

Procedimiento de actualización de FireAMP Private Cloud 3.0.1

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Requisitos de hardware](#)

[Componentes Utilizados](#)

[Proceso de actualización](#)

[1. Actualizar descarga e instalación](#)

[2. Recolección y cierre de copias de seguridad](#)

[3. Instalación de la nueva versión](#)

[4. Restauración de copia de seguridad](#)

[5. Autoridades de certificados](#)

[6. Servicio de autenticación](#)

[7. Instalación](#)

[8. Comprobaciones posteriores a la actualización](#)

[Cambios en la nube privada virtual 3.0.1](#)

[1. Conector de Windows versión 6.1.7](#)

[2. Servicio de autenticación y autoridades de certificados](#)

Introducción

Este documento describe cómo actualizar una versión 2.4.4 de FireAMP Private Cloud (vPC) a la versión 3.0.1. Tenga en cuenta que el procedimiento de actualización requiere una nueva instancia de máquina virtual para la versión 3.0.1.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Instalación de una Plantilla Open Virtual Appliance (OVA) en VMWare ESXi
- Conocimientos básicos sobre cómo funciona y funciona Virtual AMP Cloud

Requisitos de hardware

A continuación se indican los requisitos mínimos de hardware para la nube privada de FireAMP:

- vSphere ESX 5 o superior

- 8 CPU
- 64 GB de RAM
- Espacio en disco libre de 1 TB en el almacén de datos de VMWare
- Tipo de unidades: SSD requerida
- Tipo de RAID: Un grupo RAID 10 (banda de espejos)
- Tamaño mínimo del almacén de datos de VMware: 1 TB
- Lecturas aleatorias de almacenamiento de datos mínimo para el grupo RAID 10 (4K): 60 000 IOPS
- Escrituras aleatorias de almacenamiento de datos mínimo para el grupo RAID 10 (4K): 30 000 IOPS

Precaución: El OVA de nube privada crea las particiones de unidad, por lo que no es necesario especificarlas en VMWare.

Nota: Consulte la [Guía del usuario de la nube privada de FireAMP](#) para obtener más información sobre los requisitos de hardware.

Componentes Utilizados

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

- FireAMP Private Cloud 2.4.4
- FireAMP Private Cloud 3.0.1
- VMWare ESXi 5.0 o superior

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. If your network is live, make sure that you understand the potential impact of any command.

Proceso de actualización

Esta sección proporciona instrucciones paso a paso sobre cómo recopilar la copia de seguridad de la versión 2.4.4 de FireAMP Private Cloud y cómo restaurarla correctamente en la versión 3.0.1 de FireAMP Private Cloud.

Precaución: El proceso de actualización puede introducir un tiempo de inactividad en su entorno. Los conectores (que incluyen AMP para redes conectadas a su nube privada virtual) que utilizan la nube privada pueden perder la conectividad a la nube virtual y pueden tener una funcionalidad dañada debido a ello.

1. Actualizar descarga e instalación

Asegúrese de que la nube privada virtual 2.4.4 de FireAMP está actualizada.

Paso 1. Vaya a **Operaciones** -> **Actualizar dispositivo** en el Portal del administrador.

Paso 2. Haga clic en el botón **Comprobar/Descargar actualizaciones**, como se muestra en la imagen, para asegurarse de que su nube privada virtual FireAMP, desde donde se realiza la

recopilación de copias de seguridad, está actualizada (en cuanto a contenido y software).

The screenshot shows the fireAMP Private Cloud Administration Portal interface. At the top, there is a navigation bar with the fireAMP logo and the text "Private Cloud Administration Portal". To the right of the logo are links for "Support", "Help", and "Logout". Below the navigation bar is a menu with "Configuration", "Operations", "Status", "Integrations", and "Support". A message at the top reads "Updates keep your Private Cloud device up to date." Below this message is a button labeled "Check/Download Updates" which is highlighted with a red box. The main content area is divided into two sections: "Content" and "Software". Under "Content", there is a version number "2.4.4_1528990794" with the subtitle "Client Definitions, DFC, Tetra Content Version" and a blue "Update Content" button. Under "Software", there is a version number "2.4.4_1528991036" with a green checkmark icon, the subtitle "Private Cloud Software Version", and an orange "Update Software" button. Below the software version, it says "Checked 43 minutes ago; software is up to date."

