paloalto TECHDOCS

Guía del administrador de Panorama

Version 10.2



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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

June 9, 2022

Table of Contents

Panorama Overview 11

Acerca de Panorama 12
Modelos Panorama 14
Gestión de la configuración y actualización de cortafuegos centralizada 17
Cambio de contexto: cortafuegos o Panorama 17
Tamaño de configuración total para Panorama 18
Plantillas y pilas de plantillas 19
Grupos de dispositivos 20
Creación centralizada de logs e informes 26
Recopiladores gestionados y grupos de recopiladores 26
Recopilación de logs locales y distribuidos 27
Advertencias para un grupo de recopiladores con recopiladores de logs múltiples 28
Opciones de reenvío de logs 30
Informes centralizados 32
Redistribución de datos mediante Panorama 34
Control de acceso basado en funciones 35
Funciones administrativas 35
Perfiles y secuencias de autenticación 37
Dominios de acceso 38
Autenticación administrativa 39
Operaciones de confirmación, validación y previsualización de Panorama 41
Planificación de su implementación de Panorama 43
Implementación de Panorama: Descripción general de tareas 46

Configuración de Panorama 47

Determinación de requisitos de almacenamiento de logs de Panorama 48
Gestión de implementaciones de cortafuegos a gran escala 50
Evaluación de la solución óptima para implementaciones de cortafuegos a gran escala 50
Aumento de la capacidad de gestión de dispositivos en los dispositivos M-Series y los dispositivos virtuales Panorama 50
Configuración del dispositivo virtual Panorama 54
Requisitos previos de configuración del dispositivo virtual Panorama 54
Instalación del dispositivo virtual Panorama 59
Realización de la configuración inicial del dispositivo virtual Panorama 127
Configuración del dispositivo virtual Panorama como un recopilador de logs 130

 ©2023 Palo Alto Networks, Inc.

Configuración del dispositivo virtual Panorama con recopiladores de logs locales....138
Configuración de un dispositivo virtual Panorama en modo Panorama....144
Configuración de un dispositivo virtual Panorama en modo solo de gestión....145
Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual Panorama....146
Aumento de CPU y memoria en el dispositivo virtual Panorama....176
Aumento del disco del sistema en el dispositivo virtual de Panorama....184
Realización de la configuración del dispositivo virtual Panorama....190
Cómo convertir su dispositivo virtual Panorama....190
Configuración del dispositivo de la serie M....204
Interfaces del dispositivo M-Series....204
Realización de la configuración inicial del dispositivo de la serie M....207
Descripción general de VM-Series....212
Configuración del dispositivo M-Series como un recopilador de logs....214
Aumento de la capacidad de almacenamiento en el dispositivo M-Series....223
Configuración de Panorama para usar varias interfaces....229
Registro de Panorama e instalación de licencias....238
Registro de Panorama....238
Activación de una licencia de asistencia técnica de Panorama....241
Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet....241
Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet....242
Activación/recuperación de una licencia de gestión de cortafuegos en el dispositivo de la serie M....245
Instalación del certificado de dispositivo de Panorama....247
Transición a un modelo diferente de Panorama....249
Migración de un dispositivo virtual Panorama a un dispositivo de la serie M....249
Migración de dispositivos virtuales Panorama a otro hipervisor....253
Migración de un dispositivo M-Series a un dispositivo virtual Panorama....258
Migración de un dispositivo M-100 a un dispositivo M-500....265
Migración de un dispositivo M-100 o M-500 a un dispositivo M-200 o M-600....268
Acceso y navegación en las interfaces de gestión de Panorama....273
Inicio de sesión en la interfaz web de Panorama....273
Navegación en la interfaz web de Panorama....274
Inicio de sesión en la CLI de Panorama....275
Configuración del acceso administrativo a Panorama....277
Configuración de un perfil de función de administrador....277

 ©2023 Palo Alto Networks, Inc.

Configuración de un perfil de función de administración para envío selectivo en cortafuegos gestionados....278
Configuración de un dominio de acceso....280
Configurar cuentas y autenticación administrativa....280
Configuración del seguimiento de la actividad del administrador....296
Configuración de la autenticación mediante certificados personalizados....299
¿Cómo se autentican mutuamente las conexiones SSL/TLS?....299
Configuración de la autenticación mediante la utilización de certificados personalizados en Panorama....300
Configuración de la autenticación mediante la utilización de certificados personalizados en dispositivos gestionado....303
Adición de nuevos dispositivos cliente....305
Cambio de certificados....305

Gestión de cortafuegos....309

Cómo añadir un cortafuegos como dispositivo gestionado....310
Instalación del certificado del dispositivo para cortafuegos gestionados....320
Instalación del certificado del dispositivo para un cortafuegos gestionado....320
Instalación del certificado del dispositivo para varios cortafuegos gestionados....323
Configuración de Zero Touch Provisioning....327
Descripción general de ZTP....327
Instalación del complemento de ZTP....329
Configuración de la cuenta de administrador del instalador de ZTP....337
Adición de cortafuegos de ZTP a Panorama....338
Uso de la CLI para tareas de ZTP....343
Desinstalación del complemento de ZTP....346
Gestión de grupos de dispositivos....348
Adición de un grupo de dispositivos....348
Creación de una jerarquía del grupo de dispositivos....349
Creación de objetos para su uso en una política compartida o de grupo de dispositivos....351
Volver a los valores de objeto heredados....353
Gestión de objetos compartidos no utilizados....354
Gestión de la precedencia de objetos heredados....355
Movimiento o duplicación de una regla de política u objeto a un grupo de dispositivos diferente....356
Ingreso de una regla de política a un subconjunto de cortafuegos....358
Envío de grupos de dispositivos a un cortafuegos de sistemas virtuales múltiples....360
Gestión de la jerarquía de reglas....362
Gestión de plantillas y pilas de plantillas....364

 ©2023 Palo Alto Networks, Inc.

Funciones y excepciones de las plantillas 364
Cómo añadir una plantilla 364
Configuración de una pila de plantillas 367
Configuración de una variable en una plantilla o una pila de plantillas 371
Importación y sobrescritura de variables de la pila de plantillas existentes 374
Cancelación de un valor de plantilla o pila de plantillas 376
Deshabilitación/eliminación de ajustes de plantilla 379
Gestión de la clave maestra en Panorama 380
Programación de un envío de configuración en cortafuegos gestionados 386
Redistribución de datos a cortafuegos gestionados 390
Transición de un cortafuegos a una gestión de Panorama 393
Planificación de la transición a la gestión de Panorama 393
Migración de un cortafuegos a la gestión de Panorama 395
Migración de un par HA del cortafuegos a la gestión de Panorama 399
Carga de una configuración de cortafuegos parcial en Panorama 405
Cómo localizar una configuración enviada de Panorama en un cortafuegos gestionado 407
Supervisión de dispositivos en Panorama 409
Supervisión del estado del dispositivo 409
Supervisión de la utilización de las reglas de la política 411
Caso de uso: Configuración de cortafuegos mediante Panorama 417
Grupos de dispositivos en este caso de uso 417
Plantillas en este caso de uso 418
Ajuste de políticas y configuración centralizadas 419

Gestión de la recopilación de logs 429

Configuración de recopiladores gestionados 430
Supervisión del estado del recopilador gestionado 437
Configuración de la autenticación para un recopilador de logs dedicado 438
Configuración de una cuenta administrativa para un recopilador de logs dedicado 438
Configuración de la autenticación RADIUS para un recopilador de logs dedicado 440
Configuración de la autenticación TACACS+ para un recopilador de logs dedicado 444
Configuración de la autenticación LDAP para un recopilador de logs dedicado 448
Gestión de grupos de recopiladores 453
Configuración de un grupo de recopiladores 453
Configuración de la autenticación con certificados personalizados entre recopiladores de logs 456

 ©2023 Palo Alto Networks, Inc.

Movimiento de un recopilador de logs a un grupo de recopiladores diferente....459
Eliminación de un cortafuegos de un grupo de recopiladores....461
Configuración del reenvío de logs a Panorama....462
Configuración del reenvío de syslog a destinos externos....467
Reenvío de logs a Cortex Data Lake....472
Comprobación del reenvío de logs a Panorama....473
Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs....475
Configuración del reenvío de logs desde Panorama a destinos externos....478
Implementaciones de recopilación de logs....481
Implementación de Panorama con recopiladores de logs dedicados....481
Implementación de dispositivos M-Series de Panorama con recopiladores de logs locales....490
Implementación de dispositivos virtuales Panorama con recopiladores de logs locales....498
Implementación de dispositivos virtuales Panorama en modo heredado con recopilación de logs local....504

Gestión de dispositivos WildFire....507

Agregue dispositivos independientes WildFire para gestionar con Panorama....508
Configure la configuración básica del dispositivo WildFire en Panorama....514
Configuración de la autenticación para un dispositivo WildFire....514
Configuración de la autenticación utilizando certificados personalizados en dispositivos y clústeres WildFire....528
Configuración de un certificado personalizado para un dispositivo WildFire gestionado de Panorama....528
Configuración de la autenticación con un certificado personalizado para un clúster WildFire....531
Aplicación de certificados personalizados en un dispositivo WildFire configurado en Panorama....533
Elimine un dispositivo WildFire de la gestión de Panorama....536
Gestión de clústeres Wildfire....537
Configuración de un clúster centralmente en Panorama....537
Visualización del estado del clúster WildFire con Panorama....564

Gestión de licencias y actualizaciones....567

Gestión de licencias en cortafuegos mediante Panorama....568

Supervisión de la actividad de red....571

Uso de Panorama para lograr visibilidad....572
Supervisión de la red con el ACC y Appscope....572
Análisis de datos de log....575

 ©2023 Palo Alto Networks, Inc.

Generación, programación y envío por correo electrónico de informes..... 575
Configuración de los límites de claves para informes programados.....579
Asimilación de logs de Traps ESM en Panorama.....582
Caso de uso: supervisión de aplicaciones mediante Panorama..... 584
Caso de uso: Respuesta a un incidente mediante Panorama..... 587
Notificación de incidentes.....587
Revisión de widgets en el ACC..... 588
Revisión de logs de amenaza..... 588
Revisión de logs de WildFire.....589
Revisión de logs de filtrado de datos..... 590
Actualización de reglas de seguridad..... 590

Alta disponibilidad de Panorama.....593

Requisitos previos de HA de Panorama..... 594
Prioridad y conmutación por error en Panorama en HA..... 596
Activadores de conmutación por error.....598
Sondeos de heartbeat y mensajes de saludo de HA..... 598
Supervisión de rutas de HA..... 598
Consideraciones sobre logs en HA de Panorama..... 600
Conmutación por error del logging en un dispositivo virtual Panorama en modo heredado.....600
Conmutación por error del logging en un dispositivo M-Series o dispositivo virtual Panorama en modo Panorama..... 601
Sincronización entre peers de HA de Panorama.....603
Gestión de un par de HA de Panorama..... 604
Configuración de HA en Panorama..... 604
Configurar la autenticación mediante certificados personalizados entre peers de HA.....607
Prueba de conmutación por error de HA de Panorama.....609
Cambio de prioridad tras una conmutación por error de Panorama para reanudar los logs en NFS..... 610
Restauración del Panorama principal al estado activo..... 611

Administración de Panorama.....613

Previsualización, validación o compilación de cambios de configuración..... 614
Compilación de cambios de configuración selectivos para dispositivos gestionados.....617
Envío de cambios de configuración selectivos a dispositivos gestionados..... 619
Habilitación de la recuperación de confirmación automatizada..... 622
Gestión de las copias de seguridad de configuración de Panorama y del cortafuegos.....624
Programación de la exportación de los archivos de configuración.....625

 ©2023 Palo Alto Networks, Inc.

Guardado y exportación de configuraciones de Panorama y de cortafuegos....626
Reversión de los cambios de configuración de Panorama....628
Configuración del número máximo de copias de seguridad de configuración en Panorama....632
Carga de una copia de seguridad de configuración en un cortafuegos gestionado....633
Comparación de cambios en configuraciones de Panorama....634
Gestión de bloqueos para restringir cambios de configuración....635
Adición de logotipos personalizados a Panorama....638
Uso del gestor de tareas de Panorama....639
Gestión de cuotas de almacenamiento y períodos de vencimiento de logs e informes....640
Almacenamiento de logs e informes....640
Períodos de vencimiento de logs e informes....641
Configuración de cuotas de almacenamiento y períodos de vencimiento de logs e informes....641
Configuración del tiempo de ejecución para los informes de Panorama....644
Supervisión de Panorama....645
Logs de sistema y de configuración de Panorama....645
Supervisión de estadísticas de Panorama y recopiladores de logs mediante SNMP....646
Reinicio o cierre de Panorama....650
Configuración de perfiles de contraseña y complejidad de contraseña de Panorama....651

Complementos de Panorama....653

Acerca de los complementos de Panorama....654
Instalación de los complementos de Panorama....656
Complemento VM-Series y complementos de Panorama....658
Instalación del complemento VM-Series en Panorama....658

Solución de problemas....661

Solución de problemas del sistema Panorama....662
Generación de archivos de diagnóstico para Panorama....662
Diagnóstico de estado suspendido de Panorama....662
Supervisión de la comprobación de integridad del sistema de archivos....662
Gestión de almacenamiento de Panorama para actualizaciones de software y contenido....663
Recuperación del síndrome de cerebro dividido en implementaciones HA de Panorama....664
Solución de problemas de almacenamiento de logs y conexión....666
Verificación de la utilización del puerto de Panorama....666

 ©2023 Palo Alto Networks, Inc.

Resolución de almacenamiento cero de logs para un grupo de recopiladores....669
Sustitución de un disco con fallos en un dispositivo de la serie M....670
Sustitución del disco virtual en un servidor ESXi....670
Sustitución del disco virtual en vCloud Air....671
Migración de logs a un nuevo dispositivo serie M en modo de recopilación de logs....672
Migración de logs a un nuevo dispositivo de la serie M en modo Panorama....679
Migración de logs a un nuevo modelo de dispositivo serie M en modo Panorama con alta disponibilidad....687
Migración de logs al mismo modelo de dispositivo serie M en modo Panorama con alta disponibilidad....696
Migración de recopiladores de logs después de un error o RMA de un Panorama que no es de HA....706
Regeneración de metadatos para pares de RAID para un dispositivo serie M....710
Visualización de trabajos de consulta de logs....711
Sustitución de un cortafuegos con una autorización de devolución de mercancía....713
Generación de estado de dispositivo parcial para cortafuegos....713
Antes de iniciar una sustitución de un cortafuegos con RMA....714
Restablecimiento de la configuración del cortafuegos tras su sustitución....715
Solución de problemas de fallos de compilación....721
Solución de problemas de errores de registro o números de serie....722
Solución de problemas de errores de creación de informes....723
Solución de problemas de errores de licencia de gestión de dispositivos....724
Solución de problemas de las configuraciones del cortafuegos revertidas automáticamente....725
Visualización de tareas que se realizaron correctamente o tienen errores....727
Pruebas de coincidencia con políticas y conectividad de dispositivos gestionados....728
Solución de problemas de coincidencias del tráfico con las reglas de políticas....728
Solución de problemas de conectividad a recursos de red....729
Cómo generar un archivo de volcado de estadísticas para un cortafuegos gestionado....731
Cómo recuperar la conectividad a Panorama en dispositivos gestionados....733

 ©2023 Palo Alto Networks, Inc.

Panorama Overview

El servidor de gestión de Panorama™ proporciona supervisión y gestión centralizadas de múltiples cortafuegos de última generación de Palo Alto Networks, y de dispositivos y clústeres de dispositivos de WildFire. Proporciona una ubicación única desde la que puede supervisar todas las aplicaciones, usuarios y contenidos que atraviesan la red, y emplear esta información para crear políticas de activación de aplicaciones que protejan y controlen toda la red. Si se usa Panorama para gestionar de forma centralizada las políticas y cortafuegos, es posible aumentar la eficiencia operativa a la hora de gestionar y mantener una red distribuida de cortafuegos. La utilización de Panorama para la gestión centralizada del dispositivo WildFire y el Clúster de dispositivos WildFire aumenta el número de cortafuegos que admite una única red, proporciona alta disponibilidad para la tolerancia a fallos y aumenta la eficiencia de la administración.

- Acerca de Panorama
- Modelos Panorama
- Gestión de la configuración y actualización de cortafuegos centralizada
- Creación centralizada de logs e informes
- Redistribución de datos mediante Panorama
- Control de acceso basado en funciones
- Operaciones de confirmación, validación y previsualización de Panorama
- Planificación de su implementación de Panorama
- Implementación de Panorama: Descripción general de tareas

Acerca de Panorama

Panorama le permite configurar, gestionar y supervisar de forma efectiva sus cortafuegos de Palo Alto Networks mediante una supervisión central. Los tres puntos fundamentales en los que Panorama añade valor son:

- **Configuración e implementación centralizadas**: puede simplificar la gestión central e implementar rápidamente los cortafuegos y los dispositivos WildFire de su red si utiliza Panorama para las fases previas a la implementación de los cortafuegos y los dispositivos WildFire. A continuación, puede reunir los cortafuegos en grupos y crear plantillas para aplicar una configuración de dispositivos y red base, y usar grupos de dispositivos para administrar globalmente reglas de políticas locales y compartidas. Consulte Gestión de la configuración y actualización de cortafuegos centralizada.
- **Logs agregados con perspectiva central para análisis e informes**: recopile información de actividades en los cortafuegos gestionados de la red y analice, investigue y cree informes de forma centralizada sobre los datos. Esta exhaustiva vista del tráfico de la red, la actividad del usuario y los riesgos asociados le permiten responder a posibles amenazas usando la rica gama de políticas para activar de forma segura las aplicaciones de su red. Consulte Creación centralizada de logs e informes.
- **Administración distribuida**: le permite delegar o restringir el acceso a políticas y configuraciones de cortafuegos globales y locales. Consulte Control de acceso basado en funciones para saber cómo delegar los niveles apropiados de acceso para la administración distribuida.

Hay seis modelos de Panorama disponibles: el dispositivo virtual Panorama y los dispositivos M-600, M-500 y M-200 son compatibles con PAN-OS 10.0. El dispositivo M-300 y el dispositivo M-700 son compatibles con PAN-OS 10.2.Gestión centralizada de Panorama ilustra cómo puede implementar Panorama en una configuración de alta disponibilidad (HA) para gestionar cortafuegos.

 ©2023 Palo Alto Networks, Inc.

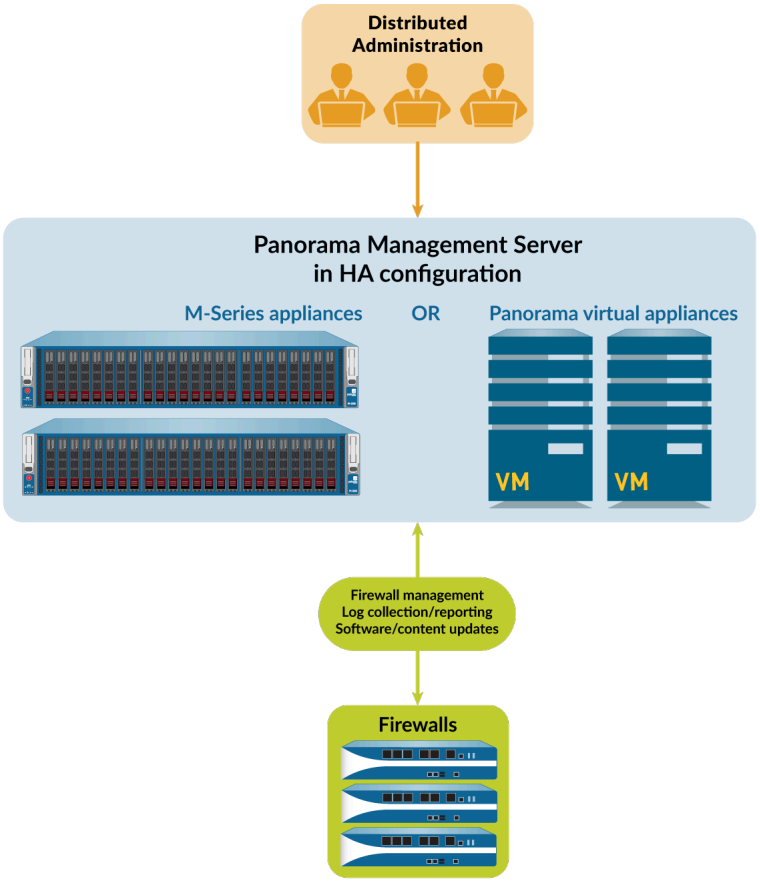


Figure 1: Gestión centralizada de Panorama

©2023 Palo Alto Networks, Inc.

Modelos Panorama

Panorama está disponible como dispositivo físico o virtual. Cada uno admite licencias para gestionar 25, 100 o 1000 cortafuegos. Además, los dispositivos M-600 y M-700 admiten licencias para administrar hasta 5000 cortafuegos y los dispositivos virtuales Panorama con recursos similares admiten licencias para administrar hasta 2500 cortafuegos:

- **Dispositivo virtual Panorama**: este modelo permite una instalación sencilla y facilita la consolidación del servidor para los sitios que necesitan un dispositivo de gestión virtual. Puede instalar Panorama en Alibaba Cloud, Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), KVM, Hyper-V, Oracle Cloud Infrastructure (OCI), un servidor VMware ESXi o VMware vCloud Air. El dispositivo virtual puede recopilar logs de cortafuegos localmente a velocidades de hasta 20.000 logs por segundo y puede gestionar recopiladores de logs dedicados para obtener mayores tasas de creación de logs. El dispositivo virtual puede funcionar como un servidor de gestión dedicado, un servidor de gestión de Panorama con capacidades de recopilación de logs locales o como un recopilador de logs dedicado. Para obtener información sobre las interfaces compatibles, la capacidad de almacenamiento de logs y las tasas máximas de recopilación de logs, consulte Requisitos previos de configuración del dispositivo virtual Panorama. Puede implementar el dispositivo virtual en los siguientes modos:
  - **Modo Panorama**: en este modo, el dispositivo virtual Panorama admite un recopilador de logs local con 1 a 12 discos virtuales de logging (consulte Implementar dispositivos virtuales Panorama con recopiladores de logs locales) Cada disco de logging tiene 2 TB de capacidad de almacenamiento para un máximo total de 24 TB en un único dispositivo virtual y 48 TB en un par de alta disponibilidad (HA). Solo el modo Panorama le permite añadir múltiples discos virtuales de logging sin perder logs en los discos existentes. El modo Panorama también proporciona el beneficio de una generación de informes más rápida. En el modo Panorama, el dispositivo virtual no es compatible con el almacenamiento NFS.

    Se recomienda implementar el dispositivo virtual en modo Panorama para optimizar el almacenamiento de logs y la generación de informes.
  - **Modo heredado** (solo ESXi y vCloud Air): en este modo, el dispositivo virtual Panorama recibe y almacena logs de cortafuegos sin utilizar un recopilador de logs local (consulte Implementación de dispositivos virtuales Panorama en modo heredado con recopilación de logs local). De manera predeterminada, el dispositivo virtual en modo heredado tiene una partición de disco para todos los datos. Aproximadamente 11 GB de la partición se asignan al almacenamiento de logs. Si necesita más almacenamiento local para los logs, puede añadir un disco virtual de hasta 8 TB en ESXi 5.5 o versiones posteriores. Las versiones anteriores de ESXi admiten un disco de hasta 2 TB. Si necesita más de 8 TB, puede montar el dispositivo virtual en modo heredado en un almacén de datos NFS pero solo en el servidor ESXi, no en vCloud Air. Este modo solo está disponible si el dispositivo virtual Panorama está en modo heredado durante la actualización a PAN-OS 10.0. En la actualización a PAN-OS 9.0 y versiones posteriores, el modo Legacy (Heredado) ya no estará disponible si cambia a cualquier

 ©2023 Palo Alto Networks, Inc.

otro modo. Si cambia el modo del dispositivo virtual Panorama del modo heredado a uno de los modos disponibles, ya no podrá regresar al modo heredado.

> ***Aunque es compatible, el modo Legacy (Heredado) no es recomendable para entornos de producción, pero aún se puede usar en entornos de laboratorio o de demostración.***

- **Modo solo de gestión:** en este modo, el dispositivo virtual Panorama es un dispositivo de gestión dedicado para sus dispositivos gestionados y recopiladores de logs dedicados. Además, los dispositivos virtuales Panorama con recursos adecuados también pueden gestionar hasta 2500 cortafuegos en este modo. El dispositivo virtual Panorama no cuenta con capacidades de recopilación de logs, a excepción de los logs de configuración y sistema, y requiere un recopilador de logs dedicado para almacenar esos logs. De manera predeterminada, el dispositivo virtual en el modo Management Only (Solo gestión) tiene solo una partición de disco para todos los datos, por lo que todos los logs reenviados a un dispositivo virtual Panorama en ese modo se descartarán. Por lo tanto, para almacenar los datos de logs de sus dispositivos gestionados, debe configurar el reenvío de logs para almacenar los datos de logs de sus dispositivos gestionados. Para obtener más información, consulte Requisitos para aumentar la capacidad de gestión de dispositivos.
- **Modo de recopilación de logs**: el dispositivo virtual Panorama funciona como un recopilador de logs dedicado. Si varios cortafuegos reenvían grandes volúmenes de datos de logs, un dispositivo virtual Panorama en modo de recopilación de logs proporciona una escala y un rendimiento mayor. En este modo, el dispositivo no posee una interfaz web para el acceso administrativo, solo una interfaz de línea de comandos (Command Line Interface, CLI). Sin embargo, puede gestionar el dispositivo utilizando la interfaz web del servidor de gestión de Panorama. El acceso a la CLI de un dispositivo virtual Panorama en modo de recopilación de logs solo es necesario para la configuración inicial y la depuración. Para obtener más información sobre la configuración, consulte Implementación de Panorama con recopiladores de logs dedicados.

- **Dispositivo M-Series**: M-200, M-300, M-500 y M-600 son dispositivos de hardware dedicados que están diseñados para las implementaciones a gran escala. En entornos con elevados requisitos de conservación de logs y tasas de logs altas (más de 10 000 logs por segundo), estos dispositivos permiten ampliar su infraestructura de recopilación de logs. Para obtener información sobre las interfaces compatibles, la capacidad de almacenamiento de logs y las tasas máximas de recopilación de logs, consulte Interfaces del dispositivo M-Series. Todos los modelos serie M comparten los siguientes atributos:
  - Unidades RAID para almacenar logs de cortafuegos y replicación de RAID 1 para protegerse contra los fallos de disco.
  - SSD para almacenar los logs que Panorama y los recopiladores de logs generan.
  - Interfaces MGT, Eth1, Eth2 y Eth3 que admiten un rendimiento de 1 Gbps
  - Fuentes de alimentación redundantes e intercambiables en caliente

 ©2023 Palo Alto Networks, Inc.

- Flujo de aire de adelante hacia atrás

Los dispositivos M-500 y M-600 tienen los siguientes atributos adicionales, que los hacen más adecuados para centros de datos:

- Interfaces Eth4 y Eth5 que admiten un rendimiento de 10 Gbps

Además, el siguiente atributo hace que los dispositivos M-600 y M-700 sean más adecuados para implementaciones de cortafuegos a gran escala:

- Los dispositivos M-600 y M-700 en el modo de solo gestión puede gestionar hasta 5000 cortafuegos.

Puede implementar los dispositivos M-Series en los siguientes modos:

- **Modo Panorama**: El dispositivo funciona como un servidor de gestión de Panorama para gestionar cortafuegos y recopiladores de logs dedicados. El dispositivo también admite un recopilador de logs local para añadir logs de cortafuegos. El modo Panorama es el modo predeterminado. Para obtener más información sobre la configuración, consulte Implementación de dispositivos M-Series de Panorama con recopiladores de logs locales.
- **Modo solo de gestión:** el dispositivo Panorama es un dispositivo de gestión dedicado para sus dispositivos gestionados y recopiladores de logs dedicados. El dispositivo Panorama no cuenta con capacidades de recopilación de logs, a excepción de los logs de configuración y sistema, y su implementación requiere un recopilador de logs dedicado para almacenar esos logs. De manera predeterminada, el dispositivo Panorama en el modo Management Only (Solo gestión) tiene solo una partición de disco para todos los datos, por lo que todos los logs reenviados a un dispositivo virtual Panorama en ese modo se descartarán. Por lo tanto, para almacenar los datos de logs de sus dispositivos gestionados, debe configurar el reenvío de logs para almacenar los datos de logs de sus dispositivos gestionados.
- **Modo de recopilación de logs**: el dispositivo funciona como un recopilador de logs dedicado. Si varios cortafuegos reenvían grandes volúmenes de datos de logs, un dispositivo M-Series en el modo de recopilación de logs proporciona una escala y un rendimiento mayor. En este modo, el dispositivo no posee una interfaz web para el acceso administrativo, solo una interfaz de línea de comandos (Command Line Interface, CLI). Sin embargo, puede gestionar el dispositivo utilizando la interfaz web del servidor de gestión de Panorama. El acceso a la CLI de un dispositivo de la serie M en el modo de recopilación de logs solamente es necesario para la configuración inicial y la depuración. Para obtener más información sobre la configuración, consulte Implementación de Panorama con recopiladores de logs dedicados.

Para obtener más detalles y especificaciones de los dispositivos serie M, consulte las Guías de referencia de hardware de dispositivos serie M.

 ©2023 Palo Alto Networks, Inc.

Gestión de la configuración y actualización de cortafuegos centralizada

Panorama™ usa ***grupos de dispositivos*** y ***plantillas*** para agrupar cortafuegos en conjuntos lógicos que requieren una configuración similar. Utilice grupos de dispositivos y plantillas para gestionar de manera centralizada todos los elementos de configuración, las políticas y los objetos de los cortafuegos gestionados. Panorama también le permite gestionar centralmente las actualizaciones de licencias, software (software PAN-OS®, software de cliente SSL-VPN, software de agente/aplicación GlobalProtect™) y contenido (aplicaciones, amenazas, WildFire® y antivirus). Todos los objetos de configuración de grupos de dispositivos, plantillas y pilas de plantillas deben tener un nombre único.

En caso de que se produzca un reinicio imprevisto del cortafuegos gestionado o Panorama, todos los cambios de configuración no confirmados en los grupos de dispositivos y plantillas se conservan de forma local hasta que confirme correctamente los cambios. Un reinicio puede ser el reinicio del cortafuegos o Panorama o de un proceso de administración de PAN-OS relacionado con la gestión de la configuración. Para los cortafuegos o Panorama en una configuración de alta disponibilidad (HA), los cambios de configuración no confirmados no se sincronizan automáticamente entre los peers de HA en caso de un reinicio imprevisto.

- Cambio de contexto: cortafuegos o Panorama
- Tamaño de configuración total para Panorama
- Plantillas y pilas de plantillas
- Grupos de dispositivos

Cambio de contexto: cortafuegos o Panorama

La interfaz web de Panorama™ le permite alternar entre una vista centrada en Panorama y una vista centrada en los cortafuegos mediante el menú desplegable **Context (Contexto)** en la parte superior izquierda de cada pestaña. Configure el **Context (Contexto)** en **Panorama** para gestionar los cortafuegos de forma centralizada o cambiar el contexto a la interfaz web de un cortafuegos específico para configurarlo de manera local. La similitud de las interfaces web del cortafuegos y Panorama le permite cambiar sin problemas entre ellos para supervisar y gestionar los cortafuegos.

El menú desplegable **Context (Contexto)** solo detalla los cortafuegos que están conectados a Panorama. Para el administrador de grupos de dispositivos y plantillas, el menú desplegable detalla solo los cortafuegos conectados que están dentro de los dominios de acceso asignados a ese administrador. Para buscar una lista larga, use los filtros del menú desplegable.

Para los cortafuegos con una configuración de alta disponibilidad (high availability, HA), los iconos tienen fondos de color para indicar el estado de HA (de la siguiente manera). Conocer el estado de HA resulta útil al seleccionar el contexto de un cortafuegos. Por ejemplo, generalmente realizará cambios de configuración específicos para el cortafuegos en un cortafuegos activo.

- **Verde:** activo.
- **Amarillo:** pasivo o iniciándose (el estado de inicio puede durar hasta 60 segundos desde el arranque).

©2023 Palo Alto Networks, Inc.

- **Rojo:** el cortafuegos no está operativo (estado de error), está suspendido (deshabilitado por un administrador) o provisional (para un evento de supervisión de enlace o ruta en una configuración de HA activo/activo).

Cuando configura un perfil de función de administrador para un administrador de grupo de dispositivos y plantilla, debe asignar una **función de administrador de dispositivos** que se envía a los cortafuegos gestionados para cambiar el contexto entre la interfaz web el cortafuegos y Panorama.

Durante el cambio de contexto, Panorama valida si el administrador tiene acceso a un vsys específico o a todos los vsys. Si el administrador tiene acceso a todos los vsys, Panorama utiliza el modificador de contexto de la función de administrador del dispositivo. Si el administrador tiene acceso a uno o algunos de los vsys, Panorama usa la función de administrador de vsys para cambiar de contexto.

Tamaño de configuración total para Panorama

El tamaño total del archivo de configuración de Panorama™ M-Series y los dispositivos virtuales es un aspecto importante de la métrica de rendimiento cuando se determina qué dispositivo M-Series o la cantidad mínima de recursos virtuales que hay que asignar en su dispositivo virtual Panorama para asegurarse de que cumple los requisitos de seguridad. El aumento del tamaño de archivo de configuración total admitido del servidor de gestión Panorama da como resultado un rendimiento reducido cuando se realizan cambios de configuración, confirmaciones y envíos a cortafuegos gestionados.

El servidor de gestión Panorama en el modo Panorama admite un tamaño de archivo de configuración total de 80 MB para todas las plantillas, grupos de dispositivos y configuraciones específicas de Panorama. Panorama en el modo Management Only (Solo administración) admite hasta 120 MB o 180 MB de tamaño total de archivo de configuración, según el modelo de Panorama o los recursos que asigne al dispositivo virtual de Panorama. Consulte la tabla siguiente para conocer el tamaño máximo de archivo de configuración recomendado según el modelo de dispositivo Panorama M-Series o los recursos que asigne al dispositivo virtual Panorama.

Modelo de Panorama	Recursos virtuales necesarios	Tamaño máximo de archivo de configuración de Panorama recomendado
M-200	n/c	120 MB
M-300		150 MB
M-500		120 MB
M-600		150 MB
M-700		180MB
Dispositivo virtual Panorama Consulte Requisitos previos de configuración	• 16 vCPU • 128 GB de memoria	120 MB
	• 56 vCPU	150 MB

©2023 Palo Alto Networks, Inc.

Modelo de Panorama	Recursos virtuales necesarios	Tamaño máximo de archivo de configuración de Panorama recomendado
del dispositivo virtual Panorama para obtener información adicional sobre la configuración.	• 256 GB de memoria	

Plantillas y pilas de plantillas

Puede utilizar plantillas y pilas de plantillas para configurar los ajustes que permiten que los cortafuegos funcionen en la red. Las plantillas son los componentes básicos que utiliza para configurar las pestañas **Network (Red)** y **Device (Dispositivo)** en Panorama™. Puede utilizar las plantillas para definir las configuraciones de interfaz y de zona para gestionar los perfiles de servidor para logging y acceso a syslog, o para definir configuraciones VPN. Las pilas de plantillas le ofrecen la capacidad de superponer varias plantillas y crear una configuración combinada. Las pilas de plantillas simplifican la gestión debido a que le permiten definir una configuración base común para todos los dispositivos adjuntos a la pila de plantillas y le ofrecen la capacidad de superponer plantillas para crear una configuración combinada. Esto le permite definir plantillas con ajustes específicos para una ubicación o función, y agrupar las plantillas en orden descendiente de prioridad, de modo que los cortafuegos hereden los ajusten según el orden de las plantillas dentro de la pila.

Las plantillas y las pilas de plantillas admiten variables. Las variables le permiten crear objetos de marcador de posición con valores especificados en la plantilla o la pila de plantillas según sus necesidades de configuración. Cree una variable de plantilla o pila de plantillas para sustituir direcciones IP, ID de grupo e interfaces en sus configuraciones. Las variables de plantillas se heredan de la pila de plantillas y puede cancelarlas para crear una variable de pila de plantillas. Sin embargo, las plantillas no heredan variables definidas en la pila de plantillas. Cuando se define una variable en la plantilla o en la pila de plantillas y se envía al cortafuegos, el valor que define la variable se muestra en el cortafuegos.

Use plantillas para adaptar cortafuegos que tengan configuraciones únicas. También puede enviar una configuración de base común más amplia y cancelar determinados ajustes enviados con valores específicos para el cortafuegos en cortafuegos individuales. Cuando cancela una configuración en el cortafuegos, el cortafuegos la guarda en su configuración local y Panorama ya no la gestiona. Para restaurar los valores de la plantilla después de cancelarlos, utilice Panorama para forzar la configuración de plantilla o pila de plantillas en el cortafuegos. Por ejemplo, después de definir un servidor NTP común en una plantilla y cancelar la configuración de servidor NTP en un cortafuegos para adaptar su zona horaria local, puede volver más adelante al servidor NTP definido en la plantilla.

Cuando define una pila de plantillas, considere asignar los cortafuegos que sean del mismo modelo de hardware y necesiten acceso a recursos de red similares, como puertas de enlace y servidores syslog. Esto le permite evitar la redundancia de añadir cada ajuste de configuración a cada pila de plantillas. La siguiente ilustración muestra una configuración de ejemplo en la que usted asigna cortafuegos de centros de datos en la región de Asia-Pacífico (APAC) a una pila con ajustes globales, una plantilla con ajustes específicos para APAC y una plantilla con ajustes específicos para el centro de datos. Para gestionar los cortafuegos de una sucursal de APAC, puede reutilizar las plantillas global y específica para APAC agregándolas a otra pila que incluya una plantilla con una configuración específica para la sucursal. Las plantillas de una pila tienen un orden de prioridad configurable que garantiza que Panorama introduzca solo un valor de cualquier configuración duplicada. Panorama

 ©2023 Palo Alto Networks, Inc.

evalúa las plantillas detalladas en la configuración de pila de arriba a abajo donde las plantillas más arriba tienen prioridad. La siguiente ilustración muestra la pila de un centro de datos en la que la plantilla del centro de datos tiene mayor prioridad que la plantilla global: Panorama introduce el valor del intervalo de espera por inactividad de la plantilla del centro de datos e ignora el valor de la plantilla global.

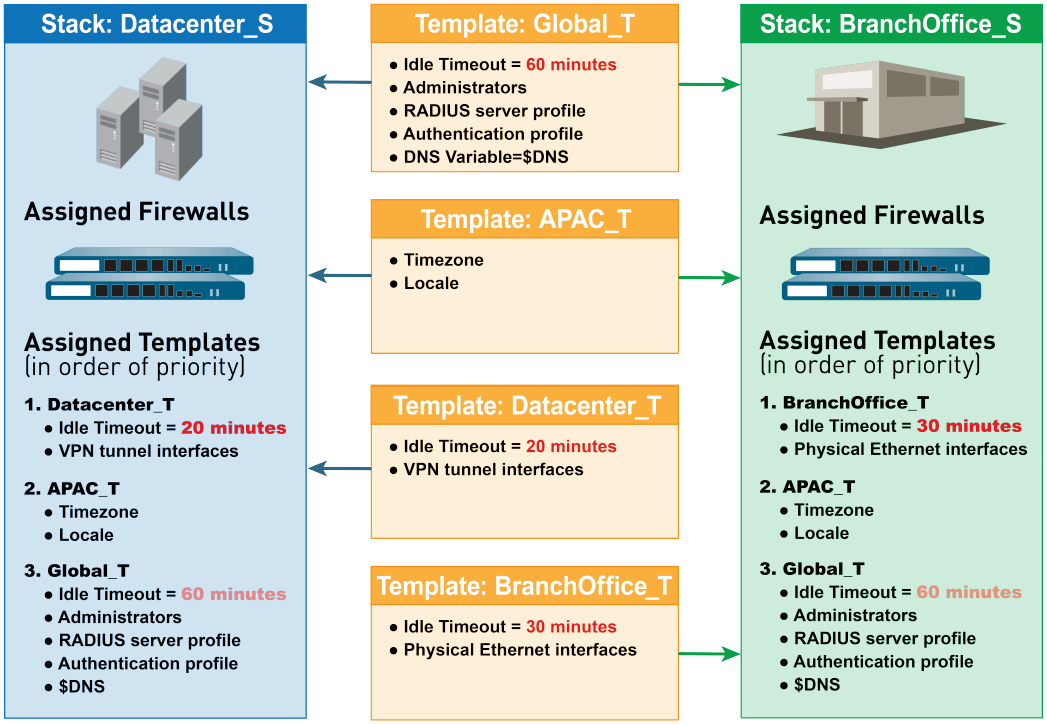


Figure 2: Pilas de plantillas

No puede utilizar plantillas o pilas de plantillas para configurar los modos de cortafuegos: modo de red privada virtual (virtual private network, VPN), modo de sistemas virtuales múltiples (vsys múltiples) o modo operativo (normal o modo FIPS-CC). Para obtener más detalles, consulte Funciones y excepciones de las plantillas. Sin embargo, puede asignar cortafuegos que tengan modos no coincidentes a la misma plantilla o pila. En estos casos, Panorama ingresa la configuración específica del modo solo a los cortafuegos compatibles con ese modo. Como excepción, puede configurar Panorama para que envíe los ajustes del vsys predeterminado en una plantilla a los cortafuegos que no son compatibles con los sistemas virtuales o que no tienen sistemas virtuales configurados.

Para obtener los procedimientos relevantes, consulte Gestión de plantillas y pilas de plantillas.

Grupos de dispositivos

Para usar Panorama de manera efectiva, debe agrupar los cortafuegos de la red en unidades lógicas denominadas ***grupos de dispositivos***. Un grupo de dispositivos permite la agrupación según segmentación de red, ubicación geográfica, función de la organización o cualquier otro aspecto común del cortafuegos que requiera configuraciones de política similares. Mediante los grupos de dispositivos, puede configurar reglas de políticas y los objetos a los que hacen referencia. Puede organizar grupos de dispositivos jerárquicamente en los que las reglas compartidas y objetos estén en la parte superior y los objetos y reglas específicas del grupo en los niveles subsiguientes. Esto le permite crear una jerarquía de reglas que indican el método de gestión del tráfico por parte de

 ©2023 Palo Alto Networks, Inc.

los cortafuegos. Por ejemplo, puede definir un conjunto de reglas compartidas como una política de uso corporativa aceptable. A continuación, para que solo las oficinas regionales accedan al tráfico de peer-a-peer como bittorrent, puede definir una regla del grupo de dispositivos que Panorama solo ingrese en las oficinas regionales (o definir una regla de seguridad compartida y dirigirla a las oficinas regionales). Para conocer los procedimientos pertinentes, consulte Gestión de grupos de dispositivos. En los siguientes temas se describen los componentes y conceptos del grupo de dispositivos en profundidad:

- Jerarquía del grupo de dispositivos
- Políticas de grupo de dispositivos
- Objetos de grupos de dispositivos

Jerarquía del grupo de dispositivos

Puede Creación de una jerarquía del grupo de dispositivos para anidar grupos de dispositivos en una jerarquía de árbol de hasta cuatro niveles en la que los grupos de nivel inferior hereden la configuración (reglas de políticas y objetos) de los grupos de mayor nivel. En el nivel inferior, un grupo de dispositivos puede tener grupos de dispositivos primarios, primarios de segundo nivel y primarios de tercer nivel (***ancestros***). En el nivel superior, un grupo de dispositivos puede tener grupos de dispositivos secundarios, secundarios de segundo nivel y secundarios de tercer nivel (***descendientes***). Todos los grupos de dispositivos heredan ajustes de la ubicación ***compartida***, un contenedor en la parte superior de la jerarquía para las configuraciones que son comunes en todos los grupos de dispositivos.

Crear una jerarquía de grupos de dispositivos le permite organizar cortafuegos según los requisitos de políticas comunes sin una configuración redundante. Por ejemplo, puede configurar ajustes compartidos que sean globales para todos los cortafuegos, configurar grupos de dispositivos con ajustes específicos para la función en el primer nivel y configurar grupos de dispositivos con ajustes específicos para la ubicación en los niveles inferiores. Sin una jerarquía, debería establecer tanto la configuración específica para la ubicación como para la función de cada grupo de dispositivos en un nivel individual en Compartido.

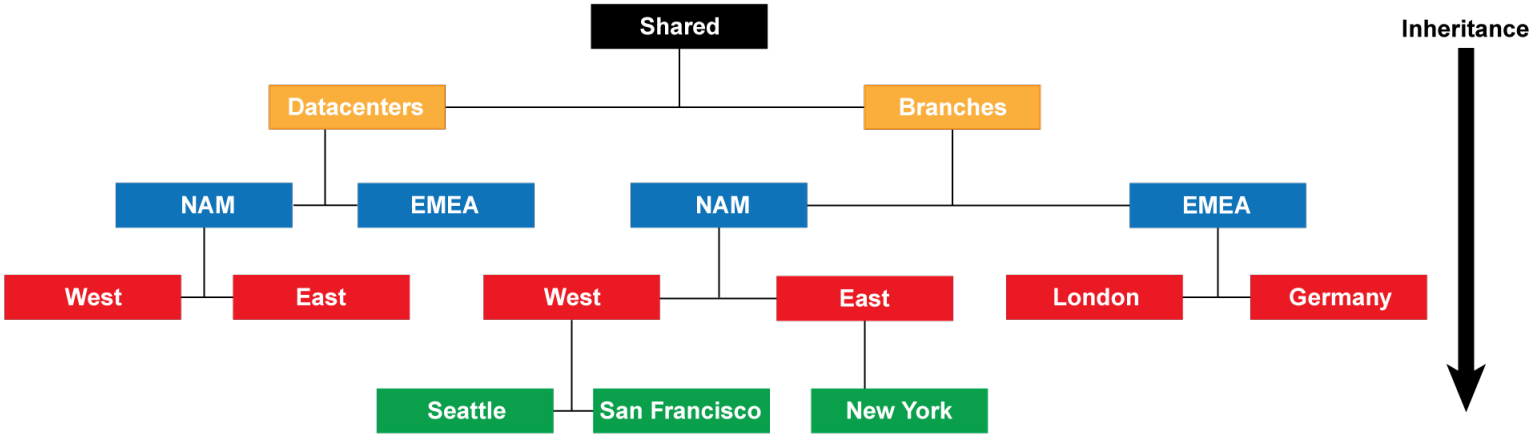
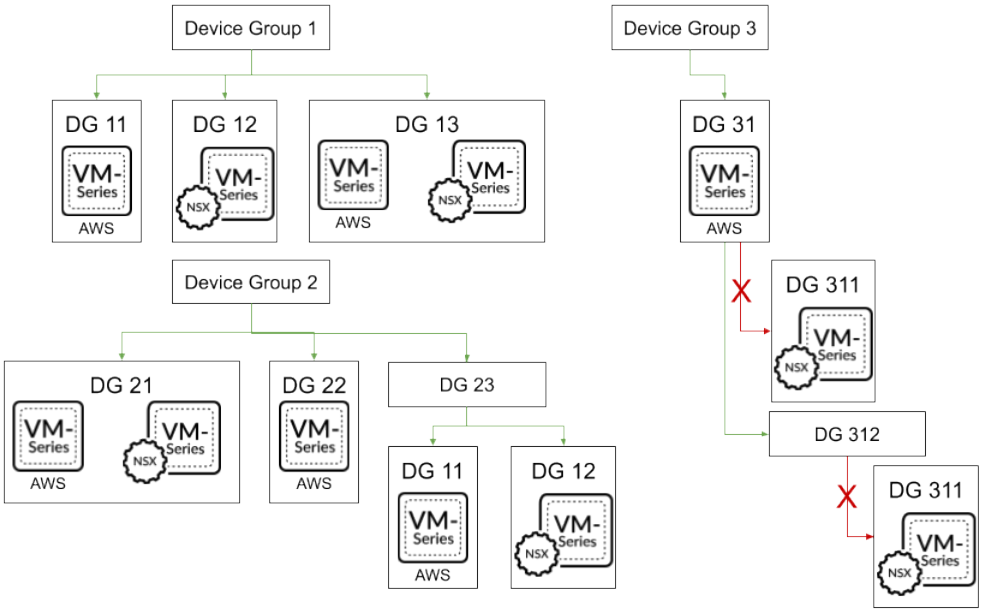


Figure 3: Jerarquía del grupo de dispositivos

Para obtener detalles sobre el orden en el que los cortafuegos evalúan las reglas de políticas en una jerarquía de grupo de dispositivos, consulte Políticas de grupo de dispositivos. Para obtener detalles sobre la cancelación de valores de objetos que los grupos de dispositivos heredan de los grupos de dispositivos primarios, consulte Objetos de grupos de dispositivos.

©2023 Palo Alto Networks, Inc.

En una implementación de varios complementos de Panorama, un grupo de dispositivos que contiene cortafuegos implementados en un hipervisor particular no puede ser el elemento principal o secundario un grupo de dispositivos que contiene cortafuegos implementados en un hipervisor diferente. Por ejemplo, si Panorama recibe actualizaciones de direcciones IP de VMware NSX-V y AWS, no puede crear un grupo de dispositivos de cortafuegos NSX-V VM-Series que sea secundario de un grupo de dispositivos de cortafuegos AWS VM-Series.

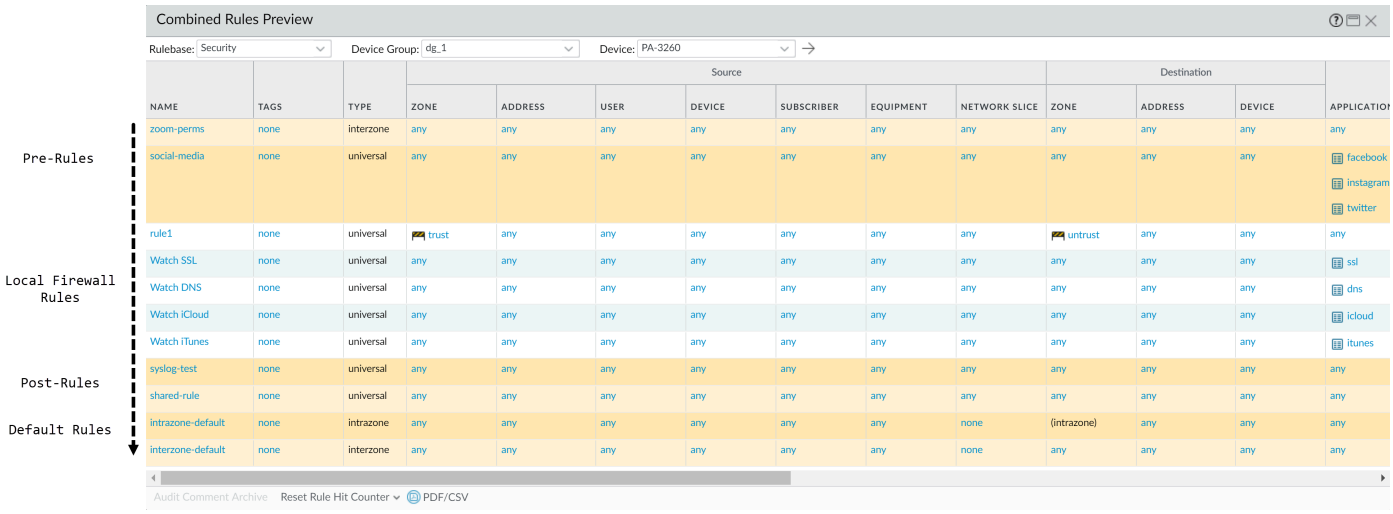


Políticas de grupo de dispositivos

Los grupos de dispositivos son una forma de implementar un método de capas para gestionar políticas en una red de cortafuegos gestionados. Un cortafuegos evalúa las reglas de políticas por capa (compartido, grupos de dispositivos y local) y por tipo (reglas previas, reglas posteriores y reglas predeterminadas) en el siguiente orden de la parte superior a la inferior. Cuando el cortafuegos recibe tráfico, lleva a cabo la acción definida en la primera regla evaluada que coincida con el tráfico y omite todas las reglas subsiguientes. Para modificar el orden de evaluación de las reglas dentro de una capa, un tipo y una base de reglas en especial (por ejemplo, reglas previas de seguridad compartida), consulte Gestión de la jerarquía de reglas.

Ya sea que vea las reglas en un cortafuegos o en Panorama, la interfaz web las muestra en el orden de evaluación. Todas las reglas compartidas, predeterminadas y del grupo de dispositivos que el cortafuegos hereda de Panorama tienen un color naranja. Las reglas de cortafuegos locales se muestran entre las reglas previas y las reglas posteriores.

©2023 Palo Alto Networks, Inc.



Orden de evaluación	Descripción y alcance de la regla	Dispositivo de administración
Reglas previas compartidas	Panorama ingresa reglas previas compartidas en todos los cortafuegos en todos los grupos de dispositivos. Panorama ingresa reglas previas específicas del grupo de dispositivos en todos los cortafuegos de un grupo de dispositivos determinado y sus grupos de dispositivos secundarios. Si un cortafuegos hereda reglas de los grupos de dispositivos en múltiples niveles de la jerarquía de grupos de dispositivos, evalúa las reglas previas de mayor a menor nivel. Esto significa que el cortafuegos primero evalúa las reglas compartidas y por último evalúa las reglas de los grupos de dispositivos sin descendientes. Puede usar las reglas previas para aplicar la política de uso aceptable de una organización. Por ejemplo, una regla previa podría bloquear el acceso a categorías URL específicas o permitir el tráfico del Sistema de nombres de dominios (Domain Name System, DNS) para todos los usuarios.	Estas reglas son visibles en los cortafuegos pero solo puede gestionarlas en Panorama.
Reglas previas de grupos de dispositivos		

©2023 Palo Alto Networks, Inc.

Orden de evaluación	Descripción y alcance de la regla	Dispositivo de administración
Reglas de cortafuegos locales	Las reglas locales son específicas para un sistema virtual (vsys) o cortafuegos individual.	Un administrador del cortafuegos local o de Panorama que cambia a un contexto de cortafuegos local puede editar reglas de cortafuegos locales.
Reglas posteriores de grupos de dispositivos Reglas posteriores compartidas	Panorama ingresa reglas posteriores compartidas en todos los cortafuegos en todos los grupos de dispositivos. Panorama ingresa reglas posteriores específicas del grupo de dispositivos en todos los cortafuegos de un grupo de dispositivos determinado y sus grupos de dispositivos secundarios. Si un cortafuegos hereda reglas de los grupos de dispositivos en múltiples niveles de la jerarquía de grupos de dispositivos, evalúa las reglas posteriores de menor a mayor nivel. Esto significa que el cortafuegos primero evalúa las reglas de los grupos de dispositivos sin descendientes y por último evalúa las reglas compartidas. Las reglas posteriores suelen incluir reglas para impedir el acceso al tráfico basado en firmas de App-ID™, información de User-ID™ (usuarios o grupos de usuario) o servicio.	Estas reglas son visibles en los cortafuegos pero solo puede gestionarlas en Panorama.
Predeterminada intrazonal Predeterminada interzonal	Las reglas predeterminadas solo se aplican a la base de reglas de seguridad y están predefinidas en Panorama (en el nivel compartido) y el cortafuegos (en cada vsys). Estas reglas especifican cómo PAN-OS gestiona el tráfico que no coincide con otra regla. La regla predeterminada intrazonal permite todo el tráfico dentro de una zona. La regla predeterminada interzonal impide todo el tráfico entre las zonas.	Inicialmente, las reglas predeterminadas son de solo lectura, ya sea porque forman parte de la configuración predeterminada o porque Panorama las ingresó en los cortafuegos. Sin embargo, puede cancelar la configuración de regla para etiquetas, acción, creación de logs y perfiles de seguridad. El contexto determina el nivel en el que puede cancelar las reglas: • Panorama: en el nivel de grupo de dispositivos o compartido,

 ©2023 Palo Alto Networks, Inc.

Orden de evaluación	Descripción y alcance de la regla	Dispositivo de administración
	Si cancela las reglas predeterminadas, su orden de precedencia va desde el contexto más bajo al más alto: la configuración cancelada en el nivel del cortafuegos tomará precedencia sobre la configuración en el nivel de grupo de dispositivos, la cual toma precedencia sobre la configuración en el nivel compartido.	puede cancelar las reglas predeterminadas que forman parte de la configuración predefinida. • Cortafuegos: puede anular las reglas predeterminadas que formen parte de la configuración predeterminada en el cortafuegos o vsys, o que Panorama ingresó desde un grupo de dispositivos o la ubicación compartida.

Objetos de grupos de dispositivos

Los objetos son elementos de configuración a los que se hace referencia en las reglas políticas, por ejemplo: direcciones IP, categorías de URL, perfiles de seguridad, usuarios, servicios y aplicaciones. Las reglas de cualquier tipo (reglas previas, reglas posteriores, reglas predeterminadas y reglas definidas localmente en un cortafuegos) y cualquier base de reglas (seguridad, NAT, QoS, Reenvío basado en la política, descifrado, cancelación de aplicación, portal cautivo y protección DoS) pueden hacer referencia a objetos. Puede reutilizar un objeto en varias reglas que tengan el mismo alcance que ese objeto en la jerarquía del grupo de dispositivos. Por ejemplo, si añade un objeto a la ubicación compartida, todas las reglas de la jerarquía pueden hacer referencia a ese ***objeto compartido*** porque todos los grupos de dispositivos heredan objetos del nivel compartido. Si añade un objeto a un grupo de dispositivos determinado, solo las reglas de ese grupo de dispositivos y sus grupos de dispositivos secundarios pueden hacer referencia a ese ***objeto del grupo de dispositivos***. Si los valores de objeto en un grupo de dispositivos deben diferir de aquellos heredados de un grupo de dispositivos primario, puede omitir valores de objetos heredados (consulte el paso Cancele los valores de objeto heredados. También puede volver a los valores de objeto heredados en cualquier momento. Cuando crea objetos para su uso en una política compartida o de grupo de dispositivos una vez y los usa varias veces, reduce los gastos generales administrativos y garantiza la consistencia en todas las políticas de cortafuegos.

Puede configurar el modo en que Panorama gestiona los objetos en todo el sistema:

- **Enviar objetos no usados**: de manera predeterminada, Panorama ingresa todos los objetos en los cortafuegos independientemente de si las reglas de políticas compartidas o del grupo de dispositivos hacen referencia a los objetos. De manera opcional, puede configurar Panorama para que ingrese solo los objetos a los que se hace referencia. Para obtener más detalles, consulte Gestión de objetos compartidos no utilizados.
- **Precedencia de los objetos primarios y secundarios**: de manera predeterminada, cuando los grupos de dispositivos de múltiples niveles en la jerarquía tienen un objeto con el mismo nombre pero valores diferentes (por ejemplo, debido a cancelaciones), las reglas de políticas de un grupo de dispositivos secundario usan los valores de objeto de ese grupo secundario en lugar de los heredados de los grupos de dispositivos primarios o del nivel compartido. De manera opcional, puede revertir este orden de precedencia para enviar valores desde el nivel compartido o el grupo primario más alto que contenga el objeto en todos los grupos de dispositivos secundarios. Para obtener más detalles, consulte Gestión de la precedencia de objetos heredados.

 ©2023 Palo Alto Networks, Inc.

Creación centralizada de logs e informes

Panorama añade logs de todos los cortafuegos gestionados y consigue visibilidad en todo el tráfico de su red. También proporciona un seguimiento auditado para todas las modificaciones de políticas y cambios de configuración realizados en los cortafuegos gestionados. Además de la agregación de logs, Panorama puede reenviarlos como traps SNMP, notificaciones de correo electrónico, mensajes de Syslog y cargas útiles HTTP a un servidor externo.

Para la creación de logs y la generación de informes centralizados, también tiene la opción de usar la función basada en la nube Cortex Data Lake que está diseñado para funcionar sin problemas con Panorama. Cortex Data Lake permite que sus cortafuegos gestionados reenvíen logs a la infraestructura de Cortex Data Lake en lugar de a Panorama o a los Recopiladores de log gestionados, para que pueda aumentar su configuración de recopilación de logs distribuidos existente o ampliar su infraestructura de creación de logs actual sin tener que invertir tiempo y esfuerzo.

El Centro de comando de aplicación (Application Command Center, ACC) en Panorama proporciona un panel individual para la elaboración de informes unificada en todos los cortafuegos. Le permite supervisar la actividad de red de forma centralizada para analizar, investigar e informar sobre el tráfico y los incidentes de seguridad. En Panorama, puede ver logs y generar informes de logs reenviados a Cortex Data Lake, Panorama o a los recopiladores de logs gestionados, si están configurados, o consultar los cortafuegos gestionados directamente. Por ejemplo, puede generar informes sobre tráfico, amenazas o actividad de los usuarios en la red gestionada basada en logs almacenados en Panorama (y en recopiladores de logs gestionados) o accediendo a los logs almacenados localmente en los cortafuegos gestionados o en Cortex Data Lake.

Si decide no configurar un reenvío de logs a Panorama o Cortex Data Lake, puede programar la ejecución de informes en cada uno de los cortafuegos gestionados y reenviar los resultados a Panorama para obtener una vista combinada de la actividad del usuario y el tráfico de red. Aunque los informes no proporcionan un desglose detallado de datos y actividades específicos, sí proporcionan un enfoque de supervisión unificado.

- Recopiladores gestionados y grupos de recopiladores
- Recopilación de logs locales y distribuidos
- Advertencias para un grupo de recopiladores con recopiladores de logs múltiples
- Opciones de reenvío de logs
- Informes centralizados

Recopiladores gestionados y grupos de recopiladores

Panorama utiliza Recopiladores de logs para añadir logs de cortafuegos gestionados. Al generar informes, Panorama consulta a los recopiladores de logs para obtener información de logs, lo que le proporciona visibilidad de toda la actividad de red que supervisan sus cortafuegos. Dado que usa Panorama para configurar y gestionar recopiladores de logs, también reciben el nombre de ***recopiladores gestionados***. Panorama puede administrar dos tipos de Recopiladores de logs:

 ©2023 Palo Alto Networks, Inc.

- **Recopilador de logs local**: este tipo de recopilador de logs se ejecuta localmente en el servidor de gestión de Panorama. Solo un dispositivo M-700, M-600, M-500, M-300 o M-100, o dispositivo virtual Panorama en modo Panorama admite un recopilador de logs local.

  Si reenvía los logs a un dispositivo virtual Panorama en modo heredado, este almacena los logs localmente sin un recopilador de logs.

- **Recopilador de logs dedicado**: este es un dispositivo M-700, M-600, M-500, M-300, M-200 o M-100, o dispositivo virtual Panorama en modo recopilador de logs. Puede utilizar un dispositivo serie M en modo Panorama o un dispositivo virtual Panorama en modo Panorama o heredado (ESXi y vCloud Air) para gestionar recopiladores de logs dedicados. Para utilizar el servidor de gestión de Panorama para gestionar recopiladores de logs dedicados, debe añadirlos como recopiladores gestionados. De lo contrario, el acceso administrativo a un recopilador de logs dedicado solo está disponible a través de su CLI utilizando la cuenta del usuario administrativo predefinida (***admin***). Los recopiladores de logs dedicados no admiten cuentas de usuarios administrativos adicionales.

Puede utilizar uno o ambos tipos de recopiladores de logs para lograr la mejor solución de logging para su entorno (consulte Recopilación de logs locales y distribuidos).

Un grupo de recopiladores consta de 1 a 16 recopiladores gestionados que funcionan como una sola unidad de recopilación de logs lógica. Si el grupo de recopiladores contiene recopiladores de logs dedicados, Panorama distribuye los logs uniformemente entre todos los discos de un recopilador de logs y entre todos los miembros del grupo de recopiladores. Esta distribución optimiza el espacio de almacenamiento disponible. Para permitir que un recopilador de logs reciba logs, debe añadirlo a un grupo de recopiladores. Puede habilitar la redundancia de logs asignando varios recopiladores de logs a un grupo de recopiladores (consulte Advertencias para un grupo de recopiladores con recopiladores de logs múltiples). La configuración del grupo de recopiladores especifica qué cortafuegos gestionados pueden enviar logs a los recopiladores de logs del grupo.

Para configurar recopiladores de logs y grupos de recopiladores, consulte Gestión de recopilación de logs.

Recopilación de logs locales y distribuidos

Antes de Configurar el reenvío de logs a Panorama, debe decidir si usar recopiladores de logs locales, recopiladores de logs dedicados o ambos.

Un Recopilador de logs local es fácil de implementar porque no requiere hardware adicional o instancia de máquina virtual. En una configuración de alta disponibilidad (HA), puede enviar logs al Recopilador de logs local en ambos peers de Panorama; el Panorama pasivo no espera a que la conmutación por error comience para recopilar logs.

Para la recopilación de logs locales, también puede reenviar logs a un dispositivo virtual Panorama en el modo heredado, que almacena los logs sin usar un recopilador de logs como contenedor lógico.

Los recopiladores de logs dedicados son dispositivos M-700, M-600, M-500, M-300, M-200 o dispositivo virtual Panorama en modo de recopilador de logs. Debido a que solo realizan la recopilación de logs, no la gestión del cortafuegos, los recopiladores de logs dedicados permiten un entorno más sólido que los recopiladores de logs locales. Los recopiladores de logs dedicados brindan los siguientes beneficios:

 ©2023 Palo Alto Networks, Inc.

- Permiten que el servidor de gestión de Panorama use más recursos para las funciones de gestión en vez de la función de logging.
- Proporcionan un almacenamiento de logs de alto volumen en un dispositivo de hardware especializado.
- Permiten mayores tasas de registro de logs.
- Proporcionan capacidad de ampliación horizontal y redundancia con un almacenamiento en RAID 1.
- Optimizan los recursos de ancho de banda en redes en las que hay más ancho de banda disponible para que los cortafuegos envíen logs a recopiladores de logs cercanos que en un servidor de gestión remoto de Panorama.
- Le permiten cumplir los requisitos reglamentarios (por ejemplo, las regulaciones podrían no permitir que los logs dejen una región en particular).

Recopilación de logs distribuidos ilustra una topología en la que los peers de Panorama en una configuración HA gestionan la implementación y configuración del cortafuegos y los recopiladores de logs dedicados.

Puede implementar el servidor de administración de Panorama en una configuración HA, pero no en los Recopiladores de logs dedicados.

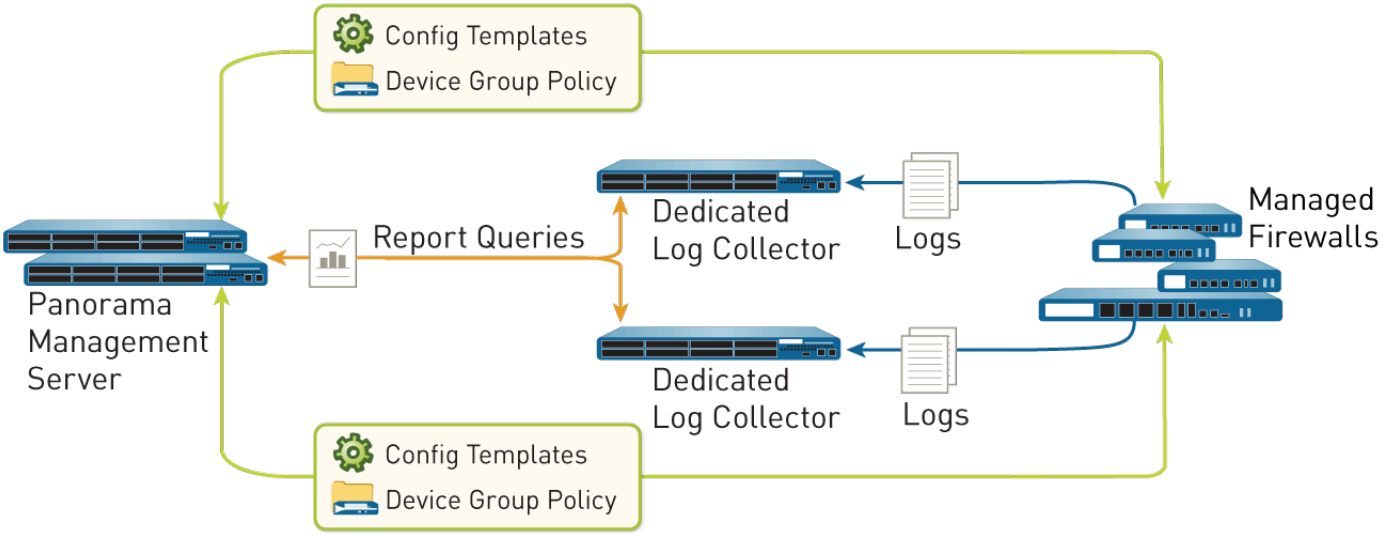


Figure 4: recopilación de logs distribuida

Advertencias para un grupo de recopiladores con recopiladores de logs múltiples

Puede configurar un grupo de recopiladores con múltiples recopiladores de logs para garantizar la redundancia de logs, aumentar el período de conservación de logs y para ajustar las tasas de logging que superan la capacidad de un único recopilador de logs (consulte Modelos de Panorama para obtener información sobre la capacidad). Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama. Por ejemplo, si un único cortafuegos

 ©2023 Palo Alto Networks, Inc.

gestionado genera 48 TB de logs, el grupo de recopiladores que recibe estos logs requerirá al menos seis recopiladores de logs que sean dispositivos M-200 o dos recopiladores de logs que sean dispositivos M-500 o dispositivos virtuales de Panorama.

Un grupo de recopiladores con múltiples recopiladores de logs usa el espacio de almacenamiento disponible como una unidad lógica y distribuye uniformemente los logs en todos sus recopiladores de logs. La distribución de logs se basa en la capacidad del disco de los recopiladores de logs (consulte Modelos de Panorama) y un algoritmo de hash que decide dinámicamente qué recopilador de logs posee los logs y escribe en el disco. Aunque Panorama utiliza una lista de preferencias para priorizar la lista de recopiladores de logs a los que puede reenviar logs un cortafuegos gestionado, Panorama no escribe necesariamente los logs en el primer recopilador de logs especificado en la lista de preferencias. Por ejemplo, consideremos la siguiente lista de preferencias:

Cortafuegos gestionado	Lista de preferencias de reenvío de logs definida en un grupo de recopiladores
FW1	L1,L2,L3
FW2	L4,L5,L6

FW1 usa esta lista para reenviar los logs a L1, siempre que ese recopilador de logs primario esté disponible. Sin embargo, en función del algoritmo hash, Panorama podría elegir L2 como el propietario que escribe los logs en sus discos. Si no se puede acceder a L2 o este tiene un fallo de bastidor, FW1 no detectará este fallo porque aún puede conectarse a L1.

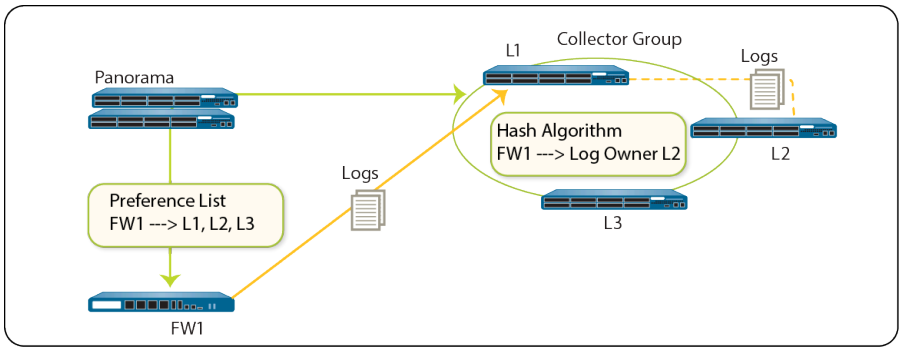


Figure 5: Ejemplo: configuración típica del grupo de recopiladores de logs

En el caso en que un grupo de recopiladores solo tenga un recopilador de logs y el recopilador de logs falle, el servidor de seguridad almacenará los logs en su HDD/SSD (el espacio de almacenamiento disponible varía según el modelo de cortafuegos) Tan pronto como se restablezca la conectividad en el recopilador de logs, el cortafuegos reanudará el reenvío de logs donde lo dejó antes de que se produjera el error.

En el caso de un Grupo de recopiladores con múltiples recopiladores de logs, el cortafuegos no almacena los logs en su almacenamiento local si solo un recopilador de logs está inactivo. Por ejemplo, si L2 está inactiva, FW1 sigue enviando logs a L1, que almacena los datos de logs que se deberían haber enviado a L2. En cuanto L2 vuelve a estar activa, L1 deja de almacenar los datos de logs dirigidos a L2 y la distribución se reanuda tal como estaba prevista. Si uno de los recopiladores de logs del grupo se queda inactivo, los logs dirigidos a él se redistribuyen al siguiente recopilador de logs de la lista de preferencias.

©2023 Palo Alto Networks, Inc.

Palo Alto Networks recomienda añadir al menos tres recopiladores de logs a un grupo de recopiladores para evitar problemas de condiciones de división e ingesta de logs en caso de que un recopilador de logs falle. Consulte los cambios en el comportamiento predeterminado del grupo de recopiladores para obtener más información.

Se admiten dos recopiladores de logs en un grupo de recopiladores, pero el grupo de recopiladores deja de funcionar si un recopilador de logs falla.

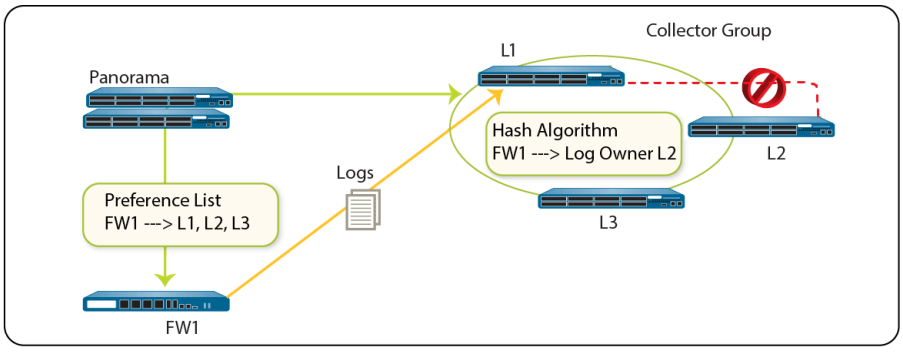


Figure 6: Ejemplo: cuando un recopilador de logs falla

Palo Alto Networks recomienda las siguientes soluciones si se usan recopiladores de logs en un grupo de recopiladores:

- Habilite la redundancia de logs cuando configure un grupo de recopiladores. Esto garantiza que no se pierdan logs si alguno de los recopiladores de logs del grupo de recopiladores no está disponible. Cada log tendrá dos copias y cada copia residirá en un recopilador de logs diferente. La redundancia de logs está disponible solo si cada recopilador de logs tiene el mismo número de discos de logs.

  Al habilitar la redundancia se crean más logs, por lo que esta configuración requiere más capacidad de almacenamiento. Si un grupo de recopiladores se queda sin espacio, elimina logs antiguos.

  Al habilitar la redundancia se dobla el tráfico de procesamiento de logs en un grupo de recopiladores, que reduce su tasa de logs máxima a la mitad, ya que cada recopilador de logs debe distribuir una copia de cada log que reciba.

- Obtenga un recambio (OSS) para disponer de una unidad de sustitución si se produce un fallo del recopilador.
- Además de reenviar logs a Panorama, configure el reenvío a un servicio externo como almacenamiento de copias de seguridad. El servicio externo puede ser un servidor Syslog, un servidor de correo electrónico o un servidor trap SNMP o un servidor HTTP.

Opciones de reenvío de logs

De manera predeterminada, cada cortafuegos almacena todos sus archivos de logs localmente. Para usar Panorama para la supervisión de logs y la generación de informes centralizadas, debe configurar el reenvío de logs a Panorama Panorama permite reenviar logs a un recopilador de logs, a Cortex Data Lake o a ambos en paralelo. También puede usar servicios externos para archivar, notificar o analizar reenviando logs a los servicios directamente desde los cortafuegos o de Panorama. Los servicios externos incluyen servidores syslog, servidores de correo electrónico, servidores de traps SNMP o servicios basados en HTTP. Además de reenviar los logs de los cortafuegos, puede reenviar

 ©2023 Palo Alto Networks, Inc.

los logs que generan el servidor de gestión de Panorama y los recopiladores de logs. El servidor de gestión de Panorama, el recopilador de logs o el cortafuegos que reenvía los logs los convierte a un formato apropiado para el destino (mensaje syslog, notificación por correo electrónico, captura SNMP o carga útil HTTP).

Los cortafuegos de Palo Alto Networks y Panorama admiten las siguientes opciones de reenvío de logs. Antes de seleccionar una opción, considere las capacidades de logging de sus Modelos de Panorama y lleve a cabo la Determinación de requisitos de almacenamiento de logs de Panorama.

- Reenvío de logs desde cortafuegos a Panorama y desde Panorama a servicios externos: esta configuración es la mejor para las implementaciones en las que las conexiones entre cortafuegos y servicios externos no tienen suficiente ancho de banda para mantener la tasa de log, lo cual sucede con frecuencia cuando las conexiones son remotas. Esta configuración mejora el rendimiento del cortafuegos descargando parte del procesamiento a Panorama.

  Puede configurar cada grupo de recopiladores para que reenvíe logs a diferentes ubicaciones.

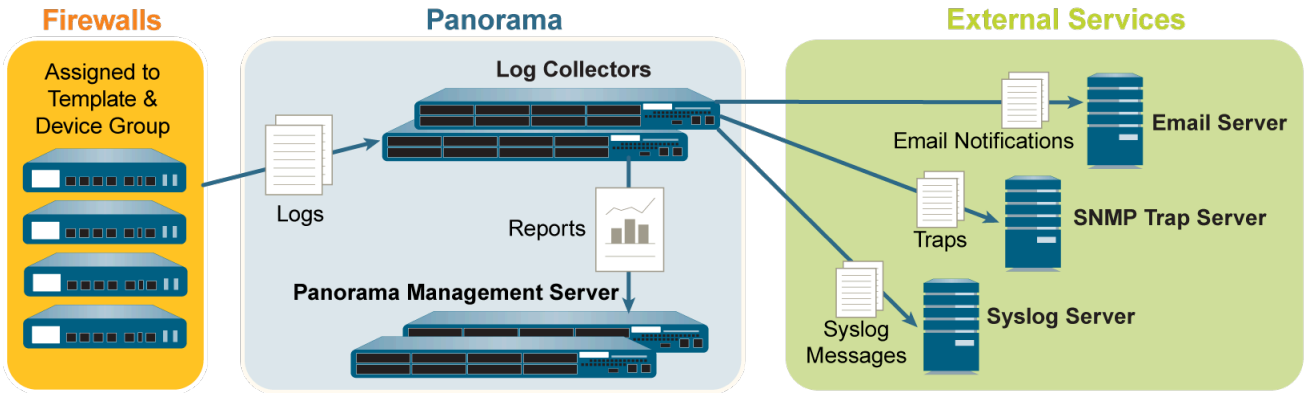


Figure 7: Reenvío de logs a Panorama y, a continuación, a servicios externos

- Reenvío de logs desde los cortafuegos a Panorama y a servicios externos en paralelo: en esta configuración, tanto Panorama como los servicios externos son extremos de flujos de reenvío de logs separados; los cortafuegos no confían en Panorama para reenviar logs a los servicios externos. Esta configuración es la mejor para las implementaciones en las que las conexiones entre cortafuegos y servicios externos tienen suficiente ancho de banda para mantener la tasa de log, lo cual sucede con frecuencia cuando las conexiones son locales.

©2023 Palo Alto Networks, Inc.

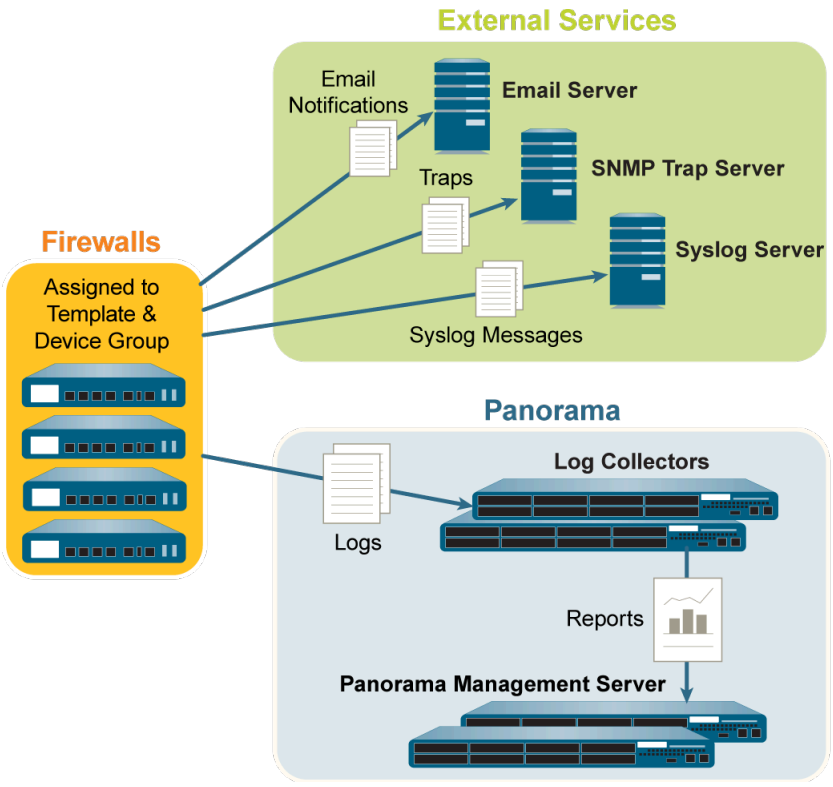


Figure 8: Reenvío de logs a servicios externos y a Panorama en paralelo

Informes centralizados

Panorama añade logs procedentes de todos los cortafuegos gestionados y permite la creación de informes sobre los datos agregados para obtener una visión global de la utilización de las aplicaciones, la actividad del usuario y los patrones de tráfico de toda la red. Tan pronto como los cortafuegos se añaden a Panorama, el ACC puede mostrar todo el tráfico que atraviesa su red. Con la creación de informes habilitada, podrá acceder directamente a los detalles específicos sobre la aplicación. haciendo clic en la entrada de un log en el ACC.

Para generar informes, Panorama utiliza dos fuentes: la base de datos local de Panorama y los cortafuegos remotos que gestiona. La base de datos de Panorama se refiere al almacenamiento local de Panorama asignado para almacenar tanto logs resumidos como algunos logs detallados. Si dispone de una implementación de recopilación de logs distribuida, la base de datos de Panorama incluirá el almacenamiento local en Panorama y todos los recopiladores de logs gestionados. Panorama resume la información (tráfico, aplicaciones, amenazas) recogida de todos los cortafuegos gestionados en intervalos de 15 minutos. Usando la base de datos local de Panorama se consiguen unos tiempos de respuesta más rápidos. Sin embargo, si prefiere no reenviar logs a Panorama, Panorama puede acceder directamente al cortafuegos remoto y ejecutar informes sobre datos almacenados localmente en los cortafuegos gestionados.

Panorama ofrece más de 40 informes predefinidos que se pueden utilizar tal cual o que se pueden personalizar combinando elementos de otros informes para generar informes personalizados y grupos de informes que se pueden guardar. Los informes se pueden generar según se necesiten, con una planificación recurrente, y se puede programar su envío diario por correo electrónico. Estos informes proporcionan información sobre el usuario y el contexto, así que puede hacer corresponder eventos e identificar patrones, tendencias y áreas potenciales de interés. Con el método integrado

 ©2023 Palo Alto Networks, Inc.

de creación de logs e informes, el ACC permite la correlación de entradas de varios logs relacionados con el mismo evento.

Para obtener más información, consulte Supervisión de la actividad de red.

©2023 Palo Alto Networks, Inc.

Redistribución de datos mediante Panorama

Con la redistribución de datos, solo tiene que configurar cada origen una vez. Después, puede redistribuir varios tipos de datos a tantos clientes como necesite. Esto le ayuda a escalar su red para que pueda añadir o eliminar orígenes y clientes fácilmente a medida que cambian las necesidades de su red.

La redistribución de datos también proporciona detalles mediante la redistribución solo de tipos de información únicamente a los cortafuegos o sistemas de gestión de Panorama que especifique. Puede utilizar subredes, intervalos y regiones para reducir aún más el tráfico de red y maximizar la capacidad del dispositivo.

Uno de los beneficios clave del cortafuegos de Palo Alto Networks es que puede aplicar políticas y generar informes basados en nombres de usuario y etiquetas en lugar de direcciones IP. El desafío para las redes a gran escala es garantizar que cada cortafuegos que aplica las políticas y genera informes tenga las asignaciones y etiquetas que se aplican a todas sus reglas de políticas. Además, cada cortafuegos que aplica Políticas de autenticación requiere un conjunto completo e idéntico de marcas de tiempo de autenticación para su base de usuarios. Cada vez que los usuarios se autentican para acceder a servicios y aplicaciones, los cortafuegos individuales registran las marcas de tiempo asociadas, pero no las comparten automáticamente con otros cortafuegos para garantizar la coherencia. La redistribución de datos resuelve estos desafíos para las redes a gran escala mediante la redistribución de los datos necesarios. Sin embargo, en lugar de configurar conexiones adicionales para redistribuir los datos entre cortafuegos, puede aprovechar su infraestructura de Panorama para Redistribución de datos a cortafuegos gestionados. La infraestructura tiene conexiones existentes que le permiten redistribuir datos en capas, desde cortafuegos a Panorama. Panorama puede redistribuir la información a los cortafuegos que hacen cumplir las políticas y generan informes.

Cada cortafuegos o servidor de gestión Panorama puede recibir datos de hasta 100 puntos de redistribución. Los puntos de redistribución pueden ser otros cortafuegos o servidores de gestión Panorama. Sin embargo, también puede usar agentes de User-ID basados en Windows para realizar la asignación y redistribuir la información a los cortafuegos. Solo los cortafuegos registran las marcas de tiempo de autenticación cuando el tráfico del usuario coincide con las reglas de la política de autenticación.

 ©2023 Palo Alto Networks, Inc.

Control de acceso basado en funciones

El Control de acceso basado en funciones (Role-based access control, RBAC) le permite definir los privilegios y las responsabilidades correspondientes de los usuarios administrativos (administradores). Cada administrador debe tener una cuenta de usuario que especifique la función y el método de autenticación. Funciones administrativas definen el acceso a ajustes de configuración, logs e informes específicos dentro de los contextos de Panorama y el cortafuegos. Para los administradores de plantillas y grupos de dispositivos, puede asignar funciones a los Dominios de acceso, que definen el acceso a grupos de dispositivos, plantillas y cortafuegos específicos (a través de los cambios de contexto). Mediante la combinación de cada dominio de acceso con una función, puede aplicar la separación de la información entre las áreas funcionales o regionales de su organización. Por ejemplo, puede limitar a un administrador a actividades de supervisión de los cortafuegos del centro de datos pero permitirle que establezca políticas para probar los cortafuegos. De manera predeterminada, cada dispositivo Panorama (dispositivo virtual o de la serie M) tiene una cuenta administrativa predeterminada (admin) que proporciona acceso completo de escritura y lectura (acceso de súper usuario) a todas las áreas funcionales y a todos los grupos de dispositivos, plantillas y cortafuegos. Para cada administrador, puede definir un perfil de autenticación que determine la forma en que Panorama verifica las credenciales de acceso del usuario.

En lugar de usar la cuenta predeterminada para todos los administradores, es recomendable que cree una cuenta administrativa diferente para cada persona que necesite acceder a las funciones de administración o informes de Panorama. Esto mejora la protección frente a los cambios de configuración no autorizados y permite que Panorama registre e identifique las acciones de cada administrador.

- Funciones administrativas
- Perfiles y secuencias de autenticación
- Dominios de acceso
- Autenticación administrativa

Funciones administrativas

Puede configurar las cuentas de administrador según los requisitos de seguridad de su organización, los servicios de autenticación existentes que usa su red y las funciones administrativas que necesite. Una ***función*** define el tipo de acceso al sistema que está disponible para un administrador. Puede definir y restringir el acceso de forma tan amplia o limitada como necesite, según los requisitos de seguridad de su organización. Por ejemplo, puede decidir que el administrador de un centro de datos tenga acceso a toda la configuración de los dispositivos o la red, pero que un administrador de seguridad pueda tener control sobre las definiciones de políticas de seguridad, mientras que otras personas concretas tengan acceso limitado a la CLI o API XML. Los tipos de funciones son:

- **Funciones dinámicas**: Funciones integradas que proporcionan acceso a Panorama y a los cortafuegos gestionados. Al añadir nuevas funciones, Panorama actualiza automáticamente las definiciones de funciones dinámicas; no necesitará actualizarlas manualmente en ningún momento. En la siguiente tabla se enumeran los privilegios de acceso asociados con las funciones dinámicas.

 ©2023 Palo Alto Networks, Inc.

Función dinámica	Privilegios
Superusuario	Acceso de lectura y escritura completo a Panorama
Superusuario (solo lectura)	Acceso de solo lectura a Panorama
Administrador de Panorama	Acceso completo a Panorama a excepción de las siguientes acciones: • Crear, modificar o eliminar los administradores y funciones de Panorama o el cortafuegos. • Exportar, validar, revertir, guardar, cargar o importar una configuración de la página **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**. • Configurar la funcionalidad **Scheduled Config Export (Exportación de configuración programada)** en la pestaña **Panorama**. • **Generate Tech Support File (Generar archivo de soporte técnico)**, **Generate Stats Dump File (Generar archivo de volcado de estadísticas)** y **Download Core Files (Descargar archivos principales)** (**Panorama** > **Support [Soporte]**)

- **Perfiles de función de administrador**: Para ofrecer un control de acceso más granular sobre las áreas funcionales de la interfaz web, CLI y API XML, puede crear funciones personalizadas. Al añadir nuevas funciones al producto, debe actualizar las funciones con los privilegios de acceso correspondientes. Panorama no añade nuevas funciones automáticamente a las definiciones de funciones personalizadas. Seleccione uno de los siguientes tipos de perfil al Configuración de un perfil de función de administrador.

Perfil de función de administrador	Description (Descripción)
Panorama	Para estas funciones, puede asignar acceso de lectura y escritura, asignar acceso de solo lectura o excluir el acceso a todas las funciones de Panorama disponibles para la función dinámica de superusuario, excepto la gestión de administradores y funciones de Panorama. En el caso de las dos últimas funciones, puede asignar acceso de solo lectura o excluir el acceso, pero no puede asignar acceso de lectura y escritura. Por ejemplo, se podría usar una función de Panorama para los administradores de seguridad que requieren acceso a definiciones de políticas de seguridad, logs e informes en Panorama. Las funciones de administración personalizadas de Panorama tienen las siguientes limitaciones: • Sin acceso a **Reboot Panorama (Reiniciar Panorama)** (**Panorama** > **Setup [Configuración]** > **Operations [Operaciones]**)

©2023 Palo Alto Networks, Inc.

Perfil de función de administrador	Description (Descripción)
	• Sin acceso a **Generate Tech Support File (Generar archivo de soporte técnico)**, **Generate Stats Dump File (Generar archivo de volcado de estadísticas)** y **Download Core Files (Descargar archivos principales)** (**Panorama** > **Support [Soporte]**)

Grupo de dispositivo y plantilla	Para estas funciones, puede asignar acceso de lectura y escritura, acceso de solo lectura o no asignar acceso a las áreas funcionales específicas dentro de grupos de dispositivos, plantillas y contextos de cortafuegos Mediante la combinación de estas funciones con Dominios de acceso, puede aplicar la separación de la información entre las áreas funcionales o regionales de su organización. Las funciones de grupos de dispositivos y plantillas tienen las siguientes limitaciones:
	• Sin acceso a la CLI o API XML
	• Sin acceso a la configuración o los logs del sistema
	• Sin acceso a fuentes de información de VM
	• Sin acceso a **Reboot Panorama (Reiniciar Panorama)** (**Panorama** > **Setup [Configuración]** > **Operations [Operaciones]**)
	• Sin acceso a **Generate Tech Support File (Generar archivo de soporte técnico)**, **Generate Stats Dump File (Generar archivo de volcado de estadísticas)** y **Download Core Files (Descargar archivos principales)** (**Panorama** > **Support [Soporte]**)
	• En la pestaña **Panorama**, el acceso está limitado a lo siguiente:
	  • funciones de implementación del dispositivo (acceso de lectura y escritura, acceso de solo lectura o sin acceso);
	  • grupos de dispositivos especificados en la cuenta del administrador (acceso de lectura y escritura, acceso de solo lectura o sin acceso);
	  • plantillas y cortafuegos gestionados especificados en la cuenta del administrador (acceso de solo lectura o sin acceso).
	Por ejemplo, esta función podría aplicarse a administradores de su equipo de operaciones que requieren acceso a las zonas de configuración de red y de dispositivos de la interfaz web para grupos de dispositivos o plantillas específicos.

Perfiles y secuencias de autenticación

Un perfil de autenticación define el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores cuando estos acceden a Panorama. El servicio puede ser la Autenticación local o un servicio de autenticación externo. Algunos servicios (SAML, TACACS + y RADIUS) ofrecen la opción de gestionar tanto la autenticación como la autorización para cuentas administrativas en el servidor externo en lugar de en Panorama. Además del servicio de autenticación, el perfil de autenticación define opciones como el inicio de sesión único (SSO) de Kerberos y el cierre de sesión único (SSO) de SAML.

©2023 Palo Alto Networks, Inc.

Algunas redes tienen múltiples bases de datos (como TACACS+ y LDAP) para distintos usuarios y grupos de usuarios. Para autenticar administradores en esos casos, configure una secuencia de autenticación: una clasificación ordenada de perfiles de autenticación con los que Panorama compara al administrador durante el inicio de sesión. Panorama compara cada perfil en orden hasta que uno autentica correctamente al administrador. Solo se impide el acceso del administrador si falla la autenticación con todos los perfiles definidos en la secuencia.

Dominios de acceso

Los dominios de acceso controlan el acceso administrativo a Grupos de dispositivos y plantillas específicos y también controlar la habilidad de cambiar el contexto a la interfaz web de los cortafuegos gestionados. Los dominios de acceso se aplican solo a los administradores con funciones de grupos de dispositivos y plantillas. La asignación de Funciones administrativas para acceder a dominios ofrece un control muy detallado sobre la información a la que pueden acceder los administradores en Panorama. Por ejemplo, imagine una situación en la que configura un dominio de acceso que incluye todos los grupos de dispositivos de los cortafuegos en sus centros de datos y que asigna ese dominio de acceso a un administrador que tenga permiso para supervisar el tráfico del centro de datos pero que no pueda configurar los cortafuegos. En este caso, asignaría el dominio de acceso a una función que proporcione todos los privilegios de supervisión, pero que no dé acceso a la configuración del grupo de dispositivos. Además, los administradores de plantillas y grupos de dispositivos pueden realizar tareas administrativas para cortafuegos gestionados en su dominio de acceso, como ver la configuración y los logs del sistema, realizar auditorías de configuración, revisar las tareas pendientes y acceder directamente a las operaciones del cortafuegos, como reiniciar, generar un archivo de soporte técnico, ejecutar un volcado de estadísticas y exportar un archivo central.

Configure los dominios de acceso en la configuración de Panorama local y luego asígnelos a cuentas y funciones administrativas. Puede realizar la tarea localmente o usar un servidor SAML, TACACS o RADIO externo. La utilización de un servidor externo le permite reasignar rápidamente los dominios de acceso a través de su servicio de directorio en lugar de reconfigurar los ajustes en Panorama. Para utilizar un servidor externo, debe definir un perfil de servidor que permita a Panorama acceder al servidor. También debe definir los Atributos específicos de proveedor (VSA) en el servidor TACACS+ o RADIUS, o los atributos SAML en el servidor SAML IdP.

Por ejemplo, si usa un servidor RADIUS, definiría un número y valor VSA para cada administrador. El valor definido debe coincidir con el dominio de acceso configurado en Panorama. Cuando un administrador intenta iniciar sesión en Panorama, Panorama consulta al servidor RADIUS el dominio de acceso del administrador y el número de atributo. Sobre la base de la respuesta del servidor RADIUS, se autoriza el acceso del administrador y se lo restringe a los cortafuegos, sistemas virtuales, grupos de dispositivos y plantillas asignadas en el dominio de acceso.

Para obtener los procedimientos relevantes, consulte:

- Configuración de un dominio de acceso.
- Configuración de la autenticación de RADIUS para los administradores de Panorama.
- Configuración de la autenticación de TACACS+ para los administradores de Panorama.
- Configuración de la autenticación de SAML para los administradores de Panorama.

 ©2023 Palo Alto Networks, Inc.

Autenticación administrativa

Puede configurar los siguientes tipos de autenticación y autorización (Funciones administrativas y Dominios de acceso para los administradores de Panorama:

Authenticatio Method	Método de autorización	Description (Descripción)
Local	Local	Las credenciales de la cuenta de administrador y los mecanismos de autenticación se encuentran en Panorama. Utilice Panorama para asignar funciones administrativas y dominios de acceso a las cuentas. Para añadir un nivel de protección adicional a las cuentas, cree un perfil de contraseña que defina un período de validez para las contraseñas y establezca ajustes de complejidad de la contraseña para todo Panorama. Para obtener más detalles, consulte Configuración de la autenticación local o externa para los administradores de Panorama.
Claves SSH	Local	Las cuentas administrativas se encuentran en Panorama, pero la autenticación de la CLI se realiza en función de las claves SSH. Utilice Panorama para asignar funciones administrativas y dominios de acceso a las cuentas. Para obtener más detalles, consulte Configuración de un administrador con autenticación basada en claves de SSH para la CLI.
certificates	Local	Las cuentas administrativas se encuentran en Panorama, pero la autenticación de la interfaz web se realiza en función de los certificados de los clientes. Utilice Panorama para asignar funciones administrativas y dominios de acceso a las cuentas. Para obtener más detalles, consulte Configuración de un administrador de Panorama con autenticación basada en certificado para la interfaz web.
Servicio externo	Local	Las cuentas administrativas que define localmente Panorama funcionan como referencias de las cuentas definidas en un servidor de autenticación multifactor, SAML, Kerberos, TACACS+, RADIUS o LDAP externo. El servidor externo realiza la autenticación. Utilice Panorama para asignar funciones administrativas y dominios de acceso a las cuentas. Para obtener más detalles, consulte Configuración de la autenticación local o externa para los administradores de Panorama.
Plataforma	Servicio externo	Las cuentas administrativas se definen únicamente en un servidor SAML, TACACS+ o RADIUS externo. El servidor realiza la autenticación y la autorización. En el caso de la autorización, puede definir los Vendor-Specific Attributes (Atributos específicos del proveedor, VSA) en el servidor TACACS+ o RADIUS, o los atributos SAML en el servidor SAML. Panorama asigna los atributos a las

 ©2023 Palo Alto Networks, Inc.

Authenticatio Method	Método de autorización	Description (Descripción)
		funciones de administrador y accede a los dominios que define en Panorama. Para obtener los detalles, consulte: • Configuración de la autenticación de SAML para los administradores de Panorama • Configuración de la autenticación de TACACS+ para los administradores de Panorama • Configuración de la autenticación de RADIUS para los administradores de Panorama

©2023 Palo Alto Networks, Inc.

Operaciones de confirmación, validación y previsualización de Panorama

Cuando esté listo para activar los cambios que realizó en la configuración candidata en Panorama o para enviar cambios a los dispositivos que gestiona Panorama (cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire), puede Previsualización, validación o compilación de cambios de configuración. Por ejemplo, si añade un recopilador de logs a la configuración de Panorama, los cortafuegos no pueden enviar logs a ese recopilador de logs hasta que confirme el cambio en Panorama y luego envíe el cambio al grupo de recopiladores que contiene el recopilador de logs.

Puede filtrar los cambios por administrador o ***ubicación*** y, a continuación, compilar, enviar, validar o previsualizar solo esos cambios. La ubicación pueden ser grupos de dispositivos, plantillas, grupos de recopiladores, recopiladores de logs, configuraciones compartidas específicos o el servidor de gestión Panorama.

Al compilar los cambios, estos se convierten en parte de la configuración en ejecución. Los cambios que no haya compilado son parte de la configuración candidata. Panorama pone en cola las solicitudes de compilación de modo que pueda iniciar nuevas compilaciones mientras una previa está en curso. Panorama compila en el orden en que se inician las solicitudes, pero prioriza las compilaciones automáticas iniciadas por Panorama (como las actualizaciones de FQDN). Sin embargo, si la cola ya tiene el número máximo de confirmaciones iniciadas (10) por el administrador, debe esperar a que Panorama termine de procesar una compilación pendiente antes de iniciar una nueva. Puede Uso del gestor de tareas de Panorama (Tasks) para cancelar las confirmaciones pendientes o ver detalles de la confirmaciones que están completas, pendientes, en curso o que tienen errores. Para comprobar qué cambios activará una confirmación, puede ejecutar una previsualización de la confirmación.

Cuando inicia una compilación, Panorama verifica la validez de los cambios antes de activarlos. El resultado de la validación exhibe condiciones que bloquean la confirmación (errores) o que son importantes de conocer (advertencias). Por ejemplo, la validación podría indicar un destino de ruta no válido que debe fijar para que la confirmación se realice correctamente. La validación le permite encontrar y corregir errores antes de compilar (no realiza cambios en la configuración en ejecución). Esto es útil si tiene una fecha límite de compilación y quiere asegurarse de que la compilación funcionará sin errores.

La recuperación de confirmación automática está habilitada de manera predeterminada, lo que permite que los cortafuegos gestionados prueben localmente la configuración que se envía desde Panorama para verificar que los nuevos cambios no interrumpan la conexión entre Panorama y el firewall gestionado. Si la configuración confirmada interrumpe la conexión entre Panorama y un cortafuegos gestionado, el cortafuegos rechazará automáticamente la confirmación, la configuración se revertirá a la configuración anterior en ejecución y la política compartida o el estado de la plantilla (**Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**) se desincronizarán según los objetos de configuración que se hayan enviado. Además, los cortafuegos gestionados prueban la conexión a Panorama cada 60 minutos y si esos cortafuegos detectan que ya no puede conectarse correctamente a Panorama, revertirán su configuración a la configuración anterior en ejecución.

 ©2023 Palo Alto Networks, Inc.

Si desea información detallada sobre configuraciones candidatas y en ejecución, consulte Gestión de las copias de seguridad de configuración de Panorama y del cortafuegos.

Para prevenir que varios administradores realicen cambios en la configuración durante sesiones simultáneas, consulte Gestión de bloqueos para restringir cambios de configuración.

Al enviar configuraciones a cortafuegos gestionados, Panorama envía la configuración en ejecución. Por este motivo, Panorama no le permite enviar cambios a cortafuegos gestionados hasta que confirme los cambios en Panorama.

©2023 Palo Alto Networks, Inc.

Planificación de su implementación de Panorama

- Determine el método de gestión. ¿Planea utilizar Panorama para configurar y gestionar las políticas o administrar las actualizaciones de software, contenido y licencia de forma centralizada? ¿O bien para centralizar la creación de logs e informes en todos los cortafuegos gestionados de la red?

  Si ya ha implementado y configurado los cortafuegos de Palo Alto Networks en su red, determine si va a realizar la transición de los cortafuegos a la gestión centralizada. Este proceso necesita migrar toda la configuración y las políticas de los cortafuegos a Panorama. Para obtener más detalles, consulte Transición de un cortafuegos a una gestión de Panorama.
- Verifique las versiones de software de Panorama y el cortafuegos. Panorama puede gestionar cortafuegos que ejecutan versiones de PAN-OS que coinciden con la versión de Panorama o son anteriores a esta. Por ejemplo, un Panorama que ejecuta PAN-OS 10.2 admite la administración de cortafuegos y que ejecutan las versiones PAN-OS 10.2, 10.1, 10.0, 9.1, 9.0 o 8.1. Consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.
- Determine su método de autenticación entre Panorama y sus dispositivos gestionados y su peer de alta disponibilidad. De forma predeterminada, Panorama usa certificados predefinidos para autenticar las conexiones SSL utilizadas para la gestión y la comunicación entre dispositivos. Sin embargo, puede configurar una autenticación personalizada basada en certificado para mejorar la seguridad de las conexiones SSL entre Panorama, el cortafuegos y los recopiladores de logs. Mediante la utilización de certificados personalizados, puede establecer una cadena de confianza única para garantizar la autenticación mutua entre Panorama y los dispositivos que gestiona. Puede importar los certificados desde la infraestructura de clave pública (PKI) de su empresa o generarlos en Panorama.
- Planifique utilizar Panorama en una configuración de alta disponibilidad; configúrelo como un clúster en alta disponibilidad activo/pasivo. Seleccione Alta disponibilidad de Panorama.
- Planifique cómo acomodar la segmentación de red y los requisitos de seguridad en una implementación a gran escala. De forma predeterminada, cuando Panorama se ejecuta en un dispositivo serie M, utiliza la interfaz de gestión (MGT) para el acceso administrativo a Panorama y para gestionar dispositivos (cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire), recopilar logs, comunicarse con grupos de recopiladores e implementar actualizaciones de software y de contenido para dispositivos. Sin embargo, para mejorar la seguridad y habilitar la segmentación de red, puede reservar la interfaz MGT para acceso administrativo y usar interfaces de dispositivos serie M (Eth1, Eth2, Eth3, Eth4 y Eth5) dedicadas para los otros servicios.
- Para obtener informes de alto contenido sobre la actividad de la red, planifique una solución de registro:
  - Verifique la asignación de recursos a su dispositivo virtual Panorama implementado en modo de recopilador de logs en AWS o Azure. El dispositivo virtual Panorama no mantiene el modo de recopilador de logs si se cambia el tamaño. Esto provoca una pérdida de datos de logs.
  - Calcule la capacidad de almacenamiento de logs que necesita su red para satisfacer los requisitos de seguridad y cumplimiento. Debe tener en cuenta una serie de factores como la capacidad de logging de sus modelos de Panorama, la topología de red, el número de cortafuegos que envían logs, el tipo de tráfico de log (por ejemplo, logs de filtrado de URL y logs de amenazas frente a logs de tráfico), la velocidad a la que los cortafuegos generan logs y

 ©2023 Palo Alto Networks, Inc.

el número de días que desea almacenar los logs en Panorama. Para obtener más información, consulte Determinación de requisitos de almacenamiento de logs de Panorama.

- ¿Necesita reenviar logs a servicios externos (como un servidor Syslog) además de a Panorama? Consulte Opciones de reenvío de logs.
- ¿Desea poseer o gestionar su propio almacenamiento de logs en las instalaciones o desea aprovechar Cortex Data Lake de Palo Alto Networks?
- Si necesita una solución de almacenamiento a largo plazo, ¿cuenta con una solución de gestión de eventos e información de seguridad (Security Information and Event Management, SIEM), como Splunk o ArcSight, a la que pueda reenviar los logs?
- ¿Necesita redundancia en la creación de logs?

  Si configura un grupo de recopiladores con múltiples recopiladores de logs, puede habilitar la redundancia para garantizar que no se pierda ningún log si alguno de los recopiladores de logs deja de estar disponible (consulte Advertencias para un grupo de recopiladores con recopiladores de logs múltiples)

  Si implementa dispositivos virtuales Panorama en el modo heredado en una configuración de HA, los cortafuegos gestionados pueden enviar logs a ambos peers de HA para que una copia de cada log resida en cada peer. Esta opción de redundancia se encuentra habilitada de manera predeterminada (consulte Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs).
- ¿Almacenará los logs en un sistema de archivos de red (NFS)? Si el dispositivo virtual Panorama está en modo heredado y no gestiona recopiladores de logs dedicados, el almacenamiento NFS es la única opción para aumentar la capacidad de almacenamiento de logs por encima de los 8 TB. El almacenamiento NFS está disponible solo si Panorama se ejecuta en un servidor ESXi. Si utiliza el almacenamiento NFS, tenga en cuenta que los cortafuegos pueden enviar logs solo al peer primario de un par de HA y que solo el peer primario se monta en el NFS, en el que además se puede escribir.

- ❑ Determine qué privilegios de acceso basados en roles requieren los administradores para acceder a los cortafuegos gestionados y Panorama. Consulte Configuración del acceso administrativo a Panorama.
- ❑ Planifique los grupos de dispositivos necesarios. Considere si desea agrupar los cortafuegos según la función, la política de seguridad, la ubicación geográfica o la segmentación de la red. Un ejemplo de grupo de dispositivos basado en funciones es uno que contenga todos los cortafuegos que usa el equipo de I+D. Considere si desea crear grupos de dispositivos más pequeños según las características en común, grupos de dispositivos más grandes para escalar más fácilmente o una jerarquía del grupo de dispositivos para simplificar las capas de administración complejas.
- ❑ Planifique una estrategia de capa para administrar las políticas. Considere cómo deben heredarse y evaluarse las reglas de políticas de los cortafuegos dentro de la jerarquía del grupo de dispositivos y cómo implementar mejor las reglas compartidas, reglas de grupos de dispositivos y reglas específicas del cortafuegos para cumplir las necesidades de su red. Para tener visibilidad y obtener una gestión de política centralizada, considere utilizar Panorama para administrar reglas, incluso si desea excepciones específicas del cortafuegos para las reglas compartidas o de grupo de dispositivos. Si es necesario, puede ingresar una regla de política a un subconjunto de cortafuegos dentro de un grupo de dispositivos.

 ©2023 Palo Alto Networks, Inc.

- Planifique la organización de sus cortafuegos según la forma en que heredan los ajustes de configuración de red de plantillas y pilas de plantillas. Por ejemplo, considere asignar cortafuegos a las plantillas basadas en moldeos de hardware, proximidad geográfica y necesidades de red similares para zonas horarias, servidor DNS y ajustes de la interfaz.

©2023 Palo Alto Networks, Inc.

Implementación de Panorama: Descripción general de tareas

En la siguiente lista de tareas se resumen los pasos para empezar a utilizar Panorama. En Caso de uso: Configuración de cortafuegos mediante Panorama puede ver un ejemplo de cómo usar Panorama para la gestión central.

STEP 1 | (Solo dispositivo de la serie M) Monte el dispositivo en bastidor.

STEP 2 | Realice la configuración inicial para habilitar el acceso de red a Panorama. Consulte Configuración del dispositivo virtual Panorama o Configuración del dispositivo de la serie M.

STEP 3 | Registro de Panorama e instalación de licencias.

STEP 4 | Instale las actualizaciones de contenido y software de Panorama.

STEP 5 | (Recomendado) Configure Panorama con unos ajustes de alta disponibilidad. Consulte Alta disponibilidad de Panorama.

STEP 6 | Cómo añadir un cortafuegos como dispositivo gestionado.

STEP 7 | Adición de un grupo de dispositivos o Creación de una jerarquía del grupo de dispositivos, Cómo añadir una plantilla, y (si corresponde) Configuración de una pila de plantillas.

STEP 8 | (Opcional) Configure el reenvío de logs a Panorama o servicios externos. Consulte Gestión de la recopilación de logs.

STEP 9 | Supervisión de la actividad de red mediante las herramientas de visibilidad y creación de informes en Panorama.

©2023 Palo Alto Networks, Inc.

Configuración de Panorama

Para la realización centralizada de informes y una gestión de políticas cohesiva en todos los cortafuegos de la red, puede implementar el servidor de gestión Panorama™ como dispositivo virtual o dispositivo de hardware (dispositivo M-200, M-300, M-500, M-600 o M-700).

En los siguientes temas se describe cómo configurar Panorama en la red:

- Determinación de requisitos de almacenamiento de logs de Panorama
- Gestión de implementaciones de cortafuegos a gran escala
- Configuración del dispositivo virtual Panorama
- Configuración del dispositivo de la serie M
- Registro de Panorama e instalación de licencias
- Instalación del certificado de dispositivo de Panorama
- Transición a un modelo diferente de Panorama
- Acceso y navegación en las interfaces de gestión de Panorama
- Configuración del acceso administrativo a Panorama
- Configuración de la autenticación mediante certificados personalizados

Determinación de requisitos de almacenamiento de logs de Panorama

Cuando planifique la implementación de Panorama, estime la capacidad de almacenamiento de logs que Panorama requiere para determinar qué modelos de Panorama hay que implementar, y si debe expandir el almacenamiento en estos modelos por encima de sus capacidades predeterminadas, implementar recopiladores de logs dedicados y configurar el reenvío de logs desde Panorama a destinos externos. Cuando el almacenamiento de logs alcanza la capacidad máxima, Panorama elimina automáticamente los logs anteriores para crear espacio para los nuevos.

Lleve a cabo estos pasos para determinar el almacenamiento de logs aproximado que Panorama requiere. Para obtener más detalles y casos de uso, consulte la Guía de diseño y tamaño de Panorama.

STEP 1 | Determine los requisitos de conservación de logs de su organización.

Los factores que afectan los requisitos de conservación de logs incluyen los siguientes:

- La política de TI de su organización.
- Redundancia de logs: si habilita la redundancia de logs cuando configura un grupo de recopiladores, cada log tendrá dos copias, lo cual duplica su capacidad de almacenamiento de logs requerida.
- Los requisitos reglamentarios, como aquellos especificados por el Estándar de Seguridad de Datos para la industria de Tarjeta de Pago (Payment Card Industry Data Security Standard, PCI DSS), la ley Sarbanes-Oxley y la Ley de transferencia y responsabilidad de los seguro médicos (Health Insurance Portability and Accountability Act, HIPAA).



Si su organización requiere la eliminación de logs después de un determinado período, puede configurar el período de vencimiento para cada tipo de log. También puede configurar una cuota de almacenamiento para cada tipo de log como un porcentaje del espacio total si necesita priorizar la conservación de logs por tipo. Para obtener más información, consulte Gestión de cuotas de almacenamiento y períodos de vencimiento de logs e informes.

STEP 2 | Determine las tasas de creación de logs diarias promedio.

Realice esto varias veces al día durante las horas punta y fuera de las horas punta para estimar el promedio. Cuanto más a menudo realice las muestras de las tasas, más precisa será su estimación.

1. Visualice la tasa de generación de logs actual en logs por segundo:
   - Si Panorama aún no recopila logs, acceda a la CLI de cada cortafuegos, ejecute el siguiente comando y calcule las tasas totales de todos los cortafuegos. Este comando muestra el número de logs recibidos en el último segundo.

     ```
     > debug log-receiver statistics
     ```

   - Si Panorama ya recopila logs, ejecute el siguiente comando en la CLI de cada dispositivo que recibe logs (el servidor de gestión de Panorama o el recopilador de logs dedicado) y

 ©2023 Palo Alto Networks, Inc.

calcule las tasas totales. Este comando proporciona la tasa de creación de logs promedio durante los últimos cinco minutos.

```
> debug log-collector log-collection-stats show incoming-logs
```

También puede usar un administrador de SNMP para determinar las tasas de creación de logs de los recopiladores de logs (consulte el MIB panLogCollector, OID 1.3.6.1.4.1.25461.1.1.6) y los cortafuegos (consulte panDEviceLogging, OID 1.3.6.1.4.1.25461.2.1.2. 7).

2. Calcule el promedio de las tasas de la muestra.
3. Calcule la tasa de creación de logs promedio multiplicando la cantidad promedio de logs por segundo por 86 400.

STEP 3 | Estime la capacidad de almacenamiento requerida.

Esta fórmula solo proporciona una estimación; la cantidad exacta de almacenamiento requerido será diferente del resultado de la fórmula.

Utilice esta fórmula:

<required_storage_duration> x <average_log_size> x <average_logging_rate>

El tamaño de log promedio varía en gran medida de acuerdo al tipo de log. Sin embargo, puede usar 500 bytes como un tamaño de log promedio aproximado.

Por ejemplo, si Panorama debe almacenar logs durante 30 días y la tasa de creación de logs total promedio de todos los cortafuegos es de 21 254 400 logs por día, entonces la capacidad de almacenamiento requerida es la siguiente: 30 x 500 x 21 254 400 = 318 816 000 000 bytes (318 GB aproximadamente).

STEP 4 | Pasos siguientes:

Si determina que Panorama requiere más capacidad de almacenamiento de logs:

- Amplíe la capacidad de almacenamiento del log en el dispositivo virtual Panorama.
- Aumente la capacidad de almacenamiento en el dispositivo M-Series.

 ©2023 Palo Alto Networks, Inc.

Gestión de implementaciones de cortafuegos a gran escala

Panorama™ ofrece varias opciones para gestionar las implementaciones de cortafuegos a gran escala. Con el fin de consolidar todas las funciones de gestión, Panorama permite administrar hasta 5000 cortafuegos con un dispositivo M-600 o M-700 en el modo Management Only (Solo gestión) o hasta 2500 cortafuegos con un dispositivo virtual Panorama en ese mismo modo. Para simplificar la implementación y la gestión operativa de las instalaciones a gran escala con más de 5000 cortafuegos, el complemento Panorama Interconnect permite gestionar varios nodos de servidores de gestión de Panorama con un solo controlador de Panorama.

- Evaluación de la solución óptima para implementaciones de cortafuegos a gran escala
- Aumento de la capacidad de gestión de dispositivos en los dispositivos M-Series y los dispositivos virtuales Panorama

Evaluación de la solución óptima para implementaciones de cortafuegos a gran escala

Para aliviar la carga operativa que supone gestionar la configuración de las implementaciones de cortafuegos a gran escala y adaptarse a cada caso particular, Palo Alto Networks ofrece distintas opciones de gestión de cortafuegos.

Si su implementación de cortafuegos a gran escala se compone de uno o de pocos servidores de gestión Panorama, puede implementar un dispositivo M-600 o M-700 para gestionar hasta 5000 cortafuegos, o un dispositivo virtual Panorama para gestionar hasta 2500, para aprovechar todas las capacidades de Panorama de un único servidor de gestión Panorama. El aumento de la capacidad (consulte Aumento de la capacidad de gestión de dispositivos en los dispositivos M-Series y los dispositivos virtuales Panorama) es el procedimiento idóneo para las implementaciones con escalabilidad vertical. En ellas, gestiona numerosos cortafuegos con un solo servidor de gestión de Panorama, en lugar de implementar varios para gestionar menos cortafuegos.

Si la implementación de cortafuegos a gran escala tiene varios servidores de gestión Panorama con configuraciones parecidas, el complemento Panorama Interconnect permite gestionar varios nodos de Panorama con un solo controlador de Panorama. El complemento simplifica la implementación y la gestión operativa de implementaciones de cortafuegos a larga escala debido a que puede gestionar centralmente la política y la configuración desde un controlador Panorama. En el controlador de Panorama, se sincroniza la configuración de los grupos de dispositivos y de la pila de plantillas con los nodos de Panorama y se envía a los dispositivos gestionados. El complemento Panorama Interconnect es perfecto para las implementaciones de cortafuegos con escalabilidad horizontal, que cuentan con varios servidores de gestión de Panorama distribuidos.

Aumento de la capacidad de gestión de dispositivos en los dispositivos M-Series y los dispositivos virtuales Panorama

Los dispositivos M-600 y M-700 en el modo Management Only (Solo gestión) puede gestionar hasta 5000 cortafuegos, o un dispositivo virtual Panorama en el mismo modo hasta 2500, para reducir la huella de gestión de su implementación de cortafuegos a gran escala.

 ©2023 Palo Alto Networks, Inc.

- Requisitos para aumentar la capacidad de gestión de dispositivos
- Instalación de Panorama para aumentar la capacidad de gestión de dispositivos

Requisitos para aumentar la capacidad de gestión de dispositivos

Puede gestionar hasta 5000 cortafuegos con un solo dispositivo M-600 o M-700 en modo Management Only (Solo gestión), o gestionar hasta 2500 con un solo dispositivo virtual Panorama en ese mismo modo. La posibilidad de gestionar implementaciones de tanta envergadura con un único servidor de gestión de Panorama no solo simplifica la gestión de la configuración, sino que también reduce los riesgos para la seguridad y el cumplimiento que entraña gestionar varios servidores de gestión de Panorama.

A la hora de recopilar logs, no tiene que acceder a varios servidores de gestión de Panorama, ya que ese servidor único constituye la ubicación centralizada idónea para consultar y analizar los datos de logs de los dispositivos gestionados. Palo Alto Networks recomienda implementar dos servidores de gestión de Panorama en una configuración de alta disponibilidad (high availability, HA) para tener redundancia en caso de fallo del sistema o de la red. Para el sistema Panorama y los logs de configuración, se requiere un disco adicional con una capacidad mínima de 92 GB. El dispositivo virtual de Panorama detecta automáticamente este disco adicional cuando se reinicia Panorama y se monta como una partición para el almacenamiento del log de configuración y del sistema.

Si desea generar informes predefinidos, habilite en Panorama el uso de datos de Panorama para informes predefinidos. De esta forma, se generan informes predefinidos que usan los datos de logs que Panorama o el recopilador de logs dedicado ya han recopilado y se reduce la utilización de recursos durante la generación de informes. Es obligatorio habilitar esta opción para que no disminuya el rendimiento de Panorama, ni este deje de responder.

Para gestionar hasta 5000 cortafuegos, el servidor de gestión de Panorama debe cumplir los siguientes requisitos mínimos:

Requisito	Dispositivo M-Series	Dispositivo virtual Panorama
Modelo	M-600 M-700	Todos los hipervisores de Panorama admitidos. Para obtener más información, consulte Modelos Panorama.
Modo de Panorama	Solo de gestión	Solo de gestión
Número de cortafuegos gestionados	5000	2.500
Disco de sistema	SSD de 240 GB: sirve para almacenar los archivos del sistema operativo y los logs del sistema.	• 81 GB. Sirve para almacenar los archivos del sistema operativo y los logs del sistema. • Disco adicional con una capacidad mínima de 92 GB utilizado para almacenar el

©2023 Palo Alto Networks, Inc.

Requisito	Dispositivo M-Series	Dispositivo virtual Panorama
		sistema Panorama y los logs de configuración.
CPU	56	28
Memoria	256GB	128GB
Recopilación de logs	Recopilación local de logs no admitida. Consulte Implementación de Panorama con recopiladores de logs dedicados para configurar la recopilación de logs.	
Creación de logs e informes	En **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Logging and Reporting Settings (Configuración de creación de logs e informes)** > **Log Export and Reporting (Exportación de logs y creación de informes)**, habilite el ajuste **Use Panorama Data for Pre-Defined Reports (Usar datos de Panorama en informes predefinidos)**.	

Instalación de Panorama para aumentar la capacidad de gestión de dispositivos

Active la licencia de gestión de dispositivos para administrar más de 1000 cortafuegos desde un solo servidor de gestión Panorama™ M-600 o un solo dispositivo virtual Panorama.

STEP 1 | Póngase en contacto con el representante de ventas de Palo Alto Networks para obtener la licencia de gestión de dispositivos de Panorama que permite gestionar hasta 5000 cortafuegos.

- Si desea implementar un dispositivo M-600, obtenga la licencia de gestión de dispositivos `PAN-M-600-P-1K`.
- Si desea implementar un dispositivo M-700, obtenga la licencia de gestión de dispositivos `PAN-M-700-P-1K`.
- Si desea implementar un dispositivo virtual Panorama, obtenga la licencia de gestión de dispositivos `PAN-PRA-1000`.

STEP 2 | Configure el servidor de gestión de Panorama.

- (Solo dispositivos M-600 y M-700) Configuración del dispositivo de la serie M.

O

- Configuración del dispositivo virtual Panorama.

STEP 3 | Si el servidor de gestión de Panorama no está todavía en el modo Management Only (Solo gestión), cámbielo.

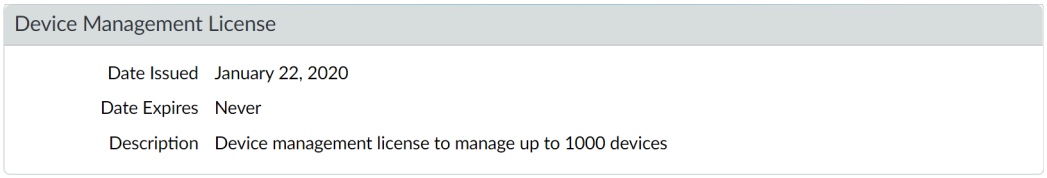
- Realice el procedimiento Configuración de un dispositivo serie M en modo solo de gestión desde el paso 5.
- Configuración de un dispositivo virtual Panorama en modo solo de gestión.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Registre el servidor de gestión de Panorama e instale las licencias.

1. Registro de Panorama.
2. Activación de una licencia de asistencia técnica de Panorama.
3. Active la licencia de gestión de dispositivos en el servidor de gestión de Panorama.
   - Activación/recuperación de una licencia de gestión de cortafuegos en el dispositivo de la serie M.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.

STEP 5 | Seleccione **Panorama** > **Licenses (Licencias)** y verifique si está activada la licencia de gestión de dispositivos.



Si ha activado la licencia de gestión de un nuevo dispositivo en Panorama, puede gestionar hasta 5000 cortafuegos con un dispositivo M-600 o M-700, y hasta 2500 con un dispositivo virtual Panorama a pesar de que la descripción indique `Device management license to manage up to 2,500 devices or more (Licencia para gestionar hasta 1000 dispositivos o más)`.

 ©2023 Palo Alto Networks, Inc.

Configuración del dispositivo virtual Panorama

El dispositivo virtual Panorama le permite usar su infraestructura virtual existente de VMware para gestionar y supervisar de forma centralizada los cortafuegos de Palo Alto Networks y los recopiladores de logs dedicados. Puede instalar el dispositivo virtual en un servidor ESXi, Alibaba Cloud, Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), KVM, Hyper-V o en vCloud Air. Además o en lugar de desplegar recopiladores de logs dedicados, puede reenviar logs de cortafuegos directamente al dispositivo virtual Panorama. Para una mayor capacidad de almacenamiento de logs y generación de informes más rápida, tiene la opción de cambiar el dispositivo virtual del modo heredado al modo Panorama y configurar un recopilador de logs local. Para obtener información detallada sobre el dispositivo virtual Panorama y sus modos, consulte Modos de Panorama.

Estos temas suponen que usted está familiarizado con los hipervisores públicos y privados requeridos para crear el dispositivo virtual y no abarcan conceptos o terminología de VMware.

- Requisitos previos de configuración del dispositivo virtual Panorama
- Instalación del dispositivo virtual Panorama
- Realización de la configuración inicial del dispositivo virtual Panorama
- Configuración del dispositivo virtual Panorama como un recopilador de logs
- Configuración del dispositivo virtual Panorama con recopiladores de logs locales
- Configuración de un dispositivo virtual Panorama en modo Panorama
- Configuración de un dispositivo virtual Panorama en modo solo de gestión
- Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual Panorama
- Aumento de CPU y memoria en el dispositivo virtual Panorama
- Aumento del disco del sistema en el dispositivo virtual de Panorama
- Realización de la configuración del dispositivo virtual Panorama
- Cómo convertir su dispositivo virtual Panorama

Requisitos previos de configuración del dispositivo virtual Panorama

Complete las siguientes tareas antes de instalar el dispositivo virtual Panorama:

- Utilice su navegador para acceder al sitio web de atención al cliente de Palo Alto Networks y registre Panorama. Necesitará el número de serie de Panorama que recibió en el correo electrónico de procesamiento del pedido. Después de registrar Panorama, puede acceder a la página de descargas de software de Panorama.
- Revise los hipervisores de Panorama admitidos para verificar si el suyo cumple los requisitos mínimos para implementar Panorama.
- Si instalará Panorama en un servidor VMware ESXi, verifique que el servidor cumpla con los requisitos mínimos que se detallan en Requisitos del sistema para el dispositivo virtual Panorama. Estos requisitos se aplican a Panorama 5.1 y versiones posteriores. Los requisitos dependen de

 ©2023 Palo Alto Networks, Inc.

si pretende ejecutar el dispositivo virtual en el modo de Panorama o en el modo de solo gestión. Para obtener más información sobre los modos, consulte Modelos Panorama.

Si instala Panorama en VMware vCloud Air, la configuración del sistema se establecerá durante la instalación.

Revise los requisitos mínimos de recursos para implementar el dispositivo virtual Panorama en Alibaba Cloud, Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), Hyper-V, KVM, Oracle Cloud Infrastructure (OCI) y VMware ESXi para garantizar que la máquina virtual cumpla con los requisitos mínimos de recursos para el modo deseado (Panorama, Solo gestión o recopilador de logs). Los requisitos mínimos de recursos para el dispositivo virtual Panorama están diseñados para ayudarlo a alcanzar el número máximo de logs por segundo (Logs Per Second, LPS) para la recopilación de logs en el modo Panorama y el modo de recopilación de logs. Si añade o elimina discos de creación de logs virtuales que dan como resultado una configuración que no cumple o supera el número de discos de creación de logs virtuales recomendados (a continuación), el LPS se reducirá.

Si no se cumplen los requisitos mínimos de recursos para usar el modo Panorama cuando Instalación del dispositivo virtual Panorama, Panorama elige de forma predeterminada el modo Solo gestión para todos los hipervisores admitidos, tanto públicos (Alibaba Cloud, AWS, AWS GovCloud, Azure, GCP y OCI) como privados (Hyper-V, KVM y VMware ESXi). Si no se cumplen los requisitos mínimos de recursos para usar el modo de solo gestión, Panorama elige de forma predeterminada el modo de mantenimiento para todos los hipervisores públicos admitidos, Hyper-V y KVM. Si no se cumplen los requisitos mínimos de recursos para usar el modo de solo gestión cuando realiza el procedimiento Instalación de Panorama en VMware, Panorama elige de forma predeterminada el modo heredado.

Se recomienda implementar el servidor de gestión de Panorama en el modo de Panorama para usar las funciones de gestión de dispositivos y de recopilación de logs. Aunque todavía es compatible, el modo Legacy (Heredado) no es recomendable para entornos de producción. Además, ya no puede cambiar Panorama al modo Legacy (Heredado). Para obtener más información sobre los modos admitidos, consulte Modelos Panorama.

Table 1: Requisitos del sistema del dispositivo virtual Panorama

Requisitos	Dispositivo virtual Panorama en modo solo de gestión	Dispositivo virtual Panorama en modo Panorama	Dispositivo virtual Panorama en modo recopilador de logs
Versión de hardware virtual	• **VMware ESXi y vCloud Air**: VMware ESXi 6.0, 6.5, 6.7, o 7.0 basado en kernel de 64 bits. La versión compatible del tipo de familia de hardware virtual (también recibe el nombre de versión de hardware virtual de VMware) en el servidor ESXi es vmx-10. • **Hyper-V**: Windows Server 2016 con función Hyper-V o Hyper-V 2016. • **KVM**: Ubuntu, versión 16.04 o CentOS7 En el modo Panorama, el dispositivo virtual que se ejecuta en cualquier versión ESXi admite hasta 12 discos virtuales de logging con 2 TB de almacenamiento de logs cada uno, para una capacidad máxima total de 24 TB.		

©2023 Palo Alto Networks, Inc.

Requisitos	Dispositivo virtual Panorama en modo solo de gestión	Dispositivo virtual Panorama en modo Panorama	Dispositivo virtual Panorama en modo recopilador de logs
	(Solo VMware ESXi y vCloud Air) En el modo Legacy (Heredado), el dispositivo virtual admite un disco de creación de logs virtual. (ESXi 5.5 o las versiones posteriores pueden admitir un disco virtual de hasta 8 TB. Las versiones anteriores de ESXi admiten un disco virtual de hasta 2 TB.		
(Solo ESXi y vCloud Air) Equipo cliente	Para instalar el dispositivo virtual Panorama y gestionar sus recursos, debe instalar un Cliente VMware vSphere o VMware Infrastructure que sea compatible con su servidor ESXi.		
Disco de sistema	• **Predeterminado**: 81 GB • (Solo para ESXi y GCP) **Actualizado**: 224 GB Se requiere un disco de sistema actualizado para SD-WAN.	• **Predeterminado**: 81 GB • (Solo para ESXi y GCP) **Actualizado**: 224 GB Se requiere un disco de sistema actualizado para SD-WAN. Para el almacenamiento de logs, Panorama utiliza discos virtuales de logging en lugar del disco del sistema o un almacén de datos NFS.	81GB Para el almacenamiento de logs, Panorama utiliza discos virtuales de logging en lugar del disco del sistema o un almacén de datos NFS.

©2023 Palo Alto Networks, Inc.

Requisitos	Dispositivo virtual Panorama en modo solo de gestión	Dispositivo virtual Panorama en modo Panorama	Dispositivo virtual Panorama en modo recopilador de logs

CPU, memoria y discos de creación de logs	• Gestión de hasta 500 dispositivos gestionados
	  • 16 CPU
	  • 32 GB de memoria
	  • Almacenamiento de logs local no compatible
	• Gestión de hasta 1000 dispositivos gestionados
	  • 32 CPU
	  • 128 GB de memoria
	  • Almacenamiento de logs local no compatible
	• Para gestionar más de 1000 cortafuegos, consulte Requisitos para aumentar la capacidad de gestión de dispositivos.
		Se requieren los recursos mínimos a continuación para lograr la tasa de creación de logs especificada.
		• Hasta 10 000 registros/seg (RPS):
		  • 16 CPU
		  • 32 GB de memoria
		  • 4 discos de creación de logs de 2 TB
		  Si no se requiere lograr el LPS especificado, se requiere un mínimo de 1x2TB.
		  • Gestión de hasta 500 dispositivos gestionados
		• Hasta 20 000 logs/s (RPS):
		  • 32 CPU
		  • 128 GB de memoria
		  • 8 discos de creación de logs de 2 TB
		  Si no se requiere lograr el LPS especificado, se requiere un mínimo de 1x2TB.
		  • Gestión de hasta 1000 dispositivos gestionados
			Se requieren los recursos mínimos a continuación para lograr la tasa de creación de logs especificada.
			• Hasta 15 000 logs/s (RPS):
			  • 16 CPU
			  • 32 GB de memoria
			  • 4 discos de creación de logs de 2 TB
			  Si no se requiere lograr el LPS especificado, se requiere un mínimo de 1x2TB.
			• Hasta 25 000 registros/seg (RPS)
			  • 32 CPU
			  • 128 GB de memoria
			  • 8 discos de creación de logs de 2 TB
			  Si no se requiere lograr el RPS especificado, se requiere un mínimo de 1x2TB.

CPU y memoria mínimas	• 16 CPU • 32 GB de memoria	Los recursos mínimos siguientes no tienen en cuenta LPS y solo son necesarios para que el dispositivo virtual Panorama funcione en función del número de discos de creación de logs agregados. Palo Alto Networks recomienda que consulte los recursos recomendados anteriormente.	

©2023 Palo Alto Networks, Inc.

Requisitos	Dispositivo virtual Panorama en modo solo de gestión	Dispositivo virtual Panorama en modo Panorama	Dispositivo virtual Panorama en modo recopilador de logs
		Para implementaciones de Panorama más grandes, tenga en cuenta que puede estar aprovisionando de manera insuficiente su Panorama. Esto puede afectar el rendimiento y hacer que Panorama deje de responder en función del número de cortafuegos gestionados, el tamaño de la configuración, la cantidad de administradores que iniciaron sesión en Panorama y el volumen de logs incorporados. • **De 2 TB a 8 TB**: 16 CPU, 32 GB de memoria • **De 10 TB a 24 TB**: 16 CPU, 64 GB de memoria	
Capacidad de almacenamiento de logs	El modo solo de gestión de Panorama requiere el reenvío de logs a un recopilador de logs dedicado.	De 2TB a 24TB	De 2TB a 24TB

Interfaces admitidas

Las interfaces se pueden usar para la gestión de dispositivos, la recopilación de logs, la comunicación entre grupos de dispositivos, la activación de licencias y las actualizaciones de software. El dispositivo virtual Panorama admite hasta seis interfaces (MGT y Eth1 - Eth5).

Table 2: Interfaces compatibles con hipervisores públicos

Función	Alibaba Cloud	Amazon Web Services (AWS) y AWS GovCloud		Microsoft Azure	Google Cloud Platform (GCP)	OCI
Gestión de dispositivos	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz
Recopilación de logs del dispositivo	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz
Comunicación del grupo de recopiladores	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz

©2023 Palo Alto Networks, Inc.

Función	Alibaba Cloud	Amazon Web Services (AWS) y AWS GovCloud		Microsoft Azure	Google Cloud Platform (GCP)	OCI
Activación de licencias y actualizaciones de software	Solo interfaz MGT	Solo interfaz MGT	Solo interfaz MGT	Solo interfaz MGT	Solo interfaz MGT	Solo interfaz MGT

Table 3: Interfaces compatibles con hipervisores privados

Función	KVM	Hyper-V	VMware (ESXi, vCloud Air)
Gestión de dispositivos	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz
Recopilación de logs del dispositivo	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz
Comunicación del grupo de recopiladores	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz
Activación de licencias y actualizaciones de software	Se admite cualquier interfaz	Se admite cualquier interfaz	Se admite cualquier interfaz

Instalación del dispositivo virtual Panorama

Antes de la instalación, decida si desea ejecutar el dispositivo virtual en modo Panorama, solo de gestión, recopilador de logs o heredado (solo WMware). Cada modo tiene diferentes requisitos de recursos, como se describe en Requisitos previos de configuración del dispositivo virtual Panorama. Debe completar los requisitos previos antes de comenzar la instalación.

Se recomienda instalar el dispositivo virtual en modo Panorama para optimizar el almacenamiento de logs y la generación de informes. Para obtener información detallada sobre los modos Panorama y heredado, consulte Modelos de Panorama.

- Instalación de Panorama en VMware
- Configuración de Panorama en Alibaba Cloud
- Instalación de Panorama en AWS
- Instalación de Panorama en AWS GovCloud
- Instalación de Panorama en Azure
- Instalación de Panorama en Google Cloud Platform
- Instalación de Panorama en KVM

©2023 Palo Alto Networks, Inc.

- Instalación de Panorama en Hyper-V
- Configuración de Panorama en Oracle Cloud Infrastructure (OCI)

Instalación de Panorama en VMware

Puede instalar el dispositivo virtual Panorama en las plataformas VMware ESXi y vCloud Air.

- Instalación de Panorama en un servidor ESXi
- Instalación de Panorama en vCloud Air
- Compatibilidad para herramientas VMware en el dispositivo virtual Panorama.

Instalación de Panorama en un servidor ESXi

Utilice estas instrucciones para instalar un nuevo dispositivo virtual Panorama en un servidor VMware ESXi. Para actualizaciones a un dispositivo virtual Panorama existente, vaya a Instalación de actualizaciones de contenido y software de Panorama.

STEP 1 | Descargue el archivo del dispositivo virtual abierto (OVA) de la imagen básica de Panorama 10.2.

1. Visite el sitio de descargas de software de Palo Alto Networks. (Si no puede iniciar sesión, visite el sitio web de Atención al cliente de Palo Alto Networks para obtener asistencia).
2. En la columna Download (Descargar) de la sección Panorama Base Images (Imágenes básicas de Panorama), descargue la última versión del archivo OVA de Panorama (`Panorama-ESX-10.0.0.ova`).

STEP 2 | Instale Panorama.

1. Inicie el cliente VMware vSphere y conéctese al servidor VMware.
2. Seleccione **File (Archivo)** > **Deploy OVF Template (Implementar plantilla OVF)**.
3. Haga clic en **Browse (Explorar)** para seleccionar el archivo OVA de Panorama y haga clic en **Next (Siguiente)**.
4. Confirme que el nombre y la descripción del producto coinciden con la versión descargada y haga clic en **Next (Siguiente)**.
5. Introduzca un nombre descriptivo para el dispositivo virtual Panorama y haga clic en **Next (Siguiente)**.
6. Seleccione una ubicación del almacén de datos (disco del sistema) donde instalar la imagen de Panorama. Consulte los Requisitos previos de configuración del dispositivo virtual Panorama para conocer los tamaños de disco del sistema admitidos. Después de seleccionar el almacén de datos, haga clic en **Next (Siguiente)**.
7. Seleccione **Thick Provision Lazy Zeroed (Suministro estándar diferido a cero)** como el formato de disco y haga clic en **Next (Siguiente)**.
8. Especifique las redes del inventario que se deben utilizar para el dispositivo virtual Panorama y haga clic en **Next (Siguiente)**.
9. Confirme las opciones seleccionadas y haga clic en **Finish (Finalizar)** para comenzar el proceso de instalación, y haga clic en **Close (Cerrar)** cuando termine. No encienda el dispositivo virtual Panorama todavía.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure los recursos en el dispositivo virtual Panorama.

1. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
2. En la configuración de **Hardware**, asigne CPU y memoria según considere.

   *El dispositivo virtual se inicia en modo Panorama si asigna suficientes **CPU** y **Memory (Memoria)** y añade un disco de logging virtual (más adelante en este procedimiento). De lo contrario, el dispositivo se inicia en el modo de solo gestión. Para obtener más información sobre los modos, consulte* Modelos Panorama**.**
3. Configure **SCSI Controller (Controlador SCSI)** en **LSI Logic Parallel**.
4. (Opcional) Agregue un disco virtual de creación de logs.

   Este paso es obligatorio en los siguientes escenarios:

   - *En el modo Panorama para almacenar logs en una creación de logs dedicada.*
   - *Gestione su implementación de SD-WAN en modo Management Only (Solo gestión).*

   1. Seleccione **Add (Añadir)** para añadir un disco, seleccione **Hard disk (Disco duro)** como el tipo de hardware y haga clic en **Next (Siguiente)**.
   2. Seleccione **Create a new virtual disk (Crear un nuevo disco virtual)** y haga clic en **Next (Siguiente)**.
   3. Establezca el **tamaño de disco** exactamente en 2 TB.

      En el modo Panorama, puede añadir discos de creación de logs adicionales *más adelante (para un total de 12) con 2 TB de almacenamiento cada uno. No se admite la ampliación del tamaño de un disco de creación de logs ya añadido a Panorama.*
   4. Seleccione su formato de **aprovisionamiento de disco** preferido.

      Tenga en cuenta las necesidades de su empresa cuando seleccione el formato de aprovisionamiento de disco. Para obtener más información sobre las consideraciones de rendimiento del aprovisionamiento de disco, consulte el documento Thick vs Thin Disks and All Flash Arrays (Discos gruesos frente a discos finos y matrices totalmente flash) de VMware o la documentación adicional de VMware.

      *Cuando añada varios discos de creación de logs, se recomienda seleccionar el mismo formato de **aprovisionamiento de disco** para todos los discos para evitar cualquier problema de rendimiento inesperado que pueda surgir.*
   5. Seleccione **Specify a datastore or datastore structure (Especifique una estructura de almacén de datos o almacén de datos)** como la ubicación, seleccione **Browse**

 ©2023 Palo Alto Networks, Inc.

(Examinar) y vaya a un almacén de datos que tenga suficiente almacenamiento, haga clic en **OK (Aceptar)** y en **Next (Siguiente)**.

6. Seleccione un **Virtual Device Node (Nodo de dispositivo virtual)** en formato de Interfaz de sistemas de ordenador pequeño (Small Computer Systems Interface, SCSI) (puede usar la selección predeterminada) y haga clic en **Next (Siguiente)**.

   Panorama no arrancará si selecciona un formato que no sea SCSI.

7. Verifique que la configuración sea correcta y luego haga clic en **Finish (Terminar)**.

5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Active el dispositivo virtual Panorama.

1. En el cliente vSphere, haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**. Espere a que Panorama arranque antes de continuar.
2. Inicie sesión en la CLI del dispositivo virtual Panorama desde la consola ESXi:
   1. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Open Console (Abrir consola)**.
   2. Introduzca el nombre de usuario y la contraseña para iniciar sesión (el valor predeterminado es **admin** para ambos).

STEP 5 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web o la CLI del dispositivo virtual Panorama. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

Cuando inicia sesión por primera vez en la CLI de Panorama, se le solicita que introduzca la **contraseña anterior** y la **contraseña nueva** para el usuario `administrador` antes de que pueda continuar.

STEP 6 | Verifique que Panorama esté ejecutando el modo de sistema correcto.

```
admin> show system info
```

En el resultado, el modo de sistema `system-mode` indica los modos `panorama` o `management-only (solo gestión)`.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.
2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.
3. Active una licencia de gestión de cortafuegos.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.
4. Active una licencia de asistencia técnica de Panorama.

STEP 8 | Aumento del disco del sistema para Panorama en un servidor ESXi si tiene la intención de utilizar el dispositivo virtual Panorama para lo siguiente:

- Gestionar su implementación de SD-WAN en modo Panorama.
- Requerir espacio de almacenamiento adicional para actualizaciones dinámicas cuando gestione implementaciones de cortafuegos a gran escala.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en un servidor ESXi según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en un servidor ESXi.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.
- Para implementaciones de SD-WAN.
  1. Aumento del disco del sistema para Panorama en un servidor ESXi

     Para aprovechar SD-WAN en Panorama implementado en ESXi, debe aumentar el disco del sistema a 224 GB.

     No puede volver a migrar a un disco del sistema de 81 GB después de haber aumentado correctamente el disco del sistema a 224 GB.
  2. Configure un dispositivo virtual Panorama en modo Solo gestión.
  3. Cómo añadir un disco virtual a Panorama en un servidor ESXi.

     Para aprovechar SD-WAN, debe agregar un solo disco de creación de logs de 2TB a Panorama en el modo Solo gestión.

Instalación de Panorama en vCloud Air

Utilice estas instrucciones para instalar un nuevo dispositivo virtual Panorama en VMware vCloud Air. Si está actualizando un dispositivo virtual Panorama implementado en vCloud Air, continúe con Instalación de actualizaciones de contenido y software de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Descargue el archivo del dispositivo virtual abierto (OVA) de la imagen básica de Panorama 10.2.

1. Visite el sitio de descargas de software de Palo Alto Networks. (Si no puede iniciar sesión, visite el sitio web de Atención al cliente de Palo Alto Networks para obtener asistencia).
2. En la columna Download (Descargar) en la sección Panorama Base Images (Imágenes básicas de Panorama), descargue el archivo OVA de Panorama 10.2 (`Panorama-ESX-10.0.0.ova`).

STEP 2 | Importe la imagen de Panorama al catálogo de vCloud Air.

Para obtener más detalles sobre estos pasos, consulte la Guía de usuario de la herramienta OVF.

1. Instale la herramienta OVF en su sistema de cliente.
2. Acceda a la CLI del sistema de cliente.
3. Diríjase al directorio de la herramienta OVF (por ejemplo C:\Program Files\VMware \VMware OVF Tool).
4. Convierta el archivo OVA en un paquete OVF:

```
ovftool.exe <OVA-file-pathname> <OVF-file-pathname>
```

5. Use un navegador para acceder a la consola web de vCloud Air, seleccione la ubicación de **Virtual Private Cloud OnDemand (Nube privada virtual a petición)** y registre la URL del navegador. Utilizará la información de la URL para completar el siguiente paso. El formato de la URL es: **`https://<virtual-cloud-location>.vchs.vmware.com/compute/cloud/org/<vCloud-account-number>/#/catalogVAppTemplateList?catalog=<catalog-ID>`**.
6. Importe el paquete OVF, utilizando la información de la URL de vCloud Air para completar las variables <virtual#cloud#location>, <vCloud#account#number> y <catalog#ID>. Las otras variables son su nombres de usuario y dominio de <user>@<domain>, un centro de datos virtual <datacenter> y una plantilla de vCloud Air <template>.

```
ovftool.exe -st="OVF" "<OVF-file-pathname>"
 "vcloud://<user>@<domain>:password@<virtual-cloud-
location>.vchs.vmware.com?vdc=<datacenter>&org=<vCloud-
account-number>&vappTemplate=<template>.ovf&catalog=default-
catalog"
```


©2023 Palo Alto Networks, Inc.

STEP 3 | Instale Panorama.

1. Acceda a la consola web de vCloud Air y seleccione su región de **Virtual Private Cloud OnDemand (Nube privada virtual a petición)**.
2. Cree una máquina virtual Panorama. Para obtener los pasos, consulte Añadir una máquina virtual desde una plantilla en el centro de documentación de vCloud Air. Configure **CPU**, **Memory (Memoria)** y **Storage (Almacenamiento)** de la siguiente manera:
   - Configure la **CPU** y la **memoria** según el modo de dispositivo virtual: consulte Requisitos previos de configuración del dispositivo virtual Panorama.
   - Establezca el **almacenamiento** para configurar el disco del sistema del dispositivo virtual de Panorama. Consulte Requisitos previos de configuración del dispositivo virtual Panorama para conocer los tamaños de disco admitidos según el modo de dispositivo virtual de Panorama. Para obtener un mejor rendimiento de la creación de logs e informes, seleccione la opción **SSD-Accelerated (Acelerado por SSD)**.

     Para aumentar la capacidad de almacenamiento de logs, debe Añadir un disco virtual a Panorama en vCloud Air. En el modo Panorama, el dispositivo virtual no utiliza el disco del sistema para el almacenamiento de logs; debe añadir un disco de logs virtual.

STEP 4 | Cree reglas NAT de vCloud Air en la puerta de enlace para permitir el tráfico entrante y saliente para el dispositivo virtual Panorama.

Consulte Añadir una regla NAT en el centro de documentación de vCloud Air para obtener instrucciones detalladas:

1. Añada una regla NAT que permita que Panorama reciba tráfico de los cortafuegos y que los administradores accedan a Panorama.
2. Añada una regla NAT que permita que Panorama obtenga actualizaciones del servidor de actualizaciones de Palo Alto Networks y acceda a los cortafuegos.

STEP 5 | Cree una regla de cortafuegos de vCloud Air para permitir el tráfico entrante en el dispositivo virtual Panorama.

El tráfico saliente está permitido de manera predeterminada.

Consulte Añadir una regla de cortafuegos en el Centro de documentación de vCloud Air para obtener instrucciones detalladas.

STEP 6 | Encienda el dispositivo virtual Panorama si no está activado.

En la consola web de vCloud Air, seleccione la pestaña **Virtual Machines (Máquinas virtuales)**, seleccione la máquina virtual Panorama y haga clic en **Power On (Encender)**.

Ahora está listo para realizar la configuración inicial del dispositivo virtual Panorama.

Compatibilidad para herramientas VMware en el dispositivo virtual Panorama.

VMware Tools incluye la imagen de software (ovf) para el dispositivo virtual Panorama. La compatibilidad para las herramientas VMware le permite usar el entorno de vSphere (vCloud Director y servidor vCenter) para lo siguiente:

- Visualice la dirección IP asignada a la interfaz de gestión de Panorama.
- Visualice las métricas de uso de recursos en el disco duro, la memoria y el CPU. Puede usar estas métricas para habilitar alarmas o acciones en el servidor vCenter o vCloud Director.

 ©2023 Palo Alto Networks, Inc.

- Cierre y reinicio ordenados de Panorama con la función de apagado en el servidor vCenter o vCloud Director.
- Permite un mecanismo de latidos entre el servidor vCenter y Panorama para verificar que este último funcione, o si el cortafuegos o Panorama se reinician. Si el cortafuegos pasa al modo de mantenimiento, los latidos se deshabilitan de modo que el servidor vCenter no apaga el cortafuegos. Si deshabilita los latidos, permite que el cortafuegos siga funcionando en modo de mantenimiento cuando no puede enviar controles periódicos al servidor vCenter.

Configuración de Panorama en Alibaba Cloud

Configure un dispositivo virtual Panorama™ en Alibaba Cloud para administrar de forma centralizada la configuración de los cortafuegos físicos y VM-Series.

- Cómo cargar la imagen del dispositivo virtual Panorama en Alibaba Cloud
- Instalación de Panorama en Alibaba Cloud

Cómo cargar la imagen del dispositivo virtual Panorama en Alibaba Cloud

Complete el siguiente procedimiento para cargar un archivo qcow2 del servidor de gestión Panorama para KVM y cree la imagen personalizada que necesita para iniciar el dispositivo virtual Panorama. Cargar y crear la imagen solo es necesario una vez. Puede utilizar la misma imagen para todas las implementaciones posteriores del dispositivo virtual Panorama.

STEP 1 | Descargue el archivo qcow2 de Panorama para KVM desde el Portal de atención al cliente (CSP) de Palo Alto Networks.

1. Inicie sesión en el CSP de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y **Panorama Base Images (Imágenes básicas de Panorama)** en el menú desplegable de filtros de actualizaciones de software.
3. Descargue la última versión del archivo qcow2 de `Panorama-KVM`.

STEP 2 | Inicie sesión en Alibaba Cloud Console.

STEP 3 | Cree un depósito de Servicio de almacenamiento de objetos (OSS) para la imagen del dispositivo virtual Panorama.

1. En el menú de Alibaba Cloud, seleccione **Object Storage Service (Servicio de almacenamiento de objetos)** > **Buckets (Depósitos)** y **Create Bucket (Crear depósito)**.
2. Introduzca un nombre descriptivo en **Bucket Name (Nombre de depósito)**.
3. En **Region (Región)**, seleccione la región del depósito.

   Esta región debe estar en la misma que planea implementar el dispositivo virtual Panorama y en la misma que los cortafuegos que planea gestionar con Panorama.
4. Configure los ajustes restantes del depósito de OSS según sea necesario.
5. Haga clic en **OK (Aceptar)**.

   Se lo redirigirá a la página de descripción general del depósito de OSS después de una creación exitosa.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Cargue el archivo qcow2 en el depósito de OSS.

1. En la Descripción general del depósito de OSS, seleccione **Files (Archivos)** y **Upload (Cargar)** para cargar el archivo qcow2 que descargó en el paso anterior.
2. En el destino **Upload To (Cargar a)**, seleccione **Current (Actual)**.
3. En **File ACL (ACL de archivo)**, seleccione **Inherited from Bucket (Heredado del depósito)**.
4. Haga clic en **Select Files (Seleccionar archivos)** y seleccione el archivo qcow2.

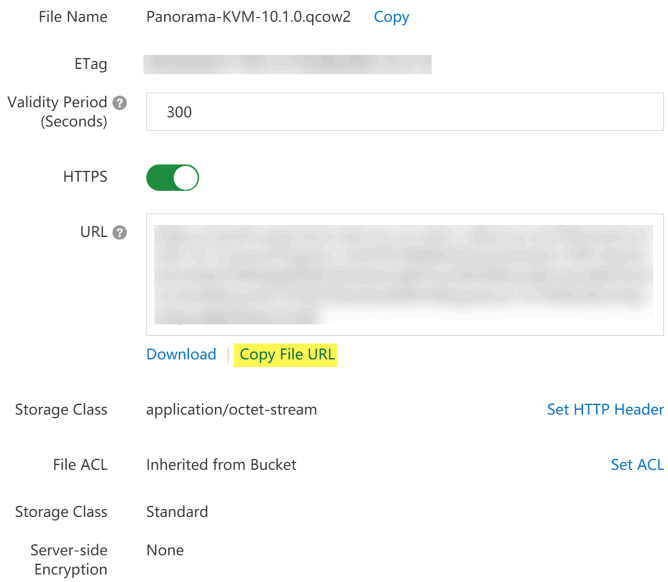
   O bien, puede arrastrar y soltar el archivo qcow2 en la sección **Files to Upload (Archivos para cargar)**.
5. Haga clic en **Upload (Cargar)** para cargar el archivo qcow2.

   Aparece la ventana "Task List " (Lista de tareas) que muestra el estado de carga. Continúe con el siguiente paso después de que el estado de carga del archivo qcow2 en **Status (Estado)** muestre **Uploaded (Cargado)**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Convierta el archivo qcow2 en una imagen que se pueda iniciar.

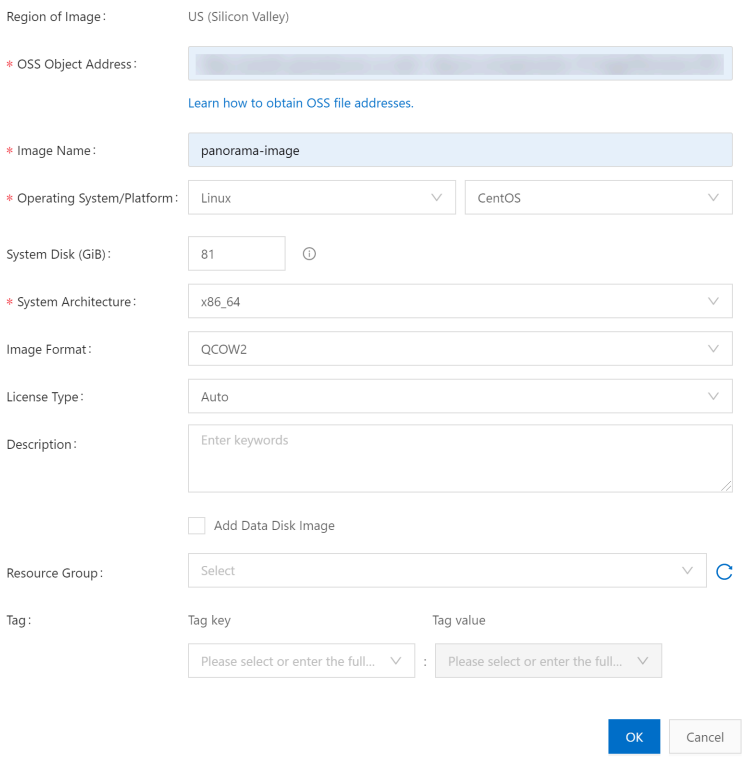
1. En la Descripción general del depósito de OSS, seleccione **Files (Archivos)** y haga clic en el archivo qcow2 que cargó para ver los detalles del archivo.
2. Haga clic en **Copy File URL (Copiar URL del archivo)** y salga de los detalles del archivo.



3. En el menú de Alibaba Cloud, seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Images (Imágenes)** e **Import Image (Importar imagen)**.
4. Pegue la dirección de **OSS Object Address (Dirección del objeto OSS)** para el archivo qcow2.

   Esta es la URL del archivo que copió en el paso anterior.
5. Introduzca un nombre en **Image Name (Nombre de imagen)**.
6. En **Operating System/Platform (Plataforma o sistema operativo)**, seleccione **Linux CentOS**.
7. En **System Disk (GiB) (Disco del sistema [GiB])**, ingrese **81**.
8. En **System Architecture (Arquitectura del sistema)**, seleccione **x86_64**.
9. En **Image Format (Formato de imagen)**, seleccione **QCOW2**.
10. Haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.



Instalación de Panorama en Alibaba Cloud

Utilice Elastic Compute Service (ECS) para crear una instancia de dispositivo virtual Panorama™ en Alibaba Cloud. Una instancia de ECS es compatible con una única NIC de forma predeterminada y una interfaz de red elástica (ENI) adjunta automáticamente. Debe cargar manualmente una imagen qcow2 del dispositivo virtual Panorama descargada del Portal de atención al cliente (CSP) de Palo Alto Networks a Alibaba Cloud para instalar correctamente el dispositivo virtual Panorama en Alibaba Cloud.

El dispositivo virtual Panorama que se implementó en Alibaba Cloud es de tipo traiga su propia licencia (BYOL), admite todos los modos de implementación (Panorama, recopilador de logs y solo gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware M-Series. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

Revise Requisitos previos de configuración del dispositivo virtual Panorama para determinar el tipo de instancia de Elastic Computer Service (ECS) correcto para sus necesidades. El requisito de recursos virtuales para el dispositivo virtual Panorama se basa en la cantidad total de cortafuegos gestionados por el dispositivo virtual Panorama y los Logs por segundo (LPS) necesarios para reenviar logs de los cortafuegos gestionados al recopilador de logs.

Palo Alto Networks admite los siguientes tipos de instancia.

- `ecs.g5.xlarge`, `ecs.g5.2xlarge`, `ecs.g5.4xlarge`
- `ecs.sn2ne.xlarge`, `ecs.sn2ne.2xlarge`, `ecs.sn2ne.4xlarge`

El aprovisionamiento insuficiente del dispositivo virtual Panorama afectará al rendimiento de la gestión. Esto incluye que el dispositivo virtual Panorama se vuelva lento o no responda en función del aprovisionamiento insuficiente del dispositivo virtual Panorama.

©2023 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en Alibaba Cloud Console.

STEP 2 | Cómo cargar la imagen del dispositivo virtual Panorama en Alibaba Cloud.

STEP 3 | Configure la nube privada virtual (VPC) para sus necesidades de red.

Tanto si inicia el dispositivo virtual Panorama en una VPC existente o crea una nueva VPC, el dispositivo virtual Panorama debe poder recibir tráfico desde las instancias en la VPC y realizar comunicaciones de entrada y salida entre la VPC e internet según sea necesario.

Consulte la documentación de la VPC de Alibaba Cloud para obtener más información.

1. Cree una VPC y configure redes o utilice una VPC existente.
2. Compruebe que los componentes de red y seguridad estén definidos adecuadamente.
   - Cree una puerta de enlace de Internet para permitir el acceso a Internet a la subred de su dispositivo virtual Panorama. Se requiere acceso a Internet para instalar actualizaciones de contenido y software, activar licencias y aprovechar los servicios en la nube de Palo Alto Networks. De lo contrario, debe instalar las actualizaciones y activar las licencias manualmente.
   - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de Alibaba Cloud. Se recomienda que el dispositivo virtual Panorama pertenezca a la subred de gestión de modo que pueda configurarlo para acceder a Internet si es necesario.
   - Añada rutas a la tabla de enrutamiento de una subred privada a fin de garantizar que el tráfico se pueda dirigir a través de subredes en la VPC y desde Internet, según corresponda.

     Asegúrese de crear rutas entre subredes para permitir la comunicación entre:

     - Panorama, cortafuegos gestionados y recopiladores de logs.
     - (Opcional) Panorama e Internet.
   - Asegúrese de que las siguientes reglas de seguridad de entrada estén permitidas para que la VPC administre el tráfico de VPC. La fuente de tráfico de entrada para cada regla es única para su topología de implementación.

     Consulte Puertos utilizados para Panorama para obtener más información.

     - Permita el tráfico SSH (puerto **22**) para permitir el acceso a la CLI de Panorama.
     - Permita el tráfico HTTPS (puerto **443** y **27280**) para permitir el acceso a la interfaz web de Panorama.
     - Permita el tráfico en el puerto **3978** para habilitar la comunicación entre Panorama, administrar cortafuegos y recopiladores de logs gestionados. Los recopiladores de logs también utilizan este puerto para reenviar logs a Panorama.
     - Permita el tráfico en el puerto **28443** para permitir que los cortafuegos gestionados obtengan actualizaciones de software y contenido de Panorama.

STEP 4 | Seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Instances (Instancias)** y haga clic en **Create Instance (Crear instancia)** en la esquina superior derecha.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Cree la instancia del dispositivo virtual Panorama.

1. Seleccione **Custom Launch (Inicio personalizado)**.
2. Configure la instancia del dispositivo virtual Panorama.
   - **Billing Method (Método de facturación)**: seleccione el método de suscripción deseado para la instancia.
   - **Region (Región)**: seleccione una región de su elección. La región que seleccione debe proporcionar uno de los tipos de instancia admitidos.
   - **Instance Type (Tipo de instancia)**: seleccione uno de los tipos de instancia admitidos. Puede elegir la selección basada en tipo para buscar el tipo de instancia.
   - **Image (Imagen)**: seleccione **Custom Image (Imagen personalizada)** y seleccione la imagen del dispositivo virtual Panorama que cargó.
   - **Storage (Almacenamiento)**: elija un tipo de disco e introduzca **81**GiB como capacidad del disco del sistema.
   - (Opcional) **Add Disk (Agregar disco)**: añada discos de creación de logs adicionales.

     Si desea utilizar el dispositivo virtual Panorama en modo Panorama o como un recopilador de logs dedicado, añada los discos virtuales de logging durante la implementación inicial. De manera predeterminada, el dispositivo virtual Panorama se encuentra en modo Panorama para la implementación inicial cuando cumple con los requisitos de recursos del modo Panorama y añadió, al menos, un disco virtual de logging. De lo contrario, los valores del dispositivo virtual Panorama vuelven al valor predeterminado en modo solo de gestión. Cambie el modo del dispositivo virtual Panorama al modo solo de gestión si desea gestionar dispositivos y recopiladores de logs dedicados, y no desea recopilar logs localmente.

     El dispositivo virtual Panorama en Alibaba Cloud solo admite discos de creación de logs de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging con menos de 2 TB o un disco de logging con un tamaño que no sea divisible por los 2 TB del requisito para discos de logging. El dispositivo virtual Panorama divide los discos de logging con más de 2 TB en particiones de 2 TB.
   - (Opcional) **Snapshot (Instantánea)**: especifique la frecuencia con la que se toma automáticamente una instantánea de la instancia del dispositivo virtual Panorama para evitar riesgos y la eliminación accidental de datos.
   - **Duration (Duración)**: especifique la duración de la instancia del dispositivo virtual Panorama.

STEP 6 | Configure las opciones de red del dispositivo virtual Panorama.

1. Seleccione **Siguiente: Redes**.
2. Configure las opciones de red de la instancia del dispositivo virtual Panorama.
   - **Network Type (Tipo de red)**: seleccione la VPC y vSwitch de gestión que creó.
   - **Public IP Address (Dirección IP pública)**: si no tiene una dirección IP pública, habilite (marque) **Assign Public IPv4 Address (Asignar dirección IP IPv4 pública)** y se asigna

 ©2023 Palo Alto Networks, Inc.

automáticamente una dirección IPv4 pública a la instancia del dispositivo virtual Panorama.

Si debe utilizar una dirección IP específica o una dirección en un rango específico, puede solicitar una dirección IP personalizada. Consulte la Guía del usuario de direcciones IP elásticas.

- **Security Group (Grupo de seguridad)**: seleccione el grupo de seguridad de administración que creó y habilite el **puerto 443 (HTTPS)**, el **puerto 22** y el **puerto 3389.**
- **Elastic Network Interface (Interfaz de red elástica)**: no necesita configuración. La interfaz de gestión ya está adjunta a eth0.

STEP 7 | Configure las opciones del sistema de la instancia del dispositivo virtual Panorama.

1. Seleccione **Siguiente: Configuraciones del sistema**.
2. Configure las opciones del sistema de la instancia del dispositivo virtual Panorama.
   - **Logon Credentials (Credenciales de inicio de sesión)**: seleccione **Key Pair (Par de claves)** y elija el par de claves. Si aún no se ha creado un par de claves, seleccione **Create Key Pair (Crear par de claves)** para crear un nuevo par en Alibaba Cloud o importar un par existente.

     No se admite la autenticación de contraseña.

   - **Instance Name (Nombre de instancia)**: introduzca un nombre descriptivo para el dispositivo virtual Panorama. Este es el nombre que se muestra para la instancia en Alibaba Cloud Console.
   - **Host**: escriba un nombre de host para la instancia del dispositivo virtual Panorama.

STEP 8 | (Opcional) Seleccione **Next: Grouping (Siguiente: Agrupación)** para configurar la agrupación de todos los recursos de Alibaba Cloud asociados con la instancia del dispositivo virtual Panorama.

STEP 9 | Seleccione **Preview (Vista previa)** para ver la configuración antes de realizar el pedido.

STEP 10 | Vea y consulte las **Condiciones del servicio de ECS** y las **Condiciones del servicio del producto**.

STEP 11 | **Create Instance (Crear instancia)** para crear la instancia del dispositivo virtual Panorama.

Cuando se le solicite, haga clic en **Console (Consola)** para ver el estado de creación de la instancia.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Asigne las direcciones IP elásticas (EIP).

La EIP es una dirección IP pública que se utiliza para conectarse al dispositivo virtual Panorama.

Este paso solo es necesario si desea habilitar el acceso a Internet para el dispositivo virtual Panorama.

1. Seleccione **Elastic Compute Service** > **Network & Security (Red y seguridad)** > **VPC** > **Elastic IP Addresses (Direcciones IP elásticas)** > **Elastic IP Addresses (Direcciones IP elásticas)**.

   Seleccione **Create EIP (Crear EIP)** si no tiene ninguna EIP existente.
2. En la columna **Actions (Acciones)**, seleccione **Bind Resource (Enlazar recurso)** para enlazar una EIP a cualquier interfaz expuesta a Internet.

STEP 13 | Inicio de sesión en la CLI de Panorama con el SSH para configurar las opciones de red del dispositivo virtual Panorama.

Debe configurar la contraseña de `administración`, la dirección IP del sistema, la máscara de red y la puerta de enlace predeterminada. Además, debe añadir los servidores DNS de Alibaba Cloud para conectarse correctamente al servidor de actualización de Palo Alto Networks.

*También puede acceder a la CLI de Panorama desde la consola de Alibaba. Para acceder a la CLI de Panorama desde la consola de Alibaba, seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Instances (Instancias)** y elija la instancia del dispositivo virtual Panorama. En Instance Details (Detalles de la instancia), seleccione **Connect (Conectar)**.*

Se le pedirá que cree una contraseña de VCN para la instancia del dispositivo virtual Panorama en la primera conexión desde la VCN de Alibaba. Asegúrese de guardar esta contraseña, ya que no se puede recuperar y es necesaria para conectarse con la VCN o para actualizar la contraseña en el futuro.

STEP 14 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web o la CLI del dispositivo virtual Panorama. Para acceder a la CLI, se requiere la clave privada utilizada para iniciar el dispositivo virtual de Panorama.

La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúscula, un carácter en mayúscula y un número o carácter especial.

Configure una nueva contraseña usando los siguientes comandos y siga las indicaciones en pantalla:

```
admin> configure admin# set mgt-config users admin password
```

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Configure las opciones de red iniciales para el dispositivo virtual Panorama.

```
admin> configure
```

```
admin#  set deviceconfig system type static
```

```
admin#  set deviceconfig system ip-address <instance-private-IP
 address> netmask <netmask> default-gateway <default-gateway-IP>
```

La puerta de enlace predeterminada en Alibaba Cloud termina en ***.253****. Por ejemplo, si la dirección IP privada de la instancia del dispositivo virtual Panorama es 192.168.100.20, la puerta de enlace predeterminada es 192.168.100.253.*

```
admin#  set deviceconfig system dns-setting servers primary
 100.100.2.136
```

```
admin#  set deviceconfig system dns-setting servers secondary
 100.100.2.138
```

```
admin# commit
```

STEP 16 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.
2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.
3. Active una licencia de gestión de cortafuegos.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.
4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 17 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- (Modo de Solo gestión) Configuración de un dispositivo virtual Panorama en modo solo de gestión.
- (Modo recopilador de logs) Comience en el paso 6 para realizar el Cambio del modo Panorama al modo de recopilación de logs.

  ***Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión de Panorama. No puede especificar la* IP Address (Dirección IP), Netmask (Máscara de red) *o* Gateway (Puerta de enlace).**

- (En Panorama en modo de solo gestión) Realice el procedimiento Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama. El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

STEP 18 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en Alibaba Cloud según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     ***Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la* IP Address (Dirección IP), Netmask (Máscara de red) *o* Gateway (Puerta de enlace).**

- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en Alibaba Cloud según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

 ©2023 Palo Alto Networks, Inc.

Instalación de Panorama en AWS

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en Amazon Web Services (AWS). El modelo que implementó Panorama en AWS es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware serie M. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

STEP 1 | Inicie sesión en la consola de Amazon Web Service (AWS) y seleccione el panel EC2.

- Consola de Amazon Web Services
- Consola de AWS GovCloud Web Service

STEP 2 | Configure la nube privada virtual (VPC) para sus necesidades de red.

Tanto si inicia el dispositivo virtual Panorama en una VPC existente o crea una nueva VPC, el dispositivo virtual Panorama debe poder recibir tráfico desde las instancias en la VPC y realizar comunicaciones de entrada y salida entre la VPC e internet según sea necesario.

Consulte las instrucciones para crear una VPC y configurar el acceso a esta en la documentación de la VPC de AWS.

1. Cree una nueva VPC o use una existente. Consulte la documentación de la Guía de inicio de AWS.
2. Compruebe que los componentes de red y seguridad estén definidos adecuadamente.
   - Cree una puerta de enlace de Internet para permitir el acceso a Internet a la subred de su dispositivo virtual Panorama. Se requiere acceso a Internet para instalar actualizaciones de contenido y software, activar licencias y aprovechar los servicios en la nube de Palo Alto Networks. De lo contrario, debe instalar las actualizaciones y activar las licencias manualmente.
   - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de AWS. Se recomienda que el dispositivo virtual Panorama pertenezca a la subred de gestión de modo que pueda configurarlo para acceder a Internet si es necesario.
   - Añada rutas a la tabla de enrutamiento de una subred privada a fin de garantizar que el tráfico se pueda dirigir a través de subredes en la VPC y desde Internet, según corresponda.

     Asegúrese de crear rutas entre subredes para permitir la comunicación entre:

     - Panorama, cortafuegos gestionados y recopiladores de logs.
     - (Opcional) Panorama e Internet.

 ©2023 Palo Alto Networks, Inc.

- Asegúrese de que las siguientes reglas de seguridad entrantes estén permitidas para que la VPC administre el tráfico de VPC. La fuente de tráfico de entrada para cada regla es única para su topología de implementación.

  Consulte Puertos utilizados para Panorama para obtener más información.

  - Permita el tráfico SSH (puerto **22**) para permitir el acceso a la CLI de Panorama.
  - Permita el tráfico HTTPS (puerto **443**) para permitir el acceso a la interfaz web de Panorama.
  - Permita el tráfico en el puerto **3978** para habilitar la comunicación entre Panorama, administrar cortafuegos y recopiladores de logs gestionados. Los recopiladores de logs también utilizan este puerto para reenviar logs a Panorama.
  - Permita el tráfico en el puerto **28443** para permitir que los cortafuegos gestionados obtengan actualizaciones de software y contenido de Panorama.

STEP 3 | Implemente Panorama en Amazon Web Services.

1. Seleccione **Services (Servicios)** > **EC2** > **Instances (Instancias)** y **Launch Instance (Iniciar instancia)**.
2. Seleccione **AWS Marketplace (Mercado de AWS)**, busque **`Palo Alto Networks Panorama`**, haga clic en **Select (Seleccionar)** para seleccionar la AMI de Panorama y haga clic en **Continue (Continuar)**.
3. Elija el **EC2 instance type (Tipo de instancia de EC2)** para asignar los recursos requeridos para el dispositivo virtual Panorama y haga clic en **Next: Configure Instance Details (Siguiente: Configuración de los detalles de la instancia)**. Para saber los requisitos de recursos, consulte Requisitos previos de configuración del dispositivo virtual Panorama.

   Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar el dispositivo con los recursos necesarios durante la implementación inicial. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.
4. Configure los detalles de la instancia.

   1. Seleccione **Siguiente: Configure Instance Details (Siguiente: Configuración de los detalles de la instancia)**.
   2. En **Network (Red)**, seleccione la VPC.
   3. Seleccione la **Subnet (Subred)**.
   4. Para **asignar automáticamente una IP pública**, seleccione **Enable (Habilitar)**.

      Debe ser posible acceder a la IP desde los cortafuegos que desea gestionar con Panorama. Esto le permite obtener una dirección IP de acceso público para la interfaz de gestión del dispositivo virtual Panorama. Luego, puede adjuntar una dirección IP elástica para la interfaz de gestión. A diferencia de la dirección IP pública, que deshace la asociación con el dispositivo virtual cuando se finaliza la instancia, la dirección IP elástica ofrece continuidad y puede adjuntar la dirección IP a una instancia nueva (o sustituta) del dispositivo virtual Panorama sin necesidad de volver a configurar la dirección IP aunque la instancia del dispositivo virtual Panorama esté apagada.

 ©2023 Palo Alto Networks, Inc.

5. Configure la información adicional de la instancia según sea necesario.

5. (Opcional) Configure el almacenamiento del dispositivo virtual Panorama.

   1. Seleccione **Siguiente: Añada almacenamiento**.
   2. **Añada un nuevo volumen** para agregar almacenamiento de registro adicional.

      (Solo SD-WAN) Si piensa gestionar la implementación de SD-WAN en modo Management Only (Solo gestión), debe agregar un disco de creación de logs de 2 TB.

      Si desea utilizar el dispositivo virtual Panorama en modo Panorama o como un recopilador de logs dedicado, añada los discos virtuales de logging durante la implementación inicial. De manera predeterminada, el dispositivo virtual Panorama se encuentra en modo Panorama para la implementación inicial cuando cumple con los requisitos de recursos del modo Panorama y añadió, al menos, un disco virtual de logging. De lo contrario, los valores del dispositivo virtual Panorama vuelven al valor predeterminado en modo solo de gestión. Cambie el modo del dispositivo virtual Panorama al modo solo de gestión si desea gestionar dispositivos y recopiladores de logs dedicados, y no desea recopilar logs localmente.

      El dispositivo virtual Panorama en AWS admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging con menos de 2 TB o un disco de logging con un tamaño que no sea divisible por los 2 TB del requisito para discos de logging. El dispositivo virtual Panorama divide los discos de logging con más de 2 TB en particiones de 2 TB.

6. (Opcional) Seleccione **Next: Add Tags (Siguiente: añadir etiquetas)** y agregue una o más etiquetas como metadatos para permitirle identificar y agrupar el dispositivo virtual Panorama. Por ejemplo, añada una etiqueta de **Name (Nombre)** con un **Value (Valor)** que le ayude a identificar qué cortafuegos gestiona el dispositivo virtual Panorama.

7. Configure el grupo de seguridad de la instancia.

   1. Seleccione **Siguiente: Configure el grupo de seguridad**.
   2. **Seleccione un grupo de seguridad existente** para asignar un grupo de seguridad de la instancia del dispositivo virtual Panorama.
   3. Seleccione el grupo de seguridad que creó anteriormente.

      Puede seleccionar el grupo de seguridad `default (predeterminado)` para permitir todos los tipos de tráfico entrante y saliente.

8. **Revise e inicie** la instancia del dispositivo virtual Panorama para verificar que sus selecciones sean precisas antes del **inicio**.

9. Seleccione un par de claves existente o cree uno nuevo y acepte el descargo de responsabilidad.

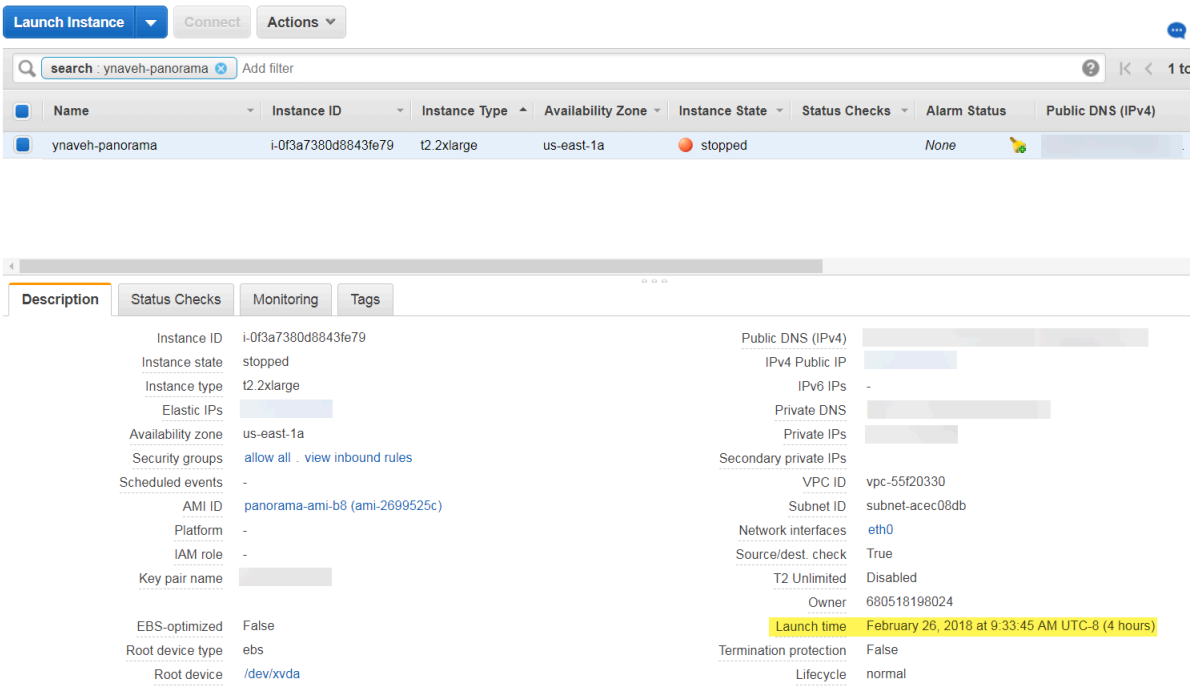
   

   Si creó una clave nueva desde AWS, descargue y guarde la clave en una ubicación segura. La extensión del archivo es `.pem`. Debe cargar la clave pública en PuTTYgen y guardarla en formato `.ppk`. Si pierde la clave, no se puede volver a regenerar.

