paloalto
TECHDOCS

Administración de dispositivos WildFire

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

August 23, 2023

Table of Contents

Descripción general del dispositivo WildFire

WildFire™ proporciona detección y prevención del malware de día cero utilizando una combinación de análisis dinámico y estático para detectar amenazas y crear protecciones para bloquear el malware. WildFire amplía las capacidades de los cortafuegos de nueva generación de Palo Alto Networks para identificar y bloquear el malware de destino y desconocido.

Acerca del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire ofrece una nube privada local WildFire, lo que permite analizar archivos sospechosos en un entorno aislado sin necesidad de que el cortafuegos quite los archivos de la red. Para utilizar el dispositivo WildFire para albergar una nube privada de WildFire, configure el cortafuegos para que envíe muestras al dispositivo WildFire para análisis. El dispositivo WildFire aísla todos los archivos localmente y los analiza para detectar actividad sospechosa utilizando el mismo motor utilizado por la nube pública de WildFire. En pocos minutos, la nube privada devuelve los resultados del análisis a los logs de **WildFire Submissions (envíos de WildFire)** del cortafuegos.

La Administración de WildFire Appliance cubre la instalación y configuración del dispositivo WildFire, pero comparte gran parte del diseño operativo y las capacidades con la nube pública de WildFire. Para obtener más información sobre las capacidades de análisis de WildFire, consulte la Administración avanzada de WildFire.

Puede habilitar un dispositivo WildFire para lo siguiente:

- ❑ Generar localmente antivirus y firmas DNS para el malware descubierto, y asignar una categoría URL a enlaces malintencionados. Entonces, puede habilitar cortafuegos conectados para recuperar las firmas y categorías URL más recientes cada cinco minutos.
- ❑ Envío de malware a la nube pública de WildFire. La nube pública de WildFire vuelve a analizar la muestra y genera una firma para detectar el malware. Esta firma puede estar disponible en minutos para proteger a usuarios globales
- ❑ Enviar informes de malware generados localmente (sin enviar el contenido básico de la muestra) a la nube pública de WildFire, para contribuir a las estadísticas de malware y la inteligencia contra amenazas.

Puede configurar hasta 100 cortafuegos de Palo Alto Networks, cada uno con suscripciones válidas de WildFire para que realicen reenvíos a un mismo dispositivo WildFire. Más allá de las suscripciones de cortafuegos WildFire, no se necesita ninguna suscripción WildFire adicional para habilitar la implementación de una nube privada de WildFire.

Puede gestionar dispositivos WildFire utilizando la CLI del dispositivo local o puede realizar la Gestión de dispositivos WildFire con Panorama centralmente. A partir de PAN-OS 8.0.1, también puede agrupar dispositivos WildFire en clústeres de dispositivos WildFire y gestionar los clústeres localmente o desde Panorama.

Nube privada de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En una implementación de nube privada de Palo Alto Networks, los cortafuegos de Palo Alto Networks reenvían archivos a un dispositivo WildFire de su red corporativa que se utiliza para alojar una ubicación de análisis de nube privada. Una nube privada de WildFire puede recibir y analizar archivos de hasta 100 cortafuegos de Palo Alto Networks.

Debido a que la nube privada de WildFire es un espacio aislado local, las muestras benignas, de grayware y phishing que analiza nunca salen de su red. De manera predeterminada, la nube privada tampoco envía el malware fuera de la red; sin embargo, puede optar por enviar automáticamente el malware a la nube pública de WildFire, para la generación de firmas y su distribución. En este caso, la nube pública de WildFire vuelve a analizar la muestra, genera una firma para identificar la muestra y distribuye la firma a todos los cortafuegos de Palo Alto Networks con suscripciones WildFire o de prevención de amenazas.

Si no desea que la nube privada de WildFire envíe incluso muestras malintencionadas fuera de su red, usted puede:

- Habilitar el dispositivo WildFire para reenviar el informe de malware (y no la propia muestra) a la nube pública de WildFire. Los informes de WildFire proporcionan información estadística que ayuda a Palo Alto Networks a evaluar la penetración y propagación del malware. Si desea información más detallada, consulte Envío de malware o informes desde el dispositivo WildFire.
- Cargue archivos manualmente al portal de WildFire en lugar de reenviar automáticamente todo el malware o utilice la API de WildFire para enviar archivos a la nube pública de WildFire.

También puede Habilitación de firmas locales y generación de categorías URL en el dispositivo WildFire. Las firmas generadas por el dispositivo WildFire se distribuyen a los cortafuegos conectados, de modo que los cortafuegos puedan bloquear eficazmente el malware la próxima vez que se detecte.

Los archivos Android Application Package (APK) y MAC OSX no son compatibles con el análisis de la nube privada de WildFire.

Nube híbrida de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Un cortafuegos en una implementación de nube híbrida de WildFire puede reenviar ciertas muestras a las nubes públicas de WildFire alojadas en Palo Alto Networks y otras muestras a una nube privada de WildFire alojada en un dispositivo WildFire. Una implementación de nube híbrida de WildFire ofrece la flexibilidad para analizar documentos privados localmente y dentro de la red, mientras que la nube pública de WildFire analiza los archivos obtenidos de Internet. Por ejemplo, reenvíe datos asociados con la Industria de Medios de Pago (PCI) e Información de Salud Protegida (PHI) exclusivamente a la nube privada de WildFire para el análisis, y envíe portables ejecutables (PE) a la nube pública de WildFire para su análisis. En una implementación de nube híbrida de WildFire, la descarga de archivos en la nube pública para su análisis le brinda la ventaja de un veredicto rápido para los archivos que se procesaron anteriormente en la nube pública de WildFire, y también libera la capacidad del dispositivo WildFire para procesar contenido confidencial. Además, puede reenviar ciertos tipos de archivos a la nube pública de WildFire que actualmente no son compatibles con el análisis del dispositivo WildFire, tal como los archivos del Paquete de Aplicaciones de Android (Android Application Package, APK).

En una implementación de nube híbrida de WildFire, es posible que haya casos en los que archivo coincida con sus criterios de análisis de nube pública y de análisis de nube privada; en estos casos, el archivo se envía únicamente a la nube privada para el análisis como una medida preventiva.

Para configurar el reenvío de nube híbrida, consulte Reenviar archivos para el análisis del dispositivo WildFire.

Interfaces de dispositivos WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Los dispositivos WF-500 cuentan con cuatro puertos Ethernet RJ-45 ubicados en la parte posterior del dispositivo. Estos puertos tienen la etiqueta **MGT**, **1**, **2** y **3**, y corresponden a interfaces específicas.

El dispositivo WildFire tiene tres interfaces:

- **MGT** (Gestión): recibe todos los archivos enviados desde los cortafuegos y devuelve logs que detallan los resultados a los cortafuegos. Consulte Configuración del dispositivo WildFire.
- **Virtual Machine Interface (VM interface)** Interfaz de máquina virtual (interfaz VM): ofrece acceso a la red para los sistemas de sandbox de WildFire para permitir que los archivos de muestra se comuniquen con Internet, lo que permite que WildFire analice mejor el comportamiento de la muestra. Cuando se configura la interfaz de VM, WildFire puede observar comportamientos malintencionados que el malware habitualmente no realizaría sin acceso a la red, tal como la actividad de llamada a casa. Sin embargo, para prevenir que el malware entre en la red desde la sandbox, configure la interfaz de VM en una red aislada con conexión a Internet. También puede habilitar la opción Tor para ocultar la dirección IP pública utilizada por la empresa de sitios malintencionados a los que accede la muestra. Para obtener más información sobre la interfaz VM, consulte Configuración de la interfaz de VM del dispositivo WildFire.
- **Interfaz de gestión del clúster:** proporciona comunicación en el clúster entre los nodos de dispositivos WildFire que son miembros de un clúster de dispositivos WildFire. Es una interfaz diferente a la interfaz MGT para las operaciones de los cortafuegos. Puede configurar la interfaz Ethernet2 o la interfaz Ethernet3 (con etiquetas **2** y **3**, respectivamente) como la interfaz de gestión del clúster.

Obtenga la información necesaria para configurar la conectividad de red en el puerto MGT (gestión), la interfaz de VM y la interfaz de gestión de clúster (solo para clústeres de dispositivos WildFire) desde su administrador de red (dirección IP, máscara de subred, puerta de enlace, nombre de host, servidor DNS). Toda la comunicación entre los cortafuegos y el dispositivo se produce en el puerto MGT, incluidos los envíos de archivos, la distribución de logs de WildFire y la administración de dispositivos. Por lo tanto, asegúrese de que los cortafuegos tengan conectividad con el puerto MGT en el dispositivo. Además, el dispositivo debe ser capaz de conectarse al sitio updates.paloaltonetworks.com para recuperar sus actualizaciones de software del sistema operativo.

Compatibilidad con tipos de archivos del dispositivo WildFire

La siguiente tabla enumera los tipos de archivos admitidos para el análisis en la nube privada del dispositivo WildFire y a través de cargas directas del portal WildFire.

Tipos de archivos compatibles para el análisis	Nube privada de WildFire (dispositivo WildFire)	Portal de Wildfire | API (carga directa; todas las regiones)
Los enlaces se encuentran en los correos electrónicos	✓	✓
Archivos de paquete de aplicaciones Android (Android application package, APK)	✗	✓
Archivos de Adobe Flash	✓	✓
Archivos de almacenamiento Java (Java Archive, JAR)	✓	✓
Archivos de Microsoft Office (incluye archivos SLK e IQY**)	✓	✓
Archivos ejecutables portátiles (incluye archivos MSI**)	✓	✓
Archivos con formato de documento portable (Portable document format, PDF)	✓	✓
Archivos Mac OS X	✗	✓
Archivos de Linux (archivos ELF y scripts de Shell)	✗	✓
Archivar archivos (RAR, 7-Zip, ZIP)*	✓	✓

Tipos de archivos compatibles para el análisis	Nube privada de WildFire (dispositivo WildFire)	Portal de Wildfire | API (carga directa; todas las regiones)
Archivos de script (BAT, JS, VBS, PS1 y HTA)	✓	✓
Secuencias de comandos (Perl y Python)	✗	✓
Archivar archivos (ZIP [carga directa] e ISO)*	✗	✓

* Los archivos ZIP no se reenvían directamente a la nube de Wildfire para su análisis. En su lugar, primero son decodificados por el cortafuegos y los archivos que coinciden con los criterios del perfil de WildFire Analysis se envían por separado para su análisis.

** El dispositivo WildFire no es compatible con el análisis de archivos MSI, IQY y SLK.

Configuración y gestión de un dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire™ puede configurarse como una nube privada de WildFire alojada localmente. Los siguientes temas describen cómo preparar el dispositivo WildFire para recibir archivos para análisis, cómo gestionar el dispositivo y cómo habilitar el dispositivo para generar localmente firmas de amenazas y categorías de URL.

Configuración del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Esta sección describe los pasos necesarios para integrar un dispositivo WildFire en una red y realizar la configuración básica.

STEP 1 | Monte el dispositivo en el rack y conecte los cables del dispositivo.

Consulte la Guía de referencia de hardware del dispositivo WildFire para obtener instrucciones.

STEP 2 | Conecte un ordenador al dispositivo usando el puerto MGT o el puerto de consola, y encienda el dispositivo.

1. Conéctese al puerto de la consola o al puerto MGT. Ambos se encuentran en la parte posterior del dispositivo.
   - **Console Port** (Puerto de la consola): conector serie macho de 9 clavijas. Utilice la siguiente configuración en la aplicación de la consola: 9600-8-N-1. Conecte el cable proporcionado al puerto de serie en el dispositivo de gestión o al conversor USB-serie.
   - **Puerto MGT:** este es un puerto Ethernet RJ-45. De forma predeterminada, la dirección IP del puerto MGT es 192.168.1.1. La interfaz del ordenador de gestión debe estar en la misma subred que el puerto MGT. Por ejemplo, establezca la dirección IP del ordenador de gestión en 192.168.1.5.
2. Encienda el dispositivo.

   El dispositivo se encenderá en cuanto establezca la conexión con la primera fuente de alimentación y sonará un pitido de advertencia hasta que conecte la segunda fuente de alimentación. Si el dispositivo ya está conectado, pero está apagado, utilice el botón de encendido de la parte frontal del dispositivo para encenderlo.

STEP 3 | Registre el dispositivo WildFire.

1. Obtenga el número de serie de la etiqueta de número de serie del dispositivo o ejecute el siguiente comando y consulte el campo `serial`:

   ```
   admin@WF-500> Mostrar informacióndel sistema
   ```

2. En un navegador, vaya al Portal de asistencia técnica de Palo Alto Networks e inicie sesión.
3. Registre el dispositivo de la siguiente forma:
   - Si es el primer dispositivo de Palo Alto Networks que registra y aún no dispone de inicio de sesión, haga clic en **Register** (Registrar) en la parte inferior de la página.

     Para el registro debe proporcionar una dirección de correo electrónico y el número de serie del dispositivo. Cuando se le solicite, establezca un nombre de usuario y una contraseña para acceder a la comunidad de asistencia técnica de Palo Alto Networks.
   - Con cuentas existentes, inicie sesión y haga clic en **My Devices (Mis dispositivos)**. Desplácese hasta la sección **Register Device** (Registrar dispositivo) de la parte inferior de la pantalla e introduzca el número de serie del dispositivo, su ciudad y código postal, y haga clic en **Register Device** (Registrar dispositivo).
4. Para confirmar el registro de WildFire en el dispositivo WildFire, inicie sesión en el dispositivo con un cliente SSH o mediante el puerto de la consola. Introduzca el nombre de usuario/contraseña admin/admin e introduzca el siguiente comando en el dispositivo:

   ```
   admin@WF-500> registrode wildfire de prueba
   ```

   El siguiente resultado indica que el dispositivo está registrado en uno de los servidores de nube de WildFire de Palo Alto Networks.

   ```
   Registro de wildfire de prueba: lista de servidores de
    descarga exitosos: seleccione con éxito el mejor servidor:
    cs-s1.wildfire.paloaltonetworks.com
   ```


STEP 4 | Restablezca la contraseña del administrador.

1. Establezca una nueva contraseña ejecutando el comando:

```
admin@WF-500> establecer contraseña
```

2. Introduzca la contraseña anterior, pulse Intro y, a continuación, introduzca y confirme la nueva contraseña. Confirme la configuración para asegurarse de que se ha guardado la nueva contraseña, por si tuviera que reiniciar.

   A partir de PAN-OS 9.0.4, la contraseña de administrador predefinida y predeterminada (admin/admin) debe cambiarse la primera vez que inicie sesión en el dispositivo. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas y otro en mayúsculas, así como un número y un carácter especial.

   Asegúrese de seguir las prácticas recomendadas sobre seguridad de la contraseña *para garantizar que la contraseña sea segura.*

3. Escriba **`exit`** para cerrar la sesión y, a continuación, vuelva a iniciarla para confirmar que se ha establecido la nueva contraseña.

STEP 5 | Configure los ajustes de interfaz de gestión.

En este ejemplo se utilizan los siguientes valores de IPv4, pero el dispositivo también admite direcciones IPv6:

- Dirección IPv4: 10.10.0.5/22
- Máscara de subred: 255.255.252.0
- Puerta de enlace predeterminada: 10.10.0.1
- Nombre de host: wildfire-corp1
- Servidor DNS: 10.0.0.246

1. Inicie sesión en el dispositivo con un cliente SSH o mediante el puerto de la consola y acceda al modo de configuración.

```
admin@WF-500> configurar
```

2. Establezca la información de IP:

```
admin@WF-500# set deviceconfig system ip-address 10.10.0.5
 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting
 servers primary 10.0.0.246
```

Configure un segundo servidor DNS al reemplazar "primary" (primario) por "secondary"(secundario) en el comando anterior, sin incluir los demás parámetros IP. Por ejemplo:

```
admin@WF-500# establecer deviceconfig sistema dns-setting
 servidores secundarios 10.0.0.247
```

3. Establezca el nombre de host (wildfire-corp1 en este ejemplo):

```
admin@WF-500# set deviceconfig nombre de host del sistema
 wildfire-corp1
```

4. Confirme la configuración para activar la nueva configuración del puerto de gestión (MGT):

```
admin@WF-500# confirmación
```

5. Conecte el puerto de la interfaz de gestión a un conmutador de red.
6. Vuelva a ubicar el PC de gestión en la red corporativa o en cualquier red necesaria para acceder al dispositivo en la red de gestión.
7. En el ordenador de gestión, utilice un cliente SSH para establecer la conexión con la dirección IP o el nombre de host nuevos asignados al puerto MGT en el dispositivo. En este ejemplo, la dirección IP es 10.10.0.5.

STEP 6 | Active el dispositivo con el código de autorización de WildFire que ha recibido de Palo Alto Networks.

Si bien funcionará sin un código de autorización, el dispositivo WildFire no puede recuperar las actualizaciones de software o de contenido sin un código de autorización válido.

1. Cambie al modo de operación:

```
admin@WF-500# salida
```

2. Obtenga e instale la licencia de WildFire:

```
admin@WF-500> solicitar licencia obtener código <auth-code>de
 autenticación
```

3. Verifique la licencia:

```
admin@WF-500> solicitar verificaciónde soporte
```

Se muestra información sobre el sitio de asistencia técnica y la fecha del contrato de asistencia. Confirme que la fecha mostrada es válida.

STEP 7 | Configure el reloj del dispositivo WildFire

Hay dos formas de realizarlo. Puede establecer la fecha, la hora y la zona horaria de forma manual, o puede configurar el dispositivo WildFire para sincronizarlo con el reloj local con un servidor de protocolo de tiempo de redes (Network Time Protocol, NTP).

- Para configurar el reloj manualmente, introduzca los siguientes comandos:

```
admin@WF-500> establecer la hora de <hh:mm:ss> la fecha <YYYY/MM/
DD> del reloj admin@WF-500> configurar admin@WF-500# establecer
 la zona <timezone>
```

horaria del sistema deviceconfig La marca de tiempo que aparecerá en el informe detallado de WildFire utilizará la zona horaria establecida en el dispositivo. Si los administradores de varias regiones van a ver los informes, considere la posibilidad de establecer la zona horaria en UTC.

- Para configurar el dispositivo WildFire para que se sincronice con un servidor NTP, escriba los siguientes comandos:

```
admin@WF-500> configure admin@WF-500# set deviceconfig system
 ntp-servers primary-ntp-server ntp-server-address <NTP primary
 server IP address> admin@WF-500# set deviceconfig system ntp-
```



```
servers secondary-ntp-server ntp-server-address <NTP secondary
 server IP address>
```

El dispositivo WildFire no prioriza el servidor NTP primario o secundario; se sincroniza con cualquiera de los servidores.

STEP 8 | (Opcional para la configuración del NTP) Configure una autenticación de NTP.

- Deshabilitar la autenticación NTP:

```
admin@WF-500# establecer dispositivoconfigurar sistema ntp-
servidores primario-ntp-servidor autenticación-tipo ninguno
```

- Habilitar el intercambio de claves simétricas (secretos compartidos) para autenticar las actualizaciones de hora del servidor NTP:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server authentication-type symmetric-key
```

  Continue to enter the **key-ID** (1 - 65534), elija el algoritmo **que se va a usar en la autenticación** NTP (**MD5** o **SHA1**) y, a continuación, escriba y confirme el algoritmo de autenticación **clave**de autenticación.

- Usar autoclave (criptografía de clave pública) para autenticar las actualizaciones de hora del servidor NTP:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server authentication-type autokey
```

STEP 9 | Seleccione la imagen de máquina virtual que el dispositivo debe utilizar para el análisis de archivos.

La imagen se debe basar en los atributos que mejor representen el software instalado en los ordenadores del usuario final. Cada imagen virtual contiene distintas versiones de los sistemas operativos y el software, como Windows XP o Windows 7 (32 bits o 64 bits) y versiones específicas de Adobe Reader

y Flash. Aunque configure el dispositivo para utilizar una sola configuración de la imagen de máquina virtual, el dispositivo utiliza varias instancias de la imagen para mejorar el rendimiento.

- Para ver una lista de máquinas virtuales disponibles para determinar cuál representa mejor su entorno:

```
admin@WF-500> mostrar imágenes de vm de wildfire
```

- Para ver la imagen de máquina virtual actual, ejecute el siguiente comando y consulte el campo `Selected VM`:

```
admin@WF-500> show wildfire status
```

- Seleccione la imagen que el dispositivo utilizará para el análisis:

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>
```

Por ejemplo, para usar vm-5:

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

STEP 10 | Habilite el dispositivo WildFire y observe los comportamientos malintencionados donde el archivo que se está analizando busca acceso a la red.

Configuración de la interfaz de VM del dispositivo WildFire.

STEP 11 | #unique_16

STEP 12 | (Opcional) Habilite el dispositivo WildFire para que realice búsquedas rápidas de veredictos y los sincronice con la nube pública de WildFire.

Con el siguiente comando de la CLI, se permite al dispositivo WildFire realizar búsquedas rápidas de veredictos y sincronizarlos con la nube pública de WildFire. Esta función se encuentra deshabilitada de forma predeterminada; establezca el comando **yes** para habilitar la función.

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 cloud-query sí | no
```

STEP 13 | (Opcional) Habilite el dispositivo WildFire para obtener actualizaciones diarias de los contenidos de Palo Alto Networks y, de este modo, facilitar y mejorar el análisis del malware.

Habilitación de las funciones de análisis del dispositivo WildFire

STEP 14 | (Opcional) Habilite el dispositivo WildFire para generar firmas de DNS y antivirus, y categorías de URL, y para distribuir nuevas firmas y categorizaciones de URL a los cortafuegos conectados.

Habilitación de firmas locales y generación de categorías URL

STEP 15 | (Opcional) Envíe automáticamente el malware descubierto en la nube privada de WildFire a la nube pública de WildFire para respaldar la protección global contra el malware.

Envío de malware a la nube pública de WildFire.

STEP 16 | (Opcional) Si no desea reenviar muestras de malware fuera de la nube privada de WildFire, envíe informes de análisis de WildFire a la nube pública de WildFire.

Si no desea enviar malware descubierto localmente a la nube pública de WildFire, la práctica recomendada es habilitar los envíos de informes de análisis de malware para mejorar y refinar inteligencia de amenazas de WildFire.

Envío de informes de análisis a la nube pública de WildFire.

STEP 17 | (Opcional) Permita que usuarios adicionales gestionen el dispositivo WildFire.

Puede asignar dos tipos de roles: superusuario y superlector. El superusuario es equivalente a la cuenta de administrador, mientras que el superlector solamente tiene acceso de lectura.

En este ejemplo, se crea una cuenta de superlector para el usuario bsimpson:

1. Introduzca el modo de configuración:

```
admin@WF-500> configurar
```

2. Cree la cuenta de usuario:

```
admin@WF-500# set mgt-config users bsimpson <password>
```

3. Introduzca y confirme la nueva contraseña.
4. Asigne la función de superlector:

```
admin@WF-500# establecer usuarios MGT-CONFIG BSIMPSON Permisos
 Superreader basado en roles Sí
```


STEP 18 | Configure la autenticación RADIUS para el acceso de administrador.

1. Cree un perfil de RADIUS mediante las opciones siguientes:

   ```
   admin@WF-500# establecer radio de perfil <profile-name>de
    servidor compartido
   ```

   (Configure el servidor de RADIUS y otros atributos).
2. Cree un perfil de autenticación:

   ```
   admin@WF-500# establecer el método de perfil <profile-name>
    de autenticación compartido RADIUS Server-Profile <server-
   profile-name>
   ```
3. Asigne el perfil a una cuenta de administrador local.

   ```
   admin@WF-500# set mgt-config usuarios nombre de usuario
    autenticación-perfil <authentication-profile-name>
   ```


Reenviar archivos para el análisis del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Configure el cortafuegos de Palo Alto Networks para reenviar archivos desconocidos o enlaces de correo electrónico y archivos bloqueados que coincidan con las firmas de antivirus existentes para el análisis. Utilice el perfil de **WildFire Analysis (Análisis de WildFire)** para definir archivos para enviar a la nube privada de WildFire (o de forma adicional, la nube pública para implementaciones de nube híbridas) y luego adjunte el perfil a una regla de seguridad para activar la inspección de malware de día cero.

Especifique el tráfico que debe enviarse para el análisis en función de la aplicación en uso, el tipo de archivo detectado, los enlaces incluidos en los mensajes de correo electrónico o la dirección de la transmisión de la muestra (carga, descarga o ambas). Por ejemplo, puede configurar el cortafuegos para que envíe archivos portables ejecutables (PE) o cualquier archivo que los usuarios intenten descargar durante una sesión de exploración web. Además de las muestras desconocidas, el cortafuegos reenvía los archivos bloqueados que coinciden con las firmas de antivirus existentes. Esto le proporciona a Palo Alto Networks una fuente valiosa de inteligencia de amenazas basada en las variantes de malware que las firmas evitaron correctamente, pero que ni WildFire ni el cortafuegos observaron antes.

Puede ampliar los recursos de análisis de WildFire a un Nube híbrida de WildFire configurando el cortafuegos para que continúe reenviando archivos sensibles a su nube privada de WildFire para su análisis local, y reenviar tipos de archivos menos sensibles o no compatibles a la nube pública de WildFire.

Además, puede dedicar recursos del dispositivo WildFire para analizar tipos de archivos específicos: documentos (archivos de Microsoft Office y PDF) o PE. Por ejemplo, si implementa una Nube híbrida de WildFire para analizar documentos de manera local y PE en las nubes públicas de WildFire, puede dedicar todos los entornos de análisis a los documentos. Esto le permite descargar análisis de PE a la nube pública, lo que le permite asignar recursos adicionales del dispositivo WildFire al procesamiento de documentos confidenciales.

Antes de comenzar

- ❑ Si hay otro cortafuegos entre el cortafuegos que está configurando para reenviar los archivos y la nube de WildFire o el dispositivo WildFire, asegúrese de que el cortafuegos en medio permita los siguientes puertos:

Puerto	Uso
443	• Inscripción • Descargas de PCAP • Descargas de muestras • Recuperación de informes • Envío de archivos • Descargas de informes en PDF

Puerto	Uso
10443	Actualizaciones dinámicas

STEP 1 | (Solo para cortafuegos PA-7000 Series) Para habilitar un cortafuegos PA-7000 Series a fin de que reenvíe muestras para el análisis de WildFire, primero debe configurar un puerto de datos en una NPC como una interfaz de tarjeta de logs. Si tiene un dispositivo PA-7000 Series que cuenta con una LFC (tarjeta de reenvío de logs),debe configurar un puerto que utilice la LFC. Cuando se configura, el puerto de la tarjeta de log o la interfaz LFC tiene prioridad sobre el puerto de gestión al reenviar muestras de WildFire.

STEP 2 | Especifique la nube privada o híbrida de WildFire a la que desea reenviar las muestras.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y edite la configuración general en función de su implementación de nube WildFire (privada o híbrida).

Nube privada de WildFire:

1. Introduzca la dirección IP o FQDN del dispositivo WildFire en el campo **WildFire Private Cloud (Nube privada de WildFire)**.

Nube híbrida de WildFire:

1. Introduzca la URL de la **WildFire Public Cloud (nube pública de WildFire)**:
   - Estados Unidos: **wildfire.paloaltonetworks.com**
   - Europa: **eu.wildfire.paloaltonetworks.com**
   - Japón: **jp.wildfire.paloaltonetworks.com**
   - Singapur: **sg.wildfire.paloaltonetworks.com**
   - Reino Unido: **uk.wildfire.paloaltonetworks.com**
   - Canadá: **ca.wildfire.paloaltonetworks.com**
   - Australia: **au.wildfire.paloaltonetworks.com**
   - Alemania: **de.wildfire.paloaltonetworks.com**
   - India: **in.wildfire.paloaltonetworks.com**
   - Suiza: **ch.wildfire.paloaltonetworks.com**
   - Polonia: **pl.wildfire.paloaltonetworks.com**
   - Indonesia: **id.wildfire.paloaltonetworks.com**
   - Taiwán: **tw.wildfire.paloaltonetworks.com**
   - Francia: **fr.wildfire.paloaltonetworks.com**
   - Qatar: **qatar.wildfire.paloaltonetworks.com**
   - Corea del Sur: **kr.wildfire.paloaltonetworks.com**
   - Israel: **il.wildfire.paloaltonetworks.com**
   - Arabia Saudita: **sa.wildfire.paloaltonetworks.com**
   - España: **es.wildfire.paloaltonetworks.com**
2. Introduzca la dirección IP o FQDN del dispositivo WildFire en el campo **WildFire Private Cloud (Nube privada de WildFire)**.

STEP 3 | Defina los límites de tamaño para los archivos que el cortafuegos reenvía y realice la configuración de registro e informes de WildFire.

Continúe editando la configuración general de WildFire (**Device (Dispositivo)** > **Setup (Configuración)** > **WildFire**).

- Revise los **límites de tamaño de archivo para los** archivos reenviados desde el cortafuegos.

  *Es una práctica recomendada de WildFire establecer el **tamaño de archivo** para PE en el límite de tamaño máximo de 10 MB y dejar el **tamaño de archivo** para todos los demás tipos de archivo establecido en el valor predeterminado.*

- Seleccione **Report Benign Files (Informar archivos benignos)** para permitir el registro de archivos que reciben un veredicto benigno de WildFire.
- Seleccione **Report Grayware Files (Reportar archivos de grayware)** para permitir el log de archivos que reciben un veredicto de grayware desde WildFire.
- Defina la información de sesión que se registra en los informes de análisis de WildFire editando la configuración de información de sesión. De manera predeterminada, toda la información de sesión se muestra en los informes de análisis de WildFire. Desmarque las casillas de verificación para quitar los campos correspondientes de los informes de análisis de WildFire y haga clic en **OK (Aceptar)** para guardar la configuración.

STEP 4 | (Solo Panorama) Configure Panorama para recoger información adicional sobre las muestras recogidas de cortafuegos que ejecutan una versión de PAN-OS anterior a PAN-OS 7.0.

Algunos campos de log de envíos de WildFire introducidos en PAN-OS 7.0 no se rellenan en aquellas muestras enviadas por cortafuegos que utilizan versiones de software anteriores. Si utiliza Panorama para gestionar cortafuegos que utilizan versiones de software anteriores a PAN-OS 7.0, Panorama puede comunicarse con WildFire para recoger información de análisis completa de las muestras enviadas por esos cortafuegos desde el **WildFire Server (servidor de WildFire)** definido (la nube global de WildFire, de manera predeterminada) para completar los detalles de los logs.

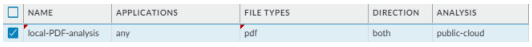
Seleccione **Panorama** > **Setup (Configuración)** > **WildFire** e introduzca un **WildFire Server (servidor WildFire)** si desea modificar la configuración predeterminada para permitir que Panorama recoja detalles de la nube de WildFire especificada o de un dispositivo WildFire.

STEP 5 | Defina el tráfico que debe reenviarse para el análisis de WildFire.

Si tiene un dispositivo WildFire configurado, puede utilizar la nube privada y la nube pública en una implementación de nube híbrida. Analice los archivos confidenciales localmente en la red, a la vez que envía todos los demás archivos desconocidos a la nube pública de WildFire para el análisis integral y obtención de avisos de veredicto.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)**, haga clic en**Add (Añadir)** para añadir un nuevo perfil de análisis de WildFire y asigne al perfil un **Name (Nombre)** descriptivo.
2. **Add (Añada)** una regla de perfil para definir el tráfico que debe enviarse para el análisis y asigne a la regla un **Name (Nombre)** descriptivo, tal como local-PDF-análisis.
3. Defina la regla de perfil para que coincida con el tráfico desconocido y para que reenvíe muestras para el análisis en función de lo siguiente:
   - **Applications (Aplicaciones)**: envíe archivos para el análisis según la aplicación en uso.
   - **File Types (Tipos de archivos)**: envíe archivos para el análisis según el tipo de archivo, incluidos los enlaces de mensajes de correo electrónico. Por ejemplo, seleccione **PDF** para reenviar PDF desconocidos detectados por el cortafuegos para el análisis.
   - **Direction (Dirección)**: envíe archivos para el análisis según la dirección de transmisión del archivo (carga, descarga o ambas). Por ejemplo, seleccione **both (ambas)** para enviar todos los PDF desconocidos para el análisis, independientemente de la dirección de transmisión.
4. Seleccione la ubicación de **Analysis (Análisis)** a la que el cortafuegos envía los archivos que coinciden con la regla.
   - Seleccione **public-cloud (nube pública)** para enviar las muestras que coincidan con la regla a la nube pública de WildFire para el análisis.
   - Seleccione **private-cloud (nube privada)** para enviar las muestras que coincidan con la regla a la nube pública de WildFire para el análisis.

     Por ejemplo, para analizar PDF que podrían contener información confidencial o exclusiva sin enviar estos documentos fuera de la red, establezca la ubicación del **Analysis (Análisis)** para el análisis de PDF local de la regla en la **private-cloud (nube privada)**.



Diferentes reglas pueden enviar muestras que coincidan a distintas ubicaciones, según sus necesidades. El ejemplo anterior muestra una regla que envía tipos de archivos sensibles para el análisis local en un nube privada de WildFire. Puede crear otra regla para enviar archivos de tipos menos sensibles, como PE, a la nube pública de WildFire. Esta flexibilidad se respalda con una implementación de nube híbrida de WildFire.

*En una implementación de nube híbrida, los archivos que coinciden con las reglas de **private-cloud (nube privada)** y **public-cloud (nube pública)** se reenvían únicamente a la nube privada como medida de precaución.*

5. (Opcional) Continúe añadiendo reglas al perfil de análisis de WildFire según sea necesario. Por ejemplo, puede añadir una segunda regla al perfil para reenviar archivos de paquete de

aplicaciones de Android (APK), portables ejecutables (PE) y Flash a la nube pública de WildFire para el análisis.

6. Haga clic en **OK (Aceptar)** para guardar el perfil de análisis de WildFire.
7. (Opcional) Continúe añadiendo reglas al perfil de análisis de WildFire según sea necesario. Por ejemplo, puede añadir una segunda regla al perfil para reenviar archivos de paquete de aplicaciones de Android (APK), portables ejecutables (PE) y Flash a la nube pública de WildFire para el análisis.
8. Haga clic en **OK (Aceptar)** para guardar el perfil de análisis de WildFire.

STEP 6 | (Opcional) Asigne recursos del dispositivo WildFire al análisis de documentos o ejecutables.

Si implementa una nube híbrida para analizar los tipos de archivo específicos a nivel local y en la nube pública de WildFire, puede dedicar los entornos de análisis al procesamiento de un tipo de archivo. Esto le permite asignar mejor los recursos en función de su configuración de entorno de análisis. Si no dedica recursos a un entorno de análisis, los recursos se asignan utilizando la configuración predeterminada.

Utilice el siguiente comando de la CLI:

```
admin@WF-500# set deviceconfig setting wildfire preferred-analysis-environment documents | executables | default
```

y seleccione una de las siguientes opciones:

- documentos: dedique los recursos de análisis para analizar simultáneamente 25 documentos, 1 PE y 2 enlaces de correo electrónico.
- ejecutables: dedique los recursos de análisis para analizar simultáneamente 25 PE, 1 documento y 2 enlaces de correo electrónico.
- predeterminado: el dispositivo analiza simultáneamente 16 documentos, 10 ejecutables portables (PE) y 2 enlaces de correo electrónico.

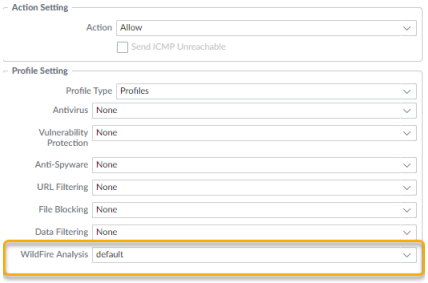
Confirme que todos los procesos de dispositivos WildFire se ejecutan con el siguiente comando:

```
admin@WF-500> show system software status
```


STEP 7 | Adjunte el perfil de WildFire Analysis a una regla de la política de seguridad.

El tráfico permitido por la regla de política de seguridad se evalúa en función del perfil de análisis de WildFire adjunto; los cortafuegos envían el tráfico que coincide con el perfil para el análisis de WildFire.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política.
2. Haga clic en la pestaña **Actions (Acciones)** en la regla de la política.
3. En la sección de Profile Settings (Configuración de perfil), seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)** y seleccione un perfil de **WildFire Analysis (Análisis de WildFire)** para adjuntar la regla de la política



STEP 8 | Asegúrese de habilitar el cortafuegos para garantizar el Reenvío de tráfico descifrado SSL para el análisis de WildFire.

Es una práctica recomendada de WildFire.

STEP 9 | Revise e implemente las prácticas recomendadas de WildFire.

STEP 10 | Haga clic en **Commit (Confirmar)** para aplicar la configuración de WildFire.

STEP 11 | (Opcional) Verificación de los envíos de WildFire.

STEP 12 | Seleccione que hacer a continuación...

- Verifique los envíos de WildFire para confirmar que el cortafuegos reenvía archivos correctamente para el análisis de WildFire.
- Envío de malware o informes desde el dispositivo WildFire Habilite esta característica para enviar automáticamente el malware identificado en su nube privada de WildFire a la nube pública de WildFire. La nube pública de WildFire volverá a analizar la muestra y generará una firma si determina que la muestra es malintencionada. La firma se distribuye a los usuarios globales a través de las actualizaciones de firma de WildFire.
- Supervisar la actividad del dispositivo WildFire para evaluar alertas y detalles informados para el malware.

Envío de malware o informes desde el dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Habilite la característica de inteligencia de nube del dispositivo WildFire para enviar automáticamente muestras de malware descubiertas en la nube privada de WildFire a la nube pública de WildFire. La nube pública de WildFire volverá a analizar el malware y generará una firma para identificar la muestra. La firma luego se añade a las actualizaciones de firmas de WildFire y se distribuye a los usuarios globales para prevenir las futuras exposiciones a la amenaza. Si no desea enviar muestras de malware fuera de la red, puede optar por enviar solo los informes de WildFire para el malware descubierto en la red, para contribuir con las estadísticas de WildFire y la inteligencia contra amenazas.

- Envíe malware a la nube pública de WildFire.

  Ejecute el siguiente comando de la CLI en el dispositivo WildFire para permitir que el dispositivo envíe muestras de malware automáticamente a la nube pública de WildFire:

  ```
  admin@WF-500admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
  ```

  Si el cortafuegos que envió originalmente la muestra para el análisis a la nube privada de WildFire tiene capturas de paquetes (PCAP) habilitadas, los PCAP para el malware también se reenviarán a la nube pública de WildFire.

- Envíe informes de análisis a la nube pública de WildFire

  Si el dispositivo WildFire está habilitado para enviar informes de análisis a la nube pública de WildFire*, no es necesario que habilite también el dispositivo para que envíe informes de malware a la nube pública. Cuando el malware se envía a la nube pública de WildFire, la nube pública genera un nuevo informe de malware para la muestra.*

  Para que el dispositivo WildFire envíe automáticamente informes de malware a la nube pública de WildFire (y no la muestra de malware), ejecute el siguiente comando de CLI en el dispositivo WildFire:

  ```
  admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
   submit-report yes
  ```

- Verificación de los ajustes de inteligencia de nube

  Compruebe que la inteligencia de nube está habilitada para enviar malware o enviar informes de malware a la nube pública de WildFire al ejecutar el siguiente comando:

  ```
  admin@WF-500> show wildfire status
  ```

  Consulte los campos `Submit sample` (Enviar muestra) y `Submitreport` (Enviar informe).

Configuración de la autenticación mediante un certificado personalizado en un dispositivo WildFire independiente

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

De forma predeterminada, un dispositivo WildFire usa certificados predefinidos para la autenticación mutua a fin de establecer las conexiones SSL utilizadas para el acceso de gestión y la comunicación entre dispositivos. Sin embargo, puede configurar la autenticación con certificados personalizados en su lugar. Los certificados personalizados le permiten establecer una cadena de confianza única para garantizar la autenticación mutua entre el dispositivo WildFire y los cortafuegos o Panorama. Puede generar estos certificados localmente en Panorama o en un cortafuegos, obtenerlos de una entidad de certificación (certificate authority, CA) externa de confianza u obtener certificados de una infraestructura de clave privada (private key infrastructure, PKI) de empresa.

