

# セキュアエンドポイント仮想プライベートクラウドのインストールと設定

## 内容

---

[概要](#)

[前提条件](#)

[VPCの導入](#)

[VMのインストール](#)

[管理インターフェイスの初期設定](#)

[Web GUIによるvPCの初期設定](#)

[コンフィギュレーション](#)

[サービス](#)

[AirGapアップデートパッケージ](#)

[問題#1 - データストアのスペースが使い果たされた](#)

[問題#2 - 古いアップデート](#)

[基本的なトラブルシューティング](#)

[問題#1 - FQDNとDNSサーバ](#)

[問題#2 : ルートCAの問題](#)

## 概要

このドキュメントでは、ESXi環境のサーバに仮想プライベートクラウド(VPC)を正常に導入する方法について説明し、重点的に説明します。クイックスタートガイド、導入戦略、エンタイトルメントガイド、コンソール、管理者ユーザガイドなどの他のドキュメントについては、このサイトの[ドキュメント](#)を参照してください。

著者 : Cisco TACエンジニア、Roman Valenta

## 前提条件

要件 :

VMware ESX 5以降

- クラウドプロキシモード (のみ) :128 GB RAM、8 CPUコア (4コアのCPU 2基を推奨)、VMwareデータストアの最小ディスク空き容量1 TB
- ドライブのタイプ : エアギャップモードにはSSDが必要、プロキシにはSSDが推奨
- RAIDタイプ : 1つのRAID 10グループ (ストライプ・ミラー)
- VMwareデータストアの最小サイズ : 2 TB
- RAID 10グループの最小データストア・ランダム読み取り(4,000):60,000 IOPS
- RAID 10グループの最小データストア・ランダム書き込み(4,000):30,000 IOPS

次の項目に関する専門知識があることが推奨されます。

- 証明書の操作方法に関する基本的な知識。
- DNSサーバ ( WindowsまたはLinux ) でDNSをセットアップする方法に関する基本的な知識
- VMware ESXiへのOpen Virtual Appliance(OVA)テンプレートのインストール

この実習で使用：

VMware ESX 6.5


- クラウドプロキシモード ( のみ ) :48 GB RAM、8 CPUコア ( 4コアのCPU 2基を推奨 ) 、  
VMwareデータストアの最小ディスク空き容量1 TB
- ドライブの種類：SATA
- RAIDタイプ：1つのRAID 1
- VMwareデータストアの最小サイズ：1 TB
- MobaXterm 20.2 ( PuTTYと同様のマルチターミナルプログラム )
- Cygwin64 ( AirGapアップデートのダウンロードに使用 )

さらに

- opensslまたはXCAを使用して作成した証明書
- DNSサーバ ( LinuxまたはWindows ) ラボでは、Windows Server 2016とCentOS-8を使用しました
- テストエンドポイント用のWindows VM
- ライセンス

メモリが48 GB以下の場合、バージョン3.2+ VPCは使用できなくなります。


---

 注：プライベートクラウドOVAはドライブパーティションを作成するため、それらをVMWare.サーバに指定する必要はありません。これにより、クリーンインターフェイスのホスト名が解決されます。

---

バージョン固有のハードウェア要件の詳細については、『[VPCアプライアンスのデータシート](#)』を参照してください。

---

 注：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

---

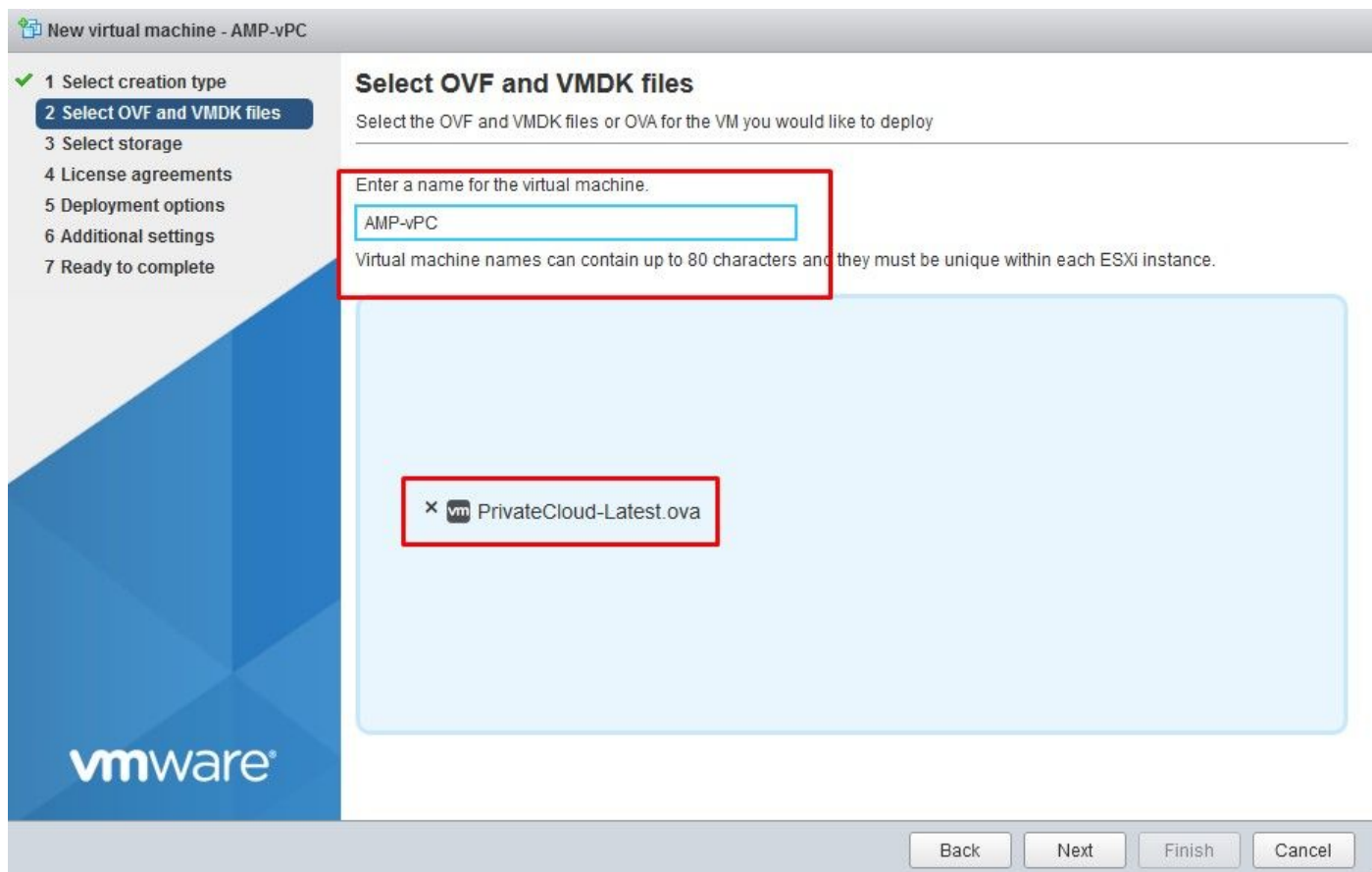
## VPCの導入

eDeliveryまたはエンタイトルメントメールに記載されているURLを選択します。OVAファイルをダウンロードし、インストールを続行します

### VMのインストール

ステップ1:

図に示すように、File > Deploy OVF Templateの順に移動し、Deploy OVF Templateウィザードを開きます。



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.

vmware

Back Next Finish Cancel

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

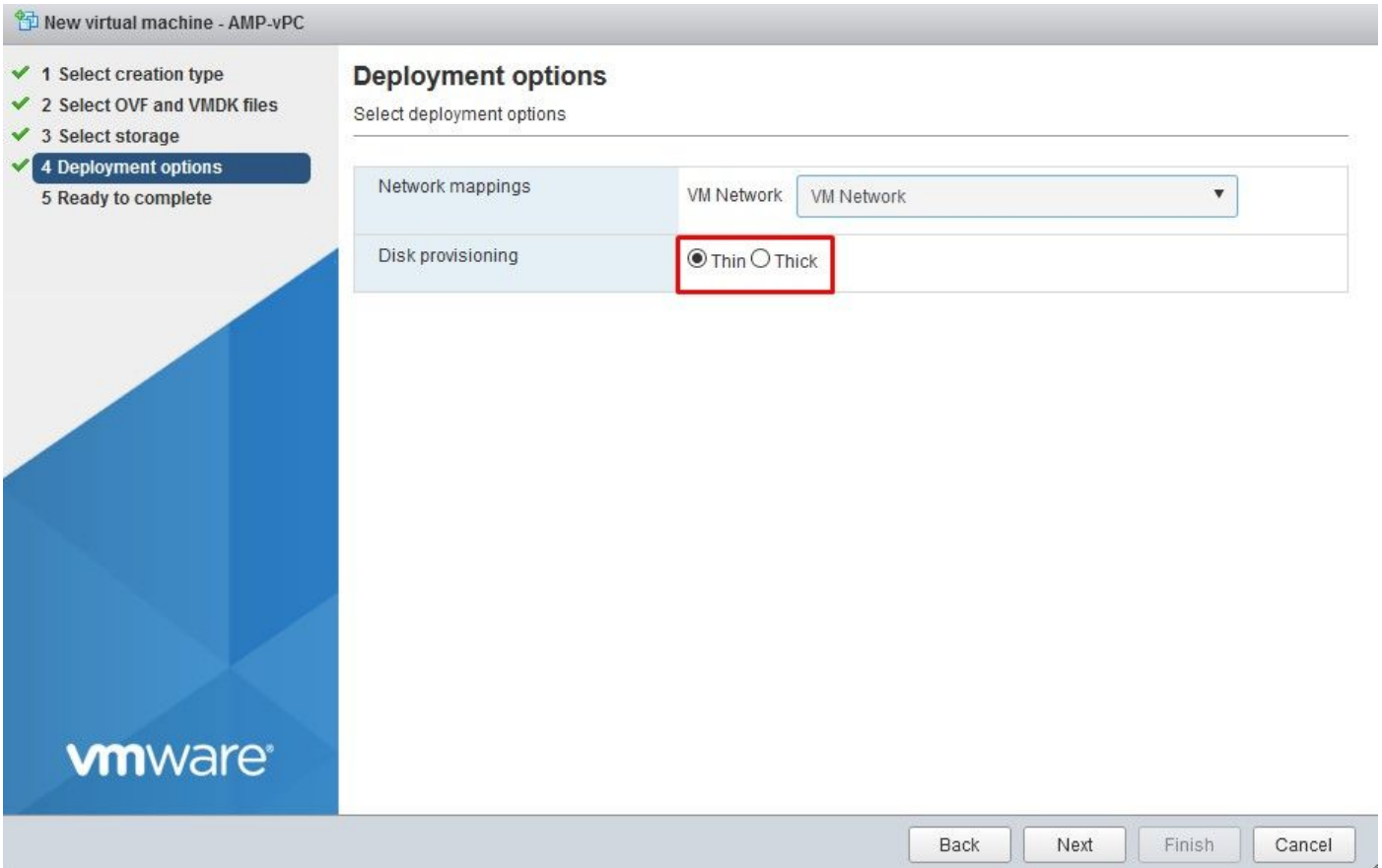
4 items

vmware

Back Next Finish Cancel

注:シックプロビジョニングでは、ディスクの作成時に領域が予約されます。このオプションを選択すると、シンプロビジョニングよりもパフォーマンスが向上します。ただし、これ

 は必須ではありません。次の図に示すように、Nextを選択します。



The screenshot shows the 'New virtual machine - AMP-vPC' wizard. On the left, a progress list shows five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains a 'Select deployment options' section. This section has two rows: 'Network mappings' with a dropdown menu set to 'VM Network', and 'Disk provisioning' with radio buttons for 'Thin' (selected) and 'Thick'. A red box highlights the 'Thin' radio button. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

ステップ 2 :

Browse...を選択してOVAファイルを選択し、Nextを選択します。図に示すように、OVF Template DetailsページにデフォルトのOVAパラメータが表示されます。Nextを選択します。


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.

vmware

Back Next Finish Cancel

## 管理インターフェイスの初期設定


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.

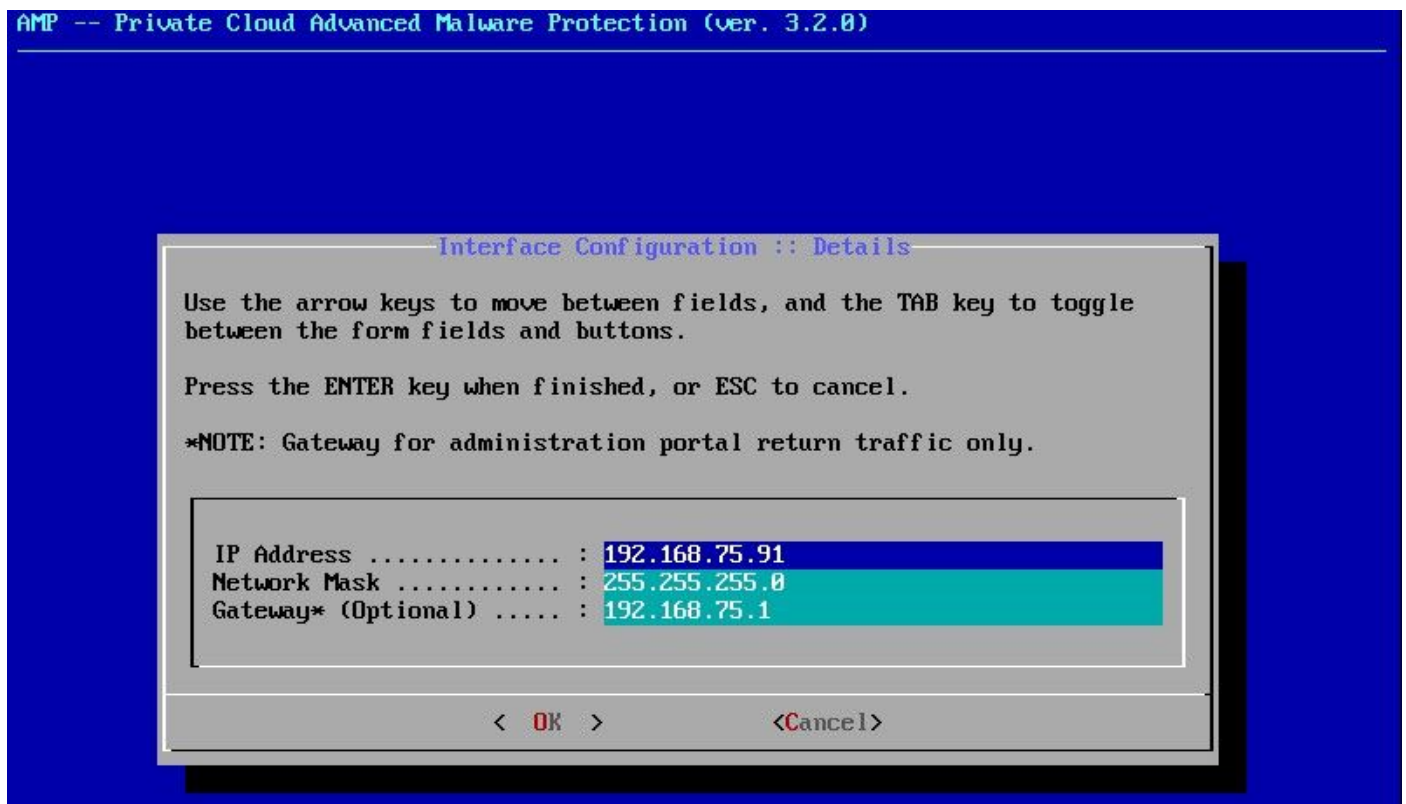
vmware

Back Next Finish Cancel

VMが起動したら、VMコンソールから初期設定を行います。

## ステップ 1 :

インターフェイスがDHCPサーバからIPアドレスを受信しなかった場合、URLに [UNCONFIGURED]と表示されることがあります。このインターフェイスは「管理」インターフェイスであることに注意してください。これは実稼働インターフェイスではありません。



## ステップ 2 :

Tab、Enter、および矢印キーを使用して移動できます。

CONFIG\_NETWORKに移動し、キーボードのEnterキーを選択して、セキュアエンドポイントのプライベートクラウドの管理IPアドレスの設定を開始します。DHCPを使用しない場合は、Noを選択し、Enterキーを選択します。

Interface Configuration :: Mode

Would you like to configure your interface with DHCP?