   Llevará aproximadamente 30 minutos completar la implementación del dispositivo virtual Panorama después de iniciarlo en AWS. Es posible que la implementación del dispositivo virtual Panorama lleve más tiempo según el número y el tamaño de los discos adjuntos a

 ©2023 Palo Alto Networks, Inc.

la instancia. Visualice el tiempo de inicio seleccionando la instancia del dispositivo virtual Panorama (**Instances [Instancias]**).



Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de suministrarle el dispositivo los recursos necesarios. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.

STEP 4 | Apague el dispositivo virtual Panorama.

1. En el panel EC2, seleccione **Instances (Instancias)**.
2. Seleccione el dispositivo virtual Panorama y haga clic en **Instance State (Estado de instancia)** > **Stop Instance (Detener instancia)**.

STEP 5 | Cree o asigne una dirección IP elástica (Elastic IP, EIP) a la interfaz de gestión.

1. Seleccione **Services (Servicios)** > **EC2** > **Elastic IPs (IP elásticas)** y **Allocate Elastic IP address (Asignar dirección IP elástica)**.
2. Seleccione **Network Border Group (Grupo de borde de red)**para especificar el grupo lógico de zonas desde donde se anuncia la dirección IP4v pública.
3. Para el grupo de direcciones IPv4 públicas, seleccione **Amazon's pool of IPv4 addresses (Grupo de direcciones IPv4 de Amazon)**.
4. Seleccione **Allocate (Asignar)** para asignar la EIP.
5. Haga clic en la dirección IPv4 en la columna "Allocated IPv4 address" (Dirección IPv4 asignada) y en **Associate Elastic IP address (Asociar dirección IP elástica)**.
6. Seleccione la **Instance (Instancia)** del dispositivo virtual Panorama.
7. Seleccione la **Private IP address (Dirección IP privada)** del dispositivo virtual Panorama a la que asociar la EIP.

©2023 Palo Alto Networks, Inc.

STEP 6 | Active el dispositivo virtual Panorama.

1. En el panel EC2, seleccione **Instance (Instancia)**.
2. En la lista, seleccione el dispositivo virtual Panorama y haga clic en **Actions (Acciones)** > **Instance State (Estado de la instancia)** > **Start (Iniciar)**.

©2023 Palo Alto Networks, Inc.

STEP 7 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web del dispositivo virtual Panorama. Para acceder a la CLI, es necesaria la clave privada utilizada para iniciar el dispositivo virtual Panorama.

La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

- Si cuenta con un servidor SSH instalado en su ordenador:
  1. Introduzca el siguiente comando para iniciar sesión en el dispositivo virtual Panorama:

     ```
     ssh -i <private_key.ppk> admin@<public-ip_address>
     ```

  2. Configure una nueva contraseña utilizando los siguientes comandos y siga las indicaciones en la pantalla:

     ```
     admin> configure admin# set mgt-config users admin password
     ```

  3. Si debe activar una BYOL, establezca la dirección IP del servidor DNS de modo que el dispositivo virtual Panorama pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

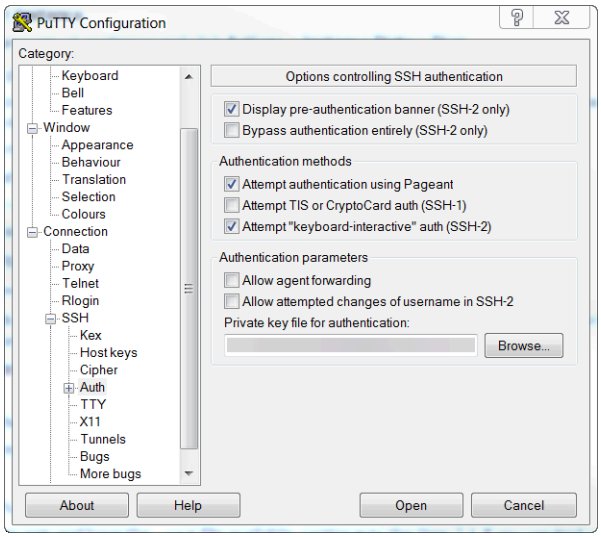
     ```
     admin# set deviceconfig system dns-setting servers
      primary <ip_address>
     ```

  4. Confirme los cambios con el comando:

     ```
     admin# commit
     ```

  5. Finalice la sesión SSH.
- Si está utilizando PuTTY para abrir una sesión SSH en el dispositivo virtual Panorama:
  1. Si está utilizando un par de claves existente y cuenta con el archivo `.ppk`, vaya al paso 7.3. Si creó un nuevo par de claves o solo cuenta con el archivo `.pem` del par de claves existente, abra PuTTYgen y haga clic en **Load (Cargar)** para cargar el archivo `.pem`.
  2. **Guarde la clave privada** en un destino local accesible.
  3. Abra PuTTY, seleccione **SSH** > **Auth** y haga clic en **Browse (Examinar)** para buscar el archivo `.ppk` que guardó en el paso anterior.

 ©2023 Palo Alto Networks, Inc.



4. Seleccione **Sessions (Sesiones)** e introduzca la dirección IP pública del dispositivo virtual Panorama. Haga clic en **Open (Abrir)** y en **Yes (Sí)** cuando aparezca el mensaje de seguridad.
5. Inicie sesión como admin cuando se le solicite.
6. Configure una nueva contraseña utilizando los siguientes comandos y siga las indicaciones en la pantalla:

```
admin> configure admin# set mgt-config users admin password
```

7. Configure la dirección IP del servidor DNS, de modo que el dispositivo virtual Panorama pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

```
admin# set deviceconfig system dns-setting servers
 primary <ip_address>
```

8. Confirme los cambios con el comando:

```
admin# commit
```

9. Finalice la sesión SSH.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.

2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.

3. Active una licencia de gestión de cortafuegos.

   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en AWS según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en AWS.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

Instalación de Panorama en AWS GovCloud

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en Amazon Web Services (AWS) GovCloud. AWS GovCloud es una región aislada de AWS que cumple los requisitos normativos y de cumplimiento de los organismos oficiales y los clientes de la Administración de EE. UU. El modelo que implementó Panorama en AWS GovCloud es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión). Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

Para proteger su cargas de trabajo que contienen todas las categorías de datos de Información controlada no clasificada (Controlled Unclassified Information, CUI) y datos disponibles al público orientados al gobierno en la región AWS GovCloud (EE. UU.), el dispositivo virtual Panorama proporciona las mismas funciones de seguridad en la nube pública AWS estándar en AWS GovCloud. El dispositivo virtual Panorama en AWS GovCloud y la nube pública estándar de AWS admiten las mismas funciones y capacidades.

Consulte los Requisitos previos de configuración del dispositivo virtual Panorama para revisar los tipos de instancia EC2 compatibles. Cuando esté preparado, consulte Instalación de Panorama en AWS para instalar el dispositivo virtual Panorama en AWS GovCloud.

 ©2023 Palo Alto Networks, Inc.

Consulte los siguientes procedimientos para añadir almacenamiento de registro de logs adicional a su dispositivo virtual Panorama o para aumentar los núcleos y la memoria de la CPU asignada:

- Cómo añadir un disco virtual a Panorama en AWS
- Aumento de CPU y memoria para Panorama en AWS

Instalación de Panorama en Azure

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en Microsoft Azure. El modelo que implementó Panorama en Azure es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware serie M. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

STEP 1 | Inicie sesión en el portal de Microsoft Azure.

STEP 2 | Configure la red virtual para sus necesidades de red.

Tanto si inicia el dispositivo virtual Panorama en una red virtual existente como si crea una nueva red virtual, el dispositivo virtual Panorama debe poder recibir tráfico de otras instancias de la red virtual y realizar comunicaciones entrantes y salientes entre la red virtual e Internet según sea necesario.

Consulte la documentación de Microsoft Azure Virtual Network para obtener más información.

1. Cree una red virtual o utilice una existente.
2. Compruebe que los componentes de red y seguridad estén definidos adecuadamente.
   - Cree una puerta de enlace NAT si desea habilitar solo el acceso saliente a Internet para la subred a la que pertenece el dispositivo virtual Panorama.
   - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de Microsoft Azure. Se recomienda que

 ©2023 Palo Alto Networks, Inc.

el dispositivo virtual Panorama pertenezca a la subred de gestión de modo que pueda configurarlo para acceder a Internet si es necesario.

- Añada rutas a la tabla de enrutamiento de una subred privada a fin de garantizar que el tráfico se pueda dirigir a través de subredes en la VPC y desde Internet, según corresponda.

  Asegúrese de crear rutas entre subredes para permitir la comunicación entre:

  - Panorama, cortafuegos gestionados y recopiladores de logs.
  - (Opcional) Panorama e Internet.
- Asegúrese de que las siguientes reglas de seguridad de entrada estén permitidas para que la VPC administre el tráfico de VPC. La fuente de tráfico de entrada para cada regla es única para su topología de implementación.

  Consulte Puertos utilizados para Panorama para obtener más información.

  - Permita el tráfico SSH (puerto **22**) para permitir el acceso a la CLI de Panorama.
  - Permita el tráfico HTTPS (puerto **443**) para permitir el acceso a la interfaz web de Panorama.
  - Permita el tráfico en el puerto **3978** para habilitar la comunicación entre Panorama, administrar cortafuegos y recopiladores de logs gestionados. Los recopiladores de logs también utilizan este puerto para reenviar logs a Panorama.
  - Permita el tráfico en el puerto **28443** para permitir que los cortafuegos gestionados obtengan actualizaciones de software y contenido de Panorama.

STEP 3 | Implemente el dispositivo virtual Panorama.

1. En el panel de Azure, seleccione **Virtual machines (Máquinas virtuales)** y haga clic en **Add (Añadir)** para añadir una nueva máquina virtual.
2. Busque Palo Alto Networks y seleccione la última imagen del dispositivo virtual Panorama.
3. Haga clic en **Create (Crear)** para crear el dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure el dispositivo virtual Panorama.

1. Seleccione su **Subscription (Suscripción)** de Azure.
2. Seleccione el **grupo de recursos** de Azure para que contenga todos sus recursos de instancia de Azure.
3. Introduzca un **nombre de máquina virtual** para el dispositivo virtual Panorama.
4. Seleccione la **región** para implementar el dispositivo virtual Panorama.
5. (Opcional) Seleccione las **opciones de disponibilidad**. Consulte Cómo utilizar los conjuntos de disponibilidad para obtener más información.
6. Seleccione la **imagen** utilizada para implementar el servidor de gestión Panorama. **Explore todas las imágenes públicas y privadas** para implementar el servidor de gestión Panorama desde la imagen de Panorama en el mercado de Azure.
7. Configure el tamaño del dispositivo virtual Panorama. Para saber los requisitos de tamaño, consulte Requisitos previos de configuración del dispositivo virtual Panorama.

   Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar el dispositivo con los recursos necesarios durante la implementación inicial. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.
8. Configure las credenciales únicas de administrador del dispositivo virtual de Panorama.

   Debe configurar una contraseña administrativa única para poder acceder a la interfaz web y la CLI del dispositivo virtual Panorama.

   1. Introduzca un **Username (Nombre de usuario)** para el administrador del dispositivo virtual Panorama. Para garantizar que su nombre de usuario sea seguro, la palabra admin no es una opción válida.
   2. Introduzca una **Password (Contraseña)** o copie y pegue una **SSH public key (clave pública SSH)** para proteger el acceso administrativo al dispositivo virtual Panorama.

      Debe habilitar la autenticación de clave SSH si planea usar esta instancia del dispositivo virtual Panorama en el modo operativo FIPS-CC. Aunque puede implementar el dispositivo virtual Panorama con un nombre de usuario y una contraseña, no podrá autenticarse con ellos después de cambiar el modo operativo a FIPS-CC. Después del restablecimiento al modo FIPS-CC, debe usar la clave SSH para iniciar sesión y, continuación, podrá configurar un nombre de usuario y contraseña que podrá usar para iniciar sesión posteriormente en la interfaz web de Panorama. Para obtener detalles sobre la creación de la clave SSH, consulte la Documentación de Azure**.**
9. Configuración de la **red** de la instancia del dispositivo virtual Panorama

   1. Seleccione una **red virtual** existente o cree una nueva red virtual.
   2. Configure la **Subnet (Subred)**. La subred depende de la red virtual que seleccionó o creó en el paso anterior. Si seleccionó una red virtual existente, puede elegir una de las subredes para la red virtual seleccionada.
   3. Seleccione una **Public IP address (Dirección IP pública)** existente o cree una nueva. De esta manera, se crea la interfaz de gestión que se utiliza para acceder a su dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

4. Seleccione un **grupo de seguridad de red NIC** existente o cree un nuevo grupo de seguridad. Los grupos de seguridad de red controlan el tráfico a la máquina virtual. Asegúrese de que se permita HTTPS y SSH para las reglas entrantes.

10. Configure los ajustes de **gestión** de la instancia.
    1. Decida si desea habilitar el **Auto-shutdown (Apagado automático)**. La opción de apagado automático le permite configurar un periodo diurno para el apagado automático de la máquina virtual, de modo que pueda deshabilitar el apagado automático y evitar la posibilidad de que una nueva dirección IP pública se asigne a la máquina virtual, los logs se eliminen o no, o que no pueda gestionar sus cortafuegos mientras el dispositivo virtual Panorama esté apagado.
    2. Decida si desea habilitar la **supervisión** del arranque. Seleccione la cuenta de almacenamiento de diagnóstico si la opción se encuentra habilitada. El servicio de supervisión envía automáticamente logs de diagnóstico de arranque a su cuenta de almacenamiento de diagnósticos. Para obtener más información, consulte Descripción general de la supervisión en Microsoft Azure.
    3. Configure cualquier otra configuración si fuese necesario.
11. Revise el resumen, acepte los términos de uso y la política de privacidad, y haga clic en **Create (Crear)** para crear el dispositivo virtual Panorama.

STEP 5 | Verifique que el dispositivo virtual Panorama se haya implementado correctamente.

1. Seleccione **Dashboard (Panel)** > **Resource Groups (Grupos de recursos)** y seleccione el grupo de recursos al que pertenece el dispositivo virtual Panorama.
2. En Settings (Ajustes), seleccione **Deployments (Implementaciones)** para obtener información sobre el estado de implementación de la máquina virtual.

   Llevará aproximadamente 30 minutos implementar el dispositivo virtual Panorama. Es posible que iniciar el dispositivo virtual Panorama lleve más tiempo en función de los recursos configurados para la máquina virtual. Microsoft Azure no permite que el protocolo ICMP pruebe si se implementó correctamente.

   Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar correctamente el dispositivo con los recursos necesarios. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.

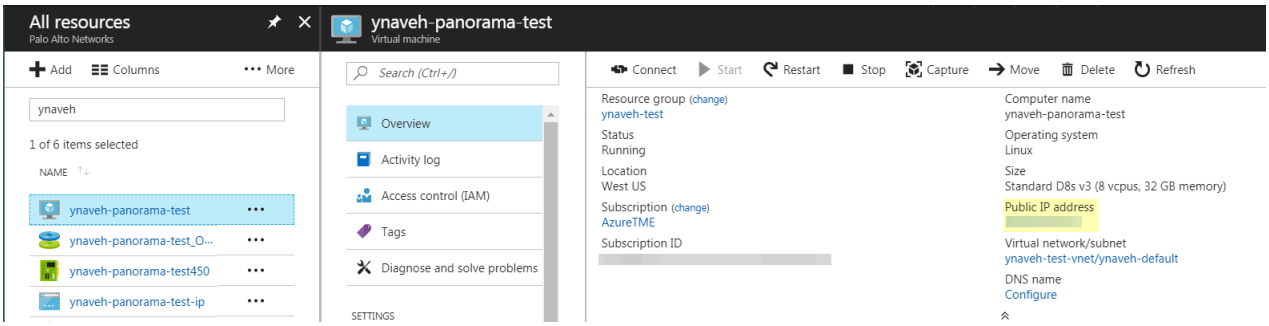
STEP 6 | Configure una dirección IP pública estática.

1. En el portal de Azure, seleccione **Virtual machines (Máquinas virtuales)** y seleccione el dispositivo virtual Panorama.
2. Seleccione **Overview (Descripción general)** y haga clic en **Public IP address (Dirección IP pública)**.
3. En Assignment (Asignación), seleccione **Static (Estático)** y haga clic en **Save (Guardar)** para guardar la nueva configuración de dirección IP.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Inicie sesión en la interfaz web del dispositivo virtual Panorama.

1. En el portal de Azure, en **All Resources (Todos los recursos)**, seleccione el dispositivo virtual Panorama y visualice la dirección IP pública en la sección Overview (Descripción general).



2. Utilice una conexión segura (https) desde su navegador web para iniciar sesión en el dispositivo virtual Panorama utilizando la dirección IP pública.
3. Introduzca el nombre de usuario y la contraseña para el dispositivo virtual Panorama. Aparecerá una advertencia de certificado. Acepte la advertencia de certificado y continúe a la página web.

STEP 8 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.
2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.
3. Active una licencia de gestión de cortafuegos.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.
4. Active una licencia de asistencia técnica de Panorama.

©2023 Palo Alto Networks, Inc.

STEP 9 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Añada un disco virtual a Panorama en Azure según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en Azure.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

Instalación de Panorama en Google Cloud Platform

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en Google Cloud Platform (GCP). El modelo que implementó Panorama en GCP es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware serie M. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

Para implementar el dispositivo virtual Panorama en GCP, debe generar una imagen personalizada. Para comenzar este proceso, debe descargar el archivo `tar.gz` de Panorama del portal de atención al cliente de Palo Alto Networks y cargarlo a un depósito de almacenamiento de GCP. Puede crear la imagen personalizada y usarla para implementar el dispositivo virtual Panorama en GCP.

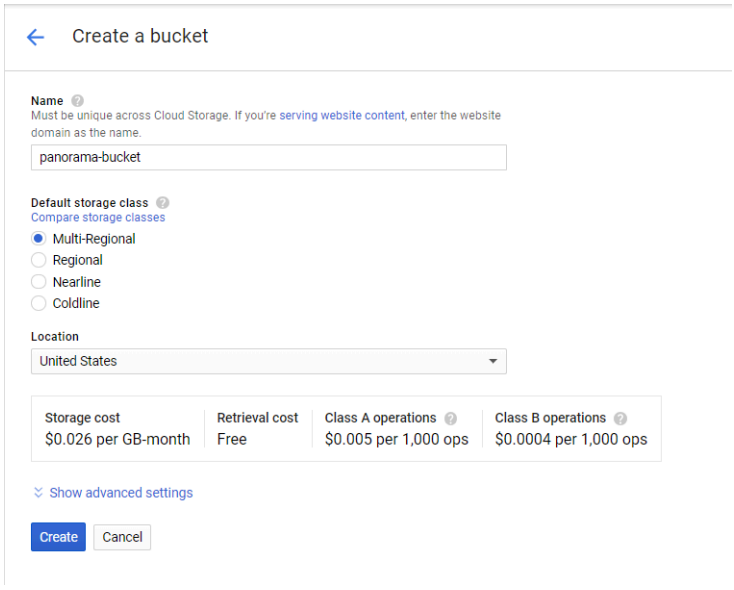
STEP 1 | Descargue la imagen del dispositivo virtual Panorama.

1. Inicie sesión en el Portal de soporte de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y filtre por **Panorama Base Images (Imágenes base de Panorama)**.
3. Descargue la versión más reciente de Panorama en la imagen `tar.gz` de GCP.

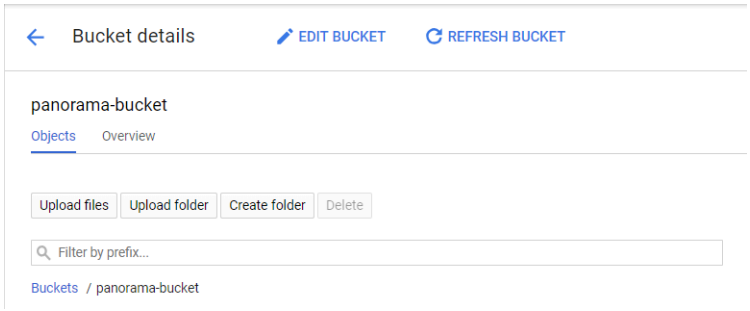
 ©2023 Palo Alto Networks, Inc.

STEP 2 | Cargue la imagen del dispositivo virtual Panorama a Google Cloud Platform.

1. Inicie sesión en la consola de Google Cloud.
2. En el menú **Products and Services (Productos y servicio)**, seleccione **Storage (Almacenamiento)**.
3. Haga clic en **Create Bucket (Crear depósito)**, configure el nuevo depósito de almacenamiento y haga clic en **Create (Crear)**.



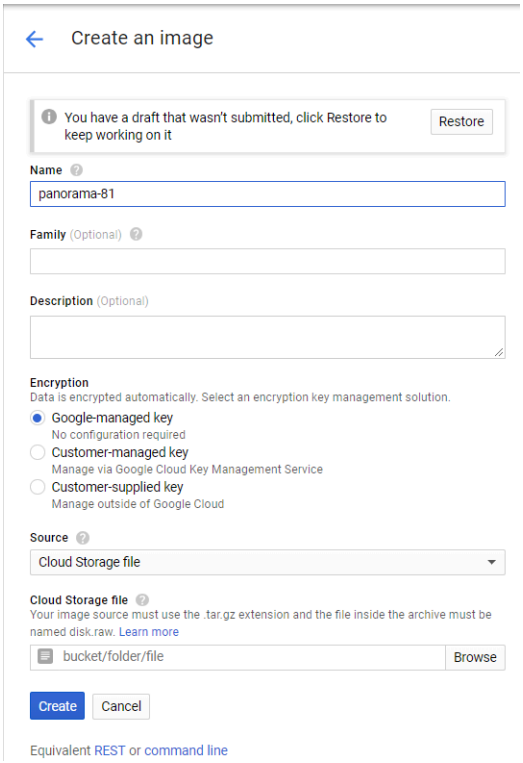
4. Seleccione el depósito de almacenamiento que creó en el paso anterior, haga clic en **Upload files (Cargar archivos)** y seleccione la imagen del dispositivo virtual Panorama que descargó.



5. En el menú **Products and Services (Productos y servicio)**, seleccione **Compute Engine** > **Images (Imágenes)**.
6. Haga clic en **Create Image (Crear imagen)** y cree la imagen del dispositivo virtual Panorama:
   1. Haga clic en **Name (Nombre)** para asignar un nombre a la imagen del dispositivo virtual Panorama.
   2. En el campo **Source (Origen)**, seleccione **Cloud Storage file (Archivo de almacenamiento en la nube)** del menú desplegable.
   3. Haga clic en **Browse (Examinar)** y vaya al depósito de almacenamiento donde cargó la imagen del dispositivo virtual Panorama y haga clic en **Select (Seleccionar)** para seleccionar la imagen cargada.

©2023 Palo Alto Networks, Inc.

4. Haga clic en **Create (Crear)** para crear la imagen del dispositivo virtual Panorama.



STEP 3 | Configure el dispositivo virtual Panorama.

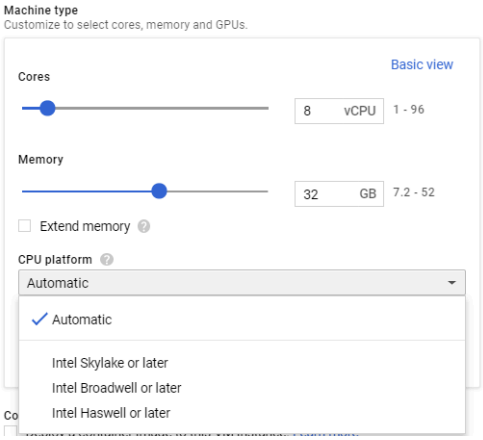
1. En el menú **Products and Services (Productos y servicio)** y seleccione **Compute Engine**.
2. Haga clic en **Create Instance (Crear instancia)** para comenzar a implementar el dispositivo virtual Panorama.
3. Añada un **Name (Nombre)** descriptivo para identificar con facilidad el dispositivo virtual Panorama.
4. Seleccione la **Region (Región)** y la **Zone (Zona)** donde desea implementar el dispositivo virtual Panorama.
5. Asigne el **Machine Type (Tipo de máquina)** y haga clic en **Customize (Personalizar)** para personalizar los núcleos de la CPU, la memoria y la plataforma de la CPU. Revise

 ©2023 Palo Alto Networks, Inc.

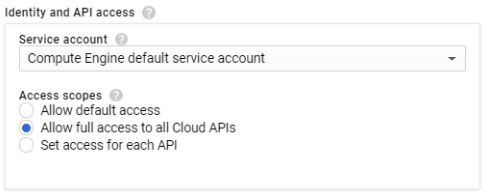
los Requisitos previos de configuración del dispositivo virtual Panorama para obtener información sobre los requisitos mínimos de recursos.

Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar el dispositivo con los recursos necesarios durante la implementación inicial. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.

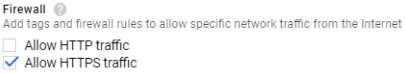
La selección de zona de GCP determina las plataformas de CPU disponibles. Para obtener más información, consulte Regiones y zonas**.**



6. Configure el disco de inicio de Panorama.
   1. En **Boot Disk (Disco de arranque)**, haga clic en **Change (Cambiar)** > **Custom image (Imagen personalizada)** y seleccione el archivo de imagen de Panorama que cargó en el paso 2.
   2. Revise el tamaño del disco de arranque en **Size (Tamaño)** y verifique que el disco del sistema sea de **81**GB.
   3. Haga clic en **Select (Seleccionar)** para guardar la configuración.
7. En **Identity and API access (Acceso a la identidad y la API)**, seleccione **Allow full access to all Cloud APIs (Permitir acceso total a todas las API de la nube)**.



8. En **Firewall (Cortafuegos)**, seleccione **Allow HTTPS traffic (Permitir tráfico de HTTPS)**.

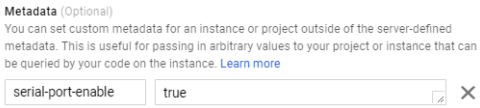


STEP 4 | Expanda **Management, security, disks, networking, sole tenancy (Gestión, seguridad, discos, redes, tenencia individual)** Management, security, disks, networking, sole tenancy .

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Habilite el acceso al puerto de serie de modo que pueda gestionar el dispositivo virtual Panorama.

1. Seleccione **Management (Gestión)**.
2. Introduzca el siguiente par de nombre y valor en el campo Metadata (Metadatos):
   `serial-port-enable true`



 ©2023 Palo Alto Networks, Inc.

STEP 6 | Reserve una dirección IP estática para la interfaz de gestión.

Reserve direcciones IP estáticas internas y externas para la interfaz de gestión. Así, si el dispositivo virtual Panorama se reinicia, los dispositivos gestionados no pierden la conexión a él cuando se vuelven a asignar las direcciones IP.

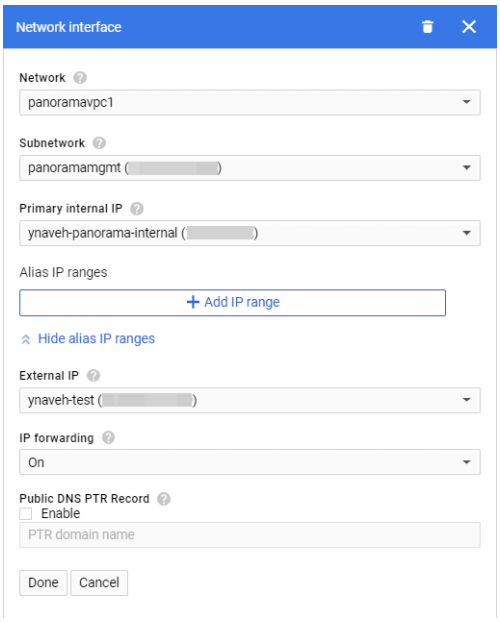
Para obtener más información sobre cómo reservar direcciones IP, consulte Reserva de una dirección IP estática interna y Reserva de una dirección IP estática externa.

1. Seleccione **Networking**.
2. Haga clic en **Edit (Editar)** para cambiar la interfaz de la red.



3. Seleccione la **Network (Red)** del dispositivo virtual Panorama.
4. Seleccione la **Subnetwork (Subred)** del dispositivo virtual Panorama. Las instancias en la misma subred se comunicarán entre sí utilizando sus direcciones IP internas.
5. Configure la dirección **Primary internal IP (IP interna principal)**.
   - **Ephemeral (Efímero) (automático):** asigne automáticamente una dirección IP interna principal.
   - **Ephemeral (Efímero) (personalizado):** configure un rango de IP personalizado que GCP utiliza para asignar una dirección IP interna principal.
   - **Reserve a static internal IP address (Reservar una dirección IP estática interna):** configure manualmente una dirección IP estática interna principal.
6. Configure la dirección **External IP (IP externa)**.
   - **Ephemeral (Efímero):** asigne automáticamente una dirección IP externa de un grupo de IP compartidas.
   - Seleccione una dirección IP externa reservada existente.
   - **Create IP address (Crear dirección IP):** reserve una dirección IP externa.
7. Configure **IP forwarding (Reenvío de IP)** en **On (Encendido)** para permitir que el dispositivo virtual Panorama reciba paquetes de destinos que no coincidan o direcciones IP de origen.

 ©2023 Palo Alto Networks, Inc.



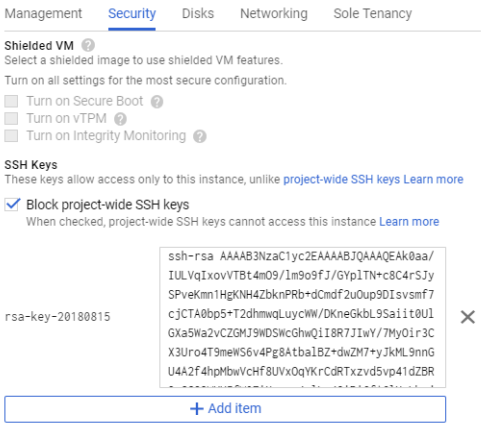
 ©2023 Palo Alto Networks, Inc.

STEP 7 | Configure la clave SSH. Necesita una clave SSH para acceder a la CLI del dispositivo virtual Panorama con el fin de configurar la contraseña del usuario administrativo tras la implementación inicial.

- **Usuarios de PuTTY**

  1. Seleccione **Security (Seguridad)**.
  2. Seleccione la casilla de verificación **Block project-wide SSH keys (Bloquear claves SSH para todo el proyecto)**. Actualmente, solo se admiten claves de la instancia para el registro de logs en el dispositivo virtual Panorama después de la implementación inicial.
  3. Pegue la clave SSH en los comentarios. Para obtener información sobre el formato de clave SSH correcto y cómo generar claves SSH para GCP, consulte Gestión de claves SSH en los metadatos.

  Cuando genere la clave SSH, guarde la clave privada en formato .ppk. Se requiere la clave privada para iniciar sesión en el dispositivo virtual Panorama después de la implementación inicial antes de que pueda configurar la contraseña administrativa.



- **Usuarios de Linux y macOS**

  1. Genere la clave SSH desde la CLI de su dispositivo Linux.

     ```
     ssh-keygen -C admin@panorama -f <panorama_key_name>
     ```

     En el que **admin@panorama** es un comentario que requiere GCP y **<panorama_key_name>** es el nombre del archivo de clave que se está generando.
  2. Cree un archivo de salida para la clave SSH.

     ```
     cat <panorama_key_name>.pub
     ```

     Una vez creado el archivo de salida para la clave SSH, copie manualmente el contenido de la clave SSH.
  3. Pegue la clave pública en la sección de claves SSH de la creación de la instancia de GCP.

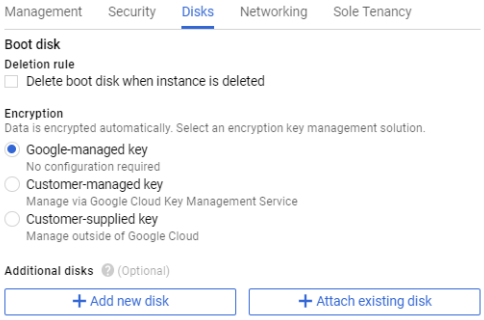
©2023 Palo Alto Networks, Inc.

STEP 8 | (Opcional) Agregue almacenamiento adicional para la recopilación de registros. Repita este paso las veces que fuera necesario para añadir discos de logging virtuales adicionales.

Si desea utilizar el dispositivo virtual Panorama en modo Panorama o como un recopilador de logs dedicado, añada los discos virtuales de registro de logs durante la implementación inicial. De manera predeterminada, el dispositivo virtual Panorama se encuentra en modo Panorama para la implementación inicial cuando cumple con los requisitos de recursos del modo Panorama y añadió, al menos, un disco virtual de logging. De lo contrario, el dispositivo virtual Panorama cambia a su valor predeterminado de modo solo de gestión en el cual puede gestionar dispositivos y recopiladores de logs dedicados, y no puede recopilar logs localmente.

El dispositivo virtual Panorama en GCP admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging con menos de 2 TB o un disco de logging con un tamaño que no sea divisible por los 2 TB del requisito para discos de logging. El dispositivo virtual Panorama divide los discos de logging con más de 2 TB en particiones de 2 TB.

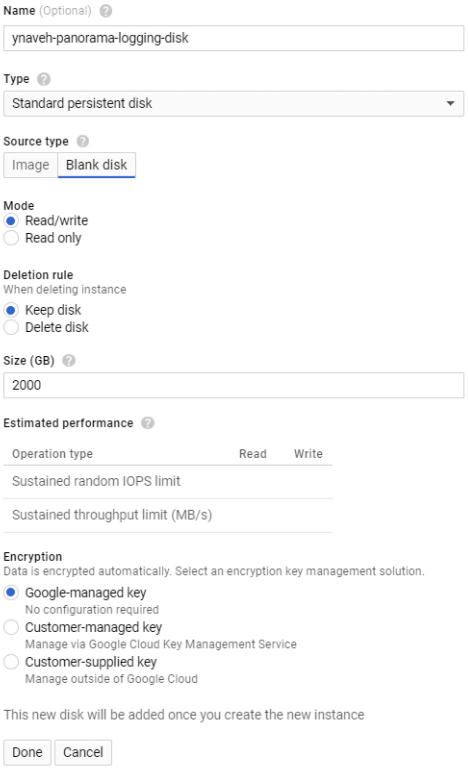
1. Seleccione **Disks (Discos)** > **Add new disk (Añadir disco nuevo)**.



2. Introduzca el **Name (Nombre)**.
3. Expanda el menú desplegable **Type (Tipo)** y seleccione el tipo deseado.
4. En **Source type (Tipo de origen)**, seleccione **Blank disk (disco en blanco)**.
5. En **Mode (Modo)**, seleccione **Read/write (Leer/escribir)**.
6. Seleccione la **Deletion rule** para configurar que se elimine el disco virtual de registro de logs si la instancia del dispositivo virtual de Panorama se elimina. Para
7. Configure el **Size (Tamaño) (GB)** del disco virtual de logging.
8. Configure su solución de **Encryption (Cifrado)** preferida para los datos en el disco virtual de registro de logs.

 ©2023 Palo Alto Networks, Inc.

9. Haga clic en **Done (Listo)**.



STEP 9 | Haga clic en **Create (Crear)** para crear el dispositivo virtual Panorama. Los dispositivos virtuales Panorama tardan aproximadamente 10 minutos en arrancar después de la implementación inicial.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web del dispositivo virtual Panorama. Para acceder a la CLI, utilice la clave privada para iniciar el dispositivo virtual Panorama.

La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

- Si cuenta con un servidor SSH instalado en su ordenador:
  1. Introduzca el siguiente comando para iniciar sesión en el dispositivo virtual Panorama:
     - Dispositivos Windows

       ```
       ssh -i <private_key.ppk> admin @<public-ip_address>
       ```

     - Dispositivos Linux

       ```
       ssh -i panorama <public-ip_address>
       ```

  2. Configure una nueva contraseña utilizando los siguientes comandos y siga las indicaciones en la pantalla:

     ```
     admin> configure admin# set mgt-config users admin password
     ```

  3. Si tiene una BYOL que necesita, configure la dirección IP del servidor DNS, de modo que el dispositivo virtual Panorama pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

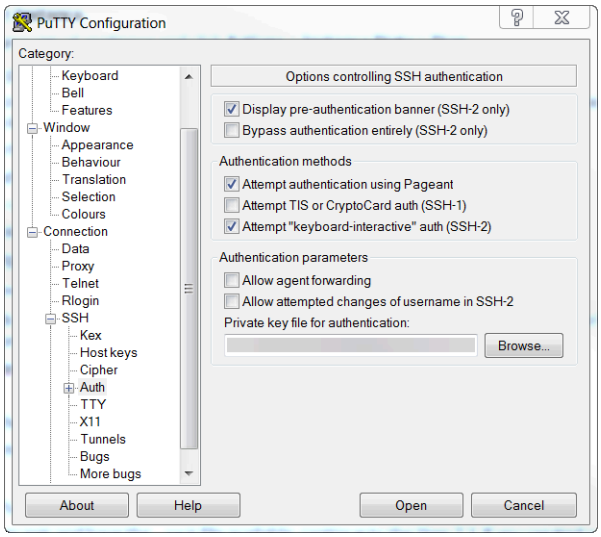
     ```
     admin# set deviceconfig system dns-setting servers
      primary <ip_address>
     ```

  4. Confirme los cambios:

     ```
     admin# commit
     ```

  5. Finalice la sesión SSH.
- Si está utilizando PuTTY para abrir una sesión SSH en el dispositivo virtual Panorama:
  1. Si está utilizando un par de claves existente y cuenta con el archivo `.ppk`, vaya al paso 11.3. Si creó un nuevo par de claves o solo cuenta con el archivo `.pem` del par de claves existente, abra PuTTYgen y haga clic en **Load (Cargar)** para cargar el archivo `.pem`.
  2. **Guarde la clave privada** en un destino local accesible.
  3. Abra PuTTY, seleccione **SSH** > **Auth** y haga clic en **Browse (Examinar)** para buscar el archivo `.ppk` que guardó en el paso anterior.

 ©2023 Palo Alto Networks, Inc.



4. Seleccione **Sessions (Sesiones)** e introduzca la dirección IP pública del dispositivo virtual Panorama. Luego, haga clic en **Open (Abrir)** y en **Yes (Sí)** cuando aparezca el mensaje de seguridad.
5. Inicie sesión como admin cuando se le solicite.
6. Configure una nueva contraseña utilizando los siguientes comandos y siga las indicaciones en la pantalla:

```
admin> configure admin# set mgt-config users admin password
```

7. Configure la dirección IP del servidor DNS, de modo que el dispositivo virtual Panorama pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

```
admin# set deviceconfig system dns-setting servers
 primary <ip_address>
```

8. Confirme los cambios con el comando:

```
admin# commit
```

9. Finalice la sesión SSH.

 ©2023 Palo Alto Networks, Inc.

STEP 11 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.

2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.

3. Active una licencia de gestión de cortafuegos.

   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en Google Cloud Platform según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en Google Cloud Platform.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.
- Para implementaciones de SD-WAN.
  1. Aumento del disco del sistema para Panorama en Google Cloud Platform

     Para aprovechar SD-WAN en un Panorama implementado en GCP, debe aumentar el disco del sistema a 224 GB.

     No puede volver a migrar a un disco del sistema de 81 GB después de haber aumentado correctamente el disco del sistema a 224 GB.
  2. Configure un dispositivo virtual Panorama en modo Solo gestión.
  3. Cómo añadir un disco virtual a Panorama en Google Cloud Platform.

     Para aprovechar SD-WAN, debe agregar un solo disco de creación de logs de 2TB a Panorama en el modo Solo gestión.

Instalación de Panorama en KVM

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en KVM. El modelo que implementó Panorama en KVM es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión), y comparte los mismos

 ©2023 Palo Alto Networks, Inc.

procesos y funcionalidades de los dispositivos de hardware serie M. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

STEP 1 | Descargue la imagen del dispositivo virtual Panorama para KVM.

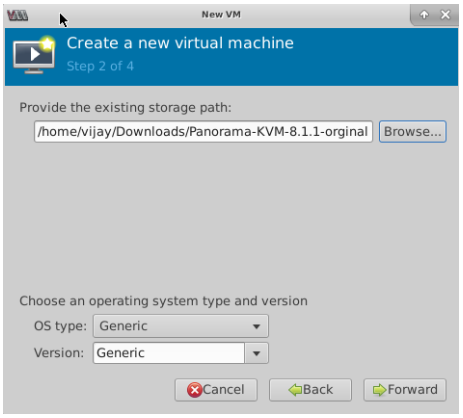
1. Inicie sesión en el Portal de soporte de Palo Alto Networks.
2. Seleccione **Software Updates (Actualizaciones de software)** y busque la imagen base de Panorama para KVM.
3. Descargue el último archivo .qcow2 de Panorama disponible.

STEP 2 | Cree una nueva imagen de máquina virtual y añada la imagen del dispositivo virtual Panorama para KVM al gestor de máquinas virtuales.

1. En el gestor de máquinas virtuales, seleccione **Create a new virtual machine (Crear nueva máquina virtual)**.
2. Seleccione **Import Existing disk image (Importar imagen de disco existente)** y haga clic en **Forward (Reenviar)**.



3. Haga clic en **Browse (Examinar)** y seleccione el volumen de la imagen del dispositivo virtual Panorama y haga clic en **Choose volume (Seleccionar volumen)**.
4. Haga clic en **Forward (Reenviar)**.



 ©2023 Palo Alto Networks, Inc.

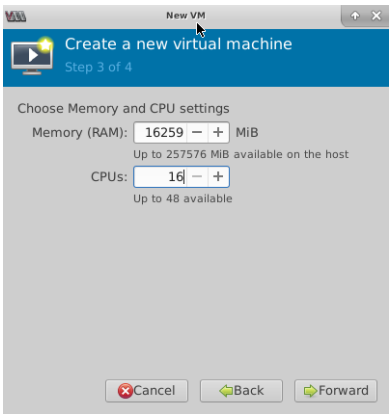
STEP 3 | Configure los ajustes de memoria y CPU.

Revise los Requisitos previos de configuración del dispositivo virtual Panorama para obtener información sobre los requisitos mínimos de recursos.

Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar el dispositivo con los recursos necesarios durante la implementación inicial. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.

1. Configure la **Memory (Memoria)** según los requisitos para el modo operativo deseado.

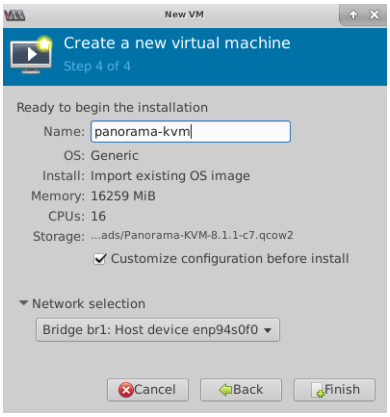
   Es posible que el gestor de máquinas virtuales utilice MiB (mebibyte) para asignar memoria según la versión que ejecute. Si se utiliza MiB, asegúrese de convertir correctamente la asignación de memoria necesaria para evitar la subestimación de recursos en el dispositivo virtual Panorama.
2. Configure la **CPU** según los requisitos para el modo operativo deseado.
3. Haga clic en **Forward (Reenviar)**.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Asigne un nombre al dispositivo virtual Panorama, habilite la personalización de la configuración y seleccione el puente para la interfaz de gestión.

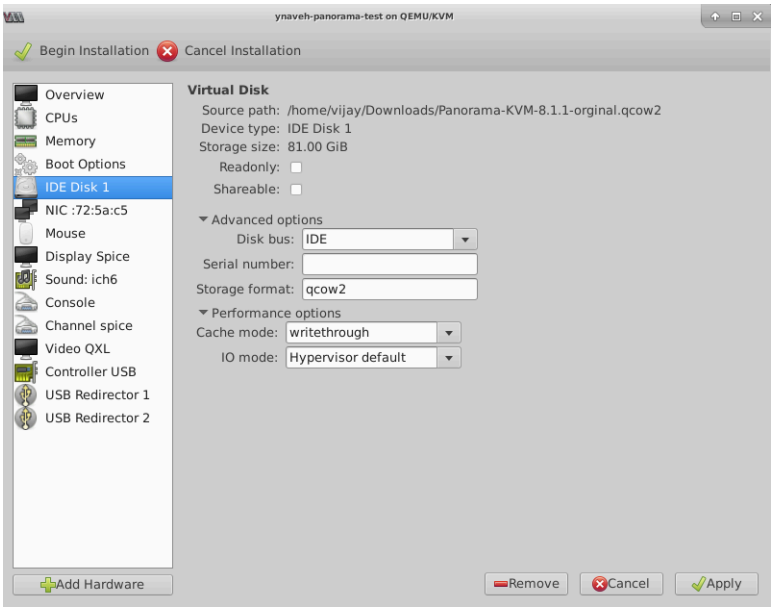
1. Introduzca un **Name (Nombre)** descriptivo para el dispositivo virtual Panorama.
2. Seleccione **Customize configuration before install (Personalizar configuración antes de la instalación)**.
3. Realice una **selección de red**: seleccione el puente para la interfaz de gestión y acepte la configuración predeterminada.
4. Haga clic en **Finish (Finalizar)**.



 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure los ajustes del disco de sistema virtual.

1. Seleccione **IDE Disk 1**, vaya a **Advanced options (Opciones avanzadas)** y seleccione lo siguiente:
   - **Disk Bus (Bus del disco): VirtIO** o **IDE** según su configuración.
   - **Storage format (Formato de almacenamiento): qcow2**
2. Vaya a **Performance options (Opciones de rendimiento)** y configure **Cache mode (Modo de caché)** en **writethrough**. Esta configuración mejora el tiempo de instalación y la velocidad de ejecución en el dispositivo virtual Panorama.
3. Haga clic en **Apply (Aplicar)**.



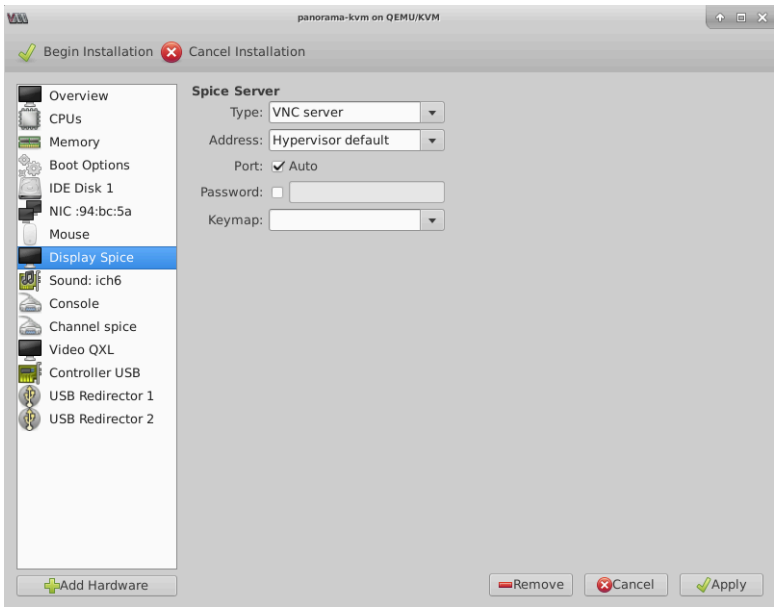
 ©2023 Palo Alto Networks, Inc.

STEP 6 | Configure la visualización de la consola de la máquina virtual para que utilice el servidor VNC a fin de interactuar con la máquina virtual.

1. Seleccione **Display Spice (Spice de visualización)**.

   *Continúe al siguiente paso si **Display VNC (VNC de visualización)** se encuentra en la lista de hardware dado que la máquina virtual ya está configurada para utilizar el servidor VNC para la visualización.*

2. En la lista desplegable **Type (Tipo)**, seleccione **VNC server (Servidor VNC)**.
3. Haga clic en **Apply (Aplicar)**.



STEP 7 | (Opcional) Agregue almacenamiento adicional para la recopilación de registros. Repita este paso las veces que fuera necesario para añadir discos de logging virtuales adicionales.

Si desea utilizar el dispositivo virtual Panorama en modo Panorama o como un recopilador de logs dedicado, añada los discos virtuales de logging durante la implementación inicial. De manera predeterminada, el dispositivo virtual Panorama se encuentra en modo Panorama para la implementación inicial cuando cumple con los requisitos de recursos del modo Panorama y añadió, al menos, un disco virtual de logging. De lo contrario, los valores del dispositivo virtual Panorama vuelven al valor predeterminado en modo solo de gestión. Cambie el modo del dispositivo virtual Panorama al modo solo de gestión si desea gestionar dispositivos y recopiladores de logs dedicados, y no desea recopilar logs localmente.

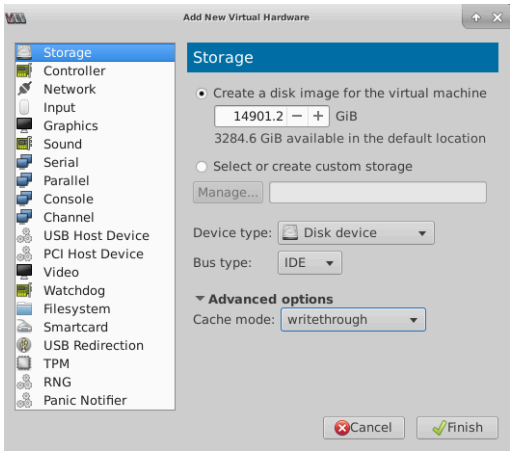
El dispositivo virtual Panorama en KVM admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging con menos de 2 TB o un disco de logging con un tamaño que no sea divisible por los 2 TB del requisito para discos de logging. El dispositivo virtual Panorama divide los discos de logging con más de 2 TB en particiones de 2 TB.

1. **Añada el hardware**.

 ©2023 Palo Alto Networks, Inc.

2. Configure el nuevo disco de **almacenamiento**:
    1. **Cree una imagen de disco para una máquina virtual** y configure la capacidad de almacenamiento del disco virtual en 14901.2 GiB (equivalente a 2 TB).

        Es posible que el gestor de máquinas virtuales utilice GiB (gibibyte) para asignar memoria según la versión que ejecute. Si se utiliza GiB, asegúrese de convertir correctamente la capacidad de almacenamiento necesaria para evitar la subestimación de recursos en el disco virtual de logging y el envío del dispositivo virtual Panorama en modo de mantenimiento.
    2. Establezca **Device type (Tipo de dispositivo)** como dispositivo de **Disk (Disco)**.
    3. Configure **Bus type (Tipo de bus)** en **VirtIO** o **IDE** según su configuración.
    4. Vaya a **Advanced options (Opciones avanzadas)** y configure **Cache mode (Modo de caché)** en **writethrough**.
3. Haga clic en **Finish (Finalizar)**.



STEP 8 | **Comience la instalación** (Begin Installation). Los dispositivos virtuales Panorama tardan aproximadamente 10 minutos en arrancar.

STEP 9 | Abra una conexión a la consola del dispositivo virtual Panorama.

Se le solicitará que inicie sesión en el cortafuegos utilizando el nombre de usuario y la contraseña predeterminados: **`admin`**/**`admin`**.

STEP 10 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web o la CLI del dispositivo virtual Panorama. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

Cuando inicia sesión por primera vez en la CLI de Panorama, se le solicita que introduzca la **contraseña anterior** y la **contraseña nueva** para el usuario **`administrador`** antes de que pueda continuar.

 ©2023 Palo Alto Networks, Inc.

STEP 11 | Defina la configuración de acceso a la red para la interfaz de gestión.

1. Acceda al modo de configuración con el siguiente comando:

```
admin> configure
```

2. Use los siguientes comandos para configurar y permitir el acceso a la interfaz de gestión:

```
admin# set deviceconfig system type static admin# set
 deviceconfig system ip-address <Panorama-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

donde *<Panorama-IP>* es la dirección IP que quiere asignar a la interfaz de gestión, *<netmask>* es la máscara de subred, *<gateway-IP>* es la dirección IP de la puerta de enlace de la red e *<DNS-IP>* es la dirección IP del servidor DNS.

```
admin# commit
```

STEP 12 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.

2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.

3. Active una licencia de gestión de cortafuegos.

   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 13 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en KVM según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en KVM.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

Instalación de Panorama en Hyper-V

Ahora, puede implementar Panorama™ y un recopilador de logs dedicado en Hyper-V. El modelo que implementó Panorama en Hyper-V es de traiga su propia licencia (BYOL), que admite todos los modos de implementación (Panorama, recopilador de logs y solo de gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware serie M. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama. Solo puede usar los dispositivos virtuales Panorama y los recopiladores de logs dedicados virtuales en Hyper-V con PAN-OS 8.1.3 y versiones posteriores.

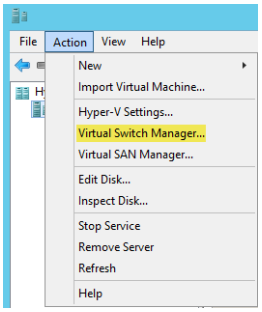
STEP 1 | Descargue el archivo VHDX.

1. Inicie sesión en el Portal de soporte de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**, filtre por **Panorama Base Images (Imágenes base de Panorama)** y descargue el archivo VHDX.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configure el vSwitch o vSwitches que necesitará. Para obtener más información, revise los Tipos de conmutador virtual.

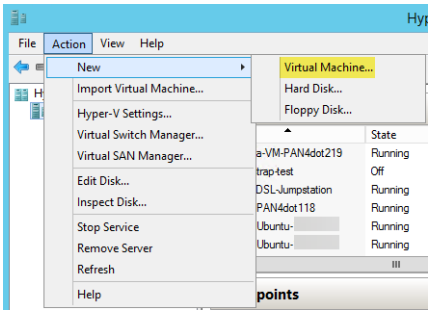
1. En el gestor de Hyper-V, seleccione el host y seleccione **Action (Acción)** > **Virtual Switch Manager (Gestor de conmutadores virtuales)** para abrir la ventana del gestor de conmutadores virtuales.



2. En **Create virtual switch (Crear conmutador virtual)**, seleccione el tipo de vSwitch para su creación y haga clic en **Create virtual switch (Crear conmutador virtual)**.

STEP 3 | Instale el dispositivo virtual Panorama.

1. En el gestor de Hyper-V, seleccione el host y seleccione **Action (acción)** > **New (Nuevo)** > **Virtual Machine (Máquina virtual)**. Configure los siguientes ajustes en el asistente de nueva máquina virtual:



1. Seleccione un **Name (Nombre)** y una **Location (Ubicación)** para el dispositivo virtual Panorama. El dispositivo virtual Panorama guarda el archivo VHDX en la ubicación especificada.
2. Elija **Generation 1 (Generación 1)**. Es la opción por defecto y la única versión compatible.
3. En **Startup Memory (Memoria de arranque)**, asigne la memoria según el modo de sistema deseado. Consulte los Requisitos previos de configuración del dispositivo virtual Panorama para obtener información sobre los requisitos de memoria para cada modo.

   No habilite la memoria dinámica; el dispositivo virtual Panorama necesita asignación estática de la memoria.
4. Configure **Networking**. Seleccione un vSwitch externo para conectar la interfaz de gestión en el cortafuegos.
5. Para conectar el **Virtual Hard Disk (Disco duro virtual)**, seleccione **Use an existing virtual hard disk (Usar un disco duro virtual existente)** y navegue hasta el archivo VHDX descargado anteriormente.
6. Revise el resumen y haga clic en **Finish (Finalizar)**.

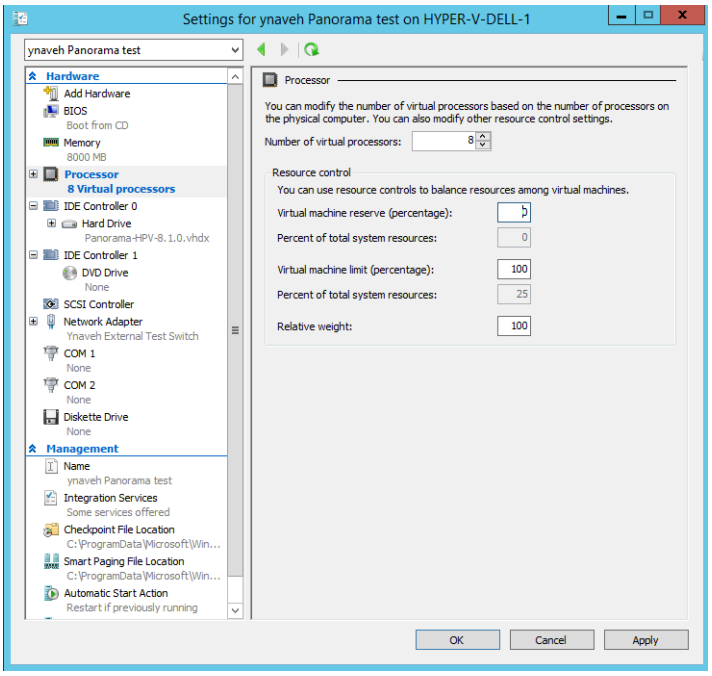
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Asigne los núcleos de la CPU del dispositivo virtual Panorama.

Revise los Requisitos previos de configuración del dispositivo virtual Panorama para obtener información sobre los requisitos mínimos de recursos.

Si planea utilizar el dispositivo virtual Panorama como recopilador de logs dedicado, asegúrese de configurar el dispositivo con los recursos necesarios durante la implementación inicial. Un dispositivo virtual Panorama no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto provoca una pérdida de datos de logs.

1. En la lista **Hardware**, seleccione **Processor (Procesador)**.
2. Edite el **Number of virtual processors (Número de procesadores virtuales)** asignados actualmente.



STEP 5 | Conecte al menos un adaptador de red para la interfaz del plano de datos en el cortafuegos. Repítalo para crear interfaces de red adicionales en el dispositivo virtual Panorama.

1. Seleccione **Settings (Configuración)** > **Hardware** > **Add Hardware (Añadir hardware)** y seleccione **Hardware type (Tipo de hardware)** para su adaptador de red.

   No son compatibles adaptadores de red heredados y SR-IOV. Si se selecciona, el cortafuegos VM-Series se reiniciará en el modo de mantenimiento.

2. Haga clic en **OK (Aceptar)**.

STEP 6 | (Opcional) Agregue almacenamiento adicional para la recopilación de registros. Repita este paso las veces que fuera necesario para añadir discos de logging virtuales adicionales. Si desea implementar el dispositivo virtual Panorama en modo solo de gestión, continúe con el paso 6.

Si desea utilizar el dispositivo virtual Panorama en modo Panorama o como un recopilador de logs dedicado, añada los discos virtuales de logging durante la implementación inicial. De manera predeterminada, el dispositivo virtual Panorama se encuentra en modo Panorama para

 ©2023 Palo Alto Networks, Inc.

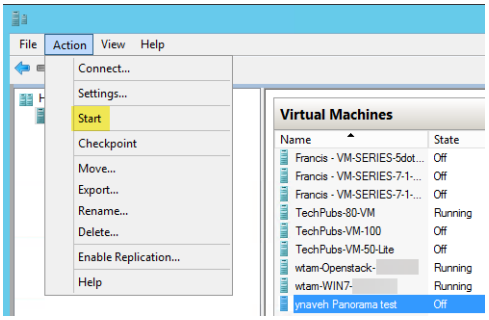
la implementación inicial cuando cumple con los requisitos de recursos del modo Panorama y añadió, al menos, un disco virtual de logging. De lo contrario, los valores del dispositivo virtual Panorama vuelven al valor predeterminado en modo solo de gestión. Cambie el modo del dispositivo virtual Panorama al modo solo de gestión si desea gestionar dispositivos y recopiladores de logs dedicados, y no desea recopilar logs localmente.

El dispositivo virtual Panorama en Hyper-V admite solo discos de registro de logs de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging con menos de 2 TB o un disco de logging con un tamaño que no sea divisible por los 2 TB del requisito para discos de logging. El dispositivo virtual Panorama divide los discos de logging con más de 2 TB en particiones de 2 TB.

1. En el gestor de Hyper-V, seleccione el host y seleccione **Action (acción)** > **New (Nuevo)** > **Hard Disk (Disco duro)**.
2. Si ve la solicitud Before You Begin (Antes de comenzar), haga clic en **Next (Siguiente)** para comenzar a añadir el disco virtual de registro de logs.
3. En Disk Format (Formato de disco), seleccione **VHDX**. Haga clic en **Next (Siguiente)** para continuar.
4. En Disk Type (Tipo de disco), seleccione **Fixed Size (Tamaño fijo)** o **Dynamically Expanding (Expansión dinámica)** según sus necesidades. Haga clic en **Next (Siguiente)** para continuar.
5. Especifique el **Name (Nombre)** y la **Location (Ubicación)** del archivo del disco virtual de registro de logs. Haga clic en **Next (Siguiente)** para continuar.
6. Para configurar el disco, seleccione **Create a new virtual hard disk (Crear un nuevo disco virtual)** e introduzca el tamaño del disco. Haga clic en **Next (Siguiente)** para continuar.
7. Revise el resumen y haga clic en **Finish (Finalizar)** para completar la adición del disco duro virtual de registro de logs.

STEP 7 | Active el dispositivo virtual Panorama.

1. Seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Action (Acción)** > **Start (Iniciar)** para encender la instancia del dispositivo virtual Panorama.



STEP 8 | Conéctese a la consola del dispositivo virtual Panorama desde Hyper-V Manager.

1. En la lista de **Virtual Machines (Máquinas virtuales)**, seleccione el dispositivo virtual Panorama.
2. Seleccione **Actions (Acciones)** > **Connect (Conectar)** e introduzca el nombre de usuario y la contraseña para iniciar sesión (el valor predeterminado es admin para ambos).

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web o la CLI del dispositivo virtual Panorama. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

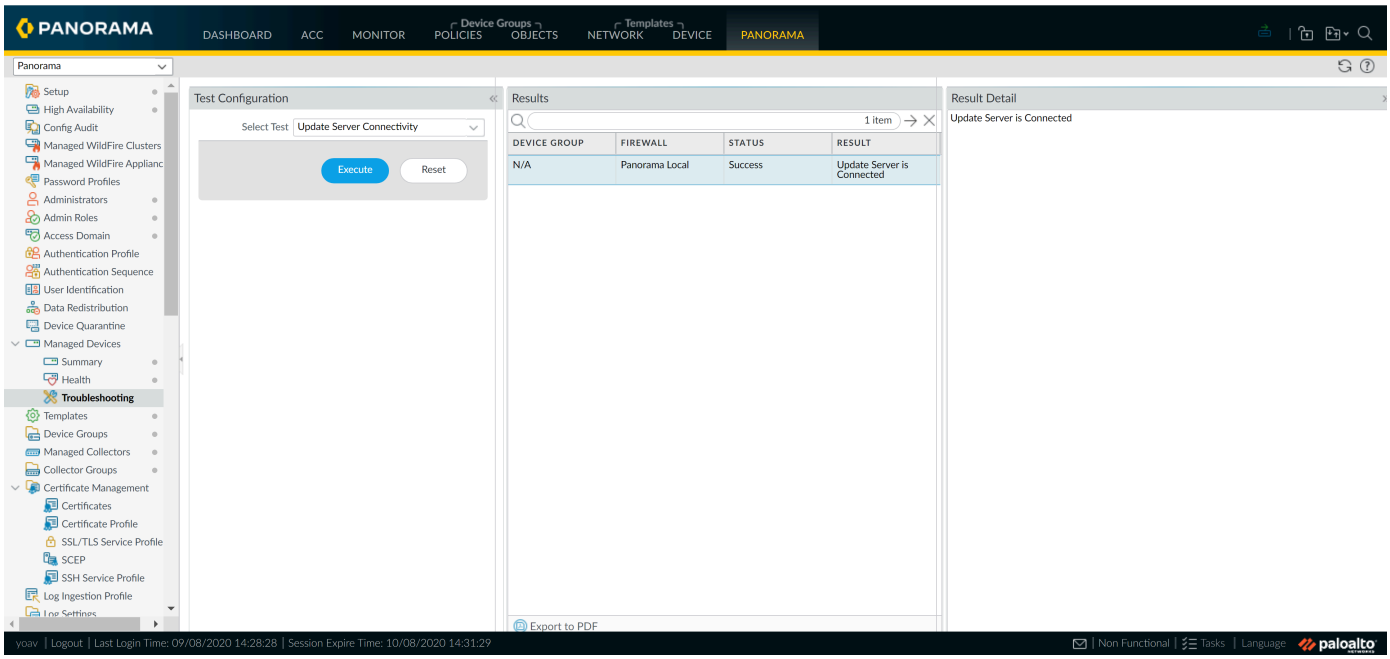
Cuando inicia sesión por primera vez en la CLI de Panorama, se le solicita que introduzca la **contraseña anterior** y la **contraseña nueva** para el usuario `administrador` antes de que pueda continuar.

STEP 10 | Configure la dirección IP de la interfaz de gestión.

1. Introduzca los siguientes comandos, donde ***<Panorama-IP>*** es la dirección IP que quiere asignar a la interfaz de gestión de Panorama, ***<netmask>*** es la máscara de subred, ***<gateway-IP>*** es la dirección IP de la puerta de enlace de la red e ***<DNS-IP>*** es la dirección IP del servidor DNS.

```
admin> configure admin# set deviceconfig system ip-
address <Panorama-IP> netmask <netmask> default-
gateway <gateway-IP> dns-setting servers primary <DNS-IP>
 admin# commit admin# exit
```

2. Solución de problemas de conectividad a recursos de red y verifique el acceso de red a los servicios externos indispensables para gestionar los cortafuegos, como el cortafuegos predeterminado, el servidor DNS y el servidor de actualizaciones de Palo Alto Networks, tal como se muestra en el ejemplo siguiente:



 ©2023 Palo Alto Networks, Inc.

STEP 11 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.

2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.

3. Active una licencia de gestión de cortafuegos.

   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en Hyper-V. según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en Hyper-V..

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

Configuración de Panorama en Oracle Cloud Infrastructure (OCI)

Configure un dispositivo virtual Panorama™ en Oracle Cloud Infrastructure (OCI) para administrar de forma centralizada la configuración de cortafuegos físicos y VM-Series.

- Cómo descargar la imagen del dispositivo virtual Panorama en OCI
- Instalación de Panorama en Oracle Cloud Infrastructure (OCI)
- Cómo generar una clave SSH para Panorama en OCI

Cómo descargar la imagen del dispositivo virtual Panorama en OCI

Complete el siguiente procedimiento para cargar un archivo qcow2 de Panorama para KVM y cree la imagen personalizada que necesita para iniciar el dispositivo virtual Panorama. Cargar y crear la imagen solo es necesario una vez. Puede utilizar la misma imagen para todas las implementaciones posteriores del dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Descargue el archivo qcow2 de Panorama para KVM desde el Portal de atención al cliente (CSP) de Palo Alto Networks.

1. Inicie sesión en el CSP de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y **Panorama Base Images (Imágenes básicas de Panorama)** en el menú desplegable de filtros de actualizaciones de software.
3. Descargue la última versión de la imagen qcow2 de `Panorama-KVM`.

STEP 2 | Inicie sesión en la consola de Oracle Cloud Infrastructure.

STEP 3 | Cree un depósito de almacenamiento para el archivo qcow2.

1. Seleccione **Object Storage (Almacenamiento de objetos)** > **Object Storage (Almacenamiento de objetos)** y **Create Bucket (Crear depósito)**.
2. Introduzca un nombre descriptivo en **Bucket Name (Nombre de depósito)**.
3. En el nivel de almacenamiento, seleccione **Standard (Estándar)**.
4. **Create Bucket (Crear depósito)**.

STEP 4 | Cargue la imagen de qcow2 en el depósito de almacenamiento de OCI.

1. Haga clic en el depósito de almacenamiento que creó en el paso anterior para ver los detalles del depósito.
2. Haga clic en **Upload (Cargar)** y seleccione la imagen de qcow2 que descargó del CSP de Palo Alto Networks.
3. Haga clic en **Upload (Subir)** para subir la imagen.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Cree una solicitud previamente autenticada para el archivo de qcow2.

Esto es necesario para crear la dirección URL del objeto utilizada en la creación de la imagen personalizada para el dispositivo virtual Panorama.

1. Seleccione **Object Storage (Almacenamiento de objetos)** > **Object Storage (Almacenamiento de objetos)** y haga clic en el depósito que creó en el paso anterior.
2. Seleccione **Pre-Authenticated Requests (Solicitudes pre-autenticadas)** > **Create Pre-Authenticated Request (Crear solicitud pre-autenticada)**.
3. Introduzca un **Name (Nombre)** descriptivo para su solicitud pre-autenticada.
4. Seleccione **Object (Objeto)** e introduzca el nombre de imagen de qcow2 para el **Object Name (Nombre de objeto)**.
5. Haga clic en **Create Pre-Authenticated Request (Crear solicitud previamente autenticada)**.
6. En "Access Type " (Tipo de acceso), seleccione **Permit object reads and writes (Permitir lecturas y escrituras de objetos)**.
7. Introduzca una fecha y hora de **Expiration (Caducidad)**.
8. Haga clic en **Create Pre-Authenticated Request (Crear solicitud previamente autenticada)**.
9. En Pre-Authenticated Request Details (Detalles de la solicitud previamente autenticada), copie la URL de la solicitud previamente autenticada.

   La URL de solicitud previamente autenticada es necesaria para crear la imagen personalizada y debe copiarse cuando se le muestre.

   La URL de la solicitud previamente autenticada solo se muestra después de crear la solicitud y no se vuelve a mostrar.
10. **Cierre** los detalles de la solicitud previamente autenticada después de copiar la dirección URL.

STEP 6 | Importe el archivo de qcow2 y cree una imagen de dispositivo virtual Panorama personalizada.

1. Seleccione **Compute (Calcular)** > **Custom Images (Imágenes personalizadas)** e **Import Image (Importar imágenes)**.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para su imagen.
3. Seleccione **Import from an Object Storage URL (Importar desde una URL de almacenamiento de objetos)** y pegue la URL de almacenamiento de objetos.
4. En "Image type" (Tipo de imagen), seleccione **QCOW2**.
5. En "Launch Mode" (Modo de inicio), seleccione **Paravirtualized Mode (Modo paravirtualizado)**.
6. **Import Image (Importar imagen)**.

Instalación de Panorama en Oracle Cloud Infrastructure (OCI)

Cree una instancia de dispositivo virtual Panorama™ en Oracle Cloud Infrastructure (OCI). Una instancia de OCI admite una única NIC de forma predeterminada. Debe cargar manualmente una imagen qcow2 del dispositivo virtual Panorama descargada del Portal de atención al cliente (CSP) de Palo Alto Networks a OCI para instalar correctamente el dispositivo virtual Panorama en OCI.

 ©2023 Palo Alto Networks, Inc.

El dispositivo virtual Panorama que se implementó en OCI es de tipo traiga su propia licencia (BYOL), admite todos los modos de implementación (Panorama, recopilador de logs y solo gestión), y comparte los mismos procesos y funcionalidades de los dispositivos de hardware M-Series. Para obtener más información sobre los modos de Panorama, consulte Modelos Panorama.

Se requiere que una máquina que ejecute un sistema operativo Linux instale correctamente Panorama en OCI. Para instalar correctamente Panorama en OCI, debe generar una clave `.pub` mediante OpenSSH. Además, solo puede usar una máquina Linux para iniciar sesión en la CLI de Panorama para la configuración de red inicial.

Revise Requisitos previos de configuración del dispositivo virtual Panorama para determinar los recursos virtuales requeridos para sus necesidades. El requisito de recursos virtuales para el dispositivo virtual Panorama se basa en la cantidad total de cortafuegos gestionados por el dispositivo virtual Panorama y los Logs por segundo (LPS) necesarios para reenviar logs de los cortafuegos gestionados al recopilador de logs.

El aprovisionamiento insuficiente del dispositivo virtual Panorama afectará al rendimiento de la gestión. Esto incluye que el dispositivo virtual Panorama se vuelva lento o no responda en función del aprovisionamiento insuficiente del dispositivo virtual Panorama.

STEP 1 | Inicie sesión en la consola de Oracle Cloud Infrastructure.

STEP 2 | Configure Virtual Cloud Network (VCN) para sus necesidades de red.

Tanto si inicia el dispositivo virtual Panorama en una VCN existente o crea una nueva VCN, el dispositivo virtual Panorama debe poder recibir tráfico desde las instancias en la VCN y realizar comunicaciones de entrada y salida entre la VCN e Internet según sea necesario.

Consulte la documentación de VCN de OCI para obtener más información.

1. Configure una VCN o utilice una existente.
2. Compruebe que los componentes de red y seguridad estén definidos adecuadamente.
   - Cree una puerta de enlace de Internet para permitir el acceso a Internet a la subred de su dispositivo virtual Panorama. Se requiere acceso a Internet para instalar actualizaciones de contenido y software, activar licencias y aprovechar los servicios en la nube de Palo Alto Networks. De lo contrario, debe instalar las actualizaciones y activar las licencias manualmente.

     Si la instancia del dispositivo virtual Panorama forma parte de una subred privada, puede configurar una puerta de enlace NAT para habilitar solo el acceso saliente a Internet para la subred.
   - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VCN en las que puede iniciar las instancias de OCI. Se recomienda que el dispositivo virtual Panorama pertenezca a la subred de gestión de modo que pueda configurarlo para acceder a Internet si es necesario.

 ©2023 Palo Alto Networks, Inc.

- Añada rutas a la tabla de enrutamiento de una subred privada a fin de garantizar que el tráfico se pueda dirigir a través de subredes en la VCN y desde Internet, según corresponda.

  Asegúrese de crear rutas entre subredes para permitir la comunicación entre:

  - Panorama, cortafuegos gestionados y recopiladores de logs.
  - (Opcional) Panorama e Internet.
- Asegúrese de que las siguientes reglas de seguridad de entrada estén permitidas para que la VCN administre el tráfico de VCN. La fuente de tráfico de entrada para cada regla es única para su topología de implementación.

  Consulte Puertos utilizados para Panorama para obtener más información.

  - Permita el tráfico SSH (puerto **22**) para permitir el acceso a la CLI de Panorama.
  - Permita el tráfico HTTPS (puerto **443** y **28270**) para permitir el acceso a la interfaz web de Panorama.
  - Permita el tráfico en el puerto **3978** para habilitar la comunicación entre Panorama, administrar cortafuegos y recopiladores de logs gestionados. Los recopiladores de logs también utilizan este puerto para reenviar logs a Panorama.
  - Permita el tráfico en el puerto **28443** para permitir que los cortafuegos gestionados obtengan actualizaciones de software y contenido de Panorama.

STEP 3 | Seleccione **Compute (Procesar)** > **Instances (Instancias)** y haga clic en **Create Instance (Crear instancia)**.

STEP 4 | Introduzca un **Name (Nombre)** descriptivo para la imagen del dispositivo virtual Panorama.

STEP 5 | Seleccione el **Availability domain (Dominio de disponibilidad)**.

STEP 6 | Seleccione la imagen de Panorama de Palo Alto Networks.

Consulte Cómo descargar la imagen del dispositivo virtual Panorama en OCI *para cargar y mantener su propia* ***imagen personalizada*** *del dispositivo virtual de Panorama en OCI.*

1. En "Image and Shape" (Imagen y forma), seleccione **Change Image (Cambiar imagen)**.
2. Para Image Source (Fuente de la imagen), seleccione **Partner Image (Imagen de socio)**.

   Si mantiene su propia imagen de dispositivo virtual de Panorama, seleccione **Imagen personalizada** en su lugar y seleccione la imagen de dispositivo virtual de Panorama que cargó en OCI.
3. Busque **`Palo Alto Networks Panorama`** y seleccione (marque) la imagen.

   Omita este paso si seleccionó ***Custom Image (Imagen personalizada)*** *en el paso anterior.*

   PAN-OS 10.2.0 es la versión predeterminada de PAN-OS.
4. **Select Image (Seleccionar imagen)**.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Configure los recursos de la instancia.

Consulte Requisitos previos de configuración del dispositivo virtual Panorama para obtener más información sobre los recursos mínimos requeridos en función de sus necesidades de uso de Panorama.

1. En "Image and Shape" (Imagen y forma), seleccione **Change Shape (Cambiar forma)**.
2. Seleccione la forma con el número de CPU, la cantidad de RAM y el número de interfaces que necesita.
3. **Select Shape (Seleccionar forma)**.

STEP 8 | Configure las opciones de red de la instancia.

1. En "Network" (Red), haga clic en **Select existing virtual cloud network (Seleccionar red de nube virtual existente)** y seleccione la VCN.
2. En "Subnet" (Subred), haga clic en **Select existing subnet (Seleccionar subred existente)** y seleccione la subred.

   Se recomienda implementar la instancia del dispositivo virtual Panorama en una subred de administración para permitir de forma segura el acceso a Internet si es necesario.
3. (Opcional) Para la dirección IP pública, seleccione **Assign a public IPv4 address (Asignar una dirección IPv4 pública)** si desea que se pueda acceder al dispositivo virtual Panorama desde fuera de la VCN.

STEP 9 | Configure el volumen de arranque de la instancia del dispositivo virtual Panorama.

1. En "Boot volume" (Volumen de arranque), seleccione **specify a custom boot volume size (especificar un tamaño de volumen de arranque personalizado)**.
2. En "Boot volume size" (Tamaño de volumen de arranque), escriba **81**.

STEP 10 | Haga clic en **Create (Crear)** para crear la imagen del dispositivo virtual Panorama.

STEP 11 | Inicie sesión en la CLI del dispositivo virtual Panorama desde la consola OCI.

1. Cómo generar una clave SSH para Panorama en OCI.
2. En la consola de OCI, seleccione **Instances (Instancias)** y seleccione la instancia del dispositivo virtual Panorama.
3. Seleccione **Console Connection (Conexión de la consola)** y **Create Console Connection (Crear conexión de consola)**.
4. Seleccione **Upload public key files (.pub) (Cargar archivos de clave pública [.pub])** y cargue la clave SSH pública que generó para **Create Console Connection (Crear conexión de consola)**.
5. En la pantalla "Instance Details" (Detalles de la instancia), expanda las opciones de conexión de consola y seleccione **Copy Serial Connection for Linux/Mac (Copiar conexión en serie para Linux/Mac)**.
6. En su máquina Linux, abra un terminal y pegue la conexión en serie.

STEP 12 | Configure una nueva contraseña de administración para el dispositivo virtual Panorama.

Debe configurar una contraseña administrativa única para poder acceder a la interfaz web o la CLI del dispositivo virtual Panorama. La nueva contraseña debe tener un mínimo de ocho

 ©2023 Palo Alto Networks, Inc.

caracteres e incluir un mínimo de un carácter en minúsculas, otro en mayúsculas y un número y un carácter especial.

Cuando inicia sesión por primera vez en la CLI de Panorama, se le solicita que introduzca la **contraseña anterior** y la **contraseña nueva** para el usuario `administrador` antes de que pueda continuar.

STEP 13 | Configure los ajustes de la dirección IP del sistema para el dispositivo virtual Panorama.

1. Configure las opciones de red iniciales para el dispositivo virtual Panorama.

```
admin> configure
```

```
admin#  set deviceconfig system type static
```

```
admin#  set deviceconfig system ip-address <instance-private-
IP address> netmask <netmask> default-gateway <default-
gateway-IP>
```

```
admin#  set deviceconfig system dns-setting servers primary
 <primary-dns-IP>
```

```
admin#  set deviceconfig system dns-setting servers secondary
 <secondary-dns-IP>
```

```
admin# commit
```

2. Compruebe que puede iniciar sesión en la interfaz web de Panorama.

   Si no puede iniciar sesión en la interfaz web de Panorama, revise la tabla de enrutamiento y las reglas de seguridad de VCN para asegurarse de que se crean las rutas y reglas de seguridad correctas.

 ©2023 Palo Alto Networks, Inc.

STEP 14 | Registre el dispositivo virtual Panorama y active la licencia de gestión de dispositivos y la licencia de asistencia técnica.

1. (Solo para licencias de VM Flex) Aprovisionamiento del número de serie del dispositivo virtual Panorama.

   Al aprovechar las licencias de VM Flex, este paso es necesario para generar el número de serie del dispositivo virtual Panorama necesario para registrarlo en el portal de atención al cliente (CSP) de Palo Alto Networks.

2. Registro de Panorama.

   Debe registrar el dispositivo virtual Panorama utilizando el número de serie proporcionado por Palo Alto Networks en el correo electrónico de entrega del pedido.

   Este paso no es necesario cuando se aprovechan las licencias de VM Flex, ya que el número de serie se registra automáticamente con el CSP cuando se genera.

3. Active una licencia de gestión de cortafuegos.

   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
   - Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

4. Active una licencia de asistencia técnica de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Complete la configuración del dispositivo virtual Panorama según las necesidades de su implementación.

- Para Panorama en modo de recopilación de logs.
  1. Cómo añadir un disco virtual a Panorama en Oracle Cloud Infrastructure (OCI) según sea necesario.

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo de recopilación de logs.
  2. Comience en el paso 6 para cambiar al modo de recopilación de logs.

     Introduzca la dirección IP pública del recopilador de logs dedicado cuando añada el recopilador de logs como un recopilador gestionado al servidor de gestión Panorama. No puede especificar la IP Address (Dirección IP), Netmask (Máscara de red) o Gateway (Puerta de enlace).
- Para Panorama en modo Panorama.
  1. Cómo añadir un disco virtual a Panorama en Oracle Cloud Infrastructure (OCI).

     Debe añadir un disco virtual de creación de logs antes de poder cambiar el dispositivo virtual Panorama al modo Panorama.
  2. Configuración de un dispositivo virtual Panorama en modo Panorama.
  3. Configuración de recopiladores gestionados.
- Para Panorama en el modo Solo gestión.
  1. Configure un dispositivo virtual Panorama en modo Solo gestión.
  2. Configuración de recopiladores gestionados para añadir un recopilador de logs dedicado al dispositivo virtual Panorama.

     El modo solo de gestión no admite la recopilación de logs y requiere un recopilador de logs dedicado para almacenar los logs.

Cómo generar una clave SSH para Panorama en OCI

Para conectarse al dispositivo virtual Panorama™ instalado en Oracle Cloud Infrastructure (OCI), debe generar una clave SSH pública y privada en una máquina Linux. Utilice la clave SSH generada para iniciar sesión en la CLI de Panorama a fin de configurar una nueva contraseña administrativa y configurar los ajustes de red de Panorama.

Se requiere una máquina Linux para generar la clave SSH y acceder a la CLI de Panorama para la configuración inicial. No se admite la generación de una SSH a partir de OCI o aplicaciones de terceros como PuTTygen.

STEP 1 | Abra el terminal en su máquina Linux.

STEP 2 | Desplácese hasta el directorio `.ssh` oculto.

```
admin:~$ cd~/.ssh
```

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Genere una clave SSH en el directorio `.ssh.`.

```
admin:~/.ssh$ ssh-keygen
```

Cuando se le solicite, guarde la clave en el directorio `.ssh` predeterminado. Una contraseña para la clave es opcional.

El nombre predeterminado de la clave privada es `id_rsa` y el nombre predeterminado de la clave pública es `id_rsa.pub`.

STEP 4 | Copie la clave pública del directorio `.ssh` al directorio principal.

Este paso es necesario para cargar la clave pública en OCI.

```
admin: ~/.ssh$ cp id_rsa.pub ~
```

Realización de la configuración inicial del dispositivo virtual Panorama

Según su modelo de Panorama, use Alibaba Cloud Console, AWS, Azure, GCP o la interfaz web de OCI, KVM Virtual Machine Manager, Hyper-V Manager, VMware vSphere Client o la consola web de vCloud Air para configurar el acceso de red al dispositivo virtual Panorama. De manera predeterminada, el dispositivo virtual Panorama se implementa en modo de Panorama. Para la creación de informes unificada, considere utilizar la Hora del meridiano de Greenwich (Greenwich Mean Time, GMT) o la Hora universal coordinada (Coordinated Universal Time, UTC) como la zona horaria uniforme en Panorama y todos los cortafuegos y recopiladores de logs gestionados.

STEP 1 | Obtenga la información necesaria de su administrador de red.

Reúna la siguiente información para la interfaz de gestión (MGT):

- Dirección IP para la interfaz de gestión (management, MGT)

  *La dirección IP predeterminada de la interfaz de gestión es 192.168.1.1 si no configura la interfaz de gestión como se describe cuando*instala el dispositivo virtual Panorama*.*

- Máscara de red
- Puerta de enlace predeterminada
- Dirección IP de servidor DNS

  Debe especificar la dirección IP, la máscara de red (para IPv4) o la longitud del prefijo (para IPv6) y la puerta de enlace predeterminada para acabar de configurar la interfaz de la interfaz MGT. Si omite ajustes (por ejemplo, la puerta de enlace predeterminada), puede acceder a Panorama a través del puerto de la consola para futuros cambios de configuración. Se recomienda confirmar siempre una configuración completa de la interfaz de MGT.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Acceda a la consola del dispositivo virtual Panorama.

Panorama usa la interfaz MGT para el tráfico de gestión, la sincronización de alta disponibilidad, la recopilación de logs y la comunicación en grupos de recopiladores.

A partir de PAN-OS 9.0.4, las credenciales de `administrador` predeterminadas ya no son compatibles. Cuando instala el dispositivo virtual Panorama por primera vez, debe iniciar sesión en la CLI de Panorama para configurar una contraseña de `administrador` única.

*Si es la primera vez que inicia sesión en la CLI de Panorama, se le solicitará que introduzca la **contraseña anterior** y la **contraseña nueva** para el usuario `administrador` antes de que pueda continuar con la configuración inicial del dispositivo virtual Panorama.*

1. Acceda a la consola.

   En un servidor ESXi:

   1. Inicie el cliente VMware vSphere.
   2. Seleccione la pestaña **Console (Consola)** para el dispositivo virtual Panorama y pulse Intro para acceder a la pantalla de inicio de sesión.

   En vCloud Air:

   1. Acceda a la consola web de vCloud Air y seleccione su región de **Virtual Private Cloud OnDemand (Nube privada virtual a petición)**.
   2. Seleccione la pestaña **Virtual Machines (Máquinas virtuales)**, haga clic derecho en la máquina virtual Panorama y seleccione **Open In Console (Abrir en consola)**.
2. Introduzca su nombre de usuario y contraseña para iniciar sesión (el valor predeterminado es admin para ambos).

   En Alibaba Cloud, AWS, Azure, GCP, KVM, Hyper-V y OCI:

   - Inicio de sesión en la CLI de Panorama.

STEP 3 | Defina la configuración de acceso a la red para la interfaz de gestión.

Panorama usa la interfaz MGT para el tráfico de gestión, la sincronización de alta disponibilidad, la recopilación de logs y la comunicación en grupos de recopiladores.

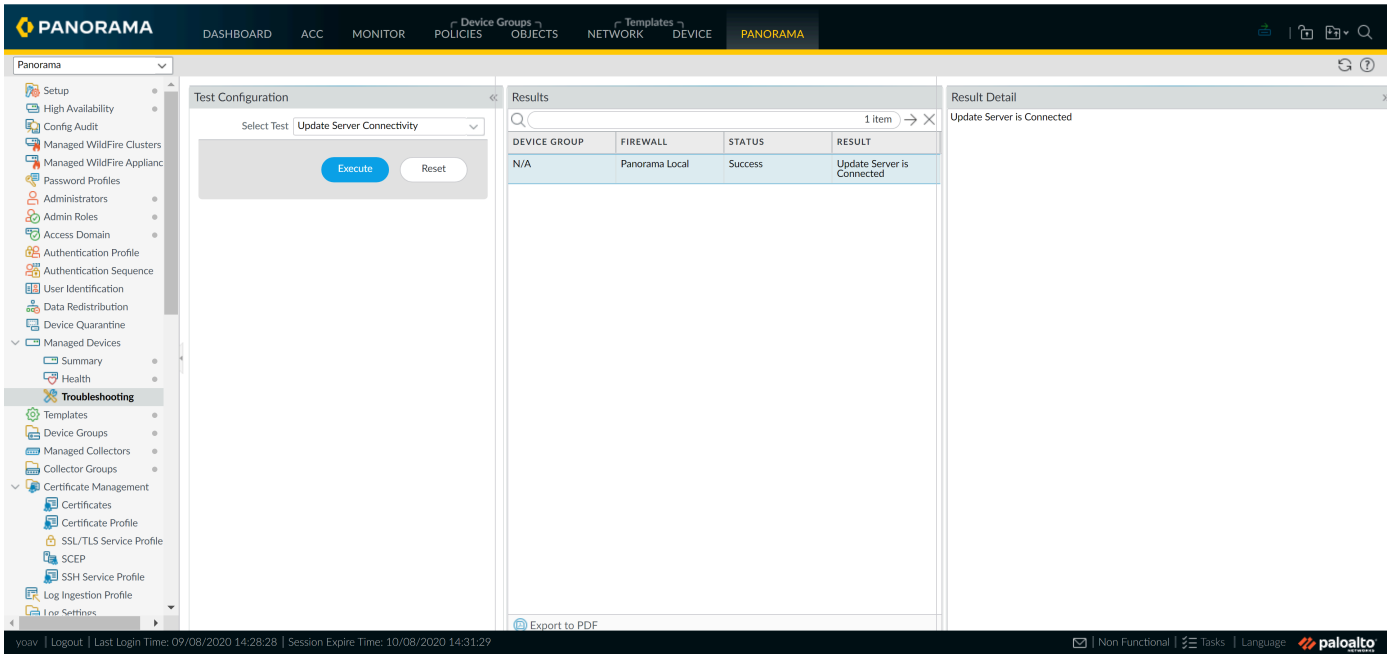
1. Introduzca los siguientes comandos, donde *<Panorama-IP>* es la dirección IP que quiere asignar a la interfaz de gestión de Panorama, *<netmask>* es la máscara de subred, *<gateway-IP>* es la dirección IP de la puerta de enlace de la red e *<DNS-IP>* es la dirección IP del servidor DNS.

   ```
   > configure # set deviceconfig system ip-address <Panorama-IP>
    netmask <netmask> default-gateway <gateway-IP> dns-setting
    servers primary <DNS-IP> # commit # exit
   ```

2. Solución de problemas de conectividad a recursos de red y verifique el acceso de red a los servicios externos indispensables para gestionar los cortafuegos, como el cortafuegos

 ©2023 Palo Alto Networks, Inc.

predeterminado, el servidor DNS y el servidor de actualizaciones de Palo Alto Networks, tal como se muestra en el ejemplo siguiente:



STEP 4 | Configure los ajustes generales.

1. Si usa una conexión segura (HTTPS) desde un navegador web, inicie sesión en la interfaz web de Panorama usando la dirección IP y la contraseña que asignó a la interfaz de gestión (https://<IP address>).
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
3. Introduzca el **Hostname (Nombre de host)** del servidor y el nombre de dominio de red en **Domain (Dominio)**. El nombre de dominio tan solo es una etiqueta. Panorama no lo utilizará para unirse al dominio.
4. Alinee el reloj de Panorama y de los cortafuegos gestionados para que utilicen la misma **Time Zone (Zona horaria)**, por ejemplo GMT o UTC. Si piensa usar Cortex Data Lake, debe configurar NTP para que Panorama pueda mantenerse sincronizado con Cortex Data Lake.

   Las marcas de tiempo se registran cuando Panorama recibe los logs y los cortafuegos gestionados generan los logs. La alineación de las zonas horarias en Panorama y en los cortafuegos garantiza que las marcas de tiempo estén sincronizadas y que el proceso de consulta de los logs y de generación de informes en Panorama sea armónico.
5. Introduzca los valores **Latitude (Latitud)** y **Longitude (Longitud)** para permitir la colocación precisa del servidor de gestión de Panorama en el mapamundi.
6. Introduzca el número de serie (**Serial Number [Número de serie]**) que recibió en el correo electrónico de procesamiento de pedido.
7. Haga clic en **OK (Aceptar)** para guardar los cambios.

©2023 Palo Alto Networks, Inc.

STEP 5 | (Optional) Modifique la configuración de la interfaz de gestión.

Para configurar la conectividad a Panorama con una dirección IP IPv6, debe configurar tanto una IPv4 como una IPv6 para configurar correctamente Panorama con una dirección IP IPv6. Panorama no admite la configuración de la interfaz de gestión con solo una dirección IP IPv6.

1. Seleccionar **Panorama** > **Setup (Configuración)** > **Interfaces (Interfaces)** y haga clic en **Management (Gestión)**.
2. Si sus cortafuegos se conectan al servidor de gestión de Panorama usando una dirección IP pública que se traduce en una dirección IP privada (NAT), introduzca la dirección IP pública en el campo **Public IP Address (Dirección IP pública)** y la dirección IP privada en el campo **IP Address (Dirección IP)** para enviar ambas direcciones a sus cortafuegos.
3. Seleccione qué Servicios de conectividad de red permitir en la interfaz (por ejemplo, acceso **SSH**).

   *No seleccione **Telnet** o **HTTP**. Estos servicios usan texto plano y son menos seguros que otros.*
4. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.

STEP 6 | Confirme sus cambios de configuración.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 7 | Pasos siguientes:

1. Si es necesario, amplíe la capacidad de almacenamiento de logs en el dispositivo virtual Panorama
2. (Recomendación) Sustituya el certificado predeterminado que Panorama usa para asegurar el tráfico HTTPS en la interfaz de MGT.
3. Active una licencia de asistencia técnica de Panorama.
4. Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
5. Instale las actualizaciones de contenido y software de Panorama.
6. Configuración del acceso administrativo a Panorama

Configuración del dispositivo virtual Panorama como un recopilador de logs

Si desea un dispositivo virtual dedicado para la recopilación de logs, configure un dispositivo virtual de Panorama en ESXi, Alibaba Cloud, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM, Hyper-V u Oracle Cloud Infrastructure (OCI) en modo de recopilación de logs. Para hacerlo, primero debe llevar a cabo la configuración inicial del dispositivo virtual en modo Panorama, que incluye la activación de licencias, la instalación de software y actualizaciones de contenido, y la configuración de la interfaz de gestión (MGT). Luego, cambie el dispositivo virtual Panorama a modo de recopilación de logs y complete la configuración del recopilador de logs. Además, si desea usar interfaces dedicadas Interfaces de dispositivos M-Series (recomendado) en lugar de la interfaz MGT

 ©2023 Palo Alto Networks, Inc.

para la recopilación de logs y la comunicación del grupo de recopiladores, primero debe configurar las interfaces para el servidor de gestión de Panorama, luego configurarlas para el recopilador de logs y luego, llevar a cabo una compilación de Panorama seguida de una compilación del grupo de recopiladores.

Realice los siguientes pasos para configurar un nuevo dispositivo virtual como un recopilador de logs o convertir un dispositivo virtual existente que se implementó previamente como un servidor de gestión de Panorama.

El cambio del dispositivo virtual del modo de Panorama al modo de recopilador de logs reinicia el dispositivo, elimina el recopilador de logs local, elimina todos los datos de logs existentes y elimina todas las configuraciones excepto los ajustes de acceso de gestión. Si cambia el modo, no se eliminan las licencias ni las actualizaciones de software o contenido.

STEP 1 | Configure el servidor de gestión del dispositivo virtual Panorama que gestionará el recopilador de logs si ya no lo ha hecho.

Lleve a cabo una de las siguientes tareas:

- Configuración del dispositivo virtual Panorama
- Configuración del dispositivo de la serie M

STEP 2 | Registre la dirección IP de gestión del servidor de gestión de Panorama.

Si implementó Panorama en una configuración de alta disponibilidad (high availability, HA), necesita la dirección IP de cada peer de HA.

1. Inicie sesión en la interfaz web del servidor de gestión de Panorama.
2. Registre el valor en **IP Address (Dirección IP)** del Panorama solitario (no HA) o activo (HA) seleccionando **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y revisando la configuración de Interfaz de gestión.
3. Para una implementación de HA, registre el valor en **Peer HA IP Address (Dirección IP del peer de HA)** del Panorama pasivo seleccionando **Panorama** > **High Availability (Alta disponibilidad)** y revisando la sección Configuración.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el dispositivo virtual Panorama que servirá como recopilador de logs dedicado.

Si previamente implementó este dispositivo como servidor de gestión de Panorama, puede omitir este paso porque la interfaz MGT ya está configurada y las licencias y actualizaciones ya están instaladas.

El dispositivo virtual Panorama en el modo de recopilación de logs no tiene una interfaz web para las tareas de configuración, solo una CLI. Por lo tanto, antes de cambiar el modo en el dispositivo virtual Panorama, utilice la interfaz web en modo Panorama para realizar los siguientes pasos:

1. Configure el dispositivo virtual Panorama en uno de los siguientes hipervisores compatibles:
   - Instalación de Panorama en un servidor ESXi
   - Instalación de Panorama en Alibaba Cloud
   - Instalación de Panorama en AWS
   - Instalación de Panorama en AWS GovCloud
   - Instalación de Panorama en Azure
   - Instalación de Panorama en Google Cloud Platform
   - Instalación de Panorama en Hyper-V
   - Configuración de Panorama en Oracle Cloud Infrastructure (OCI)
2. Realice la configuración inicial del dispositivo virtual Panorama.
3. Registre Panorama e instale las licencias.
4. Instale las actualizaciones de contenido y software de Panorama.

STEP 4 | (Solo Panorama en Azure) Modifique la contraseña de administrador.

El recopilador de logs dedicado solo admite el usuario administrador admin para cambiar al modo de recopilador de logs. Modifique la contraseña de admin para permitirle iniciar sesión con el usuario administrador admin.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Administrators (Administradores)** y seleccione **Admin**.
3. Especifique el valor de **Password (Contraseña)**, haga clic en **Confirm Password (Confirmar contraseña)** y en **OK (Aceptar)**.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 5 | (Solo en Panorama en AWS y Azure) Elimine todos los usuarios, excepto el usuario administrador.

1. Lleve a cabo el Inicio de sesión en la interfaz web de Panorama como admin.
2. Seleccione **Panorama** > **Administrators (Administradores)**.
3. Seleccione los administradores existentes, excepto admin y haga clic en **Delete (Eliminar)**.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 6 | Inicio de sesión en la CLI de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Cambie del modo Panorama al modo de recopilación de logs.

1. Para cambiar al modo de recopilación de logs, introduzca el siguiente comando:

```
> request system system-mode logger
```

2. Ingrese **Y** para confirmar el cambio de modo. El dispositivo virtual se reinicia. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectarse al dispositivo virtual para ver la solicitud de inicio de sesión a Panorama.

   *Si ve la solicitud **CMS Login**, esto significa que el recopilador de logs finalizó el reinicio. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.*

3. Vuelva a iniciar sesión en la CLI.
4. Verifique que el cambio al modo de recopilador de logs se realizó correctamente:

```
> show system info | match system-mode
```

   Si el cambio de modo es correcto, se muestra lo siguiente:

```
system-mode: logger
```

STEP 8 | Habilite la conectividad entre el recopilador de logs y el servidor de gestión de Panorama.

Introduzca los siguientes comandos en la CLI del recopilador de logs, donde *<IPaddress1>* es para la interfaz de MGT del Panorama solitario (no HA) o activo (HA) y *<IPaddress2>* es para la interfaz de MGT del Panorama pasivo (HA), si corresponde.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 9 | Registro del número de serie del recopilador de logs.

Necesitará el número de serie para añadir el recopilador de logs como recopilador gestionado en el servidor de gestión de Panorama.

1. En la CLI del recopilador de logs, introduzca el siguiente comando para mostrar su número de serie:

```
> show system info | match serial
```

2. Registre el número de serie.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Añada el recopilador de logs como recopilador gestionado en el servidor de gestión de Panorama.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir un recopilador gestionado.
2. En la configuración **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el recopilador de logs.
3. En el campo **Panorama Server IP (IP del servidor de Panorama)**, introduzca la dirección IP o el FQDN del Panorama solitario (no HA) o activo (HA). Para una implementación de HA, introduzca la dirección IP o el FQDN del peer pasivo de Panorama en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)**.

   Estas direcciones IP deben especificar una interfaz Panorama que tenga servicios **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo** habilitados. De forma predeterminada, estos servicios solo están disponibles en la interfaz MGT. Sin embargo, es posible que haya habilitado los servicios en otras interfaces cuando realizó la Configuración del dispositivo M-Series que es un servidor de gestión de Panorama.
4. Seleccione **Interfaces**, haga clic en **Management (Gestión)** e introduzca la **Public IP Address (Dirección IP pública)** del recopilador de logs dedicado.
5. Haga clic en **OK (Aceptar)** dos veces para guardar los cambios en el recopilador de logs.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.
7. Verifique que **Panorama** > **Managed Collectors (Recopiladores gestionados)** muestre en la lista el recopilador de logs que añadió. La columna Conectado muestra un icono de marca de verificación para indicar que el recopilador de logs está conectado a Panorama. Es posible que deba esperar unos minutos para que la página muestre el estado de conexión actualizado.

   En este punto, la columna Estado de configuración muestra Out of Sync y la columna Estado de tiempo de ejecución muestra disconnected (desconectado). El estado cambiará a In Sync (Sincronizado) y connected (conectado) después de que configure un grupo de recopiladores.

STEP 11 | Habilite los discos de registro.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada disco.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 12 | (Recomendado) Configure las interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** y **Ethernet5** si el servidor de gestión de Panorama y recopilador de logs los usará para la **Device**

 ©2023 Palo Alto Networks, Inc.

Log Collection (Recopilación de logs del dispositivo) [recepción de logs del cortafuegos] y **Collector Group Communication (Comunicación del grupo de recopiladores)**.

Si implementó previamente el recopilador de logs como un servidor de gestión de Panorama y configuró estas interfaces, debe volver a configurarlas porque al cambiar al modo de recopilador de logs habría borrado todas las configuraciones excepto la configuración de acceso a gestión.

1. Configure cada interfaz en el servidor de gestión de Panorama (que no sea la interfaz MGT) si aún no lo ha hecho:
   1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces** y haga clic en el nombre de la interfaz.
   2. Seleccione ***<interface-name>*** para habilitar la interfaz.
   3. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:
      - Para ESXi
        - IPv4: **Public IP Address (Dirección IP pública)**, **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

          IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
      - Para Alibaba Cloud, AWS, Azure, GCP y OCI
        - **Dirección IP pública**
   4. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

      Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo: puede asignar una o más interfaces.

      Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.

      Device Deployment (Implementación de dispositivos) [software y actualizaciones de contenido]: puede asignar solo una interfaz.
   5. Haga clic en **OK (Aceptar)** para guardar los cambios.
2. Configure cada interfaz en el recopilador de logs (que no sea la interfaz MGT):
   1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
   2. Seleccione **Interfaces** y haga clic en el nombre de la infertfaz.
   3. Seleccione ***<interface-name>*** para habilitar la interfaz.
   4. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:
      - Para ESXi
        - IPv4: **Public IP Address (Dirección IP pública)**, **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

 ©2023 Palo Alto Networks, Inc.

IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**

- Para Alibaba Cloud, AWS, Azure, GCP y OCI
  - **Dirección IP pública**

5. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

   Device Log Collection (Recopilación de logs del dispositivo): puede asignar una o más interfaces.

   Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.

6. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.

3. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 13 | (Opcional) Si su implementación utiliza certificados personalizados para la autenticación entre Panorama y los dispositivos gestionados, implemente el certificado de dispositivo cliente personalizado. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y elija el perfil del certificado del menú desplegable o haga clic en **New Certificate Profile (Nuevo perfil de certificado)** para crear uno.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)** para un recopilador de logs.
3. Seleccione la casilla de verificación **Secure Client Communication (Comunicación de cliente segura)**.
4. Seleccione el tipo de certificado de dispositivo en el menú desplegable Tipo.
   - Si está utilizando un certificado de dispositivo local, seleccione **Certificate (Certificado)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
   - Si está utilizando SCEP como certificado del dispositivo, seleccione el **SCEP Profile (Perfil de SCEP)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
5. Haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 14 | (Opcional) Configure la comunicación de servidor segura en un recopilador de logs. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)**.
2. Verifique que la casilla de verificación **Custom Certificate Only (Certificado personalizado únicamente)** no está seleccionada. Esto le permite continuar gestionando todos los dispositivos mientras migra a certificados personalizados.

   Cuando se selecciona la casilla de verificación Certificado personalizado únicamente, el Recopilador de logs no se autentica y no puede recibir logs de dispositivos que usan certificados predefinidos.
3. Seleccione el perfil del servicio SSL/TLS del menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre el recopilador de logs y los dispositivos que le envían los logs.
4. Seleccione el perfil de certificado del menú desplegable **Certificate Profile (Perfil del certificado)**.
5. Seleccione **Authorize Client Based on Serial Number (Autorizar clientes según el número de serie)** para hacer que el servidor compruebe los clientes contra los números de serie de los dispositivos gestionados. El certificado de cliente debe tener la palabra clave especial $UDID establecida como CN para autorizar según los números de serie.
6. En **Disconnect Wait Time (min) (Tiempo de espera para desconexión [min])**, introduzca los minutos que debe esperar Panorama antes de interrumpir y restablecer la conexión con los dispositivos que gestiona. Este campo está en blanco por defecto y el rango es de 0 a 44,640 minutos.

   El tiempo de espera de desconexión no comienza la cuenta atrás hasta que confirme la nueva configuración.
7. (Opcional) Configure una lista de autorizaciones.
   1. Haga clic en **Add (Añadir)** en lista de autorizaciones.
   2. Seleccione el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** como el tipo de Identificador.
   3. Introduzca un identificador del tipo seleccionado.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Check Authorization List (Comprobar lista de autorización)** para hacer cumplir la lista de autorizaciones.
8. Haga clic en **OK (Aceptar)**.
9. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 15 | Asigne el recopilador de logs a un grupo de recopiladores.

1. Configure un grupo de recopiladores. Debe llevar a cabo una compilación de Panorama y luego una del grupo de recopiladores para sincronizar la configuración del recopilador de

 ©2023 Palo Alto Networks, Inc.

logs con Panorama y colocar las interfaces Eth1, Eth2, Eth3, Eth4 y Eth5 (si las configuró) en un estado operativo en el recopilador de logs.

Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.

*Se recomienda **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si añade varios recopiladores de logs a un solo grupo de recopiladores. Esta opción requiere que cada recopilador de logs tenga el mismo número de discos de creación de logs.*

2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que la configuración del recopilador de logs se sincronizó con Panorama.

   La columna Estado de configuración debe mostrar In Sync (Sincronizado) y la columna Estado de tiempo de ejecución muestra connected (conectado).

3. Acceda a la CLI del recopilador de logs e ingrese el siguiente comando para verificar que sus interfaces son funcionales:

   ```
   > show interface all
   ```

   El resultado muestra `state` como `up` para cada interfaz que sea funcional.

4. Si el grupo tiene varios recopiladores de logs, consulte Solución de problemas de conectividad a recursos de red, para verificar que se pueden comunicar entre sí, ejecute una prueba de conectividad con ping en todas las interfaces que emplean los recopiladores. En la dirección IP de `source (origen)`, especifique la interfaz de uno de los recopiladores de logs. Para la dirección IP `host`, especifique la interfaz de coincidencia de otro recopilador de logs en el mismo grupo de recopiladores.

STEP 16 | Pasos siguientes:

Para permitir que el recopilador de logs reciba logs del cortafuegos:

1. Configure el reenvío de logs a Panorama.
2. Verifique el reenvío de logs a Panorama.

Configuración del dispositivo virtual Panorama con recopiladores de logs locales

Si el dispositivo virtual Panorama está en modo heredado después de actualizar de Panorama 8.0 o una versión anterior a Panorama 8.1 o una versión posterior, cambie al modo Panorama con el fin de crear un recopilador de logs local, añada varios discos de logging sin perder los logs existentes, aumente el almacenamiento de logs hasta 24 TB y habilite una generación de informes más ágil.

Cuando cambie de modo heredado a modo Panorama, el modo heredado ya no estará disponible.

 ©2023 Palo Alto Networks, Inc.

Después de actualizar a Panorama 8.1, el primer paso es aumentar los recursos del sistema en el dispositivo virtual al mínimo requerido para el modo Panorama. Panorama se reinicia cuando aumenta los recursos, por lo tanto, realice este procedimiento durante una periodo de mantenimiento. Debe instalar un disco de sistema más grande (81 GB), aumentar las CPU y memoria en función de la capacidad de almacenamiento del log y añadir un disco de logging virtual. El nuevo disco de logging debe tener al menos la misma capacidad que el dispositivo utiliza actualmente en el modo heredado y no puede ser inferior a 2 TB. La adición de un disco virtual le permite migrar logs existentes al Recopilador de logs y permite que el Recopilador de logs almacene logs nuevos.

Si Panorama se implementa en una configuración de HA, realice los siguientes pasos en el peer secundario y luego, en el peer principal.

STEP 1 | Determine qué recursos del sistema debe aumentar antes de que el dispositivo virtual pueda operar en modo Panorama.

Debe ejecutar el comando especificado en este paso, incluso si ha determinado que Panorama ya cuenta con los recursos adecuados.

1. Acceda a la CLI de Panorama:
   1. Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP que especificó para la interfaz de MGT de Panorama.
   2. Inicie sesión en la CLI cuando se le solicite.
2. Compruebe los recursos que debe aumentar mediante la ejecución del siguiente comando:

```
> request system system-mode panorama
```

Introduzca **y** cuando se le solicite continuar. El resultado especifica los recursos que debe aumentar. Por ejemplo:

```
El modo Panorama no es compatible con el disco del sistema
 actual de tamaño 52,0 GB. Conecte un disco de tamaño 81,0 GB
 y, a continuación, utilice  request system clone-system-disk
 para migrar el disco del sistema actual. Añada un nuevo disco
 de creación de logs virtual con más de 50,00 GB de capacidad
 de almacenamiento. No hay suficientes núcleos de CPU: Se
 encontraron 4 núcleos, se necesitan 8 núcleos
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Aumente las CPU y la memoria, y reemplace el disco del sistema con un disco más grande.

1. En el cliente VMware ESXi vSphere, seleccione **Virtual Machines (Máquinas virtuales)**, haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
2. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
3. Seleccione **Memory (Memoria)** e introduzca el nuevo **Memory Size (Tamaño de la memoria)**.
4. Seleccione **CPUs (CPU)** y especifique el número de CPU (el valor en **Number of virtual sockets [Número de conectores virtuales]** multiplicado por el valor en **Number of cores per socket [Número de núcleos por conector]**).
5. Añada un disco virtual.

   Utilizará este disco para reemplazar el disco de sistema existente.

   1. En la configuración de **Hardware**, seleccione **Add (Añadir)** un disco, seleccione **Hard Disk (Disco duro)** como el tipo de hardware, y haga clic en **Next (Siguiente)**.
   2. Seleccione **Create a new virtual disk (Crear un nuevo disco virtual)** y haga clic en **Next (Siguiente)**.
   3. Establezca el **Disk Size (Tamaño de disco)** a exactamente 81 GB y seleccione el formato de disco **Thick Provision Lazy Zeroed (Suministro estándar diferido a cero)**.
   4. Seleccione **Specify a datastore or datastore structure (Especifique una estructura de almacén de datos o almacén de datos)** como la ubicación, seleccione **Browse**

 ©2023 Palo Alto Networks, Inc.

(Examinar) y vaya a un almacén de datos que tenga al menos 81 GB, haga clic en **OK (Aceptar)** y en **Next (Siguiente)**.

5. Seleccione un **Virtual Device Node (Nodo de dispositivo virtual)** en formato de Interfaz de sistemas de ordenador pequeño (Small Computer Systems Interface, SCSI) (puede usar la selección predeterminada) y haga clic en **Next (Siguiente)**.

   Panorama no arrancará si selecciona un formato que no sea SCSI.

6. Verifique que la configuración sea correcta y luego haga clic en **Finish (Terminar)** y **OK (Aceptar)**.

6. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**. Espere a que Panorama se reinicie antes de continuar.
7. Regrese a la CLI de Panorama y copie los datos del disco de sistema original al nuevo disco del sistema:

   ```
   > request system clone-system-disk target sdb
   ```

   Introduzca **y** cuando se le solicite continuar.

   El proceso de copia tarda alrededor de 20 a 25 minutos, durante los cuales Panorama se reinicia. Cuando el proceso finaliza, el resultado le solicita que cierre Panorama.
8. Vuelva a la consola del cliente vSphere, haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
9. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
10. Seleccione el disco del sistema original, haga clic **Remove (Retirar)**, seleccione **Remove from virtual machine (Eliminar de la máquina virtual)** y haga clic **OK (Aceptar)**.
11. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
12. Seleccione el nuevo disco del sistema, establezca el **Virtual Device Node (Nodo de dispositivo virtual)** a **SCSI (0: 0)** y haga clic en **OK (Aceptar)**.
13. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**. Antes de continuar, espere a que Panorama se reinicie en el nuevo disco de sistema (alrededor de 15 minutos).

STEP 3 | Añada un disco de logging virtual.

Este es el disco al que migrarán los logs existentes.

1. En el cliente VMware ESXi vSphere, haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
2. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
3. Repita los pasos para Añadir un disco virtual. Establezca el **Disk Size (Tamaño de disco)** a un múltiplo de 2 TB basado en la cantidad de almacenamiento de logs que necesita. La capacidad debe ser al menos tan grande como el disco virtual existente o el almacenamiento NFS que Panorama utiliza actualmente para los logs. La capacidad del disco debe ser un múltiplo de 2 TB y puede ser de hasta 24 TB. Por ejemplo, si el disco

 ©2023 Palo Alto Networks, Inc.

existente tiene 5 TB de almacenamiento de logs, debe añadir un nuevo disco de al menos 6 TB.

Después de cambiar al modo Panorama, Panorama dividirá automáticamente el nuevo disco en particiones de 2 TB, cada una de las cuales funcionará como un disco virtual independiente.

4. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**. Espere a que Panorama se reinicie antes de continuar.

STEP 4 | Cambie del modo Legacy al modo Panorama.

Después de cambiar el modo, el dispositivo se reinicia y luego crea automáticamente un recopilador de logs local y un grupo de recopiladores. Los logs existentes no estarán disponibles para consultas o informes hasta que los migre más adelante en este procedimiento.

1. Regrese a la CLI de Panorama y ejecute el siguiente comando.

```
> request system system-mode panorama
```

Introduzca **y** cuando se le solicite continuar. Después de reiniciar, Panorama crea automáticamente un recopilador de logs local (llamado Panorama) y crea un grupo de recopiladores (denominado por defecto) para contenerlo. Panorama también configura el disco de logging virtual que usted ha añadido y lo divide en discos separados de 2 TB. Espere a que el proceso finalice y que Panorama se reinicie (alrededor de cinco minutos) antes de continuar.

2. Inicie sesión en la interfaz web de Panorama.
3. En el **Dashboard (Panel)**, la configuración **General Information (Información general)**, verifique que el **Mode (Modo)** es ahora **panorama**.

En una implementación de HA, el par secundario está en un estado suspendido en este punto porque su modo (Panorama) no coincide con el modo en el peer primario (Legacy).

 ©2023 Palo Alto Networks, Inc.

Retirará la suspensión del peer secundario después de cambiar el peer primario al modo Panorama más adelante en este procedimiento.

4. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** para verificar que el grupo de recopilador **default (predeterminado)** se haya creado y que el recopilador de logs local sea parte del grupo de recopiladores predeterminado.
5. Envíe la configuración a los dispositivos gestionados.
   - Si no existen cambios pendientes:
     1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
     2. Seleccione **Collector Group (Grupo de recopiladores)** y asegúrese de que el grupo de recopiladores **default (predeterminado)** se haya seleccionado.
     3. Haga clic en **OK (Aceptar)** y **Push (Enviar)**.
   - Si existen cambios pendientes:
     1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y, luego, en **Edit Selections (Editar selección)**.
     2. Verifique que se incluyan los dispositivos y las **Templates (Plantillas)** en su **Device Group (Grupo de dispositivos)**.
     3. Seleccione **Collector Group (Grupo de recopiladores)** y asegúrese de que el grupo de recopiladores **default (predeterminado)** se haya seleccionado.
     4. Haga clic en **OK (Aceptar)** y en **Commit and Push (Confirmar y enviar)**.
6. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y compruebe que las columnas muestran la siguiente información para el recopilador de logs local.
   - Nombre del recopilador: de forma predeterminada, es el nombre de host de Panorama. Debería estar listado bajo el Grupo de recopiladores **predeterminado**.
   - Conectado: marca de verificación
   - Estado de configuración: sincronizado
   - Estado del tiempo de ejecución: Conectado

STEP 5 | (Solo HA) Cambie el Panorama principal del modo heredado al modo Panorama.

Este paso activa la conmutación por error.

1. Repita del paso 1 al paso 4 en el Panorama principal.

   Espere a que el Panorama principal se reinicie y vuelva a un estado HA activo. Si la opción de preferencia no está habilitada, debe realizar la conmutación por recuperación manualmente: seleccione **Panorama** > **High Availability (Alta disponibilidad)** y, en la sección Operational Commands (Comandos operativos), **Make local Panorama functional (Hacer que la instancia local de Panorama sea funcional)**.
2. En el Panorama principal, seleccione **Dashboard (Panel)** y, en la sección de Alta disponibilidad, **Sync to peer (Sincronizar en el peer)**, haga clic en **Yes (Sí)** y espere a

 ©2023 Palo Alto Networks, Inc.

que la **Running Config (Configuración en ejecución)** muestre el estado **Synchronized (Sincronizado)**.

3. En el Panorama secundario, seleccione **Panorama** > **High Availability (Alta disponibilidad)** y, en la sección Comandos de operación, haga clic en **Make local Panorama functional (Hacer Panorama local funcional)**.

   Este paso es necesario para sacar el Panorama secundario de su estado de HA suspendido.

STEP 6 | Migre los logs existentes a los nuevos discos virtuales de logging.

Si implementó Panorama en una configuración HA, realice esto solo en el peer principal.

Palo Alto Networks recomienda migrar los logs existentes a los nuevos discos virtuales de creación de logs durante su período de mantenimiento. La migración de logs requiere una gran cantidad de núcleos de CPU del dispositivo virtual Panorama para ejecutarse y afecta el rendimiento operativo de Panorama.

1. Vuelva a la CLI de Panorama.
2. Inicie la migración de logs:

   ```
   > request logdb migrate vm start
   ```

   La duración del proceso varía según el volumen de datos de logs que está migrando. Para ver el estado del RAID, ejecute el comando siguiente:

   ```
   > request logdb migrate vm status
   ```

   Cuando la migración finaliza, el resultado muestra: `migrationhas been done (Se realizó la migración)`.
3. Verifique que los logs existentes están disponibles.
   1. Inicie sesión en la interfaz web de Panorama.
   2. Seleccione **Panorama** > **Monitor (Supervisar)**, seleccione un tipo de log que sepa que coincide con algunos logs existentes (por ejemplo, **Panorama** > **Monitor [Supervisar]** > **System [Sistema]**) y verifique que se muestren los logs.

STEP 7 | Pasos siguientes:

Configure el reenvío de logs a Panorama para que el Recopilador de logs reciba nuevos logs de los cortafuegos.

Configuración de un dispositivo virtual Panorama en modo Panorama

El modo Panorama permite al dispositivo virtual Panorama™ funcionar como un servidor de gestión de Panorama con capacidades de recopilación de logs locales. De forma predeterminada, el dispositivo virtual Panorama se implementa en modo Panorama cuando al menos un disco de virtual de creación de logs está conectado a un dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

Aunque sigue siendo compatible, no se recomienda cambiar del modo heredado con un disco de creación de logs de 50 GB al modo Panorama para entornos de producción. Si cambia al modo Panorama con un disco de creación de logs de 50 GB, no podrá añadir discos de creación de logs adicionales.

STEP 1 | Inicio de sesión en la CLI de Panorama.

STEP 2 | Cambie a modo Panorama.

1. Cambie a modo Panorama:

```
> request system system-mode panorama
```

2. Ingrese **Y** para confirmar el cambio de modo. El dispositivo virtual Panorama se reinicia. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectarse al dispositivo virtual Panorama para ver la solicitud de inicio de sesión a Panorama.

   Si ve la solicitud `CMS Login`, esto significa que el reinicio del dispositivo virtual Panorama no finalizó. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.

STEP 3 | Verifique que el cambio al modo Panorama se realizó correctamente.

1. Vuelva a iniciar sesión en la CLI.
2. Verifique que el cambio al modo Panorama se realizó correctamente:

```
> show system info | match system-mode
```

   Si el cambio de modo es correcto, se muestra lo siguiente:

```
> system mode:panorama
```

Configuración de un dispositivo virtual Panorama en modo solo de gestión

El modo solo de gestión le permite al dispositivo virtual Panorama funcionar como un servidor de gestión de Panorama sin capacidades de recopilación de logs locales. De manera predeterminada, el dispositivo virtual Panorama está en modo Panorama para la implementación inicial. Se recomienda cambiar el modo del dispositivo virtual Panorama al modo solo de gestión inmediatamente después de la implementación inicial debido a que el cambio al modo solo de gestión requiere que no se reenvíen logs al servidor de gestión de Panorama porque el dispositivo virtual Panorama en modo solo de gestión no admite la recopilación de logs. Después de cambiar al modo solo de gestión, los datos de logs existentes almacenados en el dispositivo virtual Panorama no se pueden acceder, y el ACC y las funciones de creación de informes no pueden consultar los logs almacenados en el dispositivo virtual Panorama.

(Panorama en modo heredado) El dispositivo virtual Panorama no afecta al dispositivo virtual Panorama cuando se cambia el dispositivo virtual Panorama del modo heredado al modo de solo administración. Como medida de precaución, Palo Alto Networks recomienda tomar una instantánea

 ©2023 Palo Alto Networks, Inc.

de la máquina virtual del dispositivo virtual Panorama que puede utilizar para restaurar Panorama en caso de impacto inesperado.

> ***Si configuró un** recopilador de registros local**, el recopilador de logs local sigue existiendo en Panorama cuando cambia al modo Solo gestión a pesar de no tener capacidades de recopilación de logs. Cuando se elimina el recopilador de logs local (**Panorama** > **Managed Collectors [Recopiladores gestionados]**) se elimina la configuración de interfaz Eth1/1 que utiliza el recopilador de logs de forma predeterminada. Si decide eliminar el recopilador de logs local, debe** volver a configurar la interfaz Eth1/1**.*

STEP 1 | Inicio de sesión en la CLI de Panorama.

STEP 2 | Cambie a modo solo de gestión.

1. Cambie a modo solo de gestión:

   ```
   > request system system-mode management-only
   ```

2. Ingrese **Y** para confirmar el cambio de modo. El dispositivo virtual Panorama se reinicia. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectarse al dispositivo virtual Panorama para ver la solicitud de inicio de sesión a Panorama.

   Si ve la solicitud `CMS Login`, esto significa que el reinicio del dispositivo virtual Panorama no finalizó. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.

STEP 3 | Verifique que el cambio al modo solo de gestión se realizó correctamente.

1. Vuelva a iniciar sesión en la CLI.
2. Verifique que el cambio al modo solo de gestión se realizó correctamente:

   ```
   > show system info | match system-mode
   ```

   Si el cambio de modo es correcto, se muestra lo siguiente:

   ```
   > system mode:management-only
   ```

Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual Panorama

Después de que se lleve a cabo la Realización de la configuración inicial del dispositivo virtual Panorama, la capacidad de almacenamiento de logs disponible y las opciones de expansión dependen de la plataforma virtual (VMware ESXi, vCloud Air, Alibaba Cloud, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM, Hyper-V u OCI) y el modo (heredado, Panorama o recopilador de logs): consulte Modelos de Panorama para obtener información detallada.

Para ampliar la capacidad de almacenamiento de logs en el dispositivo virtual Panorama, debe añadir discos de creación de logs adicionales. No se admite la expansión de la capacidad de almacenamiento de logs de un disco de creación de logs existente, y Panorama no reconoce la capacidad de almacenamiento adicional. Por ejemplo; si añadió un disco de creación de logs de 2 TB

 ©2023 Palo Alto Networks, Inc.

y luego amplió ese disco de creación de logs existente a 4 TB, Panorama continuará reconociendo que el disco de creación de logs tiene 2 TB de capacidad de almacenamiento e ignorará los 2 TB adicionales de capacidad de almacenamiento.

Para obtener almacenamiento adicional, también puede reenviar los logs del cortafuegos a los recopiladores de logs dedicados (consulte Configuración de un recopilador gestionado*) o* configurar el reenvío de logs desde Panorama a destinos externos.

Antes de ampliar la capacidad de almacenamiento de logs en Panorama, lleve a cabo la Determinación de los requisitos de almacenamiento de logs de Panorama.

- Conserve logs existentes al añadir almacenamiento en el dispositivo virtual Panorama en modo heredado
- Cómo añadir un disco virtual a Panorama en un servidor ESXi
- Cómo añadir un disco virtual a Panorama en vCloud Air
- Cómo añadir un disco virtual a Panorama en Alibaba Cloud
- Cómo añadir un disco virtual a Panorama en AWS
- Cómo añadir un disco virtual a Panorama en Azure
- Cómo añadir un disco virtual a Panorama en Google Cloud Platform
- Cómo añadir un disco virtual a Panorama en KVM
- Cómo añadir un disco virtual a Panorama en Hyper-V.
- Cómo añadir un disco virtual a Panorama en Oracle Cloud Infrastructure (OCI)
- Montaje de servidor ESXi de Panorama en un almacén de datos NFS

Conserve logs existentes al añadir almacenamiento en el dispositivo virtual Panorama en modo heredado

El dispositivo virtual Panorama en modo heredado solo puede usar un disco virtual para la creación de logs. Por lo tanto, si añade un disco virtual que esté dedicado a los logs, Panorama deja de utilizar el almacenamiento de logs predeterminado de 11 GB en el disco del sistema y copia automáticamente los logs existentes en el disco nuevo. (Panorama continúa usando el disco del sistema para los datos que no sean logs).

Si reemplaza un disco de registro dedicado existente de hasta 2 TB de almacenamiento con un disco de hasta 8 TB, perderá los logs en el disco existente. Para conservar los logs, tiene las siguientes opciones:

- Configure el reenvío de logs a destinos externos antes de reemplazar el disco virtual.
- Configure un nuevo dispositivo virtual Panorama para el disco nuevo de 8 TB y conserve el acceso a Panorama que tiene el disco anterior mientras necesite los logs. Para reenviar logs de cortafuegos al nuevo dispositivo virtual Panorama, una opción es volver a configurar los cortafuegos para conectarlos con la nueva dirección IP de Panorama (seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama), añada los cortafuegos como dispositivos gestionados al nuevo Panorama y Configuración del reenvío de logs a Panorama. Para reutilizar la dirección IP anterior de Panorama en el nuevo Panorama, otra opción es exportar la configuración del Panorama anterior y luego importar y cargar la configuración al nuevo Panorama.

 ©2023 Palo Alto Networks, Inc.

- Copie los logs del disco anterior al disco nuevo. La copia de logs puede tardar varias horas, según la cantidad de logs que el disco almacena actualmente; y Panorama no puede recopilar logs durante el proceso. Comuníquese con Atención al cliente de Palo Alto Networks para obtener instrucciones.

Cómo añadir un disco virtual a Panorama en un servidor ESXi

Para ampliar la capacidad de almacenamiento de logs en el dispositivo virtual Panorama, puede añadir discos de logging virtual. Si el dispositivo está en modo Panorama, puede añadir de 1 a 12 discos virtuales de creación de logs de 2 TB cada uno o un disco de creación de logs de 24 TB, para un total máximo de 24 TB. Si el dispositivo está en modo heredado, puede añadir un disco de logging virtual de hasta 8 TB en ESXi 5.5 y versiones posteriores o un disco de hasta 2 TB en versiones anteriores de ESXi. Además, se recomienda añadir discos de registro con el mismo formato de aprovisionamiento de disco para evitar cualquier rendimiento inesperado que pueda surgir por tener varios discos con diferentes formatos de aprovisionamiento.

Si Panorama pierde conectividad con el nuevo disco virtual, es posible que Panorama pierda los logs durante el intervalo de fallo.

Para permitir la redundancia, utilice el disco virtual en una configuración de RAID. RAID 10 ofrece el mejor rendimiento de escritura para aplicaciones con características de registro elevado.

Si es necesario, puede reemplazar el disco virtual en un servidor ESXi*.*

STEP 1 | Añada discos adicionales a Panorama

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. Acceda al cliente VMware vSphere y seleccione **Virtual Machines (Máquinas virtuales)**.
2. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
3. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar ajustes)**.
4. Haga clic en **Add (Añadir)** en la pestaña **Hardware** para iniciar el asistente de adición de hardware.
5. Seleccione **Hard disk (Disco duro)** como el tipo de hardware y haga clic en **Next (Siguiente)**.
6. Seleccione **Create a new virtual disk (Crear un nuevo disco virtual)** y haga clic en **Next (Siguiente)**.
7. Configure el **Disk Size (Tamaño de disco)**. Si el dispositivo virtual Panorama está en modo Panorama, configure el tamaño en al menos 2 TB. Si el dispositivo está en modo heredado, puede establecer el tamaño en hasta 8 TB.

 ©2023 Palo Alto Networks, Inc.

En el modo Panorama, puede añadir tamaños de disco superiores a 2 TB y Panorama creará automáticamente tantas particiones de 2 TB como sea posible. Por ejemplo, si el disco sdc tenía 24 TB, creará 12 particiones de 2 TB. Estos discos se llamarán sdc1 a sdc12.

8. Seleccione el formato **Disk Provisioning (Aprovisionamiento de disco)** y haga clic en **Next (Siguiente)**.
9. **Specify a datastore or datastore structure (Especifique una estructura de almacén de datos o almacén de datos)**, seleccione **Browse (Examinar)** hasta un almacén de datos con suficiente espacio para el **Disk Size (Tamaño de disco)** especificado, haga clic en **OK (Aceptar)** y haga clic **Next (Siguiente)**.
10. Seleccione un **Virtual Device Node (Nodo de dispositivo virtual)** en formato de Interfaz de sistemas de ordenador pequeño (Small Computer Systems Interface, SCSI) (puede usar la selección predeterminada) y haga clic en **Next (Siguiente)**.

    El nodo seleccionado debe estar en formato SCSI; Panorama no se iniciará si selecciona otro formato.

11. Verifique que la configuración sea correcta y luego haga clic en **Finish (Terminar)** y **OK (Aceptar)**.

    El nuevo disco aparece en la lista de dispositivos del dispositivo virtual.
12. Repita los pasos 4 a 11 para añadir discos adicionales al dispositivo virtual Panorama si es necesario.
13. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**. El disco virtual se inicializa para su primer uso. El tamaño del disco nuevo determina cuánto tiempo llevará la inicialización.

STEP 2 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   ```
   show system disk details
   ```

   El usuario verá la siguiente respuesta:

   ```
   Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador habilitado Nombre: sdc
   ```

 ©2023 Palo Alto Networks, Inc.

```
Estado : Tamaño actual: 2048000 MB Estado: Motivo disponible:
Administrador deshabilitado
```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   > *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe al paso 3 cuando todas las respuestas de discos añadidos recientemente muestran `Reason : Admin enabled`.

STEP 3 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
3. Seleccione **Disks (Discos)** y haga clic en Add (Añadir) para incorporar los discos recién añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   > *Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.*

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 4 | Configure Panorama para recibir los logs.

Este paso está destinado a las nuevas implementaciones de Panorama en modo Panorama. Si está añadiendo discos de registro de logs a un dispositivo virtual Panorama existente, continúe al paso 5.

1. Configure un recopilador gestionado.
2. Configure un grupo de recopiladores.
3. Configure el reenvío de logs a Panorama.

STEP 5 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama.
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

 ©2023 Palo Alto Networks, Inc.

Cómo añadir un disco virtual a Panorama en vCloud Air

Puede añadir discos virtuales de logging para expandir la capacidad de almacenamiento de logs en el dispositivo virtual Panorama™. Si el dispositivo está en modo Panorama, puede añadir de 1 a 12 discos virtuales de creación de logs de 2 TB cada uno o un disco de creación de logs de 24 TB, para un total máximo de 24 TB. Si el dispositivo está en modo Legacy, puede añadir un disco de logging virtual de hasta 8 TB.

Si Panorama pierde conectividad con el nuevo disco virtual, es posible que Panorama pierda los logs durante el intervalo de fallo.

Si es necesario, puede sustituir el disco virtual en vCloud Air.

STEP 1 | Añada discos adicionales a Panorama.

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de logging es inferior a 2 TB, no podrá añadir espacio adicional en el disco.

1. Acceda a la consola web de vCloud Air y seleccione su región de **Virtual Private Cloud On Demand (Nube privada virtual a petición)**.
2. Seleccione el dispositivo virtual Panorama en la pestaña **Virtual Machines (Máquinas virtuales)**.
3. **Añada otro disco** (**Actions [Acciones]** > **Edit Resources [Editar recursos]**).
4. Seleccione el tamaño de **Storage (Almacenamiento)**. Si el dispositivo virtual Panorama está en modo Panorama, configure el tamaño en al menos 2 TB. Si el dispositivo está en modo heredado, puede establecer el tamaño en hasta 8 TB.

   En el modo Panorama, puede añadir tamaños de disco superiores a 2 TB y Panorama creará automáticamente tantas particiones de 2 TB como sea posible. Por ejemplo, si el disco sdc tenía 24 TB, Panorama creará 12 particiones de 2 TB. Estos discos se nombrarán sdc1 a sdc12.
5. Establezca el nivel de almacenamiento en **Standard (Estándar)** o **SSD-Accelerated (SSD-acelerado)**.
6. Repita los pasos anteriores para añadir discos adicionales al dispositivo virtual Panorama si es necesario.
7. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 2 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

```
Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
Motivo disponible: Administrador habilitado Nombre: sdc
```


©2023 Palo Alto Networks, Inc.

```
Estado : Tamaño actual: 2048000 MB Estado: Motivo disponible:
Administrador deshabilitado
```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   > *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 3 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada discos nuevos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   > *Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.*

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 4 | Configure Panorama para recibir los logs.

Este paso está destinado a las nuevas implementaciones de Panorama en modo Panorama. Si está añadiendo discos de logging a un dispositivo virtual Panorama existente, continúe con el siguiente paso.

1. Configure un recopilador gestionado.
2. Configure un grupo de recopiladores.
3. Configure el reenvío de logs a Panorama.

STEP 5 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama.
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestre la capacidad del disco nuevo con precisión.

 ©2023 Palo Alto Networks, Inc.

Cómo añadir un disco virtual a Panorama en Alibaba Cloud

Después de Instalación de Panorama en Alibaba Cloud, añada discos de creación de logs virtuales para ampliar la capacidad de almacenamiento de logs en el dispositivo virtual Panorama™ para logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. Para añadir discos virtuales, debe poder acceder a la consola de Alibaba Cloud, la interfaz de línea de comandos (CLI) de Panorama y la interfaz web de Panorama.

El dispositivo virtual Panorama en Alibaba Cloud admite solo discos de creación de logs de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Inicie sesión en Alibaba Cloud Console.

STEP 2 | Seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Instances (Instancias)** y navegue a la instancia del dispositivo virtual Panorama.

STEP 3 | Añada un disco virtual de logging a Panorama.

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. En la columna "Actions" (Acciones), seleccione **Manage (Administrar)**.
2. Seleccione **Cloud Disk (Disco en la nube)** y **Create Disk (Crear disco)**.
3. Configure el disco virtual de creación de logs.
   - **Attach (Adjuntar)**: seleccione **Attach to ECS Instance (Adjuntar a instancia de ECS)**.
   - **ECS Instance (Instancia de ECS)**: seleccione la región y la instancia del dispositivo virtual de Panorama.
   - **Storage (Almacenamiento)**: seleccione el tipo de disco virtual e ingrese la capacidad del disco.
   - (Opcional) **Quantity (Cantidad)**: especifique cuántos discos virtuales se crearán. De forma predeterminada, se crea **1** disco virtual. Cuando se crean varios discos de registro, asegúrese de que la suma de todos los discos virtuales no supere los 24 TB.
   - **Terms of Service (Condiciones del servicio)**: revise las condiciones del servicio de Alibaba Cloud y marque la casilla después de revisarlas.
4. Seleccione **Preview (Vista previa)** para obtener una vista previa de la creación del disco virtual.
5. Seleccione **Create (Crear)** para crear el nuevo disco virtual.

   Aparece una ventana de estado después de crear el nuevo disco virtual. Después de que el disco virtual se haya creado correctamente, **vaya a la Lista de discos** para confirmar que el disco se creó correctamente.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

   ```
   Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador deshabilitado
   ```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en la CLI de Panorama *y continúe con el siguiente paso para verificar que se agregó el disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 5 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 6 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de logging a un dispositivo virtual Panorama existente, omita el paso 6.

1. Configuración de un grupo de recopiladores.
2. Configuración del reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Cómo añadir un disco virtual a Panorama en AWS

Después de instalar Panorama en AWS o Instalación de Panorama en AWS GovCloud, añada discos de creación de logs virtuales a la instancia del dispositivo virtual Panorama™ para proporcionar almacenamiento a los logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. Para añadir discos virtuales, debe poder acceder a la consola de Amazon Web Service, la interfaz de línea de comandos (CLI) de Panorama y la interfaz web de Panorama.

El dispositivo virtual Panorama en AWS admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Inicie sesión en la consola de Amazon Web Service (AWS) y seleccione el panel EC2.

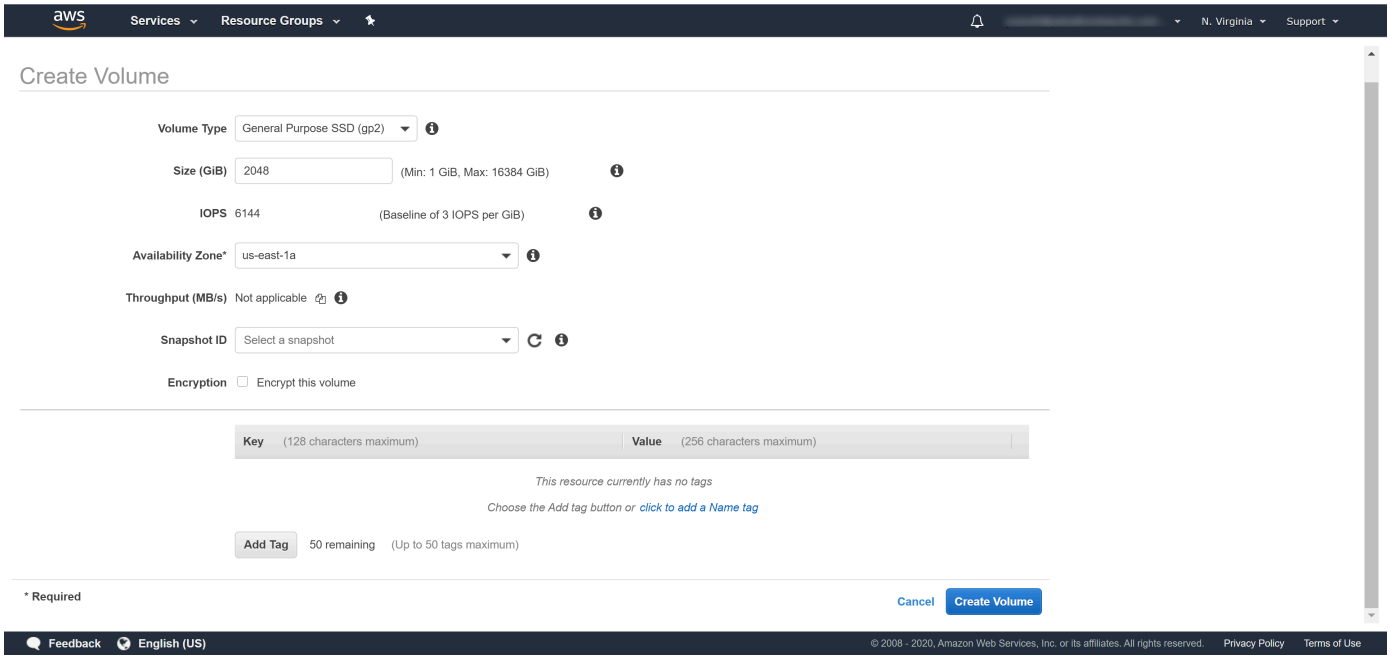
- Consola de Amazon Web Services
- Consola de AWS GovCloud Web Service

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada un disco virtual de logging a Panorama.

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. En el panel EC2, seleccione **Volumes (Volúmenes)** y haga clic en **Create Volume (Crear volumen)**:
   - Seleccione el Tipo de volumen preferido. Para la utilización general, seleccione **SSD de uso general (GP2)**.
   - Configure el **tamaño** del volumen como 2048 GiB.
   - Seleccione la misma Zona de disponibilidad en la que se encuentra ubicado su dispositivo virtual Panorama.
   - (Opcional) Cifre el volumen.
   - (Opcional) Añada etiquetas a tu volumen.
2. Haga clic en **Create Volume (Crear volumen)**.



3. En la página Volumes (Volúmenes), seleccione el volumen que desee y seleccione **Actions (Acciones)** > **Attach Volume (Adjuntar volumen)**.
4. Adjunte la instancia del dispositivo virtual Panorama.
   1. Seleccione su **instancia** de Panorama.
   2. Especifique el **nombre del dispositivo** para el volumen de disco de creación de logs que ha creado.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

   ```
   Nombre : nvme1n1 Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador habilitado Nombre : nvme2n1
   Estado : Tamaño actual: 2048000 MB Estado: Motivo disponible:
   Administrador deshabilitado
   ```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add nvme2n1`

   *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 4 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 5 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de logging a un dispositivo virtual Panorama existente, omita el paso 6.

1. Configure un grupo de recopiladores.
2. Configure el reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Cómo añadir un disco virtual a Panorama en Azure

Después de la Instalación de Panorama en Azure, añada discos virtuales de logging a la instancia del dispositivo virtual Panorama™ para proporcionar almacenamiento a los logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. Para añadir discos virtuales, debe poder acceder al portal de Microsoft Azure, la interfaz de línea de comandos (CLI) de Panorama y la interfaz web de Panorama.

El dispositivo virtual Panorama en Azure admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

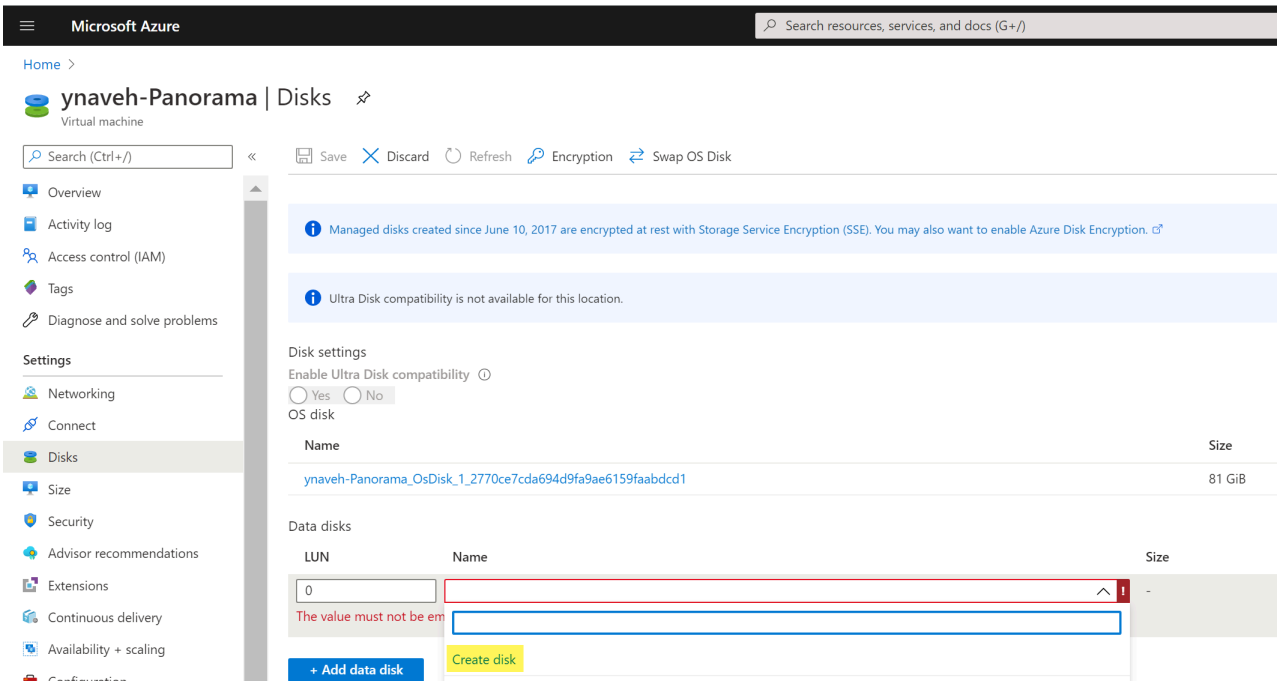
STEP 1 | Inicie sesión en el portal de Microsoft Azure.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada un disco virtual de logging a Panorama.

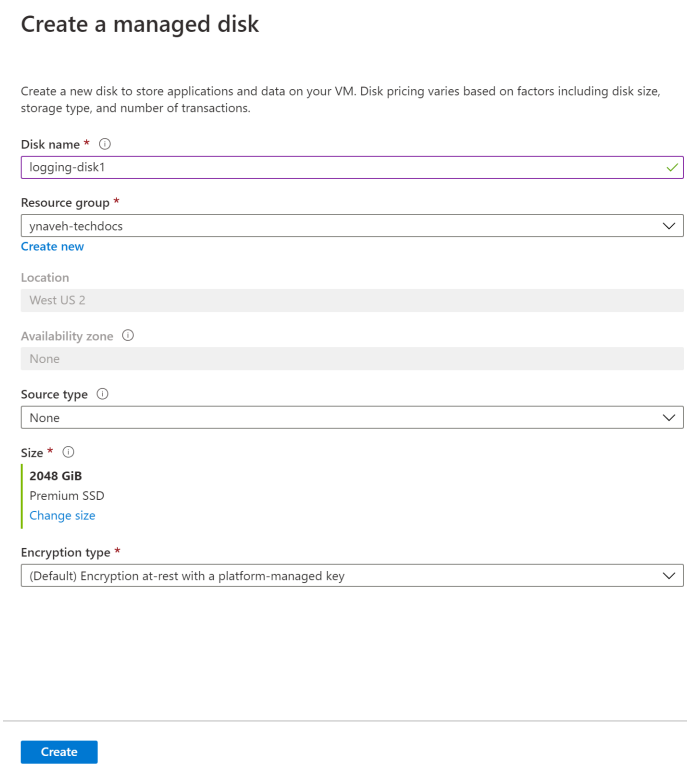
En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. En el panel de Azure, seleccione las **máquinas virtuales** Panorama a las que desea añadir un disco de logging.
2. Seleccione **Disks (Discos)**.
3. Haga clic en **+Add data disk (Añadir disco de datos)**.
4. En el menú desplegable del disco nuevo, haga clic en **Create disk (Crear disco)**.



5. Configure el disco de logging.
   1. Introduzca el **Name (Nombre)** del disco.
   2. Seleccione el grupo de recursos. Si hace clic en **Create new (Crear nuevo)** para crear nuevos grupos de recursos, introduzca el nombre del grupo.
   3. Verifique el **Account type (Tipo de cuenta)** (este campo se completa automáticamente).
   4. En el menú desplegable **Source type (Tipo de origen)**, seleccione **None (Ninguno)**.
   5. Seleccione **Change Size (Cambiar tamaño)** y seleccione un disco de creación de registros de 2048 GiB.
   6. **Cree** el nuevo disco de creación de registros.

 ©2023 Palo Alto Networks, Inc.



7. Para el **almacenamiento en caché de host**, seleccione **Read/write (Leer/escribir)**.



STEP 3 | Habilite cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

```
Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
Motivo disponible: Administrador habilitado Nombre: sdc
```

 ©2023 Palo Alto Networks, Inc.

```
Estado : Tamaño actual: 2048000 MB Estado: Motivo disponible:
Administrador deshabilitado
```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   > *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 4 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   > *Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.*

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 5 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de logging a un dispositivo virtual Panorama existente, omita el paso 6.

1. Configure un grupo de recopiladores.
2. Configure el reenvío de logs a Panorama.

STEP 6 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Cómo añadir un disco virtual a Panorama en Google Cloud Platform

Después de la Instalación de Panorama en Google Cloud Platform, añada discos virtuales de logging a la instancia del dispositivo virtual Panorama™ para proporcionar almacenamiento a los logs

 ©2023 Palo Alto Networks, Inc.

generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. El dispositivo virtual Panorama en Google Cloud Platform admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Inicie sesión en la consola de Google Cloud.

STEP 2 | Añada el disco virtual de logging.



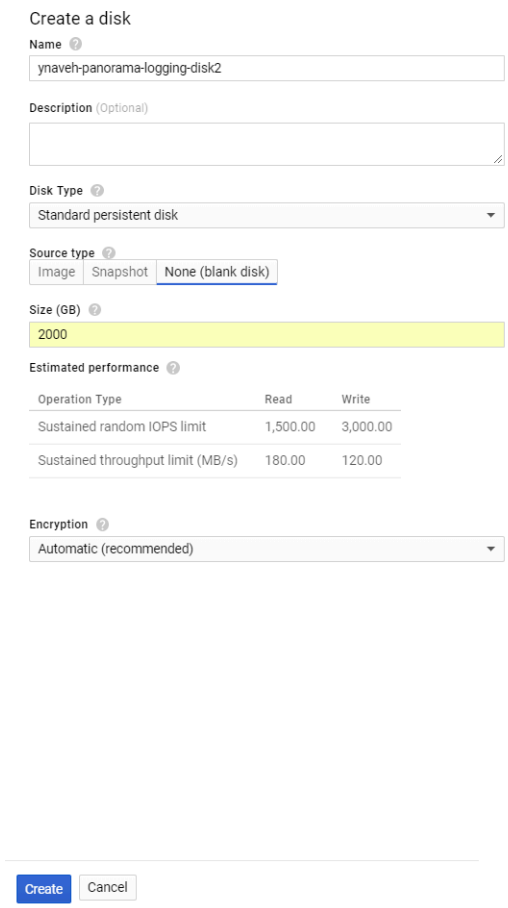
En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. En el menú Products & Services (Productos y servicios), seleccione y haga clic en **Edit (Editar)** para editar la instancia del dispositivo virtual de Panorama (**Compute Engine** > **VM Instances [Instancias de VM]**).
2. En la sección Additional Disks (Discos adicionales), haga clic en **Add Item (Añadir elementos)**.
3. Haga clic en **Create disk (Crear disco)** (en el menú desplegable **Name [Nombre]**).

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure los discos virtuales de logging.

1. Introduzca el **Name (Nombre)**.
2. Expanda el menú desplegable **Disk Type (Tipo de disco)** y seleccione el tipo deseado.
3. En **Source type (Tipo de origen)**, seleccione **None (Ninguno) (disco en blanco)**.
4. Configure el **Size (Tamaño) (GB)** del disco virtual de logging.
5. Haga clic en **Create (Crear)**.



6. Haga clic en **Save (Guardar)** para guardar los cambios y actualizar la instancia del dispositivo virtual Panorama.

STEP 4 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   ```
   show system disk details
   ```

   El usuario verá la siguiente respuesta:

   ```
   Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador habilitado Nombre: sdc
   ```

 ©2023 Palo Alto Networks, Inc.

```
Estado : Tamaño actual: 2048000 MB Estado: Motivo disponible:
Administrador deshabilitado
```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   > *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 5 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   > *Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.*

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 6 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de registro de logs a un dispositivo virtual Panorama existente, omita el paso 7.

1. Configure un grupo de recopiladores.
2. Configure el reenvío de logs a Panorama.

STEP 7 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

 ©2023 Palo Alto Networks, Inc.

Cómo añadir un disco virtual a Panorama en KVM

Después de la Instalación de Panorama en KVM, añada discos virtuales de logging a la instancia del dispositivo virtual Panorama™ para proporcionar almacenamiento a los logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. El dispositivo virtual Panorama en KVM admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Haga clic en **Shutdown (Apagar)** para apagar la instancia del dispositivo virtual Panorama en el gestor de máquinas virtuales.

STEP 2 | Haga doble clic en la instancia del dispositivo virtual Panorama en el gestor de máquinas virtuales y seleccione **Show virtual hardware details (Mostrar detalles de hardware virtual)** .

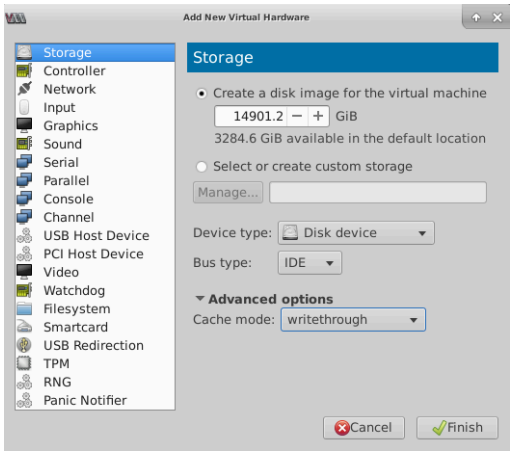
 ©2023 Palo Alto Networks, Inc.

STEP 3 | Añada el disco virtual de logging. Repita este paso las veces que fuera necesario.

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. **Cree una imagen de disco para una imagen virtual** (**Add Hardware [Añadir hardware]** > **Storage [Almacenamiento]**) y configure la capacidad de almacenamiento del disco virtual al valor adecuado de 2 TB: 2.000 GB o 14.901,2 GiB según el gestor de máquina virtual.

   Según la versión, algunos gestores de máquinas virtuales utilizan GiB (gibibyte) para asignar memoria. Asegúrese de convertir correctamente la capacidad de almacenamiento necesaria para evitar la subestimación de recursos en el disco virtual de logging y el envío del dispositivo virtual Panorama en modo de mantenimiento.
2. En el menú desplegable **Device type (Tipo de dispositivo)**, seleccione **Disk device (Dispositivo de disco)**.
3. En el menú desplegable **Bus type (Tipo de bus)**, seleccione **VirtIO** o **IDE** según su configuración.
4. Expanda las **Advanced options (Opciones avanzadas)** y en el menú desplegable **Cache mode (Modo de caché)**, seleccione **writethrough**.
5. Haga clic en **Finish (Finalizar)**.



STEP 4 | Haga clic en **Power on (Encender)** para encender la instancia del dispositivo virtual Panorama.

©2023 Palo Alto Networks, Inc.

STEP 5 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

   ```
   Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador habilitado Nombre: sdc
   Estado : Tamaño actual: 2048 MB Estado : Motivo disponible:
   Administrador deshabilitado
   ```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:

   `request system disk add sdc`

   *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 6 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 7 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de registro de logs a un dispositivo virtual Panorama existente, omita el paso 8.

1. Configure un grupo de recopiladores.
2. Configure el reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Cómo añadir un disco virtual a Panorama en Hyper-V.

Después de la Instalación de Panorama en Hyper-V, añada discos de creación de logs virtuales a la instancia del dispositivo virtual Panorama™ para proporcionar almacenamiento a los logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. El dispositivo virtual Panorama en Hyper-V admite solo discos de logging de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Desactive el dispositivo virtual de Panorama.

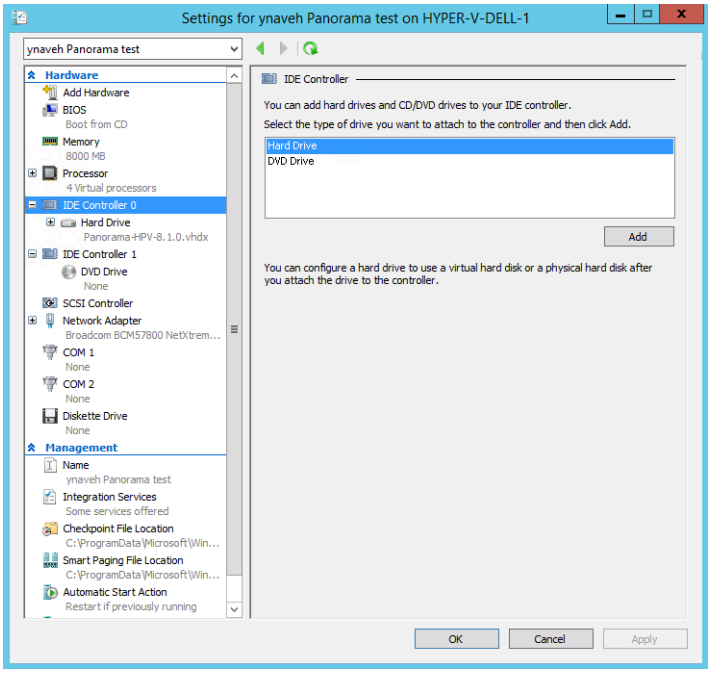
1. En el gestor de Hyper-V, seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Action (Acción)** > **Turn Off (Apagar)** para apagar el dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada el disco virtual de logging. Repita este paso las veces que fuera necesario.

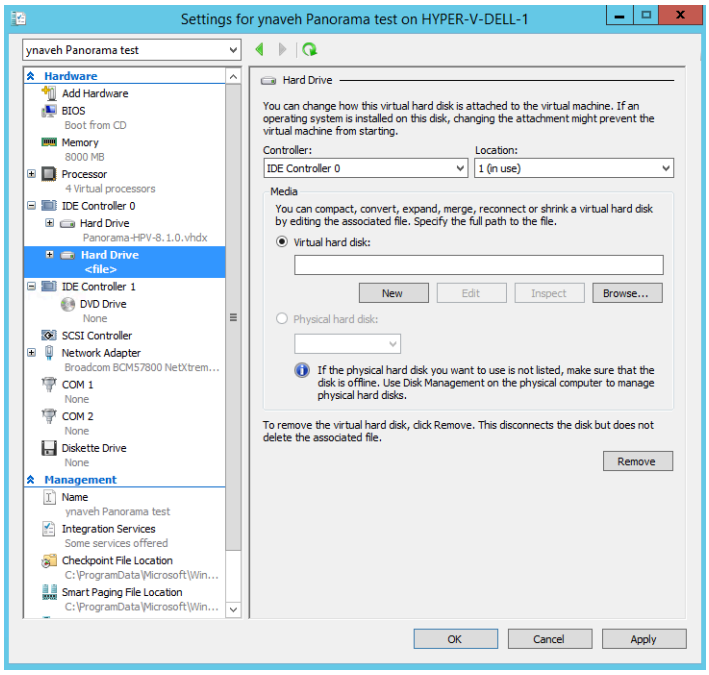
En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. Seleccione el dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)** y seleccione **Action (Acción)** > **Settings (Ajustes)**.
2. En la lista **Hardware**, seleccione **IDE Controller 0 (Controlador IDE 0)**.
3. En la lista de unidades del **IDE Controller (Controlador IDE)**, seleccione **Hard Drive (Disco duro)** y haga clic en **Add (Añadir)** para añadir el nuevo disco virtual de registro de logs.



4. Seleccione el nuevo **Hard Drive (Disco duro)** creado en **IDE Controller 0 (Controlador IDE 0)**.
5. En **Media (Medio)**, añada un disco duro **New (Nuevo)**.

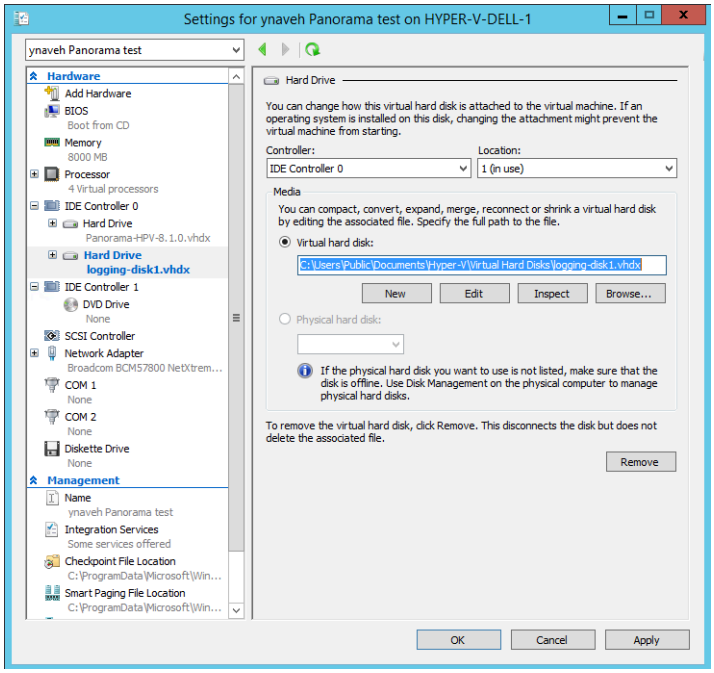
 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure los nuevos discos virtuales de registro de logs.

1. Si ve la solicitud Before You Begin (Antes de comenzar), haga clic en **Next (Siguiente)** para comenzar a añadir el disco virtual de registro de logs
2. En Disk Format (Formato de disco), seleccione **VHDX**. Haga clic en **Next (Siguiente)** para continuar.
3. En Disk Type (Tipo de disco), seleccione **Fixed Size (Tamaño fijo)** o **Dynamically Expanding (Expansión dinámica)** según sus necesidades. Haga clic en **Next (Siguiente)** para continuar.
4. Especifique el **Name (Nombre)** y la **Location (Ubicación)** del archivo del disco virtual de registro de logs. Haga clic en **Next (Siguiente)** para continuar.
5. Para configurar el disco, seleccione **Create a new virtual hard disk (Crear un nuevo disco virtual)** e introduzca el tamaño del disco. Haga clic en **Next (Siguiente)** para continuar.
6. Revise el resumen y haga clic en **Finish (Finalizar)** para completar la adición del disco duro virtual de registro de logs.
7. Haga clic en **Apply (Aplicar)** para aplicar la nueva adición de disco duro.



STEP 4 | Active el dispositivo virtual Panorama.

1. Seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Action (Acción)** > **Start (Iniciar)** para encender la instancia del dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:

   `show system disk details`

   El usuario verá la siguiente respuesta:

   ```
   Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
   Motivo disponible: Administrador habilitado Nombre: sdc
   Estado : Tamaño actual: 2048 MB Estado : Motivo disponible:
   Administrador deshabilitado
   ```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Respuesta a Admindisabled`:

   `request system disk add sdc`

   *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. En modo Panorama,* inicie sesión en el CLI de Panorama *y continúe al* paso 4 *para verificar la adición del disco.*

4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

STEP 6 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.

6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 7 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de registro de logs a un dispositivo virtual Panorama existente, omita el paso 8.

1. Configure un grupo de recopiladores.
2. Configure el reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Cómo añadir un disco virtual a Panorama en Oracle Cloud Infrastructure (OCI)

Después de Instalación de Panorama en Oracle Cloud Infrastructure (OCI), añada discos de creación de logs virtuales para ampliar la capacidad de almacenamiento de logs en el dispositivo virtual Panorama™ para logs generados por cortafuegos gestionados. Puede añadir discos virtuales a un recopilador de logs local para un dispositivo virtual Panorama en modo Panorama o para un recopilador de logs dedicado. Para añadir discos virtuales, debe poder acceder a la consola de OCI, la interfaz de línea de comandos (CLI) de Panorama y la interfaz web de Panorama.

El dispositivo virtual Panorama en OCI admite solo discos de creación de logs de 2 TB y, en total, admite hasta 24 TB de almacenamiento de logs. No puede añadir un disco de logging menor a 2 TB o un disco de logging de un tamaño que no sea divisible por 2 TB debido a que el dispositivo virtual Panorama divide los discos de logging en particiones de 2 TB. Por ejemplo, si adjunta un disco de logging de 4 TB, Panorama creará dos particiones de 2 TB. Sin embargo, no puede añadir un disco de logging de 5 TB debido a que el 1 TB restante no se admitirá como partición.

STEP 1 | Inicie sesión en la consola de Oracle Cloud Infrastructure.

STEP 2 | Cree un volumen de bloque de 2 TB.

1. Seleccione **Block Storage (Almacenamiento de bloque)** > **Block Volumes (Volúmenes de bloques)** y **Create Block Volume (Crear volumen de bloque)**.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para el volumen.
3. Seleccione el mismo **Availability Domain (Dominio de disponibilidad)** que la instancia del dispositivo virtual Panorama.
4. Seleccione el tamaño de volumen personalizado en **Custom (Personalizar)**.
5. En “Volumen Size” (Tamaño de volumen), ingrese **`2000`**.
6. Haga clic en **Create Block Volume (Crear volumen de bloque)**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Adjunte un disco virtual de creación de logs a la instancia del dispositivo virtual Panorama.

En todos los modos, el primer disco de logging en la VM de Panorama debe tener al menos 2 TB para añadir discos adicionales. Si el primer disco de log es más pequeño que 2 TB, no podrá añadir espacio adicional en el disco.

1. Seleccione **Compute (Procesar)** > **Instances (Instancias)** y haga clic en el nombre de la instancia del dispositivo virtual Panorama.
2. En "Resources" (Recursos), seleccione **Attached Block Volumes (Volúmenes de bloques adjuntos)** y **Attach Block Volume (Adjuntar volumen de bloque)**.
3. En Volumen, **seleccione Volumen** y seleccione el disco virtual de creación de logs.
4. Para el tipo de adjunto, seleccione **Paravirtualized (Paravirtualizado)**.
   Esto es necesario para que el dispositivo virtual Panorama reconozca el disco de creación de logs virtual.
5. En Access (Acceso), seleccione **Read/Write (Lectura/Escritura)**.
6. Seleccione **Attach (Adjuntar)** para adjuntar el disco virtual de registro.

STEP 4 | Configure cada disco.

El siguiente ejemplo usa el disco virtual sdc.

1. Inicio de sesión en la CLI de Panorama.
2. Introduzca el siguiente comando para ver los discos en el dispositivo virtual Panorama:
   `show system disk details`
   El usuario verá la siguiente respuesta:

```
 Nombre : sdb Estado : Tamaño actual: 2048000 MB Estado:
Motivo no disponible: Administrador deshabilitado
```

3. Introduzca el siguiente comando y confirme la solicitud cuando se solicite para todos los discos con el `Reason : Admin disabled` respuesta:
   `request system disk add sdc`

   *El comando **`request system disk add`** no está disponible en un servidor de gestión de Panorama en modo solo de gestión debido a que no se admite el registro de logs en este modo. Si no ve el comando,* Configuración de un dispositivo virtual Panorama en modo Panorama *para habilitar los discos de creación de logs. Una vez en modo Panorama,* Inicio de sesión en la CLI de Panorama *y continúe con el siguiente paso para verificar que se añadió el disco.*
4. Introduzca el comando **`show system disk details`** para verificar el estado de la adición del disco. Continúe con el siguiente paso cuando las respuestas de los nuevos discos añadidos muestren `Reason : Admin enabled`.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Haga que los discos estén disponibles para la creación de logs.

1. Inicie sesión en la interfaz web de Panorama.
2. Edite un recopilador de logs (**Panorama** > **Managed Collectors [Recopiladores gestionados]**).
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir nuevos discos añadidos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

   Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, espere a que se complete la sincronización de HA antes de continuar.
6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe los cambios al grupo de recopiladores al que pertenece el recopilador de logs.

STEP 6 | (Nuevas implementaciones de Panorama solo en modo de Panorama) Configure Panorama para recibir logs.

Si está añadiendo discos de logging a un dispositivo virtual Panorama existente, omita el paso 6.

1. Configuración de un grupo de recopiladores.
2. Configuración del reenvío de logs a Panorama.

STEP 7 | Verifique que se haya aumentado la capacidad de almacenamiento de logs de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione el grupo de recopiladores al que pertenece el dispositivo virtual Panorama (**Panorama** > **Collector Groups [Grupos de recopiladores]**).
3. Verifique que la capacidad de **Log Storage (Almacenamiento de logs)** muestra con precisión la capacidad del disco.

Montaje de servidor ESXi de Panorama en un almacén de datos NFS

Cuando el dispositivo virtual Panorama en modo heredado se ejecuta en un servidor ESXi, el montaje en un almacén de datos del Sistema de archivos de red (Network File System, NFS) permite el logging a una ubicación centralizada y la ampliación de la capacidad de almacenamiento de logs más allá de lo que admite un disco virtual. (ESXi 5.5 o una versión posterior puede admitir un disco virtual de hasta 8 TB. Las versiones anteriores de ESXi admiten un disco virtual de hasta 2 TB). Antes de configurar un almacenamiento de datos de NFS en una configuración de alta disponibilidad (HA) de Panorama, consulte Consideraciones sobre logs en HA de Panorama.

El dispositivo virtual Panorama en modo Panorama no es compatible con NFS.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y en la sección Varios, haga clic en **Storage Partition Setup (Configuración de partición de almacenamiento)**.

STEP 2 | Configure el tipo de **Storage Partition (Partición de almacenamiento)** en **NFS V3**.

STEP 3 | Introduzca la dirección IP del **Server (Servidor)** NFS.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Introduzca la ruta de **Log Directory (Directorio de logs)** para almacenar los archivos de logs. Por ejemplo, export/panorama.

STEP 5 | En **Protocol (Protocolo)**, seleccione **TCP** o **UDP**, e introduzca **Port (Puerto)** para acceder al servidor NFS.

Para utilizar NFS en TCP, el servidor NFS debe ser compatible. Los puertos NFS más frecuentes son UDP/TCP 111 para RPC y UDP/TCP 2049 para NFS.

STEP 6 | Para un rendimiento óptimo de NFS, en los campos **Read Size (Tamaño de lectura)** y **Write Size (Tamaño de escritura)**, especifique el tamaño máximo de los grupos de datos que el cliente y el servidor se transfieren de uno a otro. La definición del tamaño de lectura/escritura optimiza el volumen y la velocidad de transferencia de los datos entre Panorama y el almacén de datos de NFS.

STEP 7 | (Opcional) Seleccione **Copy On Setup (Copiar en configuración)** para copiar los logs existentes almacenados en Panorama en el volumen NFS. Si Panorama dispone de muchos logs, esta opción podría iniciar la transferencia de un gran volumen de datos.

STEP 8 | Haga clic en **Test Logging Partition (Probar partición de registro de logs)** para verificar que Panorama pueda acceder al **Server (Servidor)** y **Log Directory (Directorio de logs)** de NFS.

STEP 9 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 10 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios Hasta que reinicie, el dispositivo virtual Panorama escribirá los logs en el disco de almacenamiento local.

STEP 11 | Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y luego **Reboot Panorama (Reiniciar Panorama)** en la sección Operaciones de dispositivo. Después de reiniciar, Panorama iniciará la escritura de logs en el almacén de datos de NFS.

Aumento de CPU y memoria en el dispositivo virtual Panorama

Cuando lleve a cabo la Realización de la configuración inicial del dispositivo virtual Panorama, especifique la memoria y el número de CPU en función de si el dispositivo está en modo Panorama o solo de gestión, y según la capacidad de almacenamiento de logs o el número de cortafuegos gestionados. Si luego añade capacidad de almacenamiento o cortafuegos gestionados, también deberá aumentar la memoria y las CPU. Un dispositivo virtual Panorama en modo de recopilador de logs debe cumplir con los requisitos del sistema y no es necesario que los requisitos de CPU y memoria sean superiores a los valores mínimos. Consulte Requisitos previos de configuración del dispositivo virtual Panorama para ver los requisitos de CPU y memoria de cada modo Panorama.

- Aumento de CPU y memoria para Panorama en un servidor ESXi
- Aumento de CPU y memoria para Panorama en vCloud Air
- Aumento de CPU y memoria para Panorama en Alibaba Cloud
- Aumento de CPU y memoria para Panorama en AWS
- Aumento de CPU y memoria para Panorama en Azure
- Aumento de CPU y memoria para Panorama en Google Cloud Platform

 ©2023 Palo Alto Networks, Inc.

- Aumento de CPU y memoria para Panorama en KVM
- Aumento de CPU y memoria para Panorama en Hyper-V
- Aumento de las CPU y la memoria para Panorama en Oracle Cloud Infrastructure (OCI)

Aumento de CPU y memoria para Panorama en un servidor ESXi

Para ver los requisitos mínimos de las CPU y la memoria que requiere Panorama, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

STEP 1 | Acceda al cliente VMware vSphere y seleccione **Virtual Machines (Máquinas virtuales)**.

STEP 2 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.

STEP 3 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar ajustes)**.

STEP 4 | Seleccione **Memory (Memoria)** e introduzca el nuevo **Memory Size (Tamaño de la memoria)**.

STEP 5 | Seleccione **CPUs (CPU)** y especifique el número de CPU (el valor en **Number of virtual sockets [Número de conectores virtuales]** multiplicado por el valor en **Number of cores per socket [Número de núcleos por conector]**).

STEP 6 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 7 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**.

Aumento de CPU y memoria para Panorama en vCloud Air

Para ver los requisitos mínimos de CPU y memoria que requiere Panorama, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

STEP 1 | Acceda a la consola web de vCloud Air y seleccione su región de **Virtual Private Cloud OnDemand (Nube privada virtual a petición)**.

STEP 2 | En la pestaña **Virtual Machines (Máquinas virtuales)**, seleccione la máquina virtual Panorama y **Power Off (Apagar)**.

STEP 3 | Seleccione **Actions (Acciones)** > **Edit Resources (Editar recursos)**.

STEP 4 | Seleccione el **CPU** y la **Memory (Memoria)**.

STEP 5 | Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 6 | Seleccione la máquina virtual Panorama y **Power On (Encender)**.

Aumento de CPU y memoria para Panorama en Alibaba Cloud

Puede cambiar el tipo de instancia del dispositivo virtual Panorama™ para aumentar las CPU y la memoria asignadas a la instancia del dispositivo virtual Panorama. Asegúrese de revisar los tipos de instancia de Alibaba Cloud admitidos y Requisitos previos de configuración del dispositivo virtual Panorama antes de cambiar el tipo de instancia.

STEP 1 | Inicie sesión en Alibaba Cloud Console.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Instances (Instancias)** y navegue a la instancia del dispositivo virtual Panorama.

STEP 3 | En la columna "Actions" (Acciones), seleccione **More (Más)** > **Instance Status (Estado de instancia)** > **Stop (Detener).**

STEP 4 | Cambie el tipo de instancia del dispositivo virtual Panorama.

1. Seleccione el dispositivo virtual Panorama si aún no está seleccionado.
2. En la columna "Actions" (Acciones), seleccione **Change Instance Type (Cambiar tipo de instancia)**.
3. Seleccione el tipo de instancia deseado y **Change (Cambiar)** para cambiarlo.
4. Cuando se le solicite, seleccione **Console (Consola)** para ver la instancia del dispositivo virtual Panorama.

STEP 5 | En la columna "Actions" (Acciones) de la instancia del dispositivo virtual Panorama, seleccione **More (Más)** > **Instance Status (Estado de instancia)** > **Start (Iniciar).**

STEP 6 | Verifique el aumento de la CPU y la memoria.

1. Inicio de sesión en la CLI de Panorama.
2. Consulte la información del sistema del dispositivo virtual Panorama.

```
admin> show system info
```

3. Compruebe que `num-cpus` y `ram-in-gb` muestran el número correcto de CPU y la cantidad de memoria según el tipo de instancia seleccionado.

Aumento de CPU y memoria para Panorama en AWS

Para obtener información sobre los requisitos mínimos de CPU y memoria de Panorama™, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

Un dispositivo virtual Panorama en modo de recopilador de logs no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto puede provocar una pérdida de datos de logs.

STEP 1 | Inicie sesión en la consola de Amazon Web Service (AWS) y seleccione el panel EC2.

- Consola de Amazon Web Services
- Consola de AWS GovCloud Web Service

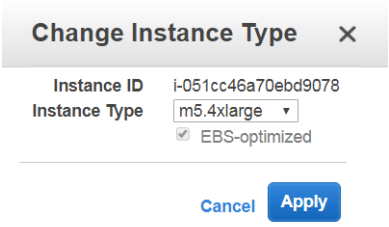
STEP 2 | En el panel EC2, seleccione **Instances (Instancias)** y seleccione la instancia del dispositivo virtual Panorama.

STEP 3 | Seleccione **Actions (Acciones)** > **Instance State (Estado de la instancia)** > **Stop (Detener)** para apagar la instancia del dispositivo virtual Panorama.

STEP 4 | Seleccione **Actions (Acciones)** > **Instance Settings (Configuración de la instancia)** > **Change Instance Type (Cambiar tipo de instancia)** para cambiar el tipo de instancia del dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Seleccione el **Instance Type (Tipo de instancia)** que desea actualizar y haga clic en **Apply (Aplicar)** para aplicarla.



STEP 6 | Seleccione **Actions (Acciones)** > **Instance State (Estado de la instancia)** > **Start (Iniciar)** para encender la instancia del dispositivo virtual Panorama.

Aumento de CPU y memoria para Panorama en Azure

Para obtener información sobre los requisitos mínimos de CPU y memoria de Panorama™, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

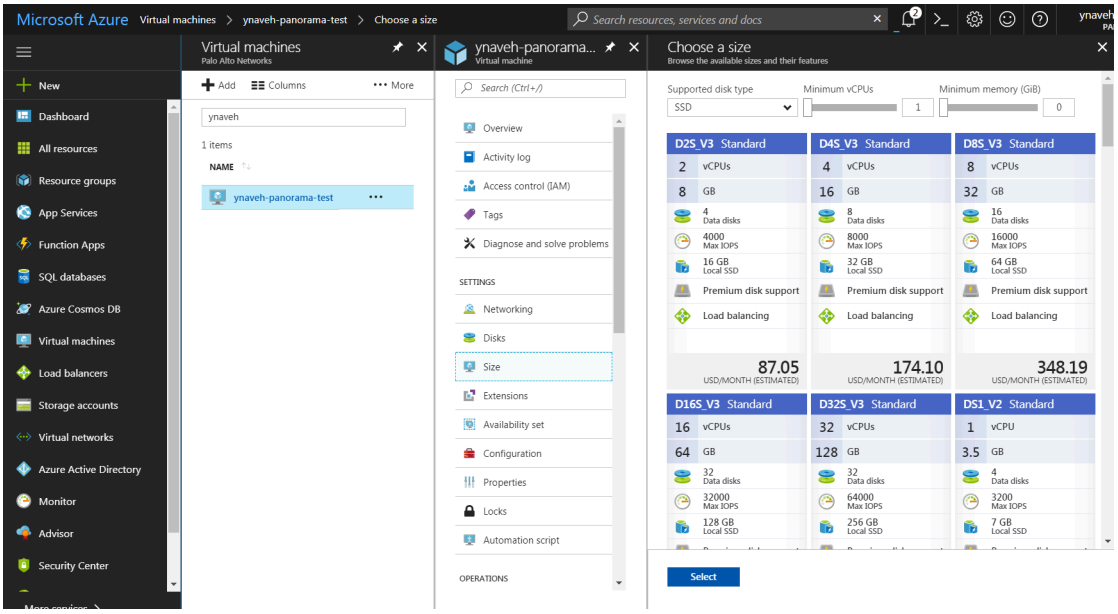
Un dispositivo virtual Panorama en modo de recopilador de logs no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto puede provocar una pérdida de datos de logs.

STEP 1 | Inicie sesión en el portal de Microsoft Azure.

STEP 2 | En el panel de Azure, seleccione **Virtual machines (Máquinas virtuales)** y seleccione el dispositivo virtual Panorama.

STEP 3 | Seleccione **Overview (Descripción general)** y haga clic en **Stop (Detener)** para apagar el dispositivo virtual Panorama.

STEP 4 | Seleccione el **Size (Tamaño)** de la nueva máquina virtual y haga clic en **Select (Seleccionar)** para seleccionarla.



 ©2023 Palo Alto Networks, Inc.

STEP 5 | Seleccione **Overview (Descripción general)** y haga clic en **Start (Iniciar)** para encender el dispositivo virtual Panorama.

Aumento de CPU y memoria para Panorama en Google Cloud Platform

Para obtener información sobre los requisitos mínimos de CPU y memoria de Panorama™, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

Un dispositivo virtual Panorama en modo de recopilador de logs no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto puede provocar una pérdida de datos de logs.

