

Instalação e configuração de nuvem privada virtual de endpoint segura

Contents

[Introdução](#)

[Pré-requisitos](#)

[Implantação de VPC](#)

[Instalação da VM](#)

[Configuração inicial da interface do administrador](#)

[Configuração inicial do vPC via GUI da Web](#)

[Configuração](#)

[Services](#)

[Pacote de atualização AirGap](#)

[Problema #1 - Espaço esgotado no Repositório de Dados](#)

[Problema #2 - Atualização antiga](#)

[Troubleshooting Básico](#)

[Problema #1 - FQDN e Servidor DNS](#)

[Problema #2 - Problema com CA Raiz](#)

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.

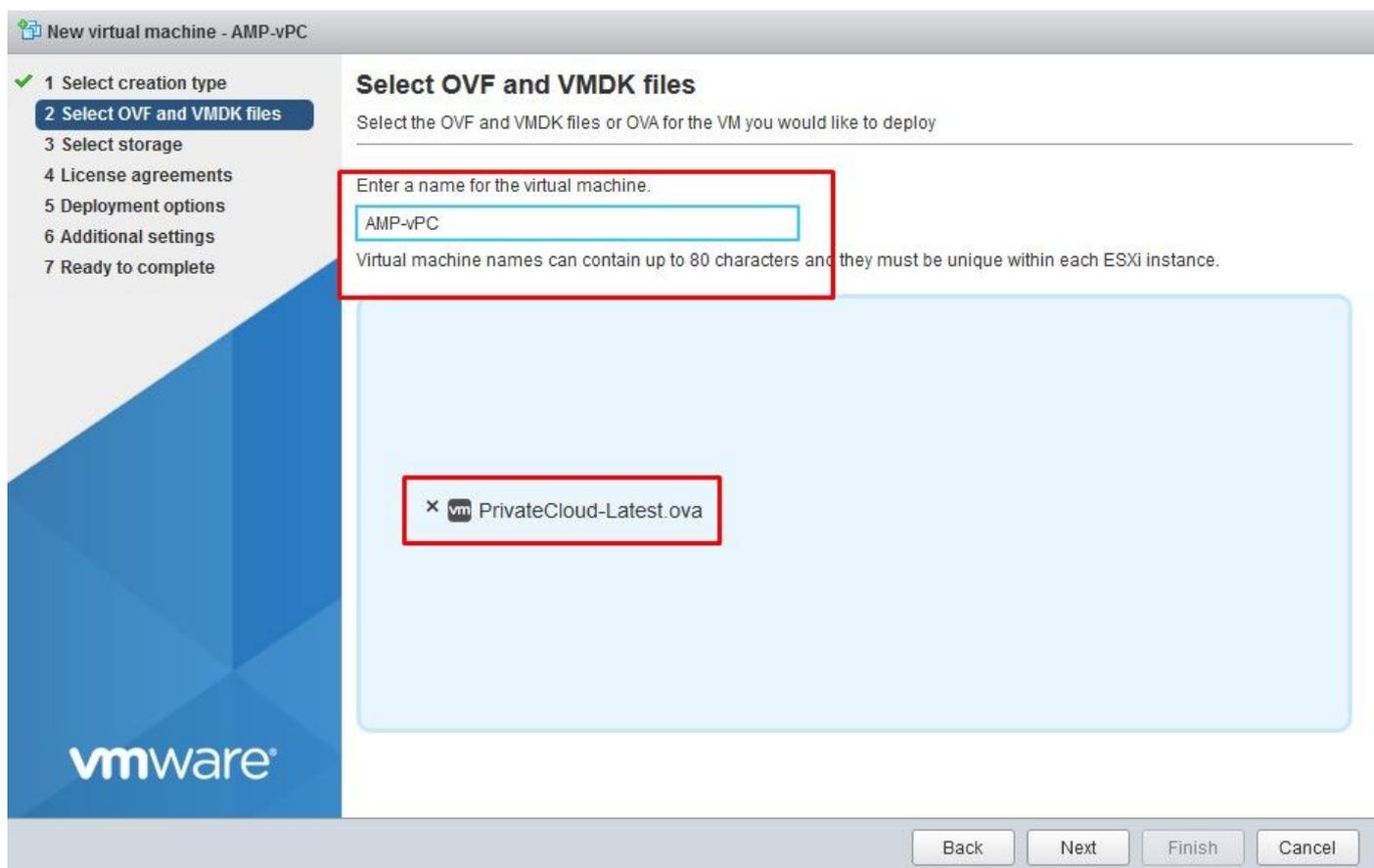
Implantação de VPC

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.



New virtual machine

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

Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file**
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

vmware

Back Next Finish Cancel

New virtual machine - AMP-vPC

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

Select storage

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

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	Supported	Single
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	Supported	Single

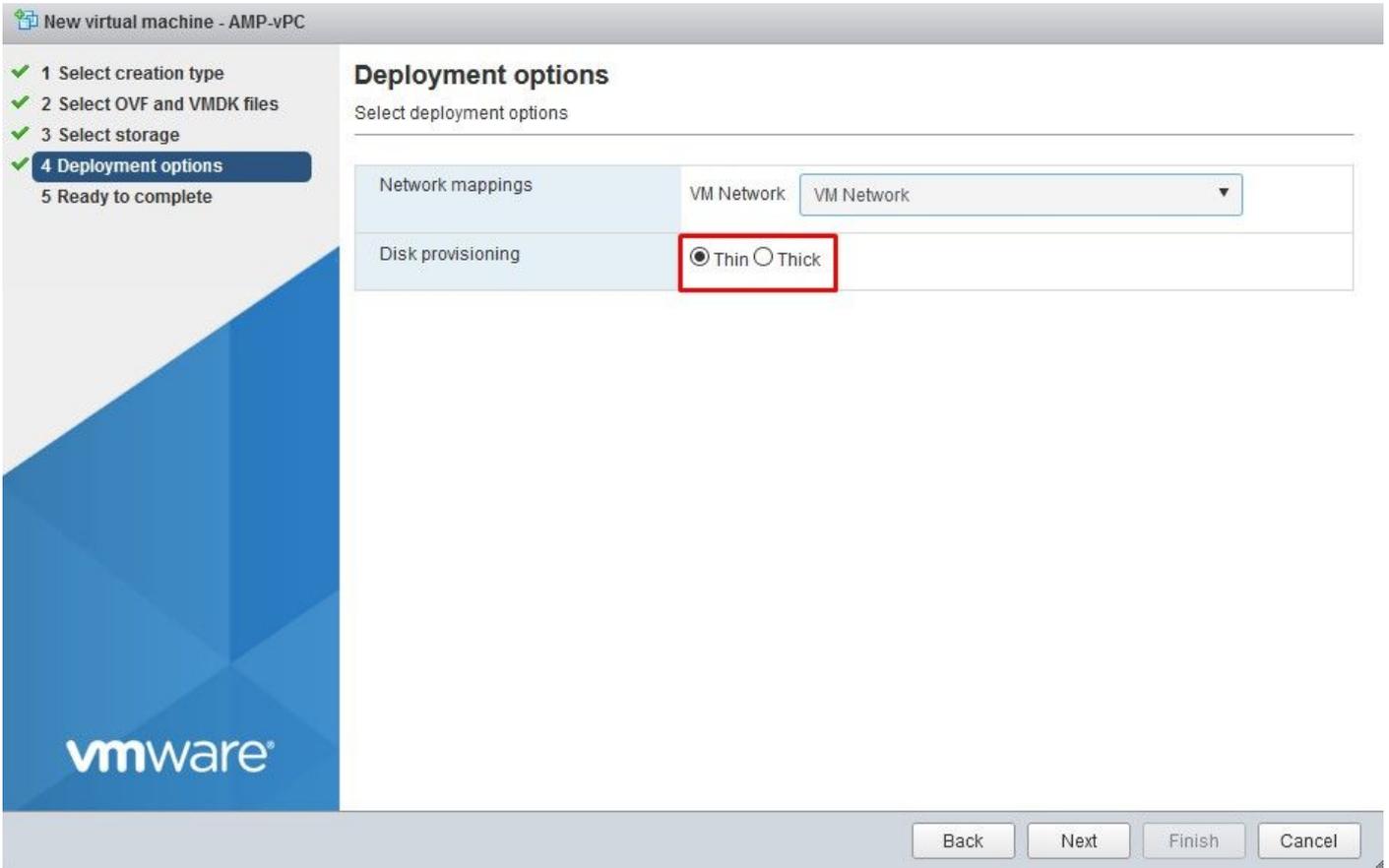
4 items

vmware

Back Next Finish Cancel

✎ 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.



The screenshot shows the 'New virtual machine - AMP-vPC' wizard in VMware Workstation. The left sidebar lists five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains a 'Select deployment options' section. Under 'Network mappings', the 'VM Network' is set to 'VM Network'. Under 'Disk provisioning', the 'Thin' radio button is selected and highlighted with a red box, while the 'Thick' radio button is unselected. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

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.

New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

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

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

Back Next Finish Cancel



Configuração inicial da interface do administrador

New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

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

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

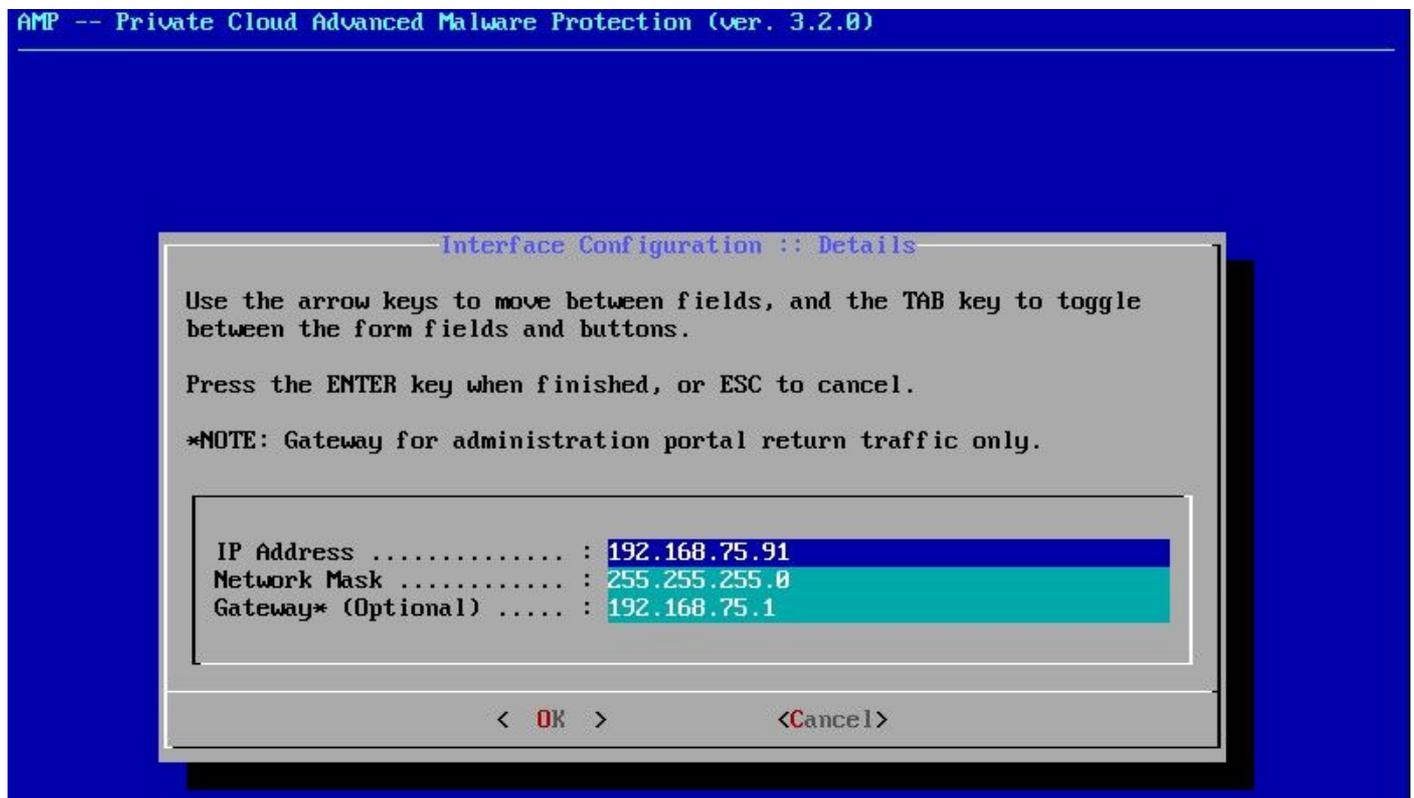
Back Next Finish Cancel



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.

Interface Configuration :: Mode

Would you like to configure your interface with DHCP?

< Yes > < No >

Main Menu

Your AMP Private Cloud device can be managed at:

URL : https://192.168.75.208
MAC Address ... : 00:0c:29:a6:4a:11
Password : PGBd~HbCgZ

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

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

60%

< OK >

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.

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

ERROR: The interface failed to reconfigure.

```
=====
```

Press ENTER key to continue...

-

Interface Configuration :: Details

Use the arrow keys to move between fields, and the TAB key to toggle between the form fields and buttons.

