Instalación y configuración de la nube privada virtual de terminal seguro

Contenido

- Introducción
- Prerequisites
- Implementación de VPC
  - Instalación de VM
  - Configuración inicial de la interfaz de administración
  - Configuración inicial de vPC mediante GUI web
  - Configuración
  - Services
  - Paquete de actualización de AirGap
    - Problema #1: espacio agotado en el almacén de datos
    - Problema #2: actualización anterior
- Resolución de problemas básicos
  - Problema #1: FQDN y servidor DNS
  - Problema #2 - Problema con la CA raíz

Introducción

Este documento describe y se centra en cómo implementar correctamente la nube privada virtual (VPC) en servidores en el entorno ESXi. Para obtener otros documentos como la guía de inicio rápido, la estrategia de implementación, la guía de derechos, la guía del usuario de la consola y del administrador, visite este sitio Documentación

Colaboración de Roman Valenta, ingenieros del TAC de Cisco.

Prerequisites

Requerimientos:

VMware ESXi 5 o posterior

- Modo proxy de nube (solo): 128 GB de RAM, 8 núcleos de CPU (se recomiendan 2 CPU con 4 núcleos cada una), 1 TB de espacio libre mínimo en el almacenamiento de datos VMware
- Tipo de unidades: Se requiere SSD para el modo Air Gap y se recomienda para proxy
- Tipo de RAID: Un grupo RAID 10 (réplica seccionada)
- Tamaño mínimo del almacén de datos de VMware: 2 TB
- Lecturas aleatorias mínimas del almacén de datos para el grupo RAID 10 (4K): 60 000 IOPS
- Escrituras aleatorias mínimas de almacén de datos para el grupo RAID 10 (4K): 30 000

IOPS

Cisco le recomienda que tenga conocimiento acerca de este tema:

- Conocimientos básicos sobre cómo trabajar con certificados.
- Conocimientos básicos sobre cómo configurar DNS en un servidor DNS (Windows o Linux)
- Instalación de una plantilla de dispositivo virtual abierto (OVA) en VMWare ESXi

Utilizado en este LABORATORIO:

VMware ESX 6.5

- Modo proxy de nube (solo): 48 GB de RAM, 8 núcleos de CPU (se recomiendan 2 CPU con 4 núcleos cada una), 1 TB de espacio libre mínimo en el almacenamiento de datos VMware
- Tipo de unidades: SATA
- Tipo de RAID: Un RAID 1
- Tamaño mínimo del almacén de datos de VMware: 1 TB
- MobaXterm 20.2 (programa multiterminal similar a PuTTY)
- Cygwin64 (se utiliza para descargar la actualización de AirGap)

Adicionalmente

- Certificado que se crea con openSSL o con cualquier otro método compatible.
- Servidor DNS (Linux o Windows) En mi laboratorio usé Windows Server 2016 y CentOS-8
- Windows VM para el terminal de prueba
- Licencia

Si su memoria está por debajo de 48GB de RAM en la versión 3.2+ VPC se vuelven inutilizables.

Nota: El OVA de la nube privada crea las particiones de unidad, por lo que no es necesario especificarlas en VMWare. servidor que resuelve el nombre de host de interfaz limpia.

Consulte la hoja de datos del dispositivo VPC para obtener más información sobre los requisitos de hardware específicos de la versión.

Nota: La información de este documento se creó a partir de los dispositivos de un entorno de laboratorio específico y su única intención es ofrecerle una guía a través de la implementación que puede variar en función de la versión que se esté implementando. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

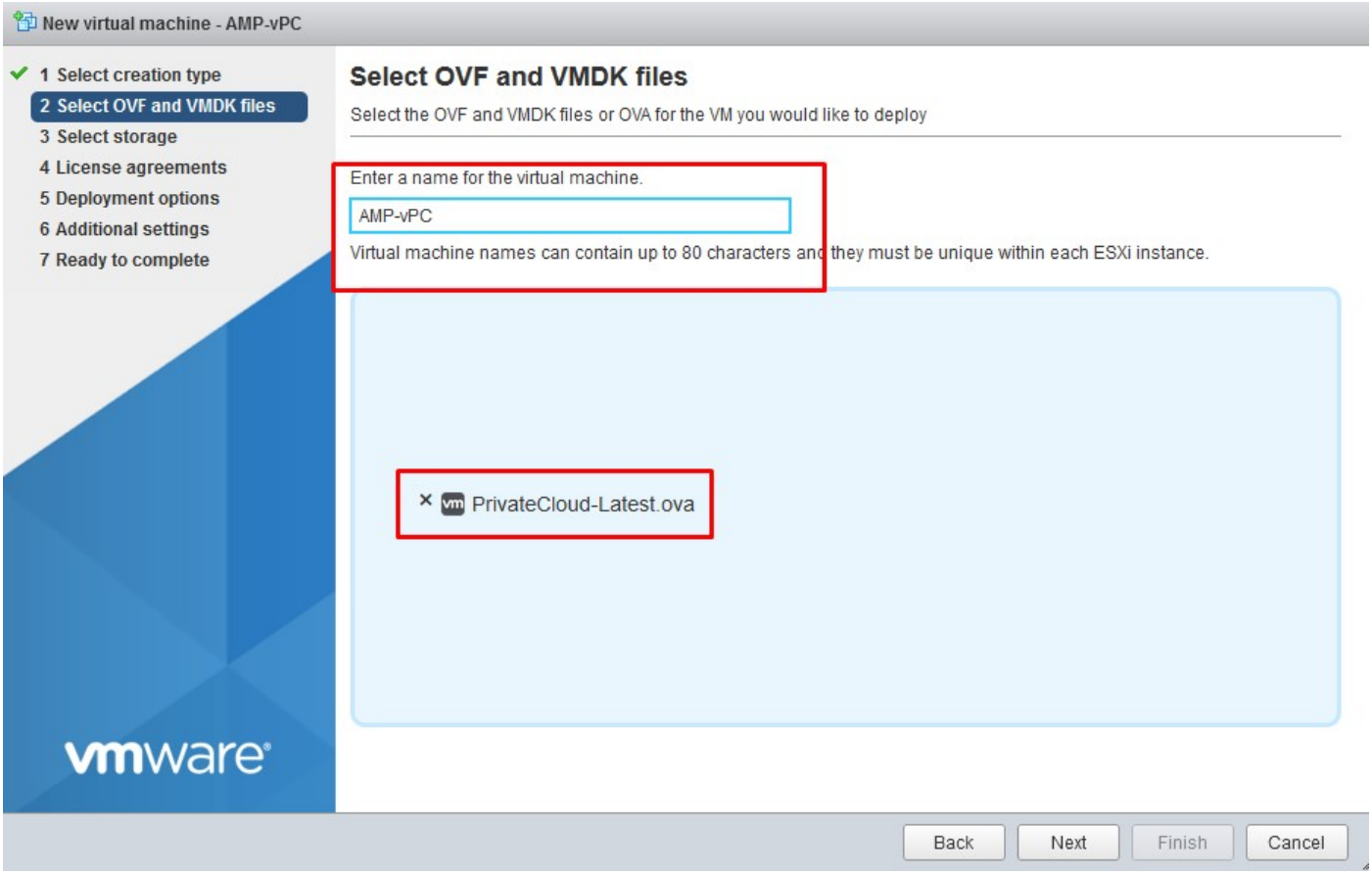
Implementación de VPC

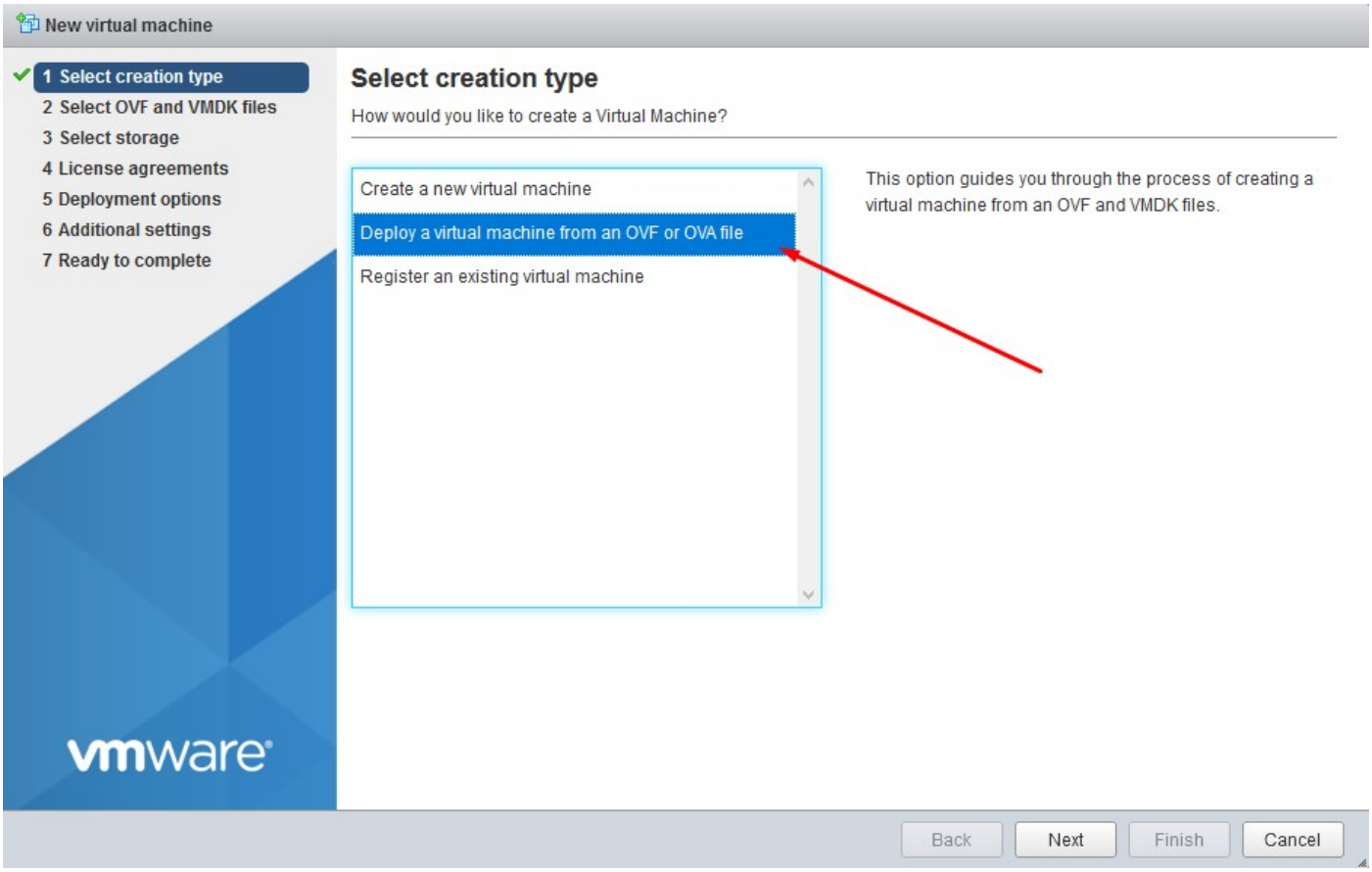
Seleccione la URL proporcionada en el correo electrónico de entrega electrónica o de autorización. Descargue el archivo OVA y continúe con la instalación

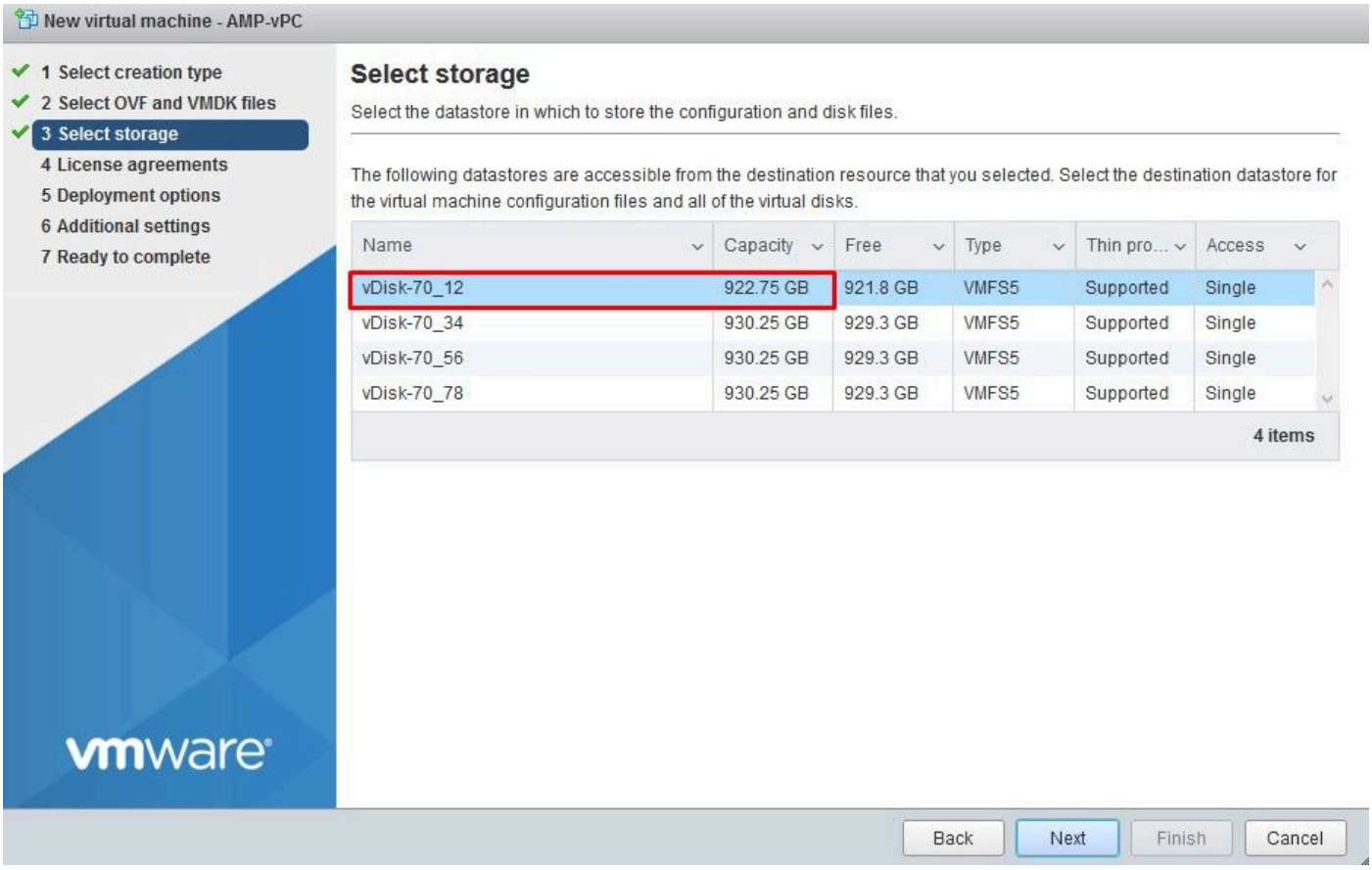
Instalación de VM

Paso 1:

Vaya a File > Deploy OVF Template para abrir el asistente Deploy OVF Template, como se muestra en la imagen.

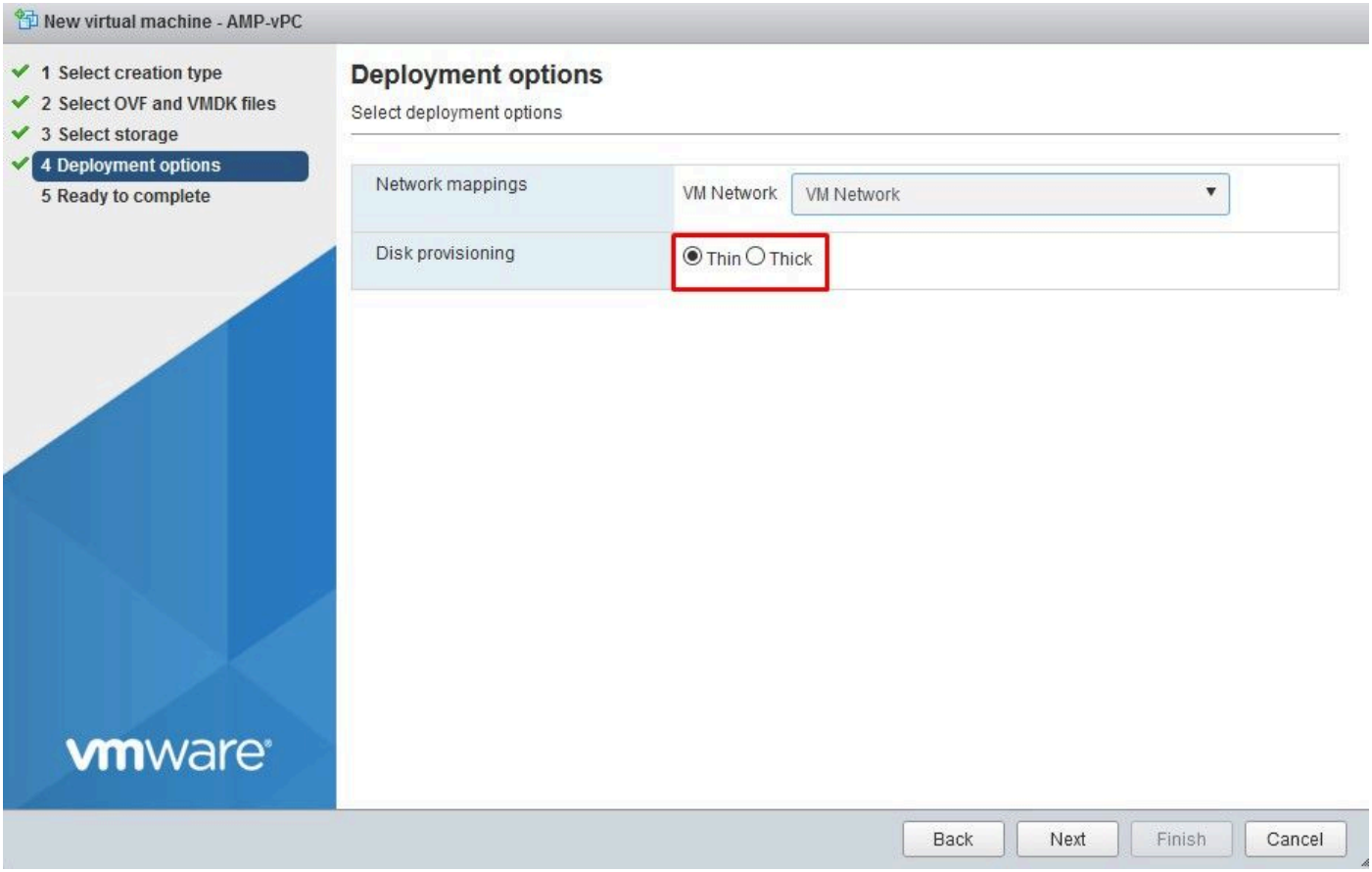






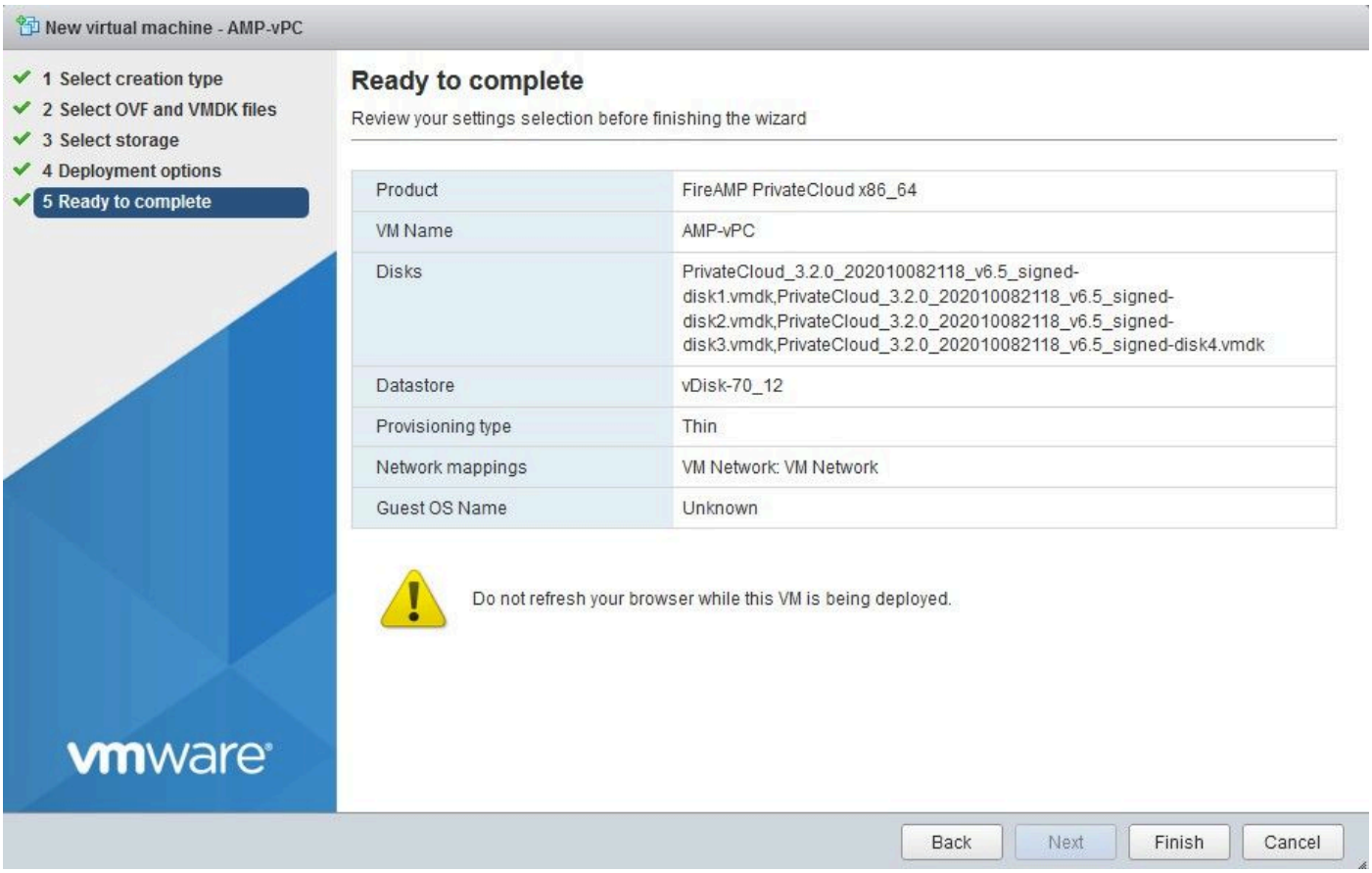
Nota: Aprovisionamiento grueso reserva espacio cuando se crea un disco. Si selecciona esta opción, puede mejorar el rendimiento con respecto a Thin Provisioning. Sin embargo,

esto no es obligatorio. Ahora seleccione en Next, como se muestra en la imagen.

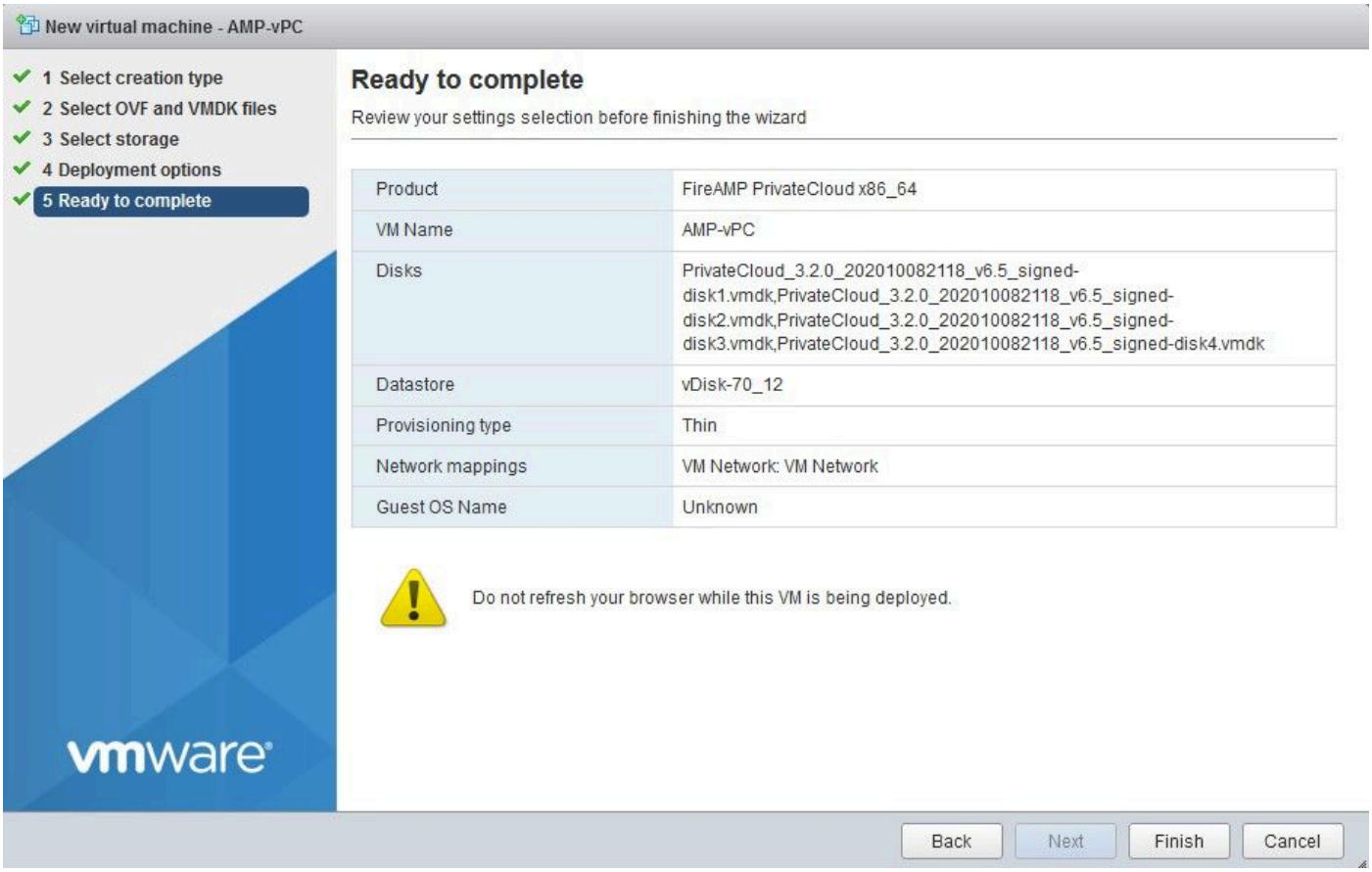


Paso 2:

Seleccione Browse... para seleccionar un archivo OVA y, a continuación, seleccione en Next. Observe los parámetros OVA predeterminados en la página OVF Template Details, como se muestra en la imagen. seleccione en Siguiente.



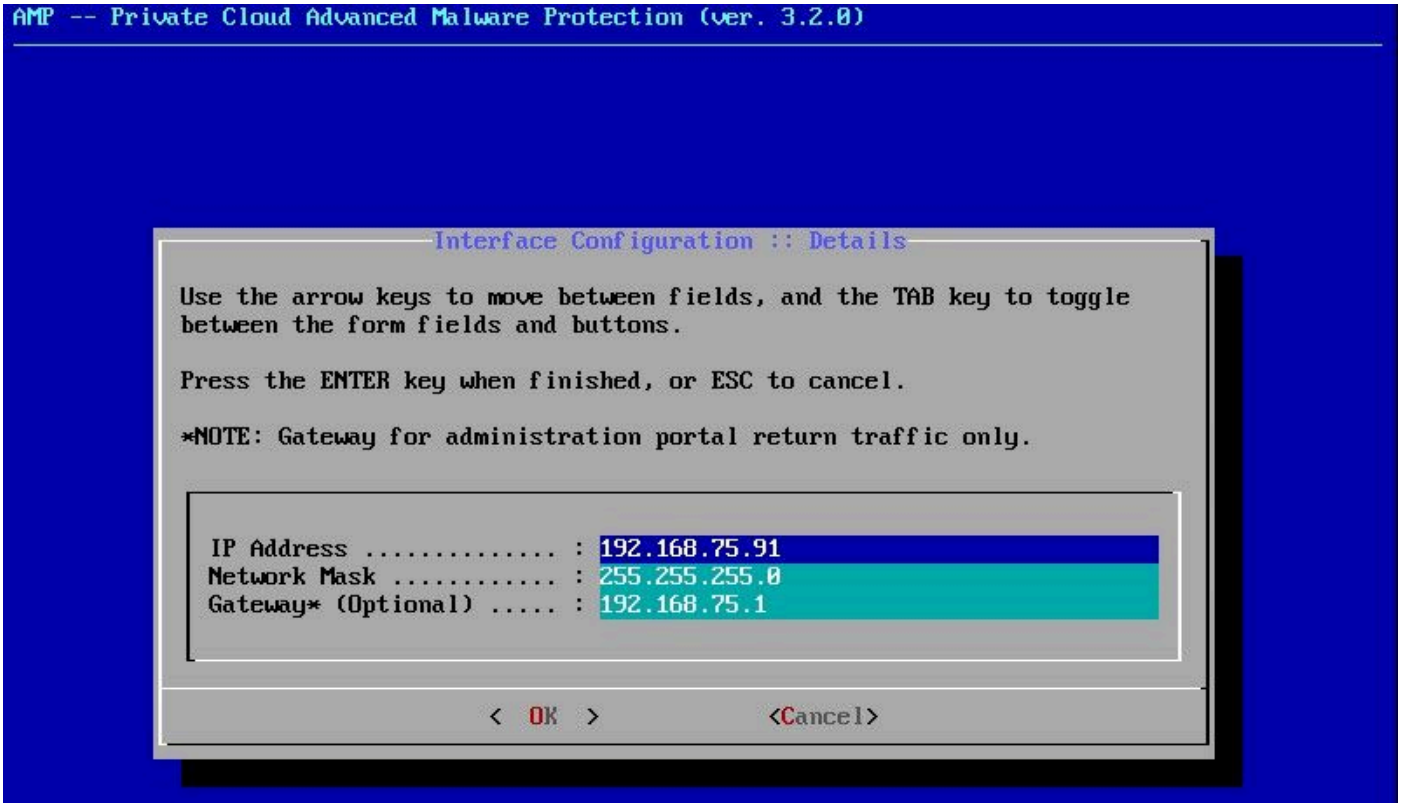
Configuración inicial de la interfaz de administración



Una vez que se inicia la VM, se realiza la configuración inicial a través de la consola de VM.

Paso 1:

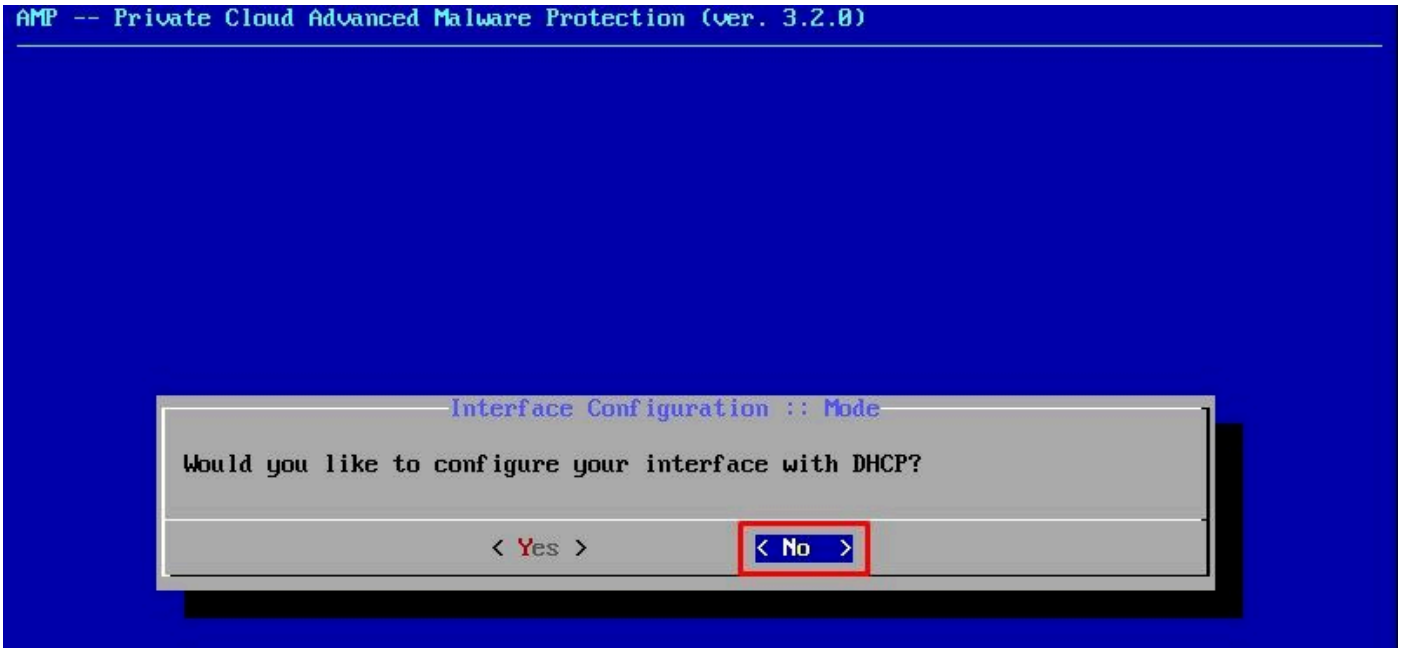
Es posible que observe que la dirección URL muestra [UNCONFIGURED] si la interfaz no recibió una dirección IP del servidor DHCP. Tenga en cuenta que esta interfaz es la interfaz de administración. Esta no es la interfaz de Producción.

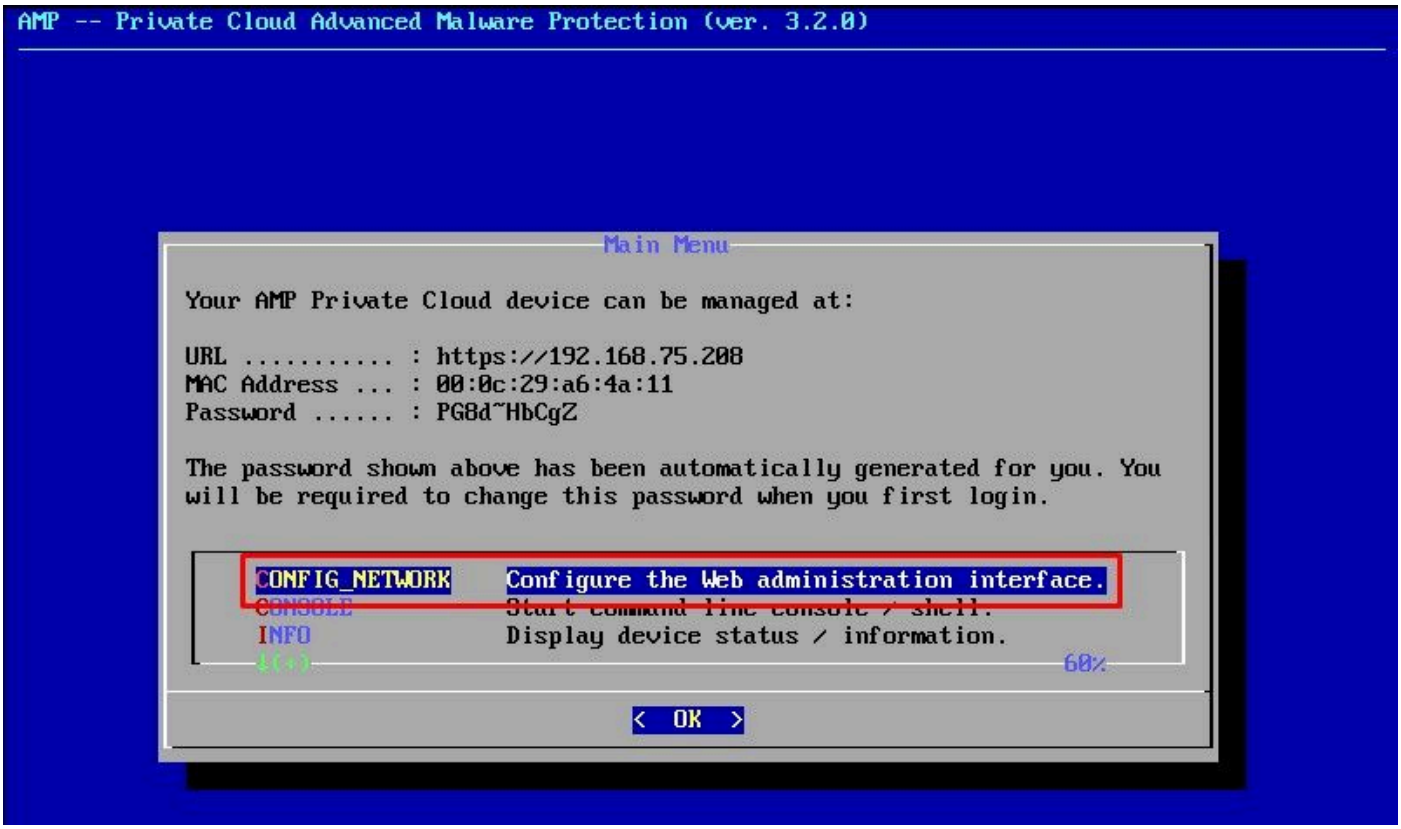


Paso 2:

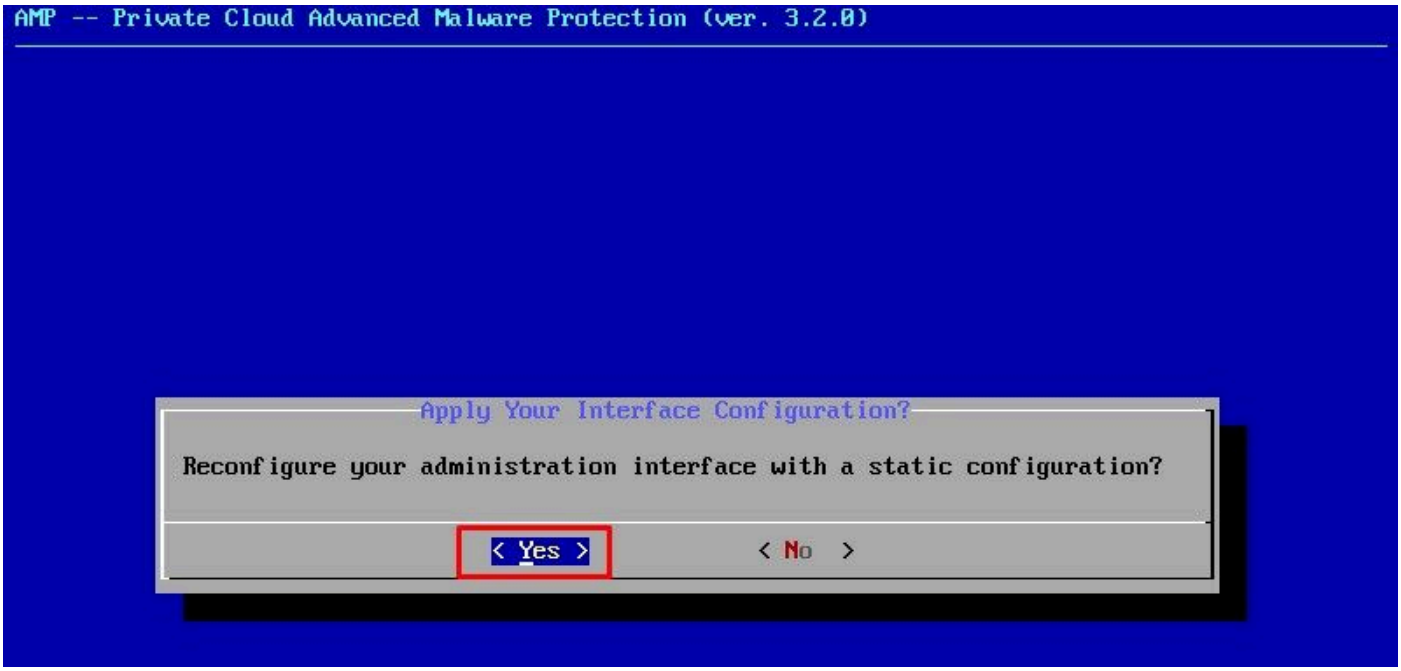
Puede desplazarse por las teclas Tab, Enter y Arrow.