< Yes >      < No >

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 ..... : PGBd~HbCgZ

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

<b>CONFIG_NETWORK</b>	<b>Configure the Web administration interface.</b>
CONSOLE	Start command line console / shell.
INFO	Display device status / information.

60%

< OK >

表示されたウィンドウでYesを選択し、Enterキーを選択します。





IPがすでに使用されている場合は、このエラーログで処理されます。単に戻って、使用されていないユニークなものを選んでください。

```
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...  
-
```

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

< OK >                      <Cancel>

すべてがうまくいけば、次のような出力が表示されます

```

- 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
* templated[etc/ssh/sshd_config] action create
- update content in file /etc/ssh/sshd_config from c85f41 to badlab
--- /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
* templated[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

```

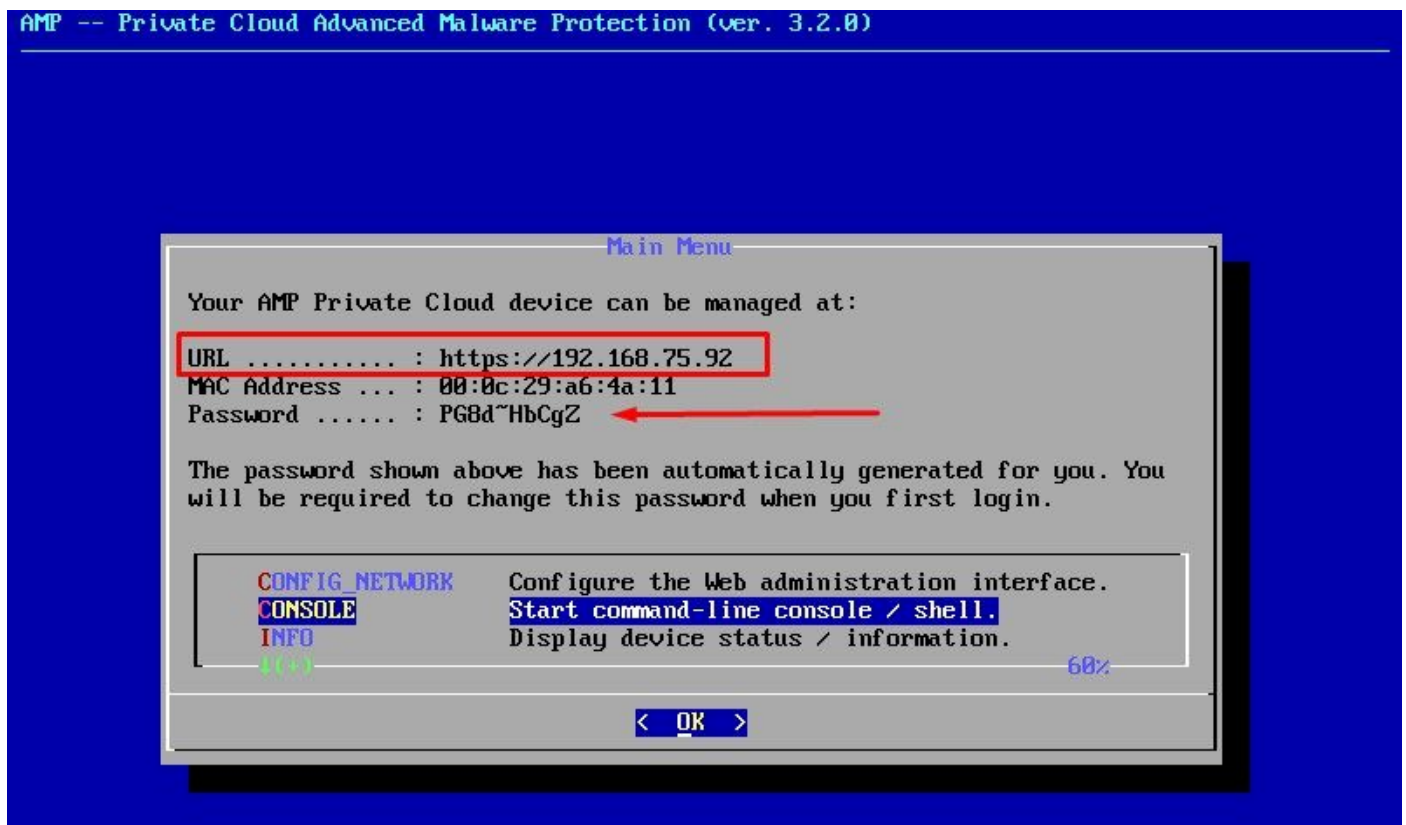
```
Restarting eth0...
```

```
Reconfiguring...
```

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

### ステップ 3 :

新しいSTATIC IPでブルースクリーンが再び表示されるまで待ちます。また、ワンタイムパスワードにも注意してください。メモを取り、ブラウザを開きましょう。

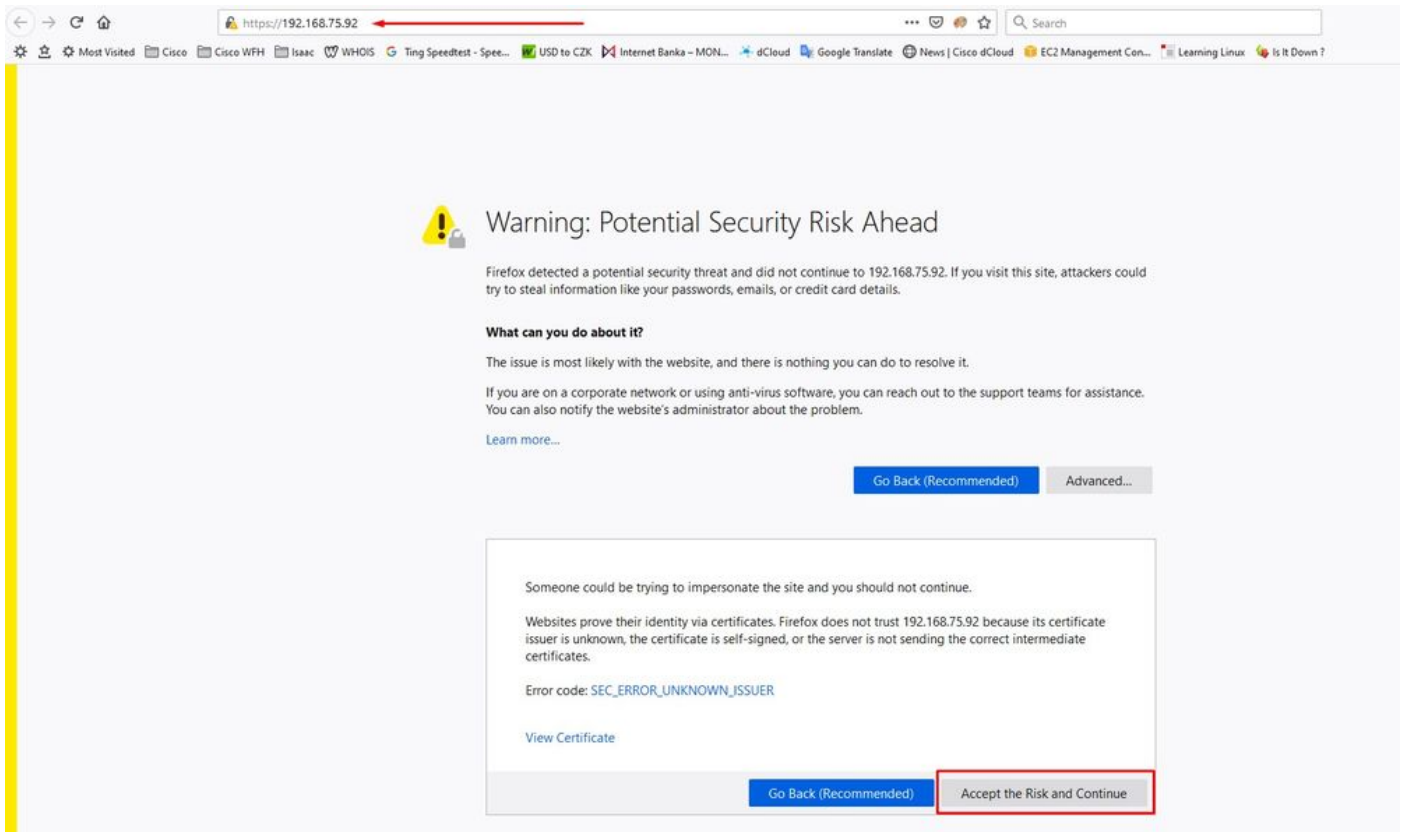


## Web GUIによるvPCの初期設定

### ステップ 1 :

Web ブラウザを開き、アプライアンスの管理 IP アドレスに移動します。図に示すように、Secure Endpoint Private Cloudが最初に独自のHTTPS証明書を生成すると、証明書エラーを受け取る場合があります。Secure Endpoint Private Cloudの自己署名HTTPS証明書を信頼するようにブラウザを設定します。

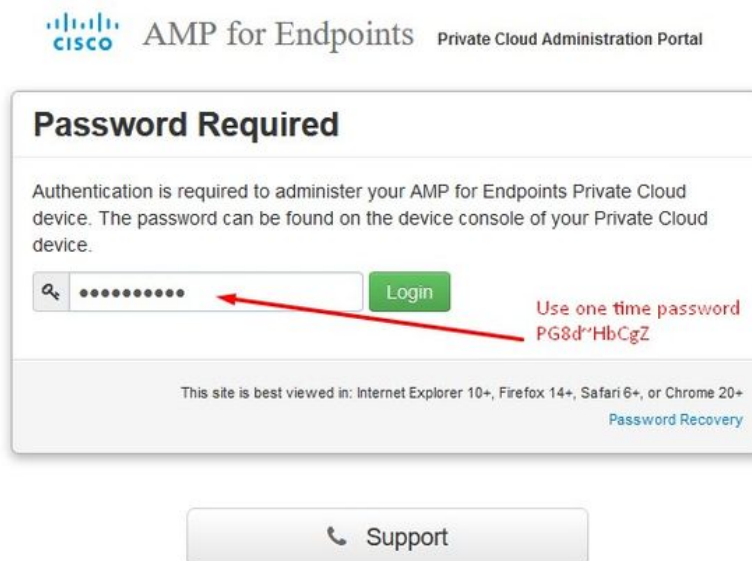
ブラウザで、先ほど設定したSTATIC IPを入力します。



## ステップ 2 :

ログイン後、パスワードをリセットする必要があります。コンソールのOld Passwordフィールドにある初期パスワードを使用します。New Passwordフィールドに新しいパスワードを入力します。New Passwordフィールドに新しいパスワードを再入力し、Change Passwordを選択します

。



## ステップ 3 :

ログイン後、パスワードをリセットする必要があります。コンソールのOld Passwordフィールドにある初期パスワードを使用します。New Passwordフィールドに新しいパスワードを入力します。New Passwordフィールドに新しいパスワードを再入力し、Change Passwordを選択します。

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. A yellow warning banner at the top left reads 'Password Expired' with a red arrow pointing to it. Below the banner, a message states: '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.' A 'Warning' box below this message explains that the device password is used for authentication and that complex passwords may not be pasted into the console. The password change form consists of three input fields: the first is labeled 'Old one time password', the second is for the new password, and the third is for the confirmation password. A green 'Change Password' button is located at the bottom of the form.

ステップ 4 :

次のページで、下までスクロールしてライセンス契約に同意します。[読み取りと同意]を選択します。



ステップ 5 :

契約に同意すると、図に示すようにインストール画面が表示されます。バックアップから復元する場合は、ここで行うことができませんが、このガイドでは「クリーンインストール」オプションを使用します。Clean Installationセクションでon Startを選択します。

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

# Install or Restore

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

## Clean Installation

Start > ←

## Restore

Local Remote Upload

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

+ Choose Restore File

/data

Start >

ステップ 6 :

最初に必要なのは、さらに前進するためのライセンスです。ライセンスとパスフレーズは、製品購入時に受け取ります。+Upload License Fileを選択します。ライセンスファイルを選択し、パスフレーズを入力します。Upload Licenseを選択します。アップロードが失敗した場合は、パスフレーズが正しいかどうかを確認してください。アップロードが成功すると、有効なライセンス情報を含む画面が表示されます。Nextを選択します。それでもライセンスをインストールできない場合は、シスコ テクニカル サポートに問い合わせてください。

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License

# License

Device ID  
EG[REDACTED]V5

License  
No license has been installed.

Install New License

license + Upload License File

.....

Upload License

License was successfully uploaded

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server

# License

**Device ID**  
E60[REDACTED]/5

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

Replace License [\(click to expand\)](#)

Next >

手順 7 :

図に示すように、ウェルカムページが表示されます。このページには、プライベートクラウドを設定する前に必要な情報が表示されます。要件を注意深く読みます。Nextを選択して、インストール前の設定を開始します。

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

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

# 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.

Next >

## コンフィギュレーション

### ステップ 1 :

注 : 次のスライドでは、図に示すように、AIR GAPモードに固有の排他的な部分が含まれています ( 図を参照 )。これらはAIRGAP ONLYとして囲み、マークする必要があります





Installation Options

Only the License section can be altered after installation.

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

Configuration

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

# Deployment Mode

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

**Cloud Proxy**

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

**Standalone**

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

≡ ≡ AIRGAPのみ ≡ ≡



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

# Deployment Mode

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

**Cloud Proxy**

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

**Standalone**

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

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

## 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.

[Air Gap](#)

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

≪ ≪ AIRGAPのみ ≪ ≪

ステップ 2 :

Secure Endpoint Console Accountページに移動します。管理ユーザーは、ポリシー、コンピューターグループの作成、およびユーザーの追加を行うためにコンソールで使用されます。コンソールアカウントの名前、電子メールアドレス、およびパスワードを入力します。Nextを選択します

。

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 ✓

## 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	.....	
	.....	

Next >

OVAファイルから導入するときこの問題が発生する場合は、2つの選択肢があります。続行して後でこの問題を修正するか、または導入したVMに合わせてシャットダウンしてから調整します。再起動後は、そのまま続行します。

注：バージョン3.5.2のOVAファイルでは、128 GB RAMおよび8 CPUコアで正常にロードされるため、この問題は修正されています

**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.

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

**Shutdown** [I understand the risks](#)

注：ラボ目的でない限り、推奨値のみを使用してください

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

Virtual Hardware | VM Options

8 CPU | 131072 MB Memory

It will work with 48Gb as well

再起動したら、残った場所に移動します。



## 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 Met


Your current configuration meets or exceeds the hardware requirements.

