Instalação e configuração de nuvem privada virtual de endpoint segura

Contents

Introdução

Este documento descreve e se concentra em como implantar com sucesso a Virtual Private Cloud (VPC) em servidores no ambiente ESXi. Para outros documentos, como o Guia de início rápido, Estratégia de implantação, Guia de qualificação, Console e Guia do usuário administrador, visite a Documentação deste site

Contribuição de Roman Valenta, Engenheiros do Cisco TAC.

Pré-requisitos

Requisitos:

VMware ESX 5 ou posterior

- Modo de proxy de nuvem (somente): 128 GB de RAM, 8 núcleos de CPU (2 CPUs com 4 núcleos cada recomendado), 1 TB de espaço livre mínimo em disco no armazenamento de dados VMware
- Tipo de unidades: SSD necessária para o modo de lacuna de ar e recomendada para proxy
- Tipo de RAID: um grupo de RAID 10 (espelho distribuído)
- Tamanho mínimo do armazenamento de dados VMware: 2 TB
- Mínimo de leituras aleatórias de armazenamento de dados para o grupo RAID 10 (4K): 60K IOPS

- Mínimo de gravações aleatórias de armazenamento de dados para o grupo RAID 10 (4K): 30K IOPS

A Cisco recomenda ter conhecimento deste tópico:

- Conhecimento básico sobre como trabalhar com certificados.
- Conhecimento básico sobre como configurar o DNS no servidor DNS (Windows ou Linux)
- Instalação de um modelo de Open Virtual Appliance (OVA) no VMWare ESXi

Usado neste laboratório:

VMware ESX 6.5

- Modo de proxy de nuvem (somente): 48 GB de RAM, 8 núcleos de CPU (2 CPUs com 4 núcleos cada recomendado), 1 TB de espaço livre mínimo em disco no armazenamento de dados VMware
- Tipo de unidades: SATA
- Tipo de RAID: um RAID 1
- Tamanho mínimo do armazenamento de dados VMware: 1 TB
- MobaXterm 20.2 (programa multiterminal semelhante ao PuTTY)
- Cygwin64 (Usado para baixar a Atualização AirGap)

Adicionalmente

- Certificado criado com openSSL ou XCA
- Servidor DNS (Linux ou Windows) No meu laboratório, usei o Windows Server 2016 e o CentOS-8
- Windows VM para nosso endpoint de teste
- Licença

Se a memória estiver abaixo de 48 GB de RAM na versão 3.2+, o VPC ficará inutilizável.

Observação: o OVA de nuvem privada cria as partições da unidade, portanto, não há necessidade de especificá-las no servidor VMWare. que resolve o nome de host da interface limpa.

Consulte a Folha de dados do equipamento VPC para obter mais informações sobre os requisitos de hardware específicos da versão.

Nota:As informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

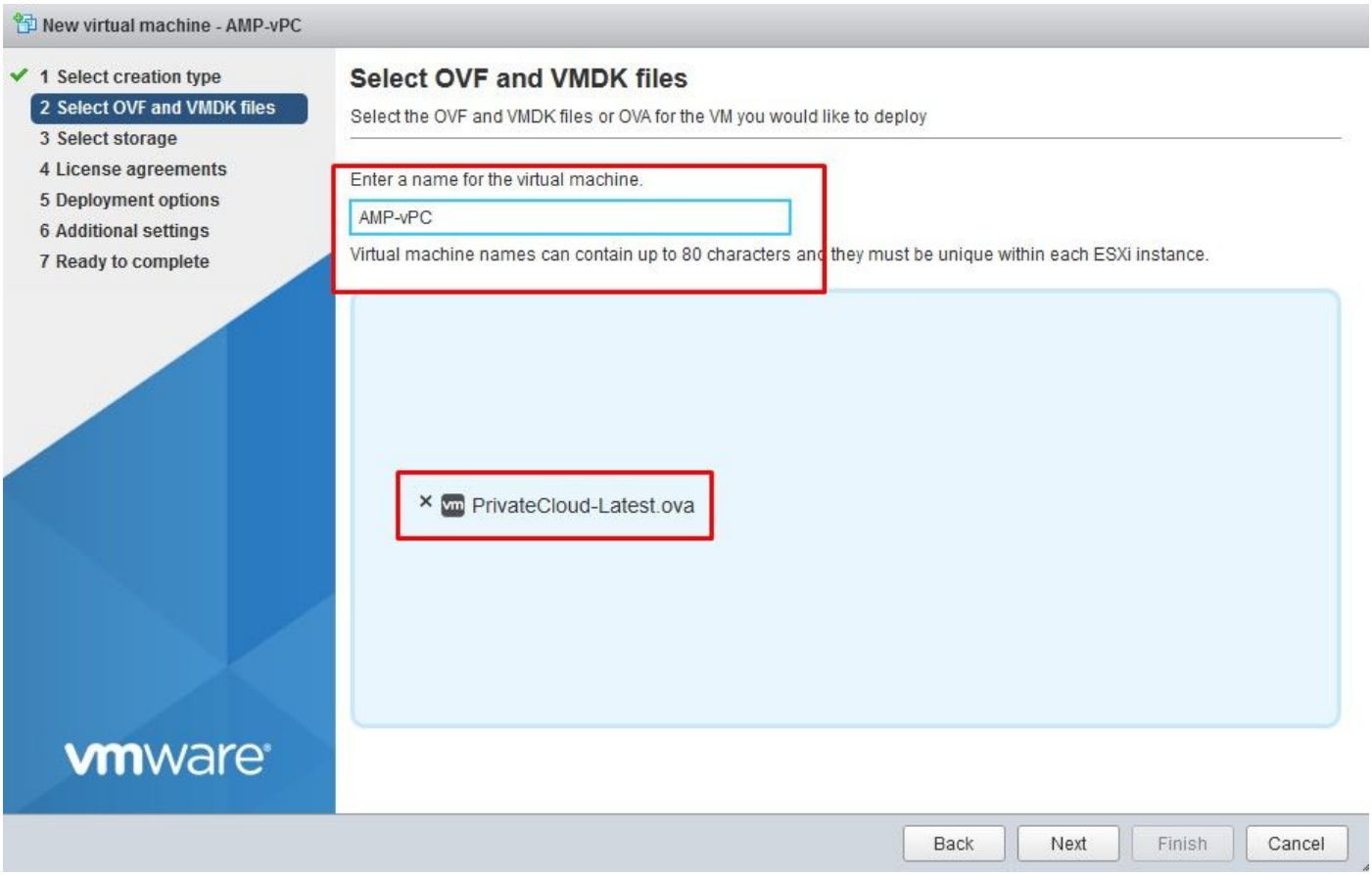
Implantação de VPC

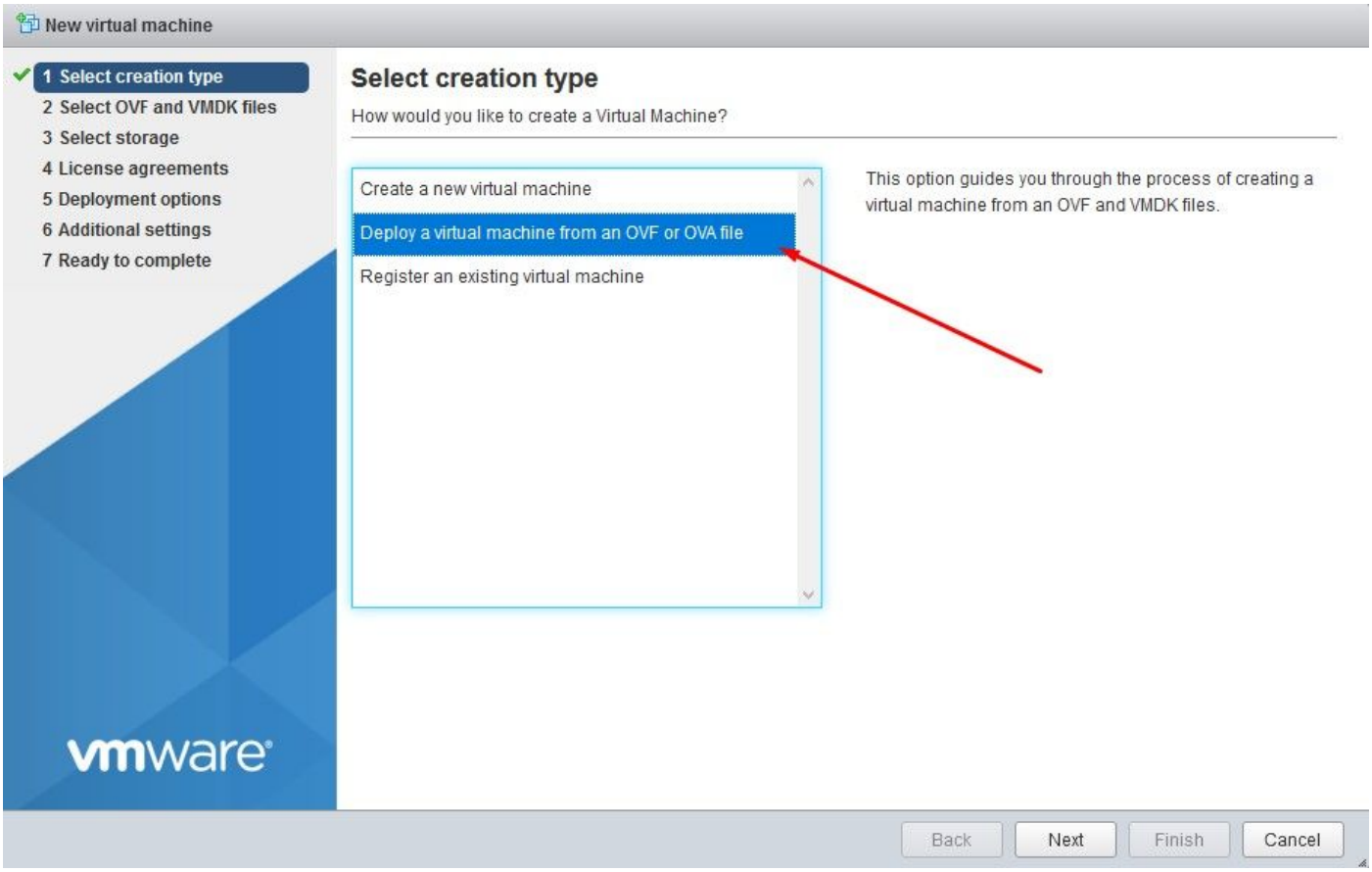
Selecione o URL fornecido no eDelivery ou no e-mail de qualificação. Faça o download do arquivo OVA e continue com a instalação

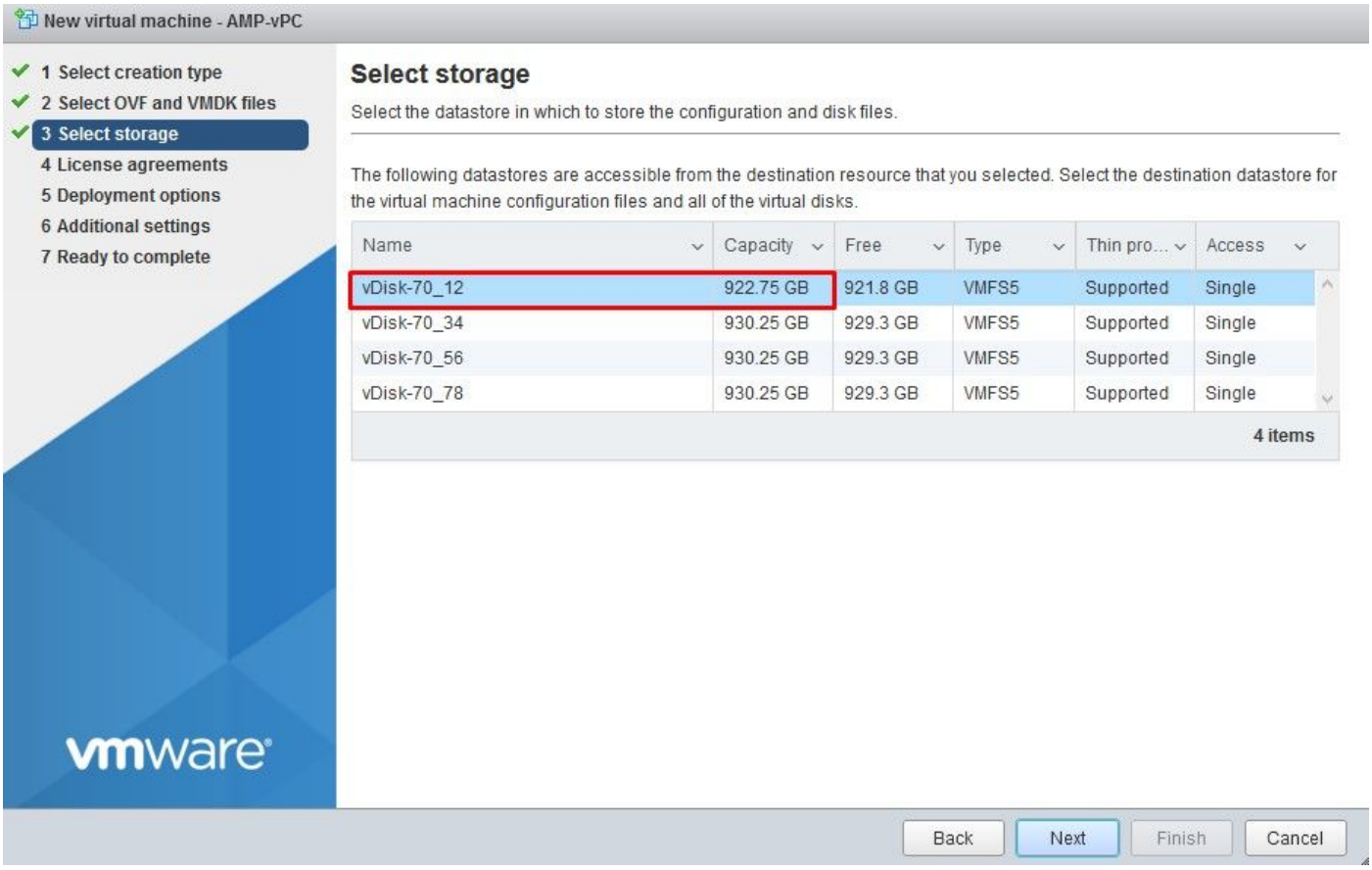
Instalação da VM

Etapa1:

Navegue até File > Deploy OVF Template para abrir o assistente Deploy OVF Template, como mostrado na imagem.

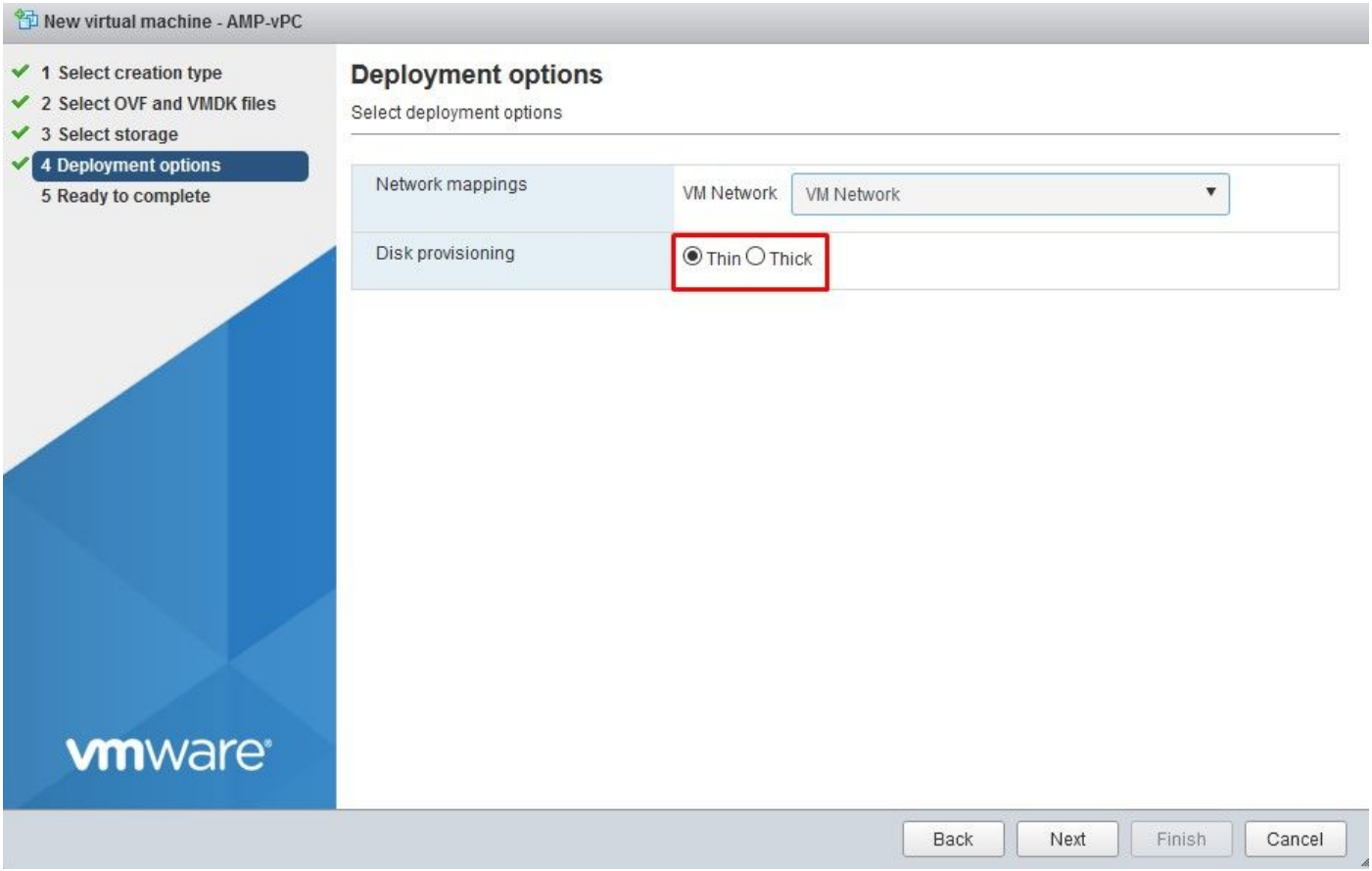






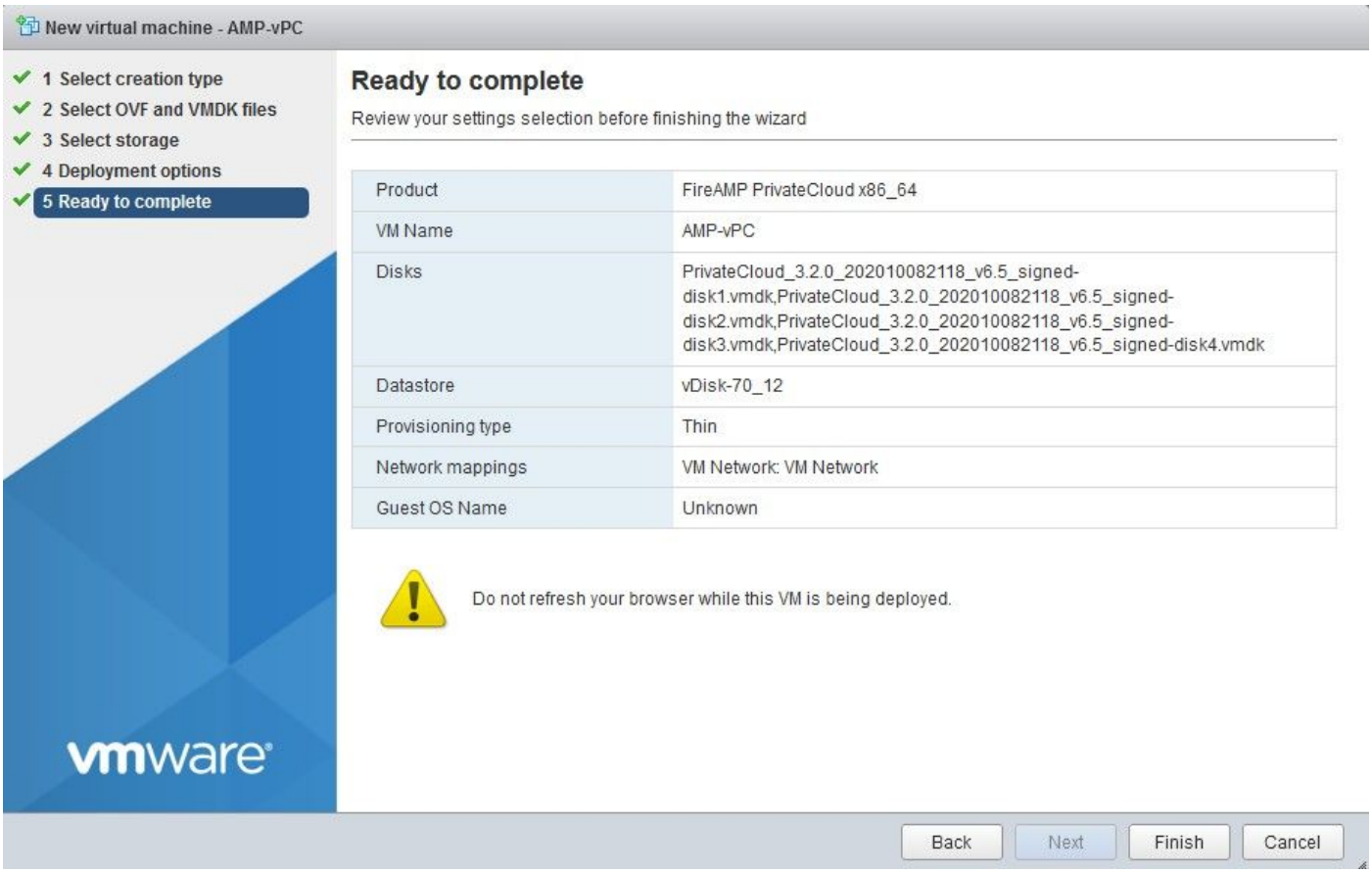
Observação: o Provisionamento espesso reserva espaço quando um disco é criado. Se você selecionar essa opção, ela poderá melhorar o desempenho em relação ao

provisionamento thin. No entanto, isso não é obrigatório. Agora, selecione Next, conforme mostrado na imagem.

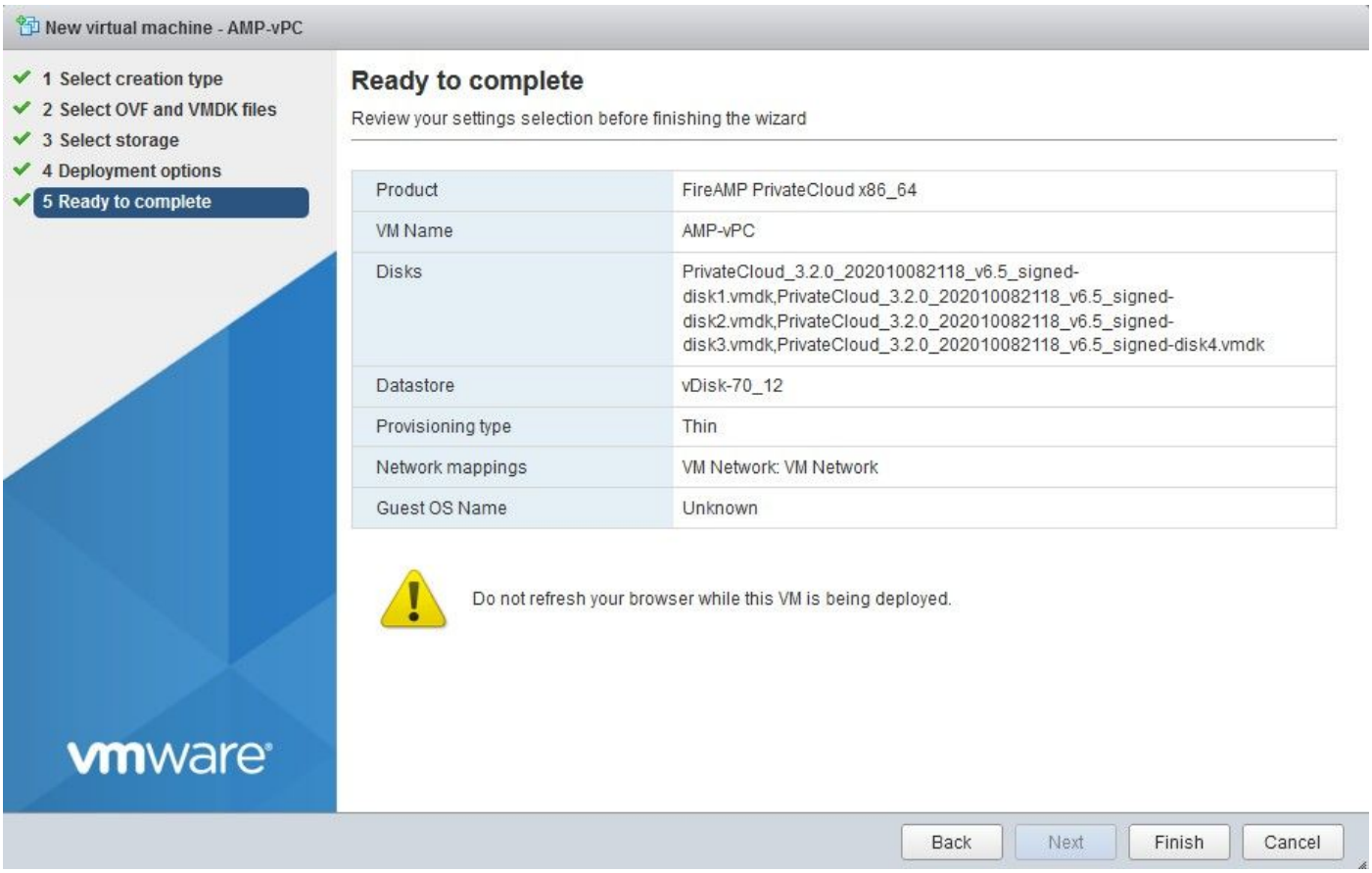


Passo 2:

Selecione Procurar... para selecionar um arquivo OVA e, em seguida, selecione Próximo. Você observa os parâmetros OVA default na página Detalhes do Modelo OVF, conforme mostrado na imagem. selecione em Próximo.



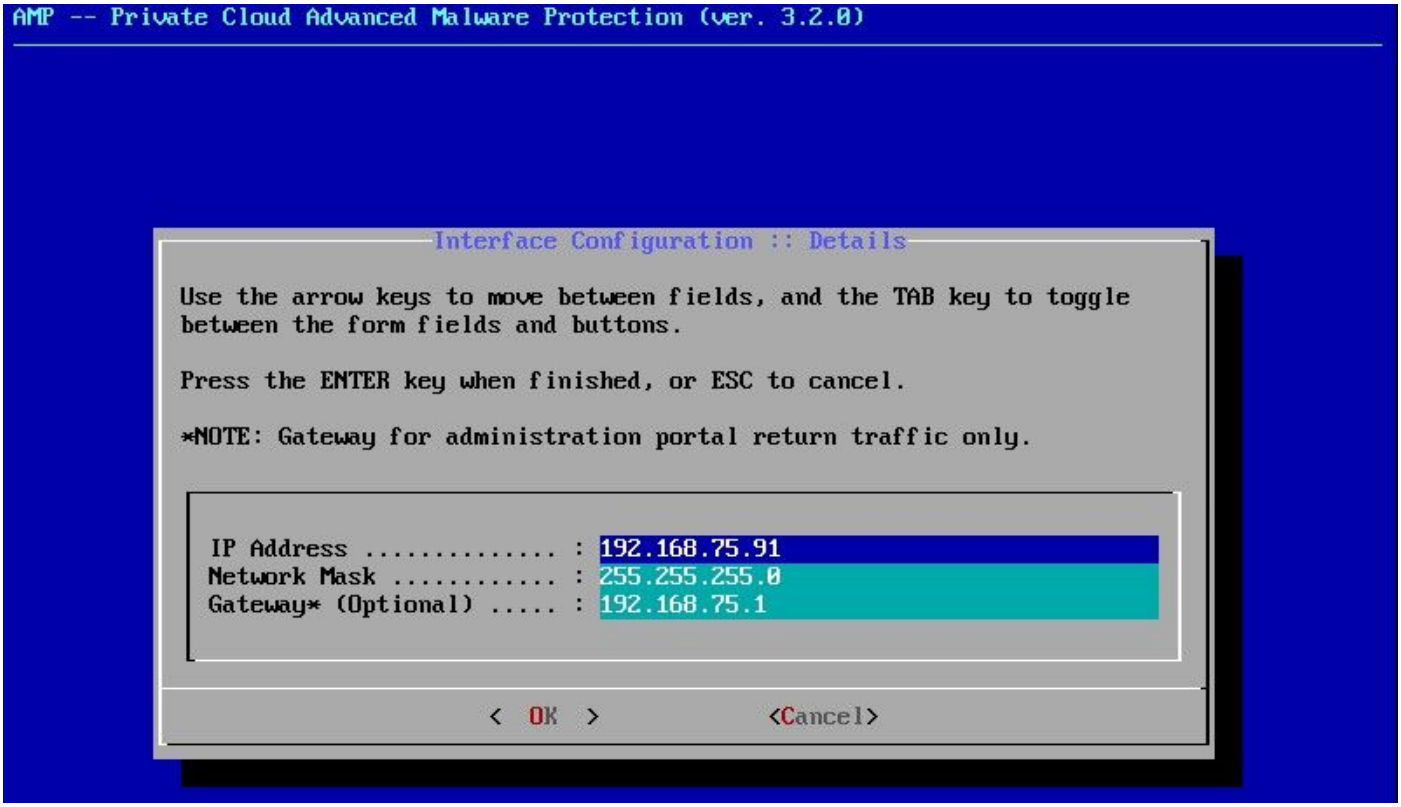
Configuração inicial da interface do administrador



Depois que a VM for inicializada, faça a configuração inicial por meio do Console da VM.

Passo 1:

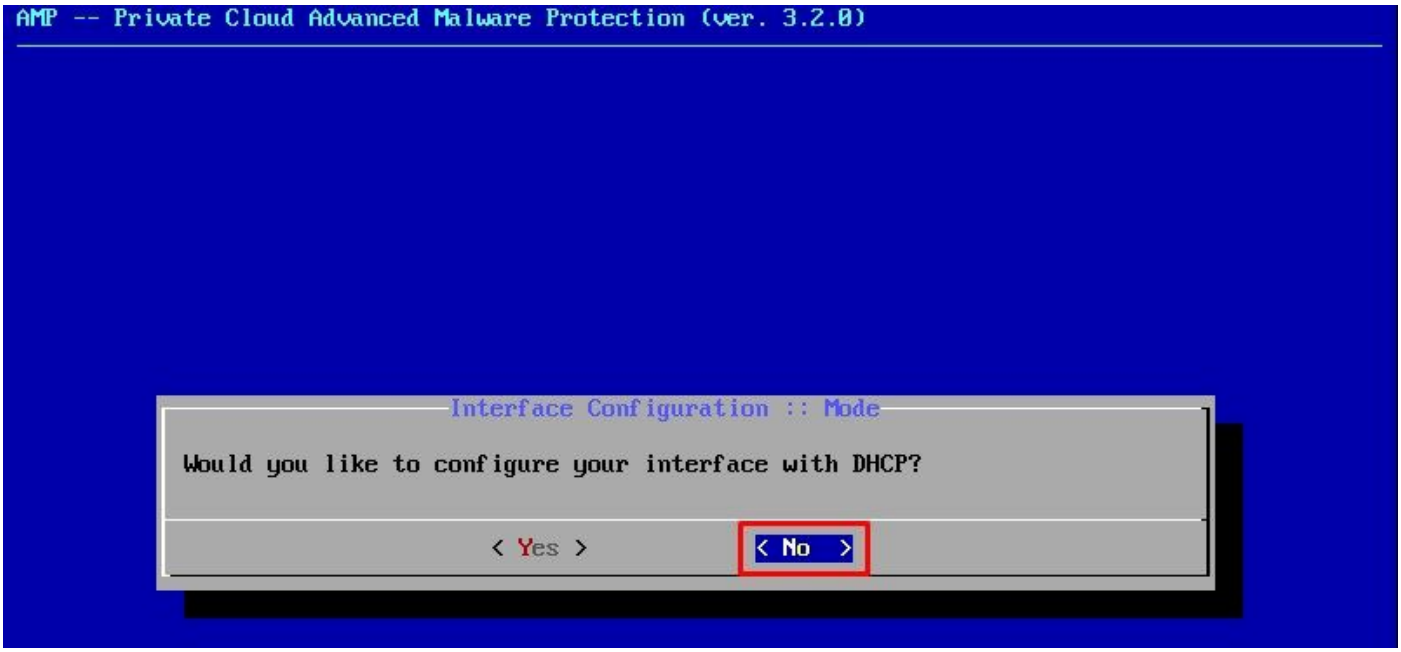
Você pode observar que a URL mostra [UNCONFIGURED] se a interface não recebeu um endereço IP do servidor DHCP. Observe que essa interface é a interface de gerenciamento. Essa não é a interface de produção.

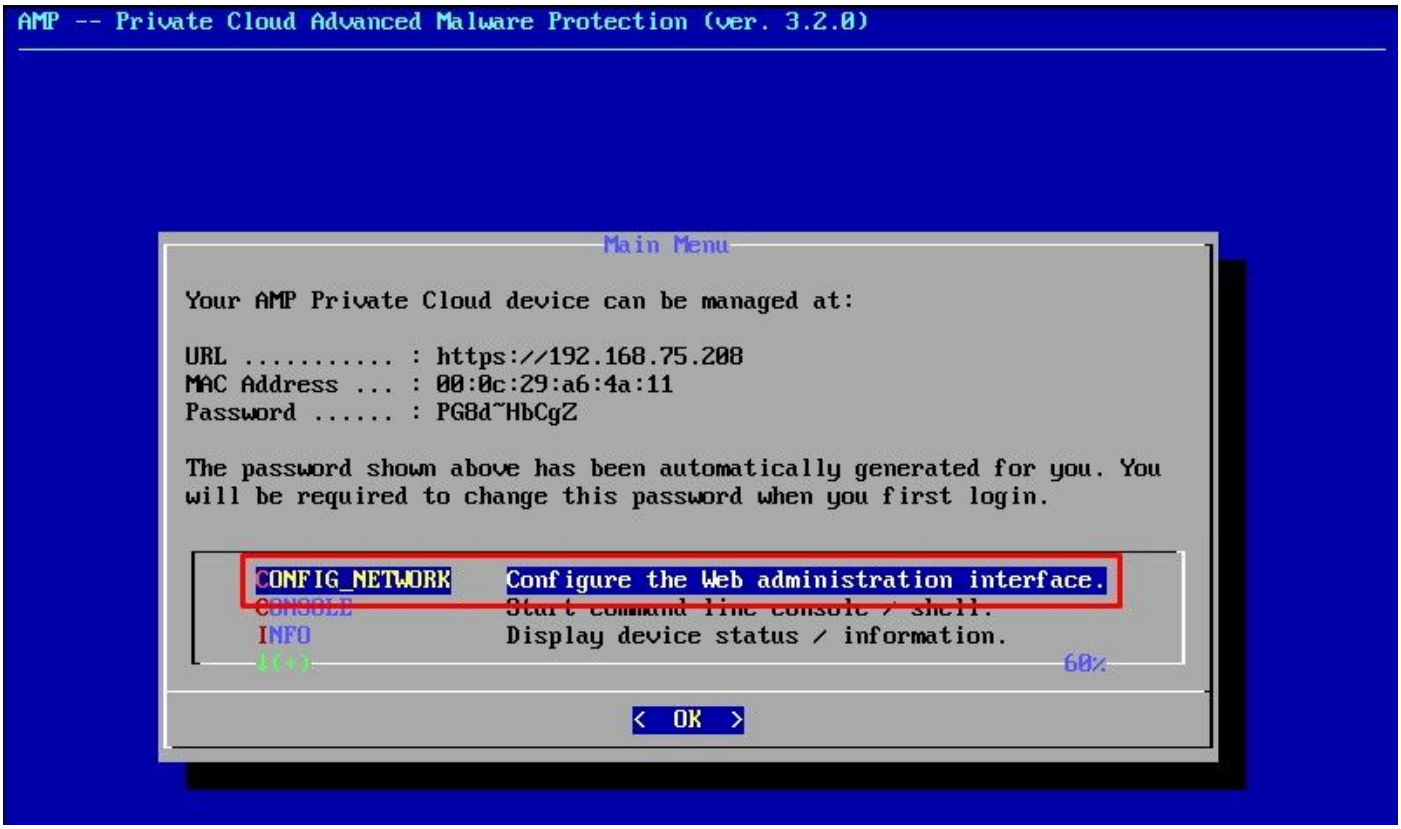


Passo 2:

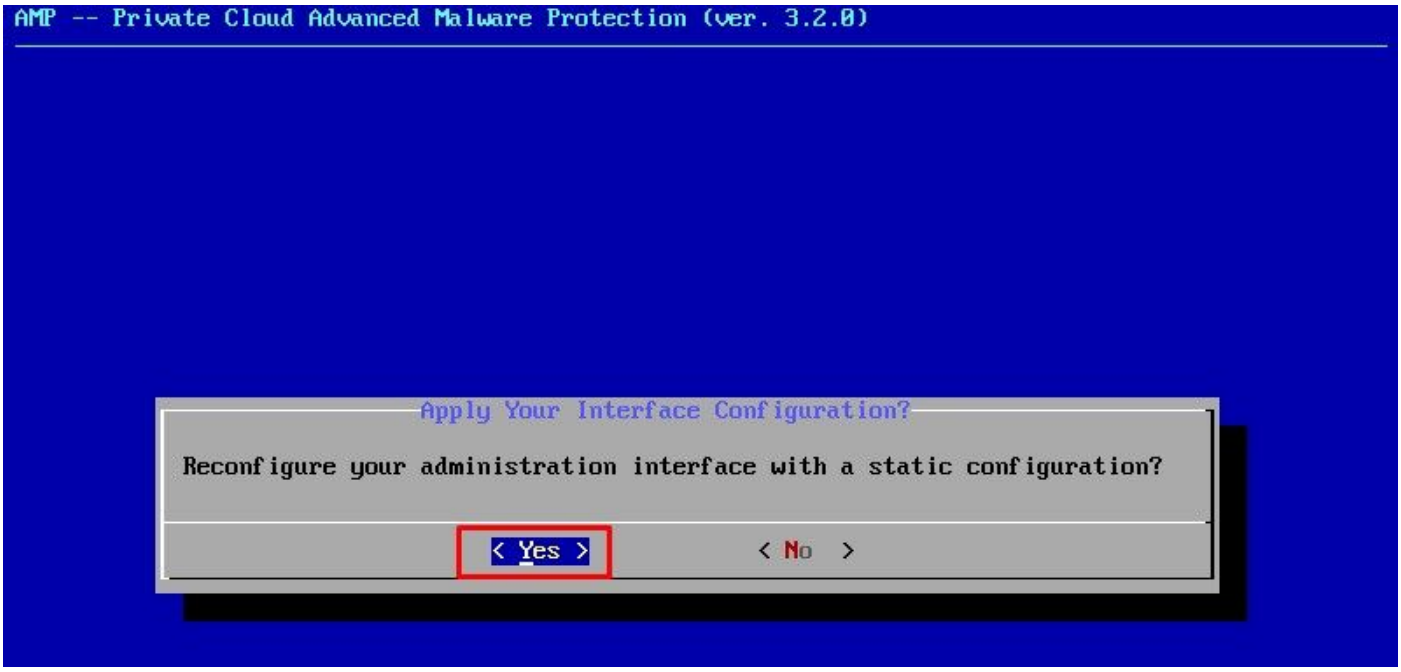
Você pode navegar pelas teclas Tab, Enter e Seta.