Navegue hasta CONFIG_NETWORK y seleccione la tecla Enter en su teclado para comenzar la configuración de la dirección IP de administración para el Secure Endpoint Private Cloud. Si no desea utilizar DHCP, seleccione No y Enter key.

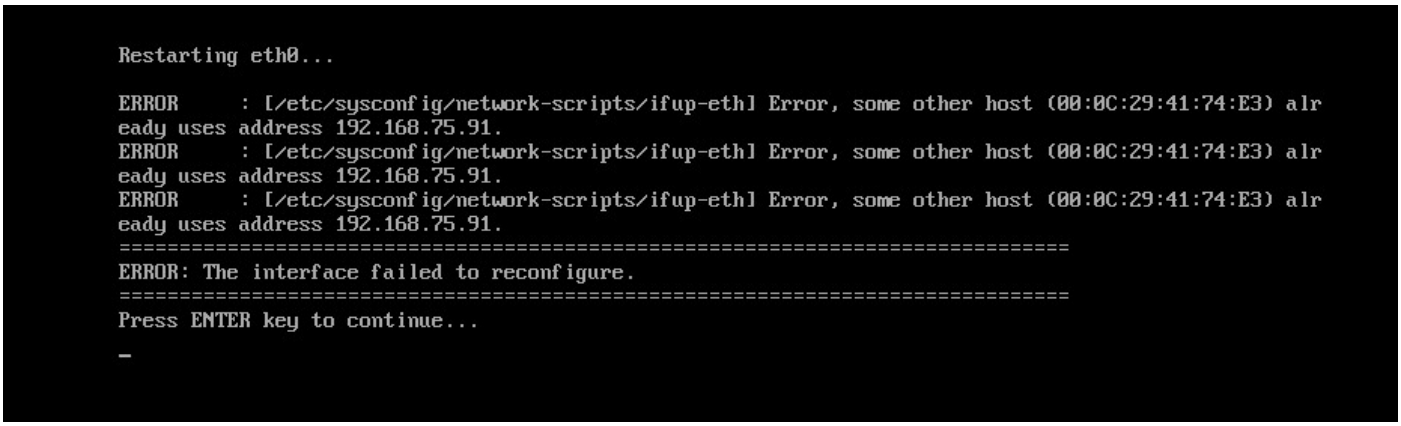


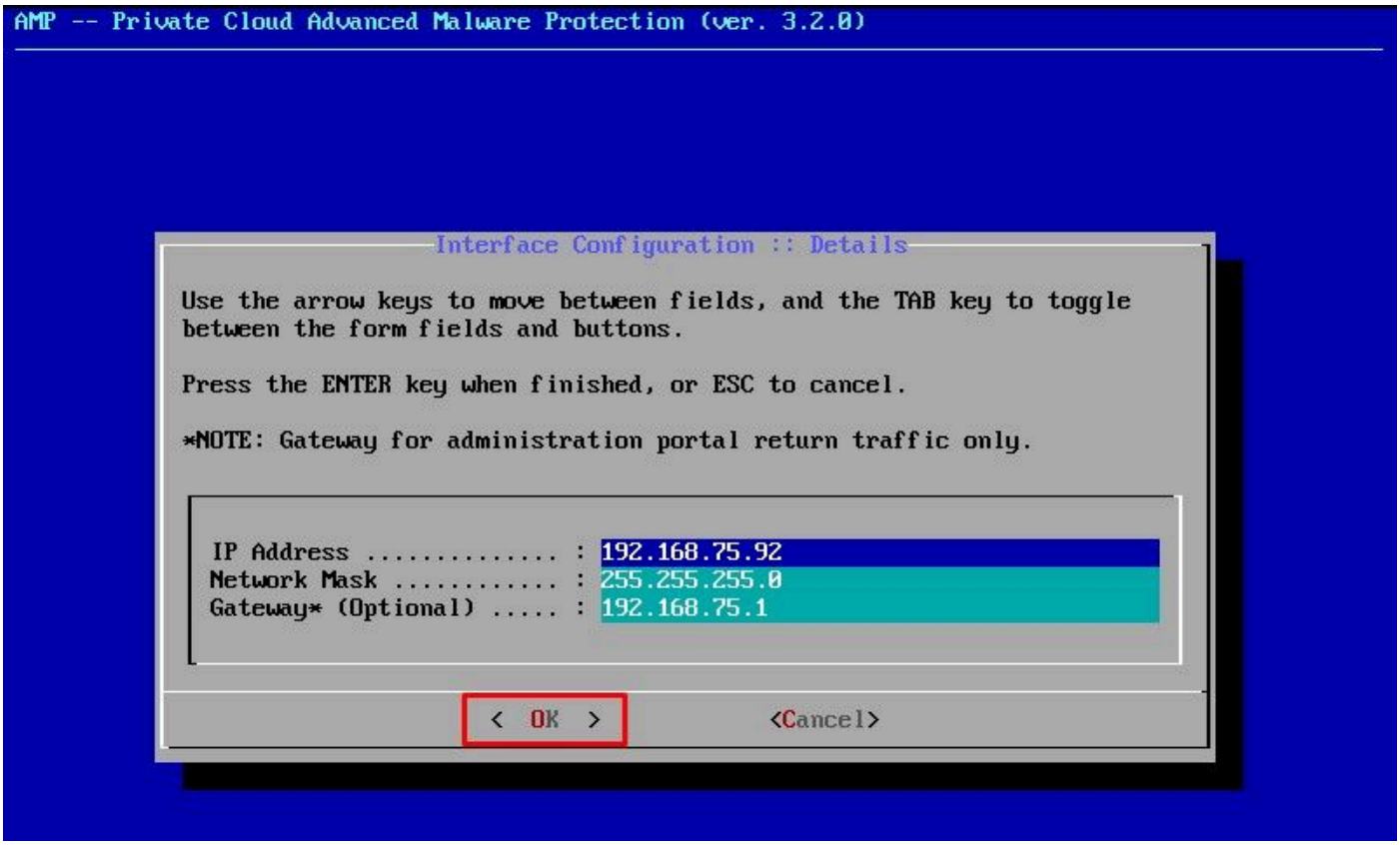


En la ventana que aparece, elija Yes y seleccione Enter key.



Si la IP ya está en uso, se le tratará con este registro de errores. Solo tiene que volver y elegir algo que sea único y no esté en uso.





