

Vuelva a crear la imagen de AMP Private Cloud PC3000 y restaure la copia de seguridad

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo recrear la imagen del dispositivo de hardware de protección frente a malware avanzado (AMP) de la nube privada en el estado de fábrica y, a continuación, restaurar la copia de seguridad. Si sólo desea volver al estado de fábrica del dispositivo, omita el paso 8 y siga la instalación normal.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PC3000 de nube privada de Cisco AMP
- Acceso de máquina virtual (KVM) basado en el núcleo a través de Cisco Integrated Management Controller (CIMC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco AMP para PC3000 3.1.1
- Navegador cromado para acceder a la consola KVM

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1. Inicie sesión en CIMC. Abra la consola KVM.

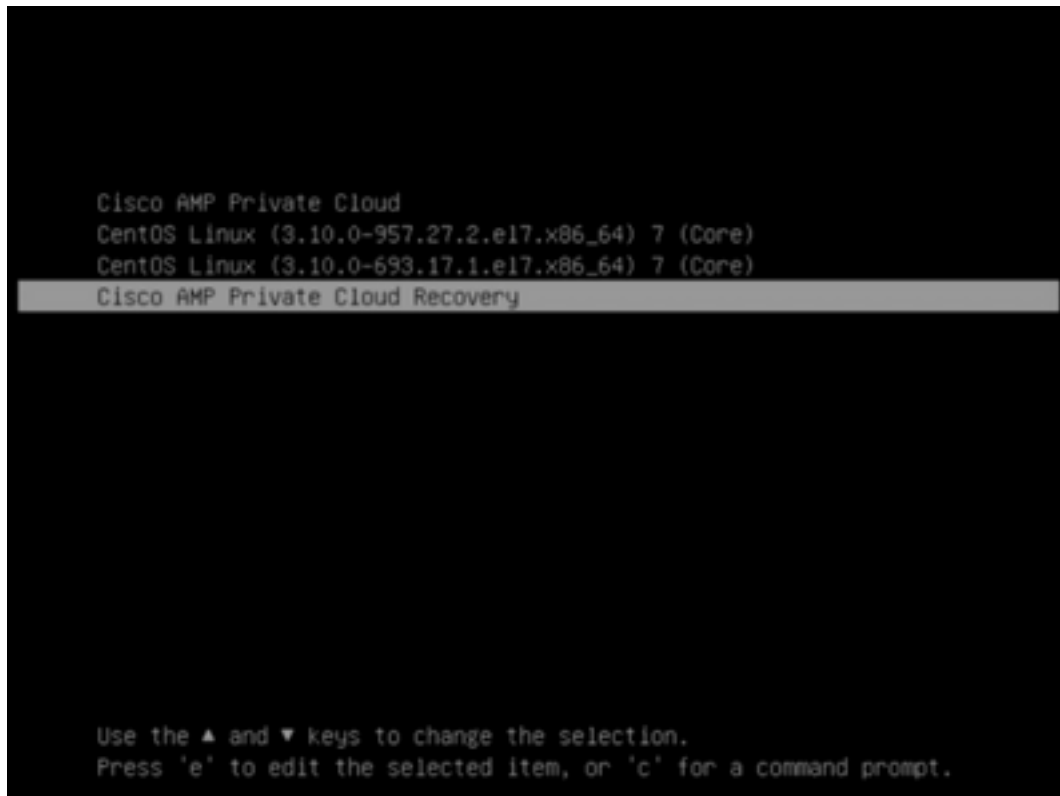
Asegúrese de que las ventanas emergentes están habilitadas para esa página en el explorador.