En los siguientes temas se describe cómo configurar dispositivos WildFire independientes que no estén administrados por Panorama. Para configurar certificados personalizados para dispositivos WildFire y un clúster WildFire administrado por Panorama, consulte la Guía de administración de Panorama.

- Autenticación mutua de SSL del dispositivo WildFire
- Configuración de la autenticación con certificados personalizados en el dispositivo WildFire

Autenticación mutua de SSL del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Cuando un cortafuegos o Panorama envían una muestra a un dispositivo WildFire para el análisis, el cortafuegos actúa como el cliente y el dispositivo WildFire, como el servidor. Para autenticarse mutuamente, cada dispositivo muestra un certificado a fin de identificarse con el otro dispositivo.

Para implementar certificados personalizados para la autenticación mutua en su implementación, necesita lo siguiente:

- **Perfil de servicio SSL/TLS**: un perfil de servicio SSL/TLS define la seguridad de las conexiones haciendo referencia a su certificado personalizado y estableciendo las versiones de protocolo SSL/TLS utilizadas por dispositivo del servidor para comunicarse con los dispositivos cliente.
- **Certificado y perfil del servidor**: un dispositivo WildFire requiere un certificado y un perfil de certificado para identificarse con los cortafuegos. Usted puede implementar este certificado desde la infraestructura de claves públicas (PKI) de su empresa, compre una de una entidad de CA de terceros fiable o genere un certificado autofirmado localmente. El certificado del servidor debe incluir la dirección IP o el FQDN de la interfaz de gestión del dispositivo WildFire en el nombre común del certificado (certificate common name, CN) o el nombre alternativo del sujeto. El cortafuegos coincide

con el CN o el nombre alternativo del sujeto en el certificado que el servidor presenta frente a la dirección IP o el FQDN del dispositivo WildFire para verificar la identidad del dispositivo WildFire.

Además, use el perfil del certificado para definir el estado de la revocación de certificado (OCSP / CRL) y las acciones tomadas en función del estado de revocación.

- **Certificados y perfil de cliente**: cada cortafuegos requiere un certificado de cliente y perfil del certificado. El dispositivo cliente utiliza su certificado para identificarse en el dispositivo del servidor. Usted puede implementar certificados desde la PKI de su empresa utilizando el Protocolo de inscripción de certificados simple (SCEP), compre uno de una CA de terceros de confianza o genere un certificado autofirmado localmente.

  Los certificados personalizados pueden ser únicos para cada dispositivo cliente o comunes en todos los dispositivos. Los certificados únicos del dispositivo usan un hash del número de serie del dispositivo gestionado y el CN. El servidor compara el CN o el nombre alternativo del sujeto con los números de serie configurados de los dispositivos cliente. Para que la validación del certificado de cliente basada en el CN tenga lugar, el nombre de usuario debe establecerse como Nombre común del sujeto.

Configuración de la autenticación con certificados personalizados en el dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Use el siguiente flujo de trabajo para reemplazar los certificados por certificados personalizados en su implementación de WildFire. Cuando un cortafuegos o Panorama envían una muestra a un dispositivo WildFire para el análisis, el cortafuegos actúa como el cliente y el dispositivo WildFire, como el servidor.

STEP 1 | Obtenga los certificados de la entidad de certificación (certificate authority, CA) y los pares de claves para el dispositivo WildFire y el cortafuegos o Panorama.

STEP 2 | Importe el certificado de CA para validar el certificado en el cortafuegos.

1. Inicie sesión en la CLI del dispositivo WildFire y acceda al modo de configuración.

   ```
   admin@WF-500> configure
   ```

2. Use TFTP o SCP para importar el certificado.

   ```
   admin@WF-500#{tftp | scp} import certificate from <value>
    file <value> remote-port <1-65535> source-ip <ip/netmask>
    certificate-name <value> passphrase <value> format {pkcs12 |
    pem}
   ```


STEP 3 | Use TFTP o SCP para importar el par de claves que contiene el certificado del servidor y la clave privada para el dispositivo WildFire.

```
admin@WF-500# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | Configure un perfil de certificados que incluya la CA de raíz y la CA intermedia. Este perfil de certificado define cómo el dispositivo WildFire y los cortafuegos se autenticarán mutuamente.

1. En la CLI del dispositivo WildFire, acceda al modo de configuración.

   ```
   admin@WF-500> configure
   ```

2. Asigne un nombre al perfil de certificado.

   ```
   admin@WF-500# set shared certificate-profile <name>
   ```

3. Configure la CA.

   Los comandos default-ocsp-url y ocsp-verify-cert son opcionales.

   ```
   admin@WF-500# set shared certificate-profile <name> CA <name>
   ```

   ```
   admin@WF-500# set shared certificate-profile <name> CA <name>
    [default-ocsp-url <value>]
   ```

   ```
   admin@WF-500# set shared certificate-profile <name> CA <name>
    [ocsp-verify-cert <value>]
   ```


STEP 5 | Configure un perfil SSL/TLS para el dispositivo WildFire. Este perfil define el certificado y el rango de protocolo SSL/TLS que el dispositivo WildFire y los cortafuegos usan para los servicios SSL/TLS.

1. Identifique el perfil SSL/TLS.

```
admin@WF-500# set shared ssl-tls-service-profile <name>
```

2. Seleccione el certificado.

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. Defina el alcance de SSL/TLS.

PAN-OS 8.0 y las versiones posteriores admiten únicamente TLS 1.2 y las versiones posteriores. Debe configurar la versión máxima para TLS 1.2.

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2}
```

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 |
 max}
```

STEP 6 | Configure la comunicación segura del servidor en el dispositivo WildFire.

1. Establezca el perfil SSL/TLS. Este perfil de certificado SSL/TLS se aplica a toda la conexión SSL entre WildFire y los dispositivos cliente.

```
admin@WF-500# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. Establezca el perfil de certificado.

```
admin@WF-500# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```


Configuración de la interfaz de VM del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

La interfaz de máquina virtual (vm-interface) facilita la conectividad de red externa desde las máquinas virtuales aisladas en el dispositivo WildFire para permitir la observación de comportamientos malintencionados en que el archivo analizado intenta acceder a la red. En las siguientes secciones se describen la interfaz VM y los pasos necesarios para configurarla. Además, puede habilitar la función Tor con la interfaz VM, lo que enmascarará el tráfico malintencionado enviado desde el dispositivo WildFire mediante la interfaz VM, de modo que los sitios de malware a los que se puede enviar el tráfico no puedan detectar su dirección IP de acceso público.

En esta sección también se describen los pasos necesarios para conectar la interfaz VM a un puerto especializado en un cortafuegos de Palo Alto Networks para habilitar la conectividad a Internet.

- Descripción general de la interfaz de máquina virtual
- Configuración de la interfaz VM en el dispositivo WildFire
- Conexión del cortafuegos a la interfaz VM del dispositivo WildFire

Descripción general de la interfaz de máquina virtual

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

WildFire utiliza la interfaz VM (con la etiqueta **1** en la parte posterior del dispositivo) para mejorar la capacidad de detección de malware. Esta interfaz permite que una muestra ejecutada en las máquinas virtuales de WildFire se comunique con Internet, de modo que el dispositivo WildFire analice mejor el comportamiento de la muestra para determinar si presenta características de malware.

- *Si bien se recomienda que habilite la interfaz VM, es muy importante que no la conecte a una red que permita el acceso a cualquiera de sus servidores o hosts, ya que el malware ejecutado en las máquinas virtuales de WildFire puede utilizar esta interfaz para propagarse.*
- *Esta conexión puede ser una línea DSL dedicada o una conexión de red que solamente permita el acceso directo desde la interfaz VM a Internet y restrinja cualquier acceso a los servidores o hosts de cliente internos.*
- *La interfaz de VM en los dispositivos WildFire que funcionan en modo FIPS/CC está deshabilitada.*

En la siguiente ilustración se muestran dos opciones para conectar la interfaz VM a la red.

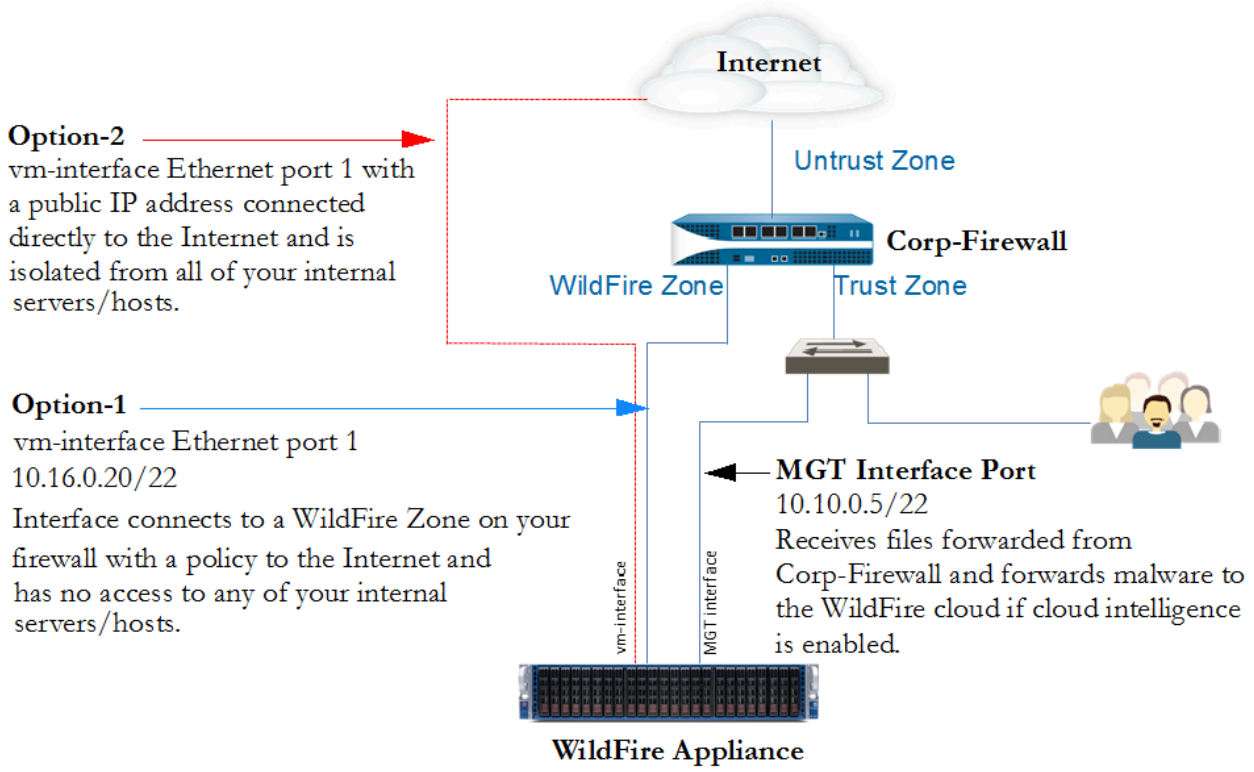


Figure 1: Ejemplo de interfaz de máquina virtual

- **Opción-1 (**recomendada): conecte la interfaz de VM a una interfaz en una zona especializada de un cortafuegos con una política que solamente permita el acceso a Internet. Es importante porque el malware que se ejecuta en las máquinas virtuales de WildFire puede utilizar potencialmente esta interfaz para propagarse. Esta es la opción recomendada porque los logs del cortafuegos proporcionarán visibilidad de cualquier tráfico generado por la interfaz VM.
- **Opción-2**: utilice una conexión dedicada del proveedor de Internet, como una conexión DSL, para conectar la interfaz VM a Internet. Asegúrese de que no hay acceso desde esta conexión a los servidores o hosts internos. Aunque esta es una solución sencilla, el tráfico generado por el malware fuera de la interfaz VN no se registrará a menos que incluya un cortafuegos o una herramienta de supervisión de tráfico entre el dispositivo WildFire y la conexión DSL.

Configuración de la interfaz VM en el dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En esta sección, se describen los pasos necesarios para configurar la interfaz de VM en el dispositivo WildFire utiliza con la configuración de la opción 1 detallada en Ejemplo de interfaz de máquina virtual. Después de configurar la interfaz de VM mediante esta opción, también debe configurar una interfaz en un cortafuegos de Palo Alto Networks por el que se enrutará el tráfico desde la interfaz de VM según se describe en Conexión del cortafuegos a la interfaz de VM del dispositivo WildFire.

De forma predeterminada, la interfaz VM está configurada del modo siguiente:

- IP address: 192.168.2.1
- Máscara de red: 255.255.255.0
- Puerta de enlace predeterminada: 192.168.2.254
- DNS: 192.168.2.254

Si tiene pensado habilitar esta interfaz, configúrela con los ajustes adecuados para la red. Si no tiene pensado utilizar esta interfaz, mantenga los ajustes predeterminados. Tenga en cuenta que la interfaz debe tener valores de red configurados, ya que en caso contrario se producirá un error de compilación.

STEP 1 | Establezca la información de dirección IP para la interfaz VM en el dispositivo WildFire. En este ejemplo se utilizan los siguientes valores de IPv4, pero el dispositivo también admite direcciones IPv6:

- Dirección IP: 10.16.0.20/22
- Máscara de subred: 255.255.252.0
- Puerta de enlace predeterminada: 10.16.0.1
- Servidor DNS: 10.0.0.246

La interfaz VM no puede estar en la misma red que la interfaz de gestión (MGT).

1. Introduzca el modo de configuración:

```
admin@WF-500> configure
```

2. Establezca la información de IP para la interfaz de VM:

```
admin@WF-500# set deviceconfig system vm-interface ip-address
 10.16.0.20 netmask 255.255.252.0 default-gateway 10.16.0.1
 dns-server 10.0.0.246
```

Solamente puede configurar un servidor DNS en la interfaz VM. La práctica recomendada es utilizar el servidor DNS del ISP o un servicio DNS abierto.

STEP 2 | Habilite la interfaz VM.

1. Habilite la interfaz VM:

```
admin@WF-500# set deviceconfig setting wildfire vm-network-
enable yes
```

2. Confirme la configuración:

```
admin@WF-500# commit
```

STEP 3 | Pruebe la conectividad de la interfaz VM.

Haga ping a un sistema y especifique la interfaz VM como el origen. Por ejemplo, si la dirección IP de la interfaz de la VM es 10.16.0.20, ejecute el siguiente comando, donde *ip-or-hostname* es la dirección IP o el nombre de host de un servidor o una red con la opción de ping habilitada:

```
admin@WF-500> ping source 10.16.0.20 host ip-or-hostname
```

Por ejemplo:

```
admin@WF-500> ping source 10.16.0.20 host 10.16.0.1
```


STEP 4 | (Opcional) Envíe el tráfico malintencionado que genera el malware a Internet. La red Tor enmascara su dirección IP de acceso público a fin de que los propietarios del sitio malintencionado no puedan determinar la fuente del tráfico.

1. Habilite la red Tor:

```
admin@WF-500# set deviceconfig setting wildfire vm-network-use-tor
```

2. Confirme la configuración:

```
admin@WF-500# commit
```

STEP 5 | (Opcional) Compruebe que la conexión de red Tor esté activa y tenga un estado correcto.

1. Emita los siguientes comandos de la CLI para buscar los ID de eventos Tor en los logs del dispositivo. Un dispositivo WildFire que se haya configurado y funcione correctamente no debe generar ID de eventos:
   - **admin@WF-500(active-controller)>showlog system direction equal backward | match anonymous-network-unhealthy**: el servicio Tor está apagado o no funciona. Reinicie el servicio Tor y compruebe que funciona correctamente.
   - **admin@WF-500(active-controller)>show log systemdirection equal backward | match anonymous-network-unavailable**: el servicio Tor funciona correctamente, pero la interfaz de la VM del dispositivo WildFire no puede establecer una conexión. Compruebe sus conexiones de red y la configuración, y vuelva a realizar la prueba.

STEP 6 | Conexión del cortafuegos a la interfaz de VM del dispositivo WildFire.

Conexión del cortafuegos a la interfaz VM del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En el siguiente flujo de trabajo de ejemplo, se describe cómo conectar la interfaz VM a un puerto en un cortafuegos de Palo Alto Networks. Antes de conectar la interfaz VM al cortafuegos, este debe tener una zona no fiable conectada a Internet. En este ejemplo, se configura una nueva zona denominada “zona wf-vm” que contiene la interfaz utilizada para conectar la interfaz VM del dispositivo al cortafuegos. La política asociada a la zona wf-vm solamente permite la comunicación de la interfaz VM con la zona que no es de confianza.

STEP 1 | Configure la interfaz en el cortafuegos al que se conectará la interfaz VM y establezca el enrutador virtual.

La zona wf-vm solamente debe contener la interfaz (Ethernet1/3 en este ejemplo) utilizada para conectar la interfaz VM del dispositivo al cortafuegos. Esto permite evitar que el tráfico generado por el malware llegue a otras redes.

1. En la interfaz web del cortafuegos, seleccione **Network (Red)** > **Interfaces** y, a continuación, seleccione una interfaz, por ejemplo **Ethernet1/3**.
2. En la lista desplegable **Tipo de interfaz**, seleccione **Capa3**.
3. En la pestaña **Config (Configurar)**, en el cuadro desplegable **Security Zone (Zona de seguridad)**, seleccione **New Zone (Nueva zona)**.
4. En el campo **Name (Nombre)** del cuadro de diálogo Zone (Zona), introduzca wf-vm-zone y haga clic en **OK (Aceptar)**.
5. En el cuadro desplegable **Virtual Router (Enrutador virtual)**, seleccione **default (predeterminado)**.
6. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlos a la interfaz; por ejemplo, 10.16.0.0/22 (IPv4) o 2001:db8:123:1::1/64 (IPv6).
7. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 2 | Cree una política de seguridad en el cortafuegos para permitir el acceso de la interfaz VM a Internet y bloquear todo el tráfico entrante. En este ejemplo, el nombre de la política es Interfaz de VM de WildFire. Dado que no creará una política de seguridad desde la zona que no es de confianza a la zona de la interfaz wf-vm, todo el tráfico entrante se bloqueará de forma predeterminada.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**
2. En la pestaña **General (General)**, introduzca un **Name (Nombre)**.
3. En la pestaña **Source (Origen)**, establezca la **Source Zone (Zona de origen)** en **wf-vm-zone**.
4. En la pestaña **Destination (Destino)**, establezca la **Destination Zone (Zona de destino)** como **Untrust (No fiable)**.
5. En las pestañas **Application (Aplicación)** y **Service/ URL Category (Categoría de URL/ servicio)**, deje de forma predeterminada **Any (Cualquiera)**.
6. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
7. En **Log Setting (Ajuste de log)**, seleccione la casilla de verificación **Log at Session End (Log al finalizar sesión)**.

*Si le preocupa que alguien pueda añadir de forma accidental otras interfaces a la zona wf-vm, clone la política de la seguridad de la interfaz VM de WildFire y, a continuación, en la pestaña **Action (Acción)** de la regla clonada, seleccione **Deny (Denegar)**. Asegúrese de que esta nueva política de seguridad aparezca debajo de la política de la interfaz VM de WildFire. Esta acción cancela la regla de permiso de la intrazona implícita que permite la comunicación entre las interfaces de la misma zona y deniega o bloquea toda la comunicación en la intrazona.*

STEP 3 | Conecte los cables.

Conecte físicamente la interfaz VM del dispositivo WildFire al puerto que ha configurado en el cortafuegos (Ethernet 1/3 en este ejemplo) con un cable RJ-45 directo. La interfaz VM se indica con la etiqueta **1** en la parte posterior del dispositivo.

Habilitación de las funciones de análisis del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

- Configuración de las actualizaciones de contenido del dispositivo WildFire
- Habilitación de firmas locales y generación de categorías URL
- Envío de malware descubierto localmente o informes a la nube pública de WildFire

Configuración de las actualizaciones de contenido del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Configure actualizaciones diarias de contenido para el dispositivo WildFire. Las actualizaciones de contenido de WildFire proporcionan al dispositivo inteligencia de amenazas para facilitar la detección precisa de malware, mejorar la capacidad del dispositivo para diferenciar muestras malintencionadas de muestras benignas y garantizar que el dispositivo tenga la información más reciente necesaria para generar firmas.

- Instalación de las actualizaciones de contenido de WildFire directamente desde el servidor de actualizaciones
- Instalación de las actualizaciones de contenido de WildFire desde un servidor habilitado con SCP

Instalación de las actualizaciones de contenido de WildFire directamente desde el servidor de actualizaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

STEP 1 | Compruebe la conectividad del dispositivo con el servidor de actualizaciones e identifique las actualizaciones de contenido que se deben instalar.

1. Inicie sesión en el dispositivo WildFire y ejecute el siguiente comando para mostrar la versión de contenido actual:

```
admin@WF-500> show system info | match wf-content-version
```

2. Confirme que el dispositivo se puede comunicar con el servidor de actualizaciones de Palo Alto Networks y ve las actualizaciones disponibles:

```
admin@WF-500> request wf-content upgrade check
```

El comando envía una consulta al servidor de actualizaciones de Palo Alto Networks, proporciona información sobre las actualizaciones disponibles e identifica la versión instalada actualmente en el dispositivo.

```
Version Size  Released on      Downloaded Installed
 -------------------------------------------------
 2-253   57MB 2014/09/20 20:00:08 PDT no         no 2-39
 44MB 2014/02/12 14:04:27 PST yes     current
```

Si el dispositivo no puede conectarse con el servidor de actualizaciones, debe permitir la conectividad del dispositivo con el servidor de actualizaciones de Palo Alto Networks (updates.paloaltonetworks.com) o descargar e instalar las actualizaciones mediante SCP, como se describe en Instalación de las actualizaciones de contenido de WildFire desde un servidor habilitado con SCP.

STEP 2 | Descargue e instale la última actualización de contenido.

1. Descargue la última actualización de contenido:

```
admin@WF-500> request wf-content upgrade download latest
```

2. Vea el estado de la descarga:

```
admin@WF-500> show jobs all
```

Puede ejecutar **show jobs pending** para ver los trabajos pendientes. En el siguiente resultado se muestra que la descarga (ID de trabajo 5) ha finalizado (estado FIN):

```
Enqueued          ID  Type Status Result Completed
 ------------------------------------------------
 2014/04/22 03:42:20  5  Downld  FIN   OK   03:42:23
```

3. Una vez finalizada la descarga, instale la actualización:

```
admin@WF-500> request wf-content upgrade install version
 latest
```

Vuelva a ejecutar el comando **show jobs all** para supervisar el estado de la instalación.

STEP 3 | Compruebe la actualización de contenido.

Ejecute el siguiente comando y consulte el campo `wf-content-version`:

```
admin@WF-500> show system info
```

A continuación se muestra un resultado de ejemplo con la versión de actualización de contenido 2-253 instalada:

```
admin@WF-500> show system info hostname: WildFire ip-address:
 10.5.164.245 netmask: 255.255.255.0 default-gateway: 10.5.164.1
 mac-address: 00:25:90:c3:ed:56 vm-interface-ip-address:
 192.168.2.2 vm-interface-netmask: 255.255.255.0 vm-interface-
default-gateway: 192.168.2.1 vm-interface-dns-server: 192.168.2.1
 time: Mon Apr 21 09:59:07 2014 uptime: 17 days, 23:19:16 family:
 m model: WildFire serial: abcd3333 sw-version: 6.1.0 wf-content-
version: 2-253 wfm-release-date: 2014/08/20 20:00:08 logdb-version:
 6.1.2 platform-family: m
```

STEP 4 | (Opcional) Programe las actualizaciones de contenido para que se instalen de forma diaria o semanal.

1. Programe el dispositivo para descargar e instalar las actualizaciones de contenido:

```
admin@WF-500# set deviceconfig system update-schedule wf-content recurring [daily | weekly] action [download-and-install | download-only]
```

   Por ejemplo, para descargar e instalar las actualizaciones diariamente a las 8:00 a.m.:

```
admin@WF-500# set deviceconfig system update-schedule wf-content recurring daily action download-and-install at 08:00
```

2. Confirme la configuración

```
admin@WF-500# commit
```

Instalación de las actualizaciones de contenido de WildFire desde un servidor habilitado con SCP

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En el siguiente procedimiento, se describe cómo instalar las actualizaciones de contenido de inteligencia de amenazas en un dispositivo WildFire sin conectividad directa con el servidor de actualizaciones de Palo Alto Networks. Necesitará un servidor habilitado para Secure Copy (SCP) que almacene temporalmente la actualización de contenido.

STEP 1 | Recupere el archivo de actualización de contenido del servidor de actualizaciones.

1. Inicie sesión en el portal de asistencia técnica de Palo Alto Networks y haga clic en **Dynamic Updates (Actualizaciones dinámicas)**.
2. En la sección del dispositivo WildFire, busque la última actualización de contenido del dispositivo WildFire y descárguela.
3. Copie el archivo de actualización de contenido en un servidor habilitado con SCP y anote el nombre del archivo y la ruta de acceso al directorio.

STEP 2 | Instale la actualización de contenido en el dispositivo WildFire.

1. Inicie sesión en el dispositivo WildFire y descargue el archivo de actualización de contenido del servidor SCP:

   ```
   admin@WF-500> scp import wf-content from username@host:path
   ```

   Por ejemplo:

   ```
   admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/
   updates/panup-all-wfmeta-2-253.tgz
   ```

   Si el servidor SCP se ejecuta en un puerto no estándar o si necesita especificar la dirección IP de origen, también puede definir estas opciones en el comando ***scp import****.*

2. Instale la actualización:

   ```
   admin@WF-500> request wf-content upgrade install file panup-
   all-wfmeta-2-253.tgz
   ```

3. Vea el estado de la instalación:

   ```
   admin@WF-500> show jobs all
   ```

STEP 3 | Compruebe la actualización de contenido.

Compruebe la versión de contenido:

```
admin@WF-500> show system info | match wf-content-version
```

En el siguiente resultado se muestra ahora la versión 2-253:

```
wf-content-version: 2-253
```

Habilitación de firmas locales y generación de categorías URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire puede generar firmas localmente en función de las muestras recibidas de los cortafuegos conectados y la API de WildFire, como alternativa al envío de malware a la nube pública para la generación de firmas. El dispositivo puede generar los siguientes tipos de firmas para que los cortafuegos utilicen para bloquear el malware y todo comando asociado, y controlar el tráfico:

- **Antivirus signatures** (Firmas de antivirus): detectan y bloquean archivos malintencionados. WildFire añade estas firmas a las actualizaciones de contenido de WildFire y antivirus.

- **DNS signatures** (Firmas DNS): detectan y bloquean los dominios de devolución de llamada para el tráfico de comandos y control asociado al malware. WildFire añade estas firmas a las actualizaciones de contenido de WildFire y antivirus.
- **URL categories** (Categorización de URL): categoriza los dominios de devolución de llamadas como malware y actualiza la categoría de URL en PAN-DB.

Configure los cortafuegos para recuperar las firmas generadas por el dispositivo WildFire cada cinco minutos. También puede enviar la muestra de malware a la nube pública de WildFire a fin de habilitar la firma para que se distribuya a nivel global a través de las publicaciones de contenido de Palo Alto Networks.

Incluso si utiliza el dispositivo WildFire para el análisis de archivos locales, también puede habilitar los cortafuegos conectados para recibir las firmas más recientes distribuidas por la nube pública de WildFire.

STEP 1 | Configuración de las actualizaciones de contenido del dispositivo WildFire.

Esto permite que el dispositivo WildFire pueda recibir la inteligencia de amenazas más reciente de Palo Alto Networks.

STEP 2 | Habilite las firmas y la generación de categorías URL

1. Inicie sesión en el dispositivo y escriba **`configure`** para acceder al modo de configuración.
2. Habilite todas las opciones de prevención de amenazas:

```
admin@WF-500# set deviceconfig setting wildfire signature-
generation av yes dns yes url yes
```

3. Confirme la configuración:

```
admin@WF-500# commit
```

Puede mostrar el estado de una firma para las firmas generadas en el entorno de WildFire 8.0.1 o posterior utilizando este comando:

```
admin@WF-500# show wildfire global signature-status sha256
 equal <sha-256
value>
```

Los dispositivos WildFire no pueden mostrar el estado de las firmas generadas antes de la actualización a WildFire 8.0.1.

STEP 3 | Establezca la programación para que los cortafuegos conectados recuperen las firmas y categorías de URL que genera el dispositivo WildFire.

La práctica recomendada es configurar sus cortafuegos para recuperar las actualizaciones de contenido de la nube pública de WildFire y el dispositivo WildFire. Esto garantiza que los cortafuegos reciban firmas según las amenazas detectadas en todo el mundo y no solo las firmas generadas desde el dispositivo local.

- Para varios cortafuegos administrados por Panorama:

  Inicie Panorama y seleccione **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, haga clic en **Schedules (Programaciones)** y **Add (Añadir)** actualizaciones de contenido programadas para dispositivos gestionados.

  Para obtener más información sobre el uso de Panorama para configurar cortafuegos administrados para recibir firmas y categorías de URL de un dispositivo WildFire, consulte Programar actualizaciones de contenido en dispositivos mediante Panorama.
- Para un único cortafuegos:
  1. Inicie sesión en la interfaz web del cortafuegos y seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**.

     Para los cortafuegos configurados para reenviar archivos a un dispositivo WildFire (en una nube privada de WildFire o una implementación de nube híbrida), se muestra la sección WF-Private.
  2. Establezca **Schedule (Programación)** para que el cortafuegos descargue e instale actualizaciones de contenido desde el dispositivo WildFire.

Envío de malware descubierto localmente o informes a la nube pública de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Habilitación del dispositivo WildFire para enviar automáticamente muestras de malware a la nube pública de WildFire. La nube pública de WildFire volverá a analizar el malware y generará una firma para identificar la muestra. La firma luego se añade a las actualizaciones de firmas de WildFire y se distribuye a los usuarios globales para prevenir las futuras exposiciones a la amenaza. Si no desea enviar muestras de malware fuera de la red, puede optar por enviar solo los informes de WildFire para el malware descubierto en la red, para contribuir y mejorar las estadísticas de WildFire y la inteligencia contra amenazas.

- Envíe malware a la nube pública de WildFire.
  1. Ejecute el siguiente comando de la CLI en el dispositivo WildFire para permitir que el dispositivo envíe muestras de malware automáticamente a la nube pública de WildFire:

     ```
     admin@WF-500# set deviceconfig setting wildfire cloud-
     intelligence submit-sample yes
     ```

     Si el cortafuegos que envió originalmente la muestra para el análisis a la nube privada de WildFire tiene capturas de paquetes (PCAP) habilitadas, los PCAP para el malware también se reenviarán a la nube pública de WildFire.
  2. Entre en el portal de WildFire para ver informes de análisis de malware enviados automáticamente a la nube pública de WildFire. Cuando el malware se envía a la nube pública de WildFire, la nube pública genera un nuevo informe de análisis para la muestra.

- Envío de informes de análisis a la nube pública de WildFire

  Para enviar automáticamente informes de malware a la nube pública de WildFire (y no la muestra de malware), ejecute el siguiente comando de la CLI en el dispositivo WildFire:

  ```
  admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
   submit-report yes
  ```

  Si ha habilitado el dispositivo WildFire para enviar automáticamente malware a la nube pública de WildFire, no necesita habilitar esta opción; la nube pública de WildFire generará un nuevo informe de análisis para la muestra.

  Los informes enviados a la nube pública de WildFire no pueden verse en el portal de WildFire. El portal de WildFire muestra solamente informes de la red pública de WildFire.

- Verificación del malware y configuración del envío de informes

  Marque para confirmar que la inteligencia de nube está habilitada para enviar malware o enviar informes a la nube pública de WildFire al ejecutar el siguiente comando:

  ```
  admin@WF-500> show wildfire status
  ```

  Consulte los campos `Submit sample` (Enviar muestra) y `Submitreport` (Enviar informe).

Actualización de un dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Utilice el siguiente flujo de trabajo para actualizar el sistema operativo del dispositivo WildFire. Si desea actualizar un dispositivo que es parte de un clúster WildFire, consulte Actualización de dispositivos WildFire en un clúster. Dado que el dispositivo solamente puede utilizar un entorno cada vez para analizar las muestras, después de actualizar el dispositivo, revise la lista de imágenes de VM disponibles y seleccione la imagen que mejor se adapte a su entorno. En el caso de Windows 7, si en su entorno se combinan los sistemas Windows 7 de 32 bits y Windows 7 de 64 bits, se recomienda seleccionar la imagen de Windows 7 de 64 bits para que WildFire analice los archivos PE de 32 y 64 bits. Aunque configure el dispositivo para utilizar una sola configuración de la imagen de máquina virtual, el dispositivo utiliza varias instancias de la imagen para el análisis de archivos.

Según la cantidad de muestras que analizó y almacenó el dispositivo WildFire, el tiempo necesario para actualizar el software del dispositivo varía; esto se debe a que la actualización requiere la migración de todas las muestras de malware y 14 días de muestras benignas. Dedique de 30 a 60 minutos a la actualización del dispositivo WildFire que utilizó en un entorno de producción.

El procedimiento a continuación utiliza un nombre de archivo de ejemplo de una versión de PAN-OS 10.2.2. El nombre de archivo exacto de la versión que instale en el dispositivo WildFire puede variar en función de la versión específica.

STEP 1 | Si configura un dispositivo WildFire por primera vez, comience por la configuración del dispositivo WildFire.

STEP 2 | Suspenda temporalmente el análisis de muestras.

1. Evite que los cortafuegos reenvíen nuevas muestras al dispositivo WildFire.
   1. Inicie sesión en la interfaz web del cortafuegos.
   2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y modifique **General Settings (Configuración general)**.
   3. Borre el campo **WildFire Private Cloud (Nube privada de WildFire)**.
   4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
2. Confirme que el análisis de las muestras que el cortafuegos envío al dispositivo haya finalizado:

```
admin@WF-500> show wildfire latest samples
```

Si no desea esperar a que el dispositivo WildFire complete el análisis de las muestras recién enviadas, puede continuar con el próximo paso. Sin embargo, considere que el dispositivo WildFire descarta las muestras pendientes en la cola de análisis.

STEP 3 | Instale las últimas actualizaciones de contenido del dispositivo WildFire. Esta actualización le proporciona al dispositivo la información de amenazas más reciente para detectar malware con mayor precisión.

Este proceso puede tardar hasta 6 horas o más en dispositivos más antiguos.

1. Verifique que esté ejecutando la última actualización de contenido en su dispositivo WildFire.

```
admin@WF-500> request wf-content upgrade check
```

2. Descargue el último paquete de actualización de contenido de WildFire.

```
admin@WF-500> request wf-content upgrade download latest
```

Si no tiene una conectividad directa con el servidor de actualizaciones de Palo Alto Networks, puede descargar las actualizaciones y realizar la Instalación de actualizaciones de contenido desde un servidor habilitado para SCP.

3. Ver el estado de la descarga.

```
admin@WF-500> show jobs all
```

4. Una vez completada la descarga, instale la actualización.

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 4 | (Necesario al actualizar a PAN-OS 10.2.2) Actualice las imágenes de VM en el dispositivo WildFire.

1. Inicie sesión y acceda a la página de descarga de software del portal de atención al cliente de Palo Alto Networks. También puede navegar manualmente a la página de descarga de software desde la página de inicio de Soporte yendo a **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.

2. En la página de actualizaciones de software, seleccione **Imágenes de VM host de WF-500** y descargue los siguientes archivos de imagen de VM:

   Palo Alto Networks actualiza periódicamente los archivos de imagen de VM; como resultado, el nombre de archivo específico cambia según la versión disponible. Asegúrese de descargar la última versión, donde m-x.x.x en el nombre del archivo indica el número de versión; además, hay una fecha de lanzamiento a la que se puede hacer referencia para ayudar a determinar la versión más reciente.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Cargue las imágenes de VM en el dispositivo WildFire.
   1. Importe la imagen de VM desde el servidor SCP:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Por ejemplo:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Para comprobar el estado de la descarga, utilice el siguiente comando:

      ```
      admin@WF-500> show jobs all
      ```

   3. Repita el proceso para las imágenes de VM restantes.
4. Instale la imagen de la máquina virtual.
   1. ```
      admin@WF-500> request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. Repita el proceso para las imágenes de VM restantes.
5. Confirme que las imágenes de VM se han instalado y habilitado correctamente en el dispositivo WildFire.
   1. (Opcional) Vea una lista de imágenes de máquinas virtuales disponibles:

      ```
      admin@WF-500> show wildfire vm-images
      ```

      El resultado muestra las imágenes de VM disponibles.
   2. Confirme la configuración:


      ```

```
admin@WF-500# commit
```

3. Vea las imágenes de la máquina virtual activa ejecutando el siguiente comando:

```
admin@WF-500> show wildfire status
```

STEP 5 | Descargar la versión de software PAN-OS 10.2.2 al dispositivo WildFire.

No puede omitir ninguna versión importante al actualizar el dispositivo WildFire. Por ejemplo, si desea actualizar de PAN-OS 6.1 a PAN-OS 7.1, debe descargar e instalar PAN-OS 7.0 en primer lugar.

En los ejemplos de este procedimiento, se muestra cómo actualizar a PAN-OS 10.2.2. Reemplace 10.2.2 por la versión final correspondiente para su actualización.

Descargue la versión de software 10.2.2:

- Conectividad directa con internet:
  1. `admin@WF-500> request system software download version 10.2.2`
  2. Para comprobar el estado de la descarga, utilice el siguiente comando:

     ```
     admin@WF-500> show jobs all
     ```
- Sin conectividad a internet:
  1. Vaya al sitio de Asistencia técnica de Palo Alto Networks y en la sección Tools (Herramientas), haga clic en **Software Updates (Actualizaciones de software)**.
  2. Descargue el archivo de imagen del software de WildFire que desea instalar en un ordenador que ejecuta el software del servidor SCP.
  3. Importe el archivo de imagen del software desde el servidor SCP:

     ```
     admin@WF-500> scp import software from <username@ip_address>/
     <folder_name>/<imagefile_name>
     ```

     Por ejemplo:

     ```
     admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
     WildFire_m-10.2.2
     ```
  4. Para comprobar el estado de la descarga, utilice el siguiente comando:

     ```
     admin@WF-500> show jobs all
     ```

STEP 6 | Confirme que todos los servicios se ejecuten.

```
admin@WF-500> show system software status
```


STEP 7 | Instale la versión de software 10.2.2.

```
admin@WF-500> request system software install version 10.2.2
```

STEP 8 | Complete la actualización de software.

1. Confirme que la actualización se haya completado. Ejecute el siguiente comando y busque el tipo de trabajo `Install` y el estado `FIN`:

   ```
   admin@WF-500> show jobs all Enqueued
    Dequeued ID Type Status Result Completed
    ---------------------------------------------------- 02:42:36
    02:42:36 5 Install FIN OK 02:43:02
   ```

2. Reinicie el dispositivo:

   ```
   admin@WF-500> request restart system
   ```

   El proceso de actualización puede tardar 10 minutos o más de una hora, según la cantidad de muestras almacenadas en el dispositivo WildFire.

STEP 9 | Compruebe que el dispositivo WildFire esté listo para reanudar el análisis de muestras.

1. Compruebe si en el campo `sw-version` (versión de software) figura 10.2.2:

   ```
   admin@WF-500> show system info | match sw-version
   ```

2. Confirme que todos los servicios se ejecuten:

   ```
   admin@WF-500> show system software status
   ```

3. Confirme que el trabajo de confirmación automática (`AutoCom`) se haya completado:

   ```
   admin@WF-500> show jobs all
   ```


STEP 10 | (Opcional) Habilite la imagen de VM que el dispositivo WildFire utiliza para realizar el análisis. Cada imagen de VM disponible representa un sistema operativo y admite varios entornos de análisis diferentes en función de ese sistema operativo.

- *Si su entorno de red tiene una combinación de Windows 7 de 32 bits y Windows 7 de 64 bits, se recomienda seleccionar la imagen de Windows 7 de 64 bits para que WildFire analice los archivos PE de 32 y 64 bits.*
- *vm-3 (Windows XP), vm-5 (Windows 7 de 64 bits) y vm-7 (Windows 10 de 64 bits) son los entornos de análisis actualmente disponibles.*

- Para ver la imagen de la máquina virtual activa, ejecute el siguiente comando y consulte el campo `Selected VM` (VM seleccionada):

```
admin@WF-500> show wildfire status
```

- Ver una lista de imágenes de máquinas virtuales disponibles:

```
admin@WF-500> show wildfire vm-images
```

  El siguiente resultado muestra que `vm-5` es la imagen de Windows 7 de 64 bits:

```
vm-5 Windows 7 de 64 bits, Adobe Reader 11, Flash 11, Office
 2010. Compatibilidad con PE, PDF, Office 2010 y versiones
 anteriores
```

- Establecer la imagen que se utilizará para el análisis:

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-
image-number>
```

  Por ejemplo, para usar vm-5, ejecute el siguiente comando:

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

  Y confirme la configuración:

```
admin@WF-500# commit
```

STEP 11 | Siguientes pasos:

- (Opcional) Actualice los cortafuegos a PAN-OS 10.2.2. Consulte las instrucciones de actualización del cortafuegos, que se incluyen en la nueva guía de funciones de PAN-OS 10.2. Los cortafuegos que ejecutan versiones anteriores a PAN-OS 10.2.2 pueden continuar reenviando muestras a un dispositivo WildFire que ejecuta la versión 10.2.2.
- (Solución de problemas) Si observa problemas de migración de daos o un error tras la actualización, reinicie el dispositivo WildFire para reiniciar el proceso de actualización; el reinicio del dispositivo WildFire no provocará una pérdida de datos.