Press the ENTER key when finished, or ESC to cancel.

*NOTE: Gateway for administration portal return traffic only.

IP Address	: 192.168.75.92
Network Mask	: 255.255.255.0
Gateway* (Optional)	: 192.168.75.1

< OK > <Cancel>

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 badlab
--- /etc/ssh/sshd_config      2021-04-09 13:25:01.969995024 +0000
+++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.889389544 +0000
@@ -18,7 +18,7 @@
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
-ListenAddress 192.168.75.208
+ListenAddress 192.168.75.92

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

```

```
Restarting eth0...
```

```
Reconfiguring...
```

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

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.

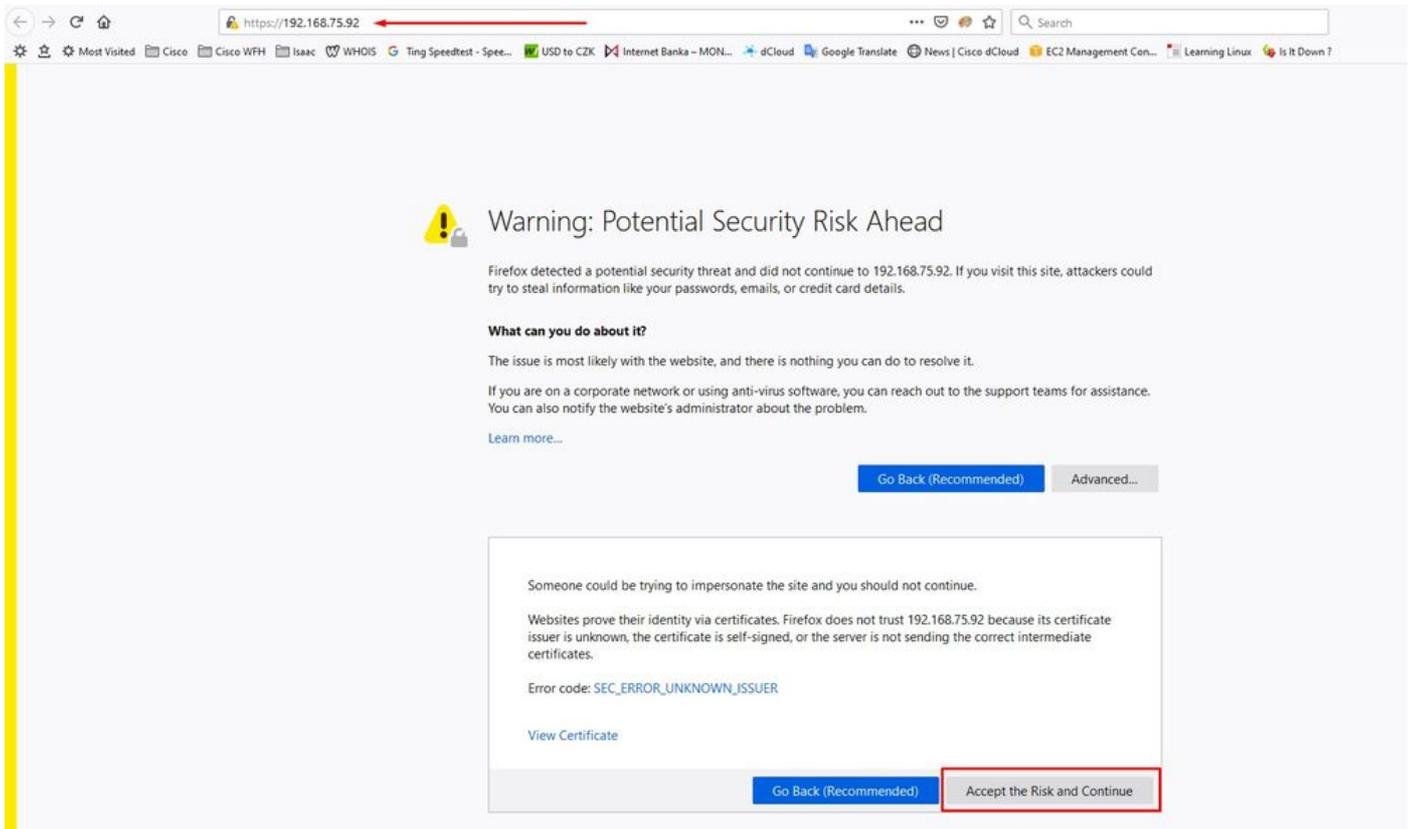


Configuração inicial do vPC via GUI da Web

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:

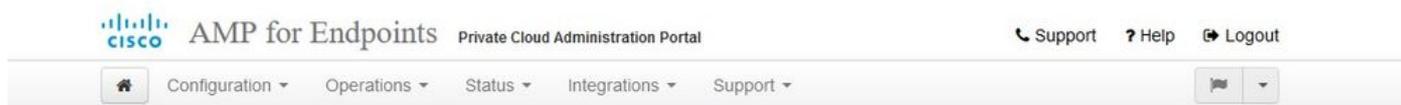
Depois de fazer login, você será solicitado a redefinir a senha. Use a senha inicial do console no campo Antiga senha. Use sua nova senha no campo Nova senha. Insira novamente sua nova senha no campo Nova senha. Selecione em Alterar senha.



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.



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

Warning
Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the device console.

Old one time password

Change Password

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.



Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License

Install or Restore

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

Clean Installation

Start >



Restore

Local Remote Upload

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

+ Choose Restore File

/data

Start >

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.



Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License

License

Device ID
EG[REDACTED]V5

License
No license has been installed.

Install New License

license + Upload License File

.....

Upload License



License was successfully uploaded



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

License

Device ID
E60[redacted]/5

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

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

Next >

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.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Welcome to Private Cloud

Before you begin

AMP for Endpoints Private Cloud needs certain network and infrastructure resources in place.



You will be asked to provide this information as you proceed through the installation. For more information and examples, please refer to the Private Cloud Deployment Strategy guide.



Two Static IP Addresses

One for administrative use, and the other for enterprise-facing services.



DNS Server

Provides hostname resolution to the Private Cloud device.



Hostnames and Trusted Certificates

One hostname and trusted certificate for each of the following services:

- Authentication.
- AMP for Endpoints Console.
- Disposition Server.
- Disposition Server - Extended Protocol.
- Disposition Update Service.
- Firepower Management Center Link.

Note: Hostnames can not be changed once the device has finished installation.



SMTP Server

Used for emails, alerts, and notifications.



NTP Server

Provides time synchronization across your Private Cloud device and endpoints.



External Internet connection (Proxy Mode only)

Proxy Mode devices perform anonymized disposition queries against the Cisco Cloud.

Next >

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



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Deployment Mode

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

Cloud Proxy

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

Standalone

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

≡ ≡ AIRGAP SOMENTE ≡ ≡



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Deployment Mode

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

Cloud Proxy

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

Standalone

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

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Standalone Operation

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

Air Gap

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

⌘ ⌘ AIRGAP 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.

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

AMP for Endpoints Console Account

Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

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

Next >

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

Hardware Requirements

Hardware Requirements Not Met
Your current configuration does not meet the hardware requirements.

It is recommended that you shutdown this device and adjust its hardware allocation to meet or exceed the minimum requirements. If you proceed, you may experience system instability.

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

Shutdown [I understand the risks >](#)

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

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

Virtual Hardware | VM Options

Add hard disk | Add network adapter | Add other device

CPU	8		
Memory	131072	MB	It will work with 48Gb as well
Hard disk 1	376.52343	MB	
Hard disk 2	17.272949	GB	
Hard disk 3	1.7216082	TB	
Hard disk 4	4.765625	GB	
SCSI Controller 0	LSI Logic Parallel		
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect	
Network Adapter 2	VM Network	<input checked="" type="checkbox"/> Connect	
CD/DVD Drive 1	Host device	<input type="checkbox"/> Connect	
Video Card	Specify custom settings		

Save | Cancel

Uma vez reiniciados, continuamos de onde paramos.

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Hardware Requirements

✓ **Hardware Requirements Met**

Your current configuration meets or exceeds the hardware requirements.

Hardware Configuration

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

Next >

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:



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

Start Installation

Network Configuration

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

Administration Portal eth0 / 00:0C:29:A6:4A:11
IP Assignment 192.168.75.92
[More details](#)

Interface Configuration eth1 / 00:0C:29:A6:4A:1B
IP Assignment 192.168.75.209
[More details](#)

IP Assignment Static
IP Address 192.168.75.93
 Check for IP Address conflicts
Subnet Mask 255.255.255.0
Gateway 192.168.75.1

DNS

Primary DNS Server 8.8.8.8 Use public DNS temporary.
Secondary DNS Server

Next (Applies Configuration)

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.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Date and Time

NTP Servers

192.168.75.254 Optional Verify hostname resolution

Current System Time

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

Next >

≡ ≡ AIRGAP SOMENTE ≡ ≡



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Prepare amp-sync

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

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

[Download amp-sync](#)

Next >

≡ ≡ AIRGAP 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.

Installation Options

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

Certificate Authorities

Add Certificate Authority

No certificate authorities have been uploaded to this device.

Next >

Installation Options

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

Configuration

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

Services

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

Add Certificate Authority

Certificate Root (PEM .crt) Disable Strict TLS Check

- ✓ Certificate file has been uploaded.
- ✓ Certificate is in a readable format.
- ✓ Certificate start and end dates are valid.
- ✓ Certificate end date is later than 20 months from today.
- ✓ Certificate file only contains one certificate.
- ✓ Certificate does not use sha-1 signature algorithm.
- ✓ Certificate using RSA keys must use a key size of 2048 or more.

AMP-vPC-Root-CA.pem + Add Certificate Root

Cancel

Upload

Installation Options

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

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓

Certificate Authorities

Add Certificate Authority

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

Next >

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.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes the Cisco logo, 'AMP for Endpoints', 'Private Cloud Administration Portal', and links for 'Support', 'Help', and 'Logout'. Below this is a secondary navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. On the left, a sidebar menu lists 'Installation Options' (Install or Restore, License, Welcome, Deployment Mode, AMP for Endpoints Console, Account, Hardware Requirements) and 'Configuration' (Network, Date and Time, Certificate Authorities, Upstream Proxy Server, Cisco Cloud, Email, Notifications, Backup, SSH, Syslog, Updates). The main content area is titled 'Cisco Cloud' and contains two sections: 'Cisco Cloud Configuration' with a 'Region' dropdown set to 'Cisco Cloud, North America' and a 'View Hostnames (click to expand)' button; and 'Cisco Cloud Identity' with a 'Client Identity' field containing '0f476ea8[redacted]dbbc272a6c'. A green 'Next >' button is highlighted with a red box at the bottom right.

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.

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Notifications

Notification Frequency

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

Notification Addresses

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

Device Name

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

Next >

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.

Maintenance Mode

Sanity Check Failing

This page allows you to add and remove SSH keys on your Cisco AMP for Endpoints Private Cloud device. SSH keys allow administrators remote root authentication to the device. Only trusted users should be granted access.

Add SSH Key

Windows PuTTY

2021-11-17 23:01:01 +0000
created 20 days ago

2021-11-17 23:01:01 +0000
20 days since last update

Edit

```
ecdsa-sha2-nistp256 AAAAE2K...oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7Q6fd0g4vT9eD5XOXZd
I4DKhrTNBv8/77T0d/Jagx7Przxs=
```

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"

Installation Options
Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

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

+ Choose Key

+ Choose Certificate

[Next >](#)

Sem verificação TLS rigorosa

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and install

Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate

Disable Strict TLS Check Undo Replace Certificate

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

Next >

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.

An error occurred while processing your request.

- Hostname does not resolve

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

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

+ Choose Certificate

+ Choose Key

Next >

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.

- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓
- Services**
- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

1. Download Recovery File

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

[Download](#)

2. Verify Recovery File

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

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

Recovery File Ready for Download
created less than a minute ago

[Next >](#)



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery ✓
- > Review and Install ✓

[▶ Start Installation](#)

Review and Install

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

Clean Installation

A clean installation will be performed.

Installation Type [Edit](#)

Cloud Proxy

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

AMP for Endpoints Console Account [Edit](#)

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

Recovery [Edit](#)

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

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

Clean Installation

A clean installation will be performed.

Installation Type ✎ Edit

Standalone Air Gap ←

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

AMP for Endpoints Console Account ✎ Edit

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

Recovery ✎ Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

⌘ ⌘ AIRGAP APENAS ⌘ ⌘

Você vê uma entrada similar como esta...

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

The device is installing...

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

State	Started	Finished	Duration
▶ Running	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```
le_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP::StreamHandler calling Chef::HTTP::Decompressor::NoopInflater#handle_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: HTTP server did not include a Content-Length header in response, cannot identify truncated downloads.
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::CookieManager#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONOutput#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONInput#handle_stream_complete
[2021-04-10T17:36:20+00:00] INFO: Storing updated cookbooks/rabbitmq/recipes/default.rb in the cache.
[2021-04-10T17:36:20+00:00] DEBUG: Creating directory /var/run/cookbooks/rabbitmq/recipes
```

Download Output

Após concluir a instalação, pressione o botão de reinicialização

The device is installing...

