

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 con éxito la nube privada virtual (VPC) en servidores en el entorno ESXi. Para consultar 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 ESX 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) y 1 TB de espacio libre mínimo en el disco duro del almacén de datos VMware
- Tipo de unidades: SSD necesario para el modo Air Gap y recomendado para proxy
- Tipo de RAID: un grupo RAID 10 (duplicación a rayas)
- Tamaño mínimo del almacén de datos de VMware: 2 TB
- Lecturas aleatorias mínimas del almacén de datos para el grupo RAID 10 (4K): 60K IOPS
- Mínimo de escrituras aleatorias del almacén de datos para el grupo RAID 10 (4K): 30K 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) y 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 creado con openssl o XCA
- 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 hay necesidad de especificarlas en el servidor VMWare. que resuelve el nombre de host de la 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. 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.

- 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 OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

AMP-vPC

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

x  PrivateCloud-Latest.ova



Back Next Finish Cancel

- 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

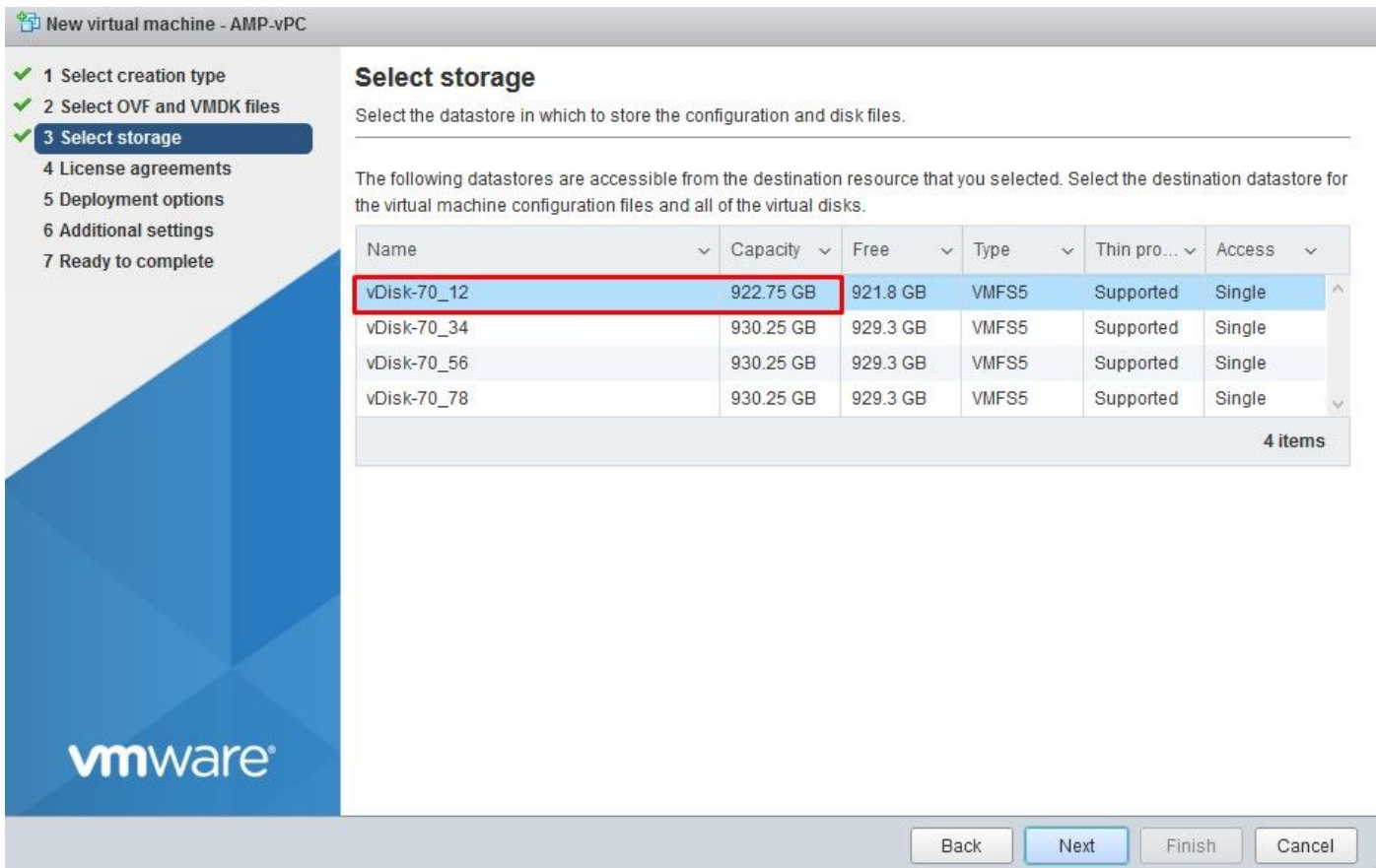
Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

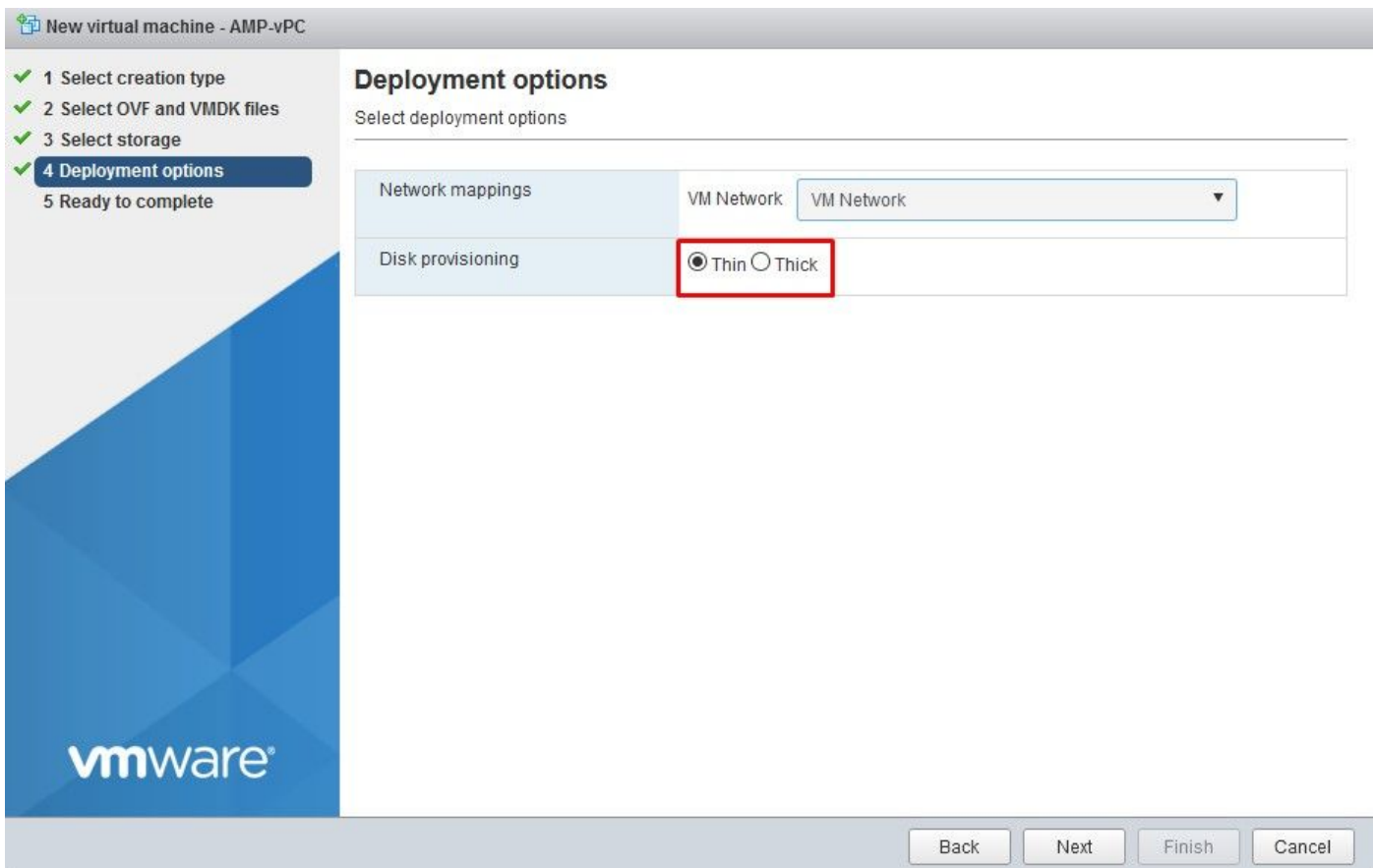
This option guides you through the process of creating a virtual machine from an OVF and VMDK files.



Back Next Finish Cancel



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 **Next**.

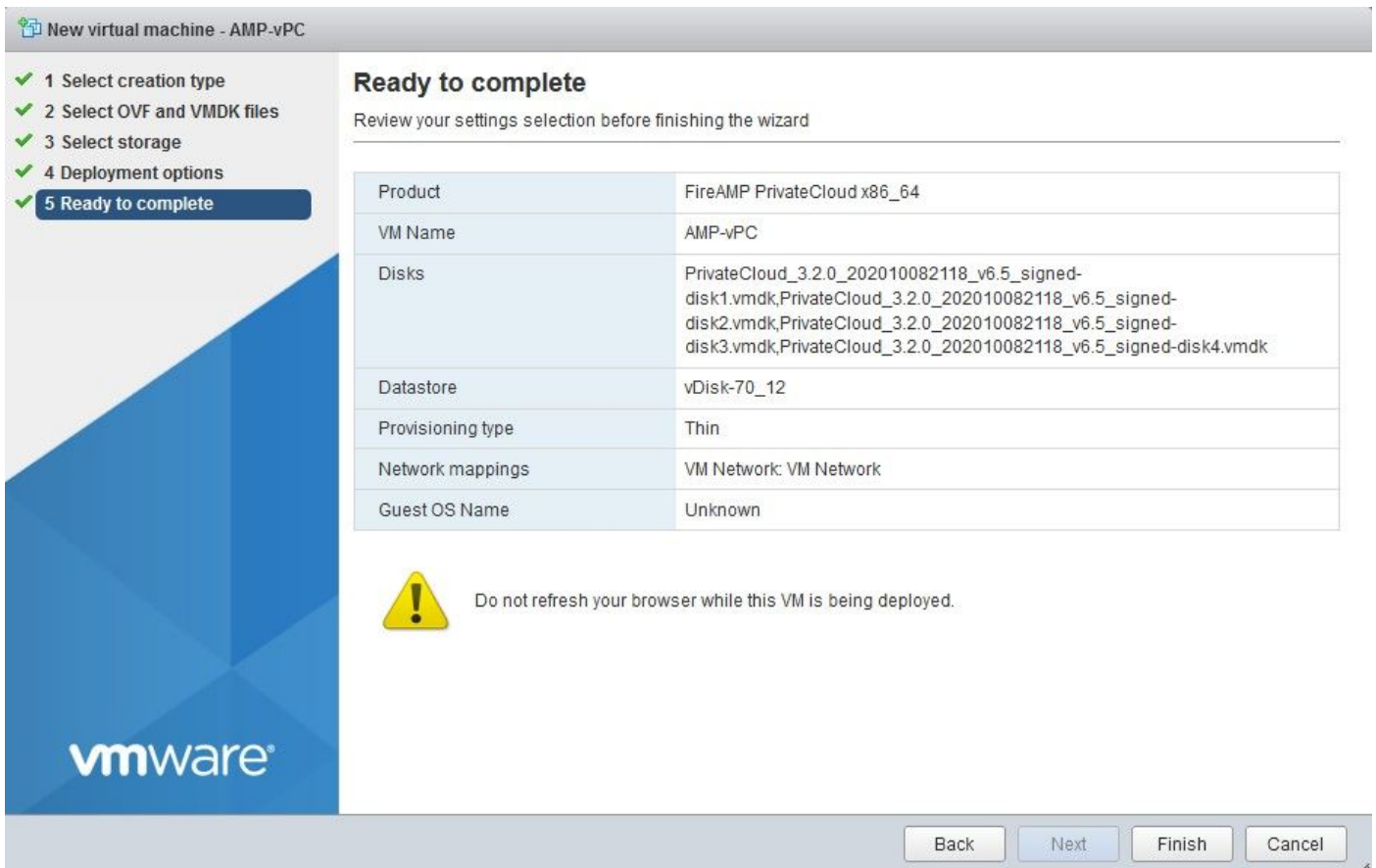
The screenshot shows the 'New virtual machine - AMP-vPC' wizard in the 'Ready to complete' stage. On the left, a progress bar indicates five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options, and 5. Ready to complete (highlighted). The main area displays a summary table of the VM configuration. Below the table is a warning icon and text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