Instale el certificado del dispositivo WildFire Appliance con una conexión a Internet

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire ❑ Cuenta del Portal de atención al cliente (CSP) con una de las siguientes funciones de usuario: Superusuario, usuario estándar, usuario limitado, investigador de amenazas, función de prueba de AutoFocus, superusuario de grupo, usuario estándar de grupo, usuario limitado de grupo, investigador de amenazas de grupo, usuario del Centro de servicio autorizado (ASC) y usuario de Servicio completo de ASC. ❑ Acceso de superusuario al dispositivo WildFire

Para recuperar el certificado del dispositivo en el dispositivo WF-500, cuando hay una conexión a Internet disponible, debe iniciar sesión en el portal de soporte de Palo Alto Networks para generar una contraseña de un solo uso necesaria para acceder al certificado. A continuación, esta OTP se utiliza para recuperar el certificado del dispositivo en el dispositivo específico.

Los dispositivos WF-500B vienen equipados con un Módulo de plataforma fiable (TPM) que se utiliza para identificarse de forma segura y obtener automáticamente el certificado del dispositivo; no es necesaria la intervención del usuario para gestionar los certificados del dispositivo WF-500B.

Si está operando una Nube privada de WildFire y no se conecta a ninguno de los servicios de WildFire, no necesita actualizar los certificados de dispositivo del dispositivo WildFire. En su lugar, el dispositivo WildFire usa certificados predefinidos para la autenticación mutua a fin de establecer las conexiones SSL utilizadas para el acceso de gestión y la comunicación entre dispositivos, sin embargo, puede Configuración de la autenticación mediante un certificado personalizado en un dispositivo WildFire independiente en su lugar.

Si su dispositivo WF-500B no está conectado a Internet, es posible que observe trabajos fallidos debido a los intentos repetidos del dispositivo de recuperar los certificados del dispositivo.

Para instalar correctamente el certificado de dispositivo en su cortafuegos, se deben permitir los siguientes FQDN y puertos en la red.

FQDN	Ports (Puertos)
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • certificatetrusted.paloaltonetworks.com • certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 y TCP 443

STEP 1 | Compruebe que esté ejecutando una de las siguientes versiones de PAN-OS en el dispositivo WildFire:

- PAN-OS 11.0.1 y posterior
- PAN-OS 10.2.4 y posterior
- PAN-OS 10.1.10 y posteriores (no compatibles con el dispositivo WF-500B)
- PAN-OS 10.0.12 y posteriores (no compatibles con el dispositivo WF-500B)
- PAN-OS 9.1.17 y posteriores (no compatibles con el dispositivo WF-500B)

STEP 2 | Genere la contraseña de un solo uso (One Time Password, OTP).

1. Inicie sesión en el Portal de atención al cliente con una función de usuario que tiene permiso para generar una OTP.
2. Seleccione **Products (Productos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **Device Type (Tipo de dispositivo)**, seleccione **Generate OTP for WF-500 (Generar OTP para WF-500)**.
4. Seleccione el número de serie de su **WF-500 Device (dispositivo WF-500)**.
5. **Genere el OTP** y cópielo.

STEP 3 | Acceda a la CLI del dispositivo WF-500 con privilegios administrativosde superusuario.

STEP 4 | Configure el dispositivo WildFire para sincronizarlo con un servidor NTP:

```
admin@WF-500> configure admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server ntp-server-address <NTP primary server IP address> admin@WF-500# set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address <NTP secondary server IP address>
```


STEP 5 | Descargue e instale el certificado de dispositivo del dispositivo WF-500 usando el siguiente comando CLI (recuerde usar la **One-time Password (Contraseña de un solo uso)** correcta que generó en el Portal de atención al cliente):

```
admin@WF-500> request certificate fetch otp <otp_value>
```

STEP 6 | Su dispositivo WF-500 recupera e instala correctamente el certificado del dispositivo.

STEP 7 | (Opcional) Verifique la descarga e instalación correcta de un certificado de dispositivo usando el siguiente comando CLI:

```
admin@WF-500> show device-certificate status
```

Una instalación correcta del certificado del dispositivo muestra la siguiente respuesta:

```
Información del certificado del dispositivo: Estado actual del
 certificado del dispositivo: Válido No válido antes de: 2022/11/30
 15:17:47 PST No válido después de: 2023/02/28 15:17:47 PST
 Última marca de tiempo recuperada 2022/11/30 15:29:42 PST Último
 estado recuperado: correcto Información de última recuperación:
 Certificado de dispositivo obtenido correctamente
```

STEP 8 | Actualice la configuración del dispositivo WildFire para establecer una conexión a la nube avanzada de WildFire con el certificado del dispositivo actualizado mediante el siguiente comando CLI:

Table 1:

Versión de PAN-OS ejecutándose en el dispositivo WildFire	Comando de la CLI
• PAN-OS 11.0.1 y posterior • PAN-OS 10.2.5 y posterior • PAN-OS 10.1.10 y posterior	`admin@WF-500> registrode wildfire de prueba`
• PAN-OS 10.2.4 • PAN-OS 10.0.12 y posterior • PAN-OS 9.1.17 y posterior	`admin@WF-500> request restart system` *Este proceso puede tardar hasta 20 minutos en completarse.*
Cualquier versión configurada como un nodo del clúster WildFire	`admin@WF-500(passive-controller)> request clust er reboot-local-node`

Versión de PAN-OS ejecutándose en el dispositivo WildFire	Comando de la CLI

	Puede ver el estado de la tarea de reinicio en el nodo del controlador WildFire usando el siguiente comando CLI:
	`admin@WF-500(active-controller)> show cluster task pending`
	Cuando no queden tareas pendientes, utilice el siguiente comando CLI para verificar un reinicio correcto:
	`admin@WF-500(active-controller)> mostrar el historial de tareas del clúster.`
	Al finalizar, debería ver el estado `Finalizado: correcto en AAAA-MM- DD HH:MM:SS UTC`*, que indica cuándo se completó el proceso de reinicio.*

Supervisar la actividad del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede ver los resultados del análisis de las muestras enviadas al dispositivo WildFire accediendo al cortafuegos que envió la muestra (o Panorama, si está gestionando de forma centralizada varios cortafuegos) o mediante la API de WildFire.

Una vez que WildFire ha analizado una muestra y enviado un veredicto de malintencionado, phishing, grayware o benigno, se genera un informe detallado para la muestra. Los informes de análisis de WildFire visualizados en el cortafuegos que envió la muestra también incluyen datos de la sesión durante la cual se detectó la muestra. En el caso de las muestras identificadas como malware, el informe de análisis de WildFire incluye detalles sobre las firmas de WildFire existentes que pueden estar relacionadas con el malware identificado recientemente e información sobre los atributos del archivo, su comportamiento y la actividad que indicaban que la muestra era malintencionada.

Consulte los siguientes temas para usar el portal de WildFire o un cortafuegos conectado para supervisar los envíos de WildFire, visualizar los informes de las muestras analizadas y establecer alertas y notificaciones según los envíos y resultados de los análisis:

- Acerca de los logs e informes de WildFire
- Uso de la CLI de WildFire para supervisar el dispositivo WildFire
- Utilice el cortafuegos para supervisar los envíos de dispositivos WildFire

Acerca de los logs e informes de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede supervisar los logs del dispositivo WildFire en el cortafuegos, con el portal de WildFire o con la API de WildFire.

Para cada muestra que WildFire analiza, WildFire clasifica la muestra como malware, phishing, grayware o benigno, y detalla la información y el comportamiento de la muestra en el informe de análisis de WildFire. Se puede acceder a los informes de análisis de WildFire en el cortafuegos que envió la muestra y la nube de WildFire (pública o privada) que analizó la muestra, o se pueden recuperar usando la API de WildFire:

- En el cortafuegos: todas las muestras que envía un cortafuegos para el análisis de WildFire se registran como entradas de envíos de WildFire (**Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)**). La columna Acción en el log de envíos de WildFire indica si el cortafuegos permitió o bloqueó un archivo. Para cada entrada de envío de WildFire, puede abrir una vista de log detallado para visualizar el informe de análisis de WildFire para la muestra o para descargar el informe como PDF.
- En el portal de WildFire: supervise la actividad de WildFire, incluso el informe de análisis de WildFire para cada muestra, que también puede descargarse como PDF. En una implementación de nube privada de WildFire, el portal de WildFire proporciona detalles de las muestras que se cargan manualmente en el portal y las muestras enviadas por un dispositivo WildFire con la inteligencia de nube habilitada.

  La opción para ver informes de análisis de WildFire en el portal solo es compatible para dispositivos WildFire con la función de inteligencia de nube *habilitada.*
- Con la API de WildFire: recupere informes de análisis de WildFire desde un dispositivo WildFire o desde la nube pública de WildFire.

Uso del dispositivo WildFire para supervisar el estado del análisis de muestras

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Utilice la CLI de WildFire (interfaz de línea de comandos) para supervisar la información relacionada con el análisis en su dispositivo WildFire. Puede ver la información de utilización de la plataforma de análisis, la cola de muestras actual y los detalles del proceso de muestra.

Consulte las secciones siguientes para obtener detalles sobre el uso del dispositivo WildFire para supervisar la actividad de WildFire:

- Visualización de la utilización del entorno de análisis de WildFire
- +Visualización de la información del procesamiento del análisis de muestras de WildFire

Visualización de la utilización del entorno de análisis de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire utiliza varios entornos de análisis para detectar comportamientos maliciosos dentro de las muestras. Puede ver qué entornos de análisis se están utilizando, cuántos están disponibles y cuántos archivos están en cola a la espera de que se realice el análisis. Si la utilización de un entorno de análisis en particular siempre está en la capacidad máxima de carga de trabajo (o cerca de ella), considere descargar el análisis de archivos menos confidenciales en una nube pública de WildFire alojada en Palo Alto Networks, actualizar la política de reenvío de archivos o redefinir los límites de reenvío de archivos (Palo Alto Networks recomienda utilizar los valores de reenvío de archivos predeterminados para todos los tipos de archivos).

STEP 1 | Acceda a la CLI y a uno de los siguientes comandos según el entorno de análisis para el que desee ver las estadísticas de utilización.

- Portable Executable Analysis Environment Utilization—**show wildfire wf-vm-pe-utilization**
- Document Analysis Environment Utilization—**show wildfire wf-vm-doc-utilization**
- Email Link Analysis Environment Utilization—**show wildfire wf-vm-elinkda-utilization**
- Archive Analysis Environment Utilization—**show wildfire wf-vm-archive-utilization**

Para un entorno de análisis determinado, el dispositivo indica cuántos están en uso y cuántos están disponibles:

```
{ available: 2, in_use: 1, }
```

STEP 2 | Vea el número y el desglose de las muestras de dispositivos WildFire a la espera de analizarse. Las muestras se procesan a medida que los entornos de análisis están disponibles.

show wildfire wf-sample-queue-status

```
{ DW-ARCHIVE: 4, DW-DOC: 2, DW-ELINK: 0, DW-PE: 21, DW-
URL_UPLOAD_FILE: 2, }
```

+Visualización de la información del procesamiento del análisis de muestras de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire retiene registros de la actividad de análisis dentro de un registro de eventos. Puede ver detalles sobre qué servicios o dispositivos conectados en su red analizaron una muestra en particular, así como cuántas muestras se analizaron en un período determinado. Puede usar esta información para supervisar la actividad y desarrollar políticas y contramedidas frente a la actividad maliciosa. La actividad inusualmente intensa puede indicar una actividad sospechosa. También considere usar una herramienta de inteligencia de amenazas como AutoFocus para investigar y determinar la naturaleza de una amenaza.

STEP 1 | Vea el número de muestras procesadas localmente dentro de un intervalo de tiempo especificado o en función de un número máximo de muestras.

show wildfire local sample-processed {time [last-12-hrs| last-15-minutes | last-1-hr | last-24-hrs | last-30-days | last-7-days| last-calender-day | last-calender-month] \ count <number_of_samples>}.

```
Latest samples information:
 +-------------------------------------------------------------------
```



```
+---------------------+-----------+------------+-----------
+------------+-------------------+ | SHA256 | Create Time
 | File Name | File Type | File Size | Malicious | Status |
 +-------------------------------------------------------------------
+---------------------+-----------+------------
+-----------+------------+-------------------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
 2018-12-09 16:55:53 | | Email Link | 31,522 | | download complete
 | |
 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
 2018-12-09 16:53:40 | | Email Link | 39,679 | | download complete
 |
 +-------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+-------------------+
```

STEP 2 | Identifique los dispositivos que enviaron una muestra específica para el análisis de WildFire.

show wildfire global sample-device-lookup sha256igual a <SHA_256>.

```
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+
```


Uso de la CLI de WildFire para supervisar el dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

Utilice la CLI de WildFire™ (interfaz de línea de comandos) para ver los logs internos del sistema. Puede revisar los eventos de registro para supervisar el estado de los componentes de WildFire, como los nodos del clúster, los servicios centrales y del analizador, y para solucionar problemas y verificar la configuración del sistema. Para obtener información sobre otros comandos de PAN-OS, consulte el Inicio rápido de la CLI de PAN-OS.

- Visualización del log del sistema del dispositivo WildFire

Visualización del log del sistema del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

Utilice un emulador de terminal, como PuTTY, para conectarse al dispositivo WildFire con una conexión de Shell seguro (SSH) o una conexión física directa en serie desde una interfaz en serie en su ordenador de gestión al puerto de la consola en el dispositivo.

STEP 1 | Inicie el software de emulación del terminal y seleccione el tipo de conexión (en serie o SSH).

- Para establecer una conexión SSH, introduzca el nombre de host de WildFire o la dirección IP del dispositivo al que desee conectarse y establezca el puerto en **22**.
- Para establecer una conexión en serie, conecte una interfaz en serie en el ordenador de gestión al puerto de la consola en el dispositivo. Configure los ajustes de conexión en serie en el software de emulación del terminal de la siguiente manera:
  - Tasa de datos: **9600**
  - Bits de datos: **8**
  - Paridad: **ninguna**
  - Bits de terminación: **1**
  - Control de flujo: **ninguno**

STEP 2 | Cuando se le solicite inicia sesión, introduzca las credenciales administrativas.

STEP 3 | En un dispositivo WildFire, especifique el siguiente comando:

admin@WF-500>show log system subtype direction equal backward

Este comando muestra todos los eventos registrados de WildFire categorizados como un subtipo de dispositivo Wildfire desde el más antiguo hasta el más nuevo.

- Puede invertir la visualización de los registros del más nuevo al más antiguo añadiendo el argumento de comando `direction equal backward`.
- Los mensajes de log devueltos por la CLI del dispositivo WildFire pueden incluir diversos subtipos. Puede filtrar los logs por una palabra clave común. Utilice el siguiente argumento de comando para filtrar por una cadena específica: `match queue < keyword>`.

  El siguiente log del dispositivo WildFire muestra los procesos de inicialización del sistema durante el arranque.

```
Time Severity Subtype Object EventID ID Description
 ================================================================================
 2017/03/29 12:04:33 medium general general 0 Hostname changed
 to WF-500 2017/03/29 12:04:40 info general general 0 VPN Disable
 mode = off 2017/03/29 12:04:41 info hw ps-inse 0 Power Supply
 #1 (top) inserted 2017/03/29 12:04:41 high general system- 1 The
 system is starting up. 2017/03/29 12:04:41 info raid pair-de 0
 New Disk Pair A detected. 2017/03/29 12:04:41 info raid pair-de 0
 New Disk Pair A detected. 2017/03/29 12:04:41 info raid pair-de 0
 New Disk Pair B detected. 2017/03/29 12:04:41 info raid pair-de 0
 New Disk Pair B detected. 2017/03/29 12:04:41 info cluster cluster
 0 Cluster daemon is initializing. 2017/03/29 12:04:41 info port
 eth1 link-ch 0 Port eth1: Up 1Gb/s Full duplex 2017/03/29 12:04:41
 info port MGT link-ch 0 Port MGT: Up 1Gb/s Full duplex 2017/03/29
 12:04:41 info port eth3 link-ch 0 Port eth3: Up 1Gb/s Full duplex
 2017/03/29 12:04:41 info port eth2 link-ch 0 Port eth2: Up 1Gb/
s Full duplex 2017/03/29 12:04:41 info general general 0 Power
 Supply #1 (top) is not present on startup 2017/03/29 12:04:41
 info general general 0 Power Supply #2 (bottom) is not present on
 startup
```


Utilice el cortafuegos para supervisar los envíos de dispositivos WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

Las muestras enviadas por el cortafuegos (a las nubes públicas y/o privadas de WildFire) se añaden como entradas a los logs de **envíos de WildFire**. Se muestra un informe de análisis de WildFire en la vista ampliada para cada entrada de envíos de WildFire. Para obtener más información sobre el uso del cortafuegos para supervisar malware, consulte Supervisar la actividad de WildFire.

Ver logs e informes de análisis del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Los logs de WildFire contienen información sobre muestras (archivos y enlaces de correo electrónico) analizadas por WildFire. Incluye artefactos, que son propiedades, actividades o comportamientos asociados con el evento registrado, como el tipo de aplicación o la dirección IP de un atacante, así como cualidades específicas de WildFire, como resultados de análisis de alto nivel, incluida la categorización de la muestra. como malware, phishing, grayware o información benigna, y detalla información de muestra. La revisión de los logs de envíos de WildFire también puede indicar si un usuario en sus redes descargó un archivo sospechoso. En el informe del análisis de WildFire se muestra información detallada de la muestra, además de información sobre los usuarios de destino, información del encabezado de correo electrónico (si está habilitado), la aplicación que entregó el archivo y todas las URL involucradas en la actividad de comando y control del archivo. Le informa de si el archivo es malintencionado, ha modificado las claves de registro, ha leído/escrito en archivos, ha creado nuevos archivos, ha abierto canales de comunicación de red, ha causado bloqueos de aplicaciones, ha generado procesos, ha descargado archivos o ha mostrado otro comportamiento malintencionado.

STEP 1 | Reenviar archivos para el análisis del dispositivo WildFire.

STEP 2 | Configuración de los ajustes del log de envíos a WildFire.

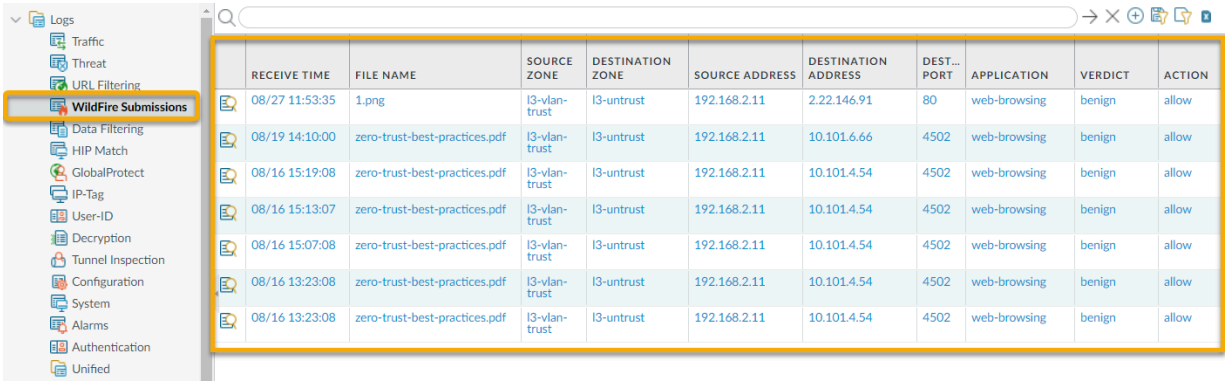
STEP 3 | Para visualizar las muestras enviadas por un cortafuegos a una nube pública, privada o híbrida de WildFire, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **WildFire Submissions (Envíos de WildFire)**. Cuando WildFire completa el análisis de una muestra, los resultados se devuelven al cortafuegos que envió la muestra y se ponen a disposición en los logs de envíos de WildFire. Los logs de envío incluyen detalles sobre una muestra determinada, que incluye la siguiente información:

- La columna Verdict (veredicto) indica si la muestra es benigna, malintencionada, phishing o grayware.
- La columna Action (Acción) indica si el cortafuegos permitió o bloqueó la muestra.

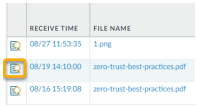
- La columna Severity (Gravedad) indica el grado de amenaza que implica una muestra para una organización con los siguientes valores: crítico, alto, intermedio, bajo e informativo.

  Los valores de los siguientes niveles de gravedad se determinan con una combinación de veredictos y valores de acción.

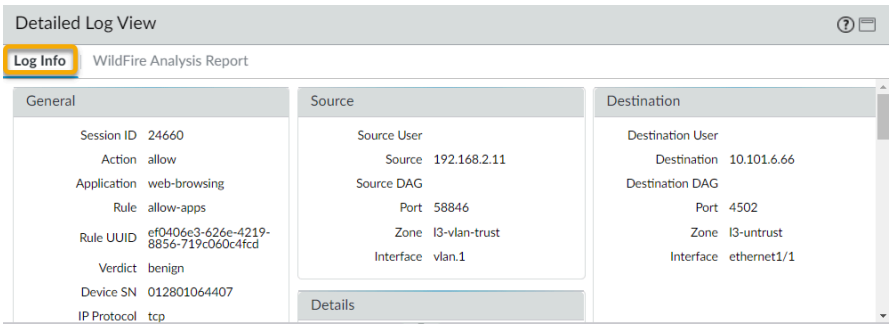
  - *Baja: muestras de grayware con la acción allow (permitir).*
  - *Alta: muestras maliciosas con la acción allow (permitir).*
  - *Informativo:*
    - *Muestras benignas con la acción allow (permitir).*
    - *Muestras con cualquier veredicto y la acción block (bloquear).*



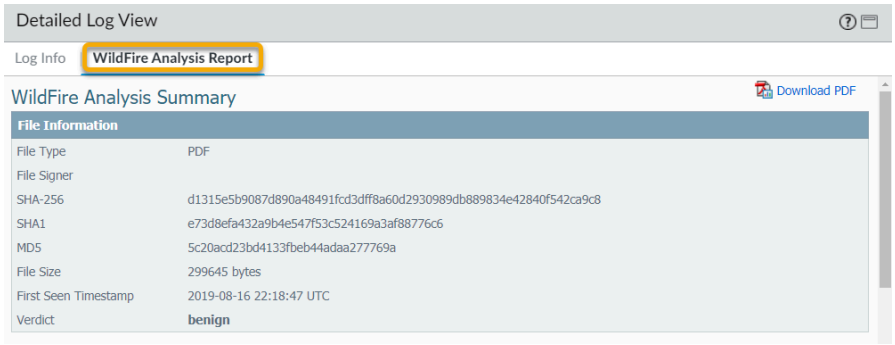
STEP 4 | En cualquiera de las entradas, seleccione el icono de detalles del log para abrir una vista detallada del log para cada entrada:



La vista detallada del log muestra la información del log y el informe de WildFire Analysis de la entrada. Si el cortafuegos tiene capturas de paquetes (PCAP) habilitadas, las PCAP de la muestra también se mostrarán.



Para todas las muestras, el informe del análisis de WildFire muestra información del archivo y la sesión. Para las muestras de malware, el informe de análisis de WildFire se amplía para incluir detalles sobre los atributos del archivo y el comportamiento que indicaron que el archivo era malintencionado.



STEP 5 | (Opcional) Haga clic en **Download PDF (Descargar PDF)** para descargar el informe de WildFire Analysis.

Clústeres de dispositivos WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Un *clúster de dispositivos WildFire* es un grupo interconectado de dispositivos WildFire que agrupa recursos para incrementar la capacidad de análisis y almacenamiento de muestras, admitir grupos más numerosos de cortafuegos y simplificar la configuración y la gestión de varios dispositivos WildFire. Esto se utiliza especialmente en entornos donde no se permite el acceso a la nube pública de WildFire. Puede configurar y gestionar hasta veinte dispositivos WildFire como un clúster de dispositivos WildFire en una sola red. Los clústeres también proporcionan un solo paquete de firmas que el clúster distribuye a todos los cortafuegos conectados, arquitectura de alta disponibilidad (high-availability, HA) para la tolerancia de averías y la capacidad de gestionar clústeres centralmente utilizando Panorama. Además, puede gestionar dispositivos WildFire independientes utilizando Panorama.

Para crear clústeres de dispositivos WildFire, todos los dispositivos WildFire que desee ubicar en un clúster deben ejecutar PAN-OS 8.0.1 o posterior. Cuando utiliza Panorama para gestionar clústeres de dispositivos WildFire, Panorama también debe ejecutar PAN-OS 8.0.1 o posterior. No es necesario que tenga una licencia separada para crear y gestionar los clústeres de dispositivos WildFire.

- Resistencia y magnitud del clúster de dispositivos WildFire
- Gestión de clústeres de dispositivos Wildfire
- Configuración local de un clúster en dispositivos WildFire
- Configuración del cifrado de dispositivo a dispositivo de WildFire
- Supervisión de un clúster WildFire
- Actualización de dispositivos WildFire en un clúster
- Solución de problemas en un clúster WildFire

Resistencia y magnitud del clúster de dispositivos WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

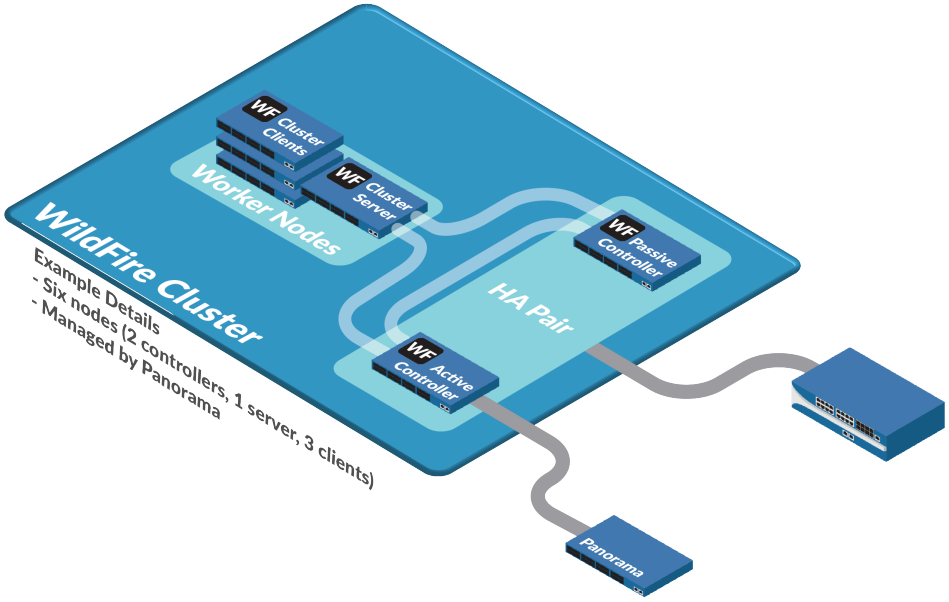
Los clústeres de dispositivos WildFire agregan la capacidad de análisis y almacenamiento de muestras de hasta veinte dispositivos WildFire, de modo que pueda admitir grandes implementaciones de cortafuegos en una red. Tiene la flexibilidad para gestionar y realizar la Configuración local de un clúster en dispositivos WildFire con la CLI, o gestionar y realizar la Configuración de un clúster centralmente en Panorama de servidores de dispositivos serie M o dispositivos virtuales. Un entorno de clúster de dispositivos WildFire incluye lo siguiente:

- De 2 a 20 dispositivos WildFire que desea agrupar y gestionar como un clúster. Como mínimo, un clúster debe tener dos dispositivos WildFire configurados en un par de alta disponibilidad (HA).
- Cortafuegos que reenvían muestras al clúster para el análisis de tráfico y la generación de firmas.
- (Opcional) Uno o dos dispositivos Panorama para la gestión centralizada del clúster si decide no gestionar el clúster localmente. Para proporcionar HA, utilice dos dispositivos Panorama configurados como un par de HA.

Cada dispositivo WildFire que añade a un clúster de dispositivos WildFire se convierte en un nodo en ese clúster (a diferencia de un dispositivo WildFire independiente). Panorama puede gestionar hasta 10 clústeres de dispositivos WildFire con un total de 200 *nodos de clústeres* WildFire (10 clústeres, cada uno con un máximo de 20 nodos).

Panorama puede gestionar dispositivos WildFire independientes*, además de clústeres de dispositivos WildFire. La cantidad total combinada de dispositivos WildFire independientes y nodos de clústeres de dispositivos WildFire que Panorama puede gestionar es de 200. Por ejemplo, si Panorama gestiona tres clústeres con un total de 15 nodos de clúster WildFire y ocho dispositivos WildFire independientes, Panorama gestiona un total de 23 dispositivos WildFire y puede gestionar hasta 177 dispositivos WildFire más.*

Los dispositivos WildFire conectados a Panorama no tienen un límite de registro; puede conectar la cantidad de dispositivos que desee sin afectar su licencia de capacidad*. Para obtener más información sobre la concesión de licencias de Panorama, consulte* Registro de Panorama e instalación de licencias*.*



Los nodos del clúster cumplen una de tres funciones:

- **Nodo controlador:** dos nodos controladores gestionan el servicio de cola y la base de datos, generan firmas y gestionar el clúster localmente si no gestiona el clúster con un dispositivo Panorama serie M o un dispositivo virtual. Cada clúster puede tener un máximo de dos nodos controladores. Para la tolerancia a las averías, cada clúster de dispositivos WildFire debe tener un mínimo de dos nodos configurados como un par de HA de nodo controlador principal y nodo controlador de copia de seguridad. A excepción de las condiciones normales de mantenimiento o averías, cada clúster debe tener dos nodos controladores.
- **Nodo de trabajo (cliente del clúster):** los nodos del clúster que no son nodos controladores son nodos de trabajo. Los nodos de trabajo incrementan la capacidad de análisis, la capacidad de almacenamiento y la resistencia de los datos del clúster.
- **Nodo servidor (servidor del clúster)**: el tercer nodo en un clúster WildFire se configura automáticamente como un nodo servidor, un tipo especial de nodo de trabajo que proporciona funciones de redundancia de base de datos e infraestructura, además de capacidades de nodo de trabajo estándar.

Cuando un cortafuegos se registra con un nodo del clúster o cuando añade un dispositivo WildFire que ya tiene cortafuegos registrados en un clúster, el clúster inserta una lista de registro en los cortafuegos conectados. La lista de registro contiene cada nodo en el clúster. Si un nodo del clúster se avería, los cortafuegos conectados a ese clúster se vuelven a registrar con otro nodo del clúster. Este tipo de resistencia es una de las ventajas de crear clústeres de dispositivos WildFire.

Ventaja	Description (Descripción)
Escala	Un clúster de dispositivos WildFire incrementa el rendimiento del análisis y la capacidad de almacenamiento disponibles en una red, de modo que pueda servir a una red mayor de cortafuegos sin segmentar su red.
Alta disponibilidad	Si un nodo del clúster se avería, la configuración de HA proporciona tolerancia a las averías para evitar la pérdida de datos y servicios fundamentales. Si gestiona clústeres centralmente con Panorama, la

Ventaja	Description (Descripción)
	configuración de HA de Panorama proporciona tolerancia a las averías de gestión central.
Distribución única de paquetes de firmas	Todos los cortafuegos conectados a un clúster reciben el mismo paquete de firmas, independientemente del nodo del clúster que recibió o analizó los datos. El paquete de firmas se basa en la actividad y los resultados de todos los miembros del clúster, lo que significa que cada cortafuegos conectado se beneficia del conocimiento combinado del clúster.
Gestión centralizada (Panorama)	Puede ahorrar tiempo y simplificar el proceso de gestión cuando utiliza Panorama para gestionar los clústeres de dispositivos WildFire. En lugar de utilizar la CLI y scripting para gestionar un dispositivo o clúster WildFire, Panorama proporciona una vista unificada de los dispositivos en su red. También puede insertar configuraciones comunes, actualizaciones de configuración y actualizaciones de software en varios clústeres de dispositivos WildFire, y puede realizarlo todo utilizando la interfaz web de Panorama en lugar de la CLI del dispositivo WildFire.
Equilibrio de carga	Cuando un clúster tiene dos o más nodos activos, el clúster automáticamente distribuye y equilibra la carga de los análisis, la generación de informes, la creación de firmas, el almacenamiento y la distribución de contenido de WildFire entre los nodos.

Alta disponibilidad del clúster WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

La alta disponibilidad es una ventaja fundamental de los clústeres de dispositivos WildFire debido a que la HA evita la pérdida de los datos y los servicios fundamentales. Un clúster de HA copia y distribuye datos fundamentales, como los resultados de los análisis, los informes y las firmas en los nodos, de modo que si se produce una avería en un nodo, no se pierdan los datos. Un clúster de HA también proporciona servicios fundamentales redundantes, como la funcionalidad del análisis, la API de WildFire y la generación de firmas, de modo que una avería en un nodo no interrumpa el servicio. Un clúster debe tener al menos dos nodos para proporcionar beneficios de alta disponibilidad. Las averías en el nodo del clúster no afectan al cortafuegos, dado que el cortafuegos registrado en un nodo averiado utiliza la lista de registro del clúster para registrarse en otro nodo del clúster.

El usuario configura cada uno de los dos dispositivos en el par de HA como un dispositivo principal y secundario. Según esta configuración de valor de prioridad inicial, WildFire también asigna un estado operativo activo al dispositivo principal y un estado pasivo al dispositivo secundario. Estos estados determinan cuál dispositivo WildFire se utiliza como el punto de contacto para la gestión y los controles de infraestructura. El dispositivo pasivo siempre se sincroniza con el dispositivo activo y está listo para asumir la función si se produce una avería en el sistema o la red. Por ejemplo, cuando el dispositivo principal en un estado activo (activo-principal) sufre una avería, se produce un evento de conmutación de error y pasa

a un estado pasivo-principal, mientras que el dispositivo secundario pasa al estado activo-secundario. El valor de prioridad asignado originalmente permanece igual independientemente del estado del dispositivo.

La conmutación por error se produce cuando el par de HA ya no es capaz de comunicarse entre sí, no responde o sufre un error fatal. Mientras que el par de HA de WildFire intentará resolver las interrupciones menores de manera automática, los eventos más importantes requieren la intervención del usuario. La conmutación por error también puede producirse cuando el usuario suspende o retira un controlador.

No configure un clúster con un solo nodo controlador. Cada clúster debe tener un par de controladores de HA. Un clúster debe tener un nodo controlador solo en situaciones temporales, por ejemplo, cuando intercambia nodos controladores o si un nodo controlador se avería.

En un par de HA de un clúster de dos nodos, si un nodo controlador se avería, el otro nodo controlador no puede procesar muestras. Para que el nodo del clúster que queda activo procese las muestras, debe configurarlo para que funcione como dispositivo WildFire independiente: elimine la HA y las configuraciones del clúster en el nodo de clúster que queda activo y reinícielo. El nodo vuelve a funcionar como dispositivo WildFire independiente.

Los clústeres de tres nodos operan un par de HA y un nodo de servidor para proporcionar redundancia adicional. El servidor opera los mismos servicios de base de datos e infraestructura del servidor que un controlador, pero no genera firmas. Esta implementación permite al clúster funcionar si un nodo controlador se avería.

Los nodos adicionales que se añaden a un clúster WildFire funcionan como nodos de trabajo o de servidor. El tercer nodo se configura automáticamente como un servidor, mientras que cada una de las siguientes incorporaciones se añade como un trabajador.

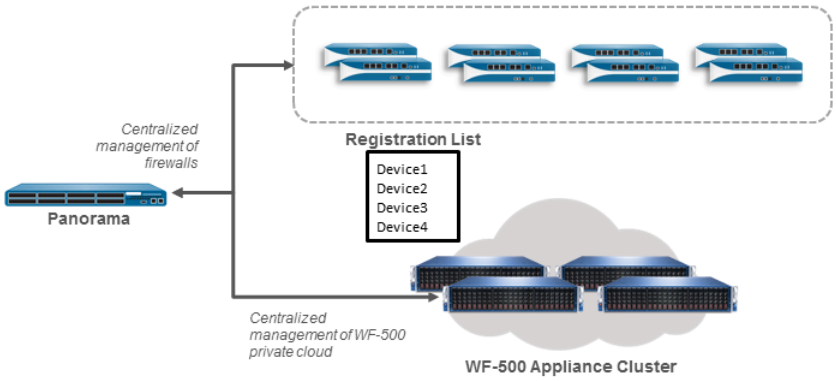
Beneficios de gestionar los clústeres de WildFire con Panorama

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

Si gestiona los clústeres de dispositivos WildFire con Panorama, puede configurar dos dispositivos Panorama serie M o dispositivos virtuales en un par de HA para proporcionar redundancia de gestión. Si no configura dispositivos Panorama redundantes y Panorama se avería, podrá gestionar los clústeres localmente desde un nodo controlador.

Si utiliza un par de HA de Panorama para gestionar el clúster y un Panorama se avería, el otro dispositivo Panorama asume la gestión del clúster. Si un peer de HA de Panorama se avería, restaure el servicio desde el peer de Panorama averiado cuanto antes para restaurar la HA de gestión.

Para proporcionar análisis, almacenamiento y HA de gestión centralizada, se requieren, al menos, dos dispositivos WildFire configurados como nodos controladores de clúster y nodos controladores de copia de seguridad, y dos dispositivos virtuales o serie M de Panorama.



Los cortafuegos reciben una lista de registro que contiene todos los dispositivos WildFire miembros del clúster. Los cortafuegos se pueden registrar con cualquier nodo en el clúster y el clúster automáticamente equilibra la carga entre sus nodos.

Gestión de clústeres de dispositivos Wildfire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para gestionar un clúster de dispositivos WildFire, debe conocer las capacidades de los clústeres y las recomendaciones de gestión.