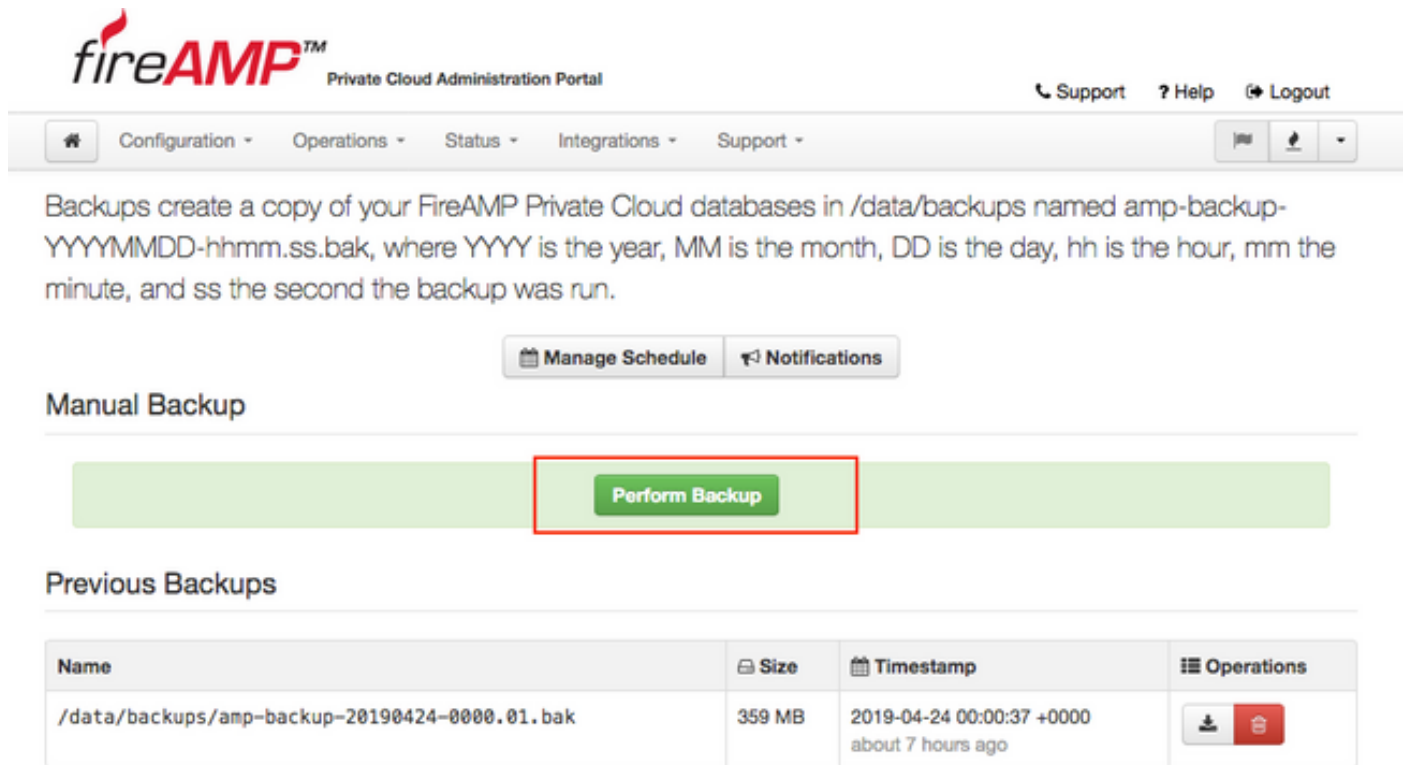
Paso 3. Una vez instaladas las actualizaciones de contenido y software, la página de actualización muestra la información de que el dispositivo está actualizado, como se muestra en la imagen.

This screenshot shows the same fireAMP Private Cloud Administration Portal interface as the previous one, but with updated information. The "Check/Download Updates" button is now greyed out. In the "Content" section, the version number is "2.4.4.20190424060125" with the subtitle "Client Definitions, DFC, Tetra Content Version" and a blue "Update Content" button. Below the content version, it says "Checked 1 minute ago; content is up to date." In the "Software" section, the version number is "2.4.4_1528991036" with a green checkmark icon, the subtitle "Private Cloud Software Version", and an orange "Update Software" button. Below the software version, it says "Checked 35 minutes ago; software is up to date."

2. Recolección y cierre de copias de seguridad

Paso 1. Vaya a **Operaciones** -> **Copias de seguridad**.

Paso 2. En la sección Copia de seguridad manual, haga clic en el botón **Realizar copia de seguridad**. El procedimiento inicia una creación de copia de seguridad.



fireAMP™ Private Cloud Administration Portal

Support ? Help Logout

Configuration Operations Status Integrations Support



Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications

Manual Backup

Perform Backup

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 7 hours ago	 

Paso 3. Cuando el proceso finaliza correctamente, aparece la notificación correcta, como se muestra en la imagen.

The backup was successful.

Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications





Manual Backup


Perform Backup

Last Manual Backup Successful

Backup Job Details

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0825.43.bak	352 MB	2019-04-24 08:26:18 +0000 less than a minute ago	 
/data/backups/amp-backup-20190424-0800.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 8 hours ago	 

Paso 4. Haga clic  para abrir el Navegador. Asegúrese de que la copia de seguridad se descargue correctamente y se guarde en una ubicación segura.

