

# Installation et configuration d'un cloud privé virtuel de point de terminaison sécurisé

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Déploiement VPC](#)

[Installation de VM](#)

[Configuration initiale de l'interface Admin](#)

[Configuration initiale du vPC via l'interface utilisateur graphique Web](#)

[Configuration](#)

[Services](#)

[Ensemble de mise à jour AirGap](#)

[Problème #1 - Salle épuisée dans le magasin de données](#)

[Problème #2 - Ancienne mise à jour](#)

[Dépannage de base](#)

[Problème #1 - FQDN et serveur DNS](#)

[Problème #2 - Problème avec l'autorité de certification racine](#)

---

## Introduction

Ce document décrit et se concentre sur la façon de déployer avec succès le cloud privé virtuel (VPC) sur les serveurs dans l'environnement ESXi. Pour d'autres documents tels que le guide de démarrage rapide, la stratégie de déploiement, le guide d'autorisation, le guide de l'utilisateur de la console et de l'administrateur, consultez la [documentation de](#) ce site

Contribution de Roman Valenta, Ingénieurs du centre d'assistance technique Cisco.

## Conditions préalables

Exigences:

VMware ESX 5 ou version ultérieure

- Mode proxy cloud (uniquement) : 128 Go de RAM, 8 coeurs de processeur (2 processeurs avec 4 coeurs chacun recommandés), 1 To d'espace disque libre minimum sur le data store VMware
- Type de lecteurs : SSD requis pour le mode d'entrefier et recommandé pour le proxy
- Type RAID : un groupe RAID 10 (miroir agrégé par bandes)
- Taille minimale du data store VMware : 2 To
- Lectures aléatoires minimales du datastore pour le groupe RAID 10 (4 000) : 60 000 E/S par seconde

- Nombre minimal d'écritures aléatoires de data store pour le groupe RAID 10 (4 000) : 30 000 E/S par seconde

Cisco recommande que vous ayez une connaissance de ce sujet :

- Connaissances de base sur l'utilisation des certificats.
- Connaissances de base sur la configuration de DNS sous un serveur DNS (Windows ou Linux)
- Installation d'un modèle OVA (Open Virtual Appliance) dans le VMware ESXi

Utilisé dans ces travaux pratiques :

VMware ESX 6.5


- Mode proxy cloud (uniquement) : 48 Go de RAM, 8 coeurs de processeur (2 processeurs avec 4 coeurs chacun recommandés), 1 To d'espace disque libre minimum sur le data store VMware
- Type de disques : SATA
- Type RAID : un RAID 1
- Taille minimale du data store VMware : 1 To
- MobaXterm 20.2 (programme multiterminal similaire à PuTTY)
- Cygwin64 (Utilisé pour télécharger la mise à jour AirGap)

En outre

- Certificat que vous créez avec openssl ou XCA
- Serveur DNS (Linux ou Windows) Dans mes travaux pratiques, j'ai utilisé Windows Server 2016 et CentOS-8
- VM Windows pour notre terminal de test
- Licence

Si votre mémoire est inférieure à 48 Go RAM sur la version 3.2+ VPC deviennent inutilisables.


---

 Remarque : l'OVA de cloud privé crée les partitions de lecteur, il n'est donc pas nécessaire de les spécifier dans VMWare. serveur qui résout le nom d'hôte de l'interface propre.

---

Référez-vous à la [Fiche technique de l'appliance VPC](#) pour plus d'informations sur la configuration matérielle spécifique à la version.

---

 Remarque : les informations de ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

---

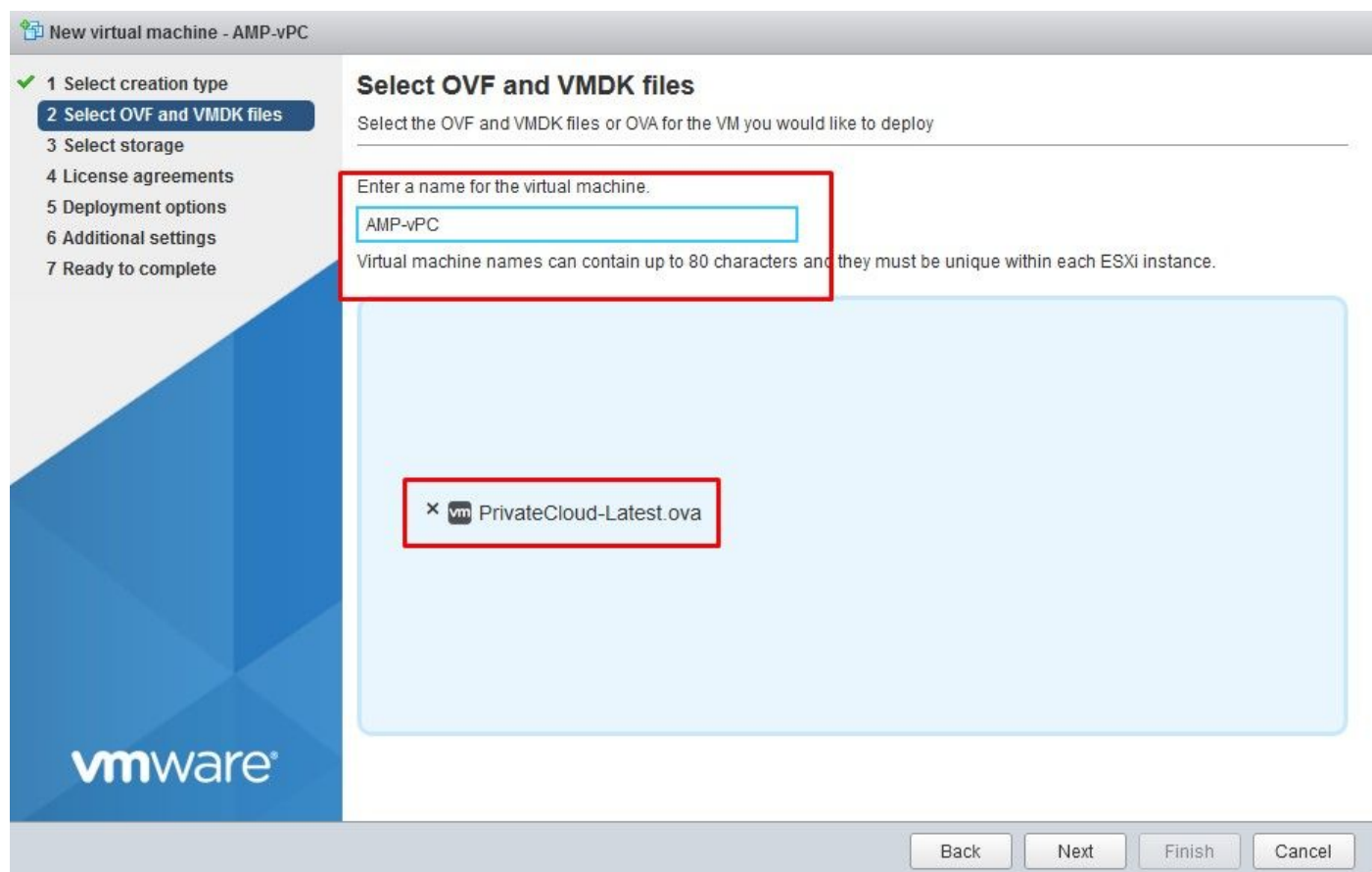
## Déploiement VPC

Sélectionnez l'URL fournie dans l'e-mail de livraison électronique ou d'autorisation. Téléchargez le fichier OVA et poursuivez l'installation

## Installation de VM

Étape 1 :

Accédez à File > Deploy OVF Template pour ouvrir l'assistant Deploy OVF Template, comme indiqué dans l'image.



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

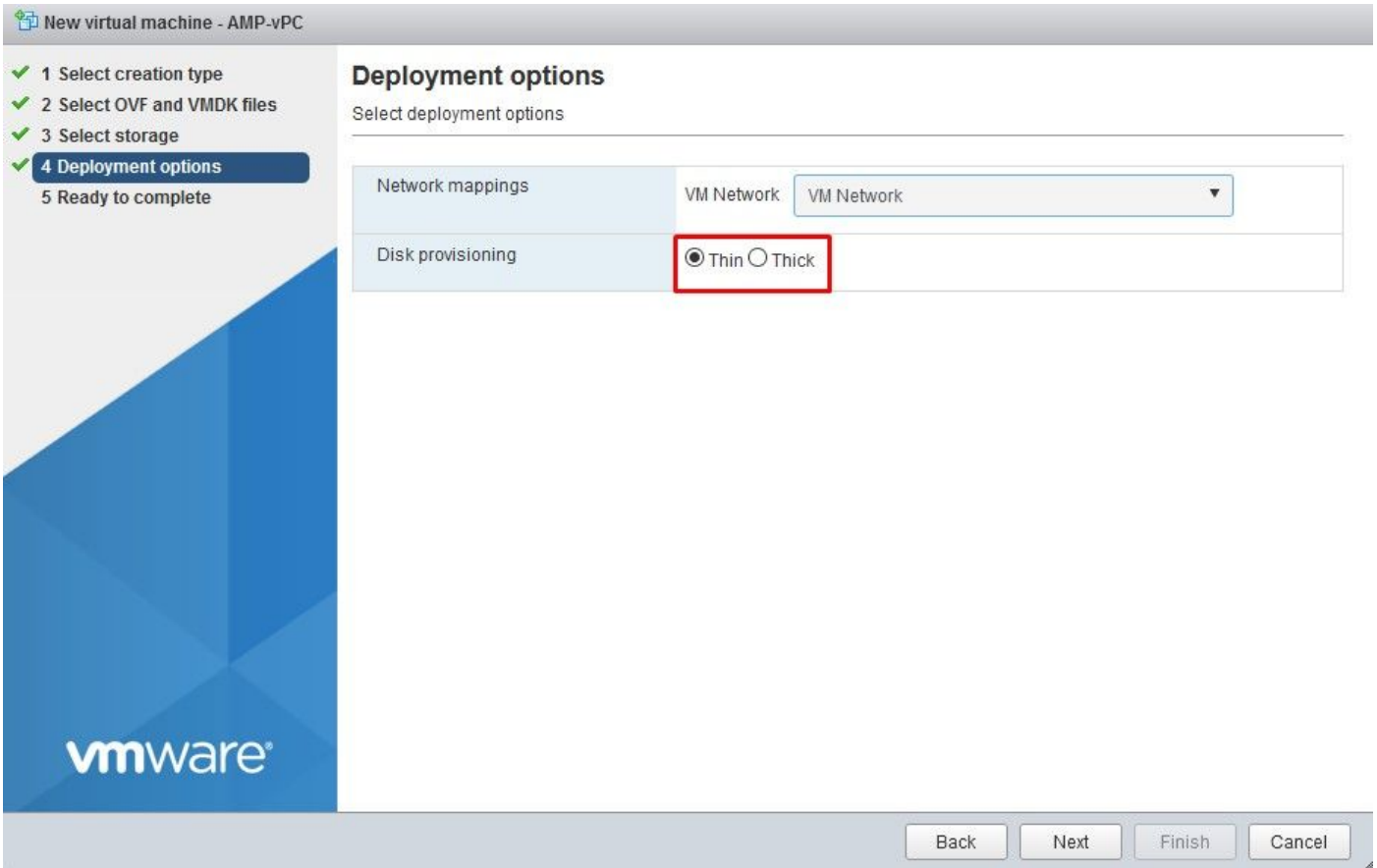
vmware

Back Next Finish Cancel

 Remarque : le provisionnement épais réserve de l'espace lors de la création d'un disque. Si vous sélectionnez cette option, elle peut améliorer les performances par rapport à Thin



 Provisioned. Toutefois, cela n'est pas obligatoire. Sélectionnez ensuite Next, comme indiqué dans l'image.



The screenshot shows the 'New virtual machine - AMP-vPC' wizard in the 'Deployment options' step. On the left, a progress bar indicates 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 'VM Network' dropdown menu, 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'.

Étape 2 :

Sélectionnez Parcourir... pour sélectionner un fichier OVA, puis cliquez sur Suivant. Vous remarquerez les paramètres OVA par défaut sur la page OVF Template Details, comme indiqué dans l'image. sélectionnez Next.


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.

Back Next Finish Cancel



## Configuration initiale de l'interface Admin


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.

Back Next Finish Cancel

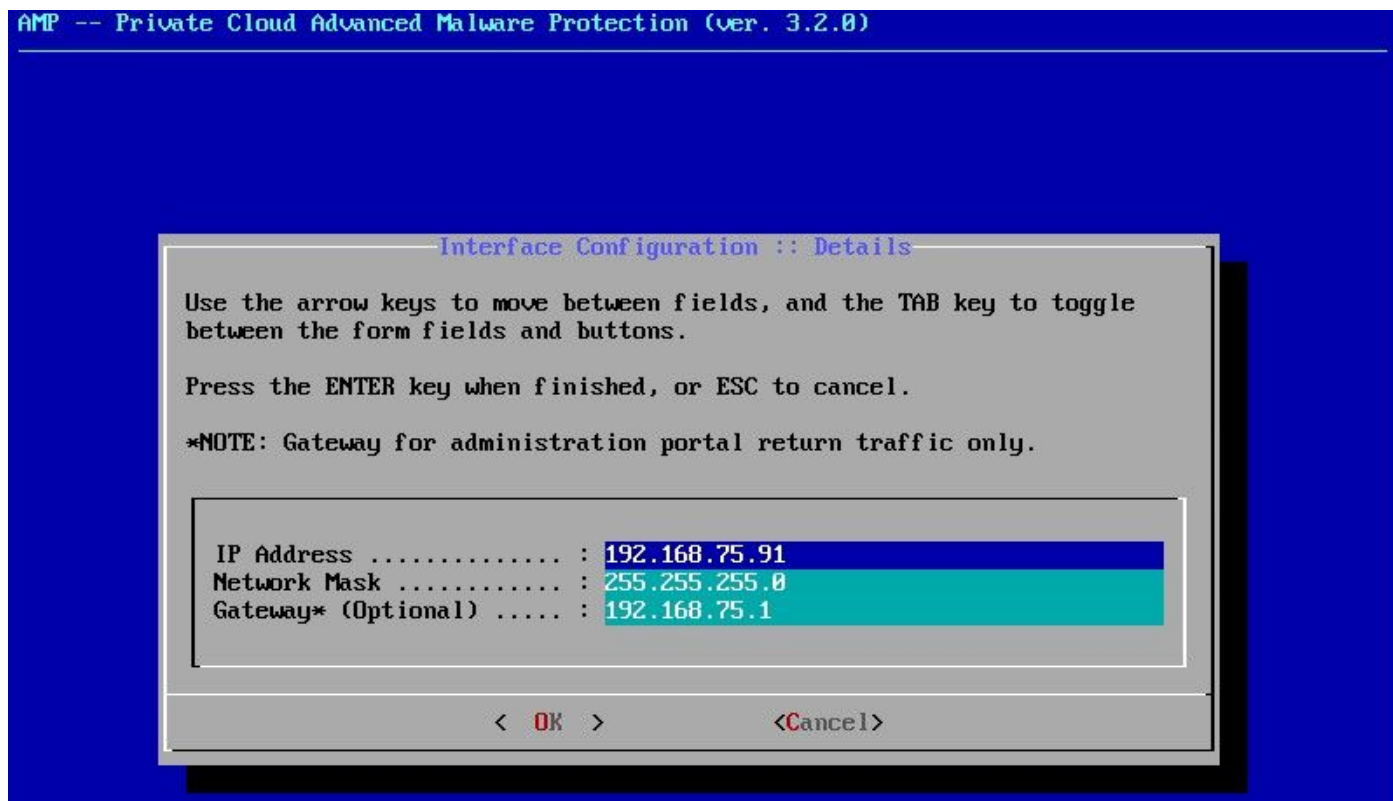


Une fois la machine virtuelle démarrée, vous effectuez la configuration initiale via la console de la

machine virtuelle.

