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 d'utilisation 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 ESXi 5 ou version ultérieure

- Mode Cloud-proxy (uniquement) : 128 Go de RAM, 8 coeurs de processeur (2 processeurs avec 4 coeurs recommandés chacun), 1 To d'espace disque libre minimum sur le datastore VMware
- Type de lecteurs : SSD requis pour le mode air gap 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 data store pour le groupe RAID 10 (4 000) : 60 000 IOPS
- Nombre minimal d'écritures aléatoires de data store pour le groupe RAID 10 (4 000) : 30 000

IOPS

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 Cloud-proxy (uniquement) : 48 Go de RAM, 8 coeurs de processeur (2 processeurs avec 4 coeurs recommandés chacun), 1 To d'espace disque libre minimum sur le datastore VMware
- Type de lecteurs : 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 toute autre méthode prise en charge.
- 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 contenues dans ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique et elles ont uniquement pour but de vous fournir des conseils tout au long du déploiement, qui peuvent varier en fonction de la version déployée. 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.

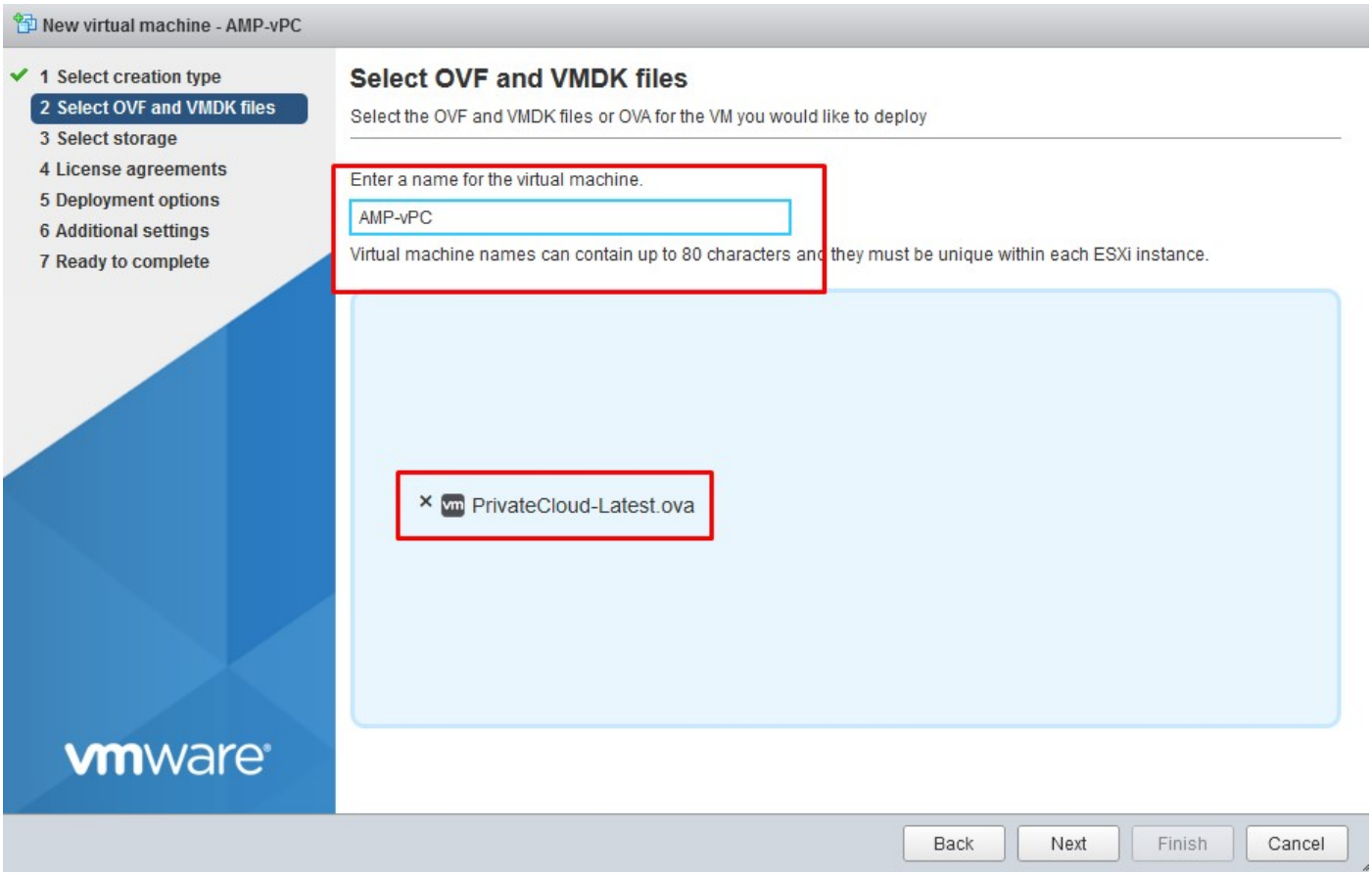
Déploiement VPC

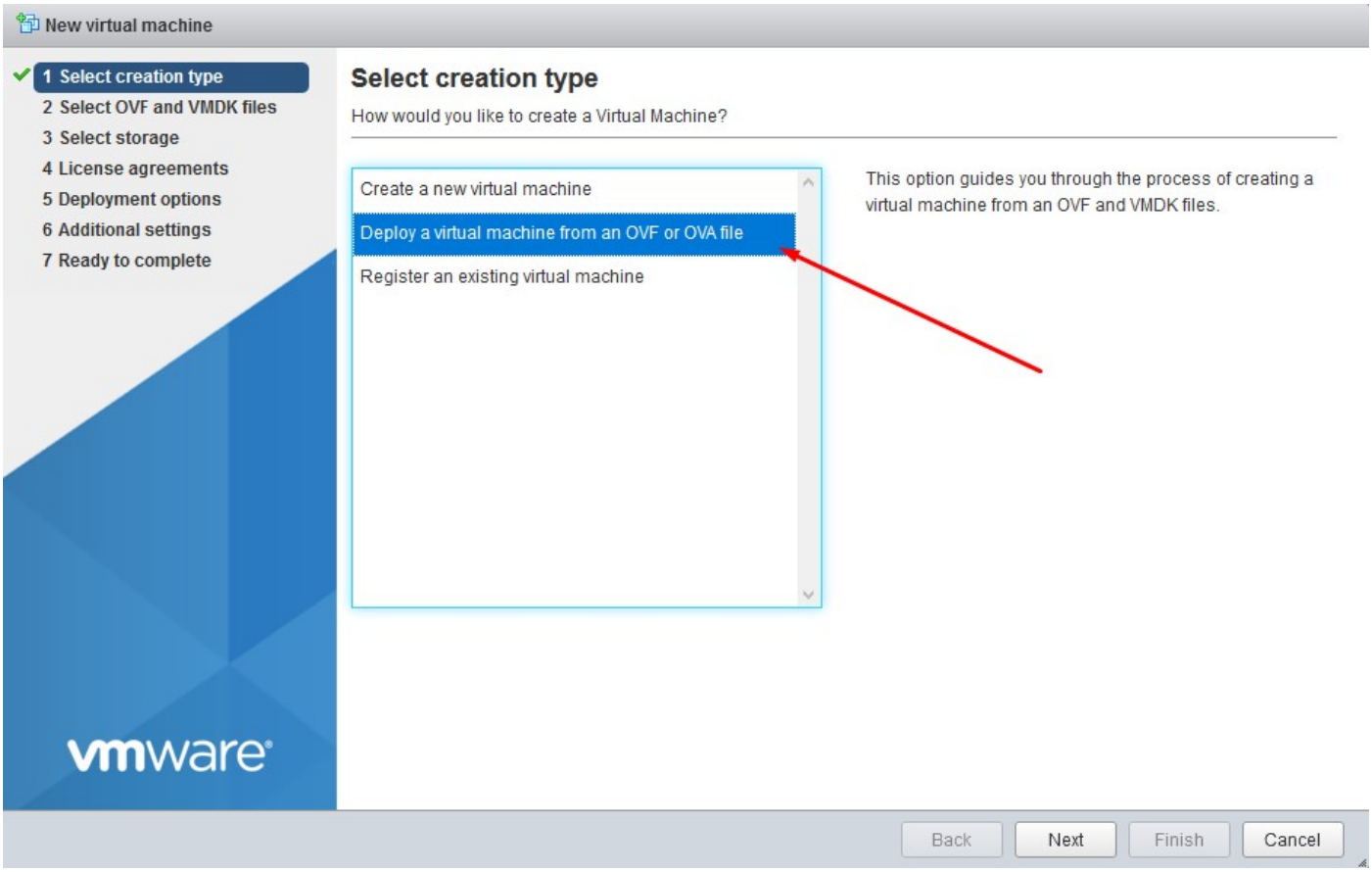
Sélectionnez l'URL fournie dans l'e-mail de livraison électronique ou d'autorisation. Téléchargez le fichier OVA et poursuivez l'installation

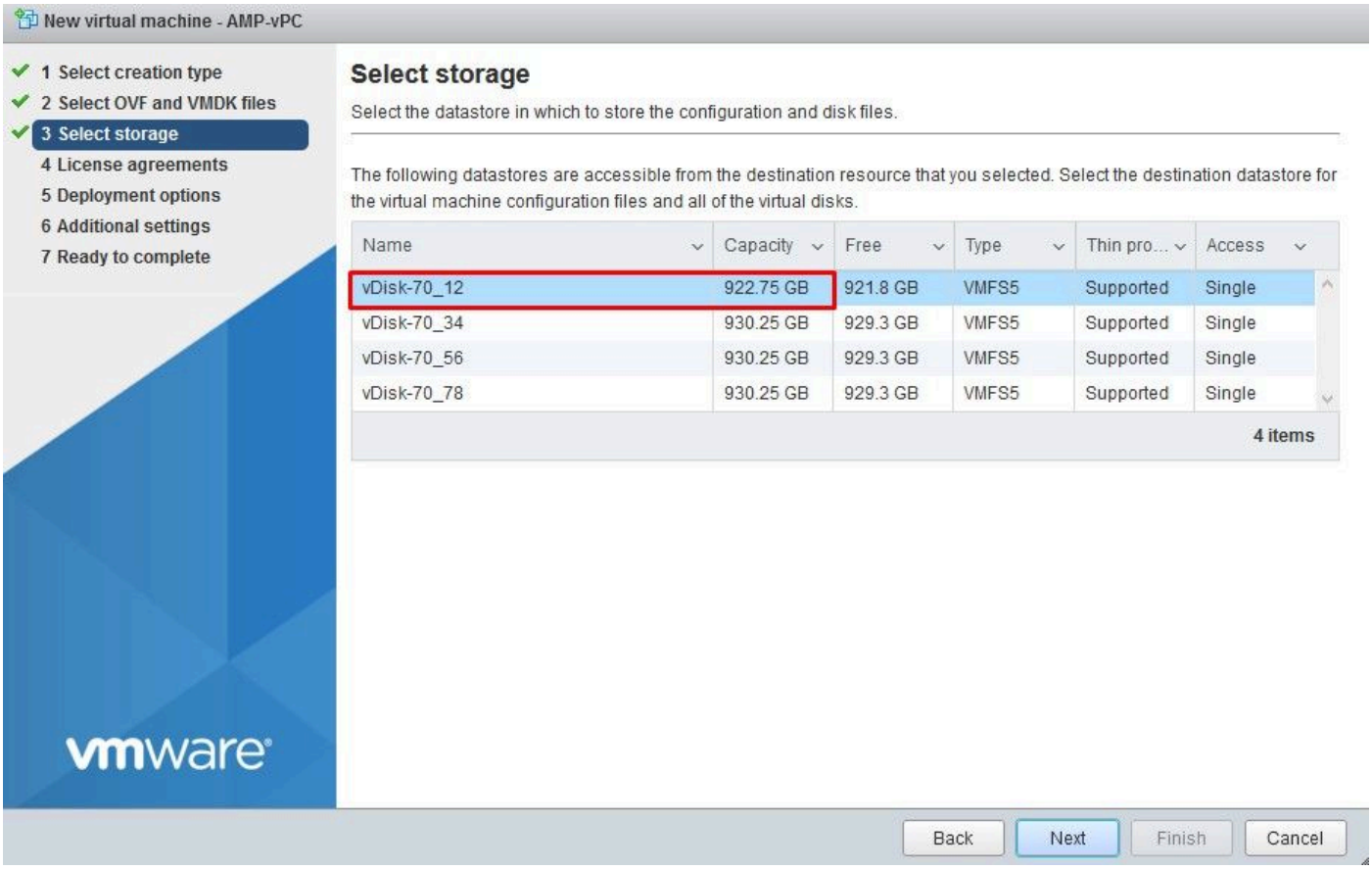
Installation de VM

Étape 1 :

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

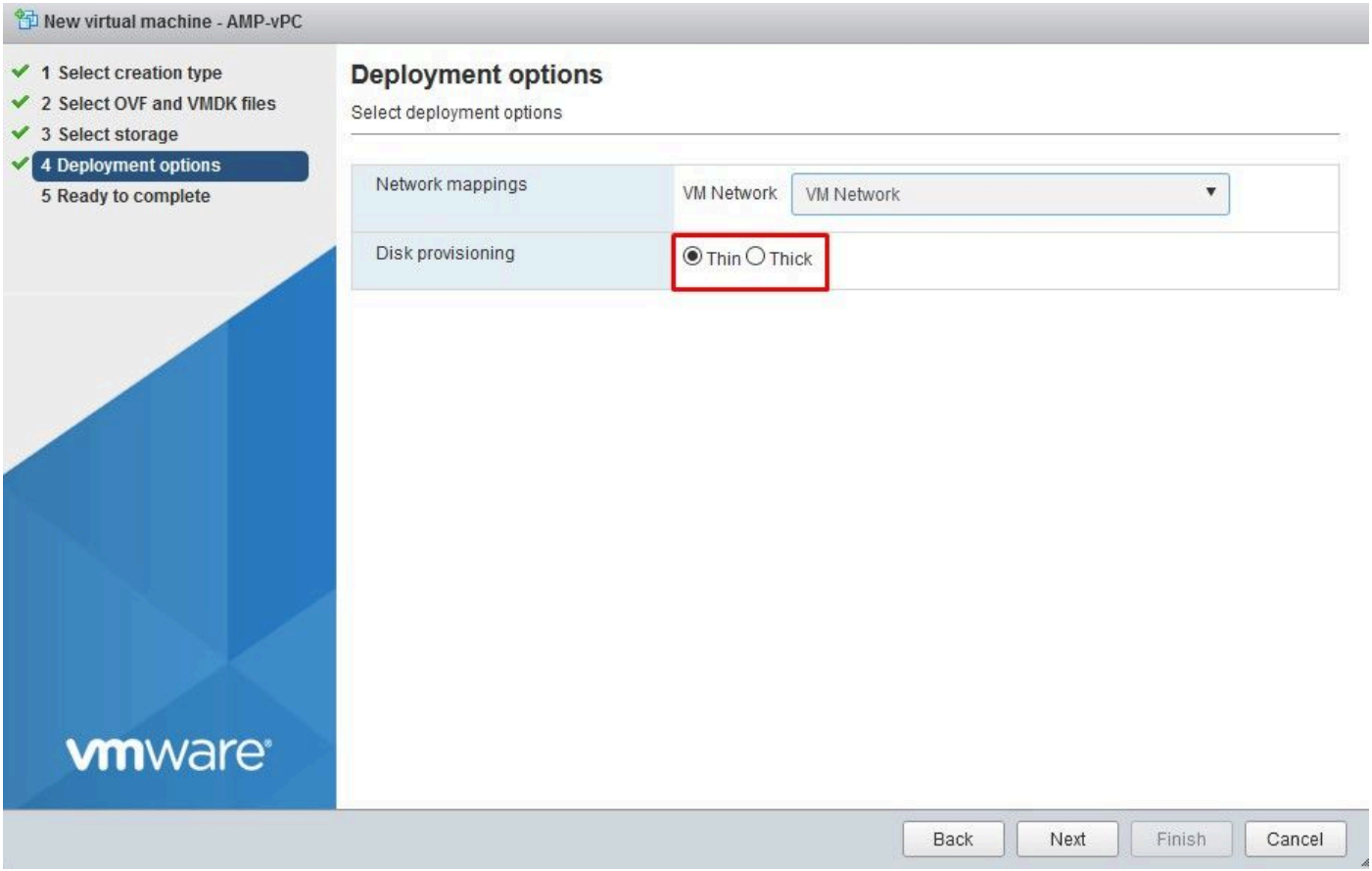






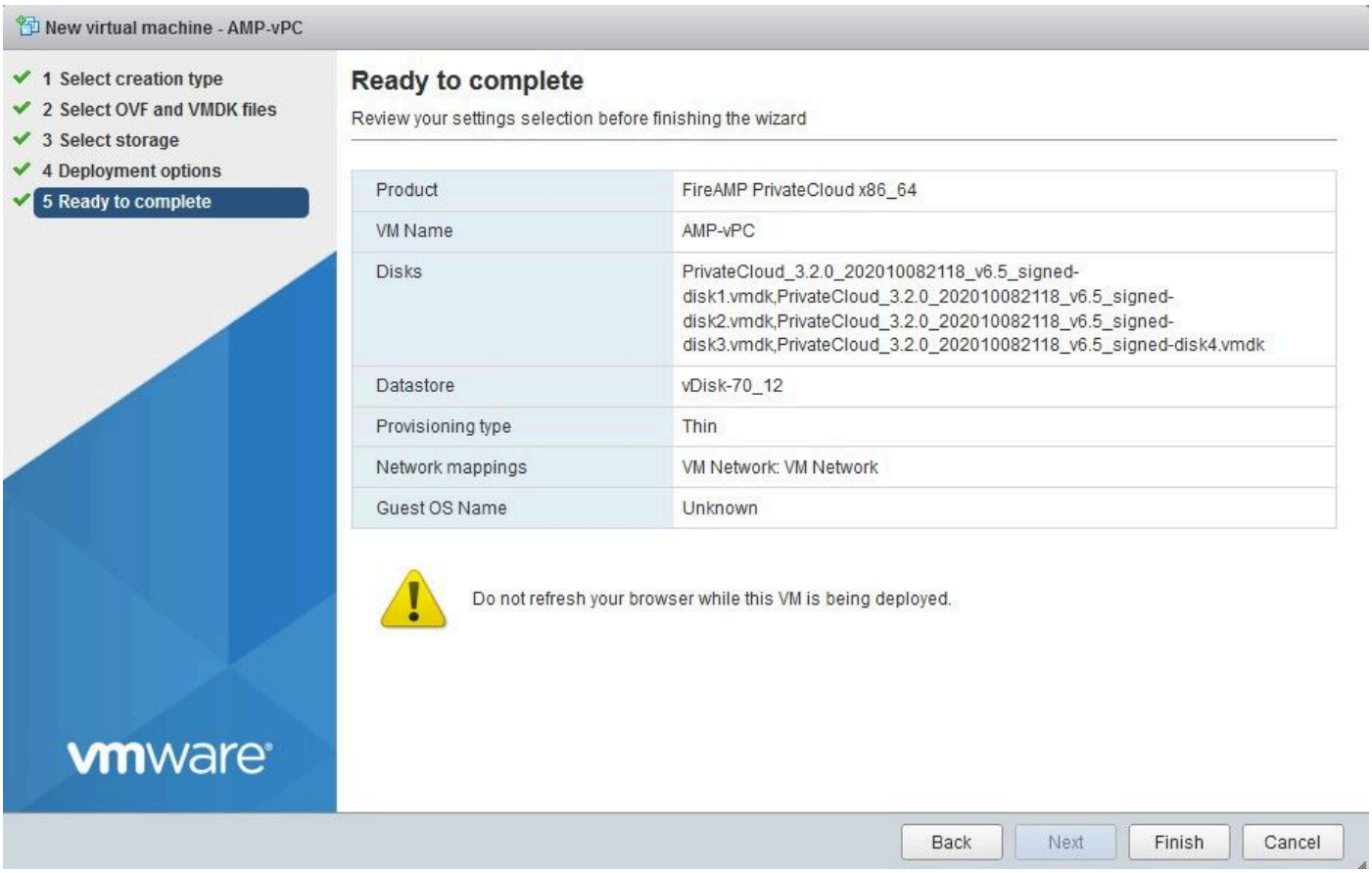
Remarque : Le provisionnement épais réserve de l'espace lors de la création d'un disque. Si vous sélectionnez cette option, elle peut améliorer les performances par rapport à Thin

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

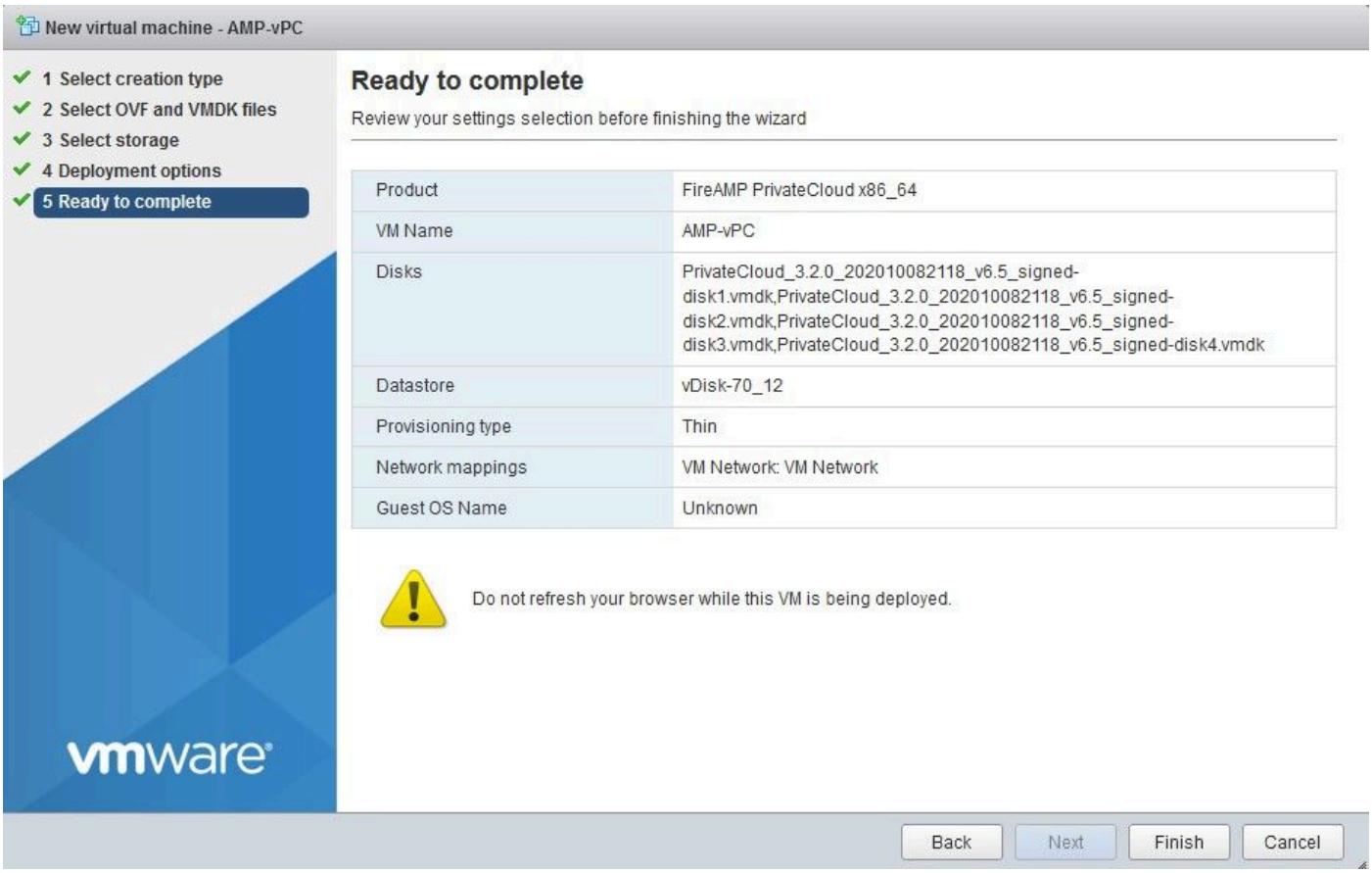


Étape 2 :

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 illustré dans l'image. sélectionnez Suivant.



Configuration initiale de l'interface Admin

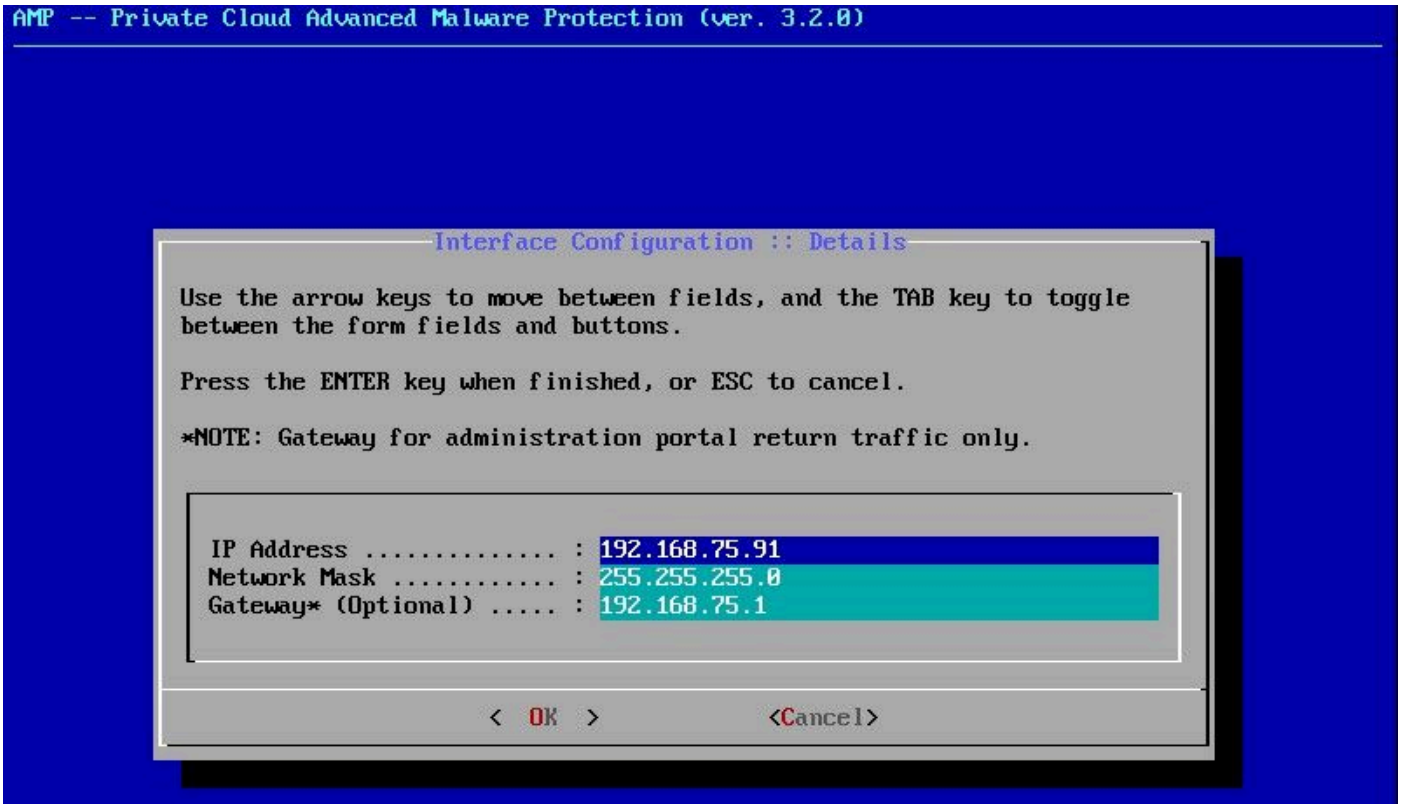


Une fois la machine virtuelle démarrée, vous effectuez la configuration initiale via la console de la

machine virtuelle.

Étape 1 :

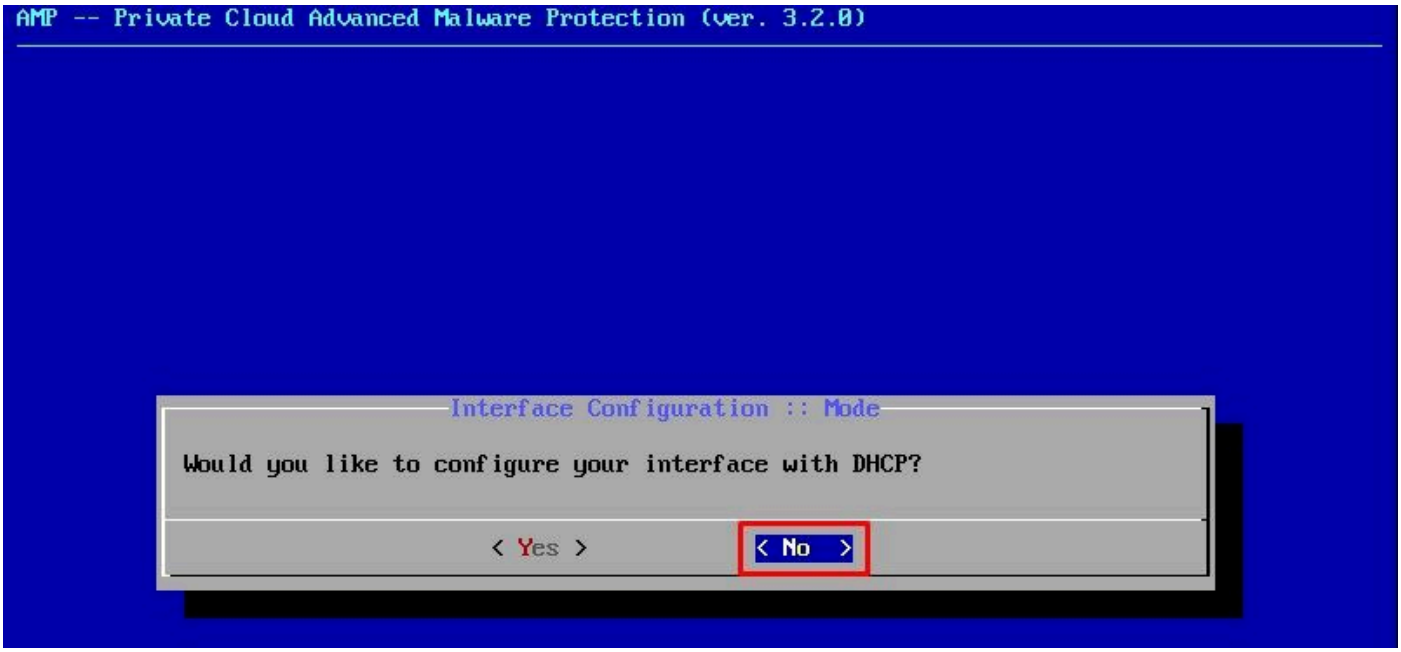
Vous remarquerez peut-être que l'URL indique [UNCONFIGURED] si l'interface n'a pas reçu d'adresse IP du serveur DHCP. Notez que cette interface est l'interface de gestion. Il ne s'agit pas de l'interface Production.

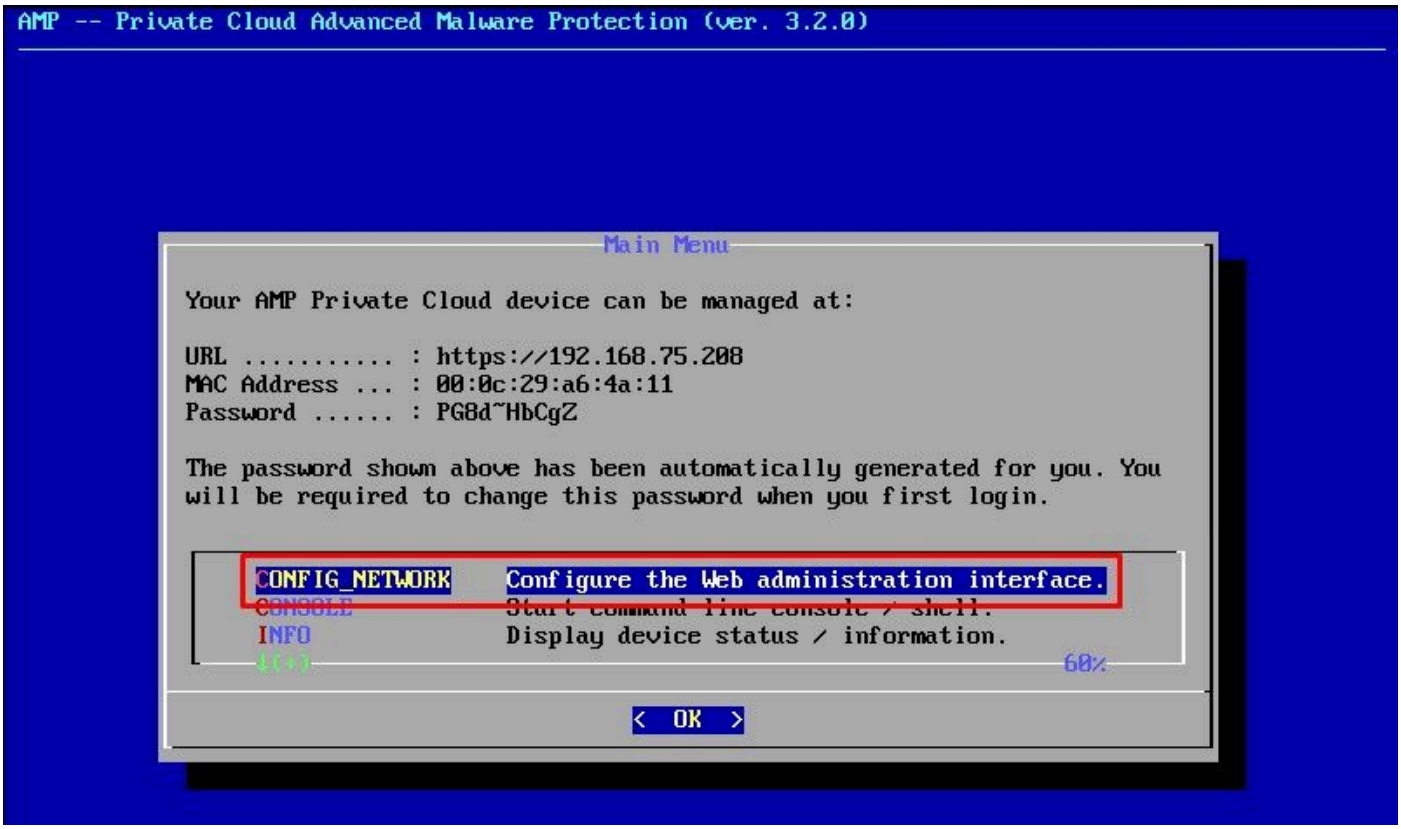


Étape 2 :

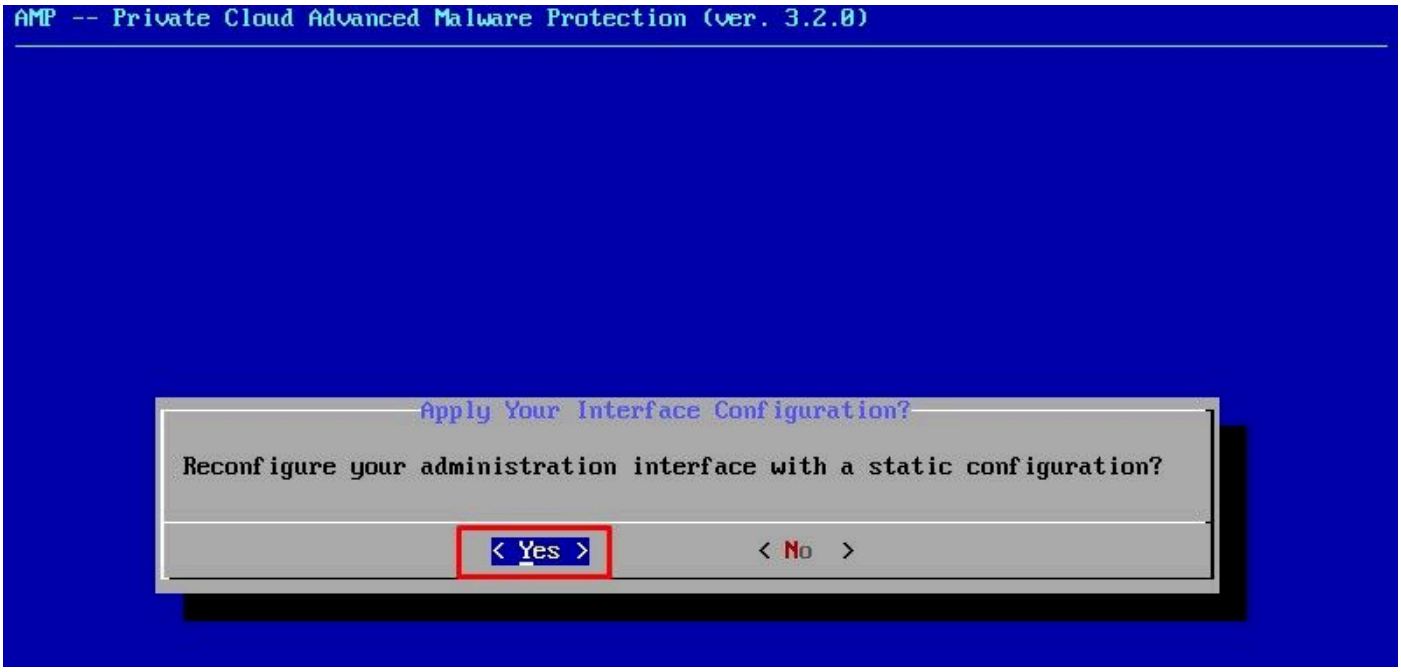
Vous pouvez naviguer entre les touches Tab, Entrée et Flèche.

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.

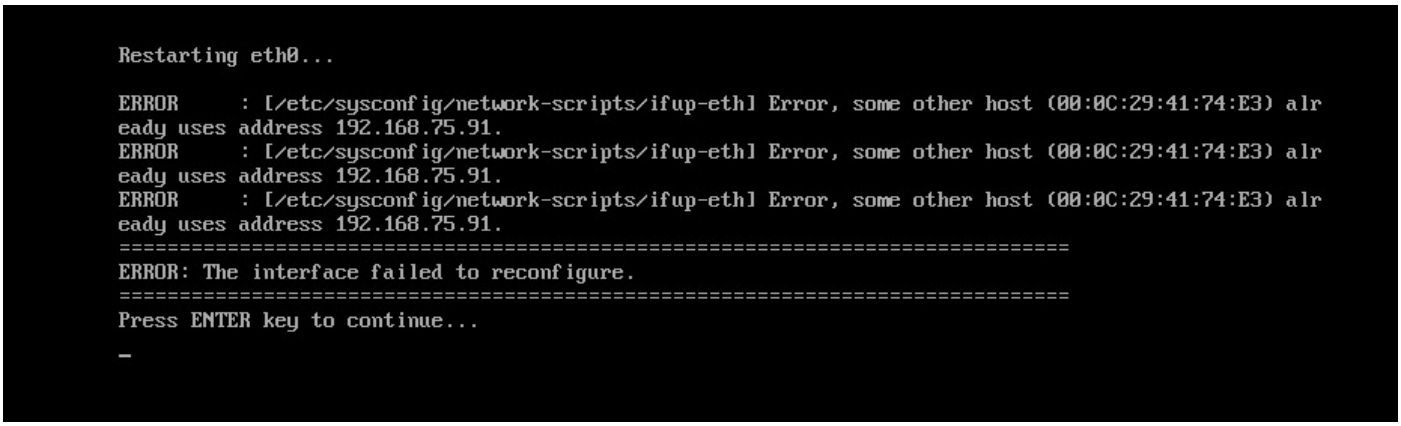


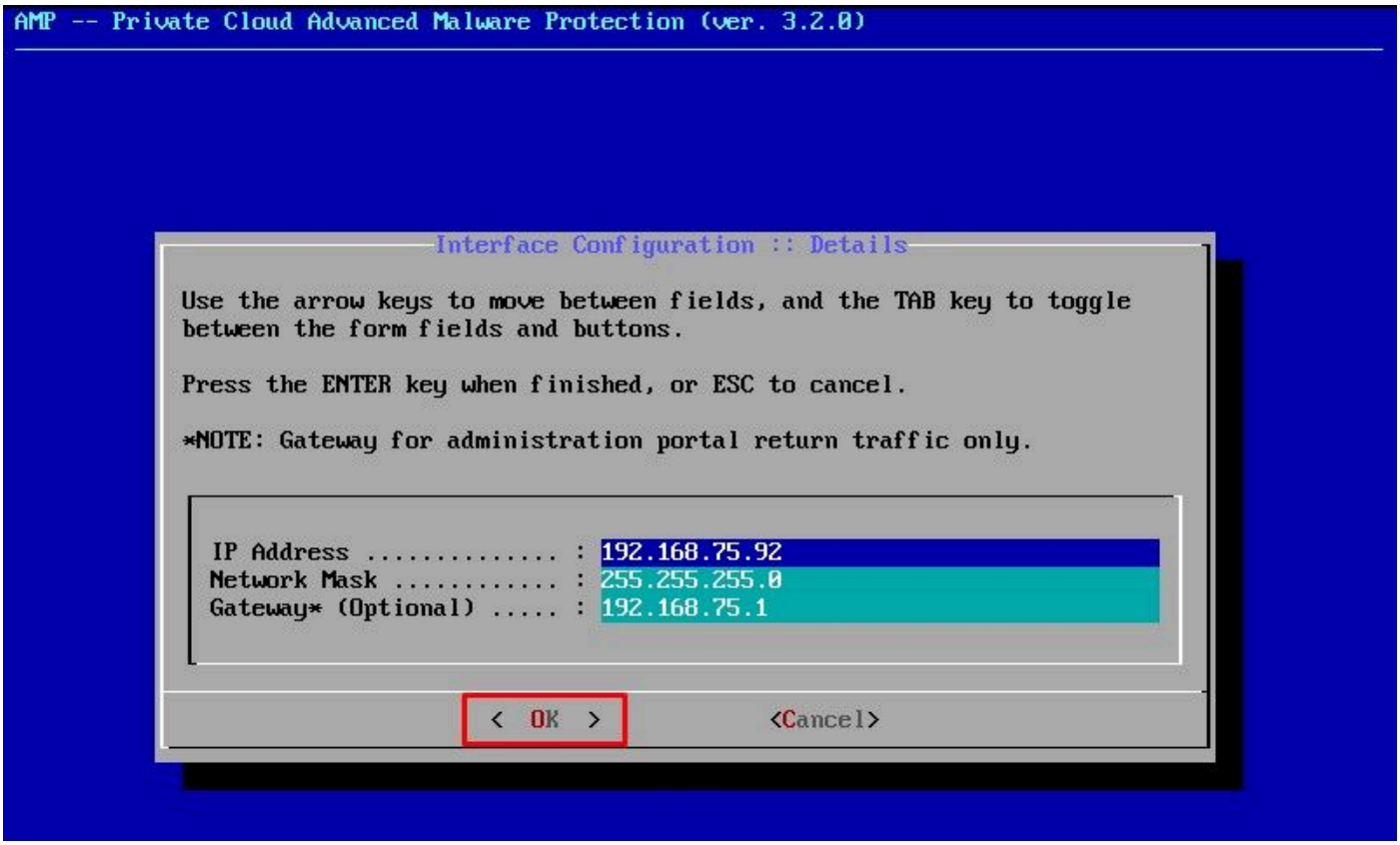


Dans la fenêtre qui s'affiche, choisissez Yes et sélectionnez Enter key.