#### Hardware Configuration

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

[Next >](#)

ETH1にもスタティックIPが設定されていることを確認します。

 注：インターフェイスのMACアドレス予約を作成していない限り、DHCPを使用するようにデバイスを設定しないでください。インターフェイスのIPアドレスが変更されると、展開されているセキュアエンドポイントコネクタに重大な問題が発生する可能性があります。DNSサーバが設定されていない場合は、パブリックDNS一時を使用してインストールを完了できます。

ステップ 3 :

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
- > Firewall Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

# Network Configuration

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

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

IP Assignment 192.168.75.92 [More details](#)

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

IP Assignment 192.168.75.209 [More details](#)

IP Assignment Static ←

IP Address 192.168.75.93

Check for IP Address conflicts

Subnet Mask 255.255.255.0

Gateway 192.168.75.1

**DNS**

Primary DNS Server 8.8.8.8 ← Use public DNS temporary.

Secondary DNS Server

Next (Applies Configuration) ▶

ステップ 4 :

日付と時刻のページが表示されます。日付と時刻の同期に使用する1つ以上のNTPサーバのアドレスを入力します。内部または外部のNTPサーバを使用し、カンマまたはスペースで区切られたリストを使用して複数のNTPサーバを指定できます。ブラウザで時刻を同期するか、デバイスコンソールからamp-ctl ntpdateを実行して、NTPサーバとの時刻の即時同期を強制します。Nextを選択します。

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

## Date and Time

### NTP Servers

192.168.75.254 ← Optional  Verify hostname resolution

### Current System Time

2021 / 4 / 10  
 8 : 17 : 24 UTC  
 Set by NTP

Next >

≪ ≪ AIRGAPのみ ≫ ≫

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

## Prepare amp-sync

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

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

[Download amp-sync](#)

Next >

≪ ≪ AIRGAPのみ ≫ ≫

ステップ 5 :

図に示すように、Certificate Authoritiesページが表示されます。Add Certificate Authorityを選択して、ルート証明書を追加します。

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 ✓

## Certificate Authorities

Add Certificate Authority

No certificate authorities have been uploaded to this device.

Next >

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓

## 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 + Add Certificate Root

Cancel Upload

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 ✓

## Certificate Authorities

Add Certificate Authority

Certificate		(click to collapse)
Issuer	AMP-vPC	Download
Subject	AMP-vPC	
Validity	2021-04-09 16:28:00 UTC - 2031-04-09 16:28:00 UTC	Delete

Next >

ステップ 6 :

次のステップは、図に示すように、Cisco Cloudページを設定します。適切なCisco Cloud Regionを選択します。Secure Endpoint Private CloudデバイスがCisco Cloudと通信してファイル

検索やデバイス更新を行うためにファイアウォール例外を作成する必要がある場合は、View Hostnamesを展開します。Nextを選択します。

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes the Cisco logo, 'AMP for Endpoints', 'Private Cloud Administration Portal', and links for 'Support', 'Help', and 'Logout'. Below this is a secondary navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. The left sidebar contains 'Installation Options' and 'Configuration' sections, both with expandable sub-items. The main content area is titled 'Cisco Cloud' and contains 'Cisco Cloud Configuration' and 'Cisco Cloud Identity' sections. The 'Region' dropdown is set to 'Cisco Cloud, North America'. Below it is a 'View Hostnames (click to expand)' button. The 'Client Identity' section shows a partially obscured ID: '0f476ea8[REDACTED]dbbc272a6c'. A green 'Next >' button is highlighted with a red box at the bottom right of the configuration area.

手順 7 :

図に示すように、通知ページに移動します。重要な通知と通常のお知らせの頻度を選択します。セキュアエンドポイントデバイスのアラート通知を受信する電子メールアドレスを入力します。電子メールエイリアスを使用するか、カンマ区切りリストを使用して複数のアドレスを指定できます。また、デバイスで使用される送信者名と電子メールアドレスを指定することもできます。これらの通知は、Secure Endpoint Consoleサブスクリプションとは異なります。複数のSecure Endpoint Private Cloudデバイスがある場合は、一意のデバイス名を指定することもできます。Nextを選択します。



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

## Notifications

### Notification Frequency

Critical Notification Frequency	HELP	Every 5 Minutes
Notification Frequency	HELP	Every Week

### Notification Addresses

Notification Recipients	HELP	rv[REDACTED]om
Notification Sender Address	HELP	donotreply@cisco.com
Notification Sender Name	HELP	AMP for Endpoints Device

### Device Name

Device Name	HELP	CyberNet vPC 2
-------------	------	----------------

Next >

### ステップ 8 :

次に、図に示すように、SSHキーページに移動します。Add SSH Keyを選択して、デバイスに追加する公開キーを入力します。SSHキーを使用すると、root権限を持つリモートシェル経由でデバイスにアクセスできます。アクセス権を付与できるのは、信頼できるユーザのみです。プライベートクラウドデバイスには、OpenSSH形式のRSAキーが必要です。後で、管理ポータル(Configuration > SSH)を使用して、SSHキーをさらに追加できます。Nextを選択します。

Maintenance Mode

Sanity Check Failing

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.

Add SSH Key

## 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 AAAAE2K...oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7QGfd0g4vT9eD5XOXZd
I4DKhrTNBv8/77T0d/Jagx7Przxs=
```

次に、サービスセクションが表示されます。次のページでは、ホスト名を割り当て、これらのデバイスサービスに適切な証明書と鍵のペアをアップロードする必要があります。以降のスライドでは、6つの証明書のうちの1つの設定について説明します。

## サービス

ステップ 1:

設定プロセス中に、次のエラーが発生する場合があります。

最初に気付く「エラー」は、3つの矢印で強調表示されています。これを回避するには、単に「厳密なTLSチェックを無効にする」をオフにします

**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

Validate DNS Name

**Authentication Certificate**  Disable Strict TLS Check Undo Replace Certificate

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

+ Choose Key

+ Choose Certificate

[Next >](#)

厳密なTLSチェックなし

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

vPC2-Authentication.cyberworld.local  Validate DNS Name

Authentication Certificate

Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	vPC2-Authenticat + Choose Key
<input checked="" type="checkbox"/> Certificate matches hostname.	vPC2-Authentication.cyberworld.local.pem
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
vPC2-Authenticat + Choose Certificate	vPC2-Authentication.cyberworld.local.crt

Next >

ステップ 2 :

次に表示されるエラーは、「Validate DNS Name」にチェックマークを付けたままにすることです。ここでは2つの選択肢があります。

#1: 「DNSの検証」チェック・マークをオフにします。

#2: DNSサーバーに戻り、残りのホストレコードを構成します。

An error occurred while processing your request.

• Hostname does not resolve

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)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	

Next >

残りの証明書に対して、同じプロセスをさらに5回繰り返します。

[Authentication]

- 認証サービスは、今後のバージョンのプライベートクラウドでユーザ認証の処理に使用される予定です。

セキュアなエンドポイントコンソール

- Consoleは、セキュアエンドポイント管理者がセキュアエンドポイントコンソールにアクセスでき、セキュアエンドポイントコネクタが新しいポリシーと更新を受信できるDNS名です。

評価サーバー

- Disposition Serverは、Secure Endpoint Connectorがクラウドルックアップ情報を送信および取得するDNS名です。

Disposition Server – 拡張プロトコル

- Disposition Server - Extended Protocolは、新しいセキュアエンドポイントコネクタがクラウドのバックアップ情報を送信および取得するDNS名です。


## 廃棄更新サービス

- Disposition Update Serviceは、Cisco Threat Gridアプライアンスをプライベートクラウドデバイスにリンクするときに使用されます。Threat Gridアプライアンスは、分析用のファイルをSecure Endpoint Consoleから送信するために使用されます。また、Threat Gridは、分析後にファイルの廃棄(クリーンまたは悪意のある)を更新するために廃棄更新サービスを使用します。

## Firepower Management Center

-Firepower Management Centerリンクを使用すると、シスコのFirepower Management Center(FMC)デバイスをプライベートクラウドデバイスにリンクできます。これにより、FMCダッシュボードにセキュアエンドポイントのデータを表示できます。Secure EndpointとのFMC統合の詳細については、FMCのマニュアルを参照してください。

---

 注意：デバイスのインストールが完了した後は、ホスト名を変更できません。

---

必要なホスト名を書き留めます。Secure Endpoint Private Cloud用に6つの一意のDNS Aレコードを作成する必要があります。各レコードは仮想プライベートクラウドコンソールインターフェイス(eth1)の同じIPアドレスを指し、プライベートクラウドとセキュアエンドポイントの両方で解決される必要があります。

### ステップ 3：

次のページで、リカバリファイルをダウンロードして確認します。

図に示すように、「リカバリ」ページが表示されます。インストールを開始する前に、設定のバックアップをダウンロードして確認する必要があります。リカバリファイルには、すべての設定とサーバキーが含まれています。回復ファイルが失われると、構成を復元できず、すべてのセキュアエンドポイントコネクタを再インストールする必要があります。元のキーがなければ、新しいキーでプライベートクラウドインフラストラクチャ全体を再設定する必要があります。リカバリファイルには、opadminポータルに関連するすべての設定が含まれています。バックアップファイルには、リカバリファイルの内容と、イベントやコネクタ履歴などのダッシュボードポータルデータが含まれています。イベントデータとすべてなしでopadminだけを復元する場合は、回復ファイルを使用できます。バックアップファイルから復元すると、opadminとダッシュボードポータルデータが復元されます。

Downloadを選択して、バックアップをローカルコンピュータに保存します。ファイルがダウンロードされたら、Choose Fileを選択してバックアップファイルをアップロードし、破損していないことを確認します。Nextを選択してファイルを確認し、次に進みます。

- > 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 ✓

## 1. Download Recovery File

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

[Download](#)

## 2. Verify Recovery File

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

[Browse...](#) pre-install-backup.bak

Recovery File Ready for Download  
created less than a minute ago

[Next >](#)



### Installation Options

Only the License section can be altered after installation.

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

### Configuration

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

### Services

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

### Other

- > Recovery ✓
- > Review and Install ✓

[▶ Start Installation](#)

## Review and Install

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

### Clean Installation

A clean installation will be performed.

#### Installation Type

[Edit](#)

#### Cloud Proxy

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

#### AMP for Endpoints Console Account

[Edit](#)

Name	Roman Valenta
Email Address	rva[REDACTED].com
Business Name	Cisco - rvalenta

#### Recovery

[Edit](#)

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

≡ ≡ AIRGAPのみ ≡ ≡

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery ✓
- > Review and Install

▶ Start Installation

# Review and Install

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

**Clean Installation**

A clean installation will be performed.

Installation Type ✎ Edit

**Standalone Air Gap** ←

- Does not require an Internet Connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates must be downloaded separately and applied to this Private Cloud device.

AMP for Endpoints Console Account ✎ Edit

Name	Roman Valenta
Email Address	rvalenta@xxxxxxxxx.com
Business Name	Cisco vamrodia PC v2

Recovery ✎ Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

≧ ≧ AIRGAPのみ ≧ ≧

次のような入力が表示されます。

**⚠ 注意：**このページを表示している場合は、更新すると問題が発生する可能性があるため、更新しないでください。



# 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.

Reboot

☰ Output