Category	Description (Descripción)
Operación y configuración del clúster	Configure todos los nodos de los clústeres de manera idéntica para garantizar la consistencia en el análisis y en la comunicación entre dispositivos: • Todos los nodos de los clústeres deben utilizar la misma versión de PAN-OS (PAN-OS 8.0.1 o posterior). Panorama debe ejecutar la misma versión de software que los nodos del clúster o una versión más reciente. Los cortafuegos pueden ejecutar las mismas versiones de software que les permiten enviar muestras a un dispositivo WildFire. Los cortafuegos no requieren una versión determinada de software para enviar muestras a un clúster de dispositivos WildFire. • Los nodos del clúster heredan su configuración del nodo controlador, a excepción de la configuración de la interfaz. Los miembros del clúster supervisan la configuración del nodo controlador y actualizan sus configuraciones cuando el nodo controlador confirma una configuración actualizada. Los nodos de trabajo heredan los ajustes, como la configuración del servidor de actualización de contenido, la configuración del servidor de la nube de WildFire, la imagen del análisis de las muestras, el período de tiempo de conservación de los datos de las muestras, la configuración del entorno de análisis, la configuración de la generación de firmas, la configuración de los logs, la configuración de autenticación, y la configuración del servidor de Panorama, el servidor del DNS y el servidor del NTP. • Cuando gestiona un clúster con Panorama, el dispositivo Panorama inserta una configuración consistente en todos los nodos del clúster. A pesar de que puede cambiar la configuración localmente en un nodo del dispositivo WildFire, Palo Alto Networks no lo recomienda debido a que la próxima vez que un dispositivo Panorama inserte una configuración, sustituirá la configuración actual en el nodo. Por lo general, los cambios locales de los nodos del clúster que gestiona Panorama causan errores de desincronización. • Si la lista de pertenencia de nodos del clúster difiere en los dos nodos controladores, el clúster genera una advertencia de desincronización. Para evitar una condición donde ambos nodos controladores actualicen continuamente la lista de pertenencia desincronizada del otro nodo, se detiene el cumplimiento de la pertenencia del clúster. Cuando esto

Category	Description (Descripción)
	sucede, puede sincronizar las listas de pertenencia del clúster en la CLI local de los nodos controladores y los nodos controladores de copia de seguridad ejecutando el comando operativo **`request high-availability sync-to-remote running-configuration`**. Si existe una diferencia entre la configuración del nodo controlador principal y la configuración del nodo controlador de copia de seguridad, la configuración del nodo controlador principal anula la configuración del nodo controlador de copia de seguridad. En cada nodo controlador, ejecute **`show cluster all-peers`**, y compare y corrija las listas de pertenencia. • Un clúster solo puede tener dos nodos del controlador (principal y de copia de seguridad); los intentos de añadir localmente un tercer nodo del controlador al clúster fallarán. (La interfaz web de Panorama automáticamente evita que añada un tercer nodo controlador). El tercer nodo y los siguientes que se añadan a un clúster deben estar en modo trabajador. • Una característica de las configuraciones de HA es que el clúster distribuye y conserva varias copias de la base de datos, los servicios en cola y los envíos de muestras para proporcionar redundancia en caso de una avería en los nodos del clúster. La ejecución de los servicios adicionales requeridos para proporcionar redundancia de HA tiene un impacto mínimo en el rendimiento. • El clúster comprueba automáticamente si se utilizan direcciones IP duplicadas para la red de entornos de análisis. • Si un nodo pertenece a un clúster y desea moverlo a un clúster diferente, primero debe eliminar el nodo del clúster actual. • No cambie la dirección IP de los dispositivos WildFire que estén operando en ese momento en un clúster. Si lo hace, se anulará el registro del nodo del cortafuegos asociado.
Políticas de conservación de datos del clúster	Las políticas de conservación de datos determinan por cuánto tiempo el clúster de dispositivos WildFire almacena los diferentes tipos de muestras. • **Muestras benignas y de grayware:** el clúster retiene las muestras benignas y de grayware de 1 a 90 días (el valor predeterminado es 14). • **Muestras malintencionadas:** el clúster retiene las muestras malintencionadas por un mínimo de 1 día (el valor predeterminado es indefinido, no se eliminan). Las muestras malintencionadas pueden incluir muestras con veredicto de phishing. Configure la misma política de conservación de datos en todo el clúster (4 en Configuración general del clúster localmente o 4en Configuración general del clúster en Panorama).

Category	Description (Descripción)
Networking	No se permite la comunicación entre clústeres de dispositivos WildFire. Los nodos se comunican entre sí dentro de un clúster determinado, pero no se comunican con nodos en otros clústeres. Todos los miembros del clúster deben respetar lo siguiente: • utilizar una interfaz dedicada de gestión de clúster para la gestión y la comunicación del clúster (forzada en Panorama), • tener una dirección IP estática en la misma subred, y • utilizar conexiones de baja latencia entre los nodos del clúster. El valor máximo de latencia para una conexión no debe ser mayor a 500 ms.
Interfaz dedicada de gestión del clúster	La interfaz dedicada de gestión del clúster permite que los nodos controladores gestionen el clúster y es una interfaz diferente a la interfaz de gestión estándar (Ethernet0). Panorama fuerza la configuración de una interfaz dedicada de gestión del clúster. *Si el enlace de gestión del clúster falla entre dos nodos controladores en una configuración de dos nodos, los servicios del nodo controlador de copia de seguridad y el análisis de la muestra continúan incluso si no existe comunicación de gestión con el nodo controlador principal. Esto se debe a que cuando el enlace de gestión del clúster falla, el nodo controlador de copia de seguridad no sabe si el nodo controlador principal funciona, lo que produce una condición de división. El nodo controlador de copia de seguridad debe continuar proporcionando servicios del clúster en caso de que el nodo controlador principal no funcione. Cuando el enlace de gestión del clúster se restaura, los datos de cada nodo controlador se fusionan.*
DNS:	Puede utilizar el nodo controlador en un clúster de dispositivos WildFire como el servidor DNS de autoridad para el clúster. (Un servidor DNS de autoridad sirve a las direcciones IP reales de los miembros del clúster, a diferencia de un servidor DNS recursivo, que envía una consulta al servidor DNS de autoridad y pasa la información solicitada al host que realizó la solicitud inicial). Los cortafuegos que envían muestras al clúster de dispositivos WildFire deben enviar consultas de DNS a sus servidores DNS regulares, por ejemplo, un servidor DNS corporativo interno. El servidor DNS interno reenvía la consulta de DNS al controlador del clúster de dispositivos WildFire (según el dominio de la consulta). Utilizar el controlador del clúster como servidor DNS proporciona varias ventajas: • **Equilibrio automático de carga:** cuando el controlador del clúster resuelve el nombre del host de anuncio de servicio, los nodos del clúster

Category	Description (Descripción)
	del host están en orden aleatorio, lo que equilibra de manera orgánica la carga de los nodos. • **Tolerancia a las averías:** si un nodo del clúster se avería, el controlador del clúster lo retira de la respuesta del DNS automáticamente, de modo que los cortafuegos puedan enviar las solicitudes nuevas a los nodos que se encuentran en funcionamiento. • **Flexibilidad y facilidad de gestión:** cuando añade nodos al clúster, dado que el controlador actualiza la respuesta del DNS automáticamente, no debe realizar cambios en el cortafuegos y las solicitudes se dirigen automáticamente a los nuevos nodos, además de los nodos existentes. A pesar de que el registro del DNS no debe almacenarse en caché, para solucionar problemas, si la búsqueda de DNS se produce correctamente, el TTL es 0. Sin embargo, cuando la búsqueda de DNS brinda un resultado de NXDOMAIN, el TTL y el TTL mínimo son ambos 0.
Gestión	Puede gestionar los clústeres de dispositivos WildFire con la CLI local de WildFire o Panorama. Existen dos funciones administrativas disponibles localmente en los nodos del clúster WildFire: • **Superreader (superlector)**: acceso de solo lectura. • **Superuser (superusuario)**: acceso de lectura y escritura.
Registro del cortafuegos	Los clústeres de dispositivos WildFire insertan una lista de registro que contiene todos los nodos en un clúster en cada cortafuegos conectado a un nodo del clúster. Cuando registra un cortafuegos con un dispositivo en un clúster, el cortafuegos recibe la lista de registro. Cuando añade un dispositivo WildFire independiente que ya tiene cortafuegos conectados a un clúster, de modo que se convierte en un nodo de clúster, estos cortafuegos reciben una lista de registro. Si un nodo se avería, los cortafuegos conectados utilizan la lista de registro para registrar el próximo nodo en la lista.
Migración de datos	Para proporcionan redundancia de datos, los nodos del dispositivo WildFire en un clúster comparten la base de datos, el servicio de cola y el contenido de envío de muestras. Sin embargo, la ubicación precisa de este dato depende de la topología del clúster. Como resultado, los dispositivos WildFire en un clúster realizan migración de datos o reorganización de los datos siempre que se realizan cambios de topología. Los cambios de topología incluyen la incorporación y la eliminación de nodos, además del cambio de función de un nodo existente. La migración de datos también se produce cuando las bases de datos se convierten a una versión más reciente, como la actualización de WildFire 7.1 a 8.0. El estado de la migración de datos puede verse si se ejecutan los comandos de estado desde la CLI de WildFire. Este proceso puede tardar varias horas, según la cantidad de datos en los dispositivos WildFire.

Implementación de un clúster WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para implementar un clúster de dispositivos WildFire, debe actualizar todos los dispositivos que se inscribirán en el clúster, crear el clúster WildFire y configurarlo para que se adapte a sus necesidades. Puede realizar estas tareas localmente desde la CLI del dispositivo WildFire o mediante Panorama, lo que le permite aplicar cambios de configuración y actualizaciones rápidamente a dispositivos WildFire conectados.

El siguiente procedimiento muestra cómo crear y configurar un par de alta disponibilidad (high availability, HA) de WildFire y añadir nodos de dispositivos adicionales a un clúster.

STEP 1 | Actualice sus dispositivos WildFire localmente a PAN-OS 8.0.1 o posterior, la versión mínima compatible para operar los clústeres.

STEP 2 | Cree, configure y añada nodos a un clúster de dispositivos WildFire.

- Configuración de clústeres e incorporación de nodos localmente
- Configuración de clústeres e incorporación de nodos en Panorama

STEP 3 | Configuración general del clúster de dispositivos WildFire.

- Configuración general del clúster localmente
- Configuración general del clúster en Panorama

STEP 4 | (Opcional) Realice el cifrado de comunicaciones de dispositivo a dispositivo dentro de un clúster de WildFire.

- Configuración del cifrado de dispositivo a dispositivo con certificados predefinidos mediante la CLI
- Configuración del cifrado de dispositivo a dispositivo con certificados personalizados mediante la CLI
- Configuración del cifrado de dispositivo a dispositivo mediante certificados predefinidos centralmente en Panorama
- Configuración del cifrado de dispositivo a dispositivo mediante certificados personalizados centralmente en Panorama

STEP 5 | Compruebe que su clúster de dispositivos WildFire funcione normalmente.

- Visualización del estado del clúster WildFire con la CLI
- Visualización del estado del clúster WildFire con Panorama

STEP 6 | (Opcional) Actualice los dispositivos WildFire ya inscritos en un clúster.

- Actualización de un clúster localmente con una conexión a internet
- Actualización de un clúster localmente sin una conexión a internet
- Actualización de un clúster centralmente en Panorama con una conexión a internet
- Actualización de un clúster centralmente en Panorama sin una conexión a internet

Configuración local de un clúster en dispositivos WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Antes de configurar un clúster de dispositivos WildFire localmente, proporcione dos dispositivos WildFire para configurarlos como par de nodos controladores de alta disponibilidad y los dispositivos WildFire necesarios que funcionen como nodos de trabajo para incrementar la capacidad de análisis y almacenamiento, y la resistencia del clúster.

Si los dispositivos WildFire son nuevos, consulte Comenzar con WildFire para garantizar que ha completado los pasos básicos como confirmar que su licencia de WildFire esté activa, habilitar el registro, conectar los cortafuegos a los dispositivos WildFire y configurar las funciones básicas de WildFire.

Si administra el clúster del dispositivo WildFire con Panorama, también puede configurar el clúster de WildFire centralmente en Panorama.

Para crear clústeres de dispositivos WildFire, debe actualizar todos los dispositivos WildFire que desee ubicar en un clúster a PAN-OS 8.0.1 o posterior. En cada dispositivo que desee añadir a un clúster, ejecute ***show system info | match version*** *en la CLI del dispositivo WildFire para garantizar que el dispositivo ejecute la versión PAN-OS 8.0.1 o posterior.*

Cuando sus dispositivos WildFire estén disponibles, realice las siguientes tareas:

- Configuración de clústeres e incorporación de nodos localmente
- Configuración general del clúster localmente
- Eliminación de un nodo de un clúster localmente

Configuración de clústeres e incorporación de nodos localmente

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Cuando añade nodos a un clúster, el clúster automáticamente configura la comunicación entre los nodos según las interfaces que configura para el nodo controlador.

STEP 1 | Asegúrese de que cada dispositivo WildFire que desea añadir al clúster ejecute PAN-OS 8.0.1 o posterior.

En cada dispositivo WildFire, ejecute lo siguiente:

```
admin@WF-500> show system info | match version
```

STEP 2 | Verifique que los dispositivos WildFire no analicen las muestras y que se encuentren en estado independiente (no sean miembros de otro clúster).

1. En cada dispositivo, muestre si el dispositivo está analizando las muestras:

   ```
   admin@WF-500> show wildfire global sample-analysis
   ```

   Ninguna muestra debe mostrar el valor `pending`. Todas las muestras deben estar en estado Finalizado. Si las muestras tienen un valor `pending`, espere a que el análisis finalice. Las muestras con valor `Pending` se muestran separadas de las muestras malintencionadas y no malintencionadas. El valor `Finish Date` muestra la fecha y la hora en la que finalizó el análisis.
2. En cada dispositivo, verifique que todos los procesos se están ejecutando:

   ```
   admin@WF-500> show system software status
   ```
3. En cada dispositivo, verifique que el dispositivo se encuentre en estado independiente y que no pertenezca a un clúster:

   ```
   admin@WF-500> show cluster membership Service Summary: wfpc
    signature Cluster name: Address: 10.10.10.100 Host name:
    WF-500 Node name: wfpc-000000000000-internal Serial number:
    000000000000 Node mode: stand_alone Server role: True HA
    priority: Last changed: Mon, 06 Mar 2017 16:34:25 -0800
    Services: wfcore signature wfpc infra Monitor status: Serf
    Health Status: passing Agent alive and reachable Application
    status: global-db-service: ReadyStandalone wildfire-apps-
   service: Ready global-queue-service: Servicio de gestión de
    wildfire ReadyStandalone Done siggen-db: ReadyMaster Diag
    report: 10.10.10.100: reported leader '10.10.10.100', age 0.
    10.10.10.100: local node passed sanity check.
   ```

   Las líneas resaltadas muestran que el nodo se encuentra en modo independiente y está listo para convertirse de un dispositivo independiente a un nodo de un clúster.

   El número de serie de 12 dígitos en estos ejemplos (`000000000000`) es un ejemplo genérico y no es un número de serie real. Los dispositivos WildFire en su red tienen números de serie reales y únicos.

STEP 3 | Configure el nodo controlador principal.

Esto incluye configurar el nodo como el controlador principal del par de HA, habilitar la HA y definir las interfaces que utiliza el dispositivo para el enlace de control de HA, y para la comunicación y la gestión de los clústeres.

1. Habilite la alta disponibilidad y configure la conexión de la interfaz del enlace de control al nodo controlador de copia de seguridad, por ejemplo, en la interfaz eth3:

   ```
   admin@WF-500# set deviceconfig high-availability enabled yes
    interface ha1 port eth3 peer-ip-address <secondary-node-eth3-
   ip-address>
   ```

2. Configure el dispositivo como el nodo controlador principal:

   ```
   admin@WF-500# set deviceconfig high-availability election-
   option priority primary
   ```

3. (Opcional) Configure la interfaz de alta disponibilidad de copia de seguridad entre el nodo controlador y el nodo controlador de copia de seguridad, por ejemplo, en la interfaz de gestión:

   ```
   admin@WF-500# set deviceconfig high-availability interface
    ha1-backup port management peer-ip-address <secondary-node-
   management-ip-address>
   ```

4. Configure la interfaz especializada para la comunicación y la gestión en el clúster, especifique el nombre del clúster y configure la función del nodo como nodo controlador:

   ```
   admin@WF-500# set deviceconfig cluster cluster-name <name>
    interface eth2 mode controller
   ```

   Este ejemplo utiliza eth2 como el puerto de comunicación del clúster especializado.

   El nombre del clúster debe ser un nombre de subdominio válido con una longitud mínima de 63 caracteres. Solo se permiten caracteres en minúsculas y números, además de guiones y puntos si no están al principio o al final del nombre del clúster.

STEP 4 | Configure el nodo controlador de copia de seguridad.

Esto incluye configurar el nodo como el controlador de copia de seguridad del par de HA, habilitar la HA y definir las interfaces que utiliza el dispositivo para el enlace de control de HA, y para la comunicación y la gestión de los clústeres.

1. Habilite la alta disponibilidad y configure la conexión de la interfaz del enlace de control al nodo controlador principal en la misma interfaz utilizada en el nodo controlador principal (eth3 en este ejemplo):

   ```
   admin@WF-500# set deviceconfig high-availability enabled yes
    interface ha1 port eth3 peer-ip-address <primary-node-eth3-
   ip-address>
   ```

2. Configure el dispositivo como el nodo controlador de copia de seguridad:

   ```
   admin@WF-500# set deviceconfig high-availability election-
   option priority secondary
   ```

3. (Recomendado) Configure la interfaz de alta disponibilidad de copia de seguridad entre el nodo controlador de copia de seguridad y el nodo controlador, por ejemplo, en la interfaz de gestión:

   ```
   admin@WF-500# set deviceconfig high-availability interface
    ha1-backup port management peer-ip-address <primary-node-
   management-ip-address>
   ```

4. Configure la interfaz especializada para la comunicación y la gestión en el clúster, especifique el nombre del clúster y configure la función del nodo como nodo controlador:

   ```
   admin@WF-500# set deviceconfig cluster cluster-name <name>
    interface eth2 mode controller
   ```

STEP 5 | Confirme las configuraciones en ambos nodos controladores.

En cada nodo controlador:

```
admin@WF-500# commit
```

Confirmar la configuración en ambos nodos controladores forma un clúster de dos nodos.

STEP 6 | Verifique la configuración en el nodo controlador principal.

En el nodo controlador principal:

```
admin@WF-500(active-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: mycluster Address:
 10.10.10.100 Host name: WF-500 Node name: wfpc-000000000000-
internal Serial number: 000000000000 Node mode: controller
 Server role: True HA priority: primary Last changed: Sat, 04
 Mar 2017 12:52:38 -0800 Services: wfcore signature wfpc infra
 Monitor status: Serf Health Status: passing Agent alive and
 reachable Application status:  global-db-service: JoinedCluster
```



```
 wildfire-apps-service: Ready  global-queue-service: JoinedCluster
 wildfire-management-service: Done  siggen-db: ReadyMaster Diag
 report: 10.10.10.110: reported leader '10.10.10.100', age 0.
 10.10.10.100: local node passed sanity check.
```

El mensaje (`active-controller`) y las líneas resaltadas `Application status` muestran que el nodo está en modo controlador, está listo y es el nodo controlador principal.

STEP 7 | Verifique la configuración en el nodo controlador secundario.

En el nodo controlador secundario:

```
admin@WF-500(passive-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: mycluster Address:
 10.10.10.110 Host name: WF-500 Node name: wfpc-000000000000-
internal Serial number: 000000000000 Node mode: controller Server
 role: True HA priority: secondary Last changed: Fri, 02 Dec
 2016 16:25:57 -0800 Services: wfcore signature wfpc infra
 Monitor status: Serf Health Status: passing Agent alive and
 reachable Application status:  global-db-service: JoinedCluster
 wildfire-apps-service: Ready  global-queue-service: JoinedCluster
 wildfire-management-service: Done  siggen-db: ReadySlave Diag
 report: 10.10.10.110: reported leader '10.10.10.100', age 0.
 10.10.10.110: local node passed sanity check.
```

El mensaje (`passive-controller`) y las líneas resaltadas `Application status` muestran que el nodo está en modo controlador, está listo y es el nodo del controlador de copia de seguridad.

STEP 8 | Compruebe la configuración del nodo.

Verifique que las claves de API del nodo controlador se visualicen globalmente:

```
admin@WF-500(passive-controller)> show wildfire global api-keys
 allService Summary: wfpc signatureCluster name: mycluster
```

Las claves de API de ambos dispositivos deben visualizarse.

STEP 9 | Sincronice manualmente las configuraciones de alta disponibilidad en los nodos controladores.

La sincronización de los nodos controladores garantiza que las configuraciones coincidan y solo debe hacerse una vez. Tras sincronizar las configuraciones de alta disponibilidad, los nodos controladores mantienen las configuraciones sincronizadas y no debe volver a sincronizarlas.

1. En el nodo controlador principal, sincronice la configuración de alta disponibilidad con el nodo controlador del peer remoto:

   ```
   admin@WF-500(active-controller)> request high-availability
    sync-to-remote running-config
   ```

   Si existe una diferencia entre la configuración del nodo controlador principal y la configuración del nodo controlador de copia de seguridad, la configuración del nodo controlador principal anula la configuración del nodo controlador de copia de seguridad.
2. Confirme la configuración:

   ```
   admin@WF-500# commit
   ```

STEP 10 | Verifique que el clúster funcione adecuadamente.

Para verificar información relacionada con el cortafuegos, primero debe conectar al menos un cortafuegos a un nodo de clúster seleccionando ***Device (Dispositivo)*** *>* ***Setup (Configuración)*** *>* ***WildFire*** *y editando la* ***General Settings (Configuración general)*** *para que apunte al nodo.*

1. Muestre los peer del clúster para garantizar que ambos controladores sean miembros del clúster:

   ```
   admin@WF-500(active-controller)> show cluster all-peers
   ```
2. Muestre las claves del API de ambos nodos (si creó claves de API) de cada nodo controlador:

   ```
   admin@WF-500(active-controller)> show wildfire global api-keys
    all
   ```
3. Acceda a cualquier muestra desde cualquier nodo controlador:

   ```
   admin@WF-500(active-controller)> show wildfire global sample-
   status sha256 equal <value>
   ```
4. Los cortafuegos pueden registrar y cargar archivos a ambos nodos. Confirme que el cortafuegos reenvía muestras correctamente.
5. Ambos nodos pueden descargar y analizar archivos.
6. Todos los archivos que se analizan tras la creación del clúster muestran dos ubicaciones de almacenamiento, una en cada nodo.

STEP 11 | (Opcional) Configure un nodo trabajador y añádalo al clúster.

Los nodos de trabajo utilizan la configuración del nodo controlador de modo que el clúster tenga una configuración consistente. Puede añadir hasta 18 nodos de trabajo a un clúster para obtener un total de 20 nodos en un clúster.

1. En el nodo controlador principal, añada el trabajador a la lista de trabajadores del nodo controlador:

   ```
   admin@WF-500(active-controller)> configure
    admin@WF-500(active-controller)# set deviceconfig cluster
    mode controller worker-list <ip>
   ```

   La *<ip>es la dirección IP de la interfaz de gestión del clúster* del nodo trabajador que desea añadir al clúster. Utilice comandos separados para añadir cada nodo trabajador al clúster.
2. Confirme la configuración del nodo controlador:

   ```
   admin@WF-500(active-controller)# commit
   ```
3. En el dispositivo WildFire que desea convertir a un nodo trabajador del clúster, configure el clúster al que se unirá, establezca la interfaz de comunicación del clúster y ubique el dispositivo en modo `worker`:

   ```
   admin@WF-500> configure admin@WF-500# set deviceconfig cluster
    cluster-name <name> interface eth2 mode worker
   ```

   La interfaz de comunicación del clúster debe ser la misma interfaz especificada para las comunicaciones dentro del clúster en los nodos controladores. En este ejemplo, `eth2` es la interfaz configurada en los nodos controladores para la comunicación del clúster.
4. Confirme la configuración en el nodo trabajador:

   ```
   admin@WF-500# commit
   ```
5. Espere a que todos los servicios aparezcan en el nodo trabajador. Ejecute **`show cluster membership`** y compruebe que el `estado de la aplicación` muestre todos los servicios, y que `siggen-db` esté en el estado `Ready (Listo)` cuando todos los servicios funcionen.
6. En cualquier nodo controlador del clúster, compruebe que se añadió el nodo trabajador:

   ```
   admin@WF-500> show cluster all-peers
   ```

   El nodo trabajador que añadió aparece en la lista de nodos del clúster. Si añadió el dispositivo WildFire equivocado a un clúster accidentalmente, es posible llevar a cabo la Eliminación de un nodo de un clúster localmente.

STEP 12 | Verifique la configuración en el nodo trabajador.

1. En el nodo trabajador, realice la comprobación para garantizar que el campo `Node mode` muestre que el nodo está en modo trabajador:

   ```
   admin@WF-500> show cluster membership
   ```

2. Verifique que los cortafuegos puedan registrarse en el nodo trabajador y que en nodo trabajador pueda descargar y analizar archivos.

Configuración general del clúster localmente

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Algunos ajustes son opcionales y parte de la configuración general se rellena previamente con valores predeterminados. Se recomienda comprobar al menos esta configuración para garantizar que la configuración del clúster se adapte a sus necesidades. La configuración general incluye lo siguiente:

- la conexión a la nube pública de WildFire y el envío de muestras a la nube pública,
- la configuración de las políticas de conservación de datos,
- la configuración del registro,
- la configuración del entorno de análisis (la imagen de VM que se adapta mejor a su entorno) y la personalización del entorno de análisis para analizar mejor a los tipos de muestras que el cortafuegos envía a WildFire, y
- la configuración de las direcciones IP para el servidor DNS, el servidor NTP, etc.

Lleve a cabo la Configuración de WildFire utilizando la CLI en el nodo controlador principal del clúster. El resto de los nodos del clúster utilizan la configuración en el controlador del clúster.

STEP 1 | Realice la configuración general del clúster WildFire. Este proceso es similar a la Configuración del dispositivo WildFire.

1. (Recomendado) Restablezca la contraseña del administrador.
2. Configure los ajustes de interfaz de gestión. Establezca las direcciones IP del nodo del clúster de dispositivos WildFire y la puerta de enlace predeterminada. Cada nodo del clúster de dispositivos WildFire debe tener una dirección IP estática en la misma subred. Además, establezca las direcciones IP del servidor DNS.
3. Configure el reloj del dispositivo WildFire Establezca el reloj manualmente o especificando los servidores NTP, y establezca la autenticación del servidor NTP.
4. Seleccione la imagen de máquina virtual que el dispositivo debe utilizar para el análisis de archivos.
5. (Opcional) Permita que usuarios adicionales gestionen el dispositivo WildFire. Añada cuentas de administrador y asígneles funciones para gestionar el clúster.
6. Configure la autenticación RADIUS para el acceso de administrador.

STEP 2 | (Opcional) Conecte el clúster a la nube pública de WildFire y configure los servicios de nube que utilizará el clúster.

Si los motivos comerciales no evitan que conecte el clúster de dispositivos WildFire a la nube pública de WildFire, la conexión del clúster a la nube proporciona beneficios como los siguientes:

- Utilizar los recursos de la nube para realizar análisis de muestras en varios entornos y utilizar diferentes métodos.
- Consultar automáticamente a la nube acerca de los veredictos antes de realizar el análisis local para reducir el trabajo del clúster. (De forma predeterminada, esta opción está deshabilitada).
- Ventajas y contribuciones a la inteligencia de la comunidad global de WildFire.

Las funciones que se describen en esta fila de la tabla no son específicas de un clúster. También puede configurar estas funciones en dispositivos WildFire independientes.

1. Ventajas de la inteligencia recogida de todos los dispositivos WildFire conectados:

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-server <hostname-value>
```

   El valor predeterminado para el nombre de host del servidor de nube pública de WildFire es `wildfire-public-cloud`. Puede realizar el Envío de archivos para el análisis de WildFire a cualquier nube pública de WildFire.

2. Si conecta el clúster a una nube pública de WildFire, configure si desea consultar automáticamente a la nube pública acerca de los veredictos antes de realizar el análisis local. Consultar a la nube pública en primer lugar reduce la carga del clúster local de WildFire:

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-intelligence cloud-query (no | yes)
```

3. Si conecta el clúster a una nube pública de WildFire, configure los tipos de información para los que desea realizar el Envío de malware descubierto localmente o informes a la nube pública de WildFire (datos de diagnóstico, informes XML acerca del análisis de malware, muestras de malware). Si envía muestras de malware, el clúster no envía informes.

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-intelligence submit-diagnostics (no | yes)
 submit-report (no | yes) submit-sample (no | yes)
```

STEP 3 | (Opcional) Configure el nodo controlador para que anuncie el estado del servicio utilizando un protocolo DNS.

```
admin@WF-500(active-controller)# set deviceconfig cluster mode
 controller service-advertisement dns-service enabled yes
```


STEP 4 | (Opcional) Configure las políticas de conservación de datos para las muestras malintencionadas y benignas o de grayware.

1. Seleccione la cantidad de tiempo durante el cual se conservarán los diferentes tipos de datos:

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire file-retention malicious <indefinite | 1-2000> non-
malicious <1-90>
```

El valor predeterminado para conservar las muestras malintencionadas es indefinido (no se eliminan). El valor predeterminado para conservar las muestras no malintencionadas (benignas y grayware) es de 14 días.

STEP 5 | (Opcional) Configure el entornos de análisis preferido.

1. Si su entorno de análisis analiza en su mayoría muestras ejecutables o muestras de documentos, puede asignar la mayoría de los recursos del clúster al análisis de esos tipos de muestras:

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire preferred-analysis-environment (Documents |
 Executables | default)
```

En cada dispositivo WildFire en el clúster:

- La opción `default` (predeterminado) permite analizar simultáneamente 16 documentos, 10 ejecutables portables (portable executables, PE) y 2 enlaces de correo electrónico.
- La opción Documents (Documentos) permite analizar simultáneamente 25 documentos, 1 PE y 2 enlaces de correo electrónico.
- La opción Executables (Ejecutables) permite analizar simultáneamente 25 PE, 1 documento y 2 enlaces de correo electrónico.

Puede configurar un entorno de análisis preferido diferente para cada nodo en el clúster. (Si gestiona el clúster desde Panorama, Panorama puede establecer el entorno de análisis para todo el clúster).

STEP 6 | Configure el análisis del nodo.

1. (Opcional) Realice la Configuración de las actualizaciones de contenido para mejorar el análisis del malware.
2. Realice la Configuración de la interfaz de VM para permitir que el clúster observe los comportamientos malintencionados donde la muestra que se analiza busca acceso a la red.
3. (Opcional) Realice la Habilitación de firmas locales y generación de categorías URL para generar firmas de DNS y antivirus, además de categorías de URL.

STEP 7 | Configure el registro.

1. Configuración de los ajustes del log de envíos a WildFire.

Eliminación de un nodo de un clúster localmente

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede eliminar nodos del clúster utilizando la CLI local. El procedimiento para eliminar un nodo es diferente en un clúster de dos nodos que en un clúster con tres o más nodos.

- Elimine el nodo de trabajo de un clúster de tres o más nodos.
  1. Retire el nodo de trabajo desde la CLI del nodo de trabajo:

     ```
     admin@WF-500> request cluster decommission start
     ```

     El comando `decommission` solo funciona en los clústeres con tres o más nodos. No utilice `decommission` para eliminar un nodo de un clúster de dos nodos.
  2. Confirme que el retiro del nodo se haya realizado con éxito:

     ```
     admin@WF-500> show cluster membership
     ```

     Este comando informa `decommission: success` una vez que se haya eliminado el nodo de trabajo del clúster. Si el comando no muestra una retirada correcta, espere unos minutos para permitir que se complete la retirada y ejecute el comando nuevamente.
  3. Elimine la configuración del clúster desde la CLI del nodo de trabajo:

     ```
     admin@WF-500># delete deviceconfig cluster
     ```
  4. Confirme la configuración:

     ```
     admin@WF-500># commit
     ```
  5. Confirme que todos los procesos funcionen:

     ```
     admin@WF-500> show system software status
     ```
  6. Elimine el nodo de trabajo de la lista de trabajo del nodo controlador:

     ```
     admin@WF-500(active-controller)# delete deviceconfig cluster
      mode controller worker-list <worker-node-ip>
     ```
  7. Confirme la configuración:

     ```
     admin@WF-500(active-controller)# commit
     ```
  8. En el nodo controlador, compruebe que el nodo de trabajo se haya eliminado:

     ```
     admin@WF-500(active-controller)> show cluster all-peers
     ```

     El nodo de trabajo que eliminó no aparece en la lista de nodos del clúster.

- Elimine un nodo controlador de un clúster de dos nodos.

  Cada clúster debe tener dos nodos de controlador en una configuración de alta disponibilidad bajo condiciones normales. Sin embargo, es posible que el mantenimiento o el intercambio de los nodos controladores requiera eliminar un nodo controlador de un clúster utilizando la CLI:

  1. Suspenda el nodo controlador que desea eliminar:

     ```
     admin@WF-500(passive-controller)> debug cluster suspend on
     ```

  2. En el nodo controlador que desea eliminar, quite la configuración de alta disponibilidad. Este ejemplo le muestra cómo eliminar el nodo controlador de copia de seguridad:

     ```
     admin@WF-500(passive-controller)> configure
      admin@WF-500(passive-controller)# delete deviceconfig high-availability
     ```

  3. Elimine la configuración del clúster:

     ```
     admin@WF-500(passive-controller)# delete deviceconfig cluster
     ```

  4. Confirme la configuración:

     ```
     admin@WF-500(passive-controller)# commit
     ```

  5. Espere que los servicios vuelvan a funcionar. Ejecute **`show cluster membership`** y compruebe `Application status`, que muestra a todos los servicios y a `siggen-db` en un estado `Ready` cuando todos los servicios funcionan. El `Node mode` (modo del nodo) debe ser `stand_alone` (independiente).
  6. En el nodo restante del clúster, compruebe que se eliminó el nodo:

     ```
     admin@WF-500(active-controller)> show cluster all-peers
     ```

     El nodo controlador que eliminó no aparece en la lista de nodos del clúster.
  7. Si tiene otro dispositivo WildFire listo, añádalo al clúster cuanto antes para restaurar la alta disponibilidad (Configuración de clústeres e incorporación de nodos localmente).

     Si no tiene otro dispositivo WildFire listo para sustituir el nodo del clúster eliminado, debe eliminar las configuraciones de alta disponibilidad y del clúster del nodo restante del clúster debido a que los clústeres de un nodo no se recomiendan y no proporcionan alta disponibilidad. Se recomienda gestionar un dispositivo WildFire como un dispositivo independiente, no como un clúster de un nodo.

     Para eliminar las configuraciones de alta disponibilidad y de clúster del nodo restante (en este ejemplo, el nodo controlador principal), ejecute los siguientes comandos:

     ```
     admin@WF-500(active-controller)> configure
      admin@WF-500(active-controller)# delete deviceconfig
     ```



```
high-availability admin@WF-500(active-controller)# delete
deviceconfig cluster admin@WF-500(active-controller)# commit
```

Espere que los servicios vuelvan a funcionar. Ejecute **`show cluster membership`** y compruebe `Application status`, que muestra a todos los servicios y a `siggen-db` en un estado `Ready` cuando todos los servicios funcionan. El `Node mode` (modo del nodo) debe ser `stand_alone` (independiente).

Configuración del cifrado de dispositivo a dispositivo de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede cifrar las comunicaciones de WildFire entre dispositivos implementados en un clúster. De manera predeterminada, los dispositivos WildFire envían datos sin formato cuando se comunican con dispositivos de gestión, así como entre peers de clústeres de WildFire. Puede usar los certificados predefinidos o personalizados para autenticar las conexiones entre el dispositivo WildFire mediante el protocolo IKE/IPsec. Los certificados predefinidos cumplen con los requisitos actuales de cumplimiento y la certificación aprobada por FIPS/CC/UCAPL. Si desea usar los certificados personalizados, debe seleccionar un certificado que cumplan con FIPS/CC/UCAPL o no podrá importar el certificado.

Puede configurar el cifrado de dispositivo a dispositivo de WildFire localmente utilizando la CLI de WildFire o centralmente con Panorama. Tengan en cuenta que todos los dispositivos WildFire dentro de un clúster determinado deben ejecutar una versión de PAN-OS que admita las comunicaciones cifradas.

Si los dispositivos WildFire de su clúster usan el modo FIPS/CC, el cifrado se habilita automáticamente con los certificados predefinidos.

De acuerdo con la forma en que desea implementar el cifrado de dispositivo a dispositivo, lleve a cabo una de las siguientes tareas:

- Configuración del cifrado de dispositivo a dispositivo mediante certificados predefinidos centralmente en Panorama
- Configuración del cifrado de dispositivo a dispositivo mediante certificados personalizados centralmente en Panorama
- Configuración del cifrado de dispositivo a dispositivo con certificados predefinidos mediante la CLI
- Configuración del cifrado de dispositivo a dispositivo con certificados personalizados mediante la CLI

Configuración del cifrado de dispositivo a dispositivo con certificados predefinidos mediante la CLI

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Cuando configura el cifrado de dispositivo a dispositivo con la CLI, debe emitir todos los comandos desde el dispositivo WildFire designado como el controlador activo. Los cambios en la configuración se distribuyen automáticamente al controlador pasivo. Si opera un clúster con 3 o más nodos, también debe configurar que los dispositivos del clúster WildFire actúen como nodos servidores con los mismos ajustes que el controlador activo.

STEP 1 | Actualice cada dispositivo WildFire gestionado a PAN-OS 9.0.

STEP 2 | Verifique que su clúster de dispositivos WildFire se haya configurado correctamente y funcione de manera aceptable.

STEP 3 | Habilite la comunicación segura del clúster en el dispositivo WildFire designado como el controlador activo.

```
set deviceconfig cluster encryption enabled yes
```

STEP 4 | (Recomendado) Haga clic en **Enable (Habilitar)** para habilitar el cifrado de tráfico de HA. Esta configuración opcional cifra el tráfico de HA entre el par de HA y es una de las mejores prácticas recomendadas de Palo Alto Networks.

El cifrado del tráfico de HA no se puede deshabilitar cuando funciona en modo FIPS/CC.

```
set deviceconfig high availability encryption enabled yes
```

STEP 5 | (Solo en clústeres de dispositivos con 3 o más nodos) Repita los pasos del 2 al 4 para el tercer nodo de servidor del dispositivo WildFire inscrito en el clúster.

Configuración del cifrado de dispositivo a dispositivo con certificados personalizados mediante la CLI

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Cuando configura el cifrado de dispositivo a dispositivo con la CLI, debe emitir todos los comandos desde el dispositivo WildFire designado como el controlador activo. Los cambios en la configuración se distribuyen automáticamente al controlador pasivo. Si opera un clúster con 3 o más nodos, también debe configurar que los dispositivos del clúster WildFire actúen como nodos servidores con los mismos ajustes que el controlador activo.

STEP 1 | Actualice cada dispositivo WildFire gestionado a PAN-OS 9.0.

STEP 2 | Verifique que su clúster de dispositivos WildFire se haya configurado correctamente y funcione de manera aceptable.

STEP 3 | Importe (u opcionalmente, genere) un certificado con una clave privada y su certificado de CA. Tenga en cuenta que si ya configuró el dispositivo WildFire y el cortafuegos para las comunicaciones seguras mediante la utilización de un certificado personalizado, también puede utilizar ese certificado personalizado para garantizar las comunicaciones seguras entre los dispositivos WildFire.

1. Para importar un certificado personalizado, escriba lo siguiente desde la CLI del dispositivo WildFire: **certificado de importación scp desde el formato <value>**de frase de contraseña <value> de nombre <value> de certificado de origen-ip <ip/netmask> de puerto <1-65535> remoto de <value> archivo <value>

2. Para generar un certificado personalizado, especifique lo siguiente en la CLI del dispositivo WildFire: **request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry hostname [...] request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry ip [...] request certificate generate certificate-name name**.

STEP 4 | Importe el par de claves del dispositivo WildFire que contienen el certificado del servidor y la clave privada.

```
SCP Importar par de claves desde <value> el archivo <value> de
 puerto <1-65535> remoto origen-IP <ip/netmask> formato de frase de
 contraseña <value> de nombre <value> de certificado <pkcs12|pem>
```

STEP 5 | Configure y especifique un perfil SSL/TLS para definir el certificado y protocolo que los dispositivos WildFire usan para los servicios SSL/TLS.

set deviceconfig setting management secure-conn-server ssl-tls-service-profile <profile name><profile name>

1. Cree el perfil SSL/TLS.

   ```
   Establecer ssl-tls-service-profile compartido <name>
   ```

2. Especifique el certificado personalizado.

   ```
   Establecer certificado ssl-tls-service-profile <name>
    compartido <value>
   ```

3. Defina el alcance de SSL/TLS.

   ```
   Establecer SSL-TLS-Service-Profile <name> Protocol-Settings
    Min-Version <tls1-0|tls1-1|tls1-2>
   ```

   ```
   Establecer SSL-TLS-Service-Profile <name> Protocol-Settings
    Max-Version <tls1-0|tls1-1|tls1-2|max>
   ```

4. Especifique el perfil SSL/TLS. Este perfil de servicio SSL/TLS se aplica a todas las conexiones entre los dispositivos WildFire y el cortafuegos, así como también a los peers del dispositivo WildFire.

   ```
   set deviceconfig setting management secure-conn-server ssl-
   tls-service-profile <profile name><ssltls-profile>
   ```


STEP 6 | Configure y especifique un perfil de certificado para definir el certificado y protocolo que los dispositivos WildFire usan para los servicios SSL/TLS.

1. Cree el perfil de certificado.

```
establecer perfil de certificado compartido <name>
```

2. (Opcional) Establezca el nombre de sujeto (nombre común) o el nombre de sujeto alternativo.