Étape 1 :

Vous remarquerez peut-être que l'URL indique [UNCONFIGURED] si l'interface n'a pas reçu d'adresse IP du serveur DHCP. Notez que cette interface est l'interface de gestion. Il ne s'agit pas de l'interface Production.



Étape 2 :

Vous pouvez naviguer entre les touches Tab, Entrée et Flèche.

Accédez à CONFIG\_NETWORK et sélectionnez la touche Entrée sur votre clavier pour commencer la configuration de l'adresse IP de gestion pour le cloud privé de point de terminaison sécurisé. Si vous ne voulez pas utiliser DHCP, sélectionnez No et sélectionnez Enter key.

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.

**CONFIG\_NETWORK**    Configure the Web administration interface.

CONSOLE            Start command line console / shell.

INFO                Display device status / information.

ESC

60%

< OK >

Dans la fenêtre qui s'affiche, choisissez Yes et sélectionnez Enter key.



Si l'adresse IP est déjà utilisée, vous serez traité avec ce journal d'erreurs. Il suffit de revenir en arrière et de choisir quelque chose qui est unique et pas en cours d'utilisation.

```
Restarting eth0...  
  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already 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>

Si tout se passe bien, vous voyez un résultat qui ressemble à ceci

```

- 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 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
* 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_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
```

Étape 3 :

Attendez que l'écran bleu s'affiche à nouveau avec votre nouvelle adresse IP STATIQUE. Notez également le mot de passe à usage unique. Prenez note et nous allons ouvrir notre navigateur.



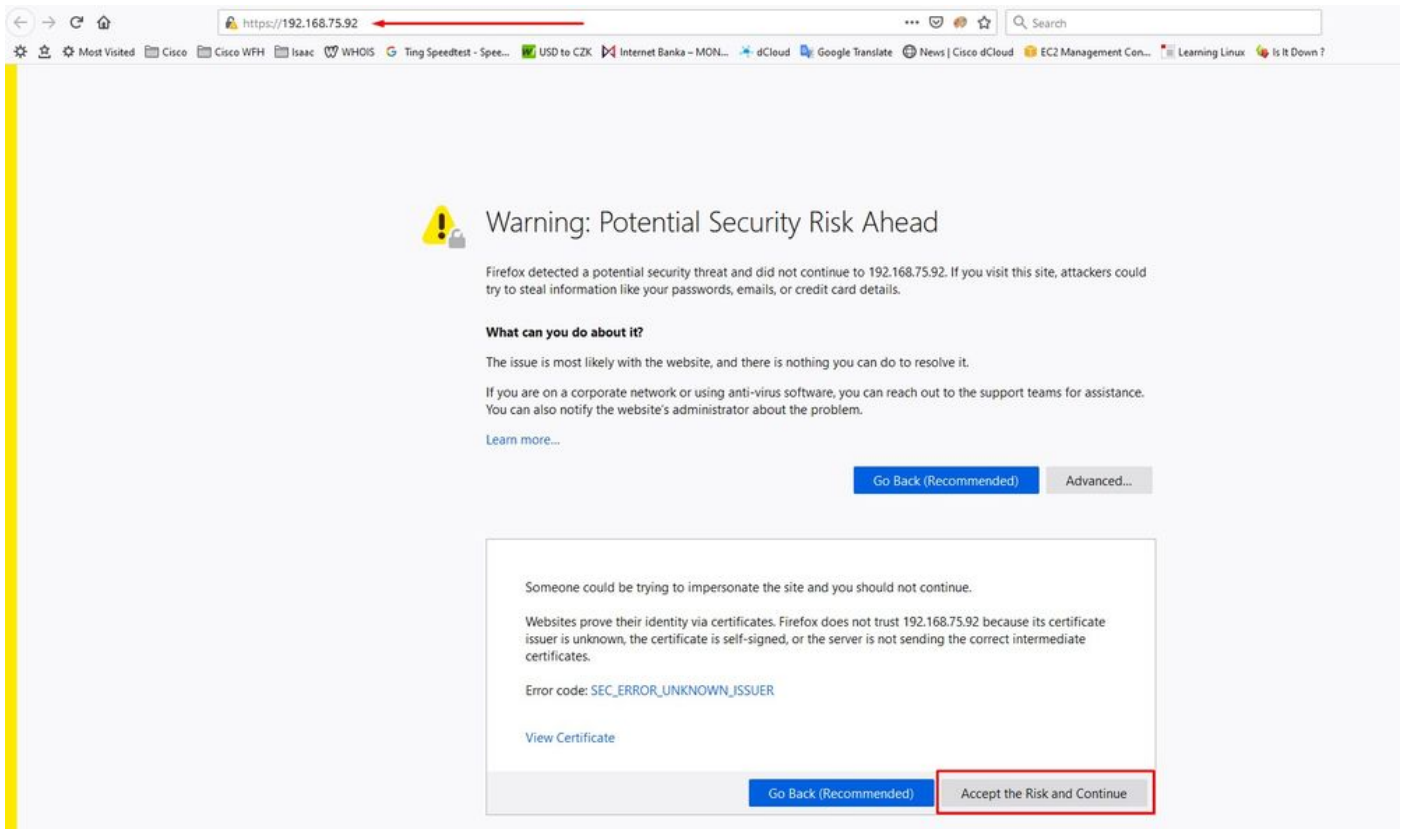
## Configuration initiale du vPC via l'interface utilisateur graphique Web

Étape 1 :

Ouvrez un navigateur Web et accédez à l'adresse IP de gestion de l'apppliance. Vous pouvez recevoir une erreur de certificat car le cloud privé Secure Endpoint génère initialement son propre certificat HTTPS, comme illustré dans l'image. Configurez votre navigateur pour qu'il approuve le certificat HTTPS auto-signé du cloud privé Secure Endpoint.

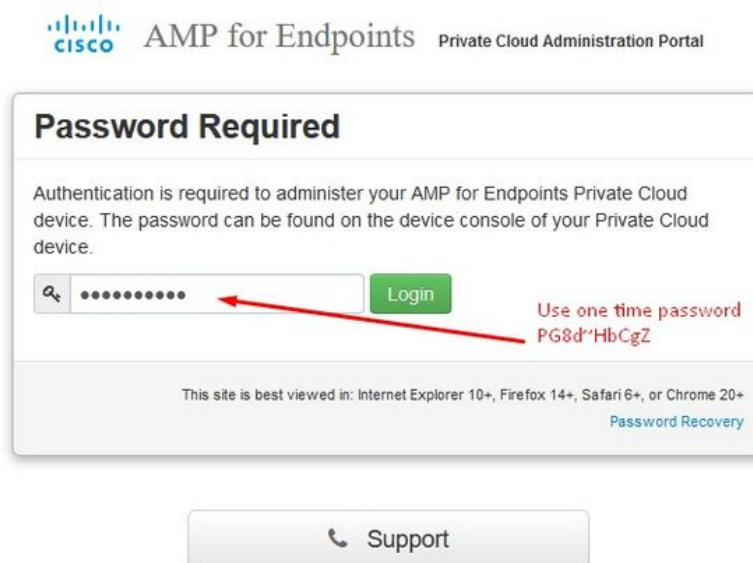
Dans votre navigateur, tapez l'adresse IP STATIQUE que vous avez configurée précédemment.





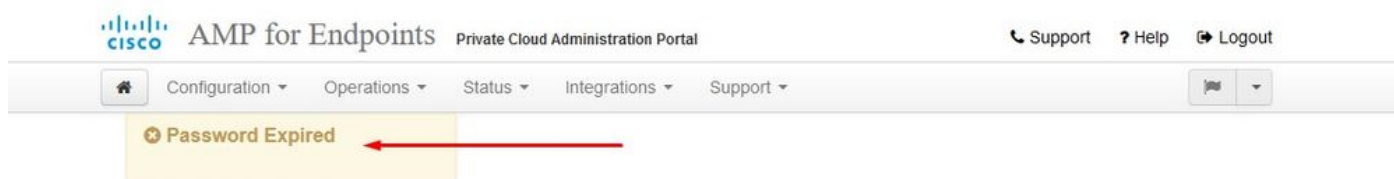
Étape 2 :

Une fois connecté, vous devez réinitialiser le mot de passe. Utilisez le mot de passe initial de la console dans le champ Ancien mot de passe. Utilisez votre nouveau mot de passe dans le champ Nouveau mot de passe. Saisissez à nouveau votre nouveau mot de passe dans le champ Nouveau mot de passe. sélectionnez Modifier le mot de passe.

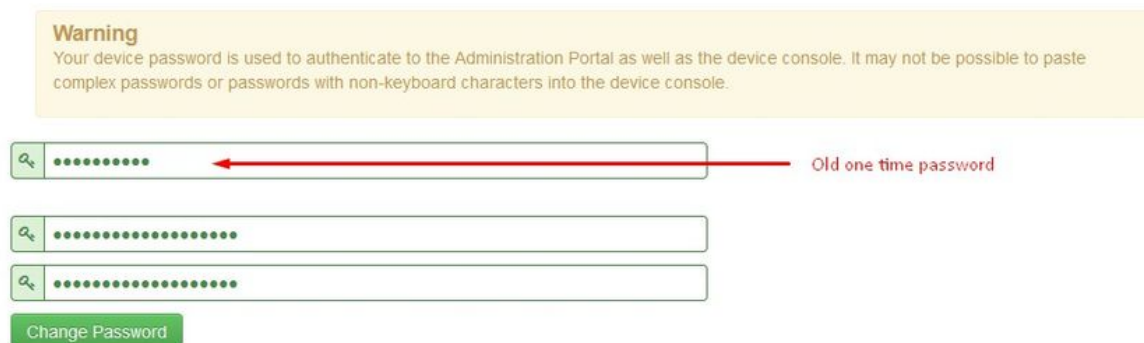


Étape 3 :

Une fois connecté, vous devez réinitialiser le mot de passe. Utilisez le mot de passe initial de la console dans le champ Ancien mot de passe. Utilisez votre nouveau mot de passe dans le champ Nouveau mot de passe. Saisissez à nouveau votre nouveau mot de passe dans le champ Nouveau mot de passe. sélectionnez Modifier le mot de passe.



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. ?



Étape 4 :

Sur la page suivante, faites défiler la page vers le bas pour accepter le contrat de licence. sélectionnez J'ai lu et j'accepte.



Étape 5 :

Après avoir accepté le contrat, vous obtenez l'écran d'installation, comme illustré dans l'image. Si vous voulez restaurer à partir d'une sauvegarde, vous pouvez le faire ici, cependant, ce guide continue avec l'option Clean Installation. Sélectionnez sur Démarrer dans la section Nettoyer l'installation.



Installation Options

Only the License section can be altered after installation.

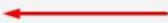
- Install or Restore
- License

# 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 >

Étape 6 :

La première chose dont vous avez besoin est une licence pour aller de l'avant. Vous recevez une licence et une phrase de passe lorsque vous achetez le produit. Sélectionnez on +Upload License File. Sélectionnez le fichier de licence et saisissez la phrase de passe. Sélectionnez sur Upload License. Si le téléchargement échoue, vérifiez si la phrase de passe est correcte. Si le téléchargement a réussi, un écran contenant des informations de licence valides s'affiche. Sélectionnez Suivant. Si vous ne parvenez toujours pas à installer votre licence, contactez le support technique Cisco.



Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License

# License

Device ID  
E6[REDACTED]V5

License  
No license has been installed.

Install New License

license + 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 >

## Étape 7 :

Vous recevez la page d'accueil, comme illustré dans l'image. Cette page affiche les informations dont vous avez besoin avant de configurer le cloud privé. Lisez attentivement les exigences. Sélectionnez sur Next pour démarrer la configuration de pré-installation.



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 >

## Configuration

Étape 1 :

 Remarque : veuillez noter que dans les prochaines séries de diapositives, nous incluons des éléments exclusifs, comme illustré dans l'image, qui sont uniques uniquement au mode AIR GAP , ceux-ci doivent être inclus et marqués comme AIRGAP ONLY





Installation Options

Only the License section can be altered after installation.

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

Configuration

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

# Deployment Mode

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

**Cloud Proxy**

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

**Standalone**

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

≡ ≡ ENTREFER UNIQUEMENT ≡ ≡



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.



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

### ⌘ ⌘ AIRGAP UNIQUEMENT ⌘ ⌘

Étape 2 :

Accédez à la page Secure Endpoint Console Account. Un utilisateur administrateur est utilisé pour la console afin de créer des stratégies, des groupes d'ordinateurs et d'ajouter des utilisateurs supplémentaires. Saisissez le nom, l'adresse e-mail et le mot de passe du compte de console. Sélectionnez sur Suivant.

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	.....	
	.....	

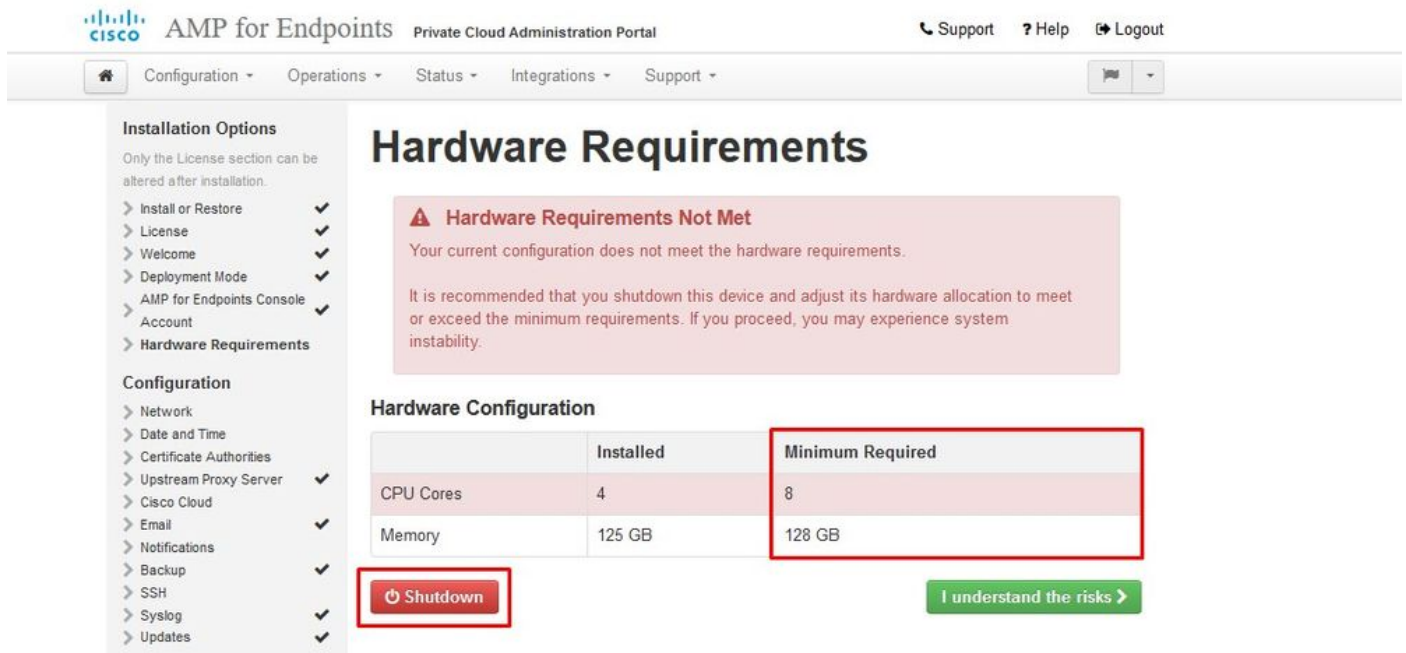
Next >

Si vous vous connectez à ce problème lorsque vous effectuez le déploiement à partir du fichier OVA, vous avez deux choix : soit continuer et résoudre ce problème ultérieurement, soit arrêter, afin d'installer votre machine virtuelle déployée et de l'ajuster en conséquence. Après le



redémarrage, vous continuez là où vous étiez.


 Remarque : ceci a été corrigé dans le fichier OVA pour la version 3.5.2 qui se charge correctement avec 128 Go de RAM et 8 coeurs de CPU

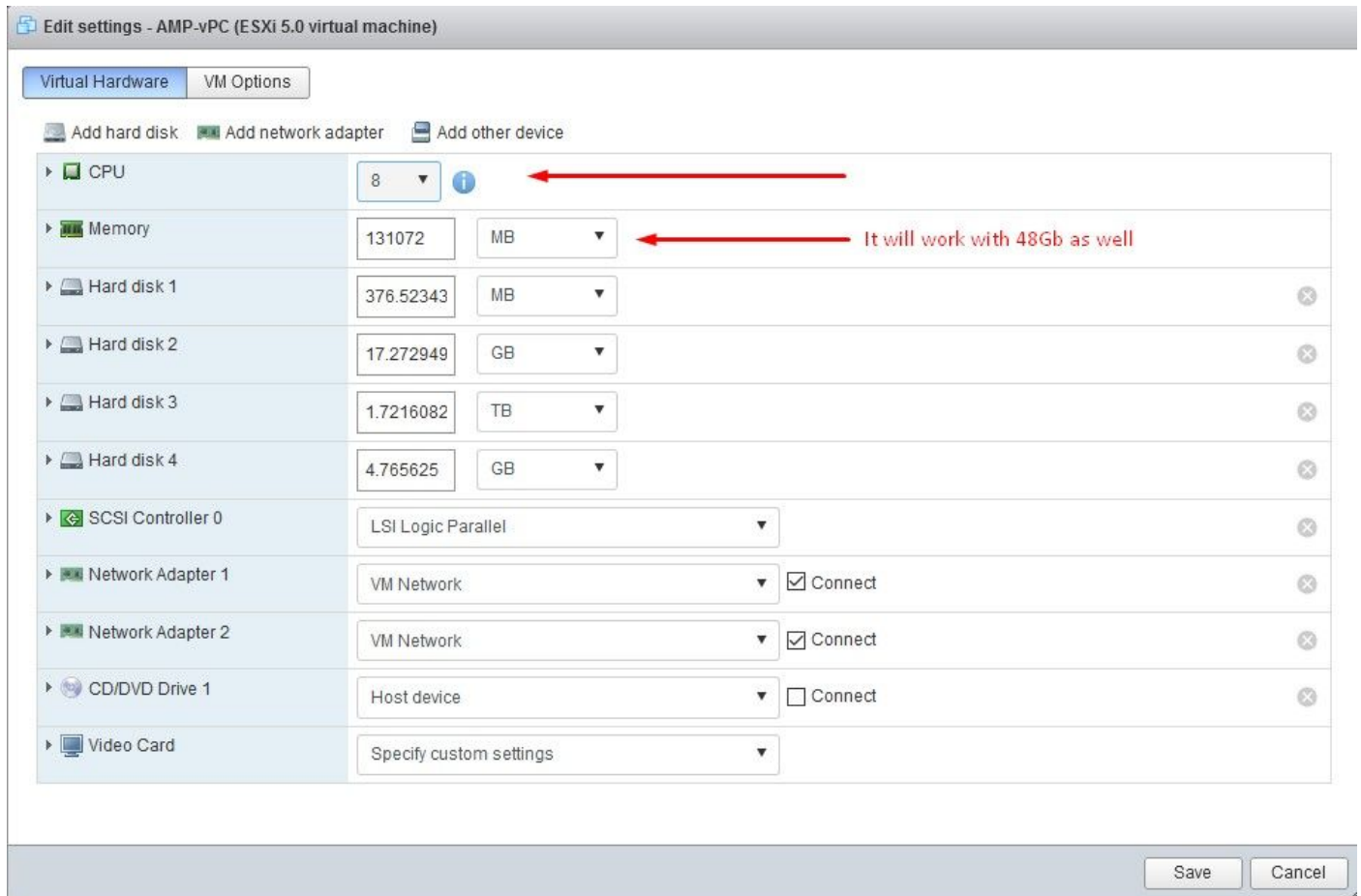


The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. The left sidebar contains 'Installation Options' and 'Configuration' menus. The main content area is titled 'Hardware Requirements' and features a red warning box: 'Hardware Requirements Not Met. Your current configuration 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.' Below this is a 'Hardware Configuration' table:

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

Below the table are two buttons: a red 'Shutdown' button and a green 'I understand the risks' button.

 Remarque : utilisez uniquement les valeurs recommandées, sauf pour les travaux pratiques



The screenshot shows the 'Edit settings - AMP-vPC (ESXi 5.0 virtual machine)' window. The 'Virtual Hardware' tab is active. The settings list includes:

- CPU: 8 (with an information icon and a red arrow pointing to it)
- Memory: 131072 MB (with a red arrow pointing to it and the text '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 (checked)
- Network Adapter 2: VM Network (checked)
- CD/DVD Drive 1: Host device (unchecked)
- Video Card: Specify custom settings

At the bottom right, there are 'Save' and 'Cancel' buttons.


Une fois redémarré, nous continuons là où nous sommes partis.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The left sidebar contains navigation options under 'Installation Options' and 'Configuration'. The main content area is titled 'Hardware Requirements' and features a green success message: 'Hardware Requirements Met. Your current configuration meets or exceeds the hardware requirements.' Below this is a table titled 'Hardware Configuration' with the following data:

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

A green 'Next >' button is located at the bottom right of the table.

Assurez-vous également de configurer ETH1 avec l'adresse IP STATIQUE.

 Remarque : vous ne devez jamais configurer votre périphérique pour qu'il utilise DHCP, sauf si vous avez créé des réservations d'adresses MAC pour les interfaces. Si les adresses IP de vos interfaces changent, cela peut entraîner de graves problèmes avec les connecteurs Secure Endpoint Connectors déployés. Si votre serveur DNS n'est pas configuré, vous pouvez utiliser le service DNS public temporaire pour terminer votre installation.