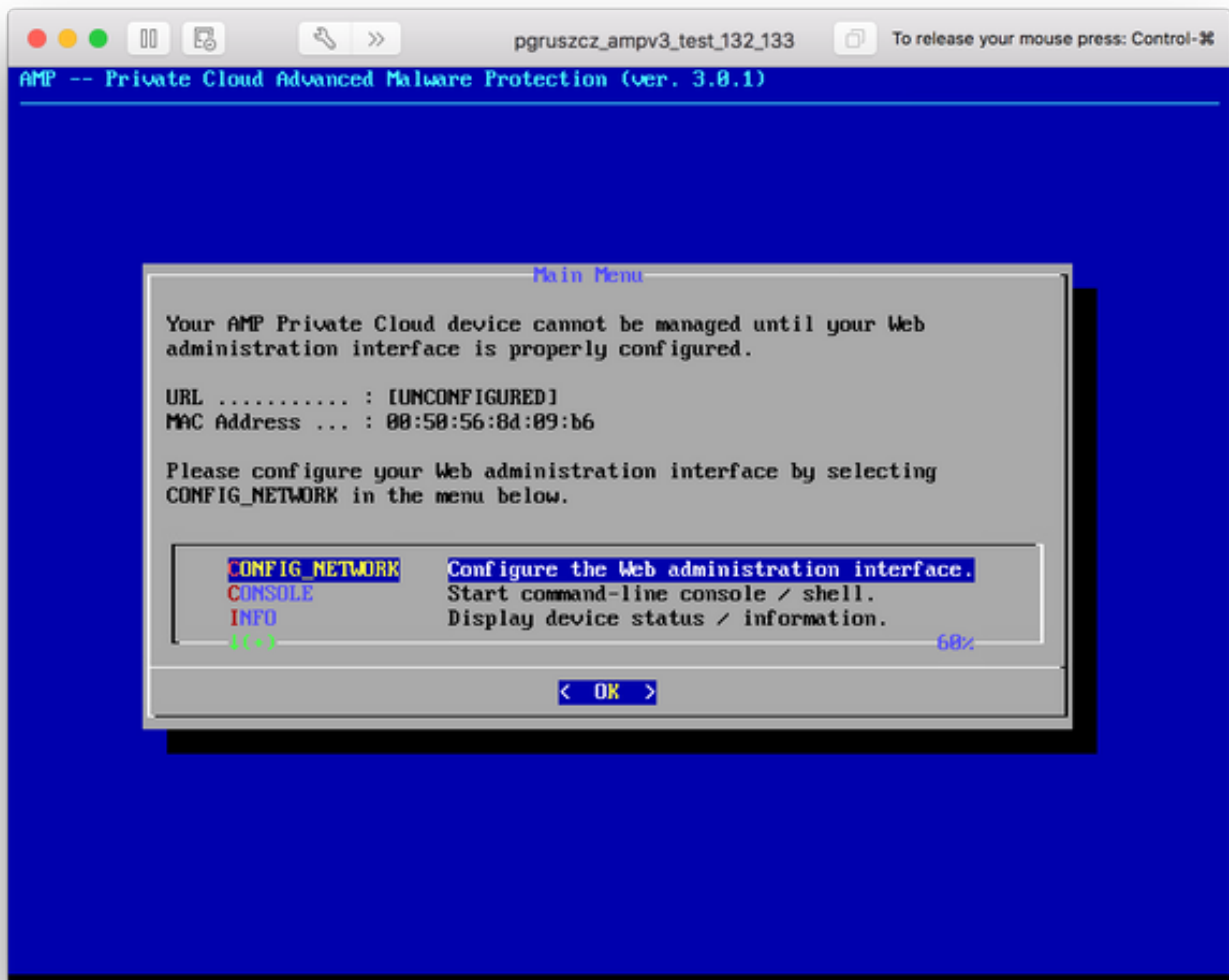
3. Instalación de la nueva versión

En esta sección se asume que la máquina virtual para la nube privada virtual FireAMP 3.0.1 ya está implementada. El procedimiento de instalación de la máquina virtual para OVA 3.0.1 en VMWare ESXi se puede encontrar en el enlace: [Implemente un archivo OVA en un servidor ESX.](#)

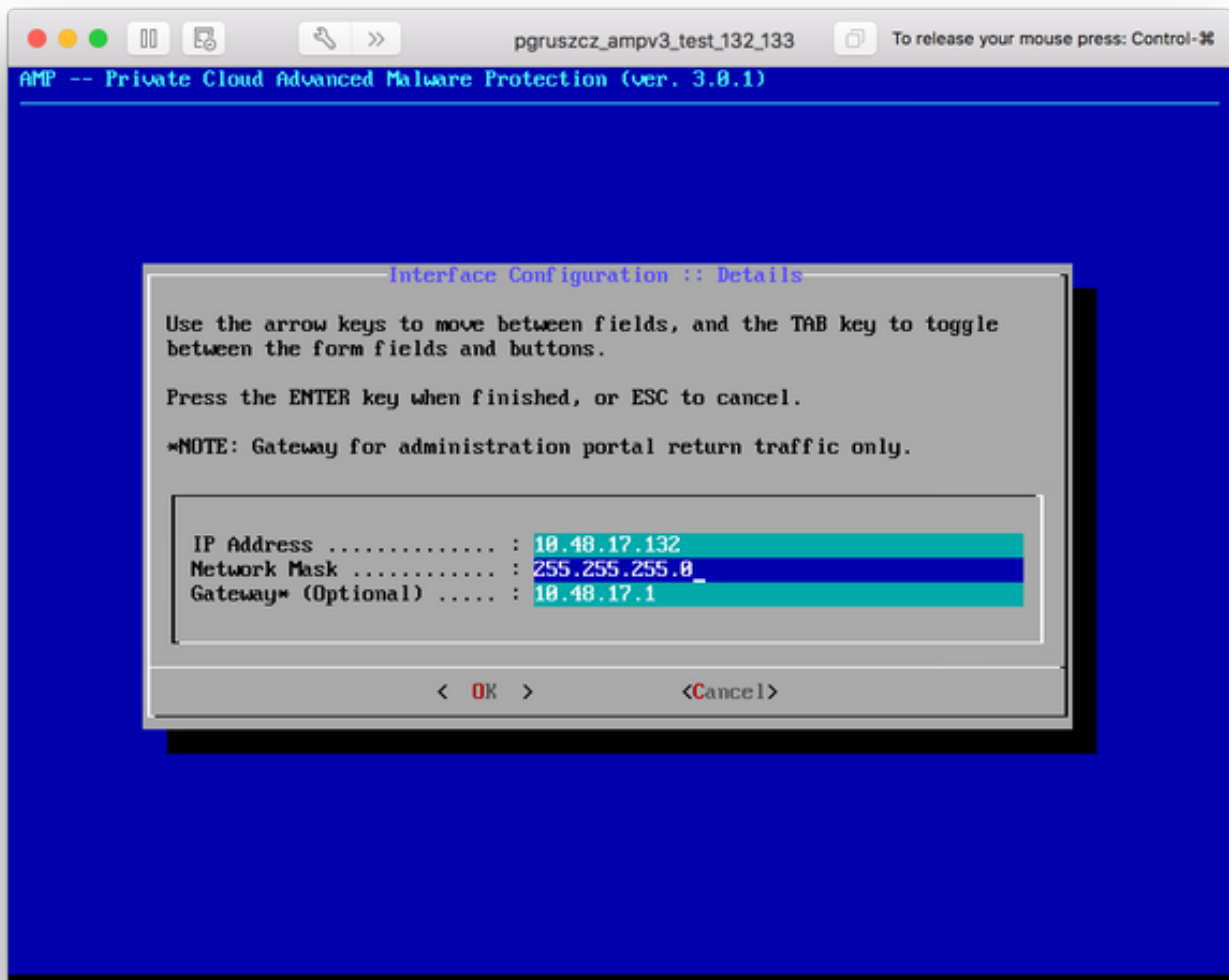
Nota: El procedimiento presentado en el artículo utiliza exactamente los mismos nombres de host y direcciones IP para FireAMP Virtual Private Cloud 2.4.4 y 3.0.1. Cuando siga esta guía, debe cerrar FireAMP Virtual Private Cloud 2.4.4 después de recopilar la copia de seguridad.