```
establecer certificado compartido-perfil <name> nombre de
 usuario-campo asunto <common-name>
```

```
Establecer certificado compartido-perfil <name> nombre de
 usuario-campo asunto-ALT <email|principal-name>
```

3. (Opcional) Establezca el dominio del usuario.

```
establecer dominio de perfil <name> de certificado compartido
 <value>
```

4. Configure la CA.

```
establecer CA de perfil <name> de certificado compartido
 <name>
```

```
Establecer la CA <name> de perfil <name> de certificado
 compartido default-ocsp-url <value>
```

```
Establecer certificado compartido-perfil <name> CA <name>
 OCSP-VERIFY-Cert <value>
```

5. Especifique el perfil de certificado.

```
establecer deviceconfig configuración administración secure-
conn-server certificate-profile <certificate-profile>
```

STEP 7 | Importe el certificado y el par de claves privadas.

STEP 8 | Configure los **Secure Communication Settings (Ajustes de comunicación segura)** del cortafuegos en Panorama para asociar el clúster de dispositivos WildFire con el certificado personalizado del cortafuegos. Esto proporciona un canal de comunicaciones seguro entre el cortafuegos y el clúster de dispositivos WildFire. Si ya configuró las comunicaciones seguras entre el cortafuegos y el clúster del dispositivos WildFire, y utiliza el certificado personalizado existente, continúe al paso 9.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**.
2. Configuración de un perfil de certificado.

3. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión) > Secure Communication Settings (Ajustes de comunicación segura)** y haga clic en el icono **Edit (Editar)** en **Secure Communication Settings (Ajustes de comunicación segura)** para configurar los ajustes de certificado personalizado del cortafuegos.
4. Seleccione **Certificate Type (Tipo de certificado)**, **Certificate (Certificado)** u **Certificate Profile (Perfil de certificado)** desde los menús desplegables correspondientes y configúrelos para usar el certificado personalizado que se creó en el paso 2.
5. En Customize Communication (Personalizar comunicación), seleccione **WildFire Communication (Comunicación de WildFire)**.
6. Haga clic en **OK (Aceptar)**.

STEP 9 | Deshabilite el uso del certificado predefinido.

```
set deviceconfig setting management secure-conn-server disable-pre-defined-cert yes
```

STEP 10 | Especifique el nombre DNS usado para la autenticación que se encuentra en el certificado personalizado (generalmente, SubjectName o SubjectAltName). Por ejemplo, el nombre de dominio predeterminado es **`wfpc.service.mycluster.paloaltonetworks.com`**.

```
set deviceconfig setting wildfire custom-dns-name <custom_dns_name><custom_dns_name>
```.

STEP 11 | (Solo en clústeres de dispositivos con 3 o más nodos) Repita los pasos del 2 al 10 para el tercer nodo de servidor del dispositivo WildFire inscrito en el clúster.

Supervisión de un clúster WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede comprobar el estado operativo de su clúster WildFire utilizando la CLI o Panorama. Esto le permite verificar que las aplicaciones y los servicios que se ejecutan en un nodo determinado funcionan correctamente. Para que un clúster de WildFire funcione correctamente, los servicios y aplicaciones adecuados deben estar activos en cada nodo y el estado de cada uno de ser el correcto. Es posible que los clústeres que operen fuera de estos parámetros no funcionen bajo condiciones óptimas o que esto indique otros problemas y problemas de configuración.

La CLI muestra información que no está disponible desde Panorama. Se recomienda encarecidamente utilizar la CLI de WildFire cuando se solucionen problemas relacionados con el clúster.

Puede ver el estado actual de un nodo del controlador de WildFire ejecutando una serie de comandos show en la CLI de WildFire. Los comandos muestran detalles de configuración, las aplicaciones y los servicios actuales que se ejecutan en el dispositivo, además de los mensajes de estado/error. Puede utilizar estos detalles para determinar el estado de su clúster. Ver el estado no interrumpe los servicios de WildFire y se puede ejecutar en cualquier momento.

Consulte las secciones siguientes para obtener detalles sobre cómo supervisar el dispositivo WildFire:

- Visualización del estado del clúster WildFire con la CLI
- Visualización del estado del clúster WildFire con Panorama
- Estados de aplicación de WildFire
- Estados de servicio de WildFire

Visualización del estado del clúster WildFire con la CLI

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para confirmar que el clúster WildFire funciona dentro de los parámetros operativos normales, debe ejecutar los siguientes comandos show:

- **`show cluster controller`**: muestra el estado de los nodos del clúster WildFire activos/pasivos.
- **`show cluster all-peers`**: muestra la información acerca de todos los miembros en un clúster WildFire determinado.
- **`show cluster membership`**: muestra la información del dispositivo WildFire para los nodos en clústeres e independientes.

- **show cluster data-migration-status**: muestra el estado actual del proceso de migración de datos.
- **show log system**: muestra el log de eventos de WildFire, incluidos los detalles del estado del sistema.

STEP 1 | En un nodo controlador del dispositivo WildFire, ejecute lo siguiente:

```
admin@WF-500(active-controller)>show clustercontroller
```

Un clúster WildFire correcto muestra los siguientes detalles:

- El nombre del clúster al que se inscribió el dispositivo y su función configurada.
- El `K/V API online status` (estado en línea de la API K/V) indica el valor `True` (Verdadero) cuando la interfaz del clúster interno funciona correctamente. Un estado `False` (Falso) puede indicar un nodo configurado de manera inadecuada o un problema de red.
- `Task processing` (Procesamiento de tareas) indica el valor `True` (Verdadero) en los controladores activos (principales) y `False` (Falso) en los controladores pasivos (copia de seguridad).
- Las direcciones IP de todos los nodos WildFire en el clúster se enumeran bajo `App Service Avail` (Disponibilidad del servicio de la aplicación).
- Hasta tres `Core Servers` (Servidores centrales) buenos. La cantidad de `Core Servers` (Servidores centrales) buenos depende de la cantidad de nodos en el clúster . Si tiene un tercer nodo en un clúster, se configura automáticamente como nodo servidor para maximizar la integridad del clúster.
- No existen `Suspended Nodes` (Nodos suspendidos).
- La `Current Task` (Tarea actual) proporciona información de entorno sobre las operaciones en el nivel del clúster, como las tareas de reinicio, retiro y suspensión.

El siguiente ejemplo muestra el resultado de un controlador activo configurado en un clúster WildFire de 2 nodos que funciona en un estado correcto.

```
Nombre del clúster: WildFire_Cluster K/V API en línea: Verdadero
 procesamiento de tareas: en el controlador activo: Anuncio de DNS
 verdadero: Nombre DNS del servicio de aplicaciones: Disponibilidad
 del servicio de aplicaciones: 2.2.2.14, 2.2.2.15 Servidores
 centrales: 009701000026: 2.2.2.15 009701000043: 2.2.2.14 Buenos
 servidores centrales: 2 nodos suspendidos: Tarea actual: *
 Muestra la última tarea completada Solicitud: inicio desde qa14
 (009701000043/80025) en 2017-09-18 21:43:34 UTC respuesta nula:
 permiso por qa15 en 2017-09-18 21:45:15 UTC 1/ 2 servidores
 centrales disponibles. Terminado: éxito en 2017-09-18 21:43:47 UTC
```


STEP 2 | En un nodo controlador del dispositivo WildFire, ejecute lo siguiente:

```
admin@WF-500>mostrar todos los pares del clúster
```

Un clúster WildFire correcto muestra los siguientes detalles:

- La información general acerca de los nodos de WildFire en el clúster se enumera en `Address` (Dirección), `Mode` (Modo), `Server` (Servidor), `Node` (Nodo) y `Name` (Nombre).
- Todos los nodos del clúster WildFire ejecutan el servicio `wfpc`, un servicio de análisis de muestras de archivos internos.
- Los nodos que operan como activo, pasivo o servidor muestran el valor `Serverrole applied` (Función del servidor aplicado) junto a `Status` (Estado). Si el nodo se ha configurado como servidor, pero no funciona como servidor, el campo `status` (estado) muestra el valor `Serverrole assigned` (Función de servidor asignada).

  En una implementación de 3 nodos, el tercer nodo servidor se categoriza como de trabajo.
- Es posible que los nodos que se eliminaron recientemente estén presentes, pero se muestran como `Disconnected` (Desconectados). Es posible que eliminar un nodo desconectado de la lista de nodos del clúster demore varios días.
- El nodo de controlador activo muestra `siggen-db:ReadyMaster`.
- El nodo controlador pasivo muestra `siggen-db:ReadySlave`.

  Para obtener más información detallada acerca del estado general de la aplicación y el servicio de WildFire, consulte Estados de aplicación de WildFire *y* Estados de servicio de WildFire.
- El `Diag report` (Informe de diagnóstico) muestra los eventos del sistema y los mensajes de error del clúster:

Mensaje de error	Description (Descripción)
`Unreachable`	El nodo no se pudo acceder desde el controlador del clúster.
`Unexpected member`	El nodo no forma parte de la configuración del clúster. Es posible que el nodo se haya eliminado recientemente de la configuracion del clúster o que se deba a una configuración incorrecta.
`Left cluster`	El nodo ya no se puede acceder desde el controlador del clúster.
`Incorrect cluster name`	El nodo tiene un nombre de clúster configurado incorrectamente.

Mensaje de error	Description (Descripción)
`Connectivity unstable`	La conexión del nodo al controlador del clúster es inestable.
`Connectivity lost`	La conectividad del nodo al controlador del clúster se ha perdido.
`Unexpected server serial number`	Se ha detectado la presencia inesperada de un nodo servidor.

El siguiente ejemplo muestra un clúster WildFire de 3 nodos que funciona en un estado correcto:

```
Modo de dirección Nombre de nodo del servidor ------- ----
 ------ --------- 2.2.2.15 controlador Self True qa15 Servicio:
 firma infra wfcore wfpc Estado: Conectado, rol de servidor
 aplicado Cambiado: Lunes, 18 de septiembre de 2017 15:37:40
 -0700 Aplicación WF: global-db-service: Servicio de aplicaciones
 de wildfire de JoinedCluster: global-queue-service Servicio de
 gestión de wildfire de JoinedCluster: Hecho siggen-db: ReadySlave
 2.2.2.14 controlador Peer True qa14 Servicio: infra firma wfcore
 wfpc Estado: Conectado, rol de servidor aplicado Cambiado:
 Lunes, 18 de septiembre de 2017 15:37:40 -0700 Aplicación WF:
 global-db-service: commit-lock wildfire-apps-service: global-
queue-service Servicio de gestión de wildfire ReadyStandalone:
 Hecho siggen-db: ReadyMaster 2.2.2.16 trabajador True wf6240
 Servicio: infra wfcore wfpc Estado: Conectado, rol de servidor
 aplicado Cambiado: miércoles, 22 de febrero de 2017 11:11:15 -0800
 Aplicación WF: wildfire-apps-service: global-db-service Servicio
 de cola global de JoinedCluster: Servicio de base de datos local
 de JoinedCluster: Informe de diagnóstico DataMigrationFailed:
 2.2.2.14: líder notificado '2.2.2.15', edad 0. 2.2.2.15: el nodo
 local superó la comprobación de estado.
```

STEP 3 | En un nodo controlador del dispositivo WildFire, ejecute lo siguiente:

```
admin@WF-500>mostrar membresía de clúster
```

Un clúster WildFire correcto muestra los siguientes detalles:

- Los detalles de configuración general del dispositivo WildFire, como el nombre del clúster, la dirección IP del dispositivo, el número de serie, etc.
- `Server role` (Función del servidor) indica si el dispositivo funciona como un servidor del clúster o no. Los servidores de los clústeres operan aplicaciones y servicios de infraestructura adicional. Puede añadir un máximo de tres servidores por clúster.
- `Node mode` (Modo del nodo) describe la función de un dispositivo WildFire. Los dispositivos WildFire inscriptos en un clúster pueden ser nodos `controller` (controlador) o `worker` (de

trabajo) según su configuración y la cantidad de nodos en su implementación. Los dispositivos que no forman parte de un clúster muestran el valor `stand_alone` (independiente).

- Opera los siguientes `Services` (Servicios) según la función del nodo del clúster:

Tipo de nodo	Servicios que se operan en el nodo
Nodo controlador (activo o pasivo)	• `infra` • `wfpc` • `signature` • `wfcore`
Nodo servidor	• `infra` • `wfpc` • `wfcore`
Nodo de trabajo	• `infra` • `wfpc`

- `HA priority` (Prioridad de HA) muestra principal o secundario según su función configurada; sin embargo, esta configuración es independiente del estado de HA actual del dispositivo.
- `Work queue status` (Estado de la cola de trabajo) muestra el trabajo pendiente de análisis de muestras, además de las muestras que se analizan actualmente. Esto también indica cuánta carga recibe un dispositivo WildFire particular.

Para obtener más información detallada acerca del estado de la aplicación y el servicio de WildFire, consulte Estados de aplicación de WildFire *y* Estados de servicio de WildFire.

El siguiente ejemplo muestra un controlador WildFire que funciona en un estado correcto:

```
Resumen del servicio: firma wfpc Nombre del clúster: qa-auto-0ut1
 Dirección: 2.2.2.15 Nombre de host: qa15 Nombre de nodo:
 wfpc-009701000026-interno Número de serie: 009701000026 Modo de
 nodo: controlador Función del servidor: Prioridad HA verdadera:
 secundaria Última modificación: viernes, 22 de septiembre de
 2017 11:30:47 -0700 Servicios: wfcore firma wfpc infra Estado del
 monitor: Estado de salud de Serf: aprobación del agente activo y
 accesible Comprobación de servicio 'infra': aprobación del estado
 de la aplicación: servicio global-db: Servicio de aplicaciones
 ReadyLeader wildfire: global-queue-service Servicio de gestión
 de wildfire ReadyLeader: Hecho siggen-db: Listo Estado de cola
 de trabajo: análisis de muestra en cola: 0 análisis de muestra
 en ejecución: 0 copia de muestra en cola: 0 copia de muestra en
 ejecución: 0 Informe de diagnóstico: 2.2.2.14: líder notificado
 '2.2.2.15', edad 0. 2.2.2.15: el nodo local superó la comprobación
 de estado.
```

STEP 4 | En un nodo controlador del dispositivo WildFire, ejecute lo siguiente:

```
admin@WF-500(active-controller)>show clusterdata-migration-status
```

El dispositivo WildFire muestra los siguientes detalles sobre la migración de datos:

- No reenvíe archivos al clúster de dispositivos WildFire cuando la migración de datos esté en curso. Cuando finalice la migración de datos, aparecerá la marca de tiempo de finalización.
- Los cambios de topología en el clúster de WildFire (por ejemplo, añadir o eliminar nodos y cambiar las funciones de nodos) desencadena eventos de migración de datos.
- La migración de datos se puede realizar al actualizar a una nueva versión de WildFire. Después de la actualización, asegúrese de comprobar el estado operativo del clúster de WildFire para verificar la funcionalidad adecuada.

En el siguiente ejemplo se muestra el progreso de la migración de datos en un clúster de dispositivos WildFire:

```
admin @ WF-500 (controlador activo)>: mostrar el estado de
 migración de datos 100% completado el lunes 9 de septiembre
 21:44:48 PDT 2019
```


STEP 5 | En un dispositivo WildFire activo, pasivo y nodos de servidor, ejecute:

`admin@WF-500(active-controller)>show log systemsubtype direction equal backward`

Este comando muestra todos los eventos registrados de WildFire categorizados como un subtipo de dispositivo Wildfire desde el más reciente al más antiguo.

- Debe emitir este comando a todos los nodos en un clúster. Por ejemplo, si utiliza un clúster de 3 nodos, debe comprobar el estado en el controlador activo, el controlador pasivo y el nodo del servidor.
- Los mensajes de log devueltos por la CLI del dispositivo WildFire pueden incluir diversos subtipos. Puede filtrar los logs por una palabra clave de subtipo común. Utilice el siguiente argumento de comando para filtrar por un componente específico:
  - global-queue—**`matchqueue`**, por ejemplo **`show log system directionequal backward | match queue`**
  - global-database—**`match global`**, por ejemplo **`show log system direction equal backward | matchglobal`**
  - signature-generation: **`match signature`**, por ejemplo, **`show log system direction equal backward| match signature`**
- Los clústeres de dispositivos WildFire que funcionan normalmente devuelven las siguientes lecturas de estado para cada nodo en un clúster de 2 nodos. Los nodos del clúster de WildFire en buen estado tienen lecturas de estado diferentes según la función del dispositivo.

  Utilice la siguiente lista de verificación para verificar que los servicios del dispositivo WildFire se ejecutan correctamente en la implementación de su clúster.

  - **Controlador activo**

Componente	Estado del controlador activo
`global-queue`	❑ `infowildfire cluster 0 Formación del clúster de cola global (rabbitmq) realizada correctamente con el estado ReadyLeaderestado ReadyLeader` ❑ `info general general 0 Configurar política para servicio global-queue`
`global-database`	❑ `infogeneral general 0 Soy líder de clúster, arranque para el servicio de base de datos global` ❑ `info general general 0 Configurar política para el servicio global-queue`
`signature-generation`	❑ `infowildfir cluster 0 Estado del servicio de generación de firma establecido en ReadyMaster` ❑ `info wildfir cluster 0 Estado del servicio de generación de firmaestablecido en ReadyMaster`

Componente	Estado del controlador activo

Los mensajes de log devueltos por los dispositivos WildFire se muestran del más reciente al más antiguo. Si no utiliza el argumento del comando ***`direction equal backward`*** *como se muestra en el procedimiento anterior, la CLI del dispositivo WildFire devuelve los mensajes de registro del más antiguo al más reciente.*

- **Controlador pasivo**

Componente	Ejemplo de estado del controlador pasivo
`global-queue`	❑ `infogeneral general 0 Política de configuración para servicio global-queue` ❑ `info wildfire cluster 0 Formación del clúster de cola global (rabbitmq)realizada correctamente con el estado JoinedCluster` ❑ `info general general 0 Unirse al clúster para el servicioglobal-queue - realizado correctamente` ❑ `info general general 0 Configurar política para el servicio global-queue`
`global-database`	❑ `infogeneral general 0 Configurar política para el servicio global-queue` ❑ `info general general 0 Restaurar aplicaciones:hecho, Para arrancar global-db y unirse al clúster` ❑ `info general general 0 Iniciar vm_mgr, Para arrancar global-dby unirse al clúster` ❑ `info general general 0 Iniciar uwsgi, Para arrancar global-dby unirse al clúster` ❑ `info general general 0 Iniciar wf_services, Paraarrancar global-db y unirse al clúster` ❑ `info general general 0 Suspender aplicaciones:hecho, Para arrancar global-db y unirse al clúster` ❑ `info general general 0 Detener vm_mgr, Para arrancar global-dby unirse al clúster` ❑ `info general general 0 Detener uwsgi, Para arrancar global-dby unirse al clúster` ❑ `info general general 0 Detener wf_services, Paraarrancar global-db y unirse al clúster`

Componente	Ejemplo de estado del controlador pasivo
	❑ info general general 0 Arrancar y unirse al clústerpara el servicio global-db
signature-generation	❑ infowildfir cluster 0 Estado del servicio de generación de firma establecido en ReadySlave ❑ info wildfir cluster 0 Estado del servicio de generaciónde firma establecido en ReadySlave

Los mensajes de log devueltos por el o los dispositivos de WildFire se muestran del más antiguo al más reciente. Si no utiliza el argumento del comando ***direction equal backward*** *como se muestra en el procedimiento anterior, la CLI del dispositivo WildFire devuelve los mensajes de registro del más antiguo al más reciente.*

- Los clústeres de dispositivos WildFire que funcionan normalmente devuelven las siguientes lecturas de estado para cada nodo en un clúster de 3 nodos. Los nodos del clúster de WildFire en buen estado tienen lecturas de estado diferentes según la función del dispositivo.

  Utilice la siguiente lista de verificación para verificar que los servicios del dispositivo WildFire se ejecutan correctamente en la implementación de su clúster.

  - **Controlador activo**

Componente	Estado del controlador activo
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) formación del clúster correcta conestado JoinedCluster ❑ info general general 0 Unirse al clúster para global-queueservice - realizado correctamente ❑ info general general 0 Configurar política para servicio global-queue
global-database	❑ infogeneral general 0 Restaurar aplicaciones: hecho, Para arrancar global-db yunirse al clúster ❑ info general general 0 Iniciar vm_mgr, Para arrancarglobal-db y unirse al clúster ❑ info general general 0 iniciar uwsgi, Para arrancar global-dby unirse al clúster ❑ info general general 0 Iniciar wf_services, Paraarrancar global-db y unirse al clúster

Componente	Estado del controlador activo
	❑ info general general 0 Suspender aplicaciones:hecho, Para arrancar global-db y unirse al clúster ❑ info general general 0 Detener vm_mgr, Para arrancar global-dby unirse al clúster ❑ info general general 0 Detener uwsgi, Para arrancar global-dby unirse al clúster ❑ info general general 0 Detener wf_services, Paraarrancar global-db y unirse al clúster ❑ 2019/07/19 14:40:19 info general general 0Arrancar y unirse al clúster para el servicio global-db
signature-generation	❑ infowildfire cluster 0 Estado de la generación de firmas establecido en ReadyMaster

Los mensajes de log devueltos por el/los dispositivos WildFire se muestran de más reciente al más antiguo. Si no utiliza el argumento del comando ***direction equal backward*** *como se muestra en el procedimiento anterior, la CLI del dispositivo WildFire devuelve los mensajes de registro del más antiguo al más reciente.*

- **Controlador pasivo**

Componente	Estado de controlador pasivo
global-queue	❑ infogeneral general 0 Configurar política para el servicio global-queue ❑ info general general 0 Configurar política para el servicio global-queue ❑ info wildfire cluster 0 Información de clúster de cola global (rabbitmq)realizado correctamente con el estado ReadyLeader ❑ info general general 0 Configurar política para el servicio de cola global
global-database	❑ infogeneral general 0 Soy líder del clúster, arranque para el servicio global-db ❑ info general general 0 Configurar política para el servicio global-queue

Componente	Estado de controlador pasivo
signature-generation	❑ infowildfire cluster 0 Estado del servicio de generación de firmas establecido en ReadySlave ❑ info wildfire cluster 0 Estado del servicio degeneración de firmas establecido en ReadySlave

Los mensajes de log devueltos por los dispositivos WildFire se muestran del más reciente al más antiguo. Si no utiliza el argumento del comando ***direction equal backward*** *como se muestra en el procedimiento anterior, la CLI del dispositivo WildFire devuelve los mensajes de registro del más antiguo al más reciente.*

- **Nodo de servidor**

Componente	Estado del nodo de servidor
global-queue	❑ infowildfire cluster 0 Formación del clúster de cola global (rabbitmq) realizada correctamente con el estado JoinedCluster ❑ info general general 0 Unirse al clúster para el servicioglobal-queue - realizado correctamente ❑ info general general 0 Configurar política para el servicio global-queue ❑ info wildfire cluster 0 Formación de clúster de cola global (rabbitmq)realizada correctamente con estado StandbyAsWorker
global-database	❑ infogeneral general 0 Restaurar aplicaciones: hecho, Para arrancar global-db yunirse al clúster ❑ info general general 0 Iniciar vm_mgr, Para arrancar global-dby unirse al clúster ❑ info general general 0 Iniciar uwsgi, Para arrancar global-dby unirse al clúster ❑ info general general 0 Iniciar wf_services, Paraarrancar global-db y unirse al clúster ❑ info general general 0 Suspender aplicaciones:hecho, Para arrancar global-db y unirse al clúster ❑ info general general 0 Detener vm_mgr, Para arrancar global-dby unirse al clúster

Componente	Estado del nodo de servidor
	❑ `info general general 0 Detener uwsgi, Para arrancar global-dby unirse al clúster` ❑ `info general general 0 Detener wf_services, Paraarrancar global-db y unirse al clúster` ❑ `2019/07/19 14:32:50 info general general 0Promover nodo trabajador y unirse al clúster para el servicio global-db`
`signature-generation`	❑ `infowildfire cluster 0 Estado del servicio de generación de firmas establecido en Detenido` ❑ `critical wildfire cluster 0 Signature DataMigrationDone`

Los mensajes de log devueltos por los dispositivos WildFire se muestran del más reciente al más antiguo. Si no utiliza el argumento del comando ***`direction equal backward`*** *como se muestra en el procedimiento anterior, la CLI del dispositivo WildFire devuelve los mensajes de registro del más antiguo al más reciente.*

Estados de aplicación de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire opera una serie de aplicaciones internas para gestionar y coordinar el procesamiento de los datos de muestra. Estas aplicaciones y sus estados necesarios se muestran cuando se visualiza el estado de un clúster de dispositivos WildFire.

La siguiente lista muestra los componentes, el propósito y las condiciones de estado del clúster:

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
global-db-service	Esta base de datos de aplicación se utiliza para almacenar datos de análisis de WildFire.	AcquiringSessionSpinLock	En espera del cerrojo de la sesión hasta adquirir el bloqueo o el tiempo de espera.
		Bootstrapping	La aplicación de la base de datos de muestra está actualmente en estado de arranque.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
		BootstrappingNoMeet	El servicio de base de datos de muestras local se inició sin formar un clúster con otros dispositivos WildFire.
		FailedToBecomeWorker	Se produjo un error en la unión al clúster como un nodo trabajador.
		FailedToBootstrap	Se produjo un error en el proceso de arranque.
		FailedToJoinCluster	Se produjo un error en la unión al clúster.
		FailedToStartServices	Se produjo un error en el inicio de los servicios de la base de datos interna.
		MaintenanceDecommission	Inicio del proceso de retiro para los servicios de base de datos.
		MaintenanceDecommissionDone	El servicio de la base de datos se retiró.
		MaintenanceFailover	Inicio del proceso para disminuir el nivel del servicio local y las réplicas de reserva de la conmutación por error.
		MaintenanceFailed	Se produjo un error en la conmutación por error.
		MaintenanceFailoverDone	Se produjo la conmutación por error del servicio.
		MaintenanceRecoverFromSplitbrain	Si el dispositivo WildFire se encuentra actualmente en modo de cerebro dividido, el estado del servicio de base de datos se establecerá en MaintenanceRecoverFromSplitbrain al iniciar el servicio.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
		MaintenanceSuspend	El servicio de la base de datos se encuentra en proceso de suspensión como resultado de la ejecución de uno de los siguientes comandos por parte del usuario: debug cluster suspend o request cluster decommission.
		MaintenanceSuspendDone	El servicio de la base de datos completó el proceso de suspensión.
		DataMigration	El contenido de la base de datos local se fusiona con la base de datos principal. Esto sucede cuando un dispositivo WildFire se une a un clúster.
		DataMigrationDone	El proceso de migración de datos finalizó.
		DataMigrationFailed	El proceso de migración de datos finalizó con errores.
		JoinedCluster	El servicio de base de datos local se unió al clúster.
		Listo	El servicio de base de datos está listo.
		ReadyLeader	El servicio de base de datos está listo y el dispositivo se configura como el líder.
		ReadyStandalone	El servicio de base de datos está listo y el dispositivo opera como un dispositivo independiente.
		Splitbrain	Se detectó una condición de división y los servicios de base de datos ingresaron a un modo de división. El servicio pasará a ReadyStandalone en breve.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
		StandbyAsWorker	El servicio de base de datos del nodo de trabajo está en modo de espera.
		WaitingforLeaderReady	El nodo local está en espera para unirse al nodo líder.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
global-queue-service	Gestiona la gestión y la priorización de las muestras que se envían para el análisis de WildFire.	Bootstrapping	La aplicación del servicio de cola está actualmente en estado de arranque.
		FailedToBecomeWorker	Se produjo un error en la unión al clúster como un nodo trabajador.
		FailedToBootstrap	Se produjo un error en el proceso de arranque.
		FailedToJoinCluster	Se produjo un error en la unión al clúster.
		FailedToStartServices	Se produjo un error en el inicio de los servicios de cola internos.
		MaintenanceDecommission	Inicio del proceso de retiro para los servicios de cola.
		MaintenanceDecommissionDone	El servicio de cola se retiró.
		MaintenanceFailover	Inicio del proceso para disminuir el nivel del servicio local y las réplicas de reserva de la conmutación por error.
		MaintenanceFailed	Se produjo un error en la conmutación por error.
		MaintenanceFailoverDone	Se produjo la conmutación por error del servicio.
		MaintenanceRecoverFromSplitbrain	Si el dispositivo WildFire se encuentra actualmente

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
			en modo de condición de división, el estado del servicio de cola será
		MaintenanceSuspend	El servicio de cola se encuentra en proceso de suspensión como resultado de la ejecución de uno de los siguientes comandos por parte del usuario: depurar suspensión del clúster o solicitar retiro del clúster.
		MaintenanceSuspendDone	El servicio de cola completó el proceso de suspensión.
		JoinedCluster	El servicio de cola se unió al clúster.
		Listo	El servicio de cola está listo.
		ReadyLeader	El servicio de cola está listo y el dispositivo se configura como el líder.
		ReadyStandalone	El servicio de cola está listo y el dispositivo opera como un dispositivo independiente.
		Splitbrain	Se detectó una condición de división y los servicios de cola ingresaron a un modo de división. El servicio pasará a ReadyStandalone en breve.
		StandbyAsWorker	El servicio de cola del nodo de trabajo está en modo de espera.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
siggen-db	Genera firmas privadas y muestras de	DatabaseFailover	Cuando se produce una conmutación por error de HA, el controlador pasivo se convierte en el controlador

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
	análisis de WildFire.		activo. El servicio de firmas en el controlador pasivo se convierte en el principal y el estado se establece como DatabaseFailover.
		DatabaseFailoverFaild	La conmutador por error de la base de datos de firmas finalizó con errores.
		DataMigration	El contenido de la base de datos de firmas local se fusiona con la base de datos principal. Esto sucede cuando un dispositivo WildFire se une a un clúster.
		DataMigrationDone	El proceso de migración de datos finalizó.
		DataMigrationFailed	El proceso de migración de datos finalizó con errores.
		Deregistered	El servicio de base de datos de firmas se dio de baja.
		MaintenanceDecommission	Inicio del proceso de retiro para los servicios de base de datos de firmas.
		MaintenanceDecommissionDone	El servicio de cola se retiró.
		MaintenanceFailover	Inicio del proceso para disminuir el nivel del servicio local y las réplicas de reserva de la conmutación por error.
		MaintenanceFailoverDone	Se produjo la conmutación por error del servicio.
		MaintenanceSuspend	El servicio de la base de datos de firmas se encuentra en proceso de suspensión como resultado de la ejecución de uno de los siguientes comandos por parte del usuario: depurar suspensión

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
			del clúster o solicitar retiro del clúster.
		MaintenanceSuspendDone	El servicio de la base de datos de firmas completó el proceso de suspensión.
		MigrateMalwareDatabase	Cuando se actualiza PAN-OS de la versión 7.1 a 8.0, los datos de las muestras se convierten a un formato diferente. Estos estados indican el progreso del proceso de migración de datos.
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	
		Listo	El servicio de base de datos de firmas está listo.
		ReadyMaster	El servicio de base de datos de firmas está en modo principal y opera en el controlador activo.
		ReadySlave	El servicio de base de datos de firmas está en modo de reserva y opera en el controlador pasivo.
		ReadyStandalone	El servicio de base de datos de firma está listo y el dispositivo opera como un dispositivo independiente.
		Splitbrain	Se detectó una condición de división y los servicios de base de datos de firma ingresaron a un modo de división. El servicio pasará a ReadyStandalone en breve.
		Detenido	El servicio de la base de datos de firmas se detuvo en el dispositivo.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
wildfire-management-service	El servicio de gestión del modo de trabajo de WildFire.	En ejecución	El servicio de gestión de WildFire está en un estado operativo.
		Listo	El servicio de gestión de WildFire finalizó su ejecución.

Nombre	Description (Descripción)	Condiciones posibles del estado	Definición
wildfire-apps-service	Aplicaciones de infraestructura de WildFire.	Deregistered	El servicio de las aplicaciones de WildFire se dio de baja.
		Listo	El servicio de las aplicaciones de WildFire está listo.
		Restored	El servicio de las aplicaciones de WildFire finalizó los procedimientos de mantenimiento.
		Scheduling	El servicio de las aplicaciones de WildFire está en estado de programación.
		SetupSampleStorage	El servicio de las aplicaciones de WildFire opera cuando WildFire se actualiza de 7.1 a 8.0.
		Detenido	El servicio de las aplicaciones de WildFire se detuvo en el dispositivo.
		Suspendido	El servicio de las aplicaciones de WildFire se suspendió debido al mantenimiento.

Estados de servicio de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El dispositivo WildFire opera una serie de servicios internos para gestionar y coordinar el procesamiento de los datos de muestra. Estos servicios y sus estados necesarios se muestran cuando se visualiza el estado de un clúster de dispositivos WildFire.

La siguiente lista muestra los componentes, la descripción, las condiciones del estado y otros detalles relevantes del servicio de WildFire:

Nombre	Función	Nodos afectados	estado
`infra`	Indica que un servicio de infraestructura de clúster WildFire opera en un modo determinado.	Todos los nodos	Muestra una pantalla de estado en la CLI cuando el servicio se encuentra en operación. Si estos servicios no están presentes en un nodo determinado, verifique la configuración del dispositivo.
`wfpc`	Indica que el servicio de análisis de muestras de archivos (nube privada de WildFire) puede realizar el análisis de los archivos y la generación de informes.		
`signature`	Genera firmas privadas y muestras de análisis de WildFire.	Controlador activo (principal) / pasivo (copia de seguridad)	
`wfcore`	Indica que el nodo funciona como un servidor para los servicios de infraestructura de clúster WildFire.	Nodo servidor	

Actualización de dispositivos WildFire en un clúster

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Puede utilizar la CLI para actualizar los dispositivos WildFire inscriptos en un clúster individualmente o utilizar Panorama para actualizar el clúster como un grupo.

Según la cantidad de muestras que analizó y almacenó el dispositivo WildFire, el tiempo necesario para actualizar el software del dispositivo varía; esto se debe a que la actualización requiere la migración de todas las muestras de malware y 14 días de muestras benignas. Dedique de 30 a 60 minutos a cada uno de los dispositivos WildFire que utilizó en un entorno de producción.

- *Todos los nodos en un clúster deben ejecutar la misma versión de sistema operativo.*
- *Panorama puede gestionar dispositivos WildFire y clústeres de dispositivos con versiones de software PAN-OS 8.0.1 o posteriores.*
- *Asegúrese de que todos los dispositivos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los dispositivos pueden resultar inútiles.*

Según su implementación, realice una de las siguientes tareas para actualizar su clúster WildFire:

- Actualización de un clúster centralmente en Panorama con una conexión a internet
- Actualización de un clúster centralmente en Panorama sin una conexión a internet
- Actualización de un clúster localmente con una conexión a internet
- Actualización de un clúster localmente sin una conexión a internet

Actualización de un clúster localmente con una conexión a internet

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para actualizar un clúster localmente, debe actualizar individualmente cada dispositivo WildFire inscrito en un clúster. Cuando finaliza la actualización de un dispositivo, este se vuelve a inscribir automáticamente en el clúster al que se asignó en primer lugar.

STEP 1 | Suspenda temporalmente el análisis de muestras.

1. Evite que los cortafuegos reenvíen nuevas muestras al dispositivo WildFire.
   1. Inicie sesión en la interfaz web del cortafuegos.
   2. Seleccione **Device > Setup > WildFire (Dispositivo > Configuración > WildFire)** y edite **General Settings (Configuración general)**.
   3. Borre el campo **WildFire Private Cloud (Nube privada de WildFire)**.
   4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
2. Confirme que el análisis de las muestras que el cortafuegos envío al dispositivo haya finalizado:

```
admin@WF-500(passive-controller)> show wildfire latest samples
```

Si no desea esperar a que el dispositivo WildFire complete el análisis de las muestras recién enviadas, puede continuar con el próximo paso. Sin embargo, considere que el dispositivo WildFire descarta las muestras pendientes en la cola de análisis.

STEP 2 | Instale las últimas actualizaciones de contenido del dispositivo WildFire. Esta actualización le proporciona al dispositivo la información de amenazas más reciente para detectar malware con mayor precisión.

Este proceso puede tardar hasta 6 horas o más en dispositivos más antiguos.

1. Verifique que esté ejecutando la última actualización de contenido en su dispositivo WildFire.

```
admin@WF-500> request wf-content upgrade check
```

2. Descargue el último paquete de actualización de contenido de WildFire.

```
admin@WF-500> request wf-content upgrade download latest
```

Si no tiene una conectividad directa con el servidor de actualizaciones de Palo Alto Networks, puede descargar las actualizaciones y realizar la Instalación de actualizaciones de contenido desde un servidor habilitado para SCP.

3. Ver el estado de la descarga.

```
admin@WF-500> show jobs all
```

4. Una vez completada la descarga, instale la actualización.

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 3 | (Necesario al actualizar a PAN-OS 10.2.2) Actualice las imágenes de VM en el dispositivo WildFire.

1. Inicie sesión y acceda a la página de descarga de software del portal de atención al cliente de Palo Alto Networks. También puede navegar manualmente a la página de descarga de software

desde la página de inicio de Soporte yendo a **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.

2. En la página de actualizaciones de software, seleccione **Imágenes de VM host de WF-500** y descargue los siguientes archivos de imagen de VM:

   Palo Alto Networks actualiza periódicamente los archivos de imagen de VM; como resultado, el nombre de archivo específico cambia según la versión disponible. Asegúrese de descargar la última versión, donde m-x.x.x en el nombre del archivo indica el número de versión; además, hay una fecha de lanzamiento a la que se puede hacer referencia para ayudar a determinar la versión más reciente.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Cargue las imágenes de VM en el dispositivo WildFire.
   1. Importe la imagen de VM desde el servidor SCP:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Por ejemplo:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Para comprobar el estado de la descarga, utilice el siguiente comando:

      ```
      admin@WF-500> show jobs all
      ```

   3. Repita el proceso para las imágenes de VM restantes.
4. Instale la imagen de la máquina virtual.
   1. ```
      admin@WF-500> request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. Repita el proceso para las imágenes de VM restantes.
5. Confirme que las imágenes de VM se han instalado y habilitado correctamente en el dispositivo WildFire.
   1. (Opcional) Vea una lista de imágenes de máquinas virtuales disponibles:

      ```
      admin@WF-500> show wildfire vm-images
      ```

      El resultado muestra las imágenes de VM disponibles.
   2. Confirme la configuración:
      ```

```
admin@WF-500# commit
```

3. Vea la imagen de VM activa ejecutando el siguiente comando:

```
admin@WF-500> show wildfire status
```

STEP 4 | Verifique que esté disponible la versión de software del dispositivo WildFire que desea instalar.

```
admin@WF-500(passive-controller)> request system software check
```

STEP 5 | Descargar la versión de software PAN-OS 10.2.2 al dispositivo WildFire.

No puede omitir ninguna versión importante al actualizar el dispositivo WildFire. Por ejemplo, si desea actualizar de PAN-OS 6.1 a PAN-OS 7.1, debe descargar e instalar PAN-OS 7.0 en primer lugar. En los ejemplos de este procedimiento, se muestra cómo actualizar a PAN-OS 10.2.2. Reemplace 10.2.2 por la versión final correspondiente para su actualización.

Descargue la versión de software 10.2.2.

```
admin@WF-500(passive-controller)> request system software download
 version 10.2.2
```

Para comprobar el estado de la descarga, utilice el siguiente comando

```
admin@WF-500(passive-controller)> show jobs all
```

STEP 6 | Confirme que todos los servicios se ejecuten.

```
admin@WF-500(passive-controller)> show system software status
```

STEP 7 | Instale la versión de software 10.2.2.