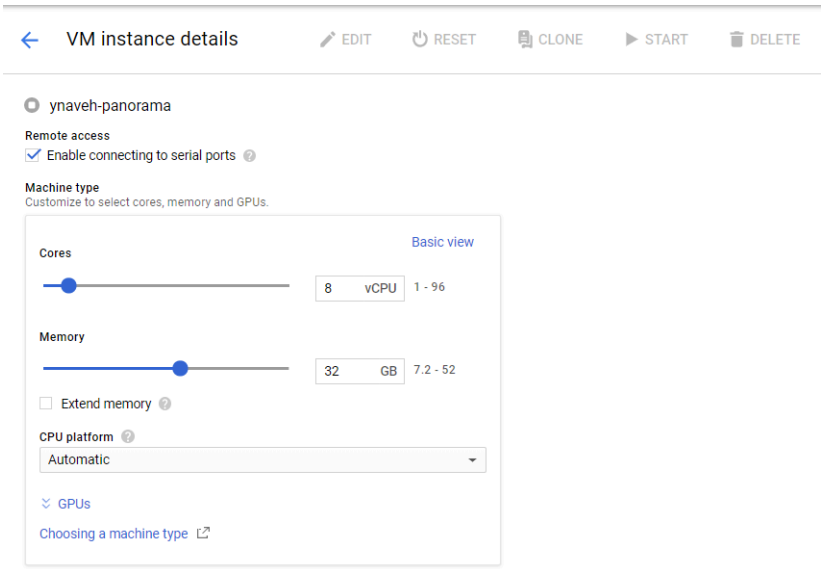
STEP 1 | Inicie sesión en la consola de Google Cloud.

STEP 2 | Detenga la instancia del dispositivo virtual Panorama.

1. Seleccione la instancia del dispositivo virtual Panorama en el menú Products & Services (Productos y servicios) (**Compute Engine** > **VM Instances [Instancias de VM]**).
2. **Detenga** la instancia del dispositivo virtual Panorama. Es posible que el dispositivo virtual Panorama demore de 2 a 3 minutos para apagarse completamente.

STEP 3 | Vuelva a configurar los recursos del dispositivo virtual Panorama.

1. Haga clic en **Edit (Editar)** para editar los detalles de la instancia del dispositivo virtual Panorama.
2. En Machine Type (Tipo de máquina), haga clic en **Customize (Personalizar)** para personalizar los núcleos y la memoria de la CPU del dispositivo virtual.



STEP 4 | Haga clic en **Save (Guardar)** para guardar los cambios y actualizar la instancia del dispositivo virtual Panorama.

STEP 5 | Haga clic en **Start (Iniciar)** para encender el dispositivo virtual Panorama.

©2023 Palo Alto Networks, Inc.

Aumento de CPU y memoria para Panorama en KVM

Para obtener información sobre los requisitos mínimos de CPU y memoria de Panorama™, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

Un dispositivo virtual Panorama en modo de recopilador de logs no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto puede provocar una pérdida de datos de logs.

STEP 1 | Haga clic en **Shutdown (Apagar)** para apagar la instancia del dispositivo virtual Panorama en el gestor de máquinas virtuales.

STEP 2 | Haga doble clic en la instancia del dispositivo virtual Panorama en el gestor de máquinas virtuales y seleccione **Show virtual hardware details (Mostrar detalles de hardware virtual)** .

STEP 3 | Edite los núcleos de la CPU del dispositivo virtual Panorama asignado.

1. Edite las **CPU** asignadas actualmente.
2. Haga clic en **Apply (Aplicar)** para aplicar la asignación del núcleo de la CPU reconfigurado.

STEP 4 | Edite la memoria del dispositivo virtual Panorama asignado.

1. Edite la **memoria** asignada actualmente.
2. Haga clic en **Apply (Aplicar)** para aplicar la asignación de la memoria reconfigurada.

STEP 5 | Haga clic en **Power on (Encender)** para encender la instancia del dispositivo virtual Panorama.

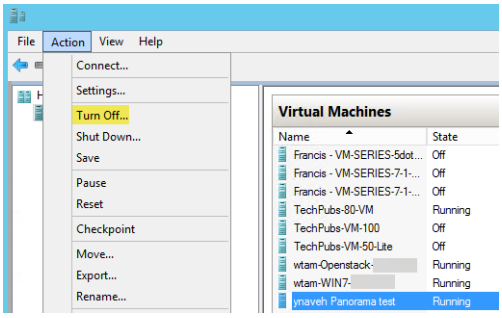
Aumento de CPU y memoria para Panorama en Hyper-V

Para obtener información sobre los requisitos mínimos de CPU y memoria de Panorama™, consulte Aumento de CPU y memoria en el dispositivo virtual Panorama.

Un dispositivo virtual Panorama en modo de recopilador de logs no permanece en modo de recopilador de logs si cambia el tamaño de la máquina virtual después de implementarla. Esto puede provocar una pérdida de datos de logs.

STEP 1 | Desactive el dispositivo virtual de Panorama.

1. En el gestor de Hyper-V, seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Action (Acción)** > **Turn Off (Apagar)** para apagar el dispositivo virtual Panorama.

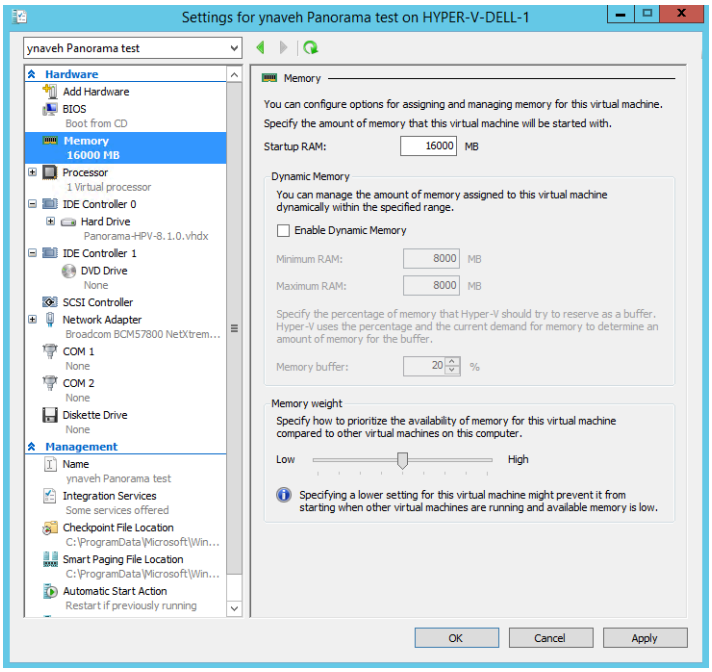


 ©2023 Palo Alto Networks, Inc.

STEP 2 | En el gestor de Hyper-V, seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)** y seleccione **Action (Acción)** > **Settings (Ajustes)** para editar los recursos del dispositivo virtual Panorama.

STEP 3 | Edite la memoria del dispositivo virtual Panorama asignado.

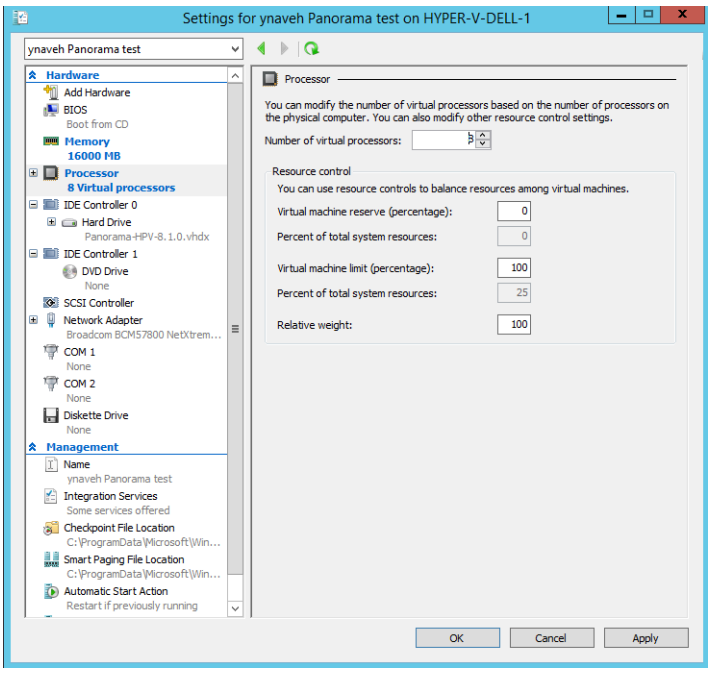
1. En la lista **Hardware**, seleccione **Memory (Memoria)**.
2. Edite la **Startup RAM (RAM de arranque)** asignada actualmente.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Edite los núcleos de la CPU del dispositivo virtual Panorama asignado.

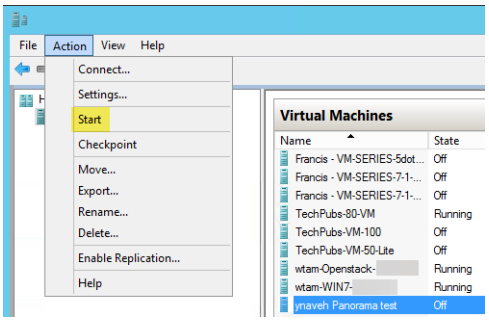
1. En la lista **Hardware**, seleccione **Processor (Procesador)**.
2. Edite el **Number of virtual processors (Número de procesadores virtuales)** asignados actualmente.



STEP 5 | Haga clic en **Apply (Aplicar)** para aplicar la memoria y los núcleos de la CPU reasignados.

STEP 6 | Active el dispositivo virtual Panorama.

1. Seleccione la instancia del dispositivo virtual Panorama de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Action (Acción)** > **Start (Iniciar)** para encender la instancia del dispositivo virtual Panorama.



Aumento de las CPU y la memoria para Panorama en Oracle Cloud Infrastructure (OCI)

Puede cambiar el tipo de instancia del dispositivo virtual Panorama™ para aumentar las CPU y la memoria asignadas a la instancia del dispositivo virtual Panorama. Asegúrese de revisar Requisitos previos de configuración del dispositivo virtual Panorama antes de modificar la CPU y la memoria de la instancia del dispositivo virtual Panorama.

STEP 1 | Inicie sesión en la consola de Oracle Cloud Infrastructure.

©2023 Palo Alto Networks, Inc.

STEP 2 | Apague la instancia del dispositivo virtual Panorama.

1. Seleccione **Compute (Procesar)** > **Instances (Instancias)** y haga clic en el nombre de la instancia del dispositivo virtual Panorama.
2. **Detenga** la instancia del dispositivo virtual Panorama.

STEP 3 | Aumente las CPU y la memoria.

1. En los detalles de la instancia, seleccione **Edit (Editar)** > **Edit Shape (Editar forma)**.
2. Aumente el número de CPU y memoria asignadas a la instancia.
3. Haga clic en **Save changes (Guardar cambios)**.

STEP 4 | En los detalles de la instancia, haga clic en **Start (Iniciar)** para iniciar el dispositivo virtual Panorama.

STEP 5 | Verifique el aumento de la CPU y la memoria.

1. Inicio de sesión en la CLI de Panorama.
2. Consulte la información del sistema del dispositivo virtual Panorama.

```
admin> show system info
```

3. Compruebe que `num-cpus` y `ram-in-gb` muestran el número correcto de CPU y la cantidad de memoria según el tipo de instancia seleccionado.

Aumento del disco del sistema en el dispositivo virtual de Panorama

Amplíe la capacidad de disco del sistema a 224 GB para que el dispositivo virtual Panorama admita grandes conjuntos de datos para permitir suficiente espacio en disco para elementos como actualizaciones dinámicas cuando Gestión de implementaciones de cortafuegos a gran escala. Además, un disco del sistema de 224 GB amplía el almacenamiento para supervisar y reportar datos del estado del cortafuegos gestionado si pretendía usar el dispositivo virtual Panorama en modo Panorama para gestionar su implementación de SD-WAN.

- Aumento del disco del sistema para Panorama en un servidor ESXi
- Aumento del disco del sistema para Panorama en Google Cloud Platform

Aumento del disco del sistema para Panorama en un servidor ESXi

Añada un disco del sistema de 224 GB para reemplazar el disco del sistema predeterminado de 81 GB. Para conocer los requisitos de recursos mínimos del dispositivo virtual Panorama, consulte Requisitos previos de configuración del dispositivo virtual Panorama.

No es posible reducir el disco del sistema del dispositivo virtual Panorama a 81 GB.

STEP 1 | (Prácticas recomendadas) Guardado y exportación de configuraciones de Panorama y de cortafuegos.

Guarde y exporte su configuración de cortafuegos y Panorama para asegurarse de que puede recuperar Panorama si se produce algún problema.

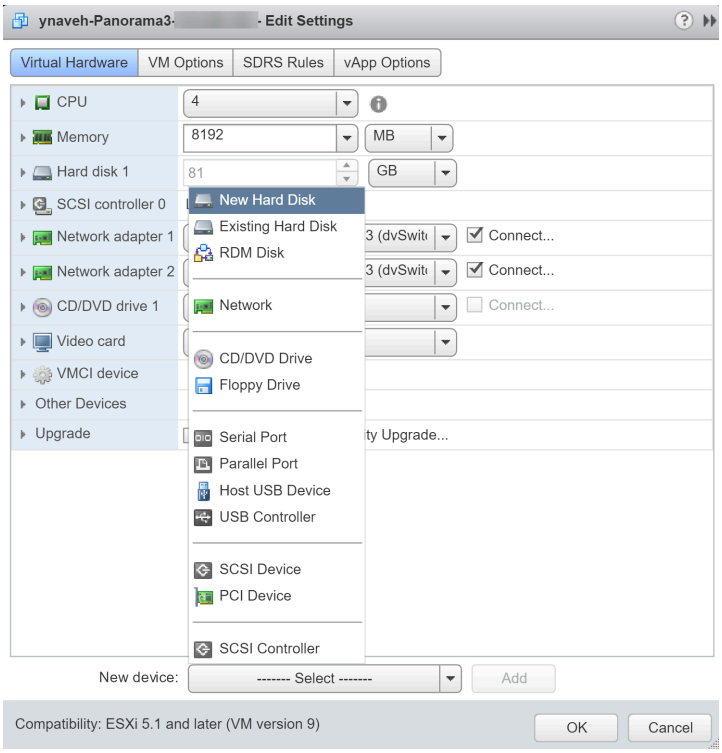
STEP 2 | Acceda al cliente de VMware vSphere y vaya hasta su dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.

STEP 4 | Añada el nuevo disco del sistema de 224 GB.

1. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
2. Seleccione **New Hard Disk (Nuevo disco duro)** como **New Device (Nuevo dispositivo)** y **añada** el nuevo dispositivo.
3. Configure el nuevo disco duro con 224 GB y haga clic en **OK (Aceptar)**.



STEP 5 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**.

Panorama puede tardar hasta 30 minutos en inicializar el nuevo disco del sistema. Durante ese tiempo, la interfaz web de Panorama y la CLI no están disponibles.

©2023 Palo Alto Networks, Inc.

STEP 6 | Migre los datos del disco del disco del sistema anterior al disco del sistema nuevo.

En este ejemplo, se realiza la migración al disco del sistema recién añadido con la etiqueta sdb.

1. Inicio de sesión en la CLI de Panorama.
2. Especifique el siguiente comando para ver los discos del sistema disponibles para la migración:

```
admin> request system clone-system-disk target ?
```

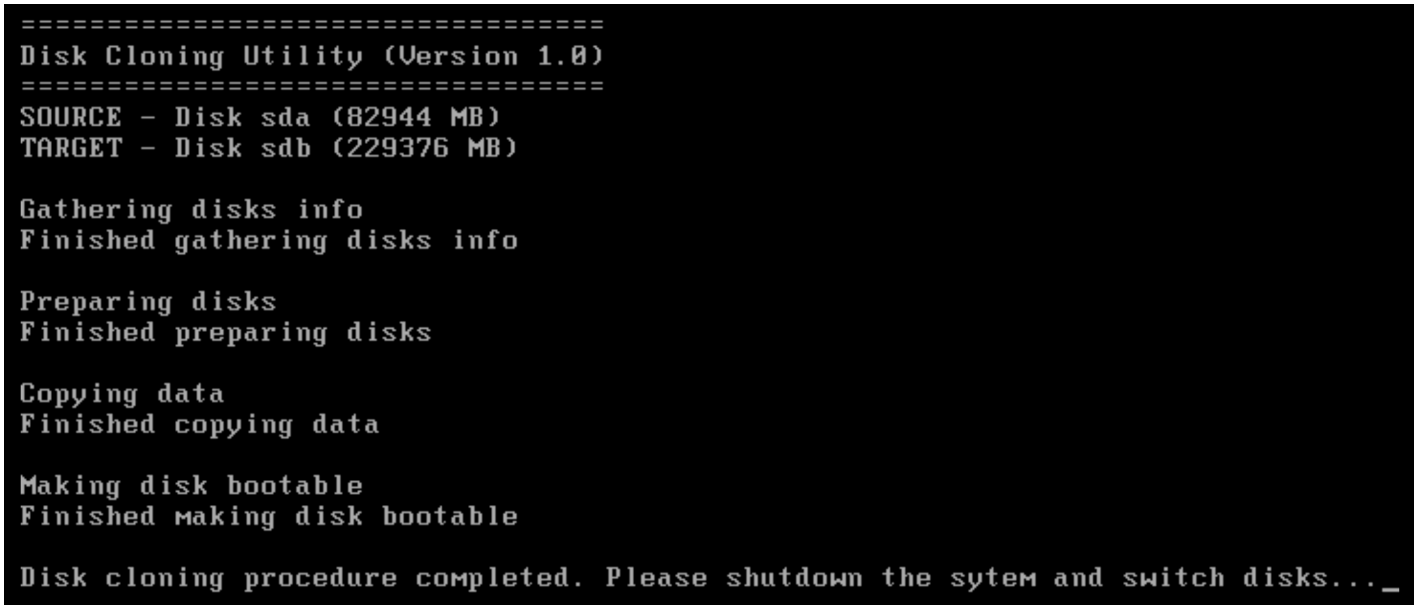
3. Migre los datos del disco al nuevo disco del sistema con el siguiente comando:

```
admin> request system clone-system-disk target sdb
```

Especifique **Y (S)** cuando se le solicite para iniciar la migración del disco.

Para iniciar la migración, Panorama se reinicia y tarda al menos 20 minutos en completar la migración del disco. Durante ese tiempo, la interfaz web de Panorama y la CLI no están disponibles.

4. Supervise la migración del disco desde la consola web. Continúe con el siguiente paso solo después de que Panorama muestre el siguiente mensaje para indicar que la migración del disco se ha completado.



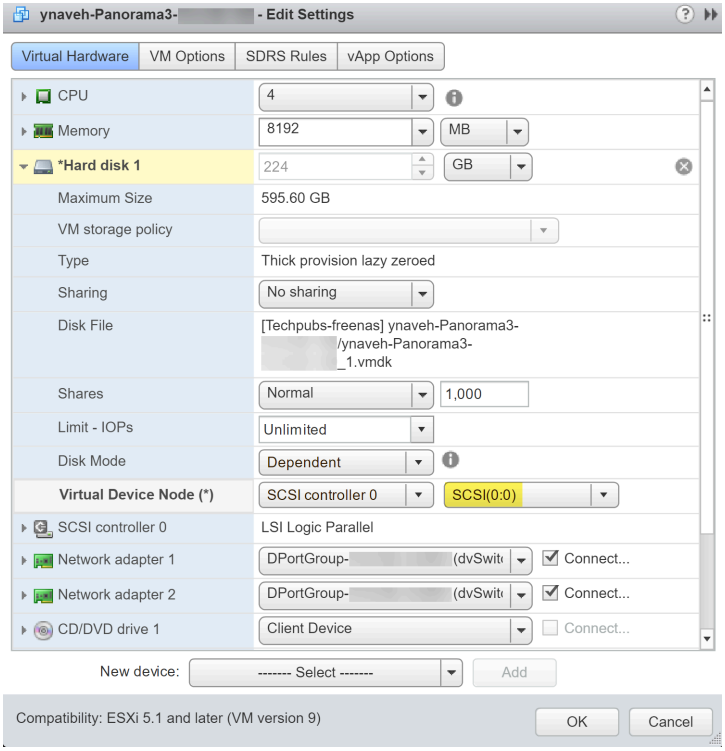
STEP 7 | Elimine el disco del sistema anterior.

1. Acceda al cliente de VMware vSphere y vaya hasta su dispositivo virtual Panorama.
2. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
3. Haga clic con el botón derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar configuración)**.
4. Elimine el disco del sistema de 81 GB antiguo y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Modifique el nodo del dispositivo virtual para el nuevo disco del sistema.

1. Expanda las opciones de configuración para el nuevo disco del sistema.
2. Seleccione **SCSI(0:0)** como **nodo de dispositivo virtual**.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.



STEP 9 | Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**.

STEP 10 | Compruebe que la migración al nuevo disco del sistema se haya realizado correctamente.

1. Inicio de sesión en la CLI de Panorama.
2. Especifique el siguiente comando para ver las particiones del disco del sistema.

   Debe añadir las particiones `/dev/root`, `/dev/sda5`, `/dev/sda6` y `/dev/sda8` para confirmar que el tamaño del disco ha aumentado.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```


©2023 Palo Alto Networks, Inc.

Aumento del disco del sistema para Panorama en Google Cloud Platform

Añada un disco del sistema de 224 GB para reemplazar el disco del sistema predeterminado de 81 GB. Para conocer los requisitos de recursos mínimos del dispositivo virtual Panorama, consulte Requisitos previos de configuración del dispositivo virtual Panorama.

STEP 1 | (Prácticas recomendadas) Guardado y exportación de configuraciones de Panorama y de cortafuegos.

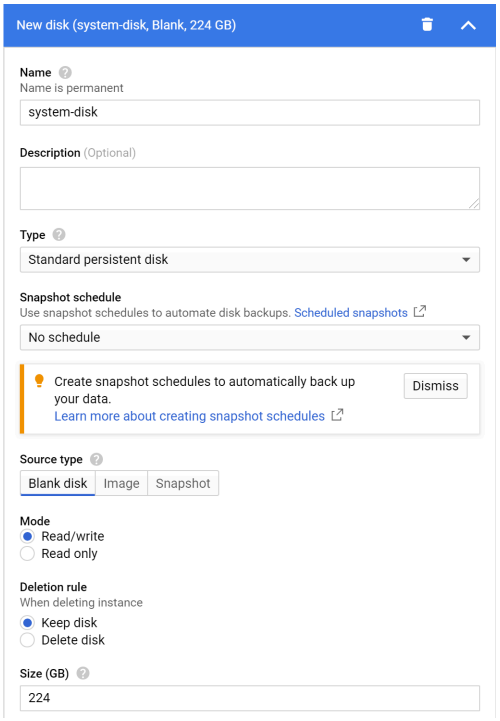
Guarde y exporte su configuración de cortafuegos y Panorama para asegurarse de que puede recuperar Panorama si se produce algún problema.

STEP 2 | Inicie sesión en la consola de Google Cloud.

STEP 3 | En **VM Instances (Instancias de VM)**, **detenga** la instancia de VM de Panorama.

STEP 4 | Añada el nuevo disco del sistema de 224 GB.

1. Seleccione la instancia de VM de Panorama y elija **Edit (Editar)**.
2. En la sección **Additional disks (Discos adicionales)**, seleccione **Add new disk (Añadir nuevo disco)**.
3. Configure el nuevo disco con 224 GB y haga clic en **OK (Aceptar)**.



STEP 5 | En **VM Instances (Instancias de VM)**, **inicie** la instancia de VM de Panorama.

©2023 Palo Alto Networks, Inc.

STEP 6 | Migre los datos del disco del disco del sistema anterior al disco del sistema nuevo.

En este ejemplo, se realiza la migración al disco del sistema recién añadido con la etiqueta sdb.

1. Inicio de sesión en la CLI de Panorama.
2. Especifique el siguiente comando para ver los discos del sistema disponibles para la migración:

```
admin> request system clone-system-disk target ?
```

3. Migre los datos del disco al nuevo disco del sistema con el siguiente comando:

```
admin> request system clone-system-disk target sdb
```

Especifique **Y (S)** cuando se le solicite para iniciar la migración del disco.

Para iniciar la migración, Panorama se reinicia y tarda al menos 20 minutos en completar la migración del disco. Durante ese tiempo, la interfaz web de Panorama y la CLI no están disponibles.

4. Supervise la migración del disco. Para ello, intente iniciar sesión en la CLI de Panorama. El servidor de gestión Panorama pasará al modo de mantenimiento después de que se complete la migración del disco del sistema. Podrá iniciar sesión en la CLI de Panorama mientras esté en ese modo.

STEP 7 | Conecte el nuevo disco del sistema de 224 GB.

1. En **VM Instances (Instancias de VM)**, **detenga** la instancia de VM de Panorama.
2. Seleccione la instancia de VM de Panorama y elija **Edit (Editar)**.
3. En la sección **Additional disks (Discos adicionales)**, desconecte el nuevo disco del sistema de 224 GB.
4. En la sección **Boot Disk (Disco de inicio)**, desconecte el disco del sistema antiguo de 81 GB.
5. En la sección **Boot Disk (Disco de inicio)**, **añada el elemento** y seleccione el nuevo disco del sistema de 224 GB.
6. **Guarde** los cambios de configuración.

STEP 8 | En **VM Instances (Instancias de VM)**, **inicie** la instancia de VM de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Compruebe que la migración al nuevo disco del sistema se haya realizado correctamente.

1. Inicio de sesión en la CLI de Panorama.
2. Especifique el siguiente comando para ver las particiones del disco del sistema.

   Debe añadir las particiones **/dev/root**, **/dev/sda5**, **/dev/sda6** y **/dev/sda8** para confirmar que el tamaño del disco ha aumentado.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Realización de la configuración del dispositivo virtual Panorama

Después de Realización de la configuración inicial del dispositivo virtual Panorama, continúe con las siguientes tareas para una configuración adicional:

- Activación de una licencia de asistencia técnica de Panorama
- Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet
- Instalación de actualizaciones de contenido y software de Panorama
- Acceso y navegación en las interfaces de gestión de Panorama
- Configuración del acceso administrativo a Panorama
- Gestión de cortafuegos

Cómo convertir su dispositivo virtual Panorama

Puede convertir su dispositivo virtual Panorama™ de evaluación en un dispositivo virtual Panorama de producción para conservar su configuración existente y comenzar a aprovechar la plataforma de gestión.

Si utiliza las licencias de Enterprise License Agreement (ELA), puede convertir un dispositivo virtual Panorama de producción existente para aprovechar los beneficios de las licencias de ELA.

- Cómo convertir el dispositivo virtual de evaluación Panorama en uno de producción con el recopilador de logs local
- Cómo convertir el dispositivo virtual de evaluación Panorama en uno de producción sin el recopilador de logs local
- Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex con el recopilador de logs local
- Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex sin el recopilador de logs local

 ©2023 Palo Alto Networks, Inc.

- Cómo convertir el dispositivo virtual de producción Panorama en uno ELA

Cómo convertir el dispositivo virtual de evaluación Panorama en uno de producción con el recopilador de logs local

Si tiene un dispositivo virtual Panorama™ de evaluación en modo Panorama configurado con un recopilador de logs local, puede convertirlo en un Panorama de producción migrando la configuración del Panorama de evaluación al Panorama de producción y modificándolo según sea necesario.

Los logs incorporados por el recopilador de logs en un dispositivo virtual Panorama no se pueden migrar.

Si necesita mantener el acceso a los logs almacenados en el dispositivo virtual Panorama de evaluación, después de migrar la configuración del Panorama de evaluación ***al Panorama de producción, mantenga el Panorama de evaluación encendido para acceder a los registros localmente durante el resto de la vida útil de la licencia de evaluación. No se puede agregar el Panorama de evaluación al Panorama de producción como recopilador gestionado.***

STEP 1 | Planifique la migración.

- ☐ Actualice el software del dispositivo virtual Panorama antes de convertir el dispositivo virtual Panorama de evaluación en un dispositivo virtual Panorama de producción. Revise la Matriz de compatibilidad para conocer la versión mínima de PAN-OS requerida para el hipervisor. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
- ☐ Programe un periodo de mantenimiento para la migración.

STEP 2 | Configure su dispositivo virtual Panorama de producción.

1. Configuración del dispositivo virtual Panorama.
2. Registre el dispositivo virtual Panorama con el portal de atención al cliente (CSP, Customer Support Portal) de Palo Alto Networks.

   El número de serie y el código de autorización de Panorama se encuentran en el correo electrónico de resumen del pedido de Palo Alto Networks.
3. Instale las actualizaciones de contenido y software de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Active la licencia de administración de dispositivos en el Portal de atención al cliente (CSP) de Palo Alto Networks para el dispositivo virtual Panorama de producción.

1. Inicie sesión en el CSP de Palo Alto Networks.
2. Seleccione **Assets (Activos)** > **Devices (Dispositivos)** y localice su dispositivo virtual Panorama.
3. En la columna **Action (Acción)**, haga clic en el icono del lápiz para editar las licencias del dispositivo.
4. Seleccione **Activate Auth-Code (Activar código de autenticación)** y especifique el **código de autorización**.
5. Seleccione **Agree and Submit (Aceptar y enviar)** para activar la licencia de gestión de dispositivos.

STEP 4 | Exporte la configuración de Panorama desde el dispositivo virtual Panorama de evaluación.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione `running-config.xml` y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.
4. Busque el archivo `running-config.xml` que exportó y cambie el nombre del archivo XML. Esto es necesario para importar la configuración, ya que Panorama no admite la importación de un archivo XML con el nombre `running-config.xml`.

STEP 5 | Cargue la instantánea de configuración de Panorama exportada del dispositivo virtual Panorama de evaluación en el dispositivo virtual Panorama de producción.

1. Inicio de sesión en la interfaz web de Panorama del dispositivo virtual de producción Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)** y en **Browse (Explorar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo virtual Panorama, y luego haga clic en **OK (Aceptar)**.
4. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, deje en blanco **Decryption Key (Clave de descifrado)** y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración.
5. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Modifique la configuración del dispositivo virtual Panorama de producción.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
2. Edite la configuración general, modifique el nombre de host en **Hostname (Nombre de host)** y haga clic en **OK (Aceptar)**.
3. Edite la configuración de la interfaz de administración para configurar la dirección IP de administración y haga clic en **OK (Aceptar)**.

   El método más eficiente consiste en asignar una dirección IP nueva al dispositivo virtual Panorama de evaluación y reutilizar su dirección IP anterior para el dispositivo virtual Panorama de producción. Esto garantiza que el dispositivo virtual Panorama de evaluación permanezca accesible y que los cortafuegos puedan dirigirse al dispositivo de producción sin tener que volver a configurar la dirección IP de Panorama en cada cortafuegos.
4. Quite la configuración del recopilador de logs importada desde el Panorama de evaluación.
   1. Seleccione **Panorama** > **Collector Group (Grupo de recopiladores)** y **elimine** todos los grupos de recopiladores configurados.
   2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Delete (Eliminar)** para borrar todos los recopiladores de logs configurados.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 7 | Configure sus recopiladores de logs y grupos de recopiladores.

Debe añadir los recopiladores gestionados, la configuración del grupo de recopiladores y las configuraciones de reenvío de logs que eliminó en el paso anterior, y agregar el recopilador de logs local.

1. Configuración de recopiladores gestionados.
2. Configuración de un grupo de recopiladores.
3. Configuración del reenvío de logs a Panorama.

STEP 8 | Verifique que las licencias de gestión de dispositivos y soporte se hayan activado correctamente.

1. Seleccione **Panorama** > **Licenses (Licencias)** y **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
2. Verifique que la **licencia de gestión de dispositivos** muestre la cantidad correcta de dispositivos.
3. Seleccione **Panorama** > **Support (Soporte)** y verifique que aparezca el **nivel** y la **fecha de caducidad** del soporte correctos.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Sincronice el dispositivo virtual Panorama de producción con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama de producción, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que aparece **Connected (Conectado)** en la columna "Device State" (Estado de dispositivo) correspondiente a los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Cómo convertir el dispositivo virtual de evaluación Panorama en uno de producción sin el recopilador de logs local

Cambie el número de serie del dispositivo virtual Panorama de evaluación en modo Solo gestión o en modo Panorama sin ningún recopilador de logs local configurado para convertirlo en un dispositivo virtual Panorama de producción.

Si se configura un recopilador de logs local, consulte Cómo convertir el dispositivo virtual de evaluación Panorama en uno de producción con el recopilador de logs local.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.

STEP 3 | Ingrese el **número de serie** proporcionado por Palo Alto Networks.

El número de serie de Panorama y el código de autorización se obtienen en el perfil de implementación que creó en el paso anterior.

STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Reinicie el servidor de gestión en el dispositivo virtual Panorama.

1. Inicio de sesión en la CLI de Panorama.
2. Reinicie el servidor de gestión.

```
admin> debug software restart process management-server
```

Cuando se reinicia el servidor de gestión, se cierra la sesión de todos los administradores de la interfaz web de Panorama y la CLI.

STEP 7 | Verifique que las licencias de gestión de dispositivos y soporte se hayan activado correctamente.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Licenses (Licencias)** y **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
3. Verifique que la **licencia de gestión de dispositivos** muestre la cantidad correcta de dispositivos.
4. Seleccione **Panorama** > **Support (Soporte)** y verifique que aparezca el **nivel** y la **fecha de caducidad** del soporte correctos.

STEP 8 | Sincronice el dispositivo virtual Panorama de producción con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama de producción, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que aparece **Connected (Conectado)** en la columna "Device State" (Estado de dispositivo) correspondiente a los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex con el recopilador de logs local

Si tiene un dispositivo virtual de evaluación Panorama™ en modo Panorama configurado con un recopilador de logs local, puede convertirlo en un Panorama de producción con las licencias de

 ©2023 Palo Alto Networks, Inc.

VM Flex migrando la configuración del Panorama de evaluación al Panorama de producción y modificándolo según sea necesario.

Si no se ha configurado un recopilador de logs local, consulte Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex sin el recopilador de logs local.

Los logs incorporados por el recopilador de logs en un dispositivo virtual Panorama no se pueden migrar.

Si necesita mantener el acceso a los logs almacenados en el dispositivo virtual Panorama de evaluación, después de** migrar la configuración del Panorama de evaluación **al Panorama de producción, mantenga el Panorama de evaluación encendido para acceder a los registros localmente durante el resto de la vida útil de la licencia de evaluación. No se puede agregar el Panorama de evaluación al Panorama de producción como recopilador gestionado.

STEP 1 | Planifique la migración.

- ❑ Actualice el software del dispositivo virtual Panorama antes de convertir el dispositivo virtual Panorama de evaluación en un dispositivo virtual Panorama de producción. Revise la Matriz de compatibilidad para conocer la versión mínima de PAN-OS requerida para el hipervisor. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
- ❑ Programe un periodo de mantenimiento para la migración.

STEP 2 | Obtenga el número de serie de Panorama y el código de autenticación de su perfil de implementación de licencias flexible de VM-Series.

1. Inicie sesión en el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks.
2. Cree un perfil de implementación que habilite un dispositivo virtual Panorama.
3. Haga clic en Provision Panorama (Aprovisionar Panorama) para generar un número de serie.
4. Copie el **Serial Number (Número de serie)** y el **Auth Code (Código de autenticación)**.

STEP 3 | Configure su dispositivo virtual Panorama de producción.

1. Inicie sesión en el CSP de Palo Alto Networks.
2. Configuración del dispositivo virtual Panorama.
3. Registre el dispositivo virtual Panorama con el portal de atención al cliente (CSP, Customer Support Portal) de Palo Alto Networks.

   El número de serie de Panorama y el código de autorización que generó en el paso anterior.
4. Instale las actualizaciones de contenido y software de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Active la licencia de administración de dispositivos en el CSP de Palo Alto Networks para el dispositivo virtual Panorama de producción.

1. Seleccione **Assets (Activos)** > **Devices (Dispositivos)** y localice su dispositivo virtual Panorama.
2. En la columna **Action (Acción)**, haga clic en el icono del lápiz para editar las licencias del dispositivo.
3. Seleccione **Activate Auth-Code (Activar código de autenticación)** y especifique el **código de autorización**.
4. Seleccione **Agree and Submit (Aceptar y enviar)** para activar la licencia de gestión de dispositivos.

STEP 5 | Exporte la configuración de Panorama desde el dispositivo virtual Panorama de evaluación.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione `running-config.xml` y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.
4. Busque el archivo `running-config.xml` que exportó y cambie el nombre del archivo XML. Esto es necesario para importar la configuración, ya que Panorama no admite la importación de un archivo XML con el nombre `running-config.xml`.

STEP 6 | Cargue la instantánea de configuración de Panorama exportada del dispositivo virtual Panorama de evaluación en el dispositivo virtual Panorama de producción.

1. Inicio de sesión en la interfaz web de Panorama del dispositivo Panorama virtual de producción.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)** y en **Browse (Explorar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo virtual Panorama, y luego haga clic en **OK (Aceptar)**.
4. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, deje en blanco **Decryption Key (Clave de descifrado)** y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración.
5. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Modifique la configuración del dispositivo virtual Panorama de producción.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
2. Edite la configuración general, modifique el nombre de host en **Hostname (Nombre de host)** y haga clic en **OK (Aceptar)**.
3. Edite la configuración de la interfaz de administración para configurar la dirección IP de administración y haga clic en **OK (Aceptar)**.

   El método más eficiente consiste en asignar una dirección IP nueva al dispositivo virtual Panorama de evaluación y reutilizar su dirección IP anterior para el dispositivo virtual Panorama de producción. Esto garantiza que el dispositivo virtual Panorama de evaluación permanezca accesible y que los cortafuegos puedan dirigirse al dispositivo de producción sin tener que volver a configurar la dirección IP de Panorama en cada cortafuegos.
4. Quite la configuración del recopilador de logs importada desde el Panorama de evaluación.
   1. Seleccione **Panorama** > **Collector Group (Grupo de recopiladores)** y **elimine** todos los grupos de recopiladores configurados.
   2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Delete (Eliminar)** para borrar todos los recopiladores de logs configurados.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 8 | Vuelva a configurar sus recopiladores de logs y grupos de recopiladores.

Debe añadir los recopiladores gestionados, la configuración del grupo de recopiladores y las configuraciones de reenvío de logs que eliminó en el paso anterior, y agregar el recopilador de logs local.

1. Configuración de recopiladores gestionados.
2. Configuración de un grupo de recopiladores.
3. Configuración del reenvío de logs a Panorama.

STEP 9 | Verifique que las licencias de gestión de dispositivos y soporte se hayan activado correctamente.

1. Seleccione **Panorama** > **Licenses (Licencias)** y **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
2. Verifique que la **licencia de gestión de dispositivos** muestre la cantidad correcta de dispositivos.
3. Seleccione **Panorama** > **Support (Soporte)** y verifique que aparezca el **nivel** y la **fecha de caducidad** del soporte correctos.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Sincronice el dispositivo virtual Panorama de producción con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama de producción, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que aparece **Connected (Conectado)** en la columna "Device State" (Estado de dispositivo) correspondiente a los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex sin el recopilador de logs local

Cambie el número de serie del dispositivo virtual Panorama de evaluación en modo Solo gestión o en modo Panorama sin ningún recopilador de logs local configurado para convertirlo en un dispositivo virtual Panorama de producción.

Si se configura un recopilador de logs local, consulte Cómo convertir el dispositivo virtual de evaluación Panorama en licencias de VM Flex con el recopilador de logs local.

STEP 1 | Obtenga el número de serie de Panorama y el código de autenticación de su perfil de implementación de licencias flexible de VM-Series.

1. Inicie sesión en el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks.
2. Cree un perfil de implementación que habilite un dispositivo virtual Panorama.
3. Haga clic en Provision Panorama (Aprovisionar Panorama) para generar un número de serie.
4. Copie el **Serial Number (Número de serie)** y el **Auth Code (Código de autenticación)**.

STEP 2 | Inicie sesión en la interfaz web de Panorama.

STEP 3 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.

STEP 4 | Ingrese el **número de serie** proporcionado por Palo Alto Networks.

El número de serie de Panorama y el código de autorización que generó en el paso anterior.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 7 | Reinicie el servidor de gestión en el dispositivo virtual Panorama.

1. Inicio de sesión en la CLI de Panorama.
2. Reinicie el servidor de gestión.

```
admin> debug software restart process management-server
```

Cuando se reinicia el servidor de gestión, se cierra la sesión de todos los administradores de la interfaz web de Panorama y la CLI.

STEP 8 | Verifique que las licencias de gestión de dispositivos y soporte se hayan activado correctamente.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Licenses (Licencias)** y **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
3. Verifique que la **licencia de gestión de dispositivos** muestre la cantidad correcta de dispositivos.
4. Seleccione **Panorama** > **Support (Soporte)** y verifique que aparezca el **nivel** y la **fecha de caducidad** del soporte correctos.

STEP 9 | Sincronice el dispositivo virtual Panorama de producción con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama de producción, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que aparece **Connected (Conectado)** en la columna "Device State" (Estado de dispositivo) correspondiente a los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

 ©2023 Palo Alto Networks, Inc.

Cómo convertir el dispositivo virtual de producción Panorama en uno ELA

Puede convertir su dispositivo virtual Panorama™ de producción para seguir aprovechando su Panorama con los beneficios de las licencias de ELA. Para convertir la implementación de producción, Panorama debe tener acceso a Internet externo.

La conversión del Panorama de producción a una licencia de ELA se admite en el modo Solo gestión y modo Panorama con o sin un recopilador de logs local configurado. Si su Panorama tiene configurado un recopilador de logs local, debe enviar una incidencia de asistencia técnica con Palo Alto Networks para convertir su Panorama a una licencia de ELA.

Durante la conversión de un Panorama de producción a una licencia de ELA, no cambie el número de serie de Panorama si está configurado un recopilador de logs local.

El log del recopilador de logs local se vuelve inaccesible y otros recopiladores de logs del grupo de recopiladores pueden volverse inaccesibles y ya no incorporar logs si se cambia el número de serie de un recopilador de logs.

STEP 1 | Convierta su Panorama en una licencia de ELA.

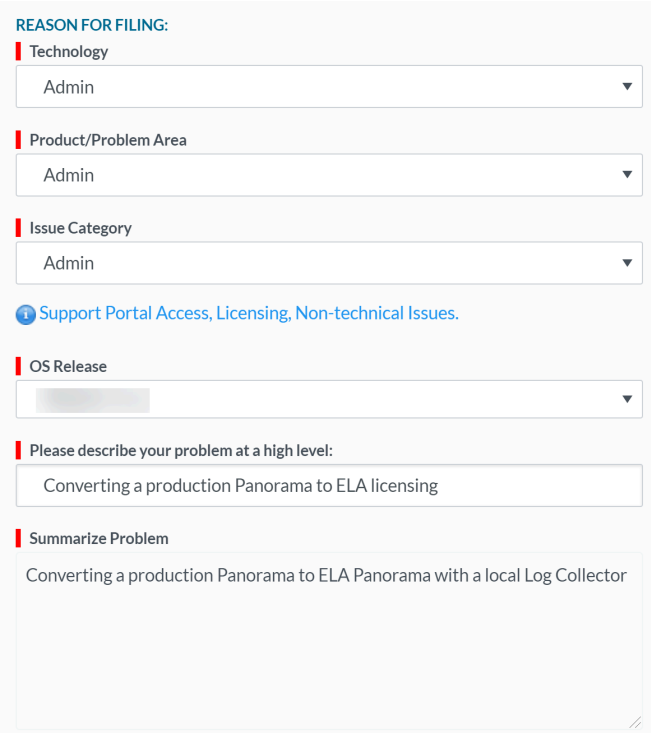
- **Dispositivo virtual Panorama en modo Panorama con un recopilador de logs local.**

  Envíe una incidencia de asistencia técnica con Palo Alto Networks para convertir su Panorama en una licencia de ELA. Esto es necesario para conservar todos los logs existentes en el recopilador de logs local cuando convierte un Panorama con un recopilador de logs local en una licencia de ELA. A continuación, se proporciona un ejemplo para ayudar a presentar

 ©2023 Palo Alto Networks, Inc.

la incidencia de asistencia técnica. Cree la incidencia exactamente como se muestra a continuación y seleccione la **versión del sistema operativo** que ejecute su Panorama.

Continúe con el siguiente paso solo después de que el soporte de Palo Alto Networks resuelva correctamente su incidencia de asistencia técnica.



- **Dispositivo virtual Panorama en modo Solo gestión o modo Panorama sin recopilador de logs local.**

  1. Genere un número de serie a partir de su grupo de licencias de ELA.

     1. Inicie sesión en el CSP de Palo Alto Networks.
     2. Seleccione **Assets (Activos)** > **VM-Series Auth-Codes (Códigos de autenticación VM-Series)** y localice su grupo de licencias de ELA.
     3. En la columna "Actions" (Acciones), seleccione **Panorama** y **Provision (Aprovisionar)** un nuevo número de serie.

        Confirme la nueva provisión de número de serie cuando se le solicite.
     4. Copie el número de serie recién aprovisionado.
  2. Inicie sesión en la interfaz web de Panorama.
  3. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
  4. Introduzca el **Serial Number (Número de serie)** que aprovisionó.
  5. Haga clic en **OK (Aceptar)**.
  6. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 2 | Inicie sesión en la interfaz web de Panorama si aún no lo ha hecho.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Seleccione **Panorama** > **Licenses (Licencias)** y **Retrieve new license from license server (Recuperar licencia nueva del servidor de licencias)**.

STEP 4 | Verifique que Panorama haya recuperado las nuevas licencias según su acuerdo de ELA.

STEP 5 | Verifique que las licencias de gestión de dispositivos y soporte se hayan activado correctamente.

1. Seleccione **Panorama** > **Licenses (Licencias)** y verifique que se activaron las licencias correctas.
2. Seleccione **Panorama** > **Support (Soporte)** y verifique que aparezca el **nivel** y la **fecha de caducidad** del soporte correctos.

 ©2023 Palo Alto Networks, Inc.

Configuración del dispositivo de la serie M

Los dispositivos M-700, M-600, M-500, M-300 y M-200 son dispositivos de hardware de alto rendimiento que puede implementar en modo de solo administración (como servidores de administración Panorama sin colección de registros local), en modo Panorama (como servidores de administración Panorama con recopilación de registros local) o en modo recopilador de registros (como recopiladores de registros dedicados). Los dispositivos proporcionan múltiples interfaces que puede asignar a diversos servicios de Panorama, como gestión de cortafuegos y recopilación de logs. Antes de configurar el dispositivo, considere cómo puede configurar las interfaces para optimizar la seguridad, habilitar la segmentación de red (en implementaciones a gran escala) y equilibrar la carga del tráfico para los servicios de Panorama.

- Interfaces del dispositivo M-Series
- Realización de la configuración inicial del dispositivo de la serie M
- Descripción general de VM-Series
- Configuración del dispositivo M-Series como un recopilador de logs
- Aumento de la capacidad de almacenamiento en el dispositivo M-Series
- Configuración de Panorama para usar varias interfaces

Interfaces del dispositivo M-Series

Los dispositivos Panorama M-700, M-600, M-500, M-300, M-200 y M-100 tienen varias interfaces para comunicarse con otros sistemas, como los cortafuegos gestionados y los sistemas cliente de los administradores de Panorama. Panorama se comunica con estos sistemas para realizar diversos servicios, incluidos la gestión de dispositivos (cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire), recopilación de logs, comunicación con grupos de recopiladores, implementación de software y actualizaciones de contenido en dispositivos y acceso administrativo a Panorama. De forma predeterminada, Panorama usa la interfaz de gestión (MGT) para estas funciones. Sin embargo, puede mejorar la seguridad reservando la interfaz de MGT para el acceso administrativo y dedicando interfaces separadas para los otros servicios. En una red a gran escala con múltiples subredes y un gran tráfico de logs, la utilización de varias interfaces para la gestión de dispositivos y la recopilación de logs también permite la segmentación de la red y el equilibrio de carga (consulte Configuración de Panorama para usar varias interfaces)

Al asignar servicios de Panorama a varias interfaces, tenga en cuenta que solo la interfaz MGT permite el acceso administrativo a Panorama para tareas de configuración y supervisión. Puede asignar cualquier interfaz a otros servicios cuando lleva a cabo la Realización de la configuración inicial del dispositivo serie M. Las Guías de referencia de hardware de dispositivos serie M explican dónde conectar los cables para estas interfaces. El dispositivo M-100 admite un rendimiento de 1 Gbps en todas sus interfaces: MGT, Eth1, Eth2 y Eth3. Además de estas interfaces, el dispositivo M-500 admite un rendimiento de 10 Gbps en sus interfaces Eth4 y Eth5.

Los dispositivos M-Series no son compatibles con el Protocolo de control de agregación de enlaces (Link Aggregation Control Protocol, LACP) para añadir estas interfaces.

 ©2023 Palo Alto Networks, Inc.

Interfaces admitidas

Las interfaces se pueden usar para la gestión de dispositivos, la recopilación de logs, la comunicación entre grupos de dispositivos, la activación de licencias y las actualizaciones de software. Consulte Configuración de Panorama para usar varias interfaces para obtener más información sobre la segmentación de la red.

Interface (Interfaz)	Velocidad máxima	Dispositiv M-700	Dispositivo M-600	Dispositivo M-500	Dispositiv M-300	Dispositivo M-200
Gestión (Management, MGT)	1Gbps	✓	✓	✓	✓	✓
Ethernet 1 (Eth1)	1Gbps	✓	✓	✓	✓	✓
Ethernet 2 (Eth2)	1Gbps	—	✓	✓	—	✓
Ethernet 3 (Eth3)	1Gbps	—	✓	✓	—	✓
Ethernet 4 (Eth4)	10Gbps	✓	✓	✓	—	—
Ethernet 5 (Eth5)	10Gbps	✓	✓	✓	—	—

Tasas de registro de logs

Revise las tasas de registro de logs para todos los modelos de dispositivos serie M. Para conseguir las velocidades de creación de logs que aparecen continuación, el dispositivo M-Series debe ser un único recopilador de logs en un grupo de recopiladores, y debe instalar todos los discos de creación de logs para su modelo M-Series. Por ejemplo, para lograr 30 000 logs/s para el dispositivo M-500, debe instalar los 12 discos de creación de logs con discos de 1 TB o 2 TB.

Funciones y capacidades del modelos	Dispositivo M-700	Dispositivo M-600	Dispositivo M-500	Dispositivo M-300	Dispositivo M-200
Velocidad máxima de creación de logs para Panorama en modo Management	El almacenamiento de logs local no es compatible.				

©2023 Palo Alto Networks, Inc.

Funciones y capacidades del modelos	Dispositivo M-700	Dispositivo M-600	Dispositivo M-500	Dispositivo M-300	Dispositivo M-200
Only (Solo gestión)					
Velocidad máxima de creación de logs para Panorama en el modo Panorama	36 500 logs por segundo	25 000 logs por segundo	20 000 logs por segundo	16 500 logs por segundo	10 000 logs por segundo
Velocidad de creación de logs máxima para Panorama en el modo de recopilación de logs	73 000 logs por segundo	50 000 logs por segundo	30 000 logs por segundo	33 000 logs por segundo	28 000 logs por segundo
Máximo almacenamiento de logs en el dispositivo	48 TB (12 discos RAID de 8 TB)	48 TB (12 discos RAID de 8 TB)	• 24 TB (24 discos RAID de 2 TB) • 12 TB (24 discos RAID de 1 TB)	16 TB (4 discos RAID de 8 TB)	16 TB (4 discos RAID de 8 TB)
Almacenamiento de logs predeterminado en dispositivo	16 TB (4 discos RAID de 8 TB)	16 TB (4 discos RAID de 8 TB)	4 TB (4 discos RAID de 2 TB)	16 TB (4 discos RAID de 8 TB)	16 TB (4 discos RAID de 8 TB)
Almacenamiento de disco SSD en el dispositivo (para logs que generan los dispositivos de la serie M)	240GB	240GB	240GB	240GB	240GB
Almacenamiento de logs adjunto NFS	No disponible				

©2023 Palo Alto Networks, Inc.

Realización de la configuración inicial del dispositivo de la serie M

De forma predeterminada, Panorama tiene una dirección IP de 192.168.1.1 y el nombre de usuario/contraseña es admin/admin. Por motivos de seguridad, debe cambiar estos ajustes antes de continuar con otras tareas de configuración. Debe realizar estas tareas de configuración inicial desde la interfaz de gestión (MGT) o usando una conexión del puerto de serie directa al puerto de la consola del dispositivo M-700, M-600, M-500, M-300 o M-200.

Si está configurando un dispositivo M-Series en modo de recopilación de logs con interfaces de 10 GB, debe completar todo este procedimiento de configuración para que las interfaces de 10 GB se muestren como Up (Activada).

STEP 1 | Obtenga la información sobre interfaz y servidor necesaria de su administrador de red.

- Obtenga la dirección IP, la máscara de red (para IPv4) o la longitud del prefijo (para IPv6) y la puerta de enlace predeterminada para cada interfaz que planee configurar (MGT, Eth1, Eth2, Eth3, Eth4, Eth5). Únicamente la interfaz MGT es obligatoria.

  Palo Alto Networks recomienda que especifique todas estas configuraciones para la interfaz MGT. Si omite los valores de algunos de estos ajustes (por ejemplo, la puerta de enlace predeterminada), solo puede acceder a Panorama a través del puerto de la consola para futuros cambios de configuración. No puede compilar la configuración de otras interfaces a menos que especifique todos estos ajustes.

  Si planea utilizar el dispositivo como servidor de gestión de Panorama, Palo Alto Networks recomienda usar la interfaz MGT solo para gestionar Panorama y usar otras interfaces para gestionar dispositivos, recopilar logs, comunicarse con grupos de recopiladores e implementar actualizaciones en los dispositivos (consulte Interfaces de dispositivos M-Series)
- Obtenga las direcciones IP de los servidores DNS.

STEP 2 | Acceda al dispositivo de la serie M desde su ordenador.

1. Conéctese al dispositivo de la serie M de uno de estos modos:
   - Conecte un cable serie desde un ordenador al puerto de la consola del dispositivo de la serie M y conecte usando un software de emulación de terminal (9600-8-N-1).
   - Conecte un cable Ethernet RJ-45 desde un ordenador hasta el puerto de gestión del dispositivo de la serie M. En un navegador, vaya a https://192.168.1.1. Para habilitar el acceso a esta URL tal vez deba cambiar la dirección IP del ordenador por una dirección de la red 192.168.1.0 (por ejemplo, 192.168.1.2).
2. Cuando se le pida, inicie sesión usando el nombre de usuario y contraseña predeterminados (admin/admin). El dispositivo comenzará a iniciarse.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Cambie la contraseña de administrador predeterminada.

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 y revise la* configuración de complejidad de la contraseña*.*

1. Haga clic en el enlace de **admin** en la parte inferior izquierda de la interfaz web.
2. Ingrese las contraseñas **Old Password (Contraseña anterior)**, **New Password (Contraseña nueva)** y **Confirm New Password (Confirmar contraseña nueva)** en los campos correspondientes, y luego haga clic en **OK (Aceptar)**. Almacene la nueva contraseña en un lugar seguro.

*Para garantizar la seguridad de la interfaz de MGT, configure los ajustes de Complejidad mínima de la contraseña (seleccione **Panorama** > **Setup [Configuración]** > **Management [Gestión]**) y especifique el intervalo en el cual los administradores deben cambiar sus contraseñas.*

STEP 4 | Configure las configuraciones de acceso a la red para cada interfaz que usará para gestionar Panorama, gestionar dispositivos, recopilar logs, comunicarse con grupos de recopiladores e implementar actualizaciones en los dispositivos.

Para configurar la conectividad a Panorama con una dirección IP IPv6, debe configurar tanto una IPv4 como una IPv6 para configurar correctamente Panorama con una dirección IP IPv6. Panorama no admite la configuración de la interfaz de gestión con solo una dirección IP IPv6.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces** y haga clic en el nombre de la interfaz.
2. (Solo interfaces que no son MGT) **Enable (Habilitar)**la interfaz.
3. Edite la configuración de acceso a la red de cada interfaz que Panorama utilizará. Únicamente la interfaz MGT es obligatoria. Las interfaces Eth1, Eth2, Eth3, Eth4 y Eth5

 ©2023 Palo Alto Networks, Inc.

son opcionales y solo se aplican si planea utilizar el dispositivo de la serie M como un servidor de gestión de Panorama.

1. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

   IPv4: **Public IP Address (Dirección IP pública)**, **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

   *Si sus cortafuegos se conectan al servidor de gestión de Panorama usando una dirección IP pública que se traduce en una dirección IP privada (NAT), introduzca la dirección IP pública en el campo **Public IP Address (Dirección IP pública)** y la dirección IP privada en el campo **IP Address (Dirección IP)** para enviar ambas direcciones a sus cortafuegos.*

   IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
2. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

   Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo: puede asignar una o más interfaces.

   Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.

   Device Deployment (Implementación de dispositivos) [software y actualizaciones de contenido]: puede asignar solo una interfaz.
3. (Opcional) Seleccione los Servicios de conectividad de red compatibles con la interfaz.

   *(Solo interfaz MGT) Deshabilite **Telnet** y **HTTP**; estos servicios usan texto simple y, por lo tanto, son menos seguros que otros servicios.*
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | Establezca el nombre de host, la zona horaria y la configuración general.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
2. Alinee el reloj de Panorama y de los cortafuegos gestionados para que utilicen la misma **Time Zone (Zona horaria)**, por ejemplo GMT o UTC. Si piensa usar Cortex Data Lake, debe configurar NTP para que Panorama pueda mantenerse sincronizado con Cortex Data Lake.

   El cortafuegos registra marcas de tiempo cuando genera logs y Panorama las registra cuando recibe los logs. La alineación de las zonas horarias garantiza que las marcas de tiempo estén sincronizadas y que el proceso de consulta de los logs y de generación de informes en Panorama sea armónico.
3. Introduzca un **Hostname (Nombre de host)**para el servidor. Panorama lo utilizará como el nombre/etiqueta que se mostrará para el dispositivo. Por ejemplo, este es el nombre que aparecerá en el mensaje de la CLI. También aparecerá en el campo Nombre del recopilador si añade el dispositivo como recopilador gestionado en la página **Panorama** > **Managed Collectors (Recopiladores gestionados)**.
4. (Opcional) Introduzca los valores de **Latitude (Latitud)** y **Longitude (Longitud)** para permitir la colocación precisa del dispositivo M-Series en el mapamundi. El **App Scope** > **Traffic**

 ©2023 Palo Alto Networks, Inc.

Maps (Mapas de tráfico) y el **App Scope** > **Threat Maps (Mapas de amenazas)** usan estos valores.

5. Haga clic en **OK (Aceptar)** para guardar sus entradas.

STEP 6 | Configure los servidores DNS y el servidor de actualizaciones de Palo Alto Networks.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Services (Servicios)** y edite la configuración.
2. Introduzca la dirección IP de su **Primary DNS Server (Servidor DNS principal)** y, de manera opcional, de su **Secondary DNS Server (Servidor DNS secundario)**.
3. Introduzca la dirección estática o URL de **Update Server (Servidor de actualización)** (la predeterminada es updates.paloaltonetworks.com).

   *Seleccione **Verify Update Server Identity (Verificar identidad del servidor de actualización)** si quiere que Panorama verifique que el servidor de actualizaciones desde el que descarga software o paquetes de contenido cuenta con un certificado SSL firmado por una autoridad fiable. Esta opción añade un nivel adicional de seguridad para la comunicación entre el servidor de gestión y el servidor de actualizaciones de Panorama.*

4. Haga clic en **OK (Aceptar)** para guardar sus entradas.

STEP 7 | Confirme sus cambios de configuración.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

*Si planea usar el dispositivo M-Series como un servidor de gestión de Panorama y configuró otras interfaces que no sean MGT, debe asignar esas interfaces a las funciones **Device Log Collection (Recopilación de logs del dispositivo)** o **Collector Group Communication (Comunicación del grupo de recopiladores)** cuando configure un recopilador gestionado. Para que las interfaces funcionen, debe configurar un grupo de recopiladores para el recopilador gestionado y llevar a cabo una compilación del grupo de recopiladores.*

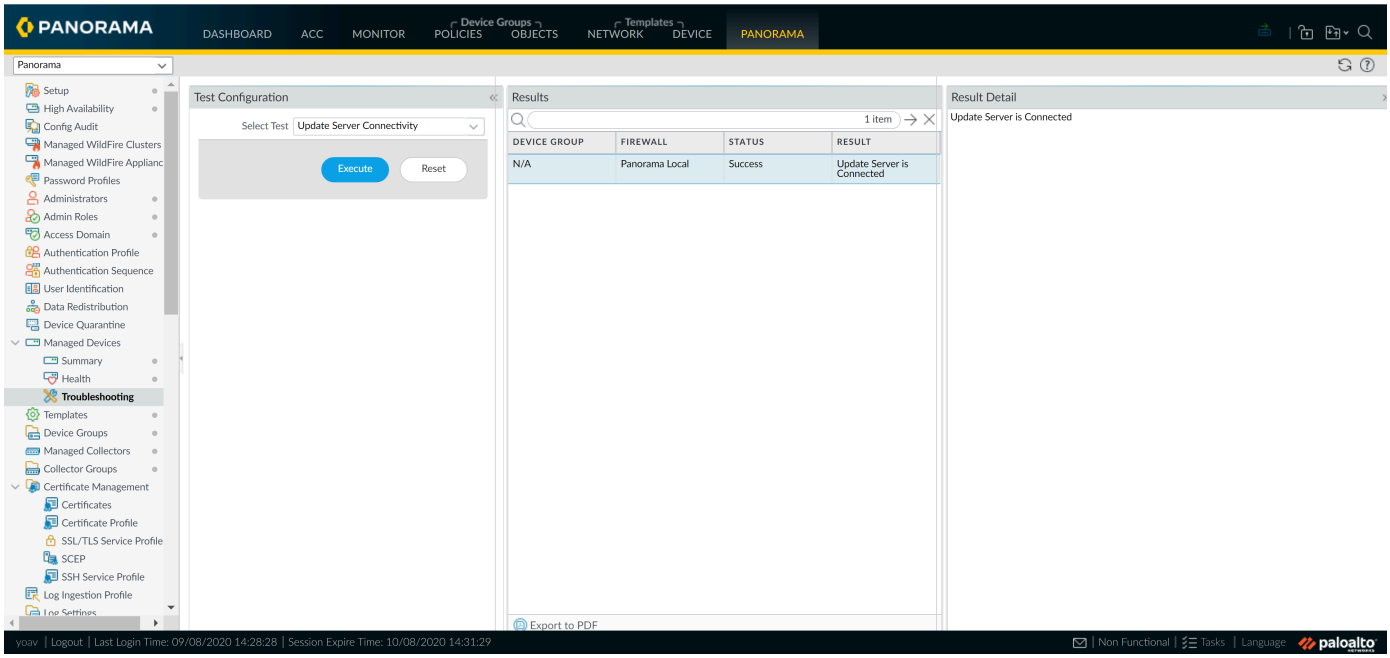
 ©2023 Palo Alto Networks, Inc.

STEP 8 | Verifique el acceso a la red para los servicios externos requeridos para la gestión de Panorama, como el servidor de actualizaciones de Palo Alto Networks.

1. Conéctese al dispositivo de la serie M de uno de estos modos:
   - Conecte un cable serie desde un ordenador hasta el puerto de consola del dispositivo de la serie M. A continuación, utilice un software de emulación de terminal (9600-8-N-1) para conectarse.
   - Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP que especificó para la interfaz de MGT del dispositivo de la serie M durante la configuración inicial.
2. Inicie sesión en la CLI cuando se le solicite. Utilice la cuenta y la contraseña admin predeterminadas que especificó durante la configuración inicial.
3. Para verificar la conectividad de red al servidor de actualizaciones de Palo Alto Networks, realice la prueba que se muestra en el siguiente ejemplo.
   1. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Troubleshooting (Solución de problemas)** y, luego, seleccione **Update Server Connectivity (Conectividad al servidor de actualizaciones)** en el menú desplegable Select Test (Seleccionar prueba).

 ©2023 Palo Alto Networks, Inc.

2. Haga clic en **Execute (Ejecutar)** para comprobar la conectividad al servidor de actualizaciones.



4. Use el siguiente comando de la CLI para recuperar información sobre el derecho a la asistencia técnica para Panorama del servidor de actualizaciones:

```
admin> request support check
```

Si tiene conectividad, el servidor de actualizaciones responde con el estado de asistencia para Panorama. Debido a que Panorama no está registrado, el servidor de actualizaciones brinda el siguiente mensaje:

```
Póngase en contacto con nosotros https://
www.paloaltonetworks.com/company/contact-us.html. Asistencia
 de inicio Https://www.paloaltonetworks.com/support/tabs/
overview.html. Dispositivo no encontrado en este servidor de
 actualización
```

STEP 9 | Pasos siguientes:

1. Registre Panorama e instale las licencias.
2. Instale las actualizaciones de contenido y software de Panorama.

Se recomienda reemplazar el certificado predeterminado que Panorama usa para asegurar el tráfico HTTPS en la interfaz de MGT.

Descripción general de VM-Series

Utilice los siguientes procedimientos para configurar un dispositivo M-Series:

- Configuración de un dispositivo serie M en modo solo de gestión

 ©2023 Palo Alto Networks, Inc.

- Configuración de dispositivo M-Series en modo Panorama
- Configuración de un dispositivo M-Series en modo de recopilador de logs

Configuración de un dispositivo serie M en modo solo de gestión

Configure el servidor de gestión Panorama en el modo Solo gestión para dedicar Panorama a la administración de cortafuegos y recopiladores de logs dedicados. Panorama en el modo Solo gestión no tiene capacidades de recopilación de logs, excepto para la configuración y los logs del sistema, y requiere un recopilador de logs dedicado para almacenar logs.

***Si configuró un** recopilador de logs local**, el recopilador de logs local aún existe en Panorama cuando cambia al modo Solo gestión a pesar de no tener capacidades de recopilación de logs. Cuando se elimina el recopilador de logs local (**Panorama** > **Managed Collectors [Recopiladores gestionados]**) se elimina la configuración de interfaz Eth1/1 que utiliza el recopilador de logs de forma predeterminada. Si decide eliminar el recopilador de logs local, debe** volver a configurar la interfaz Eth1/1**.*

STEP 1 | Monte en rack el dispositivo de la serie M. Consulte la Guía de referencia de hardware del dispositivo serie M para obtener instrucciones.

STEP 2 | Lleve a cabo la configuración inicial del dispositivo de la serie M.

STEP 3 | Registre Panorama e instale las licencias.

STEP 4 | Instale las actualizaciones de contenido y software de Panorama.

STEP 5 | Cambie a modo solo de gestión.

1. Inicio de sesión en la CLI de Panorama.
2. Cambie del modo Panorama al modo solo de gestión:

   ```
   request system system-mode management-only
   ```
3. Ingrese **Y** para confirmar el cambio de modo. El servidor de gestión de Panorama se reinicia. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectarse al servidor de gestión de Panorama para ver la solicitud de inicio de sesión a Panorama.

   Si ve la solicitud `CMS Login`, esto significa que el reinicio del servidor de gestión de Panorama no finalizó. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.
4. Vuelva a iniciar sesión en la CLI.
5. Verifique que el cambio al modo solo de gestión se realizó correctamente:

   ```
   show system info | match system-mode
   ```

   Si el cambio de modo es correcto, se muestra lo siguiente:

   ```
   system mode:management-only
   ```

STEP 6 | Configuración del acceso administrativo a Panorama

STEP 7 | Gestión de cortafuegos

STEP 8 | Gestión de la recopilación de logs

 ©2023 Palo Alto Networks, Inc.

Configuración de dispositivo M-Series en modo Panorama

STEP 1 | Monte en rack el dispositivo de la serie M. Consulte la Guía de referencia de hardware del dispositivo serie M para obtener instrucciones.

STEP 2 | Lleve a cabo la configuración inicial del dispositivo de la serie M.

STEP 3 | Registre Panorama e instale las licencias.

STEP 4 | Instale las actualizaciones de contenido y software de Panorama.

STEP 5 | Configure cada conjunto. Esta tarea es necesaria para que los discos RAID estén disponibles para el logging. De manera opcional, puede añadir discos para Aumentar la capacidad de almacenamiento del dispositivo M-Series).

STEP 6 | Configure el acceso administrativo a Panorama.

STEP 7 | Gestione los cortafuegos.

STEP 8 | Gestione la recopilación de logs.

Configuración de un dispositivo M-Series en modo de recopilador de logs

STEP 1 | Monte en rack el dispositivo de la serie M. Consulte la Guía de referencia de hardware del dispositivo serie M para obtener instrucciones.

STEP 2 | Realización de la configuración inicial del dispositivo de la serie M

STEP 3 | Registro de Panorama e instalación de licencias

STEP 4 | Instalación de actualizaciones de contenido y software de Panorama

STEP 5 | Configure cada conjunto. Esta tarea es necesaria para que los discos RAID estén disponibles para el logging. De manera opcional, puede añadir discos para Aumentar la capacidad de almacenamiento del dispositivo M-Series).

STEP 6 | Configuración del dispositivo M-Series como un recopilador de logs

STEP 7 | Gestión de la recopilación de logs

Configuración del dispositivo M-Series como un recopilador de logs

Si desea un dispositivo dedicado para la recopilación de logs, configure un dispositivo M-200, M-300, M-500, M-600 o M-700 en el modo de recopilador de logs. Para hacerlo, primero debe llevar a cabo la configuración inicial del dispositivo en modo Panorama, que incluye la activación de licencias, la instalación de software y actualizaciones de contenido, y la configuración de la interfaz de gestión (management, MGT). Luego, cambie el dispositivo serie M al modo de recopilación de logs y complete la configuración del recopilador de logs. Además, si desea usar interfaces dedicadas Interfaces de dispositivos M-Series (recomendado) en lugar de la interfaz MGT para la recopilación de logs y la comunicación del grupo de recopiladores, primero debe configurar las interfaces para el servidor de gestión de Panorama, luego configurarlas para el recopilador de logs y luego, llevar a cabo una compilación de Panorama seguida de una compilación del grupo de recopiladores.

 ©2023 Palo Alto Networks, Inc.

Realice los siguientes pasos para configurar un dispositivo de la serie M como un recopilador de logs o convertir un dispositivo existente de la serie M que se implementó previamente como un servidor de gestión de Panorama.

Si está configurando un dispositivo M-Series en modo de recopilación de logs con interfaces de 10 GB, debe completar todo este procedimiento de configuración para que las interfaces de 10 GB se muestren como `Up (Activada)`.

El cambio del dispositivo M-Series del modo Panorama al modo de Recopilador de logs reinicia el dispositivo, elimina el recopilador de logs local, elimina todos los datos de logs existentes y elimina todas las configuraciones excepto los ajustes de acceso de gestión. Si cambia el modo, no se eliminan las licencias ni las actualizaciones de software o contenido.

STEP 1 | Configure el servidor de gestión de Panorama que gestionará el recopilador de logs si ya no lo ha hecho.

Lleve a cabo una de las siguientes tareas:

- Configuración del dispositivo virtual Panorama
- Configuración del dispositivo de la serie M

STEP 2 | Registre la dirección IP de gestión del servidor de gestión de Panorama.

Si implementó Panorama en una configuración de alta disponibilidad (high availability, HA), necesita la dirección IP de cada peer de HA.

1. Inicie sesión en la interfaz web del servidor de gestión de Panorama.
2. Registre el valor en **IP Address (Dirección IP)** del Panorama solitario (no HA) o activo (HA) seleccionando **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y revisando la configuración de Interfaz de gestión.
3. Para una implementación de HA, registre el valor en **Peer HA IP Address (Dirección IP del peer de HA)** del Panorama pasivo seleccionando **Panorama** > **High Availability (Alta disponibilidad)** y revisando la sección Configuración.

STEP 3 | Configure el dispositivo de la serie M que servirá como recopilador de logs dedicado.

Si previamente implementó este dispositivo como servidor de gestión de Panorama, puede omitir este paso porque la interfaz MGT ya está configurada y las licencias y actualizaciones ya están instaladas.

El dispositivo de la serie M en el modo de recopilación de logs no tiene una interfaz web para las tareas de configuración, solo una CLI. Por lo tanto, antes de cambiar el modo en el dispositivo de la serie M, use la interfaz web en modo Panorama para realizar los siguientes pasos:

1. Lleve a cabo la configuración inicial del dispositivo de la serie M.
2. Registre Panorama e instale las licencias.
3. Instale las actualizaciones de contenido y software de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Acceda a la CLI del dispositivo de la serie M.

1. Conéctese al dispositivo de la serie M de uno de estos modos:
   - Conecte un cable serie desde un ordenador hasta el puerto de consola del dispositivo de la serie M. A continuación, utilice el software de emulación de terminal (9600-8-N-1) para conectarse.
   - Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP que especificó para la interfaz de MGT del dispositivo de la serie M durante la configuración inicial.
2. Inicie sesión en la CLI cuando se le solicite. Utilice la cuenta y la contraseña admin predeterminadas que especificó durante la configuración inicial.

STEP 5 | Cambie del modo Panorama al modo de recopilación de logs.

1. Para cambiar al modo de recopilación de logs, introduzca el siguiente comando:

   ```
   > request system system-mode logger
   ```

2. Ingrese **Y** para confirmar el cambio de modo. El dispositivo de la serie M se reiniciará. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectar el dispositivo de la serie M para ver la solicitud de inicio de sesión a Panorama.

   *Si ve la solicitud **CMS Login**, esto significa que el recopilador de logs finalizó el reinicio. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.*

3. Vuelva a iniciar sesión en la CLI.
4. Verifique que el cambio al modo de recopilador de logs se realizó correctamente:

   ```
   > show system info | match system-mode
   ```

   Si el cambio de modo es correcto, se muestra lo siguiente:

   ```
   system-mode: logger
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Configure los discos de creación de logs como pares RAID1.

Si previamente implementó el dispositivo como servidor de gestión de Panorama, puede omitir este paso porque los pares de discos ya están configurados y disponibles.

El tiempo necesario para copiar las unidades puede variar entre algunos minutos a horas según la cantidad de datos almacenados en las unidades.

1. Determine cuáles pares de discos están presentes para configurar como pares de RAID en el dispositivo de la serie M:

   ```
   > show system raid detail
   ```

   Lleve a cabo los pasos restantes para configurar cada par de disco que tiene discos `present`. Este ejemplo usa el par de discos A1/A2.
2. Para añadir el primer disco del par, introduzca el siguiente comando e ingrese **y** cuando se le indique para confirmar la solicitud:

   ```
   > request system raid add A1
   ```

   Espere que el proceso finalice antes para añadir el siguiente disco del par. Para supervisar el progreso de la configuración RAID, vuelva a introducir el siguiente comando:

   ```
   > show system raid detail
   ```

   Después de que termine el proceso del primer disco, el resultado muestra el estado del par de discos como `Available` pero `degraded`.
3. Añada el segundo disco del par:

   ```
   > request system raid add A2
   ```
4. Verifique que la configuración del disco está completa:

   ```
   > show system raid detail
   ```

   Después de que termine el proceso del segundo disco, el resultado muestra el estado del par de discos como `Disponible` y `Correcto`:

   ```
   Disk Pair A      Available Status        clean
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Habilite la conectividad entre el recopilador de logs y el servidor de gestión de Panorama.

Introduzca los siguientes comandos en la CLI del recopilador de logs, donde ***<IPaddress1>*** es para la interfaz de MGT del Panorama solitario (no HA) o activo (HA) y ***<IPaddress2>*** es para la interfaz de MGT del Panorama pasivo (HA), si corresponde.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 8 | Registro del número de serie del recopilador de logs.

Necesitará el número de serie para añadir el recopilador de logs como recopilador gestionado en el servidor de gestión de Panorama.

1. En la CLI del recopilador de logs, introduzca el siguiente comando para mostrar su número de serie:

   ```
   > show system info | match serial
   ```

2. Registre el número de serie.

STEP 9 | Añada el recopilador de logs como recopilador gestionado en el servidor de gestión de Panorama.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir un recopilador gestionado.
2. En la configuración **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el recopilador de logs.
3. En el campo **Panorama Server IP (IP del servidor de Panorama)**, introduzca la dirección IP o el FQDN del Panorama solitario (no HA) o activo (HA). Para una implementación de HA, introduzca la dirección IP o el FQDN del peer pasivo de Panorama en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)**.

   Estas direcciones IP deben especificar una interfaz Panorama que tenga servicios **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo** habilitados. De forma predeterminada, estos servicios solo están disponibles en la interfaz MGT. Sin embargo, es posible que haya habilitado los servicios en otras interfaces cuando realizó la Configuración del dispositivo M-Series que es un servidor de gestión de Panorama.

 ©2023 Palo Alto Networks, Inc.

4. Seleccione **Interfaces**, haga clic en **Management (Gestión)** y configure uno o ambos de los conjuntos de campo siguientes para la interfaz de MGT, según los protocolos IP de su red.
   - IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
5. Haga clic en **OK (Aceptar)** dos veces para guardar los cambios en el recopilador de logs.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

   Este paso es necesario para que pueda habilitar los discos de creación de logs.
7. Verifique que **Panorama** > **Managed Collectors (Recopiladores gestionados)** muestre en la lista el recopilador de logs que añadió. La columna Conectado muestra un icono de marca de verificación para indicar que el recopilador de logs está conectado a Panorama. Es posible que deba esperar unos minutos para que la página muestre el estado de conexión actualizado.

   En este punto, la columna Estado de configuración muestra Out of Sync y la columna Estado de tiempo de ejecución muestra disconnected (desconectado). El estado cambiará a In Sync (sincronizado) y connected (conectado) después de que configure un grupo de recopiladores (Paso Asigne el recopilador de logs a un grupo de recopiladores*).*

STEP 10 | Habilite los discos de registro.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada par de discos RAID.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 11 | (Recomendado) Configure las interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** y **Ethernet5** si el servidor de gestión de Panorama y recopilador de logs los usará para la **Device Log Collection (Recopilación de logs del dispositivo)** [recepción de logs del cortafuegos] y **Collector Group Communication (Comunicación del grupo de recopiladores)**.

Si desplegó previamente el recopilador de logs como un servidor de gestión de Panorama y configuró estas interfaces, debe reconfigurarlas porque al cambiar al modo Recopilador de

 ©2023 Palo Alto Networks, Inc.

logs (Cambio del modo Panorama al modo de recopilación de logs) habría borrado todas las configuraciones excepto la configuración de acceso a gestión.

1. Configure cada interfaz en el servidor de gestión de Panorama (que no sea la interfaz MGT) si aún no lo ha hecho:
   1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces** y haga clic en el nombre de la interfaz.
   2. Seleccione ***<interface-name>*** para habilitar la interfaz.
   3. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

      IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

      IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
   4. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

      Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo: puede asignar una o más interfaces.

      Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.

      Device Deployment (Implementación de dispositivos) [software y actualizaciones de contenido]: puede asignar solo una interfaz.
   5. Haga clic en **OK (Aceptar)** para guardar los cambios.
2. Configure cada interfaz en el recopilador de logs (que no sea la interfaz MGT):
   1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
   2. Seleccione **Interfaces** y haga clic en el nombre de la infertfaz.
   3. Seleccione ***<interface-name>*** para habilitar la interfaz.
   4. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

      IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

      IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
   5. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

      Device Log Collection (Recopilación de logs del dispositivo): puede asignar una o más interfaces.

      Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.
   6. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.

 ©2023 Palo Alto Networks, Inc.

4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 12 | (Opcional) Si su implementación utiliza certificados personalizados para la autenticación entre Panorama y los dispositivos gestionados, implemente el certificado de dispositivo cliente personalizado. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y elija el perfil del certificado del menú desplegable o haga clic en **New Certificate Profile (Nuevo perfil de certificado)** para crear uno.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)** para un recopilador de logs.
3. Seleccione la casilla de verificación **Secure Client Communication (Comunicación de cliente segura)**.
4. Seleccione el tipo de certificado de dispositivo en el menú desplegable Tipo.
   - Si está utilizando un certificado de dispositivo local, seleccione **Certificate (Certificado)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
   - Si está utilizando SCEP como certificado del dispositivo, seleccione el **SCEP Profile (Perfil de SCEP)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
5. Haga clic en **OK (Aceptar)**.

STEP 13 | (Opcional) Configure Secure Server Communication (Comunicación de servidor segura) en un recopilador de logs. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)**.
2. Verifique que la casilla de verificación **Custom Certificate Only (Certificado personalizado únicamente)** no está seleccionada. Esto le permite continuar gestionando todos los dispositivos mientras migra a certificados personalizados.

   Cuando se selecciona la casilla de verificación Certificado personalizado únicamente, el Recopilador de logs no se autentica y no puede recibir logs de dispositivos que usan certificados predefinidos.
3. Seleccione el perfil del servicio SSL/TLS del menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre el recopilador de logs y los dispositivos que le envían los logs.
4. Seleccione el perfil de certificado del menú desplegable **Certificate Profile (Perfil del certificado)**.
5. Seleccione **Authorize Client Based on Serial Number (Autorizar clientes según el número de serie)** para hacer que el servidor compruebe los clientes contra los números de serie de los dispositivos gestionados. El certificado de cliente debe tener la palabra clave especial $UDID establecida como CN para autorizar según los números de serie.
6. En **Disconnect Wait Time (min) (Tiempo de espera para desconexión [min])**, introduzca los minutos que debe esperar Panorama antes de interrumpir y restablecer la conexión con

 ©2023 Palo Alto Networks, Inc.

los dispositivos que gestiona. Este campo está en blanco por defecto y el rango es de 0 a 44,640 minutos.

El tiempo de espera de desconexión no comienza la cuenta atrás hasta que confirme la nueva configuración.

7. (Opcional) Configure una lista de autorizaciones.
   1. Haga clic en **Add (Añadir)** en lista de autorizaciones.
   2. Seleccione el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** como el tipo de Identificador.
   3. Introduzca un identificador del tipo seleccionado.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Check Authorization List (Comprobar lista de autorización)** para hacer cumplir la lista de autorizaciones.
8. Haga clic en **OK (Aceptar)**.
9. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 14 | Asigne el recopilador de logs a un grupo de recopiladores.

1. Configure un grupo de recopiladores. Debe llevar a cabo una compilación de Panorama y luego una del grupo de recopiladores para sincronizar la configuración del recopilador de logs con Panorama y colocar las interfaces Eth1, Eth2, Eth3, Eth4 y Eth5 (si las configuró) en un estado operativo en el recopilador de logs.

   Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.

   *Se recomienda **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si añade varios recopiladores de logs a un solo grupo de recopiladores. Esta opción requiere que cada recopilador de logs tenga el mismo número de discos de creación de logs.*

2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que la configuración del recopilador de logs se sincronizó con Panorama.

   La columna Estado de configuración debe mostrar In Sync (Sincronizado) y la columna Estado de tiempo de ejecución muestra connected (conectado).

3. Acceda a la CLI del recopilador de logs e ingrese el siguiente comando para verificar que sus interfaces son funcionales:

   ```
   > show interface all
   ```

   El resultado muestra `state` como `up` para cada interfaz que sea funcional.

4. Si el grupo tiene varios recopiladores de logs, consulte Solución de problemas de conectividad a recursos de red, para verificar que se pueden comunicar entre sí, ejecute una prueba de conectividad con ping en todas las interfaces que emplean los recopiladores. En la dirección IP de `source (origen)`, especifique la interfaz de uno de

 ©2023 Palo Alto Networks, Inc.

los recopiladores de logs. Para la dirección IP `host`, especifique la interfaz de coincidencia de otro recopilador de logs en el mismo grupo de recopiladores.

STEP 15 | Pasos siguientes:

Para permitir que el recopilador de logs reciba logs del cortafuegos:

1. Configure el reenvío de logs a Panorama.
2. Verifique el reenvío de logs a Panorama.

Aumento de la capacidad de almacenamiento en el dispositivo M-Series

Después de Realizar la configuración inicial del dispositivo M-Series, puede aumentar la capacidad de almacenamiento de logs del dispositivo actualizando las unidades existentes a unidades de mayor capacidad o instalando unidades pares adicionales en bahías de unidades vacías. Por ejemplo, usted puede optar por actualizar las unidades existentes de 1 TB a 2 TB en un dispositivo M-500, o puede añadir unidades de 2 TB a las bahías de unidades vacías (de B1 a D2).

Los dispositivos M-series aprovechan RAID 1 para redundancia de datos en caso de fallo del disco. Por lo tanto, el par de unidades en un conjunto RAID 1 debe ser idéntico. Sin embargo, puede mezclar capacidades de unidad en diferentes matrices de RAID 1. Por ejemplo, las unidades en la matriz A1/A2 RAID 1 pueden ser unidades de 1TB y las unidades en la matriz B1/B2 RAID 1 pueden ser unidades de 2TB.

La siguiente tabla enumera la cantidad máxima de bahías de unidad (discos) y las capacidades de unidades de disco disponibles admitidas en los dispositivos M-series.

Debido a que cada par de unidades (A1/A2, por ejemplo) está en una matriz RAID 1, la capacidad total de almacenamiento es la mitad del total de unidades instaladas. Por ejemplo, si un dispositivo M-500 tiene unidades de 2 TB instaladas en bahías de unidades A1/A2 y B1/B2, la matriz A1/A2 proporciona 2 TB de almacenamiento total y la matriz B1/B2 proporciona otros 2 TB para un total de 4 TB.

Aparato	Número de bahías de unidades (discos) admitidas	Capacidad de unidades admitidas
Dispositivo M-200	4	8TB
Dispositivo M-300	4	8TB
Dispositivo M-500	24	1 TB/2 TB
Dispositivo M-600	12	8TB

 ©2023 Palo Alto Networks, Inc.

Aparato	Número de bahías de unidades (discos) admitidas	Capacidad de unidades admitidas
Dispositivo M-700	12	8TB

Antes de ampliar la capacidad de almacenamiento de logs, determine los requisitos previos de almacenamiento de logs de Panorama. Si necesita más almacenamiento de logs de lo que admite un solo dispositivo de la serie M, puede añadir recopiladores de logs dedicados (consulte Configuración de un recopilador gestionado) o puede configurar el reenvío de logs de Panorama a destinos externos.

*No es necesario que desconecte el dispositivo M-series para ampliar el almacenamiento cuando añade unidades a un dispositivo M-series que ya está implementado. Cuando las unidades adicionales estén disponibles y se puedan configurar, el dispositivo de la serie M redistribuirá los logs entre las unidades disponibles. El proceso de redistribución de logs se produce en segundo plano y no tiene influencia en el tiempo de actividad o la disponibilidad del dispositivo de la serie M Sin embargo, el proceso no disminuye la tasa de creación de logs máxima. La columna Estado de redistribución (**Panorama > Collector Groups [Grupos de recopiladores]**) indica el estado de finalización del proceso como un porcentaje.*

- Cómo añadir unidades a un dispositivo de la serie M
- Actualización de unidades en un dispositivo M-Series

Cómo añadir unidades a un dispositivo de la serie M

STEP 1 | Instale las nuevas unidades de disco en las bahías de unidades adecuadas.

Asegúrese de añadir unidades secuencialmente en las siguientes ranuras de la bahía de discos abiertas. Por ejemplo, añada unidades a B1 y B2 antes de añadir unidades a C1 y C2.

STEP 2 | Acceda a la Interfaz de línea de comandos (command line interface, CLI) en el dispositivo de la serie M.

Conéctese al dispositivo M-Series de uno de estos modos:

- Conecte un cable serie desde su ordenador al puerto de la consola y conecte el dispositivo de la serie M usando el software de emulación de terminal (9600-8-N-1).
- Use un software de emulación de terminal (como PuTTY) para abrir una sesión de shell seguro (Secure Shell, SSH) en la dirección IP del dispositivo M-Series.

STEP 3 | Cuando se le indique, inicie sesión en el dispositivo.

Utilice la cuenta de administrador predeterminada y la contraseña asignada.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure todos los conjuntos.

> *El tiempo necesario para reflejar los datos en la unidad puede variar entre algunos minutos, unas pocas horas o más de un día dependiendo de la cantidad de datos almacenados en la unidad.*

El siguiente ejemplo utiliza las unidades de las bahías B1 y B2.

1. Introduzca los siguientes comandos y confirme la solicitud cuando se le indique:

```
> request system raid add B1 > request system raid add B2
```

2. Para supervisar el progreso de la configuración RAID, introduzca el siguiente comando:

```
> show system raid detail
```

Cuando la configuración de RAID finalice, aparece la siguiente respuesta:

```
Disk Pair A       Available Status          clean Disk
 id A1     Present model : ST91000640NS size : 953869 MB
 status : active sync Disk id A2     Present        model :
 ST91000640NS size : 953869 MB status : active sync Disk
 Pair B        Available Status          clean Disk id
 B1      Present model : ST91000640NS size : 953869 MB
 status : active sync Disk id B2     Present        model :
 ST91000640NS size : 953869 MB status : active sync
```

STEP 5 | Haga que la matriz esté disponible para la realización de logs.

Para habilitar la matriz para la creación de logs, primero debe añadir el dispositivo como recopilador gestionado en Panorama. Si aún no lo añadió, consulte Configuración de un recopilador gestionado.

1. Inicie sesión en la interfaz web del servidor de gestión de Panorama que gestiona este Recopilador de logs.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
3. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada matriz.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.
6. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**, seleccione el grupo de recopiladores y haga clic en **Push (Enviar)** para enviar los cambios.

Actualización de unidades en un dispositivo M-Series

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Acceda a la Interfaz de línea de comandos (command line interface, CLI) en el dispositivo de la serie M.

Conéctese al dispositivo M-Series de uno de estos modos:

- Conecte un cable serie desde su ordenador al puerto de la consola y conecte el dispositivo de la serie M usando el software de emulación de terminal (9600-8-N-1).
- Use un software de emulación de terminal (como PuTTY) para abrir una sesión de shell seguro (Secure Shell, SSH) en la dirección IP del dispositivo M-Series.

STEP 2 | Cuando se le indique, inicie sesión en el dispositivo.

Utilice la cuenta de administrador predeterminada y la contraseña asignada.

STEP 3 | Verifique que el estado de RAID 1 para las unidades instaladas muestre que hay al menos dos conjuntos de RAID 1 en funcionamiento. Durante la actualización, actualizará un conjunto de RAID 1 a la vez y debe haber al menos otro conjunto de RAID 1 disponible en el dispositivo. El dispositivo mostrará un error de interrupción si intenta quitar el único conjunto en funcionamiento de la configuración.

Introduzca el siguiente comando para ver el estado de RAID:

```
> show system raid detail
```

Por ejemplo, lo siguiente muestra un resultado de un dispositivo M-500 con dos conjuntos disponibles (Par de disco A y Par de disco B). Si solo existe una matriz disponible, debe añadir una segunda matriz como se describe en Cómo añadir unidades adicionales a un dispositivo de la serie M antes de actualizar las unidades.

```
Disk Pair A                                Available
 Status                                      clean Disk id
 A1                                Present model        :
 ST91000640NS size          : 953869 MB status       :
 active sync Disk id A2 Present model        : ST91000640NS
 size          : 953869 MB status       : active sync
 Disk Pair B                                Available
 Status                                      clean Disk id
 B1                                Present model        : ST91000640NS
 size          : 953869 MB status       : active sync Disk id
 B2                                Present model        : ST91000640NS
 size          : 953869 MB status       : active sync
```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Quite la primera unidad de 1 TB y reemplácela por una unidad de 2 TB.

1. Para quitar la primera unidad de la configuración del conjunto de RAID 1 (A1 en este ejemplo), introduzca el siguiente comando e introduzca **y** cuando se le indique para confirmar la solicitud:

   ```
   > request system raid remove A1
   ```

2. Retire físicamente la primera unidad de la bahía de unidades. Presione el botón eyector del soporte de unidades en la bahía de unidades A1 para liberar la palanca de este. Luego tire de la palanca hacia usted y deslice la unidad hacia afuera del dispositivo.
3. Quite una unidad de 2 TB de su empaquetado y colóquela en una mesa junto a la unidad que acaba de quitar. Observe cómo está instalada la unidad en el soporte porque deberá instalar la unidad de 2 TB en este mismo soporte.
4. Quite los cuatro tornillos que sostienen la unidad de 1 TB y quite la unidad del soporte.
5. Coloque la unidad de 2 TB en el soporte con los mismos cuatro tornillos que quitó de la unidad de 1 TB y luego vuelva a insertar el soporte con la unidad de 2 TB en la bahía de unidades A1.
6. Introduzca el siguiente comando para comprobar que la unidad de 2 TB se reconoce:

   ```
   show system raid detail
   ```

   Verifique que el disco A1 muestre el modelo y el tamaño correctos (aproximadamente 2 TB). Si el modelo y el tamaño no son correctos, vuelva a ejecutar el comando anterior hasta que se muestren el modelo y el tamaño correctos.

   Si el modelo y el tamaño incorrectos se muestran consistentemente, introduzca el siguiente comando:

   ```
   request system raid remove A1
   ```

   Espere 30 segundos una vez que ejecute el comando anterior, luego retire el disco y vuelva a insertarlo y repita el comando **show system raid detail** para verificar el tamaño y el modelo.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Copie los datos de la unidad de 1 TB instalada en el conjunto de RAID 1 a la unidad de 2 TB recientemente instalada en ese conjunto.

El tiempo necesario para copiar los datos puede variar entre algunos minutos a horas según la cantidad de datos almacenados en la unidad.

1. Para copiar los datos de la unidad de 1 TB en la bahía de unidades A2 a la unidad de 2 TB recientemente instalada en la bahía de unidades A1, introduzca el siguiente comando e ingrese **y** cuando se le solicite:

```
> request system raid copy from A2 to A1
```

2. Para ver el estado del proceso de copia, ejecute el siguiente comando:

```
> show system raid detail
```

Continúe ejecutando este comando para ver el resultado detallado de RAID hasta que vea que el conjunto (A1/A2 en este ejemplo) se muestra como `Available`

En este punto, la unidad A2 mostrará `not in use` porque existe una discrepancia de tamaño de la unidad.

STEP 6 | Actualice la segunda unidad del conjunto RAID 1 a una unidad de 2 TB.

1. Quite la segunda unidad de 1 TB (de la bahía de unidades A2 en este ejemplo) de la configuración del conjunto de RAID 1:

```
> request system raid remove A2
```

2. Inserte el soporte con la unidad de 2 TB recientemente agregada en la bahía de unidades A2 y añádala en la configuración del conjunto de RAID 1:

```
> request system raid add A2
```

El sistema copiará los datos de A2 a A1 para reflejar las unidades.

3. Para ver el estado del proceso de copia, ejecute el siguiente comando:

```
> show system raid detail
```

Continúe viendo el resultado detallado de RAID hasta que vea que el conjunto (A1/A2 en este ejemplo) muestra l`Available` y ambos discos muestran `active sync`.

```
Disk Pair A       Available Status         clean Disk id A1
     Present        model        : ST2000NX0253 size         :
 1907138 MB status       : active sync Disk id A2     Present
        model        : ST2000NX0253 size         : 1907138 MB
 status       : active sync
```

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Actualice las unidades para conjuntos RAID 1 adicionales según sea necesario.

Para actualizar conjuntos de RAID 1 adicionales a unidades de 2 TB, repita este procedimiento reemplazando los indicadores de unidades según corresponda. Por ejemplo, reemplace A1 con B1 y A2 con B2 para actualizar las unidades en el conjunto B1/B2 RAID 1.

Configuración de Panorama para usar varias interfaces

En una red a gran escala, puede mejorar la seguridad y reducir la congestión implementando la segmentación de la red, lo que implica segregar las subredes según la utilización de los recursos, las funciones de los usuarios y los requisitos de seguridad. Panorama admite la segmentación de red al permitirle usar múltiples Interfaces del dispositivo M-Series para gestionar dispositivos (cortafuegos, Recopiladores de logs y dispositivos y clústeres de dispositivos de WildFire) y recopilar logs; puede asignar interfaces separadas a los dispositivos en subredes diferentes.

La utilización de múltiples interfaces para recopilar logs también proporciona las ventajas del equilibrio de carga, que es particularmente útil en entornos donde los cortafuegos reenvían grandes volúmenes de logs a los recopiladores de logs. Si habilita la configuración de **reenvío a todos los recopiladores de logs** en la lista de preferencias de reenvío de logs del grupo de recopiladores, los logs se envían en todas las interfaces configuradas. De lo contrario, los logs se reenvían a través de una única interfaz y, si esa interfaz deja de funcionar, el reenvío de logs continúa en la siguiente interfaz configurada. Por ejemplo, configura Eth1/1, Eth1/2 y Eth1/3 para el reenvío de logs. En caso de que la interfaz Eth1/1 se caiga, el reenvío de logs continúa a través de Eth1/2.

Debido a que los administradores acceden y gestionan Panorama a través de la interfaz MGT, asegurar esa interfaz es especialmente importante. Un método para mejorar la seguridad de la interfaz MGT es descargar los servicios de Panorama a otras interfaces. Además de la gestión de dispositivos y la recopilación de logs, también puede descargar la comunicación del Grupo de recopiladores y la implementación del software y las actualizaciones de contenido en los cortafuegos, recopiladores de logs y dispositivos y clústeres de dispositivos de WildFire. Al descargar estos servicios, puede reservar la interfaz MGT para el tráfico administrativo y asignarla a una subred segura que se segrega de las subredes donde residen sus cortafuegos, recopiladores de logs y dispositivos y clústeres de dispositivos de WildFire.

- Múltiples interfaces para la segmentación de red Ejemplo
- Configuración de Panorama para la segmentación de red

Múltiples interfaces para la segmentación de red Ejemplo

Figure 1 ilustra una implementación que usa varias interfaces en dispositivos M-500 en modo Panorama y en modo Recopilador de logs. En este ejemplo, las interfaces admiten la segmentación de red de la siguiente forma:

- **Red de gestión de Panorama**: para proteger la interfaz web de Panorama, la CLI y la API XML del acceso no autorizado, la interfaz de MGT en Panorama se conecta a una subred a la que solo pueden acceder los administradores.
- **Internet**: Panorama usa la interfaz MGT para comunicarse con servicios externos como el servidor de actualizaciones de Palo Alto Networks.
- **Puerta de enlace perimetral** y **Centro de datos**: Panorama usa un par de interfaces separadas para gestionar los cortafuegos y Recopiladores de logs en cada una de estas subredes. La gestión de cortafuegos generalmente genera menos tráfico que la consulta de Recopiladores de logs para obtener información de informes. Por lo tanto, Panorama utiliza interfaces de 1 Gbps (Eth1 y

 ©2023 Palo Alto Networks, Inc.

Eth2) para gestionar los cortafuegos y utiliza interfaces de 10 Gbps (Eth4 y Eth5) para consultar y gestionar los Recopiladores de logs. Cada recopilador de logs usa su interfaz MGT para responder a las consultas, pero usa sus interfaces Eth4 y Eth5 para el tráfico más intenso asociado con la recopilación de logs de los cortafuegos.

- **Actualizaciones de software y contenidos**: los cortafuegos y los Recopiladores de logs en ambas subredes recuperan actualizaciones de software y de contenido a través de la interfaz Eth3 en Panorama.

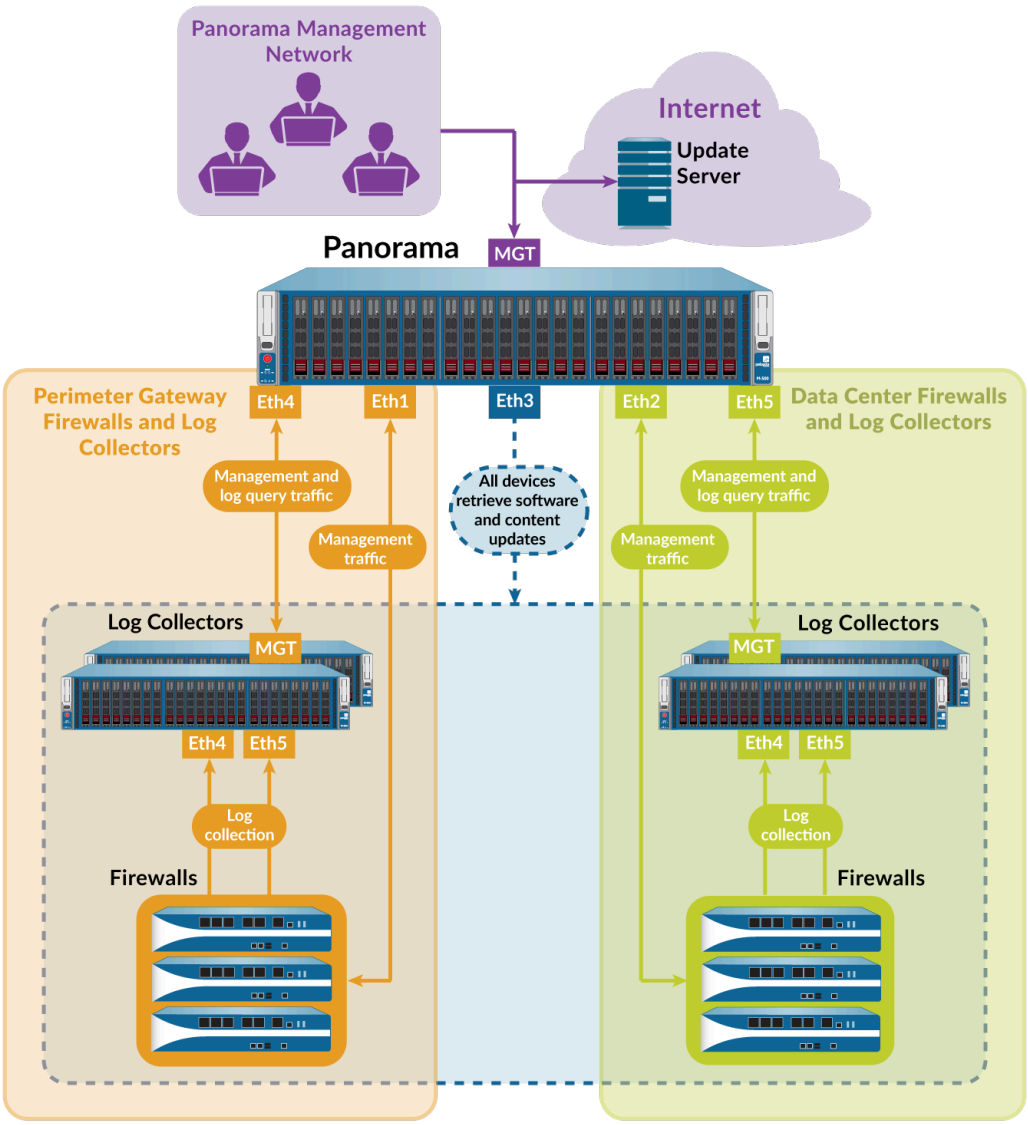


Figure 9: Varias interfaces de Panorama

Configuración de Panorama para la segmentación de red

Para descargar los servicios Panorama desde la interfaz MGT a otras interfaces, comience configurando las interfaces en el servidor de gestión de Panorama. Si su red tiene mucho tráfico de logs, recuerde que las interfaces Eth4 y Eth5 de los dispositivos M-500, M-600 y M-700 admiten un mayor rendimiento (10 Gbps) que las otras interfaces (1 Gbps). Luego configure los recopiladores de logs en cada subred para conectarse con interfaces específicas en Panorama. Para cada Recopilador de logs, también selecciona una interfaz para la comunicación del grupo de recopiladores y una o

 ©2023 Palo Alto Networks, Inc.

más interfaces para recopilar logs de los cortafuegos. Por último, configure los recopiladores en cada subred para conectarse con interfaces en Panorama.

Si está configurando un dispositivo M-Series en modo de recopilación de logs con interfaces de 10 GB, debe completar todo este procedimiento de configuración para que las interfaces de 10 GB se muestren como Up (`Activada`).

Palo Alto Networks recomienda especificar la dirección IP, la máscara de red (para IPv4) o la longitud de prefijo (para IPv6), y la puerta de enlace predeterminada para la interfaz MGT. Si omite uno de estos ajustes (por ejemplo, la puerta de enlace predeterminada), puede acceder al dispositivo M-Series solo a través del puerto de la consola para futuros cambios de configuración.

Siga estos pasos para configurar Panorama y los recopiladores de logs dedicados para usar múltiples interfaces:

STEP 1 | Verifique que los dispositivos Panorama y los cortafuegos admiten varias interfaces y disponen de las versiones de software y las configuraciones imprescindibles.

- Los dispositivos M-Series deben ejecutar Panorama 8.0 o posterior para utilizar una interfaz independiente para implementar actualizaciones y para usar múltiples interfaces para la gestión de dispositivos y la recopilación de logs. Los dispositivos M-200 y M-600 deben ejecutar Panorama 8.1 o posterior, mientras que los M-300 y M-700 deben correr en Panorama 10.2 o posterior. Los dispositivos Panorama implementados en ESXi, vCloud, Air, Hyper-V y KVM deben ejecutar Panorama 8.1 o versiones posteriores.
- Si ha implementado Panorama o un recopilador de logs como dispositivo virtual, compruebe las interfaces compatibles con el dispositivo virtual de Panorama.
- Los dispositivos M-Series deben ejecutar Panorama 6.1 o posterior para usar interfaces independientes para la recopilación de logs o la comunicación del grupo de recopiladores.
- La configuración inicial de cada servidor de gestión de Panorama se ha completado. Esto incluye la configuración de la interfaz MGT.

  Para configurar una dirección IP IPv6 para la interfaz MGT de Panorama, debe configurar tanto una IPv4 como una IPv6 para configurar correctamente Panorama con una dirección IP IPv6. Panorama no admite la configuración de la interfaz MGT con solo una dirección IP IPv6.
- Se configuran Recopiladores de logs y Grupos de recopiladores. Esto incluye la configuración de la interfaz MGT en los recopiladores de logs.

  Para configurar una dirección IP IPv6 para la interfaz MGT de un recopilador de logs, debe configurar tanto una IPv4 como una IPv6 para configurar correctamente Panorama con una dirección IP IPv6. Panorama no admite la configuración de la interfaz MGT con solo una dirección IP IPv6.
- La configuración inicial de los cortafuegos se ha completado, ha añadido los cortafuegos a Panorama como dispositivos gestionados, y los cortafuegos en cada subred se han asignado a una plantilla separada.
- La configuración inicial de los dispositivos WildFire se ha completado y usted ha añadido dispositivos WildFire a Panorama como dispositivos gestionados.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configure las interfaces en el servidor de gestión de Panorama solitario (no HA) o activo (HA).



Debido a que la interfaz MGT se configuró durante la configuración inicial de Panorama, no tiene que configurarla nuevamente.

Lleve a cabo estos pasos para cada interfaz:

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama solitario (no HA) o activo (HA).
2. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces (Interfaces)**.
3. Haga clic en un Interface Name (Nombre de interfaz) para editar la interfaz.
4. Seleccione ***<interface-name>*** para habilitar la interfaz.
5. Configure uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:
   - IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
6. Seleccione los servicios compatibles con la interfaz.
   - **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo)**: administre cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire, recopile los logs generados por los recopiladores de logs y consulte los recopiladores de logs para obtener información de informes. Para admitir una red segmentada, puede habilitar estos servicios en varias interfaces.
   - **Collector Group Communication (Comunicación del grupo de recopiladores)**: comuníquese con los grupos de recopiladores que Panorama gestiona en todas las subredes.
   - **Device Deployment (Implementación del dispositivo)**: implemente actualizaciones de software y contenido para cortafuegos gestionados, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire en todas las subredes.
7. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
8. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para confirmar los cambios.
9. Haga clic en **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** para enviar los cambios al grupo que contiene los recopiladores de logs modificados.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | (HA únicamente) Configure las interfaces del servidor de gestión de Panorama pasivo.

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama activo.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y elija el peer de HA pasivo.
3. Seleccione **Interfaces** y haga clic en una interfaz para editarla.
4. Haga clic en la casilla de verificación **Enable Interface (Habilitar interfaz)** para habilitar la interfaz.
5. Configure uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:
   - IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
6. Seleccione los servicios compatibles con la interfaz.
   - **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo)**: administre cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire, recopile los logs generados por los recopiladores de logs y consulte los recopiladores de logs para obtener información de informes. Para admitir una red segmentada, puede habilitar estos servicios en varias interfaces.
   - **Collector Group Communication (Comunicación del grupo de recopiladores)**: comuníquese con los grupos de recopiladores que Panorama gestiona en todas las subredes.
   - **Device Deployment (Implementación del dispositivo)**: implemente actualizaciones de software y contenido para cortafuegos gestionados, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire en todas las subredes.
7. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
8. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar los cambios en Panorama y enviarlos a los grupos de recopiladores con el peer de HA pasivo que modificó.

STEP 4 | Configure cada Recopilador de logs para conectarse con una interfaz de Panorama.

Para admitir una red segmentada, puede conectar los recopiladores de logs en cada subred interfaces de Panorama separadas. Las interfaces deben tener habilitado la **Device Management**

 ©2023 Palo Alto Networks, Inc.

and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo), como se describe en el paso anterior.

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama solitario (no HA) o activo (HA).
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
3. En el campo **Panorama Server IP (IP del servidor de Panorama)**, introduzca la dirección IP de una interfaz en Panorama solitario (no HA) o activo (HA).
4. (Solo HA) En el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)**, introduzca la dirección IP de una interfaz en el Panorama pasivo que será compatible con **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo)** si se produce una conmutación por error en el Panorama activo.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.
6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar los cambios en Panorama y para enviar los cambios a los grupos de recopiladores con los recopiladores de logs que modificó.
7. Lleve a cabo los siguientes pasos en cada recopilador de logs dedicado:
   1. Acceda a la CLI de Recopilador de logs utilizando un software de emulación como PuTTY para abrir una sesión SSH en el Recopilador de logs utilizando la dirección IP de su interfaz MGT. Cuando se le solicite, inicie sesión utilizando las credenciales del administrador de Panorama.
   2. Ejecute los siguientes comandos, donde ***<IPaddress1>*** es para el servidor de gestión de Panorama solitario (no HA) o activo (HA) y ***<IPaddress2>*** es para el servidor de gestión de Panorama pasivo (si corresponde).

```
> configure # set deviceconfig system panorama-
server <IPaddress1> panorama-server-2 <IPaddress2> # commit
```

 ©2023 Palo Alto Networks, Inc.

STEP 5 | (Solo HA) Configure una interfaz en el servidor de gestión de Panorama pasivo para implementar actualizaciones en caso de que el Panorama activo falle.

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama pasivo.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces (Interfaces)**.
3. Haga clic en un Interface Name (Nombre de interfaz) para editar la interfaz.
4. Seleccione ***<interface-name>*** para habilitar la interfaz.
5. Configure uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:
   - IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
6. Seleccione **Device Deployment (Implementación del dispositivo)**.
7. Haga clic en **OK (Aceptar)** para guardar los cambios.
8. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para confirmar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Configure las interfaces que usarán los recopiladores de logs para recopilar logs de los cortafuegos y comunicarse con otros recopiladores de logs.

Debido a que la interfaz MGT se configuró durante la configuración inicial de los recopiladores de logs, no es necesario configurarla nuevamente.

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama solitario (no HA) o activo (HA).
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
3. Seleccione **Interfaces** y realice los siguientes pasos para cada interfaz:
   1. Haga clic en el nombre de una interfaz para editarla.
   2. Seleccione *<interface-name>* para habilitar la interfaz.
   3. Configure uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

      IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

      IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
   4. Seleccione las funciones compatibles con la interfaz:

      Device Log Collection (Recopilación de logs del dispositivo): Recopila logs de los cortafuegos. Puede equilibrar la carga del tráfico de logs habilitando múltiples interfaces para realizar esta función.

      Collector Group Communication (Comunicación del grupo de recopiladores): comuníquese con otros recopiladores de logs en el grupo de recopiladores.
   5. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
4. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.
5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar sus cambios en Panorama y para enviar los cambios a los grupos de recopiladores que contienen los recopiladores de logs que modificó.
6. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que los recopiladores de logs están sincronizados y conectados con Panorama.

   La columna Configuration Status (Estado de configuración) debe mostrar `In Sync` y la columna Run Time Status (Estado de tiempo de ejecución) debe mostrar `connected`.

STEP 7 | Configure los cortafuegos para conectarse con una interfaz de Panorama.

Para admitir una red segmentada, puede conectar los cortafuegos en cada subred a interfaces de Panorama separadas. Las interfaces deben tener habilitada la **Device Management and Device Log Collection (Gestión de dispositivos y Recopilación de logs del dispositivo)**. Este

 ©2023 Palo Alto Networks, Inc.

paso asume que usted utiliza plantillas separadas para configurar los cortafuegos en subredes separadas.

En esta implementación de ejemplo, Panorama usa estas interfaces para gestionar los cortafuegos pero no para recopilar logs de cortafuegos. Usted especifica qué recopiladores de logs dedicados recopilarán logs de cortafuegos cuando selecciona configurar grupos de recopiladores.

1. Inicio de sesión en la interfaz web de Panorama del servidor de gestión de Panorama solitario (no HA) o activo (HA).
2. En Panorama, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, seleccione una **Template (Plantilla)** y edite la configuración de Panorama.
3. En el primer campo de **Panorama Servers (Servidores de Panorama)**, introduzca la dirección IP del Panorama solitario (no HA) o activo (HA).
4. (Solo HA) En el segundo campo de **Panorama Servers (Servidores de Panorama)**, introduzca la dirección IP de una interfaz en el Panorama pasivo que admitirá la gestión del dispositivo si ocurre la conmutación por error.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.
6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar sus cambios en Panorama y enviar los cambios a los cortafuegos.
7. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que los cortafuegos están sincronizados y conectados con Panorama.

   La columna Estado del dispositivo debería mostrar `Connected` (Conectado). Las columnas de Shared Policy (Política compartida) y Template (Plantilla) deben mostrar `in Sync`.

 ©2023 Palo Alto Networks, Inc.

Registro de Panorama e instalación de licencias

Antes de que pueda empezar a utilizar Panorama para una gestión centralizada, realizar logs y crear informes, debe registrar, activar y recuperar las licencias de gestión y asistencia técnica de dispositivos Panorama. Todas las instancias de Panorama necesitan licencias válidas que le permitan gestionar cortafuegos y obtener asistencia técnica. La licencia de gestión de dispositivos del cortafuegos activa el número máximo de cortafuegos que Panorama puede gestionar. Esta licencia está basada en los números de serie de los cortafuegos, no en el número de los sistemas virtuales en cada cortafuegos. La licencia de asistencia técnica permite las actualizaciones de software de Panorama y las de contenido dinámico (para las últimas firmas de amenazas y aplicaciones, por ejemplo). Además, los dispositivos virtuales Panorama en AWS y Azure deben adquirirse en Palo Alto Networks, y no se pueden adquirir en los mercados de AWS o Azure.

Después de actualizar su dispositivo virtual Panorama a PAN-OS 8.1, aparecerá un mensaje si no se instaló correctamente una licencia de capacidad o si el número total de cortafuegos gestionados por Panorama supera el valor establecido por la licencia de gestión de dispositivos. Cuenta con 180 días desde la fecha de la actualización para instalar una licencia de gestión de dispositivos válida si no se instaló una licencia. Si el número de cortafuegos gestionados supera el valor establecido por la licencia de gestión de dispositivos, cuenta con 180 días para eliminar los cortafuegos para satisfacer los requisitos de la licencia de gestión de dispositivos o actualizar su licencia de gestión de dispositivos. Todas las confirmaciones son fallidas si no se instala una licencia de gestión de dispositivos válida o si no se respeta el límite existente en la licencia de gestión de dispositivos, dentro de un plazo de 180 días posteriores a la actualización. Para adquirir una licencia de gestión de dispositivos, póngase en contacto con su representante de ventas o distribuidor autorizado de Palo Alto Networks.

Si desea usar la tecnología basada en la nube Cortex Data Lake, necesita una licencia de Cortex Data Lake, además de la licencia de administración del cortafuegos y la licencia de soporte premium. Para adquirir licencias, póngase en contacto con su ingeniero de sistemas de Palo Alto Networks o distribuidor.

Si ejecuta una licencia de evaluación para la gestión del cortafuegos en su dispositivo virtual Panorama y desea aplicar una licencia de Panorama que ha adquirido, realice las siguientes tareas: Registro de Panorama ***y*** Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.

- Registro de Panorama
- Activación de una licencia de asistencia técnica de Panorama
- Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet
- Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet
- Activación/recuperación de una licencia de gestión de cortafuegos en el dispositivo de la serie M

Registro de Panorama

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Registre el número de serie de Panorama o el código de autorización y registre su número de pedido de venta o ID de cliente.

Para obtener el código de autorización, el número de pedido de venta o el ID de cliente, consulte el correo electrónico de procesamiento del pedido que le envió el servicio de atención al cliente de Palo Alto Networks cuando realizó su pedido de Panorama.

Para obtener el número de serie, la ubicación depende del modelo:

- Dispositivo de la serie M: inicie sesión en la interfaz web de Panorama y registre el valor de **Serial # (N.° de serie)** en la pestaña **Dashboard (Panel)**, sección Información general.
- Dispositivo virtual Panorama: consulte el correo electrónico de cumplimiento de pedidos o consulte el número de serie generado al aprovisionar Panorama mediante licencias de VM Flex.



El dispositivo virtual Panorama se registra automáticamente cuando se asigna un número de serie mediante licencias de VM Flex.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Registre Panorama en el Portal de atención al cliente (CSP) de Palo Alto Networks.

Los pasos dependerán de si ya tiene un inicio de sesión en el CSP de Palo Alto Networks.

- Si es el primer dispositivo de Palo Alto Networks que registra y aún no tiene un inicio de sesión de CSP:
  1. Vaya a Palo Alto Networks CSP.
  2. Haga clic en **Create my account (Crear mi cuenta)**.
  3. Introduzca **Your Email Address (Su dirección de correo electrónico)** y responda al mensaje de reCAPTCHA.
  4. Haga clic en **Submit (Enviar)** después de responder correctamente al mensaje reCAPTCHA.
  5. Seleccione **Register device using Serial Number or Authorization Code (Registrar dispositivo con número de serie o código de autorización)** y haga clic en **Submit (Enviar)**
  6. Complete los campos de las secciones **Create Contact Details (Crear detalles de contacto)** y **Create UserID and Password (Crear ID de usuario y contraseña)** .
  7. Introduzca el **Device Serial Number (Número de serie del dispositivo)** de Panorama o **Auth Code (Código de autenticación)**.
  8. Introduzca su **Sales Order Number (Número de pedido de venta)** o **Customer ID (ID de cliente)**.
  9. Responda al mensaje de reCAPTCHA.
  10. Haga clic en **Submit (Enviar)** después de responder correctamente al mensaje reCAPTCHA.
- Si ya tiene un inicio de sesión CSP:
  1. Inicie sesión en Palo Alto Networks CSP.
  2. Haga clic en **Assets (Activos)** > **Devices (Dispositivos)** > **Register New Device (Registrar nuevo dispositivo)**.

     *También puede **registrar un dispositivo** en la página principal de soporte **de CSP.***
  3. Seleccione **Register device using Serial Number (Registrar dispositivo con el número de serie)** y haga clic en **Next (Siguiente)**.
  4. Introduzca el **Serial Number (Número de serie)** de Panorama.
  5. Introduzca el **Device Name (Nombre del dispositivo)** para aplicar un nombre para buscar e identificar su Panorama.
  6. (Opcional) Seleccione una **etiqueta de dispositivo** para agrupar Panorama con cualquier otro dispositivo para el que haya seleccionado una etiqueta de dispositivo.

     La etiqueta de dispositivo debe crearse primero en el nivel de cuenta (**Assets (Activos)** > **Devices (Dispositivos)** > **Device Tag (Etiqueta de dispositivo)**) antes de que se pueda seleccionar al registrar Panorama.
  7. Si el servidor de gestión de Panorama no está conectado a internet, seleccione la opción **Device will be used offline (El dispositivo se utilizará fuera de línea)** y seleccione la **OS Release (Versión de SO)**.
  8. Introduzca la información de ubicación obligatoria (como lo indican los asteriscos) si adquirió la RMA de 4 horas.

 ©2023 Palo Alto Networks, Inc.

9. **Acepte y envíe** el EULA.

   Después de ver el mensaje de registro completo, cierre el cuadro de diálogo Device Registration (Registro del dispositivo).

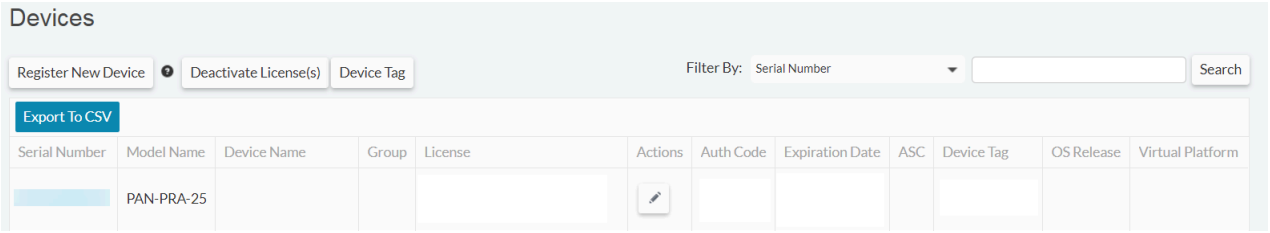
Activación de una licencia de asistencia técnica de Panorama

Antes de activar una licencia de asistencia técnica de Panorama en un dispositivo de la serie M de Panorama o un dispositivo virtual Panorama, debe realizar el Registro de Panorama.

Si la licencia de asistencia técnica vence, Panorama aún puede gestionar cortafuegos y recopilar logs, pero las actualizaciones de software y contenido no estarán disponibles. Las versiones de contenido y software de Panorama deben ser las mismas o superiores a las versiones de los cortafuegos gestionados o, de lo contrario, se producirán errores. Para obtener más información, consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire**.**

STEP 1 | Inicie sesión en el portal de Atención al cliente de Palo Alto Networks para activar el código de autenticación.

1. Seleccione **Assets (Activos)** > **Devices (Dispositivos)** e introduzca su número de serie de Panorama para filtrar por el **Serial Number (Número de serie)**.



2. Seleccione el ícono de lápiz en la columna Acción, seleccione **Activate Auth-Code (Activar código de autenticación)** e introduzca el **Authorization Code (Código de Autorización)** de su licencia de asistencia técnica y haga clic en **Agree and Submit (Aceptar y enviar)**.

STEP 2 | Inicie sesión en la interfaz web de Panorama y seleccione **Panorama** > **Support (Asistencia técnica)** > **Activate feature using authorization code (Activar característica mediante código de autorización)**.

STEP 3 | Introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.

STEP 4 | Verifique que la suscripción esté activada. Verifique los detalles (por ejemplo, la **Expiry Date [Fecha de vencimiento]**, el **Support Level [Nivel de asistencia]** y la **Description [Descripción]**) en la sección de Asistencia de la página.

Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet

Si desea gestionar dispositivos con Panorama, debe activar la licencia de gestión de cortafuegos que genera PAN-OS. El número de dispositivos que puede gestionar depende de la licencia activada. Los recopiladores de logs y los dispositivos de WildFire no se consideran dispositivos gestionados y, por lo tanto, no cuentan en el número permitido por la licencia.

 ©2023 Palo Alto Networks, Inc.

Antes de activar y recuperar una licencia de gestión de cortafuegos en el dispositivo virtual de Panorama, debe realizar el Registro de Panorama. Si está ejecutando una licencia de evaluación y quiere aplicar una licencia que ha adquirido, debe registrar y activar/recuperar la licencia adquirida. A continuación, cambie el número de serie de evaluación por el de producción.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.

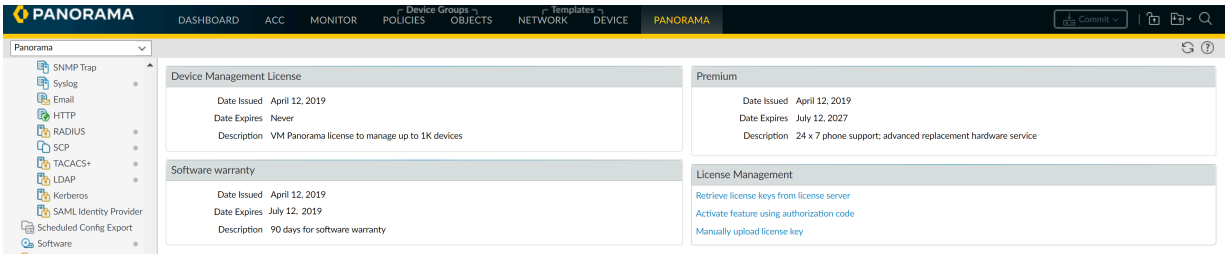
STEP 3 | Introduzca el **Serial Number (Número de serie)** de Panorama (incluido en el correo electrónico de procesamiento del pedido) y haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione **Panorama** > **Licenses (Licencias)** para activar o recuperar la licencia de gestión de cortafuegos:

- **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**: Panorama recupera la licencia de gestión de cortafuegos del servidor de actualizaciones de Panorama y la activa automáticamente.
- **Activate feature using authorization code (Activar función con código de autorización)**: introduzca el código de autorización de la licencia de gestión de cortafuegos y haga clic en **OK (Aceptar)** para activarla. Este código figura en el correo electrónico de confirmación del pedido, pero también puede buscarlo en la sección sobre el servidor de gestión de Panorama del sitio web de atención al cliente de Palo Alto Networks.
- **Manually upload license key (Cargar clave de licencia manualmente)**: inicie sesión en el sitio web de atención al cliente de Palo Alto Networks, busque el servidor de gestión de Panorama y descargue la clave de la licencia de gestión de cortafuegos para el dispositivo local. Después de descargar la clave de licencia, haga clic en **Choose File (Seleccionar archivo)** para seleccionarla y, luego, haga clic en **OK (Aceptar)**.

STEP 5 | Verifique que la licencia de gestión de cortafuegos está activada.

Ahora debe aparecer la sección Device Management License (Licencia de gestión de dispositivos) con la fecha de emisión, la fecha de vencimiento y la descripción.



Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet

Antes de activar y recuperar una licencia de gestión de cortafuegos en el dispositivo virtual de Panorama, debe realizar el Registro de Panorama. Para administrar dispositivos en Panorama, deberá activar una licencia de gestión de capacidad. La licencia de gestión de dispositivos que active determinará el número de dispositivos que Panorama puede gestionar. Los recopiladores de logs y los dispositivos WildFire no se tratan como dispositivos gestionados y no cuentan para el número de

 ©2023 Palo Alto Networks, Inc.

dispositivos asignados por la licencia de gestión de dispositivos. Si está ejecutando una licencia de evaluación y quiere aplicar una licencia que ha adquirido, debe registrar y activar/recuperar la licencia adquirida.

Después de actualizar a PAN-OS 8.1, se le solicitará que recupere una licencia de gestión de Panorama válida cuando inicie sesión por primera vez en la interfaz web de Panorama al completarse el reinicio. Para activar o recuperar la licencia de gestión válida si el dispositivo virtual Panorama está fuera de línea o incapaz de conectarse el servidor de actualización de Palo Alto Networks, debe obtener la información de dispositivo relevante para el dispositivo virtual Panorama y cargarla al sitio web de atención al cliente.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | (Solo en la implementación inicial) Introduzca el **número de serie** de Panorama.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
2. Introduzca el **Serial Number (Número de serie)** de Panorama (incluido en el correo electrónico de procesamiento del pedido) y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

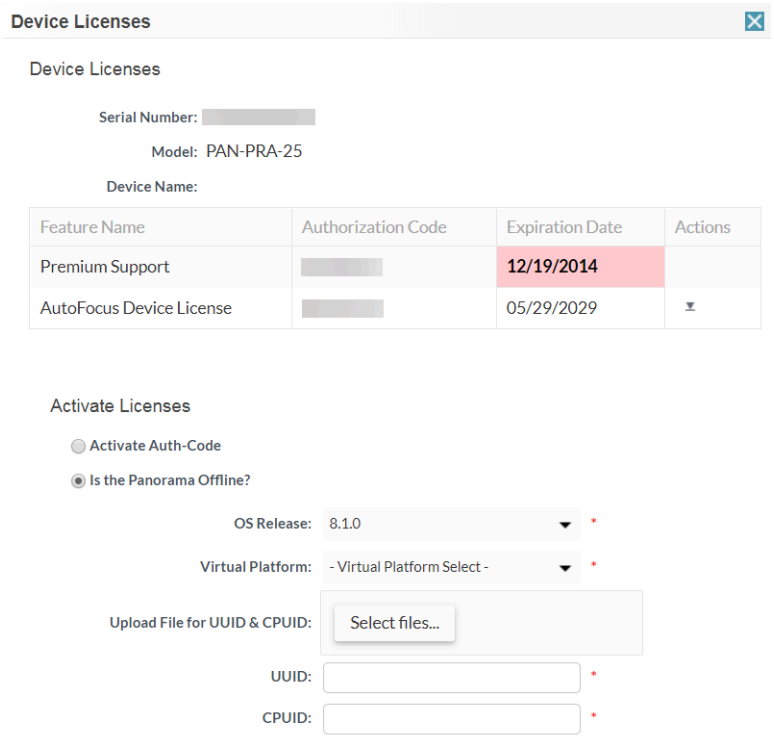
STEP 3 | Cargue la información del dispositivo virtual Panorama al sitio web de atención al cliente.

1. En el cuadro de diálogo Retrieve Management License (Recuperar licencia de gestión), haga clic el enlace **here (aquí)** para reunir información de UUID, CPUID, la versión de Panorama y la plataforma virtual. Haga clic en **Download Link (Descargar enlace)** para descargar un archivo XML con la información necesaria de Panorama que se puede cargar al portal de atención al cliente.

   En la implementación inicial, es posible que deba cerrar sesión y regresar a la interfaz web para ver el cuadro de diálogo.
2. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
3. Haga clic en **Get Support (Obtener asistencia técnica)** en la esquina superior derecha.
4. Seleccione **Assets (Activos)** > **Devices (Dispositivos)**, busque su dispositivo virtual Panorama y, en la columna Action (Acción), haga clic en el icono editar (✎).
5. Seleccione **Is the Panorama Offline? (¿Está Panorama fuera de línea?)** e introduzca la información de Panorama reunida en el paso 2 o haga clic en **Select files... (Seleccionar archivos...)** para cargar el archivo XML descargado.

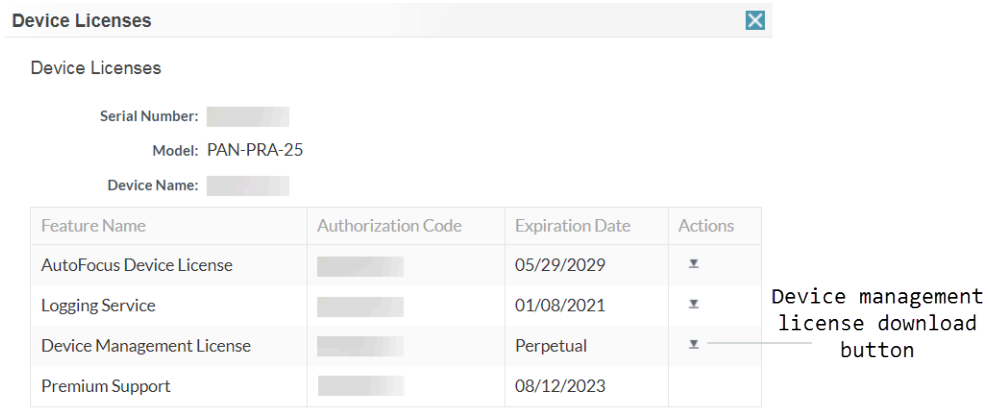
 ©2023 Palo Alto Networks, Inc.

6. Haga clic en **Agree and Submit (Aceptar y enviar)** para aceptar y enviar el EULA.



STEP 4 | Instale la licencia de gestión de dispositivos.

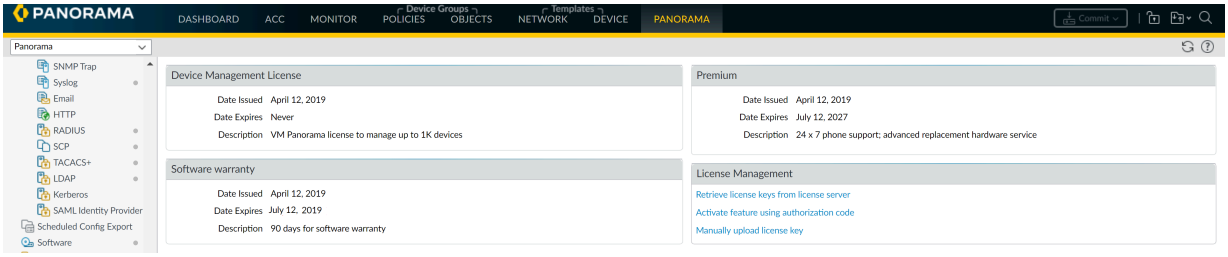
1. En la columna Action (Acción), descargue la licencia de gestión de dispositivos.



2. En la interfaz web de Panorama, seleccione **Panorama** > **Licenses (Licencias)** y haga clic en **Manually upload license key (Carga manual de la clave de la licencia)**.
3. Haga clic en **Choose file (Seleccionar archivo)**, ubique la clave de la licencia de gestión de dispositivos descargada y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Confirme que la licencia de gestión de dispositivos se cargó correctamente verificando que la licencia de gestión de dispositivos se muestre con la información de la licencia.



Activación/recuperación de una licencia de gestión de cortafuegos en el dispositivo de la serie M

Para administrar dispositivos en Panorama, deberá activar una licencia de capacidad. La licencia de capacidad determina el número de dispositivos que Panorama puede gestionar. Los recopiladores de logs y los dispositivos WildFire no se tratan como dispositivos gestionados y no cuentan para el número de dispositivos asignados por la licencia de capacidad.

Antes de activar y recuperar una licencia de gestión de cortafuegos de Panorama en el dispositivo de la serie M:

- Registre Panorama.
- Encuentre los códigos de activación del producto/suscripción que ha adquirido. Al realizar el pedido, el servicio de atención al cliente de Palo Alto Networks le envió un correo electrónico que indicaba el código de autenticación asociado a la compra. Si no encuentra este correo electrónico, póngase en contacto con el servicio de Atención al cliente de Palo Alto Networks para recibir sus códigos antes de continuar.

Después de activar y recuperar la licencia, la página **Panorama** > **Licenses (Licencias)** muestra la fecha de emisión asociada, la fecha de vencimiento y el número de cortafuegos que Panorama puede gestionar con la licencia.

Para activar y recuperar la licencia, las opciones son las siguientes:

- Utilice la interfaz web para activar y recuperar la licencia.

  Seleccione esta opción si Panorama está listo para conectarse al servidor de actualizaciones de Palo Alto Networks (ha realizado la tarea Realización de la configuración inicial del dispositivo de la serie M) pero no ha activado la licencia en el sitio web de asistencia técnica de Palo Alto Networks.

  1. Seleccione **Panorama** > **Licenses (Licencias)** y haga clic en **Activate feature using authorization code (Activar característica mediante código de autorización)**.
  2. Introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**. Panorama recuperará y activará la licencia.

- Recupere la clave de licencia del servidor de licencias.

  Si Panorama no está listo para conectarse al servidor de actualizaciones (por ejemplo, no ha realizado la configuración inicial del dispositivo de la serie M), puede activar la licencia en el sitio web de asistencia técnica para que, cuando Panorama esté listo para conectarse, pueda utilizar

 ©2023 Palo Alto Networks, Inc.

la interfaz web para recuperar la licencia activada. El proceso de recuperación de una licencia activada es más rápido que el proceso de recuperación y activación.

1. Active la licencia en el sitio web de Atención al cliente de Palo Alto Networks.
   1. En un host con acceso a Internet, utilice un navegador web para acceder al sitio web de asistencia al cliente de Palo Alto Networks e iniciar sesión.
   2. En la pestaña **Assets (Activos)** > **Devices (Dispositivos)**, busque su dispositivo serie M y, en la columna Action (Acción), haga clic en el icono editar ( ).
   3. Seleccione **Activate Auth-Code (Activar código de autenticación)**, introduzca el **Authorization Code (Código de autorización)** y haga clic en **Agree and Submit (Aceptar y enviar)** para activar la licencia.
2. Configure Panorama para que se conecte al servidor de actualizaciones: consulte Realización de la configuración inicial del dispositivo de la serie M.
3. Seleccione **Panorama** > **Licenses (Licencias)** y haga clic en **Retrieve license keys from the license server (Recuperar claves de licencia del servidor de licencias)**. Panorama recuperará la licencia activada.

- Cargue la licencia manualmente desde un host en Panorama. Panorama debe tener acceso a dicho host.

  Si Panorama está configurado (ha finalizado la tarea Realización de la configuración inicial del dispositivo de la serie M) pero no tiene una conexión con el servidor de actualizaciones, active la licencia en el sitio web de asistencia técnica, descárguela en un host que tenga una conexión con el servidor de actualizaciones y, a continuación, cárguela en Panorama.

  1. Active y descargue la licencia del sitio web de Atención al cliente de Palo Alto Networks.
     1. En un host con acceso a Internet, utilice un navegador web para acceder al sitio web de asistencia al cliente de Palo Alto Networks e iniciar sesión.
     2. En la pestaña **Assets (Activos)** > **Devices (Dispositivos)**, busque su dispositivo serie M y, en la columna Action (Acción), haga clic en el icono editar ( ).
     3. Seleccione **Activate Auth-Code (Activar código de autenticación)**, introduzca el **Authorization Code (Código de autorización)** y haga clic en **Agree and Submit (Aceptar y enviar)** para activar la licencia.
     4. En la columna Acción, haga clic en el icono de descarga y guarde el archivo de clave de licencia en el host.
  2. En la interfaz web de Panorama, seleccione **Panorama** > **Licenses (Licencias)**, haga clic en **Manually upload license key (Carga manual de la clave de licencia)** y en **Browse (Examinar)**.
  3. Seleccione el archivo de clave que descargó en el host y haga clic en **Open (Abrir)**.
  4. Haga clic en **OK (Aceptar)** para cargar la clave de licencia activada.

 ©2023 Palo Alto Networks, Inc.

Instalación del certificado de dispositivo de Panorama

En PAN-OS 9.1.3 y versiones posteriores, debe instalar el certificado del dispositivo en el servidor de gestión Panorama™ para autenticar correctamente Panorama con el portal de atención al cliente (CSP, Customer Support Portal) de Palo Alto Networks y aprovechar los servicios en la nube como el aprovisionamiento táctil cero (ZTP, Zero Touch Provisioning), la telemetría de dispositivos, IoT y la prevención de pérdida de datos empresariales (DLP, Enterprise Data Loss Prevention). Panorama debe disponer de acceso a Internet para instalar correctamente el certificado del dispositivo.

Si está aprovechando el complemento de servicios en la nube, debe tener instalado el complemento de servicios en la nube 1.5 o una versión posterior para instalar correctamente el certificado del dispositivo Panorama.

STEP 1 | Registro de Panorama con el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks

STEP 2 | Configure el servidor de protocolo de tiempo de redes (Network Time Protocol, NTP).

Es necesario un servidor NTP para validar la fecha de vencimiento de la certificación del dispositivo y asegurarse de que el certificado del dispositivo no caduque antes de tiempo o no sea válido.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Services (Servicios)**.
3. Seleccione **NTP** y especifique el nombre de host **`pool.ntp.org`** como **servidor NTP principal** o especifique la dirección IP de su servidor NTP principal.
4. (Opcional) Introduzca una dirección **Secondary NTP Server**.
5. (Opcional) Para autenticar actualizaciones de tiempo de los servidores NTP, en **Authentication Type (Tipo de autenticación)**, seleccione uno de los siguientes en cada servidor:
   - **None (Ninguna)** (opción por defecto): deshabilita la autenticación NTP.
   - **Symmetric Key (Clave simétrica)**: el cortafuegos usa intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de tiempo.
     - **Key ID (ID de clave)**: introduzca el ID de clave (1-65534).
     - **Algorithm (Algoritmo)**: seleccione el algoritmo que se debe utilizar en la autenticación del NTP (**MD5** o **SHA1**).
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

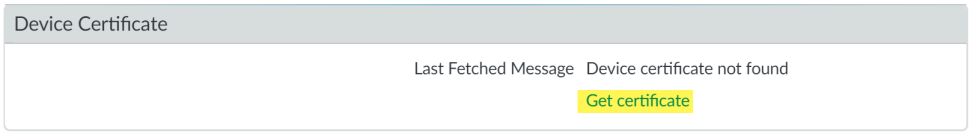
 ©2023 Palo Alto Networks, Inc.

STEP 3 | Genere la contraseña de un solo uso (One Time Password, OTP).

1. Inicie sesión en el Portal de atención al cliente.
2. Seleccione **Assets (Activos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **tipo de dispositivo**, seleccione **Generate OTP for Panorama (Generar OTP para Panorama)** y **Generate OTP (Generar OTP)**.
4. Seleccione el número de serie del **dispositivo Panorama**.
5. **Genere el OTP** y cópielo.

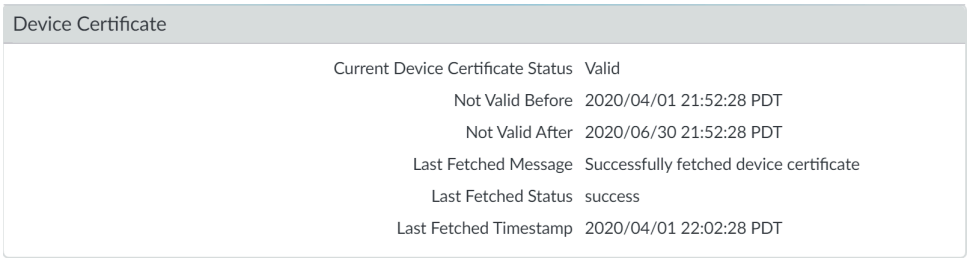
STEP 4 | Inicio de sesión en la interfaz web de Panorama como usuario administrador.

STEP 5 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Device Certificate Settings (Configuración del certificado del dispositivo)** y **Get certificate (Obtener certificado)**.



STEP 6 | Especifique la **contraseña de un solo uso** generada y haga clic en **OK (Aceptar)**.

STEP 7 | Panorama recupera e instala correctamente el certificado.



 ©2023 Palo Alto Networks, Inc.

Transición a un modelo diferente de Panorama

Si cambian los requisitos de la red (por ejemplo, aumenta la frecuencia de creación de logs), migre el servidor de gestión de Panorama y los recopiladores de logs dedicados a los Modelos Panorama más apropiados para satisfacerlos.

- Migración de un dispositivo virtual Panorama a un dispositivo de la serie M
- Migración de dispositivos virtuales Panorama a otro hipervisor
- Migración de un dispositivo M-Series a un dispositivo virtual Panorama
- Migración de un dispositivo M-100 a un dispositivo M-500
- Migración de un dispositivo M-100 o M-500 a un dispositivo M-200 o M-600

Migración de un dispositivo virtual Panorama a un dispositivo de la serie M

Puede migrar la configuración de Panorama desde un dispositivo virtual Panorama a un dispositivo de la serie M en modo Panorama. Sin embargo, no puede migrar los logs porque el formato de log en el dispositivo virtual Panorama no es compatible con el de los dispositivos de la serie M. Por lo tanto, si desea mantener el acceso a los logs anteriores almacenados en el dispositivo virtual Panorama, debe continuar ejecutando el dispositivo virtual Panorama después de la migración. El dispositivo de la serie M conectará los logs nuevos que los cortafuegos reenvíen después de la migración. Una vez que los logs previos a la migración venzan o se vuelvan irrelevantes debido a la antigüedad, podrá apagar el dispositivo virtual Panorama.

El modo heredado ya no se admite en PAN-OS 8.1 ni en las versiones posteriores. Si el dispositivo virtual Panorama anterior está en modo heredado, debe cambiar al modo de Panorama antes de migrar al nuevo hipervisor para conservar la configuración de los logs y las configuraciones de reenvío a los recopiladores de logs. Si importa la configuración de la anterior instancia en modo heredado a la nueva instancia en modo de Panorama, se eliminan todos los ajustes de los logs y del reenvío de logs.

No puede migrar los logs de un hipervisor a otro. Por lo tanto, si desea mantener el acceso a los logs almacenados en el anterior dispositivo virtual Panorama, debe seguir ejecutándolo tras la migración y añadirlo al nuevo dispositivo virtual Panorama como un recopilador de logs gestionado. De ese modo, el nuevo dispositivo recopila los logs nuevos que reenvían los cortafuegos después de la migración y se mantiene el acceso a los datos de logs antiguos. Una vez que los logs previos a la migración venzan o se vuelvan irrelevantes debido a la antigüedad, podrá apagar el dispositivo virtual Panorama.

Si almacena logs de cortafuegos en recopiladores de logs dedicados (dispositivos de la serie M en modo de recopilador de logs) en lugar de en el dispositivo virtual Panorama, puede conservar el acceso a los logs migrando los recopiladores de logs dedicados ***al dispositivo de la serie M en modo Panorama.***

STEP 1 | Planifique la migración.

- ☐ Actualice el software del dispositivo virtual Panorama antes de la migración si el dispositivo de la serie M requiere una versión posterior del software actual (el dispositivo M-500 requiere Panorama 7.0 o una versión posterior. Los dispositivos M-600 y M-200 requieren Panorama

 ©2023 Palo Alto Networks, Inc.

8.1 o una versión posterior. Los M-700 y M-300 requieren Panorama 10.2 o una versión posterior. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.

- Programe un periodo de mantenimiento para la migración. Aunque los cortafuegos puedan almacenar logs en el búfer después de que el dispositivo virtual Panorama se desconecte y reenviar logs después de que el dispositivo de la serie M se conecte, completar la migración durante un período de mantenimiento minimiza el riesgo de que los logs superen las capacidades del búfer y se pierdan durante la transición entre los modelos de Panorama.
- Piense si desea mantener el acceso al dispositivo virtual Panorama después de que la migración acceda a los logs existentes. El método más eficiente es asignar una nueva dirección IP al dispositivo virtual Panorama y volver a utilizar su dirección IP anterior para el dispositivo de la serie M. Esto garantiza que el dispositivo virtual Panorama permanezca accesible y que los cortafuegos puedan dirigirse al dispositivo de la serie M sin tener que volver a configurar la dirección IP de Panorama en cada cortafuegos.

STEP 2 | Adquiera el nuevo dispositivo M-Series y migre las suscripciones a este.

1. Adquiera el nuevo dispositivo M-Series.
2. Adquiera la nueva licencia de asistencia técnica y la licencia de migración.
3. En el momento de adquirir la licencia del nuevo dispositivo M-Series, facilite al representante de ventas el número de serie y el código de autorización de gestión de dispositivos del dispositivo virtual Panorama antiguo, así como la fecha de migración de la licencia que desee. Cuando reciba el dispositivo M-Series, regístrelo y active las licencias de gestión de dispositivos y de asistencia técnica usando los códigos de autorización de migración y de asistencia que le haya proporcionado Palo Alto Networks. En la fecha de la migración, se retira la licencia de gestión de dispositivos del dispositivo virtual Panorama antiguo, de modo que ya no puede gestionar dispositivos ni recopilar logs con él. En cambio, conserva la licencia de asistencia técnica, así que mantiene la cobertura de ese dispositivo Panorama. Aunque puede realizar la migración después de la fecha de entrada en vigor, no se aplica ningún cambio en la configuración del dispositivo retirado.

STEP 3 | (Solo en modo heredado) En el dispositivo virtual Panorama antiguo, cambie al modo Panorama.

Este paso es obligatorio para conservar los datos de logs, los ajustes y la configuración de reenvío de logs del dispositivo virtual Panorama. Si exporta la configuración de Panorama con el modo heredado activo, se pierden todos estos ajustes. Si no cambia el modo antes de proseguir, debe realizar el paso 9.

Si el dispositivo virtual Panorama ya está en los modos de Panorama o de solo gestión, vaya al paso siguiente.

STEP 4 | Exporte la configuración de Panorama desde el dispositivo virtual Panorama.

1. Inicie sesión en el dispositivo virtual Panorama y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que

 ©2023 Palo Alto Networks, Inc.

acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.

STEP 5 | Apague el dispositivo virtual Panorama si no va a necesitar acceder a él después de la migración o asigne una nueva dirección IP a su interfaz de gestión (management, MGT) si tiene que acceder a ella.

Para apagar el dispositivo virtual Panorama, consulte la documentación del producto de VMware.

Para cambiar la dirección IP en el dispositivo virtual Panorama, realice lo siguiente:

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de interfaz de gestión.
2. Introduzca la contraseña de IP nueva en **IP Address (Dirección IP)** y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 6 | Realice la configuración inicial del dispositivo de la serie M.

1. Monte en rack el dispositivo de la serie M. Consulte la Guía de referencia de hardware del dispositivo serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M para definir las conexiones de red necesarias para activar las licencias e instalar las actualizaciones.
3. Registre Panorama.
4. Active una licencia de asistencia técnica de Panorama.
5. Active o recupere una licencia de gestión de cortafuegos en el dispositivo de la serie M. Use el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Instale las mismas versiones que aquellas que se ejecutan en el dispositivo virtual Panorama.

STEP 7 | Cargue la instantánea de configuración de Panorama que exportó desde el dispositivo virtual Panorama en el dispositivo de la serie M.

*En la regla de **Policy (Política)** , las fechas de **Creation (Creación)** y **Modified (Modificación)** se actualizan para reflejar la fecha en la que compiló la configuración importada de Panorama en el nuevo Panorama. El identificador único universal (UUID) para cada regla de políticas persiste cuando migra la configuración de Panorama.*

*La fecha de **Creation (Creación)** y **Modified (Modificación)** para cortafuegos gestionados no se ven afectadas cuando supervisa el uso de una regla de políticas para un cortafuegos gestionado porque estos datos se almacenan de forma local en el cortafuegos gestionado y no en Panorama.*

1. En el dispositivo de la serie M, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)** y en **Browse (Explorar)** para ir al archivo de

 ©2023 Palo Alto Networks, Inc.

configuración de Panorama que exportó desde el dispositivo virtual Panorama, y luego haga clic en **OK (Aceptar)**.

3. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, seleccione una **Decryption Key (Clave de descifrado)** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración.
4. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.

STEP 8 | Modifique la configuración del dispositivo de la serie M.

Se requiere si el dispositivo de la serie M utilizará valores diferentes a los del dispositivo virtual Panorama. Si conservará el acceso al dispositivo virtual Panorama para acceder a sus logs, use un nombre de host y dirección IP diferentes para el dispositivo de la serie M.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
2. Edite la configuración general, modifique el nombre de host en **Hostname (Nombre de host)** y haga clic en **OK (Aceptar)**.
3. Edite la configuración de la interfaz de gestión, modifique los valores según sea necesario y haga clic en **OK (Aceptar)**.

STEP 9 | Añada el recopilador gestionado predeterminado y el grupo de recopiladores de nuevo al dispositivo serie M.

Si carga la configuración del dispositivo virtual Panorama (paso 7), se eliminan el recopilador gestionado y el grupo de recopiladores predeterminados que están predefinidos en todos los dispositivos M-Series.

1. Configure un recopilador gestionado que sea local en el dispositivo de la serie M.
2. Configure un grupo de recopiladores para el recopilador gestionado predeterminado.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Sincronice el dispositivo de la serie M con los cortafuegos para reanudar la gestión del cortafuegos.

> ***Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.***

1. En el dispositivo de la serie M, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que la columna Estado del dispositivo muestre **Connected (Conectado)** para los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Migración de dispositivos virtuales Panorama a otro hipervisor

Migre la configuración de los dispositivos virtuales Panorama de un hipervisor a otro compatible en los modos de solo gestión o de Panorama. Antes de realizar la migración, consulte Modelos Panorama para comprobar si se admite el nuevo hipervisor. Asimismo, si la configuración de Panorama incluye varias interfaces para la gestión de dispositivos, la recopilación de logs, la comunicación de los grupos de recopiladores, las licencias y las actualizaciones de software, consulte Requisitos previos de configuración del dispositivo virtual Panorama para verificar que el hipervisor nuevo admite más de una interfaz.

El modo heredado ya no se admite en PAN-OS 8.1 ni en las versiones posteriores. Si el dispositivo virtual Panorama anterior está en modo heredado, debe cambiar al modo de Panorama antes de migrar al nuevo hipervisor para conservar la configuración de los logs y las configuraciones de reenvío a los recopiladores de logs. Si importa la configuración de la anterior instancia en modo heredado a la nueva instancia en modo de Panorama, se eliminan todos los ajustes de los logs y del reenvío de logs.

No puede migrar logs desde el dispositivo virtual Panorama. Por lo tanto, si desea mantener el acceso a los logs almacenados en el anterior dispositivo virtual Panorama, debe seguir ejecutándolo en el modo de recopilación de logs tras la migración y añadirlo al nuevo dispositivo virtual Panorama como un recopilador de logs gestionado. De ese modo, el nuevo dispositivo recopila los logs nuevos que reenvían los cortafuegos después de la migración y se mantiene el acceso a los datos de logs antiguos. Una vez que los logs previos a la migración venzan o se vuelvan irrelevantes debido a la antigüedad, podrá apagar el dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

Si no almacena los logs de los cortafuegos en el dispositivo virtual Panorama sino en recopiladores de logs dedicados (esto es, el dispositivo virtual Panorama en modo de recopilador de logs), puede mantener el acceso a los logs migrando los recopiladores de logs dedicados *al nuevo dispositivo virtual Panorama en modo de Panorama.*

STEP 1 | Planifique la migración.

- Actualice el software del dispositivo virtual Panorama antes de la migración si el nuevo exige una versión posterior del software actual. Para obtener la versión mínima de PAN-OS para cada hipervisor, consulte Compatibilidad con el hipervisor de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
- Programe un periodo de mantenimiento para la migración. Aunque los cortafuegos pueden almacenar los logs en el búfer cuando se desconecta el dispositivo virtual Panorama y reenviarlos cuando se conecta el nuevo dispositivo, si realiza la migración durante un intervalo de mantenimiento, minimiza el riesgo de que se supere la capacidad del búfer y se pierdan logs durante la transición entre los hipervisores.
- Plantéese si desea seguir accediendo a los logs existentes del dispositivo virtual Panorama anterior después de la migración. El método más eficiente consiste en asignar una dirección IP nueva al dispositivo virtual Panorama antiguo y reutilizar su dirección IP anterior para el nuevo. Así, no solo sigue teniendo acceso al antiguo, sino que los cortafuegos apuntan al nuevo sin tener que volver a configurar la dirección IP de Panorama en cada uno de ellos.

  Si desea mantener el acceso al dispositivo virtual Panorama antiguo, debe adquirir una nueva licencia de administración de dispositivos y una licencia de soporte para el nuevo dispositivo virtual Panorama antes de poder completar la migración correctamente.

STEP 2 | (Solo para modo heredado) En el dispositivo virtual Panorama antiguo, Configuración de un dispositivo virtual Panorama en modo Panorama.

*Este paso es necesario para conservar la configuración de logs (**Panorama** > **Log Settings [Configuración de logs]**) en el dispositivo virtual Panorama antiguo. Si exporta la configuración de Panorama con el modo heredado activo, se pierden todos estos ajustes.*

Si el dispositivo virtual Panorama ya está en los modos de Panorama o de solo gestión, vaya al paso siguiente.

STEP 3 | Exporte la configuración de Panorama del dispositivo virtual Panorama antiguo.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione `running-config.xml` y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.
4. Busque el archivo `running-config.xml` que exportó y cambie el nombre del archivo XML. Esto es necesario para importar la configuración, ya que Panorama no admite la importación de un archivo XML con el nombre `running-config.xml`.

STEP 4 | Instale el dispositivo virtual Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Migre el número de serie del dispositivo virtual Panorama antiguo al nuevo dispositivo virtual Panorama.

Este paso es necesario para migrar todas las suscripciones y la licencia de administración de dispositivos vinculada al número de serie de Panorama y solo si tiene la intención de apagar el antiguo dispositivo virtual Panorama. Si tiene la intención de mantener el acceso al antiguo dispositivo virtual Panorama, continúe con el paso siguiente.

Tiene hasta 90 días para apagar el antiguo dispositivo virtual Panorama. La ejecución de varios dispositivos virtuales Panorama con el mismo número de serie infringe el EULA.

1. Inicie sesión en la interfaz web de Panorama del dispositivo virtual Panorama antiguo.
2. En **Dashboard (Panel)**, copie el número de `Serial # (Número de serie)` del antiguo dispositivo virtual Panorama ubicado en el widget de Información general.
3. Inicie sesión en la interfaz web de Panorama del dispositivo virtual Panorama nuevo.
4. Agregue el número de serie del dispositivo virtual Panorama antiguo al nuevo dispositivo virtual Panorama.
   1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
   2. Introduzca (pegue) **Serial Number (Número de serie)** y haga clic en **OK (Aceptar)**.
   3. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 6 | Ejecute la configuración inicial del dispositivo virtual Panorama nuevo.

1. Realización de la configuración inicial del dispositivo virtual Panorama para definir las conexiones de red necesarias para activar licencias e instalar actualizaciones.
2. (Solo para mantener el acceso al antiguo dispositivo virtual Panorama solamente) Registre Panorama.
3. (Solo para mantener el acceso al antiguo dispositivo virtual Panorama) Active una licencia de soporte de Panorama.
4. (Para mantener el acceso al antiguo dispositivo virtual Panorama) Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet. Use el código de autorización asociado con la licencia de migración.
5. Instale las actualizaciones de contenido y software de Panorama. Instale las mismas versiones que tenía en el dispositivo virtual Panorama anterior.

   Este paso es necesario antes de cargar la configuración desde el antiguo dispositivo virtual Panorama. Asegúrese de que todas las actualizaciones de contenido necesarias estén instaladas para evitar interrupciones de seguridad.
6. Seleccione **Panorama** > **Plugins (Complementos)** e instale todos los complementos que se instalaron en el antiguo dispositivo virtual Panorama.

©2023 Palo Alto Networks, Inc.

STEP 7 | Apague el dispositivo virtual Panorama anterior si no tiene que acceder a él después de la migración o bien asigne una dirección IP nueva a su interfaz de gestión en el caso contrario.

Para apagar el dispositivo, consulte la documentación del hipervisor donde está implementado.

Para cambiar la dirección IP en el dispositivo virtual Panorama, realice lo siguiente:

1. En la interfaz web del dispositivo virtual Panorama antiguo, seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite los ajustes de la interfaz de gestión.
2. Introduzca la contraseña de IP nueva en **IP Address (Dirección IP)** y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 8 | (Prisma Access) Transfiera la licencia de Prisma Access del antiguo dispositivo virtual Panorama al nuevo dispositivo virtual Panorama.

STEP 9 | Cargue en el dispositivo virtual Panorama nuevo la instantánea de configuración de Panorama exportada del dispositivo anterior.

*En la regla de **Policy (Política)** , las fechas de **Creation (Creación)** y **Modified (Modificación)** se actualizan para reflejar la fecha en la que compiló la configuración importada de Panorama en el nuevo Panorama. El identificador único universal (UUID) para cada regla de políticas persiste cuando migra la configuración de Panorama.*

*La fecha de **Creation (Creación)** y **Modified (Modificación)** para cortafuegos gestionados no se ven afectadas cuando supervisa el uso de una regla de políticas para un cortafuegos gestionado porque estos datos se almacenan de forma local en el cortafuegos gestionado y no en Panorama.*

1. Inicio de sesión en la interfaz web de Panorama del nuevo dispositivo virtual Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)** y en **Browse (Explorar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo virtual Panorama, y luego haga clic en **OK (Aceptar)**.
4. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, deje en blanco **Decryption Key (Clave de descifrado)** y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración.
5. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Modifique la configuración del dispositivo virtual Panorama nuevo.

Este paso es obligatorio si el dispositivo virtual Panorama debe utilizar valores diferentes de los especificado en el antiguo. Si desea mantener el acceso a los logs del dispositivo antiguo, use un nombre de host y una dirección IP diferentes para el nuevo.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
2. Edite la configuración general, modifique el nombre de host en **Hostname (Nombre de host)** y haga clic en **OK (Aceptar)**.
3. Edite la configuración de la interfaz de gestión, modifique los valores según sea necesario y haga clic en **OK (Aceptar)**.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 11 | Añada el recopilador gestionado y el grupo de recopiladores predeterminados al dispositivo virtual Panorama nuevo.

Si carga la configuración del dispositivo virtual Panorama anterior (paso 7), se eliminan el recopilador gestionado y el grupo de recopiladores predeterminados que están predefinidos en todos los dispositivos virtuales Panorama en modo de Panorama.

1. Para mantener el acceso a los logs almacenados en el antiguo dispositivo virtual Panorama, cambie al modo Recopilador de logs y agregue el Recopilador de logs dedicado al nuevo dispositivo virtual Panorama.
   1. Configuración del dispositivo virtual Panorama como un recopilador de logs.
   2. Configuración de recopiladores gestionados.
2. Configure un recopilador gestionado local en el dispositivo virtual Panorama.
3. Configure un grupo de recopiladores para el recopilador gestionado predeterminado.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Sincronice el nuevo dispositivo virtual Panorama con los cortafuegos para reanudar su gestión.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama nuevo, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que aparece **Connected (Conectado)** en la columna Device State (Estado de dispositivo) correspondiente a los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Migración de un dispositivo M-Series a un dispositivo virtual Panorama

Puede migrar la configuración de Panorama desde un dispositivo M-100, M-200, M-300, M-500, M-600, M-700 a un dispositivo virtual Panorama en modo Panorama. Sin embargo, no puede migrar los logs porque el formato de log en los dispositivos M-Series no son compatibles con los logs de los dispositivos virtuales Panorama. Por lo tanto, si desea mantener el acceso a los logs antiguos almacenados en el dispositivo M-Series, debe continuar ejecutando el dispositivo M-Series como recopilador de logs dedicado después de la migración y añadirlo al dispositivo virtual Panorama como un recopilador gestionado.

Si su servidor de gestión de Panorama forma parte de una configuración de alta disponibilidad, debe implementar un segundo dispositivo virtual Panorama para el mismo hipervisor o entorno en la nube, y adquirir las licencias de gestión de dispositivos y de asistencia técnica necesarias. Consulte Requisitos previos de HA de Panorama para obtener una lista completa de los requisitos de HA.

STEP 1 | Planifique la migración.

- Actualice el dispositivo M-Series a PAN-OS 10.2 o una versión posterior antes de la migración al dispositivo virtual Panorama. Para realizar la actualización de Panorama, consulte Instalación de actualizaciones de contenido y software de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
- Programe un periodo de mantenimiento para la migración. Aunque los cortafuegos puedan almacenar logs en el búfer después de que el dispositivo serie M se desconecte y reenviar logs después de que el dispositivo virtual Panorama se conecte, completar la migración durante

 ©2023 Palo Alto Networks, Inc.

un período de mantenimiento minimiza el riesgo de que los logs superen las capacidades del búfer durante la transición entre los modelos de Panorama.

STEP 2 | Adquiera licencias de gestión y asistencia técnica para el nuevo dispositivo virtual Panorama.

1. Póngase en contacto con su representante de ventas para adquirir las licencias nuevas de asistencia técnica y gestión de dispositivos.
2. Indique a su representante de ventas el número de serie del dispositivo M-Series que desee eliminar, el número de serie y el código de autenticación de soporte que recibió cuando adquirió el nuevo dispositivo virtual Panorama, y la fecha en la que espera que se complete la migración del dispositivo anterior al nuevo dispositivo virtual. Antes de la fecha de migración, registre el número de serie y active el código de autenticación de soporte en el nuevo dispositivo virtual para poder iniciar la migración. El código de autenticación de capacidad del antiguo dispositivo M-Series se eliminará automáticamente en la fecha esperada de finalización de la migración que haya indicado.

STEP 3 | Realice la configuración inicial del dispositivo virtual Panorama.

1. Configuración del dispositivo virtual Panorama.
2. Lleve a cabo la configuración inicial del dispositivo virtual Panorama para definir las conexiones de red necesarias para activar las licencias e instalar las actualizaciones.
3. Registre Panorama.
4. Active una licencia de asistencia técnica de Panorama.
5. Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet
6. Instale las actualizaciones de contenido y software de Panorama. Instale las mismas versiones que aquellas que se ejecutan en el dispositivo M-Series.

STEP 4 | Edite la configuración de interfaz Panorama del dispositivo serie M para que solo utilice la interfaz de gestión.

El dispositivo virtual Panorama solo admite la interfaz de gestión para la gestión de dispositivos y la recopilación de logs.

1. Inicie sesión en la interfaz web de Panorama del dispositivo serie M.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
3. Edite la configuración general, modifique el nombre de host en **Hostname (Nombre de host)** y haga clic en **OK (Aceptar)**.
4. Seleccione **Interfaces** y edite la interfaz de **Management (Gestión)** para habilitar los servicios necesarios.
5. Deshabilite los servicios para las interfaces restantes.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 5 | Añada la dirección IP del nuevo dispositivo virtual Panorama.

En el dispositivo serie M, añada la dirección IP pública del dispositivo virtual Panorama como el segundo servidor Panorama para gestionar dispositivos desde el nuevo servidor de gestión de

 ©2023 Palo Alto Networks, Inc.

Panorama. Si el dispositivo virtual Panorama se implementa en Alibaba Cloud, AWS, Azure, GCP u OCI, utilice la dirección IP pública.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)**.
2. En el menú desplegable Template (Plantilla), seleccione la plantilla o la pila de plantillas que contiene la configuración del servidor Panorama.
3. Edite los ajustes de Panorama.
4. Introduzca la dirección IP pública del dispositivo virtual Panorama y haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.

STEP 6 | Exporte la configuración del dispositivo M-Series.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML. Guarde la configuración en una ubicación externa al dispositivo Panorama.

STEP 7 | Apague el dispositivo serie M o asigne una nueva dirección IP a la interfaz de gestión (MGT).

Si el dispositivo serie M está en modo Panorama y tiene logs almacenados en el recopilador de logs local al que necesita acceso en el nuevo dispositivo virtual Panorama, debe cambiar la dirección IP del dispositivo serie M para añadirlo al dispositivo virtual Panorama como un recopilador de logs gestionado.

- **Para apagar el dispositivo VM-Series:**

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y en Device Operations (Operaciones de dispositivo), haga clic en **Shutdown Panorama (Apagar Panorama)**. Haga clic en **Yes (Sí)** para confirmar que se apague.

- **Para cambiar la dirección IP en el dispositivo M-Series:**

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de interfaz de gestión.
3. Introduzca la contraseña de IP nueva en **IP Address (Dirección IP)** y haga clic en **OK (Aceptar)**.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Cargue la instantánea de configuración de Panorama que exportó desde el dispositivo M-Series al dispositivo virtual Panorama.

*En la regla de **Policy (Política)** , las fechas de **Creation (Creación)** y **Modified (Modificación)** se actualizan para reflejar la fecha en la que compiló la configuración importada de Panorama en el nuevo Panorama. El* identificador único universal (UUID) *para cada regla de políticas persiste cuando migra la configuración de Panorama.*

*La fecha de **Creation (Creación)** y **Modified (Modificación)** para cortafuegos gestionados no se ven afectadas cuando* supervisa el uso de una regla de políticas para un cortafuegos gestionado *porque estos datos se almacenan de forma local en el cortafuegos gestionado y no en Panorama.*

1. Inicie sesión en la interfaz web de Panorama del dispositivo virtual Panorama y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, **Browse (Examinar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo V-Series, y luego haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, seleccione una **Decryption Key (Clave de descifrado)** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración.

Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida. La configuración se ha cargado una vez que la confirmación es correcta.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Cambie el dispositivo serie M a modo recopilador de logs para conservar los datos de logs existentes.

Los datos de logging se eliminan si cambia a modo recopilador de logs mientras los discos de logging aún están insertados en el dispositivo serie M. Los discos de logging se deben retirar antes de cambiar el modo para evitar la pérdida de datos de log.

La generación de metadatos para cada par de discos reconstruye los índices. Por lo tanto, dependiendo del tamaño de los datos, este proceso puede tardar mucho tiempo en realizarse. Para acelerar el proceso, puede iniciar múltiples sesiones CLI y ejecutar el comando de regeneración de metadatos en cada sesión para completar el proceso simultáneamente para cada par. Para obtener más detalles, consulte Regeneración de metadatos para pares de RAID de un dispositivo de la serie M.

1. Retire los discos RAID del dispositivo anterior de la serie M.
   1. Apague el dispositivo serie M presionando el botón de encendido hasta que el sistema se apague.
   2. Retire los pares de discos. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.
2. Encienda el dispositivo serie M presionando el botón de encendido.
3. Configure una cuenta de administrador superusuario `admin`Configuración de una cuenta de administrador de Panorama..

   Si ya se ha creado una cuenta de administrador `admin`, diríjase al siguiente paso.

   Se debe crear una cuenta de `administración` con privilegios de superusuario antes de cambiar al modo de recopilación de logs o de que pierda el acceso al dispositivo M-Series después de alternar los modos.
4. Inicie sesión en la CLI de Panorama en el dispositivo serie M anterior.
5. Cambie del modo Panorama al modo de recopilación de logs.
   - Para cambiar al modo de recopilación de logs, introduzca el siguiente comando:

     ```
     > request system system-mode logger
     ```
   - Ingrese **Y** para confirmar el cambio de modo. El dispositivo de la serie M se reiniciará. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectar el dispositivo de la serie M para ver la solicitud de inicio de sesión a Panorama.

     *Si ve la solicitud **`CMS Login`**, esto significa que el recopilador de logs finalizó el reinicio. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.*
   - Vuelva a iniciar sesión en la CLI.
   - Verifique que el cambio al modo de recopilador de logs se realizó correctamente:

     ```
     > show system info | match system-mode
     ```

 ©2023 Palo Alto Networks, Inc.

Si el cambio de modo es correcto, se muestra lo siguiente:

```
> system-mode: logger
```

6. Inserte los discos nuevamente en el dispositivo serie M anterior. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

   Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 en la ranura B1/B2, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.
7. Habilite los pares de discos ejecutando el siguiente comando de la CLI para cada par:

   ```
   > request system raid add <slot> force no-format
   ```

   Por ejemplo:

   ```
   > request system raid add A1 force no-format > request system
    raid add A2 force no-format
   ```

   Los argumentos **force** y **no-format** son obligatorios. El argumento **force** asocia el par de discos con el nuevo dispositivo. El argumento **no-format** evita la aplicación de formato de las unidades y mantiene almacenados los logs en los discos.
8. Genere los metadatos para cada par de discos.

   ```
   > request metadata-regenerate slot <slot_number>
   ```

   Por ejemplo:

   ```
   > request metadata-regenerate slot 1
   ```
9. Habilite la conectividad entre el recopilador de logs y el servidor de gestión de Panorama.

   Introduzca los siguientes comandos en la CLI del recopilador de logs, donde *<IPaddress1>* es para la interfaz de MGT del Panorama solitario (no HA) o activo (HA) y *<IPaddress2>* es para la interfaz de MGT del Panorama pasivo (HA), si corresponde.

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress1> panorama-server-2 <IPaddress2> # commit
    # exit
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Sincronice el dispositivo virtual Panorama con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo virtual Panorama, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que la columna Device State (Estado del dispositivo) muestre a los cortafuegos como **Connected (Conectado)**.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione cada grupo de dispositivos y haga clic en **Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
   3. Seleccione **Collector Groups (Grupos de recopiladores)**, seleccione cada grupo de recopiladores y haga clic en **OK (Aceptar)**.
   4. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

STEP 11 | (Solo HA) Configure el peer de HA Panorama.

Si los servidores de gestión de Panorama se encuentran en una configuración de alta disponibilidad, realice los pasos a continuación en el peer de HA.

1. Realice la configuración inicial del dispositivo virtual Panorama.
2. Edite la configuración de interfaz Panorama del dispositivo serie M para que solo utilice la interfaz de gestión.
3. Añada la dirección IP del nuevo dispositivo virtual Panorama.
4. Apague el dispositivo serie M o asigne una nueva dirección IP a la interfaz de gestión (MGT).
5. Cambie el dispositivo serie M a modo recopilador de logs para conservar los datos de logs existentes.

STEP 12 | (Solo HA) Modifique la configuración del peer de HA del dispositivo virtual Panorama.

1. En un peer de HA, inicie sesión en la interfaz web de Panorama, seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la **Setup (Configuración)**.
2. En el campo **Peer HA IP Address (Dirección IP del peer de HA)**, introduzca la nueva dirección IP del peer de HA y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para confirmar el cambio.
4. Repita estos pasos en el otro peer del peer de HA.

 ©2023 Palo Alto Networks, Inc.

STEP 13 | (Solo de HA) Sincronice los peers de Panorama.

1. Acceda al **Dashboard (Panel)** en uno de los peers de HA y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
2. **Sync to peer (Sincronizar en el peer)**, haga clic en **Yes (Sí)** y espere a que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.
3. Acceda al **Dashboard (Panel)** en el peer de HA restante y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
4. Verifique que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.

Migración de un dispositivo M-100 a un dispositivo M-500

Puede migrar la configuración de Panorama y los logs del cortafuegos desde un dispositivo M-100 a uno M-500 en el modo Panorama (servidor de gestión de Panorama). También puede migrar los logs del cortafuegos desde un dispositivo M-100 a uno M-500 en el modo de recopilación de logs (recopilador de logs dedicado). Debido a que todos los recopiladores de logs de un grupo de recopiladores deben ser del mismo modelo de Panorama, debe migrar todos o ninguno de los dispositivos M-100 en cualquier grupo de recopiladores.

En el siguiente procedimiento, el servidor de gestión de Panorama está implementado en una configuración de Alta disponibilidad (high availability, HA) activa/pasiva; usted migrará la configuración y los logs, y los dispositivos M-500 reutilizarán las direcciones IP de los dispositivos M-100.

En este procedimiento se da por sentado que ya no va a usar el dispositivo M-100 para gestionar dispositivos ni recopilar logs. Si pretende utilizarlo como recopilador de logs dedicado, tiene que instalar en él una licencia de gestión de dispositivos. Sin ella, el dispositivo M-100 retirado no se puede emplear como recopilador de logs dedicado.

Si no pretende utilizar el dispositivo M-100 como recopilador de logs dedicado, pero contiene datos de logs a los que debe acceder con posterioridad, puede consultarlos y generar informes a partir de ellos. Palo Alto Networks recomienda revisar la política de conservación de logs antes de retirar el dispositivo M-100.

Si va a migrar solo los logs y no la configuración de Panorama, lleve a cabo las tareas Migración de logs a un nuevo dispositivo de la serie M en modo de recopilación de logs *o* Migración de logs a un nuevo dispositivo de la serie M en modo Panorama.

Si va a migrar a un nuevo servidor de gestión de Panorama que no está implementado en una configuración de HA y el nuevo Panorama debe acceder a los logs en los recopiladores de logs dedicados existentes, lleve a cabo la tarea Migración de recopiladores de logs después de un error o RMA de un Panorama que no es de HA.

STEP 1 | Planifique la migración.

- Actualice el software del dispositivo M-100 si su versión actual es anterior a 7.0; el dispositivo M-500 requiere Panorama 7.0 o una versión posterior. Para obtener detalles importantes

 ©2023 Palo Alto Networks, Inc.

sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.

- Reenvíe los logs de sistema y la configuración que Panorama y los recopiladores de logs generan a un destino externo antes de la migración si desea conservar esos logs. El dispositivo de la serie M en el modo Panorama almacena estos tipos de logs en su SSD, que no puede mover entre modelos. Solo puede mover las unidades RAID, que almacenan logs del cortafuegos.
- Programe un periodo de mantenimiento para la migración. Aunque los cortafuegos puedan almacenar logs en el búfer después de que el dispositivo M-100 se desconecte y reenviar logs después de que el dispositivo M-500 se conecte, completar la migración durante un período de mantenimiento minimiza el riesgo de que los logs superen las capacidades del búfer y se pierdan durante la transición entre los modelos de Panorama.

STEP 2 | Adquiera el nuevo dispositivo M-500 y migre las suscripciones a este.

1. Adquiera el nuevo dispositivo M-500.
2. Adquiera la nueva licencia de asistencia técnica y la licencia de migración.
3. En el momento de adquirir el nuevo dispositivo M-500, facilite al representante de ventas el número de serie y el código de autorización de gestión de dispositivos del M-100 antiguo, así como la fecha de migración de la licencia que desee. Cuando reciba el dispositivo M-500, regístrelo y active las licencias de gestión de dispositivos y de asistencia técnica usando los códigos de autorización de migración y de asistencia que le haya proporcionado Palo Alto Networks. En la fecha de la migración, se retira la licencia de gestión de dispositivos del dispositivo M-100, de modo que ya no puede gestionar dispositivos ni recopilar logs con él. En cambio, conserva la licencia de asistencia técnica, así que mantiene la cobertura de ese dispositivo Panorama. Aunque puede realizar la migración después de la fecha de entrada en vigor, no se aplica ningún cambio en la configuración del dispositivo M-100 retirado.

STEP 3 | Exporte la configuración de Panorama de cada dispositivo M-100 en el modo Panorama.

Lleve a cabo esta tarea en cada peer de HA del dispositivo M-100:

1. Inicie sesión en el dispositivo M-100 y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.

STEP 4 | Apague cada dispositivo M-100 en el modo Panorama.

1. Inicie sesión en el peer de HA del dispositivo M-100 que apagará.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Shutdown Panorama (Apagar Panorama)**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Realice la configuración inicial de cada dispositivo M-500.

1. Monte en rack los dispositivos M-500. Consulte la Guía de referencia de hardware del dispositivo M-500 para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M para definir las conexiones de red necesarias para activar las licencias e instalar las actualizaciones.
3. Registre Panorama.
4. Active una licencia de asistencia técnica de Panorama.
5. Active una licencia de gestión de cortafuegos. Use el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Instale las mismas versiones que aquellas que se ejecutan en el dispositivo M-100.
7. (Solo en recopilador de logs dedicado) Configure el dispositivo de la serie M como un recopilador de logs.

STEP 6 | Cargue la instantánea de configuración de Panorama que exportó de cada dispositivo M-100 en cada dispositivo M-500 en el modo Panorama (ambos peers de HA).



*En la regla de **Policy (Política)** , las fechas de **Creation (Creación)** y **Modified (Modificación)** se actualizan para reflejar la fecha en la que compiló la configuración importada de Panorama en el nuevo Panorama. El* identificador único universal (UUID) *para cada regla de políticas persiste cuando migra la configuración de Panorama.*

*La fecha de **Creation (Creación)** y **Modified (Modificación)** para cortafuegos gestionados no se ven afectadas cuando* supervisa el uso de una regla de políticas para un cortafuegos gestionado *porque estos datos se almacenan de forma local en el cortafuegos gestionado y no en Panorama.*

Lleve a cabo esta tarea en cada peer de HA del dispositivo M-500:

1. Inicie sesión en el dispositivo M-500 y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)** y en **Browse (Explorar)** para navegar al archivo de configuración exportado del dispositivo M-100 que tiene la misma prioridad de HA (primaria o secundaria) que el dispositivo M-500 tendrá y haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, seleccione una **Decryption Key (Clave de descifrado)** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Validate Commit (Validar confirmación)**. Resuelva cualquier error antes de continuar.
5. Seleccione **Commit (Confirmar)** los cambios en la configuración de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Sincronice la configuración entre los peers de HA del dispositivo M-500 en el modo Panorama.

1. En el dispositivo M-500, seleccione la pestaña **Dashboard (Panel)** y, en el widget de alta disponibilidad, haga clic en **Sync to peer (Sincronizar con peer)**.
2. En el widget de alta disponibilidad, verifique que **Local** (dispositivo M-500 primario) sea **active**, el **Peer** sea pasivo y **Running Config** esté **synchronized**.

STEP 8 | Mueva las unidades RAID de cada dispositivo M-100 a su dispositivo M-500 de reemplazo para migrar los logs recopilados del cortafuegos.

En las siguientes tareas, omita cualquier paso que ya haya completado en el dispositivo M-500.

- Realice la migración de logs a un nuevo dispositivo de la serie M en modo Panorama. Migre los logs del dispositivo M-100 solo si utiliza un recopilador gestionado predeterminado para la recopilación de logs.
- Realice la migración de logs a un nuevo dispositivo de la serie M en modo de recopilación de logs.

STEP 9 | Sincronice el dispositivo activo M-500 en el modo Panorama con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo M-500 activo, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que la columna Estado del dispositivo muestre **Connected (Conectado)** para todos los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran **Out of sync (No sincronizado)** para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

Migración de un dispositivo M-100 o M-500 a un dispositivo M-200 o M-600

Este procedimiento describe la migración de configuración de Panorama para los siguientes dispositivos de M-Series en modo Panorama (servidor de gestión Panorama):

 ©2023 Palo Alto Networks, Inc.