Paso 1. Abra el terminal de la consola para la instancia de la máquina virtual recién creada con la versión 3.0.1 instalada. Puede navegar por las **teclas Tab, Enter y arrow.**

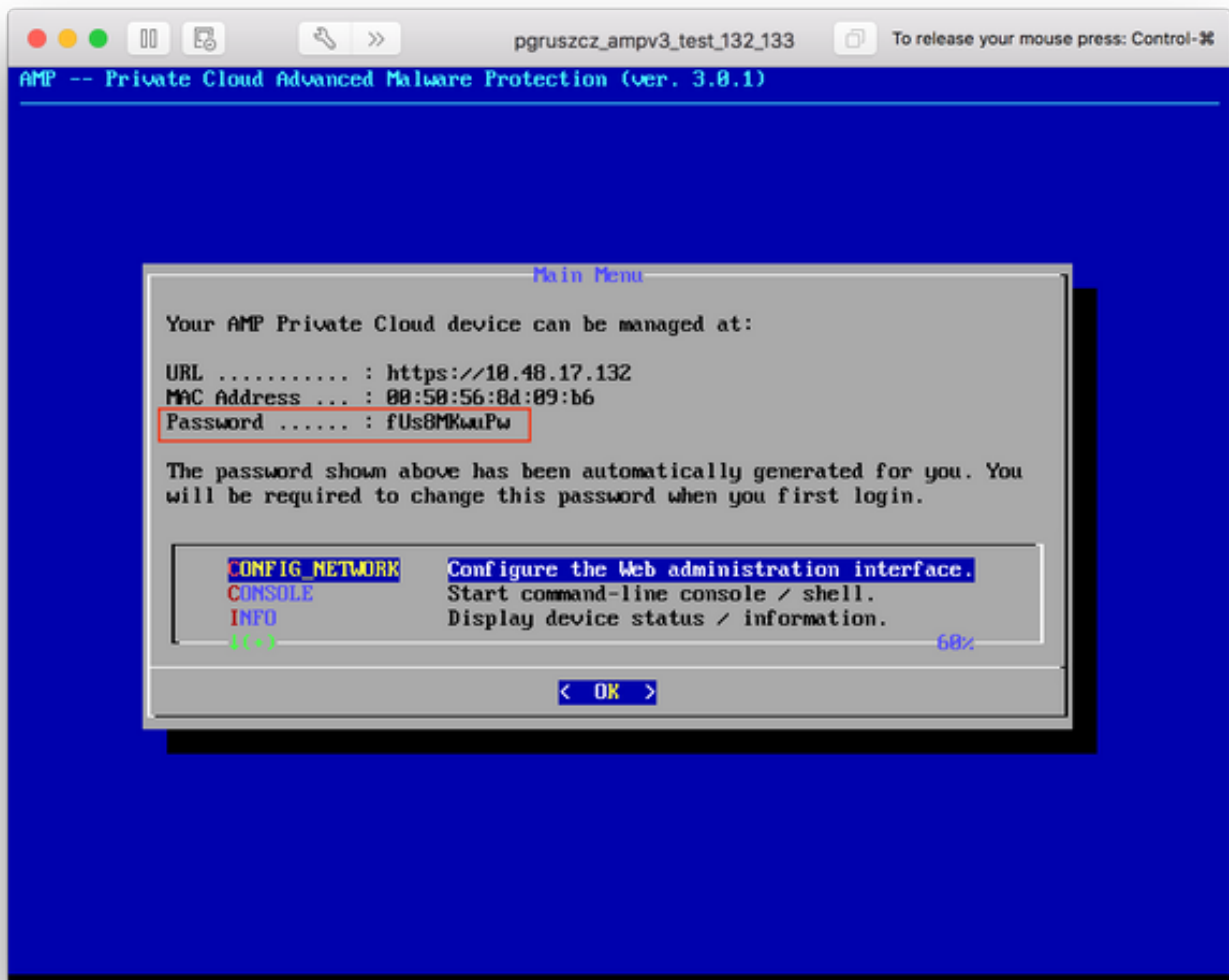
Paso 2. Navegue hasta **CONFIG_NETWORK** y haga clic en la tecla **Intro** del teclado para comenzar la configuración de la dirección IP de administración para la nube privada de FireAMP. Si no desea utilizar DHCP, seleccione **No** y presione **Intro**.