Property	Value
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

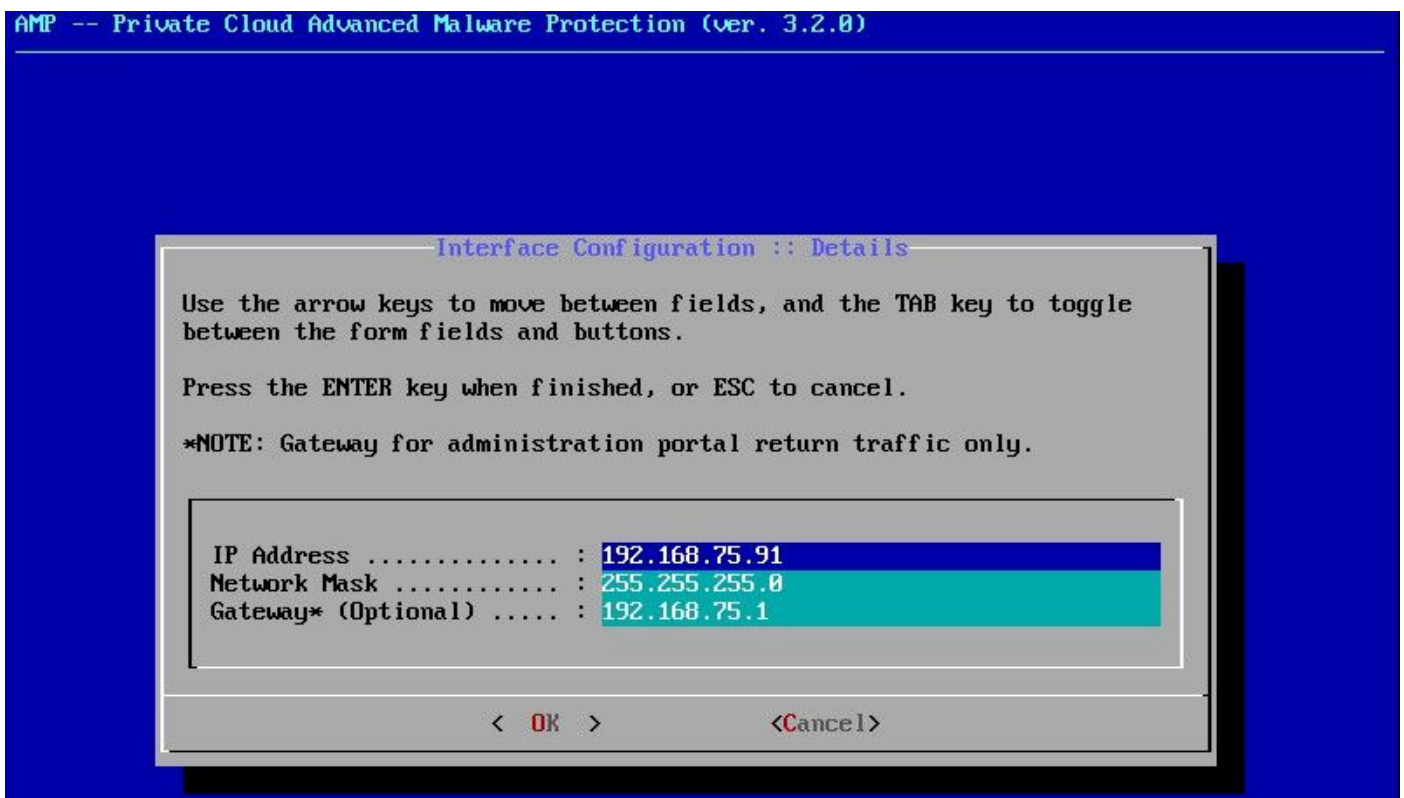
Configuración inicial de la interfaz de administración



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

Paso 1:

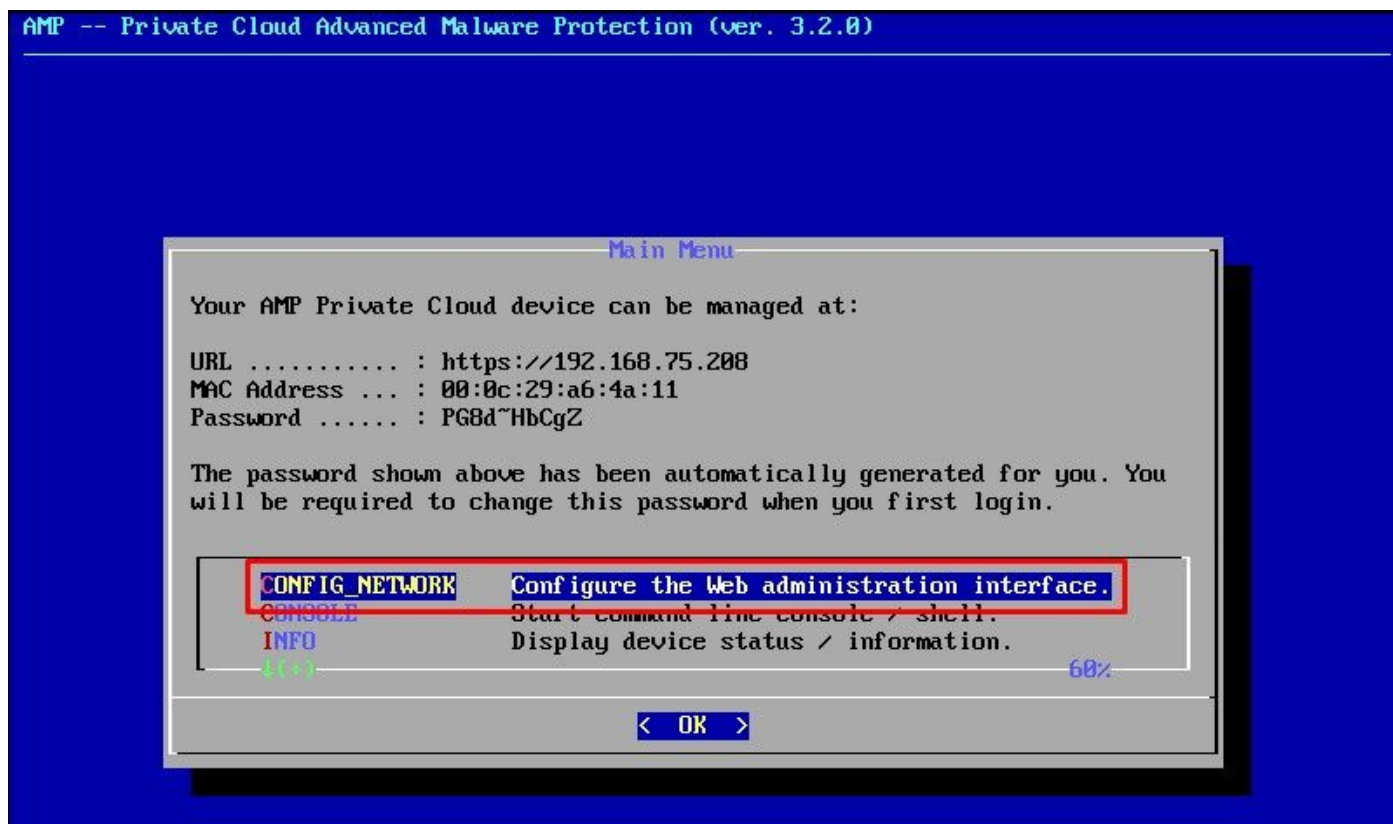
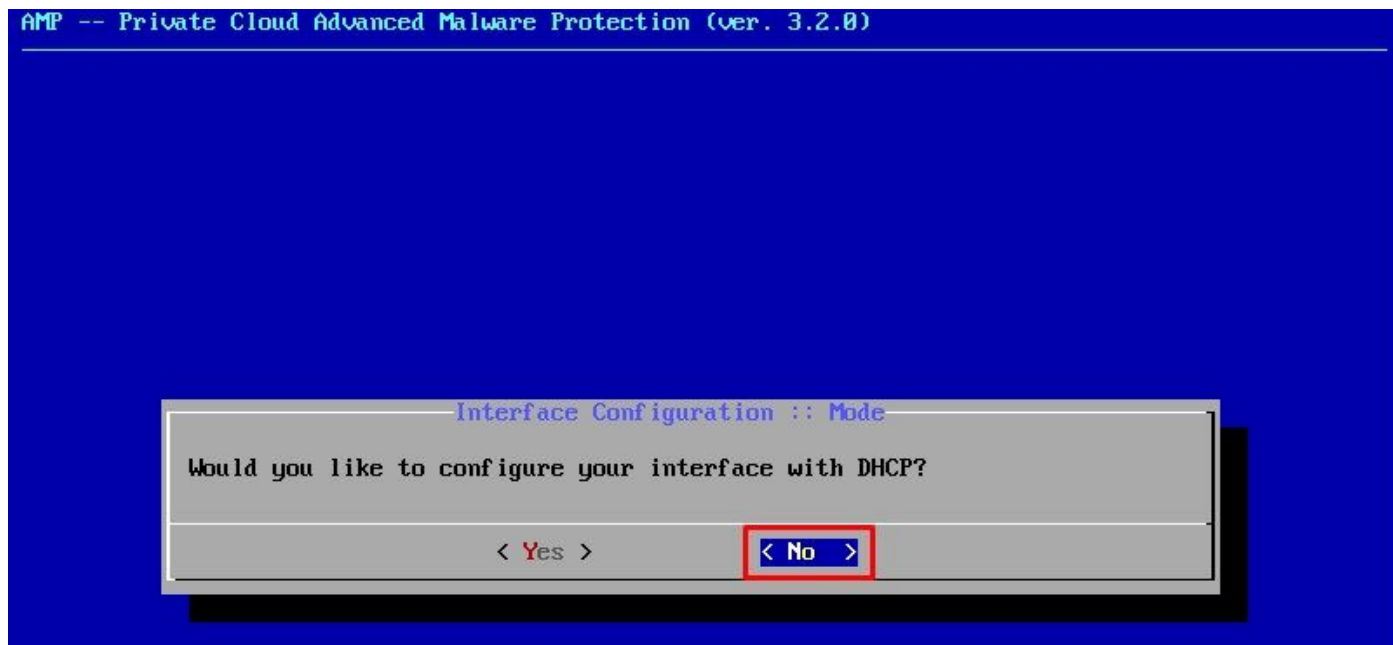
Es posible que observe que la dirección URL muestra **[UNCONFIGURED]** si la interfaz no recibió una dirección IP del servidor DHCP. Tenga en cuenta que esta interfaz es la interfaz de **administración**. Esta no es la interfaz de **Producción**.



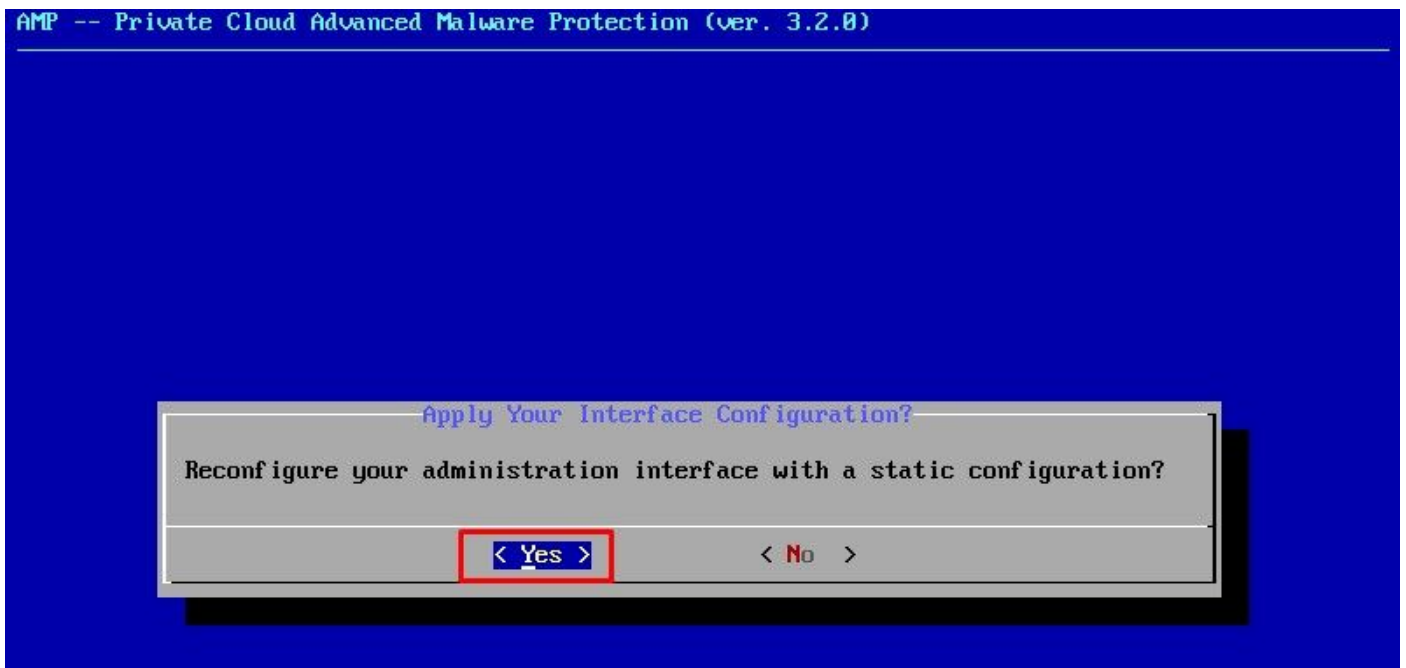
Paso 2:

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.

```
Restarting eth0...
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 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>

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_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
```

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.

```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)
```

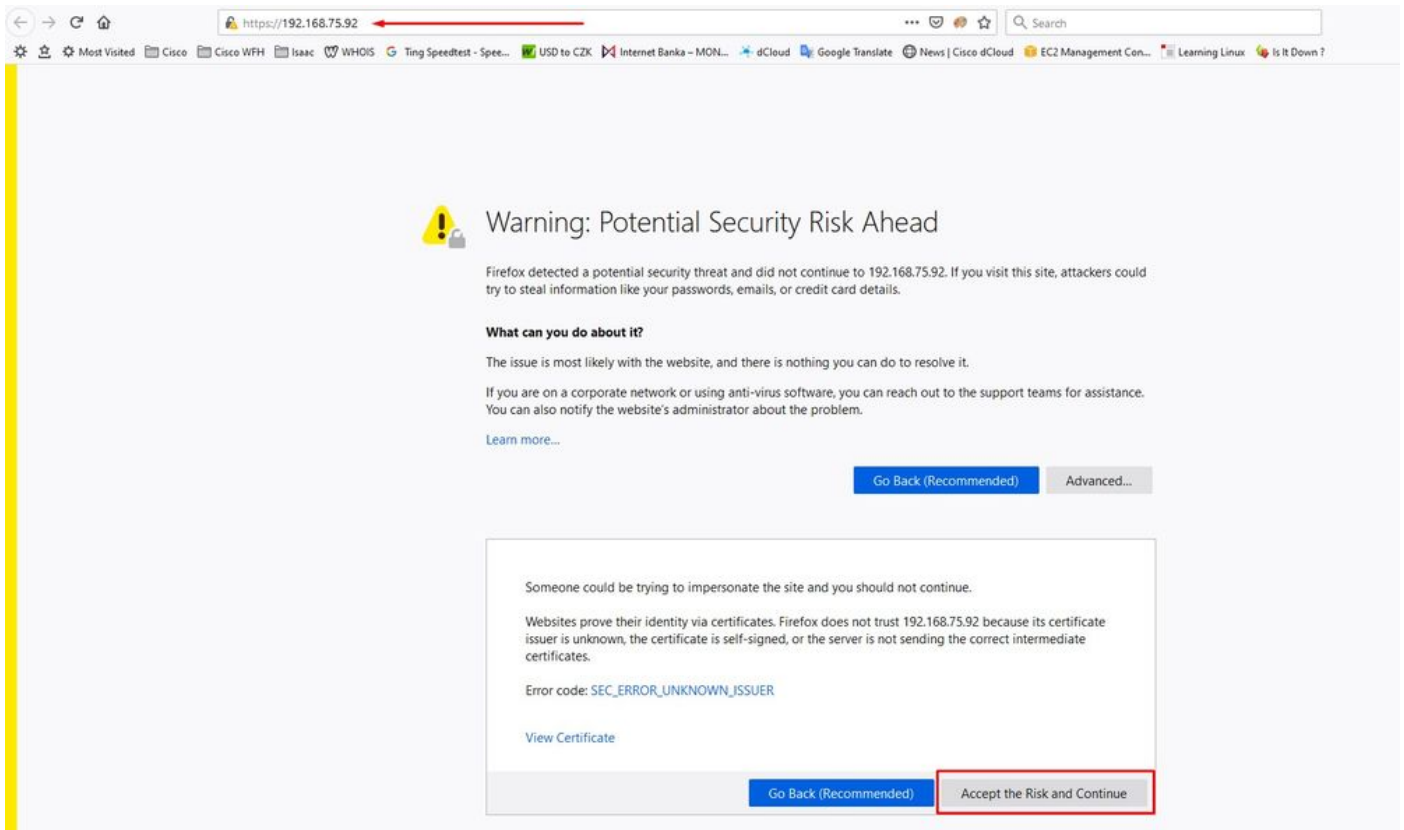


Configuración inicial de vPC mediante GUI web

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:

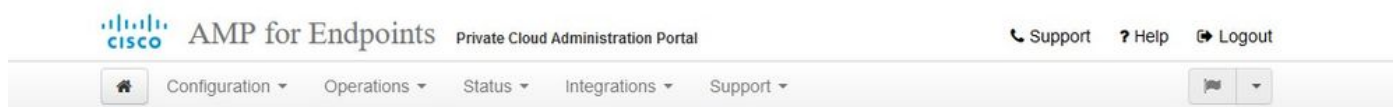
Después de iniciar sesión, se le pedirá que restablezca la contraseña. Utilice la **contraseña inicial** de la consola en el campo **Contraseña Antigua**. Utilice la nueva contraseña en el campo **Nueva contraseña**. Vuelva a introducir la nueva contraseña en el campo **Nueva contraseña**. seleccione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

en Cambiar contraseña.



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.

The screenshot shows a password change form. It consists of three input fields, each with a green 'a' icon on the left and a red arrow pointing to it from the right. The top field is labeled 'Old one time password'. Below the input fields is a green button labeled 'Change Password'.

Paso 4:

En la página siguiente, desplácese hacia abajo para aceptar el acuerdo de licencia. Seleccione **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**.

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 >

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 soporte técnico de Cisco.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

License

Device ID
EG-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 >

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.

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 >](#)

Configuración

Paso 1:

Nota: Tenga en cuenta que en los siguientes conjuntos de diapositivas incluimos algunos exclusivos, como se muestra en la imagen, que son únicos solo en el modo **AIR GAP**, los cuales deben incluirse y marcarse como **AIRGAP ONLY (SOLO AIRGAP)**



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.

≡ ≡ **SÓLO AIRGAP** ≡ ≡



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Deployment Mode

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

Cloud Proxy

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

Standalone

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

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Standalone Operation

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



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

⌘ ⌘ AIRGAP 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**.

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	
Password	[redacted]	

Next >

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

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 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.

Hardware Configuration

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

[Shutdown](#)[I understand the risks >](#)

Nota: Utilice sólo los valores recomendados, a menos que se trate de un análisis de laboratorio

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](#)

Una vez reiniciados continuamos donde nos fuimos.



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 >

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:



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
- > Firewall 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)

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**.



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 ≡ ≡



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 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.

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 >

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**.

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 ✓

Cisco Cloud

Cisco Cloud Configuration

Region

Cisco Cloud, North America

[View Hostnames \(click to expand\)](#)

Cisco Cloud Identity

Client Identity

0f476ea8 [redacted] ddbc272a6c

Next >

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**.

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](#) rva [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 >

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**.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. Below the navigation bar, there are two red status boxes: 'Maintenance Mode' and 'Sanity Check Failing'. The main content area has a heading 'SSH Keys' and a sub-heading 'Add SSH Key'. Below this, there is a section titled 'Windows PuTTY' which contains a table of SSH keys. The table has two columns for key details and an 'Edit' button. The first key is 'ecdsa-sha2-nistp256 AAAAE2...' and the second is 'ssh-rsa AAAAB3...'. The first key's details are: '2021-11-17 23:01:01 +0000 created 20 days ago'. The second key's details are: '2021-11-17 23:01:01 +0000 20 days since last update'. The 'Edit' button is red and has a trash icon next to it.

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"**

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

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

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

vPC2-Authenticator + Choose Key

vPC2-Authenticator + Choose Certificate

[Next >](#)

Sin verificación TLS estricta

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)

- ✓ Certificate file has been uploaded.
- ✓ Certificate is in a readable format.
- ✓ Certificate start and end dates are valid.
- ✓ Certificate contains a subject.
- ✓ Certificate contains a common name.
- ✓ Certificate contains a public key matching the uploaded key.
- ✓ Certificate matches hostname.
- ✓ Certificate is signed by a trusted root authority.

vPC2-Authenticatic

+ Choose Certificate

Key (PEM .key)

- ✓ Key file has been uploaded.
- ✓ Key contains a supported key type.
- ✓ Key contains public key material.
- ✓ Key contains private key material.
- ✓ Key contains a public key matching the uploaded certificate.

vPC2-Authenticatic

+ Choose Key

vPC2-Authentication.cyberworld.local.pem

vPC2-Authentication.cyberworld.local.crt

[Next >](#)

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 a su servidor DNS y configure el resto de los registros de 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 Key

+ Choose Certificate

Next >

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 >](#)

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](#)

≡ ≡ **SÓLO AIRGAP** ≡ ≡

- 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 ✓
 - > 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 SOLAMENTE ^^

Se ve una entrada similar como esta...

Precaución: cuando se encuentre en esta página, no realice la actualización, 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 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