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

State	Started	Finished	Duration
✓ Successful	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 24 minutes, 14 seconds ago	Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 3 minutes, 17 seconds ago	0 day, 0 hour, 20 minutes, 57 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration against the AMP for Endpoints Disposition Server has previously succeeded.

=====
Installation has finished successfully! Please reboot!
=====
```

Download Output

≈ ≈ AIRGAP SOMENTE ≈ ≈

The device is installing...

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

State	Started	Finished	Duration
✓ Successful	Tue Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 21 minutes, 21 seconds ago	Tue Nov 02 2021 15:07:02 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 49 seconds ago	0 day, 0 hour, 20 minutes, 32 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-11-02T19:07:01+00:00] INFO: Running report handlers
[2021-11-02T19:07:01+00:00] INFO: Report handlers complete
[2021-11-02T19:07:01+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-11-02T19:07:01+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-11-02T19:07:01+00:00] DEBUG: Forked instance successfully reaped (pid: 29292)
[2021-11-02T19:07:01+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration is not possible in air gap mode.
=====
Installation has finished successfully! Please reboot!
=====
```

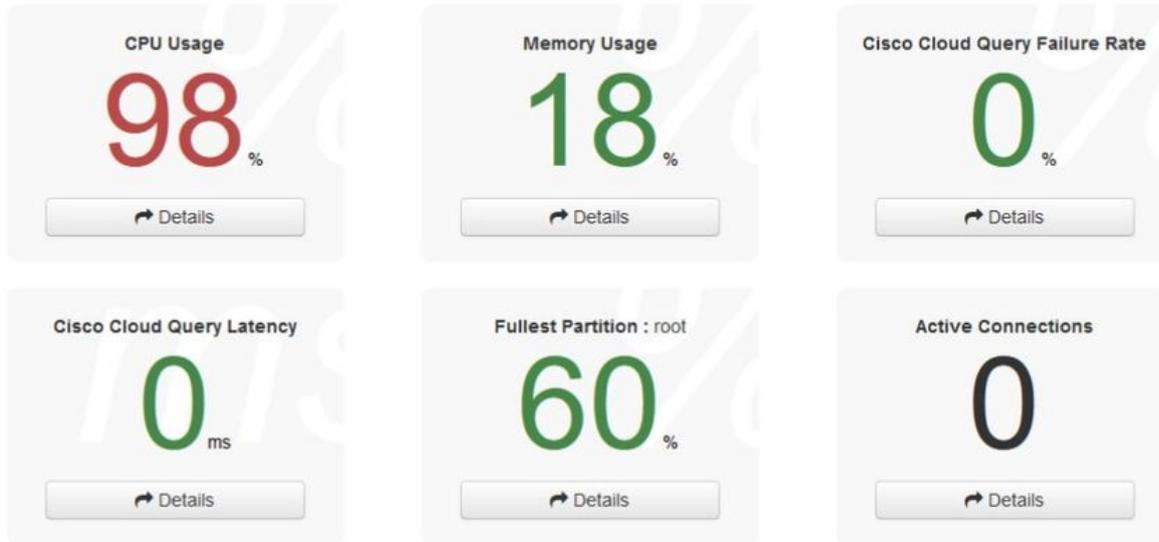
Download Output

⌘ ⌘ AIRGAP 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.



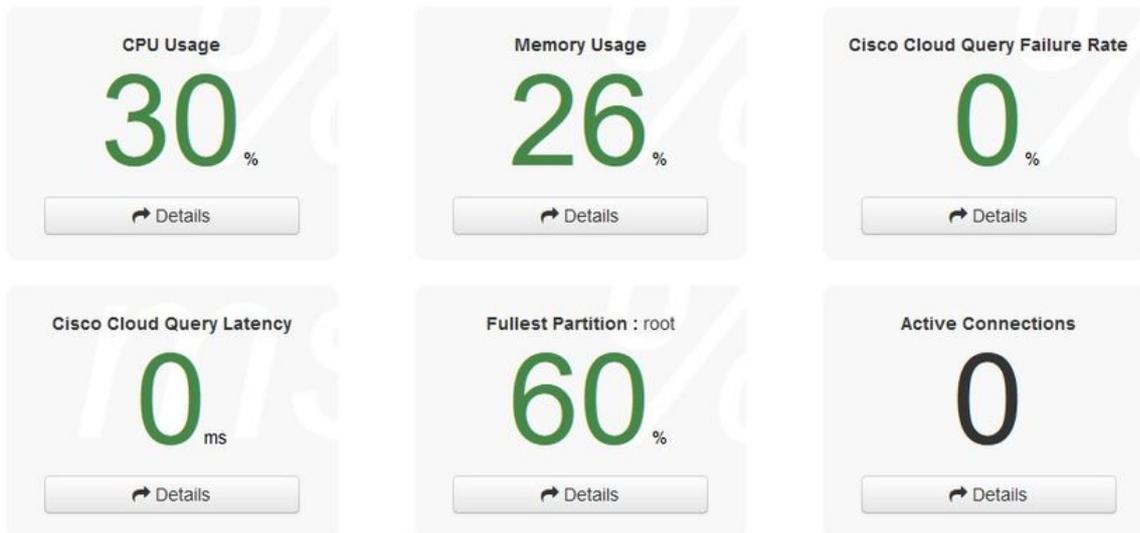
Key Metrics



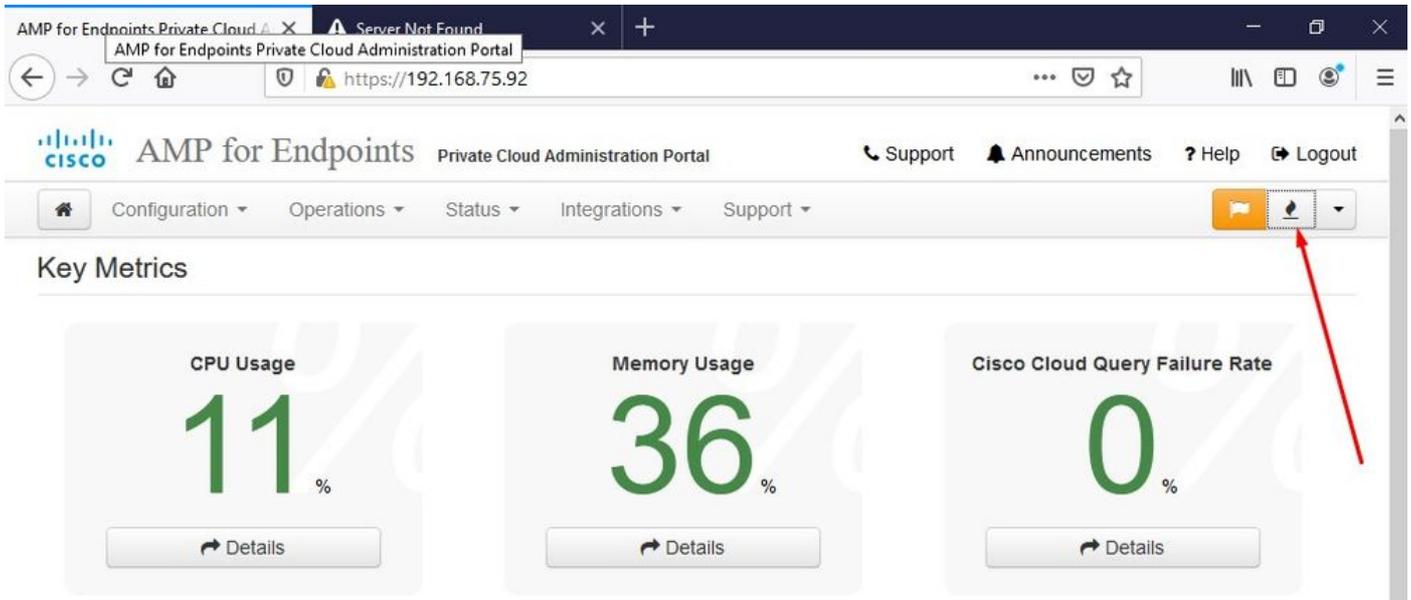
Depois de alguns minutos...



Key Metrics



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.



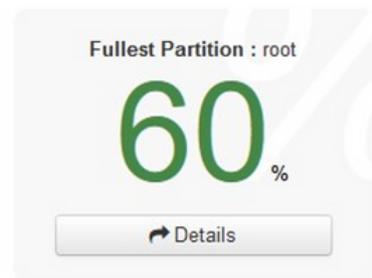
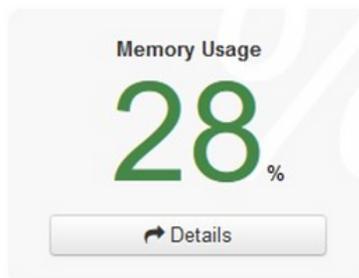
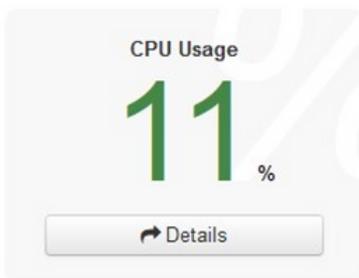
Sanity Check Failing

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

Details

FAIL: A Protect DB snapshot has not been loaded. Devices configured in standalone mode should have a Protect DB snapshot loaded. Protect DB snapshots contain threat intelligence about known clean and known malicious files.

Key Metrics



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

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

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked 1 minute ago; the update check failed.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

Checked 1 minute ago; the update check failed.

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. Dependendo 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

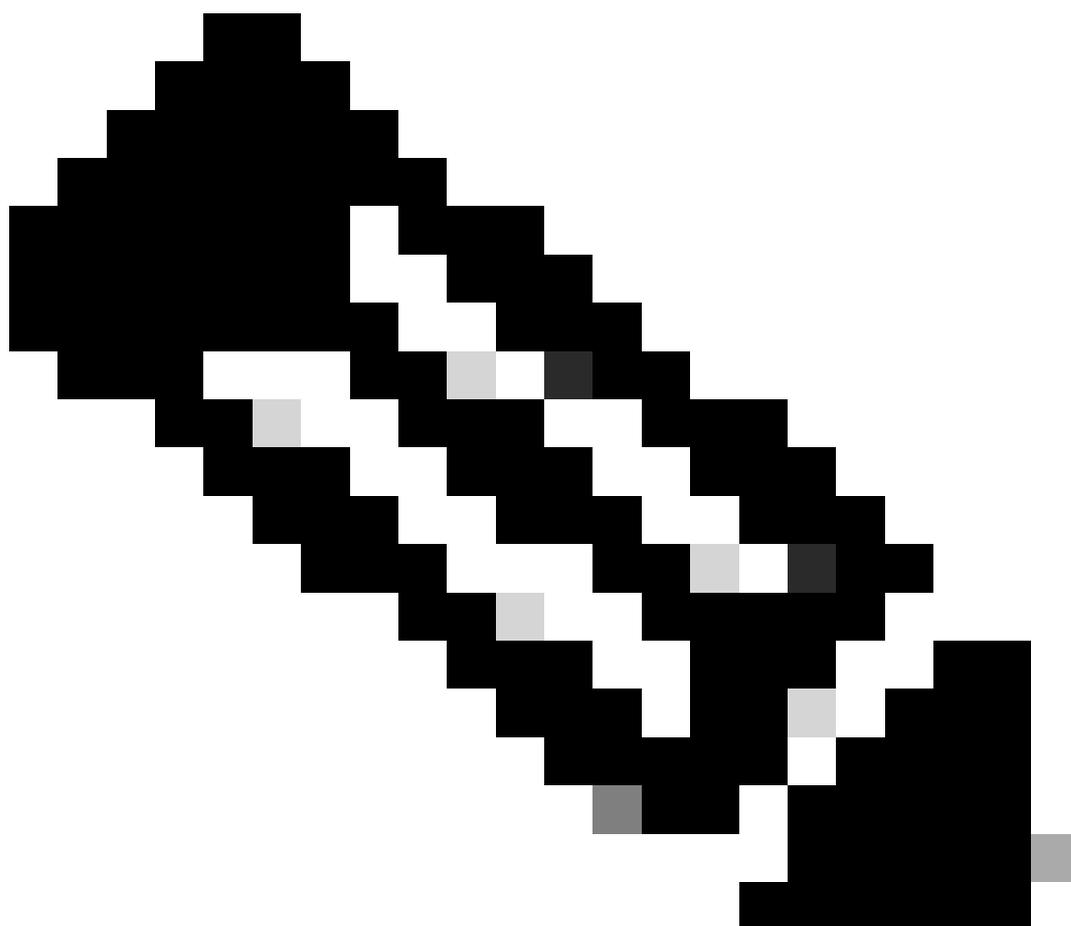
* VPC 3.8.x superior - > xorriso

```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2991 100 2991 0 0 15991 0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 11331 100 11331 0 0 98544 0 --:--:-- --:--:-- --:--:-- 97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 915k 100 915k 0 0 3324k 0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1094k 100 1094k 0 0 3302k 0 --:--:~ --:~:~ --:~:~ 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 135k 100 135k 0 0 747k 0 --:~:~ --:~:~ --:~:~ 756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 54480 100 54480 0 0 383k 0 --:~:~ --:~:~ --:~:~ 385k
```

```
User@VMStation-1 ~
99.91% done, estimate finish Thu Nov 4 08:39:50 2021
99.91% done, estimate finish Thu Nov 4 08:39:51 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:51 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:51 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:52 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
100.00% done, estimate finish Thu Nov 4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)

Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso

User@VMStation-1 ~
$
```