Si todo va bien, verá un resultado similar a este

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

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

```
Restarting eth0...

Reconfiguring...

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

Paso 3:

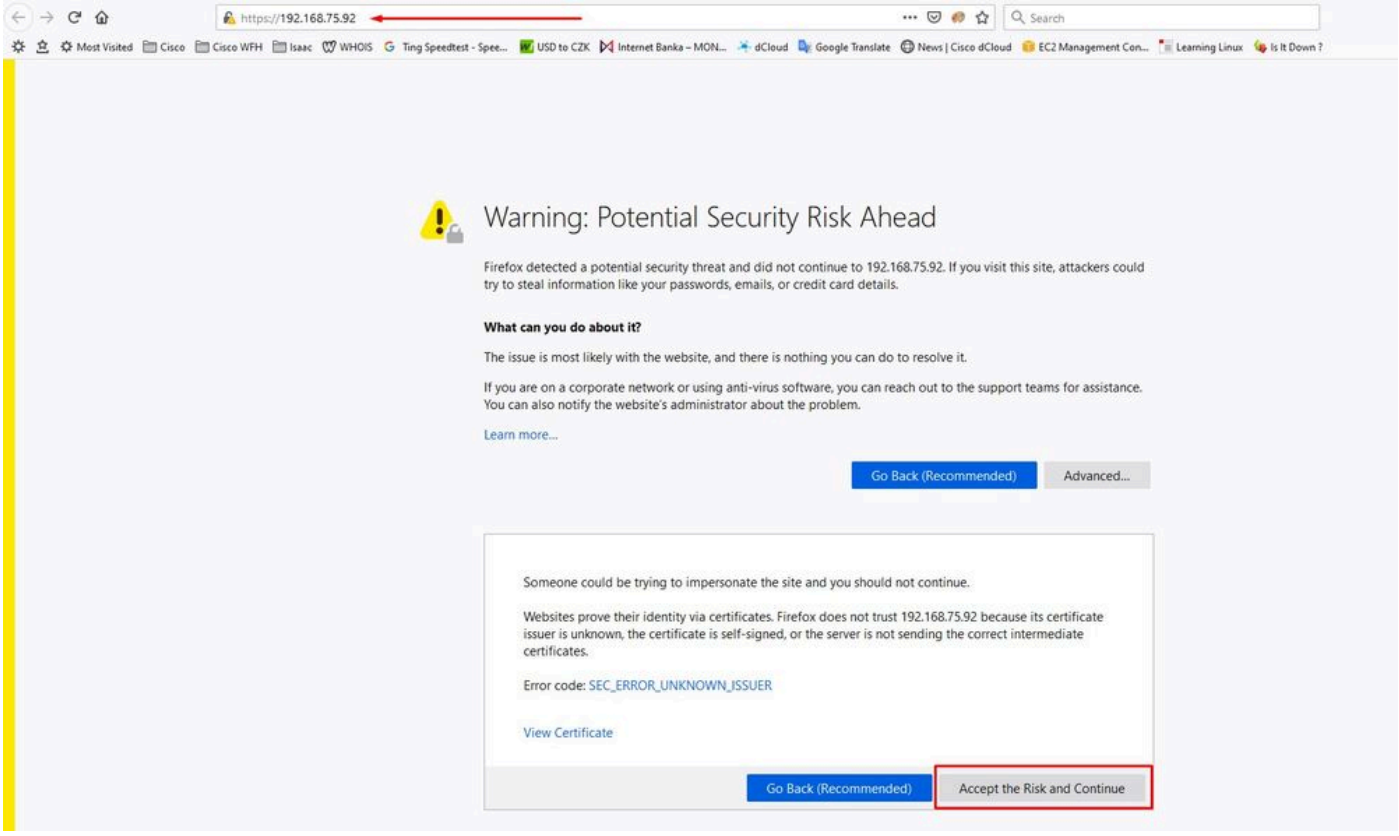
Espere hasta que aparezca de nuevo la pantalla azul con la nueva IP ESTÁTICA. Además, tenga en cuenta la contraseña para una sola vez. Tome nota y vamos a abrir nuestro navegador.

Configuración inicial de vPC mediante GUI web

Paso 1:

Abra un navegador web y navegue hasta la dirección IP de administración del dispositivo. Puede recibir un error de certificado cuando la nube privada de terminal seguro genere inicialmente su propio certificado HTTPS, como se muestra en la imagen. Configure el navegador para que confíe en el certificado HTTPS autofirmado de Secure Endpoint Private Cloud.

En el explorador, escriba la IP ESTÁTICA que configuró anteriormente.

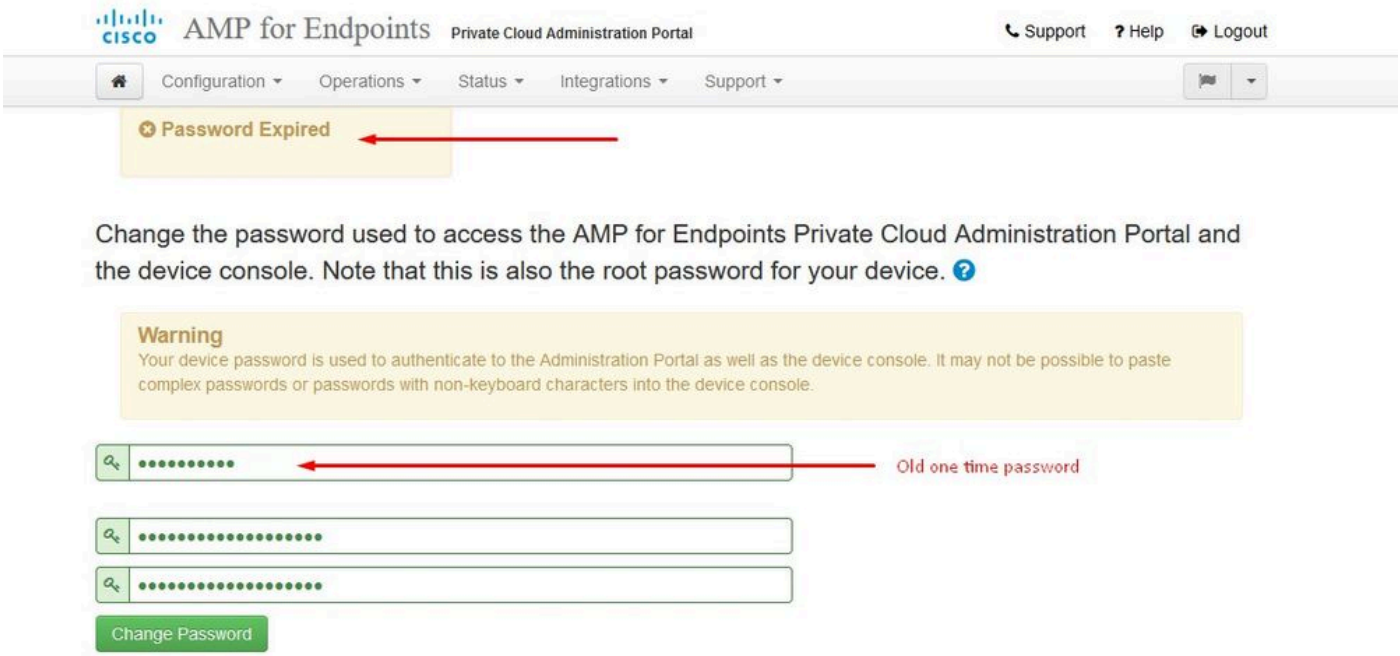


Paso 2:

Después de iniciar sesión, se le pedirá que restablezca la contraseña. Utilice la contraseña inicial de la consola en el campo Contraseña Antigua. Utilice la nueva contraseña en el campo Nueva contraseña. Vuelva a introducir la nueva contraseña en el campo New Password (Nueva contraseña). seleccione en Cambiar contraseña.

Paso 3:

Después de iniciar sesión, se le pedirá que restablezca la contraseña. Utilice la contraseña inicial de la consola en el campo Contraseña Antigua. Utilice la nueva contraseña en el campo Nueva contraseña. Vuelva a introducir la nueva contraseña en el campo New Password (Nueva contraseña). seleccione en Cambiar contraseña.

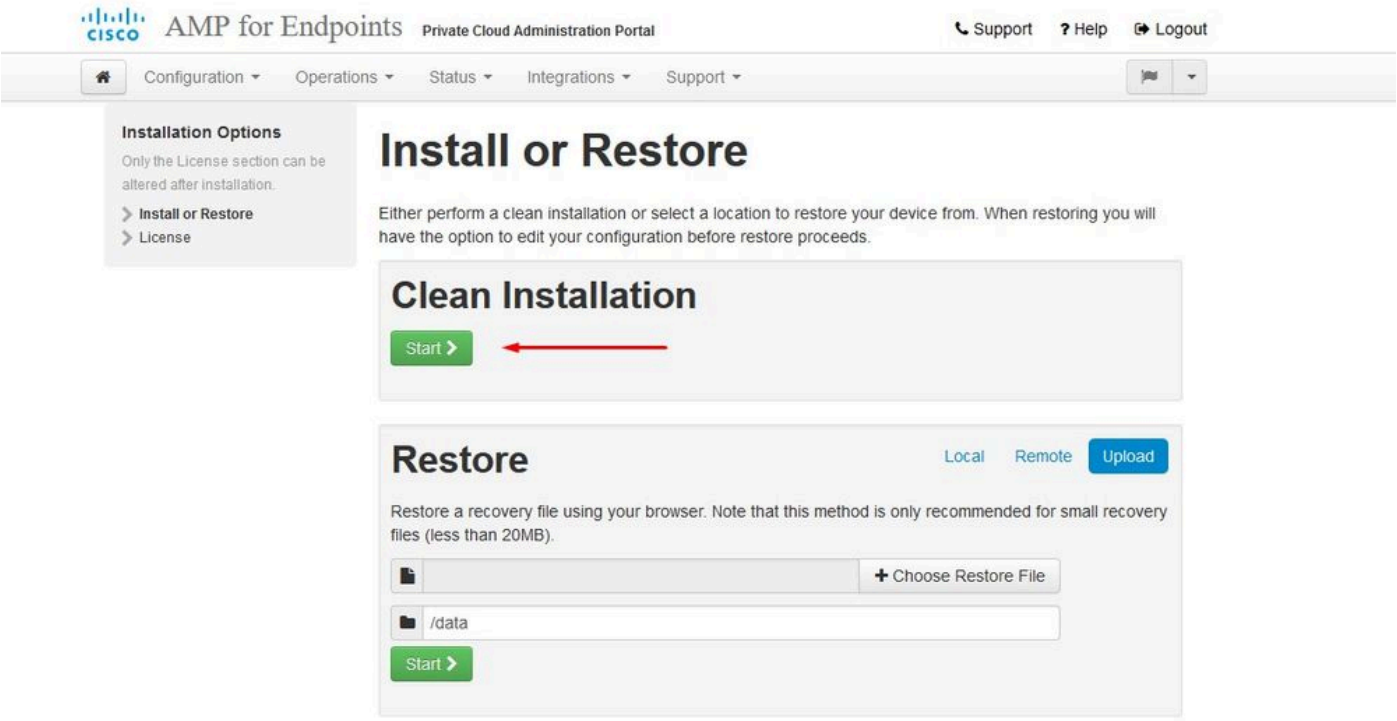


Paso 4:

En la página siguiente, desplácese hacia abajo para aceptar el acuerdo de licencia. seleccione en He leído y acepto.

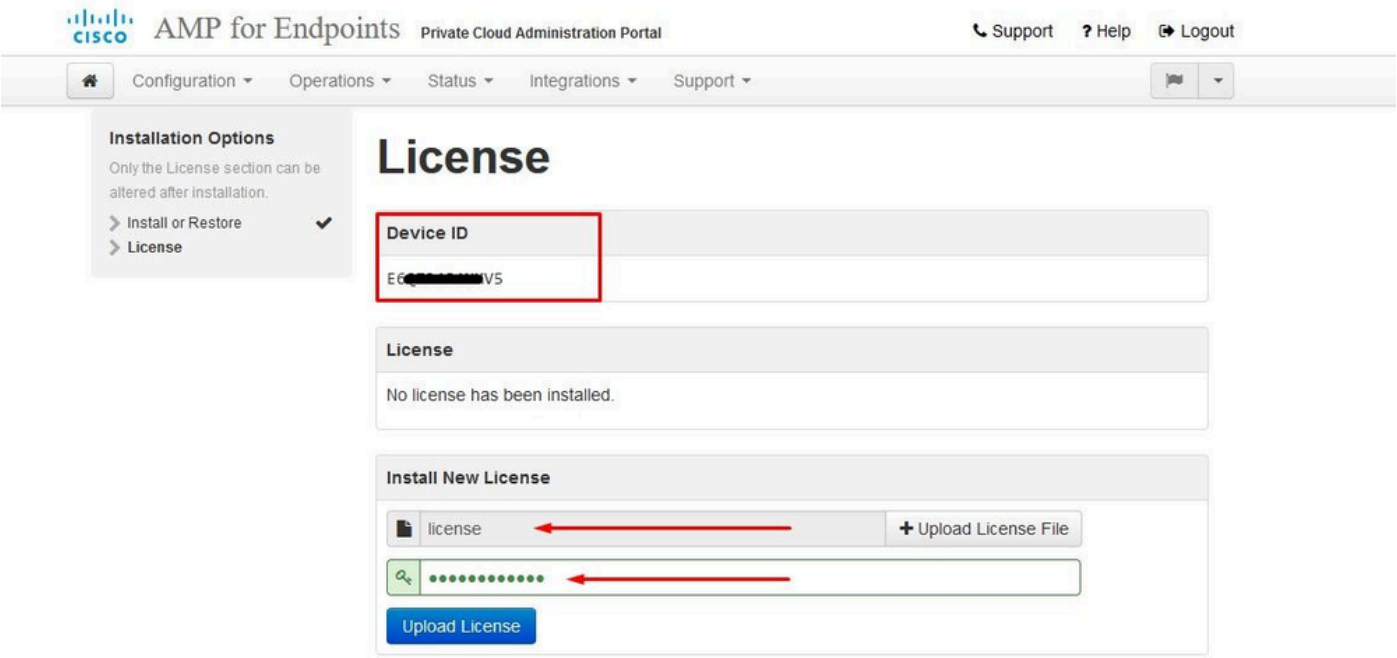
Paso 5:

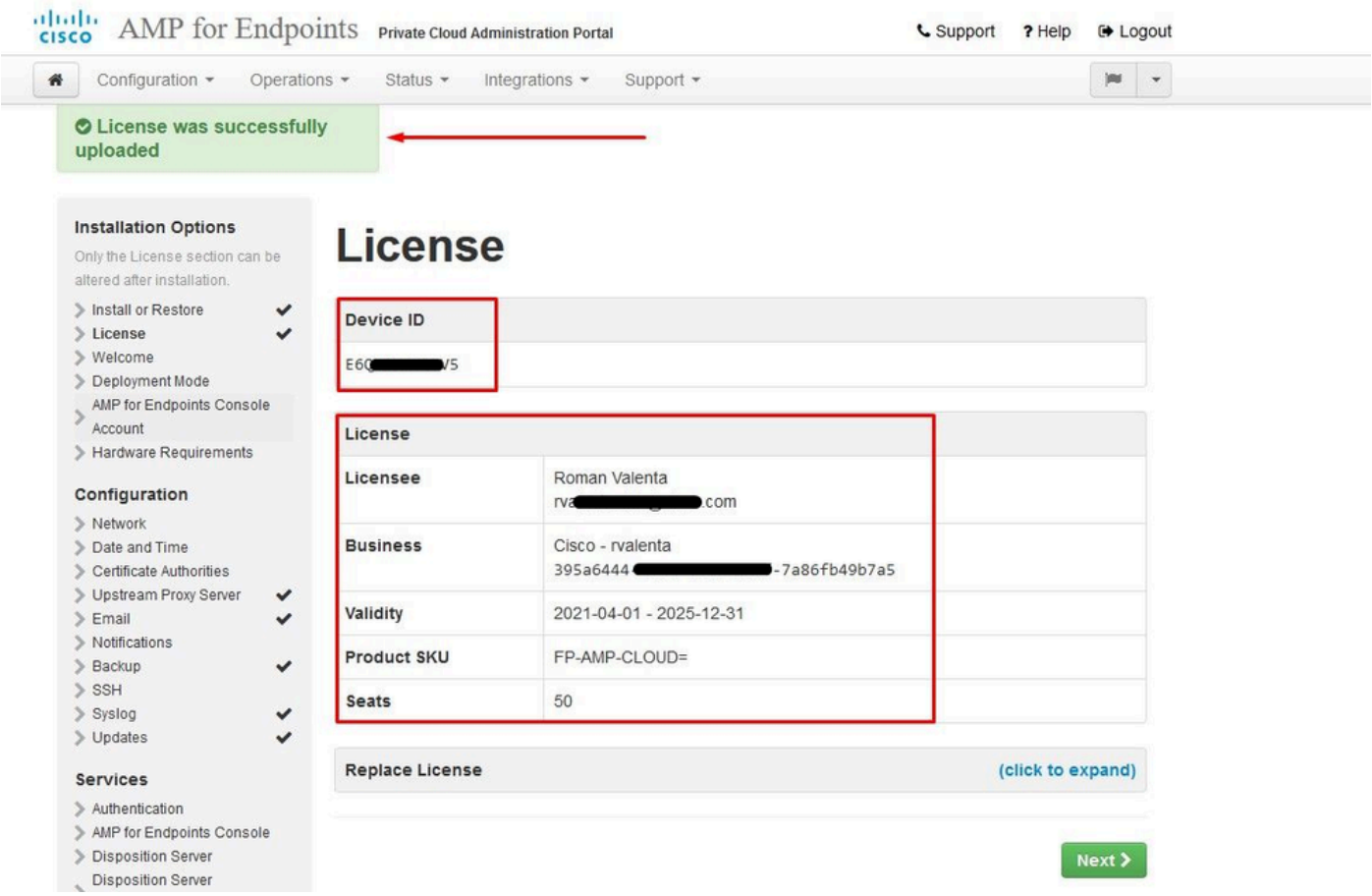
Después de aceptar el acuerdo, aparece la pantalla de instalación, como se muestra en la imagen. Si desea restaurar desde una copia de seguridad, puede hacerlo aquí; sin embargo, esta guía continúa con la opción Instalación limpia. Seleccione en Inicio en la sección Instalación limpia.



Paso 6:

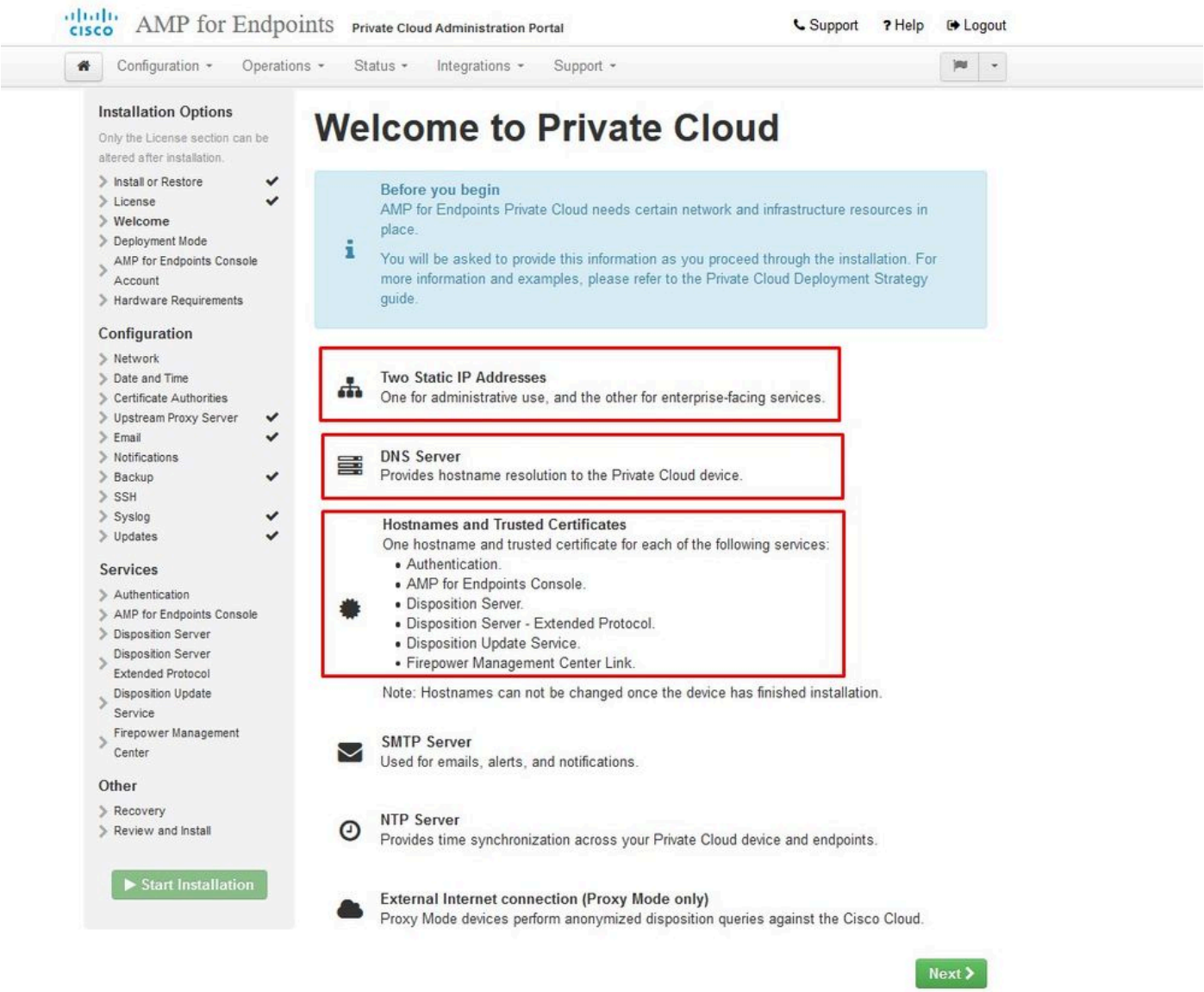
Lo primero que necesita es una licencia para seguir adelante. Al adquirir el producto, recibirá una licencia y una frase de contraseña. Seleccione en +Cargar archivo de licencia. Elija el archivo de licencia e introduzca la frase de paso. Seleccione en Cargar licencia. Si la carga no se realiza correctamente, compruebe que la frase de contraseña es correcta. Si la carga se realiza correctamente, se muestra una pantalla con información de licencia válida. Seleccione en Siguiente. Si sigue sin poder instalar la licencia, póngase en contacto con el servicio de asistencia técnica de Cisco.





Paso 7:

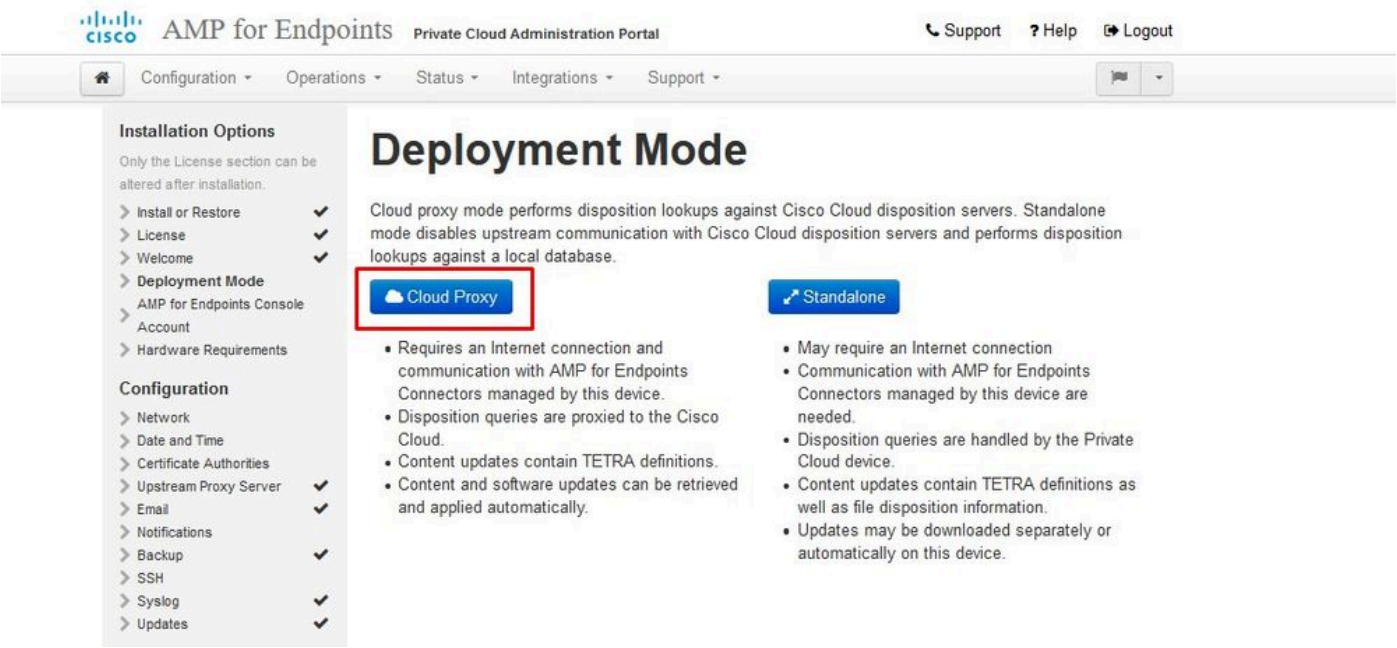
Recibirá la página de bienvenida, como se muestra en la imagen. Esta página muestra la información que debe tener antes de configurar la nube privada. Lea atentamente los requisitos. Seleccione en Siguiente para iniciar la configuración previa a la instalación.



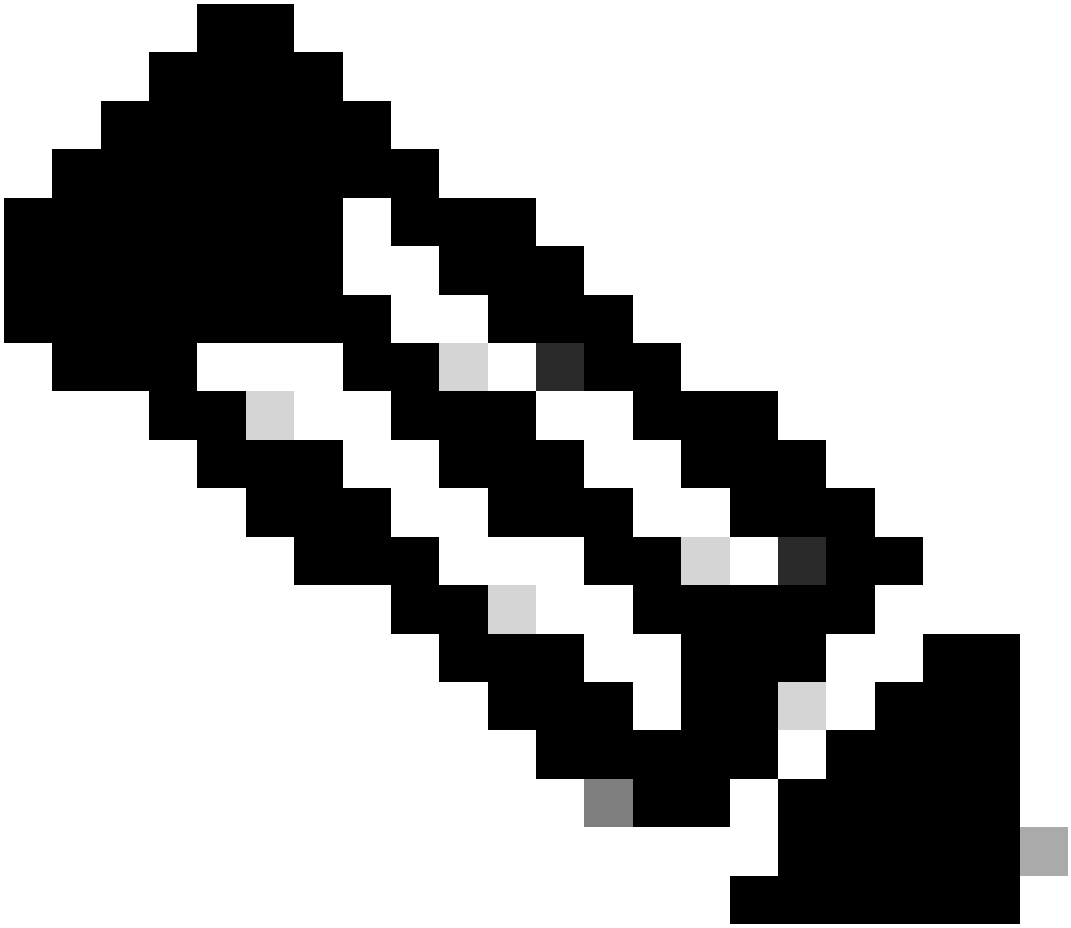
Configuración

Paso 1:

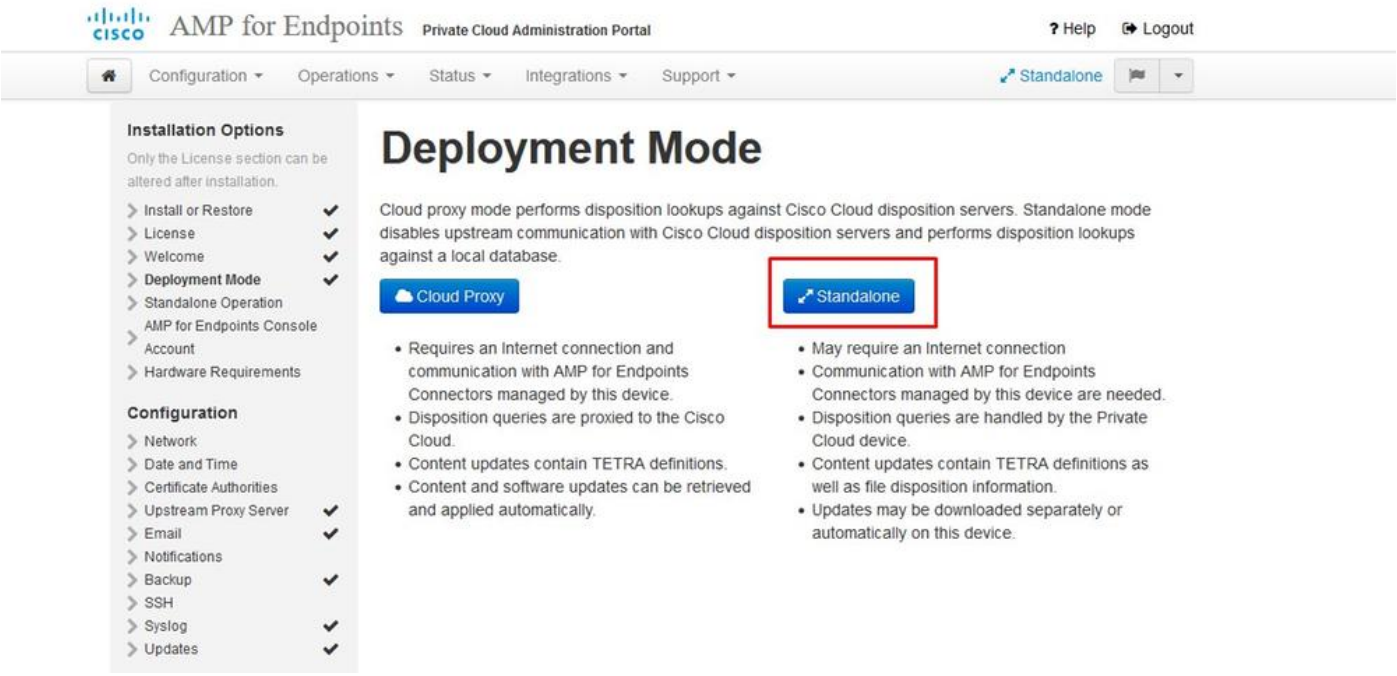
Nota: Tenga en cuenta que en los siguientes conjuntos de diapositivas incluimos algunas exclusivas, como se muestra en la imagen, que son exclusivas solo para el modo AIR GAP , las que se deben incluir y marcar como AIRGAP ONLY (SOLO AIRGAP)

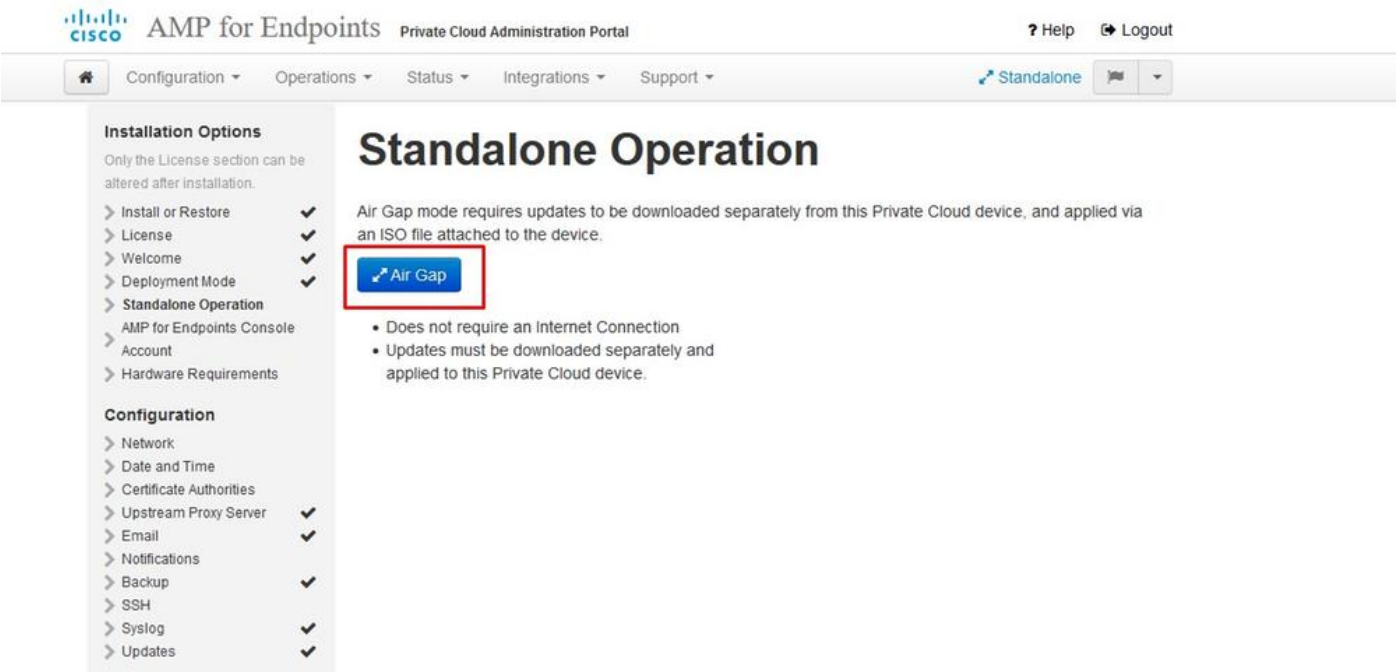

AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware 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
Standalone
• 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.
• 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.

⩔ ⩔ SÓLO AIRGAP ⩔ ⩔



Nota: Estos pasos sólo son aplicables a los dispositivos físicos.

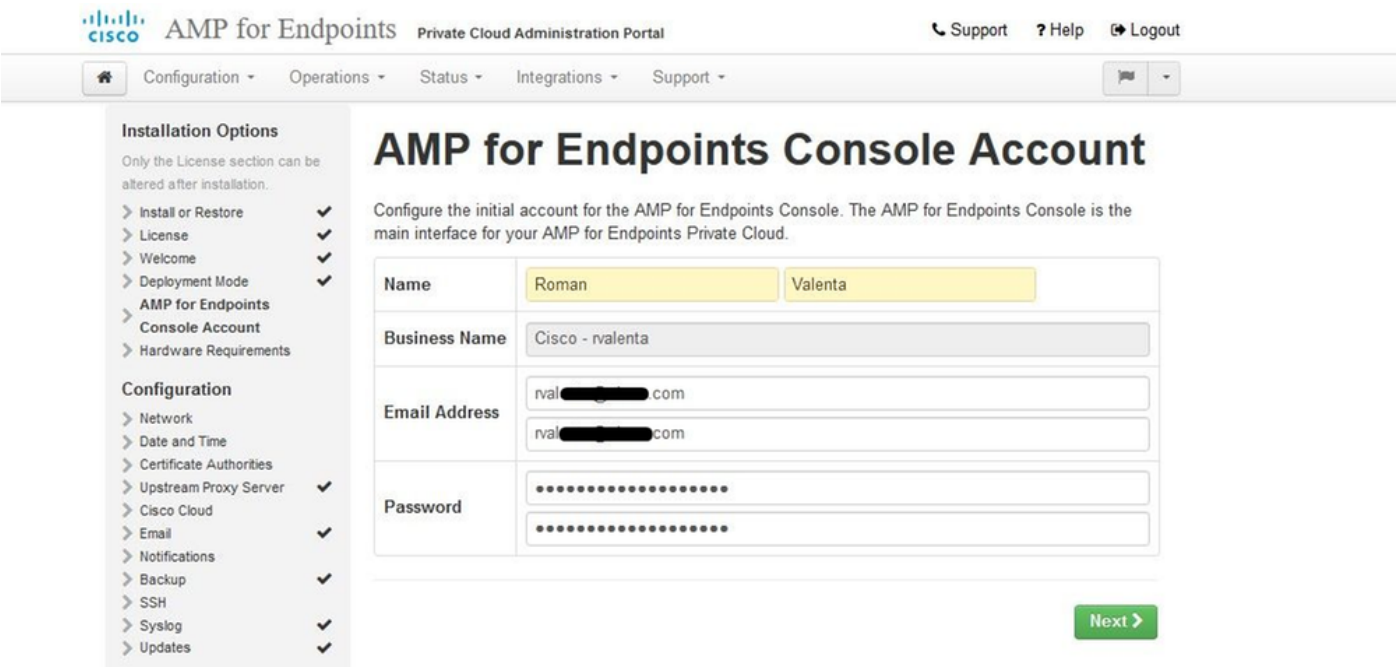




⩓ ⩓ AIRGAP SOLAMENTE ⩓ ⩓

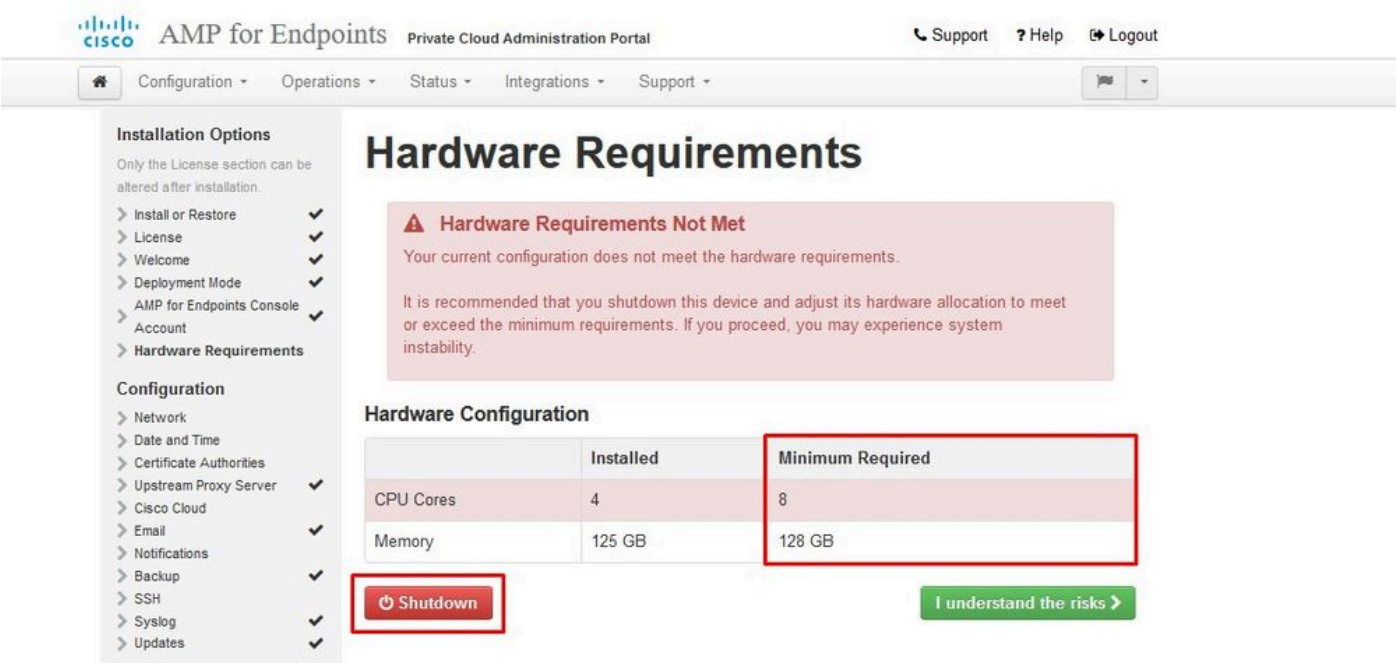
Paso 2:

Vaya a la página Secure Endpoint Console Account. La consola utiliza un usuario administrativo para crear directivas, grupos de equipos y agregar usuarios adicionales. Introduzca el nombre, la dirección de correo electrónico y la contraseña de la cuenta de consola. Seleccione en Siguiente.

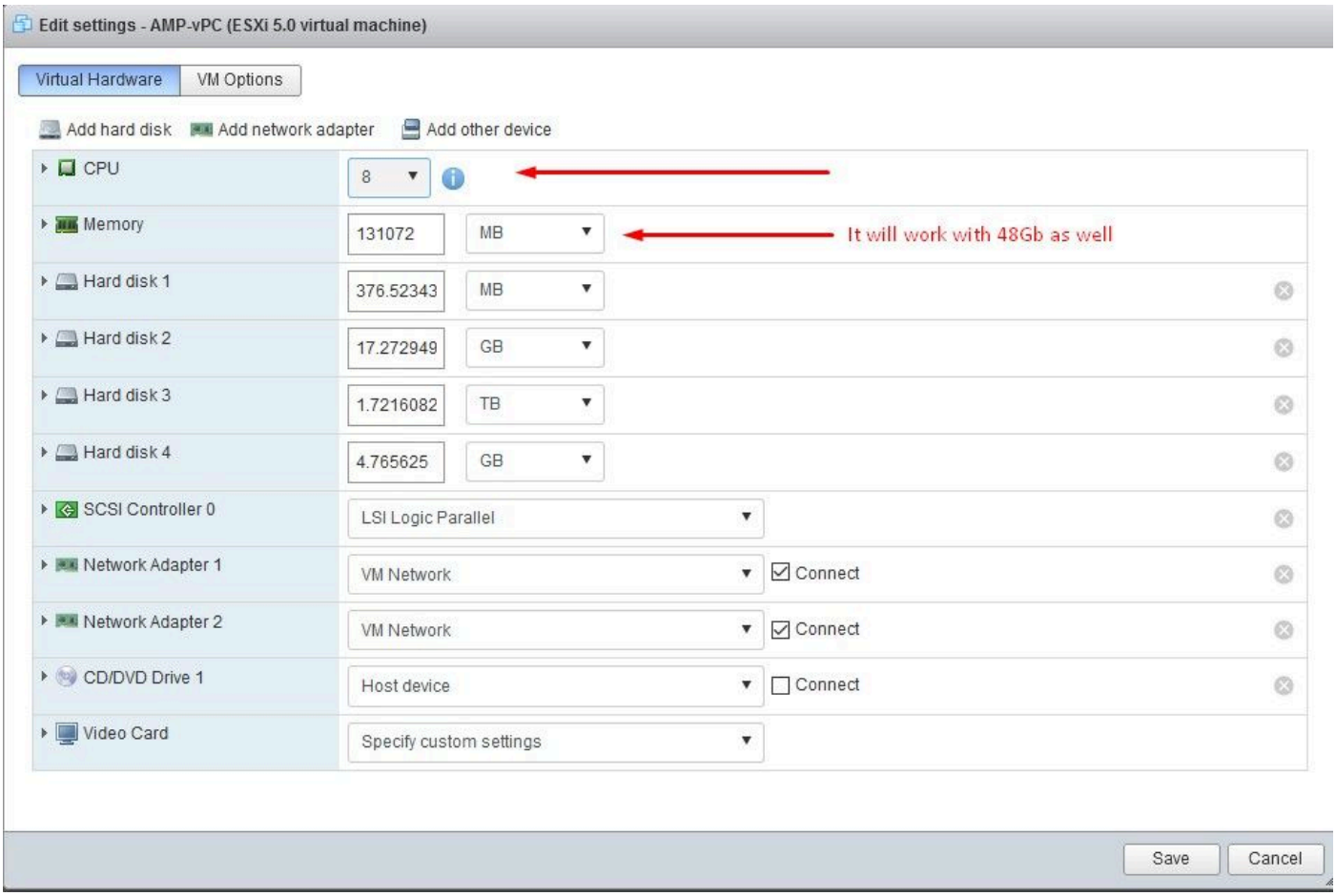


Si se ejecuta en este problema cuando implementa desde el archivo OVA, entonces tiene dos opciones, continuar y corregir este problema más tarde o apagar entonces para su VM implementada y ajustar en consecuencia. Después de reiniciar, continúe por donde se fue.

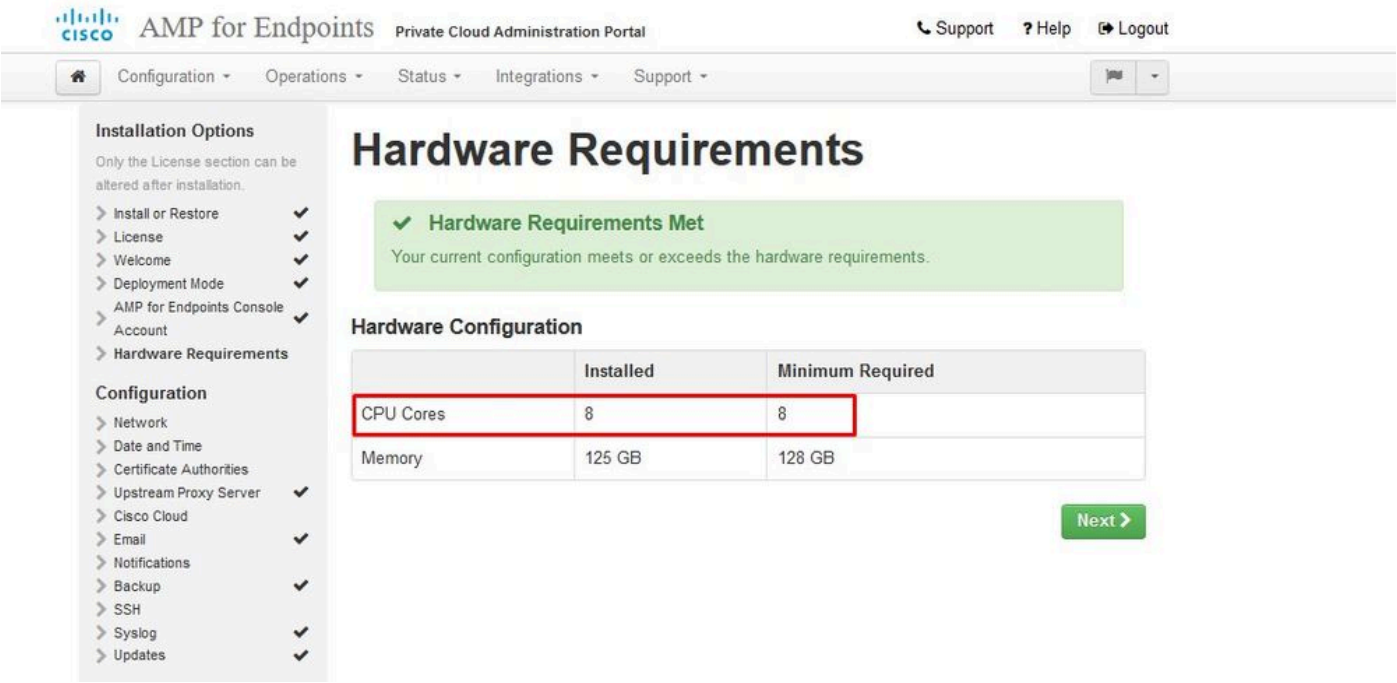
Nota: Esto se corrigió en el archivo OVA para la versión 3.5.2, que se carga correctamente con 128 GB de RAM y 8 núcleos de CPU



Nota: Utilice sólo los valores recomendados, a menos que sea para fines de laboratorio



Una vez reiniciados continuamos donde nos fuimos.

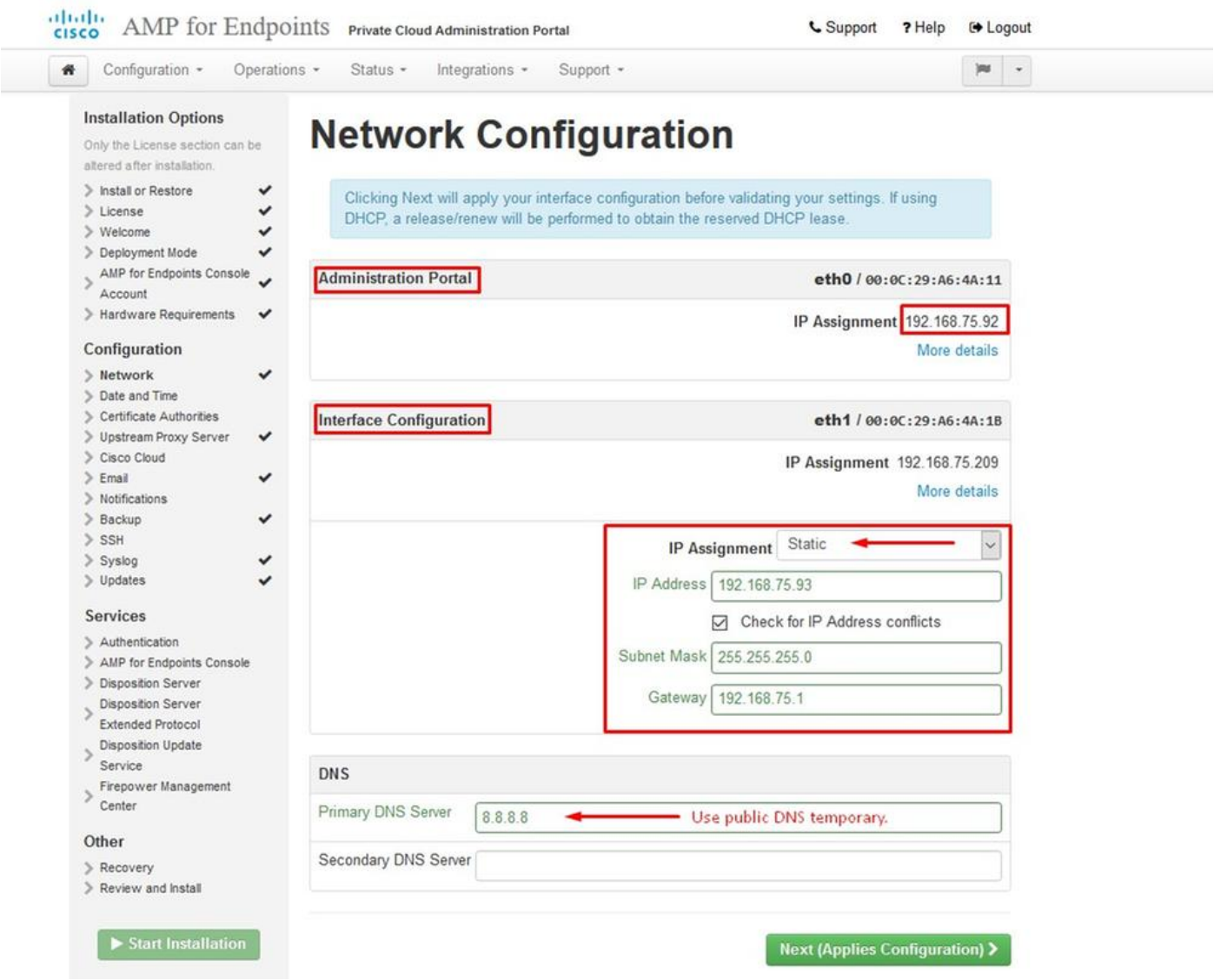


Asegúrese también de configurar ETH1 con IP ESTÁTICA.

Nota: Nunca debe configurar el dispositivo para utilizar DHCP a menos que haya creado reservas de direcciones MAC para las interfaces. Si las direcciones IP de sus interfaces

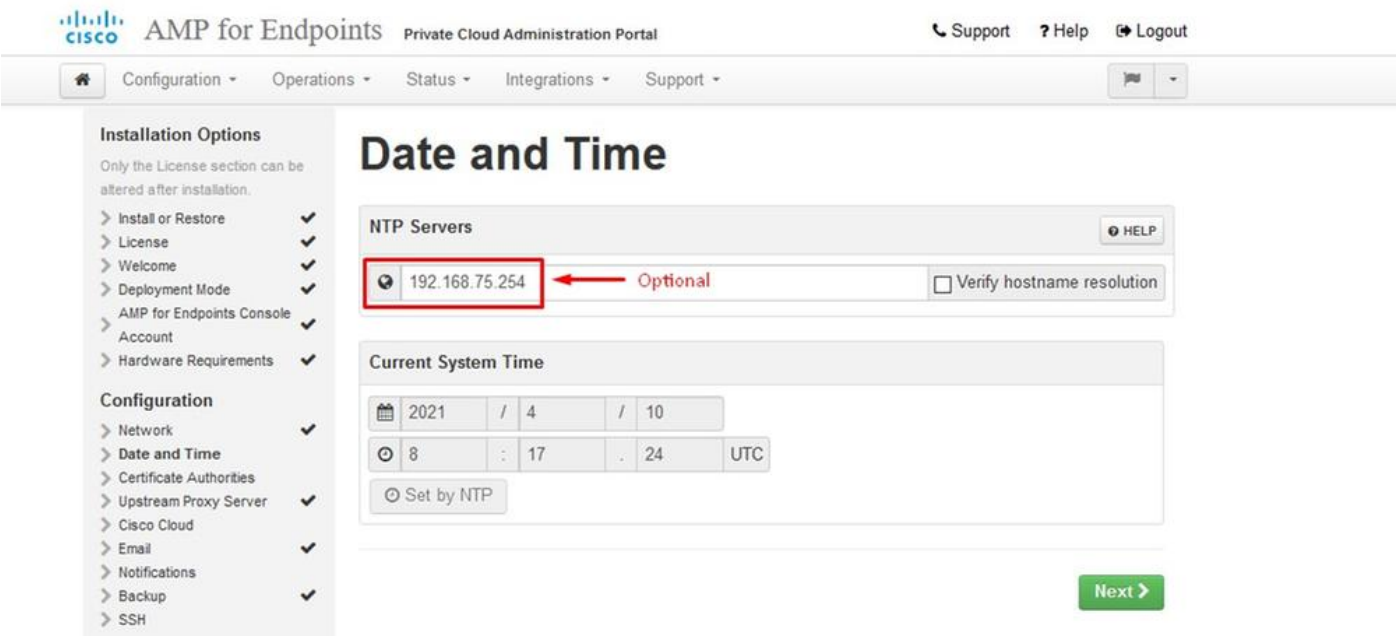
cambian, esto puede causar serios problemas con los Secure Endpoint Connectors implementados. Si no ha configurado el servidor DNS, puede utilizar DNS público temporal para finalizar la instalación.

Paso 3:

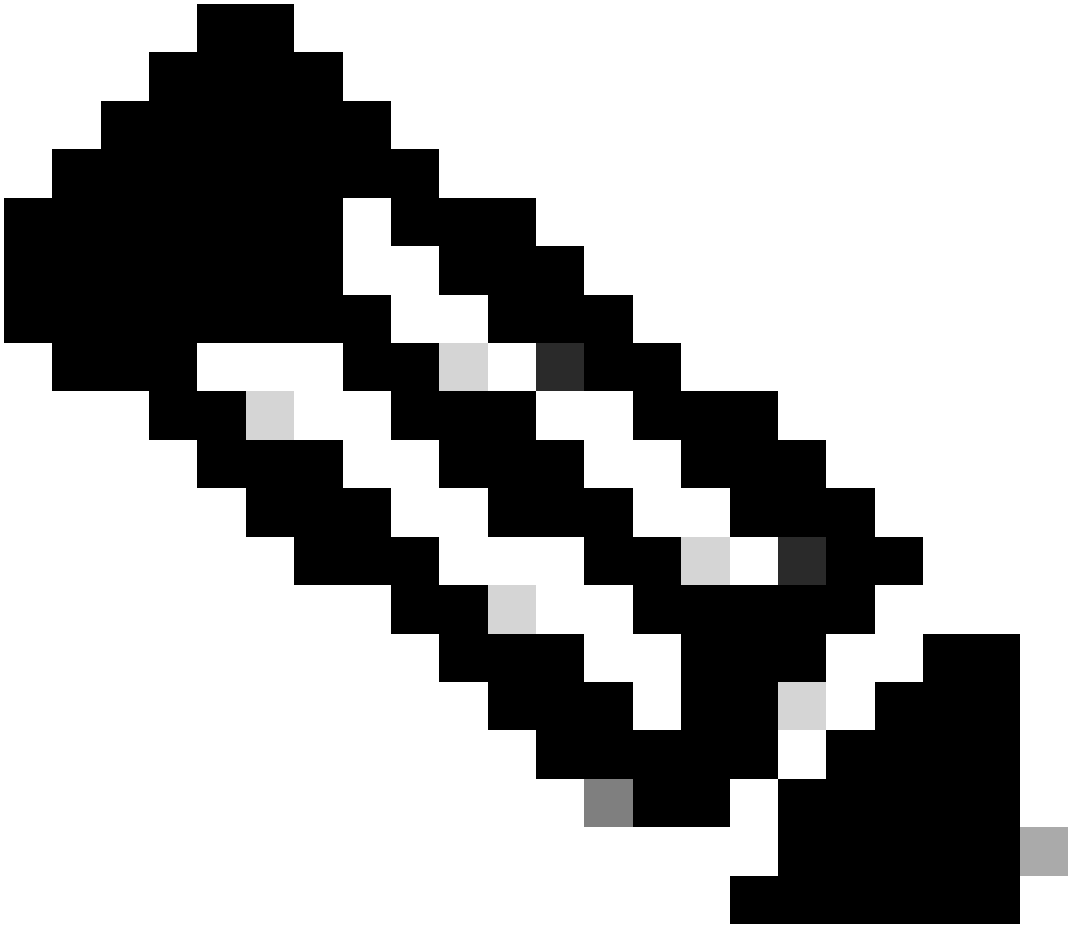


Paso 4:

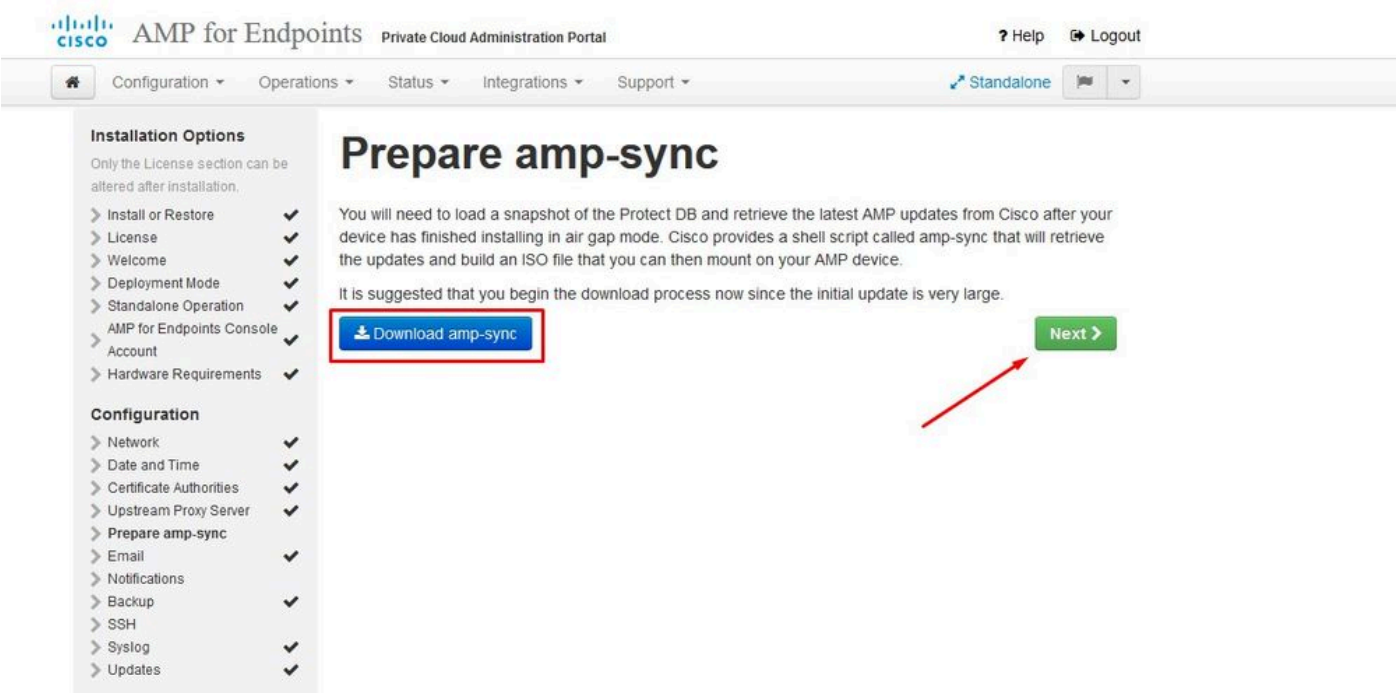
Aparecerá la página Fecha y hora. Introduzca las direcciones de uno o varios servidores NTP que desee utilizar para la sincronización de fecha y hora. Puede utilizar servidores NTP internos o externos y especificar más de uno mediante una lista delimitada por comas o espacios. Sincronice la hora con su navegador o ejecute amp-ctl ntpdate desde la consola del dispositivo para forzar una sincronización de hora inmediata con sus servidores NTP. Seleccione en Siguiente.


AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
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
HELP
192.168.75.254
Optional
Verify hostname resolution
Current System Time
2021 / 4 / 10
8 : 17 . 24 UTC
Set by NTP
Next

⩔ ⩔ SÓLO AIRGAP ⩔ ⩔



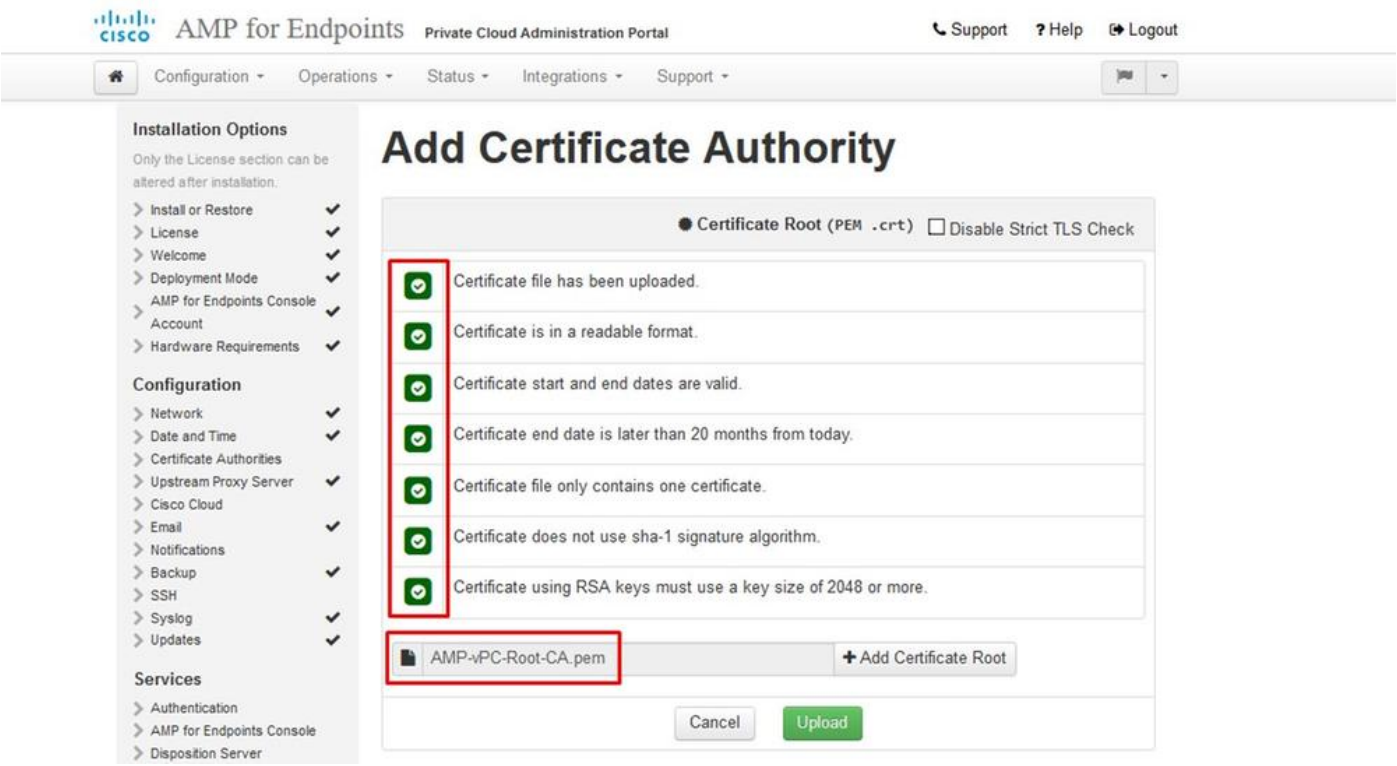
Nota: Estos pasos sólo son aplicables a los dispositivos físicos.

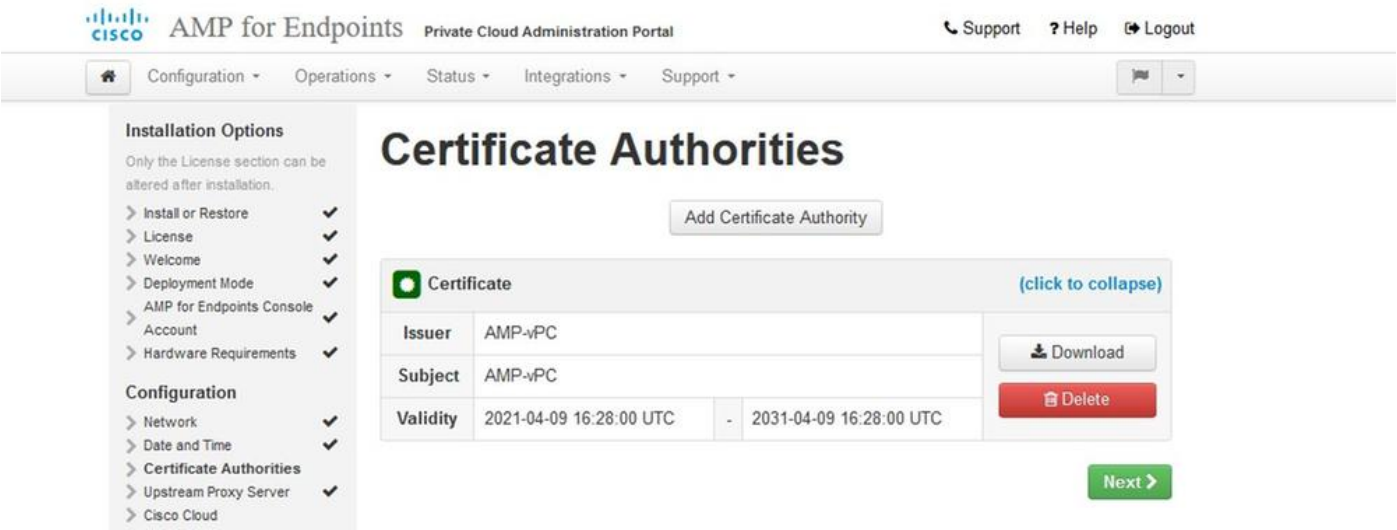


⩔ ⩔ AIRGAP SOLAMENTE ⩔ ⩔

Paso 5:

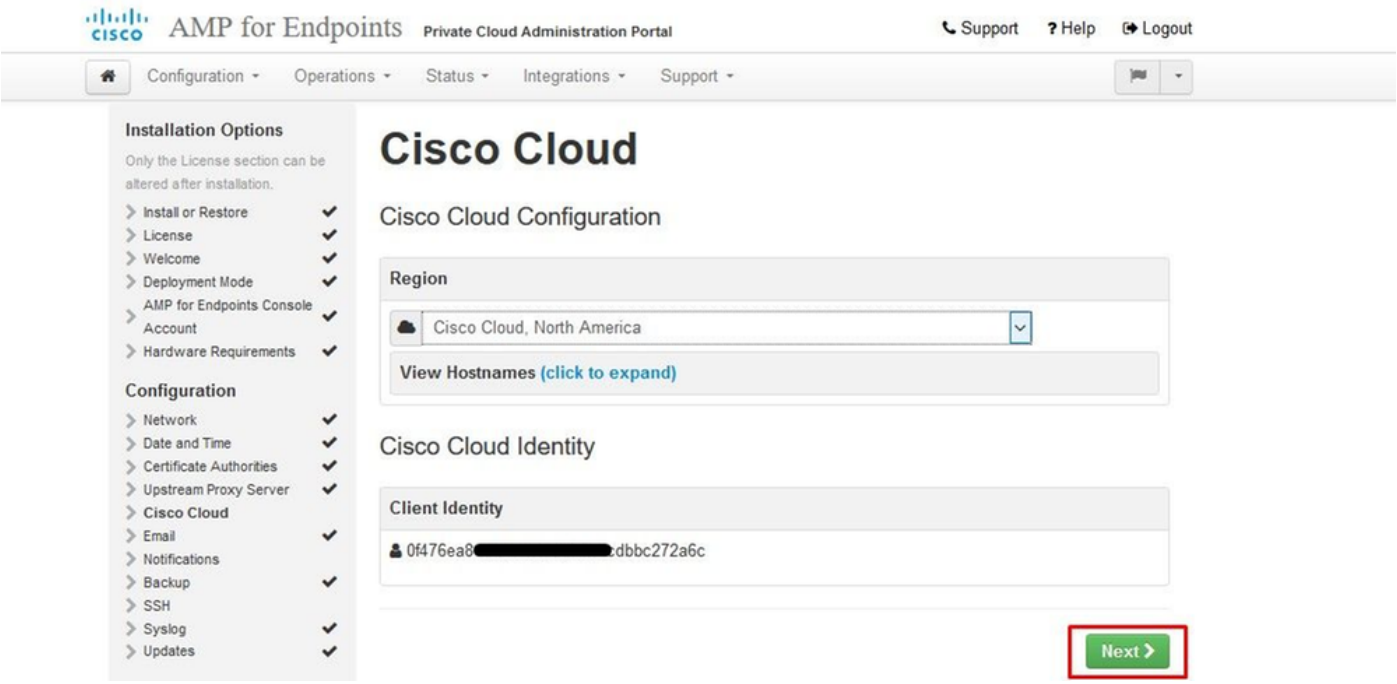
Aparece la página Autoridades de certificados, como se muestra en la imagen. Seleccione en Agregar autoridad certificadora para agregar su certificado raíz.





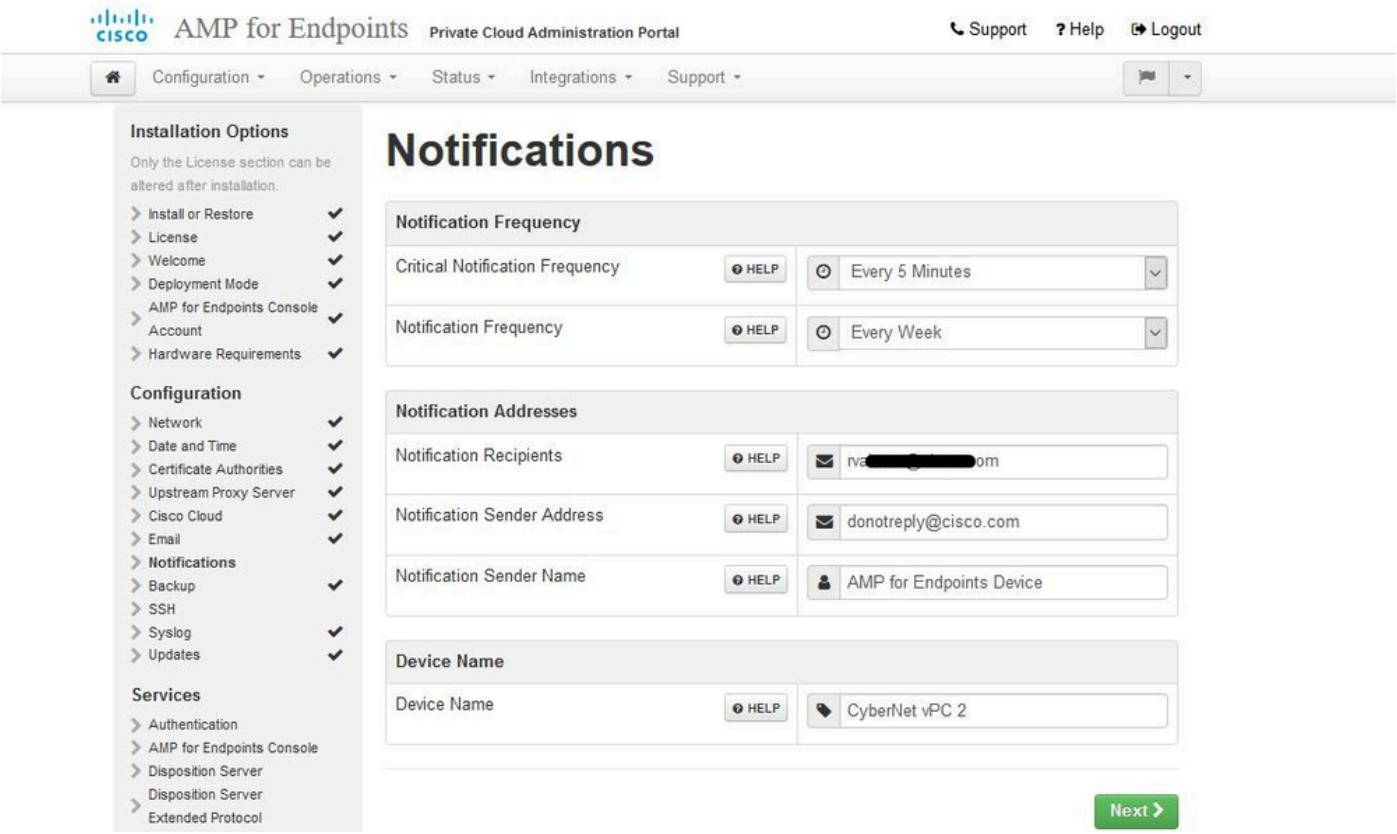
Paso 6:

El siguiente paso es configurar la página Cisco Cloud, como se muestra en la imagen. Seleccione la región de la nube de Cisco adecuada. Expanda Ver nombres de host si necesita crear excepciones de firewall para su dispositivo Secure Endpoint Private Cloud para comunicarse con la nube de Cisco para búsquedas de archivos y actualizaciones de dispositivos. Seleccione en Siguiente.



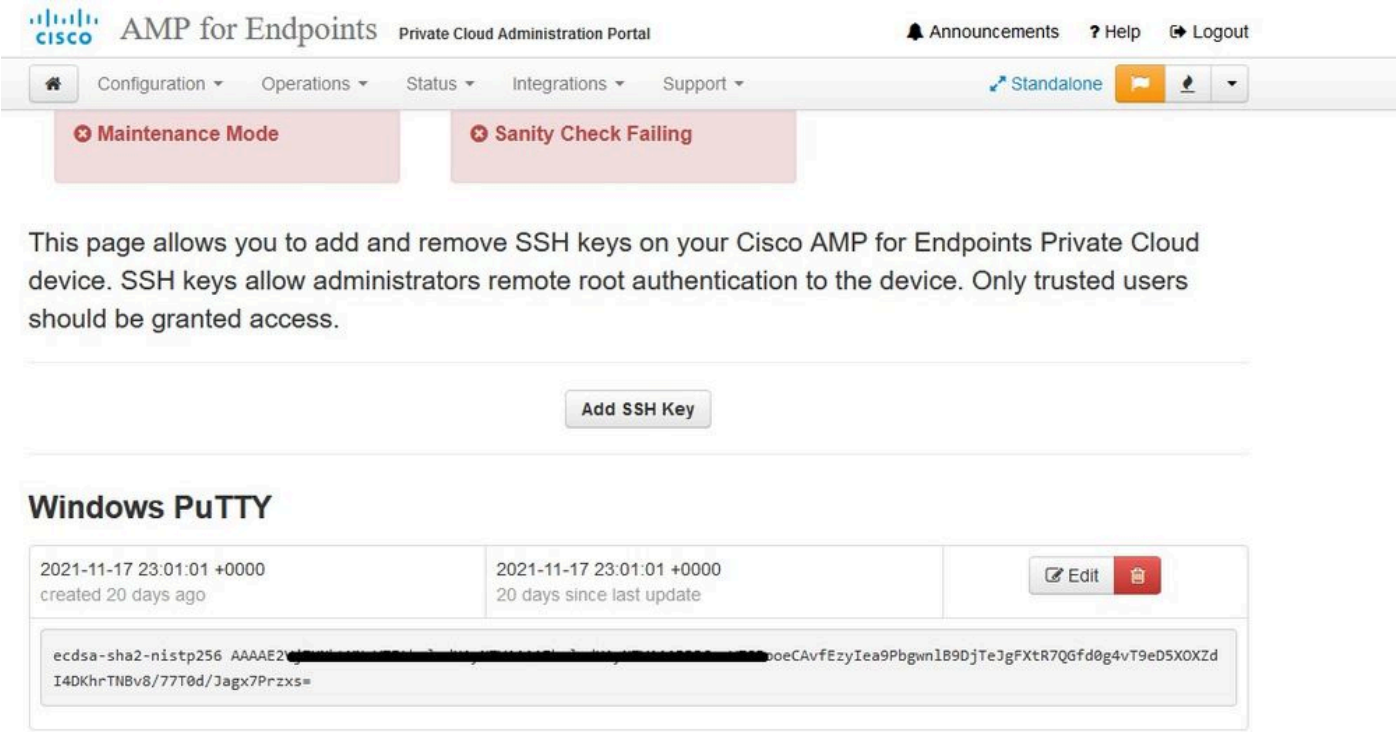
Paso 7:

Vaya a la página de notificaciones, como se muestra en la imagen. Seleccione la frecuencia de las notificaciones críticas y regulares. Introduzca las direcciones de correo electrónico a las que desea que se envíen notificaciones de alerta para el dispositivo de terminal seguro. Puede utilizar alias de correo electrónico o especificar varias direcciones mediante una lista separada por comas. También puede especificar el nombre del remitente y la dirección de correo electrónico que utiliza el dispositivo. Estas notificaciones no son las mismas que las suscripciones de Secure Endpoint Console. También puede especificar un nombre de dispositivo único si tiene varios dispositivos de nube privada de terminal seguro. Seleccione en Siguiente.



Paso 8:

A continuación, acceda a la página SSH Keys (Claves SSH), como se muestra en la imagen. Seleccione en Agregar clave SSH para introducir cualquier clave pública que desee agregar al dispositivo. Las claves SSH le permiten acceder al dispositivo a través de un shell remoto con privilegios de root. Sólo los usuarios de confianza deben tener acceso. El dispositivo de nube privada requiere una clave RSA con formato OpenSSH. Puede agregar más claves SSH más adelante mediante Configuration > SSH en el portal de administración. Seleccione en Siguiente.



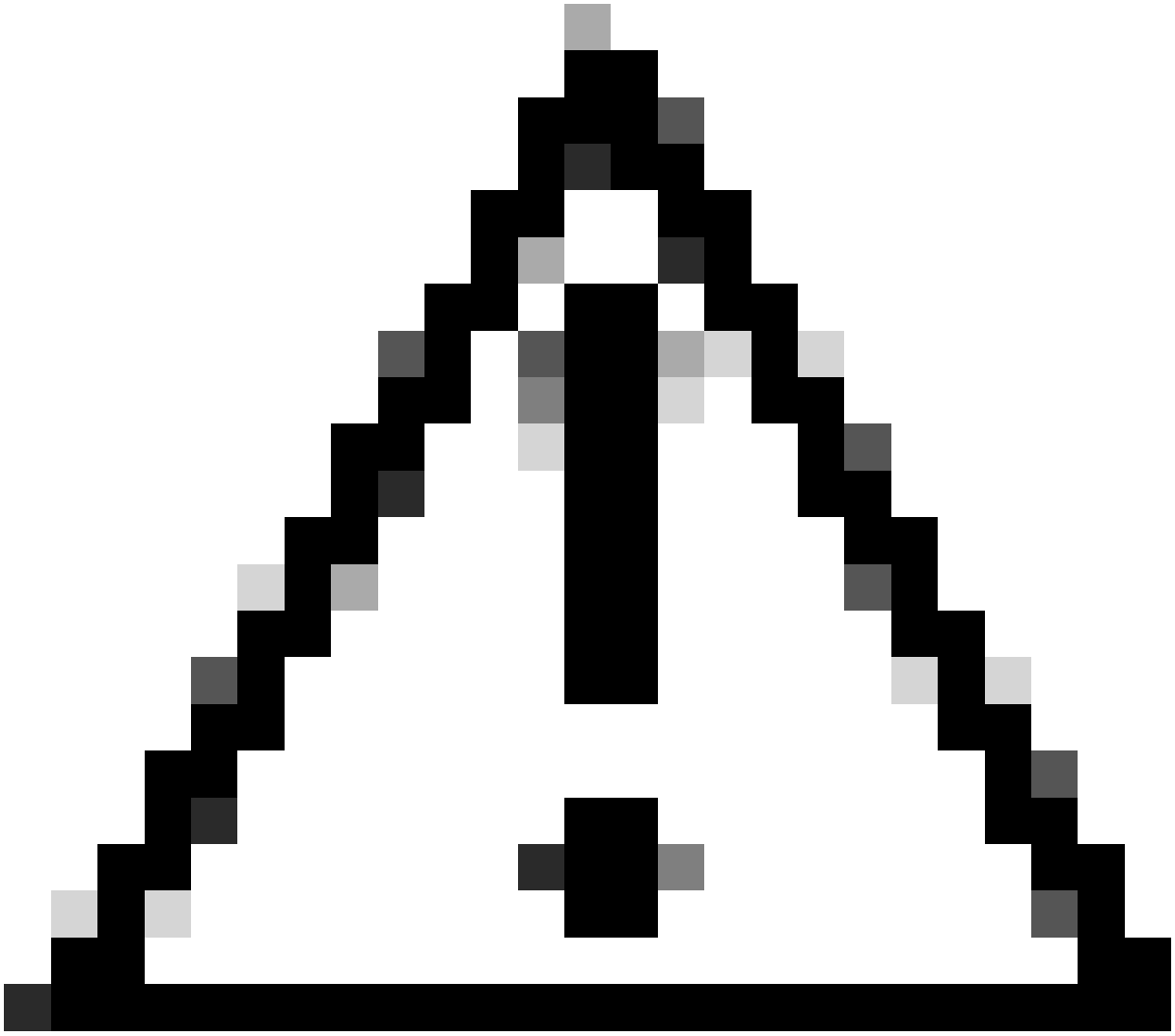
A continuación, accederá a la sección Servicios. En las páginas siguientes, debe asignar nombres de host y cargar los pares de certificado y clave adecuados para estos servicios de dispositivos. En las siguientes diapositivas podemos ver la configuración de uno de los 6 certificados.

Services

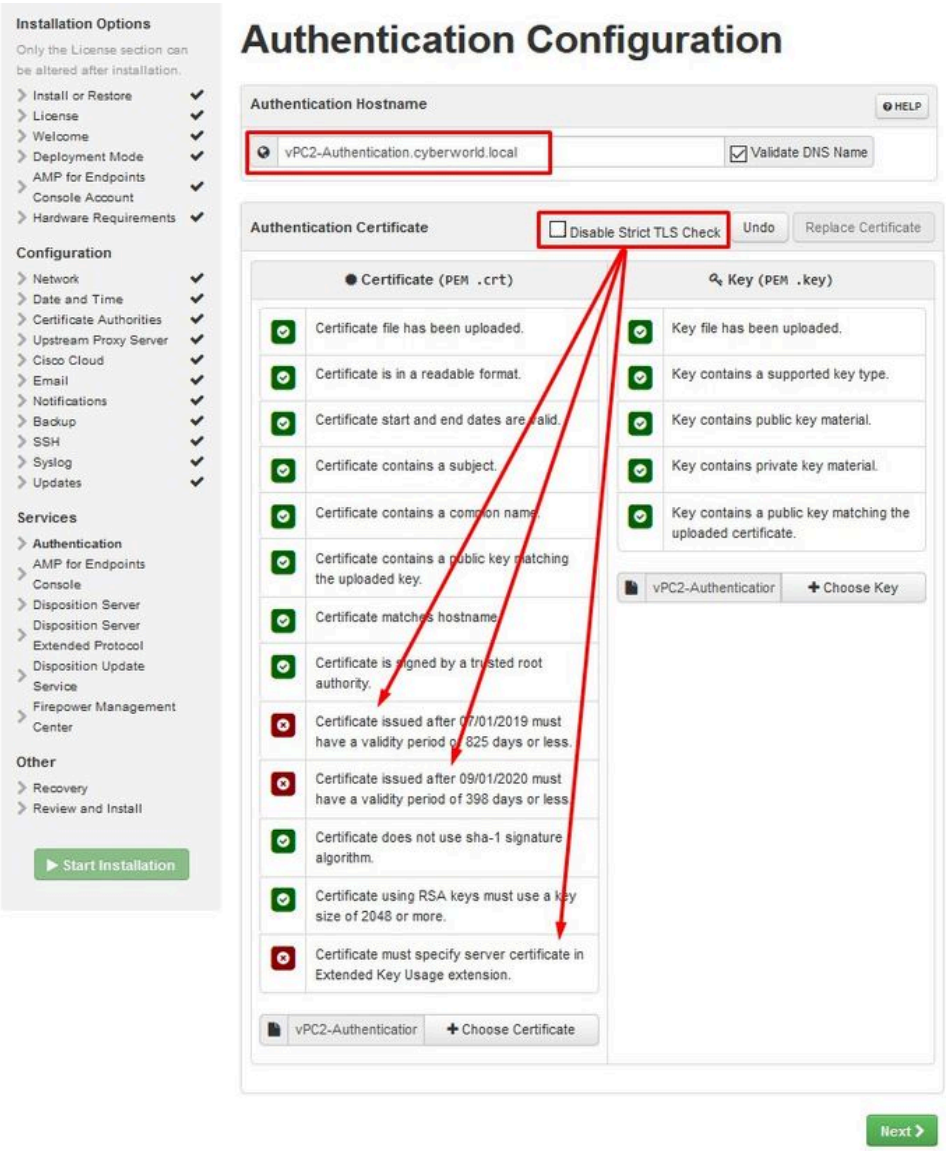
Paso 1:

Durante el proceso de configuración, es posible que se ejecute en estos errores.

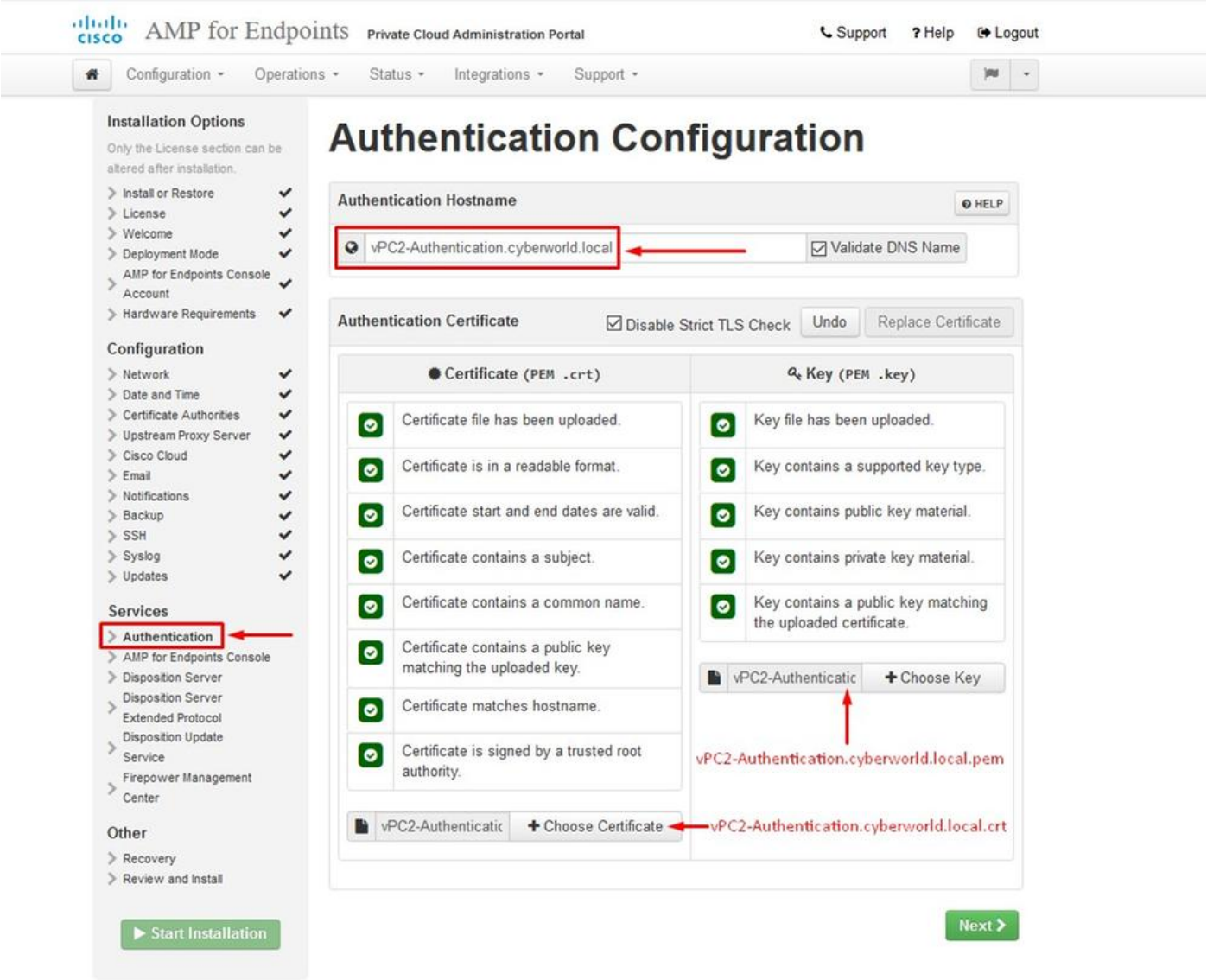
El primer "error" que observe se resalta con las 3 flechas. Para omitir esto simplemente desmarque "Desactivar verificación TLS estricta"



Precaución: En VPC 3.8.2 y versiones posteriores de TLS Web Server se requiere ahora la autenticación para que se acepte el certificado, el certificado de servicio no puede exceder la validez de 398 días.



Sin verificación TLS estricta

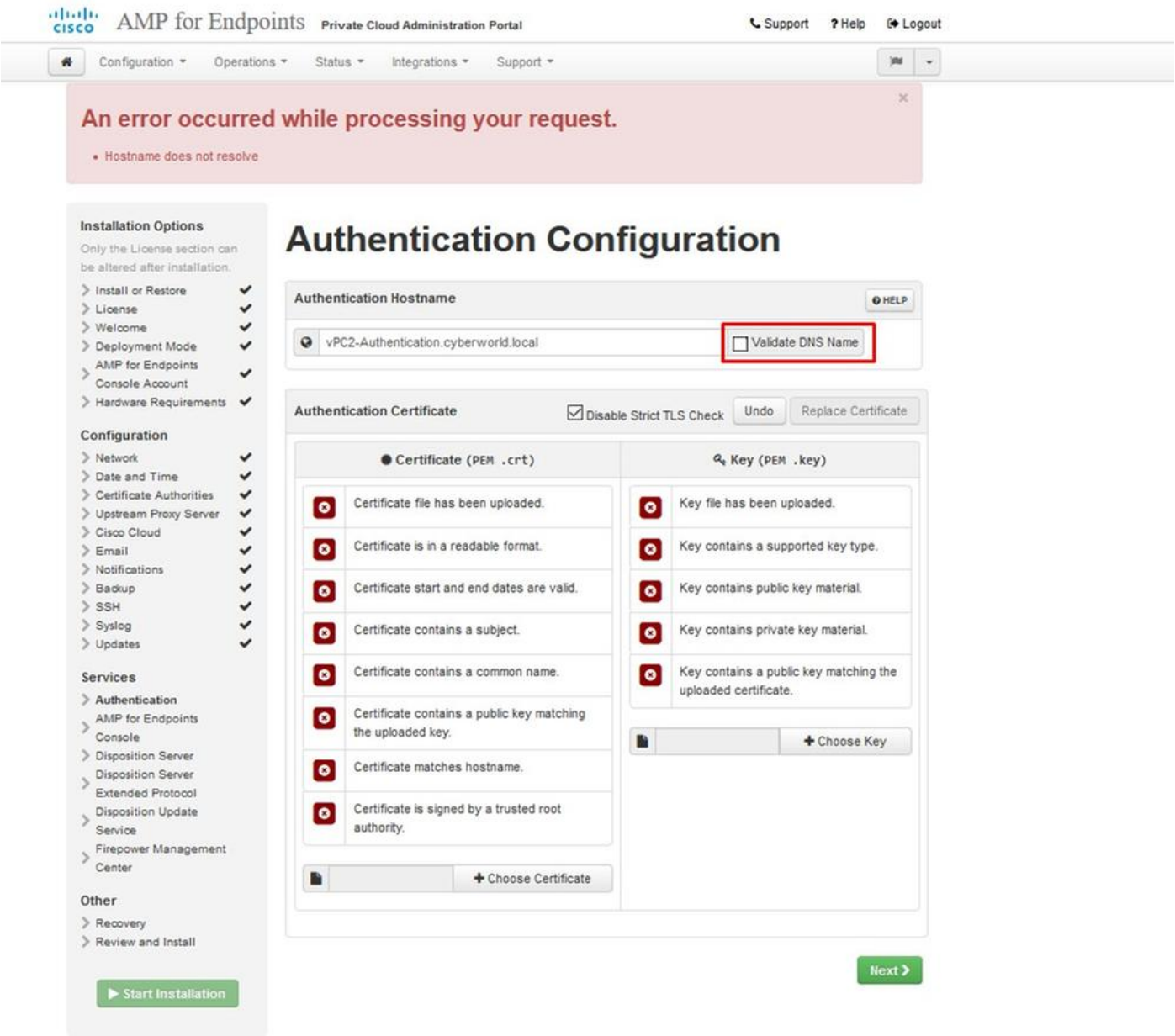


Paso 2:

El siguiente error que aparece es si deja la opción "Validar nombre DNS" activada. Aquí tiene dos opciones.

#1: Desactive la marca de verificación Validar DNS

#2: Vuelva al servidor DNS y configure el resto de los registros de host.



Ahora repita el mismo proceso cinco veces más para el resto de los certificados.

Autenticación

- El servicio de autenticación se puede utilizar en versiones futuras de la nube privada para gestionar la autenticación de usuarios.

Consola de terminal segura

- Consola es el nombre DNS donde el administrador de Secure Endpoint puede acceder a la consola de Secure Endpoint y los conectores de Secure Endpoint reciben nuevas políticas y actualizaciones.

Servidor de disposición

- Servidor de disposición es el nombre DNS donde los conectores de terminal seguro envían y recuperan la información de búsqueda en la nube.

Servidor de disposición - Protocolo extendido

- Servidor de disposición: el protocolo extendido es el nombre DNS donde los nuevos conectores de terminal seguro envían y recuperan la información de búsqueda en la nube.

Servicio de actualización de disposición

- El servicio de actualización de disposición se utiliza cuando se enlaza un dispositivo Cisco Threat Grid a un dispositivo de nube privada. El dispositivo Threat Grid se utiliza para enviar archivos para su análisis desde Secure Endpoint Console y Disposition Update Service se utiliza en Threat Grid para actualizar la disposición (limpia o malintencionada) de los archivos una vez analizados.

Centro de administración FirePOWER

-El enlace a Firepower Management Center le permite vincular un dispositivo Cisco Firepower Management Center (FMC) a su dispositivo de nube privada. Esto le permite mostrar datos de terminales seguros en el panel de FMC. Para obtener más información sobre la integración de FMC con un terminal seguro, consulte la documentación de FMC.

⚠ Precaución: los nombres de host no se pueden cambiar una vez que el dispositivo ha finalizado la instalación.

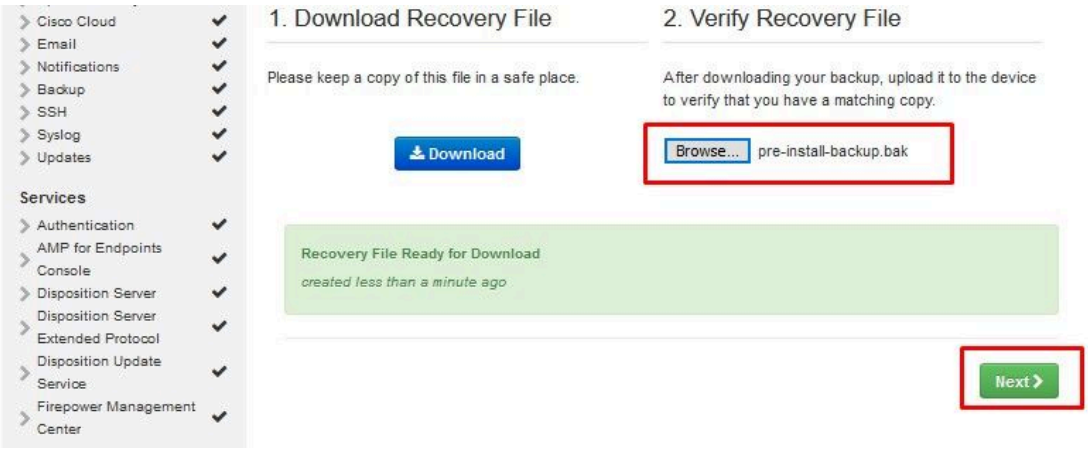
Anote los nombres de host necesarios. Debe crear seis registros A de DNS únicos para la nube privada de terminal seguro. Cada registro apunta a la misma dirección IP de la interfaz de Virtual Private Cloud Console (eth1) y deben resolverse tanto en la nube privada como en el terminal seguro.

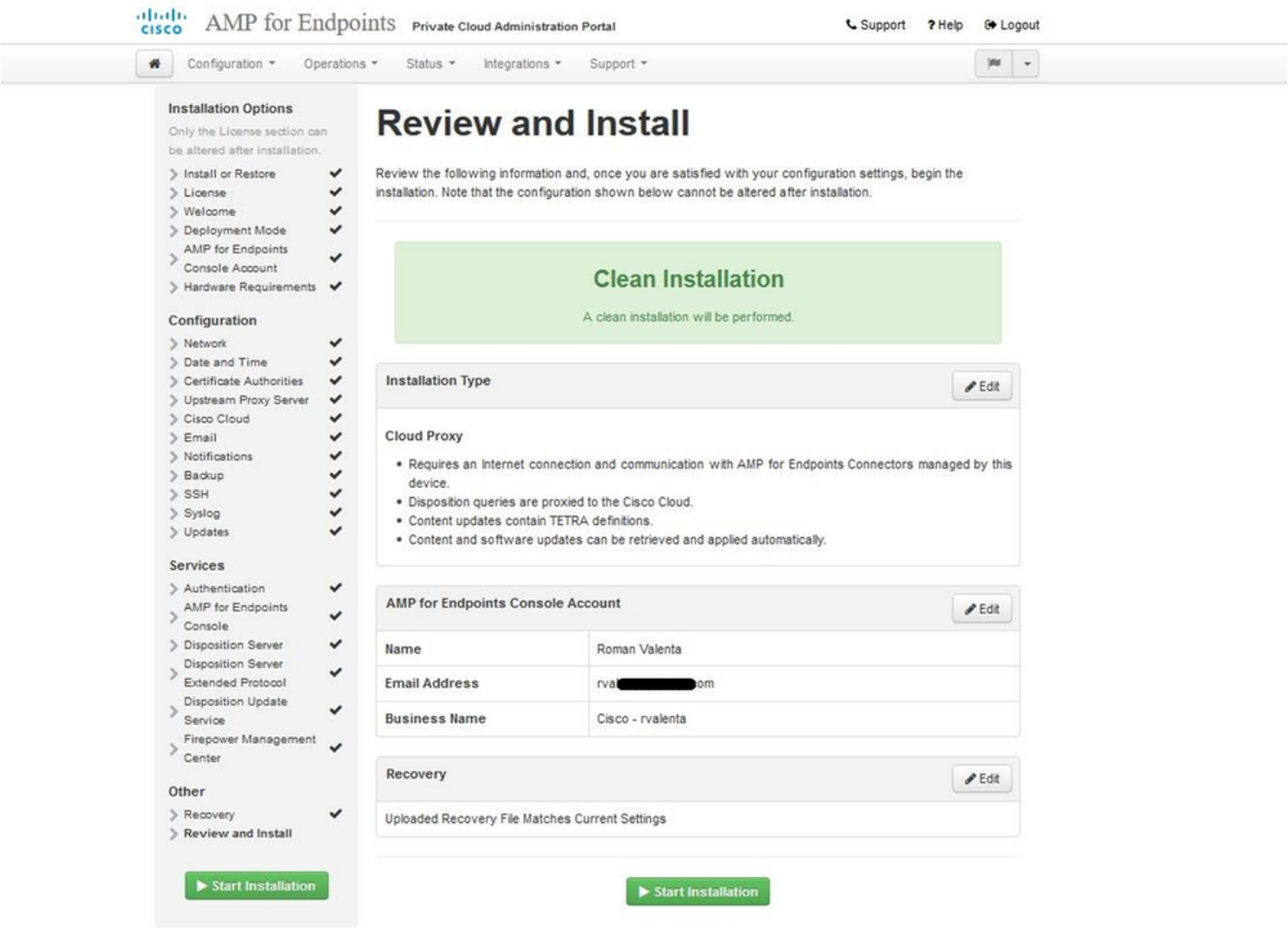
Paso 3:

En la página siguiente, descargue y verifique Recovery File.

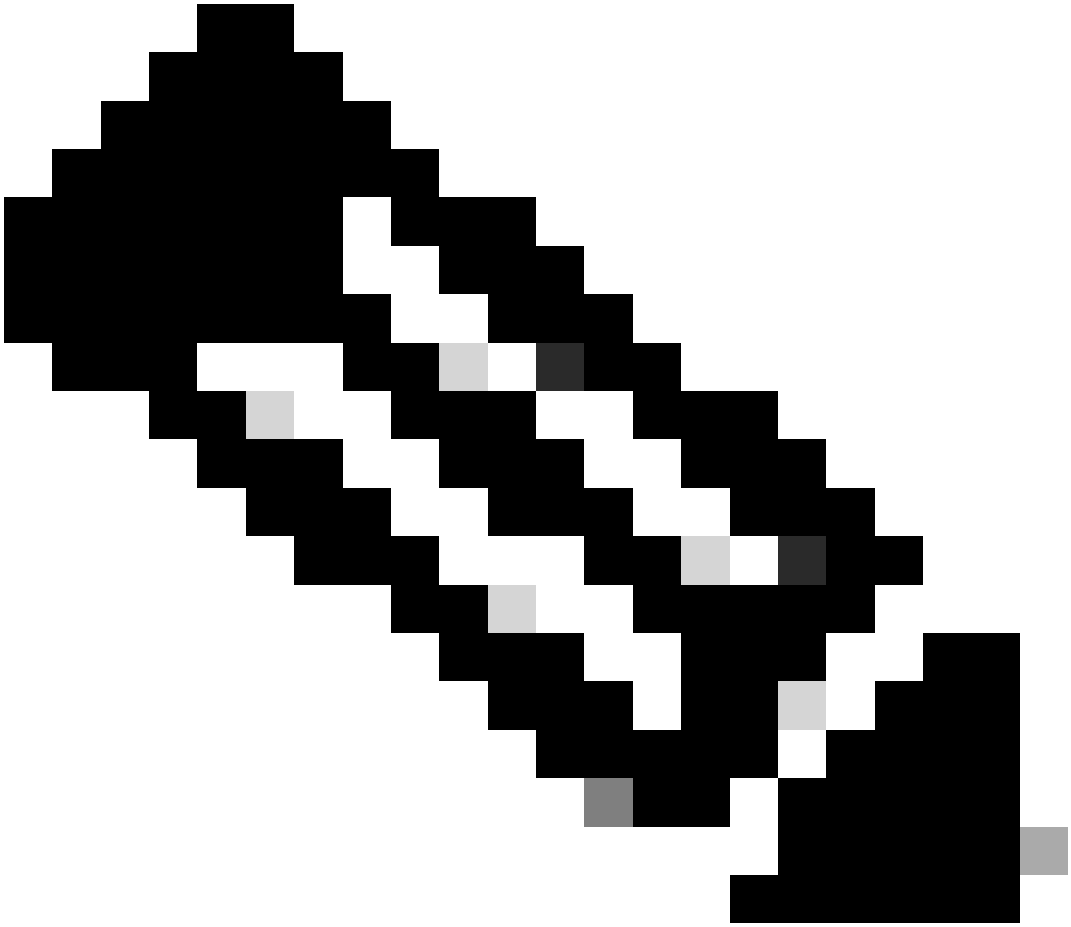
Usted obtiene la página de recuperación, como se muestra en la imagen. Debe descargar y verificar una copia de seguridad de la configuración antes de iniciar la instalación. El archivo de recuperación contiene toda la configuración, así como las claves del servidor. Si pierde un archivo de recuperación, no podrá restaurar la configuración y tendrá que volver a instalar todos los conectores de Secure Endpoint. Sin una clave original, tendrá que volver a configurar toda la infraestructura de nube privada con nuevas claves. El archivo de recuperación contiene todas las configuraciones relacionadas con el portal opadmin. El archivo de copia de seguridad contiene el contenido del archivo de recuperación, así como cualquier dato del portal del panel, como eventos, historial de conectores, etc. Si desea restaurar solo el opadmin sin los datos del evento y todo, puede utilizar el archivo de recuperación. Si restaura desde el archivo de copia de seguridad, se restaurarán los datos de opadmin y del portal de paneles.

Seleccione en Descargar para guardar la copia de seguridad en el ordenador local. Una vez descargado el archivo, seleccione en Choose File para cargar el archivo de copia de seguridad y verificar que no esté dañado. Seleccione en Siguiente para verificar el archivo y continuar.

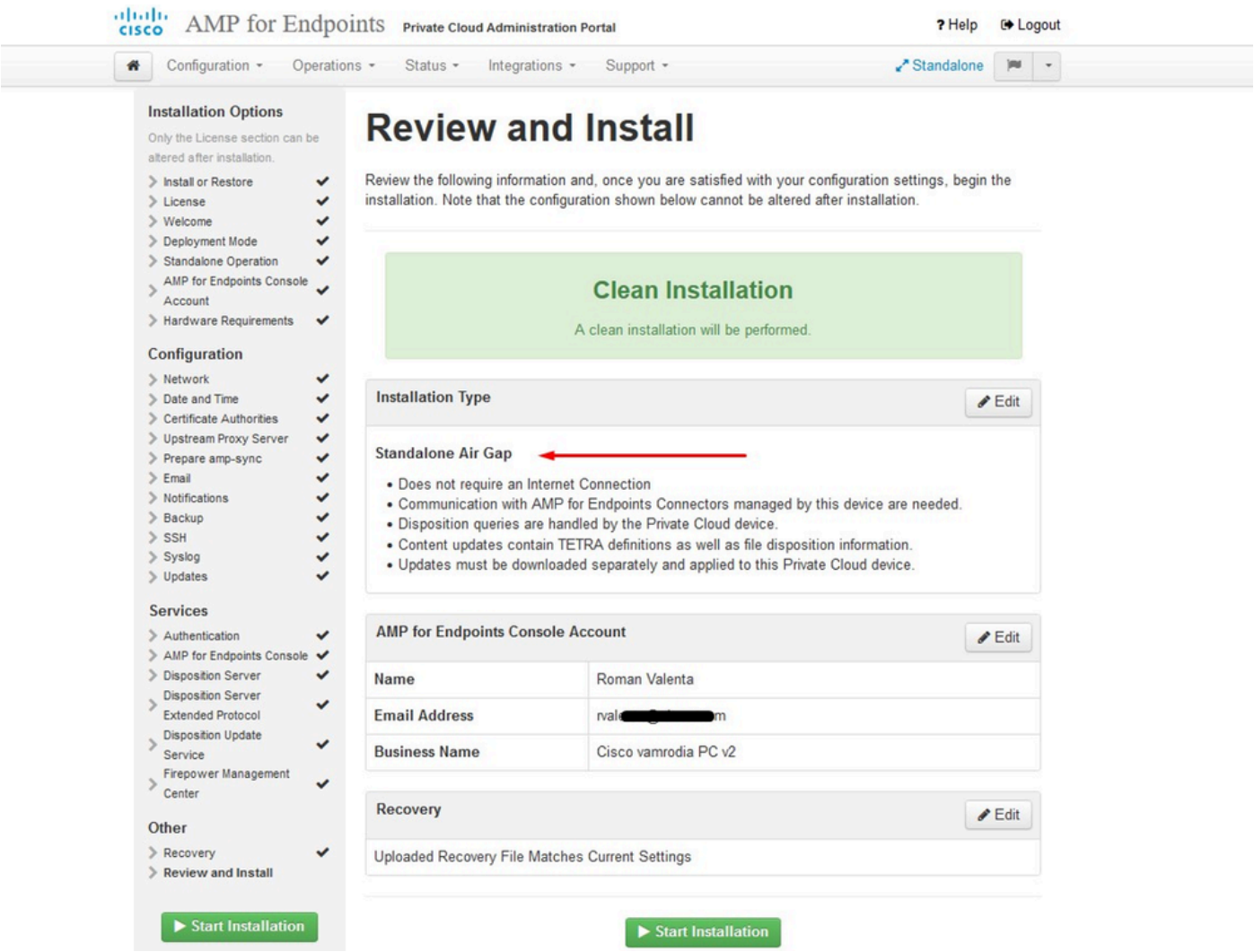

Cisco Cloud
Email
Notifications
Backup
SSH
Syslog
Updates
Services
Authentication
AMP for Endpoints Console
Disposition Server
Disposition Server Extended Protocol
Disposition Update Service
Firepower Management Center
1. Download Recovery File
Please keep a copy of this file in a safe place.
Download
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


AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
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]om
Business Name
Cisco - rvalenta
Recovery
Edit
Uploaded Recovery File Matches Current Settings
Start Installation

⩔ ⩔ SÓLO AIRGAP ⩔ ⩔



Nota: Estos pasos sólo son aplicables a los dispositivos físicos.



⩔ ⩔ AIRGAP SOLAMENTE ⩔ ⩔

Se ve una entrada similar como esta...

⚠ Precaución: Cuando esté en esta página, no la actualice, ya que puede 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 dow
nloads.
[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

Una vez finalizada la instalación, pulse el botón de reinicio

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

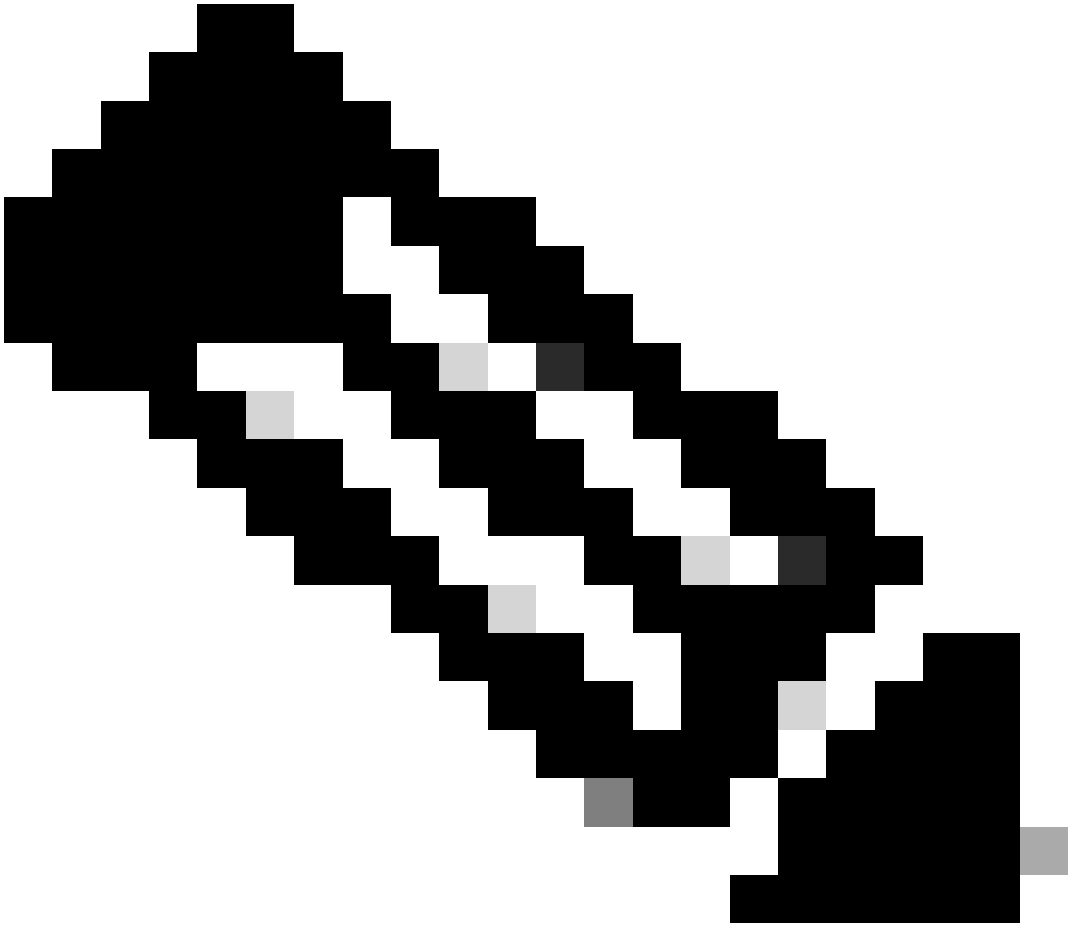
Output