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 ≡ ≡

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!
=====
```

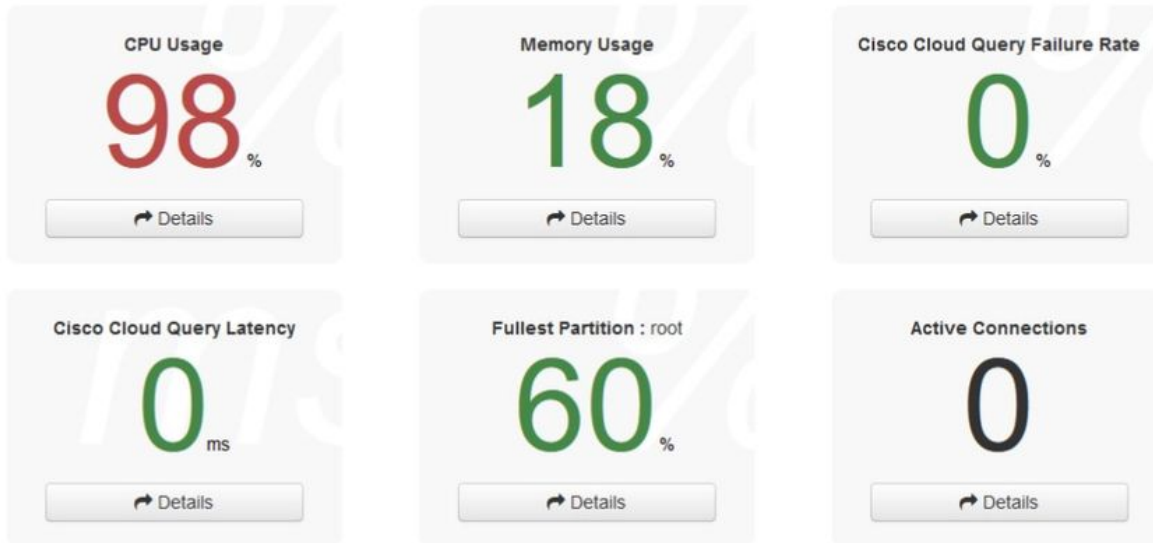
Download Output

^^ AIRGAP SOLAMENTE ^^

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.



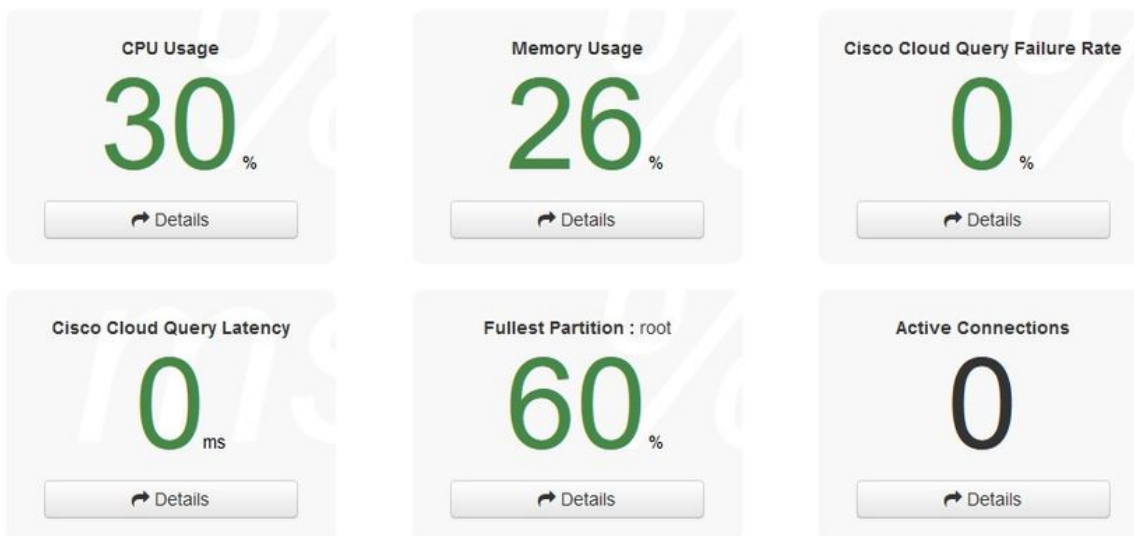
Key Metrics



Después de unos minutos...



Key Metrics



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.

The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. The browser address bar displays `https://192.168.75.92`. The page header includes the Cisco logo, the title "AMP for Endpoints Private Cloud Administration Portal", and navigation links for Support, Announcements, Help, and Logout. Below the header is a navigation menu with options: Configuration, Operations, Status, Integrations, and Support. On the right side of the navigation menu, there is a red arrow pointing to a small icon that looks like a flame or a warning symbol. Below the navigation menu is a section titled "Key Metrics" which contains three cards:

Metric	Value
CPU Usage	11%
Memory Usage	36%
Cisco Cloud Query Failure Rate	0%

Each card has a "Details" button below it.

≡ ≡ SÓLO AIRGAP ≡ ≡

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



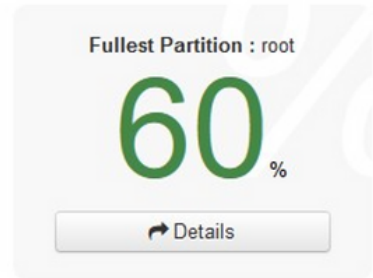
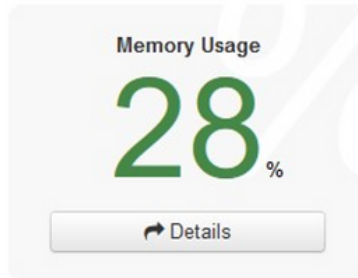
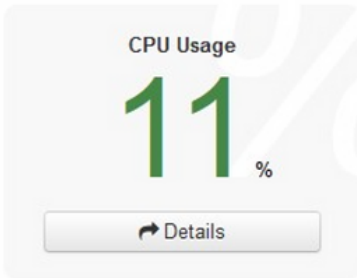
Sanity Check Failing

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.

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 a través de este comando y luego verifique que podría tardar **más de 24 horas**. 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
% 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/e6f73d52f5c079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-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
99.97% 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 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

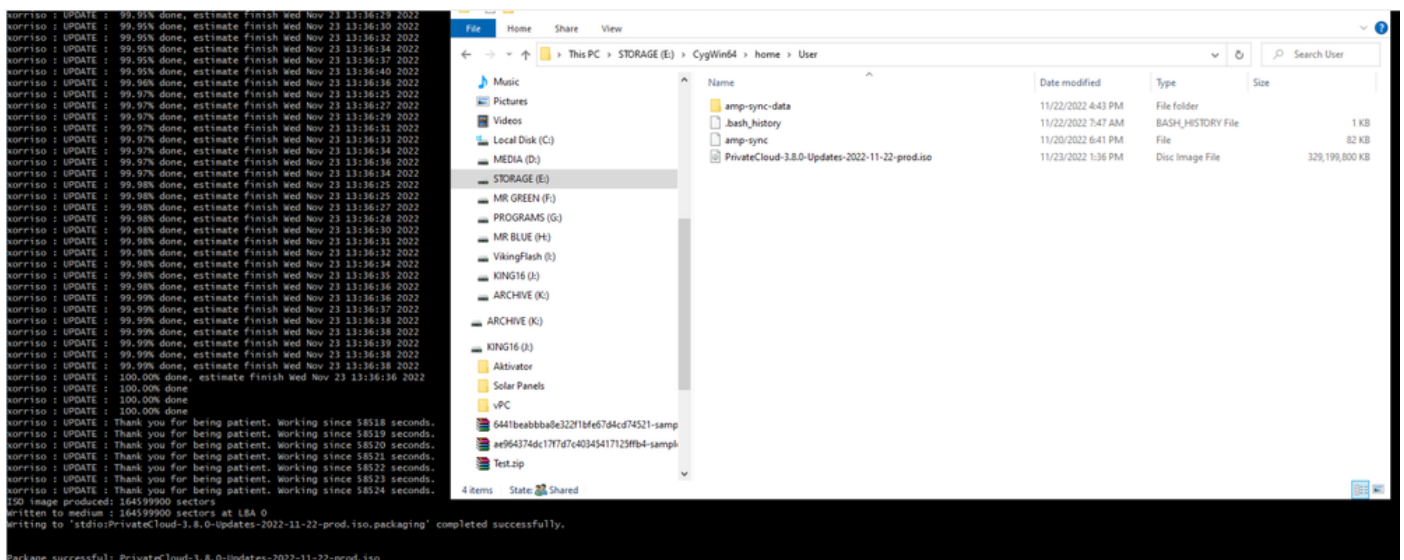
To run amp-sync you will first have to install xorriso and xmlstarlet.

- 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 utilizar CygWin de nuevo, debe descargar manualmente xorriso desde el repositorio de GitHub. Abra el explorador y escriba <Última versión preliminar de xorriso.exe 1.5.2 para Windows> debería aparecer como el primer vínculo denominado <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 encuentre, entre otros pocos archivos denominados <xorriso.exe> copie y pegue este archivo en <CygWin6Win4\bin > de su 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.

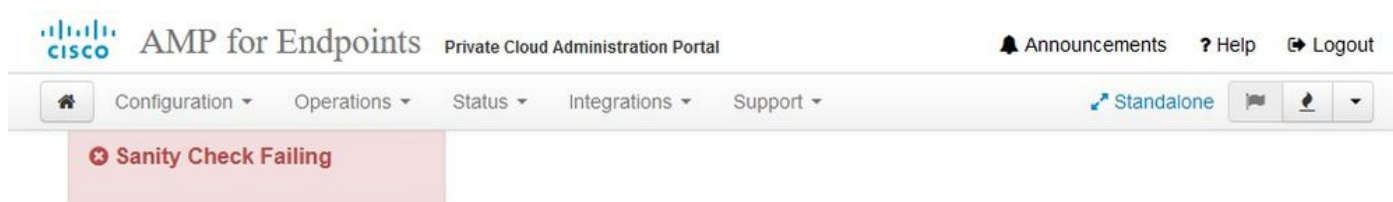


Realice la copia de respaldo de la VPC (*en este caso*) actual 3.2.0 en el modo Airgap.

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.



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](#)

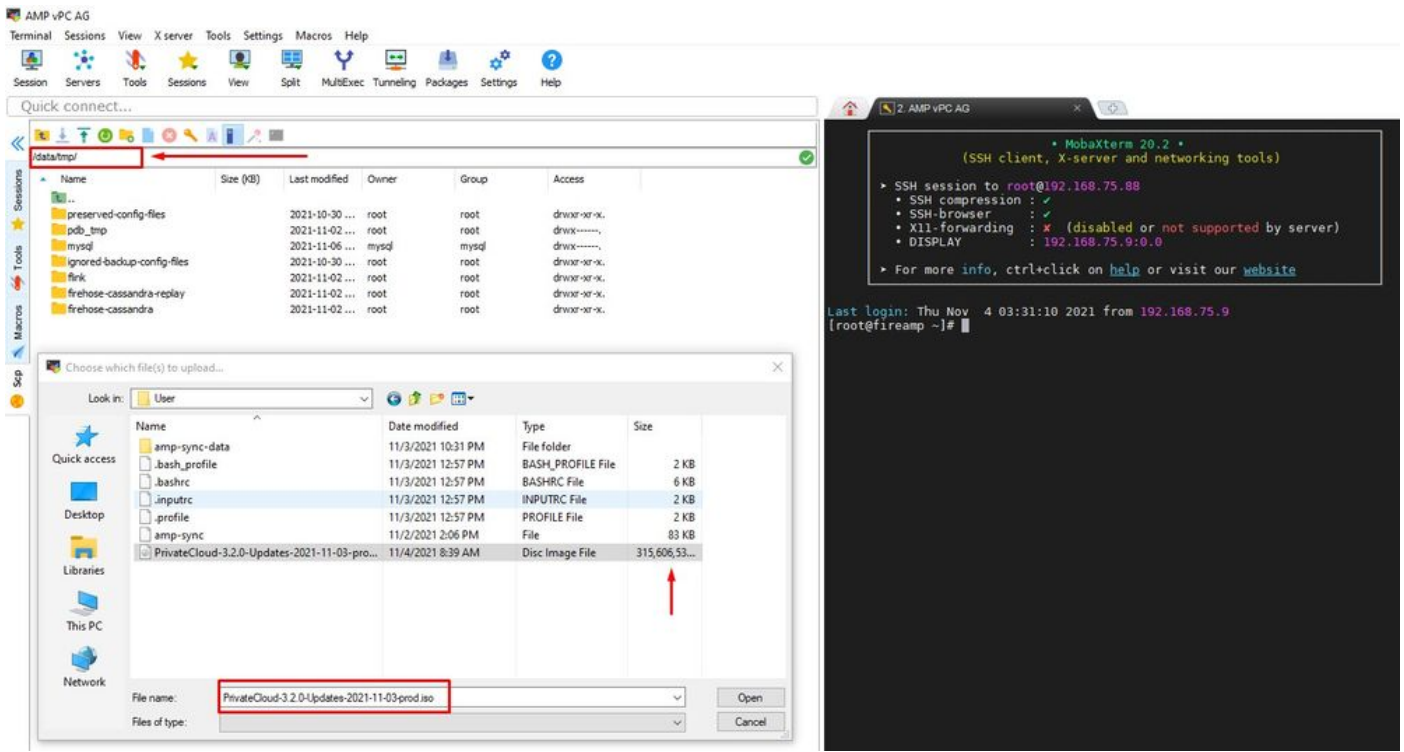
Previous Backups

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	Download Delete

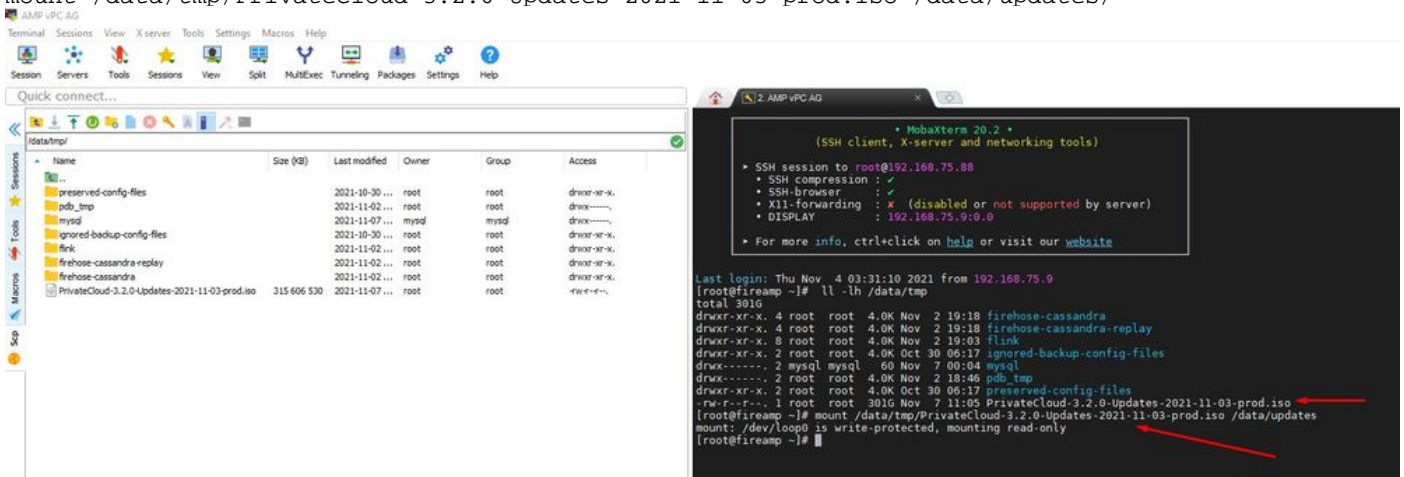
Transfiera el último ISO generado con amp-sync al VPC. Esto puede tardar hasta varias horas, así en función de su velocidad. En este caso la transferencia tomó más de 16Hrs

```
/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.**



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.

En este ejemplo, procedo con **Update Content** primero



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

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

A content update is available.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

A continuación, seleccione Importar proteger BD.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. On the right, there are links for 'Announcements', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. A 'Sanity Check Failing' alert is visible in a red box. The main content area has a section for 'Updates' with a 'Download amp-sync' button and a 'Check Update ISO' button. Below this is a 'Content' section. It displays a green checkmark and the version '20211102210054' for 'Client Definitions, DFC, Tetra Content Version'. To the right are buttons for 'Update Content' and 'Import Protect DB', with a red arrow pointing to the latter. Below the content version, there is a red warning icon and the text 'ABSENT Protect DB Version'. A message states 'Import a Protect DB snapshot to your standalone device.' and another message says 'Checked less than a minute ago; content is up to date.' The 'Software' section shows a version '3.2.0_202010082118' for 'Private Cloud Software Version' with an 'Update Software' button and a message 'A software update is available.'