Étape 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
- > Firepower 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)

## Étape 4 :

Vous obtenez la page Date et heure. Saisissez les adresses d'un ou plusieurs serveurs NTP que vous souhaitez utiliser pour la synchronisation de date et d'heure. Vous pouvez utiliser des serveurs NTP internes ou externes et en spécifier plusieurs via une liste délimitée par des virgules ou des espaces. Synchronisez l'heure avec votre navigateur ou exécutez amp-ctl ntpdate à partir de la console du périphérique pour forcer une synchronisation immédiate avec vos serveurs NTP. Sélectionnez Suivant.



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 >

≡ ≡ ENTREFER UNIQUEMENT ≡ ≡



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 UNIQUEMENT ≡ ≡

Étape 5 :

Vous obtenez la page Autorités de certification, comme illustré dans l'image. Sélectionnez sur Add Certificate Authority pour ajouter votre certificat racine.

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 >

Étape 6 :

L'étape suivante consiste à configurer la page Cisco Cloud, comme illustré dans l'image. Sélectionnez la région de cloud Cisco appropriée. Développez View Hostnames si vous devez



créer des exceptions de pare-feu pour votre périphérique de cloud privé Secure Endpoint afin de communiquer avec le cloud Cisco pour les recherches de fichiers et les mises à jour de périphériques. Sélectionnez sur Suivant.



## Étape 7 :

Accédez à la page Notifications, comme illustré dans l'image. Sélectionnez la fréquence des notifications critiques et régulières. Saisissez les adresses e-mail auxquelles vous souhaitez recevoir des notifications d'alerte pour le périphérique Secure Endpoint. Vous pouvez utiliser des alias de messagerie ou spécifier plusieurs adresses via une liste séparée par des virgules. Vous pouvez également spécifier le nom de l'expéditeur et l'adresse e-mail utilisés par le périphérique. Ces notifications ne sont pas identiques aux abonnements à la console Secure Endpoint. Vous pouvez également spécifier un nom de périphérique unique si vous disposez de plusieurs périphériques de cloud privé Secure Endpoint. Sélectionnez Suivant.

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 >

### Étape 8 :

Ensuite, vous accédez à la page SSH Keys, comme indiqué dans l'image. Sélectionnez Add SSH Key (Ajouter une clé SSH) pour entrer les clés publiques que vous souhaitez ajouter au périphérique. Les clés SSH vous permettent d'accéder au périphérique via un shell distant avec des privilèges de racine. Seuls les utilisateurs approuvés doivent avoir accès à ce service. Votre périphérique de cloud privé nécessite une clé RSA au format OpenSSH. Vous pouvez ajouter d'autres clés SSH ultérieurement via Configuration > SSH dans votre portail d'administration. Sélectionnez sur Suivant.



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	<a href="#">Edit</a> <a href="#">Delete</a>
<pre>ecdsa-sha2-nistp256 AAAAE2K...oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7QGfd0g4vT9eD5XOXZd I4DKhrTNBv8/77T0d/Jagx7Przxs=</pre>		

Ensuite, vous obtenez la section Services. Dans les pages suivantes, vous devez attribuer des noms d'hôte et télécharger les paires de certificats et de clés appropriées pour ces services de périphérique. Dans les diapositives suivantes, nous pouvons voir la configuration de l'un des 6 certificats.

### Services

#### Étape 1 :

Au cours du processus de configuration, vous risquez de rencontrer ces erreurs.

La première « erreur » que vous remarquerez peut-être est mise en surbrillance avec les 3 flèches. Pour contourner cela, décochez simplement «Désactiver le contrôle TLS strict»

**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.	
<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.	

vPC2-Authenticatior [+ Choose Key](#)

vPC2-Authenticatior [+ Choose Certificate](#)

[Next >](#)

Sans contrôle TLS strict

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.	

vPC2-Authenticatic

+ Choose Key

vPC2-Authentication.cyberworld.local.pem

vPC2-Authenticatic

+ Choose Certificate

vPC2-Authentication.cyberworld.local.crt

Next >

Étape 2 :

L'erreur suivante se produit si vous laissez la case « Valider le nom DNS » cochée. Ici, vous avez deux choix.

#1 : désactivez la case à cocher Valider le DNS

#2 : Retournez à votre serveur DNS et configurez le reste de vos enregistrements d'hôte.

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 >

Répétez maintenant le même processus cinq fois de plus pour le reste des certificats.

### Authentication

- Le service d'authentification sera utilisé dans les futures versions du cloud privé pour gérer l'authentification des utilisateurs.

### Console Secure Endpoint

- Console est le nom DNS auquel l'administrateur Secure Endpoint peut accéder. Secure Endpoint Console et Secure Endpoint Connectors reçoivent les nouvelles stratégies et mises à jour.

### Serveur de disposition

- Disposition Server est le nom DNS auquel les connecteurs de point de terminaison sécurisé envoient et récupèrent les informations de recherche dans le cloud.

### Disposition Server - Protocole étendu

- Serveur de disposition : le protocole étendu est le nom DNS auquel les connecteurs de point d'extrémité sécurisé plus récents envoient et récupèrent des informations de recherche dans le cloud.


### Service De Mise À Jour De La Disposition

- Le service de mise à jour de la destruction est utilisé lorsque vous liez un appareil Cisco Threat Grid à votre périphérique de cloud privé. L'appliance Threat Grid est utilisée pour envoyer des fichiers à analyser à partir de la console Secure Endpoint et le service Disposition Update Service est utilisé par Threat Grid pour mettre à jour la disposition (propre ou malveillante) des fichiers après leur analyse.

### Centre de gestion Firepower

-Firepower Management Center Link vous permet de relier un périphérique Cisco Firepower Management Center (FMC) à votre périphérique de cloud privé. Cela vous permet d'afficher les données Secure Endpoint dans votre tableau de bord FMC. Pour plus d'informations sur l'intégration de FMC avec Secure Endpoint, consultez votre documentation FMC.

---

 Attention : les noms d'hôte ne peuvent pas être modifiés une fois que le périphérique a terminé l'installation.

---

Notez les noms d'hôte requis. Vous devez créer six enregistrements DNS A uniques pour le cloud privé Secure Endpoint. Chaque enregistrement pointe vers la même adresse IP de l'interface de console de cloud privé virtuel (eth1) et doit être résolu par le cloud privé et le point d'extrémité sécurisé.

### Étape 3 :

Sur la page suivante, téléchargez et vérifiez Fichier de récupération.

Vous obtenez la page Récupération, comme illustré dans l'image. Vous devez télécharger et vérifier une sauvegarde de votre configuration avant de commencer l'installation. Le fichier de récupération contient l'ensemble de la configuration ainsi que les clés du serveur. Si vous perdez un fichier de récupération, vous ne pouvez pas restaurer votre configuration et tous les connecteurs Secure Endpoint doivent être réinstallés. Sans clé d'origine, vous devez reconfigurer l'ensemble de l'infrastructure de cloud privé avec de nouvelles clés. Le fichier de récupération contient toutes les configurations liées au portail opadmin. Le fichier de sauvegarde contient le contenu du fichier de récupération ainsi que toutes les données du portail du tableau de bord comme les événements, l'historique des connecteurs, etc. Si vous souhaitez restaurer seulement l'opadmin sans les données d'événement et tout, vous pouvez utiliser le fichier de récupération. Si vous effectuez une restauration à partir du fichier de sauvegarde, les données de l'opadmin et du portail du tableau de bord seront restaurées.

Sélectionnez sur Download pour enregistrer la sauvegarde sur votre ordinateur local. Une fois le fichier téléchargé, sélectionnez Choose File pour télécharger le fichier de sauvegarde et vérifiez qu'il n'est pas endommagé. Sélectionnez sur Next pour vérifier le fichier et continuer.

- > 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](#)

≡ ≡ ENTREFER UNIQUEMENT ≡ ≡



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

<b>Name</b>	Roman Valenta
<b>Email Address</b>	rvalenta@xxxxxxxxx.com
<b>Business Name</b>	Cisco vamrodia PC v2

**Recovery** ✎ Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

⌘ ⌘ AIRGAP UNIQUEMENT ⌘ ⌘

Vous voyez des entrées similaires comme ceci...

Attention : lorsque vous êtes sur cette page ne pas actualiser car il peut causer des problèmes.



# 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

Une fois l'installation terminée, appuyez sur le bouton de redémarrage

# 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

≡ ≡ ENTREFER UNIQUEMENT ≡ ≡

## 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!
=====
```