Navegue até CONFIG_NETWORK e selecione a tecla Enter em seu teclado para iniciar a configuração do endereço IP de gerenciamento para o Secure Endpoint Private Cloud. Se você não quiser usar o DHCP, selecione No e selecione Enter.

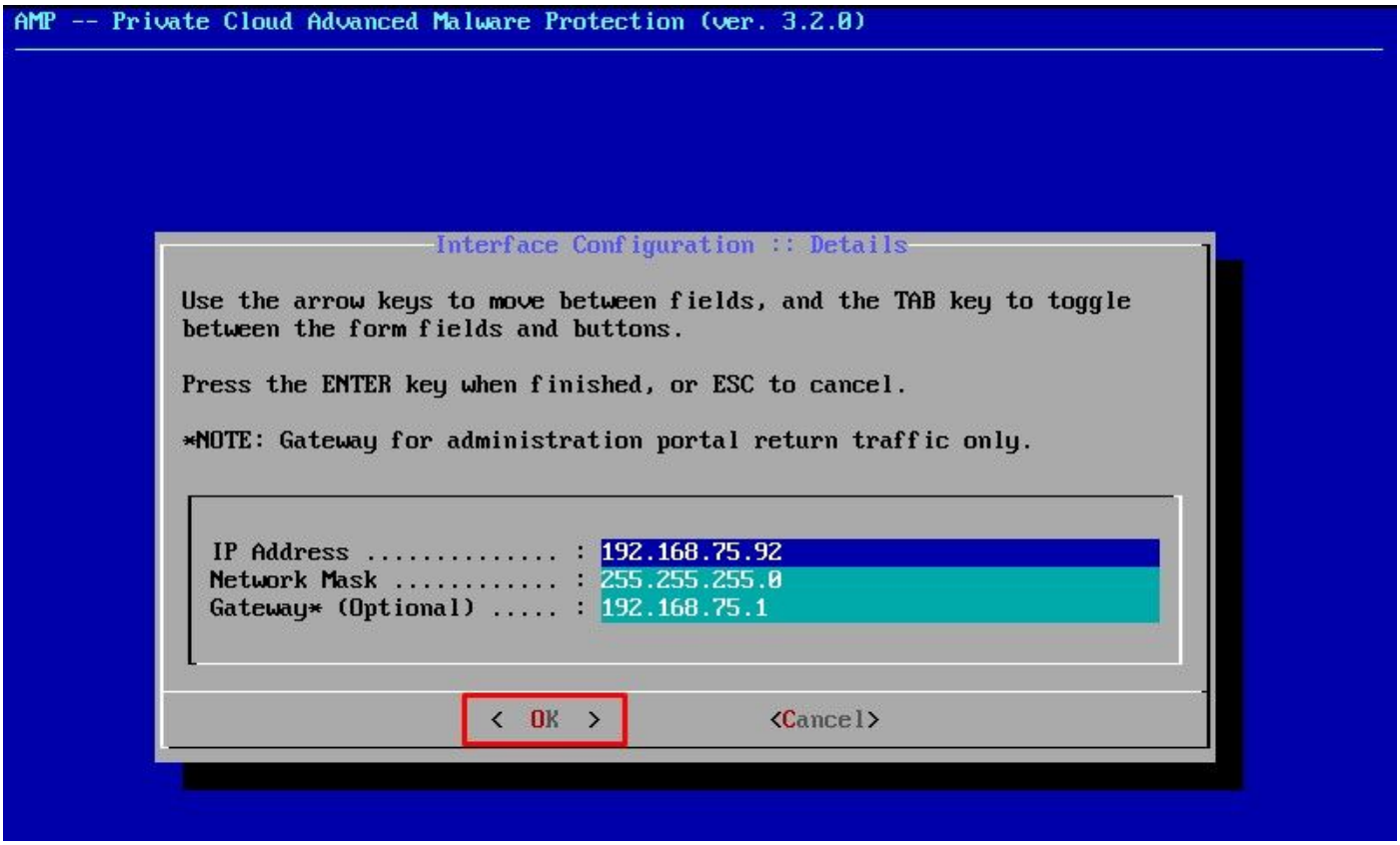




Na janela exibida, escolha Yes e selecione a tecla Enter .

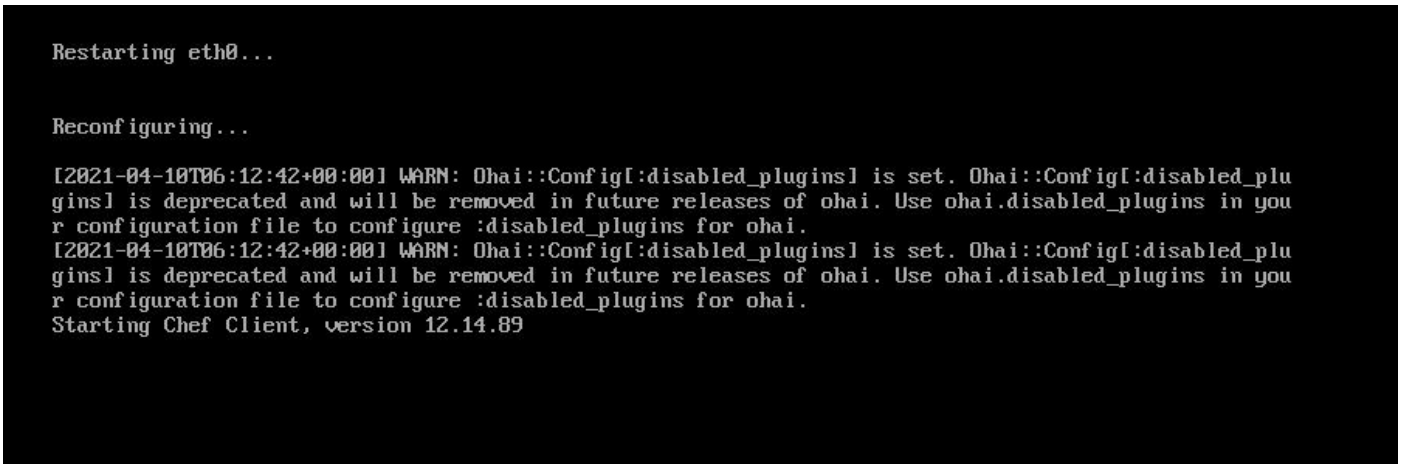


Se o IP já estiver em uso, você será tratado com esse registro de erros. Basta voltar e escolher algo que seja único e não esteja em uso.



Se tudo correr bem, você verá uma saída parecida com esta

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

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



Passo 3:

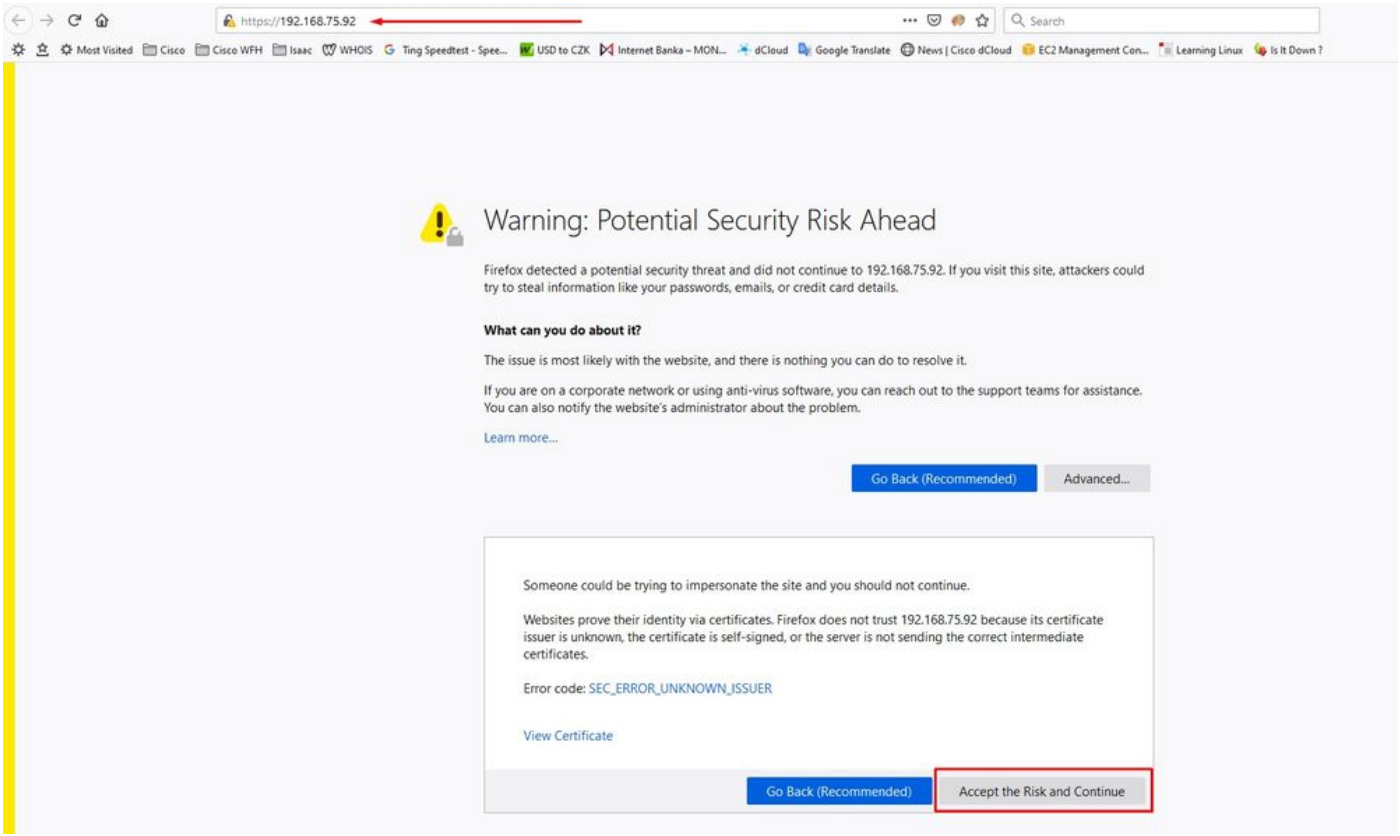
Aguarde até que a tela azul seja exibida novamente com o novo IP ESTÁTICO. Além disso, observe a Senha ocasional. Tome nota e vamos abrir nosso navegador.

Configuração inicial do vPC via GUI da Web

Passo 1:

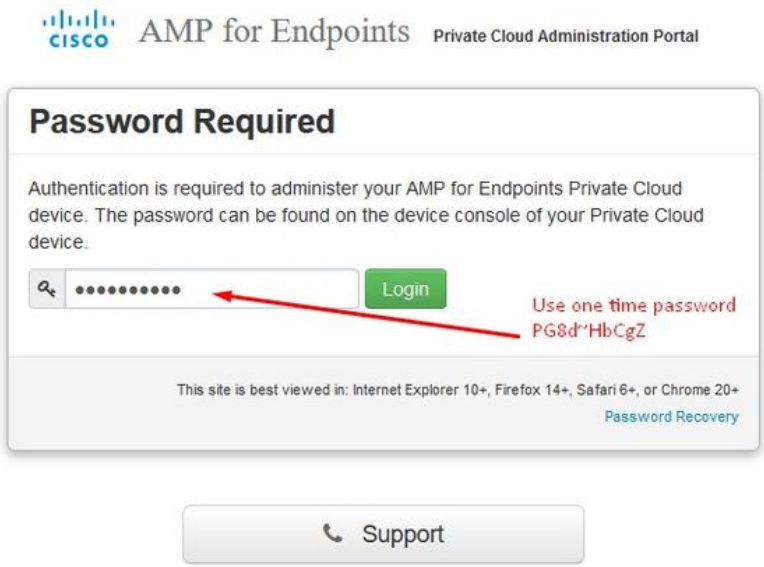
Abra um navegador da Web e navegue até o endereço IP de gerenciamento do equipamento. Você pode receber um erro de certificado quando a Secure Endpoint Private Cloud gerar inicialmente seu próprio certificado HTTPS, como mostrado na imagem. Configure seu navegador para confiar no certificado HTTPS autoassinado da Secure Endpoint Private Cloud.

No navegador, digite o IP ESTÁTICO que você configurou anteriormente.



Passo 2:

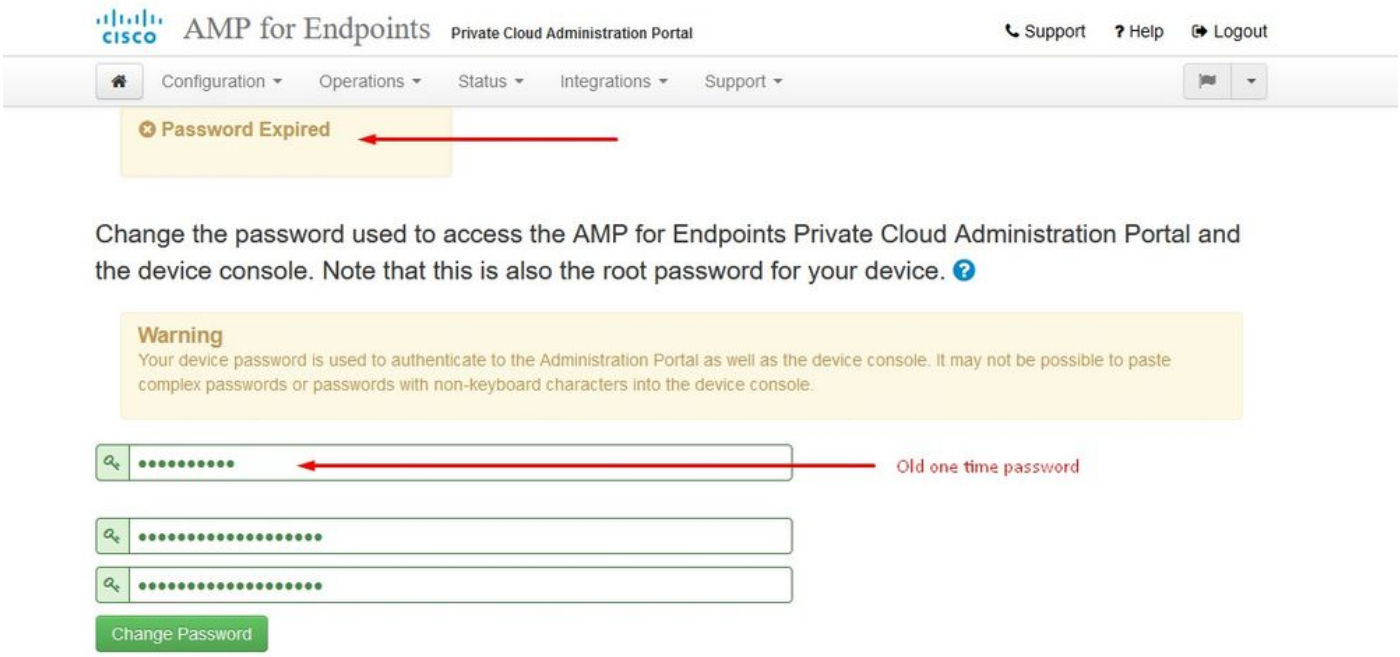
Depois de fazer login, você será solicitado a redefinir a senha. Use a senha inicial do console no campo Antiga senha. Use sua nova senha no campo Nova senha. Insira novamente sua nova senha no campo Nova senha. Selecione em Alterar senha.



Passo 3:

Depois de fazer login, você será solicitado a redefinir a senha. Use a senha inicial do console no

campo Antiga senha. Use sua nova senha no campo Nova senha. Insira novamente sua nova senha no campo Nova senha. Selecione em Alterar senha.

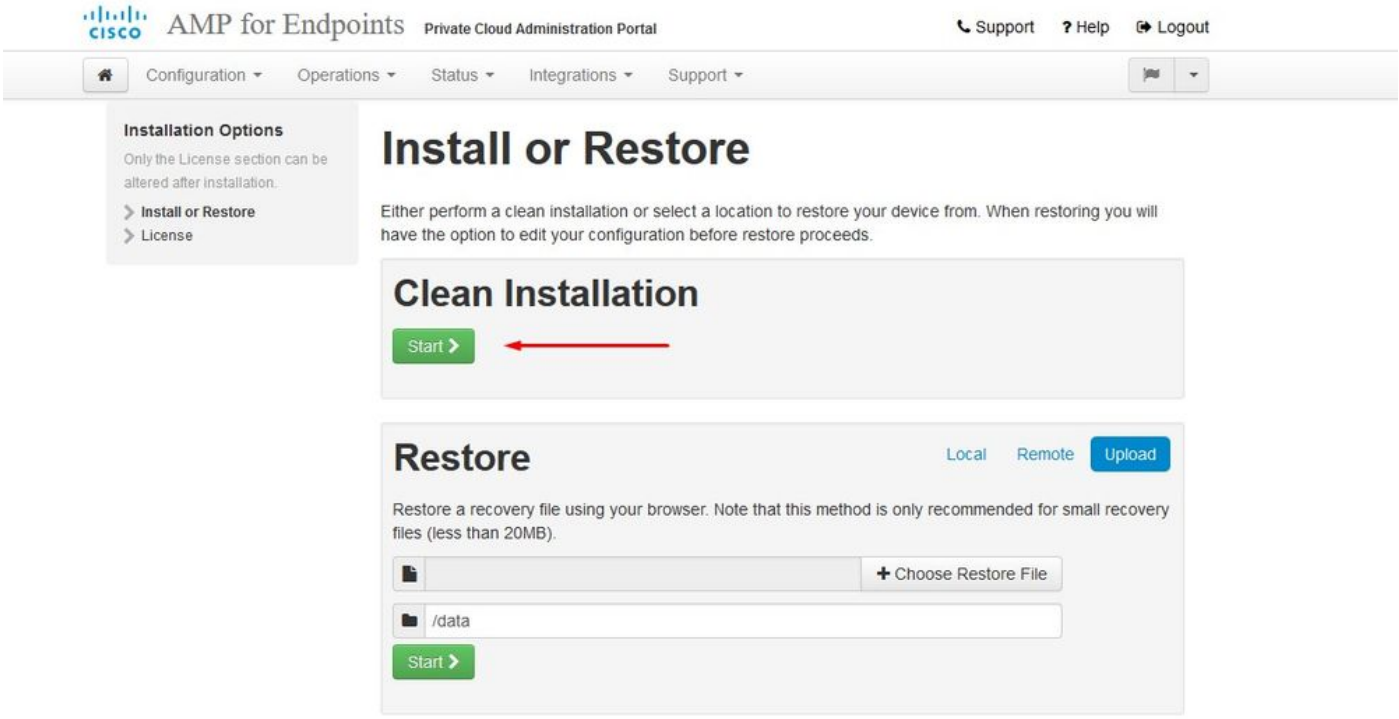


Passo 4:

Na próxima página, role para baixo até o final para aceitar o contrato de licença. selecione I have read and agree.

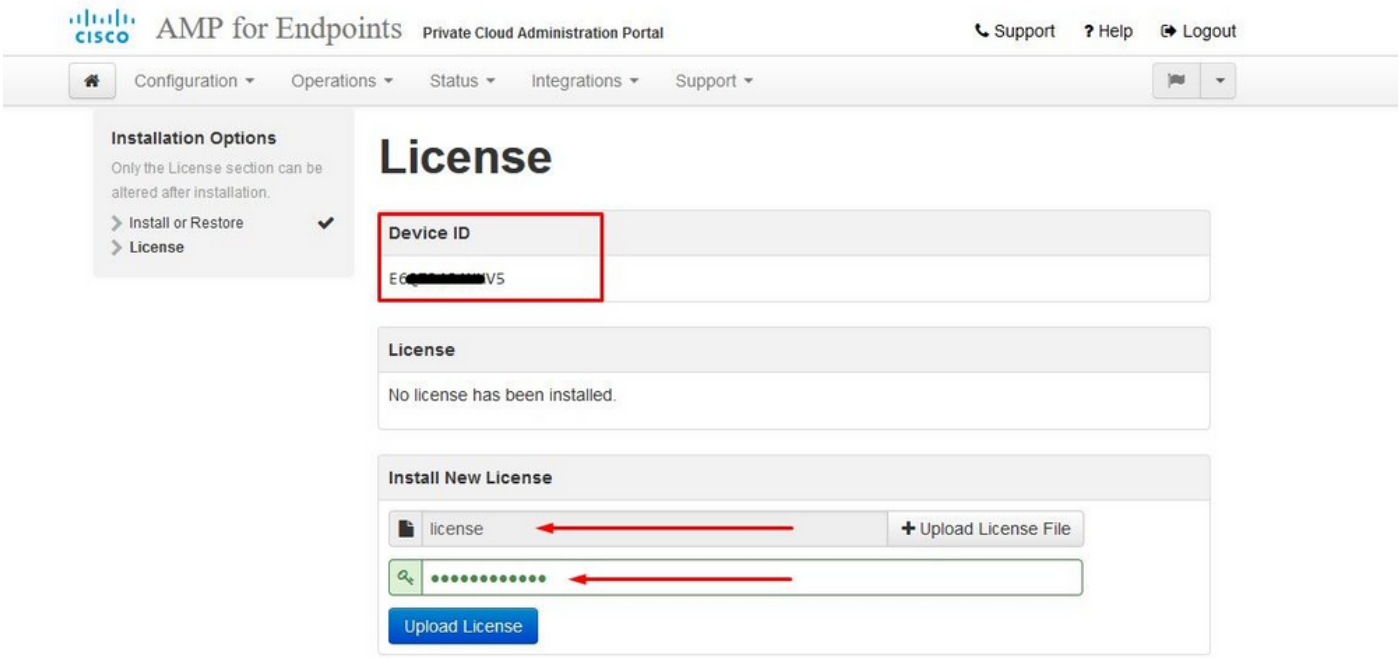
Passo 5:

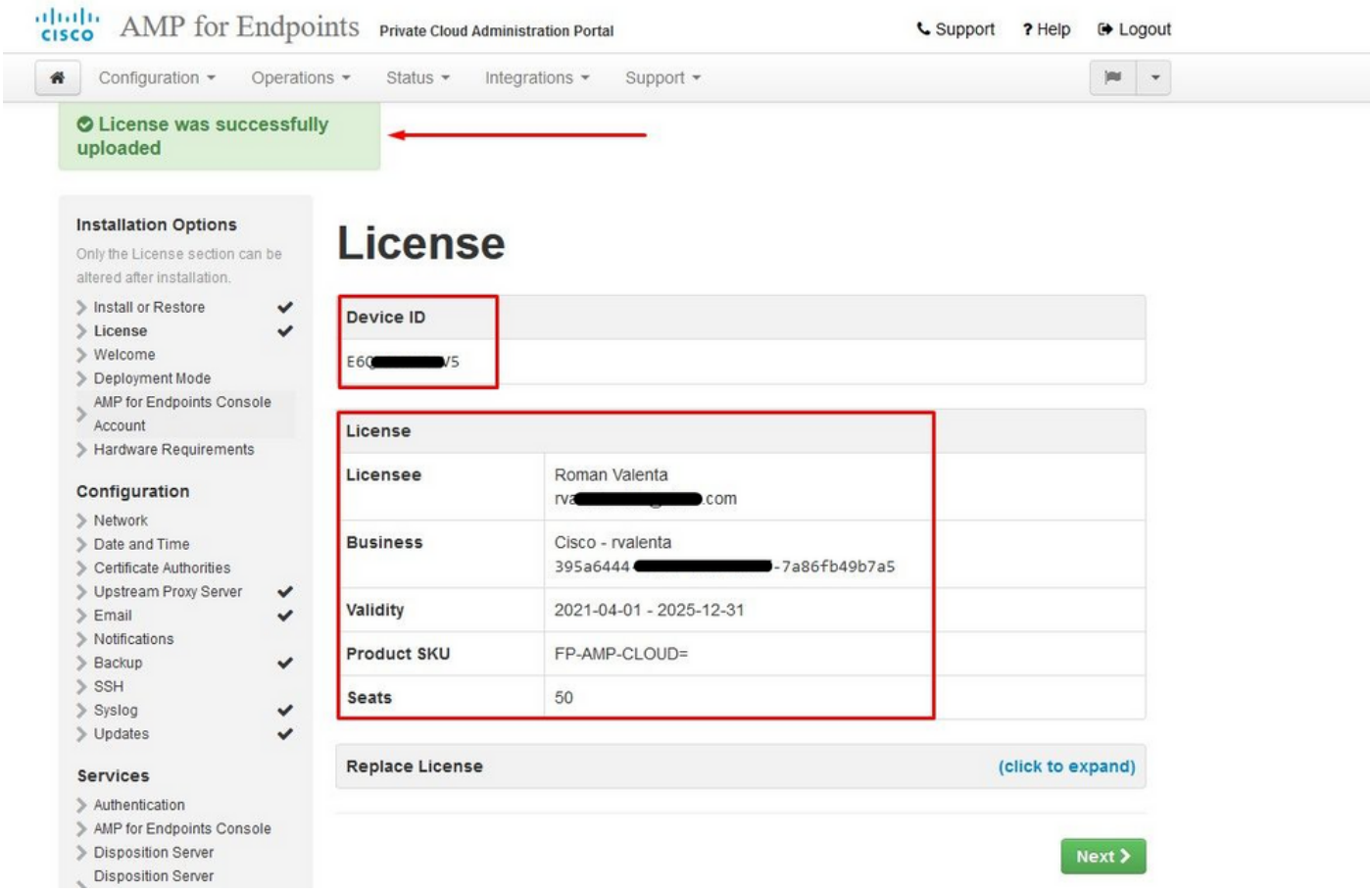
Depois de aceitar o contrato, você obtém a tela de instalação, como mostrado na imagem. Se quiser restaurar a partir de um backup, você pode fazer isso aqui. No entanto, este guia continua com a opção Clean Installation. Selecione Start na seção Clean Installation.



Passo 6:

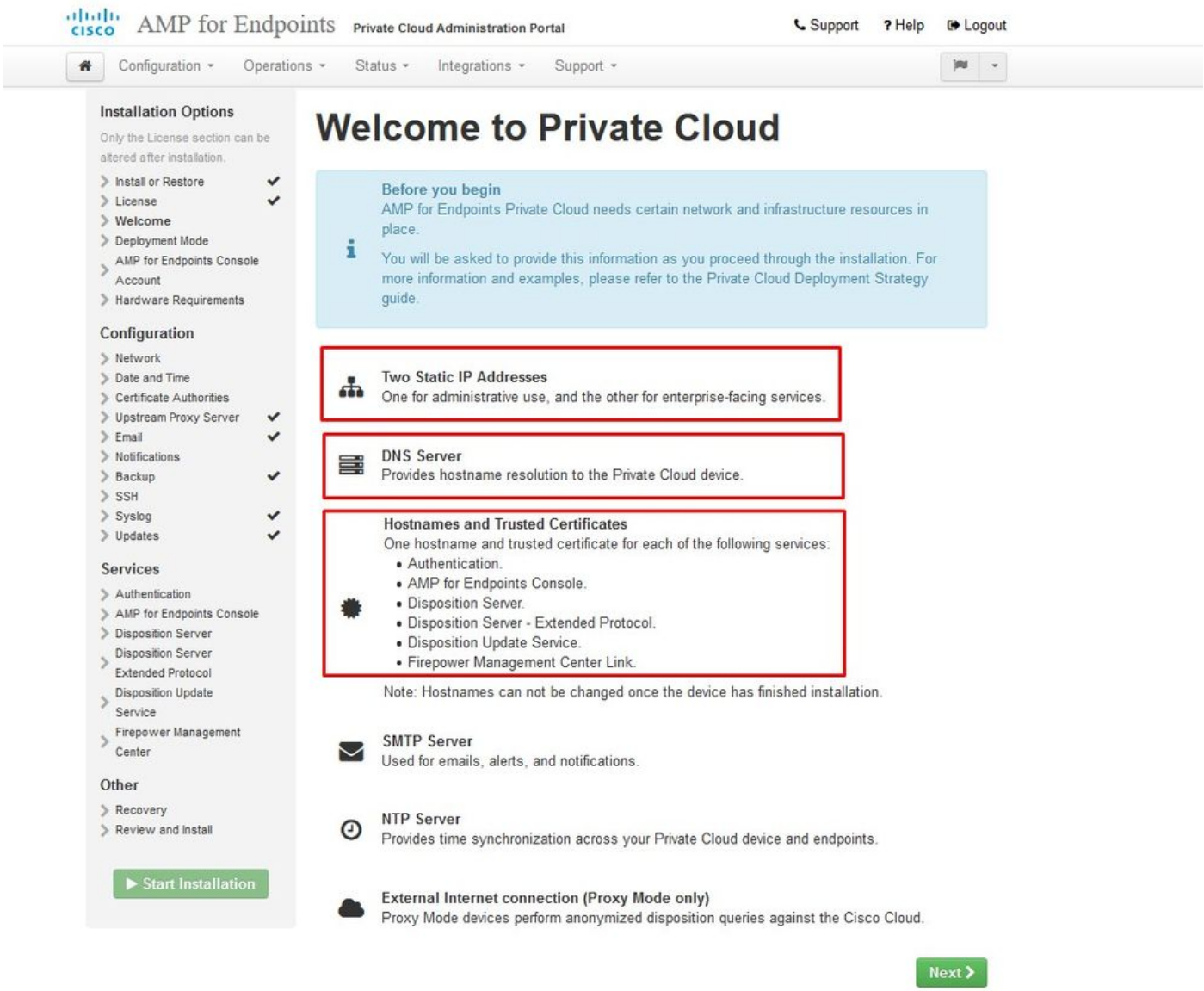
A primeira coisa de que você precisa é licença para até mesmo seguir em frente. Você recebe uma licença e uma senha ao adquirir o produto. Selecione on +Upload License File. Escolha o arquivo de licença e insira a senha. Selecione Upload License. Se o carregamento não for bem-sucedido, verifique se a senha está correta. Se o carregamento for bem-sucedido, uma tela com informações de licença válidas será exibida. Selecione Avançar. Se você ainda não conseguir instalar sua licença, entre em contato com o Suporte Técnico da Cisco.





Passo 7:

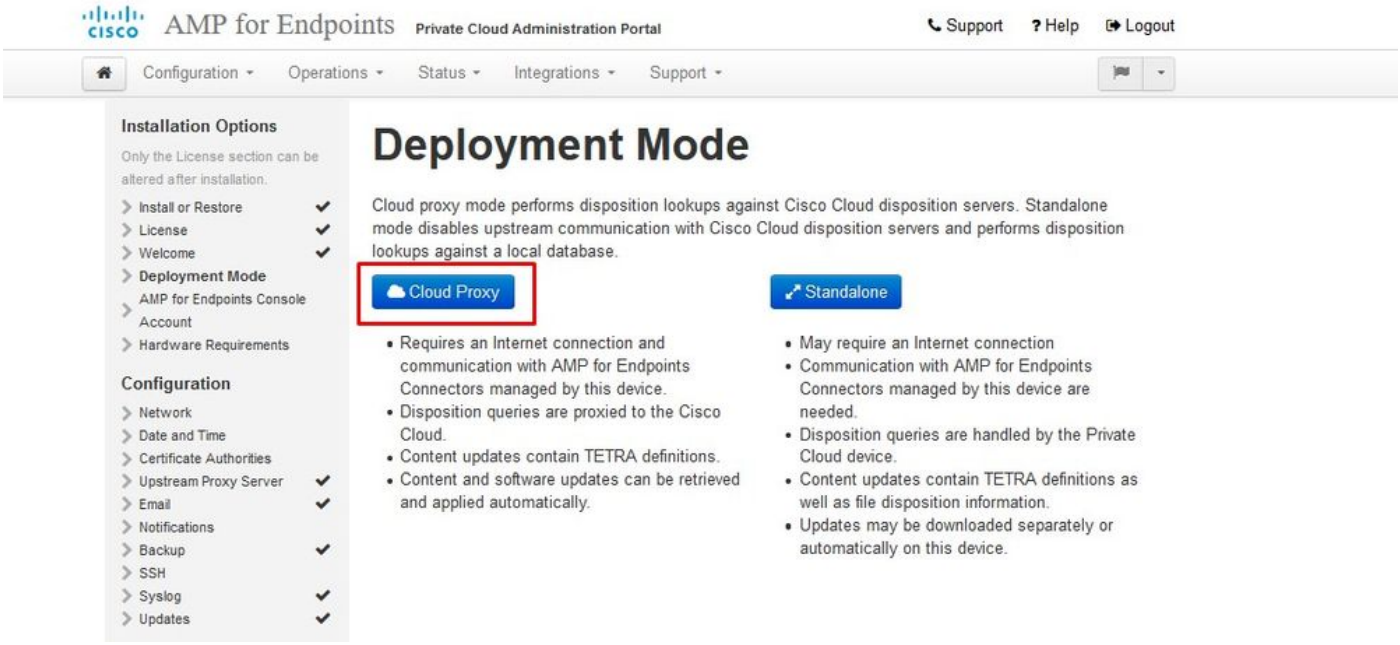
Você recebe a página de boas-vindas, como mostrado na imagem. Esta página mostra as informações que você deve ter antes da configuração da nuvem privada. Leia atentamente os requisitos. Selecione Avançar para iniciar a configuração de pré-instalação.



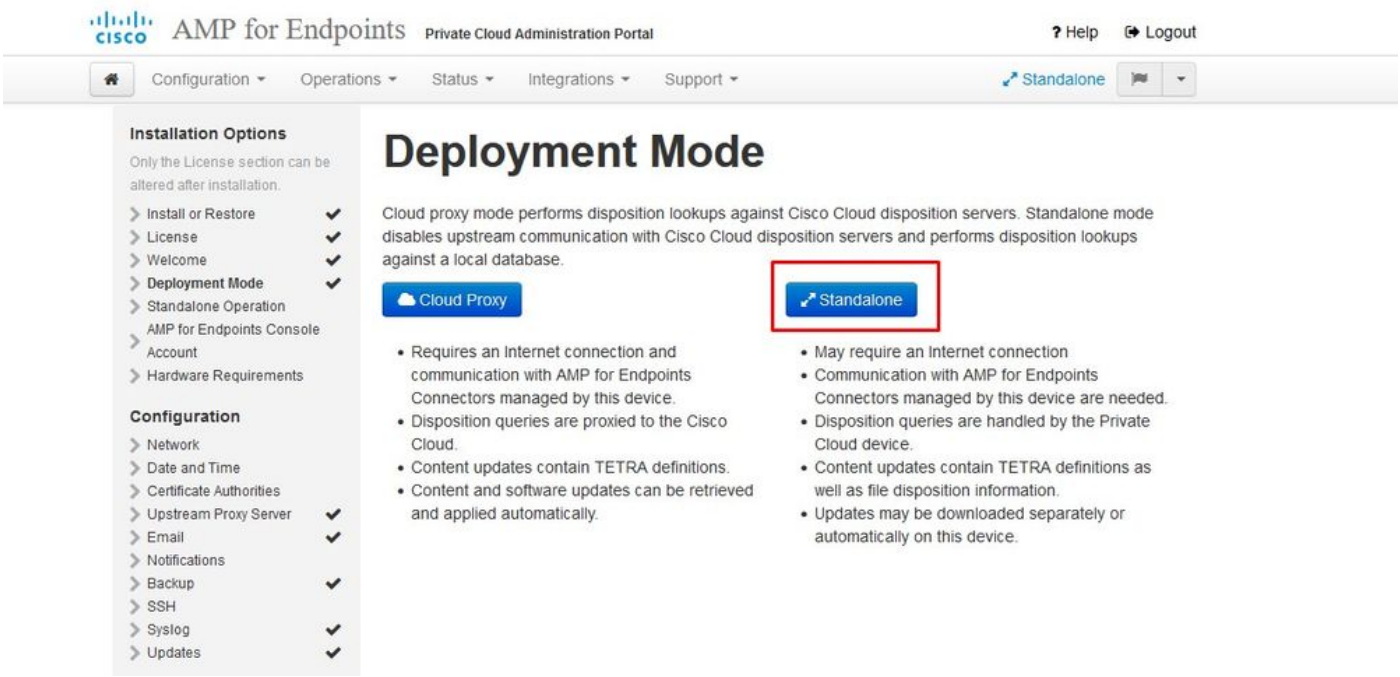
Configuração

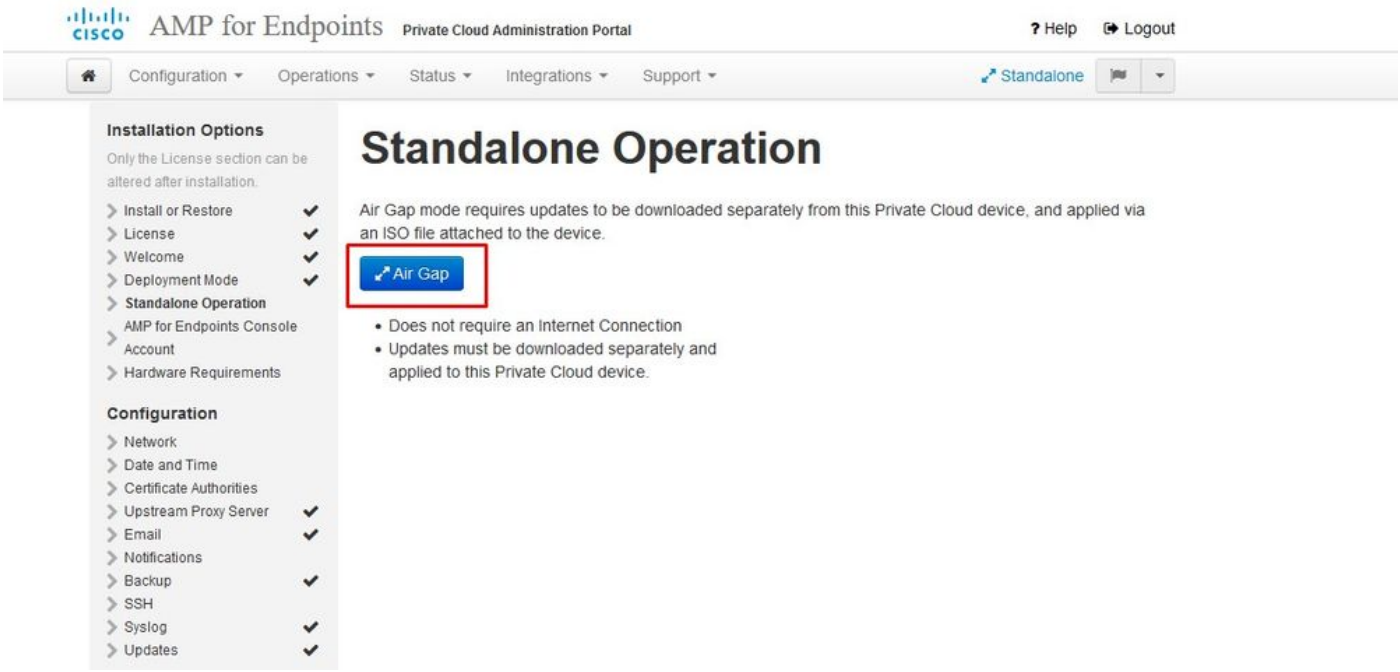
Passo 1:

Observação: observe que nos próximos conjuntos de slides incluímos alguns exclusivos, conforme mostrado na imagem, que são exclusivos apenas para o modo AIR GAP , que devem ser incluídos e marcados como AIRGAP ONLY



⩔⩔ AIRGAP SOMENTE ⩔⩔

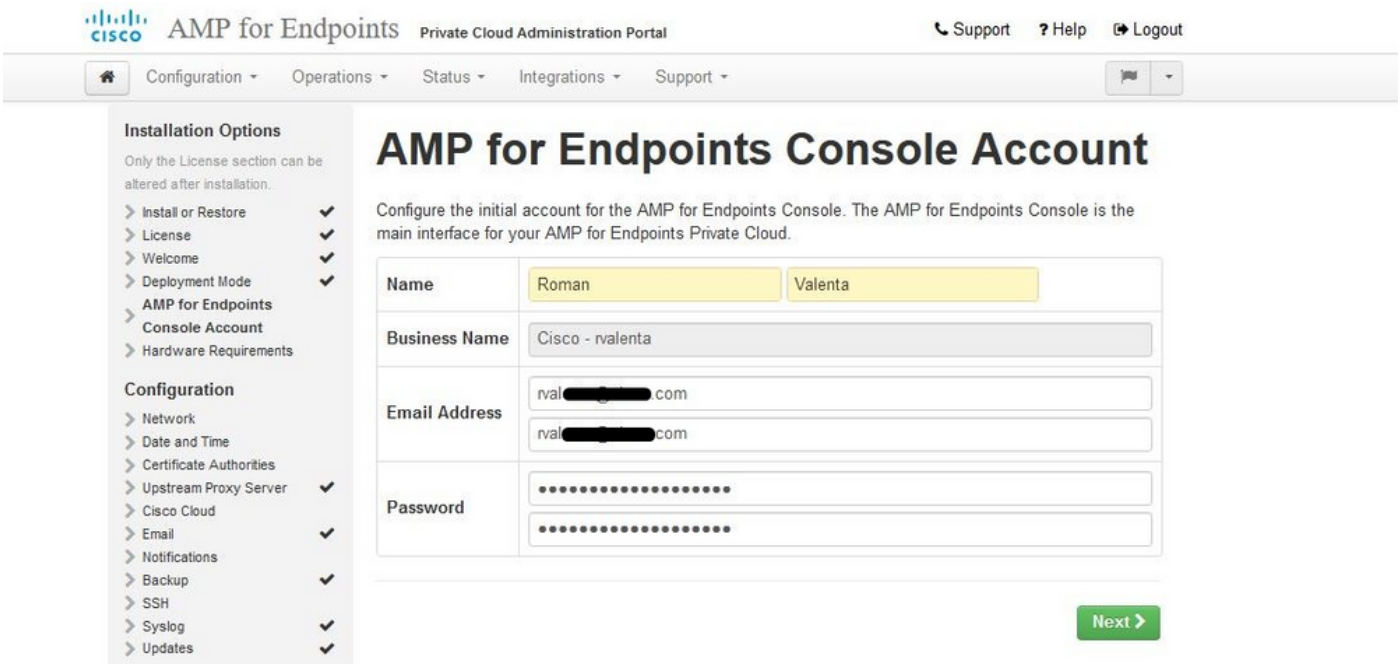




⩓ ⩓ AIRGAP APENAS ⩓ ⩓

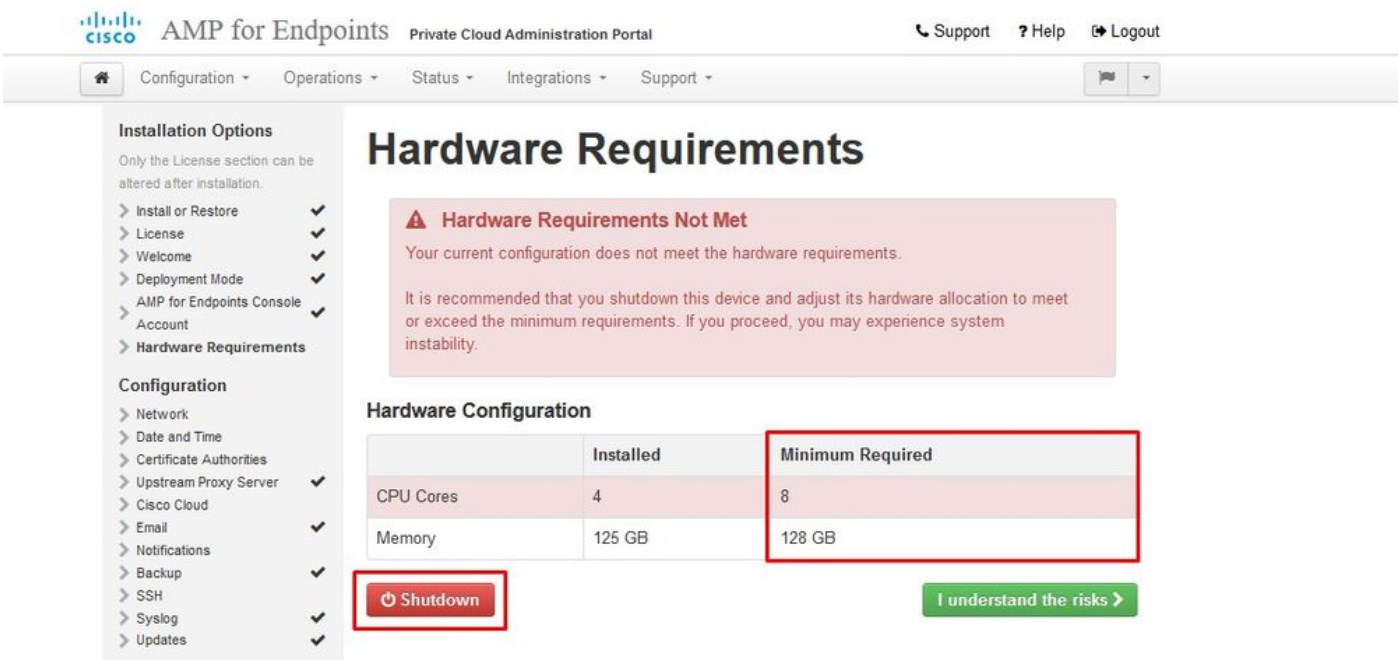
Passo 2:

Navegue até a página Conta do Console do Secure Endpoint. Um usuário administrativo é usado para o console criar políticas, grupos de computadores e adicionar outros usuários. Insira o nome, o endereço de e-mail e a senha da conta do console. Selecione Avançar.

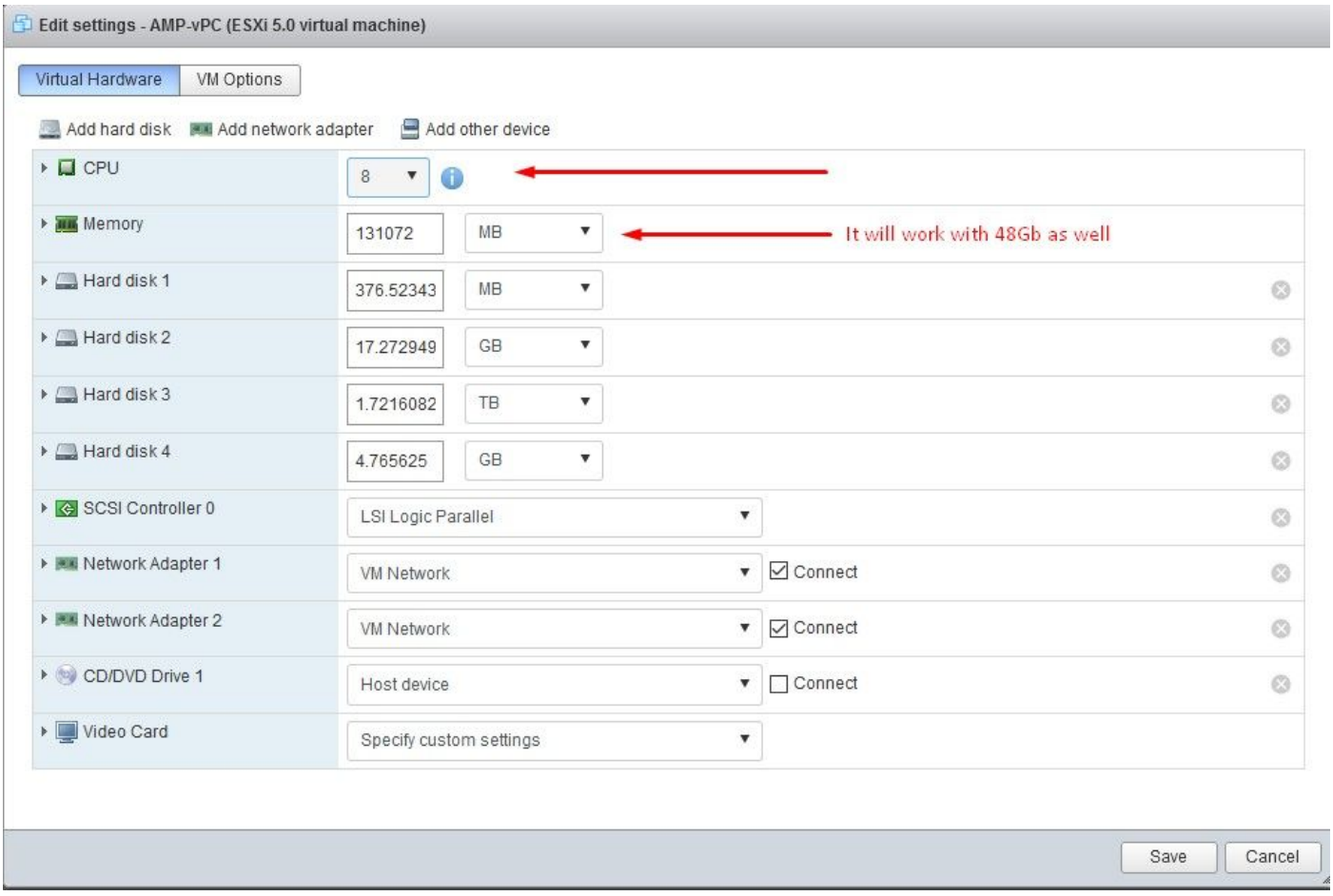


Se você se deparar com esse problema ao implantar a partir do arquivo OVA, terá duas opções: continuar e corrigir esse problema mais tarde ou desligar em seguida para a VM implantada e ajustar de acordo. Após a reinicialização, você continua do ponto em que estava.

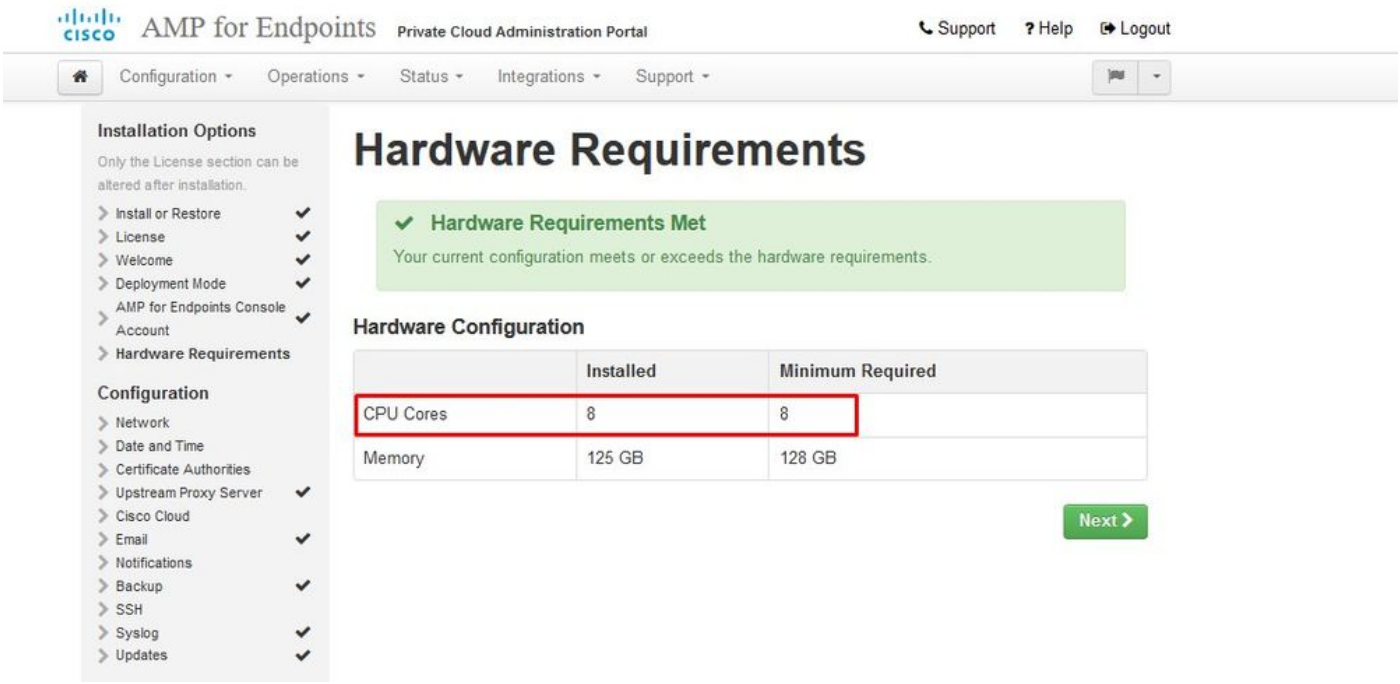
Observação: isso foi corrigido no arquivo OVA para a versão 3.5.2, que é carregada corretamente com 128 GB RAM e 8 núcleos de CPU



Observação: use apenas valores recomendados, a menos que isso seja para fins de laboratório



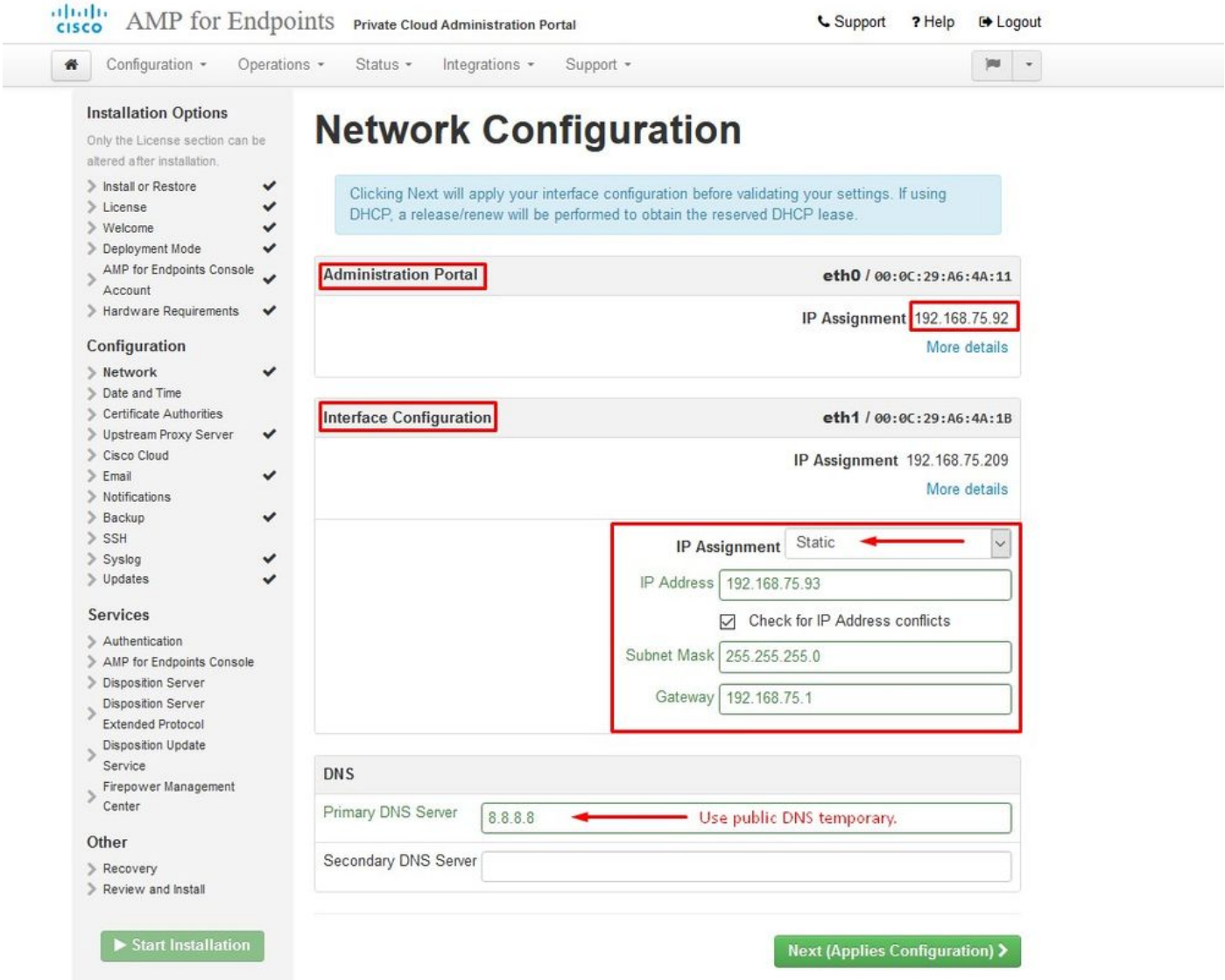
Uma vez reiniciados, continuamos de onde paramos.



Certifique-se de configurar o ETH1 com o IP ESTÁTICO também.

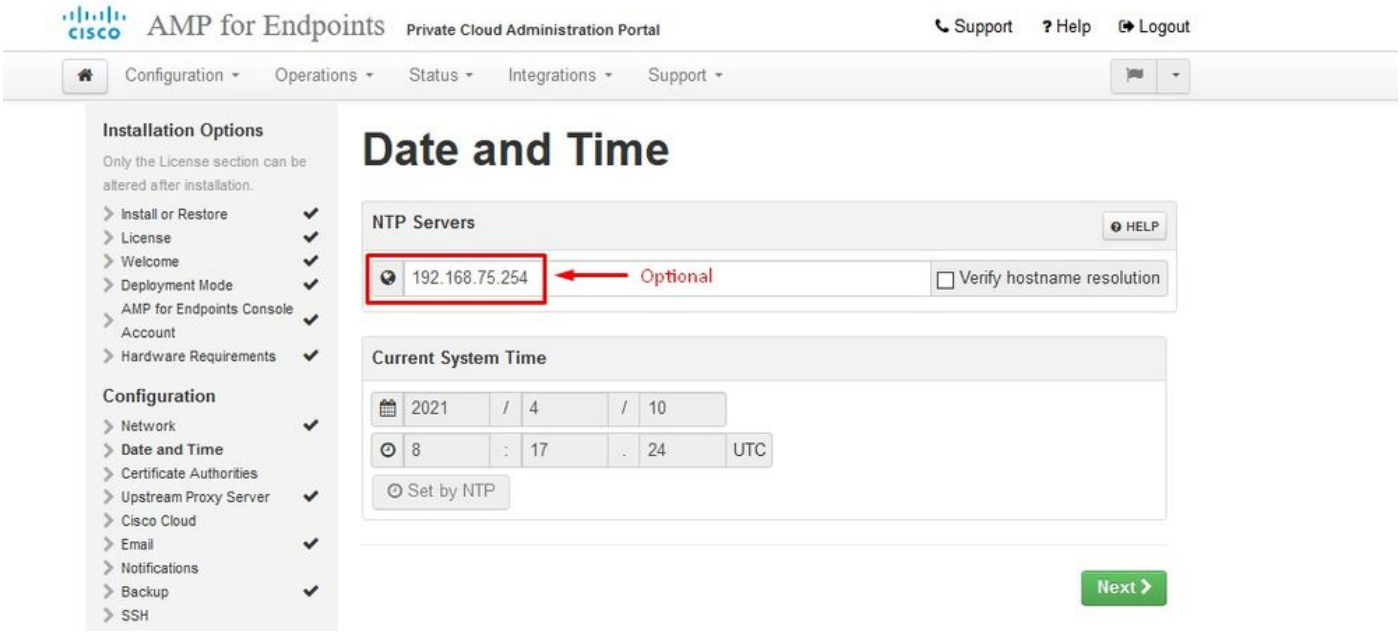
Observação: você nunca deve configurar seu dispositivo para usar DHCP, a menos que tenha criado reservas de endereço MAC para as interfaces. Se os endereços IP de suas interfaces mudarem, isso poderá causar sérios problemas com os Conectores de Ponto de Extremidade Seguro implantados. Se o servidor DNS não estiver configurado, você poderá usar o DNS público temporário para concluir a instalação.

Passo 3:

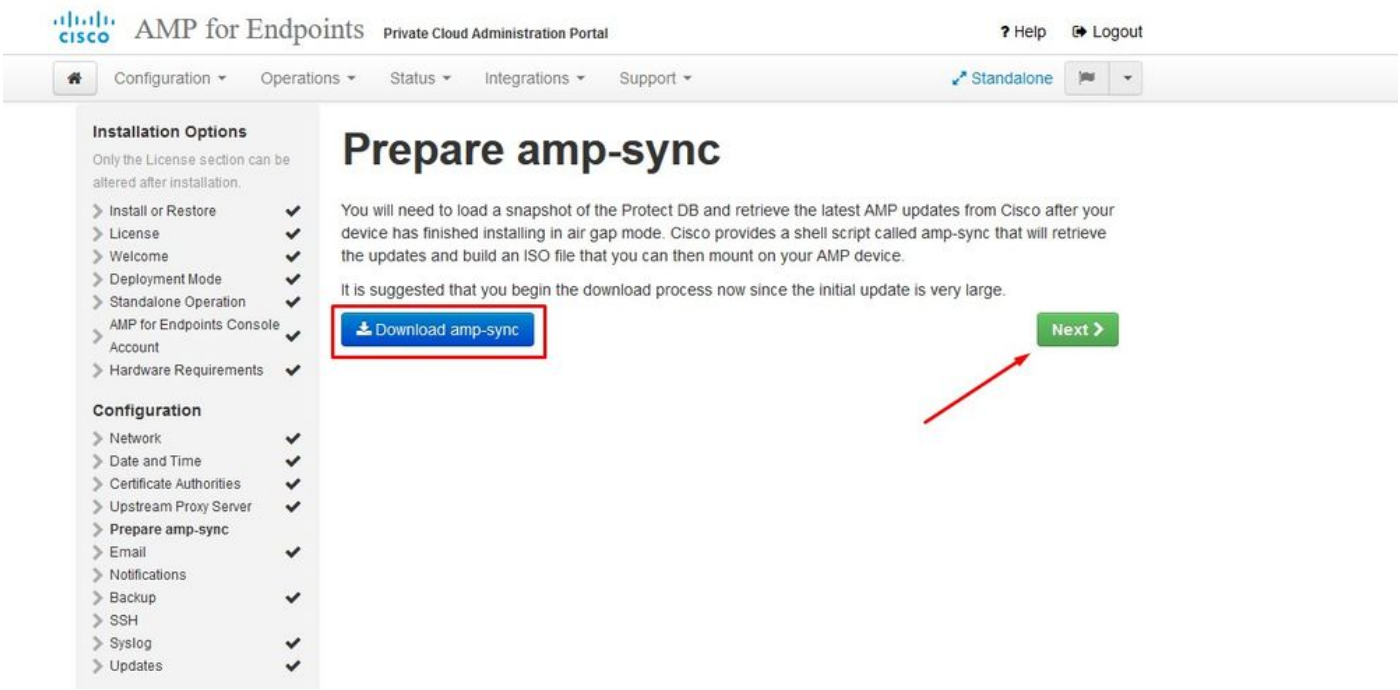


Passo 4:

Você obtém a página Data e hora. Insira os endereços de um ou mais servidores NTP que deseja usar para a sincronização de Data e Hora. Você pode usar servidores NTP internos ou externos e especificar mais de um por meio de uma lista delimitada por vírgula ou espaço. Sincronize o horário com seu navegador ou execute o amp-ctl ntpdate no console do dispositivo para forçar uma sincronização imediata com seus servidores NTP. Selecione Avançar.



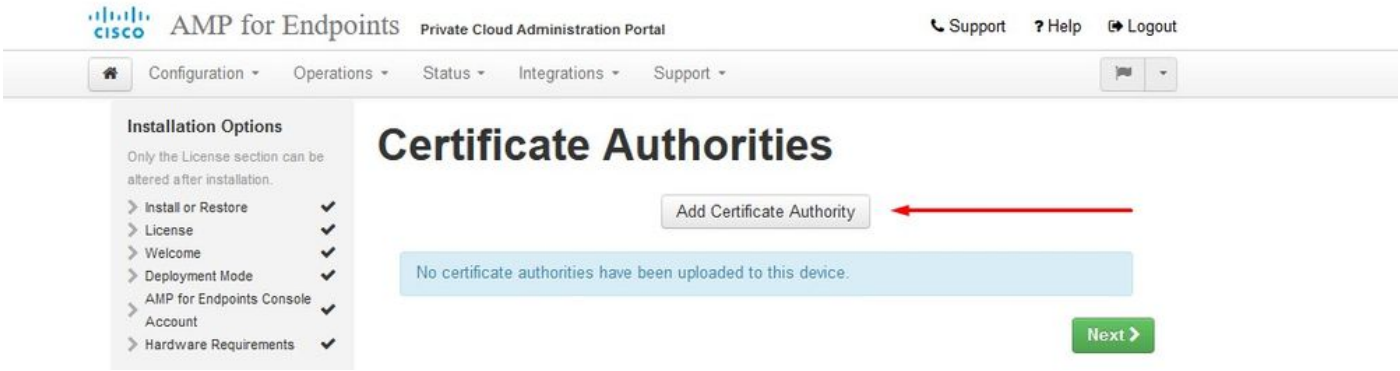
⩔⩔ AIRGAP SOMENTE ⩔⩔

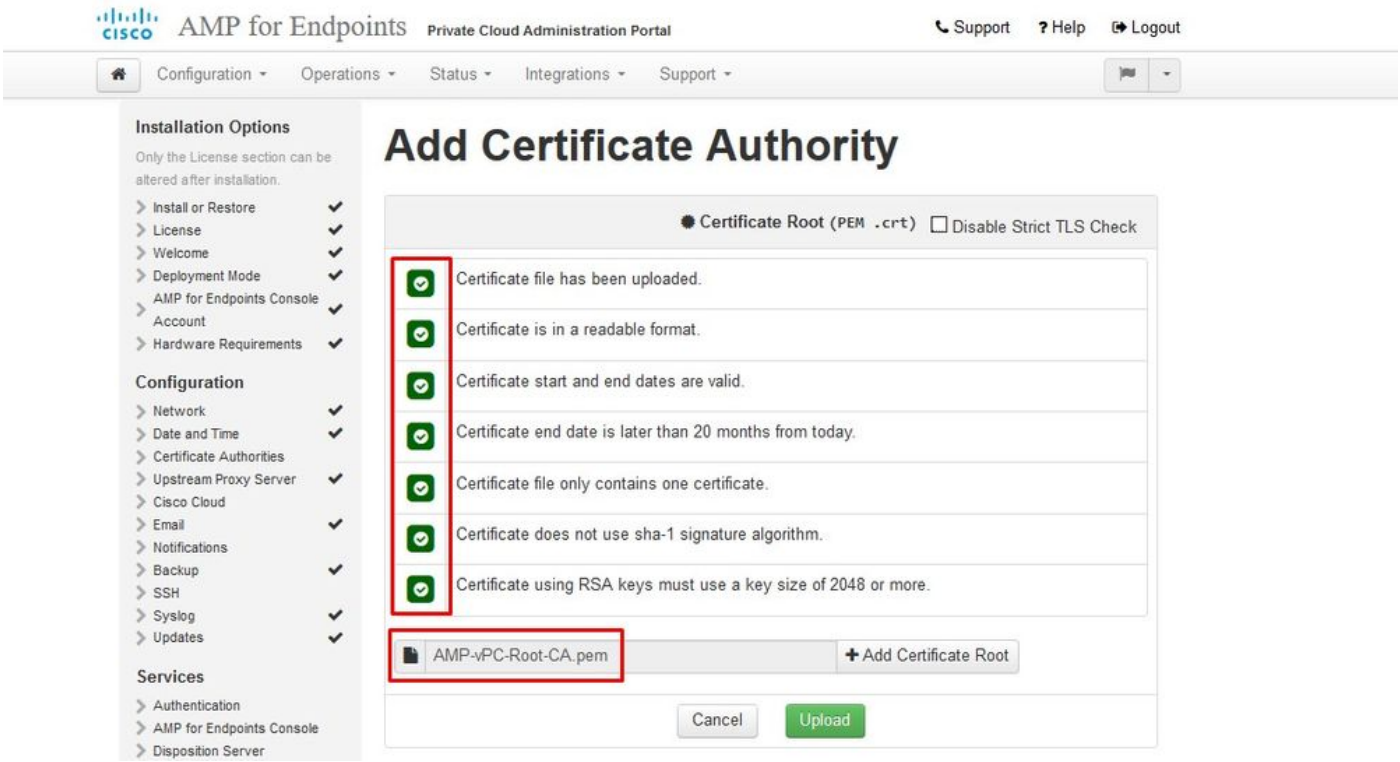


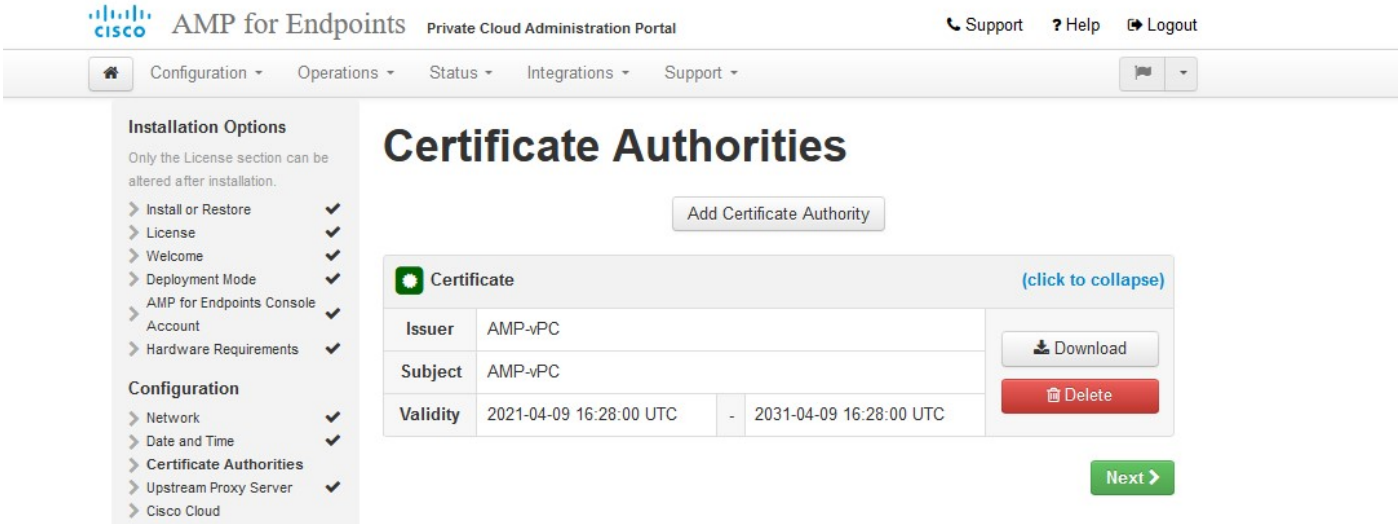
⩓⩓ AIRGAP APENAS ⩓⩓

Passo 5:

A página Autoridades de certificação é exibida, conforme mostrado na imagem. Selecione em Adicionar autoridade de certificação para adicionar seu certificado raiz.



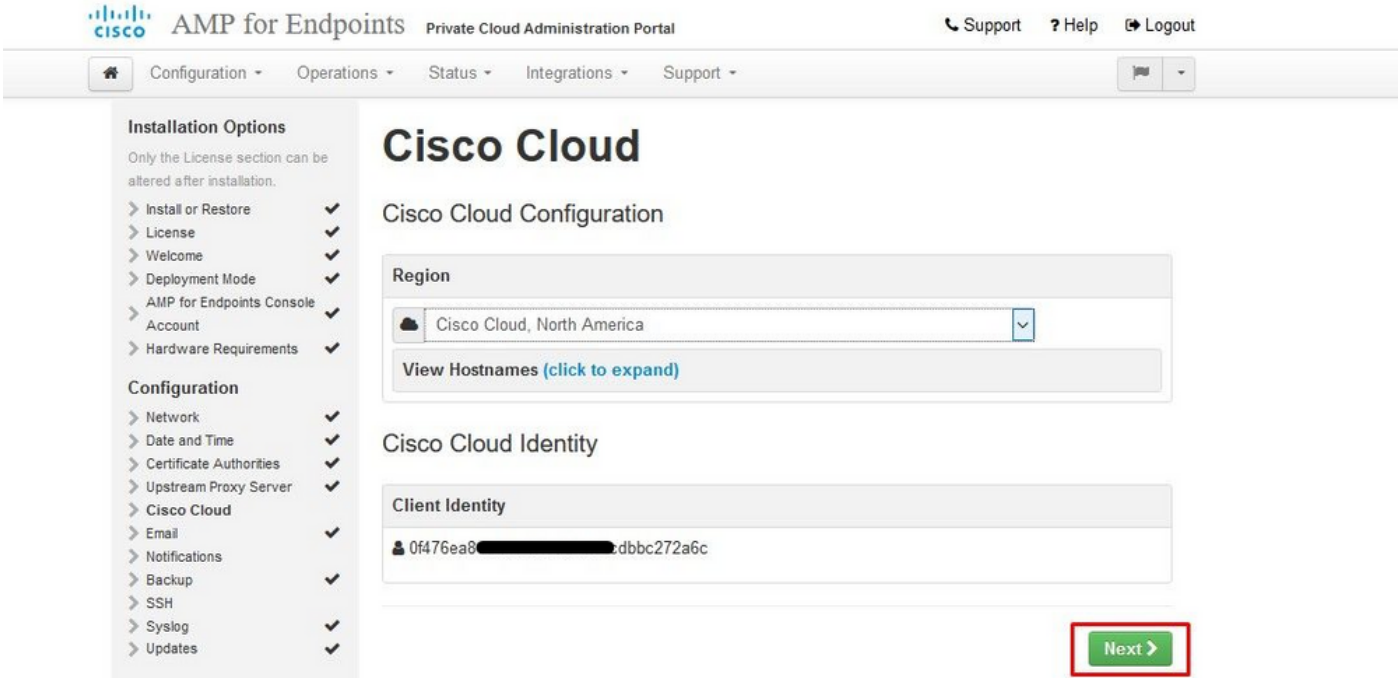




Passo 6:

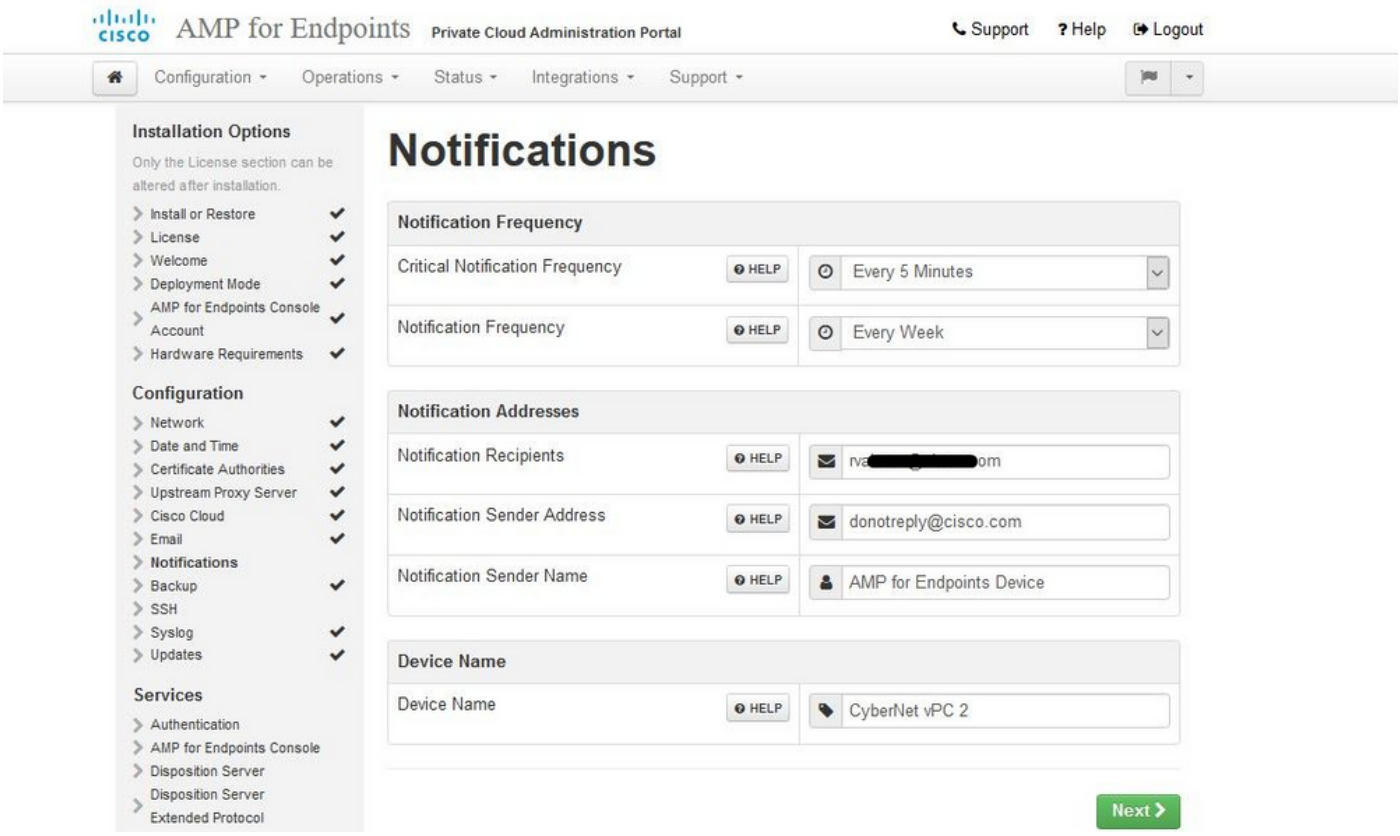
A próxima etapa é configurar a página do Cisco Cloud, como mostrado na imagem. Selecione a região de nuvem da Cisco apropriada. Expanda View Hostnames se precisar criar exceções de

firewall para seu dispositivo Secure Endpoint Private Cloud se comunicar com o Cisco Cloud para pesquisas de arquivos e atualizações de dispositivos. Selecione Avançar.