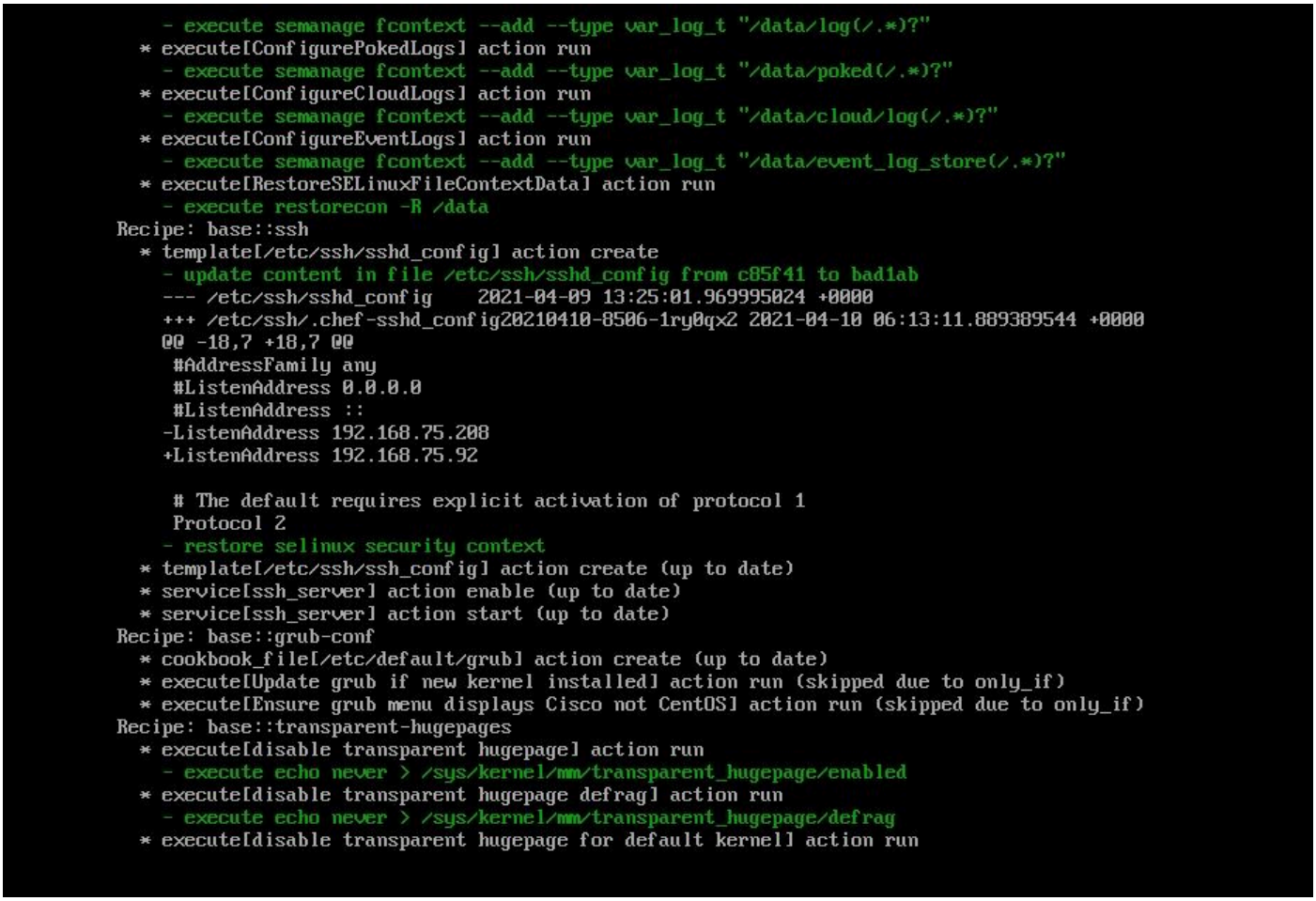


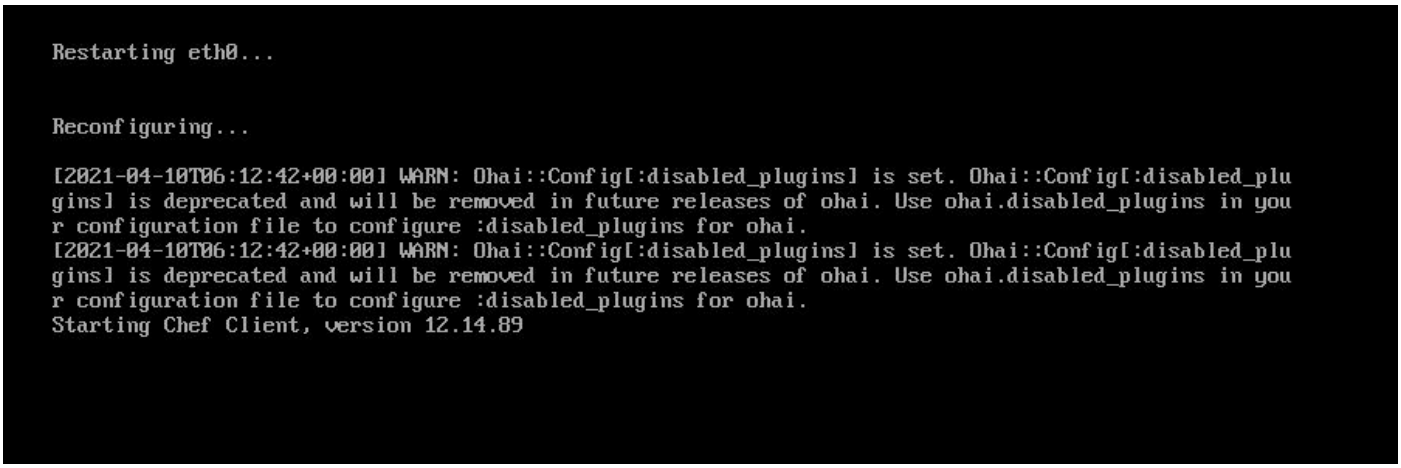
Si l'adresse IP est déjà utilisée, vous serez traité avec ce journal d'erreurs. Il suffit de revenir en arrière et de choisir quelque chose qui est unique et pas en cours d'utilisation.





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





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.

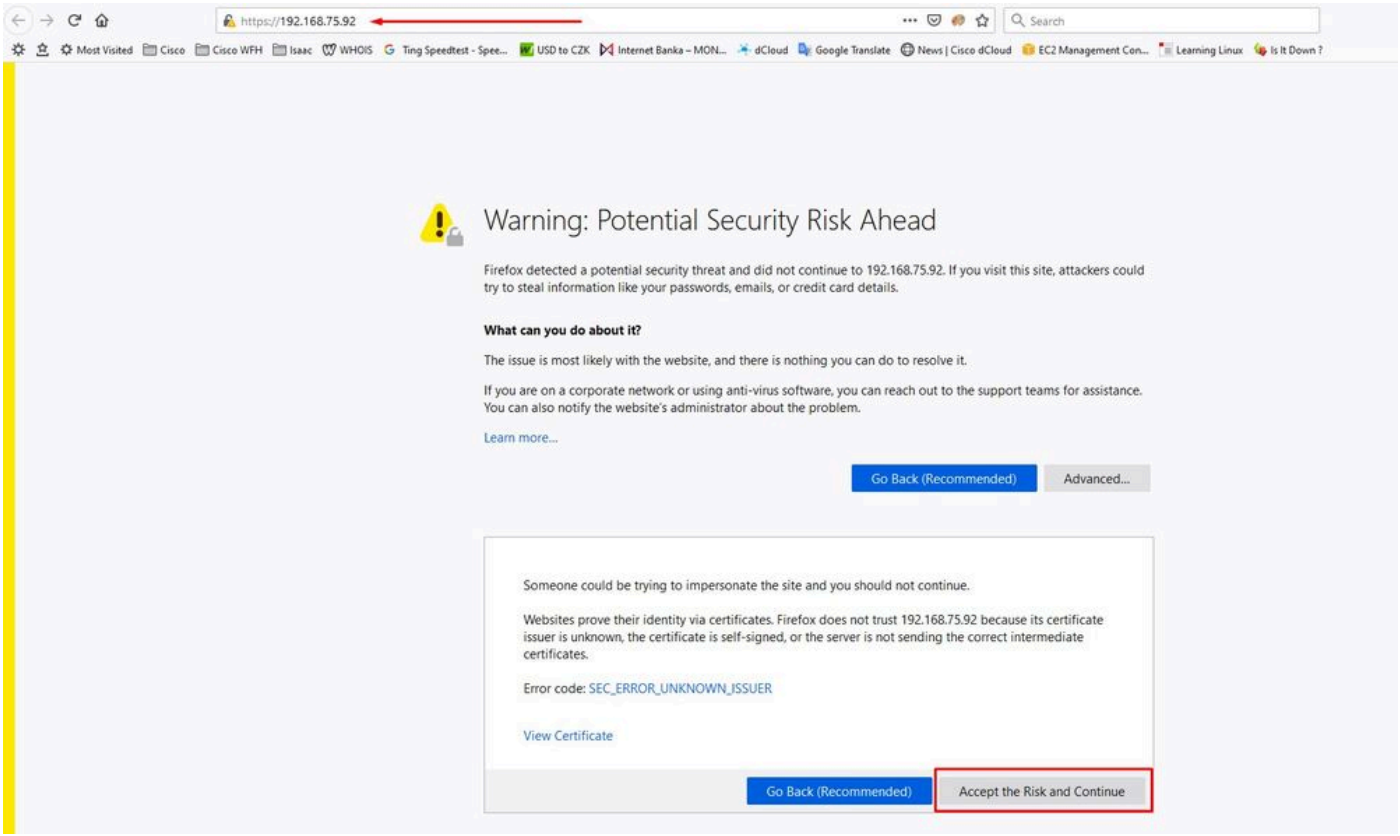


Configuration initiale du vPC via l'interface utilisateur graphique Web

Étape 1 :

Ouvrez un navigateur Web et accédez à l'adresse IP de gestion de l'appliance. 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.



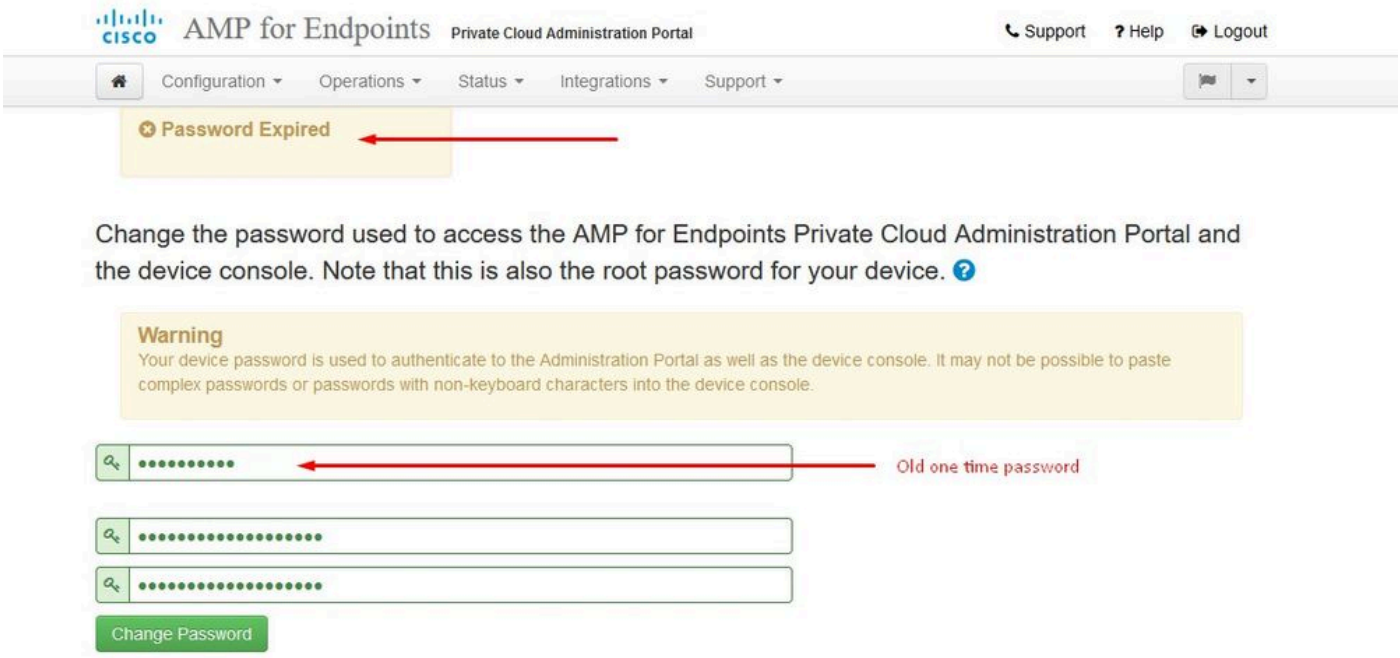
Étape 2 :

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.



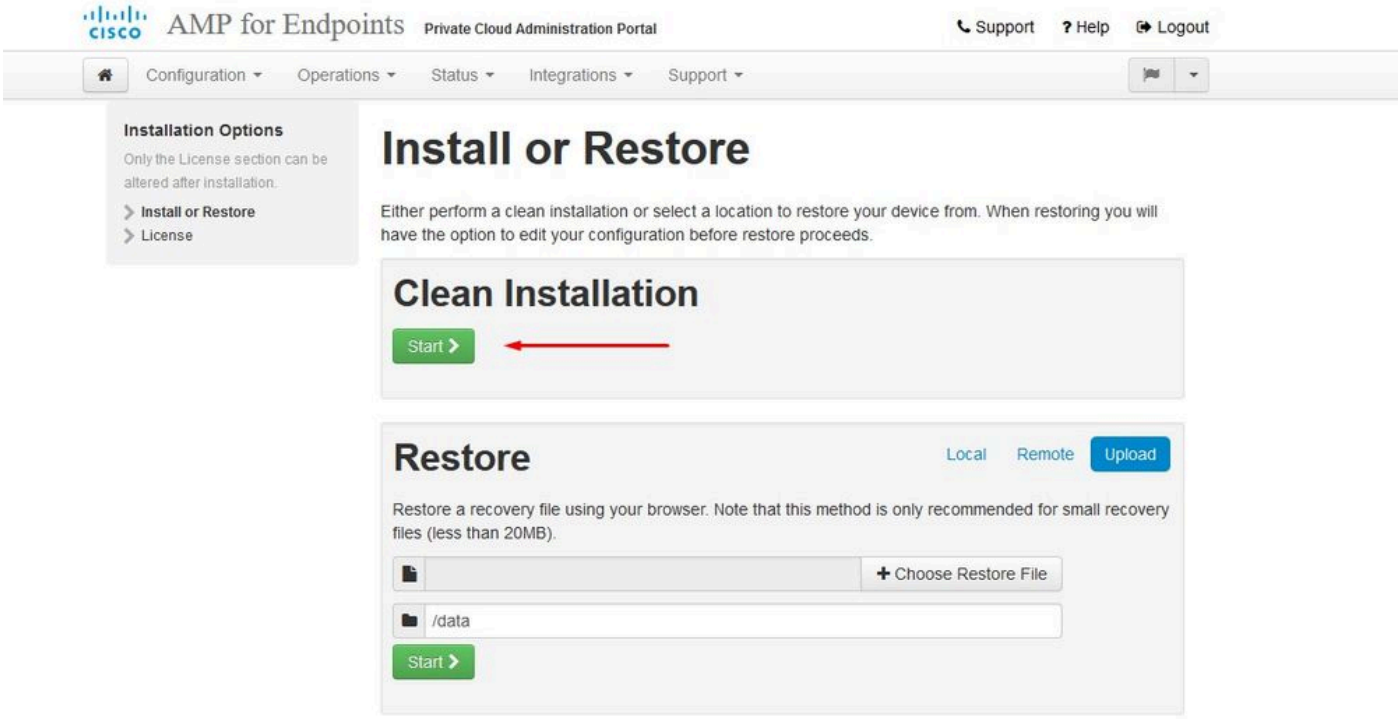
Étape 4 :

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



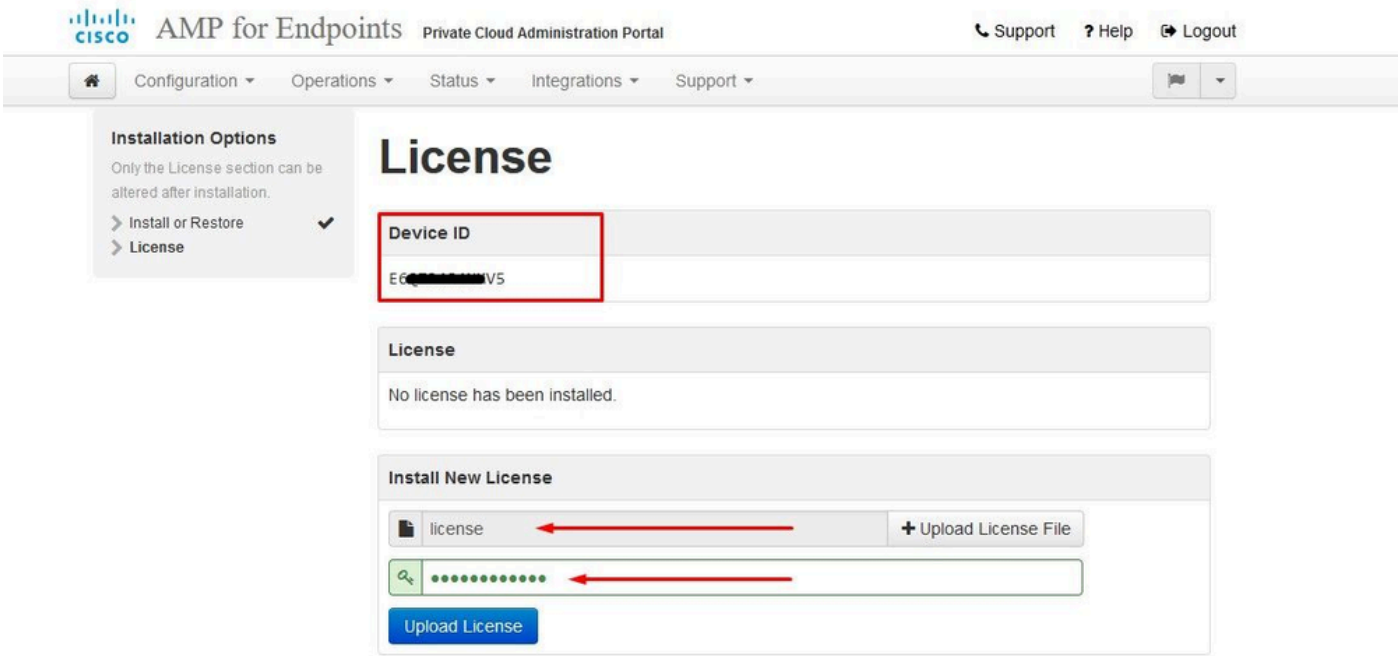
Étape 5 :

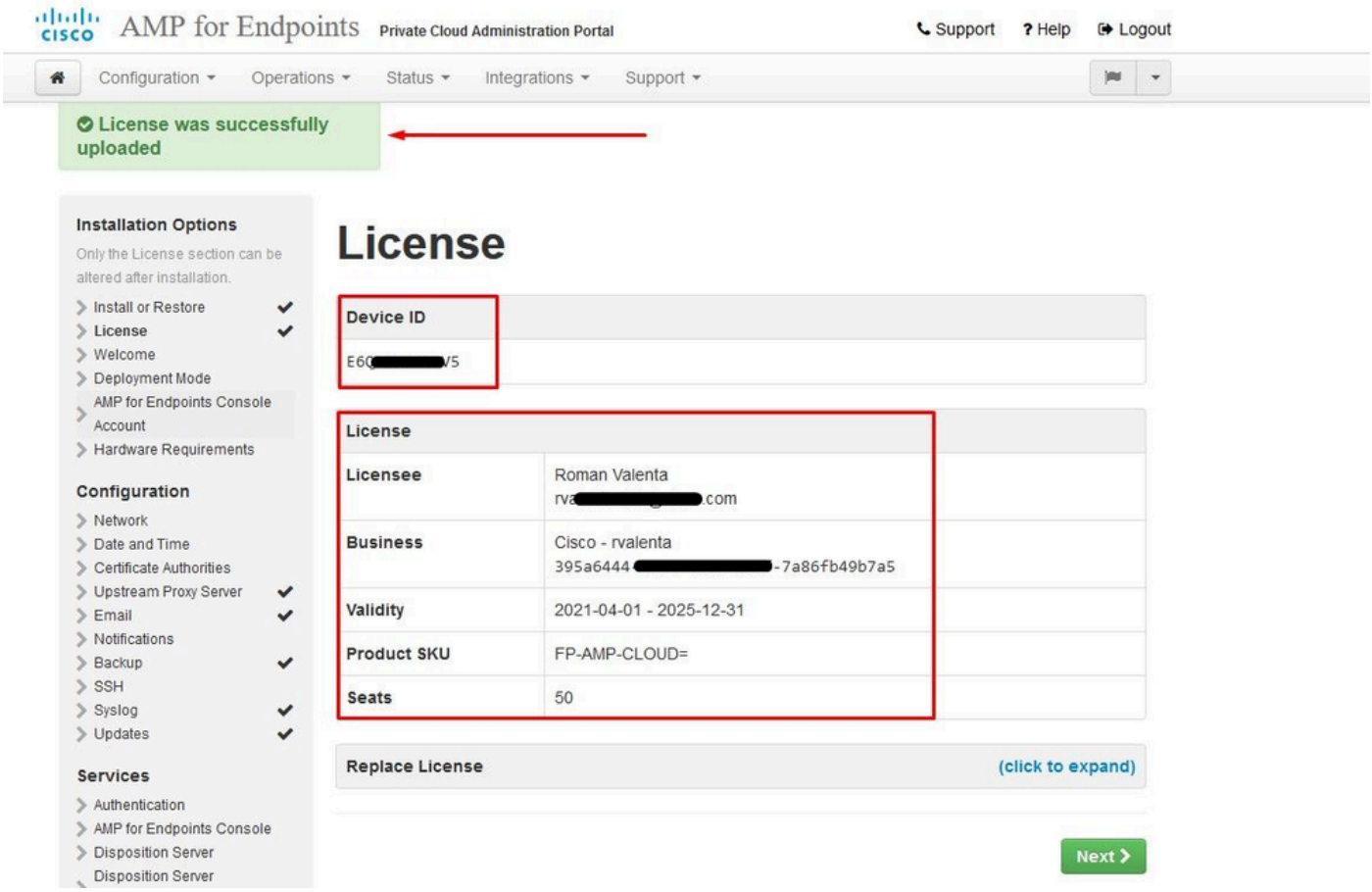
Après avoir accepté le contrat, vous obtenez l'écran d'installation, comme illustré dans l'image. Si vous voulez restaurer à partir d'une sauvegarde, vous pouvez le faire ici, cependant, ce guide continue avec l'option Clean Installation. Sélectionnez sur Démarrer dans la section Nettoyer l'installation.



Étape 6 :

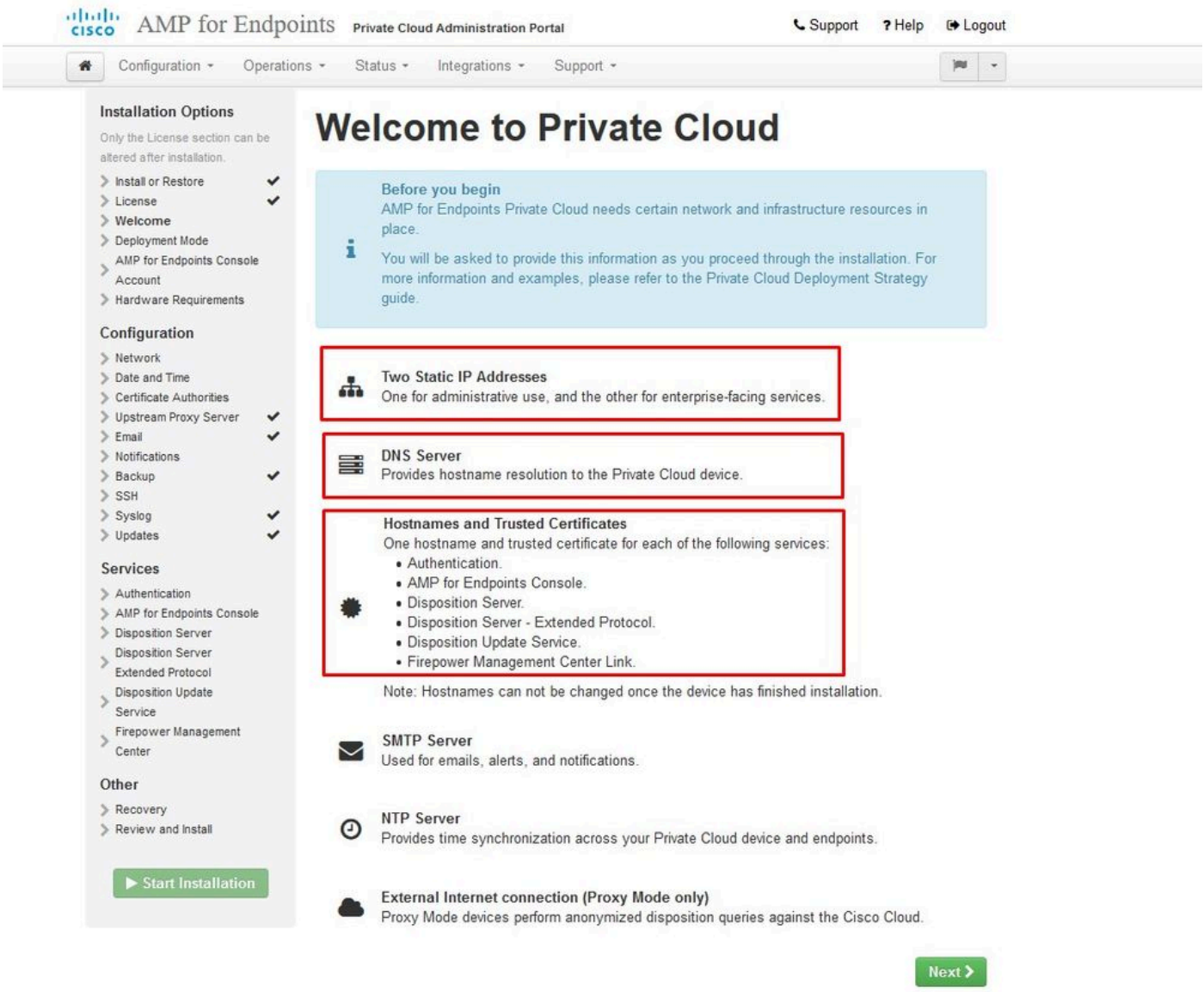
La première chose dont vous avez besoin est une licence pour aller de l'avant. Vous recevez une licence et une phrase de passe lorsque vous achetez le produit. Sélectionnez on +Upload License File. Sélectionnez le fichier de licence et saisissez la phrase de passe. Sélectionnez sur Upload License. Si 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.





Étape 7 :

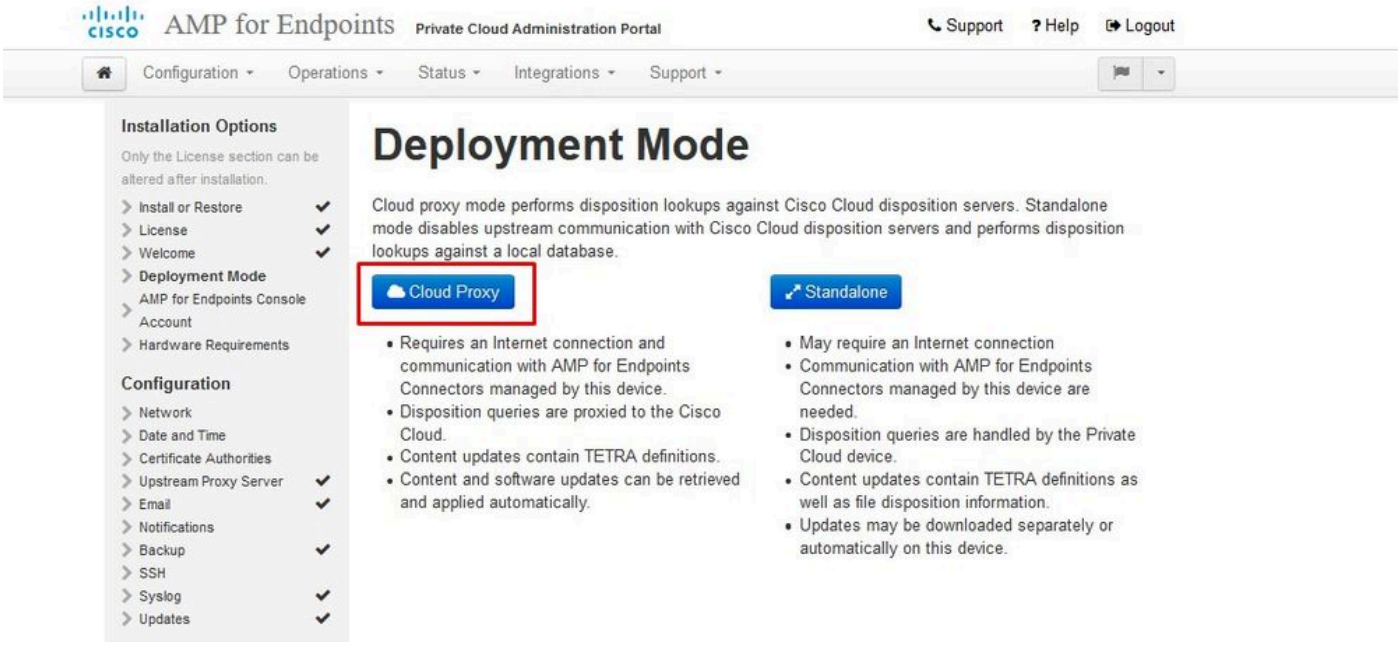
Vous recevez la page d'accueil, comme illustré dans l'image. Cette page affiche les informations dont vous avez besoin avant de configurer le cloud privé. Lisez attentivement les exigences. Sélectionnez sur Next pour démarrer la configuration de pré-installation.



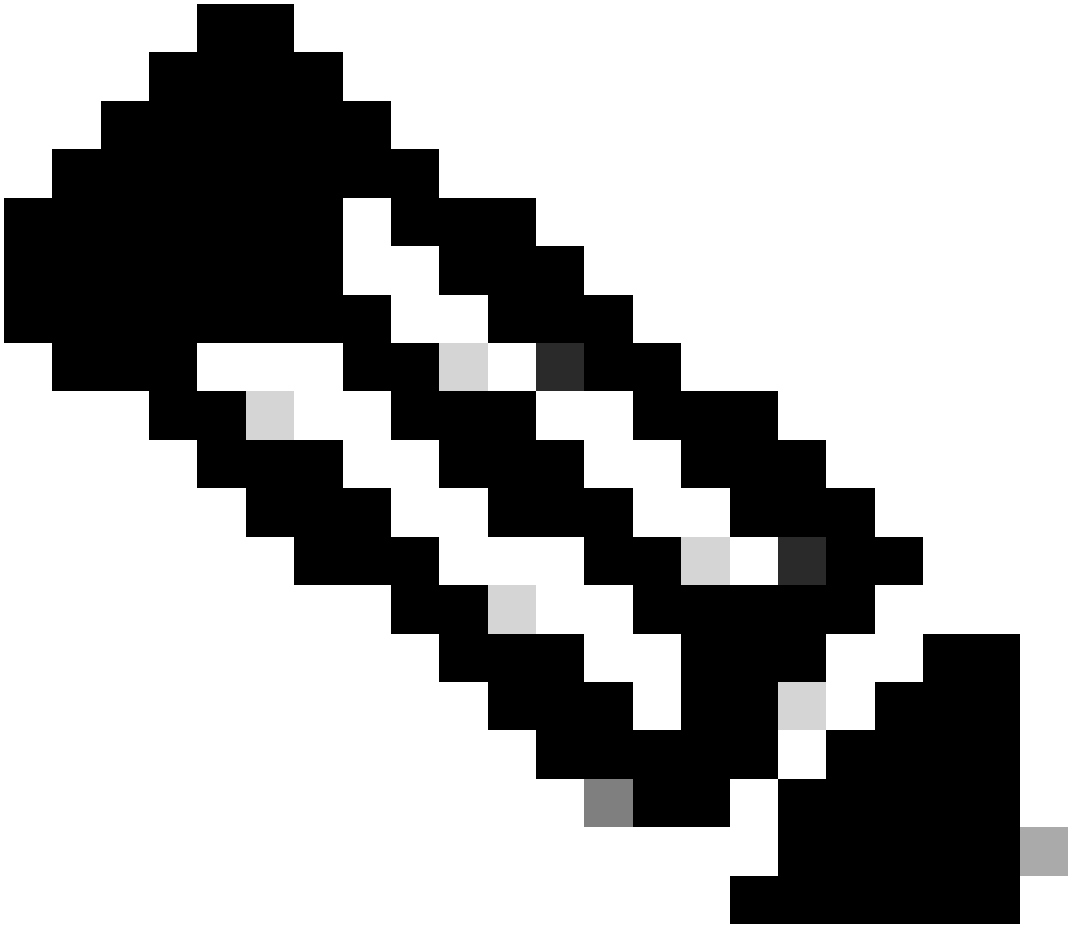
Configuration

Étape 1 :

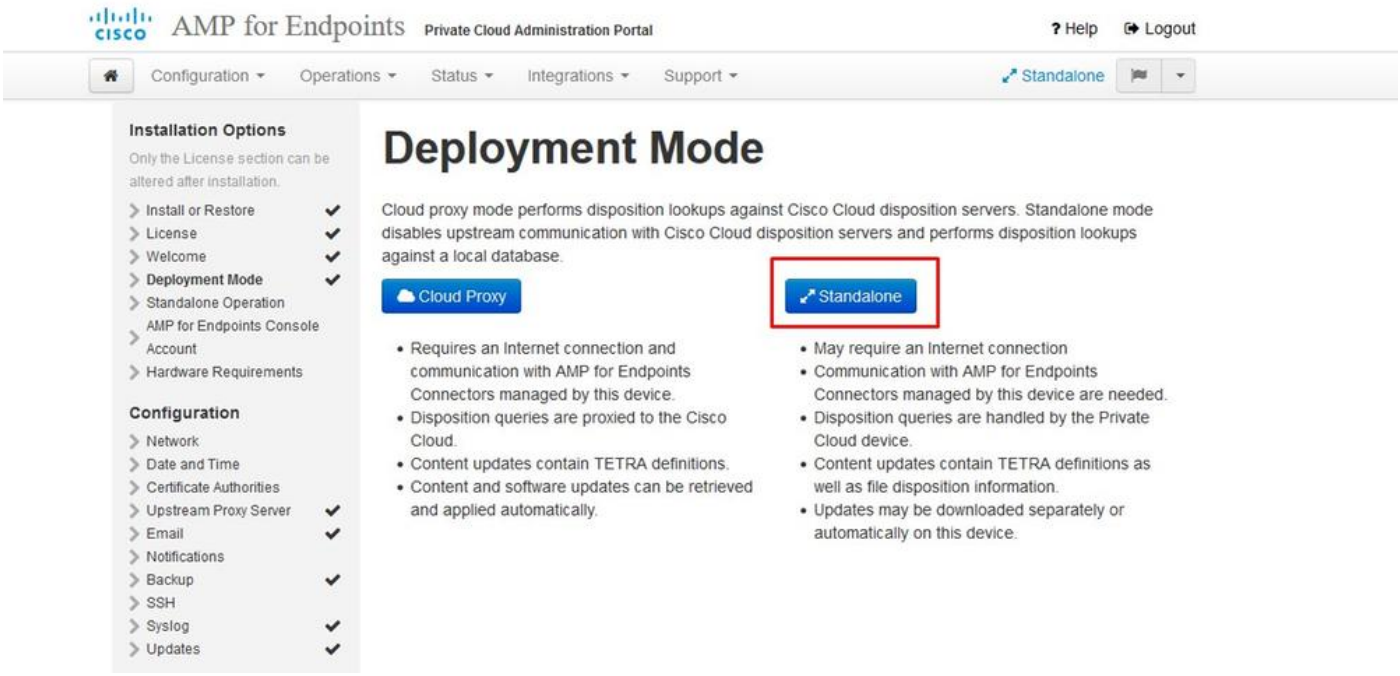
Remarque : Veuillez noter que dans les prochaines séries de diapositives, nous incluons certaines exclusivités, telles qu'illustrées dans l'image, qui sont uniques uniquement au mode AIR GAP , celles-ci doivent être jointes et marquées comme AIRGAP ONLY

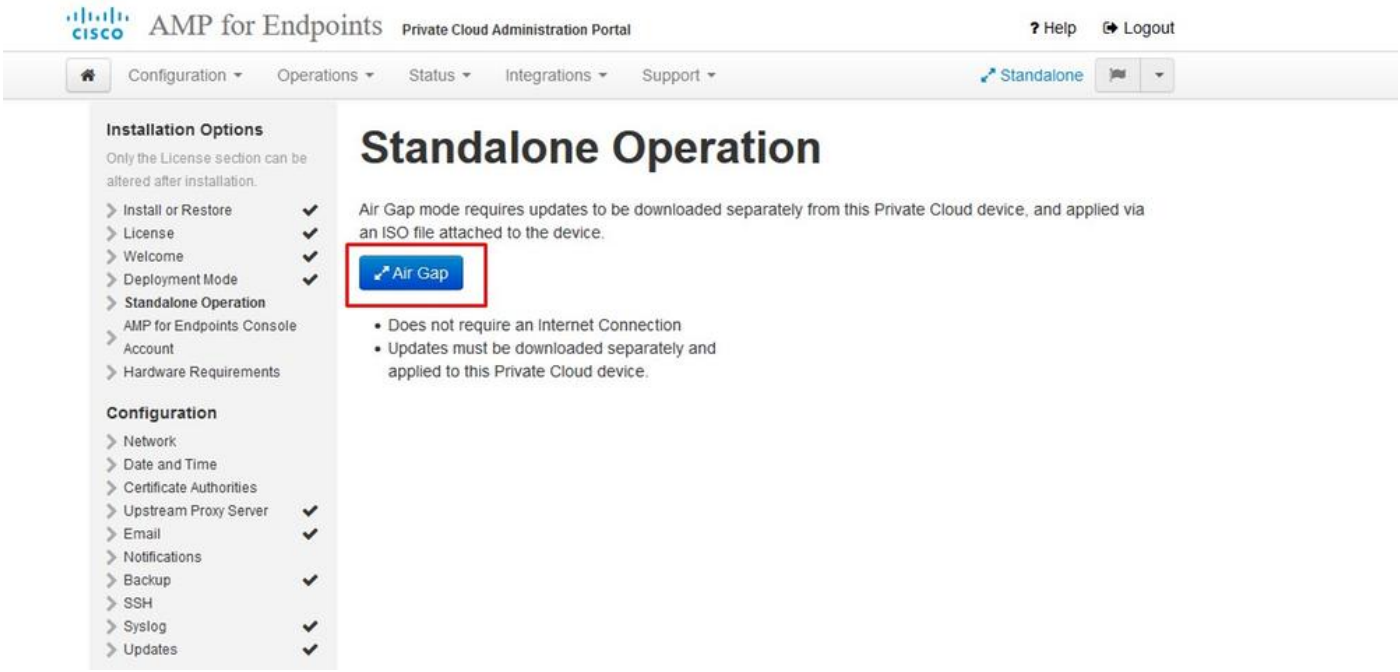


⩔⩔ ENTREFER UNIQUEMENT ⩔⩔



Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.