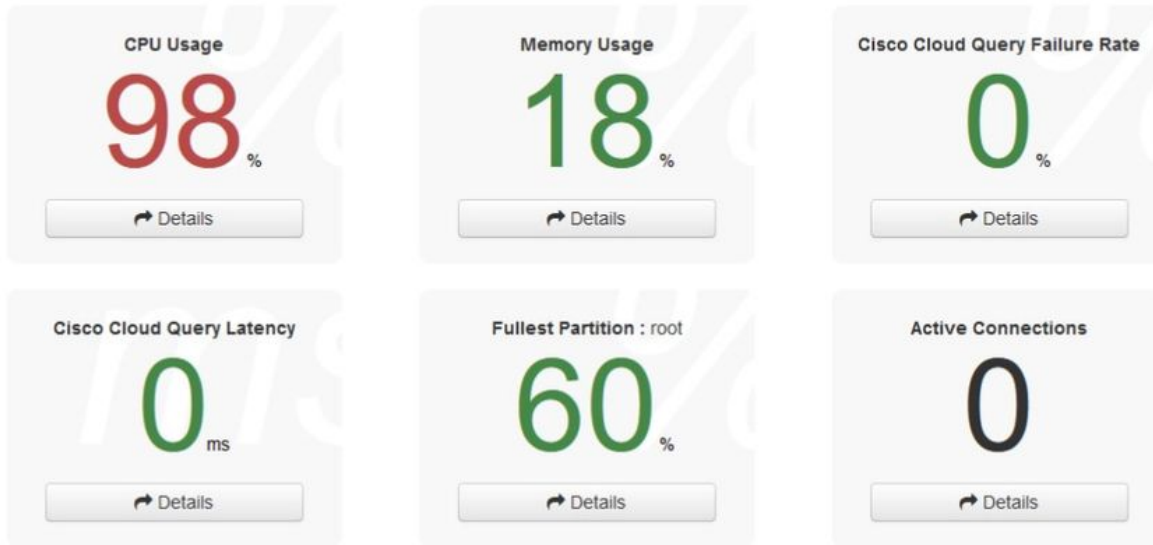
Download Output

### ⌘ ⌘ AIRGAP UNIQUEMENT ⌘ ⌘

Une fois l'appliance entièrement amorcée, la prochaine fois que vous vous connecterez avec votre interface d'administration, ce tableau de bord vous sera présenté. Vous remarquerez peut-être un processeur élevé au début, mais si vous donnez quelques minutes, il se calme.



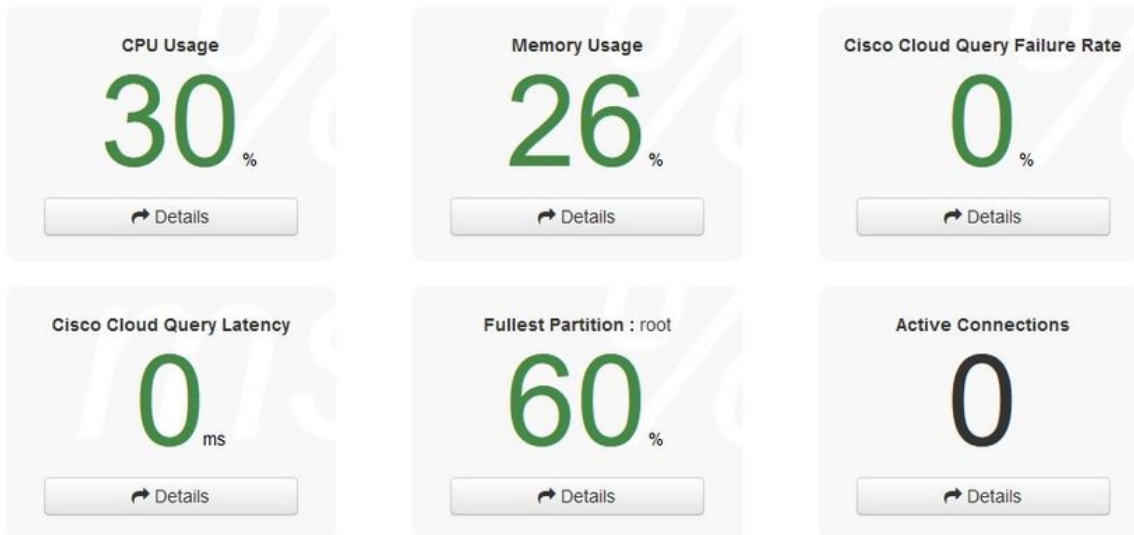
### Key Metrics



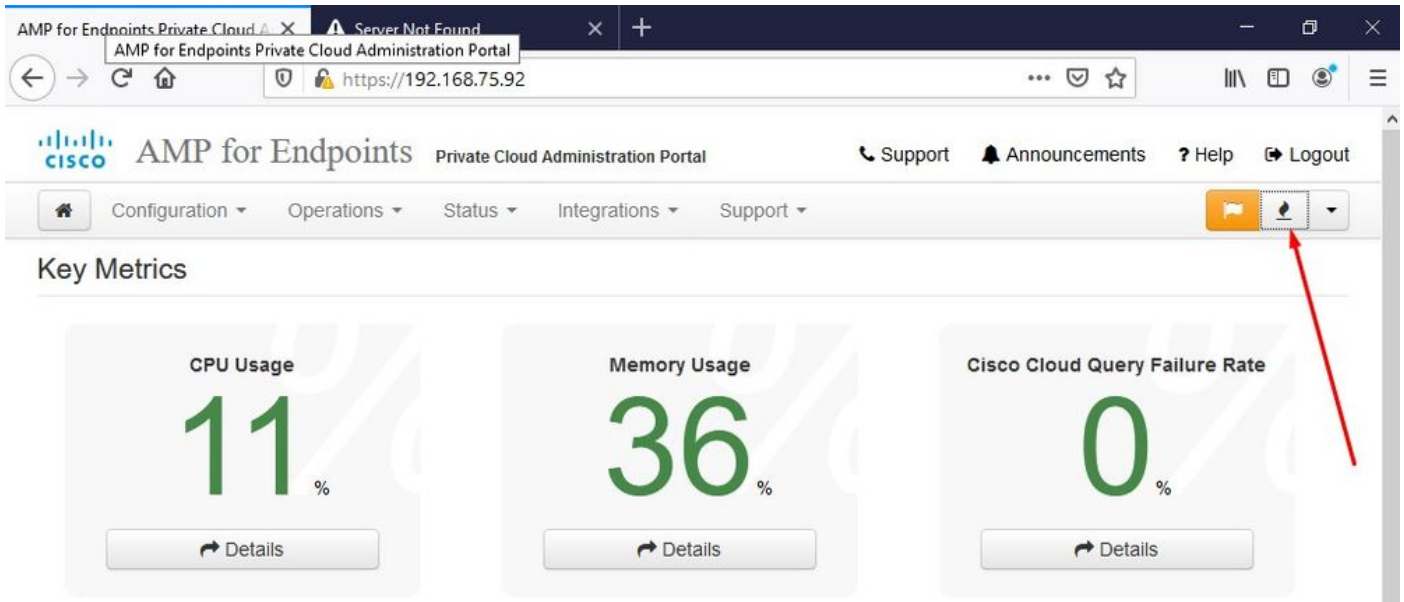
Après quelques minutes...



### Key Metrics



De là, vous accédez à la console Secure Endpoint. Cliquez sur la petite icône qui ressemble à un feu dans le coin droit à côté du drapeau.



≡ ≡ ENTREFER UNIQUEMENT ≡ ≡

Comme vous pouvez le voir, nous avons échoué à la vérification de la santé mentale en raison de DB Protect Snapshot , aussi Client Definitions, DFC et Tetra. Cette opération doit être effectuée par mise à jour hors ligne via un fichier ISO téléchargé préalablement préparé par amp-sync et téléchargé sur la machine virtuelle ou stocké dans l'emplacement NFS.



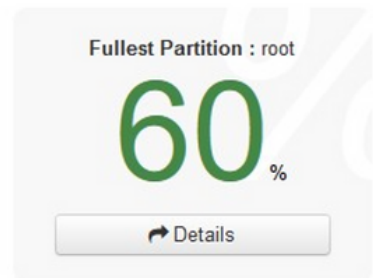
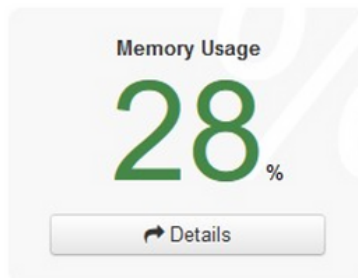
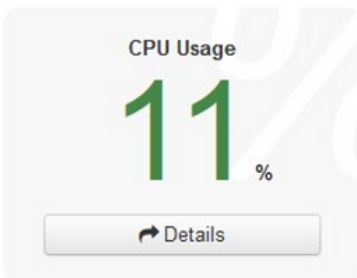
**Sanity Check Failing**

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.

## Ensemble de mise à jour AirGap

Pour la première fois, nous devons utiliser cette commande afin de recevoir la base de données Protect

```
./amp-sync a11
```

 Remarque : téléchargez tous les packages à l'aide de cette commande, puis vérifiez qu'ils peuvent prendre plus de 24 heures. Dépend de la vitesse et de la qualité de la liaison. Dans mon cas, avec la fibre 1Gig, il faut encore 25 heures pour le réaliser. En partie, cela est également dû au fait que ce téléchargement est directement à partir d'AWS et donc est limité. Enfin, notez que ce téléchargement est assez volumineux. Dans mon cas, le fichier téléchargé était de 323 Go.

Dans cet exemple, nous avons utilisé CygWin64

1. Téléchargez et installez la version x64 de Cygwin.
2. Exécutez setup-x86\_64.exe et suivez le processus d'installation en sélectionnant toutes les valeurs par défaut.

3. Choisissez un miroir de téléchargement.

4. Sélectionnez les packages à installer :

Tout -> Filet -> boucle

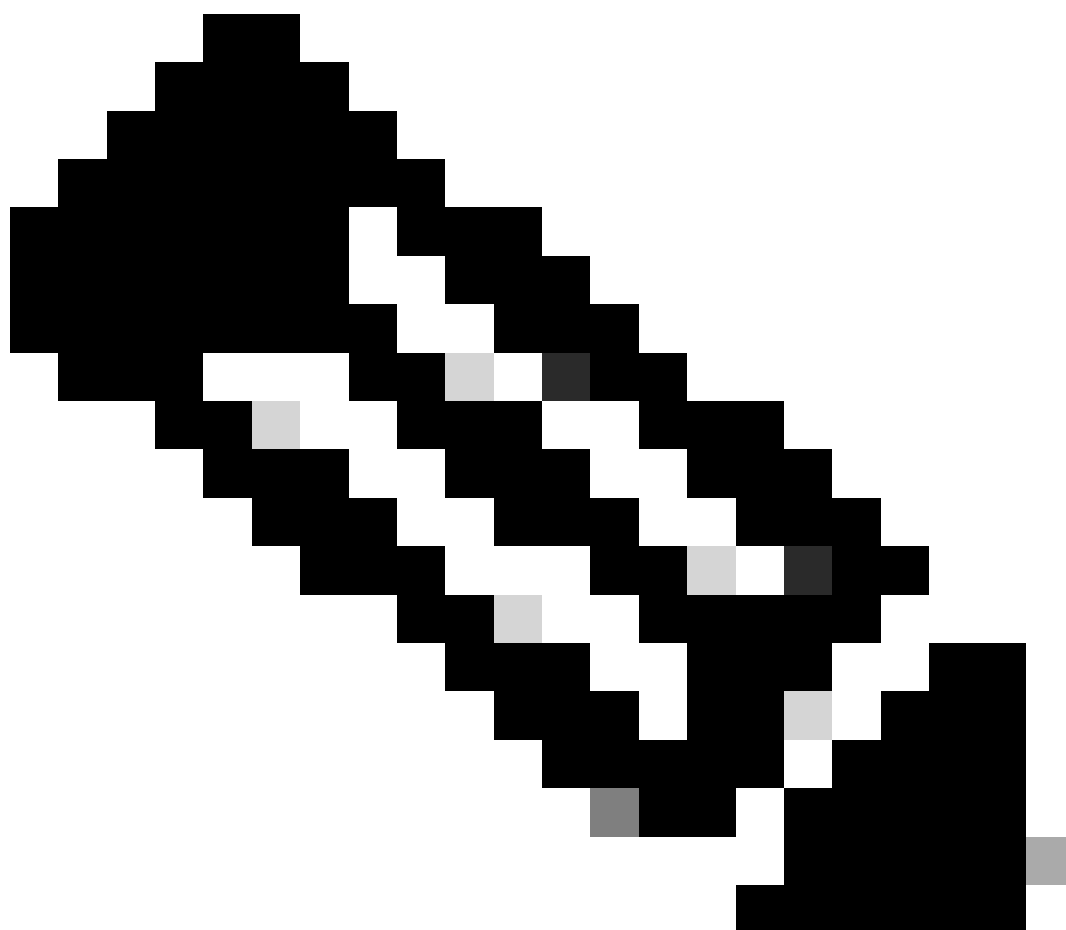
Tous -> Utils -> genisoimage

Tous -> Utilitaires -> 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/e6f73d52fc5079064aff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-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
```

```
User@VMStation-1 ~
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 ~
$
```



Remarque : Dans la dernière mise à jour VPC 3.8.x avec CygWin64 comme outil de téléchargement principal, vous pouvez rencontrer ce problème décrit ci-dessous.

---