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

⚙️ 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: 9:28:21 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 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

Event Details

Type: **error** User: **root** Time: **11/15/2021 12:24:43 PM** Target: **AMP-vPC AirGap**

Description:  11/15/2021 12:24:43 PM, Error message on AMP-vPC AirGap on UCS-2 in ha-datacenter: Failed to power on VM.

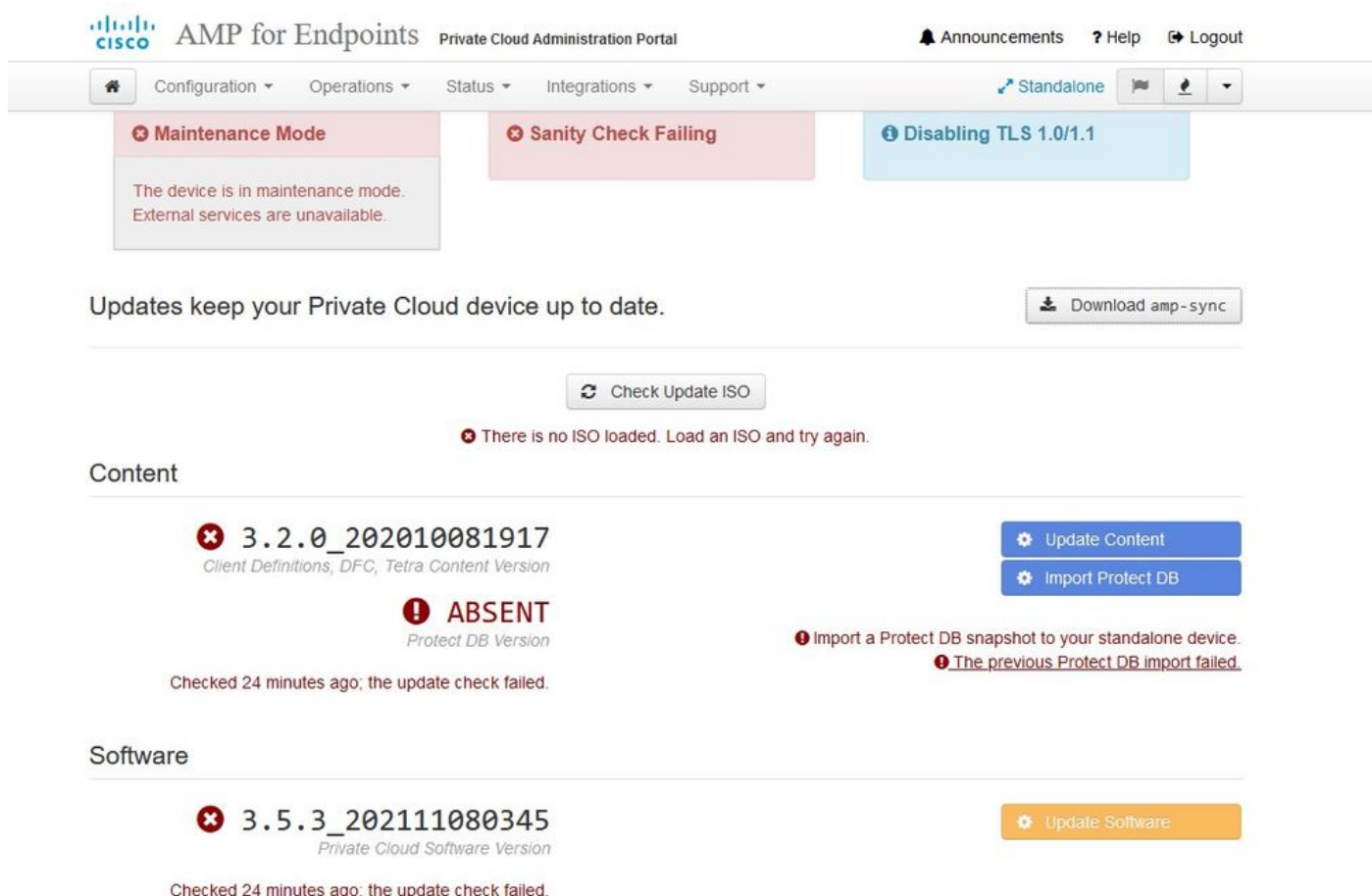
Error Stack: [Hide](#)

- ↳ Failed to power on VM.
- ↳ Could not power on virtual machine: msg.vmk.status.VMK_NO_SPACE.
- ↳ Failed to extend the virtual machine swap file
- ↳ Current swap file size is 0 KB.
- ↳ Failed to extend swap file from 0 KB to 134217728 KB.
- ↳ File system specific implementation of LookupAndOpen[file] failed
- ↳ File system specific implementation of Lookup[file] failed

Related Events: [Show](#)

Problema #2: actualización anterior

El problema 2nd es si se ejecuta la actualización de software primero como lo hice en mi 2^o 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.



The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. At the top, there are navigation tabs for Configuration, Operations, Status, Integrations, and Support. A notification bar at the top right contains 'Announcements', 'Help', and 'Logout'. Below the navigation, three status boxes are visible: 'Maintenance Mode' (red), 'Sanity Check Failing' (red), and 'Disabling TLS 1.0/1.1' (blue). The 'Maintenance Mode' box states: 'The device is in maintenance mode. External services are unavailable.' Below this, a section titled 'Updates keep your Private Cloud device up to date.' includes a 'Download amp-sync' button and a 'Check Update ISO' button. A red error message below the 'Check Update ISO' button reads: 'There is no ISO loaded. Load an ISO and try again.' The 'Content' section shows a red error for version '3.2.0_202010081917' (Client Definitions, DFC, Tetra Content Version) with 'Update Content' and 'Import Protect DB' buttons. A red error for 'ABSENT' (Protect DB Version) is also present, with a note: 'Import a Protect DB snapshot to your standalone device. The previous Protect DB import failed.' The 'Software' section shows a red error for version '3.5.3_202111080345' (Private Cloud Software Version) with an 'Update Software' button. All update check messages indicate they were checked 24 minutes ago and failed.

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



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Home / Operations - Update Device / Update Check Details

The update check failed

Something went wrong while checking for updates.

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

Output

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

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

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

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

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

Download Output

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.



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.

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

La siguiente actualización se inicia automáticamente



⚙ Importing Protect DB deltas.

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

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

Queued Updates



Protect DB

20211116-2135

Queued Protect DB Update Version

20210531-0613

0.80%

Update Progress

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.

✔ 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 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
    