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

```
User@VMStation-1 ~
$ ./amp-sync all

=====
Prerequisite Program(s) Missing
=====

A prerequisite tool was not found in your PATH, or is not an appropriate
version. You must have the following tools installed in order for the AMP for En
dpoints
Air-Gap Update Tool to function:

    awk
    base64
    basename
    cat
    comm
    curl
    dirname
    mv
MISSING -> xorriso
            sha256 / sha256sum / shasum
            sort
            tr
            xmlstarlet

These tools should be available in both Windows Subsystem for Linux and most
Unix-like operating systems.
```

[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

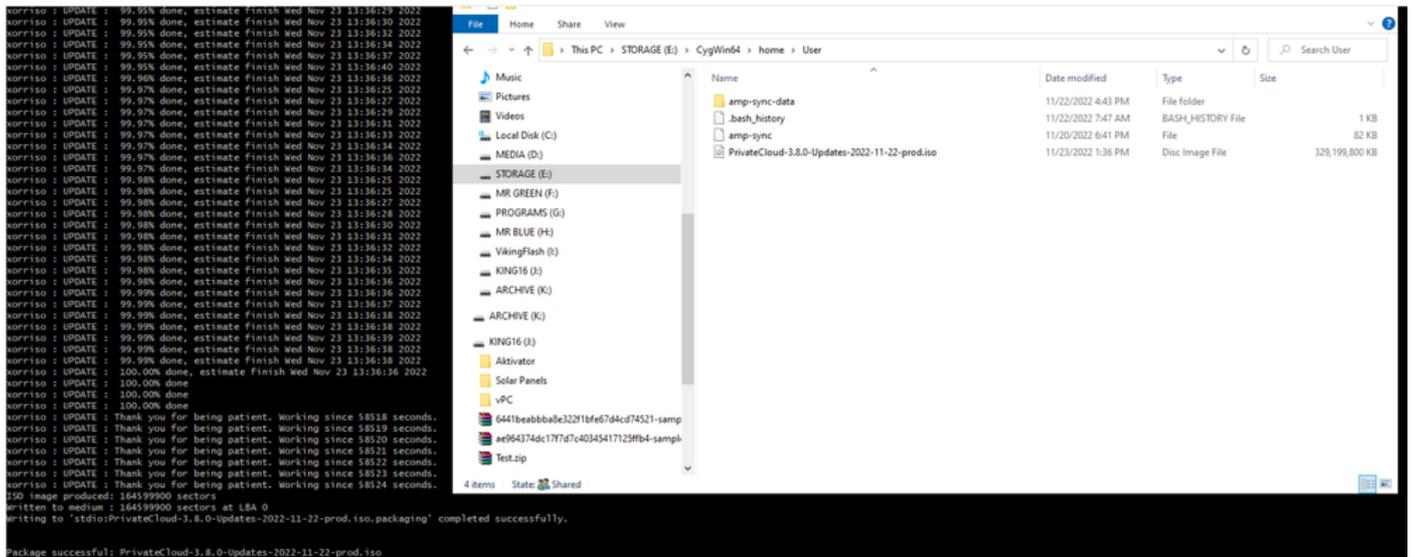
To run amp-sync you will first have to install xorriso and xmlstarlet.

- 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.



Sanity Check Failing

Backups create a copy of your configuration and databases.

Manual Backup

Perform Backup

Last Backup Successful

Transferring Backups To External Storage Is Recommended

To facilitate disaster recovery, you are strongly encouraged to transfer backup archives to a secure external backup location. Transfer of backup archives can be performed via download, sftp, or rsync.

Backup Job Details

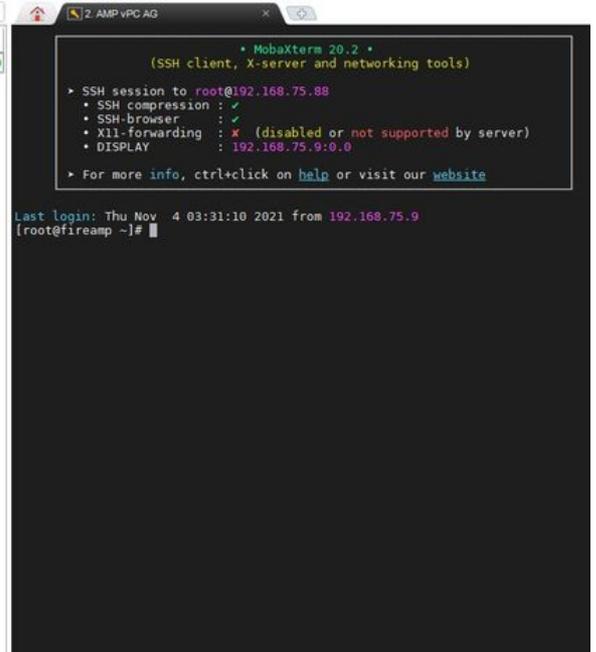
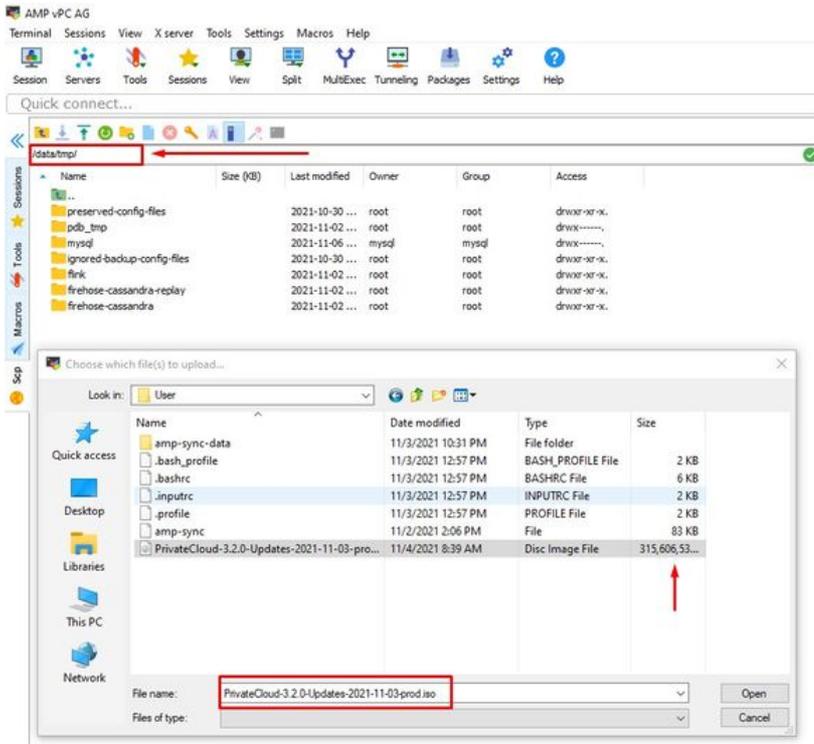
Previous Backups

The number of backups that will be stored on disk is: 1.

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20211106-0000.18.bak	738 MB	2021-11-06 00:03:43 +0000 about 17 hours ago	 

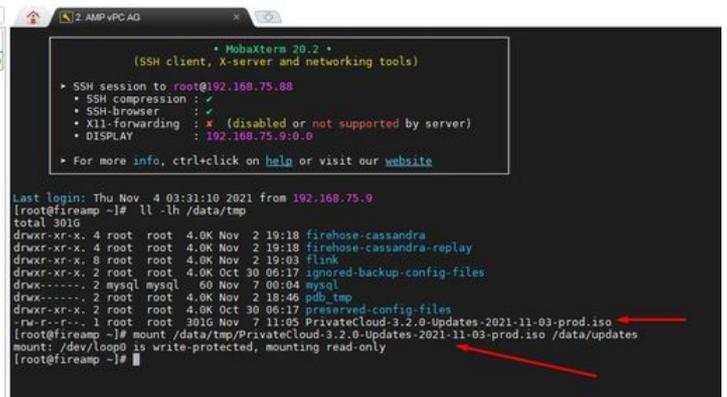
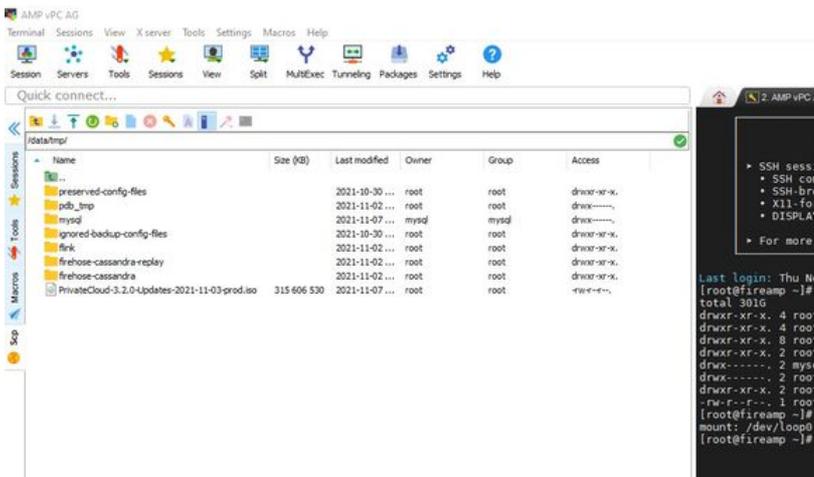
Transfira o ISO mais recente gerado com amp-sync para o VPC. Isso também pode levar várias horas com base na sua velocidade. Neste caso, a transferência levou mais de 16 horas

/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.

The screenshot displays the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. On the right, there are links for 'Announcements', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. A 'Sanity Check Failing' notification is visible in a red box. The main content area is divided into sections: 'Updates keep your Private Cloud device up to date.' with a 'Download amp-sync' button; 'Check Update ISO' button with a red arrow pointing to it and a 'Checking ISO for updates...' status; 'Content' section showing version '3.2.0_202010081917' with a status of 'ABSENT' and a message 'Import a Protect DB snapshot to your standalone device.'; and 'Software' section showing version '3.2.0_202010082118' with a message 'A software update is available.' and an 'Update Software' button.

Sanity Check Failing

Updates keep your Private Cloud device up to date. [Download amp-sync](#)

[Check Update ISO](#) ←

[Checking ISO for updates...](#)

Content

[3.2.0_202010081917](#)
Client Definitions, DFC, Tetra Content Version

[Update Content](#)

[Import Protect DB](#)

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked 9 minutes ago; the update check failed.

Software

[3.2.0_202010082118](#)
Private Cloud Software Version

[Update Software](#)

[A software update is available.](#)

Neste exemplo, eu continuo com Atualizar conteúdo primeiro

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

A content update is available.

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

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

Em seguida, selecione Importar Proteger BD.



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

20211102210054
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

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

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

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

Protect DB importing

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

State	Started	Finished	Duration
Running	2021-11-07 18:48:44 +0000 less than a minute ago	Please wait...	Please wait...

Output

```
Attempting to mount an ISO, if one is present.  
mount: special device /dev/cdrom does not exist  
Starting update.  
Stopping apply-cloud-deltas...  
Stopping authentication_web...  
Stopping authentication_worker...
```

Download Output

⚙️ Protect DB importing

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

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

☰ Output

```
Extraction 14.9GB at 6.6MB/s eta: 9:28:03 0% [---]
Extraction 14.9GB at 6.6MB/s eta: 9:28:21 6% [==]
Extraction 14.9GB at 6.6MB/s eta: 9:28:27 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:40 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:46 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:58 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:29:12 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:29:26 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [==]
Extraction 15.0GB at 6.6MB/s eta: 9:28:20 6% [==]
Extraction 15.0GB at 6.6MB/s eta: 9:28:28 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:44 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:51 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:48 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:29:10 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:29:23 6% [==]
```

⬇️ Download Output

⚙️ Protect DB importing

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

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

☰ Output

```
Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
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.

Maintenance Mode

The device is in maintenance mode. External services are unavailable.

Sanity Check Failing

Disabling TLS 1.0/1.1

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

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

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

The previous Protect DB import failed.

Checked 24 minutes ago; the update check failed.

Software

3.5.3_202111080345
Private Cloud Software Version

Update Software

Checked 24 minutes ago; the update check failed.

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

Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Home / Operations - Update Device / Update Check Details

The update check failed

Something went wrong while checking for updates.

State	Started	Finished	Duration
Failed	2021-11-16 16:29:23 +0000 less than a minute ago	2021-11-16 16:29:30 +0000 less than a minute ago	less than a minute

Output

```
Attempting to mount an ISO, if one is present.
Starting update check.
http://127.0.0.1:8080/PrivateCloud/3.5.3/prod/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below wiki article

https://wiki.centos.org/yum-errors

If above article doesn't help to resolve this issue please use https://bugs.centos.org/.