Paso 3. Ingrese la dirección IP, la máscara de red y la puerta de enlace predeterminada. Navegue hasta **Aceptar**, como se muestra en la imagen. Pulse la tecla **Intro**.



Paso 4. El cambio en la configuración de la red requiere un reinicio de la interfaz. Después del reinicio, reaparece el menú de consola principal, como se muestra en la imagen. Esta vez verá una dirección IP en la línea de URL. Tenga en cuenta que se muestra la **contraseña** inicial. Se trata de una contraseña de una sola vez (a la que posteriormente se hace referencia como **contraseña inicial**) que se utiliza en la configuración basada en Web.



Paso 5. Abra un navegador web y navegue hasta la dirección IP de administración del dispositivo. Recibe un error de certificado, ya que FireAMP Private Cloud genera inicialmente su propio certificado HTTPS. Configure su navegador para confiar temporalmente en el certificado autofirmado de la nube privada de FireAMP.

Paso 6. Aparece una pantalla para introducir una contraseña, como se muestra en la imagen. Utilice la **contraseña inicial** de la consola. Haga clic en **Login**.



Password Required

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

Login

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

Support

Paso 7. Después de iniciar sesión correctamente, debe cambiar la contraseña. Utilice la **contraseña inicial** de la consola en el campo **Contraseña antigua**. Utilice su nueva contraseña dos veces en los campos **New Password**. Haga clic en **Cambiar contraseña**.

The screenshot shows the FireAMP Private Cloud Administration Portal. At the top left is the fireAMP logo and the text "Private Cloud Administration Portal". At the top right are links for "Support", "Help", and "Logout". Below the header is a navigation menu with "Configuration", "Operations", "Status", "Integrations", and "Support". A yellow warning box at the top left says "Password Expired". The main content area has a heading "Change the password used to access the FireAMP Private Cloud Administration Portal and the device console. Note that this is also the root password for your device." Below this is another yellow warning box: "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." There are three password input fields, each with a "Q" icon on the left. Below the fields is a green "Change Password" button.

4. Restauración de copia de seguridad

Paso 1. La página de bienvenida del portal de administración presenta dos formas de instalación de la nube virtual de FireAMP 3.0.1, como se muestra en la imagen.

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 2. Puede elegir uno de los tres métodos diferentes para cargar el archivo de copia de seguridad en la instancia de nube privada virtual de FireAMP creada recientemente:

Local: restaura la configuración de un archivo de copia de seguridad ya presentado en el dispositivo (debe colocar el archivo en el dispositivo a través de SFTP o SCP). Los archivos se extraen al directorio correcto una vez que comienza el proceso de restauración. Por esta razón, se recomienda el directorio /datos.

Remoto: restaura desde un archivo en un servidor HTTP accesible de forma remota.

Cargar: restaura el archivo cargado por el explorador. Funciona sólo si el archivo de copia de seguridad es inferior a 20 MB.

En este ejemplo, se eligió la opción remota.

Nota: Se debe permitir una conectividad adecuada para el servidor HTTP. Es necesario poder acceder al archivo de copia de seguridad desde la perspectiva de la nube privada.

Haga clic en el botón **Start** para continuar con la restauración, como se muestra en la imagen.

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 from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

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 from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

Paso 3. El procedimiento de restauración de una copia de seguridad reemplaza la configuración actual. Se sustituyen las claves de host SSH del dispositivo y la contraseña del Portal de administración. Puede revisar partes de su configuración con respecto a la instalación.

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.

Preparing Restore

Your restore file is being processed, please wait.

```
portal/fireAMP/linux/1.7.0.545/rhel/7/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/rhel/6
portal/fireAMP/linux/1.7.0.545/rhel/6/ciscoampconnector-1.7.0.545-1.el6.x86_64.rpm
portal/fireAMP/linux/1.7.0.545/rhel/6/fireamp-linux.tar.gz
portal/fireAMP/linux/1.7.0.545/rhel/6/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/update.xml
portal/fireAMP/protectent
portal/fireAMP/protectent/REVISION
portal/fireAMP/protectent/5.1.15.10683
portal/fireAMP/protectent/5.1.15.10683/installer-32-tcp.exe
```

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

Start >

Paso 4. Después de una copia correcta del archivo de copia de seguridad, la página de restauración presenta un mensaje emergente como se muestra en la imagen. Haga clic en el botón **Reconfigure Administration Portal Now** para finalizar el procedimiento de restauración.