```
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 downloads.
[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
```

⬇ Download Output

インストールが完了したら、再起動ボタンを押します

# 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のみ ≫ ≫

## 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.

Reboot

Output

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

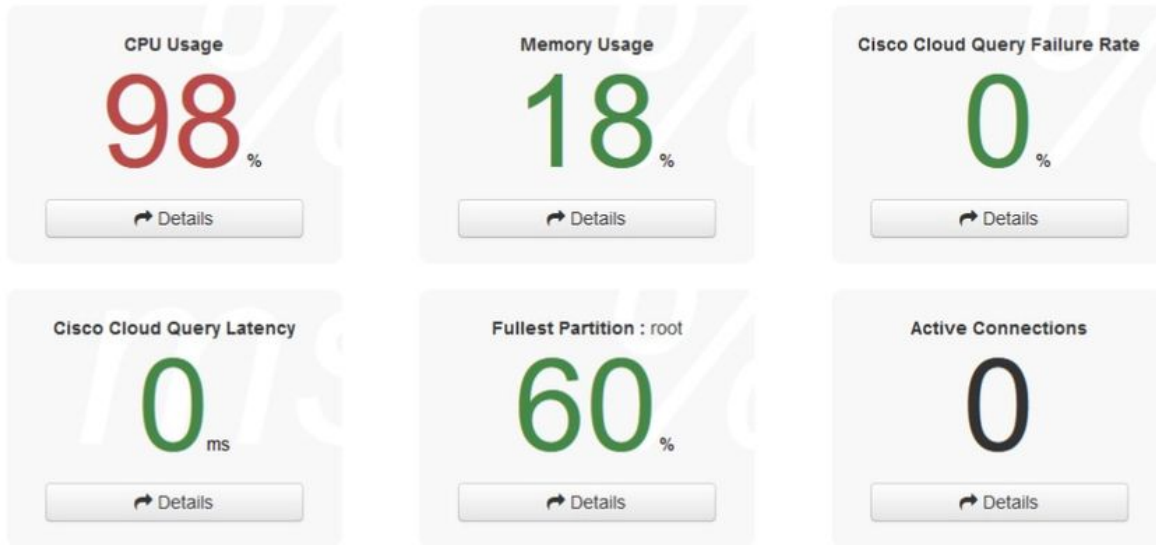
Download Output

### ⌘ ⌘ AIRGAPのみ ⌘ ⌘

アプライアンスが完全に起動すると、次に管理インターフェイスでログインしたときに、このダッシュボードが表示されます。最初はCPUの使用率が高くなっていることに気付くかもしれませんが、数分待つと安定します。



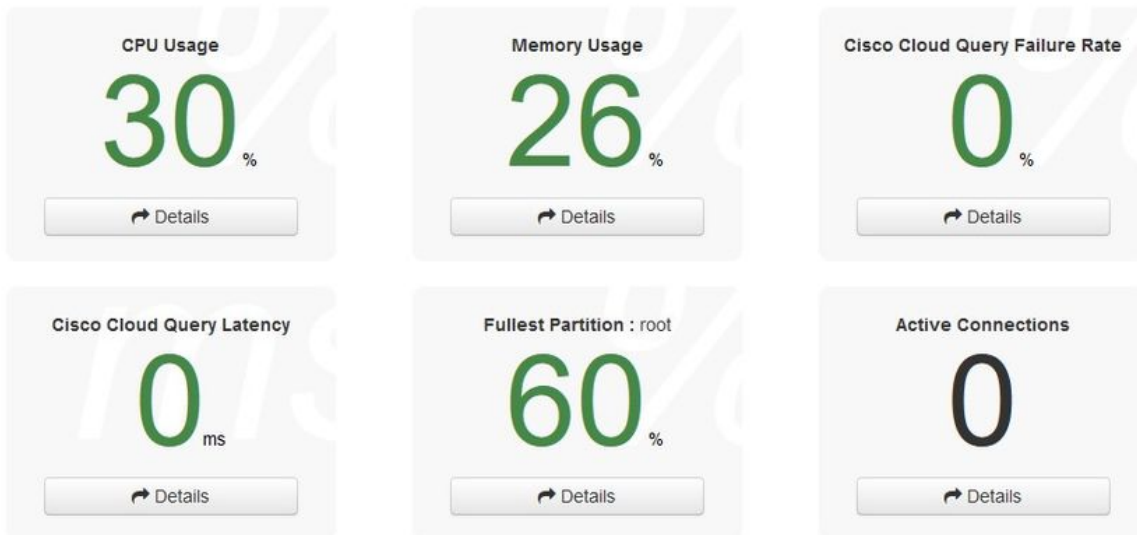
### Key Metrics



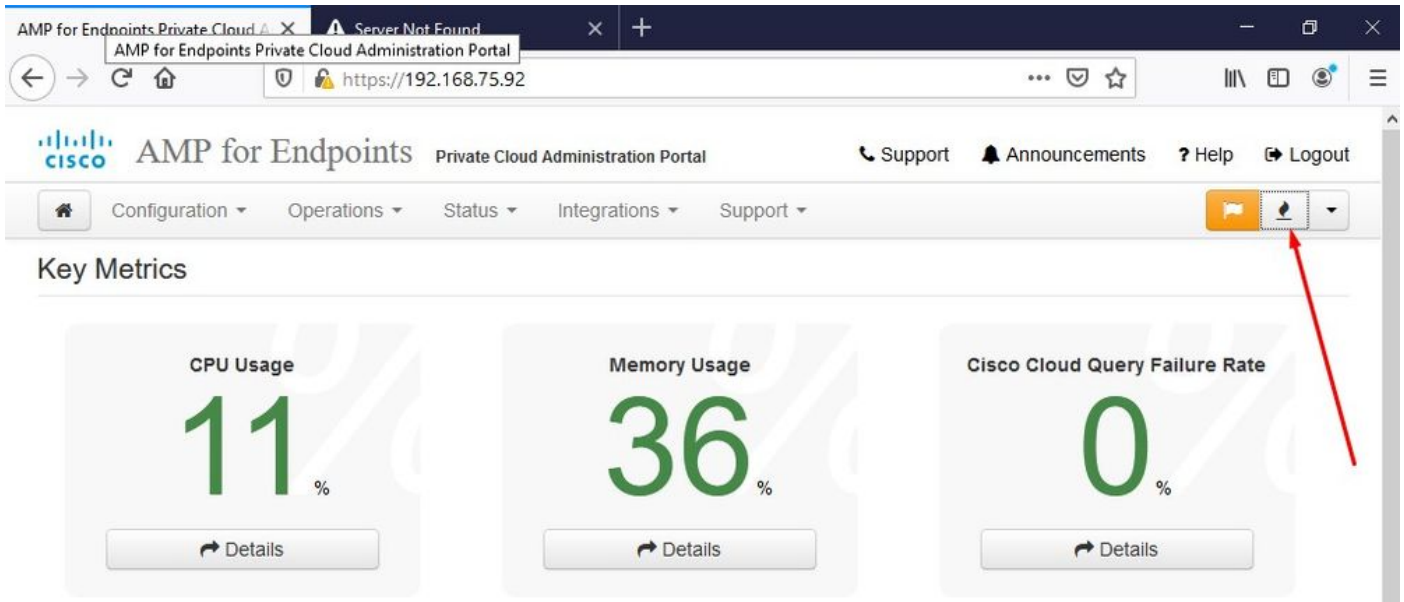
数分後...



### Key Metrics



ここから、セキュアエンドポイントコンソールに移動します。旗の隣の右隅にある火のように見える小さなアイコンをクリックします。



≪ ≪ AIRGAPのみ ≫ ≫

ご覧のように、DB Protect Snapshot ( DB保護スナップショット )、またClient Definitions、DFC、およびTetraが原因で、健全性チェックに失敗しました。これは、事前にamp-syncで作成し、VMにアップロードするか、NFSロケーションに保存したダウンロード済みISOファイルによるオフライン更新で行う必要があります。



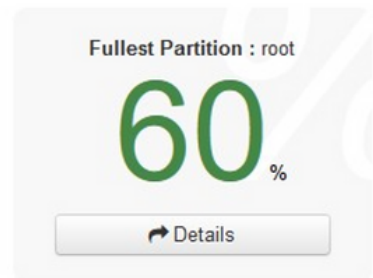
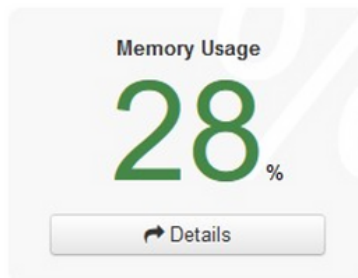
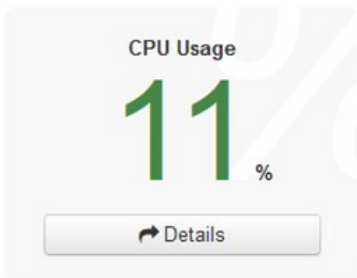
### Sanity Check Failing

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

#### Details

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





✖ Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

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

## Content

✖ 3.2.0\_202010081917

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

! 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


Update Software

Checked 1 minute ago; the update check failed.

## AirGapアップデートパッケージ

保護DBを受信するには、このコマンドを初めて使用する必要があります

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

 注：このコマンドを使用してすべてのパッケージをダウンロードし、24時間以上かかることを確認します。速度とリンク品質によって異なります。私の場合、1ギガビットファイバの場合は、完了までまだ25時間近くかかります。これは、このダウンロードがAWSから直接行われるため抑制されるためです。最後に、このダウンロードはかなり大きいことに注意してください。私の場合、ダウンロードされたファイルは323GBでした。

この例では、CygWin64を使用しています

1. Cygwinのx64バージョンをダウンロードしてインストールします。
2. setup-x86\_64.exeを実行し、インストールプロセスを実行してすべてのデフォルトを選択します。
3. ダウンロードミラーを選択します。
4. インストールするパッケージの選択：

All -> Net -> curl

All -> Utils -> genisoimage

All -> Utils -> xmlstarlet

\* VPC 3.8.x アップ -> xorriso

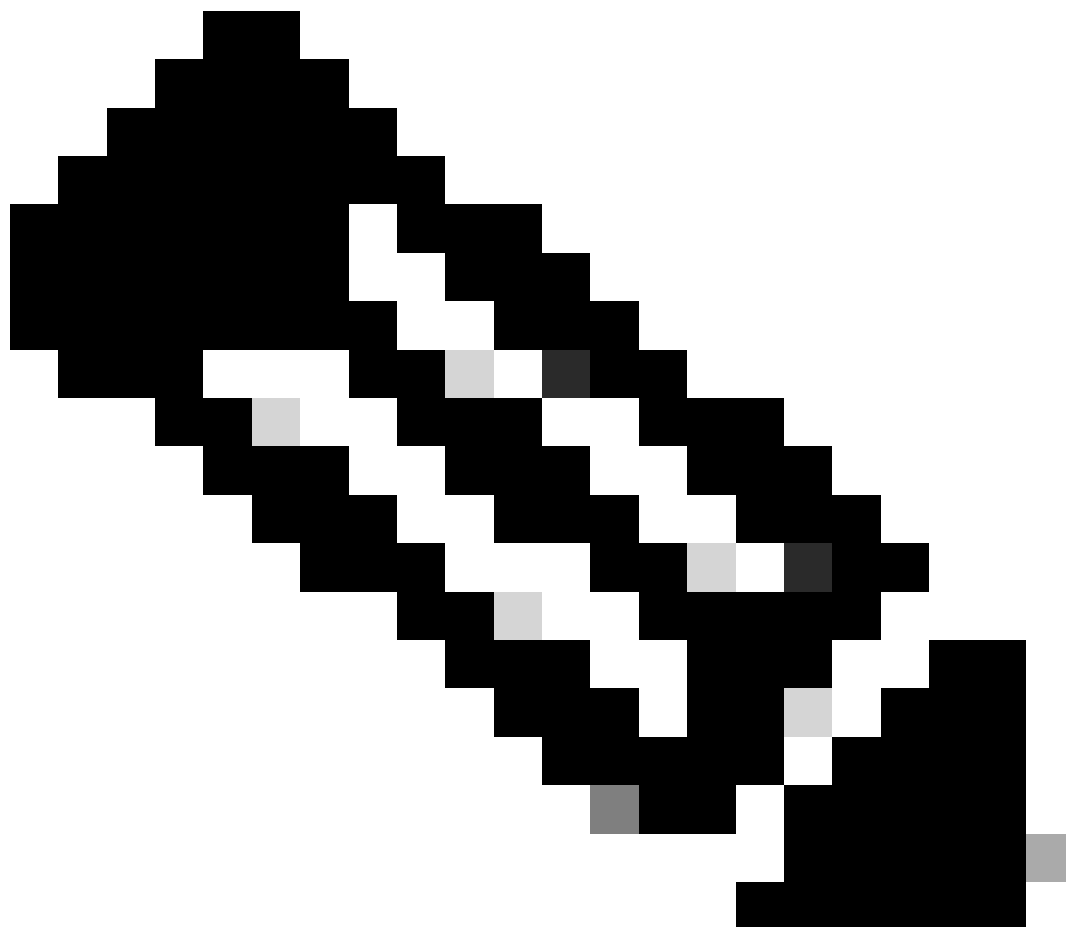
```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD 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/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-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/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-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/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-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/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-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 08:39:51 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:CygWin64をメインダウンロードツールとして使用する最新のアップデートVPC 3.8.xでは、次に説明するこの問題が発生する可能性があります。

---

```
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.
```

[リリースノート](#) ページ#58 ご覧のとおり、「xorriso」が必要です。ISOのフォーマットをISO 9660に変更しました。この依存関係によって、イメージが適切なフォーマットに変換され、更新が完了します。残念ながら、CygWin64は組み込みリポジトリにxorrisoを提供していません。しかし、まだCygWin64を使用したい人のために、この問題を克服する方法があります。

# 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

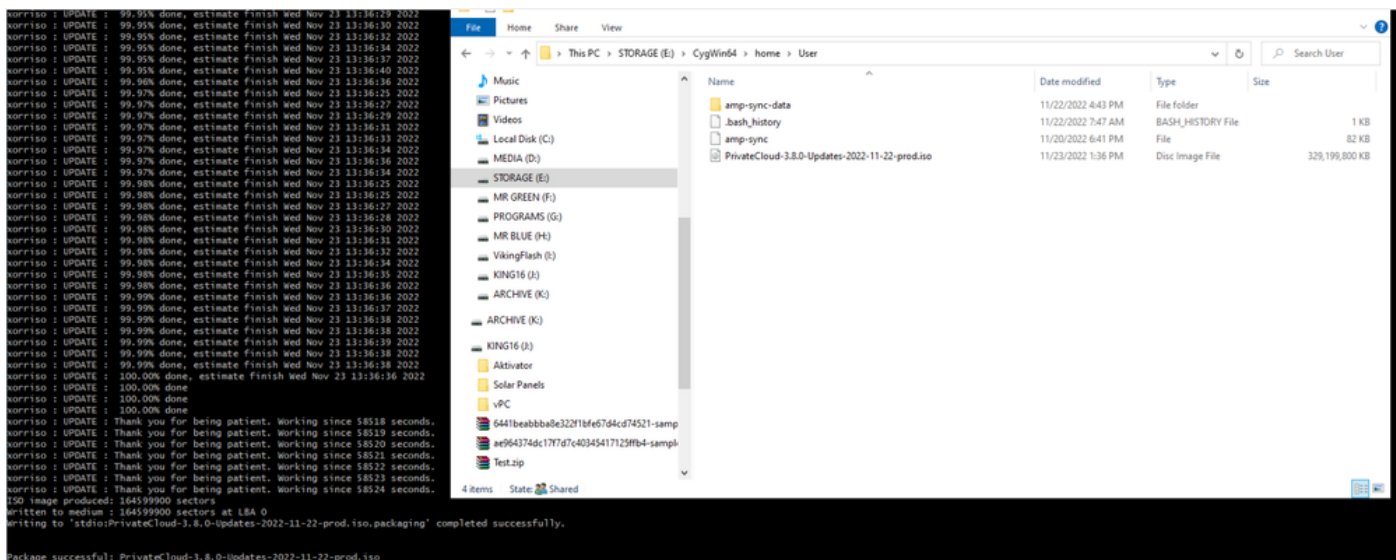
To run amp-sync you will first have to install xorriso and xmlstarlet.

- 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`

CygWinをもう一度使用できるようにするには、GitHubリポジトリからxorrisoを手動でダウンロードする必要があります。ブラウザを開き、「Latest xorriso.exe 1.5.2 pre-build for Windows」と入力します。最初のリンクは<PeyTy/xorriso-exe-for-windows - GitHub>です。そのGitHubページに移動し、<xorriso.exe>という名前の他のファイルの中にある<xorriso-exe-for-windows-master.zip>ファイルをダウンロードします。ローカルCygWinインストールのパス。<amp-sync>コマンドを再実行してください。次の図に示すように、エラーメッセージとダウンロードの開始と終了が表示されなくなります。



Airgapモードで現在の（この場合）3.2.0 VPCのバックアップを実行します。

このコマンドはCLIから使用できます

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

または、図に示すようにOperations > Backupsの順に移動し、そこでPerform Backupを選択することもできます。



Sanity Check Failing

Backups create a copy of your configuration and databases.

### Manual Backup

Perform 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.

Backup Job Details

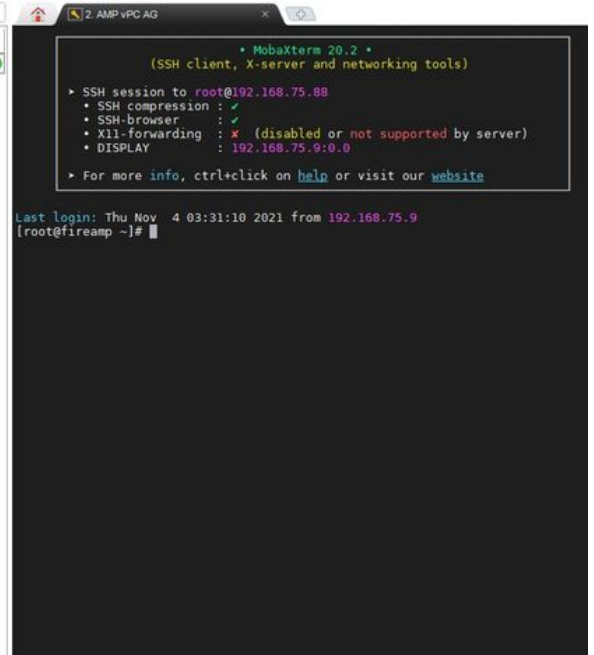
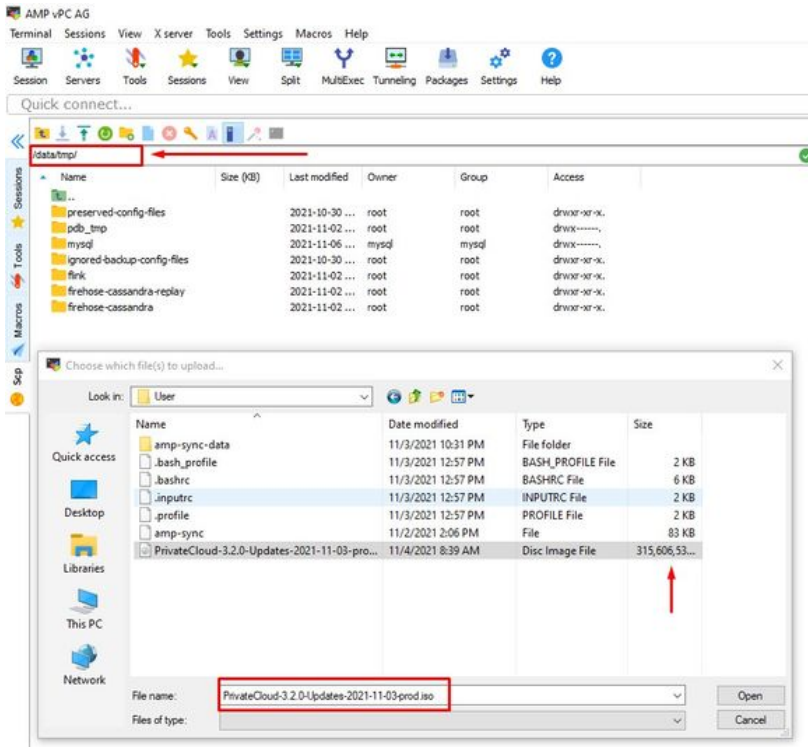
### Previous Backups