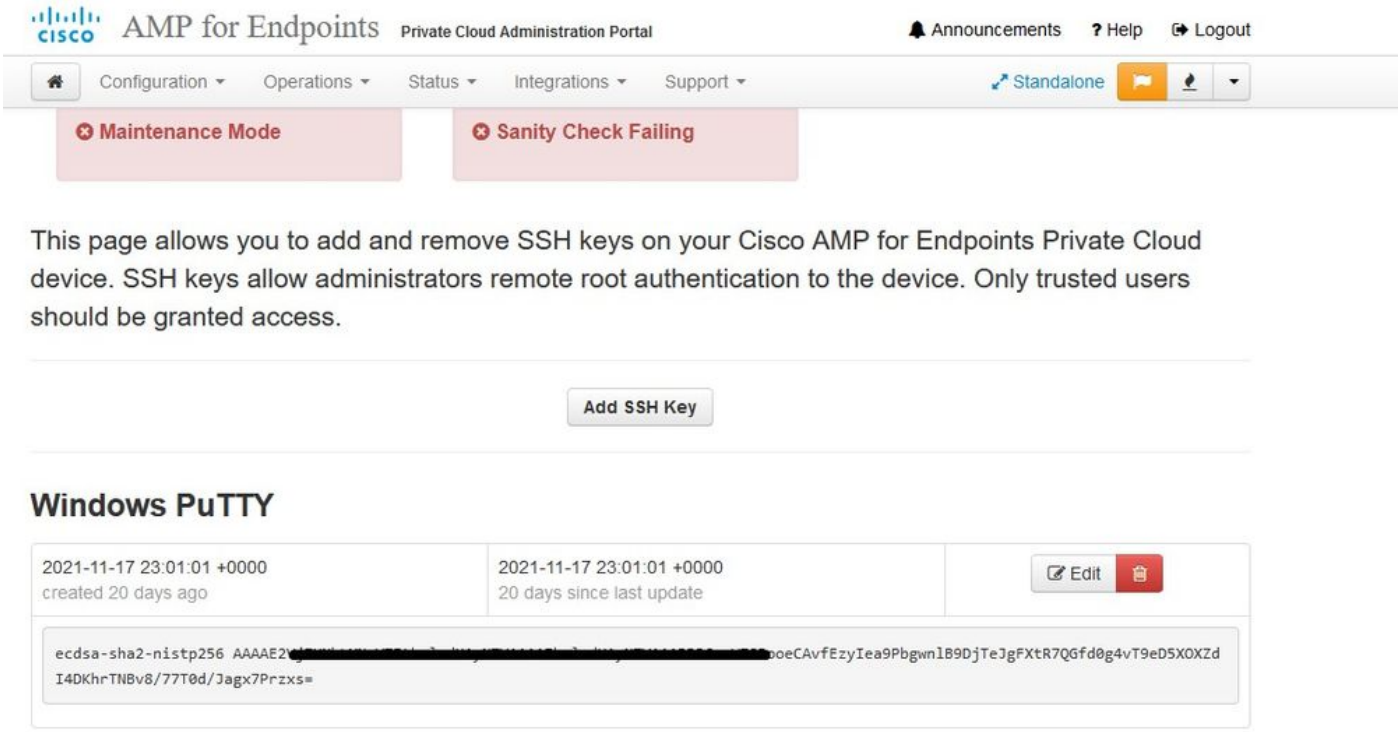
Passo 7:

Navegue até a página de notificações, conforme mostrado na imagem. Selecione a frequência para Notificações críticas e regulares. Digite os endereços de e-mail que você deseja receber notificações de alerta para o dispositivo Secure Endpoint. Você pode usar aliases de email ou especificar vários endereços por meio de uma lista separada por vírgulas. Você também pode especificar o nome do remetente e o endereço de email usados pelo dispositivo. Essas notificações não são iguais às assinaturas do Console de endpoint seguro. Você também pode especificar um nome de dispositivo exclusivo se tiver vários dispositivos Secure Endpoint Private Cloud. Selecione Avançar.



Passo 8:

Em seguida, navegue até a página Chaves SSH, como mostrado na imagem. Selecione em Add SSH Key para inserir as chaves públicas que você deseja adicionar ao dispositivo. As chaves SSH permitem que você acesse o dispositivo através de um shell remoto com privilégios de raiz. Somente usuários confiáveis devem receber acesso. Seu dispositivo de nuvem privada requer uma chave RSA formatada com OpenSSH. Você pode adicionar mais chaves SSH posteriormente por meio de Configuração > SSH no Portal de Administração. Selecione Avançar.



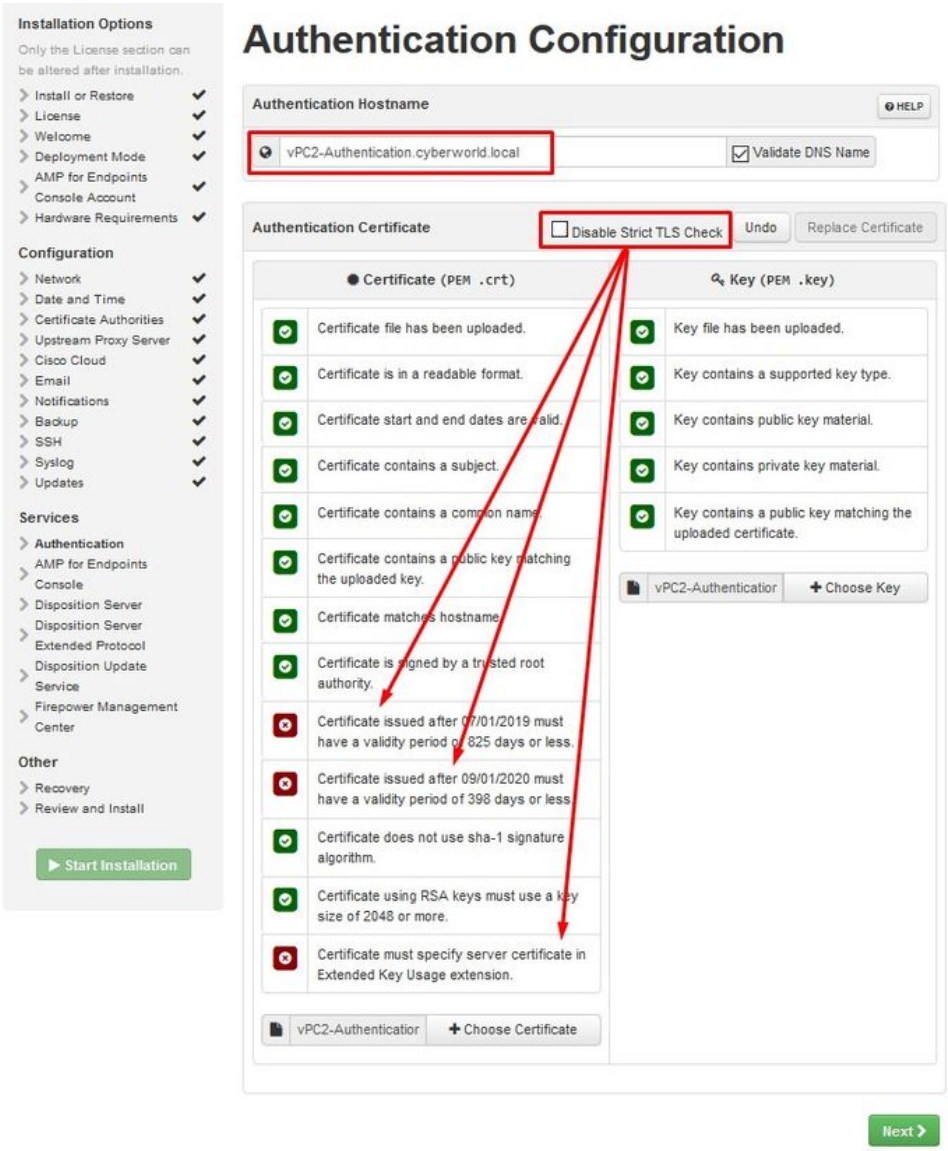
Em seguida, você obterá a seção Serviços. Nas próximas páginas, você precisa atribuir nomes de host e carregar o certificado e os pares de chaves apropriados para esses serviços de dispositivo. Nos próximos slides, veremos a configuração de um dos 6 certificados.

Services

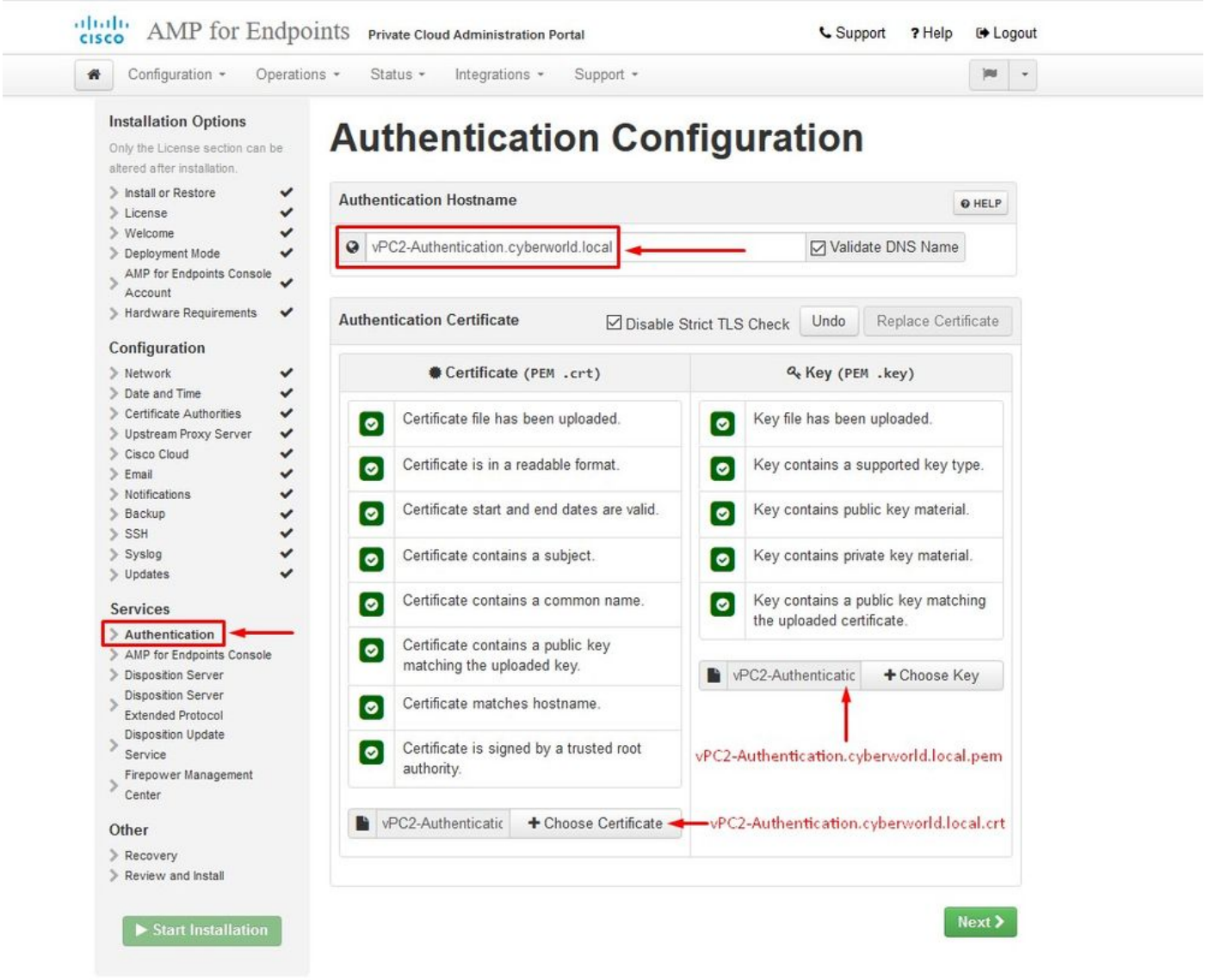
Passo 1:

Durante o processo de configuração, você pode se deparar com esses erros.

O primeiro "erro" que você poderá observar é realçado com as 3 setas. Para ignorar isso, basta desmarcar "Desabilitar verificação TLS estrita"



Sem verificação TLS rigorosa

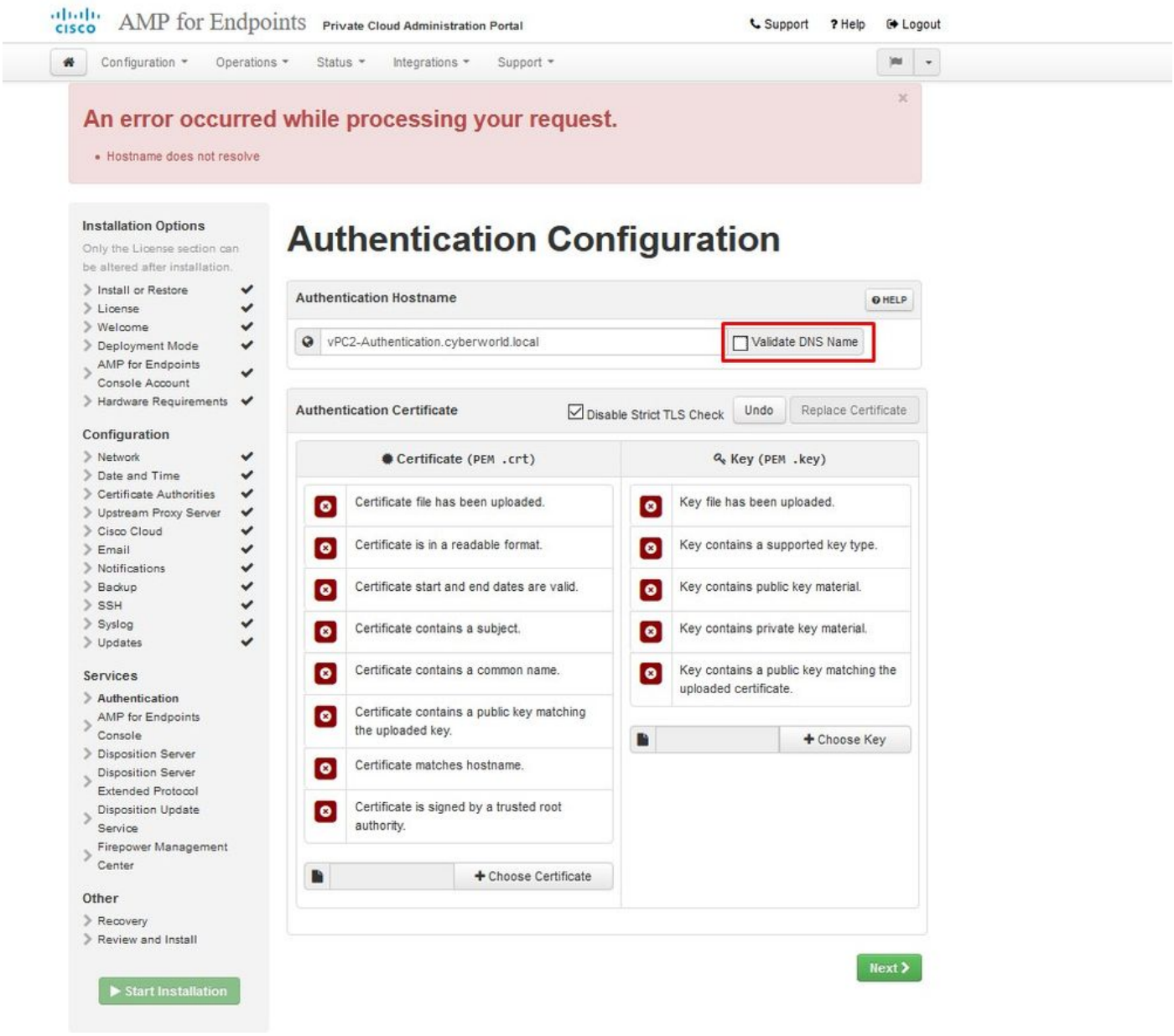


Passo 2:

O próximo erro ocorre se você deixar a opção "Validar nome DNS" marcada. Aqui você tem duas opções.

#1: Desmarque a marca de seleção Validar DNS

#2: Retorne ao Servidor DNS e configure o restante dos registros do host.



Agora repita o mesmo processo mais cinco vezes para o restante dos certificados.

Autenticação

- O serviço de Autenticação pode ser usado em versões futuras da Nuvem Privada para lidar com a autenticação de usuário.

Console de endpoint seguro

- Console é o nome DNS no qual o administrador do Secure Endpoint pode acessar o Secure Endpoint Console e os Secure Endpoint Connectors recebem novas políticas e atualizações.

Servidor de disposição

- Servidor de disposição é o nome DNS em que os conectores de endpoint seguro enviam e recuperam informações de pesquisa na nuvem.

Servidor de descarte - Protocolo estendido

- Servidor de disposição - Protocolo estendido é o nome DNS onde os conectores de ponto de extremidade seguro mais recentes enviam e recuperam informações de pesquisa na nuvem.

Serviço de atualização de disposição

- O Disposition Update Service é usado quando você vincula um dispositivo do Cisco Threat Grid ao dispositivo de nuvem privada. O dispositivo Threat Grid é usado para enviar arquivos para análise a partir do Console de endpoint seguro e o Serviço de atualização de descarte é usado pelo Threat Grid para atualizar a disposição (limpa ou mal-intencionada) dos arquivos depois que eles forem analisados.

Firepower Management Center

-O Firepower Management Center Link permite vincular um dispositivo Cisco Firepower Management Center (FMC) ao dispositivo de nuvem privada. Isso permite exibir dados do Secure Endpoint no painel do FMC. Para obter mais informações sobre a integração do FMC com o Secure Endpoint, consulte a documentação do FMC.

⚠ Cuidado: os nomes de host não podem ser alterados depois que o dispositivo tiver concluído a instalação.

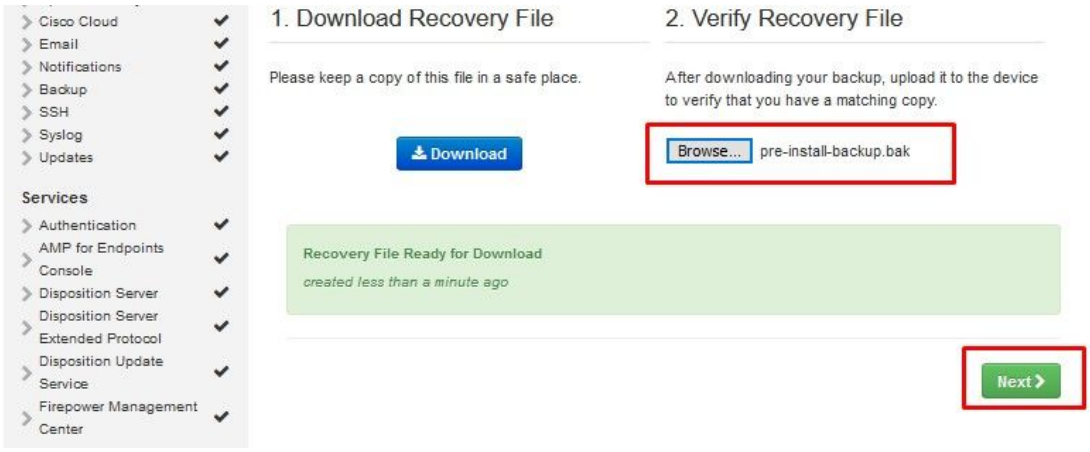
Anote os nomes de host necessários. Você precisa criar seis registros DNS A exclusivos para a Secure Endpoint Private Cloud. Cada registro aponta para o mesmo endereço IP da interface do Virtual Private Cloud Console (eth1) e deve ser resolvido pela nuvem privada e pelo endpoint seguro.

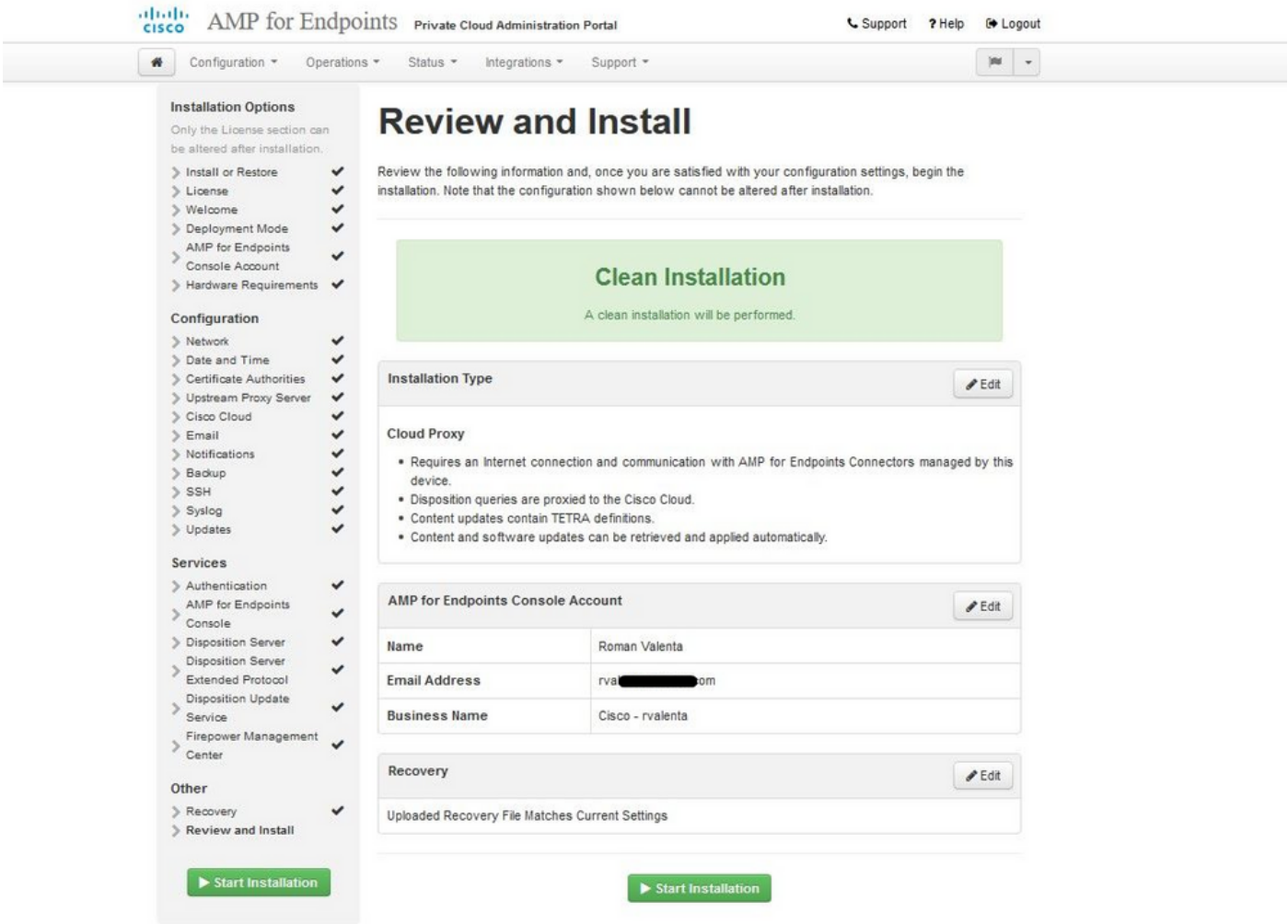
Passo 3:

Na próxima página, faça o download e verifique o Arquivo de Recuperação.

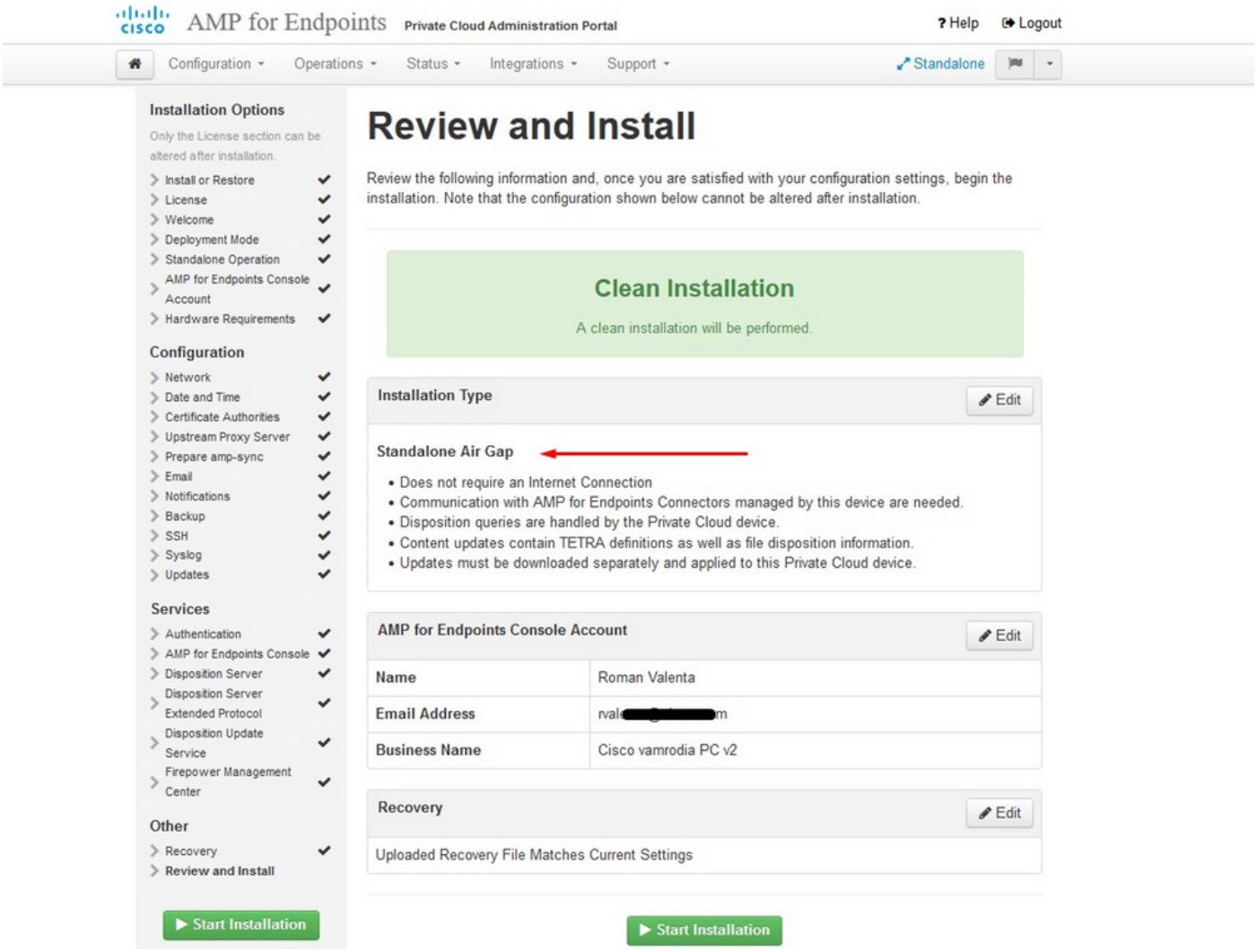
Você obtém a página Recuperação, como mostrado na imagem. Você deve baixar e verificar um backup da sua configuração antes do início da instalação. O arquivo de recuperação contém toda a configuração, bem como as chaves do servidor. Se você perder um arquivo de recuperação, não poderá restaurar sua configuração e todos os conectores do Secure Endpoint deverão ser reinstalados. Sem uma chave original, você precisa reconfigurar toda a infraestrutura de nuvem privada com novas chaves. O arquivo de recuperação contém todas as configurações relacionadas ao portal opadmin. O arquivo de backup contém o conteúdo do arquivo de recuperação, bem como quaisquer dados do portal do painel, como eventos, histórico do conector e assim por diante. Se você deseja restaurar apenas o opadmin sem os dados de evento e tudo, você pode usar o arquivo de recuperação. Se você restaurar a partir do arquivo de backup, os dados do opadmin e do portal do painel serão restaurados.

Selecione em Download para salvar o backup no computador local. Depois que o arquivo tiver sido baixado, selecione Choose File para carregar o arquivo de backup e verificar se ele não está corrompido. Selecione Avançar para verificar o arquivo e continuar.





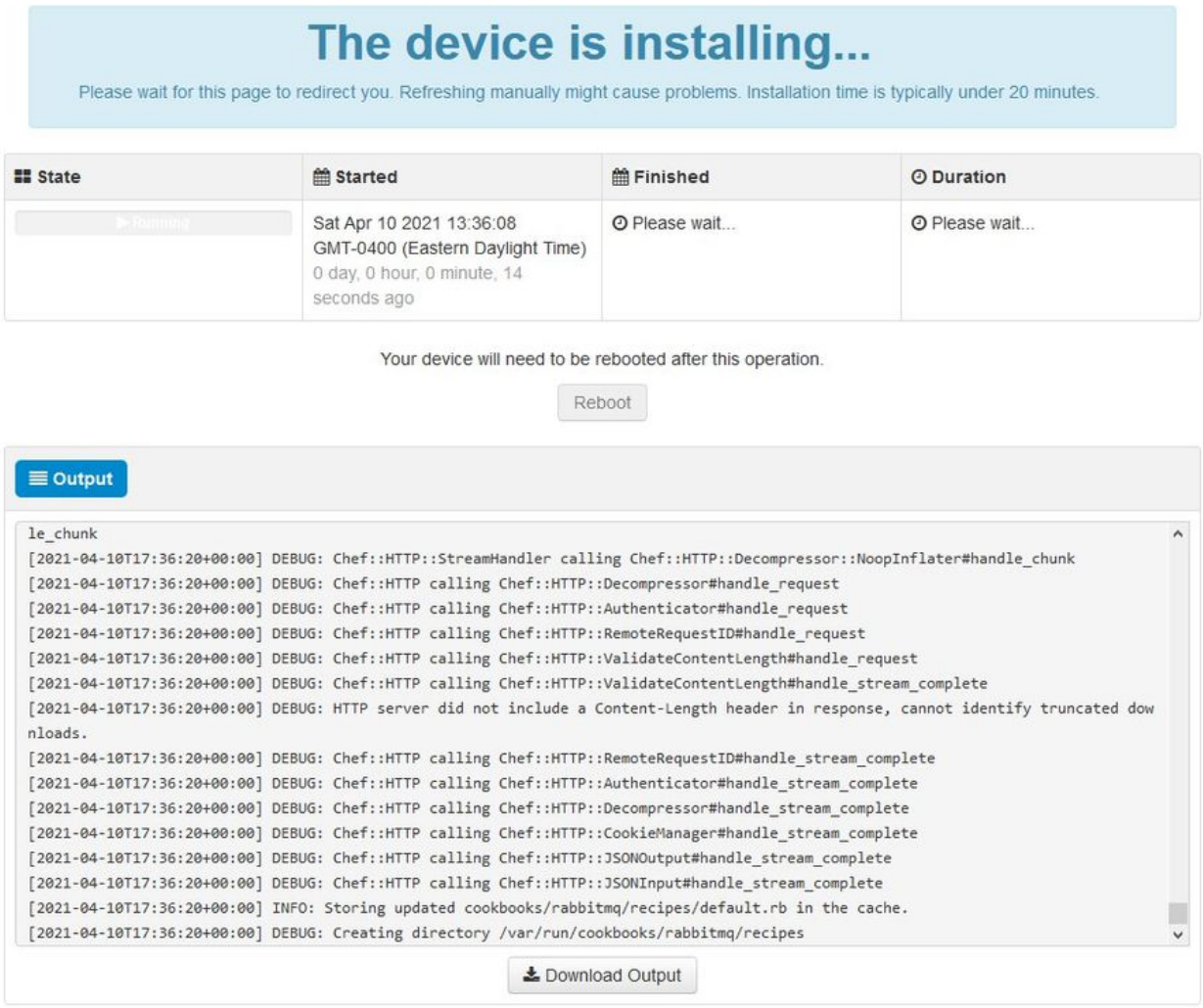
⩔⩔ AIRGAP SOMENTE ⩔⩔



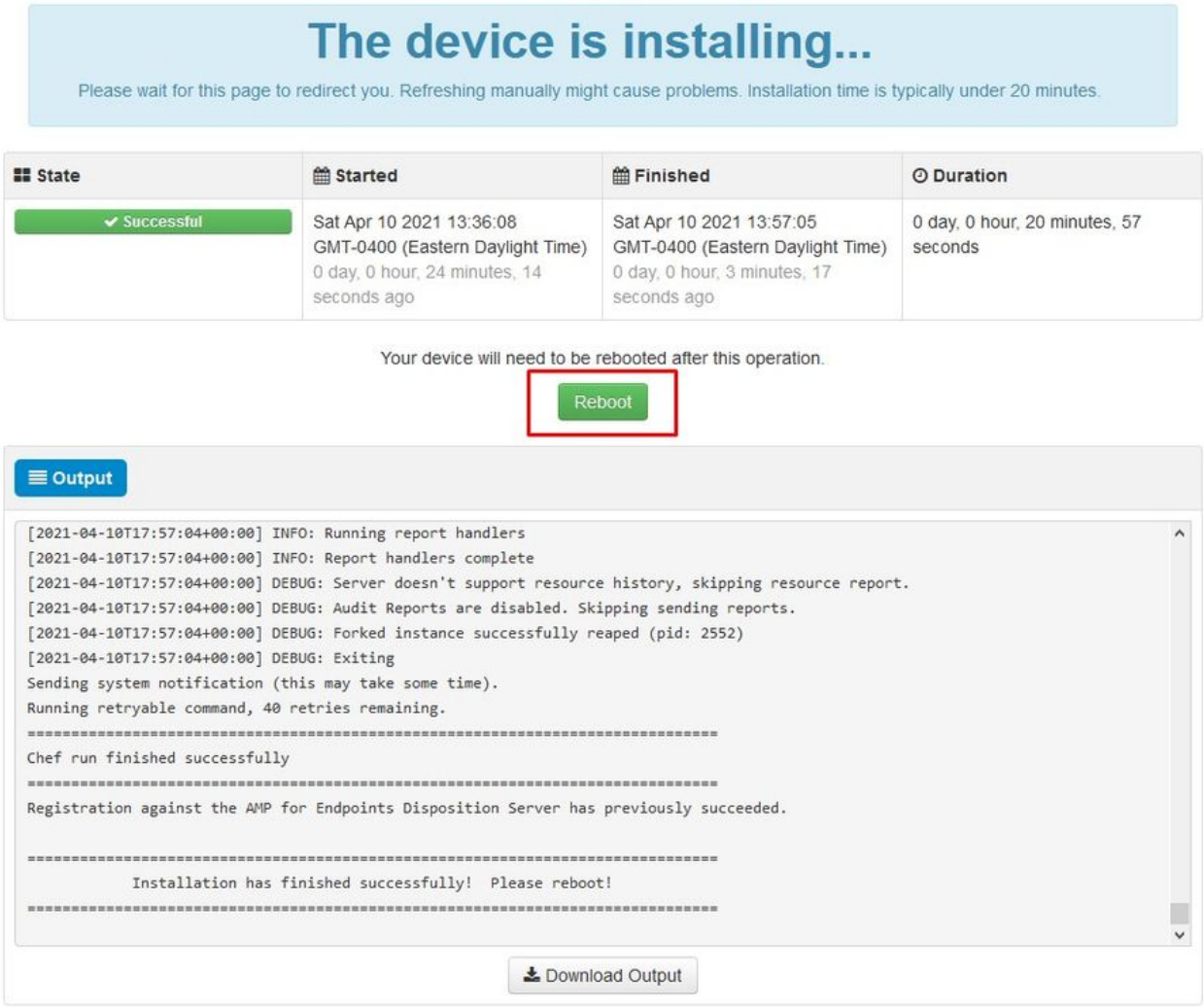
⩓⩓ AIRGAP APENAS ⩓⩓

Você vê uma entrada similar como esta...

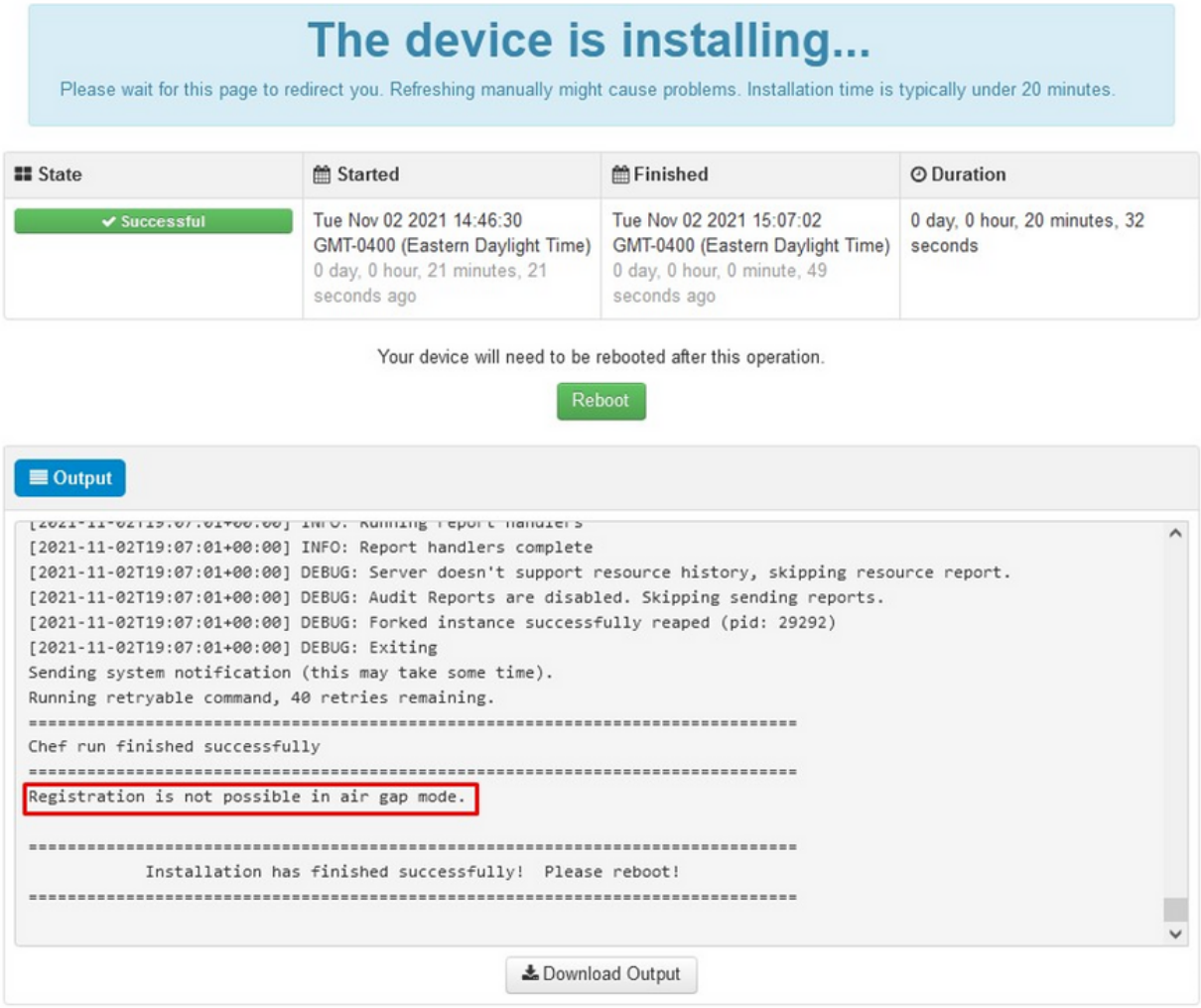
⚠ Cuidado: Quando você estiver nesta página, não atualize, pois isso pode causar problemas.