```
[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

⩔ ⩔ SÓLO AIRGAP ⩔ ⩔



Nota: Estos pasos sólo son aplicables a los dispositivos físicos.

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

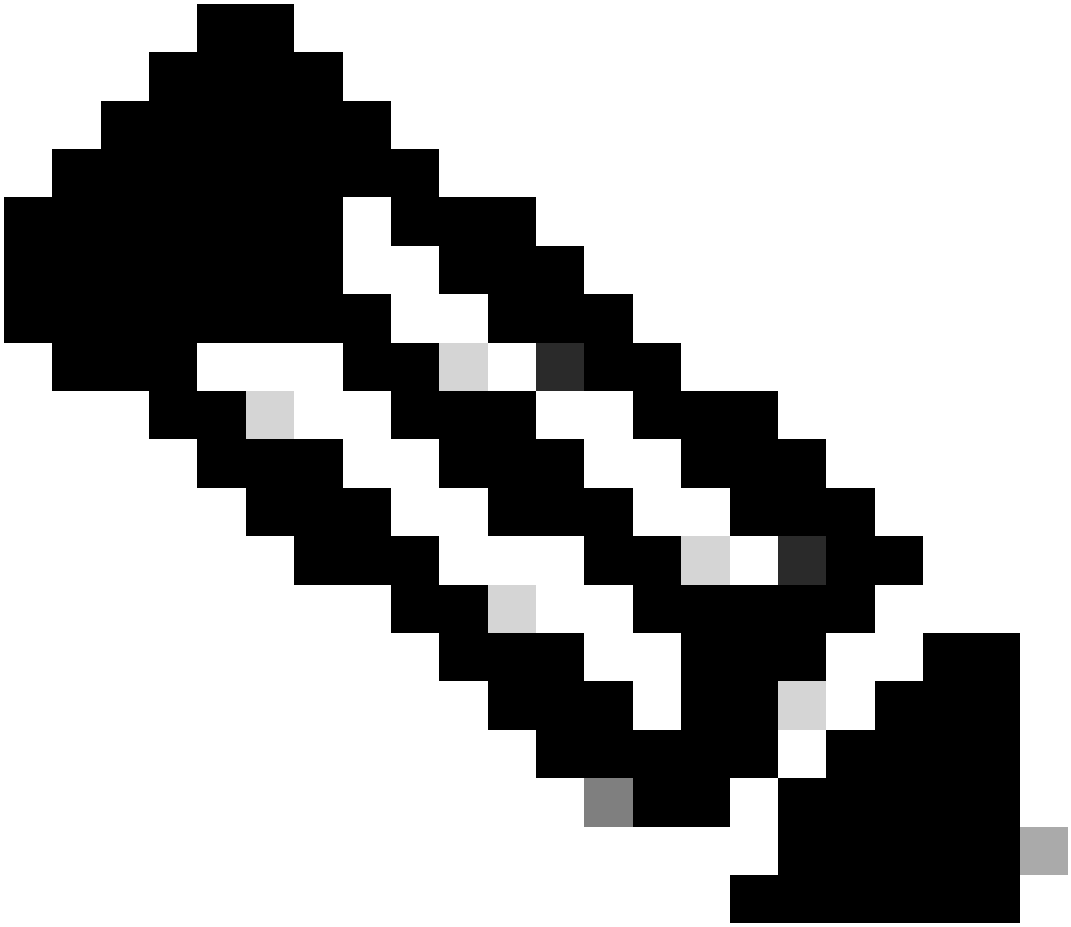
Output

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

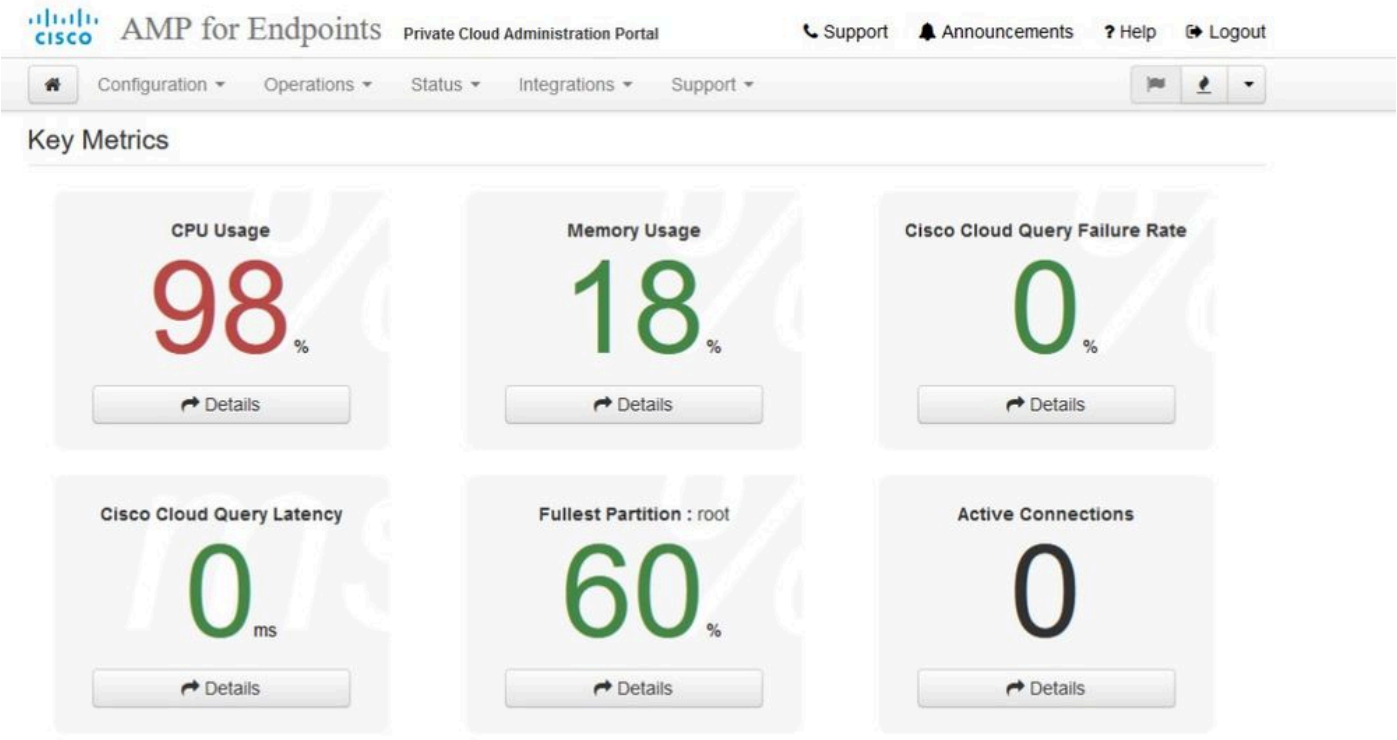
Download Output

⌃ ⌃ AIRGAP SOLAMENTE ⌃ ⌃

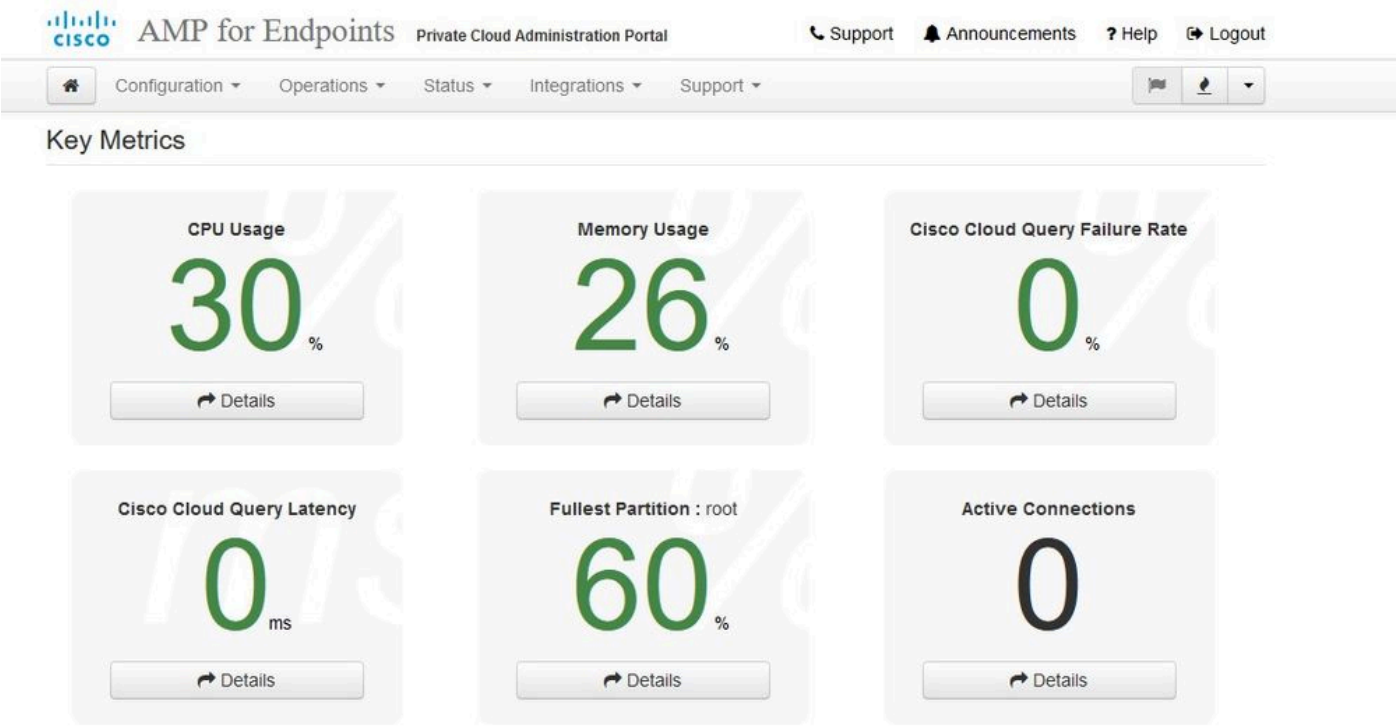


Nota: Estos pasos sólo son aplicables a los dispositivos físicos.

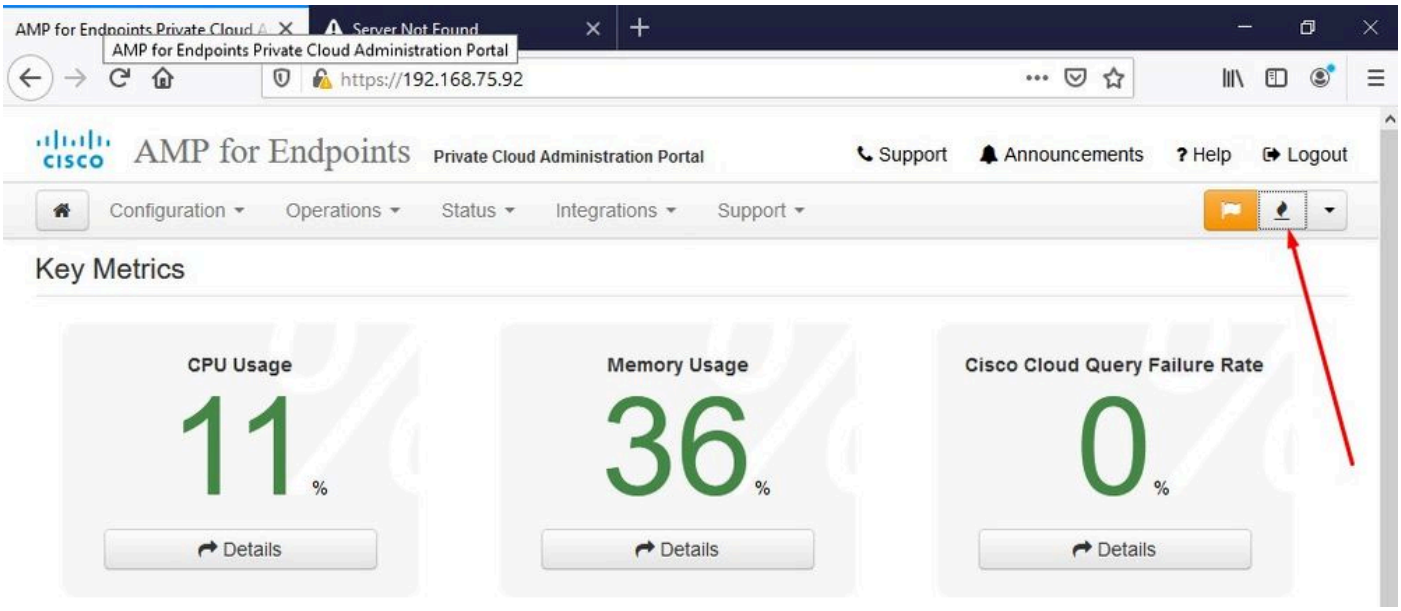
Una vez que el dispositivo se haya iniciado por completo, la próxima vez que inicie sesión con la interfaz de administración, se le mostrará este panel. Usted puede notar alto CPU al principio, pero si usted da unos minutos se asienta abajo.



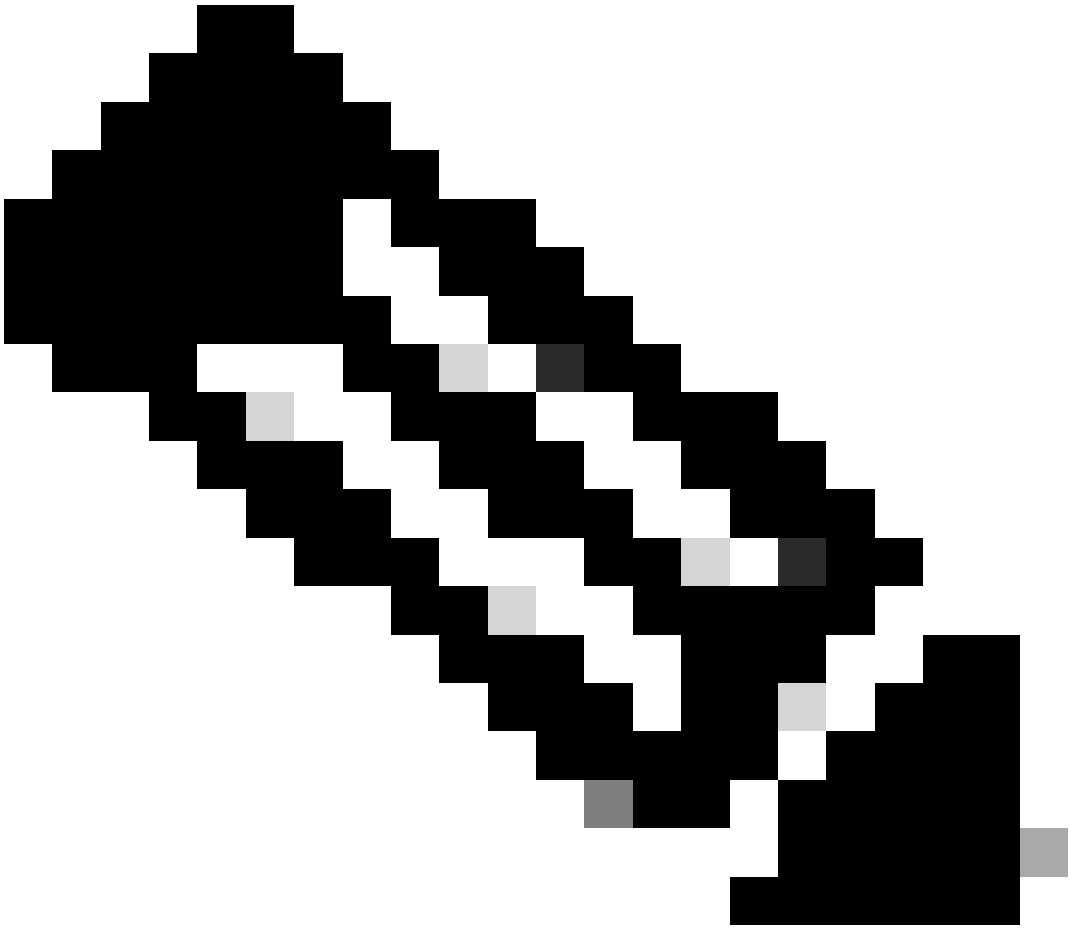
Después de unos minutos...



Desde aquí, acceda a la consola de Secure Endpoint. Haga clic en el pequeño icono que parece fuego en la esquina derecha junto a la bandera.

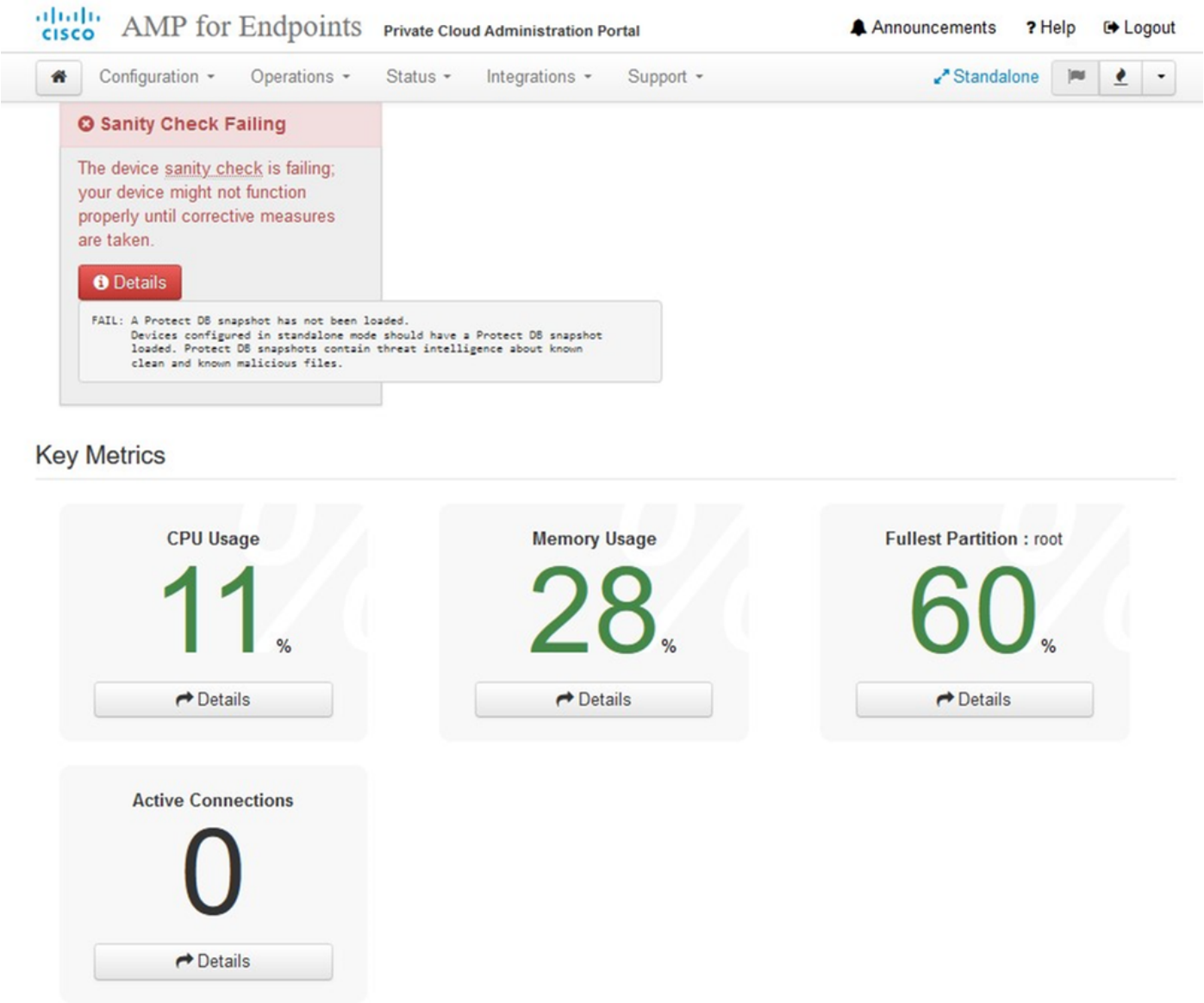

AMP for Endpoints Private Cloud
Server Not Found
AMP for Endpoints Private Cloud Administration Portal
https://192.168.75.92
AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Key Metrics
CPU Usage
11 %
Details
Memory Usage
36 %
Details
Cisco Cloud Query Failure Rate
0 %
Details

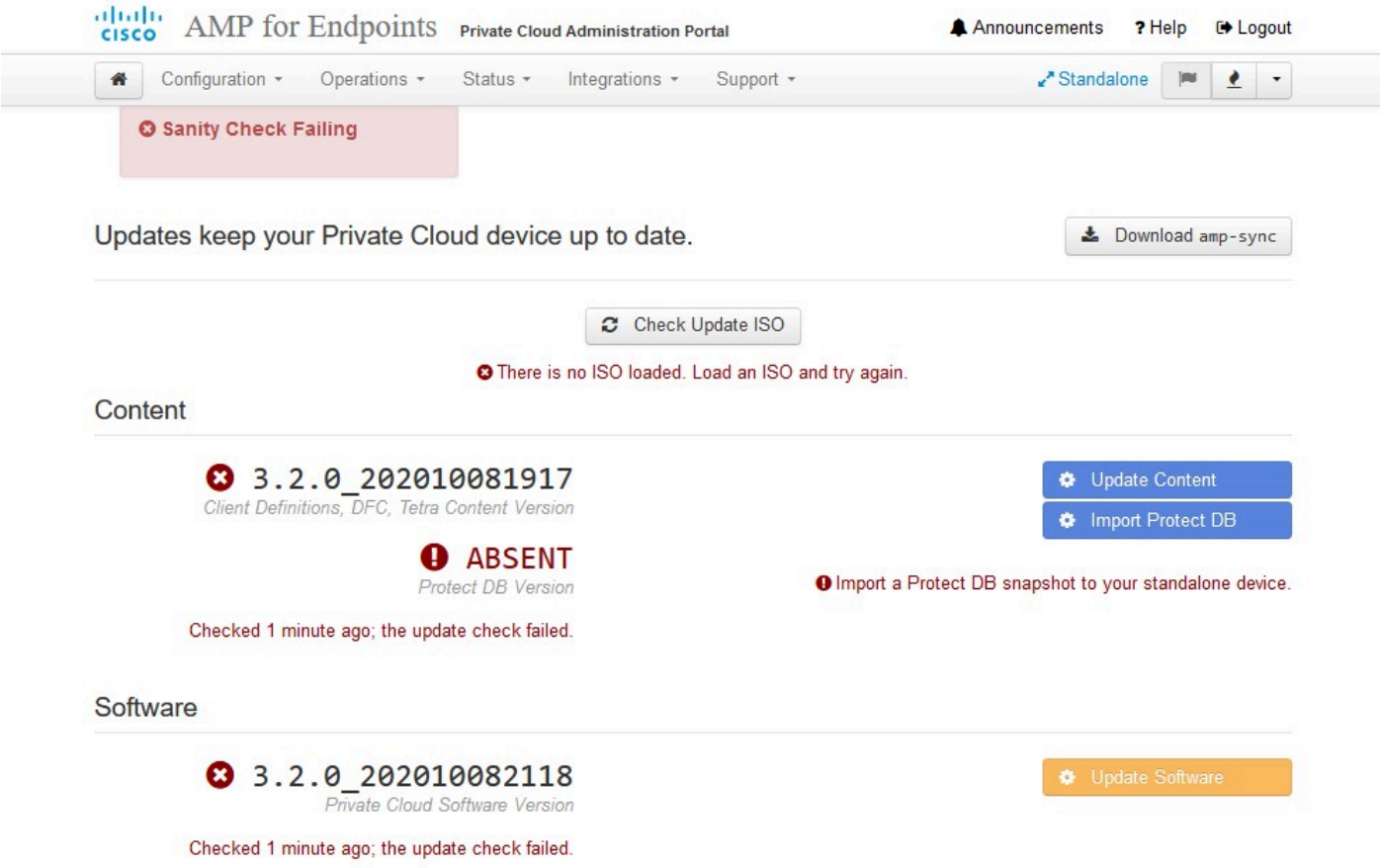
⩔ ⩔ SÓLO AIRGAP ⩔ ⩔



Nota: Estos pasos sólo son aplicables a los dispositivos físicos.

Como puede ver, fallamos en la comprobación de integridad debido a DB Protect Snapshot , también a las definiciones de cliente, DFC y Tetra. Esto se debe hacer mediante una actualización sin conexión a través del archivo ISO descargado previamente preparado a través de amp-sync y cargado en la ubicación NFS.





Paquete de actualización de AirGap

Por primera vez tenemos que utilizar este comando para recibir el Protect DB

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

Nota: Descargue todos los paquetes mediante este comando y, a continuación, verifique que puede tardar mucho tiempo. Depende de la velocidad y de la calidad del link. En mi caso, con fibra de 1 giga, todavía se tarda casi 25 horas en completarse. En parte, esto también se debe al hecho de que esta descarga es directamente desde AWS y, por lo tanto, se limita. Por último, tenga en cuenta que esta descarga es bastante grande. En mi caso el archivo descargado era de 323GB.

En este ejemplo hemos utilizado CygWin64

1. Descargue e instale la versión x64 de Cygwin.
2. Ejecute setup-x86_64.exe y siga el proceso de instalación para elegir todos los valores predeterminados.
3. Seleccione un espejo de descarga.

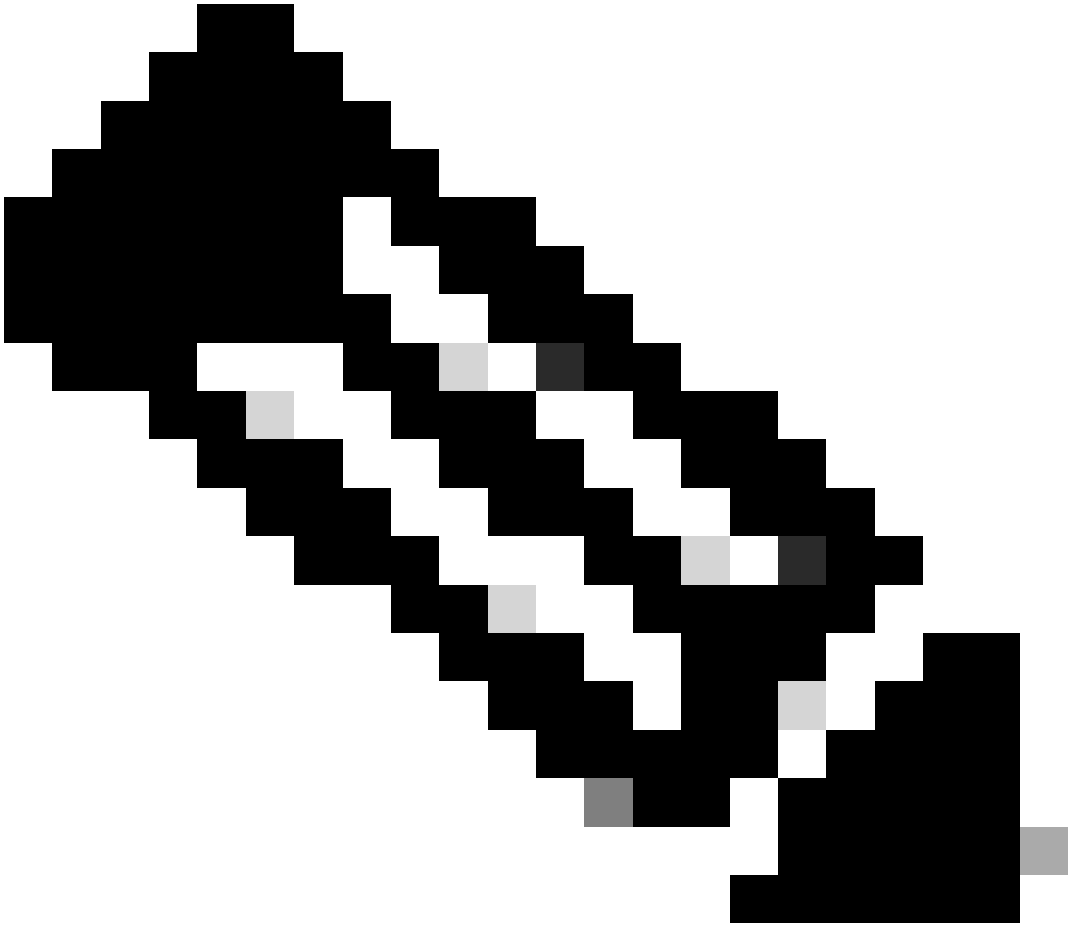
4. Seleccione los paquetes que desea instalar:
Todo -> Red -> rizo
Todos -> Utils -> genisoimage
Todos -> Utils -> xmlstarlet
* VPC 3.8.x up - > xorriso

```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2991  100  2991    0     0  15991      0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11331  100 11331    0     0  98544      0 --:--:-- --:--:-- --:--:--   97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  915k  100  915k    0     0  3324k      0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1094k  100 1094k    0     0  3302k      0 --:--:-- --:--:-- --:--:-- 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  135k  100  135k    0     0   747k      0 --:--:-- --:--:-- --:--:--  756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 54480  100 54480    0     0   383k      0 --:--:-- --:--:-- --:--:--  385k
```

```
 99.91% done, estimate finish Thu Nov  4 08:39:50 2021
 99.91% done, estimate finish Thu Nov  4 08:39:51 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:51 2021
 99.93% done, estimate finish Thu Nov  4 08:39:50 2021
 99.93% done, estimate finish Thu Nov  4 08:39:50 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: En la actualización más reciente VPC 3.8.x con CygWin64 como su principal herramienta de descarga se puede encontrar este problema descrito a continuación.

```
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 la versión Página #58. Como puede ver "xorriso" es ahora necesario. Cambiamos el formato de la ISO a la ISO 9660 y esa dependencia es lo que convierte la imagen al formato apropiado para que la actualización pueda completarse. Desafortunadamente, CygWin64 no ofrecen xorriso en ninguno de sus repositorios incorporados. Sin embargo, para aquellos que todavía les gustaría utilizar CygWin64 hay una manera 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.

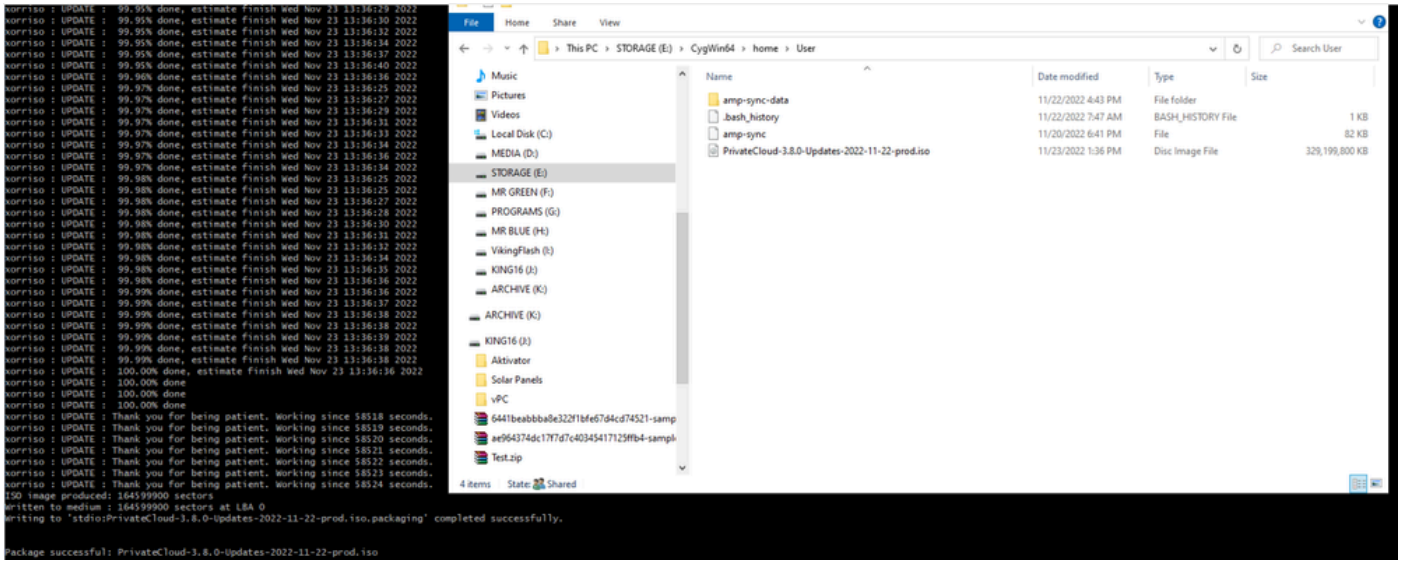
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

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 CygWin de nuevo, debe descargar manualmente xorriso desde el repositorio de GitHub. Abra su navegador y escriba <Latest xorriso.exe 1.5.2 pre-build for Windows> debe aparecer como el primer enlace llamado <PeyTy/xorriso-exe-for-windows - GitHub> navegue hasta esa página de GitHub y descargue el archivo <xorriso-exe-for-windows-master.zip> dentro del archivo zip que encuentra entre otros archivos llamados <xorriso.exe> copie y pegue este archivo en la ruta <CygWin64\bin> de la instalación local de CygWin. Vuelva a intentar ejecutar el comando <amp-sync>. Ya no debería ver el mensaje de error ni iniciar y finalizar la descarga, como se muestra en la imagen.

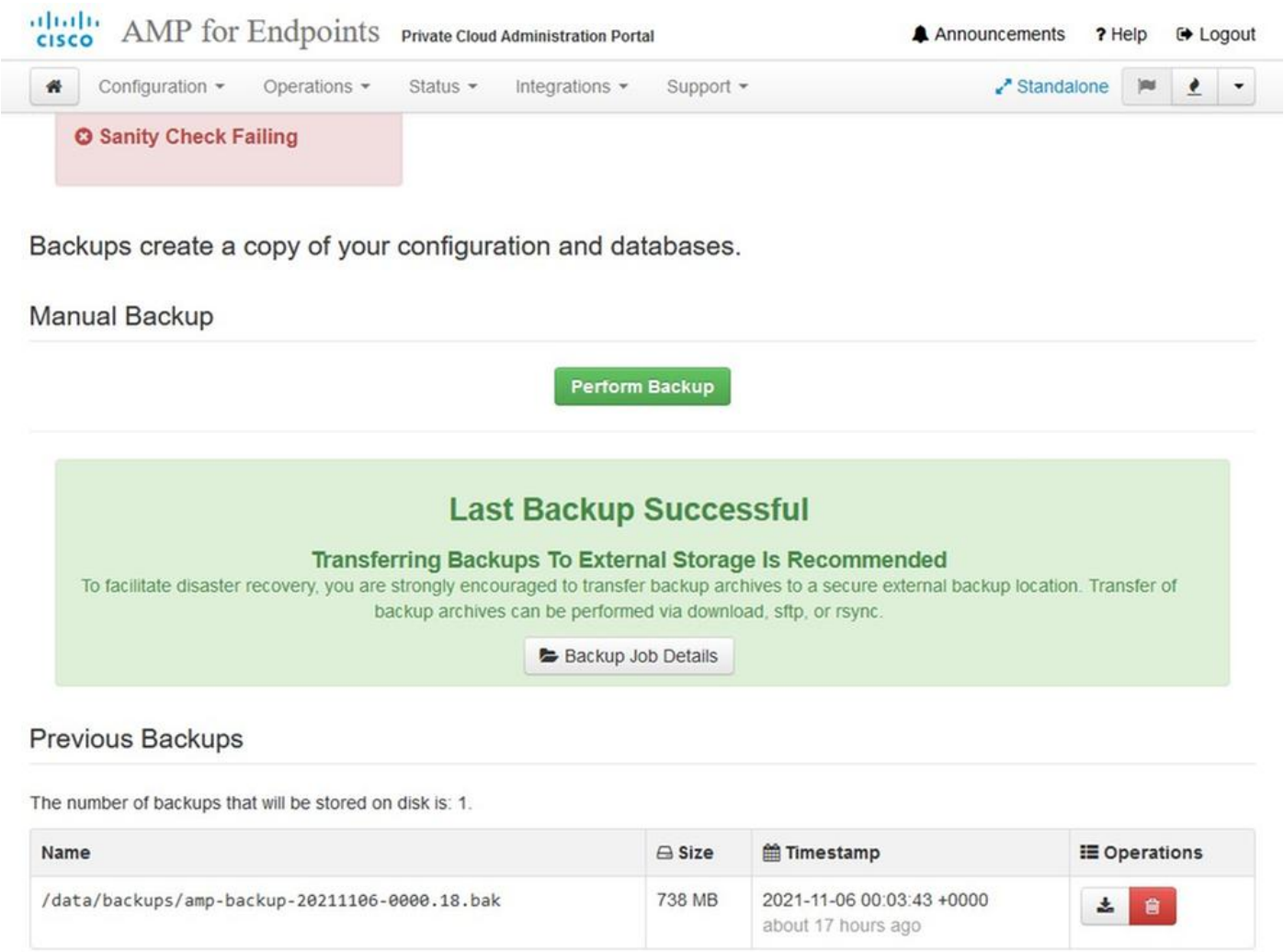


Realice la copia de respaldo de la VPC (en este caso) actual 3.2.0 en el modo Airgap.

Puede utilizar este comando desde la CLI

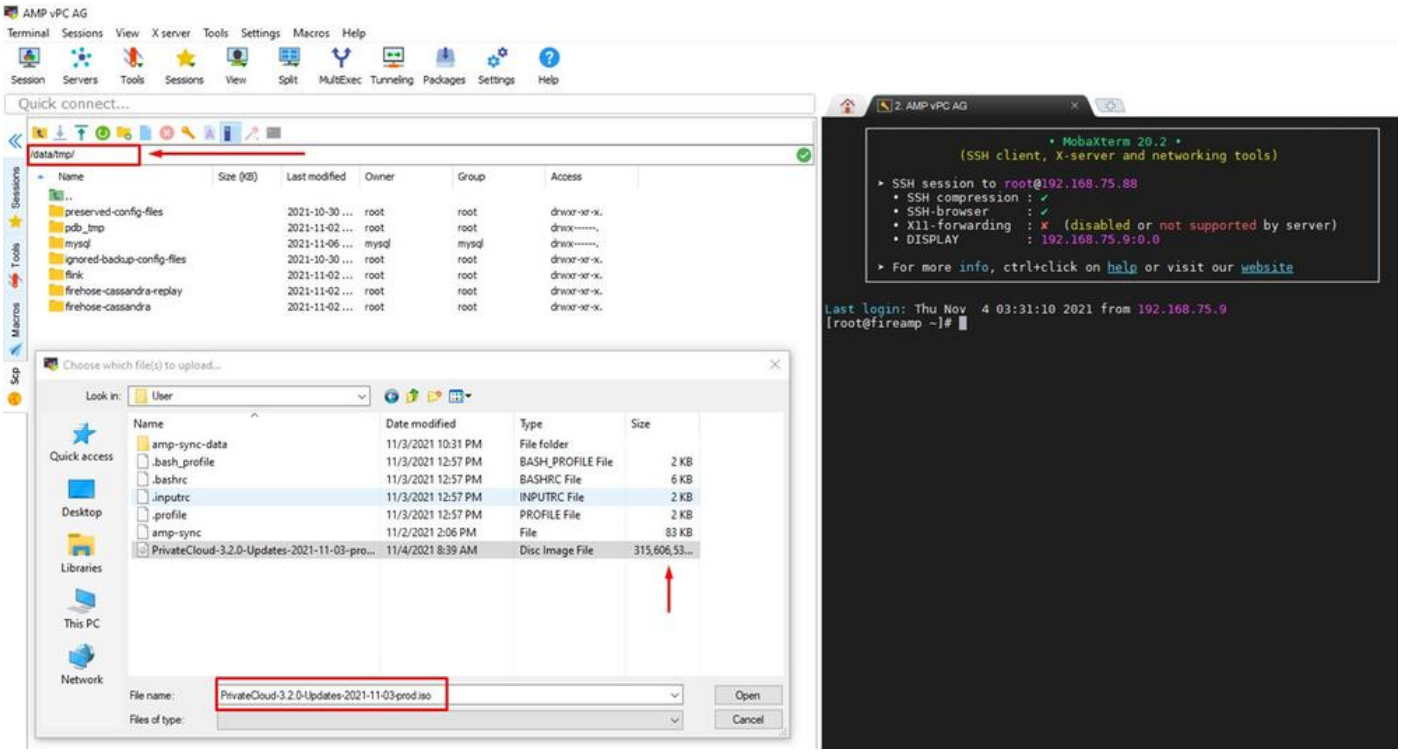
```
rpm -qa | grep Pri
```

O también puede navegar hasta Operaciones > Copias de seguridad, como se muestra en la imagen y Realizar copia de seguridad allí.