One of the configured repositories failed (FireAMP PrivateCloud Repository),
and yum doesn't have enough cached data to continue. At this point the only
safe thing yum can do is fail. There are a few ways to work "fix" this:

1. Contact the upstream for the repository and get them to fix the problem
```

Download Output

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.



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Mount an Update ISO

ISO Configuration

HELP

Mount Type

- ISO
- ISO
- NFS4
- NFS3

Mount Status

No ISO mounted



Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

Mount an Update ISO

ISO Configuration

HELP

Mount Type

NFS3

Remote Share

192.168.75.4:/AMPAG

Remote ISO File

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

Mount

Mount Status

Mounted ISO

nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Unmount

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

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



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

⚙️ Protect DB importing

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

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

☰ Output

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

[Download Output](#)

✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

State	Started	Finished	Duration
✔ Successful	2021-11-19 17:04:05 +0000 about 1 month ago	2021-12-21 01:08:11 +0000 less than a minute ago	about 1 month

Output

```
Starting firehose_cassandra...
Starting firehose_cassandra_replay...
Starting firehose_publisher...
Starting firehose_publisher_replay...
Starting install-token-api...
Starting mgmt_unicorn...
Starting mongo_event_consumer...
Starting portal_unicorn...
Starting redis...
Starting retro-dipper...
Starting retrohose...
Starting retrohose-replay...
Starting tevent_listener...
Starting crond...
Starting flight...
Starting docker...
Sending notification (this may take some time).
```

Download Output

A próxima atualização começa automaticamente



⚙ Importing Protect DB deltas.

Your Protect DB is being updated with threat intelligence that was queued during a previous content update. Each delta can take several hours to import, and system performance might be impacted during this time.

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

Queued Updates

20211116-2135

Queued Protect DB Update Version



Protect DB

20210531-0613

0.80%

Update Progress

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.

✔ Content updated successfully

The device successfully performed a content update.

State	Started	Finished	Duration
✔ Successful	2021-12-21 03:10:11 +0000 28 minutes ago	2021-12-21 03:37:53 +0000 less than a minute ago	28 minutes

Output

```

Attempting to mount an ISO, if one is present.
PASS: The mount point / has sufficient space available: 23273033728 >= 1000000000
PASS: The mount point / has sufficient inodes available: 2018323 >= 100000
All checks succeeded!
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
--> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
--> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
--> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
--> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
    
```

Download Output

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

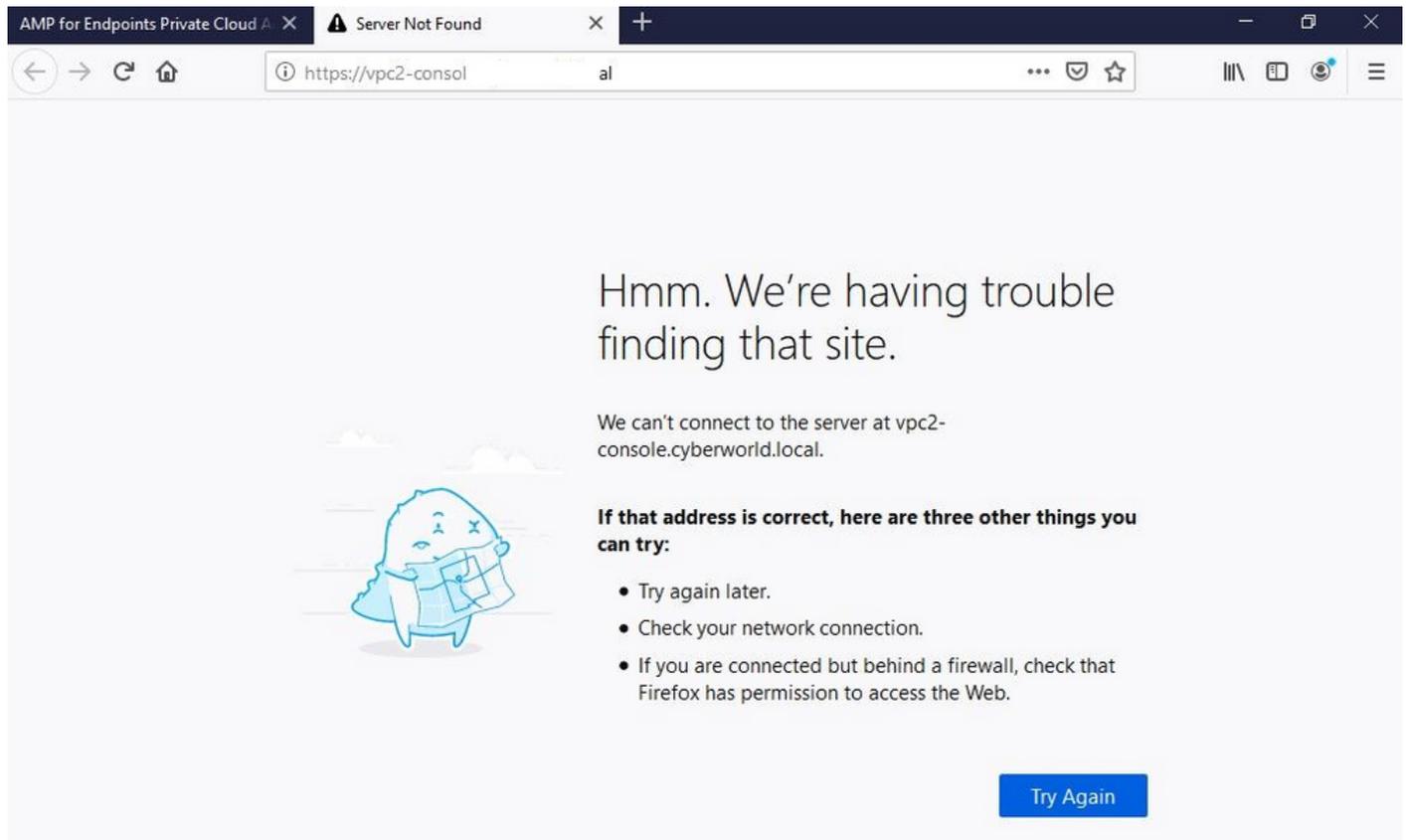
Para o dispositivo VPC, visite este TZ que contém outros métodos para atualizar o dispositivo de hardware, montar o arquivo ISO e inicializar a partir do USB.

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

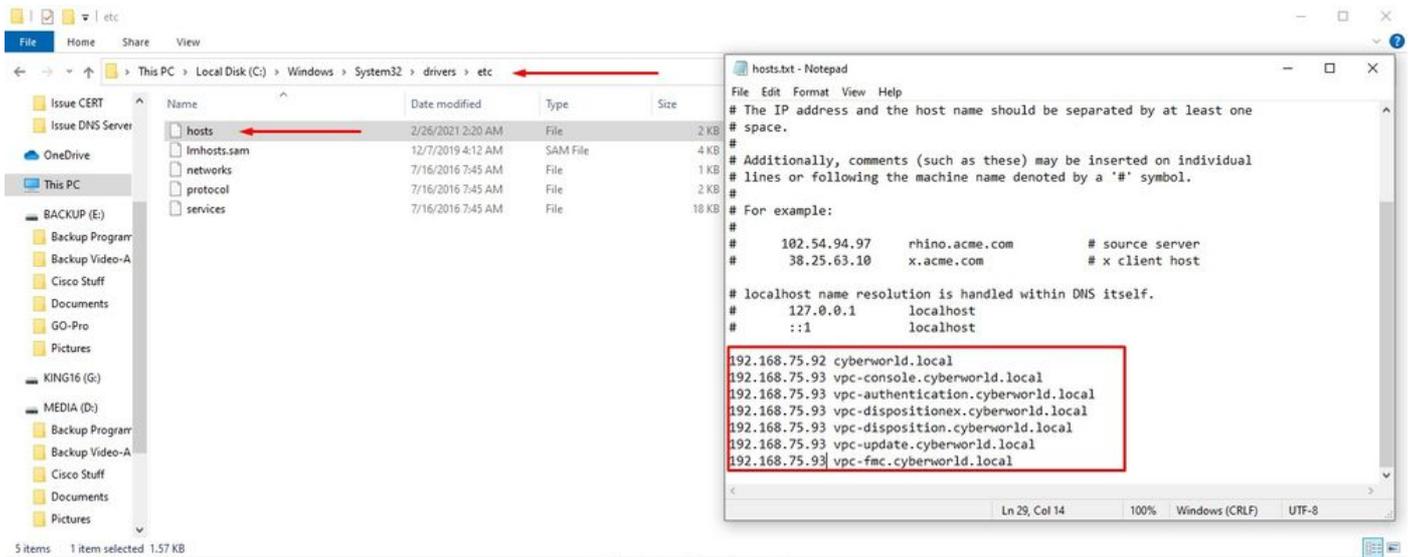
Troubleshooting Básico

Problema #1 - FQDN e Servidor DNS

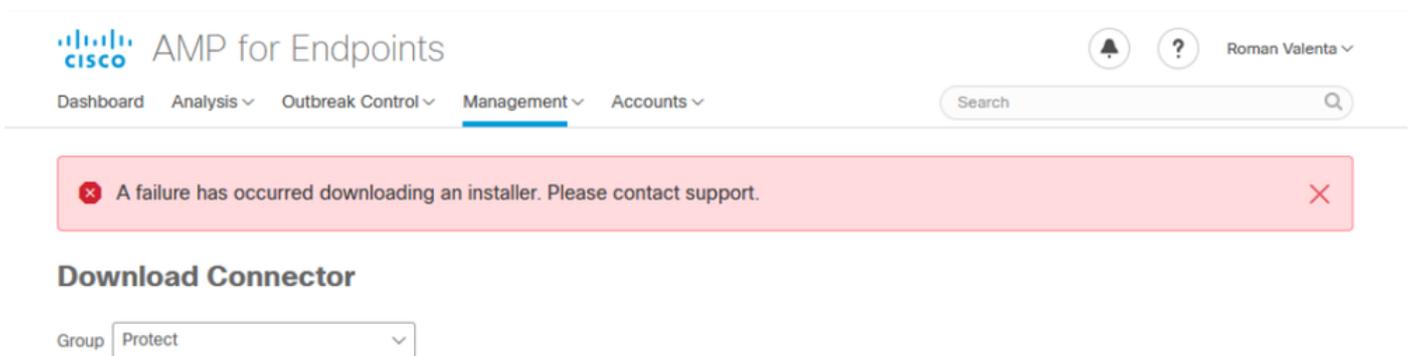
O primeiro problema que você pode encontrar é se o seu servidor DNS não está estabelecido e todos os FQDN não estão registrados e resolvidos corretamente. O problema pode parecer assim quando você tenta navegar para o console do Secure Endpoint por meio do ícone "fire" do Secure Endpoint. Se você usar 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.



Configuration network settings.

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

Admin	eth0 / 00:0C:29:A6:4A:11
	IP Assignment 192.168.75.92 More details
Interface	eth1 / 00:0C:29:A6:4A:1B
	IP Assignment 192.168.75.93 More details
	IP Assignment <input type="text" value="Static"/>
	IP Address <input type="text" value="192.168.75.93"/>
	<input checked="" type="checkbox"/> Check for IP Address conflicts
	Subnet Mask <input type="text" value="255.255.255.0"/>
	Gateway <input type="text" value="192.168.75.1"/>

Warning: Address and Hostname Changes

If you change the IP address of the interface you must also update the DNS records for each of your configured hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.

[View the Configuration help page for a list of affected services.](#)

DNS
Primary DNS Server <input type="text" value="192.168.75.4"/>



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.



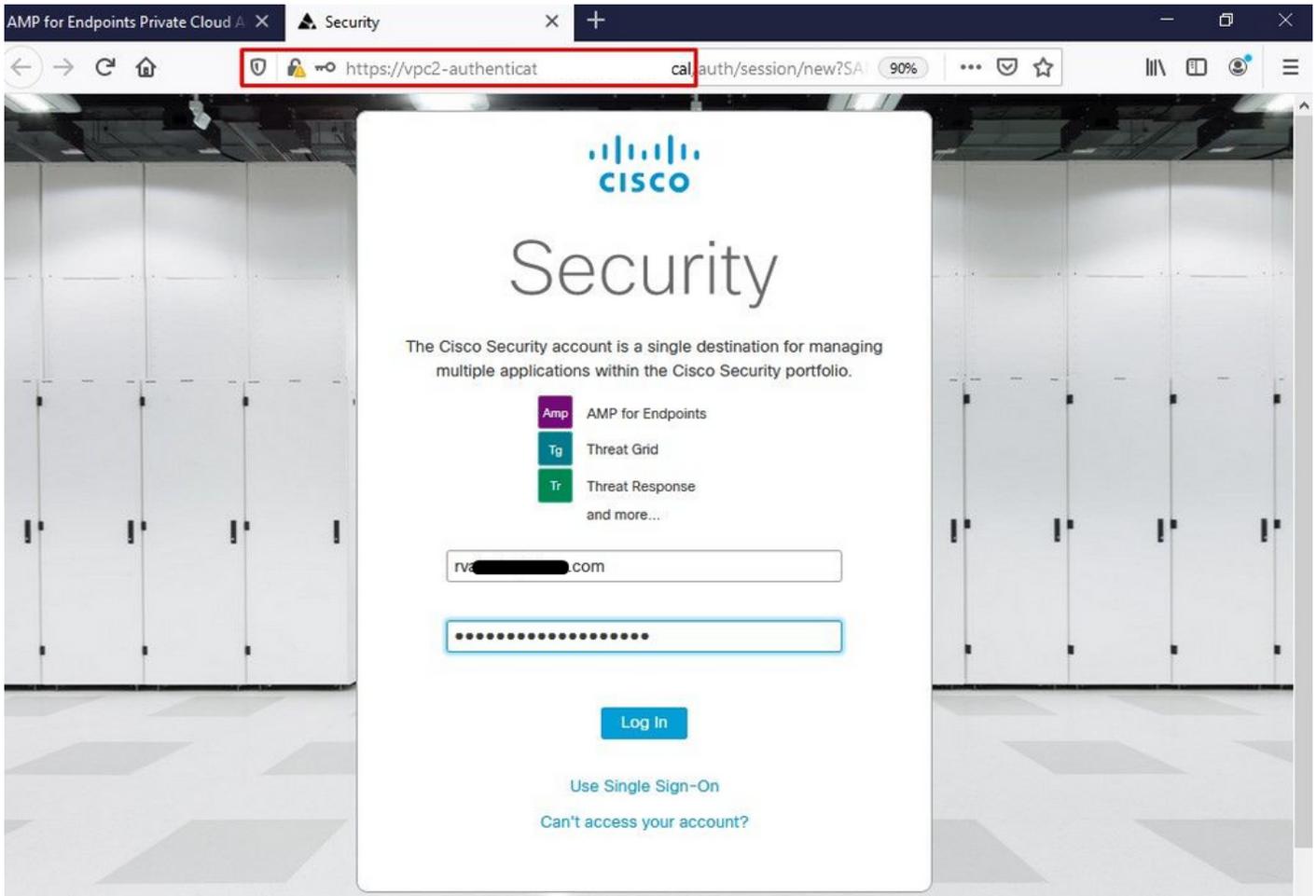
State	Started	Finished	Duration
	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

Output