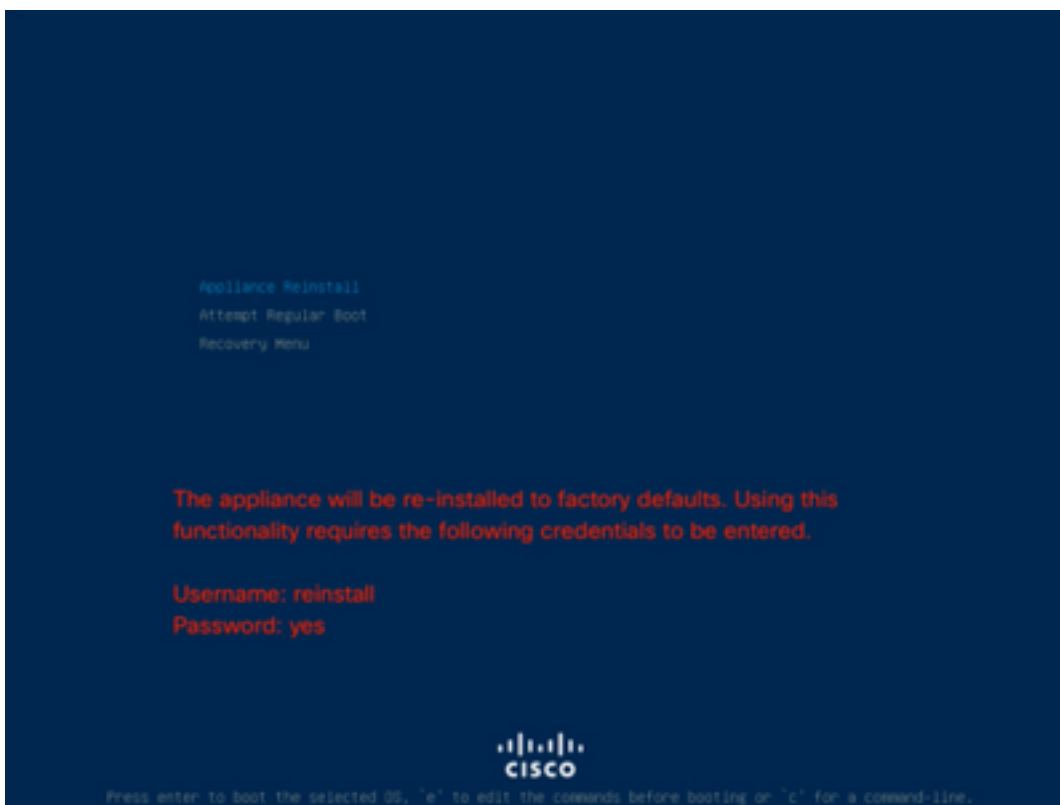
Paso 2. Recargue el dispositivo.

Puede reiniciar el dispositivo mediante el portal de administración, Secure Shell (SSH) o CIMC KVM.

Paso 3. Una vez finalizada la prueba automática de encendido (POST) del sistema de salida de entrada básico (BIOS), aparece el menú GRUB cargador de arranque unificado (GRUB) de GNU:

Seleccione **Cisco AMP Private Cloud Recovery > Appliance Reinstall Options > Appliance Reinstall**.





Paso 4. Introduzca el nombre de usuario y la contraseña.

Nombre de usuario: **reinstalar**

Contraseña **sí**

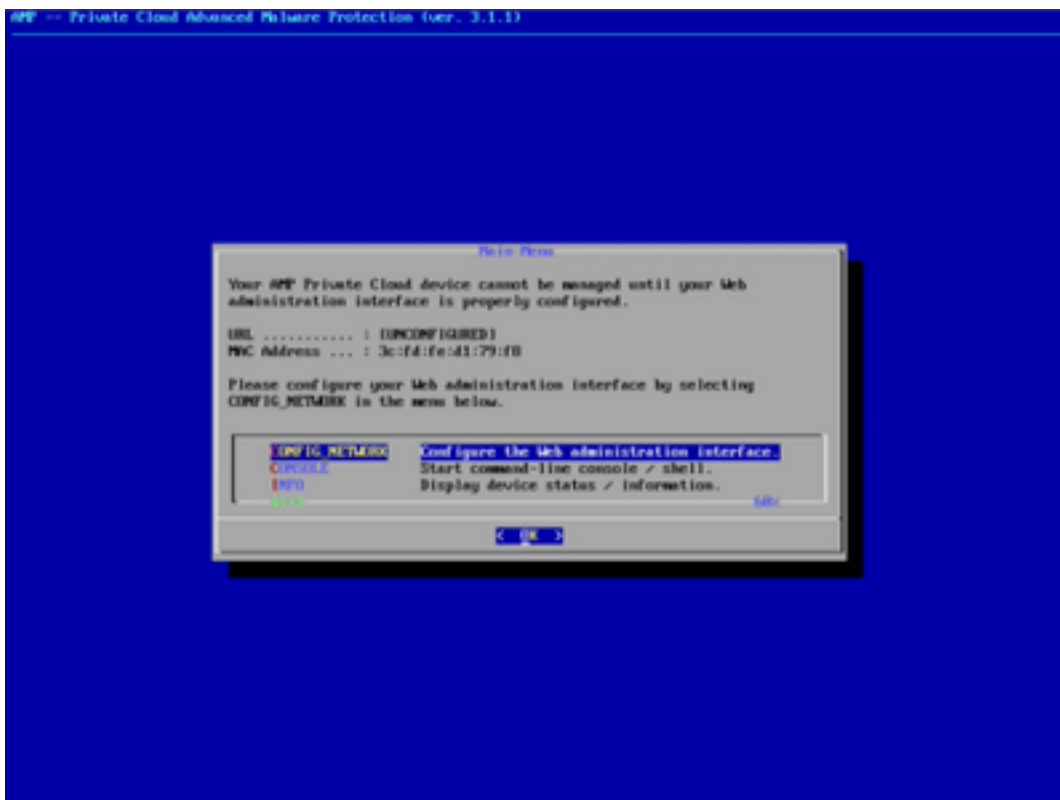
```
Enter username:
reinstall
Enter password:
_
```