```

Download Output

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.

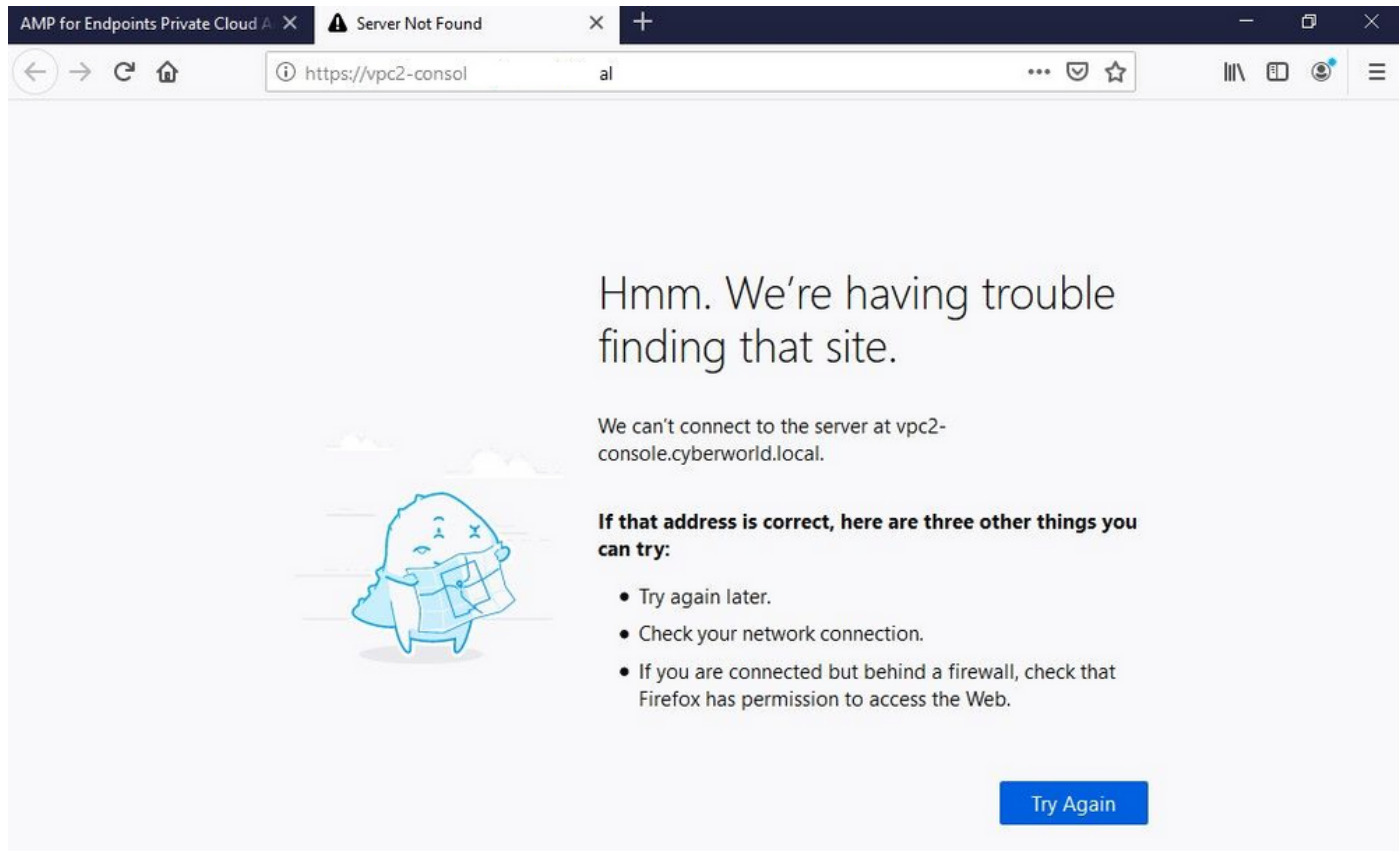
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5>

^^ AIRGAP SOLAMENTE ^^

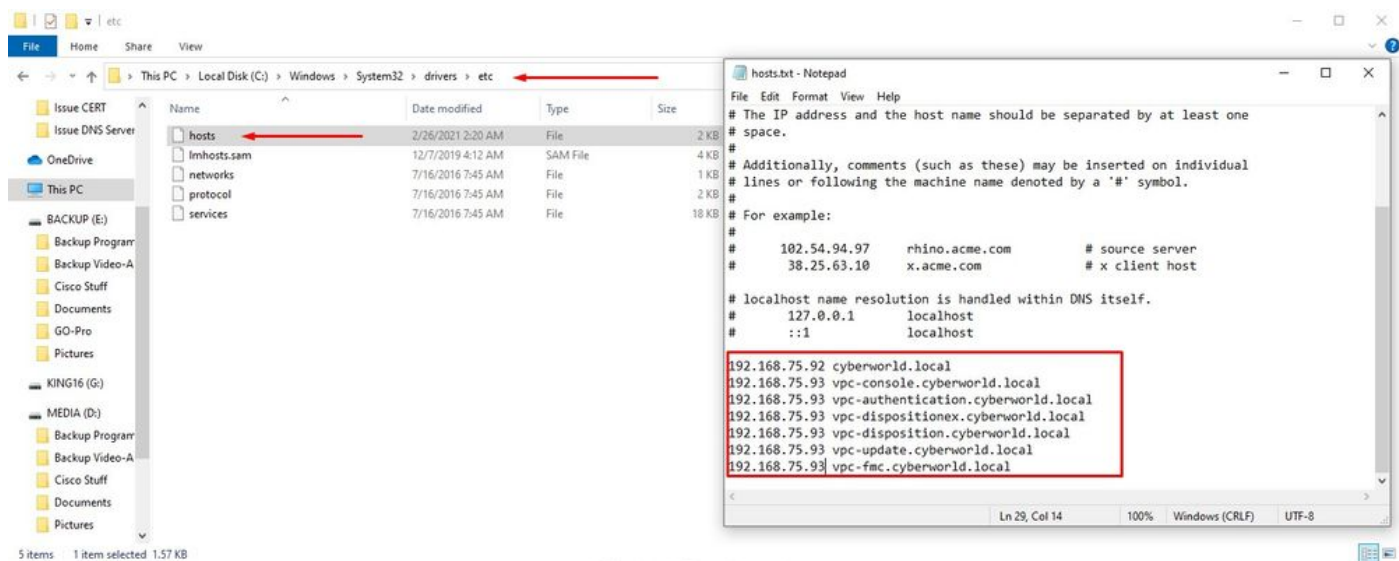
Resolución de problemas básicos

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 3^a imagen a continuación.



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



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

❌ A failure has occurred downloading an installer. Please contact support. ❌

Download Connector

Group ▾

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 +0000, finish 2021-03-02 15:43:00 +0000, duration 0.047382799
===== 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.



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



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.



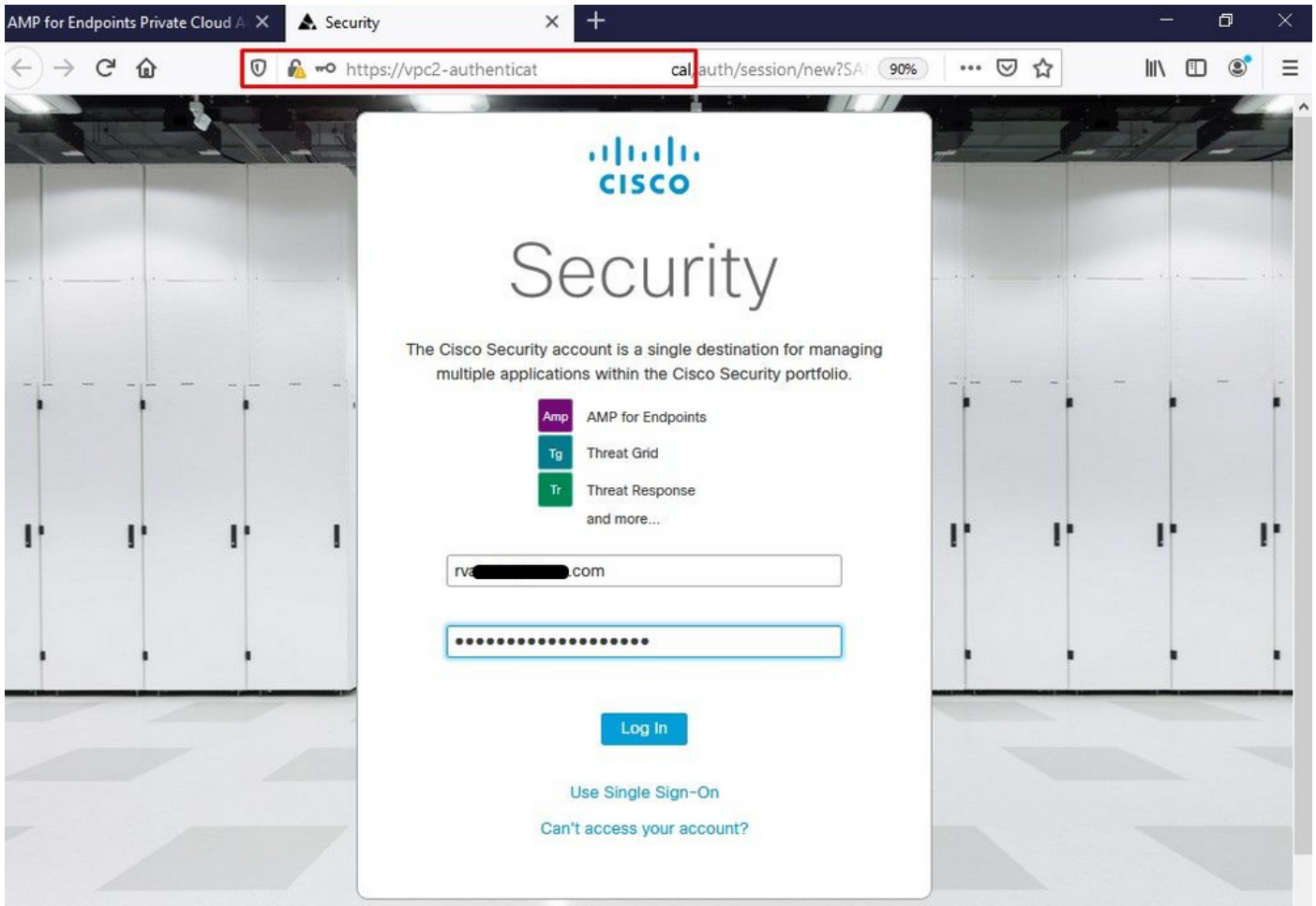
State	Started	Finished	Duration
	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

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

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**.

AMP for Endpoints Private Cloud | Dashboard | <https://vpc-console> | 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.

Descargar conector.

AMP for Endpoints | Roman Valenta

Dashboard | Analysis | Outbreak Control | Management | Accounts

Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

Audit Only	Protect	Triage	Server	Windows Domain Controllers