```
[2021-04-12T00:20:43+00:00] DEBUG: Found current_uid == nil, so we are creating a new file, updating owner
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] owner changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_gid == nil, so we are creating a new file, updating group
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] group changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_mode == nil, so we are creating a new file, updating mode
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] mode changed to 600
[2021-04-12T00:20:43+00:00] DEBUG: Restoring selinux security content with /sbin/restorecon -R "/tmp/cqlsh_check_superuser_password.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/run/cookbooks/cassandra/providers/cqlsh.rb line 16)
[2021-04-12T00:20:43+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:43+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provider::Execute
[2021-04-12T00:20:43+00:00] INFO: Retrying execution of execute[cqlsh_check_superuser_password], 19 attempt(s) left
[2021-04-12T00:20:45+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:45+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provider::Execute
```

Download Output

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.

AMP for Endpoints Private Cloud X Dashboard X +

https://vpc2-consol dashboard/fresh

AMP for Endpoints Roman Valenta

Dashboard Analysis Outbreak Control Management Accounts

Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

Getting Started

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

Deploy AMP for Endpoints Connectors

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

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by populating your Console with replayed data from actual malware infections. Enabling Demo Data will add computers and events to your Cisco AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, and Detections and Events displays behave when malware is detected. Demo Data can coexist with live data from your Cisco AMP for Endpoints deployment, however, because of the severity of some of the Demo Data

Demo Computers

WannaCry [Click here to view PDF](#)
The WannaCry attack involves a remote compromise through the Windows SMB (Server Message Block) service using the ETERNALBLUE exploit. Upon system compromise, the attacker drops the WannaCry ransomware variant that is initially identified by AMP for Endpoints using ransomware indicators of compromise, and later by AMP Cloud signatures.

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

ZAccess [Click here to view PDF](#)
Use Device Trajectory to watch a rootkit exploit privilege escalation on a computer, and use File Trajectory to discover which other endpoints have been compromised.

ZBot [Click here to view PDF](#)
See how a vulnerable version of Internet Explorer can expose you to malware. Use Device Trajectory to learn what happened and use application blocking lists to stop the future execution of vulnerable programs.

CozyDuke [Click here to view PDF](#)
Trace a detection back to an abused DLL search path, block any communications to its upstream CnC, and deploy an Endpoint IOC to contain further attacks.

Baixar conector.

🟢 Step 1: Existing Security Products

🟢 Step 2: Set Up Proxy

🟢 Step 3: Download Connector

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

[Back](#)

[Next](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

amp_Protect.exe

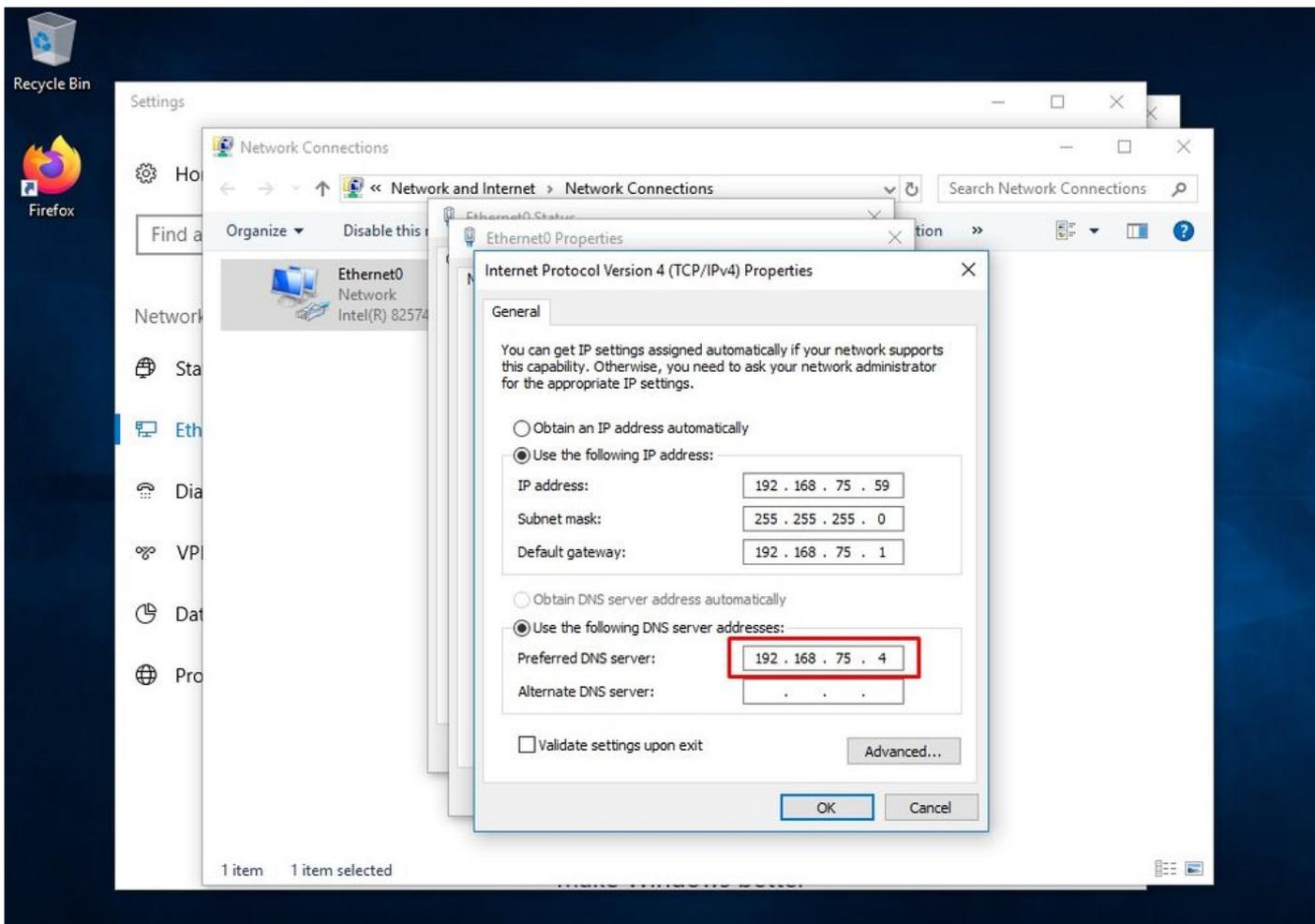
which is: **exe File**

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