```
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.
```

[Notes de version](#) Page #58. Comme vous pouvez le voir, «xorriso» est maintenant nécessaire. Nous avons changé le format de l'ISO en ISO 9660 et cette dépendance est ce qui convertit l'image au format approprié afin que la mise à jour puisse se terminer. Malheureusement, CygWin64 n'offre xorriso dans aucun de leurs dépôts intégrés. Cependant, pour ceux qui voudraient toujours utiliser CygWin64, il y a un moyen de surmonter ce problème.

# 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

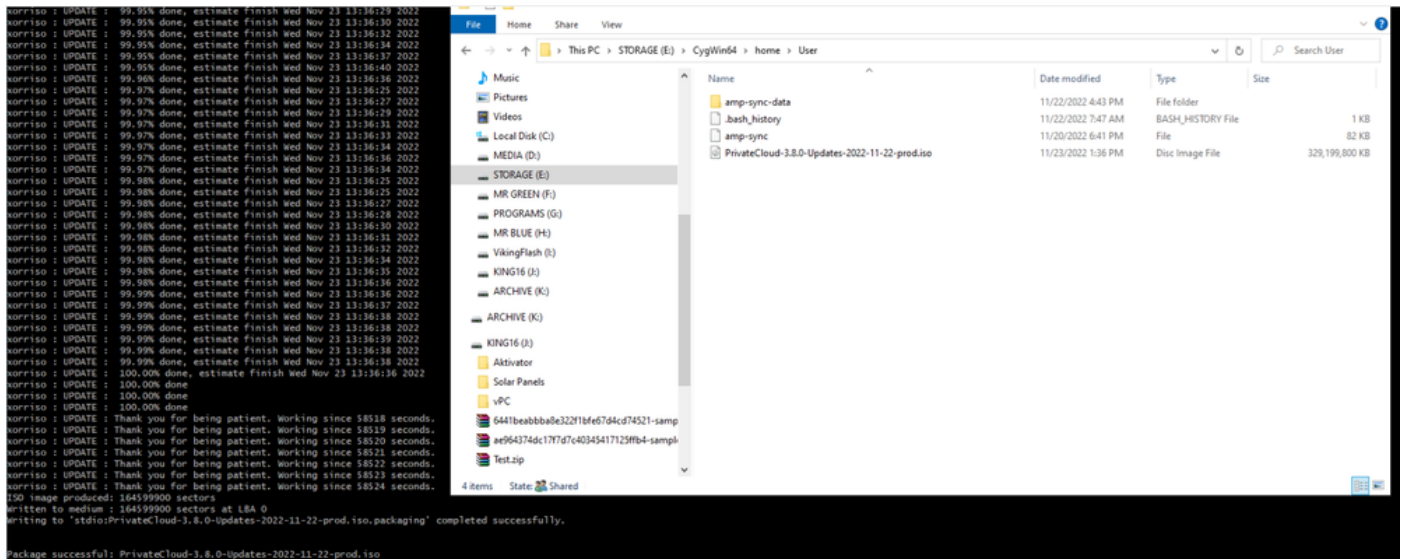
To run amp-sync you will first have to install xorriso and xmlstarlet.

- 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`

Pour pouvoir utiliser CygWin une fois de plus, vous devez télécharger manuellement xorriso à partir du référentiel GitHub. Ouvrez votre navigateur et tapez <Latest xorriso.exe 1.5.2 pre-build for Windows> il devrait apparaître comme premier lien nommé comme <PeyTy/xorriso-exe-for-windows - GitHub> naviguez jusqu'à cette page GitHub et téléchargez le fichier <xorriso-exe-for-windows-master.zip> à l'intérieur du fichier zip que vous trouvez parmi quelques autres fichiers nommés <xorriso.exe> copiez et collez ce fichier dans le <CygWin64\bin> chemin votre installation locale de CygWin. Réessayez d'exécuter la commande <amp-sync>. Vous ne devriez plus voir le message d'erreur et le début et la fin du téléchargement comme indiqué dans l'image.



Effectuez la sauvegarde du VPC 3.2.0 actuel (dans ce cas) en mode d'entrefre.

Vous pouvez utiliser cette commande à partir de CLI

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

Vous pouvez également accéder à Opérations > Sauvegardes, comme indiqué dans l'image et Effectuer la sauvegarde là.





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

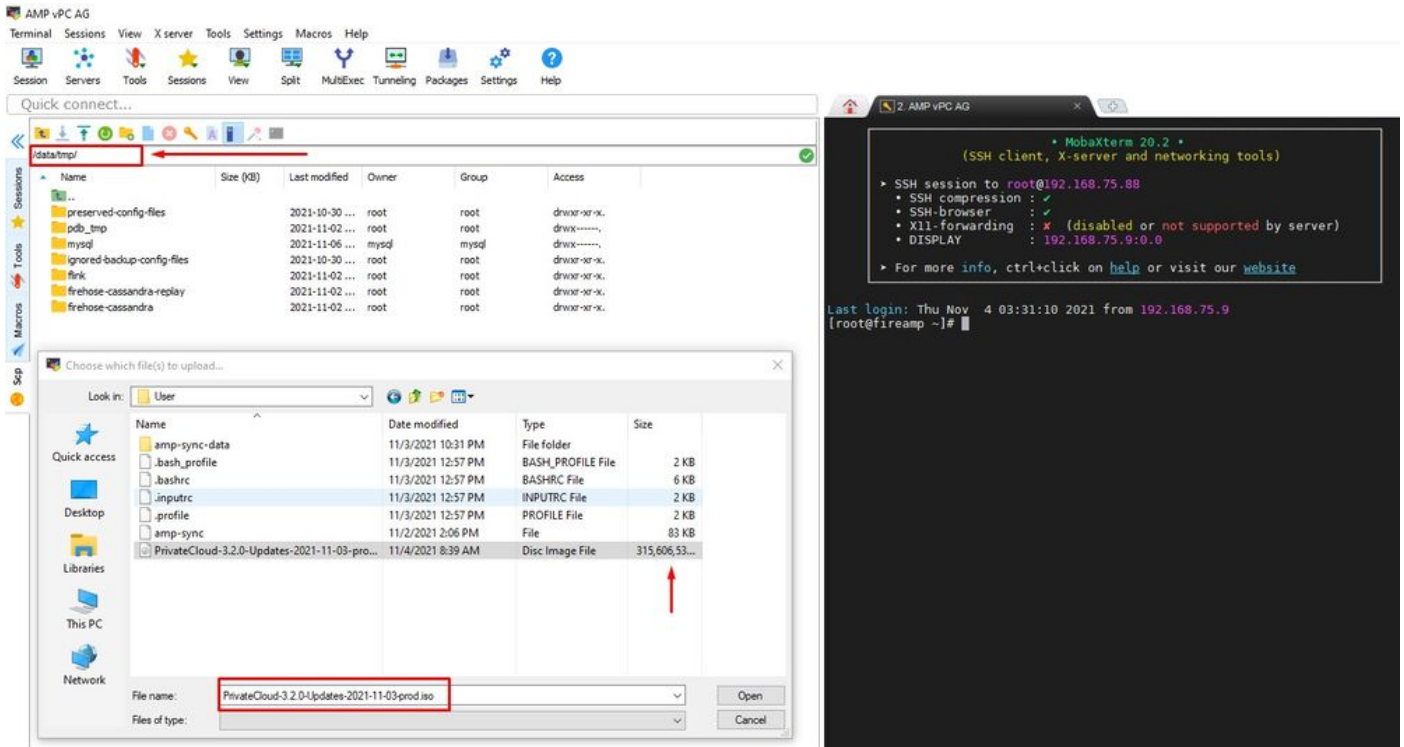
### Previous Backups

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	 

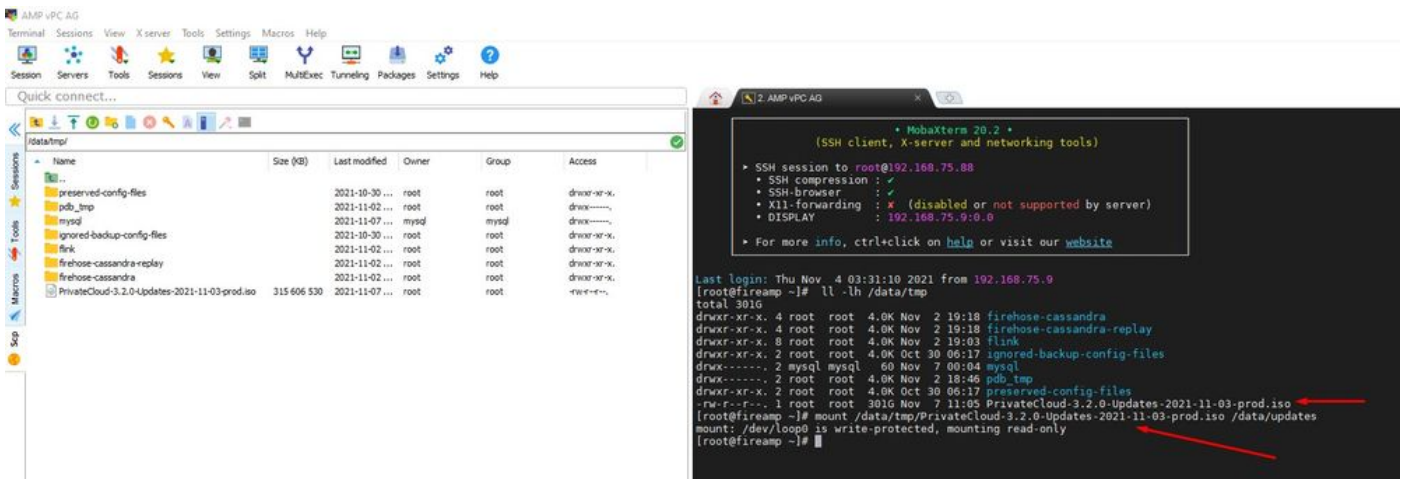
Transférez la dernière image ISO générée avec amp-sync vers le VPC. Cela peut prendre jusqu'à plusieurs heures en fonction de votre vitesse. Dans ce cas, le transfert a pris plus de 16 heures

/data/tmp



Une fois le téléchargement terminé, montez l'ISO

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



Accédez à opadin UI pour effectuer la mise à jour Operations > Update Device > Sélectionnez

Check update ISO.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. On the right, there are links for 'Announcements', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. A 'Sanity Check Failing' alert is visible in a red box. The main content area has a heading '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 displays version '3.2.0\_202010081917' for 'Client Definitions, DFC, Tetra Content Version' with an 'ABSENT' status for 'Protect DB Version'. It includes buttons for 'Update Content' and 'Import Protect DB', and a message: 'Import a Protect DB snapshot to your standalone device.' The 'Software' section displays version '3.2.0\_202010082118' for 'Private Cloud Software Version' with a message: 'A software update is available.' and an 'Update Software' button.

Dans cet exemple, je passe d'abord à la mise à jour du contenu

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.

Sélectionnez ensuite Importer la base de données protégée.

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.

Comme vous pouvez le constater, il s'agit d'un autre processus très long qui peut prendre beaucoup de temps.

## 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
<span style="background-color: #f96; padding: 2px;">▶ Running</span>	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
<span style="background-color: #f96; padding: 2px;">▶ Running</span>	<span style="border: 1px solid red; padding: 2px;">2021-11-19 17:04:05 +0000 about 20 hours ago</span>	⌚ 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).
```



## Problème #1 - Salle épuisée dans le magasin de données

Ici, vous pouvez courir à deux questions. Puisque les vPC antérieurs à la version 3.5.2 n'ont pas la possibilité de monter un stockage NFS externe, vous devez télécharger le fichier ISO de mise à jour dans le répertoire /data/temp. Dans mon cas, comme mon datastore ne comptait que 1 To, je suis sorti de la pièce en courant et la machine virtuelle s'est écrasée. En d'autres termes, vous avez besoin d'au moins 2 To d'espace sur votre Data Store pour déployer avec succès le VPC AirGap dont la version est inférieure à 3.5.2

L'image ci-dessous provient du serveur ESXi. Elle indique l'erreur suivante : il n'y a plus d'espace disponible sur le disque dur lorsque vous essayez de démarrer la machine virtuelle. J'ai pu récupérer de cette erreur en basculant temporairement les 128 Go de RAM sur 64 Go. Puis j'ai pu redémarrer à nouveau. Rappelez-vous également que si vous provisionnez cette machine virtuelle en tant que client léger, l'inconvénient du déploiement du client léger est que la taille du disque peut augmenter, mais elle ne diminuerait pas même si vous libérez de l'espace. En d'autres termes, supposons que vous avez téléchargé votre fichier de 300 Go dans le répertoire du vPC, puis que vous l'avez supprimé. Le disque d'ESXi présente toujours 300 Go d'espace en moins sur votre disque dur



## Problème #2 - Ancienne mise à jour

Le 2<sup>e</sup> problème est que si vous exécutez la mise à jour logicielle d'abord comme je l'ai fait dans mon 2<sup>e</sup> essai et à partir de 3.2.0 je me retrouve avec VPC pour mettre à niveau vers 3.5.2 et à cause de cela, j'ai dû télécharger un nouveau fichier de mise à jour ISO depuis la 3.2.0 est devenu invalide en raison d'un fait que je n'étais plus sur la version originale 3.2.0.

**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.

Il s'agit de l'erreur que vous voyez si vous essayez de monter à nouveau le fichier de mise à jour ISO.



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

Cette image montre une autre façon de monter une image de mise à jour sur votre VPC. Dans la version 3.5.x, vous pouvez utiliser un emplacement distant tel que le stockage NFS pour partager le fichier de mise à jour avec votre VPC.



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.](#)

Sanity Check Failing est lié à Protect DB qui n'est pas actuellement disponible sur le VPC



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

La prochaine mise à jour démarre automatiquement



### ⚙ 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*

Après ce très long processus d'importation de la base de données Protect DB, vous pouvez déplacer et mettre à jour la définition du client et le logiciel, ce qui peut prendre approximativement plus de 3 heures.

## ✔ 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

Enfin, notez que ce processus prendra beaucoup de temps.

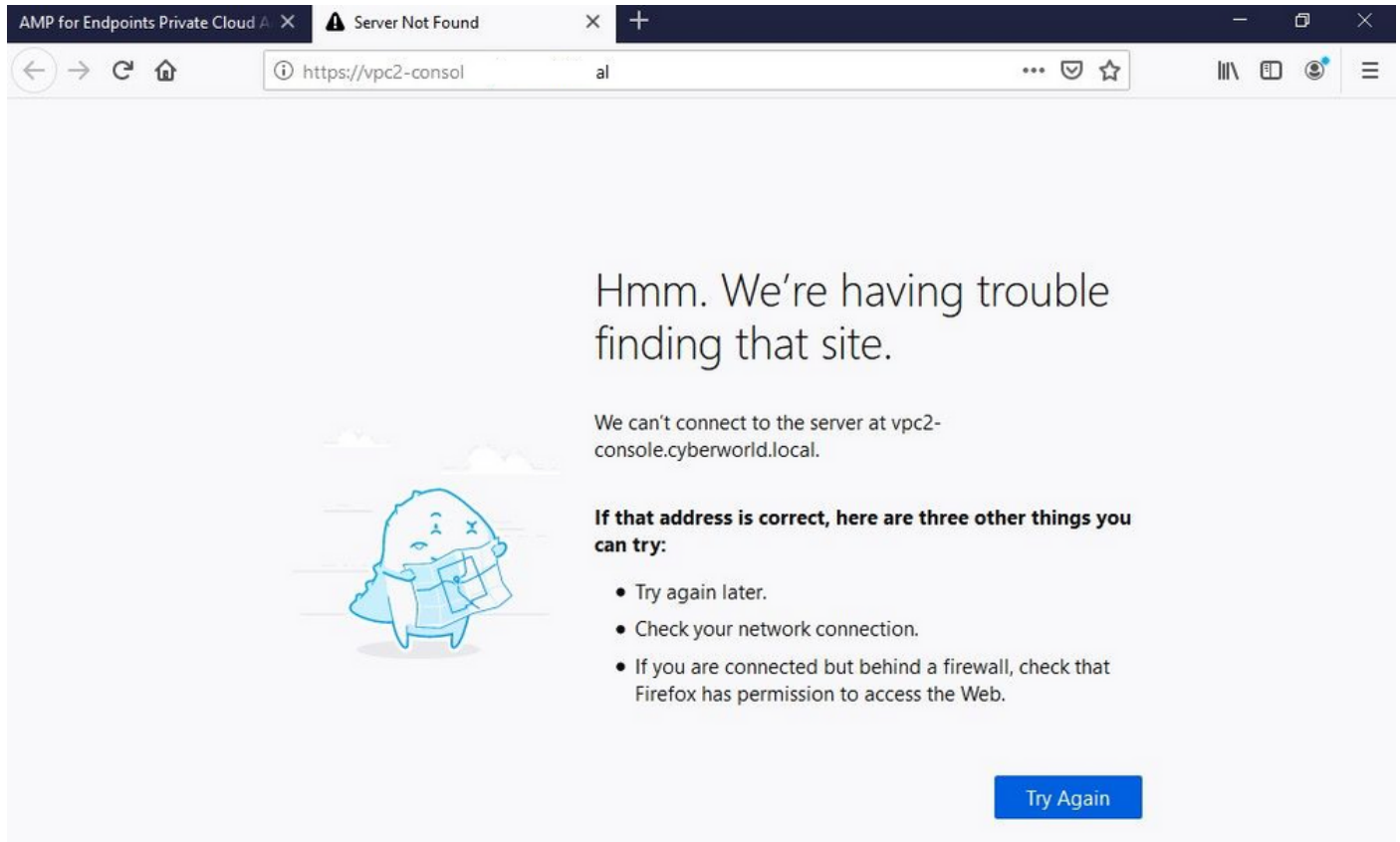
Pour l'appliance VPC visitez ce TZ qui contiennent d'autres méthodes comment mettre à jour l'appliance matérielle, monter le fichier ISO et démarrer à partir de l'USB.