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	 

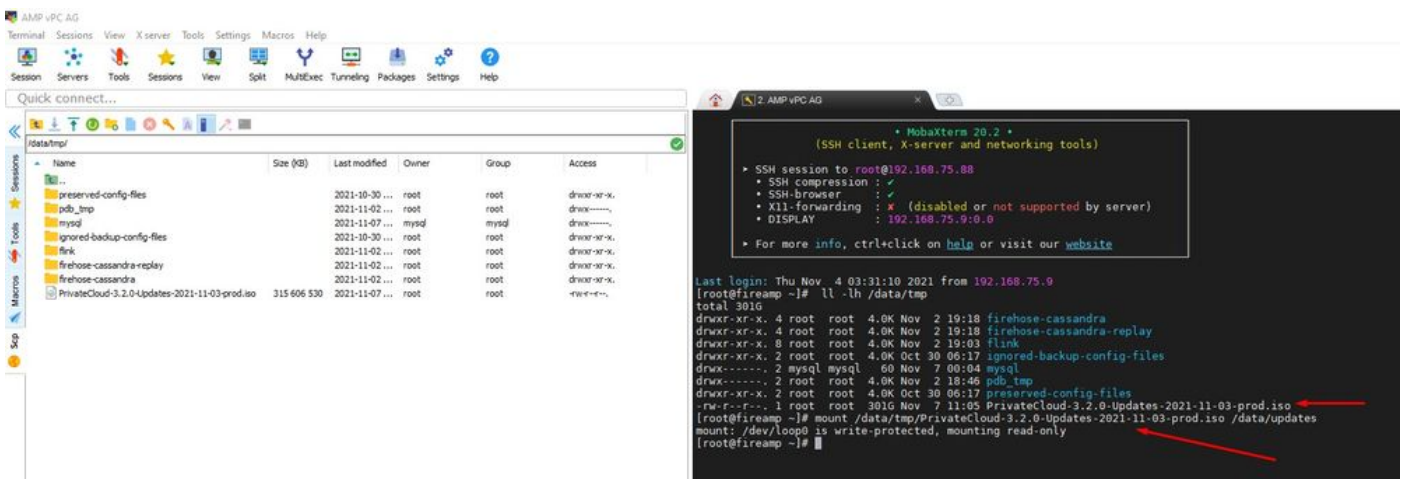
amp-syncで生成された最新のISOをVPCに転送します。速度によっては、数時間かかる場合もあります。この場合、転送には16時間かかりました

/data/tmp



アップロードが完了したら、ISOをマウントします

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



更新を実行するには、opdadmin UIに移動します [操作]>[デバイスの更新]>[ISOの更新の確認]を選

択します。

The screenshot displays the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, the text "AMP for Endpoints Private Cloud Administration Portal", and links for "Announcements", "Help", and "Logout". Below this is a secondary navigation bar with "Configuration", "Operations", "Status", "Integrations", and "Support" menus, along with a "Standalone" button and a user profile icon.

A red banner at the top left indicates "Sanity Check Failing". Below this, a message states "Updates keep your Private Cloud device up to date." with a "Download amp-sync" button. A "Check Update ISO" button is highlighted with a red arrow, and a status indicator shows "Checking ISO for updates...".

The "Content" section shows a version "3.2.0\_202010081917" for "Client Definitions, DFC, Tetra Content Version". It includes buttons for "Update Content" and "Import Protect DB". A red "ABSENT" status is shown for the "Protect DB Version", with a note: "Import a Protect DB snapshot to your standalone device." and a timestamp: "Checked 9 minutes ago; the update check failed."

The "Software" section shows a version "3.2.0\_202010082118" for "Private Cloud Software Version" and an "Update Software" button. A blue information icon indicates "A software update is available."

この例では、まず「コンテンツの更新」に進みます

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

### Content

3.2.0\_202010081917  
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

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

Update Software

A software update is available.

次に、Import Protect DBを選択します。



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

20211102210054  
Client Definitions, DFC, Tetra Content Version

Update Content  
Import Protect DB

ABSENT  
Protect DB Version

Import a Protect DB snapshot to your standalone device.

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

Software

3.2.0\_202010082118  
Private Cloud Software Version

Update Software

A software update is available.

これももう1つの非常に長いプロセスで、完了までに長い時間がかかることがあります。

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...

Output

```
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...
```

Download Output

## ⚙️ Protect DB importing

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

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

☰ Output

```
Extraction 14.9GB at 6.6MB/s eta: 9:28:03 0% [---]
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% [==]
```

⬇️ 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	2021-11-19 17:04:05 +0000 about 20 hours ago	⌚ Please wait...	⌚ Please wait...

☰ Output

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

## 問題#1 – データストアのスペースが使い果たされた

ここでは、2つの問題に対処できます。3.5.2より前のvPCには外部NFSストレージをマウントする機能がないため、更新ISOファイルを/data/tempディレクトリにアップロードする必要があります。私の場合、データストアは1 TBしかなかったため、部屋を飛び出してVMがクラッシュしました。つまり、バージョン3.5.2以下のAirGap VPCを正常に導入するには、データストアに少なくとも2 TBの容量が必要です

次のイメージはESXiサーバのもので、これは、VMを起動しようとしたときに、HDD上に使用可能な領域がもうないことを示します。128 GBのRAMを一時的に64 GBに切り替えることによって、このエラーから回復することができました。その後、再び起動することができました。また、このVMをシンククライアントとしてプロビジョニングする場合、シンククライアントの導入の欠点は、ディスクサイズが増加しても容量を解放しても縮小しないことです。つまり、300 GBのファイルをvPCのディレクトリにアップロードしてから削除したとします。ESXiのディスクでは、HDDの容量が300 GB少なくなっています



## 問題#2 – 古いアップデート

2<sup>nd</sup>の問題は、ソフトウェアアップデートを2<sup>nd</sup>のトライアルと同様に最初に実行した場合、3.2.0から3.5.2にアップグレードするためにVPCが必要になり、そのため3.2.0が無効になったため、元の3.2.0バージョンではなくなったため、新しいISOアップデートファイルをダウンロードする必要があったことです。

**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.

Download amp-sync

Check Update ISO

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

Content

**3.2.0\_202010081917**  
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

**ABSENT**  
Protect DB Version

Import a Protect DB snapshot to your standalone device.

The previous Protect DB import failed.

Checked 24 minutes ago; the update check failed.

Software

**3.5.3\_202111080345**  
Private Cloud Software Version

Update Software

Checked 24 minutes ago; the update check failed.

これは、ISO更新ファイルを再度マウントしようとする则表示されるエラーです。

Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Home / Operations - Update Device / Update Check Details

## 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

### Output

```
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 ask them to fix the problem
```

Download Output

次の図は、アップデートイメージをVPCにマウントする別の方法を示しています。バージョン 3.5.xでは、NFSストレージなどのリモートロケーションを使用して、アップデートファイルをVPCと共有できます。



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

### Mount an Update ISO

#### ISO Configuration

HELP

Mount Type

- ISO
- ISO
- NFS4
- NFS3

### Mount Status

No ISO mounted



Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

### Mount an Update ISO

#### ISO Configuration

HELP

Mount Type

NFS3

Remote Share

192.168.75.4:/AMPAG

Remote ISO File

PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Mount

### 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.

Download amp-sync

Check Update ISO

### Content

3.5.2\_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content  
Import Protect DB

**ABSENT**

Protect DB Version

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

A content update is available.

### Software

3.5.2\_202110130433

Private Cloud Software Version

Update Software

A software update is available.

健全性チェックの失敗は、現在VPCで使用できない保護データベースに関連しています



AMP for Endpoints

Private Cloud Administration Portal

Announcements Help Logout

Configuration Operations Status Integrations Support

Standalone

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

### Content

3.5.2\_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content  
Import Protect DB

**ABSENT**

Protect DB Version

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

A content update is available.

### Software

3.5.2\_202110130433

Private Cloud Software Version

Update Software

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...

☰ Output

```
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).
```

⬇️ Download Output



## ✔ 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).
```

Download Output

次の更新が自動的に開始されます



## ⚙ 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



Protect DB

20211116-2135

*Queued Protect DB Update Version*

20210531-0613

0.80%

*Update Progress*

この非常に長いインポート保護DBデータベースのプロセスの後、クライアント定義とソフトウェアを移動および更新できます。この処理には約3時間以上かかる可能性があります。

## ✔ 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

### Output