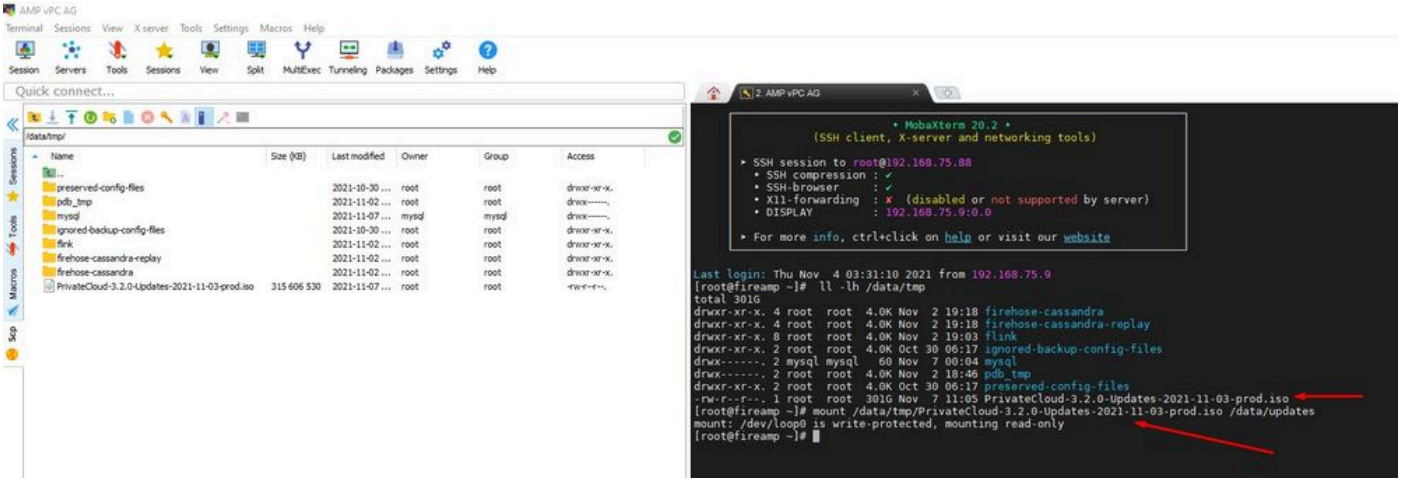
Transfiera el último ISO generado con amp-sync al VPC. Esto puede tardar hasta varias horas, así en función de su velocidad. En este caso la transferencia tomó más de 16Hrs

```
/data/tmp
```



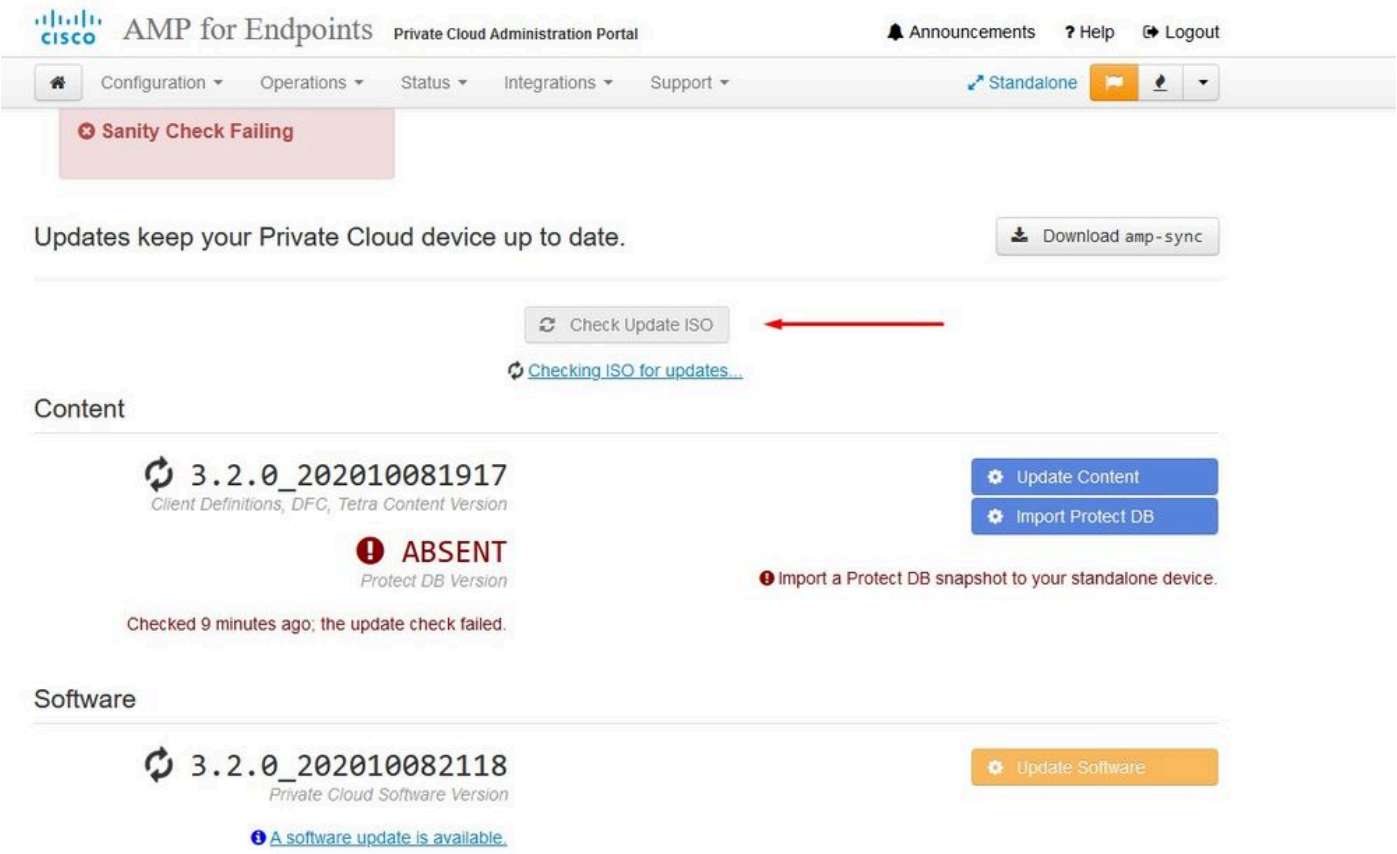
Una vez que se haya realizado la carga, monte el ISO

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

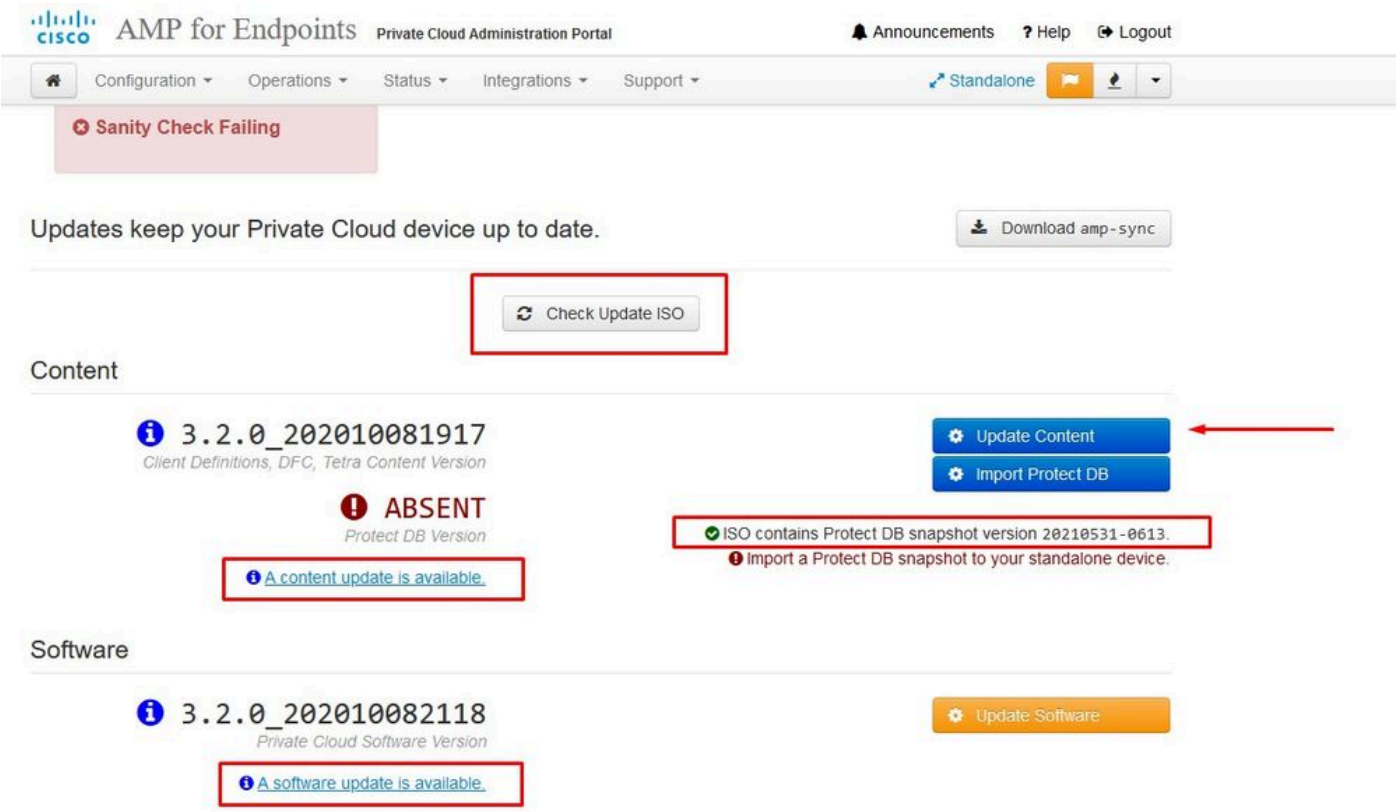


Vaya a la interfaz de usuario de opdamin para realizar la actualización Operations > Update

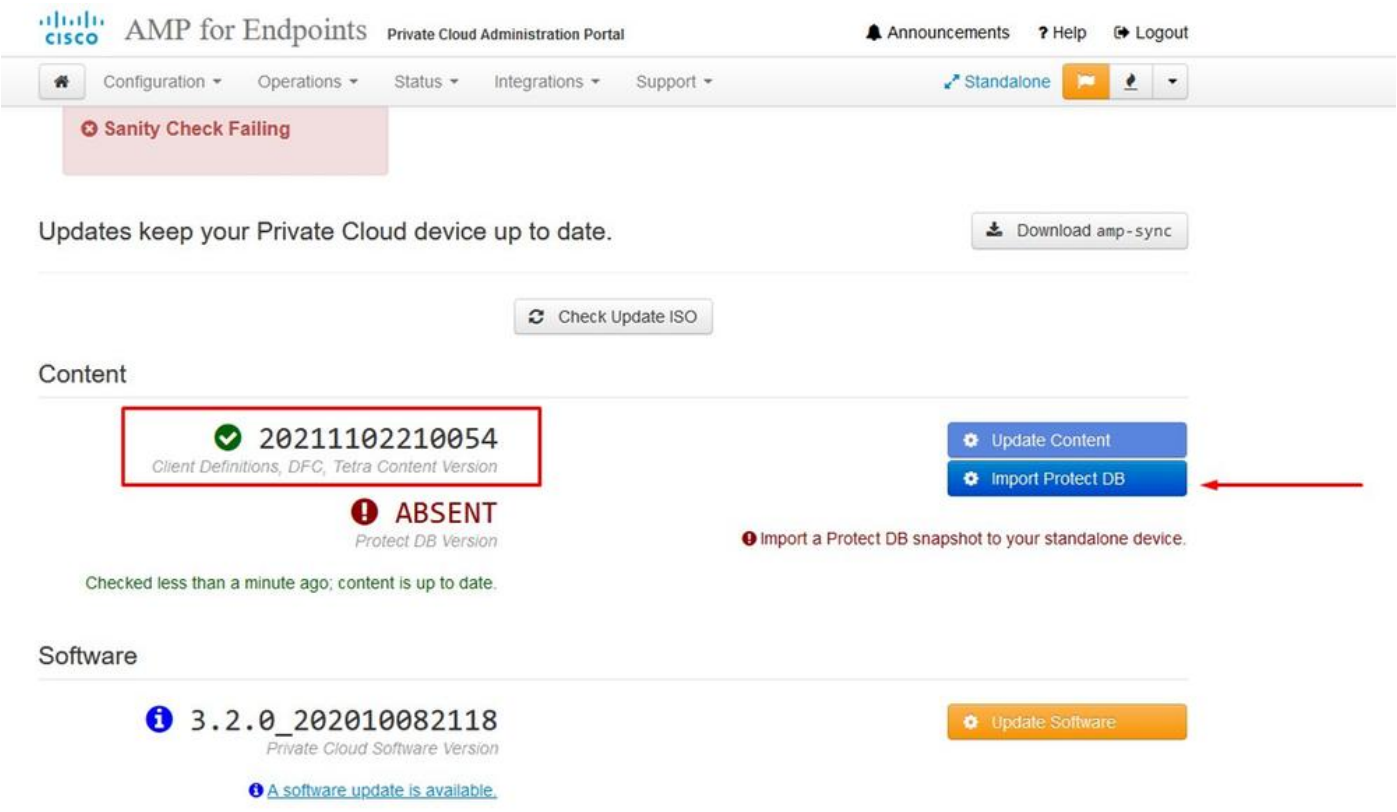
Device > Select Check update ISO.



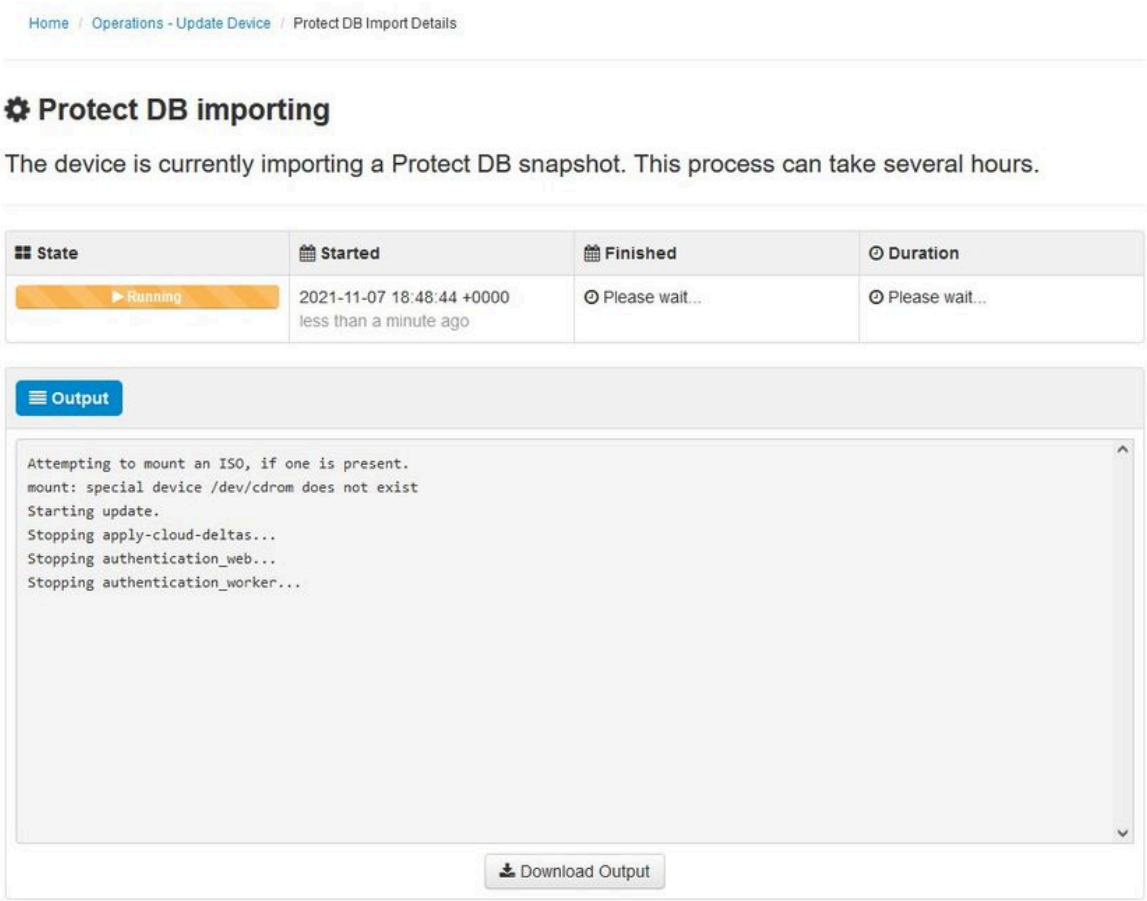
En este ejemplo, procedo con Update Content primero



A continuación, seleccione Importar proteger BD.



Como puede ver, este es otro proceso muy largo que puede tardar mucho tiempo en completarse.



Home / Operations - Update Device / Protect DB Import Details

Protect DB importing

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

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

Output

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

Download Output

Protect DB importing

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

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

Output

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

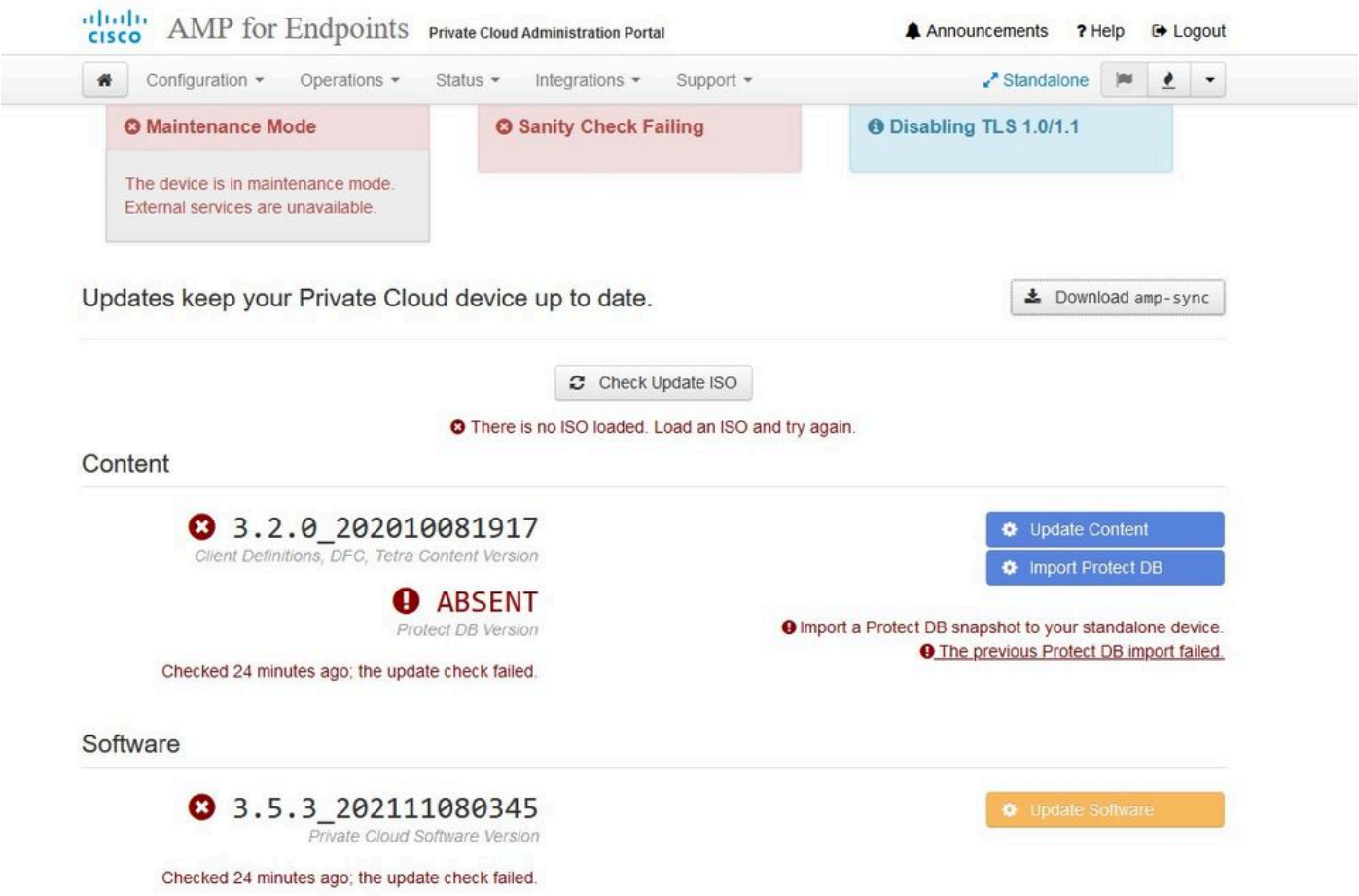
Problema #1: espacio agotado en el almacén de datos

Aquí puede ver dos números. Dado que vPC anterior a 3.5.2 no tiene la capacidad de montar almacenamiento NFS externo, debe cargar el archivo ISO de actualización en el directorio /data/temp. En mi caso, como mi almacén de datos tenía sólo 1 TB, me quedé sin la sala y la máquina virtual se bloqueó. En otras palabras, necesita al menos 2 TB de espacio en su almacén de datos para implementar correctamente AirGap VPC que está por debajo de la versión 3.5.2

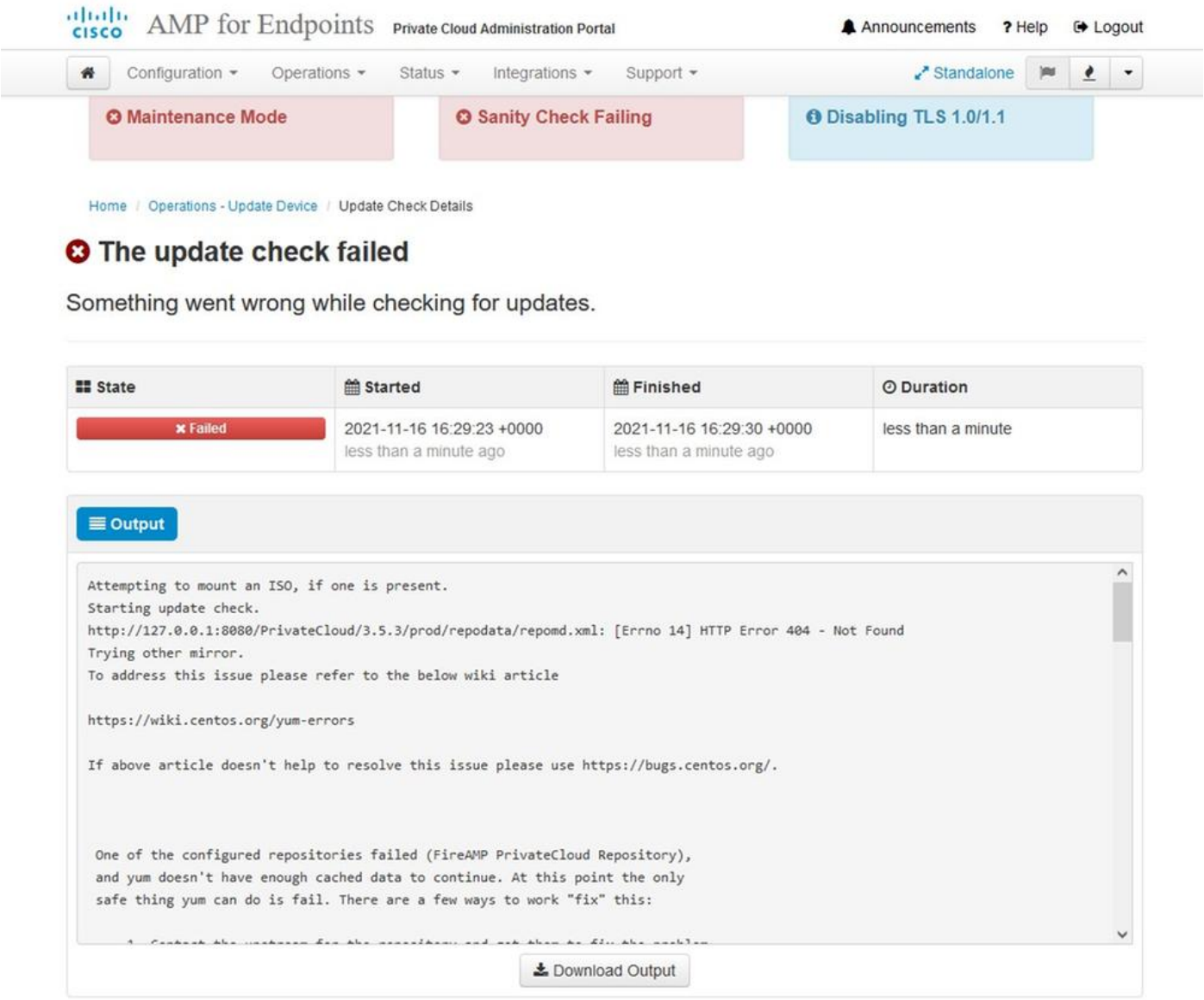
Esta imagen de abajo es del servidor ESXi que muestra el error de que no hay más espacio disponible en el disco duro cuando intenta arrancar la VM. Pude recuperarme de este error cambiando temporalmente la RAM de 128 GB a 64 GB. Entonces fui capaz de arrancar de nuevo. También recuerde que si aprovisiona esta VM como cliente ligero, el inconveniente de la implementación de cliente ligero es que el tamaño del disco puede aumentar, pero no se reduciría incluso si libera algo de espacio. En otras palabras, supongamos que ha cargado el archivo de 300 GB en el directorio del vPC y, a continuación, lo ha eliminado. El disco de ESXi todavía muestra 300 GB menos de espacio en el disco duro

Problema #2: actualización anterior

El problema 2nd es si se ejecuta la actualización de software primero como lo hice en mi 2° prueba y de 3.2.0 termino con VPC para actualizar a 3.5.2 y debido a eso tuve que descargar el nuevo archivo de actualización de ISO ya que el 3.2.0 se vuelven inválidos debido a un hecho de que ya no estaba en la versión 3.2.0 original.



Este es el error que aparece si intenta montar el archivo de actualización ISO de nuevo.



Esta imagen muestra una forma alternativa de montar la imagen de actualización en su VPC. En la versión 3.5.x puede utilizar la ubicación remota, como el almacenamiento NFS, para compartir el archivo de actualización con su VPC.

AMP for Endpoints Private Cloud Administration Portal

Announcements ? Help Logout

Configuration Operations Status Integrations Support Standalone

Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Mount an Update ISO

ISO Configuration HELP

Mount Type	ISO

ISO
NFS4
NFS3

Mount Status

No ISO mounted

AMP for Endpoints Private Cloud Administration Portal

Announcements ? Help Logout

Configuration Operations Status Integrations Support Standalone

Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

Mount an Update ISO

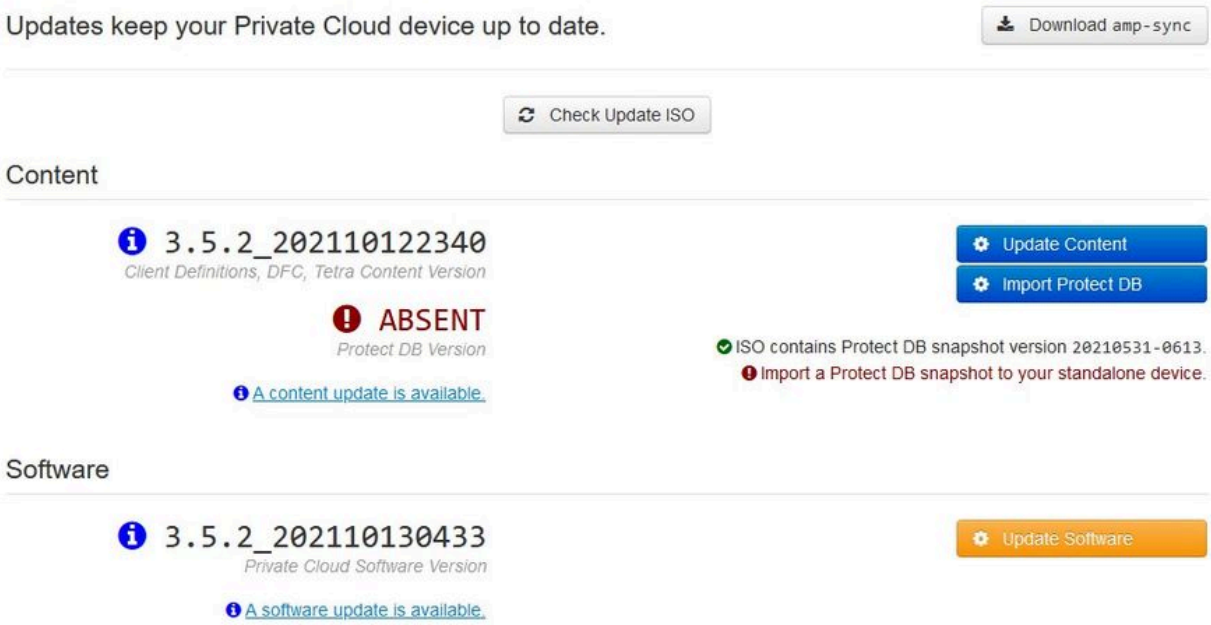
ISO Configuration HELP

Mount Type	NFS3
Remote Share	192.168.75.4:/AMPAG
Remote ISO File	PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

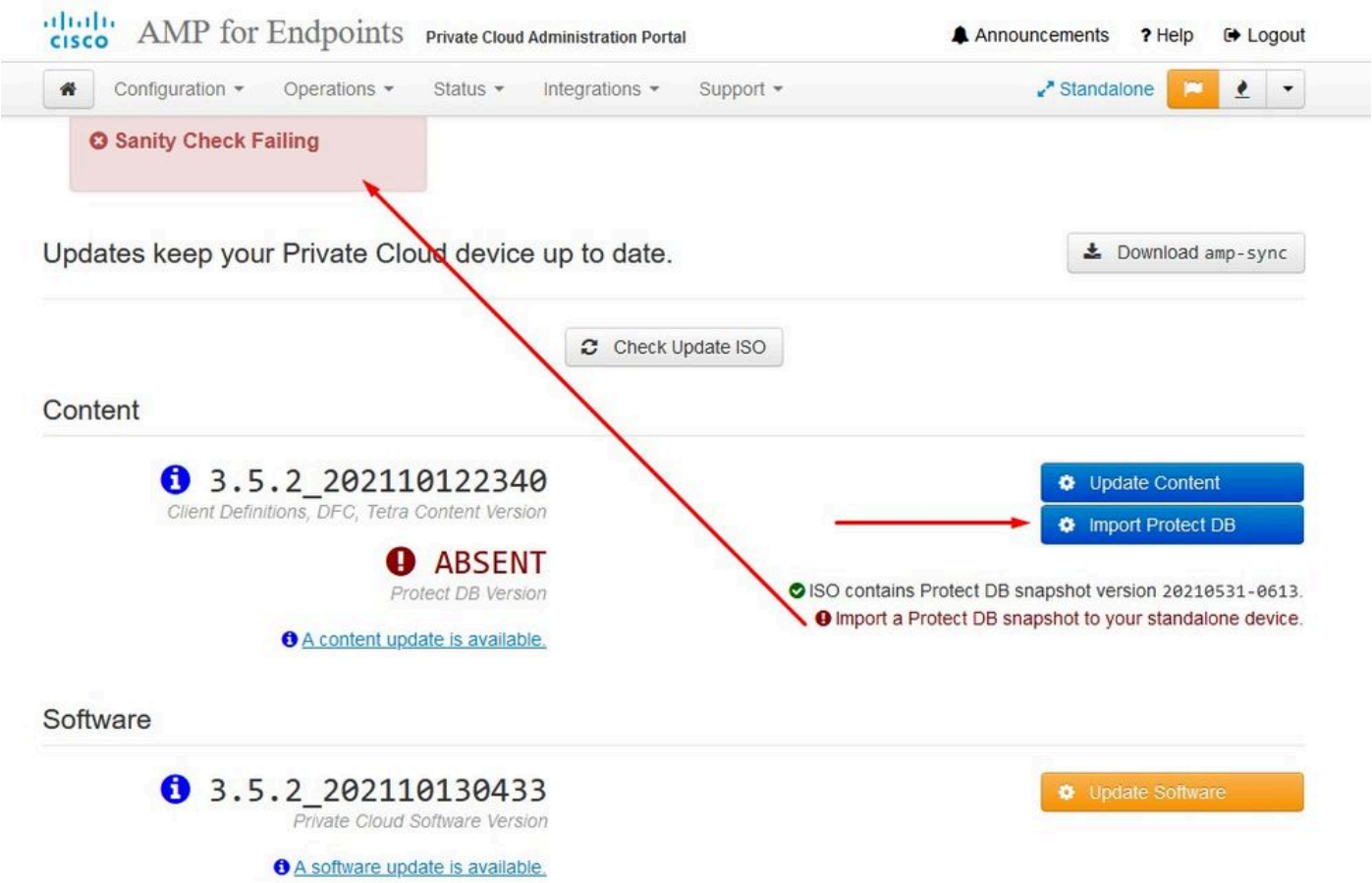
Mount

Mount Status

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



La falla de comprobación de integridad está relacionada con la protección de BD que no está disponible actualmente en el VPC



Protect DB importing

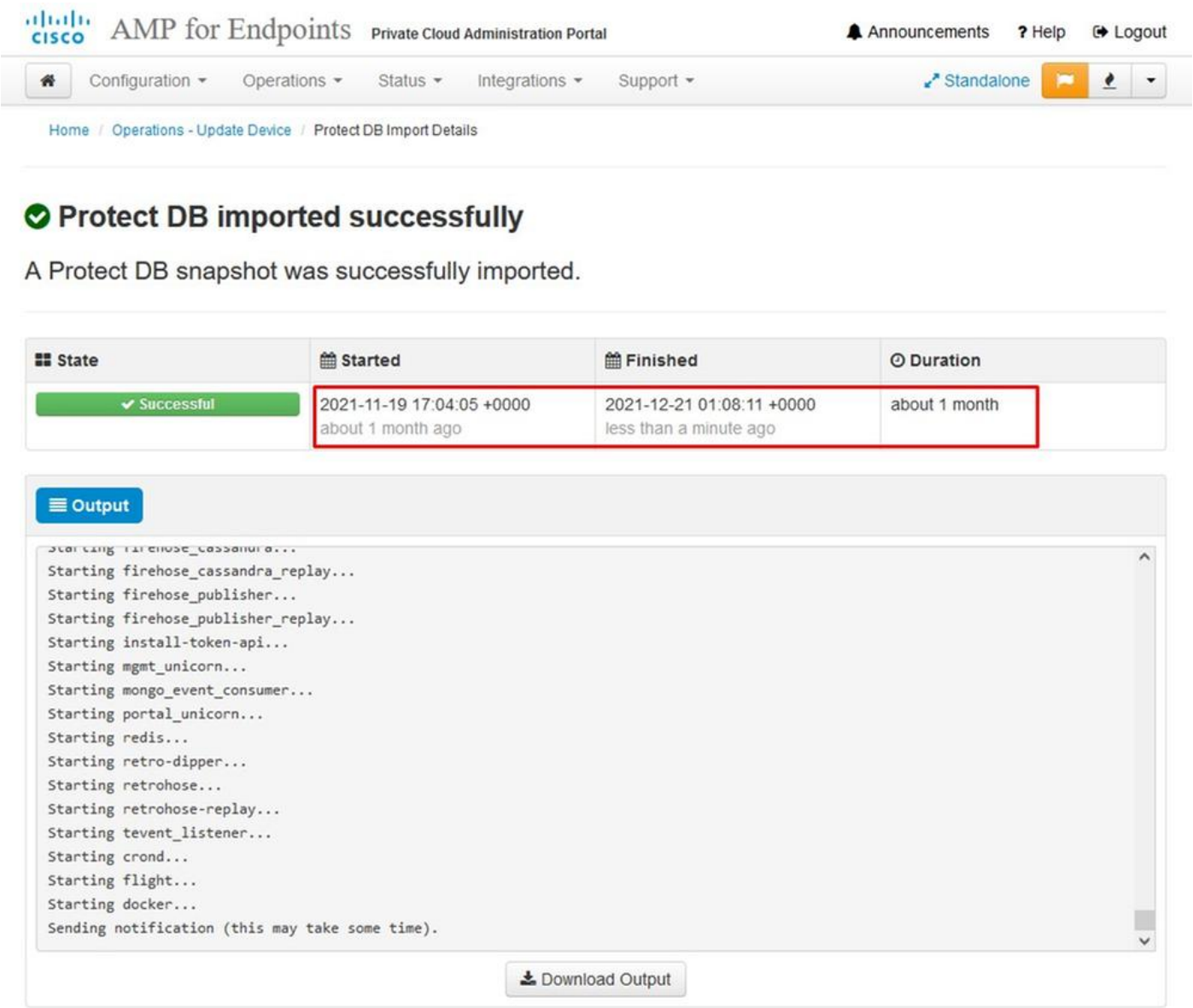
The device is currently importing a Protect DB snapshot. This process can take several hours.