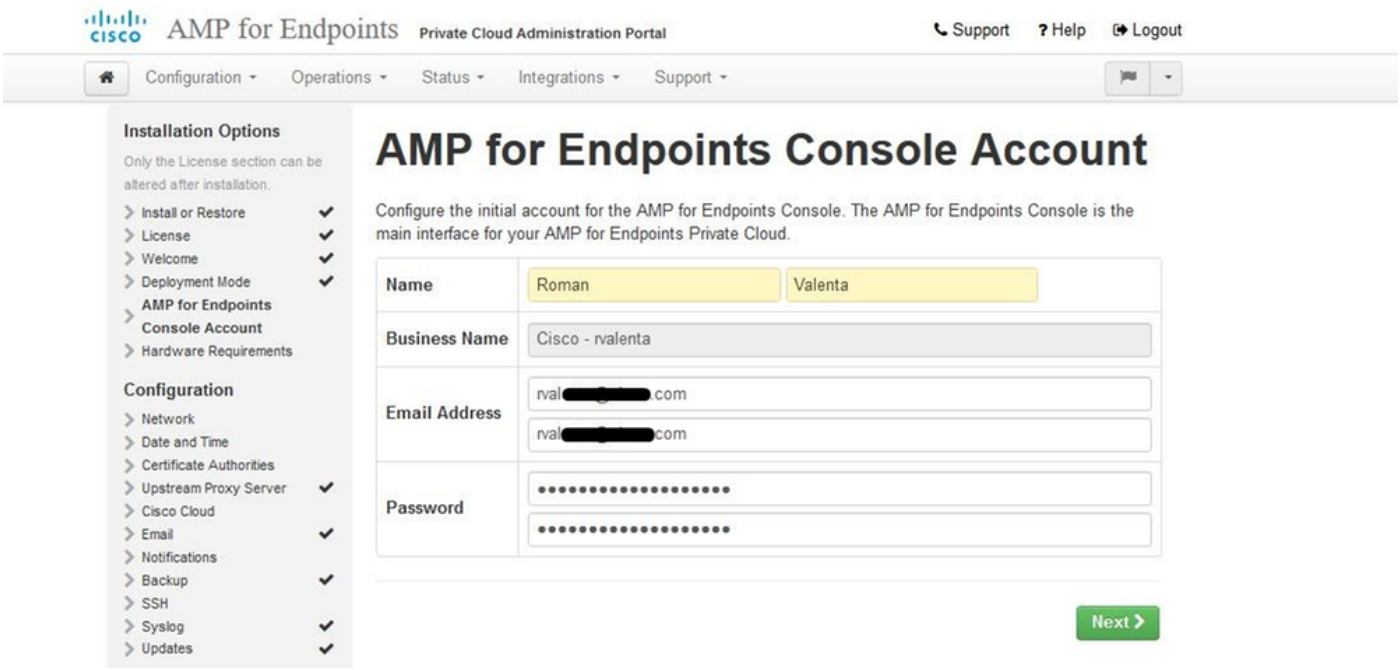


⩓ ⩓ AIRGAP UNIQUEMENT ⩓ ⩓

Étape 2 :

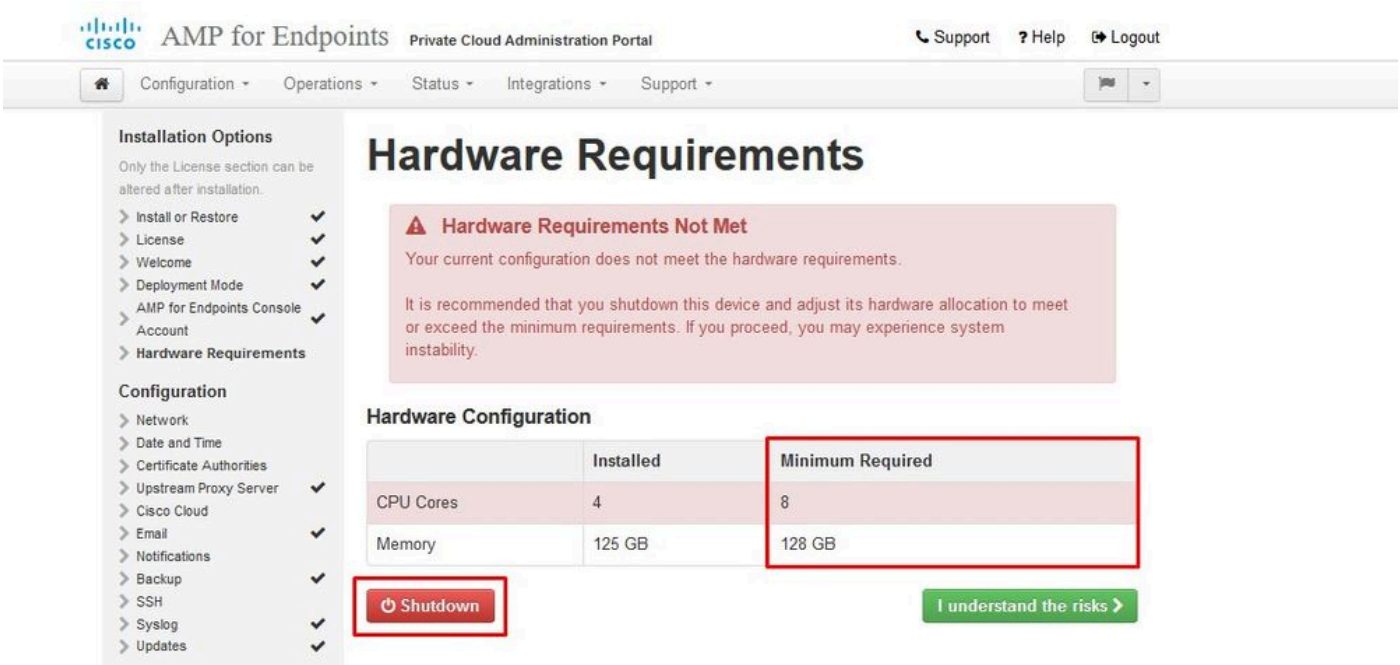
Accédez à la page Secure Endpoint Console Account. Un utilisateur administrateur est utilisé pour la console afin de créer des stratégies, des groupes d'ordinateurs et d'ajouter des utilisateurs supplémentaires. Saisissez le nom, l'adresse e-mail et le mot de passe du compte de console.

Sélectionnez sur Suivant.

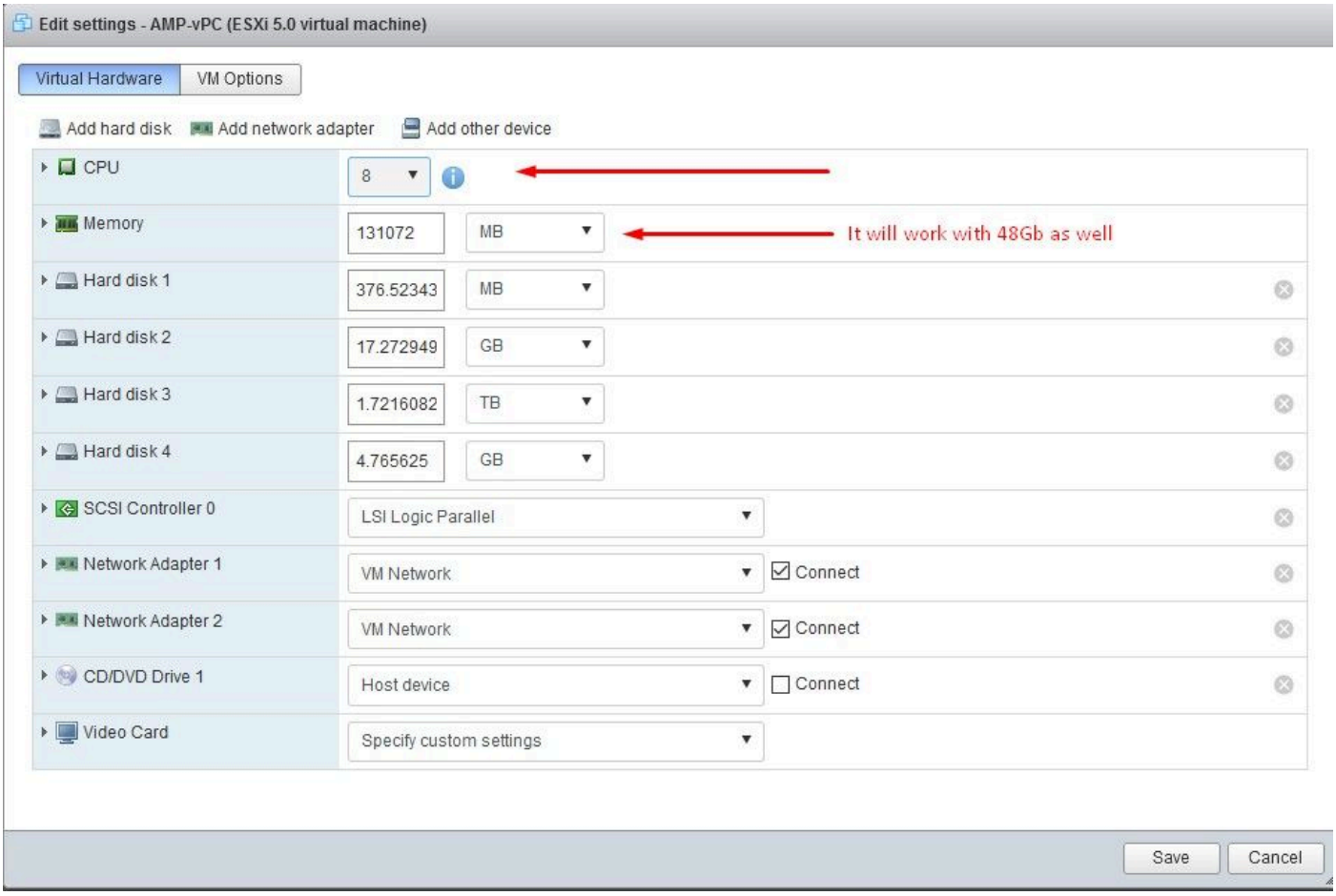


Si vous vous connectez à ce problème lorsque vous effectuez le déploiement à partir du fichier OVA, vous avez deux choix : soit continuer et résoudre ce problème ultérieurement, soit arrêter, afin d'installer votre machine virtuelle déployée et de l'ajuster en conséquence. Après le redémarrage, vous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

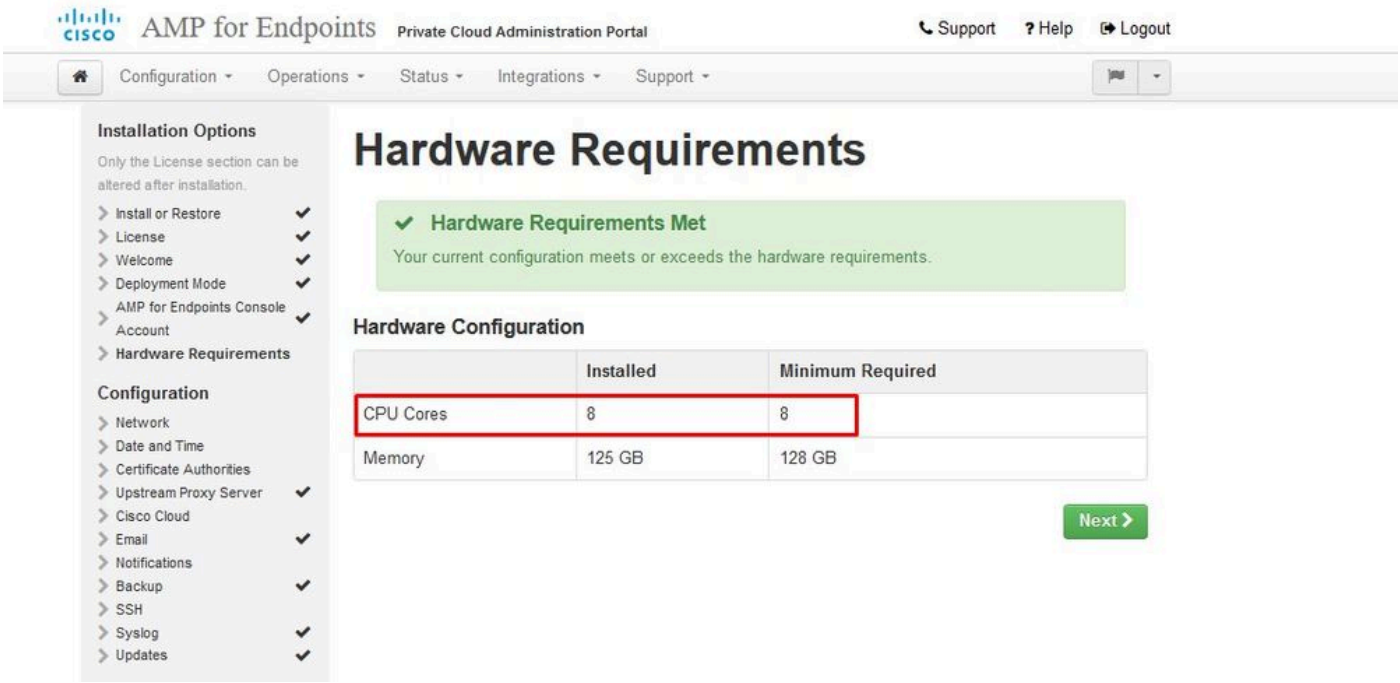
Remarque : Ceci a été corrigé dans le fichier OVA pour la version 3.5.2 qui se charge correctement avec 128 Go de RAM et 8 coeurs de CPU



Remarque : Utilisez uniquement les valeurs recommandées, sauf si elles sont destinées aux travaux pratiques



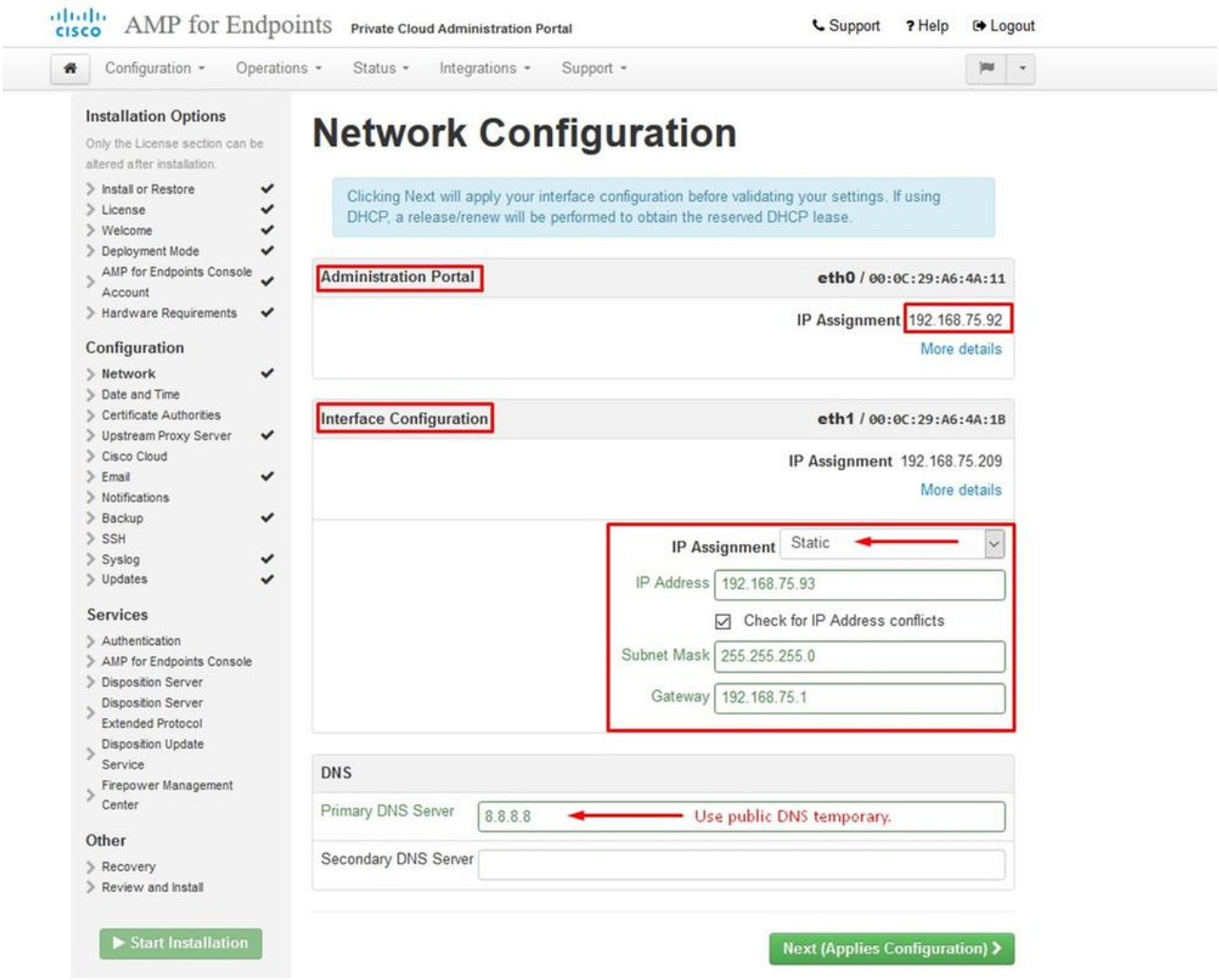
Une fois redémarré, nous continuons là où nous sommes partis.



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

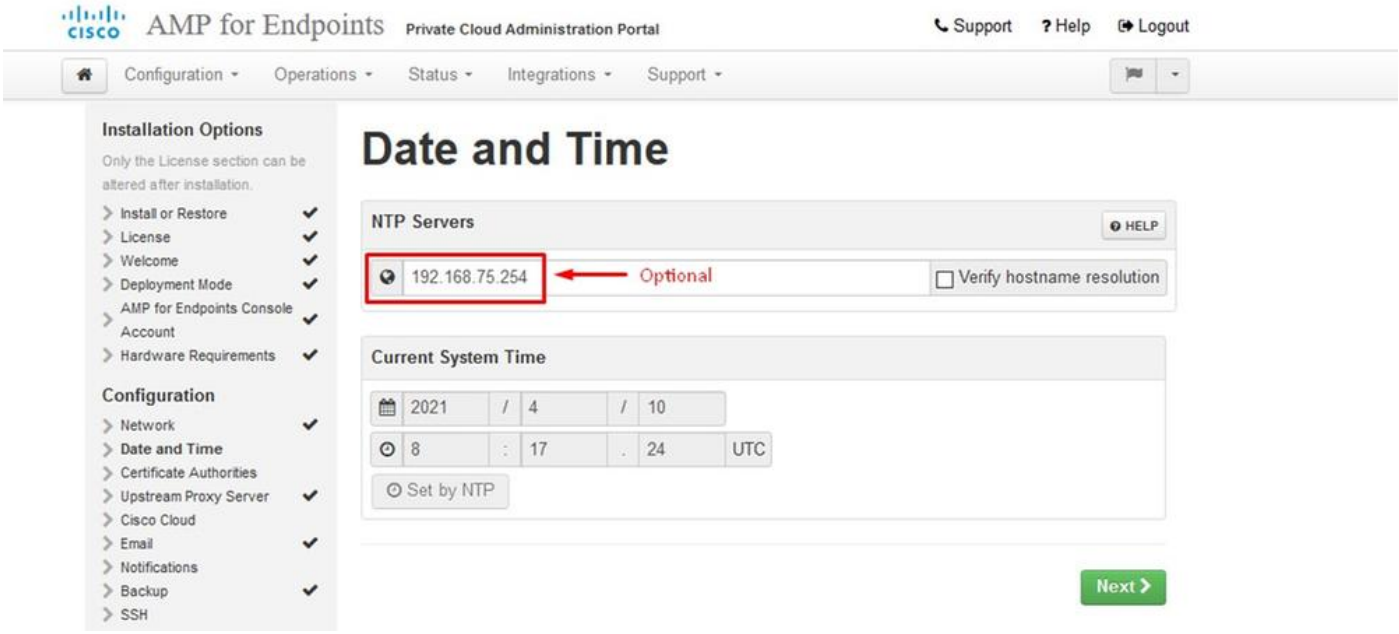
Remarque : Vous ne devez jamais configurer votre périphérique pour qu'il utilise DHCP, sauf si vous avez créé des réservations d'adresses MAC pour les interfaces. Si les adresses IP de vos interfaces changent, cela peut entraîner de graves problèmes avec les connecteurs Secure Endpoint Connectors déployés.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

Étape 3 :

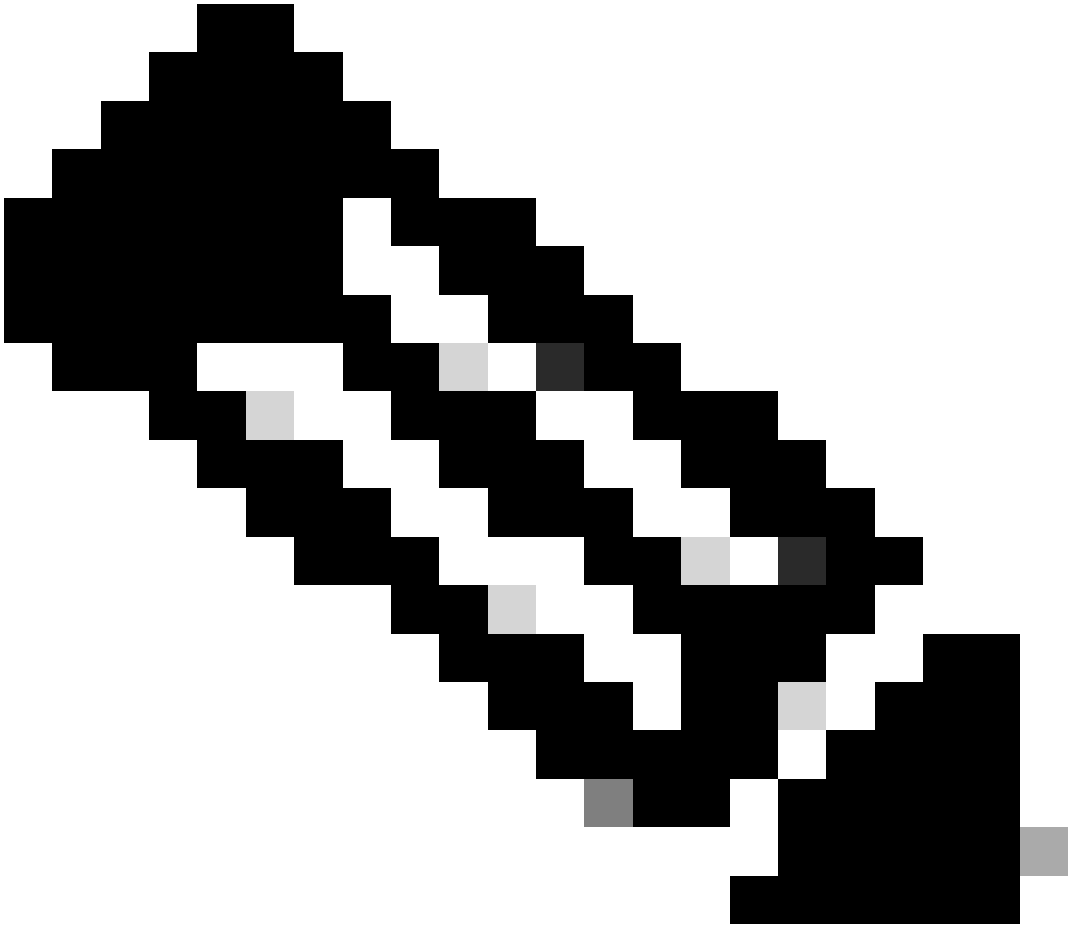


Étape 4 :

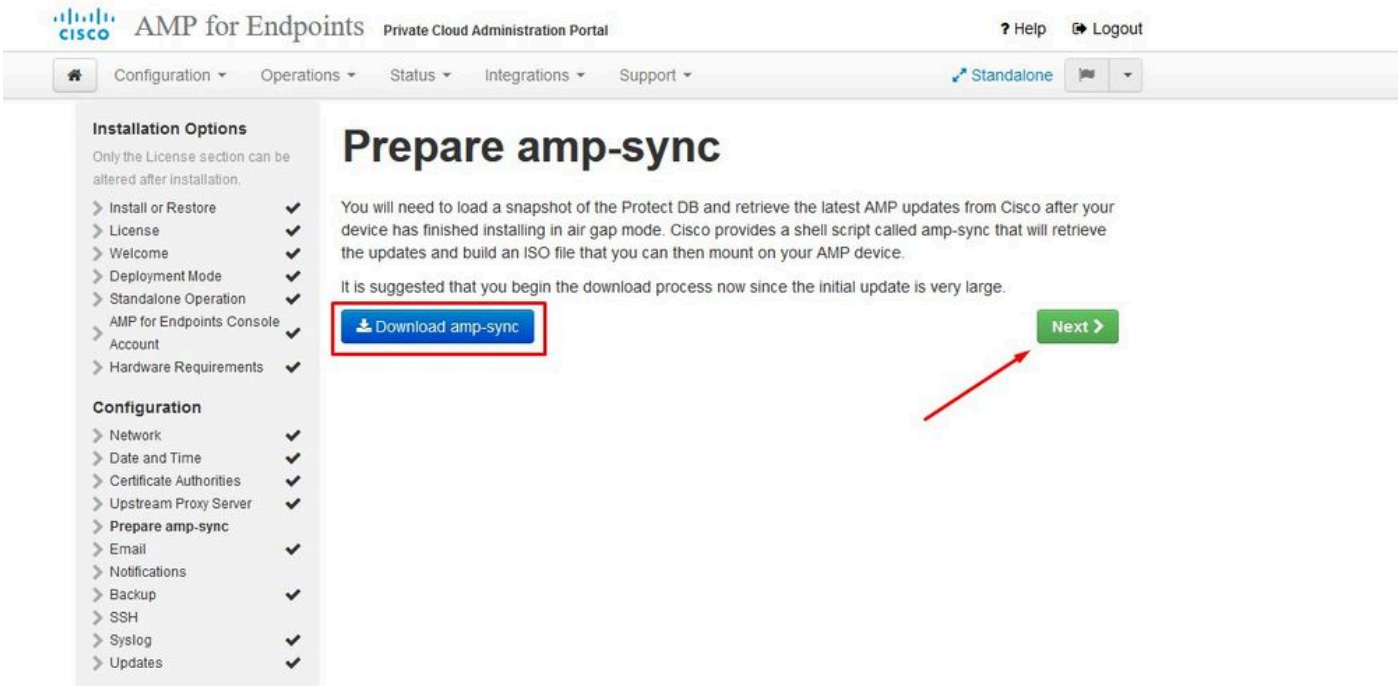
Vous obtenez la page Date et heure. Saisissez les adresses d'un ou plusieurs serveurs NTP que vous souhaitez utiliser pour la synchronisation de date et d'heure. Vous pouvez utiliser des serveurs NTP internes ou externes et en spécifier plusieurs via une liste délimitée par des virgules ou des espaces. 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.



⩔⩔ ENTREFER UNIQUEMENT ⩔⩔



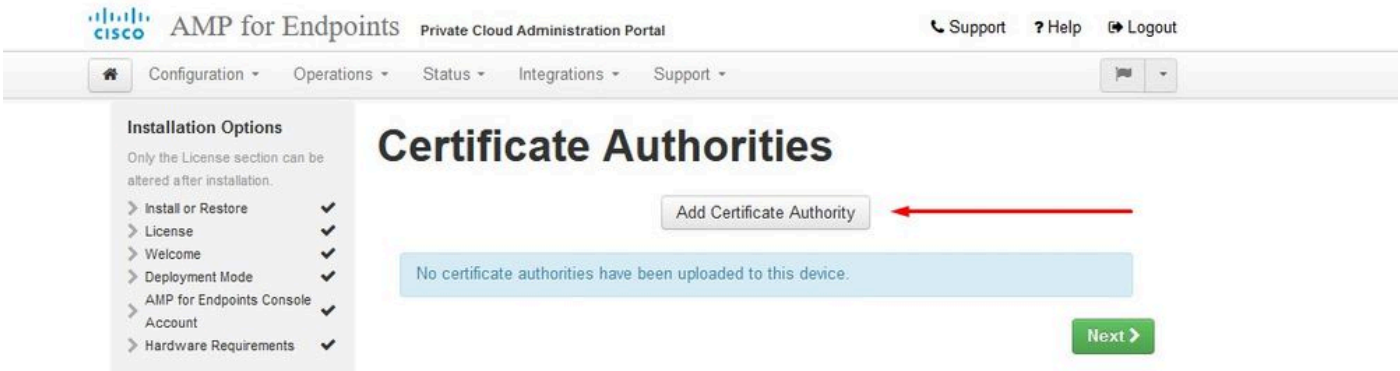
Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.

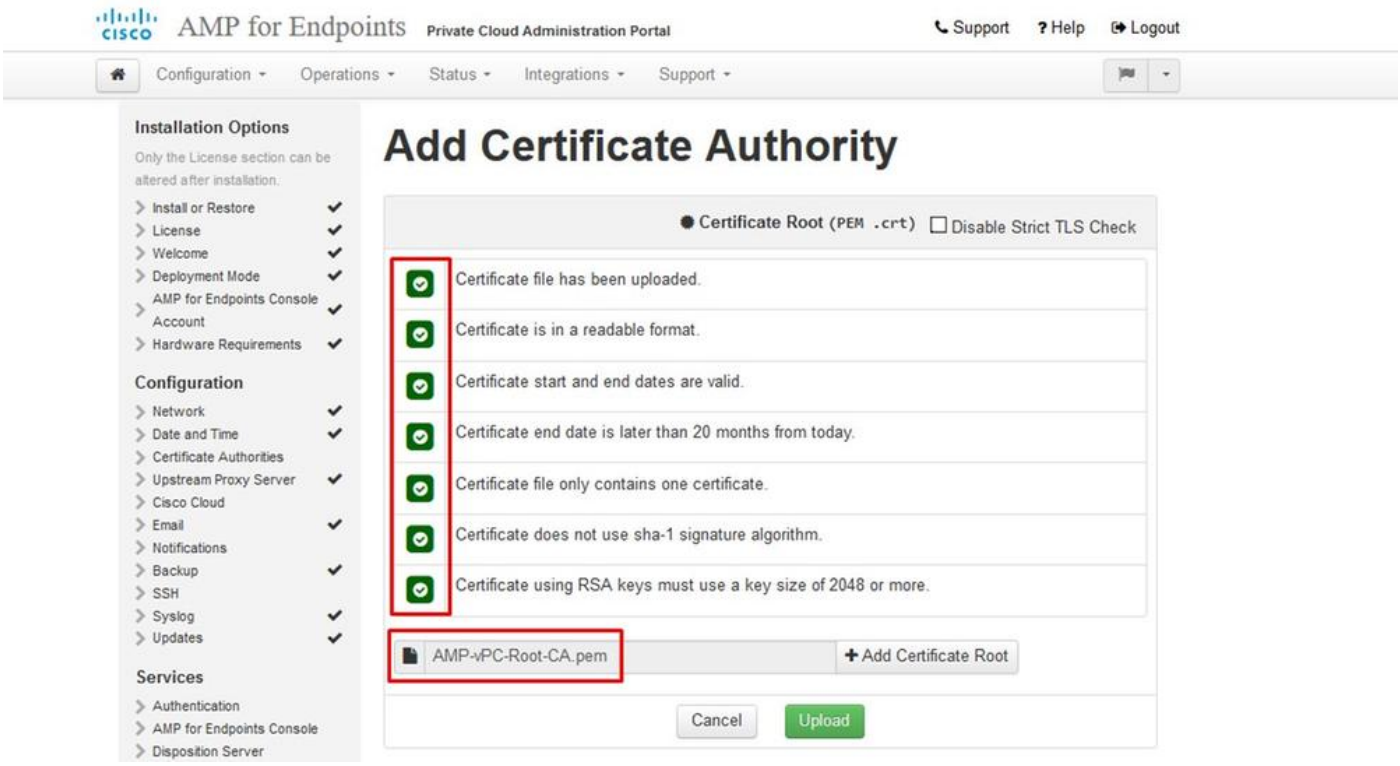


⩔ ⩔ AIRGAP UNIQUEMENT ⩔ ⩔

Étape 5 :

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







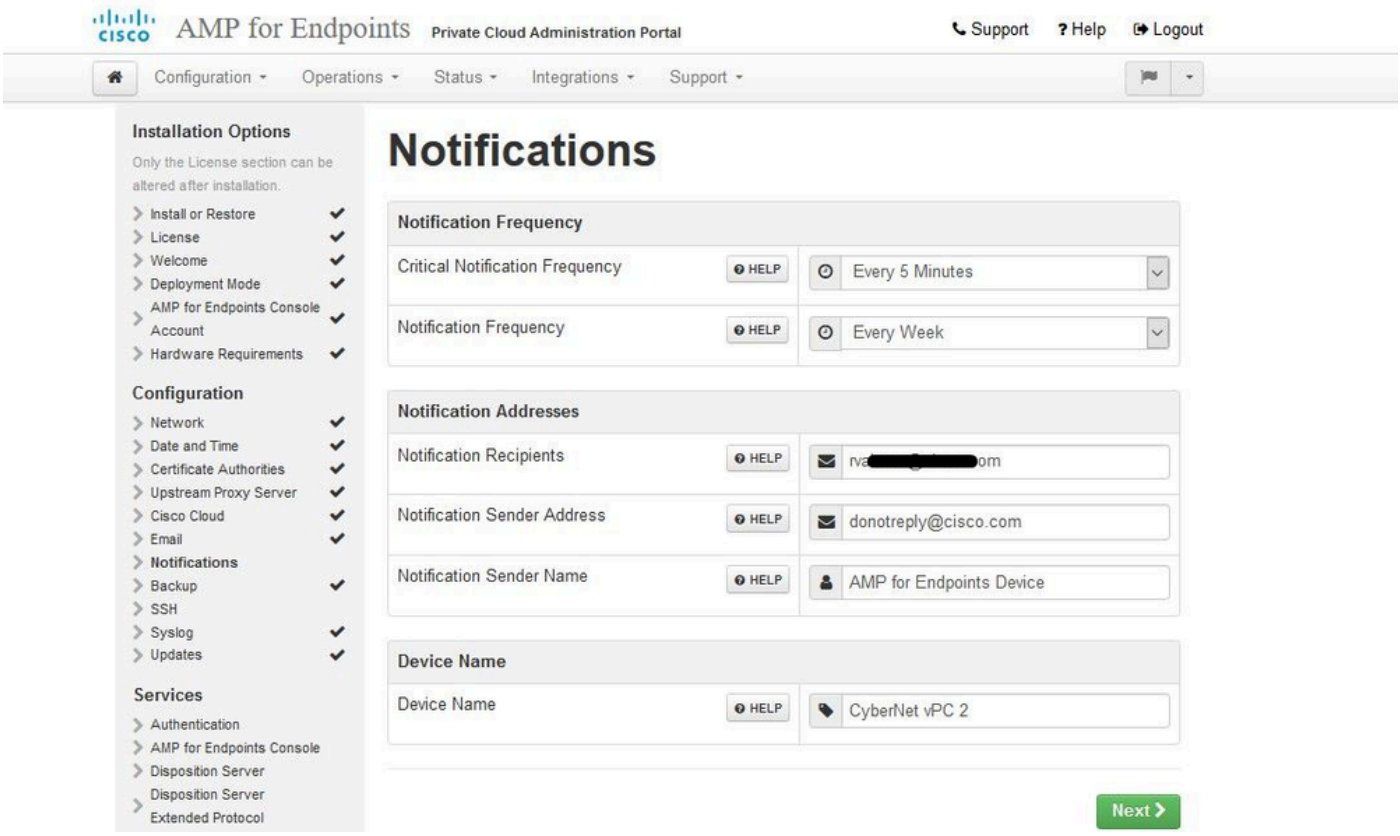
Étape 6 :

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.



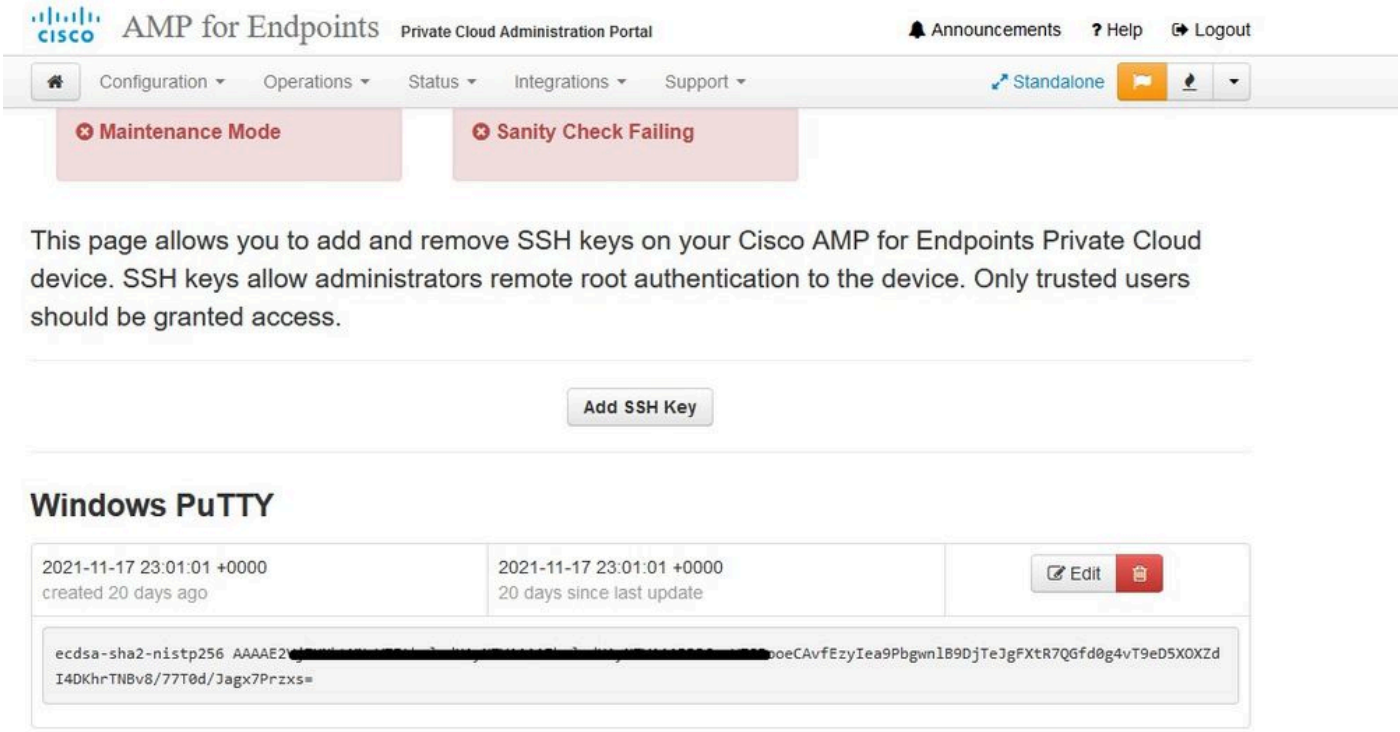
Étape 7 :

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.



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.



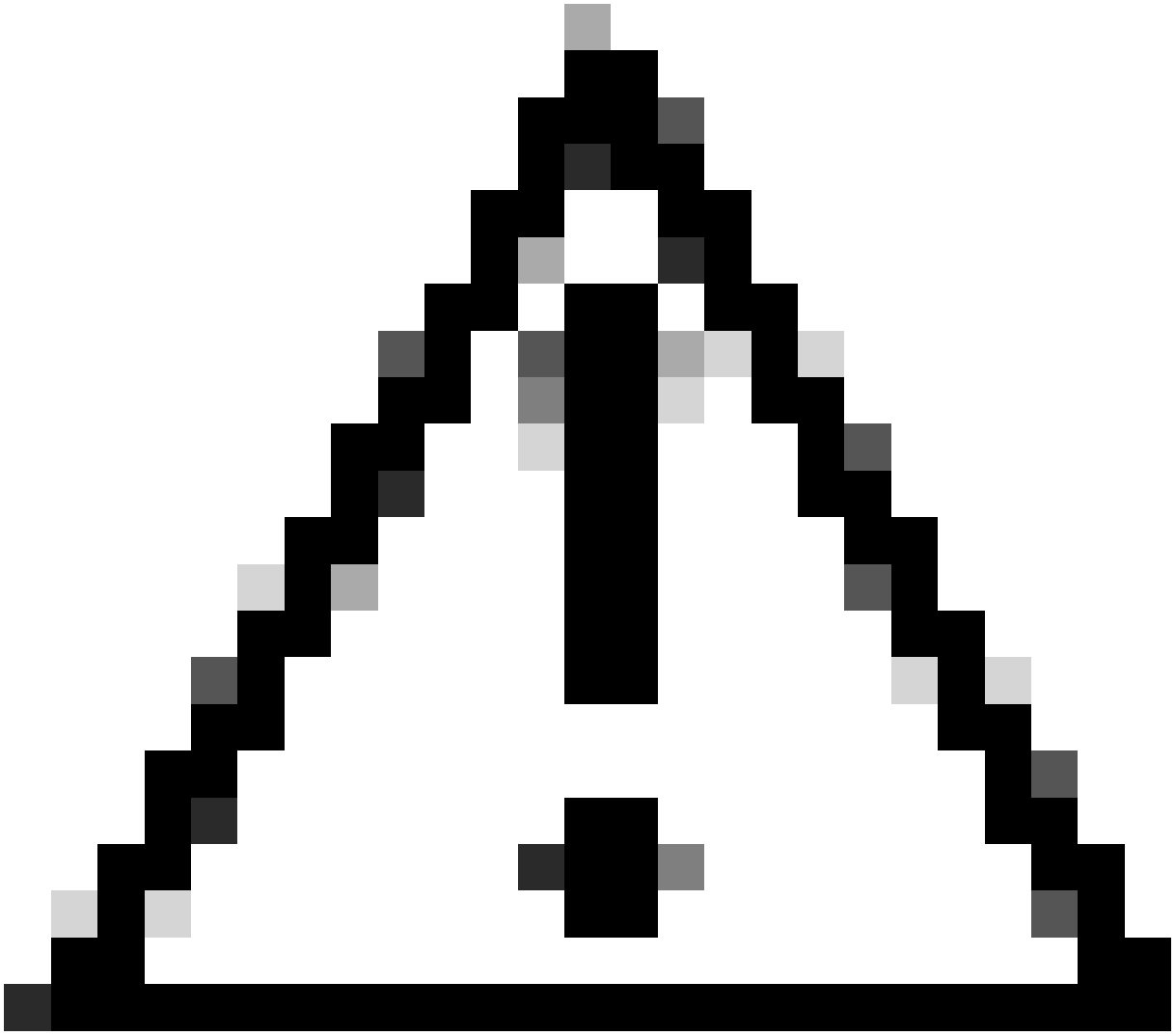
Ensuite, vous obtenez la section Services. Dans les pages suivantes, vous devez attribuer des noms d'hôte et télécharger les paires de certificats et de clés appropriées pour ces services de périphérique. Dans les diapositives suivantes, nous pouvons voir la configuration de l'un des 6 certificats.