```
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!
Repdata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
--> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
--> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
--> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
--> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
```

Download Output

そして最後に完了しました、このプロセスは非常に長い時間がかかることに注意してください。

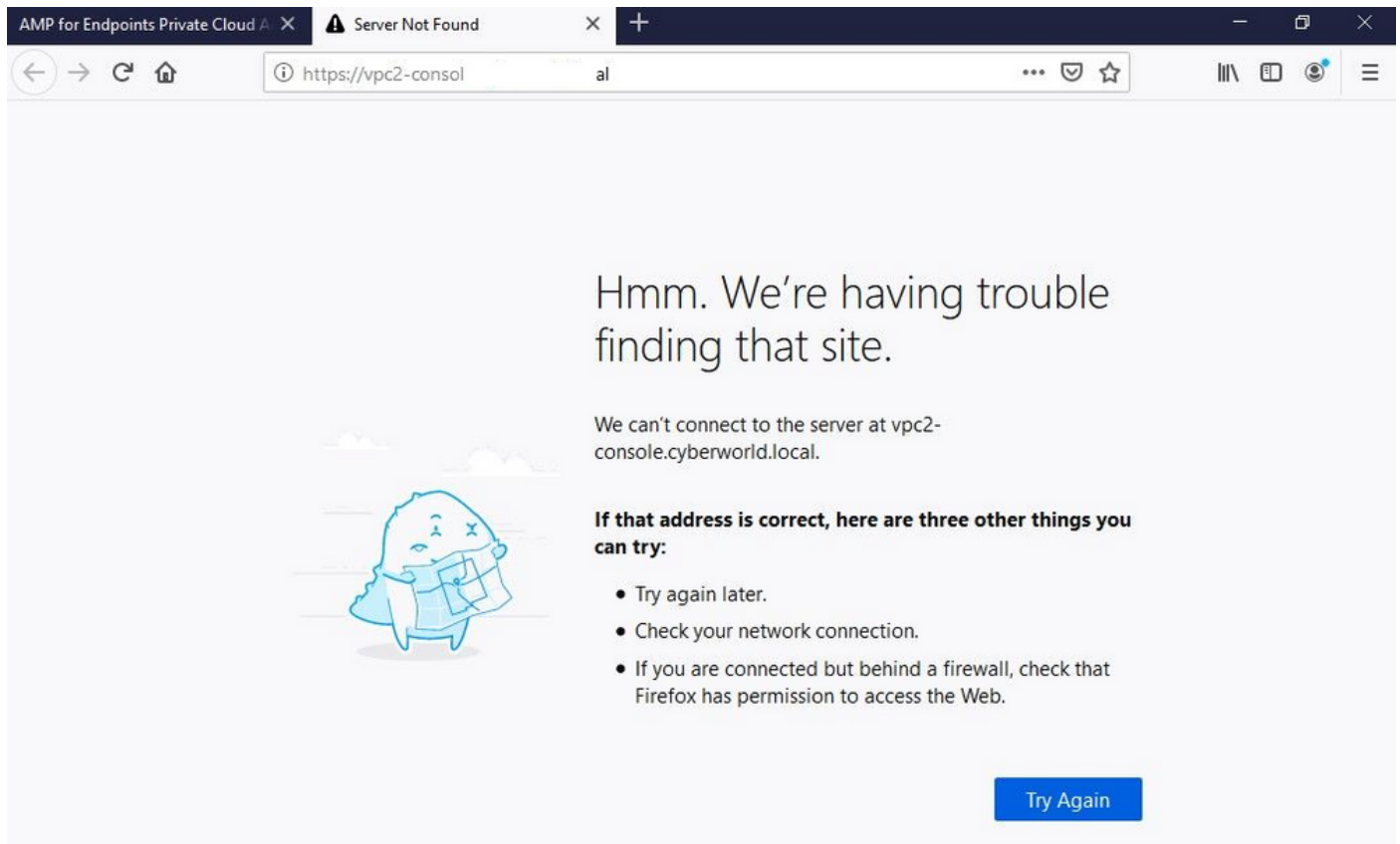
VPCアプライアンスについては、このTZにアクセスしてください。このTZには、HWアプライアンスのアップデート、ISOファイルのマウント、およびUSBからのブートを行う他の方法が含まれています。

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

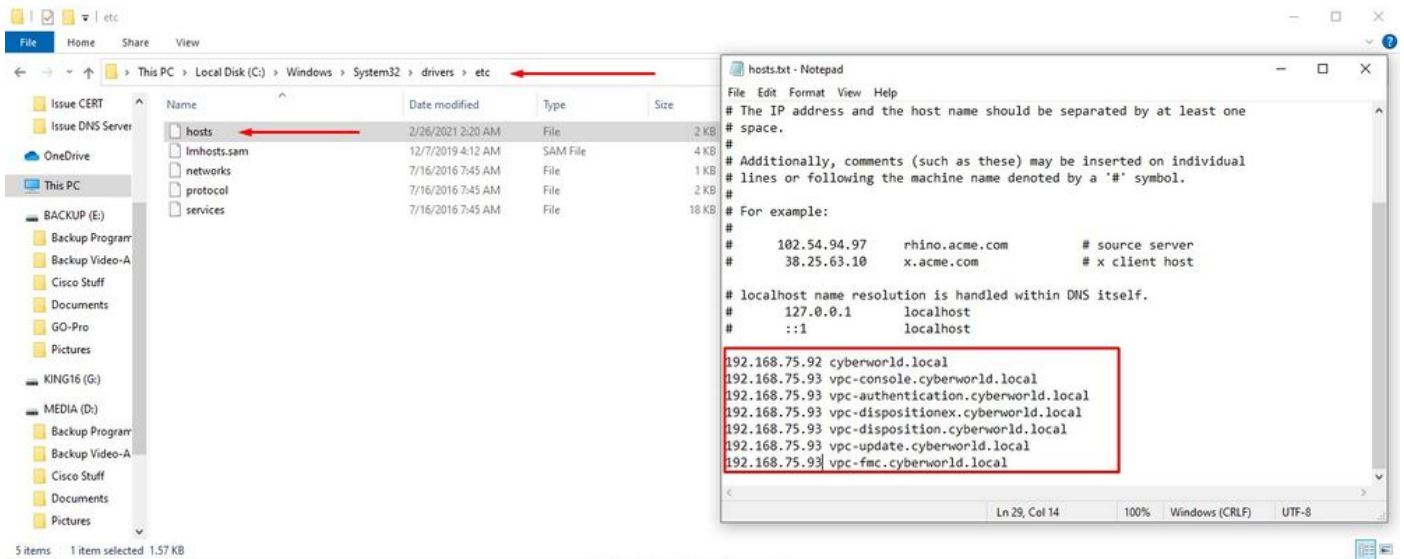
# 基本的なトラブルシューティング

## 問題#1 - FQDNとDNSサーバ

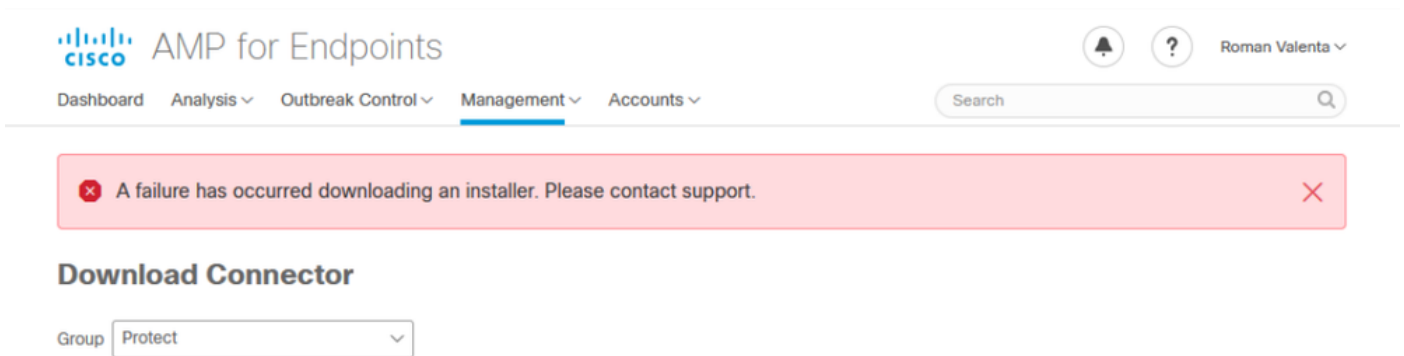
最初に発生する可能性のある問題は、DNSサーバが確立されておらず、すべてのFQDNが正しく記録および解決されていない場合です。セキュアエンドポイントの「fire」アイコンを使用してセキュアエンドポイントコンソールに移動しようとする時、問題が次のように表示される場合があります。IPアドレスだけを使用すると機能しますが、コネクタをダウンロードできません。3rdの図を見ればわかるように、下に示します。



次の図に示すようにローカルマシンのHOSTSファイルを変更すると、問題が解決し、エラーが発生しません。



Secure Endpoint Connectorインストーラをダウンロードしようとする時、このエラーが発生します。



トラブルシューティングを行った後の唯一の正しい解決策は、DNSサーバをセットアップすることでした。

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

DNSサーバにすべてのFQDNを記録し、仮想プライベートクラウドのレコードをパブリックDNSからDNSサーバに変更すると、すべてが想定どおりに動作し始めます。



### Configuration network settings.

- Device Summary
- Change Password
- Cisco Cloud
- Network**
- Date and Time
- Certificate Authorities
- Proxy
- Notifications
- License
- Email
- Backup
- SSH
- Syslog
- Updates
- Services

Admin	eth0 / 00:0C:29:A6:4A:11
	IP Assignment 192.168.75.92 <a href="#">More details</a>
Interface	eth1 / 00:0C:29:A6:4A:1B
	IP Assignment 192.168.75.93 <a href="#">More details</a>
	IP Assignment <input type="text" value="Static"/>
	IP Address <input type="text" value="192.168.75.93"/>
	<input checked="" type="checkbox"/> Check for IP Address conflicts
	Subnet Mask <input type="text" value="255.255.255.0"/>
	Gateway <input type="text" value="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 <input type="text" value="192.168.75.4"/>



#### Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.



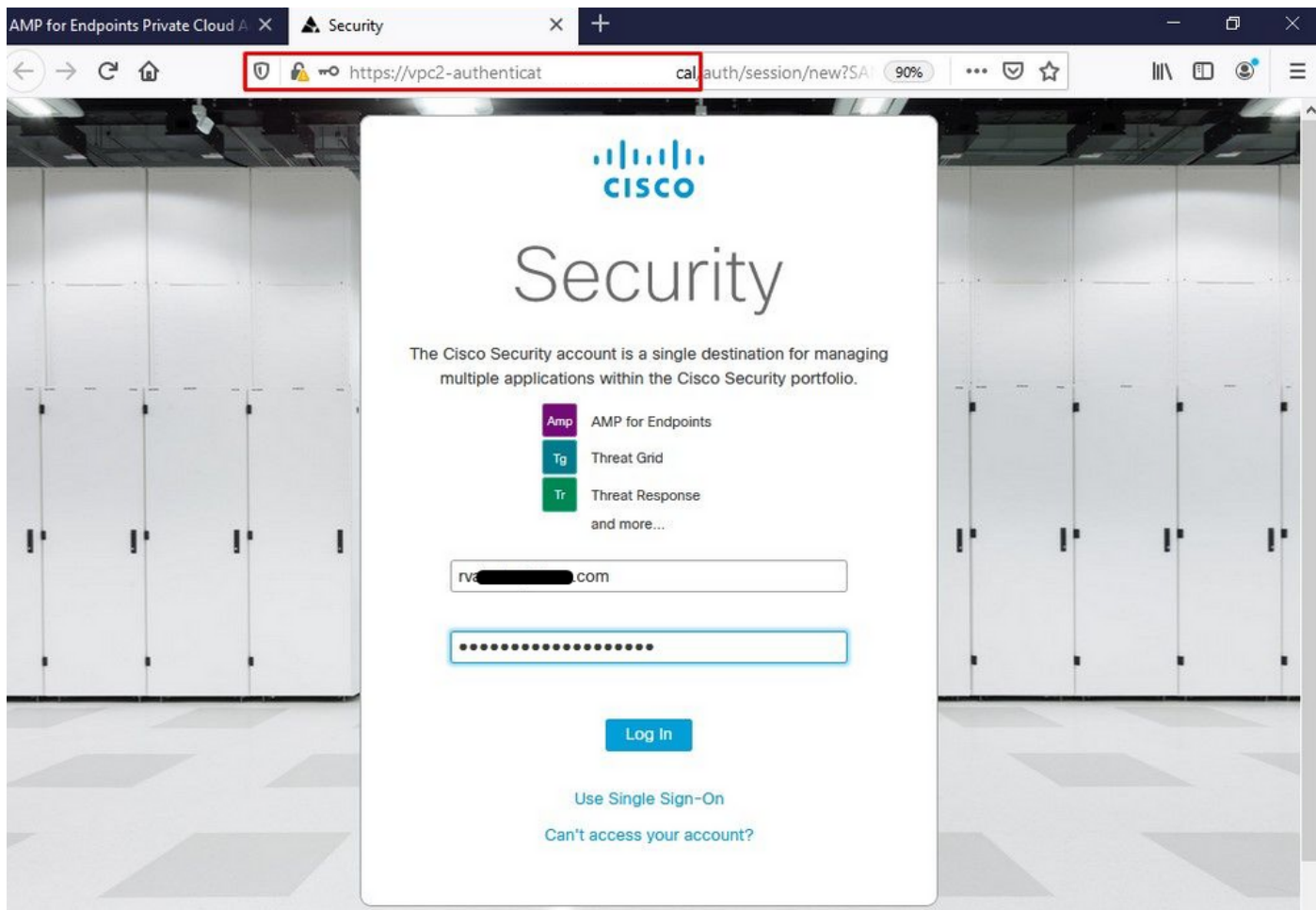
State	Started	Finished	Duration
	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

**Output**

