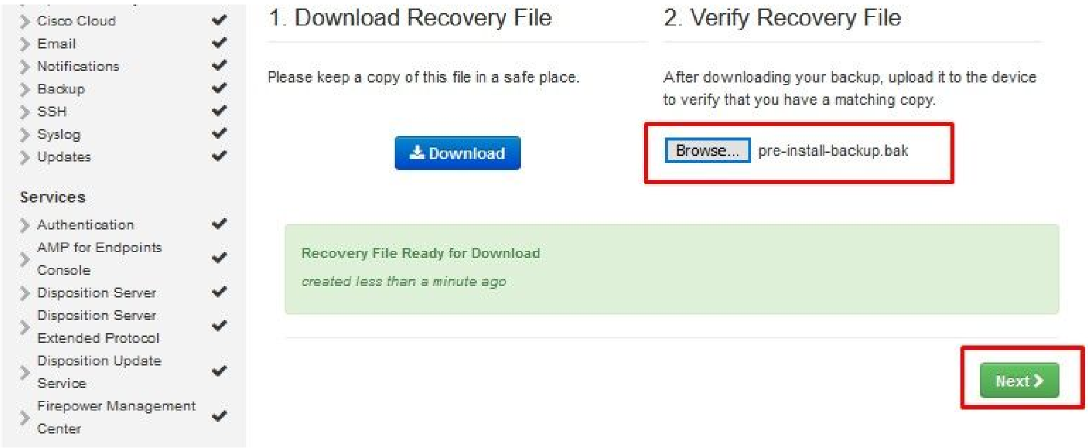
记下所需的主机名。您需要为安全终端私有云创建六个唯一的DNS A记录。每个记录都指向虚拟私有云控制台接口(eth1)的相同IP地址，并且必须由私有云和安全终端解析。

步骤 3：

在下一页下载，然后验证恢复文件。

您将看到“恢复”页面，如图所示。在开始安装之前，您必须下载并验证配置的备份。恢复文件包含所有配置以及服务器密钥。如果丢失恢复文件，则无法恢复配置，必须重新安装所有安全终端连接器。如果没有原始密钥，您必须使用新密钥重新配置整个私有云基础设施。恢复文件包含与opadmin门户相关的所有配置。备份文件包含恢复文件的内容以及任何控制面板门户数据（如事件、连接器历史记录等）。如果您希望只恢复opadmin而不恢复事件数据及所有数据，则可以使用恢复文件。如果从备份文件恢复，则会恢复opadmin和控制面板门户数据。

选择on Download以将备份保存到本地计算机。下载文件后，选择Choose File上传备份文件并验证其未损坏。选择Next以验证文件并继续。



1. Download Recovery File

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

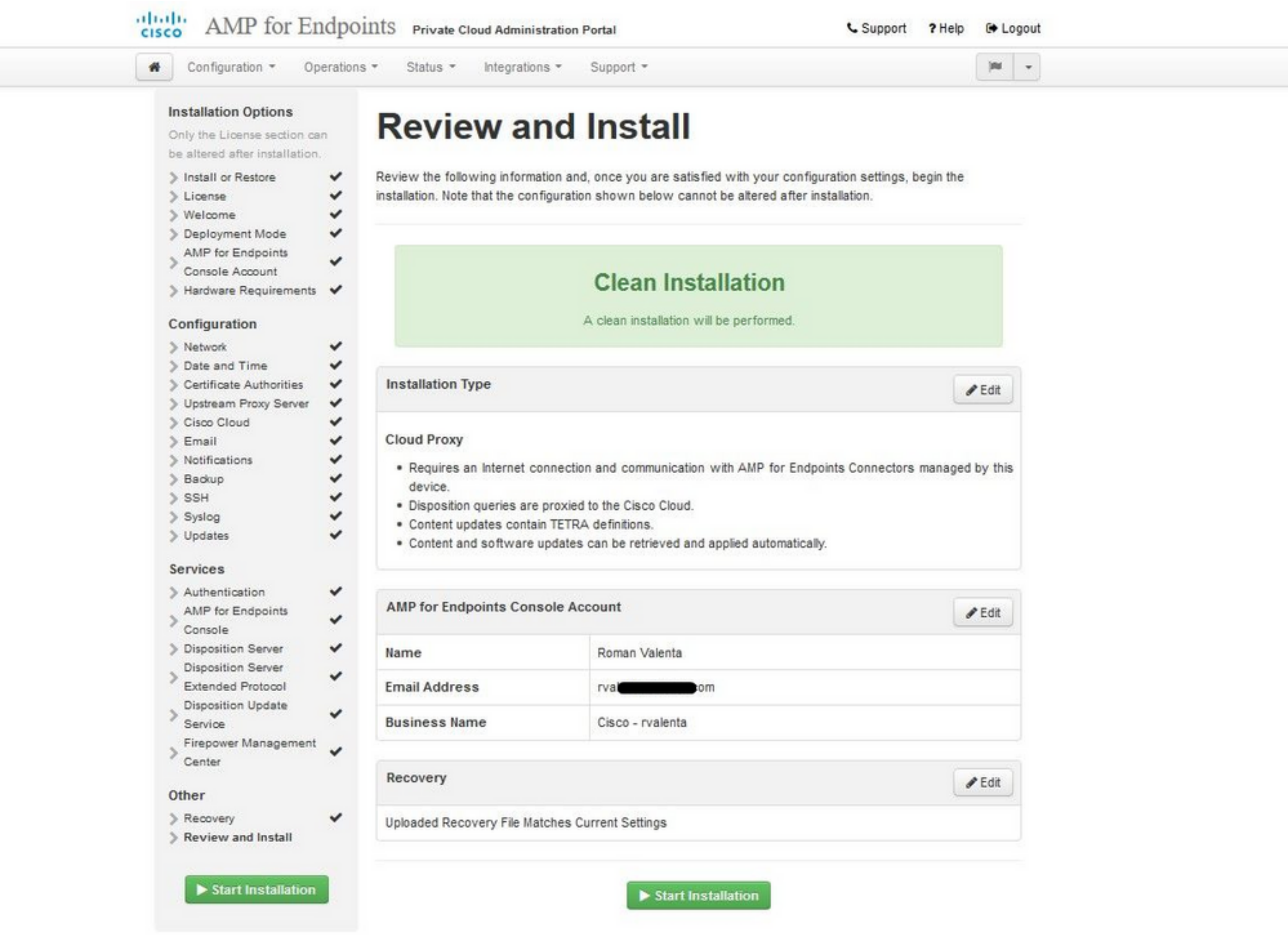
2. Verify Recovery File

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

pre-install-backup.bak

Recovery File Ready for Download

created less than a minute ago


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 ✓
- 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

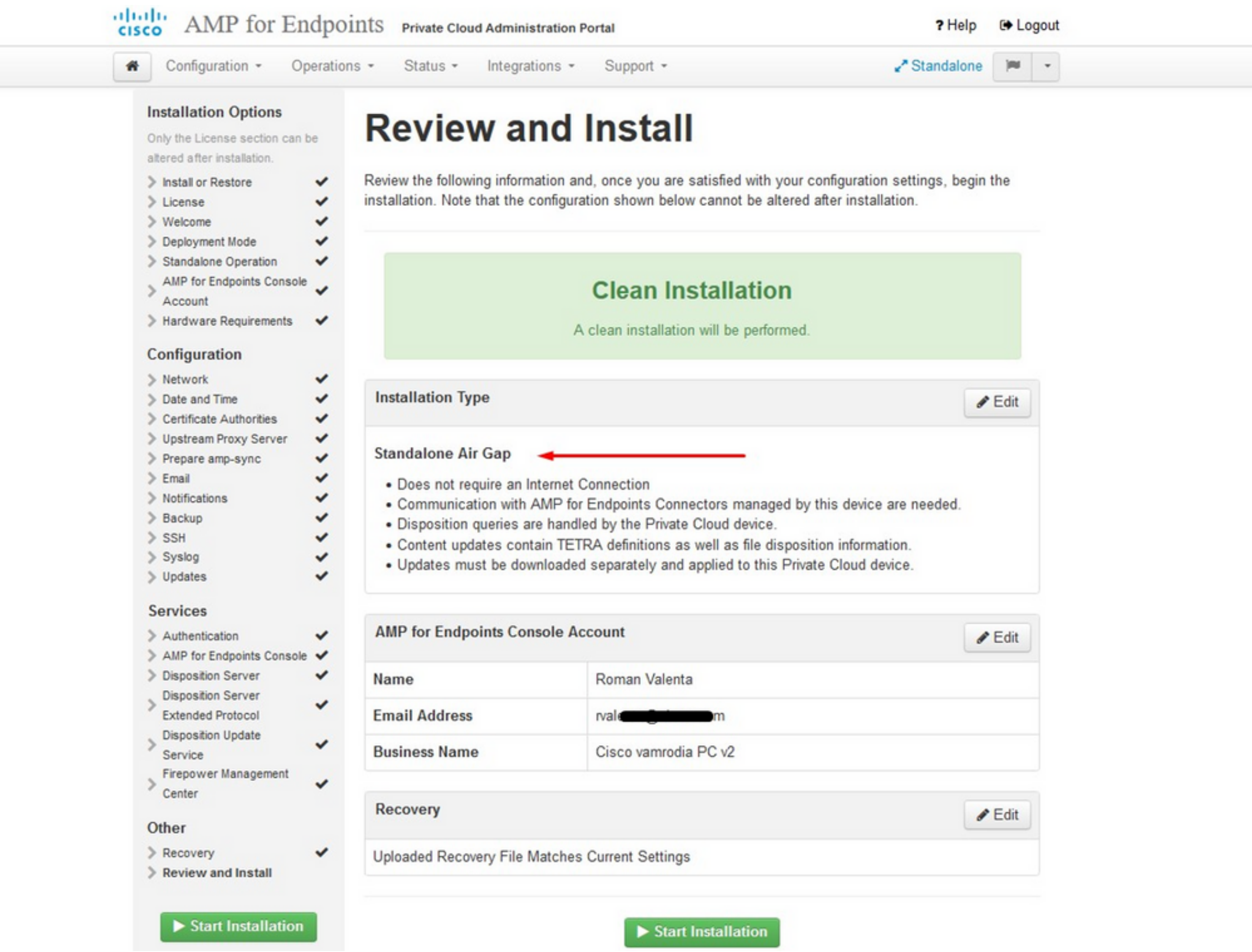
Name	Roman Valenta
Email Address	rva[redacted]om
Business Name	Cisco - rvalenta

Recovery Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

︾︾ AIRGAP ONLY ︾︾



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

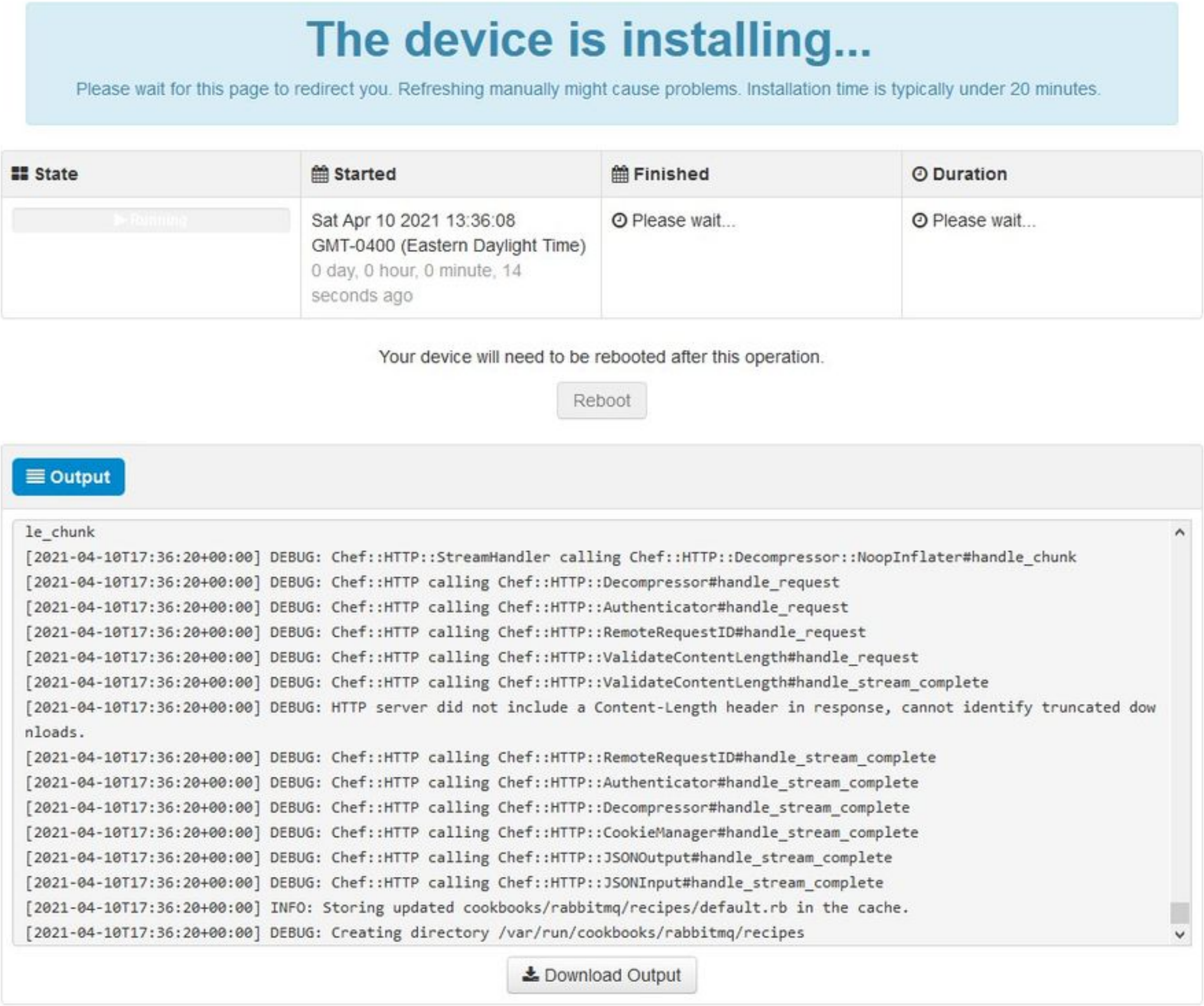
Uploaded Recovery File Matches Current Settings

▶ Start Installation

仅︽︽AIRGAP︽︽

您会看到类似输入内容......

⚠ 注意：当您位于此页面时，不会刷新，因为它可能会导致问题。



The device is installing...

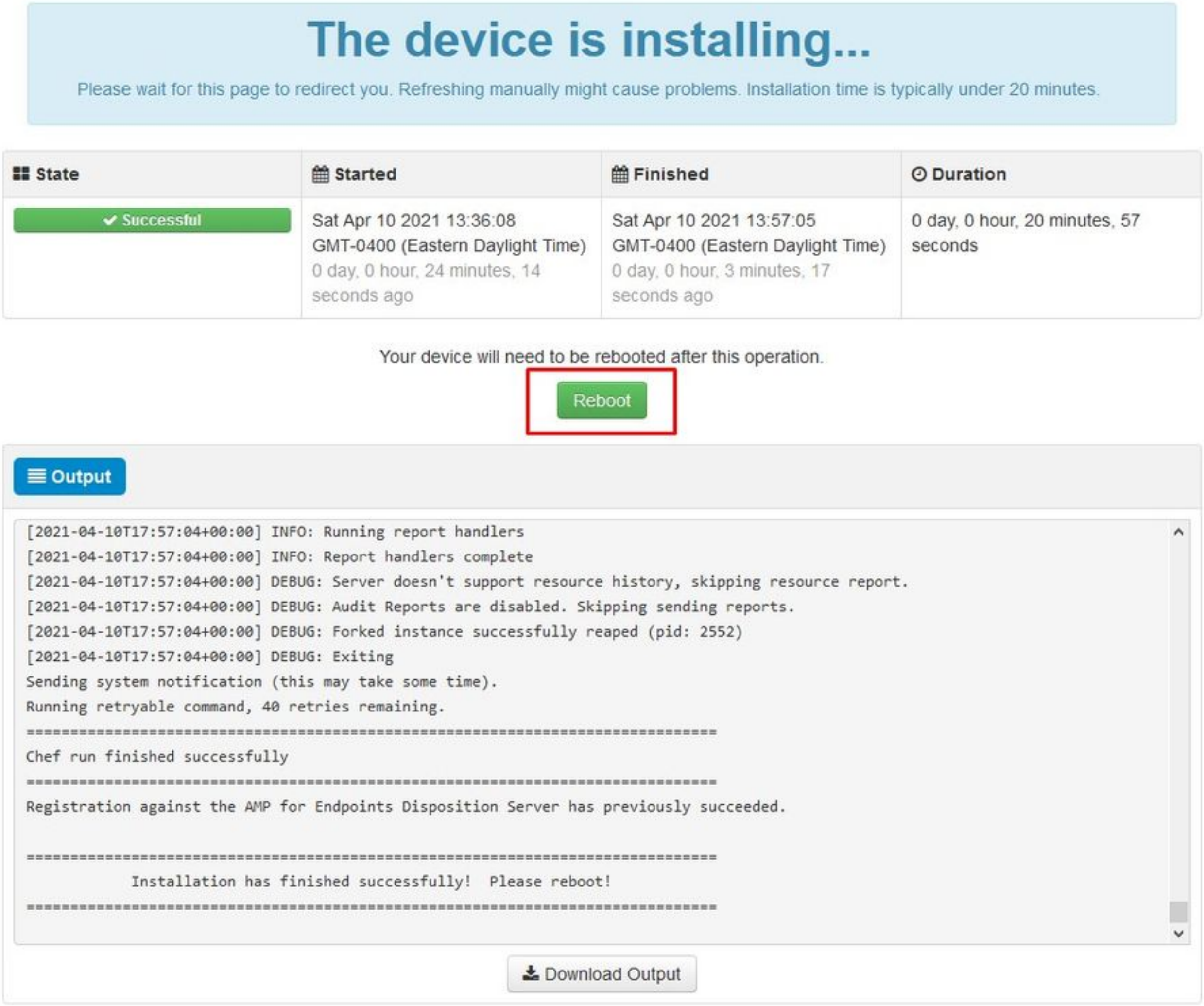
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

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
```

安装完成后，点击reboot按钮



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.

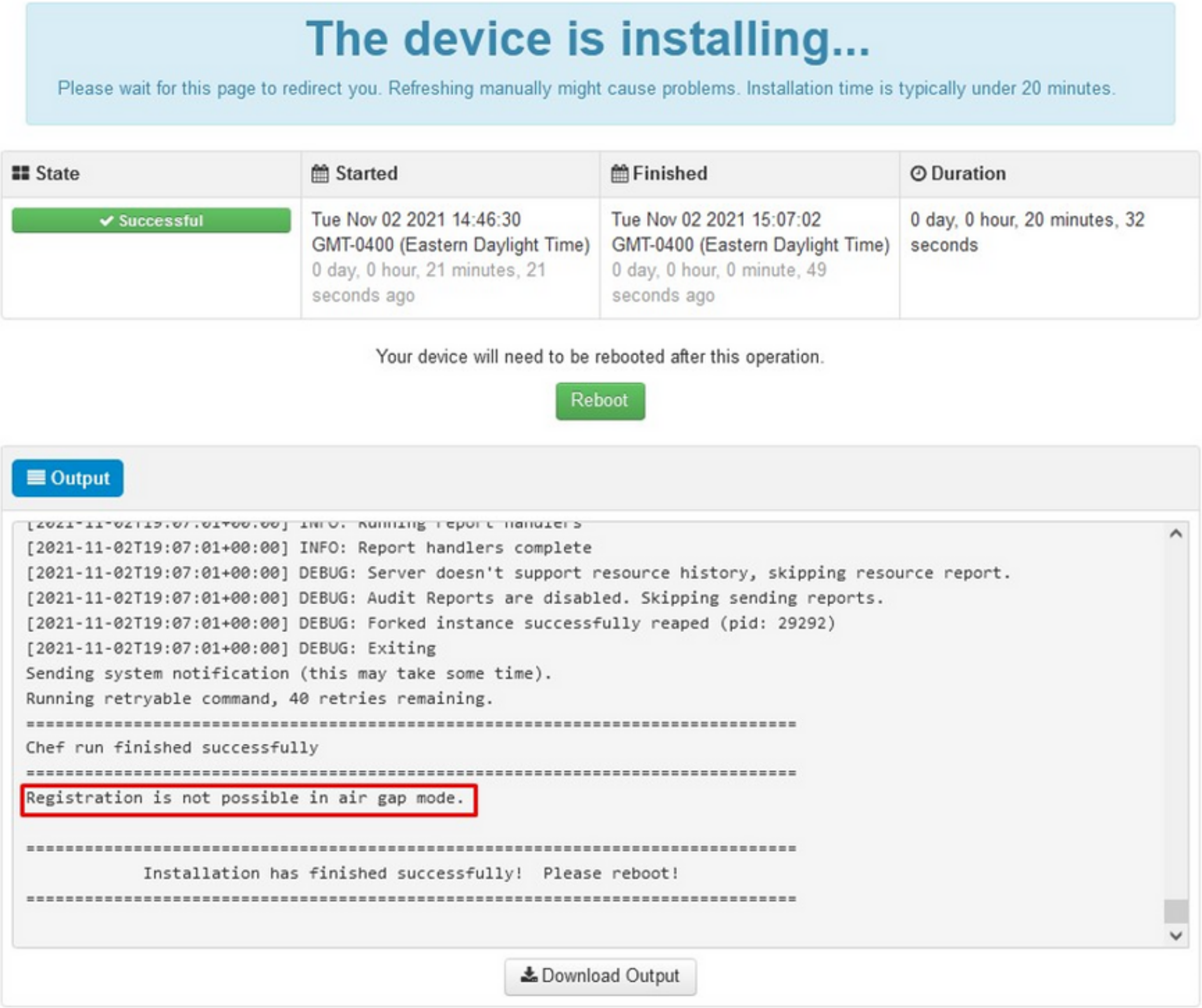
Reboot

Output

```
[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!
================================================================================
```

Download Output

︾ ︾ 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

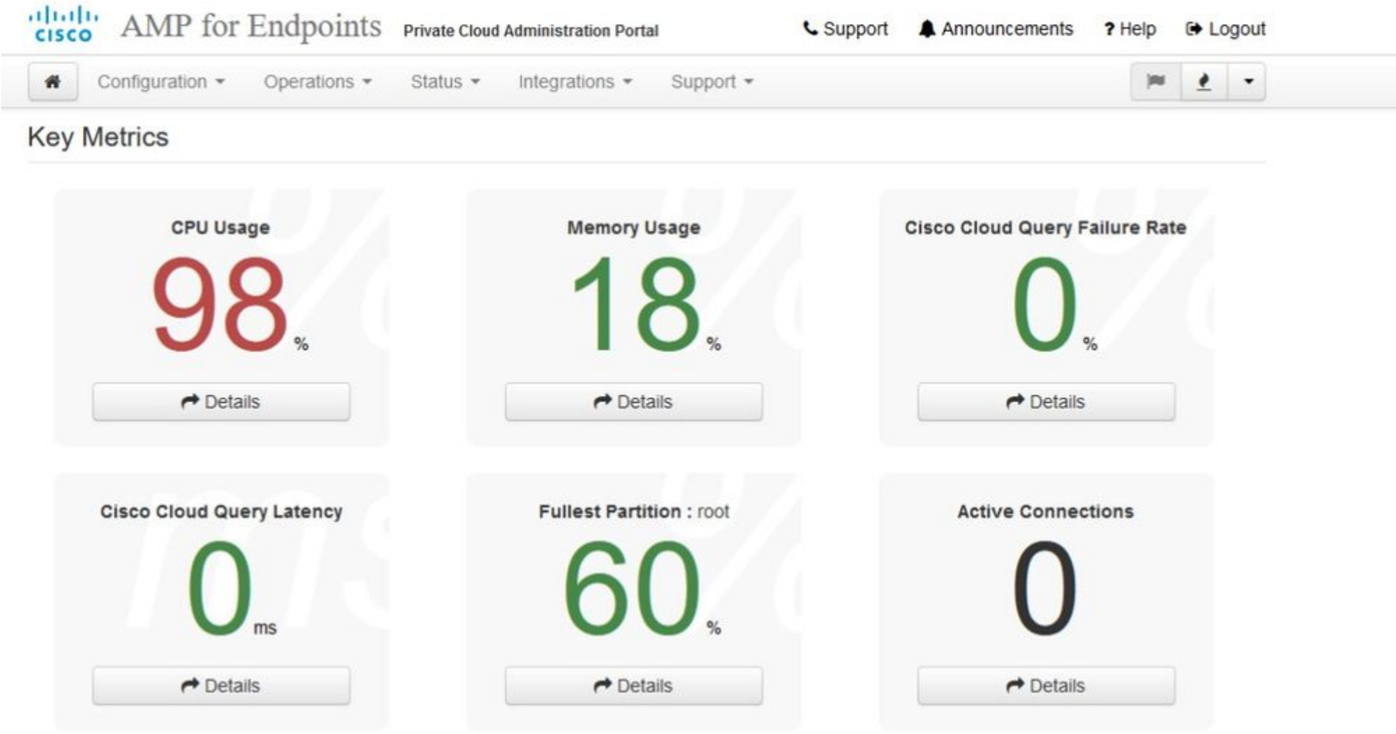
Your device will need to be rebooted after this operation.