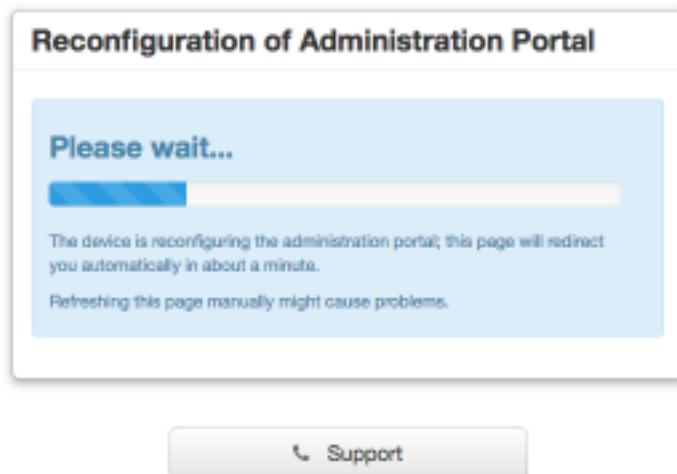


Reconfiguration of Administration Portal

Reconfiguration of the Administration Portal must be performed to update authentication configuration and certificates.

Reconfigure Administration Portal Now

Support



Paso 5. Una vez finalizada la reconfiguración, se muestra de nuevo la página del portal de administración, como se muestra en la imagen. A partir de ahora, para iniciar sesión, debe utilizar la contraseña de la copia de seguridad de la nube privada virtual de FireAMP 2.4.4.

La imagen muestra la mayor parte del trabajo realizado para la instalación correcta (marcas de verificación). Se espera ya que la copia de seguridad restaure la configuración desde FireAMP Virtual Private Cloud 2.4.4.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > FireAMP 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.

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.

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

Start >

5. Autoridades de certificados

La versión 3.0.1 de FireAMP para nube privada virtual presenta nuevas características y comportamientos en lo que respecta al funcionamiento del sistema. Estos deben configurarse y completarse antes de poder iniciar la instalación.

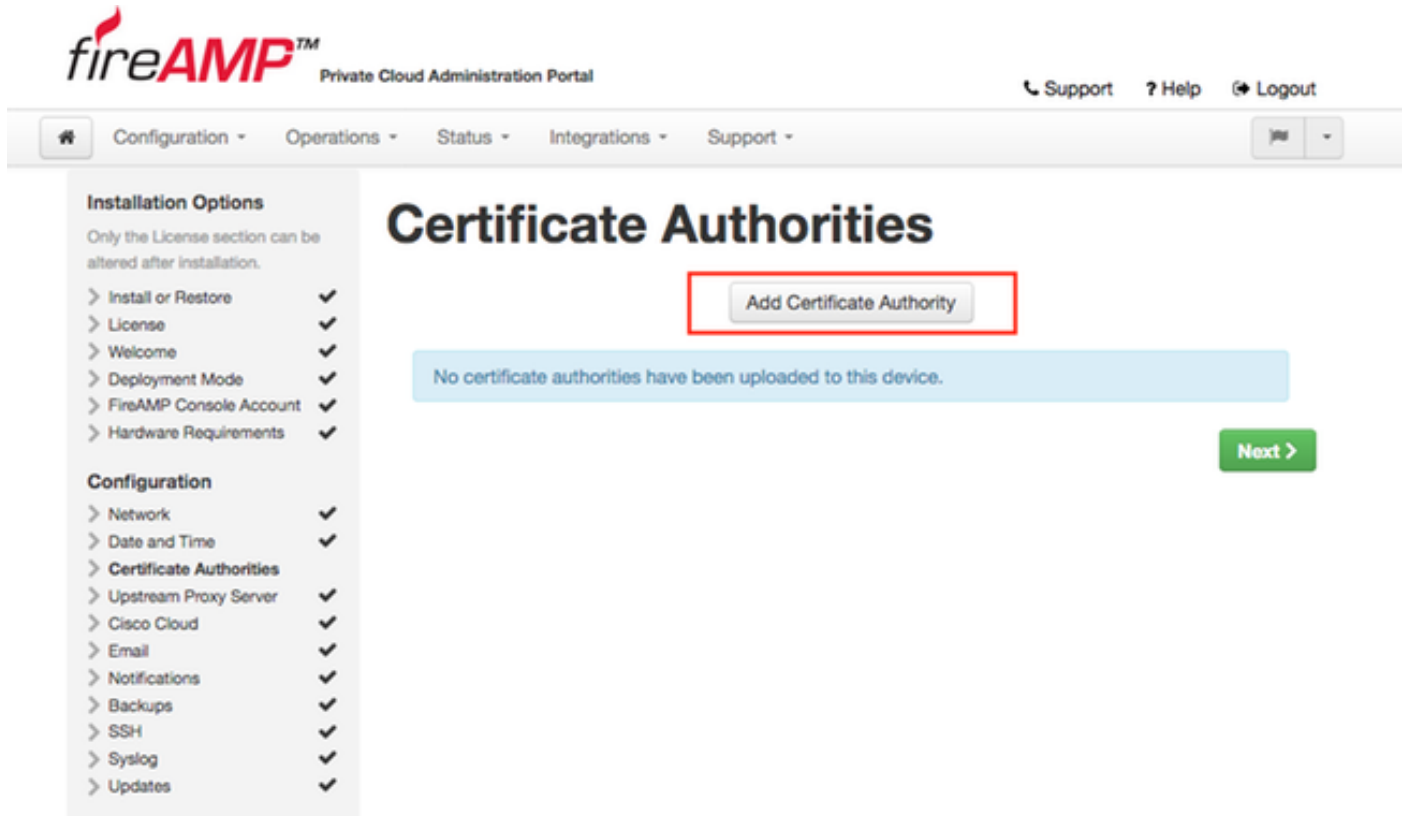
El primer componente que es nuevo y no estaba presente en la versión anterior son **Autoridades de Certificados**.