```
[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
```

[Download Output](#)

この時点で、ログインしてコネクタをダウンロードできます



環境内の最初のセキュアエンドポイントポリシーウィザードが表示されます。ここでは、使用するアンチウイルス製品（存在する場合）、プロキシ（存在する場合）、および導入するポリシーのタイプを順を追って説明します。コネクタのOSに応じて、適切な[Set Up...]ボタンを選択します。

図に示すように、Existing Security Productsページが表示されます。使用するセキュリティ製品を選択します。エンドポイントのパフォーマンスの問題を防ぐために、適用可能な除外が自動的に生成されます。Nextを選択します。



AMP for Endpoints Private Cloud X Dashboard X +

← → ↻ 🏠 🔒 https://vpc2-consol 'dashboard/fresh' 📄 ⋮ 📌 ☆ 🏠 📄 👤

**CISCO** AMP for Endpoints 🔔 ? Roman Valenta ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾ 🔍 Search

### Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

#### Getting Started

- [View Online Help](#)
- [Download Cisco AMP for Endpoints User Guide](#)
- [Download Cisco AMP for Endpoints Deployment Strategy](#)

#### Deploy AMP for Endpoints Connectors

- [Set Up Windows Connector](#)
- [Set Up Mac Connector](#)
- [Set Up Linux Connector](#)

#### 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.

コネクタをダウンロードします。

🟢 Step 1: Existing Security Products

🟢 Step 2: Set Up Proxy

🟢 Step 3: Download Connector

<p style="text-align: center;"><b>Audit Only</b></p> <p>Used when you're still learning about the product and want to install it without any impact to your existing systems.</p> <p style="text-align: center;"><a href="#">Policy Details</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Files</b></p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Network</b></p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Offline Engine</b></p> <p>TETRA</p> </div> <p style="text-align: center;"><a href="#">Download</a></p>	<p style="text-align: center;"><b>Protect</b></p> <p>Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.</p> <p style="text-align: center;"><a href="#">Policy Details</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Files</b></p> <p> Quarantined</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Network</b></p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Offline Engine</b></p> <p>TETRA</p> </div> <p style="text-align: center;"><a href="#">Download</a></p>	<p style="text-align: center;"><b>Triage</b></p> <p>Used when you have a known or suspected infected machine.</p> <p style="text-align: center;"><a href="#">Policy Details</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Files</b></p> <p> Quarantined</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Network</b></p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Offline Engine</b></p> <p>TETRA</p> </div> <p style="text-align: center;"><a href="#">Download</a></p>	<p style="text-align: center;"><b>Server</b></p> <p>Used when you're installing a connector on standard Windows servers.