```
[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!
===============================================================================
```

仅︽︽AIRGAP︽︽

设备完全启动后，下次使用管理员界面登录时，您会看到此控制面板。 您可能会注意到开始时的CPU使用率较高，但如果您用几分钟时间，CPU使用率会降低。

从此处导航至安全终端控制台。点击标志右边看上去像火的小图标。



Key Metrics

CPU Usage 98 %

Memory Usage 18 %

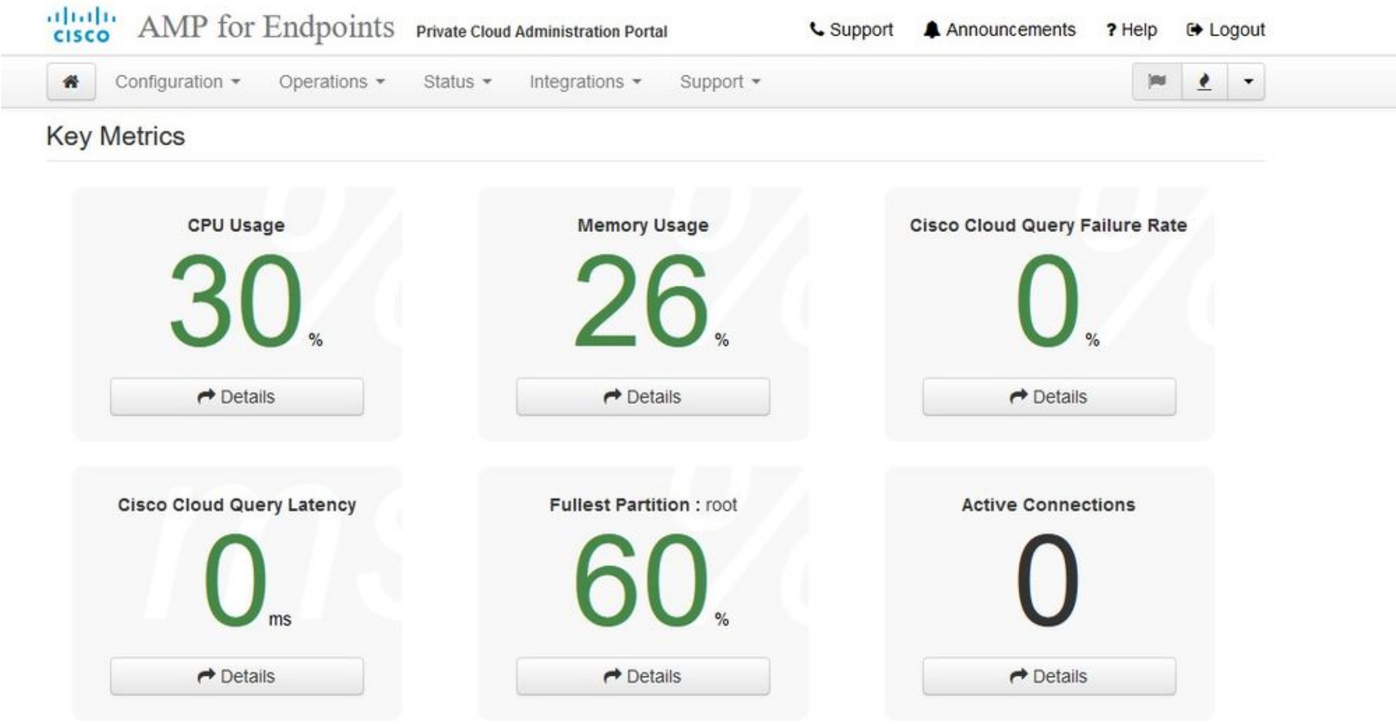
Cisco Cloud Query Failure Rate 0 %

Cisco Cloud Query Latency 0 ms

Fullest Partition : root 60 %

Active Connections 0

几分钟后……



Key Metrics

CPU Usage 30 %

Memory Usage 26 %

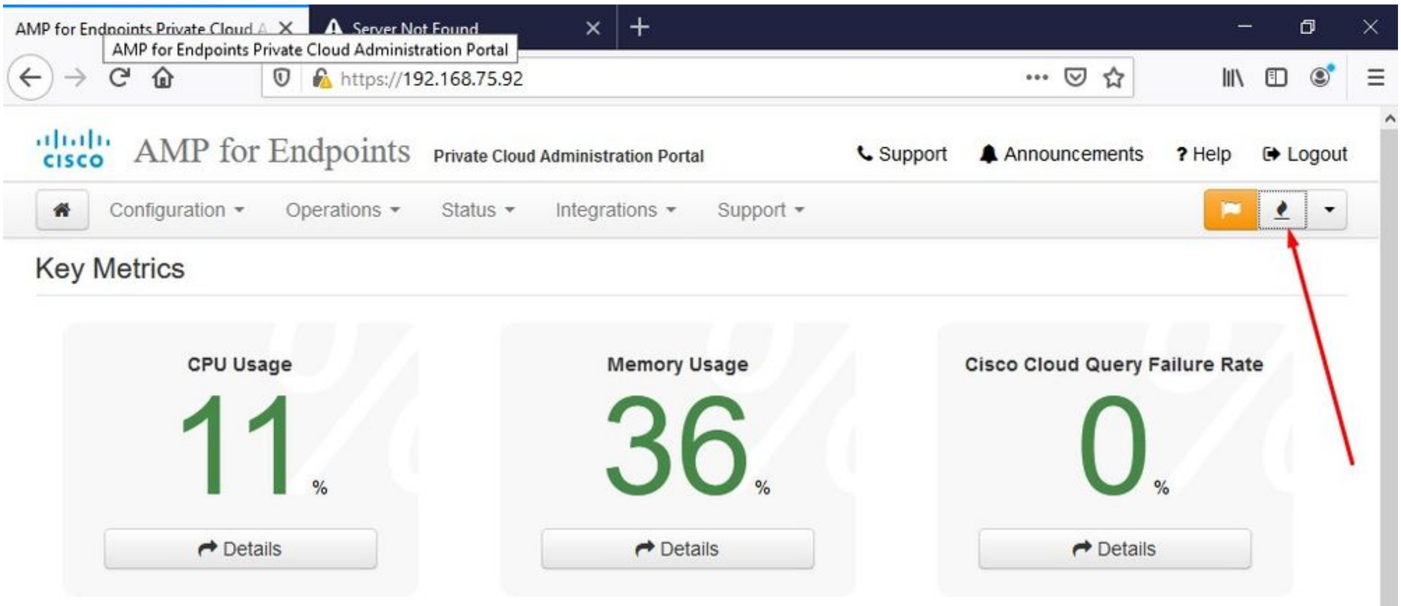
Cisco Cloud Query Failure Rate 0 %

Cisco Cloud Query Latency 0 ms

Fullest Partition : root 60 %

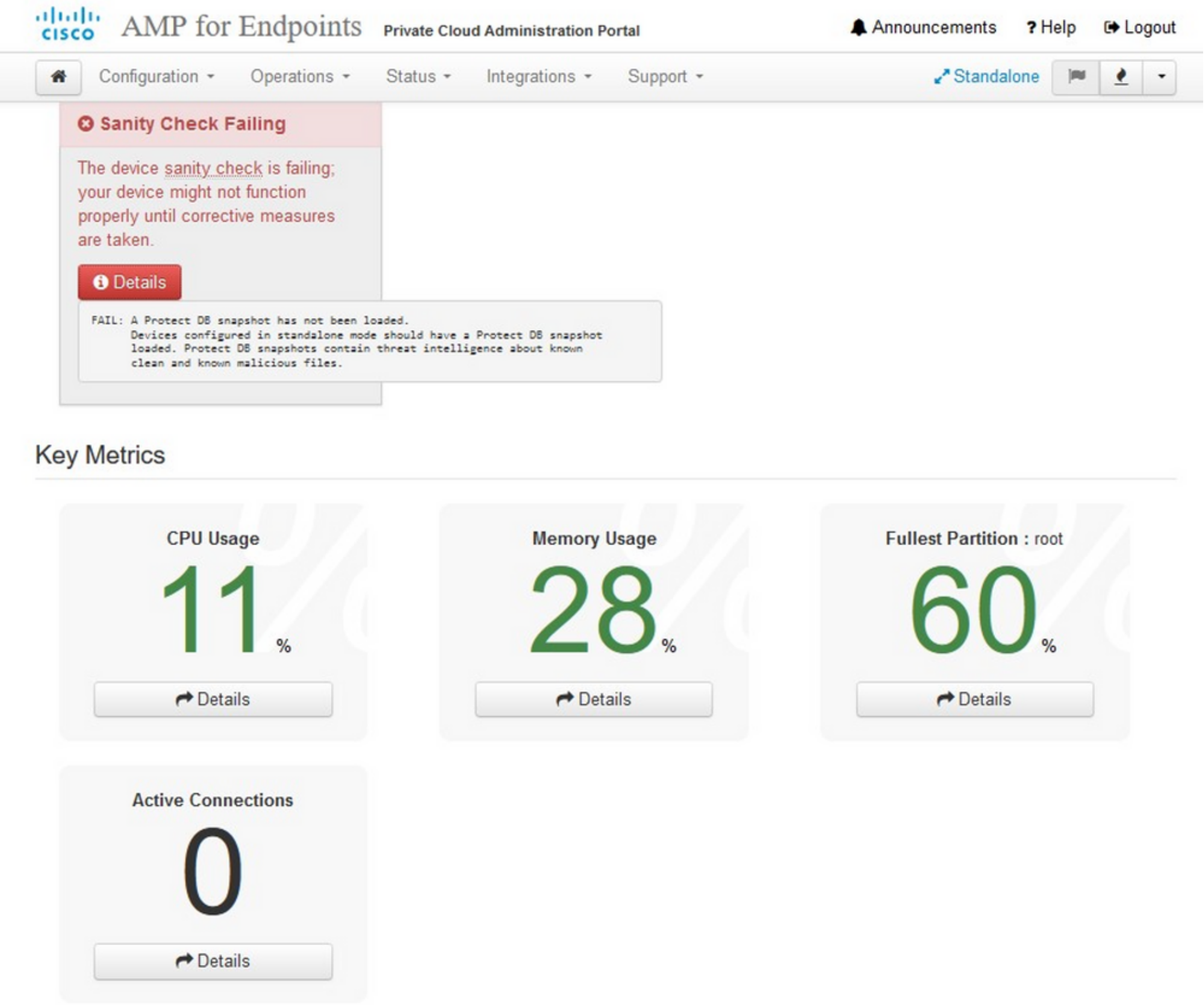
Active Connections 0

从此处导航至安全终端控制台。点击标志右边看上去像火的小图标。



︾︾ AIRGAP ONLY ︾︾

如您所见，由于DB Protect Snapshot（DB保护快照），以及客户端定义、DFC和Tetra，我们未通过健全性检查。这必须通过下载的ISO文件来完成，该文件之前通过amp-sync准备并上传到VM或存储在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.
```

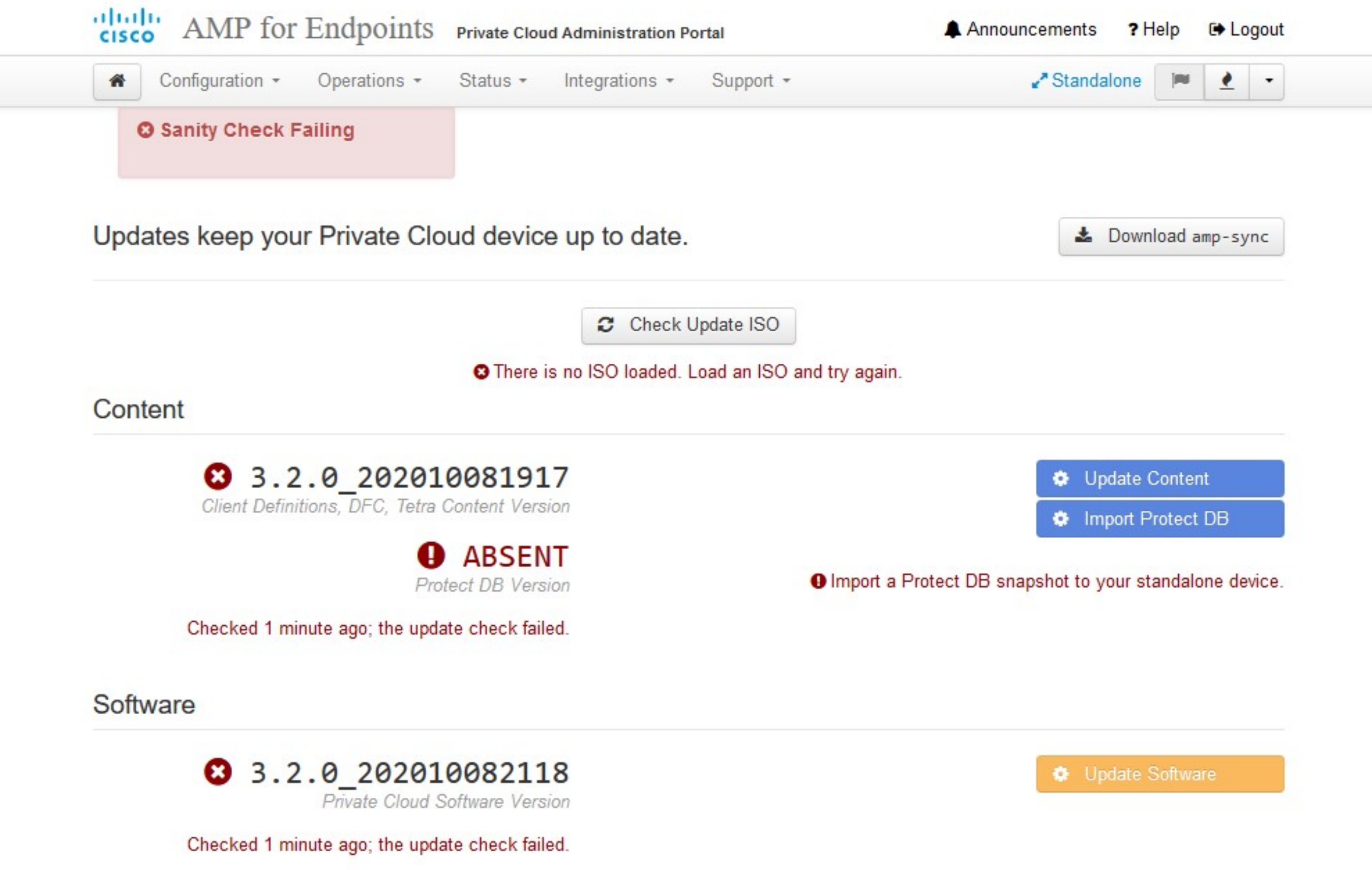
Key Metrics

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

Import a Protect DB snapshot to your standalone device.

Checked 1 minute ago; the update check failed.

Software

3.2.0_202010082118
Private Cloud Software Version

Checked 1 minute ago; the update check failed.

AirGap更新软件包

为了接收Protect DB，我们必须第一次使用此命令

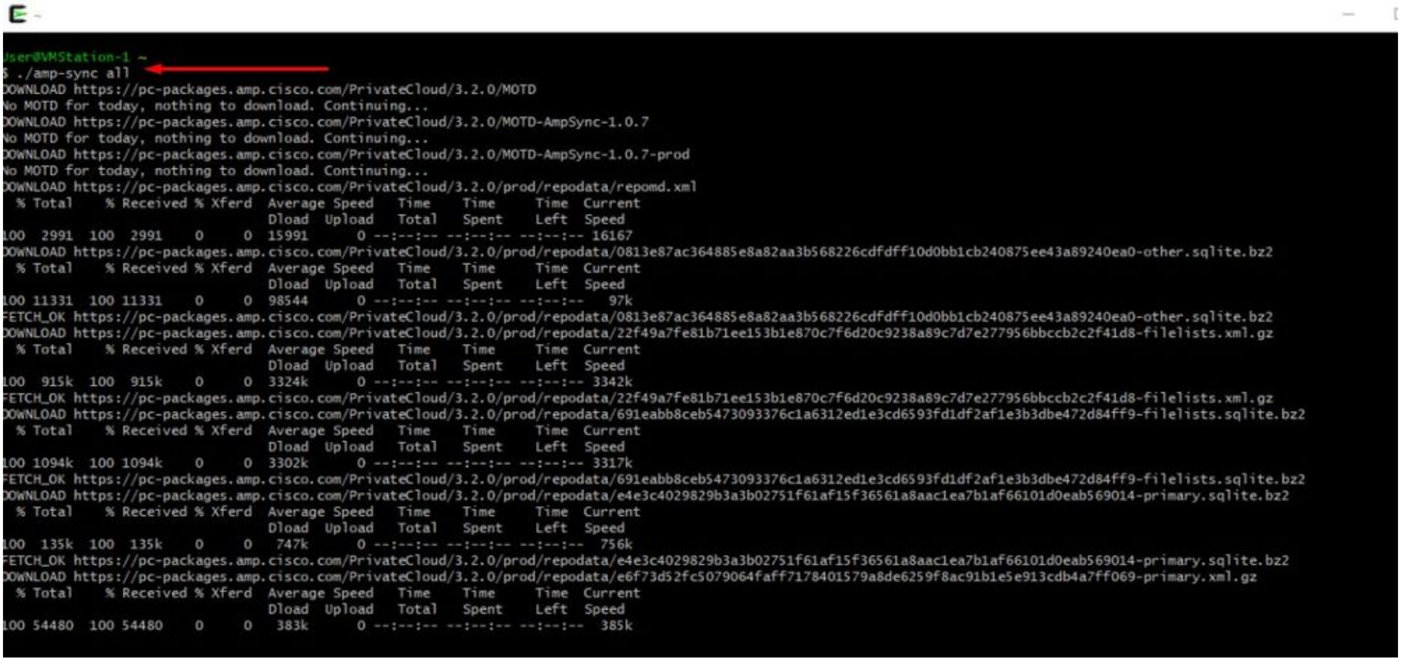
```
./amp-sync all
```

注：请通过此命令下载所有软件包，然后进行验证，耗时可能超过24小时。取决于速度和链路质量。对于使用1Gig光纤的情况，最终需要近25小时才能完成。部分原因还在于此下载直接从AWS进行，因此被限制。 最后，请注意此下载量相当大。就我而言，下载的文件是323GB。

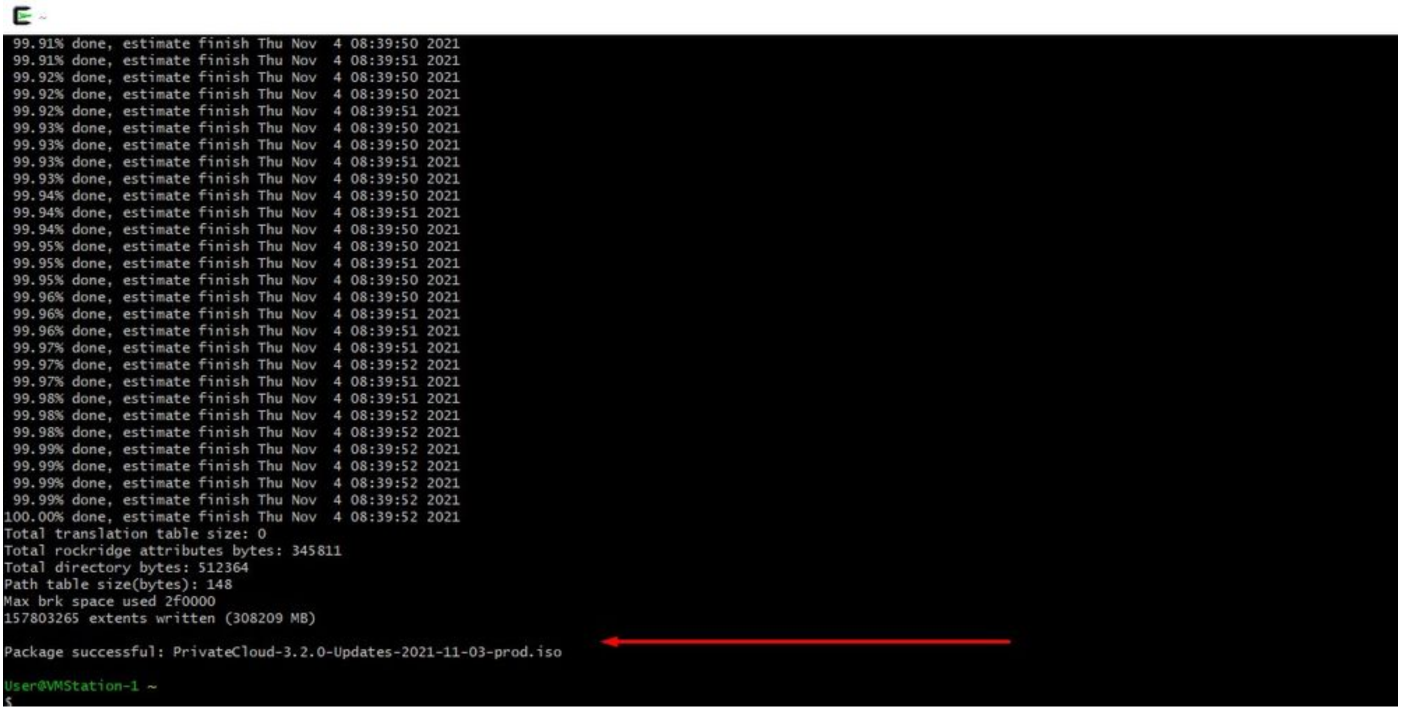
在本示例中，我们使用CygWin64

1.下载并安装x64版本的Cygwin。
2.运行setup-x86_64.exe并完成安装过程，选择所有默认值。
3.选择下载镜像。
4.选择要安装的软件包：
All -> Net -> curl
所有 — >实用程序 — > genisoimage

All -> Utils -> xmlstarlet
* VPC 3.8.x up - > xorriso

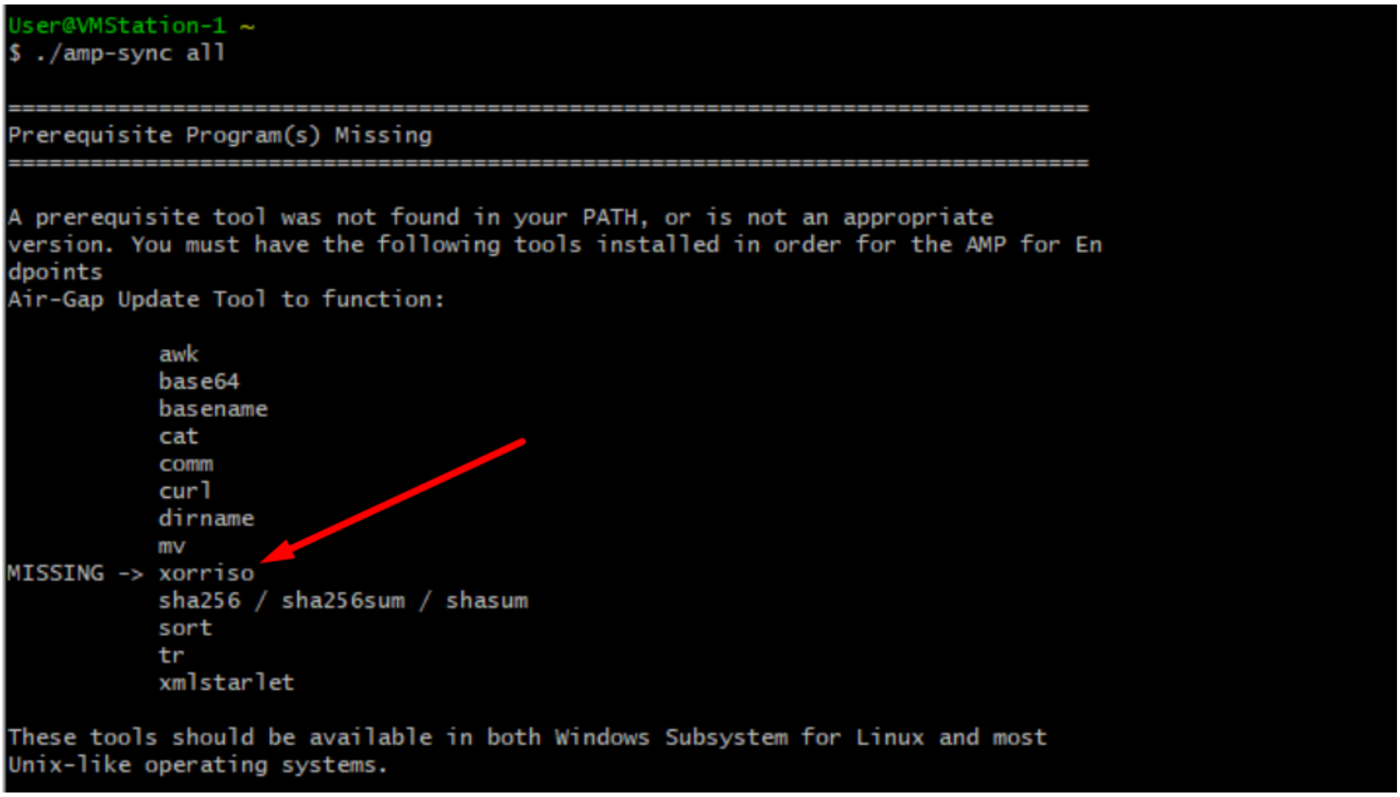


```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD 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
```