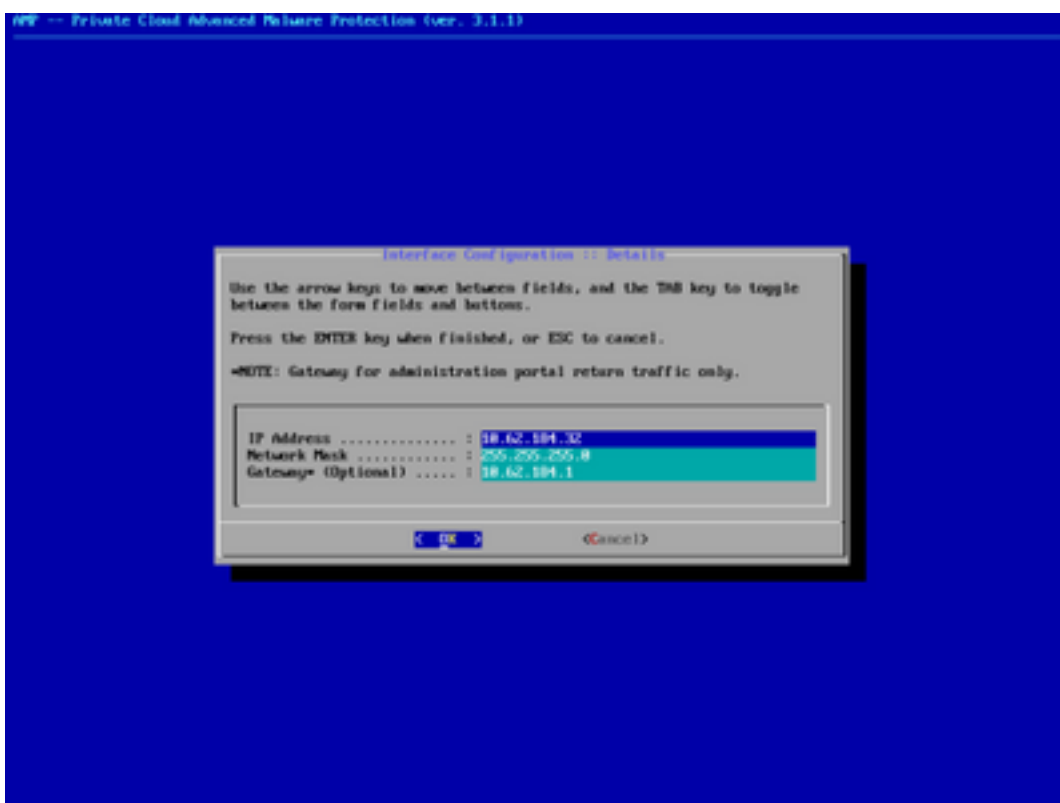
Paso 5. Se inicia la recreación de imágenes y después de la recarga se le presenta el menú inicial.



```
l 11.777038l usbcore: registered new interface driver usbserial_generic
l 11.777038l usbserial: USB Serial support registered for generic
l 11.753899l USB42: FW: No FW/2 controller found. Probing ports directly.
l 11.783337l usb 1-6: new high-speed USB device number 2 using ohci_hcd
l 11.102201l usb 1-6: New USB device found, IDVendor=5a1b, IDProduct=0400
l 11.123101l usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
l 11.130534l usb 1-6: Product: Emulex Flib4 HighSpeed HB
l 11.130533l usb 1-6: Manufacturer: Emulex Communications
l 11.140912l usb 1-6: SerialNumber: 8d9082f0c2
l 11.146133l hub 1-6:1.0: USB hub found
l 11.150654l hub 1-6:1.0: 7 ports detected
l 11.267537l usb 1-7: new high-speed USB device number 3 using ohci_hcd
l 11.270523l USB42: Can't read CTR while initializing USB42
l 11.302622l USB42: probe of USB42 failed with error -5
l 11.303993l mousedev: PS/2 mouse device common for all mice
l 11.311348l rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0
l 11.320472l rtc_cmos 00:00: rtc core: alarm up to max month, yrb, 114 bytes max. 1psr 1r
l 11.325435l intel_pstate: intel P-state driver initializing
l 11.332253l intel_pstate: HWP enabled
l 11.370280l cpuidle: using governor menu
l 11.394827l EFI Variables Facility v0.01 2004-Sep-17
l 11.398265l tsc: refined TSC clocksource calibration: 2593.766 MHz
l 11.399133l Switched to clocksource tsc
l 11.401702l hidraw: *xx_VID_XXXX_XXXX_XX:1101 Busina...
l 11.409674l usbhid: USB HID core driver
l 11.411940l usb 1-7: New USB device found, IDVendor=04b4, IDProduct=0570
l 11.411952l usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
l 11.417953l usb 1-7: Product: USB2.0 Hub
l 11.417941l hub 1-7:1.0: USB hub found
l 11.417942l hub 1-7:1.0: 4 ports detected
l 11.441224l Detected 3 PCI Subspaces
l 11.445423l Registering PCC driver as Mailbox controller
l 11.451900l drbg_core: Initializing network drbg_monitor service
l 11.456276l TUP: cuckoo registered
l 11.462456l Initializing IPv6 netlink socket
l 11.466622l NET: Registered protocol family 10
l 11.472926l NET: Registered protocol family 17
l 11.472940l usb 1-8:1: new high-speed USB device number 4 using ohci_hcd
l 11.481900l nftx_pcc: RTL8125 support
l 11.477773l intel_rdt: Intel RDT SR allocation detected
l 11.505636l sdcmcode: s1p-0x50054, pf-0x00, revision-0x200004d
l 11.513480l sdcmcode: Mmcocode Update Driver: v2.01 cl1qran@ubuntu.com (c) 2013, Peter Grech
```