</p> <p style="text-align: center;"><a href="#">Requirements</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Files</b></p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Network</b></p> <p> Off</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Offline Engine</b></p> <p>TETRA</p> </div> <p style="text-align: center;"><a href="#">Download</a></p>	<p style="text-align: center;"><b>Windows Domain Controllers</b></p> <p>installing a connector on Windows Domain Controllers.</p> <p style="text-align: center;"><a href="#">Requirements</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Files</b></p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Network</b></p> <p> Off</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>Offline Engine</b></p> <p>TETRA</p> </div> <p style="text-align: center;"><a href="#">Download</a></p>
--	--	--	---	--

[Back](#) [Next](#)

Step 4: Verify, Contain, and Protect

Opening amp\_Protect.exe

You have chosen to open:

**amp\_Protect.exe**

which is: `exe File`

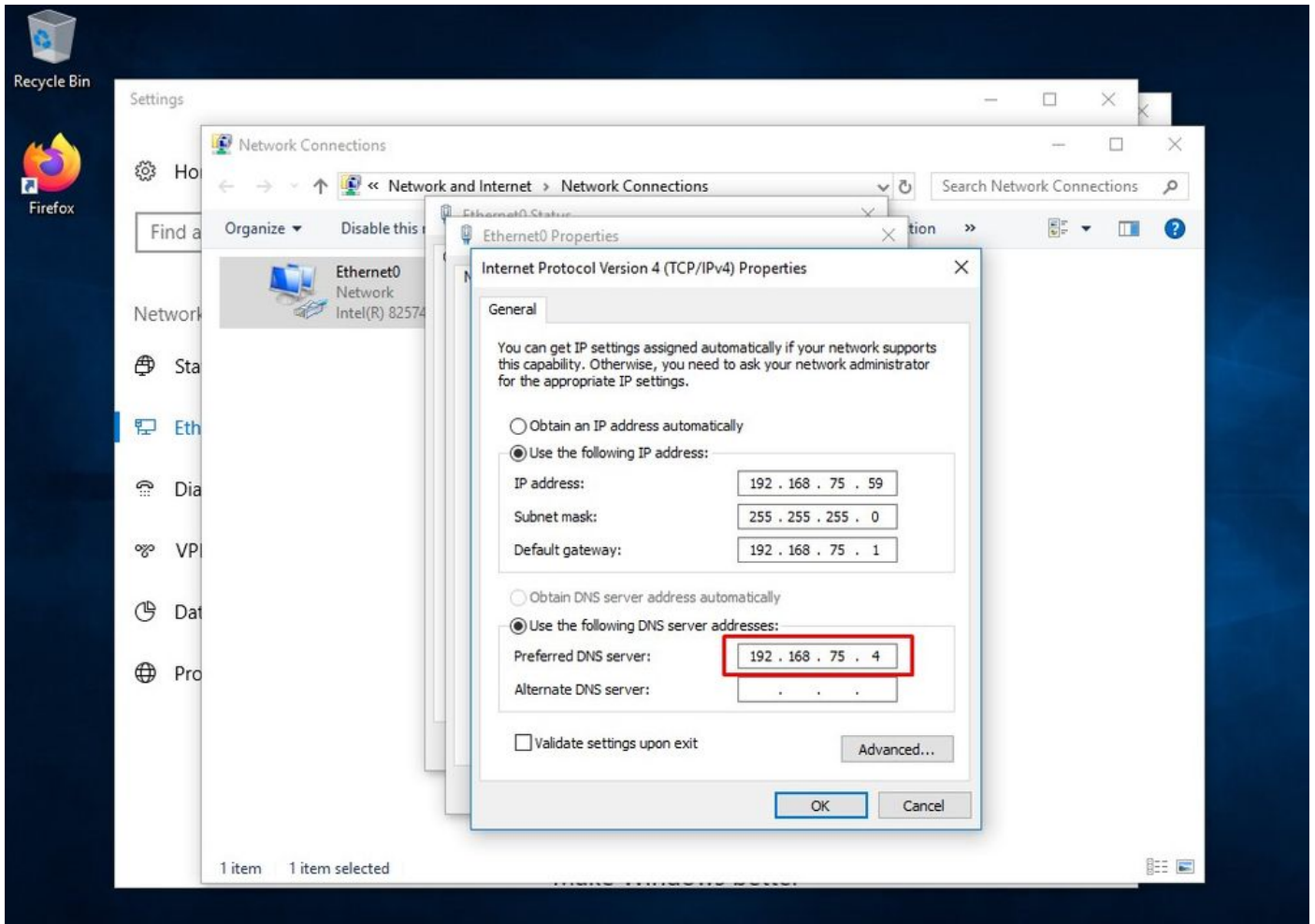
from: `https://vpc-console.cyberworld.local`

Would you like to save this file?

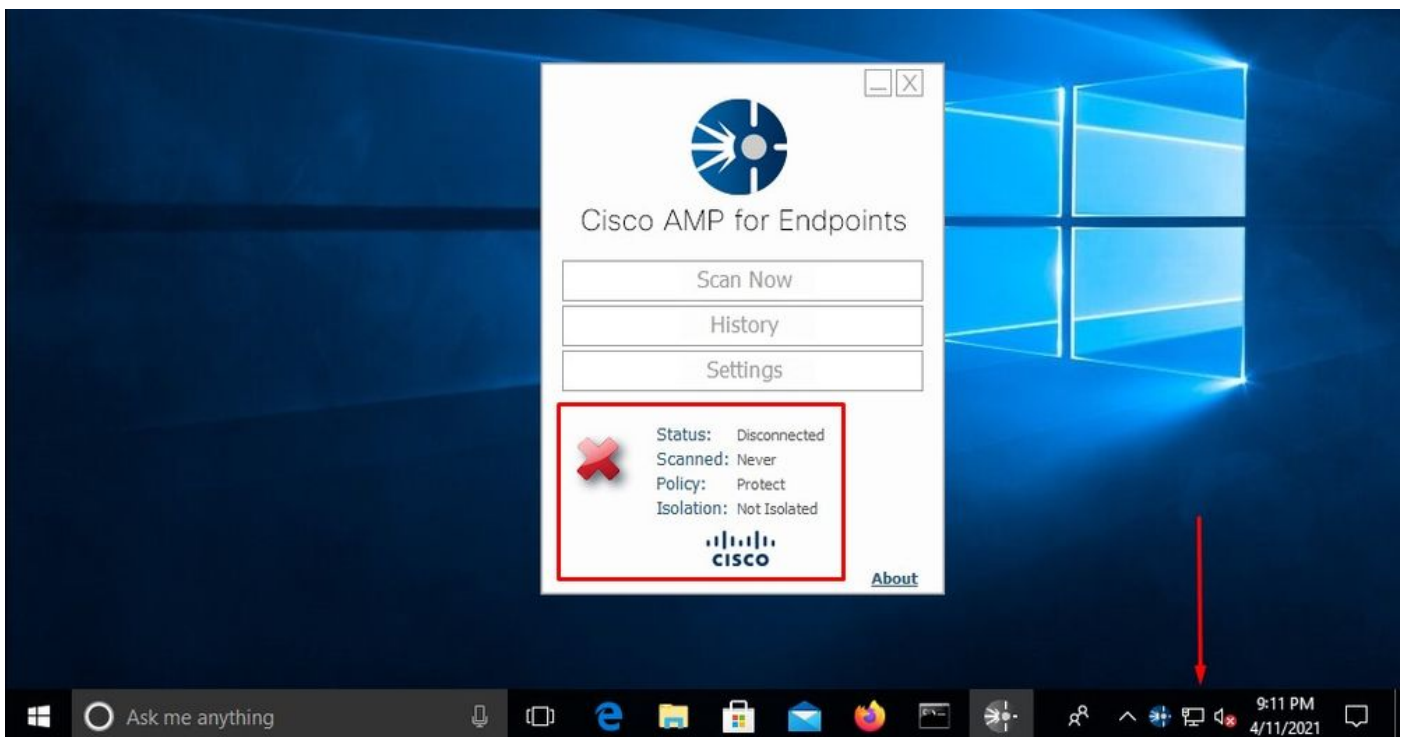
[Save File](#) [Cancel](#)

## 問題#2 : ルートCAの問題

次に発生する可能性のある問題は、独自の社内証明書を使用する場合、最初のインストール後にコネクタが接続解除として表示される可能性があることです。



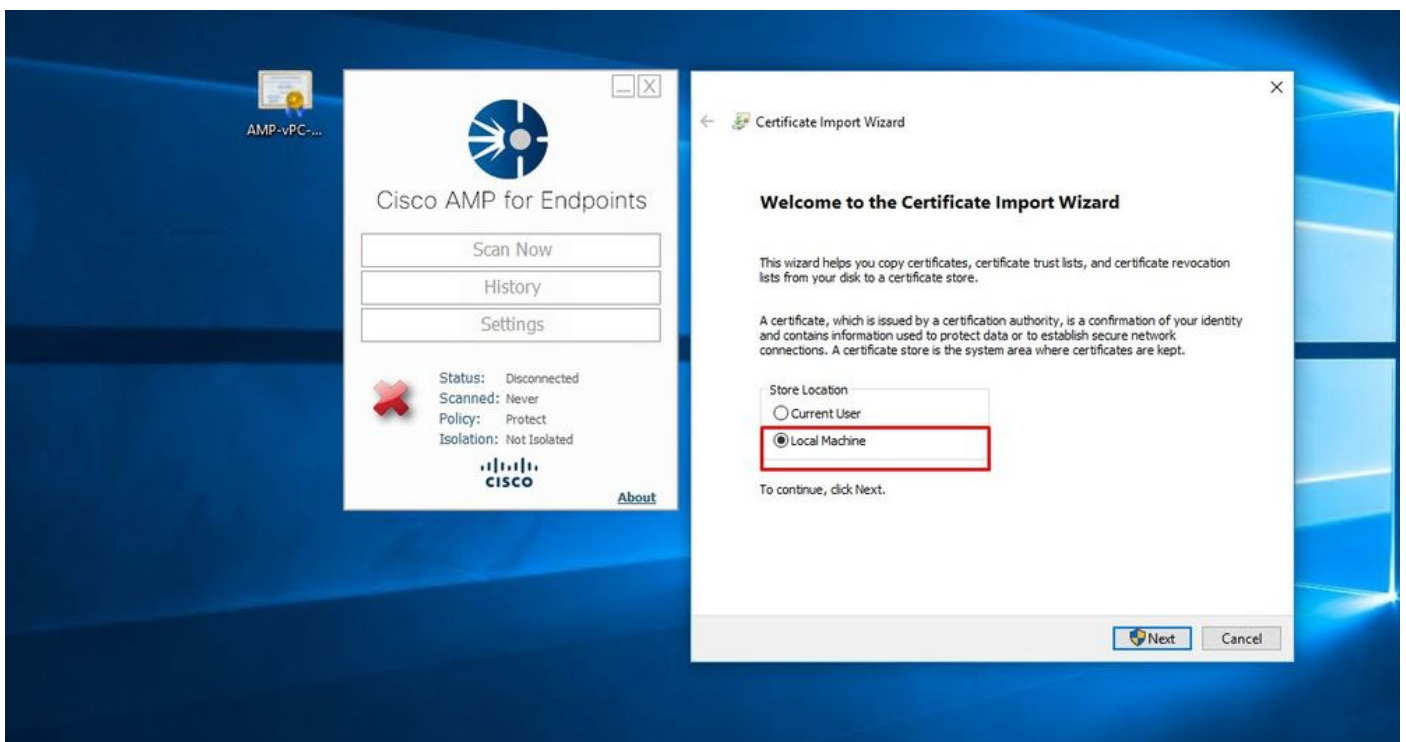
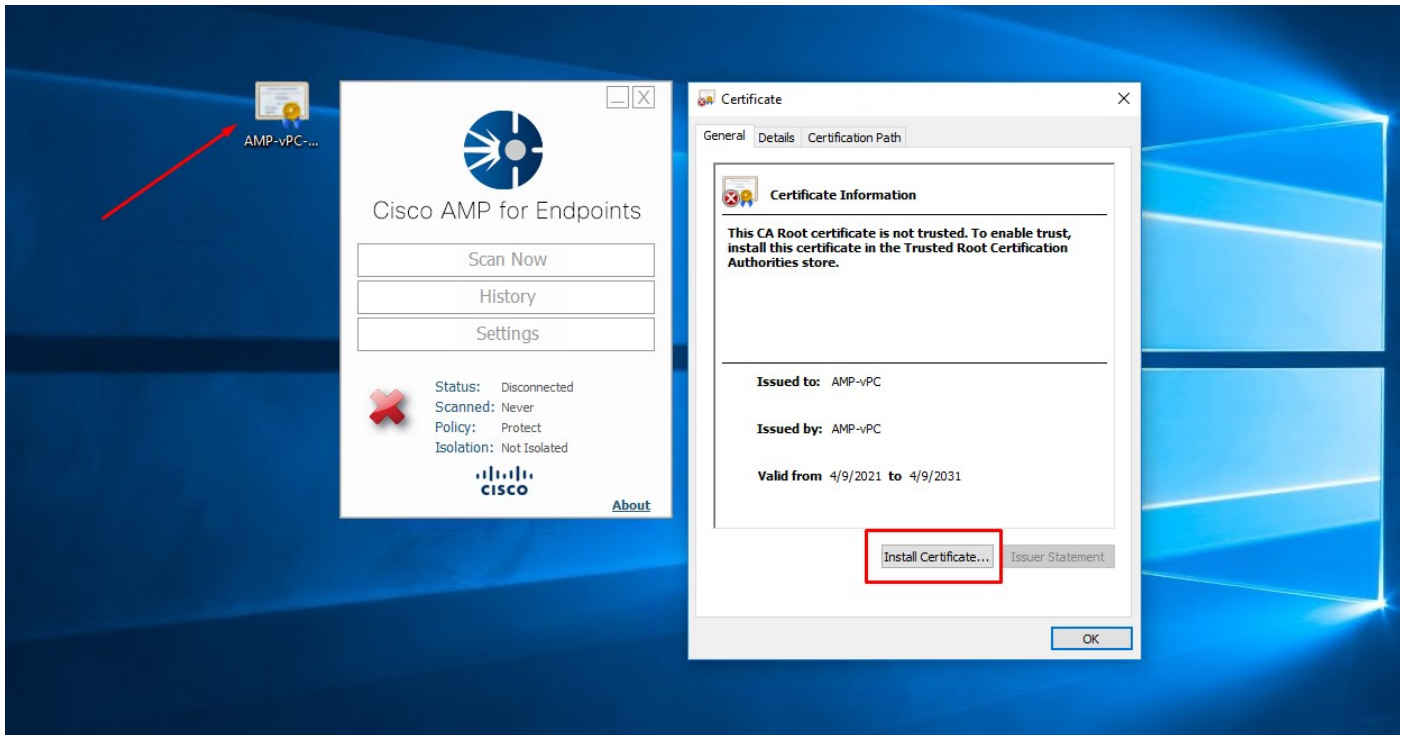
コネクタをインストールすると、セキュアエンドポイントが接続解除と表示されます。診断バンドルを実行し、ログを確認すると、問題を特定できます。

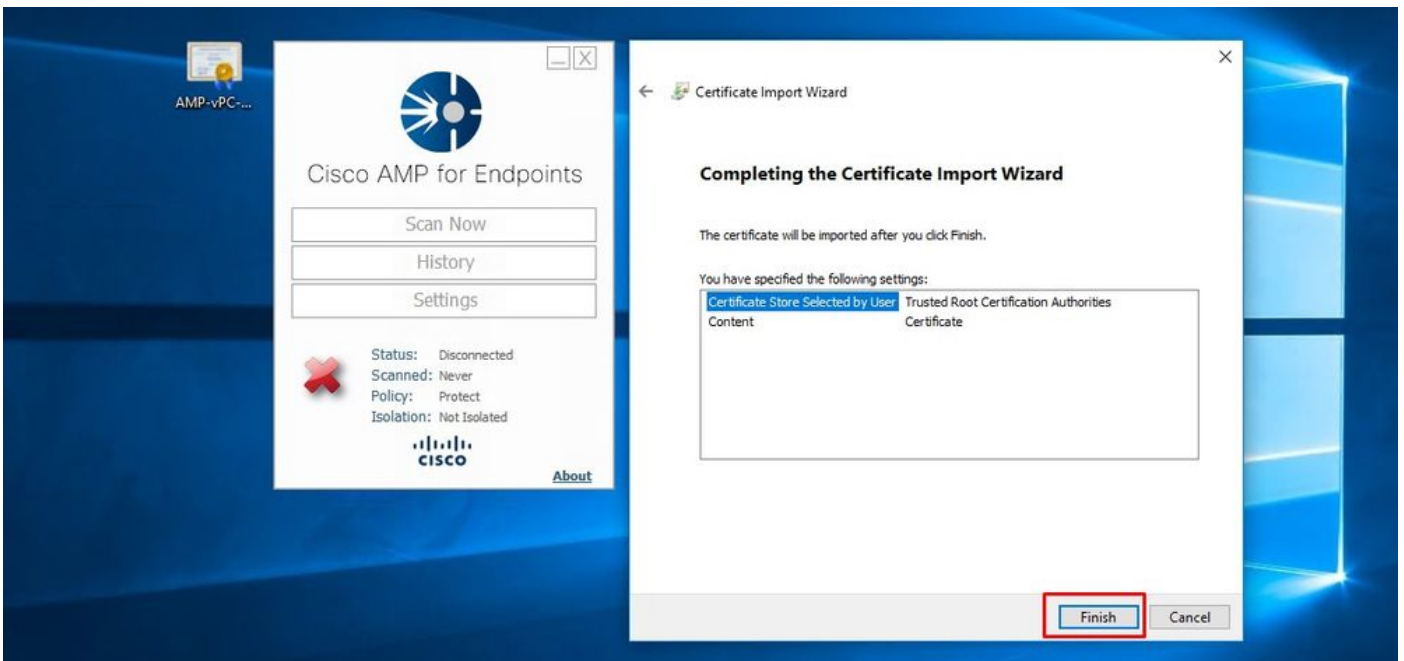
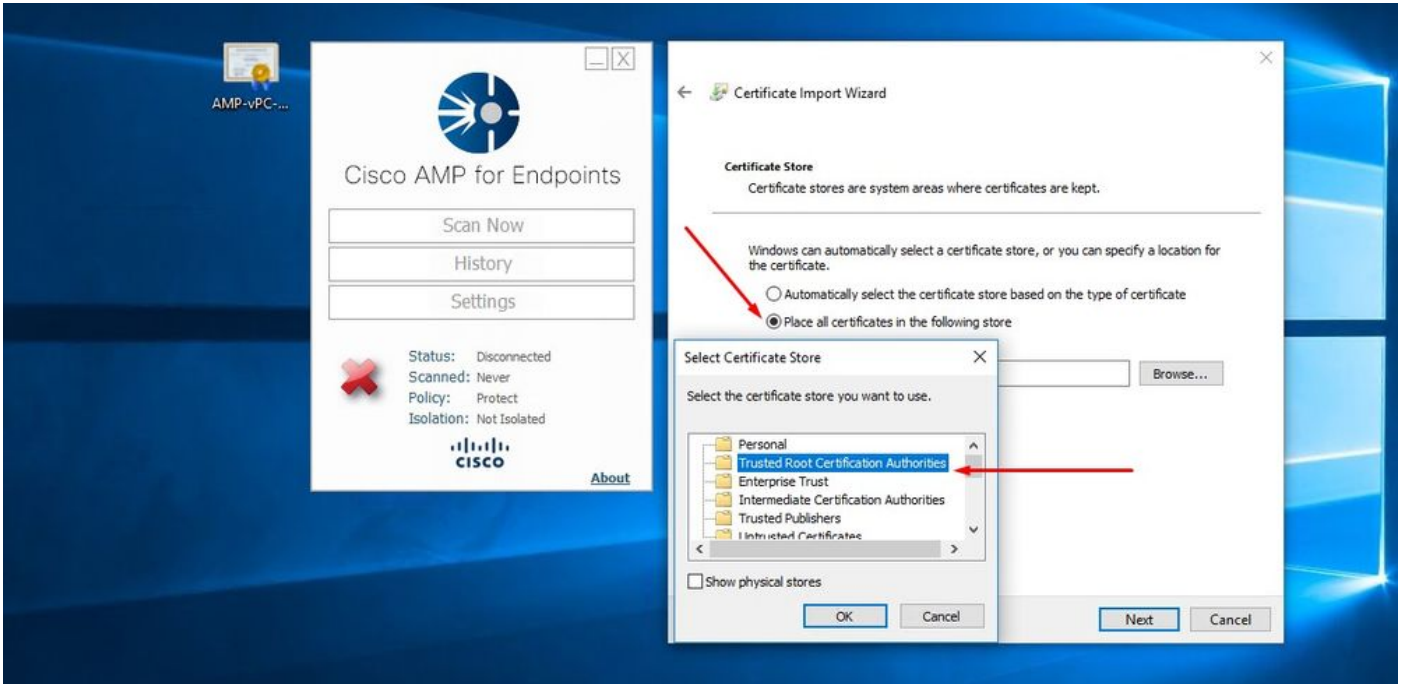


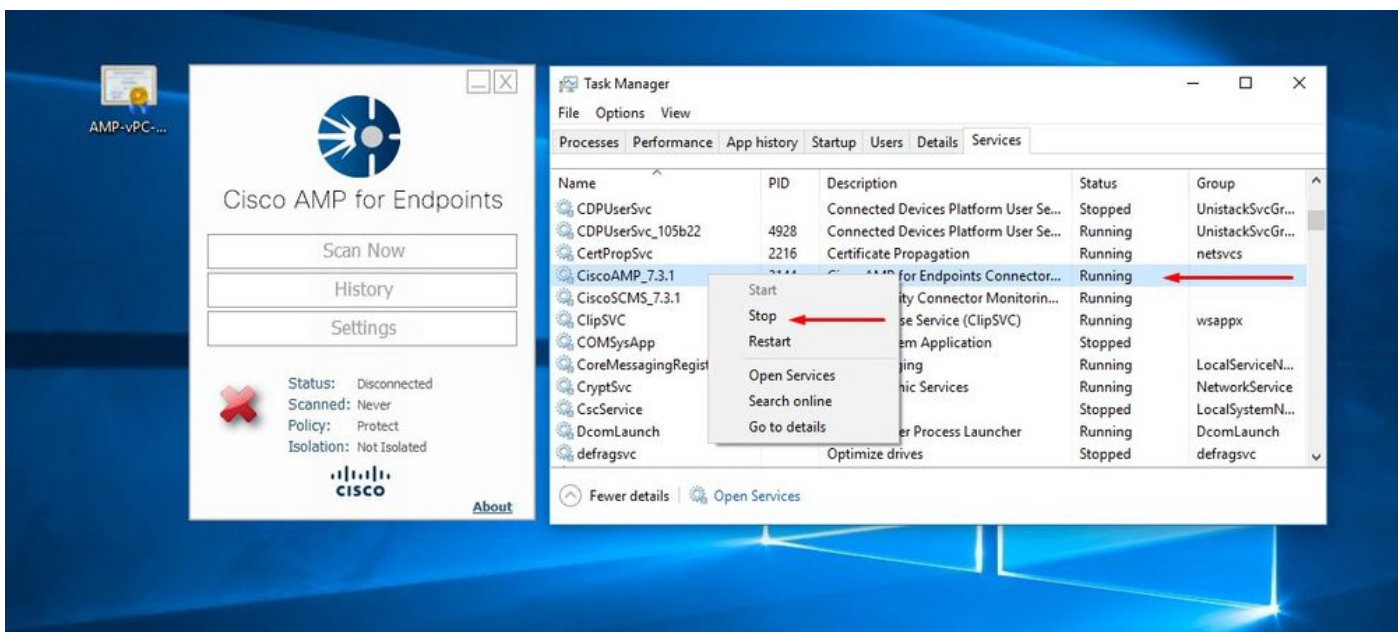
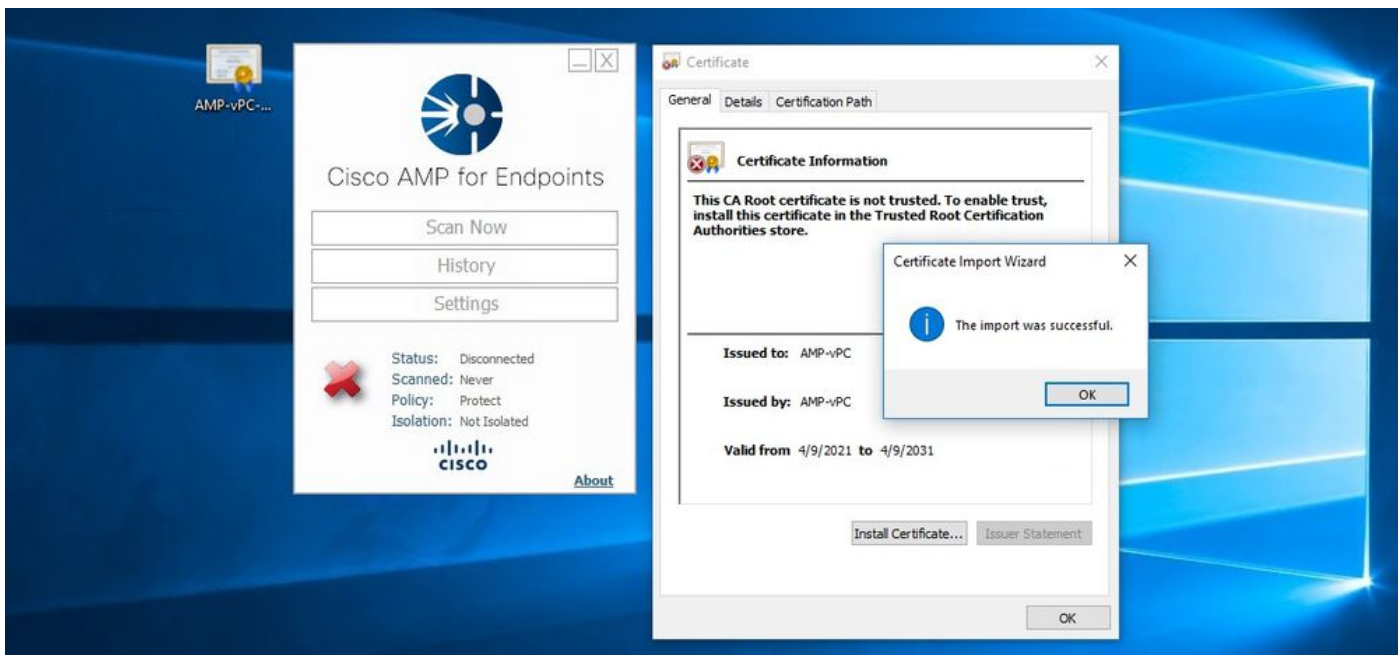
診断バンドルから収集されたこの出力に基づいて、ルートCAエラーを確認できます

(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

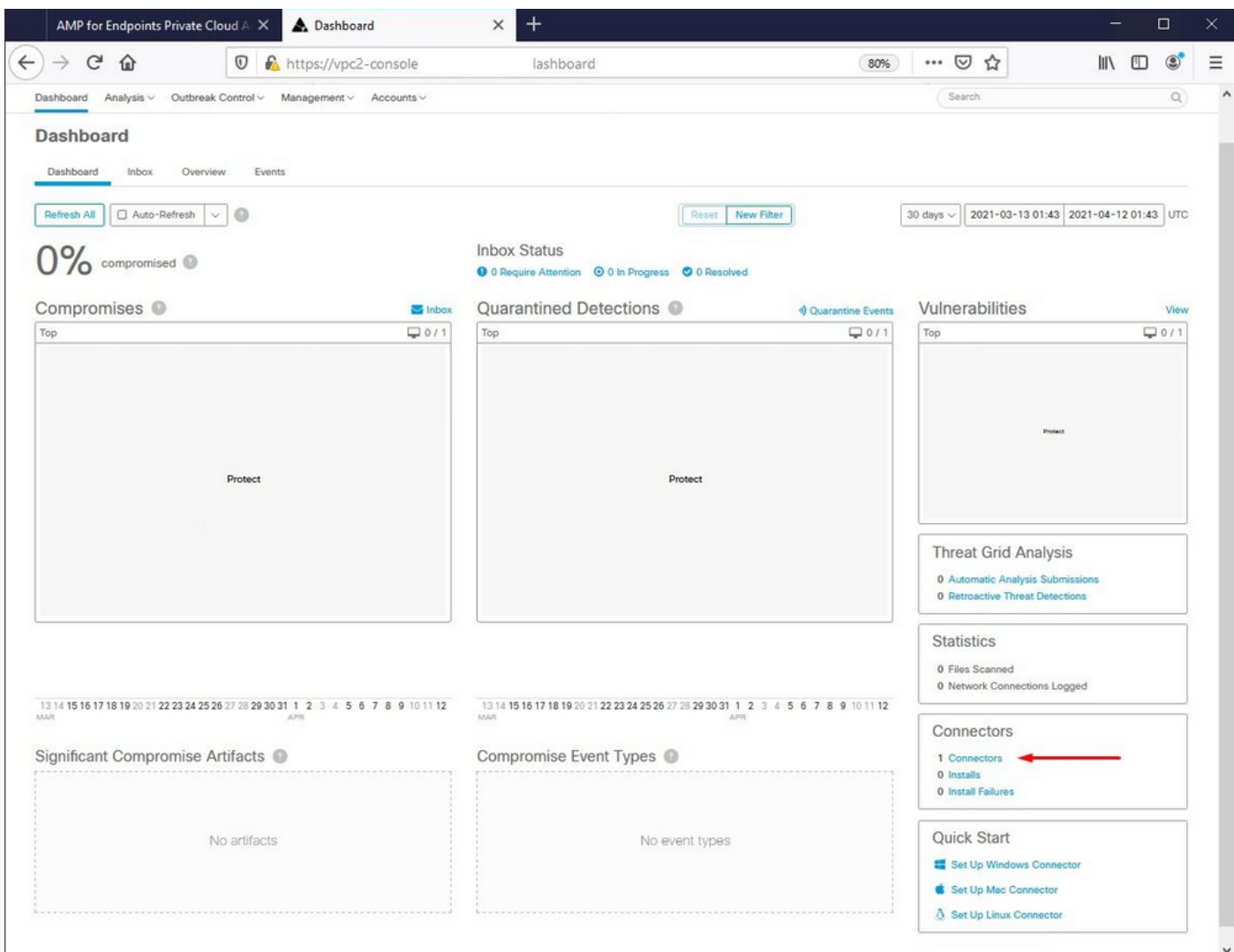
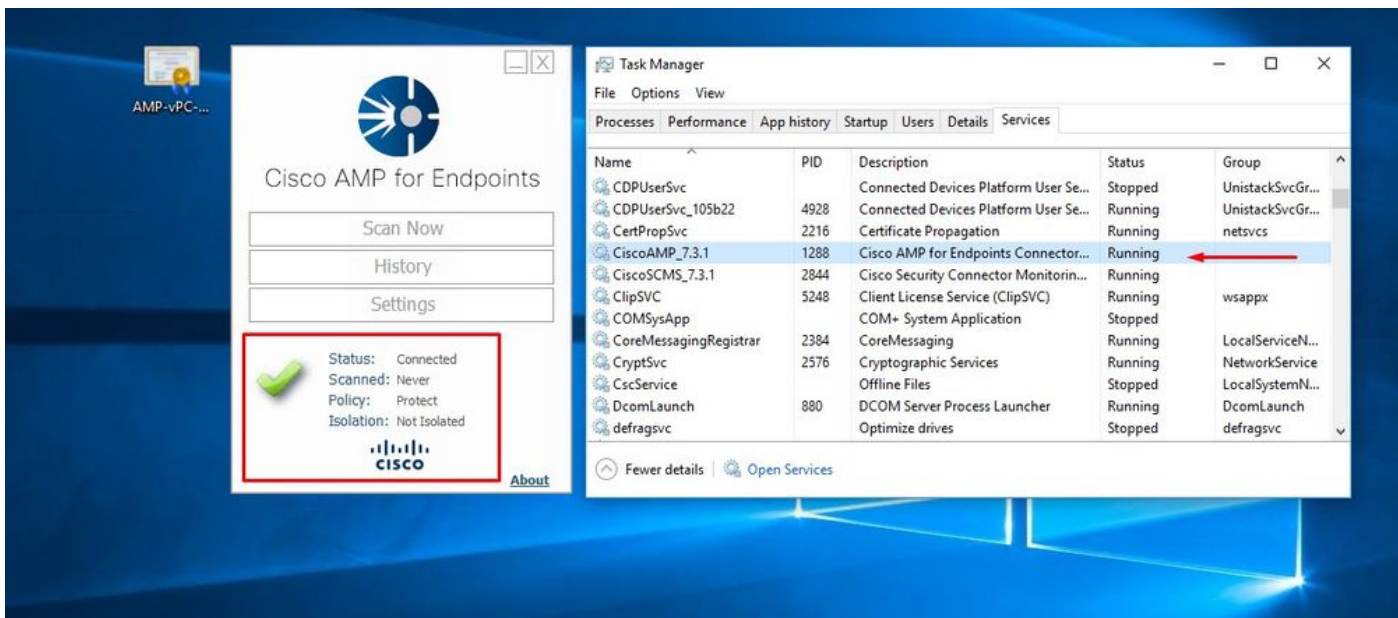
ルートCAを信頼されたルートCAストアにアップロードし、セキュアエンドポイントサービスを再起動します。すべてが期待どおりに動作し始めます。







バウンスすると、Secure Endpointサービスコネクタがオンラインになります。



テスト済みの悪意のあるアクティビティ

### Dashboard

Dashboard **Inbox** Overview Events

Refresh All Auto-Refresh

Reset New Filter

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

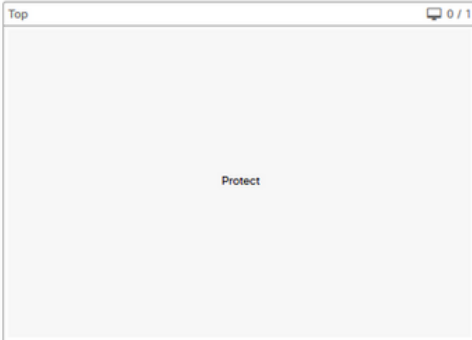
0% compromised

#### Inbox Status

0 Require Attention 0 In Progress 0 Resolved

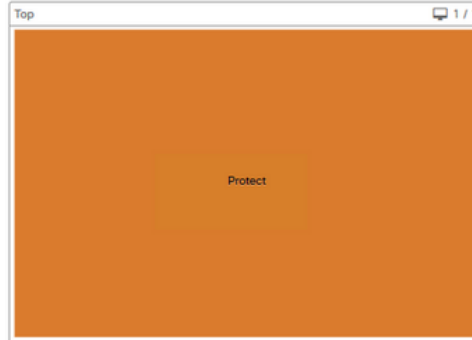
#### Compromises

Inbox



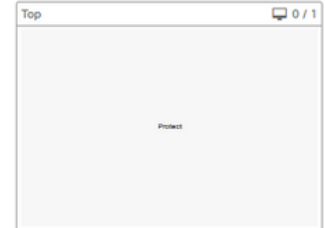
#### Quarantined Detections

Quarantine Events



#### Vulnerabilities

View



#### 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

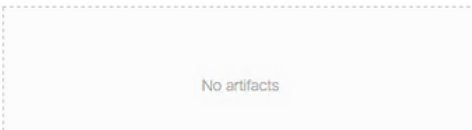
#### Quick Start

Set Up Windows Connector

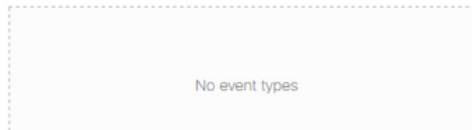
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12  
MAR APR

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  
MAR APR

#### Significant Compromise Artifacts



#### Compromise Event Types





## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。