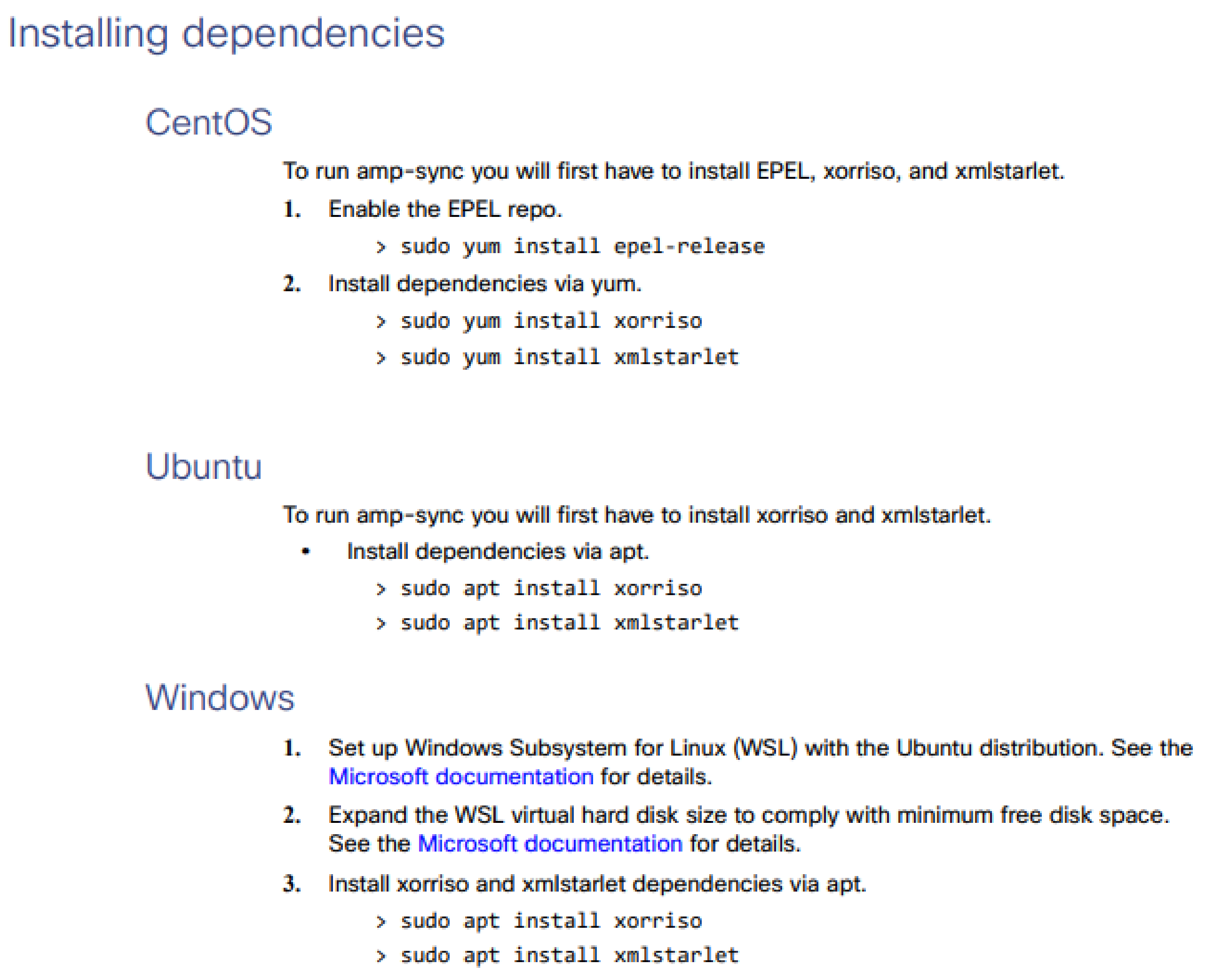
```
 99.91% done, estimate finish Thu Nov  4 08:39:50 2021
 99.91% done, estimate finish Thu Nov  4 08:39:51 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:51 2021
 99.93% done, estimate 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作为主要下载工具，您可能会遇到下面描述的问题。



```
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.
```

发行说明第#58页。您可以看到，xorriso现在为必填项。我们将ISO的格式更改为ISO 9660，该依赖关系是将图像转换为正确的格式，以便完成更新。遗憾的是，CygWin64不在其任何内置存储库中提供xorriso。然而，对于那些仍希望使用CygWin64的客户，有办法克服这个问题。



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.

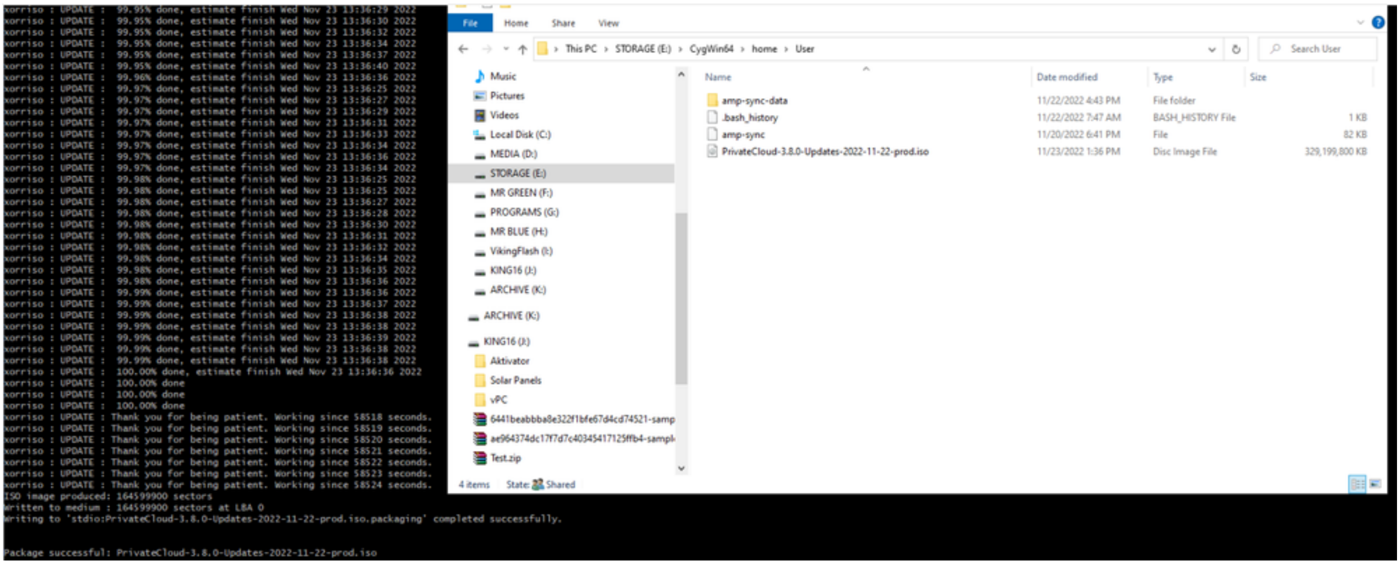
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

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
```

为了能够再次使用CygWin，您必须从GitHub存储库手动下载xorriso。 打开浏览器并键入<Latest xorriso.exe 1.5.2 pre-build for Windows>，它应该作为名为<PeyTy/xorriso-exe-for-windows - GitHub>的第一个链接导航到该GitHub页面，然后下载<xorriso-exe-for-windows-master.zip>文件到您找到的其他几个名为<xorriso.exe>的文件中，复制此文件，并将其粘贴到您的本地Cyg的<CygWin64\bin路径Win安装。请尝试再次运行<amp-sync>命令。您不应再看到错误消息并下载开始和完成，如图所示。



```
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
```

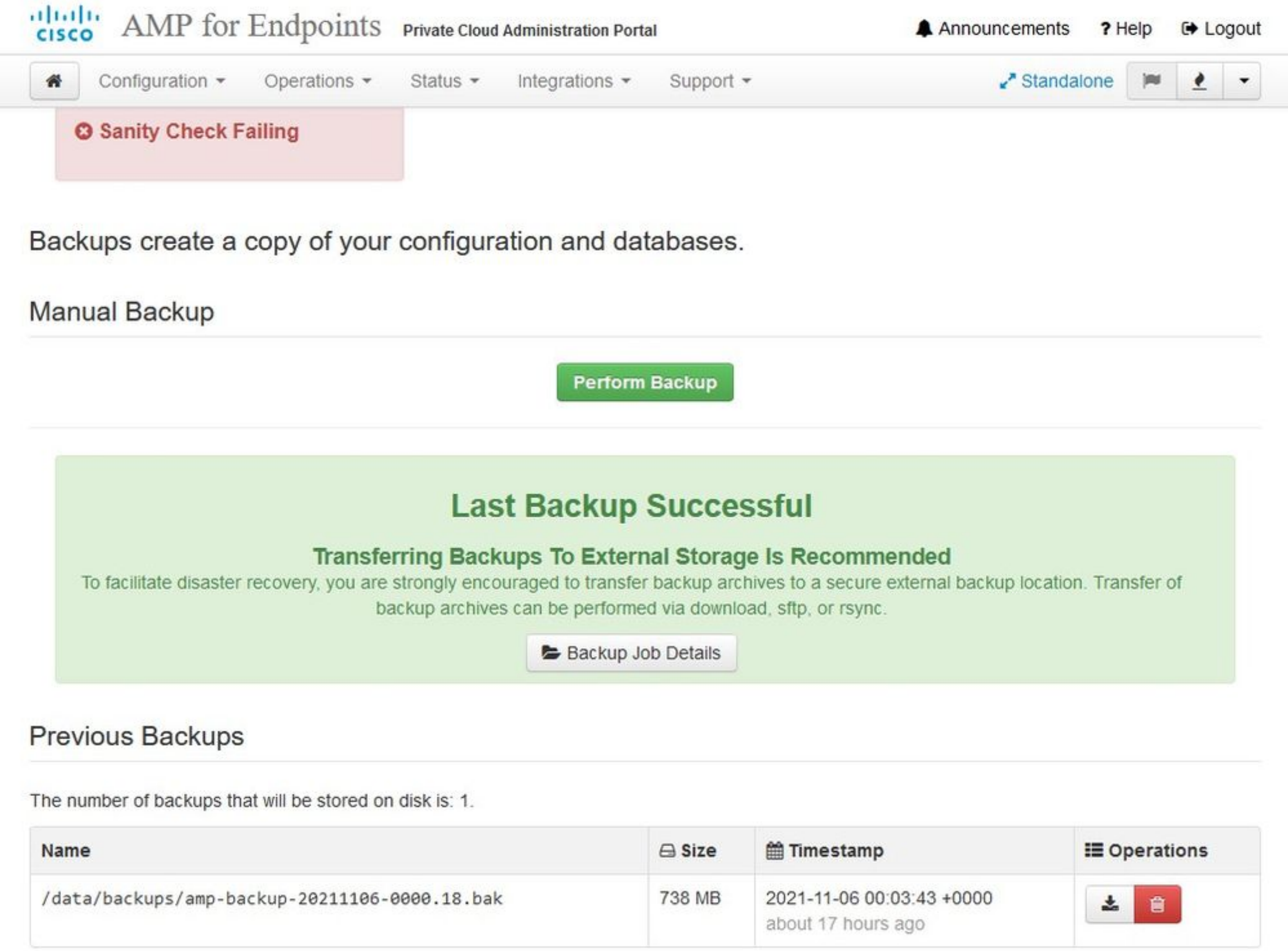
Name	Date modified	Type	Size
amp-sync-data	11/22/2022 4:43 PM	File folder	
.bash_history	11/22/2022 7:47 AM	BASH_HISTORY File	1 KB
amp-sync	11/20/2022 6:41 PM	File	82 KB
PrivateCloud-3.8.0-Updates-2022-11-22-prod.iso	11/23/2022 1:36 PM	Disc Image File	329,199,800 KB

在Airgap模式下执行当前(在本例中)3.2.0 VPC的备份。

您可以从CLI使用此命令

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

也可以导航到操作>备份，如映像中所示，并在那里执行备份。



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.

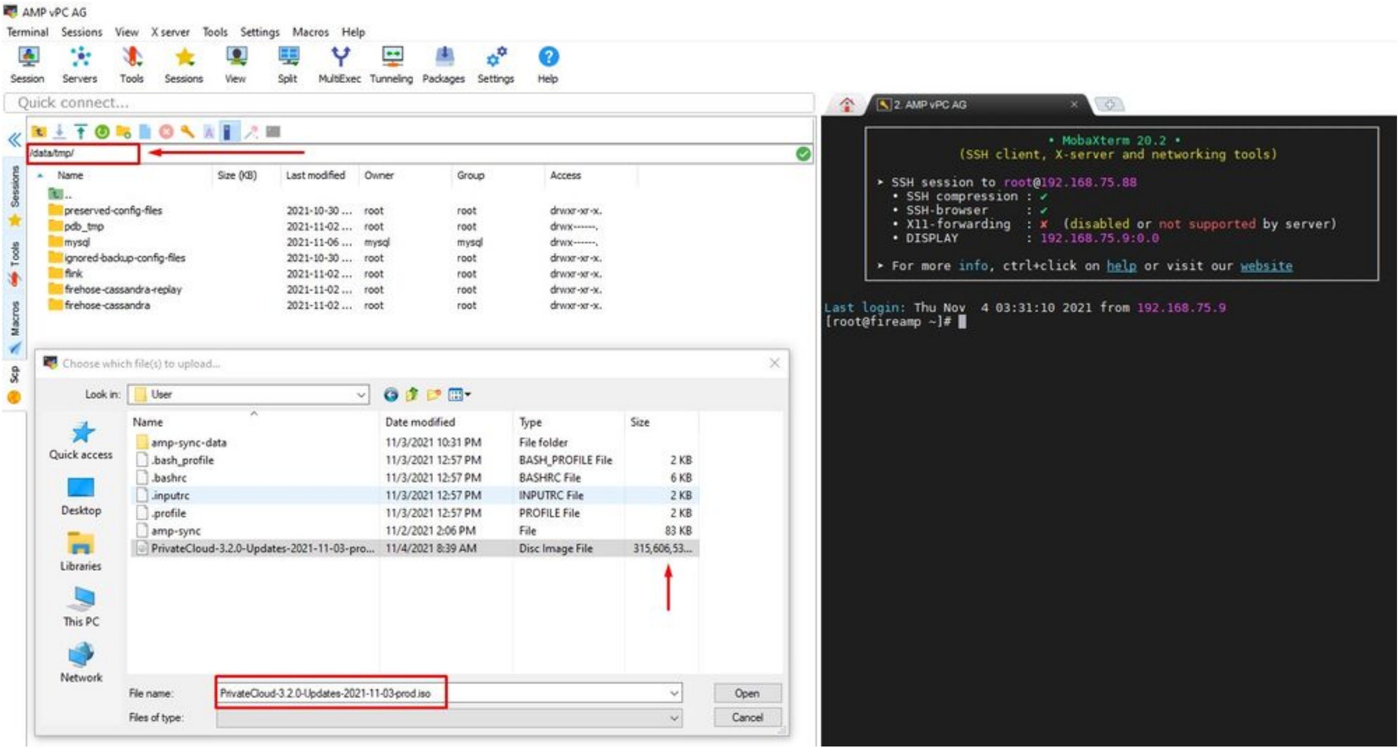
Previous Backups

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	

将通过amp-sync生成的最新ISO传输到VPC。根据您的速度，这最多也可能需要几个小时。在本例中，传输时间超过16小时

```
/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...
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.

Look in: User

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...

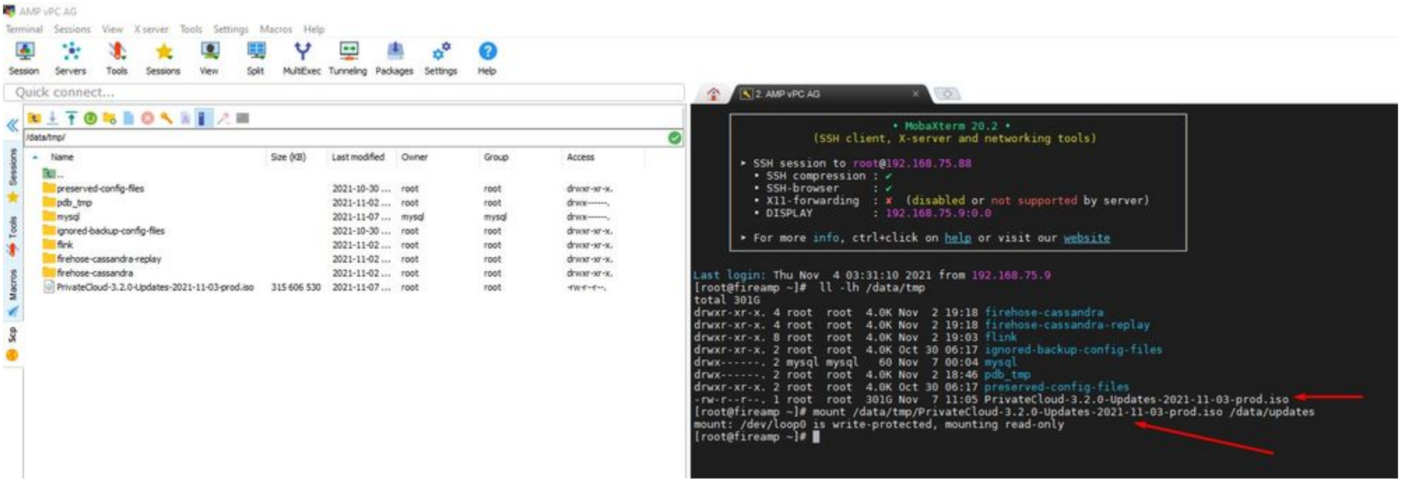
File name: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso

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 ~]#
```

上传完成后，安装ISO

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

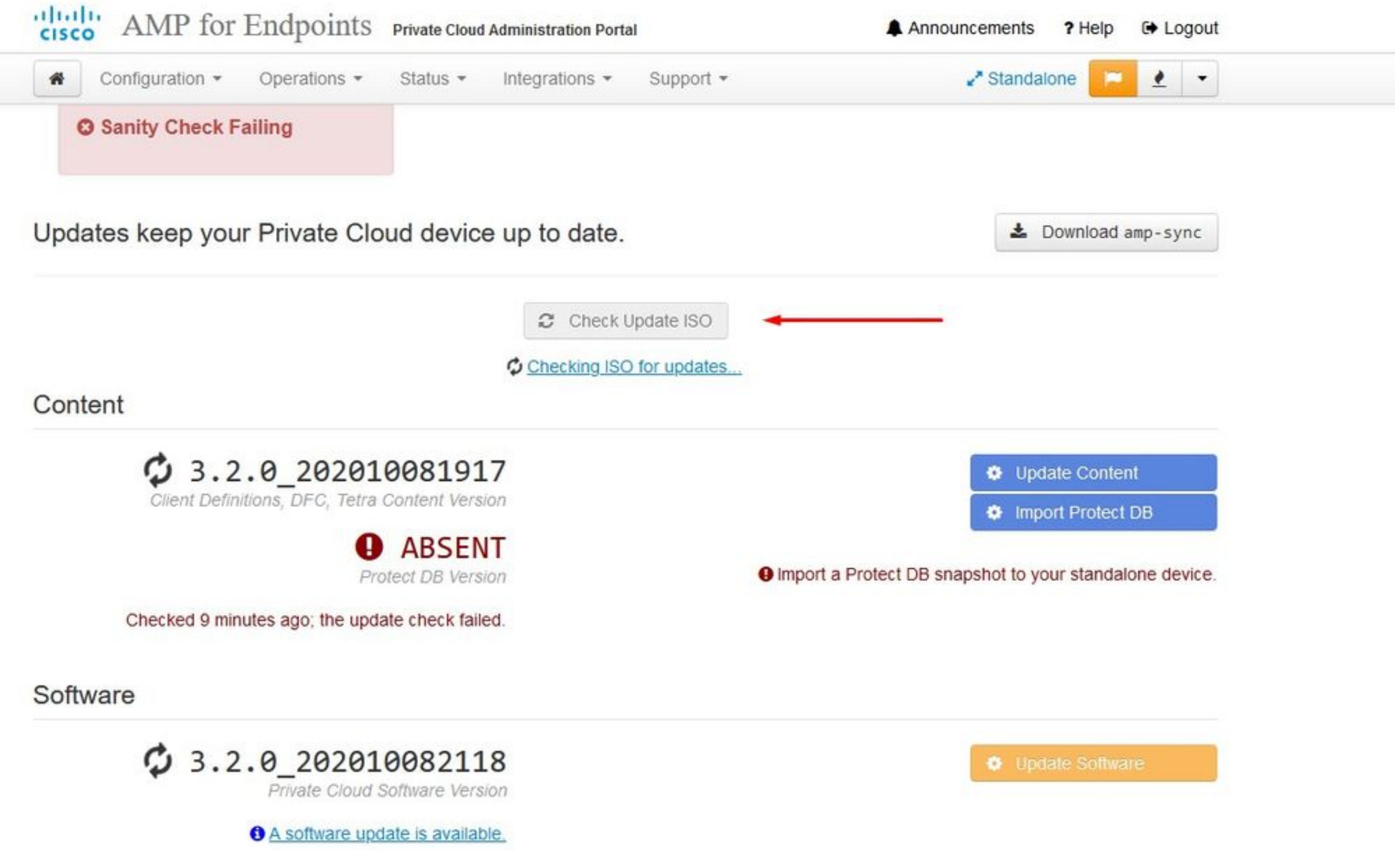

AMP vPC AG
Terminal Sessions View X server Tools Settings Macros Help
Session Servers Tools Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
Sessions Tools Macros Sftp
2. AMP vPC AG