Paso 6. Configure la red en el submenú CONFIG_NETWORK.



Paso 7. Inicie sesión en el portal OAdmin de AMP con la contraseña del paso 5.



Password Required

Authentication is required to administer your AMP for Endpoints Private Cloud device. The password can be found on the device console of your Private Cloud device.

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

[Password Recovery](#)

Support

Paso 8. Utilice SFTP o SCP para descargar la copia de seguridad desde el servidor remoto a /data/.



Configuration Operations Status Integrations Support

Standalone

Installation Options

Only the Licenses section can be altered after installation.

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

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

- Review and Install

Start Installation

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.

Preparing Restore

Your restore file is being processed, please wait.

- + Adding mongo_event_consumer account.
- + Running startup script to generate new password. Generating a random password for mongo_event_consumer
- + Removing the .rpmnew file
- + Removing event_mongo_store service
- + Adding firehose_cassandra account.
- + Running startup script to generate new password. Generating a random password for firehose_cassandra
- Checking for bios and bmc updates. This may take some time. If an update is available and the update is successful, you will be asked to reboot the box.

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 >

Restore

Local Remote Upload

Restore from a backup file present on the device. Files will be extracted to the directory your backup is located in during the restore process; for this reason, it is recommended that the file be located in the /data directory.

/data/amp.bak

Paso 9. Confirm Hardware Configuration (Confirmar configuración de hardware), haga clic en Next (Siguiente) > Start Installation (Iniciar instalación).

CISCO AMP for Endpoints Private Cloud Administration Portal Help Logout

Configuration Operations Status Integrations Support Standalone

Hardware Configuration

	Installed	Minimum Required
CPU Cores	48	8
Memory	1510 GB	128 GB

Next >

Start Installation

Installation Options

Only the License section can be altered after installation.

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

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 ✓
- > Firewall Management Center ✓

Other

- > 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.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type ✎ Edit

- Standalone Connected**
- Requires 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.

AMP for Endpoints Console Account ✎ Edit

Name	Wojciech Cecot
Email Address	wcecot@cisco.com
Business Name	Cisco - wcecot

Recovery

When restoring from a backup, a recovery image is not required.

Start Installation

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
▶ Pending	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 46 seconds ago	⊙ Please wait...	⊙ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```

[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/os.rb
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -s' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -r' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -v' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -m' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -p' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -o' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'env lscod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0
    
```

Download Output

Paso 10. El reinicio es obligatorio después de la restauración correcta.

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 May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 34 minutes, 19 seconds ago	Tue May 12 2020 10:22:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 17 minutes, 19 seconds ago	0 day, 0 hour, 16 minutes, 59 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2020-05-12T00:22:15+00:00] INFO: Mapping folders of resource table from disk cache
[2020-05-12T00:22:15+00:00] INFO: Running report handlers
[2020-05-12T00:22:15+00:00] INFO: Report handlers complete
[2020-05-12T00:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T00:22:15+00:00] DEBUG: Audit Reports are disabled, skipping sending reports.
[2020-05-12T00:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T00:22:15+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.

=====
Chef run finished successfully
=====

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

Download Output

Verificación

Después de reiniciar el dispositivo, verifique si ambos portales funcionan correctamente. Intente abrir OPadmin y el portal de consola en el navegador web. Ambos portales tardan unos minutos en ser accesibles.

Troubleshoot

En caso de proceso de restauración de respaldo, la contraseña para los portales OPadmin y Console es la misma que antes. De lo contrario, debe utilizar lo que ha configurado en el asistente.