Used when you're still learning about the product and want to install it without any impact to your existing systems.	Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.	Used when you have a known or suspected infected machine.	Used when you're installing a connector on standard Windows servers.	Installing a connector on Windows Domain Controllers.
Policy Details	Policy Details	Policy Details	Requirements	Requirements
Files Audited	Files Quarantined	Files Quarantined	Files Audited	Files Audited
Network Blocked	Network Blocked	Network Blocked	Network Off	Network Off
Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA
Download	Download	Download	Download	Download

[Back](#) [Next](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

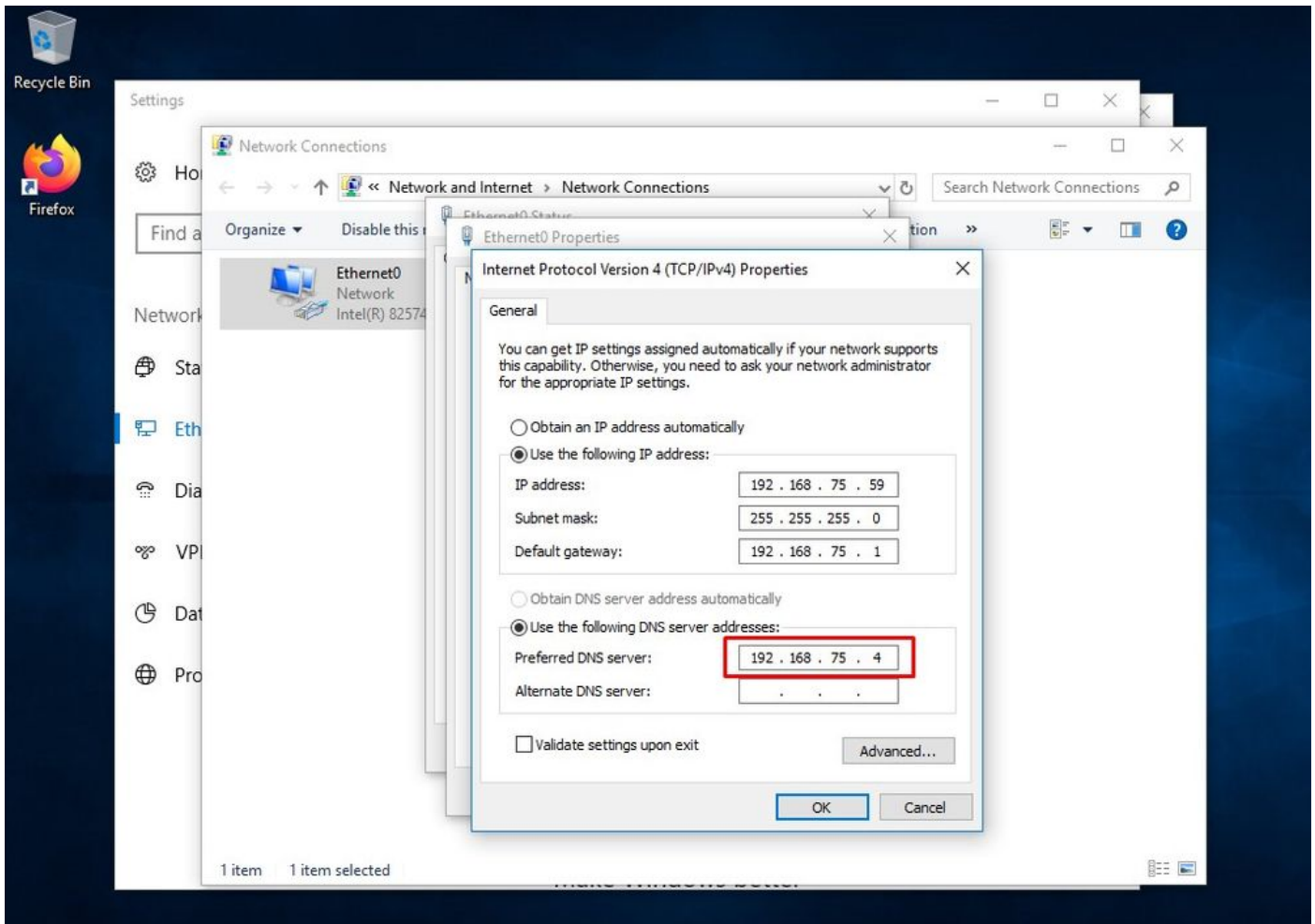
amp_Protect.exe
which is: exe File
from: https://vpc-console.cyberworld.local

Would you like to save this file?

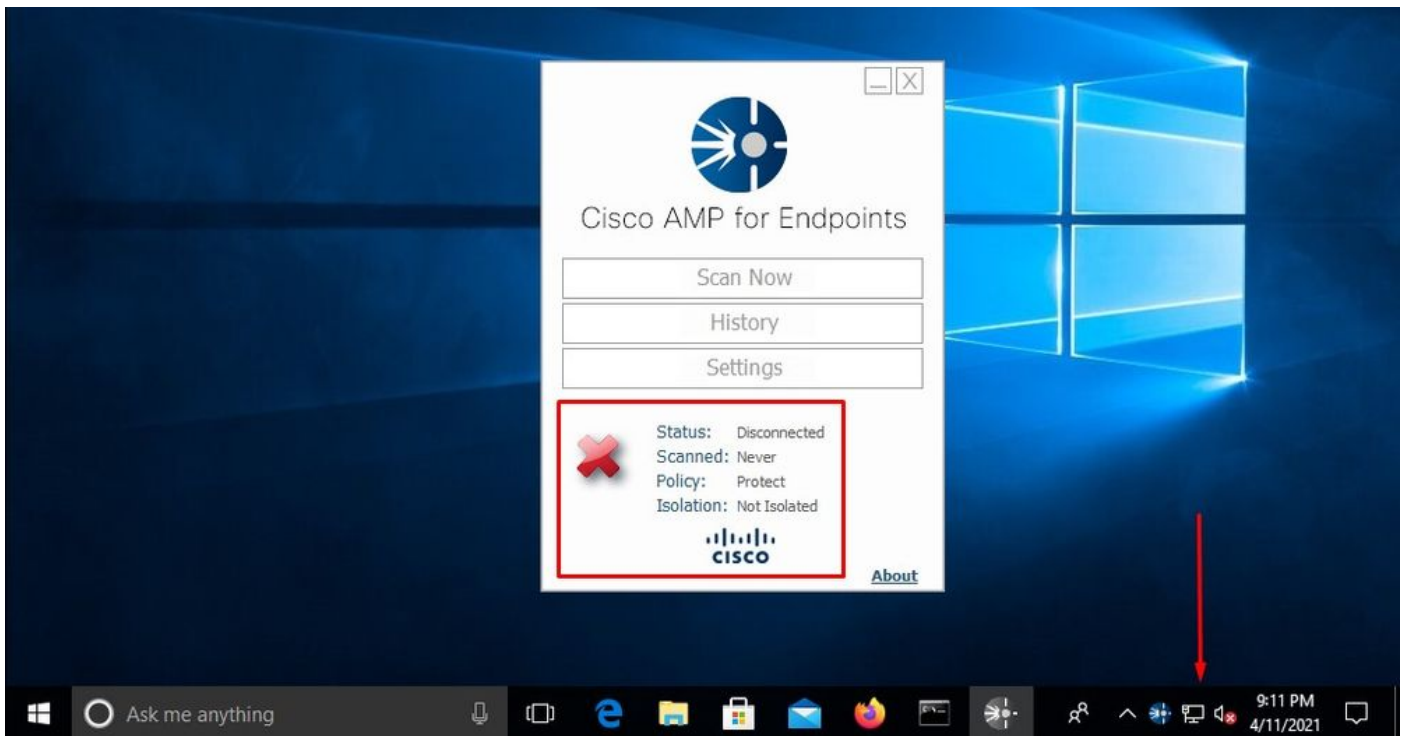
[Save File](#) [Cancel](#)

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.



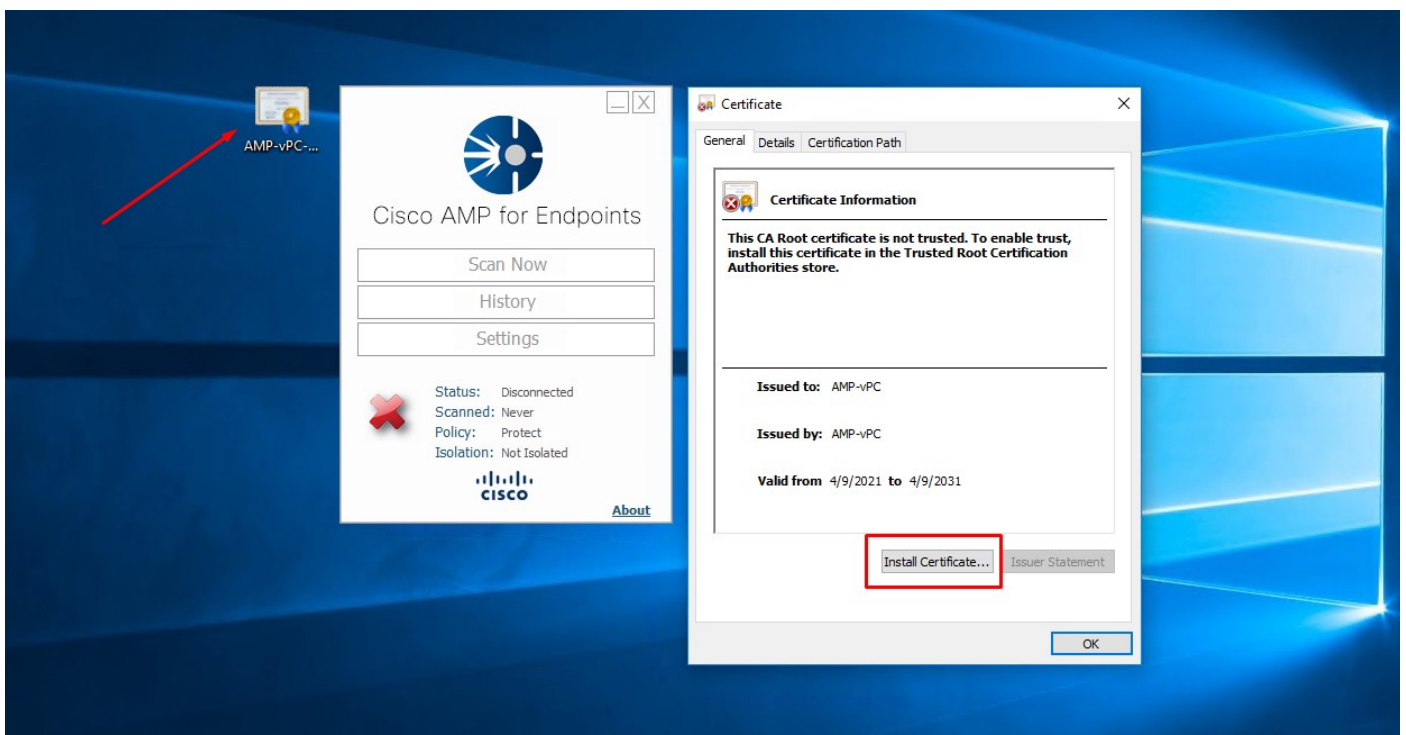
Una vez instalado el conector, el terminal seguro puede considerarse como desconectado. Ejecute el paquete de diagnóstico y revise los registros, podrá determinar el problema.

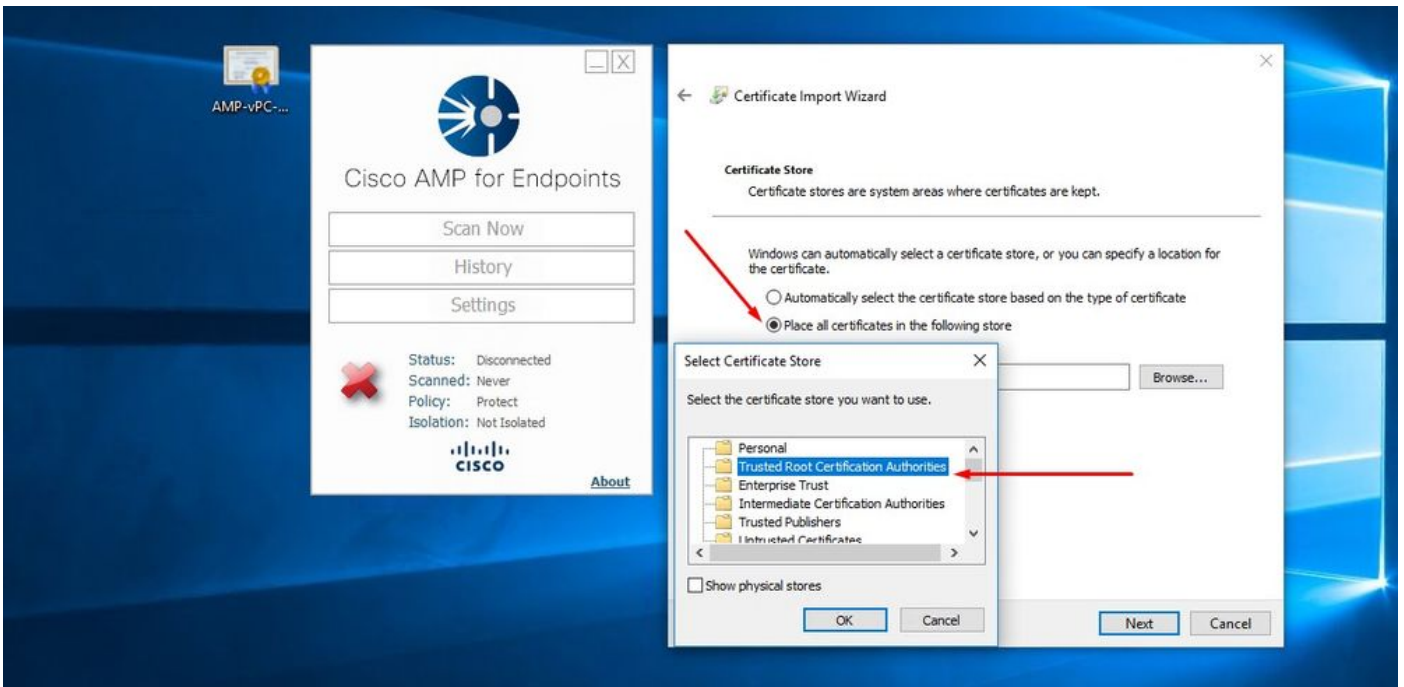
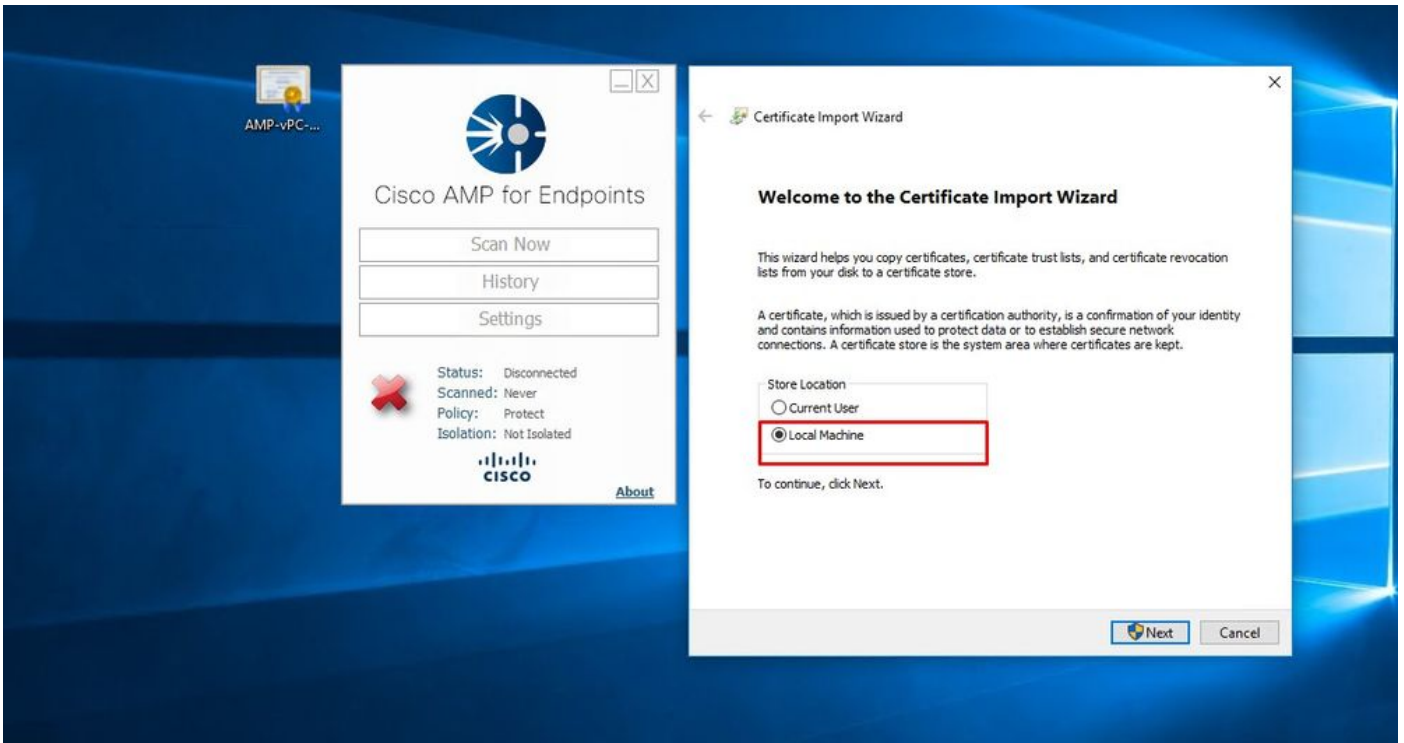


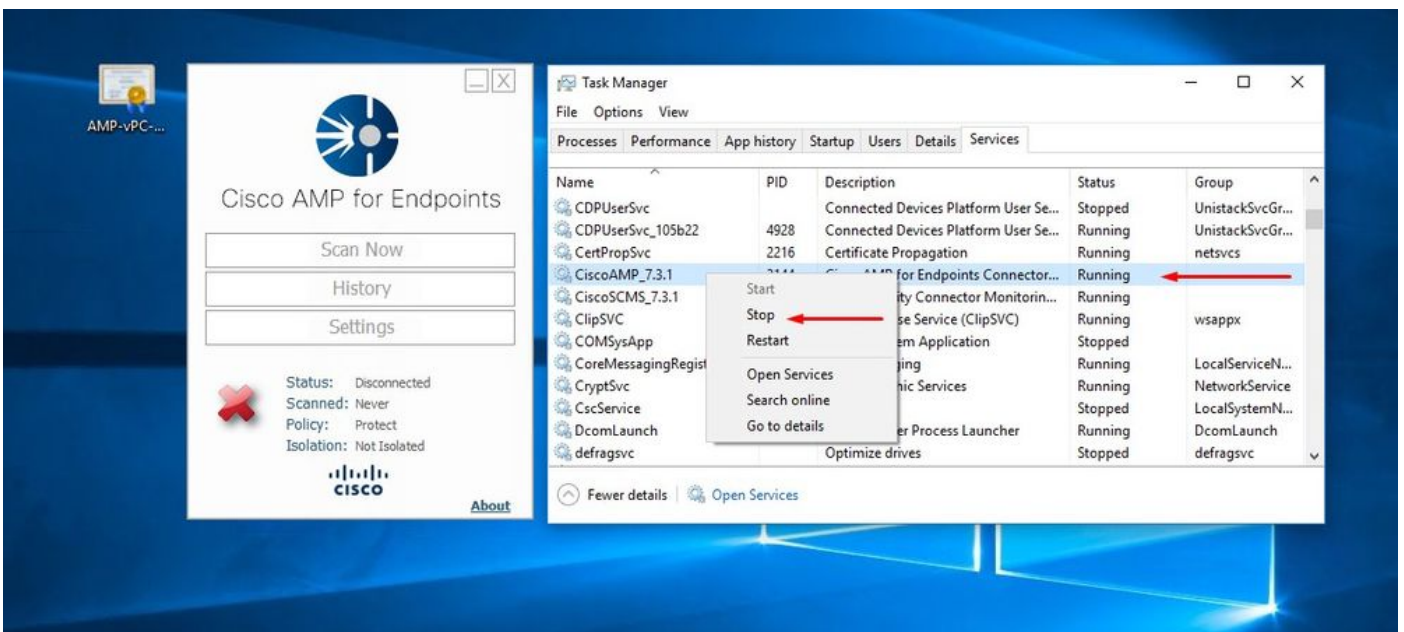
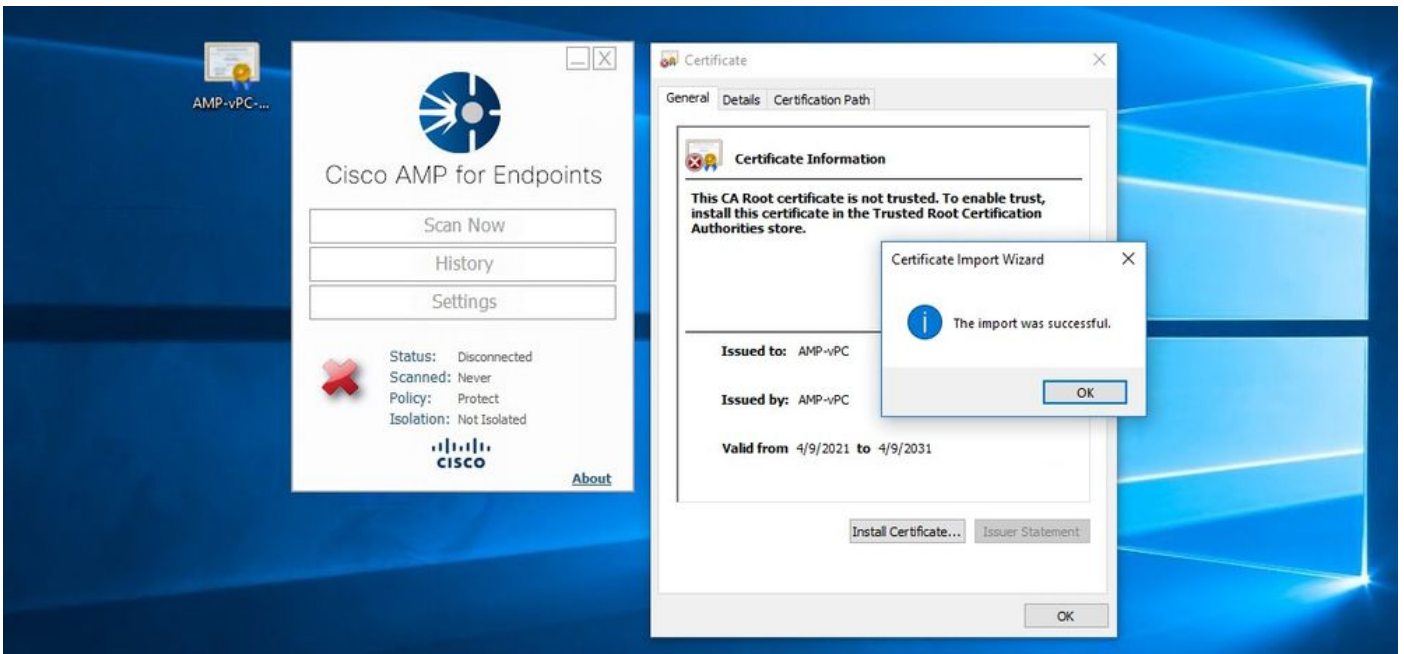
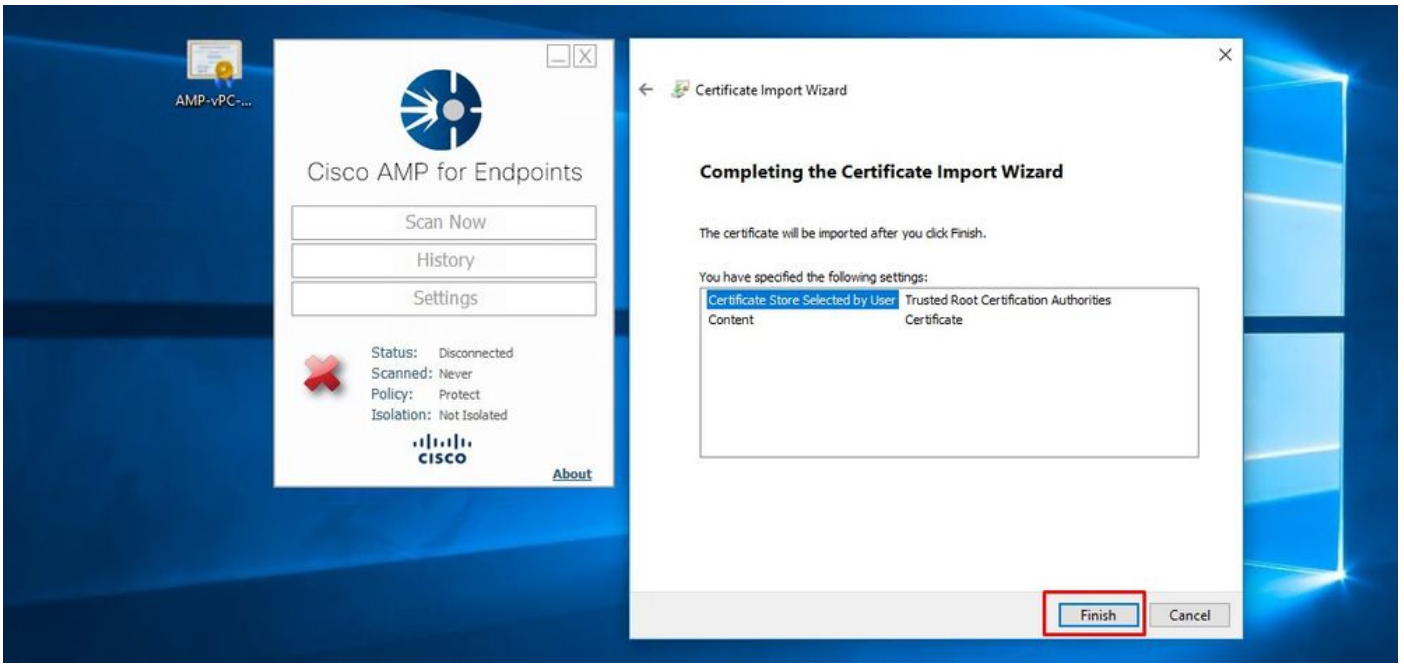
En función de este resultado recopilado del paquete de diagnóstico, puede ver el error de CA raíz