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

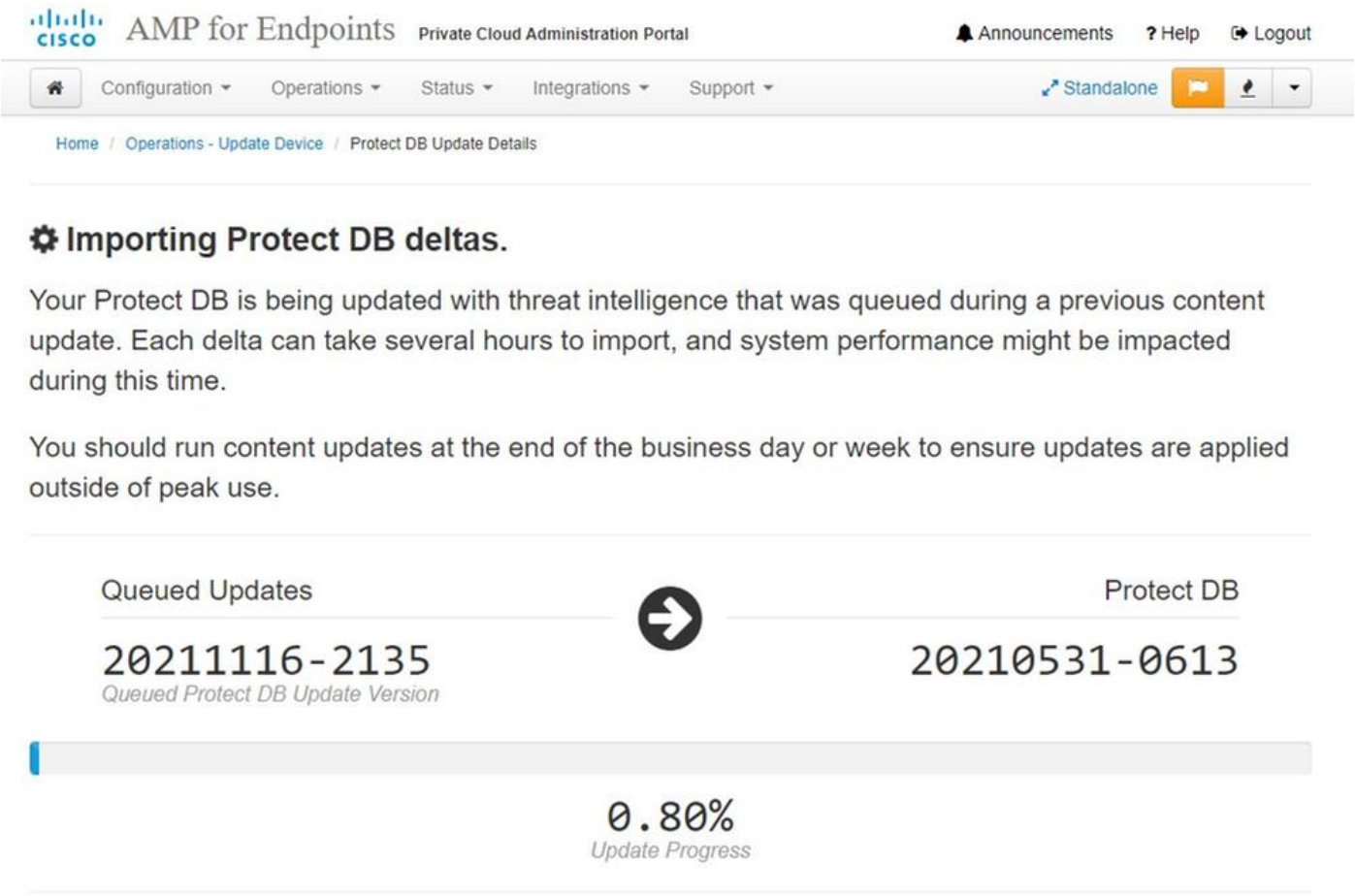
Output

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

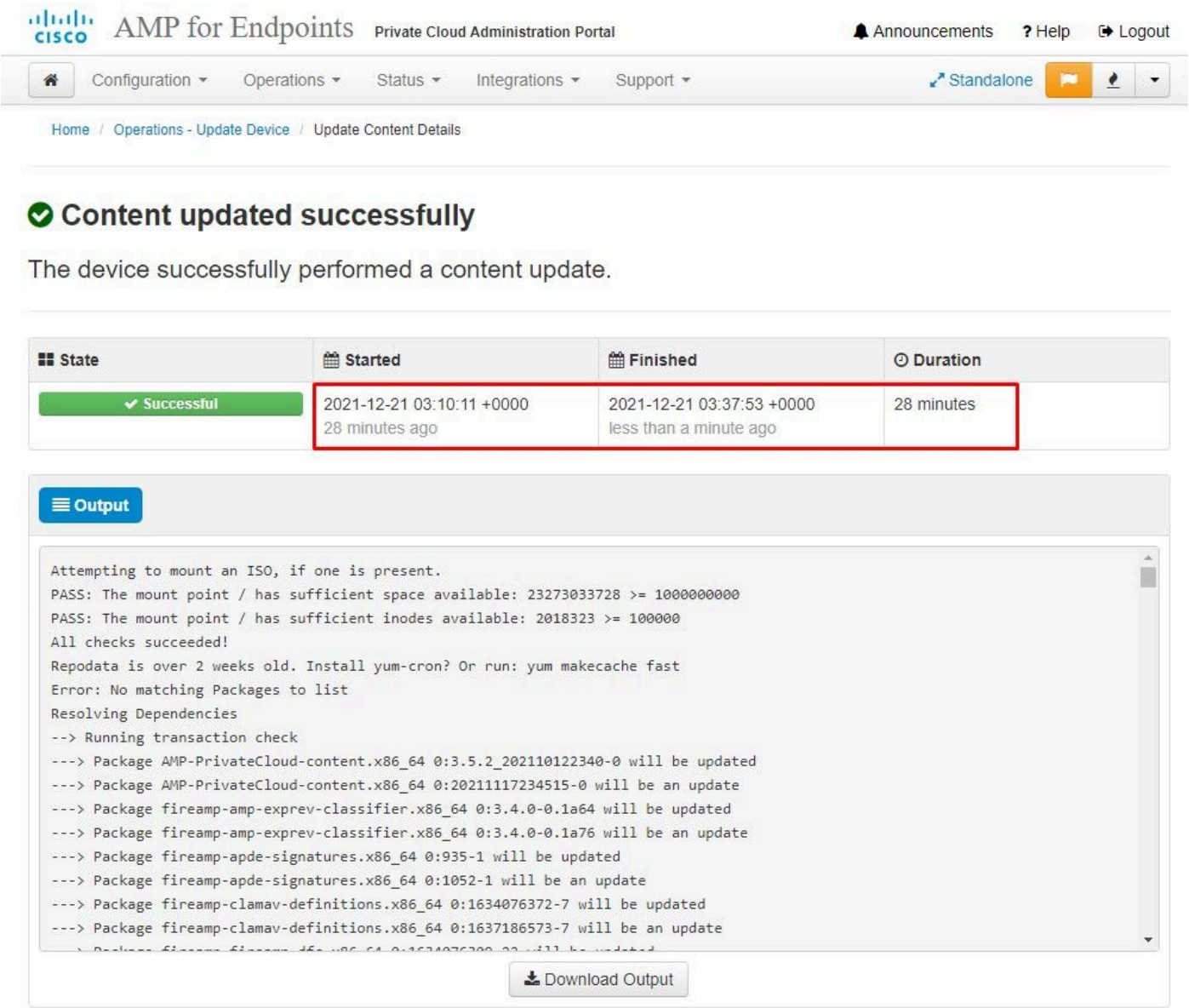
Download Output



La siguiente actualización se inicia automáticamente



Después de este proceso muy largo de la importación de la base de datos Protect DB puede mover y actualizar la definición del cliente y el software que aproximadamente puede tomar más de 3 horas adicionales.



Y finalmente hecho, por favor tenga en cuenta que este proceso tomará mucho tiempo.

Para el dispositivo VPC visite esta TZ que contiene otros métodos de cómo actualizar el dispositivo HW, montar el archivo ISO y arrancar desde USB.

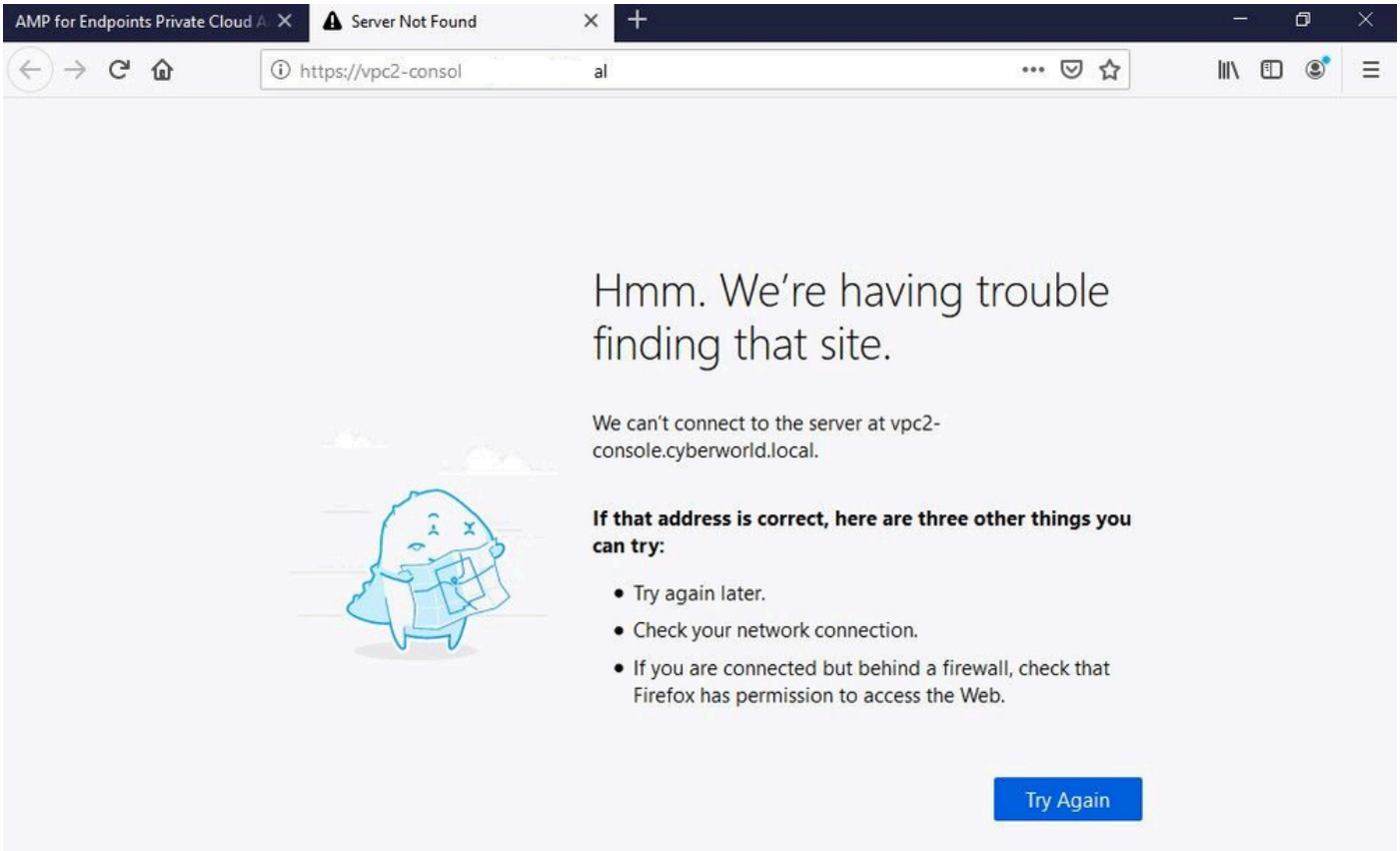
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

⌃ ⌃ AIRGAP SOLAMENTE ⌃ ⌃

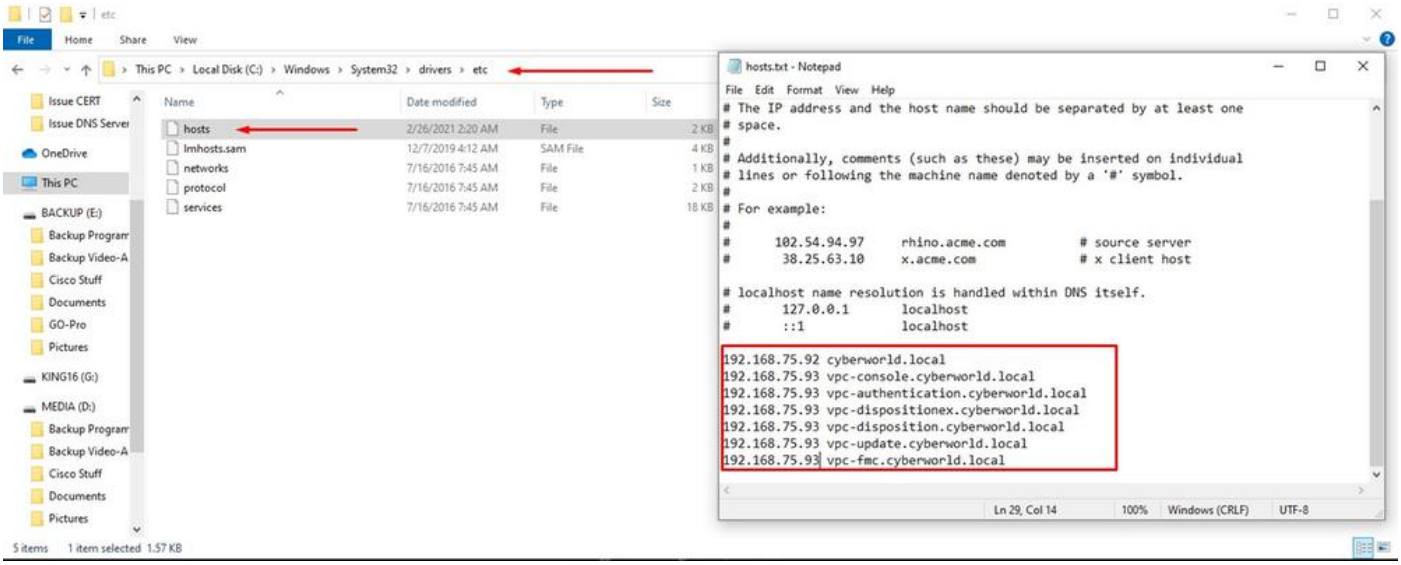
Resolución de problemas básicos

Problema #1: FQDN y servidor DNS

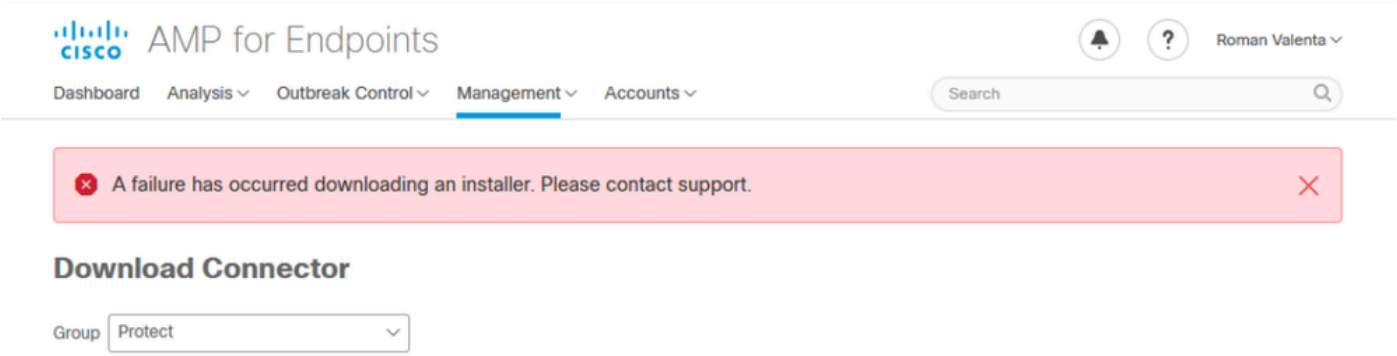
El primer problema que puede encontrar es si su servidor DNS no está establecido y todos los FQDN no están correctamente registrados y resueltos. El problema podría verse así cuando intente navegar a la consola de Secure Endpoint a través del icono "fire" de Secure Endpoint. Si sólo utiliza una dirección IP, funcionará, pero no podrá descargar el conector. Como puede ver en la 3ª imagen a continuación.



Si modifica el archivo HOSTS en su máquina local como se muestra en la imagen, resuelva el problema y terminará con errores.



Recibe este error mientras intenta descargar el instalador de Secure Endpoint Connector.