- De un dispositivo M-100 a un dispositivo M-200 o M-600.

  No se admite la migración de logs. El factor de forma de disco de logging del dispositivo M-100 no es compatible con los dispositivos M-200 y M-600.
- De un dispositivo M-500 a un dispositivo M-200 o M-600.

  No se admite la migración de logs. El factor de forma de disco de logging del dispositivo M-500 no es compatible con los dispositivos M-200 y M-600.

Además, todos los recopiladores de logs de un grupo de recopiladores deben ser del mismo modelo Panorama. Por ejemplo, si desea añadir el recopilador de logs local en el nuevo dispositivo M-200 a un grupo de recopiladores, el grupo de recopiladores de destino debe contener solo dispositivos M-200. Lo mismo ocurre con el recopilador de logs local para un dispositivo M-600.

En este procedimiento se da por sentado que ya no va a usar el dispositivo M-100 o M-500 para gestionar dispositivos ni recopilar logs. Si pretende utilizarlos como recopiladores de logs dedicados, tiene que instalar en ellos una licencia de gestión de dispositivos. Sin ella, el dispositivo M-100 o M-50 retirado no se puede emplear como recopilador de logs dedicado.

Aún puede acceder a los datos de logs existentes en una fecha posterior si no planea utilizar el dispositivo M-100 o M-500 como recopilador de logs dedicado. Después de migrar correctamente al nuevo dispositivo M-Series, encienda el dispositivo M-100 o M-500 para consultar y generar informes desde la interfaz web de Panorama del dispositivo M-Series fuera de servicio. Palo Alto Networks recomienda revisar la política de conservación de logs antes de retirar el dispositivo M-100 o M-500.

STEP 1 | Planifique la migración.

- Actualice el software del dispositivo M-100 o M-500 a una versión PAN-OS compatible. Revise la Matriz de compatibilidad de Palo Alto Networks para obtener la versión mínima compatible de PAN-OS.

  Consulte el Resumen del fin de la vida útil de Palo Alto Networks para obtener una lista de las versiones de PAN-OS actualmente compatibles. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
- Programe un periodo de mantenimiento para la migración. Aunque los cortafuegos puedan almacenar logs en el búfer después de que el dispositivo M-100 o M-500 se desconecte y reenviar logs después de que el dispositivo M-200 o M-600 se conecte, completar la migración durante un período de mantenimiento minimiza el riesgo de que los logs superen las capacidades del búfer y se pierdan durante la transición entre los modelos de Panorama.

STEP 2 | Adquiera el nuevo dispositivo M-200 o M-600 y migre las suscripciones a este.

1. Adquiera el nuevo dispositivo M-200 o M-600.
2. Adquiera la nueva licencia de asistencia técnica y la licencia de migración.
3. En el momento de adquirir el nuevo dispositivo M-200 o M-600, facilite al representante de ventas el número de serie y el código de autorización de gestión de dispositivos del M-100 o M-500 antiguo, así como la fecha de migración de la licencia que desee. Cuando reciba el dispositivo M-200 o M-600, regístrelo y active las licencias de gestión

 ©2023 Palo Alto Networks, Inc.

de dispositivos y de asistencia técnica usando los códigos de autorización de migración y de asistencia que le haya proporcionado Palo Alto Networks. En la fecha de la migración, se retira la licencia de gestión de dispositivos del dispositivo M-100 o M-500, de modo que ya no puede gestionar dispositivos ni recopilar logs con ellos. En cambio, conserva la licencia de asistencia técnica, así que mantiene la cobertura de ese dispositivo Panorama. Aunque puede realizar la migración después de la fecha de entrada en vigor, no se aplica ningún cambio en la configuración del dispositivo M-100 o M-500 retirado.

Palo Alto Networks permite un período de gracia de migración de hasta 90 días al migrar entre dispositivos de la M-Series. Póngase en contacto con su representante de ventas de Palo Alto Networks para obtener más información sobre su migración.

STEP 3 | Exporte la configuración de Panorama de cada dispositivo M-100 en el modo Panorama.

(Configuración de HA) Realice este paso en cada peer de HA del dispositivo M-100 o M-500. Realice un seguimiento de la prioridad de HA (principal o secundaria) del dispositivo M-100 o M-500.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
4. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.

STEP 4 | En la interfaz web de Panorama del peer de HA del dispositivo M-100 o M-500 que va a apagar, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Shutdown Panorama (Apagar Panorama)**.

(Configuración de HA) Repita este paso para los peers de HA de dispositivos M-100 o M-500.

STEP 5 | Realice la configuración inicial del dispositivo de la M-Series.

(Configuración de HA) Repita este paso para los peers de HA de dispositivos M-200 o M-600.

1. Monte en rack los dispositivos M-500. Consulte la Guía de referencia de hardware del dispositivo M-200 o M-600 para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M para definir las conexiones de red necesarias para activar las licencias e instalar las actualizaciones.
3. Registre Panorama.
4. Active una licencia de asistencia técnica de Panorama.
5. Active una licencia de gestión de cortafuegos. Use el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Instale las mismas versiones que las del dispositivo M-100 o M-500.
7. (Solo en recopilador de logs dedicado) Configure el dispositivo de la serie M como un recopilador de logs.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Cargue la instantánea de configuración de Panorama que exportó de cada dispositivo M-100 o M-500 en cada dispositivo M-200 o M-600 en el modo Panorama.

(Configuración de HA) Repita este paso para los peers de HA de dispositivos M-200 o M-600.



*Las fechas de **creación** y **modificación** de la regla **de política** de Panorama se actualizan para reflejar la fecha en que se compila la configuración de Panorama importada en el nuevo Panorama. El* identificador único universal (UUID) *para cada regla de directiva persiste al migrar la configuración de Panorama.*

*La **creación** y **modificación** para cortafuegos gestionados no se ve afectada cuando se supervisa el uso de* reglas de políticas para un cortafuegos gestionado *porque estos datos se almacenan localmente en el cortafuegos gestionado y no en Panorama.*

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración Panorama con nombre)**.
4. **Busque** el archivo de configuración que exportó desde el dispositivo M-100 o M-500 que tiene la misma prioridad de HA (principal o secundaria) que tendrá el dispositivo M-200 o M-600 y haga clic en **OK (Aceptar)**.
5. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)** y seleccione el **Name (Nombre)** de la configuración que acaba de importar.
6. Seleccione una **clave de descifrado** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**.
7. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.
8. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Validate Commit (Validar confirmación)**. Resuelva cualquier error antes de continuar.
9. Seleccione **Commit (Confirmar)** los cambios en la configuración de Panorama.

STEP 7 | Sincronice la configuración entre los peers de HA del dispositivo M-200 o M-600 en el modo Panorama.

1. En la interfaz web de Panorama del dispositivo M-200 o M-600 activo, seleccione el **panel**.
2. En el widget de alta disponibilidad, haga clic en **Sync to peer (Sincronizar con peer)**.
3. En el widget de alta disponibilidad, verifique que **Local** (dispositivo M-200 primario) esté **active**, el **Peer** esté passive y **Running Config** esté `synchronized`.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Sincronice el dispositivo activo M-200 o M-600 en el modo Panorama con los cortafuegos para reanudar la gestión del cortafuegos.

Complete este paso en un período de mantenimiento para minimizar el tiempo de interrupción de la red.

1. En el dispositivo M-200 o M-600 activo, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y verifique que la columna Estado del dispositivo muestre `Connected (Conectado)` para todos los cortafuegos.

   En este punto, las columnas Política compartida (grupos de dispositivos) y Plantilla muestran `Out of ssnc (No sincronizado)` para los cortafuegos.
2. Envíe los cambios a los grupos de dispositivos y plantillas.
   1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione todos los grupos de dispositivos, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y haga clic **OK (Aceptar)**.
   3. Seleccione **Push (Enviar)** sus cambios.
3. En la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, verifique que las columnas Política compartida y Plantilla muestren **In sync (Sincronizado)** para los cortafuegos.

 ©2023 Palo Alto Networks, Inc.

Acceso y navegación en las interfaces de gestión de Panorama

Panorama proporciona tres interfaces de gestión:

- **Interfaz web**: la interfaz web de Panorama tiene una apariencia similar a la interfaz web del cortafuegos. Si conoce esta última, podrá navegar, completar tareas administrativas y generar informes con facilidad desde la interfaz web de Panorama. Esta interfaz gráfica le permite acceder a Panorama con HTTPS y es la mejor forma de realizar tareas administrativas. Consulte Inicio de sesión en la interfaz web de Panorama y Navegación en la interfaz web de Panorama. Si necesita habilitar el acceso HTTP a Panorama, edite la Configuración de interfaz de gestión en la pestaña **Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
- **Interfaz de línea de comandos (Command line interface, CLI)**: la CLI es una interfaz sencilla que le permite introducir los comandos con rapidez para completar una serie de tareas. La CLI admite dos modos de comandos (operativos y de configuración), cada uno de los cuales con su propia jerarquía de comandos e instrucciones. Cuando se familiariza con la estructura de anidamiento y la sintaxis de los comandos, la CLI permite tipos de respuesta rápidos y ofrece eficacia administrativa. Consulte Inicio de sesión en la CLI de Panorama.
- **API XML**: la API basada en XML se proporciona como servicio web implementado usando solicitudes y respuestas de HTTP/HTTPS. Le permite dinamizar las operaciones e integrarse con las aplicaciones y repositorios existentes desarrollados internamente. Para obtener información sobre cómo utilizar la API de Panorama, consulte la Guía de uso de la API XML de Panorama y PAN-OS.

Inicio de sesión en la interfaz web de Panorama

STEP 1 | Inicie un navegador de Internet e ingrese la dirección IP de Panorama con una conexión segura (https://<IP address>).

STEP 2 | Inicie sesión en Panorama según el tipo de autenticación que utilice su cuenta. Si inicia sesión en Panorama por primera vez, utilice el valor predeterminado **admin** como nombre de usuario y contraseña.

- **SAML:** haga clic en **Use Single Sign-On (SSO) (Utilizar el inicio de sesión único)**. Si Panorama realiza la autenticación (asignación de funciones) para los administradores, introduzca un nombre de usuario en **Username (Nombre de usuario)** y haga clic en **Continue (Continuar)**. Si el proveedor de identidad (identity provider, IdP) mediante SAML realiza la autorización, haga clic en **Continue (Continuar)** sin introducir ningún valor en **Username (Nombre de usuario)**. En ambos casos, Panorama le redirige al IdP, que le pide que introduzca un nombre de usuario y una contraseña. Después de la autenticación en el IdP, se muestra la interfaz web de Panorama.
- **Cualquier otro tipo de autenticación:** introduzca el nombre de su usuario en **Name (Nombre)** y la contraseña en **Password (Contraseña)**. Lea el banner de inicio de sesión y seleccione **I Accept and Acknowledge the Statement Below (Acepto el siguiente enunciado)** si la página de inicio de sesión tiene el banner y la casilla de verificación. Luego, haga clic en **Login (Iniciar sesión)**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Lea y haga clic en **Close (Cerrar)** para cerrar cualquier mensaje del día.

Navegación en la interfaz web de Panorama

Use la interfaz web de Panorama para configurar Panorama, gestionar y supervisar cortafuegos, recopiladores de logs, y dispositivos WildFire y clústeres de dispositivos, además de acceder a la interfaz web de cada cortafuegos mediante el menú desplegable **Context (Contexto)**. Consulte la ayuda en línea de Panorama para obtener detalles sobre las opciones y los campos en cada pestaña de interfaz web. Lo siguiente es una descripción general de las pestañas:

Pestaña	Description (Descripción)
Dashboard (Panel)	Visualice información general acerca del modelo de Panorama y la configuración de acceso a la red. Esta pestaña incluye widgets que muestran información sobre aplicaciones, logs, recursos del sistema y ajustes del sistema.
ACC	Visualice el nivel de riesgo y amenaza general de la red, basado en información que Panorama ha recopilado de los cortafuegos gestionados.
Monitor (Supervisar)	Visualice y gestione logs e informes.
Grupos de dispositivos > **Políticas**	Cree reglas de políticas centralizadas y aplíquelas a varios grupos de dispositivos/cortafuegos. Debe realizar la Adición de un grupo de dispositivos para que aparezca esta pestaña.
Grupos de dispositivos > **Objetos**	Defina los objetos de políticas a los que las reglas de políticas puedan hacer referencia y que los cortafuegos gestionados o grupos de dispositivos puedan compartir. Debe realizar la Adición de un grupo de dispositivos para que aparezca esta pestaña.
Plantillas > **Red**	Establezca la configuración de red, como los perfiles de red, y aplíquelos en múltiples cortafuegos. Debe realizar la Cómo añadir una plantilla para que aparezca esta pestaña.
Plantillas > **Dispositivo**	Establezca la configuración del dispositivo, como los perfiles de servidores y las funciones de administrador, y aplíquelos a múltiples cortafuegos. Debe realizar la Cómo añadir una plantilla para que aparezca esta pestaña.
Panorama	Configure Panorama, gestione licencias, establezca una alta disponibilidad, acceda a actualizaciones de software y alertas

 ©2023 Palo Alto Networks, Inc.

Pestaña	Description (Descripción)
	de seguridad, gestione el acceso administrativo y gestione los cortafuegos implementados, recopiladores de logs, y dispositivos WildFire y clústeres de dispositivos.

Inicio de sesión en la CLI de Panorama

Puede iniciar sesión en la CLI de Panorama usando una conexión de puerto de serie o remotamente usando un cliente de Shell seguro (Secure Shell, SSH).

- Utilice SSH para iniciar sesión en la CLI de Panorama.

  Se aplican las mismas instrucciones a un dispositivo de la serie M en el modo de recopilación de logs.

  También puede usar la opción de Configuración de un administrador con autenticación basada en claves de SSH para la CLI.

  1. Asegúrese de que se cumplen los siguientes requisitos previos:
     - Tiene un ordenador con acceso de red a Panorama.
     - Conoce la dirección IP de Panorama.
     - La interfaz de gestión admite SSH, la cual es la configuración predeterminada. Si un administrador ha deshabilitado SSH y desea volver a habilitarlo: seleccione **Panorama** > **Setup (Configuración)** > **Interfaces**, haga clic en **Management (Gestión)**, seleccione **SSH**, haga clic en **OK (Aceptar)**, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.
  2. Para acceder a la CLI usando SSH:
     1. Introduzca la dirección IP de Panorama en el cliente SSH y utilice el puerto 22.
     2. Introduzca las credenciales de acceso administrativo cuando se le soliciten. Después de iniciar sesión, se muestra el mensaje del día, seguido del mensaje de la CLI en modo operativo. Por ejemplo:

        ```
        admin@ABC_Sydney>
        ```


©2023 Palo Alto Networks, Inc.

- Utilice un puerto de serie para iniciar sesión en la CLI de Panorama.
  1. Asegúrese de contar con lo siguiente:
     - Un cable serie de módem nulo que conecta Panorama a un ordenador con un puerto de serie DB-9
     - Un programa de emulación de terminal instalado en el ordenador
  2. Utilice la siguiente configuración en el software de emulación para conectar: 9600 baudios, 8 bits de datos, 1 bit de terminación, sin paridad, sin control de flujo del hardware.
  3. Introduzca las credenciales de acceso administrativo cuando se le soliciten. Después de iniciar sesión, se muestra el mensaje del día seguido del mensaje de la CLI en modo operativo.

- Cambie al modo de configuración.

  Para cambiar al modo de configuración, introduzca el siguiente comando en el mensaje:

  ```
  admin@ABC_Sydney> configure
  ```

  El mensaje cambia a `admin@ABC_Sydney#`

 ©2023 Palo Alto Networks, Inc.

Configuración del acceso administrativo a Panorama

Panorama implementa Control de acceso basado en funciones (RBAC) para permitirle especificar los privilegios y las responsabilidades de los administradores. Los siguientes temas describen cómo crear funciones de administrador, dominios de acceso y cuentas para acceder a la interfaz web de Panorama y a la Interfaz de línea de comandos (Command line interface, CLI).

- Configuración de un perfil de función de administrador
- Configuración de un perfil de función de administración para envío selectivo en cortafuegos gestionados
- Configuración de un dominio de acceso
- Configurar cuentas y autenticación administrativa
- Configuración del seguimiento de la actividad del administrador

Configuración de un perfil de función de administrador

Los perfiles de función de administración son Funciones administrativas personalizados que le permiten definir los privilegios específicos de acceso administrativo para garantizar la protección de información confidencial de la empresa y la privacidad de los usuarios finales. Se recomienda crear perfiles de funciones de administrador que permitan a los administradores acceder únicamente a las áreas de las interfaces de gestión requeridas para realizar sus tareas.

STEP 1 | Seleccione **Device (Dispositivo)** > **Admin Roles (Funciones de administrador)** y seleccione la **Template (Plantilla)** en la cual configurar un admin role profile (perfil de función de administrador) del cortafuegos.

Debe crear un perfil de función de administración en el cortafuegos y asignarlo al perfil de la función de administrador del servidor de gestión Panorama para permitir que los administradores cambien el contexto entre Panorama y las interfaces web del cortafuegos gestionado.

STEP 2 | Seleccione **Panorama** > **Admin Roles (Funciones de administrador)** y haga clic en **Add (Añadir)**.

STEP 3 | Introduzca un nombre de perfil en **Name (Nombre)** y seleccione el tipo de función en **Role (Función)**: **Panorama** o **Device Group and Template (Grupo de dispositivos y plantilla)**.

STEP 4 | Configure los privilegios de acceso a cada área funcional de Panorama (**Web UI [IU web]**) alternando los íconos a la configuración deseada: Habilitar (lectura y escritura), Solo lectura o Deshabilitar.



*Si los administradores con funciones personalizadas compilarán cambios del grupo de dispositivos o plantillas en los cortafuegos gestionados, debe otorgar a estas funciones acceso de lectura y escritura a **Panorama** > **Device Groups (Grupos de dispositivos)** y **Panorama** > **Templates (Plantillas)**. Si actualiza desde una versión anterior de Panorama, el proceso de actualización otorga acceso de solo lectura a estos nodos.*

STEP 5 | Si el tipo de función en **Role (Función)** es **Panorama**, configure el acceso a **XML API (API XML)** alternando el icono de habilitado/deshabilitado para cada área funcional.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Si el tipo de función en **Role (Función)** es **Panorama**, seleccione un nivel de acceso para la interfaz **Command Line (Línea de comandos)**: **None (Ninguno)** (predeterminado), **superuser (superusuario)**, **superreader (superlector)** o **panorama-admin (administrador de Panorama)**.

STEP 7 | (Opcional) Para permitir que los administradores de **Panorama cambien de contexto** entre la interfaz web de Panorama y el cortafuegos, escriba el nombre de la **función de administrador del dispositivo** que configuró en el paso 1.

STEP 8 | Haga clic en **OK (Aceptar)** para guardar el perfil.

Configuración de un perfil de función de administración para envío selectivo en cortafuegos gestionados

Para permitir un mayor control de los cambios de configuración de los cortafuegos gestionados, cree un perfil de función de administración para permitir que un administrador de Panorama envíe la configuración de uno o más administradores de Panorama desde el servidor de administración de Panorama™ a los cortafuegos gestionados. Después de compilar cambios de configuración selectivos en Panorama, puede seleccionar cambios específicos del administrador de Panorama para revisar los cambios de configuración y, a continuación, enviar solo los cambios realizados por los administradores seleccionados a los cortafuegos gestionados. Aprovechar los envíos selectivos en cortafuegos gestionados también reduce el riesgo de enviar configuraciones de plantillas y grupos de dispositivos incompletas a cortafuegos gestionados al permitirle excluir explícitamente los cambios de configuración incompletos cuando se insertan en cortafuegos gestionados. Esto ayuda a mitigar y evitar posibles interrupciones y problemas relacionados con la configuración que podrían causar interrupciones en la red.

Los administradores con privilegios de función de administración Superusuario o Panorama pueden enviar y revisar los cambios a nivel de objeto de otros administradores de forma predeterminada. Sin embargo, puede modificar las funciones de administrador de Panorama para modificar los privilegios de configuración de nivel de objeto según sea necesario.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | (Opcional) Seleccione **Device (Dispositivo)** > **Admin Roles (Funciones de administración)** y seleccione la **Template (Plantilla)** en la cual configurar un admin role profile (perfil de función de administración) del cortafuegos.

Debe crear un perfil de función de administración en el cortafuegos y asignarlo al perfil de la función de administrador del servidor de gestión Panorama para permitir que los administradores cambien el contexto entre Panorama y las interfaces web del cortafuegos gestionado.

STEP 3 | Seleccione **Panorama** > **Admin Roles (Funciones de administración)** y **añada** una nueva función de administración.

STEP 4 | Introduzca un **nombre** descriptivo para la función de administración.

STEP 5 | Seleccione la función de administración **Panorama**.

STEP 6 | Seleccione la**Web UI** (Interfaz de usuario web) y desplácese hasta los privilegios de compilación.

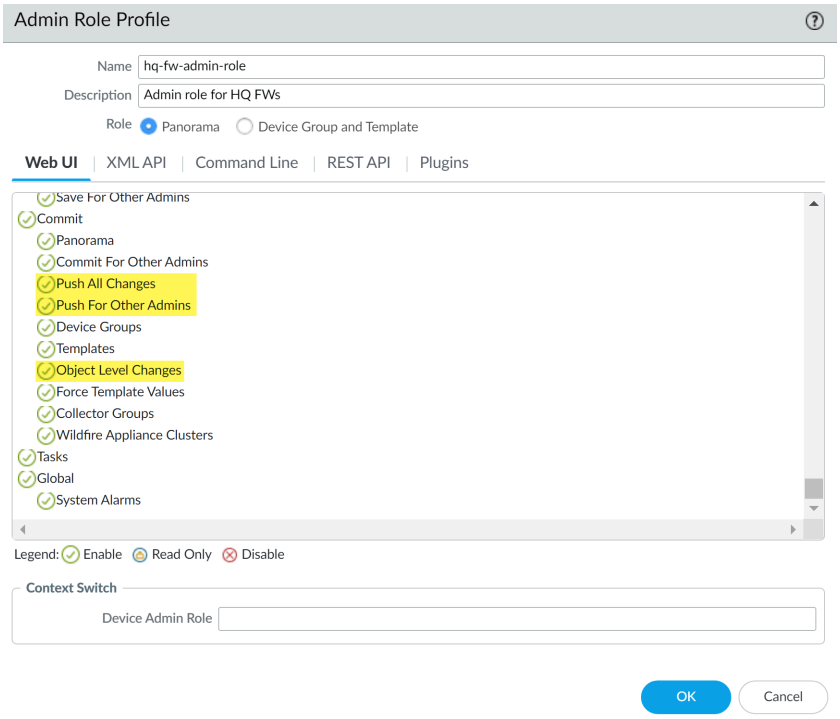
 ©2023 Palo Alto Networks, Inc.

STEP 7 | Configure los privilegios de configuración de nivel de objeto según sea necesario.

Todos los privilegios de configuración de nivel de objeto están habilitados de forma predeterminada.

Los privilegios predeterminados de la función de administración Superusuario o Panorama admiten privilegios de configuración de nivel de objeto completo.

- **Enviar todos los cambios:**permite al administrador enviar todos los cambios realizados por todos los administradores.
- **Enviar para otros administradores:**permite al administrador seleccionar y enviar los cambios de configuración realizados por otros administradores.
- **Cambios en el nivel de objeto:** permite al administrador ver los objetos de configuración individuales que desea enviar. Si está deshabilitada, la lista de objetos de configuración no se muestra en el alcance de envío.



STEP 8 | (Opcional) Para permitir que los administradores de **Panorama cambien de contexto** entre la interfaz web de Panorama y el cortafuegos, escriba el nombre de la **función de administrador del dispositivo** que configuró en el paso 1.

STEP 9 | Haga clic en **OK (Aceptar)**.

STEP 10 | Configure un administrador de Panorama personalizado y seleccione la **función de administración** que ha creado.

STEP 11 | Seleccione **Confirmar** y en **Confirmar en Panorama**.

 ©2023 Palo Alto Networks, Inc.

Configuración de un dominio de acceso

Use Dominios de acceso para definir el acceso de los administradores de grupos de dispositivos y plantillas para grupos de dispositivos y plantillas específicos, y también para controlar la capacidad de estos administradores para cambiar el contexto a la interfaz web de los cortafuegos gestionados. Panorama admite hasta 4.000 dominios de acceso.

STEP 1 | Seleccione **Panorama** > **Access Domain (Dominio de acceso)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un nombre en **Name (Nombre)** para identificar el dominio de acceso.

STEP 3 | Seleccione un privilegio de acceso para **Shared Objects (Objetos compartidos)**:

- **write (escritura)**: Los administradores pueden realizar todas las operaciones con objetos compartidos. Es el valor predeterminado.
- **read (lectura)**: Los administradores pueden mostrar y duplicar pero no pueden realizar otras operaciones en los objetos compartidos. Al añadir objetos no compartidos o duplicar objetos compartidos, el destino debe ser un grupo de dispositivos dentro del dominio de acceso, no en la ubicación Compartido.
- **shared-only (solo compartido)**: Los administradores pueden añadir objetos solo a la ubicación Compartido. Los administradores pueden mostrar, editar y eliminar objetos compartidos pero no pueden moverlos o duplicarlos.

> ***Si elige esta opción, los administradores no podrán realizar operaciones con objetos no compartidos excepto mostrarlos. Un ejemplo del motivo por el cual podría seleccionar esta opción es para una organización que requiere que todos los objetos estén en un único repositorio global.***

STEP 4 | Alterne los iconos en la pestaña **Device Groups (Grupos de dispositivos)** para habilitar el acceso de lectura y escritura o el de solo lectura para los grupos de dispositivos en el dominio de acceso.

> ***Si define el acceso Shared Objects (Objetos compartidos) en shared-only (solo compartido), Panorama aplica acceso de solo lectura a los objetos en cualquier grupo de dispositivos para el cual especifique el acceso de lectura y escritura.***

STEP 5 | Seleccione la pestaña **Templates (Plantillas)** y en **Add (Añadir)**, añada cada plantilla que desea asignar al dominio de acceso.

STEP 6 | Seleccione la pestaña **Device Context (Contexto del dispositivo)**, seleccione los cortafuegos que asignar al dominio de acceso y haga clic en **OK (Aceptar)**. Los administradores pueden acceder a la interfaz web de estos cortafuegos usando el menú desplegable **Context (Contexto)** en Panorama.

Configurar cuentas y autenticación administrativa

Si ya ha configurado un perfil de autenticación o no necesita uno para autenticar administradores, está listo para Configuración de una cuenta de administrador de Panorama.. De lo contrario, realice uno de los siguientes procedimientos que se enumeran a continuación para configurar cuentas administrativas para tipos específicos de autenticación.

 ©2023 Palo Alto Networks, Inc.

- Configuración de una cuenta de administrador de Panorama.
- Configuración de la autenticación local o externa para los administradores de Panorama.
- Configuración de un administrador de Panorama con autenticación basada en certificado para la interfaz web
- Configuración de un administrador con autenticación basada en claves de SSH para la CLI
- Configuración de la autenticación de RADIUS para los administradores de Panorama
- Configuración de la autenticación de TACACS+ para los administradores de Panorama
- Configuración de la autenticación de SAML para los administradores de Panorama

Configuración de una cuenta de administrador de Panorama.

Las cuentas administrativas especifican las Funciones administrativas y la autenticación para los administradores de Panorama. El servicio que utiliza para asignar funciones y realizar la autenticación determina si añade las cuentas a Panorama, a un servidor externo o a ambos (consulte Autenticación administrativa). Para un servicio de autenticación externo, debe configurar un perfil de autenticación antes de añadir una cuenta administrativa (consulte Configuración de cuentas administrativas y autenticación). Si ya configuró el perfil de autenticación o si va a utilizar el mecanismo de autenticación que es local para Panorama, realice los siguientes pasos para añadir una cuenta administrativa a Panorama.

STEP 1 | Modifique la cantidad de cuentas de administrador admitidas.

Configure la cantidad total de sesiones simultáneas admitidas de cuentas administrativas para Panorama en el modo de operación normal o en el modo FIPS-CC. Puede permitir hasta cuatro

 ©2023 Palo Alto Networks, Inc.

sesiones simultáneas de cuentas administrativas o configurar Panorama para que admita una cantidad ilimitada de sesiones simultáneas de cuentas administrativas.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de autenticación.
2. Edite **Max Session Count (Recuento máximo de sesiones)** para especificar la cantidad de sesiones simultáneas admitidas (el rango es de **0** a **4**) que se permiten para todas las cuentas de administrador y usuario.

   Ingrese **0** para configurar Panorama de modo que admita una cantidad ilimitada de cuentas administrativas.
3. Edite el tiempo en **Max Session Time (Tiempo máximo de sesión)** en minutos para una cuenta administrativa. El valor predeterminado es `720` minutos.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Confirmar** y en **Confirmar en Panorama**.

También puede configurar la cantidad total de sesiones simultáneas admitidas iniciando sesión en la CLI de Panorama.

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# commit
```

STEP 2 | Seleccione **Panorama** > **Administrators (Administradores)** y **Add (Añadir)** para añadir una cuenta.

STEP 3 | Introduzca un **Name (Nombre)** para el administrador.

STEP 4 | Seleccione un **Authentication Profile (Perfil de autenticación)** o una secuencia si ha configurado alguno de ellos para el administrador.

Esto es necesario si Panorama usa un SSO de Kerberos o un servicio externo para la autenticación.

Si Panorama utilizará la autenticación local, configure el **Authentication Profile (Perfil de autenticación)** en **None (Ninguno)** e introduzca una **Password (Contraseña)** y luego **Confirm Password (Confirmar contraseña)**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Seleccione el **Administrator Type (Tipo de administrador)**.

- **Dynamic (Dinámico)**: seleccione un rol de administrador predefinido.
- **Custom Panorama Admin (Administrador de Panorama personalizado)**: seleccione el **Profile (Perfil)** de la función de administrador que creó para este administrador (consulte Configuración de un perfil de función de administrador).
- **Device Group and Template Admin (Administrador de plantillas y grupo de dispositivos)**: Asignan los dominios de acceso a funciones administrativas como se describe en el siguiente paso.

STEP 6 | (Solo grupo de dispositivos y Administrador de plantillas) En la sección Acceso a la función de administrador del dominio, haga clic en **Add (Añadir)**, seleccione un dominio de acceso del menú desplegable (consulte Configurar un dominio de acceso), haga clic en la casilla Función de administrador adyacente y seleccione un perfil de función de administrador.

STEP 7 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 8 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

Configuración de la autenticación local o externa para los administradores de Panorama.

Puede usar un servicio de autenticación externo o el servicio que es local a Panorama para autenticar a los administradores que acceden a Panorama. Estos métodos de autenticación les piden a los administradores que respondan a uno o más desafíos de autenticación, como una página de inicio de sesión en la que introduce un nombre de usuario y una contraseña.

Si utiliza un servicio externo para gestionar la autenticación y la autorización (asignaciones de funciones y dominios de acceso), consulte las siguientes secciones:

- Configuración de la autenticación de RADIUS para los administradores de Panorama
- Configuración de la autenticación de TACACS+ para los administradores de Panorama
- Configuración de la autenticación de SAML para los administradores de Panorama

Para autenticar a los administradores sin un mecanismo de respuesta a desafíos, puede realizar la Configuración de una autenticación de administrador basada en certificados en la interfaz web *y la* Configuración de un administrador con autenticación basada en claves de SSH para la CLI.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | (Solo autenticación externa) Permita que Panorama se conecte a un servidor externo para autenticar a los administradores.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)**, seleccione el tipo de servicio (**RADIUS**, **TACACS+**, **SAML**, **LDAP** o **Kerberos**) y configure el perfil de servidor:
   - Configuración de la autenticación de RADIUS para los administradores de Panorama.

     Puede utilizar un servidor RADIUS para admitir servicios de autenticación de RADIUS o servicios de autenticación multifactor (MFA)**.**
   - Configuración de la autenticación de TACACS+ para los administradores de Panorama.
   - Añada un perfil de servidor SAML IdP. No puede combinar el inicio de sesión único (single sign-on, SSO) mediante Kerberos con SSO mediante SAML, ya que solo puede utilizar un tipo de servicio de SSO.
   - Añada un perfil de servidor Kerberos.
   - Añada un perfil de servidor LDAP.

STEP 2 | (Opcional) Defina la complejidad de la contraseña y la configuración de caducidad si Panorama utiliza la autenticación local.

Esta configuración puede ayudar a proteger Panorama contra el acceso no autorizado al hacer más difícil que los atacantes adivinen las contraseñas.

1. Define la complejidad de la contraseña global y los ajustes de vencimiento para todos los administradores locales.
   1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de complejidad de contraseña mínima.
   2. Seleccione **Enabled (Habilitado)**.
   3. Defina los ajustes de la contraseña y haga clic en **OK (Aceptar)**.
2. Defina un perfil de contraseña.

   Asigna el perfil a las cuentas administrativas en las que desea anular la configuración de vencimiento de contraseña global.
   1. Seleccione **Panorama** > **Password Profiles (Perfiles de contraseña)** y luego **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil.
   3. Defina los ajustes de vencimiento de la contraseña y haga clic en **OK (Aceptar)**.

STEP 3 | (Solo SSO de Kerberos) Cree una keytab de Kerberos.

Un keytab es un archivo que contiene información de cuenta de Kerberos para Panorama. Para respaldar el SSO de Kerberos, su red debe contar con una infraestructura Kerberos.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure un perfil de autenticación.



Si las cuentas administrativas están almacenadas en varios tipos de servidores, puede crear un perfil de autenticación para cada tipo y añadir todos los perfiles a una secuencia de autenticación*.*

En el perfil de autenticación, especifique el **Type (Tipo)** de servicio de autenticación y la configuración relacionada:

- **Servicio externo:** seleccione el **Type (Tipo)** de servicio externo y seleccione el **Server Profile (Perfil de servidor)** que creó para él.
- **Autenticación local**: configure el **Type (Tipo)** como **None (Ninguno)**.
- **SSO de Kerberos**: especifique el **Kerberos Realm (Dominio Kerberos)** y seleccione **Import (Importar)** para importar el **Kerberos Keytab** que creó.

STEP 5 | (Solo grupos de dispositivos y administradores de plantillas) Configure un dominio de acceso.

Configure uno o más dominios de acceso.

STEP 6 | (Solo funciones personalizadas) Configure un perfil de función de administrador.

Configure uno o más perfiles de función de administrador.

Para los administradores de Panorama personalizados, el perfil define los privilegios de acceso para la cuenta. Para los administradores de plantillas y grupos de dispositivos, el perfil define los privilegios de acceso para uno o más dominios de acceso asociados con la cuenta.

STEP 7 | Configure un administrador.

1. Configure una cuenta de administrador de Panorama..
   - Asigne el **Authentication Profile (Perfil de autenticación)** o la secuencia que configuró.
   - (Solo grupos de dispositivos y administrador de plantillas) Asigne los dominios de acceso a los perfiles de función de administrador.
   - (Solo autenticación local) Seleccione un **Password Profile (Perfil de contraseña)** si configuró uno.
2. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.
3. (Opcional) Realice la Comprobación de la conectividad del servidor de autenticación para comprobar que el cortafuegos puede utilizar el perfil de autenticación para autenticar a los administradores.

Configuración de un administrador de Panorama con autenticación basada en certificado para la interfaz web

Como una alternativa más segura a la autenticación basada en contraseña para la interfaz web de Panorama, puede configurar una autenticación basada en certificado para las cuentas de administradores que sean locales en Panorama. La autenticación basada en certificados implica el intercambio y verificación de una firma digital en lugar de una contraseña.

 ©2023 Palo Alto Networks, Inc.

Configurar una autenticación basada en certificado para cualquier administración deshabilita los inicios de sesión con nombre de usuario y contraseña para todos los administradores en panorama y, por consiguiente, todos los administradores requieren la certificación para iniciar sesión.

STEP 1 | Genere un certificado de la Autoridad de certificado (certificate authority, CA) en Panorama.

Puede usar este certificado de CA para firmar el certificado de cliente de cada administrador.

Cree un certificado de CA raíz autofirmado.

De manera alternativa, puede importar un certificado *desde la CA de su empresa.*

STEP 2 | Configure un perfil de certificado para proteger el acceso a la interfaz web.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el perfil de certificado en **Name (Nombre)** y configure **Username Field (Campo de nombre de usuario)** en **Subject (Tema)**.
3. Seleccione **Add (Añadir)** en la sección Certificados de CA y seleccione el certificado de CA que acaba de crear en **CA Certificate (Certificado de CA)**.
4. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Configure Panorama para que use el perfil de certificado para autenticar administradores.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de autenticación.
2. Seleccione el perfil de certificado que acaba de crear en **Certificate Profile (Perfil del certificado)** y haga clic en **OK (Aceptar)**.

STEP 4 | Configure las cuentas de administrador para usar la autenticación de certificado cliente.

Configuración de una cuenta de administrador de Panorama. para cada administrador que accederá a la interfaz web de Panorama. Seleccione la casilla de verificación **Use only client certificate authentication (Web) (Solo usar la autenticación de certificado cliente [Web])**.

Si ya ha implementado certificados de cliente que ha generado su CA de empresa, vaya al Paso 8. De lo contrario, continúe con el Paso 5.

STEP 5 | Genere un certificado de cliente para cada administrador.

Genere un certificado en Panorama. En el menú desplegable **Signed By (Firmado por)**, seleccione el certificado de CA que creó.

STEP 6 | Exporte los certificados de cliente.

1. Exporte los certificados.
2. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

   Panorama reinicia y finaliza su sesión. Así, los administradores pueden acceder a la interfaz web únicamente desde sistemas cliente que tengan el certificado de cliente que ha generado.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Importe el certificado de cliente en el sistema cliente de cada administrador que vaya a acceder a la interfaz web.

Consulte la documentación de su navegador web según sea necesario para completar este paso.

STEP 8 | Verifique que los administradores pueden acceder a la interfaz web.

1. Abra la dirección IP de Panorama en un navegador del ordenador que tenga el certificado de cliente.
2. Cuando se le indique, seleccione el certificado que ha importado y haga clic en **OK**. El explorador muestra una advertencia de certificado.
3. Añada el certificado a la lista de excepciones del explorador.
4. Haga clic en **Login (Inicio de sesión)**. La interfaz web debería aparecer sin pedirle un nombre de usuario o contraseña.

Configuración de un administrador con autenticación basada en claves de SSH para la CLI

Para los administradores que usan Shell seguro (Secure Shell, SSH) para acceder a la CLI de Panorama, las claves SSH proporcionan un método de autenticación más seguro que las contraseñas. Las claves SSH prácticamente eliminan el riesgo de ataques de fuerza bruta, ofrecen la posibilidad de una autenticación de dos factores (clave privada y frase de contraseña) y no envían contraseñas por la red. Las claves SSH también permiten que las secuencias de comandos automatizadas accedan al CLI.

STEP 1 | Utilice una herramienta de generación de claves de SSH para crear un par de claves asimétricas en el sistema cliente del administrador.

Los formatos de clave admitidos son IETF SECSH y Open SSH. Los algoritmos admitidos son DSA (1024 bits) y RSA (768-4096 bits).

Para que los comandos generen el par de claves, consulte la documentación de su cliente SSH.

La clave pública y la privada son archivos distintos. Guarde ambos en una ubicación a la que Panorama pueda acceder. Para una mayor seguridad, introduzca una frase de contraseña para cifrar la clave privada. Panorama solicita al administrador esta frase de contraseña durante el inicio de sesión.

STEP 2 | Configure la cuenta del administrador para usar la autenticación de clave pública.

1. Configuración de una cuenta de administrador de Panorama..
   - Configure uno o dos métodos de autenticación para utilizar como reserva si la autenticación con clave SSH falla:

     Servicio de autenticación externo: seleccione un **Authentication Profile (Perfil de autenticación)**.

     Autenticación local: Configure el **Authentication Profile (Perfil de autenticación)** en **None (Ninguno)** e introduzca una **Password (Contraseña)**, y seleccione **Confirm Password (Confirmar contraseña)**.
   - Seleccione la casilla de verificación **Use Public Key Authentication (SSH) (Usar la autenticación de clave pública [SSH])**, haga clic en **Import Key (Importar clave)** y en

 ©2023 Palo Alto Networks, Inc.

Browse (Explorar) para navegar hasta la clave pública que acaba de generar, y haga clic en **OK (Aceptar)**.

2. Haga clic en **OK (Aceptar)** para guardar la cuenta.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 3 | Configure el cliente SSH para utilizar la clave privada para autenticar en Panorama.

Realice esta tarea en el sistema cliente del administrador. Consulte la documentación de su cliente SSH según sea necesario para completar este paso.

STEP 4 | Verifique que el administrador pueda acceder a la CLI de Panorama mediante la autenticación de clave SSH.

1. Use un navegador en el sistema cliente del administrador para ir a la dirección IP de Panorama.
2. Inicie de sesión en la CLI de Panorama como administrador. Después de escribir un nombre de usuario, verá la siguiente salida (el valor de clave es un ejemplo):

   ```
   Authenticating with public key “dsa-key-20130415”
   ```
3. Si se le solicita, introduzca la frase de contraseña definida al crear las claves.

Configuración de la autenticación de RADIUS para los administradores de Panorama

Puede usar un servidor RADIUS para autenticar el acceso administrativo a la interfaz web de Panorama. También puede definir Atributos específicos de proveedor (VSA) en el servidor RADIUS para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.



Puede usar un servidor RADIUS para autenticar el acceso administrativo a la interfaz web de Panorama. También puede definir Atributos específicos de proveedor (VSA) en el servidor RADIUS para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

Importe el diccionario de RADIUS de Palo Alto Networks al servidor RADIUS con objeto de definir los atributos de autenticación necesarios para facilitar la comunicación entre Panorama y dicho servidor.

También puede usar un servidor RADIUS para implementar la autenticación multifactor (MFA) para los administradores.

STEP 1 | Añada un perfil de servidor RADIUS.

El perfil define de qué manera Panorama se conecta con el servidor RADIUS.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** y haga clic en **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.

 ©2023 Palo Alto Networks, Inc.

3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).

   Si utiliza el perfil del servidor para integrar Panorama con un servicio MFA, introduzca un intervalo que proporcione a los administradores tiempo suficiente para responder al desafío de autenticación. Por ejemplo, si el servicio MFA solicita una única contraseña (OTP), los administradores necesitan tiempo para ver la OTP en su dispositivo de endpoint y, a continuación, introducir la OTP en la página de inicio de sesión de MFA.

4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que Panorama utiliza para autenticarse en el servidor RADIUS.

   *Seleccione **CHAP** si el servidor RADIUS admite ese protocolo; es más seguro que **PAP**.*

5. Seleccione **Add (Añadir)** para añadir cada servidor RADIUS e ingrese lo siguiente:
   - Un nombre en **Name** para identificar el servidor.
   - La dirección IP o FQDN del **RADIUS Server (Servidor RADIUS)**.
   - **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
   - El **Port (Puerto)** del servidor para las solicitudes de autenticación (el valor predeterminado es 1812).
6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Asigne el perfil del servidor RADIUS a un perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
3. Configure el **Type (Tipo)** en **RADIUS**.
4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
5. Seleccione **Retrieve user group from RADIUS (Recuperar grupo de usuarios desde RADIUS)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor RADIUS.

   Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure Panorama para que utilice el perfil de autenticación para todos los administradores.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de autenticación.
2. Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró y haga clic en **OK (Aceptar)**.

STEP 4 | Configure los roles y dominios de acceso que definen los ajustes de autorización para los administradores.

1. Configure un perfil de rol de administrador si el administrador utiliza un rol personalizado en lugar de un rol predefinido (dinámico).
2. Configure un dominio de acceso si el administrador utiliza una función de grupo de dispositivos y plantilla.

STEP 5 | Confirme los cambios.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 6 | Configure el servidor RADIUS.

Consulte la documentación de su servidor RADIUS a fin de obtener instrucciones específicas para realizar los siguientes pasos:

1. Añada la dirección IP o el nombre de host de Panorama como cliente de RADIUS.
2. Añada las cuentas de administrador.

   Si el perfil de servidor RADIUS especifica CHAP como el Authentication Protocol (Protocolo de autenticación), debe definir cuentas con** contraseñas cifradas de manera reversible**. De lo contrario, la autenticación CHAP fallará.

3. Defina el código de proveedor para Panorama (25461) y defina los VSA RADIUS para el rol, el dominio de acceso y el grupo de usuario de cada administrador.

   Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba **`superuser (superusuario)`**, no **`SuperUser (SuperUsuario)`**.

STEP 7 | Verifique que el servidor RADIUS realice la autenticación y autorización de los administradores.

1. Inicie sesión en la interfaz web de Panorama usando una cuenta de administrador que haya añadido al servidor RADIUS.
2. Verifique que pueda acceder solo a las páginas de la interfaz web que están permitidas para el rol que usted asoció con el administrador.
3. En las pestañas **Monitor (Supervisar)**, **Policies (Políticas)** y **Objects (Objetos)**, verifique que puede acceder únicamente a los grupos de dispositivos que están permitidos para el dominio de acceso que asoció con el administrador.

Configuración de la autenticación de TACACS+ para los administradores de Panorama

Puede usar un servidor TACACS para autenticar el acceso administrativo a la interfaz web de Panorama. También puede definir Atributos específicos de proveedor (VSA) en el servidor TACACS+ para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez

 ©2023 Palo Alto Networks, Inc.

las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

STEP 1 | Añada un perfil de servidor TACACS+.

El perfil define de qué manera Panorama se conecta con el servidor TACACS+.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACACS+** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que Panorama utiliza para autenticarse en el servidor TACACS+.

   *Seleccione **CHAP** si el servidor TACACS+ admite ese protocolo; es más seguro que **PAP**.*
5. Seleccione **Add (Añadir)** para añadir cada servidor TACACS+ e ingrese lo siguiente:
   - Un nombre en **Name** para identificar el servidor.
   - La dirección IP o FQDN del **TACACS+ Server (Servidor TACACS+)**.
   - **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
   - El **Port (Puerto)** del servidor para las solicitudes de autenticación (el valor predeterminado es 49).
6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Asigne el perfil del servidor TACACS+ a un perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Configure el **Type (Tipo)** en **TACACS+**.
4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
5. Seleccione **Retrieve user group from TACACS+ (Recuperar grupo de usuarios desde TACACS+)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor TACACS+.

   Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure Panorama para que utilice el perfil de autenticación para todos los administradores.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de autenticación.
2. Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró y haga clic en **OK (Aceptar)**.

STEP 4 | Configure los roles y dominios de acceso que definen los ajustes de autorización para los administradores.

1. Configure un perfil de rol de administrador si el administrador utilizará un rol personalizado en lugar de un rol predefinido (dinámico).
2. Configure un dominio de acceso si el administrador utiliza una función de grupo de dispositivos y plantilla.

STEP 5 | Confirme los cambios.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 6 | Configure el servidor TACACS+ para que autentique y autorice administradores.

Consulte la documentación de su servidor TACACS+ a fin de obtener instrucciones específicas para realizar los siguientes pasos:

1. Añada la dirección IP o el nombre de host de Panorama como cliente de TACACS+.
2. Añada las cuentas de administrador.

   *Si seleccionó **CHAP** como el **Authentication Protocol (Protocolo de autenticación)**, debe definir cuentas con contraseñas cifradas de manera reversible. De lo contrario, la autenticación CHAP fallará.*
3. Defina VSA TACACS+ para el rol, dominio de acceso y grupo de usuario de cada administrador.

   *Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba **`superuser (superusuario)`**, no **`SuperUser (SuperUsuario)`**.*

STEP 7 | Verifique que el servidor TACACS+ realice la autenticación y autorización de los administradores.

1. Inicie sesión en la interfaz web de Panorama usando una cuenta de administrador que haya añadido al servidor TACACS+.
2. Verifique que pueda acceder solo a las páginas de la interfaz web que están permitidas para el rol que usted asoció con el administrador.
3. En las pestañas **Monitor (Supervisar)**, **Policies (Políticas)** y **Objects (Objetos)**, verifique que puede acceder únicamente a los sistemas virtuales que están permitidos para el dominio de acceso que asoció con el administrador.

Configuración de la autenticación de SAML para los administradores de Panorama

Puede usar el Lenguaje de marcado de aserción de seguridad (SAML) 2.0 para el acceso administrativo a la interfaz web de Panorama (pero no a la CLI). También puede usar atributos SAML

 ©2023 Palo Alto Networks, Inc.

para gestionar la autorización del administrador. Los atributos de SAML le permiten cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, en lugar de volver a configurar el cortafuegos y Panorama.

Para configurar el inicio de sesión único (single sign-on, SSO) y el cierre de sesión único (single logout, SLO) mediante SAML, debe registrar Panorama y el proveedor de identidad (identity provider, IdP) entre sí para habilitar su comunicación. Si el IdP proporciona un archivo de metadatos que contiene información de registro, usted puede importarlo Panorama para registrar el IdP y crear un perfil de servidor IdP. El perfil de servidor define cómo conectarse con el IdP y especifica el certificado que el IdP utiliza para firmar los mensajes de SAML. También puede usar un certificado para que Panorama firme los mensajes de SAML. La utilización de certificados es opcional, pero lo recomendamos para asegurar las comunicaciones entre Panorama y el IdP.

STEP 1 | (Recomendado) Obtenga los certificados que el IdP y Panorama utilizarán para firmar los mensajes de SAML.

Si los certificados no especifican atributos de uso clave, todos los usos se permitirán de manera predeterminada, incluidos los mensajes de firmas. En este caso, usted puede obtener certificados mediante cualquier método.

Si el certificado especifica atributos de uso de clave, uno de los atributos debe ser la firma digital, que no está disponible en los certificados que usted genera en Panorama. En este caso, debe importar los certificados:

- **Certificado que Panorama utiliza para firmar mensajes de SAML:** importe el certificado desde la autoridad de certificados (certificate authority, CA) de su empresa o una CA de terceros.
- **Certificado que el IdP utiliza para firmar mensajes de SAML:** importe un archivos de metadatos que contenga el certificado del IdP (consulte el paso a continuación). El certificado IdP está limitado a los siguientes algoritmos:
  - **Public key algorithms (Algoritmos de clave pública)**: RSA (1.024 bits o mayor) y ECDSA (todos los tamaños).
  - **Signature algorithms (Algoritmos de firma)**: SHA1, SHA256, SHA384 y SHA512.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada un perfil de servidor SAML IdP.

El perfil de servidor registra el IdP en Panorama y define cómo se conectan.

En este ejemplo, usted importa un archivos de metadatos de SAML desde el IdP, de manera que Panorama puede crear automáticamente un perfil de servidor y completar la información de conexión, registro y certificado de IdP.

*Si el IdP no proporciona un archivo de metadatos, seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad de SAML)** y haga clic en **Add (Añadir)** para añadir el perfil de servidor, e introduzca manualmente la información (consulte a su administrador de IdP para obtener los valores).*

1. Exporte el archivo de metadatos desde el IdP a un sistema cliente al cual Panorama pueda acceder.

   El certificado especificado en el archivo debe reunir los requisitos enumerados en el paso anterior. Consulte su documentación de IdP para obtener instrucciones sobre cómo exportar el archivo.
2. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad de SAML)** y haga clic en **Import (Importar)** para importar el archivo de metadatos en Panorama.
3. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
4. Seleccione **Browse (Examinar)** para buscar el archivo de **Identity Provider Metadata (Metadatos de proveedor de identidad)**.
5. (Recomendado) Seleccione **Validate Identity Provider Certificate (Validar certificado de proveedor de identidad)** (valor predeterminado) para que Panorama valide el **Identity Provider Certificate (Certificado de proveedor de identidad)**.

   La validación se produce después de asignar el perfil del servidor a un perfil de autenticación y **Commit (Confirmar)**. Panorama utiliza el **perfil de certificado** en el perfil de autenticación para validar el certificado.

   La validación del certificado es una práctica recomendada para lograr mayor seguridad.
6. Ingrese el **Maximum Clock Skew (Desplazamiento de reloj máximo)**, que es la diferencia permitida en segundos entre los tiempos del sistema del IdP y Panorama al momento en que Panorama valida los mensajes de IdP (el valor predeterminado es 60; el intervalo es de 1 a 900). Si la diferencia supera este valor, la autenticación falla.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
8. Haga clic en el nombre del perfil de servidor para que aparezcan los ajustes del perfil. Verifique que la información importada sea correcta y modifíquela si fuera necesario.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure un perfil de autenticación.

El perfil de autenticación especifica un perfil de servidor SAML IdP y define opciones para el proceso de autenticación, como SLO.

1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Configure el **Type (Tipo)** en **SAML**.
4. Seleccione el **IdP Server Profile (Perfil de servidor IdP)** que configuró.
5. Seleccione el **Certificate for Signing Requests (Certificado para las solicitudes de firma)**.

   Panorama utiliza este certificado para firmar mensajes que envía al IdP.
6. (Opcional) **Enable Single Logout (Habilitar cierre de sesión único)** (está inhabilitado de manera predeterminada).
7. Seleccione el **Certificate Profile (Perfil de certificado)** que Panorama utilizará para validar el **Identity Provider Certificate (Certificado de proveedor de identidad)**.
8. Ingrese el **Username Attribute (Atributo de nombre de usuario)** que los mensajes de IdP utilizan para identificar a los usuarios (el valor predeterminado es **`username [nombre de usuario]`**).

   *Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba **`superuser (superusuario)`**, no **`SuperUser (SuperUsuario)`**. Si gestiona la autorización de administrador a través del almacén de identidades, especifique el **Admin Role Attribute (Atributo de rol de administrador)** y también el **Access Domain Attribute (Atributo de dominio de acceso).***
9. Seleccione **Advanced (Avanzado)** y **Add (Añadir)** para añadir los administradores que pueden autenticarse con este perfil de autenticación.
10. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure Panorama para que utilice el perfil de autenticación para todos los administradores.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**, edite la configuración de autenticación y seleccione el **Authentication Profile (Perfil de autenticación)** que configuró.
2. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** para activar sus cambios en Panorama y validar el **Identity Provider Certificate (Certificado de proveedor de identidad)** que asignó al perfil del servidor SAML IdP.

 ©2023 Palo Alto Networks, Inc.

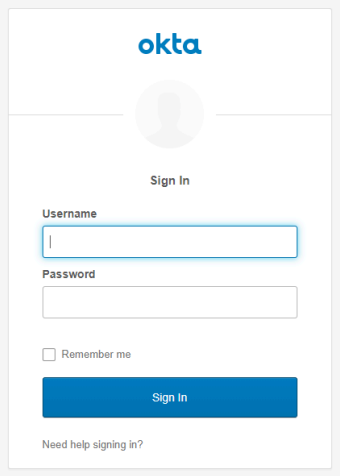
STEP 5 | Cree un archivo de metadatos SAML para registrar Panorama en el IdP.

1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y, en la columna Authentication (Autenticación) del perfil de autenticación que configuró, haga clic en **Metadata (Metadatos)**.
2. Establezca **Management Choice (Opción de gestión)** en **Interface (Interfaz)** (predeterminado está seleccionado) y seleccione la interfaz de gestión (MGT).
3. Haga clic en **OK (Aceptar)** y guarde el archivo de metadatos en su sistema cliente.
4. Importe el archivo de metadatos al servidor de IdP para registrar Panorama Consulte la documentación del IdP para obtener instrucciones.

STEP 6 | Compruebe que los administradores puedan autenticarse usando el SSO de SAML.

1. Vaya a la URL de la interfaz web de Panorama.
2. Haga clic en **Use Single Sign-On (Usar inicio de sesión único)**.
3. Haga clic en **Continue (Continuar)**.

   Panorama lo redirigirá para autenticarse en el IdP, que muestra una página de inicio de sesión. Por ejemplo:



4. Inicie sesión usando su nombre de usuario y contraseña de SSO.

   Una vez autenticado correctamente en el IdP, será redirigido nuevamente a Panorama, que mostrará la interfaz web.
5. Utilice su cuenta de administrador de Panorama para solicitar acceso a otra aplicación de SSO.

   El acceso correcto indica que la autenticación de SSO SAML se realizó correctamente.

Configuración del seguimiento de la actividad del administrador

Realice un seguimiento de la actividad del administrador en la interfaz web y la CLI de su servidor de gestión Panorama™, cortafuegos gestionados y recopiladores de logs para lograr informes en tiempo real de la actividad en toda la implementación. Si tiene razones para creer que una cuenta de administrador está comprometida, tiene un historial completo de la navegación de esta cuenta de administrador por la interfaz web o qué comandos operativos se ejecutaron para que pueda analizar en detalle y responder a todas las acciones que tomó el administrador comprometido.

 ©2023 Palo Alto Networks, Inc.

Cuando se produce un evento, se genera un log de auditoría y se reenvía al servidor syslog especificado cada vez que un administrador navega por la interfaz web o cuando se ejecuta un comando operativo en la CLI. Se genera un log de auditoría para cada navegación o comando ejecutado. Por ejemplo, si desea crear un nuevo objeto de dirección. Se genera un log de auditoría cuando hace clic en **Objects (Objetos)**, y se genera un segundo log de auditoría cuando hace clic en Addresses (Direcciones).

Los logs de auditoría solo son visibles como syslogs reenviados a su servidor syslog y no se pueden ver en la interfaz web del cortafuegos gestionado o Panorama. Los logs de auditoría solo se pueden reenviar a un servidor syslog, no se pueden reenviar a Cortex Data Lake (CDL) y no se almacenan localmente en el cortafuegos, Panorama o recopilador de logs.

STEP 1 | Configure un perfil de servidor syslog para reenviar los logs de auditoría de la actividad del administrador para Panorama, cortafuegos gestionados y recopiladores de logs.

Este paso es necesario para almacenar correctamente los logs de auditoría a fin de realizar un seguimiento de la actividad del administrador.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **Syslog** y haga clic en **Add (Añadir)** para agregar un nuevo perfil de servidor Syslog.
2. Configure un perfil de servidor syslog.

STEP 2 | Configure el seguimiento de la actividad del administrador para el cortafuegos gestionado.

Este paso es necesario para almacenar correctamente los logs de auditoría a fin de realizar un seguimiento de la actividad del administrador en los cortafuegos gestionados.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de registro e informes.
2. Configure el seguimiento de la actividad del administrador.
3. Seleccione **Commit (Compilar)** y **Commit and Push (Compilar y enviar)**.

STEP 3 | Configure el seguimiento de la actividad del administrador para Panorama.

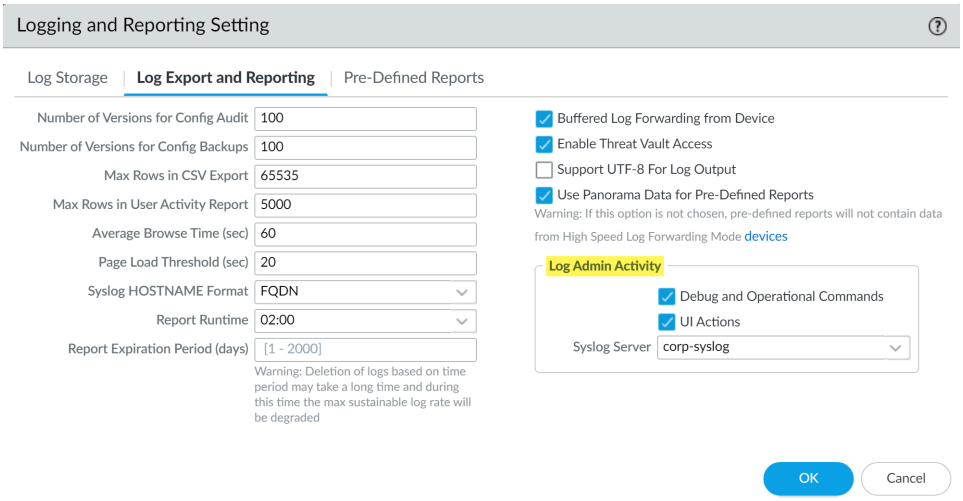
1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de logs e informes.
2. Seleccione **Log Export and Reporting (Exportación de logs e informes)**.
3. En la sección “Log Admin Activity” (Actividad de administración de logs), configure la actividad de administrador de la cual realizará un seguimiento.
   - **Comandos operativos**: genere un log de auditoría cuando un administrador ejecute un comando operativo o de depuración en la CLI o un comando operativo activado desde la interfaz web. Consulte la Jerarquía de comandos operativos de la CLI para obtener una lista completa de los comandos operativos y de depuración de PAN-OS.
   - **Acciones de la interfaz de usuario**: genere un log de auditoría cuando un administrador navega por la interfaz web. Esto incluye la navegación entre pestañas de configuración, así como objetos individuales dentro de una pestaña.

     Por ejemplo, se genera un log de auditoría cuando un administrador navega desde el **ACC** hasta la pestaña **Policies (Políticas)**. Además, se genera un log de auditoría cuando un administrador navega de **Objects (Objetos)** > **Addresses (Direcciones)** a**Objects (Objetos)** > **Tags (Etiquetas)**.

 ©2023 Palo Alto Networks, Inc.

- **Servidor Syslog**: seleccione un perfil de servidor Syslog de destino para reenviar los registros de auditoría.

4. Haga clic en **OK (Aceptar)**.



5. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 4 | Configure el seguimiento de la actividad del administrador para un recopilador de logs.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y elija el recopilador de logs.
2. Seleccione **Audit (Auditar)**.
3. En la sección “Log Admin Activity” (Actividad de administración de logs), configure el seguimiento de auditoría de la actividad de la CLI.

   Solo puede realizar un seguimiento de la actividad de la CLI para los recopiladores de logs, ya que estos solo pueden acceder a los recopiladores de logs a través de la CLI.

   - **Comandos operativos**: generan un log de auditoría cuando un administrador ejecuta un comando operativo o de depuración en la CLI. Consulte la Jerarquía de comandos operativos de la CLI para obtener una lista completa de los comandos operativos y de depuración de PAN-OS.
   - **Servidor Syslog**: seleccione un perfil de servidor Syslog de destino para reenviar los registros de auditoría.
4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

 ©2023 Palo Alto Networks, Inc.

Configuración de la autenticación mediante certificados personalizados

De forma predeterminada, los dispositivos de Palo Alto Networks utilizan certificados predefinidos para la autenticación mutua con el fin de establecer las conexiones SSL que se usan para el acceso de gestión y la comunicación entre dispositivos. Sin embargo, puede configurar la autenticación con certificados personalizados en su lugar. Además, puede usar certificados personalizados para proteger las conexiones de alta disponibilidad (HA) entre peers de HA de Panorama. Los certificados personalizados le permiten establecer una cadena de confianza única para garantizar la autenticación mutua entre Panorama, y los cortafuegos gestionados y los recopiladores de logs. Consulte la Gestión de certificados para obtener información detallada sobre los certificados y cómo implementarlos en Panorama, los recopiladores de logs y los cortafuegos.

Los siguientes temas describen cómo configurar y gestionar los certificados personalizados utilizando Panorama.

- ¿Cómo se autentican mutuamente las conexiones SSL/TLS?
- Configuración de la autenticación mediante la utilización de certificados personalizados en Panorama
- Configuración de la autenticación mediante la utilización de certificados personalizados en dispositivos gestionado
- Adición de nuevos dispositivos cliente
- Cambio de certificados

¿Cómo se autentican mutuamente las conexiones SSL/TLS?

En una conexión SSL regular, solo el servidor debe identificarse ante el cliente presentando su certificado. Sin embargo, en la autenticación SSL mutua, el cliente también presenta su certificado al servidor. Panorama, el peer de HA principal de Panorama, los recopiladores de logs, los dispositivos WildFire y los dispositivos PAN-DB pueden actuar como el servidor. Los cortafuegos, los recopiladores de logs, los dispositivos WildFire y el peer secundario de Ha de Panorama pueden actuar como cliente. El rol que asume un dispositivo depende de la implementación. Por ejemplo, en el siguiente diagrama, Panorama gestiona una cantidad de cortafuegos y un grupo de recopiladores y actúa como servidor para los cortafuegos y los recopiladores de logs. El Recopilador de logs actúa como el servidor de los cortafuegos que le envían logs.

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 el dispositivo del servidor para comunicarse con los dispositivos cliente.
- **Certificado y perfil del servidor:** los dispositivos en rol de servidor requieren un certificado y un perfil del certificado para identificarse en los dispositivos cliente. 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 de dispositivos en el nombre común del certificado (common name, CN) o el nombre alternativo del sujeto. El

 ©2023 Palo Alto Networks, Inc.

cortafuegos del cliente o el recopilador de logs coinciden 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 servidor para verificar la identidad del servidor.

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 de cliente y perfil:** cada dispositivo gestionado requiere un certificado de cliente y perfil del certificado. El dispositivo cliente utiliza su certificado para identificarse en el dispositivo del servidor. Puede implementar certificados desde la PKI de su empresa utilizando el protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, 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. El comportamiento del certificado de cliente también se aplica a las conexiones de peers de HA de Panorama.

  Puede configurar el certificado de cliente y el perfil del certificado en cada dispositivo cliente o enviar la configuración de Panorama a cada dispositivo como parte de una plantilla.

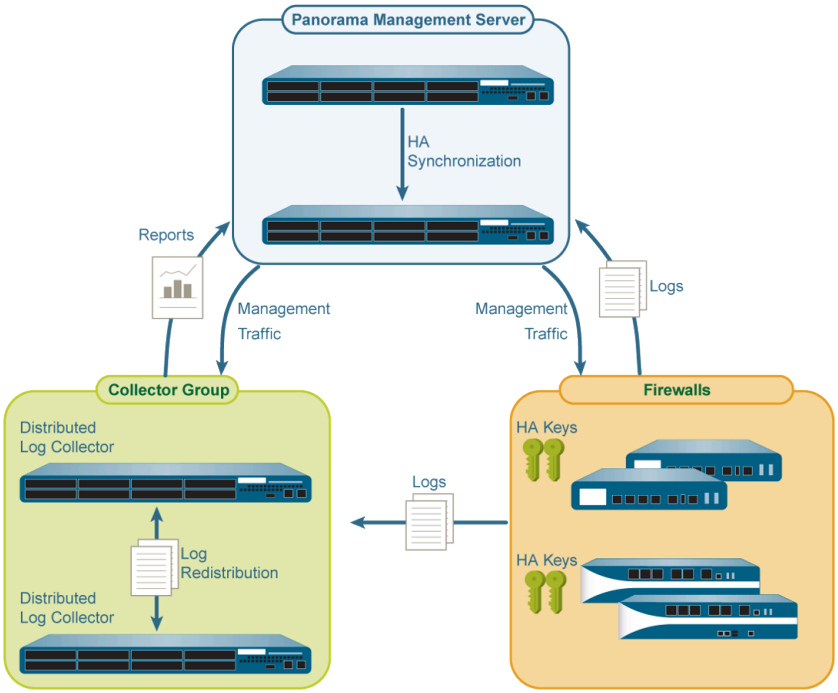


Figure 10: Autenticación SSL/TLS

Configuración de la autenticación mediante la utilización de certificados personalizados en Panorama

Complete el siguiente procedimiento para configurar la parte del servidor (Panorama) para usar certificados personalizados en lugar de certificados predefinidos para la autenticación mutua con

©2023 Palo Alto Networks, Inc.

dispositivos gestionados en su implementación. Consulte Configurar la autenticación mediante certificados personalizados entre peers de HA para configurar certificados personalizados en un par de HA de Panorama.

STEP 1 | Implemente el certificado de servidor.

Usted puede implementar certificados en Panorama o en un recopilador de logs del servidor generando un certificado autofirmado en Panorama u obteniendo un certificado de la entidad de certificación (Certificate Authority, CA) de su empresa o de una CA externa de confianza.

STEP 2 | En Panorama, configure un perfil del certificado. Este perfil del certificado define qué certificado usar y en qué campo de certificado buscar la dirección IP o el FQDN.

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

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

STEP 3 | Configure un perfil de servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Configuración de un perfil SSL/TLS para definir el certificado y protocolo que Panorama y sus dispositivos gestionados usan para servicios SSL/TLS.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure la Comunicación de servidor segura en Panorama o en un Recopilador de logs en la función de servidor.

1. Seleccione uno de las siguientes rutas de navegación:
   - Para Panorama: **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para editar los ajustes de Secure Communication (Comunicación segura).
   - Para un recopilador de logs: **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)**
2. Seleccione la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
3. Verifique que la casilla de verificación **Allow Custom Certificate Only (Permitir certificado personalizado únicamente)** no está seleccionada. Esto le permite continuar gestionando todos los dispositivos mientras migra a certificados personalizados.

   Cuando se selecciona la casilla de verificación Solo certificado personalizado, Panorama no se autentica y no puede gestionar dispositivos usando certificados predefinidos.
4. Seleccione el **SSL/TLS Service Profile**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre Panorama, los cortafuegos, recopiladores de logs y los peers de HA de Panorama.
5. Seleccione el **Certificate Profile (Perfil del certificado)** que identifica el certificado que se utilizará para establecer una comunicación segura con clientes tales como los cortafuegos.
6. (Opcional) Configure una lista de autorizaciones. La lista de autorizaciones añade una capa adicional de seguridad más allá de la autenticación del certificado. La lista de autorizaciones verifica el Asunto o Nombre alternativo del sujeto del certificado del cliente. Si el Sujeto o el Nombre alternativo del sujeto presentado con el certificado del cliente no coincide con un identificador en la lista de autorizaciones, se deniega la autenticación.

   También puede autorizar dispositivos cliente en función de sus números de serie.

   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Selecciona el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** configurado en el perfil del certificado como el tipo de identificador.
   3. Introduzca el Nombre común si el identificador es Sujeto o una dirección IP, nombre de host o correo electrónico si el identificador es Nombre alternativo del sujeto.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Check Authorization List (Comprobar lista de autorización)** para hacer cumplir la lista de autorizaciones.
7. Seleccione **Authorize Client Based on Serial Number (Autorizar clientes según el número de serie)** para hacer que el servidor autentique a los clientes en base a los números de serie de los dispositivos gestionados. El CN o el sujeto en el certificado del cliente debe tener la palabra clave $UDID especial para habilitar este tipo de autenticación.
8. Seleccione la opción **Data Redistribution (Redistribución de datos)** en la sección **Customize Communication (Personalizar comunicación)** para usar un certificado

 ©2023 Palo Alto Networks, Inc.

personalizado para garantizar la comunicación saliente con los clientes de redistribución de datos.

9. En **Disconnect Wait Time (min) [Tiempo de espera de desconexión (min)]**, especifique el periodo de tiempo que Panorama debe esperar antes de terminar la sesión actual y restablecer la conexión con sus dispositivos gestionados. Este campo está en blanco por defecto y el rango es de 0 a 44,640 minutos. Dejar este campo en blanco es lo mismo que establecerlo en 0.

   El tiempo de espera de desconexión no comienza la cuenta atrás hasta que confirme la nueva configuración.

10. Haga clic en **OK (Aceptar)**.
11. **Commit (Confirmar)** los cambios.

Configuración de la autenticación mediante la utilización de certificados personalizados en dispositivos gestionado

Complete el siguiente procedimiento para configurar la parte del cliente (cortafuegos o recopilador de logs) para usar certificados personalizados en lugar de certificados predefinidos para la autenticación mutua con dispositivos gestionados en su implementación.

STEP 1 | Actualice cada cortafuegos gestionado o Recopilador de logs. Todos los dispositivos gestionados deben ejecutar PAN-OS 8.0 o posterior para hacer cumplir la autenticación de certificados personalizados.

Actualice el cortafuegos. Después de la actualización, cada cortafuegos se conecta a Panorama utilizando los certificados predefinidos predeterminados.

STEP 2 | Obtenga o genere el certificado del dispositivo.

Usted puede implementar certificados en Panorama o en un recopilador de logs del servidor generando un certificado autofirmado en Panorama u obteniendo un certificado de la entidad de certificación (Certificate Authority, CA) de su empresa o de una CA externa de confianza.

Establezca el nombre común en $UDID o sujeto a CN=$UDID (en el perfil SCEP) si autoriza dispositivos cliente en función del número de serie.

- Puede generar un certificado autofirmado en Panorama u obtener un certificado de la CA de su empresa o de una CA externa de confianza.
- Si está utilizando SCEP para el certificado del dispositivo, configure un perfil SCEP. SCEP le permite implementar automáticamente certificados en dispositivos gestionados. Cuando un nuevo dispositivo cliente con un perfil SCEP intenta autenticarse con Panorama, el servidor SCEP envía el certificado al dispositivo.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el perfil de certificado para el dispositivo de cliente.

Puede configurar esto en cada dispositivo cliente individualmente o puede enviar esta configuración al dispositivo gestionado como parte de una plantilla.

1. Seleccione uno de las siguientes rutas de navegación:
   - Para cortafuegos: seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**.
   - Para recopiladores de logs: seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)**.
2. Configuración del perfil del certificado:

STEP 4 | Implemente certificados personalizados en cada cortafuegos o recopilador de logs.

1. Seleccione uno de las siguientes rutas de navegación:
   - Para cortafuegos: Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y seleccione **Edit (Editar)** para editar la configuración de Panorama.
   - Para recopiladores de logs: Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir un nuevo recopilador de logs o seleccionar uno existente. Seleccione **Communication (Comunicación)**.
2. Seleccione la casilla de verificación **Secure Client Communication (Comunicación de cliente segura)** (solo cortafuegos).
3. Seleccione el **Interface Type (Tipo de interfaz)**.
   - Si está utilizando un certificado de dispositivo local, seleccione **Certificate (Certificado)** y **Certificate Profile (Perfil del certificado)**.
   - Si está utilizando SCEP para implementar el certificado del dispositivo, seleccione **SCEP Profile (Perfil de SCEP)** y **Certificate Profile (Perfil del certificado)**.
   - Si utiliza el certificado de Panorama predeterminado, seleccione **Predefined (Predefinido)**.
4. (Opcional) Habilite **Check Server Identity (Verificar la identidad del servidor)**. El cortafuegos o Recopilador de logs comprueba el CN en el certificado del servidor frente a la dirección IP o el FQDN de Panorama para verificar su identidad.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

   Después de confirmar los cambios, el dispositivo gestionado no finaliza su sesión actual con Panorama hasta que el Tiempo de espera de desconexión se completa.

STEP 5 | Seleccione los tipos de comunicaciones entrantes para los que desee utilizar un certificado personalizado:

- **HA Communication (Comunicación de HA)**
- **WildFire Communication (Comunicación de WildFire)**
- **Data Redistribution (Redistribución de datos)**

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Después de implementar certificados personalizados en todos los dispositivos gestionados, aplique la autenticación mediante certificados personalizados.

> ***El dispositivo WildFire no admite actualmente certificados personalizados. Si su Panorama está gestionando un dispositivo WildFire, no seleccione* Allow Custom Certificates Only (Permitir solo certificados personalizados).**

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y **edite** la configuración de Panorama.
2. Seleccione **Allow Custom Certificate Only (Permitir certificado personalizado únicamente)**.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

   Después de confirmar este cambio, todos los dispositivos gestionados por Panorama deben usar certificados personalizados. De lo contrario, la autenticación entre Panorama y el dispositivo falla.

Adición de nuevos dispositivos cliente

Al añadir un nuevo cortafuegos o Recopilador de logs a Panorama, el flujo de trabajo depende de si estos dispositivos están configurados o no para usar certificados personalizados solo para la autenticación mutua.

- Si la opción Solo los certificados personalizados no está seleccionada en Panorama, puede añadir el dispositivo a Panorama y luego implementar el certificado personalizado siguiendo el proceso que comienza en el paso Configuración de la autenticación mediante la utilización de certificados personalizados en dispositivos gestionado.
- Si la opción Solo los certificados personalizados se selecciona en Panorama, debe implementar los certificados personalizados en el cortafuegos antes de añadirlo a Panorama. De lo contrario, el dispositivo gestionado no podrá autenticarse con Panorama. Esto puede hacerse manualmente a través de la interfaz web del cortafuegos o mediante el arranque como parte del archivo bootstrap.xml.

Cambio de certificados

Si un certificado personalizado en su implementación ha caducado o ha sido revocado y es necesario reemplazarlo, puede completar una de las siguientes tareas.

- Cambio de un certificado de servidor
- Cambio de un certificado de cliente
- Cambio de un certificado de CA raíz o intermedio

Cambio de un certificado de servidor

Complete la siguiente tarea para reemplazar un certificado de servidor.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Implemente el nuevo certificado de servidor.

Usted puede implementar certificados en Panorama o en un recopilador de logs del servidor generando un certificado autofirmado en Panorama u obteniendo un certificado de la CA de su empresa o de una CA externa de confianza.

STEP 2 | Cambie el certificado en el perfil del servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** y seleccione el perfil de servicio SSL/TLS.
2. Seleccione el **Certificate (Certificado)**.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Restablezca la conexión entre el servidor (Panorama o Recopilador de log) y los dispositivos cliente.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y **Edit (Editar)** para modificar la configuración de Panorama para Panorama o seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)** para un Recopilador de logs.
2. Seleccione **Disconnect Wait Time (Tiempo de espera de desconexión)**.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

Cambio de un certificado de cliente

Complete la siguiente tarea para reemplazar un certificado de cliente.

STEP 1 | Obtenga o genere el certificado del dispositivo.

Usted puede implementar certificados en Panorama o en un recopilador de logs del servidor generando un certificado autofirmado en Panorama u obteniendo un certificado de la CA de su empresa o de una CA externa de confianza.

Establezca el nombre común en $UDID o sujeto a CN=$UDID (en el perfil SCEP) si autoriza dispositivos cliente en función del número de serie.

- Puede generar un certificado autofirmado en Panorama u obtener un certificado de la CA de su empresa o de una CA externa de confianza.
- Si está utilizando SCEP para el certificado del dispositivo, configure un perfil SCEP. SCEP le permite implementar automáticamente certificados en dispositivos gestionados. Cuando un nuevo dispositivo cliente con un perfil SCEP intenta autenticarse con Panorama, el servidor SCEP envía el certificado al dispositivo.

STEP 2 | Cambie el certificado en el perfil del certificado.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificate Profile (Perfil de certificados)** y seleccione el perfil de certificado.
2. En los Certificados de CA, seleccione **Add (Añadir)** para añadir el nuevo certificado que va a asignar al perfil de certificado.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

 ©2023 Palo Alto Networks, Inc.

Cambio de un certificado de CA raíz o intermedio

Complete la siguiente tarea para reemplazar un certificado de CA raíz o intermedio.

STEP 1 | Configure el servidor para que acepte certificados predefinidos de los clientes.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y **edite** la configuración de Panorama.
2. Retire la marca de **Custom Certificate Only (Certificado personalizado únicamente)**.
3. Seleccione **None (Ninguno)** del menú desplegable de perfil del certificado
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

STEP 2 | Implemente el nuevo certificado de CA raíz o intermedio.

Usted puede implementar certificados en Panorama o en un recopilador de logs del servidor generando un certificado autofirmado en Panorama u obteniendo un certificado de la CA de su empresa o de una CA externa de confianza.

STEP 3 | Actualice el certificado de CA en el perfil de certificado del servidor.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y seleccione el perfil de certificado que desea actualizar.
2. Seleccione **Delete (Eliminar)** para eliminar el antiguo certificado de CA.
3. Seleccione **Add (Añadir)** para añadir el nuevo certificado de CA.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Genere o importe el nuevo certificado de cliente.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
2. Cree un certificado de CA raíz autofirmado o importe un certificado de su empresa CA.

STEP 5 | Actualice el certificado de CA en el perfil de certificado del cliente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en el icono **Edit (Editar)** en la configuración de Panorama para un servidor de seguridad o Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** > **Add (Añadir)** > **Communication (Comunicación)** para un recopilador de logs y seleccione el perfil del certificado para actualizar.
2. Seleccione **Delete (Eliminar)** para eliminar el antiguo certificado de CA.
3. Seleccione **Add (Añadir)** para añadir el nuevo certificado de CA.
4. Haga clic en **OK (Aceptar)**.

©2023 Palo Alto Networks, Inc.

STEP 6 | Después de actualizar los certificados de CA en todos los dispositivos gestionados, aplique la autenticación de certificado personalizado.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y **edite** la configuración de Panorama.
2. Seleccione **Custom Certificate Only (Certificado personalizado únicamente)**.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

   Después de confirmar este cambio, todos los dispositivos gestionados por Panorama deben usar certificados personalizados. De lo contrario, la autenticación entre Panorama y el dispositivo falla.

 ©2023 Palo Alto Networks, Inc.

Gestión de cortafuegos

Para usar el servidor de gestión Panorama™ para la gestión de cortafuegos de Palo Alto Networks, debe añadir los cortafuegos como dispositivos gestionados y luego asignarlos a un grupo de dispositivos y plantillas o pilas de plantillas. Las siguientes tareas están indicadas para la primera implementación de un cortafuegos. Antes de continuar, revise la Planificación de la implementación de Panorama para comprender las opciones de implementación.

- Cómo añadir un cortafuegos como dispositivo gestionado
- Instalación del certificado del dispositivo para cortafuegos gestionados
- Configuración de Zero Touch Provisioning
- Gestión de grupos de dispositivos
- Gestión de plantillas y pilas de plantillas
- Gestión de la clave maestra en Panorama
- Programación de un envío de configuración en cortafuegos gestionados
- Redistribución de datos a cortafuegos gestionados
- Transición de un cortafuegos a una gestión de Panorama
- Supervisión de dispositivos en Panorama
- Caso de uso: Configuración de cortafuegos mediante Panorama

Para ver las pestañas **Objects (Objetos)** y **Policies (Políticas)** en la interfaz web de Panorama, primero debe crear al menos un grupo de dispositivos. Para ver las pestañas **Network (Red)** y **Device (Dispositivo)**, debe crear al menos una plantilla. Estas pestañas contienen las opciones para configurar y gestionar los cortafuegos de su red.

Cómo añadir un cortafuegos como dispositivo gestionado

Para utilizar un servidor de gestión Panorama™ para administrar los cortafuegos, debe habilitar una conexión entre el cortafuegos y el servidor de gestión Panorama. Para fortalecer su estrategia de seguridad cuando incorpore nuevos cortafuegos, debe crear una clave única de autenticación de registro de dispositivo en el servidor de gestión Panorama para la autenticación mutua entre un cortafuegos nuevo y el servidor en la primera conexión. Una primera conexión correcta requiere que añada la dirección IP de Panorama en cada cortafuegos que administrará el servidor, añada el número de serie en el servidor para cada cortafuegos y especifique la clave de autenticación de registro del dispositivo tanto en el servidor como en el cortafuegos. Si añade un cortafuegos como dispositivo gestionado, también puede asociarlo a un grupo de dispositivos, una pila de plantillas, un grupo de recopiladores y un recopilador de logs durante la implementación inicial. Además, tiene la posibilidad de enviar automáticamente la configuración al cortafuegos recién añadido cuando se conecte por primera vez al servidor de Panorama. Esto garantiza que los cortafuegos estén configurados y preparados para proteger la red al instante.

Solo puede importar de forma masiva cortafuegos de un solo vsys al servidor de gestión Panorama.

El cortafuegos utiliza la dirección IP del servidor de gestión Panorama para el registro en el servidor. El servidor de Panorama y el cortafuegos se autentican entre sí con certificados de 2048 bits y conexiones SSL AES-256 cifradas para la gestión de la configuración y la recopilación de logs.

Para configurar la clave de autenticación de registro de dispositivos, especifique la duración de la clave y la cantidad de veces que puede utilizar la clave de autenticación para incorporar nuevos firewalls. Además, puede especificar uno o más números de serie de cortafuegos para los que la clave de autenticación es válida.

La clave de autenticación caduca 90 días después de que caduque la vida útil de la clave. Después de 90 días, se le pedirá que vuelva a certificar la clave de autenticación para mantener su validez. Si no la vuelve a certificar, la clave de autenticación no será válida. Se genera un log del sistema cada vez que un cortafuegos utiliza la clave de autenticación generada por Panorama. El cortafuegos utiliza la clave de autenticación para autenticar el servidor de Panorama cuando entrega el certificado del dispositivo que se utiliza para todas las comunicaciones posteriores.

(PAN-OS 10.2 solo) Para cortafuegos que ejecutan una versión PAN-OS 10.2, Panorama que ejecuta PAN-OS 10.2 o una versión posterior admite cortafuegos de incorporación que ejecutan PAN-OS 10.1.3 o una versión posterior solamente. No puede añadir un cortafuegos que ejecute PAN-OS 10.1.2 o una versión anterior de PAN-OS 10.2 a la gestión de Panorama si Panorama ejecuta PAN-OS 10.2 o una versión posterior.

Panorama admite cortafuegos de incorporación que ejecutan las siguientes versiones:

- ***Panorama que ejecuta PAN-OS 10.2 o una versión posterior:** cortafuegos que ejecutan PAN-OS 10.1.3 o una versión posterior, y cortafuegos que ejecutan PAN-OS 10.0 o una versión anterior de PAN-OS.*

No hay ningún impacto en los cortafuegos ya gestionados por Panorama en la actualización a PAN-OS 10.2.

©2023 Palo Alto Networks, Inc.

STEP 1 | Configure el cortafuegos.

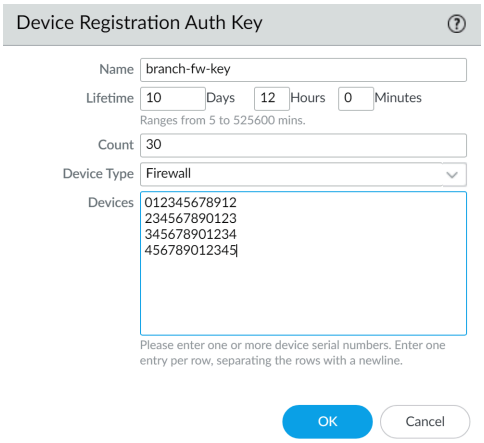
1. Realice una configuración inicial en el cortafuegos, de modo que sea accesible y pueda comunicarse con el servidor de Panorama a través de la red.
2. Configure cada interfaz de datos que tenga la intención de utilizar en el cortafuegos y adjúntela a una zona de seguridad para que pueda introducir los ajustes de configuración y las reglas de políticas desde el servidor de Panorama.

 ©2023 Palo Alto Networks, Inc.

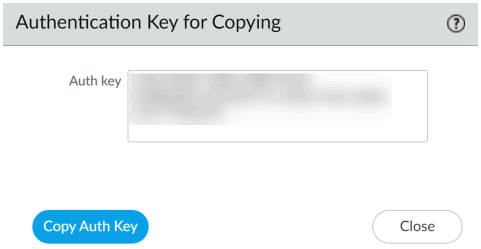
STEP 2 | Cree una clave de autenticación de registro de dispositivo.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.
3. Configure la clave de autenticación.
   - **Name (Nombre)**: agregue un nombre descriptivo para la clave de autenticación.
   - **Lifetime (Duración)**: especifique la duración de la clave a fin de limitar durante cuánto tiempo puede utilizar la clave de autenticación para incorporar nuevos cortafuegos.
   - **Count (Conteo)**: especifique cuántas veces puede utilizar la clave de autenticación para incorporar nuevos cortafuegos.
   - **Device Type (Tipo de dispositivo)**: especifique que esta clave de autenticación se utiliza para autenticar solo un **cortafuegos**.

     *Puede seleccionar **Any (Cualquiera)** para utilizar la clave de autenticación de registro de dispositivos para incorporar cortafuegos, recopiladores de logs y dispositivos WildFire.*
   - (Opcional) **Devices (Dispositivos)**: introduzca uno o más números de serie de dispositivo para especificar para qué cortafuegos es válida la clave de autenticación.
4. Haga clic en **OK (Aceptar)**.



5. Seleccione **Copy Auth Key (Copiar la clave de autenticación)** y **Close (Cerrar)**.

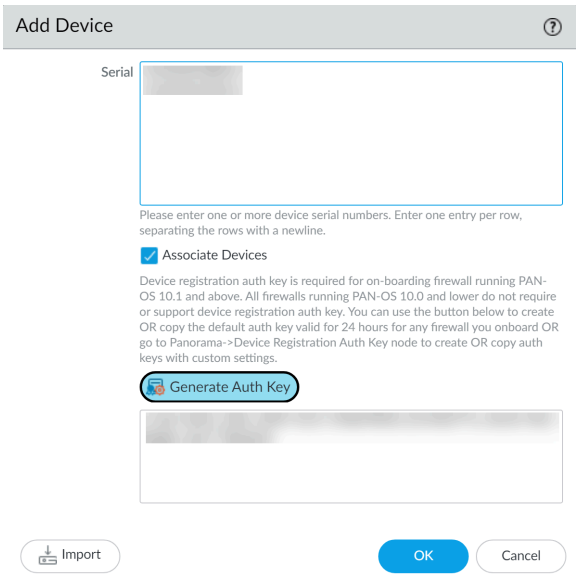


 ©2023 Palo Alto Networks, Inc.

STEP 3 | Añada cortafuegos a un servidor de gestión Panorama. Puede añadir manualmente uno o más cortafuegos, o importar cortafuegos de forma masiva con un archivo CSV.

No puede importar cortafuegos de forma masiva con más de un sistema virtual (vsys).

- Añada uno o más cortafuegos manualmente.
  1. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y **Add (Añadir)** para agregar un cortafuegos nuevo.
  2. En **Serial (Número de serie)**, introduzca el número del cortafuegos. Si desea añadir varios, introduzca cada número de serie en una línea aparte.
  3. (Opcional) Seleccione **Associate Devices (Asociar dispositivos)** para asociar el cortafuegos con un grupo de dispositivos, una pila de plantillas, un recopilador de logs o un grupo de recopiladores cuando el cortafuegos se conecte por primera vez al servidor de gestión Panorama.
  4. Introduzca la clave de autenticación de registro de dispositivo que creó.



  5. Haga clic en **OK (Aceptar)**.
  6. Asocie sus cortafuegos gestionados según sea necesario.

     Si no seleccionó **Associate Devices (Asociar dispositivos)**, omita este paso y continúe configurando el cortafuegos para comunicarse con Panorama.

     1. Asigne **Device Group (Grupo de dispositivos)**, **Template Stack (Pila de plantillas)**, **Collector Group (Grupo de recopiladores)** y **Log Collector (Recopilador de logs)** según sea necesario desde el menú desplegable en cada columna.
     2. Habilite **Auto Push on 1st connect (Enviar automáticamente al conectar por primera vez)** para enviar la configuración del grupo de dispositivos y de la pila de plantillas a

 ©2023 Palo Alto Networks, Inc.

los dispositivos nuevos de forma automática cuando se conecten por primera vez al servidor Panorama.

*La opción **Auto Push on 1st connect (Enviar automáticamente al conectar por primera vez)** solo se admite en los cortafuegos que ejecutan PAN-OS® 8.1 y versiones posteriores. El trabajo `commit all` se ejecuta en Panorama y se aplica a todos los dispositivos gestionados que ejecutan PAN-OS 8.1 o versiones posteriores.*

3. (Opcional) Seleccione una versión de lanzamiento de PAN-OS (en la columna **To SW Version [Para la versión de SW]**) para comenzar a actualizar automáticamente el

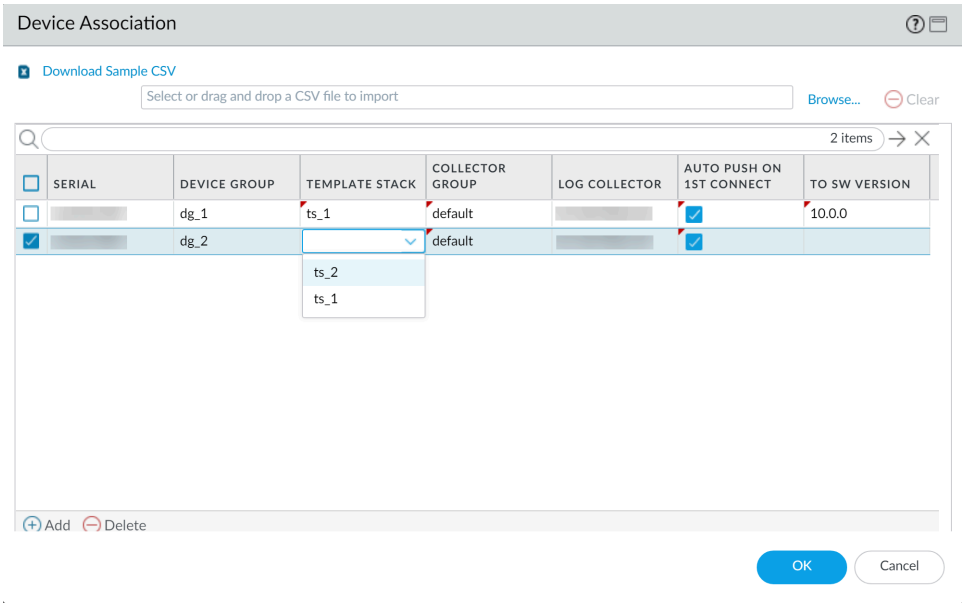
 ©2023 Palo Alto Networks, Inc.

cortafuegos gestionado a la versión de PAN-OS especificada una vez que se realice una conexión correcta con el servidor de gestión Panorama.

Para actualizar un cortafuegos gestionado a una versión PAN-OS de destino en la primera conexión, debe instalar la versión de contenido mínima requerida para esa versión PAN-OS antes de agregar el cortafuegos como dispositivo gestionado. Para ello, debe registrar el cortafuegos, activar la licencia de soporte e instalar la actualización de contenido antes de añadir el cortafuegos a la administración de Panorama.

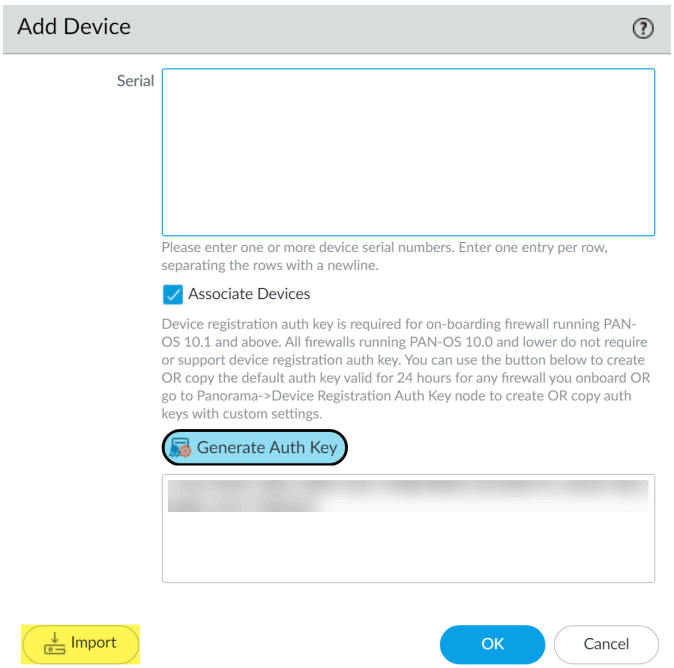
Deje esta columna vacía si no desea actualizar automáticamente el cortafuegos gestionado.

4. Haga clic en **OK (Aceptar)** para añadir los dispositivos.

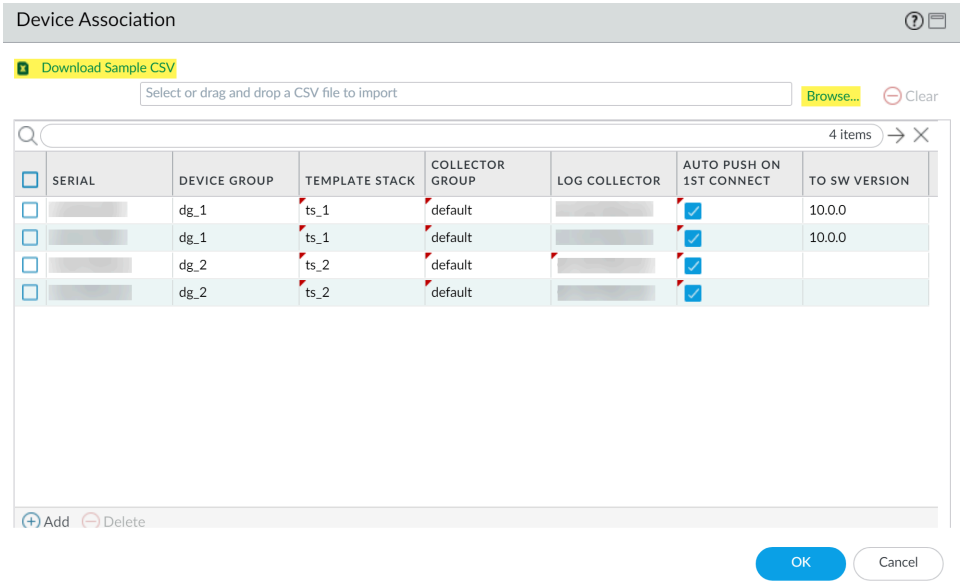


- Importe varios cortafuegos de forma masiva con un archivo CSV.
  1. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y **Add (Añadir)** para agregar nuevos cortafuegos.
  2. Añada la clave de autenticación de registro de dispositivo que creó.
  3. Haga clic en **Import (Importar)**.

©2023 Palo Alto Networks, Inc.



4. Haga clic en **Download Sample CSV (Descargar CSV de muestra)** y edite el archivo CSV descargado con los cortafuegos que desea añadir. Puede asignarlos a un grupo de dispositivos, una pila de plantillas, un grupo de recopiladores y un recopilador de logs en el propio archivo CSV o bien introducir solo su número de serie y asignarlos después en la interfaz web. Guarde el archivo CSV cuando termine de modificarlo.
5. Haga clic en **Browse (Examinar)** y seleccione el archivo CSV que acaba de editar.



6. Si no ha realizado la asignación en el archivo CSV, seleccione los valores oportunos en los menús desplegables de las columnas **Device Group (Grupo de dispositivos)**, **Template**

 ©2023 Palo Alto Networks, Inc.

Stack (Pila de plantillas), **Collector Group (Grupo de recopiladores)** o **Log Collector (Recopilador de logs)**.

7. Si no ha habilitado ya esta opción en el archivo CSV, habilite **Auto Push on 1st connect (Enviar automáticamente al conectar por primera vez)** para enviar la configuración del grupo de dispositivos y de la pila de plantillas a los dispositivos nuevos de forma automática cuando se conecten por primera vez al servidor de Panorama.
8. (Opcional) Seleccione una versión de lanzamiento de PAN-OS (en la columna **To SW Version [Para la versión de SW]**) para comenzar a actualizar automáticamente el cortafuegos gestionado a la versión de PAN-OS especificada una vez que se realice una conexión correcta con el servidor de Panorama.

   Para actualizar un cortafuegos gestionado a una versión PAN-OS de destino en la primera conexión, debe instalar la versión de contenido mínima requerida *para esa versión PAN-OS antes de agregar el cortafuegos como dispositivo gestionado. Para ello, debe* registrar el cortafuegos**,** activar la licencia de soporte ***e*** instalar la actualización de contenido ***antes de añadir el cortafuegos a la administración de Panorama.***

   Deje esta columna vacía si no desea actualizar automáticamente el cortafuegos gestionado.
9. Haga clic en **OK (Aceptar)** para agregar los cortafuegos.

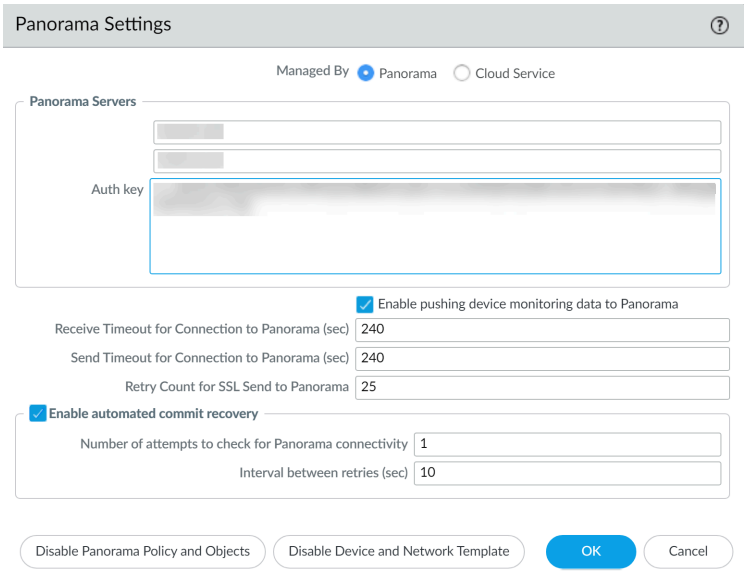
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure el cortafuegos para comunicarse con servidor de gestión Panorama.

Repita este paso para cada cortafuegos que administrará el servidor de Panorama.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Configure los ajustes de Panorama para el cortafuegos.
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
   2. Introduzca la dirección IP de Panorama en este campo.

      Panorama emite una sola dirección IP para la gestión de dispositivos, la recopilación de logs, la creación de informes y las actualizaciones dinámicas. Introduzca la dirección IP externa vinculada a internet para garantizar el acceso de Panorama a los dispositivos gestionados y a los recopiladores de logs tanto existentes como nuevos. Si configura una dirección IP interna de Panorama, quizá no pueda gestionar algunos dispositivos. Por ejemplo, si realiza el procedimiento Instalación de Panorama en AWS e introduce la dirección IP interna, Panorama no puede gestionar los dispositivos gestionados ni los recopiladores de logs que se encuentran fuera del grupo de seguridad de AWS.
   3. (Opcional) Si configuró un par de alta disposnibilidad (high availability, HA) en Panorama, introduzca la dirección IP de la instancia secundaria de Panorama en el segundo campo.
   4. Introduzca la **clave de autenticación** que creó en Panorama.
   5. Haga clic en **Aceptar**.



   6. **Commit (Confirmar)** los cambios.

STEP 5 | (Opcional) Añada una **Tag (Etiqueta)**. Gracias a las etiquetas, resulta más fácil buscar cortafuegos en listas extensas, ya que sirven para filtrarlos y acotarlos dinámicamente. Por ejemplo, si añade una etiqueta denominada **`sucursal`**, podrá filtrar todos los cortafuegos de sucursal de su red.

1. Seleccione cada uno de los cortafuegos y haga clic en **Tag (Etiqueta)**.

 ©2023 Palo Alto Networks, Inc.

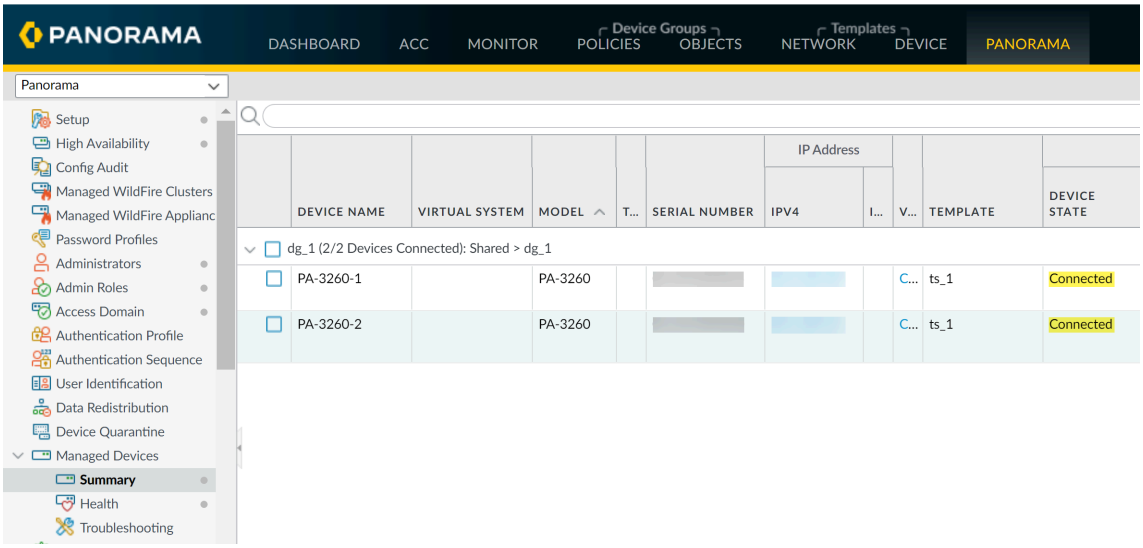
2. Haga clic en **Add (Añadir)**, introduzca una cadena de hasta 31 caracteres (sin espacios en blanco) y haga clic en **OK (Aceptar)**.

STEP 6 | Si su implementación utiliza certificados personalizados para la autenticación entre Panorama y los dispositivos gestionados, implemente el certificado de dispositivo cliente personalizado. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados y Adición de nuevos dispositivos cliente.

STEP 7 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 8 | Verifique que el cortafuegos está conectado a Panorama.

1. Haga clic en**Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
2. Verifique que **Device State (Estado de dispositivo)** muestra `Connected (Conectado)` en la fila correspondiente al dispositivo nuevo.



 ©2023 Palo Alto Networks, Inc.

Instalación del certificado del dispositivo para cortafuegos gestionados

En PAN-OS 10.2 y versiones posteriores, debe instalar el certificado del dispositivo en sus cortafuegos gestionados para autenticar con éxito sus cortafuegos gestionados y aprovechar los servicios en la nube de Palo Alto Networks como la telemetría de dispositivos, IoT y la prevención de pérdida de datos (DLP) empresarial. Puede instalar el certificado del dispositivo para un solo cortafuegos gestionado o varios cortafuegos gestionados a la vez.

Consulte** Device Certificates (Certificados del dispositivo) **para instalar el certificado del dispositivo del cortafuegos localmente.

- Instalación del certificado del dispositivo para un cortafuegos gestionado
- Instalación del certificado del dispositivo para varios cortafuegos gestionados

Instalación del certificado del dispositivo para un cortafuegos gestionado

En PAN-OS 10.2 y versiones posteriores, debe instalar el certificado de dispositivo para un cortafuegos gestionado desde el servidor de gestión Panorama. El cortafuegos gestionado debe disponer de acceso a Internet para instalar correctamente el certificado del dispositivo.

STEP 1 | Registro de Panorama y cortafuegos gestionados con el portal de atención al cliente (CSP) de Palo Alto Networks.

STEP 2 | Inicio de sesión en la interfaz web de Panorama como usuario administrador.

©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el servidor de protocolo de tiempo de redes (Network Time Protocol, NTP).

Es necesario un servidor NTP para validar la fecha de vencimiento de la certificación del dispositivo y asegurarse de que el certificado del dispositivo no caduque antes de tiempo o no sea válido.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y seleccione la **plantilla**.
2. Seleccione una de las siguientes opciones según su plataforma:
   - En plataformas de múltiples sistemas virtuales, seleccione **Global** y edite la sección Services.
   - En plataformas de un único sistema virtual, edite la sección Servicios.
3. Seleccione **NTP** y especifique el nombre de host **`pool.ntp.org`** como **servidor NTP principal** o especifique la dirección IP de su servidor NTP principal.
4. (Opcional) Introduzca una dirección **Secondary NTP Server**.
5. (Opcional) Para autenticar actualizaciones de tiempo de los servidores NTP, en **Authentication Type (Tipo de autenticación)**, seleccione uno de los siguientes en cada servidor:
   - **None (Ninguna)** (opción por defecto): deshabilita la autenticación NTP.
   - **Symmetric Key (Clave simétrica)**: el cortafuegos usa intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de tiempo.
     - **Key ID (ID de clave)**: introduzca el ID de clave (1-65534).
     - **Algorithm (Algoritmo)**: seleccione el algoritmo que se debe utilizar en la autenticación del NTP (**MD5** o **SHA1**).
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Seleccione las opciones**Confirmar** y **Confirmar y enviar** a sus cortafuegos de gestión.

STEP 4 | Seleccione **Panorama** > **Managed Devices** > **Summary** (Resumen) y seleccione un cortafuegos gestionado.

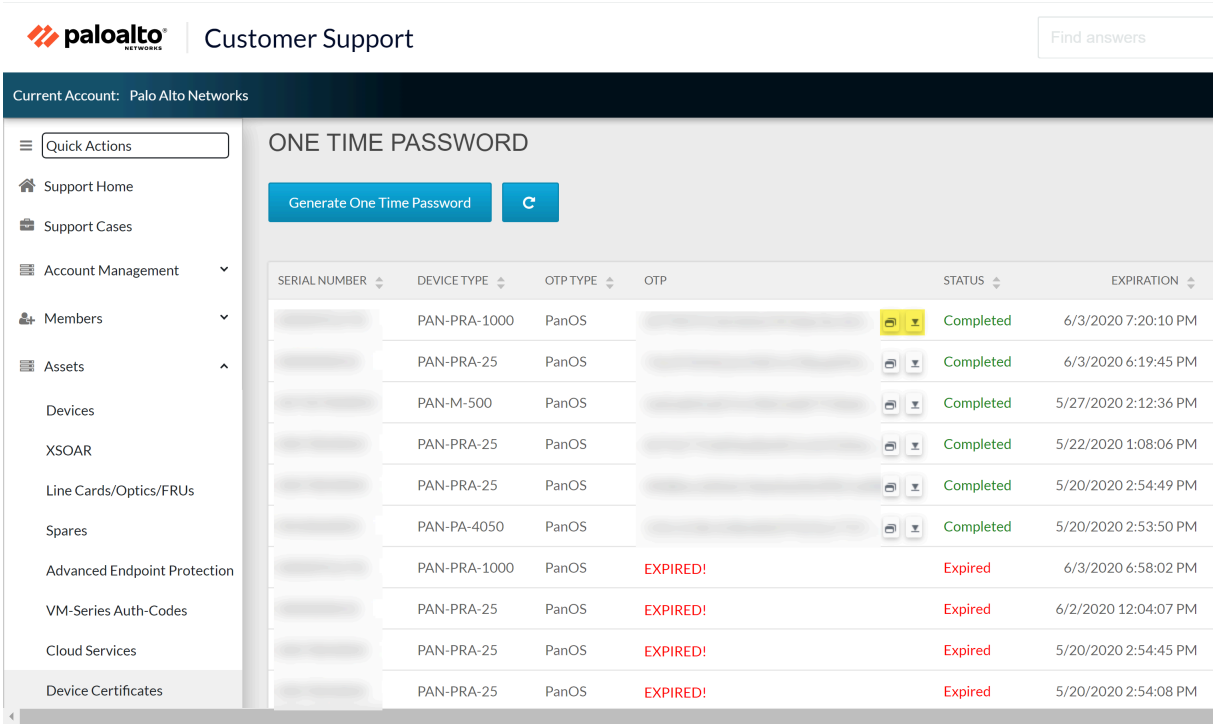
STEP 5 | Seleccione **Request OTP From CSP (Solicitar OTP desde CSP)** > **Custom selected devices (Dispositivos seleccionados personalizados)**.

STEP 6 | Copie todo el token de solicitud de OTP.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Genere la contraseña de un solo uso (One Time Password, OTP) para cortafuegos gestionados.

1. Inicie sesión en el Portal de atención al cliente.
2. Seleccione **Assets (Activos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **tipo de dispositivo**, seleccione **Generate OTP for Panorama managed firewalls (Generar OTP para cortafuegos gestionados de Panorama)**.
4. Pegue la solicitud de OTP que copió en el paso anterior y **genere la OTP**.
5. Haga clic en **Done (Listo)** y espere unos minutos para que la OTP se genere correctamente. Puede actualizar la página si no se muestra la nueva OTP.
6. **Copie al portapapeles** o **descargue** la OTP.



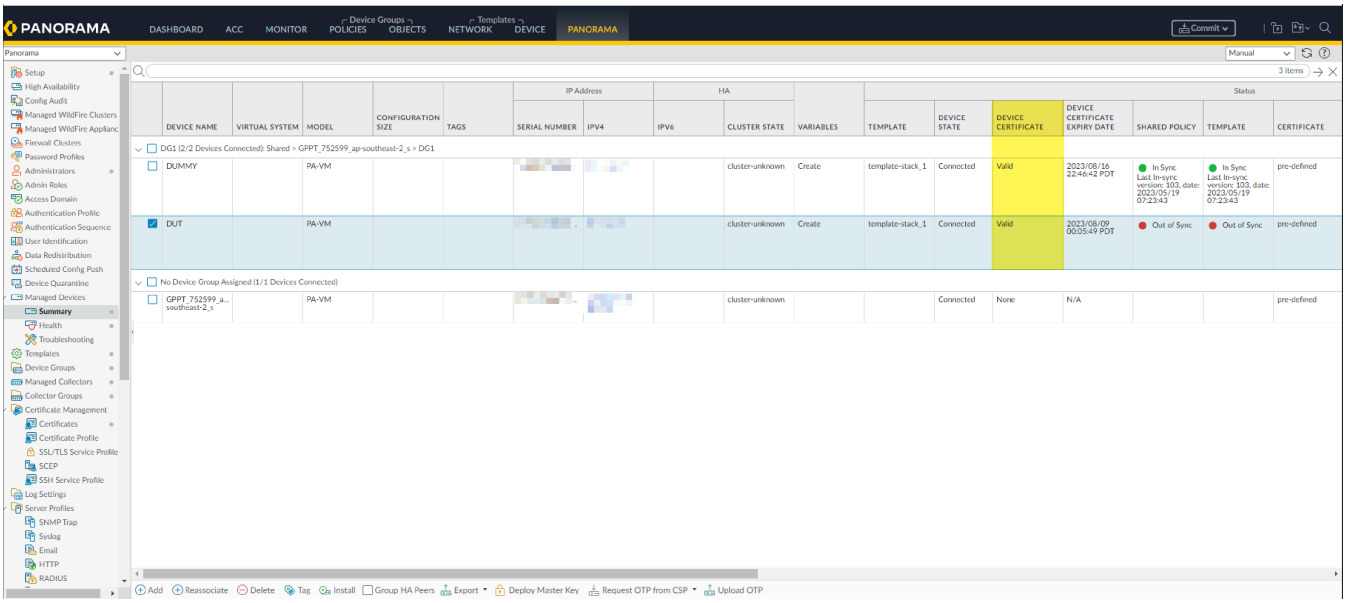
STEP 8 | Inicio de sesión en la interfaz web de Panorama como usuario administrador.

STEP 9 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y **Upload OTP (Cargar OTP)**.

STEP 10 | Pegue la OTP que generó y haga clic en **Upload (Cargar)**.

©2023 Palo Alto Networks, Inc.

STEP 11 | Verifique que la columna **Device Certificate (Certificado del dispositivo)** se muestre como `Valid (Válido)` y que la **fecha de vencimiento del certificado del dispositivo** muestre una fecha de vencimiento.



Instalación del certificado del dispositivo para varios cortafuegos gestionados

En PAN-OS 10.2 y versiones posteriores, debe instalar el certificado de dispositivo para cortafuegos gestionados desde el servidor de gestión Panorama. Los cortafuegos gestionados deben disponer de acceso a Internet para instalar correctamente el certificado del dispositivo.

STEP 1 | Registro de Panorama y cortafuegos gestionados con el portal de atención al cliente (CSP) de Palo Alto Networks.

STEP 2 | Inicio de sesión en la interfaz web de Panorama como usuario administrador.

©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el servidor de protocolo de tiempo de redes (Network Time Protocol, NTP).

Es necesario un servidor NTP para validar la fecha de vencimiento de la certificación del dispositivo y asegurarse de que el certificado del dispositivo no caduque antes de tiempo o no sea válido.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y seleccione la **plantilla**.
2. Seleccione una de las siguientes opciones según su plataforma:
   - En plataformas de múltiples sistemas virtuales, seleccione **Global** y edite la sección Services.
   - En plataformas de un único sistema virtual, edite la sección Servicios.
3. Seleccione **NTP** y especifique el nombre de host **`pool.ntp.org`** como **servidor NTP principal** o especifique la dirección IP de su servidor NTP principal.
4. (Opcional) Introduzca una dirección **Secondary NTP Server**.
5. (Opcional) Para autenticar actualizaciones de tiempo de los servidores NTP, en **Authentication Type (Tipo de autenticación)**, seleccione uno de los siguientes en cada servidor:
   - **None (Ninguna)** (opción por defecto): deshabilita la autenticación NTP.
   - **Symmetric Key (Clave simétrica)**: el cortafuegos usa intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de tiempo.
     - **Key ID (ID de clave)**: introduzca el ID de clave (1-65534).
     - **Algorithm (Algoritmo)**: seleccione el algoritmo que se debe utilizar en la autenticación del NTP (**MD5** o **SHA1**).
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Seleccione las opciones**Confirmar** y **Confirmar y enviar** a sus cortafuegos de gestión.

STEP 4 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.

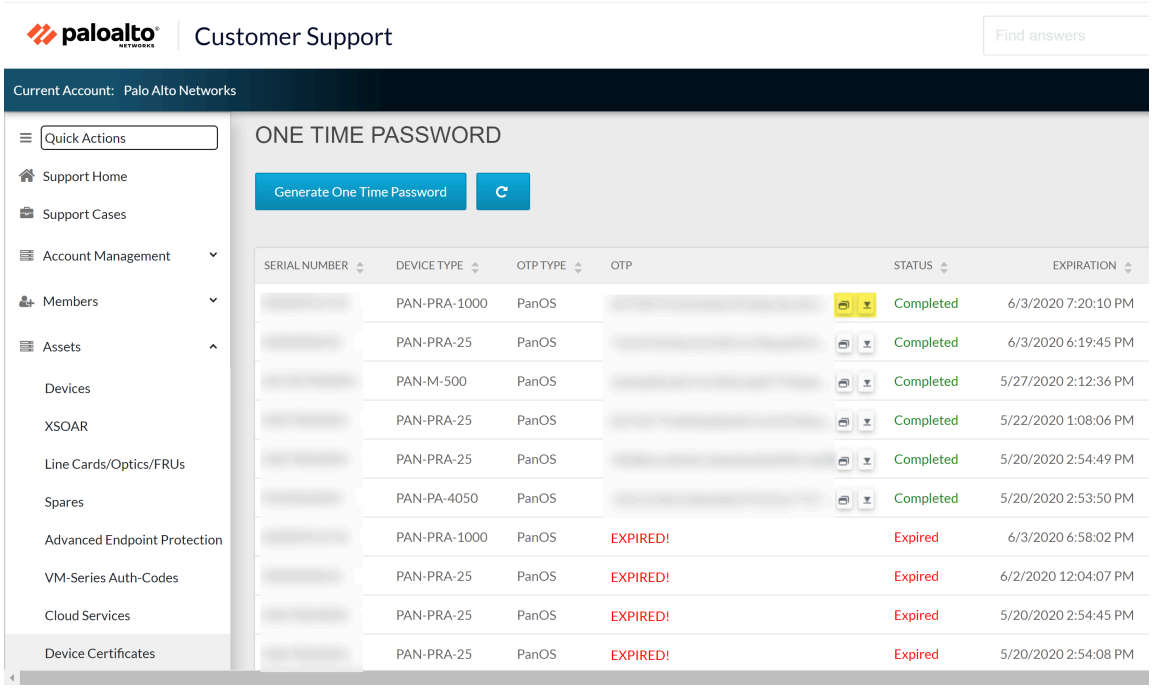
STEP 5 | Seleccione **Request OTP From CSP (Solicitar OTP desde CSP)** > **Select all devices without a certificate (Seleccionar todos los dispositivos sin certificado)**.

STEP 6 | Copie todo el token de solicitud de OTP.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Genere la contraseña de un solo uso (One Time Password, OTP) para cortafuegos gestionados.

1. Inicie sesión en el Portal de atención al cliente.
2. Seleccione **Assets (Activos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **tipo de dispositivo**, seleccione **Generate OTP for Panorama managed firewalls (Generar OTP para cortafuegos gestionados de Panorama)**.
4. Pegue la solicitud de OTP que copió en el paso anterior y **genere la OTP**.
5. Haga clic en **Done (Listo)** y espere unos minutos para que la OTP se genere correctamente. Puede actualizar la página si no se muestra la nueva OTP.
6. **Copie al portapapeles** o **descargue** la OTP.



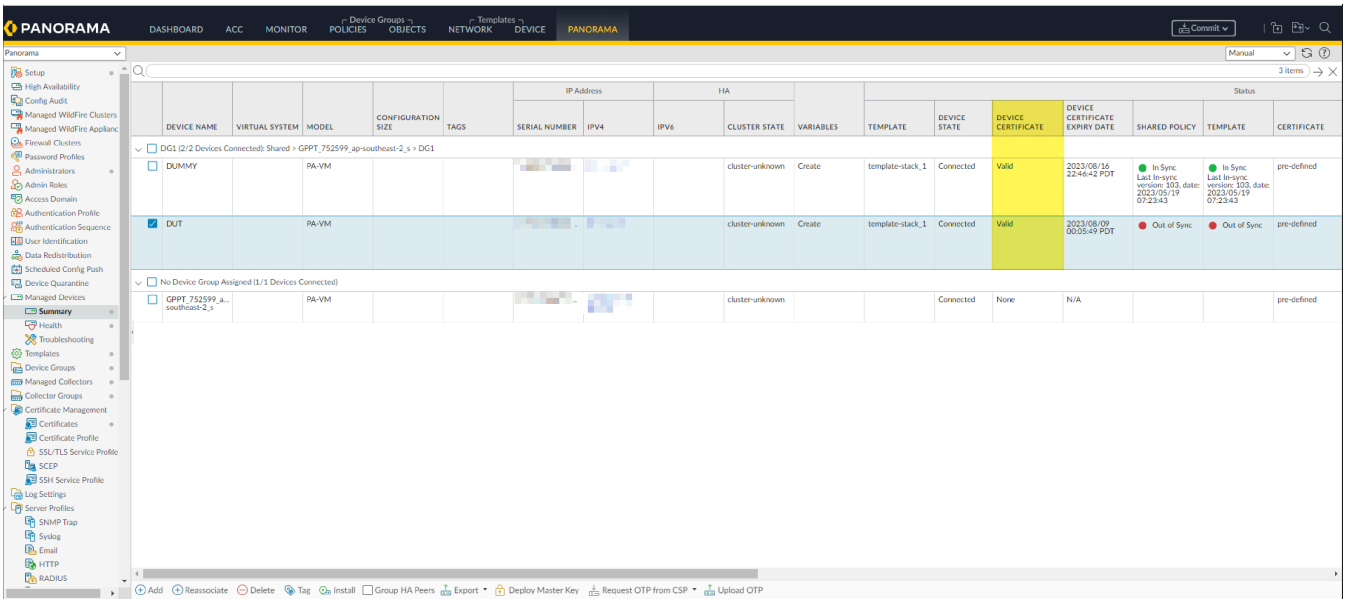
STEP 8 | Inicio de sesión en la interfaz web de Panorama como usuario administrador.

STEP 9 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y **Upload OTP (Cargar OTP)**.

STEP 10 | Pegue la OTP que generó y haga clic en **Upload (Cargar)**.

©2023 Palo Alto Networks, Inc.

STEP 11 | Verifique que la columna **Device Certificate (Certificado del dispositivo)** se muestre como `Valid (Válido)` y que la **fecha de vencimiento del certificado del dispositivo** muestre una fecha de vencimiento.



 ©2023 Palo Alto Networks, Inc.

Configuración de Zero Touch Provisioning

Configure Zero Touch Provisioning (ZTP) para simplificar y agilizar las implementaciones iniciales del cortafuegos mediante la automatización de la incorporación del nuevo cortafuegos gestionado sin necesidad de que los administradores de red realicen un aprovisionamiento manual del cortafuegos.

Para aprovechar con éxito el servicio ZTP, incorpore sus cortafuegos ZTP con la versión PAN-OS predeterminada de fábrica antes de actualizar a PAN-OS 10.0.0 o a una versión posterior.

El complemento ZTP es compatible con PAN-OS 10.0.1 y versiones posteriores.

- Descripción general de ZTP
- Instalación del complemento de ZTP
- Configuración de la cuenta de administrador del instalador de ZTP
- Adición de cortafuegos de ZTP a Panorama
- Uso de la CLI para tareas de ZTP
- Desinstalación del complemento de ZTP

Descripción general de ZTP

Obtenga más información sobre Zero Touch Provisioning (ZTP) y sus elementos de configuración.

- Acerca de ZTP
- Elementos de configuración de ZTP

Acerca de ZTP

Zero Touch Provisioning (ZTP) se ha diseñado para simplificar y automatizar la inclusión de nuevos cortafuegos en el servidor de gestión Panorama™. ZTP agiliza el proceso de implementación del cortafuegos inicial, ya que ofrece a los administradores de red la posibilidad de enviar cortafuegos gestionados directamente a sus sucursales y añadir automáticamente el cortafuegos al servidor de gestión Panorama™ después de que el cortafuegos de ZTP se conecte adecuadamente al servicio de ZTP de Palo Alto Networks. Esto permite a las empresas ahorrar tiempo y recursos al implementar nuevos cortafuegos en sucursales, ya que elimina la necesidad de que los administradores de TI realicen un aprovisionamiento manual del nuevo cortafuegos gestionado. Después de que se realice la incorporación correctamente, Panorama proporciona los medios para configurar y gestionar sus cortafuegos y configuración de ZTP.

Revise y suscríbase a los eventos de ZTP Service Status (Estado del servicio ZTP) para recibir notificaciones sobre los períodos de mantenimiento programados, las interrupciones y las soluciones.

ZTP es compatible con los siguientes cortafuegos ZTP:

- PA-220-ZTP y PA-220R-ZTP
- PA-410, PA-440, PA-450 y PA-460
- PA-820-ZTP y PA-850-ZTP

 ©2023 Palo Alto Networks, Inc.

- PA-3220-ZTP, PA-3250-ZTP y PA-3260-ZTP
- PA-5450

Antes de comenzar a configurar ZTP en Panorama, revise las Guías de referencia e inicio rápido de hardware de cortafuegos para comprender cómo instalar correctamente su cortafuegos para aprovechar ZTP de manera adecuada.

Elementos de configuración de ZTP

Los siguientes elementos funcionan conjuntamente para permitirle incorporar rápidamente los cortafuegos ZTP recién implementados añadiéndolos automáticamente al servidor de gestión Panorama mediante el servicio ZTP.

- **ZTP Plugin (Complemento ZTP)**: el complemento ZTP permite que Panorama se conecte al servicio ZTP y reclame un cortafuegos ZTP para una integración simplificada.
- **Portal de atención al cliente (Customer Support Portal, CSP)**: el portal de atención al cliente de Palo Alto Networks se utiliza para que Panorama se conecte a él y registre automáticamente los cortafuegos de ZTP recién añadidos.
- **Contraseña de un solo uso (One-time Password, OTP)**: la contraseña de un solo uso proporcionada por Palo Alto Networks que se utiliza para recuperar e instalar un certificado en Panorama para que se comunique con el CSP y el servicio ZTP.
- **Instalador**: un usuario administrador creado mediante la función de administración `installeradmin` para el cortafuegos de ZTP incorporado. Este usuario administrador tiene acceso limitado a la interfaz web de Panorama. Solo se le permite acceder para especificar la clave de reclamación y el número de serie del cortafuegos de ZTP para registrar los cortafuegos en el CSP y Panorama. El administrador del instalador puede crearse en Panorama o mediante autenticación remota, como RADIUS, SAML o TACACS +.
- **Clave de reclamación**: clave numérica de ocho dígitos conectada físicamente al cortafuegos de ZTP que se utiliza para registrar el cortafuegos de ZTP con el CSP.
- **To-SW-Version (Versión de SW de destino)**: designa la versión de software de PAN-OS del cortafuegos de ZTP (**Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**). Seleccione la versión de PAN-OS de destino, y si el cortafuegos está ejecutando una versión anterior a la versión indicada, iniciará un ciclo de actualización hasta que la versión de destino se instale correctamente.

> *Panorama solo puede gestionar cortafuegos que ejecuten una versión de PAN-OS igual o inferior a la instalada en Panorama.*

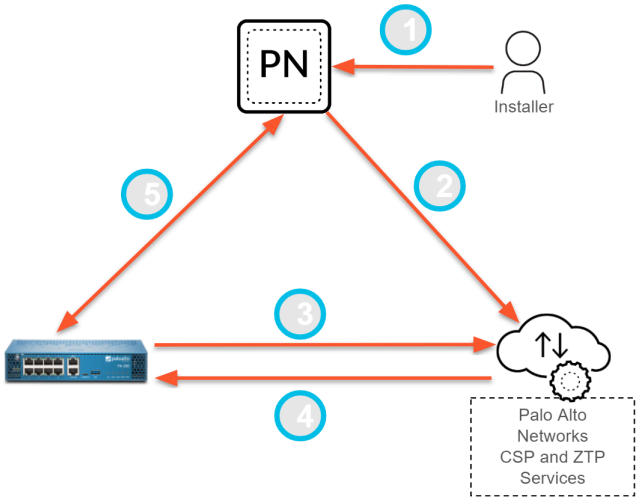
Después de instalar correctamente el complemento ZTP en Panorama y registrar Panorama con el servicio ZTP, el proceso de incorporación de ZTP continúa de la siguiente manera:

1. El instalador o administrador de TI registra los cortafuegos ZTP agregándolos a Panorama mediante el número de serie del cortafuegos y la clave de reclamación.
2. Panorama registra los cortafuegos con el CSP. Una vez que los cortafuegos se registren con éxito, este se asociará con el mismo inquilino ZTP que Panorama en el servicio ZTP.

   Los cortafuegos ZTP registrados correctamente con el servicio ZTP se añaden automáticamente como cortafuegos gestionados (**Panorama** > **Managed Devices [Dispositivos gestionados]**) en Panorama.

©2023 Palo Alto Networks, Inc.

3. Cuando el cortafuegos se conecta a Internet, el cortafuegos ZTP solicita un certificado de dispositivo al CSP para conectarse al servicio ZTP.
4. El servicio ZTP envía la IP de Panorama o el FQDN a los cortafuegos ZTP.
5. Los cortafuegos ZTP se conectan a Panorama y el grupo de dispositivos y las configuraciones de la plantilla se envían desde Panorama a los cortafuegos ZTP.



Instalación del complemento de ZTP

Instale el complemento de ZTP en su servidor de gestión Panorama™ para registrar Panorama con el servicio de ZTP para reclamar cortafuegos de ZTP para una incorporación simplificada.

Si su Panorama está en una configuración de alta disponibilidad (HA, High Availability), instale el complemento ZTP y registre ambos peers de HA de Panorama con el servicio ZTP.

- Instalación del complemento de ZTP en Panorama
- Registro de Panorama con el servicio de ZTP

Instalación del complemento de ZTP en Panorama

Simplifique la incorporación y gestión de los cortafuegos de ZTP mediante la instalación del complemento de ZTP en su servidor de gestión Panorama.

STEP 1 | Instalación del certificado de dispositivo de Panorama.

STEP 2 | Inicie sesión en la interfaz web de Panorama como superusuario o administrador de Panorama con acceso a complementos de Panorama (**Panorama** > **Plugins (Complementos)**).

STEP 3 | Seleccione **Panorama** > **Plugins (Complementos)** y busque el complemento **`ztp`**.

STEP 4 | **Descargue** e **instale** la versión más reciente del complemento de ZTP.

Registro de Panorama con el servicio de ZTP

Registre el servidor de gestión Panorama™ con el servicio de ZTP para las implementaciones de ZTP nuevas y existentes.

- Registro de Panorama con el servicio de ZTP para nuevas implementaciones

©2023 Palo Alto Networks, Inc.

- Registro de Panorama con el servicio de ZTP para implementaciones existentes

Registro de Panorama con el servicio de ZTP para nuevas implementaciones

Después de instalar el complemento de ZTP en el servidor de gestión Panorama™, debe registrar Panorama con el servicio de ZTP para permitir que dicho servicio asocie los cortafuegos con Panorama. Como parte del proceso de registro para la nueva implementación de ZTP, genere automáticamente las configuraciones del grupo de dispositivos y de la plantilla necesarias para conectar sus cortafuegos de ZTP al servicio de ZTP. Después de que el grupo de dispositivos y la plantilla se generan automáticamente, debe añadir los cortafuegos de ZTP al grupo de dispositivos y la plantilla para que puedan conectarse al servicio de ZTP después de conectarse por primera vez a Panorama.

STEP 1 | Instalación del certificado de dispositivo de Panorama.

STEP 2 | Inicie sesión en el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks.

STEP 3 | Asocie Panorama con el servicio de ZTP en el CSP de Palo Alto Networks.

El servicio de ZTP admite la asociación de hasta dos soluciones Panorama solo si tienen establecida una configuración de alta disponibilidad (High Availability, HA). Si Panorama no está en una configuración de HA, solo se puede asociar una única solución Panorama.

1. Seleccione **Assets (Activos)** > **ZTP Service (Servicio de ZTP)** y **Associate Panorama(s) [Asociar Panorama]**.
2. Seleccione el número de serie de Panorama que gestiona sus cortafuegos de ZTP.
3. (Solo HA) Seleccione el número de serie del peer de HA de Panorama.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Inicio de sesión en la interfaz web de Panorama.

STEP 5 | Seleccione **Panorama** > **Zero Touch Provisioning** > **Setup (Configuración)** y edite la configuración de ZTP **General**.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Registre Panorama con el servicio de ZTP.

1. **Habilite el servicio de ZTP**.
2. Especifique el **FQDN o dirección IP de Panorama**.

   Este es el FQDN o dirección IP pública del complemento de ZTP de Panorama instalado y que el CSP enviará a los cortafuegos ZTP.

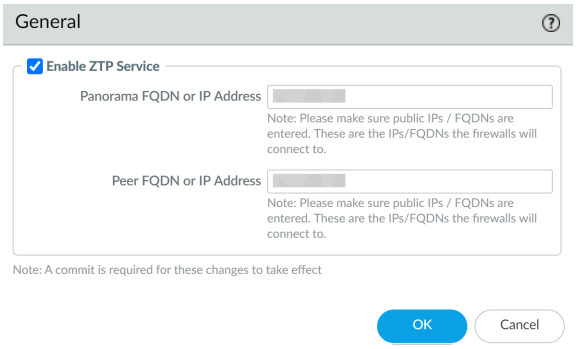
   (Cortafuegos gestionados que ejecutan PAN-OS 10.1.4 y versiones anteriores) Introduzca la dirección IP de Panorama para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización exitosa de PAN-OS.

   Si necesita usar el FQDN de Panorama, configure una ruta de destino estática para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización correcta de PAN-OS.
3. (Solo HA) Especifique el **FQDN o la dirección IP del peer**.

   Este es el FQDN o dirección IP pública del peer de Panorama en el que está instalado el complemento de ZTP y que el CSP envía a los cortafuegos ZTP en caso de conmutación por error.

   (Cortafuegos gestionados que ejecutan PAN-OS 10.1.4 y versiones anteriores) Introduzca la dirección IP de Panorama para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización exitosa de PAN-OS.

   Si necesita usar el FQDN de Panorama, configure una ruta de destino estática para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización correcta de PAN-OS.
4. Haga clic en **Aceptar** para guardar los cambios.



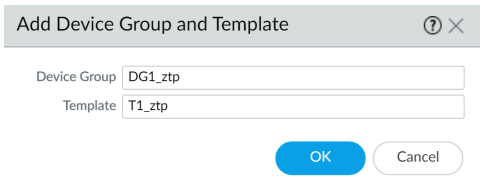
 ©2023 Palo Alto Networks, Inc.

STEP 7 | Cree el grupo de dispositivos y la plantilla predeterminados para generar automáticamente la configuración necesaria para conectar sus cortafuegos de ZTP a Panorama.

La adición del grupo de dispositivos y la plantilla genera automáticamente un nuevo grupo de dispositivos y plantilla que contienen la configuración predeterminada para conectar los cortafuegos de ZTP y Panorama.

Palo Alto Networks recomienda dar al grupo de dispositivos ZTP y a la plantilla un nombre descriptivo que deje claro su propósito. La modificación involuntaria de la configuración predeterminada de ZTP da lugar a problemas de conectividad si desea reutilizar el grupo de dispositivos y la plantilla para incorporar nuevos cortafuegos ZTP en el futuro.

1. **Añada un grupo de dispositivos y plantilla**.
2. Especifique el nombre del **grupo de dispositivos**.
3. Especifique el **nombre de la plantilla**.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.



STEP 8 | Añada sus cortafuegos de ZTP al grupo de dispositivos y la plantilla especificados en el paso anterior.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y elija el grupo de dispositivos creado automáticamente.
2. Seleccione los **dispositivos** de ZTP.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.
5. En la sección **Templates (Plantillas)**, **añada** la plantilla que se creó automáticamente.
6. Seleccione los **dispositivos** de ZTP.
7. Haga clic en **Aceptar** para guardar los cambios.

STEP 9 | Modifique el grupo de dispositivos ZTP, las plantillas y la pila de plantillas según sea necesario.

No se admite el traslado de un cortafuegos ZTP a un grupo de dispositivos o pila de plantillas diferente. Debe mantener los cortafuegos ZTP en el grupo de dispositivos ZTP y la pila de plantillas que incluye la plantilla ZTP que se creó. Esto es necesario para que el cortafuegos mantenga la conectividad con Panorama y evite que la configuración no deseada se revierta en el cortafuegos.

Cuando considere la jerarquía de grupo de dispositivos y la prioridad de la plantilla en su pila de plantillas, asegúrese de que el grupo de dispositivos y la plantilla que contienen la configuración de ZTP necesaria que permite que el cortafuegos de ZTP y Panorama se

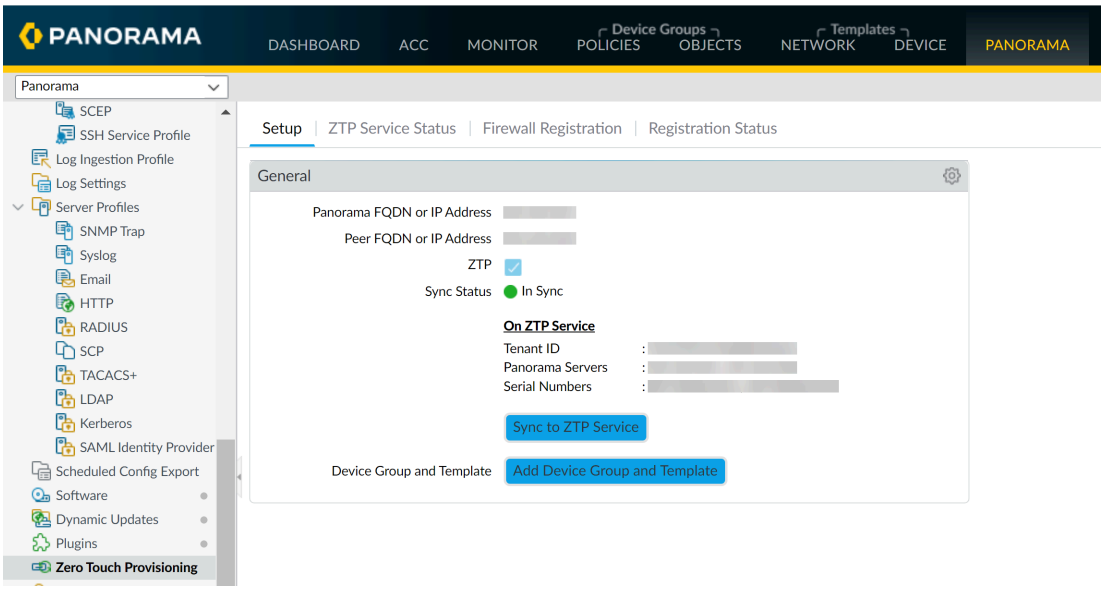
 ©2023 Palo Alto Networks, Inc.

comuniquen tengan configurada una prioridad que permita que la configuración no se anule en caso de configuraciones conflictivas.

Si modifica el grupo de dispositivos ZTP y la plantilla utilizados para incorporar el cortafuegos ZTP, tenga cuidado de no modificar ninguna de las configuraciones ZTP que se rellenaron automáticamente cuando creó el grupo de dispositivos y la plantilla en el paso anterior. Esto incluye configuraciones como la dirección IP de Panorama, el enrutador virtual, la interfaz `ethernet1/1` la zona de seguridad de la interfaz `ethernet1/1` la interfaz de bucle invertido `loopback.900` la regla de la política de seguridad `rule1`, la regla de la política NAT `ztp-nat` y la ruta de servicio. Estas configuraciones son necesarias para conectar el cortafuegos ZTP a Panorama y pueden provocar problemas de conectividad si se modifican.

STEP 10 | Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 11 | **Sincronice al servicio de ZTP** y compruebe que el estado de la sincronización de Panorama muestre `In Sync (En sincronización)`.



Registro de Panorama con el servicio de ZTP para implementaciones existentes

Después de instalar el complemento de ZTP en el servidor de gestión Panorama™, debe registrar Panorama con el servicio de ZTP para permitir que dicho servicio asocie los cortafuegos con Panorama. Como parte del proceso de registro, añada sus cortafuegos de ZTP a un grupo de dispositivos ZTP existente y a una pila de plantillas que contengan la configuración de ZTP necesaria para conectar sus cortafuegos de ZTP con el servicio de ZTP después de conectarse por primera vez a Panorama.

Este procedimiento supone

STEP 1 | Instalación del certificado de dispositivo de Panorama.

STEP 2 | Inicie sesión en el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Asocie Panorama con el servicio de ZTP en el CSP de Palo Alto Networks.

El servicio de ZTP admite la asociación de hasta dos soluciones Panorama solo si tienen establecida una configuración de alta disponibilidad (High Availability, HA). Si Panorama no está en una configuración de HA, solo se puede asociar una única solución Panorama.

1. Seleccione **Assets (Activos)** > **ZTP Service (Servicio de ZTP)** y **Modify Association (Modificar asociación)**.
2. Seleccione el número de serie de Panorama que gestiona sus cortafuegos de ZTP.
3. (Solo HA) Seleccione el número de serie del peer de HA de Panorama.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Inicio de sesión en la interfaz web de Panorama.

STEP 5 | Seleccione **Panorama** > **Zero Touch Provisioning** > **Setup (Configuración)** y edite la configuración de ZTP **General**.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Registre Panorama con el servicio de ZTP.

1. **Habilite el servicio de ZTP**.
2. Especifique el **FQDN o dirección IP de Panorama**.

   Este es el FQDN o dirección IP pública del complemento de ZTP de Panorama instalado y que el CSP enviará a los cortafuegos ZTP.

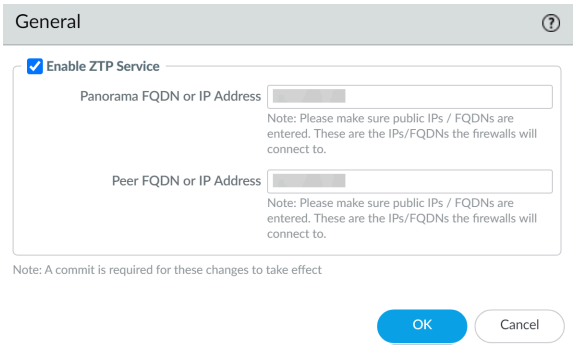
   (Cortafuegos gestionados que ejecutan PAN-OS 10.1.4 y versiones anteriores) Introduzca la dirección IP de Panorama para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización exitosa de PAN-OS.

   Si necesita usar el FQDN de Panorama, configure una ruta de destino estática para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización correcta de PAN-OS.
3. (Solo HA) Especifique el **FQDN o la dirección IP del peer**.

   Este es el FQDN o dirección IP pública del peer de Panorama en el que está instalado el complemento de ZTP y que el CSP envía a los cortafuegos ZTP en caso de conmutación por error.

   (Cortafuegos gestionados que ejecutan PAN-OS 10.1.4 y versiones anteriores) Introduzca la dirección IP de Panorama para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización exitosa de PAN-OS.

   Si necesita usar el FQDN de Panorama, configure una ruta de destino estática para evitar que el cortafuegos gestionado se desconecte de Panorama al reiniciar o después de una actualización correcta de PAN-OS.
4. Haga clic en **Aceptar** para guardar los cambios.



 ©2023 Palo Alto Networks, Inc.

STEP 7 | Añada los cortafuegos ZTP al grupo de dispositivos ZTP existente y a la pila de plantillas que contengan la configuración ZTP necesaria.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y seleccione el grupo de dispositivos ZTP.
2. Seleccione los **dispositivos** de ZTP.
3. Haga clic en **Aceptar** para guardar los cambios.
4. Seleccione **Panorama** > **Templates (Plantillas)** y seleccione la pila de plantillas que contiene la plantilla ZTP.
5. Seleccione los **dispositivos** de ZTP.
6. Haga clic en **Aceptar** para guardar los cambios.

STEP 8 | Modifique el grupo de dispositivos ZTP, las plantillas y la pila de plantillas según sea necesario.

No se admite el traslado de un cortafuegos ZTP a un grupo de dispositivos o pila de plantillas diferente. Debe mantener los cortafuegos integrados de ZTP en el grupo de dispositivos ZTP y las plantillas que se crearon. Esto es necesario para que el cortafuegos mantenga la conectividad con Panorama y evite que la configuración no deseada se revierta en el cortafuegos.

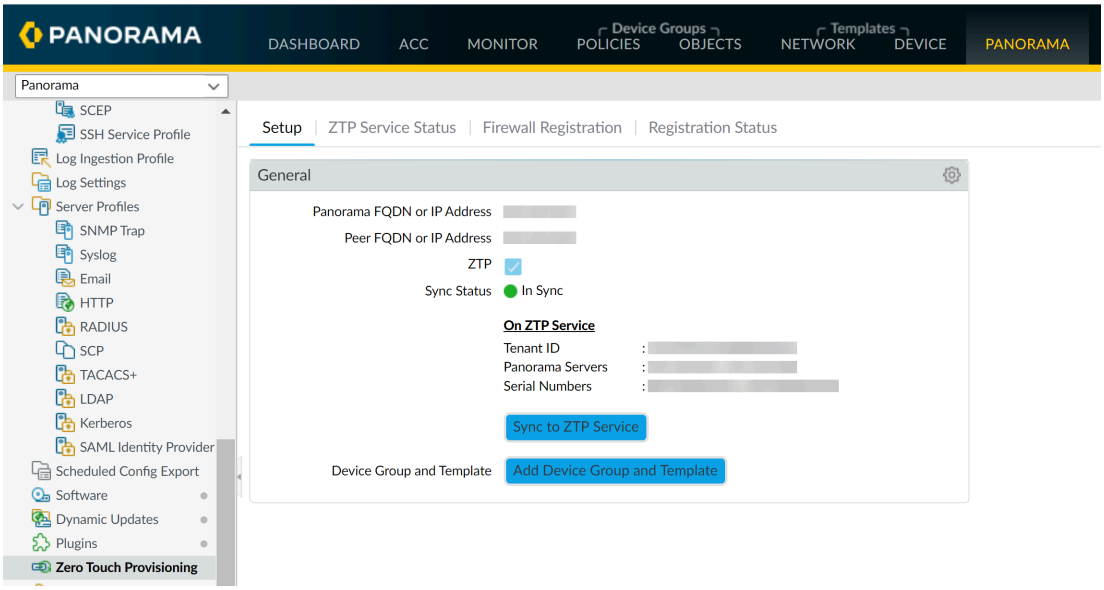
Cuando considere la jerarquía de grupo de dispositivos y la prioridad de la plantilla en su pila de plantillas, asegúrese de que el grupo de dispositivos y la plantilla que contienen la configuración de ZTP necesaria que permite que el cortafuegos de ZTP y Panorama se comuniquen tengan configurada una prioridad que permita que la configuración no se anule en caso de configuraciones conflictivas.

Si modifica el grupo de dispositivos ZTP y la plantilla utilizados para incorporar el cortafuegos ZTP, tenga cuidado de no modificar ninguna de las configuraciones ZTP que se rellenaron automáticamente cuando creó el grupo de dispositivos y la plantilla en el paso anterior. Esto incluye configuraciones como la dirección IP de Panorama, el enrutador virtual, la interfaz `ethernet1/1` la zona de seguridad de la interfaz `ethernet1/1` la interfaz de bucle invertido `loopback.900` la regla de la política de seguridad `rule1`, la regla de la política NAT `ztp-nat` y la ruta de servicio. Estas configuraciones son necesarias para conectar el cortafuegos ZTP a Panorama y pueden provocar problemas de conectividad si se modifican.

STEP 9 | Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | **Sincronice al servicio de ZTP** y compruebe que el estado de la sincronización de Panorama muestre `In Sync (En sincronización)`.



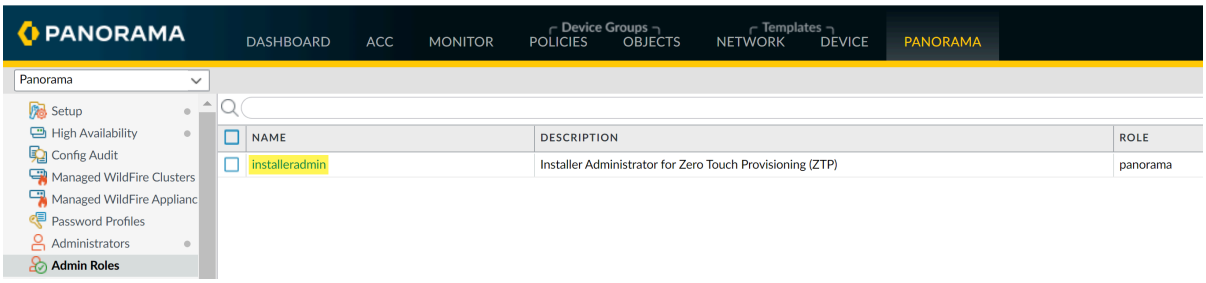
Configuración de la cuenta de administrador del instalador de ZTP

El usuario administrador del instalador de ZTP es una cuenta de administrador creada para el personal que no es de TI o el contratista de instalación para incorporar nuevos cortafuegos de ZTP. El administrador del instalador utiliza una función de administración `installeradmin` creada automáticamente para limitar la visibilidad en la interfaz web de Panorama y solo permite al instalador la capacidad de especificar el número de serie y la clave de reclamación del cortafuegos de ZTP en Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Admin Roles (Funciones de administrador)** y compruebe que se haya creado la función de administración `installeradmin`.

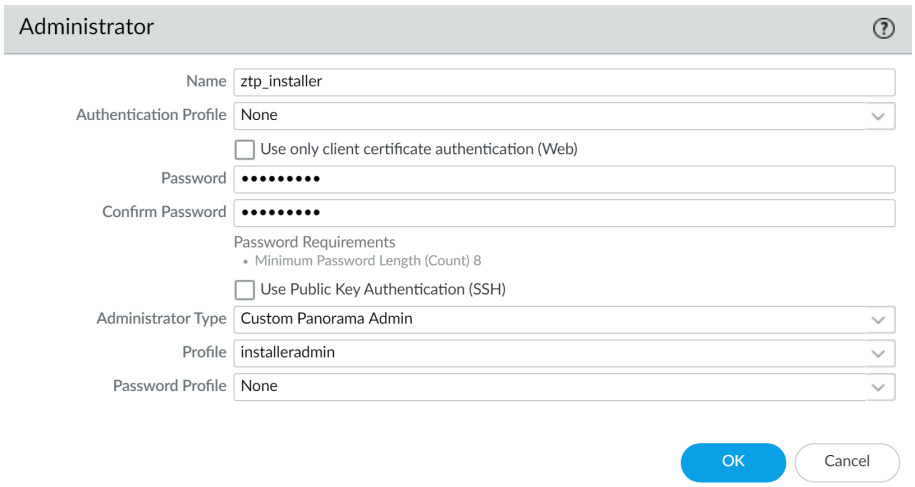
`installeradmin` se crea automáticamente después de instalar el complemento de ZTP en Panorama correctamente.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el usuario administrador del instalador de ZTP.

1. Seleccione **Panorama** > **Administrators (Administradores)** y **añada** un nuevo usuario administrador.
2. Especifique un **nombre** descriptivo para el usuario administrador del instalador de ZTP.
3. Introduzca una **contraseña** segura y **confírmela**.
4. En **Administrator Type (Tipo de administrador)**, seleccione **Custom Panorama Admin (Administrador de Panorama personalizado)**.
5. En **Profile (Perfil)**, seleccione **installeradmin**.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.



STEP 4 | Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

Adición de cortafuegos de ZTP a Panorama

Puede añadir un único cortafuegos de ZTP o importar varios en el servidor de gestión Panorama™.

- Adición de un cortafuegos a Panorama
- Importación de varios cortafuegos de ZTP a Panorama

Adición de un cortafuegos a Panorama

Inicie sesión en la interfaz web del servidor de gestión Panorama™ como superusuario, administrador de Panorama o administrador del instalador de ZTP para añadir un cortafuegos de ZTP a Panorama. Para agregar el cortafuegos de ZTP, debe especificar el número de serie del cortafuegos y la clave de reclamación proporcionados por Palo Alto Networks y, después, registrar el cortafuegos con el servicio de ZTP. Al registrar el cortafuegos, se reclama como un activo en su cuenta en el Portal de atención al cliente y se permite que el servicio de ZTP asocie el cortafuegos con Panorama.

No se admite la migración de un cortafuegos añadido a la gestión de Panorama mediante ZTP de un Panorama a otro.

 ©2023 Palo Alto Networks, Inc.

Mientras añade cortafuegos ZTP a Panorama, no realice ninguna confirmación en el cortafuegos ZTP antes de verificar que se haya agregado correctamente a Panorama en el paso 4. La realización de una confirmación local en el cortafuegos ZTP deshabilita la funcionalidad ZTP y provoca que no se pueda añadir correctamente el cortafuegos a Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Añada un cortafuegos a Panorama.

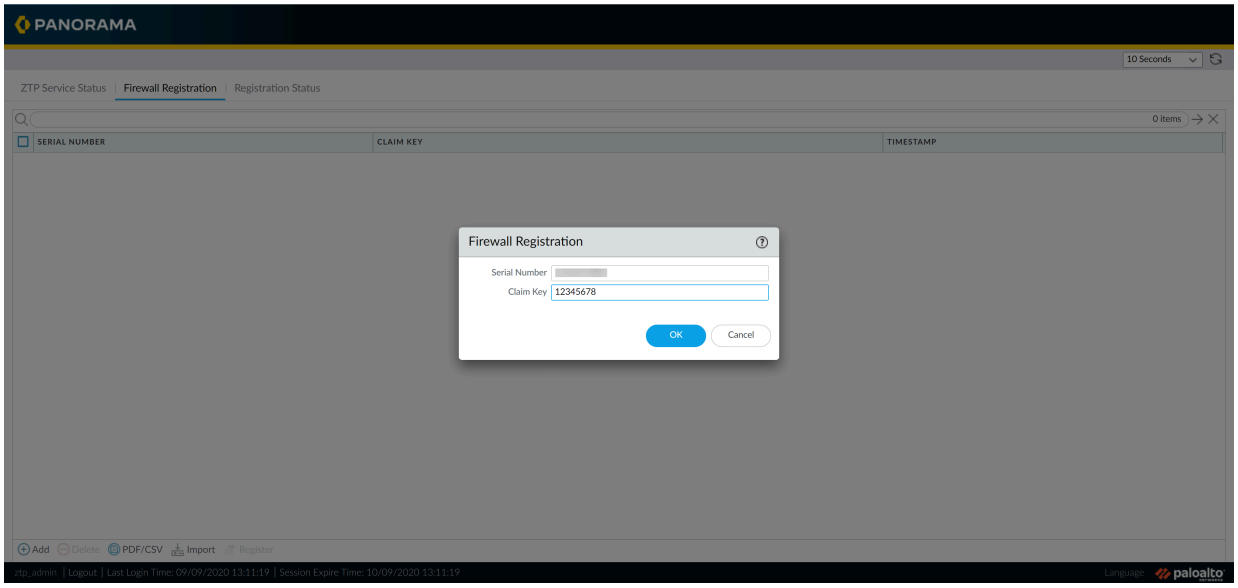
Debe conectar la interfaz Eth1/1 en los cortafuegos ZTP para registrar correctamente los cortafuegos ZTP con el CSP e impulsar la política y las configuraciones de red.

1. Seleccione **Firewall Registration (Registro del cortafuegos)** y **añada** un nuevo cortafuegos de ZTP.
2. Especifique el **número de serie** del cortafuegos de ZTP.
3. Introduzca la **clave de reclamación** del cortafuegos de ZTP proporcionada por Palo Alto Networks.

   La clave numérica de reclamación (ocho dígitos) está impresa en una etiqueta física sobre la parte posterior del cortafuegos de ZTP enviado por Palo Alto Networks.



4. Haga clic en **OK (Aceptar)** para guardar los cambios.



 ©2023 Palo Alto Networks, Inc.

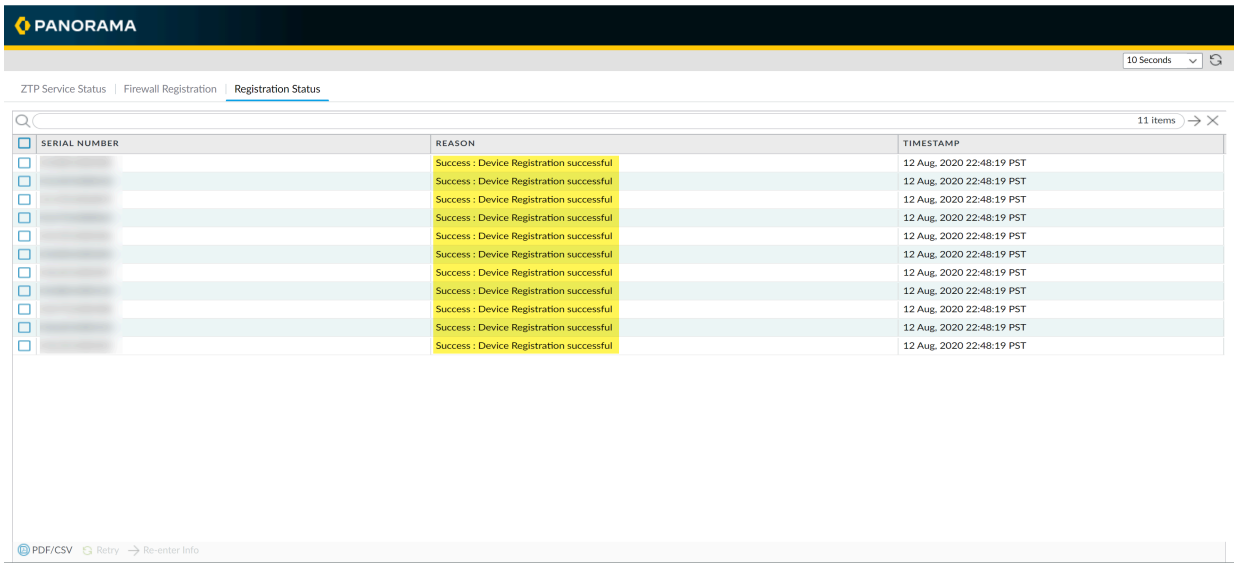
STEP 3 | Registre el cortafuegos de ZTP.

1. Seleccione el cortafuegos de ZTP recién añadido y **regístrelo**.
2. Cuando se le solicite, haga clic en **Yes (Sí)** para confirmar el registro del cortafuegos de ZTP.

STEP 4 | Compruebe que el cortafuegos se haya registrado correctamente con el CSP.

El cortafuegos debe registrarse correctamente con el CSP para obtener el certificado del dispositivo.

1. Seleccione **Registration Status (Estado de registro)** y compruebe que el cortafuegos de ZTP se haya registrado correctamente con el CSP.



2. Inicio de sesión en la interfaz web de Panorama mediante credenciales de administrador.
3. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y compruebe que el cortafuegos de ZTP se haya añadido correctamente como cortafuegos gestionado.

*Asegúrese de que la columna **To SW Version (Versión de SW de destino)** esté configurada en la versión de PAN-OS correcta de manera que el cortafuegos no se actualice o se revierta a una versión anterior de forma no intencionada. La funcionalidad de ZTP solo es compatible con PAN-OS 10.0.1 y versiones posteriores. Además, la versión PAN-OS debe ser la misma o una versión anterior de la versión PAN-OS que se ejecute en Panorama.*

Para obtener más información, consulte Actualización de un cortafuegos ZTP*.*

©2023 Palo Alto Networks, Inc.

STEP 5 | Añada los cortafuegos ZTP al grupo de dispositivos y la pila de plantillas que contengan la configuración de ZTP necesaria.

Debe añadir el cortafuegos ZTP a un grupo de dispositivos y una pila de plantillas para que sus cortafuegos se muestren como `Connected (Conectado)` para impulsar configuraciones de red y políticas.

Debe mantener el cortafuegos ZTP en el grupo de dispositivos ZTP y la pila de plantillas a la que está asociada la plantilla ZTP. Esto es necesario para que el cortafuegos mantenga la conectividad con Panorama y evite que la configuración no deseada se revierta en el cortafuegos.

1. Inicio de sesión en la interfaz web de Panorama mediante credenciales de administrador.
2. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y añada el cortafuegos ZTP al grupo de dispositivos creado cuando registró Panorama con el servicio ZTP.

   Esto es necesario para que el cortafuegos ZTP se conecte correctamente a Panorama.
3. Seleccione **Panorama** > **Templates (Plantillas)**, añada el cortafuegos ZTP a la pila de plantillas que creó cuando registró Panorama con el servicio ZTP.

   Esto es necesario para que el cortafuegos ZTP se conecte correctamente a Panorama.

Importación de varios cortafuegos de ZTP a Panorama

Inicie sesión en la interfaz web del servidor de gestión Panorama™ como superusuario, administrador de Panorama o administrador del instalador de ZTP para importar varios cortafuegos de ZTP en Panorama. Para importar varios cortafuegos de ZTP, debe importar un archivo CSV del número de serie del cortafuegos de ZTP y la clave de reclamación correspondiente proporcionados por Palo Alto Networks y, después, registrar los cortafuegos con el servicio de ZTP. Al registrar el cortafuegos, se reclama como un activo en su cuenta en el Portal de atención al cliente y se permite que el servicio de ZTP asocie el cortafuegos con Panorama.

No se admite la migración de un cortafuegos añadido a la gestión de Panorama mediante ZTP de un Panorama a otro.

Mientras añade cortafuegos ZTP a Panorama, no realice ninguna confirmación en el cortafuegos ZTP antes de verificar que se haya agregado correctamente a Panorama en el paso 5. La realización de una confirmación local en el cortafuegos ZTP deshabilita la funcionalidad ZTP y provoca que no se pueda añadir correctamente el cortafuegos a Panorama.

STEP 1 | Reúna los números de serie y las claves de reclamación para sus cortafuegos de ZTP.

La clave numérica de reclamación (ocho dígitos) está impresa en una etiqueta física sobre la parte posterior del cortafuegos de ZTP enviado por Palo Alto Networks.



 ©2023 Palo Alto Networks, Inc.

STEP 2 | Cree un archivo CSV que contenga los números de serie y las claves de reclamación del cortafuegos de ZTP. La primera columna debe contener los números de serie y la segunda la clave de reclamación correspondiente para ese cortafuegos. Consulte el siguiente ejemplo como referencia.

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

STEP 3 | Importe los cortafuegos de ZTP a Panorama.

Debe conectar la interfaz Eth1/1 en los cortafuegos ZTP para registrar correctamente los cortafuegos ZTP con el CSP e impulsar la política y las configuraciones de red.

1. Inicio de sesión en la interfaz web de Panorama mediante las credenciales de administrador del instalador de ZTP.
2. Seleccione **Panorama** > **Zero Touch Provisioning** > **Firewall Registration (Registro de cortafuegos)** e **importe** los cortafuegos de ZTP.
3. **Busque** y seleccione el archivo CSV que contiene la información del cortafuegos de ZTP y haga clic en **OK (Aceptar)**.

STEP 4 | Registre los cortafuegos de ZTP.

1. Seleccione los cortafuegos de ZTP recién añadidos y **regístrelos**.
2. Cuando se le solicite, haga clic en **Yes (Sí)** para confirmar el registro de los cortafuegos de ZTP.

STEP 5 | Compruebe que el cortafuegos se haya registrado correctamente con el servicio de ZTP.

1. Seleccione **Registration Status (Estado de registro)** y compruebe que los cortafuegos de ZTP se hayan registrado correctamente con el servicio de ZTP.
2. Inicio de sesión en la interfaz web de Panorama mediante credenciales de administrador.
3. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y compruebe que los cortafuegos de ZTP se hayan añadido correctamente como cortafuegos gestionados.

*Asegúrese de que la columna **To SW Version (Versión de SW de destino)** esté configurada en la versión de PAN-OS correcta de manera que el cortafuegos no se actualice o se revierta a una versión anterior de forma no intencionada. La funcionalidad de ZTP solo es compatible con PAN-OS 10.0.1 y versiones posteriores. Además, la versión PAN-OS debe ser la misma o una versión anterior de la versión PAN-OS que se ejecute en Panorama.*

Para obtener más información, consulte Actualización de un cortafuegos ZTP.

©2023 Palo Alto Networks, Inc.

STEP 6 | Añada los cortafuegos ZTP al grupo de dispositivos y la pila de plantillas que contengan la configuración de ZTP necesaria.

Debe añadir el cortafuegos ZTP a un grupo de dispositivos y una pila de plantillas para que sus cortafuegos se muestren como `Connected (Conectado)` para impulsar configuraciones de red y políticas.



Debe mantener el cortafuegos ZTP en el grupo de dispositivos ZTP y la pila de plantillas a la que está asociada la plantilla ZTP. Esto es necesario para que el cortafuegos mantenga la conectividad con Panorama y evite que la configuración no deseada se revierta en el cortafuegos.

1. Inicio de sesión en la interfaz web de Panorama mediante credenciales de administrador.
2. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y añada el cortafuegos ZTP al grupo de dispositivos creado cuando registró Panorama con el servicio ZTP.

   Esto es necesario para que el cortafuegos ZTP se conecte correctamente a Panorama.
3. Seleccione **Panorama** > **Templates (Plantillas)**, añada el cortafuegos ZTP a la pila de plantillas que creó cuando registró Panorama con el servicio ZTP.

   Esto es necesario para que el cortafuegos ZTP se conecte correctamente a Panorama.

Uso de la CLI para tareas de ZTP

Utilice los siguientes comandos de la CLI para realizar tareas de Zero Touch Provisioning (ZTP) y ver el estado del servicio de ZTP.

Si quiere...	Use...
Administer the firewall from the firewall CLI (Administrar el cortafuegos desde la CLI del cortafuegos)	
Muestra el estado de la conexión al servicio ZTP.	`> show system ZTP status`
Muestra el estado de la conexión al servidor de gestión Panorama.	`> show panorama status`
Muestra el número de modelo de ZTP y la información del sistema del cortafuegos.	`> show system info`
Desactiva la máquina de estado ZTP en el cortafuegos. La ejecución de este comando no elimina ninguna configuración ZTP existente.	`> request disable-ztp`

©2023 Palo Alto Networks, Inc.

Si quiere...	Use...
No puede volver a habilitar la máquina de estado ZTP en el cortafuegos después de que se deshabilite desde la CLI. *Para volver a habilitarlo, debe* restablecer el cortafuegos a la configuración predeterminada de fábrica.	
Registro, configuración y gestión de los cortafuegos de ZTP en Panorama	

Cree una plantilla o un grupo de dispositivos que contenga las configuraciones necesarias para conectar cortafuegos gestionados con Panorama mediante el servicio de ZTP en la interfaz Eth1/1.	`> request plugins ztp create dgroup-template device-group <device group name>`
	
	`> request plugins ztp create dgroup-template template <template name>`

Añada un cortafuegos de ZTP a la lista de cortafuegos para el registro posterior con el servicio de ZTP.	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`
Modifique el número de serie del firewall de ZTP que ya se ha añadido a la lista de firewalls para su posterior registro en el servicio de ZTP.	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
Elimine un cortafuegos de ZTP de la lista de cortafuegos para el registro posterior con el servicio de ZTP.	`> request plugins ztp firewall-delete firewall <serial number>`
Añada un cortafuegos de ZTP a la lista de cortafuegos por si vuelve a registrarlo posteriormente con el servicio de ZTP. Utilice este comando cuando un cortafuegos de ZTP no consiga realizar inicialmente el registro con el servicio de ZTP y sea necesario realizarlo.	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`

©2023 Palo Alto Networks, Inc.

Si quiere...	Use...
Registre su servidor de gestión Panorama™ con el servicio de ZTP.	`> request plugins ztp panorama-registration`
Registre un cortafuegos de ZTP con el servicio de ZTP.	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
Vuelva a registrar los cortafuegos de ZTP con el servicio de ZTP. Use este comando para iniciar el proceso de reinscripción para un cortafuegos de ZTP para el que falló el registro inicial con el servicio de ZTP.	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
Importe la información de la clave de reclamación y el número de serie del cortafuegos de ZTP. El archivo especificado debe estar en formato CSV.	`> request plugins ztp ztp-add-import import-path <file path>`
Consulta de información del cortafuegos de ZTP y del estado del servicio de ZTP en Panorama	
Recupere la lista de cortafuegos de ZTP registrados en Panorama a partir del servicio de ZTP.	`> request plugins ztp ztp-service-info` Se muestra la siguiente información: • `first-firewall-connect-time`: marca de tiempo de cuando el cortafuegos de ZTP se conectó por primera vez al servicio de ZTP. • `last-firewall-connect-time`: marca de tiempo de cuándo se conectó por última vez el cortafuegos de ZTP al servicio de ZTP. • `registration-time`: marca de tiempo de cuando el cortafuegos de ZTP se registró con el servicio de ZTP. • `isZTPFirewall`: si el cortafuegos es un cortafuegos de ZTP. • `created_by`: usuario administrativo que añadió el cortafuegos de ZTP.

©2023 Palo Alto Networks, Inc.

Si quiere...	Use...
	• `IP address (Dirección IP)`: dirección IP del cortafuegos de ZTP.
Consulte la lista de cortafuegos de ZTP en la lista de cortafuegos que se registrarán con el servicio de ZTP.	`> show plugins ztp device-add-list`
Consulte el estado de registro de sus cortafuegos de ZTP.	`> show plugins ztp device-reg-status`
Consulte el estado de sincronización del servicio de ZTP para los cortafuegos de ZTP.	`> request plugins ztp ztp-sync-status`
Muestra el historial de conectividad ZTP del plano de gestión completo. Esto es útil para solucionar problemas de conectividad con el servicio ZTP.	`> tail follow yes mp-log ms.log`

Desinstalación del complemento de ZTP

Siga el procedimiento para eliminar la configuración ZTP de su servidor de gestión Panorama™ y desinstale el complemento ZTP. Si su dispositivo Panorama está en una configuración de alta disponibilidad (HA), repita estos pasos en ambos peers de HA de Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Elimine la cuenta de administrador del instalador de ZTP.

1. Seleccione **Panorama** > **Administrators (Administradores)** y elija la cuenta de administrador del instalador ZTP configurado anteriormente.
2. **Elimine** la cuenta de administrador del instalador de ZTP.
3. Seleccione **Panorama** > **Administrators (Administradores)** y la función de administración `installeradmin`.
4. **Elimine** la función de administración `installeradmin`.
5. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

©2023 Palo Alto Networks, Inc.

STEP 3 | Desinstale el complemento de ZTP.

1. Seleccione **Panorama** > **Plugins (Complementos)** y diríjase al complemento ZTP instalado en Panorama.
2. En la columna Actions (Acciones), utilice **Remove Config (Eliminar configuración)** para eliminar configuraciones relacionadas con ZTP de Panorama.
3. Haga clic en **OK (Aceptar)** cuando se le solicite que confirme la eliminación de la configuración ZTP de Panorama.
4. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.
5. **Desinstale** el complemento de ZTP.
6. Haga clic en **OK (Aceptar)** cuando se le solicite desinstalar el complemento ZTP de Panorama.

 ©2023 Palo Alto Networks, Inc.

Gestión de grupos de dispositivos

- Adición de un grupo de dispositivos
- Creación de una jerarquía del grupo de dispositivos
- Creación de objetos para su uso en una política compartida o de grupo de dispositivos
- Volver a los valores de objeto heredados
- Gestión de objetos compartidos no utilizados
- Gestión de la precedencia de objetos heredados
- Movimiento o duplicación de una regla de política u objeto a un grupo de dispositivos diferente
- Ingreso de una regla de política a un subconjunto de cortafuegos
- Envío de grupos de dispositivos a un cortafuegos de sistemas virtuales múltiples
- Gestión de la jerarquía de reglas

Adición de un grupo de dispositivos

Después de añadir cortafuegos (consulte Cómo añadir un cortafuegos como dispositivo gestionado), siga este procedimiento para reunirlos en Grupos de dispositivos (hasta 1024). Asegúrese de asignar ambos cortafuegos en una configuración de Alta disponibilidad (high availability, HA) activa-pasiva al mismo grupo de dispositivos de forma tal que Panorama ingrese las mismas reglas de políticas y objetos a estos cortafuegos. PAN-OS no sincroniza las reglas ingresadas en todos los peers de HA. Si desea gestionar las reglas y los objetos en diferentes niveles administrativos de la organización, consulte Creación de una jerarquía del grupo de dispositivos.

STEP 1 | Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.

STEP 3 | En la sección Dispositivos, seleccione las casillas de verificación para asignar cortafuegos al grupo. Para buscar una lista larga de cortafuegos, use los filtros.

> ***Puede asignar cada cortafuegos a solo un grupo de dispositivos. Puede asignar cada sistema virtual de un cortafuegos a un grupo de dispositivos diferente.***

STEP 4 | En la sección Reference Template (Plantilla de referencia), haga clic en **Add (Añadir)** para especificar las plantillas o las pilas de plantillas con objetos a los que se hace referencia en la configuración del grupo de dispositivos.

Debe asignar al grupo de dispositivos las referencias adecuadas a plantillas o pilas de plantillas para que estas se asocien al grupo. De ese modo, puede hacer referencia a objetos configurados en plantillas o pilas de plantillas sin tener que añadir el dispositivo no relacionado a pilas de plantillas.

Omita este paso si la configuración del grupo de dispositivos no hace referencia a ningún objeto configurado en plantillas o pilas de plantillas.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Seleccione **Group HA Peers (Peers de HA del grupo)** para los cortafuegos que sean peers de HA.

Solo puede agrupar peers de HA gestionados de cortafuegos si están en el mismo grupo de dispositivos.

El nombre del cortafuegos del peer secundario activo o pasivo se encuentra entre paréntesis. La agrupación de peers de HA supone un cambio visual y no se produce ningún cambio de configuración.

STEP 6 | Seleccione **Parent Device Group (Grupo de dispositivos primario)** (de manera predeterminada, **Shared** [Compartido]) que estará justo por encima del grupo de dispositivos que está creando en la jerarquía del grupo de dispositivos.

STEP 7 | Si sus reglas de políticas harán referencia a usuarios y grupos, asigne un cortafuegos **Master (Maestro)**.

Este será el único cortafuegos el grupo de dispositivos desde el cual Panorama recopila información de nombre y grupo de usuarios.

STEP 8 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 9 | Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego seleccione **Commit and Push (Confirmar y enviar)** para enviar sus cambios a la configuración de Panorama y al grupo de dispositivos que agregó.

Creación de una jerarquía del grupo de dispositivos

STEP 1 | Planifique la jerarquía del grupo de dispositivos.

1. Decida los niveles del grupo de dispositivos y qué cortafuegos y sistemas virtuales asignará a cada grupo de dispositivos y la ubicación compartida. Puede asignar cualquier cortafuegos o sistema virtual (vsys) a solo un grupo de dispositivos. Si un grupo de dispositivos será solo un contenedor de organización para los grupos de dispositivos de nivel inferior, no es necesario que asigne cortafuegos a este.
2. Elimine las asignaciones de cortafuegos o vsys del grupo de dispositivos existente si estas no se ajustan a su jerarquía planificada.
   1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y seleccione el grupo de dispositivos.
   2. En la sección Dispositivos, cancele la selección de las casillas de verificación de los cortafuegos y los sistemas virtuales que desea eliminar, y haga clic en **OK (Aceptar)**.
3. Si es necesario, añada más cortafuegos para asignarlos a los grupos de dispositivos: consulte Cómo añadir un cortafuegos como dispositivo gestionado.
4. Si está utilizando varios complementos de Panorama para realizar la supervisión de endpoints, un grupo de dispositivos que contiene cortafuegos implementados en un hipervisor en particular no puede ser el elemento principal o secundario de un grupo de dispositivos que contenga cortafuegos implementados en un hipervisor diferente. Consulte Jerarquía del grupo de dispositivos para obtener más información.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada un grupo de dispositivos para cada grupo de dispositivos de nivel superior.

1. En la página **Panorama** > **Device Groups (Grupos de dispositivos)**, haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para identificar el grupo de dispositivos.
2. En la sección Dispositivos, seleccione las casillas de verificación para asignar cortafuegos y sistemas virtuales al grupo de dispositivos.
3. Deje la opción **Parent Device Group (Grupo de dispositivos primario)** en **Shared (Compartido)** (opción predeterminada) y haga clic en **OK (Aceptar)**.

STEP 3 | Añada un grupo de dispositivos para cada grupo de dispositivos de nivel inferior.

- Para los grupos de dispositivos nuevos en cada nivel inferior, repita el paso anterior, pero configure el **Parent Device Group (Grupo de dispositivos primario)** para un grupo de dispositivos en el siguiente nivel por encima.
- Para cada grupo de dispositivos existente, en la página **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos para editarlo, seleccione un **Parent Device Group (Grupo de dispositivos primario)** y haga clic en **OK (Aceptar)**.



Si mueve un grupo de dispositivos a uno primario diferente, todos sus grupos de dispositivos secundarios se moverán con él, junto con todos los cortafuegos, las reglas de políticas y los objetos asociados con el grupo de dispositivos y sus descendientes. Si el nuevo grupo primario está en otro dominio de acceso, el grupo de dispositivos trasladado ya no tendrá membresía en el dominio de acceso original. Si el nuevo dominio de acceso tiene acceso de escritura y lectura para el grupo de dispositivos primario, también tendrá acceso de lectura y escritura para el grupo de dispositivos trasladado. Si el nuevo dominio de acceso solo tiene acceso de lectura para el grupo primario, no tendrá acceso para el grupo de dispositivos trasladado. Para volver a configurar el acceso para los grupos de dispositivos, consulte Configuración de un dominio de acceso*.*

STEP 4 | Configure, traslade y duplique objetos y reglas de políticas según sea necesario para la herencia en la jerarquía del grupo de dispositivos.

- Cree objetos para su uso en una política compartida o de grupo de dispositivos o edite los objetos existentes.

Puede editar los objetos solo en su ***ubicación***: el grupo de dispositivos al cual se asignaron. Los grupos de dispositivos secundarios heredan las instancias de solo lectura de los objetos de esa ubicación. Sin embargo, puede consultar de manera opcional el Paso Cancele los valores de objeto heredados.

- Cree o edite políticas.
- Mueva o duplique una regla de política u objeto a un grupo de dispositivos diferente.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Cancele los valores de objeto heredados.

Solo se aplica si los valores de objeto de un grupo de dispositivos determinado difieren de los valores heredados de un grupo de dispositivos primario.

Después de cancelar un objeto, puede anularlo de nuevo en los grupos de dispositivos secundarios. Sin embargo, nunca puede cancelar objetos compartidos o predefinidos (predeterminados).

En la pestaña **Objects (Objetos)**, los objetos heredados tienen un icono verde en la columna Nombre y la columna Ubicación muestra el grupo de dispositivos primario.

1. En la pestaña **Objects (Objetos)**, seleccione el tipo de objeto (por ejemplo, **Objects [Objetos]** > **Addresses [Direcciones]**).
2. En **Device Group (Grupo de dispositivos)**, seleccione el grupo de dispositivos que tendrá la instancia de cancelación.
3. Seleccione el objeto y haga clic en **Override (Cancelar)**.
4. Edite los valores. No puede editar la configuración de **Name (Nombre)** o **Shared (Compartido)**.
5. Haga clic en **OK (Aceptar)**. La columna Nombre muestra un icono amarillo que se superpone al verde para que el objeto indique que se canceló.



Si es necesario, puede volver a los valores de objeto heredados *más tarde.*

STEP 6 | Guarde y compile los cambios.



Confirme con Panorama y envíe a grupos de dispositivos después de cualquier cambio en la jerarquía.

También debe enviar los cambios a las plantillas si una plantilla hace referencia a objetos de un grupo de dispositivos (por ejemplo, interfaces que hacen referencia a direcciones) y un cortafuegos asignado a la plantilla ya no está asignado a ese grupo de dispositivos debido a su cambio de jerarquía.

Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a la configuración de Panorama y a los grupos de dispositivos que añadió o cambió.

Creación de objetos para su uso en una política compartida o de grupo de dispositivos

Puede usar objetos en las reglas de cualquier política que estén en la ubicación compartida, en el mismo grupo de dispositivos o en grupos secundarios de dicho grupo; para obtener más información, consulte Objetos de grupos de dispositivos.

Los objetos de grupo de dispositivos compartidos se pueden ver y referenciar en un grupo de dispositivos específico. Cambiar el nombre de un objeto de grupo de dispositivos compartidos en un grupo de dispositivos cambia el nombre del objeto compartido en todos los grupos de dispositivos. Esto incluye cualquier configuración a la que se haga referencia en el objeto compartido, como en

 ©2023 Palo Alto Networks, Inc.

las reglas de política. Cambiar el nombre de un objeto de grupo de dispositivos compartidos puede hacer que falle la transferencia de configuración a los cortafuegos gestionados.

Por ejemplo, crea un objeto compartido llamado ObjectA y crea una regla de política de seguridad en el grupo de dispositivos DG1 donde se hace referencia a ObjectA. Esta configuración se envía a sus cortafuegos gestionados. Más tarde, en el grupo de dispositivos DG1, cambia el nombre de ObjectA a ObjectB e intenta enviar la configuración a sus cortafuegos gestionados. Este envío falla porque sus cortafuegos gestionados tienen el objeto compartido con el nombre ObjectA como parte de su configuración y esperan que ese objeto de configuración tenga el mismo nombre.



Consulte Uso de grupos de direcciones dinámicas en políticas *y verifique el número de direcciones IP registradas que admite Panorama si pretende aprovechar los grupos de direcciones dinámicas para crear políticas que se adapten de forma automática a los cambios en la red.*

- Cree un objeto compartido.

  En este ejemplo, añadimos un objeto compartido a categorías de filtrado de URL en las que queremos activar alertas.

  1. Seleccione la pestaña **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y haga clic en **Add (Añadir)**.

     La pestaña **Objects (Objetos)** solo aparece si ha añadido al menos un grupo según el procedimiento Adición de un grupo de dispositivos.
  2. Introduzca un **Name (Nombre)** y una **Description (Descripción)**.
  3. Seleccione **Sharded (Compartido)**.
  4. La opción **Disable Override (Deshabilitar cancelación)** está sin seleccionar de manera predeterminada, lo que significa que puede cancelar las instancias heredadas del objeto en todos los grupos de dispositivos. Para deshabilitar la cancelación para el objeto, seleccione la casilla de verificación.
  5. En la pestaña **Categories (Categorías)**, seleccione cada Categoría para la cual desea obtener la notificación.
  6. En la columna **Action (Acción)**, seleccione **Alert (Alerta)**.
  7. Haga clic en **OK (Aceptar)** para guardar los cambios al objeto.
  8. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

- Cree un objeto de grupo de dispositivos.

  En este ejemplo, añadimos un objeto de dirección para los servidores web específicos de su red.

  1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y **Device Group (Grupo de dispositivos)** en el que utilizará el objeto.
  2. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para identificar el objeto.
  3. Asegúrese de dejar la opción **Shared (Compartido)** sin seleccionar.
  4. La opción **Disable Override (Deshabilitar cancelación)** está sin seleccionar de manera predeterminada, lo que significa que puede cancelar las instancias heredadas del objeto en los grupos de dispositivos secundarios del **Device Group (Grupo de dispositivos)** seleccionado. Para deshabilitar las cancelaciones para el objeto, seleccione la opción **Disable Override (Deshabilitar cancelación)**.
  5. Seleccione el tipo de objeto de dirección en **Type (Tipo)** y el valor asociado. Por ejemplo, seleccione **IP Range (Rango de IP)** e introduzca el rango de dirección IP de los servidores web.
  6. Haga clic en **OK (Aceptar)** para guardar los cambios al objeto.
  7. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a la configuración de Panorama y al grupo de dispositivos donde añadió el objeto.

     Cuando activa una licencia de antivirus en un cortafuegos, se agrega automáticamente una lista de listas de IP predefinidas al cortafuegos. Como resultado, esto reduce la cantidad total de objetos de direcciones individuales, grupos dinámicos, listas de IP externas, listas de direcciones IP bloqueadas predefinidas y listas de IP predefinidas externas que puede insertar desde Panorama.

- Visualice los objetos compartidos y los objetos de grupo de dispositivos en Panorama.

  En las páginas de la pestaña **Objects (Objetos)**, la columna Ubicación indica si un objeto está compartido o especificado en un grupo de dispositivos.

  1. En la pestaña **Objects (Objetos)**, seleccione el tipo de objeto (**Objects [Objetos]** > **Addresses [Direcciones]**, en este ejemplo).
  2. Seleccione el **Device Group (Grupo de dispositivos)** al cual añadirá el objeto.

     *La pestaña **Objects (Objetos)** solo muestra objetos que están en el **Device Group (Grupo de dispositivos)** seleccionado o que se heredan de un grupo de dispositivos primario o la ubicación compartida.*
  3. Verifique que aparece el objeto del grupo de dispositivos. Observe que el nombre del grupo de dispositivos en la columna Ubicación coincida con la selección en el menú desplegable **Device Group (Grupo de dispositivos)**.

Volver a los valores de objeto heredados

Después de cancelar los valores que el objeto de un grupo de dispositivos hereda de un grupo de dispositivos primario, puede volver a los valores primarios del objeto en cualquier momento. En la

 ©2023 Palo Alto Networks, Inc.

pestaña **Objects (Objetos)**, los objetos cancelados tienen un icono amarillo que se superpone al verde ( ) en la columna Nombre.

Si desea enviar valores primarios en todos los objetos cancelados en lugar de volver a un objeto específico, consulte Gestión de la precedencia de objetos heredados.

Para obtener los pasos para cancelar valores, consulte el paso 5.

Para obtener detalles sobre las cancelaciones y herencias del objeto, consulte Objetos de grupos de dispositivos.

STEP 1 | En la pestaña **Objects (Objetos)**, seleccione el tipo de objeto (por ejemplo, **Objects [Objetos]** > **Addresses [Direcciones]**) y seleccione el **Device Group (Grupo de dispositivos)** que tiene una instancia cancelada del objeto.

STEP 2 | Seleccione el objeto, haga clic en **Revert (Revertir)** y haga clic en **Yes (Sí)**. La columna Nombre muestra un ícono verde para el objeto, lo que indica que ahora hereda todos los valores de un grupo de dispositivos primario.

STEP 3 | Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego seleccione **Commit and Push (Confirmar y enviar)** para enviar sus cambios a la configuración de Panorama y al grupo de dispositivos donde revirtió el objeto.

Gestión de objetos compartidos no utilizados

Cuando envía cambios en la configuración a Grupos de dispositivos, Panorama envía a los cortafuegos todos los objetos compartidos de manera predeterminada, con independencia de si las reglas de políticas compartidas o de los grupos de dispositivos hacen referencia a ellos. Sin embargo, puede configurar Panorama para que solo introduzca los objetos compartidos a los que las reglas hacen referencia en los grupos de dispositivos. La opción **Share Unused Address and Service Objects with Devices (Compartir objetos de servicio y direcciones no utilizadas con dispositivos)** le permite limitar los objetos que Panorama envía en los cortafuegos gestionados.

Si no marca ***Share Unused Address and Service Objects with Devices (Compartir direcciones y objetos de servicio no usados con dispositivos)****, Panorama pasa por alto los cortafuegos especificados en* ***Target (Destino)*** *cuando realiza el procedimiento* Ingreso de una regla de política a un subconjunto de cortafuegos*. Por lo tanto, se envían todos los objetos a los que se haga referencia en cualquier regla a todos los cortafuegos del grupo de dispositivos.*

Para limitar el número de objetos que se envía a un conjunto de cortafuegos gestionados, añada las reglas de las políticas a un grupo de dispositivos secundario y haga referencia a los objetos compartidos que sean precisos. Consulte Creación de una jerarquía del grupo de dispositivos *para obtener más información sobre cómo crear un grupo de dispositivos secundarios.*

En modelos de bajo nivel, como PA-220, considere introducir únicamente los objetos compartidos relevantes en los cortafuegos gestionados. Esto se debe a que el número de objetos que se puede

 ©2023 Palo Alto Networks, Inc.

almacenar en los modelos de bajo nivel es considerablemente inferior al de los modelos de media y alta gama. Asimismo, si tiene muchos objetos de direcciones y servicios no utilizados, al cancelar la selección de **Share Unused Address and Service Objects with Devices (Compartir objetos de servicio y direcciones no utilizadas con dispositivos)** se reducen considerablemente los tiempos de compilación en los cortafuegos debido a que la configuración introducida en cada cortafuegos es menor. Sin embargo, deshabilitar esta opción puede aumentar el tiempo de confirmación en Panorama porque Panorama debe verificar dinámicamente si las reglas de la política hacen referencia a un objeto en particular.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.

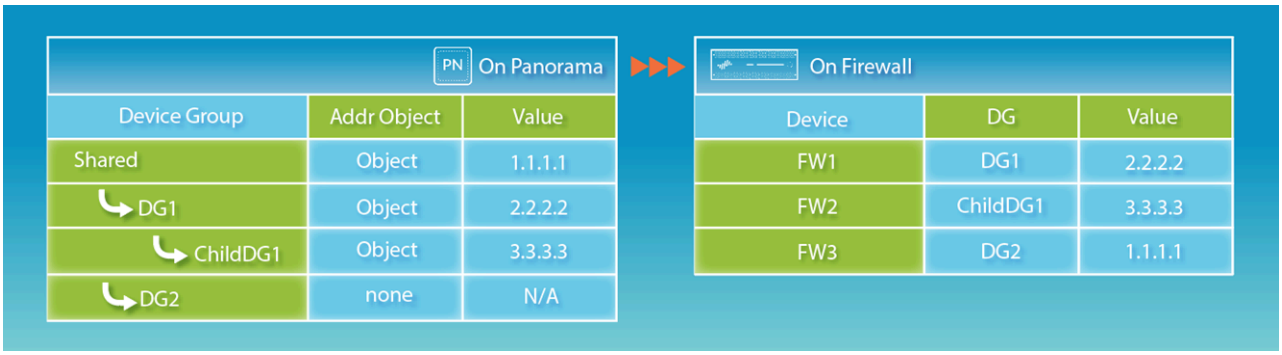
STEP 2 | Cancele la opción **Share Unused Address and Service Objects with Devices (Compartir objetos de servicio y direcciones no utilizadas con dispositivos)** para enviar solo los objetos compartidos a los que la regla hace referencia o seleccione la opción para volver a habilitar el envío de todos los objetos compartidos.

STEP 3 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

Gestión de la precedencia de objetos heredados

De manera predeterminada, cuando los grupos de dispositivos de diferentes niveles de la Jerarquía del grupo de dispositivos tienen un objeto con el mismo nombre pero valores distintos (por ejemplo, debido a sustituciones), las reglas de las políticas de los grupos de dispositivos secundarios usan los valores de ese objeto en dichos grupos, en lugar de utilizar los heredados de los grupos de dispositivos primarios. De manera opcional, puede revertir este orden de precedencia para enviar valores desde el grupo primario más alto que contenga el objeto a todos los grupos de dispositivos secundarios. Después de habilitar esta opción, la próxima vez que envíe cambios de configuración a grupos de dispositivos, los valores de los objetos heredados reemplazan los valores de cualquier objeto anulado en los grupos de dispositivos descendientes. En la figura siguiente se ilustra la precedencia de los objetos heredados de los grupos de dispositivos:



Si un cortafuegos tiene objetos definidos localmente con el mismo nombre que un objeto compartido u objeto de grupo de dispositivos que Panorama ingresa, se produce un fallo de compilación.

Si desea revertir un objeto sustituido concreto a sus valores primarios, en lugar de enviar estos a todos los objetos sustituidos, consulte Volver a los valores de objeto heredados.

©2023 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.

STEP 2 | Si desea invertir el orden predeterminado de precedencia, seleccione **Objects defined in ancestors will take higher precedence (Objetos definidos en ancestros tendrán mayor precedencia)**. El cuadro de diálogo muestra el enlace **Find Overridden Objects (Buscar objetos cancelados)**, que ofrece la opción de ver cuántos objetos cancelados (sombreados) tendrán valores primarios después de compilar este cambio. Puede pasar el puntero del ratón sobre el mensaje de cantidad para mostrar los nombres de los objetos.

Si desea invertir el orden predeterminado de precedencia, seleccione **Objects defined in ancestors will take higher precedence (Objetos definidos en ancestros tendrán mayor precedencia)**.

*La opción **Find Overridden Objects (Buscar objetos sustituidos)** solo detecta los objetos compartidos de grupos de dispositivos que tienen el mismo nombre que otro objeto del grupo en cuestión.*

STEP 3 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 5 | (Opcional) Si seleccionó **Objects defined in ancestors will take higher precedence (Objetos definidos en ancestros tendrán mayor precedencia)**, Panorama no envía los objetos del antecesor hasta que no haya enviado cambios de configuración a los grupos de dispositivos: seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a los dispositivos)** y seleccione **Push (Enviar)** para enviar sus cambios.

Movimiento o duplicación de una regla de política u objeto a un grupo de dispositivos diferente

En Panorama, si una regla de política u objeto que moverá o duplicará de un grupo de dispositivos tiene referencias a objetos que no están disponibles en el grupo de dispositivos de destino (**Destination (Destino)**), debe mover o duplicar los objetos a los que se hace referencia y la regla u objeto de referencia en la misma acción. En una jerarquía de grupo de dispositivos, recuerde que los objetos a los que se hace referencia podrían estar disponibles a través de la herencia. Por ejemplo, los objetos compartidos están disponibles en todos los dispositivos. Puede llevar a cabo una búsqueda global para verificar las referencias. Si mueve o duplica un objeto cancelado, asegúrese de que las cancelaciones estén habilitadas para ese objeto en el grupo de dispositivos primario de **Destination (Destino)** (consulte Creación de objetos para su uso en una política compartida o de grupo de dispositivos).

Cuando clona varias reglas de la política, el orden en el que selecciona las reglas determinará el orden en el que se copian al grupo de dispositivos. Por ejemplo, si tiene las reglas de 1 a 4 y su orden de selección es 2-1-4-3, el grupo de dispositivos donde se clonarán estas reglas mostrará las reglas en el mismo orden en el que las seleccionó. Sin embargo, puede reorganizar las reglas como lo desee cuando se copien correctamente.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en Panorama y seleccione la base de reglas (por ejemplo, **Policy [Política]** > **Security [Seguridad]** > **Pre Rules [Reglas previas]**) o tipo de objeto (por ejemplo, **Objects [Objetos]** > **Addresses [Direcciones]**).

STEP 2 | Seleccione el **Device Group (Grupo de dispositivos)** y una o más reglas u objetos.

STEP 3 | Seleccione uno de los siguientes pasos:

- (Solo en el caso de reglas) Haga clic en **Move (Mover)** > **Move to other device group (Mover a otro grupo de dispositivos)**
- (Solo en el caso de objetos) **Move (Mover)**
- (Reglas u objetos) **Clone (Duplicar)**

STEP 4 | En el menú desplegable **Destination (Destino)**, seleccione el grupo de dispositivos nuevo o **Shared (Compartido)**. La opción predeterminada es el **Device Group (Grupo de dispositivos)** seleccionado.

STEP 5 | (Solo en el caso de reglas) Seleccione **Rule order (Orden de reglas)**:

- **Move top**: la regla precederá al resto de las reglas.
- **Move bottom**: la regla seguirá a todas las demás reglas.
- **Before rule**: en el menú desplegable adyacente, seleccione la regla que viene después de las reglas seleccionadas.
- **After rule**: en el menú desplegable adyacente, seleccione la regla que viene antes de las reglas seleccionadas.

STEP 6 | La casilla de verificación **Error out on first detected error in validation (Error en el primer error detectado en la validación)** está seleccionada de manera predeterminada, lo que significa que Panorama mostrará el primer error que encuentra y detendrá la verificación de más errores. Por ejemplo, se produce un error si el grupo de dispositivos de **Destination (Destino)** no incluye un objeto al que se haga referencia en la regla que está moviendo. Cuando mueve o duplica varios elementos a la vez, seleccione esta casilla de verificación para poder simplificar la solución de problemas. Si cancela la selección de la casilla de verificación, Panorama buscará todos los errores antes de mostrarlos. Independientemente de esta configuración, Panorama no moverá ni duplicará ningún elemento hasta que solucione los errores de todos los elementos seleccionados.

STEP 7 | Haga clic en **OK** para iniciar la validación de errores. Si Panorama encuentra errores, corríjalos y vuelva a enviar el movimiento o duplicación. Si Panorama no encuentra errores, lleve a cabo la acción.

STEP 8 | Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**, **Edit Selections (Editar selecciones)** en Push Scope, seleccione **Device Groups (Grupos de dispositivos)**, seleccione los grupos de dispositivos originales y de destino, haga clic **OK (Aceptar)**, y entonces seleccione **Commit and Push (Confirmar y enviar)** sus cambios a la configuración de Panorama y a los grupos de dispositivos.

 ©2023 Palo Alto Networks, Inc.

Ingreso de una regla de política a un subconjunto de cortafuegos

Dirigir políticas le permite especificar los cortafuegos de un grupo de dispositivos en los que introducir las reglas de políticas. Le permite excluir uno o más cortafuegos o sistemas virtuales, o bien únicamente aplicar una regla a cortafuegos o sistemas virtuales específicos de un grupo de dispositivos.

A medida que se desarrolla la base de reglas y que envía reglas nuevas o modificadas a los cortafuegos, los cambios y la información de auditoría se van perdiendo, a menos que los archive en el momento en que se crean o modifican las reglas. En el archivo de observaciones de auditoría, puede ver los comentarios y el historial de logs de configuración relativos a la regla seleccionada, así como comparar dos versiones de ella para comprobar en qué ha cambiado. Si envía el archivo de observaciones de auditoría de una regla desde Panorama, solo puede consultarlo en el servidor de gestión de Panorama. Sin embargo, sí puede leer las observaciones de los logs de configuración enviados a Panorama desde los cortafuegos gestionados, aunque no puede ver el archivo correspondiente a las reglas creadas o modificadas en los cortafuegos de forma local. Para garantizar que las observaciones de auditoría se incluyan en el momento en que se crean o modifican las reglas, siga el procedimiento Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas.

La capacidad de dirigir una regla le permite mantener a las políticas centralizadas en Panorama. Si define reglas específicas como reglas previas o posteriores compartidas o para grupos de dispositivos en Panorama, mejora la visibilidad y la eficiencia a la hora de gestionarlas (consulte Políticas de grupo de dispositivos). El archivo de observaciones de auditoría aporta incluso más visibilidad, pues permite realizar el seguimiento de cómo y por qué han cambiado las reglas de las políticas a lo largo del tiempo. De ese modo, puede auditar la evolución de las reglas durante toda su vigencia.

STEP 1 | (Práctica recomendada) Exija que se introduzcan observaciones de auditoría en las reglas de las políticas.

Aunque este paso es opcional, se recomienda aplicarlo para que se motive siempre la creación o la modificación de las reglas y para que su historial tenga la precisión que exigen las auditorías.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite Policy Rulebase Settings (Configuración de base de reglas de políticas).
2. Marque la opción **Require audit comment on policies (Exigir observaciones de auditoría sobre políticas)**.
3. En Audit Comment Regular Expression (Expresión regular de observaciones de auditoría), especifique el formato de estas notas.

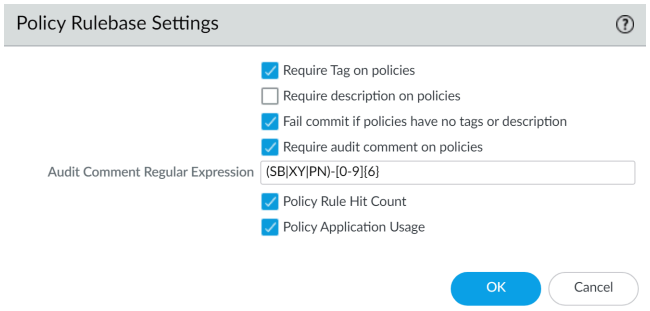
   Exija que, al crear o modificar reglas, las observaciones tengan un formato ajustado a sus requisitos empresariales y de auditoría. Para ello, especifique expresiones formadas por letras y números; por ejemplo, introduzca una expresión regular que coincida con el formato de sus números de tickets:

   - **`[0-9]{<Number of digits>}`**: exige que las observaciones de auditoría incluyan un número mínimo de cifras del 0 al 9. Por ejemplo, **`[0-9]{6}`** exige una expresión de seis cifras como mínimo con números del 0 al 9. Configure el número mínimo de cifras que estime oportuno.
   - **`<Expresión con letras>`**: exige que las observaciones de auditoría incluyan alguna expresión alfabética. Por ejemplo, **`Reason for Change- (Motivo del cambio:)`** exige que el administrador empiece las observaciones con estas palabras.

 ©2023 Palo Alto Networks, Inc.

- **<Expresión con letras>-[0-9]{<Number of digits>}**: exige que las observaciones de auditoría incluyan un prefijo alfabético fijo, con un número mínimo de cifras del 0 al 9. Por ejemplo, **SB-[0-9]{6}** exige que las observaciones empiecen con **SB-**, seguido de una expresión con seis cifras como mínimo del 0 al 9, como **SB-012345**.
- **(<Expresión de letras>)|(<Expresión de letras>)|(<Expresión de letras>)|-[0-9]{<Number of digits>}**: requiere que el comentario de auditoría contenga un prefijo que utilice uno de los conjuntos configurados de expresiones de letras con un número mínimo de dígitos que van de 0 a 9. Por ejemplo, **(SB|XY|PN)-[0-9]{6}** exige que las observaciones empiecen con **SB-**, **XY-**, o **PN-** seguido de una expresión con seis cifras como mínimo del 0 al 9, como **SB-012345**, **XY-654321**, o **PN-012543**.

4. Haga clic en **OK (Aceptar)** para aplicar la nueva configuración de la base de reglas de las políticas.



5. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 2 | Cree una regla.

En este ejemplo, se define una regla previa en la base de reglas de seguridad que permita a los usuarios de la red interna acceder a los servidores de DMZ.

1. En la pestaña **Policies (Políticas)**, seleccione en **Device Group (Grupo de dispositivos)** el grupo en el que desea definir un regla.
2. Seleccione la base de reglas. En este ejemplo, seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre-Rules (Reglas previas)** y haga clic en **Add (Añadir)** para añadir una regla.
3. En la pestaña **General**, introduzca un nombre descriptivo para la regla en **Name (Nombre)** y las notas pertinentes en **Audit Comment (Observaciones de auditoría)**.
4. En la pestaña **Source (Origen)**, en **Source Zone (Zona de origen)**, seleccione Trust (Fiable).
5. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** en **DMZ**.
6. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, establezca **Service (Servicio)** como **application-default (Valor predeterminado de aplicación)**.
7. En la pestaña **Actions (Acciones)**, defina **Action (Acción)** en **Allow (Permitir)**.
8. Deje los valores predeterminados en todas las demás opciones.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Dirija la regla para incluir o excluir un subconjunto de cortafuegos.

Para aplicar la regla a un conjunto seleccionado de cortafuegos, realice lo siguiente:

1. Seleccione la pestaña **Target (Destino)** del cuadro de diálogo Policy Rule (Regla de política).
2. Seleccione los cortafuegos a los que desea aplicar la regla.

   Si no selecciona los cortafuegos de destino, la regla se añade a todos los cortafuegos (sin marcar) del grupo de dispositivos.

   Aunque la casilla de verificación que corresponde a los sistemas virtuales del grupo de dispositivos no está marcada de forma predeterminada, todos ellos heredan la regla al confirmar la selección, a menos que seleccione algunos concretos a los que aplicar la regla.
3. (Opcional) Si no quiere que un subconjunto de cortafuegos herede la regla, marque **Install on all but specified devices (Instalar en todos los dispositivos menos los especificados)** y seleccione los cortafuegos que desea excluir.

   *Si marca **Install on all but specified devices (Instalar en todos los dispositivos menos los especificados)**, pero no selecciona ningún cortafuegos, no se añade la regla a ninguno de los cortafuegos del grupo de dispositivos.*
4. Haga clic en **OK (Aceptar)** para añadir la regla.

STEP 4 | Confirme y envíe los cambios de configuración:

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos donde añadió la regla y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** para enviar sus cambios a la configuración de Panorama y a los grupos de dispositivos.

STEP 5 | Solución de problemas de coincidencias del tráfico con las reglas de políticas para verificar que las reglas permiten y deniegan el tráfico tal como pretendía.

Envío de grupos de dispositivos a un cortafuegos de sistemas virtuales múltiples

Los cambios en la configuración de grupos de dispositivos introducidos manualmente o desde un envío de configuración programada de un grupo de dispositivos desde el servidor de gestión Panorama™ a un cortafuegos de sistemas virtuales múltiples se agrupan automáticamente en un solo trabajo. Cuando se ejecuta un envío desde Panorama a cortafuegos gestionados, Panorama inspecciona los cortafuegos gestionados asociados con el envío del grupo de dispositivos. Si Panorama detecta que los sistemas virtuales múltiples que pertenecen al mismo cortafuegos de sistemas virtuales múltiples están asociados con un envío del grupo de dispositivos, agrupa el trabajo de compilación para cada sistema virtual múltiple en un solo trabajo de compilación en el cortafuegos gestionado a fin de reducir el tiempo general de finalización del trabajo de compilación.

Si falla uno de los trabajos de compilación incluidos, se produce un error en todo el envío y debe volver a enviar todos los cambios de configuración del grupo de dispositivos desde Panorama. Además, si se incluyen varios cortafuegos de sistemas virtuales múltiples en un envío desde

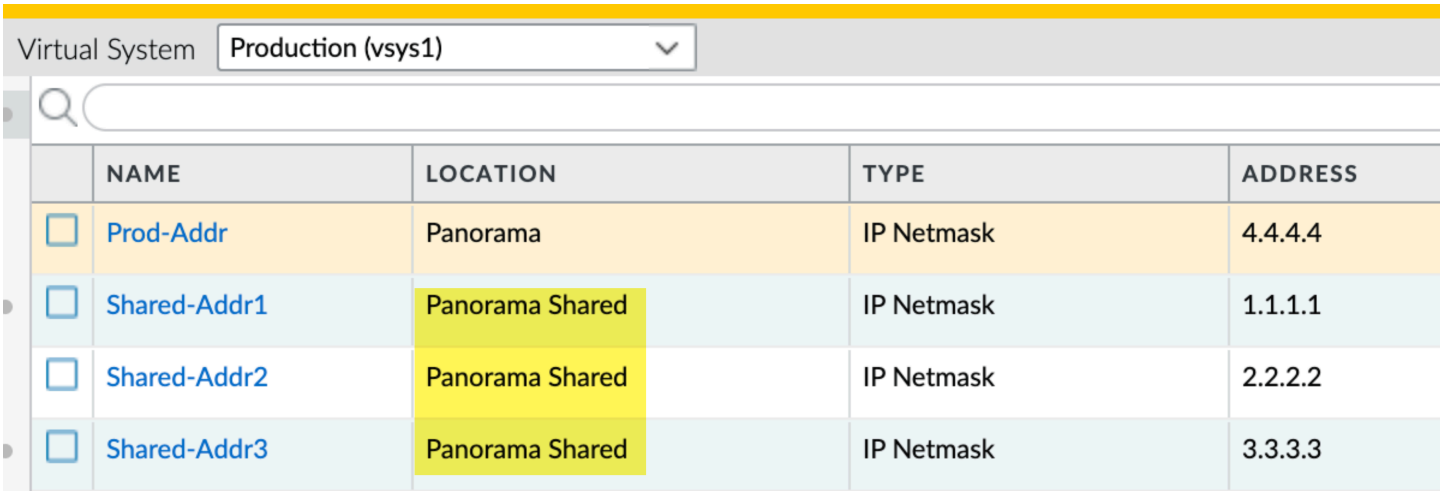
 ©2023 Palo Alto Networks, Inc.

Panorama y falla un envío, todo el envío falla en todos los cortafuegos incluidos en el envío desde Panorama. Cuando supervisa el envío del grupo de dispositivos localmente en el cortafuegos, se muestra un solo trabajo en lugar de varios trabajos individuales. Si se producen advertencias de errores, se muestra una descripción del error que indica los vsys afectados.

Esta funcionalidad es compatible con cortafuegos de sistemas virtuales múltiples gestionados por Panorama que ejecutan PAN-OS 10.2 y versiones posteriores de forma predeterminada.

Objetos compartidos enviados a un cortafuegos de sistemas virtuales múltiples

Para reducir la carga operativa de escalar configuraciones para cortafuegos de sistemas virtuales múltiples, los objetos de configuración compartida enviados a un cortafuegos de sistemas virtuales múltiples se envían a la ubicación compartida de Panorama en el cortafuegos de sistemas virtuales múltiples gestionado. La ubicación compartida de Panorama está disponible para todos los vsys del cortafuegos, lo que significa que los objetos compartidos no se replican en cada vsys.



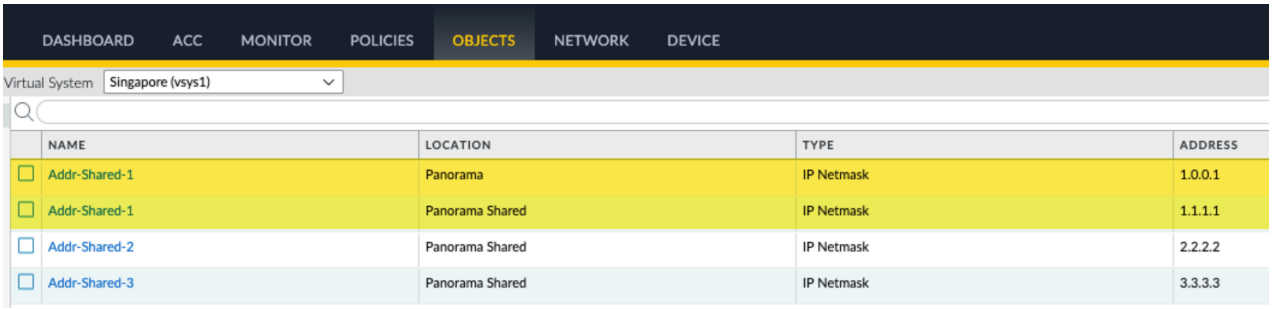
Las siguientes configuraciones no se pueden añadir a la ubicación compartida de Panorama y se replican en la ubicación de Panorama de cada vsys de un cortafuegos de sistemas virtuales múltiples.

- *Reglas previas y posteriores*
- *Listas dinámicas externas (EDL)*
- *Grupos de perfiles de seguridad*
- *Objetos y perfiles HIP*
- *Objetos de URL personalizados*
- *Perfiles de descifrado*
- *Perfiles de gestión de enlaces SD-WAN*

©2023 Palo Alto Networks, Inc.

Si un objeto compartido de Panorama se anula en un grupo de dispositivos, se crea un nuevo objeto con el mismo nombre pero con el valor anulado en la ubicación de Panorama de ese grupo de dispositivos y se envía a todos los vsys de un cortafuegos de sistemas virtuales múltiples. Si un objeto de configuración con el mismo nombre está presente en Panorama y en las ubicaciones compartidas de Panorama, la preferencia en la configuración otorgada al objeto en la ubicación de Panorama se debe a que es específico de ese vsys en el cortafuegos.

Por ejemplo, el vsys a continuación muestra el objeto de dirección `Addr-Shared-1` en Panorama y en las ubicaciones de Panorama. Si el objeto `Addr-Shared-1` se usa en una regla de política, se usa la dirección IP `1.0.0.1`.



Gestión de la jerarquía de reglas

El orden de las reglas de políticas es crítico para la seguridad de su red. Dentro de una capa de política (reglas compartidas, definidas localmente o de grupos de dispositivos) y la base de reglas (por ejemplo, reglas previas de seguridad compartidas), el cortafuegos evalúa las reglas desde la parte superior a la inferior en el orden en que aparecen en las páginas de la pestaña **Policies (Políticas)**. El cortafuegos compara un paquete con la primera regla que cumple con los criterios definidos e ignora las reglas siguientes. Por lo tanto, para aplicar la coincidencia más específica, mueva las reglas más específicas por encima de las reglas más genéricas.

Para comprender el orden en el que el cortafuegos evalúa las reglas por capa y por tipo (reglas previas, reglas posteriores y reglas predeterminadas) en toda la jerarquía del grupo de dispositivos*, consulte* Políticas del grupo de dispositivos*.*

STEP 1 | Visualice la jerarquía de reglas de cada base de reglas.

1. Seleccione la pestaña **Policies (Políticas)** y haga clic en **Preview Rules (Vista previa de reglas)**.
2. Filtre la vista previa por **Rulebase (Base de reglas)** (por ejemplo, **Security [Seguridad]** o **QoS**).
3. Filtre la vista previa para mostrar las reglas de un grupo de dispositivos específico en **Device Group (Grupo de dispositivos)** y las reglas que hereda de los grupos de dispositivos primarios y la ubicación compartida. Debe seleccionar un grupo de dispositivos que tenga cortafuegos asignados a él.
4. Filtre la vista previa por **Device (Dispositivo)** para mostrar sus reglas definidas localmente.
5. Haga clic en el icono de la flecha verde para aplicar sus selecciones de filtro a la vista previa (consulte Políticas del grupo de dispositivos).
6. Cierre el diálogo Vista previa de reglas combinada cuando finalice la previsualización de las reglas.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Elimine o desactive las reglas si es necesario.



*Para determinar las reglas que un cortafuegos actualmente no usa, seleccione ese cortafuegos en el menú desplegable **Context (Contexto)** en Panorama, seleccione la base de reglas (por ejemplo, **Policies [Políticas]** > **Security [Seguridad]**) y seleccione la casilla de verificación **Highlight Unused Rules (Destacar reglas no utilizadas)**. Un fondo punteado naranja indica las reglas que el cortafuegos no usa.*

1. Seleccione la base de reglas (por ejemplo, **Policies [Políticas]** > **Security [Seguridad]** > **Pre Rules [Reglas previas]**) que contiene la regla que eliminará o deshabilitará.
2. Seleccione el grupo de dispositivos que contiene la regla en **Device Group (Grupo de dispositivos)**.
3. Seleccione la regla y haga clic en **Delete (Borrar)** o **Disable (Deshabilitar)** según lo desee. Las reglas deshabilitadas aparecen en cursiva.

STEP 3 | Vuelva a establecer reglas dentro de una base de reglas, si es necesario.



*Para volver a establecer reglas locales en un cortafuegos, acceda a su interfaz web seleccionando ese cortafuegos en el menú desplegable **Context (Contexto)** antes de llevar a cabo este paso.*

1. Seleccione la base de reglas (por ejemplo,**Policies [Políticas]** > **Security [Seguridad]** > **Pre Rules [Reglas previas]**) que contiene la regla que va a mover.
2. Seleccione el grupo de dispositivos que contiene la regla en **Device Group (Grupo de dispositivos)**.
3. Seleccione la regla, **Move (Mover)** y luego seleccione lo siguiente:
   - **Move Top (Mover a la parte superior)**: mueve la regla arriba de todas las otras reglas del grupo de dispositivos (pero no arriba de las reglas heredadas de grupos de dispositivos primarios o compartidos).
   - **Move Up (Mover hacia arriba)**: mueve la regla arriba de la que le precede (pero no arriba de las reglas heredadas de grupos de dispositivos primarios o compartidos).
   - **Move Down (Mover hacia abajo)**: mueve la regla abajo de la que le sigue.
   - **Move Bottom (Mover a la parte inferior)**: mueve la regla abajo de todas las otras reglas.
   - **Move to other device group (Mover a otro grupo de dispositivos)**: consulte Movimiento o duplicación de una regla de política u objeto a un grupo de dispositivos diferente.

STEP 4 | Si modificó las reglas, confirme y envíe los cambios.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos que contiene las reglas que modificó o eliminó, y haga clic **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** para enviar sus cambios a la configuración de Panorama y a los grupos de dispositivos.

 ©2023 Palo Alto Networks, Inc.

Gestión de plantillas y pilas de plantillas

Use las plantillas y pilas de plantillas para definir las configuraciones básicas en común que permiten a los cortafuegos funcionar en la red. Consulte Plantillas y pilas de plantillas para obtener una descripción general de los problemas que debe considerar al decidir qué cortafuegos debe añadir a cada plantilla, ordenar plantillas en una pila para gestionar las capas de configuración en común y específica del grupo de cortafuegos, y cancelar la configuración de la plantilla con valores específicos del cortafuegos.

Para eliminar una plantilla, primero debe** deshabilitar o eliminar los ajustes de plantilla **de manera local en el cortafuegos. Solo los administradores con la función de superusuario pueden deshabilitar una plantilla.

- Funciones y excepciones de las plantillas
- Cómo añadir una plantilla
- Configuración de una pila de plantillas
- Configuración de una variable en una plantilla o una pila de plantillas
- Importación y sobrescritura de variables de la pila de plantillas existentes
- Cancelación de un ajuste de plantilla
- Deshabilitación/eliminación de ajustes de plantilla

Funciones y excepciones de las plantillas

Puede usar Plantillas y pilas de plantillas para definir una amplia variedad de ajustes, pero puede realizar las siguientes tareas en cada cortafuegos gestionado solo de manera local:

- Configurar una lista de bloqueos de dispositivos.
- Borrado de logs.
- Habilitar modos operativos como el modo normal, el modo de vsys múltiples o el modo FIPS-CC.
- Configurar las direcciones IP de cortafuegos en un par HA.
- Configuración de una clave maestra y un diagnóstico.
- Comparación de archivos de configuración (auditoría de configuraciones).

Para** gestionar licencias y actualizaciones **(software o contenido) para los cortafuegos, use las opciones de la pestaña **Panorama > Device Management (Gestión de dispositivos)**, no las plantillas.

- Volver a nombrar un vsys en un cortafuegos de vsys múltiples.

Cómo añadir una plantilla

Debe añadir, al menos, una plantilla antes de que Panorama™ muestre las pestañas **Device (Dispositivo)** y **Network (Red)** necesarias para definir la configuración de red y los elementos de configuración del dispositivo para los cortafuegos. Panorama admite hasta 1.024 plantillas. Cada cortafuegos gestionado debe pertenecer a una pila de plantillas. Si bien las plantillas contienen

©2023 Palo Alto Networks, Inc.

configuraciones de dispositivos gestionados, las pilas de plantillas le permiten gestionar y enviar configuraciones de plantillas a todos los cortafuegos gestionados asignados a la pila de plantillas.

Combine plantillas en una pila de plantillas para evitar duplicar configuraciones en las plantillas (consulte Plantillas y pilas de plantillas *y* Configuración de una pila de plantillas*).*

STEP 1 | Añada una plantilla.

1. Seleccione **Panorama** > **Templates (Plantillas)**.
2. Haga clic en **Add (Añadir)** e introduzca un nombre único en **Name (Nombre)** para identificar la plantilla.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. Haga clic en **OK (Aceptar)** para guardar la plantilla.
5. Si la plantilla tiene un sistema virtual (virtual system, vsys) con configuraciones (por ejemplo, interfaces) que desea que Panorama envíe a los cortafuegos que no tienen sistemas virtuales, seleccione la plantilla que creó, seleccione el vsys en el menú desplegable **Default VSYS (VSYS predeterminado)** y haga clic en **OK (Aceptar)**.
6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a la configuración de Panorama y a la plantilla.

STEP 2 | Verifique que la plantilla está disponible.

Después de añadir la primera plantilla, Panorama muestra las pestañas **Device (Dispositivo)** y **Network (Red)**. Estas pestañas muestran el menú desplegable **Template (Plantilla)**. Verifique que el menú desplegable muestre la plantilla que acaba de añadir.

STEP 3 | Realice la Configuración de una pila de plantillas y añada la plantilla a la pila de plantillas.

 ©2023 Palo Alto Networks, Inc.

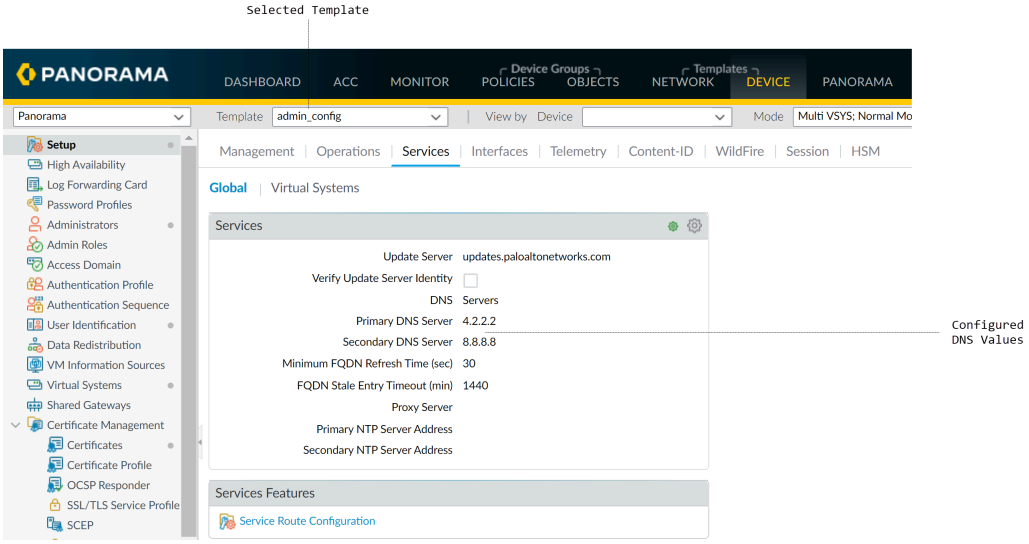
STEP 4 | Use la plantilla para enviar un cambio de configuración a los cortafuegos.

Solo se permite cambiar el nombre de un vsys en el cortafuegos local, no en Panorama. Como resultado, se obtiene un vsys completamente nuevo o el nuevo nombre del vsys se asigna al vsys incorrecto en el cortafuegos.

Por ejemplo, defina el servidor principal del sistema de nombres de dominios (Domain Name System, DNS) para los cortafuegos de la plantilla.

También puede realizar la Configuración de una variable en una plantilla o una pila de plantillas *para enviar valores específicos para el dispositivo a los dispositivos gestionados.*

1. En la pestaña **Device (Dispositivo)**, seleccione la **Template (Plantilla)** desde el menú desplegable.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global** y edite la sección Servicios.
3. Introduzca una dirección IP para el **Primary DNS Server (Servidor DNS principal)**.



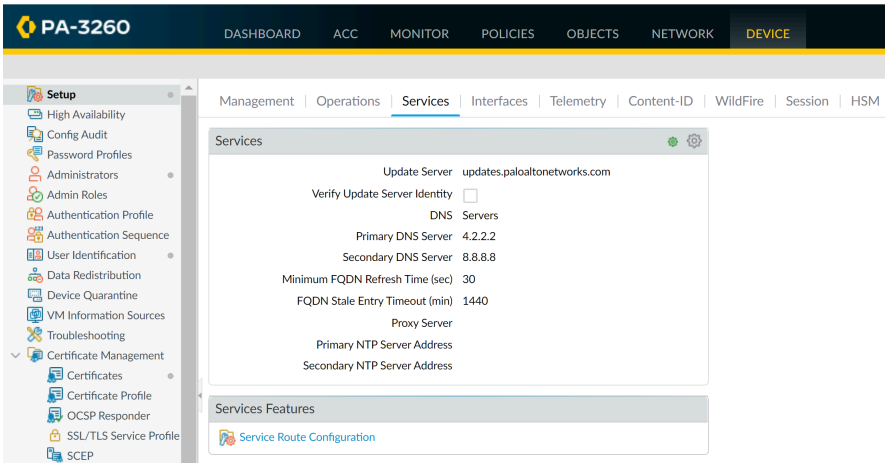
4. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a la configuración de Panorama y a la plantilla.

STEP 5 | Verifique que el cortafuegos esté configurado con los ajustes de plantilla que introdujo desde Panorama.

1. En el menú desplegable **Context (Contexto)**, seleccione uno de los cortafuegos en los que introdujo la configuración de la plantilla.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global (Global)**. Aparecerá la dirección IP que introdujo mediante la plantilla. El encabezado de la

 ©2023 Palo Alto Networks, Inc.

sección Services (Servicios) muestra el icono de plantilla ( ) para indicar que los ajustes de la sección tienen valores ingresados desde una plantilla.



STEP 6 | Solución de problemas de conectividad a recursos de red para verificar que los cortafuegos pueden acceder a los recursos de la red.

Configuración de una pila de plantillas

Las pilas de plantillas se pueden configurar y le permiten combinar varias plantillas para enviar configuraciones completas a sus cortafuegos gestionados. A pesar de que las plantillas son módulos de la configuración de su cortafuegos que puede volver a utilizar en diferentes pilas, también puede configurar la pila de plantillas para que complete los ajustes restantes que debe aplicar en todos los cortafuegos asignados a la pila. Panorama admite hasta 1024 pilas de plantillas y cada pila puede tener hasta 8 plantillas asignadas. Puede hacer referencia a objetos configurados en una pila de plantillas desde una plantilla que pertenezca a la pila de plantillas. La pila de plantillas hereda los objetos de configuración de las plantillas que añade y se basa en cómo ordena las plantillas en la pila de plantillas. También puede anular la configuración de la plantilla en la pila de plantillas para crear un objeto de configuración de la pila de plantillas. Para obtener detalles y la planificación, consulte Plantillas y pilas de plantillas.

Añada una plantilla ***para configurar interfaces, redes de área local virtuales (Virtual Local Area Network, VLAN), cables virtuales, túneles IPSec, proxy DNS y sistemas virtuales. Estos objetos deben configurarse y enviarse desde una plantilla, y no desde una pila de plantillas. Después de enviarlos desde una plantilla, puede cancelar estos objetos, excepto los sistemas virtuales en la pila de plantillas.***

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Planifique las plantillas y su orden en la pila.

Añada una planilla que desee asignar a una pila de plantillas.

Cuando planifica el orden de prioridad de las plantillas dentro de una pila (para la configuración con elementos en común), debe comprobar el orden para evitar una configuración incorrecta. Por ejemplo, considere una pila en la que la interfaz Ethernet1/1 es del tipo Capa 3 en Plantilla_A pero del tipo Capa 2 con una VLAN en Plantilla_B. Si Plantilla_A tiene una mayor prioridad, Panorama enviará Ethernet1/1 como tipo Capa 3 pero asignada a una VLAN.

Además, observe que una configuración de plantilla no puede hacer referencia a una configuración en otra plantilla, incluso aunque ambas plantillas estén en la misma pila. Por ejemplo, una configuración de zona en la Plantilla_A no puede hacer referencia a un perfil de protección de zona en la Plantilla_B.

STEP 2 | Cree una pila de plantillas.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.

   *Panorama solo admite **Add Stack (Añadir pila)** para crear una nueva pila de plantillas. No se puede clonar una pila de plantillas existente.*

2. Introduzca un nombre único en **Name (Nombre)** para identificar la pila.
3. (Opcional) Añada una **descripción** para la pila de plantillas.
4. (Opcional) Marque (habilite) **Automatically push content when software device registers to Panorama** (Enviar contenido automáticamente cuando el dispositivo de software se registre en Panorama).

   Esta configuración solo es compatible con los cortafuegos VM-Series y CN-Series. Debe añadir la **dirección IP pública** de Panorama a la interfaz de gestión (**Panorama** > **Setup** > **Interfaces** > **Management**) para enviar automáticamente las versiones de contenido de antivirus y aplicaciones y amenazas a los cortafuegos VM-Series y CN-Series.

   Los cortafuegos VM-series implementados en NSX y los cortafuegos de hardware no son compatibles.

   Habilite esta configuración para enviar automáticamente las versiones de contenido de antivirus y aplicaciones y amenazas instaladas en Panorama a los cortafuegos VM-Series y CN-Series en la primera conexión a Panorama. Panorama intenta enviar las versiones de contenido dinámico instaladas una vez y no intenta ningún envío posterior de las versiones de contenido de antivirus y aplicaciones y amenazas instaladas si el envío inicial falla por cualquier motivo.

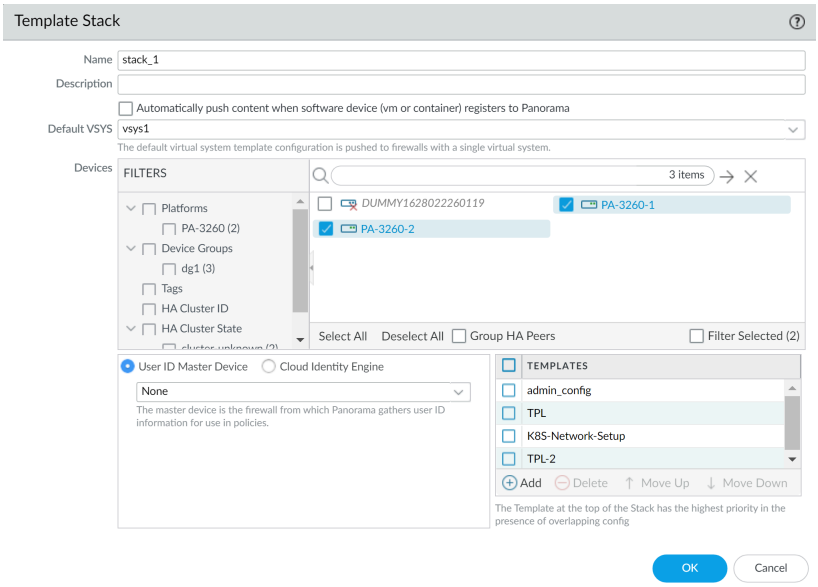
   Por ejemplo, añada un cortafuegos VM-Series a la gestión de Panorama y habilite **Auto Push on 1st Connect** (Envío automático en la primera conexión) para enviar automáticamente el grupo de dispositivos y la configuración de la pila de plantillas al cortafuegos VM-Series en la primera conexión. Sin embargo, la pila de plantillas contiene una configuración no válida y se produce un error en la inserción al cortafuegos VM-Series. En este escenario, el envío automático de contenido en el cortafuegos VM-Series también

 ©2023 Palo Alto Networks, Inc.

falla porque el envío de configuración y el envío de versiones de contenido dinámico se incluyen en la misma operación de envío al cortafuegos VM-Series.

Al aprovechar la escala automática, habilitar esta configuración le permite mantener las imágenes existentes para los cortafuegos VM-Series y CN-Series aprovechando el contenido dinámico en sus configuraciones, como en directivas y AppID. Esto ayuda a eliminar la sobrecarga operativa necesaria para actualizar las imágenes de cortafuegos de VM-Series y CN-Series cuando se introducen nuevas versiones de actualización de contenido dinámico.

5. Para cada una de las plantillas que la pila combinará (hasta 8), haga clic en **Add (Añadir)** y seleccione la plantilla. El cuadro de diálogo detalla las plantillas añadidas en orden de prioridad con respecto a la configuración duplicada, donde los valores en las plantillas más altas cancelan los que están más abajo de la lista. Para cambiar el orden, seleccione una plantilla y seleccione **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**.



6. En la sección Devices (Dispositivos), seleccione los cortafuegos para asignarlos a la pila. En el caso de los cortafuegos con varios sistemas virtuales, no puede asignar sistemas virtuales individuales, solo el cortafuegos completo. Puede asignar cada cortafuegos a solo una pila de plantillas.

Siempre que añada un nuevo cortafuegos gestionado a Panorama, debe asignarlo a la pila de plantillas adecuada; Panorama no asigna automáticamente nuevos cortafuegos a una plantilla o una pila de plantillas. Cuando realiza cambios de configuración en una plantilla, Panorama envía la configuración a cada cortafuegos asignado a la pila de plantillas.

7. (Opcional) Seleccione **Group HA Peers (Peers de HA del grupo)** para mostrar una casilla de verificación única para los cortafuegos que están en la configuración de alta disponibilidad (HA). Los iconos indican el estado de HA: verde para activo y amarillo para pasivo. El nombre del cortafuegos del peer secundario se encuentra entre paréntesis.

   Para HA activa/pasiva, añada ambos peers a la misma plantilla de modo que ambos reciban las configuraciones. Para HA activa/activa, si debe añadir ambos peers a la misma plantilla o no, depende de si cada peer requiere la misma configuración. Para obtener una lista de las

 ©2023 Palo Alto Networks, Inc.

configuraciones que PAN-OS sincroniza entre los peers de HA, consulte Sincronización de alta disponibilidad.

8. Haga clic en **OK (Aceptar)** para guardar la pila de plantillas.

STEP 3 | (Opcional) Configuración de una variable en una plantilla o una pila de plantillas.

STEP 4 | Edite la configuración de **Network (Red)** y **Device (Dispositivo)**, si es necesario.

> ***El cambio del nombre de un vsys está permitido solo en el cortafuegos local. Si cambia el nombre de un vsys en Panorama, creará un vsys completamente nuevo o el nombre del nuevo vsys se asignará al vsys incorrecto en el cortafuegos.***

En un contexto de cortafuegos individual, puede cancelar la configuración que Panorama envía desde una pila de la misma forma que cancela la configuración enviada desde una plantilla: consulte Cancelación de un valor de plantilla o pila de plantillas.

1. Filtre las pestañas para mostrar solo la configuración específica del modo que desea editar:

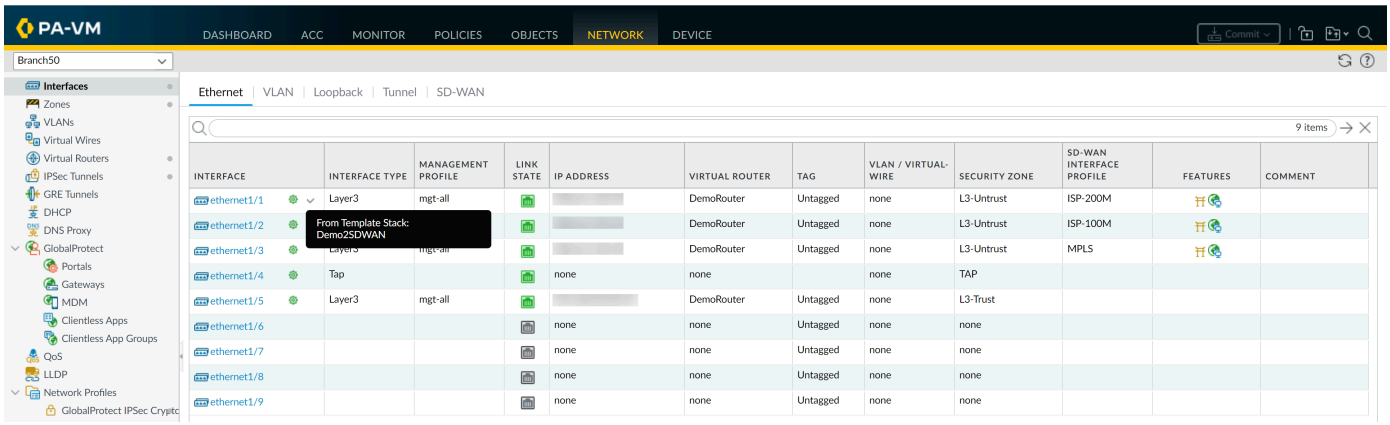
   > ***Si bien Panorama ingresa la configuración específica del modo solo a los cortafuegos que admiten estos modos, este ingreso selectivo no ajusta los valores específicos del modo. Por ejemplo, si una plantilla tiene cortafuegos en el modo Estándares Federales de Procesamiento de la Información (Federal Information Processing Standards, FIPS) y un perfil IKE Crypto que usa algoritmos que no pertenecen a FIPS, el envío de plantillas fallará. Para evitar estos errores, use el menú desplegable **Mode (Modo)** en las pestañas **Network (Red)** y **Device (Dispositivo)** para filtrar las opciones de valor y las funciones específicas del modo.***

   - En el menú desplegable **Mode (Modo)**, seleccione o cancele las opciones de filtro **Multi VSYS (VSYS múltiple)**, **Operational Mode (Modo operativo)** y **VPN Mode (Modo VPN)**.
   - Configure todas las opciones de **Mode (Modo)** para reflejar la configuración del modo de un cortafuegos determinado seleccionándolo en el menú desplegable **Device (Dispositivo)**.
2. Configure sus interfaces y conectividad de red. Por ejemplo, configure las zonas y las interfaces para segmentar su red a fin de gestionar y controlar el tráfico que pasa por su cortafuegos.
3. Edite la configuración según sea necesario.
4. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**, haga clic en **Edit Selections (Editar selecciones)** en Push Scope, seleccione **Templates (Plantillas)** y los cortafuegos asignados a la pila de plantillas, y luego haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a la configuración de Panorama y a la pila de plantillas.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Verifique que la pila de plantillas funciona como se esperaba.

1. Seleccione un dispositivo asignado a la pila de plantillas en la lista desplegable **Context (Contexto)**.
2. Seleccione una pestaña a la que envío cambios de configuración utilizando la pila de plantillas.
3. Los valores que se envían desde la pila de plantillas muestran el icono de plantilla ( ) para indicar que la configuración de la sección tiene valores ingresados desde una pila de plantillas. Pase el ratón sobre la pila para ver la pila de plantillas desde donde se envió el valor.



STEP 6 | Solución de problemas de conectividad a recursos de red para verificar que los cortafuegos pueden acceder a los recursos de la red.

Configuración de una variable en una plantilla o una pila de plantillas

Para volver a utilizar plantillas y pilas de plantillas con mayor facilidad, implemente variables de plantilla y pila de plantillas a fin de sustituir direcciones IP, IP de grupo e interfaces en sus configuraciones. Las variables de plantilla se definen en el nivel de la plantilla o la pila de plantillas, y puede utilizar variables para sustituir direcciones IP, rangos IP, FQDN, interfaces en IKE, VPN, configuraciones de HA e ID de grupo. Si varias plantillas de la pila de plantillas utilizan variables diferentes para el mismo objeto de configuración, el valor de variable heredado por la pila de plantillas se basa en el orden de herencia descrito en Plantillas y pilas de plantillas. Además, puede invalidar un valor de plantilla con una variable de pila de plantilla para administrar un objeto de configuración de la pila de plantillas.

Las variables le permiten reducir el número total de plantillas y pilas de plantillas que debe gestionar, además de permitirle conservar los valores específicos para un cortafuegos o dispositivo. Por ejemplo, si cuenta con una pila de plantillas con una configuración base, puede utilizar variables para crear valores que no se aplican a todos los cortafuegos en la plantilla o la pila de plantillas. Esto le permite gestionar y enviar configuraciones de menos plantillas o pilas de plantillas mientras considera valores específicos de un cortafuegos o dispositivo que, de lo contrario, necesitaría antes de poder crear una nueva plantilla o pila de plantillas.

Para crear una variable de plantilla o pila de plantillas:

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Cree una plantilla y una pila de plantillas.

1. Cómo añadir una plantilla
2. Lleve a cabo la Configuración de una pila de plantillas.

STEP 3 | Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Manage (Gestionar)** (columna Variables) para gestionar la plantilla o la pila de plantillas en la que desea crear una variable.

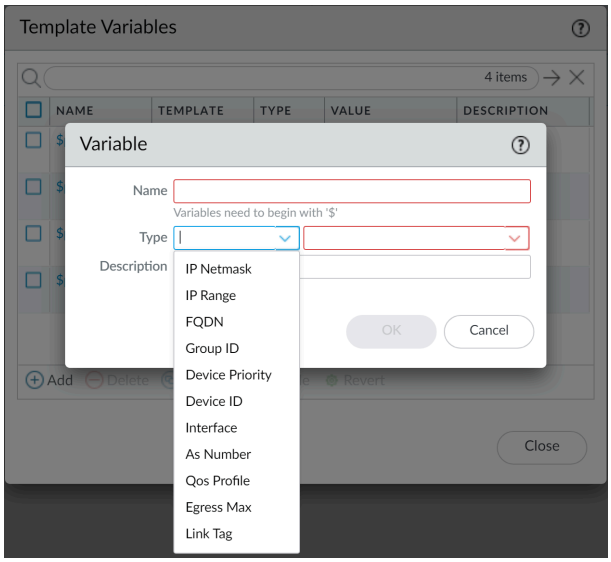
STEP 4 | Haga clic en **Add (Añadir)** para añadir la variable nueva.

Los nombres de variables deben comenzar con el símbolo de dólar ($).

1. Asigne un nombre a la variable nueva. En este ejemplo, las variables se denominan `$DNS-primary` y `$DNS-secondary`.
2. Seleccione la variable **Type (Tipo)** y especifique el valor correspondiente para el tipo de variable seleccionado.

   Para este ejemplo, seleccione **IP Netmask (Máscara de red IP)**.
3. (Opcional) Introduzca una descripción para la variable.
4. Haga clic en **OK (Aceptar)** y en **Close (Cerrar)**

Las variables también se pueden crear en línea cuando se admitan variables.



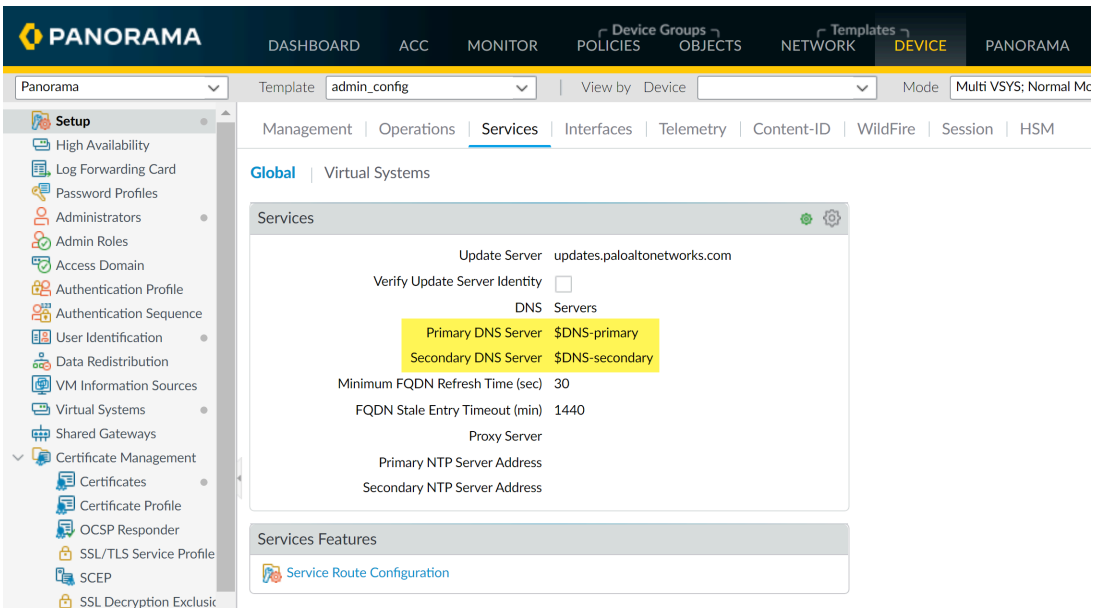
STEP 5 | En el menú desplegable **Template (Plantilla)**, seleccione la plantilla o la pila de plantillas a la que pertenece la variable.

©2023 Palo Alto Networks, Inc.

STEP 6 | Introduzca la variable en la ubicación adecuada.

En este ejemplo, mencione el valor DNS definido previamente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y edite la sección Services (Servicios).
2. Introduzca **`$DNS-primary`** o seleccione esta opción del menú desplegable de **Primary DNS Server (Servidor DNS principal)**.
3. Introduzca **$DNS-secondary** o seleccione esta opción del menú desplegable de **Secondary DNS Server (Servidor DNS secundario)**.
4. Haga clic en **OK (Aceptar)**.



STEP 7 | Haga clic en **Commit (Confirmar)** y en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a los cortafuegos gestionados.

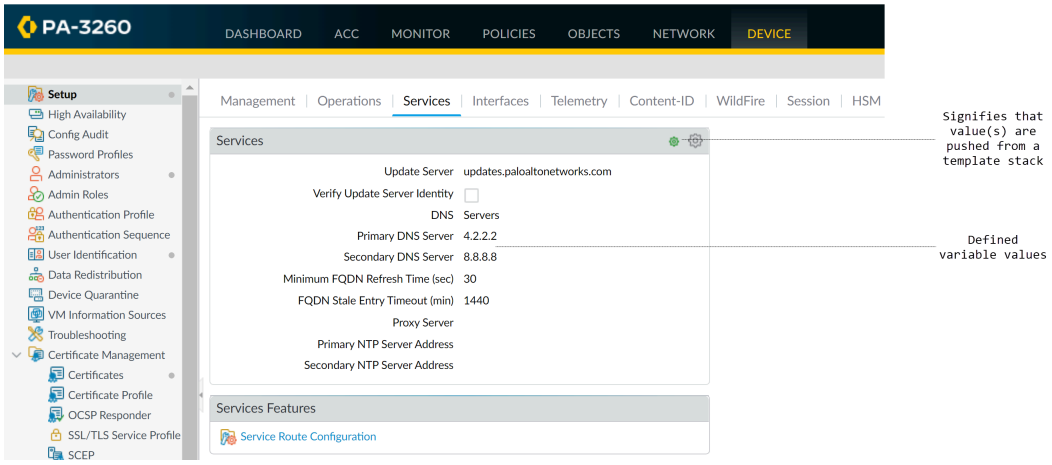
*Si envía configuraciones de grupos de dispositivos con referencias a variables de plantillas o pilas de plantillas, debe hacer clic en **Edit Selections (Editar selección)** y marcar **Include Device and Network Templates (Incluir plantillas de dispositivos y red).***

STEP 8 | Verifique que los valores de todas las variables se envíen a los dispositivos gestionados.

1. En el menú desplegable **Context (Contexto)**, seleccione un cortafuegos que pertenezca a la pila de plantillas para la que se creó la variable.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
3. Las configuraciones con valores definidos por una plantilla o una pila de plantillas se indican con un símbolo de plantilla ( ). Pase el puntero del ratón sobre el indicador para ver a cuál plantilla o pila de plantillas pertenece la definición de la variable. Cuando vea el contexto

 ©2023 Palo Alto Networks, Inc.

del cortafuegos, las variables se mostrarán como la dirección IP que configuró para la variable.



STEP 9 | Solución de problemas de conectividad a recursos de red para verificar que los cortafuegos pueden acceder a los recursos de la red.

Importación y sobrescritura de variables de la pila de plantillas existentes

Utilice variables de pila de plantillas para reemplazar direcciones IP, intervalos de IP, FQDN, interfaces o ID de grupo en las configuraciones de cortafuegos. Las variables le permiten reducir el número total de plantillas y pilas de plantillas que debe gestionar, además de permitirle conservar los valores específicos para un cortafuegos.

Importar las variables en la pila de plantillas le permite sobrescribir los valores de varias variables existentes y no puede crear nuevas variables en la pila de plantillas durante la importación. Para obtener más información sobre cómo crear una nueva variable de plantillas o pila de plantillas, consulte Configuración de una variable en una plantilla o una pila de plantillas.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Exporte las variables existentes en la pila de plantillas.

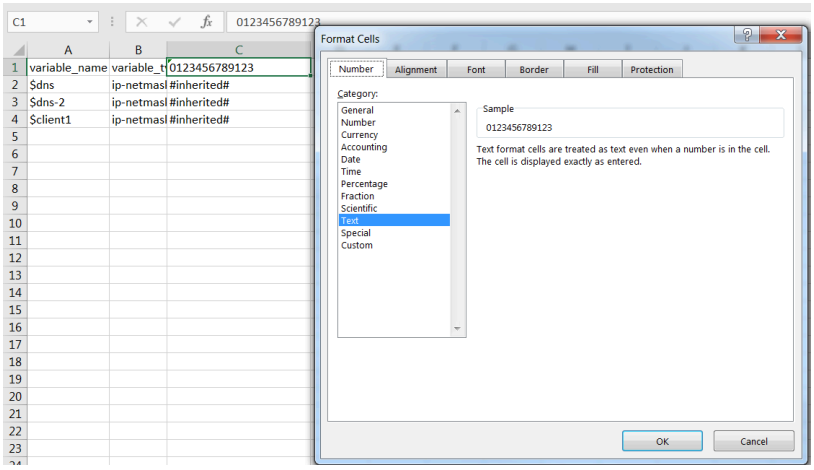
1. Seleccione **Panorama** > **Templates (Plantillas)** y elija una plantilla o pila de plantillas.
2. Seleccione **Variable CSV (CSV variable)** > **Export (Exportar)**. Las variables de pila de plantillas configuradas se descargan localmente como un archivo CSV.
3. Abra el CSV exportado.

©2023 Palo Alto Networks, Inc.

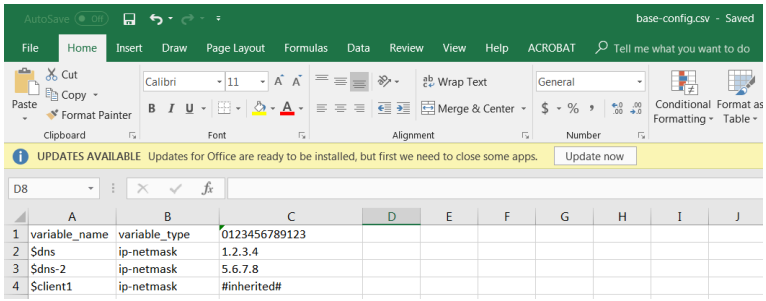
STEP 3 | Edite el archivo CSV con las variables en la pila de plantillas que se importarán en Panorama con el siguiente formato:

Los valores que se muestran como **`#inherited#`** son valores que se definen en la pila de plantillas.

1. Corrija el número de las celdas con el número de serie del cortafuegos. Repita este paso para todos los cortafuegos en el archivo CSV.
   1. Haga clic derecho en la celda con el número de serie del cortafuegos y seleccione **Format Cells (Formato de celdas)**.
   2. Seleccione **Number (Número)** > **Text (Texto)** y haga clic en **OK (Aceptar)**.
   3. Añada un **`0`** al principio del número de serie.



2. Introduzca un nuevo valor para la variable de plantillas deseada.
3. Seleccione **File (Archivo)** > **Save As (Guardar como)** y guarde el archivo en formato **CSV UTF-8**.



	A	B	C
1	variable_name	variable_type	0123456789123
2	$dns	ip-netmask	1.2.3.4
3	$dns-2	ip-netmask	5.6.7.8
4	$client1	ip-netmask	#inherited#

STEP 4 | Importe el archivo CSV a la pila de plantillas.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Templates (Plantillas)** y elija la pila de plantillas para la que ha exportado las variables en el paso 2.
3. Seleccione **Variable CSV (CSV variable)** > **Import (Importar)** y **busque** el archivo CSV editado en el paso 3.
4. Haga clic en **OK (Aceptar)** para importar las variables en la pila de plantillas.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 6 | Introduzca las variables en las ubicaciones adecuadas.

STEP 7 | Haga clic en **Commit (Confirmar)** y en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a los cortafuegos gestionados.

*Si envía configuraciones de grupos de dispositivos con referencias a variables de plantillas o pilas de plantillas, debe hacer clic en **Edit Selections (Editar selección)** y marcar **Include Device and Network Templates (Incluir plantillas de dispositivos y red)**.*

Cancelación de un valor de plantilla o pila de plantillas

Si bien las plantillas y pilas de plantillas le permiten aplicar una configuración básica en varios cortafuegos, puede que desee configurar ajustes específicos del cortafuegos que no se apliquen a todos los cortafuegos de una plantilla o pila de plantillas. En cambio, es posible que desee cancelar los ajustes de plantilla para crear una configuración de pila de plantillas que pueda aplicar como una configuración de base en todos sus cortafuegos gestionados. Las cancelaciones permiten excepciones o modificaciones para satisfacer sus necesidades de configuración. Por ejemplo, si utilizó una plantilla para crear una configuración de base, pero algunos cortafuegos en un entorno de pruebas necesitan ajustes diferentes para la dirección IP del servidor del sistema de nombres de dominios (Domain Name System, DNS) o el servidor del protocolo de tiempo de redes (Network Time Protocol, NTP), puede cancelar los ajustes de plantilla y pila de plantillas.

Si desea deshabilitar o quitar todos los ajustes de plantilla o pila de plantillas en un cortafuegos en lugar de cancelar un solo valor, consulte Deshabilitación/eliminación de ajustes de plantillas.

Puede cancelar un valor de una plantilla o una pila de plantillas de las siguientes maneras:

- Cancelación de un valor de plantilla en el cortafuegos o Cancelación de un valor de plantilla o pila de plantillas utilizando variables: existen dos maneras de cancelar valores enviados desde una plantilla o pila de plantillas. La primera manera es definir un valor local en el cortafuegos para cancelar un valor enviado desde una plantilla o pila de plantillas. La segunda manera es definir variables específicas para el cortafuegos con el fin de cancelar los valores enviados desde una plantilla o pila de plantillas.
- Cancelación de un valor de plantilla utilizando una pila de plantillas: defina los valores o las variables en la pila de plantillas para cancelar los valores enviados desde una plantilla.

Cancelación de un valor de plantilla en el cortafuegos

Cancele una configuración en el cortafuegos local que se ingresó desde una plantilla o una pila de plantillas para crear configuraciones específicas para el cortafuegos. Esto le permite gestionar la configuración de la plantilla o la pila de plantillas básicas desde Panorama™, y conservar todas las configuraciones específicas para el cortafuegos que no aplican a otros cortafuegos.

STEP 1 | Acceda a la interfaz web del cortafuegos.

Acceda directamente al cortafuegos introduciendo su dirección IP en el campo de URL de su navegador, o use el menú desplegable **Context (Contexto)** en Panorama para cambiar al contexto de cortafuegos.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Cancele un valor que ingresó desde una plantilla o una pila de plantillas.

En este ejemplo, cancelará la dirección IP del servidor DNS que asignó mediante una plantilla en Cómo añadir una plantilla.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y edite la sección Services (Servicios).
2. Haga clic en el icono de plantilla ( ) del **Primary DNS Server (Servidor DNS principal)** para habilitar la cancelación para ese campo.
3. Introduzca una nueva dirección IP para el **Primary DNS Server (Servidor DNS principal)**. Un símbolo de cancelación de plantilla ( ) indica que el valor de la plantilla se canceló.
4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

Cancelación de un valor de plantilla utilizando una pila de plantillas

Puede usar valores de una pila de plantillas para cancelar las configuraciones enviadas al cortafuegos gestionado desde una plantilla con el fin de crear una configuración de pila de plantillas que pueda utilizar para gestionar la configuración de base en sus cortafuegos gestionados desde Panorama™. Esto le permite aprovechar las capacidades de gestión de Panorama para enviar los cambios de configuración a varios dispositivos desde una sola ubicación. En este ejemplo, utilizará una pila de plantillas para cancelar la variable de la dirección IP del servidor DNS principal denominada `$DNS` que se envió desde una plantilla.

Panorama admite el uso de una pila de plantillas para anular las interfaces configuradas en una plantilla, excepto las subinterfaces de capa 2 de una interfaz agregada*.*

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | En el menú desplegable **Template (Plantilla)**, seleccione la pila de plantillas que cancelará la configuración de plantilla.

STEP 3 | Cancele la configuración de plantilla enviada.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y edite la sección Services (Servicios).
2. Configure el **Primary DNS (DNS principal)** con la dirección IP para cancelar la configuración de plantilla enviada y haga clic en **OK (Aceptar)**.

STEP 4 | Haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar los cambios de configuración.

Cancelación de un valor de plantilla utilizando una pila de plantillas

Puede utilizar valores y variables de una pila de plantillas para cancelar las configuraciones enviadas al cortafuegos gestionado desde una plantilla con el fin de crear una configuración de pila de plantillas que pueda utilizar para gestionar la configuración de base en sus cortafuegos gestionados desde Panorama™. Esto le permite aprovechar las capacidades de gestión de Panorama para enviar los cambios de configuración a varios cortafuegos desde una sola ubicación. En este ejemplo, creará una variable de pila de plantillas cancelando la variable de la dirección IP del servidor DNS principal denominada `$DNS` que se envió desde una plantilla.

 ©2023 Palo Alto Networks, Inc.

Panorama admite el uso de una pila de plantillas para anular las interfaces configuradas en una plantilla, excepto las subinterfaces de capa 2 de una interfaz agregada*.*

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Cancele la variable de la plantilla.

1. Seleccione **Panorama** > **Templates (Plantillas)**.
2. Haga clic en **Manage (Gestionar)** (columna Variables) para gestionar la pila de plantillas que contiene la variable de plantilla que debe cancelar.
3. Ubique y seleccione la variable **$DNS**.
4. Seleccione **Override (Cancelar)**.
5. Introduzca el nuevo valor de variable y haga clic en **OK (Aceptar)**.

STEP 3 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

Cancelación de un valor de plantilla o pila de plantillas utilizando variables

Puede utilizar variables específicas para un cortafuegos para cancelar las variables que se enviaron al cortafuegos gestionado desde una plantilla o una pila de plantillas para crear configuraciones específicas para un cortafuegos. Esto le permite gestionar la configuración de la plantilla o la pila de plantillas básicas, y conservar todas las configuraciones específicas para el cortafuegos que no aplican a otros cortafuegos, todas desde Panorama™. Esto le permite aprovechar las capacidades de gestión de Panorama y tener en cuenta las configuraciones específicas necesarias para los cortafuegos individuales. En este ejemplo, la variable de la dirección IP del servidor DNS principal denominada `$DNS` que se envió desde una plantilla se cancelará para crear una variable específica para un cortafuegos.

Puede cancelar las variables de plantilla o pila de plantillas que no se cancelaron. Si una variable de plantilla o pila de plantillas ya se canceló, haga clic en ***Revert (Revertir)*** *para revertir la cancelación y crear una variable específica para un cortafuegos.*

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Cancele la variable de plantilla o pila de plantillas.

1. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
2. Haga clic en **Edit (Editar)** (columna Variables) para editar el cortafuegos que contiene la variable que debe cancelar.
3. Ubique y seleccione la variable **$DNS**.
4. Seleccione **Override (Cancelar)**.
5. Introduzca la dirección IP específica para el nuevo cortafuegos y haga clic en **OK (Aceptar)**.

STEP 3 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

Deshabilitación/eliminación de ajustes de plantilla

Si desea dejar de utilizar una plantilla o pila de plantillas para gestionar la configuración de un cortafuegos gestionado, puede deshabilitar la plantilla o pila. Cuando la deshabilite, puede copiar los valores de la plantilla o pila a la configuración local del cortafuegos o eliminar los valores.

Si desea cancelar una única configuración en lugar de deshabilitar o eliminar toda la configuración de la plantilla o pila, consulte Cancelación de un ajuste de plantilla**.**

Consulte Plantillas y pilas de plantillas *para obtener información detallada sobre cómo usar estas para gestionar cortafuegos.*

STEP 1 | Acceda a la interfaz web del cortafuegos gestionado como administrador con la función de superusuario. Puede acceder al cortafuegos directamente introduciendo su dirección IP en el campo URL del navegador; o bien, en Panorama, seleccione el cortafuegos en el menú desplegable **Contexto**.

STEP 2 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.

STEP 3 | Haga clic en **Disable Device and Network Template (Deshabilitar plantillas de dispositivos y red)**.

STEP 4 | (Opcional) Seleccione **Import Device and Network Template before disabling (Importar plantillas de dispositivos y red antes de deshabilitarlas)** para guardar los ajustes de configuración localmente en el cortafuegos. Si no selecciona esta opción, PAN-OS eliminará todas las configuraciones introducidas por Panorama desde el cortafuegos.

STEP 5 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para confirmar los cambios.

 ©2023 Palo Alto Networks, Inc.

Gestión de la clave maestra en Panorama

Panorama, los cortafuegos, los recopiladores de logs y los dispositivos WF-500 emplean una clave maestra para cifrar los elementos confidenciales de la configuración. También poseen una clave maestra predeterminada que sirve para cifrar las contraseñas y los elementos de configuración. Como medida de seguridad estándar, conviene sustituir la clave maestra predeterminada por otra en cada cortafuegos, recopilador de logs, dispositivo de WildFire e instancia de Panorama antes de que venza.

Para fortalecer su estrategia de seguridad, configure una clave maestra única para Panorama y para cada cortafuegos gestionado. Cuando configura claves maestras únicas, puede asegurarse de que una clave maestra en riesgo no comprometa el cifrado de configuración de toda su implementación. Las claves maestras únicas son compatibles solo con Panorama y cortafuegos gestionados. Los recopiladores de logs y los dispositivos WildFire deben compartir la misma clave maestra que Panorama. Para Panorama o cortafuegos gestionados en una configuración de alta disponibilidad (HA), debe implementar la misma clave maestra para ambos peers de HA ya que la clave maestra no está sincronizada entre peers de HA.

La configuración de una clave maestra única también alivia la carga operativa de actualizar sus claves maestras. Con la configuración de una clave maestra única para un cortafuegos gestionado, puede actualizar cada clave maestra individualmente sin la necesidad de coordinar el cambio de la clave maestra en una gran cantidad de cortafuegos gestionados.

Cuando una clave maestra caduca, debe ingresar la clave maestra actual para configurar una nueva.

Asegúrese de realizar un seguimiento de la clave maestra que implementa en sus cortafuegos gestionados, recopiladores de logs y dispositivos WildFire porque las claves maestras no se pueden recuperar. Debe restablecer los valores predeterminados de fábrica si no puede proporcionar la clave maestra actual cuando caduque.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | (Práctica recomendada) Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración pendientes y, luego, en **Commit and Push (Confirmar y enviar)**.

Panorama tiene que volver a cifrar los datos con la nueva clave maestra. Para garantizar que este proceso se aplica a todos los elementos de configuración, confirme los cambios pendientes antes de implementar la clave maestra nueva.

©2023 Palo Alto Networks, Inc.

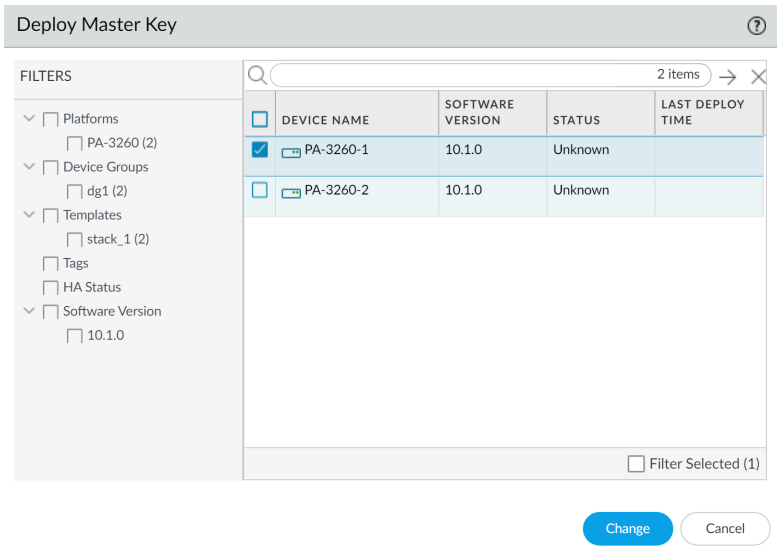
STEP 3 | Configure una clave maestra única para un cortafuegos gestionado.

1. (Solo HA) Deshabilite Config Sync para cortafuegos gestionados.

   Es obligatorio realizar este paso antes de implementar una clave maestra nueva en un par de HA del cortafuegos.

   1. Inicio de sesión en la interfaz web de Panorama.
   2. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y seleccione la **plantilla** que contiene la configuración de HA del cortafuegos gestionado.
   3. Edite los ajustes de la **configuración**de par de HA.
   4. Deshabilite (quite la marca) **Enable Config Sync (Habilitar sincronización de configuración)** y haga clic en **OK (Aceptar)**.
   5. Seleccione las opciones**Commit (Compilar)** y **Commit and Push (Compilar y enviar)** para aplicar esos cambios en su configuración.
2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y haga clic en **Deploy Master Key (Implementar clave maestra)**.
3. Seleccione un cortafuegos gestionado y cambie la clave maestra con la opción **Change (Cambiar)**.

   Si desea implementar una clave maestra única para un conjunto específico de cortafuegos gestionados, también puede seleccionar esos cortafuegos específicos.



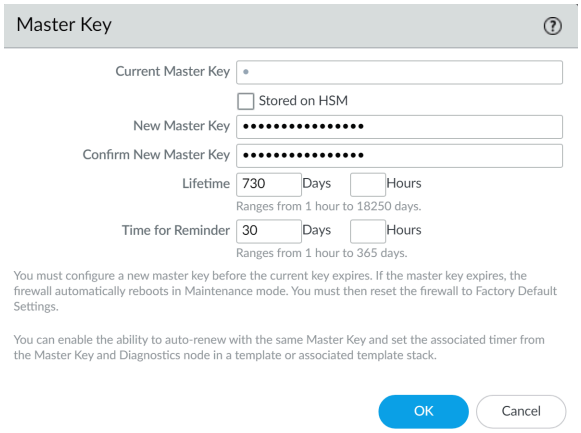
4. Configure la clave maestra:

   1. Si desea renovar la clave maestra, introdúzcala en **Current Master Key (Clave maestra actual)**. Si desea sustituir la clave maestra predeterminada por otra, deje en blanco **Current Master Key (Clave maestra actual)**.
   2. (Opcional) Habilite (marque) **Stored on HSM (Almacenado en HSM)** si la clave maestra está cifrada en un Módulo de seguridad de hardware (HSM).
   3. Especifique el valor oportuno en **New Master Key (Nueva clave maestra)** y en **Confirm Master Key (Confirmar clave maestra)**.

©2023 Palo Alto Networks, Inc.

4. Configure los valores oportunos para la clave maestra en **Lifetime (Duración)** y en **Time for Reminder (Recordatorio)**.
5. Haga clic en **OK (Aceptar)**.

   La nueva clave maestra se envía automáticamente a sus cortafuegos gestionados después de hacer clic en OK (Aceptar). Continúe solo si está seguro de que está listo para cambiar la clave maestra para sus cortafuegos gestionados.



5. Verifique que la clave maestra se ha implementado correctamente en todos los cortafuegos gestionados.

   Cuando implementa una clave maestra nueva desde Panorama, se genera un log del sistema.
6. (Opcional) Configure la clave maestra para que se renueve automáticamente para sus cortafuegos gestionados.

   Configure esta opción para renovar automáticamente la clave maestra implementada en los cortafuegos gestionados asociados con la plantilla seleccionada. De lo contrario, la clave maestra caduca según la vida útil configurada y debe implementar una nueva clave maestra.

   1. Seleccione **Device (Dispositivo)** > **Master Key and Diagnostic (Clave maestra y diagnóstico)** y seleccione la **Template (Plantilla)** que contiene los cortafuegos gestionados de destino.
   2. Edite la configuración de **Master Key (Clave maestra)** y configure la opción **Auto Renew With Same Master Key (Renovación automática con la misma clave maestra)**.
   3. Haga clic en **OK (Aceptar)**.
   4. Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

©2023 Palo Alto Networks, Inc.

STEP 4 | Configure la clave maestra en Panorama.

1. (Solo HA) Deshabilite la configuración de HA para Panorama.

   Este paso es necesario para cambiar correctamente el maestro para ambos peers de HA de Panorama. No puede compilar cambios de configuración en el peer de HA secundario cuando Panorama está en una configuración de HA.

   1. Inicio de sesión en la interfaz web de Panorama.
   2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración de HA.
   3. Deshabilite (quite la marca) **Enable HA (Habilitar HA)** y haga clic en **OK (Aceptar)**.
   4. Seleccione **Confirmar** y en **Confirmar en Panorama**.
2. Seleccione **Panorama** > **Master Key and Diagnostics (Clave maestra y diagnóstico)** y configure la clave maestra.

   1. Si desea renovar la clave maestra, introdúzcala en **Current Master Key (Clave maestra actual)**. Si desea sustituir la clave maestra predeterminada por otra, deje en blanco **Current Master Key (Clave maestra actual)**.
   2. Configure el valor oportuno en **New Master Key (Nueva clave maestra)** y en **Confirm Master Key (Confirmar clave maestra)**.
   3. Configure los valores oportunos para la clave maestra en **Lifetime (Duración)** y en **Time for Reminder (Recordatorio)**.
   4. Haga clic en **OK (Aceptar)**.

   > ***La nueva clave maestra se compila automáticamente a Panorama después de hacer clic en OK (Aceptar). Continúe solo si está seguro de que está listo para cambiar la clave maestra en Panorama.***
3. (Opcional) Configure la clave maestra de Panorama para que se renueve automáticamente.

   Configure esta opción para renovar automáticamente la clave maestra implementada en Panorama. De lo contrario, la clave maestra caduca según la vida útil configurada y debe implementar una nueva clave maestra.

   1. Seleccione **Panorama** > **Master Key and Diagnostic (Clave maestra y diagnóstico)** y edite la configuración de **Master Key (Clave maestra)**.
   2. Configure la opción **Auto Renew With Same Master Key (Renovación automática con la misma clave maestra)**.
   3. Haga clic en **OK (Aceptar)**.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios
5. (Solo HA) Repita este paso para configurar una clave maestra idéntica en el peer de HA secundario.

   Debe configurar manualmente una clave maestra idéntica en los peers de HA principales y secundarios cuando Panorama se encuentra en una configuración de HA. La clave maestra no está sincronizada entre los peers de HA principal y secundario.

©2023 Palo Alto Networks, Inc.

STEP 5 | Implemente la clave maestra en los recopiladores de logs.

La clave maestra configurada para sus recopiladores de logs debe ser idéntica a la clave maestra configurada para Panorama.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Deploy Master Key (Implementar clave maestra)**.
2. Seleccione todos los dispositivos y haga clic en **Change (Cambiar)** para modificar la clave maestra.
3. Configure la clave maestra:
   1. Si desea renovar la clave maestra, introdúzcala en **Current Master Key (Clave maestra actual)**. Si desea sustituir la clave maestra predeterminada por otra, deje en blanco **Current Master Key (Clave maestra actual)**.
   2. Especifique el valor oportuno en **New Master Key (Nueva clave maestra)** y en **Confirm Master Key (Confirmar clave maestra)**.
   3. Configure los valores oportunos para la clave maestra en **Lifetime (Duración)** y en **Time for Reminder (Recordatorio)**.
   4. Haga clic en **OK (Aceptar)**.

   *La nueva clave maestra se envía automáticamente a sus recopiladores de logs después de hacer clic en **OK (Aceptar)**. Continúe solo si está seguro de que está listo para cambiar la clave maestra de sus recopiladores de logs.*
4. Verifique que la clave maestra se ha implementado correctamente en todos los dispositivos seleccionados.

   Cuando implementa una clave maestra nueva desde Panorama, se genera un log del sistema.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Implemente la clave maestra en los dispositivos de WildFire gestionados.

La clave maestra configurada para sus dispositivos WildFire debe ser idéntica a la clave maestra configurada para Panorama.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos de WildFire gestionados)** y haga clic en **Deploy Master Key (Implementar clave maestra)**.
2. Seleccione todos los dispositivos y haga clic en **Change (Cambiar)** para modificar la clave maestra.
3. Configure la clave maestra:
   1. Si desea renovar la clave maestra, introdúzcala en **Current Master Key (Clave maestra actual)**. Si desea sustituir la clave maestra predeterminada por otra, deje en blanco **Current Master Key (Clave maestra actual)**.
   2. Especifique el valor oportuno en **New Master Key (Nueva clave maestra)** y en **Confirm Master Key (Confirmar clave maestra)**.
   3. Configure los valores oportunos para la clave maestra en **Lifetime (Duración)** y en **Time for Reminder (Recordatorio)**.
   4. Haga clic en **OK (Aceptar)**.

   > *La nueva clave maestra se envía automáticamente a sus dispositivos WildFire después de hacer clic en **OK (Aceptar)**. Continúe solo si está seguro de que está listo para cambiar la clave maestra de sus dispositivos WildFire.*
4. Verifique que la clave maestra se ha implementado correctamente en todos los dispositivos seleccionados.

   Cuando implementa una clave maestra nueva desde Panorama, se genera un log del sistema.

STEP 7 | (Solo Panorama de HA) Vuelva a ajustar la configuración de Panorama de HA.

Repita este paso para los peers de HA principal y secundario de Panorama.

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración de HA.
2. Habilite (marque) **Enable HA (Habilite HA)** y haga clic en **OK (Aceptar)**.
3. Seleccione **Confirmar** y en **Confirmar en Panorama**.

STEP 8 | (Solo cortafuegos de HA) Habilite la sincronización de configuración para cortafuegos gestionados.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y seleccione la **plantilla** que contiene la configuración de HA del cortafuegos gestionado.
2. Edite los ajustes de la **configuración**de par de HA.
3. Habilite (marque) **Enable Config Sync (Habilite Config Sync)** y haga clic en **OK (Aceptar)**.
4. Seleccione las opciones**Commit (Compilar)** y **Commit and Push (Compilar y enviar)** para aplicar esos cambios en su configuración.

©2023 Palo Alto Networks, Inc.

Programación de un envío de configuración en cortafuegos gestionados

Para reducir la sobrecarga que implica enviar los cambios de configuración a los cortafuegos gestionados, cree un envío de configuración programado a fin de enviar de forma automática los cambios en sus cortafuegos gestionados en una fecha y hora específicas. Puede establecer un envío de configuración programado para que se produzca una vez o de forma periódica. Esto le permite enviar la configuración realizada por varios administradores a varios cortafuegos sin que los administradores deban participar. Se admite un envío de configuración programado para un cortafuegos gestionado de destino que ejecute cualquier versión de PAN-OS.

Los superusuarios y los administradores de Panorama personalizados con un perfil de función de administración definido de manera correcta pueden crear un envío de configuración programada para los cortafuegos gestionados. Para crear un envío de configuración programado, establezca los parámetros de programación de cuándo y con qué frecuencia se produce un envío y a qué cortafuegos gestionados se deben enviar. Para un Panorama en una configuración de alta disponibilidad (HA), el envío de configuración programada se sincroniza en todos los peers de HA.

Si crea varios envíos programados de configuración, debe crearlos en un intervalo mínimo de 5 minutos para permitir que el servidor de gestión Panorama valide la configuración. Los envíos programados de configuración con menos de 5 minutos entre sí pueden fallar debido a que Panorama no puede validar los primeros cambios de envíos programados de configuración.

Después de que se produzca un envío de configuración programado correctamente, puede ver el historial de ejecución de envíos de configuración programados para comprender cuándo se produjo el último envío de una programación específico y ver cuántos cortafuegos gestionados se vieron afectados. A partir de la cantidad total de cortafuegos administrados afectados, puede ver cuántos envíos de configuración a cortafuegos administrados se realizaron de con éxito y cuántos fallaron. De las envíos fallidos, puede ver la cantidad total de cortafuegos gestionados con configuraciones revertidas de forma automática debido a un cambio de configuración que interrumpió la conexión entre el cortafuegos gestionado y Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Cree un envío de configuración programado.

1. Seleccione **Panorama** > **Scheduled Config Push (Envío de configuración programado)** y **Add (Añadir)** para agregar un nuevo envío programado de configuración.

   *También puede programar un envío de configuración en compilar gestionados cuando se envía a dispositivos (**Commit [Compilar]** > **Push to Devices [Enviar a dispositivos]**).*

2. Configure el nombre y la frecuencia del envío de configuración programado.

   - **Name (Nombre)**: nombre de la programación de envío de configuración.
   - **Alcance del administrador:**el administrador para el que se enviarán los cambios de configuración.

     El nombre del administrador que ha iniciado sesión y crea el envío de configuración programado se muestra de forma predeterminada. Haga clic en el nombre del administrador para añadir más administradores de Panorama al envío de configuración programado.
   - **Date (Fecha)**: fecha en la que está programado el próximo envío de configuración.
   - **Time (Hora)**: hora (`hh:mm:ss`) a la cual está programado el envío de configuración en la **Date (Fecha)** del envío.
   - **Recurrence (Periodicidad)**: si el envío de configuración programado es un envío único o un envío programado recurrente (`monthly [mensual]`, `weekly [semanal]` o `daily [diario]`).

3. En "Push Scope Selection" (Selección de ámbito del envío), seleccione uno o más grupos de dispositivos, plantillas o pilas de plantillas.

   Debe seleccionar al menos un grupo de dispositivos, plantilla o pila de plantillas para programar correctamente un envío de configuración.

   Todos los cortafuegos gestionados asociados con los grupos de dispositivos, plantillas o pilas de plantillas seleccionados se incluyen en envío programado de configuración.

   1. Seleccione uno o más **Device Groups (Grupos de dispositivos)** que desee programar para enviar.
   2. Seleccione una o más **Templates (Plantillas)** que desee programar para enviar.

      Se admiten hasta 64 plantillas para un único envío de configuración programado.

   3. Compruebe si desea **Merge with Device Candidate config (Combinar con la configuración del candidato de dispositivo)** para combinar los cambios de

 ©2023 Palo Alto Networks, Inc.

configuración enviados desde Panorama con los cambios de configuración pendientes implementados localmente en el cortafuegos.

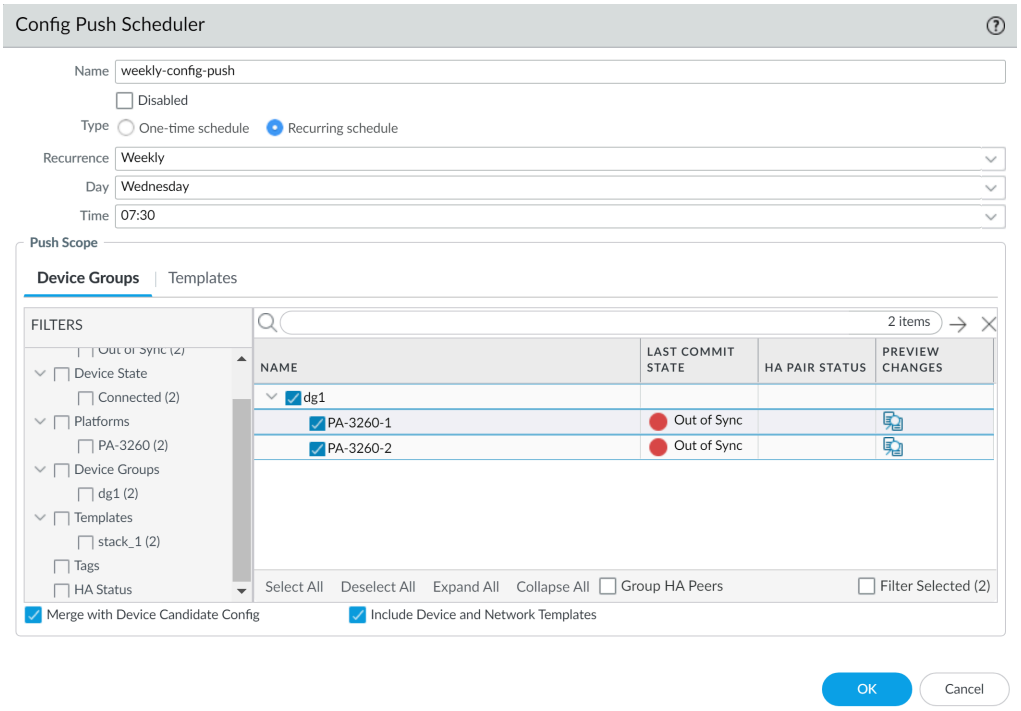
Esta configuración está habilitada de forma predeterminada.

4. Compruebe si desea **Include Device and Network Templates (Incluir plantillas de red y dispositivo)** para enviar los cambios de grupo de dispositivos y los cambios de plantilla de asociación en una sola operación.

   Esta configuración está habilitada de forma predeterminada. Si está deshabilitado, Panorama envía el grupo de dispositivos y los cambios de plantilla asociados como operaciones independientes.

   *La opción **Force Template Values (Forzar valores de plantilla)** no se admite para un envío programado de configuración a fin de evitar interrupciones durante las horas de envío que pueden generarse por un envío de configuración que sobrescribe la configuración del cortafuegos local.*

4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.



STEP 3 | Consulte el historial de ejecución para comprobar que se realizó correctamente el envío programado de configuración para todos los cortafuegos gestionados.

1. Seleccione **Panorama** > **Scheduled Config Push (Envío de configuración programado)** y haga clic en la marca de tiempo "Last Executed" (Última ejecución) en la columna "Status" (Estado).
2. Consulte el historial de ejecución del envío de configuración programado.

   Esto incluye la última vez que se produjo el envío programado de configuración y la cantidad total de cortafuegos gestionados afectados. Del número total de cortafuegos afectados, puede ver cuántos envíos de configuración programados se realizaron

©2023 Palo Alto Networks, Inc.

correctamente, cuántos fallaron y cuántos de los cortafuegos gestionados revirtieron automáticamente su configuración debido a un cambio de configuración que causó una desconexión entre el cortafuegos gestionado en Panorama.

3. Haga clic en **Tasks (Tareas)** para ver los detalles completos del último envío programado de configuración.

 ©2023 Palo Alto Networks, Inc.

Redistribución de datos a cortafuegos gestionados

Para garantizar que todos los cortafuegos que aplican las políticas y generan informes tengan los datos necesarios y las marcas de tiempo de autenticación para sus reglas de políticas, puede aprovechar su infraestructura de Panorama para redistribuir las asignaciones y las marcas de tiempo.

- Configure el servidor de gestión Panorama para redistribuir los datos.
  1. Añada cortafuegos, sistemas virtuales o agentes de User-ID de Windows como agentes de redistribución en Panorama:
     1. Seleccione **Panorama** > **Data Redistribution (Redistribución de datos)** y **añada** cada agente de redistribución.
     2. Introduzca un nombre en **Name (Nombre)** para identificar el agente de redistribución.
     3. Confirme que el agente esté **habilitado**.
     4. Introduzca el nombre de **Host** o la dirección IP de la interfaz MGT en el cortafuegos.
     5. Introduzca el número de **puerto** en el que el cortafuegos escuchará las consultas de redistribución de datos (el valor predeterminado es 5007).
     6. Si el agente de redistribución es un cortafuegos o sistema virtual, introduzca el **Collector name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida del recopilador)**.
     7. Seleccione el **tipo de datos** que desee redistribuir. Puede seleccionar todos los tipos de datos, pero debe seleccionar al menos uno de los siguientes tipos de datos:
        - **Asignaciones de usuarios de IP**
        - **Etiquetas de I**
        - **Etiquetas de usuario**
        - **HIP**
        - **Lista de cuarentena**
     8. Haga clic en **OK (Aceptar)** para guardar la configuración.
  2. Habilite la interfaz de Panorama MGT para responder a consultas de redistribución de datos desde cortafuegos:

     Si el servidor de gestión de Panorama tiene una configuración de alta disponibilidad (HA), realice este paso en cada peer de HA como una práctica recomendada para que la redistribución continúe si Panorama falla.

     1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces** y **Management (Gestión)**.
     2. Seleccione **User-ID** en la sección Network Services (Servicios de red) y haga clic en **OK (Aceptar)**.
  3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** para activar sus cambios en Panorama..

©2023 Palo Alto Networks, Inc.

- Configure cortafuegos para recibir datos que Panorama redistribuye.
  1. Seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)** y, a continuación, seleccione la **plantilla** a la que asignar los cortafuegos.
  2. **Añada** un agente y especifique un **nombre**.
  3. Seleccione cómo desea añadir el agente:
     - **Número de serie**: seleccione el **número de serie** del Panorama que desea utilizar en la lista:
       - **panorama**—El Panorama activo o solitario
       - **panorama2**—(solo HA) El Panorama pasivo
     - **Host and Port (Host y puerto)**: especifique la siguiente información:
       - Especifique el nombre de **Host** o la dirección IP de la interfaz MGT en el cortafuegos.
       - Seleccione si el host es un **proxy LDAP**.
       - Introduzca el número de **puerto** en el que el cortafuegos escuchará las consultas de redistribución de datos (el valor predeterminado es 5007).
       - Si el agente de redistribución es un cortafuegos o sistema virtual, introduzca el **Collector name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida del recopilador)**.
       - Seleccione el **tipo de datos** que desee redistribuir.
  4. Confirme que el agente esté **habilitado** y haga clic en **OK (Aceptar)** para guardar la configuración.
  5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para activar sus cambios en Panorama y enviar los cambios a los cortafuegos.

- Verifique que Panorama y los cortafuegos reciban datos redistribuidos.
  1. Vea las estadísticas del agente (**Panorama** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**) y seleccione **Status (Estado)** para ver un resumen de la actividad del agente de redistribución, como el número de asignaciones que ha recibido el cortafuegos del cliente.
  2. Confirme el **nombre de origen** en los logs de User-ID (**Monitor (Supervisar)** > **Logs** > **User-ID**) para verificar que el cortafuegos reciba las asignaciones a partir de los agentes de redistribución.
  3. Vea el log de etiquetas IP (**Monitor (Supervisor)** > **Logs** > **IP-Tag (Etiqueta IP)**) para confirmar que el cortafuegos del cliente recibe datos.
  4. Acceda a la CLI de un cortafuegos o el servidor de gestión Panorama que redistribuye los datos.
  5. Muestre todas las asignaciones de usuarios ejecutando el siguiente comando:

     ```
     > show user ip-user-mapping all
     ```

  6. Registre la dirección IP asociada con cualquier nombre de usuario.
  7. Acceda a la CLI de un cortafuegos o el servidor de gestión Panorama que recibe datos redistribuidos.

 ©2023 Palo Alto Networks, Inc.

8. Muestre la información de asignación y la marca de tiempo de autenticación para la ***<IP-address>*** que registró:

```
> show user ip-user-mapping ip <IP-address> IP
 address:    192.0.2.0 (vsys1) User:          corpdomain
\username1 From:          UIA Idle Timeout:  10229s Max.
 TTL:      10229s MFA Timestamp: first(1) - 2016/12/09
 08:35:04 Group(s): corpdomain\groupname(621)
```



Este ejemplo de resultado muestra la marca de tiempo de una respuesta a un desafío (factor) de autenticación. Para las reglas autenticación que utilizan autenticación multifactor (MFA)*, el resultado muestra múltiples marcas de tiempo.*

 ©2023 Palo Alto Networks, Inc.

Transición de un cortafuegos a una gestión de Panorama

Si ya ha implementado cortafuegos de Palo Alto Networks y los ha configurado localmente, pero ahora desea utilizar Panorama para gestionarlos centralmente, debe realizar la planificación previa a la migración. La migración implica importar configuraciones de cortafuegos en Panorama y verificar que los cortafuegos funcionan como lo esperado después de la transición. Si algunos ajustes son únicos para los cortafuegos individuales, puede continuar accediendo a los cortafuegos para gestionar la configuración única. Puede gestionar los ajustes de cualquier cortafuegos ingresando su valor desde Panorama o configurándolos localmente en el cortafuegos, pero no puede gestionar la configuración mediante Panorama y el cortafuegos. Si desea excluir determinados ajustes del cortafuegos desde la gestión de Panorama, puede llevar a cabo una de las siguientes opciones:

- Migre la configuración completa del cortafuegos y luego, en Panorama, elimine la configuración que gestionará localmente en el cortafuegos. También puede Cancelación de un valor de plantilla o pila de plantillas que Panorama envíe a un cortafuegos en lugar de eliminar la configuración en Panorama.
- Cargue una configuración de cortafuegos parcial, que incluya solo los ajustes que utilizará Panorama para gestionar.

> ***Los cortafuegos no pierden logs durante la transición a la gestión de Panorama.***

- Planificación de la transición a la gestión de Panorama
- Migración de un cortafuegos a la gestión de Panorama
- Migración de un par HA del cortafuegos a la gestión de Panorama
- Carga de una configuración de cortafuegos parcial en Panorama
- Cómo localizar una configuración enviada de Panorama en un cortafuegos gestionado

Planificación de la transición a la gestión de Panorama

Las siguientes tareas son una descripción general de alto nivel de la planificación requerida para migrar los cortafuegos a la gestión de Panorama:

- ☐ Decida qué cortafuegos migrará.
- ☐ Planifique una ventana de mantenimiento y asegúrese de que no haya cambios de configuración pendientes en Panorama o los cortafuegos.
- ☐ Si va a migrar el cortafuegos de un Panorama a otro, localice la configuración de Panorama enviada en el cortafuegos.
- ☐ Conserve sus configuraciones de cortafuegos y Panorama de trabajo conocidas antes de la migración.
  - Exporte el estado del dispositivo de sus cortafuegos.
  - Exporte una instantánea de configuración de Panorama con nombre de la configuración de Panorama en ejecución.
- ☐ Determine las versiones de contenido y el software de Panorama y el cortafuegos, y cómo administrará las licencias y las actualizaciones de software. Para obtener detalles importantes,

 ©2023 Palo Alto Networks, Inc.

consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.

- Planifique cómo gestionará la configuración compartida.

  Planifique la Jerarquía del grupo de dispositivos, Plantillas y pilas de plantillas de forma que reduzcan la redundancia y mejoren la gestión de la configuración que se comparte entre todos los cortafuegos o conjuntos de cortafuegos. Durante la migración, puede seleccionar si importar objetos desde la ubicación compartida en el cortafuegos a Compartida en Panorama, con las siguientes excepciones:

  - Si un objeto de cortafuegos compartido se llama igual y tiene el mismo valor que un objeto de Panorama existente, la importación excluye el objeto del cortafuegos.
  - Si el nombre o el valor del objeto compartido del cortafuegos no coinciden con el objeto compartido existente de Panorama, este importa el objeto del cortafuegos en cada grupo de dispositivos nuevo que se crea para la importación.
  - Si una configuración importada en una plantilla hace referencia a un objeto del cortafuegos compartido, o si un objeto del cortafuegos compartido hace referencia a una configuración compartida en una plantilla, Panorama importa el objeto como un objeto compartido independientemente de si selecciona la casilla de verificación **Import devices' shared objects into Panorama's shared context (Importar objetos compartidos de dispositivos al contexto compartido de Panorama)**.

- Determine si el cortafuegos tiene elementos de configuración (políticas, objetos y otros ajustes) que no desea importar, ya sea porque Panorama ya contiene elementos similares o porque estos elementos son específicos del cortafuegos (por ejemplo, la configuración de la zona horaria) y no usará Panorama para gestionarlos. Puede realizar una búsqueda global para determinar si existen elementos similares en Panorama.
- Decida las zonas comunes para cada grupo de dispositivos. Esto incluye una estrategia de denominación de zonas para los cortafuegos y los sistemas virtuales de cada grupo de dispositivos. Por ejemplo, si tiene zonas denominadas LAN y WAN de sucursal, Panorama puede introducir centralmente reglas de políticas que hagan referencia a esas zonas sin tener en cuenta las variaciones en el tipo de puerto o medio, el modelo o el esquema de dirección lógica.
- Cree un plan de prueba posterior a la migración.

  Utilizará el plan de prueba para verificar que después de la migración los cortafuegos funcionan de manera tan eficiente como antes de esta. El plan podría incluir tareas tales como las siguientes:

  - Supervisión de los cortafuegos por al menos 24 horas después de la migración.
  - Supervisión de logs de cortafuegos y Panorama en busca de anomalías.
  - Verificación de los inicios de sesión del administrador en Panorama.
  - Prueba de diferentes tipos de tráfico desde varios orígenes. Por ejemplo, revise los gráficos de anchos de banda, conteos de sesiones y entradas de logs de tráfico de la regla de negación (consulte Uso de Panorama para lograr visibilidad). La prueba debe cubrir una muestra representativa de las configuraciones de política.
  - Compruebe con su Centro de operaciones de red (network operations center, NOC) y Centro de operaciones de seguridad (security operations center, SOC) en caso de que haya problemas informados por los usuarios.
  - Incluya cualquier otro criterio de prueba que ayude a verificar la funcionalidad del cortafuegos.

 ©2023 Palo Alto Networks, Inc.

Migración de un cortafuegos a la gestión de Panorama

Cuando importa una configuración de cortafuegos, Panorama crea automáticamente una plantilla para incluir la configuración del dispositivo y red importada. Para incluir los objetos y políticas importados, Panorama crea automáticamente un grupo de dispositivos para cada cortafuegos o un grupo de dispositivos para cada sistema virtual (virtual system, vsys) en un cortafuegos de vsys múltiple.

Cuando lleva a cabo los siguientes pasos, Panorama importa la configuración completa del cortafuegos. De manera alternativa, puede cargar una configuración de cortafuegos parcial en Panorama.

Para migrar un peer de HA del cortafuegos a la gestión de Panorama, consulte Migración de un par HA del cortafuegos a la gestión de Panorama.

Panorama puede importar configuraciones de los cortafuegos que ejecutan PAN-OS 5.0 o versiones posteriores e enviar configuraciones en estos cortafuegos. La excepción es que Panorama 6.1 y versiones posteriores no pueden enviar configuraciones en cortafuegos que ejecuten de PAN-OS 6.0.0 a 6.0.3.

Panorama puede importar configuraciones de los cortafuegos que ya sean dispositivos gestionados pero solo si estos no están ya asignados a grupos de dispositivos o plantillas.

STEP 1 | Planifique la migración.

Consulte la lista de verificación en Planificación de la transición a la gestión de Panorama.

STEP 2 | Añada un cortafuegos como dispositivo gestionado

Consulte Añadir un cortafuegos como dispositivo gestionado para obtener más información sobre cómo añadir un cortafuegos a la gestión de Panorama.

1. Inicio de sesión en la interfaz web de Panorama
2. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.

   Copie la clave de autenticación después de crear correctamente la clave de autenticación de registro de dispositivo.
3. Seleccione **Panorama** > **Managed Devices** > **Summary** (Resumen de dispositivos gestionados de Panorama) para **añadir** un cortafuegos como dispositivo gestionado.
4. Introduzca el número de serie del cortafuegos y haga clic en **OK (Aceptar)**.

   Si importará múltiples configuraciones de cortafuegos, introduzca el número de serie de cada uno en una línea separada. De manera opcional, puede copiar y pegar los números de serie desde una hoja de datos de Microsoft Excel.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 3 | Configure una conexión entre el cortafuegos y Panorama.

1. Inicie sesión en la interfaz web del cortafuegos
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.

 ©2023 Palo Alto Networks, Inc.

3. En los campos **Panorama Servers (Servidores de Panorama)**, introduzca las direcciones IP del servidor de gestión de Panorama.
4. Pegue la **clave de autenticación** que copió en el paso anterior.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 4 | Importe una configuración de cortafuegos en Panorama.

*Si, más adelante, decide volver a importar una configuración de cortafuegos, elimine primero los grupos de dispositivos y las plantillas de los que forma parte. Si el nombre de estos es el mismo que el nombre de host de los cortafuegos, puede eliminar los grupos y las plantillas antes de volver a importar la configuración de los cortafuegos. Si no, defina un nombre nuevo para los grupos de dispositivos y las plantillas creados con la nueva importación en los campos **Device Group Name Prefix (Prefijo de nombre de grupo de dispositivos)**. Además, los cortafuegos no pierden logs cuando los elimina de los grupos de dispositivos o de las plantillas.*

1. Desde Panorama, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import device configuration to Panorama (Importar configuración de dispositivo a Panorama)** y seleccione **Device (Dispositivo)**.

   Panorama no puede importar una configuración de un cortafuegos que esté asignado a un grupo de dispositivos o plantilla existente.
2. (Opcional) Edite el valor de **Template Name (Nombre de plantilla)**. El valor predeterminado es el nombre del cortafuegos. No puede usar el nombre de plantillas o pilas de plantillas existentes.
3. (Opcional) Edite los nombres de **Device Group (Grupo de dispositivos)**. Para un cortafuegos con vsys múltiple, cada grupo de dispositivos tiene un nombre vsys por defecto, añada una cadena de caracteres a cada uno, por ejemplo, un Device Group Name Prefix (Prefijo del nombre de grupo de dispositivos). De lo contrario, el valor predeterminado es el nombre del cortafuegos. No puede usar los nombres de grupos de dispositivos existentes.

   *La casilla de verificación **Import devices' shared objects into Panorama's shared context (Importar objetos compartidos de dispositivos al contexto compartido de Panorama)** está seleccionada de manera predeterminada, lo que significa que Panorama compara e importa objetos de Compartidos en el cortafuegos a Compartidos en Panorama. Si un objeto importado no está en el contexto Compartido del cortafuegos, se aplica a cada grupo de dispositivos que se está importando. Si desactiva la casilla de verificación, las copias de Panorama no compararán los objetos importados y aplicarán todos los objetos de cortafuegos compartidos en grupos de dispositivos importados en lugar de compartidos. Esto podría crear objetos duplicados, de modo que seleccionar la casilla de verificación es la acción recomendada en la mayoría de los casos. Para comprender las consecuencias de importar objetos compartidos o duplicados en Panorama, consulte* Planificación sobre cómo gestionar la configuración compartida.
4. Seleccione una **Rule Import Location (Ubicación de importación de regla)** para las reglas de políticas importadas: **Pre Rulebase (Base de regla previa)** o **Post Rulebase (Base**

 ©2023 Palo Alto Networks, Inc.

de regla posterior). Independientemente de su selección, Panorama importa reglas de seguridad predeterminadas (predeterminada intrazona y predeterminada entre zonas) en la base de reglas posterior.

Si Panorama tiene una regla que se llama igual que una regla de cortafuegos que está importando, Panorama muestra ambas reglas. Elimine una de las reglas antes de realizar la compilación de Panorama para evitar un error de compilación.

5. Haga clic en **OK (Aceptar)**. Panorama muestra el estado de la importación, el resultado, los detalles de sus selecciones, los detalles de lo que se importó y las advertencias. Haga clic en **Close (Cerrar)**.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 5 | Envíe el lote de configuración de Panorama al cortafuegos recién agregado para eliminar todas las reglas de políticas y objetos de su configuración local.

Este paso es necesario para evitar nombres de objetos o reglas duplicados, lo cual provocaría errores de compilación cuando ingresa la configuración del grupo de dispositivos desde Panorama al cortafuegos en el siguiente paso.

*Cuando envía la configuración del cortafuegos importada desde Panorama para eliminar la configuración del cortafuegos local, en la regla de **Policy (Política)** se actualizan las fechas de **Creation (Creación)** y **Modified (Modificación)** para reflejar la fecha en la que envió los cortafuegos recién gestionados cuando* supervisa el uso de la regla de políticas para un cortafuegos gestionado*. Además, se crea un nuevo* identificador único universal (UUID) *para cada regla de políticas.*

Este paso es obligatorio para migrar la gestión del cortafuegos al servidor de gestión de Panorama. Si no se realiza, se producen errores de configuración y de confirmación.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Export or push device config bundle (Exportar o enviar lote de configuraciones de dispositivos)**.
3. Seleccione el **Device (Dispositivo)** desde el cual importó la configuración y haga clic en **OK (Aceptar)**.

   *Si se configura una clave maestra, seleccione **Use Master Key (Usar clave maestra)** e introduzca la clave maestra antes de hacer clic en **OK (Aceptar)**.*
4. Seleccione **Push & Commit (Enviar y compilar)**. Panorama ingresa el lote e inicia una compilación en el cortafuegos.
5. Haga clic en **Close (Cerrar)** cuando se haya confirmado el envío.
6. Inicie la interfaz web del cortafuegos y compruebe que se ha confirmado la configuración. Si no es así, haga clic en **Commit (Confirmar)** para aceptar los cambios de forma local en el cortafuegos.
7. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Ingrese la configuración del grupo de dispositivos y plantilla para completar la transición a la gestión centralizada.

Este paso sobrescribe cualquier configuración de **Network (Red)** y **Device (Dispositivo)** configurada en el cortafuegos.

Si migra varios cortafuegos, lleve a cabo todos los pasos anteriores (incluido este) en cada cortafuegos antes de continuar.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Device Groups (Grupos de dispositivos)** y seleccione los grupos de dispositivos que contienen las configuraciones de cortafuegos importadas.
3. Seleccione **Merge with Device Candidate Config (Integrar con configuración candidata del dispositivo)**, **Include Device and Network Templates (Incluir plantillas de dispositivo y red)** y **Force Template Values (Forzar valores de plantilla)**.
4. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
5. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 7 | En la interfaz web de Panorama, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y verifique que el grupo de dispositivos y la pila de plantillas están sincronizados en el cortafuegos. En la interfaz web del cortafuegos, verifique que los objetos de configuración muestran una rueda dentada de color verde ( ), que significa que se han enviado desde Panorama.

STEP 8 | Ajuste la configuración importada.

1. En Panorama, seleccione **Panorama** > **Config Audit (Auditoría de configuraciones)**, seleccione **Running config (Configuración en ejecución)** y **Candidate config (Configuración candidata)** para la comparación, haga clic en **Go (Ir)**, y revise los resultados.
2. Actualice las configuraciones del grupo de dispositivos y plantillas según sea necesario sobre la base de la auditoría de configuración y las advertencias que Panorama mostró después de la importación. Por ejemplo:
   - Elimine las reglas de política y los objetos redundantes.
   - Mueva o duplique una regla de política u objeto a un grupo de dispositivos diferente.
   - Mueva los cortafuegos a grupos de dispositivos o plantillas diferentes.
   - Mueva el grupo de dispositivos que Panorama creó durante la importación a un grupo de dispositivos primario diferente: Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos que desea mover y un nuevo **Parent Device Group (Grupo de dispositivos primario)**, y haga clic en **OK (Aceptar)**.

STEP 9 | Consolide toda la configuración importada del cortafuegos.

Este paso es obligatorio para migrar varios cortafuegos.

1. Después de importar todas las configuraciones de cortafuegos, actualice los grupos de dispositivos y las plantillas como sea necesario para eliminar la redundancia y optimizar la

 ©2023 Palo Alto Networks, Inc.

gestión de las configuraciones; consulte el paso para ajustar la configuración importada. (No es necesario volver a enviar los lotes de configuración del cortafuegos).

2. Configure los ajustes específicos del cortafuegos.

   Si los cortafuegos van a tener zonas locales, debe crearlos antes de realizar una compilación del grupo de dispositivos y plantillas. Panorama no puede sondear los cortafuegos por nombre de zona o configuración de zona. Si utiliza las reglas del cortafuegos local, asegúrese de que sus nombres sean únicos (no estén duplicados en Panorama). Si es preciso sustituir algún valor específico del cortafuegos, realice el procedimiento Cancelación de un valor de plantilla o pila de plantillas.

3. Confirme y envíe sus cambios:

   1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
   2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos que ha cambiado y seleccione **Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
   3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
   4. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 10 | Lleve a cabo un plan de prueba posterior a la migración.

Lleve a cabo las tareas de verificación concebidas al planificar la migración para confirmar que los cortafuegos funcionan con la configuración enviada por Panorama de manera tan eficiente como con la configuración local original; consulte el paso para trazar un plan de pruebas posteriores a la migración.

Migración de un par HA del cortafuegos a la gestión de Panorama

Si tiene un par de cortafuegos en una configuración HA que desea gestionar con Panorama, tiene la opción de importar la configuración de su par de HA de cortafuegos a Panorama sin necesidad de volver a crear configuraciones o políticas. Primero, importe a Panorama las configuraciones de los cortafuegos, que sirven para crear grupos de dispositivos y plantillas. Realizará una configuración especial de envío del grupo de dispositivos y la plantilla a los cortafuegos para sobrescribir las configuraciones de cortafuegos locales y sincronizar los cortafuegos con Panorama.

STEP 1 | Planifique la migración.

Consulte la lista de verificación en Planificación de la transición a la gestión de Panorama.

STEP 2 | Deshabilite la sincronización de configuración entre los peers de HA.

Repita estos pasos para ambos cortafuegos en el par de HA.

1. Inicie sesión en la interfaz web en cada cortafuegos, seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Quite la marca de **Enable Config Sync (Habilitar sincronización de configuración)** y haga clic **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Añada cada cortafuegos como dispositivo gestionado.

Si Panorama ya está recibiendo logs de estos cortafuegos, no es necesario que realice este paso. Continúe al paso 5.

Consulte Añadir un cortafuegos como dispositivo gestionado para obtener más información sobre cómo añadir un cortafuegos a la gestión de Panorama.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.

   Copie la clave de autenticación después de crear correctamente la clave de autenticación de registro de dispositivo.
3. Seleccione **Panorama** > **Managed Devices** > **Summary** (Resumen de dispositivos gestionados de Panorama) para **añadir** un cortafuegos como dispositivo gestionado.
4. Introduzca el número de serie de cada cortafuegos y haga clic en **OK (Aceptar)**.
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.
6. Verifique que el "Device State" (Estado del dispositivo) para cada cortafuegos sea `Connected (Conectado)`.

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address		VARIABL...	TEMPLATE	DEVICE STATE	DEVICE CERTIFICATE	DEVICE CERTIFICATE EXPIRY DATE	HA STATUS
						IPV4	I...						
>	Alaap_LTD (2/2 Devices Connected): Shared > Alaap_LTD												
v	No Device Group Assigned (2/2 Devices Connected)												
	adept-vm-2		PA-VM					Edit		Connected			Passive
	adept-vm-1							Edit		Connected			Active

STEP 4 | Conecte cada cortafuegos a Panorama.

Si Panorama ya está recibiendo logs de estos cortafuegos, no es necesario que realice este paso. Continúe al paso 5.

Repita estos pasos para ambos cortafuegos en el par de HA.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
3. En los campos **Panorama Servers (Servidores Panorama)**, introduzca las direcciones IP de los servidores de gestión de Panorama, confirme que **Panorama Policy and Objetcs (Política y objetos de Panorama)** y **Device and Network Template (Plantilla de dispositivo y de red)** están habilitados.
4. Pegue la **clave de autenticación** que copió en el paso anterior.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

©2023 Palo Alto Networks, Inc.

STEP 5 | Importe cada una de las configuraciones de cortafuegos en Panorama.

No envíe ningún grupo de dispositivos o configuración de pila de plantillas a sus cortafuegos gestionados en este paso. Al enviar el grupo de dispositivos y la configuración de la pila de plantillas durante este paso, se borra la configuración de HA del cortafuegos local en los siguientes pasos.

Si, más adelante, decide volver a importar una configuración de cortafuegos, elimine primero los grupos de dispositivos y las plantillas de los que forma parte. Si el nombre de estos es el mismo que el nombre de host de los cortafuegos, puede eliminar los grupos y las plantillas antes de volver a importar la configuración de los cortafuegos. Si no, introduzca un nombre nuevo para los grupos de dispositivos y las plantillas creados con la nueva importación en los campos ***Device Group Name Prefix (Prefijo de nombre de grupo de dispositivos)****. Además, los cortafuegos no pierden logs cuando los elimina de los grupos de dispositivos o de las plantillas.*

1. Desde Panorama, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import device configuration to Panorama (Importar configuración de dispositivo a Panorama)** y seleccione **Device (Dispositivo)**.

   Panorama no puede importar configuraciones de cortafuegos asignados a grupos de dispositivos o pilas de plantillas existentes.
2. (Opcional) Edite el valor de **Template Name (Nombre de plantilla)**. El valor predeterminado es el nombre del cortafuegos. No puede usar el nombre de plantillas o pilas de plantillas existentes.
3. (Opcional) Edite los nombres de **Device Group (Grupo de dispositivos)**. Para un cortafuegos con vsys múltiple, cada grupo de dispositivos tiene un nombre vsys por defecto, añada una cadena de caracteres a cada uno, por ejemplo, un Device Group Name Prefix (Prefijo del nombre de grupo de dispositivos). De lo contrario, el valor predeterminado es el nombre del cortafuegos. No puede usar los nombres de grupos de dispositivos existentes.

   La casilla de verificación ***Imported devices' shared objects into Panorama's shared context (Importar objetos compartidos de dispositivos al contexto compartido de Panorama)*** *está seleccionada de manera predeterminada, lo que significa que Panorama compara e importa objetos de Compartidos en el cortafuegos a Compartidos en Panorama. Si un objeto importado no está en el contexto Compartido del cortafuegos, se aplica a cada grupo de dispositivos que se está importando. Si desactiva la casilla de verificación, las copias de Panorama no compararán los objetos importados y aplicarán todos los objetos de cortafuegos compartidos en grupos de dispositivos importados en lugar de compartidos. Esto podría crear objetos duplicados, de modo que seleccionar la casilla de verificación es la acción recomendada en la mayoría de los casos. Para comprender las consecuencias de importar objetos compartidos o duplicados en Panorama, consulte* Planificación sobre cómo gestionar la configuración compartida**.**
4. **Commit to Panorama (Confirmar en Panorama)**.
5. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Export or push device config bundle (Exportar o enviar lote de configuraciones de**

 ©2023 Palo Alto Networks, Inc.

dispositivos). Seleccione el dispositivo en **Device (Dispositivo)** y, luego, haga clic en **OK (Aceptar)** y en **Push & Commit (Enviar y compilar)** la configuración.

> ***Debe quitar la marca del ajuste Enable Config Sync (Habilitar sincronización de configuraciones) en el paso 2 en ambos cortafuegos antes de enviar el grupo de dispositivos y la pila de plantillas.***

6. Inicie la interfaz web del peer de HA del cortafuegos y compruebe que la configuración enviada en el paso anterior se haya compilado correctamente. Si no es así, haga clic en **Commit (Confirmar)** para aceptar los cambios de forma local en el cortafuegos.
7. Repita los pasos 1-6 anteriores en el segundo cortafuegos. En el proceso, se crea un grupo de dispositivos y una pila de plantillas para cada cortafuegos.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Añada el par de cortafuegos de HA al mismo grupo de dispositivos y a la misma pila de plantillas.

(Cortafuegos en configuración activa/activa) Se recomienda añadir peers de HA al mismo grupo de dispositivos, pero no a la misma pila de plantillas, ya que los cortafuegos en una configuración de HA activa/activa suelen necesitar configuraciones de red únicas. Esto simplifica la administración de políticas para los peers de HA al tiempo que reduce la carga operativa de administrar la configuración de red de cada peer de HA cuando sus configuraciones de red son independientes entre sí. Por ejemplo, los cortafuegos en una configuración de HA activa/activa a menudo necesitan configuraciones de red únicas, como IP flotante única que se utilizan como puerta de enlace predeterminada para los hosts.

En última instancia, decidir si añadir cortafuegos en una configuración de HA activa/activa al mismo grupo de dispositivos y pila de plantillas es una decisión de diseño que debe tomar al diseñar su jerarquía de configuración.

1. Seleccione **Panorama** > **Device Group (Grupo de dispositivos)**, seleccione el grupo de dispositivos del segundo cortafuegos y elimine el segundo cortafuegos del grupo de dispositivos.
2. Seleccione el grupo de dispositivos del que eliminó el segundo cortafuegos y haga clic en **Delete (Eliminar)**.
3. Seleccione el grupo de dispositivos para el primer cortafuegos, seleccione el segundo cortafuegos, haga clic en **OK (Aceptar)** y **Commit to Panorama (Confirmar en Panorama)** para añadirlo al mismo grupo de dispositivos que el peer de HA.
4. Seleccione **Panorama** > **Templates (Plantillas)**, seleccione la pila de plantillas del segundo cortafuegos y elimine el segundo cortafuegos de la pila de plantillas.
5. Seleccione la pila de plantillas de la que eliminó el segundo cortafuegos y haga clic en **Delete (Eliminar)**.
6. Seleccione la pila de plantillas del primer cortafuegos, añada el segundo cortafuegos y haga clic en **OK (Aceptar)** y en **Commit to Panorama (Confirmar en Panorama)** para añadirlo a la misma pila de plantillas que el peer de HA.
7. Elimine la configuración de HA en la plantilla asociada con los cortafuegos recién migrados.
   1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** y elija la **Template (Plantilla)** que contenga la configuración de HA.
   2. Seleccione **Remove All (Eliminar todo)**.
   3. **Commit to Panorama (Confirmar en Panorama)**.
8. Inserte el grupo de dispositivos y las configuraciones de la pila de plantillas en sus cortafuegos gestionados.

Primero, envíe el grupo de dispositivos y la configuración de la pila de plantillas a su peer de HA pasivo y luego al activo.

©2023 Palo Alto Networks, Inc.

*Cuando envía la configuración del cortafuegos importada desde Panorama para eliminar la configuración del cortafuegos local, en la regla de **Policy (Política)** se actualizan las fechas de **Creation (Creación)** y **Modified (Modificación)** para reflejar la fecha en la que envió los cortafuegos recién gestionados cuando* supervisa el uso de la regla de políticas para un cortafuegos gestionado*. Además, se crea un nuevo* identificador único universal (UUID) *para cada regla de políticas.*

1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
2. Habilite (seleccione) **Merge Device Candidate Config (Integrar configuración candidata del dispositivo)**, **Include Device and Network Templates (Incluir plantillas de dispositivo y red)** y **Force Template Values (Forzar valores de plantilla)**.
3. Haga clic en **OK (Aceptar)**.
4. **Realice el envío** a sus cortafuegos gestionados.
5. Inicie la interfaz web del peer de HA activo y seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Operational Commands (Comandos operativos)** en **Suspend local device (Suspender dispositivo local)**.

   Realice la conmutación por error al peer de HA pasivo antes de modificar el peer de HA activo para mantener su estrategia de seguridad mientras completa la migración de la configuración.
6. Repita los pasos del 1 al 4 para el peer de HA ahora pasivo.
7. Inicie la interfaz web del ahora peer de HA activo y seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Operational Commands (Comandos operativos)** en **Suspend local device (Suspender dispositivo local)**.

   Con este procedimiento, se restauran las funciones de peer de HA activos/pasivos originales.

9. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y verifique que el grupo de dispositivos y la plantilla están sincronizados en el cortafuegos pasivo. Verifique que las reglas de política, los objetos y la configuración de red en el cortafuegos pasivo coinciden con el cortafuegos activo.

STEP 7 | Habilite la sincronización de la configuración entre los peers de HA.

Repita estos pasos para ambos cortafuegos en el par de HA si planea mantener una configuración local que necesita sincronizarse.

1. Inicie sesión en la interfaz web en cada cortafuegos, seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Seleccione **Enable Config Sync (Habilitar sincronización de configuración)** y haga clic **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.

 ©2023 Palo Alto Networks, Inc.

Carga de una configuración de cortafuegos parcial en Panorama

Si algunos ajustes de configuración en un cortafuegos son comunes con otros cortafuegos, puede cargar esos en Panorama y luego enviarlos en todos los demás cortafuegos o a los cortafuegos en grupos de dispositivos y plantillas específicas.

La carga de una configuración en el servidor de gestión Panorama requiere una confirmación completa y debe realizarla un superusuario. Se requerirán confirmaciones completas cuando se realicen determinadas operaciones de Panorama, como revertir y cargar una instantánea de configuración, y no serán compatibles con los perfiles de función de administración personalizados.

STEP 1 | Planifique la transición a Panorama.

Consulte la lista de verificación en Planificación de la transición a la gestión de Panorama.

STEP 2 | Resuelva cómo gestionar la configuración duplicada, que son los ajustes que tienen los mismos nombres en Panorama y en un cortafuegos.

Antes de cargar una configuración de cortafuegos parcial, Panorama y el cortafuegos ya podrían tener ajustes duplicados. Cargar una configuración de cortafuegos podría también añadir ajustes a Panorama que son duplicados de los ajustes en otros cortafuegos gestionados.

Si Panorama tiene reglas de política u objetos con los mismos nombres que aquellos en un cortafuegos, se podría producir una falla de compilación cuando intenta enviar ajustes del grupo de dispositivos a ese cortafuegos. Si Panorama tiene ajustes de plantilla con el mismo nombre que aquellos en un cortafuegos, los valores de la plantilla cancelarán los valores del cortafuegos cuando ingrese la plantilla.

1. En Panorama, realice una búsqueda global para determinar si existen ajustes duplicados.
2. Elimine o vuelva a nombrar los ajustes duplicados en el cortafuegos si utilizará Panorama para gestionarlos, o elimine o vuelva a nombrar los ajustes duplicados si utilizará el cortafuegos para gestionarlos. Si utilizará el cortafuegos para gestionar ajustes de red o dispositivo, en lugar de eliminar o volver a nombrar los duplicados en Panorama, también puede enviar los ajustes desde Panorama (paso 6) y luego Cancelación de un valor de plantilla o pila de plantillas en el cortafuegos con valores específicos del cortafuegos.

STEP 3 | Exporte la configuración completa del cortafuegos a su computadora local.

1. En el cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named configuration snapshot (Guardar instantánea de configuración con nombre)**, introduzca un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named configuration snapshot (Exportar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. El cortafuegos exporta la configuración como un archivo XML.

©2023 Palo Alto Networks, Inc.

STEP 4 | Importe una instantánea de configuración del cortafuegos en Panorama.

1. En Panorama, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, haga clic en **Browse (Explorar)** para ir al archivo de configuración del cortafuegos que exportó en su computadora y haga clic en **OK (Aceptar)**.

   Después de usar esta opción para importar un archivo de configuración del cortafuegos, puede usar la interfaz web de Panorama para cargarlo. Debe usar la CLI o API XML, como se describe en el siguiente paso.

STEP 5 | Cargue la parte deseada de la configuración del cortafuegos en Panorama.

Para especificar una parte de la configuración (por ejemplo, todos los objetos de aplicación), debe identificar lo siguiente:

- Xpath de origen: el nodo XML en el archivo de configuración del cortafuegos desde el cual realiza la carga.
- Xpath de destino: el nodo XML en la configuración de Panorama al cual realiza la carga.

Use la CLI o API XML para identificar y cargar la configuración parcial:

1. Use la CLI o API XML del cortafuegos para identificar el xpath de origen.

   Por ejemplo, el xpath para los objetos de la aplicación en vsys 1 del cortafuegos es el siguiente:

   ```
   /config/devices/entry[@name='localhost.localdomain']/vsys/
   entry[@name='vsys1']/aplicación
   ```

2. Use la CLI o API XML de Panorama para identificar el xpath de destino.

   Por ejemplo, para cargar objetos de aplicación en un grupo de dispositivos llamado US-West, el xpath es el siguiente:

   ```
   /config/devices/entry[@name='localhost.localdomain']/device-
   group/entry[@name='US-West']/aplicación
   ```

3. Use la CLI de Panorama para cargar la configuración y compilar el cambo:

   ```
   # load config partial mode [append|merge|replace]
    from-xpath <source-xpath> to-xpath <destination-xpath>
    from <filename> # commit
   ```

   Por ejemplo, introduzca lo siguiente para cargar objetos de aplicación desde vsys1 en una configuración de cortafuegos importada con el nombre fw1-config.xml en un grupo de dispositivos llamado US-West en Panorama:

   ```
   # load config partial mode merge from-xpath
    devices/entry[@name='localhost.localdomain']/vsys/
   entry[@name='vsys1']/application to-xpath /config/
   devices/entry[@name='localhost.localdomain']/device-group/
   ```

 ©2023 Palo Alto Networks, Inc.

```
entry[@name='US-West']/application from fw1-config.xml
 # commit
```

STEP 6 | Ingrese la configuración parcial de Panorama en el cortafuegos para completar la transición a la gestión centralizada.

1. En el cortafuegos, elimine las reglas u objetos que tienen los mismos nombres que aquellos en Panorama. Si el grupo de dispositivos de ese cortafuegos tiene otros cortafuegos con reglas u objetos que están duplicados en Panorama, lleve a cabo este paso en esos cortafuegos también. Para obtener más información, consulte el paso 2.
2. En Panorama, envíe la configuración parcial al cortafuegos.
    1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
    2. Seleccione **Device Groups (Grupos de dispositivos)** y seleccione los grupos de dispositivos que contienen las configuraciones de cortafuegos importadas.
    3. Seleccione **Merge with Device Candidate Config (Integrar con configuración candidata del dispositivo)**, **Include Device and Network Templates (Incluir plantillas de dispositivo y red)** y **Force Template Values (Forzar valores de plantilla)**.
    4. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
    5. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.
3. Si el cortafuegos tiene una configuración de dispositivo o red que no usará Panorama para gestionarla, Cancelación de un valor de plantilla o pila de plantillas en el cortafuegos.

STEP 7 | Lleve a cabo un plan de prueba posterior a la migración.

Lleve a cabo las tareas de verificación que concibió durante la planificación de la migración para confirmar que el cortafuegos funciona de manera tan eficiente con la configuración ingresada en Panorama como lo hace con su configuración local original: consulte Creación de un plan de prueba posterior a la migración.

Cómo localizar una configuración enviada de Panorama en un cortafuegos gestionado

Puede localizar las configuraciones de plantilla y grupo de dispositivos enviadas desde el servidor de gestión Panorama™ para:

- Eliminar el cortafuegos de la gestión de Panorama
- Migrar la gestión del cortafuegos a un Panorama diferente
- En el caso de una emergencia en la que no se pueda acceder a Panorama, asegúrese de que los administradores puedan modificar la configuración del cortafuegos gestionado localmente.

STEP 1 | Inicie la interfaz web del cortafuegos gestionado como administrador con la función de superusuario. Puede acceder al cortafuegos directamente introduciendo su dirección IP en el campo URL del navegador; o bien, en Panorama, seleccione el cortafuegos en el menú desplegable **Contexto**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | (Práctica recomendada) Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y **Export device state (Exportar estado de dispositivo)**.

Guarde una copia del estado del sistema del cortafuegos, incluida la configuración del grupo de dispositivos y la plantilla enviada desde Panorama, en caso de que necesite volver a cargar una configuración de trabajo conocida en el cortafuegos gestionado.

STEP 3 | Deshabilite la configuración de la plantilla a fin de dejar de usar plantillas y pilas de plantillas para administrar los objetos de configuración de red del cortafuegos gestionado.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
2. Haga clic en **Disable Device and Network Template (Deshabilitar plantillas de dispositivos y red)**.
3. (Opcional) Seleccione **Import Device and Network Template before disabling (Importar plantillas de dispositivos y red antes de deshabilitarlas)** para guardar los ajustes de configuración de la plantilla localmente en el cortafuegos. Si no selecciona esta opción, PAN-OS elimina todas las configuraciones introducidas por Panorama desde el cortafuegos.
4. Haga clic en **OK (Aceptar)** dos veces para continuar.

STEP 4 | Deshabilite la configuración del grupo de dispositivos a fin de dejar de usar un grupo de dispositivos para administrar la política y las configuraciones de objetos del cortafuegos gestionado.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
2. (Opcional) Seleccione **Import Panorama Policy Objects before disabling (Importar objetos de política de Panorama antes de deshabilitar)** para guardar la política y las configuraciones de objetos localmente en el cortafuegos. Si no selecciona esta opción, PAN-OS elimina todas las configuraciones introducidas por Panorama desde el cortafuegos.
3. Haga clic en **OK (Aceptar)** para continuar.



No intente compilar los cambios de configuración en el cortafuegos gestionado todavía, ya que todas las compilaciones fallan hasta que se completen con éxito los siguientes pasos.

STEP 5 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Save named configuration snapshot (Guardar instantánea de configuración con nombre)**.

STEP 6 | **Cargue la instantánea de configuración con nombre** y habilite (marque) **Regenerate Rule UUIDs for selected named configuration (Regenerar UUID de regla para la configuración con nombre seleccionada)** a fin de generar nuevos UUID de regla de política.

Este paso es necesario para localizar correctamente las reglas de política introducidas por Panorama en los cortafuegos gestionados.

STEP 7 | Haga clic en **OK (Aceptar)** para cargar la instantánea de configuración con nombre.

STEP 8 | Haga clic en **Commit (Compilar)** para confirmar la carga de la instantánea de configuración con nombre.

 ©2023 Palo Alto Networks, Inc.

Supervisión de dispositivos en Panorama

Tras añadir sus cortafuegos y configurar las reglas de la política, puede supervisar el estado para garantizar que sus cortafuegos funcionen dentro de parámetros aceptables. En el caso de las reglas de la política, supervise las coincidencias de tráfico de reglas para identificar las reglas que coinciden con sus necesidades de aplicación de tráfico.

- Supervisión del estado del dispositivo
- Supervisión de la utilización de las reglas de la política

Supervisión del estado del dispositivo

Supervise la información de estado de sus cortafuegos gestionados para identificar y solucionar problemas de hardware antes de que afecten a la seguridad de su red. Tanto Panorama™ como los cortafuegos gestionados deben ejecutar PAN-OS® 8.1 o versiones posteriores, pero no hace falta que los cortafuegos formen parte de ningún grupo de dispositivos ni de ninguna pila de plantillas para supervisar el resumen de las sesiones, la creación de logs, los recursos ni el rendimiento del entorno. Panorama almacena los datos de los últimos 90 días de estadísticas de supervisión de estado de sus cortafuegos gestionados, de modo que cuando seleccione un cortafuegos, pueda ver los gráficos con tendencias en el tiempo y tablas de sesiones, información ambiental, interfaces, logging, recursos y rendimiento de alta disponibilidad. Panorama calcula el rendimiento de referencia de cada métrica utilizando promedios de siete días y la desviación estándar para determinar un rango operativo normal para el cortafuegos específico. Además de realizar el seguimiento de los valores de referencia y comparar el rendimiento en tendencias en el tiempo, puede ver qué cortafuegos poseen métricas desviadas y aislar los problemas de rendimiento antes de que afecten a su red. Cuando Panorama identifica que una métrica se encuentra fuera del rango operativo normal, marca la métrica y completa la pestaña Deviating Devices (Dispositivos desviados) con la información del cortafuegos desviado.

Los datos de supervisión del estado se almacenan en Panorama y se guardan en caso de que se elimine el cortafuegos. Cuando se elimina un cortafuegos de la gestión de Panorama, los datos de supervisión de estado ya no se muestran, pero se guardan por 90 días. Después de 90 días, todos los datos de supervisión de estado del cortafuegos eliminado se borran de Panorama. Si se vuelve a añadir un cortafuegos a la gestión de Panorama, se muestran los datos de supervisión de estado más recientes desde el momento en el que se eliminó el cortafuegos.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Health (Estado)** para supervisar el estado de los cortafuegos gestionados.

Vea **All Devices (Todos los dispositivos)** para acceder a una lista de todos los cortafuegos gestionados y las métricas de estado supervisadas. Seleccione un cortafuegos individual para

 ©2023 Palo Alto Networks, Inc.

ver la vista detallada de los dispositivos con gráficos con tendencias en el tiempo y tablas de las métricas supervisadas.

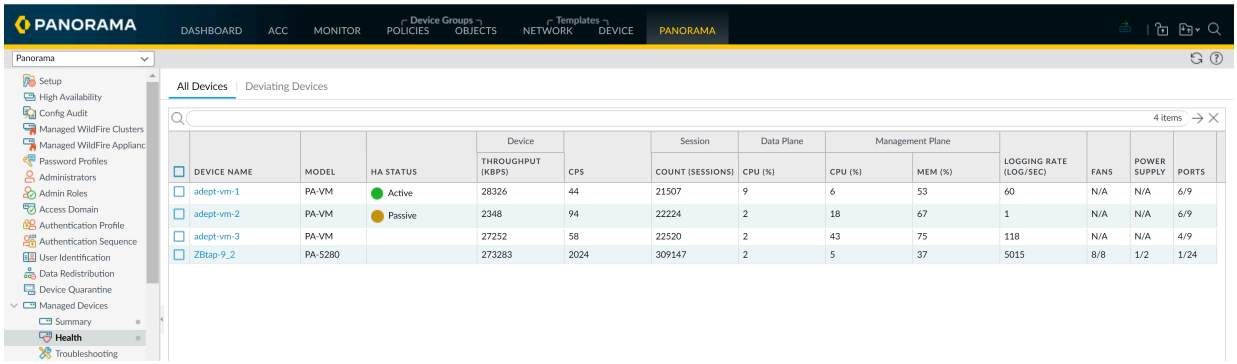


Figure 11: Supervisión de estado de los cortafuegos gestionados

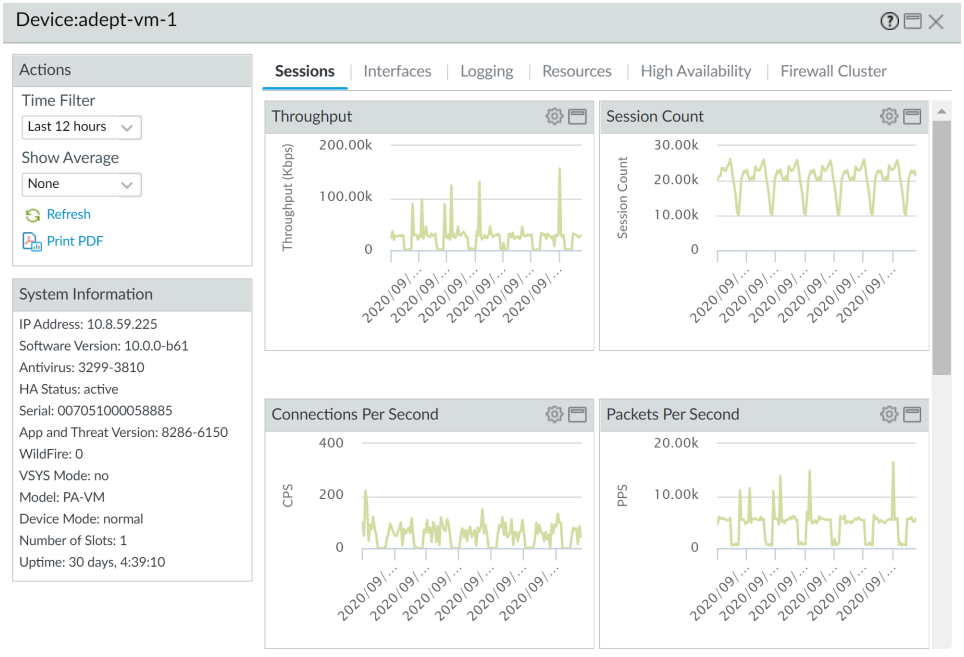
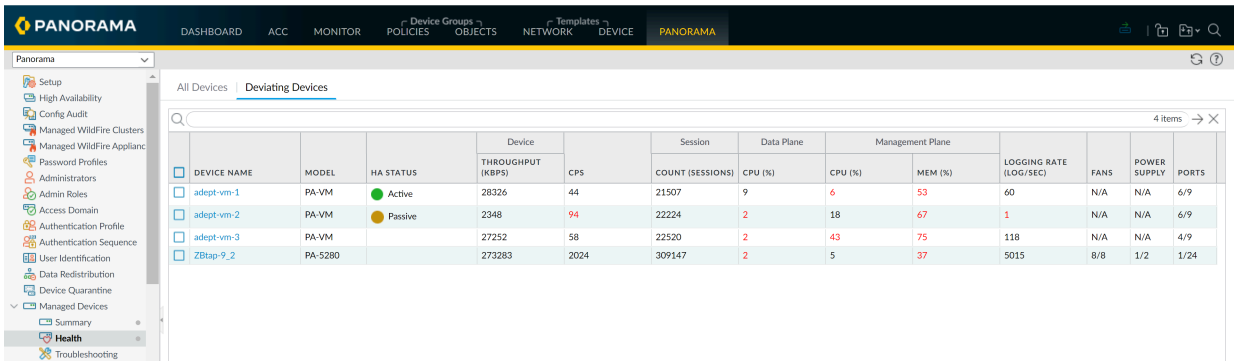


Figure 12: Vista detallada de los dispositivos

©2023 Palo Alto Networks, Inc.

STEP 3 | Seleccione **Deviating Devices (Dispositivos desviados)** para ver cortafuegos con métricas de estado que se desviaron de la referencia calculada.

Panorama muestra una lista de todos los cortafuegos que informan métricas que se desvían de la referencia calculada y muestra más métricas desviadas en rojo.



Supervisión de la utilización de las reglas de la política

Dado que sus políticas cambian, realizar un seguimiento de la utilización de las reglas en Panorama le ayuda a evaluar si la implementación de la política continúa adaptándose a sus necesidades de aplicación. Esta visibilidad le permite identificar y eliminar las reglas que no se utilizan para reducir los riesgos de seguridad y mantener la base de reglas de su política organizada. Además, el seguimiento de la utilización de las reglas le permite validar con rapidez adiciones de nuevas reglas y cambios de reglas, y supervisar la utilización de las reglas en las operaciones y las tareas de solución de problemas. En Panorama, puede consultar el uso de las reglas en los cortafuegos del grupo de dispositivos al que haya enviado las políticas para averiguar si hay coincidencias de tráfico en todos los cortafuegos, en algunos o en ninguno, en lugar de supervisar únicamente el número total de coincidencias en todos ellos. Filtre las reglas al instante según los datos de uso (por ejemplo, fecha de creación o fecha de modificación) del período que elija. La información acerca de la utilización de las reglas que se muestra permanece durante el reinicio, los reinicios en el plano de datos y las actualizaciones.

En Panorama, puede consultar los detalles sobre el uso de las reglas en los cortafuegos gestionados que ejecutan PAN-OS 8.1 o versiones posteriores, que tienen habilitado el recuento de resultados de las reglas de las políticas (que es la opción predeterminada) y a los que ha enviado las reglas de políticas definidas mediante grupos de dispositivos. Sin embargo, Panorama no puede recuperar los detalles relativos a las reglas configuradas en los cortafuegos de manera local; para consultarlos, debe iniciar sesión en el cortafuegos oportuno.

Después de filtrar su base de reglas de políticas, los administradores pueden tomar medidas para eliminar, deshabilitar, habilitar y etiquetar reglas de políticas directamente desde el optimizador de políticas. Por ejemplo, puede filtrar las reglas no utilizadas y, a continuación, etiquetarlas para su revisión con el fin de determinar si pueden eliminarse de forma segura o mantenerse en la base de reglas. Si se permite que los administradores actúen directamente desde el optimizador de políticas, se reducirá la sobrecarga de gestión necesaria, lo que contribuirá a simplificar la administración del ciclo de vida de las reglas y garantizar que sus cortafuegos no estén sobreaprovisionados.

Los datos de uso de las reglas de las políticas también resultan útiles cuando emplea** Policy Optimizer **(Optimizador de políticas) para priorizar las reglas que se deben migrar o limpiar en primer lugar.

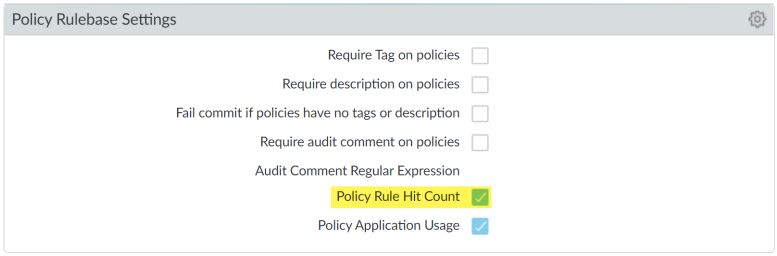
©2023 Palo Alto Networks, Inc.

Para ver la utilización de la reglas en reglas compartidas o un grupo de dispositivos específico:

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Verifique si está marcada la opción **Policy Rule Hit Count (Recuento de resultados de reglas de políticas)**.

1. Diríjase a Policy Rulebase Settings (Configuración de base de reglas de políticas) (**Panorama** > **Setup (Configuración)** > **Management (Gestión)**.
2. Verifique que **Policy Rule Hit Count (Recuento de resultados de reglas de políticas)** está marcada.



STEP 3 | Seleccione **Policies (Políticas)** > ***<policy rule>*** para ver una regla.

STEP 4 | Cambie el contexto de Device Group (Grupo de dispositivos) a **Shared (Compartido)** o al grupo de dispositivos específico que desea ver.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Determine si la regla se está utilizando (Rule Usage (Utilización de reglas)). El estado de utilización de las reglas de la política es uno de los siguientes:

Los cortafuegos deben ejecutan la versión PAN-OS 8.1 o posterior y la opción Policy Rule Hit Count (Conteo de resultados de reglas de la política) debe estar habilitada para que Panorama determine la utilización de las reglas.

- **Used (Utilizada):** cuando todos los cortafuegos en el grupo de dispositivos (al que envió la regla de la política) cuentan con coincidencias de tráfico para la regla de la política.
- **Partially Used (Utilizada parcialmente):** cuando algunos de los cortafuegos en el grupo de dispositivos (al que envió la regla de la política) cuentan con coincidencias de tráfico para la regla de la política.
- **Unused (No utilizada):** cuando ningún cortafuegos en el grupo de dispositivos (al que envió la regla de la política) cuenta con coincidencias de tráfico para la regla de la política.
- **Raya (—):** cuando ningún cortafuegos en el grupo de dispositivos (al que envió la regla de la política) posee la opción Policy Rule Hit Count (Conteo de resultados de reglas de la política) habilitada o disponible para que Panorama determine la utilización de la regla.
- **Modified (Fecha de modificación)**: fecha y hora de la última modificación de la regla de la política.
- **Modified (Fecha de creación)**: fecha y hora de creación de la regla de la política.

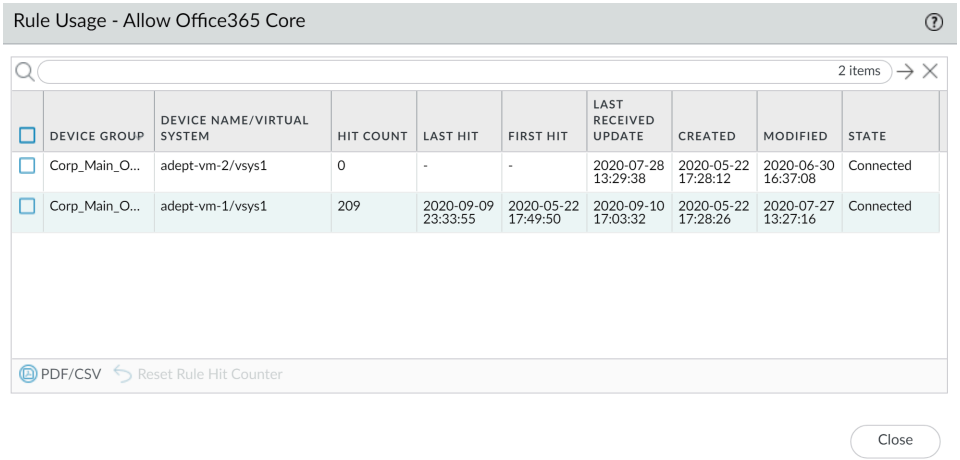


Si la regla se creó cuando Panorama ejecutaba PAN-OS 8.1 y estaba marcada la opción Policy Rule Hit Count (Recuento de resultados de reglas de políticas), se usa la fecha y la hora de First Hit (Primer resultado) en Created (Fecha de creación) al actualizar a PAN-OS 9.0 o versiones posteriores. Si la regla se creó cuando se utilizaba PAN-OS 8.1, pero dicha opción no estaba marcada, o si la regla se creó cuando Panorama ejecutaba PAN-OS 8.0 o una versión anterior, se usa en Created date (Fecha de creación) la fecha y la hora cuando se haya actualizado Panorama a PAN-OS 9.0 o versiones posteriores.

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

©2023 Palo Alto Networks, Inc.

STEP 6 | Haga clic en el estado de Rule Usage (Uso de reglas) para ver la lista de cortafuegos que utilizan la regla y los datos del conteo de resultados para el tráfico que coincida con la regla en cada cortafuegos.



STEP 7 | (Opcional) Vea los datos del conteo de resultados de la regla de la política para los cortafuegos individuales en el grupo de dispositivos.

1. Haga clic en **Preview Changes (Previsualizar los cambios)**.
2. Desde Device context (Contexto del dispositivo), seleccione el cortafuegos para ver sus datos de uso de reglas de la política.

STEP 8 | Seleccione **Policies (Políticas)** y, en el cuadro de diálogo Policy Optimizer (Optimizador de políticas), vea el filtro **Rule Usage (Uso de reglas)**.

STEP 9 | Filtre las reglas de la base seleccionada.

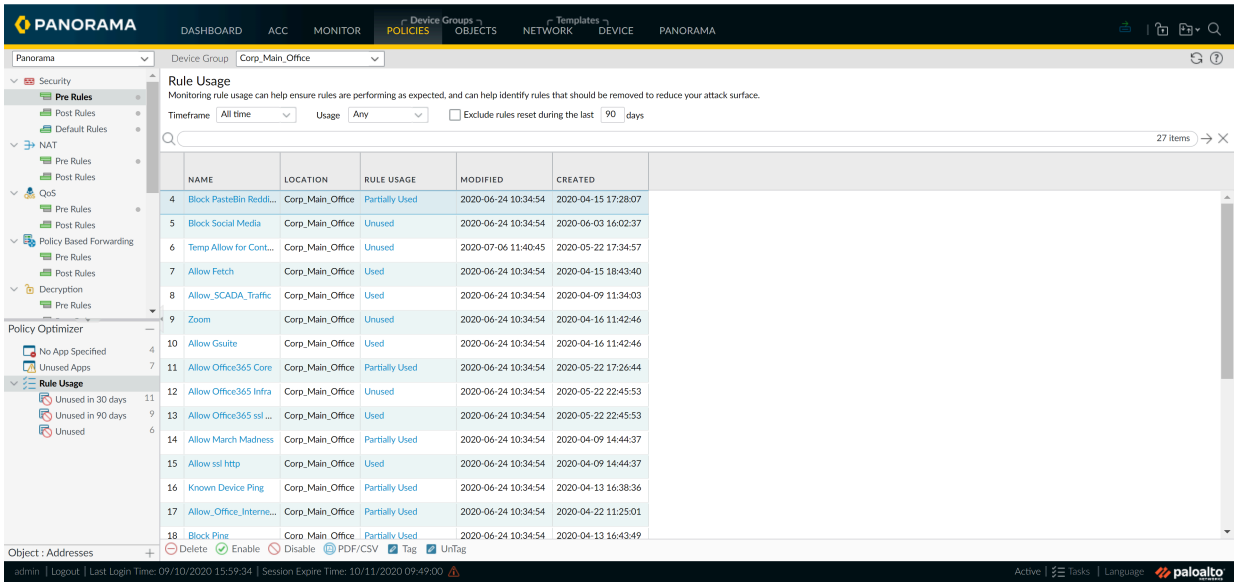
Puede filtrar el uso de las reglas enviadas a los cortafuegos desde Panorama, pero Panorama no puede filtrar el uso de las reglas configuradas en los cortafuegos de manera local.

Use el filtro de uso de las reglas para evaluar su utilización en el período especificado. Por ejemplo, filtre la base de reglas seleccionada por las reglas no utilizadas en los 30 últimos días. También puede evaluar la utilización de las reglas con otros atributos de reglas, como las fechas de creación y de modificación, que le permiten filtrar por el conjunto de reglas correcto que revisar. Estos datos resultan útiles para gestionar la vigencia de las reglas y para determinar si se deben eliminar a fin de reducir la superficie de ataque de la red.

1. Seleccione el **intervalo** por el que dese filtrar o especifique el intervalo **Custom (Personalizado)**.
2. Seleccione la regla **Usage (Uso)** en la que desee filtrar.
3. (Opcional) Si ha restablecido los datos de uso de reglas para cualquier regla, active **Exclude rules reset during the last <*number of days*> days (Excluir restablecimiento de reglas durante los últimos <número de días> días)** y decida cuándo excluir una regla en función

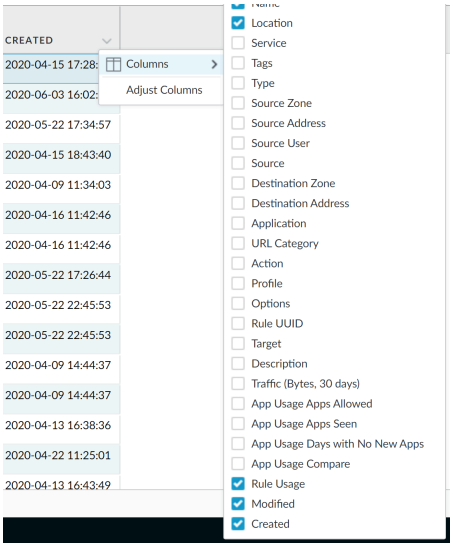
 ©2023 Palo Alto Networks, Inc.

del número de días que especifique desde que se restableció la regla. En los resultados filtrados se incluyen solo las reglas restablecidas antes del número de días especificado.



4. (Opcional) Especifique filtros de búsqueda basados en otros datos de las reglas, aparte del uso.

   1. Pase el ratón por el encabezado de las columnas y seleccione **Columns (Columnas)** en el menú desplegable.
   2. Añada cualquier otra columna que desee filtrar o visualizar.

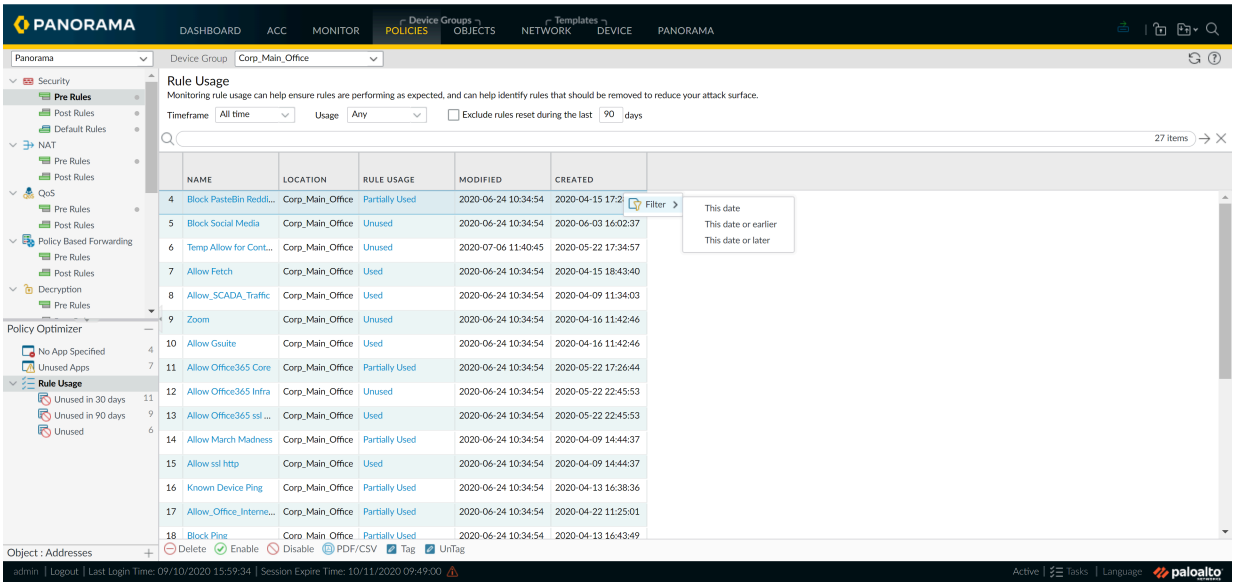


   3. Pase el ratón por los datos de la columna que desea filtrar y seleccione **Filter (Filtrar)** en el menú desplegable. Si los datos contienen fechas, seleccione la opción de filtro

©2023 Palo Alto Networks, Inc.

adecuada: **This date (Esta fecha)**, **This date or earlier (Esta fecha o una anterior)** o **This date or later (Esta fecha o una posterior)**.

4. Haga clic en **Apply Filter (Aplicar filtro)** (→).



STEP 10 | Actúe sobre una o más reglas de políticas no utilizadas.

1. Seleccione una o más reglas de políticas no utilizadas.
2. Lleve a cabo una de las siguientes acciones:
   - **Delete (Eliminar)**: permite eliminar una o más reglas de políticas seleccionadas.
   - **Enable (Habilitar)**: permite activar una o más reglas de políticas seleccionadas cuando están deshabilitadas.
   - **Disable (Deshabilitar)**: permite desactivar una o más reglas de políticas seleccionadas.
   - **Tag (Etiquetar)**: permite aplicar una o más etiquetas de grupo a una o más reglas de políticas seleccionadas. Para etiquetar la regla de políticas, la etiqueta de grupo ya debe existir.
   - **Untag (Desetiquetar)**: permite eliminar una o más etiquetas de grupo de una o más reglas de políticas seleccionadas.
3. Seleccione **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** los cambios.

©2023 Palo Alto Networks, Inc.

Caso de uso: Configuración de cortafuegos mediante Panorama

Supongamos que desea utilizar Panorama con una configuración de alta disponibilidad para gestionar doce cortafuegos de su red: tiene seis cortafuegos implementados en seis sucursales, un par de cortafuegos con una configuración de alta disponibilidad en cada uno de los dos centros de datos y un cortafuegos en cada una de las dos oficinas centrales regionales.

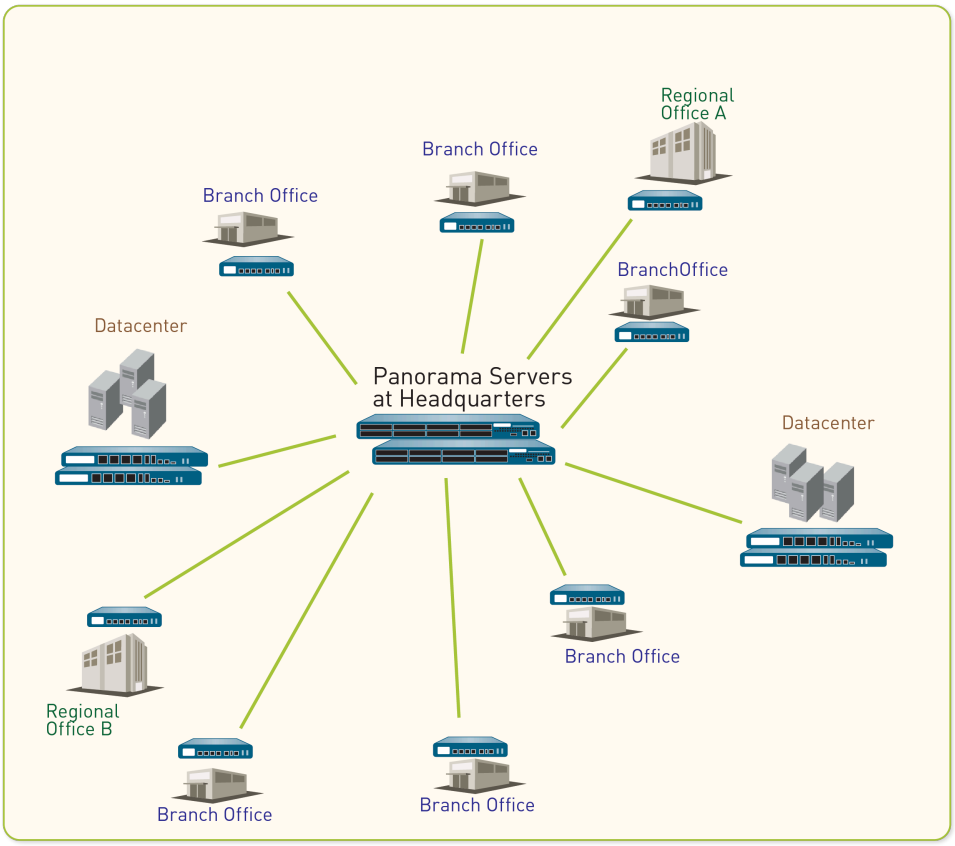


Figure 13: Ejemplo de distribución de cortafuegos

El primer paso para crear su estrategia de gestión central es determinar cómo agrupar los cortafuegos en grupos de dispositivos y plantillas para enviar configuraciones desde Panorama de manera eficiente. Puede basar el agrupamiento en las funciones comerciales, ubicaciones geográficas o dominios administrativos de los cortafuegos. En este ejemplo, puede crear dos grupos de dispositivos y tres plantillas para administrar los cortafuegos mediante Panorama:

- Grupos de dispositivos en este caso de uso
- Plantillas en este caso de uso
- Ajuste de políticas y configuración centralizadas

Grupos de dispositivos en este caso de uso

En Caso de uso: Configuración de cortafuegos mediante Panorama, necesitamos definir dos grupos de dispositivos basados en las funciones que realizarán los cortafuegos:

©2023 Palo Alto Networks, Inc.

- GD_SucursalYRegional para agrupar cortafuegos que sirvan de puertas de enlace de seguridad en las sucursales y las oficinas centrales regionales. Colocamos los cortafuegos de las sucursales y los cortafuegos de las oficinas regionales en el mismo grupo de cortafuegos porque los dispositivos con funciones parecidas requerirán bases de reglas de políticas similares.
- GD_CentroDeDatos para agrupar los cortafuegos que protegen los servidores en los centros de datos.

A continuación, podemos administrar las reglas de políticas compartidas entre ambos grupos de dispositivos y administrar las reglas de grupo de dispositivos distintas entre los grupos de oficinas regionales y sucursales. Para aumentar la flexibilidad, el administrador local de una oficina regional o sucursal puede crear reglas locales que coincidan con flujos de origen, destino y servicio específicos para acceder a aplicaciones y servicios necesarios para dicha oficina o sucursal. En este ejemplo, se creará la siguiente jerarquía para reglas de seguridad; puede utilizar un enfoque parecido para cualquiera de las otras bases de reglas:

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	**Regional**	**Branch**	**Datacenter**
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

Figure 14: Jerarquía de las reglas de seguridad

Plantillas en este caso de uso

Al agrupar cortafuegos para plantillas, debemos tener en cuenta las diferencias en la configuración de red. Por ejemplo, los cortafuegos deben incluirse en plantillas separadas si la configuración de interfaz no es la misma (las interfaces son distintas en cuanto a su tipo, las interfaces utilizadas no son iguales en el esquema de numeración y la capacidad de vinculación o las asignaciones de zona a interfaz son diferentes). Además, el modo en que se configuran los cortafuegos para acceder a los recursos de red puede ser diferente debido a que los cortafuegos están separados geográficamente; por ejemplo, el servidor DNS, los servidores Syslog y las puertas de enlace a los que acceden pueden ser diferentes. Por lo tanto, para lograr una configuración básica óptima, en Caso de uso: Configuración de cortafuegos mediante Panorama debemos colocar los cortafuegos en plantillas separadas, de la manera siguiente:

 ©2023 Palo Alto Networks, Inc.

- P_Sucursales para los cortafuegos de sucursales
- P_Regionales para los cortafuegos de oficinas regionales
- P_CentroDeDatos para los cortafuegos de centros de datos

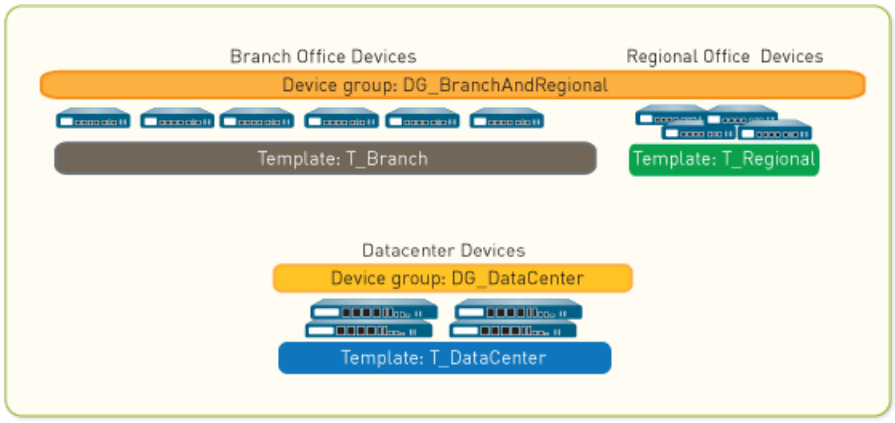


Figure 15: Ejemplo de grupo de dispositivos

Si tiene la intención de implementar sus cortafuegos en una configuración de HA activa/activa, asigne cada cortafuegos del par de HA a una plantilla separada. Al hacerlo logrará la flexibilidad necesaria para establecer configuraciones de red separadas para cada peer. Por ejemplo, puede gestionar las configuraciones de red en una plantilla separada para cada peer de modo que cada uno pueda conectarse a diferentes enrutadores hacia el norte y hacia el sur y pueda tener diferentes configuraciones de peer OSPF o BGP.

Ajuste de políticas y configuración centralizadas

En Caso de uso: Configuración de cortafuegos mediante Panorama, necesitaríamos llevar a cabo las siguientes tareas para implementar y gestionar cortafuegos de manera centralizada:

- Cómo añadir cortafuegos gestionados e implementar actualizaciones
- Uso de plantillas para administrar una configuración básica
- Uso de grupos de dispositivos para enviar reglas de políticas
- Vista previa de reglas y compilación de los cambios

Cómo añadir cortafuegos gestionados e implementar actualizaciones

La primera tarea en Caso de uso: Configuración de cortafuegos mediante Panorama es añadir los cortafuegos como dispositivos gestionados e implementar las actualizaciones de contenido y el software de PAN-OS en esos cortafuegos.

STEP 1 | Para cada cortafuegos que gestionará Panorama, Cómo añadir un cortafuegos como dispositivo gestionado.

En este ejemplo, añada 12 cortafuegos.

STEP 2 | Implemente las actualizaciones de contenido en los cortafuegos. Si ha adquirido una suscripción a la prevención de amenazas, tendrá a su disposición las bases de datos de contenido

 ©2023 Palo Alto Networks, Inc.

y antivirus. En primer lugar, instale la base de datos de **Applications (Aplicaciones)** o **Applications and Threats (Aplicaciones y amenazas)**, luego el **Antivirus**.

Para revisar el estado o el progreso de todas las tareas realizadas en Panorama, consulte Uso del gestor de tareas de Panorama.

1. Seleccione **Panorama** > **Device Deployment (Implementación de dispositivos)** > **Dynamic Updates (Actualizaciones dinámicas)**.
2. Haga clic en **Check Now (Comprobar ahora)** para comprobar la actualización más reciente. Si el valor de la columna Acción es **Download (Descargar)**, esto indica que hay una actualización disponible.
3. Haga clic en **Download (Descargar)**. Cuando se complete la descarga, el valor en la columna Action (Acción) cambia a **Install (Instalar)**.
4. En la columna **Action (Acción)**, haga clic en **Install (Instalar)**. Utilice los filtros o las etiquetas definidas por el usuario para seleccionar los cortafuegos gestionados en los que desee instalar esta actualización.
5. Haga clic en **OK (Aceptar)**; a continuación, supervise el estado, progreso y resultado de la actualización de contenido en cada cortafuegos. La columna **Result (Resultado)** muestra si la instalación es correcta o no.

STEP 3 | Implemente las actualizaciones de software en los cortafuegos.

1. Seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **Software**.
2. Haga clic en **Check Now (Comprobar ahora)** para comprobar la actualización más reciente. Si el valor de la columna Acción es **Download (Descargar)**, esto indica que hay una actualización disponible.
3. Localice la versión que necesita para cada modelo de hardware y, a continuación, haga clic en **Download (Descargar)**. Cuando se complete la descarga, el valor en la columna Action (Acción) cambia a **Install (Instalar)**.
4. En la columna Acción, haga clic en el enlace **Install (Instalar)**. Utilice los filtros o las etiquetas definidas por el usuario para seleccionar los cortafuegos gestionados en los que se instalará esta versión.
5. Marque la casilla de verificación para **Reboot device after install (Reiniciar dispositivo después de la instalación)** o **Upload only to device (do not install) (Cargar solamente en dispositivo [no instalar])** y haga clic en **OK (Aceptar)**. La columna **Results (Resultados)** muestra si la instalación es correcta o no.

Uso de plantillas para administrar una configuración básica

La segunda tarea en Caso de uso: Configuración de cortafuegos mediante Panorama sirve para crear las plantillas que necesitará para ingresar la configuración básica a los cortafuegos.

STEP 1 | Añada una plantilla para cada plantilla que utilizará, y asigne los cortafuegos adecuados a cada una.

En este ejemplo, cree plantillas con los nombres P_Sucursales, P_Regionales y P_CentroDeDatos.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Defina un servidor DNS, servidor NTP, servidor Syslog y titular de inicio de sesión. Repita este paso para cada plantilla.

1. En la pestaña **Device (Dispositivo)**, seleccione la **Template (Plantilla)** desde el menú desplegable.
2. Defina los servidores DNS y NTP:
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global (Global)** y edite los Servicios.
   2. En la pestaña **Services (Servicios)**, introduzca una dirección IP para **Primary DNS Server (Servidor DNS principal)**.

      *Para cualquier cortafuegos que tenga más de un sistema virtual (virtual system, vsys), añada un perfil de servidor DNS a cada plantilla para cada vsys (**Device [Dispositivo] > Server Profiles [Perfiles de servidor] > DNS**).*
   3. En la pestaña **NTP**, introduzca una dirección IP para **Primary NTP Server (Servidor NTP principal)**.
   4. Haga clic en **OK (Aceptar)** para guardar los cambios.
3. Añada un titular de inicio de sesión: seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, edite la configuración general, introduzca texto en **Login Banner (Titular de inicio de sesión)** y haga clic en **OK (Aceptar)**.
4. Configure un perfil de servidor Syslog (**Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Syslog**).

STEP 3 | Habilite el acceso HTTPS, SSH y SNMP a la interfaz de gestión de los cortafuegos gestionados. Repita este paso para cada plantilla.

1. En la pestaña **Device (Dispositivo)**, seleccione la **Template (Plantilla)** desde el menú desplegable.
2. Seleccione **Setup (Configuración)** > **Management (Gestión)** y edite Configuración de interfaz de gestión.
3. En Servicios, seleccione las casillas de verificación **HTTPS**, **SSH** y **SNMP** y haga clic en **OK (Aceptar)**.

STEP 4 | Cree un perfil de protección de zona para los cortafuegos en la plantilla del centro de datos (P_CentroDeDatos).

1. Seleccione la pestaña **Network (Red)** y, en el menú desplegable **Template (Plantilla)** seleccione P_CentroDeDatos.
2. Seleccione **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y haga clic en **Add (Añadir)**.
3. Para este ejemplo, se habilita la protección contra Inundación SYN: en la pestaña **Flood Protection (Protección contra inundaciones)**, seleccione la casilla de verificación **SYN**, defina la **Action (Acción)** como **SYN Cookies (Cookies SYN)**, defina **Alert (Alerta)** paquetes/seg. a **100**, defina **Activate (Activar)** paquetes/seg. en **1000** y defina **Maximum (Máximo)** paquetes/seg. en **10000**.
4. En este ejemplo, se habilitan las alertas: en la pestaña **Reconnaissance Protection (Protección de reconocimiento)**, seleccione las casillas de verificación **Enable (Habilitar)** para **TCP Port Scan (Examen de puerto TCP)**, **Host Sweep (Limpieza de host)** y **UDP Port**

 ©2023 Palo Alto Networks, Inc.

Scan (Examen de puerto de UDP). Compruebe que los valores de Acción estén definidos en **Alert (Alerta)** (el valor predeterminado).

5. Haga clic en **OK (Aceptar)** para guardar el perfil de protección de zona.

STEP 5 | Configure la interfaz y la configuración de zona en la plantilla del centro de datos (P_CentroDeDatos) y, a continuación, incluya el perfil de protección de zona que acaba de crear.

Antes de realizar este paso, debe haber configurado las interfaces de manera local en los cortafuegos. Como mínimo, para cada interfaz, debe haber definido el tipo de interfaz, haberla asignado a un enrutador virtual, si es necesario, y haber incluido una zona de seguridad.

1. Seleccione la pestaña **Network (Red)** y, en el menú desplegable **Template (Plantilla)** seleccione P_CentroDeDatos.
2. Seleccione **Network (Red)** > **Interface (Interfaz)** y, en la columna Interfaz, haga clic en el nombre de la interfaz.
3. Seleccione el **Interface Type (Tipo de interfaz)** en la lista desplegable.
4. En el menú desplegable **Virtual Router (Enrutador virtual)**, haga clic en **New Virtual Router (Nuevo enrutador virtual)**. Al definir el enrutador, compruebe que el **Name (Nombre)** coincide con el definido en el cortafuegos.
5. En el menú desplegable **Security Zone (Zona de seguridad)**, haga clic en **New Zone (Nueva zona)**. Al definir la zona, compruebe que el **Name (Nombre)** coincide con el definido en el cortafuegos.
6. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
7. Seleccione **Network (Red)** > **Zones (Zonas)**, y seleccione la zona que acaba de crear. Verifique que se ha adjuntado la interfaz correcta a la zona.
8. En el menú desplegable **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil que creó y haga clic en **OK (Aceptar)**.

STEP 6 | Envíe los cambios de plantilla.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Templates (Plantillas)** y seleccione los cortafuegos asignados a las plantillas donde realizó los cambios.
3. Seleccione **Commit and Push (Confirmar y enviar)** para enviar sus cambios a la configuración de Panorama y a la plantilla.

Uso de grupos de dispositivos para enviar reglas de políticas

La tercera tarea en Caso de uso: Configuración de cortafuegos mediante Panorama es crear los grupos de dispositivos para gestionar reglas de política en los cortafuegos.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Cree grupos de dispositivos y asigne los cortafuegos adecuados a cada grupo de dispositivos: consulte Cómo añadir un grupo de dispositivos.

En este ejemplo, cree grupos de dispositivos con el nombre GD_SucursalYRegional y GD_CentrosDeDatos.

Al configurar el grupo de dispositivos GD_SucursalYRegional, debe asignar un cortafuegos **Master (Maestro)**. Este es el único cortafuegos del grupo de dispositivos que recopila información de asignación de usuarios y grupos para la evaluación de políticas.

STEP 2 | Cree una regla previa compartida para permitir servicios de DNS y SNMP.

1. Cree un grupo de aplicaciones compartido para los servicios de DNS y SNMP.
    1. Seleccione **Objects (Objetos)** > **Application Group (Grupo de aplicaciones)** y haga clic en **Add (Añadir)**.
    2. Introduzca un nombre en **Name (Nombre)** y seleccione la casilla de verificación **Shared (Compartido)** para crear un objeto de grupo de aplicación compartida.
    3. Haga clic en **Add (Añadir)**, escriba **DNS** y seleccione **dns** en la lista. Repita la operación para SNMP y seleccione **snmp**, **snmp-trap**.
    4. Haga clic en **OK (Aceptar)** para crear el grupo de aplicaciones.
2. Cree la regla compartida.
    1. Seleccione la pestaña **Policies (Políticas)** y en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione **Shared (Compartido)**.
    2. Seleccione la base de reglas **Security (Seguridad)** > **Pre-Rules (Reglas previas)**.
    3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para la regla de seguridad.
    4. En las pestañas **Source (Origen)** y **Destination (Destino)** de la regla, haga clic en **Add (Añadir)** e introduzca una **Source Zone (Zona de origen)** y una **Destination Zone (Zona de destino)** para el tráfico.
    5. En la pestaña **Applications (Aplicaciones)**, haga clic en **Add (Añadir)**, escriba el nombre del objeto de grupo de aplicaciones que acaba de crear y selecciónelo en el menú desplegable.
    6. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como **Allow (Permitir)** y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Defina la política de uso aceptable corporativa para todas las oficinas. En este ejemplo, se creará una regla compartida que restrinja el acceso a algunas categorías de URL y niegue el acceso al tráfico punto a punto con un nivel de riesgo 3, 4 o 5.

1. Seleccione la pestaña **Policies (Políticas)** y en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione **Shared (Compartido)**.
2. Seleccione **Security (Seguridad)** > **Pre-Rules (Reglas previas)** y haga clic en **Add (Añadir)**.
3. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla de seguridad.
4. En las pestañas **Source (Origen)** y **Destination (Destino)**, haga clic en **Add (Añadir)** y seleccione **any (cualquiera)** para el tráfico **Source Zone (Zona de origen)** y **Destination Zone (Zona de destino)**.
5. En la pestaña **Application (Aplicación)**, defina el filtro de la aplicación.
   1. Haga clic en **Add (Añadir)** y en **New Application Filter (Nuevo filtro de aplicación)** en el pie de página del menú desplegable.
   2. Introduzca un **Name (Nombre)** y seleccione la casilla de verificación **Shared (Compartido)**.
   3. En la columna Riesgo, seleccione los niveles **3**, **4** y **5**.
   4. En la columna Tecnología, seleccione **peer-to-peer (punto a punto)**.
   5. Haga clic en **OK (Aceptar)** para guardar el nuevo filtro.
6. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, en la sección Categoría de URL, haga clic en **Add (Añadir)** y seleccione las categorías que desearía bloquear (por ejemplo, **streaming-media [archivos multimedia en secuencia]**, **dating [fechas]** y **online-personal-storage [almacenamiento personal en línea]**).
7. También puede incluir el perfil de filtrado de URL predeterminado: en la pestaña **Actions (Acciones)**, sección Ajuste de perfil, seleccione la opción de **Profile Type (Tipo de perfil) Profiles (Perfiles)**, y seleccione la opción de **URL Filtering (Filtrado de URL) default (predeterminado)**.
8. Haga clic en **OK (Aceptar)** para guardar la regla previa de seguridad.

©2023 Palo Alto Networks, Inc.

STEP 4 | Permite conectarse a través de Facebook con todos los usuarios del grupo de marketing únicamente en las oficinas regionales.

Habilitar una regla de seguridad basada en usuarios y grupos tiene las siguientes tareas de requisitos previos:

- Configure el ID de usuario en los cortafuegos.
- Habilite el ID de usuario para cada zona que contenga los usuarios que desea identificar.
- Defina un cortafuegos maestro para el grupo de dispositivos DG_BranchAndRegional (consulte paso 1).

1. Seleccione la pestaña **Policies (Políticas)** y, en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione GD_SucursalYRegional.
2. Seleccione la base de reglas **Security (Seguridad)** > **Pre-Rules (Reglas previas)**.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para la regla de seguridad.
4. En la pestaña **Source (Origen)**, haga clic en **Add (Añadir)** para añadir la zona de origen que contiene los usuarios del grupo de marketing.
5. En la pestaña **Destination (Destino)**, seleccione **Add (Añadir)** para añadir la zona de destino.
6. En la pestaña **User (Usuario)**, haga clic en **Add (Añadir)** para añadir el grupo de usuarios de marketing a la lista Usuario de origen.
7. En la pestaña **Application (Aplicación)**, haga clic en **Add (Añadir)**, escriba **Facebook** y, a continuación, selecciónelo en el menú desplegable.
8. En la pestaña **Action (Acción)**, establezca **Action (Acción)** como **Allow (Permitir)**.
9. En la pestaña **Target (Destino)**, seleccione los cortafuegos de oficinas regionales y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Permite el acceso a la aplicación en la nube de Amazon para los hosts/servidores especificados del centro de datos.

1. Cree un objeto de direcciones para los servidores/hosts del centro de datos que necesitan acceder a la aplicación en la nube de Amazon.
   1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione GD_CentroDeDatos.
   2. Haga clic en **Add (Añadir)** e introduzca un nombre en **Name (Nombre)** para el objeto de direcciones.
   3. Seleccione **Type (Tipo)**, y especifique una dirección IP y máscara de red (**IP Netmask [Máscara de red de IP]**), el rango de direcciones IP (**IP Range [Rango de IP]**) o **FQDN**.
   4. Haga clic en **OK (Aceptar)** para guardar el objeto.
2. Cree una regla de seguridad que permita acceder a la aplicación en la nube de Amazon.
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre-Rules (Reglas previas)** y en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione GD_CentroDeDatos.
   2. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para la regla de seguridad.
   3. Seleccione la pestaña **Source (Origen)**, haga clic en **Add (Añadir)** para añadir la zona de rigen del centro de datos y en **Add (Añadir)** para añadir el objeto de dirección (dirección de origen) que acaba de definir.
   4. Seleccione la pestaña **Destination (Destino)** y haga clic en **Add (Añadir)** para añadir la zona de destino.
   5. Seleccione la pestaña **Application (Aplicación)**, haga clic en **Add (Añadir)**, escriba **`amazon`** y seleccione las aplicaciones de Amazon de la lista.
   6. Seleccione la pestaña **Action (Acción)**, establezca **Action (Acción)** como **Allow (Permitir)**.
   7. Haga clic en **OK (Aceptar)** para guardar la regla.

STEP 6 | Para habilitar el registro de todo el tráfico de internet en su red, cree una regla que haga coincidir la zona fiable con la zona no fiable.

1. Seleccione la pestaña **Policies (Políticas)** y en el menú desplegable **Device Group (Grupo de dispositivos)**, seleccione **Shared (Compartido)**.
2. Seleccione la base de reglas **Security (Seguridad)** > **Pre-Rules (Reglas previas)**.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para la regla de seguridad.
4. En las pestañas **Source (Origen)** y **Destination (Destino)** de la regla, haga clic en **Add (Añadir)** para añadir **`trust_zone`** como la zona de origen y **`untrust_zone`** como la zona de destino.
5. En la pestaña **Action (Acción)**, defina la **Action (Acción)** en **Deny (Denegar)**, defina el **Log Setting (Configuración de log)** en **Log at Session end (Log al finalizar sesión)** y haga clic **OK (Aceptar)**.

Vista previa de reglas y compilación de los cambios

La tarea final en Caso de uso: Configuración de cortafuegos mediante Panorama es revisar las reglas y confirmar los cambios que ha realizado en Panorama, los grupos de dispositivos y las plantillas.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Vista previa de las reglas.

Esta vista previa le permite evaluar visualmente de qué modo se organizan las reglas por capas para una base de reglas específica.

1. Seleccione **Policies (Políticas)** y **Preview Rules (Reglas de vista previa)**.
2. Seleccione un **Rulebase (Base de reglas)**, **Device Group (Grupo de dispositivos)**y **Device (Dispositivo)**.
3. Cierre el cuadro de diálogo de vista previa cuando termine.

STEP 2 | Confirme y envíe sus cambios de configuración.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos que ha añadido y seleccione **Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 3 | Verifique que Panorama aplicó la configuración de la plantilla y la política.

1. En el encabezado de Panorama, configure el **Context (Contexto)** en el cortafuegos para acceder a su interfaz web.
2. Revise la plantilla y la configuración de las políticas para asegurarse de que los cambios se hayan realizado.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Gestión de la recopilación de logs

Todos los cortafuegos de Palo Alto Networks pueden generar logs que ofrecen un seguimiento auditado de las actividades del cortafuegos. Para la Creación centralizada de logs e informes, debe reenviar los logs generados en los cortafuegos a la infraestructura en sus instalaciones que incluya el servidor de gestión de Panorama™ o los recopiladores de logs, o enviar los logs a Cortex Data Lake basado en la nube. Opcionalmente, puede configurar Panorama para reenviar los logs a destinos de log externos (como servidores syslog).

Si reenvía logs a un dispositivo virtual Panorama en modo heredado, no necesita realizar ninguna tarea adicional para habilitar el logging. Si reenvía los logs a los recopiladores de logs, debe configurarlos como recopiladores gestionados y asignarlos a los grupos de recopiladores. Un recopilador gestionado puede ser local en un dispositivo virtual serie M o en un dispositivo virtual Panorama en modo Panorama. Además, un dispositivo serie M o un dispositivo virtual Panorama en modo de recopilador de logs puede ser un recopilador de logs dedicado. Para determinar si debe implementar una opción o la otra, o ambos tipos de recopiladores gestionados, consulte Recopilación de logs local y distribuida.

Para gestionar los logs de sistema y configuración que Panorama genera de manera local, consulte Supervisión de Panorama.

- Configuración de recopiladores gestionados
- Supervisión del estado del recopilador gestionado
- Configuración de la autenticación para un recopilador de logs dedicado
- Gestión de grupos de recopiladores
- Configuración del reenvío de logs a Panorama
- Configuración del reenvío de syslog a destinos externos
- Reenvío de logs a Cortex Data Lake
- Comprobación del reenvío de logs a Panorama
- Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs
- Configuración del reenvío de logs desde Panorama a destinos externos
- Implementaciones de recopilación de logs

Configuración de recopiladores gestionados

Para habilitar el servidor de gestión de Panorama para que gestione un recopilador de logs, debe añadirlo como recopilador gestionado. Los recopiladores de logs admiten la comunicación mediante una dirección IPv4 o IPv6 pública o privada únicamente, incluso cuando configura certificados personalizados para la autenticación mutua.

Puede añadir dos tipos de recopiladores gestionados:

- **Recopilador de logs dedicado**: para configurar un nuevo dispositivo M-700, M-600, M-500, M-300 o M-200, o un dispositivo virtual Panorama como recopilador de logs o cambiar un dispositivo M-Series o un dispositivo virtual Panorama existente del modo Panorama al modo de recopilador de logs, consulte Configuración del dispositivo M-Series como un recopilador de logs. Tenga en cuenta que el cambio del modo Panorama al modo Recopilador de logs elimina el recopilador de logs local que está predefinido en el dispositivo M-Series en modo Panorama.
- **Recopilador de logs local**: un recopilador de logs puede ejecutarse localmente en el dispositivo M-700, M-600, M-500, M-300 o M-200, o dispositivo virtual Panorama en modo Panorama. El Recopilador de logs viene predeterminado en los dispositivos M-Series; en el dispositivo virtual, debe añadir el Recopilador de logs. Cuando el servidor de gestión de Panorama tiene una configuración de alta disponibilidad (high availability, HA), cada peer de HA puede tener un recopilador de logs local. Sin embargo, en relación con el Panorama principal, el Recopilador de logs en el Panorama secundario es remoto, no local. Por lo tanto, para usar Recopilador de logs en el Panorama secundario, debe añadirlo manualmente al Panorama principal (para más detalles, consulte Implementación de dispositivos M-Series de Panorama con recopiladores de logs locales o Implementación de dispositivos virtuales Panorama con recopiladores de logs locales). Si elimina un Recopilador de logs local, puede volver a añadirlo más adelante. Los siguientes pasos describen cómo añadir un Recopilador de logs local.

Si el dispositivo virtual Panorama está en modo heredado, debe cambiar al modo Panorama para crear un recopilador de logs. Para obtener más detalles, consulte Configuración del dispositivo virtual Panorama con recopiladores de logs locales.

Se utiliza una clave de autenticación de registro de dispositivo para autenticar y conectar de forma segura el servidor de gestión Panorama y el recopilador gestionado en la primera conexión. Para configurar la clave de autenticación de registro de dispositivo, especifique la duración de la clave y la cantidad de veces que puede utilizar la clave de autenticación para incorporar nuevos recopiladores de logs. Además, puede especificar uno o más números de serie del recopilador de logs para los que la clave de autenticación es válida.

La clave de autenticación caduca 90 días después de que caduque la vida útil de la clave. Después de 90 días, se le pedirá que vuelva a certificar la clave de autenticación para mantener su validez. Si no la vuelve a certificar, la clave de autenticación no será válida. Se genera un log del sistema cada vez que un recopilador de logs utiliza la clave de autenticación generada por Panorama. El recopilador de logs utiliza la clave de autenticación para autenticar Panorama cuando entrega el certificado del dispositivo que se utiliza para todas las comunicaciones posteriores.

Se recomienda conservar un recopilador de logs local y un grupo de recopiladores en el servidor de gestión Panorama, independientemente de si gestiona recopiladores de logs dedicados.

©2023 Palo Alto Networks, Inc.

(Solo para la evaluación de Panorama) Si está evaluando un dispositivo virtual Panorama con un recopilador de logs local, Configuración del reenvío de logs desde Panorama a destinos externos *para conservar los logs generados durante el período de evaluación.*

Los logs almacenados en el recopilador de logs local no se pueden conservar cuando convierte la instancia de evaluación de Panorama en una instancia de producción de Panorama *con un recopilador de logs local.*

(PAN-OS 10.2 solo) Para recopiladores de logs dedicados que ejecutan una versión PAN-OS 10.1, Panorama que ejecuta PAN-OS 10.2 o una versión posterior admite recopiladores de logs dedicados de incorporación que ejecutan PAN-OS 10.1.3 o una versión posterior solamente. No puede añadir un recopilador de logs dedicado que ejecute PAN-OS 10.1.2 o una versión anterior de PAN-OS 10.1 a la gestión de Panorama si Panorama ejecuta PAN-OS 10.2 o una versión posterior.

Panorama admite recopiladores de logs dedicados de incorporación que ejecutan las siguientes versiones:

- ***Panorama que ejecuta PAN-OS 10.2 o una versión posterior**: recopiladores de logs dedicados que ejecutan PAN-OS 10.1.3 o una versión posterior, y recopiladores de logs dedicados con PAN-OS 10.0 o una versión anterior de PAN-OS.*

No hay impacto en los recopiladores de logs dedicados que ya gestiona Panorama en la actualización a PAN-OS 10.2.

STEP 1 | Registro del número de serie del recopilador de logs.

Necesitará el número de serie cuando agregue el recopilador de logs como recopilador gestionado.

1. Acceda a la interfaz web de Panorama.
2. Seleccione **Dashboard (Panel)** y registre el **Serial # (Número de serie)** en la sección de Información general.

STEP 2 | Inicio de sesión en la interfaz web de Panorama.

STEP 3 | Cree una clave de autenticación de registro de dispositivo.

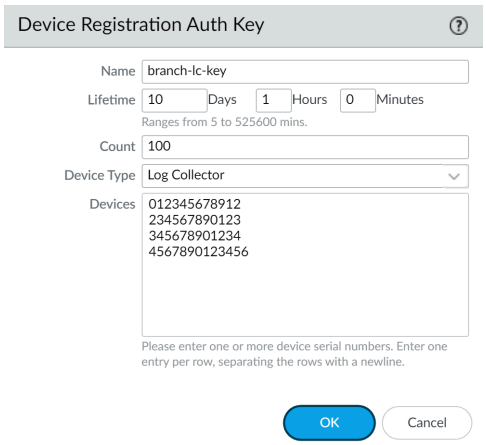
1. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.
2. Configure la clave de autenticación.
   - **Name (Nombre)**: agregue un nombre descriptivo para la clave de autenticación.
   - **Lifetime (Duración)**: especifique la duración de la clave a fin de indicar durante cuánto tiempo puede utilizar la clave de autenticación para incorporar nuevos recopiladores de logs.
   - **Count (Conteo)**: especifique cuántas veces puede utilizar la clave de autenticación para incorporar nuevos recopiladores de logs.
   - **Device Type (Tipo de dispositivo)**: especifique que esta clave de autenticación se utiliza para autenticar solo un **recopilador de logs**.

 ©2023 Palo Alto Networks, Inc.

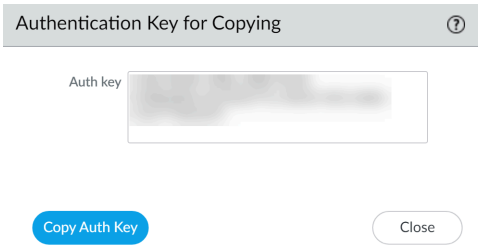
*Puede seleccionar **Any (Cualquiera)** para utilizar la clave de autenticación de registro de dispositivos para incorporar cortafuegos, recopiladores de logs y dispositivos WildFire.*

- (Opcional) **Devices (Dispositivos)**: introduzca uno o más números de serie de dispositivo para especificar para qué recopiladores de logs es válida la clave de autenticación.

3. Haga clic en **OK (Aceptar)**.



4. Seleccione **Copy Auth Key (Copiar la clave de autenticación)** y **Close (Cerrar)**.



STEP 4 | (solo para el recopilador de logs dedicado) Añada la clave de autenticación de registro de dispositivos al recopilador de logs.

Añada la clave de autenticación de registro del dispositivo solo a un recopilador de logs dedicado. Un dispositivo Panorama en modo Panorama no necesita autenticar su propio recopilador de logs local.

1. Inicie sesión en la CLI del recopilador de logs.
2. Añada la clave de autenticación de registro del dispositivo.