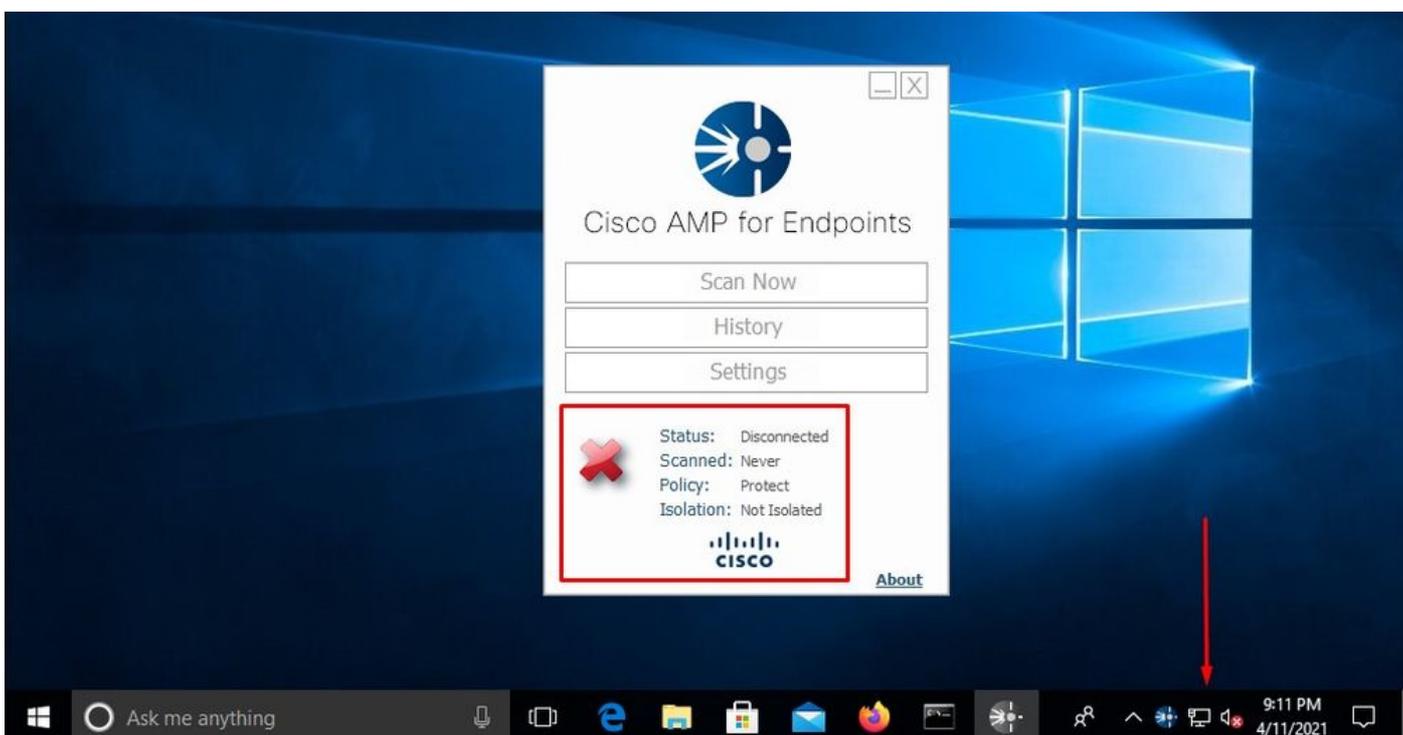
Would you like to save this file?

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.



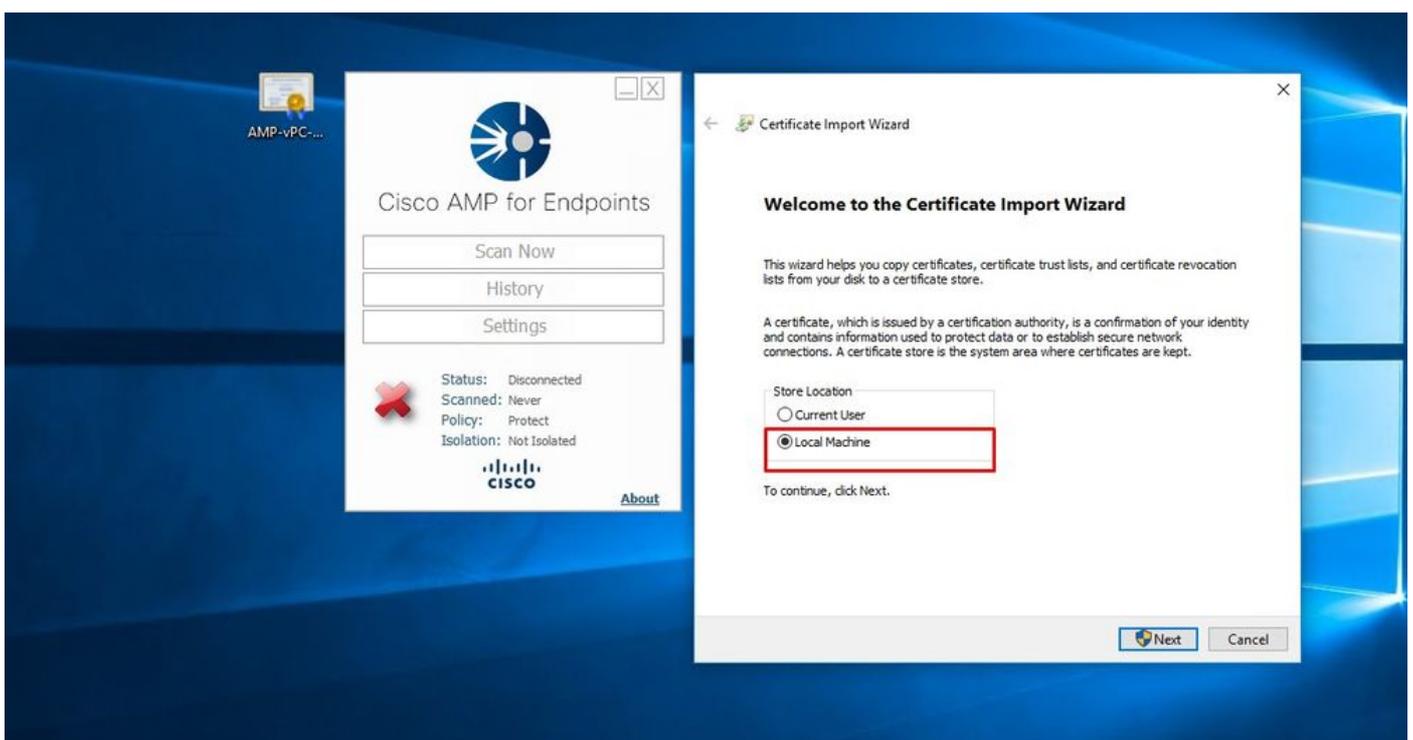
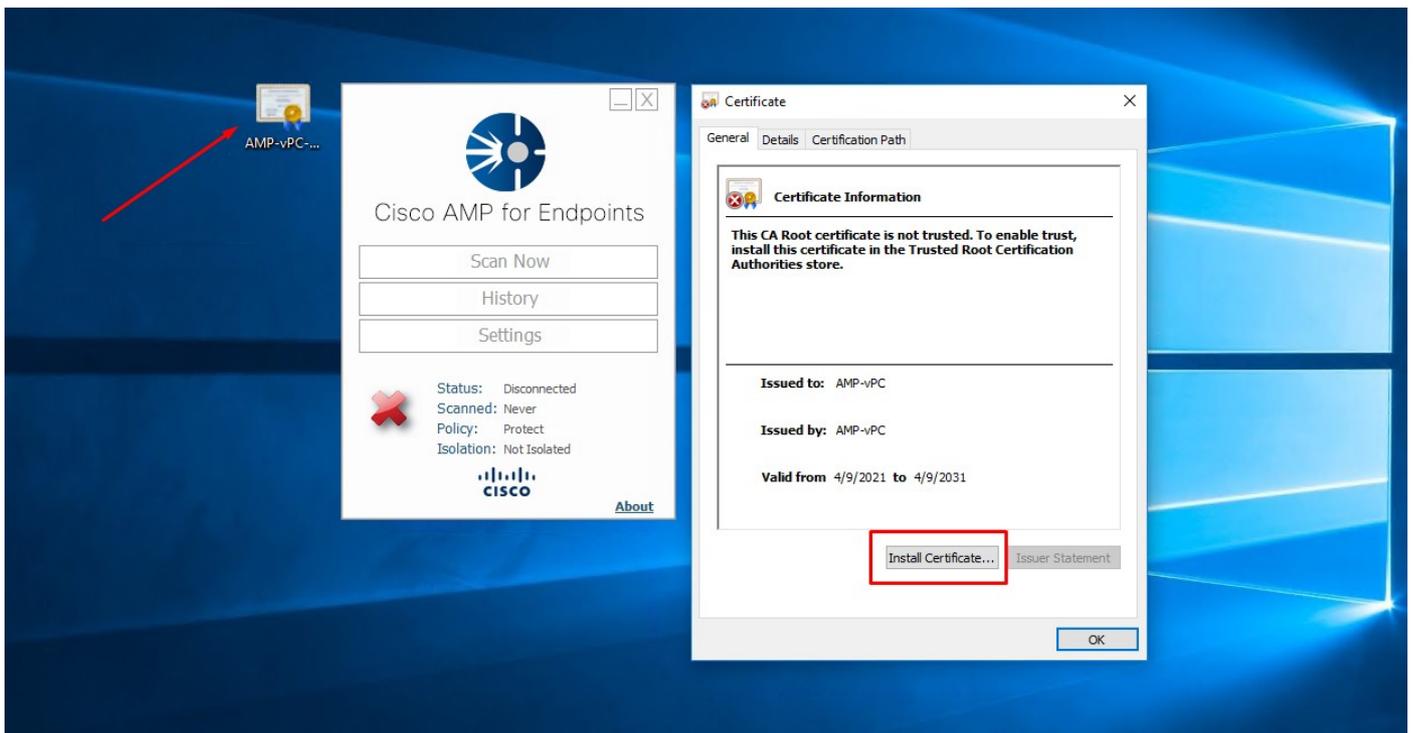
Depois de instalar o conector, o Secure Endpoint pode ser visto como Desconectado. Execute o pacote de diagnóstico e examine os logs; você poderá determinar o problema.

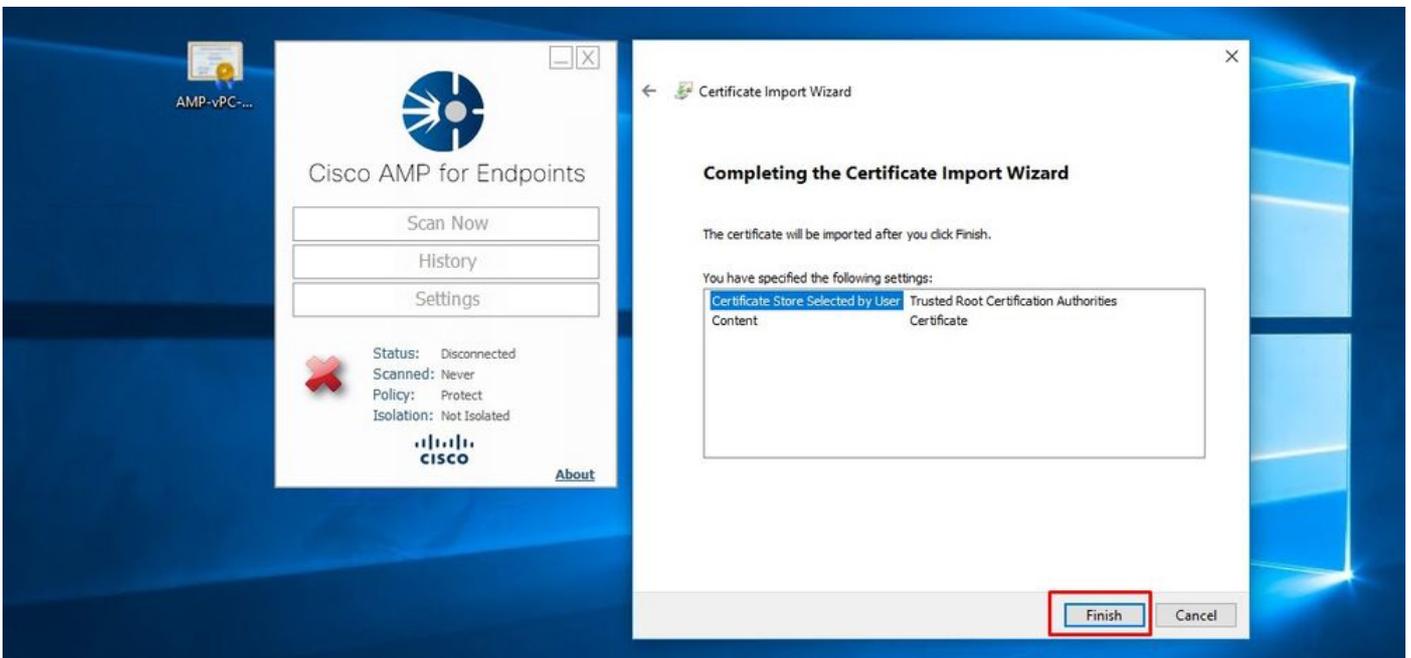
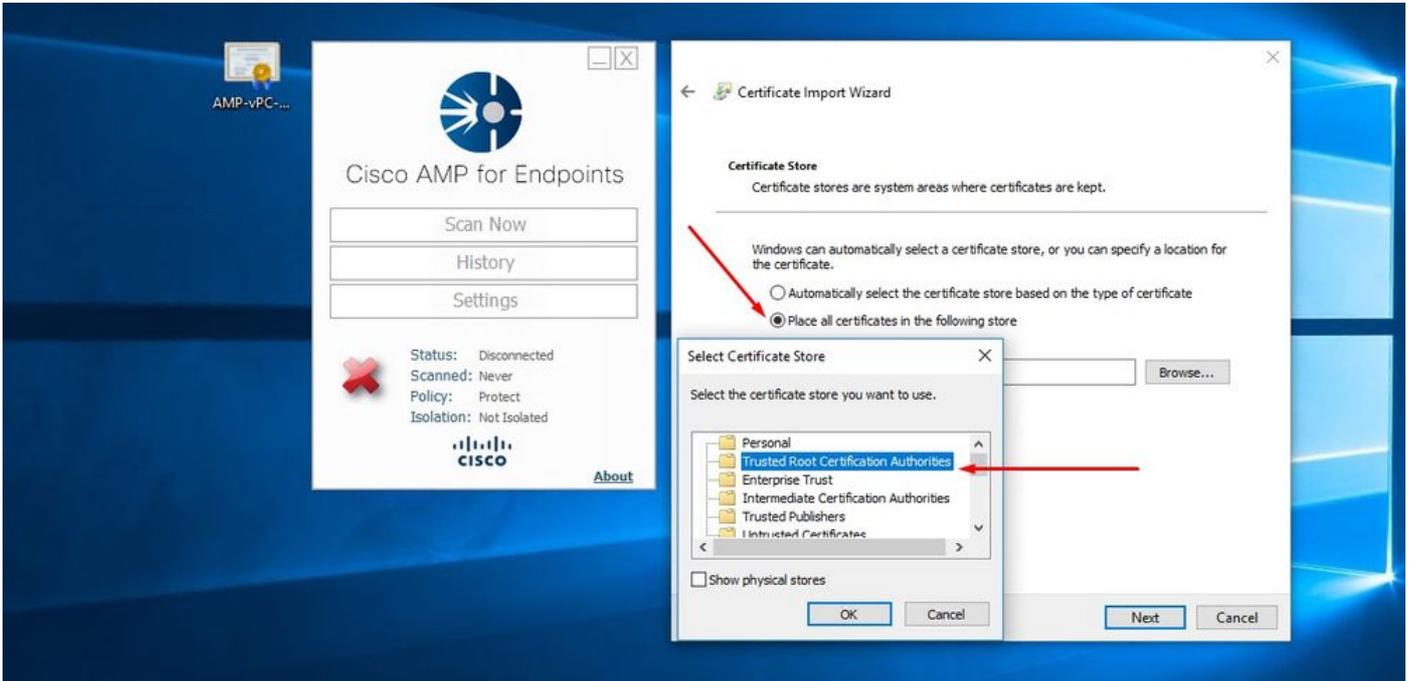


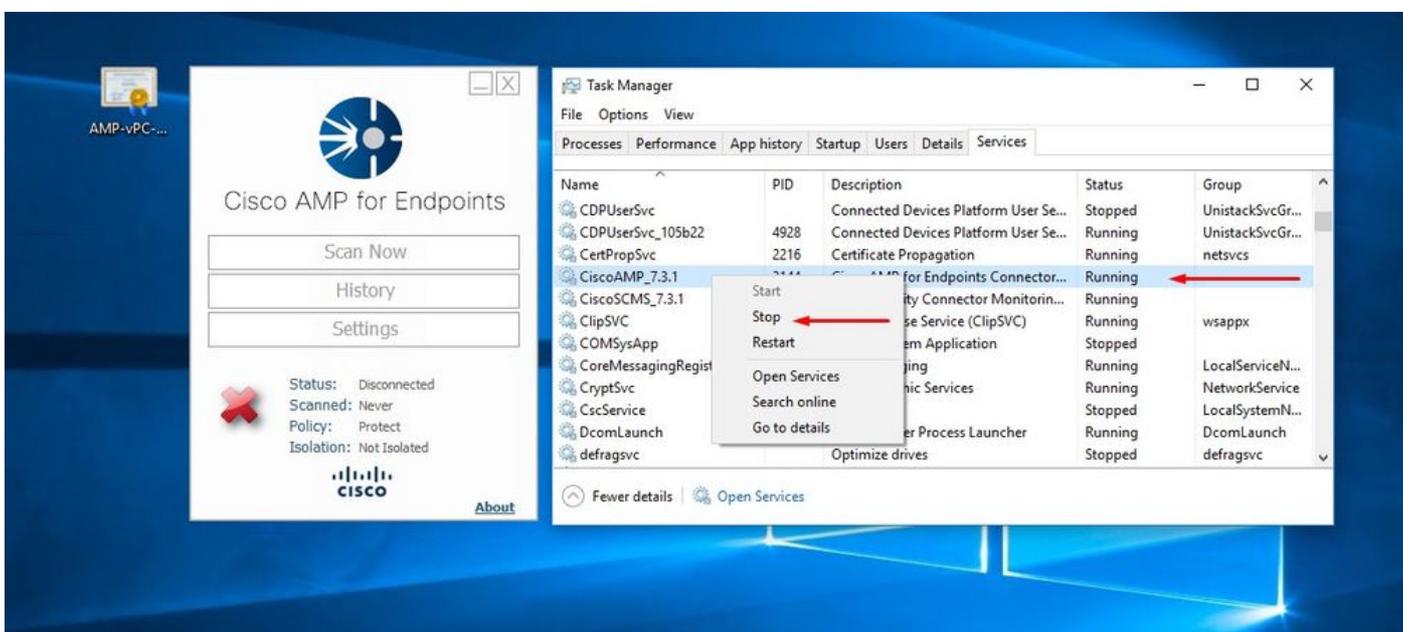
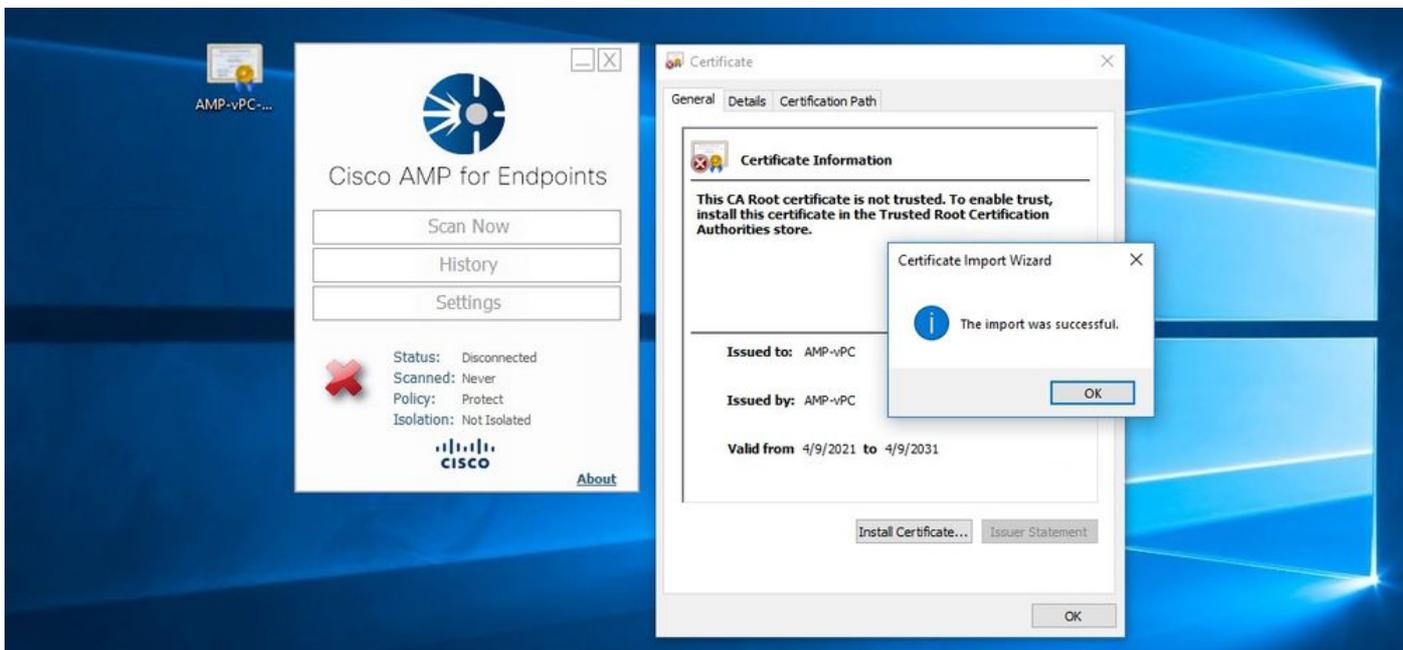
Com base nessa saída coletada do pacote de diagnóstico, você pode ver o erro de CA raiz

(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

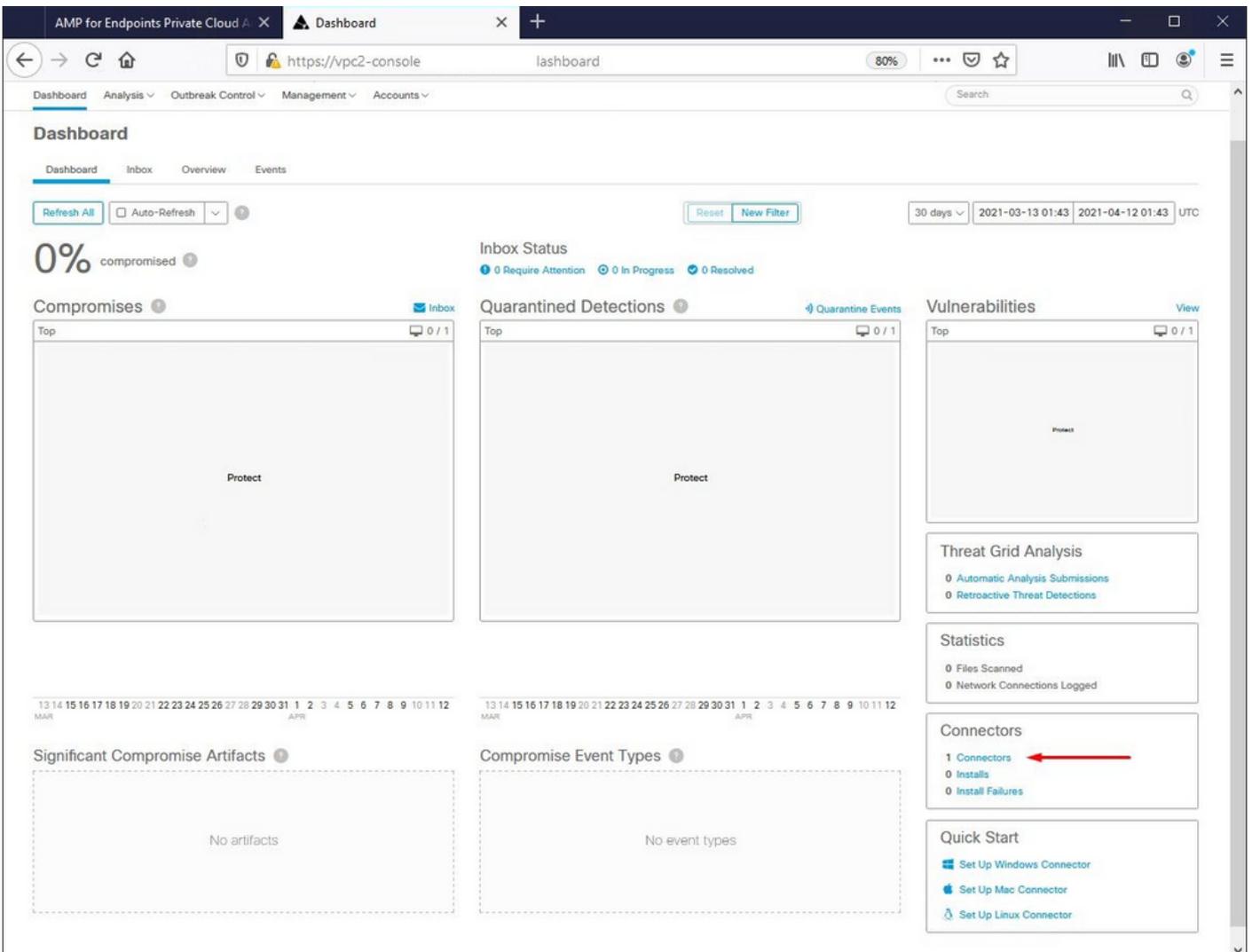
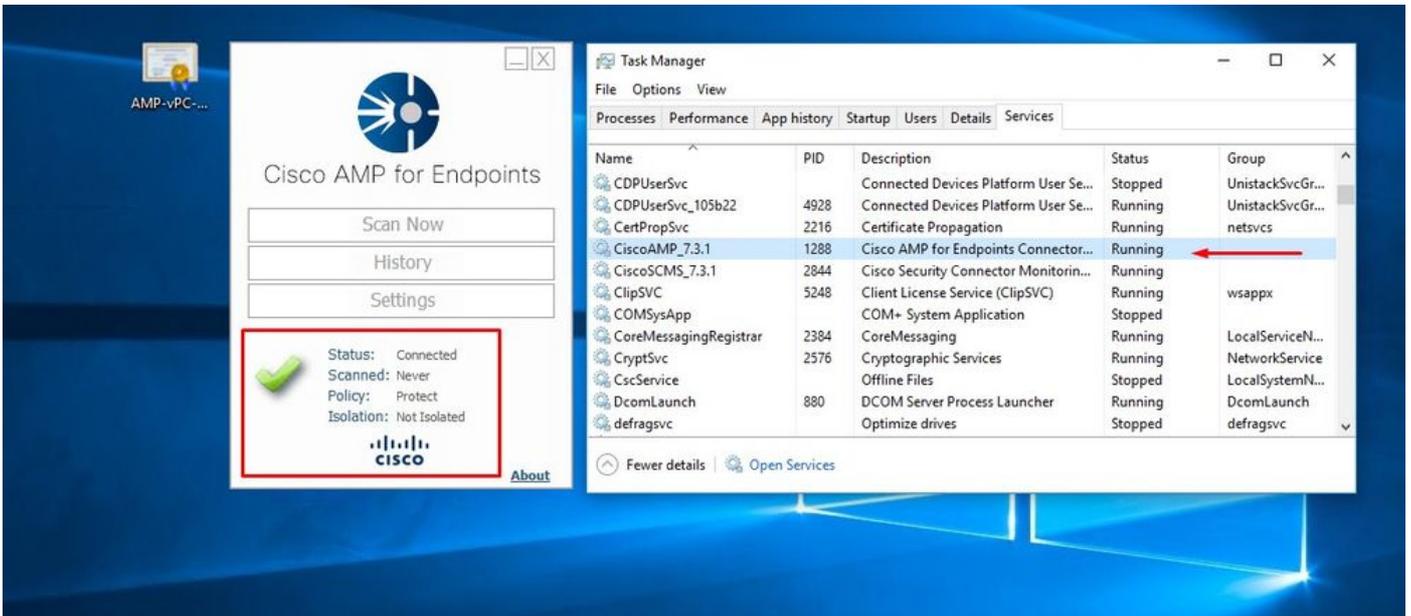
Depois de carregar a CA raiz no repositório de CA raiz confiável e reiniciar o serviço de Ponto de Extremidade Seguro. Tudo começa a funcionar como esperado.







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



Atividade mal-intencionada testada

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

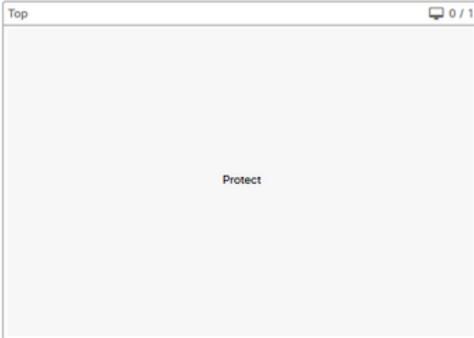
0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

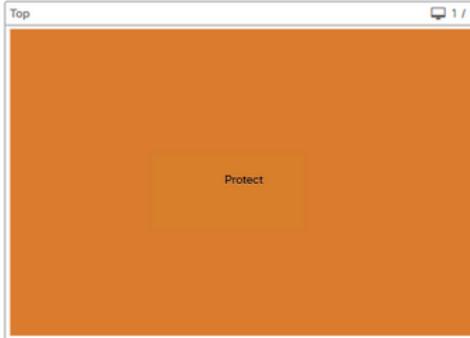
Compromises

Inbox 0 / 1



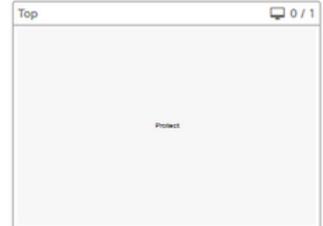
Quarantined Detections

Quarantine Events 1 / 1



Vulnerabilities

View 0 / 1



Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
0 Installs
0 Install Failures

Quick Start

Set Up Windows Connector

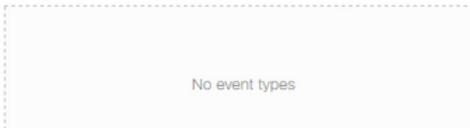
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

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

Significant Compromise Artifacts



Compromise Event Types



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.