La página **Autoridades de certificados** permite administrar certificados raíz para sus servicios si desea utilizar una autoridad de certificados personalizada. Si es necesario, puede descargar o eliminar el certificado raíz.

Nota: El almacén de confianza de las autoridades certificadoras se utiliza sólo para los servicios de nube virtual (para crear y validar la cadena de certificados adecuada). No se utiliza para varias integraciones de vPC, como ThreatGrid.

Paso 1. Vaya a la sección **Configuración** -> **Autoridades de Certificados** del panel **Opciones de**

Instalación. Haga clic en el botón **Add Certificate Authority**, como se muestra en la imagen.



Paso 2. Haga clic en **Agregar raíz de certificado**, como se muestra en la imagen, para cargar el certificado. Todos los requisitos enumerados deben cumplirse para que la nube privada virtual acepte el certificado.

Nota: Durante el procedimiento de actualización, debe agregar el **certificado raíz** utilizado para firmar el **certificado de servicio de autenticación**, explicado en la siguiente sección.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Paso 3. Una vez actualizado el certificado, haga clic en el botón **Cargar**, como se muestra en la imagen, para cargar el certificado.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Si utiliza cualquier autoridad de certificados subordinada para firmar cualquier certificado de servicio, cárguelo también en esta sección.

Precaución: Incluso si genera un certificado autofirmado para el servicio de autenticación,

asegúrese de que se cargue en la sección Autoridad de certificados antes de ir a los siguientes pasos.

6. Servicio de autenticación

El segundo componente que se agrega en la versión 3.0.1 y no se importa de la copia de seguridad, es **Authentication** en la sección Services.

El servicio de **autenticación** se utilizará en futuras versiones de la nube privada para manejar las solicitudes de autenticación de usuarios. Se agrega en la versión 3.0.1 para compatibilidad futura.

Paso 1. Vaya a la sección **Servicios** -> **Autenticación** del panel **Opciones de instalación**. Introduzca un **nombre de host de autenticación** único, la entrada DNS especificada en la sección nombre de host debe configurarse correctamente en el servidor DNS y apunta a la dirección IP de la interfaz de la consola de nube privada virtual .

The screenshot displays the FireAMP Private Cloud Administration Portal interface. The main heading is "Authentication Configuration". A red box highlights the "Authentication Hostname" field, which contains the text "authentication.amptest.pgruszczy.com". To the right of this field is a "HELP" button and a checked "Validate DNS Name" checkbox. Below this, the "Authentication Certificate" section features a "Replace Certificate" button and a light blue message box stating "No certificate has been provided for this service." At the bottom right of the configuration area, there is a green "Next >" button. The left sidebar contains a navigation menu with sections: "Installation Options" (including Install or Restore, License, Welcome, Deployment Mode, FireAMP Console Account, and Hardware Requirements), "Configuration" (including Network, Date and Time, Certificate Authorities, Upstream Proxy Server, Cisco Cloud, Email, Notifications, Backups, SSH, Syslog, and Updates), and "Services" (including Authentication, FireAMP Console, Disposition Server, Extended Protocol, Disposition Update Service, and Firepower Management Center). The "Authentication" option under Services is currently selected.

Paso 2. Una vez que se especifica el nombre de host y se puede resolver correctamente, haga clic en el botón **Reemplazar certificado**, como se muestra en la imagen.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Authentication Configuration

Authentication Hostname HELP

Validate DNS Name

Authentication Certificate Replace Certificate

No certificate has been provided for this service.

Next >

Nota: Si necesita ayuda con la generación de certificados, visite el artículo: [Cómo Generar y Agregar Certificados que se Requieren para la Instalación de AMP VPC 3.x En Adelante](#) para obtener más información sobre los Requisitos de Hardware.

Paso 3. Haga clic en el botón **Elegir certificado** para cargar el certificado del servicio de autenticación, como se muestra en la imagen.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management ✓
- > Center ✓

Other

- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

HELP

authentication.amptest.pgruszc.com

Validate DNS Name

Authentication Certificate

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.

🔑 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.

private.key

+ Choose Key

authentication_serv

+ Choose Certificate

Next >

Paso 4. El siguiente paso es cargar el archivo de clave privada para el certificado. Para agregarlo, haga clic en el botón **Elegir clave**.

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

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

authentication.amptest.pgruzszz.com Validate DNS Name

Authentication Certificate 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.	

private.key + Choose Key

authentication_serv + Choose Certificate

[Next >](#)

Paso 5. Debe asegurarse de que se cumplen todos los requisitos antes de continuar con el siguiente paso. Se cumplen los requisitos resaltados si el certificado raíz utilizado para firmar el servicio de autenticación se coloca correctamente en el almacén de autoridades de certificados.

Precaución: Puede cambiar los nombres de host para todos los demás Servicios en esta etapa solamente. Una vez finalizada la instalación, no se puede cambiar el nombre de host de los servicios. Más adelante sólo podrá cambiar los certificados. Debe asegurarse de comprender el riesgo de tal operación. Si cambia los nombres de host de los servicios que utilizan los conectores o AMP para los dispositivos de red, pueden tener problemas para comunicarse con la nube una vez que se complete la actualización.