```
admin> request authkey set <auth-key>
```



STEP 5 | Añada el recopilador de logs como recopilador gestionado.

1. En la interfaz web de Panorama, seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y **Add (Añadir)** para añadir un nuevo recopilador de logs.
2. En la configuración **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el recopilador de logs.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 6 | (Opcional) Configure la autenticación de administración del recopilador de logs.

*Palo Alto Networks recomienda añadir al menos un administrador local con privilegios de superusuario para la **autenticación** si configura una lista de autorización para su recopilador gestionado.*

Si añadió usuarios administradores de Panorama importados, debe añadir al menos un administrador local con privilegios de superusuario.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en el nombre del recopilador de logs para editarlo.
2. Configure la contraseña de administración del recopilador de logs:
   1. Seleccione el modo en **Mode (Modo)**.
   2. Si selecciona el modo **Password (Contraseña)**, introdúzcala en texto sin formato en **Password (Contraseña)** y en **Confirm Password (Confirmar contraseña)**. Si selecciona el modo **Password Hash (Hash de contraseña)**, introduzca una cadena con hash de 63 caracteres como máximo.
3. Configure los requisitos de seguridad para el inicio de sesión como administrador:

   *Si configura cualquier valor distinto de 0 en **Failed Attempts (Intentos fallidos)**, pero deja 0 en **Lockout Time (Tiempo de bloqueo)**, se bloqueado al usuario administrativo por tiempo indefinido hasta que otro administrador lo desbloquee manualmente. Si no ha creado ningún otro administrador, debe volver a configurar los ajustes **Failed Attempts (Intentos fallidos)** y **Lockout Time (Tiempo de bloqueo)** en Panorama y enviar el cambio en la configuración al recopilador de logs. Para garantizar que nunca se bloquee al administrador, mantenga el valor predeterminado de 0 tanto en **Failed Attempts (Intentos fallidos)** como en **Lockout Time (Tiempo de bloqueo)**.*

   1. Introduzca el número oportuno de inicios de sesión en **Failed Attempts (Intentos fallidos)**. El intervalo va de **0** a **10**, donde el valor predeterminado **0** especifica un número ilimitado de intentos.
   2. En **Lockout Time (Tiempo de bloqueo)**, introduzca un valor entre **0** (predeterminado) y **60** minutos.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Habilite los discos de registro.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en el nombre del recopilador de logs para editarlo.

   El nombre de Recopilador de logs tiene el mismo valor que el nombre de host del servidor de gestión de Panorama.
2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada par de discos.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 8 | (Opcional) Si su implementación utiliza certificados personalizados para la autenticación entre Panorama y los dispositivos gestionados, implemente el certificado de dispositivo cliente personalizado. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y elija el perfil del certificado del menú desplegable o haga clic en **New Certificate Profile (Nuevo perfil de certificado)** para crear uno.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir un nuevo recopilador de logs o seleccionar uno existente. Seleccione **Communication (Comunicación)**.
3. Seleccione el tipo de certificado de dispositivo en el menú desplegable Tipo.
   - Si está utilizando un certificado de dispositivo local, seleccione **Certificate (Certificado)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
   - Si está utilizando SCEP como certificado del dispositivo, seleccione el **SCEP Profile (Perfil de SCEP)** y **Certificate Profile (Perfil del certificado)** de los respectivos menús desplegables.
4. Haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | (Opcional) Configure **Secure Server Communication (Comunicación segura con servidor)** en el recopilador de logs. Para más información, consulte Configuración de la autenticación mediante la utilización de certificados personalizados.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (añadir)**. Seleccione **Communication (Comunicación)**.
2. Verifique que la casilla de verificación **Custom Certificate Only (Certificado personalizado únicamente)** no está seleccionada. Esto le permite continuar gestionando todos los dispositivos mientras migra a certificados personalizados.

   Cuando se selecciona la casilla de verificación Certificado personalizado únicamente, el Recopilador de logs no se autentica y no puede recibir logs de dispositivos que usan certificados predefinidos.
3. Seleccione el perfil del servicio SSL/TLS del menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre el recopilador de logs y los dispositivos que le envían los logs.
4. Seleccione el perfil de certificado del menú desplegable **Certificate Profile (Perfil del certificado)**.
5. Seleccione **Authorize Client Based on Serial Number (Autorizar clientes según el número de serie)** para hacer que el servidor compruebe los clientes contra los números de serie de los dispositivos gestionados. El certificado de cliente debe tener la palabra clave especial $UDID establecida como CN para autorizar según los números de serie.
6. En **Disconnect Wait Time (min) [Tiempo de espera de desconexión (min)]**, introduzca el número de minutos que Panorama debería esperar antes de terminar y volver a establecer la conexión actual con sus dispositivos gestionados. Este campo está en blanco por defecto y el rango es de 0 a 44,640 minutos.

   El tiempo de espera de desconexión no comienza la cuenta atrás hasta que confirme la nueva configuración.
7. (Opcional) Configure una lista de autorizaciones.
   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Seleccione el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** como el tipo de Identificador.
   3. Especifique un identificador del tipo seleccionado.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Check Authorization List (Comprobar lista de autorización)** para que el recopilador de logs aplique la lista de autorización.
8. Haga clic en **OK (Aceptar)**.
9. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 10 | Verifique los cambios.

1. Verifique que la página **Panorama** > **Managed Collectors (Recopiladores gestionados)** detalle los recopiladores de logs que añadió. La columna Conectado muestra un icono de marca de verificación para indicar que el recopilador de logs está conectado a Panorama. Es

 ©2023 Palo Alto Networks, Inc.

posible que deba esperar unos minutos para que la página muestre el estado de conexión actualizado.

> ***Hasta que realice el procedimiento*** Configuración de un grupo de recopiladores ***y envíe los cambios en la configuración al grupo de recopiladores, la columna Configuration Status (Estado de configuración) muestra Out of Sync (Sin sincronización); la columna Run Time Status (Estado de tiempo de ejecución), disconnected (desconectado); y el comando de la interfaz de línea de comandos (command-line interface, CLI)*** `show interface all`***, down*** `(inactivas)` ***para las interfaces.***

2. Haga clic en **Statistics (Estadísticas)** en la última columna para verificar que los discos de logs están habilitados.

STEP 11 | Pasos siguientes:

Para que un recopilador de logs pueda recibir logs de cortafuegos, debe realizar lo siguiente:

1. Configure el reenvío de logs a Panorama.
2. Configuración de un grupo de recopiladoresLos dispositivos M-Series tienen predefinido un grupo de recopiladores predeterminado que ya incluye como miembro al recopilador de logs local. En el dispositivo virtual Panorama, debe añadir el grupo de recopiladores y añadir el recopilador de logs local como miembro. En ambos modelos, asigne cortafuegos al Recopilador de logs local para el reenvío de logs.
3. Supervisión del estado del recopilador gestionado para identificar y resolver problemas que afecten la recopilación de logs en caso de que surjan.

 ©2023 Palo Alto Networks, Inc.

Supervisión del estado del recopilador gestionado

Supervise el estado del recopilador de logs gestionado para identificar y resolver los problemas que afectan a la recopilación de logs. El estado del recopilador de logs se basa en el estado de los procesos vitales del recopilador de logs y puede ver tanto el estado general como el estado de cada proceso de recopilación de logs.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de recopiladores gestionados.

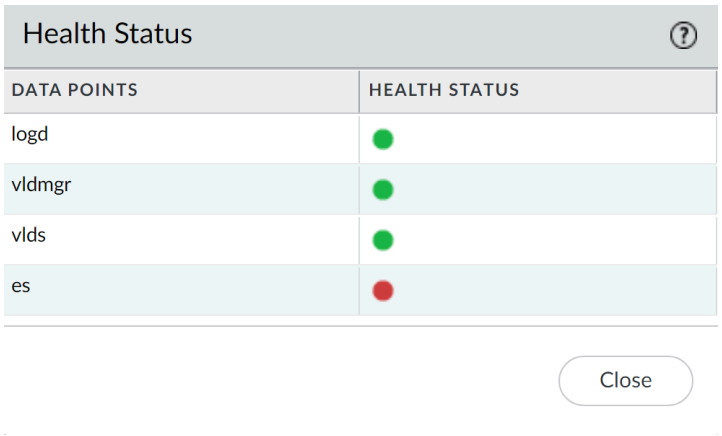
STEP 3 | Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y vaya a la columna Health (Estado).

STEP 4 | Revise el estado general del recopilador de logs.

Un círculo verde (●) indica que el recopilador de logs está en buen estado y un círculo rojo (●) indica que uno o más procesos de recopilación de logs están experimentando una degradación.

STEP 5 | Vea los **detalles del estado** para ver el estado de cada proceso de recopilación de logs.

- **logd:** proceso responsable de ingerir los logs recibidos del cortafuegos administrado y de transferir los logs ingeridos a vldmgr.
- **vldmgr:** proceso responsable de administrar los procesos vld.
- **vlds:** proceso responsable de administrar los discos de creación de logs individuales, escribir logs en los discos de creación de logs e incorporar logs en ElasticSearch.
- **es:** proceso de ElasticSearch que se ejecuta en el recopilador de logs.



 ©2023 Palo Alto Networks, Inc.

Configuración de la autenticación para un recopilador de logs dedicado

Cree y configure la autenticación mejorada para su recopilador de logs dedicado. Para ello, configure usuarios administrativos locales con parámetros de autenticación detallados y aproveche RADIUS, TACAS + o LDAP para la autorización y autenticación.

Cuando se configura y envía administradores desde Panorama, se sobrescriben los administradores existentes en los recopiladores de logs dedicados por los que configure en Panorama.

- Configuración de una cuenta administrativa para un recopilador de logs dedicado
- Configuración de la autenticación RADIUS para un recopilador de logs dedicado
- Configuración de la autenticación TACACS+ para un recopilador de logs dedicado
- Configuración de la autenticación LDAP para un recopilador de logs dedicado

Configuración de una cuenta administrativa para un recopilador de logs dedicado

Cree uno o más administradores con parámetros de autenticación detallados para que su recopilador de logs dedicado los administre desde el servidor de gestión Panorama™. Además, puede configurar administradores locales desde Panorama que se pueden configurar directamente en la CLI del recopilador de logs dedicado. Sin embargo, enviar nuevos cambios de configuración a un recopilador de logs dedicado sobrescribe a los administradores locales existentes con los administradores configurados para el recopilador de logs dedicado.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de recopiladores gestionados.

STEP 3 | (Opcional) Configure un perfil de autenticación para definir el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores que acceden a la CLI del recopilador de logs dedicado.

STEP 4 | Configure una o más cuentas de administrador según sea necesario.

Las cuentas de administrador creadas en Panorama se importan posteriormente al recopilador de logs dedicado y se administran desde Panorama.

Debe configurar la cuenta administrativa con privilegios de función de administrador de Superuser (Superusuario)para configurar correctamente la autenticación del recopilador de logs dedicado.

©2023 Palo Alto Networks, Inc.

STEP 5 | Configure la autenticación para el recopilador de logs dedicado.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador logs dedicado que añadió anteriormente.
2. (Opcional) Seleccione el **perfil de autenticación** que configuró en el paso anterior.
3. Establezca la **configuración de tiempo de espera** de autenticación para el recopilador de logs dedicado.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del recopilador de logs dedicado.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el recopilador de logs dedicado bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al recopilador de logs dedicado.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del recopilador de logs dedicado.

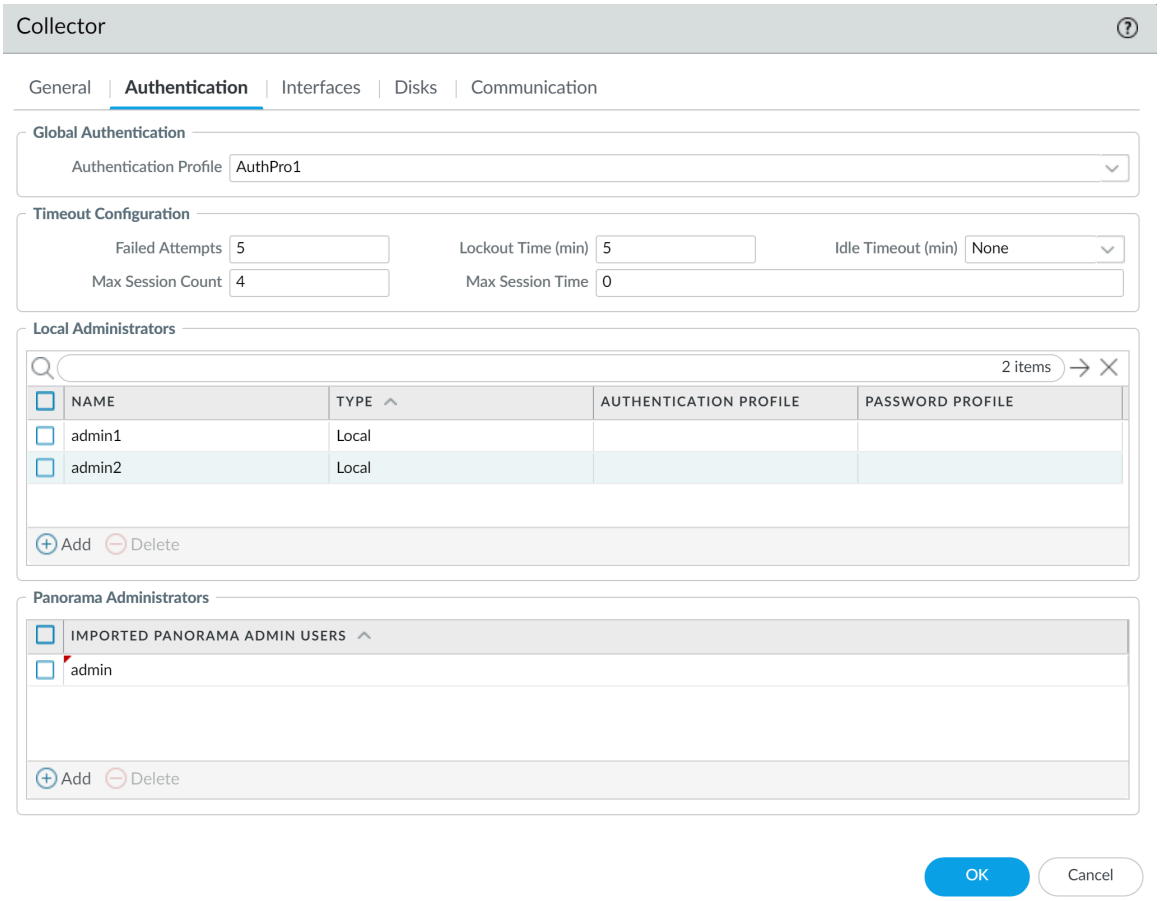
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos del recopilador de registros dedicado. Estos administradores son específicos del recopilador de logs dedicado para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan al recopilador de logs dedicado.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del recopilador de logs dedicado.



STEP 6 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 7 | Inicio de sesión en la CLI de Panorama del recopilador de logs dedicado para verificar que puede acceder correctamente al recopilador de logs dedicado mediante el usuario administrador local.

Configuración de la autenticación RADIUS para un recopilador de logs dedicado

Utilice un servidor RADIUS para autenticar el acceso administrativo a la CLI del recopilador de logs dedicado. También puede definir Atributos específicos de proveedor (VSA) en el servidor RADIUS para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y el servidor de gestión Panorama™.

 ©2023 Palo Alto Networks, Inc.

Importe el diccionario de RADIUS de Palo Alto Networks al servidor RADIUS con objeto de definir los atributos de autenticación necesarios para facilitar la comunicación entre Panorama y dicho servidor.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de recopiladores gestionados.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configuración de la autenticación RADIUS

Las cuentas de administrador configuradas para la autenticación RADIUS deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para el recopilador de logs dedicado.*

1. Añada un perfil de servidor RADIUS.

   El perfil define cómo se conecta el recopilador de logs dedicado al servidor RADIUS.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** y haga clic en **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que el recopilador de logs dedicado utiliza para autenticarse en el servidor RADIUS.

      *Seleccione **CHAP** si el servidor RADIUS admite ese protocolo; es más seguro que **PAP**.*

   5. Seleccione **Add (Añadir)** para añadir cada servidor RADIUS e ingrese lo siguiente:
      1. Un nombre en **Name (Nombre)** para identificar el servidor.
      2. La dirección IP o FQDN del **servidor RADIUS**.
      3. **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. El **Port (Puerto)** del servidor para las solicitudes de autenticación (el valor predeterminado es 1812).
   6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor RADIUS a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
   3. Configure el **Type (Tipo)** en **RADIUS**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from RADIUS (Recuperar grupo de usuarios desde RADIUS)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor RADIUS.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
   6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el recopilador de logs dedicado.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador logs dedicado que añadió anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Establezca la **configuración de tiempo de espera** de autenticación para el recopilador de logs dedicado.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del recopilador de logs dedicado.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el recopilador de logs dedicado bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al recopilador de logs dedicado.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del recopilador de logs dedicado.

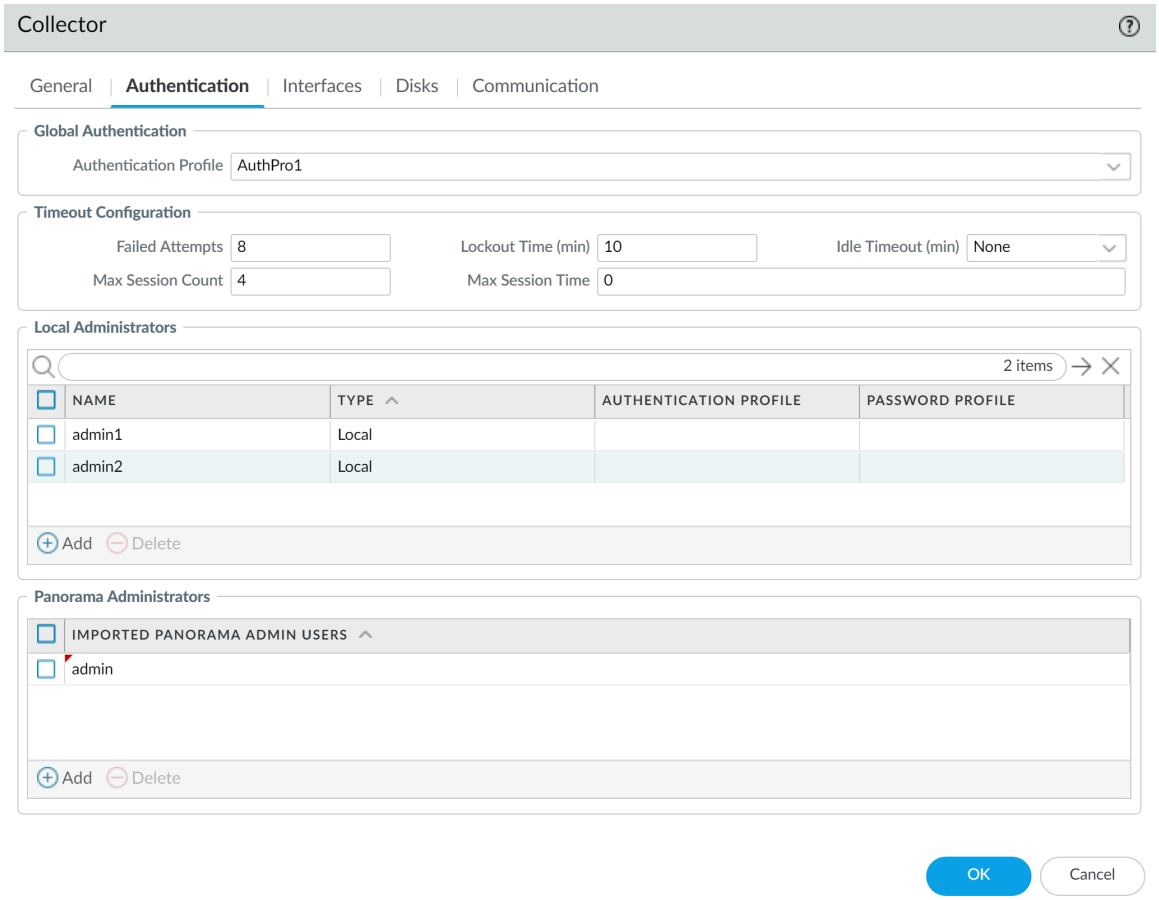
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos del recopilador de registros dedicado. Estos administradores son específicos del recopilador de logs dedicado para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan al recopilador de logs dedicado.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del recopilador de logs dedicado.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Inicio de sesión en la CLI de Panorama del recopilador de logs dedicado para verificar que puede acceder correctamente al recopilador de logs dedicado mediante el usuario administrador local.

Configuración de la autenticación TACACS+ para un recopilador de logs dedicado

Utilice un servidor TACACS+ para autenticar el acceso administrativo a la CLI del recopilador de logs dedicado. También puede definir Atributos específicos de proveedor (VSA) en el servidor TACACS+ para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configuración de recopiladores gestionados.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure la autenticación TACACS+.

Las cuentas de administrador configuradas para la autenticación TACACS+ deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para el recopilador de logs dedicado.*

1. Añada un perfil de servidor TACACS+.

   El perfil define cómo se conecta el recopilador de logs dedicado al servidor TACACS+.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACACS+** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que Panorama utiliza para autenticarse en el servidor TACACS+.
   5. Seleccione **CHAP** si el servidor TACACS+ admite ese protocolo; es más seguro que **PAP**.
   6. Seleccione **Add (Añadir)** para añadir cada servidor TACACS+ e introduzca lo siguiente:
      1. **Name (Nombre)** para identificar el servidor.
      2. **servidor TACACS+**.
      3. **Secret (Secreto)/Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. Port (Puerto) **del servidor** para las solicitudes de autenticación (el valor predeterminado es 49).
   7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor TACACS+ a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil.
   3. Configure el **Type (Tipo)** en **TACACS+**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from TACACS+ (Recuperar grupo de usuarios desde TACACS+)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor TACACS+.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
   6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el recopilador de logs dedicado.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador logs dedicado que añadió anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Establezca la **configuración de tiempo de espera** de autenticación para el recopilador de logs dedicado.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del recopilador de logs dedicado.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el recopilador de logs dedicado bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al recopilador de logs dedicado.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del recopilador de logs dedicado.

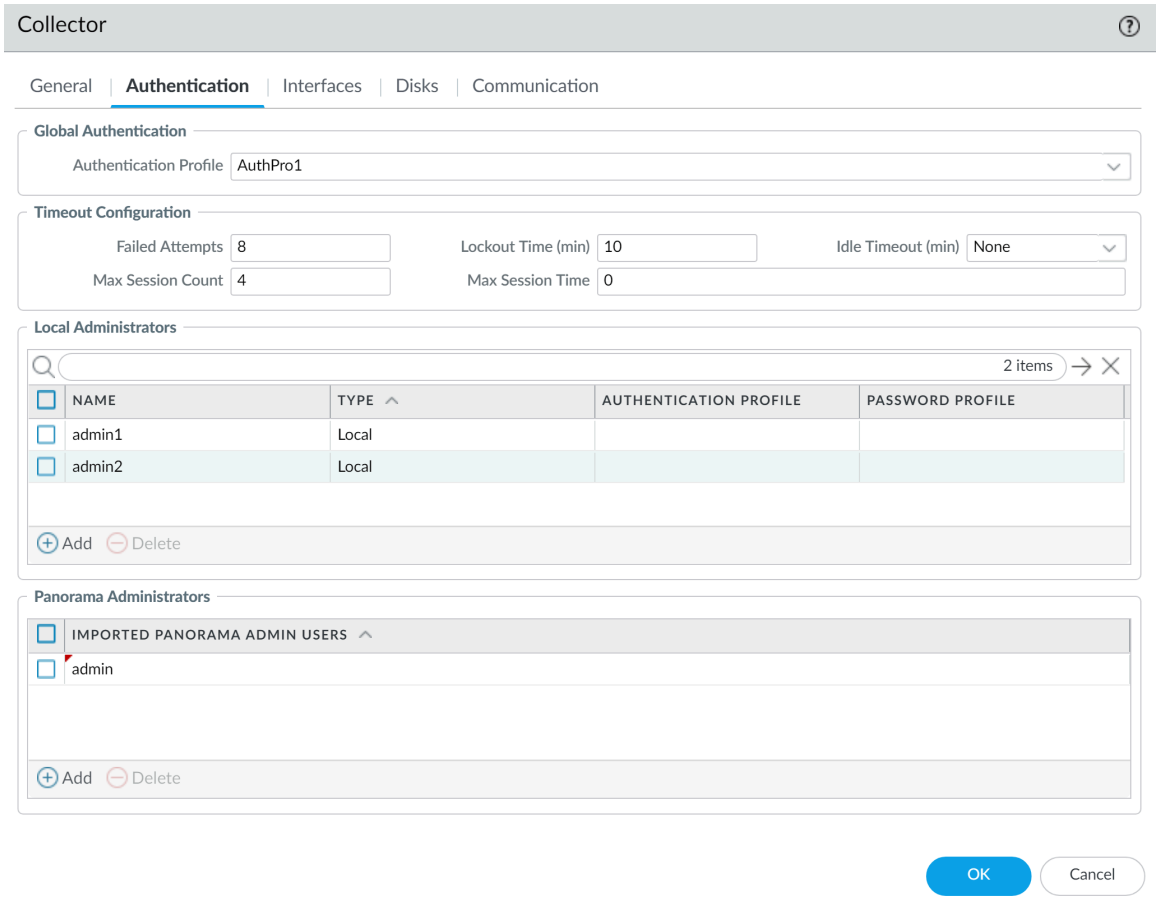
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos del recopilador de registros dedicado. Estos administradores son específicos del recopilador de logs dedicado para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan al recopilador de logs dedicado.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del recopilador de logs dedicado.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Inicio de sesión en la CLI de Panorama del recopilador de logs dedicado para verificar que puede acceder correctamente al recopilador de logs dedicado mediante el usuario administrador local.

Configuración de la autenticación LDAP para un recopilador de logs dedicado

Puede utilizar LDAP para autenticar a los usuarios finales que acceden a la interfaz web del recopilador de logs dedicado.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de recopiladores gestionados.

©2023 Palo Alto Networks, Inc.

STEP 3 | Añada un perfil de servidor LDAP.

El perfil define cómo se conecta el recopilador de logs dedicado al servidor LDAP.

Las cuentas de administrador configuradas para la autenticación LDAP deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para el recopilador de logs dedicado.*

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **LDAP** y haga clic en **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. **Add (Añada)** los servidores LDAP (máximo de cuatro). Para cada servidor, ingrese un nombre en **Name** (para identificar al servidor), una dirección IP del **LDAP Server (Servidor LDAP)** o FQDN, y un **Port (Puerto)** para el servidor (el valor predeterminado es 389).

   Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección de servidor tenga efecto.
4. Seleccione el **Type (Tipo)** de servidor.
5. Seleccione el **DN base**.

   Para identificar el DN base de su directorio, abra el complemento de la consola de administración de Microsoft **Active Directory Domains and Trusts (Dominios y confianzas de Active Directory)** y use el nombre del dominio de nivel superior.
6. Introduzca **Bind DN (DN de enlace)** y **Password (Contraseña)** para permitir que el servicio de autenticación autentique el cortafuegos.

   La cuenta DN de enlace debe tener permiso para leer el directorio LDAP.
7. Ingrese el **Bind Timeout (Tiempo de espera de enlace)** y el **Search Timeout (Tiempo de espera de búsqueda)** en segundos (el valor predeterminado es 30 para ambos).
8. Especifique el **intervalo de reintento** en segundos (el valor predeterminado es 60).
9. (Opcional) Si desea que el endpoint use SSL o TLS para una conexión más segura con el servidor del directorio, habilite la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)** (está habilitada por defecto). El protocolo que usa el endpoint depende del puerto del servidor:
   - 389 (predeterminado): TLS (específicamente, el recopilador de logs dedicado usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).
   - 636—SSL
   - Cualquier otro puerto: el recopilador de logs dedicado primero intenta utilizar TLS. Si el servidor de directorio no es compatible con TLS, el recopilador de logs dedicado recurre a SSL.
10. (Opcional) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar la verificación, debe seleccionar también la opción **Require SSL/TLS**

 ©2023 Palo Alto Networks, Inc.

secured connection (Requerir conexión segura de SSL/TLS). Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:

- Está en la lista de certificados de Panorama: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Si es necesario, importe el certificado a Panorama.
- El firmante del certificado está en la lista de autoridades de certificación confiables: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.

11. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 4 | Configure la autenticación para el recopilador de logs dedicado.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador logs dedicado que añadió anteriormente.
2. Establezca la **configuración de tiempo de espera** de autenticación para el recopilador de logs dedicado.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del recopilador de logs dedicado.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el recopilador de logs dedicado bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al recopilador de logs dedicado.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
3. Añada los administradores del recopilador de logs dedicado.

   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la

 ©2023 Palo Alto Networks, Inc.

confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **admin1** como administrador local y de Panorama.

- Configure los administradores locales.

  Configure nuevos administradores exclusivos del recopilador de logs dedicado. Estos administradores son específicos del recopilador de logs dedicado para el que se crearon y usted gestiona estos administradores desde esta tabla.

  1. **Añada** uno o más administradores locales nuevos.
  2. Especifique un **nombre** para el administrador local.
  3. Asigne un **perfil de autenticación** creado anteriormente.

     Los perfiles de autenticación LDAP solo son compatibles con administradores locales individuales.
  4. Habilite (marque) **Use Public Key Authentication (SSH) [Usar autenticación de clave pública (SSH)]** para importar un archivo de clave pública para la autenticación.
  5. Seleccione un **perfil de contraseña** para establecer los parámetros de vencimiento.

- Importación de administradores de Panorama existentes

  Importe administradores existentes configurados en Panorama. Estos administradores se configuran y administran en Panorama y se importan al recopilador de logs dedicado.

  1. **Añada** un administrador de Panorama existente.

4. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del recopilador de logs dedicado.

STEP 5 | Configure la autenticación para el recopilador de logs dedicado.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador logs dedicado que añadió anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.
3. Establezca la **configuración de tiempo de espera** de autenticación para el recopilador de logs dedicado.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del recopilador de logs dedicado.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el recopilador de logs dedicado bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al recopilador de logs dedicado.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del recopilador de logs dedicado.

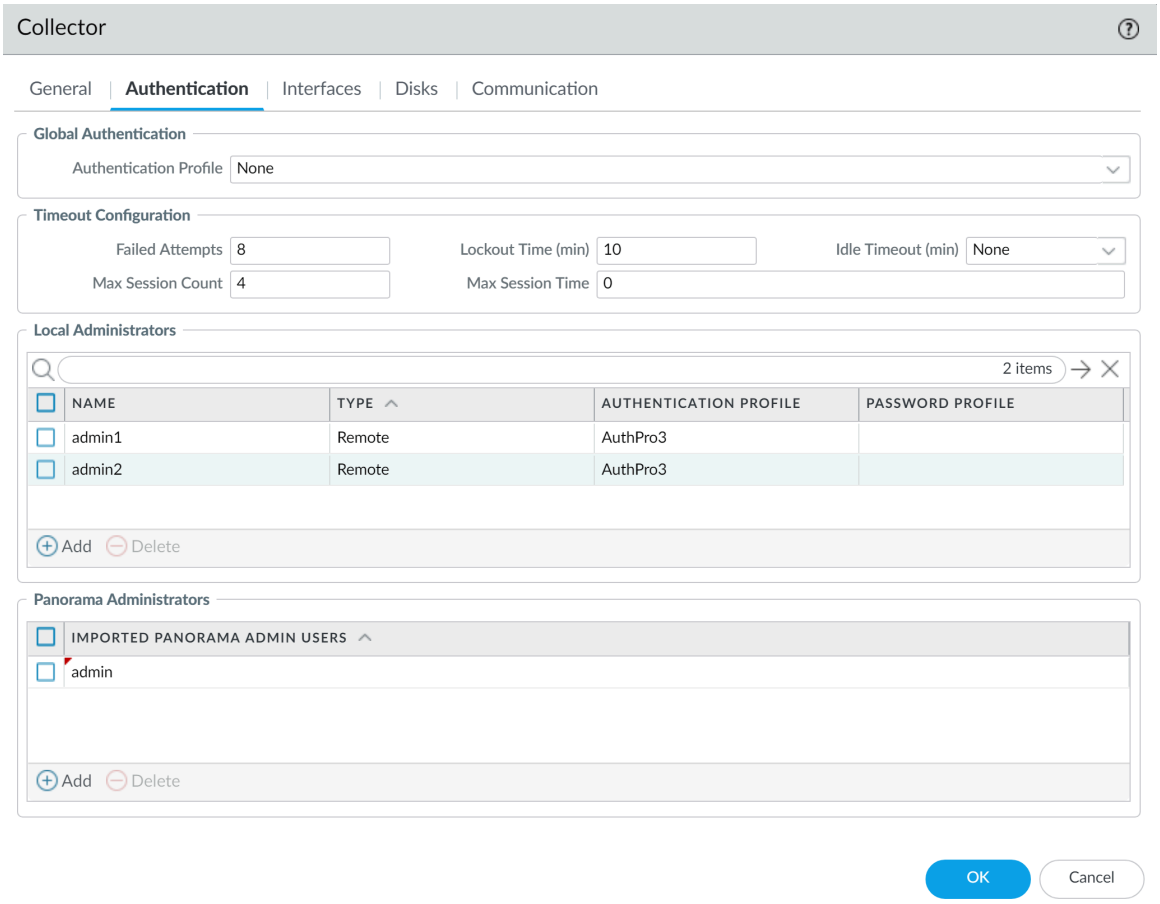
   Debe añadir el administrador (**admin**) como administrador local o como administrador de Panorama importado, pero no ambos. El envío a recopiladores administrados falla si no se

 ©2023 Palo Alto Networks, Inc.

añade un administrador o si el administrador se agrega como administrador local y como administrador de Panorama importado.

1. **Añada** y configure nuevos administradores exclusivos del recopilador de registros dedicado. Estos administradores son específicos del recopilador de logs dedicado para el que se crearon y usted gestiona estos administradores desde esta tabla.
2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan al recopilador de logs dedicado.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del recopilador de logs dedicado.



STEP 6 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 7 | Inicio de sesión en la CLI de Panorama del recopilador de logs dedicado para verificar que puede acceder correctamente al recopilador de logs dedicado mediante el usuario administrador local.

©2023 Palo Alto Networks, Inc.

Gestión de grupos de recopiladores

Un Grupo de recopiladores consta de 1 a 16 recopiladores de logs que funcionan como una sola unidad lógica de recopilación de logs de los cortafuegos. Debe asignar al menos un recopilador de logs a un grupo de recopiladores para que los cortafuegos envíen logs exitosamente a un recopilador de logs. Los logs del cortafuegos se eliminan si no hay un grupo de recopiladores configurado o si ninguno de los recopiladores de logs está asignado a un grupo de recopiladores. Puede configurar un grupo de recopiladores con múltiples recopiladores de logs para garantizar la redundancia de logs o para ajustar tasas de logs que superan la capacidad de un único recopilador de logs (consulte Modelos de Panorama). Para comprender los riesgos y mitigaciones recomendadas, consulte Advertencias para un grupo de recopiladores con múltiples recopiladores de logs.

Los dispositivos M-700, M-600, M-500, M-300 y M-200 en modo Panorama tienen un grupo de recopiladores predefinido que contiene un recopilador de logs local predefinido. Puede editar todos los ajustes del grupo de recopiladores predefinido excepto su nombre (predeterminado).

Si elimina un grupo de recopiladores, perderá logs.

Palo Alto Networks recomienda mantener el recopilador de logs y el grupo de recopiladores predeterminados en el servidor de gestión de Panorama, independientemente de si Panorama gestiona recopiladores de logs dedicados.

Si cambia un dispositivo M-Series del modo Panorama al modo Recopilador de logs, el dispositivo perderá su Grupo de recopiladores y recopilador de logs predefinidos. Entonces tendría que Configurar el dispositivo M-Series como un recopilador de logs, agréguelo como un recopilador gestionado a Panorama y configure un Grupo de recopiladores para que contenga el recopilador gestionado.

- Configuración de un grupo de recopiladores
- Configuración de la autenticación con certificados personalizados entre recopiladores de logs
- Movimiento de un recopilador de logs a un grupo de recopiladores diferente
- Eliminación de un cortafuegos de un grupo de recopiladores

Configuración de un grupo de recopiladores

Antes de configurar Grupos colectores, decida si cada uno tendrá un solo recopilador de logs o múltiples recopiladores de logs (hasta 16). Un grupo de recopiladores con múltiples recopiladores de logs admite tasas de logging y redundancia de logs más altas, pero tiene los siguientes requisitos:

- Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.
- La redundancia de logs está disponible solo si cada recopilador de logs tiene el mismo número de discos de logs. Para añadir discos a un Recopilador de logs, consulte Aumento de la capacidad de almacenamiento en el dispositivo M-Series.

©2023 Palo Alto Networks, Inc.

- (Práctica recomendada) Es conveniente que todos los recopiladores de logs del mismo grupo estén en la misma red de área local (local area network, LAN). No añada recopiladores de logs que se encuentren en la misma red de área extensa (wide area network, WAN) o en otra al mismo grupo, ya que se producen muchas más interrupciones en la red y puede llegar a perder datos de logs. También se recomienda que los recopiladores de logs del mismo grupo estén cercanos físicamente para que Panorama pueda realizar consultas en ellos con rapidez.

STEP 1 | Lleve a cabo las siguientes tareas antes de configurar el grupo de recopiladores.

1. Añada un cortafuegos como dispositivo gestionado para cada cortafuegos que asignará al grupo de recopiladores.
2. Configure un recopilador gestionado para cada recopilador de logs que asignará al grupo de recopiladores.

STEP 2 | Añada el grupo de recopiladores.

1. Acceda a la interfaz web de Panorama, seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)**, y haga clic en **Add (Añadir)** para añadir un grupo de recopiladores o edite uno existente.
2. Introduzca un nombre en **Name (Nombre)** para el grupo de recopiladores si añade uno.

   No puede volver a nombrar un grupo de recopiladores existente.
3. Introduzca el **Minimum Retention Period (Período de retención mínimo)** en días (de 1 a 2000) que el grupo de recopiladores conservará los logs del cortafuegos.

   De forma predeterminada, el campo está en blanco, lo que significa que el grupo de recopiladores conserva los logs indefinidamente.
4. Seleccione **Add (Añadir)** recopiladores de logs (1 a 16) a la lista de Miembros del grupo de recopiladores.
5. (Recomendado) Seleccione **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si está añadiendo múltiples recopiladores de logs a un solo grupo de recopiladores.

   la redundancia garantiza que no se pierdan logs si alguno de los recopiladores de logs no está disponible. Cada log tendrá dos copias y cada copia residirá en un recopilador de logs diferente. Por ejemplo, si tiene dos recopiladores de logs en el grupo de recopiladores, el log se escribe en ambos recopiladores.

   Al habilitar la redundancia se crean más logs, por lo que esta configuración requiere más capacidad de almacenamiento y se reduce la capacidad de almacenamiento a la mitad. Si un grupo de recopiladores se queda sin espacio, elimina logs antiguos. La redundancia también duplica el tráfico de procesamiento de logs en un grupo de recopiladores, que reduce su tasa de logs máxima a la mitad, ya que cada recopilador de logs debe distribuir una copia de cada log que reciba.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Asigne recopiladores de logs y cortafuegos al grupo de recopiladores.

1. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y **Add (Añadir)** para añadir ***listas de preferencia de reenvío de logs*** para los cortafuegos.

   Los datos de logs se reenvían a través de un canal TCP separado. Al añadir una preferencia de reenvío de logs, la lista habilita la creación de conexiones TCP independientes para reenviar datos de logs.

   Una lista de preferencias determina el orden en que los Recopiladores de logs recibirán los logs de un cortafuegos. Si no se asigna una lista de preferencias de reenvío de logs, puede encontrar uno de los siguientes escenarios:

   - *Si Panorama está en modo Management Only (Solo administración), descarta todos los logs entrantes.*
   - *Si el recopilador de logs local no está configurado como recopilador gestionado cuando Panorama está en modo Panorama, Panorama descarta todos los logs entrantes.*
   - *Si el recopilador de logs local está configurado como recopilador gestionado cuando Panorama está en modo Panorama, se reciben logs entrantes, pero Panorama puede actuar como cuello de botella porque todos los cortafuegos gestionados reenvían primero logs al recopilador de logs local antes de que se redistribuyan a otros recopiladores de logs disponibles.*

1. En la sección Dispositivos, haga clic en **Modify (Modificar)** para modificar las listas de cortafuegos y haga clic en **OK (Aceptar)**.
2. En la sección de Recopiladores, seleccione **Add (Añadir)** recopiladores de logs a la lista de preferencias.

   Si ha habilitado la redundancia en el paso 2, se recomienda que añada al menos dos recopiladores de logs. Si asigna múltiples recopiladores de logs, el primero deberá ser el principal; si el principal deja de estar disponible, los cortafuegos enviarán los logs al siguiente recopilador de logs de la lista. Para cambiar la prioridad de un recopilador de logs, selecciónelo y haga clic en **Move up (Mover hacia arriba)** (mayor prioridad) o **Move Down (Mover hacia abajo)** (menor prioridad).
3. Haga clic en **OK (Aceptar)**.

©2023 Palo Alto Networks, Inc.

STEP 4 | Defina la capacidad de almacenamiento (cuotas de logs) y el período de vencimiento de cada tipo de log.

1. Regrese a la pestaña **General** y haga clic en el valor **Log Storage (Almacenamiento de logs)**.

   Si el campo muestra 0 MB, compruebe que ha habilitado los pares de disco para logs y compilado los cambios (consulte Configuración de un recopilador gestionado*, pestaña* ***Disks [Discos]****).*

2. Introduzca la **Quota(%) (Cuota[%])** de almacenamiento de logs para cada tipo de log.
3. Introduzca el **Max Days (Número máx. de días)** (periodo de vencimiento) para cada tipo de log (1 a 2.000).

   De manera predeterminada, los campos están en blanco, lo que significa que los logs nunca se vencen.

STEP 5 | Compile y compruebe sus cambios.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y al grupo de recopiladores que configuró.
2. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que los recopiladores de logs en el grupo de recopiladores están:

   - **Conectados a Panorama**: la columna Conectado muestra un icono de marca de verificación para indicar que el recopilador de logs está conectado a Panorama.
   - **Sincronizado con Panorama**: la columna de estado de configuración indica si un recopilador de logs esta sincronizado `In Sync` (icono verde) o sin sincronización `Out of Sync` (icono rojo) con Panorama.

STEP 6 | Solución de problemas de conectividad a recursos de red para verificar que los cortafuegos se han conectado al recopilador de logs.

STEP 7 | Pasos siguientes:

1. Configure el reenvío de logs a Panorama.

   El grupo de recopiladores no recibirá logs de cortafuegos hasta que configure los cortafuegos para reenviar a Panorama.

2. (Opcional) Configure el reenvío de logs desde Panorama a destinos externos.

   Puede configurar cada grupo de recopiladores para que reenvíe logs a diferentes ubicaciones (por ejemplo el servidor syslog).

Configuración de la autenticación con certificados personalizados entre recopiladores de logs

Complete el siguiente procedimiento para configurar los certificados personalizados para la comunicación entre recopiladores de logs. Debe configurar la comunicación de servidor segura y la comunicación de cliente segura en cada recopilador de logs en un grupo de recopiladores debido a que los roles de servidor y cliente se seleccionan de manera dinámica. Utilice los certificados

 ©2023 Palo Alto Networks, Inc.

personalizados para crear una cadena de confianza única que garantice la autenticación mutua entre los miembros de su grupo de recopiladores de logs.

Para obtener más información sobre la utilización de los certificados personalizados, consulte ¿Cómo se autentican mutuamente las conexiones SSL/TLS?

STEP 1 | Obtenga pares de claves y certificados de autoridades de certificados (CA) para cada recopilador de logs.

STEP 2 | Importe el certificado de CA para validar la identidad del recopilador de logs cliente, el par de claves del servidor y el par de claves cliente de cada recopilador de logs en el grupo de recopiladores.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Import (Importar)**.
2. Importe el certificado de CA, el par de claves del servidor y el par de claves de cliente.
3. Repita este paso para cada recopilador de logs.

STEP 3 | Configure un perfil de certificado que incluya la CA raíz y la CA intermedia para la comunicación de servidor segura. Este perfil de certificado define la autenticación entre los recopiladores de logs.

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

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

STEP 4 | Configure el perfil de certificado para garantizar una comunicación de cliente segura. Puede configurar este perfil en cada recopilador de logs cliente individualmente o puede enviar la configuración desde Panorama™ a los recopiladores de logs gestionados.

Si está utilizando SCEP para el certificado cliente, configure un perfil SCEP *en lugar de un perfil de certificado.*

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

STEP 5 | Configure un perfil de servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Lleve a cabo la Configuración de un perfil de servicio SSL/TLS para definir el certificado y protocolo que utilizan los recopiladores de logs para los servicios SSL/TLS.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Después de implementar los certificados personalizados en todos los recopiladores de logs, aplique la autenticación de certificados personalizados.

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y seleccione el grupo de recopiladores.
2. En la pestaña General, haga clic en **Enable secure inter LC Communication (Habilitar la comunicación segura entre LC)**.

   Si habilita la comunicación segura entre LC y el grupo de recopiladores incluye un recopilador de logs local, debe aparecer un enlace que indique que el **recopilador de logs en la instancia local de Panorama utiliza la configuración de cliente segura de los ajustes > de comunicación segura de Panorama**. Puede hacer clic en este enlace para abrir el cuadro de diálogo de Secure Communication Settings (Ajustes de comunicación segura), y configurar los ajustes de servidor seguro y cliente seguro para el recopilador de logs local.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

STEP 7 | Configure la comunicación de servidor segura en cada recopilador de logs.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para los recopiladores de logs dedicados o **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para editar los ajustes de comunicación segura para un recopilador de logs local.
2. Para los recopiladores de logs dedicados, haga clic en el recopilador de logs y seleccione **Communications (Comunicaciones)**.
3. Habilite la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
4. Seleccione el perfil del servicio SSL/TLS del menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre recopiladores de logs.
5. Seleccione el perfil en el menú desplegable **Certificate Profile (Perfil de certificados)**.
6. Verifique que la opción **Custom Certificates Only (Solo los certificados personalizados)** esté deshabilitada (sin marca). Esto permite que continúe la comunicación entre recopiladores de logs con los certificados predefinidos mientras configura los certificados personalizados.
7. Configure el tiempo de espera de desconexión, es decir, el número de minutos que los recopiladores de logs esperan antes de interrumpir y restablecer la conexión con otros recopiladores de logs. Este campo está en blanco de manera predeterminada (el rango es de 0 a 44 640).
8. (Opcional) Configure una lista de autorizaciones. La lista de autorizaciones añade una capa adicional de seguridad más allá de la autenticación del certificado. La lista de autorizaciones verifica el Asunto o Nombre alternativo del sujeto del certificado del cliente. Si el Subject (Sujeto) o el Subject Alt Name (Nombre alternativo del sujeto) presentado con el certificado del cliente no coincide con un identificador en la lista de autorizaciones, se deniega la autenticación.

   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Selecciona el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** configurado en el perfil del certificado como el tipo de identificador.

 ©2023 Palo Alto Networks, Inc.

3. Introduzca un nombre en Common Name (Nombre común) si el identificador es `Subject (Asunto)` o bien una dirección IP, un nombre de host o un correo electrónico si el identificador es `Subject Alt Name (Nombre alternativo de asunto)`.
4. Haga clic en **OK (Aceptar)**.
5. Habilite la opción **Check Authorization List (Comprobar lista de autorización)** para configurar Panorama a fin que aplique la lista de autorización.

9. Haga clic en **OK (Aceptar)**.
10. **Commit (Confirmar)** los cambios.

Después de confirmar estos cambios, inicia la cuenta regresiva del tiempo de espera de desconexión. Cuando el tiempo de espera finaliza, los recopiladores de logs en el grupo de recopiladores no se pueden conectar sin los certificados configurados.

STEP 8 | Configure la comunicación de cliente segura en cada recopilador de logs.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para los recopiladores de logs dedicados o **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para editar los ajustes de comunicación segura para un recopilador de logs local.
2. Para los recopiladores de logs dedicados, haga clic en el recopilador de logs y seleccione **Communications (Comunicaciones)**.
3. En Secure Client Communications (Comunicación de cliente segura), seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)** en los menús desplegables correspondientes.
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

Movimiento de un recopilador de logs a un grupo de recopiladores diferente

Los dispositivos M-700, M-600, M-500, M-300, M-200 y los dispositivos virtuales Panorama pueden tener uno o más recopiladores de logs en cada grupo de recopiladores. Asigne los recopiladores de logs a un grupo de recopiladores basado en la tasa de creación de logs y los requisitos de almacenamiento de logs de ese grupo de recopiladores. Si las tasas y el almacenamiento requerido aumentan en el grupo de recopiladores, se recomienda realizar el Aumento de la capacidad de almacenamiento en el dispositivo serie M o la Configuración de un grupo de recopiladores con recopiladores de logs adicionales. Sin embargo, en algunas implementaciones, podría ser más económico mover los recopiladores de logs entre los grupos de recopiladores.

 ©2023 Palo Alto Networks, Inc.

Si el recopilador de logs local de un dispositivo M-700, M-600, M-500, M-300 o M-200 funciona en modo de Panorama, solo puede moverlo si el dispositivo es el peer pasivo de una configuración de alta disponibilidad (HA). La sincronización de HA aplica las configuraciones asociadas al nuevo grupo de recopiladores. Nunca mueva un recopilador de logs que sea local al peer activo de HA.

Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.

La redundancia de logs está disponible solo si cada recopilador de logs tiene el mismo número de discos de logs. Para añadir discos a un Recopilador de logs, consulte Aumento de la capacidad de almacenamiento en el dispositivo M-Series.

STEP 1 | Elimine el recopilador de logs desde la gestión de Panorama.

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y edite el grupo de recopiladores que contiene el recopilador de logs que moverá.
2. En la lista de Miembros del grupo de recopiladores, seleccione y elija **Delete (Eliminar)** para eliminar el recopilador de logs.
3. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y, en la lista de preferencias de reenvío de logs, lleve a cabo los siguientes pasos para cada conjunto de cortafuegos asignado al recopilador de logs que moverá.
   1. En la columna Dispositivos, haga clic en el enlace asignado al recopilador de logs.
   2. En la columna recopiladores, seleccione **Delet (Eliminar)** el Recopilador de logs.

      *Para reasignar los cortafuegos, haga clic en **Add (Añadir)** para añadir los recopiladores de logs a los cuales reenviarán los logs.*

   3. Haga clic en **OK (Aceptar)** dos veces para guardar los cambios.
4. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y luego seleccione y haga clic en **Delete (Eliminar)** para eliminar el recopilador de logs que moverá.

STEP 2 | Configure un grupo de recopiladores.

Añada el recopilador de logs a su nuevo grupo de recopiladores y asigne los cortafuegos al recopilador de logs.

*Cuando envía los cambios a la configuración del grupo de recopiladores, Panorama inicia la redistribución de logs en los recopiladores de logs. Este proceso puede demorar horas por cada terabyte de logs. Durante el proceso de redistribución, se reduce la tasa máxima de logs. En la página **Panorama** > **Collector Groups (Grupos de recopiladores)**, la columna Estado de redistribución de logs indica el estado de finalización del proceso con un porcentaje.*

STEP 3 | Configuración del reenvío de logs a Panorama en el grupo de recopiladores nuevo que ha configurado.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Si todavía no lo ha hecho, haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para aceptar los cambios realizados en Panorama y enviarlos a los grupos de dispositivos, las plantillas y los grupos de recopiladores.

Eliminación de un cortafuegos de un grupo de recopiladores

Si usa un dispositivo virtual Panorama en el modo heredado para gestionar los recopiladores de logs dedicados, tiene la opción de reenviar los logs del cortafuegos a Panorama en lugar de reenviarlos a los recopiladores de logs. Para tales casos, debe eliminar el cortafuegos del Grupo de recopiladores; a continuación, el cortafuegos reenviará automáticamente sus logs a Panorama.

Para eliminar temporalmente la lista de preferencias de reenvío de logs del cortafuegos, puede eliminarla con la CLI en el cortafuegos. Sin embargo, debe eliminar los cortafuegos asignados en la configuración del grupo de recopiladores de Panorama. De lo contrario, la próxima vez que envíe cambios en el grupo de recopiladores, el cortafuegos volverá a configurarse para enviar logs al recopilador de logs asignado.

STEP 1 | Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y modifique el grupo de recopiladores.

STEP 2 | Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)**, haga clic en el cortafuegos en la lista Dispositivos, seleccione **Modify (Modificar)** la lista de dispositivos, borre la casilla de verificación del cortafuegos y haga clic en **OK (Aceptar)** tres veces.

STEP 3 | Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y elija **Commit and Push (Confirmar y enviar)** sus cambios a Panorama y al grupo de recopiladores de donde eliminó el cortafuegos.

 ©2023 Palo Alto Networks, Inc.

Configuración del reenvío de logs a Panorama

Cada cortafuegos almacena sus archivos de log localmente de forma predeterminada y no puede mostrar los logs que residen en otros cortafuegos. Por lo tanto, para lograr una visibilidad global de la actividad de red que supervisan todos sus cortafuegos, debe reenviar todos los logs de cortafuegos a Panorama y hacer Uso de Panorama para lograr visibilidad. En los casos en que algunos equipos de su organización puedan lograr mayor eficiencia al supervisar solo los logs que son relevantes para sus operaciones, puede crear filtros de reenvío basados en cualquier atributo de logs (tal como un tipo de amenaza o usuario de origen). Por ejemplo, un analista de operaciones de seguridad que investiga ataques de malware puede estar interesado únicamente en logs de amenazas con el atributo de tipo configurado en wildfire-virus.

Los siguientes pasos describen cómo usar las plantillas de Panorama y los grupos de dispositivos para configurar múltiples cortafuegos para que reenvíen logs.

Si Panorama gestiona los cortafuegos que ejecutan versiones de software anteriores a PAN-OS 7.0, especifique un servidor WildFire® desde el cual Panorama pueda recopilar información de análisis para las muestras de WildFire que aquellos cortafuegos envíen. Panorama usa la información para completar los logs WildFire Submissions (Presentaciones de WildFire) a los que les falta valores de campo en PAN-OS 7.0. Los cortafuegos que ejecutan versiones anteriores no completarán estos campos. Para especificar el servidor, seleccione ***Panorama*** *>* ***Setup (Configuración)*** *>* ***WildFire****, edite la Configuración general e introduzca el nombre de* ***WildFire Private Cloud (Nube privada de WildFire)****. El valor predeterminado es* ***wildfire-public-cloud****, que es la nube de WildFire alojada en los Estados Unidos.*

También puede reenviar logs de cortafuegos a servicios externos (como un servidor syslog). Para obtener más detalles, consulte Opciones de reenvío de logs**.**

STEP 1 | Agregue un grupo de dispositivos para los cortafuegos que reenviarán logs.

Panorama requiere un grupo de dispositivos para enviar un perfil de reenvío de logs en los cortafuegos. Cree un grupo de dispositivos nuevo o asigne los cortafuegos a un grupo de dispositivos existente.

STEP 2 | Agregue una plantilla para los cortafuegos que reenviarán logs.

Panorama requiere una plantilla para enviar la configuración de logs en los cortafuegos. Cree una plantilla nueva o asigne los cortafuegos a una plantilla existente.

STEP 3 | Cree un perfil de reenvío de logs.

El perfil define los destinos para tráfico, amenaza, envío de WildFire, filtro de URL, filtro de datos, túnel y logs de autenticación.

1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**, elija el grupo de dispositivos de los cortafuegos que reenviarán logs en **Device Group (Grupo de dispositivos)** y haga clic en **Add (Añadir)** para añadir un perfil.
2. Introduzca un nombre en **Name (Nombre)** para identificar el perfil de reenvío de logs.
3. Seleccione **Add (Añadir)** para añadir uno o más *perfiles de la lista de coincidencias*.

 ©2023 Palo Alto Networks, Inc.

Los perfiles especifican los filtros de la consulta de log, los destinos de reenvío y las acciones automáticas, así como el etiquetado. Para cada perfil de lista de coincidencia:

1. Introduzca un **Name (Nombre)** para identificar el perfil.
2. Seleccione el **Log Type (Tipo de log)**.
3. En la lista desplegable **Filter (Filtro)**, seleccione **Filter Builder (Generador de filtro)**. Especifique lo siguiente y luego seleccione **Add (Añadir)** para añadir cada consulta:

   Lógica de **Connector (Conector)** (y/o)

   Attribute (Atributo) de log

   Operator (Operador) para definir lógica de inclusión o exclusión

   Value (Valor) de atributo para coincidencia de la consulta
4. Seleccione **Panorama**.

4. Haga clic en **OK (Aceptar)** para guardar el perfil de reenvío de logs.

STEP 4 | Asigne el perfil de reenvío de logs a las reglas de política y zonas de red.

Las reglas de seguridad, autenticación y protección DoS admiten el reenvío de logs. En este ejemplo, se asigna el perfil a una regla de seguridad.

Realice los siguientes pasos para cada regla que activará el reenvío de logs:

1. Seleccione la base de reglas (por ejemplo, **Policies [Políticas]** > **Security [Seguridad]** > **Pre Rules [Reglas previas]**), elija el **Device Group (Grupo de dispositivos)** de los cortafuegos que reenviarán logs y edite la regla.
2. Seleccione **Actions (Acciones)** y seleccione el perfil de **Log Forwarding (Reenvío de logs)** que creó.
3. Configure el **Profile Type (Tipo de perfil)**, en **Profiles (Perfiles)** o **Group (Grupo)**, y luego seleccione los perfiles de seguridad o **Group Profile (Perfil de grupo)** requeridos para activar la generación y el reenvío de logs para lo siguiente:
   - Logs de amenazas: El tráfico debe coincidir con cualquier perfil de seguridad asignado a una regla.
   - Logs de WildFire: El tráfico debe coincidir con un perfil de análisis de WildFire asignado a una regla.
4. Para los logs de tráfico, seleccione **Log At Session Start (Log al iniciar sesión)** o **Log At Session End (Log al finalizar sesión)**.
5. Haga clic en **OK (Aceptar)** para guardar la regla.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure los destinos para los logs del sistema, los logs de configuración, los logs de User-ID™ y los logs de HIP Match.



Panorama genera logs de correlación basados en los logs de cortafuegos que recibe, en lugar de agrupar logs de correlación de los cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de logs)** y elija la plantilla de los cortafuegos que reenviarán logs en **Template (Plantilla)**.
2. Para cada tipo de log que el cortafuegos reenviará, consulte el paso Añada uno o más perfiles de lista de coincidencia.

STEP 6 | (Solo cortafuegos PA-7000 Series) Configure una interfaz de tarjeta de log para realizar el reenvío de logs.

Cuando configura un puerto de datos en una de las tarjetas de procesamiento de red (NPC) de la serie PA-7000 como una interfaz de tarjeta de log, el cortafuegos automáticamente comenzará a usar esta interfaz para reenviar logs a los destinos de log que ha configurado y reenviar archivos

 ©2023 Palo Alto Networks, Inc.

para el análisis de WildFire. Asegúrese de que la interfaz que configure pueda conectarse con los destinos de reenvío de logs y la nube de WildFire, el dispositivo WildFire o ambos.

Dado que el cortafuegos serie PA-7000 ahora puede reenviar los logs a Panorama, Panorama ya no trata a los cortafuegos serie PA-7000 que gestiona como recopiladores de logs. Si no ha configurado los cortafuegos PA-7000 Series para reenviar los logs a Panorama, todos los logs que genera un cortafuegos PA-7000 Series gestionado solo se pueden ver desde el cortafuegos local y no desde Panorama. Si aún no cuenta con una infraestructura de reenvío de archivos de log que sea capaz de gestionar la velocidad y el volumen de logs de los cortafuegos PA-7000 Series, a partir de PAN-OS 8.0.8 puede habilitar Panorama para que consulte directamente a los cortafuegos PA-7000 Series cuando supervisa los logs. Para usar esta función, el cortafuegos PA-7000 Series y Panorama deben utilizar PAN-OS 8.0.8 o una versión posterior. Habilite Panorama para consultar directamente los cortafuegos PA-7000 Series introduciendo el siguiente comando desde la CLI de Panorama:

```
> debug reportd send-request-to-7k yes
```

*Después de ejecutar este comando, podrá ver los logs de los cortafuegos gestionados PA-7000-Series en la pestaña **Monitor** de Panorama. Además, al igual que con todos los dispositivos gestionados, también puede generar informes que incluyan datos de log de la serie PA-7000 Series seleccionando **Remote Device Data (Datos de dispositivo remoto)** como el **Data Source (Origen de datos)**. Si luego decide habilitar los cortafuegos serie PA-7000 para reenviar los logs a Panorama, primero debe deshabilitar esta opción usando el comando **debug reportd send-request-to-7k no**.*

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**, seleccione la **Template (Plantilla)** de los cortafuegos que reenviarán los logs y seleccione **Add Interface (Añadir interfaz)**.
2. Seleccione la **Slot** y el **Interface Name**.
3. Cambie el **Interface Type (Tipo de interfaz)** a **Log Card (Tarjeta de log)**.
4. Introduzca los valores oportunos en **IP Address (Dirección IP)**, **Default Gateway (Puerta de enlace predeterminada)** y, solo para IPv4, **Netmask (Máscara de red)**.
5. Seleccione **Advanced (Avanzado)** y especifique **Link Speed (Velocidad del enlace)**, **Link Duplex (Dúplex de enlace)** y **Link State (Estado de enlace)**.

   *Estos campos están configurados por defecto en **auto**, que especifica que el cortafuegos determina automáticamente los valores según la conexión. Sin embargo, el valor mínimo recomendado de **Link Speed** para cualquier conexión es de **1000** (Mbps).*
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

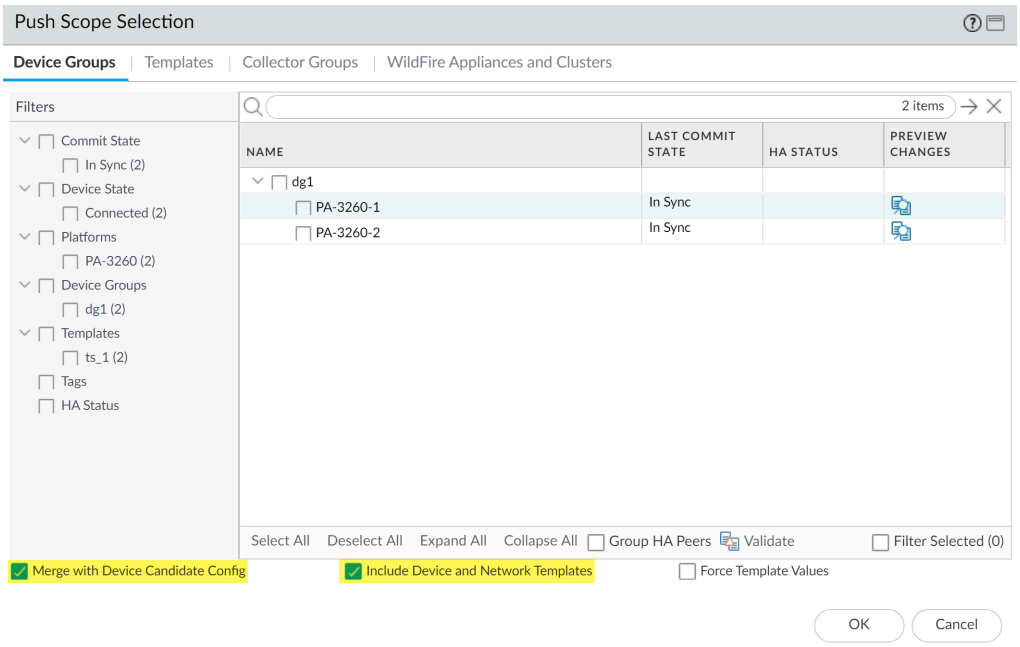
STEP 7 | Configure Panorama para recibir los logs.

Si va a reenviar logs a un dispositivo virtual Panorama en modo heredado, puede omitir este paso.

1. Para cada recopilador de logs que recibirá logs, configure un recopilador gestionado.
2. Configure un grupo de recopiladores para asignar cortafuegos a recopiladores de logs específicos para el reenvío de logs.

STEP 8 | Confirme sus cambios de configuración.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y, luego, en **Edit Selections (Editar selección)**.
2. Marque **Merge with Device Candidate Config (Fusionar con configuración candidata de dispositivos)** e **Include Device and Network Templates (Incluir plantillas de dispositivos y red)** y haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit and Push (Confirmar y enviar)** para aceptar los cambios realizados en Panorama y enviarlos a los grupos de dispositivos, las plantillas y los grupos de recopiladores.
4. Verifique el reenvío de logs a Panorama para confirmar que la configuración es correcta.

Para cambiar el modo de reenvío de logs que los cortafuegos usan para enviar logs a Panorama, puede Modificar los valores predeterminados de almacenamiento en búfer y reenvío de logs. *También puede consultar* Gestión de cuotas de almacenamiento y períodos de vencimiento de logs e informes.

©2023 Palo Alto Networks, Inc.

Configuración del reenvío de syslog a destinos externos

En el caso de una implementación con una alta tasa de generación de logs, puede reenviar syslogs a través de una interfaz Ethernet para evitar la pérdida de logs y reducir la carga en la interfaz de gestión, lo que optimiza las operaciones de administración.

El reenvío de syslogs mediante una interfaz Ethernet solo es compatible con un servidor de gestión Panorama™ en modo Panorama o en modo de recopilación de logs. Además, puede habilitar el reenvío de syslogs en una sola interfaz, independientemente de si Panorama está en modo Panorama o en modo de recopilación de logs.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Configuración de recopiladores gestionados.

STEP 3 | Configuración de un grupo de recopiladores.

Los dispositivos M-Series tienen predefinido un grupo de recopiladores predeterminado, que ya incluye como miembro el recopilador de logs local. Sin embargo, en el dispositivo virtual Panorama, debe añadir el grupo de recopiladores y añadir el recopilador de logs local como miembro. Para ambas configuraciones, debe asignar cortafuegos a un recopilador de logs para el reenvío de logs.

STEP 4 | Configure un perfil de servidor Syslog.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **Syslog** y **añada** un nuevo perfil de servidor Syslog.
2. Introduzca un **nombre** para el perfil del servidor Syslog.
3. Para cada servidor Syslog, **añada** la información que Panorama o el recopilador de logs dedicado requieren para conectarse a él:
   - **Name (Nombre)**: nombre único para el servidor Syslog.
   - **Syslog Server**: dirección IP o nombre de dominio completo (fully qualified domain name, FQDN) del servidor Syslog.
   - **Transport (Transporte)**: seleccione **UDP**, **TCP** o **SSL** como método de comunicación con el servidor Syslog.
   - **Port (Puerto)**: el número de puerto que se utilizará al enviar mensajes de syslog (el valor predeterminado es UDP en el puerto 514); debe utilizar el mismo número de puerto en Panorama y en el recopilador de logs dedicado.
   - **Format**: seleccione el formato de mensaje de Syslog que se debe utilizar: **BSD** (valor predeterminado) o **IETF**. Normalmente, el formato **BSD** se realiza mediante UDP y el formato **IETF** mediante TCP o SSL.
   - **Facility (Instalación)**: seleccione el valor de syslog estándar (por defecto es **LOG_USER**) para calcular el campo de prioridad (PRI) en la implementación del servidor syslog. Seleccione el valor que asigna cómo usa el campo PRI para gestionar sus syslogs.
4. (Opcional) Para personalizar el formato de los mensajes de syslog que envía Panorama o el recopilador de logs dedicado, seleccione **Custom Log Format (Formato de log**

 ©2023 Palo Alto Networks, Inc.

personalizado). Si desea más información sobre cómo crear formatos personalizados para los distintos tipos de log, consulte Guía de configuración de formato de eventos comunes.

5. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor Syslog.

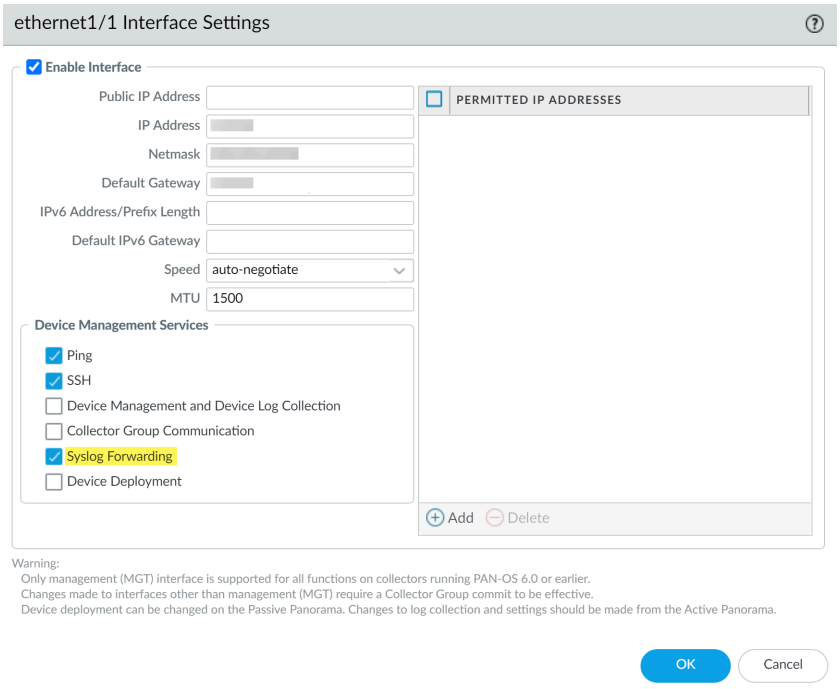
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure una interfaz Ethernet para reenviar syslogs.

De forma predeterminada, el reenvío de syslog está habilitado en la interfaz de gestión y solo se admite en una interfaz a la vez.

- Configure una interfaz Ethernet en el recopilador de logs local desde la interfaz web de Panorama.
  1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces** y seleccione una interfaz Ethernet.
  2. **Habilite la interfaz**.
  3. Configure la interfaz Ethernet según corresponda.
  4. En la sección Device Management Services (Servicios de gestión de dispositivos), habilite **Syslog Forwarding (Reenvío de syslogs)**.
  5. Seleccione **Yes (Sí)** para confirmar el cambio de reenvío de syslog.

     Solo puede hacerlo en una única interfaz Ethernet en el recopilador de logs local.
  6. Haga clic en **OK** (Aceptar) para guardar los cambios.
  7. **Commit (Compilar)** y **Commit and Push (Compilar y enviar)** para aplicar esos cambios en su configuración.



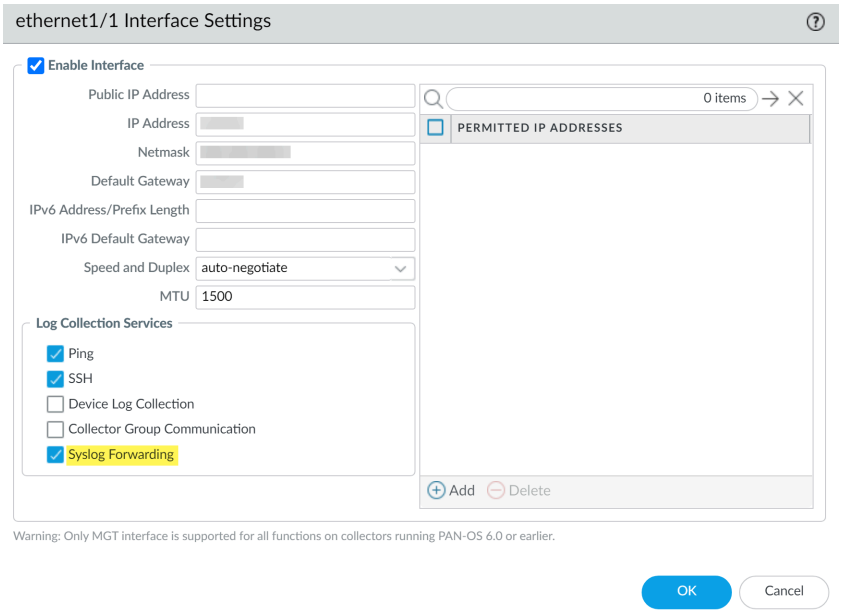
- Configure una interfaz Ethernet en un recopilador de logs dedicado.
  1. Panorama**Managed Collectors** > **(Recopiladores gestionados)** y elija un recopilador de logs dedicado.
  2. **Habilite la interfaz**.
  3. Configure la interfaz Ethernet según corresponda.
  4. En la sección Log Collection Services (Servicios de recopilación de logs), habilite **Syslog Forwarding**

 ©2023 Palo Alto Networks, Inc.

5. Seleccione **Yes (Sí)** para confirmar el cambio de reenvío de syslog.

   Solo puede hacerlo en una única interfaz Ethernet en el recopilador de logs dedicado.

6. Haga clic en **OK** (Aceptar) para guardar los cambios.
7. **Commit (Compilar)** y **Commit and Push (Compilar y enviar)** para aplicar esos cambios en su configuración.



- Configure una interfaz de Ethernet interface en el recopilador de logs local o en el recopilador de logs dedicado de la CLI de Panorama.

  Para configurar con éxito el reenvío de syslogs a través de una interfaz Ethernet desde la CLI, primero debe deshabilitar el reenvío de syslogs en la interfaz de gestión y luego habilitar el reenvío de syslogs en la interfaz Ethernet desde la CLI; Panorama no deshabilita automáticamente el reenvío de syslogs a través de la interfaz de gestión; se habilita el reenvío de syslogs en una interfaz Ethernet desde la CLI, por lo que el reenvío de syslogs continúa a través de la interfaz de gestión si lo habilita en las interfaces de gestión y Ethernet.

  1. Inicio de sesión en la CLI de Panorama
  2. Deshabilitar el reenvío de syslog en la interfaz de gestión:

```
admin@Panorama> configure
```

```
admin@Panorama> set log-collector <Log Collector Serial Number>
 deviceconfig system service disable-syslog-forwarding yes
```

 ©2023 Palo Alto Networks, Inc.

3. Habilitar el reenvío de syslog en la interfaz Ethernet:

```
admin@Panorama> configure
```

```
admin@Panorama> set log-collector <Log Collector Serial Number>
 deviceconfig system eth<Interface Number> service disable-
syslog-forwarding no
```

```
admin@Panorama> commit
```

4. Confirmar los cambios de configuración:

```
admin@Panorama> run commit-all log-collector-config log-
collector-group <Collector Group name>
```

STEP 6 | Configuración del reenvío de logs a Panorama.

STEP 7 | Configure el reenvío de syslogs desde Panorama a un servidor Syslog.

 ©2023 Palo Alto Networks, Inc.

Reenvío de logs a Cortex Data Lake

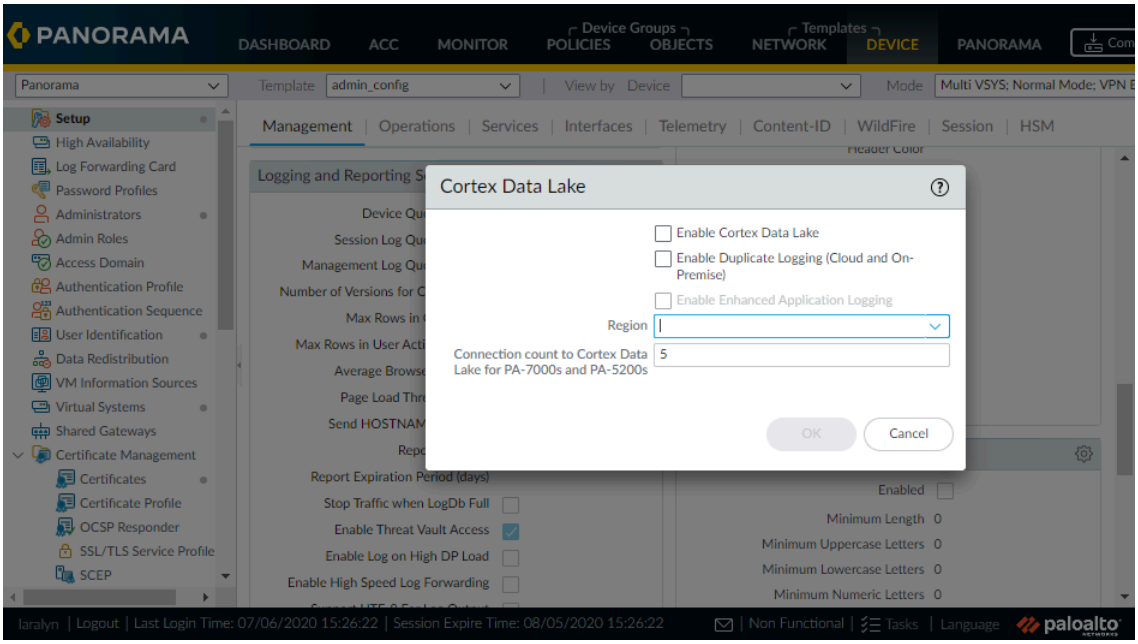
Cortex Data Lake es la infraestructura de creación de logs basada en la nube de Palo Alto Networks. Antes de que pueda configurar sus cortafuegos gestionados para que envíen los logs a Cortex Data Lake (anteriormente Servicio de creación de logs), debe comprar una licencia para el volumen de logs en su implementación e instalar el complemento de servicios en la nube. Si ya posee recopiladores de logs en las instalaciones, puede utilizar Cortex Data Lake para complementar y aumentar la configuración existente.

Puede ver los logs reenviados a Cortex Data Lake en los últimos 30 días en Panorama. No puede ver los logs reenviados a Cortex Data Lake si los logs reenviados tienen más de 30 días de antigüedad o si **habilita la creación de logs duplicada**. Para ver estos logs, inicie sesión en el hub y navegue hasta la aplicación Cortex Data Lake para usar la pestaña Explore (Explorar) para ver los logs con más de 30 días de antigüedad.

STEP 1 | Realice la Instalación de los complementos de Panorama.

STEP 2 | Realice la Configuración de los cortafuegos para enviar logs a Cortex Data Lake.

En los cortafuegos que ejecutan PAN-OS 8.1 o versiones posteriores, puede decidir enviar logs a Cortex Data Lake y a Panorama, y a la configuración de recopilación de logs en las instalaciones cuando selecciona la opción **Enable Duplicate Logging (Cloud and On-Premise) (Habilitar creación duplicada de logs [en la nube y localmente])**. Cuando se habilita esta opción, los cortafuegos que pertenecen a la plantilla seleccionada guardarán una copia de los logs en ambas ubicaciones. Puede seleccionar **Enable Duplicate Logging (Cloud and On-Premise) (Habilitar creación duplicada de logs [en la nube y localmente])** o **Enable Cortex Data Lake (Habilitar Cortex Data Lake)**, pero no ambas opciones.



 ©2023 Palo Alto Networks, Inc.

Comprobación del reenvío de logs a Panorama

Una vez configurado el reenvío de logs a Panorama o a Cortex Data Lake, compruebe si la configuración es correcta y se produce el reenvío.

Después de configurar el reenvío de logs a los recopiladores, los cortafuegos gestionados establecen una conexión por el protocolo de control de transmisión (transmission control protocol, TCP) a todos los recopiladores de logs configurados que se agota cada 60 segundos, pero no significa que hayan perdido la conexión a los recopiladores. Si configura el reenvío de logs a recopiladores locales o dedicados por una interfaz de Ethernet admitida, el tráfico de los cortafuegos muestra que las sesiones tienen el estado **incomplete (incompleto)** aunque se haya establecido la conexión. Si lo configura por el puerto de gestión, no se genera ningún log de tráfico de sesiones con el estado **incomplete (incompleto)**. Generan logs de tráfico de sesiones con el estado **incomplete (incompleto)** todos los cortafuegos, menos los modelos PA-5200 y PA-7000 Series.

STEP 1 | Acceda a la CLI del cortafuegos.

STEP 2 | Si configuró recopiladores de logs, verifique que cada cortafuegos tiene una lista de preferencia de reenvío de logs.

```
> show log-collector preference-list
```

Si el grupo de recopiladores tiene un único recopilador de logs, el resultado será similar a este:

```
Forward to all: No Log collector Preference List Serial Number:
 003001000024 IP Address: 10.2.133.48 IPV6 Address: unknown
```

STEP 3 | Verifique que cada cortafuegos reenvía logs.

```
> show logging-status
```

Para el reenvío correcto, el resultado indica que el agente de reenvío de logs está activo.

- En un dispositivo virtual Panorama, el agente es **Panorama**
- En los dispositivos M-Series, el agente es **LogCollector** (recopilador de logs).
- En Cortex Data Lake, el agente es **Log CollectionService** (servicio de recopilación de logs). Y

  ‘Log Collection log forwarding agent’ está activo y conectado a *<IP_address>*.

©2023 Palo Alto Networks, Inc.

STEP 4 | Visualice la tasa de creación de logs promedio. La tasa mostrada será los logs por segundo promedio durante los últimos cinco minutos.

- Si los recopiladores de logs reciben los logs, acceda a la interfaz web de Panorama, seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en el enlace **Statistics (Estadísticas)** en la columna del extremo derecho.
- Si un dispositivo virtual Panorama en modo heredado recibe los logs, acceda a la CLI de Panorama y ejecute el siguiente comando: **`debug log-collector log-collection-stats show incoming-logs`**



Este comando también funciona en un dispositivo de la serie M.

 ©2023 Palo Alto Networks, Inc.

Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs

Puede definir el modo de reenvío de logs que utilizan los cortafuegos para enviar logs a Panorama y, en el caso de una configuración de alta disponibilidad (high availability, HA), especificar qué peer de Panorama puede recibir logs. Para acceder a estas opciones, seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**, edite los ajustes de logs e informes y seleccione **Log Export and Reporting (Exportación e informes de logs)**.

- Defina el modo de reenvío de logs en el cortafuegos: Los cortafuegos pueden reenviar logs a Panorama (en lo referente al dispositivo de la serie M y el dispositivo virtual Panorama) en modo Reenvío de log en búfer o en el modo Reenvío de log en modo en vivo.

Opciones de creación de logs	Description (Descripción)
(Recomendada) **Buffered Log Forwarding from Device (Reenvío de logs en búfer desde dispositivo)** Default: Habilitado	Permite que cada cortafuegos gestionado almacene logs en búfer y envíe los logs a intervalos de 30 segundos a Panorama (no configurable por el usuario). El reenvío de logs con almacenamiento en búfer es muy valioso cuando el cortafuegos pierde la conexión con Panorama. El cortafuegos almacena las entradas de log en búfer en su disco duro local y mantiene un puntero para registrar la última entrada de log enviada a Panorama. Cuando se restablece la conexión, el cortafuegos reanuda el reenvío de logs desde donde lo dejó. El espacio en disco disponible para el almacenamiento en búfer depende de la cuota de almacenamiento de logs para el modelo de cortafuegos y el volumen de logs pendientes de sustitución. Si el cortafuegos está desconectado durante mucho tiempo y el último log reenviado se ha sustituido, todos los logs de su disco duro local se reenviarán a Panorama cuando vuelva a conectarse. Si se consume el espacio disponible del disco duro local del cortafuegos, las entradas más antiguas se eliminarán para permitir el registro de nuevos eventos.
Live Mode Log Forwarding from Device (Reenvío de logs en modo en directo desde dispositivo) Esta opción está habilitada cuando se cancela la selección de la casilla de verificación **Buffered Log Forwarding from Device (Reenvío de log en búfer desde dispositivo)**.	En el modo en directo, el cortafuegos gestionado envía cada transacción de log a Panorama al mismo tiempo que la registra en el cortafuegos.

©2023 Palo Alto Networks, Inc.

- Defina su preferencia de reenvío de logs en un dispositivo virtual Panorama en modo heredado que se ha implementado con una configuración de alta disponibilidad (HA):
  - Cuando se registre en un disco virtual, habilite el registro únicamente en el disco local del peer de Panorama principal. De manera predeterminada, ambos peers de Panorama con la configuración de HA reciben logs.

    En los cortafuegos 5200 y 7000-Series, solo reciben logs los peers activos.
  - Cuando se registre en un NFS (solo servidor ESXi), habilite los cortafuegos para que únicamente envíen los logs recién generados a un peer de Panorama secundario, que se promociona a principal, después de un fallo.

Opciones de creación de logs	Relativo a	Description (Descripción)
Only Active Primary Logs to Local Disk (Solo logs principales activos al disco local) Default: Disabled (Deshabilitado)	Dispositivo virtual Panorama en modo heredado que se registra en un disco virtual y se implementa en una configuración de alta disponibilidad (HA).	Le permite configurar únicamente el peer de Panorama principal para guardar logs en el disco local.
Get Only New Logs on Convert to Primary (Obtener únicamente nuevos logs al convertir a principal) Default: Disabled (Deshabilitado)	Dispositivo virtual Panorama en modo heredado montado en un almacén de datos del Sistema de archivos de red (NFS), se ejecuta en un servidor ESXi de VMware y se implementa en una configuración HA	Con el registro de NFS, cuando tiene un par de servidores de Panorama con una configuración de alta disponibilidad, solamente el peer de Panorama principal monta el almacén de datos de NFS. Por lo tanto, los cortafuegos solamente pueden enviar logs al peer de Panorama principal, que puede escribir en el almacén de datos de NFS. Cuando se produce una conmutación por error de HA, la opción **Get Only New Logs on Convert to Primary (Obtener únicamente nuevos logs al convertir a principal)** permite que un administrador configure los cortafuegos gestionados únicamente para enviar los logs recién generados a Panorama. Este evento se activa cuando la prioridad de Panorama activo-secundario se promociona a principal y puede empezar a registrar en NFS. Este

©2023 Palo Alto Networks, Inc.

Opciones de creación de logs	Relativo a	Description (Descripción)
		comportamiento suele habilitarse para impedir que los cortafuegos envíen grandes volúmenes de logs almacenados en búfer cuando se restablezca la conexión con Panorama después de un período de tiempo significativo.

©2023 Palo Alto Networks, Inc.

Configuración del reenvío de logs desde Panorama a destinos externos

Panorama le permite reenviar logs a servidores externos, incluidos los servidores Syslog, correo electrónico, trap SNMP y servicios basados en HTTP. La utilización de un servicio externo le permite recibir alertas de eventos importantes, archivar información monitorizada de sistema con almacenamiento dedicado a largo plazo e integrarse con herramientas de monitorización de seguridad de terceros. Además de reenviar los logs de los cortafuegos, puede reenviar los logs que generan el servidor de gestión de Panorama y los recopiladores de logs. El servidor de gestión de Panorama o Recopilador de logs que reenvía los logs los convierte a un formato apropiado para el destino (mensaje syslog, notificación por correo electrónico, trap SNMP o carga útil HTTP).



Si su servidor de gestión de Panorama es un dispositivo virtual Panorama en modo heredado, este convierte y reenvía los logs a servicios externos sin utilizar los recopiladores de logs.

También puede reenviar logs directamente desde cortafuegos a servicios externos: ver Opciones de reenvío de logs.

En un dispositivo virtual Panorama que ejecuta Panorama 5.1 o versiones posteriores, puede usar los comandos Secure Copy (SCP) de la CLI *para exportar la base de datos de logs completa a un servidor SCP e importarla a otro dispositivo virtual Panorama. Un dispositivo virtual Panorama que ejecuta Panorama 6.0 o versiones posteriores, y los dispositivos de la serie M que ejecutan cualquier versión, no admiten estas opciones debido a que la base de datos de logs en estos modelos es demasiado grande para que una exportación o importación sea conveniente.*

Para reenviar logs a servicios externos, debe configurar los cortafuegos para que reenvíen logs a Panorama. Luego, debe configurar los perfiles del servidor que definen cómo se conectan Panorama y Recopilador de logs a los servicios. Por último, asigne los perfiles del servidor a la configuración de log de Panorama y a los grupos de recopiladores.

STEP 1 | Configure los cortafuegos para reenviar logs a Panorama.

Configure el reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configure un perfil de servidor para cada servicio externo que recibirá información de logs.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** y seleccione el tipo de servidor que recibirá los datos de logs: **SNMP Trap (Trap SNMP)**, **Syslog**, **Email (Correo electrónico)** o **HTTP**.
2. Configure el perfil de servidor:
   - Configure un perfil de servidor de captura de SNMP. Para obtener más detalles sobre cómo funciona SNMP en Panorama y los recopiladores de logs, consulte la asistencia de SNMP.
   - Configure un perfil de servidor de syslog. Si el servidor Syslog requiere la autenticación de cliente, use la página **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** para crear un certificado y asegurar la comunicación Syslog por SSL.
   - Configure un perfil del servidor de correo electrónico.
   - Configure un perfil de servidor HTTP.

STEP 3 | Configure los destinos para:

- logs que generan el servidor de gestión de Panorama y los recopiladores de logs.
- logs de cortafuegos que un dispositivo virtual Panorama en modo heredado recopila.

1. Seleccione **Panorama** > **Log Settings (Configuración de log)**.
2. Seleccione **Add (Añadir)** uno o más *perfiles de la lista de coincidencias* para cada tipo de log.

   Los perfiles especifican los filtros de la consulta de log, los destinos de reenvío y las acciones automáticas, así como el etiquetado. Para cada perfil de lista de coincidencia:

   1. Introduzca un **Name (Nombre)** para identificar el perfil.
   2. Seleccione el **Log Type (Tipo de log)**.
   3. En la lista desplegable **Filter (Filtro)**, seleccione **Filter Builder (Generador de filtro)**. Especifique lo siguiente y luego seleccione **Add (Añadir)** para añadir cada consulta:

      Lógica de **Connector (Conector)** (y/o)

      Attribute (Atributo) de log

      Operator (Operador) para definir lógica de inclusión o exclusión

      Value (Valor) de atributo para coincidencia de la consulta
   4. Seleccione **Add (Añadir)** para añadir los perfiles del servidor que configuró para cada servicio externo.
   5. Haga clic en **OK (Aceptar)** para guardar el perfil.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure los destinos de los logs del cortafuegos que reciben los recopiladores de logs.

Cada grupo de recopiladores puede reenviar logs a diferentes ubicaciones. Si los recopiladores de logs son locales para un par de alta disponibilidad (HA) de servidores de gestión de Panorama, debe iniciar sesión en cada peer de HA para configurar el reenvío de logs para su grupo de recopiladores.

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y modifique el grupo de recopiladores que recibe los logs del cortafuegos.
2. (Opcional, solo reenvío de trap SNMP) Seleccione **Monitoring (Supervisión)** y configure los ajustes de SNMP.
3. Seleccione **Collector Log Forwarding (Reenvío de logs del recopilador)** y haga clic en **Add (Añadir)** para añadir los perfiles de la lista de coincidencias según sea necesario.
4. Haga clic en **OK (Aceptar)** para guardar los cambios en el grupo de recopiladores.

STEP 5 | (Solo reenvío de Syslog) Si el servidor Syslog requiere la autenticación de cliente, y los cortafuegos reenvían logs a recopiladores de logs dedicados, asigne un certificado que asegure la comunicación de Syslog por SSL.

Lleve a cabo los siguientes pasos para cada recopilador de logs dedicado:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
2. Seleccione **Certificate for Secure Syslog (Certificado para asegurar la comunicación Syslog)** y haga clic en **OK (Aceptar)**.

STEP 6 | (Solo para el reenvío de trap SNMP) Habilite su gestor SNMP para interpretar traps.

Cargue MIB compatibles y, si es necesario, confírmelas. Para ver los pasos específicos, consulte la documentación de su gestor SNMP.

STEP 7 | Confirme y verifique sus cambios de configuración.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar sus cambios en Panorama y enviar los cambios a grupos de dispositivos, plantillas y grupos de recopiladores.
2. Compruebe que los servicios externos estén recibiendo la información de los logs.
   - **Servidor de correo electrónico**: compruebe que los destinatarios especificados reciben logs como notificaciones de correo electrónico.
   - **Servidor de syslog**: consulte la documentación de su servidor syslog para comprobar que recibe logs como mensajes de syslog.
   - **Gestor SNMP**: consulte la documentación de su servidor trap SNMP para comprobar que recibe logs como mensajes de traps SNMP.
   - **Servidor HTTP**: verifique que el servidor basado en HTTP recibe logs en el formato de carga útil correcto.

 ©2023 Palo Alto Networks, Inc.

Implementaciones de recopilación de logs

Los siguientes temas describen cómo configurar la recopilación de logs en las implementaciones más típicas. Antes de empezar, Planificación de su implementación de Panorama de acuerdo con sus necesidades de logging actuales y futuras.

Todas las implementaciones en estos temas describen Panorama en una configuración de alta disponibilidad (high availability, HA). Palo Alto Networks recomienda HA porque permite la recuperación automática (en caso de una falla del sistema) de los componentes que no están guardados como parte de las copias de seguridad de configuración. En las implementaciones HA, el servidor de gestión de Panorama solo es compatible con una configuración activa/pasiva.

- Implementación de Panorama con recopiladores de logs dedicados
- Implementación de dispositivos M-Series de Panorama con recopiladores de logs locales
- Implementación de dispositivos virtuales Panorama con recopiladores de logs locales
- Implementación de dispositivos virtuales Panorama en modo heredado con recopilación de logs local

Implementación de Panorama con recopiladores de logs dedicados

Las siguientes ilustraciones muestran Panorama en una implementación de recopilación de logs distribuida. En estos ejemplos, el servidor de gestión de Panorama consta de dos dispositivos virtuales de Panorama o M-Series en modo Panorama que se implementan en una configuración de alta disponibilidad (High Availability, HA) activa/pasiva. Los cortafuegos envían logs a recopiladores de logs dedicados (dispositivos virtuales de Panorama o M-Series en el modo de recopilación de logs). Esta es la configuración recomendada si los cortafuegos generan más de 10.000 logs por segundo.

Si asigna más de un recopilador de logs a un grupo de recopiladores, consulte** Advertencias para un grupo de recopiladores con recopiladores de logs múltiples **para entender los requisitos, riesgos y mitigaciones recomendadas.

©2023 Palo Alto Networks, Inc.

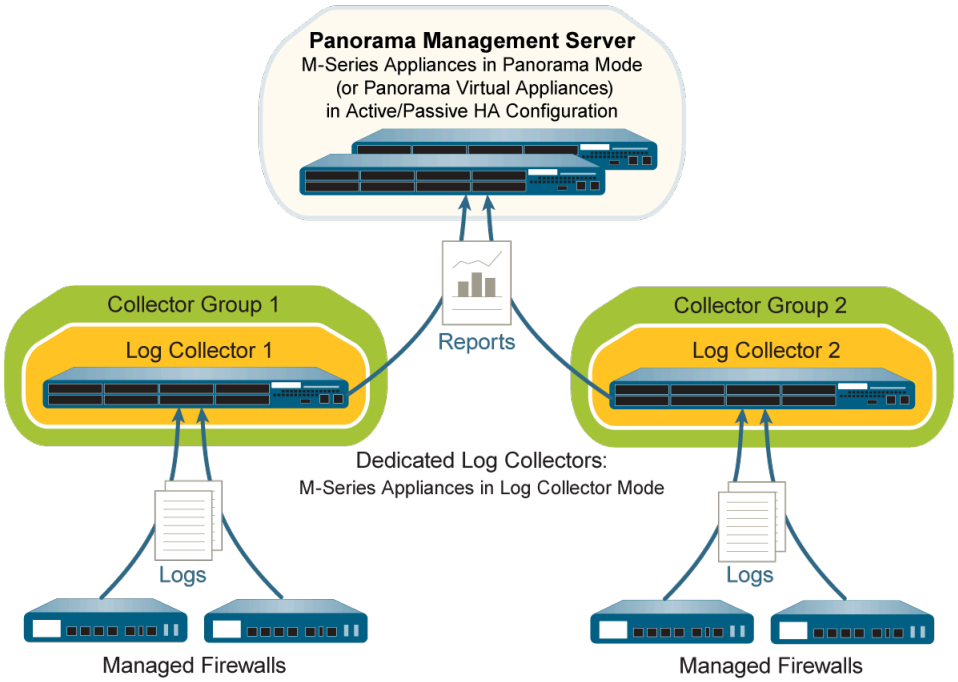


Figure 16: Un recopilador de logs dedicado por grupo de recopiladores

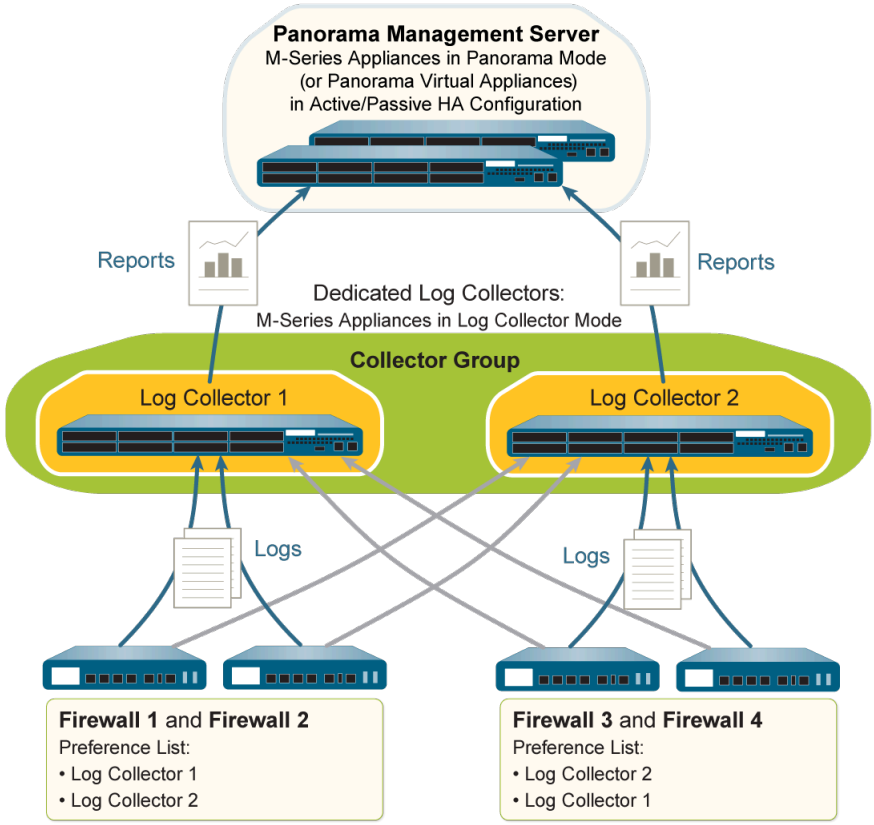


Figure 17: Varios recopiladores de logs dedicados por grupo de recopiladores

Siga estos pasos para implementar Panorama con recopiladores de logs dedicados. Omita cualquier paso que ya haya realizado (por ejemplo, la configuración inicial).

©2023 Palo Alto Networks, Inc.

STEP 1 | Realice la configuración inicial del servidor de gestión de Panorama (dispositivos virtuales o dispositivos de la serie M) y los recopiladores de logs dedicados.

Para cada dispositivo de la serie M:

1. Monte en rack el dispositivo de la serie M. Consulte la Guía de referencia de hardware serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.

   Palo Alto Networks recomienda reservar la interfaz de gestión (MGT) para el acceso administrativo a Panorama y dedicar** Interfaces de dispositivos M-Series **independientes a otros servicios de Panorama.
3. Configure todos los conjuntos. Esta tarea es necesaria para que los discos RAID estén disponibles para el logging. De manera opcional, puede añadir discos para Aumentar la capacidad de almacenamiento del dispositivo M-Series).
4. Registre Panorama e instale las licencias.
5. Instale las actualizaciones de contenido y software de Panorama.

Para cada dispositivo virtual (de haberlo):

1. Instale el dispositivo virtual Panorama.
2. Realice la configuración inicial del dispositivo virtual Panorama.
3. Registre Panorama e instale las licencias.
4. Instale las actualizaciones de contenido y software de Panorama.

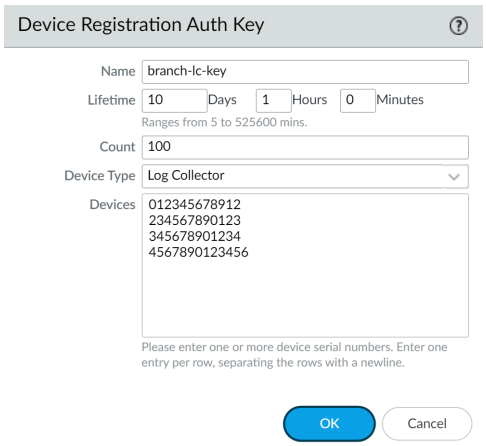
Para el servidor de gestión de Panorama (dispositivo virtual o de la serie M), también debe configurar HA en Panorama.

 ©2023 Palo Alto Networks, Inc.

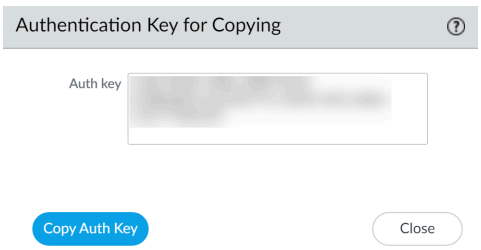
STEP 2 | En el servidor de gestión Panorama, cree una clave de autenticación de registro de dispositivo para añadir de forma segura el recopilador de logs dedicado a la gestión de Panorama.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione**Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para añadir una nueva clave de autenticación.
3. Configure la clave de autenticación.
   - **Name (Nombre)**: agregue un nombre descriptivo para la clave de autenticación.
   - **Lifetime (Duración)**: especifique la duración de la clave a fin de indicar durante cuánto tiempo puede utilizar la clave de autenticación para incorporar nuevos recopiladores de logs.
   - **Count (Conteo)**: especifique cuántas veces puede utilizar la clave de autenticación para incorporar nuevos recopiladores de logs.
   - **Device Type (Tipo de dispositivo)**: especifique que esta clave de autenticación se utiliza para autenticar solo un **recopilador de logs**.

     *Puede seleccionar **Any (Cualquiera)** para utilizar la clave de autenticación de registro de dispositivos para incorporar cortafuegos, recopiladores de logs y dispositivos WildFire.*
   - (Opcional) **Devices (Dispositivos)**: introduzca uno o más números de serie de dispositivo para especificar para qué recopiladores de logs es válida la clave de autenticación.
4. Haga clic en **OK (Aceptar)**.



5. Seleccione **Copy Auth Key (Copiar la clave de autenticación)** y **Close (Cerrar)**.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Cambie del modo Panorama al modo de recopilador de logs en cada servidor de gestión de Panorama que será un recopilador de logs dedicado.

Cambiar el modo de un dispositivo virtual de Panorama o M-Series elimina todos los datos de log existentes y las configuraciones excepto la de acceso de gestión. Tras el cambio, el dispositivo virtual de Panorama o M-Series conserva el acceso a la CLI pero pierde el acceso a la interfaz web.

1. Conéctese a Panorama de uno de estos modos:
   - (Solo dispositivos M-Series) Conecte un cable serie desde un ordenador hasta el puerto de consola del dispositivo M-Series. A continuación, utilice el software de emulación de terminal (9600-8-N-1) para conectarse.
   - Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP que especificó para la interfaz de MGT del servidor de gestión Panorama durante la configuración inicial.
2. Inicie sesión en la CLI cuando se le solicite. Utilice la cuenta y la contraseña admin predeterminadas que especificó durante la configuración inicial.
3. Para cambiar al modo de recopilación de logs, introduzca el siguiente comando:

   ```
   > request system system-mode logger
   ```
4. Ingrese **Y** para confirmar el cambio de modo. El servidor de gestión de Panorama se reinicia. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectarse a Panorama para ver la solicitud de inicio de sesión a Panorama.

   Si ve la solicitud `CMS Login`, esto significa que el recopilador de logs finalizó el reinicio. Presione Intro en la solicitud sin escribir un nombre de usuario y contraseña.
5. Vuelva a iniciar sesión en la CLI.
6. Verifique que el cambio al modo de recopilador de logs se realizó correctamente:

   ```
   > show system info | match system-mode
   ```

   Si el cambio de modo es correcto, se muestra lo siguiente:

   ```
   system-mode: logger
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | En la CLI del recopilador de logs dedicado, restablezca el estado de conexión segura.

1. Restablezca el estado de conexión segura.

   Este comando restablece la conexión del dispositivo gestionado y es irreversible.

   ```
   admin> request sc3 reset
   ```

2. Reinicie el servidor de administración en el dispositivo gestionado.

   ```
   admin> debug software restart process management-server
   ```

STEP 5 | Añada la clave de autenticación de registro del dispositivo al recopilador de logs dedicado.

```
admin> request authkey set <auth-key>
```



STEP 6 | Habilite la conectividad entre cada recopilador de logs y el servidor de gestión de Panorama.

Este paso es necesario para que pueda habilitar los discos de logs en los recopiladores de logs.

Introduzca los siguientes comandos en la CLI de cada recopilador de logs. ***<IPaddress1>*** es para la interfaz de MGT del Panorama activo y ***<IPaddress2>*** es para la interfaz de MGT del interfaz del Panorama pasivo.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 7 | Registre el número de serie de cada recopilador de logs.

Necesitará los números de serie para añadir los recopiladores de logs como recopiladores gestionados en el servidor de gestión de Panorama.

1. En la CLI de cada recopilador de logs, introduzca el siguiente comando para mostrar su número de serie.

   ```
   > show system info | match serial
   ```

2. Registre el número de serie.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Añada el nuevo recopilador de logs como recopilador gestionado.

Use la interfaz web del peer del servidor de gestión principal de Panorama para configurar un recopilador gestionado:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir el recopilador gestionado.
2. En la pestaña **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el recopilador de logs.
3. Ingrese la dirección IP o FQDN de los peers activos y pasivos de HA de Panorama en el campo **Panorama Server IP (IP de servidor de Panorama)** y en el campo **Panorama Server IP 2 (IP 2 de servidor de Panorama)** respectivamente. Estos campos son obligatorios.
4. Seleccione **Interfaces**, haga clic en **Management (Gestión)** y configure uno o ambos de los conjuntos de campo siguientes para la interfaz de MGT, según los protocolos IP de su red.

   *Si configura una **dirección IP pública** para la interfaz, los recopiladores de logs del grupo de recopiladores siempre utilizan la dirección IP pública para la comunicación dentro del grupo de recopiladores. Para asegurarse de que los recopiladores de logs de un recopilador utilizan la dirección IP privada para comunicarse, no configure una dirección IP pública.*

   - IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
5. (Opcional) Seleccione **SNMP** si va a utilizar un gestor SNMP para supervisar las estadísticas del recopilador de logs.

   La utilización de SNMP requiere pasos adicionales además de la configuración del recopilador de logs (consulte Supervisión de estadísticas de Panorama y recopiladores de logs mediante SNMP)
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

   Este paso es necesario para que pueda habilitar los discos de logs en los recopiladores de logs.
8. Verifique que la página **Panorama** > **Managed Collectors (Recopiladores gestionados)** detalle los recopiladores de logs que añadió. La columna Conectado muestra un icono de marca de verificación para indicar que el recopilador de logs está conectado a Panorama. Es posible que deba esperar unos minutos para que la página muestre el estado de conexión actualizado.

   En este punto, la columna Estado de configuración muestra Out of Sync y la columna Estado de tiempo de ejecución muestra disconnected (desconectado). El estado cambiará a In Sync (Sincronizado) y connected (conectado) después de que configure un Grupo de recopiladores (paso 9).

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Habilite los discos de logging en cada recopilador de logs.

Use la interfaz web del peer del servidor de gestión de Panorama principal para realizar estos pasos:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
2. Seleccione **Disks (Discos)**, seleccione **Add (Añadir)** para añadir cada par de discos y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 10 | (Recomendado) Configure las interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** y **Ethernet5** si recopilador de logs los usará para la **Device Log Collection (Recopilación de logs del dispositivo)** [recepción de logs del cortafuegos] y **Collector Group Communication (Comunicación del grupo de recopiladores)**.

De forma predeterminada, el recopilador de logs utiliza la interfaz de gestión para la recopilación de logs y la comunicación de grupos de recopiladores. La asignación de otras interfaces a estas funciones le permite reservar la interfaz MGT para el tráfico de gestión. En un entorno con mucho tráfico de log, considere utilizar las interfaces de 10 Gbps (**Ethernet4** y **Ethernet5**) en el dispositivo M-500 para la recopilación de logs y la comunicación del grupo de recopiladores. Para equilibrar la carga del tráfico de logs en las interfaces, puede habilitar **Device Log Collection (Recopilación de logs del dispositivo)** en múltiples interfaces.

Use la interfaz web del servidor de gestión de Panorama principal para realizar estos pasos en cada recopilador de logs:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)**, edite el recopilador de logs y seleccione **Interfaces**.

 ©2023 Palo Alto Networks, Inc.

2. Realice los siguientes pasos para cada interfaz:
   1. Haga clic en el nombre de la interfaz para editarla.
   2. Seleccione **<interface-name>** para habilitar la interfaz.
   3. Complete uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

      IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

      IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
   4. Seleccione los Servicios de gestión de dispositivos que admite la interfaz:

      Device Log Collection (Recopilación de logs del dispositivo): puede asignar una o más interfaces.

      Collector Group Communication (Comunicación del grupo de recopiladores): puede asignar solo una interfaz.
   5. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

STEP 11 | Añada un cortafuegos como un dispositivo gestionado.

Use la interfaz web del peer de servidor de gestión del Panorama principal para realizar esta tarea para cada cortafuegos que reenvíe logs a los Recopiladores de logs.

STEP 12 | Configure el grupo de recopiladores.

Si cada grupo de recopiladores tendrá solo un recopilador de logs, repita este paso para cada grupo de recopiladores antes de continuar.

Si asignará todos los recopiladores de logs a un grupo de recopiladores, realice este paso solo una vez.

Use la interfaz web del peer del servidor de gestión principal de Panorama para configurar un grupo de recopiladores:

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y haga clic en **Add (Añadir)** para añadir el grupo de recopiladores.
2. Introduzca un nombre en **Name (Nombre)** para identificar el grupo de recopiladores.
3. Seleccione **Add (Añadir)** para añadir uno o más recopiladores de logs a la lista de miembros del grupo de recopiladores.

   Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.
4. (Recomendación) Seleccione **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si añade múltiples recopiladores de logs a un

 ©2023 Palo Alto Networks, Inc.

solo grupo de recopiladores. Esta opción requiere que cada recopilador de logs tenga el mismo número de discos de creación de logs.

5. (Opcional) Seleccione **Monitoring (Supervisión)** y configure los ajustes si utilizará SNMP para supervisar las estadísticas y traps de los recopiladores de logs.
6. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y configure la lista Preferencias de reenvío de logs. Esta lista define qué cortafuegos envían los logs a qué recopiladores de logs. Asigne cortafuegos según el número de recopiladores de logs en este grupo de recopiladores:
   - **Único**: asigne los cortafuegos que reenviarán logs a ese recopilador de logs, como se muestra en Recopilador único de logs dedicado por grupo de recopiladores
   - **Múltiple**: asigne cada cortafuegos a ambos recopiladores de logs para lograr redundancia. Cuando configure las preferencias, asigne al recopilador de logs 1 la máxima prioridad para la mitad de los cortafuegos y al recopilador de logs 2 la segunda máxima prioridad para la otra mitad, como se muestra en Recopiladores de logs dedicados múltiples por grupo de recopiladores
7. Haga clic en **OK (Aceptar)** para guardar los cambios en el grupo de recopiladores.
8. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y a los grupos de recopiladores que añadió.
9. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que la configuración del recopilador de logs se sincronizó con Panorama.

   La columna Estado de configuración debe mostrar In Sync (Sincronizado) y la columna Estado de tiempo de ejecución muestra connected (conectado).

STEP 13 | Configure el reenvío de logs de los cortafuegos a Panorama.

Use la interfaz web del peer del servidor de gestión de Panorama principal para :

1. Configure el reenvío de logs a Panorama.
2. Verifique el reenvío de logs a Panorama.
3. (Opcional) Configure el reenvío de logs desde Panorama a destinos externos.

Implementación de dispositivos M-Series de Panorama con recopiladores de logs locales

Las siguientes ilustraciones muestran Panorama en una implementación de recopilación de logs centralizada. En estos ejemplos, el servidor de gestión de Panorama consta de dos dispositivos de la serie M en modo Panorama que se implementan en una configuración de alta disponibilidad (high availability, HA) activa/pasiva. Los cortafuegos envían los logs al recopilador de logs local predeterminado (preconfigurado) en cada dispositivo de la serie M de Panorama. Esta es la implementación recomendada si los cortafuegos generan hasta 10.000 logs por segundo.

 ©2023 Palo Alto Networks, Inc.

Si asigna más de un recopilador de logs a un grupo de recopiladores, consulte Advertencias para un grupo de recopiladores con recopiladores de logs múltiples *para entender los requisitos, riesgos y mitigaciones recomendadas.*

Tras realizar esta implementación, si la tasa de logs supera los 10 000 logs por segundo, Palo Alto Networks recomienda que añada recopiladores de logs dedicados (dispositivos de la serie M en el modo de recopilación de logs) como se describe en Implementación de Panorama con recopiladores de logs dedicados*. Tal expansión podría requerir una reasignación de cortafuegos de los recopiladores de logs locales a los recopiladores de logs dedicados.*

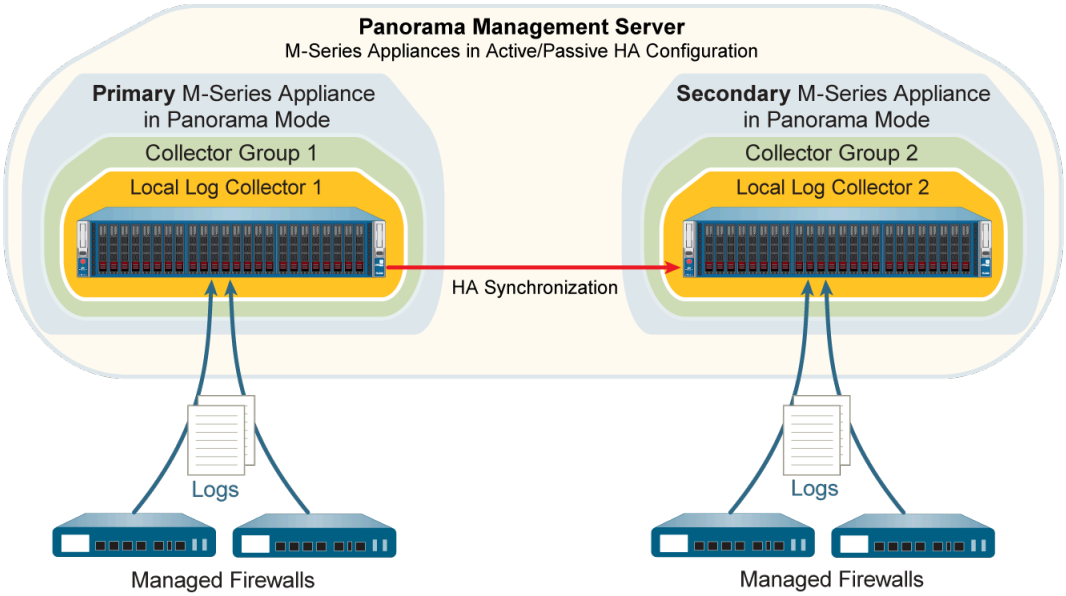


Figure 18: Un recopilador de logs local por grupo de recopiladores

©2023 Palo Alto Networks, Inc.

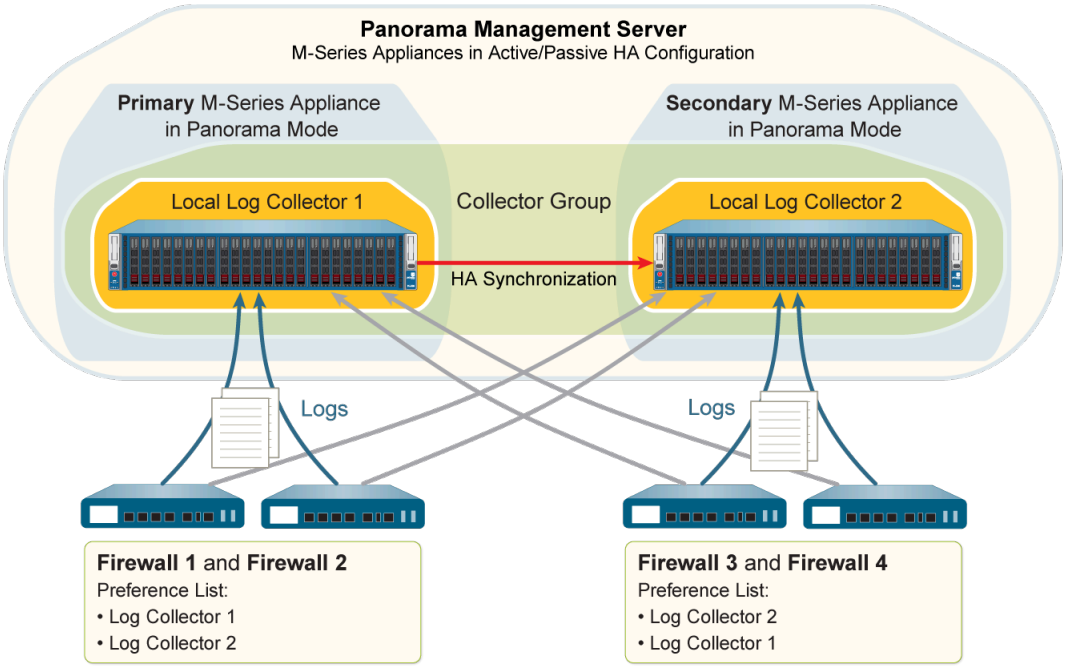


Figure 19: Varios recopiladores de logs locales por grupo de recopiladores

Siga estos pasos para implementar Panorama con recopiladores de logs locales. Omita cualquier paso que ya haya realizado (por ejemplo, la configuración inicial).

STEP 1 | Realice la configuración inicial de cada dispositivo de la serie M.

1. Monte en rack el dispositivo de la serie M. Consulte las Guías de referencia de hardware serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.

   Palo Alto Networks recomienda reservar la interfaz de gestión (MGT) para el acceso administrativo a Panorama y dedicar Interfaces de dispositivos M-Series *independientes a otros servicios de Panorama.*
3. Configure todos los conjuntos. Esta tarea es necesaria para que los discos RAID estén disponibles para el logging. De manera opcional, puede añadir discos para Aumentar la capacidad de almacenamiento del dispositivo M-Series).
4. Registre Panorama e instale las licencias.
5. Instale las actualizaciones de contenido y software de Panorama.
6. Configure HA en Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Siga estos pasos para preparar Panorama para la recopilación de logs.

1. Conéctese al Panorama principal de uno de estos modos:
   - Conecte un cable serie desde un ordenador hasta el puerto de consola del Panorama principal. A continuación, utilice el software de emulación de terminal (9600-8-N-1) para conectarse.
   - Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP que especificó para la interfaz de MGT del Panorama principal durante la configuración inicial.
2. Inicie sesión en la CLI cuando se le solicite. Utilice la cuenta y la contraseña admin predeterminadas que especificó durante la configuración inicial.
3. Habilite el Panorama principal para conectarse al Panorama secundario ingresando el siguiente comando, donde ***<IPaddress2>*** representa la interfaz de MGT del Panorama secundario:

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress2> # commit
   ```

4. Inicie sesión en la CLI del Panorama secundario.
5. Habilite el Panorama secundario para conectarse al Panorama principal introduciendo el siguiente comando, donde ***<IPaddress1>*** representa la interfaz de MGT del Panorama principal:

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress1> # commit # exit
   ```

6. En la CLI del Panorama secundario, introduzca el siguiente comando para mostrar el número de serie, y luego regístrelo:

   ```
   > show system info | match serial
   ```

   Necesitará el número de serie para añadir el recopilador de logs del Panorama secundario como un recopilador gestionado al Panorama principal.

STEP 3 | Edite el recopilador de logs que sea local para el Panorama principal.

Use la interfaz web del Panorama principal para realizar estos pasos:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y elija el recopilador de logs (local) predeterminado.
2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada par de discos de logs.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure el recopilador de logs que sea local para el Panorama secundario.

Panorama trata este recopilador de logs como remoto porque no es local para el Panorama principal. Por tanto, debe añadirlo manualmente en el Panorama principal.

Use la interfaz web del Panorama principal para configurar un Recopilador gestionado:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir el recopilador de logs.
2. Introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el recopilador de logs del Panorama secundario.
3. Ingrese la dirección IP o FQDN de los peers de HA de Panorama primario y secundario en el campo **Panorama Server IP (IP del servidor de Panorama)** y en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)** respectivamente.

   Estos campos son obligatorios.
4. Configure las **Interfaces** y configure cada interfaz que el recopilador de logs usará. La interfaz **Management (Gestión)** es obligatoria. Realice los siguientes pasos para cada interfaz:
   1. Haga clic en el nombre de la interfaz.
   2. Configure uno o ambos de los siguientes conjuntos de campos, según los protocolos IP de su red:

      IPv4: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**

      IPv6: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
   3. (Solo interfaz de gestión) Seleccione **SNMP** si va a utilizar un gestor SNMP para supervisar las estadísticas del recopilador de logs.

      La utilización de SNMP requiere pasos adicionales además de la configuración del recopilador de logs (consulte Supervisión de estadísticas de Panorama y recopiladores de logs mediante SNMP)
   4. Haga clic en **OK (Aceptar)** para guardar los cambios en la interfaz.
5. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

   Este paso es necesario para que pueda habilitar los discos de creación de logs.
7. Edite el Recopilador de logs haciendo clic en su nombre.
8. Seleccione **Disks (Discos)**, seleccione **Add (Añadir)** cada par de discos RAID y haga clic en **OK (aceptar)**.
9. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 5 | Añada un cortafuegos como un dispositivo gestionado.

Use la interfaz web de Panorama principal para realizar esta tarea para cada cortafuegos que reenvíe registros a Recopiladores de logs.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Edite el recopilador de logs predeterminado que está predefinido en el Panorama principal.

Use la interfaz web del Panorama principal para configurar un grupo de recopiladores:

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y edite el grupo de recopiladores **default (predeterminado)**.
2. Seleccione **Add (Añadir)** para añadir el recopilador de logs local del Panorama secundario a la lista de Miembros del grupo de recopiladores si está añadiendo múltiples recopiladores de logs a un solo grupo de recopiladores. Por defecto, La lista muestra el recopilador de logs local del Panorama principal porque está preasignado al grupo de recopiladores predeterminado.

   Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.
3. (Recomendación) Seleccione **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si añade múltiples recopiladores de logs a un solo grupo de recopiladores. Esta opción requiere que cada recopilador de logs tenga el mismo número de discos de creación de logs.
4. (Opcional) Seleccione **Monitoring (Supervisión)** y configure los ajustes si utilizará SNMP para supervisar las estadísticas y traps de los recopiladores de logs.
5. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y configure la lista Preferencias de reenvío de logs. Esta lista define qué cortafuegos envían los logs a qué recopiladores de logs. Asigne cortafuegos según el número de recopiladores de logs en este grupo de recopiladores:
   - **Único**: Asigne los cortafuegos que reenviarán logs al recopilador de logs local del Panorama principal, como se muestra en Recopilador de logs local único por grupo de recopiladores
   - **Múltiple**: asigne cada cortafuegos a ambos recopiladores de logs para lograr redundancia. Cuando configure las preferencias, asigne al recopilador de logs 1 la máxima prioridad para la mitad de los cortafuegos y al recopilador de logs 2 la segunda máxima prioridad para la otra mitad, como se muestra en Varios recopiladores de logs locales por grupo de recopiladores
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Configure un grupo de recopiladores que contiene el recopilador de logs del Panorama secundario.

Se requiere si cada grupo de recopiladores tiene un solo recopilador de logs.

Use la interfaz web del Panorama principal para configurar un grupo de recopiladores:

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y haga clic en **Add (Añadir)** para añadir el grupo de recopiladores.
2. Introduzca un nombre en **Name (Nombre)** para identificar el grupo de recopiladores.
3. Seleccione **Add (Añadir)** para añadir el recopilador de logs local del Panorama secundario a la lista de Miembros del grupo de recopiladores.
4. (Opcional) Seleccione **Monitoring (Supervisión)** y configure los ajustes si va a utilizar un gestor SNMP para supervisar las estadísticas y traps de los recopiladores de logs.
5. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y **Add (añadir)** para añadir una entrada a la lista Preferencias de reenvío de logs.
    1. **Modificar** en la lista Dispositivos, seleccione los cortafuegos que reenviarán los logs al recopilador de logs local del Panorama secundario (consulte Recopilador de logs local único por grupo de recopiladores), y haga clic **DE ACUERDO**.
    2. Seleccione **Add (Añadir)** para añadir al recopilador de logs local del Panorama secundario a la lista de recopiladores y haga clic en **OK (Aceptar)**.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 8 | Confirme y envíe sus cambios a la configuración de Panorama y a los grupos de recopiladores.

En la interfaz web del Panorama principal, seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y a los grupos de recopiladores que añadió.

STEP 9 | Realice una conmutación por error manual para que el Panorama secundario se active.

Use la interfaz web del Panorama principal para realizar los siguientes pasos:

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)**.
2. Haga clic en **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos operativos.

 ©2023 Palo Alto Networks, Inc.

STEP 10 | En el Panorama secundario, configure los ajustes de red del recopilador de logs que es local para el Panorama principal.

Use la interfaz web del Panorama secundario para realizar los siguientes pasos:

1. En la interfaz web de Panorama, seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador de logs que sea local para el Panorama principal.
2. Ingrese la dirección IP o FQDN de los peers de HA de Panorama primario y secundario en el campo **Panorama Server IP (IP del servidor de Panorama)** y en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)** respectivamente.

   Estos campos son obligatorios.
3. Seleccione **Interfaces**, haga clic en **Management (Gestión)** y complete uno o ambos de los siguientes conjuntos de campos (según los protocolos de IP de su red) con los valores de la interfaz de gestión (MGT) del Panorama principal:
   - **IPv4**: **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace predeterminada)**
   - **IPv6**: **IPv6 Address/Prefix Length (Dirección IPv6/longitud de prefijo)** y **Default IPv6 Gateway (Puerta de enlace IPv6 predeterminada)**
4. Haga clic en **OK (Aceptar)** para guardar los cambios.
5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y a los grupos de recopiladores que añadió.

STEP 11 | Realice una conmutación por recuperación manual para el Panorama principal se active.

Use la interfaz web del Panorama secundario para realizar los siguientes pasos:

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)**.
2. Haga clic en **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos operativos.

STEP 12 | Configure el reenvío de logs de los cortafuegos a Panorama.

Use la interfaz web de Panorama principal para :

1. Configure el reenvío de logs a Panorama.
2. Verifique el reenvío de logs a Panorama.
3. (Opcional) Configure el reenvío de logs desde Panorama a destinos externos.



*También puede asignar diferentes perfiles externos a cada peer de HA de Panorama. Por ejemplo, podría querer que cada peer reenvíe logs a un servidor Syslog diferente. Para que cada peer de Panorama reenvíe logs a servicios externos diferentes, inicie sesión en la interfaz web de cada peer, seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)**, elija el grupo de recopiladores, seleccione **Collector Log Forwarding (Reenvío de logs del recopiladores)**, asigne los perfiles del servidor y haga clic en **OK (Aceptar)**.*

 ©2023 Palo Alto Networks, Inc.

Implementación de dispositivos virtuales Panorama con recopiladores de logs locales

Puede configurar cortafuegos para enviar logs a un Recopilador de logs que se ejecuta localmente en un dispositivo virtual Panorama en modo Panorama. En una configuración de alta disponibilidad (high availability, HA), cada peer de HA puede tener un recopilador de logs local. Puede asignar los recopiladores de logs locales en los peers HA al mismo grupo de recopiladores o a grupos de recopiladores independientes, como se ilustra en las siguientes ilustraciones. Consulte Requisitos previos de configuración del dispositivo virtual Panorama para revisar los logs compatibles por segundo cuando implemente el dispositivo virtual Panorama con recopiladores de logs locales en una infraestructura virtual de VMware.

Si asigna más de un recopilador de logs a un grupo de recopiladores, consulte** Advertencias para un grupo de recopiladores con recopiladores de logs múltiples **para entender los requisitos, riesgos y mitigaciones recomendadas.

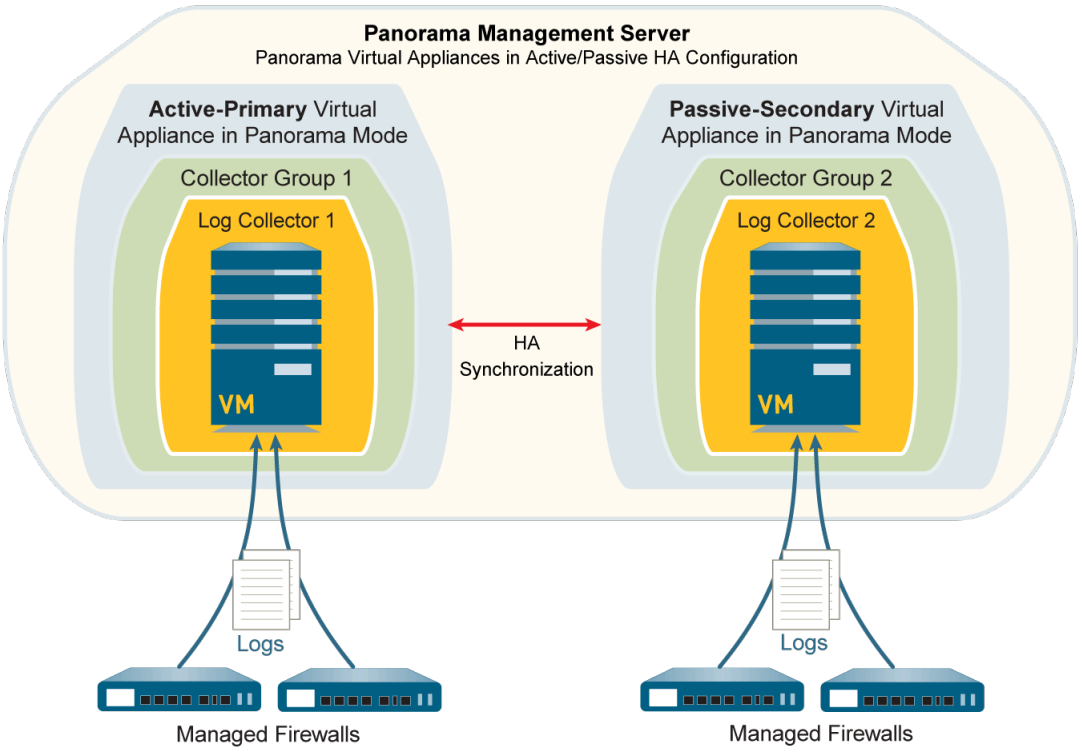


Figure 20: Recopilador de logs único por grupo de recopiladores

©2023 Palo Alto Networks, Inc.

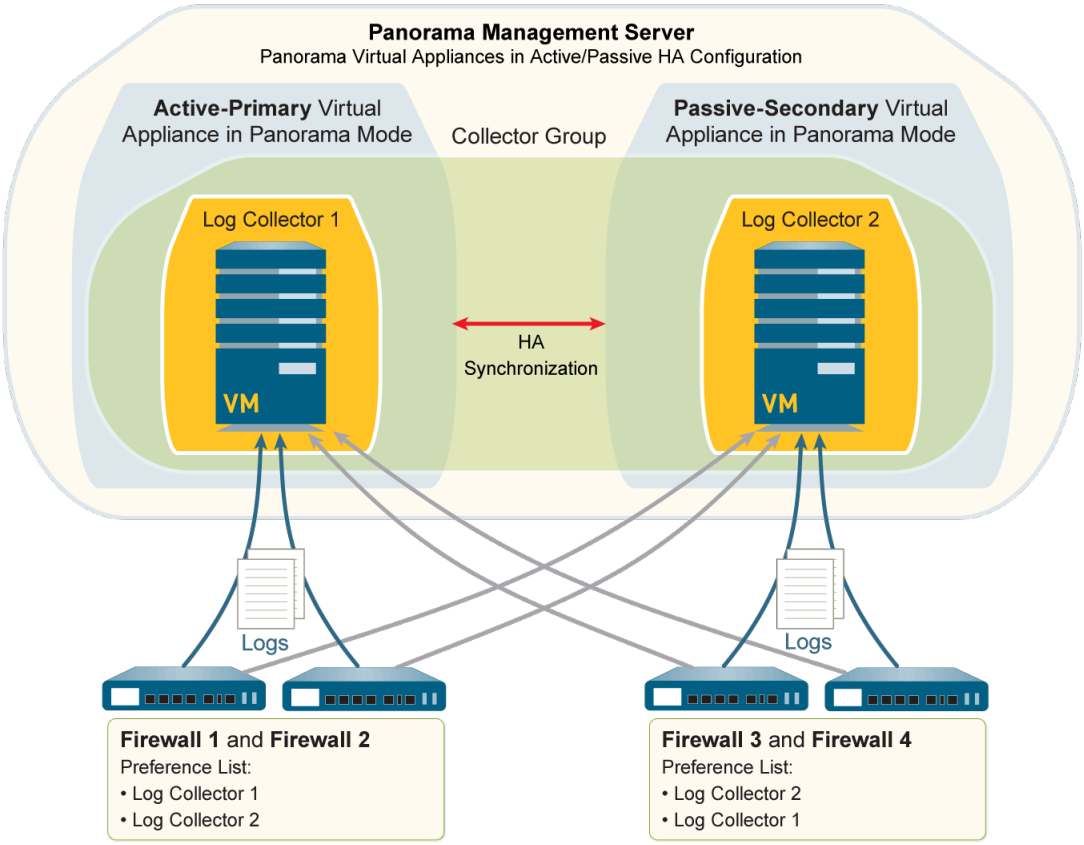


Figure 21: Recopiladores de logs múltiples por grupo de recopiladores

Siga estos pasos para implementar Panorama con recopiladores de logs locales. Omita cualquier paso que ya haya realizado (por ejemplo, la configuración inicial).

STEP 1 | Realice la configuración inicial de cada dispositivo Panorama.

1. Instale el dispositivo virtual Panorama. Debe configurar los siguientes recursos para garantizar que el dispositivo virtual se inicie en modo Panorama:
   - Disco del sistema con exactamente 81 GB de almacenamiento.
   - CPU y memoria suficientes para la cantidad de logs que Panorama recibirá y almacenará.
   - Disco de logging virtual con 2-24 TB de almacenamiento.

   Panorama divide automáticamente el nuevo disco en particiones de 2 TB, cada una de las cuales funcionará como un disco virtual separado.
2. Realice la configuración inicial del dispositivo virtual Panorama.
3. Registre Panorama e instale las licencias.
4. Instale las actualizaciones de contenido y software de Panorama.

STEP 2 | Configure los dispositivos virtuales Panorama en una configuración de HA

1. Configure HA en Panorama.
2. Prueba de conmutación por error de HA de Panorama.

©2023 Palo Alto Networks, Inc.

STEP 3 | Añada un recopilador de logs que sea local para el Panorama principal.

En la instancia principal de Panorama:

1. Registre el número de serie de Panorama.
   1. Acceda a la interfaz web de Panorama.
   2. Seleccione **Dashboard (Panel)** y registre el **Serial # (Número de serie)** en la sección de Información general.
2. Añada el recopilador de logs como recopilador gestionado.
   1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir un nuevo recopilador de logs.
   2. En la configuración **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para Panorama.
   3. Haga clic en **OK (Aceptar)** para guardar los cambios.
   4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

      Este paso es necesario para que pueda añadir los discos virtuales de logging.
3. Añada los discos virtuales de logging.
   1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en el nombre del recopilador de logs para editarlo.

      El nombre del Recopilador de logs tiene el mismo valor que el nombre de host del Panorama principal.
   2. Seleccione **Disks (Discos)** y **Add (Añadir)** para añadir los discos virtuales de logging.
   3. Haga clic en **OK (Aceptar)** para guardar los cambios.
   4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

©2023 Palo Alto Networks, Inc.

STEP 4 | Añada un recopilador de logs que sea local para el Panorama secundario.

Panorama trata este recopilador de logs como remoto porque no se ejecuta de forma local para el Panorama principal.

1. Registre el número de serie del Panorama secundario.
   1. Acceda a la interfaz web del Panorama secundario.
   2. Seleccione **Dashboard (Panel)** y registre el **Serial # (Número de serie)** en la sección de Información general.
2. Acceda a la interfaz web del Panorama principal.
3. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en **Add (Añadir)** para añadir el recopilador de logs.
4. En la configuración **General**, introduzca el número de serie (**Collector S/N [N.º de serie del recopilador]**) que registró para el Panorama secundario.
5. Ingrese la dirección IP o FQDN de los peers de HA de Panorama primario y secundario en el campo **Panorama Server IP (IP del servidor de Panorama)** y en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)** respectivamente.

   Estos campos son obligatorios.
6. Haga clic en **OK (Aceptar)** para guardar los cambios en el recopilador de logs.
7. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

   Este paso es necesario para que pueda añadir los discos virtuales de logging.
8. Edite el Recopilador de logs haciendo clic en su nombre.

   El nombre del Recopilador de logs tiene el mismo valor que el nombre de host del Panorama secundario.
9. Seleccione **Disks (Discos)** y **Add (Añadir)** para añadir los discos de log virtual y haga clic en **OK (Aceptar)**.
10. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 5 | Añada un cortafuegos como un dispositivo gestionado.

Use el Panorama principal para realizar esta tarea para cada cortafuegos que reenvíe registros a Recopiladores de logs.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Configure el grupo de recopiladores.

Realice este paso una vez si va a asignar ambos recopiladores de logs al mismo grupo de recopiladores. De lo contrario, configure un grupo de recopiladores para cada recopilador de logs.

En la instancia principal de Panorama:

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y haga clic en **Add (Añadir)** para añadir un grupo de recopiladores.
2. **Add (Añadir)** uno o ambos Recopiladores de logs como miembros de grupos de recopiladores.

   Todos los recopiladores de logs de un grupo de recopiladores deben ejecutarse en el mismo modelo de Panorama: todos los dispositivos M-700, todos los dispositivos M-600, todos los dispositivos M-500, todos los dispositivos M-300, todos los dispositivos M-200 o todos los dispositivos virtuales Panorama.
3. (Recomendación) Seleccione **Enable log redundancy across collectors (Habilitar la redundancia de logs en los recopiladores)** si añade múltiples recopiladores de logs a un solo grupo de recopiladores. Esta opción requiere que cada recopilador de logs tenga el mismo número de discos de logging virtuales.

   Al habilitar la redundancia, se duplica la cantidad de logs y el tráfico de procesamiento de logs en un Grupo de recopiladores. Si es necesario, amplíe la capacidad de almacenamiento de logs en el dispositivo virtual Panorama
4. Seleccione **Device Log Forwarding (Reenvío de logs del dispositivo)** y configure la lista Preferencias de reenvío de logs. Esta lista define qué cortafuegos envían los logs a qué recopiladores de logs. Asigne cortafuegos según el número de recopiladores de logs en este grupo de recopiladores:
   - **Único**: asigne los cortafuegos que reenviarán logs al recopilador de logs local de la instancia principal de Panorama, como se muestra en Recopilador de logs local único por grupo de recopiladores
   - **Múltiple**: asigne cada cortafuegos a ambos recopiladores de logs para lograr redundancia. Cuando configure la lista de preferencias, asigne al recopilador de logs 1 máxima prioridad para la mitad de los cortafuegos y al recopilador de logs 2, máxima prioridad para la otra mitad, como se muestra en Varios recopiladores de logs por grupo de recopiladores.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.
6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y a los grupos de recopiladores que añadió.

STEP 7 | Active una conmutación por error en el Panorama principal para que el Panorama secundario se active.

En la instancia principal de Panorama:

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)**.
2. Haga clic en **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos operativos.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Configure la conexión del Panorama secundario al recopilador de logs que es local para el Panorama principal.

En el Panorama secundario.

1. En la interfaz web de Panorama, seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y seleccione el recopilador de logs que sea local para el Panorama principal.
2. Ingrese la dirección IP o FQDN de los peers de HA de Panorama primario y secundario en el campo **Panorama Server IP (IP del servidor de Panorama)** y en el campo **Panorama Server IP 2 (IP 2 del servidor de Panorama)** respectivamente.

   Estos campos son obligatorios.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y a los grupos de recopiladores.

STEP 9 | Restaure la funcionalidad de HA en el Panorama principal.

1. Inicie sesión en la interfaz web de Panorama del Panorama principal.
2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)**.
3. **Haga que Panorama local sea funcional para una alta disponibilidad**.

STEP 10 | Active la conmutación por recuperación en el Panorama secundario para que el Panorama principal se active.

En el Panorama secundario.

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)**.
2. Haga clic en **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos operativos.
3. **Haga que Panorama local sea funcional para una alta disponibilidad** para restaurar la funcionalidad de alta disponibilidad en el Panorama secundario.
4. En el **panel**, compruebe en el widget de alta disponibilidad que el Panorama secundario sea `secundario-pasivo`.
5. Inicie sesión en la interfaz web de Panorama del Panorama principal y, en el **panel**, compruebe en el widget de alta disponibilidad que el Panorama principal sea `principal-activo`.

STEP 11 | Configure el reenvío de logs de los cortafuegos a Panorama.

En la instancia principal de Panorama, para realizar las siguientes tareas:

1. Configuración del reenvío de logs a Panorama desde los cortafuegos.
2. Verifique el reenvío de logs a Panorama.

 ©2023 Palo Alto Networks, Inc.

Implementación de dispositivos virtuales Panorama en modo heredado con recopilación de logs local

La siguiente ilustración muestra Panorama en una implementación de recopilación de logs centralizada. En este ejemplo, el servidor de gestión de Panorama consta de dos dispositivos virtuales Panorama que se implementan en una configuración de alta disponibilidad (HA) activa/pasiva. Esta configuración se ajusta a la gestión del cortafuegos dentro de una infraestructura virtual VMware en la que Panorama procesa hasta 10 000 logs por segundo. Los cortafuegos envían logs al almacén de datos de NFS (solo servidor ESXi) o al disco virtual en el servidor de gestión de Panorama. De manera predeterminada, los peers activo y pasivo reciben logs, aunque puede modificar los valores predeterminados de almacenamiento en búfer y reenvío de logs de modo que solo lo haga el peer activo. En los cortafuegos 5200 y 7000-Series, solo reciben logs los peers activos. De manera predeterminada, el dispositivo virtual Panorama en modo heredado usa aproximadamente 11 GB, de su partición de disco interno, para el almacenamiento de logs, aunque puede expandir la capacidad de almacenamiento de logs en el dispositivo virtual Panorama si es necesario.

Si la tasa de logs supera los 10.000 logs por segundo, se recomienda que realice la Implementación de Panorama con recopiladores de logs dedicados.

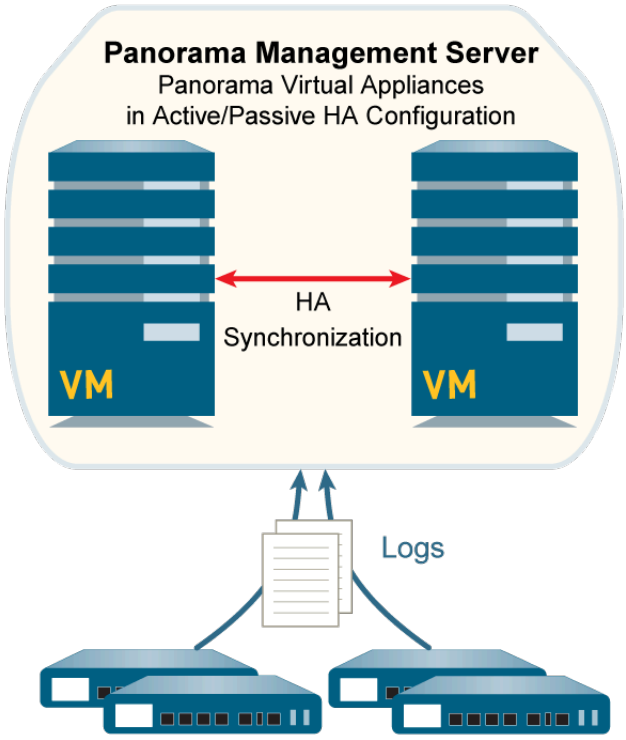


Figure 22: Dispositivos virtuales Panorama en modo heredado con recopilación de logs local

Siga estos pasos para implementar dispositivos virtuales Panorama con recopiladores de logs locales. Omita cualquier paso que ya haya realizado (por ejemplo, la configuración inicial).

©2023 Palo Alto Networks, Inc.

STEP 1 | Realice la configuración inicial de cada dispositivo Panorama.

1. Instale el dispositivo virtual Panorama. Para garantizar que el dispositivo virtual se inicie en modo Panorama, no añada un disco de log virtual durante la instalación.

   De forma predeterminada, Panorama usa una partición de 11 GB en su disco de sistema para el almacenamiento de logs. Si desea más espacio de almacenamiento, puede añadir un disco de log virtual dedicado de hasta 8 TB después de la instalación.

2. Realice la configuración inicial del dispositivo virtual Panorama.
3. Registre Panorama e instale las licencias.
4. Instale las actualizaciones de contenido y software de Panorama.

STEP 2 | Configure los dispositivos virtuales Panorama en una configuración de HA

1. Configure HA en Panorama.
2. Prueba de conmutación por error de HA de Panorama.

STEP 3 | Siga estos pasos para preparar Panorama para la recopilación de logs.

1. Añada un cortafuegos como un dispositivo gestionado para cada cortafuegos que reenviará logs a Panorama.
2. Configure el reenvío de logs a Panorama.

STEP 4 | Confirme los cambios.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Gestión de dispositivos WildFire

Puede gestionar hasta 200 dispositivos WildFire independientes y nodos de Clúster de dispositivos WildFire de forma centralizada utilizando un dispositivo virtual o M-Series de Panorama. En comparación con la gestión individual de los clústeres de dispositivos y dispositivos WildFire utilizando la CLI local, la utilización de Panorama proporciona gestión y supervisión centralizadas de varios dispositivos y clústeres de dispositivos. La gestión centralizada le permite enviar configuraciones comunes, actualizaciones de configuración y actualizaciones de software a todos o a un subconjunto de los dispositivos WildFire gestionados, lo que facilita garantizar que los dispositivos y clústeres de dispositivos de WildFire tengan configuraciones consistentes.

Cuando utiliza Panorama para gestionar clústeres de dispositivos WildFire, Panorama debe ejecutar una versión igual o posterior a la versión en los dispositivos WildFire que se gestionan.

- Agregue dispositivos independientes WildFire para gestionar con Panorama
- Configure la configuración básica del dispositivo WildFire en Panorama
- Configuración de la autenticación utilizando certificados personalizados en dispositivos y clústeres WildFire
- Elimine un dispositivo WildFire de la gestión de Panorama
- Gestión de clústeres Wildfire

Agregue dispositivos independientes WildFire para gestionar con Panorama

Puede gestionar hasta 200 dispositivos WildFire® desde un dispositivo M-Series o virtual Panorama®. El límite de 200 dispositivos WildFire es el total combinado de dispositivos autónomos y nodos de clústeres de dispositivos WildFire (si también Configura un clúster y añade nodos en Panorama).

Asegúrese de que el servidor Panorama ejecuta PAN-OS® 8.1.0 o una versión posterior de PAN-OS, y que cualquier dispositivo WildFire que agregue al servidor de gestión Panorama también ejecute PAN-OS 8.1.0 o una versión posterior.

Se utiliza una clave de autenticación de registro de dispositivo para autenticar y conectar de forma segura el servidor de gestión Panorama y el dispositivo WildFire en la primera conexión. Para configurar la clave de autenticación de registro de dispositivos, especifique la duración de la clave y la cantidad de veces que puede utilizar la clave de autenticación para incorporar nuevos dispositivos WildFire. Además, puede especificar uno o más números de serie de dispositivos WildFire para los que la clave de autenticación es válida.

La clave de autenticación caduca 90 días después de que caduque la vida útil de la clave. Después de 90 días, se le pedirá que vuelva a certificar la clave de autenticación para mantener su validez. Si no la vuelve a certificar, la clave de autenticación no será válida. Se genera un log del sistema cada vez que un dispositivo WildFire utiliza la clave de autenticación generada por Panorama. El dispositivo WildFire utiliza la clave de autenticación para autenticar Panorama cuando entrega el certificado del dispositivo que se utiliza para todas las comunicaciones posteriores.

(PAN-OS 10.2 solo) Para dispositivos WildFire que ejecutan una versión PAN-OS 10.1, Panorama que ejecuta PAN-OS 10.2 o una versión posterior admite dispositivos WildFire de incorporación que ejecutan PAN-OS 10.1.3 o una versión posterior solamente. No puede añadir un dispositivo WildFire que ejecute PAN-OS 10.1.2 o una versión anterior de PAN-OS 10.2 a la gestión de Panorama si Panorama ejecuta PAN-OS 10.2 o una versión posterior.

Panorama admite dispositivos WildFire de incorporación que ejecutan las siguientes versiones:

- ***Panorama que ejecuta PAN-OS 10.2 o una versión posterior:** dispositivos WildFire que ejecutan PAN-OS 10.1.3 o una versión posterior, y dispositivos WildFire que ejecutan PAN-OS 10.0 o una versión anterior de PAN-OS.*

No hay ningún impacto en los dispositivos WildFire ya gestionados por Panorama en la actualización a PAN-OS 10.2.

STEP 1 | Con la CLI local, verifique que cada dispositivo WildFire que desee gestionar con el servidor de gestión Panorama ejecute PAN-OS 8.1.0 o posterior.

```
admin@qa16> show system info | match version sw-version: 8.0.1-c45
 wf-content-version: 702-283 logdb-version: 8.0.15
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | En cada dispositivo Panorama que desee utilizar para administrar dispositivos WildFire, compruebe que el servidor de gestión Panorama ejecuta PAN-OS 8.1.0 o una versión posterior.

Dashboard (Panel) > **General Information (Información general)** > **Software Version (Versión del software)** muestra la versión del software en ejecución.

STEP 3 | Si no está seguro de si un dispositivo WildFire pertenece a un Clúster de dispositivos WildFire o es un dispositivo independiente en la CLI del dispositivo WildFire local, revise el **Node mode (Modo de nodo)** para asegurarse de que el estado sea **stand_alone** y revise el estado de la aplicación en **Applicationstatus** para asegurarse de que **global-db-service** y **global-queue-service** indican **ReadyStandalone**.

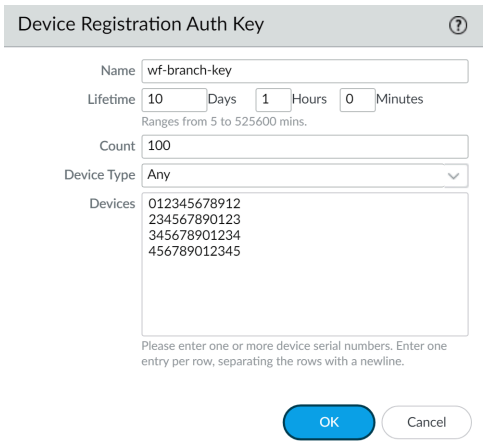
```
admin@WF-500> show cluster membership Service Summary: wfpc
 signature Cluster name: Address: 10.10.10.100 Nombre de host:
 WF-500 Nombre del nodo: wfpc-012345678901-número de serie interno:
 012345678901 Modo de nodo: stand_aloneFunción del servidor:
 Verdadera prioridad de HA: Última modificación: Lun, 06 Mar 2017
 16:34:25 -0800 Servicios: wfcore signature wfpc infra Estado del
 monitor: Serf Health Status: passing Agent alive and reachable
 Application status: global-db-service: ReadyStandalone
            wildfire-apps-service: Ready  global-queue-service:
 ReadyStandalone                       wildfire-management-service:
 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.
```

STEP 4 | Si los dispositivos WildFire que desea gestionar con Panorama son nuevos, consulte Aspectos básicos de WildFire para asegurarse de que completa los pasos básicos, como confirmar que su licencia WildFire está activa, habilitar el logging, conectar los cortafuegos a los dispositivos WildFire y configurar funciones básicas de WildFire.

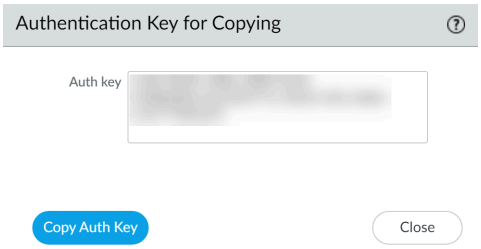
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Cree una clave de autenticación de registro de dispositivo.

1. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.
2. Configure la clave de autenticación.
   - **Name (Nombre)**: agregue un nombre descriptivo para la clave de autenticación.
   - **Lifetime (Duración)**: especifique la duración de la clave a fin de indicar durante cuánto tiempo puede utilizar la clave de autenticación para incorporar nuevos dispositivos WildFire.
   - **Count (Conteo)**: especifique cuántas veces puede utilizar la clave de autenticación para incorporar nuevos dispositivos WildFire.
   - **Device Type (Tipo de dispositivo)**: especifique que esta clave de autenticación se utiliza para autenticar **Any (Cualquier)** dispositivo.
   - (Opcional) **Devices (Dispositivos)**: introduzca uno o más números de serie de dispositivo para especificar para qué dispositivos WildFire es válida la clave de autenticación.
3. Haga clic en **OK (Aceptar)**.



4. Seleccione **Copy Auth Key (Copiar la clave de autenticación)** y **Close (Cerrar)**.



STEP 6 | En la CLI local de cada dispositivo WildFire, el servidor de Panorama gestionará, configurará la dirección IP del servidor Panorama y añadirá la clave de autenticación de registro de dispositivos.

Antes de registrar los dispositivos WildFire independientes en un dispositivo Panorama, debe configurar la dirección IP de Panorama o el FQDN y añadir la clave de autenticación de registro de dispositivos en cada uno de los dispositivos WildFire. Esto permite que cada dispositivo WildFire se conecte de forma segura al dispositivo Panorama que gestiona el dispositivo WildFire.

 ©2023 Palo Alto Networks, Inc.

La clave de autenticación de registro de dispositivos solo se utiliza para la conexión inicial al servidor de Panorama.

1. Configure la dirección IP o el FQDN de la interfaz de gestión para el servidor principal de Panorama.

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. Si usa un dispositivo Panorama de copia de seguridad para alta disponibilidad (recomendado), configure la dirección IP o FQDN de la interfaz de gestión del servidor de Panorama de copia de seguridad:

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address | FQDN>
```

3. Añada la clave de autenticación de registro del dispositivo.

```
admin> request authkey set <auth-key>
```



STEP 7 | Registre los dispositivos WildFire en el dispositivo Panorama principal.

1. Desde la interfaz web de Panorama, **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y **Add Appliance (Añadir dispositivo)**.
2. Introduzca el número de serie de cada dispositivo WildFire en una nueva línea. Si no tiene una lista de números de serie, en cada dispositivo WildFire, ejecute:

```
admin@WF-500> show system info | match serial serial:
 012345678901
```

   Varios comandos de la CLI local muestran el número de serie del dispositivo WildFire, incluido **show cluster membership**.
3. Haga clic en **OK (Aceptar)**.

   Si está disponible, se muestra la información sobre la configuración confirmada en los dispositivos WildFire, como las direcciones IP y la versión de software.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | (Opcional) Importe configuraciones de dispositivos WildFire al dispositivo Panorama.

1. Seleccione los dispositivos que tienen configuraciones que desea importar de la lista de dispositivos WildFire gestionados.
2. **Import Config (Importar configuración)**.
3. Seleccione **Yes (Sí)**.

   La importación de configuraciones actualiza la información mostrada y hace que las configuraciones importadas formen parte de la configuración candidata del dispositivo Panorama.
4. Seleccione **Commit to Panorama (Confirmar en Panorama)** para hacer que las configuraciones importadas del dispositivo WildFire sean parte de la configuración de ejecución de Panorama.

STEP 9 | Configure o confirme la configuración de las interfaces del dispositivo WildFire.

Cada dispositivo WildFire tiene cuatro interfaces: **Management (Gestión)** (Ethernet0), **Analysis Network Environment (Entorno de red de análisis)** (Ethernet1), **Ethernet2**y **Ethernet3**.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un dispositivo WildFire.
2. Seleccione **Interfaces**.
3. Seleccione una interfaz para configurarla o editarla. Puede habilitar la interfaz, establecer la velocidad y dúplex, la dirección IP y la máscara de red, la puerta de enlace predeterminada, la MTU, el servidor DNS, el estado del enlace y los **Management Services (Servicios de gestión)** para cada interfaz. También puede **Add (Añadir)** direcciones IP permitidas para que una interfaz acepte el tráfico solo desde direcciones especificadas.

   Las interfaces **Analysis Network Environment (Entorno de red de análisis)**, **Ethernet2** y **Ethernet3** admiten solo **Ping** como un opción de **Management Services (Servicios de gestión)**.

   La interfaz de **Management (Gestión)** admite **Ping**, **SSH** y **SNMP** como opciones de **Management Services (Servicios de gestión)**. Además, la interfaz de **Management (Gestión)** admite la configuración del servidor proxy en caso de que no sea posible una conexión directa a internet.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 10 | Confirme la configuración en el dispositivo Panorama y envíelo al dispositivo o en varios dispositivos.

1. **Commit and Push (Confirmar y enviar)**.
2. Si hay configuraciones en el dispositivo Panorama que no desea enviar, seleccione **Edit Selections (Editar selecciones)** para elegir los dispositivos a los que desea enviar las configuraciones. La configuración que se envía sobrescribe la configuración en ejecución en un dispositivo WildFire.

©2023 Palo Alto Networks, Inc.