Após concluir a instalação, pressione o botão de reinicialização

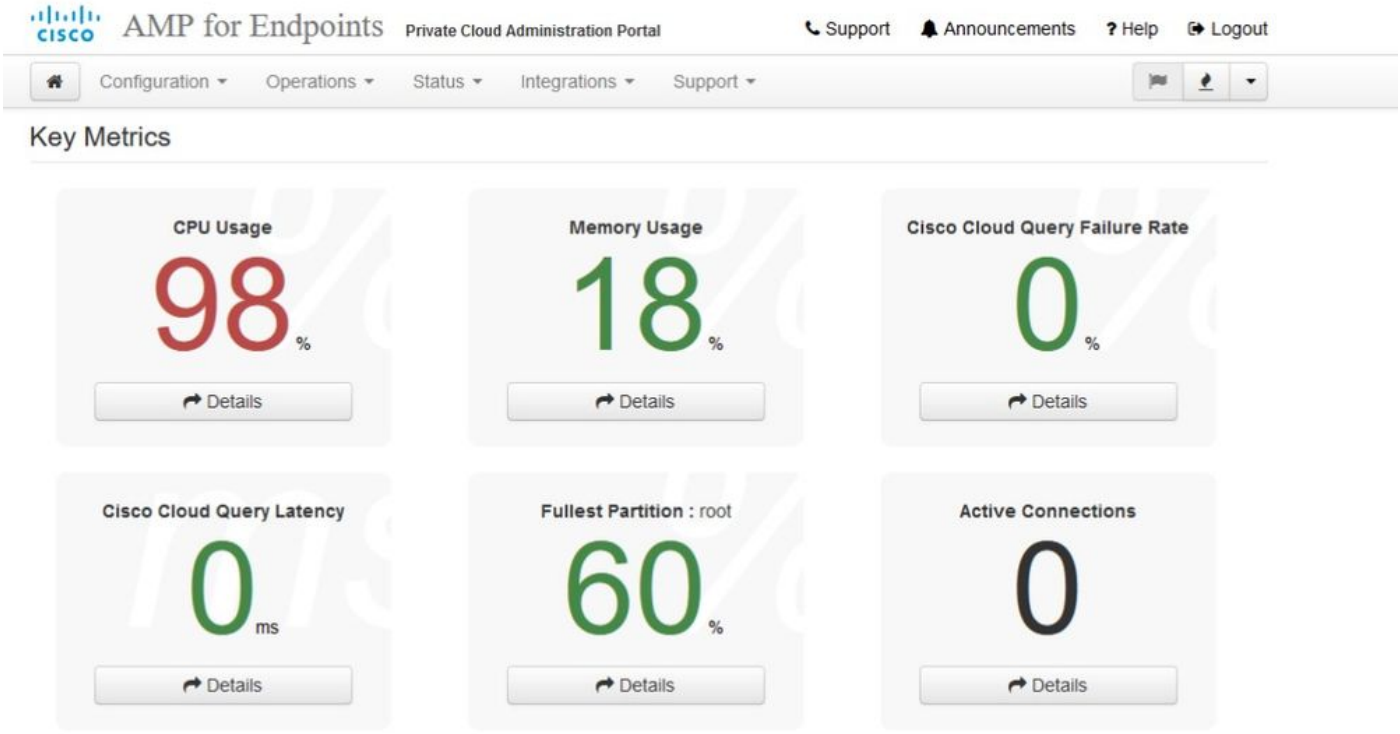


⩔ ⩔ AIRGAP SOMENTE ⩔ ⩔

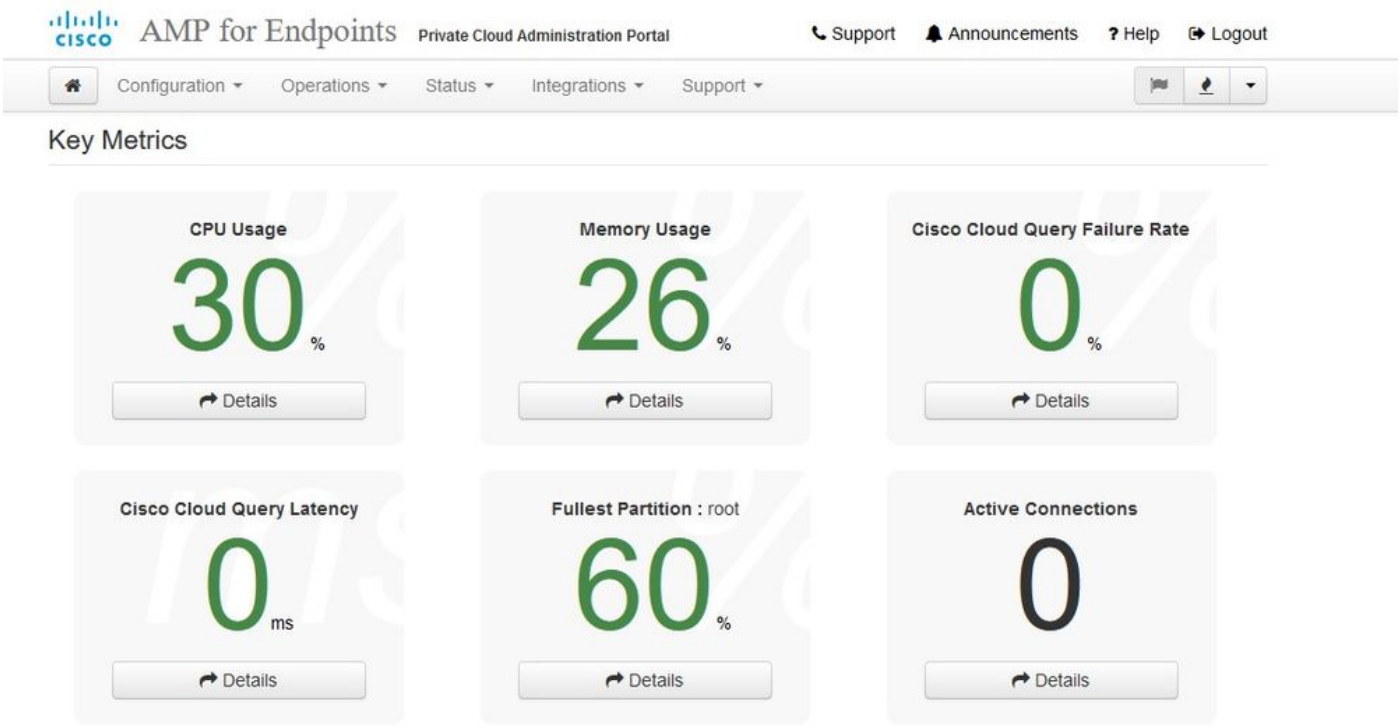


⩓ ⩓ AIRGAP APENAS ⩓ ⩓

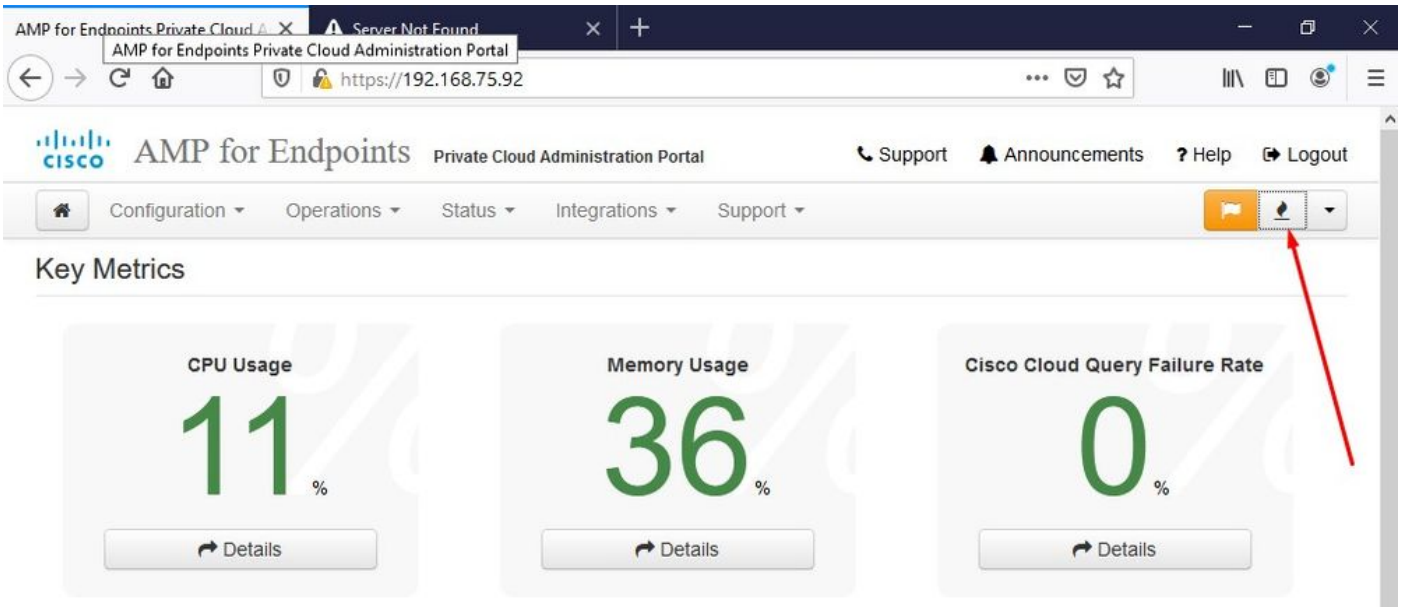
Quando o equipamento estiver totalmente inicializado, na próxima vez que você fizer login com a interface de administrador, este painel será apresentado a você. Você pode notar alta CPU no início, mas se você der alguns minutos, ela se acalmará.



Depois de alguns minutos...

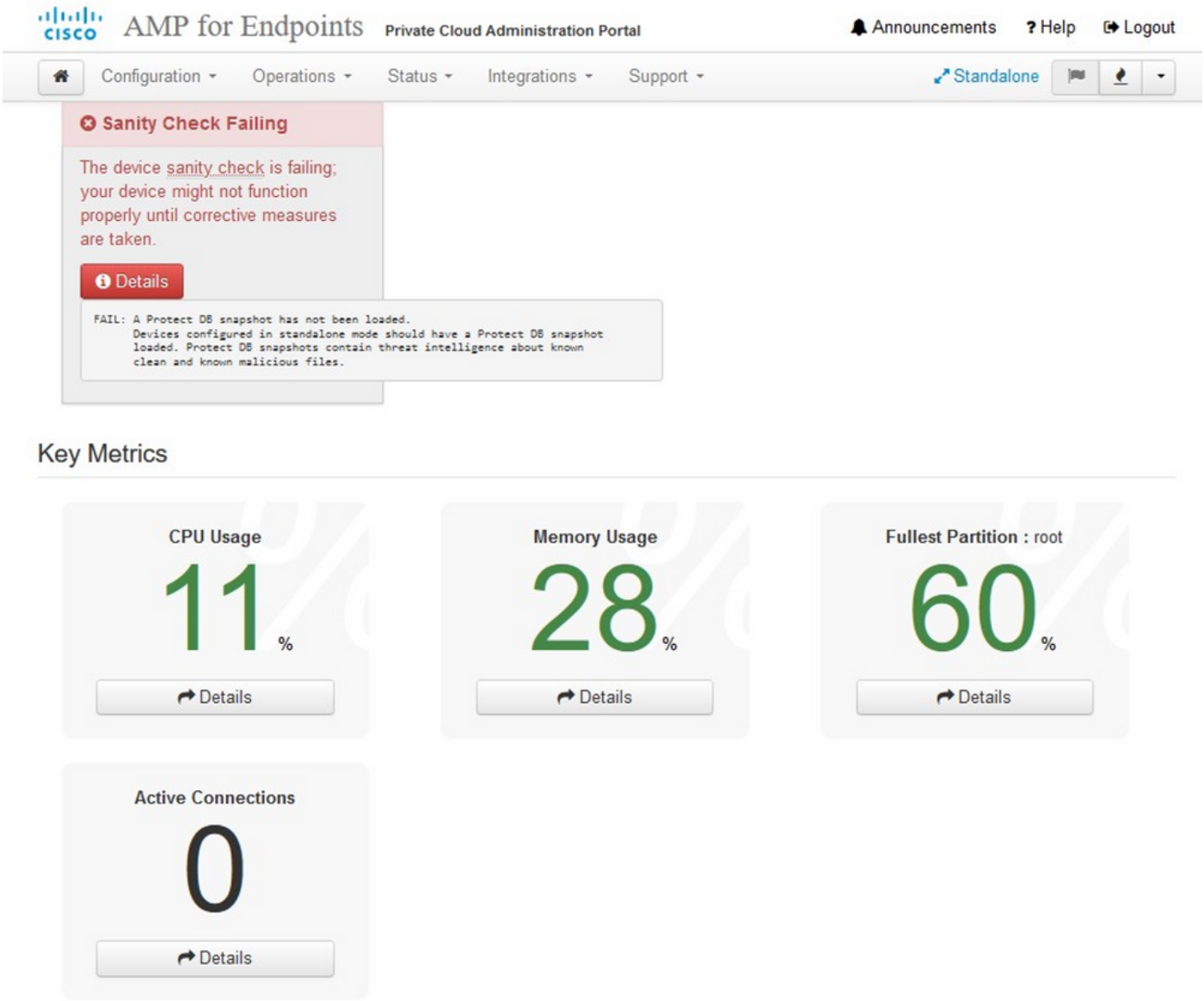


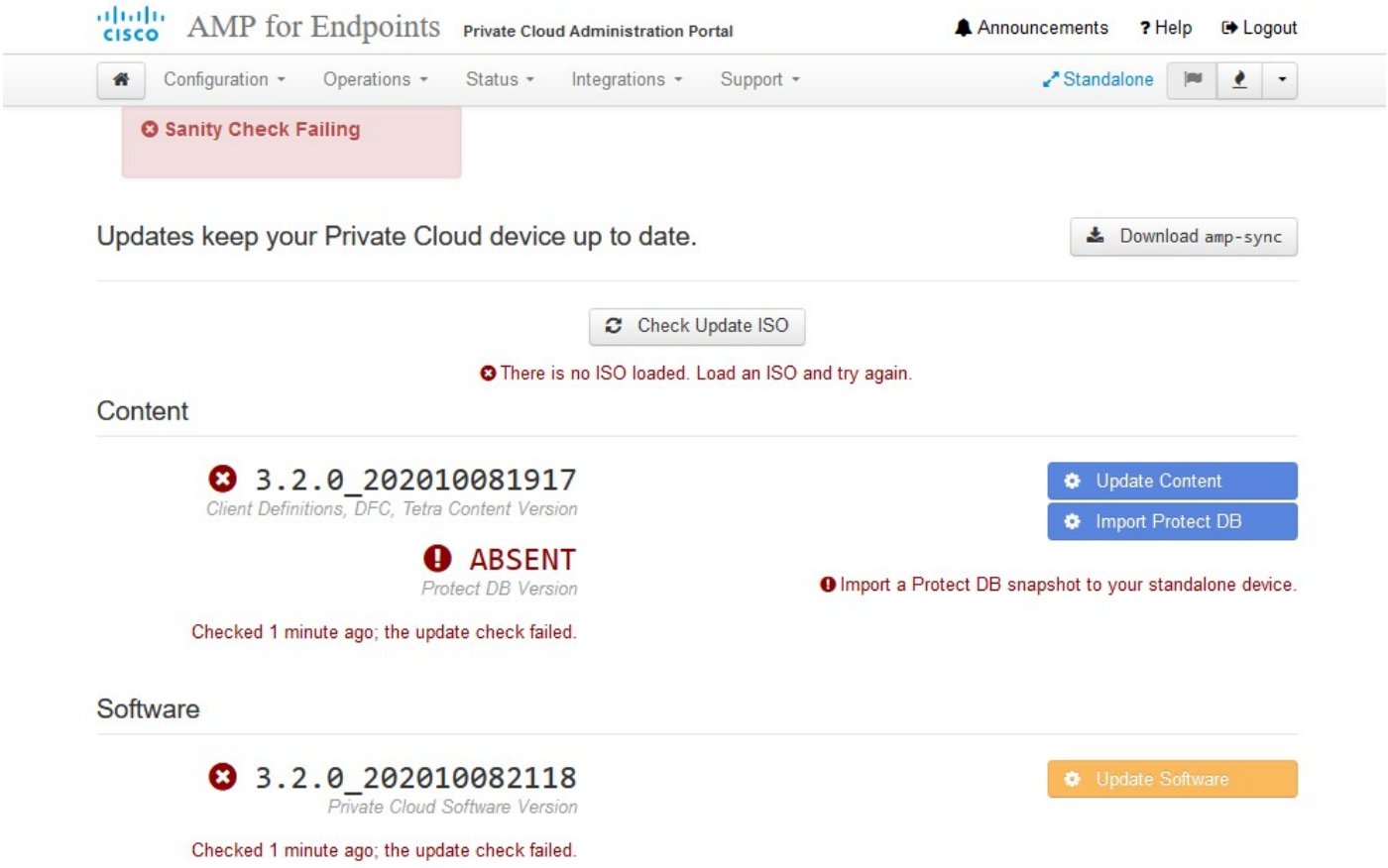
A partir daqui, você navegará para o console do Secure Endpoint. Clique no pequeno ícone que parece fogo no canto direito ao lado da bandeira.



⩔⩔ AIRGAP SOMENTE ⩔⩔

Como você pode ver, falhamos na verificação de integridade devido a DB Protect Snapshot , também Definições de Cliente, DFC e Tetra. Isso deve ser feito por atualização offline por meio de arquivo ISO baixado, previamente preparado por amp-sync e carregado na VM ou armazenado no local NFS.


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
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
CPU Usage
11 %
Details
Memory Usage
28 %
Details
Fullest Partition : root
60 %
Details
Active Connections
0
Details



Pacote de atualização AirGap

Pela primeira vez, precisamos usar este comando para receber o comando Protect DB

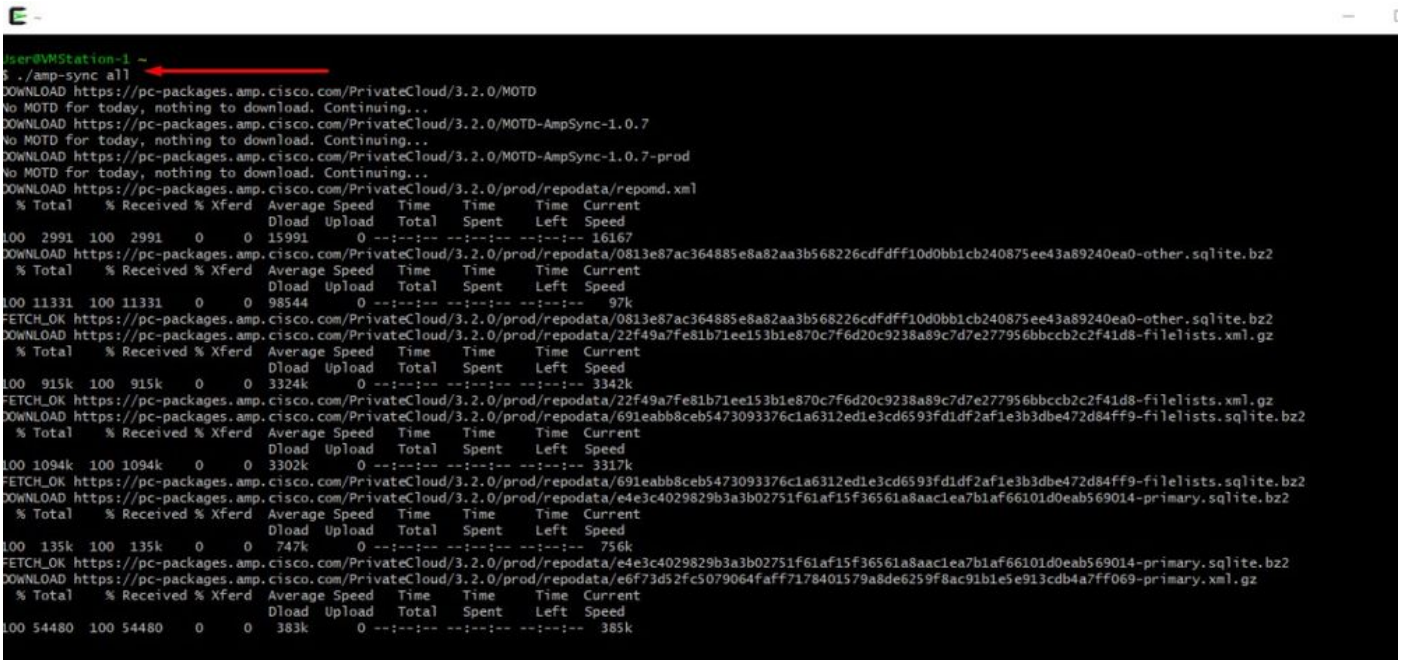
```
./amp-sync all
```

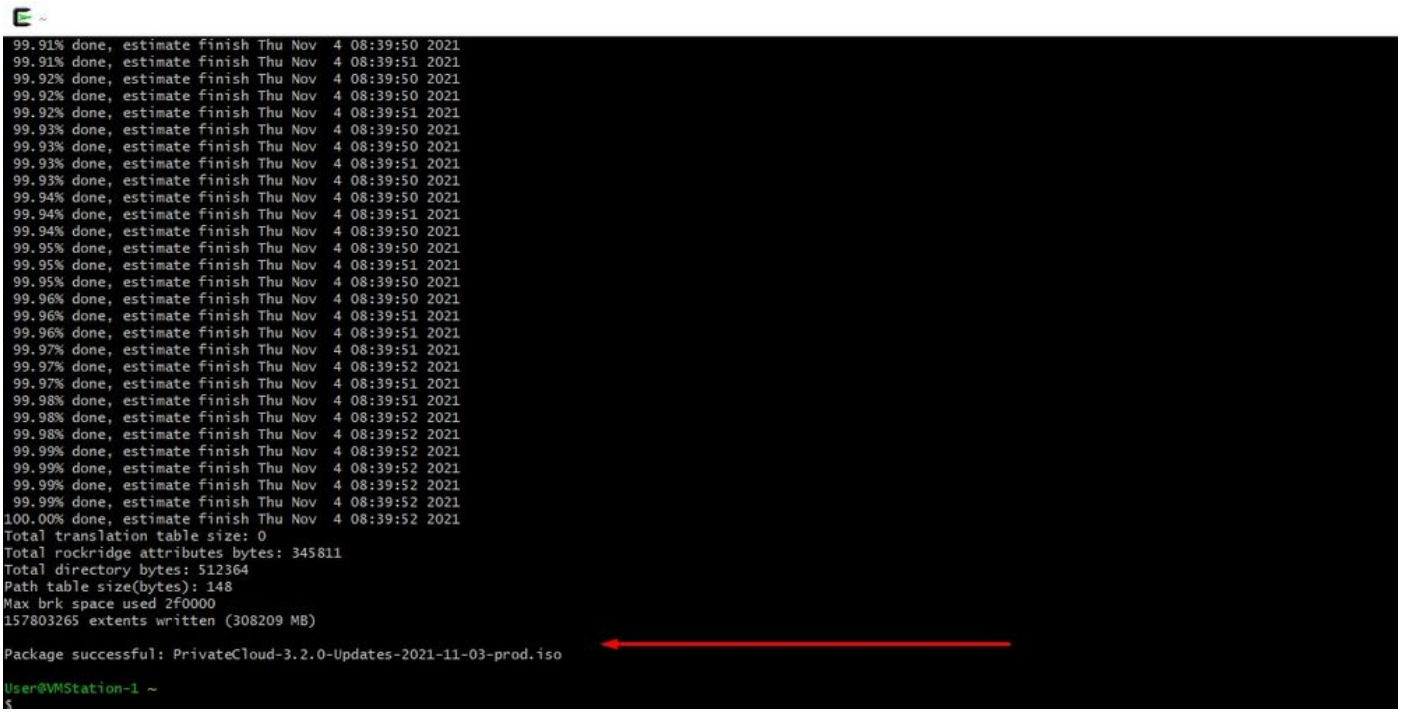
Observação: faça download de todos os pacotes por meio desse comando e verifique se pode levar mais de 24 horas. Dependa da velocidade e da qualidade do link. No meu caso com a fibra de 1Gig, ainda são necessárias quase 25 horas para concluí-la. Em parte, isso também se deve ao fato de que esse download é diretamente do AWS e, portanto, é limitado. Por fim, observe que esse download é bem grande. No meu caso, o arquivo baixado tinha 323GB.

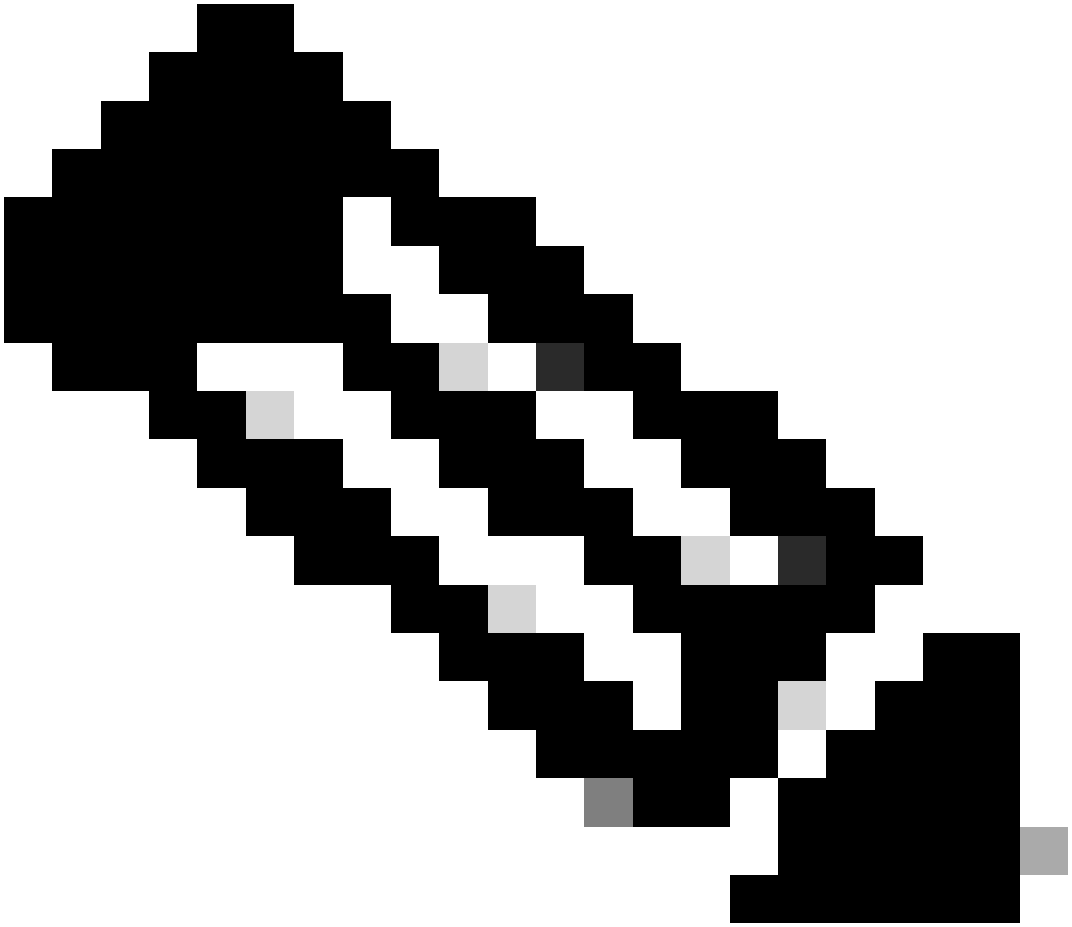
Neste exemplo, usamos CygWin64

1. Baixe e instale a versão x64 do Cygwin.
2. Execute setup-x86_64.exe e vá até o processo de instalação e escolha todos os padrões.
3. Escolha um espelho de download.
4. Selecione os pacotes a serem instalados:

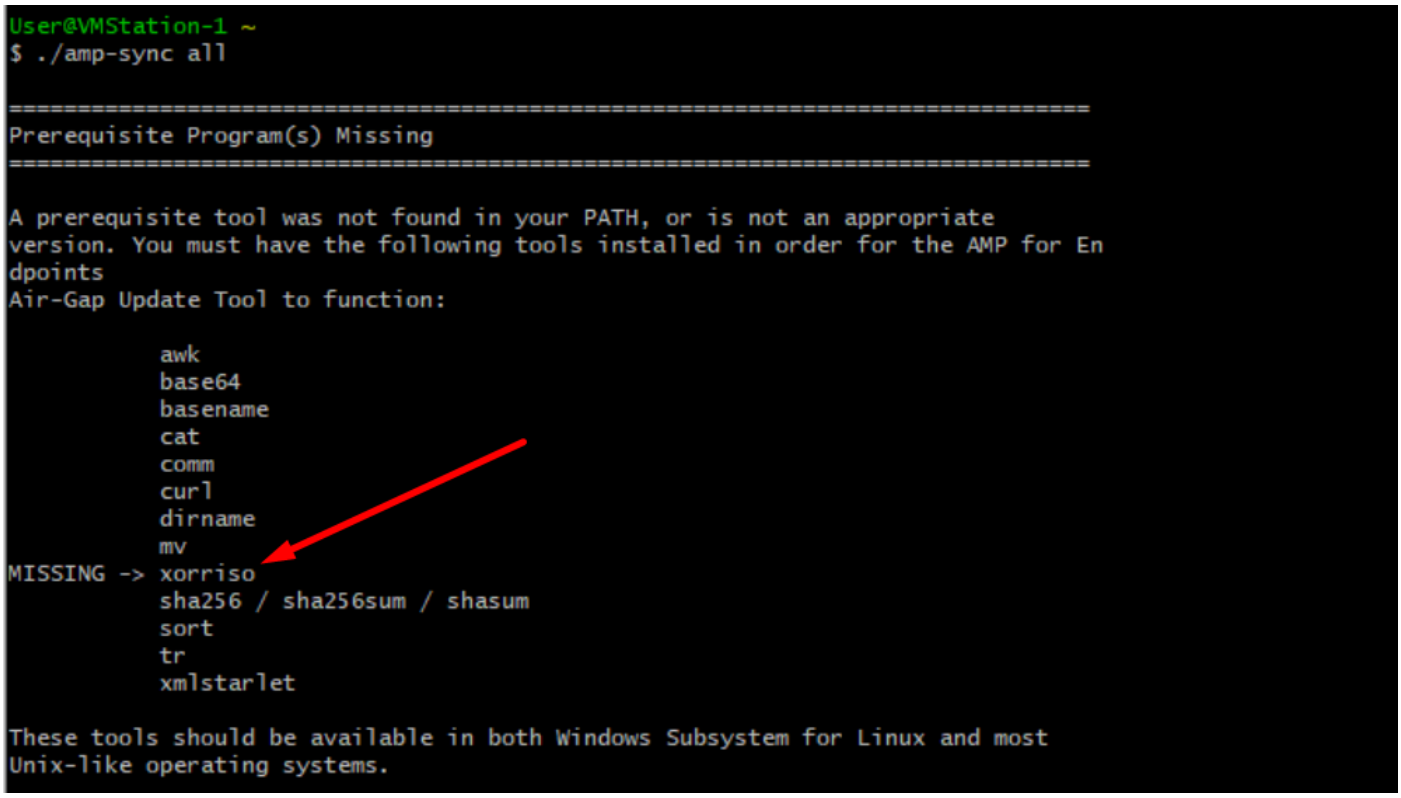
Tudo -> Rede -> Curva
Todos -> Utilitários -> genisoimage
Todos -> Utilitários -> xmlstarlet
* VPC 3.8.x superior - > xorriso







Nota: Na mais recente atualização VPC 3.8.x com CygWin64 como sua principal ferramenta de download, você pode encontrar este problema descrito abaixo.



Notas de versão Página #58. Como você pode ver "xorriso" agora é necessário. Mudamos o formato do ISO para o ISO 9660 e essa dependência é o que converte a imagem para o formato adequado para que a atualização possa ser concluída. Infelizmente, CygWin64 não oferecem xorriso em qualquer um de seus repositórios internos. No entanto, para aqueles que ainda gostariam de usar CygWin64, há uma maneira de superar este problema.

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.

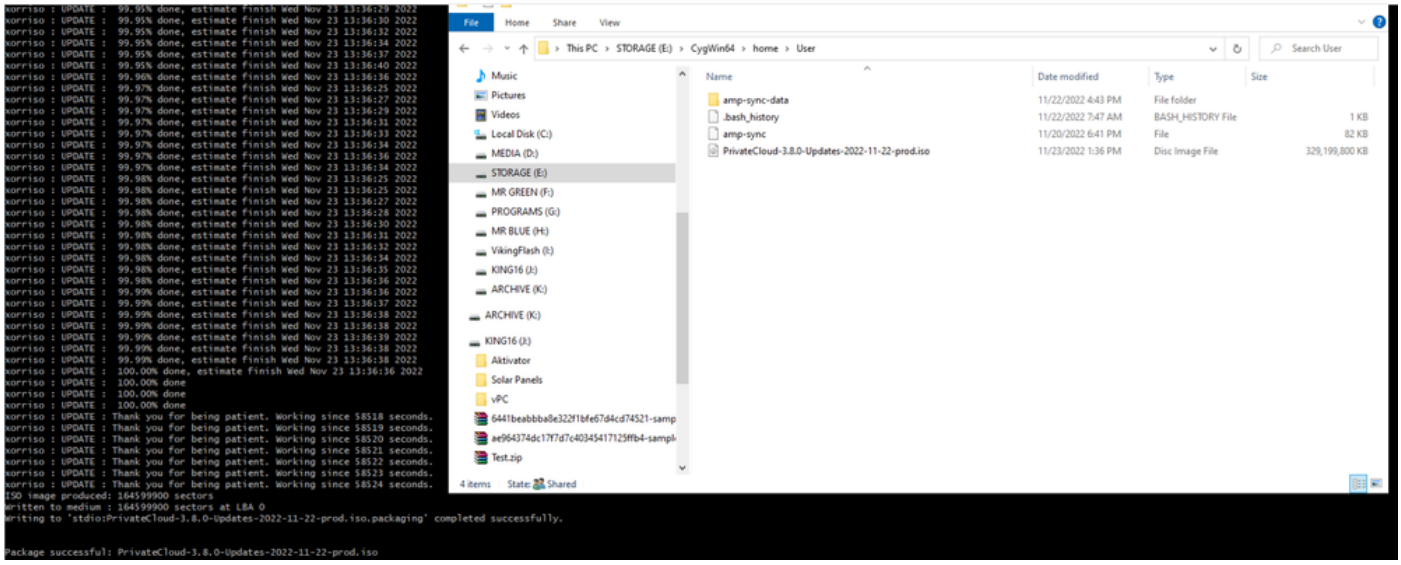
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