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

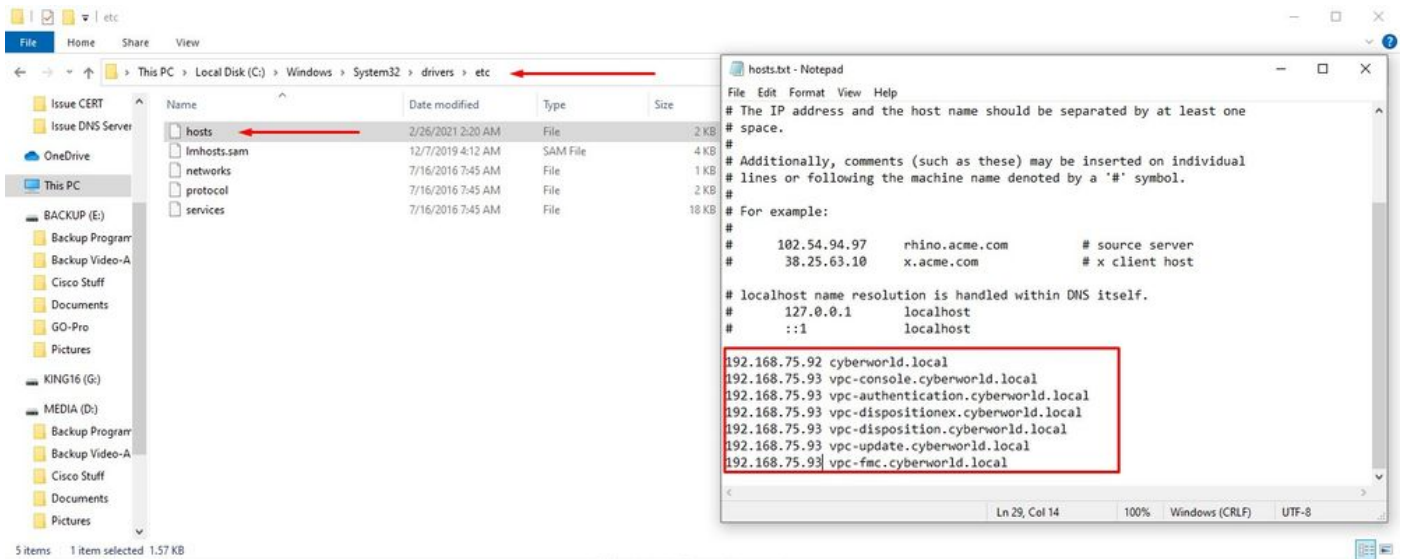
# Dépannage de base

## Problème #1 - FQDN et serveur DNS

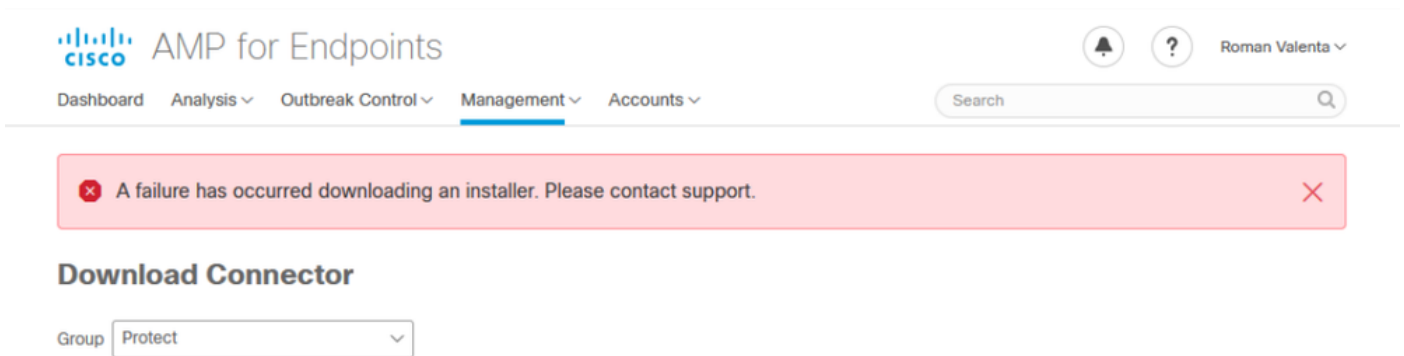
Le premier problème que vous pouvez rencontrer est si votre serveur DNS n'est pas établi et que tous les FQDN ne sont pas correctement enregistrés et résolus. Le problème peut ressembler à ceci lorsque vous essayez d'accéder à la console Secure Endpoint via l'icône « Fire » de Secure Endpoint. Si vous utilisez uniquement l'adresse IP, cela fonctionne, mais vous ne pouvez pas télécharger le connecteur. Comme vous pouvez le voir sur la 3<sup>e</sup> image ci-dessous.



Si vous modifiez le fichier HOSTS sur votre machine locale comme indiqué dans l'image, résolvez le problème et vous obtenez des erreurs.



Vous recevez cette erreur lorsque vous essayez de télécharger le programme d'installation du connecteur Secure Endpoint.



Après un dépannage, la seule solution correcte a été de configurer le serveur DNS.