Después de solucionar algunos problemas, la única solución correcta era configurar el 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
```

Una vez que registre todos los FQDN en su servidor DNS y cambie el registro en la nube privada virtual de DNS público a su servidor DNS, todo comenzará a funcionar como se supone que debe hacerlo.

AMP for Endpoints Private Cloud Administration Portal

Support | Announcements | Help | Logout

Configuration | Operations | Status | Integrations | Support

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

Con ... network settings.

Adm ... **eth0** / 00:0C:29:A6:4A:11

IP Assignment 192.168.75.92

More details

Inter ... **eth1** / 00:0C:29:A6:4A:1B

IP Assignment 192.168.75.93

More details

IP Assignment Static

IP Address 192.168.75.93

☑ Check for IP Address conflicts

Subnet Mask 255.255.255.0

Gateway 192.168.75.1

Warning: Address and Hostname Changes

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

View the Configuration help page for a list of affected services.

DNS

Primary DNS Server 192.168.75.4

AMP for Endpoints Private Cloud Administration Portal

Support | Announcements | Help | Logout

Configuration | Operations | Status | Integrations | Support

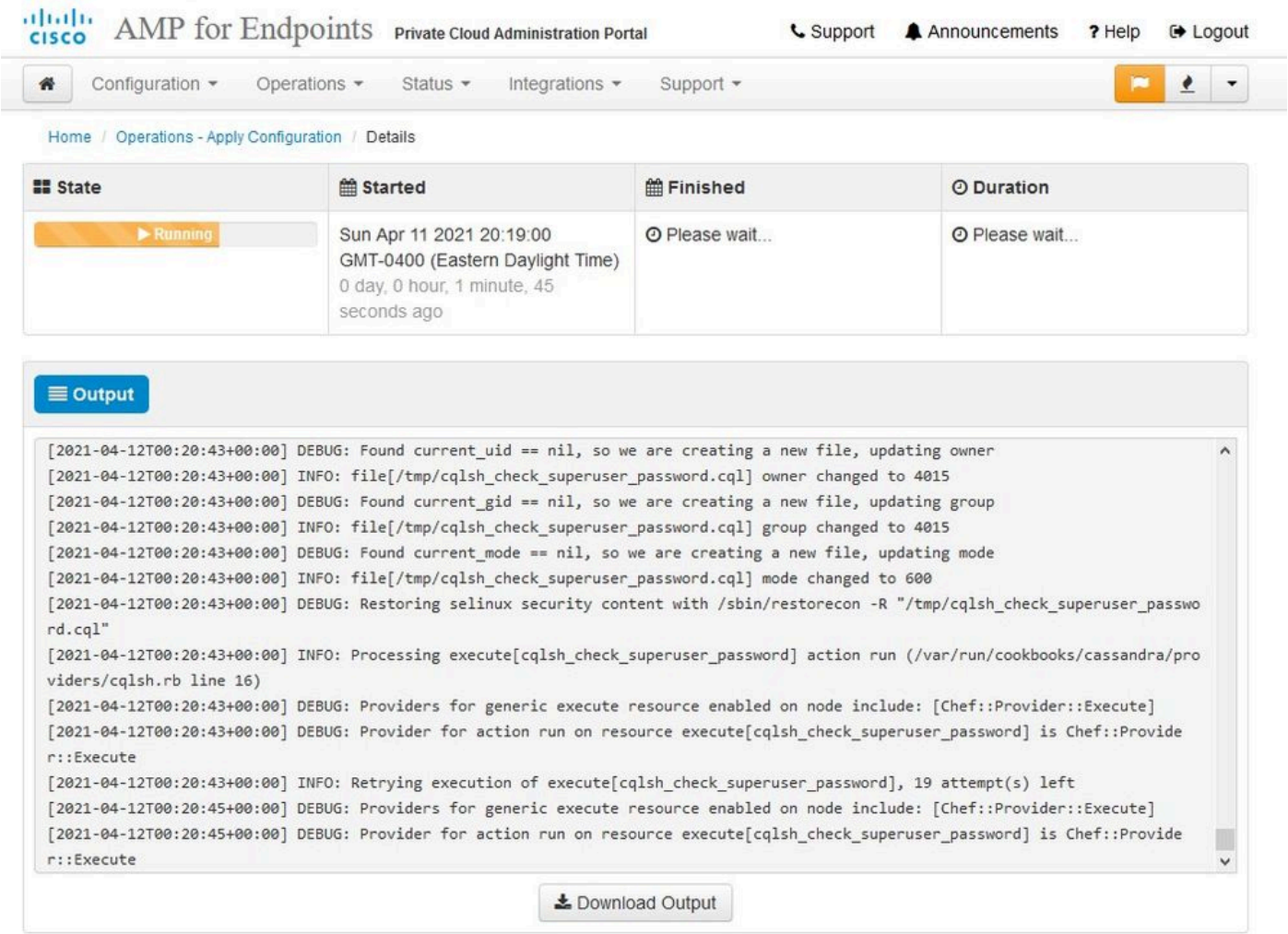
Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

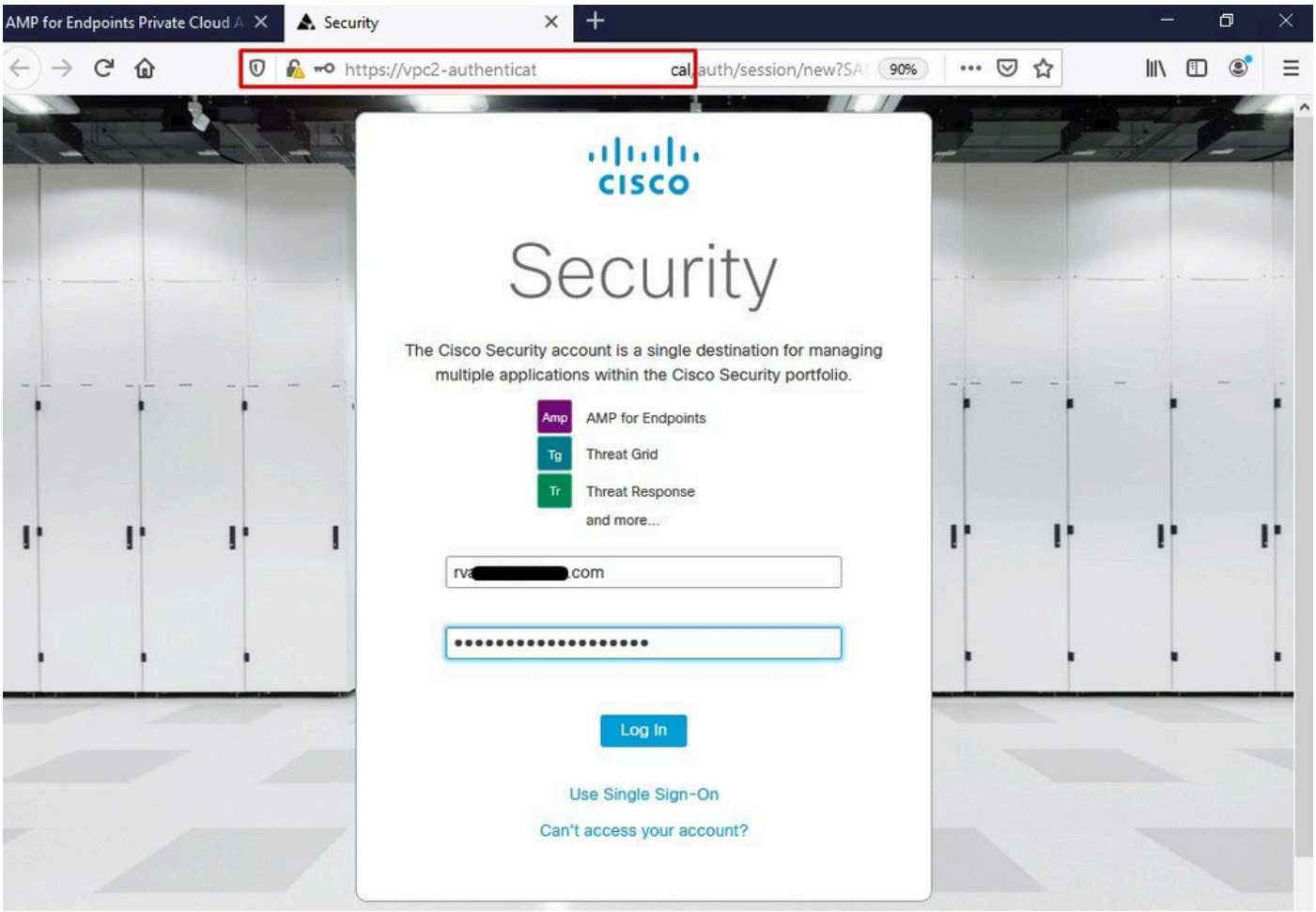
Reconfigure Now

Reconfiguration

Configuration saved.

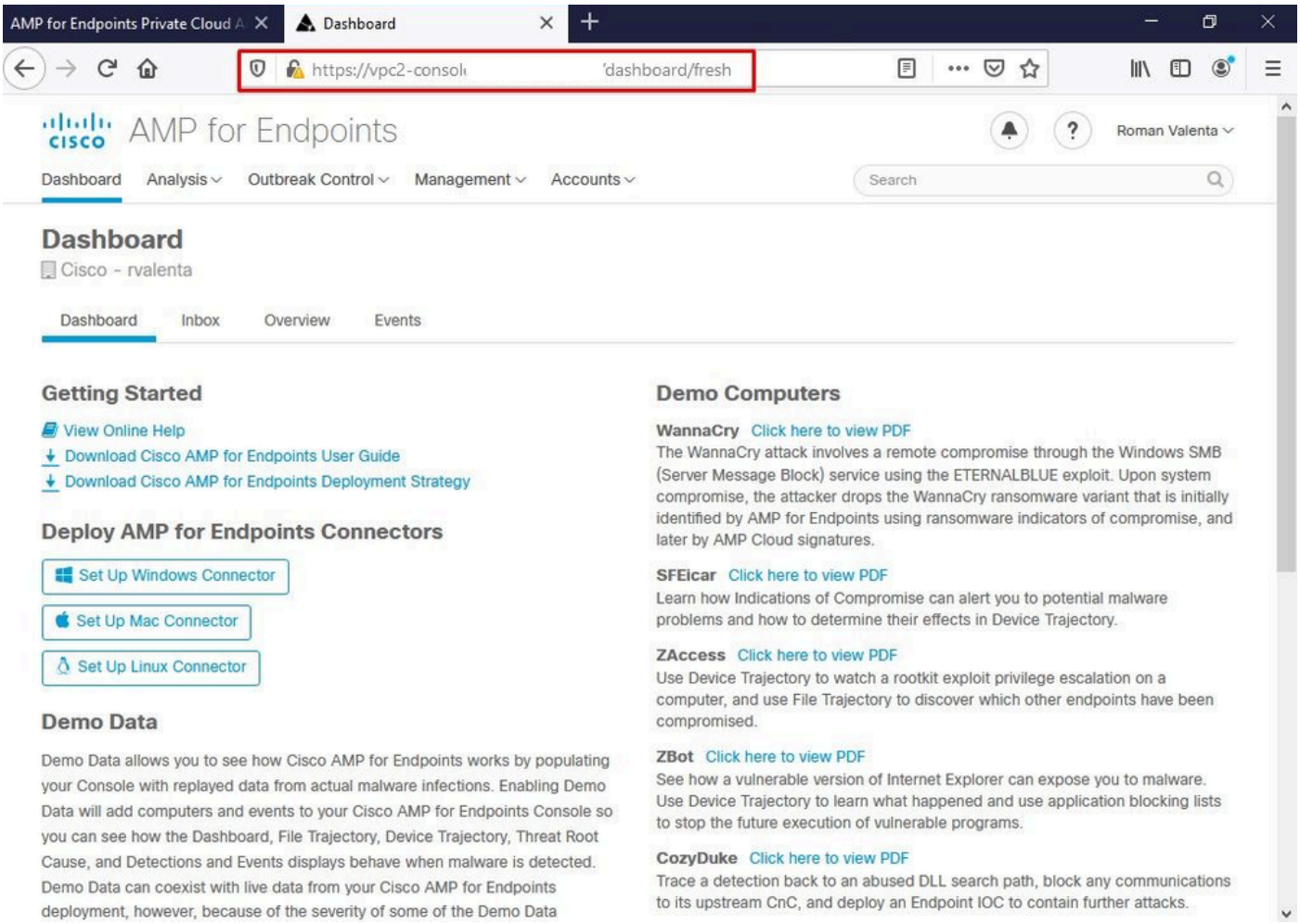


En este momento podrá iniciar sesión y descargar el conector

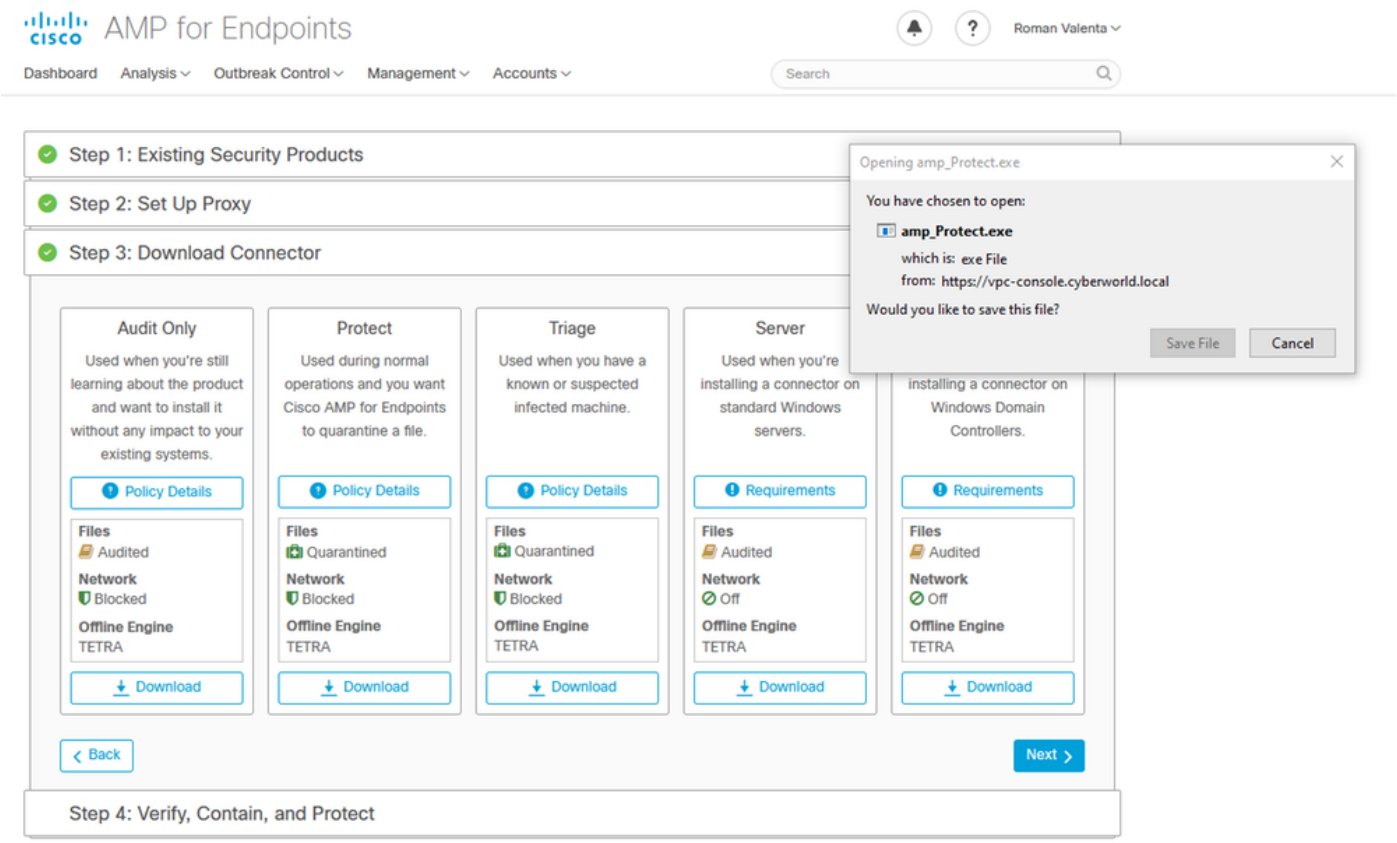


Se obtiene el asistente de política de Secure Endpoint inicial para su entorno. Le guía por la selección del producto antivirus que utiliza, si lo hubiera, así como del proxy y los tipos de políticas que desea implementar. Seleccione el botón Configurar... adecuado en función del sistema operativo del conector.

Aparece la página Productos de seguridad existentes, como se muestra en la imagen. Elija los productos de seguridad que utiliza. Genera automáticamente las exclusiones aplicables para evitar problemas de rendimiento en los terminales. Seleccione en Siguiente.

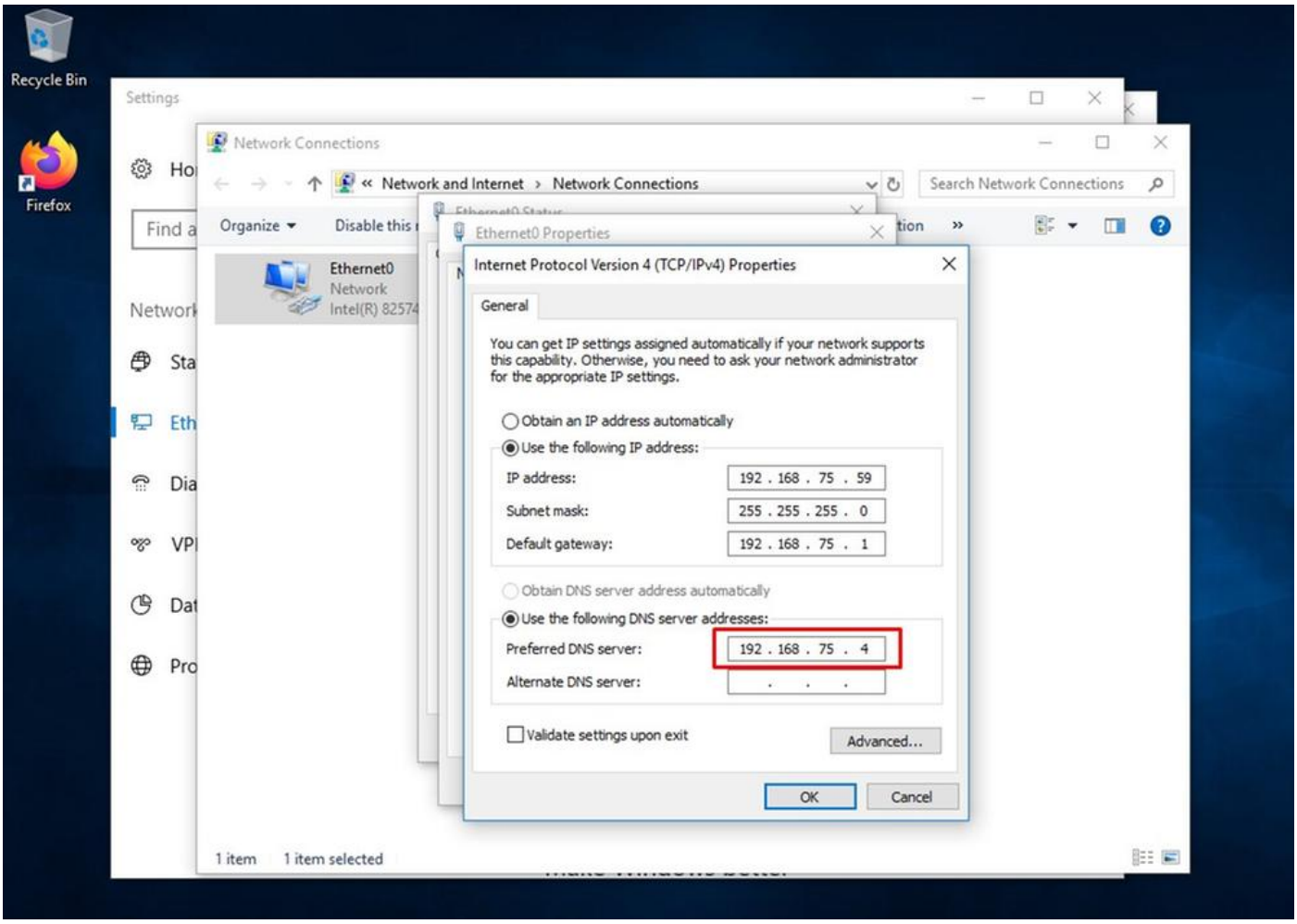


Descargar conector.

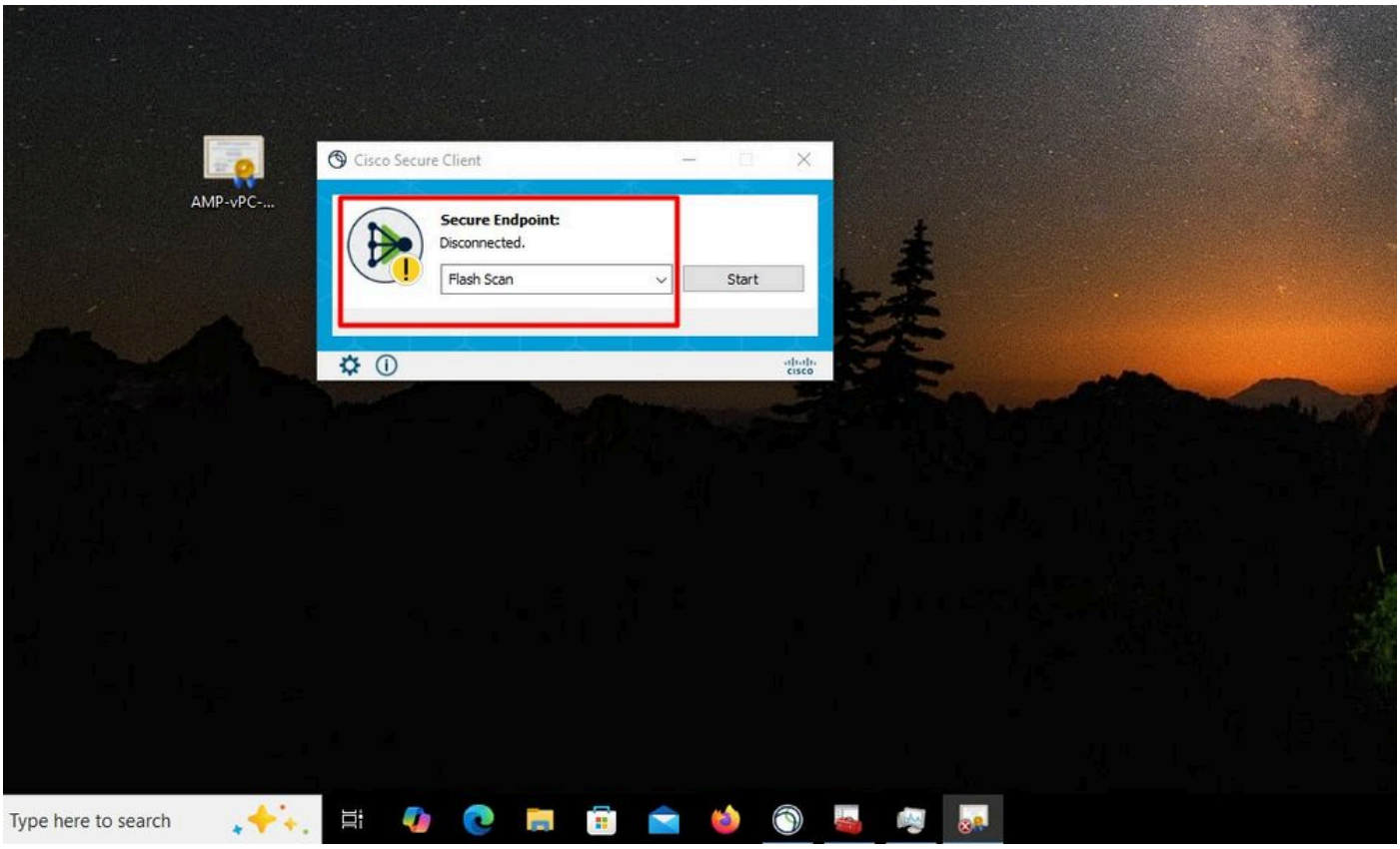


Problema #2 - Problema con la CA raíz

El siguiente problema al que puede enfrentarse es que si utiliza sus propios certificados internos es que después de la instalación inicial, el conector puede mostrarse como desconectado.



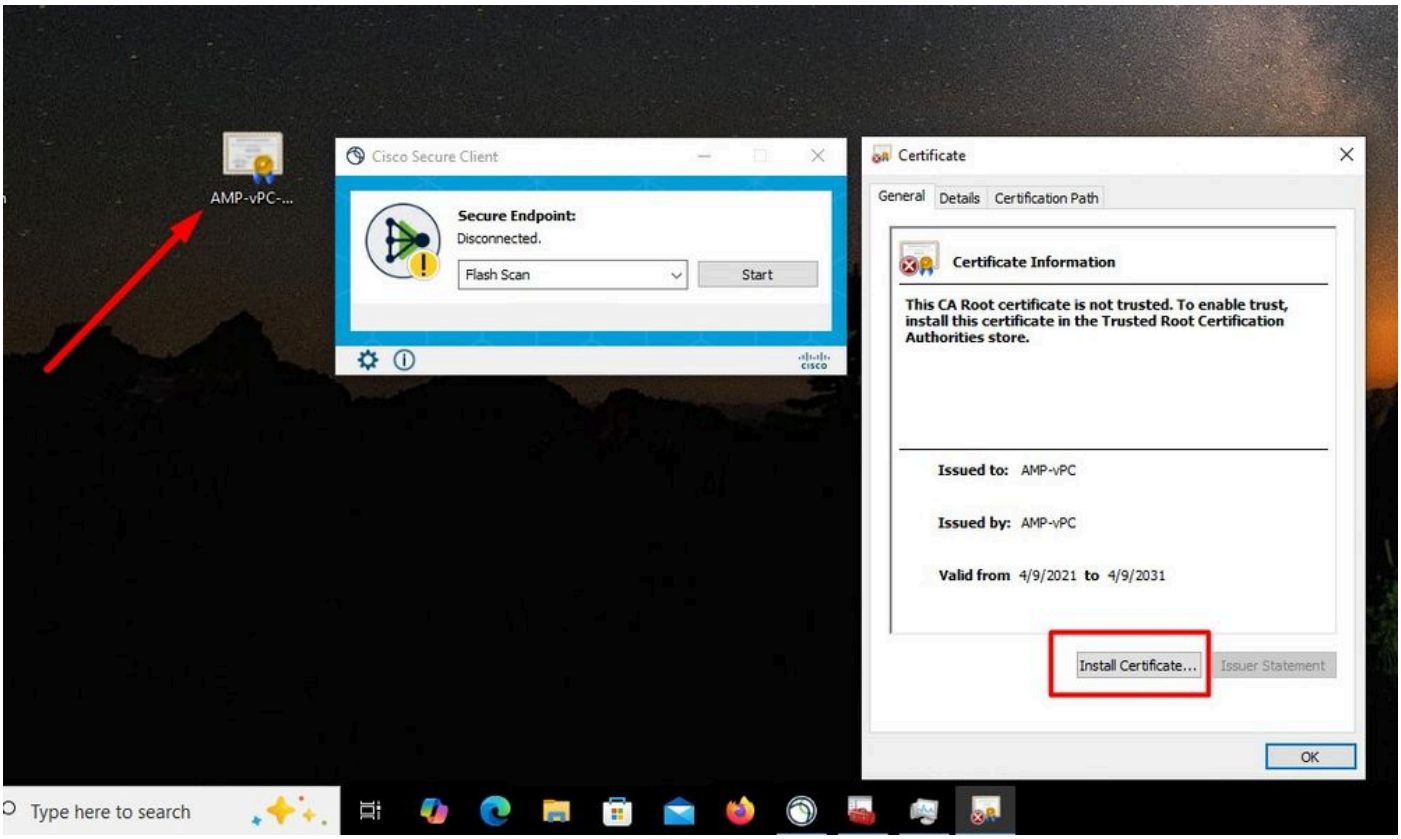
Una vez instalado el conector, el terminal seguro puede considerarse como desconectado. Ejecute el paquete de diagnóstico y revise los registros, podrá determinar el problema.

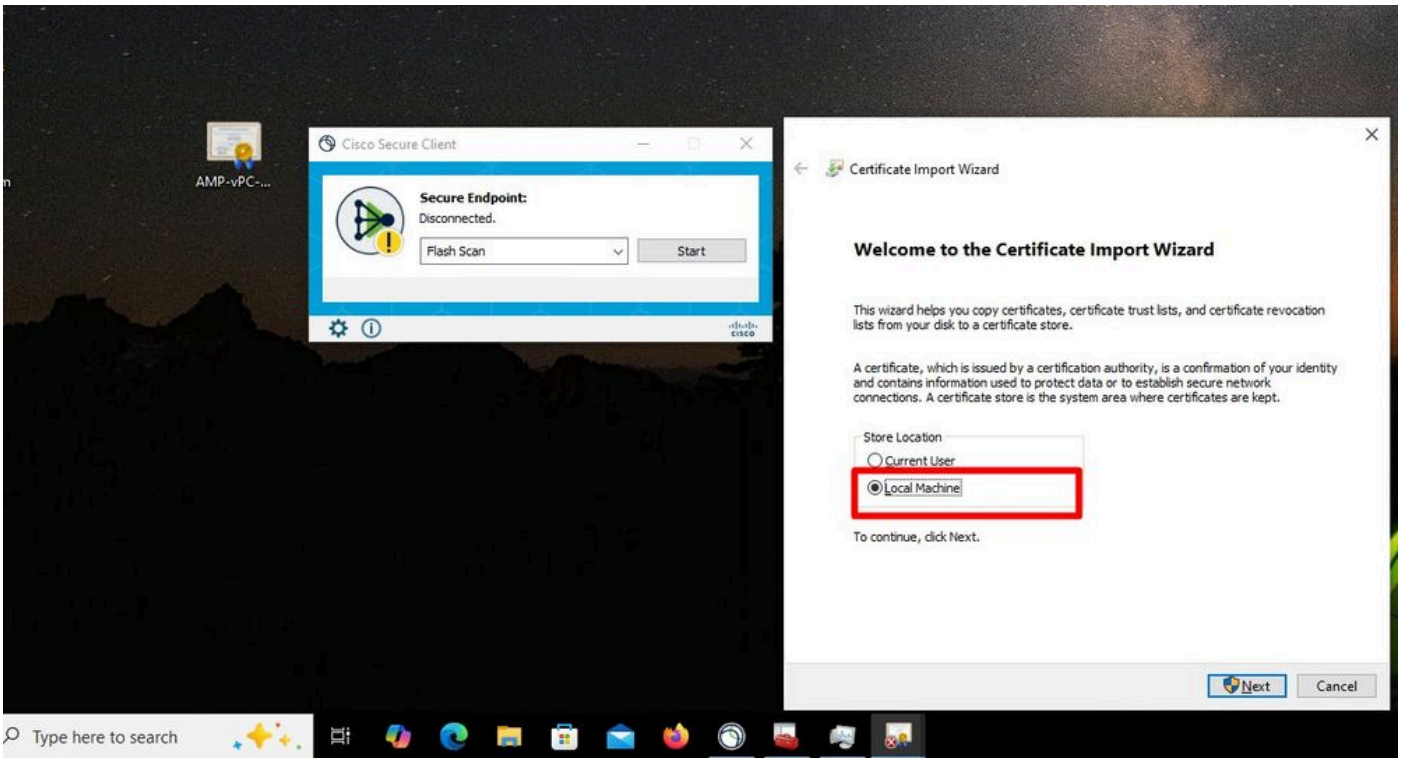


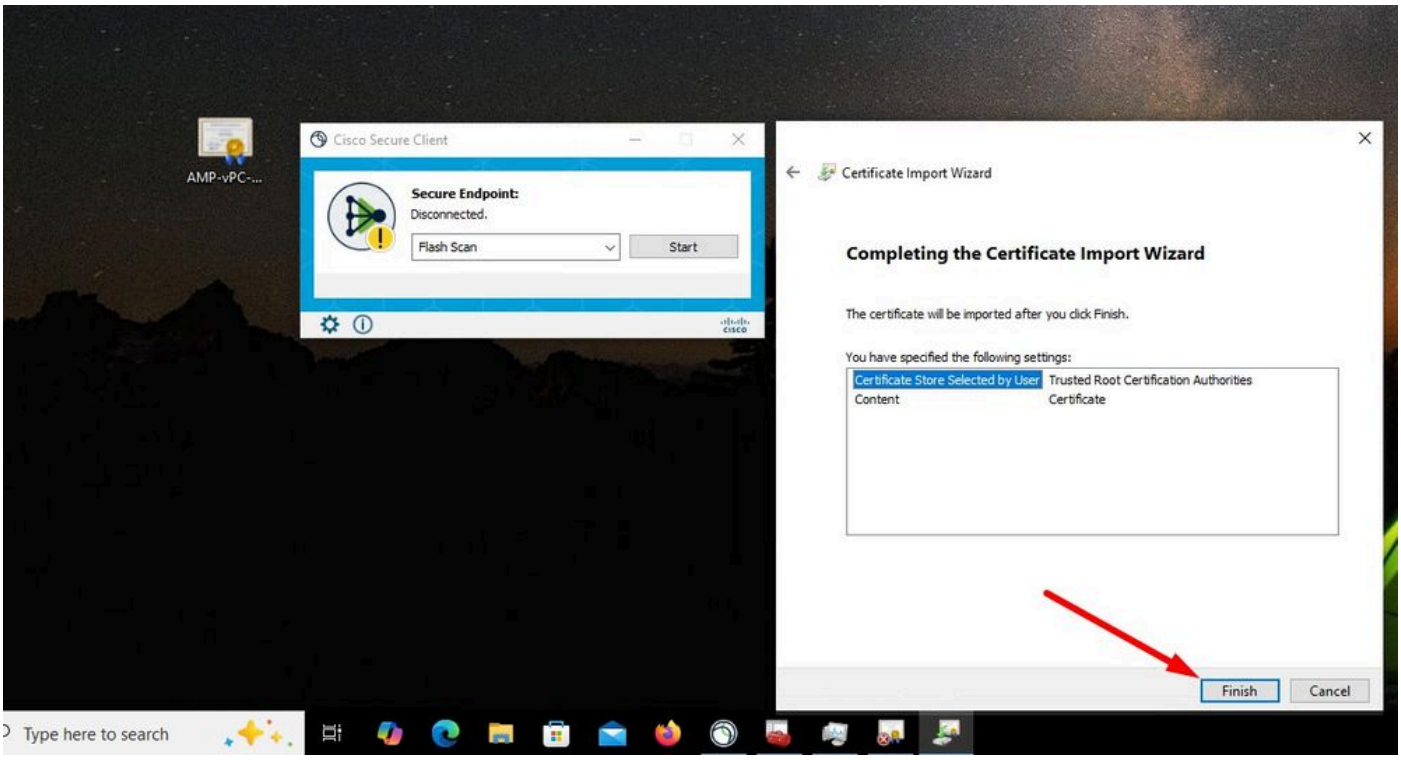
En función de este resultado recopilado del paquete de diagnóstico, puede ver el error de CA raíz

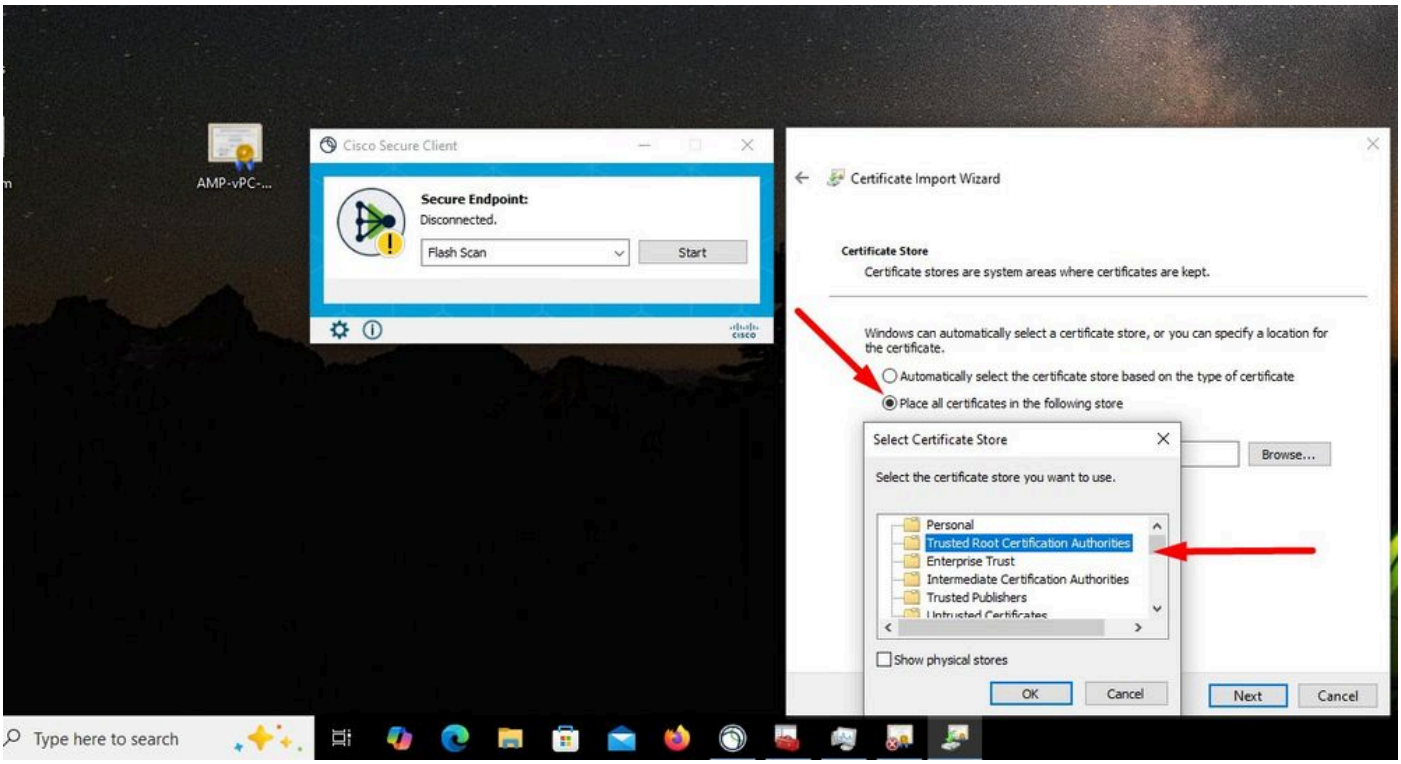
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60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

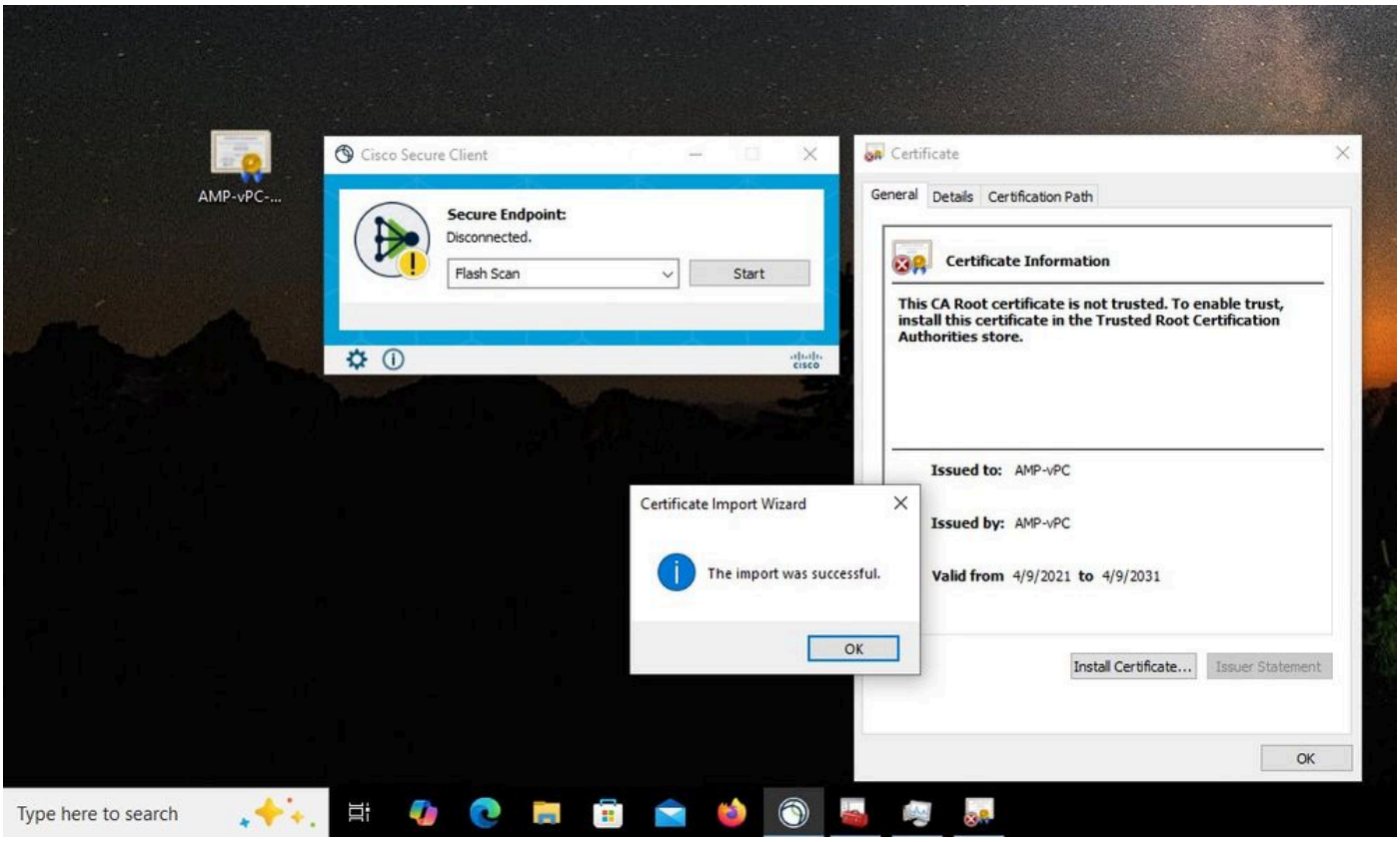
Una vez que haya cargado la CA raíz en el almacén de CA raíz de confianza y reinicie el servicio de punto final seguro. Todo empieza a funcionar como se esperaba.

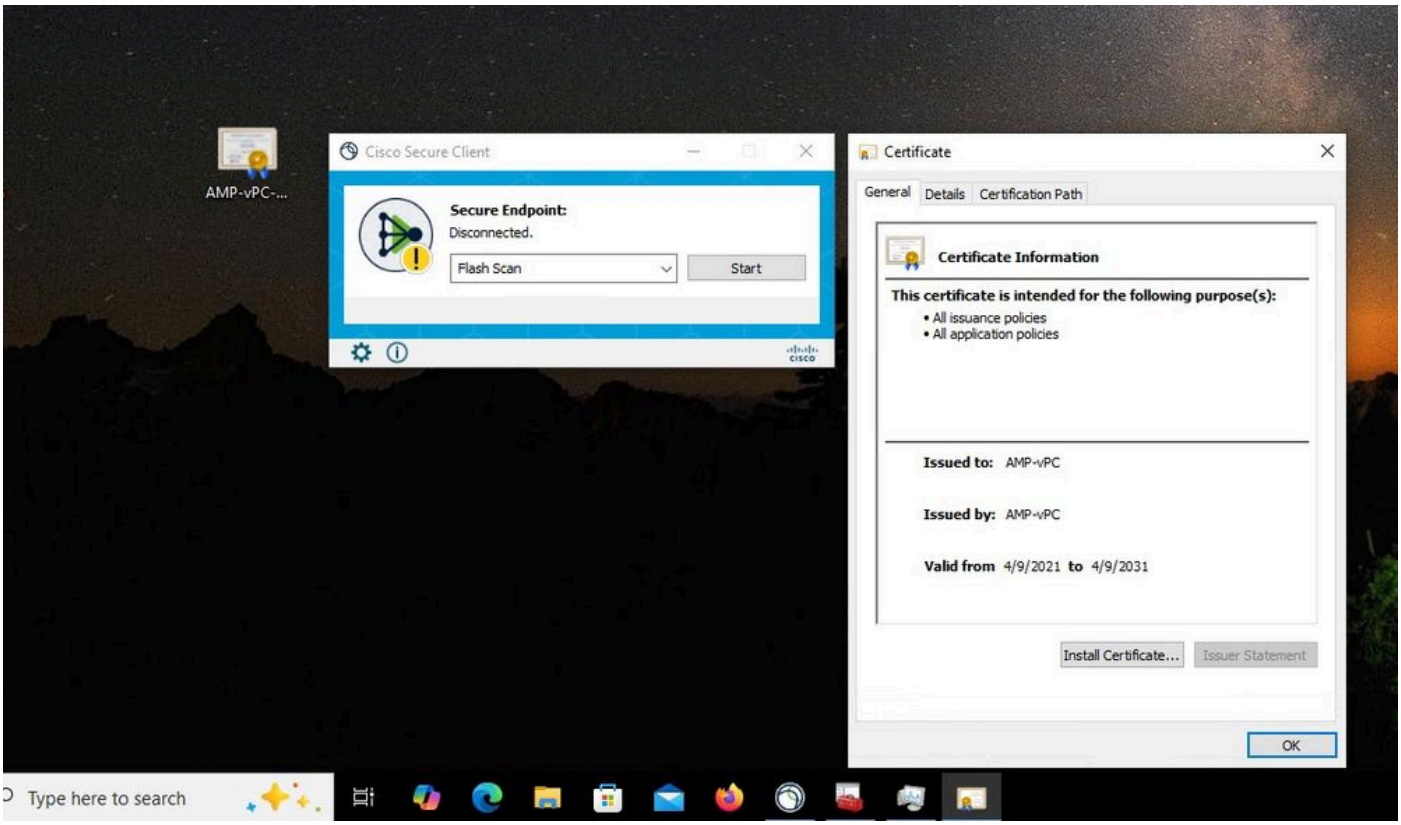


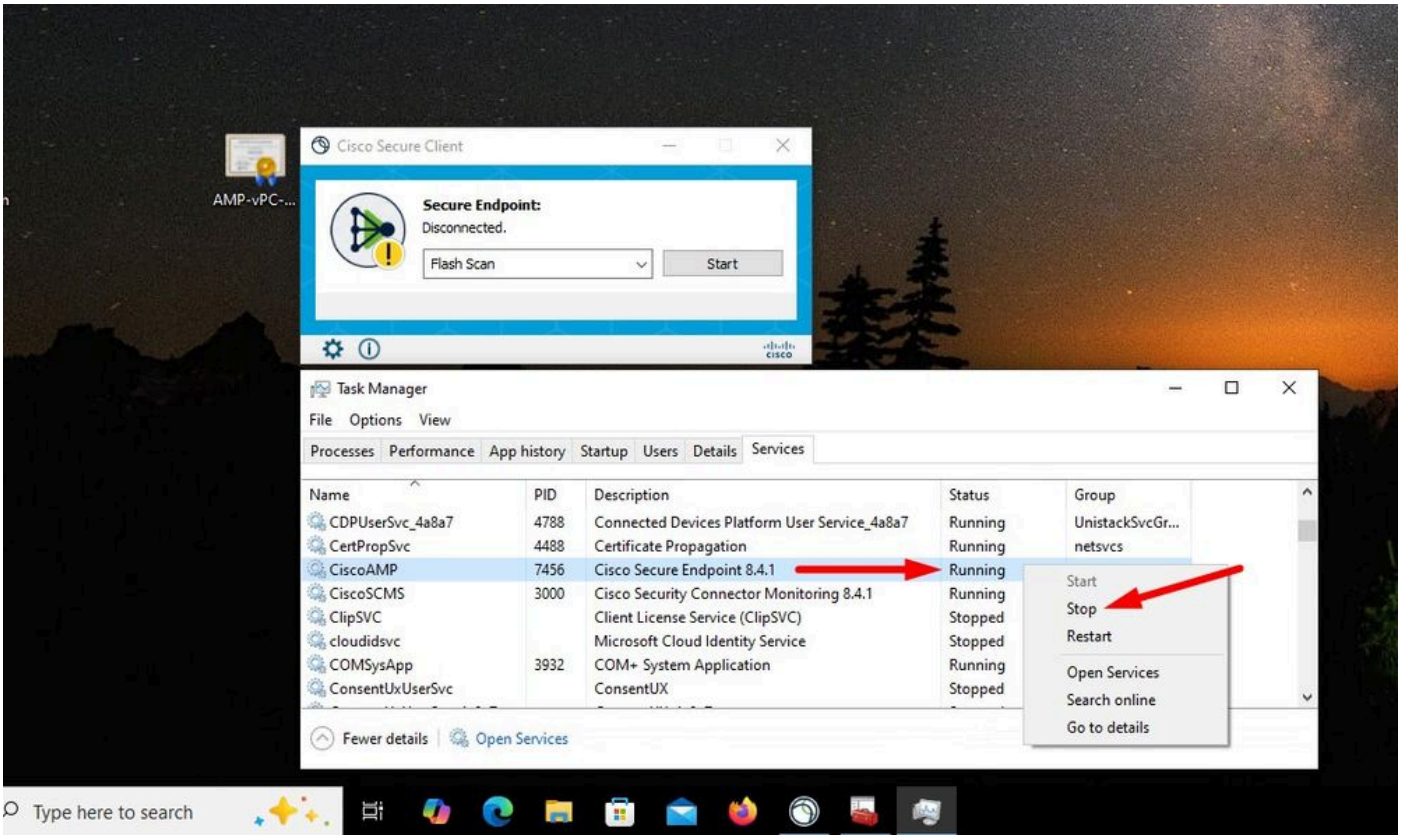

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which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

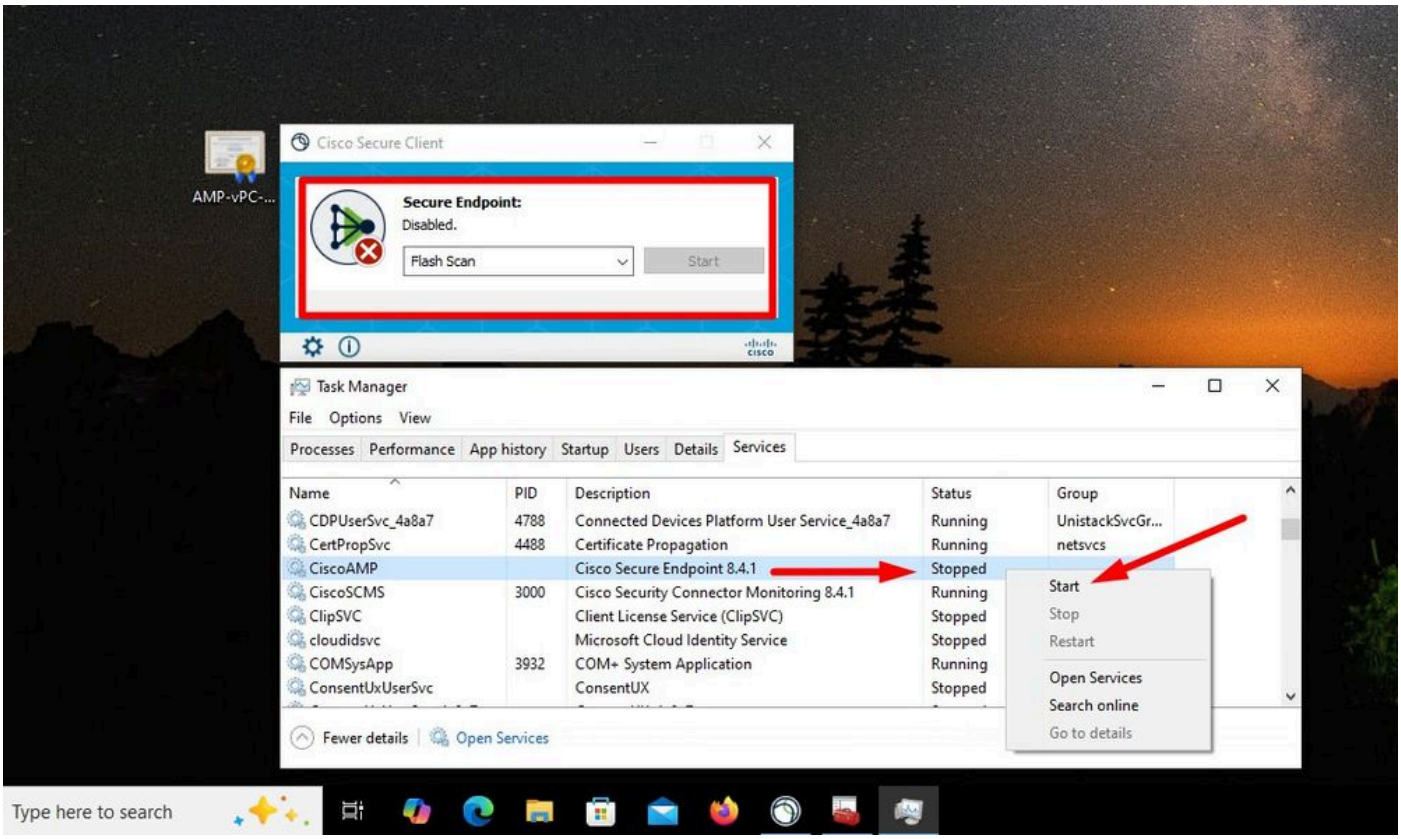

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification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


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

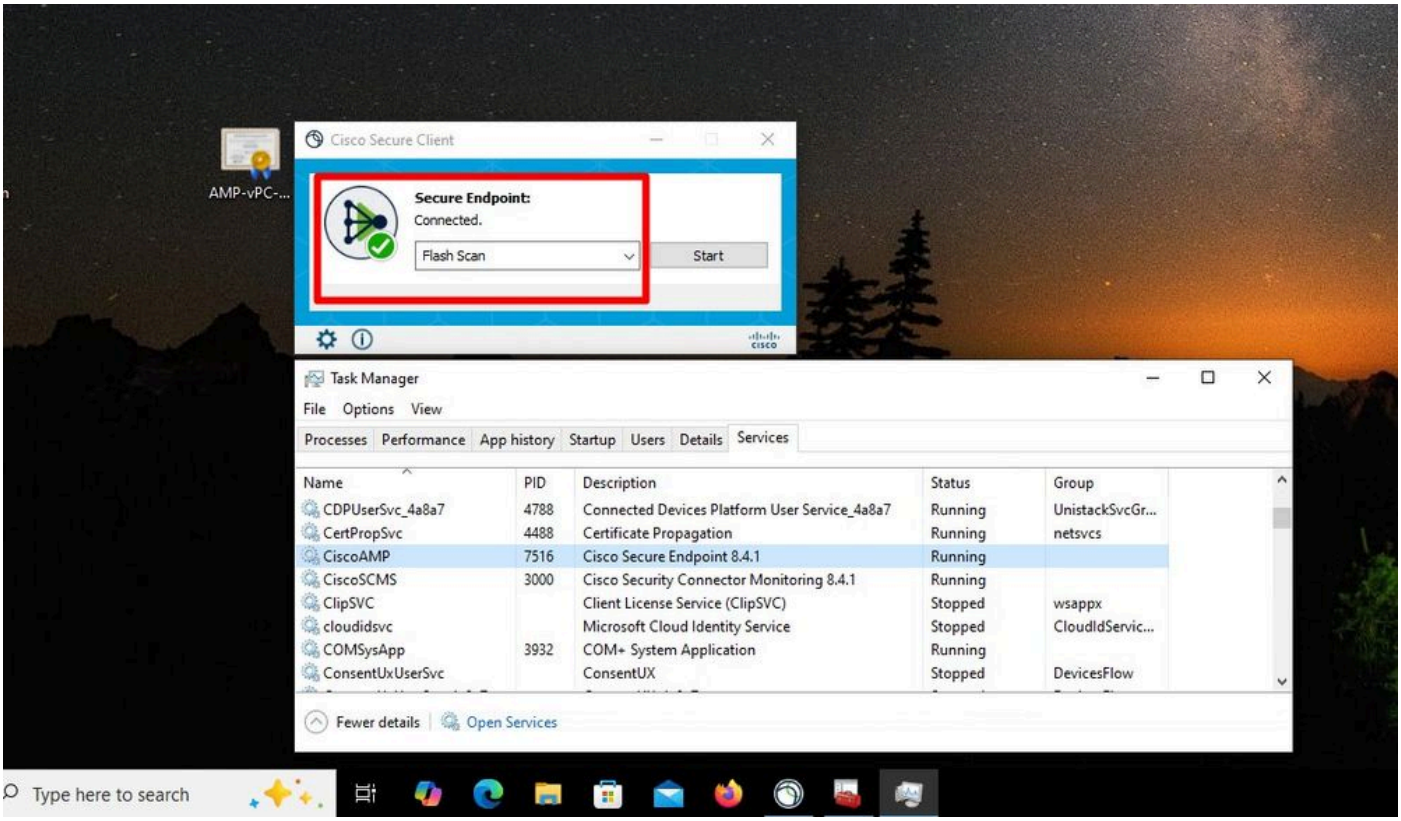

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: AMP-vPC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

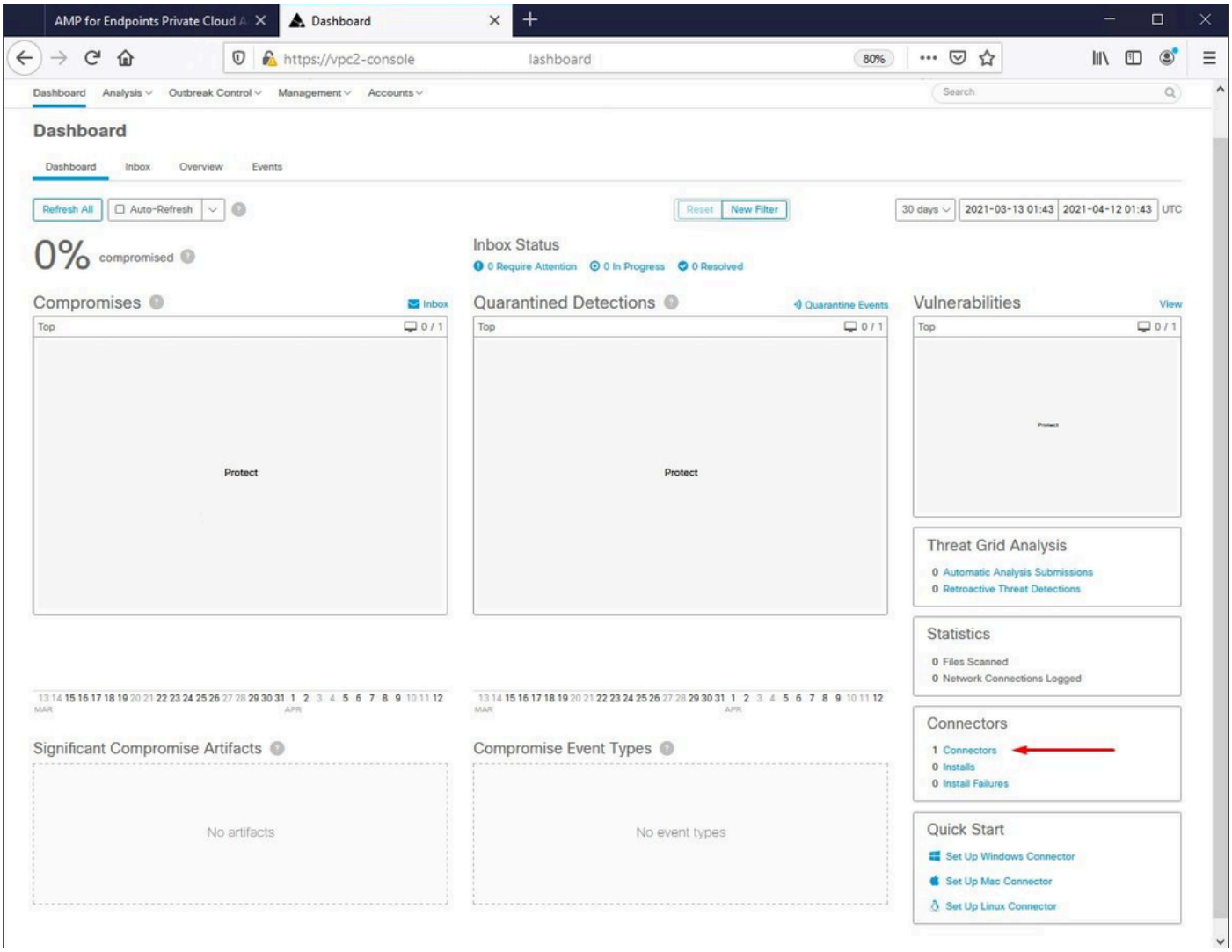

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid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


AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Task Manager
File
Options
View
Processes
Performance
App history
Startup
Users
Details
Services
Name
PID
Description
Status
Group
CDPUserSvc_4a8a7
4788
Connected Devices Platform User Service_4a8a7
Running
UnistackSvcGr...
CertPropSvc
4488
Certificate Propagation
Running
netsvcs
CiscoAMP
7456
Cisco Secure Endpoint 8.4.1
Running
CiscoSCMS
3000
Cisco Security Connector Monitoring 8.4.1
Running
ClipSVC
Client License Service (ClipSVC)
Stopped
cloudidsvc
Microsoft Cloud Identity Service
Stopped
COMSysApp
3932
COM+ System Application
Running
ConsentUxUserSvc
ConsentUX
Stopped
Start
Stop
Restart
Open Services
Search online
Go to details
Fewer details
Open Services
Type here to search

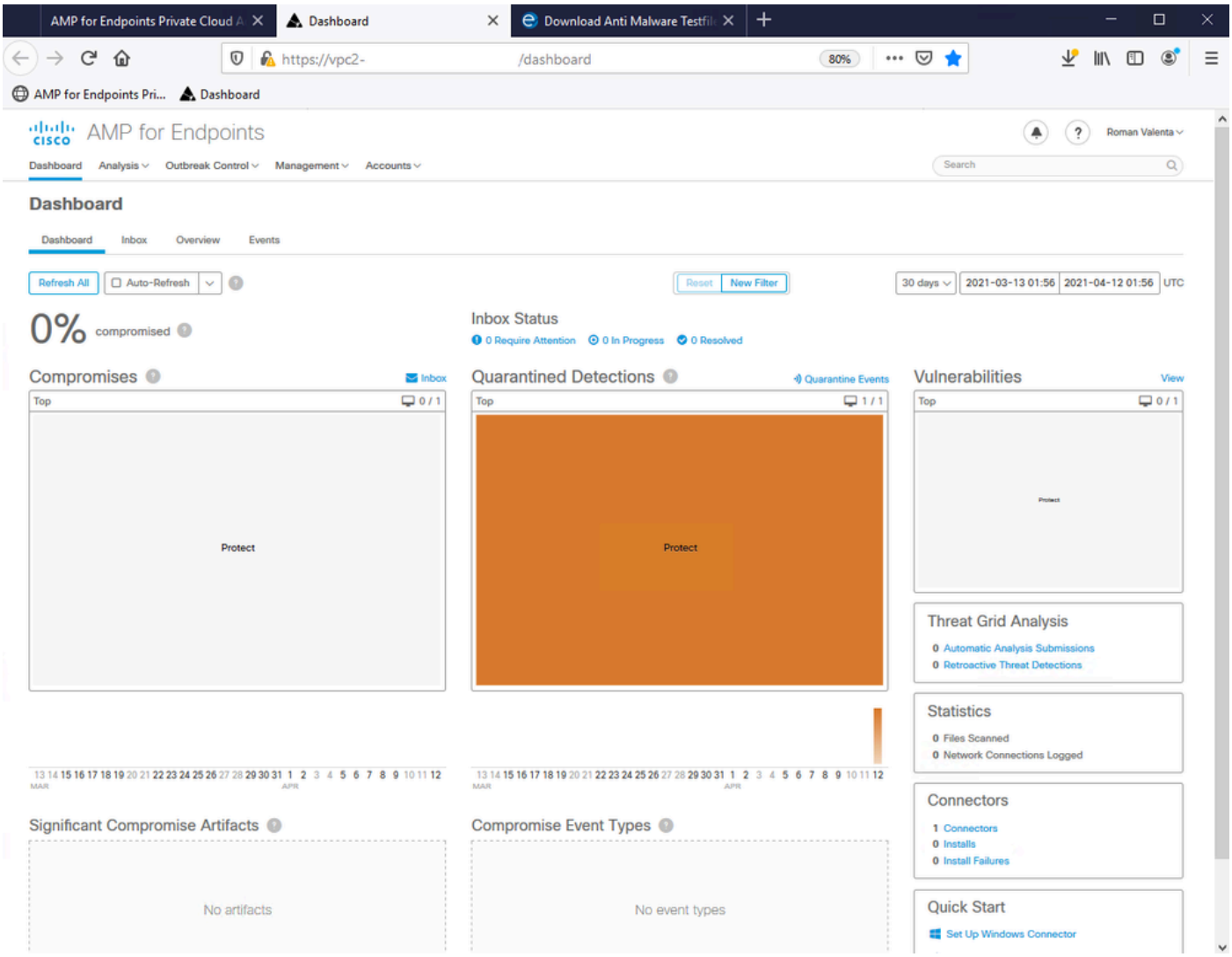


Una vez rebotado, el conector de servicio de terminal seguro se conecta como se esperaba.





Actividad maliciosa comprobada


AMP for Endpoints Private Cloud A
Dashboard
Download Anti Malware Testfil
https://vpc2-
/dashboard
80%
AMP for Endpoints Pri...
Dashboard
AMP for Endpoints
Roman Valenta
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
Refresh All
Auto-Refresh
Reset
New Filter
30 days
2021-03-13 01:56
2021-04-12 01:56
UTC
0% compromised
Inbox Status
0 Require Attention
0 In Progress
0 Resolved
Compromises
Inbox
Top
0 / 1
Protect
Quarantined Detections
Quarantine Events
Top
1 / 1
Protect
Vulnerabilities
View
Top
0 / 1
Protect
Threat Grid Analysis
0 Automatic Analysis Submissions
0 Retroactive Threat Detections
Statistics
0 Files Scanned
0 Network Connections Logged
Connectors
1 Connectors
0 Installs
0 Install Failures
Quick Start
Set Up Windows Connector
Significant Compromise Artifacts
No artifacts
Compromise Event Types
No event types

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).