/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 ~]#
```

导航至打开UI以执行更新 操作(Operations)>更新设备(Update Device)>选择检查更新ISO。



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

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.

Update Content

Import Protect DB

Import a Protect DB snapshot to your standalone device.

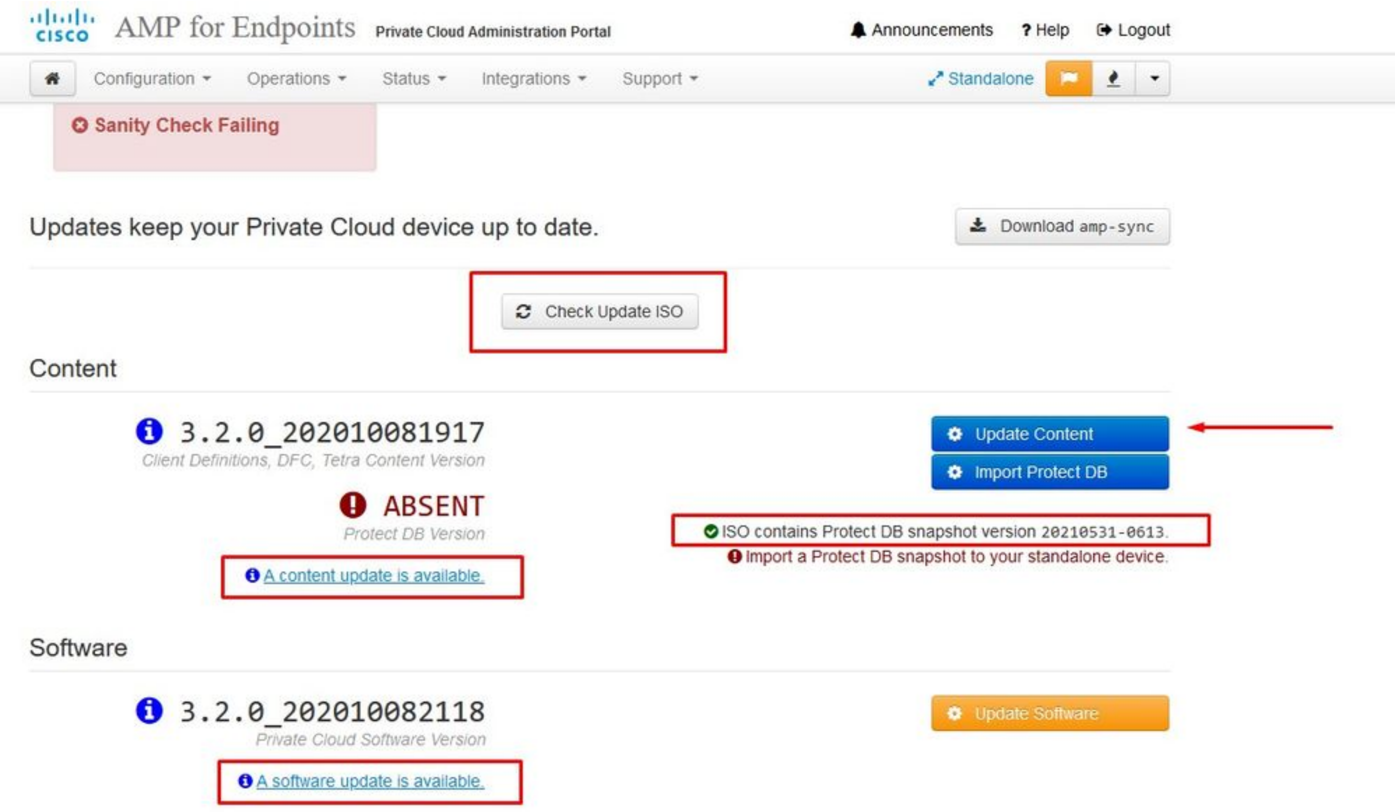
Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

Update Software

在本例中，我首先继续更新内容



AMP for Endpoints Private Cloud Administration Portal

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.

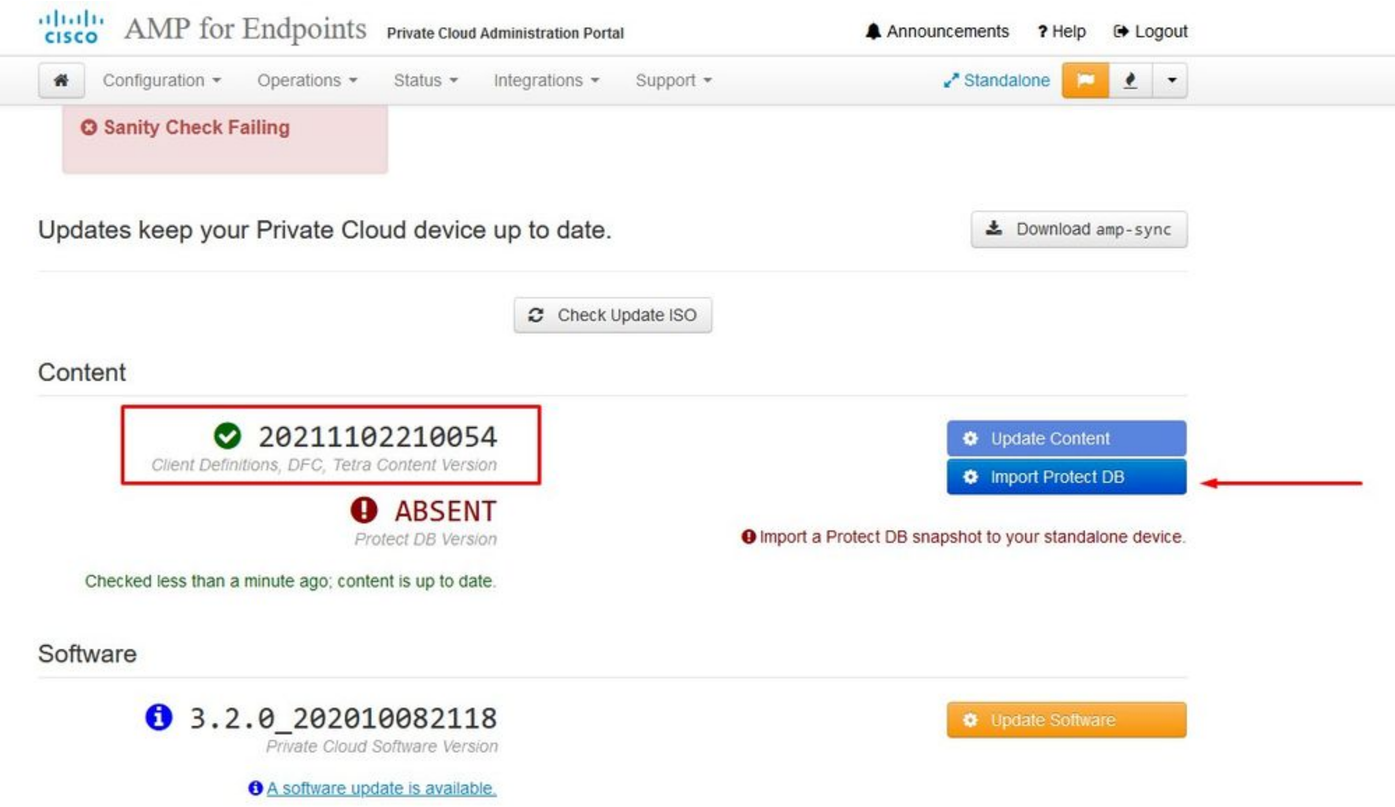
ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

然后选择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.

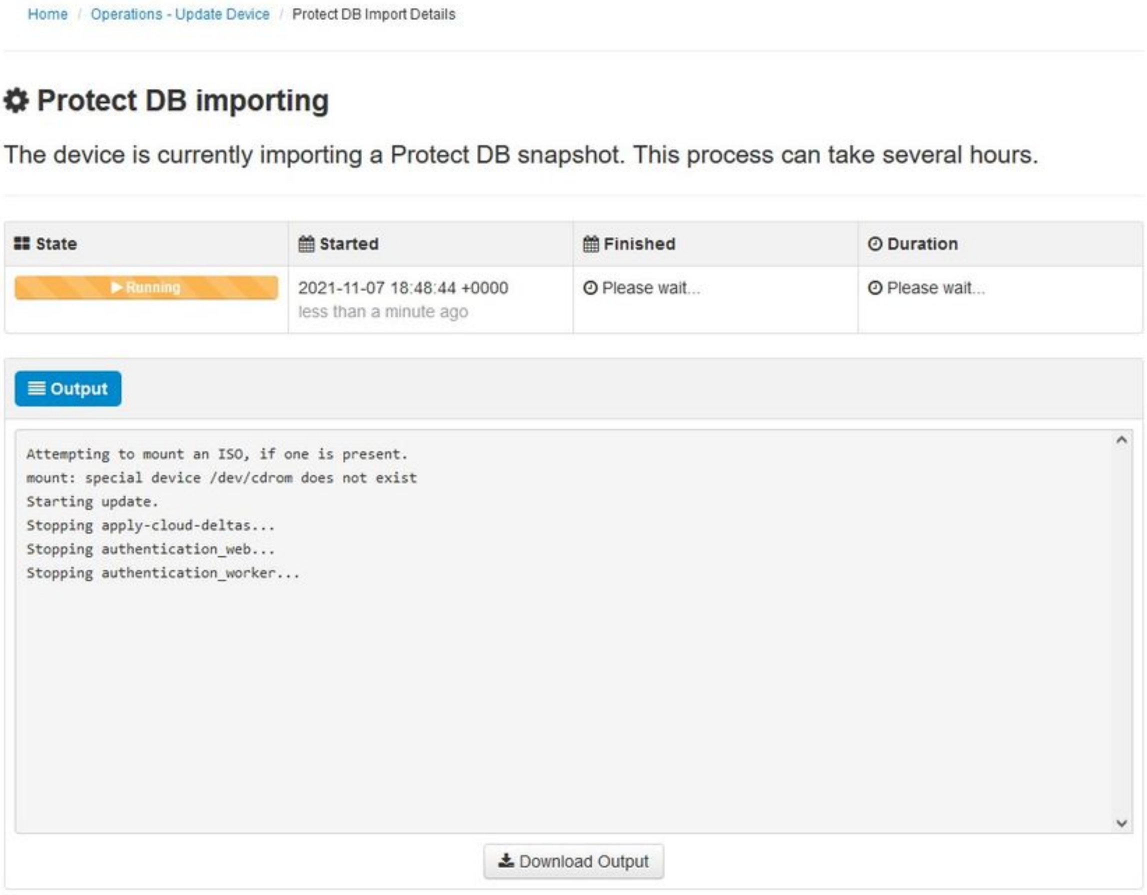
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

A software update is available.

您可以看到这是另一个很长的过程，可能需要很长时间才能完成。

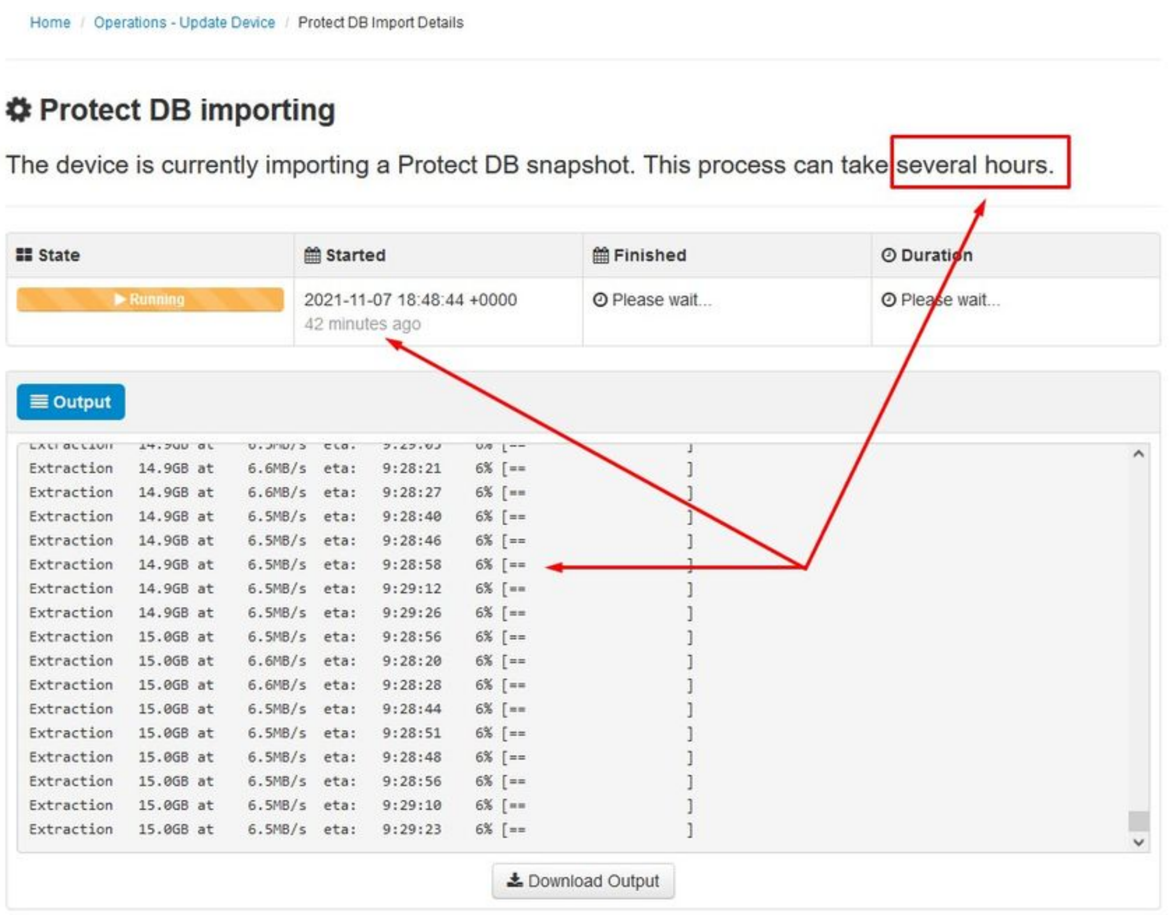

Home / Operations - Update Device / Protect DB Import Details
Output
Download Output

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...
```

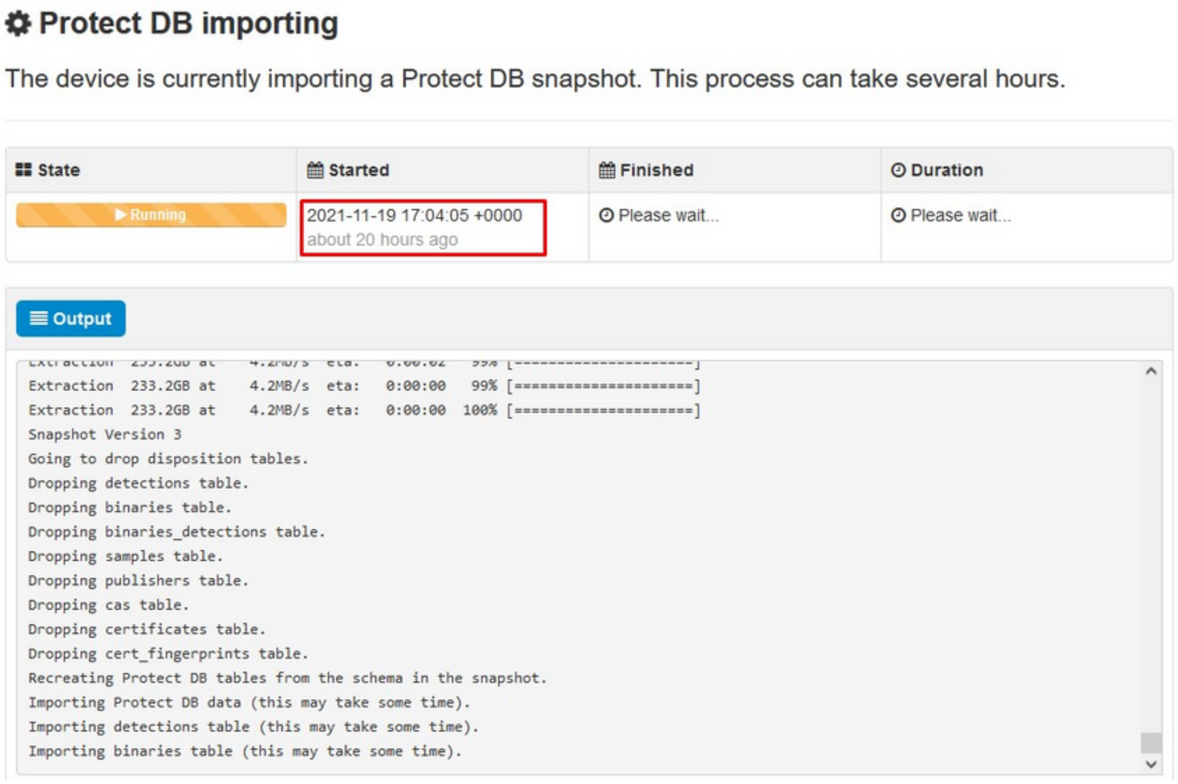

Home / Operations - Update Device / Protect DB Import Details

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   6.6MB/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.

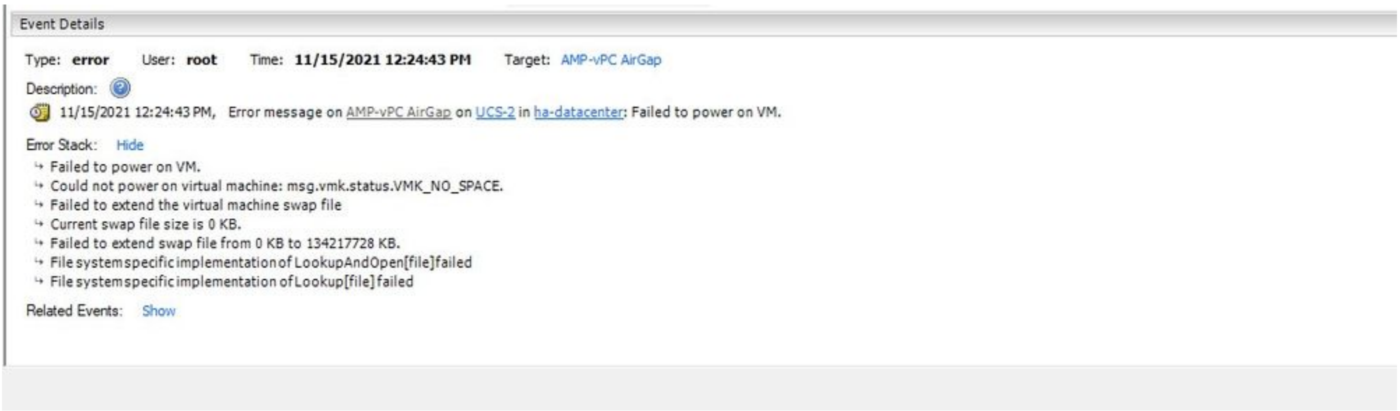
State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...	Please wait...

```
Extraction  233.2GB at   4.2MB/s  eta:  0:00:00   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).
```

问题#1 - Data Store的房间耗尽

在这里，您可以找到两个问题。由于3.5.2之前的vPC无法安装外部NFS存储，因此您必须将更新ISO文件上传到/data/temp目录。就我而言，由于我的Datastore只有1TB，我用尽了房间，VM崩溃了。换句话说，您至少需要2 TB的数据存储空间才能成功部署低于3.5.2版的AirGap VPC

以下映像来自ESXi服务器，它显示当您尝试启动VM时HDD上没有更多可用空间这一错误。通过将128 GB RAM临时切换到64 GB，我可以从此错误中恢复。然后我又能重新开始了。另请注意，如果您将此VM调配为瘦客户端，则瘦客户端部署的缺点是磁盘大小可以增加，但即使您释放一些空间，磁盘大小也不会缩小。换句话说，假设您将300GB文件上传到vPC的目录，然后将其删除。ESXi中的磁盘仍然显示硬盘上的空间减少300GB



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.

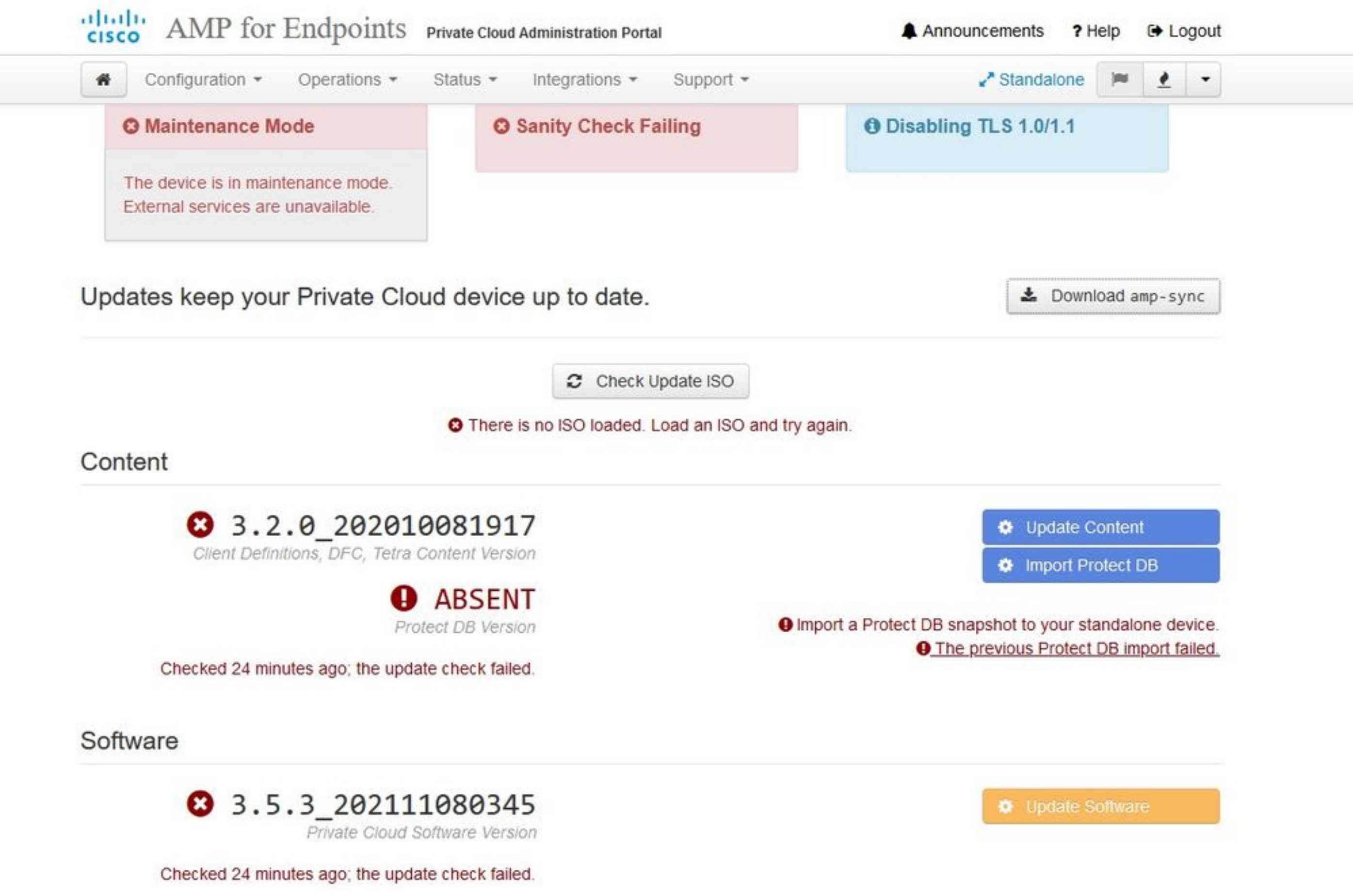
Error Stack: Hide

```
↳ 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

问题#2 — 旧更新

第2个问题是，如果您先运行软件更新，就像我在第2次试运行中执行的操作一样，从3.2.0开始，我最终使用VPC升级到3.5.2，因此，由于3.2.0版本因我不再使用原始3.2.0版本而变得无效，我不得不下载全新的ISO更新文件。


AMP for Endpoints Private Cloud Administration Portal
Announcements ? Help Logout
Configuration Operations Status Integrations Support
Standalone
Download amp-sync
Check Update ISO
Update Content
Import Protect DB
Update Software

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.

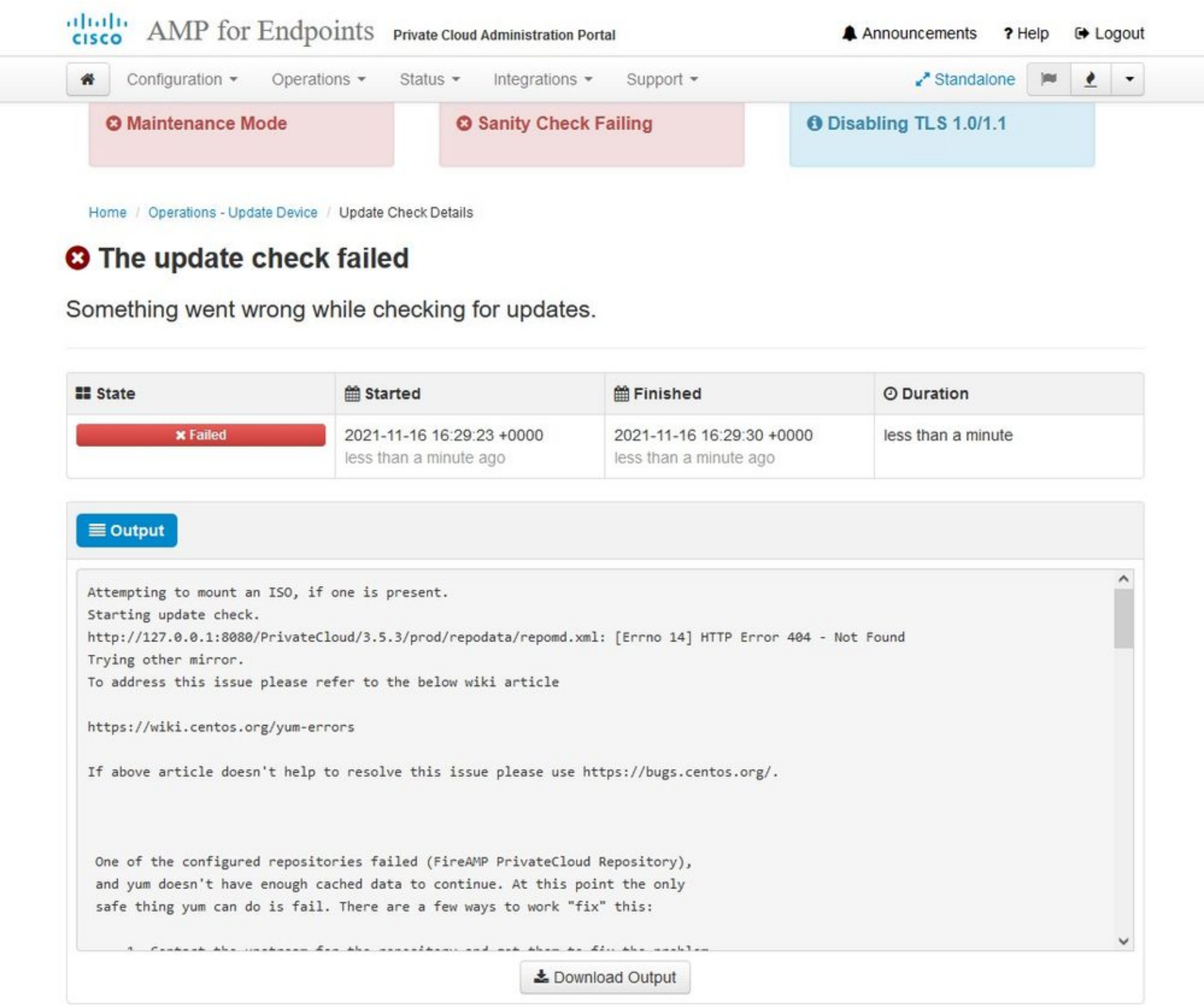
Import a Protect DB snapshot to your standalone device.
The previous Protect DB import failed.

Software

3.5.3_202111080345
Private Cloud Software Version

Checked 24 minutes ago; the update check failed.

如果您尝试再次安装ISO更新文件，则会看到此错误。



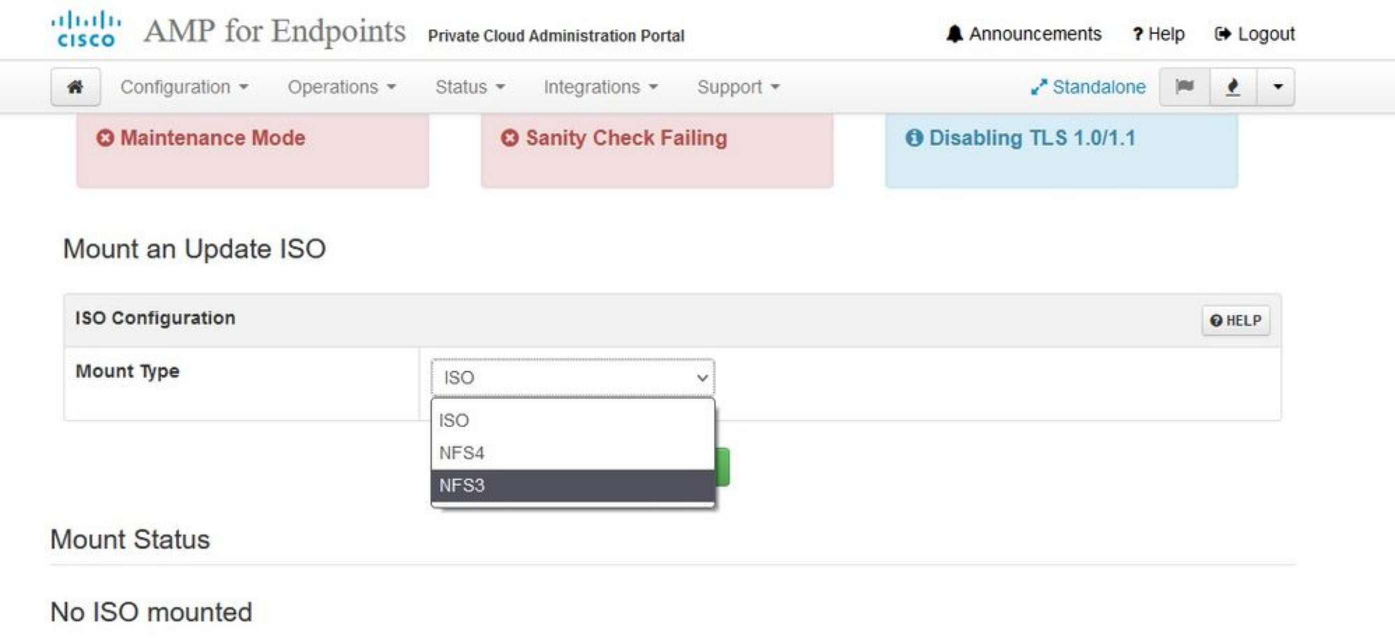
The update check failed

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.
```