```
admin@WF-500(passive-controller)> request system software install
 version 10.2
```

STEP 8 | Complete la actualización de software.

1. Confirme que la actualización se haya completado. Ejecute el siguiente comando y busque el tipo de trabajo **Install** y el estado **FIN**:

```
admin@WF-500(passive-controller)> show jobs all
 Enqueued Dequeued ID Type Status Result Completed
```



```
---------------------------------------------------- 14:53:15
14:53:15 5 Install FIN OK 14:53:19
```

2. Reinicie correctamente el dispositivo:

```
admin@WF-500(passive-controller)> request cluster reboot-
local-node
```

El proceso de actualización puede tardar 10 minutos o más de una hora, según la cantidad de muestras almacenadas en el dispositivo WildFire.

STEP 9 | Repita los pasos 1 a 8 para cada nodo trabajador de WildFire en el clúster.

STEP 10 | (Opcional) Vea el estado de las tareas de reinicio en el nodo controlador de WildFire.

En el controlador del clúster WildFire, ejecute el siguiente comando y busque el tipo de trabajo **`Install`** y el estado **`FIN`**:

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 11 | Compruebe que el dispositivo WildFire esté listo para reanudar el análisis de muestras.

1. Verifique que el campo de versión de software muestre la versión actualizada:

```
admin@WF-500(passive-controller)> show system info | match sw-
version
```

2. Confirme que todos los servicios se ejecuten:

```
admin@WF-500(passive-controller)> show system software status
```

3. Confirme que el trabajo de confirmación automática (**`AutoCom`**) se haya completado:

```
admin@WF-500(passive-controller)> show jobs all
```

4. Confirme que la migración de datos se ha realizado correctamente. Ejecute `show cluster data-migration-status` para ver el progreso de la fusión de la base de datos. Una vez completada la combinación de datos, se muestra la marca de tiempo de finalización:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

La duración de la fusión de los datos depende de la cantidad de datos almacenados en el dispositivo WildFire. Asegúrese de dedicar, al menos, varias horas a la recuperación, dado que la fusión de datos puede ser un proceso prolongado.

Actualización de un clúster localmente sin una conexión a internet

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para actualizar un clúster localmente, debe actualizar individualmente cada dispositivo WildFire inscrito en un clúster. Cuando finaliza la actualización de un dispositivo, este se vuelve a inscribir automáticamente en el clúster al que se asignó en primer lugar.

STEP 1 | Suspenda temporalmente el análisis de muestras.

1. Evite que los cortafuegos reenvíen nuevas muestras al dispositivo WildFire.
   1. Inicie sesión en la interfaz web del cortafuegos.
   2. Seleccione **Device > Setup > WildFire (Dispositivo > Configuración > WildFire)** y edite **General Settings (Configuración general)**.
   3. Borre el campo **WildFire Private Cloud (Nube privada de WildFire)**.
   4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
2. Confirme que el análisis de las muestras que el cortafuegos envío al dispositivo haya finalizado:

   ```
   admin@WF-500(passive-controller)> show wildfire latest samples
   ```

   Si no desea esperar a que el dispositivo WildFire complete el análisis de las muestras recién enviadas, puede continuar con el próximo paso. Sin embargo, considere que el dispositivo WildFire descarta las muestras pendientes en la cola de análisis.

STEP 2 | Recupere el archivo de actualización de contenido del servidor de actualizaciones.

1. Inicie sesión en el portal de asistencia técnica de Palo Alto Networks y haga clic en **Dynamic Updates (Actualizaciones dinámicas)**.
2. En la sección del dispositivo WildFire, busque la última actualización de contenido del dispositivo WildFire y descárguela.
3. Copie el archivo de actualización de contenido en un servidor habilitado con SCP y anote el nombre del archivo y la ruta de acceso al directorio.

STEP 3 | Instale la actualización de contenido en el dispositivo WildFire.

1. Inicie sesión en el dispositivo WildFire y descargue el archivo de actualización de contenido del servidor SCP:

   ```
   admin@WF-500> scp import wf-content from username@host:path
   ```

   Por ejemplo:

   ```
   admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/
   updates/panup-all-wfmeta-2-253.tgz
   ```

   Si el servidor SCP se ejecuta en un puerto no estándar o si necesita especificar la dirección IP de origen, también puede definir estas opciones en el comando ***scp import****.*

2. Instale la actualización:

   ```
   admin@WF-500> request wf-content upgrade install file panup-
   all-wfmeta-2-253.tgz
   ```

3. Vea el estado de la instalación:

   ```
   admin@WF-500> show jobs all
   ```

STEP 4 | Compruebe la actualización de contenido.

Compruebe la versión de contenido:

```
admin@WF-500> show system info | match wf-content-version
```

En el siguiente resultado se muestra ahora la versión 2-253:

```
wf-content-version: 2-253
```

STEP 5 | (Necesario al actualizar a PAN-OS 10.2.2) Actualice las imágenes de VM en el dispositivo WildFire.

1. Inicie sesión y acceda a la página de descarga de software del portal de atención al cliente de Palo Alto Networks. También puede navegar manualmente a la página de descarga de software desde la página de inicio de Soporte yendo a **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.

2. En la página de actualizaciones de software, seleccione **Imágenes de VM host de WF-500** y descargue los siguientes archivos de imagen de VM:

   Palo Alto Networks actualiza periódicamente los archivos de imagen de VM; como resultado, el nombre de archivo específico cambia según la versión disponible. Asegúrese de descargar la última versión, donde m-x.x.x en el nombre del archivo indica el número de versión; además, hay una fecha de lanzamiento a la que se puede hacer referencia para ayudar a determinar la versión más reciente.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Cargue las imágenes de VM en el dispositivo WildFire.
   1. Importe la imagen de VM desde el servidor SCP:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Por ejemplo:

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Para comprobar el estado de la descarga, utilice el siguiente comando:

      ```
      admin@WF-500> show jobs all
      ```

   3. Repita el proceso para las imágenes de VM restantes.
4. Instale la imagen de la máquina virtual.
   1.
      ```
      admin@WF-500> request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```

   2. Repita el proceso para las imágenes de VM restantes.
5. Confirme que las imágenes de VM se han instalado y habilitado correctamente en el dispositivo WildFire.
   1. (Opcional) Vea una lista de imágenes de máquinas virtuales disponibles:

      ```
      admin@WF-500> show wildfire vm-images
      ```

      El resultado muestra las imágenes de VM disponibles.
   2. Confirme la configuración:


```
admin@WF-500# commit
```

3. Vea las imágenes de la máquina virtual activa ejecutando el siguiente comando:

```
admin@WF-500> show wildfire status
```

STEP 6 | Verifique que esté disponible la versión de software del dispositivo WildFire que desea instalar.

```
admin@WF-500(passive-controller)> request system software check
```

STEP 7 | Descargar la versión de software PAN-OS 10.2.2 al dispositivo WildFire.

No puede omitir ninguna versión importante al actualizar el dispositivo WildFire. Por ejemplo, si desea actualizar de PAN-OS 6.1 a PAN-OS 7.1, debe descargar e instalar PAN-OS 7.0 en primer lugar. En los ejemplos de este procedimiento, se muestra cómo actualizar a PAN-OS 10.2.2. Reemplace 10.2.2 por la versión final correspondiente para su actualización.

Descargue la versión de software 10.2.2:

1. Vaya al sitio de Asistencia técnica de Palo Alto Networks y en la sección Tools (Herramientas), haga clic en **Software Updates (Actualizaciones de software)**.
2. Descargue el archivo de imagen del software de WildFire que desea instalar en un ordenador que ejecuta el software del servidor SCP.
3. Importe el archivo de imagen del software desde el servidor SCP:

```
admin@WF-500> scp import software from <username@ip_address>/
<folder_name>/<imagefile_name>
```

Por ejemplo:

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

4. Para comprobar el estado de la descarga, utilice el siguiente comando:

```
admin@WF-500> show jobs all
```

STEP 8 | Confirme que todos los servicios se ejecuten.

```
admin@WF-500(passive-controller)> show system software status
```

STEP 9 | Instale la versión de software 10.2.2.

```
admin@WF-500(passive-controller)> request system software install
 version 10.2.2
```


STEP 10 | Complete la actualización de software.

1. Confirme que la actualización se haya completado. Ejecute el siguiente comando y busque el tipo de trabajo **`Install`** y el estado **`FIN`**:

```
admin@WF-500(passive-controller)> show jobs all
 Enqueued Dequeued ID Type Status Result Completed
 ------------------------------------------------- 14:53:15
 14:53:15 5 Install FIN OK 14:53:19
```

2. Reinicie correctamente el dispositivo:

```
admin@WF-500(passive-controller)> request cluster reboot-
local-node
```

El proceso de actualización puede tardar 10 minutos o más de una hora, según la cantidad de muestras almacenadas en el dispositivo WildFire.

STEP 11 | Repita los pasos 1 a 10 para cada nodo trabajador de WildFire en el clúster.

STEP 12 | (Opcional) Vea el estado de las tareas de reinicio en el nodo controlador de WildFire.

En el controlador del clúster WildFire, ejecute el siguiente comando y busque el tipo de trabajo **`Install`** y el estado **`FIN`**:

```
admin@WF-500(active-controller)> show cluster task pending
```


STEP 13 | Compruebe que el dispositivo WildFire esté listo para reanudar el análisis de muestras.

1. Verifique que el campo de versión de software muestre la versión actualizada:

   ```
   admin@WF-500(passive-controller)> show system info | match sw-version
   ```

2. Confirme que todos los servicios se ejecuten:

   ```
   admin@WF-500(passive-controller)> show system software status
   ```

3. Confirme que el trabajo de confirmación automática (**AutoCom**) se haya completado:

   ```
   admin@WF-500(passive-controller)> show jobs all
   ```

4. Confirme que la migración de datos se ha realizado correctamente. Ejecute `show cluster data-migration-status` para ver el progreso de la fusión de la base de datos. Una vez completada la combinación de datos, se muestra la marca de tiempo de finalización:

   ```
   100% completed on Mon Sep 9 21:44:48 PDT 2019
   ```

   La duración de la fusión de los datos depende de la cantidad de datos almacenados en el dispositivo WildFire. Asegúrese de dedicar, al menos, varias horas a la recuperación, dado que la fusión de datos puede ser un proceso prolongado.

Solución de problemas en un clúster WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Consulte los siguientes temas para diagnosticar y solucionar los problemas de los clústeres WildFire:

- Solución de problemas de condiciones de división de WildFire

Solución de problemas de condiciones de división de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Un clúster de HA (alta disponibilidad) de 2 nodos WildFire experimenta una condición de división cuando un nodo (o ambos peer de HA) cree que el otro ya no funciona. Esto sucede cuando las conexiones de HA y del clúster fallan como resultado de la conectividad de la red o problemas de configuración, pero se permite que los dispositivos continúen procesando las muestras. Cuando esto sucede, ambos dispositivos WildFire asumen la función del controlador activo (o principal) sin una copia de seguridad, lo que evita los beneficios de una implementación de HA, como la redundancia y el equilibrio de carga. Además, esto evita que los dispositivos WildFire utilicen los recursos de análisis de manera eficaz. Cuando los clústeres de WildFire experimentan una interrupción menor, intentan recuperarse automáticamente de las condiciones de división. Los eventos más serios requerirán una intervención manual.

Cuando se produce esta división, se aplican las siguientes condiciones:

- Ninguno de los peers de WildFire es consciente del estado ni de la función de HA del otro peer.
- Ambos peers de WildFire se convierten en el servidor principal y continuarán recibiendo muestras de los cortafuegos, pero operarán como dispositivos independientes.
- Las tareas relacionadas con el clúster se suspenden cuando la HA no está disponible.

Los clústeres de dispositivos WildFire de 3 nodos no deben experimentar condiciones de división cuando se configuran correctamente debido a la redundancia adicional que proporciona el tercer nodo servidor.

¿Qué provoca una condición de división?

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Una condición de división es una respuesta correctiva a una avería en un nodo de clústeres de dos nodos, en la que el par de alta disponibilidad de WildFire ya no puede comunicarse entre sí, pero proporciona una funcionalidad limitada. A pesar de que la funcionalidad de alta disponibilidad y equilibrio de carga ya no

está disponible, puede reenviar muestras a WildFire para el análisis. Cuando se produce una división, es posible que se deba a alguna de las siguientes opciones:

- Problemas de hardware o interrupción de alimentación.
- Problemas de conectividad de la red, como averías en el conmutador/router, oscilación de la red o una partición de la red.
- Problemas de configuración o conectividad del dispositivo WildFire.

  Palo Alto Networks recomienda utilizar una conexión de cable directa para HA1 y el enlace de la interfaz del clúster.
- Nodo WildFire en mal estado.

Determinación de si un clúster WildFire se encuentra en una condición de división

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

Cuando los dispositivos en un clúster de 2 nodos WildFire presentan una condición de división, las averías del servicio generan advertencias en la CLI de WildFire y en Panorama de gestión (siempre que esté disponible).

STEP 1 | (CLI del dispositivo WildFire únicamente) En un controlador del dispositivo WildFire, ejecute:

```
admin@WF-500>show cluster membership
```

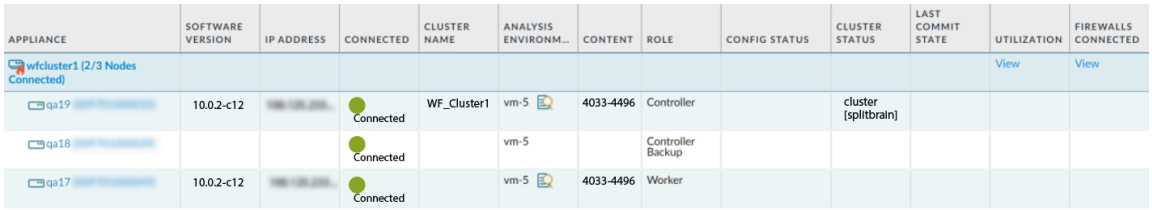
El nodo del clúster WildFire afectado muestra `Cluster:splitbrain` junto a `Service Summary`.

El siguiente ejemplo muestra un nodo en un clúster WildFire de dos nodos en una condición de división:

```
Service Summary: Cluster:splitbrain Cluster name: Dirección
 WF_Cluster_1: 2.2.2.114 Host name: wf1 Node name:
 wfpc-009707000380-internal Serial number: 009707000380 Node mode:
 controller Server role: True HA priority: secondary Last changed:
 Tue, 24 Oct 2017 15:13:18 -0700 Services: wfcore signature wfpc
 infra Monitor status: Serf Health Status: passing Agent alive
 and reachable Service 'infra' check: passing Application status:
 global-db-service: Servicio de aplicaciones ReadyLeader wildfire:
 global-queue-service Servicio de gestión de wildfire ReadyLeader:
 Done siggen-db: ReadyMaster Work queue status: sample anaysis
 queued: 0 sample anaysis running: 0 copia de muestra en cola: 0
 copia de muestra en ejecución: 0 Diag report: 2.2.2.114: reported
 leader '2.2.2.114', age 0. 2.2.2.114: local node passed sanity
 check.
```


STEP 2 | (Solo Panorama) En el dispositivo Panorama que gestiona el clúster WildFire:

1. Seleccione **Panorama** > **Managed WildFire Clusters (Panorama** > **Clústeres WildFire gestionados)**.
2. En la columna **Cluster Status (Estado del clúster)**, compruebe la presencia de **cluster [splitbrain]**. Esto indica que el dispositivo está en modo de división.



APPLIANCE	SOFTWARE VERSION	IP ADDRESS	CONNECTED	CLUSTER NAME	ANALYSIS ENVIRONM...	CONTENT	ROLE	CONFIG STATUS	CLUSTER STATUS	LAST COMMIT STATE	UTILIZATION	FIREWALLS CONNECTED
wfcluster1 (2/3 Nodes Connected)											View	View
qa19	10.0.2-c12		Connected	WF_Cluster1	vm-5	4033-4496	Controller		cluster [splitbrain]			
qa18			Connected		vm-5		Controller Backup					
qa17	10.0.2-c12		Connected		vm-5	4033-4496	Worker					

Recuperación de una condición de división

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para resolver una condición de división, depure los problemas de red y restaure la conectividad entre el par de HA de WildFire. Los clústeres de dispositivos WildFire intentan recuperarse de condiciones de división automáticamente pero, si esas medidas fallan, debe iniciar manualmente el proceso de recuperación.

STEP 1 | Verifique que su red funcione normalmente y que el dispositivo WildFire transmita y reciba tráfico.

1. Habilite la capacidad de hacer ping a una interfaz del dispositivo WildFire.
   - Habilite ping en una interfaz específica de dispositivos: `setdeviceconfig system <interface_number> service disable-icmp no`
   - Habilite ping en todas las interfaces de dispositivos: `setdeviceconfig system service disable-icmp no`
2. Genere tráfico de ping desde una interfaz de WildFire a un dispositivo externo. Verifique que los contadores de pings recibidos y transmitidos incrementen.

   ```
   ping source <wildfire-interface-ip> host<destination-ip-address>
   ```

STEP 2 | Determine cuál dispositivo WildFire no funciona correctamente. Consulte Visualización del estado del clúster WildFire con la CLI o Visualización del estado del clúster WildFire con Panorama para ver el estado del dispositivo.

STEP 3 | Reinicie correctamente el nodo en *mal estado* utilizando el siguiente comando:

```
request cluster reboot-local-node
```

El dispositivo WildFire que se reinicia debe inscribirse automáticamente en el clúster WildFire para el que se configuró.

El nodo controlador restante en condición de división debe tener un estado correcto.

STEP 4 | Espere a que se complete la migración de datos. Ejecute `show cluster data-migration-status` para ver el progreso de la fusión de la base de datos. Una vez completada la combinación de datos, se muestra la marca de tiempo de finalización:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

La duración de la fusión de los datos depende de la cantidad de datos almacenados en el dispositivo WildFire. Asegúrese de dedicar, al menos, varias horas a la recuperación, dado que la fusión de datos puede ser un proceso prolongado.

STEP 5 | Compruebe el estado del clúster en Panorama o mediante la CLI del dispositivo WildFire.

Uso de la CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Los siguientes temas describen los comandos de la CLI específicos para el software del dispositivo WildFire™. El resto de comandos, tales como las interfaces de configuración, confirmación de la configuración y el ajuste de la información del sistema son idénticos a PAN-OS y también se muestran en la jerarquía. Para obtener información sobre los comandos PAN-OS, consulte el Inicio rápido de la CLI de PAN-OS.

- Conceptos de la CLI del software del dispositivo WildFire
- Modos de comando del CLI de WildFire
- Acceso a la CLI del dispositivo WildFire
- Operaciones de la CLI del dispositivo WildFire
- Referencia de comandos del modo de configuración del dispositivo WildFire
- Referencia de comandos del modo de operación del dispositivo WildFire

Conceptos de la CLI del software del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En esta sección se presenta la interfaz de línea de comandos (CLI) del software del dispositivo WildFire y se describe su uso:

- Estructura de la CLI del software del dispositivo WildFire
- Convenciones de comandos de la CLI del software del dispositivo WildFire
- Mensajes de comandos de la CLI del dispositivo WildFire
- Símbolos de las opciones de comandos del dispositivo WildFire
- Niveles de privilegios del dispositivo WildFire

Estructura de la CLI del software del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

La CLI del software del dispositivo WildFire se usa manejar dicho dispositivo. La CLI es la única interfaz del dispositivo. Sirve para ver información de estado y configuración, y modificar la configuración del dispositivo. Acceda a la CLI del software del dispositivo WildFire a través de SSH o de un acceso directo a la consola usando el puerto de la consola.

La CLI del software del dispositivo WildFire tiene dos modos de funcionamiento:

- **Operational mode** (Modo de operación): Permite ver el estado del sistema, navegar por la CLI del software del dispositivo WildFire y acceder al modo de configuración.
- **Configuration mode** (Modo de configuración): Permite ver y modificar la jerarquía de configuración.

Convenciones de comandos de la CLI del software del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El mensaje de comandos básico incluye el nombre de usuario y de host del dispositivo:

```
username@hostname>
```


Ejemplo:

```
admin@WF-500>
```

Al entrar en el modo de configuración, el mensaje cambia de **>** a **#**:

```
username@hostname> (Modo operativo) username@hostname> configure
 Entrar en modo de configuración [editar] username@hostname# (Modo de
 configuración)
```

En el modo de configuración, el contexto de jerarquía actual se muestra en el titular `[edit...]` que aparece entre corchetes cuando se emite un comando.

Mensajes de comandos de la CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Se pueden mostrar mensajes al emitir un comando. Los mensajes ofrecen información de contexto y pueden ayudar a corregir comandos no válidos. En los siguientes ejemplos, el mensaje se muestra en negrita.

Ejemplo: Comando desconocido

```
username@hostname# application-group Unknown command: application-
group [edit network] username@hostname#
```

Ejemplo: Modos de cambio

```
username@hostname# exit Exiting configuration mode
 username@hostname>
```

Ejemplo: Sintaxis no válida

```
username@hostname> debug 17 Unrecognized command Invalid syntax.
 username@hostname>
```

La CLI comprueba la sintaxis de cada comando. Si la sintaxis es correcta, se ejecuta el comando y se registran los cambios de la jerarquía del candidato. Si la sintaxis no es correcta, aparece un mensaje de sintaxis no válida, como en el siguiente ejemplo:

```
username@hostname# set deviceconfig setting wildfire cloud-
intelligence submit-sample yes Unrecognized command Invalid syntax.
 [edit] username@hostname#
```


Símbolos de las opciones de comandos del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El símbolo que precede a una opción puede proporcionar información adicional acerca de la sintaxis de comandos.

Símbolo	Description (Descripción)
*	Esta opción es obligatoria.
>	Hay opciones adicionales anidadas para este comando.
+	Hay opciones de comando adicionales para este comando en este nivel.
|	Hay una opción para especificar un “valor de excepción” o un “valor de coincidencia” para restringir el comando.
“ “	Aunque las comillas dobles no son un símbolo de opción de comando, debe usarse al introducir frases de varias palabras en comandos de CLI. Por ejemplo, para crear un grupo de direcciones llamado Grupo de prueba y añadir el usuario llamado usuario1 a este grupo, debe escribir el nombre del grupo entre comillas dobles del siguiente modo: establecer grupo de direcciones “Grupo de prueba” usuario1. Si no coloca comillas dobles alrededor del nombre del grupo, la CLI podría interpretar la palabra Prueba como el nombre del grupo y Grupo como el nombre de usuario y se mostraría el siguiente mensaje de error: `testis not a valid name (la prueba no tiene un nombre válido)`. *Las comillas simples tampoco serían válidas en este ejemplo.*

Los siguientes ejemplos muestran cómo se usan estos símbolos.

Ejemplo: En el siguiente comando, es obligatoria la palabra clave `from`:

```
username@hostname> configuración de importación de scp? + número
 de puerto SSH de puerto remoto en el host remoto * desde la
 configuración de importación de origen (username@host:path)
 username@hostname> scp Ejemplo: Esta salida de comando muestra
 las opciones designadas con + y >. username@hostname# set rulebase
```



```
security rules1 ? + action action + application application +
destination destination + disabled + from from + log-end log-end +
log-setting log-setting + log-start log-start + negate-destination
negate-destination negate-destination + negate-source negate-source
+ schedule schedule + service service service + source source + to >
profiles Profiles <Enter> Finish input [edit] username@hostname# set
rulebase security rules rule1
```

Cada opción de la lista marcada con + se puede añadir al comando.

La palabra clave perfiles (con >) tiene opciones adicionales:

```
username@hostname# set rulebase security rules rule1 profiles ? +
virus Help string for virus + spyware Help string for spyware +
vulnerability Help string for vulnerability + group Help string for
group <Enter> Finish input [edit] username@hostname# set rulebase
security rules rule1 profiles
```

Niveles de privilegios del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Los niveles de privilegio determinan los comandos que el usuario tiene permitido ejecutar y la información que el usuario tiene permitido ver.

Nivel	Description (Descripción)
superlector	Tiene solo acceso de lectura completo al dispositivo.
Superusuario	Tiene acceso de escritura completo al dispositivo.

Modos de comando del CLI de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Los siguientes temas describen los modos usados para interactuar con la CLI del software del dispositivo WildFire:

- Modo de configuración del CLI del dispositivo WildFire
- Modo de operación del CLI del dispositivo WildFire

Modo de configuración del CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Al introducir comandos en el modo de configuración se modifica la configuración del candidato. La configuración candidata modificada se almacena en la memoria del dispositivo y se conserva mientras el dispositivo esté en funcionamiento.

Cada comando de configuración implica una acción, y también puede incluir palabras clave, opciones y valores.

En esta sección, se describen el modo de configuración y la jerarquía de configuración:

- Uso de comandos del modo de configuración
- Jerarquía de configuración
- Rutas de jerarquía
- Navegación por la jerarquía

Uso de comandos del modo de configuración

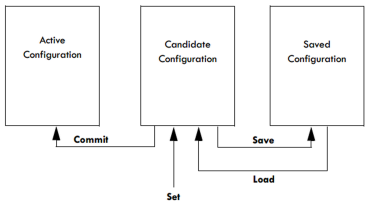
¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Use los siguientes comandos para almacenar y aplicar cambios de configuración:

- `save` (guardar): guarda la configuración del candidato en el sistema de almacenamiento no volátil del dispositivo. La configuración guardada se conserva hasta que se vuelva a usar el comando **save** para sobrescribirla. Tenga en cuenta que este comando no activa la configuración.
- `commit`: aplica la configuración del candidato al dispositivo. Una configuración confirmada vuelve activa la configuración del dispositivo.

- `set` (establecer): cambia un valor en la configuración del candidato.
- `load`: asigna la última configuración guardada o una configuración especificada para ser la configuración del candidato.

> *Si sale del modo de configuración sin emitir los comandos* ***`save`*** *(guardar) o* ***`commit`*** *(confirmar), los cambios en la configuración se pueden perder en caso de pérdida de alimentación.*



Mantener la configuración de un candidato y separar los pasos de guardado y compilación conlleva importantes ventajas en comparación con las arquitecturas CLI tradicionales:

- Distinguir entre los conceptos de save (guardar) y commit (confirmar) permite hacer múltiples cambios simultáneos y reduce la vulnerabilidad del sistema.
- Los comandos se pueden adaptar fácilmente para funciones similares. Por ejemplo, al configurar dos interfaces Ethernet, cada una con una dirección IP, puede editar la configuración de la primera interfaz, copiar el comando, modificar solo la interfaz y la dirección IP y, a continuación, aplicar el cambio a la segunda interfaz.
- La estructura de comandos siempre es constante.

Dado que la configuración del candidato siempre es exclusiva, todos los cambios autorizados de la configuración del candidato son coherentes entre sí.

Jerarquía de configuración

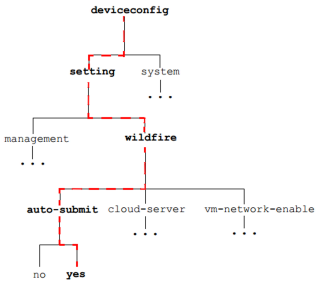
¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

La configuración del dispositivo se organiza con una estructura jerárquica. Para mostrar un segmento del nivel actual de la jerarquía, use el comando `show`. Al introducir mostrar, aparece la jerarquía completa, mientras que al introducir `mostrar` con palabras clave, aparece un segmento de la jerarquía. Por ejemplo, si se ejecuta el comando `show` en el nivel superior del modo de configuración, se muestra toda la configuración. Si se ejecuta el comando `edit mgt-config` y se introduce `show`, o se ejecuta el comando **`showmgt-config`**, solo aparece la parte de la jerarquía relativa a la configuración de gestión.

Rutas de jerarquía

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Al introducir comandos, la ruta se traza a través de la jerarquía del siguiente modo:

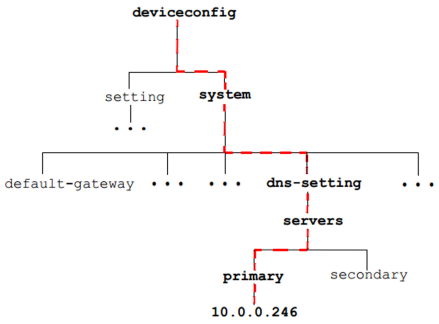


Por ejemplo, el siguiente comando asigna el servidor de DNS principal 10.0.0.246 para el dispositivo:

```
[edit] username@hostname# set deviceconfig system dns-setting servers
 primary 10.0.0.246
```

Este comando genera un nuevo elemento en la jerarquía y en los resultados del siguiente comando `show`:

```
[edit] username@hostname# show deviceconfig system dns-settings dns-
setting { servers { primary 10.0.0.246 } } [edit] username@hostname#
```



Navegación por la jerarquía

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

El titular [editar...] presentado a continuación de la línea del símbolo de sistema del modo de configuración muestra el contexto de jerarquía actual.

```
[editar]
```

indica que el contexto relativo es el máximo nivel de la jerarquía, mientras que


```
[editar deviceconfig]
```

indica que el contexto relativo está al nivel de deviceconfig.

Use los comandos de la lista para navegar por la jerarquía de configuración.

Nivel	Description (Descripción)
Editar	Establece el contexto para la configuración dentro de la jerarquía de comandos.
Superior	Cambia el contexto al nivel superior de la jerarquía.
máximo	Cambia el contexto al nivel más alto de la jerarquía.

*Si se emite el comando **`establecer`** después de usar los comandos **`arriba`** y **`principal`**, se inicia desde un nuevo contexto.*

Modo de operación del CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	☐ Licencia de WildFire

La primera vez que se inicia sesión en el dispositivo, la CLI del software del dispositivo WildFire se abre en el modo de operación. Los comandos del modo de operación tienen que ver con acciones que se ejecutan inmediatamente. No suponen cambios en la configuración y no es necesario guardarlos o compilarlos.

Los comandos del modo de operación son de varios tipos:

- **Network access** (Acceso a la red): se abre una ventana para otro host. Es compatible con SSH.
- **Monitoring and troubleshooting** (Supervisión y solución de problemas): realizar diagnósticos y análisis. Incluye los comandos `debug` y `ping`.
- **Display commands** (Mostrar comandos): muestra o borra la información actual. Incluye los comandos `clear` y `show`.
- **WildFire appliance software CLI navigation commands** (Comandos de navegación de la CLI del software del dispositivo WildFire): entrar en el modo de configuración o salir de la CLI del software del dispositivo WildFire. Incluye los comandos `configure`, `exit` y `quit`.
- **System commands** (Comandos del sistema): permite realizar solicitudes en el nivel del sistema o reiniciar. Incluye los comandos `establecer` y `solicitud`.

Acceso a la CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

En esta sección, se describe cómo acceder a la CLI del software del dispositivo WildFire:

- Establecimiento de una conexión directa con la consola
- Establecimiento de una conexión de SSH

Establecimiento de una conexión directa con la consola

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Utilice la siguiente configuración en la conexión directa de la consola:

- Tasa de datos: 9600
- Bits de datos: 8
- Paridad: no
- Bits de terminación: 1
- Control de flujo: ninguno

Establecimiento de una conexión de SSH

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Para acceder a la CLI del software del dispositivo WildFire:

STEP 1 | Utilice software de emulación de terminal para establecer una conexión de la consola SSH con el dispositivo WildFire.

STEP 2 | Introduzca el nombre del usuario administrativo. El valor predeterminado es admin.

STEP 3 | Introduzca la contraseña administrativa. El valor predeterminado es admin.

La CLI del software del dispositivo WildFire se abre en el modo de operación y se muestra el siguiente mensaje de la CLI:

```
username@hostname>
```


Operaciones de la CLI del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Acceso a los modos operativos y de configuración del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Al iniciar sesión, la CLI del software del dispositivo WildFire se abre en el modo de operación. Puede alternar entre los modos de operación y navegación en cualquier momento.

- Para introducir el modo de configuración desde el modo operativo, use el comando **`configure`**:

```
username@hostname> configurar Entrando en modo de configuración
 [editar] username@hostname #
```

- Para dejar el modo de configuración y volver al modo operativo, use el comando **`quit`** o **`exit`**:

```
username@hostname# Termine saliendo del modo de configuración
 username@hostname>
```

Para introducir un comando del modo de operación mientras está en el modo de configuración, use el comando **`ejecutar`**. Por ejemplo, para mostrar recursos del sistema desde el modo de configuración, use **`ejecutar mostrar recursos del sistema`**.

Mostrar opciones de comandos de la CLI del software del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Utilice **?** (o Meta-H) para mostrar una lista de opciones de comandos, basada en el contexto:

- Para mostrar una lista de comandos de operación, introduzca **?** en el mensaje del comando.

```
nombredeusuario@nombredehost> ? clear Borrar parámetros de tiempo
 de ejecución configure Manipular información de configuración de
 software create crear comandos debug Depurar y diagnosticar delete
 Eliminar archivos del disco duro disable deshabilitar comandos
 editar editar comandos exit Salir de esta sesión find Buscar
 comandos CLI con la palabra clave grep Busca en el archivo líneas
 que contengan una coincidencia de patrón less Examinar depuración
 contenido del archivo ping Hacer ping a hosts y redes quit Salir
 de esta sesión request Hacer solicitudes a nivel de sistema scp
 Usar scp para importar/exportar archivos set Establecer parámetros
 operativos show Mostrar parámetros operativos ssh Iniciar un shell
 seguro a otro host submit enviar comandos tail Imprimir las últimas
 10 líneas del contenido del archivo de depuración telnet Iniciar
 una sesión de telnet a otro host test verificar la configuración del
 sistema con casos de prueba tftp Usar tftp para importar/exportar
 archivos traceroute Imprime la ruta que toman los paquetes al host
 de la red nombreusuario@hostname>
```

- Para mostrar las opciones disponibles de un comando especificado, introduzca el comando seguido de **?**.

Ejemplo:

```
username@hostname> ping ? + bypass-routing Bypass routing table,
 use specified interface + count Number of requests to send
 (1..2000000000 packets) + do-not-fragment Don't fragment echo
 request packets (IPv4) + interval Delay between requests (seconds)
 + no-resolve Don't attempt to print addresses symbolically + pattern
 Hexadecimal fill pattern + size Size of request packets (0..65468
 bytes) + source Source address of echo request + tos IP type-of-
service value (0..255) + ttl IP time-to-live value (IPv6 hop-limit
 value) (0..255 hops) + verbose Display detailed output * host
 Hostname or IP address of remote host
```

Restricción de resultados de comandos del CLI del dispositivo WildFire

Algunos comandos de operación incluyen una opción para restringir el resultado que aparece. Para restringir el resultado, introduzca un símbolo de barra vertical seguido de **except** o **match** y el valor que se debe incluir o excluir:

Ejemplo:

El siguiente ejemplo de configuración pertenece al comando show system info:

```
username@hostname> show system info hostname: WildFire ip-address:
 192.168.2.20 netmask: 255.255.255.0 default-gateway: 192.168.2.1
 mac-address: 00:25:90:95:84:76 vm-interface-ip-address: 10.16.0.20
 vm-interface-netmask: 255.255.252.0 vm-interface-default-gateway:
 10.16.0.1 vm-interface-dns-server: 10.0.0.247 time: Mon Apr 15
```



```
13:31:39 2013 uptime: 0 days, 0:02:35 family: m model: WF-500
serial: 009707000118 sw-version: 8.0.1 wf-content-version:
702-283 wf-content-release-date: unknown logdb-version: 8.0.15
platform-family: m operational-mode: normal username@hostname>
The following sample displays only the system model information:
username@hostname> show system info | match model model: WF-500
username@hostname>
```

Establecimiento del formato de salida para comandos de configuración del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Cambie el formato de salida para los comandos de configuración con el comando **`set cli config-output-format`** en el modo de operación. Las opciones incluyen el formato predeterminado, JSON (JavaScript Object Notation), formato establecido y formato XML. El formato predefinido es un formato jerárquico donde las secciones de configuración tienen sangría y están entre llaves.

Referencia de comandos del modo de configuración del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de configuración que son específicos del software del dispositivo WildFire. El resto de los comandos que forman parte del software del dispositivo WildFire son idénticos a los de PAN-OS según se describe en el inicio rápido de la CLI de PAN-OS 11.0.

- set deviceconfig cluster
- set deviceconfig high-availability
- set deviceconfig setting management
- set deviceconfig setting wildfire
- set deviceconfig system eth2
- set deviceconfig system eth3
- set deviceconfig system panorama local-panorama panorama-server
- set deviceconfig system panorama local-panorama panorama-server-2
- set deviceconfig system update-schedule
- set deviceconfig system vm-interface

set deviceconfig cluster

Description (Descripción)

Configure el clúster de dispositivos WildFire en el dispositivo WildFire. Puede configurar el nombre del clúster, la interfaz que se utiliza para la comunicación del clúster y el modo (función) del dispositivo en el clúster (controlador o trabajador). En el caso de los dispositivos WildFire que configura como controladores del clúster, es posible añadir los dispositivos WildFire al clúster y establecer si el controlador proporciona servicio DNS en su interfaz de gestión.

Jerarquía de localización

```
set deviceconfig
```

Sintaxis

```
cluster { cluster-name <name>; interface {eth2 | eth3}; mode
 { controller { service-advertisement dns-service enabled {no | yes};
 worker-list {ip-address} } worker; } }
```


Opciones

`+ cluster-name`: se asigna un nombre al clúster. El nombre debe ser una sección de nombre de dominio válido.

`+ interface`: se configura la interfaz que se utilizará para la comunicación del clúster. La interfaz de comunicación del clúster debe ser la misma en todos los miembros del clúster.

`> mode`: se establece si el dispositivo WildFire es un nodo controlador o un nodo de trabajo. En los nodos controladores, establezca si el controlador proporciona servicio DNS en la interfaz de gestión (`service-advertisement`) y añada nodos de trabajo al clúster (`worker-list`). Cada clúster de dispositivos WildFire debe tener dos nodos controladores para proporcionar alta disponibilidad. Puede añadir dos controladores y hasta 18 nodos de trabajo a un clúster para obtener un total máximo de 20 nodos.

Ejemplo de configuración

```
admin@wf-500(active-controller)# show deviceconfig cluster cluster
 { cluster-name sid-6; interface eth2; mode { controller { worker-
list { 2.2.2.115; } } } }
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig high-availability

Description (Descripción)

Configure la alta disponibilidad (high-availability, HA) del clúster de dispositivos WildFire.

Jerarquía de localización

```
set deviceconfig
```

Sintaxis

```
high-availability { enabled {no | yes}; election-option { preemptive
 {no | yes}; priority {primary | secondary}; timers { advanced
 {heartbeat interval <value> | hello-interval <value> | preemption-
hold-time <value> | promotion-hold-time <value>} aggressive;
 recommended; } } interface { ha1 { peer-ip-address <ip-address>;
 port {eth2 | eth3 | management}; encryption enabled {no | yes}; }
 ha1-backup { peer-ip-address <ip-address>; port {eth2 | eth3 |
 management}; } } }
```

Opciones

`+ enabled`: se habilita la HA en ambos nodos controladores para proporcionar tolerancia a las averías al clúster. Cada clúster de dispositivos WildFire debe tener dos nodos controladores configurados como un par de HA.

`> election-option`: se configuran los valores de opción preferentes, de prioridad y temporizador de HA.

`+ preemptive`: opción que permite que el par de HA pasivo (el nodo controlador de copia de seguridad) reemplace el par de HA activo (el nodo controlador principal) en función de la configuración de `prioridad` de HA. Por ejemplo, si el nodo controlador principal se avería, el nodo controlador secundario (pasivo) asume el control del clúster. Cuando el nodo controlador principal vuelve a funcionar, si no configuró el reemplazo, el controlador secundario continúa controlando el clúster y el controlador principal actúa como el nodo controlador de copia de seguridad. Sin embargo, si configura el reemplazo en ambos peers de HA, cuando el controlador principal vuelva a funcionar, reemplazará al controlador secundario y tomará el control del clúster. El controlador secundario vuelve a realizar su función anterior como el nodo controlador de copia de seguridad. Debe configurar el reemplazo en ambos peers de HA para que esta característica funcione.

`+ priority`: opción para configurar la prioridad del reemplazo en cada controlador en el par de HA. Configure el reemplazo en ambos miembros del par de controladores de HA.

`> timers`: se configuran los temporizadores para las opciones de HA. El dispositivo WildFire proporciona dos opciones de temporizador configuradas previamente (configuración `agresiva` y `recomendada`) o puede configurar cada temporizador individualmente. Los temporizadores `avanzados` le permiten configurar los valores individualmente:

- El intervalo `heartbeat-interval` (intervalo de latidos) establece el tiempo en milisegundos para enviar pings de latidos. El rango de valores es de 1000 a 60 000 ms, con un valor predeterminado de 2000 ms.
- El intervalo `hello-interval` (intervalo Hello) establece el tiempo en milisegundos para enviar mensajes Hello. El rango de valores es de 8000 a 60 000 ms, con un valor predeterminado de 8000 ms.
- El valor `preemption-hold-time` (tiempo de espera de reemplazo) establece el tiempo en minutos durante el cual permanecerá en modo pasivo (controlador de copia de seguridad) antes de reemplazar el nodo controlador activo (principal). El rango de valores es de 1 a 60 minutos, con un valor predeterminado de 1 minuto.
- El valor `promtion-hold-time` (tiempo de espera de reemplazo) establece el tiempo en milisegundos para cambiar el estado de pasivo (controlador de copia de seguridad) a activo (principal). El rango de valores es de 0 a 60 000 ms, con un valor predeterminado de 2000 ms.