Services

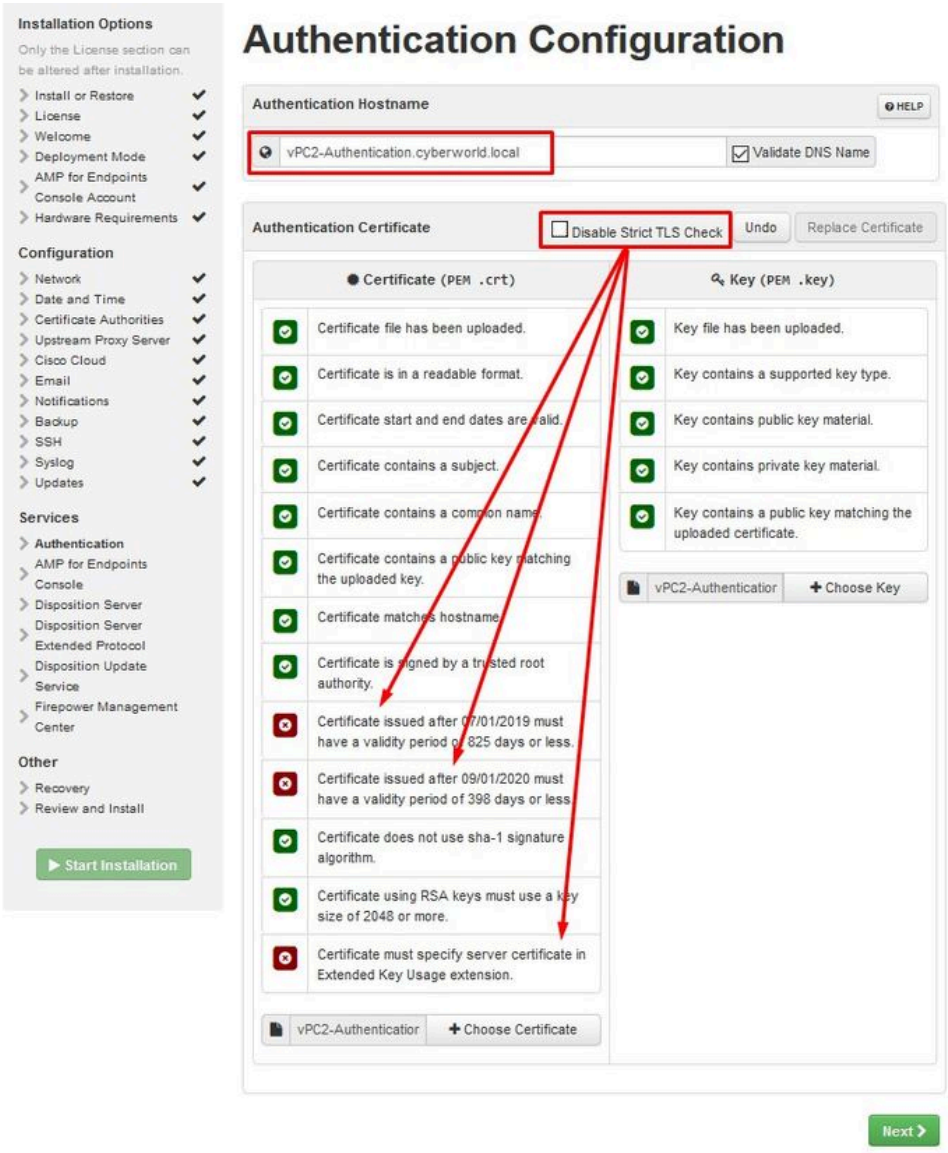
Étape 1 :

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

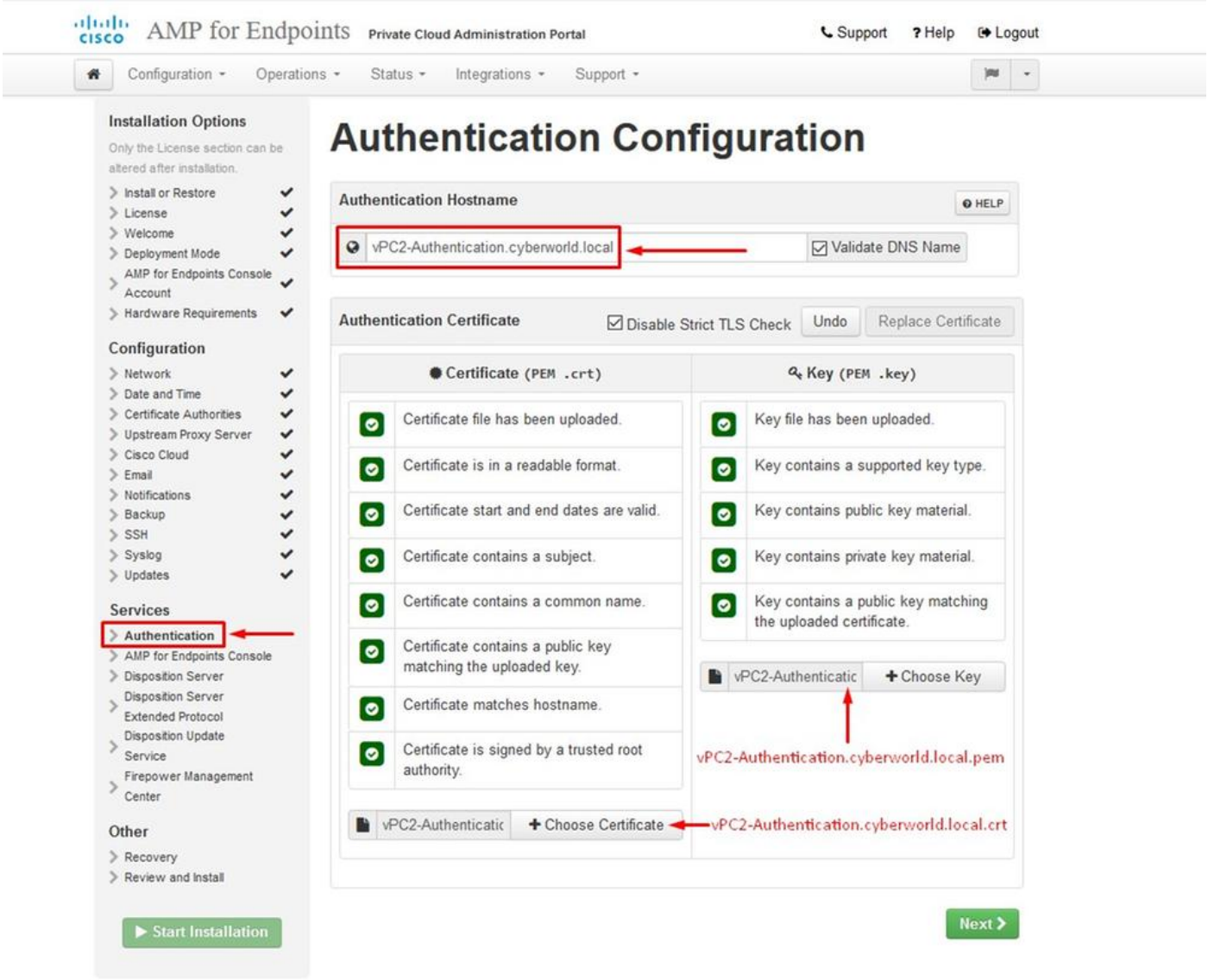
La première « erreur » que vous remarquerez peut-être est mise en surbrillance avec les 3 flèches. Pour contourner cela, décochez simplement «Désactiver le contrôle TLS strict»



Mise en garde : Sur VPC 3.8.2 et versions ultérieures, l'authentification du serveur Web TLS est désormais requise pour que le certificat soit accepté. Le certificat de service ne peut pas dépasser une validité de 398 jours.



Sans contrôle TLS strict

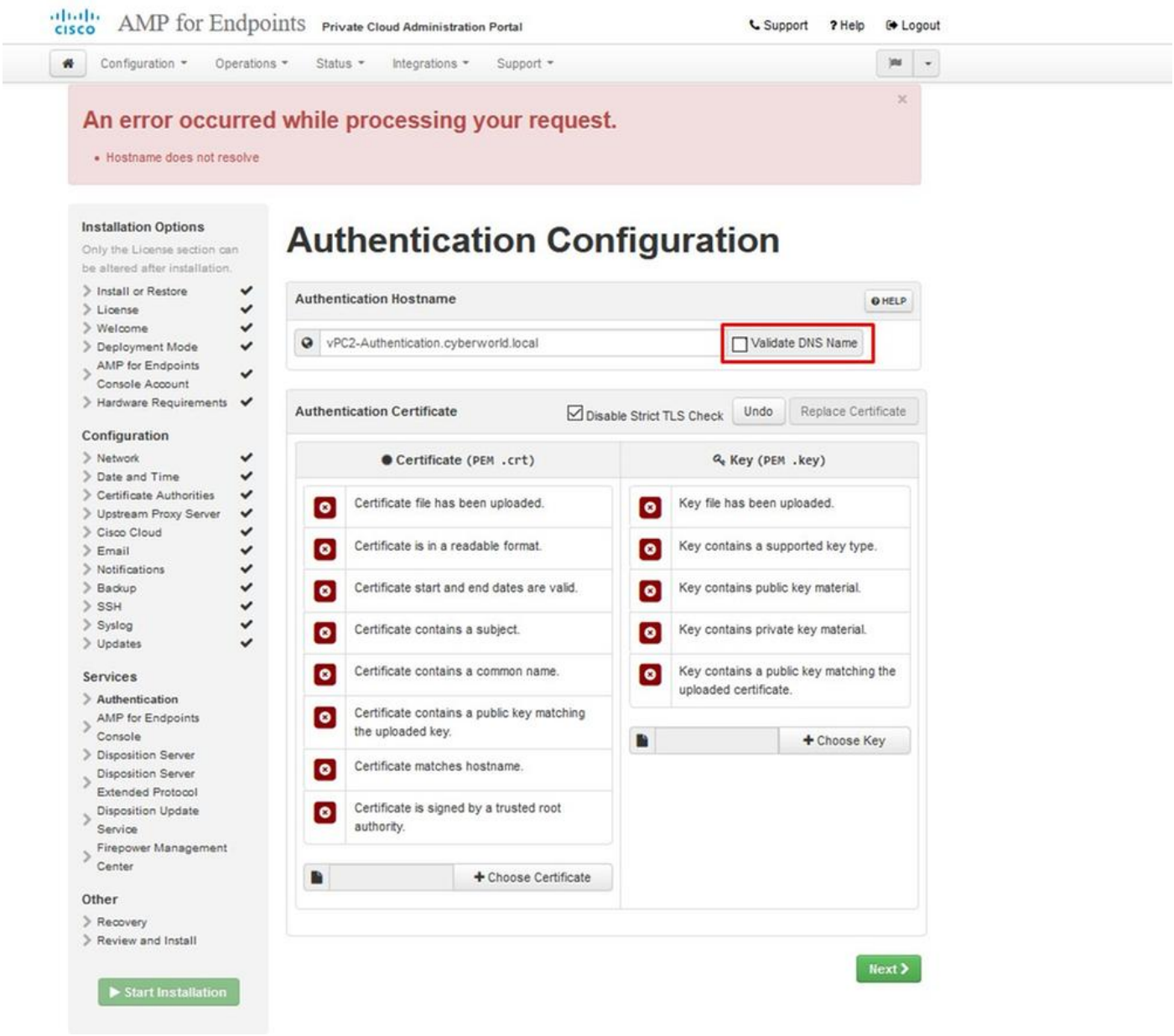


Étape 2 :

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.



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

Authentification

- 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.

⚠ Mise en garde : les noms d'hôte ne peuvent pas être modifiés une fois l'installation du périphérique terminée.

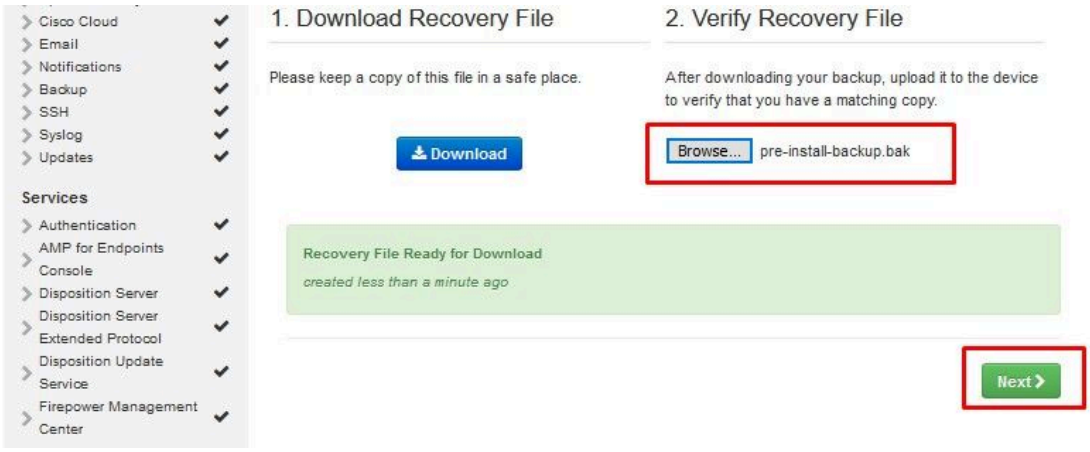
Notez les noms d'hôte requis. Vous devez créer six enregistrements DNS A uniques pour le cloud privé Secure Endpoint. Chaque enregistrement pointe vers la même adresse IP de l'interface de console de cloud privé virtuel (eth1) et doit être résolu par le cloud privé et le point d'extrémité sécurisé.

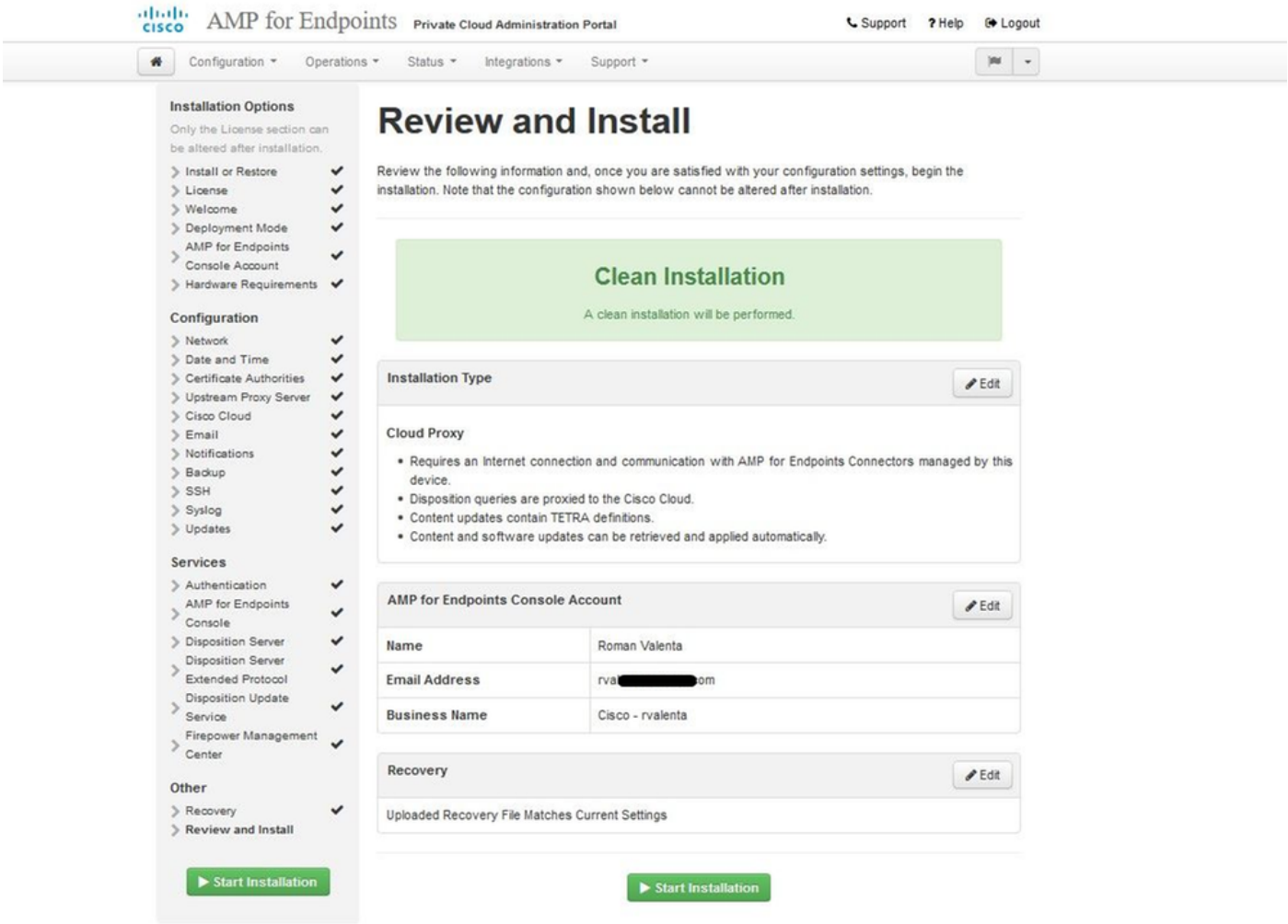
Étape 3 :

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

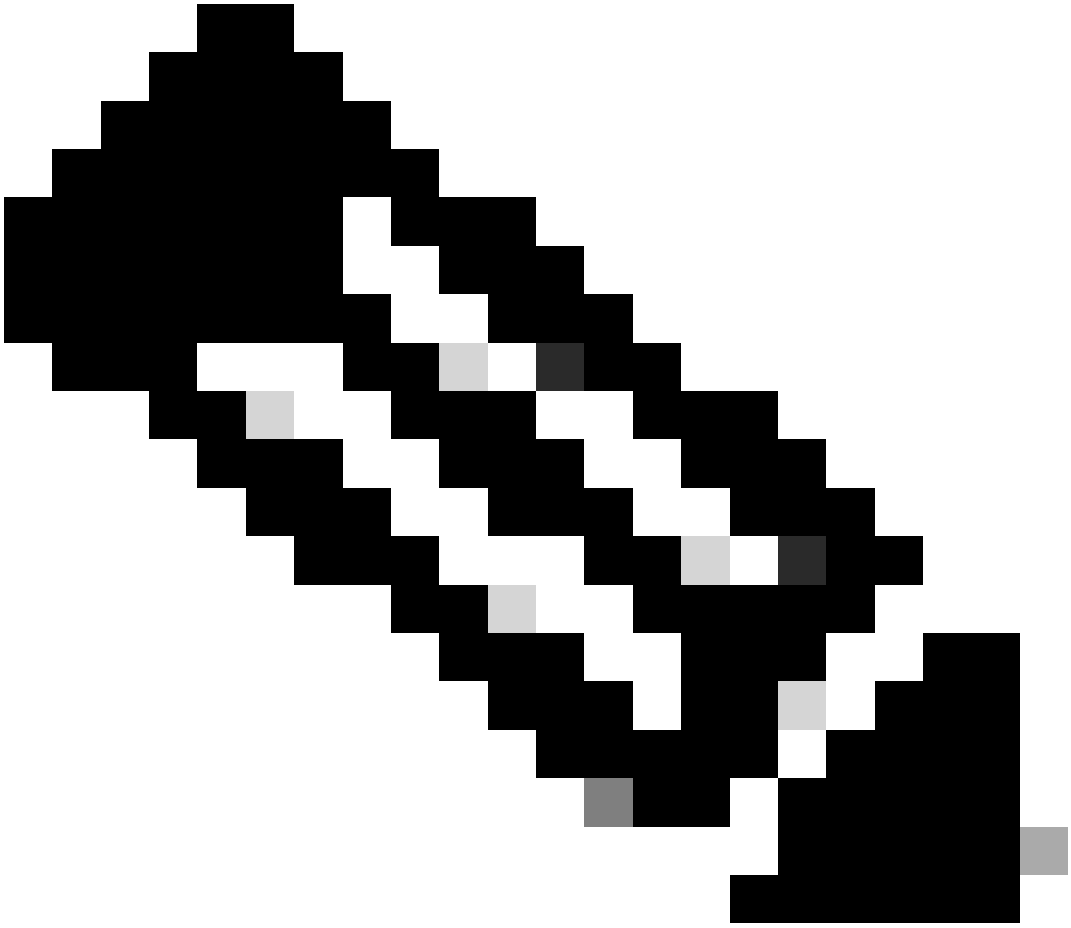
Vous obtenez la page Récupération, comme illustré dans l'image. Vous devez télécharger et vérifier une sauvegarde de votre configuration avant de commencer l'installation. Le fichier de récupération contient l'ensemble de la configuration ainsi que les clés du serveur. Si vous perdez un fichier de récupération, 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.

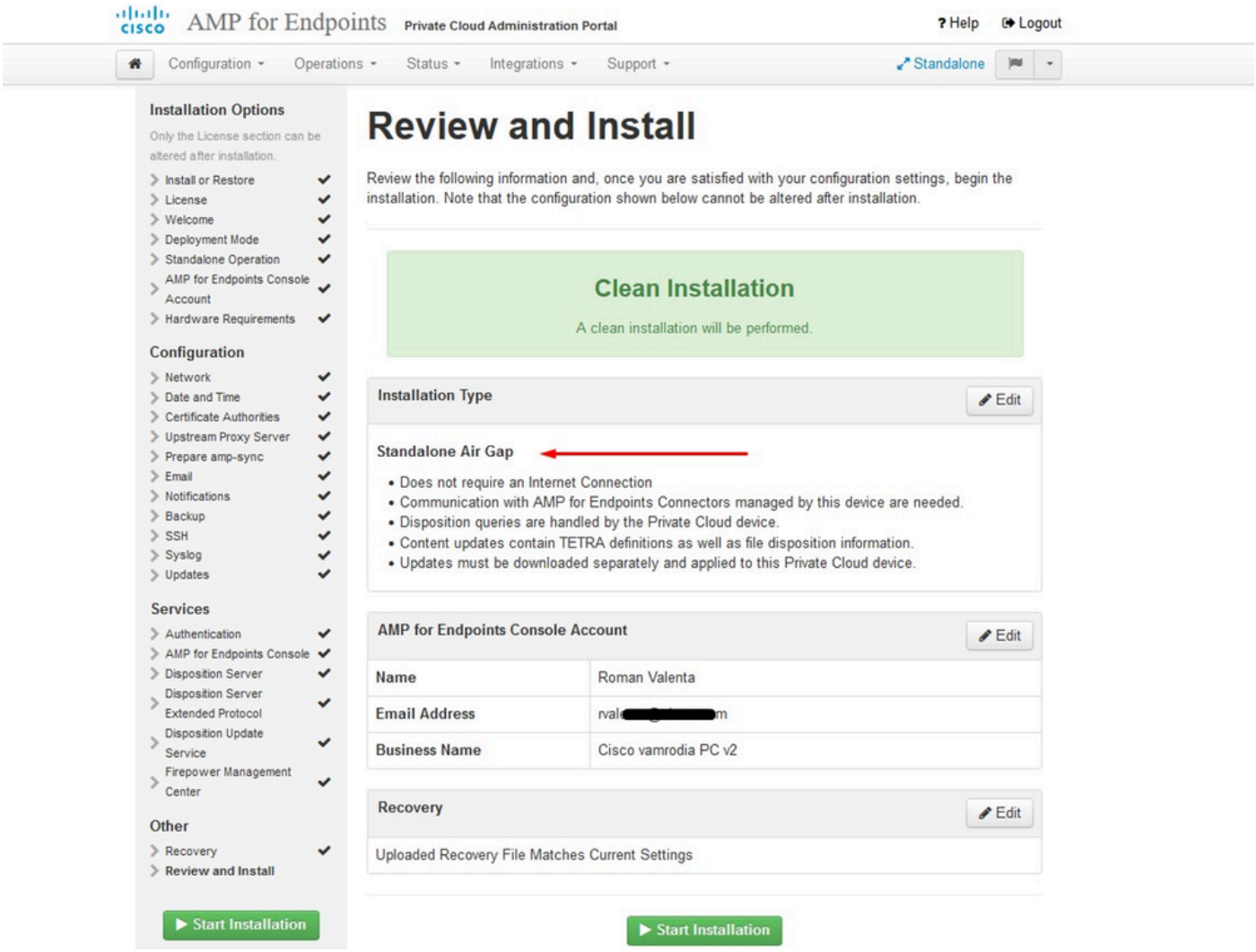




⩔⩔ ENTREFER UNIQUEMENT ⩔⩔



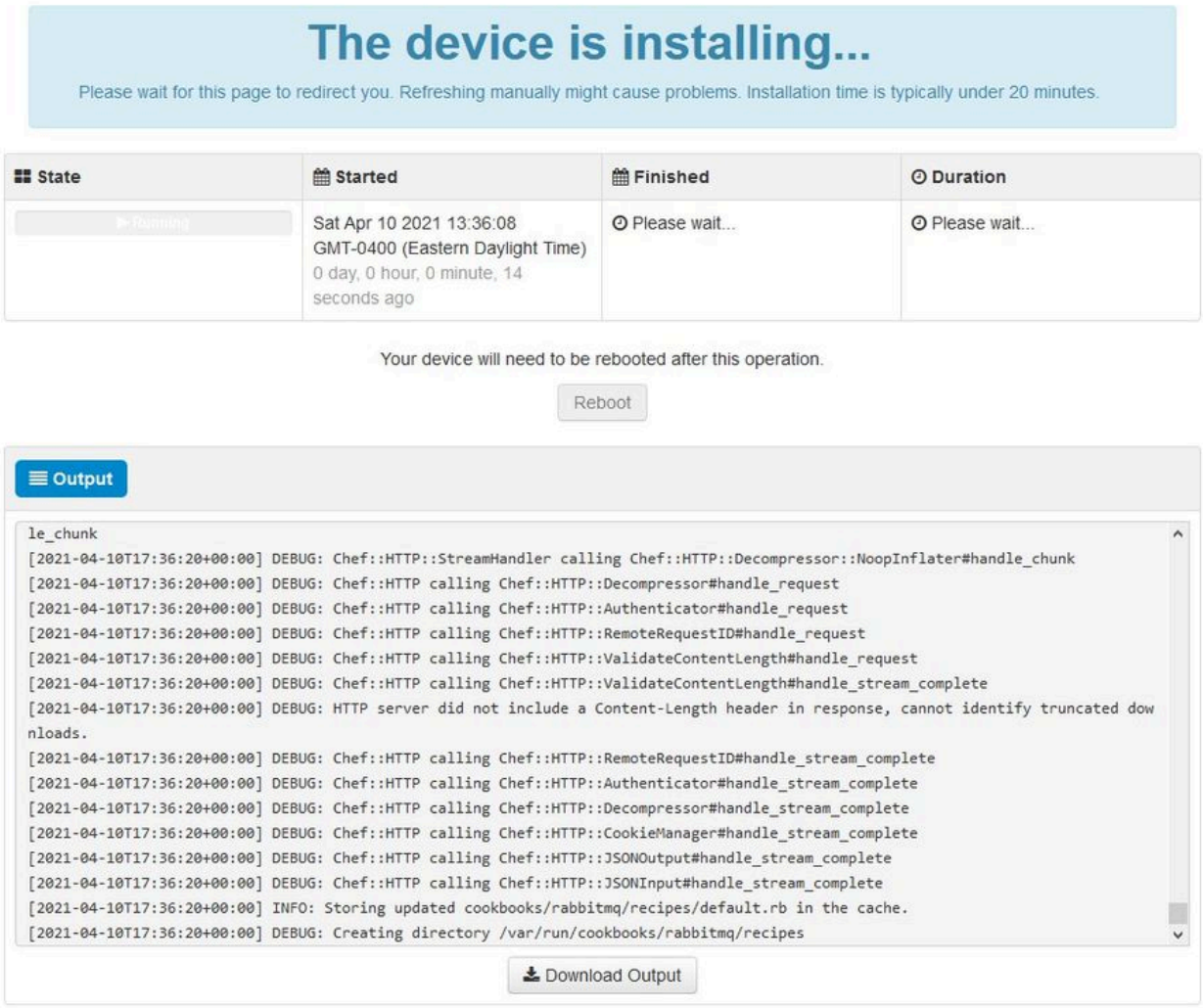
Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.



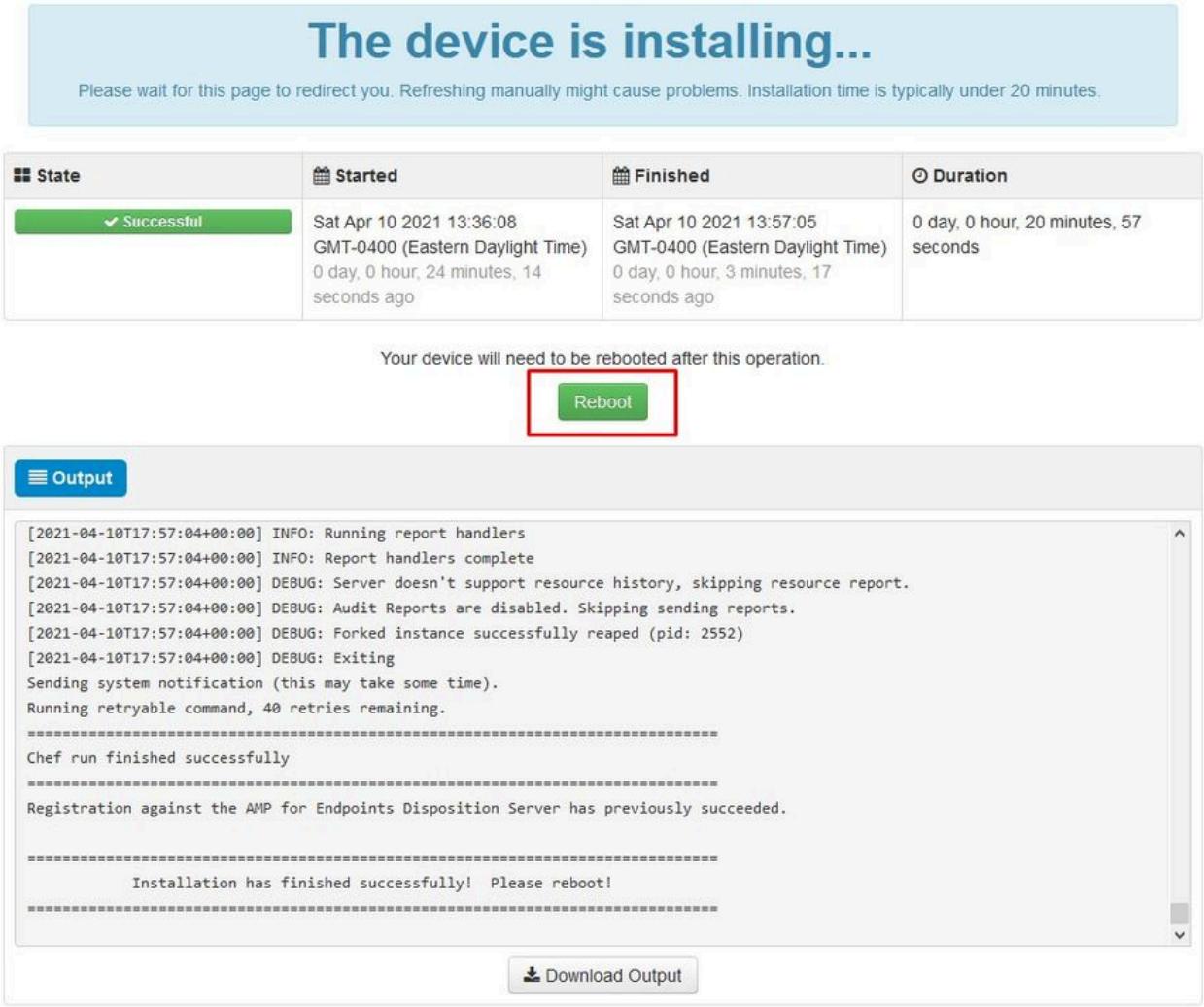
⩓ ⩓ AIRGAP UNIQUEMENT ⩓ ⩓

Vous voyez des entrées similaires comme ceci...

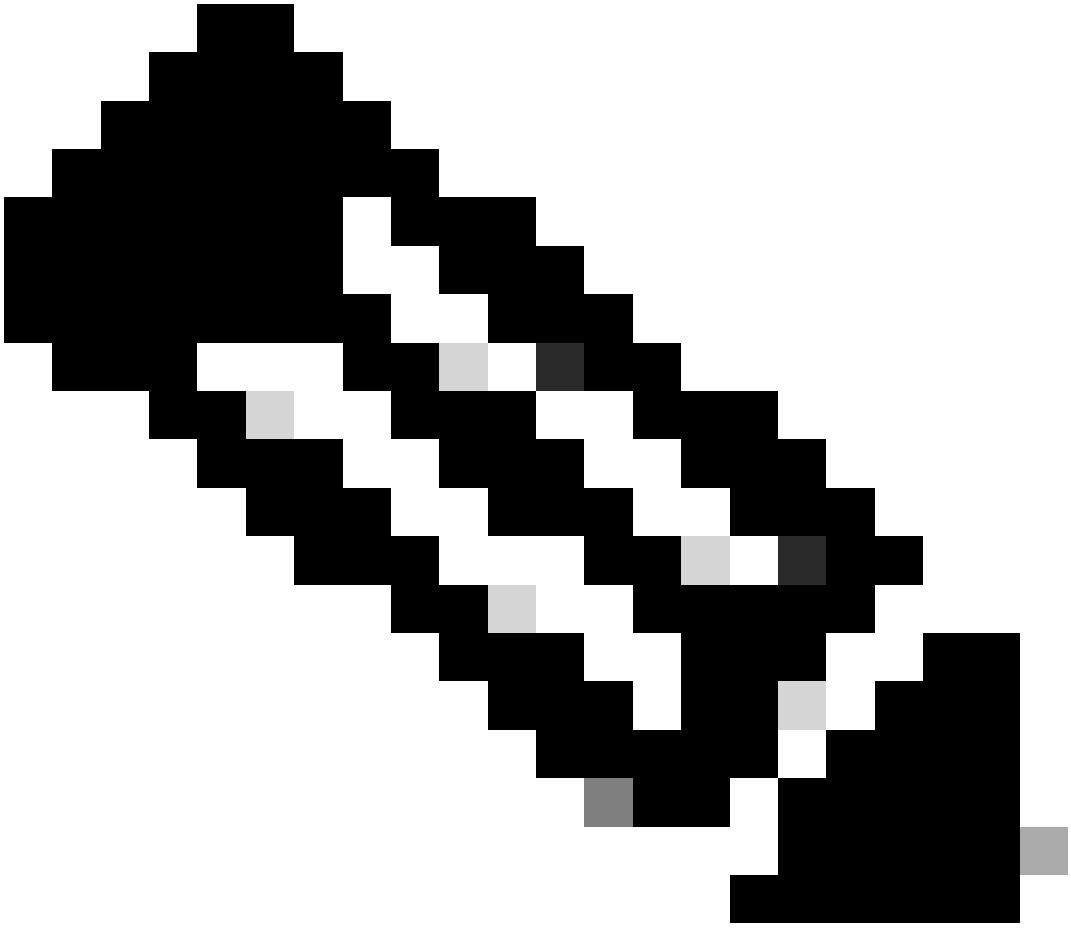
⚠ Mise en garde : Lorsque vous êtes sur cette page, ne pas actualiser car cela peut causer des problèmes.



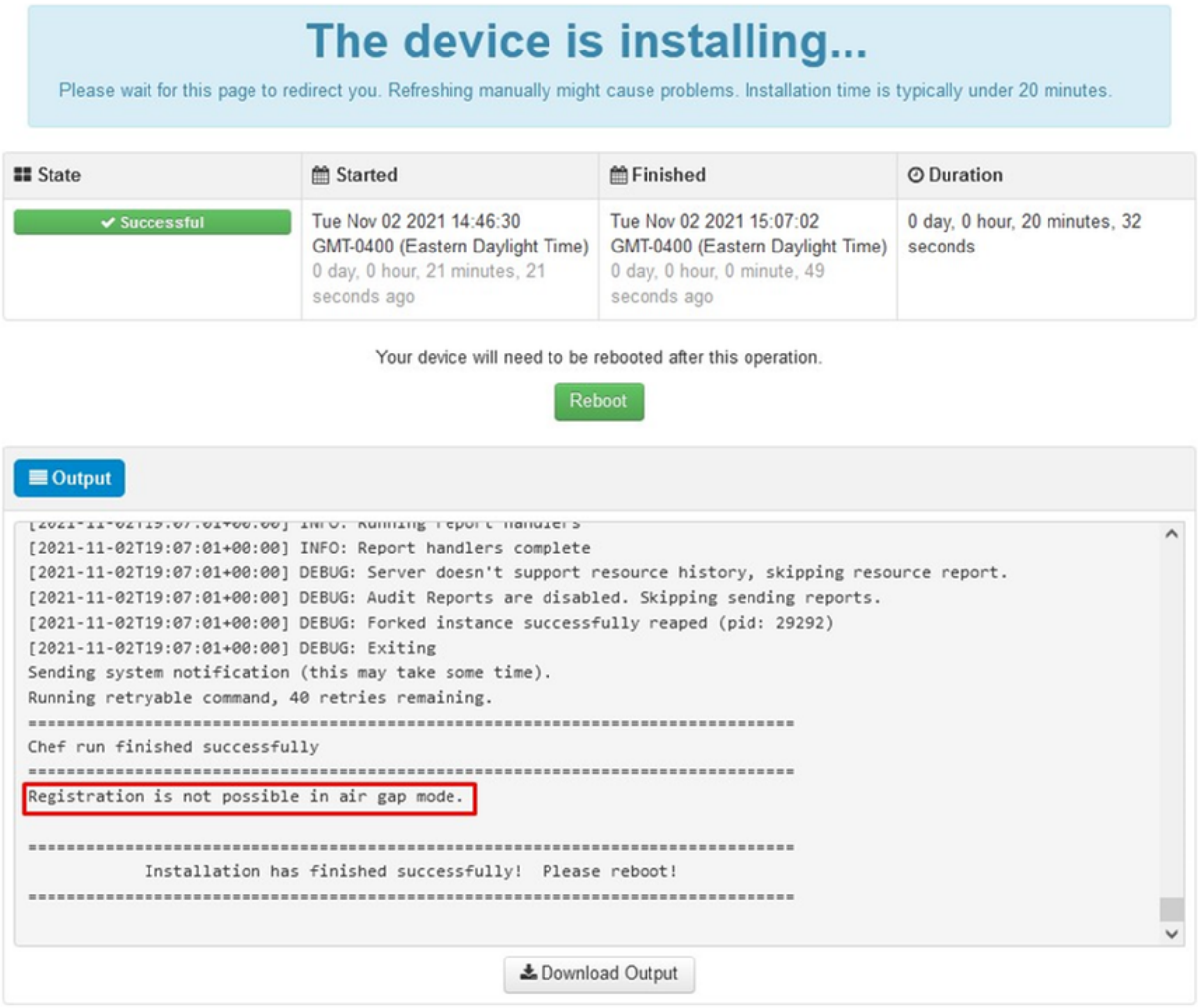
Une fois l'installation terminée, appuyez sur le bouton de redémarrage



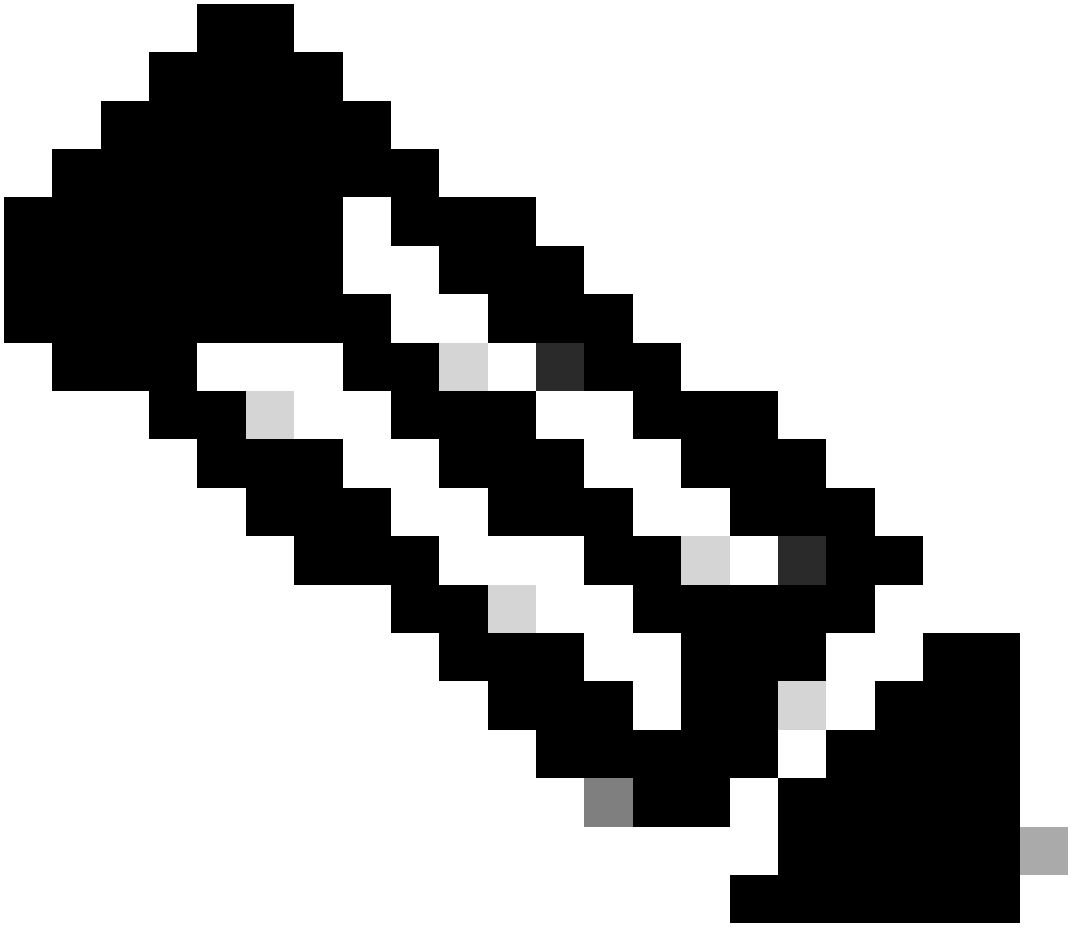
⩔ ⩔ ENTREFER UNIQUEMENT ⩔ ⩔



Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.