此图片显示了如何将更新映像装载到VPC的备用方法。在3.5.x版本中，您可以使用远程位置（如NFS存储）与VPC共享更新文件。



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

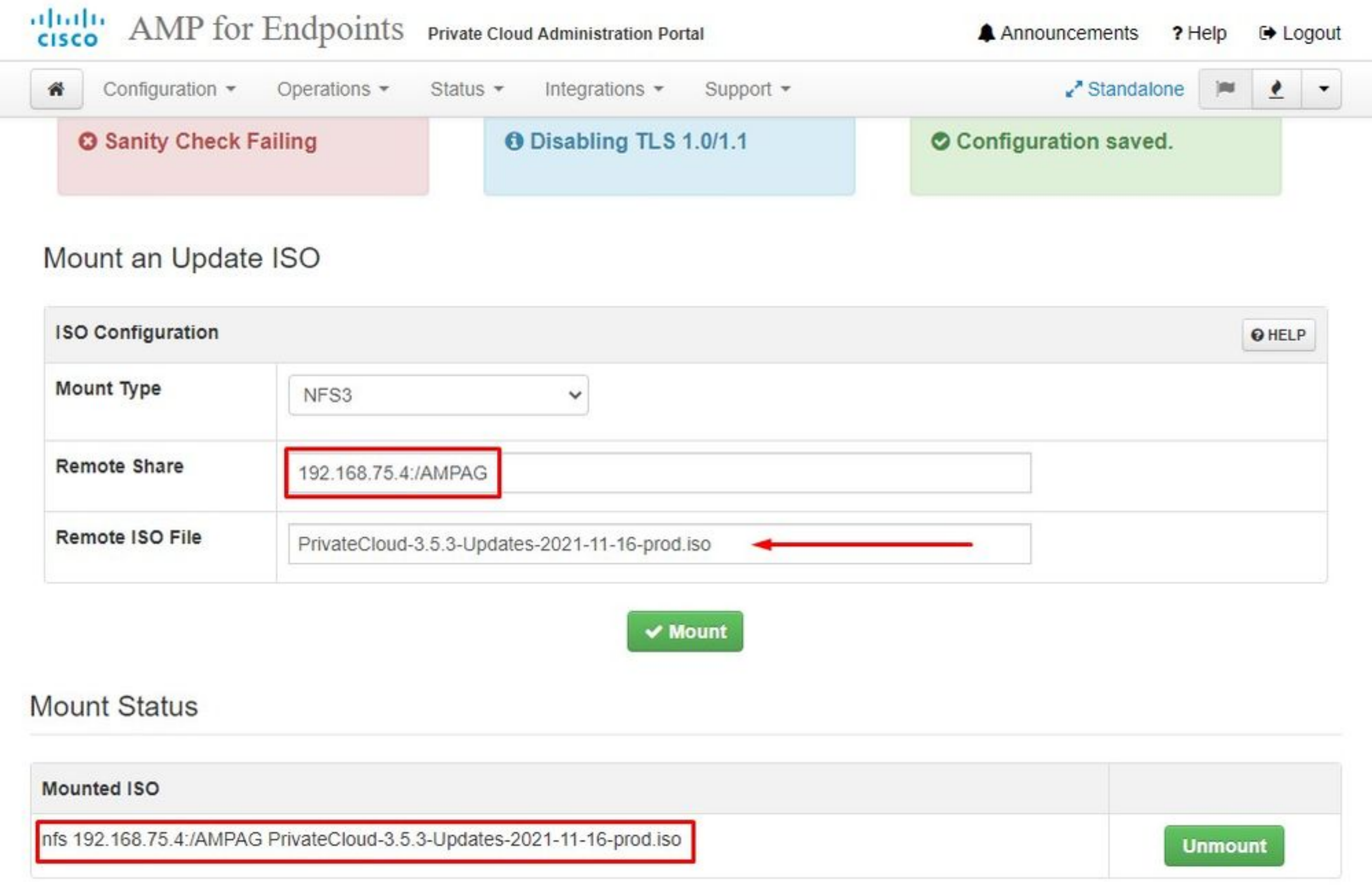
Mount an Update ISO

ISO Configuration

Mount Type: ISO

Mount Status

No ISO mounted



Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

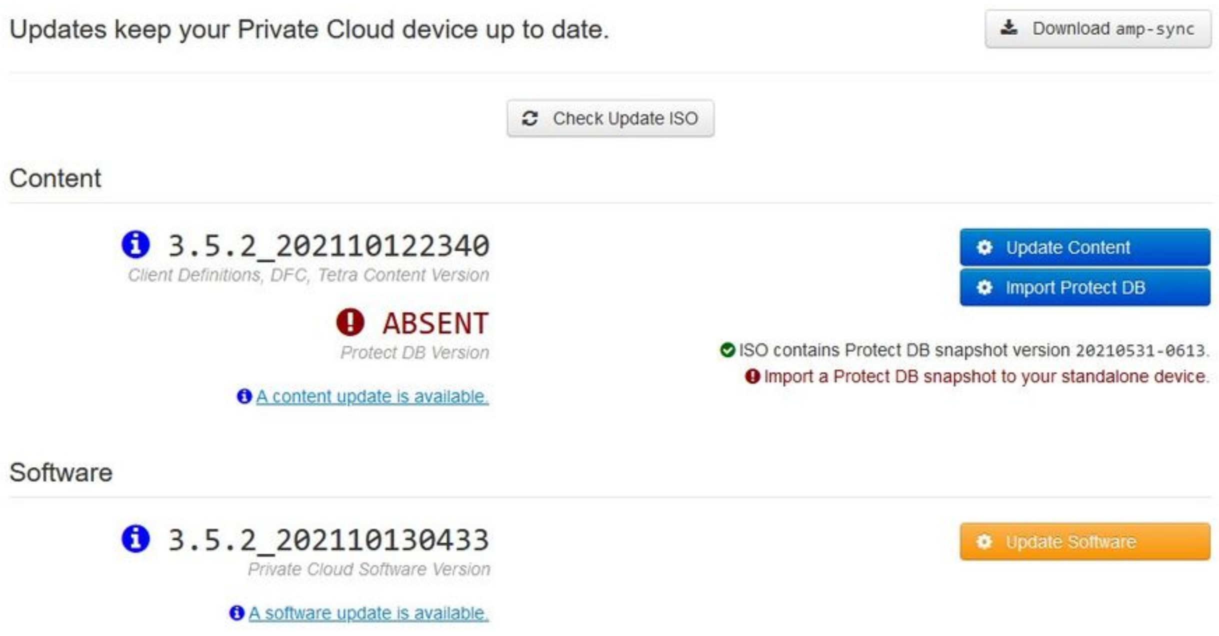
Mount an Update ISO

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.

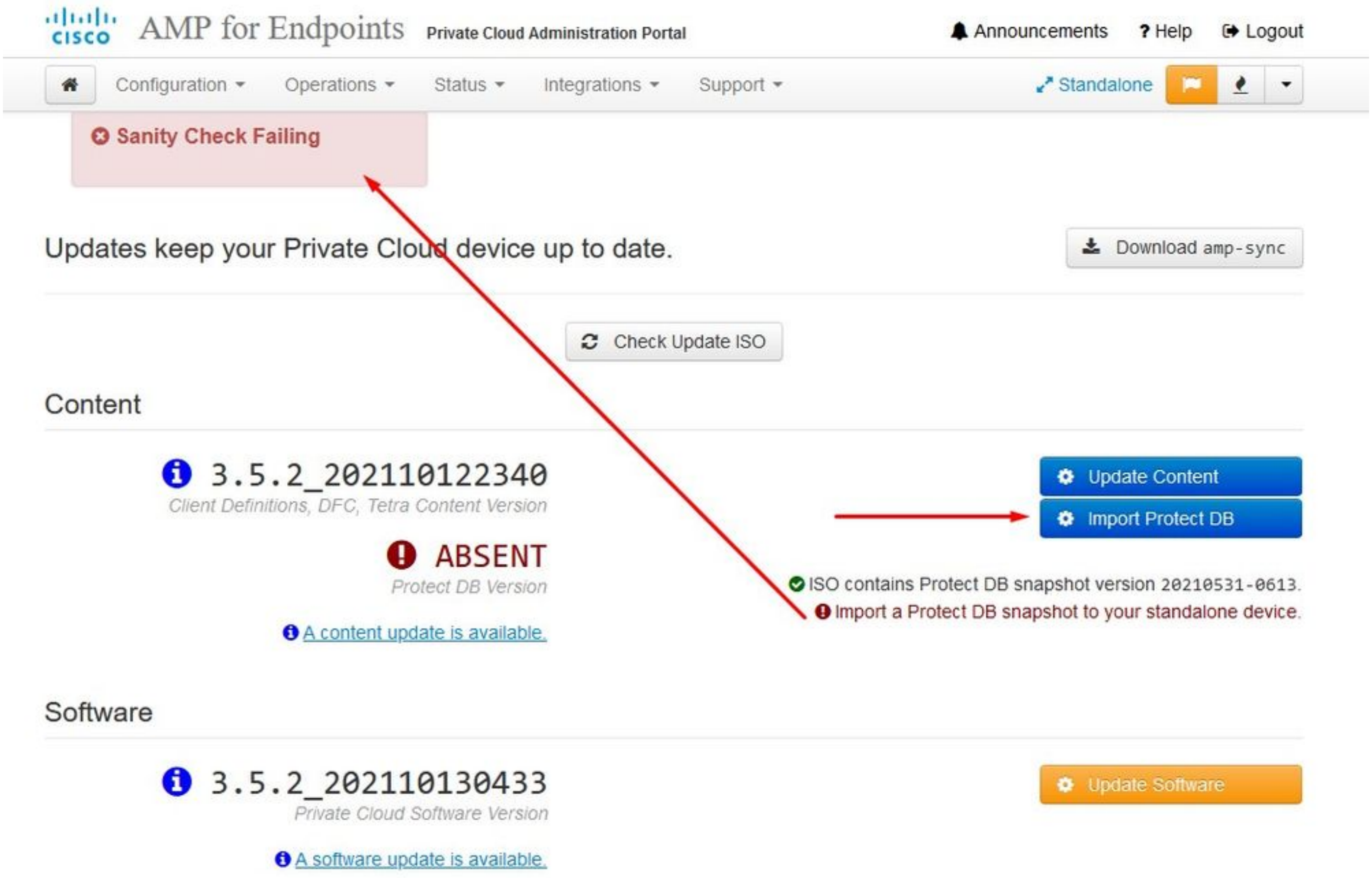
Software

3.5.2_202110130433

Private Cloud Software Version

A software update is available.

“健全性检查失败”与“保护DB当前在VPC上不可用”相关



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.

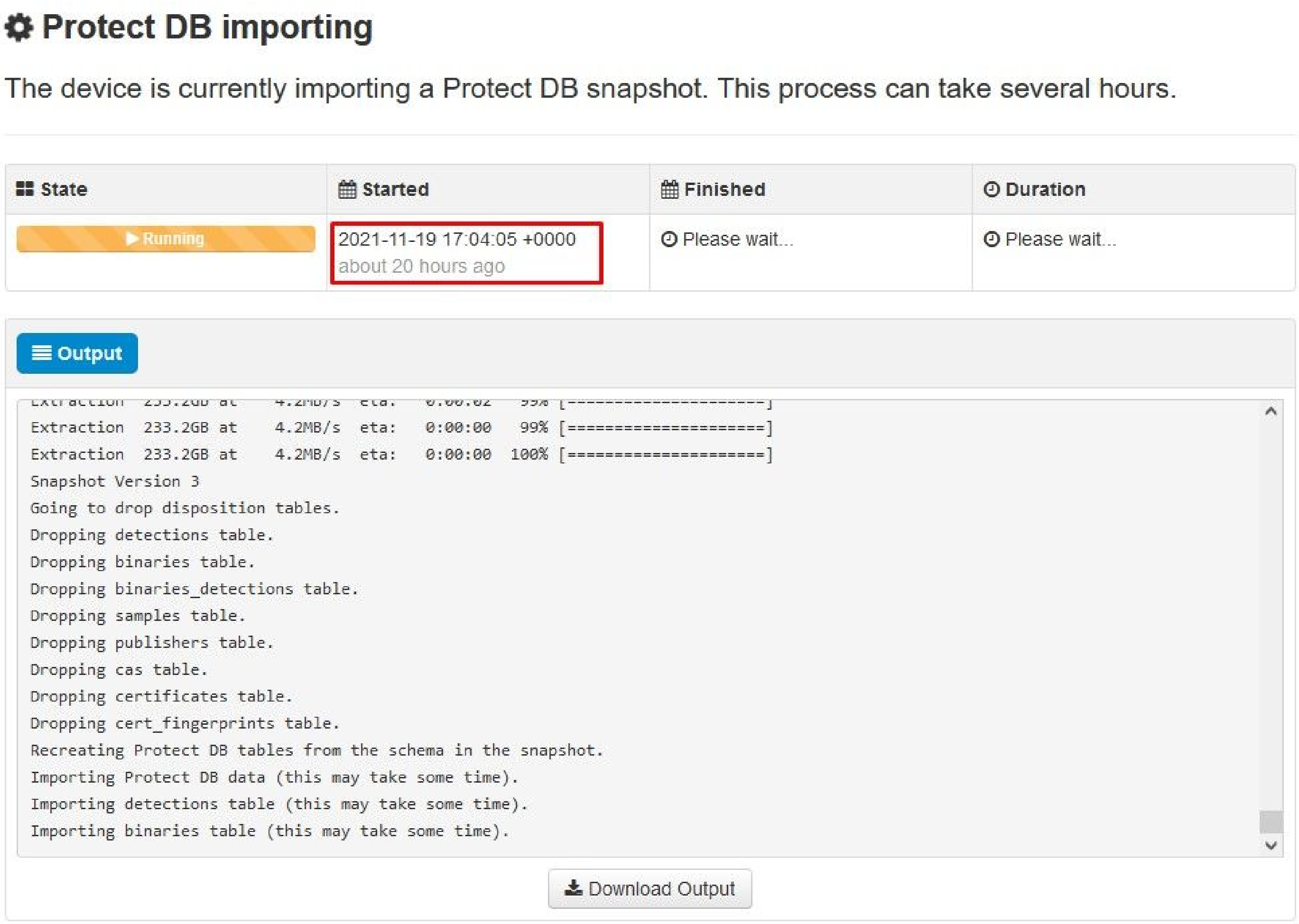
Import a Protect DB snapshot to your standalone device.

Software

3.5.2_202110130433

Private Cloud Software Version

A software update is available.

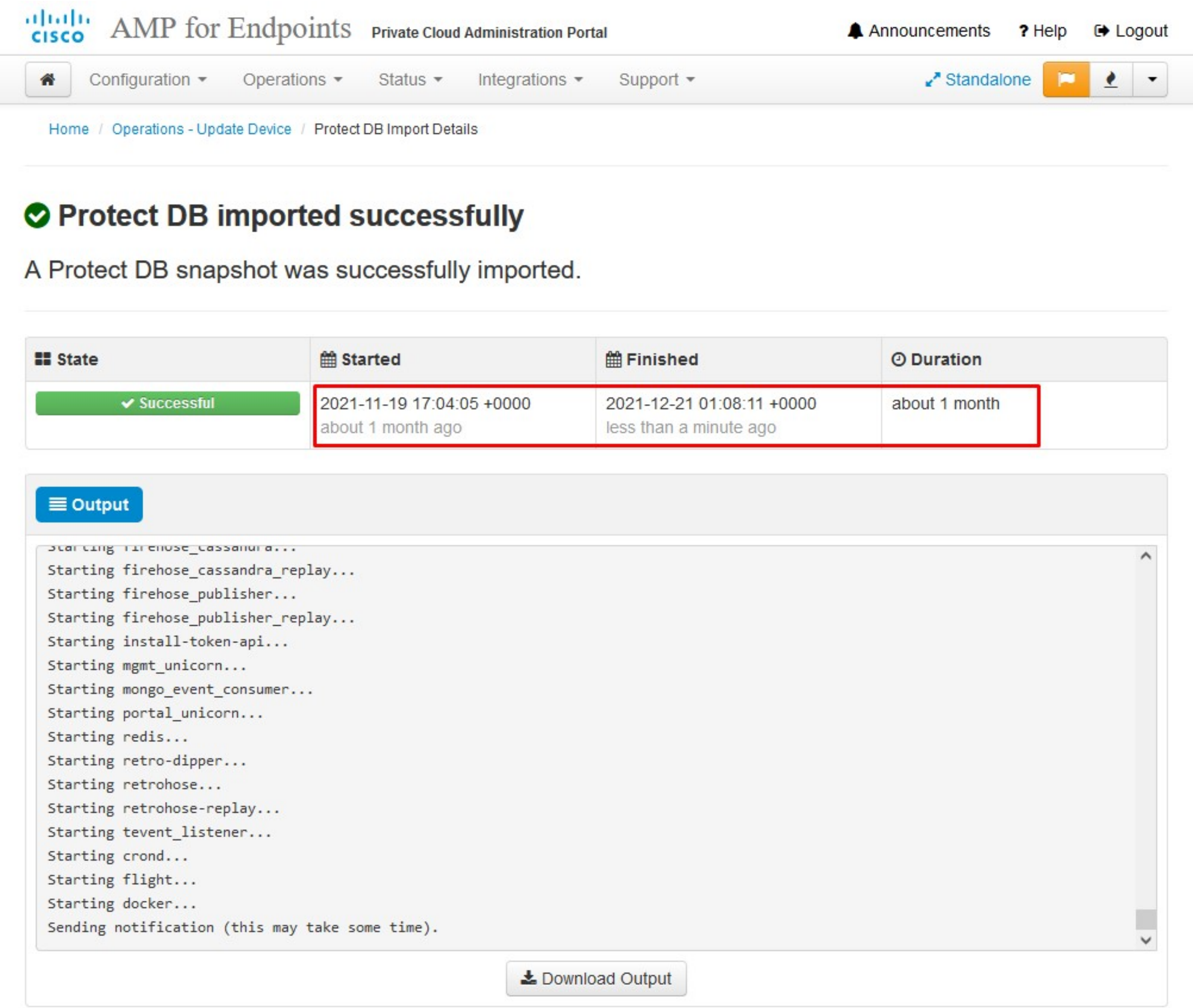


Protect DB importing

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).
```



Home / Operations - Update Device / Protect DB Import Details

Protect DB imported successfully

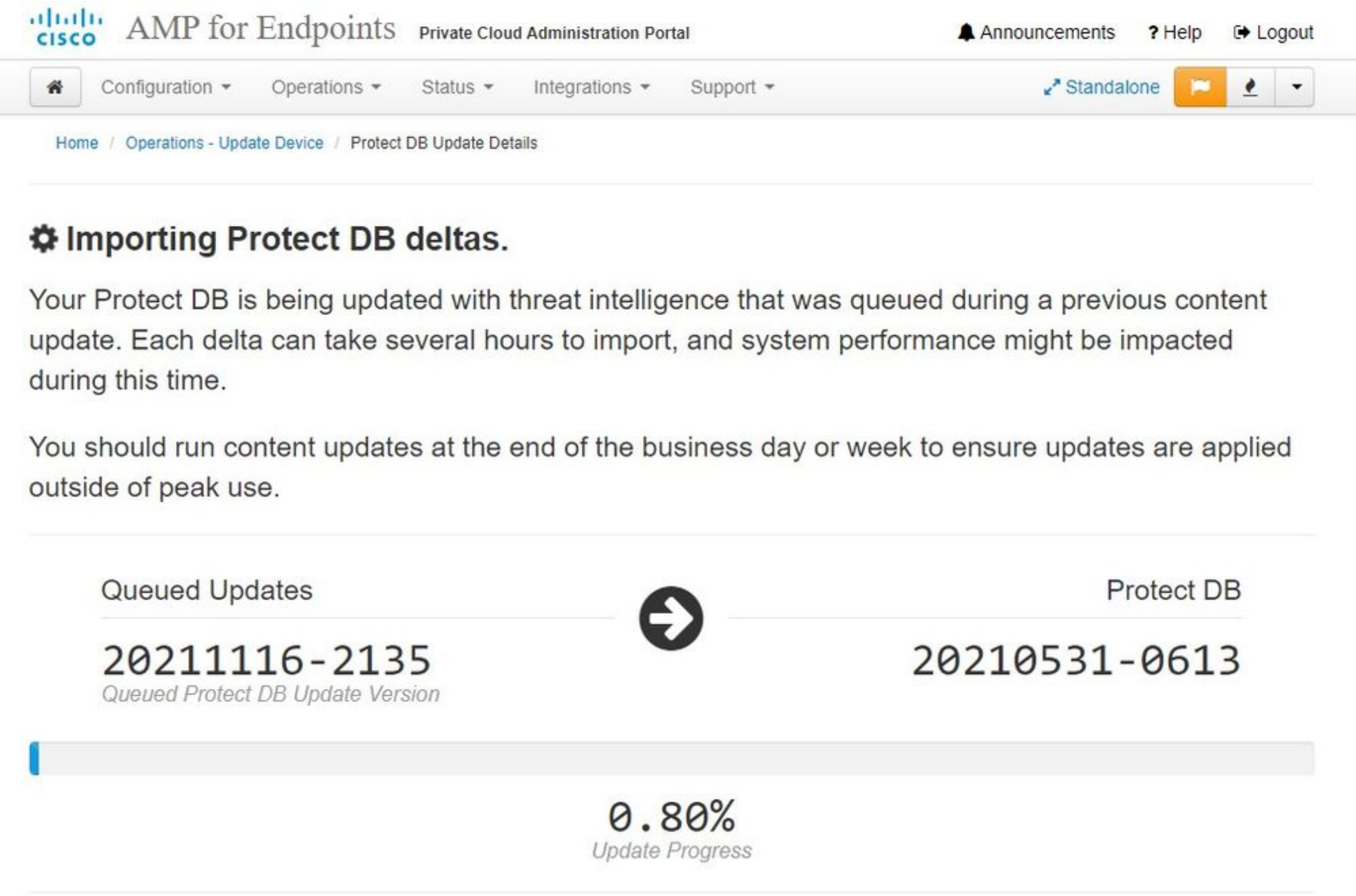
A Protect DB snapshot was successfully imported.

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

Output