`> interface` (interfaz): se configura la interfaz de HA para las interfaces de enlace de control principal principales (`ha1`) y de copia de seguridad (`ha1-backup`). Las interfaces de enlace de control permiten que el par de controladores de HA permanezcan sincronizados y preparados para la conmutación por error en caso de que el nodo controlador principal se averíe. La configuración de la interfaz `ha1` y la interfaz `ha1-backup` proporciona conectividad redundante entre los controladores en caso de una avería en un enlace. Establezca lo siguiente:

- La `peer-ip-address` (dirección IP del peer). Para la interfaz, configure la dirección IP del peer de HA. El peer de la interfaz `ha1` es la dirección IP de la interfaz `ha1` en el otro nodo controlador del par de HA. El peer de la interfaz `ha1-backup` es la dirección IP de la interfaz `ha1-backup` en el otro nodo controlador del par de HA.
- El `puerto`. En cada nodo controlador, configure el puerto que utilizará para la interfaz `ha1` y el puerto que utilizará para la interfaz `ha-backup`. Puede utilizar el puerto `eth2`, `eth3` o el puerto `management` (eth0) para las interfaces de enlace de control de HA. No puede utilizar la interfaz de la

red de entornos de análisis (eth1) como la interfaz de enlace de control `ha1` o `ha1-backup`. Utilice la misma interfaz en ambos peers como la interfaz `ha1` y utilice la misma interfaz (pero no la interfaz `ha1`) en ambos peers de HA como la interfaz de `ha1-backup`. Por ejemplo, configure `eth3` como la interfaz `ha1` en ambos nodos controladores y configure la interfaz `management` como la interfaz `ha1-backup` en ambos nodos controladores.

Ejemplo de configuración

```
admin@wf-500(active-controller)# show deviceconfig high-availability
 high-availability { election-option { priority primary; } enabled
 no; interface { ha1 { peer-ip-address 10.10.10.150; port eth2 } ha1-
backup { peer-ip-address 10.10.10.160; port management } } }
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig setting management

Description (Descripción)

Configure la sesión de gestión administrativa en el dispositivo WildFire. Puede configurar tiempos de espera para finalizar las sesiones administrativas si están inactivas durante un período prolongado y cuántos reintentos de inicio de sesión (intentos fallidos de inicio de sesión) se requieren para bloquear a un administrador.

Jerarquía de localización

```
set deviceconfig setting
```

Sintaxis

```
management { idle-timeout {0 | <value>} admin-lockout { failed-
attempts <value> lockout-time <value> } }
```

Opciones

`+ idle-timeout`: tiempo de espera de inactividad de la sesión administrativa predeterminado en minutos. Configure un tiempo de espera de inactividad de 1 a 1440 minutos o establezca el valor del tiempo de espera en 0 (cero) para que la sesión nunca entre en tiempo de espera.

`> admin-lockout`: se configura la cantidad de `failed-attempts` (intentos fallidos) necesarios para iniciar sesión en el dispositivo antes de bloquear al administrador del sistema (0 a 10) y el `tiempo de bloqueo` en minutos (0 a 60) durante el que se bloqueará a un administrador si supera el umbral de `failed-attempts` (intentos fallidos).

Ejemplo de configuración

```
management { idle-timeout 0; admin-lockout { failed-attempts 3;
 lockout-time 5; } }
```

set deviceconfig setting wildfire

Description (Descripción)

Establezca la configuración de WildFire en el dispositivo WildFire. Puede configurar el reenvío de archivos malintencionados, definir el servidor de nube que recibe los archivos infectados con malware y habilitar o deshabilitar la interfaz VM.

Jerarquía de localización

```
set deviceconfig setting
```

Sintaxis

```
wildfire { active-vm {vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | <value>};
 cloud-server <value>; custom-dns-name <value>; preferred-analysis-
environment {Documents | Executables | default}; vm-network-
enable {no | yes}; vm-network-use-tor {enable | disable}; cloud-
intelligence { cloud-query {no | yes};submit-diagnostics {no |
 yes}; submit-report {no | yes}; submit-sample {no | yes}; } file-
retention { malicious {indefinite | <1-2000>}; non-malicious <1-90> }
 signature-generation { av {no | yes}; dns {no | yes}; url {no |
 yes}; } }
```

Opciones

`+ active-vm`: seleccione el entorno de máquina virtual que WildFire va a utilizar para el análisis de muestras. Cada VM tiene una configuración diferente, como Windows XP, versiones específicas de Flash, Adobe Reader, etc. Para ver qué VM se ha seleccionado, ejecute el comando: **`show wildfire status`** y vea el campo Selected VM (VM seleccionada). Para ver la información del entorno de VM, ejecute el siguiente comando **`: show wildfire vm-images.`**

`+ cloud-server`: Nombre de host del servidor de nube al que el dispositivo reenvía las muestras malintencionadas o los informes para repetir el análisis. El servidor de nube predeterminado es wildfire-public-cloud. Para configurar el reenvío, use el siguiente comando: **`set deviceconfig setting wildfire cloud-intelligence`**.

`+ custom-dns-name`: se configura un nombre DNS personalizado que se utilizará en los certificados del servidor y la lista de servidores WildFire en lugar del nombre DNS predeterminado `wfpc.sevice.<clustername>.<domain>`.

`+ preferred-analysis-environment` : se asigna la mayoría de los recursos al análisis de los documentos o al análisis de ejecutables, según el tipo de muestras que se analizan con mayor frecuencia en su entorno. La asignación predeterminada equilibra los recursos entre las muestras de documentos

y ejecutables. Por ejemplo, para asignar la mayoría de los recursos de análisis a los documentos: **`set deviceconfig setting wildfire preferred-analysis-environment Documents`**.

`+ vm-network-enable`: Habilita o deshabilita la red de VM. Si se habilita, los archivos de muestra ejecutados en el espacio aislado de la máquina pueden acceder a Internet. Esto permite que WildFire analice mejor el comportamiento del malware para buscar elementos como la actividad de teléfono-casa.

`+ vm-network-use-tor`: Habilita o deshabilita la red Tor para la interfaz VM. Si se habilita esta opción, el tráfico malintencionado procedente de los sistemas aislados del dispositivo WildFire durante el análisis de muestras se envía a través de la red Tor. La red Tor enmascarará su dirección IP de acceso público a fin de que los propietarios del sitio malintencionado no puedan determinar la fuente del tráfico.

`> cloud-intelligence`: se configura el dispositivo para enviar los diagnósticos, los informes o las muestras de WildFire a la nube de WildFire de Palo Alto Networks o para consultar automáticamente a la nube pública de WildFire antes de realizar el análisis local para conservar los recursos del dispositivo WildFire. La opción de envío de informes permite enviar informes de las muestras malintencionadas a la nube con fines de recopilación de información estadística. La opción de envío de muestras permite enviar muestras malintencionadas a la nube. Si la opción de envío de muestras está habilitada, no es necesario habilitar la opción de envío de informes, ya que la muestra se vuelve a analizar en la nube y se generan un nuevo informe y una firma si la muestra es malintencionada.

`> file-retention`: se configura durante cuánto tiempo se guardarán las muestras malintencionadas (malware y phishing) y no malintencionadas (grayware y benignas). El valor predeterminado para las muestras malintencionadas es indefinido (no se eliminan). El valor predeterminado para las muestras no malintencionadas es de 14 días. Por ejemplo, para conservar muestras no malintencionadas por 30 días: **`set deviceconfig setting wildfire file-retention non-malicious 30`**.

`> signature-generation`: permite que el dispositivo genere firmas localmente, lo que elimina la necesidad de enviar datos a la nube pública para bloquear el contenido malintencionado. El dispositivo WildFire analizará los archivos reenviados desde los cortafuegos de Palo Alto Networks o desde la API de WildFire y generará firmas de antivirus y DNS que bloquean tanto los archivos malintencionados como el tráfico de comandos y control asociado. Si el dispositivo detecta una dirección URL malintencionada, envía la dirección URL a PAN-DB y PAN-DB le asigna la categoría de malware.

Ejemplo de configuración

A continuación se muestra un resultado de ejemplo de la configuración de WildFire:

```
admin@WF-500# show deviceconfig setting wildfire wildfire
 { signature-generation { av yes; dns yes; url yes; } cloud-
intelligence { submit-report no; submit-sample yes; submit-
diagnostics yes; cloud-query yes; } file-retention { non-malicious
 30; malicious 1000; { active-vm vm-5; cloud-server wildfire-public-
cloud; vm-network-enable yes; }
```

set deviceconfig system eth2

Description (Descripción)

Configure la interfaz eth2.

Jerarquía de localización

```
set deviceconfig system
```

Sintaxis

```
eth2 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

Opciones

+ `default-gateway`: dirección IP de la puerta de enlace predeterminada de la interfaz eth2.

+ `ip-address`: dirección IP de la interfaz eth2.

+ `mtu`: unidad de transmisión máxima (Maximum Transmission Unit, MTU) de la interfaz eth2.

+ `netmask`: máscara de red de la interfaz eth2.

+ `speed-duplex`: velocidad de la interfaz (10 Mbps, 100 Mbps, 1 Gbps o autonegociación) y modo dúplex (completo o parcial) de la interfaz eth2.

> `permitted-ip`: direcciones IP con acceso a la interfaz eth2. Si especifica una máscara de red con la dirección IP, la máscara de red debe anotarse con barras. Por ejemplo, para especificar una dirección de clase C, introduzca: 10.10.10.100/24 (no 10.10.10.100 255.255.255.0).

> `service-disable`. deshabilita ICMP en la interfaz eth2.

Ejemplo de configuración

```
admin@wf-500(active-controller)# show deviceconfig system eth2 eth2
 { ip-address 10.10.10.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig system eth3

Description (Descripción)

Configure la interfaz eth3.

Jerarquía de localización

```
set deviceconfig system
```


Sintaxis

```
eth3 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

Opciones

+ `default-gateway`: dirección IP de la puerta de enlace predeterminada de la interfaz eth3.

+ `ip-address`: dirección IP de la interfaz eth3.

+ `mtu`: unidad de transmisión máxima (Maximum Transmission Unit, MTU) de la interfaz eth3.

+ `netmask`: máscara de red de la interfaz eth3.

+ `speed-duplex`: velocidad de la interfaz (10 Mbps, 100 Mbps, 1 Gbps o autonegociación) y modo dúplex (completo o parcial) de la interfaz eth3.

> `permitted-ip`: direcciones IP con acceso a la interfaz eth3. Si especifica una máscara de red con la dirección IP, la máscara de red debe anotarse con barras. Por ejemplo, para especificar una dirección de clase C, introduzca: 10.10.10.100/24 (no 10.10.10.100 255.255.255.0).

> `service-disable`. deshabilita ICMP en la interfaz eth3.

Ejemplo de configuración

```
admin@wf-500(active-controller)# show deviceconfig system eth3 eth3
 { ip-address 10.10.20.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server

Description (Descripción)

Configure el servidor principal de Panorama para gestionar el dispositivo WildFire o el clúster de dispositivos.

Jerarquía de localización

```
set deviceconfig system panorama local-panorama
```

Sintaxis

```
panorama-server {IP address | FQDN};
```


Opciones

`+ panorama-server`: configure la dirección IP o el nombre de dominio completo (fully qualified domain name, FQDN) del servidor principal de Panorama que utilizará para gestionar el dispositivo WildFire o el clúster de dispositivos.

Ejemplo de configuración

El resultado se redujo para mostrar únicamente la estrofa de resultado que muestra la configuración del servidor de Panorama.

```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server-2

Description (Descripción)

Configure el servidor de copia de seguridad de Panorama para gestionar el dispositivo WildFire o el clúster de dispositivos. La configuración de un servidor de copia de seguridad Panorama proporciona alta disponibilidad para el clúster o gestión individual de los dispositivos.

Jerarquía de localización

```
set deviceconfig system panorama local-panorama
```

Sintaxis

```
panorama-server-2 {IP address | FQDN};
```

Opciones

`+ panorama-server-2`: se configura la dirección IP o el nombre de dominio completo (fully qualified domain name, FQDN) del servidor de copia de seguridad de Panorama que utilizará para gestionar el dispositivo WildFire o el clúster de dispositivos.

Ejemplo de configuración

El resultado se redujo para mostrar únicamente la estrofa de resultado que muestra la configuración del servidor de Panorama.


```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig system update-schedule

Description (Descripción)

Programe las actualizaciones de contenido en un dispositivo WildFire. Estas actualizaciones de contenido equipan el dispositivo con la información sobre amenazas más actualizada para garantizar la detección precisa de malware y mejorar la capacidad del equipo para diferenciar el contenido malintencionado del contenido benigno.

Jerarquía de localización

```
set deviceconfig system update-schedule
```

Sintaxis

```
wf-content recurring { daily at <value> action {download-and-install
 | download-only}; weekly { action {download-and-install | download-
only}; at <value>; day-of-week {friday | monday | saturday | sunday |
 thursday | tuesday | wednesday}; } }
```

Opciones

> `wf-content`: actualizaciones de contenido de WildFire.

> `daily`: se programa la actualización diaria.

+ `action`: Especifique la acción que se va a realizar. Puede programar el dispositivo para descargar e instalar la actualización o descargar solamente y, a continuación, instalar manualmente.

+ `at`: especificación de tiempo hh:mm (por ejemplo, 20:10).

> `hourly`: se programa la actualización cada hora.

+ `action`: Especifique la acción que se va a realizar. Puede programar el dispositivo para descargar e instalar la actualización o descargar solamente y, a continuación, instalar manualmente.

+ `at`: minutos transcurridos después de una hora.

> `weekly`: se programa la actualización una vez por semana.

+ `action`: Especifique la acción que se va a realizar. Puede programar el dispositivo para descargar e instalar la actualización o descargar solamente y, a continuación, instalar manualmente.

+ `at`: especificación de tiempo hh:mm (por ejemplo, 20:10).

+ `day-of-week`: día de la semana (viernes, lunes, sábado, domingo, jueves, martes, miércoles).

Ejemplo de configuración

```
admin@WF-500# show update-schedule { wf-content { recurring
 { weekly { at 19:00; action download-and-install; day-of-week
 friday; } } } }
```

Nivel de privilegio requerido

superuser, deviceadmin

set deviceconfig system vm-interface

Description (Descripción)

La interfaz de VM es utilizada por el malware que se ejecuta en el espacio aislado de la máquina virtual del dispositivo WildFire para acceder a internet. Se recomienda la activación de este puerto, que a su vez ayudará a WildFire a identificar mejor la actividad maliciosa si el software malintencionado accede a Internet para la actividad de llamada a casa u otra actividad. Es importante que esta interfaz tenga una conexión a Internet aislada. Si su dispositivo WildFire está funcionando en modo FIPS/CC, la interfaz de VM está desactivada. Para obtener más información, consulte Configuración de la interfaz de VM del dispositivo WildFire.

Tras configurar la interfaz vm, habilítela ejecutando el siguiente comando:

```
set deviceconfig setting wildfire vm-network-enable yes
```

Jerarquía de localización

```
set deviceconfig system
```

Sintaxis

```
set vm-interface { default-gateway <ip_address>; dns-server
 <ip_address>; ip-address <ip_address>; link-state; mtu; netmask
 <ip_address>; speed-duplex; {
```

Opciones

+ `default-gateway`: puerta de enlace predeterminada para la interfaz de VM.

+ `dns-server`: servidor DNS para la interfaz de VM.

+ `ip-address`: dirección IP para la interfaz de VM.

+ `link-state`: se establece el estado del enlace en activo o inactivo.
+ `mtu`: unidad de transmisión máxima para la interfaz de VM.
+ `netmask`: máscara de red IP para la interfaz de VM.
+ `speed-duplex`: velocidad y dúplex para la interfaz de VM.

Ejemplo de configuración

A continuación se muestra una interfaz vm configurada.

```
vm-interface { ip-address 10.16.0.20; netmask 255.255.252.0; default-
gateway 10.16.0.1; dns-server 10.0.0.246; }
```

Nivel de privilegio requerido

superuser, deviceadmin

Referencia de comandos del modo de operación del dispositivo WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Dispositivo WildFire	❑ Licencia de WildFire

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de operación que son específicos del software del dispositivo WildFire. El resto de los comandos que forman parte del software del dispositivo WildFire son idénticos a los de PAN-OS. Consulte el inicio rápido de la CLI de PAN-OS 11.0 para obtener información sobre estos comandos.

- clear high-availability
- create wildfire api-key
- delete high-availability-key
- delete wildfire api-key
- delete wildfire-metadata
- disable wildfire
- edit wildfire api-key
- load wildfire api-key
- request cluster decommission
- request cluster reboot-local-node
- request high-availability state
- request high-availability sync-to-remote
- request system raid
- request wildfire sample redistribution
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show cluster all-peers
- show cluster controller
- show cluster membership
- show cluster task
- show cluster data migration status
- show high-availability all
- show high-availability control-link

- show high-availability state
- show high-availability transitions
- show system raid
- show wildfire
- show wildfire global
- show wildfire local
- submit wildfire local-verdict-change
- test wildfire registration

clear high-availability

Description (Descripción)

Elimine la información de las estadísticas del enlace de control de alta disponibilidad (high-availability, HA) y las estadísticas de transición en el nodo controlador de un clúster de dispositivos WildFire.

Sintaxis

```
create { high-availability { control-link { statistics; }
 transitions; } }
```

Opciones

`> control-link>`: se eliminan las estadísticas del enlace de control de HA.

`> transitions>`: se eliminan las estadísticas de transición de HA (eventos que se producen durante los cambios de HA).

Ejemplo de configuración

Después de eliminar las estadísticas del enlace de control o de transición, el clúster WildFire restablece todos los valores a cero (0).

```
admin@wf-500(active-controller)> show high-availability control-
link statistics High-Availability: Estadísticas de enlaces de
 control: HA1: Messages-TX : 0 Messages-RX : 0 Capability-Msg-TX :
 0 Capability-Msg-RX : 0 Error-Msg-TX : 0 Error-Msg-RX : 0 Preempt-
Msg-TX : 0 Preempt-Msg-RX : 0 Preempt-Ack-Msg-TX: 0 Preempt-Ack-Msg-
RX: 0 Primary-Msg-TX : 0 Primary-Msg-RX : 0 Primary-Ack-Msg-TX :
 0 Primary-Ack-Msg-RX : 0 Hello-Msg-TX : 0 Hello-Msg-RX : 0 Hello-
Timeouts : 0 Hello-Failures : 0 MasterKey-Msg-TX : 0 MasterKey-Msg-
RX : 0 MasterKey-Ack-Msg-TX : 0 MasterKey-Ack-Msg-RX : 0 Connection-
Failures : 0 Connection-Tries-Failures : 0 Connection-Listener-
Tries : 00 Connection-Active-Tries : 0 Ping-TX : 0 Ping-Fail-TX :
 0 Ping-RX : 0 Ping-Timeouts : 0 Ping-Failures : 0 Ping-Error-
Msgs : 0 Ping-Other-Msgs : 0 Ping-Last-Rsp : 0 admin@wf-500(active-
controller)> show high-availability transitions High-Availability:
 Transition Statistics: Unknown : 0 Suspended : 0 Initial : 0 Non-
Functional : 0 Passive : 0 Active : 0
```


Nivel de privilegio requerido

superuser, deviceadmin

create wildfire api-key

Description (Descripción)

Genere claves de API en el dispositivo WildFire que utilizará en un sistema externo para enviar muestras al dispositivo, realizar consultas en los informes o recuperar muestras y capturas de paquetes (PCAP) del dispositivo.

Sintaxis

```
create { wildfire { api-key { key <value>; name <value>; { { {
```

Opciones

+ `key`: cree una clave de API introduciendo un valor de clave manualmente. El valor debe constar de 64 caracteres alfabéticos (a-z) o números (0-9). Si no especifica la opción de clave, el dispositivo genera una clave automáticamente.

+ `name`: de manera opcional, puede introducir un nombre para la clave API. El nombre de clave API se utiliza simplemente para etiquetar las claves y facilitar la identificación de las claves asignadas para usos específicos y no tiene ningún efecto en la funcionalidad de las claves.

Ejemplo de configuración

El siguiente resultado indica que el dispositivo tiene tres claves de API y una clave se llama `my-api-key`.

```
admin@WF-500> show wildfire global api-keys all
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------
+------------+ | <API KEY> | my-api-key | | <API
 KEY> | my-api-key | | <API KEY> | my-api-key |
 +-----------------------------------------------------+------------
+ +---------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +---------+---------------------
+---------------------+ | Enabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | | Enabled | 2016-02-06 12:13:22 | 2017-03-01 12:10:20 |
 | Enabled | 2014-08-04 17:00:42 | 2017-03-01 11:12:52 | +---------
+---------------------+---------------------+
```

Nivel de privilegio requerido

superuser, deviceadmin

delete high-availability-key

Description (Descripción)

Elimina la clave de cifrado de peer utilizada para la alta disponibilidad (high-availability, HA) en los enlaces de control del clúster de un nodo controlador del clúster de dispositivos WildFire.

Sintaxis

```
delete { high-availability-key; }
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

La línea resaltada en el resultado muestra que el cifrado no está habilitado en los enlaces de control de HA.

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability: Local Information: Versión: 1 State: active-
controller (last 1 days) Device Information: Management IPv4 Address:
 10.10.10.14/24 Management IPv6 Address: HA1 Control Links Joint
 Configuration:  Encryption Enabled: no Election Option Information:
 Priority: primary Preemptive: no Version Compatibility: Software
 Version: Match Application Content Compatibility: Match Anti-
Virus Compatibility: Match Peer Information: Connection status:
 up Version: 1 State: passive-controller (last 1 days) Device
 Information: Management IPv4 Address: 10.10.20.112/24 Management
 IPv6 Address: Connection up; Primary HA1 link Election Option
 Information: Priority: secondary Preemptive: no Configuration
 Synchronization: Enabled: yes Running Configuration: synchronized
```

Nivel de privilegio requerido

superuser, deviceadmin

delete wildfire api-key

Description (Descripción)

Elimine una clave API del dispositivo WildFire. Los sistemas configurados para el uso de la API para realizar funciones de la API en el dispositivo no pueden acceder al dispositivo una vez eliminada la clave.

Sintaxis

```
delete { wildfire { api-key { key <value>; { { {
```

Opciones

`+key <value>`: el valor de la clave que desea eliminar. Para ver una lista de claves API, ejecute el siguiente comando:

```
admin@WF-500> show wildfire global api-keys all
```

Ejemplo de configuración

```
admin @ WF-500> eliminar la clave de clave de API de Wildfire <API
 KEY> Clave API <API Key> eliminado
```

Nivel de privilegio requerido

superuser, deviceadmin

delete wildfire-metadata

Description (Descripción)

Elimine actualizaciones de contenido del dispositivo WildFire. Para obtener más información sobre las actualizaciones de contenido y cómo instalarlas, consulte request wf-content.

Sintaxis

```
delete { wildfire-metadata update <value>; {
```

Opciones

`+ update <value>`: defina la actualización de contenido que desea eliminar.

Ejemplo de configuración

En el siguiente resultado, se muestra la eliminación de una actualización con el nombre:

```
panup-all-wfmeta-2-181.candidate.tgz. admin@WF-500> eliminar
 actualización de metadatos de wildfire panup-all-
wfmeta-2-181.candidate.tgz eliminado con éxito panup-all-
wfmeta-2-181.candidate.tgz
```

Nivel de privilegio requerido

superuser, deviceadmin

disable wildfire

Description (Descripción)

Deshabilita la firma del dominio o la firma de la muestra, de modo que se excluya de la próxima versión de paquete de contenido de WildFire.

Sintaxis

```
disable wildfire { domain-signature { domain <value>; } OR... sample-signature { sha256 { equal <value>; } }
```

Opciones

`> domain-signature`: establece el estado de la firma del dominio como deshabilitado, de modo que se excluya de la próxima versión de contenido de WildFire.

`> sample-signature`: establece el estado de la firma de la muestra como deshabilitado, de modo que se excluya de la próxima versión de contenido de WildFire.

Ejemplo de configuración

Una muestra o dominio deshabilitado correctamente no muestra resultados.

```
admin@WF-500> disable wildfire sample-signature sha256 equal
 d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdb1ec08228
```

Nivel de privilegio requerido

superuser, deviceadmin

edit wildfire api-key

Description (Descripción)

Modifique un nombre de clave de API o el estado de la clave (habilitada/deshabilitada) en un dispositivo WildFire.

Sintaxis

```
edit { wildfire { api-key [name | status] key <value>; { {
```

Opciones

+ `name`: cambie el nombre de una clave API.
+ `status`: habilite o deshabilite una clave de API.
* `key`: especifique la clave que desea modificar.

Ejemplo de configuración

El valor de la clave de este comando es obligatorio. Por ejemplo, para cambiar el nombre de una clave llamada `stu` a `stu-key1`, introduzca el siguiente comando:

En el caso del siguiente comando, no es necesario introducir el nombre de la clave anterior. Solo se debe introducir el nuevo nombre de la clave.

```
admin@WF-500> edit wildfire api-key name stu-key1 key <API KEY>
 Para cambiar el estado de stu-key1 a desactivado, introduzca el
 siguiente comando: admin@WF-500> edit wildfire api-key status
 disable key <API KEY> Salida de ejemplo que muestra que queda
 desactivado:: admin@WF-500> show wildfire global api-keys all
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------+------------+
 | <API KEY> | stu-key1 |
 +-----------------------------------------------------+------------
+ +----------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +----------+---------------------
+---------------------+ | Disabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | +----------+---------------------+---------------------+
```

Nivel de privilegio requerido

superuser, deviceadmin

load wildfire api-key

Description (Descripción)

Después de importar las claves de API en el dispositivo WildFire, debe utilizar el comando load para que las claves estén disponibles para su uso. Utilice este comando para sustituir todas las claves de API existentes. Además, puede combinar las claves del archivo de importación con la base de datos de claves existentes.

Sintaxis

```
load { wildfire { from <value> mode [merge | replace]; { {
```

Opciones

* `from`: especifique el nombre de archivo de la clave de API que desea importar. Los archivos de claves utilizan la extensión de archivo .keys. Por ejemplo, my-api-keys.keys. Para ver una lista de las claves disponibles para su importación, introduzca el siguiente comando:

```
admin@WF-500> load wildfire api-key from ?
```

+ `mode`: De forma opcional, puede introducir el modo para la importación (combinación/sustitución). Por ejemplo, para sustituir la base de datos de claves del dispositivo por el contenido del nuevo archivo de claves, introduzca el siguiente comando:


```
admin@WF-500> load wildfire api-key mode replace from my-api-keys.keys
```

Si no especifica la opción **mode**, la acción predeterminada combinará las claves.

Nivel de privilegio requerido

superuser, deviceadmin

request cluster decommission

Description (Descripción)

Elimina el nodo del clúster de dispositivos WildFire de un clúster de tres o más nodos. No utilice este comando para eliminar un nodo de un clúster de dos nodos. En cambio, realice la Eliminación de un nodo de un clúster localmente utilizando los comandos `delete deviceconfig high-availability` y `delete deviceconfig cluster`.

Jerarquía de localización

request cluster

Sintaxis

```
request { cluster { decommission { show; start; stop; } } }
```

Opciones

`show`: se muestra el estado del trabajo de retirada del nodo.

`start`: se comienza el trabajo de retirada del nodo.

`stop`: se aborta el trabajo de retirada del nodo.

Ejemplo de configuración

El campo `Node mode` (modo del nodo) confirma que la retirada del nodo del clúster se realizó correctamente debido a que el modo es `stand_alone` (independiente) en lugar de `controller` (controlador) o `worker` (de trabajo).

```
admin@wf-500> show cluster membership Service Summary: wfpc signature
 Cluster name: Address: 10.10.10.86 Host name: wf-500 Node name:
 wfpc-009707000xxx-internal Serial number: 009707000xxx Node mode:
 stand_alone Server role: True HA priority: Last changed: Wed, 15 Feb
 2017 00:05:11 -0800 Services: wfcore signature wfpc infra Monitor
 status: Serf Health Status: passing Agent alive and reachable
 Application status: wildfire-apps-service: Ready global-db-service:
 ReadyStandalone global-queue-service: ReadyStandalone local-db-
service: ReadyMaster
```


Nivel de privilegio requerido

superuser, deviceadmin

request cluster reboot-local-node

Description (Descripción)

Reinicie correctamente el nodo del clúster WildFire local.

Jerarquía de localización

```
request cluster
```

Sintaxis

```
request { cluster { reboot-local-node; } }
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

Puede comprobar que el nodo del clúster local se haya reiniciado o se encuentre en el proceso de reinicio de varias maneras:

- `show cluster task local`: se muestran las tareas solicitadas en el nodo local.
- `show cluster task current`: se muestran las tareas en ejecución actualmente en el nodo local o la última tarea completada (solo nodos controladores).
- `show cluster task pending`: se muestran las tareas en cola que todavía no se ejecutaron en el nodo local (solo nodos controladores).
- `show cluster task history`: se muestran las tareas que se ejecutaron en el nodo local (solo nodos controladores).

Por ejemplo, el siguiente comando muestra que se han completado correctamente dos tareas de reinicio de nodos del clúster:

```
admin@qa15(passive-controller)> show cluster task history
 Request:        reboot from qa16 (009701000044/35533) at
 2017-02-17 19:21:53 UTC                 Reboot requested by
 admin Response:       permit by qa15 at 2017-02-17 22:11:31
 UTC                 request not affecting healthy core server.
 Progress:       Wait for kv store ready for query...
  KV store is ready, wait for cluster leader available...
                 Cluster leader is 2.2.2.16...
 Checking is sysd and clusterd are alive...                 Checking
 if cluster-mgr is ready...                  Checking global-db-
cluster readiness...               Stopping global-queue server
 and leaving cluster...                Stopping global-db servers
```



```
and doing failover...                    rebooting... Finished:
 success at 2017-02-17 22:17:56 UTC Request:        reboot from
qa16 (009701000044/35535) at 2017-02-17 22:45:50 UTC
 Reboot requested by admin Response:       permit by qa15 at
2017-02-17 23:06:44 UTC                  request not affecting
healthy core server. Progress:       Wait for kv store ready
for query...                  KV store is ready, wait for cluster
leader available...                  Cluster leader is 2.2.2.15...
                Checking is sysd and clusterd are alive...
                Checking if cluster-mgr is ready...
 Checking global-db-cluster readiness...                  Stopping
global-queue server and leaving cluster...                  Stopping
global-db servers and doing failover...                 rebooting...
Finished:       success at 2017-02-17 23:12:53 UTC
```

Nivel de privilegio requerido

superuser, deviceadmin

request high-availability state

Description (Descripción)

En un clúster de dispositivos WildFire, convierta el estado de alta disponibilidad (high-availability, HA) del nodo controlador local o el nodo controlador del peer en funcional.

Jerarquía de localización

```
request high-availability
```

Sintaxis

```
request { high-availability { state { functional; } peer {
 functional; } } }
```

Opciones

> `functional`: se convierte el estado de HA del nodo controlador principal en funcional.

> `peer`: se convierte el estado de HA del nodo controlador del peer en funcional.

Ejemplo de configuración

Las líneas resaltadas en el resultado muestras que el estado de HA del nodo controlador local es funcional en la función de controlador activo (principal) y que el estado de HA del nodo controlador del peer es funcional en la función del controlador pasivo (copia de seguridad).

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability: Local Information: Versión: 1 State: active-
controller (last 1 days) Device Information: Management IPv4 Address:
 10.10.10.14/24 Management IPv6 Address: HA1 Control Links Joint
```



```
 Configuration: Encryption Enabled: no Election Option Information:
 Priority: primary Preemptive: no Version Compatibility: Software
 Version: Match Application Content Compatibility: Match Anti-
Virus Compatibility: Match Peer Information: Connection status:
 up Version: 1 State: passive-controller (last 1 days) Device
 Information: Management IPv4 Address: 10.10.20.112/24 Management
 IPv6 Address: Connection up; Primary HA1 link Election Option
 Information: Priority: secondary Preemptive: no Configuration
 Synchronization: Enabled: yes Running Configuration: synchronized
```

Nivel de privilegio requerido

superuser, deviceadmin

request high-availability sync-to-remote

Description (Descripción)

En un clúster de dispositivos WildFire, sincronice la configuración del candidato del nodo controlador local o la configuración actual, o el reloj (hora y fecha) del nodo controlador local con el nodo controlador del peer de alta disponibilidad (high-availability, HA) remoto.

Jerarquía de localización

request high-availability

Sintaxis

```
request { high-availability { sync-to-remote { candidate-config;
 clock; running-config; } } }
```

Opciones

`> candidate-config`: se sincroniza la configuración candidata en el nodo controlador del peer local con el nodo controlador del peer de HA remoto.

`> clock`: se sincroniza el reloj (hora y fecha) en el nodo controlador del peer local con el nodo controlador del peer de HA.

`> running-config`: se sincroniza la configuración actual en el nodo controlador del peer local con el nodo controlador del peer de HA remoto.

Ejemplo de configuración

La línea resaltada en el resultado muestra que el estado de la configuración de HA está sincronizado con el nodo controlador del peer de HA.

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability: Local Information: Versión: 1 State: active-
controller (last 1 days) Device Information: Management IPv4 Address:
 10.10.10.14/24 Management IPv6 Address: HA1 Control Links Joint
 Configuration: Encryption Enabled: no Election Option Information:
 Priority: primary Preemptive: no Version Compatibility: Software
```



```
 Version: Match Application Content Compatibility: Match Anti-
Virus Compatibility: Match Peer Information: Connection status:
 up Version: 1 State: passive-controller (last 1 days) Device
 Information: Management IPv4 Address: 10.10.20.112/24 Management
 IPv6 Address: Connection up; Primary HA1 link Election Option
 Information: Priority: secondary Preemptive: no Configuration
 Synchronization: Enabled: yes Running Configuration: synchronized
```

Nivel de privilegio requerido

superuser, deviceadmin

request system raid

Description (Descripción)

Use esta opción para manejar los pares de RAID instalados en el dispositivo WildFire. El dispositivo WF-500 se entrega con cuatro unidades en los cuatro primeros conectores de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Jerarquía de localización

request system

Sintaxis

```
raid { remove <value>; OR... copy { from <value>; to <value>; } OR...
 add {
```

Opciones

- `add`: se añade una unidad al par de discos RAID correspondiente
- `copy`: se copia y migra de una unidad a otra en la plataforma
- `remove`: unidad que se eliminará del par de discos RAID

Ejemplo de configuración

El siguiente resultado muestra un dispositivo WF-500 con una RAID configurada correctamente.

```
admin@WF-500> show system raid Disk Pair A Available Disk id A1
 Present Disk id A2 Present Disk Pair B Available Disk id B1 Present
 Disk id B2 Present
```

Nivel de privilegio requerido

superuser, deviceadmin

request wildfire sample redistribution

Description (Descripción)

Redistribuye las muestras del nodo del clúster de dispositivos WildFire local a otro nodo del clúster mientras conserva las muestras opcionalmente en el nodo local.

Jerarquía de localización

```
request system
```

Sintaxis

```
request { wildfire { sample { redistribution {   keep-local-copy {no
 | yes};   serial-number <value>; } } } }
```

Opciones

* `keep-local-copy`: se mantiene o no una copia de las muestras redistribuidas en el nodo del dispositivo WildFire local.

* `serial-number`: número de serie del nodo al que redistribuye las muestras.

Ejemplo de configuración

`Storage Nodes` muestra el otro nodo al que el nodo local redistribuye las muestras. Si el nodo local no redistribuye muestras, solo se muestra una ubicación del nodo de almacenamiento. Si el nodo local redistribuye muestras, `Storage Nodes` muestra dos ubicaciones de nodo de almacenamiento. El resultado resaltado muestra los dos nodos de almacenamiento que almacenan muestras (el nodo local y el nodo al cual el nodo local redistribuye las muestras) y comprueba que se produzca la redistribución de muestras.

```
admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples
 +-------------------------------------------------------------------------
+ | SHA256 | Finish Date | Create Date | Malicious |
 +-------------------------------------------------------------------------
+ | <HASH VALUE> | 2017-03-24 17:27:40 | 2017-03-24 15:41:47 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:46 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:54 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:25:12 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:28 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:58 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:52 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:32 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:58 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:22:02 | 2017-03-24 14:55:23 | Yes |
 +-------------------------------------------------------------------------
+
 +-----------------------------------------------------------------
+ | Storage Nodes | Analysis Nodes | Status | File Type |
```



```
 +-------------------------------------------------------------------
+ | 0907:ld2_2,065:ld2_2 | qa116 | Notify Finish | Java JAR |
 | 0097:ld2_2,004:ld2_2 | qa117 | Notify Finish | Java Class
 | | 0524:ld2_2,006:ld2_2 | qa117 | Notify Finish | Java
 Class | | 0656:ld2_2,524:ld2_2 | qa117 | Notify Finish |
 Java Class | | 0024:ld2_2,056:ld2_2 | qa117 | Notify Finish
 | DLL | | 0324:ld2_2,006:ld2_2 | qa117 | Notify Finish |
 Java JAR | | 0682:ld2_2,006:ld2_2 | qa116 | Notify Finish |
 Java JAR | | 0092:ld2_2,016:ld2_2 | qa116 | Notify Finish |
 DLL | | 0682:ld2_2,002:ld2_2 | qa116 | Notify Finish | DLL
 | | 0056:ld2_2,824:ld2_2 | qa117 | Notify Finish | DLL |
 +-------------------------------------------------------------------
* lines 1-10
```

Nivel de privilegio requerido

superuser, deviceadmin

request system wildfire-vm-image

Realice actualizaciones de las imágenes del espacio aislado de la máquina virtual (virtual machine, VM) del dispositivo WildFire utilizadas para analizar archivos. Para recuperar imágenes de VM del servidor de actualizaciones de Palo Alto Networks, primero debe descargar la imagen manualmente, alojarla en un servidor habilitado para SCP y, a continuación, recuperar la imagen del dispositivo mediante el cliente SCP. Una vez descargada la imagen en el dispositivo, puede instalarla mediante este comando.

Jerarquía de localización

request system

Sintaxis

```
request { system { wildfire-vm-image { upgrade install file
 <value>; } } }
```

Opciones

`> wildfire-vm-image`: instale las imágenes de máquina virtual (VM).

`+ upgrade install file`: actualice la imagen de VM. Después de la opción de archivo, escriba `?` para ver una lista de las imágenes de VM disponibles. Por ejemplo, ejecute el siguiente comando para mostrar las imágenes disponibles:

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

Ejemplo de configuración

Para enumerar las imágenes de VM disponibles, ejecute el siguiente comando:

```
admin@WF-500> request system wildfire-vm-image upgrade install
 file ? Para instalar una imagen de máquina virtual (Windows
```



```
7 de 64 bits en este ejemplo), ejecute el siguiente comando:
admin@WF-500> request system wildfire-vm-image upgrade install file
WFWin7_64Base_m-1.0.0_64base
```

Nivel de privilegio requerido

superuser, deviceadmin

request wf-content

Realice las actualizaciones de contenido en un dispositivo WildFire. Estas actualizaciones de contenido equipan el dispositivo con la información sobre amenazas más actualizada para garantizar la detección precisa de malware y mejorar la capacidad del equipo para diferenciar el contenido malintencionado del contenido benigno. Para programar las actualizaciones de contenido de modo que se instalen automáticamente, consulte set deviceconfig system update-schedule y, para eliminar las actualizaciones de contenido en el dispositivo WildFire, consulte delete wildfire-metadata.

Jerarquía de localización

```
request
```

Sintaxis

```
request wf-content { downgrade install {previous | <value>}; upgrade
 { check download latest info install { file <filename> version
 latest; } } }
```

Opciones

> `downgrade`: Instala una versión de contenido anterior. Utilice la opción anterior para instalar el paquete de contenido instalado previamente o introduzca un valor para cambiar a una versión inferior específica del paquete de contenido.

> `upgrade`: Realiza funciones de actualización del contenido.

> `check`: Obtenga información sobre los paquetes de contenido disponibles del servidor de actualizaciones de Palo Alto Networks.

> `download`: Descargue un paquete de contenido.