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
```

Para poder usar o CygWin mais uma vez, você deve baixar manualmente o xorriso do repositório do GitHub. Abra seu navegador e digite <Latest xorriso.exe 1.5.2 pre-build for Windows> ele deve aparecer como o primeiro link nomeado como <PeyTy/xorriso-exe-for-windows - GitHub>, navegue até a página do GitHub e baixe o arquivo <xorriso-exe-for-windows-master.zip> dentro do arquivo zip que você encontra entre alguns outros arquivos nomeados <xorriso.exe> copie e cole este arquivo em <CygWin64\bin > caminho da instalação local do CygWin. Tente executar novamente o comando <amp-sync>. Você não deve mais ver a mensagem de erro e o download começa e termina como mostrado na imagem.

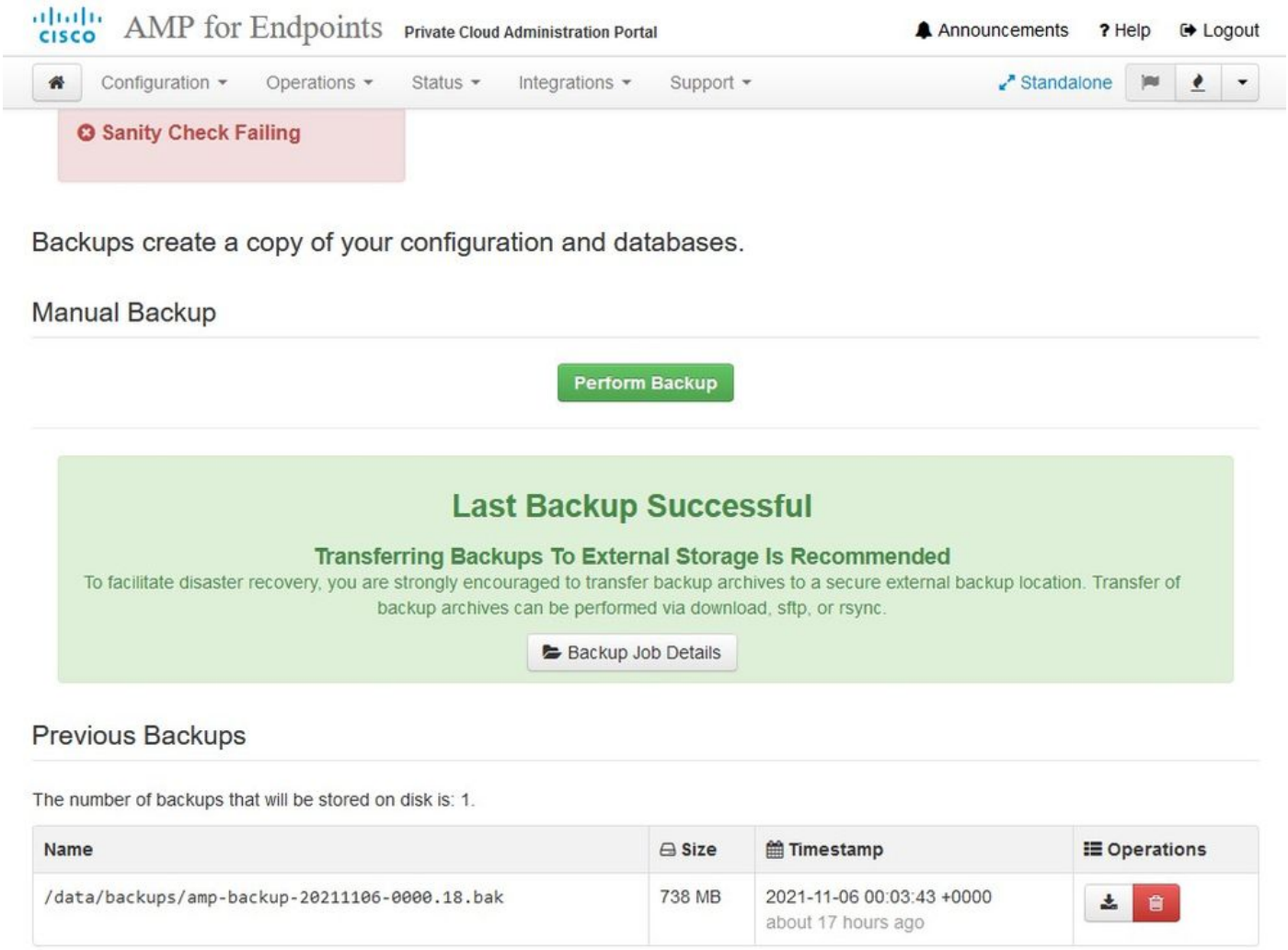


Execute o backup do VPC atual (neste caso) 3.2.0 no modo Airgap.

Você pode usar este comando na CLI

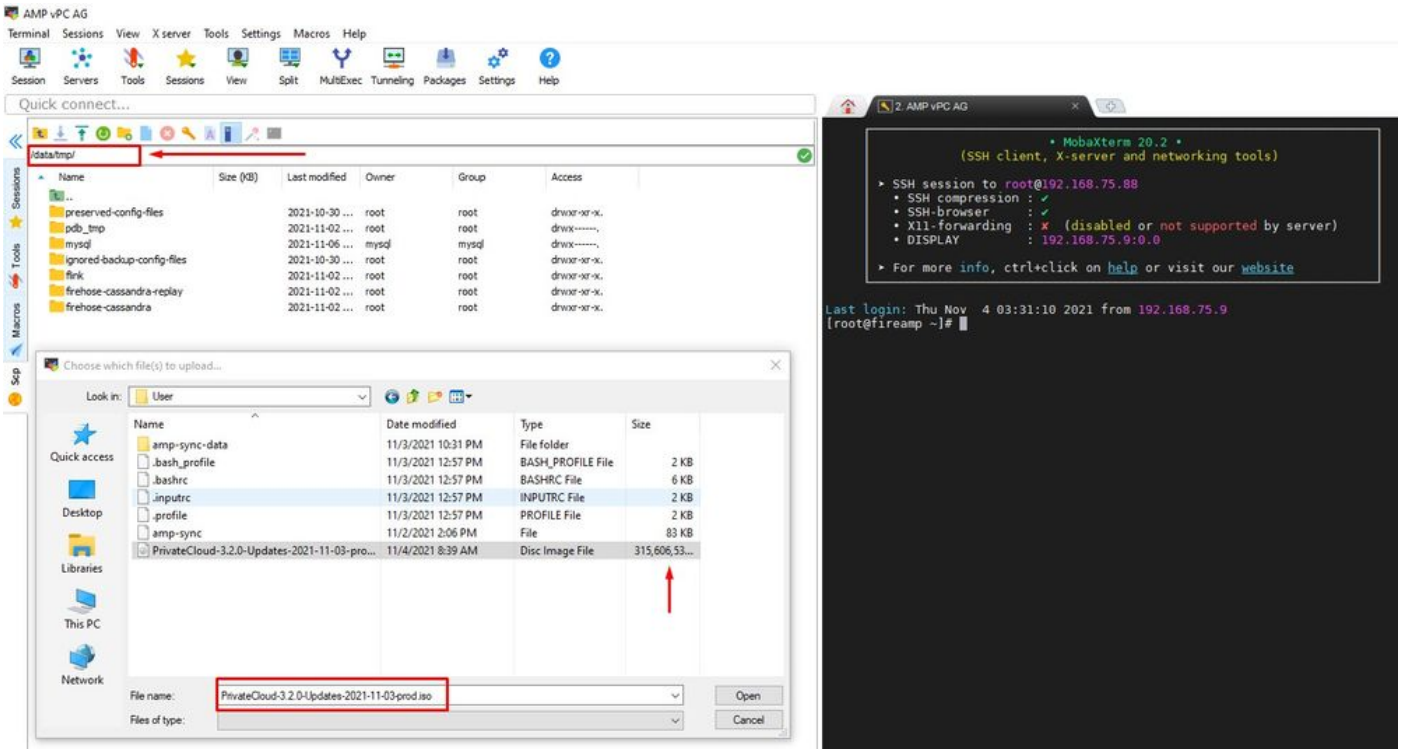
```
rpm -qa | grep Pri
```

Ou você também pode Navegar para Operações > Backups, como mostrado na imagem e Executar backup lá.



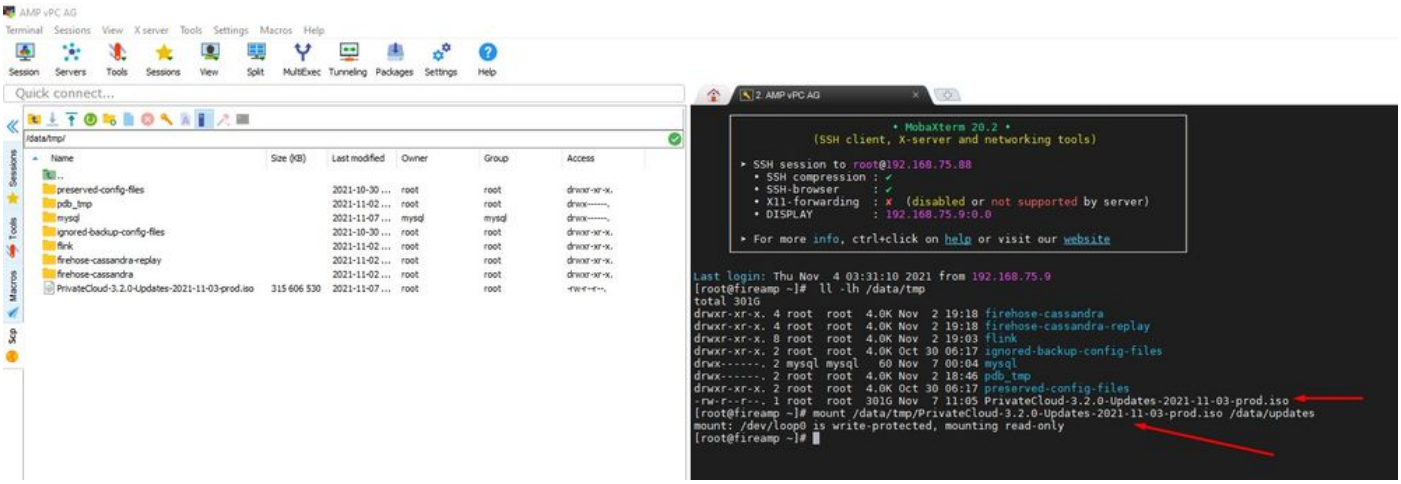
Transfira o ISO mais recente gerado com amp-sync para o VPC. Isso também pode levar várias horas com base na sua velocidade. Neste caso, a transferência levou mais de 16 horas

```
/data/tmp
```



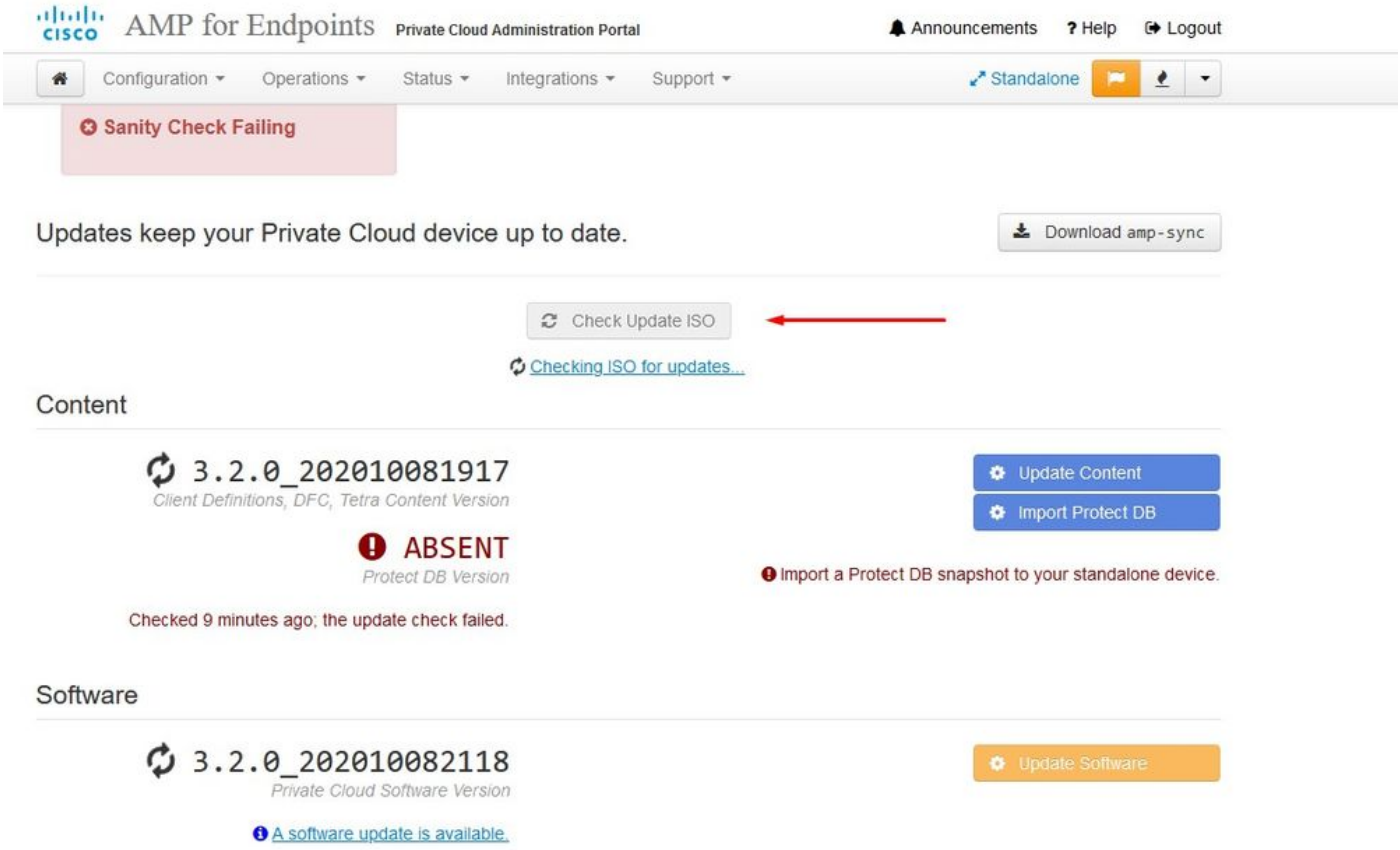
Depois que o upload for concluído, monte o ISO

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

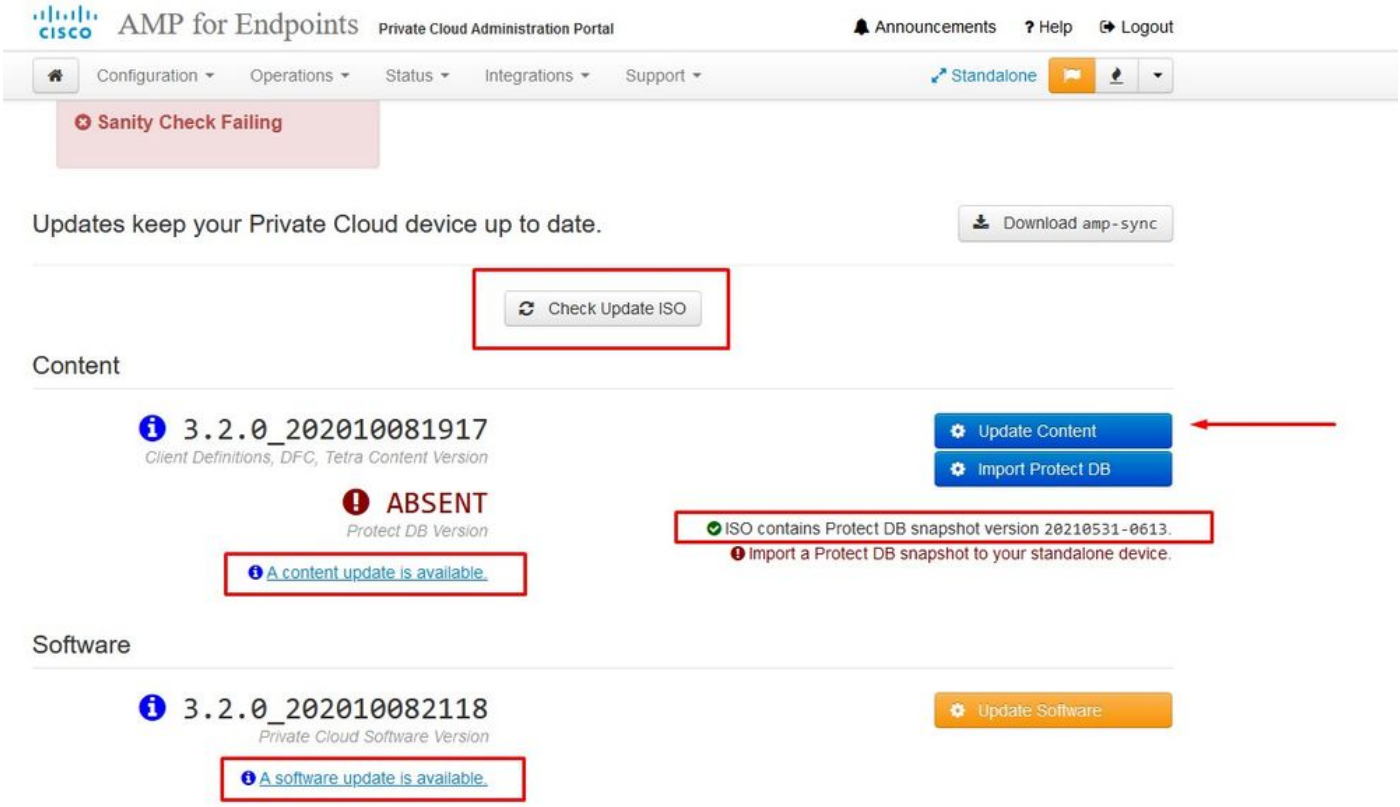


Navegue até a interface do usuário do opdamin para executar a atualização Operações >

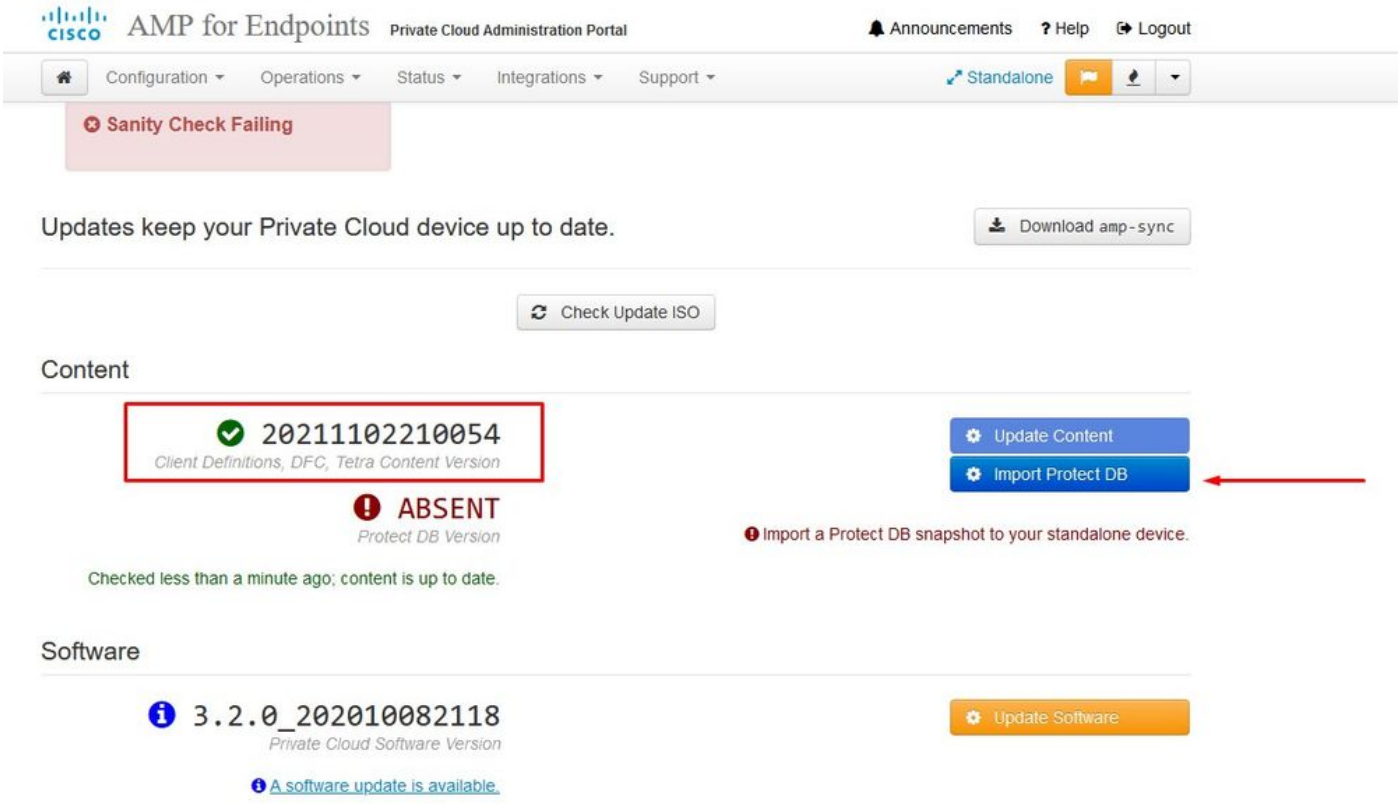
Atualizar Dispositivo > Selecionar Verificar ISO de atualização.



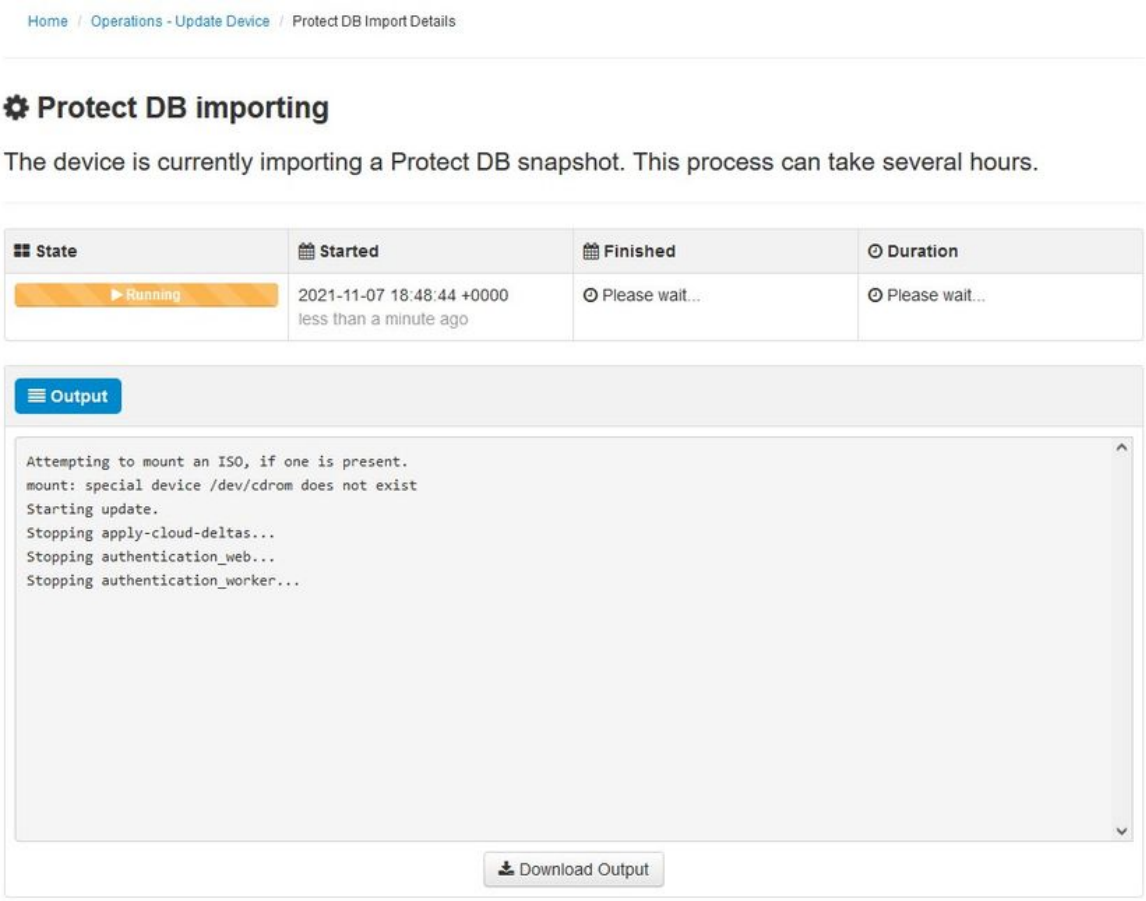
Neste exemplo, eu continuo com Atualizar conteúdo primeiro



Em seguida, selecione Importar Proteger BD.



Como você pode ver, esse é outro processo muito demorado que pode demorar muito para ser concluído.



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).
```

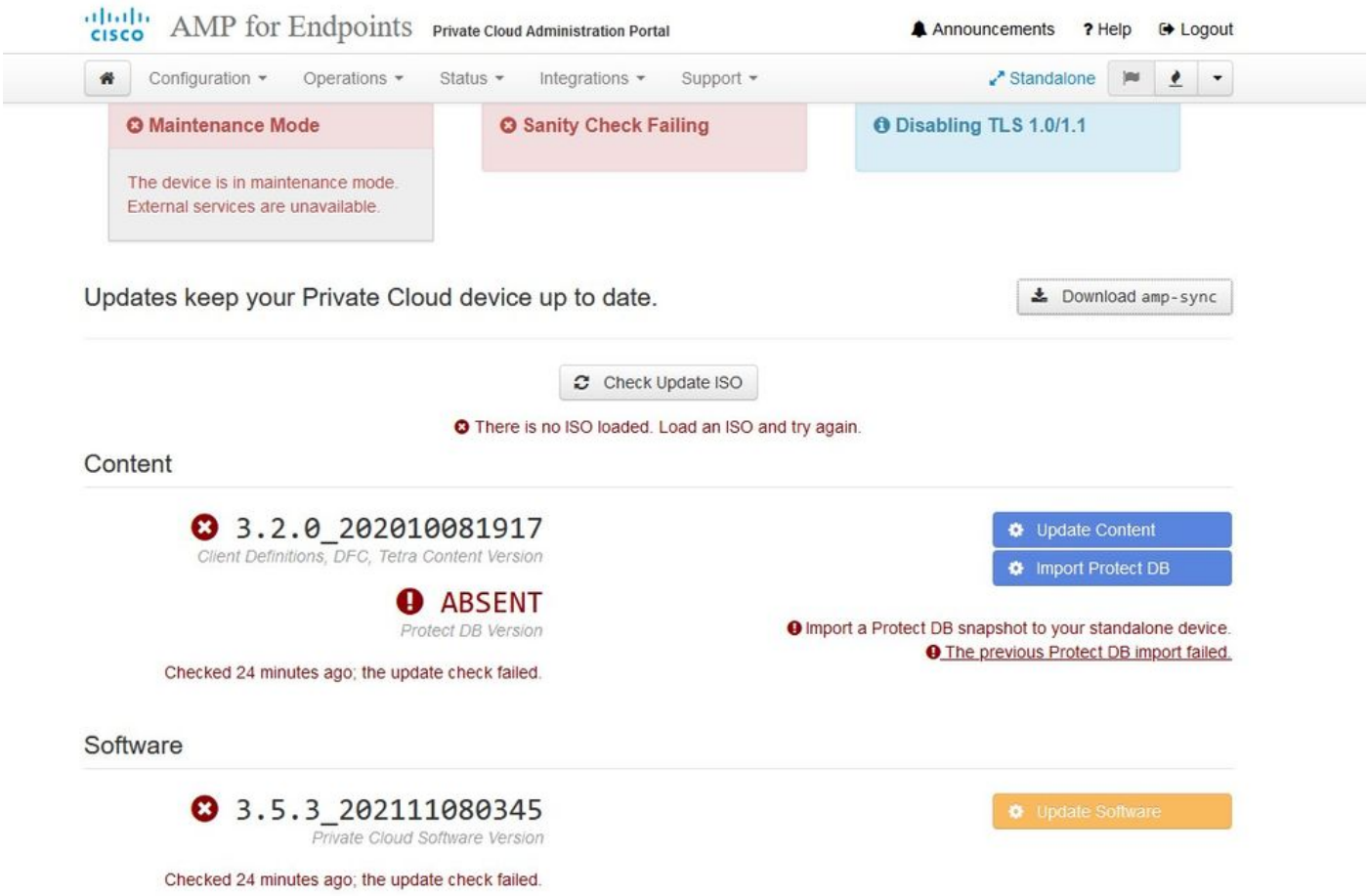
Problema #1 - Espaço esgotado no Repositório de Dados

Aqui você pode ter dois problemas. Como o vPC anterior à versão 3.5.2 não tem a capacidade de montar um armazenamento NFS externo, você precisa carregar o arquivo ISO de atualização no diretório /data/temp. No meu caso, como meu armazenamento de dados tinha apenas 1 TB, eu saí da sala e a VM caiu. Em outras palavras, você precisa de pelo menos 2 TB de espaço no seu Data Store para implantar com sucesso o VPC AirGap, que é a versão 3.5.2 abaixo

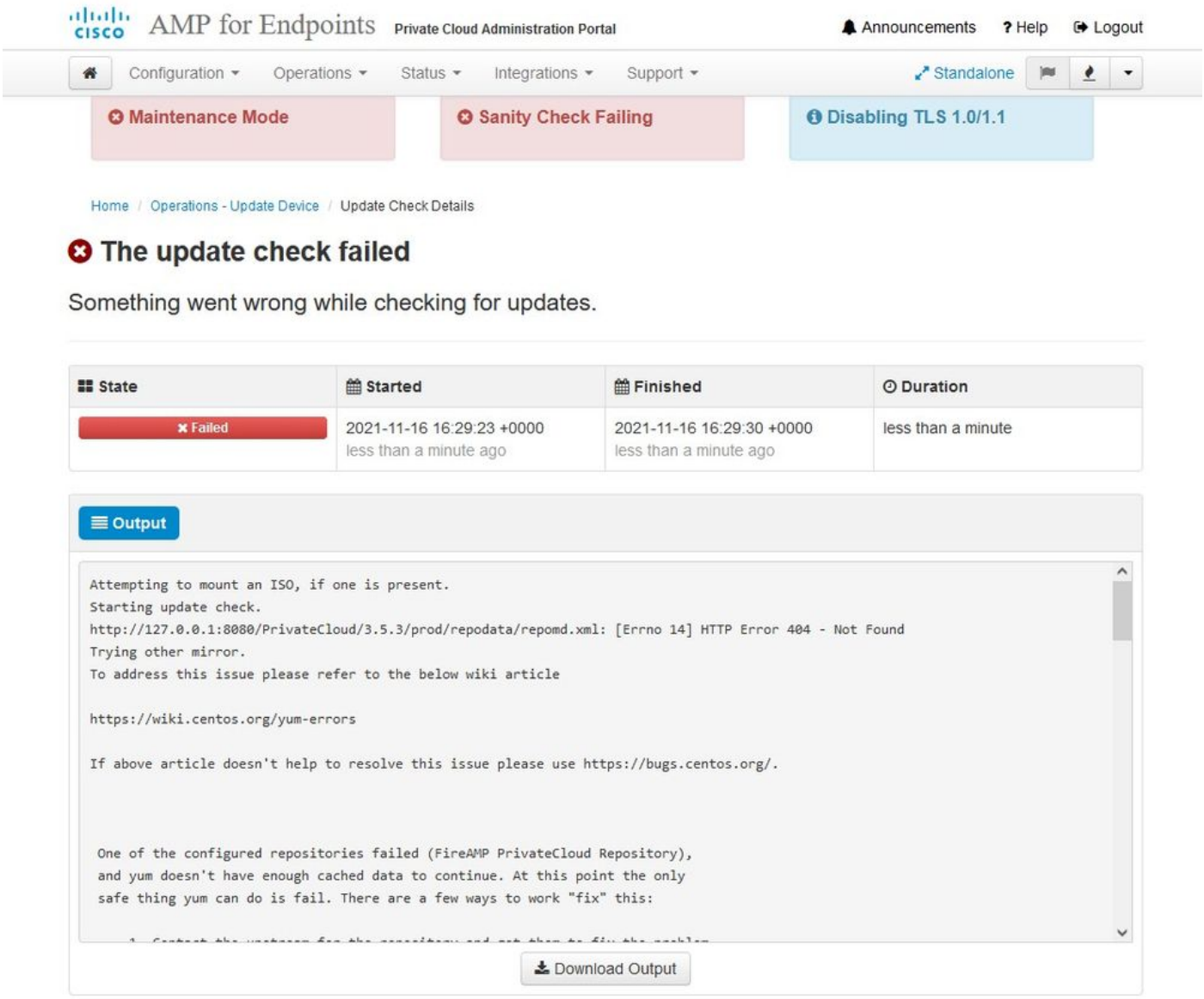
Esta imagem abaixo é do servidor ESXi que mostra o erro de que não há mais espaço disponível no HDD quando você tenta inicializar a VM. Consegui me recuperar desse erro trocando temporariamente a RAM de 128 GB para 64 GB. Então eu consegui inicializar novamente. Lembre-se também de que, se você provisionar essa VM como Thin Client, a desvantagem da implantação do Thin Client é que o tamanho do disco pode aumentar, mas não diminuiria mesmo se você liberasse espaço. Em outras palavras, digamos que você tenha carregado seu arquivo de 300 GB no diretório do vPC e excluído. O disco no ESXi ainda mostra 300 GB a menos de espaço em seu HDD

Problema #2 - Atualização antiga

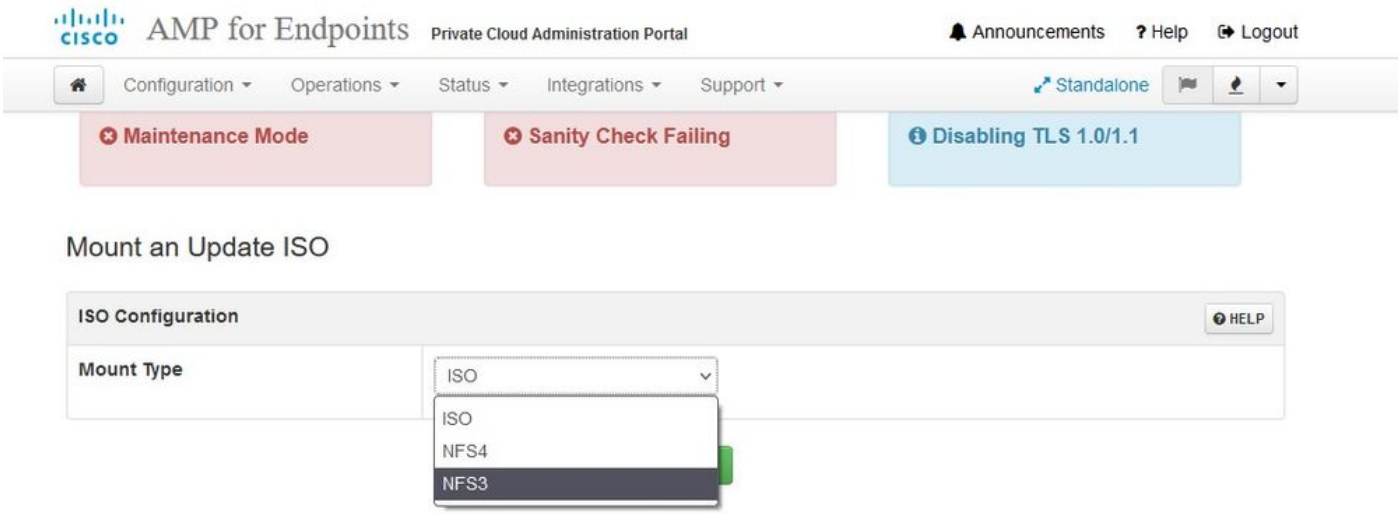
O 2º problema é se você executar a atualização de software primeiro como eu fiz na minha 2ª avaliação e a partir de 3.2.0 eu acabar com VPC para atualizar para 3.5.2 e por causa disso eu tive que baixar o novo arquivo de atualização ISO desde o 3.2.0 tornar-se inválido devido ao fato de que eu não estava mais na versão 3.2.0 original.

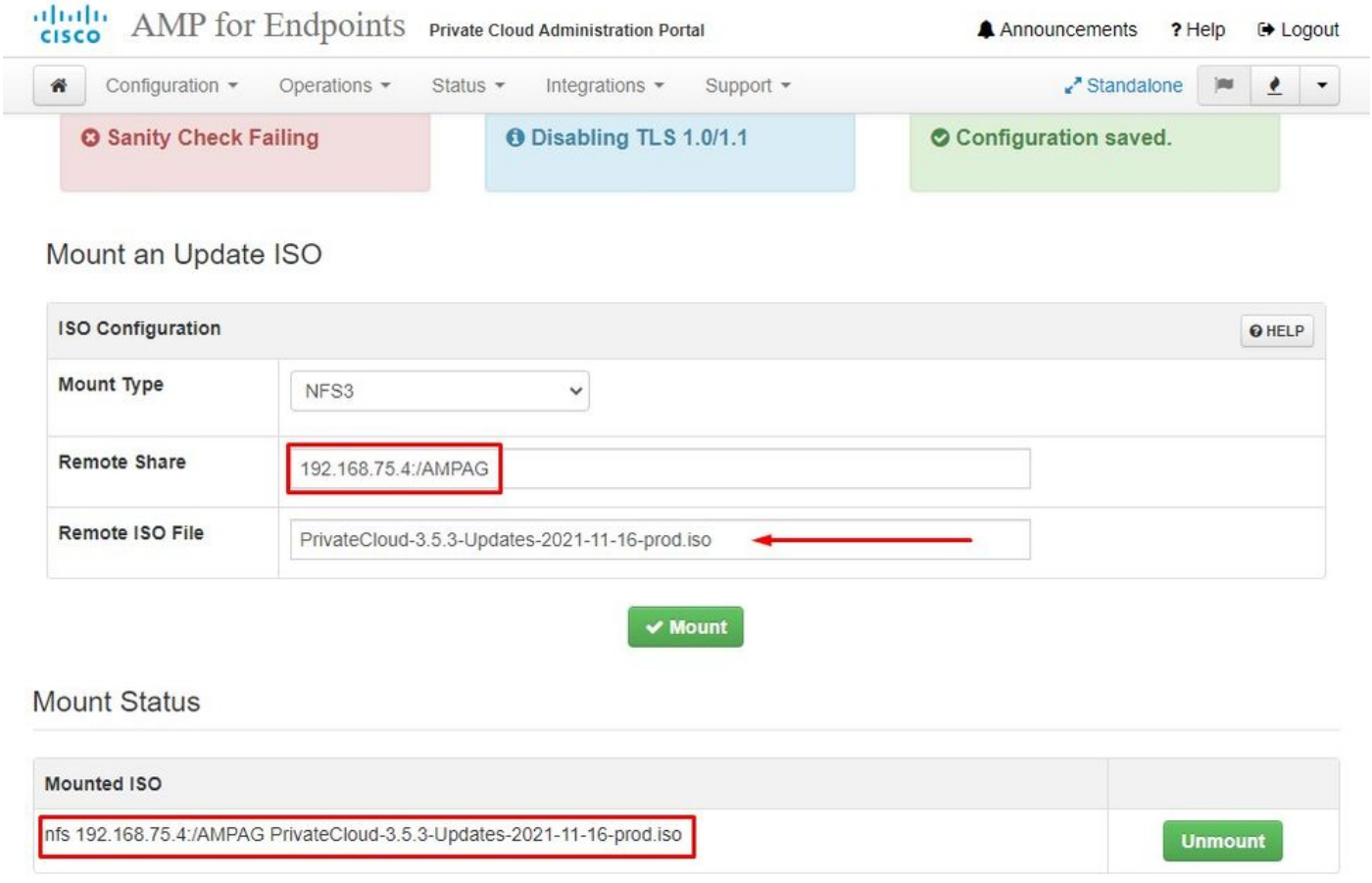


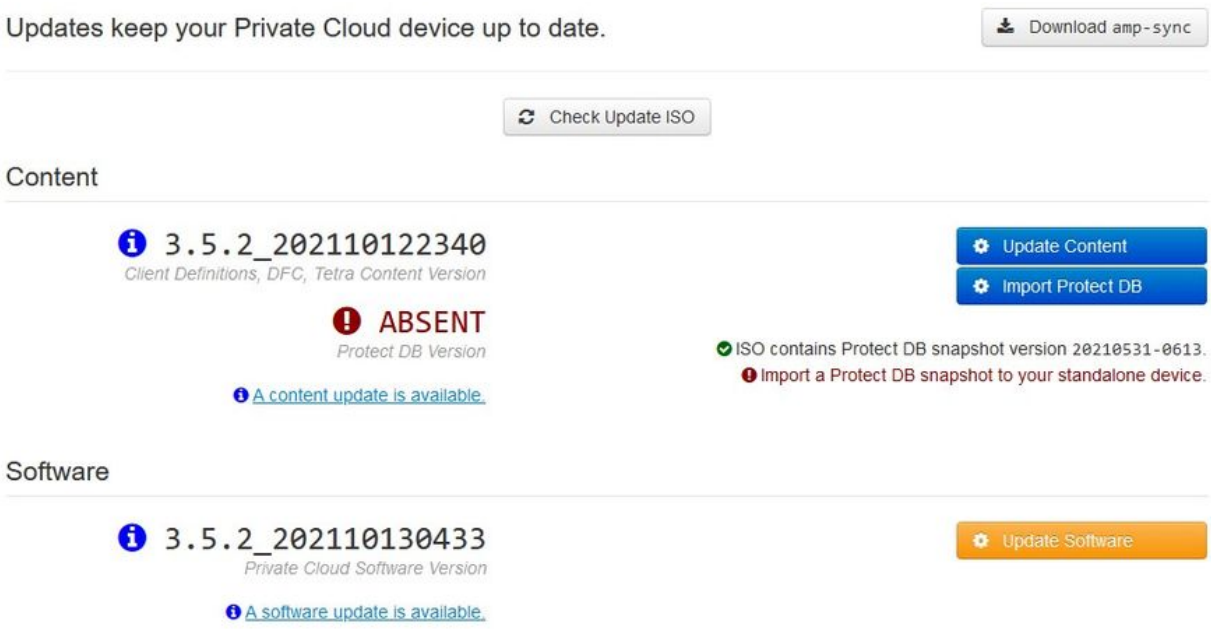
Esse é o erro que você vê ao tentar montar o arquivo de atualização ISO novamente.