```
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).
```

下一次更新自动开始



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.

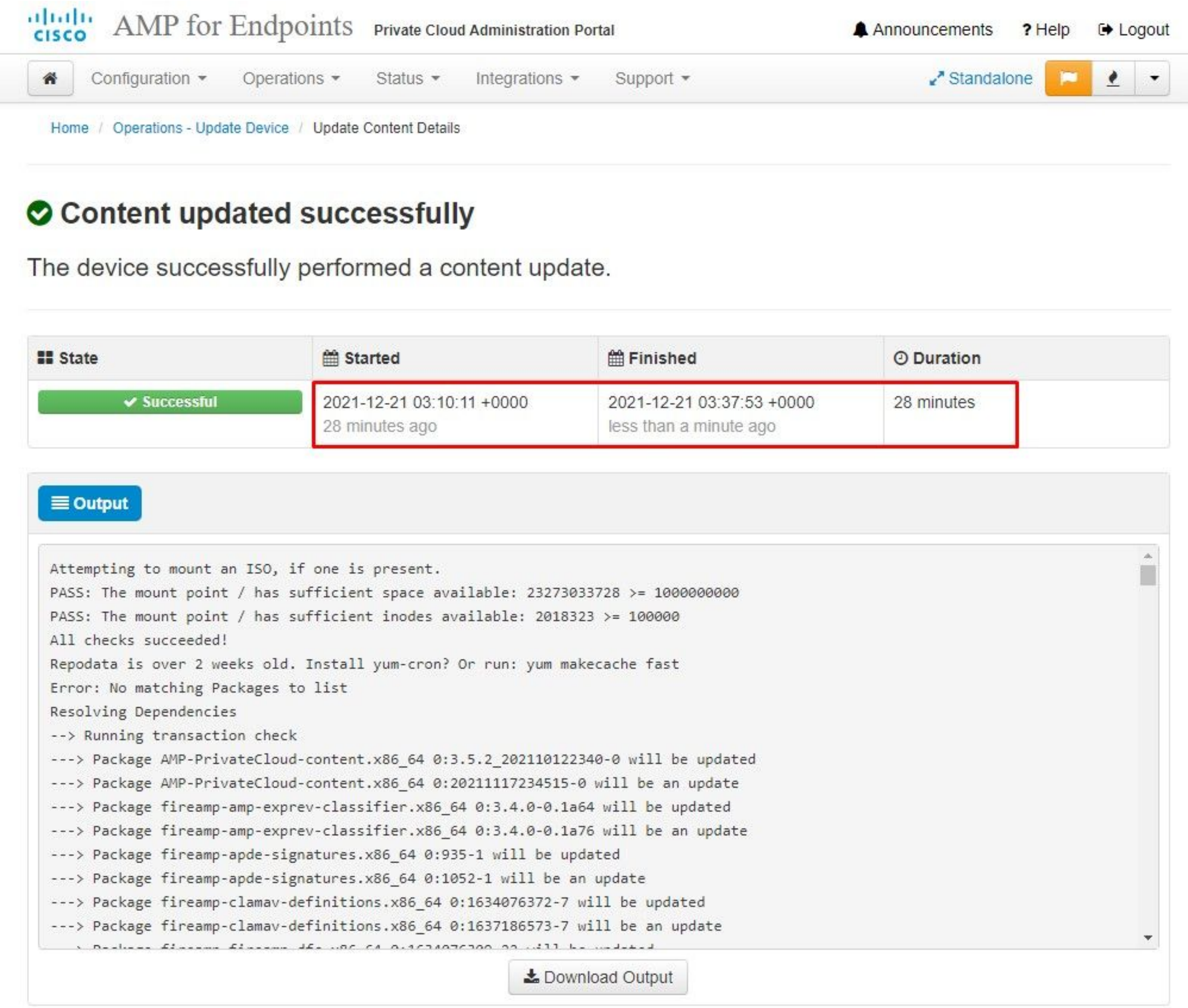
You should run content updates at the end of the business day or week to ensure updates are applied outside of peak use.

Queued Updates: 20211116-2135 (Queued Protect DB Update Version)

Protect DB: 20210531-0613

0.80% Update Progress

在导入保护数据库这一非常漫长的过程之后，您可以移动并更新客户端定义和软件，大约需要3个多小时。



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
```

最后，请注意，此过程将需要很长时间。

对于VPC设备，请访问包含如何更新HW设备、安装ISO文件以及从USB引导的其他方法的TZ。

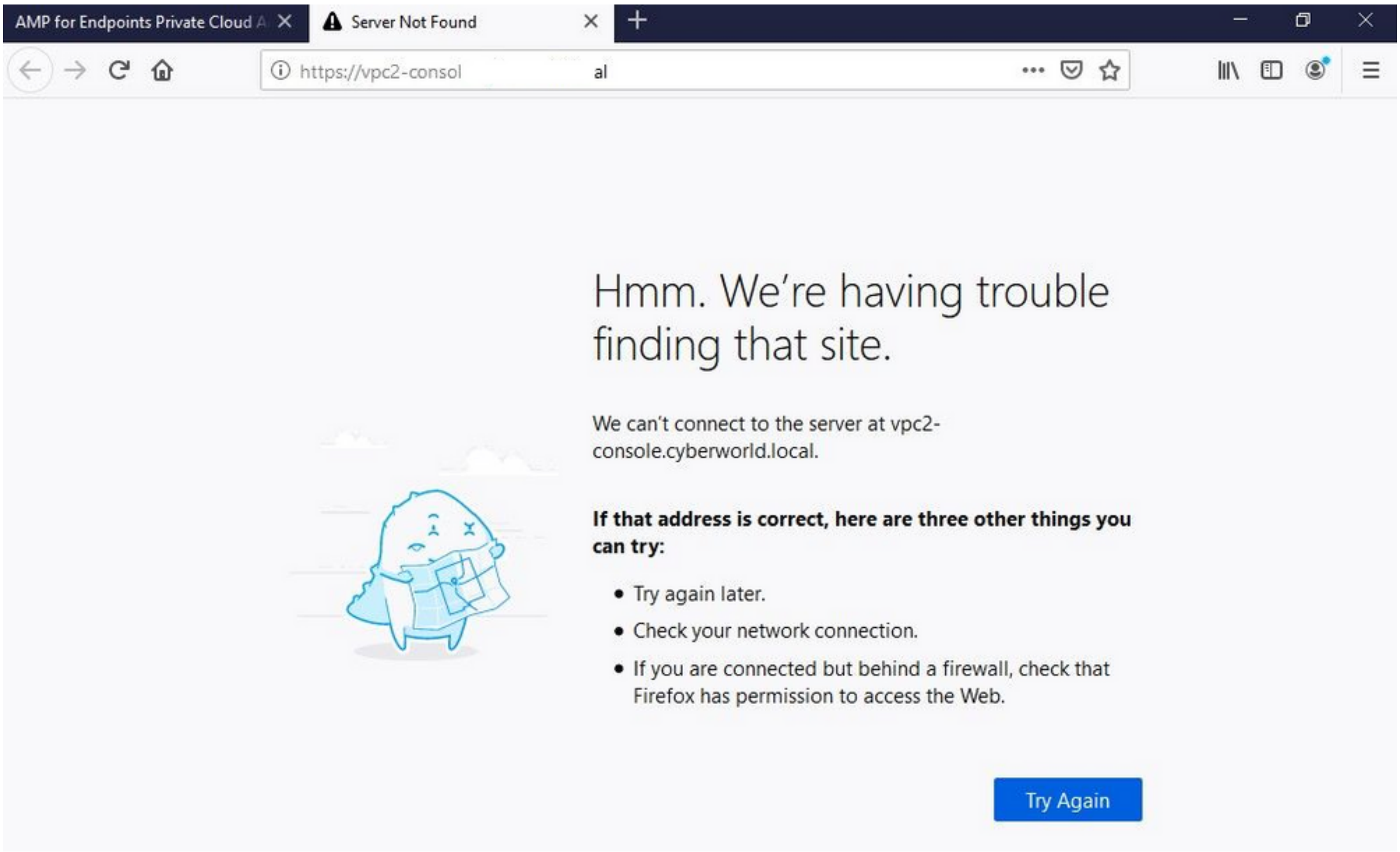
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

仅︽︽AIRGAP︽︽

基本故障排除

问题#1 - FQDN和DNS服务器

您可能遇到的第一个问题是，如果您的DNS服务器未建立，并且所有FQDN均未正确记录和解析。当您尝试通过安全终端“fire”图标导航到安全终端控制台时，问题可能如下所示。 如果只使用IP地址，则它有效，但无法下载连接器。如下面的第三张图。



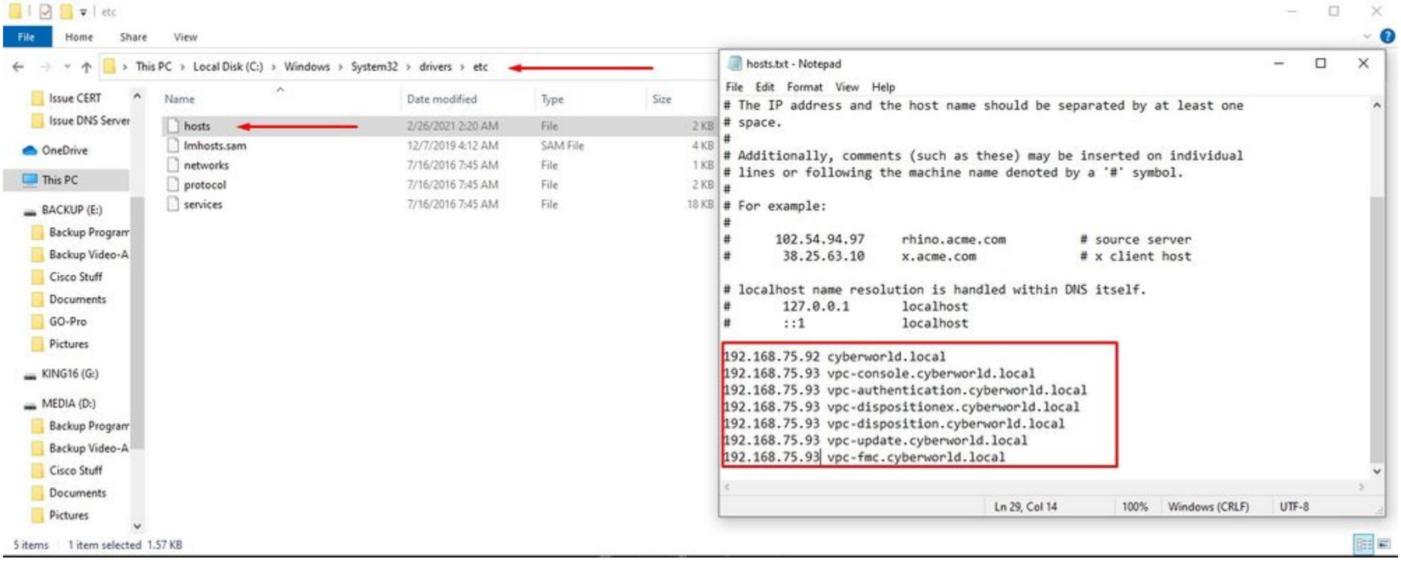
Hmm. We're having trouble finding that site.

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.

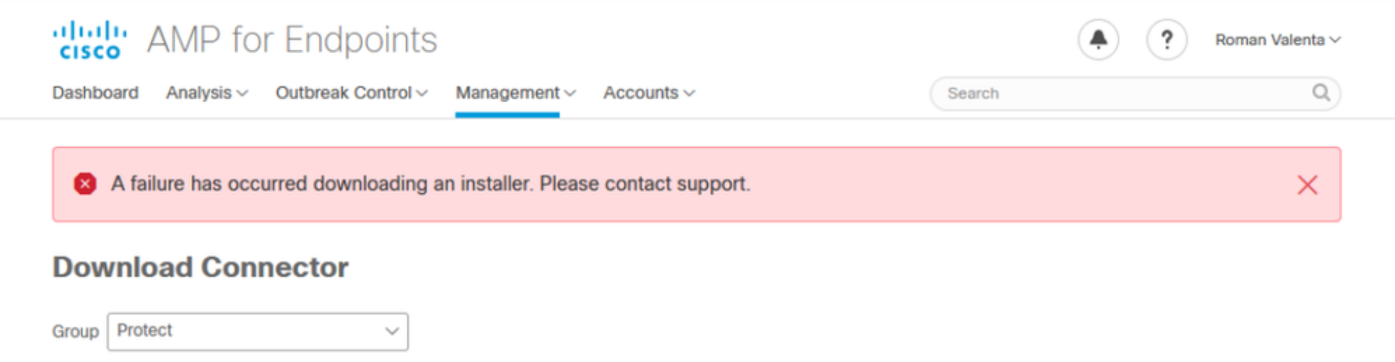
如果您如图所示修改本地计算机上的HOSTS文件，则解决了此问题，并最终出现错误。



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
```

尝试下载安全终端连接器安装程序时收到此错误。



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

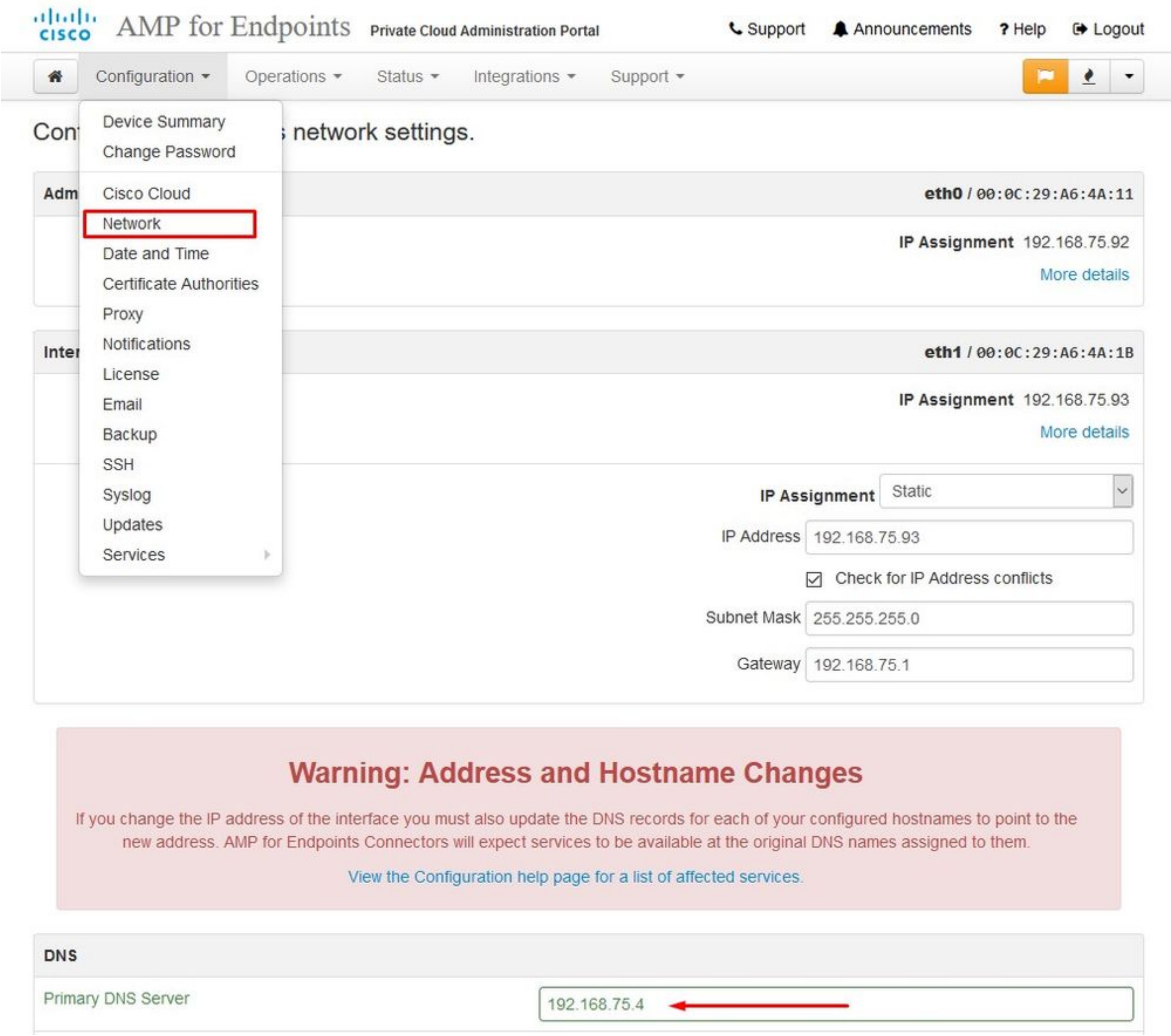
Download Connector

Group: Protect

经过一些故障排除后，唯一正确的解决方案是设置DNS服务器。

```
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服务器中记录所有FQDN并将虚拟私有云中的记录从公共DNS更改为DNS服务器后，一切都会按预期开始工作。



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

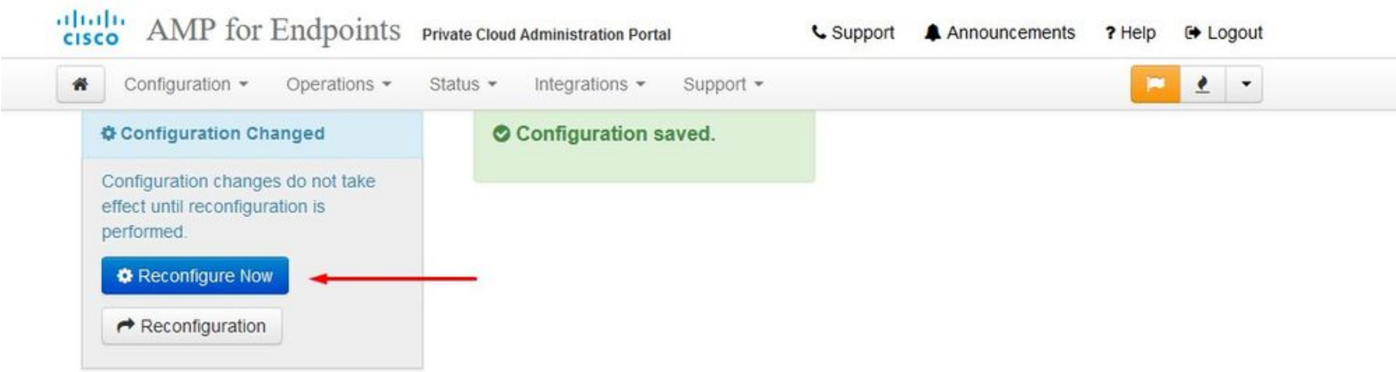
Warning: Address and Hostname Changes

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

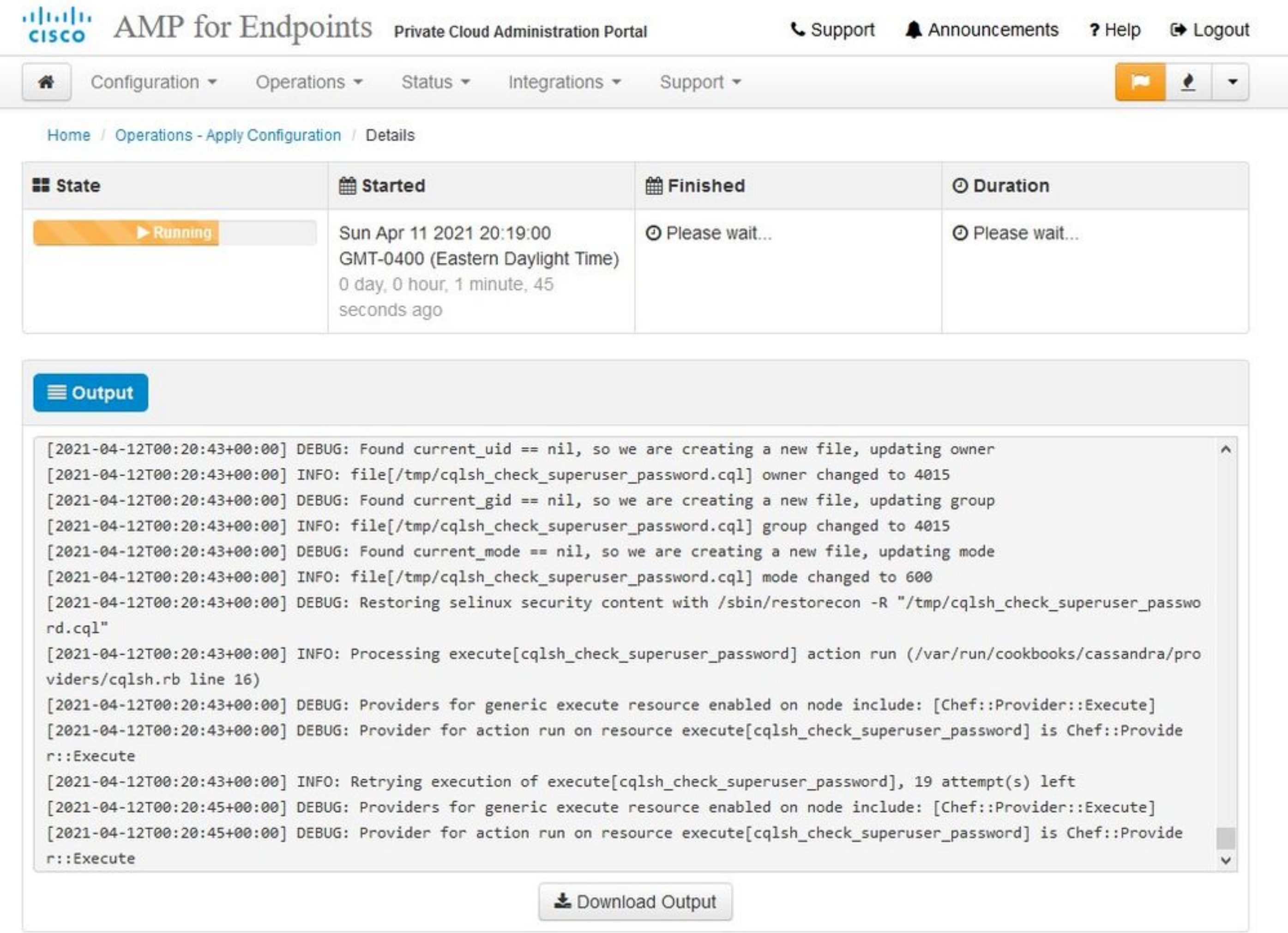
Primary DNS Server 192.168.75.4



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

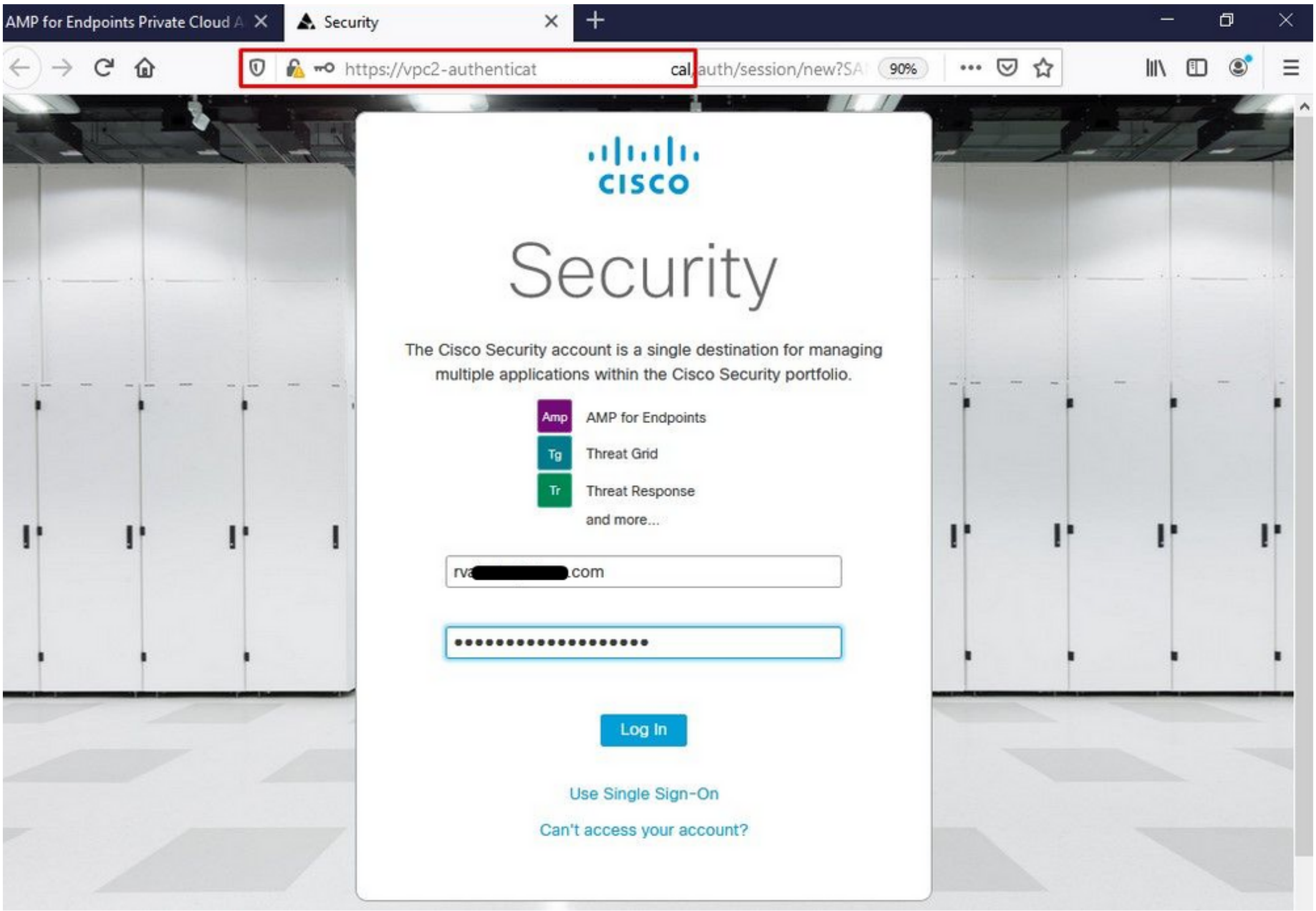
Configuration saved.