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
```

Une fois que vous avez enregistré tous les FQDN sur votre serveur DNS et que vous avez modifié l'enregistrement dans le cloud privé virtuel de DNS public à votre serveur DNS, tout commence à fonctionner comme prévu.



### Configure network settings.

Admin	Cisco Cloud	eth0 / 00:0C:29:A6:4A:11
	<b>Network</b>	IP Assignment 192.168.75.92 <a href="#">More details</a>
	Date and Time	
	Certificate Authorities	
	Proxy	
Inter	Notifications	eth1 / 00:0C:29:A6:4A:1B
	License	IP Assignment 192.168.75.93 <a href="#">More details</a>
	Email	
	Backup	
	SSH	
	Syslog	IP Assignment Static
	Updates	IP Address 192.168.75.93
	Services	<input checked="" type="checkbox"/> 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.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.





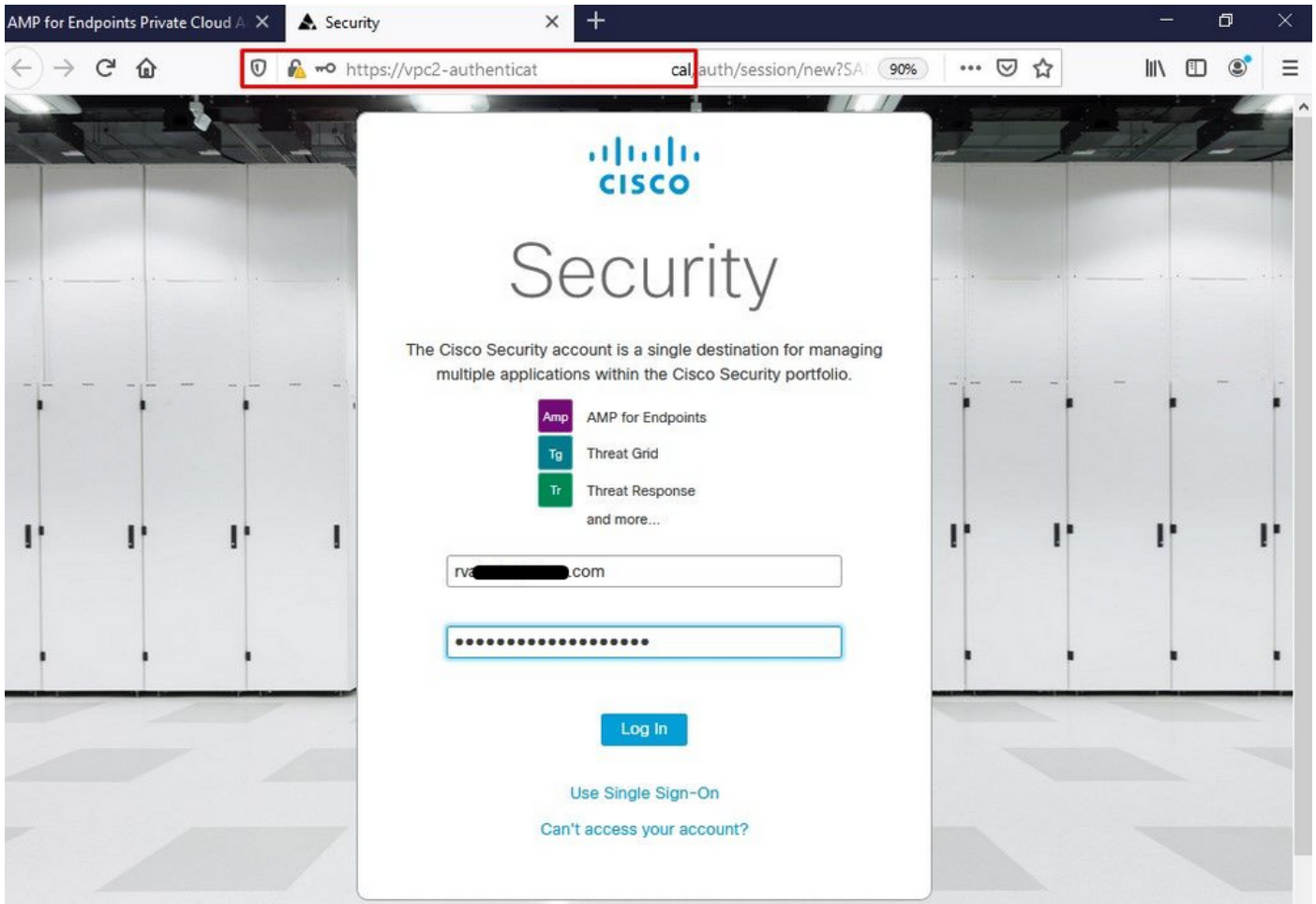
State	Started	Finished	Duration
	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

### 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

À ce stade, vous pouvez vous connecter et télécharger le connecteur



Vous obtenez l'assistant de stratégie de point de terminaison sécurisé initial pour votre environnement. Il vous guide tout au long de la sélection du produit antivirus que vous utilisez, le cas échéant, ainsi que du proxy, et des types de stratégies que vous souhaitez déployer. Sélectionnez le bouton Set Up (Configurer) approprié en fonction du système d'exploitation du connecteur.

La page Existing Security Products (Produits de sécurité existants) s'affiche, comme illustré dans l'image. Sélectionnez les produits de sécurité que vous utilisez. Il génère automatiquement des exclusions applicables pour éviter les problèmes de performances sur vos terminaux. Sélectionnez Suivant.

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.

Connecteur de téléchargement.

🟢 Step 1: Existing Security Products

🟢 Step 2: Set Up Proxy

🟢 Step 3: Download Connector

Audit Only	Protect	Triage	Server	installing a connector on Windows Domain Controllers.
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.	
<a href="#">Policy Details</a>	<a href="#">Policy Details</a>	<a href="#">Policy Details</a>	<a href="#">Requirements</a>	<a href="#">Requirements</a>
<b>Files</b> Audited <b>Network</b> Blocked <b>Offline Engine</b> TETRA	<b>Files</b> Quarantined <b>Network</b> Blocked <b>Offline Engine</b> TETRA	<b>Files</b> Quarantined <b>Network</b> Blocked <b>Offline Engine</b> TETRA	<b>Files</b> Audited <b>Network</b> Off <b>Offline Engine</b> TETRA	<b>Files</b> Audited <b>Network</b> Off <b>Offline Engine</b> TETRA
<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>

[< Back](#)
[Next >](#)

Step 4: Verify, Contain, and Protect

Opening amp\_Protect.exe

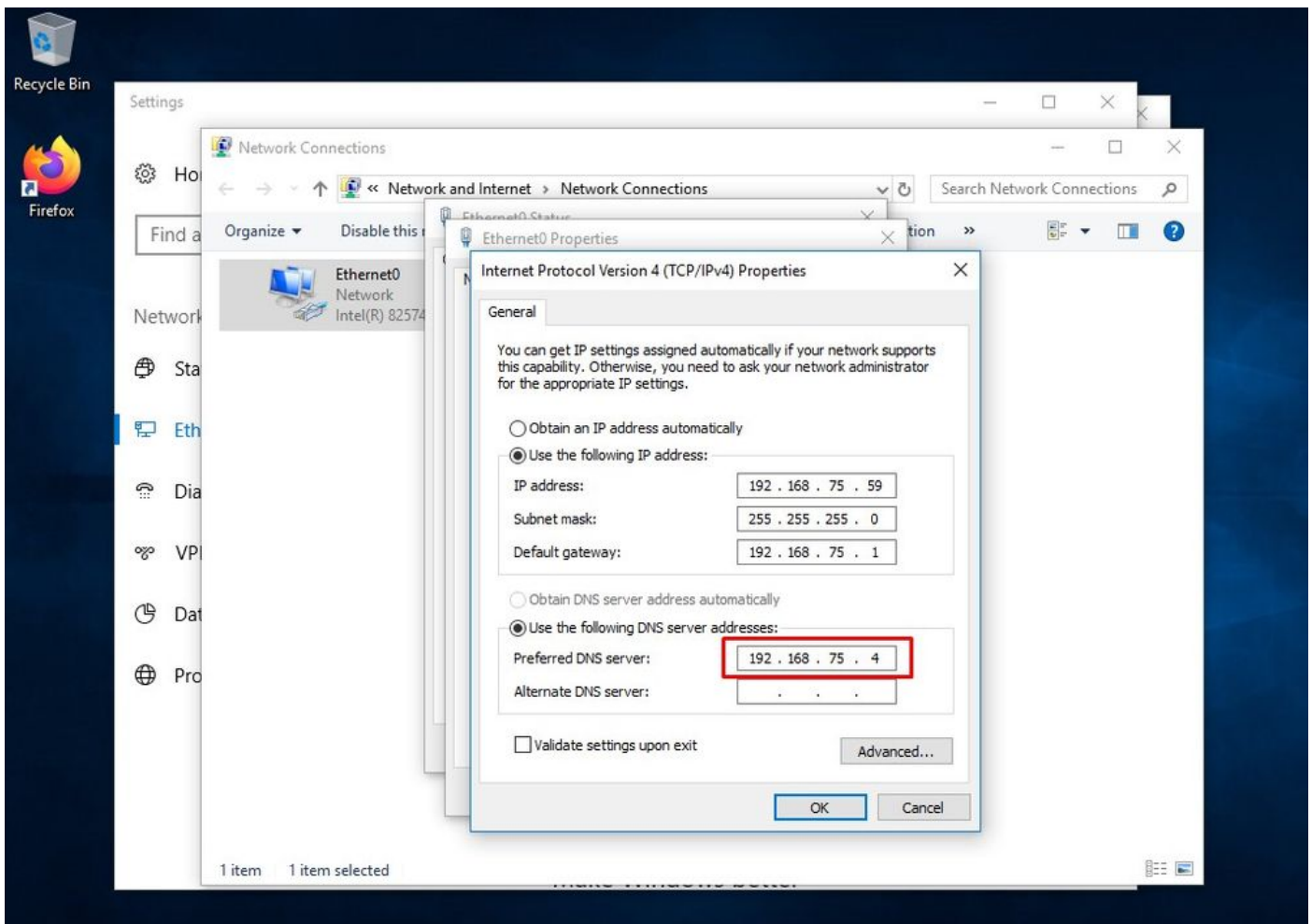
You have chosen to open:

**amp\_Protect.exe**  
 which is: **exe File**  
 from: <https://vpc-console.cyberworld.local>

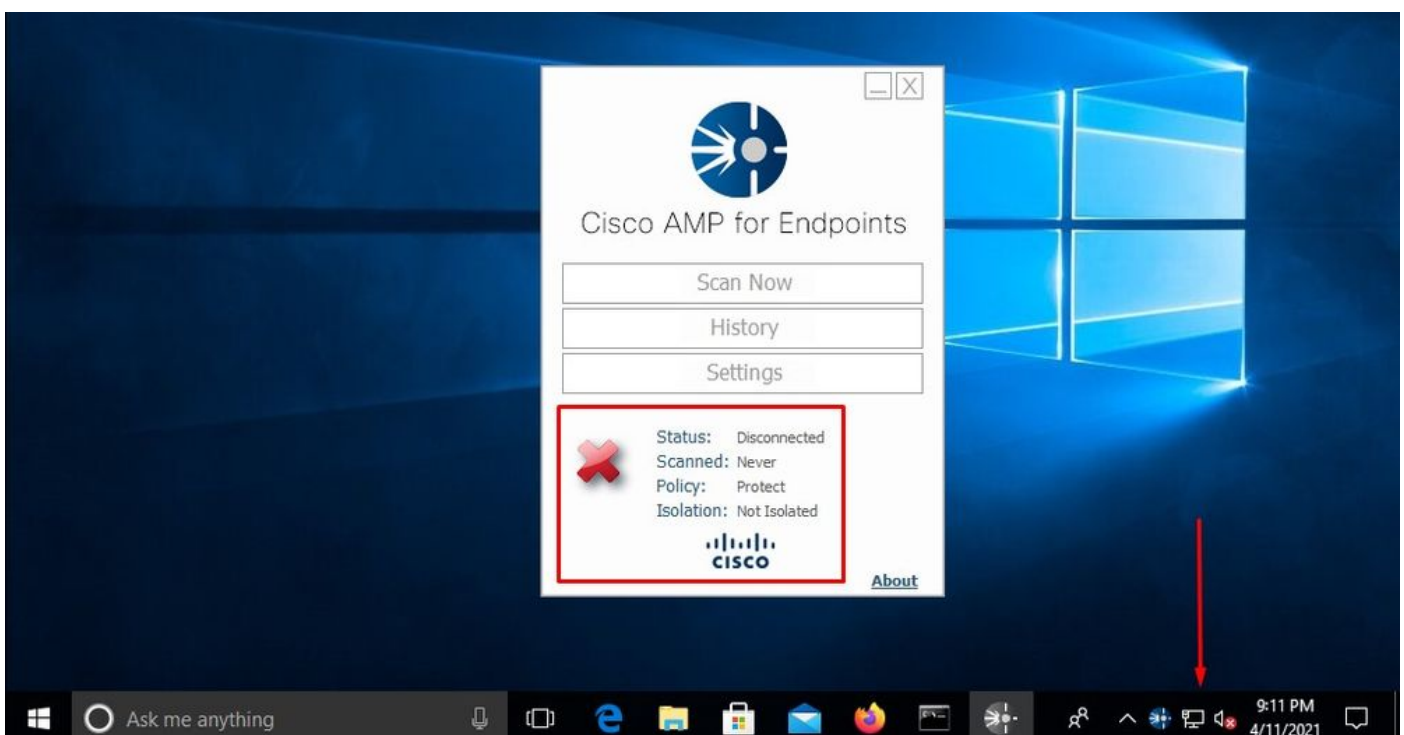
Would you like to save this file?

## Problème #2 - Problème avec l'autorité de certification racine

Si vous utilisez vos propres certificats internes, le problème suivant que vous pouvez rencontrer est qu'après l'installation initiale, le connecteur peut apparaître comme déconnecté.