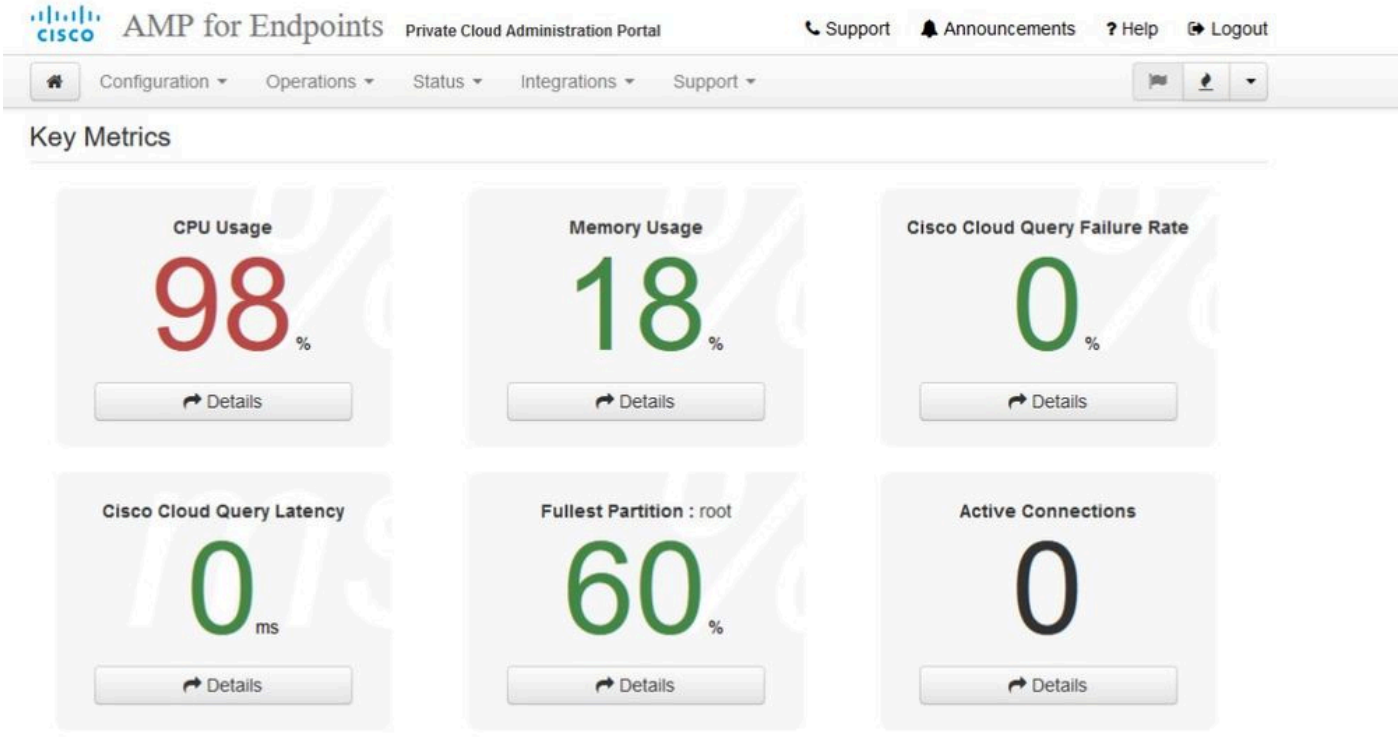


⩓ ⩓ AIRGAP UNIQUEMENT ⩓ ⩓

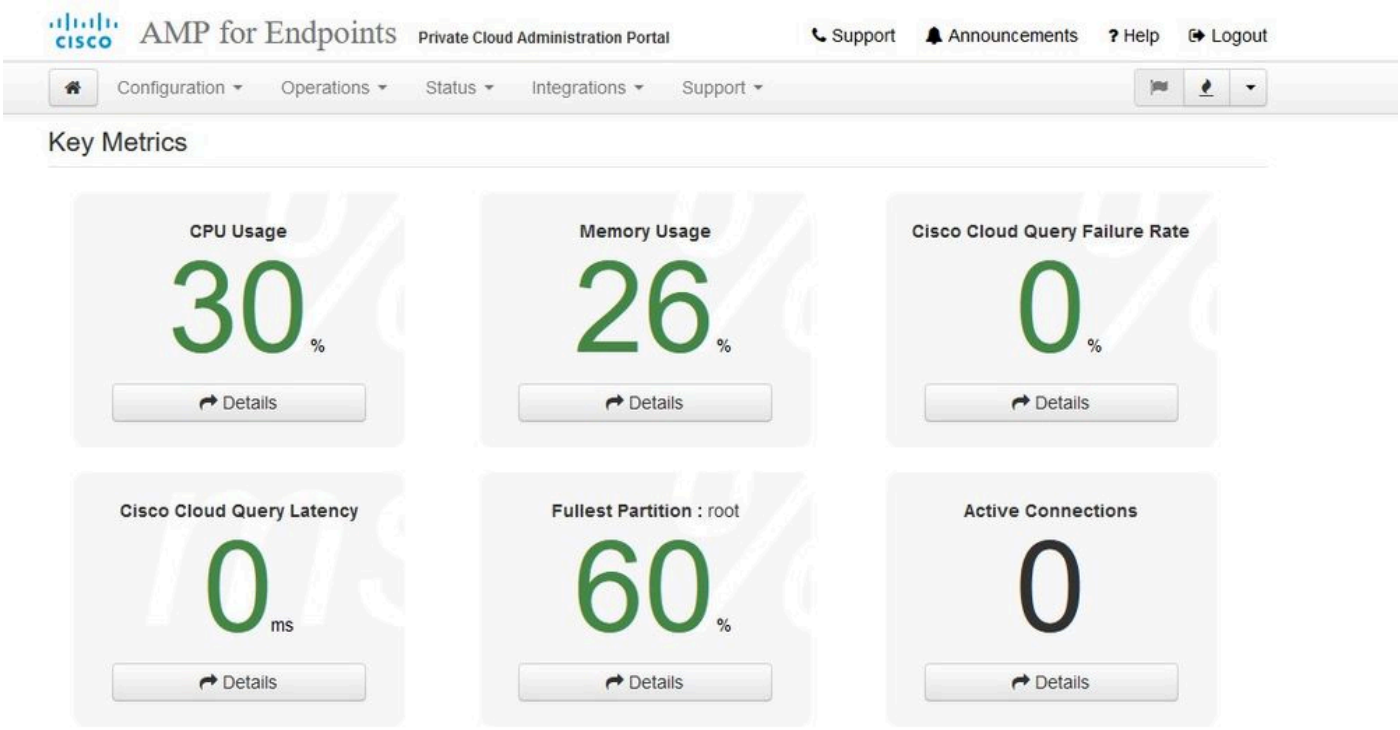


Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.

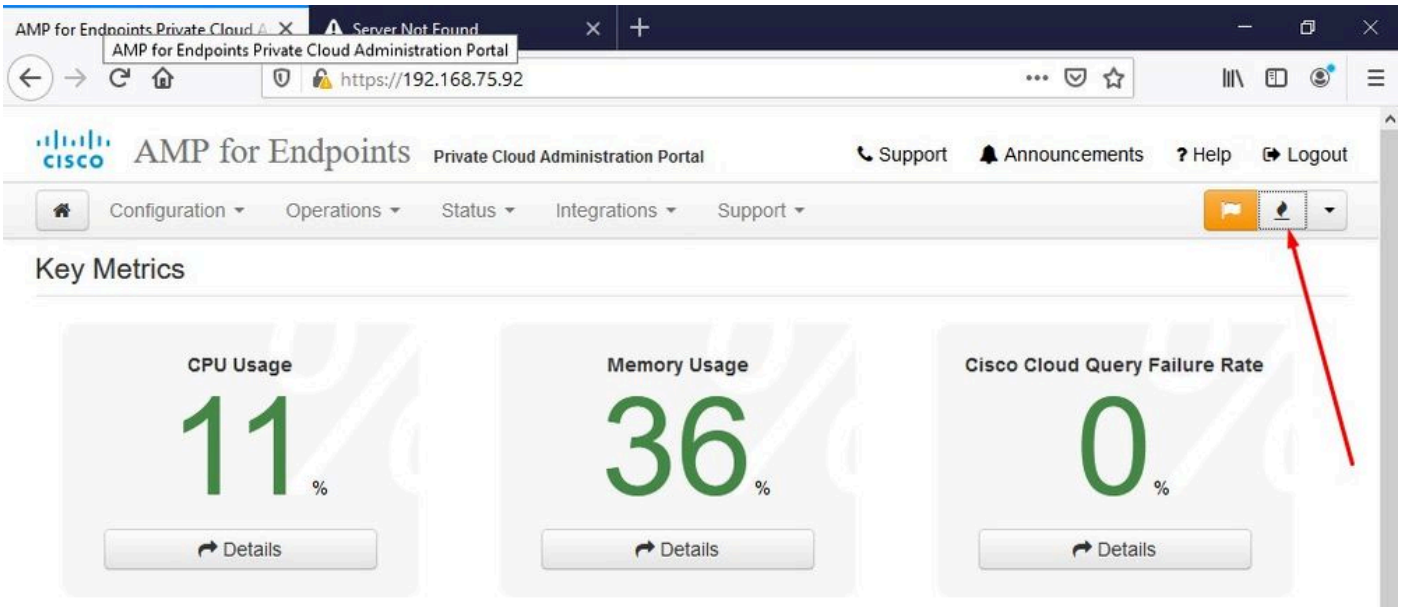
Une fois l'appliance entièrement amorcée, la prochaine fois que vous vous connecterez avec votre interface d'administration, ce tableau de bord vous sera présenté. Vous remarquerez peut-être un processeur élevé au début, mais si vous donnez quelques minutes, il se calme.



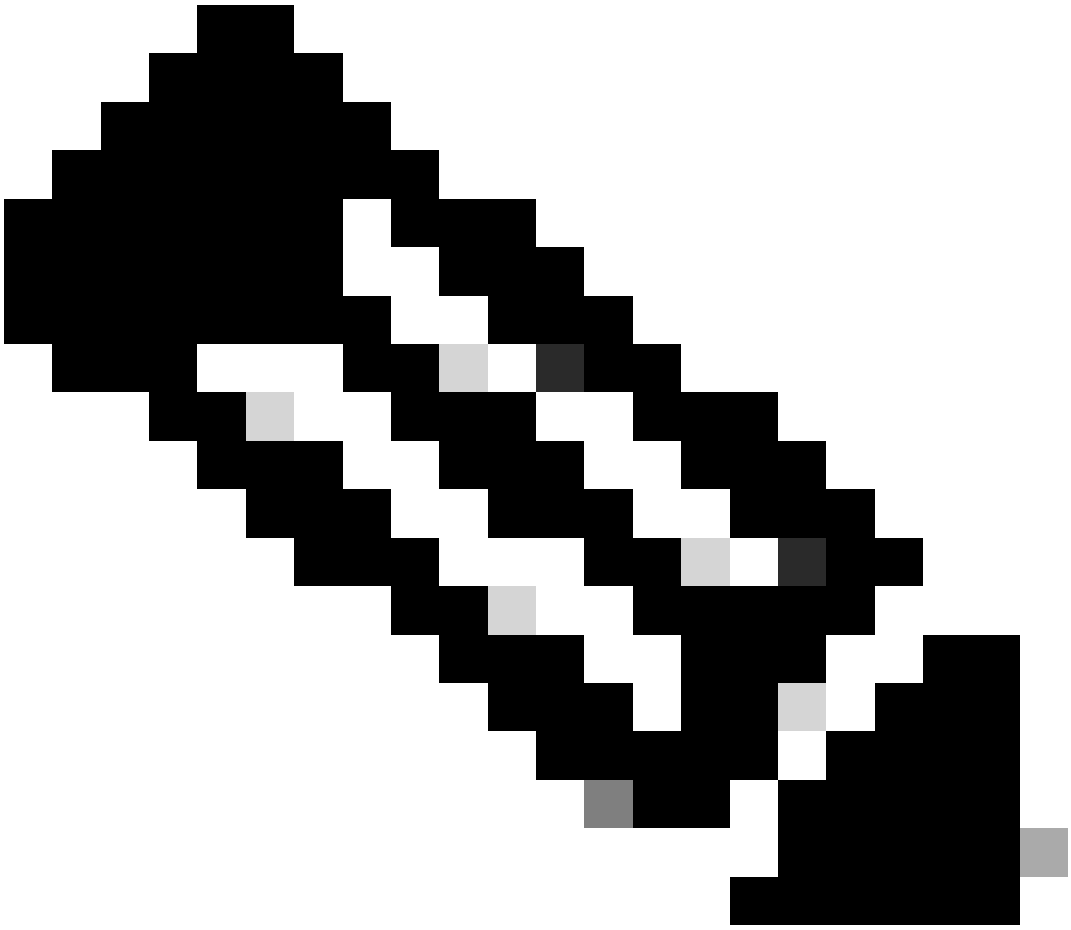
Après quelques minutes...



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.

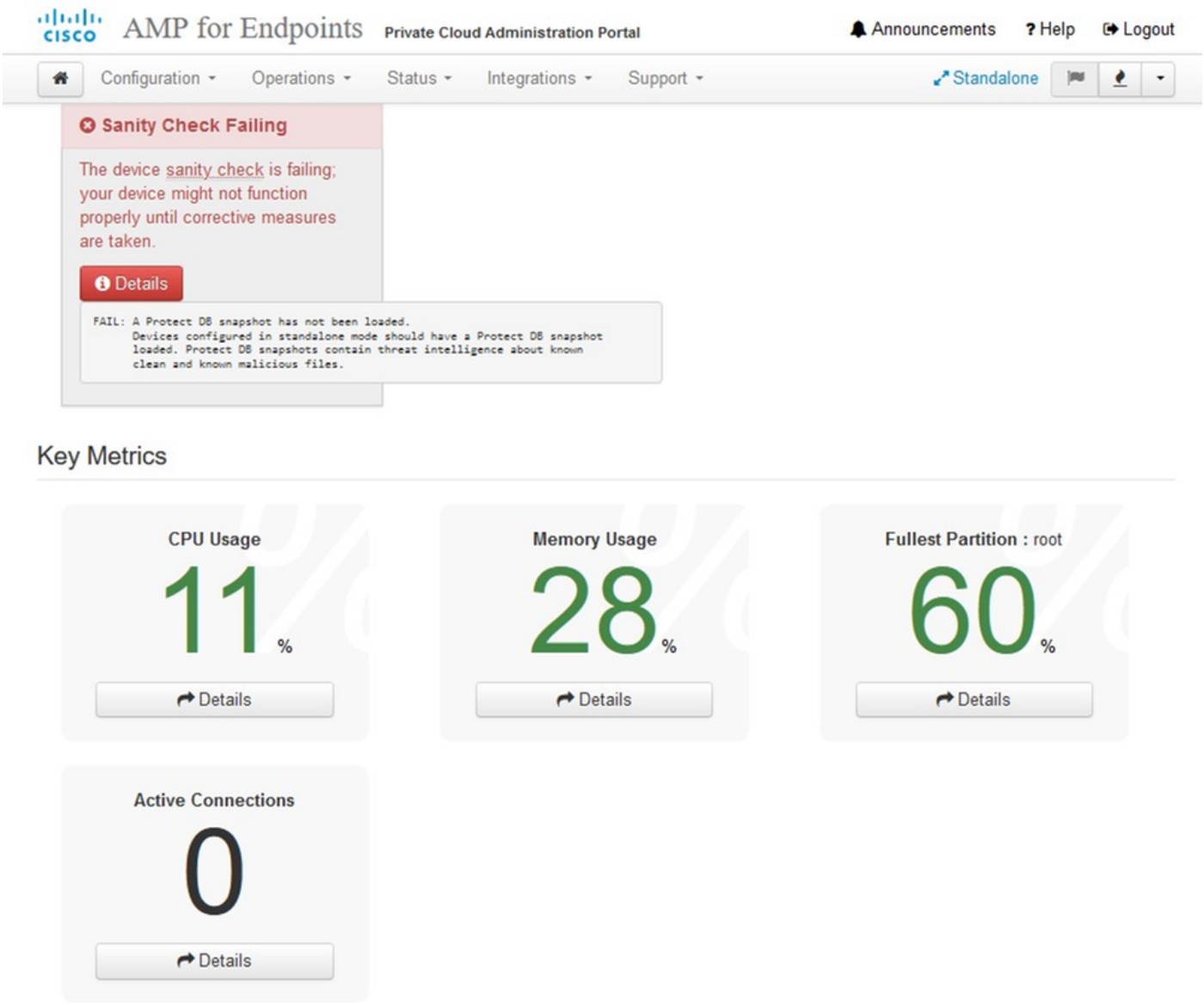


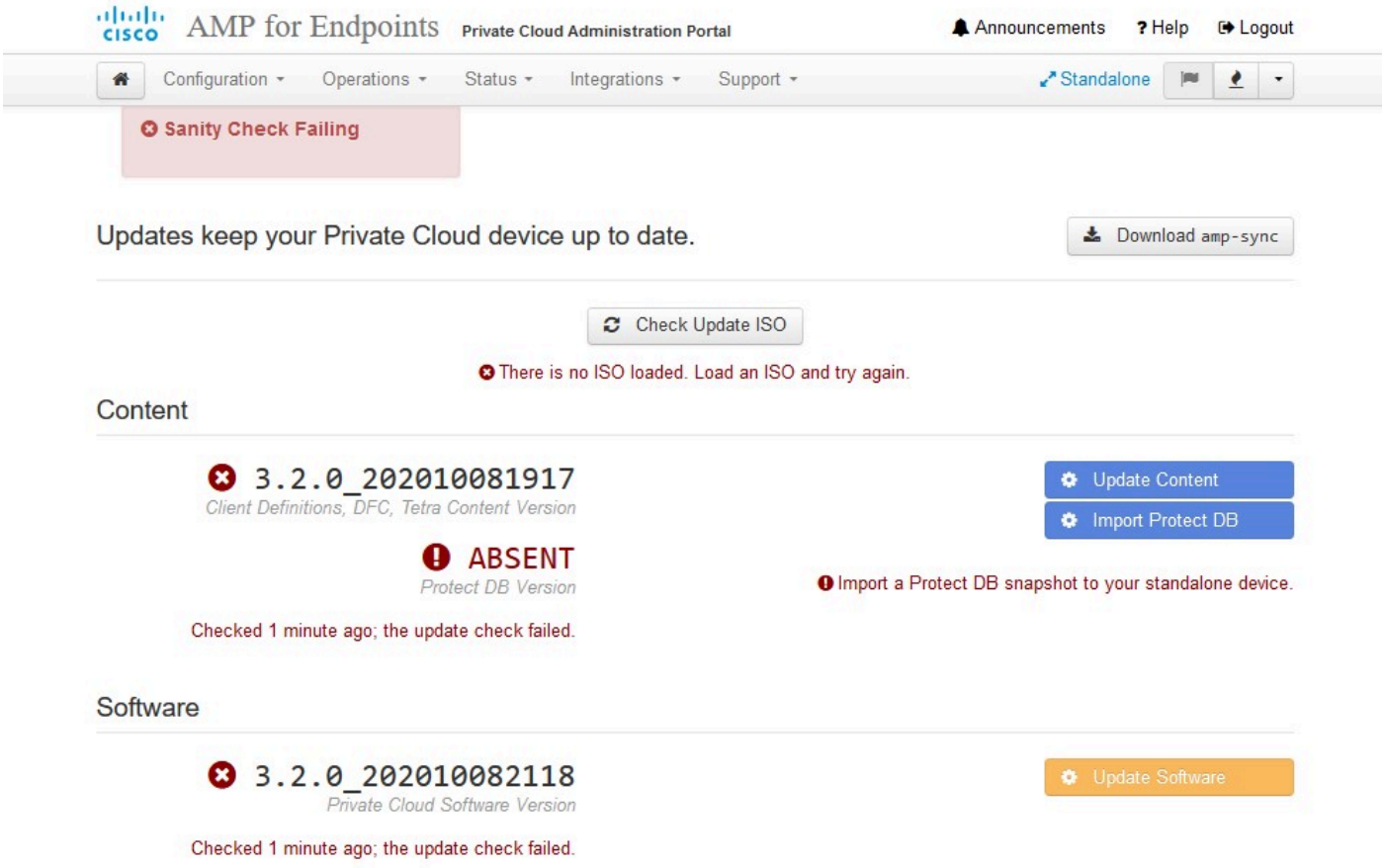
⩔⩔ ENTREFER UNIQUEMENT ⩔⩔



Remarque : Ces étapes s'appliquent uniquement à l'appliance physique.

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. Cela doit être fait par mise à jour hors ligne via le fichier ISO téléchargé préalablement préparé par amp-sync et téléchargé vers l'emplacement NFS.





Ensemble de mise à jour AirGap

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

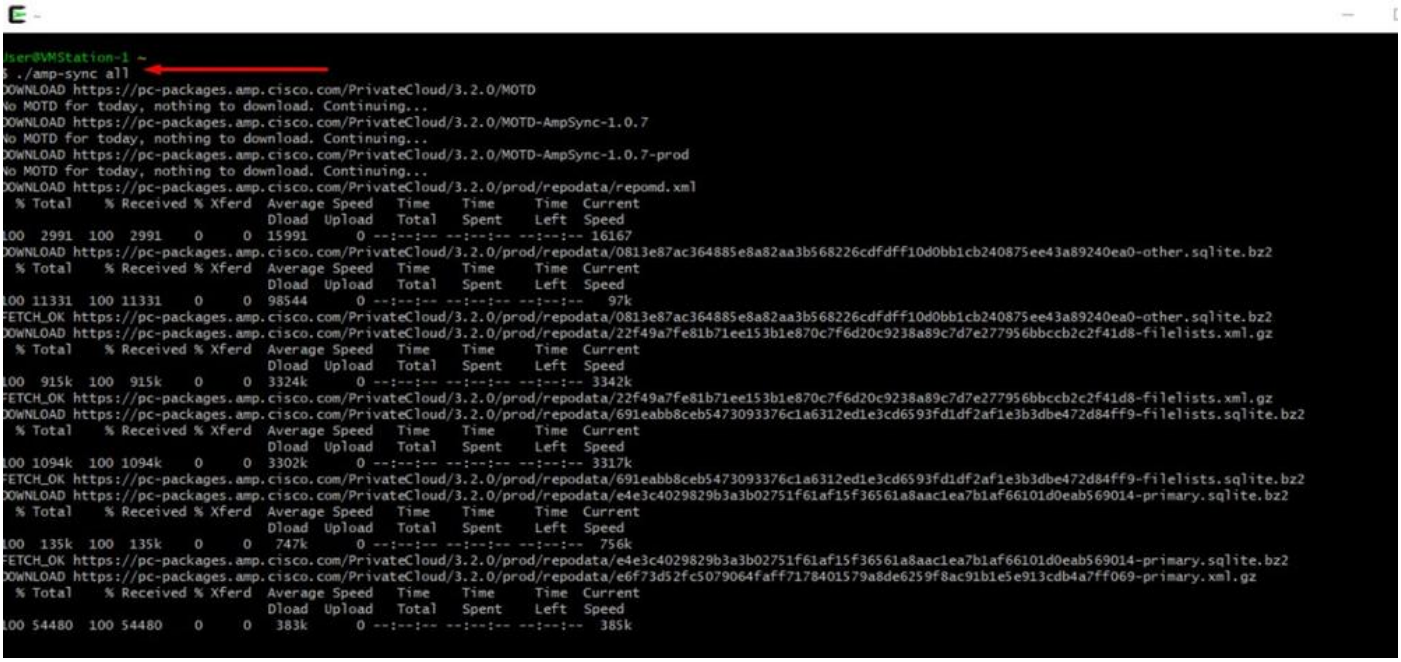
```
./amp-sync all
```

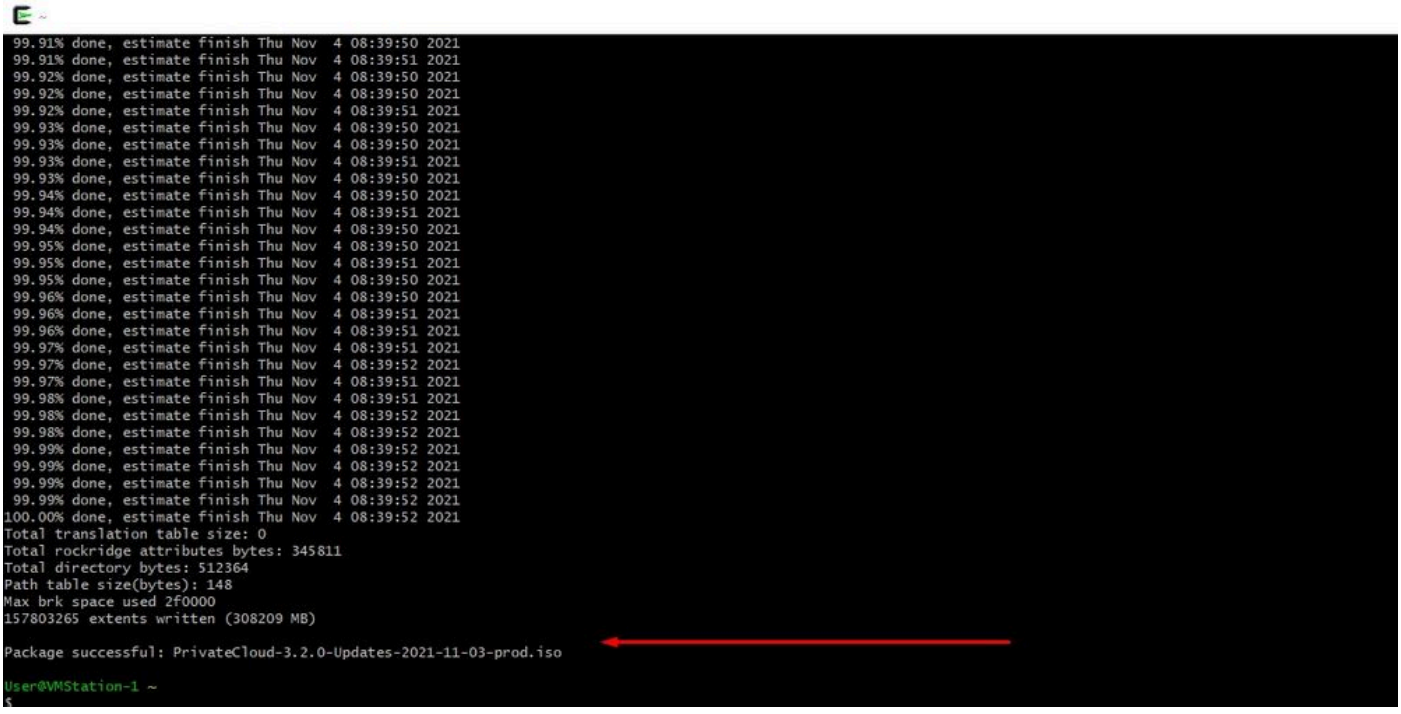
Remarque : Téléchargez tous les packages à l'aide de cette commande, puis vérifiez que peut prendre beaucoup de temps. Dépend de la vitesse et de la qualité de la liaison. Dans mon cas, avec la fibre 1Gig, il faut encore 25 heures pour le réaliser. En partie, cela est également dû au fait que ce téléchargement 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.

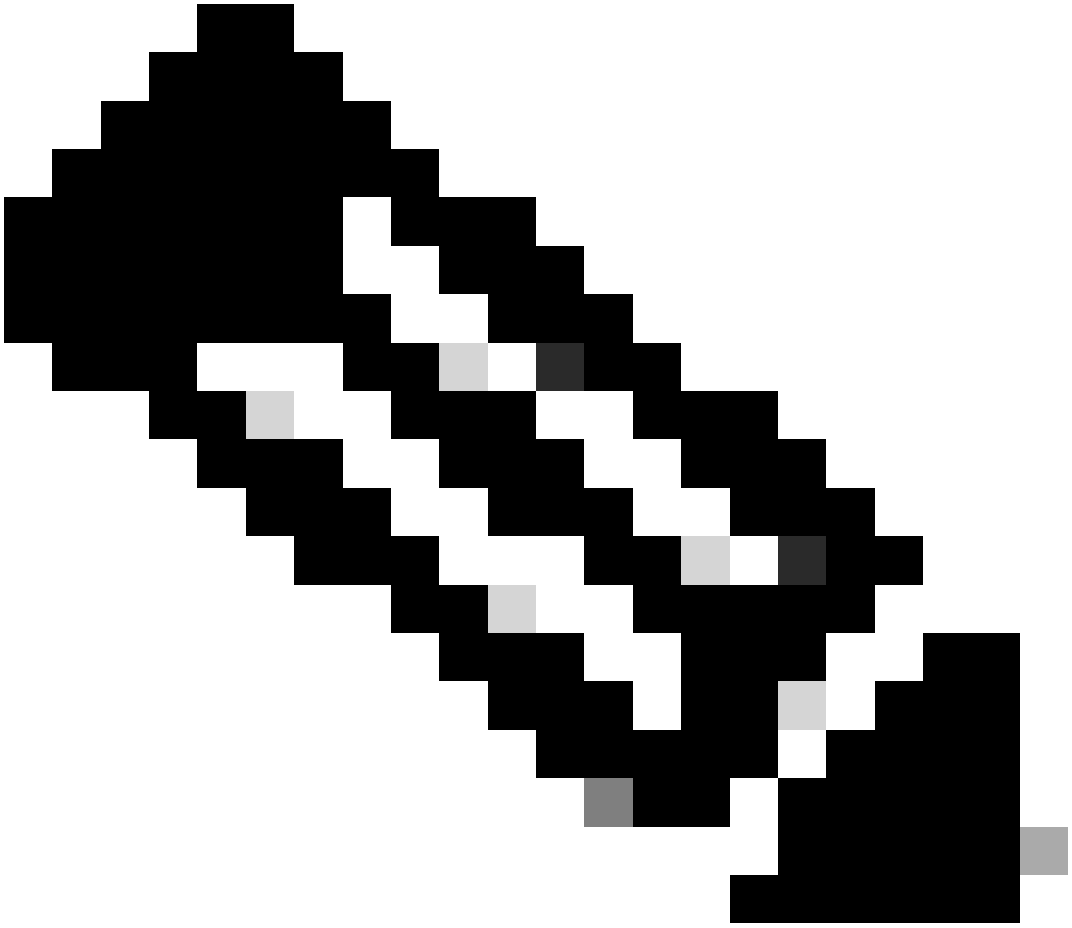
Dans cet exemple, nous avons utilisé CygWin64

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.

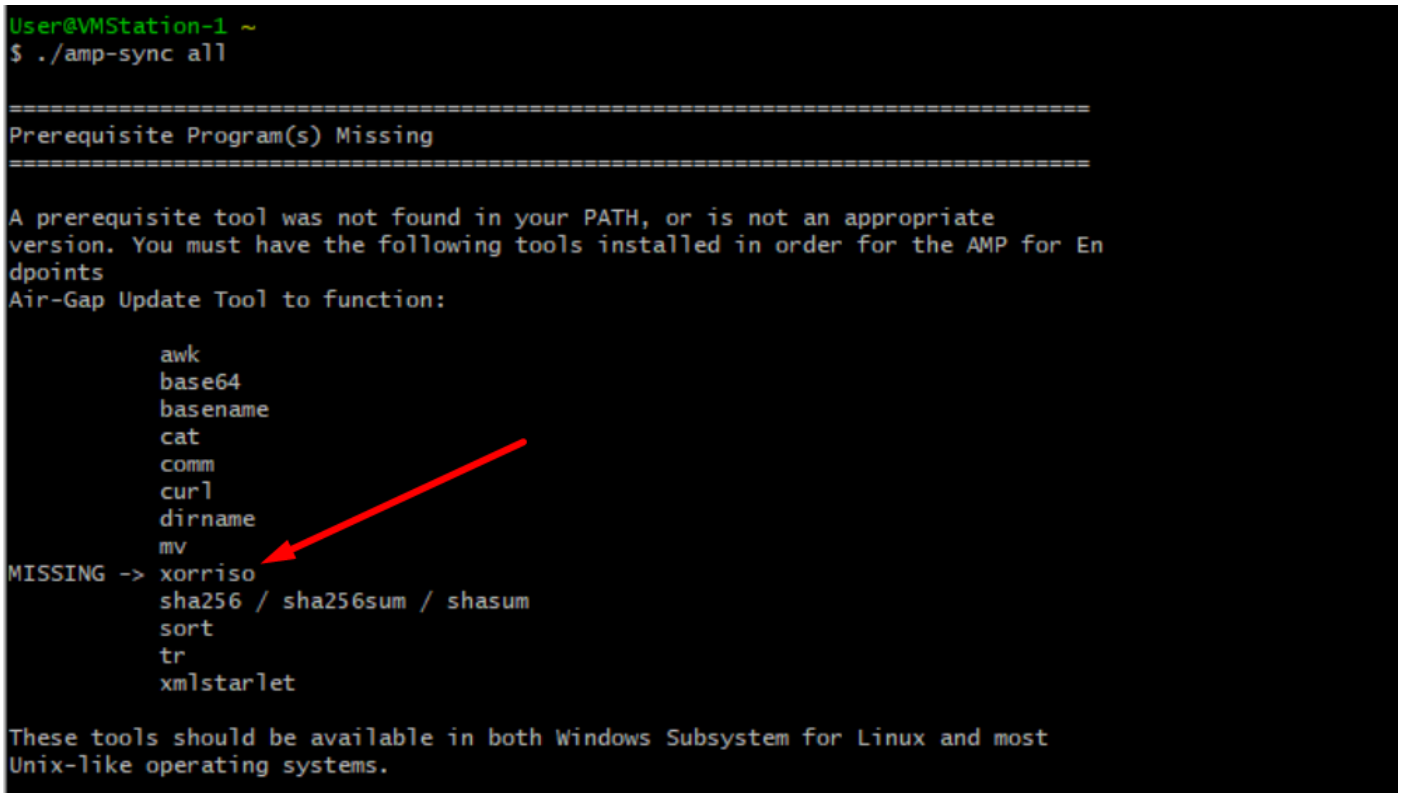
3. Choisissez un miroir de téléchargement.
4. Sélectionnez les packages à installer :
Tout -> Filet -> boucle
Tous -> Utils -> genisoimage
Tous -> Utilitaires -> xmlstarlet
* VPC 3.8.x up - > xorriso







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.



Notes de version Page #58. Comme vous pouvez le voir, «xorriso» est maintenant requis. 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.

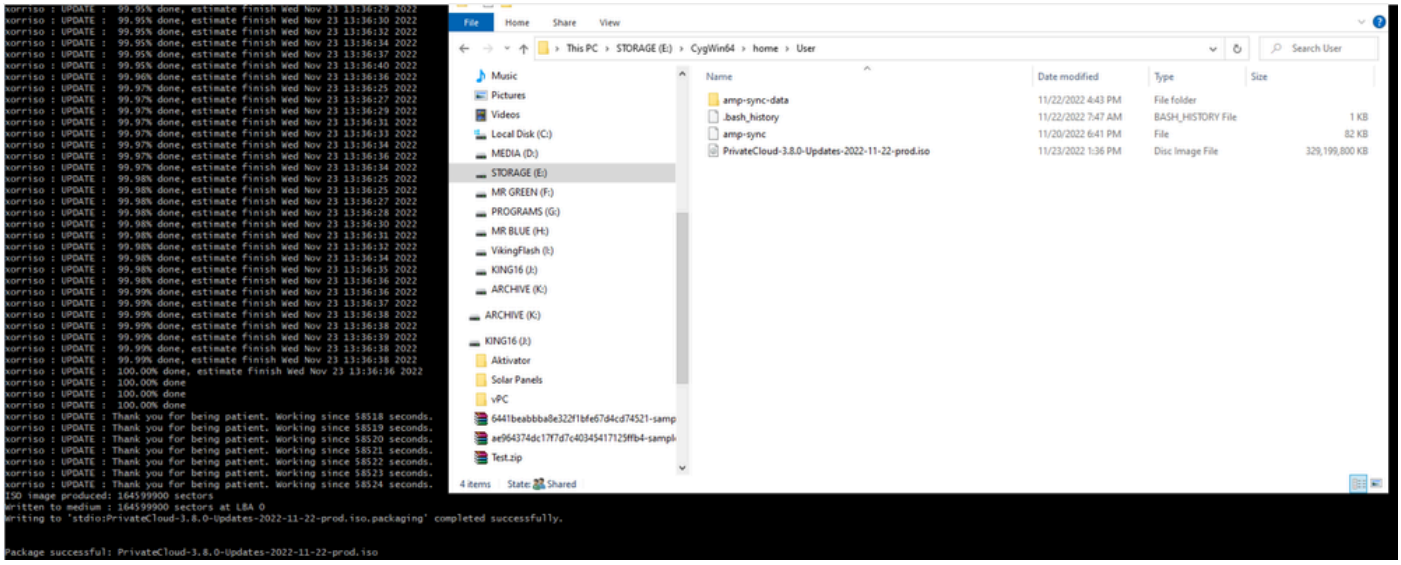
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

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 à nouveau, 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 <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 chemin <CygWin64\bin> de votre installation CygWin locale. 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.

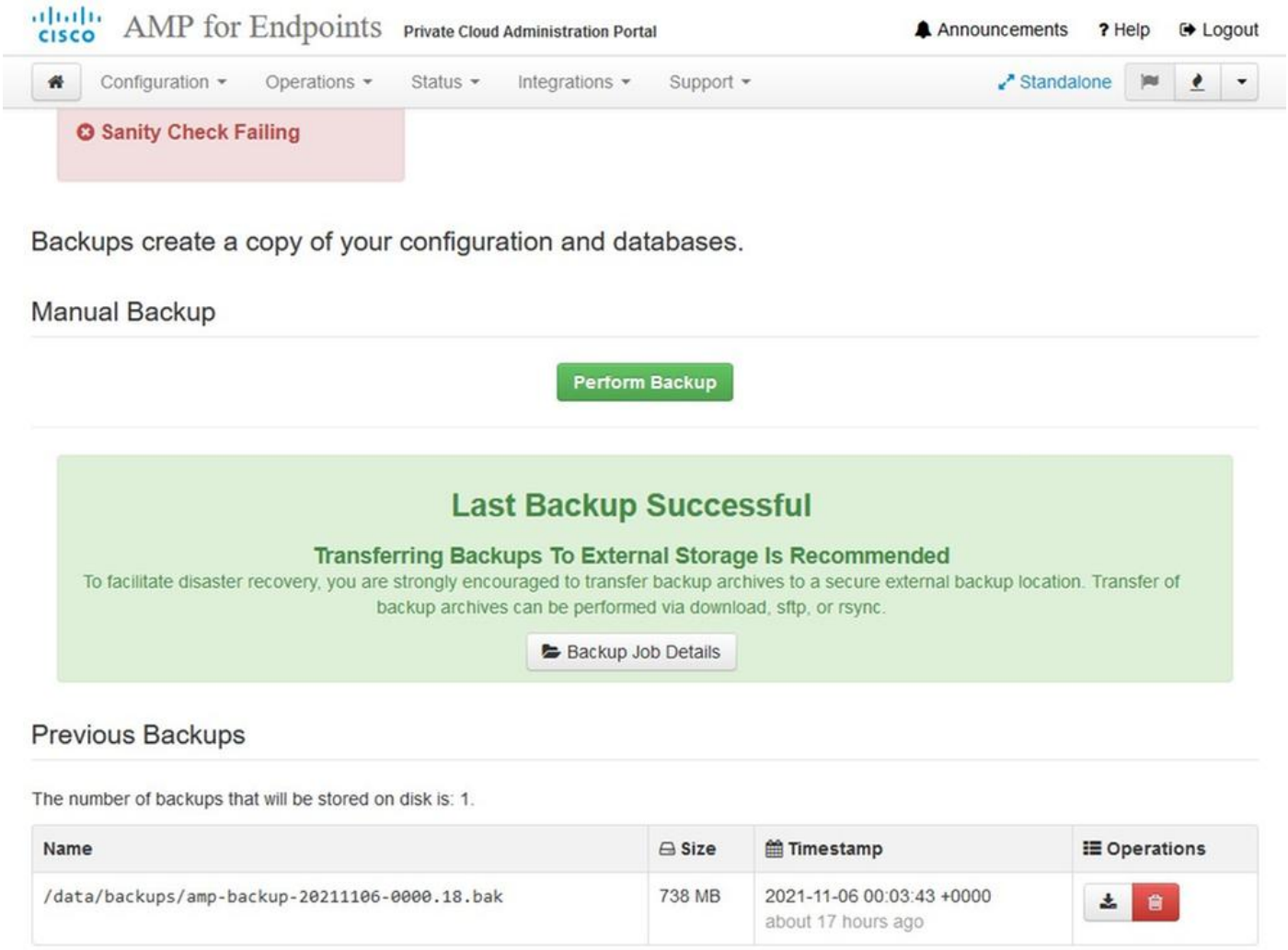


Effectuez la sauvegarde du VPC 3.2.0 actuel (dans ce cas) en mode d'entrefer.