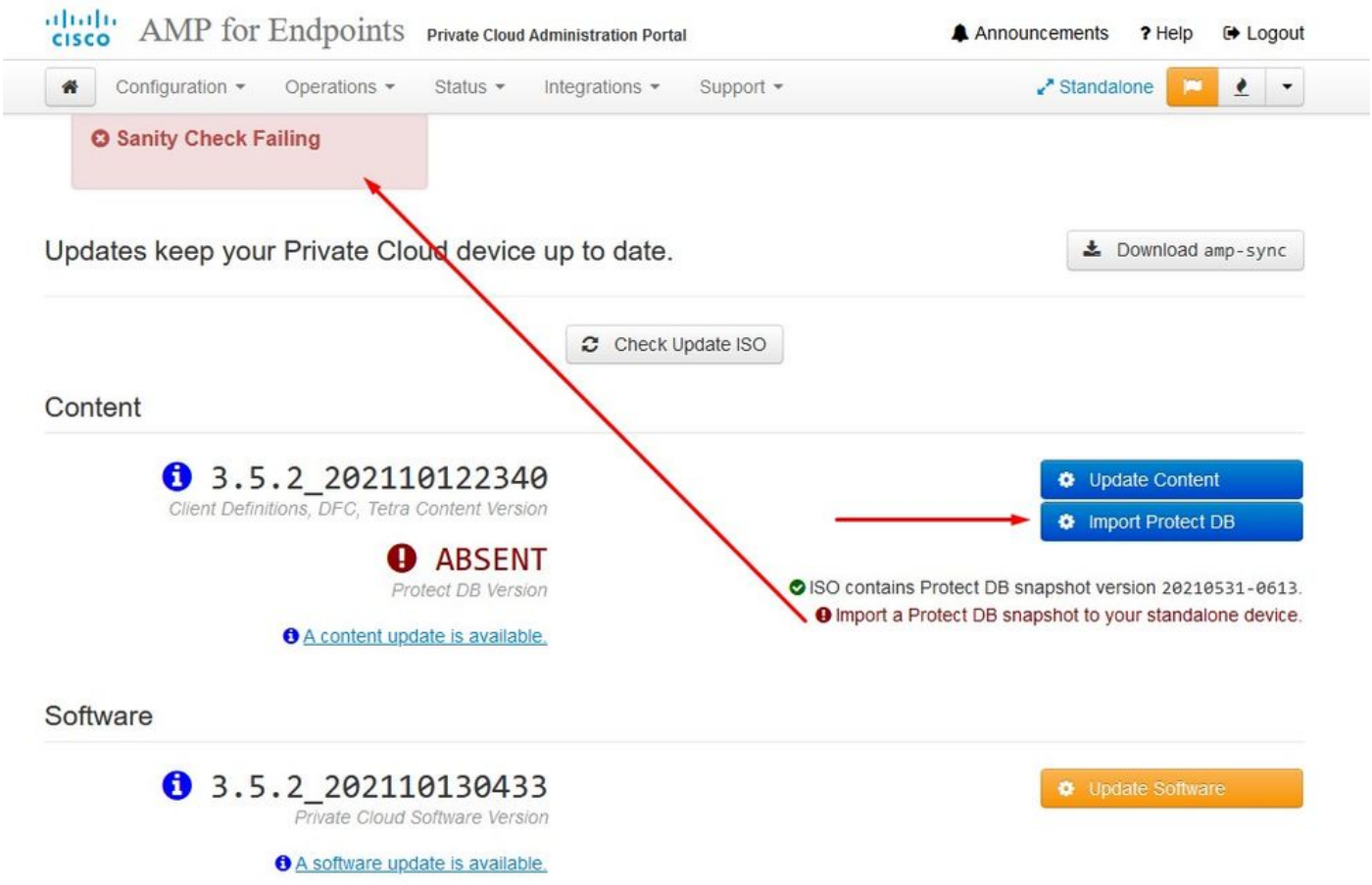
Esta imagem mostra uma maneira alternativa de montar a imagem de atualização em seu VPC. Na versão 3.5.x, você pode usar um local remoto, como o armazenamento NFS, para compartilhar o arquivo de atualização com seu VPC.


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



A falha na verificação de integridade está relacionada ao Protect DB não disponível no momento no VPC



Protect DB importing

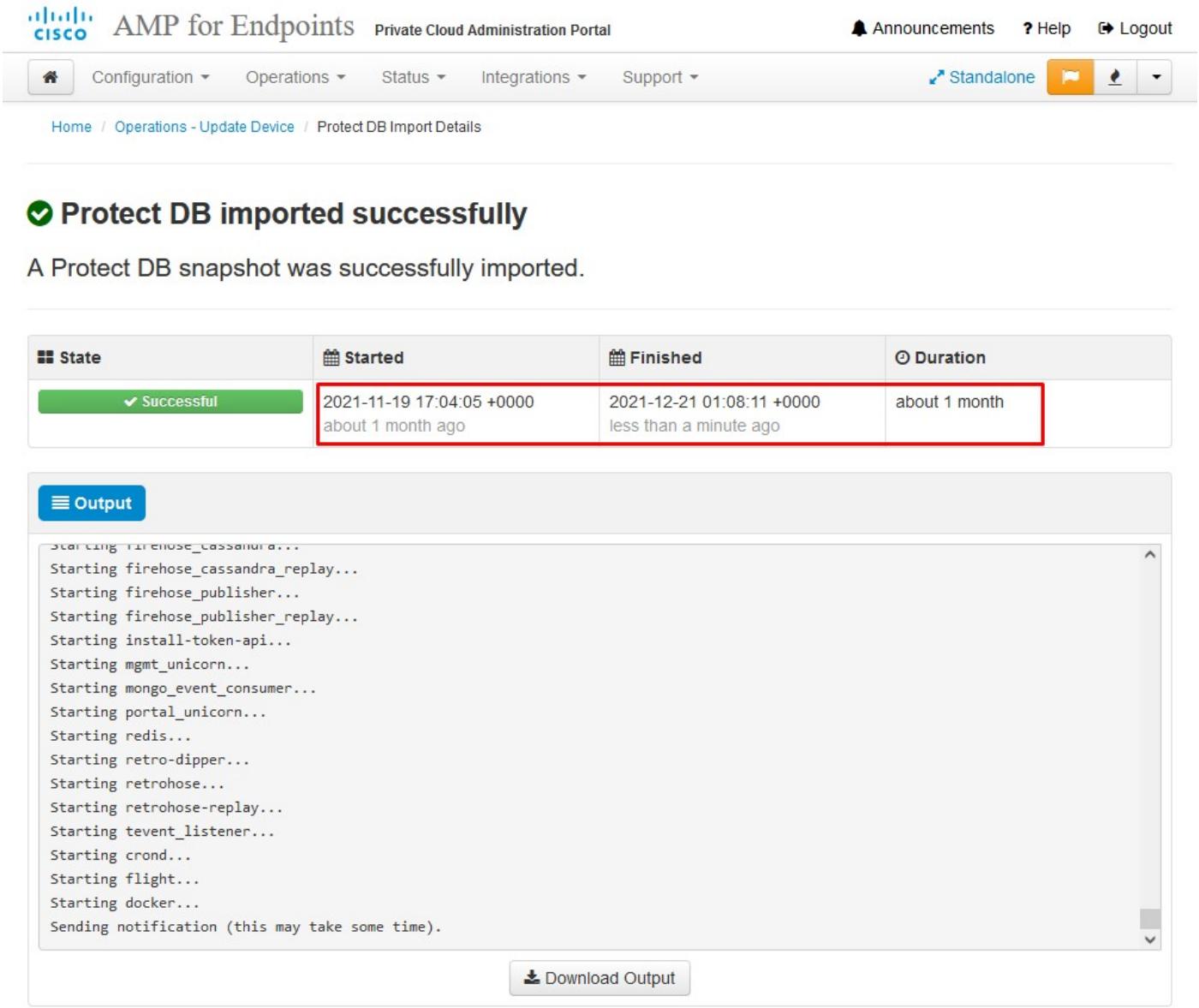
The device is currently importing a Protect DB snapshot. This process can take several hours.

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

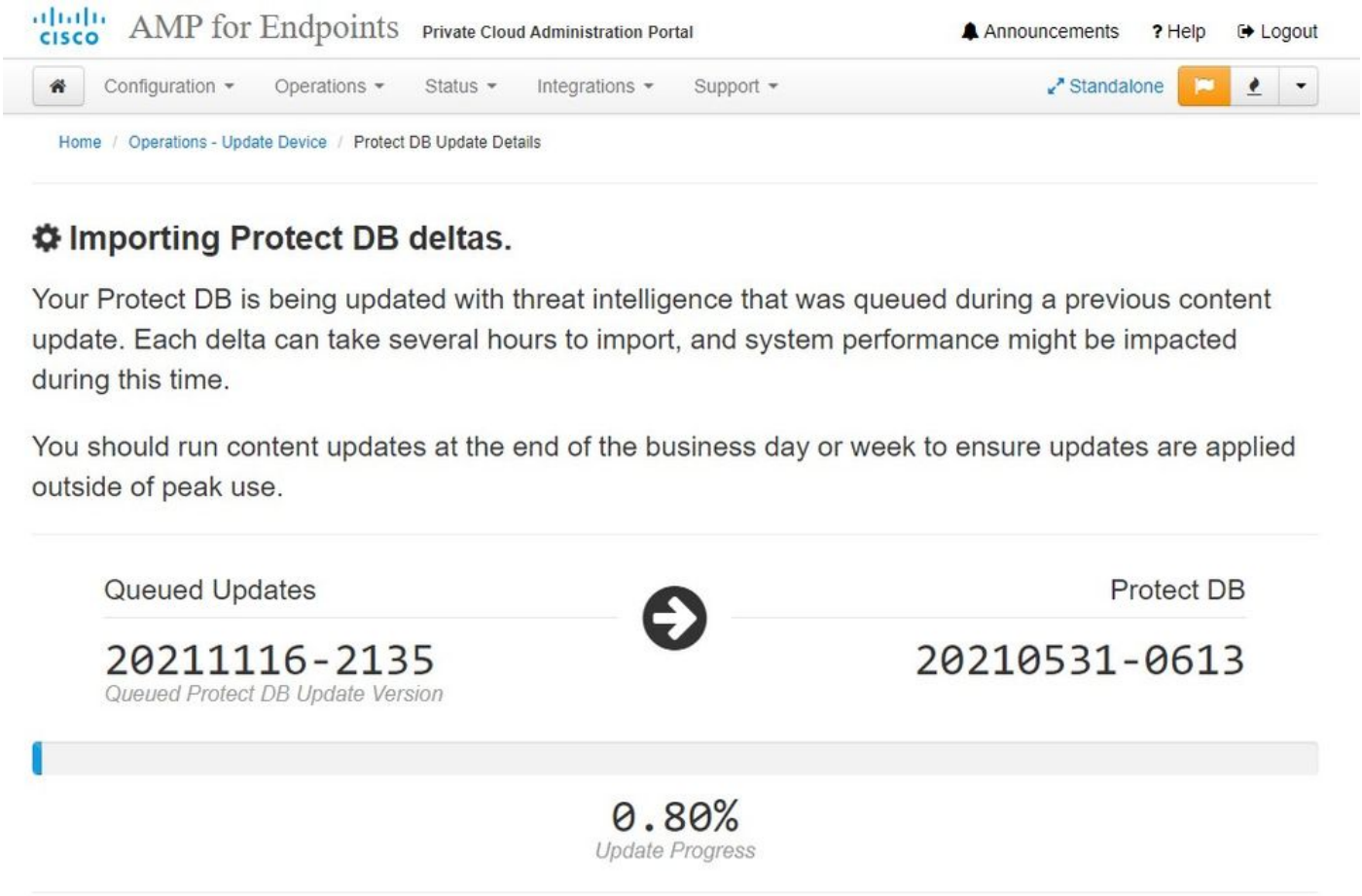
Output

```
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).
```

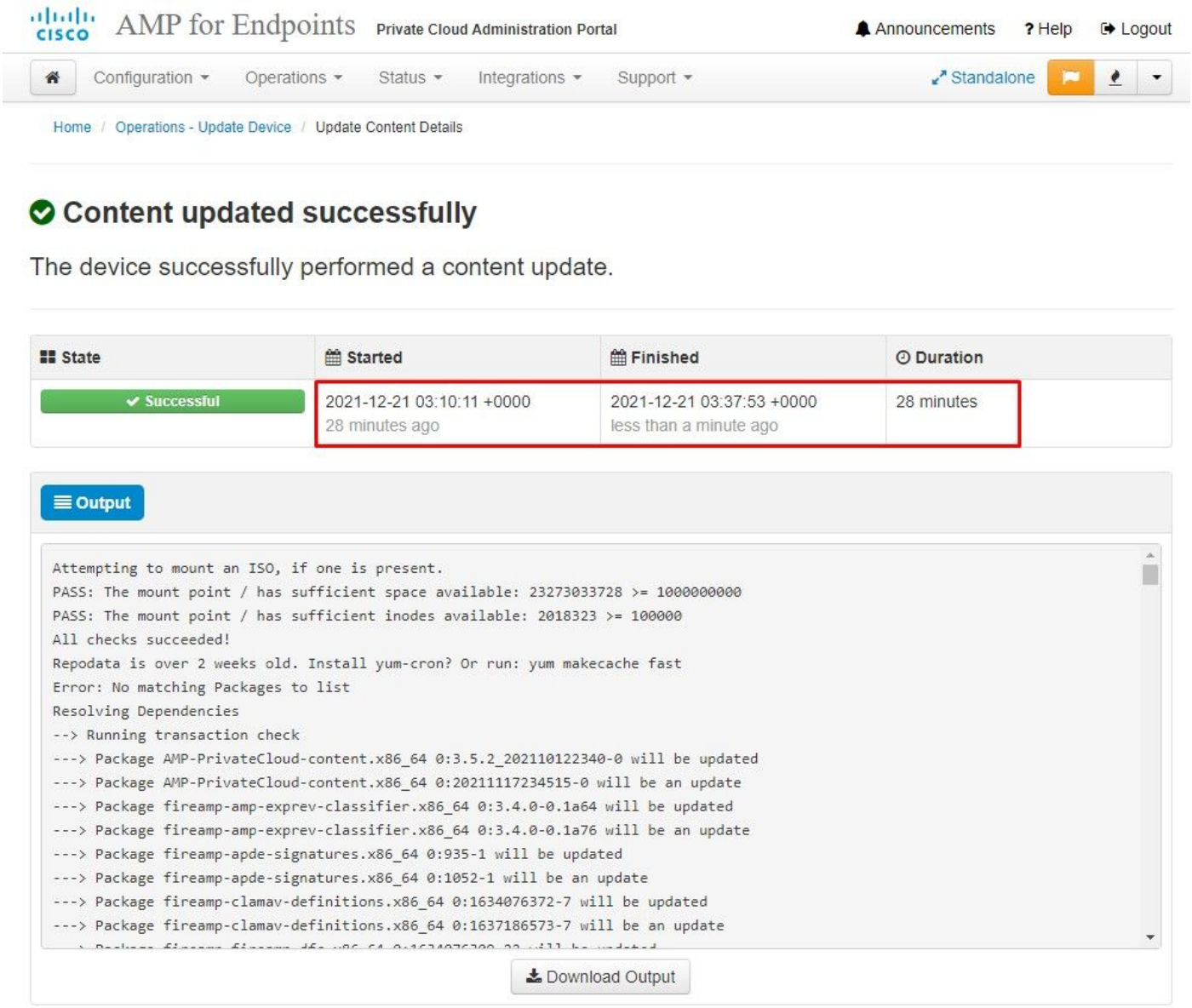
Download Output



A próxima atualização começa automaticamente



Após esse longo processo de importação do Protect DB Database, você pode mover e atualizar a Definição de Cliente e o Software, o que pode levar mais de 3 horas.



E, finalmente, observe que esse processo levará muito tempo.

Para o dispositivo VPC, visite este TZ que contém outros métodos para atualizar o dispositivo de hardware, montar o arquivo ISO e inicializar a partir do USB.

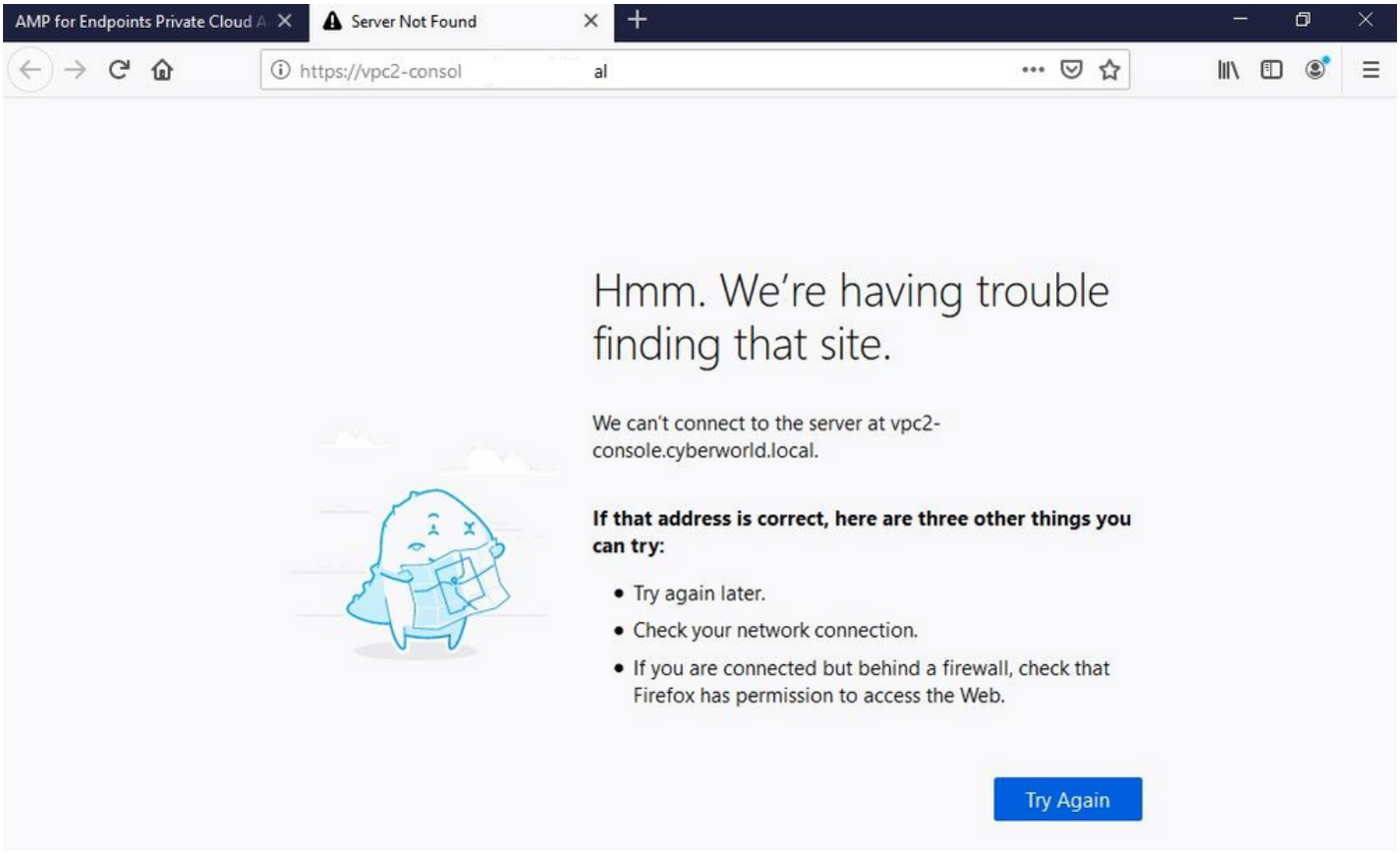
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

⩓ ⩓ AIRGAP APENAS ⩓ ⩓

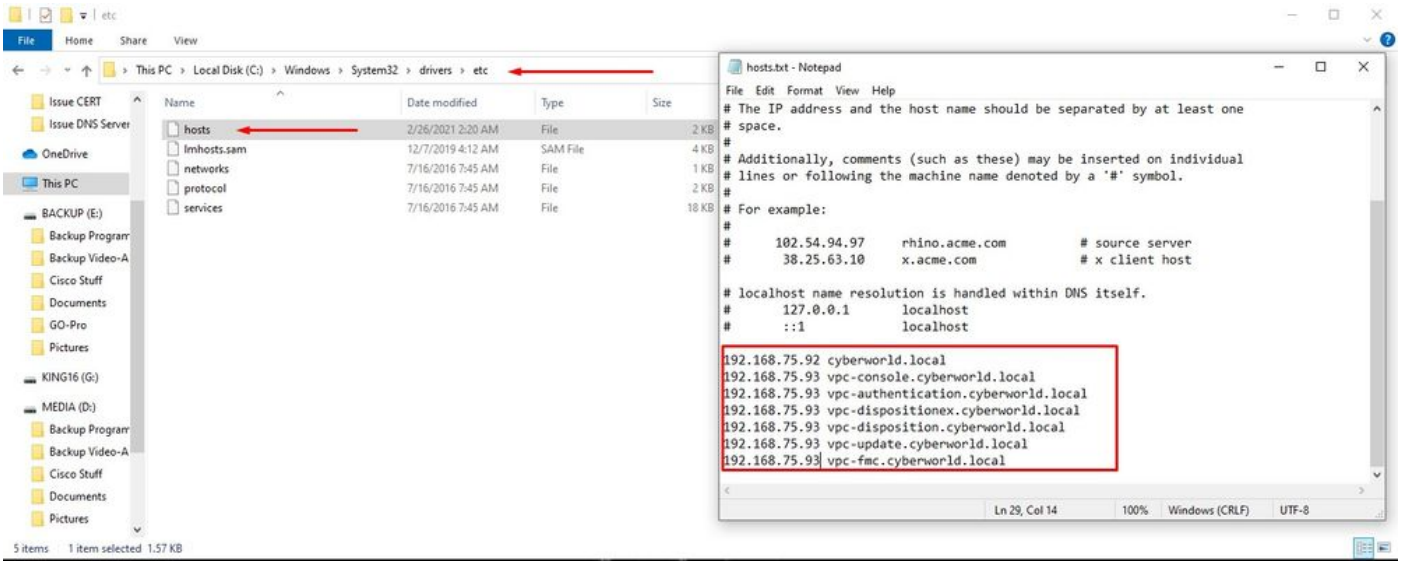
Troubleshooting Básico

Problema #1 - FQDN e Servidor DNS

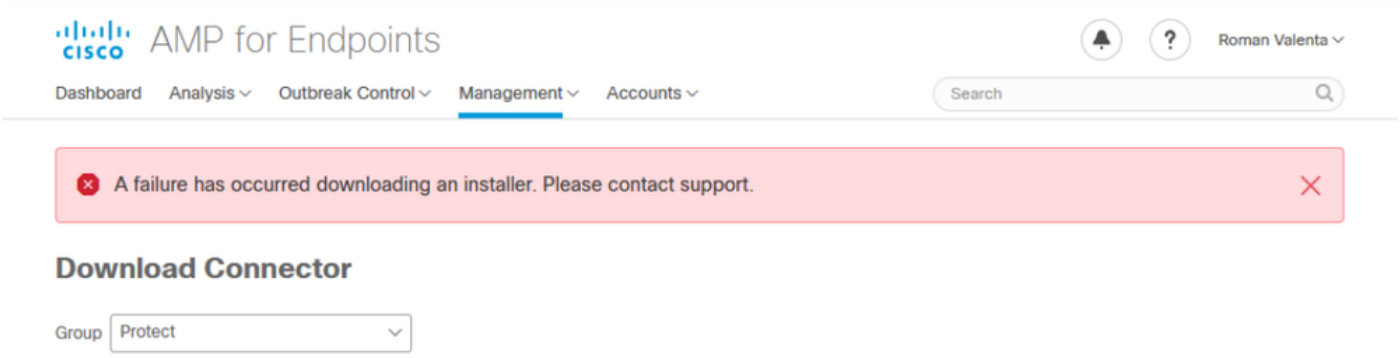
O primeiro problema que você pode encontrar é se o seu servidor DNS não está estabelecido e todos os FQDN não estão registrados e resolvidos corretamente. O problema pode parecer assim quando você tenta navegar para o console do Secure Endpoint por meio do ícone "fire" do Secure Endpoint. Se você usar apenas o endereço IP, ele funcionará, mas você não poderá baixar o conector. Como você pode ver na 3ª imagem abaixo.



Se você modificar o arquivo HOSTS em sua máquina local como mostrado na imagem, solucione o problema e você terminará com erros.



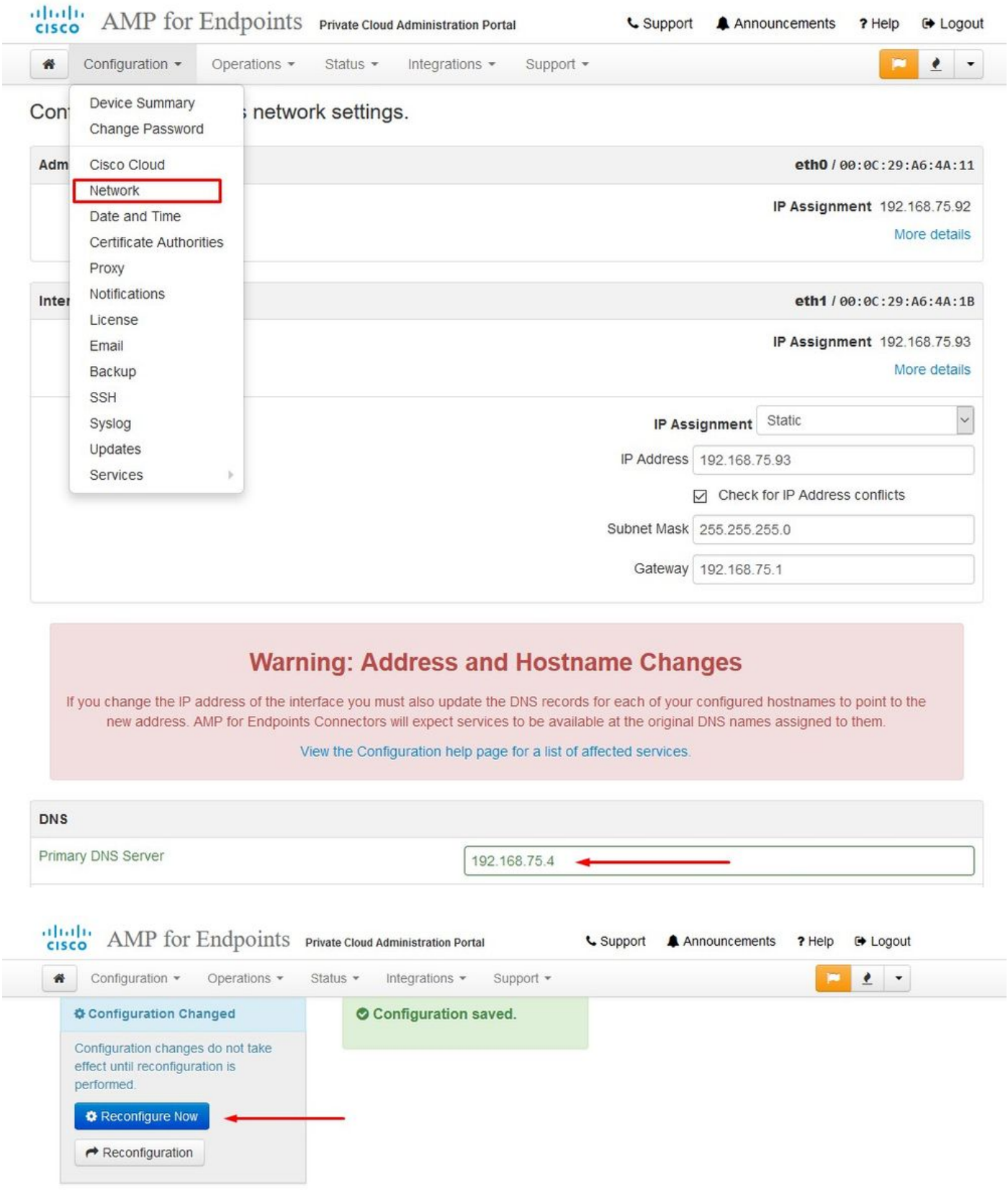
Você recebe este erro ao tentar baixar o instalador do conector de Ponto de Extremidade Seguro.



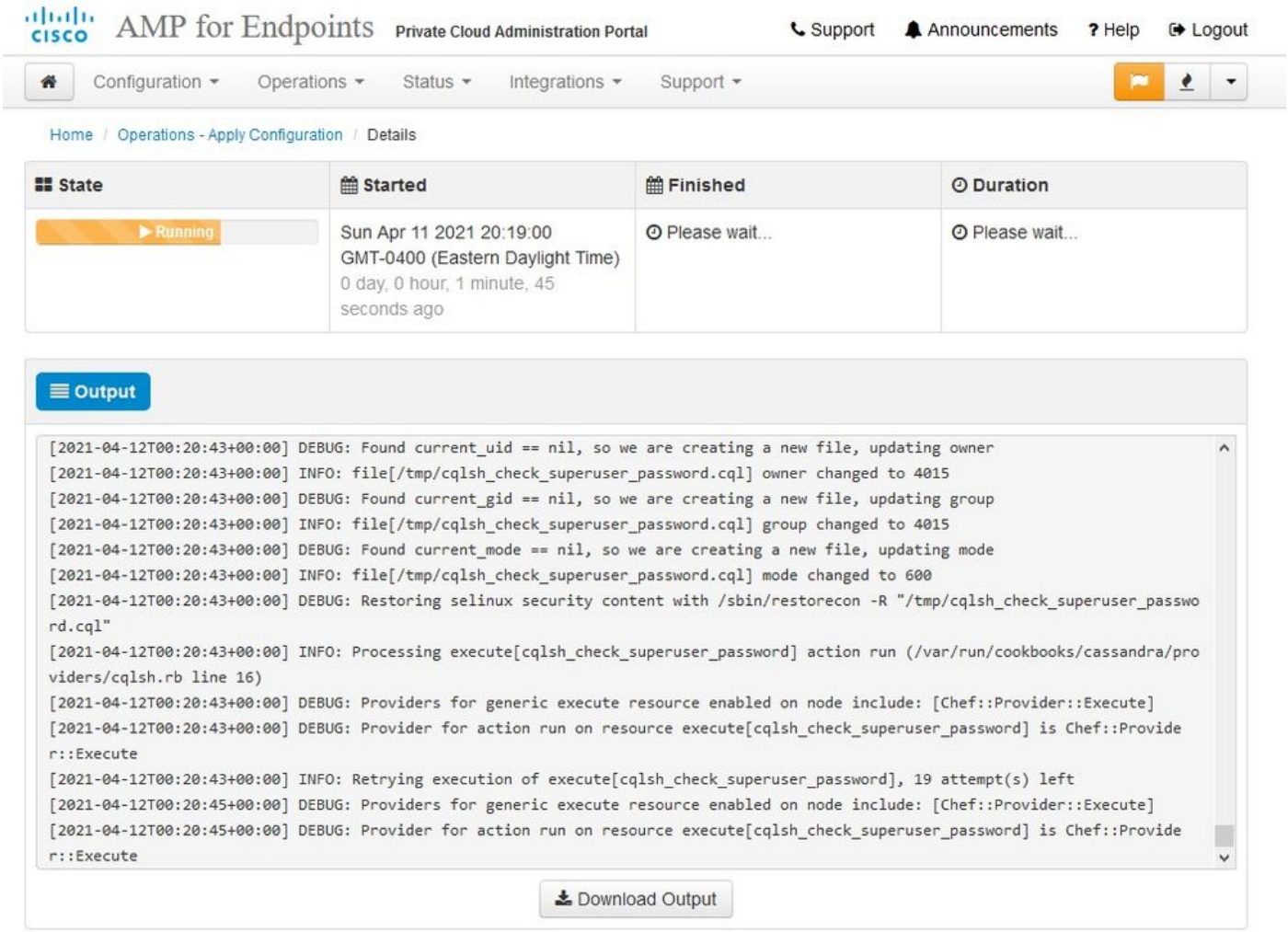
Depois de alguma solução de problemas, a única solução correta foi configurar o servidor DNS.

```
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
```

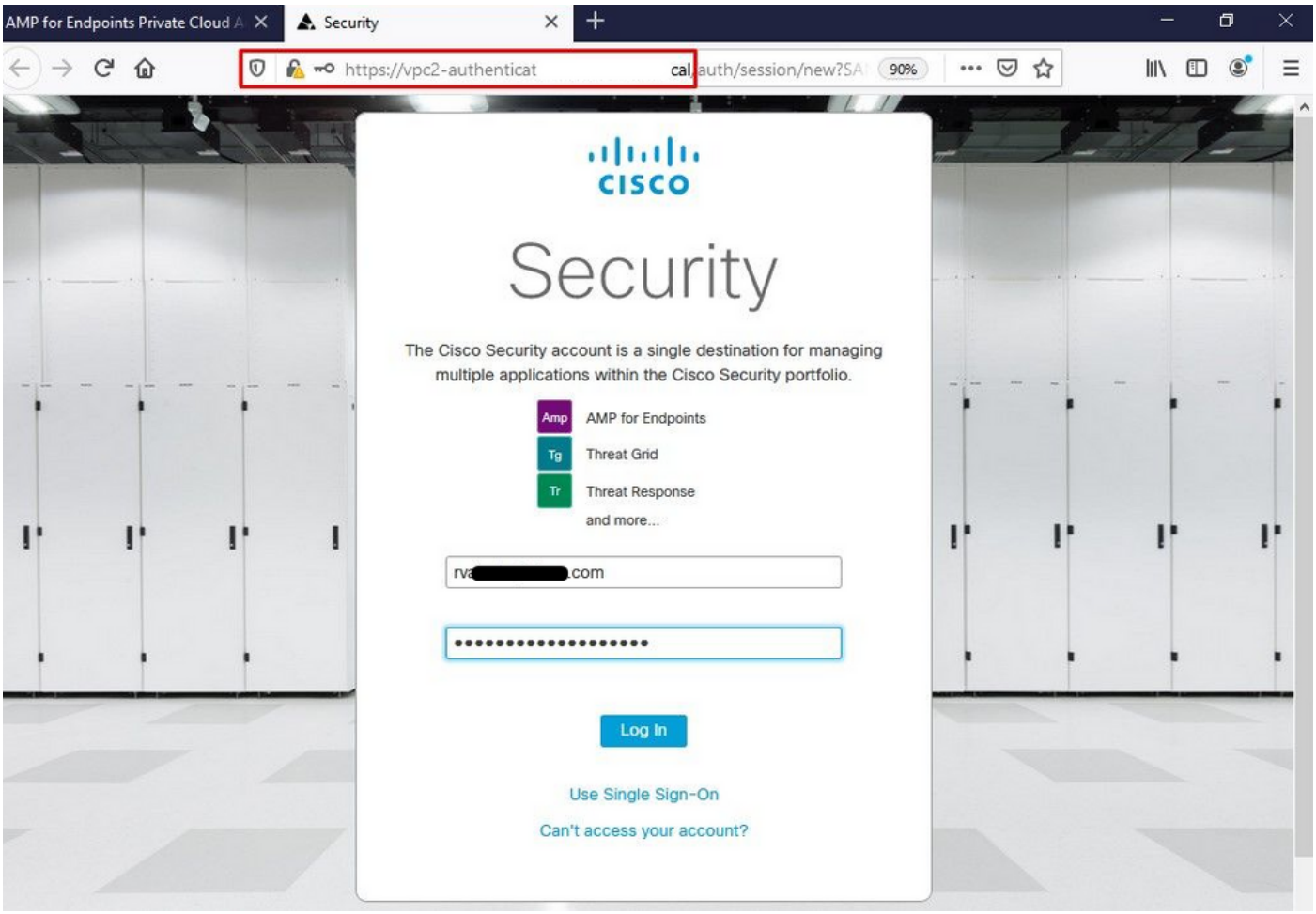
Depois de registrar todos os FQDNs no servidor DNS e alterar o registro na Nuvem privada virtual de DNS público para o servidor DNS, tudo começa a funcionar como deveria.


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.

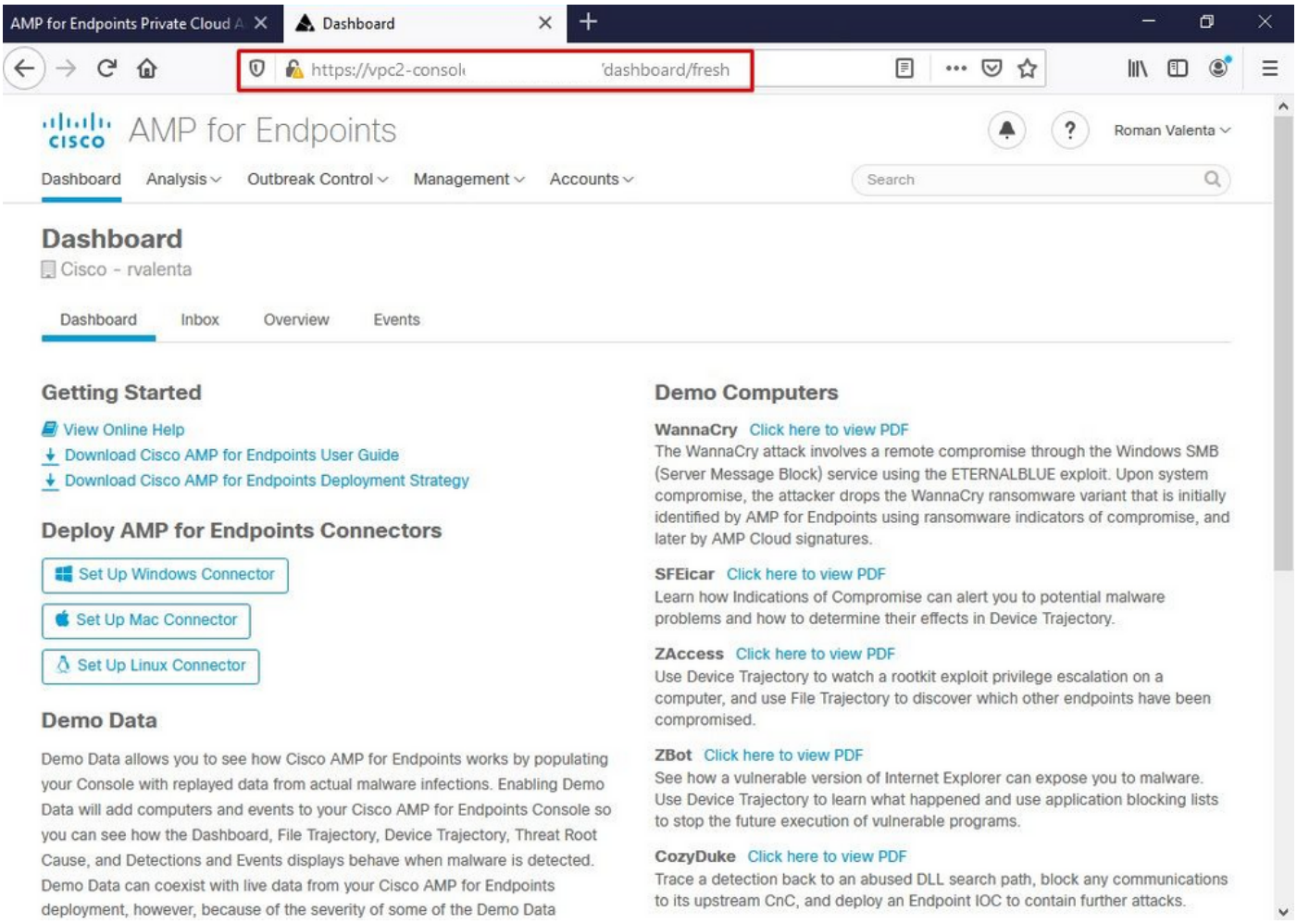


Neste ponto, você poderá fazer login e baixar o conector

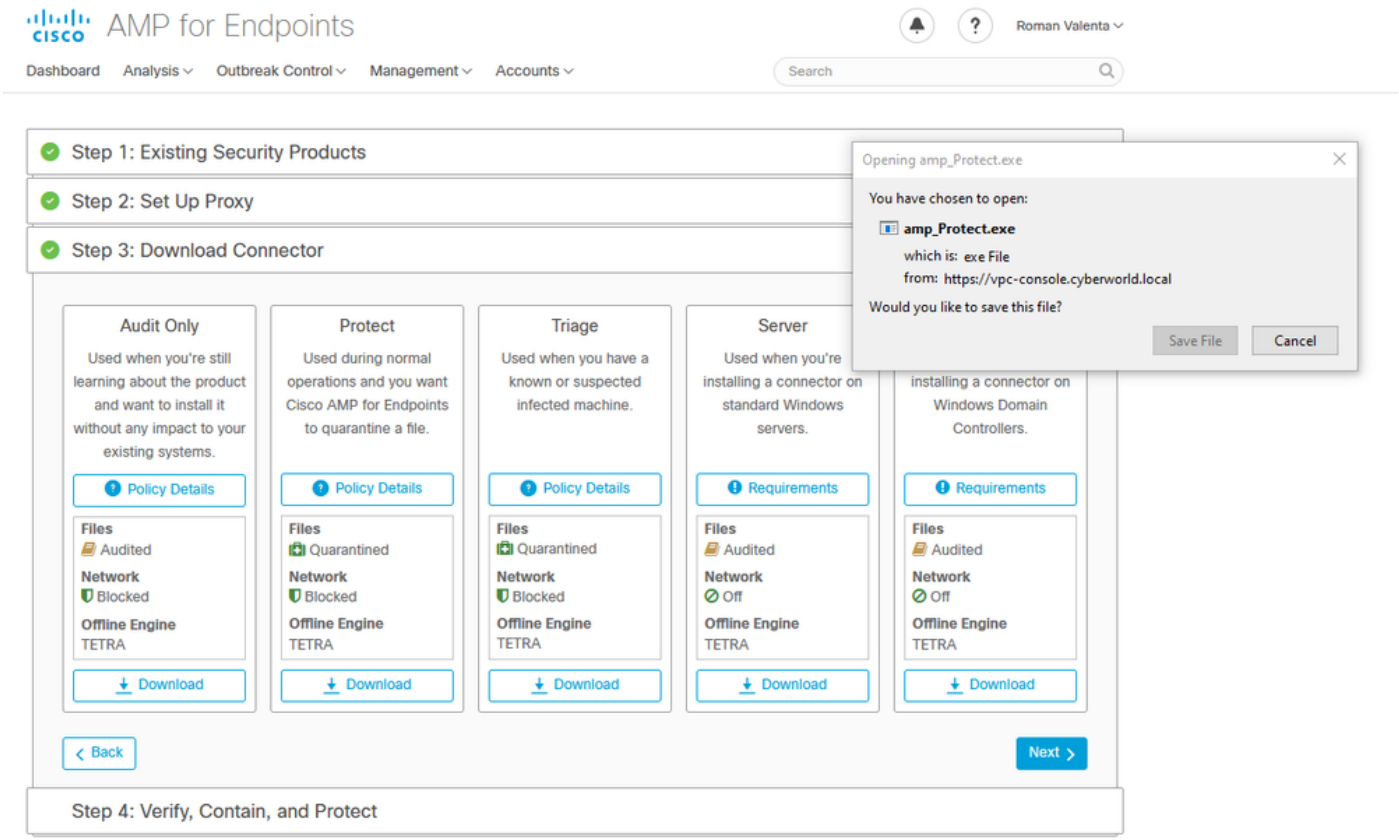


Você recebe o assistente inicial de política de Ponto de Extremidade Seguro para seu ambiente. Ele o orienta na seleção de produtos antivírus que você usa, se houver, bem como proxy e os tipos de políticas que você deseja distribuir. Selecione o botão Configurar... apropriado, dependendo do sistema operacional do conector.