```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworld.local/health failed (60): SSL peer certificate or SSH remote key was not OK (SSL certificate problem: unable to get local issuer certificate) (804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificate or SSH remote key was not OK) to https://vPC-Console.cyberworld.local/health (804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

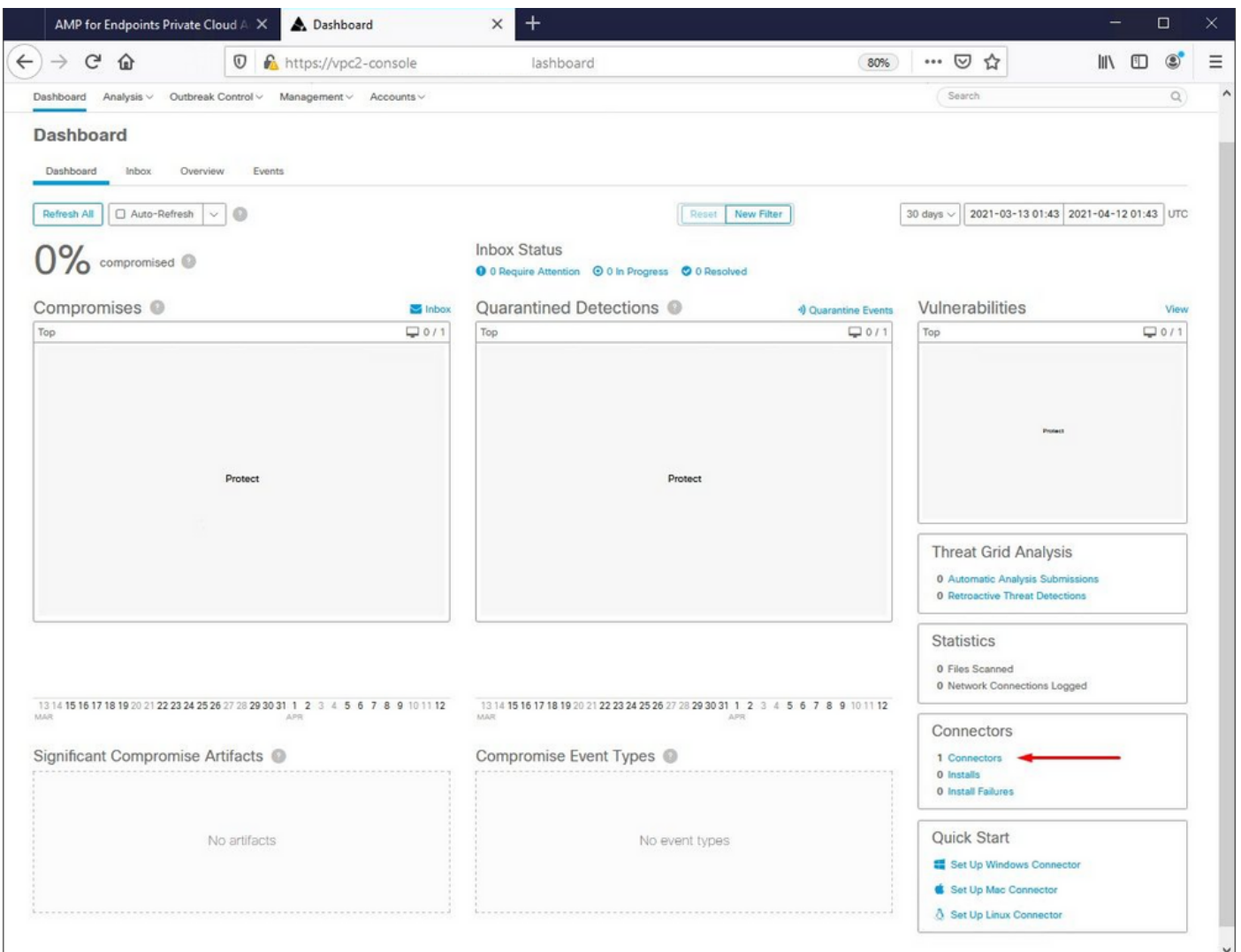
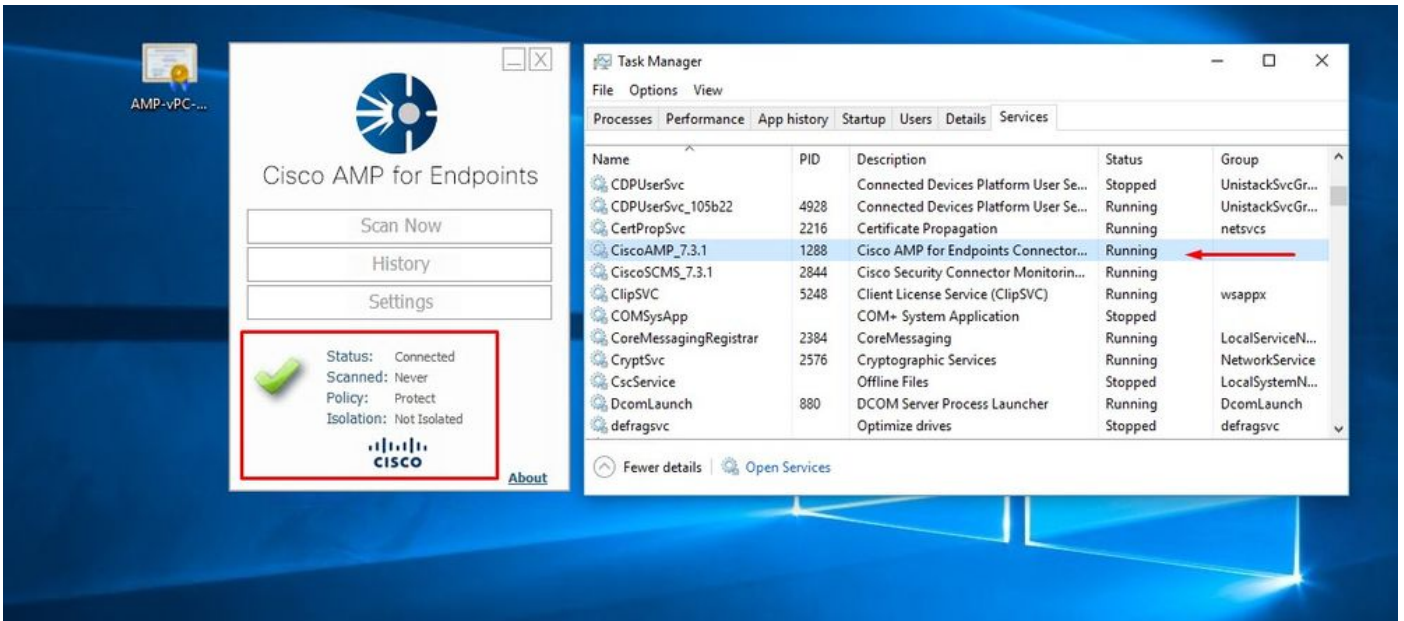
Una vez que haya cargado la CA raíz en el almacén de CA raíz de confianza y reinicie el servicio de punto final seguro. Todo empieza a funcionar como se esperaba.







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



Actividad maliciosa comprobada

AMP for Endpoints Private Cloud A X Dashboard X Download Anti Malware Testfil X +

https://vpc2- /dashboard 80%

AMP for Endpoints Private Cloud A Dashboard

AMP for Endpoints

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

Compromises

Top 0 / 1

Protect

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Quarantined Detections

Top 1 / 1

Protect

Vulnerabilities

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

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

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).