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
```

此时，您可以登录并下载连接器


AMP for Endpoints Private Cloud A
Security
https://vpc2-authenticat cal auth/session/new?SA
90%
cisco

Security

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

- Amp AMP for Endpoints
- Tg Threat Grid
- Tr Threat Response
- and more...

rva[redacted].com

••••••••••••••••••••

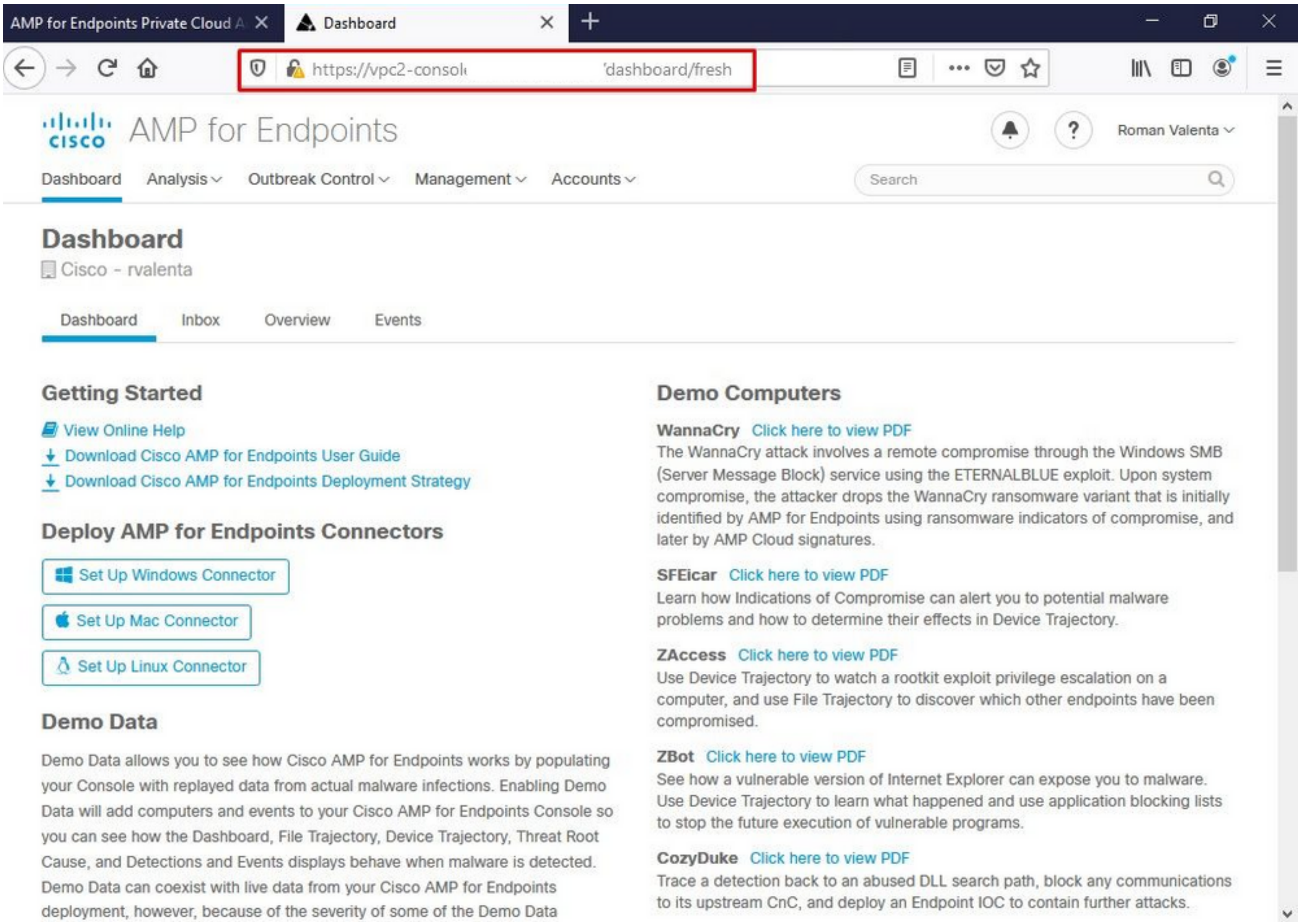
Log In

Use Single Sign-On

Can't access your account?

您将获得适用于您的环境的初始安全终端策略向导。它会引导您选择您使用的防病毒产品（如果有）以及代理（如果有的话），并引导您选择要部署的策略类型。根据连接器的操作系统选择相应的“设置……”按钮。

您将看到“现有安全产品”页面，如图所示。选择您使用的安全产品。它会自动生成适用的例外项，以防止您的终端出现性能问题。选择“下一步”。



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.

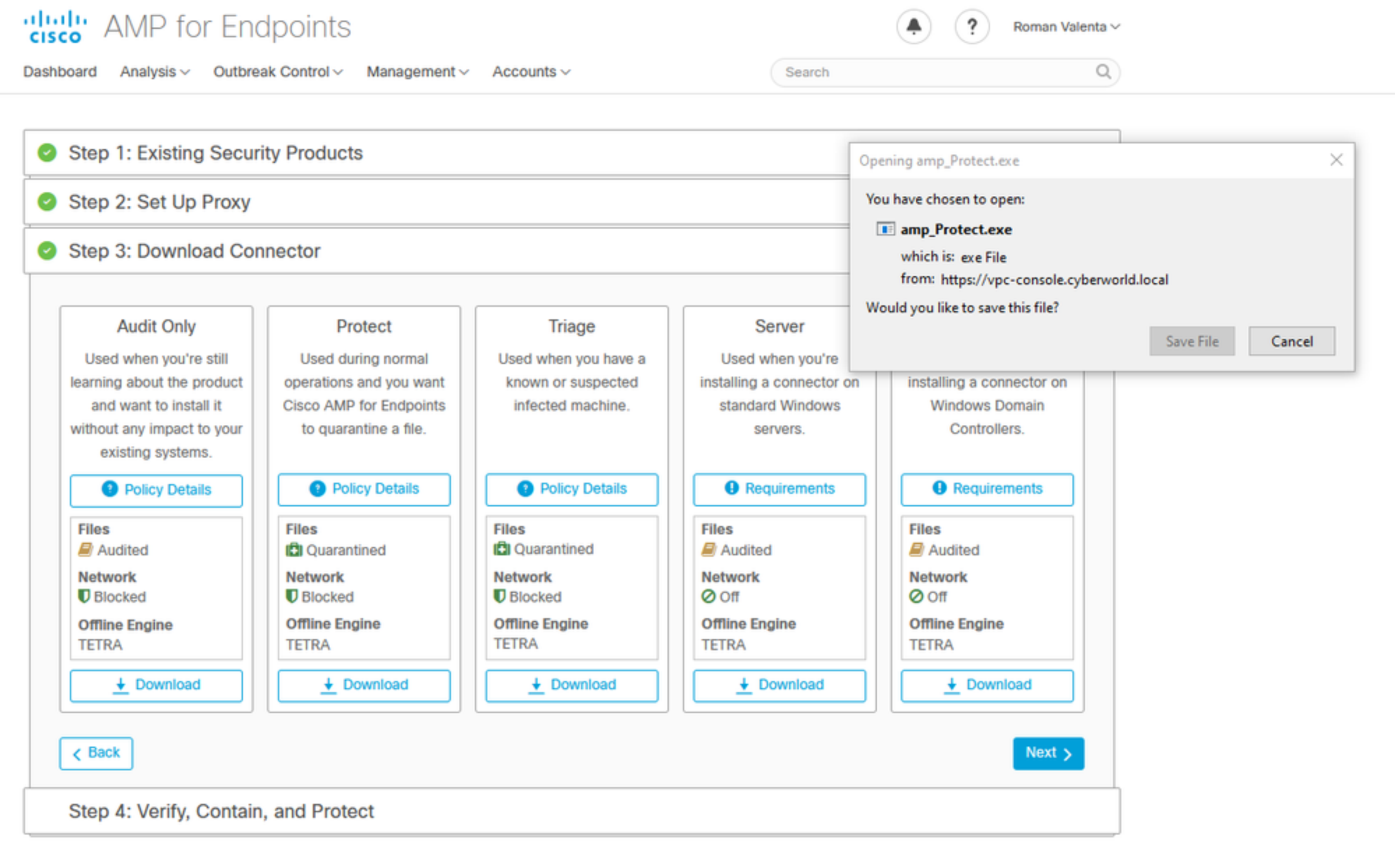
SFEicar Click here to view PDF
Learn how Indications of Compromise can alert you to potential malware problems and how to determine their effects in Device Trajectory.

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.

下载连接器。



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.
Files Audited	Files Quarantined	Files Quarantined	Files Audited	Files Audited
Network Blocked	Network Blocked	Network Blocked	Network Off	Network Off
Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

amp_Protect.exe

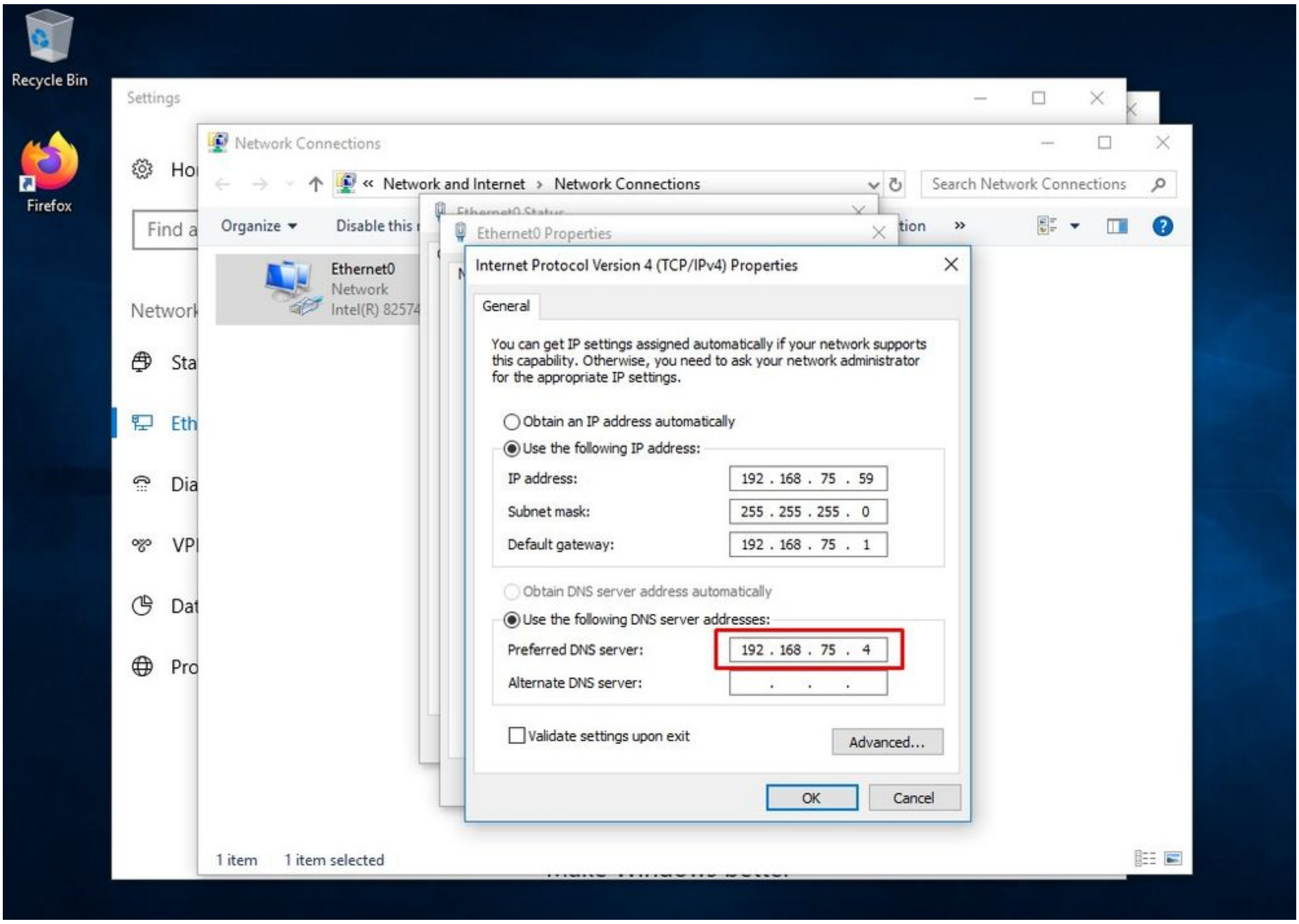
which is: exe File

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

Would you like to save this file?

问题#2 — 根CA的问题

您可能会面临的下一个问题是，如果您使用自己的内部证书，则首次安装后，连接器可能会显示为disconnected。



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:

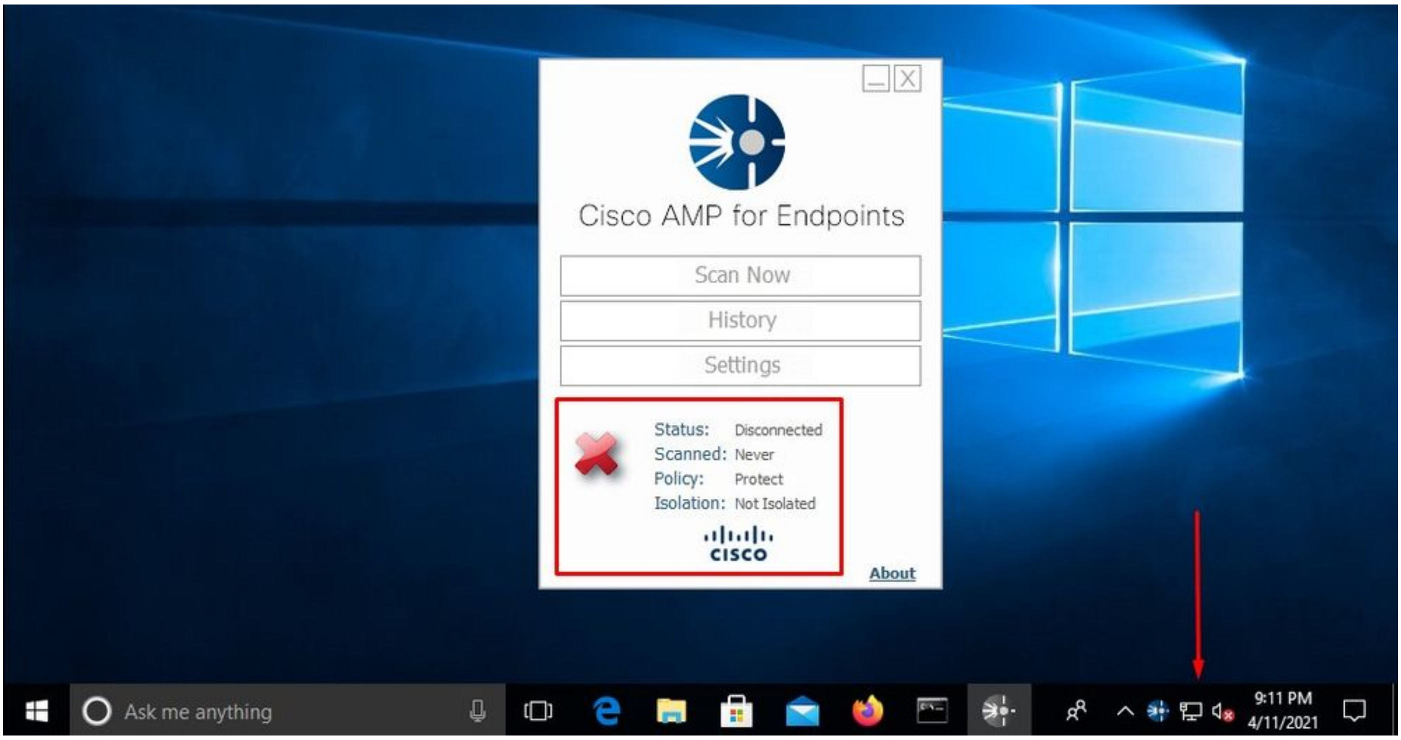
IP address: 192 . 168 . 75 . 59
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 75 . 1

○ 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

安装连接器后，安全终端会被视为已断开连接。运行诊断捆绑包并查看日志，您可以确定问题。



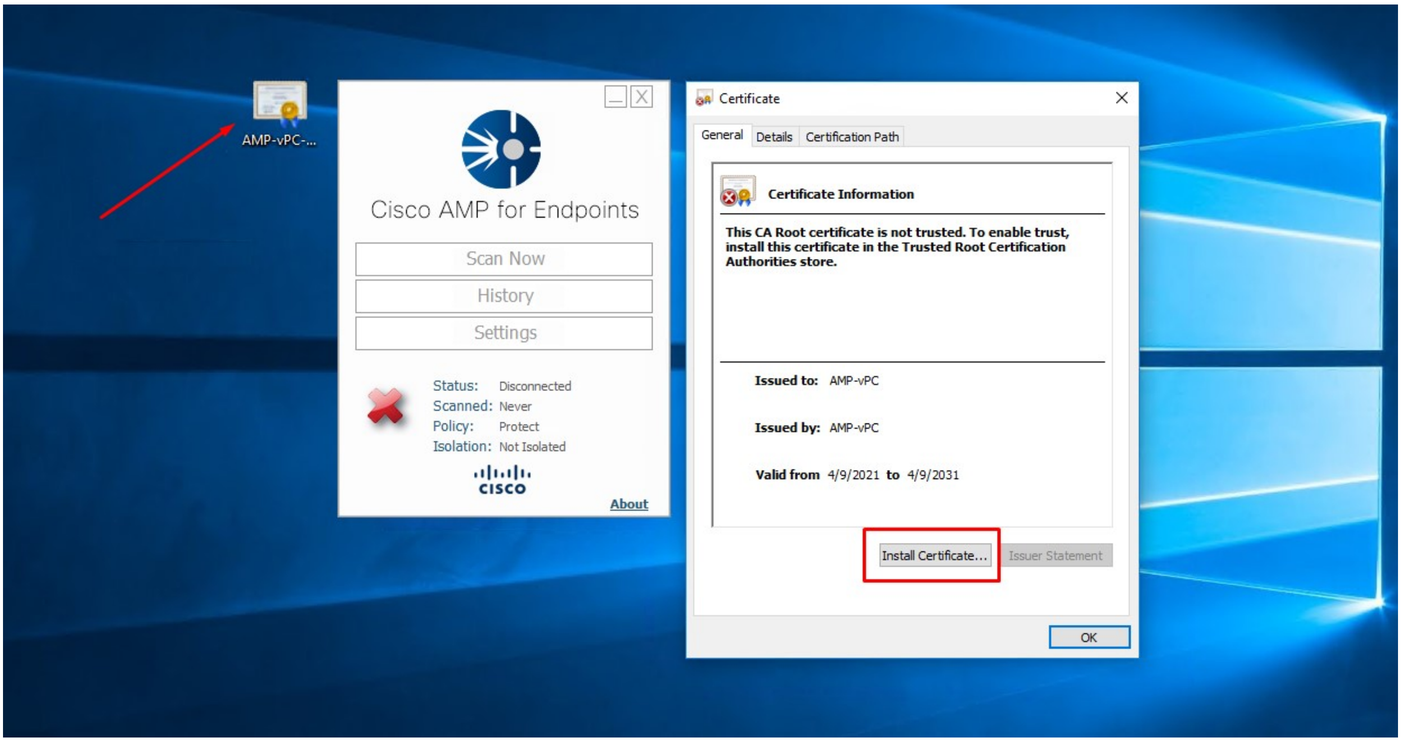
Cisco AMP for Endpoints

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

根据从诊断包收集的输出，您可以看到根CA错误