Você obtém a página Produtos de segurança existentes, como mostrado na imagem. Escolha os produtos de segurança que você usa. Ele gera automaticamente exclusões aplicáveis para evitar problemas de desempenho nos endpoints. Selecione Avançar.

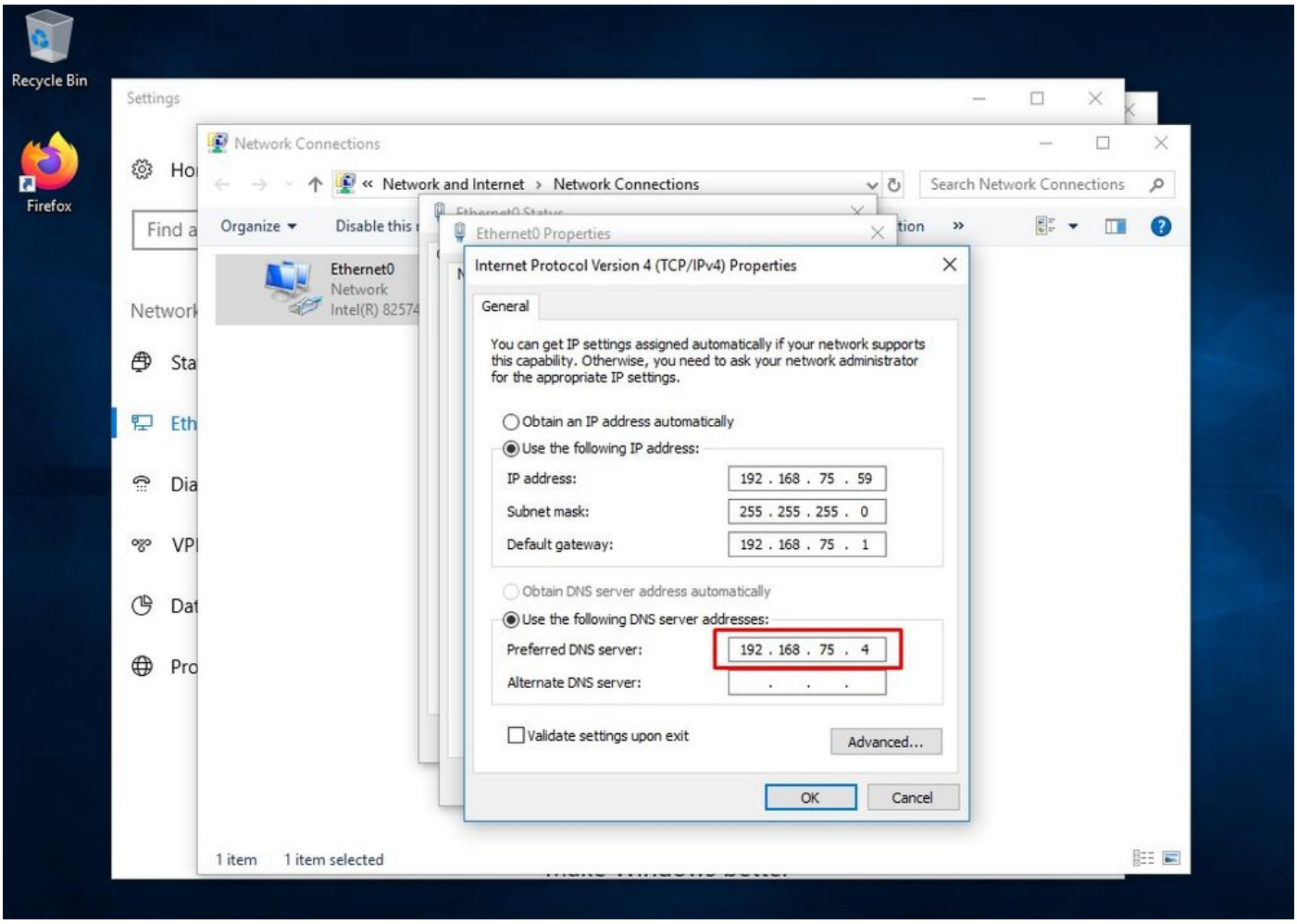


Baixar conector.

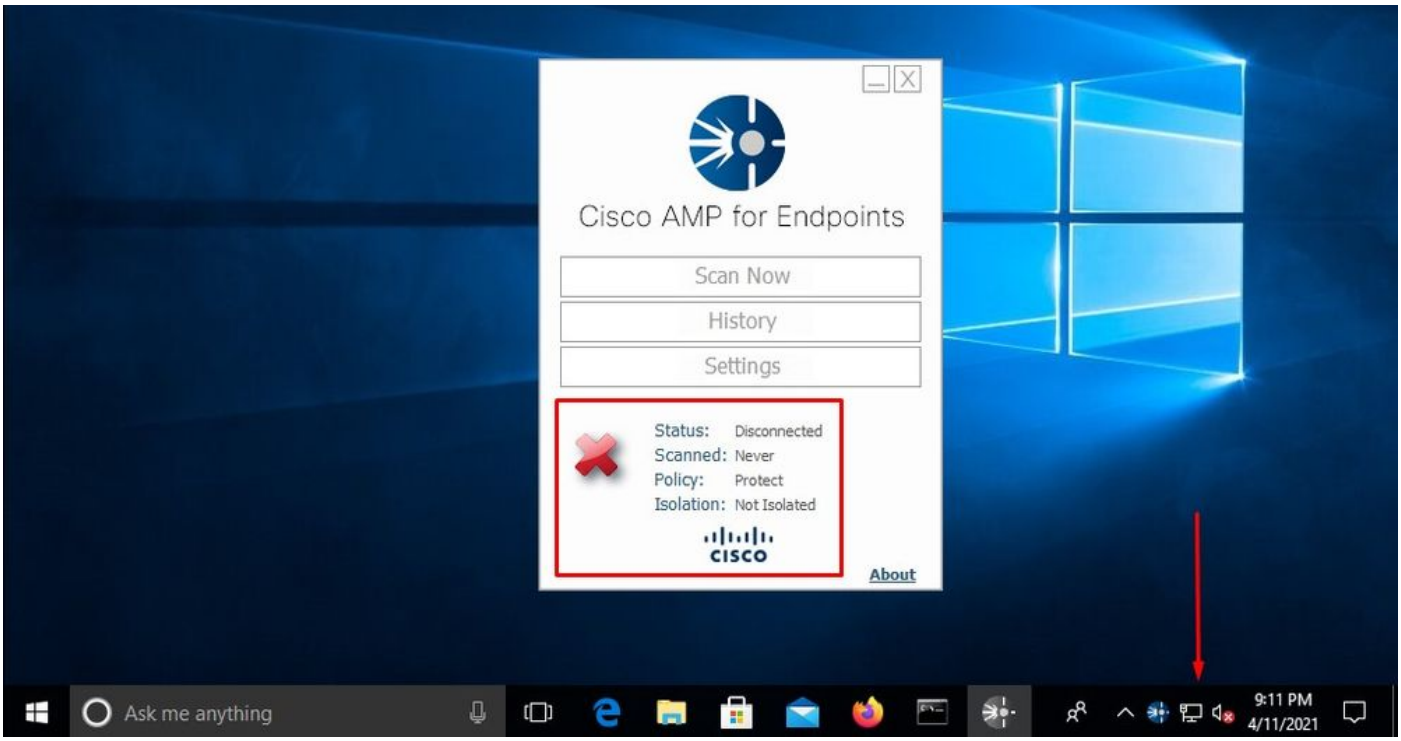


Problema #2 - Problema com CA Raiz

O próximo problema que você pode enfrentar é que se você usar seus próprios certificados internos é que após a instalação inicial, o conector pode aparecer como desconectado.



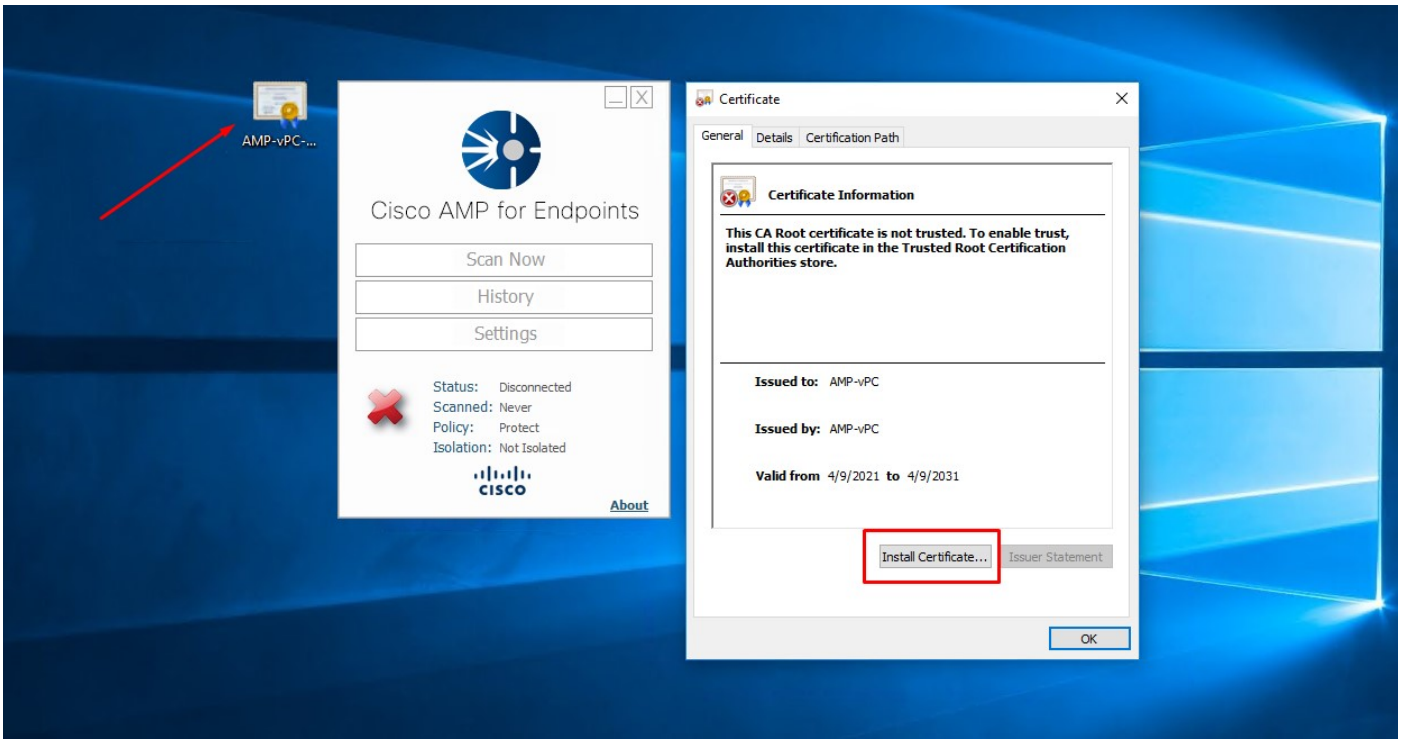
Depois de instalar o conector, o Secure Endpoint pode ser visto como Desconectado. Execute o pacote de diagnóstico e examine os logs; você poderá determinar o problema.

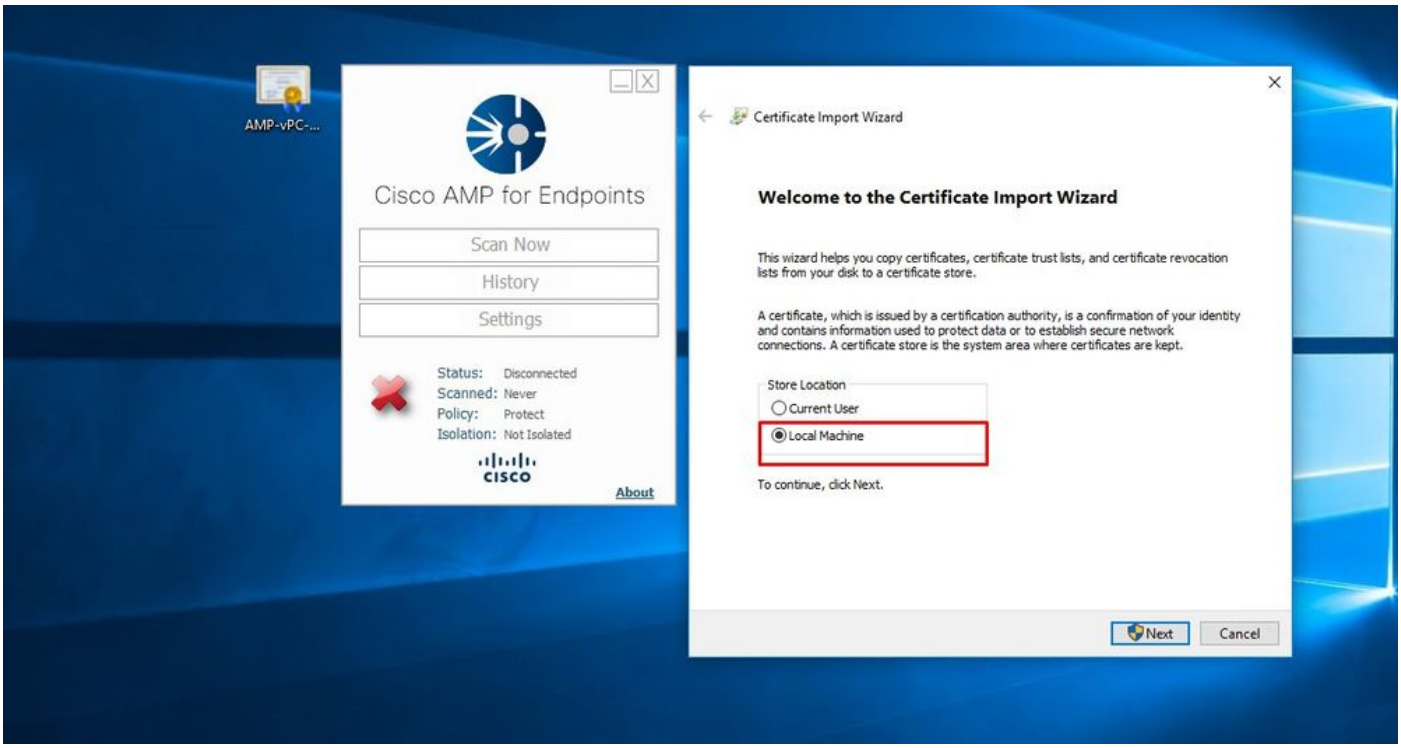


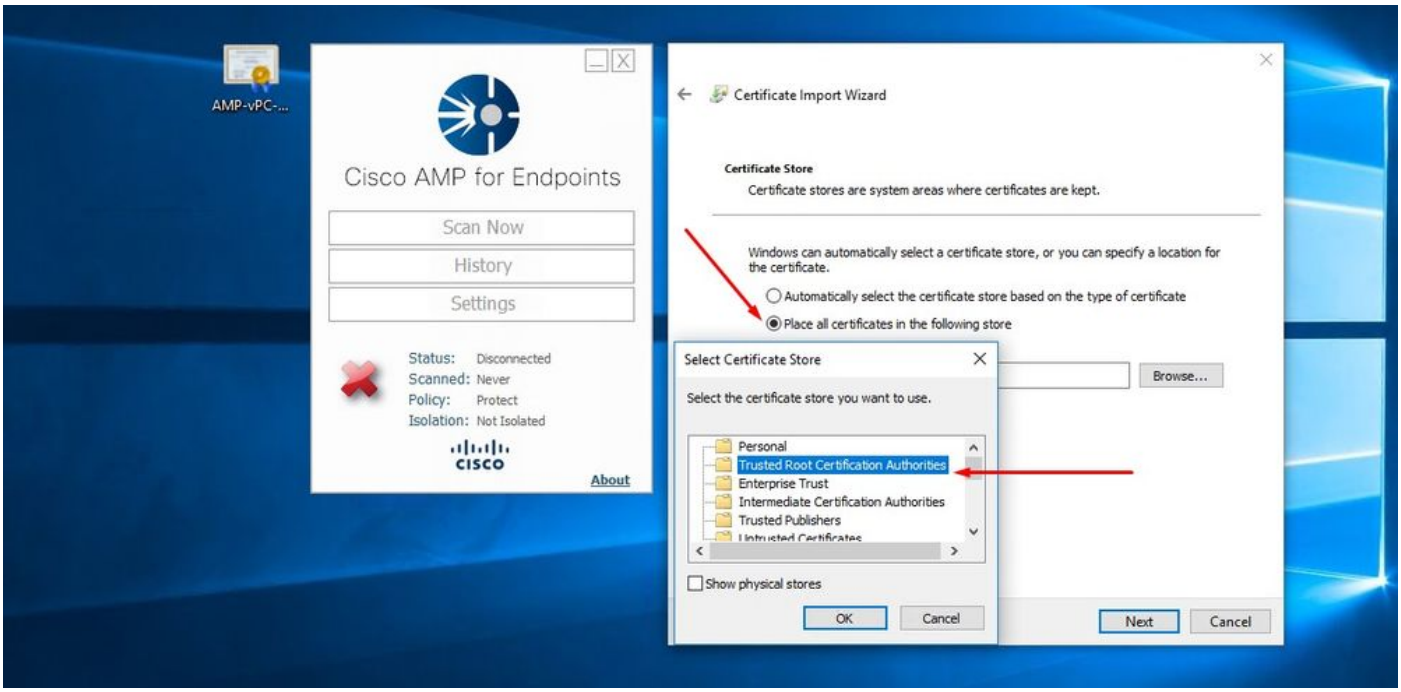
Com base nessa saída coletada do pacote de diagnóstico, você pode ver o erro de CA raiz

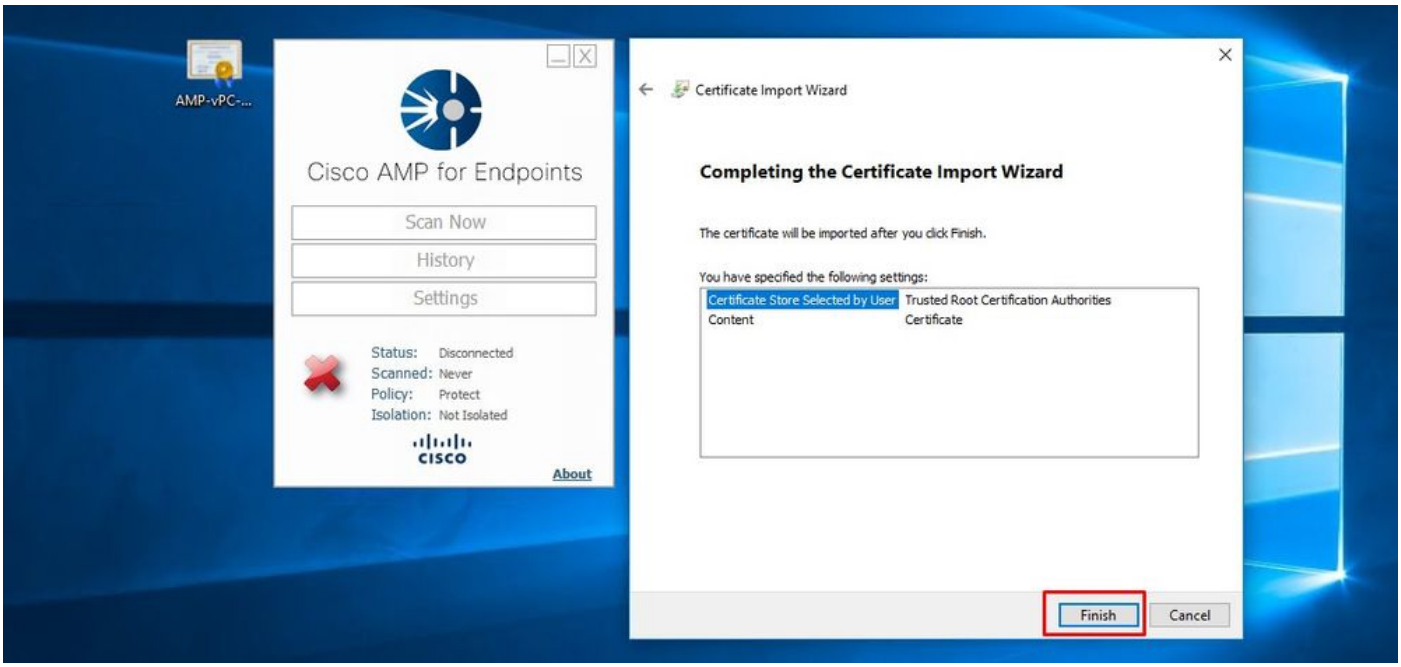
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60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

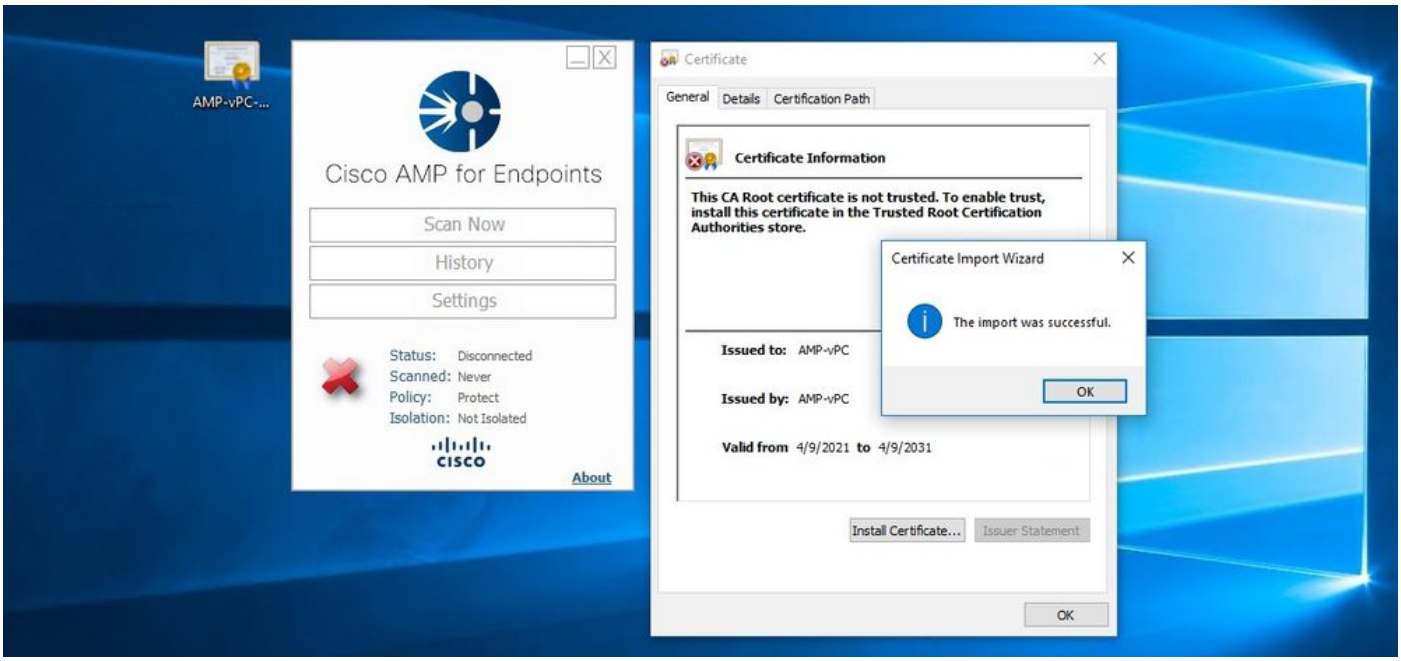
Depois de carregar a CA raiz no repositório de CA raiz confiável e reiniciar o serviço de Ponto de Extremidade Seguro. Tudo começa a funcionar como esperado.

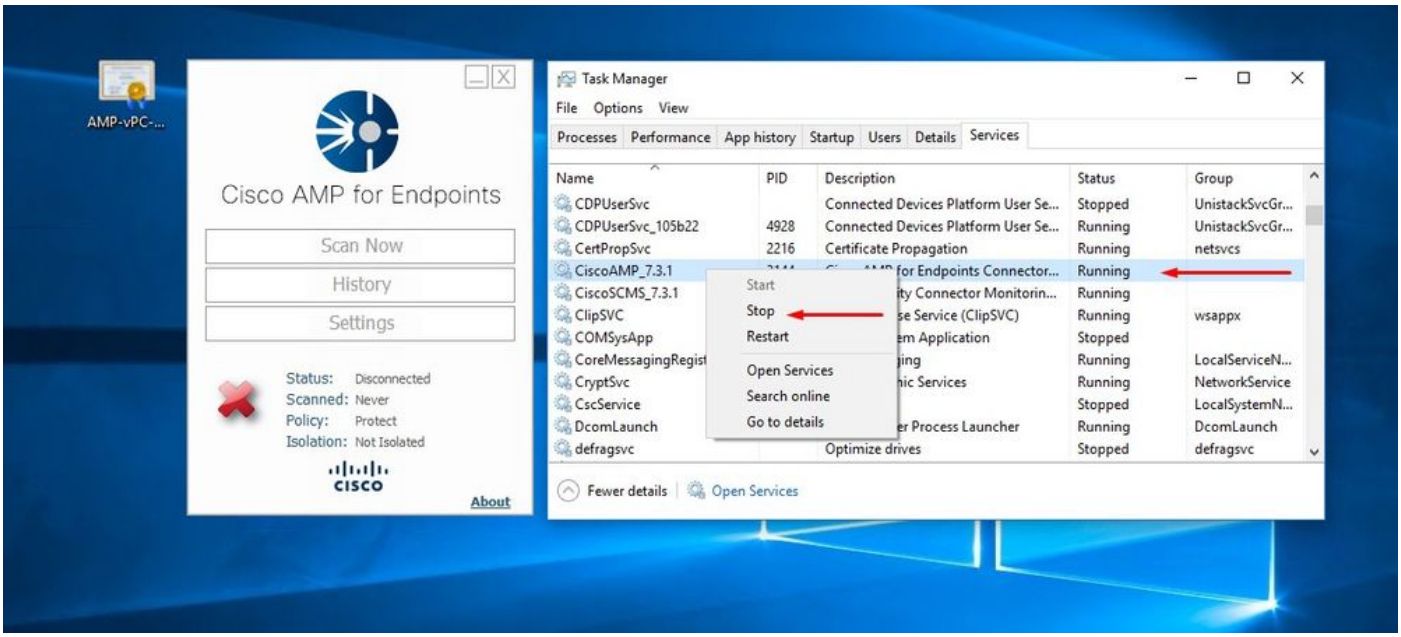




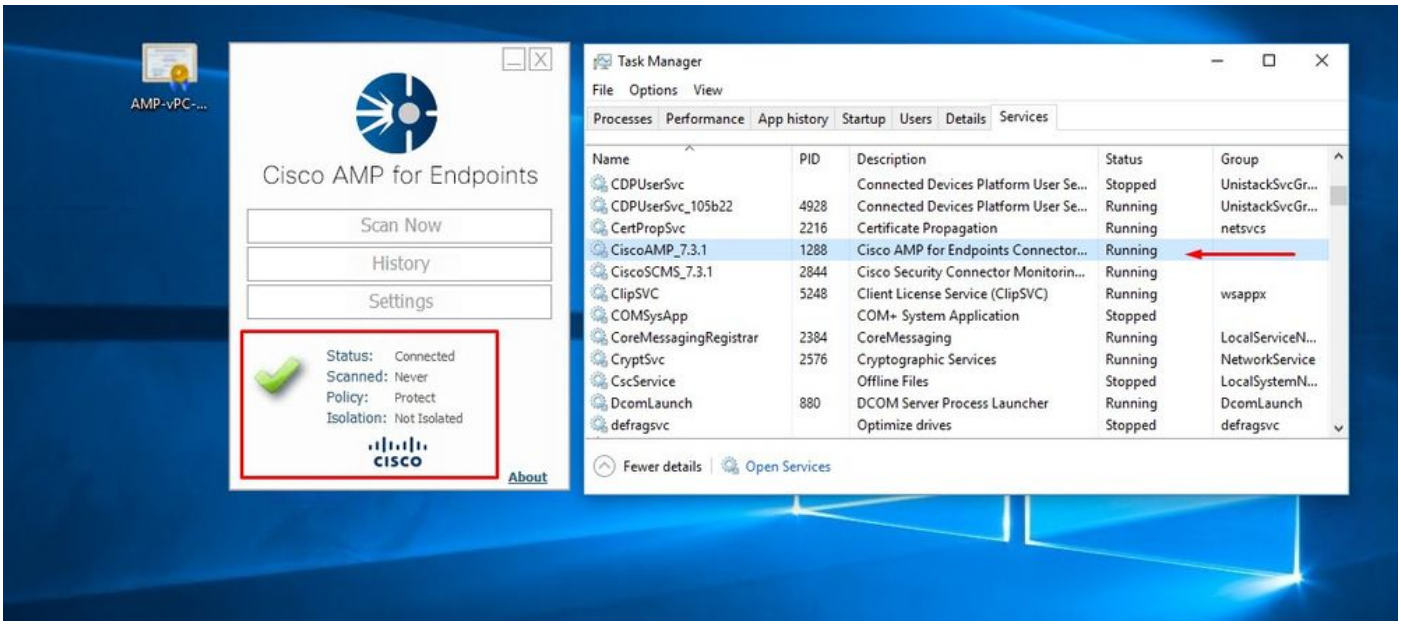

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
About
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, 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

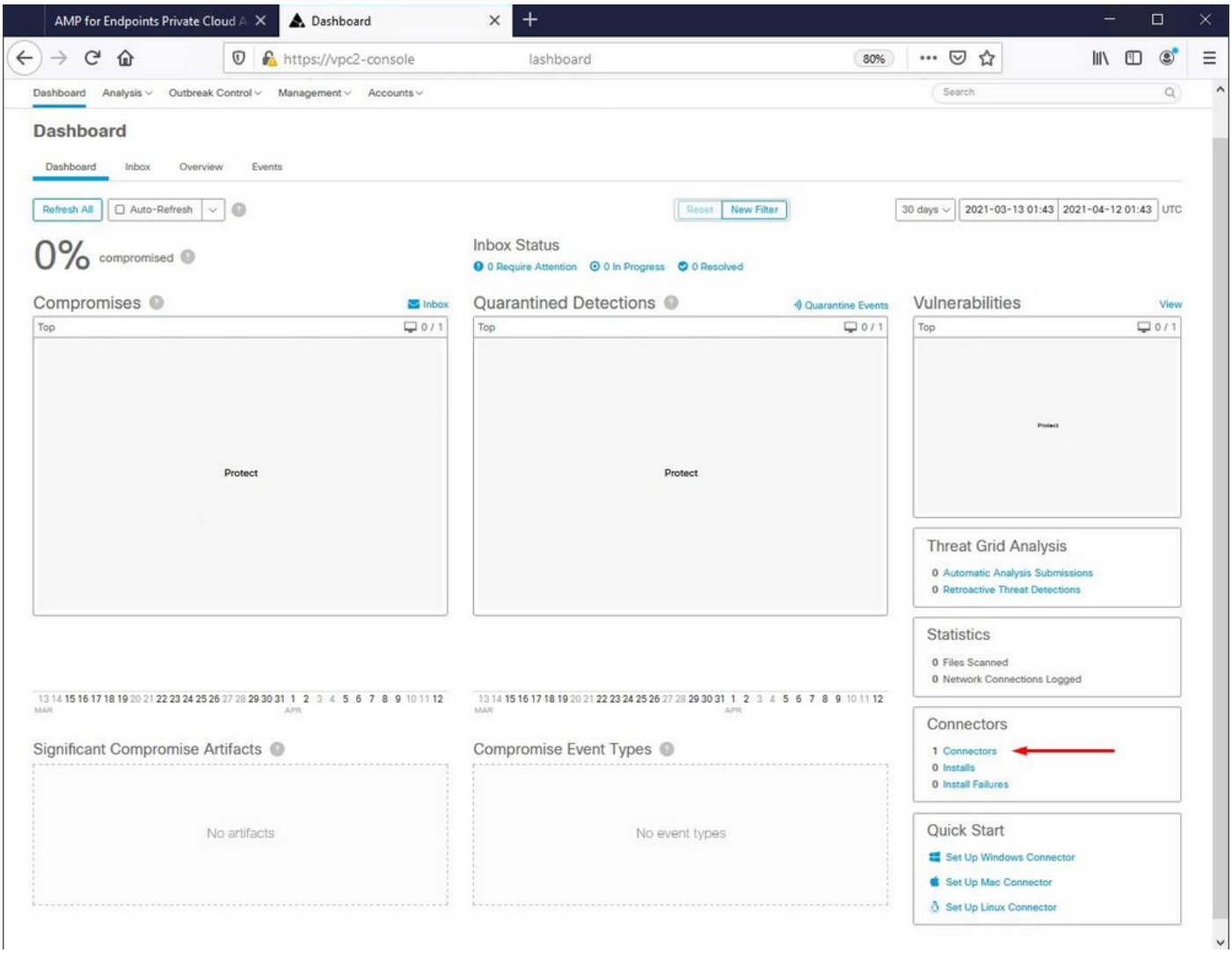

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
About
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel



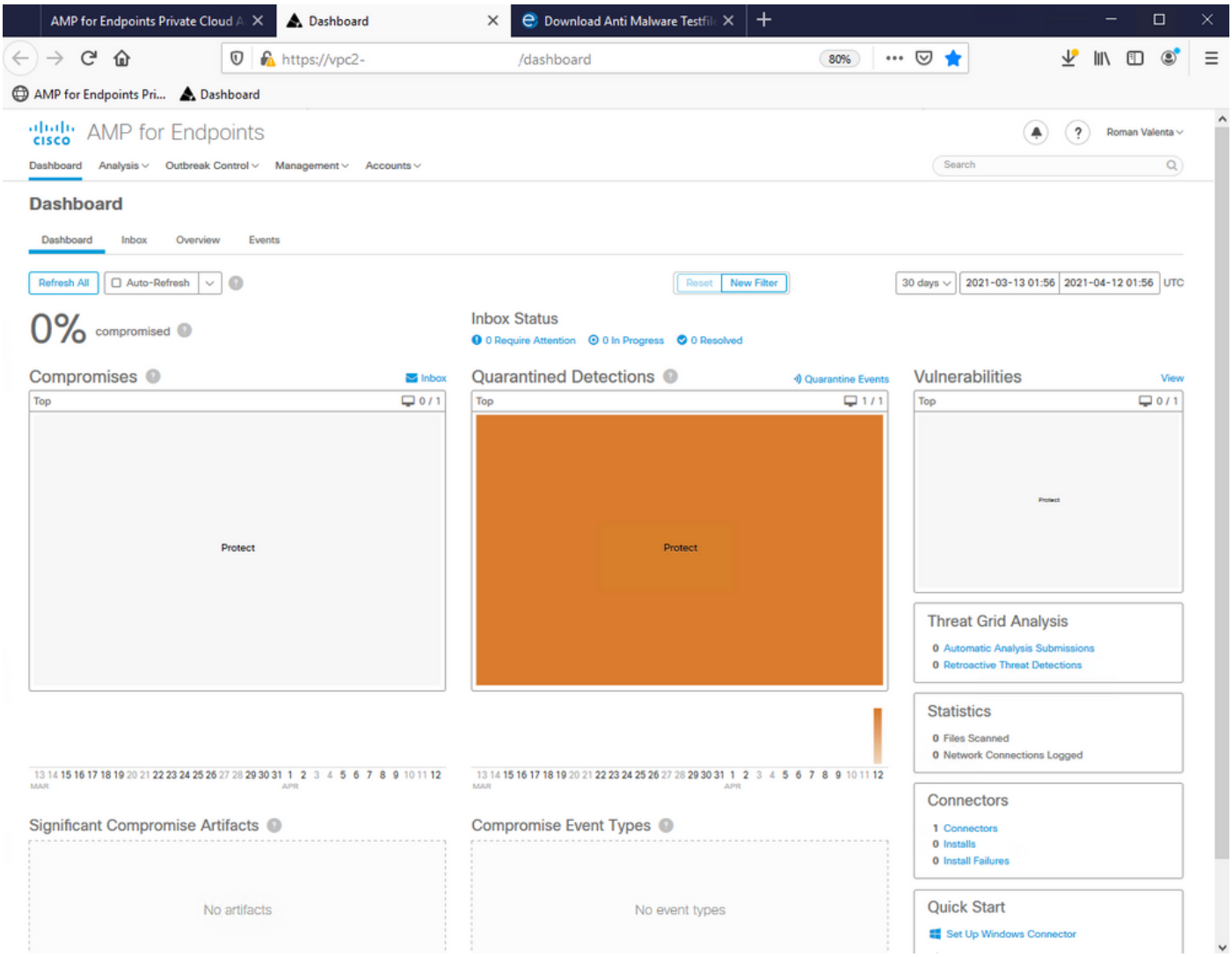


Depois que devolvermos o conector de serviço do Secure Endpoint, ele se tornará on-line conforme esperado.





Atividade mal-intencionada testada


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
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
Significant Compromise Artifacts
No artifacts
Compromise Event Types
No event types

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.