Une fois le connecteur installé, Secure Endpoint peut être considéré comme déconnecté. Exécutez l'ensemble de diagnostics et consultez les journaux, vous serez en mesure de déterminer le problème.





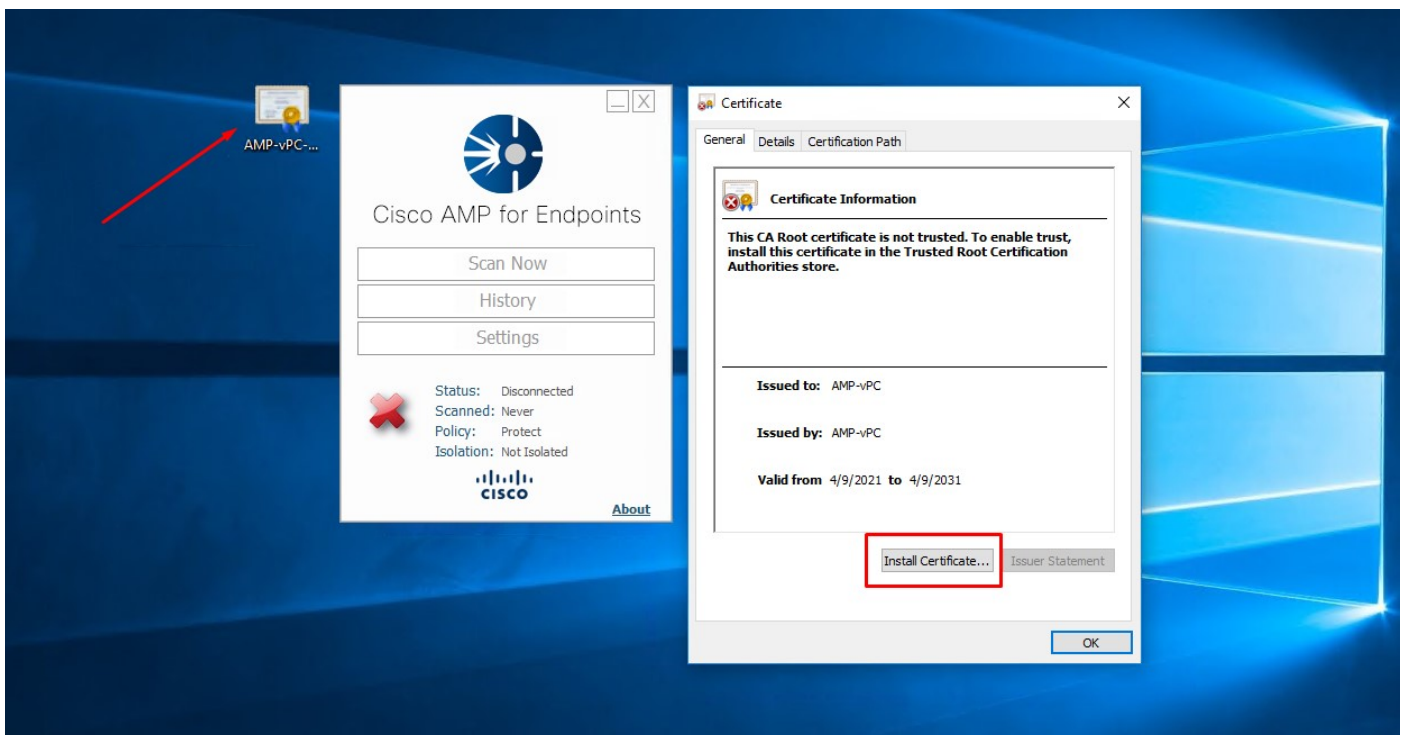
Sur la base de cette sortie collectée à partir du bundle de diagnostic, vous pouvez voir l'erreur d'autorité de certification racine

(804765, +0 ms) Mar 06 00:47:07 [8876]: [http\_client.c@1011]: GET request https://vPC-Console.cyberworl

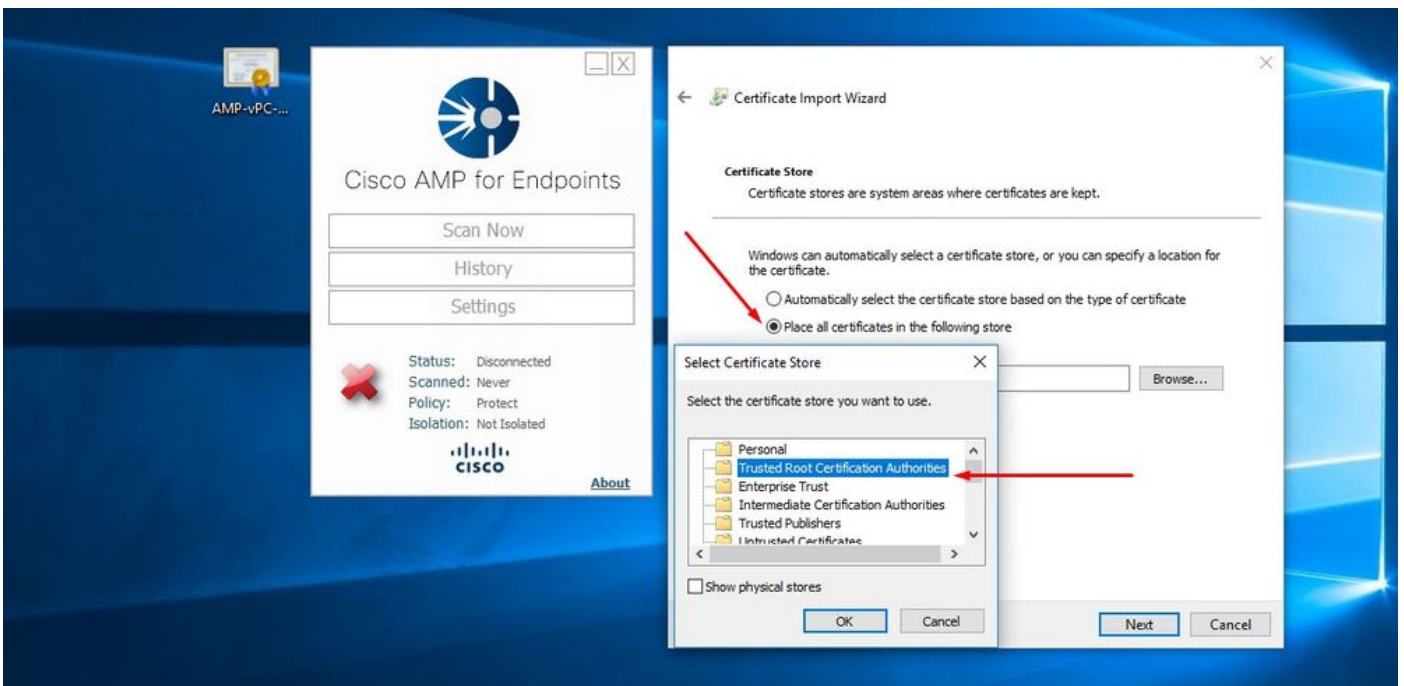
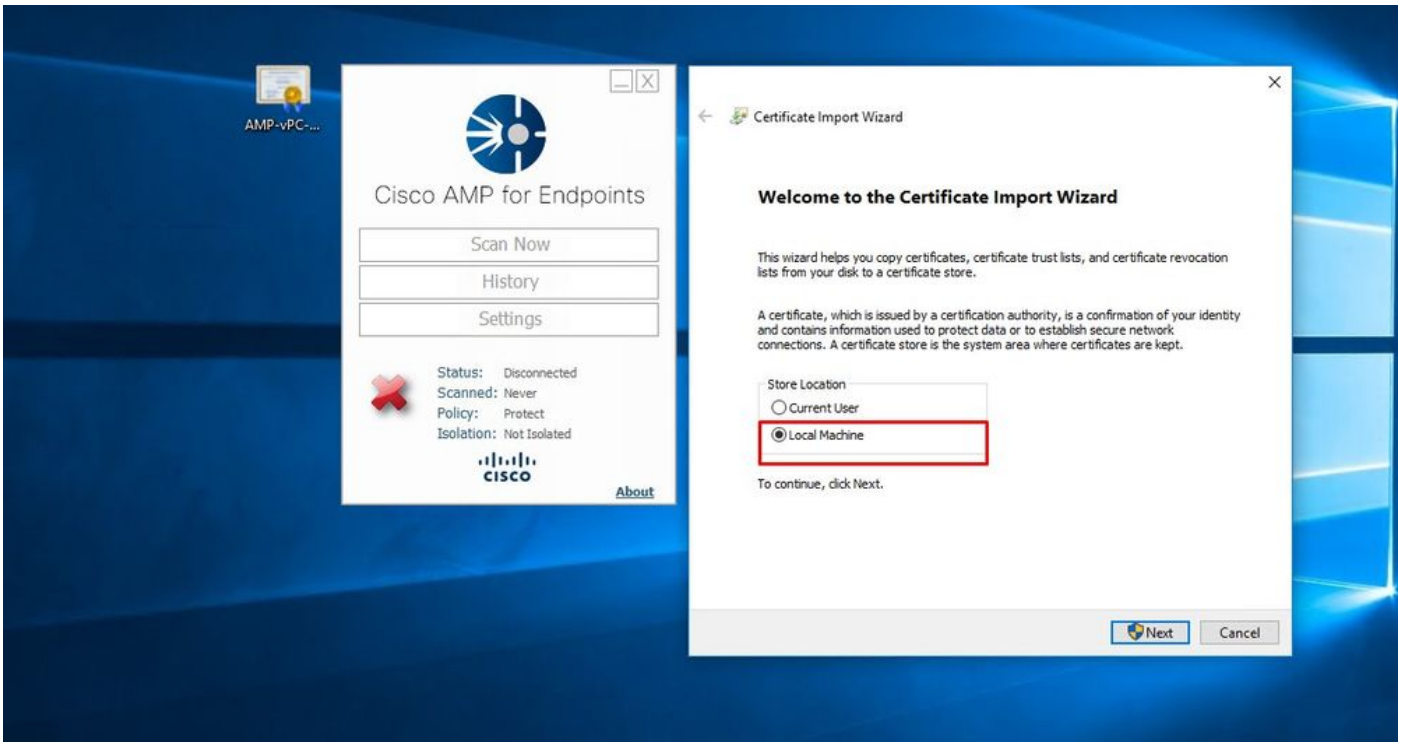
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http\_client.c@1051]: async request failed (SSL peer certificat

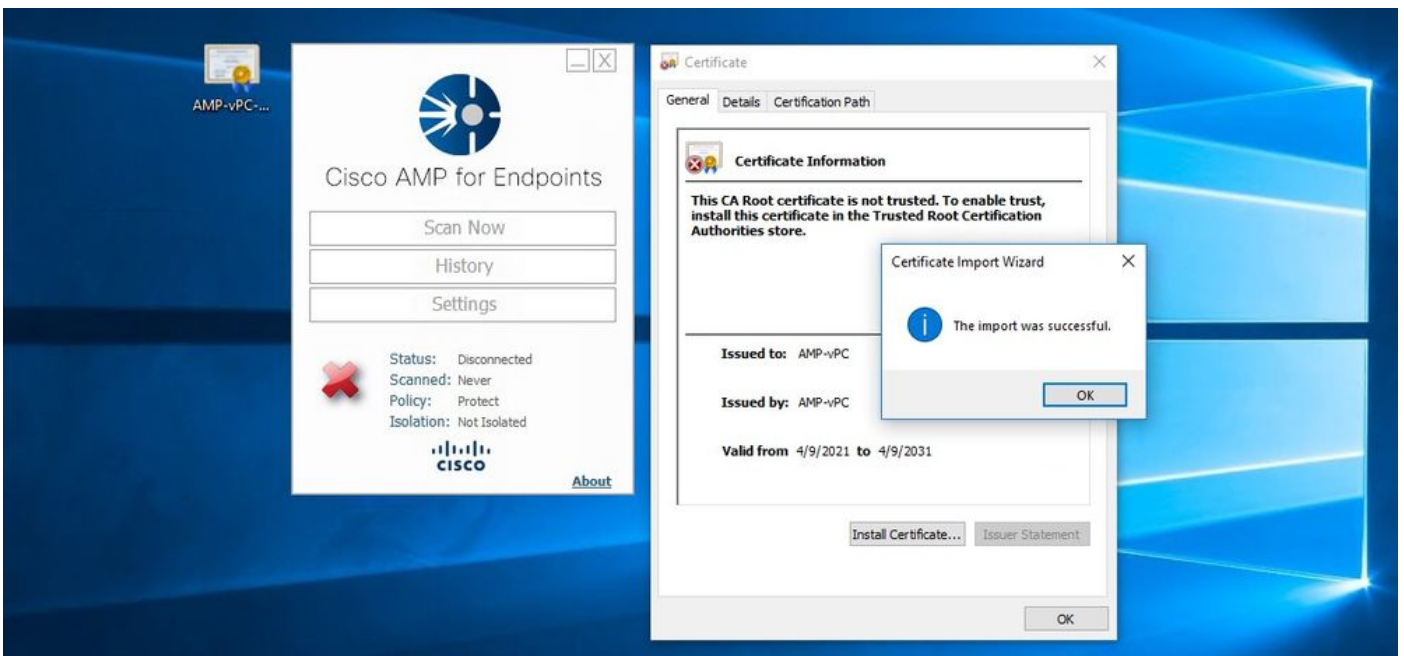
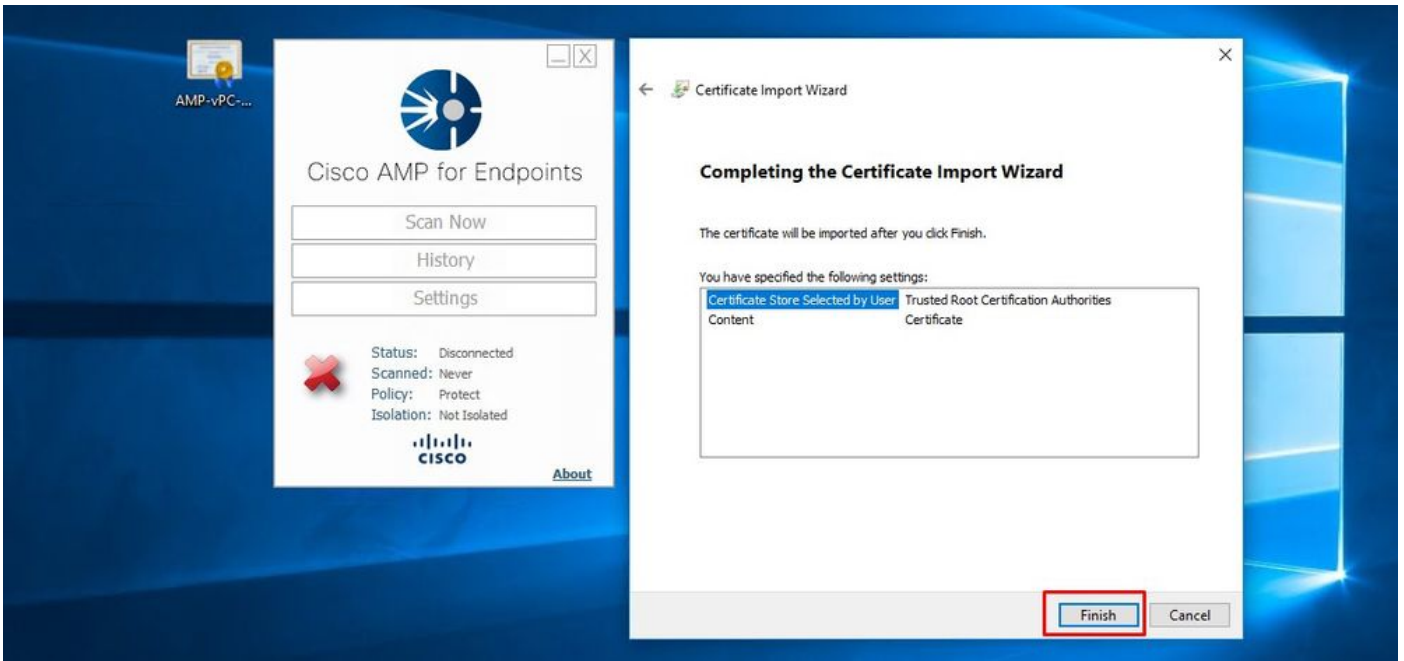
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http\_client.c@1074]: response failed with code 60

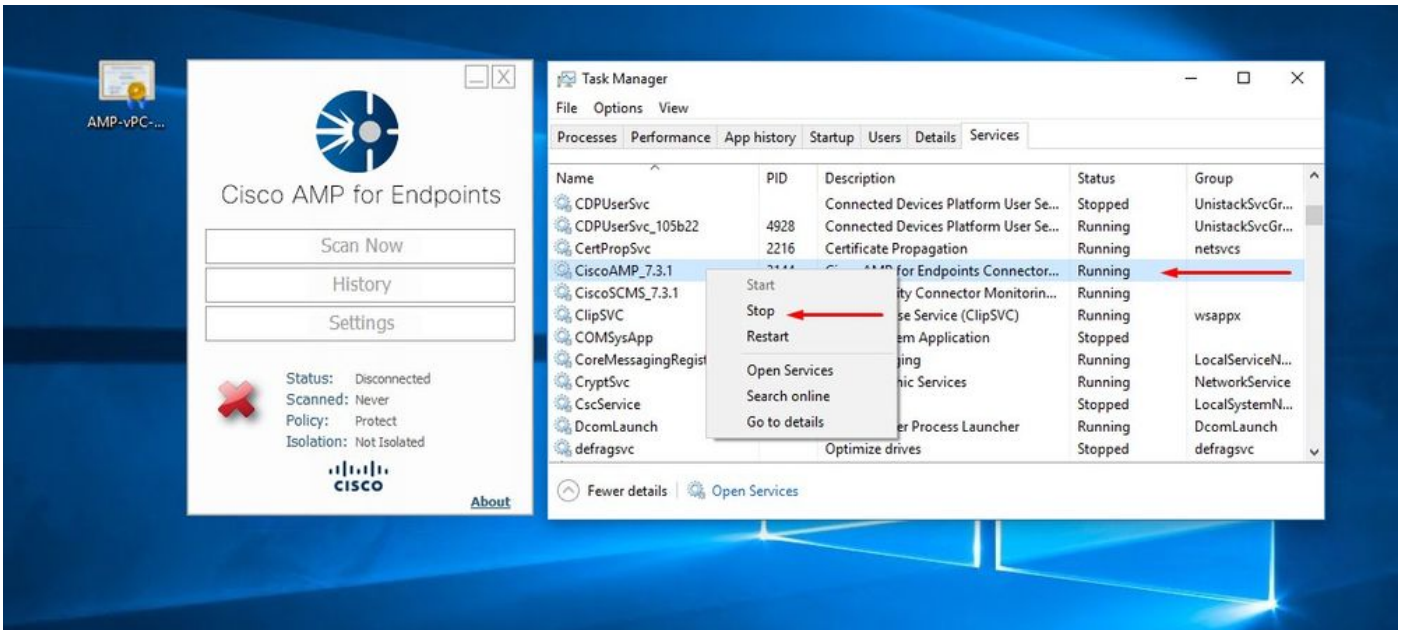
Une fois que vous avez téléchargé l'autorité de certification racine dans le magasin d'autorité de certification racine approuvée et redémarré le service Secure Endpoint. Tout commence à fonctionner comme prévu.



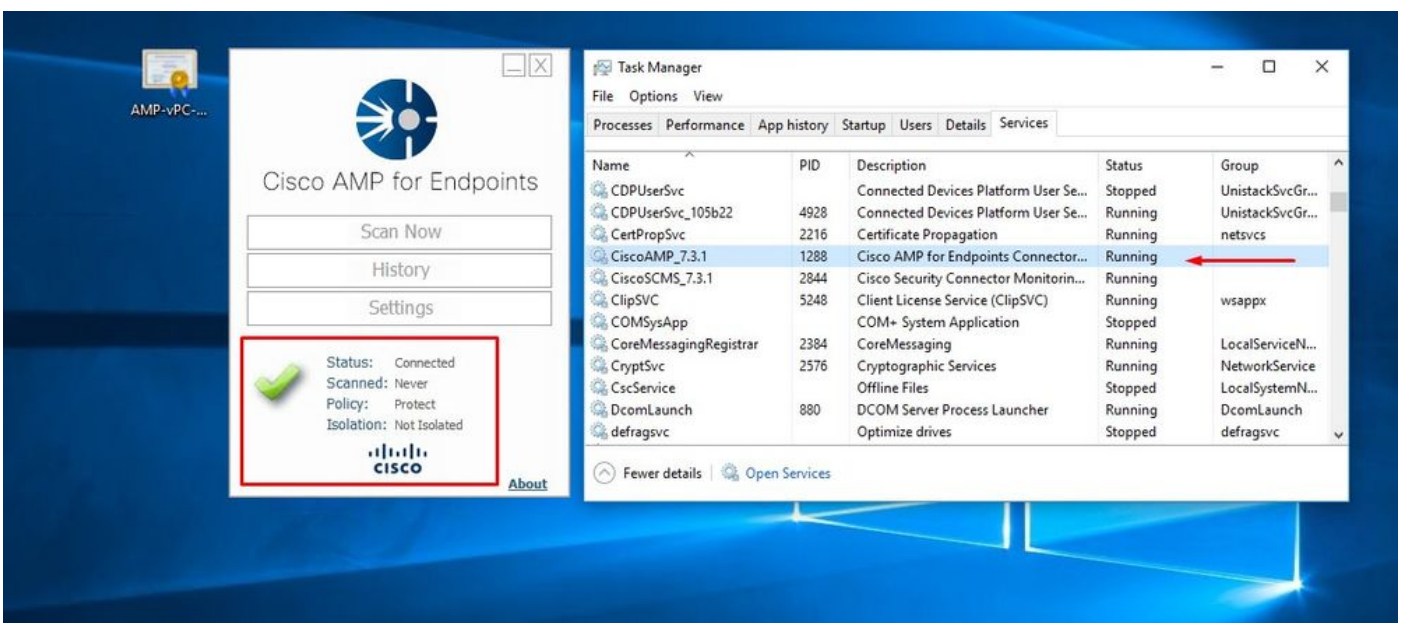








Une fois le connecteur de service Secure Endpoint remis en service, mettez-le en ligne comme prévu.



The screenshot displays the AMP for Endpoints Private Cloud console dashboard. At the top, the browser address bar shows the URL `https://vpc2-console`. The dashboard header includes navigation tabs: **Dashboard**, **Inbox**, **Overview**, and **Events**. Below the header, there are controls for **Refresh All**, **Auto-Refresh**, **Reset**, and **New Filter**. The main dashboard area is divided into several sections:

- 0% compromised**: A large percentage indicator at the top left.
- Inbox Status**: Shows 0 Require Attention, 0 In Progress, and 0 Resolved.
- Compromises**: A section with a "Protect" button and a "0 / 1" indicator.
- Quarantined Detections**: A section with a "Protect" button and a "0 / 1" indicator.
- Vulnerabilities**: A section with a "View" button and a "0 / 1" indicator.
- Threat Grid Analysis**: Shows 0 Automatic Analysis Submissions and 0 Retroactive Threat Detections.
- Statistics**: Shows 0 Files Scanned and 0 Network Connections Logged.
- Connectors**: Shows 1 Connectors (highlighted with a red arrow), 0 Installs, and 0 Install Failures.
- Quick Start**: Includes links for **Set Up Windows Connector**, **Set Up Mac Connector**, and **Set Up Linux Connector**.
- Significant Compromise Artifacts**: Shows "No artifacts".
- Compromise Event Types**: Shows "No event types".

Activité malveillante testée

### 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

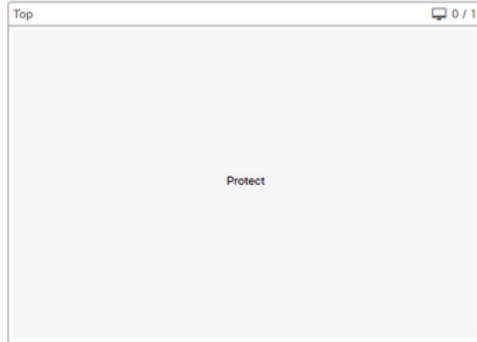
0% compromised

#### Inbox Status

0 Require Attention 0 In Progress 0 Resolved

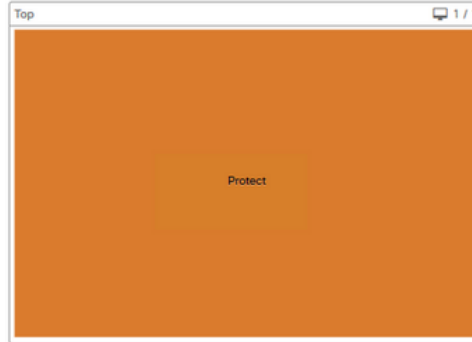
#### Compromises

Inbox



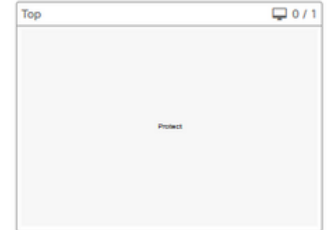
#### Quarantined Detections

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

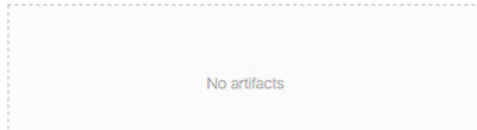
#### Quick Start

Set Up Windows Connector

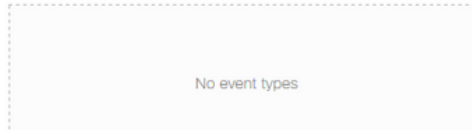
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12  
MAR APR

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



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.