```
(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
```

将根CA上传到受信任的根CA存储并重新启动安全终端服务后。一切如预期开始工作。



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

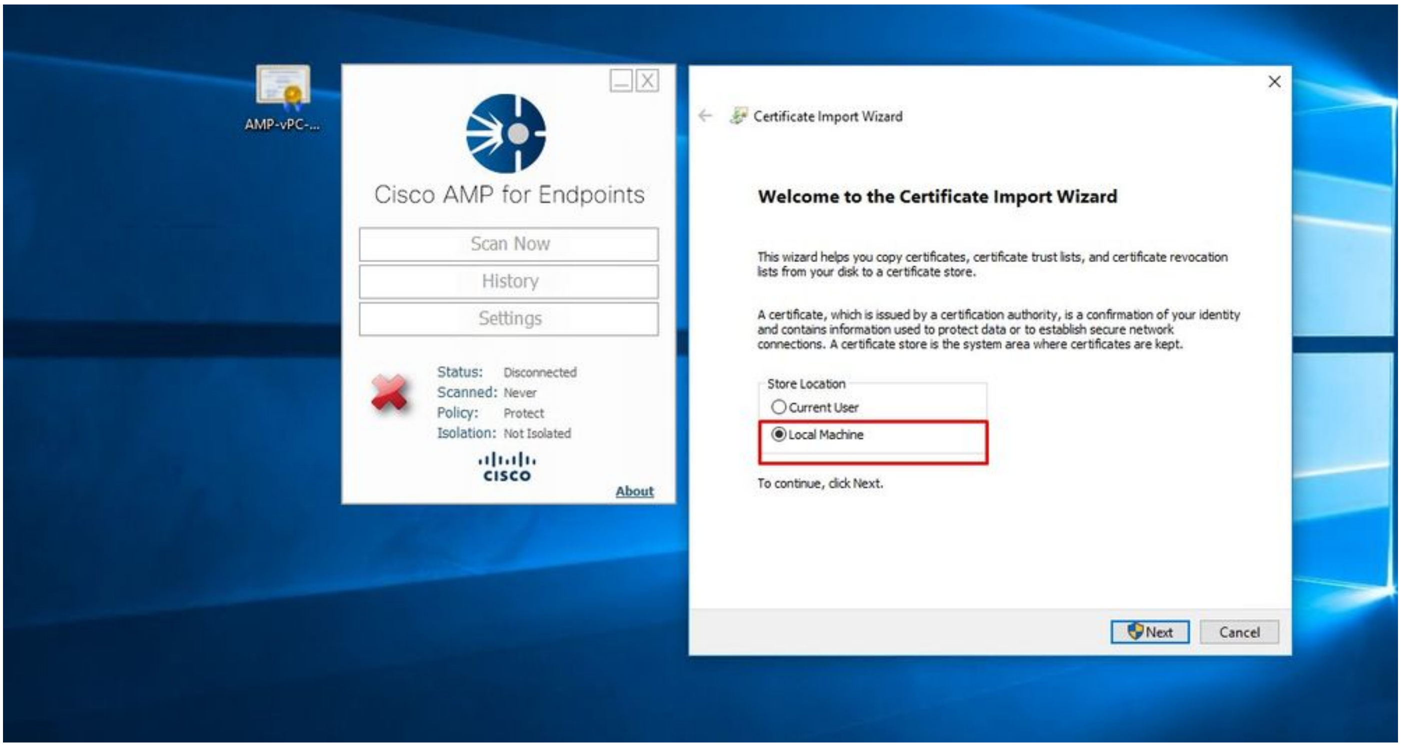
Certificate Information

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

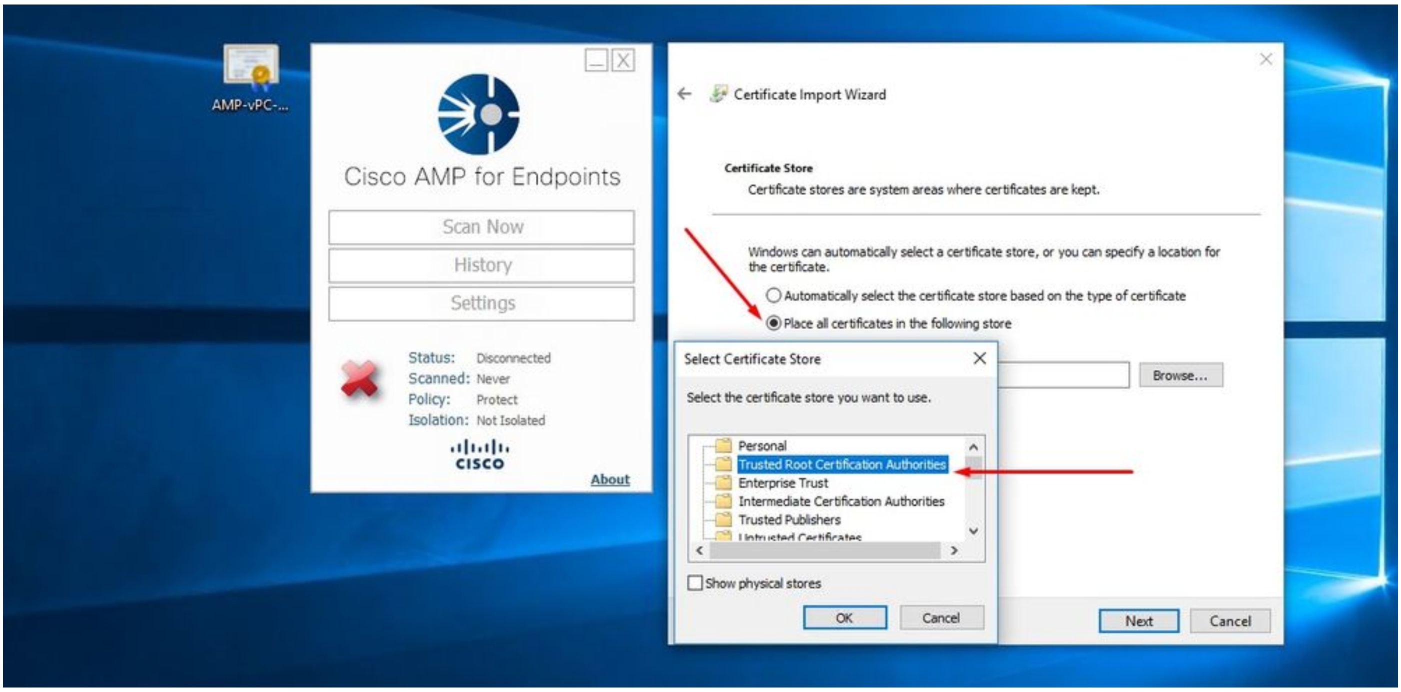
Welcome to the Certificate Import Wizard

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

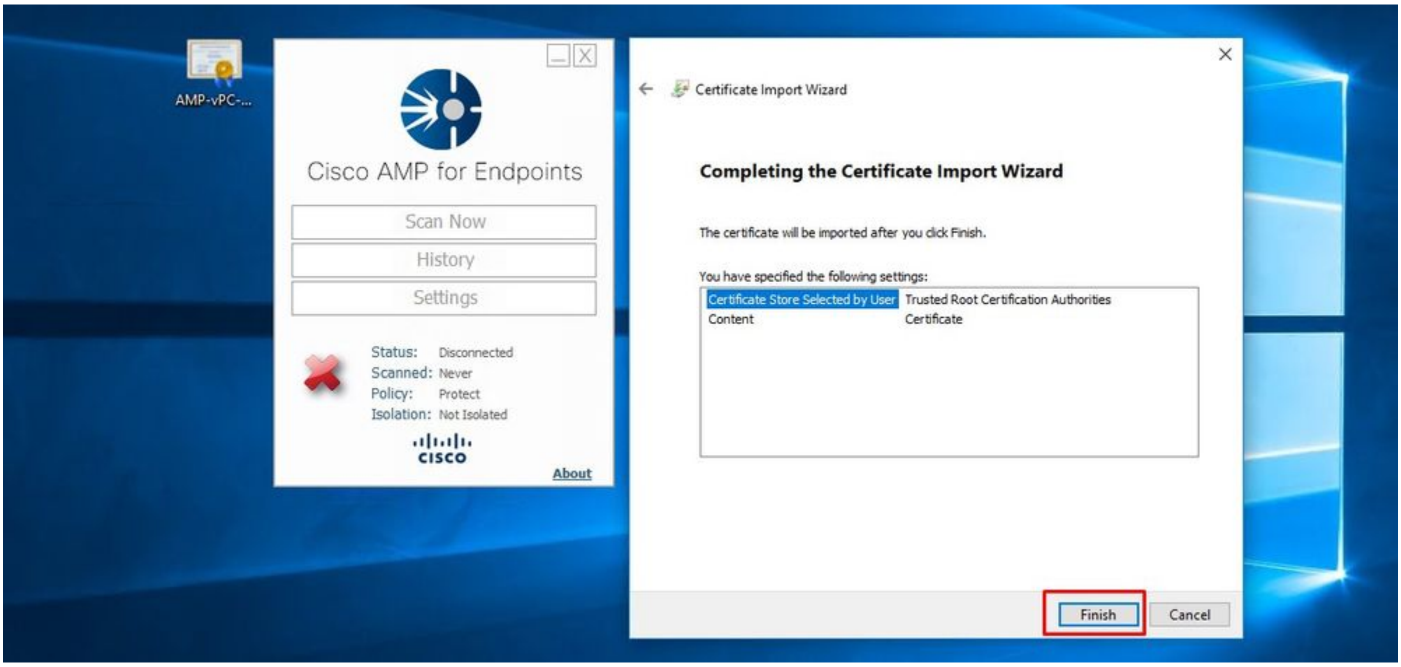
● Place all certificates in the following store

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

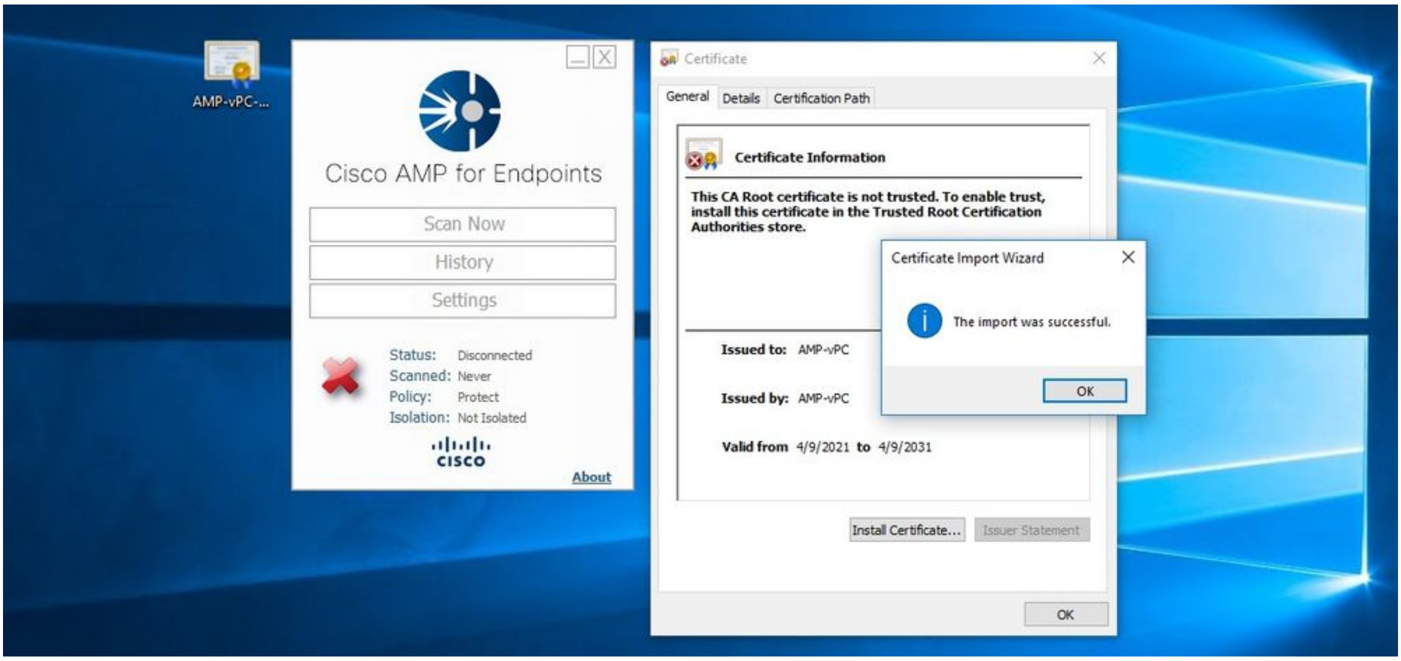
Certificate Import Wizard

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

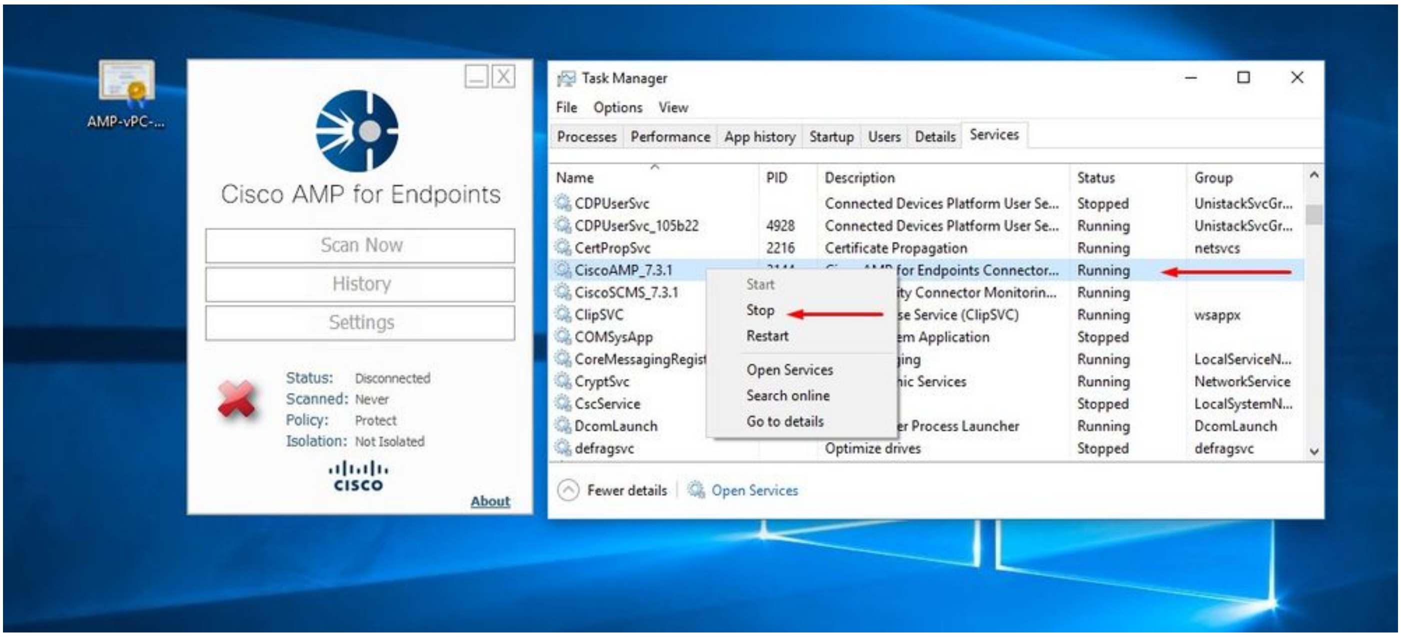
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

The import was successful.

Issued to: AMP-vPC

Issued by: AMP-vPC

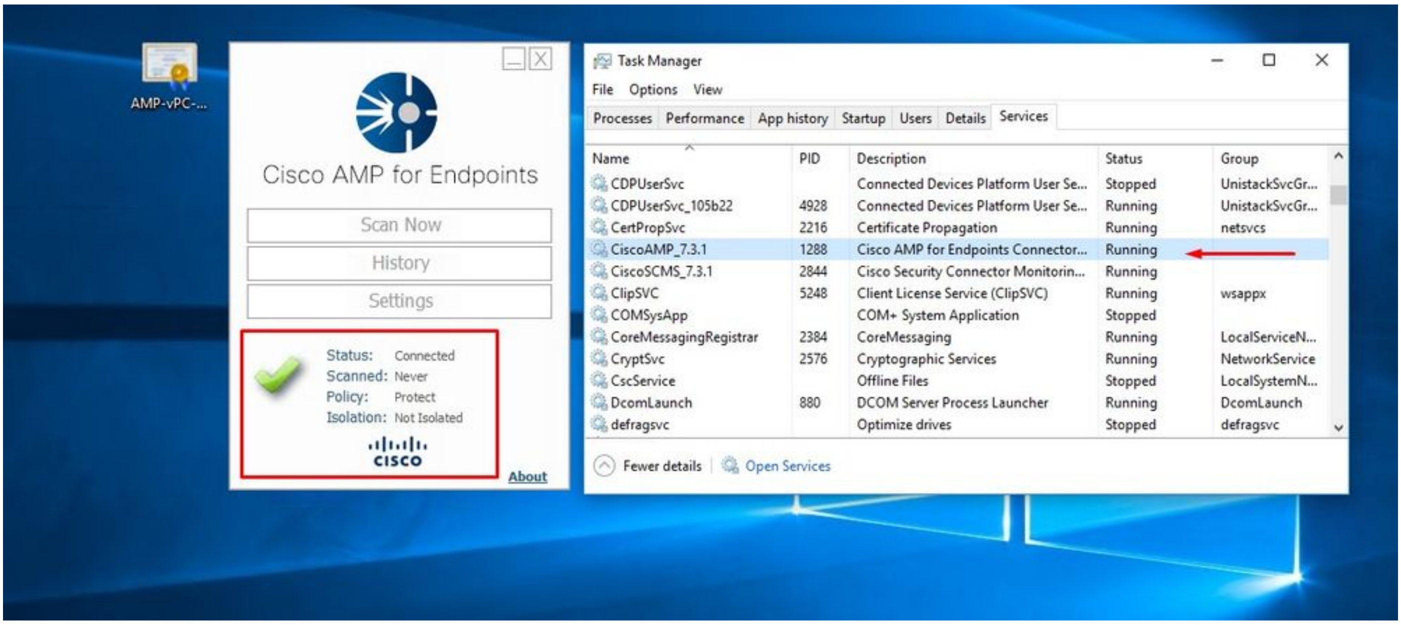
Valid from 4/9/2021 **to** 4/9/2031



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

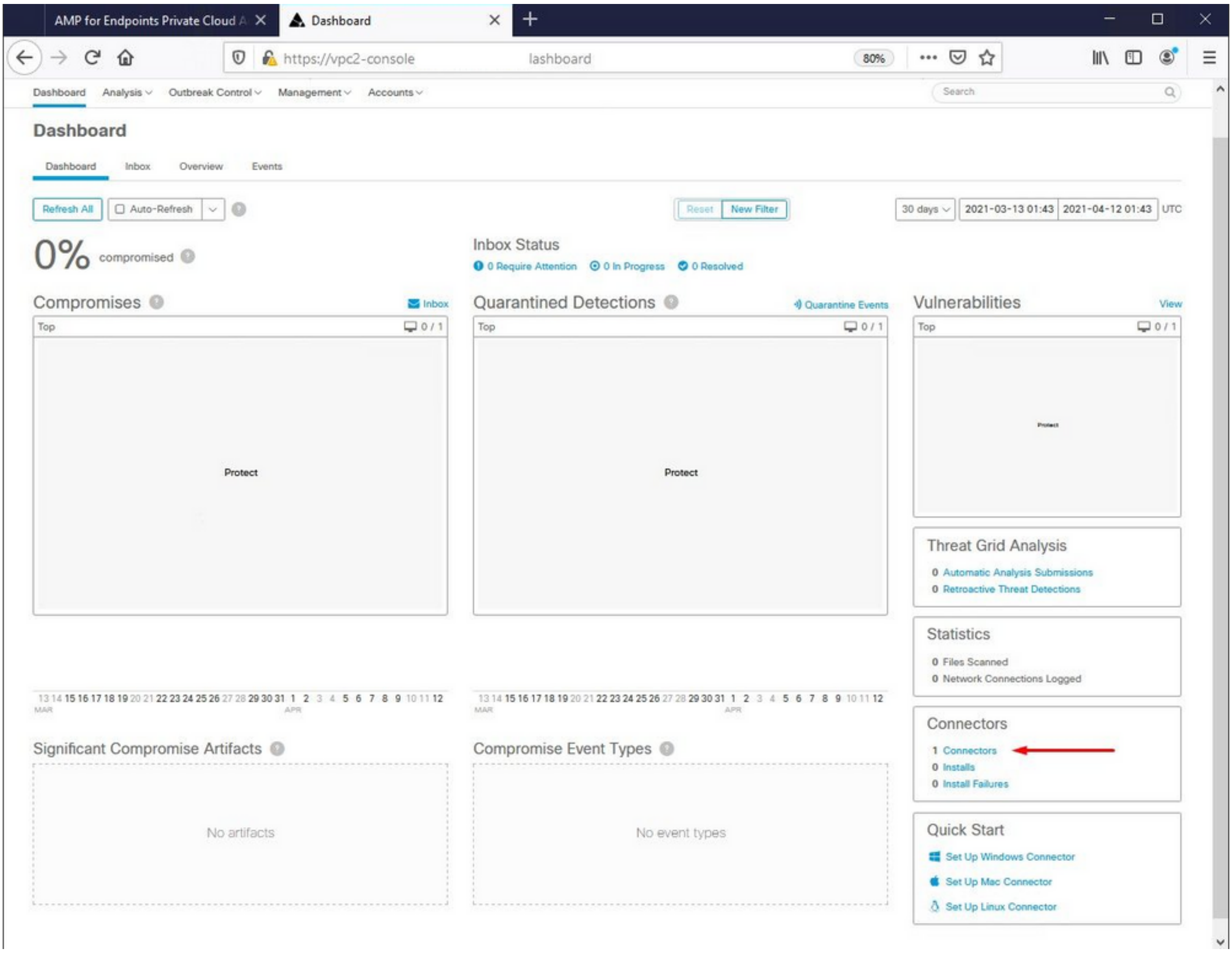
Name	PID	Description	Status	Group
CDPUserSvc		Connected Devices Platform User Se...	Stopped	UnistackSvcGr...
CDPUserSvc_105b22	4928	Connected Devices Platform User Se...	Running	UnistackSvcGr...
CertPropSvc	2216	Certificate Propagation	Running	netsvcs
CiscoAMP_7.3.1	[illegible]	for Endpoints Connector...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

退回安全终端服务连接器后，连接器将如预期一样联机。



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



Dashboard

30 days 2021-03-13 01:43 2021-04-12 01:43 UTC

0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Compromises 0 / 1

Quarantined Detections 0 / 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
Set Up Mac Connector
Set Up Linux Connector

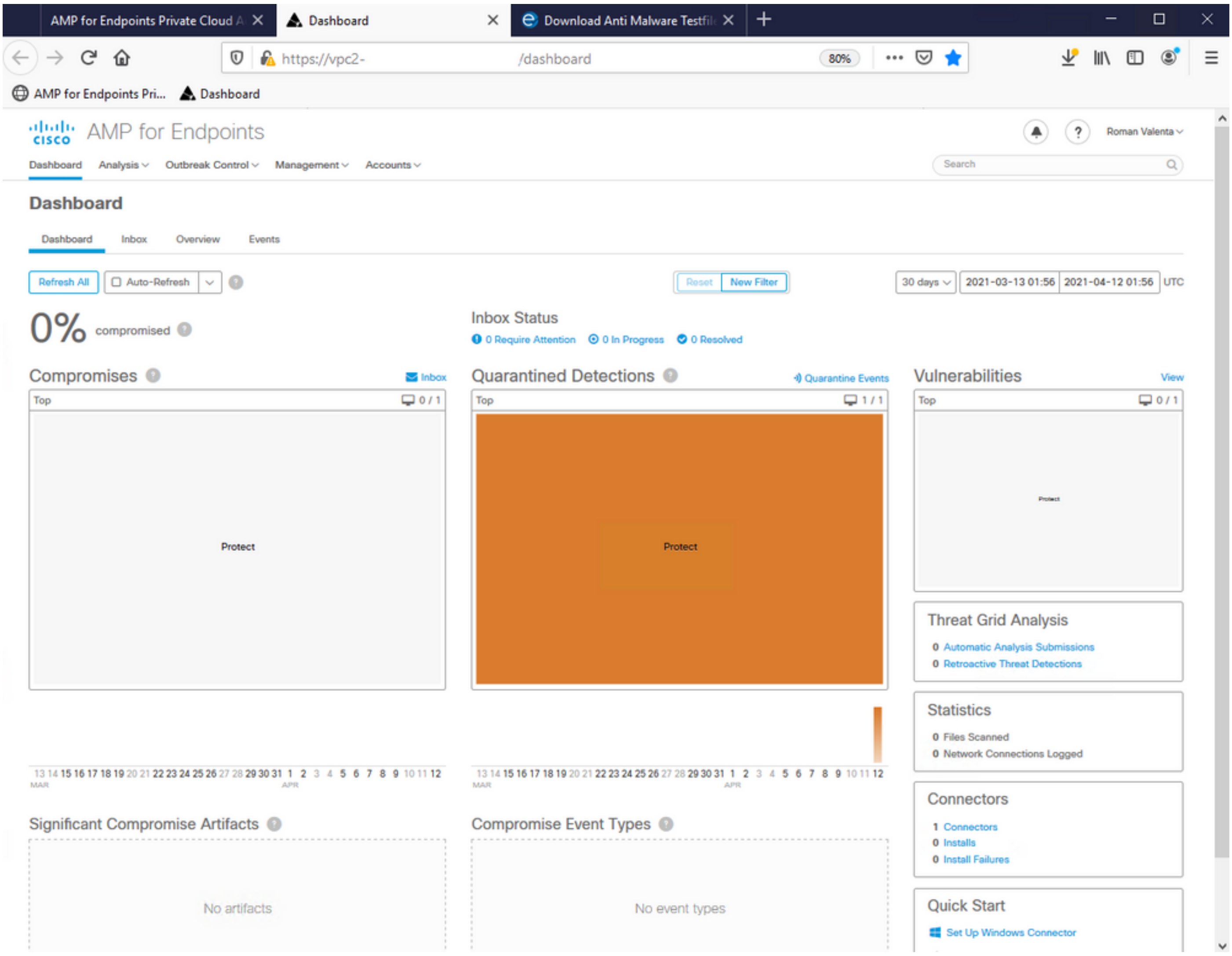
Significant Compromise Artifacts

No artifacts

Compromise Event Types

No event types

经过测试的恶意活动



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

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12

Significant Compromise Artifacts
No artifacts

Compromise Event Types
No event types

关于此翻译

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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