> `info`: Muestre la información sobre los paquetes de contenido disponibles.

> `install`: Instale un paquete de contenido.

> `file`: Especifique el nombre del archivo que contiene el paquete de contenido.

> `version`: Descargue o actualice en función del número de versión del paquete de contenido.

Ejemplo de configuración

Para enumerar las actualizaciones de contenido disponibles, ejecute el siguiente comando:


```
admin@WF-500> request wf-content upgrade check
 Version Size Released on Downloaded Installed
 ------------------------------------------------------------------------------
 2-217 58MB 2014/07/29 13:04:55 PDT yes current 2-188 58MB 2014/07/01
 13:04:48 PDT yes previous 2-221 59MB 2014/08/02 13:04:55 PDT no no
```

Nivel de privilegio requerido

superuser, deviceadmin

save wildfire api-key

Description (Descripción)

Utilice el comando save para guardar todas las claves de API del dispositivo WildFire en un archivo. Puede exportar el archivo de claves para hacer copias de seguridad o modificar las claves en bloque. Para obtener información detallada sobre el uso de la API de WildFire en un dispositivo WildFire, consulte la Referencia de la API de WildFire.

Jerarquía de localización

```
Save (Guardar).
```

Sintaxis

```
save { wildfire { api-key to <value>; { {
```

Opciones

* `to`: Introduzca el nombre de archivo para la exportación de claves. Por ejemplo, para exportar todas las claves de API de WildFire a un archivo con el nombre my-wf-keys, introduzca el siguiente comando:

```
admin@WF-500> save wildfire api-key to my-wf-keys
```

Nivel de privilegio requerido

superuser, deviceadmin

set wildfire portal-admin

Description (Descripción)

Establece la contraseña de la cuenta de administrador del portal que el administrador utilizará para ver los informes de análisis de WildFire generados por un dispositivo WildFire. El nombre de la cuenta (admin) y la contraseña son obligatorios para ver el informe en el cortafuegos o en Panorama en **Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)** > **View WildFire Report (Ver informe de WildFire)**. El nombre de usuario y la contraseña predeterminados son admin/admin.

La cuenta del administrador del portal es la única cuenta que puede configurar en el dispositivo para ver los informes del cortafuegos o Panorama. No puede crear cuentas ni cambiar el nombre de la cuenta. No es la misma cuenta de administrador utilizada para gestionar el dispositivo.

Jerarquía de localización

```
set wildfire
```

Sintaxis

```
set { wildfire { portal-admin { password <value>; } }
```

Ejemplo de configuración

A continuación se muestra el resultado de este comando.

```
admin@WF-500> set wildfire portal-admin password Enter password:
 Confirm password:
```

Nivel de privilegio requerido

superuser, deviceadmin

show cluster all-peers

Description (Descripción)

En un nodo controlador del clúster de dispositivos WildFire, muestre el estado de todos los miembros del clúster de dispositivos WildFire, incluso el modo del dispositivo WildFire (controlador o trabajador), el estado de la conexión y el estado del servicio de aplicación.

Jerarquía de localización

```
show cluster
```

Sintaxis

```
all-peers;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
admin@thing1(active-controller)> show cluster all-peers Address
 Mode Server Node Name ------- ---- ------ --------- 10.10.10.14
  controller Self True thing1 Service: infra signature wfcore wfpc
 Status: Connected, Server role applied Changed: Wed, 15 Feb 2017
 09:12:01 -0800 WF App: wildfire-apps-service: Ready global-db-
service: JoinedCluster global-queue-service: JoinedCluster siggen-
db: ReadyMaster 10.10.10.112   controller Peer True thing2 Service:
 infra signature wfcore wfpc Status: Connected, Server role applied
 Changed: Wed, 15 Feb 2017 09:13:00 -0800 WF App: wildfire-apps-
service: Ready global-db-service: ReadyLeader global-queue-service:
 ReadyLeader siggen-db: ReadySlave Diag report: 10.10.10.112:
 reported leader '10.10.10.112', age 0. 10.10.10.14: local node
 passed sanity check.
```

Nivel de privilegio requerido

superuser, deviceadmin

show cluster controller

Description (Descripción)

En un nodo controlador del clúster de dispositivos WildFire, muestra el estado de los controladores del clúster de dispositivos WildFire, incluso en nombre del clúster y la función del nodo del controlador local (si el campo `Active Controller` muestra el valor `True`, el controlador local es el controlador principal; si el campo `Active Controller` muestra el valor `False`, el controlador local es el controlador de copia de seguridad).

Jerarquía de localización

```
show cluster
```

Sintaxis

```
controller;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
admin@thing1(active-controller)> show cluster controller Cluster
 name: satriani1 K/V API online: True Task processing: on Active
 Controller: Anuncio de DNS verdadero: Nombre DNS del servicio de
 aplicaciones: App Service Avail: 10.10.10.112, 10.10.10.14 Core
```



```
 Servers: 009707000742:: 10.10.10.112 009701000043: 10.10.10.14 Good
 Core Servers: 2 Suspended Nodes: Current Task: no tasks found
```

Nivel de privilegio requerido

superuser, deviceadmin

show cluster data migration status

Description (Descripción)

Utilice este comando desde un nodo de controlador de clúster de dispositivos WildFire para mostrar el estado actual de la migración de datos. El comando aparece cuando se inicia la migración de datos y su progreso. Cuando finaliza la migración de datos, el comando muestra la marca de tiempo de finalización. Si la migración de datos falla, aparecerá `0% completed (0 % completado)` en el estado.

Jerarquía de localización

```
show cluster
```

Sintaxis

```
data-migration-status;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
adminWF-500(active-controller)> show cluster data-migration-status
 100% completed on Mon Sep 9 21:44:48 PDT 2019
```

Nivel de privilegio requerido

superuser, deviceadmin

show cluster membership

Description (Descripción)

Muestra la información de pertenencia del clúster de dispositivos WildFire del nodo del clúster o el dispositivo WildFire independiente, que incluye la dirección IP, el nombre del host, el número de serie del dispositivo WildFire, la función del dispositivo (`Node mode` [Modo del nodo]), la prioridad de alta disponibilidad y el estado de la aplicación.

Jerarquía de localización

```
show cluster
```

Sintaxis

```
membership;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

Puede mostrar la información de pertenencia del clúster de los miembros del nodo del clúster de dispositivos WildFire (nodos controladores y de trabajo) y los dispositivos WildFire independientes para comprobar si pertenecen a un clúster, el estado de su aplicación y otra información del host local. El resultado varía levemente según la función del dispositivo WildFire. Las diferencias son las siguientes:

- El mensaje indica el nodo controlador activo (principal) y el nodo controlador pasivo (copia de seguridad), pero no indica un nodo de trabajo o nodo independiente.
- El `Node mode` (Modo del nodo) indica si el dispositivo WildFire es un `controller node` (Nodo controlador), un `worker node` (Nodo de trabajo) o un dispositivo WildFire `stand_alone` (independiente).
- `HA priority` (Prioridad de HA) muestra `primary` (principal) para el nodo controlador activo, `secondary` (secundario) para el nodo controlador pasivo (copia de seguridad) y el campo permanece en blanco en el caso de los nodos de trabajo y los dispositivos WildFire independientes.
- Los campos `Application status` (Estado de la aplicación) muestran diferentes valores en algunos campos. En `global-db-service` y `global-queue-service`, los miembros del clúster muestran `ReadyLeader` o `JoinedCluster`, y los dispositivos independientes muestran `ReadyStandalone`.

  En `siggen-db`, el nodo controlador principal del clúster de dispositivos WildFire muestra `ReadyMaster`, el nodo controlador secundario del clúster de dispositivos WildFire muestra `ReadySlave`, los nodos de trabajo del clúster de dispositivos WildFire muestran `Ready` y los dispositivos WildFire independientes muestran `ReadyMaster`.

Los últimos cuatro dígitos de cada número de serie de dispositivo WildFire se cambia a "xxxx" en la pantalla para evitar revelar los números de serie reales.

Resultado en el nodo controlador principal en un clúster de dispositivos WildFire:

```
admin@thing1(active-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: satriani1 Address: 10.10.10.14
 Host name: thing1 Node name: wfpc-00970100xxxx-internal Serial
 number: 00970100xxxx Node mode: controller Server role: True HA
 priority: primary Last changed: Wed, 15 Feb 2017 09:12:01 -0800
 Services: wfcore signature wfpc infra Monitor status: Serf Health
 Status: passing Agent alive and reachable Application status:
```



```
 wildfire-apps-service: Ready global-db-service: JoinedCluster
 global-queue-service: JoinedCluster siggen-db: ReadyMaster
```

Resultado en el nodo controlador de copia de seguridad en un clúster de dispositivos WildFire:

```
admin@thing2(passive-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: satriani1 Address:
 10.10.10.112 Host name: thing2 Node name: wfpc-00970700xxxx-internal
 Serial number: 009707000xxxx Node mode: controller Server role:
 True HA priority: secondary Last changed: Wed, 15 Feb 2017 09:13:10
 -0800 Services: wfcore signature wfpc infra Monitor status: Serf
 Health Status: passing Agent alive and reachable Application status:
 wildfire-apps-service: Ready global-db-service: ReadyLeader global-
queue-service: ReadyLeader siggen-db: ReadySlave
```

Resultado en el nodo de trabajo en un clúster de dispositivos WildFire:

```
admin@grinch> show cluster membership Service Summary: wfpc Cluster
 name: satriani1 Address: 10.10.10.19 Host name: grinch Node name:
 wfpc-00970100xxxx-internal Serial number: 00970100xxxx Node mode:
 worker Server role: True HA priority: Last changed: Thu, 09 Feb
 2017 15:55:55 -0800 Services: wfcore wfpc infra Monitor status: Serf
 Health Status: passing Agent alive and reachable Application status:
 wildfire-apps-service: Ready global-db-service: JoinedCluster
 global-queue-service: JoinedCluster siggen-db: Listo
```

Resultado en un dispositivo WildFire independiente (no es miembro de un clúster de dispositivos WildFire):

```
admin@max> show cluster membership Service Summary: wfpc signature
 Cluster name: Address: 10.10.10.90 Host name: max Node name:
 wfpc-00970700xxxx-internal Serial number: 00970700xxxx Node mode:
 stand_alone Server role: True HA priority: Last changed: Mon, 13 Feb
 2017 02:54:52 -0800 Services: wfcore signature wfpc infra Monitor
 status: Serf Health Status: passing Agent alive and reachable
 Application status: wildfire-apps-service: Ready global-db-service:
 ReadyStandalone global-queue-service: ReadyStandalone siggen-db:
 ReadyMaster
```

Nivel de privilegio requerido

superuser, deviceadmin

show cluster task

Description (Descripción)

Muestra la información de la tarea del clúster de dispositivos WildFire para el nodo de clúster local o para todos los nodos de clúster, o muestra el historial de tareas del clúster completadas o las tareas pendientes del clúster.

Jerarquía de localización

```
show cluster
```

Sintaxis

```
task { current; history; local; pending; }
```

Opciones

`> current`: se muestran las tareas que se permiten actualmente en el clúster de dispositivos WildFire. Disponible únicamente en los nodos controlador del clúster.

`> history`: se muestran las tareas del clúster completadas. Disponible únicamente en los nodos controlador del clúster.

`> local`: se muestran las tareas pendientes en el nodo del clúster de dispositivos WildFire local.

`> pending`: se muestran las tareas pendientes de todo el clúster de dispositivos WildFire. Disponible únicamente en los nodos controlador del clúster.

Ejemplo de configuración

```
admin@WF-500(active-controller)> show cluster task local
 Request:        reboot from WF-500 (009701000034/74702) at
 2017-02-21 03:06:45 UTC                Reboot requested by
 admin Queued:         by WF-500                2/3 core servers
 available. reboot not allowed to maintain quorum Request:
 reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27 UTC
                Reboot requested by admin Queued:         by WF-500
                2/3 core servers available. reboot not allowed to
 maintain quorum admin@WF-500(active-controller)> show cluster task
 current no tasks found admin@WF-500(active-controller)> show cluster
 task pending Request:        reboot from WF-500 (009701000034/74702)
 at 2017-02-21 03:06:45 UTC                Reboot requested by
 admin Queued:         by WF-500                2/3 core servers
 available. reboot not allowed to maintain quorum Request:
 reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27 UTC
                Reboot requested by admin Queued:         by WF-500
                2/3 core servers available. reboot not allowed to
 maintain quorum admin@WF-500B(passive-controller)> show cluster
 task history Request:        reboot from WF-500 (009701000044/35533)
 at 2017-02-17 19:21:53 UTC                Reboot requested by
 admin Response:       permit by WF-500B at 2017-02-17 22:11:31
 UTC                request not affecting healthy core server.
 Progress:       Wait for kv store ready for query...
  KV store is ready, wait for cluster leader available...
                Cluster leader is 10.10.10.100...
 Checking is sysd and clusterd are alive...                Checking
 if cluster-mgr is ready...                Checking global-db-
cluster readiness...              Stopping global-queue server
 and leaving cluster...                 Stopping global-db servers
```



```
 and doing failover...                    rebooting... Finished:
 success at 2017-02-17 22:17:56 UTC
```

Nivel de privilegio requerido

superuser, deviceadmin

show high-availability all

Description (Descripción)

Muestra toda la información de alta disponibilidad (HA) del clúster de dispositivos WildFire, que incluye información del enlace de control de HA, del estado de HA y la transición de HA, información del software del peer, de la actualización de contenido y de compatibilidad de antivirus, además de la información de conexión del peer y de la función.

Jerarquía de localización

```
show high-availability
```

Sintaxis

```
all;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
admin@thing1(active-controller)> show high-availability all High-
Availability: Local Information: Versión: 1 State: active-controller
 (last 1 days) Device Information: Management IPv4 Address:
 10.10.10.14/24 Management IPv6 Address: HA1 Control Links Joint
 Configuration: Link Monitor Interval: 3000 ms Encryption Enabled:
 no HA1 Control Link Information: IP address: 10.10.10.140/24
 MAC Address: 00:00:5e:00:53:ff Interface: eth3 Link State: Up;
 Setting: 1Gb/s-full Key Imported : no Election Option Information:
 Priority: primary Preemptive: no Promotion Hold Interval: 2000
 ms Hello Message Interval: 8000 ms Heartbeat Ping Interval: 2000
 ms Preemption Hold Interval: 1 min Monitor Fail Hold Up Interval:
 0 ms Addon Master Hold Up Interval: 500 ms Version Information:
 Build Release: 8.0.1-c31 URL Database: Not Installed Application
 Content: 497-2688 Anti-Virus: 0 Version Compatibility: Software
 Version: Match Application Content Compatibility: Match Anti-
Virus Compatibility: Match Peer Information: Connection status:
 up Version: 1 State: passive-controller (last 1 days) Device
 Information: Management IPv4 Address: 10.10.10.30/24 Management IPv6
 Address: HA1 Control Link Information: IP address: 10.10.10.130 MAC
 Address: 00:00:5e:00:53:00 Connection up; Primary HA1 link Election
 Option Information: Priority: secondary Preemptive: no Version
```



```
 Information: Build Release: 8.0.1-c31 URL Database: Not Installed
 Application Content: 497-2688 Anti-Virus: 0 Initial Monitor Hold
 inactive; Allow Network/Links to Settle: Link and path monitoring
 failures honored Configuration Synchronization: Enabled: yes Running
 Configuration: synchronized
```

Nivel de privilegio requerido

superuser, deviceadmin

show high-availability control-link

Description (Descripción)

Muestra las estadísticas de alta disponibilidad (HA) del clúster de dispositivos WildFire para el enlace de control de HA entre los nodos controladores principal y de copia de seguridad, que incluye los diferentes tipos de mensajes transmitidos y recibidos en el enlace de control de HA, las fallos de conexión y la actividad de ping.

Jerarquía de localización

```
show high-availability
```

Sintaxis

```
control-link { statistics; }
```

Opciones

`> statistics`: se muestran las estadísticas del enlace de control de HA del nodo controlador del clúster de dispositivos WildFire.

Ejemplo de configuración

```
admin@thing1(active-controller)> show high-availability control-
link statistics High-Availability: Control Link Statistics: HA1:
 Messages-TX : 13408 Messages-RX : 13408 Capability-Msg-TX : 2
 Capability-Msg-RX : 2 Error-Msg-TX : 0 Error-Msg-RX : 0 Preempt-
Msg-TX : 0 Preempt-Msg-RX : 0 Preempt-Ack-Msg-TX: 0 Preempt-Ack-Msg-
RX: 0 Primary-Msg-TX : 1 Primary-Msg-RX : 1 Primary-Ack-Msg-TX : 1
 Primary-Ack-Msg-RX : 1 Hello-Msg-TX : 13402 Hello-Msg-RX : 13402
 Hello-Timeouts : 0 Hello-Failures : 0 MasterKey-Msg-TX: 1 MasterKey-
Msg-RX: 1 MasterKey-Ack-Msg-TX: 1 MasterKey-Ack-Msg-RX: 1 Connection-
Failures : 0 Connection-Tries-Failures : 12 Connection-Listener-
Tries : 1 Connection-Active-Tries : 12 Ping-TX : 53614 Ping-Fail-TX :
 0 Ping-0 Ping-RX :: 53613 Ping-Timeouts : 0 Ping-Failures : 0 Ping-
Error-Msgs : 0 Ping-Other-Msgs : 0 Ping-Last-Rsp : 1
```


Nivel de privilegio requerido

superuser, deviceadmin

show high-availability state

Description (Descripción)

Muestra información acerca del estado de alta disponibilidad (high-availability, HA) del clúster de dispositivos WildFire en los nodos controladores locales y del clúster de peers. Esto incluye si el nodo controlador está en estado activo (principal) o pasivo (copia de seguridad), y durante cuánto tiempo ha estado el nodo controlador en ese estado; la configuración de HA; si las configuraciones del nodo controlador local y de peer están sincronizadas; la compatibilidad de las actualizaciones de software y contenido, y la versión de antivirus entre los peers del nodo controlador.

Jerarquía de localización

```
show high-availability
```

Sintaxis

```
state;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
admin@thing1(active-controller)> show high-availability state
 High-Availability: Local Information: Versión: 1 State: active-
controller (last 1 days) Device Information: Management IPv4 Address:
 10.10.10.14/24 Management IPv6 Address: HA1 Control Links Joint
 Configuration: Encryption Enabled: no Election Option Information:
 Priority: primary Preemptive: no Version Compatibility: Software
 Version: Match Application Content Compatibility: Match Anti-
Virus Compatibility: Match Peer Information: Connection status:
 up Version: 1 State: passive-controller (last 1 days) Device
 Information: Management IPv4 Address: 10.10.10.30/24 Management
 IPv6 Address: Connection up; Primary HA1 link Election Option
 Information: Priority: secondary Preemptive: no Configuration
 Synchronization: Enabled: yes Running Configuration: synchronized
```

Nivel de privilegio requerido

superuser, deviceadmin

show high-availability transitions

Description (Descripción)

Muestra información de transición de alta disponibilidad (high-availability, HA) para clústeres de dispositivos WildFire sobre eventos que se producen durante los cambios de HA de los nodos del controlador de clústeres.

Jerarquía de localización

```
show high-availability
```

Sintaxis

```
transitions;
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

```
admin@thing1(active-controller)> show high-availability transitions
 High-Availability: Estadísticas de transición: Unknown : 1
 Suspended : 0 Initial : 0 Non-Functional : 0 Passive : 0 Active : 3
```

Nivel de privilegio requerido

superuser, deviceadmin

show system raid

Description (Descripción)

Muestra la configuración RAID del dispositivo WildFire. El dispositivo WF-500 se entrega con cuatro unidades en los cuatro primeros conectores de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Jerarquía de localización

```
show system
```

Sintaxis

```
raid { detail; {
```


Opciones

No hay opciones adicionales.

Ejemplo de configuración

A continuación se muestra la configuración de RAID en un dispositivo WF-500 en funcionamiento.

```
admin@WF-500> show system raid detail Disk Pair A Available Status
 clean Disk id A1 Present model : ST91000640NS size : 953869
 MB partition_1 : active sync partition_2 : active sync Disk id
 A2 Present model : ST91000640NS size : 953869 MB partition_1 :
 active sync partition_2 : active sync Disk Pair B Available Status
 clean Disk id B1 Present model : ST91000640NS size : 953869 MB
 partition_1 : active sync partition_2 : active sync Disk id B2
 Present model : ST91000640NS size : 953869 MB partition_1 : active
 sync partition_2 : active sync
```

Nivel de privilegio requerido

superuser, superreader

submit wildfire local-verdict-change

Description (Descripción)

Cambia los veredictos de WildFire generados localmente para las muestras que se envían desde el cortafuegos. Los cambios de veredicto solo aplican a las muestras enviadas al dispositivo WildFire, y el veredicto para la misma muestra permanece sin cambios en la nube pública de WildFire. Puede ver las muestras con veredictos cambiados utilizando el comando show wildfire global.

El paquete de contenido de la nube privada de WildFire se actualiza para reflejar los cambios de veredicto que realiza (en el cortafuegos, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** > **WF-Private** para habilitar las actualizaciones de contenido de la nube privada de WildFire). Cuando cambia el veredicto de una muestra a malintencionado, el dispositivo WildFire genera una nueva firma para detectar el malware y añade esa firma al paquete de contenido de la nube privada de WildFire. Cuando cambia el veredicto de una muestra a benigno, el dispositivo WildFire retira la firma del paquete de contenido de la nube privada de WildFire.

Además, existe una llamada de API que se puede utilizar para cambiar los veredictos de las muestras locales. Consulte la referencia de API de WildFire para obtener más información.

Jerarquía de localización

```
submit wildfire
```

Sintaxis

```
submit { wildfire { local-verdict-change { hash <value>; verdict
 <value>; comment <value>; } }
```


Opciones

* `hash`: especifique el hash SHA-256 del archivo al que desea cambiar el veredicto.

* `verdict`: introduzca el nuevo veredicto del archivo: 0 indica una muestra benigna; 1 indica malware; 2 indica grayware.

* `comment`: incluya un comentario para describir el cambio de veredicto.

Ejemplo de configuración

A continuación se muestra el resultado de este comando.

```
admin@WF-500> submit wildfire local-verdict-change comment test hash
 c323891a87a8c43780b0f2377de2efc8bf856f02dd6b9e46e97f4a9652814b5c
 verdict 2 Please enter 'Y' to commit: (y or n) verdict is changed
 (old verdict: 1, new verdict:2)
```

Nivel de privilegio requerido

superuser, deviceadmin

show wildfire

Description (Descripción)

Muestra información variada sobre el dispositivo WildFire, como el dispositivo global y local, y detalles relacionados con la muestra, el estado del dispositivo y la máquina virtual seleccionada para realizar el análisis.

Jerarquía de localización

```
show wildfire
```

Sintaxis

```
status | vm-images | wf-vm-pe-utilization | wf-vm-doc-utilization
 | wf-vm-email-link-utilization | wf-vm-archive-utilization | wf-
sample-queue-status }
```

Opciones

`> status`: muestra el estado del dispositivo y la información de configuración, como la máquina virtual (VM) utilizada para el análisis de muestras, si se van a enviar las muestras o los informes a la nube, la red de VM y la información de registro.

`> vm-images`: muestra los atributos de las imágenes de la máquina virtual disponibles utilizadas para el análisis de muestras. Para ver la imagen activa actual, ejecute el siguiente comando:

```
admin@WF-500> show wildfire status
```


and view the `VM field`.

`> wf-sample-queue-status`: muestra el número y el desglose de las muestras de dispositivos WildFire que están a la espera de analizarse.

`> wf-vm-doc-utilization`: muestra el número de entornos de análisis utilizados para procesar archivos de documentos disponibles y en uso.

`> wf-vm-elinkda-utilization`: muestra el número de entornos de análisis utilizados para procesar enlaces de correo electrónico disponibles y en uso.

`> wf-vm-pe-utilization`: muestra el número entornos de análisis utilizados para procesar archivos portable ejecutable disponibles y en uso.

Ejemplo de configuración

A continuación se muestra el resultado de este comando.

```
admin@WF-500> show wildfire status Connection info: Wildfire
 cloud: s1.wildfire.paloaltonetworks.com Status: Idle Submit
 sample: disabled Submit report: disabled Selected VM: vm-5 VM
 internet connection: disabled VM network using Tor: disabled Best
 server:                    s1.wildfire.paloaltonetworks.com Device
 registered: yes Service route IP address: 10.3.4.99 Signature
 verification: enable Server selection: enable Through a proxy: no
 admin@WF-500> show wildfire vm-images Supported VM images: vm-1
 Windows XP, Adobe Reader 9.3.3, Flash 9, Office 2003. Support PE,
 PDF, Office 2003 and earlier vm-2 Windows XP, Adobe Reader 9.4.0,
 Flash 10n, Office 2007. Support PE, PDF, Office 2007 and earlier
 vm-3 Windows XP, Adobe Reader 11, Flash 11, Office 2010. Support PE,
 PDF, Office 2010 and earlier vm-4 Windows 7 32bit, Adobe Reader 11,
 Flash 11, Office 2010. Support PE, PDF, Office 2010 and earlier vm-5
 Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010. Support
 PE, PDF, Office 2010 and earlier vm-6 Windows XP, Internet Explorer
 8, Flash 11. Support E-MAIL Links admin@WF-500> show wildfire wf-
sample-queue-status DW-ARCHIVE: 4, DW-DOC: 2, DW-ELINK: 0, DW-PE:
 21, DW-URL_UPLOAD_FILE: 2, admin@WF-500> show wildfire wf-vm-pe-
utilization { available: 2, in_use: 1, }
```

Nivel de privilegio requerido

superuser, superreader

show wildfire global

Description (Descripción)

Muestra información variada sobre los dispositivos globales y el estado de las muestras, como las claves de API disponibles, la información de registro, los cambios en el veredicto de las muestras, el origen del dispositivo de muestras, la actividad y las muestras recientes que analizó el dispositivo.

Jerarquía de localización

```
show wildfire global
```

Sintaxis

```
api-keys { all { details; } key <value>; } devices-reporting-data;
 last-device-registration { all; } local-verdict-change { all; sha256
 <value>; } } sample-analysis { number; type; } } sample-device-
lookup { sha256 { equal <value>; } sample-status { sha256 { equal
 <value>; } } signature-status { sha256 { equal <value>; } }
```

Opciones

`> api-keys`: se muestran los detalles de las claves de API generadas en el dispositivo WildFire. Puede ver la última vez que se ha utilizado la clave, el nombre de la clave, el estado (habilitada o deshabilitada) y la fecha y la hora de generación de la clave.

`> devices-reporting-data`: se muestra una lista de las últimas actividades de registro.

`> last-device-registration`: Se muestra una lista de las últimas actividades de registro.

`> local-verdict-change`: se muestran las muestras con veredictos cambiados.

`> sample-analysis`: se muestran los resultados de los análisis de WildFire hasta un máximo de 1000 muestras.

`> sample-status`: muestra el estado de la muestra de WildFire. Introduzca el valor SHA256 del archivo para ver el estado del análisis actual.

`> sample-device-lookup`: muestra el cortafuegos que envió la muestra SHA256 especificada.

`> signature-status`: se muestra el estado de la firma de WildFire. Introduzca el valor SHA256 del archivo para ver el estado del análisis actual.

Ejemplo de configuración

A continuación se muestra el resultado de este comando.

```
admin@WF-500> show wildfire global api-keys all +------------
+-----------+---------+---------------------+---------------------
+ | Apikey | Name | Status | Create Time | Last Used Time |
 +------------+-----------+---------+--------------------
+---------------------+ | <API KEY> | happykey1 | Enabled |
 2017-03-01 23:21:02 | 2017-03-01 23:21:02 | +------------
+-----------+---------+---------------------+---------------------
+ admin@WF-500> show wildfire global devices-reporting-data
 +--------------+---------------------+-------------+------------
+----------+--------+ | _Device ID | Last Registered | Device IP | SW
 Version | HW Model | Status | +--------------+--------------------
+-------------+------------+----------+--------+ | 000000000000
 | 2017-03-01 22:28:25 | 10.1.1.1 | 8.1.4 | PA-220 | OK |
 +--------------+---------------------+-------------+------------
+----------+--------+ admin@WF-500> show wildfire global last-
```



```
device-registration all +--------------+--------------------
+-------------+-----------+---------+--------+ | Device
 ID | Last Registered | Device IP | SW Version | HW Model |
 Status | +--------------+--------------------+-------------
+-----------+----------+--------+ | 000000000000 | 2017-07-31
 12:35:53 | 10.1.1.1 | 8.1.4 | PA-220 | OK | +--------------
+--------------------+------------+-----------+----------
+--------+ admin@WF-500> show wildfire global local-verdict-change
 +-------------------------------------------------------------------
+---------+--------+ | SHA256 | Verdict | Source |
 +-----------------------------------------------------------------
+---------+--------+ |
 c883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496| 2
 -> 1 | Yes |
 +-------------------------------------------------------------------
+---------+--------+ admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples +--------------
+--------------------+--------------------+-----------+ |
 SHA256 | Finish Date | Create Date | Malicious | +--------------
+--------------------+--------------------+-----------+ |
 <HASH VALUE> | 2017-03-01 23:27:57 | 2017-03-01 23:27:57 | Yes
 | +--------------+--------------------+-------------------
+-----------+ +--------------------+----------------
+---------------+---------------+ | Storage Nodes | Analysis Nodes
 | Status | File Type | +---------------------+----------------
+---------------+---------------+ | 00926ld1_2,0094:d1_2 |
 qa16 | Notify Finish | Elink File | +----------------------
+----------------+---------------+----------------+ Last Created
 100 Non-malicious Samples +--------------+--------------------
+---------------------+-----------+ | SHA256 | Finish Date |
 Create Date | Malicious | +--------------+--------------------
+---------------------+-----------+ | <HASH VALUE> | 2017-03-01
 23:31:15 | 2017-03-01 23:24:29 | No | +--------------
+---------------------+--------------------+-----------+
 +----------------------+----------------+--------------
+--------------------+ | Storage Nodes | Analysis Nodes |
 Status | File Type | +---------------------+----------------
+---------------+-------------------+ | 0712:smp_27,94:smp_7 |
 qa16 | Notify Finish | MS Office document | +----------------------
+----------------+--------------+-------------------+
 admin@WF-500> show wildfire global sample-device-lookup sha256 equal
 d75f2f71829153775fa33cf2fa95fd377f153551aadf0a642704595100efd460
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-----------------------------------------------------------------
+-----------+-----------+--------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +------------------------------------------------------------------
+-----------+-----------+--------------------+
 admin@WF-500> show wildfire global sample-status sha256 equal
 dc9f3a2a053c825e7619581f3b31d53296fe41658b924381b60aee3eeea4c088
```



```
 +---------------------+---------------------+----------
+---------------------------+ | Finish Date | Create
 Date | Malicious | Storage Nodes | +--------------------
+---------------------+----------+---------------------------
+ | 2017-03-01 22:34:17 | 2017-03-01 22:28:23 | No |
 009026:smp_27,097010smp_27 | +--------------------
+---------------------+----------+---------------------------+
 +----------------+--------------+-----------------+ | Analysis
 Nodes | Status | File Type | +----------------+--------------
+------------------+ | qa15 | Notify Finish | Adobe Flash
 File | +----------------+--------------+-----------------
+ admin@WF-500> show wildfire global signature-status sha256
 equalc883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496
 Signature Name Virus/Win32.WPCGeneric.cr Current Status: released
 Release History: +--------------+--------------------+---------
+-------------+----------+ | Build Version | Timestamp | UTID |
 Internal ID | Status | +---------------+--------------------
+---------+-------------+----------+ | 155392 | 2017-02-03 10:11:06 |
 5000259 | 10411 | released | +---------------+---------------------
+---------+-------------+----------+
```

Nivel de privilegio requerido

superuser, superreader

show wildfire local

Description (Descripción)

Muestra información variada sobre los dispositivos locales y las muestras, la actividad y las muestras recientes que el dispositivo analizó, además de las estadísticas básicas de WildFire.

Jerarquía de localización

```
show wildfire local
```

Sintaxis

```
latest { analysis { filter malicious|benign; sort-by SHA256|Submit
 Time|Start Time|Finish Time|Malicious|Status; sort-direction asc|
desc; limit 1-20000; days 1-7; } OR... samples { filter malicious|
benign; sort-by SHA256|Create Time|File Name|File Type|File Size|
Malicious|Status; sort-direction asc|desc; limit 1-20000; days
 1-7; } sample-processed { count 1-1000; time {last-1-hr|last-12-
hrs|last-15-minutes|last-24-hrs|last-30-days|last-7-days|last-
calender-day|last-calender-month; } sample-status { sha256 { equal
 <value>; } } statistics days <1-31> | hours <0-24> | minutes
 <0-60>; }
```


Opciones

`> latest`: Se muestran las últimas 30 actividades, lo que incluye las últimas 30 actividades de análisis, los últimos 30 archivos analizados, la información de sesión de red para los archivos analizados y los archivos cargados en el servidor de la nube pública.

`> sample-processed`: muestra el número de muestras procesadas localmente dentro de un intervalo de tiempo especificado o la cantidad máxima de muestras.

`> sample-status`: muestra el estado de la muestra de WildFire. Introduzca el valor SHA256 del archivo para ver el estado del análisis actual.

`> statistics`: Se muestran estadísticas de WildFire básicas.

Ejemplo de configuración

A continuación se muestra el resultado de este comando.

```
admin@WF-500> show wildfire latest analysis Latest
 analysis information: +-------------+--------------------
+---------------------+---------------------+ | SHA256 | Submit Time
 | Start Time | Finish Time | +-------------+--------------------
+---------------------+---------------------+ | <HASH VALUE>|
 2017-03-01 14:28:26 | 2017-03-01 14:28:26 | 2017-03-01 14:34:24 | |
 <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 | 2017-03-01
 14:28:41 | | <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25
 | 2017-03-01 14:28:26 | +-------------+--------------------
+---------------------+---------------------+ +------------
+-------------------------------------------------------------
+-----------+ | Malicious | VM Image | Status | +------------
+-------------------------------------------------------------
+-----------+ | Yes | Windows 7 x64 SP1, Adobe Reader
 11, Flash 11, Office 2010 | completed | | No | Java/
Jar Static Analyzer | completed | | Suspicious |
 Java/Jar Static Analyzer | completed | +------------
+-------------------------------------------------------------
+-----------+ admin@WF-500> show wildfire local latest samples
 Latest samples information: +--------------+--------------------
+----------------+--------------+ | SHA256 | Create Time |
 File Name | File Type | +--------------+--------------------
+----------------+--------------+ | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | PE | +--------------+--------------------
+----------------+--------------+ +--------------+-----------
+------------------+ | File Size | Malicious | Status |
 +--------------+-----------+-------------------+ | 20,407 |
 No | analysis complete | | 1,584 | Yes | analysis complete | |
 259,024 | No | analysis complete | +--------------+-----------
+------------------+ admin@WF-500> show wildfire local sample-
processed count 2 Time Window: last-15-minutes Display Count: 2:
 +-------------------------------------------------------------------
+--------------------+-----------+------------+-----------
+------------+------------------+ | SHA256 | Create Time
 | File Name | File Type | File Size | Malicious | Status |
 +-------------------------------------------------------------------
```



```
+---------------------+-----------+------------
+-----------+------------+-------------------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
 2018-12-09 16:55:53 | | Email Link | 31,522 | | download complete |
 | 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
 2018-12-09 16:53:40 | | Email Link | 39,679 | | download complete |
 +-------------------------------------------------------------------
+---------------------+-----------+------------
+-----------+------------+-------------------+
 admin@WF-500> show wildfire local sample-status sha256 equal
 0f2114010d00d7fa453177de93abca9643f4660457536114898c56149f819a9b
 Sample information: +---------------------+-----------
+-----------------------------------+ | Create Time | File
 Name | File Type | +---------------------+-----------
+-----------------------------------+ | 2017-03-01 22:28:24 |
 rmr.doc | Microsoft Word 97 - 2003 Document | +---------------------
+-----------+-----------------------------------+ +-----------
+-----------+-------------------+ | File Size | Malicious
 | Status | +-----------+-----------+-------------------+ |
 133120 | Yes | analysis complete | +-----------+-----------
+-------------------+ Analysis information: +---------------------
+---------------------+---------------------+------------+ | Submit
 Time | Start Time | Finish Time | Malicious | +---------------------
+---------------------+---------------------+------------+
 | 2017-03-01 22:28:24 | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | Suspicious | | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | 2017-03-01 22:34:07 | Yes | +---------------------
+---------------------+---------------------+------------+
 +-------------------------------------------------------------
+-----------+ | VM Image | Status |
 +-------------------------------------------------------------
+-----------+ | DOC/CDF Static Analyzer | completed | | Windows
 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010 | completed
 | +-------------------------------------------------------------
+-----------+ admin@WF-500> show wildfire local statistics
 Current Time: 2017-03-01 17:44:31 Received After:
 2017-02-28 17:44:31 Received Before: 2017-03-01 17:44:31
 ---------------------------------------------------------------------------
 | Wildfire Stats |
 +---------------------------------------------------------------------------
+ |
+---------------------------------------------------------------------------
+| || Executable || |
+---------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+---------------------------------------------------------------------------
+| || exe | 2 | 2 | 0 | 0 | 0 | 2 | 0 || |
+---------------------------------------------------------------------------
+| || dll | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------
+| Environment Analysis Summary for Executable:
 VM Utilization : 0/10 Files Analyzed : 2
 +---------------------------------------------------------------------------
+ || Non-Executable || |
+---------------------------------------------------------------------------
```



```
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-------------------------------------------------------------------------------
+| || pdf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || jar | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || doc | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || ppt | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || xls | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || docx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || pptx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || xlsx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || rtf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || class | 2 | 2 | 0 | 1 | 0 | 1 | 0 || |
+-------------------------------------------------------------------------------
+| || swf | 1 | 1 | 0 | 0 | 0 | 1 | 0 || |
+-------------------------------------------------------------------------------
+| Environment Analysis Summary for Non-Executable:
 VM Utilization : 0/16 Files Analyzed : 4
 +-------------------------------------------------------------------------------
+ || Links || |
+-------------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-------------------------------------------------------------------------------
+| || elink | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| Environment Analysis Summary for Links: Files Analyzed : 1
 ------------------------------------------------------- | General
 Stats | +-------------------------------------------------------
+ Total Disk Usage: 67/1283(GB) (5%) ||+-------------------------
+-----------+-+-----------+| ||| Sample Queue ||| ||
+-----------------+-----------------+--------------+| |||
 SUBMITTED | ANALYZED | PENDING ||| ||+-------------------------
+-----------+-+-----------+| ||| 7 | 7 | 0 ||| ||
+---------------------------+-----------+-+----------+||| |
+---------------------------+---------------------------+| |||
 Verdicts ||| ||+---------------------------+-------------------------
+|| ||| Malware | Grayware | Benign | Error ||| ||
+-------------------------------+-----------------------+|| ||| 3 | 0
 | 4 | 0 ||| ||+---------------------------+-----------+-+----------
+||| |+---------------------------+---------------------------+|
 ||| Session and Upload Count ||| ||+-------------------------
+-------------------------+|| ||| Sessions | Uploads ||| ||
+---------------------------+-------------------------+|| ||| 7 | 5
 ||| ||+---------------------------+-------------------------+||
```


Nivel de privilegio requerido

superuser, superreader

test wildfire registration

Description (Descripción)

Realiza una prueba para comprobar el estado de registro de un dispositivo WildFire o un cortafuegos de Palo Alto Networks en un servidor de WildFire. Si el resultado de la prueba es correcto, se muestra la dirección IP o el nombre del servidor de WildFire. Se requiere el registro correcto para que el dispositivo WildFire o el cortafuegos puedan reenviar archivos al servidor de WildFire.

Sintaxis

```
test { wildfire { registration; } }
```

Opciones

No hay opciones adicionales.

Ejemplo de configuración

A continuación se muestra el resultado correcto de un cortafuegos que puede comunicarse con un dispositivo WildFire. Si es un dispositivo WildFire que apunta a la nube de WildFire de Palo Alto Networks, el nombre del servidor de uno de los servidores de la Nube se muestra en el campo `select the best server:`.

```
Testing wildfire Public Cloud wildfire registration: successful
 download server list: successful select the best server: ca-
s1.wildfire.paloaltonetworks.com
```

Nivel de privilegio requerido

superuser, superreader