Vous pouvez utiliser cette commande à partir de CLI

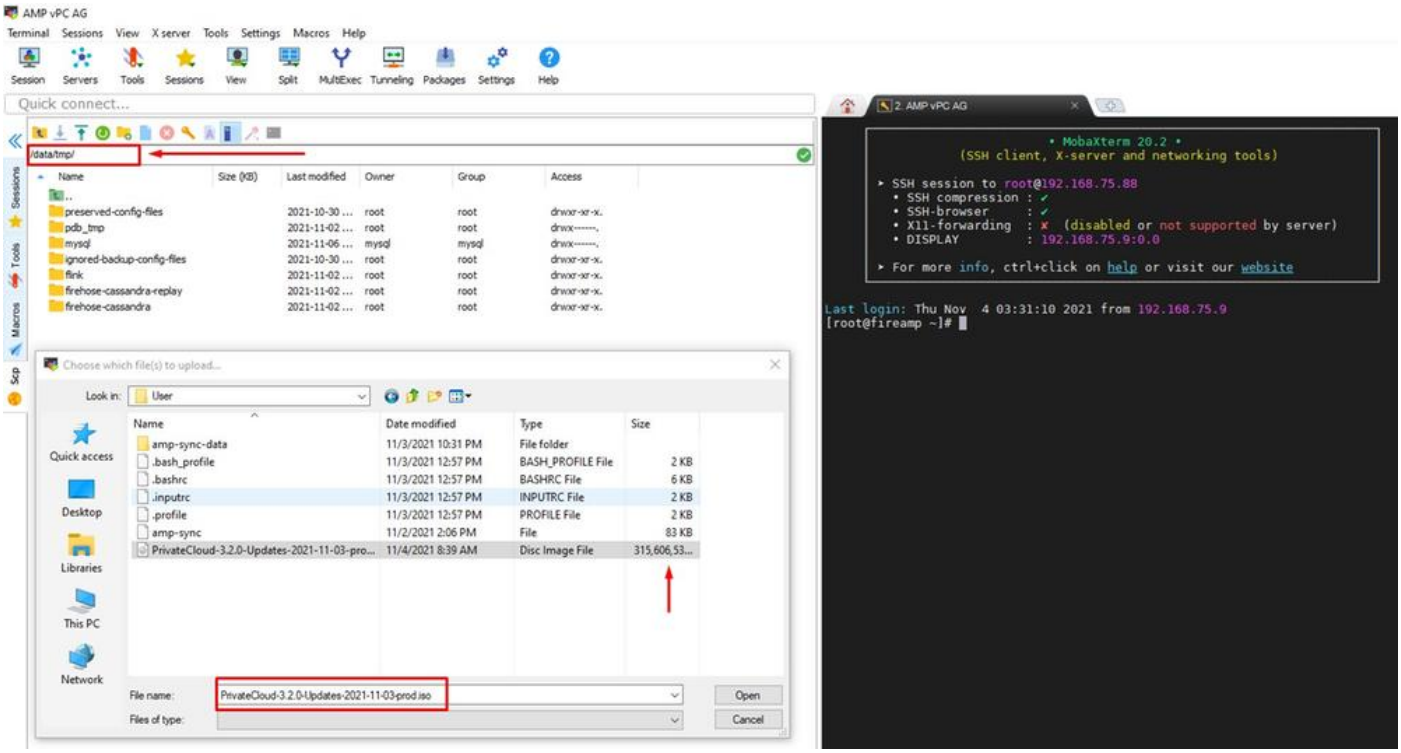
```
rpm -qa | grep Pri
```

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



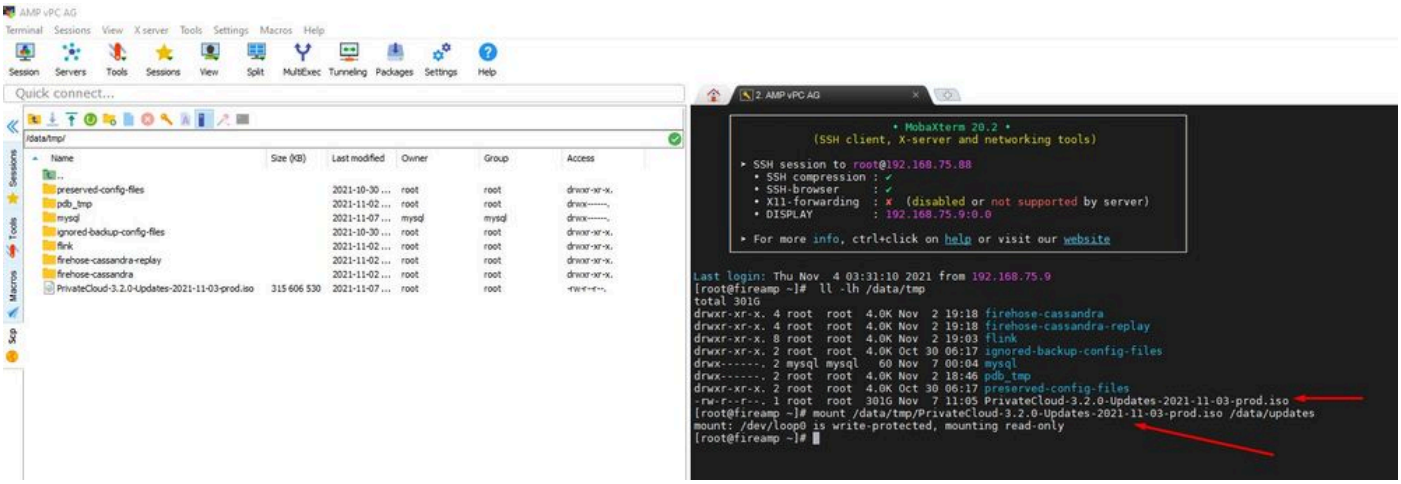
Transférez la dernière image ISO générée avec amp-sync vers le VPC. Cela peut prendre jusqu'à plusieurs heures en fonction de votre vitesse. Dans ce cas, le transfert a pris plus de 16 heures

```
/data/tmp
```



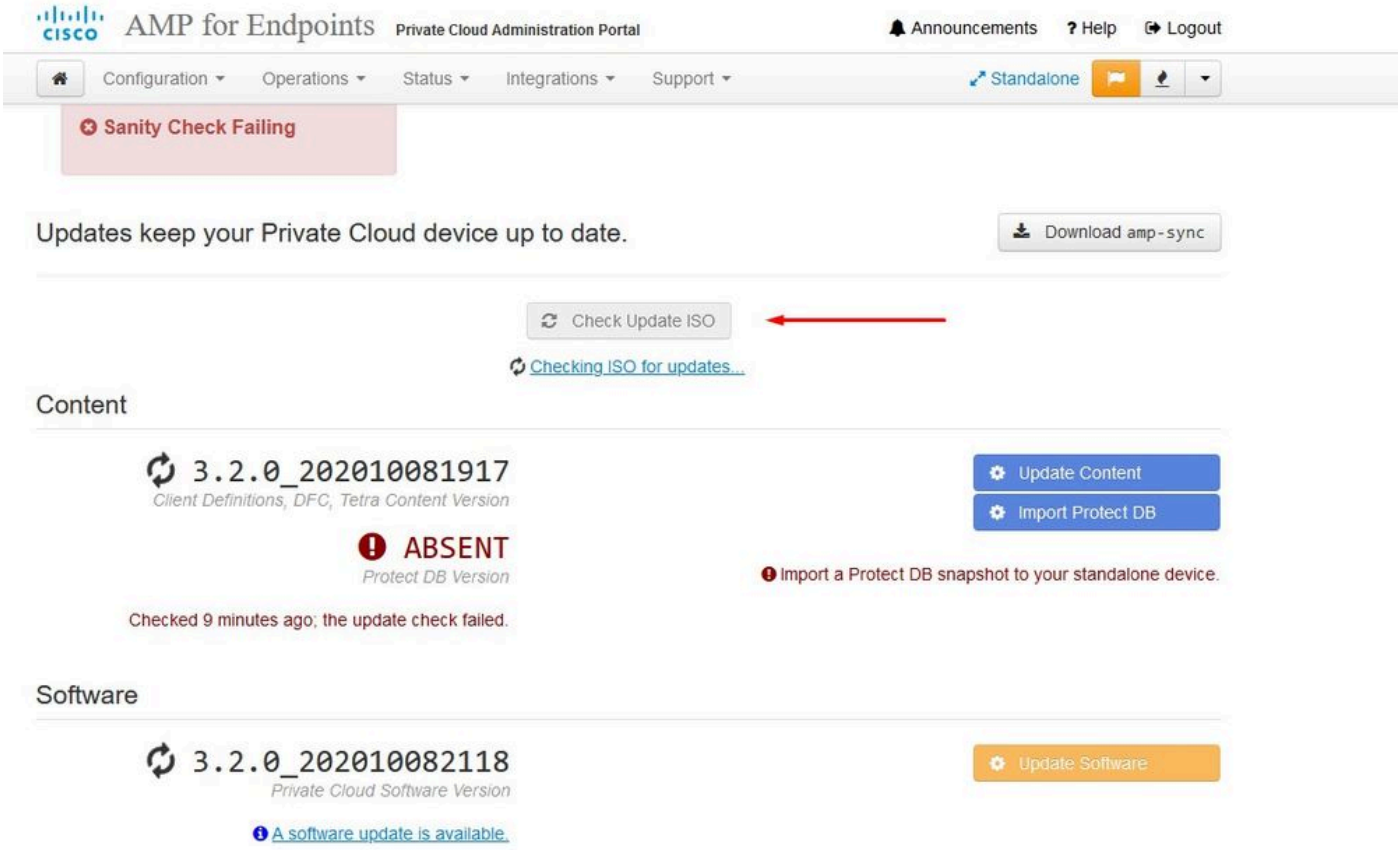
Une fois le téléchargement terminé, montez l'ISO

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

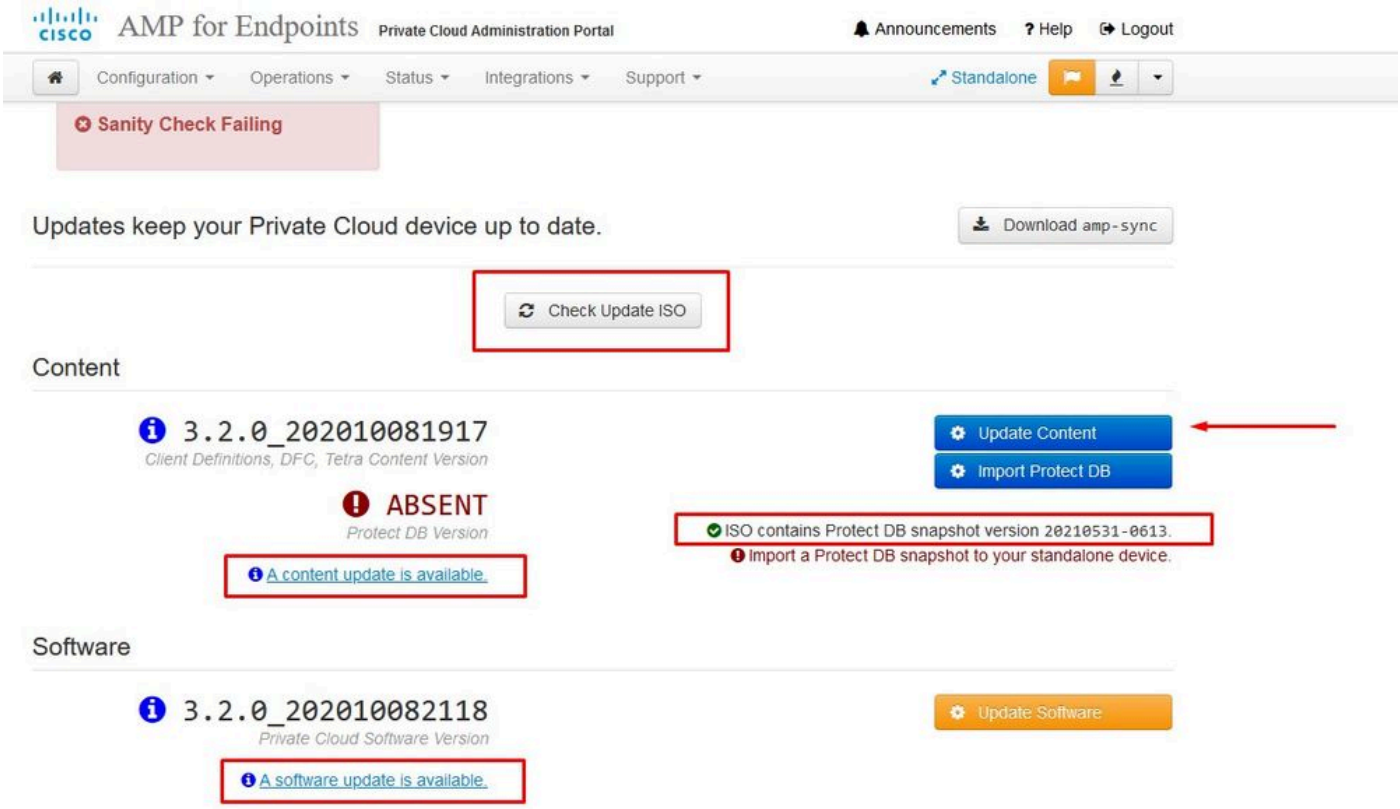


Accédez à opadin UI pour effectuer la mise à jour Operations > Update Device > Sélectionnez

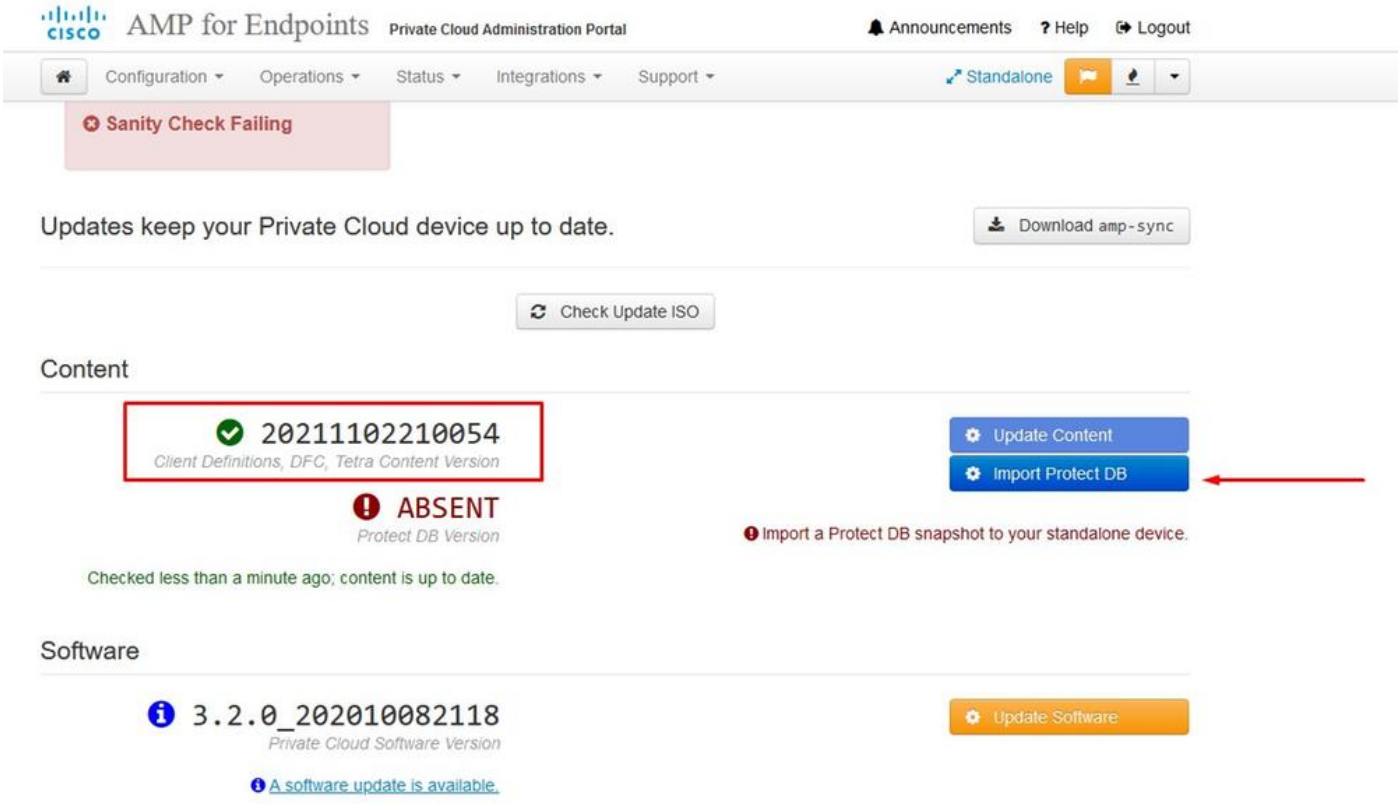
Check update ISO.



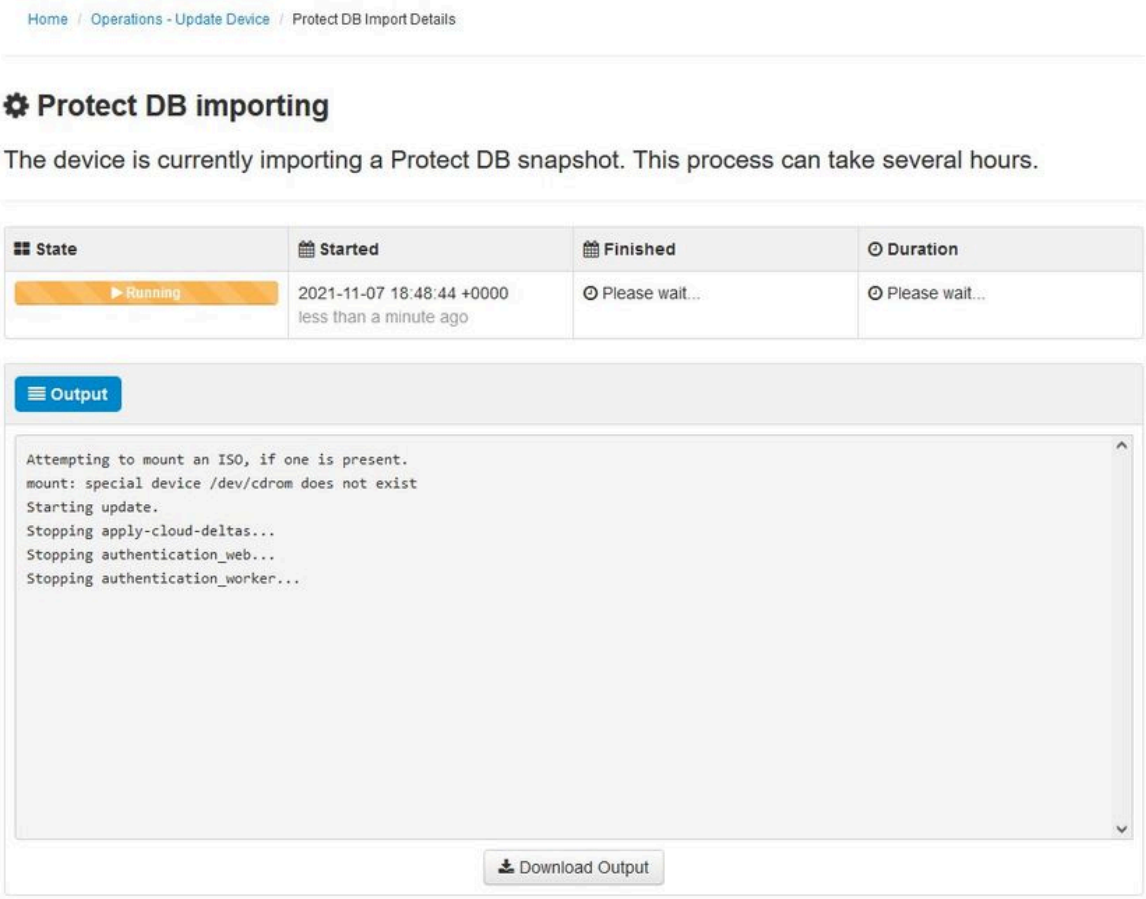
Dans cet exemple, je passe d'abord à la mise à jour du contenu



Sélectionnez ensuite Importer la base de données protégée.



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



Home / Operations - Update Device / Protect DB Import Details

Protect DB importing

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

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

Output

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

Download Output

Protect DB importing

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

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

Output

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

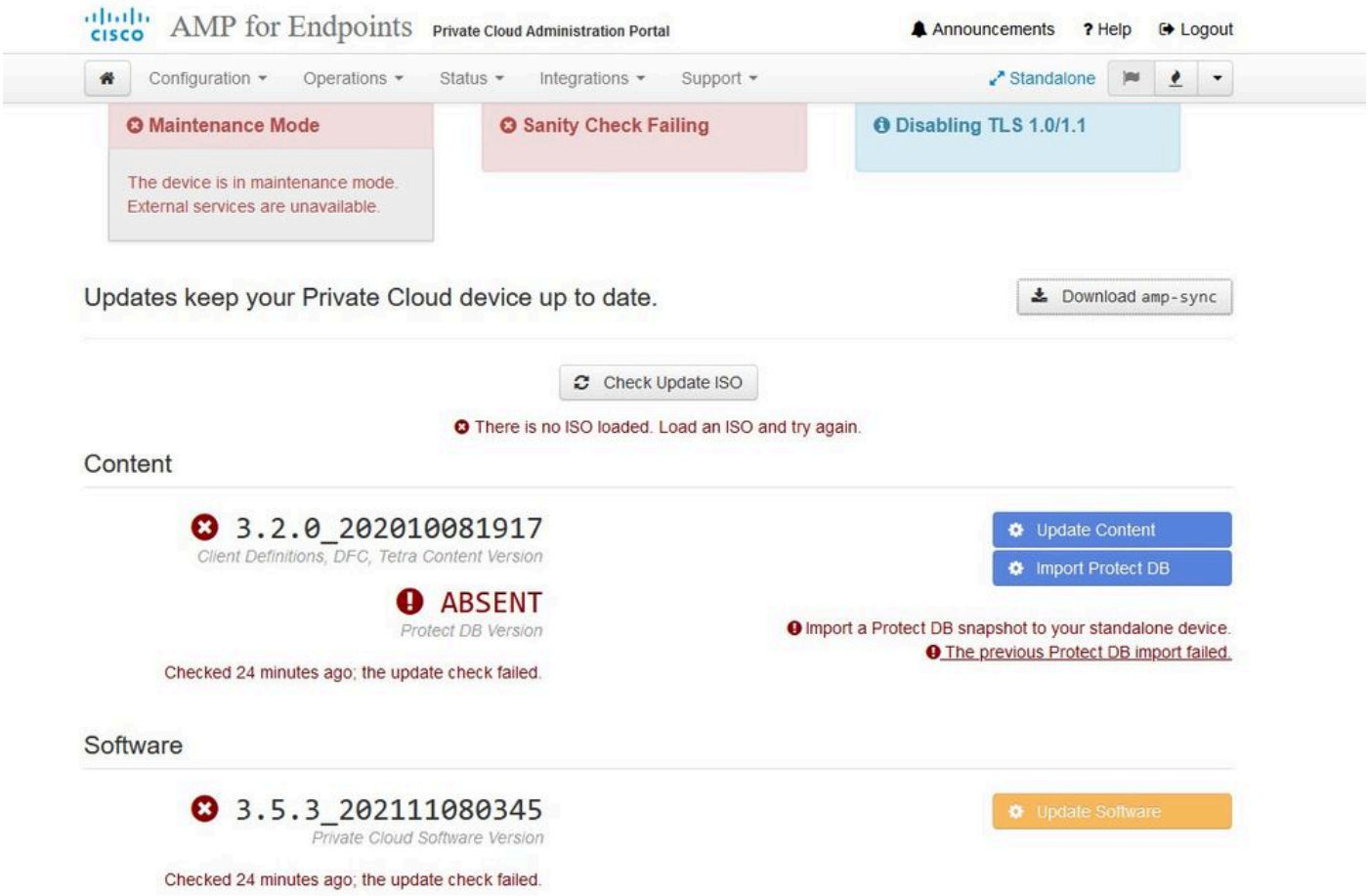
Ici, vous pouvez courir à deux questions. Puisque les vPC antérieurs à la version 3.5.2 n'ont pas la possibilité de monter un stockage NFS externe, vous devez télécharger le fichier ISO de mise à jour dans le répertoire /data/temp. Dans mon cas, comme mon datastore ne comptait que 1 To, je suis sorti 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

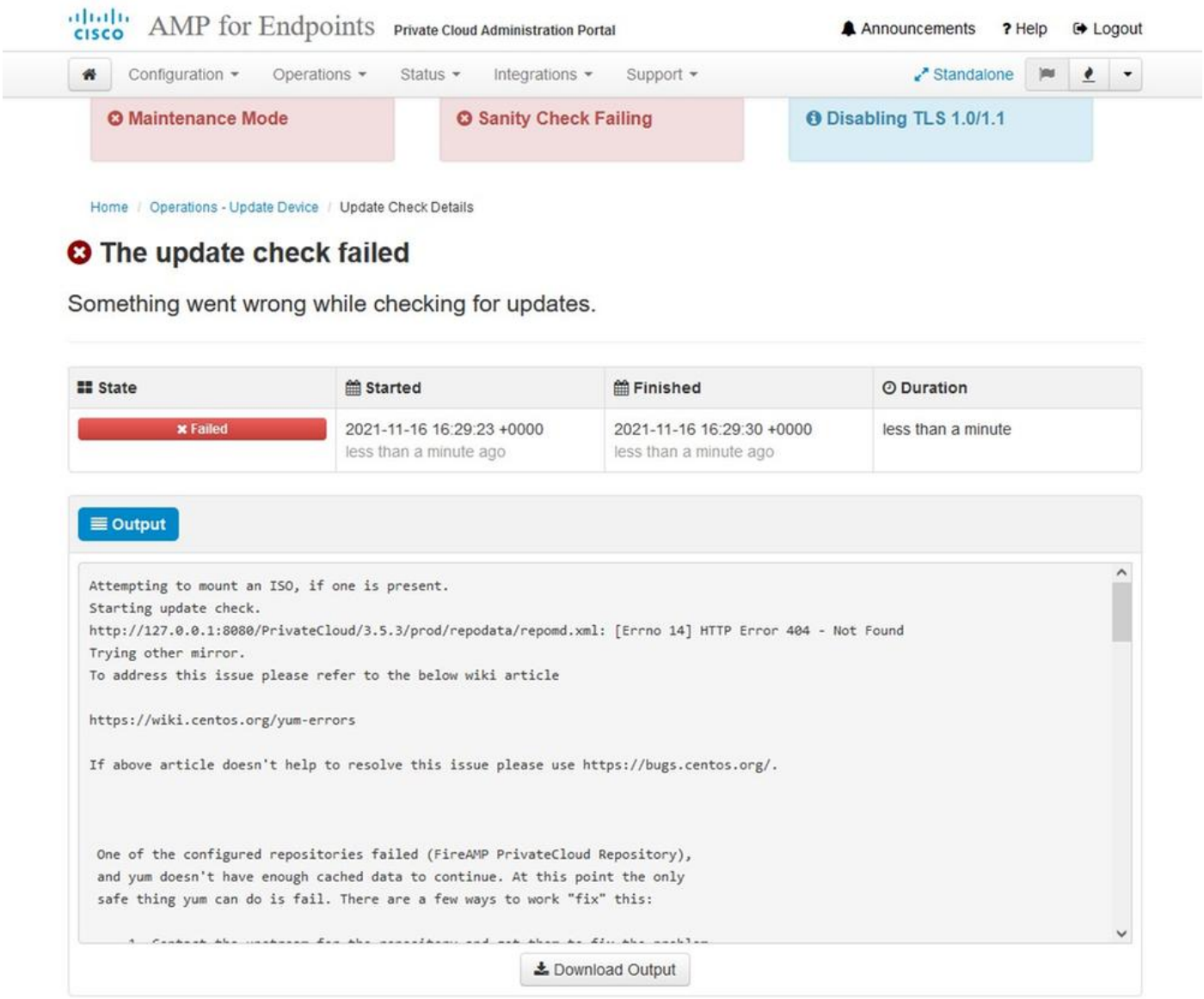


Problème #2 - Ancienne mise à jour

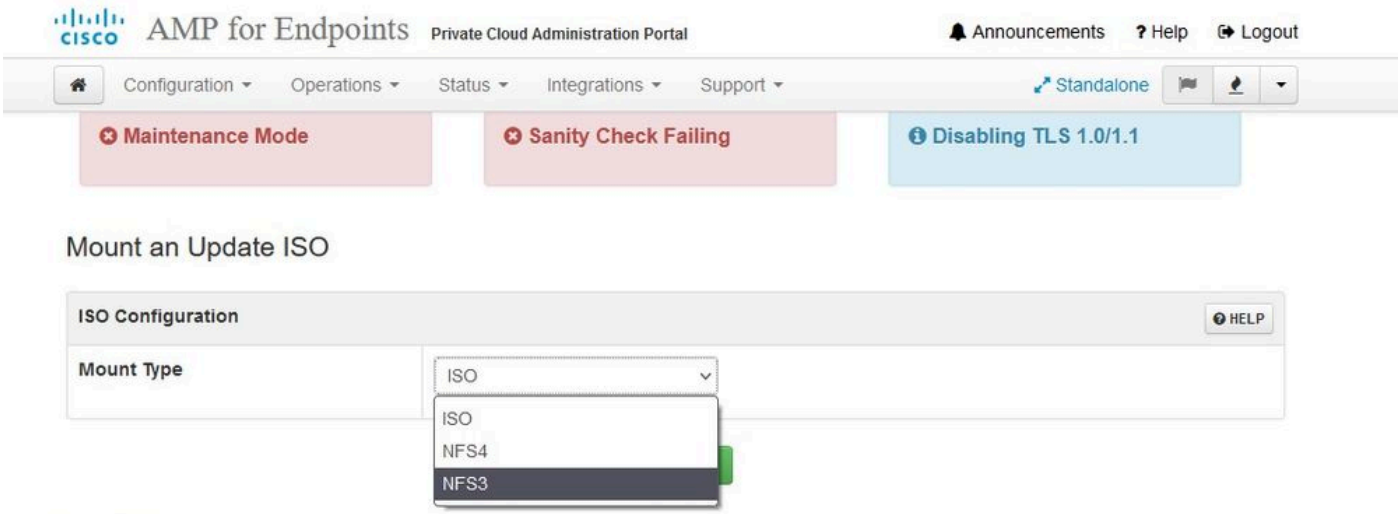
Le 2e problème est que si vous exécutez la mise à jour logicielle d'abord comme je l'ai fait dans mon 2e essai et à partir de 3.2.0 je me retrouve avec VPC pour mettre à niveau vers 3.5.2 et à cause de cela, j'ai dû télécharger un nouveau fichier de mise à jour ISO depuis la 3.2.0 est devenu invalide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

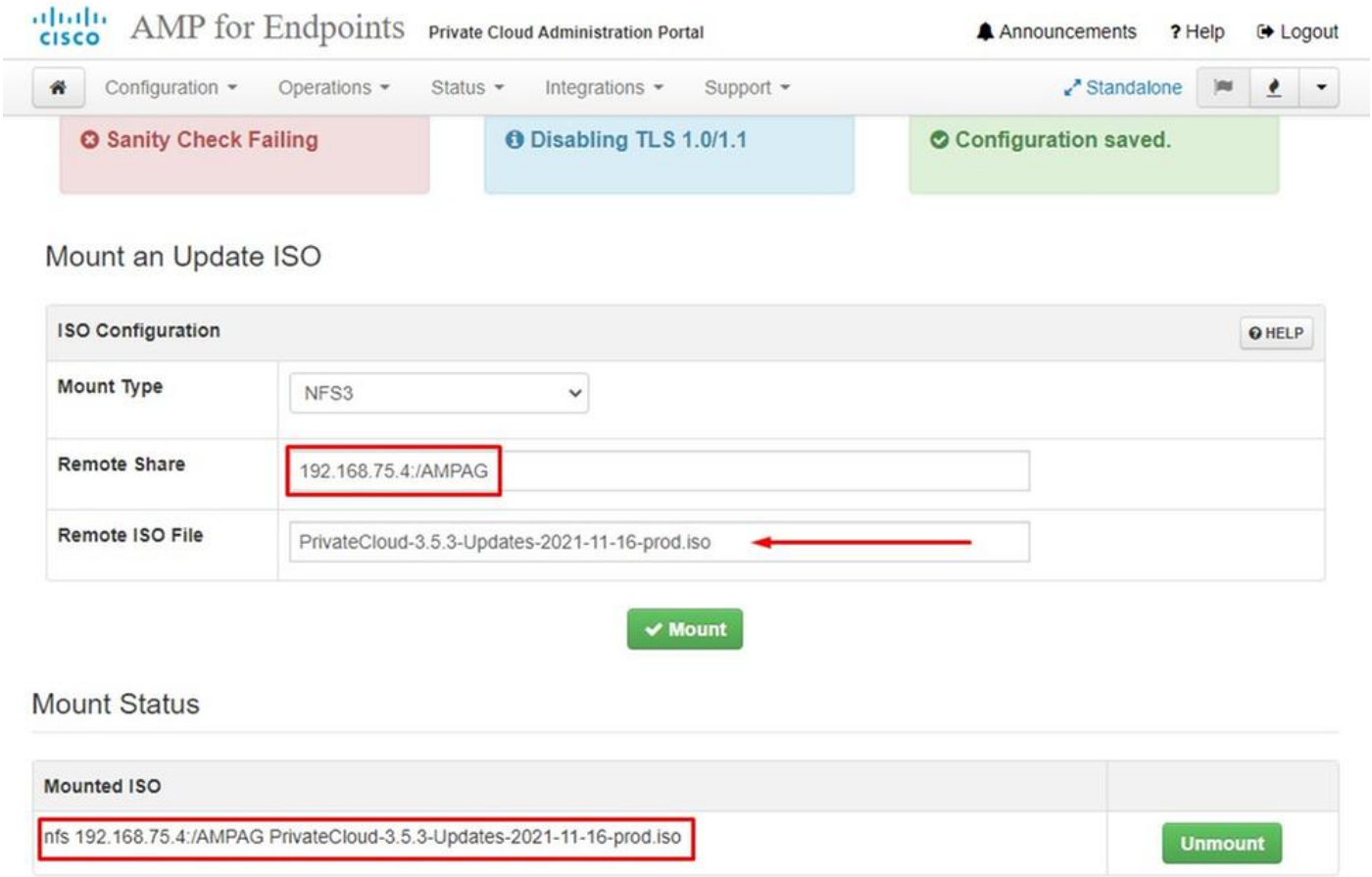


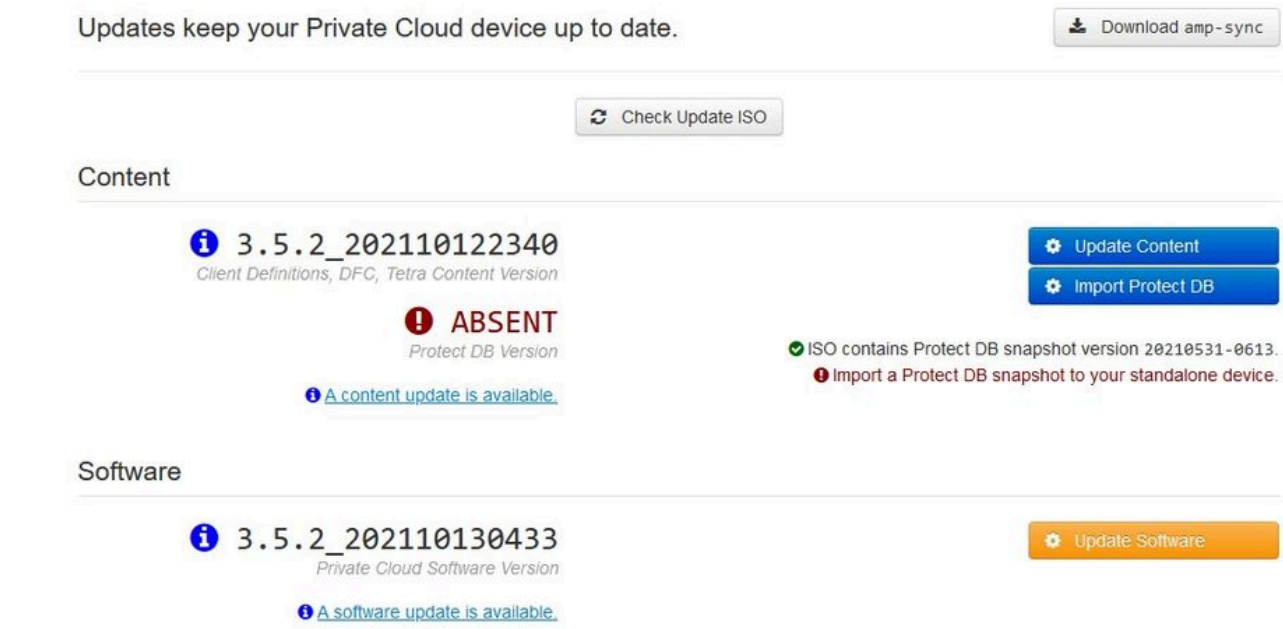
Il s'agit de l'erreur que vous voyez si vous essayez de monter à nouveau le fichier de mise à jour ISO.



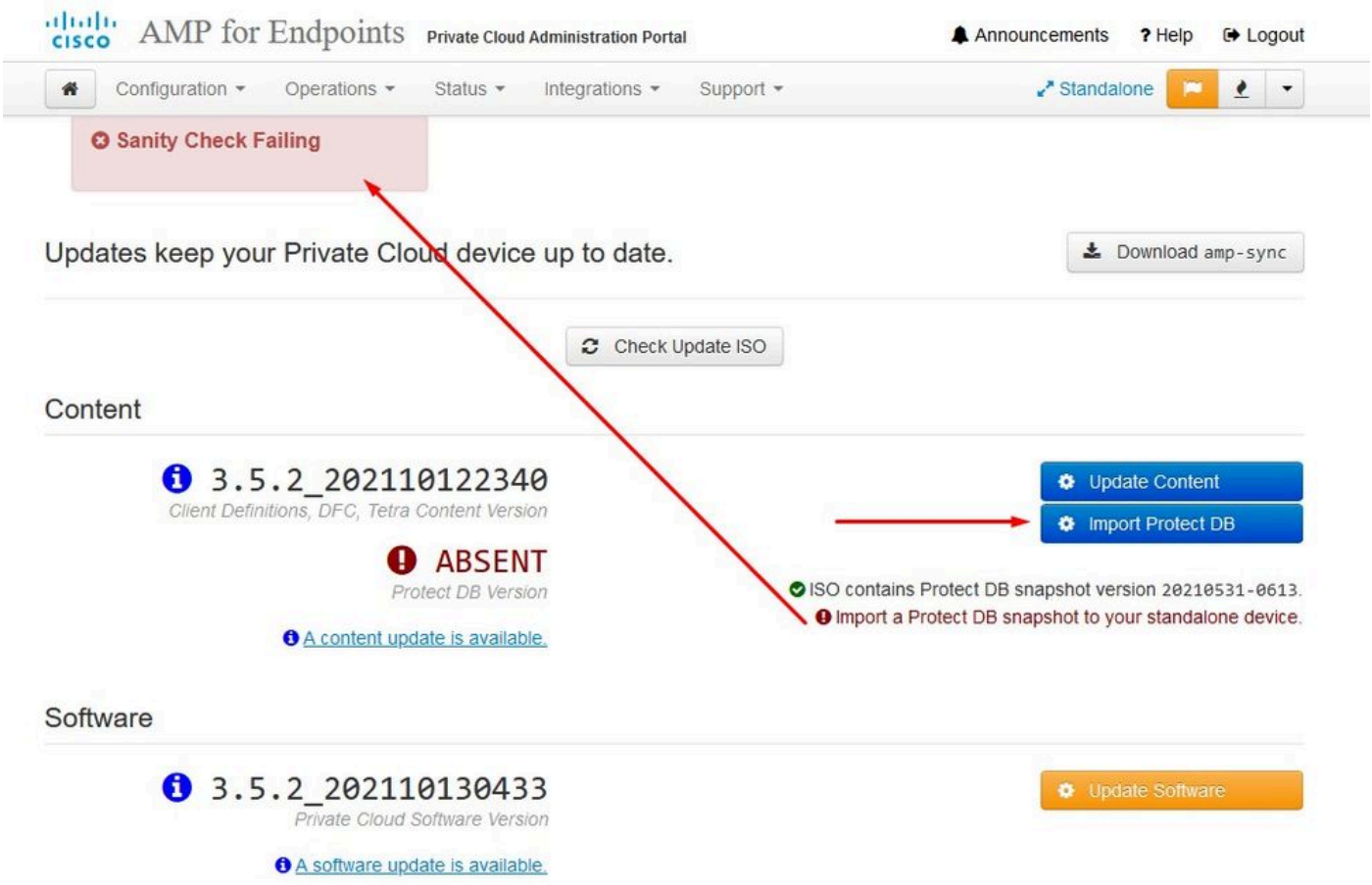
Cette image montre une autre façon de monter une image de mise à jour sur votre VPC. Dans la version 3.5.x, vous pouvez utiliser un emplacement distant tel que le stockage NFS pour partager le fichier de mise à jour avec votre VPC.


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
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


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
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



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



Protect DB importing

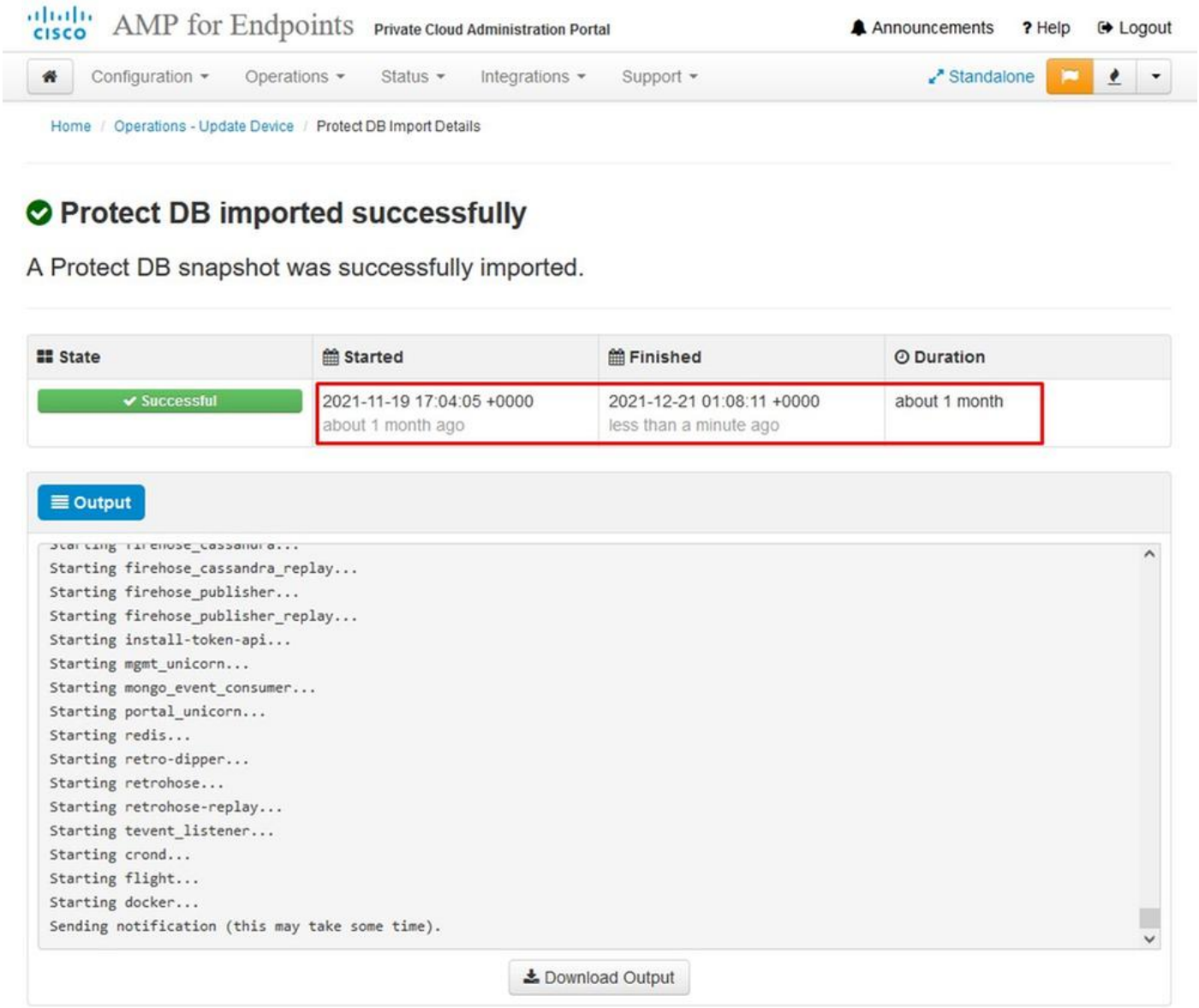
The device is currently importing a Protect DB snapshot. This process can take several hours.