7. Instalación

Paso 1. Una vez que se haya completado cada sección y se haya marcado como válida, comenzará la instalación. Vaya a la sección **Revisar e instalar** y haga clic en el botón **Iniciar**

instalación, como se muestra en la imagen.

fireAMP™ Private Cloud Administration Portal

Support ? Help Logout

Configuration - Operations - Status - Integrations - Support -

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

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

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower 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

Cloud Proxy

- Requires an Internet connection and communication with FireAMP 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.

FireAMP Console Account

Edit

Name	Piotr Gruszczynski
Email Address	pgruszcz@ciseco.com
Business Name	Cisco - pgruszcz

Recovery

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

Start Installation

Paso 2. El portal de administradores le presenta el estado actual, la fecha de inicio y los registros. Si encuentra algún error o problema que requiera atención, recopile los registros haciendo clic en el botón **Descargar salida**, como se muestra en la imagen, y adáptelos al caso TAC.

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	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 1 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 1c2c8f5383551c7c76409b59eec5833923094af0c69d8d967a552c3d47f2a609
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] updated content
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] owner changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] group changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] mode changed to 644
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] not queuing delayed action run on execute[reset_policy_network_items] (delayed), as it's already been queued
[2019-04-26T11:55:10+00:00] INFO: Processing template[/opt/fire/amp/portal/config/virtual/config_items.chef.yml] action create (fireamp-portal::config_chef line 70)
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 06c8c02083c15cab1270ec1e3e62c593d5627a387793cce53ae290817d555b1c
```

Download Output

Paso 3. Cuando la instalación se realiza correctamente, debe reiniciar el dispositivo para finalizar el proceso. Haga clic en el botón **Reboot** para continuar con el procedimiento de reinicio, como se muestra en la imagen.

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	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 10 minutes, 23 seconds ago	Fri Apr 26 2019 14:03:57 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 28 seconds ago	0 day, 0 hour, 9 minutes, 54 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
un (/opt/fire/chef/cookbooks/daemontools/providers/service.rb line 148)
[2019-04-26T12:03:39+00:00] INFO: execute[/opt/fire/embedded/bin/svc -t /service/fireamp-haproxy] ran successfully
[2019-04-26T12:03:39+00:00] INFO: template[/opt/fire/amp/portal/db/migrate/20190426120103_update_license_summary_2019
0426120051.rb] sending run action to execute[run_migrate_license_summary] (delayed)
[2019-04-26T12:03:39+00:00] INFO: Processing execute[run_migrate_license_summary] action run (fireamp-onprem::license
line 142)
[2019-04-26T12:03:57+00:00] INFO: execute[run_migrate_license_summary] ran successfully
[2019-04-26T12:03:57+00:00] INFO: Chef Run complete in 186.283958188 seconds
[2019-04-26T12:03:57+00:00] INFO: Running report handlers
[2019-04-26T12:03:57+00:00] INFO: Report handlers complete
Sending system notification (this may take some time).
Registration against the FireAMP Disposition Server has previously succeeded.
```

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

Download Output

Paso 4. Después del procedimiento de reinicio, puede iniciar sesión en el Portal **Administrador** y en el Portal **de Consola**. El procedimiento de actualización ha finalizado.

8. Comprobaciones posteriores a la actualización

Una vez reiniciado el dispositivo, asegúrese de que la restauración se haya completado correctamente:

Paso 1. Compruebe si los conectores pueden comunicarse con el dispositivo virtual 3.0.1 recientemente instalado.

Paso 2. Asegúrese de que los objetos Events, Device Trajectory y Computers se restauran correctamente y se presentan en el portal de la consola.

Paso 3. Si dispone de AMP para integraciones de red como FMC, ESA, WSA se asegura de que puedan comunicarse con el servidor de disposición de archivos.

Paso 4. Compruebe si hay actualizaciones de Contenido/Software (Operaciones -> Dispositivo de actualización) y continúe con la instalación de dichas actualizaciones.

Se recomienda realizar pruebas para garantizar una actualización correcta.

Cambios en la nube privada virtual 3.0.1

1. Conector de Windows versión 6.1.7

La nube privada 3.0.1 se envía con la versión 6.1.7 de Windows Connector, puede encontrar la documentación al respecto en el enlace: [Notas de la versión 6.1.7](#)

Precaución: Si ha realizado algún cambio en los certificados, asegúrese de que antes de realizar una actualización o instalación a la versión 6.1.7 de Windows Connector, los certificados utilizados para los servicios de nube privada son de confianza en el propio terminal. La confianza debe estar en el nivel del equipo, no en el del usuario. Si no se cumple esta condición, los conectores no confían en el certificado presentado por la nube privada que los mantiene en estado desconectado.

2. Servicio de autenticación y autoridades de certificados

Los cambios se describieron minuciosamente en la guía del usuario para 3.0: [Guía del usuario de la nube privada](#).

Autoridades de certificados le permite administrar certificados raíz para sus Servicios si desea utilizar una autoridad de certificados personalizada. Si es necesario, puede descargar o eliminar el certificado raíz.

El servicio de **autenticación** se utilizará en futuras versiones de la nube privada para manejar las solicitudes de autenticación de usuarios. Se agrega en la versión 3.0.1 para compatibilidad futura.