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

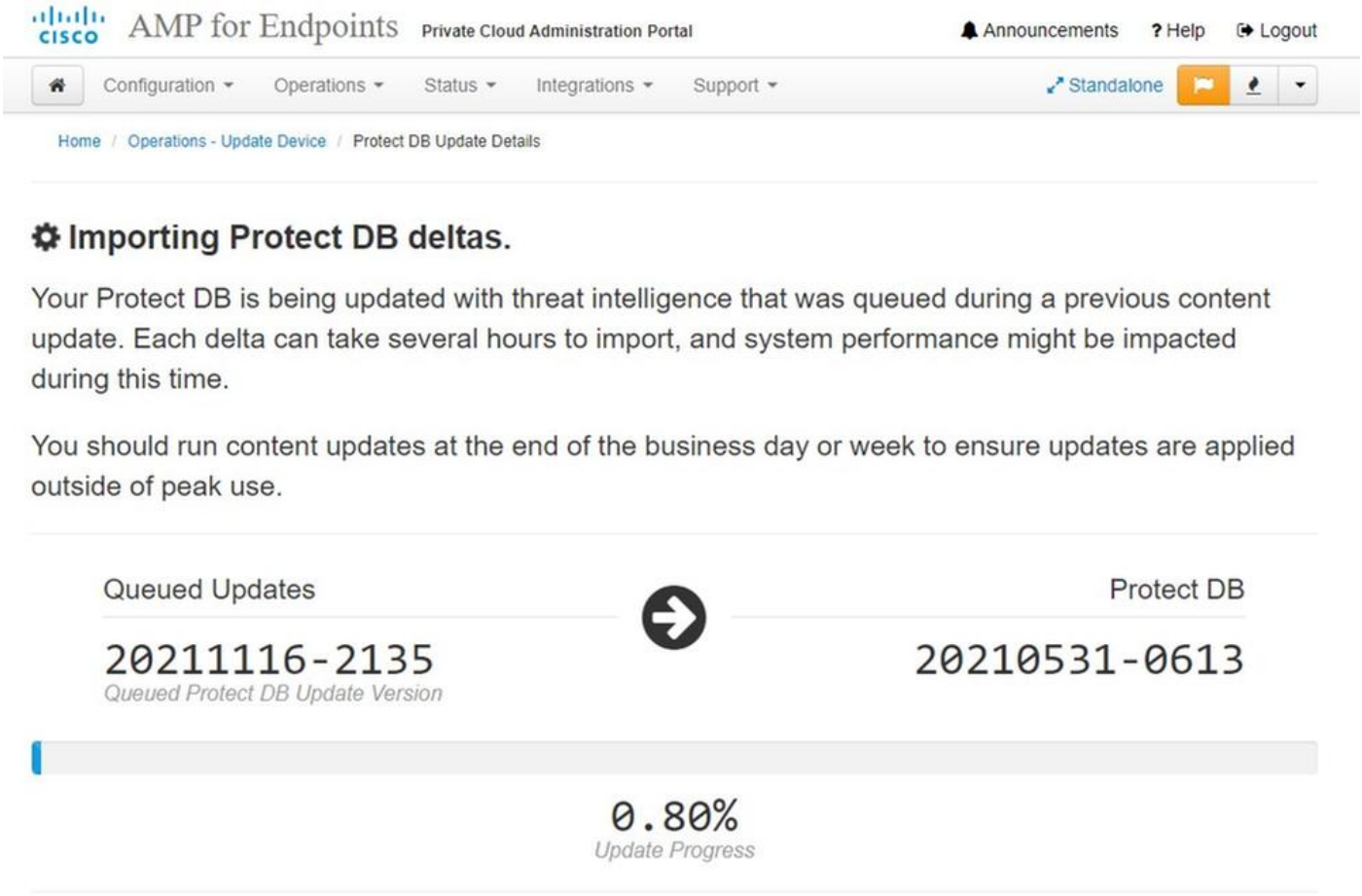
Output

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

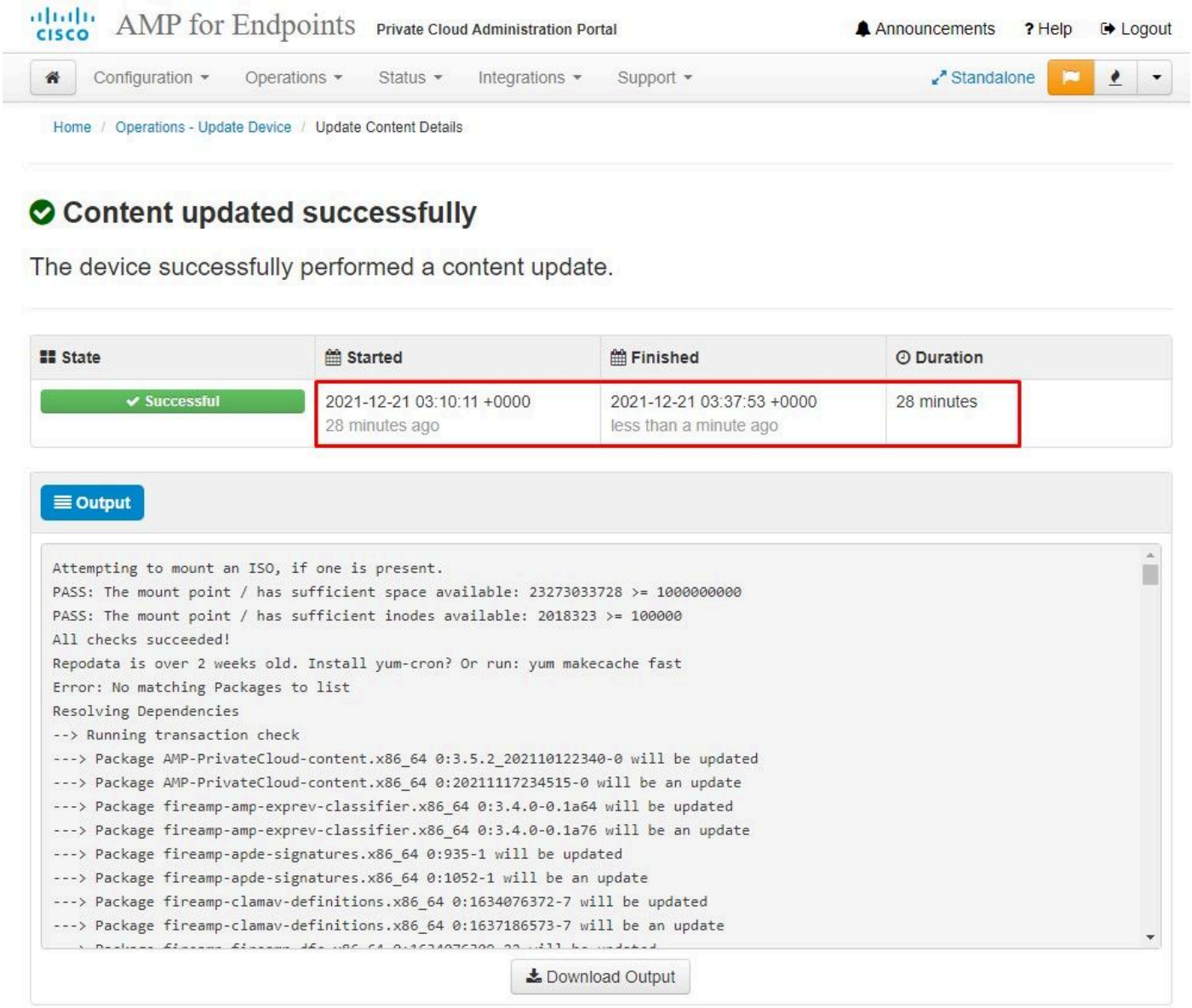
Download Output



La prochaine mise à jour démarre automatiquement



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.



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.

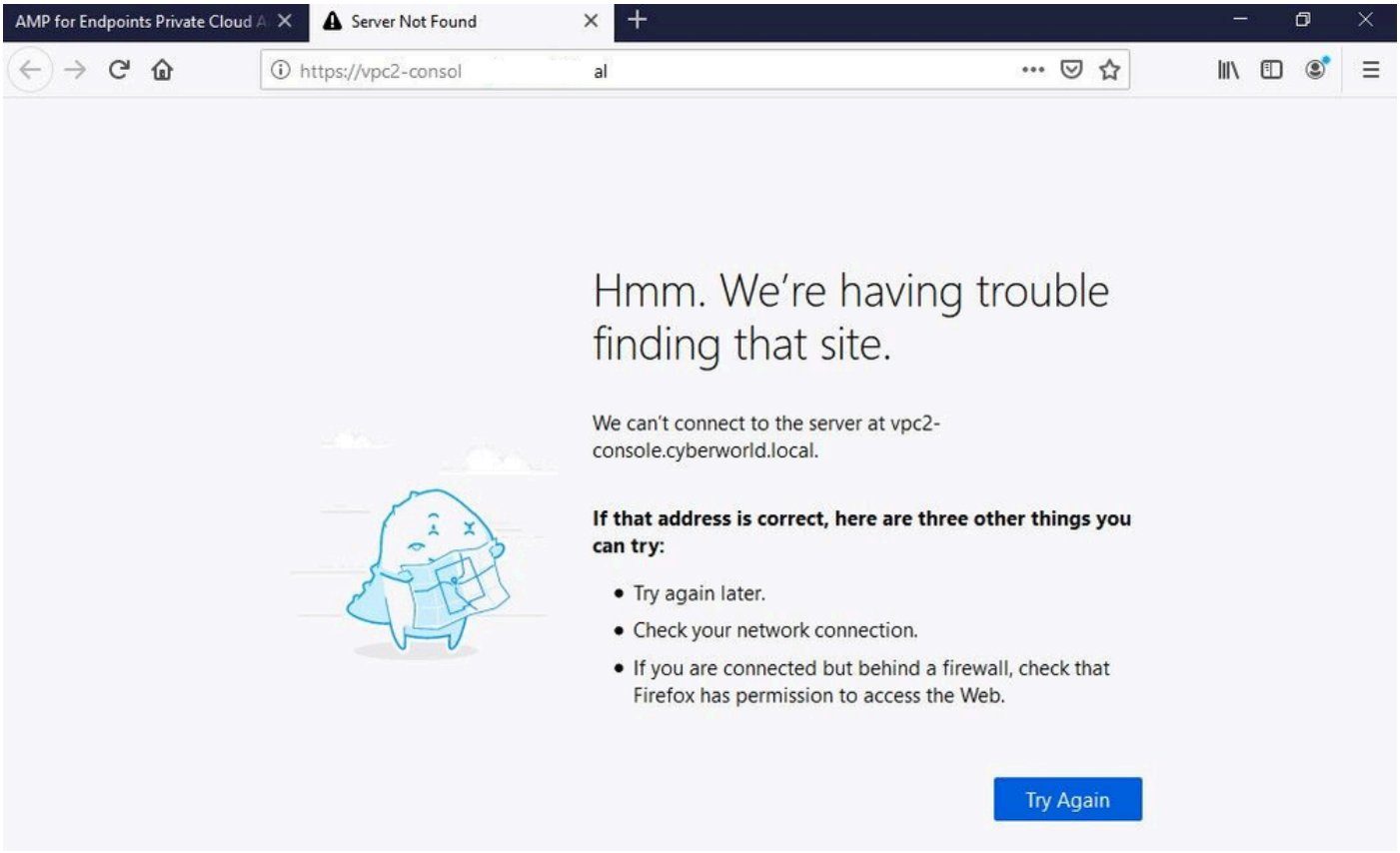
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

⩓ ⩓ AIRGAP UNIQUEMENT ⩓ ⩓

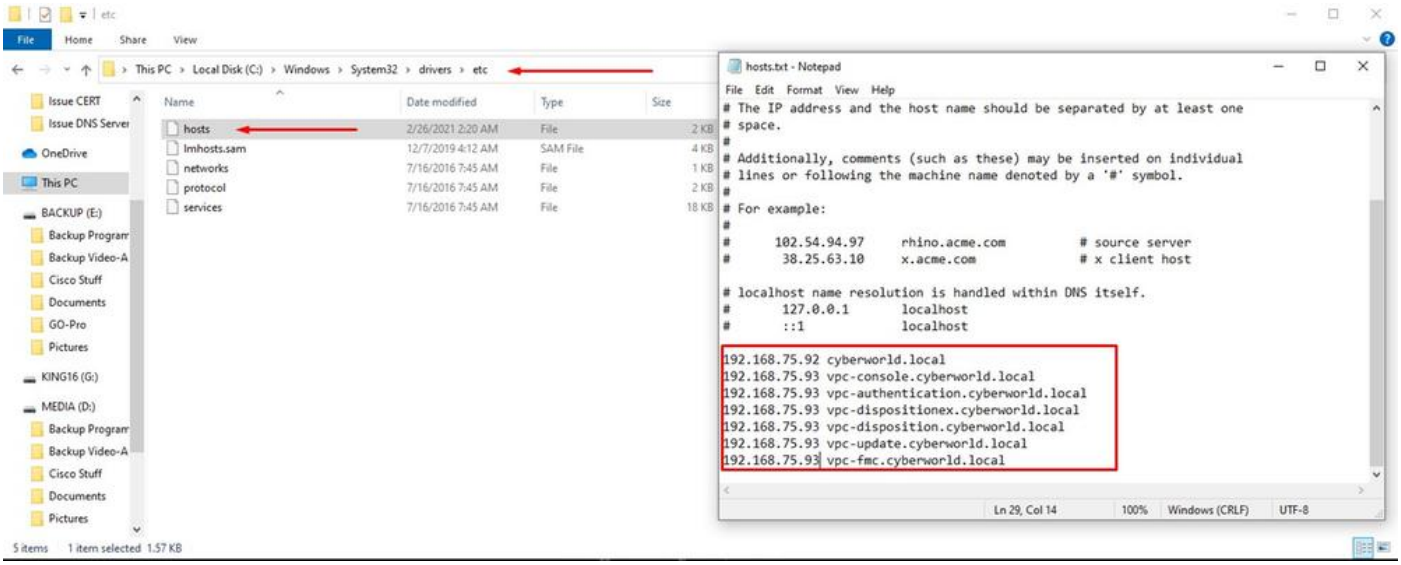
Dépannage de base

Problème #1 - FQDN et serveur DNS

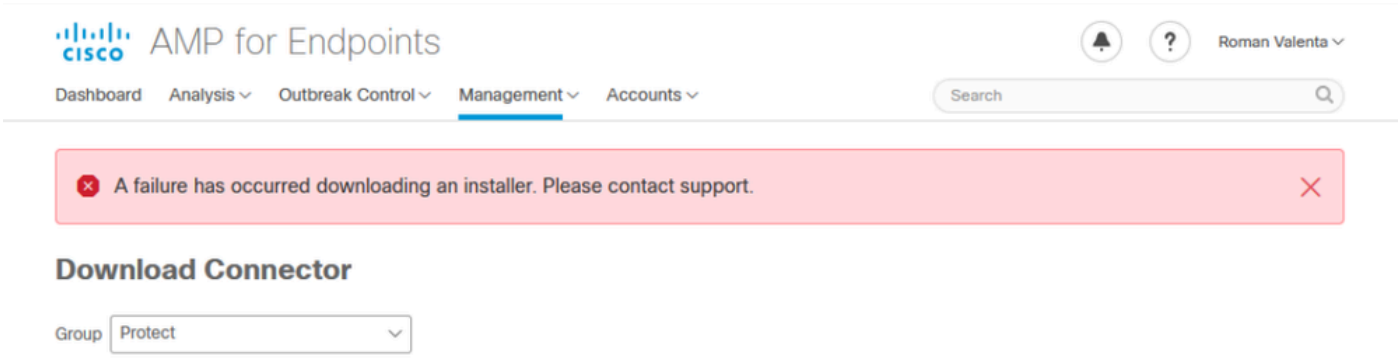
Le premier problème que vous pouvez rencontrer est si votre serveur DNS n'est pas établi et que tous les FQDN ne sont pas correctement enregistrés et résolus. Le problème peut ressembler à ceci lorsque vous essayez d'accéder à la console Secure Endpoint via l'icône « Fire » de Secure Endpoint. Si vous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

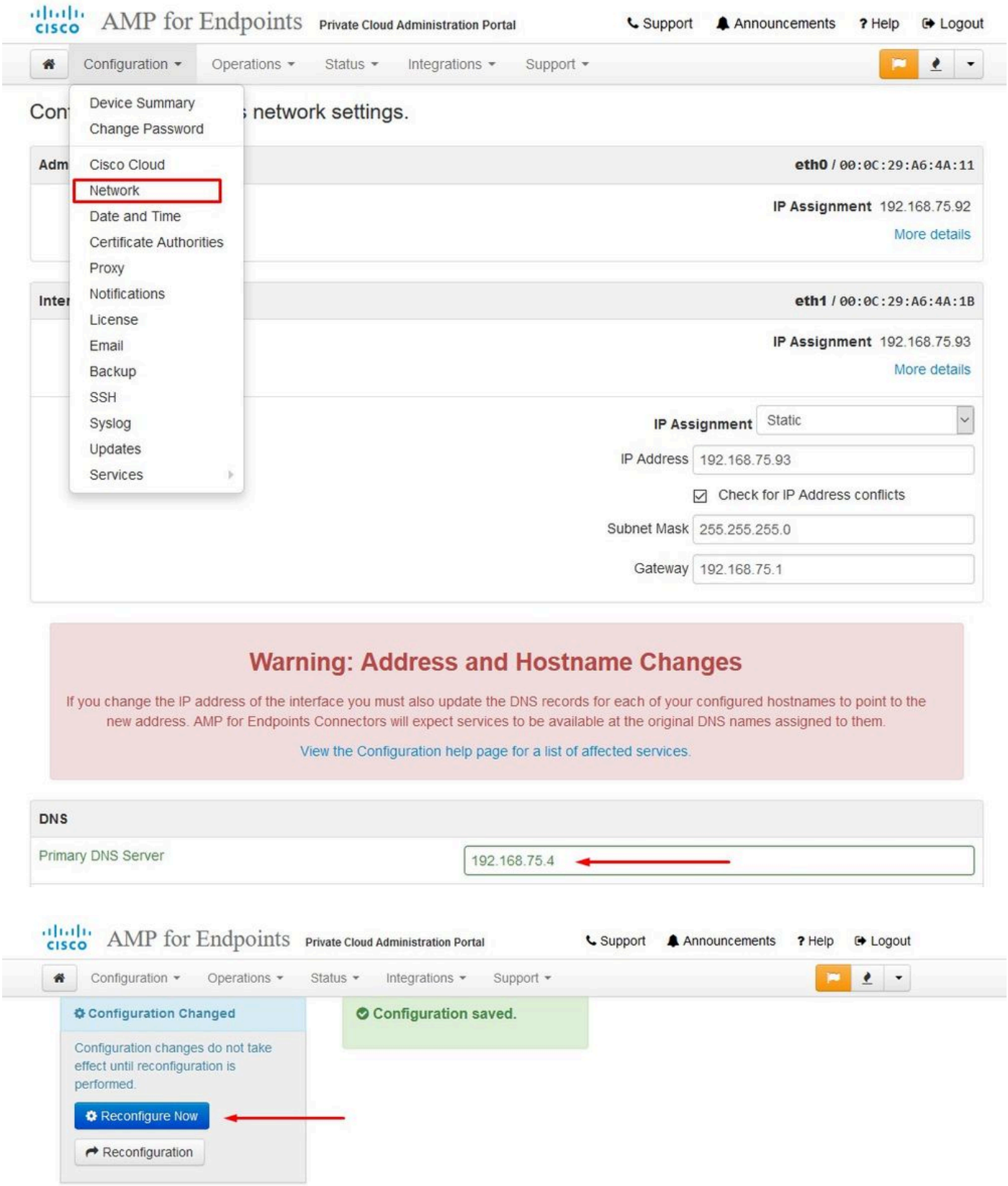
```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0

================================================================================

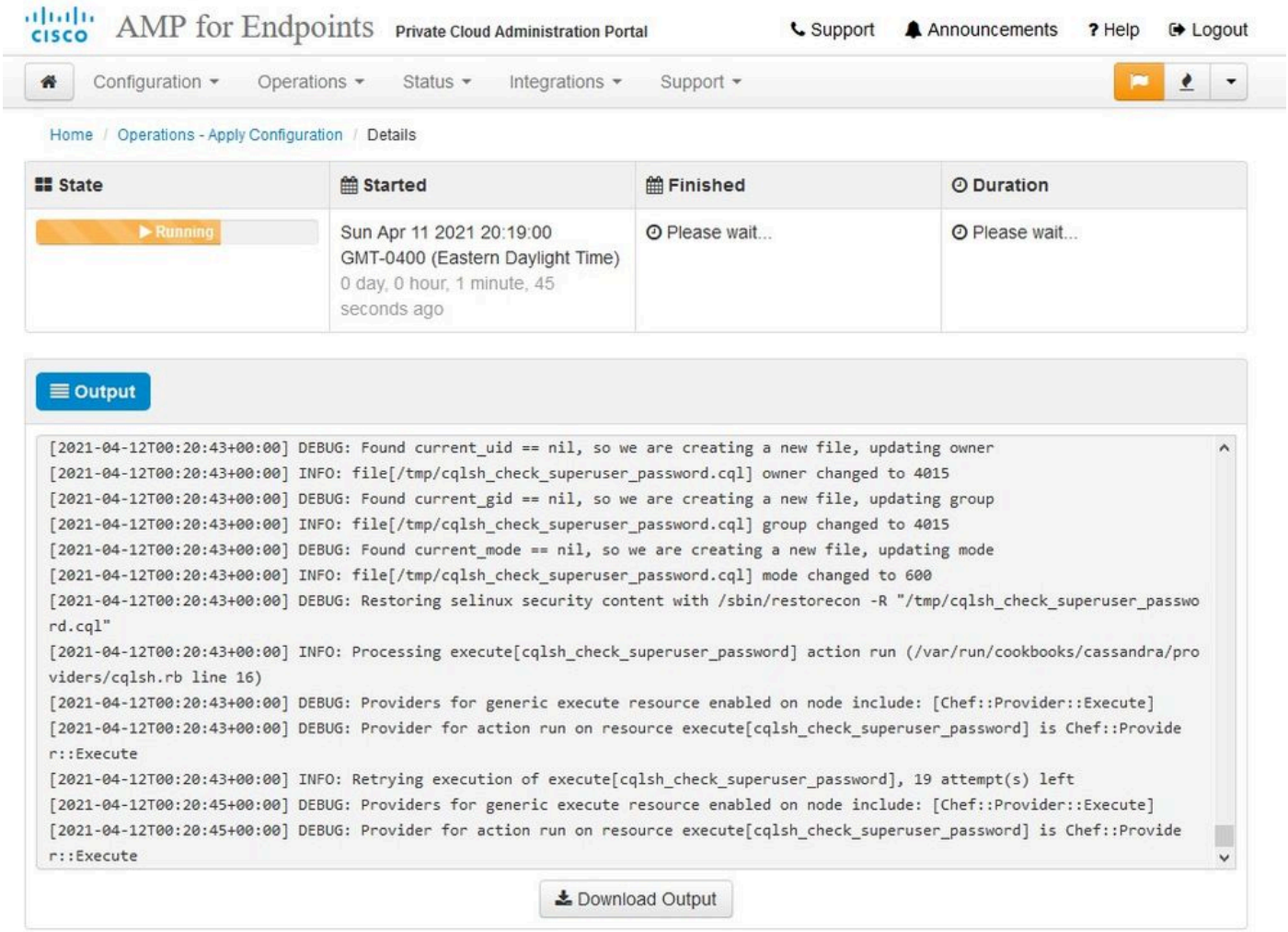
Server:         8.8.8.x
Address:        8.8.8.x#53

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

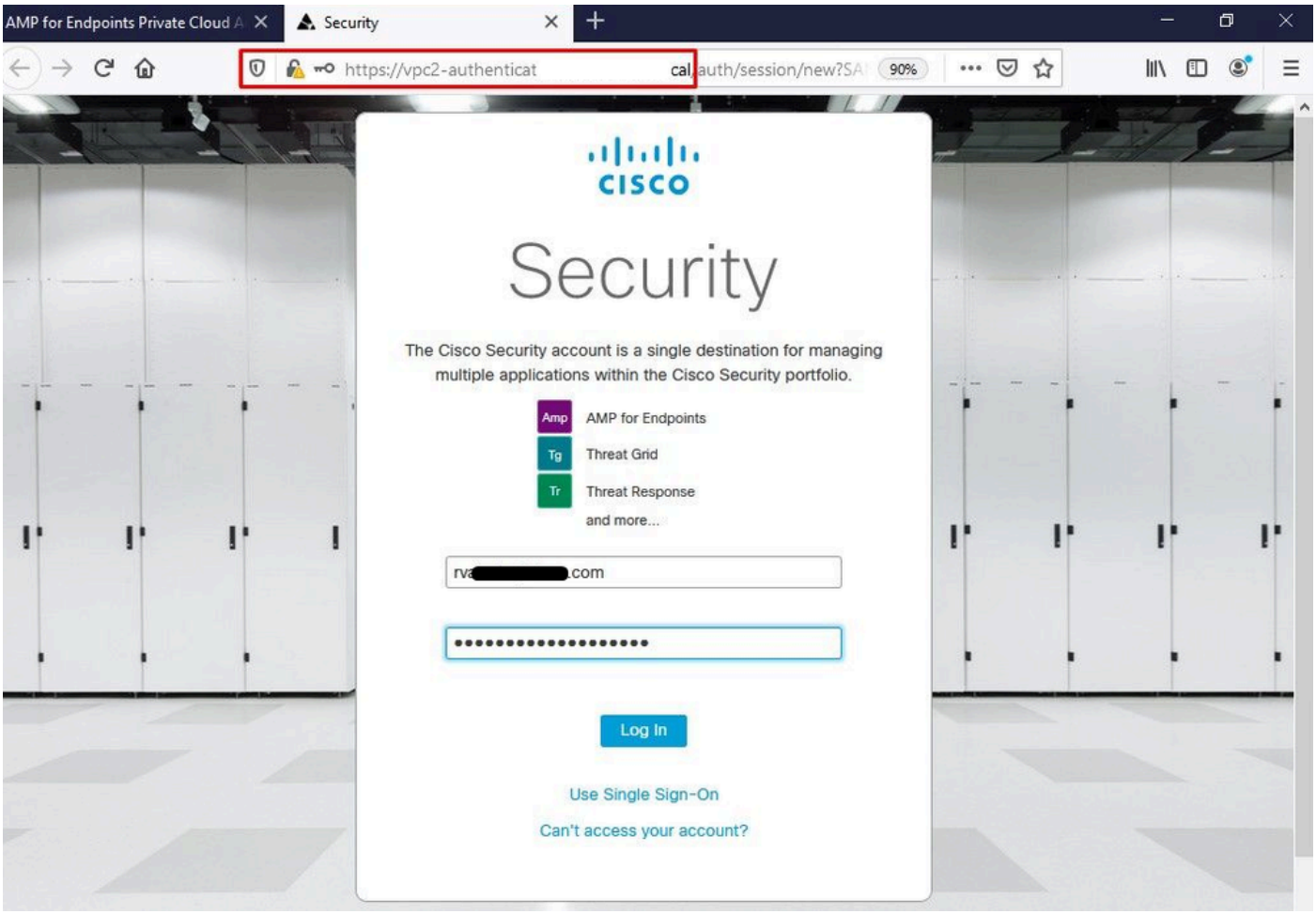
Une fois que vous avez enregistré tous les FQDN sur votre serveur DNS et que vous avez modifié l'enregistrement dans le cloud privé virtuel de DNS public à votre serveur DNS, tout commence à fonctionner comme prévu.


AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Device Summary
Change Password
Cisco Cloud
Network
Date and Time
Certificate Authorities
Proxy
Notifications
License
Email
Backup
SSH
Syslog
Updates
Services
network settings.
eth0 / 00:0C:29:A6:4A:11
IP Assignment 192.168.75.92
More details
eth1 / 00:0C:29:A6:4A:1B
IP Assignment 192.168.75.93
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
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

AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Configuration Changed
Configuration changes do not take effect until reconfiguration is performed.
Reconfigure Now
Reconfiguration
Configuration saved.

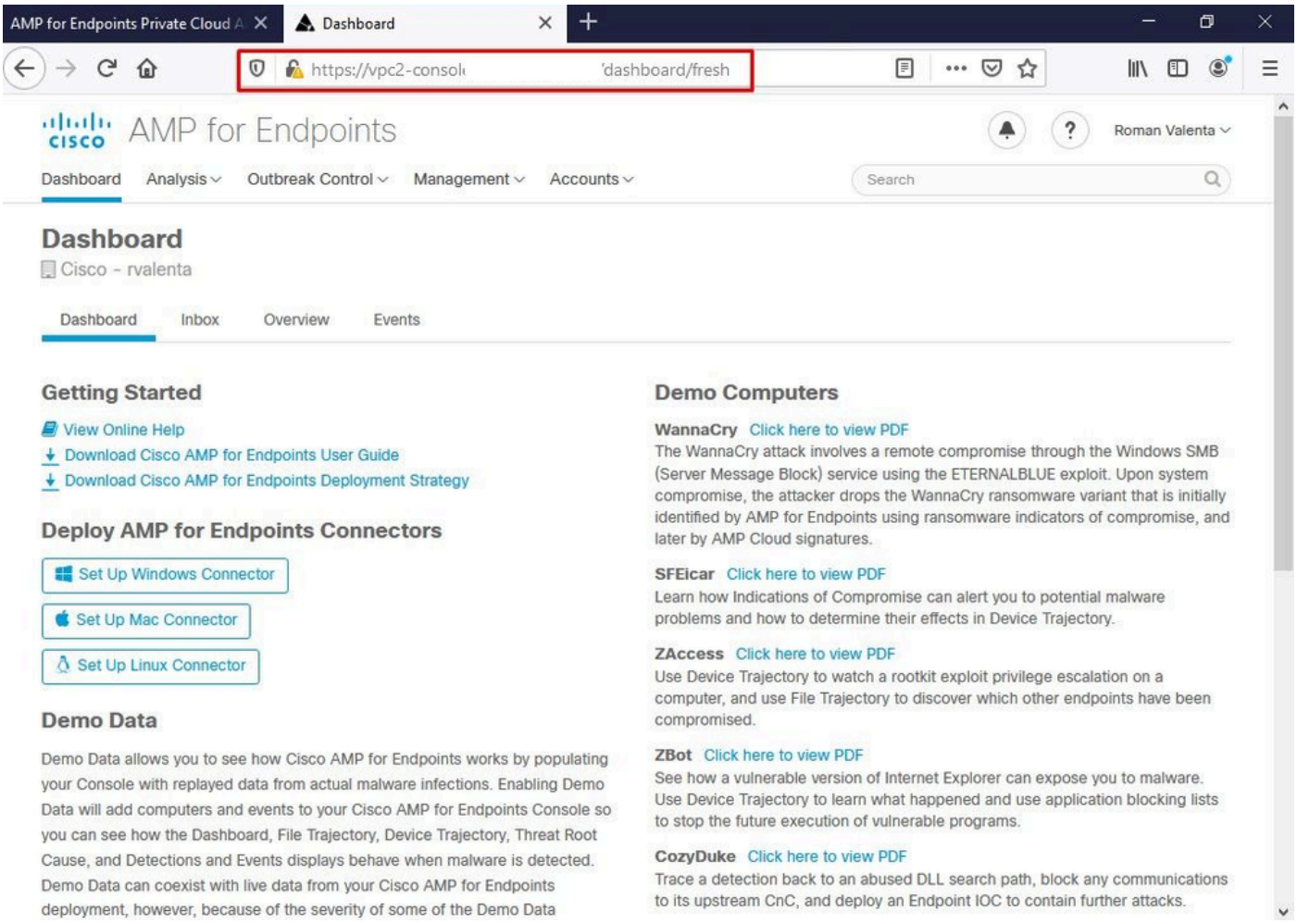


À ce stade, vous pouvez vous connecter et télécharger le connecteur

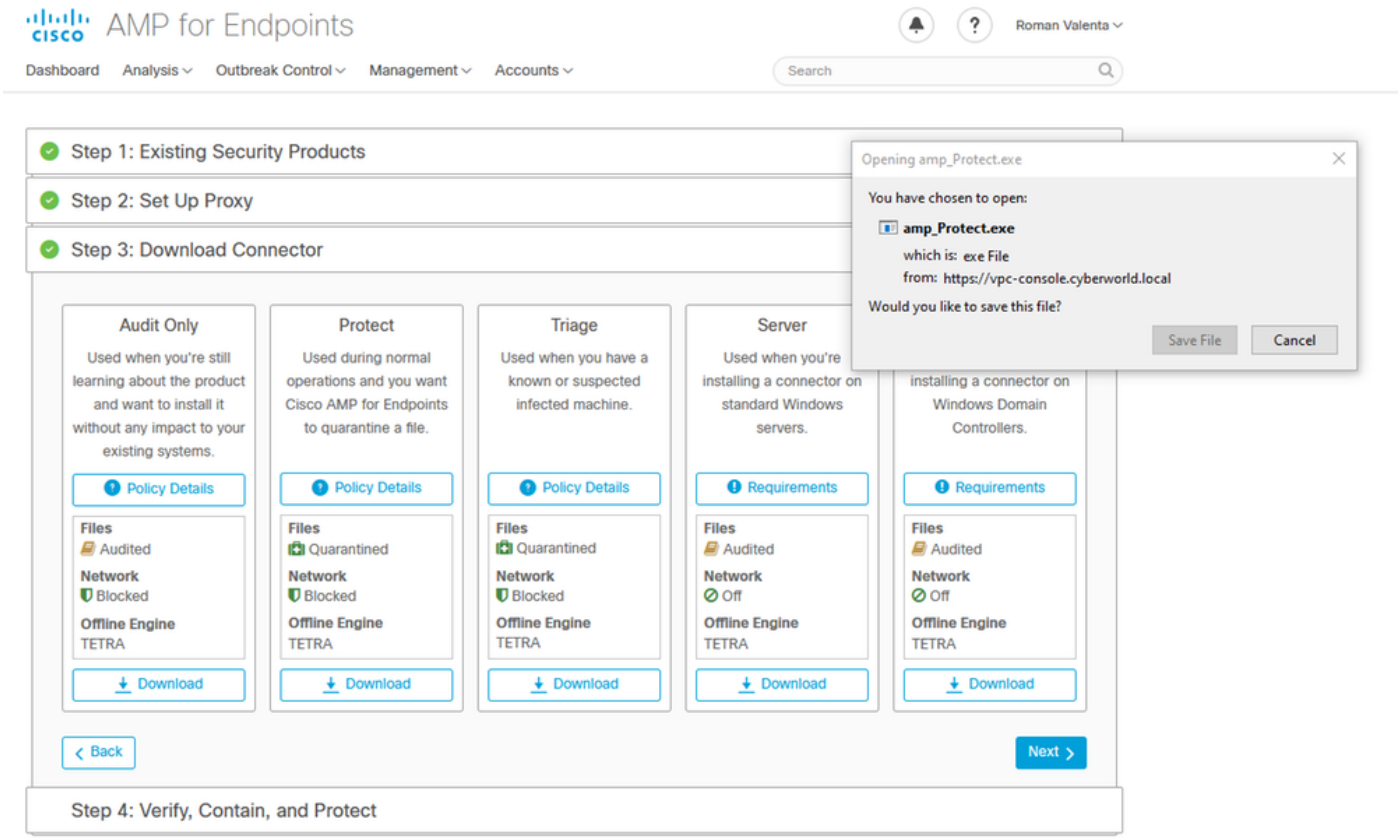


Vous obtenez l'assistant de stratégie de point de terminaison sécurisé initial pour votre environnement. Il vous guide tout au long de la sélection du produit antivirus que vous utilisez, le cas échéant, ainsi que du proxy , et des types de stratégies que vous souhaitez déployer. Sélectionnez le bouton 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.

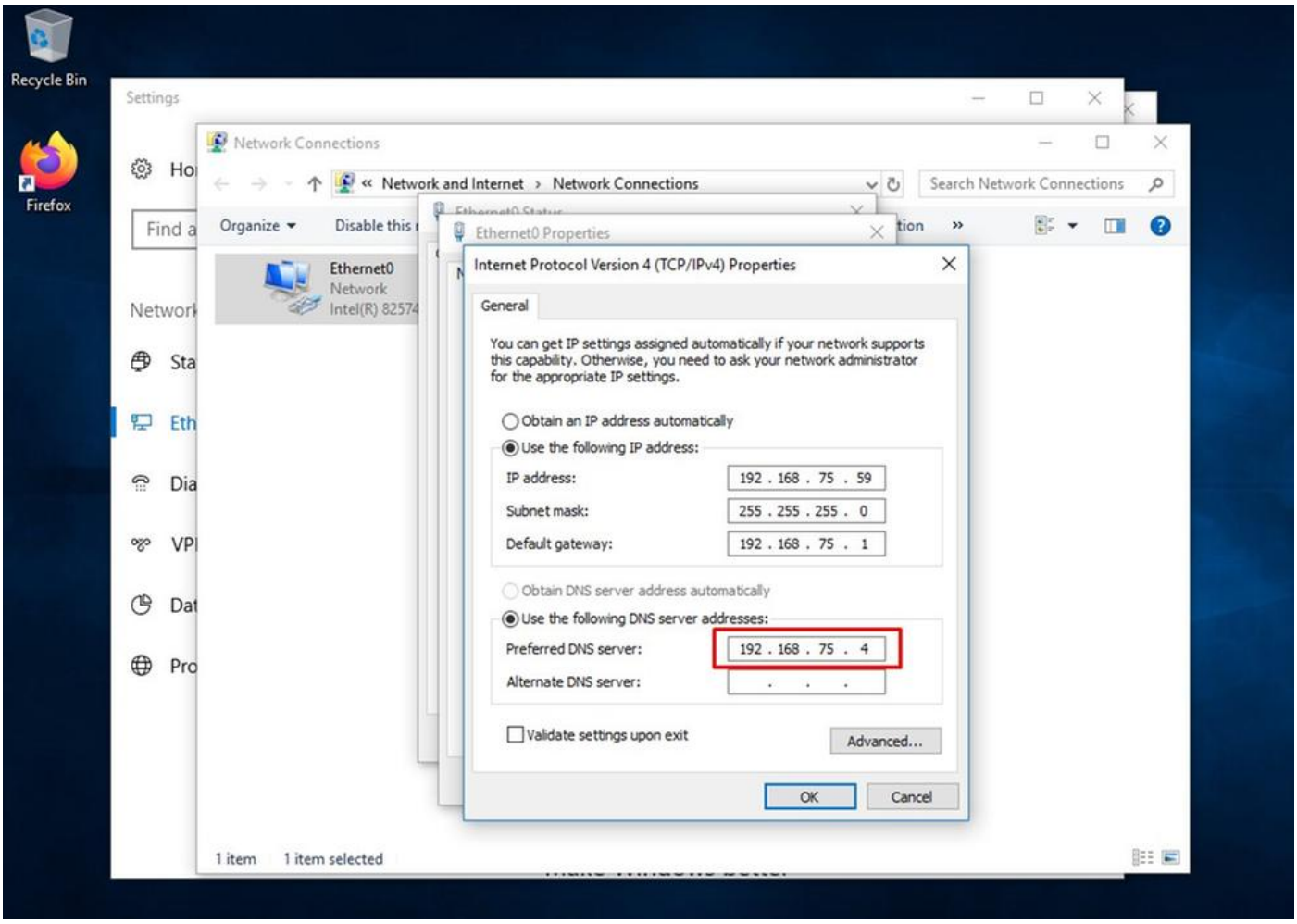


Connecteur de téléchargement.

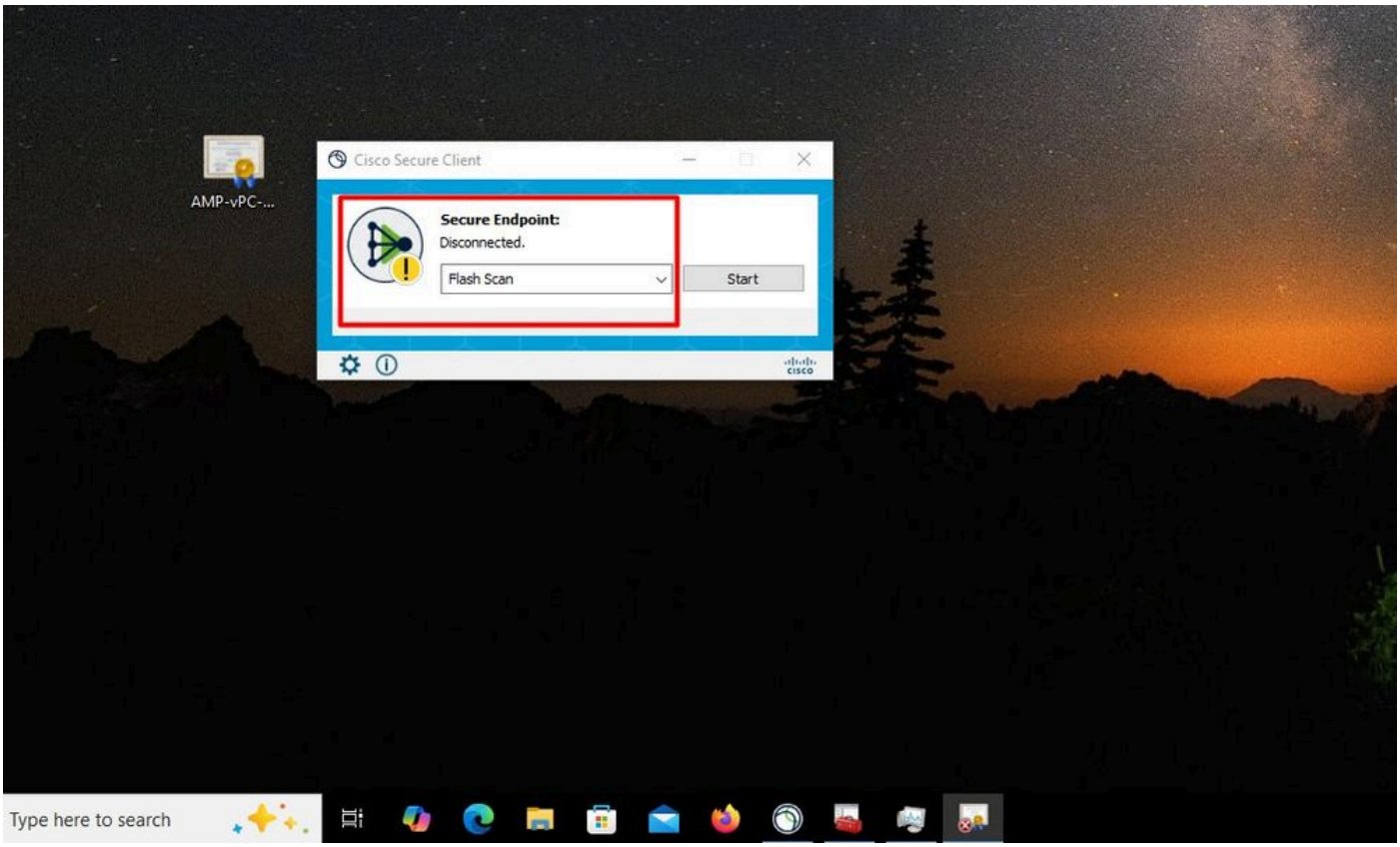


Problème #2 - Problème avec l'autorité de certification racine

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.



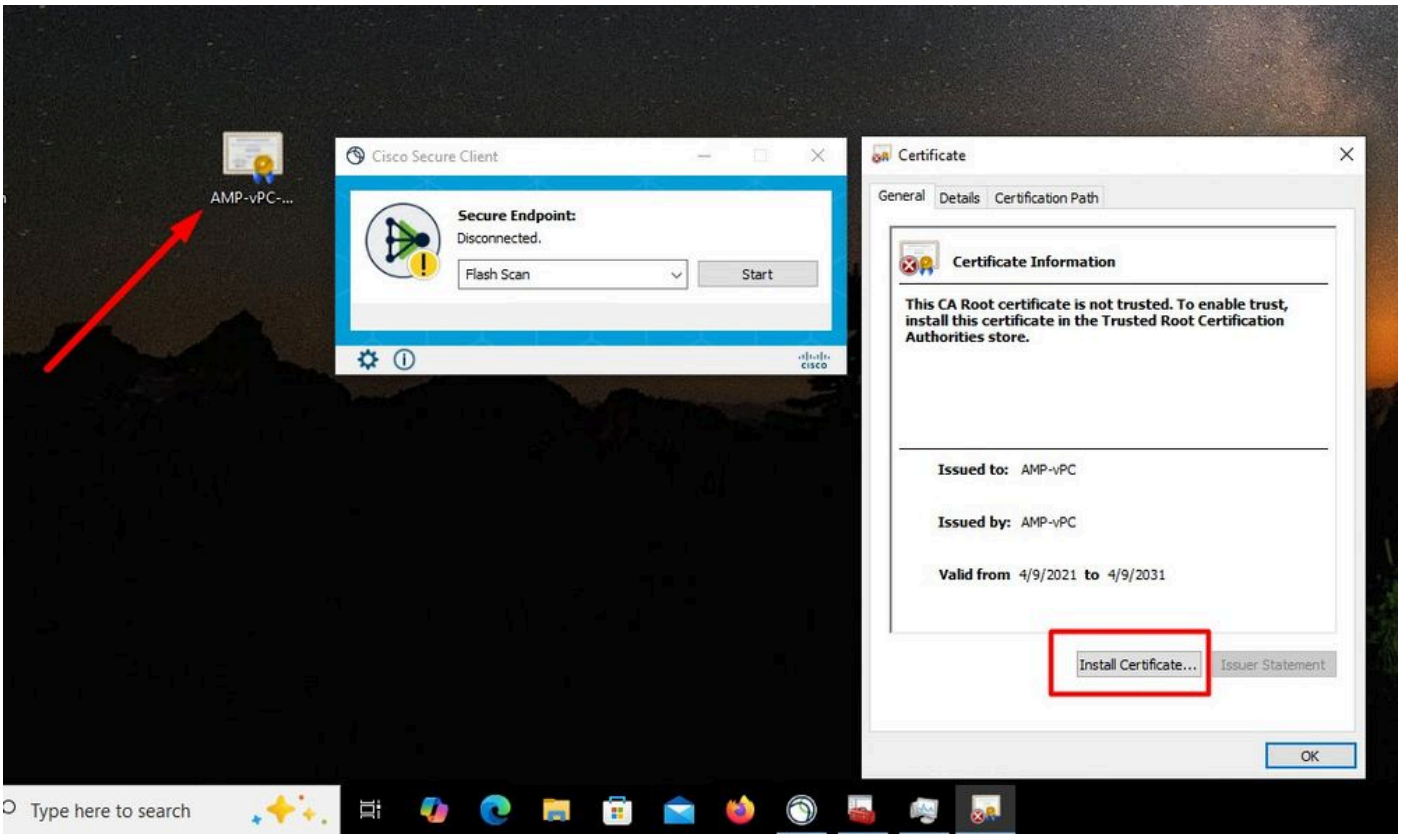
Sur la base de cette sortie collectée à partir du bundle de diagnostic, vous pouvez voir l'erreur d'autorité de certification racine

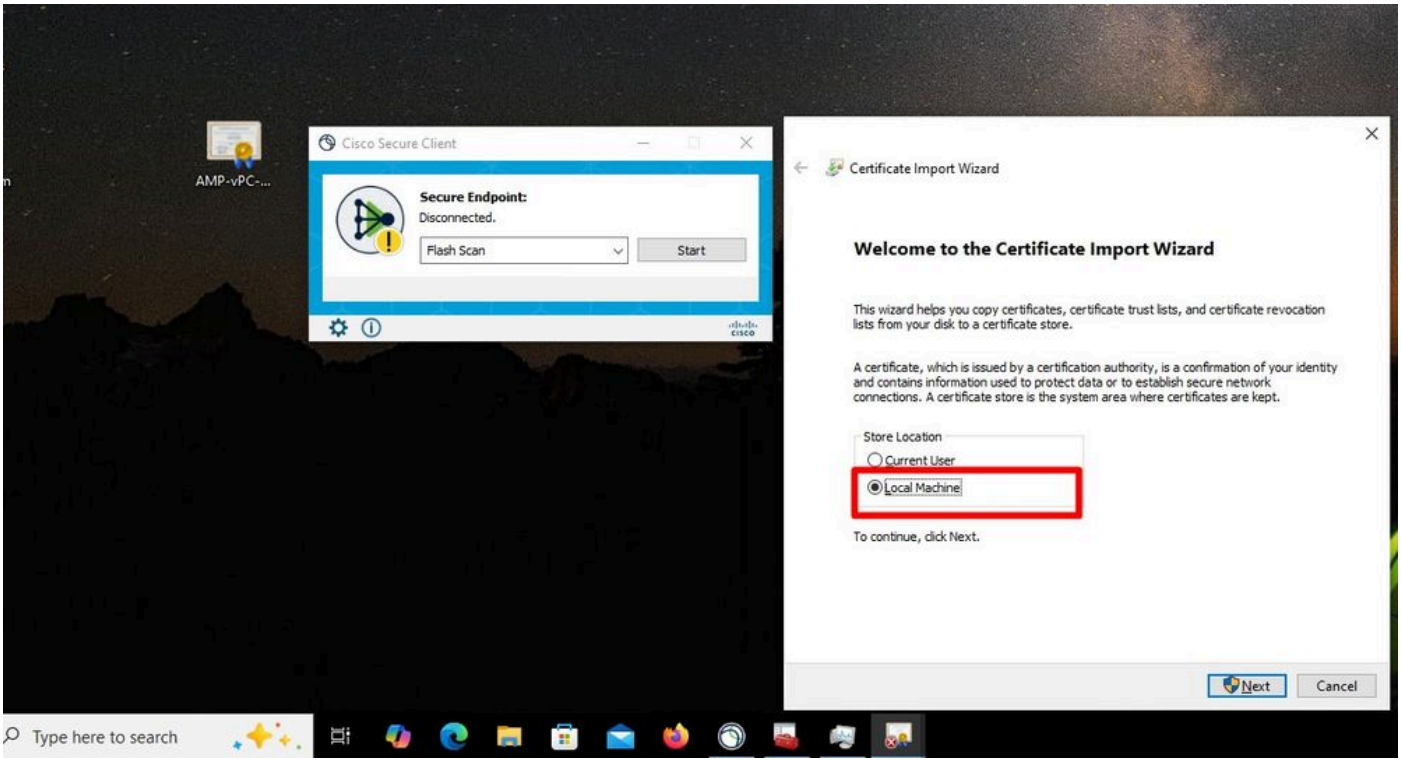
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl

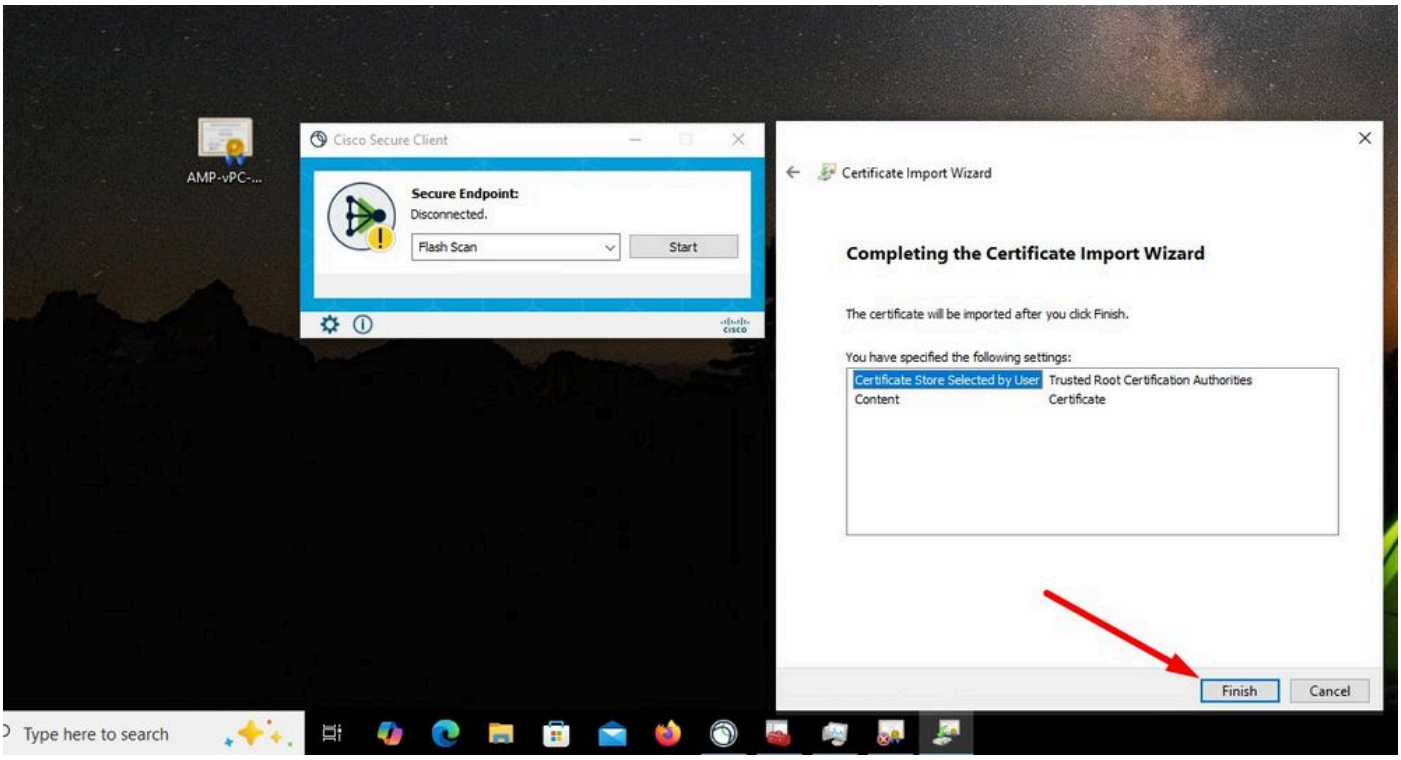
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat

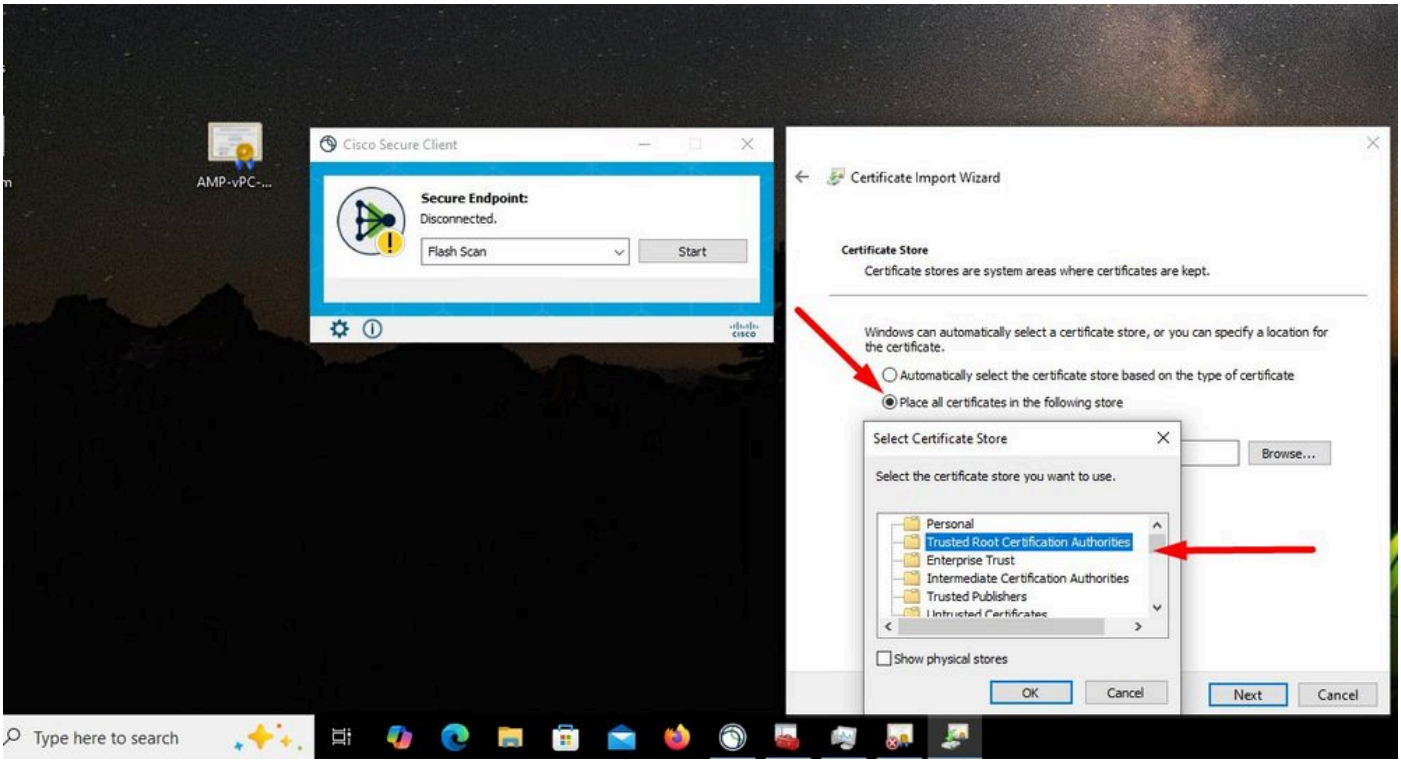
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

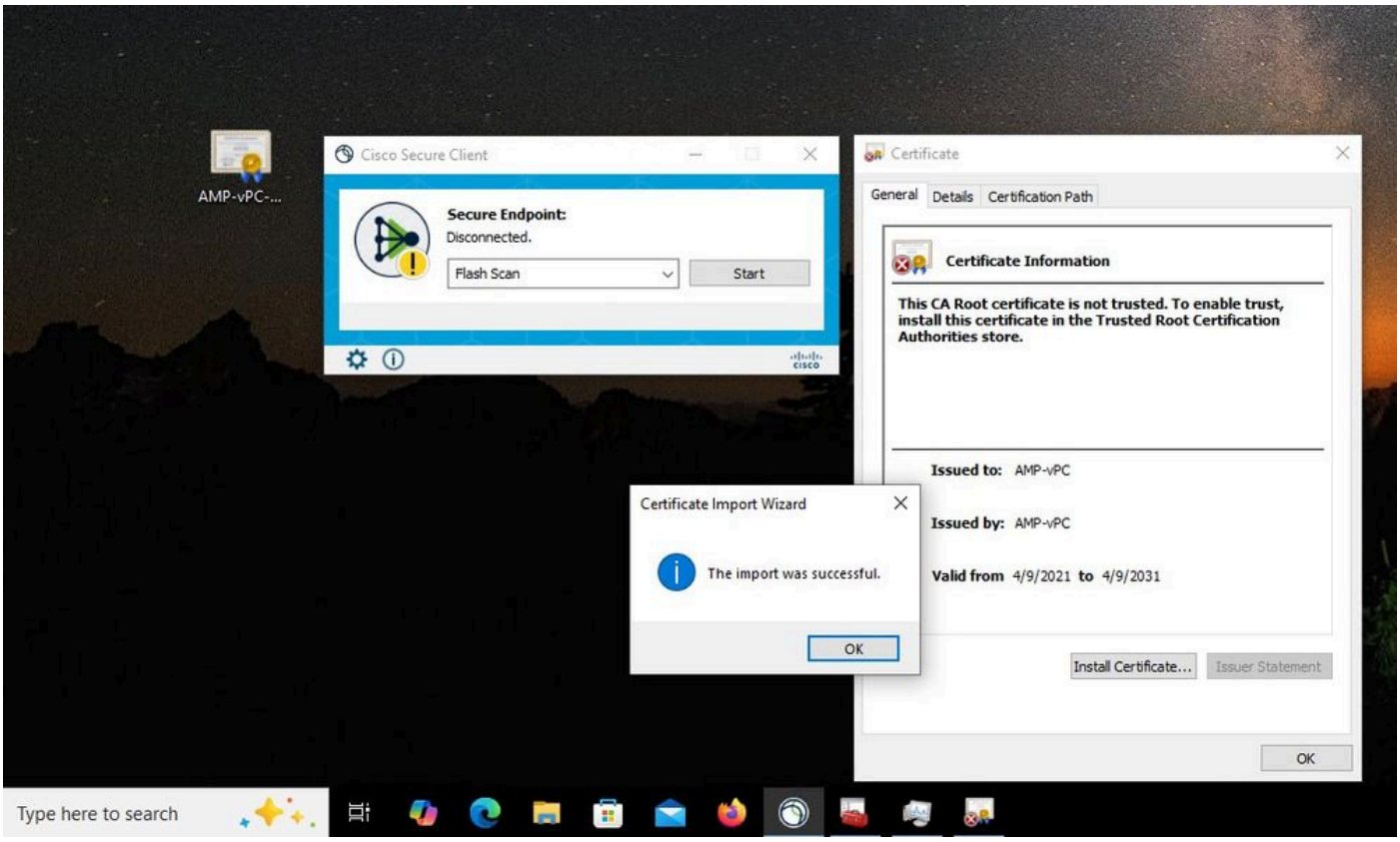
Une fois que vous avez téléchargé l'autorité de certification racine dans le magasin d'autorité de certification racine approuvée et redémarré le service Secure Endpoint. Tout commence à fonctionner comme prévu.

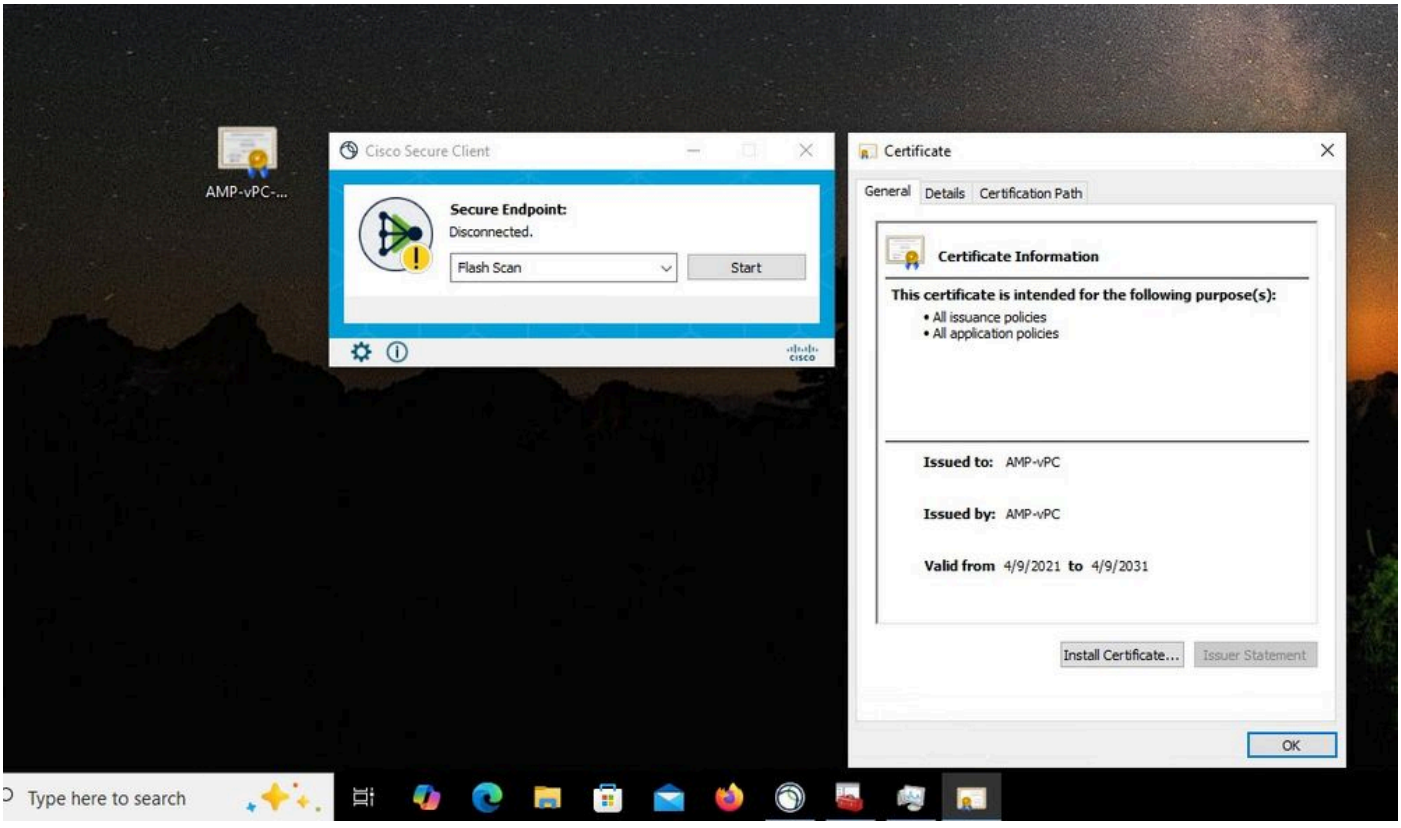

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Type here to search

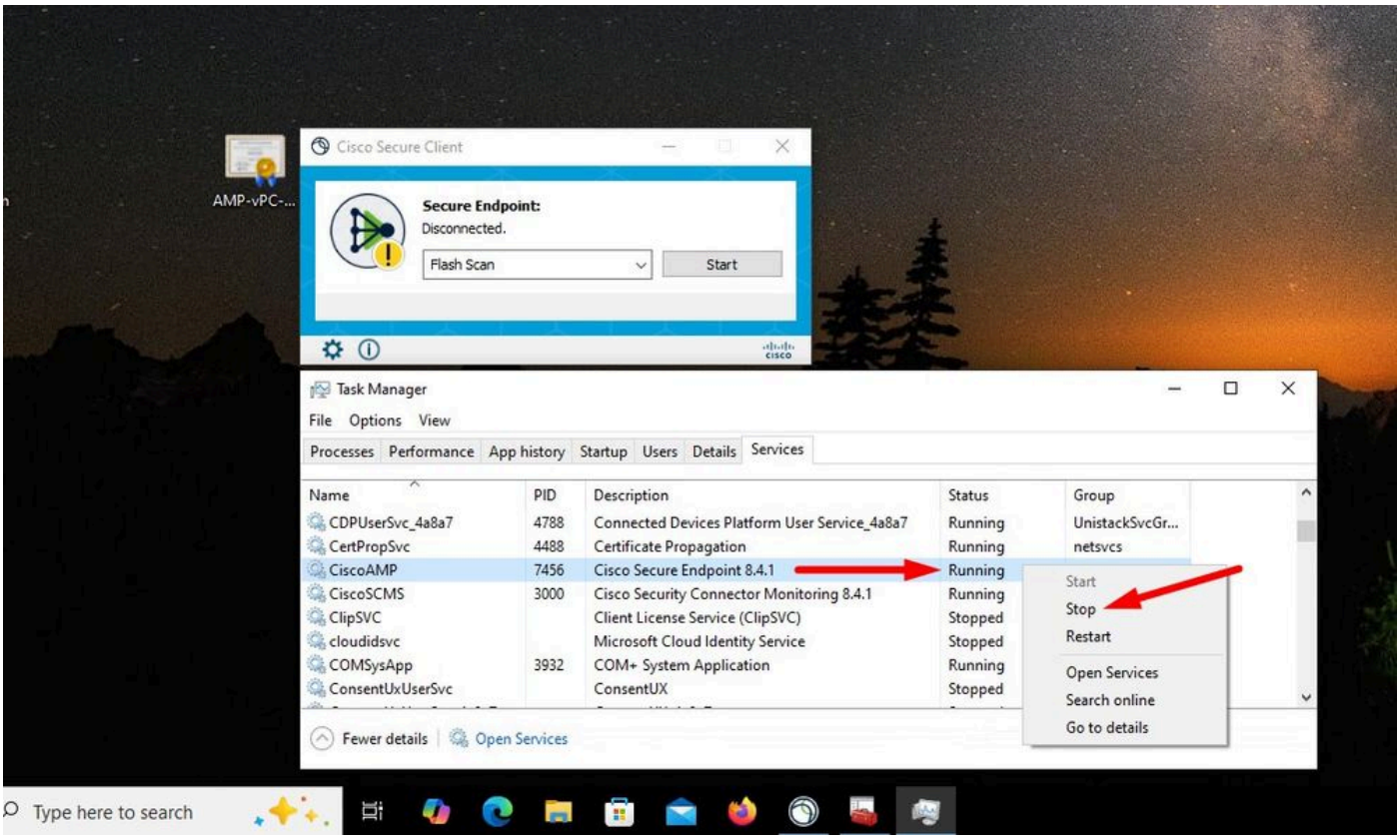

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel
Type here to search

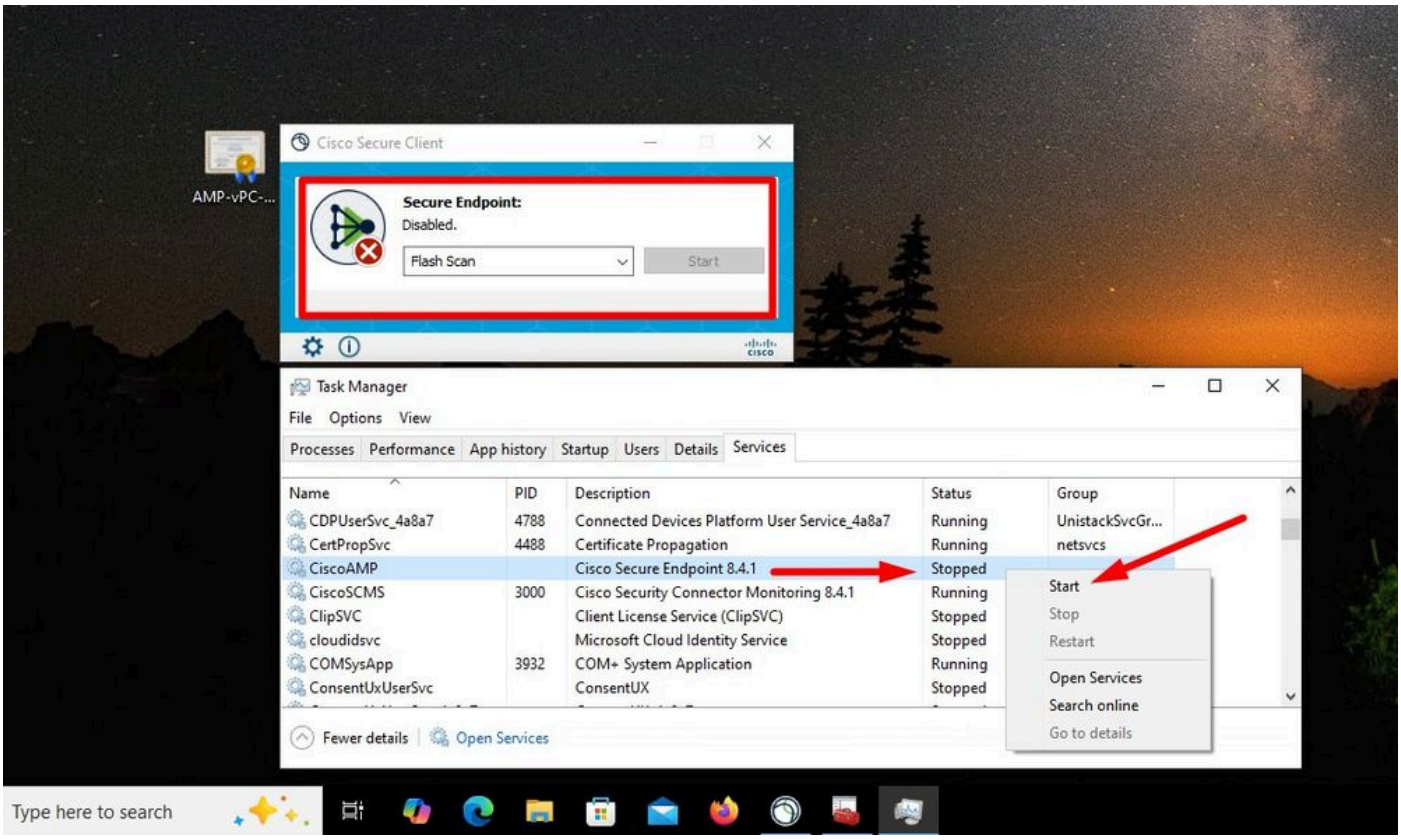

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel
Type here to search


AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Browse...
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Show physical stores
OK
Cancel
Next
Cancel
Type here to search

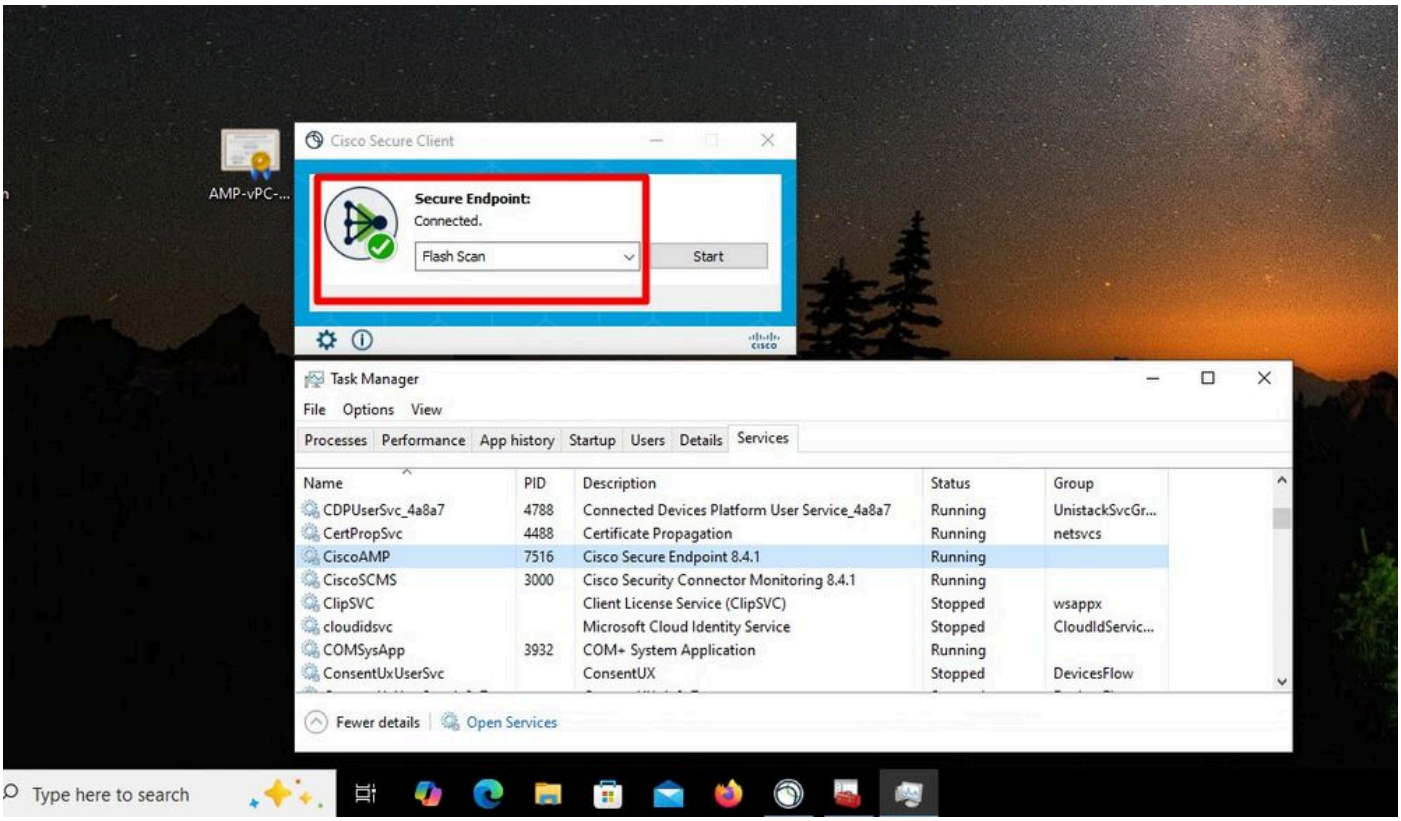

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Certificate Import Wizard
The import was successful.
OK
Type here to search

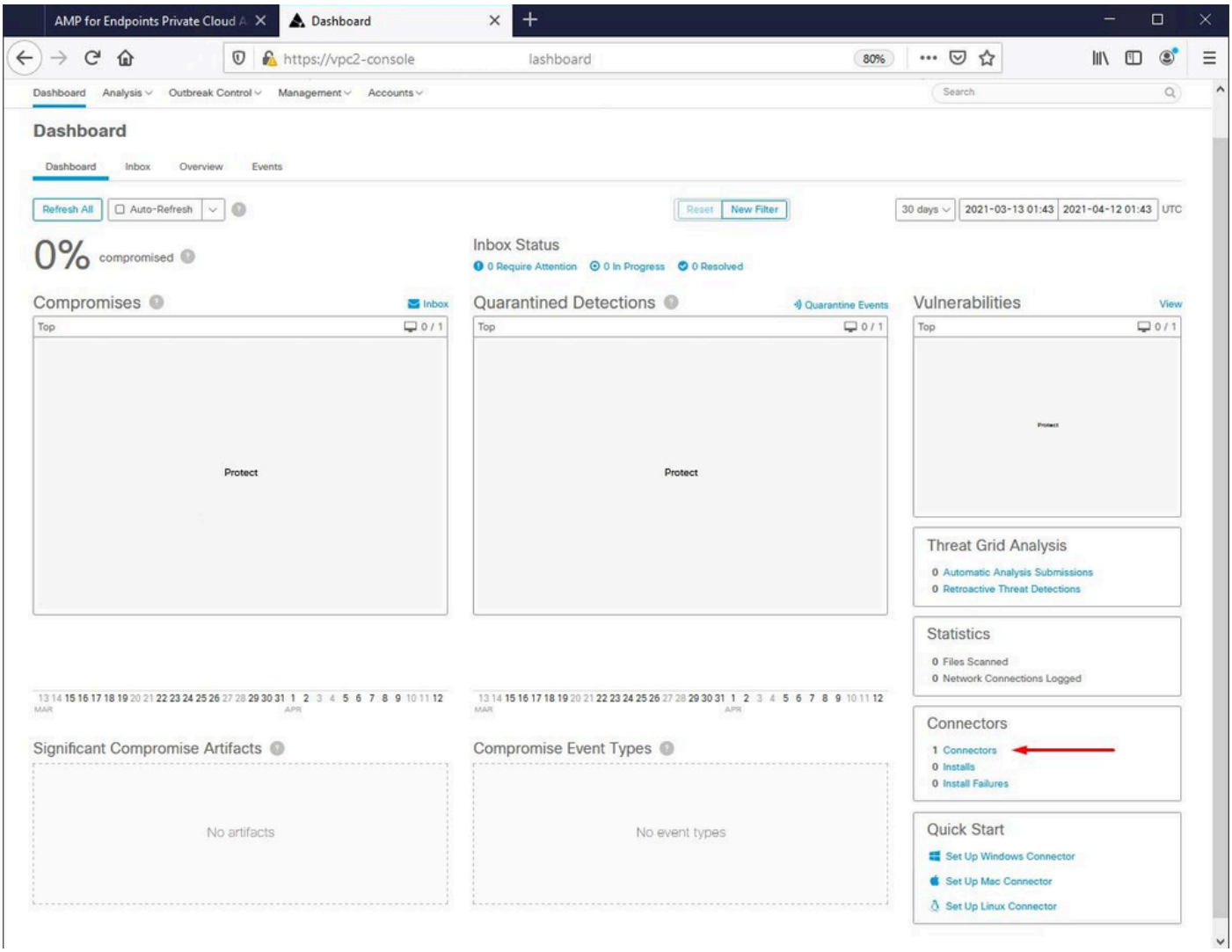

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Type here to search



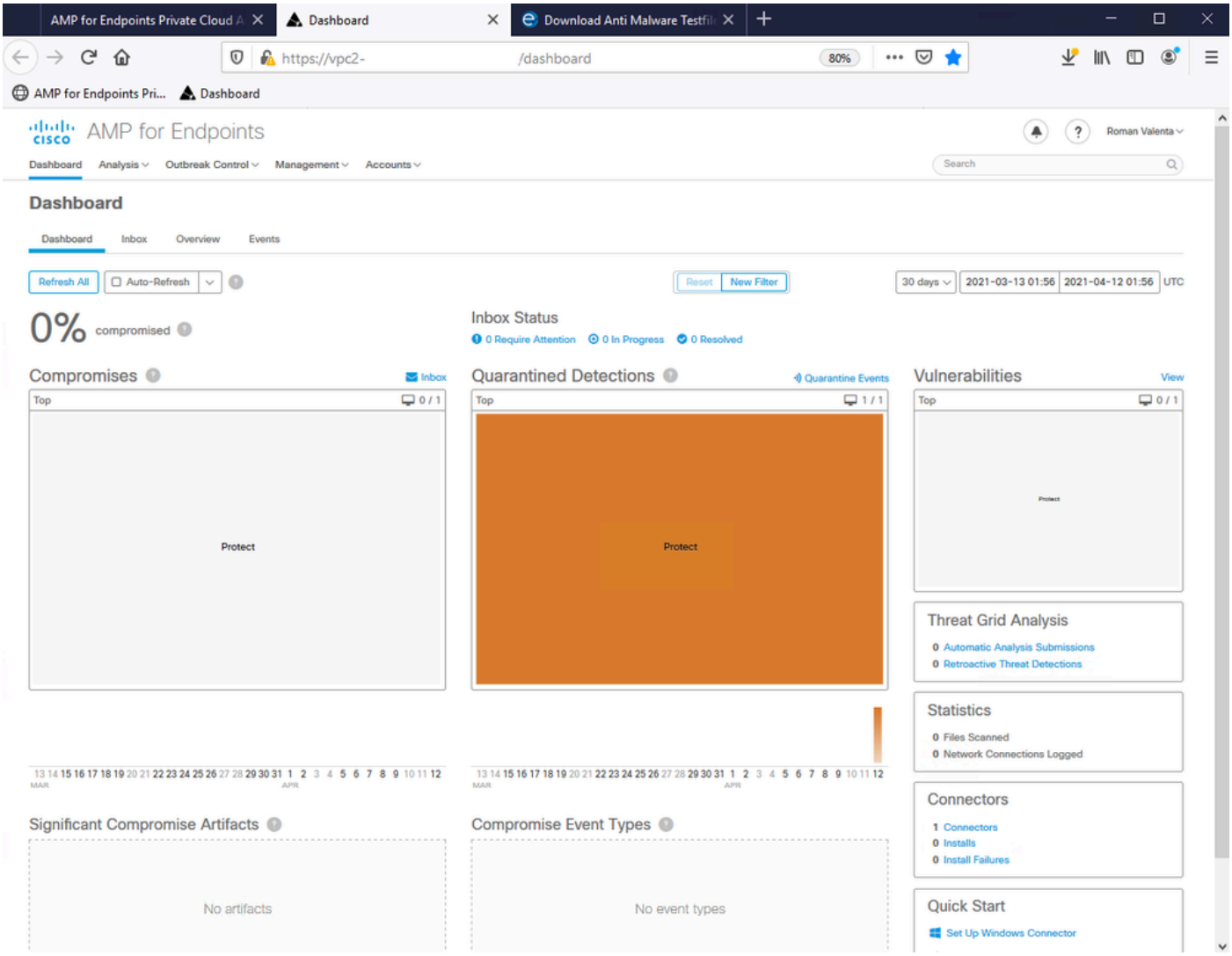


Une fois le connecteur de service Secure Endpoint remis en service, mettez-le en ligne comme prévu.


AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Connected.
Flash Scan
Start
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name PID Description Status Group
CDPUserSvc_4a8a7 4788 Connected Devices Platform User Service_4a8a7 Running UnistackSvcGr...
CertPropSvc 4488 Certificate Propagation Running netsvcs
CiscoAMP 7516 Cisco Secure Endpoint 8.4.1 Running
CiscoSCMS 3000 Cisco Security Connector Monitoring 8.4.1 Running
ClipSVC Client License Service (ClipSVC) Stopped wsappx
cloudidsvc Microsoft Cloud Identity Service Stopped CloudIdServic...
COMSysApp 3932 COM+ System Application Running
ConsentUxUserSvc ConsentUX Stopped DevicesFlow
Fewer details
Open Services
Type here to search



Activité malveillante testée


AMP for Endpoints Private Cloud A
Dashboard
Download Anti Malware Testfil
https://vpc2-
/dashboard
80%
AMP for Endpoints Pri...
Dashboard
AMP for Endpoints
Roman Valenta
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
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
Top
0 / 1
Protect
Quarantined Detections
Quarantine Events
Top
1 / 1
Protect
Vulnerabilities
View
Top
0 / 1
Protect
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
Threat Grid Analysis
0 Automatic Analysis Submissions
0 Retroactive Threat Detections
Statistics
0 Files Scanned
0 Network Connections Logged
Connectors
1 Connectors
0 Installs
0 Install Failures
Quick Start
Set Up Windows Connector
Significant Compromise Artifacts
No artifacts
Compromise Event Types
No event types

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.