STEP 11 | Verifique la configuración.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)**.
2. Verifique los siguientes campos:
   - **Connected (Conectado)**: el estado es **Connected (Conectado)**.
   - **Role (Función)**: la función de cada dispositivo WildFire es **Standalone (Independiente)**.
   - **Config Status (Estado de configuración)**: el estado es `In Sync (En sincronización)`.
   - **Last Commit State (Último estado de confirmación)**: `Commitsucceeded (Confirmación exitosa)`.

©2023 Palo Alto Networks, Inc.

Configure la configuración básica del dispositivo WildFire en Panorama

La configuración de ajustes básicos como por ejemplo la actualización de contenido y los servidores en la nube de WildFire, los servicios en la nube de WildFire, el logging, la autenticación, etc., es similar a la forma en que se realiza la Configuración de los ajustes generales del clúster en Panorama. En lugar de seleccionar un clúster y configurar los ajustes en el clúster, seleccione un dispositivo WildFire y configure los ajustes individuales para ese dispositivo. Seleccione y configure cada dispositivo WildFire que añada a Panorama.

La configuración del dispositivo WildFire describe cómo integrar un dispositivo WildFire en una red y realizar una configuración básica con la CLI, pero los conceptos son los mismos que realizar la configuración básica con Panorama.

Muchos ajustes se completan previamente con los valores predeterminados, la información de configuraciones previamente existentes en el dispositivo WildFire o los ajustes que configuró al añadir el dispositivo WildFire a Panorama.

- Configuración de la autenticación para un dispositivo WildFire

Configuración de la autenticación para un dispositivo WildFire

Cree y configure la autenticación mejorada para su dispositivo WildFire. Para ello, configure usuarios administrativos locales con parámetros de autenticación detallados y aproveche RADIUS, TACAS + o LDAP para la autorización y autenticación.

Cuando se configura y envía administradores desde Panorama, se sobrescriben los administradores existentes en el dispositivo WildFire por los que configure en Panorama.

- Configuración de una cuenta administrativa para un dispositivo WildFire
- Configuración de la autenticación RADIUS para un dispositivo WildFire
- Configuración de la autenticación TACACS+ para un dispositivo WildFire
- Configuración de la autenticación LDAP para un dispositivo WildFire

Configuración de una cuenta administrativa para un dispositivo WildFire

Cree uno o más administradores con parámetros de autenticación detallados para que su dispositivo WildFire los administre desde el servidor de gestión Panorama™. Además, puede configurar administradores locales desde Panorama que se pueden configurar directamente en la CLI del dispositivo WildFire. Sin embargo, enviar nuevos cambios de configuración a un dispositivo WildFire sobrescribe a los administradores locales con los administradores configurados para el dispositivo WildFire.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Agregue dispositivos independientes WildFire para gestionar con Panorama.

©2023 Palo Alto Networks, Inc.

STEP 3 | (Opcional) Configure un perfil de autenticación para definir el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores que acceden a la CLI del dispositivo WildFire.

STEP 4 | Configure una o más cuentas de administrador según sea necesario.

Las cuentas de administrador creadas en Panorama se importan posteriormente al dispositivo WildFire y se administran desde Panorama.

Debe configurar la cuenta administrativa con privilegios de función de administrador de Superuser (Superusuario) para configurar correctamente la autenticación del dispositivo WildFire.

STEP 5 | Configure la autenticación para el dispositivo WildFire.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un dispositivo WildFire añadido anteriormente.
2. (Opcional) Seleccione el **perfil de autenticación** que configuró en el paso anterior.
3. Configure la **configuración de tiempo de espera** de autenticación para el dispositivo WildFire.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

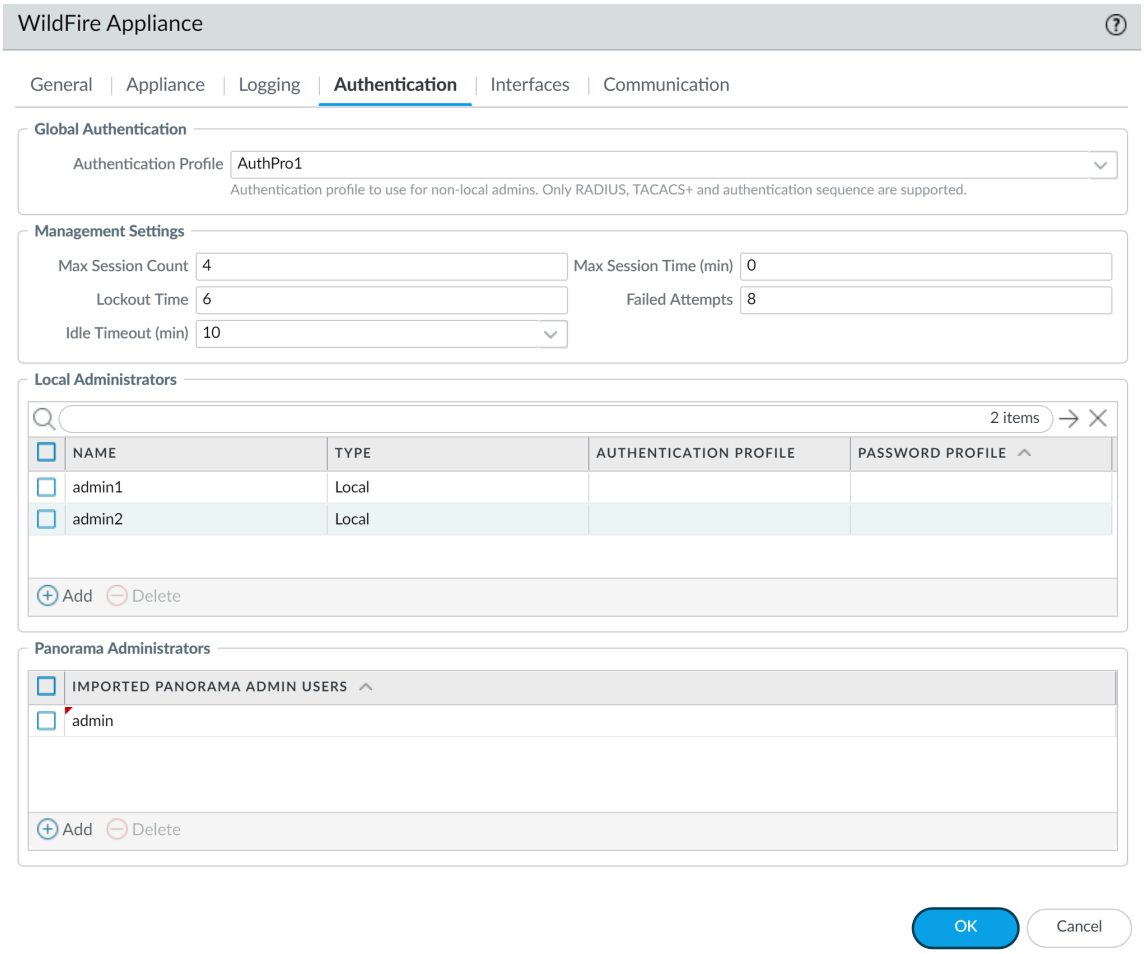
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos para el dispositivo WildFire. Estos administradores son específicos del dispositivo WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del dispositivo WildFire.



STEP 6 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 7 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación RADIUS para un dispositivo WildFire

Utilice un servidor RADIUS para autenticar el acceso administrativo a la CLI del dispositivo WildFire. También puede definir Atributos específicos de proveedor (VSA) en el servidor RADIUS para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y el servidor de gestión Panorama™.

©2023 Palo Alto Networks, Inc.

Importe el diccionario de RADIUS de Palo Alto Networks al servidor RADIUS con objeto de definir los atributos de autenticación necesarios para facilitar la comunicación entre Panorama y dicho servidor.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Agregue dispositivos independientes WildFire para gestionar con Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configuración de la autenticación RADIUS

Las cuentas de administrador configuradas para la autenticación RADIUS deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para el dispositivo WildFire.*

1. Añada un perfil de servidor RADIUS.

   El perfil define cómo se conecta el dispositivo WildFire al servidor RADIUS.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** y haga clic en **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que el dispositivo Panorama utiliza para autenticarse en el servidor RADIUS.

      *Seleccione **CHAP** si el servidor RADIUS admite ese protocolo; es más seguro que **PAP**.*

   5. Seleccione **Add (Añadir)** para añadir cada servidor RADIUS e ingrese lo siguiente:
      1. **Name (Nombre)** para identificar el servidor.
      2. **La dirección IP o FQDN del** servidor RADIUS.
      3. **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. Port (Puerto) **del servidor** para las solicitudes de autenticación (el valor predeterminado es 1812).
   6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor RADIUS a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
   3. Configure el **Type (Tipo)** en **RADIUS**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from RADIUS (Recuperar grupo de usuarios desde RADIUS)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor RADIUS.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
   6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el dispositivo WildFire.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un dispositivo WildFire añadido anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Configure la **configuración de tiempo de espera** de autenticación para el dispositivo WildFire.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

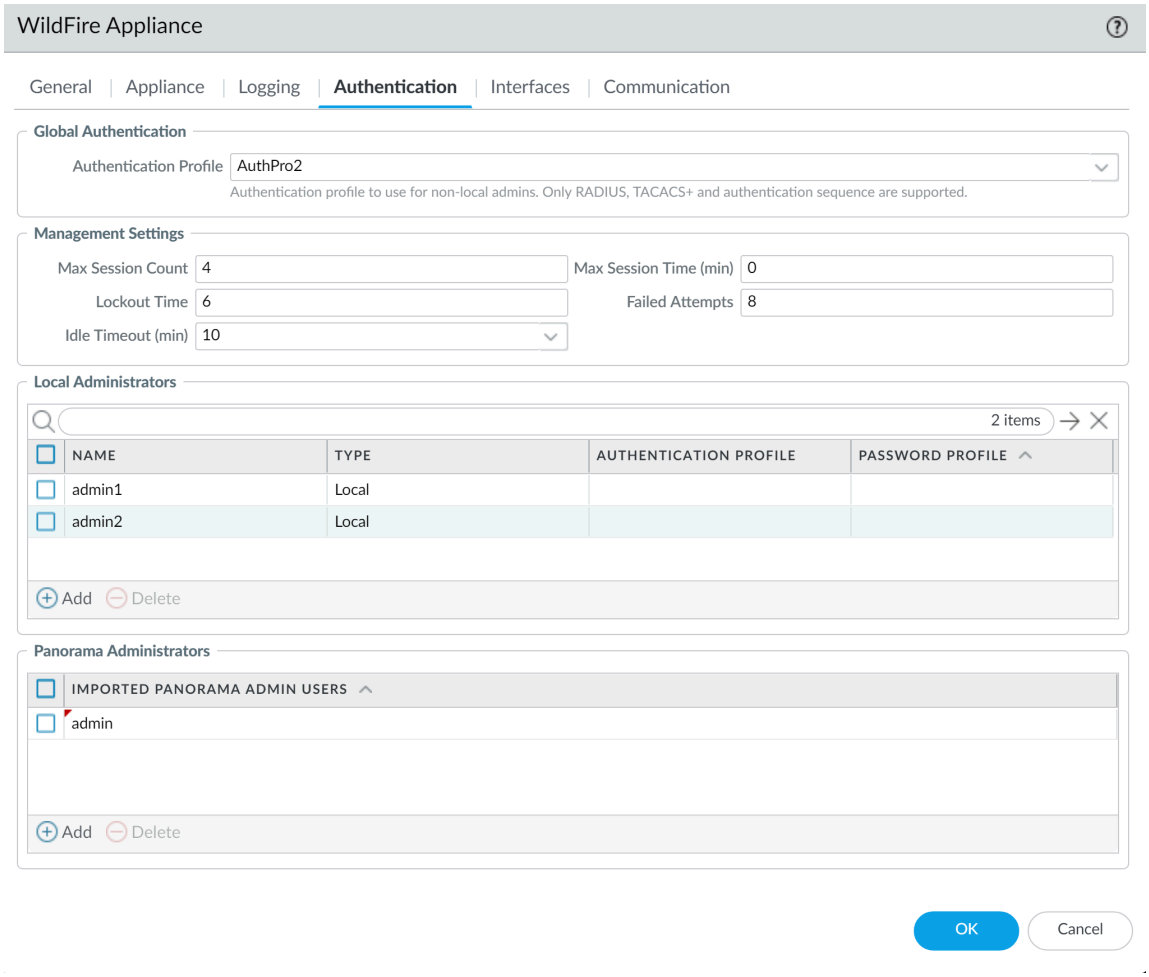
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos para el dispositivo WildFire. Estos administradores son específicos del dispositivo WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del dispositivo WildFire.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación TACACS+ para un dispositivo WildFire

Puede usar un servidor TACACS+ para autenticar el acceso administrativo a la CLI de dispositivo Panorama. También puede definir Atributos específicos de proveedor (VSA) en el servidor TACACS+ para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Agregue dispositivos independientes WildFire para gestionar con Panorama.

©2023 Palo Alto Networks, Inc.

STEP 3 | Configure la autenticación TACACS+.

Las cuentas de administrador configuradas para la autenticación TACACS+ deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para el dispositivo WildFire.*

1. Añada un perfil de servidor TACACS+.

   El perfil define cómo se conecta el dispositivo WildFire al servidor TACACS+.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACACS+** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que Panorama utiliza para autenticarse en el servidor TACACS+.
   5. Seleccione **CHAP** si el servidor TACACS+ admite ese protocolo; es más seguro que **PAP**.
   6. Seleccione **Add (Añadir)** para añadir cada servidor TACACS+ e introduzca lo siguiente:
      1. **Name (Nombre)** para identificar el servidor.
      2. **servidor TACACS+**.
      3. **Secret (Secreto)/Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. Port (Puerto) **del servidor** para las solicitudes de autenticación (el valor predeterminado es 49).
   7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor TACACS+ a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil.
   3. Configure el **Type (Tipo)** en **TACACS+**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from TACACS+ (Recuperar grupo de usuarios desde TACACS+)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor TACACS+.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
   6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el dispositivo WildFire.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un dispositivo WildFire añadido anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Configure la **configuración de tiempo de espera** de autenticación para el dispositivo WildFire.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

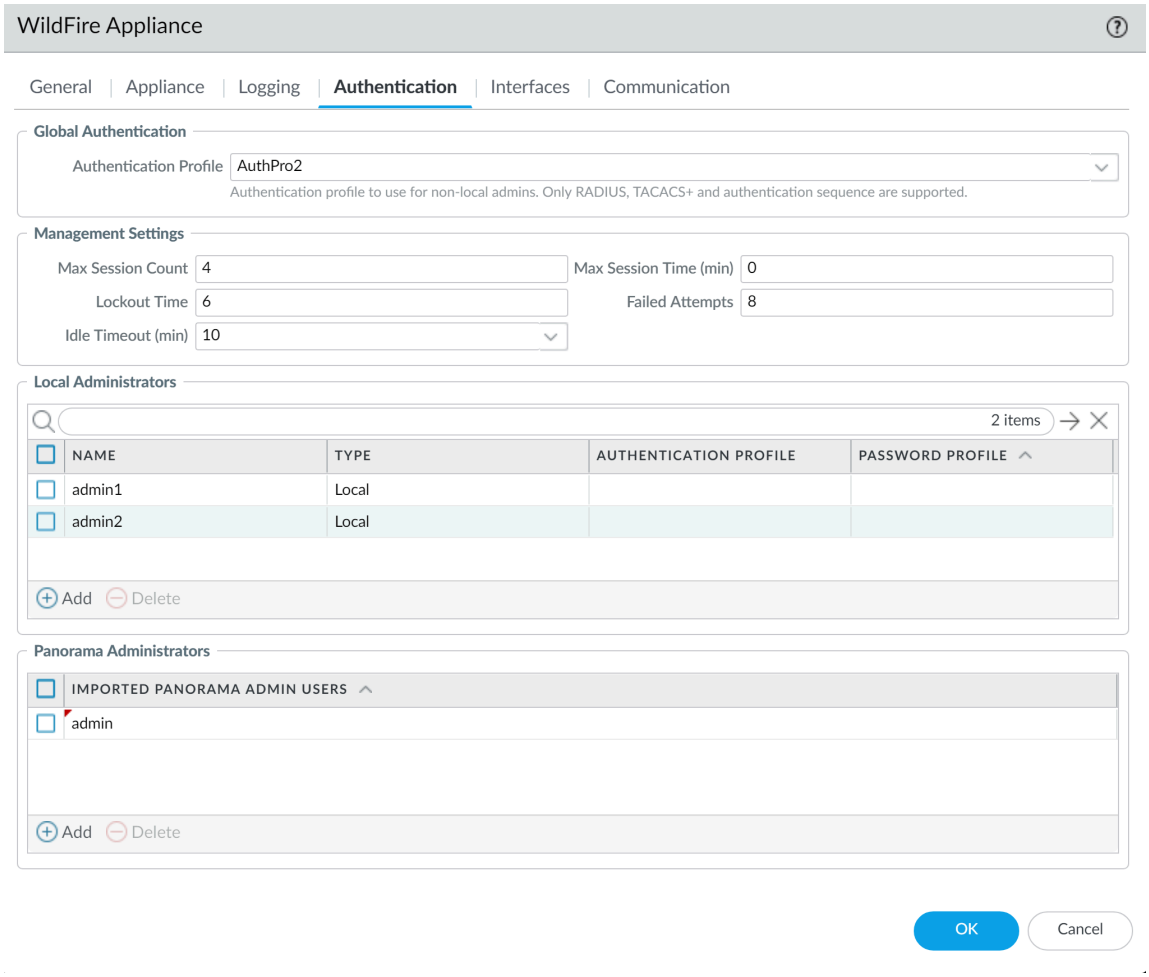
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos para el dispositivo WildFire. Estos administradores son específicos del dispositivo WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del dispositivo WildFire.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación LDAP para un dispositivo WildFire

Puede utilizar LDAP para autenticar los usuarios finales que acceden a la CLI del dispositivo WildFire.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Agregue dispositivos independientes WildFire para gestionar con Panorama.

©2023 Palo Alto Networks, Inc.

STEP 3 | Añada un perfil de servidor LDAP.

El perfil define cómo se conecta el dispositivo WildFire al servidor LDAP.

Las cuentas de administrador configuradas para la autenticación LDAP deben tener privilegios de función de administrador de Superuser (Superusuario) para configurar correctamente la autenticación para el dispositivo WildFire.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **LDAP** y haga clic en **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. **Add (Añada)** los servidores LDAP (máximo de cuatro). Para cada servidor, ingrese un nombre en **Name** (para identificar al servidor), una dirección IP del **LDAP Server (Servidor LDAP)** o FQDN, y un **Port (Puerto)** para el servidor (el valor predeterminado es 389).

   Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección de servidor tenga efecto.
4. Seleccione el **Type (Tipo)** de servidor.
5. Seleccione el **DN base**.

   Para identificar el DN base de su directorio, abra el complemento de la consola de administración de Microsoft **Active Directory Domains and Trusts (Dominios y confianzas de Active Directory)** y use el nombre del dominio de nivel superior.
6. Introduzca **Bind DN (DN de enlace)** y **Password (Contraseña)** para permitir que el servicio de autenticación autentique el cortafuegos.

   La cuenta DN de enlace debe tener permiso para leer el directorio LDAP.
7. Ingrese el **Bind Timeout (Tiempo de espera de enlace)** y el **Search Timeout (Tiempo de espera de búsqueda)** en segundos (el valor predeterminado es 30 para ambos).
8. Especifique el **intervalo de reintento** en segundos (el valor predeterminado es 60).
9. (Opcional) Si desea que el endpoint use SSL o TLS para una conexión más segura con el servidor del directorio, habilite la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)** (está habilitada por defecto). El protocolo que usa el endpoint depende del puerto del servidor:
   - 389 (predeterminado): TLS (específicamente, el dispositivo WildFire usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).
   - 636—SSL
   - Cualquier otro puerto: el dispositivo WildFire primero intenta utilizar TLS. Si el servidor de directorio no es compatible con TLS, el dispositivo WildFire recurre a SSL.
10. (Opcional) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar la verificación, debe seleccionar también la opción **Require SSL/TLS**

 ©2023 Palo Alto Networks, Inc.

secured connection (Requerir conexión segura de SSL/TLS). Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:

- Está en la lista de certificados de Panorama: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Si es necesario, importe el certificado a Panorama.
- El firmante del certificado está en la lista de autoridades de certificación confiables: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.

11. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 4 | Configure la autenticación para el dispositivo WildFire.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un dispositivo WildFire añadido anteriormente.
2. Configure la **configuración de tiempo de espera** de autenticación para el dispositivo WildFire.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que el dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
3. Añada los administradores del dispositivo WildFire.

   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la

 ©2023 Palo Alto Networks, Inc.

confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **admin1** como administrador local y de Panorama.

- Configure los administradores locales.

  Configure nuevos administradores exclusivos para los dispositivos WildFire. Estos administradores son específicos del dispositivo WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

  1. **Añada** uno o más administradores locales nuevos.
  2. Especifique un **nombre** para el administrador local.
  3. Asigne un **perfil de autenticación** creado anteriormente.

     Los perfiles de autenticación LDAP solo son compatibles con administradores locales individuales.
  4. Habilite (marque) **Use Public Key Authentication (SSH) [Usar autenticación de clave pública (SSH)]** para importar un archivo de clave pública para la autenticación.
  5. Seleccione un **perfil de contraseña** para establecer los parámetros de vencimiento.

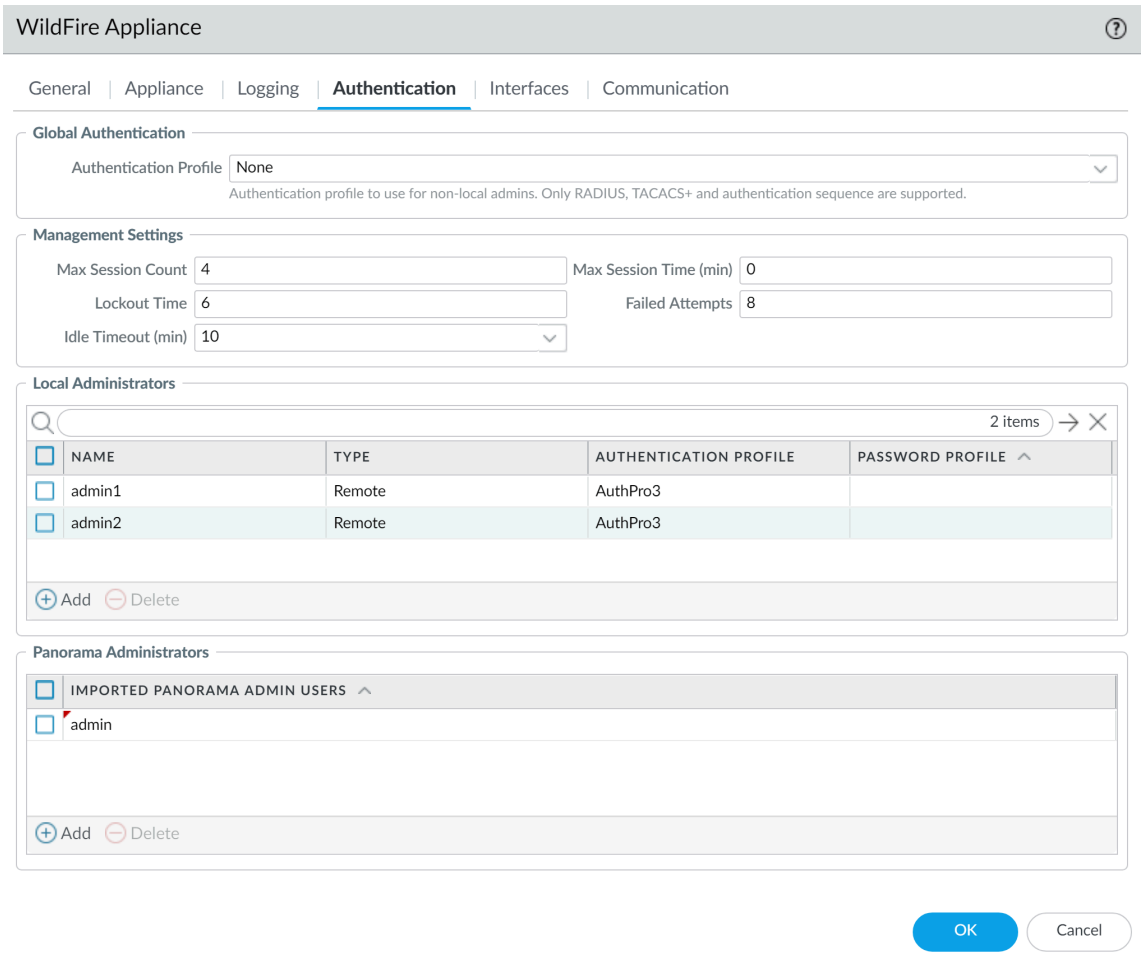
- Importación de administradores de Panorama existentes

  Importe administradores existentes configurados en Panorama. Estos administradores se configuran y administran en Panorama y se importan al dispositivo WildFire.

  1. **Añada** un administrador de Panorama existente.

4. Haga clic en **OK (Aceptar)** para guardar la configuración de autenticación del dispositivo WildFire.

©2023 Palo Alto Networks, Inc.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

©2023 Palo Alto Networks, Inc.

Configuración de la autenticación utilizando certificados personalizados en dispositivos y clústeres WildFire

De manera predeterminada, un dispositivo WildFire® utiliza certificados predefinidos para la autenticación mutua con otros cortafuegos y dispositivos Palo Alto Networks® con el fin de establecer conexiones SSL que se usan 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 su dispositivo WildFire o clúster WildFire gestionado por Panorama™, y los cortafuegos. Puede generar estos certificados localmente en Panorama o en el cortafuegos, obtenerlos desde una autoridad de certificados (certificate authority, CA) de confianza de terceros u obtener los certificados de una infraestructura de clave privada (private key infrastructure, PKI) empresarial.

Para obtener más información sobre la utilización de los certificados personalizados, consulte ¿Cómo se autentican mutuamente las conexiones SSL/TLS?

- Configuración de un certificado personalizado para un dispositivo WildFire gestionado de Panorama
- Configuración de la autenticación con un certificado personalizado para un clúster WildFire
- Aplicación de certificados personalizados en un dispositivo WildFire configurado en Panorama

Configuración de un certificado personalizado para un dispositivo WildFire gestionado de Panorama

Si utiliza Panorama™ para gestionar su dispositivo WildFire® o clúster WildFire, puede configurar la autenticación de certificados personalizados en la interfaz web de Panorama en lugar de utilizar la CLI de los dispositivos WildFire. El cortafuegos o Panorama utiliza esta conexión para reenviar muestras a WildFire para su análisis.

Este procedimiento describe cómo instalar un certificado único en un dispositivo WildFire único. Si el dispositivo WildFire forma parte de un clúster, ese dispositivo y cada miembro del clúster cuenta con un certificado cliente único. Para implementar un certificado único en todos los dispositivos WildFire en el clúster, consulte Configuración de la autenticación con un certificado personalizado para un clúster WildFire.

STEP 1 | Obtenga pares de claves y certificados de autoridades de certificados (certificate authority, CA) para el dispositivo WildFire y el cortafuegos.

STEP 2 | Importe el certificado de CA para validar la identidad del cortafuegos y el par de claves para el dispositivo WildFire.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Import (Importar)**.
2. Importe el certificado de CA y el par de claves en Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 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 autentican entre sí.

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

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

STEP 4 | Configure un perfil SSL/TLS para el dispositivo WildFire.

*PAN-OS 8.0 y las versiones posteriores admiten solo TLS 1.2 o superior, de modo que usted debe configurar la versión máxima en **TLS 1.2** o **max (máximo)**.*

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Lleve a cabo la Configuración de un perfil de servicio SSL/TLS para definir el certificado y el protocolo que el dispositivo WildFire y sus cortafuegos utilizan para los servicios SSL/TLS.

STEP 5 | Configure la comunicación de servidor segura en WildFire.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** o **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un clúster o dispositivo.
2. Seleccione **Communication (Comunicación)**.
3. Habilite la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
4. Seleccione el **SSL/TLS Service Profile**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre el dispositivo WildFire y el cortafuegos o Panorama.
5. Seleccione el **Certificate Profile (Perfil de certificado)** que configuró para la comunicación entre el dispositivo WildFire y el cortafuegos o Panorama.
6. Verifique que la opción **Custom Certificates Only (Solo los certificados personalizados)** esté deshabilitada (sin marca). Esto le permite al dispositivo WildFire continuar comunicándose con los cortafuegos con los certificados predefinidos mientras migra a los certificados personalizados.
7. (Opcional) Configure una lista de autorizaciones.
   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Selecciona el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** configurado en el perfil del certificado como el tipo de identificador.
   3. Introduzca el Nombre común si el identificador es Sujeto una dirección IP, nombre de host o correo electrónico si el identificador es Nombre alternativo del sujeto.
   4. Haga clic en **OK (Aceptar)**.
   5. Habilite **Check Authorization List (Comprobar lista de autorización)** para aplicar la lista.
8. Haga clic en **OK (Aceptar)**.
9. **Commit (Confirmar)** los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Importe el certificado de CA para validar el certificado para el dispositivo de WildFire.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Importe el certificado de CA.

STEP 7 | Configure un certificado local o SCEP para el cortafuegos.

- Si está utilizando un certificado local, importe el par de claves para el cortafuegos.
- Si está utilizando SCEP para el certificado del cortafuegos, configure un perfil SCEP.

STEP 8 | Configure el certificate profile (perfil de certificado) para el cortafuegos o Panorama. Puede configurar este perfil en cada cortafuegos cliente o dispositivo Panorama individualmente o puede utilizar una plantilla para enviar la configuración desde Panorama a los cortafuegos gestionados.

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

STEP 9 | Implemente certificados personalizados en cada cortafuegos o dispositivo Panorama.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** para un cortafuegos o **Panorama** > **Setup (Configuración)** > **Management (Gestión)** para Panorama y haga clic en **Edit (Editar)** para editar los ajustes de Secure Communication (Comunicación segura).
3. Seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)**.
4. En la configuración Customize Communication (Personalizar comunicación), seleccione **WildFire Communication (Comunicación de WildFire)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

STEP 10 | Después de implementar los certificados personalizados en todos los dispositivos gestionados, aplique la autenticación de certificados personalizados.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** o **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione un clúster o dispositivo.
3. Seleccione **Communication (Comunicación)**.
4. Seleccione **Custom Certificate Only (Certificado personalizado únicamente)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

Después de confirmar este cambio, WildFire inicia inmediatamente la aplicación de certificados personalizados.

 ©2023 Palo Alto Networks, Inc.

Configuración de la autenticación con un certificado personalizado para un clúster WildFire

En lugar de asignar certificados únicos a cada dispositivo WildFire® en un clúster, puede asignar un solo certificado de cliente compartido al clúster WildFire completo que, a su vez, le permite enviar un solo certificado a todos los dispositivos WildFire en el clúster en lugar de configurar certificados separados para cada miembro del clúster. Dado que los dispositivos WildFire individuales comparten un certificado cliente, debe configurar un nombre de host (nombre DNS) único para cada dispositivo WildFire. Luego, puede añadir todos los nombres de host como atributos del certificado al certificado compartido o utilizar una cadena de comodín que coincida con todos los nombres de host personalizados en todos los dispositivos WildFire del clúster.

Para configurar un solo certificado personalizado que su clúster WildFire utilizará cuando se comunique con Panorama™, complete el siguiente procedimiento.

STEP 1 | Obtenga un par de claves de servidor y un certificado de CA para Panorama.

STEP 2 | Configure un perfil de certificado que incluya la autoridad de certificados (certificate authority, CA) raíz y la CA intermedia. Este perfil de certificado define la autenticación entre el clúster WildFire (cliente) y el dispositivo Panorama (servidor).

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

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

STEP 3 | Configure un perfil de servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Lleve a cabo la Configuración de un perfil de servicio SSL/TLS para definir el certificado y el protocolo que el clúster WildFire y el dispositivo Panorama utilizan para los servicios SSL/TLS.

STEP 4 | Conecte cada nodo del clúster a Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure un nombre de host único (nombre DNS) en cada nodo del clúster o utilice una cadena de un comodín que coincida con todos los nombres DNS personalizados configurados en los dispositivos WildFire del clúster.

Si utilizará una cadena con un comodín, consulte RFC-6125, Sección 6.4.3 para obtener información sobre los requisitos y los límites de los valores de cadena comodín. Asegúrese de comprender estos requisitos y límites cuando configure los nombres de DNS personalizados.

1. Inicie sesión en la CLI de WildFire en un nodo.
2. Utilice el siguiente comando para asignar un nombre de DNS personalizado único al nodo.

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

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

3. Haga clic en **Commit (Confirmar)** para confirmar los cambios.
4. Repita este proceso para cada nodo en el clúster.

STEP 6 | En Panorama, genere un certificado cliente para todos los nodos en el clúster. En Certificate Attributes (Atributos del certificado), añada una entrada de nombre de host para cada nombre DNS personalizado que asignó a los nodos del clúster o añada una entrada de nombre de host con una cadena de un comodín que coincida con todos los nombres de host del nodo, como *.ejemplo.com; solo puede hacerlo si cada nombre DNS personalizado comparte una cadena común.

STEP 7 | En Panorama, configure el perfil de certificado para el dispositivo cliente del clúster.

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

STEP 8 | Implemente los certificados personalizados en cada nodo. Este perfil de certificado debe contener el certificado de CA que firmó para el certificado de servidor de Panorama.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** y haga clic en el nombre del recopilador.
2. Seleccione **Communications (Comunicaciones)**.
3. En Secure Client Communications (Comunicación de cliente segura), seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)**.
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

©2023 Palo Alto Networks, Inc.

STEP 9 | Configure la comunicación de servidor segura en Panorama.

1. Select **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para seleccionar **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
2. Habilite **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
3. Seleccione el **SSL/TLS Service Profile**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre WildFire y Panorama.
4. Seleccione el **Certificate Profile (Perfil de certificado)** para Panorama.
5. Habilite **Custom Certificates Only (Certificados personalizados únicamente)**.
6. Haga clic en **OK (Aceptar)**.
7. **Commit (Confirmar)** los cambios.

Aplicación de certificados personalizados en un dispositivo WildFire configurado en Panorama

De manera predeterminada, Panorama™ utiliza un certificado predefinido cuando se comunica con un dispositivo WildFire® para enviar configuraciones. También puede configurar certificados personalizados para establecer autenticación mutua para la conexión que utiliza Panorama a fin de enviar configuraciones a un dispositivo o clúster WildFire gestionado. Complete el siguiente procedimiento para configurar el certificado de servidor en Panorama y el certificado cliente en el dispositivo WildFire.

STEP 1 | Obtenga pares de claves y certificados de autoridades de certificados (certificate authority, CA) para Panorama y el dispositivo WildFire.

STEP 2 | Importe el certificado de CA para validar la identidad del dispositivo WildFire y el par de claves para Panorama.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Import (Importar)**.
2. Importe el certificado de CA y el par de claves en Panorama.

STEP 3 | Configure un perfil de certificados que incluya la CA de raíz y la CA intermedia. Este perfil de certificado define la autenticación entre el dispositivo WildFire (cliente) y el dispositivo virtual Panorama o dispositivo serie M (servidor).

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

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

STEP 4 | Configure un perfil de servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Lleve a cabo la Configuración de un perfil de servicio SSL/TLS para definir el certificado y el protocolo que los dispositivos WildFire y Panorama utilizan para los servicios SSL/TLS.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure la comunicación de servidor segura en el dispositivo Panorama.

1. Select **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para seleccionar **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
2. Habilite la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
3. Seleccione el **SSL/TLS Service Profile**.
4. Seleccione el perfil de certificado del menú desplegable **Certificate Profile (Perfil del certificado)**.
5. Verifique que la opción **Custom Certificates Only (Solo los certificados personalizados)** esté deshabilitada (sin marca). Esto le permite a Panorama continuar comunicándose con WildFire con los certificados predefinidos mientras migra a los certificados personalizados.
6. (Opcional) Configure una lista de autorizaciones.
   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Selecciona el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** configurado en el perfil del certificado como el tipo de identificador.
   3. Introduzca el **Common Name (Nombre común)** si el identificador es `Subject` o una **dirección IP**, un **nombre de host** o un **correo electrónico** si el identificador es `Subject Alt Name`.
   4. Haga clic en **OK (Aceptar)**.
   5. Habilite la opción **Check Authorization List (Comprobar lista de autorización)** para configurar Panorama a fin que aplique la lista de autorización.
7. Haga clic en **OK (Aceptar)**.
8. **Commit (Confirmar)** los cambios.

STEP 6 | Importe el certificado de CA para validar el certificado en Panorama.

1. Inicie sesión en la interfaz de usuario de Panorama.
2. Importe el certificado de CA.

STEP 7 | Configure un certificado local o SCEP para el dispositivo WildFire.

1. Si está utilizando un certificado local, importe el par de claves para el dispositivo WF-500.
2. Si está utilizando SCEP para el certificado del dispositivo WildFire, configure un perfil SCEP.

STEP 8 | Configure el perfil de certificado para el dispositivo WildFire.

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

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Implemente certificados personalizados en cada dispositivo WildFire gestionado.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** y haga clic en un nombre de clúster o dispositivo.
3. Seleccione **Communications (Comunicaciones)**.
4. En Secure Client Communications (Comunicación de cliente segura), seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)** en los menús desplegables correspondientes.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

STEP 10 | Después de implementar los certificados personalizados en todos los dispositivos WildFire gestionados, aplique la autenticación de certificados personalizados.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para editar los ajustes de Secure Communication (Comunicación segura).
2. Asegúrese de **Permitir certificado personalizado únicamente**.
3. Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** los cambios.

Después de confirmar este cambio, inicia el tiempo de espera de desconexión. Cuando el tiempo de espera finaliza, Panorama y sus dispositivos WildFire gestionados no se pueden conectar sin los certificados configurados.

 ©2023 Palo Alto Networks, Inc.

Elimine un dispositivo WildFire de la gestión de Panorama

Puede eliminar los dispositivos independientes WildFire de la gestión de Panorama. Cuando elimina un dispositivo WildFire independiente de la gestión de Panorama, ya no disfruta de los beneficios de la gestión centralizada y debe gestionar el dispositivo utilizando su CLI local y sus scripts.

STEP 1 | Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)**.

STEP 2 | Seleccione el dispositivo o los dispositivos WildFire que desea eliminar de la gestión de Panorama seleccionando la casilla de verificación al lado de cada dispositivo o haciendo clic en la fila de un dispositivo.

STEP 3 | Seleccione **Remove (Retirar)** los dispositivos WildFire seleccionados de la gestión de Panorama.

 ©2023 Palo Alto Networks, Inc.

Gestión de clústeres 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. Para garantizar mayor seguridad y mantener la confidencialidad del contenido transmitido, también puede cifrar las comunicaciones entre los dispositivos WildFire en un clúster. Para obtener más información sobre los clústeres de WildFire y los procesos de implementación, consulte Clústeres de dispositivos WildFire.

Las siguientes tareas se pueden realizar utilizando Panorama para gestionar su clúster WildFire.

- Configuración de un clúster centralmente en Panorama
- Visualización del estado del clúster WildFire con Panorama
- Configuración del cifrado de dispositivo a dispositivo mediante la utilización de certificados predefinidos centralmente en Panorama
- Configuración del cifrado de dispositivo a dispositivo mediante la utilización de certificados personalizados centralmente en Panorama

Configuración de un clúster centralmente en Panorama

Antes de configurar un clúster de dispositivos WildFire en un dispositivo serie M o dispositivo virtual Panorama, 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.

Para crear clústeres de dispositivos WildFire, debe** actualizar todos sus dispositivos WildFire **que desee ubicar en un clúster a PAN-OS 8.0.1 o posterior. Si utiliza Panorama para gestionar clústeres de dispositivos WildFire, Panorama también debe ejecutar 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. En cada dispositivo Panorama que utiliza para gestionar los clústeres (o dispositivos independientes), si hace clic en **Dashboard (Portal)** > **General Information (Información general)** > **Software Version (Versión de software)**, se muestra la versión de software actual.

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

- Configuración de clústeres e incorporación de nodos en Panorama
- Configuración general del clúster en Panorama
- Configuración de la autenticación para un clúster de WildFire
- Eliminación de un clúster desde la gestión de Panorama

©2023 Palo Alto Networks, Inc.

No se admite la eliminación de un nodo de un clúster utilizando Panorama. En su lugar, lleve a cabo la Eliminación de un nodo de un clúster localmente *utilizando la CLI local de WildFire.*

Configuración de clústeres e incorporación de nodos en Panorama

Antes de configurar un clúster de dispositivos WildFire desde Panorama, debe realizar la Actualización de Panorama a 8.0.1 o posterior y la Actualización de todos los dispositivos WildFire que planifica añadir al clúster a la versión 8.0.1 o posterior. Todos los dispositivos WildFire deben ejecutar la misma versión de PAN-OS.

Puede gestionar hasta 200 dispositivos WildFire desde un dispositivo M-Series o virtual Panorama. El límite de 200 dispositivos WildFire es el total combinado de dispositivos independientes y nodos del clúster de dispositivos WildFire (si también llevó a cabo la Incorporación de dispositivos WildFire independientes para gestionarlos con Panorama). A menos que se indique lo contrario, la configuración se realiza en Panorama.

Cada nodo del clúster de dispositivos WildFire debe tener una dirección IP estática en la misma subred y conexiones de baja latencia.

STEP 1 | Con la CLI local, configure la dirección IP del servidor Panorama que gestionará el clúster de dispositivos WildFire.

Antes de registrar los dispositivos WildFire en clústeres o independientes en un dispositivo Panorama, debe configurar la dirección IP de Panorama o el FQDN en cada uno de los dispositivos WildFire utilizando la CLI local de WildFire. De esta manera, cada dispositivo WildFire sabe qué dispositivo Panorama lo gestiona.

1. En cada dispositivo WildFire, configure la dirección IP o el FQDN de la interfaz de gestión del dispositivo Panorama principal:

```
admin@WF-500# set deviceconfig system panorama-server <ip-
address | FQDN>
```

2. En cada dispositivo WildFire, si utiliza un dispositivo Panorama de copia de seguridad para la alta disponibilidad (recomendado), configure la dirección IP o el FQDN de la interfaz de gestión del dispositivo Panorama de copia de seguridad:

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-
address | FQDN>
```

3. Confirme la configuración en cada dispositivo WildFire:

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

 ©2023 Palo Alto Networks, Inc.

STEP 2 | En el dispositivo Panorama principal, registre los dispositivos WildFire.

Los dispositivos recién registrados están en modo independiente a menos que pertenezcan a un clúster debido a una configuración local del clúster.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y haga clic en **Add Appliance (Añadir dispositivo)**.
2. Introduzca el número de serie de cada dispositivo WildFire en una nueva línea. Si no tiene una lista de los números de serie de los dispositivos WildFire, en la CLI local, ejecute **`show system info`** en cada uno de los dispositivos WildFire para obtener el número de serie.
3. Haga clic en **OK (Aceptar)**.

   Si está disponible, se muestra la información sobre la configuración confirmada en los dispositivos WildFire, como las direcciones IP y la versión de software. Los dispositivos WildFire que ya pertenecen a un clúster (por ejemplo, debido a una configuración local del clúster) muestran la información de su clúster y el estado de la conexión.

STEP 3 | (Opcional) Importe configuraciones de dispositivos WildFire al dispositivo Panorama.

La importación de las configuraciones ahorra tiempo debido a que puede reutilizar o editar las configuraciones en Panorama e insertarlas en uno o más clústeres de dispositivos WildFire o en dispositivos WildFire independientes. Si no desea importar configuraciones, omita este paso. Cuando inserta una configuración de Panorama, la configuración insertada sustituye a la configuración local.

1. Seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** y seleccione los dispositivos que tengan las configuraciones que desea importar de la lista de dispositivos WildFire gestionados.
2. **Import Config (Importar configuración)**.
3. Seleccione **Yes (Sí)**.

   La importación de configuraciones actualiza la información mostrada y hace que las configuraciones importadas formen parte de la configuración candidata del dispositivo Panorama.
4. Seleccione **Commit to Panorama (Confirmar en Panorama)** para hacer que las configuraciones importadas del dispositivo WildFire sean parte de la configuración de ejecución de Panorama.

STEP 4 | Cree un nuevo clúster de dispositivos WildFire.

1. Seleccione **Managed WildFire Clusters (Clústeres WildFire gestionados)**.

   En **Appliance (Dispositivo)** > **No Cluster Assigned (Sin clústeres asignados)**, se muestra los dispositivos (nodos) WildFire independientes y se indica cuántos nodos disponibles no se asignaron a un clúster.
2. Haga clic en **Create Cluster (Crear clúster)**.
3. Introduzca un nombre de clúster alfanumérico de hasta 63 caracteres en **Name (Nombre)**. El campo **Name (Nombre)** puede contener caracteres en minúsculas y números, además

 ©2023 Palo Alto Networks, Inc.

de guiones y puntos si no están al principio o al final. No se permiten espacios ni otros caracteres.

4. Haga clic en **OK (Aceptar)**.

   Se muestra el nuevo nombre del clúster, pero no se han asignado nodos de WildFire.

STEP 5 | Añada dispositivos WildFire al nuevo clúster.

El primer dispositivo WildFire añadido al clúster automáticamente se convierte en el nodo controlador y el segundo dispositivo, en el nodo controlador de copia de seguridad. El resto de los dispositivos WildFire que se añadan al clúster se convertirán en nodos de trabajo. Los nodos de trabajo utilizan la configuración del nodo controlador de modo que el clúster tenga una configuración consistente.

1. Seleccione el nuevo clúster.
2. Seleccione **Clustering (Agrupación en clústeres)**.
3. Haga clic en **Browse (Explorar)** para buscar en la lista de dispositivos WildFire que no pertenecen a un clúster.
4. Añada (⊕) cada dispositivo WildFire que desee incluir en el clúster. Puede agregar hasta veinte nodos a un clúster. Cada dispositivo WildFire que añade a un clúster se muestra junto a su función automáticamente asignada.
5. Haga clic en **OK (Aceptar)**.

STEP 6 | Configure la **Management (gestión)**, la **Analysis Environment Network (red de entornos de análisis)**, la HA y las interfaces de gestión del clúster.

Configure la **Management (gestión)**, la **Analysis Environment Network (red de entornos de análisis)** y las interfaces de gestión del clúster en cada miembro del clúster (nodo controlador y nodo de trabajo) si aún no se configuraron. La interfaz de gestión del clúster es una interfaz dedicada para la gestión y la comunicación en el clúster y es diferente a la interfaz de gestión.

Configure las interfaces de HA individualmente en el nodo controlador y en el nodo controlador de copia de seguridad. Las interfaces de HA conectan los nodos controladores principal y de copia de seguridad, y les permiten permanecer sincronizados y listos para responder ante una conmutación por error.



Los nodos del clúster requieren direcciones IP para cada una de las cuatro interfaces de dispositivos WildFire. No puede configurar los servicios de HA en los nodos de trabajo.

1. Seleccione el nuevo clúster.
2. Seleccione **Clustering (Agrupación en clústeres)**.
3. Si la interfaz de gestión no está configurada en un nodo del clúster, seleccione **Interface Name (Nombre de la interfaz)** > **Management (Gestión)** e introduzca la dirección IP, la máscara de red, los servicios y otra información para la interfaz.
4. Si la interfaz para la red de entornos de análisis no está configurada en un nodo del clúster, seleccione **Interface Name (Nombre de la interfaz)** > **Management (Red de entornos de análisis)** e introduzca la dirección IP, la máscara de red, los servicios y otra información para la interfaz.
5. En el nodo controlador y el nodo controlador de copia de seguridad, seleccione la interfaz que se utilizará para el enlace de control de HA. Debe configurar la misma interfaz en

 ©2023 Palo Alto Networks, Inc.

ambos nodos controladores para el servicio de HA. Por ejemplo, en el nodo controlador y en el nodo controlador de copia de seguridad, seleccione **Ethernet3**.

6. En cada nodo controlador, seleccione **Clustering Services (Servicios de agrupación en clústeres)** > **HA**. (La opción de **HA** no está disponible para los nodos de trabajo). Si también desea la capacidad de hacer ping a la interfaz, seleccione **Management Services (Servicios de gestión)** > **Ping**.
7. Haga clic en **OK (Aceptar)**.
8. (Recomendado) Seleccione la interfaz que utilizará como el enlace de control de HA de copia de seguridad entre el nodo controlador y el nodo controlador de copia de seguridad. Debe utilizar la misma interfaz en ambos nodos para el servicio de copia de seguridad de HA. Por ejemplo, en ambos nodos, seleccione **Management (Gestión)**.

   Seleccione **Clustering Services (Servicios de agrupación en clústeres)** > **HA Backup (Copia de seguridad de HA)** en ambos nodos. También puede seleccionar **Ping**, **SSH** y **SNMP** si desea incluir esos **Management Services (servicios de gestión)** en la interfaz.

   *La interfaz de la **Analysis Environment Network (red de entornos de análisis)** no puede ser una interfaz de HA o de copia de seguridad de HA o una interfaz de gestión del clúster.*
9. Seleccione la interfaz dedicada que se utilizará para la gestión y la comunicación en el clúster. Debe utilizar la misma interfaz en ambos nodos, por ejemplo, **Ethernet2**.
10. Seleccione **Clustering Services (Servicios de agrupación en clústeres)** > **Cluster Management (Gestión del clúster)** en ambos nodos. Si también desea la capacidad de hacer ping a la interfaz, seleccione **Management Services (Servicios de gestión)** > **Ping**.

    Los nodos de trabajo en el clúster automáticamente heredan la configuración del nodo controlador para la interfaz dedicada de gestión y comunicación.

STEP 7 | Confirme la configuración en el dispositivo Panorama e insértela en el clúster.

1. **Commit and Push (Confirmar y enviar)**.
2. Si hay configuraciones en el dispositivo Panorama que no desea enviar, elija **Edit Selections (Editar selecciones)** para elegir los dispositivos a los que desea enviar las configuraciones. La configuración que se inserta sustituye a la configuración actual en los nodos del clúster, de modo que todos los nodos del clúster funcionen con la misma configuración.

©2023 Palo Alto Networks, Inc.

STEP 8 | Verifique la configuración.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)**.
2. Verifique los siguientes campos:
   - **Appliance (Dispositivo)**: en lugar de mostrarse como dispositivos independientes, los nodos WildFire que se añaden al clúster se muestran bajo el nombre del clúster.
   - **Cluster Name (Nombre del clúster)**: se muestra el nombre del clúster de cada nodo.
   - **Role (Función)**: se muestra la función adecuada (**Controller (Controlador)**, **Controller Backup (Copia de seguridad del controlador)** o **Worker (de trabajo)**) de cada nodo.
   - **Config Status (Estado de configuración)**: el estado es `InSync (En sincronización)`.
   - **Last Commit State (Último estado de compilación)**: `Commitsucceeded (Compilación exitosa)`.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Con la CLI local en el nodo controlador principal (no en la interfaz web de Panorama), compruebe que las configuraciones estén sincronizadas.

Si no están sincronizadas, sincronice manualmente las configuraciones de alta disponibilidad en los nodos controladores y confirme la configuración.

A pesar de que puede realizar la mayor parte de la configuración en Panorama, la sincronización de las configuraciones de alta disponibilidad del nodo controlador debe realizarse en la CLI del nodo controlador principal.

1. En el nodo controlador principal, compruebe que las configuraciones estén sincronizadas:

```
admin@WF-500(active-controller)> show high-availability all
```

   Al final del resultado, busque `ConfigurationSynchronization (Sincronización de configuración)`:

```
Sincronización de configuración: Habilitado: sí Configuración
 en ejecución: sincronizado
```

   Si la configuración actual está sincronizada, no hace falta que la sincronice manualmente, pero sí debe hacerlo si no está sincronizada.
2. Si la configuración no se sincronizó, 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.
3. Confirme la configuración:

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

Configuración general del clúster en Panorama

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

 ©2023 Palo Alto Networks, Inc.

- la configuración de las direcciones IP para el servidor DNS, el servidor NTP, etc.

STEP 1 | Configure los nodos del clúster de dispositivos WildFire.

Varios ajustes se rellenan previamente con los valores predeterminados, información de ajustes existentes en el nodo controlador o los ajustes que añadió.

1. Seleccione el clúster.
2. Seleccione **Appliance (Dispositivo)**.
3. Introduzca nueva información, mantenga la información rellenada previamente del nodo controlador del clúster o edite la información rellenada previamente, que incluye lo siguiente:
   - Nombre de **Domain (dominio)**.
   - Dirección IP del **Primary DNS Server (servidor DNS principal)** y del **Secondary DNS Server (servidor DNS secundario)**.
   - **NTP Server Address (Dirección del servidor NTP)** y **Authentication Type (tipo de autenticación)** del **Primary NTP Server (servidor NTP principal)** y del **Secondary NTP Server (servidor NTP secundario)**. Las opciones de **Authentication Type (tipo de autenticación)** son **None (Ninguna)**, **Symmetric Key (Clave simétrica)** y **AutoKey**.

STEP 2 | Realice la configuración general del clúster.

Varios ajustes se rellenan previamente con los valores predeterminados, información de ajustes existentes en el nodo controlador o los ajustes que añadió.

1. Seleccione el nuevo clúster > **General**.
2. (Opcional) **Enable DNS (Habilite el DNS)** para que el nodo controlador anuncie el estado del servicio utilizando un protocolo DNS. El controlador del clúster proporciona servicios DNS en el puerto de la interfaz de gestión (management, MGT).
3. Haga clic en **Register Firewall To (Registrar el cortafuegos)** para registrarlo con el fin de utilizar el servicio que anunció el controlador del clúster. Palo Alto Networks recomienda añadir ambos controladores como servidores de autoridad, dado que esto proporciona la ventaja de la alta disponibilidad. Utilice la forma:

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   Por ejemplo, un clúster denominado *mycluster* en el dominio *paloaltonetworks.com* tendrá el siguiente nombre de dominio:

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. Introduzca el **Content Update Server (Servidor de actualizaciones de contenido)** del clúster. Utilice el FQDN predeterminado `updates.paloaltonetworks.com` para conectarse al servidor más cercano. Utilice la opción **Check Server Identity (Comprobar identidad de servidor)** para confirmar la identidad del servidor de actualizaciones haciendo coincidir el nombre común (common name, CN) del certificado con la dirección IP o FQDN del servidor (se comprueba de manera predeterminada).
5. (Opcional) Indique la ubicación pública del **WildFire Cloud Server (Servidor de la nube de WildFire)** o utilice el valor predeterminado `wildfire.paloaltonetworks.com`

 ©2023 Palo Alto Networks, Inc.

para que el clúster (o el dispositivo independiente gestionado por Panorama) pueda enviar información al servidor más cercano de la nube de WildFire. Si deja este campo vacío y no se conecta a un servidor de la nube de WildFire, el clúster no recibe las actualizaciones de firmas directamente de la nube pública de WildFire y no puede enviar muestras para el análisis ni contribuir datos a la nube pública.

6. Si conecta el clúster a la nube pública de WildFire, seleccione los servicios de la nube que desea habilitar:
   - **Send Analysis Data (Enviar datos de análisis)**: envíe un informe XML acerca del análisis de malware local. Si envía las muestras reales, el clúster no envía informes.
   - **Send Malicious Samples (Enviar muestras malintencionadas)**: se envían muestras de malware.
   - **Send Diagnostics (Enviar diagnóstico)**: se envían datos de diagnóstico.
   - **Verdict Lookup (Búsqueda de veredictos)**: se buscan veredictos automáticamente en la nube pública de WildFire antes de realizar el análisis local para reducir la carga en el clúster de dispositivos WildFire local.
7. Seleccione la **Sample Analysis Image (Imagen de análisis de muestras)** que utilizará, según las muestras que analizará el clúster.
8. Configure la cantidad de tiempo durante la que el clúster conservará los datos de muestras **Benign/Grayware (Benigna/Grayware)** (rango de 1 a 90 días, valor predeterminado de 14 días) y los datos de muestras **Malicious (Malintencionadas)** (mínimo 1 día, sin máximo [indefinido], valor predeterminado indefinido). Los datos de muestras malintencionadas incluyen veredictos de phishing.
9. (Opcional) Seleccione **Preferred Analysis Environment (Entorno de análisis preferido)** para asignar más recursos a **Executables (Ejecutables)** o a **Documents (Documentos)** según su entorno. La asignación **Default (Predeterminada)** se reparte entre las categorías **Executables (Ejecutables)** y **Documents (Documentos)**. La cantidad de recursos disponibles depende de la cantidad de nodos WildFire en el clúster.

STEP 3 | Compruebe que los servidores Panorama principal y de copia de seguridad estén configurados.

Si no configuró un servidor Panorama de copia de seguridad y desea hacerlo, puede añadirlo.

1. Seleccione el clúster.
2. Seleccione **Appliance (Dispositivo)**.
3. Compruebe (o introduzca) la dirección IP o FQDN del **Panorama Server (Servidor Panorama)**principal y del **Panorama Server 2 (Servidor Panorama 2)** de copia de seguridad si utiliza una configuración de alta disponibilidad para la gestión centralizada del clúster.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Configure el sistema y los logs de configuración del clúster, que incluye el reenvío de logs.

1. Seleccione el clúster.
2. Seleccione **Logging (Registro)**.
3. Seleccione **System (Sistema)** o **Configuration (Configuración)** para configurar un log de sistema o de configuración, respectivamente. El proceso para configurarlos es similar.
4. Haga clic en **Add (Añadir)** (⊕) y en **Name (Nombre)** para asignarle un nombre a la instancia de reenvío de logs, seleccione el **Filter (Filtro)**, y configure el **Forward Method (Método de reenvío)** (**SNMP**, **Email (Correo electrónico)**, **Syslog** o **HTTP**).

STEP 5 | Configure la autenticación administrativa.

1. Seleccione el clúster.
2. Seleccione **Authentication (Autenticación)**.
3. Seleccione el **Authentication Profile (Perfil de autenticación)**: **None (Ninguno)** o **radius**. RADIUS es el único método de autenticación externa permitido.
4. Configure el modo de **Local Authentication (Autenticación local)** para los usuarios administradores como **Password (Contraseña)** o **Password Hash (Hash de contraseña)**, e introduzca la **Password (Contraseña)**.

STEP 6 | Confirme la configuración en el dispositivo Panorama e insértela en el clúster.

1. **Commit and Push (Confirmar y enviar)**.
2. Si hay configuraciones en el dispositivo Panorama que no desea enviar, elija **Edit Selections (Editar selecciones)** para elegir los dispositivos a los que desea enviar las configuraciones. La configuración que se inserta sustituye a la configuración actual en los nodos del clúster, de modo que todos los nodos del clúster funcionen con la misma configuración.

Configuración de la autenticación para un clúster de WildFire

Cree y configure la autenticación mejorada para todos los dispositivos WildFire en un clúster de WildFire. Para ello, configure usuarios administrativos locales con parámetros de autenticación detallados y aproveche RADIUS, TACAS + o LDAP para la autorización y autenticación.

Cuando se configura y envía administradores desde Panorama, se sobrescriben los administradores existentes para todos los dispositivos WildFire en el clúster de WildFire por los que configure en Panorama.

- Configuración de una cuenta administrativa para un clúster de WildFire
- Configuración de la autenticación RADIUS para un clúster de WildFire
- Configuración de la autenticación TACACS+ para un clúster de WildFire
- Configuración de la autenticación LDAP para un clúster de WildFire

Configuración de una cuenta administrativa para un clúster de WildFire

Cree uno o más administradores con parámetros de autenticación detallados para que todos sus dispositivos WildFire en un clúster de WidlFire los administre desde el servidor de gestión Panorama™. Además, puede configurar administradores locales desde Panorama que se pueden configurar directamente en la CLI del dispositivo WildFire. Sin embargo, enviar nuevos cambios

 ©2023 Palo Alto Networks, Inc.

de configuración a un dispositivo WildFire sobrescribe a los administradores locales con los administradores configurados para el dispositivo WildFire.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un clúster centralmente en Panorama.

STEP 3 | (Opcional) Configure un perfil de autenticación para definir el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores que acceden a la CLI del dispositivo WildFire.

STEP 4 | Configure una o más cuentas de administrador según sea necesario.

Las cuentas de administrador creadas en Panorama se importan posteriormente a los dispositivos WildFire en el clúster de WildFire y se administran desde Panorama.



Debe configurar la cuenta administrativa con privilegios de función de administrador de Superuser (Superusuario) para configurar correctamente la autenticación de los dispositivos Wildfire en el clúster de WildFire.

STEP 5 | Configure la autenticación para los dispositivos WildFire en el clúster de WildFire.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres de WildFire gestionados)** y seleccione un clúster de WildFire configurado anteriormente.
2. (Opcional) Seleccione el **perfil de autenticación** que configuró en el paso anterior.
3. Establezca la **configuración de tiempo de espera** de autenticación para los dispositivos WildFire.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de la CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que un dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

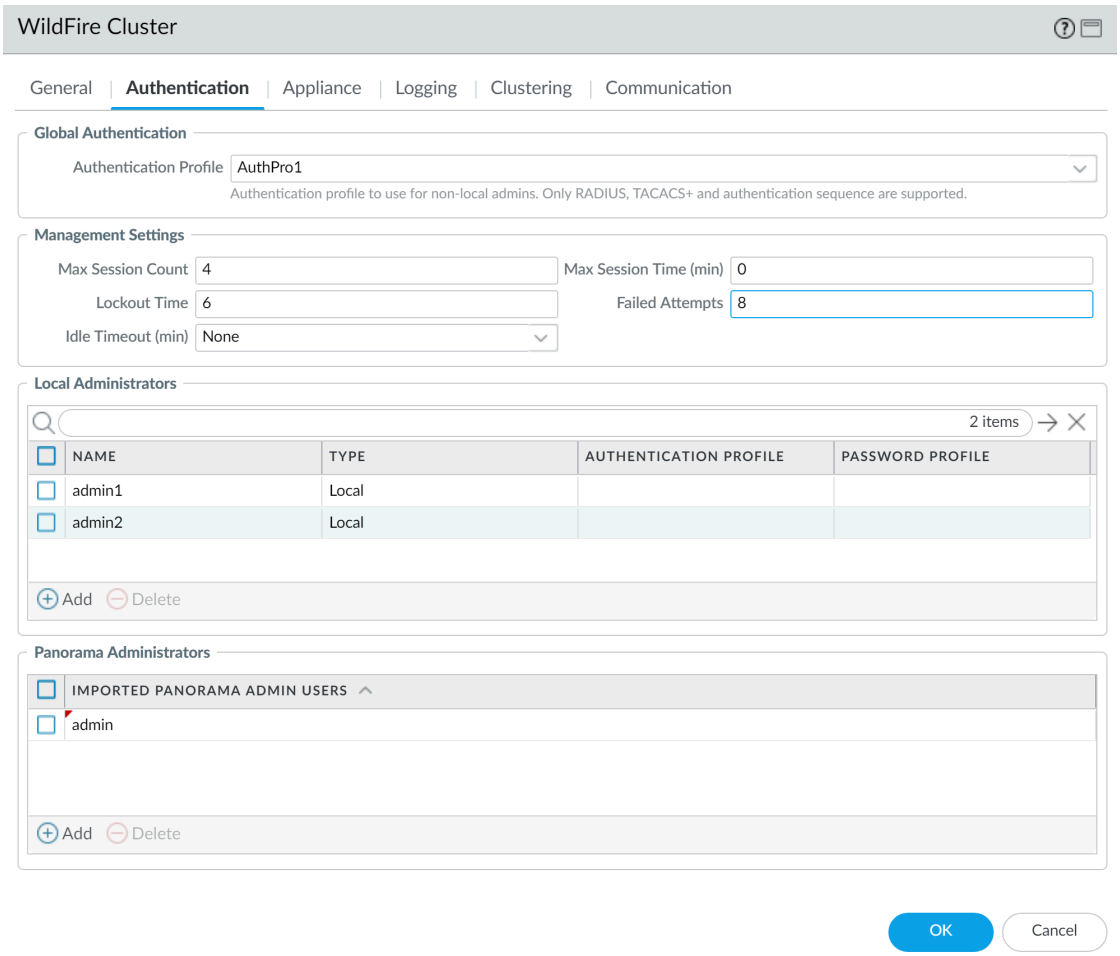
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos en el clúster de WildFire. Estos administradores son específicos del dispositivo WildFire en el clúster de WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire en el clúster de WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración del clúster de WildFire.



STEP 6 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 7 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación RADIUS para un clúster de WildFire

Utilice un servidor RADIUS para autenticar el acceso administrativo a la CLI de los dispositivos WildFire en un clúster de WildFire. También puede definir Atributos específicos de proveedor (VSA) en el servidor RADIUS para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y el servidor de gestión Panorama™.

Importe el diccionario de RADIUS de Palo Alto Networks al servidor RADIUS con objeto de definir los atributos de autenticación necesarios para facilitar la comunicación entre Panorama y dicho servidor.

©2023 Palo Alto Networks, Inc.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un clúster centralmente en Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configuración de la autenticación RADIUS

Las cuentas de administrador configuradas para la autenticación RADIUS deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para los dispositivos WildFire en el clúster WildFire.*

1. Añada un perfil de servidor RADIUS.

   El perfil define cómo se conectan los dispositivos WildFire en el clúster de WildFire al servidor RADIUS.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** y haga clic en **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que el dispositivo Panorama utiliza para autenticarse en el servidor RADIUS.

      *Seleccione **CHAP** si el servidor RADIUS admite ese protocolo; es más seguro que **PAP**.*

   5. Seleccione **Add (Añadir)** para añadir cada servidor RADIUS e ingrese lo siguiente:
      1. **Name (Nombre)** para identificar el servidor.
      2. **La dirección IP o FQDN del** servidor RADIUS.
      3. **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. Port (Puerto) **del servidor** para las solicitudes de autenticación (el valor predeterminado es 1812).
   6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor RADIUS a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
   3. Configure el **Type (Tipo)** en **RADIUS**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from RADIUS (Recuperar grupo de usuarios desde RADIUS)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor RADIUS.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el clúster de WildFire.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres de WildFire gestionados)** y seleccione un clúster de WildFire añadido anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Establezca la **configuración de tiempo de espera** de autenticación para un dispositivo WildFire.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de una CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que un dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

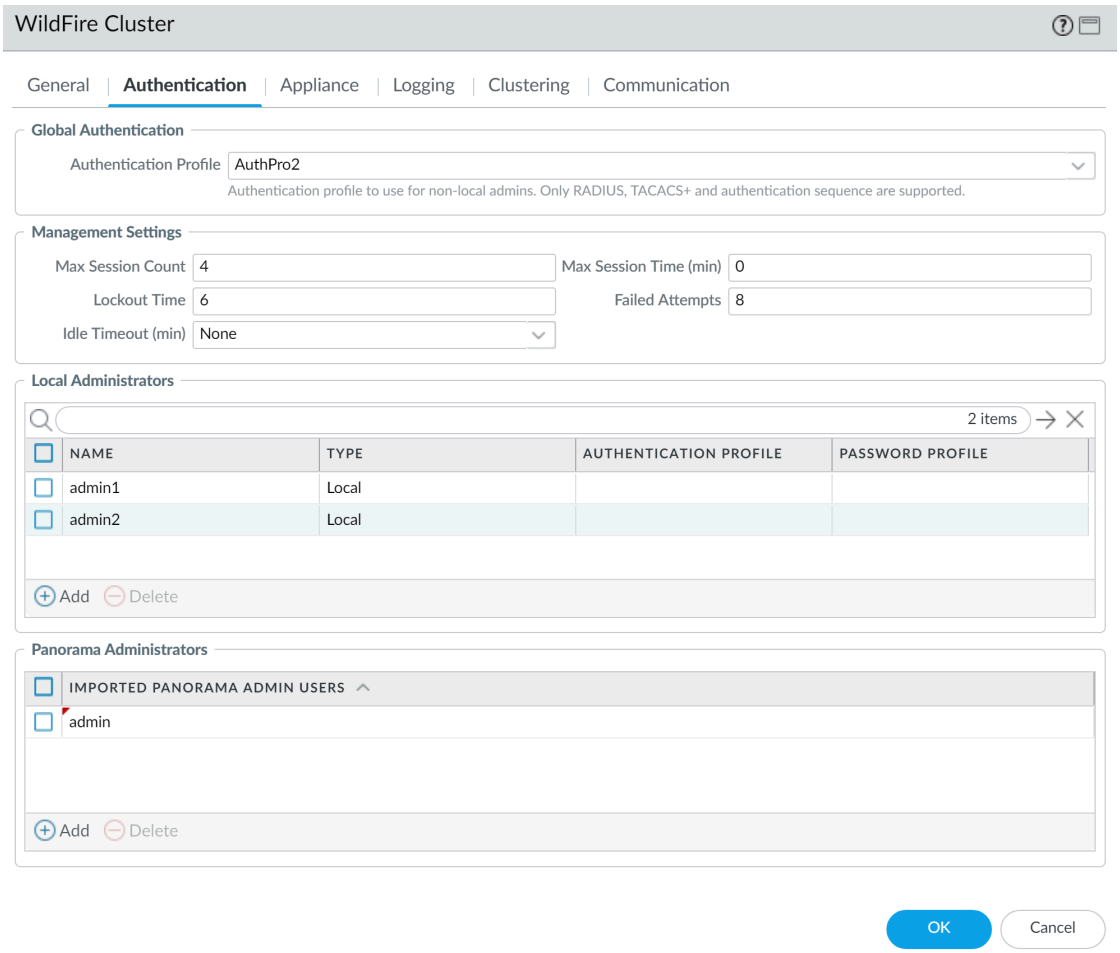
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos en el clúster de WildFire. Estos administradores son específicos del dispositivo WildFire en el clúster de WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire en el clúster de WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración del clúster de WildFire.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación TACACS+ para un clúster de WildFire

Utilice un servidor TACACS+ para autenticar el acceso administrativo a la CLI de los dispositivos WildFire en un clúster de WildFire. También puede definir Atributos específicos de proveedor (VSA) en el servidor TACACS+ para gestionar la autorización del administrador. La utilización de VSA le permite cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un clúster centralmente en Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure la autenticación TACACS+.

Las cuentas de administrador configuradas para la autenticación TACACS+ deben tener privilegios de función de administrador de Superuser (Superusuario) *para configurar correctamente la autenticación para los dispositivos WildFire en el clúster WildFire.*

1. Añada un perfil de servidor TACACS+.

   El perfil define cómo se conecta un dispositivo WildFire al servidor TACACS+.

   1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACACS+** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
   3. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
   4. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que Panorama utiliza para autenticarse en el servidor TACACS+.
   5. Seleccione **CHAP** si el servidor TACACS+ admite ese protocolo; es más seguro que **PAP**.
   6. Seleccione **Add (Añadir)** para añadir cada servidor TACACS+ e introduzca lo siguiente:
      1. **Name (Nombre)** para identificar el servidor.
      2. **servidor TACACS+**.
      3. **Secret (Secreto)/Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
      4. Port (Puerto) **del servidor** para las solicitudes de autenticación (el valor predeterminado es 49).
   7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
2. Asigne el perfil del servidor TACACS+ a un perfil de autenticación.

   El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de administradores.

   1. Seleccione **Panorama** > **Authentication Profile (Perfil de autenticación)** y **Add (Añadir)** para añadir un perfil.
   2. Introduzca un **Name (Nombre)** para identificar el perfil.
   3. Configure el **Type (Tipo)** en **TACACS+**.
   4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
   5. Seleccione **Retrieve user group from TACACS+ (Recuperar grupo de usuarios desde TACACS+)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor TACACS+.

      Panorama coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.

 ©2023 Palo Alto Networks, Inc.

6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los administradores que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Configure la autenticación para el clúster de WildFire.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres de WildFire gestionados)** y seleccione un clúster de WildFire añadido anteriormente.
2. Seleccione el **perfil de autenticación** que configuró en el paso anterior.

   Si no se asigna un perfil de autenticación global, debe asignar un perfil de autenticación a cada administrador local individual para aprovechar la autenticación remota.
3. Establezca la **configuración de tiempo de espera** de autenticación para un dispositivo WildFire.

   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de una CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que un dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
4. Añada los administradores del dispositivo WildFire.

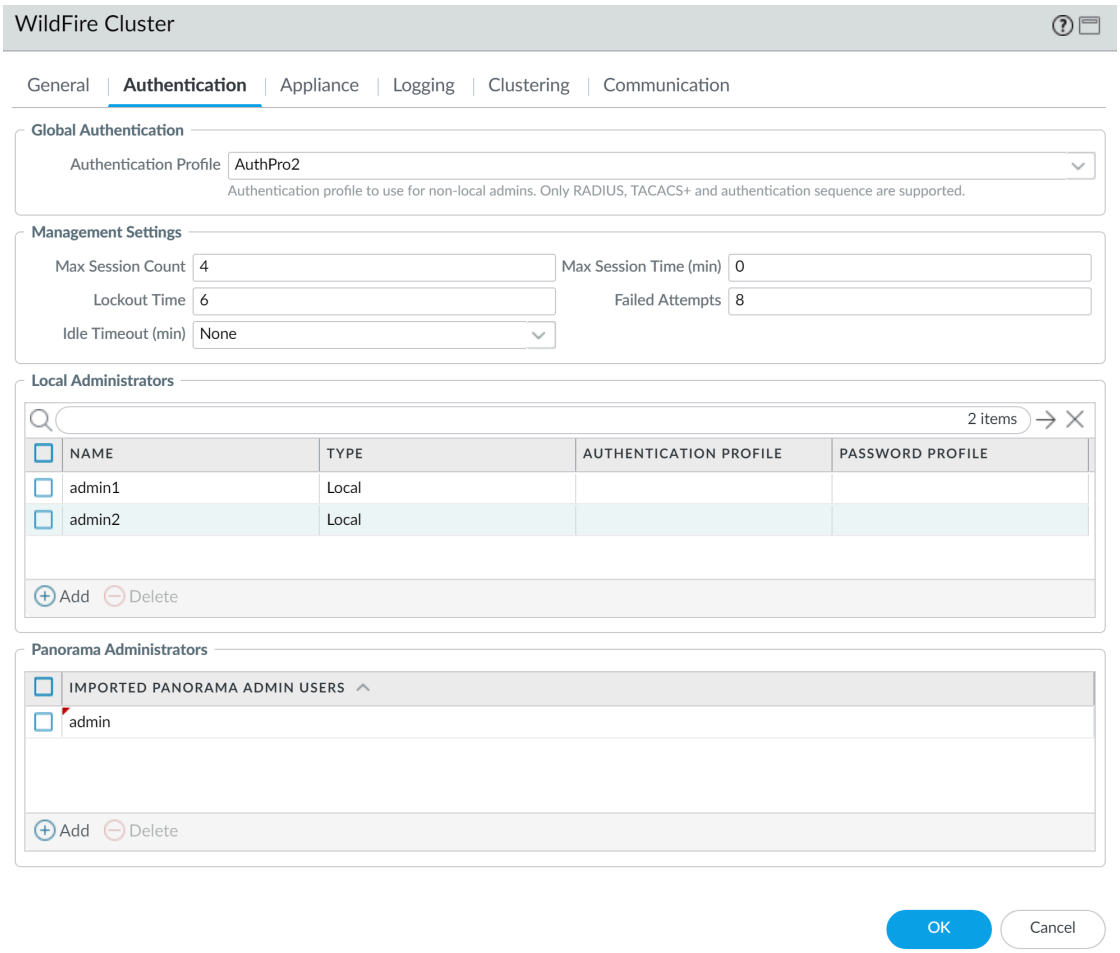
   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **`admin1`** como administrador local y de Panorama.

   1. **Añada** y configure nuevos administradores exclusivos en el clúster de WildFire. Estos administradores son específicos del dispositivo WildFire en el clúster de WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

 ©2023 Palo Alto Networks, Inc.

2. **Añada** cualquier administrador configurado en Panorama. Estos administradores se crean en Panorama y se importan en el dispositivo WildFire en el clúster de WildFire.

5. Haga clic en **OK (Aceptar)** para guardar la configuración del clúster de WildFire.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Configuración de la autenticación LDAP para un clúster de WildFire

Puede utilizar LDAP para autenticar a los usuarios finales para acceder a la CLI de los dispositivos WildFire en un clúster de WildFire.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un clúster centralmente en Panorama.

©2023 Palo Alto Networks, Inc.

STEP 3 | Añada un perfil de servidor LDAP.

El perfil define cómo se conecta un dispositivo WildFire al servidor LDAP.

Las cuentas de administrador configuradas para la autenticación LDAP deben tener privilegios de función de administrador de Superuser (Superusuario) para configurar correctamente la autenticación para los dispositivos WildFire en el clúster WildFire.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **LDAP** y haga clic en **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. **Add (Añada)** los servidores LDAP (máximo de cuatro). Para cada servidor, ingrese un nombre en **Name** (para identificar al servidor), una dirección IP del **LDAP Server (Servidor LDAP)** o FQDN, y un **Port (Puerto)** para el servidor (el valor predeterminado es 389).

   Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección de servidor tenga efecto.
4. Seleccione el **Type (Tipo)** de servidor.
5. Seleccione el **DN base**.

   Para identificar el DN base de su directorio, abra el complemento de la consola de administración de Microsoft **Active Directory Domains and Trusts (Dominios y confianzas de Active Directory)** y use el nombre del dominio de nivel superior.
6. Introduzca **Bind DN (DN de enlace)** y **Password (Contraseña)** para permitir que el servicio de autenticación autentique el cortafuegos.

   La cuenta DN de enlace debe tener permiso para leer el directorio LDAP.
7. Ingrese el **Bind Timeout (Tiempo de espera de enlace)** y el **Search Timeout (Tiempo de espera de búsqueda)** en segundos (el valor predeterminado es 30 para ambos).
8. Especifique el **intervalo de reintento** en segundos (el valor predeterminado es 60).
9. (Opcional) Si desea que el endpoint use SSL o TLS para una conexión más segura con el servidor del directorio, habilite la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)** (está habilitada por defecto). El protocolo que usa el endpoint depende del puerto del servidor:
   - 389 (predeterminado): TLS (específicamente, el dispositivo WildFire usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).
   - 636—SSL
   - Cualquier otro puerto: el dispositivo WildFire primero intenta utilizar TLS. Si el servidor de directorio no es compatible con TLS, el dispositivo WildFire recurre a SSL.
10. (Opcional) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar la verificación, debe seleccionar también la opción **Require SSL/TLS**

 ©2023 Palo Alto Networks, Inc.

secured connection (Requerir conexión segura de SSL/TLS). Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:

- Está en la lista de certificados de Panorama: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Si es necesario, importe el certificado a Panorama.
- El firmante del certificado está en la lista de autoridades de certificación confiables: **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.

11. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 4 | Configure la autenticación para el clúster de WildFire.

1. Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres de WildFire gestionados)** y seleccione un clúster de WildFire añadido anteriormente.
2. Establezca la **configuración de tiempo de espera** de autenticación para un dispositivo WildFire.
   1. Especifique el número de **intentos fallidos** antes de que se bloquee a un usuario de una CLI del dispositivo WildFire.
   2. Especifique el **tiempo de bloqueo**, en minutos, durante el que un dispositivo WildFire bloquea una cuenta de usuario después de que ese usuario alcance el número configurado de **intentos fallidos**.
   3. Especifique el **tiempo de espera de inactividad**, en minutos, antes de que la cuenta de usuario se cierre automáticamente debido a la inactividad.
   4. Introduzca el **número máximo de sesiones** para establecer cuántas cuentas de usuario pueden acceder simultáneamente al dispositivo WildFire.
   5. Especifique el**tiempo máximo de sesión** que el administrador puede estar conectado antes de cerrar la sesión automáticamente.
3. Añada los administradores del dispositivo WildFire.

   Los administradores pueden añadirse como administrador local o como administrador de Panorama importado, pero no ambos. No se admite la adición del mismo administrador como administrador local y como administrador de Panorama importado y hará que la

 ©2023 Palo Alto Networks, Inc.

confirmación de Panorama falle. Por ejemplo, la confirmación de Panorama falla si añade **admin1** como administrador local y de Panorama.

- Configure los administradores locales.

  Configure nuevos administradores exclusivos en el clúster de WildFire. Estos administradores son específicos del dispositivo WildFire en el clúster de WildFire para el que se crearon y usted gestiona estos administradores desde esta tabla.

  1. **Añada** uno o más administradores locales nuevos.
  2. Especifique un **nombre** para el administrador local.
  3. Asigne un **perfil de autenticación** creado anteriormente.

     Los perfiles de autenticación LDAP solo son compatibles con administradores locales individuales.
  4. Habilite (marque) **Use Public Key Authentication (SSH) [Usar autenticación de clave pública (SSH)]** para importar un archivo de clave pública para la autenticación.
  5. Seleccione un **perfil de contraseña** para establecer los parámetros de vencimiento.

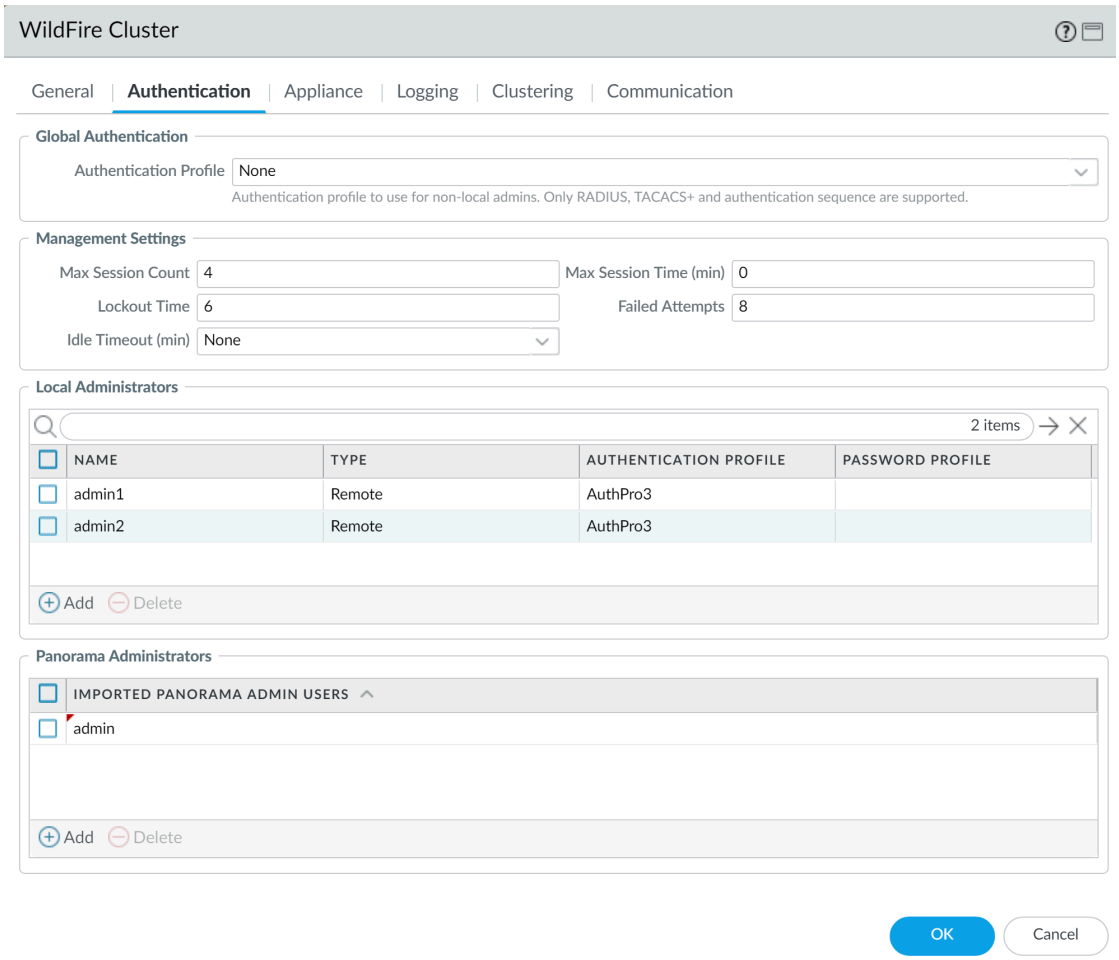
- Importación de administradores de Panorama existentes

  Importe administradores existentes configurados en Panorama. Estos administradores se configuran y gestionan en Panorama y se importan al dispositivo WildFire.

  1. **Añada** un administrador de Panorama existente.

4. Haga clic en **OK (Aceptar)** para guardar la configuración del clúster de WildFire.

 ©2023 Palo Alto Networks, Inc.



STEP 5 | Seleccione las opciones **Commit (Confirmar)** y **Commit and Push (Confirmar y enviar)** para aplicar esos cambios en su configuración.

STEP 6 | Acceda a la CLI del dispositivo WildFire para verificar que puede acceder correctamente al dispositivo WildFire mediante el usuario administrador local.

Eliminación de un clúster desde la gestión de Panorama

Para eliminar un clúster de la gestión de Panorama, haga clic en **Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** y seleccione la fila del clúster que desea eliminar (no haga clic en el nombre del clúster) y haga clic en **Remove From Panorama (Eliminar de Panorama)**.

Si elimina un clúster de dispositivos WildFire de la gestión de Panorama, la interfaz web de Panorama ubica los dispositivos WildFire de ese clúster en modo solo de lectura. A pesar de que los dispositivos WildFire en el clúster eliminado se muestren en la interfaz web de Panorama, cuando estén en modo solo lectura, no podrá insertar configuraciones en los dispositivos WildFire ni gestionarlos con Panorama. Tras su eliminación de la gestión de Panorama, los miembros del clúster de dispositivos WildFire utilizan la configuración del clúster local y puede gestionar el clúster utilizando la CLI local.

 ©2023 Palo Alto Networks, Inc.

Para gestionar los dispositivos WildFire en el clúster con Panorama tras eliminar el clúster de la gestión de Panorama, importe el clúster a Panorama (**Panorama** > **Managed WildFire Clusters (Clústeres WildFire gestionados)** > **Import Cluster Config (Importar config. de clúster)**).

STEP 1 | Seleccione el nodo controlador del clúster. El campo del nombre del clúster se rellena automáticamente con **Cluster (Clúster)**.

STEP 2 | Haga clic en **OK (Aceptar)**. El nodo del controlador de copia de seguridad y los nodos trabajadores del clúster se rellenan automáticamente.

STEP 3 | Haga clic en **OK (Aceptar)** para importar el clúster.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

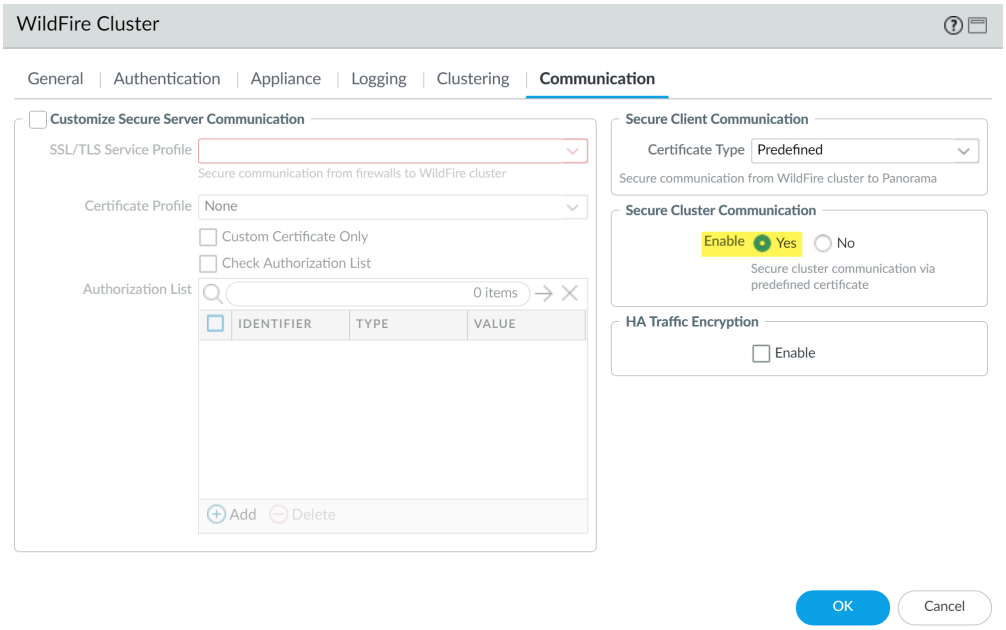
Configuración del cifrado de dispositivo a dispositivo mediante la utilización de certificados predefinidos centralmente en Panorama

STEP 1 | Actualice cada dispositivo WildFire gestionado a PAN-OS 8.1.x. Todos los dispositivos gestionados deben ejecutar PAN-OS 8.1 o posterior para habilitar el cifrado de dispositivo a dispositivo.

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

STEP 3 | En Panorama, seleccione **Panorama> Managed WildFire Clusters (Clústeres WildFire gestionados)> *WF_cluster_name*> Communication (Comunicación).**

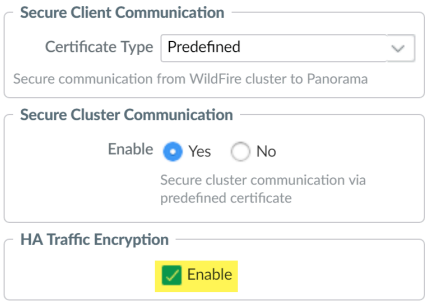
STEP 4 | Haga clic en **Enable (Habilitar)** para habilitar la comunicación de clúster segura.



 ©2023 Palo Alto Networks, Inc.

STEP 5 | (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.



STEP 6 | Haga clic en **OK (Aceptar)** para guardar la configuración de **WildFire Cluster (Clúster WildFire)**.

STEP 7 | **Commit (Confirmar)** los cambios.

Configuración del cifrado de dispositivo a dispositivo mediante la utilización de certificados personalizados centralmente en Panorama

STEP 1 | Actualice cada dispositivo WildFire gestionado a PAN-OS 8.1.x. Todos los dispositivos gestionados deben ejecutar PAN-OS 8.1 o posterior para habilitar el cifrado de dispositivo a dispositivo.

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

STEP 3 | Revise la configuración existente de comunicación segura de WildFire. 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.

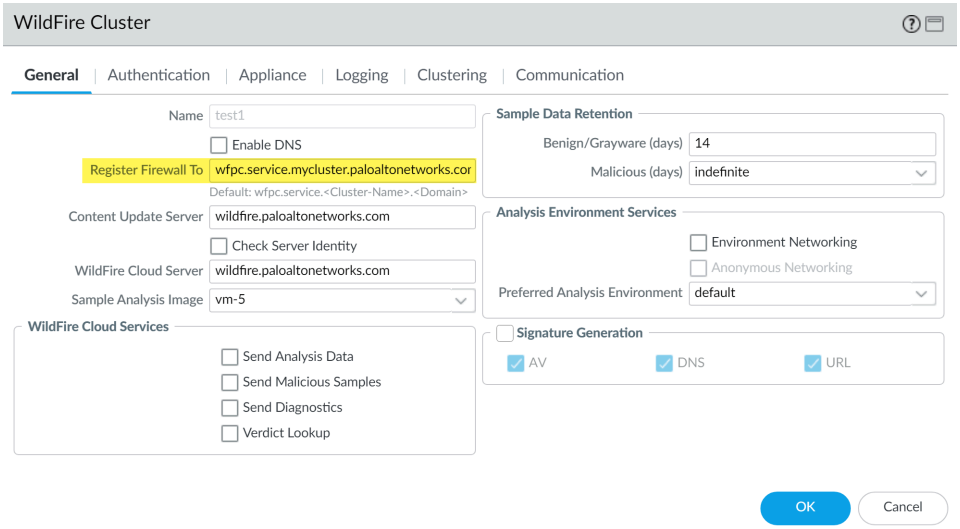
1. Seleccione **Panorama >Managed WildFire Clusters (Clústeres WildFire gestionados)> *WF_cluster_name*> Communication (Comunicación).**
2. Si se habilitó la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)** y desea utilizar ese certificado, identifique los detalles que se utilizan del certificado personalizado. De lo contrario, continúe con el paso 5 para comenzar el proceso de instalación de un nuevo certificado personalizado.
3. Determine el FQDN (nombre del DNS) del certificado personalizado que se utilizará para definir la dirección de registro del cortafuegos en el paso 4.

Asegúrese de anotar el nombre del certificado personalizado y el FQDN asociado. Estos datos se citan en diversas ocasiones durante el proceso de configuración.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure la dirección de registro del cortafuegos en Panorama.

1. En Panorama, seleccione **Panorama >Managed WildFire Clusters (Clústeres WildFire gestionados)> *WF_cluster_name*> General.**
2. En el campo **Register Firewall To (Registrar cortafuegos a)**, especifique en nombre de DNS que se utiliza para la autenticación en el certificado personalizado (generalmente, SubjectName o SubjectAltName). Por ejemplo, el nombre de dominio predeterminado es **`wfpc.service.mycluster.paloaltonetworks.com`**.



STEP 5 | Configure la **Secure Server Communication (Comunicación de servidor segura)** de WildFire en Panorama. Si ya configuró las comunicaciones seguras entre el cortafuegos y el clúster WildFire, y utiliza el certificado personalizado existente, continúe al paso 4.

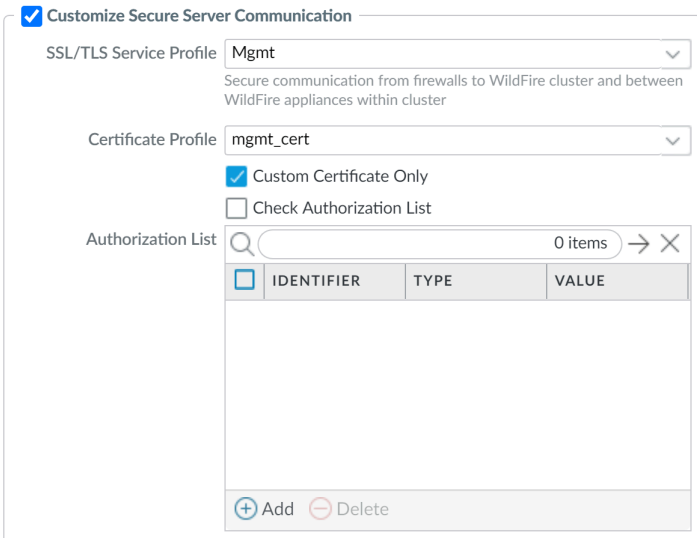
1. En Panorama, seleccione **Panorama> Managed WildFire Clusters (Clústeres WildFire gestionados)> *WF_cluster_name*> Communication (Comunicación).**
2. Haga clic en **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
3. Configure e implemente certificados personalizados utilizados por dispositivos WildFire y el cortafuegos asociado. El perfil de servicio SSL/TLS define el certificado personalizado utilizado por dispositivos WildFire para comunicarse con peers del dispositivo WildFire y el cortafuegos. Además, debe configurar los ajustes del certificado personalizado en el cortafuegos asociado al clúster de dispositivos WildFire. Esto se configura más adelante en el paso 9.

   1. Abra el menú desplegable del perfil de servicio SSL/TLS y haga clic en perfil de servicio SSL/TLS. Configure el perfil de servicio SSL/TLS con el certificado personalizado que desea utilizar. Después de configurar el perfil de servicio SSL/TLS, haga clic en OK (Aceptar) y seleccione el nuevo perfil de servicio SSL/TLS creado.

   2. Abra el menú desplegable Certificate Profile (Perfil de certificado) y haga clic en Certificate Profile (Perfil de certificado). Configure un perfil de certificado que identifique el certificado personalizado utilizado para establecer conexiones seguras entre el cortafuegos y los dispositivos WildFire, además de entre dispositivos WildFire peer. Después de configurar el perfil de certificado, haga clic en OK (Aceptar) y seleccione el nuevo perfil creado.

 ©2023 Palo Alto Networks, Inc.

4. Seleccione la casilla de verificación **Custom Certificate Only (Certificado personalizado únicamente)**. Esto le permite utilizar los certificados personalizados que configuró en lugar de los certificados configurados previamente predeterminados.
5. (Opcional) Configure una lista de autorizaciones. La lista de autorización comprueba el sujeto y el nombre alternativo del sujeto del certificado personalizado; si el **Subject (Sujeto)** o el **Subject Alt Name (Nombre alternativo del sujeto)** presentado con el certificado personalizado no coincide con un identificador en la lista de autorización, la autenticación se rechaza.
   1. Seleccione **Add (Añadir)** para añadir una lista de autorización
   2. Seleccione el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** configurado en el perfil del certificado personalizado como el tipo de identificador.
   3. Introduzca el Nombre común si el identificador es Sujeto o una dirección IP, nombre de host o correo electrónico si el identificador es Nombre alternativo del sujeto.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Check Authorization List (Comprobar lista de autorización)** para hacer cumplir la lista de autorizaciones.
6. Haga clic en **OK (Aceptar)**.



STEP 6 | Haga clic en **Enable (Habilitar)** para habilitar la comunicación de clúster segura.

STEP 7 | (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.

STEP 8 | Haga clic en **OK (Aceptar)** para guardar la configuración de **WildFire Cluster (Clúster WildFire)**.

STEP 9 | Configure los **Secure Communication Settings (Ajustes de comunicación segura)** del cortafuegos en Panorama para asociar el clúster de dispositivos WildFire con el certificado

 ©2023 Palo Alto Networks, Inc.

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 de dispositivos WildFire, y utiliza el certificado personalizado existente, continúe al paso siguiente.

1. 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.
2. Seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)** en los menús desplegables, y configúrelos para que se utilice el certificado personalizado.
3. En Customize Communication (Personalizar comunicación), seleccione **WildFire Communication (Comunicación de WildFire)**.
4. Haga clic en **OK (Aceptar)**.

STEP 10 | **Commit (Confirmar)** los cambios.

Visualización del estado del clúster WildFire con Panorama

Para confirmar que un clúster de dispositivos WildFire configurado funciona correctamente, puede ver el estado actual utilizando el dispositivo Panorama.

Palo Alto Networks recomienda utilizar la CLI del dispositivo WildFire para verificar el estado de su clúster WildFire. En el resultado del comando, se muestran los detalles de estado adicionales que no se vean en Panorama.

STEP 1 | En el dispositivo principal Panorama, seleccione **Panorama > Managed WildFire Clusters (Panorama > Clústeres de WildFire gestionados)**.

STEP 2 | En la columna **Cluster Status (Estado del clúster)**, verifique lo siguiente:

1. Los servicios de wfpc y de firma estén en funcionamiento.
2. No existan otras operaciones. Las operaciones anormales y sus condiciones de estado incluyen las siguientes:
   - Retirada [solicitado / en curso / denegado / exitoso / incorrecto]
   - Suspensión [solicitado / en curso / denegado / exitoso / incorrecto]
   - Reinicio [solicitado / en curso / denegado / exitoso / incorrecto]
   - Clúster [fuera de línea / división / no listo]
   - Servicio [suspendido / ninguno]
   - HA [peer fuera de línea / configuración desincronizada / sincronización de configuración apagada]

 ©2023 Palo Alto Networks, Inc.

STEP 3 | En la columna **Config Status (Estado de configuración)**, verifique lo siguiente:

1. La configuración del dispositivo esté **In Sync (sincronizado)** con la configuración almacenada en el dispositivo Panorama.
2. No exista otro estado. Las condiciones de estado anormales incluyen las siguientes:
   - **Out of Sync (sin sincronización)** [la configuración del dispositivo no está sincronizada con la configuración guardada en Panorama. Puede pasar el ratón por la lupa para mostrar la causa del fallo de sincronización].

STEP 4 | En la columna **Connected (Conectado)**, verifique que los dispositivos WildFire configurados muestren un estado **Connected (Conectado)**.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Gestión de licencias y actualizaciones

Puede usar el servidor de gestión Panorama™ para gestionar de forma centralizada licencias, actualizaciones de software y actualizaciones de contenido en cortafuegos y recopiladores de logs dedicados. Al implementar licencias o actualizaciones, Panorama hace una comprobación con el servidor de actualizaciones o servidor de licencias de Palo Alto Networks®, comprueba la validez de la solicitud y permite la recuperación e instalación de la licencia o actualización. Esta capacidad facilita la implementación, ya que elimina la necesidad de repetir las mismas tareas en cada dispositivo o recopilador de logs dedicado. Es de especial utilidad para gestionar los cortafuegos que no tienen un acceso directo a internet o para gestionar recopiladores de logs dedicados, que no tienen una interfaz web.

Antes de implementar las actualizaciones, consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire para obtener detalles importantes sobre la compatibilidad de la versión de actualización.

Debe activar una suscripción a la asistencia técnica directamente desde cada cortafuegos; no puede utilizar Panorama para implementar la suscripción a la asistencia técnica.

Para activar licencias o instalar actualizaciones en el servidor de gestión de Panorama, consulte Registro de Panorama e instalación de licencias e Instalación de actualizaciones de contenido y software de Panorama.

- Gestión de licencias en cortafuegos mediante Panorama

Gestión de licencias en cortafuegos mediante Panorama

En los siguientes pasos se describe cómo recuperar nuevas licencias con un código de autenticación (***auth***) y enviar las claves de licencia a los cortafuegos gestionados. También describe cómo actualizar manualmente el estado de la licencia de los cortafuegos que tienen acceso directo a Internet y los que no tienen acceso directo a Internet. En el caso de los cortafuegos que tienen acceso directo a Internet, Panorama™ automáticamente lleva a cabo comprobaciones diarias con el servidor de licencias, recupera actualizaciones y renovaciones de licencias, y las envía a los cortafuegos. La comprobación está programada para producirse entre la 1 y 2 de la mañana; y no puede modificar esta programación.

No puede utilizar Panorama para activar la licencia de asistencia técnica para los cortafuegos. Debe acceder a los cortafuegos individualmente para activar sus licencias de asistencia técnica.

Para activar las licencias de Panorama, consulte Registro de Panorama e instalación de licencias**.**

- Active las licencias adquiridas recientemente.
  1. Seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **Licenses (Licencias)** y **Activate (Activar)**.
  2. Introduzca el **Auth Code (Código de autenticación)** que Palo Alto Networks® le suministró para cada cortafuegos que tenga una licencia nueva.
  3. **Activate (Activación)** de la licencia.
  4. (Solo para suscripciones de WildFire®) Lleve a cabo una compilación en cada cortafuegos que tenga una nueva suscripción de WildFire para completar la activación:
     - Haga clic en **Commit (Confirmar)** para aceptar los cambios pendientes. Debe acceder a la interfaz web de cada cortafuegos para hacerlo.
     - Si no hay cambios de configuración pendientes, realice un cambio menor y seleccione **Commit (Confirmar)**. Por ejemplo, actualice una descripción de regla y compile el cambio. Si los cortafuegos pertenecen al mismo grupo de dispositivos, puede aplicar el cambio de regla desde Panorama para que se inicie una compilación en todos estos cortafuegos en lugar de acceder a cada cortafuegos por separado.

     Compruebe si las reglas de perfil de análisis de WildFire *incluyen los tipos de archivo avanzados que son compatibles con la suscripción a WildFire.*

- Actualice el estado de licencia de los cortafuegos.
  1. Seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **Licenses (Licencias)**.

     Cada entrada en la página indica si la licencia está activa o inactiva; también muestra la fecha de vencimiento de las licencias activas.
  2. Si activó anteriormente los códigos de autorización para la suscripción a la asistencia técnica directamente en el cortafuegos, haga clic en **Refresh (Actualizar)** y seleccione los cortafuegos de la lista. Panorama recupera la licencia, la implementa en los cortafuegos y actualiza el estado de licencia en la interfaz web de Panorama.

 ©2023 Palo Alto Networks, Inc.

3. (Solo en licencia de prevención de pérdida de datos (DLP, Data Loss Prevention) empresarial) Envíe la licencia actualizada a los cortafuegos gestionados aprovechando la DLP empresarial.

   1. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.
   2. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
   3. Seleccione **Templates (Plantillas)** y seleccione la pila de plantillas asociada con los cortafuegos gestionados que aprovechan la DLP empresarial.

      Haga clic en **OK (Aceptar)** para continuar.
   4. **Envíe** la configuración de la plantilla para actualizar correctamente la licencia de DLP empresarial.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Supervisión de la actividad de red

El servidor de gestión de Panorama™ ofrece una visión gráfica global del tráfico de red. Utilizando las herramientas de visibilidad en Panorama (el Centro de comando de aplicación (ACC), los logs y las capacidades de generación de informes) puede analizar, investigar y elaborar informes de manera centralizada sobre toda la actividad de red, identificar áreas con un posible impacto en la seguridad y traducirlas en políticas de activación de aplicaciones seguras.

Esta sección cubre los siguientes temas:

- Uso de Panorama para lograr visibilidad
- Asimilación de logs de Traps ESM en Panorama
- Caso de uso: supervisión de aplicaciones mediante Panorama
- Caso de uso: Respuesta a un incidente mediante Panorama

Uso de Panorama para lograr visibilidad

Además de sus funciones de implementación central y configuración de cortafuegos, Panorama también le permite supervisar y elaborar informes sobre todo el tráfico que atraviesa su red. Aunque las funciones de elaboración de informes de Panorama y el cortafuegos son muy parecidas, la ventaja de Panorama es que es una única vista de panel de información agregada de todos sus cortafuegos gestionados. Esta vista agregada ofrece información útil sobre tendencias en la actividad del usuario, patrones de tráfico y amenazas potenciales en toda su red.

Mediante el Centro de comando de aplicación (ACC), Appscope, el visor de logs y las opciones de elaboración de informes estándar y personalizables de Panorama, puede obtener más información rápidamente sobre el tráfico que atraviesa la red. La capacidad de ver esta información le permite evaluar en qué lugares sus políticas actuales son adecuadas y dónde son insuficientes. Luego podrá utilizar estos datos para aumentar su estrategia de seguridad de red. Por ejemplo, puede mejorar las reglas de seguridad para incrementar el cumplimiento y la responsabilidad de todos los usuarios a través de la red, o bien gestionar la capacidad de la red y reducir al mínimo los riesgos de los activos a la vez que cubre las numerosas necesidades de aplicaciones de los usuarios de su red.

En los siguientes temas se ofrece una visión de alto nivel de las capacidades de elaboración de informes en Panorama, incluido un par de casos de uso para mostrarle cómo puede utilizar estas capacidades en su propia infraestructura de red. Para obtener una lista completa de los informes y gráficos disponibles y la descripción de cada uno de ellos, consulte la ayuda en línea.

- Supervisión de la red con el ACC y Appscope
- Análisis de datos de log
- Generación, programación y envío por correo electrónico de informes
- Configuración de los límites de claves para informes programados

Supervisión de la red con el ACC y Appscope

Tanto el ACC como Appscope le permiten supervisar y elaborar informes sobre los datos registrados del tráfico que atraviesa su red.

El ACC de Panorama muestra un resumen del tráfico de red. Panorama puede consultar datos dinámicamente desde todos los cortafuegos gestionados en la red y mostrarlos en el ACC. Esta visualización le permite supervisar el tráfico por aplicaciones, usuarios y actividad de contenido (categorías de URL, amenazas, políticas de seguridad que bloquean datos o archivos de forma efectiva) en toda la red de cortafuegos de próxima generación de Palo Alto Networks.

Appscope ayuda a identificar un comportamiento inesperado o inusual en la red de un vistazo. Incluye un conjunto de gráficos e informes (informe de resumen, supervisor de cambios, supervisor de amenazas, mapa de amenazas, supervisor de red, mapa de tráfico) que le permiten analizar flujos de tráfico por amenaza o aplicación, o bien por la fuente o el destino de los flujos. También puede ordenar por sesión o por recuento de bytes.

Los administradores de plantillas y grupos de dispositivos solo pueden acceder a datos ACC y de red para grupos de dispositivos dentro de sus dominios de acceso**.**

Utilice el ACC y Appscope para responder a preguntas como las siguientes:

 ©2023 Palo Alto Networks, Inc.

ACC	Supervisar > AppScope (Appscope)
• ¿Cuáles son las principales aplicaciones utilizadas en la red y cuántas son aplicaciones de alto riesgo? ¿Quiénes son los principales usuarios de las aplicaciones de alto riesgo en la red? • ¿Cuáles son las principales categorías de URL que se visualizaron durante la última hora?	• ¿Cuáles son las tendencias de uso de aplicaciones? ¿Cuáles son las cinco principales aplicaciones que han aumentado su uso y las cinco principales que han disminuido su uso? • ¿Cómo ha cambiado la actividad de los usuarios a lo largo de la semana actual en comparación con la semana pasada o el mes pasado?
• ¿Cuáles son las principales aplicaciones que utilizan ancho de banda? ¿Cuáles son los usuarios/hosts que consumen el mayor ancho de banda? • ¿Qué contenido o archivos se están bloqueando? ¿Hay usuarios específicos que activan esta regla de filtrado de datos/bloqueo de archivos? • ¿Cuál es la cantidad de tráfico intercambiado entre dos direcciones IP específicas o generado por un usuario específico? ¿Cuál es la ubicación geográfica del servidor o cliente de destino?	• ¿Qué usuarios y aplicaciones absorben la mayor parte del ancho de banda de la red? ¿Cómo ha cambiado este consumo durante los últimos 30 días? • ¿Cuáles son las amenazas en la red y cómo se distribuyen geográficamente estas amenazas de tráfico de entrada y salida?

A continuación, podrá utilizar la información para mantener o aplicar cambios en los patrones de tráfico de su red. Consulte Caso de uso: supervisión de aplicaciones mediante Panorama para conocer brevemente cómo pueden influir las herramientas de visibilidad de Panorama en el modo en que moldea las políticas de uso aceptable para su red.

Aquí tiene algunos consejos que le ayudarán a navegar por el ACC:

©2023 Palo Alto Networks, Inc.

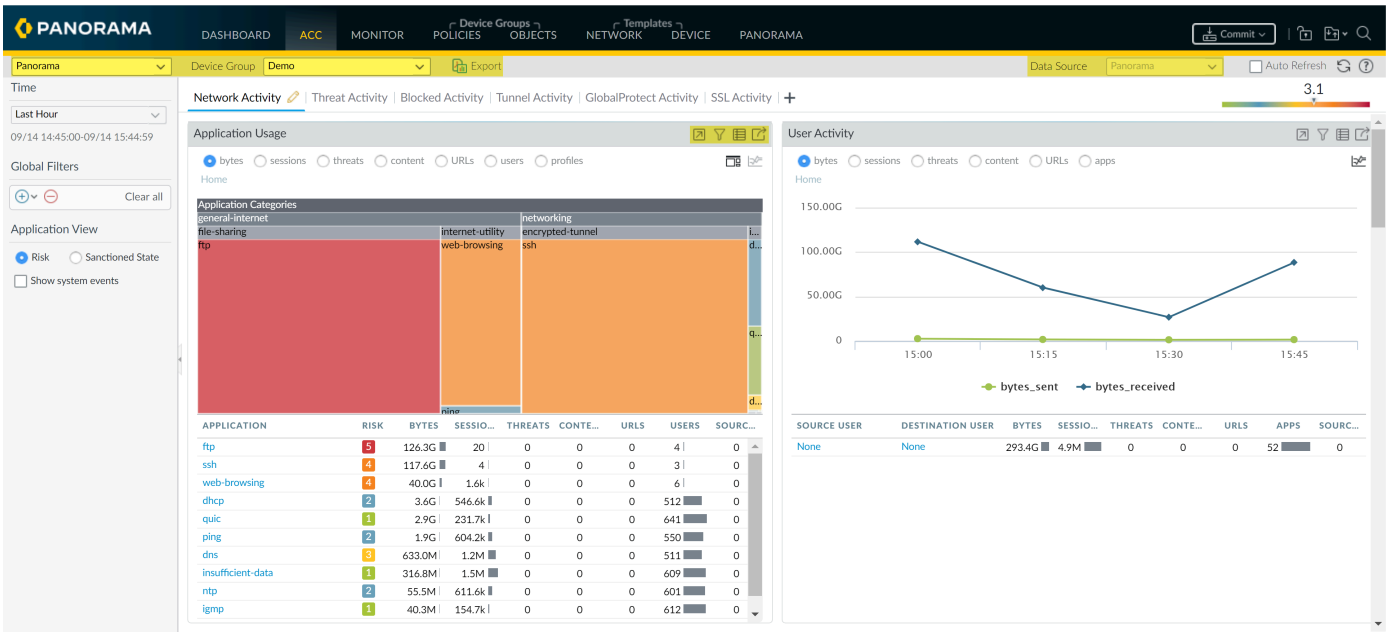


Figure 23: Consejos de navegación del ACC

- **Cambie de la vista de Panorama a la vista de dispositivo**: use el menú desplegable **Context (Contexto)** para acceder a la interfaz web de cualquier cortafuegos gestionado. Para obtener más detalles, consulte Cambio de contexto: cortafuegos o Panorama.
- **Cambie el grupo de dispositivos y el origen de datos:** el **Data Source (Fuente de datos)** predeterminado que se utiliza para mostrar las estadísticas en los gráficos del ACC son los datos locales de **Panorama**, y la configuración predeterminada de **Device Group (Grupo de dispositivos)** es **All (Todos)**. La utilización de datos locales en Panorama permite cargar rápidamente los gráficos. Sin embargo, puede cambiar el origen de datos a **Remote Device Data (Datos de dispositivo remoto)** si todos los cortafuegos gestionados se encuentran en PAN-OS 7.0 o una versión posterior. Si los cortafuegos gestionados tienen una combinación de PAN-OS 7.0 y versiones anteriores, solo puede ver los datos de Panorama. Cuando se configura para utilizar datos de un dispositivo remoto, Panorama sondeará todos los cortafuegos gestionados y presentará una vista agregada de los datos. La visualización en pantalla muestra el número total de cortafuegos que se están sondeando y el número de cortafuegos que han respondido a la consulta de información.
- **Seleccione las pestañas y los widgets para ver**: el ACC incluye tres pestañas y una variedad de widgets que le permiten encontrar la información que le interesa. A excepción del widget de uso de la aplicación y el widget de información del host, el resto de los widgets solamente muestran datos si la función correspondiente tiene licencia en el cortafuegos y el usuario ha habilitado el registro.
- **Período de tiempo para modificaciones y límite de datos**: el período de tiempo de elaboración de informes en el ACC va desde los últimos 15 minutos hasta la última hora, día, semana, mes o cualquier período de tiempo personalizado. De forma predefinida, cada widget muestra los 10 elementos principales y añade todos los elementos restantes como **other (otros)**. Puede clasificar los datos de cada widget con diferentes atributos como, por ejemplo, sesiones, bytes, amenazas, contenido y URL. También puede configurar filtros locales para filtrar la visualización dentro de la tabla y del gráfico en un widget, y luego promover el filtro del widget como un filtro global para girar la vista en todos los widgets del ACC.

 ©2023 Palo Alto Networks, Inc.

Análisis de datos de log

La pestaña **Monitor (Supervisar)** de Panorama permite acceder a datos de logs; estos logs son una lista archivada de sesiones que han sido procesadas por los cortafuegos gestionados y reenviadas a Panorama.

Los datos de logs pueden agruparse ampliamente en dos tipos: los que dan información detallada sobre los flujos de tráfico en su red como aplicaciones, amenazas, perfiles de información de host, categorías de URL, tipos de contenido/archivo y los que registran eventos del sistema, cambios de configuración e información de asignación de User-ID™.

Sobre la base de la configuración de reenvío de logs de los cortafuegos gestionados, la pestaña **Monitor (Supervisar)** > **Logs** puede incluir logs de flujos de tráfico, amenazas, filtrado de URL, filtrado de datos, coincidencias de perfil de información de host (host information profile, HIP) y envíos de WildFire™. Puede revisar los logs para consultar gran cantidad de información acerca de una sesión o transacción concretas. Algunos ejemplos de esta información son el usuario que inició la sesión, la acción (permitir o denegar) que realizó el cortafuegos en la sesión y las zonas, direcciones y puertos de origen y destino. Los logs de sistema y configuración pueden indicar un cambio de configuración o una alarma activada por el cortafuegos cuando se supera un umbral configurado.

*Si Panorama gestionará los cortafuegos que ejecutan versiones de software anteriores a PAN-OS 7.0, especifique un servidor WildFire desde el cual Panorama pueda recopilar información de análisis para las muestras de WildFire que aquellos cortafuegos envíen. Panorama usa la información para completar los logs WildFire Submissions (Presentaciones de WildFire) a los que les falta valores de campo en PAN-OS 7.0. Los cortafuegos que ejecutan versiones anteriores no completarán estos campos. Para especificar el servidor, seleccione **Panorama** > **Setup (Configuración)** > **WildFire**, edite la Configuración general e introduzca el nombre de **WildFire Private Cloud (Nube privada de WildFire)**. El valor predeterminado es **wildfire-public-cloud**, que es la nube de WildFire alojada en los Estados Unidos.*

Generación, programación y envío por correo electrónico de informes

Puede configurar informes para que se ejecuten inmediatamente o programarlos para que se ejecuten a intervalos específicos. Puede guardar y exportar los informes o enviarlos por correo electrónico a destinatarios específicos. El envío por correo electrónico es de especial utilidad si desea compartir informes con administradores que no tengan acceso a Panorama. Panorama admite los mismos tipos de informes que el cortafuegos de Palo Alto Networks.

A partir de Panorama 10.0.2 y la versión 1.8.0 del complemento Cloud Services, puede generar informes programados sobre los datos de Cortex Data Lake.

En PAN-OS 10.0.3 y versiones posteriores, esta función está habilitada de forma predeterminada.

Para ello, primero debe habilitar la función desde la CLI de Panorama introduciendo

```
admin@Panorama> request plugins cloud_services logging-service sched-report-enable
```

 ©2023 Palo Alto Networks, Inc.

Una compilación regular no habilitará este cambio. En su lugar, debe cambiar al modo de configuración:

```
admin@Panorama> configure
```

e introducir

```
admin@Panorama# commit force
```

Luego, siga los pasos a continuación para generar informes programados.

Se recomienda instalar las versiones de software correspondientes en Panorama y los cortafuegos para los que generará informes. Por ejemplo, si el servidor de gestión Panorama ejecuta Panorama 10.0, instale PAN-OS 10.2 en sus cortafuegos gestionados antes de generar los informes. Este procedimiento evita los problemas que podrían producirse si crea informes que incluyen campos compatibles con la versión de Panorama pero incompatibles con una versión anterior de PAN-OS en los cortafuegos.

STEP 1 | Configure informes predefinidos de Panorama.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite**Logging and Reporting (Logs e informes)**.
2. (Opcional) Seleccione **Log Export and Reporting (Exportación de logs y creación de informes)** y habilite (marque) **Use Data for Pre-Defined Reports (Usar datos para informes predefinidos)** para descargar la agregación de informes por hora a los recopiladores de logs.

   Se recomienda habilitar esta configuración para cortafuegos VM-50, VM-50 Lite y PA-200.
3. Seleccione **informes predefinidos** y habilite (marque) los informes predefinidos que enviar desde Panorama.
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **confirme** los cambios de configuración.
5. (Solo en cortafuegos VM-50, VM-50 Lite y PA-200) Acceda a la CLI del cortafuegos para habilitar informes predefinidos.

   Este comando debe ejecutarse en cada cortafuegos VM-50, VM-50 Lite y PA-200.

   ```
   admin> debug run-panorama-predefined-report yes
   ```

STEP 2 | Configure Panorama para recibir y almacenar información de usuarios y grupos de usuarios que recibe de los cortafuegos.

Necesario para generar informes basados en nombres de usuario y grupos en lugar de solo direcciones IP.

 ©2023 Palo Alto Networks, Inc.

1. Si desea que Panorama incluya información del grupo de usuarios en los informes, actualice los cortafuegos gestionados a PAN-OS 8.1 o una versión posterior. Panorama no puede sincronizar la información de grupo de los cortafuegos que ejecutan versiones anteriores.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**, edite la configuración de Panorama y haga clic en **Enable reporting and filtering on groups (Habilitar informes y filtrado en grupos)**.
3. Realice la Add a Device Group (Adición de un grupo de dispositivos) si aún no lo ha hecho. Para cada grupo de dispositivos:
   - Seleccione un **Master Device (Dispositivo maestro)**, que es el cortafuegos que proporciona información de usuarios y grupos de usuarios a Panorama.
   - Habilite Panorama para **Store users and groups from Master Device (Almacenar usuarios y grupos del dispositivo maestro)**.

STEP 3 | Genere informes.

Los informes de resumen programados y de Run Now (Ejecutar ahora) para la misma base de datos y el mismo período de tiempo tienen discrepancias en los datos que se muestran en cada informe. Esto se debe a la forma en que los recopiladores de logs y los cortafuegos añaden logs durante la agregación horaria.

Los pasos para generar un informe dependen del tipo.

- Informes personalizados:
  1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** y **Add (Añadir)** para añadir el informe.
  2. Introduzca un **Name (Nombre)** para identificar el informe.
  3. Seleccione una **Database (Base de datos)** para el informe.

     Puede basar el informe en **Summary Databases (Bases de datos de resumen)** o **Detailed Logs (Logs detallados)** bases de datos.

     Para basar el informe en los logs almacenados en el servidor de gestión de Panorama y los recopiladores de logs, seleccione **Panorama Data (Datos de Panorama)** (recomendado para un rendimiento más rápido)

     Para basar los informes en los logs almacenados en los cortafuegos gestionados, seleccione **Remote Device Data (Datos de dispositivo remoto)**. Esta opción es para los casos en que los cortafuegos pueden tener logs que aún no se reenviaron a Panorama. Sin embargo,

 ©2023 Palo Alto Networks, Inc.

debido a que Panorama debe consultar los cortafuegos directamente, esta opción es más lenta.

4. Seleccione **Scheduled (Programado)**.
5. Defina sus criterios de filtrado de logs seleccionando **Time Frame (Periodo de tiempo)**, **Sort By (Ordenar por)** orden, **Group By (Agrupar por)** preferencia, y las columnas (atributos de log) que mostrará el informe.

   *Es obligatorio seleccionar el orden en **Sort By (Ordenar por)** para generar informes precisos. Si no lo selecciona, los informes personalizados generados se rellenan con las últimas coincidencias de logs de la base de datos seleccionada.*
6. (Opcional) Utilice el **Query Builder (Generador de consultas)** para refinar los criterios de filtrado de logs más basado en atributos de log.
7. Para comprobar los ajustes de informes, seleccione **Run now (Ejecutar ahora)**. Si es necesario, modifique la configuración para cambiar la información que muestra el informe.
8. Haga clic en **OK (Aceptar)** para guardar el informe personalizado.

- **PDF Summary Report (Informe de resumen en PDF)**:
  1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **Manage PDF Summary (Gestión de informes de resumen en PDF)** y añada el informe.
  2. Introduzca un **Name (Nombre)** para identificar el informe.
  3. Utilice la lista desplegable para cada grupo de informes y seleccione uno o varios de los elementos para diseñar el informe de resumen en PDF. Puede incluir hasta 18 elementos.
  4. Haga clic en **OK (Aceptar)** para guardar los ajustes.

STEP 4 | Configure un **Report Group (Grupo de informes)**.

Puede incluir informes predefinidos, informes de resumen en PDF e informes personalizados. Panorama compila todos los informes incluidos en un único PDF.

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **Report Groups (Grupos de informes)** y haga clic en **Add (Añadir)** para añadir un grupo de informes.
2. Introduzca un nombre en **Name (Nombre)** para identificar el grupo de informes.
3. (Opcional) Seleccione la **Title Page (Título de página)** y añada un **Title (Título)** para el PDF creado.
4. Seleccione informes en las listas Informe predefinido, Informe personalizado e Informe de resumen en PDF.
5. Seleccione **Add (Añadir)** para añadir los informes seleccionados al grupo de informes.
6. Haga clic en **OK (Aceptar)** para guardar los ajustes.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configure un perfil del servidor de correo electrónico.

El perfil define de qué manera el cortafuegos se conecta con el servidor y envía el correo electrónico.

1. Seleccione **Panorama** > **Server Profiles (Perfiles de servidor)** > **Email (Correo electrónico)** y haga clic en **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Seleccione **Add (Añadir)** para añadir hasta cuatro servidores SMTP y **Add (Añadir)** la siguiente información para cada uno:
   - **Name (Nombre)**: un nombre para identificar el servidor SMTP (de 1a 31 caracteres). Este campo es solo una etiqueta y no tiene que ser el nombre de host de un servidor existente.
   - **Email Display Name (Nombre para mostrar en el correo electrónico)**: El nombre que aparecerá en el campo De del correo electrónico.
   - **From (De)**: la dirección de correo electrónico desde la que se enviarán las notificaciones de correo electrónico.
   - **To (Para)**: La dirección de correo electrónico a la que se enviarán las notificaciones de correo electrónico.
   - **Additional Recipient (Destinatario adicional)**: si desea que las notificaciones se envíen a una segunda cuenta, introduzca la dirección adicional aquí.
   - **Email Gateway (Puerta de enlace de correo electrónico)**: La dirección IP o el nombre de host de la puerta de enlace SMTP que se usará para enviar los mensajes de correo electrónico.
4. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 6 | Programe el informe para la entrega de correos electrónicos.

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes PDF)** > **Email Scheduler (Programador de correo electrónico)** y haga clic en **Add (Añadir)** para añadir un perfil de programador de correo electrónico.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Seleccione el **Report Group (Grupo de informes)**, el perfil del servidor de correo electrónico que recién creó (**Email Profile [Perfil de correo electrónico]**) y la **Recurrence (Frecuencia)** del informe (**Disable (Deshabilitar)** por defecto).
4. **Send test email (Enviar correo electrónico de prueba)** para verificar que la configuración del correo electrónico sea precisa.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.
6. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

Configuración de los límites de claves para informes programados

El servidor de gestión Panorama™ y los informes del cortafuegos de PA-7000 Series utilizan claves (valores únicos en los que puede añadir) de uno o más recopiladores de logs para crear y generar informes. Para mejorar la precisión de los informes programados, ahora puede configurar los límites

 ©2023 Palo Alto Networks, Inc.

de claves máximo y mínimo. Puesto que la cantidad de claves admitidas aumenta, los informes programados ahora pueden incluir más datos que se pueden añadir, ordenar y agrupar.

El límite de claves mínimo predeterminado se basa en los valores **Sort By (Ordenar por)** y **Group By (Agrupar por)** configurados para el informe programado mediante el siguiente cálculo:

<Sort By value> x 100 x <Group By value>

Por ejemplo, si **Sort By (Ordenar por)** se configura como **Top 25 (Principales 25)** y **Group By (Agrupar por)** como **5 Groups (5 grupos)**, el límite de claves mínimo predeterminado es de 12 500 claves. El valor de **Group By (Agrupar por)** no se tiene en cuenta en el cálculo cuando se establece en **None (Ninguno)**. El límite de claves mínimo predeterminado está limitado y no puede superar el límite de clave máximo.

Solo puede configurar los límites de clave para los dispositivos M-Series y los dispositivos virtuales Panorama. Los límites de claves de PA-7000 Series no se pueden configurar.

Las claves máximas y mínimas admitidas aumentan para los siguientes modelos de Panorama:

Modelo de Panorama	Límite de claves mínimo	Límite de claves máximo
PA-7000 Series	1000: predeterminado, no configurable	25 000: predeterminado, no configurable
M-200	15 000	50 000
M-500	15 000	50 000
M-600	15 000	50 000
Dispositivo virtual Panorama en modo heredado	5000	25 000
Dispositivo virtual Panorama (todos los modelos compatibles)	15 000	50 000

STEP 1 | Inicio de sesión en la CLI de Panorama.

STEP 2 | Configure el límite de claves máximo con el siguiente comando:

Puede establecer el límite máximo de claves entre 0 y 50, donde 50 equivale a 50 000 claves. En este ejemplo, establecemos el límite máximo de claves para el dispositivo virtual Panorama en 30 000 claves.

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure el límite mínimo de claves con el siguiente comando:

Puede establecer el límite mínimo de claves entre 0 y 15, donde 15 equivale a 15 000 claves. En este ejemplo, establecemos el límite mínimo de claves para el dispositivo virtual Panorama en 15 000 claves.

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | (Opcional) Establezca el límite de claves mínimo en la configuración predeterminada.

```
admin@Panorama> request min-report-keys set limit 0
```

STEP 5 | Confirme los nuevos límites de claves máximo y mínimo para Panorama con el siguiente comando:

```
admin@Panorama> commit-all
```

 ©2023 Palo Alto Networks, Inc.

Asimilación de logs de Traps ESM en Panorama

La visibilidad es un primer paso crítico para prevenir y reducir el impacto de un ataque. Para ayudarle a enfrentarse a este desafío, Panorama proporciona una vista integrada de logs de cortafuegos (eventos en la red) y de logs de Traps™ ESM Server (eventos de seguridad en los endpoints) para que pueda rastrear cualquier actividad sospechosa o maliciosa.

Para conocimiento y contexto sobre los eventos observados en la red y en sus endpoints, reenvíe los eventos de seguridad que los agentes de Traps informan al servidor ESM en Panorama. Panorama puede servir como un receptor Syslog que ingiere estos logs de los componentes de ESM de Traps utilizando Syslog a través de TCP, UDP o SSL. Luego, Panorama puede correlacionar eventos discretos de seguridad que ocurren en los endpoints con lo que está sucediendo en la red y generar evidencia de coincidencia. Esta evidencia le brinda más contexto sobre la cronología y el flujo de eventos para investigar problemas y solucionar brechas de seguridad en su red.

STEP 1 | Defina el perfil de ingestión de logs en Panorama y adjúntelo a un grupo de recopiladores.

El dispositivo virtual Panorama en modo heredado no puede ingerir logs de Traps.

1. Seleccione **Panorama** > **Log Ingestion Profile (Perfil de ingestión de log)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Haga clic en **Add (Añadir)** e introduzca los detalles para el servidor ESM. Puede añadir hasta 4 servidores ESM a un perfil.
   1. Introduzca un **Source Name (Nombre de origen)**.
   2. Especifique el **Port (Puerto)** en el que Panorama escuchará los mensajes syslog. El intervalo es de 23.000 a 23.999.
   3. Seleccione el protocolo de capa de **Transport (Transporte)**: TCP, UDP o SSL.
   4. Seleccione Traps_ESM para **External Log type (Tipo de log externo)** y la **Version (Versión)** de los Traps ESM. Por ejemplo, para Traps ESM 4.0 o 4.1, seleccione **3.4.1+**.

      A medida que los formatos de log de Traps se actualizan, las definiciones de log actualizadas estarán disponibles a través de actualizaciones de contenido en Panorama.
4. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** > **Log Ingestion (Ingestión de log)** y haga clic en **Add (Añadir)** para añadir el perfil de ingestión de logs para que el grupo de recopiladores pueda recibir logs de los servidores ESM en la lista del perfil.

   Si habilita SSL para la comunicación syslog segura entre Panorama y los servidores de ESM, debe adjuntar un certificado a los recopiladores gestionados que pertenecen al grupo de recopiladores (**Panorama** > **Managed Collectors [Recopiladores gestionados]** > **General** y seleccione el certificado que utilizará para el **Inbound Certificate for Secure Syslog [Certificado entrante de Syslog seguro]**).
5. **Commit (Confirmar)** los cambios realizados a Panorama y el Grupo de recopiladores.

STEP 2 | Configure Panorama como un receptor Syslog en el servidor ESM.

Traps ESM 4.0 y las versiones posteriores admiten el reenvío de logs a un receptor syslog externo y a Panorama. Dado que las versiones anteriores de Traps ESM no admiten el reenvío de logs

 ©2023 Palo Alto Networks, Inc.

a varios receptores syslog, debe configurar Panorama como un receptor syslog en los ajustes **Syslog** (para ESM 3.4, consulte Habilitar el envío de logs a una plataforma de logging externa).

Para Traps ESM 4.0 y versiones posteriores:

1. En la consola ESM, seleccione **Settings (Ajustes)** > **ESM** > **Panorama** y haga clic en **Enable log forwarding to Panorama (Habilitar reenvío de logs a Panorama)**.
2. Ingrese el nombre de host de Panorama o la dirección IP como **Panorama Server (Servidor Panorama)** y el **Panorama Server Port (Puerto de servidor Panorama)** en el que Panorama está escuchando. Repita este paso para un **Panorama Failover Server (Servidor de conmutación por error Panorama)** opcional.
3. Seleccione el **Communication Protocol (Protocolo de comunicación)** de transporte: TCP, TCP con SSL o UDP. Si selecciona TCP con SSL, el servidor ESM requiere un certificado de servidor para habilitar la autenticación de cliente.

   Desde Panorama, debe exportar el certificado de CA raíz para el Certificado de entrada para Syslog seguro e importar el certificado al almacén de certificados raíz de confianza del host en el que ha instalado el servidor ESM.

STEP 3 | Ver logs ESM y eventos correlacionados.

1. Seleccione **Monitor (Supervisar)** > **External Logs (Logs externos)** > **Traps ESM** para ver los logs ingeridos en Panorama.
2. Seleccione **Monitor (Supervisar)** > **Automated Correlation Engine (Motor de correlación automatizada)** > **Correlated Events (Eventos correlacionados)** y filtre en el nombre de objeto de correlación **Wildfire and Traps ESM Correlated C2 (C2 correlacionado de Wildfire y Traps ESM)** para encontrar eventos correlacionados. Panorama genera eventos correlacionados cuando un host en su red exhibe actividad de comando y control que coincide con el comportamiento observado para un archivo malicioso en el entorno virtual de WildFire. Este evento correlacionado le alerta de actividades sospechosas que un agente de Traps y el cortafuegos han observado en uno o más hosts infectados en su red.

 ©2023 Palo Alto Networks, Inc.

Caso de uso: supervisión de aplicaciones mediante Panorama

Este ejemplo le muestra todo el proceso de evaluación de la eficacia de sus políticas actuales y de determinación de los puntos donde necesita ajustarlas para fortalecer las políticas de uso aceptable para su red.

Cuando se registra en Panorama, el widget **Top Applications (Aplicaciones principales)** en el **Dashboard (Panel)** ofrece una vista previa de las aplicaciones más utilizadas durante la última hora. Para mostrar el widget, seleccione **Widgets** > **Application (Aplicación)** > **Top Applications (Aplicaciones principales)** en la barra de herramientas. Puede echar un vistazo a la lista de aplicaciones principales y pasar el ratón por encima de cada bloque de aplicaciones del que quiera obtener información detallada, o bien puede seleccionar la pestaña **ACC** para ver la misma información en una lista ordenada. La siguiente imagen es una vista del widget **Top Applications (Aplicaciones principales)** del **Dashboard (Panel)**.

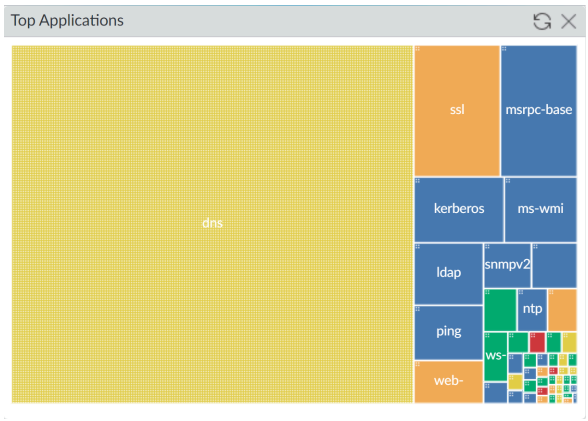


Figure 24: Widget de aplicaciones principales

El origen de datos de esta visualización es la base de datos de estadísticas de aplicación, ya que no utiliza los logs de tráfico y se genera tanto si se han habilitado los logs para reglas de seguridad como si no. Esta visualización del tráfico de su red muestra todo lo que está permitido en su red y fluye sin bloqueos por parte de las reglas de políticas que haya definido.

En la pestaña **ACC**, puede seleccionar y cambiar **Data Source (Fuente de datos)** para que sea local en **Panorama** o puede consultar los cortafuegos gestionados (**Remote Device Data [Datos de dispositivo remoto]**) para los datos; Panorama automáticamente agrega y muestra la información. Para lograr un flujo más veloz, considere utilizar Panorama como el origen de datos (con el reenvío de logs a Panorama habilitado), ya que el tiempo necesario para cargar datos desde los cortafuegos gestionados varía según el período de tiempo que seleccione para visualizar datos y el volumen de tráfico generado en su red. Si sus cortafuegos gestionados tienen una combinación de PAN-OS 7.0 y versiones anteriores, la función **Remote Device Data** no estará disponible.

El ejemplo de **Dashboard (Panel)** en Figure 1 muestra DNS como una aplicación popular. Si hace clic en el bloque de aplicaciones de DNS, Panorama abre la pestaña **ACC** > **Network Activity (Actividad de red)** con DNS aplicado como filtro global y muestra información, detalles del nivel de riesgo y características de la aplicación, y los usuarios que accedieron a ella.

©2023 Palo Alto Networks, Inc.

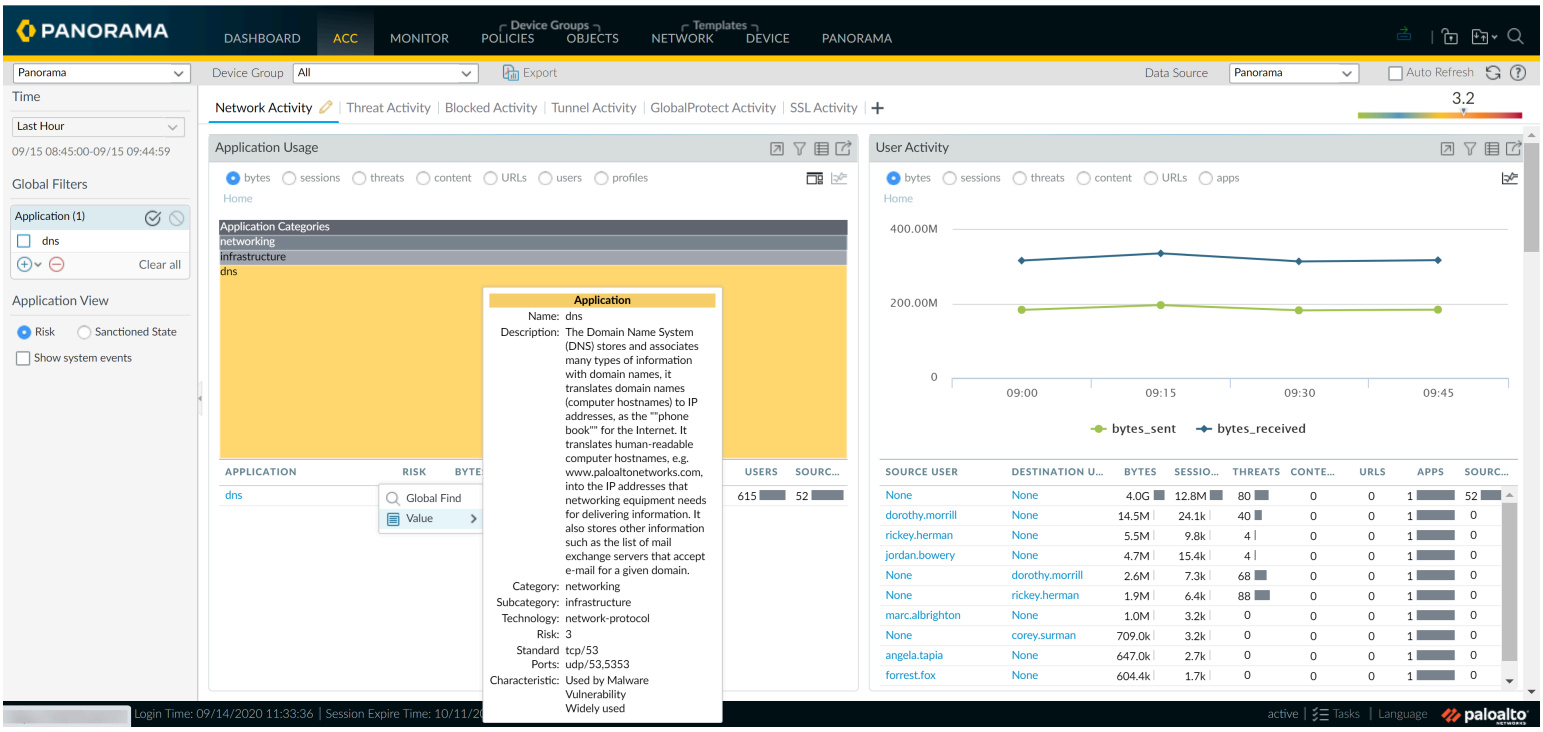


Figure 25: Pestaña Actividad de red

En el widget **User Activity (Actividad de usuario)**, puede ver cuántos usuarios están utilizando DNS y el volumen de tráfico que se está generando. Si habilitó el ID de usuario, podrá ver los nombres de los usuarios que están generando este tráfico y obtener detalles para revisar todas las sesiones, el contenido o las amenazas asociadas con cada usuario.

Visualice el widget **Compromised Hosts (Hosts comprometidos)** en la pestaña **Threat Activity (Actividad de amenazas)** para ver qué objetos de correlación coinciden y visualizar la evidencia de coincidencia asociada con el usuario y la aplicación. También puede ver el nombre de la amenaza, la categoría y el ID en el widget **Threat Activity (Actividad de amenazas)**.

Con DNS configurado como un filtro global, use los widgets **Destination IP Activity (Actividad de IP de destino)** y **Destination Regions (Regiones de destino)** para verificar hacia dónde se destinó el tráfico. También puede ver las zonas de ingreso y egreso, y la regla de seguridad que permite esta conexión.

Para obtener información más detallada, ingrese a los logs de tráfico para obtener una vista filtrada y revise cada entrada de log para conocer los puertos utilizados, los paquetes enviados y los bytes enviados y recibidos. Ajuste las columnas para ver más o menos información basándose en sus necesidades.

La pestaña **Monitor (Supervisar)** > **App-Scope Traffic Map (Mapa de tráfico)** muestra un mapa geográfico del flujo de tráfico y proporciona una vista del tráfico entrante frente al tráfico saliente. También puede utilizar la pestaña **Monitor (Supervisar)** > **App-Scope** > **Change Monitor (Supervisor de cambios)** para ver los cambios en los patrones de tráfico. Por ejemplo, compare las aplicaciones principales utilizadas durante esta hora con las utilizadas durante la semana pasada o el mes pasado para determinar si hay un patrón o tendencia.

Con toda la información que ha descubierto, ahora puede evaluar qué cambios hacer en las configuraciones de sus políticas. Aquí tiene algunas sugerencias que considerar:

©2023 Palo Alto Networks, Inc.

- Sea restrictivo y cree una regla previa en Panorama para bloquear o permitir todo el tráfico de DNS. A continuación, use los grupos de dispositivos Panorama para crear y enviar esta regla de política a uno o más cortafuegos.
- Aplique límites de uso de ancho de banda y cree una regla de política y perfil de QoS que retire la prioridad del tráfico no comercial. Use los grupos de dispositivos y las plantillas de Panorama para configurar QoS y luego enviar reglas en uno o más cortafuegos.
- Programe un grupo de informes personalizados que recopile la actividad del usuario específico y de las aplicaciones principales utilizadas en su red para observar ese patrón durante una o dos semanas más antes de realizar una acción.

Además de comprobar una aplicación específica, también puede comprobar cualquier aplicación desconocida de la lista de aplicaciones principales. Son aplicaciones que no coinciden con una firma de App-ID™ definida y aparecen como UDP desconocido y TCP desconocido. Para ahondar en estas aplicaciones desconocidas, haga clic en el nombre para desglosar los detalles del tráfico sin clasificar.

Utilice el mismo proceso para investigar las direcciones IP de origen principales de los hosts que iniciaron el tráfico desconocido junto con la dirección IP del host de destino para el que se estableció la sesión. Para el tráfico desconocido, los logs de tráfico, de manera predeterminada, realizan una captura de paquetes (PCAP) cuando se detecta una aplicación desconocida. La flecha verde de la columna de la izquierda representa el fragmento de código de captura de paquetes de los datos de la aplicación. Si hace clic en la flecha verde, mostrará la captura de paquetes (PCAP) en el explorador.

Con las direcciones IP de los servidores (IP de destino), el puerto de destino y las capturas de paquetes, estará en una posición privilegiada para identificar la aplicación y tomar una decisión sobre qué acción desea realizar en su red. Por ejemplo, puede crear una aplicación personalizada que identifique este tráfico en lugar de etiquetarlo como tráfico de TCP o UDP desconocido. Consulte el artículo Identificación de aplicaciones desconocidas para obtener más información sobre cómo identificar aplicaciones desconocidas y Firma de aplicación personalizada para obtener información sobre cómo desarrollar firmas personalizadas para distinguir la aplicación.

 ©2023 Palo Alto Networks, Inc.

Caso de uso: Respuesta a un incidente mediante Panorama

Las amenazas de red pueden originarse desde diferentes vectores, incluidas infecciones de software malintencionado y spyware debidas a descargas ocultas, ataques de phishing, servidores sin parches y ataques de denegación de servicio (DoS) aleatorios o con destino específico, por nombrar unos cuantos métodos de ataque. La capacidad de reaccionar ante una infección o un ataque a la red requiere procesos y sistemas que avisen al administrador del ataque y proporcionen las pruebas expertas necesarias para realizar un seguimiento del origen y los métodos utilizados para lanzar el ataque.

La ventaja de Panorama es una vista centralizada y consolidada de los patrones y logs recopilados desde los cortafuegos gestionados de su red. Puede usar la información del motor de correlación automatizado, sola o en conjunto con los informes y logs generados desde un Gestor de eventos, información y seguridad (Security Information Event Manager, SIEM), para investigar cómo se ha activado un ataque y cómo prevenir ataques futuros y pérdidas o daños en su red.

Las preguntas que explora este caso de uso son:

- ¿Cómo se le notifica un incidente?
- ¿Cómo corrobora que el incidente no es un falso positivo?
- ¿Cuál es su plan de acción inmediato?
- ¿Cómo utiliza la información disponible para reconstruir la secuencia de eventos que precedió o siguió al evento desencadenante?
- ¿Qué cambios debe considerar para proteger su red?

Este caso de uso hace un seguimiento a un incidente específico y muestra de qué modo las herramientas de visibilidad de Panorama pueden ayudarle a responder al informe.

- Notificación de incidentes
- Revisión de widgets en el ACC
- Revisión de logs de amenaza
- Revisión de logs de WildFire
- Revisión de logs de filtrado de datos
- Actualización de reglas de seguridad

Notificación de incidentes

Se le puede avisar de varias formas de un incidente dependiendo de cómo haya configurado los cortafuegos de Palo Alto Networks y de qué herramientas externas estén disponibles para un análisis posterior. Puede recibir una notificación por correo electrónico activada por una entrada de log registrada en Panorama o en su servidor Syslog, se le puede informar a través de un informe especializado generado en su solución SIEM, o bien una agencia o un servicio pagado externo puede notificarle. En este ejemplo, vamos a suponer que ha recibido una notificación de Panorama por correo electrónico. El mensaje de correo electrónico le informa de un evento activado por una alerta para Zero Access gent.Gen Command And Control Traffic (Comando gent.Gen de acceso cero y tráfico de control) que coincide con una firma de spyware. En el mensaje de correo electrónico

 ©2023 Palo Alto Networks, Inc.

también se indica la dirección IP del origen y el destino de la sesión, un ID de amenaza y la marca de tiempo de cuándo se registró el evento.

Revisión de widgets en el ACC

En la pestaña **ACC** > **Threat Activity (Actividad de amenazas)**, revise si existen amenazas críticas o de gravedad alta en los widgets **Compromised Hosts (Hosts comprometidos)** y **Threat Activity (Actividad de amenazas)**. En el widget **Compromised Hosts (Hosts comprometidos)**, observe los objetos coincidentes y haga clic en un valor de Recuento de coincidencia para ver la evidencia de coincidencia del incidente asociado.

Revisión de logs de amenaza

Para empezar a investigar la alerta, utilice el ID de amenaza para buscar los logs de amenazas en Panorama (**Monitor [Supervisar]** > **Logs [Logs]** > **Threat [Amenaza]**). Desde los logs de amenazas, puede buscar la dirección IP de la víctima, exportar la captura de paquetes (PCAP) haciendo clic en el icono de descarga de la entrada del log, y utilizar una herramienta de análisis de red como WireShark para revisar la información detallada del paquete. En el caso de HTTP, busque un SITIO DE REFERENCIA HTTP falso o con formato incorrecto en el protocolo, un host sospechoso, cadenas de URL, el agente del usuario, la dirección IP y el puerto para validar el incidente. Los datos de estas capturas de paquetes también son útiles para buscar patrones de datos similares y crear firmas personalizadas o modificar políticas de seguridad para enfrentarse mejor a la amenaza en el futuro.

Como resultado de esta revisión manual, si confía en la firma, considere trasladar la firma de una acción de alerta a una acción de bloqueo para un enfoque más agresivo. En algunos casos, puede decidir añadir el IP del atacante a una lista de bloqueo de IP para evitar que el tráfico de esa dirección IP vuelva a llegar a la red interna.



*Si observa una firma de spyware basada en DNS, la dirección IP de su servidor DNS local podría aparecer como la dirección **Victim IP (IP de la víctima)**. A menudo esto se debe a que el cortafuegos se encuentra al norte del servidor DNS local, por lo que las consultas DNS muestran el servidor DNS local como la IP de origen, en lugar de mostrar la dirección IP del cliente que originó la solicitud.*

Si se presenta este problema, active la acción de socavamiento de DNS en el perfil de antispyware en las reglas de seguridad para identificar los hosts afectados en su red. El socavamiento de DNS le permite controlar las conexiones salientes a dominios malintencionados y redirige las consultas de DNS a una dirección IP interna que no se utiliza; el socavamiento no saca una respuesta. Cuando el host comprometido inicia una conexión con un dominio malintencionado, en vez de salir a Internet, el cortafuegos redirige la solicitud a la dirección IP que haya definido y que está socavada. Ahora, al revisar los logs de tráfico de todos los hosts que conectaron con el socavamiento, podrá localizar todos los hosts comprometidos y tomar acciones de remedio para evitar la propagación.

Para continuar con la investigación del incidente, utilice la información del atacante y la dirección IP de la víctima para obtener información adicional, como la siguiente:

- ¿Cuál es la ubicación geográfica del atacante? ¿La dirección IP es una dirección IP individual o una dirección IP con NAT?

 ©2023 Palo Alto Networks, Inc.

- ¿El evento fue provocado al engañar a un usuario para que entrara en un sitio web o realizara una descarga, o bien se envió a través de un archivo adjunto por correo electrónico?
- ¿Se está propagando el software malintencionado? ¿Hay otros hosts/extremos en peligro en la red?
- ¿Es una vulnerabilidad de día cero?

La información detallada de log de cada entrada de log muestra los logs relacionados para el evento. Esta información lo dirige a los logs de tráfico, amenaza, filtrado de URL u otros logs que puede revisar para correlacionar los eventos que dieron lugar al incidente. Por ejemplo, filtre el log de tráfico (**Monitor [Supervisar]** > **Logs [Logs]** > **Traffic [Tráfico]**) usando la dirección IP como IP tanto de origen como de destino para obtener una imagen completa de todos los hosts/clientes externos e internos con los que esta dirección IP de la víctima haya establecido una conexión.

Revisión de logs de WildFire

Además de los logs de amenaza, utilice la dirección IP de la víctima para filtrar los logs WildFire Submissions (Presentaciones de WildFire). Los logs de WildFire Submissions (Presentaciones de WildFire) contienen información sobre los archivos cargados en el servicio WildFire para su análisis. Como el spyware suele incrustarse encubiertamente, la revisión de los logs WildFire Submissions (Presentaciones de WildFire) le indicará si la víctima ha descargado recientemente un archivo sospechoso. El informe experto de WildFire muestra información de la URL de la que se obtuvo el archivo o .exe, así como el comportamiento del contenido. 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. Utilice esta información para determinar si desea bloquear la aplicación que provocó la infección (navegación web, SMTP, FTP), crear reglas de filtrado de URL más estrictas o restringir algunas aplicaciones o acciones, como descargas de archivos a grupos de usuarios específicos.

Para acceder a los logs de WildFire desde Panorama necesita lo siguiente: una suscripción a WildFire, un perfil de bloqueo de archivos unido a una regla de seguridad y el reenvío de logs de amenaza a Panorama.

*Si Panorama gestionará los cortafuegos que ejecutan versiones de software anteriores a PAN-OS 7.0, especifique un servidor WildFire desde el cual Panorama pueda recopilar información de análisis para las muestras de WildFire que aquellos cortafuegos envíen. Panorama usa la información para completar los logs WildFire Submissions (Presentaciones de WildFire) a los que les falta valores de campo en PAN-OS 7.0. Los cortafuegos que ejecutan versiones anteriores no completarán estos campos. Para especificar el servidor, seleccione **Panorama** > **Setup (Configuración)** > **WildFire**, edite la Configuración general e introduzca el nombre de **WildFire Private Cloud (Nube privada de WildFire)**. El valor predeterminado es **wildfire-public-cloud**, que es la nube de WildFire alojada en los Estados Unidos.*

Si WildFire determina que un archivo es malintencionado, se creará una nueva firma de antivirus en 24-48 horas y se pondrá a su disposición. Si tiene una suscripción a WildFire, la firma estará disponible en 30-60 minutos como parte de la próxima actualización de firma de WildFire. Tan pronto como el cortafuegos de próxima generación de Palo Alto Networks haya recibido una firma

 ©2023 Palo Alto Networks, Inc.

para ello, su configuración se ajustará para bloquear el software malintencionado, el archivo se bloqueará y la información del archivo bloqueado estará visible en sus logs de amenaza. Este proceso está fuertemente integrado para protegerle de esta amenaza y detiene la propagación del software malintencionado por su red.

Revisión de logs de filtrado de datos

El log de filtrado de datos (**Monitor [Supervisar]** > **Logs** > **Data Filtering [Filtrado de datos]**) es otro origen valioso para investigar la actividad de red malintencionada. Si bien puede revisar periódicamente los logs de todos los archivos sobre los que se le está alertando, también puede utilizar los logs para realizar un seguimiento de las transferencias de archivos y datos hacia o desde el usuario o la dirección IP de la víctima, así como verificar la dirección y el flujo del tráfico: de servidor a cliente o de cliente a servidor. Para recrear los eventos que precedieron y siguieron a un evento, filtre los logs de la dirección IP de la víctima como destino y revise los logs en busca de la actividad de red.

Como Panorama agrega información de todos los cortafuegos gestionados, presenta una buena descripción general de toda la actividad de su red. Otras herramientas visuales que puede utilizar para realizar un seguimiento del tráfico de su red son **Threat Map (Mapa de amenazas)**, **Traffic Map (Mapa de tráfico)** y **Threat Monitor (Supervisor de amenazas)**. El mapa de amenazas y el mapa de tráfico (**Monitor** > **AppScope** > **Threat Map [Mapa de amenazas]** o **Traffic Map [Mapa de tráfico]**) le permiten visualizar las regiones geográficas del tráfico de entrada y salida. Es de especial utilidad para visualizar actividad poco frecuente que podría indicar un posible ataque desde el exterior, como un ataque DDoS. Si, por ejemplo, no tiene muchas transacciones comerciales con Europa del Este y el mapa revela un nivel anómalo de tráfico con esa región, haga clic en el área correspondiente del mapa para iniciar y ver la información del ACC sobre las aplicaciones principales, información detallada de tráfico sobre el recuento de la sesión, los bytes enviados y recibidos, los orígenes y los destinos principales, los usuarios o las direcciones IP y la gravedad de las amenazas detectadas, si las hubiera. El supervisor de amenazas (**Monitor [Supervisar]** > **AppScope** > **Threat Monitor [Supervisor de amenazas]**) muestra las diez amenazas principales de su red, o bien la lista de los atacantes principales o las víctimas principales de la red.

Actualización de reglas de seguridad

Con toda la información que ha descubierto, ahora puede hacerse una idea de cómo afectan las amenazas a su red (la escala del ataque, el origen, los host en peligro y el factor de riesgo) y evaluar qué cambios, si los hubiera, debería realizar. Aquí tiene algunas sugerencias que considerar:

- Impedir ataques DDoS mejorando su perfil de protección DoS para configurar un descarte aleatorio temprano o cancelar cookies SYN para inundaciones TCP. Considere establecer límites en el tráfico de ICMP y UDP. Evalúe las opciones que tiene a su disposición basándose en las tendencias y los patrones que ha observado en sus logs e implemente los cambios mediante plantillas de Panorama.

  Cree una lista de bloqueos dinámicos (**Objects [Objetos]** > **Dynamic Block Lists [Listas de bloqueos dinámicos]**) para bloquear direcciones IP específicas que haya descubierto a partir de diversos orígenes de inteligencia: análisis de sus propios logs de amenazas, ataques DDoS de direcciones IP específicas o una lista de bloqueo de IP de terceros.

  La lista debe ser un archivo de texto y se debe encontrar en un servidor web. Mediante grupos de dispositivos Panorama, introduzca el objeto en los cortafuegos gestionados para que estos puedan acceder al servidor web e importar la lista en una frecuencia definida. Tras crear un objeto

 ©2023 Palo Alto Networks, Inc.

de lista de bloqueos dinámicos, defina una regla de seguridad que utilice el objeto de dirección en los campos de origen y destino para bloquear el tráfico desde o hacia la dirección IP, el rango o la subred definida. Este enfoque le permite bloquear a intrusos hasta que resuelva el problema y realizar cambios de política mayores para proteger su red.

- Determine si desea crear reglas de políticas compartidas o reglas de grupos de dispositivos para bloquear aplicaciones específicas que provocaron la infección (navegación web, SMTP, FTP), crear reglas de filtrado de URL más estrictas o restringir algunas aplicaciones o acciones, como descargas de archivos a grupos de usuarios específicos.
- En Panorama, también puede cambiar al contexto de cortafuegos y configurar el cortafuegos para informes de botnets que identifiquen posibles host infectados por botnets en la red.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Alta disponibilidad de Panorama

Para proporcionar redundancia en caso de fallo del sistema o de la red, puede implementar dos servidores de gestión de Panorama™ en una configuración de alta disponibilidad (HA). Panorama admite una configuración HA en la que un peer es el primario activo y el otro es el secundario pasivo. Si ocurre un fallo en el peer primario, automáticamente realiza una conmutación por error y el peer secundario se activa.

- Requisitos previos de HA de Panorama
- Prioridad y conmutación por error en Panorama en HA
- Activadores de conmutación por error
- Consideraciones sobre logs en HA de Panorama
- Sincronización entre peers de HA de Panorama
- Gestión de un par de HA de Panorama

Requisitos previos de HA de Panorama

Para configurar Panorama en HA, necesita un clúster de servidores de Panorama idénticos, con las siguientes características cada uno:

- **El mismo factor de forma**: los peers deben ser del mismo modelo: ambos dispositivos M-700, dispositivos M-600, ambos dispositivos M-500, ambos dispositivos M-300, ambos dispositivos M-200 o ambos implementados en el mismo hipervisor compatible para dispositivos virtuales Panorama. Por ejemplo, para configurar correctamente la HA para un dispositivo virtual Panorama implementado en AWS en modo Panorama, el peer de HA también debe implementarse en AWS y estar en modo Panorama.
- **El mismo modo**: los pares deben estar en el mismo modo Panorama: ambos se ejecutan en modo Panorama, modo Solo administración o modo heredado (solo ESXi y vCloud Air).

  Los dispositivos Panorama en modo recopilador de logs no admiten HA.
- **La misma versión del sistema operativo de Panorama**: deben ejecutar la misma versión de Panorama para sincronizar la información de configuración y mantener la paridad para una conmutación por error sin problemas.
- **El mismo conjunto de licencias**: deben tener la misma licencia de capacidad de gestión del cortafuegos.
- (Solo para dispositivos virtuales Panorama) **Modo FIPCS-CC**: el modo FIPS-CC debe estar habilitado o deshabilitado en ambos peers de HA de Panorama.
- (Solo para dispositivos virtuales Panorama) **Virtual Appliance Resources (Recursos del dispositivo virtual)**: debe tener el mismo número de núcleos de vCPU y memoria asignados para sincronizar correctamente la información de configuración.
- (Solo para dispositivo virtual Panorama) **Número de serie único**: deben contar con números de serie únicos; si el número de serie es el mismo para ambas instancias de Panorama, pasarán al modo de suspensión hasta que resuelva el problema.



Si bien se recomienda que el número de discos de registro y las capacidades de disco de creación de logs coincidan entre los peers de HA de Panorama, tener un número diferente de discos de registro o capacidades de disco de registro entre los peers de HA de Panorama no afecta a la sincronización de la configuración ni a la conmutación por error de HA de Panorama

.

 ©2023 Palo Alto Networks, Inc.

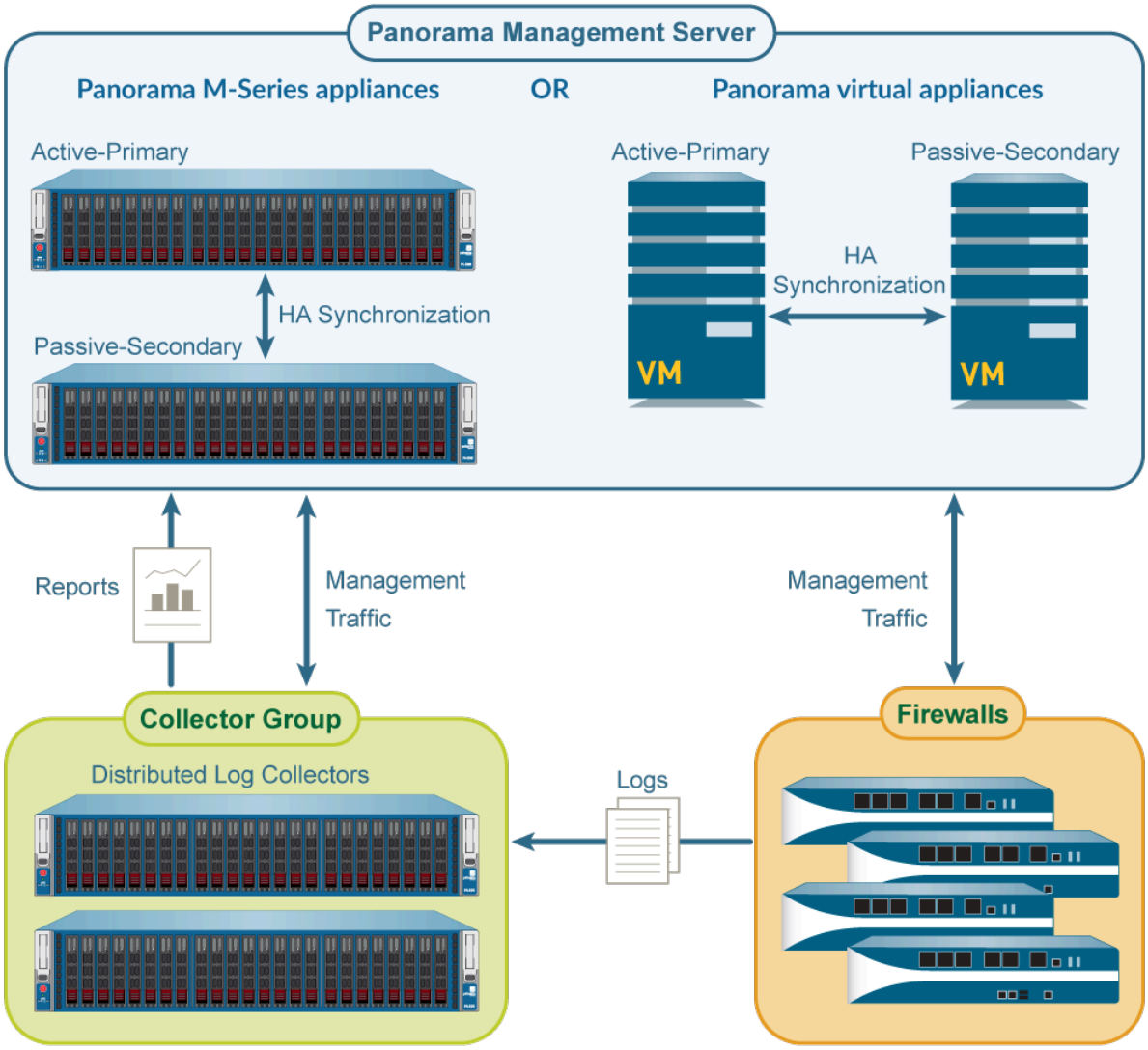


Figure 26: Organización de HA de Panorama

Los servidores de Panorama en la configuración de HA son peers y puede utilizar cualquiera de ellos (activo o pasivo) para gestionar de forma centralizada los cortafuegos, los recopiladores de logs y los dispositivos y clústeres de dispositivos WildFire, con algunas excepciones (consulte Sincronización entre peers de HA de Panorama). Los peers de HA utilizan la interfaz de gestión (MGT) para sincronizar los elementos de configuración transferidos a los cortafuegos gestionados, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire para mantener la información de estado. Normalmente, los pares de HA de Panorama se ubican geográficamente en diferentes sitios, por lo que debe asegurase de que la dirección IP de la interfaz de gestión (MGT) asignada a cada peer es enrutable a través de la red. La conectividad HA utiliza el puerto 28 TCP con cifrado activado.. Si el cifrado no está activado, los puertos 28769 y 28260 se utilizan para la conectividad HA y sincronizar la configuración entre los pares de HA. Se recomienda menos de 500 ms de latencia entre los peers. Para determinar la latencia, utilice ping durante un periodo de tráfico normal.

 ©2023 Palo Alto Networks, Inc.

Prioridad y conmutación por error en Panorama en HA

A cada peer de Panorama del par de HA se le asigna un valor de ***prioridad***. El valor de prioridad del peer principal o secundario determina cuál podrá ser seleccionado como el punto principal de administración y gestión de logs. El peer establecido como principal asume el estado activo y el secundario, el pasivo. El peer activo gestiona todos los cambios de configuración y los envía a los cortafuegos gestionados; el peer pasivo no puede realizar ningún cambio de configuración ni enviar ninguna configuración a los cortafuegos gestionados. Sin embargo, cualquier peer se puede utilizar para ejecutar informes o realizar consultas de log.

El peer pasivo se sincroniza y se prepara para la transición al estado activo, si se produjera un fallo en la ruta, enlace, sistema o red en el Panorama activo.

Cuando se produce una conmutación por error, solo cambia el estado (activo o pasivo) del peer de Panorama; la prioridad (principal o secundaria) no lo hace. Por ejemplo, cuando falla el peer principal, su estado cambia de activo-principal a pasivo-principal.

Un peer en estado activo-secundario puede realizar todas las funciones con dos excepciones:

- No puede gestionar funciones de implementación de cortafuegos o recopiladores de logs como actualizaciones de licencia o de software.
- No puede registrar en un NFS hasta que no cambie manualmente su prioridad a principal. Solo el dispositivo virtual Panorama en modo heredado admite NFS.

En la siguiente tabla se indican las capacidades de Panorama basadas en la configuración de su estado y prioridad:

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

Figure 27: Capacidades de HA de Panorama

©2023 Palo Alto Networks, Inc.

Para obtener más información, consulte Requisitos previos de HA de Panorama o Configuración de HA en Panorama.

 ©2023 Palo Alto Networks, Inc.

Activadores de conmutación por error

Cuando se produce un fallo en el Panorama activo y el Panorama pasivo toma el control de la tarea de gestionar los cortafuegos, el evento se denomina "conmutación por error". Una conmutación por error se activa cuando falla una métrica supervisada en el Panorama activo. Este fallo pasa el Panorama principal de activo-principal a pasivo-principal y el Panorama secundario se convierte en activo-secundario.

Las condiciones que activan una conmutación por error son las siguientes:

- Los peers de Panorama no se pueden comunicar entre sí y el peer activo no responde a los sondeos de estado; la métrica utilizada es Sondeos de heartbeat y mensajes de saludo de HA.

  Cuando los peers de Panorama no se pueden comunicar entre sí, el activo supervisa si los peers siguen conectados antes de que se active una conmutación por error. Esta comprobación ayuda a evitar una conmutación por error y a que no se produzca una situación de síndrome de cerebro dividido, donde los dos peers de Panorama pasan a estar activos.
- No se puede llegar a uno o varios destinos (direcciones IP) especificados en el peer activo; la métrica utilizada es Supervisión de rutas de HA.

Además de los activadores de conmutación por error enumerados anteriormente, también se produce una conmutación por error cuando el administrador coloca el peer de Panorama en un estado suspendido o cuando se produce una preemption. Esta función se refiere a la preferencia por la instancia principal de Panorama a la hora de reanudar la función activa después de recuperarse de un fallo (suspensión iniciada por el usuario). De forma predeterminada, la función de preferencia está habilitada; cuando la instancia de Panorama principal se recupera de un fallo y vuelve a estar disponible, la instancia de Panorama secundaria deja el control y vuelve al estado pasivo. Cuando se produce una preferencia, el evento se registra en el log del sistema.

Si está creando un log en un almacén de datos de NFS, no deshabilite la función de preferencia, ya que permite al peer principal (montado en el NFS) reanudar la función activa y escribir en el almacén de datos de NFS. Para otras implementaciones, la función de preferencia solo es necesaria si desea asegurarse de que un Panorama específico es el peer activo preferido.

Sondeos de heartbeat y mensajes de saludo de HA

Los peers de HA utilizan mensajes de saludo y heartbeats para comprobar que el peer responde y está operativo. Los mensajes de saludo se envían desde un peer al otro en el intervalo de saludo configurado para verificar el estado del dispositivo. El heartbeat es un ping ICMP para el peer de HA, y el peer responde al ping para establecer que los peers estén conectados y respondan. De manera predeterminada, el intervalo para el heartbeat es de 1.000 milisegundos y 8.000 milisegundos para los mensajes de saludo.

Supervisión de rutas de HA

La supervisión de rutas verifica la conectividad de red y el estado de enlace de una dirección IP o un grupo de direcciones IP (grupo de rutas). El peer activo utiliza pings ICMP para comprobar que se pueden alcanzar una o varias direcciones IP de destino. Por ejemplo, puede supervisar la disponibilidad de dispositivos de red interconectados como un enrutador o un conmutador, la conectividad a un servidor o cualquier otro dispositivo vital que se encuentre en el flujo del tráfico. Asegúrese de que no sea probable que el nodo/dispositivo configurado para la supervisión no

 ©2023 Palo Alto Networks, Inc.

responda, especialmente cuando tenga una carga inferior, ya que esto podría provocar un fallo de supervisión de rutas y activar una conmutación por error.

El intervalo de ping predeterminado es de 5.000 ms. Se considera que no se puede llegar a una dirección IP cuando fallan tres pings consecutivos (el valor predeterminado) y se activa un fallo de peer cuando no se puede llegar a alguna o todas las direcciones IP supervisadas. De forma predeterminada, si no se puede alcanzar alguna de las direcciones IP, el estado de HA pasa a ser no funcional.

 ©2023 Palo Alto Networks, Inc.

Consideraciones sobre logs en HA de Panorama

El establecimiento de una configuración de HA en Panorama proporciona redundancia para la recopilación de logs. Debido a que los cortafuegos gestionados están conectados a ambos peers de Panorama en la SSL, cuando se produce un cambio de estado, las instancias de Panorama envían un mensaje a los cortafuegos gestionados. Se informa a los cortafuegos sobre el estado de HA de Panorama y estos pueden enviar los logs correspondientes.

De forma predefinida, cuando los cortafuegos gestionados no pueden conectarse con Panorama, estos colocan en búfer los logs; cuando se restaura la conexión, reanudan el envío de logs donde se dejó.

Las opciones de logs en la instancia de Panorama basada en hardware y en el dispositivo virtual Panorama son diferentes:

- Conmutación por error del logging en un dispositivo virtual Panorama en modo heredado
- Conmutación por error del logging en un dispositivo M-Series o dispositivo virtual Panorama en modo Panorama

Conmutación por error del logging en un dispositivo virtual Panorama en modo heredado

El dispositivo virtual Panorama en modo heredado proporciona las siguientes opciones de conmutación por error de logs:

Tipo de almacenamiento de logs	Description (Descripción)
Disco virtual	De forma predeterminada, los cortafuegos gestionados envían logs como secuencias independientes a cada peer de HA de Panorama. De forma predeterminada, si un peer no está disponible, los cortafuegos gestionados guardan en el búfer los logs y cuando el peer se vuelve a conectar, continúan enviando logs a partir de donde lo dejaron la última vez (sujeto a la capacidad de almacenamiento del disco y a la duración de la desconexión). La capacidad máxima de almacenamiento de logs depende de la plataforma virtual (VMware ESXi o vCloud Air); consulte Modelos Panorama para obtener más información.

 ©2023 Palo Alto Networks, Inc.

Tipo de almacenamiento de logs	Description (Descripción)
	Puede elegir reenviar logs solo al peer activo (consulte Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs). Sin embargo, Panorama no admite la agregación de logs en el par de HA. De esta forma, si está almacenando logs en un disco virtual, para la supervisión y la creación de informes debe consultar al peer de Panorama que recopila los logs de los cortafuegos gestionados.
Sistema de archivos de red (NFS)	Puede montar el almacenamiento NFS solo en un dispositivo virtual Panorama que se ejecuta en un servidor VMware ESXi. Solamente la instancia activa-principal de Panorama se monta en la partición de logs basados en NFS y puede recibir logs. En la conmutación por error, el dispositivo principal pasa al estado pasivo-principal. En este caso, hasta que no se produzca la preferencia, la instancia activa-secundaria de Panorama gestiona los cortafuegos, pero no recibe logs ni puede escribir en el NFS. Para permitir que el peer activo-secundario cree un log en el NFS, debe cambiarlo a principal manualmente de forma que pueda montarse en la partición del NFS. Para obtener instrucciones, consulte Cambio de prioridad tras una conmutación por error de Panorama para reanudar los logs en NFS.

Conmutación por error del logging en un dispositivo M-Series o dispositivo virtual Panorama en modo Panorama

Si reenvía los logs del cortafuegos a los recopiladores de logs locales en un paer de HA de dispositivos M-700, M-600, M-500, M-300, M-200 o dispositivos virtuales Panorama en modo Panorama, debe especificar qué cortafuegos envían logs a qué recopiladores de logs cuando usted realice la Configuración de un grupo de recopiladores. Puede configurar un grupo de recopiladores por separado para el recopilador de logs de cada peer de Panorama o configurar un solo grupo de recopiladores para que contenga los recopiladores de logs de ambos peers. En un grupo de recopiladores que contiene ambos recopiladores de logs locales, la lista de preferencias de reenvío de logs determina qué Recopilador de logs recibe los logs de los cortafuegos. Para todos los cortafuegos gestionados, tiene la opción de enviar logs a todos los recopiladores de logs en el grupo de recopiladores, en cuyo caso Panorama utiliza el equilibrio de carga por turnos para seleccionar qué recopilador de logs recibe los logs en un momento determinado.

En un grupo de recopiladores que contiene ambos recopiladores de logs, también puede habilitar la redundancia para que cada log tenga dos copias y cada copia resida en un recopilador de logs diferente. Esta redundancia garantiza que si cualquiera de los recopiladores de logs deja de estar disponible, no se pierden los logs: puede ver todos los logs reenviados al grupo de recopiladores y ejecutar informes para todos la información de logs. La redundancia de logs está disponible solo si cada recopilador de logs del grupo de recopiladores tiene el mismo número de discos.

 ©2023 Palo Alto Networks, Inc.

Todos los recopiladores de logs de un grupo de recopiladores en particular deben ser del mismo modelo: todos los dispositivos M-200, todos los dispositivos M-300, todos los dispositivos M-500, todos los dispositivos M-600, todos los dispositivos M-700 o todos los dispositivos virtuales Panorama en modo Panorama.

Al habilitar la redundancia se crean más logs, por lo que esta configuración requiere más capacidad de almacenamiento. Al habilitar la redundancia se dobla el tráfico de procesamiento de logs en un grupo de recopiladores, que reduce su tasa de logs máxima a la mitad, ya que cada recopilador de logs debe distribuir una copia de cada log que reciba. (Si un grupo de recopiladores se queda sin espacio, elimina logs antiguos).

©2023 Palo Alto Networks, Inc.

Sincronización entre peers de HA de Panorama

Los peers de HA de Panorama sincronizan la configuración en ejecución cada vez que compila cambios en el peer activo de Panorama. La configuración candidata se sincroniza entre los peers cada vez que guarda la configuración en el peer activo o justo antes de que se produzca una conmutación por error.

Los ajustes comunes al par se sincronizan entre los peers de HA de Panorama, por ejemplo, objetos y reglas de políticas compartidos, objetos y reglas de grupos de dispositivos, configuración de plantillas, certificados y perfiles de servicio de capa de sockets seguros (secure sockets layer, SSL) o seguridad de capa de transporte (transport layer security, TLS), y configuración del acceso administrativo.

Cuando Habilitación de la recuperación de confirmación automatizada, la sincronización de HA se produce solo después de que el cortafuegos pruebe con éxito la conexión entre él mismo y Panorama después de un envío desde Panorama.

La configuración que no se sincroniza es aquella específica de cada peer, como la siguiente:

- Configuración de HA de Panorama: ajuste de prioridad, dirección IP del peer, grupos de supervisión de ruta y direcciones IP
- Configuración de Panorama: dirección IP del interfaz de gestión, configuración FQDN, titular de inicio de sesión, servidor de NTP, zona horaria, ubicación geográfica, servidor DNS, direcciones IP permitidas para acceder a Panorama, configuración del sistema SNMP y cronogramas dinámicos de actualización de contenido
- Exportaciones de configuración programadas
- Configuración de partición NFS y toda la asignación de cuota de disco para los logs Esto solo se aplica a un dispositivo virtual Panorama en el modo Legacy que se ejecuta en un servidor VMware ESXi
- Asignación de cuota de disco para los diferentes tipos de logs y bases de datos en el almacenamiento local de Panorama (SSD)

  Si utiliza una clave maestra para cifrar las claves privadas y los certificados de Panorama, deberá utilizar la misma clave maestra en ambos peers de HA. Si las claves maestras son diferentes, Panorama no podrá sincronizar los peers de HA.

- Contraseña para el administrador `admin` de Panorama

Para obtener más información, consulte Requisitos previos de HA de Panorama o Configuración de HA en Panorama.

 ©2023 Palo Alto Networks, Inc.

Gestión de un par de HA de Panorama

- Configuración de HA en Panorama
- Configurar la autenticación mediante certificados personalizados entre peers de HA
- Prueba de conmutación por error de HA de Panorama
- Cambio de prioridad tras una conmutación por error de Panorama para reanudar los logs en NFS
- Restauración del Panorama principal al estado activo

Para instalar actualizaciones de software o contenido, consulte Instalación de actualizaciones de Panorama en una configuración de HA**.**

Configuración de HA en Panorama

Revise Requisitos previos de HA de Panorama antes de realizar los siguientes pasos.

Si configura "Secure Communication Setting" (Ajustes de comunicación segura) entre peers de HA de Panorama**, *estos usarán el certificado personalizado especificado para la autenticación entre sí. De lo contrario, los peers de HA de Panorama utilizan el certificado predefinido para la autenticación.***

Independientemente de cómo configure los peers de HA de Panorama para autenticar la comunicación, ninguno de los dos afectará la capacidad de los peers de HA de Panorama para comunicarse entre sí.

STEP 1 | Configure la conectividad entre los puertos MGT en los peers de HA.

Los peers de Panorama se comunican entre sí usando el puerto MGT. Asegúrese de que las direcciones IP que asigna al puerto MGT en los servidores Panorama del par de HA son enrutables y que los peers se pueden comunicar entre sí a través de la red. Para configurar el puerto MGT, consulte Realización de la configuración inicial del dispositivo virtual Panorama o Realización de la configuración inicial del dispositivo de la serie M.

Seleccione un peer de Panorama del par y complete las tareas restantes.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Habilite la HA y (opcionalmente) el cifrado para la conexión de HA.

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección **Setup (Configuración)**.
2. Seleccione **Enable HA (Habilitar HA)**.
3. En el campo **Peer HA IP Address (Dirección IP del peer de HA)**, introduzca la dirección IP asignada al peer de Panorama.
4. En el campo **Peer HA Serial (HA de peer en serie)**, especifique el número de serie del peer de Panorama.

   Introduzca el número de serie del peer de HA de Panorama para reducir su superficie de ataque contra ataques de fuerza bruta en la IP de Panorama.
5. En el campo **Monitor Hold Time (Supervisar tiempo de espera)**, introduzca la cantidad de tiempo (milisegundos) que el sistema esperará antes de reaccionar ante un fallo de un enlace de control (el intervalo es 1.000-60.000; el valor predeterminado es 3.000).
6. Si no desea cifrado, cancele la selección de la casilla de verificación **Encryption Enabled (Cifrado habilitado)** y haga clic en **OK (Aceptar)**: no se necesitan más pasos. Si desea cifrado, seleccione la casilla de verificación **Encryption Enabled (Cifrado habilitado)**, haga clic en **OK (Aceptar)** y realice las siguientes tareas:

   1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.
   2. Seleccione **Export HA key (Exportar clave de HA)**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el peer de Panorama.
   3. En el peer de Panorama, vaya a **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**, seleccione **Import HA key (Importar clave de HA)**, vaya a la ubicación donde guardó la clave e impórtela.

STEP 3 | Establezca la prioridad de HA.

1. En **Panorama** > **High Availability (Alta disponibilidad)**, edite la sección **Election Settings (Configuración de elección)**.
2. Defina la prioridad del dispositivo en **Device Priority (Prioridad del dispositivo)** como **Primary (Principal)** o **Secondary (Secundaria)**. Asegúrese de establecer un peer como principal y el otro como secundario.

   Si ambos peers tienen el mismo ajuste de prioridad, el peer con el número de serie más alto quedará suspendido.
3. Defina el comportamiento como **Preemptive (Preferente)**. De forma predeterminada, la función de preferencia está habilitada. La selección de preferencia (habilitada o deshabilitada) debe ser igual en ambos peers.

   Si utiliza un NFS para los logs y ha desactivado la preferencia, para reanudar la creación de logs en el NFS, consulte Cambio de prioridad tras una conmutación por error de Panorama para reanudar los logs en NFS.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Para configurar la supervisión de ruta, defina uno o varios grupos de ruta.

El grupo de rutas indica las direcciones IP de destino (nodos) en los que Panorama debe hacer ping para comprobar la conectividad de la red.

Realice los siguientes pasos para cada grupo de rutas que incluya los nodos que quiera supervisar.

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y en la sección Grupo de rutas, haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** para el grupo de rutas.
3. Seleccione una condición de fallo en **Failure Condition (Condición de fallo)** para este grupo:
   - **any (cualquiera)** activa un fallo de supervisor de ruta en caso de que no se pueda acceder a alguna de las direcciones IP.
   - **all (todos)** activa un fallo de supervisor de ruta solamente cuando no se puede acceder a ninguna de las direcciones IP.
4. Seleccione **Add (Añadir)** para añadir cada dirección IP de destino que desee supervisar.
5. Haga clic en **OK (Aceptar)**. La sección Grupo de rutas muestra el nuevo grupo.

STEP 5 | (Opcional) Seleccione la condición de fallo para la supervisión de rutas en Panorama.

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección Supervisión de rutas.
2. Seleccione una **Failure Condition (Condición de fallo)**:
   - **all (todos)** activa una conmutación por error solamente cuando fallan todos los grupos de rutas supervisados.
   - **any (cualquiera)** activa una conmutación por error cuando falla cualquiera de los grupos de rutas supervisados.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Confirme sus cambios de configuración.

Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

STEP 7 | Configure el otro peer de Panorama.

Repita del paso 2 al paso 6 en el otro peer del par de HA.

STEP 8 | Sincronice los peers de Panorama.

1. Acceda al **Dashboard (Panel)** en el Panorama activo y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
2. **Sync to peer (Sincronizar en el peer)**, haga clic en **Yes (Sí)** y espere a que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.
3. Acceda al **Dashboard (Panel)** en el Panorama pasivo y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
4. Verifique que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | (Opcional) Configurar la autenticación mediante certificados personalizados entre peers de HA.

Debe configurar las opciones de comunicación segura para ambos peers de HA de Panorama. La configuración de "Secure Communication Setting" (Ajustes de comunicación segura) para Panorama en la configuración de HA no afecta a la conectividad de HA entre los peers de HA. Sin embargo, la funcionalidad del vínculo de comunicación segura puede fallar si la configuración de comunicación segura se estableció de manera incorrecta, o si los cortafuegos gestionados o el peer de HA no tienen el certificado correcto o tienen un certificado caducado.

Todo el tráfico en el enlace establecido con la configuración de los ajustes de comunicación segura siempre está cifrado.

*Si configura las opciones de comunicación segura para Panorama en una configuración de HA, también es necesario **personalizar la comunicación del servidor segura**. De lo contrario, los cortafuegos gestionados y los dispositivos WildFire no pueden conectarse a Panorama y la funcionalidad PAN-OS se ve afectada.*

Configurar la autenticación mediante certificados personalizados entre peers de HA

Usted puede realizar la Configuración de la autenticación utilizando certificados personalizados para asegurar la conexión de HA entre los peers de HA de Panorama.

STEP 1 | Genere un certificado de la Autoridad de certificado (certificate authority, CA) en Panorama.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.
2. Cree un certificado de CA raíz autofirmado o importe un certificado de su empresa CA.

STEP 2 | Configure un perfil de certificados que incluya la CA de raíz y la CA intermedia.

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

STEP 3 | Configure un perfil de servicio SSL/TLS.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
2. Configuración de un perfil SSL/TLS para definir el certificado y protocolo que Panorama y sus dispositivos gestionados usan para servicios SSL/TLS.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configure "Secure Server Communication" (Comunicación de servidor segura) en Panorama en el peer de HA principal.

*Si configura las opciones de comunicación segura en Panorama para Panorama en una configuración de HA, también es necesario **personalizar la comunicación del servidor segura**. De lo contrario, los cortafuegos gestionados, los recopiladores de logs dedicados y los dispositivos WildFire no pueden conectarse a Panorama y la funcionalidad PAN-OS se ve afectada.*

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en **Edit (Editar)** para editar los ajustes de "Secure Communication" (Comunicación segura).
2. En "Certificate Type" (Tipo de certificado), seleccione **Local**.
3. Seleccione el **Certificate (Certificado)** y el **Certificate Profile (Perfil del certificado)** que configuró en los pasos anteriores.
4. Marque (habilite) **HA Communication (Comunicación de HA)**, **WildFire Communication (Comunicación de WildFire)** y **Data Redistribution (Redistribución de datos)**.
5. Marque (habilite) **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
6. Seleccione el perfil del servicio SSL/TLS del menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre Panorama, los cortafuegos, recopiladores de logs y los peers de HA de Panorama.
7. Seleccione el perfil de certificado del menú desplegable **Certificate Profile (Perfil del certificado)**.
8. Configure una lista de autorizaciones.

   Cuando configura "Secure Communication Setting" (Ajustes de comunicación segura) para Panorama en una configuración de HA, debe agregar el peer de HA de Panorama a la lista de autorización.

   1. Haga clic en **Add (Añadir)** en lista de autorizaciones.
   2. Seleccione el **Subject (Sujeto)** o **Subject Alt Name (Nombre alternativo del sujeto)** como el tipo de Identificador.
   3. Introduzca el Nombre común.
9. (Opcional) Compruebe que la casilla de verificación **Allow Custom Certificate Only (Permitir solo certificado personalizado)** no esté seleccionada. Esto le permite continuar gestionando todos los dispositivos mientras migra a certificados personalizados.

   *Cuando se selecciona la casilla de verificación **Allow Custom Certificate Only (Permitir solo certificado personalizado)**, Panorama no se autentica y no puede gestionar dispositivos con certificados predefinidos.*
10. En **Disconnect Wait Time (min) [Tiempo de espera de desconexión (min)]**, introduzca el número de minutos que Panorama debería esperar antes de terminar y volver a establecer

 ©2023 Palo Alto Networks, Inc.

la conexión actual con sus dispositivos gestionados. Este campo está en blanco por defecto y el rango es de 0 a 44,640 minutos.

El tiempo de espera de desconexión no comienza la cuenta atrás hasta que confirme la nueva configuración.

1. Haga clic en **OK (Aceptar)**.
2. Seleccione **Confirmar** y en **Confirmar en Panorama**.
3. Repita este paso en el peer de HA secundario de Panorama.

   Cuando configura "Secure Communication Setting" (Ajustes de comunicación segura) en el peer de HA secundario de Panorama, agregue el peer de HA principal a la lista de autorización como se describe anteriormente.

STEP 5 | Actualice Panorama del lado del cliente a PAN-OS 10.1.

Actualice Panorama.

Prueba de conmutación por error de HA de Panorama

Para comprobar que su configuración de HA funciona correctamente, active una conmutación por error manual y verifique que el peer cambia de estado correctamente.

STEP 1 | Inicie sesión en el peer activo de Panorama.

Puede verificar el estado del servidor de Panorama en la esquina inferior derecha de la interfaz web.

STEP 2 | Suspenda el peer activo de Panorama.

Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y, a continuación, haga clic en el enlace **Suspend local Panorama (Suspender Panorama local)**, en la sección Comandos de operación.

STEP 3 | Compruebe que el peer de Panorama pasivo ha pasado a activo.

En el **Dashboard (Panel)** de Panorama, en el widget **High Availability (Alta disponibilidad)**, verifique que el estado del servidor pasivo **Local** aparece como **active (activo)** y el estado del **Peer** aparece como **suspended (suspendido)**.

STEP 4 | Restaure el peer suspendido a un estado funcional. Espere un par de minutos y, a continuación, verifique que se ha producido preemption, si se ha habilitado.

En la instancia de Panorama previamente suspendida:

1. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y, en la sección Operational Commands (Comandos de operación), haga clic en **Make local Panorama functional (Hacer que la instancia local de Panorama sea funcional)**.
2. En el widget **High Availability (Alta disponibilidad)** en el **Dashboard (Panel)**, confirme que esta instancia (local) de Panorama ha pasado como el peer activo y que el otro peer está ahora en estado pasivo.

 ©2023 Palo Alto Networks, Inc.

Cambio de prioridad tras una conmutación por error de Panorama para reanudar los logs en NFS

El dispositivo virtual de Panorama en el modo Legacy que se ejecuta en un servidor ESXi puede usar un almacén de datos NFS para la creación de logs. En una configuración de Alta disponibilidad (high availability, HA), solo el peer principal de Panorama está montado a la partición de logs basada en NFS y puede escribir en el NFS. Cuando se produce una conmutación por error y el Panorama pasivo se vuelve activo, su estado se convierte en activo-secundario. Aunque un peer secundario de Panorama puede gestionar activamente los cortafuegos, no puede recibir logs ni escribir en el NFS porque no posee la partición NFS. Cuando los cortafuegos no pueden reenviar logs al peer principal de Panorama, cada cortafuegos escribe los logs en su disco local. Los cortafuegos mantienen un puntero para el último conjunto de entradas de logs reenviados a Panorama, de forma que cuando el Panorama pasivo-principal está disponible otra vez, puede seguir reenviándole logs.

Utilice las instrucciones de esta sección para cambiar manualmente la prioridad en el peer activo-secundario de Panorama para que pueda empezar a crear logs en la partición NFS. Los casos típicos en los que debería tener que activar este cambio son los siguientes:

- Cuando la función de preferencia está deshabilitada. De forma predeterminada, la preferencia está habilitada en Panorama y el peer principal se reanuda como activo cuando vuelve a estar disponible. Cuando la preferencia está desactivada, debe cambiar la prioridad en el peer secundario a principal de forma que pueda montar la partición NFS, recibir logs de los cortafuegos gestionados y escribir en la partición NFS.
- La instancia activa de Panorama falla y no puede recuperarse del falo a corto plazo. Si no cambia la prioridad y cuando se alcance la capacidad máxima de almacenamiento de logs del cortafuegos, los logs más antiguos se sobrescriben para seguir permitiendo la creación de logs en el disco local. Esta situación puede hacer que se pierdan logs.

STEP 1 | Inicie sesión en el Panorama pasivo-principal actual, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, en la sección Operaciones de dispositivo, haga clic en **Shutdown Panorama (Apagar Panorama)**.

STEP 2 | Inicie sesión en el Panorama activo-secundario, seleccione **Panorama** > **High Availability (Alta disponibilidad)**, edite la Configuración de elección y establezca **Priority (Prioridad)** en **Primary (Principal)**.

STEP 3 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

No reinicie cuando se le pida.

STEP 5 | Inicie sesión en la CLI de Panorama e introduzca el siguiente comando para cambiar la propiedad de la partición NFS a este peer: **`request high-availability convert-to-primary`**

STEP 6 | Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, en la sección Operaciones de dispositivo, haga clic en **Reboot Panorama (Reiniciar Panorama)**.

STEP 7 | Conecte el peer de Panorama que desconectó en el paso 1. Este peer pasará ahora al estado pasivo-secundario.

 ©2023 Palo Alto Networks, Inc.

Restauración del Panorama principal al estado activo

De forma predeterminada, la función de preferencia de Panorama permite a la instancia principal de Panorama continuar funcionando como el peer activo tan pronto como está disponible. Sin embargo, si la función de preferencia está deshabilitada, la única manera de que la instancia principal de Panorama pase a estar activa tras recuperarse de un fallo, un estado no funcional o suspendido es suspendiendo el peer secundario de Panorama.

Antes de que la instancia activa-secundaria de Panorama pase a un estado suspendido, transfiere la configuración candidata a la instancia de Panorama pasiva de forma que todos los cambios de configuración no compilados se guarden y se pueda acceder a ellos a través del otro peer.

STEP 1 | Suspenda Panorama.

1. Inicie la sesión en el peer de Panorama que desea que pase al estado de suspensión.
2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y haga clic en el enlace **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos de operación.

STEP 2 | Compruebe que el estado indica que Panorama se haya suspendido bajo la solicitud del usuario.

En el **Dashboard (Panel)**, en el widget **High Availability (Alta disponibilidad)**, verifique que el estado **Local** aparece como **suspended (suspendido)**.

Cuando se suspende un peer, se activa una conmutación por error y la otra instancia de Panorama cambia a peer activo.

STEP 3 | Restaure el Panorama suspendido a un estado funcional.

1. En la pestaña **Panorama** > **High Availability (Alta disponibilidad)**, en la sección Operational Commands (Comandos de operación), haga clic en el enlace **Make local Panorama functional (Hacer que la instancia local de Panorama sea funcional)**.
2. En **Dashboard (Panel)**, en el widget **High Availability (Alta disponibilidad)**, confirme que Panorama pasó al estado activo o pasivo.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Administración de Panorama

En esta sección se describe cómo gestionar y mantener el servidor de gestión Panorama™. Incluye los siguientes temas:

- Previsualización, validación o compilación de cambios de configuración
- Compilación de cambios de configuración selectivos para dispositivos gestionados
- Envío de cambios de configuración selectivos a dispositivos gestionados
- Habilitación de la recuperación de confirmación automatizada
- Gestión de las copias de seguridad de configuración de Panorama y del cortafuegos
- Comparación de cambios en configuraciones de Panorama
- Gestión de bloqueos para restringir cambios de configuración
- Adición de logotipos personalizados a Panorama
- Uso del gestor de tareas de Panorama
- Gestión de cuotas de almacenamiento y períodos de vencimiento de logs e informes
- Supervisión de Panorama
- Reinicio o cierre de Panorama
- Configuración de perfiles de contraseña y complejidad de contraseña de Panorama

Para obtener instrucciones sobre cómo completar la configuración inicial, incluida la definición de los ajustes de acceso a la red, la creación de licencias, la actualización de la versión del software Panorama y la configuración del acceso administrativo a Panorama, consulte Configuración de Panorama.

Previsualización, validación o compilación de cambios de configuración

Realice las acciones descritas en Operaciones de confirmación, validación y previsualización de Panorama con los cambios pendientes en la configuración de Panorama y, luego, envíe esos cambios a los dispositivos que gestiona Panorama, como cortafuegos, recopiladores de logs y dispositivos o clústeres de dispositivos de WildFire. Puede filtrar los cambios pendientes por administrador o ***ubicación*** y, a continuación, compilar, enviar, validar o previsualizar solo esos cambios. Las ubicaciones pueden ser grupos de dispositivos, plantillas, grupos de recopiladores, recopiladores de logs, configuraciones compartidas específicos o el servidor de gestión Panorama.

Debido a que Panorama envía su configuración en ejecución, no puede enviar cambios en los dispositivos hasta que primero los confirme a Panorama. Si los cambios no están listos para activarse en los dispositivos, puede seleccionar **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** para confirmar los cambios a la configuración de Panorama sin enviarlos a los dispositivos. Luego, cuando los cambios estén listos para activarse en los dispositivos, puede seleccionar **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**. Si los cambios están listos para activarse tanto en Panorama como en los dispositivos, seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** como se describe en el siguiente procedimiento.

STEP 1 | Configure el alcance de los cambios de configuración que confirmará, validará o previsualizará.

1. Haga clic en **Commit (Compilar)** en la parte superior de la interfaz web.
2. Seleccione una de las siguientes opciones:
   - **Commit All Changes (Confirmar todos los cambios)** (predeterminada): se aplica a todos los cambios para los cuales usted posee privilegios administrativos. Usted no puede filtrar manualmente el alcance de la confirmación cuando selecciona esta opción. En lugar de eso, la función de administrador asignada a la cuenta que utilizó para iniciar sesión determina el alcance de la confirmación.
   - **Commit Changes Made By (Confirmar los cambios realizados por)**: le permite filtrar el alcance de la confirmación según el administrador o ubicación. La función administrativa asignada a la cuenta que usted utilizó para iniciar sesión determina qué cambios puede filtrar.

   *Para confirmar los cambios de otros administradores, la cuenta que utilizó para iniciar sesión debe estar asignada a la función de superusuario o un perfil de rol de administrador con el privilegio **Commit For Other Admins (Confirmar para otros administradores)** habilitado.*
3. (Opcional) Para filtrar el alcance de la confirmación mediante el administrador, seleccione **Commit Changes Made By (Confirmar cambios realizados por)**, haga clic en el enlace adyacente, seleccione los administradores y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

4. (Opcional) Para filtrar por ubicación, seleccione **Commit Changes Made By (Confirmar cambios realizados por)** y borre los cambios que desee excluir del alcance de la confirmación.

   Si las dependencias entre los cambios de configuración que incluyó y excluyó producen un error de validación, realice la confirmación con todos los cambios incluidos. Por ejemplo, al confirmar cambios en un grupo de dispositivos, debe incluir los cambios de todos los administradores que añadieron, eliminaron o cambiaron reglas para la misma base de reglas en ese grupo de dispositivos.

STEP 2 | Previsualice los cambios que la confirmación activará.

Si obtiene la vista previa de los cambios después de eliminar un dispositivo de una regla de una política y de volver a añadirlo, Panorama muestra, al mismo tiempo, que ese dispositivo se ha eliminado de la configuración en ejecución y que se ha añadido a la configuración candidata. Por eso, es posible que los dispositivos figuren en la lista de destinos de la configuración en ejecución con un orden distinto del de la configuración candidata, y que aparezca una modificación al obtener la vista previa, aun cuando no se haya realizado ningún cambio real en la configuración.

Esto puede ser útil si, por ejemplo, usted no recuerda todos los cambios y no está seguro de que desee activar todos.

Panorama permite comparar las configuraciones seleccionadas en Commit Scope (Ámbito de compilación) con la configuración en ejecución. La ventana de previsualización muestra las configuraciones en paralelo y utiliza codificación por color para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo).

Seleccione **Preview Changes (Previsualizar los cambios)** y seleccione las **Lines of Context (Líneas de contexto)**, que es la cantidad de líneas de los archivos de configuración comparados que se mostrarán antes y después de las diferencias resaltadas. Estas líneas pueden ayudarlo a correlacionar el resultado de previsualización con las configuraciones en la interfaz web. Cierre la ventana de previsualización cuando termine de revisar los cambios.

Debido a que los resultados de previsualización se muestran en una ventana nueva, su navegador debe permitir ventanas emergentes. Si la ventana de previsualización no se abre, consulte la documentación de su navegador para ver los pasos para desbloquear las ventanas emergentes.

STEP 3 | Previsualice los ajustes individuales en los que está confirmando cambios.

Esto puede ser útil si desea conocer detalles sobre los cambios, tales como los tipos de configuraciones y quiénes las cambiaron.

1. Haga clic en **Change Summary (Cambiar el resumen)**.
2. (Opcional) **Group By (Agrupar por)** un nombre de columna (tal como el **Type [Tipo]** de configuración).
3. Seleccione **Close (Cerrar)** el cuadro de diálogo Change Summary (Cambiar resumen) para terminar de revisar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Valide los cambios antes de confirmarlos para asegurarse de que la confirmación se realizará correctamente.

1. Seleccione **Validate Changes (Validar los cambios)**.

   Los resultados mostrarán todos los errores y advertencias que mostraría una confirmación real.
2. Resuelva todos los errores que los resultados de la validación identifiquen

STEP 5 | (Opcional) Modifique Push Scope.

De forma predeterminada, Push Scope incluye todas las ubicaciones con cambios que requieren confirmación de Panorama.

*Si selecciona **Commit (Confirmar) > Push to Devices (Enviar a dispositivos)**, el alcance de envío incluye todas las ubicaciones asociadas con dispositivos que no están sincronizados con la configuración de ejecución de Panorama.*

1. **No Default Selections (Sin selecciones predeterminadas)** para seleccionar manualmente dispositivos específicos. Los dispositivos predeterminados a los que envía Panorama se basan en los cambios de configuración de plantillas y grupos de dispositivos afectados.
2. **Edit Selections (Editar selecciones)** y seleccione:
   - **Device Groups (Grupos de dispositivos)**: seleccione grupos de dispositivos o cortafuegos individuales o sistemas virtuales.
   - **Templates (Plantillas)**: seleccione plantillas, pilas de plantillas o cortafuegos individuales.
   - **Collector Groups (Grupos de recopiladores)**: seleccione grupos de recopiladores.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.

STEP 6 | Valide los cambios que enviará a grupos de dispositivos o plantillas.

1. **Validate Device Group Push (Validar envío de grupo de dispositivos)** o **Validate Template Push (Validar envío de plantilla)**.

   Los resultados mostrarán todos los errores y advertencias que mostraría una operación de envío real.
2. Resuelva todos los errores que los resultados de la validación identifiquen

STEP 7 | Confirme sus cambios realizados a Panorama y envíe los cambios a dispositivos.

Commit and Push (Confirmar y enviar) los cambios de configuración.

Uso del gestor de tareas de Panorama *para ver detalles sobre las confirmaciones pendientes (de manera opcional, las puede cancelar), en curso, completas o con errores.*

 ©2023 Palo Alto Networks, Inc.

Compilación de cambios de configuración selectivos para dispositivos gestionados

En el servidor de gestión Panorama™, los cambios de configuración se producen con frecuencia y normalmente son realizados por varios administradores que no son conscientes de qué otros cambios de configuración se realizaron en Panorama. Es vital poder controlar qué objetos de configuración están compilados en Panorama y evitar que las configuraciones incompletas se envíen desde Panorama a sus cortafuegos gestionados. En lugar de compilar todos los cambios de configuración pendientes en Panorama, puede seleccionar un grupo de dispositivos específico y objetos de pila de plantillas para compilar. Se genera un log del sistema después de una compilación selectiva exitosa.

La capacidad de seleccionar objetos específicos para compilar permite a varios administradores realizar cambios de configuración de manera efectiva sin interrumpir a otros administradores que realizan cambios de configuración que no están listos para compilarse. Aprovechar la capacidad de compilar selectivamente los cambios de configuración en Panorama le permite mantener el procedimiento operativo definido y, al mismo tiempo, poder realizar correctamente cambios de configuración independientes que no están definidos dentro de su ámbito operativo.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Realice cambios en la configuración del grupo de dispositivos y la pila de plantillas en Panorama.

STEP 3 | Seleccione **Confirmar** y en **Confirmar en Panorama**.

STEP 4 | Cambie el alcance de la compilación a **Commit Changes Made By (Compilar cambios realizados por)** para seleccionar cambios específicos en la configuración del grupo de dispositivos y la pila de plantillas para compilar en Panorama.

El alcance del envío muestra el nombre del administrador que ha iniciado sesión actualmente. Haga clic en el nombre del administrador para ver una lista de los administradores que han realizado cambios de configuración que no se han compilado en Panorama.

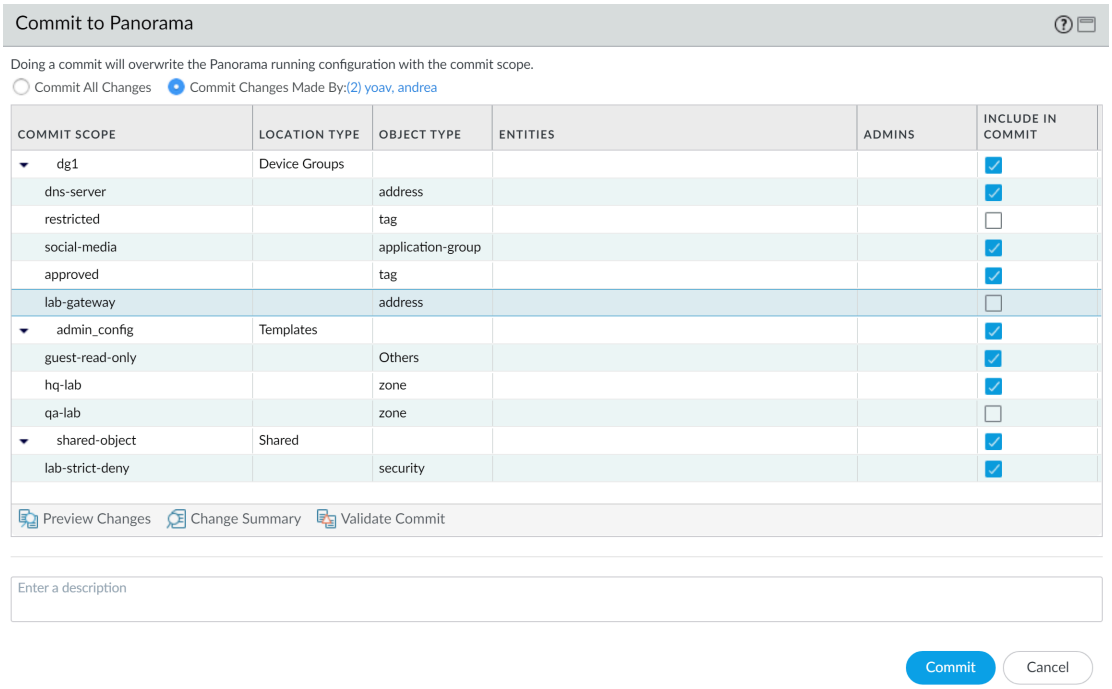
STEP 5 | En la columna Include in Commit (Incluir en compilación), marque (habilite) los objetos de configuración que desea incluir en la compilación.

STEP 6 | (Opcional) Obtenga una vista previa y valide los cambios de configuración pendientes para asegurarse de que desea compilar los cambios de configuración selectivos en Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Seleccione **Confirmar**.

La página Commit Status (Estado de compilación) muestra los administradores que realizaron los cambios de configuración que se compilaron y la ubicación de los cambios de configuración compilados.



STEP 8 | Envío de cambios de configuración selectivos a dispositivos gestionados.

Después de compilar los objetos de configuración seleccionados en Panorama, puede enviar esos objetos de configuración a los cortafuegos gestionados.

 ©2023 Palo Alto Networks, Inc.

Envío de cambios de configuración selectivos a dispositivos gestionados

Puede incluir los cambios de configuración confirmados por uno o más administradores de Panorama para enviarlos a los cortafuegos gestionados. Esto permite un mayor grado de control al realizar cambios de configuración y reduce el riesgo de enviar una configuración incompleta a los cortafuegos gestionados. Para permitir que un administrador de Panorama envíe selectivamente los cambios de configuración, debe configurar un perfil de función de administración que permita el envío selectivo y asignar el perfil de función de administración al administrador de Panorama. Se genera un log del sistema para un envío selectivo exitoso a los cortafuegos gestionados.

También puede aprovechar la compilación selectiva de los cambios de configuración para una mayor selectividad al enviar los cambios de configuración a los cortafuegos gestionados. La compilación selectiva le permite seleccionar y compilar objetos de configuración específicos. Después de compilar, puede aprovechar el envío selectivo para revisar y enviar todos los cambios de configuración compilados realizados por otros administradores de Panorama.

La capacidad de especificar qué cambios de configuración del administrador de Panorama se deben incluir en un envío a cortafuegos gestionados permite a varios administradores gestionar de manera efectiva las configuraciones de cortafuegos sin interrumpir a otros administradores y reduce el riesgo de enviar una configuración incompleta a los cortafuegos gestionados que podría provocar una interrupción. Aprovechar la capacidad de enviar selectivamente cambios de configuración le permite mantener su procedimiento operativo definido y, al mismo tiempo, poder realizar con éxito cambios de configuración independientes que no están definidos dentro de su alcance operativo.

El envío selectivo solo se admite para cortafuegos gestionados y se admite para cortafuegos gestionados que ejecutan cualquier versión de PAN-OS compatible. El envío selectivo no es compatible con los recopiladores de logs, los grupos de recopiladores, los dispositivos WildFire y los clústeres WildFire. Para Panorama en una configuración de alta disponibilidad (HA) activa/pasiva, solo se admite el envío selectivo desde el peer de HA activo.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

El administrador de Panorama debe configurarse con un perfil de función de administración que permita el envío de los cambios de configuración realizados por otros administradores a los cortafuegos gestionados. Los privilegios predeterminados de los roles de administración Superusuario o Panorama admiten privilegios de configuración de nivel de objeto completo.

STEP 2 | Seleccione **Confirmar** y **Enviar a dispositivos**.

*También puede seleccionar **Commit and Push (Compilar y enviar)** para compilar cambios de configuración selectivos en Panorama y enviar cambios ya compilados en una operación.*

No puede enviar selectivamente un cambio de configuración que no se haya compilado.

STEP 3 | Cambie el alcance de envío a **Push Changes Made By (Enviar cambios realizados por)** y filtre el alcance de envío por administrador de Panorama para seleccionar cambios específicos en

 ©2023 Palo Alto Networks, Inc.

la configuración del grupo de dispositivos y la pila de plantillas para enviar a los cortafuegos gestionados.

El alcance del envío muestra el nombre del administrador que ha iniciado sesión actualmente. Haga clic en el nombre del administrador para ver una lista de administradores con cambios de configuración compilados que no se han enviado a cortafuegos gestionados. El alcance del envío se actualiza automáticamente para mostrar una lista actualizada de grupos de dispositivos y pilas de plantillas en función de los administradores seleccionados.

STEP 4 | En la columna Include in Push (Incluir en el envío), marque (habilite) los objetos de configuración que desea incluir en la compilación.

El alcance del envío muestra solo los grupos de dispositivos y las pilas de plantillas que no están `sincronizadas`.



Debe seleccionar y enviar todo el grupo de dispositivos o la configuración de la pila de plantillas que se compiló. Los cambios de nivel de objeto que se muestran en el alcance del envío son informativos y no se pueden excluir del envío para el grupo de dispositivos o la pila de plantillas que seleccione.

STEP 5 | (Opcional) **Edite selecciones** y seleccione los cortafuegos gestionados asociados con los grupos de dispositivos y las pilas de plantillas afectados.

Omita este paso para enviar a todos los cortafuegos gestionados asociados con los grupos de dispositivos afectados y las pilas de plantillas.

STEP 6 | **Inserte** los cambios de configuración.

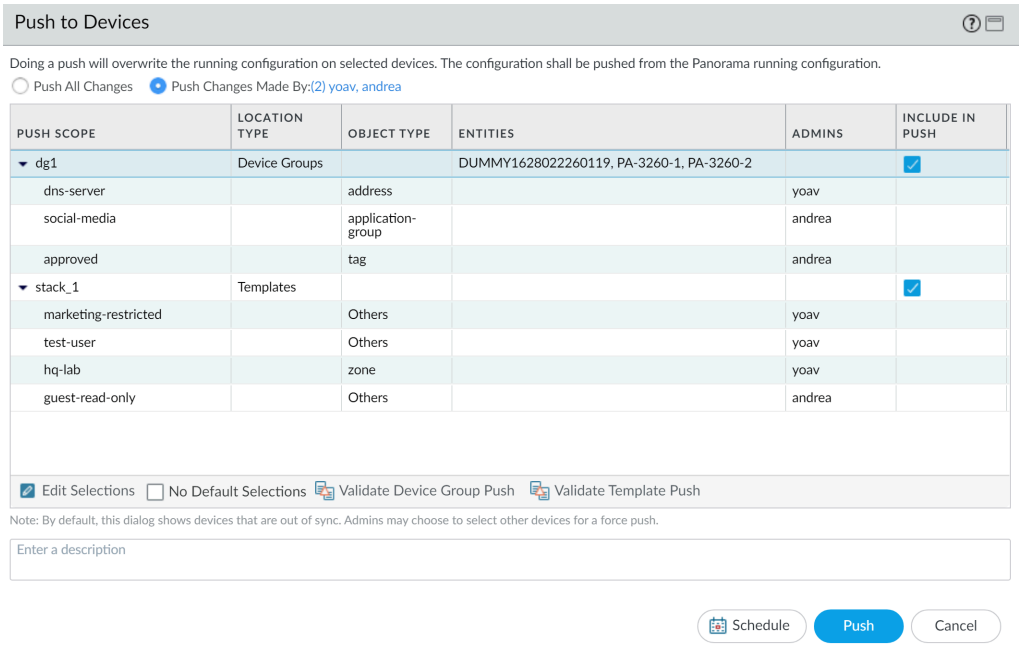
STEP 7 | Si su función de administración le permite enviar cambios de configuración para otros administradores de Panorama, revise el mensaje Confirm Push to Devices (Confirmar envío a dispositivos) y haga clic en **Push (Enviar)**.

Esta advertencia se muestra cuando los administradores incluidos en el alcance de la administración realizan cambios de configuración contradictorios en el mismo objeto. Por ejemplo, Admin1 puede enviar cambios de configuración cortafuegos gestionados, mientras que Admin2 no lo tiene permitido. Admin1 crea `SecurityRule`, agrega `ZoneA` como zona de origen y compila el cambio. A continuación, Admin2 modifica `SecurityRule`, elimina `ZoneA`, añade `ZoneB` y realiza cambios de configuración adicionales. Admin2 confirma los cambios en Panorama. Admin1 quiere incluir los cambios de configuración realizados por Admin1 en el envío

 ©2023 Palo Alto Networks, Inc.

a cortafuegos gestionados. En este escenario, se solicita a Admin1 que confirme el envío porque los cambios de configuración realizados en `SecurityRule` entran en conflicto.

Si no confía en los cambios de configuración realizados por otros administradores de Panorama, haga clic en ***Continue push with my selected changes only (Continuar el envío con mis cambios seleccionados solamente)*** *para enviar solo sus propios cambios de configuración y sobrescribir cualquier conflicto de objeto de configuración con los cambios realizados.*



STEP 8 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** y haga clic en la plantilla Last Commit State (Estado de la última compilación) para los cortafuegos afectados para revisar los detalles del estado de la última compilación.

 ©2023 Palo Alto Networks, Inc.

Habilitación de la recuperación de confirmación automatizada

Para garantizar que las configuraciones interrumpidas las originaron los cambios de configuración enviados desde el servidor de gestión Panorama™ a los cortafuegos gestionados, o confirmados localmente en el cortafuegos, habilite **Automated Commit Recovery (Recuperación de confirmación automatizada)** para permitir que los cortafuegos gestionados prueben los cambios de configuración para cada confirmación y para verificar que los cambios no interrumpieron la conexión entre Panorama y el cortafuegos gestionado. Puede configurar la cantidad de pruebas que realiza cada cortafuegos gestionado y el intervalo en el que se realiza cada prueba antes de que dicho cortafuegos revierta automáticamente su configuración a la configuración anterior en ejecución. Cuando habilite la recuperación de confirmación automatizada, se revierte la configuración del cortafuegos gestionado y no la configuración de Panorama. Además, el cortafuegos gestionado prueba su conexión a Panorama cada 60 minutos para garantizar una comunicación continua en caso de que la configuración de red no relacionada cambie la conectividad interrumpida entre el cortafuegos y Panorama o si los impactos de una configuración confirmada en el pasado afectaron la conectividad. Para configuraciones de alta disponibilidad (High Availability, HA), la sincronización de HA entre los peers de HA después de un envío desde Panorama se produce solo después de una prueba de conectividad.

La recuperación de confirmación automática está habilitada de forma predeterminada. Sin embargo, si deshabilitó la recuperación de confirmación automática y después desea volver a habilitar esa función en un entorno de producción existente, debe verificar primero que no haya reglas de políticas que interrumpan la conexión entre Panorama y el cortafuegos gestionado. Por ejemplo, en el caso de que el tráfico de gestión atraviese el plano de datos, es posible que exista una regla de políticas que restrinja el tráfico desde el cortafuegos a Panorama.

El cortafuegos genera un log de configuración después de que la configuración del cortafuegos vuelva con éxito a la última configuración en ejecución. Además, el cortafuegos genera un log del sistema cuando el administrador deshabilita esa función, cuando se inicia un evento de reversión de configuración debido a una prueba de conectividad errónea después de un envío de configuración, y cuando falla la prueba de conectividad de Panorama que se realiza cada 60 minutos y provoca que la configuración del cortafuegos se revierta.



*Habilite **Automated Commit Recovery (Recuperación de confirmación automatizada)** independientemente de cualquier otro cambio de configuración. Si se habilita junto con cualquier otro cambio de configuración que provoque una interrupción de la conexión entre Panorama y los cortafuegos gestionados, la configuración del cortafuegos no puede revertirse automáticamente.*

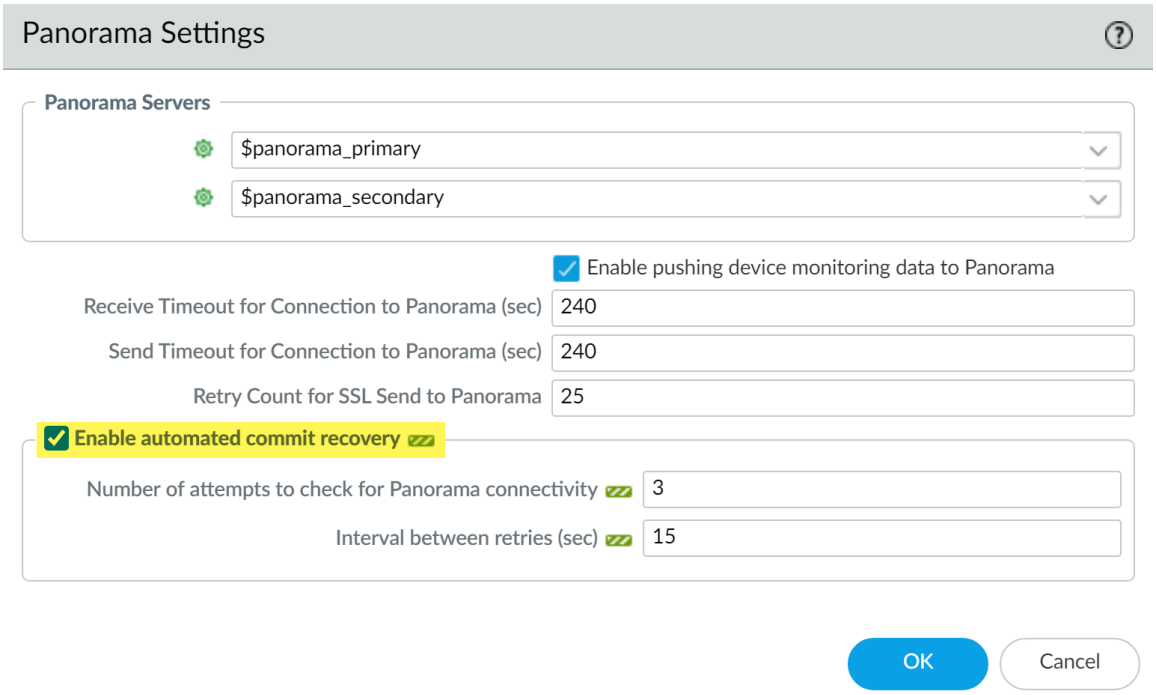
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y seleccione la plantilla o pila de plantillas deseadas en el menú contextual desplegable **Template (Plantilla)**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Habilite la recuperación de confirmación automatizada.

1. **Edite** (⚙) la configuración de Panorama.
2. **Habilite la recuperación de confirmación automatizada**.
3. Configure el **número de intentos de comprobación de la conectividad de Panorama** (el valor predeterminado es 1 intento).
4. Configure el **intervalo entre reintentos** (el valor predeterminado es de 10 segundos).
5. Haga clic en **OK (Aceptar)** para guardar los cambios.



STEP 4 | Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Commit and Push (Confirmar y enviar)** para confirmar los cambios.

STEP 5 | Compruebe que la función de recuperación de confirmación automática esté habilitada en sus cortafuegos gestionados.

1. Inicie la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y, en Panorama Settings (Configuración de Panorama), compruebe que la opción **Enable automated commit recovery (Habilitar recuperación de confirmación automatizada)** esté habilitada (activada).

 ©2023 Palo Alto Networks, Inc.

Gestión de las copias de seguridad de configuración de Panorama y del cortafuegos

La configuración en ejecución en Panorama incluye todos los ajustes que compiló y que por lo tanto están activos. La configuración candidata es una copia de la configuración en ejecución junto con los cambios inactivos que realizó desde la última compilación. Si realiza una copia de seguridad de las versiones de la configuración candidata o en ejecución, permite que luego se puedan restaurar esas versiones. Por ejemplo, si una validación de confirmación muestra que la configuración candidata actual tiene más errores que los que desea reparar, puede restaurarla a una configuración candidata anterior. También puede volver a la configuración en ejecución actual sin guardar una copia de seguridad antes.

Consulte** Operaciones de confirmación, validación y previsualización de Panorama **para obtener más información sobre la compilación de cambios de configuración en Panorama y sobre el envío de cambios a los dispositivos gestionados.

Después de una confirmación en un cortafuegos local que ejecuta PAN-OS 5.0 o una versión posterior, una copia de seguridad de su configuración en ejecución se envía a Panorama. Cualquier confirmación realizada en el cortafuegos local activará la copia de seguridad, incluidos las confirmaciones que un administrador realiza localmente en el cortafuegos o confirmaciones automáticas iniciadas por PAN-OS (como una actualización FQDN). De forma predeterminada, Panorama almacena hasta 100 copias de seguridad de cada cortafuegos, aunque esta cantidad puede configurarse. Para almacenar copias de seguridad de configuración de Panorama y los cortafuegos en un host externo, puede programar exportaciones de Panorama o exportar según lo requiera. También puede importar configuraciones de los cortafuegos a los grupos de dispositivos y plantillas de Panorama para Transición de un cortafuegos a una gestión de Panorama.

(Solo en VMware ESXi y vCloud Air) La funcionalidad de instantánea de VMware no es compatible con un dispositivo virtual de Panorama implementado en VMware ESXi y vCloud Air. La realización de instantáneas de un dispositivo virtual de Panorama puede afectar al rendimiento, provocar una pérdida de paquetes intermitente e incoherente, y Panorama puede dejar de responder. Además, es posible que pierda el acceso a la interfaz web y la CLI de Panorama y no se admite el cambio al modo Panorama En su lugar, guarde y exporte su instantánea de configuración nombrada en cualquier ubicación de red.

Si está aprovechando la** prevención de pérdida de datos (DLP) de Enterprise**, cargar una copia de seguridad de configuración de Panorama que no contenga los objetos de configuración de DLP compartidos de Enterprise elimina estos objetos compartidos necesarios para la funcionalidad de DLP de Enterprise.

- Programación de la exportación de los archivos de configuración
- Guardado y exportación de configuraciones de Panorama y de cortafuegos
- Reversión de los cambios de configuración de Panorama
- Configuración del número máximo de copias de seguridad de configuración en Panorama
- Carga de una copia de seguridad de configuración en un cortafuegos gestionado

 ©2023 Palo Alto Networks, Inc.

Programación de la exportación de los archivos de configuración

Panorama guarda una copia de seguridad de su configuración en ejecución así como también de las configuraciones en ejecución de todos los cortafuegos gestionados. Las copias de seguridad tienen formato XML y los nombres de archivo se basan en los números de serie (de Panorama y los cortafuegos). Utilice estas instrucciones para programar exportaciones diarias de las copias de seguridad a un host remoto. Panorama exporta las copias de seguridad como un único archivo gzip. Necesita privilegios de superusuario para programar la exportación.

Si Panorama tiene una configuración de alta disponibilidad (HA), debe aplicar estas instrucciones en cada peer para asegurarse de que las exportaciones programadas continúen tras una conmutación por error. Panorama no sincroniza exportaciones de configuración programadas entre peers HA.

Para exportar copias de seguridad bajo demanda, consulte Guardado y exportación de configuraciones de Panorama y de cortafuegos.

STEP 1 | Seleccione **Panorama** > **Scheduled Config Export (Exportación de configuración programada)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un nombre en **Name (Nombre)** y una descripción en **Description (Descripción)** para la exportación de archivo programada y haga clic en **Enable (Habilitar)**.

STEP 3 | Mediante el formato de reloj de 24 horas, introduzca un **Scheduled Export Start Time (Hora de inicio de exportación programada)** diario o seleccione uno en el menú desplegable.

Si va a configurar una exportación programada a dos o más servidores, escalone la hora de inicio de las exportaciones programadas. La programación de varias exportaciones con la misma hora de inicio genera discrepancias entre las configuraciones exportadas.

STEP 4 | Configure el **Protocol (Protocolo)** de exportación en Secure Copy (**SCP**) o Protocolo de transferencia de archivos (**FTP**).

*Exportar a dispositivos que ejecutan Windows solo admite **FTP**.*

STEP 5 | Introduzca los detalles para acceder al servidor, entre los que se incluyen los siguientes: **Hostname (Nombre de host)** o dirección IP, **Port (Puerto)**, **Path (Ruta)** para cargar el archivo, **Username (Nombre de usuario)** y **Password (Contraseña)**.

La **ruta** admite los siguientes caracteres: **.** (punto), **+**, **{** y **}**, **/**, **-**, **_**, **0**-**9**, **a**-**z**, y **A**-**Z**. Los espacios no son compatibles con la **ruta** del archivo.

*Si va a exportar a un servidor FTP con una dirección IPv6 como **nombre de host**, debe especificar la dirección entre corchetes ([ ]). Por ejemplo, **`[2001:0db8:0000:0000:0000:8a2e:0370:7334]`**.*

*Si está exportando a un servidor BSD, deberá modificar la solicitud de contraseña SSHD a **`<username>@<hostname> <password>:`** .*

STEP 6 | (Solo en SCP) Haga clic en **Test SCP server connection (Probar conexión de servidor SCP)**. Para activar la transferencia segura de los datos, debe verificar y aceptar la clave de host del servidor SCP. Panorama no establece la conexión hasta que acepta la clave de host. Si

 ©2023 Palo Alto Networks, Inc.

Panorama tiene una configuración de HA, realice este paso en cada peer de HA para que cada uno acepte la clave de host del servidor SCP. Si Panorama puede conectarse correctamente al servidor SCP, se crea y carga el archivo de prueba denominado ssh-export-test.txt.

STEP 7 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 8 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

Guardado y exportación de configuraciones de Panorama y de cortafuegos

Guarde una copia de seguridad de la configuración candidata en el almacenamiento permanente de Panorama por si tiene que restaurarla más adelante (consulte Reversión de los cambios de configuración de Panorama). Panorama también permite guardar y exportar las configuraciones de grupos de dispositivos, plantillas y pilas de plantillas que especifique. Esto resulta útil para preservar los cambios que, de lo contrario, se perderían si un evento del sistema o una acción del administrador hacen que Panorama se reinicie. Después del reinicio, Panorama revierte la versión de forma automática a la configuración en ejecución, que almacena en el archivo `running-config.xml`. El guardar copias de seguridad también resulta útil si desea revertir los ajustes a una configuración de Panorama que es anterior a la configuración actual en ejecución. Panorama no guarda automáticamente la configuración candidata en el almacenamiento permanente. Debe guardar la configuración candidata manualmente como el archivo de instantánea predeterminado (`.snapshot.xml`) o como un archivo de instantánea con un nombre personalizado. Panorama almacena el archivo de instantánea a nivel local, pero usted puede exportarlo a un host externo.

*No hace falta que guarde una copia de seguridad de la configuración para revertir los cambios realizados desde la última confirmación o el último reinicio; basta con que seleccione **Config (Configuración) > Revert Changes (Revertir cambios)**. Consulte* Reversión de los cambios de configuración de Panorama*.*

Palo Alto Networks le recomienda crear copias de seguridad de cualquier configuración importante en un host externo.

STEP 1 | Guarde los cambios realizados en la configuración candidata.

- Para sobrescribir el archivo de instantánea predeterminado (`.snapshot.xml`) con todos los cambios realizados por todos los administradores, realice uno de los pasos siguientes:
  - Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Save candidate Panorama configuration** (Guarde la configuración candidata de Panorama).
  - Inicie sesión en Panorama con una cuenta administrativa asignada a la función de superusuario o un perfil de función de administración con el privilegio **Save For Other Admins (Guardar para otros administradores)** habilitado. Luego seleccione **Config** > **Save Changes (Guardar cambios)** en la parte superior de la interfaz web, seleccione **Save All Changes (Guardar todos los cambios)** y **Save (Guardar)**.
- Para sobrescribir la instantánea predeterminada (`.snapshot.xml`) con los cambios que han realizado los administradores en configuraciones concretas de grupos de dispositivos, plantillas o pilas de plantillas:

 ©2023 Palo Alto Networks, Inc.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Save candidate Panorama configuration (Guardar configuración candidata de Panorama)** y en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)**.
2. Seleccione los grupos de dispositivos, las plantillas o las pilas de plantillas que desea revertir.
3. Haga clic en **OK (Aceptar)** para confirmar la operación.
4. (Opcional) Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con la instantánea.

- Para crear una instantánea que incluya todos los cambios realizados por todos los administradores, pero sin sobrescribir el archivo de instantánea predeterminado:

  1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**.
  2. En **Name (Nombre)**, especifique el nombre de un archivo de configuración nuevo o existente.
  3. Haga clic en **OK (Aceptar)** y **Close (Cerrar)**.

- Para guardar solo cambios específicos en la configuración candidata sin sobrescribir ninguna parte del archivo de instantánea predeterminado:

  1. Inicie sesión en Panorama con una cuenta administrativa que tenga los privilegios de la función necesarios para guardar los cambios deseados.
  2. Seleccione **Config** > **Save Changes (Guardar cambios)** en la parte superior de la interfaz web.
  3. Seleccione **Save Changes Made By (Guardar cambios realizados por)**.
  4. Para filtrar el alcance del guardado por administrador, haga clic en ***<administrator-name>***, seleccione los administradores y haga clic en **OK (Aceptar)**.
  5. Para filtrar el alcance del guardado por ubicación, borre las ubicaciones que desee excluir. Las ubicaciones pueden ser grupos de dispositivos, plantillas, grupos de recopiladores, recopiladores de logs, configuraciones compartidas específicos o el servidor de gestión Panorama.
  6. Haga clic en **Save (Guardar)**, especifique el **Name (Nombre)** de un archivo de configuración nuevo o existente, y haga clic en **OK (Aceptar)**.

- Para guardar una configuración concreta de grupos de dispositivos, plantillas o pilas de plantillas:

  1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)** y en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)**.
  2. Seleccione los grupos de dispositivos, las plantillas o las pilas de plantillas que desea guardar.
  3. Haga clic en **OK (Aceptar)** para confirmar la operación.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Exporte una configuración candidata o en ejecución a un host externo a Panorama o a un cortafuegos.

Puede exportar configuraciones bajo demanda o bien programar exportaciones diarias a servidores del protocolo de copia segura (SCP) o del protocolo de transferencia de archivos (FTP), tal como se explica en Programación de la exportación de los archivos de configuración. Para exportar bajo demanda, seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y seleccione una de las siguientes opciones:

- **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**: exporte la configuración en ejecución actual, una instantánea de la configuración candidata con nombre o una configuración previamente importada (candidata o en ejecución). Panorama exporta la configuración como un archivo XML con el nombre que especifique en **Name (Nombre)**. Haga clic en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)** para especificar las configuraciones de grupos de dispositivos, plantillas o pilas de plantillas que desea exportar.
- **Export Panorama configuration version (Exportar versión de configuración de Panorama)**: seleccione una **Version (Versión)** de la configuración en ejecución para exportarla como un archivo XML. Haga clic en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)** para especificar las configuraciones de grupos de dispositivos, plantillas o pilas de plantillas que desea exportar como archivo XML.
- **Export Panorama and devices config bundle (Exportar lote de configuración de dispositivos y Panorama)**: genere y exporte la versión más reciente de la copia de seguridad de configuración en ejecución de Panorama y de cada cortafuegos gestionado. Para automatizar el proceso consistente en crear y exportar a diario el lote de configuraciones a servidores SCP o FTP, consulte Programación de la exportación de los archivos de configuración.
- **Export or push device config bundle (Exportar o enviar lote de configuración del dispositivo)**: después de importar la configuración de un cortafuegos en Panorama, Panorama crea un lote de configuración de cortafuegos con el nombre <firewall_name>_import.tgz, en el que se eliminan todas las políticas y los objetos locales. A continuación, puede **exportar o enviar el paquete de configuración del dispositivo** para realizar una de las siguientes acciones:
  - **Envíe y compile** el paquete de configuración al cortafuegos para eliminar cualquier configuración local del mismo, lo que le permite gestionar el cortafuegos desde Panorama.
  - **Export (Exportar)**: exporte la configuración al cortafuegos sin cargarlo. Cuando esté listo para cargar la configuración, acceda a la CLI del cortafuegos y ejecute el comando del modo de configuración **`load device-state`**. Este comando limpia el cortafuegos del mismo modo que la opción **Push & Commit (Enviar y compilar)**.

Para realizar todo el procedimiento Transición de un cortafuegos a una gestión de Panorama*, tiene que seguir algunos pasos más.*

Reversión de los cambios de configuración de Panorama

Si revierte los cambios, sustituye los ajustes de la configuración candidata actual por los ajustes de otra configuración. La reversión de cambios es útil cuando desea deshacer los cambios de varios ajustes como una misma operación, en lugar de reconfigurar manualmente cada ajuste.

 ©2023 Palo Alto Networks, Inc.

Puede revertir los cambios pendientes que se realizaron a la configuración de Panorama desde la última vez que se guardaron los cambios. Puede revertir todos los cambios pendientes de aplicación en Panorama o en grupos de dispositivos, plantillas o pilas de plantillas concretos. Panorama ofrece la opción de filtrar los cambios pendientes por administrador o por ubicación. Las ubicaciones pueden ser grupos de dispositivos, plantillas, grupos de recopiladores, recopiladores de logs, configuraciones compartidas específicos o el servidor de gestión Panorama. Si ha guardado el archivo de instantánea de una configuración candidata anterior a la configuración actual en ejecución (consulte Guardado y exportación de configuraciones de Panorama y de cortafuegos), también puede revertir los ajustes a esa instantánea. Al revertir a una instantánea usted puede restaurar una configuración candidata que existía antes de la última vez que se guardaron los cambios. Panorama guarda automáticamente una versión nueva de la configuración en ejecución cada vez que confirma los cambios; puede restaurar cualquiera de esas versiones.

La reversión de una configuración de servidor de gestión Panorama requiere una confirmación completa y debe realizarla un superusuario. Se requerirán confirmaciones completas cuando se realicen determinadas operaciones de Panorama, como revertir y cargar una configuración de Panorama, y no serán compatibles con los perfiles de función de administración personalizados.

- Revierta a la configuración de Panorama actual en ejecución (archivo `running-config.xml`).

  Esta operación deshace todos los cambios que realizó a la configuración desde la última confirmación.

  - Para revertir todos los cambios que realizaron los administradores, realice alguno de los siguientes pasos:
    - Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**, **Revert to running Panorama configuration (Revertir a la configuración de Panorama en ejecución)** y haga clic en **Yes (Sí)** para confirmar la operación.
    - Inicie sesión en Panorama con una cuenta administrativa asignada a la función de superusuario o un perfil de rol de administrador con el privilegio **Commit For Other Admins (Confirmar para otros administradores)** habilitado. A continuación, seleccione

 ©2023 Palo Alto Networks, Inc.

Config (Configuración) > **Revert Changes (Revertir cambios)**, marque **Revert All Changes (Revertir todos los cambios)** y haga clic en **Revert (Revertir)**.

- Para revertir solo cambios específicos a la configuración candidata:
  1. Inicie sesión en Panorama con una cuenta administrativa que tenga los privilegios de rol necesarios para revertir los cambios deseados.

     Los privilegios que controlan las operaciones de confirmación también controlan las operaciones de reversión.
  2. Seleccione **Config (Configuración)** > **Revert Changes (Revertir cambios)**.
  3. Seleccione **Revert Changes Made By (Revertir cambios realizados por)**.
  4. Para filtrar el alcance de la reversión por administrador, haga clic en *<nombre-administrador>*, selecciónelo y haga clic en **OK (Aceptar)**.
  5. Para filtrar el alcance de la reversión por ubicación, borre las ubicaciones que desee excluir.
  6. Seleccione **Revert (Revertir)** para revertir los cambios.
- Para revertir los cambios realizados en grupos de dispositivos, plantillas o pilas de plantillas concretos a la configuración en ejecución:
  1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Revert to running Panorama configuration (Revertir a configuración de Panorama en ejecución)** y en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)**.
  2. Seleccione los grupos de dispositivos, las plantillas o las pilas de plantillas que desea revertir.
  3. Haga clic en **OK (Aceptar)** para confirmar la operación.
  4. (Opcional) Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con los cambios realizados.

- Revierta a la instantánea predeterminada (`.snapshot.xml`) de la configuración candidata de Panorama.
  - Para revertir todos los cambios realizados por todos los administradores:
    1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Revert to last saved Panorama configuration (Revertir a la última configuración guardada de Panorama)**.
    2. Haga clic en **Yes (Sí)** para confirmar la operación.
    3. (Opcional) Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con la instantánea.
  - Para revertir los cambios realizados en grupos de dispositivos, plantillas o pilas de plantillas concretos a la configuración en ejecución:
    1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Revert to last saved Panorama configuration (Revertir a la última configuración guardada de Panorama)** y en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)**.

 ©2023 Palo Alto Networks, Inc.

2. Seleccione los grupos de dispositivos, las plantillas o las pilas de plantillas que desea revertir.
3. Haga clic en **OK (Aceptar)** para confirmar la operación.
4. (Opcional) Para sobrescribir la configuración en ejecución con la instantánea, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)**.

- Revierta a una versión previa de la configuración en ejecución almacenada en Panorama.
  - Para revertir todos los cambios realizados por los administradores:
    1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Load Panorama configuration version (Cargar versión de configuración de Panorama)** y en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)**.
    2. Seleccione una versión de la configuración en **Version** y haga clic en **OK**.
    3. (Opcional) Para sobrescribir la configuración en ejecución con la versión que acaba de revertir, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para confirmar sus cambios.
  - Para revertir los cambios realizados en grupos de dispositivos, plantillas o pilas de plantillas concretos a la configuración en ejecución:
    1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y, luego, haga clic en **Load Panorama configuration version (Cargar versión de configuración de Panorama)** y seleccione la versión de configuración en **Name (Nombre)**.
    2. Haga clic en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)** y seleccione los grupos de dispositivos, las plantillas o las pilas de plantillas que desea revertir.
    3. Haga clic en **OK (Aceptar)** para confirmar la operación.
    4. (Opcional) Para sobrescribir la configuración en ejecución con la instantánea, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar sus cambios.

- Puede revertir a una de las siguientes opciones:
  - Versión con nombre personalizado de la configuración en ejecución de Panorama que ha importado con anterioridad.
  - Instantánea de la configuración candidata de Panorama con nombre personalizado en lugar de la instantánea predeterminada.
    1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)** y seleccione en **Name (Nombre)** el archivo de configuración que acaba de importar.
    2. (Opcional) Según lo que desee cargar, haga clic en **Load Shared Objects (Cargar objetos compartidos)** o en **Load Shared Policies (Cargar políticas compartidas)**. Puede cargar

 ©2023 Palo Alto Networks, Inc.

todas las políticas y todos los objetos compartidos o bien los configurados en los grupos de dispositivos y las plantillas que especifique en el paso siguiente.

3. (Opcional) Haga clic en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)** y seleccione las configuraciones concretas de grupos de dispositivos, plantillas o pilas de plantillas que desea cargar. Omita este paso si desea revertir toda la configuración de Panorama.
4. Haga clic en **OK (Aceptar)** para confirmar la operación.
5. (Opcional) Para sobrescribir la configuración en ejecución con la instantánea, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar sus cambios.

- Restaure una configuración candidata o en ejecución de Panorama que exportó previamente en un host externo.
  1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, seleccione **Browse (Explorar)** para buscar el archivo de configuración en el host externo y haga clic en **OK (Aceptar)**.
  2. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración de Panorama con nombre)** y seleccione en **Name (Nombre)** el archivo de configuración que acaba de importar.
  3. (Opcional) Según lo que desee cargar, haga clic en **Load Shared Objects (Cargar objetos compartidos)** o en **Load Shared Policies (Cargar políticas compartidas)**. Puede cargar todas las políticas y todos los objetos compartidos o bien los configurados en los grupos de dispositivos y las plantillas que especifique en el paso siguiente.
  4. (Opcional) Haga clic en **Select Device Group & Templates (Seleccionar grupos de dispositivos y plantillas)** y seleccione las configuraciones concretas de grupos de dispositivos, plantillas o pilas de plantillas que desea cargar. Omita este paso si desea revertir toda la configuración de Panorama.
  5. Haga clic en **OK (Aceptar)** para confirmar la operación.
  6. (Opcional) Para sobrescribir la configuración en ejecución con la instantánea que acaba de importar, seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y haga clic en **Commit (Confirmar)** para confirmar sus cambios.

Configuración del número máximo de copias de seguridad de configuración en Panorama

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de logs e informes.

STEP 2 | Seleccione **Log Export and Reporting (Exportación e informes de logs)** e introduzca el **Number of Versions for Config Backups (Número de versiones para copias de seguridad de configuración)** [por defecto es 100, el rango es de 1 a 1.048.576].

STEP 3 | Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

Carga de una copia de seguridad de configuración en un cortafuegos gestionado

Utilice Panorama para cargar una copia de seguridad de configuración en un cortafuegos gestionado. Puede elegir volver a una configuración anteriormente guardada o compilada en el cortafuegos. Panorama transfiere la versión seleccionada al cortafuegos gestionado con lo cual se sobrescribe la configuración candidata actual en el cortafuegos.

STEP 1 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.

STEP 2 | Seleccione **Manage (Gestionar)** en la columna Copias de seguridad.

STEP 3 | Seleccione en Configuraciones guardadas o Configuraciones compiladas.

- Haga clic en el número de versión para ver el contenido de esa versión.
- Haga clic en **Load (Cargar)** para cargar una versión de configuración.

STEP 4 | Inicie sesión en la interfaz web del cortafuegos y haga clic en **Commit (Compilar)** para confirmar los cambios.

 ©2023 Palo Alto Networks, Inc.

Comparación de cambios en configuraciones de Panorama

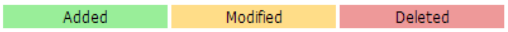
Para comparar los cambios en la configuración en Panorama, puede seleccionar cualquier par de conjuntos de archivos de configuración: la configuración candidata, la configuración en ejecución o cualquier otra versión de la configuración que se haya guardado o compilado anteriormente en Panorama. La comparación de los archivos le permite:

- Obtener una vista previa de los cambios en la configuración antes de compilarlos en Panorama. Puede, por ejemplo, obtener una vista previa de los cambios entre la configuración candidata y la configuración en ejecución. Se recomienda seleccionar la versión más antigua en el panel izquierdo y la más reciente en el derecho, para comparar e identificar las modificaciones fácilmente.
- Realice una *auditoría de configuraciones* para revisar y comparar los cambios entre dos conjuntos de archivos de configuración.

Los administradores de plantillas y grupos de dispositivos solo pueden comparar configuraciones para grupos de dispositivos y plantillas dentro de sus dominios de acceso**.**

- Comparación de cambios en configuraciones de Panorama.
  1. Seleccione **Panorama** > **Config Audit (Auditoría de configuraciones)**.
  2. En cada menú desplegable, seleccione una configuración para la comparación.
  3. Seleccione el número de líneas que desee incluir para el **Context (Contexto)** y haga clic en **Go (Ir)**.

     Panorama usa diferentes colores para destacar los elementos que agregó (verde), modificó (amarillo) o eliminó (rojo).

- Configuración del número de versiones que Panorama almacena para auditorías de configuración.
  1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de logs e informes.
  2. Ingrese el **Number of Versions for Config Audit (Número de versiones para auditorías de configuraciones)** (el intervalo es de 1 a 1 048 576; el valor predeterminado es 100).
  3. Haga clic en **OK (Aceptar)** para guardar los cambios.
  4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

- Visualización y comparación de archivos de configuración de Panorama antes de compilarlos.
  1. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Preview Changes (Previsualizar los cambios)**.
  2. Seleccione el número de **Lines of Context (Líneas de contexto)** que desea ver y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

Gestión de bloqueos para restringir cambios de configuración

Bloquear la configuración candidata o en ejecución evita que otros administradores la cambien hasta que usted elimine manualmente el bloqueo o que Panorama lo elimine automáticamente (después de una compilación). Los bloqueos garantizan que los administradores no realicen cambios conflictivos para los mismos ajustes o para ajustes interdependientes durante sesiones iniciadas simultáneas.

Si está cambiando una configuración que no está relacionada con la configuración que otros administradores están cambiando en sesiones concurrentes, los bloqueos de configuración no son necesarios para evitar la compilación de conflictos. Panorama coloca en cola las operaciones de compilación y las lleva a cabo en el orden en que los administradores inician las compilaciones. Para obtener más detalles, consulte Operaciones de confirmación, validación y previsualización de Panorama**.**

Un envío de plantilla o grupo de dispositivos fallará si un cortafuegos asignado a uno de estos tiene un bloqueo de configuración o confirmación que un administrador configuró de manera local en ese cortafuegos.

- Visualice detalles sobre los bloqueos actuales.

  Por ejemplo, puede comprobar si otros administradores configuraron bloqueos y leer los comentarios que introdujeron para explicar los bloqueos.

  Haga clic en el icono de bloqueo ( ) en la parte superior de la interfaz web. El número adyacente indica la cantidad de bloqueos actuales.

 ©2023 Palo Alto Networks, Inc.

- Bloquee una configuración.

  Los administradores con acceso de solo lectura que no pueden modificar las configuraciones del cortafuegos o de Panorama no pueden establecer bloqueos.

  1. Haga clic en el icono de bloqueo en la parte superior de la interfaz web.

     El icono varía de acuerdo a si se establecieron bloqueos existentes ( ) o no ( ).
  2. Seleccione **Take a Lock** para seleccionar un bloqueo y luego seleccione el tipo de bloqueo en **Type**:

     - **Config**: bloquea los cambios en la configuración candidata por parte de otros administradores.

       *Un administrador con función personalizada que no puede compilar cambios puede configurar un bloqueo de **Config (Configuración)** y guardar los cambios en la configuración candidata. Sin embargo, debido a que el administrador no puede compilar los cambios, Panorama no elimina el bloqueo automáticamente después de una compilación; el administrador debe eliminar manualmente el bloqueo de **Config (Configuración)** después de realizar los cambios necesarios.*

     - **Commit**: bloquea los cambios en la configuración en ejecución por parte de otros administradores.
  3. Seleccione **Location (Ubicación)** para determinar el alcance del bloqueo:

     - **Shared (Compartido)**: restringe los cambios a la configuración completa de Panorama, incluidos todos los grupos de dispositivos y plantillas.
     - **Template (Plantilla)**: restringe los cambios en los cortafuegos incluidos en la plantilla seleccionada. (No puede aplicar un bloqueo en una pila de plantillas, solo para plantillas individuales dentro de la pila).
     - **Device group (Grupo de dispositivos)**: Restringe los cambios en el grupo de dispositivos seleccionado pero no en sus grupos de dispositivos secundarios.
  4. (Opcional) Se recomienda introducir un **Comment (Comentario)** para describir el motivo del bloqueo.
  5. Haga clic en **OK (Aceptar)** y **Close (Cerrar)**.

- Desbloquee una configuración.

  Solo un superusuario o el administrador que bloqueó la configuración pueden desbloquearla manualmente. Sin embargo, Panorama quita automáticamente un bloqueo después de completar la compilación que inició el administrador que estableció el bloqueo.

  1. Haga clic en el icono de bloqueo ( ) en la parte superior de la interfaz web.
  2. Seleccione la entrada de bloqueo de la lista.
  3. Haga clic en **Remove Lock (Eliminar bloqueo)**, **OK (Aceptar)** y **Close (Cerrar)**.

 ©2023 Palo Alto Networks, Inc.

- Configure Panorama para que bloquee automáticamente la configuración en ejecución cuando cambie la configuración candidata. Este ajuste se aplica a todos los administradores de Panorama.
  1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.
  2. Seleccione **Automatically Acquire Commit Lock (Obtener bloqueo de compilación automáticamente)** y luego haga clic en **OK (Aceptar)**.
  3. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

Adición de logotipos personalizados a Panorama

Puede cargar archivos de imágenes para personalizar las siguientes áreas de Panorama:

- Imagen de fondo en la pantalla de inicio de sesión
- Encabezado de la esquina superior izquierda de la interfaz web; también puede ocultar el fondo predeterminado de Panorama
- Página de título e imagen de pie de página en informes en PDF

Los tipos de imágenes admitidas incluyen .jpg, .gif y .png. Los archivos de imágenes para su uso en informes en PDF no pueden contener un canal alfa. El tamaño de la imagen debe ser inferior a 128 kilobytes (131.072 bytes); las dimensiones recomendadas aparecen en la pantalla. Si la dimensión es mayor que el tamaño recomendado, la imagen se recortará automáticamente.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.

STEP 2 | En la sección Varios, haga clic en **Custom Logos (Logotipos personalizados)**.

STEP 3 | Haga clic en el icono Cargar logotipo y seleccione una imagen para cualquiera de las siguientes opciones: pantalla de inicio de sesión, esquina izquierda de la interfaz de usuario principal, página de título de informe en PDF y pie de página del informe en PDF.

STEP 4 | Haga clic en **Open (Abrir)** para añadir la imagen. Para obtener una vista previa de la imagen, haga clic en el icono de vista previa de logotipo.

STEP 5 | (Opcional) Para borrar el encabezado de fondo verde en la interfaz web de Panorama, seleccione la casilla de verificación **Remove Panorama background header (Eliminar encabezado de fondo de Panorama)**.

STEP 6 | Haga clic en **Close (Cerrar)** para guardar los cambios.

STEP 7 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

 ©2023 Palo Alto Networks, Inc.

Uso del gestor de tareas de Panorama

Haga clic en **Tasks (Tareas)** () en la parte inferior de la interfaz web para abrir el gestor de tareas, que muestra detalles sobre todas las operaciones que iniciaron los administradores (por ejemplo, las compilaciones manuales) o que Panorama o un cortafuegos gestionado inició (por ejemplo, la generación de informes programada) desde el último reinicio de Panorama o del cortafuegos. Puede usar el gestor de tareas para solucionar problemas de operaciones con errores, investigar advertencias asociadas con compilaciones finalizadas o cancelar compilaciones pendientes.

Los administradores de plantillas y grupos de dispositivos solo pueden ver las tareas dentro de sus dominios de acceso**.**

STEP 1 | Haga clic en **Tasks (Tareas)**.

STEP 2 | Haga clic en **Show (Mostrar)** para que se muestren las tareas en **Running (En ejecución)** (en progreso) o todas las tareas en **All (Todas)** (opción predeterminada), de manera opcional filtre por tipo (**Reports [Informes]**; **Log Requests [Solicitudes de logs]**; o compile, descargue e instale **Jobs [Tareas]**), y seleccione **Panorama** (predeterminado) o el cortafuegos del cual desea ver sus tareas.

STEP 3 | Tome una de las siguientes medidas:

- **Display or hide task details**: por defecto, el gestor de tareas muestra el tipo, estado, hora de inicio y los mensajes para cada tarea. Para ver la hora de fin y el ID de la tarea, debe mostrar manualmente estas columnas. Para mostrar u ocultar una columna, abra el menú desplegable de cualquier encabezado de columna, seleccione **Columns (Columnas)**, y seleccione o borre las columnas como desee.
- **Investigate warnings or failures**: lea las entradas en la columna de mensajes para ver detalles de las tareas. Si la columna indica `Too many messages (Demasiados mensajes)`, haga clic en la entrada en la columna Type (Tipo) para ver más información.
- **Mostrar una descripción de compilación**: si un administrador ingresó una descripción para una compilación, haga clic en **Commit Description (Descripción de compilación)** en la columna Mensajes para mostrarla.
- **Check the position of a commit in the queue**: la columna de mensajes indica la posición en cola de las confirmaciones que están en curso.
- **Cancelar confirmaciones pendientes**: haga clic en **Clear Commit Queue (Borrar cola de confirmación)** para cancelar todas las confirmaciones pendientes (disponible solo para las funciones administrativas predefinidas). Para cancelar una compilación individual, haga clic en **x** en la columna Acción (la compilación permanece en la cola hasta que Panorama la quite de allí). No puede cancelar confirmaciones que están en curso.

 ©2023 Palo Alto Networks, Inc.

Gestión de cuotas de almacenamiento y períodos de vencimiento de logs e informes

- Almacenamiento de logs e informes
- Períodos de vencimiento de logs e informes
- Configuración de cuotas de almacenamiento y períodos de vencimiento de logs e informes
- Configuración del tiempo de ejecución para los informes de Panorama

Almacenamiento de logs e informes

Puede editar las cuotas de almacenamiento predeterminadas de cada tipo de log. Cuando una cuota de log alcanza el tamaño máximo, Panorama empieza a sustituir las entradas del log más antiguas por las nuevas. No es posible configurar la capacidad de almacenamiento para los informes. Las ubicaciones de almacenamiento de logs y las capacidades de almacenamiento de informes varían según el modelo de Panorama:

- **Dispositivo virtual Panorama en modo Panorama**: el espacio de almacenamiento para los informes es de 200 MB. El dispositivo usa su disco de sistema virtual para almacenar los logs de Sistema y la Configuración que generan Panorama y los recopiladores de logs. El disco del sistema virtual también almacena los logs de estadísticas de la aplicación (App Stats) que Panorama recibe automáticamente a intervalos de 15 minutos de todos los cortafuegos gestionados. Panorama almacena todos los demás tipos de logs en sus discos virtuales de logging (1 a 12).
- **Dispositivo virtual Panorama en modo solo de gestión**: el espacio de almacenamiento para los informes es de 500 MB. El dispositivo usa su disco de sistema virtual para almacenar los logs de Sistema y la Configuración que generan Panorama y los recopiladores de logs. El disco del sistema virtual también almacena los logs de estadísticas de la aplicación (App Stats) que Panorama recibe automáticamente a intervalos de 15 minutos de todos los cortafuegos gestionados. Debe realizar la Configuración de un recopilador gestionado para reenviar logs de cortafuegos gestionados dado que Panorama en modo solo de gestión no puede almacenar otros tipos de logs.
- **Dispositivo virtual Panorama en modo heredado**: el espacio de almacenamiento para los informes es de 200 MB para Panorama 8.0 o versiones anteriores y 500 MB para Panorama 8.0.1 y versiones posteriores. Panorama guarda todos los logs en su espacio de almacenamiento asignado, el cual puede ser cualquiera de los siguientes:
  - **Disco del sistema virtual**: por defecto, aproximadamente 11 GB están asignados para el almacenamiento de logs en el disco del sistema virtual que creó al instalar Panorama. Si agrega un disco de logs virtuales o una partición NFS, Panorama todavía usa el disco del sistema para almacenar los logs de Sistema y logs de Configuración que generan los Recopiladores de logs y Panorama y para almacenar los logs de Estadísticas de la Aplicación recopilados de los cortafuegos.
  - **Disco de logging virtual dedicado**: almacena todos los tipos de logs excepto aquellos que residen en el disco del sistema.
  - **Partición NFS**: esta opción está disponible solo para Panorama cuando se ejecuta en un servidor VMware ESXi. La partición NFS almacena todos los tipos de logs excepto aquellos que residen en el disco del sistema.

 ©2023 Palo Alto Networks, Inc.

- **Dispositivo M-700, M-600, M-500 o M-200**: el espacio de almacenamiento para los informes es de 500 MB en Panorama 6.1 o versiones posteriores y de 200 MB para las versiones anteriores. Los dispositivos M-Series usan su SSD interno para almacenar los logs de configuración y del sistema que Panorama y los recopiladores de logs generan, y también para almacenar los logs de Estadísticas de aplicación (App Stats) recopilados de los cortafuegos. Panorama guarda todos los otros tipos de logs en sus discos con capacidad RAID. Los discos RAID son locales en el dispositivo de la serie M en modo Panorama o se encuentran en un recopilador de logs dedicado (dispositivo de la serie M en modo de recopilación de logs). Usted edita las cuotas de almacenamiento de logs en los discos RAID cuando realiza la Configuración de un grupo de recopiladores.

  Para obtener información detallada sobre las opciones y capacidades de almacenamiento de logs, consulte Modelos de Panorama. *Puede realizar la* Expansión de la capacidad de almacenamiento del log en el dispositivo virtual Panorama *añadiendo discos de logging virtual o almacenamiento NFS. Usted puede realizar el* Aumento de la capacidad de almacenamiento en el dispositivo serie M *añadiendo unidades RAID o actualizando de unidades de 1 TB a unidades de 2 TB.*

Períodos de vencimiento de logs e informes

Puede configurar la eliminación automática según el horario para los logs que los recopiladores de logs y el servidor de gestión de Panorama obtiene de los cortafuegos, además de los logs e informes que Panorama y los recopiladores de logs generan localmente. Esto es útil en las implementaciones en las que se desee o sea necesario eliminar periódicamente la información supervisada. Por ejemplo, eliminar la información de usuario después de un determinado período podría ser obligatorio en su organización por motivos legales. Configure períodos de vencimiento individuales para los siguientes:

- **Informes**: Panorama elimina los informes caducados al mismo tiempo que genera nuevos informes (consulte Configuración del tiempo de ejecución para los informes de Panorama)
- **Cada tipo de log**: Panorama evalúa los logs a medida que los recibe y elimina los que superan el período de vencimiento configurado.
- *Panorama sincroniza los períodos de vencimiento en todos los pares de alta disponibilidad (high availability, HA). Debido a que solo el peer activo de HA genera logs, el peer pasivo no tiene logs o informes que se deban eliminar salvo que se produzca una conmutación por error y se comience a generar logs.*

  Incluso si no configura los períodos de vencimiento, cuando una cuota de log alcanza el tamaño máximo, Panorama empieza a sustituir las entradas del log más antiguas por las nuevas.

Configuración de cuotas de almacenamiento y períodos de vencimiento de logs e informes

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Configure las cuotas de almacenamiento y los períodos de vencimiento para los siguientes:

- Logs de todos los tipos que un dispositivo virtual Panorama en modo heredado reciba de los cortafuegos.
- Logs de estadísticas de aplicaciones que Panorama recibe de los cortafuegos.
- Logs de sistema y configuración que Panorama y los recopiladores de logs generan localmente.

El servidor de gestión de Panorama almacena estos logs localmente.

Si reduce una cuota de almacenamiento de tal forma que los logs actuales la superan, después de compilar el cambio, Panorama elimina los logs antiguos para adaptar la cuota.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de logs e informes.
2. En los ajustes de **Log Storage (Almacenamiento de logs)**, introduzca la **Quota (%) (Cuota [%])** de almacenamiento de cada tipo de log.

   Al cambiar un valor del porcentaje, la página se actualiza para mostrar el valor absoluto correspondiente (columna de cuota GB/MB) basado en el almacenamiento total asignado en Panorama.
3. Introduzca el **Max Days (Número máx. de días)** (periodo de vencimiento) para cada tipo de log (el intervalo es 1 a 2.000).

   De manera predeterminada, los campos están en blanco, lo que significa que los logs nunca se vencen.

   *Seleccione **Restore Defaults (Restablecer valores predeterminados)** si desea restablecer las cuotas y los períodos de vencimiento a los valores de fábrica.*

STEP 2 | Configure el período de vencimiento de los informes que genera Panorama.

1. Seleccione **Log Export and Reporting (Exportación e informes de logs)** e introduzca el **Report Expiration Period (Periodo de vencimiento de informes)** en días (el rango es de 1 a 2000).

   De manera predeterminada, el campo está en blanco, lo que significa que los informes nunca se vencen.
2. Haga clic en **OK (Aceptar)** para guardar los cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configure las cuotas de almacenamiento y los períodos de vencimiento para los logs de todos los tipos (excepto los logs de estadísticas de aplicaciones) que los dispositivos M-700, M-600, M-500, M-300, M-200 o el dispositivo virtual Panorama recibe de los cortafuegos.

Los recopiladores de logs locales o dedicados almacenan estos logs.

Configure estas cuotas de almacenamiento en el nivel del grupo de recopiladores, no para los recopiladores individuales.

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y modifique el grupo de recopiladores.
2. En la configuración **General**, haga clic en el valor de **Log Storage (Almacenamiento de logs)**.

   No se muestra ningún valor a menos que haya asignado recopiladores de logs al grupo de recopiladores. Si el campo muestra 0 MB después de asignar recopiladores de logs, verifique que habilitó los pares de discos cuando realizó la Configuración de un recopilador gestionado *y que confirmó los cambios (**Panorama** > **Managed Collectors [Recopiladores gestionados]** > **Disks [Discos]**).*
3. Introduzca la **Quota(%) (Cuota[%])** de almacenamiento para cada tipo de log.

   Al cambiar un valor del porcentaje, la página se actualiza para mostrar el valor absoluto correspondiente (columna de cuota GB/MB) basado en el almacenamiento total asignado al grupo de recopiladores.
4. Introduzca el **Max Days (Número máx. de días)** (periodo de vencimiento) para cada tipo de log (el intervalo es 1 a 2.000).

   De manera predeterminada, los campos están en blanco, lo que significa que los logs nunca se vencen.

   *Seleccione **Restore Defaults (Restablecer valores predeterminados)** si desea restablecer las cuotas y los períodos de vencimiento a los valores de fábrica.*
5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Confirme los cambios realizados a Panorama y envíe los cambios al grupo de recopiladores.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Collector Groups (Grupos de recopiladores)**, seleccione el grupo de recopiladores que ha modificado y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 5 | Verifique que Panorama aplicó los cambios en la cuota de almacenamiento.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y en la configuración de Creación de logs e informes, verifique que los valores de **Log Storage (Almacenamiento de logs)** sean correctos para los logs que el servidor de gestión de Panorama almacena.
2. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)**, seleccione el grupo de recopiladores que modificó y verifique que los valores de **Log Storage**

 ©2023 Palo Alto Networks, Inc.

(Almacenamiento de logs) en la pestaña **General (General)** sean correctos para los logs que los recopiladores de logs almacenan.



También puede verificar las cuotas de almacenamiento del grupo de recopiladores accediendo a la CLI del recopilador de logs e ingresando el comando de operación ***`show log-diskquota-pct`***.

Configuración del tiempo de ejecución para los informes de Panorama

Panorama genera informes diariamente en el momento que usted haya programado. Panorama elimina los informes caducados después de generar los informes nuevos.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de logs e informes.

STEP 2 | Seleccione **Log Export and Reporting (Exportación de logs y creación de informes)** y defina la hora en **Report Runtime (Hora de ejecución de informes)** con el sistema de 24 horas; el valor predeterminado son las 02:00 y el intervalo va de las 00:00 (medianoche) a las 23:00.

STEP 3 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

 ©2023 Palo Alto Networks, Inc.

Supervisión de Panorama

Para supervisar Panorama y sus recopiladores gestionados, puede ver periódicamente sus logs de sistema y configuración (filtrar logs por tipo), configurar un gestor de Protocolo SNMP para que recopile estadísticas (GET) de Panorama con regularidad, o configurar traps de SNMP o alertas de correo electrónico que le notifiquen cuando una métrica supervisada cambia de estado o alcanza un umbral en Panorama. Las alertas de correo electrónico y traps SNMP son útiles para la notificación inmediata sobre eventos críticos del sistema que requieren su atención. Para configurar las alertas de correo electrónico o traps SNMP, consulte Configuración del reenvío de logs desde Panorama a destinos externos.

- Logs de sistema y de configuración de Panorama
- Supervisión de estadísticas de Panorama y recopiladores de logs mediante SNMP

Logs de sistema y de configuración de Panorama

Puede configurar Panorama para que envíe notificaciones cuando se produce un evento del sistema o se realiza un cambio en la configuración. De forma predeterminada, Panorama registra cualquier cambio de configuración en los logs de configuración. En el log de sistema, los eventos aparecen con un nivel de gravedad que indica su urgencia e impacto. Cuando usted Configuración del reenvío de logs desde Panorama a destinos externos, usted puede reenviar todos los logs del sistema y de configuración o filtrar los logs según los atributos, como el tiempo de recepción o el nivel de gravedad (solo logs del sistema). La siguiente tabla resume los niveles de gravedad de los logs del sistema.

Panorama se conecta regularmente al servicio IoT Edge para descargar recomendaciones de políticas para políticas basadas en IoT. Panorama intenta esta conexión independientemente de si la licencia de IoT está activa en cualquier cortafuegos gestionado.

Se genera un log del sistema de error de conexión gRPC de alta gravedad en caso de fallo de conexión o si Panorama no administra ningún cortafuegos con licencia de IoT. No se necesita ninguna acción con respecto a estos logs del sistema si no está aprovechando las capacidades de recomendación de políticas de IoT o si no está gestionando ningún cortafuegos con licencia de IoT.

Si está aprovechando las capacidades de recomendación de políticas de IoT, revise el log del sistema de errores de conexión gRPC para comprender qué está causando el problema de conexión entre Panorama y el servicio IoT Edge.

Panorama no admite la consulta de logs de configuración en el ***ACC*** *o cuando se supervisan logs de configuración (****Monitor [Supervisar]*** *>* ***Logs*** *) usando los filtros:*

`before-change-preview-contains`

`after-change-preview-contains`

 ©2023 Palo Alto Networks, Inc.

Gravedad	Description (Descripción)
Crítico	Indica un fallo y la necesidad de atención inmediata, como un fallo de hardware, incluida la conmutación por error de alta disponibilidad (high availability, HA) y los fallos de los enlaces.
high (alta)	Incidentes graves que afectarán al funcionamiento del sistema, incluida la desconexión de un recopilador de logs o un fallo de compilación.
Intermedia	Notificaciones de nivel medio, como actualizaciones del paquete de antivirus o el envío de una configuración del grupo de recopiladores.
low (baja)	Notificaciones de menor gravedad, como cambios de contraseña de usuario.
Informativo	Eventos de notificación como inicio y cierre de la sesión, cambios en la configuración, realización correcta de la autenticación y notificaciones de fallos, realización correcta de la compilación y todos los demás eventos no englobados en otros niveles de gravedad.

Panorama almacena los logs de configuración y sistema localmente; la ubicación exacta y la capacidad de almacenamiento varían según el modelo de Panorama (consulte Almacenamiento de logs e informes). Al alcanzar el límite de capacidad, Panorama elimina los logs más antiguos para crear espacio para nuevos logs. Si necesita almacenar los logs por períodos más largos de lo que permite el almacenamiento local, puede Configuración del reenvío de logs desde Panorama a destinos externos.

Para obtener más información sobre cómo usar Panorama para supervisar logs de cortafuegos, consulte Supervisión de la actividad de red**.**

Supervisión de estadísticas de Panorama y recopiladores de logs mediante SNMP

Puede configurar un gestor SNMP para que solicite información de un servidor de gestión de Panorama y configurar Panorama para que responda. Por ejemplo, el gestor SNMP puede solicitar el modo de alta disponibilidad (high availability, HA), el estado de Panorama y la versión de Panorama. Si el servidor de gestión de Panorama tiene un recopilador de logs local, Panorama también puede proporcionar estadísticas de logging: logs promedio por segundo, duración de almacenamiento, períodos de retención, uso de disco de los logs, estado de reenvío de logs desde cortafuegos individuales a servidores Panorama y externos, y el estado de conexiones de recopilador de cortafuegos a log. Panorama no sincroniza las configuraciones SNMP entre los peers de HA, debe habilitar las solicitudes y respuestas de SNMP en cada peer.

También puede configurar un recopilador de registro dedicado para responder a las solicitudes de las mismas estadísticas de registro que el servidor de gestión de Panorama. Esta información es útil al evaluar si necesita ampliar la capacidad de almacenamiento de logs.

 ©2023 Palo Alto Networks, Inc.

No puede configurar un gestor SNMP para que controle Panorama o los recopiladores de logs (mediante mensajes SET); un gestor SNMP solo puede recopilar estadísticas (mediante mensajes GET).

Para obtener información sobre cómo Panorama implementa SNMP, consulte a la asistencia de SNMP.

STEP 1 | Configure el gestor SNMP para obtener estadísticas de Panorama y los recopiladores de logs.

Los siguientes pasos son una descripción general de las tareas que realiza en el gestor SNMP. Para ver los pasos específicos, consulte la documentación de su gestor SNMP.

1. Para permitir que el gestor SNMP interprete las estadísticas del dispositivo, cargue los MIB compatibles y, si es necesario, realice una compilación de ellos.
2. Para cada dispositivo Panorama que el gestor SNMP supervisará, defina la configuración de conexión (dirección IP y puerto) y la configuración de autenticación (cadena de comunidad SNMPv2c o nombre de usuario y contraseña SNMPv3). Todos los dispositivos Panorama usan el puerto 161.

   El gestor SNMP puede usar la misma conexión o una diferente y los ajustes de autenticación para múltiples recopiladores de logs y servidores de gestión de Panorama. Los ajustes deben coincidir con los que define cuando configura SNMP en Panorama (consulte Configuración del servidor de gestión Panorama para que responda a las solicitudes de estadísticas de un gestor SNMP y Configuración del servidor de gestión Panorama para que responda a las estadísticas de un gestor SNMP). Por ejemplo, si usa SNMPv2c, la cadena de comunidad que defina al configurar Panorama debe coincidir con la cadena de comunidad que defina en el gestor SNMP para Panorama.
3. Determine los Identificadores de objeto (object identifiers, OID) de las estadísticas que supervisará. Por ejemplo, para supervisar la tasa de logs, un navegador MIB muestra que esta estadística corresponde al OID 1.3.6.1.4.1.25461.2.3.30.1.1 en PAN-PRODUCT-MIB.my. Para obtener más detalles, consulte Cómo usar un gestor SNMP para explorar MIB y objetos.
4. Configure el gestor SNMP para monitorizar los OID deseados.

STEP 2 | Habilite el tráfico SNMP en la interfaz de gestión (management, MGT) del servidor de gestión de Panorama.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración de interfaz de gestión.
2. En la sección Servicios, seleccione la casilla de verificación **SNMP** y haga clic en **OK (Aceptar)**.

STEP 3 | Habilite el tráfico SNMP en la interfaz de gestión (MGT) de cualquier dispositivo de la serie M en el modo de recopilación de logs:

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y elija el recopilador de logs.
2. Seleccione la pestaña **Management (Gestión)**, seleccione la casilla de verificación **SNMP** y haga clic en **OK (Aceptar)**.

STEP 4 | Configure el servidor de gestión de Panorama para que responda a las solicitudes de estadísticas de un gestor SNMP.

 ©2023 Palo Alto Networks, Inc.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y en la sección Varios, haga clic en **SNMP Setup (Configuración SNMP)**.
2. Seleccione la **Version** de SNMP y configure los valores de autenticación del siguiente modo. Para obtener más detalles, consulte a la asistencia de SNMP.
   - **V2c**: introduzca la **SNMP Community String (Cadena de comunidad SNMP)**, que identifica a una comunidad de gestores SNMP y dispositivos supervisados (en este caso, Panorama), además de servir como contraseña para autenticar a los miembros de la comunidad entre sí.

     No utilice la cadena de comunidad predeterminada ***`public (pública)`****, ya que es muy conocida y, por lo tanto, no es segura.*
   - **V3**: cree al menos un grupo de vistas SNMP y un usuario. Las cuentas de usuario y las vistas brindan control de acceso, privacidad y autenticación cuando los gestores SNMP obtienen estadísticas.

     Vistas: cada vista es un OID emparejado y una máscara binaria: el OID especifica un MIB y la máscara (en formato hexadecimal) especifica qué objetos son accesibles dentro (incluir coincidencias) o fuera (excluir coincidencias) del MIB. Haga clic en **Add (Añadir)** en la primera lista e introduzca un **Name (Nombre)** para el grupo de vistas. En cada vista del grupo, haga clic en **Add (Añadir)** y configure los campos **Name (Nombre)**, **OID (Identificador de objeto)**, **Option (Opción)** coincidente (**include [incluir]** o **exclude [excluir]**) y **Mask (Máscara)** de la vista.

     Usuarios: haga clic en **Add** en la segunda lista, introduzca un nombre de usuario en la columna Usuarios, seleccione el grupo de **View** del menú desplegable, introduzca la contraseña de autenticación (**Auth Password**) utilizada para autenticar el gestor SNMP e ingrese la contraseña de privacidad (**Priv Password**) utilizada para cifrar los mensajes SNMP en el gestor SNMP.
3. Haga clic en **OK (Aceptar)** para guardar los ajustes.

STEP 5 | Configure los recopiladores de logs dedicados (si los hubiera) para que respondan a las solicitudes de SNMP.

En cada grupo de recopiladores:

1. Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** y seleccione el grupo de recopiladores.
2. Seleccione la pestaña **Monitoring (Supervisión)**, configure los mismos ajustes en el paso Configure el servidor de gestión de Panorama para que responda a las solicitudes de estadísticas de un gestor SNMP. y haga clic en **OK (Aceptar)**.

STEP 6 | Confirme los cambios realizados a Panorama y envíe los cambios a los Grupos de recopiladores.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Collector Groups (Grupos de recopiladores)**, seleccione los grupos de recopiladores que ha editado y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Supervise las estadísticas de Panorama y recopiladores de logs mediante un gestor SNMP.

Consulte la documentación de su gestor SNMP.

 ©2023 Palo Alto Networks, Inc.

Reinicio o cierre de Panorama

La opción de reinicio activa la opción de reinicio correcto de Panorama. El cierre detiene el sistema y lo apaga. Para reiniciar Panorama, después de un cierre, desconecte y vuelva a conectar el cable de alimentación del sistema manualmente.

STEP 1 | Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.

STEP 2 | En la sección Operaciones de dispositivo, seleccione **Reboot Panorama (Reiniciar Panorama)** o **Shutdown Panorama (Apagar Panorama)**.

 ©2023 Palo Alto Networks, Inc.

Configuración de perfiles de contraseña y complejidad de contraseña de Panorama

Para asegurar la cuenta del administrador local, puede definir los requisitos de complejidad de la contraseña que se aplican cuando los administradores cambian o crean nuevas contraseñas. Al contrario de lo que pasa en los perfiles de contraseñas, que se pueden aplicar a cuentas individuales, estas reglas de complejidad de contraseña se aplican a todo el cortafuegos y a todas las contraseñas.

Para aplicar actualizaciones periódicas de la contraseña, cree un perfil de contraseña que defina un periodo de validez para las contraseñas.

STEP 1 | Configure ajustes de complejidad mínima de la contraseña.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la sección Complejidad de contraseña mínima.
2. Seleccione **Enabled (Habilitado)**.
3. Defina la opción **Password Format Requirements (Requisitos de formato de la contraseña)**. Puede aplicar los requisitos de formato que debe tener la contraseña (mayúscula, minúscula, números y caracteres especiales).
4. Para evitar que el nombre de usuario se utilice en la contraseña (o una versión invertida del nombre), seleccione **Block Username Inclusion (including reversed) (Bloquear inclusión de nombre de usuario [incluida su inversión])**.
5. Defina los **Functionality Requirements (Requisitos de funcionalidad)** de la contraseña.

   Si ha configurado un perfil de contraseña para un administrador, los valores definidos en el perfil de contraseña sobrescribirán los valores que ha definido en esta sección.

STEP 2 | Cree perfiles de contraseña.

Puede crear varios perfiles de contraseña y aplicarlos a las cuentas de administrador según sea necesario para imponer la seguridad.

1. Seleccione**Panorama** > **Password Profiles (Perfiles de contraseña)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** para el perfil de la contraseña y defina lo siguiente:
   1. **Required Password Change Period (Período necesario para el cambio de contraseña)**: frecuencia, en días, con la que deben cambiarse las contraseñas..
   2. **Expiration Warning Period (Período de advertencia de vencimiento)**: días de antelación con los que el administrador recibirá un recordatorio de contraseña antes del vencimiento.
   3. **Post Expiration Grace Period (Período de gracia posterior al vencimiento)**: número de días en los que el administrador puede seguir iniciando sesión en el sistema después del vencimiento de la contraseña.
   4. **Post Expiration Admin Login Count (Recuento de inicio de sesión de administrador posterior al vencimiento)**número de ocasiones en las que el administrador puede iniciar sesión en el sistema después del vencimiento de la contraseña.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Complementos de Panorama

La arquitectura ampliable de complementos de Panorama admite integraciones de productos ajenos, como Vmware NSX, y de otros productos de Palo Alto Networks, como el servicio en la nube GlobalProtect. Con esta arquitectura modular, puede aprovechar las nuevas capacidades sin esperar una nueva versión de PAN-OS.

En Panorama también puede configurar el complemento VM-Series. Este complemento independiente posibilita la integración con entornos de nube pública, como Google Cloud Platform (GCP), Azure o AWS, e hipervisores de nube privada, como KVM o ESXi, entre otros. El complemento VM-Series permite publicar métricas de los cortafuegos VM-Series implementados en las nubes públicas. Con Panorama puede configurar los ajustes del complemento VM-Series para las nubes públicas, así como enviar la configuración a los cortafuegos gestionados.

- Acerca de los complementos de Panorama
- Complemento VM-Series y complementos de Panorama

Acerca de los complementos de Panorama

Panorama admite una arquitectura de complementos expandible que permite la integración y la configuración de las siguientes capacidades:

- **AIOps**: el complemento AIOps le permite aplicar de manera proactiva las comprobaciones de las mejores prácticas mediante la validación de sus compilaciones, y le permite saber si una política necesita cambios antes de enviarla a Panorama.
- **AWS:** el complemento AWS le permite supervisar sus cargas de trabajo EC2 en AWS. Con él, puede habilitar la comunicación entre Panorama (con PAN-OS 8.1.3 o versiones posteriores) y las nubes privadas virtuales (Virtual Private Cloud, VPC) de AWS, de modo que Panorama pueda recopilar el conjunto de atributos (o elementos de metadatos) predefinidos en forma de etiquetas para las instancias de EC2, así como registrar la información en los cortafuegos de Palo Alto Networks. Si se hace referencia a estas etiquetas en los grupos de direcciones dinámicas y se cotejan con las reglas de la política de seguridad, esta se aplica de forma sistemática en todos los recursos implementados en las VPC.
- **Azure**: el complemento Azure le permite supervisar sus máquinas virtuales en la nube pública de Azure. Con el complemento, puede habilitar la comunicación entre Panorama (con PAN-OS 8.1.6 o versiones posteriores) y sus suscripciones a Azure, de modo que Panorama pueda recopilar un conjunto de atributos (o elementos de metadatos) predefinidos como etiquetas para sus máquinas virtuales Azure y registrar la información en sus cortafuegos Palo Alto Networks® Si se hace referencia a estas etiquetas en los grupos de direcciones dinámicas y se cotejan con las reglas de la política de seguridad, esta se aplica de forma sistemática en todos los recursos implementados en las redes virtuales de sus suscripciones.
- **Cisco ACI**: el complemento Cisco ACI permite supervisar los terminales de la estructura de Cisco ACI. Con él, puede habilitar la comunicación entre Panorama (8.1.6 y versiones posteriores) y el controlador Cisco APIC, de modo que Panorama pueda recopilar los datos de los terminales en forma de etiquetas para los grupos de terminales, así como registrar la información en los cortafuegos de Palo Alto Networks. Si se hace referencia a estas etiquetas en los grupos de direcciones dinámicas y se cotejan con las reglas de la política de seguridad, esta se aplica de forma sistemática en todos los recursos implementados en la estructura de Cisco ACI.
- **Cisco TrustSec**: el complemento de Cisco TrustSec permite la supervisión de endpoints en su entorno de Cisco TrustSec. Con él, puede habilitar la comunicación entre Panorama y el controlador servidor Cisco pxGrid, de modo que Panorama pueda recopilar los datos de los terminales en forma de etiquetas para los endpoints, así como registrar la información en los cortafuegos de Palo Alto Networks®. Si se hace referencia a estas etiquetas en los grupos de direcciones dinámicas y se cotejan con las reglas de la política de seguridad, esta se aplica de forma sistemática en todos los recursos implementados en el entorno de Cisco TrustSec.

  No se admite en Panorama en modo FIPS-CC.

- **Servicios en la nube**: el complemento de Servicios en la nube permite usar Cortex Data Lake y Prisma Access. Cortex Data Lake soluciona los desafíos de creación de logs operativos y el servicio en la nube de Prisma Access expande su infraestructura de seguridad a las ubicaciones de su red remota y a la fuerza laboral móvil.
- **Prevención de pérdida de datos (DLP)** empresarial: la prevención de pérdida de datos (DLP, Data Loss Prevention) empresarial es un conjunto de herramientas y procesos que le permiten

 ©2023 Palo Alto Networks, Inc.

proteger la información confidencial contra el acceso no autorizado, el uso indebido, la extracción o el intercambio. La DLP empresarial se habilita a través de un servicio en la nube para ayudarlo a inspeccionar el contenido y analizar los datos en el contexto correcto de modo que pueda identificar con precisión los datos confidenciales y protegerlos para evitar incidentes. DLP empresarial es compatible en Panorama y cortafuegos gestionados con PAN-OS 10.0.2 y versiones posteriores.

No se admite en Panorama en modo FIPS-CC.

- **GCP**: permite proteger los servicios de Kubernetes de los clústeres de Google Kubernetes Engine (GKE). Configure el complemento de Panorama para Google Cloud Platform (GCP) de modo que se conecte a los clústeres de GKE y obtenga información sobre los servicios expuestos a internet.
- **Panorama Interconnect**: el complemento Panorama Interconnect le permite gestionar implementaciones de cortafuegos a gran escala. Use el complemento Interconnect para configurar una implementación de Panorama de dos niveles (en Panorama con PAN-OS 8.1.3 o una versión posterior) para una arquitectura de escalabilidad horizontal. Con el complemento Interconnect, puede implementar un controlador Panorama con hasta 64 nodos de Panorama o 32 pares de HA de Panorama para gestionar centralmente una gran cantidad de cortafuegos.
- **Nutanix**: el complemento de Panorama de Nutanix permite la supervisión de la VM en el entorno de Nutanix. Le permite rastrear el inventario de máquinas virtuales dentro de Nutanix Prism Central para que pueda aplicar de manera coherente la política de seguridad que se adapta automáticamente a los cambios dentro de su entorno de Nutanix. A medida que se aprovisionan, desaprovisionan o mueven máquinas virtuales, esta solución le permite recopilar las direcciones IP y los conjuntos de atributos asociados (o elementos de metadatos) como etiquetas. Puede utilizar las etiquetas para definir grupos de direcciones dinámicas y usarlas en la política de seguridad. El complemento de Panorama para Nutanix requiere Panorama 9.0.4 o una versión posterior.
- **SD-WAN**: la red de área amplia definida por software (Software-Defined Wide Area Network, SD-WAN) es un complemento que le permite utilizar varios servicios privados y de Internet para crear una WAN inteligente y dinámica, lo que ayuda a reducir los costes y a maximizar la calidad de la aplicación y el uso. SD-WAN en un cortafuegos de Palo Alto Networks le permite usar servicios de Internet más económicos y un número inferior de piezas de equipo en lugar de utilizar MPLS costosos y que precisan mucho tiempo con componentes como enrutadores, cortafuegos, controladores de ruta WAN y optimizadores WAN para conectar su red WAN a Internet.
- **VMware NSX:** el complemento VMware NSX permite la integración entre el cortafuegos VM-Series en VMware NSX con el gestor de VMware NSX. Esta integración le permite implementar el cortafuegos serie VM como un servicio en un clúster de servidores ESXi.
- **VMware vCenter**: el complemento de Panorama para VMware vCenter le permite supervisar las máquinas virtuales en su entorno de vCenter. El complemento recupera las direcciones IP de las máquinas virtuales en su entorno de vCenter y las convierte en etiquetas que puede usar para crear políticas mediante grupos de direcciones dinámicas.
- **Zero Touch Provisioning**: Zero Touch Provisioning (ZTP, aprovisionamiento táctil cero) se ha diseñado para simplificar y automatizar la inclusión de nuevos cortafuegos en Panorama. ZTP agiliza el proceso de implementación del cortafuegos inicial, ya que ofrece a los administradores de red la posibilidad de enviar cortafuegos gestionados directamente a sus sucursales y añadir automáticamente el cortafuegos a Panorama, lo que permite a las empresas ahorrar tiempo y

 ©2023 Palo Alto Networks, Inc.

recursos al implementar nuevos cortafuegos. ZTP es compatible con PAN-OS 9.1.3 y versiones posteriores.

No se admite en Panorama en modo FIPS-CC.

- **IPS Signature Converter (Convertidor de firmas IPS)**: el complemento IPS Signature Converter (Convertidor de firmas IPS) para Panorama proporciona una solución automatizada para convertir reglas de sistemas de prevención de intrusiones de terceros, Snort y Suricata, en firmas de amenazas de Palo Alto Networks personalizadas. Después, puede registrar estas firmas en los cortafuegos que pertenecen a los grupos de dispositivos que especifique y usarlos para aplicar la política en Vulnerability Protection (Protección contra vulnerabilidades) y Anti-Spyware Security Profiles (Perfiles de seguridad antispyware).

Puede instalar varios complementos y recuperar actualizaciones de direcciones IP de varios orígenes en una sola instancia de Panorama. Esto le permite crear y hacer cumplir una política de seguridad coherente para proteger las aplicaciones y cargas de trabajo en varios entornos en la nube. Las direcciones IP recuperadas se utilizan en la política de seguridad a través de grupos de direcciones dinámicas; cuando se añade o elimina una carga de trabajo de su entorno, Panorama registra el cambio y envía la actualización a los cortafuegos. Al implementar varios complementos en Panorama, debe planificar cuidadosamente su jerarquía de grupos de dispositivos para asegurarse de que las actualizaciones se pasen a sus cortafuegos correctamente.

Para obtener información sobre la compatibilidad y sobre las distintas versiones de los complementos, consulte la matriz de compatibilidad de Palo Alto Networks.

Instalación de los complementos de Panorama

Puede instalar uno o más complementos disponibles en Panorama para habilitar la integración en Cortex Data Lake y el servicio en la nube de GlobalProtect,VMware NSX o para supervisar sus máquinas virtuales en la nube pública de AWS o Azure.

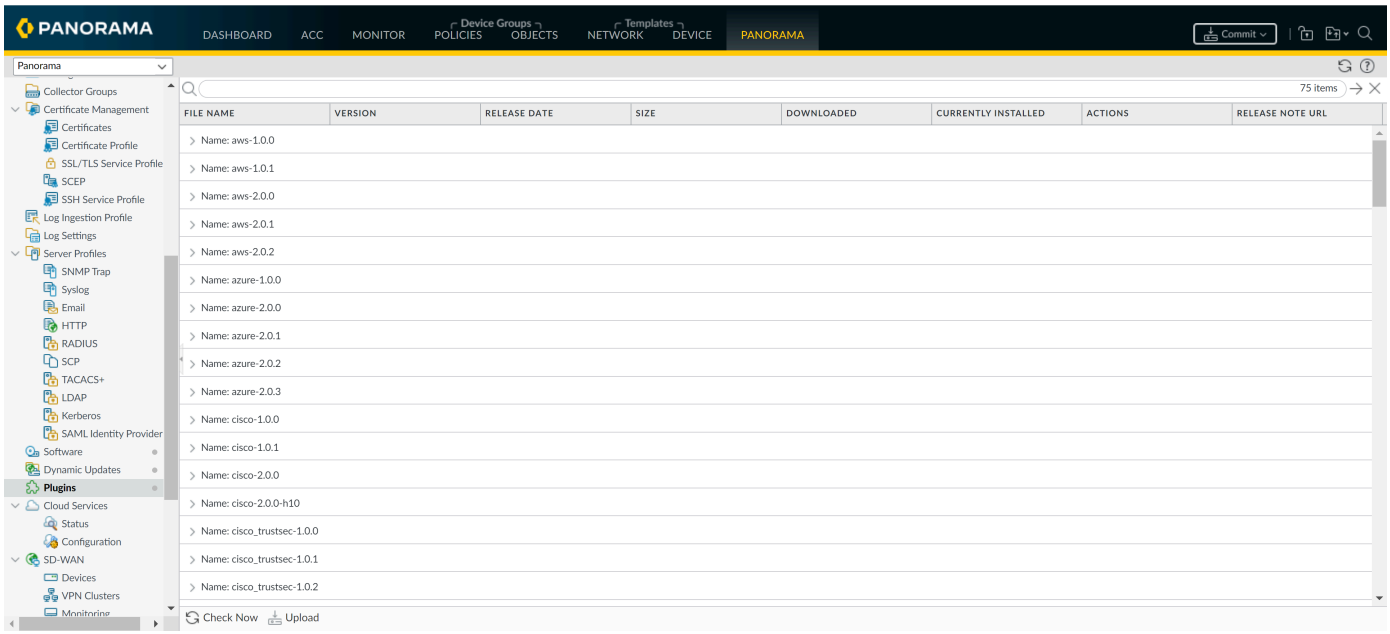
En el caso del complemento de los servicios en la nube, debe activar un código de autorización válido en el portal de atención al cliente y seleccionar la región (América o Europa) a la que desea enviar los logs.

*Si ya cuenta con una versión de complemento instalada e **instala** una nueva versión del complemento, Panorama sustituye la versión instalada actualmente.*

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Descargue el complemento.

1. Seleccione **Panorama** > **Plugins (Complementos)**



2. Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
3. Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

   Consulte la matriz de compatibilidad para conocer la versión mínima de PAN-OS admitida para cada complemento de Panorama.

STEP 2 | Instale el complemento.

Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación. Para obtener información detallada, consulte el material ofrecido para instalar el complemento VMware NSX o el complemento de servicios en la nube.

Al instalar el complemento por primera vez en un par de HA de Panorama, instale el complemento en el peer pasivo antes de hacerlo en el peer activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. Luego, después de instalar correctamente el complemento en el peer activo, el peer pasivo vuelve a un estado funcional.

©2023 Palo Alto Networks, Inc.

Complemento VM-Series y complementos de Panorama

¿Cuál es la diferencia entre el complemento de VM-Series y varios complementos para Panorama?

El complemento para VM-Series es para los cortafuegos VM-Series y es un complemento único que permite la integración con entornos de nube pública como Google Cloud Platform (GCP), Azure y AWS, e hipervisores de nube privados como KVM, ESXi y otros. Cuando implementa el cortafuegos, el complemento incorporado detecta automáticamente el entorno virtual en el que se implementa el cortafuegos y carga los componentes del complemento que le permiten gestionar las interacciones con ese entorno de nube. Por ejemplo, cuando implementa el cortafuegos VM-Series en GCP, el cortafuegos VM-Series carga los componentes del complemento que permiten la integración con GCP. Luego puede usar el complemento de VM-Series para configurar el cortafuegos VM-Series en GCP, para publicar métricas en la Supervisión de Google Stackdriver. Del mismo modo, el complemento de VM-Series en el cortafuegos VM-Series en Azure le permite configurar el cortafuegos para publicar métricas Azure Application Insights o configurar los detalles que los cortafuegos necesitan para funcionar como un par de HA. El complemento de VM-Series está preinstalado en el cortafuegos VM-Series, y puede actualizarlo o degradarlo, pero no puede eliminarlo. En Panorama, el complemento de VM-Series está disponible pero no está preinstalado. Si elige utilizar Panorama para gestionar las integraciones en sus cortafuegos, instale el complemento de VM-Series en Panorama para establecer comunicación con el complemento de VM-Series en sus cortafuegos.

Los complementos de Panorama son tanto para cortafuegos basados en hardware como para cortafuegos VM-Series. Dado que los complementos de Panorama son opcionales, puede añadirlos, eliminarlos, reinstalarlos o actualizarlos en Panorama. El complemento de Panorama no está integrado y debe instalar el complemento para permitir la comunicación con la gestión del entorno que necesita. Por ejemplo, utiliza el complemento de Servicios de nube en Panorama para habilitar la configuración entre Panorama/cortafuegos y Cortex Data Lake . El Complemento de GCP en Panorama permite la comunicación entre Panorama y su implementación de GCP para que pueda proteger el tráfico que entra o sale de un servicio implementado en un clúster de Google Kubernetes Engine (GKE).

Instalación del complemento VM-Series en Panorama

Para ver y configurar las integraciones en la nube implementadas en los cortafuegos VM-Series, es indispensable que el complemento VM-Series esté instalado tanto en ellos como en Panorama. El complemento se instala de forma automática en los cortafuegos, pero tiene que instalarlo manualmente en Panorama para poder enviar las configuraciones a los grupos de dispositivos.

Como el complemento VM-Series admite todas las nubes, quizá no tenga que actualizar los cortafuegos VM-Series. Antes de actualizar el complemento, consulte las notas de la versión. Actualícelo solo si aparecen cambios pertinentes para su nube.

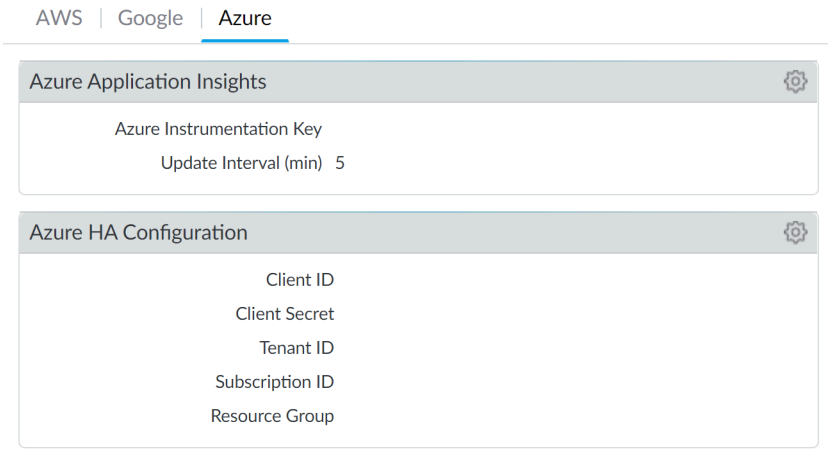
©2023 Palo Alto Networks, Inc.

STEP 1 | Descargue el complemento VM-Series.

1. Seleccione **Panorama** > **Plugins (Complementos)** y haga clic en **Check Now (Buscar ahora)** para buscar paquetes de complementos nuevos. El complemento VM-Series se llama `vm_series`.
2. Consulte las notas de las versiones del complemento para comprobar cuál aporta actualizaciones útiles para su caso.
3. Seleccione la versión apropiada del complemento y haga clic en **Download (Descargar)** en la columna Action (Acción).

STEP 2 | Instale el complemento VM-Series.

1. Haga clic en **Install (Instalar)** en la columna Action (Acción). Panorama muestra un aviso cuando termina la instalación.
2. Para ver el complemento, seleccione **Device (Dispositivo)** > **VM-Series**.
   - Si el cortafuegos está instalado en una nube privada y el hipervisor o el servicio carecen de integración, aparece la pestaña VM-Series y el mensaje predetemrinado `VM Series plugin infrastructure support is installed to allow the firewall's functionality to be enhanced in response to new features launched by hypervisor, or to meet new security needs (Se admite la infraestructura del complemento VM-Series para mejorar la funcionalidad del cortafuegos con respecto a las nuevas funciones que inicia el hipervisor o en respuesta a nuevas necesidades de seguridad)`.
   - Si el cortafuegos está implementado en una nube pública, Panorama muestra pestañas para todas las nubes admitidas.



STEP 3 | (Opcional) Guarde la configuración y envíela a los cortafuegos gestionados.

STEP 4 | (Opcional) En el cortafuegos VM-Series, seleccione **Device (Dispositivo)** > **VM-Series**. Si ha configurado la integración en la plataforma, aparece una sola pestaña para la nube donde está instalado el cortafuegos; si no lo ha hecho, se muestra el mensaje antes indicado sobre la infraestructura.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Solución de problemas

Los siguientes temas abordan problemas para el servidor de gestión de Panorama™ y los recopiladores de logs dedicados:

- Solución de problemas del sistema Panorama
- Solución de problemas de almacenamiento de logs y conexión
- Sustitución de un cortafuegos con una autorización de devolución de mercancía
- Solución de problemas de fallos de compilación
- Solución de problemas de errores de registro o números de serie
- Solución de problemas de errores de creación de informes
- Solución de problemas de errores de licencia de gestión de dispositivos
- Solución de problemas de las configuraciones del cortafuegos revertidas automáticamente
- Visualización de tareas que se realizaron correctamente o tienen errores
- Pruebas de coincidencia con políticas y conectividad de dispositivos gestionados
- Cómo generar un archivo de volcado de estadísticas para un cortafuegos gestionado
- Cómo recuperar la conectividad a Panorama en dispositivos gestionados

Solución de problemas del sistema Panorama

- Generación de archivos de diagnóstico para Panorama
- Diagnóstico de estado suspendido de Panorama
- Supervisión de la comprobación de integridad del sistema de archivos
- Gestión de almacenamiento de Panorama para actualizaciones de software y contenido
- Recuperación del síndrome de cerebro dividido en implementaciones HA de Panorama

Generación de archivos de diagnóstico para Panorama

Los archivos de diagnóstico facilitan la supervisión de la actividad del sistema y a detectar posibles problemas en Panorama. Para ayudar a los miembros del equipo de asistencia técnica de Palo Alto Networks a solucionar problemas, el representante podría pedirle un archivo de asistencia técnica. El siguiente procedimiento describe cómo descargar un archivo de asistencia técnica y cómo cargarlo en su caso de asistencia.

STEP 1 | Seleccione **Panorama** > **Support (Asistencia técnica)** y haga clic en **Generate Tech Support File (Generar archivo de asistencia técnica)**.

STEP 2 | Descargue y guarde el archivo en el ordenador.

STEP 3 | Cargue el archivo en su caso en el sitio web de Atención al cliente de Palo Alto Networks.

Diagnóstico de estado suspendido de Panorama

Si Panorama está en un estado suspendido, compruebe lo siguiente:

- **Números de serie**: compruebe que el número de serie de cada dispositivo virtual Panorama es único. Si se utiliza el mismo número de serie para crear dos o más instancias de Panorama, se suspenderán todas las instancias que utilicen el mismo número de serie.
- **Modo**: si implementa el dispositivo virtual Panorama en una configuración de alta disponibilidad (HA), verifique que ambos HA peers estén en el mismo modo: Modo Panorama o modo heredado.
- **Prioridad de HA**: compruebe que ha establecido el ajuste de prioridad de HA en un peer como ***principal*** y el otro como ***secundario***. Si el ajuste de prioridad es idéntico en ambos peers, el peer de Panorama con el número de serie más alto pasará al estado de suspensión.
- **Versión de software de Panorama**: compruebe que ambos peers de HA de Panorama estén ejecutando la misma versión de software (número de versión mayor y menor).

Supervisión de la comprobación de integridad del sistema de archivos

Panorama ejecuta periódicamente una comprobación de integridad del sistema de archivos (file system integrity check, FSCK) para evitar daños en el sistema de archivos de Panorama. Esta comprobación se realiza cada 8 reinicios o tras un reinicio 90 días después de realizar la última comprobación de integridad del sistema de archivos (FSCK). Si Panorama ejecuta una FSCK, la interfaz web y las pantallas de inicio de sesión de shell seguro (Secure Shell, SSH) mostrarán una advertencia que indica que se está llevando a cabo una FSCK. No puede iniciar la sesión hasta que

 ©2023 Palo Alto Networks, Inc.

no finalice este proceso. El tiempo necesario para completar el proceso depende del tamaño del sistema de almacenamiento; dependiendo del tamaño, puede tardar varias horas en poder iniciar sesión en Panorama.

Después de descargar e instalar correctamente una actualización de software PAN-OS en Panorama o un cortafuegos gestionado, la actualización de software se valida después de que Panorama o el cortafuegos gestionado se reinicie como parte del proceso de instalación del software para garantizar la integridad del software PAN-OS. Esto garantiza que la nueva actualización de software en ejecución sea buena y que Panorama o el cortafuegos gestionado no se vean comprometidos debido a la explotación remota o física.

Para ver el progreso de la FSCK, configure el acceso de la consola a Panorama y consulte el estado.

Gestión de almacenamiento de Panorama para actualizaciones de software y contenido

Puede instalar actualizaciones de contenido y software para Panorama, actualizar los cortafuegos y actualizar los recopiladores de logs mediante el servidor de gestión Panorama™. No puede configurar la cantidad de espacio disponible en Panorama para almacenar actualizaciones. Cuando la capacidad de almacenamiento asignada alcance el 90%, Panorama le avisará para que libere espacio (eliminando actualizaciones almacenadas) para nuevas descargas o cargas. El número máximo de actualizaciones es un ajuste global que se aplica a todas las actualizaciones que almacena Panorama. Debe acceder a la CLI para configurar este ajuste. El valor predeterminado es de dos actualizaciones de cada tipo.

- Modifique del número máximo de actualizaciones de cada tipo.

  Acceda a la CLI de Panorama e introduzca lo siguiente, donde ***<number>*** puede ser un valor entre 2 y 64:

  ```
  > set max-num-images count <number>
  ```

- Visualice el número de actualizaciones que Panorama almacena actualmente.

  Introduzca:

  ```
  > show max-num-images
  ```

 ©2023 Palo Alto Networks, Inc.

- Use la interfaz web para eliminar actualizaciones y liberar espacio en Panorama.
  1. Seleccione el tipo de actualización que desea eliminar:
     - Actualizaciones de cortafuegos o recopilador de logs:

       Imágenes de software de PAN-OS/Panorama: seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **Software**.

       Actualizaciones de software de agente/aplicación de GlobalProtect™: seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **GlobalProtect Client (Cliente GlobalProtect)**.

       Actualizaciones de contenido: seleccione **Panorama** > **Device Deployment (Implementación del dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**.
     - Imágenes de software de Panorama: seleccione **Panorama** > **Software**.
     - Actualizaciones de contenido de Panorama: seleccione **Panorama** > **Dynamic Updates (Actualizaciones dinámicas)**.
  2. Haga clic en el icono de la **X** en la columna del extremo derecho de la imagen o actualización.

- Use la CLI para eliminar actualizaciones y liberar espacio en Panorama.

  Elimine imágenes de software por versión:

  ```
  > delete software version <version_number>
  ```

  Elimine actualizaciones de contenido:

  ```
  > delete content update <filename>
  ```

Recuperación del síndrome de cerebro dividido en implementaciones HA de Panorama

Cuando Panorama está configurado en un entorno de alta disponibilidad (HA), los cortafuegos gestionados se conectan a los peers HA activo y pasivo de Panorama. Cuando falla la conexión entre los peers activo y pasivo de Panorama, antes de que el Panorama pasivo tome el control como peer activo, comprueba si hay algún cortafuegos conectado a los peers activo y pasivo. Si hay aunque sea un único cortafuegos conectado a ambos peers, la recuperación no se activa.

En el raro caso de que se active una recuperación cuando un conjunto de cortafuegos está conectado al peer activo y un conjunto de cortafuegos está conectado al peer pasivo, pero ninguno de los cortafuegos está conectado a ambos peers, se denomina división "split brain". Cuando se produce esta división, se producen las siguientes anomalías:

- Ninguno de los peers de Panorama es consciente del estado ni de la función de HA del otro peer.
- Ambos peers de Panorama quedan activos y gestionan un conjunto exclusivo de cortafuegos.

Para resolver una división, depure los problemas de red y restaure la conectividad entre los peers HA de Panorama.

 ©2023 Palo Alto Networks, Inc.

Sin embargo, si tiene que realizar cambios de configuración en sus cortafuegos sin restaurar la conexión entre los peers, existen un par de opciones:

- Añada manualmente los mismos cambios de configuración en ambos peers de Panorama. Esta acción garantiza que cuando el enlace se restablezca, la configuración quedará sincronizada.
- Si tiene que añadir o cambiar la configuración en una única ubicación de Panorama, realice los cambios y sincronice la configuración (asegúrese de que inicia la sincronización desde el peer en el que realizó los cambios) cuando el enlace entre los peers de Panorama quede restablecido. Para sincronizar los peers, seleccione la pestaña **Dashboard (Panel)** y haga clic en el enlace **Sync to peer (Sincronizar con peer)** del widget de Alta disponibilidad.
- Si solamente necesita añadir/cambiar la configuración de los cortafuegos conectados en cada ubicación, puede realizar los cambios de configuración independientemente en cada peer de Panorama. Ya que los peers están desconectados, no hay replicación y cada peer tiene ahora un archivo de configuración completamente diferente (no están sincronizados). Por lo tanto, para garantizar que no se pierden los cambios realizados en la configuración de cada peer cuando se restablezca la conexión, no puede permitir que se vuelva a sincronizar la configuración automáticamente. Para resolver este problema, exporte la configuración de cada peer de Panorama y fusione manualmente los cambios utilizando una herramienta de diferenciación y fusión externa. Tras integrar los cambios, puede importar el archivo de configuración unificado en el Panorama principal y luego sincronice el archivo de configuración importado con los peer.

 ©2023 Palo Alto Networks, Inc.

Solución de problemas de almacenamiento de logs y conexión

> ***La migración de logs solo es compatible con el dispositivo M-Series. Consulte*** Migración de dispositivos virtuales Panorama a otro hipervisor ***para migrar un dispositivo virtual Panorama.***

- Verificación de la utilización del puerto de Panorama
- Resolución de almacenamiento cero de logs para un grupo de recopiladores
- Sustitución de un disco con fallos en un dispositivo de la serie M
- Sustitución del disco virtual en un servidor ESXi
- Sustitución del disco virtual en vCloud Air
- Migración de logs a un nuevo dispositivo serie M en modo de recopilación de logs
- Migración de logs a un nuevo dispositivo de la serie M en modo Panorama
- Migración de logs a un nuevo modelo de dispositivo serie M en modo Panorama con alta disponibilidad
- Migración de logs al mismo modelo de dispositivo serie M en modo Panorama con alta disponibilidad
- Migración de recopiladores de logs después de un error o RMA de un Panorama que no es de HA
- Regeneración de metadatos para pares de RAID para un dispositivo serie M
- Visualización de trabajos de consulta de logs

Verificación de la utilización del puerto de Panorama

Para asegurarse de que Panorama puede comunicarse con cortafuegos gestionados, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire y su peer de alta disponibilidad (HA), utilice la tabla siguiente para verificar los puertos que debe abrir en su red. Panorama usa el protocolo TCP para las comunicaciones de puertos.

De forma predeterminada, Panorama utiliza la interfaz de gestión (MGT) para gestionar dispositivos (cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire), recopilar logs, comunicarse con grupos de recopiladores e implementar actualizaciones de software y de contenido para dispositivos. Sin embargo, puede asignar opcionalmente la recopilación de logs y las funciones de comunicación del grupo de recopiladores a las interfaces Eth1 o Eth2 en un dispositivo M-700, M-600, M-500, M-300 o M-200 que ejecute Panorama 300 hasta 200. Si el dispositivo ejecuta Panorama 8.0 o una versión posterior, puede asignar cualquier función a las interfaces Eth1, Eth2, Eth3, Eth4 o Eth5 en el dispositivo M-700, M-600, M-500, M-300 o M-200. Los puertos enumerados en la tabla siguiente se aplican independientemente de las funciones que asigne a las interfaces. Por ejemplo, si asigna la recopilación de logs a la interfaz MGT y asigna la comunicación de grupos de recopiladores a la interfaz Eth2, entonces MGT utilizará el puerto 3978 y Eth2 utilizará el puerto 28270. (El dispositivo virtual Panorama solamente puede utilizar la interfaz MGT para todas estas funciones.)

 ©2023 Palo Alto Networks, Inc.

Sistemas de comunicación y dirección de establecimiento de la conexión	Puertos usados en Panorama 5.x	Puertos usados en Panorama 6.x a 7.x	Puertos usados en Panorama 8.x y versiones posteriores	Description (Descripción)
Panorama y Panorama (HA) Dirección: Cada peer inicia su propia conexión con el otro	28	28	28	Para conectividad de HA y sincronización si está activado el cifrado. Se usa para la comunicación entre recopiladores de logs en un grupo de recopiladores para la distribución de logs.
Panorama y Panorama (HA) Dirección: Cada peer inicia su propia conexión con el otro	28769 y 28260 (5.1) 28769 and 49160 (5.0)	28260 y 28769	28260 y 28769	Para conectividad de HA y sincronización si no está activado el cifrado.
Panorama y cortafuegos gestionados Dirección: Iniciado por el cortafuegos	3978	3978	3978	Una conexión bidireccional en la que los logs se reenvían desde el cortafuegos a Panorama; los cambios de configuración se aplican desde Panorama a los cortafuegos gestionados. Los comandos de cambio de contexto se envían a través de la misma conexión.
Panorama y recopilador de logs Dirección: Iniciado por el recopilador de logs	3978	3978	3978	Para gestión y recopilación de logs/creación de informes. Se utiliza para la comunicación entre el recopilador de logs local en un Panorama en modo Panorama, así como para comunicarse con recopiladores de logs en una implementación

©2023 Palo Alto Networks, Inc.

Sistemas de comunicación y dirección de establecimiento de la conexión	Puertos usados en Panorama 5.x	Puertos usados en Panorama 6.x a 7.x	Puertos usados en Panorama 8.x y versiones posteriores	Description (Descripción)
				de recopilación de logs distribuida.
Panorama y dispositivos gestionados (cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire) Dirección: • Iniciado por dispositivos gestionados que ejecutan PAN-OS 8.x o versiones posteriores. • Iniciado por Panorama para dispositivos que ejecutan PAN-OS 7.x o versiones posteriores.	3978	3978	28443	Los dispositivos que ejecutan versiones de PAN-OS 8.x o versiones posteriores utilizan el puerto 28443 para recuperar software y archivos de actualización de contenido y software de Panorama. Los dispositivos que ejecutan 7.x o versiones anteriores no recuperan archivos de actualización de Panorama; Panorama envía los archivos de actualización a los dispositivos a través del puerto 3978. La compatibilidad para la gestión de Panorama de los clústeres de dispositivos y dispositivos de WildFire requiere la instalación de PAN-OS 8.0.1 o versiones posteriores en los dispositivos WildFire gestionados. Recomendamos que Panorama ejecute 8.0.1 o posterior para gestionar los dispositivos y clústeres de dispositivos de WildFire.
Recopilador de logs a recopilador de logs Dirección: Cada recopilador de logs inicia una conexión con el resto de los	49190	28270	28270	Para la distribución de bloques y todos los datos binarios entre recopiladores de logs.

©2023 Palo Alto Networks, Inc.

Sistemas de comunicación y dirección de establecimiento de la conexión	Puertos usados en Panorama 5.x	Puertos usados en Panorama 6.x a 7.x	Puertos usados en Panorama 8.x y versiones posteriores	Description (Descripción)
recopiladores de logs en el grupo de recopiladores				
De Panorama a Cortex Data Lake	N/A	N/A	444 *Versión 8.0.5 y posterior*	Para configurar un canal de comunicación seguro con Cortex Data Lake. Los cortafuegos gestionados utilizan el puerto 3978 para comunicarse con Cortex Data Lake.

Resolución de almacenamiento cero de logs para un grupo de recopiladores

La capacidad de almacenamiento de logs del grupo de recopiladores podría indicar 0 MB si los pares de discos no están habilitados para los logs en los recopiladores de logs. Para habilitar los pares de discos, realice los siguientes pasos para cada recopilador de logs en el grupo de recopiladores.

STEP 1 | Añada los pares de discos RAID.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y haga clic en Nombre del recopilador.
2. Seleccione **Disks (Discos)**, seleccione **Add (Añadir)** cada par de discos RAID y haga clic en **OK (aceptar)**.

STEP 2 | Confirme los cambios realizados a Panorama y envíe los cambios al grupo de recopiladores.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Collector Groups (Grupos de recopiladores)**, seleccione el grupo de recopiladores que ha modificado y haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Verifique el estado de los recopiladores de logs y los pares de discos.

1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para verificar que la configuración de cada recopilador de logs se sincronizó con Panorama.

   La columna Configuration Status (Estado de configuración) debe mostrar **In Sync (Sincronización)** y la columna Run Time Status (Estado de tiempo de ejecución), **connected (conectado)**.
2. Haga clic en **Statistics (Estadísticas)** en la última columna de cada recopilador de logs y verifique que los pares de discos indiquen **Enabled (Habilitado)** y **Available (Disponible)**.

Sustitución de un disco con fallos en un dispositivo de la serie M

Si falla un disco en el dispositivo de la serie M, debe sustituir el disco y volver a configurarlo en un conjunto de RAID 1. Para obtener más detalles, consulte las Guías de referencia de hardware serie M.

Sustitución del disco virtual en un servidor ESXi

No puede cambiar el tamaño de un disco virtual después de añadirlo a un dispositivo virtual Panorama que se ejecuta en el servidor ESXi de VMware. Debido a que el dispositivo virtual Panorama en modo heredado solo permite una ubicación de almacenamiento de logs, debe reemplazar el disco virtual para modificar la capacidad de almacenamiento de logs de la siguiente forma. En el modo Panorama, puede simplemente añadir otro disco (hasta un máximo de 12) a Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual Panorama.

En el dispositivo virtual Panorama en modo heredado, perderá los logs del disco existente cuando lo reemplace. Para conocer las opciones para conservar los registros existentes, consulte Conserve logs existentes al añadir almacenamiento en el dispositivo virtual Panorama en modo heredado**.**

STEP 1 | Quite el disco virtual anterior.

1. Acceda al cliente VMware vSphere y seleccione la pestaña **Virtual Machines (Máquinas virtuales)**.
2. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power Off (Apagar)**.
3. Haga clic derecho en el dispositivo virtual Panorama y seleccione **Edit Settings (Editar ajustes)**.
4. Seleccione el disco virtual en la pestaña **Hardware** y haga clic en **Remove (Eliminar)**.
5. Seleccione una de las Opciones de eliminación y haga clic en **OK (Aceptar)**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Añada el disco virtual nuevo.

1. Cómo añadir un disco virtual a Panorama en un servidor ESXi.

   La instancia de Panorama que se ejecuta en ESXi 5.5 o una versión posterior admite un disco virtual de hasta 8 TB. La instancia de Panorama que se ejecuta en una versión anterior de ESXi admite un disco virtual de hasta 2 TB.
2. En el cliente vSphere, haga clic derecho en el dispositivo virtual Panorama y seleccione **Power (Encendido/Apagado)** > **Power On (Encender)**.

   El proceso de reinicio podría tardar unos minutos. Asimismo, aparecerá el mensaje `cache data unavailable`.

STEP 3 | Verifique que la capacidad modificada de almacenamiento de logs sea la correcta.

1. Inicie sesión en el dispositivo virtual Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y verifique que la sección Configuración de log e informes, campo Almacenamiento de logs, muestra de forma precisa la capacidad de almacenamiento de logs modificada.

Sustitución del disco virtual en vCloud Air

No puede cambiar el tamaño de un disco virtual después de añadirlo a un dispositivo virtual Panorama que se ejecuta en vCloud Air de VMware. Debido a que el dispositivo virtual Panorama en modo heredado solo permite una ubicación de almacenamiento de logs, debe reemplazar el disco virtual para modificar la capacidad de almacenamiento de logs de la siguiente forma. En el modo Panorama, puede simplemente Cómo añadir un disco virtual a Panorama en vCloud Air (hasta un máximo de 12).

En el dispositivo virtual Panorama en modo heredado, perderá los logs del disco existente cuando lo reemplace. Para conocer las opciones para conservar los registros existentes, consulte Conserve logs existentes al añadir almacenamiento en el dispositivo virtual Panorama en modo heredado**.**

STEP 1 | Quite el disco virtual anterior.

1. Acceda a la consola web de vCloud Air y seleccione su región de **Virtual Private Cloud OnDemand (Nube privada virtual a petición)**.
2. Seleccione el dispositivo virtual Panorama en la pestaña **Virtual Machines (Máquinas virtuales)**.
3. Seleccione **Actions (Acciones)** > **Edit Resources (Editar recursos)**.
4. Haga clic en **x** para el disco virtual que esté quitando.

STEP 2 | Añada el disco virtual nuevo.

1. Haga clic en **Add another disk (Añadir otro disco)**.
2. Configure **Storage (Almacenamiento)** en 8 TB y especifique la capa de almacenamiento **Standard (Estándar)** o **SSD-Accelerated (Acelerado por SSD)**.
3. Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Reinicie Panorama.

1. Inicie sesión en el dispositivo virtual Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Reboot Panorama (Reiniciar Panorama)**.

STEP 4 | Verifique que la capacidad modificada de almacenamiento de logs sea la correcta.

1. Inicie sesión en el dispositivo virtual Panorama después de que se reinicie.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y verifique que la sección Configuración de log e informes, campo Almacenamiento de logs, muestra de forma precisa la capacidad de almacenamiento de logs modificada.

Migración de logs a un nuevo dispositivo serie M en modo de recopilación de logs

Si necesita reemplazar un dispositivo M-700, M-600, M-500, M-300, M-200 o M-100 en modo de recopilador de logs (recopilador de logs dedicado), puede migrar los logs que recopiló desde los cortafuegos moviendo sus discos RAID a un nuevo dispositivo serie M. Este procedimiento le permite recuperar logs después de un fallo del sistema en el dispositivo M-Series o migrar logs como parte de una actualización de hardware (de un dispositivo M-100 a uno M-500).

No es posible migrar logs mediante la eliminación de discos de creación de logs de un dispositivo M-Series y la carga de estos en un servidor de gestión Panorama M-600. Para migrar a un dispositivo M-600, configure el dispositivo M-600, configure el reenvío de logs al nuevo dispositivo M-600 y establezca el dispositivo M-Series como recopilador de logs gestionado hasta que no necesite acceso a los logs almacenados en el dispositivo M-Series.

STEP 1 | Lleve a cabo la configuración inicial del nuevo dispositivo de la serie M que será un recopilador de logs dedicado.

1. Monte en rack el dispositivo de la serie M. Consulte las Guías de referencia de hardware del dispositivo serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.

   Cuando configure las interfaces, configure solo la interfaz de gestión (Management, MGT). Si cambia al modo de recopilador de logs más adelante en este procedimiento, se eliminan las configuraciones de cualquier otra interfaz. Si el recopilador de logs va a utilizar otras interfaces aparte de la MGT, añádalas cuando lo configure (consulte el paso 2).
3. Registre Panorama.
4. Compre y active la licencia de asistencia técnica de Panorama o transfiera las licencias de la siguiente manera solamente si el nuevo dispositivo M-Series es del mismo modelo de hardware que el dispositivo M-Series anterior. Si el nuevo dispositivo M-Series es un modelo diferente al antiguo dispositivo M-Series, debe comprar nuevas licencias.
   1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
   2. Seleccione la pestaña **Assets (Activos)** y haga clic en el enlace **Spares (Repuestos)**.
   3. Haga clic en el número de serie del dispositivo nuevo de la serie M.

 ©2023 Palo Alto Networks, Inc.

4. Haga clic en **Transfer Licenses (Transferir licencias)**.
5. Haga clic en **Select (Seleccionar)** para elegir el dispositivo anterior de la serie M y, luego, haga clic en **Submit (Enviar)**.

5. Active una licencia de gestión de cortafuegos. Si migra de un dispositivo M-100 a un dispositivo M-500, introduzca el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
7. Cambie del modo Panorama al modo de recopilación de logs:
   1. Acceda a la CLI del recopilador de logs y cambie al modo de recopilación de logs:

      ```
      > request system system-mode logger
      ```

   2. Ingrese **Y** para confirmar el cambio de modo. El dispositivo de la serie M se reiniciará. Si el proceso de reinicio finaliza la sesión de software de emulación de terminal, vuelva a conectar el dispositivo de la serie M para que se muestre la solicitud de inicio de sesión a Panorama.

      *Si ve la solicitud **CMS Login**, pulse Intro sin introducir ningún nombre de usuario ni contraseña.*
8. Use la CLI del recopilador de logs para habilitar la conectividad entre el recopilador de logs y el servidor de gestión de Panorama. <IPaddress1 is for the MGT interface of the primary Panorama and <IPaddress2> es para la interfaz MGT del Panorama secundario.

```
> configure # set deviceconfig system panorama-
server <IPaddress1> panorama-server-2 <IPaddress2> # commit
 # exit
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | En el servidor de gestión de Panorama, añada el nuevo recopilador de logs como un recopilador gestionado.

Para todos los pasos con comandos que requieran un número de serie, debe introducir el número de serie completo; pulsar la tecla Tab no completará un número de serie parcial.

1. Configure el recopilador de logs como un recopilador gestionado mediante la interfaz web de Panorama o mediante los siguientes comandos de la CLI:

```
> configure # set log-collector <LC_serial_number>
 deviceconfig system hostname <LC_hostname> # exit
```

*Si el recopilador de logs anterior utilizaba interfaces diferentes a la interfaz MGT para la recopilación de logs y la comunicación del grupo de recopiladores, deberá definir esas interfaces en el nuevo recopilador de logs cuando lo configure como recopilador gestionado (**Panorama** > **Managed Collectors [Recopiladores gestionados]** > **Interfaces [Interfaces]**).*

2. Verifique que el recopilador de logs esté conectado a Panorama y que el estado de sus pares de discos sea presente o disponible.

```
> show log-collector serial-number <log-collector_SN>
```

Los pares de discos se mostrarán como desactivados en esta etapa del proceso de restauración.

3. Compile los cambios realizados en Panorama. No compile los cambios en el grupo de recopiladores aún.

```
> configure # commit # exit
```

STEP 3 | Retire los discos RAID del recopilador de logs anterior.

1. Apague el recopilador de logs anterior presionando el botón de encendido hasta que el sistema se apague.
2. Retire los pares de discos. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Prepare los discos para la migración.

La generación de metadatos para cada par de discos reconstruye los índices. Por lo tanto, dependiendo del tamaño de los datos, este proceso puede tardar mucho tiempo en realizarse. Para acelerar el proceso, puede iniciar múltiples sesiones CLI y ejecutar el comando de regeneración de metadatos en cada sesión para completar el proceso simultáneamente para cada par. Para obtener más detalles, consulte Regeneración de metadatos para pares de RAID de un dispositivo de la serie M.

1. Inserte los discos en el nuevo recopilador de logs. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

   Los portadores de disco del dispositivo M-100 no son compatibles con aquellos del dispositivo M-500. Por lo tanto, cuando se realiza una migración entre estos modelos de hardware, debe desatornillar cada disco de su portador anterior e insertarlo en el nuevo portador antes de insertar el disco en el nuevo dispositivo.

   Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 del dispositivo anterior en la ranura B1/B2 del dispositivo nuevo, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.
2. Habilite los pares de discos ejecutando el siguiente comando de la CLI para cada par:

   ```
   > request system raid add <slot> force no-format
   ```

   Por ejemplo:

   ```
   > request system raid add A1 force no-format > request system
    raid add A2 force no-format
   ```

   Los argumentos **force** y **no-format** son obligatorios. El argumento **force** asocia el par de discos con el nuevo recopilador de logs. El argumento **no-format** evita la aplicación de formato de las unidades y mantiene almacenados los logs en los discos.
3. Genere los metadatos para cada par de discos.

   ```
   > request metadata-regenerate slot <slot_number>
   ```

   Por ejemplo:

   ```
   > request metadata-regenerate slot 1
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Añada un recopilador de logs sin discos a un grupo de recopiladores.

Desde este punto, solo las confirmaciones que son necesarios para completar el proceso de migración en Panorama y los recopiladores de logs. No realice ningún otro cambio.

1. Acceda a la CLI de Panorama.
2. Sobrescriba la restricción de Panorama para permitir que el recopilador de logs sin disco se añada a un grupo de recopiladores: **request log-migration-set-start**

STEP 6 | Migre los logs.

Debe usar la CLI de Panorama para este paso, no la interfaz web.

Debe asignar el nuevo recopilador de logs al grupo de recopiladores que contiene el recopilador de logs anterior.

1. Asigne el nuevo recopilador de logs al grupo de recopiladores y compile sus cambios en Panorama.

```
> configure # set log-collector-group <collector_group_name>
 logfwd-setting collectors <new_LC_serial_number> # commit
 # exit
```

2. Para cada par de discos, migre los logs del recopilador de logs anterior y adjunte el par de discos al nuevo recopilador de logs.

```
> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

Por ejemplo:

```
> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

STEP 7 | Vuelva a configurar el grupo de recopiladores.

1. Utilice la interfaz de usuario para asignar el nuevo recopilador de logs a los cortafuegos que reenvían logs (**Panorama** > **Collector Groups (Grupos de recopiladores)** > **Device Log**

 ©2023 Palo Alto Networks, Inc.

Forwarding (Reenvío de logs del dispositivo)). Conceda al recopilador de logs la misma prioridad en las listas de preferencia del cortafuegos que el recopilador de logs anterior.

No puede usar la CLI para cambiar las asignaciones de prioridad de las listas de preferencia del cortafuegos.

2. Elimine el recopilador de logs anterior del grupo de recopiladores.

```
> configure # delete log-collector-group <group_name> logfwd-
setting collectors <old_LC_serial_number>
```

Por ejemplo:

```
# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

3. Elimine el Recopilador de logs anterior de la configuración de Panorama y compile sus cambios en Panorama.

```
# delete log-collector <old_LC_serial_number> # commit # exit
```

4. Compile los cambios del grupo de recopiladores de modo que los cortafuegos gestionados puedan enviar logs al nuevo recopilador de logs.

```
> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Por ejemplo:

```
> commit-all log-collector-config log-collector-group DC-
Collector-Group
```

STEP 8 | Genere nuevas claves en el nuevo recopilador de logs dedicado.

Este comando es necesario para añadir el nuevo recopilador de logs al grupo de recopiladores y solo debe ejecutarse para el grupo de recopiladores del recopilador de logs que se está reemplazando. Este paso elimina las claves RSA existentes y permite que Panorama cree nuevas claves RSA.

1. Acceda a la CLI de Panorama.
2. Elimine todas las claves RSA en el nuevo recopilador de logs:

```
request logdb update-collector-group-after-replace collector-
group <collector-group-name>
```

El proceso puede tomar hasta 10 minutos para completarse.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Confirme que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores.

No continúe hasta que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores. Esto dará como resultado la purga de los logs del recopilador de logs que se está sustituyendo.

1. Acceda a la CLI de Panorama.
2. Muestre los detalles del recopilador de logs ejecutando los siguientes comandos en:
   - Panorama para todos los recopiladores de logs:

     show log-collector all

     Alternativamente, puede ejecutar el siguiente comando en cada recopilador de logs dedicado:

     ```
     show log-collector detail
     ```
3. Confirme que el estado de SearchEngine es activo.

```
Estado de redistribución: ninguno
```

```
Última compilación de todo: compilación exitosa, versión
 actual del anillo 1
```

```
Estado de SearchEngine: Activo
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 actualizado en
 2017/06/14 09:58:19
```

STEP 10 | En el nuevo recopilador de logs, reemplace el número de serie del recopilador de logs anterior con el número de serie del nuevo recopilador de logs.

Debe reemplazar el antiguo número de serie del recopilador de logs con el número de serie del nuevo recopilador de logs para que el nuevo recopilador de logs no se ejecute para purgar problemas, lo que evitaría que el recopilador de logs pueda purgar los datos antiguos de los logs migrados cuando sea necesario.

1. Acceda a la CLI del recopilador de logs.
2. Reemplace el número de serie de recopilador de logs antiguo con el número de serie de nuevo recopilador de logs:

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

 ©2023 Palo Alto Networks, Inc.

Migración de logs a un nuevo dispositivo de la serie M en modo Panorama

Si necesita reemplazar un dispositivo M-700, M-600, M-500, M-300, M-200 o M-100 en modo Panorama (servidor de gestión de Panorama), puede migrar los logs que recopiló desde los cortafuegos moviendo sus discos RAID a un nuevo dispositivo serie M. Mover los discos le permite recuperar logs después de un fallo del sistema en el dispositivo M-Series o migrar logs como parte de una actualización de hardware (desde un dispositivo M-100 a uno M-500).

No es posible migrar logs mediante la eliminación de discos de creación de logs de un dispositivo M-Series y la carga de estos en un servidor de gestión Panorama M-600. Para migrar a un dispositivo M-600, configure el dispositivo M-600, configure el reenvío de logs al nuevo dispositivo M-600 y establezca el dispositivo M-Series como recopilador de logs gestionado hasta que no necesite acceso a los logs almacenados en el dispositivo M-Series.

La migración abarca las siguientes situaciones donde reemplaza un dispositivo serie M, que no se encuentra en una configuración de HA, con un recopilador gestionado (recopilador de logs) en un grupo de recopiladores.

STEP 1 | Reenvíe los logs que están en el SSD del dispositivo anterior de la serie M a un destino externo si desea conservarlos.

El SSD almacena los logs de sistema y configuración que Panorama y los recopiladores de logs generan. No puede mover el SSD entre dispositivos de la serie M.

Configuración del reenvío de logs desde Panorama a destinos externos.

STEP 2 | Exporte la configuración de Panorama de cada dispositivo serie M fuera de servicio en modo Panorama.

1. Inicie sesión en el dispositivo Panorama y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.

STEP 3 | Retire los discos RAID del dispositivo anterior de la serie M.

1. Apague el dispositivo anterior de la serie M presionando el botón de encendido hasta que el sistema se apague.
2. Retire los pares de discos. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Lleve a cabo la configuración inicial del nuevo dispositivo de la serie M.

1. Monte en rack el dispositivo de la serie M. Consulte las Guías de referencia de hardware del dispositivo serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.
3. Registre Panorama.
4. Compre y active una licencia de asistencia técnica de Panorama o transfiera las licencias de la siguiente manera solamente si el nuevo dispositivo serie M es del mismo modelo de hardware que el dispositivo serie M anterior. Si el nuevo dispositivo M-Series es un modelo diferente al antiguo dispositivo M-Series, debe comprar nuevas licencias.
   1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
   2. Seleccione la pestaña **Assets (Activos)** y haga clic en el enlace **Spares (Repuestos)**.
   3. Haga clic en el número de serie del dispositivo nuevo de la serie M.
   4. Haga clic en **Transfer Licenses (Transferir licencias)**.
   5. Haga clic en **Select (Seleccionar)** para elegir el dispositivo anterior de la serie M y, luego, haga clic en **Submit (Enviar)**.
5. Active una licencia de gestión de cortafuegos. Si migra de un dispositivo M-100 a un dispositivo M-500, introduzca el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.

STEP 5 | Cargue la instantánea de configuración de Panorama que exportó desde el dispositivo serie M fuera de servicio al nuevo dispositivo serie M en modo Panorama.

1. Inicio de sesión en la interfaz web de Panorama del nuevo dispositivo serie M y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, en **Browse (Examinar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo serie V fuera de servicio y haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, seleccione una **Decryption Key (Clave de descifrado)** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.



*Si desea sustituir una instancia de Panorama con una autorización para la devolución de bienes (return merchandise authorization, RMA), no olvide marcar **Retain Rule UUIDs (Conservar UUID de reglas)** cuando cargue la instantánea de la configuración con nombre de Panorama. Si no lo hace, Panorama elimina todos los UUID anteriores de la instantánea de configuración y asigna UUID nuevos a las reglas en Panorama. Eso implica que no se conserva la información asociada a los antiguos UUID, por ejemplo, el recuento de resultados de las reglas de las políticas.*

 ©2023 Palo Alto Networks, Inc.

4. Realice todos los demás cambios en la configuración que sean necesarios.

   *Si el anterior dispositivo M-Series utilizaba otras interfaces aparte de la MGT para los servicios de Panorama (como la recopilación de logs), debe definir esas interfaces en el nuevo dispositivo M-Series (**Panorama** > **Setup [Configuración]** > **Interfaces [Interfaces]**).*

5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Validate Commit (Validar confirmación)**. Resuelva cualquier error antes de continuar.
6. Seleccione **Commit (Confirmar)** los cambios en la configuración de Panorama.

STEP 6 | Inserte los discos en el nuevo dispositivo de la serie M. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

Los portadores de disco del dispositivo M-100 no son compatibles con aquellos del dispositivo M-500. Por lo tanto, cuando se realiza una migración entre estos modelos de hardware, debe desatornillar cada disco de su portador anterior e insertarlo en el nuevo portador antes de insertar el disco en el nuevo dispositivo.

Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 del dispositivo anterior en la ranura B1/B2 del dispositivo nuevo, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.

STEP 7 | Póngase en contacto con el servicio de Atención al cliente de Palo Alto Networks para copiar los metadatos del grupo de recopiladores de logs desde el dispositivo serie M fuera de servicio al nuevo dispositivo serie M y reiniciar el proceso mgmtsrvr.

STEP 8 | Si el dispositivo M-Series formaba parte de un grupo de recopiladores, verifique que el número de serie del dispositivo M-Series fuera de servicio todavía sea parte del grupo de recopiladores correcto:

```
debug log-collector-group show name <Log Collector Group name>
```

Si el número de serie del dispositivo serie M fuera de servicio ya no forma parte del grupo de recopiladores correcto, las carpetas de soporte técnico se copiaron incorrectamente en el paso anterior. Póngase en contacto con Asistencia al cliente de Palo Alto Networks nuevamente para copiar las carpetas de soporte técnico a la ubicación correcta.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Prepare los discos para la migración.

La generación de metadatos para cada par de discos reconstruye los índices. Por lo tanto, dependiendo del tamaño de los datos, este proceso puede tardar mucho tiempo en realizarse. Para acelerar el proceso, puede iniciar múltiples sesiones CLI y ejecutar el comando de regeneración de metadatos en cada sesión para completar el proceso simultáneamente para cada par. Para obtener más detalles, consulte Regeneración de metadatos para pares de RAID de un dispositivo de la serie M.

1. Inserte los discos en el nuevo dispositivo de la serie M. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

   Los portadores de disco del dispositivo M-100 no son compatibles con aquellos del dispositivo M-500. Por lo tanto, cuando se realiza una migración entre estos modelos de hardware, debe desatornillar cada disco de su portador anterior e insertarlo en el nuevo portador antes de insertar el disco en el nuevo dispositivo.

   Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 del dispositivo anterior en la ranura B1/B2 del dispositivo nuevo, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.
2. Habilite los pares de discos ejecutando el siguiente comando de la CLI para cada par:

```
admin> request system raid add <slot> force no-format
```

   Por ejemplo:

```
admin> request system raid add A1 force no-format
 admin> request system raid add A2 force no-format
```

   Los argumentos **force** y **no-format** son obligatorios. El argumento **force** asocia el par de discos con el nuevo dispositivo. El argumento **no-format** evita la aplicación de formato de las unidades y mantiene almacenados los logs en los discos.
3. Genere los metadatos para cada par de discos.

   Este proceso puede tardar hasta 6 horas, en función del volumen de los datos del log en los discos.

```
admin> request metadata-regenerate slot <slot_number>
```

   Por ejemplo:

```
admin> request metadata-regenerate slot 1
```

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Configure el recopilador de logs local en el nuevo dispositivo de la serie M.

> ***Para todos los pasos con comandos que requieran un número de serie, debe introducir el número de serie completo; pulsar la tecla Tab no completará un número de serie parcial.***

No habilite los discos en el nuevo dispositivo de la serie M en este punto. Cuando migre correctamente los logs, Panorama habilitará los discos de manera automática.

1. Configure el recopilador de logs local como un recopilador gestionado mediante la interfaz web de Panorama o mediante los siguientes comandos de la CLI:

   ```
   admin> configure admin# set log-collector <log-collector_SN>
    deviceconfig system hostname <log-collector-hostname>
    admin# exit
   ```

2. Verifique que el recopilador de logs local esté conectado a Panorama y que el estado de sus pares de discos sea presente o disponible.

   ```
   admin> show log-collector serial-number <log-collector_SN>
   ```

   Los pares de discos se mostrarán como desactivados en esta etapa del proceso de restauración.

3. Compile los cambios realizados en Panorama. No compile los cambios en el grupo de recopiladores aún.

   ```
   admin> configure admin# commit
   ```

STEP 11 | Añada un recopilador de logs sin discos a un grupo de recopiladores.

> ***Desde este punto, solo las confirmaciones que son necesarios para completar el proceso de migración en Panorama y los recopiladores de logs. No realice ningún otro cambio.***

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Sobrescriba la restricción de Panorama para permitir que el recopilador de logs sin disco se añada a un grupo de recopiladores: **request log-migration-set-start**
3. Confirme la restricción sobrescrita:

   ```
   admin> configure admin# commit force
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Migre los logs.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Añada el nuevo recopilador de logs local como miembro del grupo de recopiladores y compile sus cambios en Panorama.

```
admin# set log-collector-group <collector_group_name> logfwd-
setting collectors <SN_managed_collector> admin# commit
 admin# exit
```

   El recopilador de logs local anterior seguirá apareciendo en la lista de miembros, ya que todavía no lo ha eliminado de la configuración.
3. Para cada par de discos, migre los logs al nuevo dispositivo.

```
admin> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

   Por ejemplo:

```
admin> request log-migration from 003001000010 old-disk-pair A
 to 00300100038 new-disk-pair A
```

4. Compile los cambios realizados en Panorama.

```
admin> configure admin# commit
```

STEP 13 | Vuelva a configurar el grupo de recopiladores.

1. Inicio de sesión en la interfaz web de Panorama del nuevo dispositivo M-Series para asignar el nuevo recopilador de logs a los cortafuegos que reenvían logs (**Panorama** > **Collector Groups [Grupos de recopiladores]** > **Device Log Forwarding [Reenvío de logs del dispositivo]**). Conceda al recopilador de logs la misma prioridad en las listas de preferencia del cortafuegos que el recopilador de logs anterior.

   No puede usar la CLI para cambiar las asignaciones de prioridad de las listas de preferencia del cortafuegos.
2. Acceda a la CLI de Panorama del nuevo dispositivo serie M.

 ©2023 Palo Alto Networks, Inc.

3. Elimine el recopilador de logs anterior del grupo de recopiladores.

```
admin# delete log-collector-group <group_name> logfwd-setting
 collectors <old_LC_serial_number>
```

Por ejemplo:

```
admin# delete log-collector-group DC-Collector-Group logfwd-
setting collectors 003001000010
```

4. Elimine el Recopilador de logs anterior de la configuración de Panorama y compile sus cambios en Panorama.

```
admin# delete log-collector <old_LC_serial_number>
 admin# commit admin# exit
```

5. Compile los cambios del grupo de recopiladores de modo que los cortafuegos gestionados puedan enviar logs al nuevo recopilador de logs.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Por ejemplo:

```
admin> commit-all log-collector-config log-collector-group DC-
Collector-Group
```

STEP 14 | Genere nuevas claves en el nuevo recopilador de logs.

Este comando es necesario para añadir el nuevo recopilador de logs al grupo de recopiladores y solo debe ejecutarse para el grupo de recopiladores del recopilador de logs que se está reemplazando. Este paso elimina las claves RSA existentes y permite que Panorama cree nuevas claves RSA.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Elimine todas las claves RSA en el nuevo recopilador de logs:

   request logdb update-collector-group-after-replace collector-group <collector-group-name>

   El proceso puede tomar hasta 10 minutos para completarse.

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Confirme que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores.

No continúe hasta que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores. Esto dará como resultado la purga de los logs del recopilador de logs que se está sustituyendo.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Muestre los detalles del recopilador de logs ejecutando los siguientes comandos en:
   - Panorama para todos los recopiladores de logs:

     show log-collector all

     Alternativamente, puede ejecutar el siguiente comando en cada recopilador de logs dedicado:

     ```
     show log-collector detail
     ```
3. Confirme que el estado de SearchEngine es activo.

```
Estado de redistribución: ninguno
```

```
Última compilación de todo: compilación exitosa, versión
 actual del anillo 1
```

```
Estado de SearchEngine: Activo
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 actualizado en
 2017/06/14 09:58:19
```

STEP 16 | En el nuevo recopilador de logs, reemplace el número de serie del recopilador de logs anterior con el número de serie del nuevo recopilador de logs.

Debe reemplazar el antiguo número de serie del recopilador de logs con el número de serie del nuevo recopilador de logs para que el nuevo recopilador de logs no se ejecute para purgar problemas, lo que evitaría que el recopilador de logs pueda purgar los datos antiguos de los logs migrados cuando sea necesario.

1. Acceda a la CLI del recopilador de logs.
2. Reemplace el número de serie de recopilador de logs antiguo con el número de serie de nuevo recopilador de logs:

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

 ©2023 Palo Alto Networks, Inc.

Migración de logs a un nuevo modelo de dispositivo serie M en modo Panorama con alta disponibilidad

Si necesita reemplazar un dispositivo M-700, M-600, M-500, M-300, M-200 o M-100 en modo Panorama (servidores de gestión de Panorama) con un dispositivo serie M diferente al dispositivo serie M que se reemplaza, puede migrar los logs que recopiló desde los cortafuegos moviendo sus discos RAID a un nuevo dispositivo serie M. Mover los discos le permite migrar los logs como parte de una actualización de hardware (de un dispositivo M-100 a uno M-500). Puede migrar un dispositivo M-100 a un dispositivo M-500 y desde él. Los dispositivos M-100 y M-500 no se pueden migrar a o desde dispositivos M-200 o M-600.

No es posible migrar logs mediante la eliminación de discos de creación de logs de un dispositivo M-Series y la carga de estos en un servidor de gestión Panorama M-600. Para migrar a un dispositivo M-600, configure el dispositivo M-600, configure el reenvío de logs al nuevo dispositivo M-600 ***y*** establezca el dispositivo M-Series como recopilador de logs gestionado ***hasta que no necesite acceso a los logs almacenados en el dispositivo M-Series.***

Este procedimiento de migración abarca los siguientes escenarios:

- Un peer de HA de Panorama tiene un recopilador gestionado (recopilador de logs) en un grupo de recopiladores.

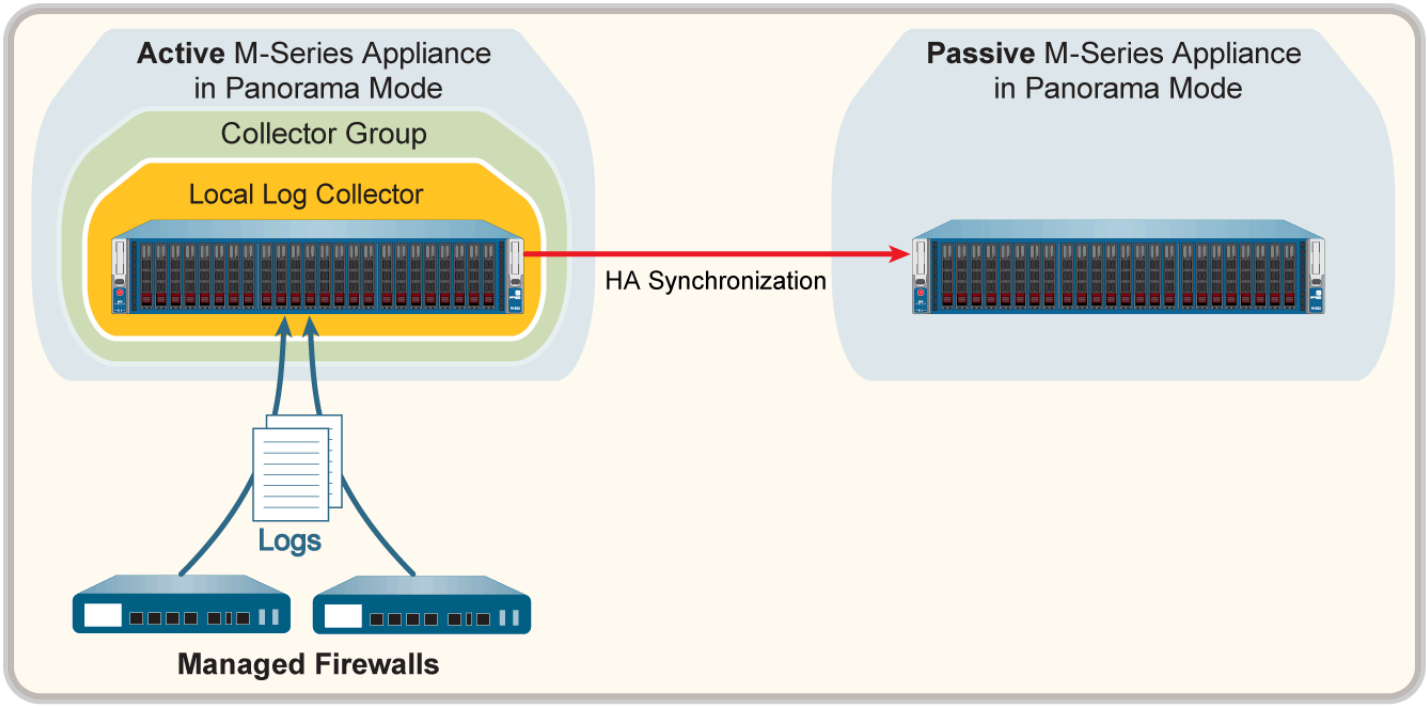


Figure 28: Peer HA de Panorama con grupo de recopiladores

- Ambos peers de HA de Panorama tienen recopiladores gestionados que pertenecen a un único grupo de recopiladores. Para obtener más detalles, consulte Varios recopiladores de logs locales por grupo de recopiladores.

©2023 Palo Alto Networks, Inc.

- Ambos peers de HA de Panorama tienen un recopilador gestionado y cada uno de ellos está asignado a un grupo de recopiladores diferente. Para obtener más detalles, consulte Recopilador de logs local único por grupo de recopiladores.

STEP 1 | Reenvíe los logs que están en el SSD del dispositivo anterior de la serie M a un destino externo si desea conservarlos.

El SSD almacena los logs de sistema y configuración que Panorama y los recopiladores de logs generan. No puede mover el SSD entre dispositivos de la serie M.

Configuración del reenvío de logs desde Panorama a destinos externos.

STEP 2 | Exporte la configuración de Panorama de cada dispositivo serie M principal fuera de servicio en modo Panorama.

1. Inicio de sesión en la interfaz web de Panorama del dispositivo serie M que reemplaza y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Save named Panorama configuration snapshot (Guardar instantánea de configuración de Panorama con nombre)**, ingrese un nombre en **Name (Nombre)** para identificar la configuración y haga clic en **OK (Aceptar)**.
3. Haga clic en **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**, seleccione el nombre de la configuración que acaba de guardar en **Name (Nombre)** y haga clic en **OK (Aceptar)**. Panorama exporta la configuración a su sistema de cliente como un archivo XML.

STEP 3 | Retire los discos RAID del dispositivo anterior de la serie M.

1. Apague el dispositivo anterior de la serie M presionando el botón de encendido hasta que el sistema se apague.
2. Retire los pares de discos. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

STEP 4 | Lleve a cabo la configuración inicial del nuevo dispositivo de la serie M.

Repita este paso en cada uno de los nuevos dispositivos serie M en la configuración de HA.

1. Monte en rack el dispositivo de la serie M. Consulte las Guías de referencia de hardware del dispositivo serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.
3. Registre Panorama.
4. Compre y active una licencia de asistencia técnica de Panorama o transfiera las licencias de la siguiente manera solamente si el nuevo dispositivo serie M es del mismo modelo de hardware que el dispositivo serie M anterior. Si el nuevo dispositivo M-Series es un modelo diferente al antiguo dispositivo M-Series, debe comprar nuevas licencias.
   1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
   2. Seleccione la pestaña **Assets (Activos)** y haga clic en el enlace **Spares (Repuestos)**.
   3. Haga clic en el número de serie del dispositivo nuevo de la serie M.
   4. Haga clic en **Transfer Licenses (Transferir licencias)**.

 ©2023 Palo Alto Networks, Inc.

5. Haga clic en **Select (Seleccionar)** para elegir el dispositivo anterior de la serie M y, luego, haga clic en **Submit (Enviar)**.

5. Active una licencia de gestión de cortafuegos. Si migra de un dispositivo M-100 a un dispositivo M-500, introduzca el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
7. Configuración de HA en Panorama. El nuevo dispositivo de la serie M debe tener la misma prioridad que el peer de HA que sustituya.

STEP 5 | Cargue la instantánea de configuración de Panorama que exportó desde el dispositivo serie M principal fuera de servicio al nuevo dispositivo serie M principal en modo Panorama.

1. Inicio de sesión en la interfaz web de Panorama del nuevo dispositivo serie M y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, en **Browse (Examinar)** para ir al archivo de configuración de Panorama que exportó desde el dispositivo serie V fuera de servicio y haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named Panorama configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el nombre de la configuración que acaba de importar en **Name (Nombre)**, seleccione una **Decryption Key (Clave de descifrado)** (la clave maestra de Panorama) y haga clic en **OK (Aceptar)**. Panorama sobrescribe su configuración candidata actual con la configuración cargada. Panorama muestra cualquier error que se produzca al cargar el archivo de configuración. Si hubiera errores, guárdelos en un archivo local. Resuelva cada error para garantizar que la configuración migrada es válida.

   *Si desea sustituir una instancia de Panorama con una autorización para la devolución de bienes (return merchandise authorization, RMA), no olvide marcar **Retain Rule UUIDs (Conservar UUID de reglas)** cuando cargue la instantánea de la configuración con nombre de Panorama. Si no lo hace, Panorama elimina todos los UUID anteriores de la instantánea de configuración y asigna UUID nuevos a las reglas en Panorama. Eso implica que no se conserva la información asociada a los antiguos UUID, por ejemplo, el recuento de resultados de las reglas de las políticas.*
4. Realice todos los demás cambios en la configuración que sean necesarios.

   *Si el anterior dispositivo M-Series utilizaba otras interfaces aparte de la MGT para los servicios de Panorama (como la recopilación de logs), debe definir esas interfaces en el nuevo dispositivo M-Series (**Panorama** > **Setup [Configuración]** > **Interfaces [Interfaces]**).*
5. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Validate Commit (Validar confirmación)**. Resuelva cualquier error antes de continuar.
6. Seleccione **Commit (Confirmar)** los cambios en la configuración de Panorama. Después de la confirmación, la configuración de Panorama se sincroniza en los peers de HA.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Inserte los discos en el nuevo dispositivo de la serie M. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

Repita este paso en cada uno de los nuevos dispositivos serie M en la configuración de HA.

> ***Los portadores de disco del dispositivo M-100 no son compatibles con aquellos del dispositivo M-500. Por lo tanto, cuando se realiza una migración entre estos modelos de hardware, debe desatornillar cada disco de su portador anterior e insertarlo en el nuevo portador antes de insertar el disco en el nuevo dispositivo.***

Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 del dispositivo anterior en la ranura B1/B2 del dispositivo nuevo, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.

STEP 7 | Póngase en contacto con el servicio de Atención al cliente de Palo Alto Networks para copiar los metadatos del grupo de recopiladores de logs desde el dispositivo serie M fuera de servicio al nuevo dispositivo serie M y reiniciar el proceso mgmtsrvr.

STEP 8 | Si el dispositivo M-Series formaba parte de un grupo de recopiladores, verifique que el número de serie del dispositivo M-Series fuera de servicio todavía sea parte del grupo de recopiladores correcto:

```
debug log-collector-group show name <Log CollectorGroup name>
```

Si el número de serie del dispositivo serie M fuera de servicio ya no forma parte del grupo de recopiladores correcto, las carpetas de soporte técnico se copiaron incorrectamente en el paso anterior. Póngase en contacto con Asistencia al cliente de Palo Alto Networks nuevamente para copiar las carpetas de soporte técnico a la ubicación correcta.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Prepare los discos para la migración.

La generación de metadatos para cada par de discos reconstruye los índices. Por lo tanto, dependiendo del tamaño de los datos, este proceso puede tardar mucho tiempo en realizarse. Para acelerar el proceso, puede iniciar múltiples sesiones CLI y ejecutar el comando de regeneración de metadatos en cada sesión para completar el proceso simultáneamente para cada par. Para obtener más detalles, consulte Regeneración de metadatos para pares de RAID de un dispositivo de la serie M.

1. Habilite los pares de discos ejecutando el siguiente comando de la CLI para cada par:

```
admin> request system raid add <slot> force no-format
```

   Por ejemplo:

```
admin> request system raid add A1 force no-format
 admin> request system raid add A2 force no-format
```

   Los argumentos **force** y **no-format** son obligatorios. El argumento **force** asocia el par de discos con el nuevo dispositivo. El argumento **no-format** evita la aplicación de formato de las unidades y mantiene almacenados los logs en los discos.
2. Genere los metadatos para cada par de discos.

   Este proceso puede tardar hasta 6 horas, en función del volumen de los datos del log en los discos.

```
admin> request metadata-regenerate slot <slot_number>
```

   Por ejemplo:

```
admin> request metadata-regenerate slot 1
```

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Configure el recopilador de logs local en el nuevo dispositivo de la serie M.

> ***Para todos los pasos con comandos que requieran un número de serie, debe introducir el número de serie completo; pulsar la tecla Tab no completará un número de serie parcial.***

No habilite los discos en el nuevo dispositivo de la serie M en este punto. Cuando migre correctamente los logs, Panorama habilitará los discos de manera automática.

1. Configure el recopilador de logs local como un recopilador gestionado mediante la interfaz web de Panorama o mediante los siguientes comandos de la CLI:

```
admin> configure admin# set log-collector <log-collector_SN>
 deviceconfig system hostname <log-collector-hostname>
 admin# exit
```

2. Compile los cambios realizados en Panorama. No compile los cambios en el grupo de recopiladores aún.

```
admin> configure admin# commit
```

3. Verifique que el recopilador de logs local esté conectado a Panorama y que el estado de sus pares de discos sea presente o disponible.

```
admin> show log-collector serial-number <log-collector_SN>
```

   Los pares de discos se mostrarán como desactivados en esta etapa del proceso de restauración.

STEP 11 | Añada un recopilador de logs sin discos a un grupo de recopiladores.

> ***Desde este punto, solo las confirmaciones que son necesarios para completar el proceso de migración en Panorama y los recopiladores de logs. No realice ningún otro cambio.***

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Sobrescriba la restricción de Panorama para permitir que el recopilador de logs sin disco se añada a un grupo de recopiladores: **requestlog-migration-set-start**
3. Compile los cambios realizados en Panorama.

```
admin> configure admin# commit force
```

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Migre los logs.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Añada el nuevo recopilador de logs local como miembro del grupo de recopiladores y compile sus cambios en Panorama.

```
admin# set log-collector-group <collector_group_name> logfwd-
setting collectors <SN_managed_collector> admin# commit
 admin# exit
```

   El recopilador de logs local anterior seguirá apareciendo en la lista de miembros, ya que todavía no lo ha eliminado de la configuración.
3. Para cada par de discos, migre los logs al nuevo dispositivo.

```
admin> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

   Por ejemplo:

```
admin> request log-migration from 003001000010 old-disk-pair A
 to 00300100038 new-disk-pair A
```

4. Compile los cambios realizados en Panorama.

```
admin> configure admin# commit
```

STEP 13 | Vuelva a configurar el grupo de recopiladores.

1. Inicio de sesión en la interfaz web de Panorama del nuevo dispositivo serie M para asignar el nuevo recopilador de logs a los cortafuegos que reenvían logs (**Panorama** > **Collector Groups [Grupos de recopiladores]** > **Device Log Forwarding [Reenvío de logs del dispositivo]**). Conceda al recopilador de logs la misma prioridad en las listas de preferencia del cortafuegos que el recopilador de logs anterior.

   No puede usar la CLI para cambiar las asignaciones de prioridad de las listas de preferencia del cortafuegos.
2. Acceda a la CLI de Panorama del nuevo dispositivo serie M.

 ©2023 Palo Alto Networks, Inc.

3. Elimine el recopilador de logs anterior del grupo de recopiladores.

```
admin# delete log-collector-group <group_name> logfwd-setting
 collectors <old_LC_serial_number>
```

Por ejemplo:

```
admin# delete log-collector-group DC-Collector-Group logfwd-
setting collectors 003001000010
```

4. Elimine el Recopilador de logs anterior de la configuración de Panorama y compile sus cambios en Panorama.

```
admin# delete log-collector <old_LC_serial_number>
 admin# commit admin# exit
```

5. Compile los cambios del grupo de recopiladores de modo que los cortafuegos gestionados puedan enviar logs al nuevo recopilador de logs.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Por ejemplo:

```
admin> commit-all log-collector-config log-collector-group DC-
Collector-Group
```

STEP 14 | Genere nuevas claves en el nuevo recopilador de logs.

Este comando es necesario para añadir el nuevo recopilador de logs al grupo de recopiladores y solo debe ejecutarse para el grupo de recopiladores del recopilador de logs que se está reemplazando. Este paso elimina las claves RSA existentes y permite que Panorama cree nuevas claves RSA.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Elimine todas las claves RSA en el nuevo recopilador de logs:

```
request logdb update-collector-group-after-replacecollector-
group <collector-group-name>
```

El proceso puede tomar hasta 10 minutos para completarse.

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Confirme que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores.

No continúe hasta que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores. Esto dará como resultado la purga de los logs del recopilador de logs que se está sustituyendo.

1. Acceda a la CLI de Panorama del nuevo dispositivo serie M.
2. Muestre los detalles del recopilador de logs ejecutando los siguientes comandos en:
   - Panorama para todos los recopiladores de logs:

     show log-collector all

     Alternativamente, puede ejecutar el siguiente comando en cada recopilador de logs dedicado:

     ```
     show log-collector detail
     ```
3. Confirme que el estado de SearchEngine es activo.

```
Estado de redistribución: ninguno
```

```
Última compilación de todo: compilación exitosa, versión
 actual del anillo 1
```

```
Estado de SearchEngine: Activo
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 actualizado en
 2017/06/14 09:58:19
```

STEP 16 | En el nuevo recopilador de logs, reemplace el número de serie del recopilador de logs anterior con el número de serie del nuevo recopilador de logs.

Debe reemplazar el antiguo número de serie del recopilador de logs con el número de serie del nuevo recopilador de logs para que el nuevo recopilador de logs no se ejecute para purgar problemas, lo que evitaría que el recopilador de logs pueda purgar los datos antiguos de los logs migrados cuando sea necesario.

1. Acceda a la CLI del recopilador de logs.
2. Reemplace el número de serie de recopilador de logs antiguo con el número de serie de nuevo recopilador de logs:

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

 ©2023 Palo Alto Networks, Inc.

STEP 17 | Configure el nuevo peer de alta disponibilidad secundario de Panorama.

1. Reenvíe los logs que están en el disco SSD del dispositivo M-Series anterior a un destino externo si desea conservarlos.
2. Extraiga los discos RAID del dispositivo M-Series anterior.
3. Ejecute la configuración inicial del dispositivo M-Series nuevo.
4. Inserte los discos en el dispositivo M-Series nuevo.
5. Repita los pasos 7 a 16 para migrar los logs desde el dispositivo serie M anterior al nuevo dispositivo serie M.
6. Configuración de HA en Panorama. El nuevo dispositivo de la serie M debe tener la misma prioridad que el peer de HA que sustituya.
7. Inicio de sesión en la interfaz web de Panorama del peer de HA principal y haga clic en **Dashboard (Panel)** > **High Availability (Alta disponibilidad)** > **Sync to peer (Sincronizar con peer)** para sincronizar la configuración de los peers de HA del dispositivo serie M.

Migración de logs al mismo modelo de dispositivo serie M en modo Panorama con alta disponibilidad

Si necesita reemplazar un dispositivo M-700, M-600, M-500, M-300, M-200 o M-100 implementado en alta disponibilidad (HA) en modo Panorama (servidores de gestión de Panorama) con el mismo dispositivo serie M que el dispositivo serie M que se reemplaza, puede migrar los logs que recopiló desde los cortafuegos moviendo sus discos RAID a un nuevo dispositivo serie M. Migrar los discos le permite recuperar los logs tras una falla del sistema en el dispositivo serie M.

Este procedimiento de migración abarca los siguientes escenarios:

- Un peer de HA de Panorama tiene un recopilador gestionado (recopilador de logs) en un grupo de recopiladores.

 ©2023 Palo Alto Networks, Inc.

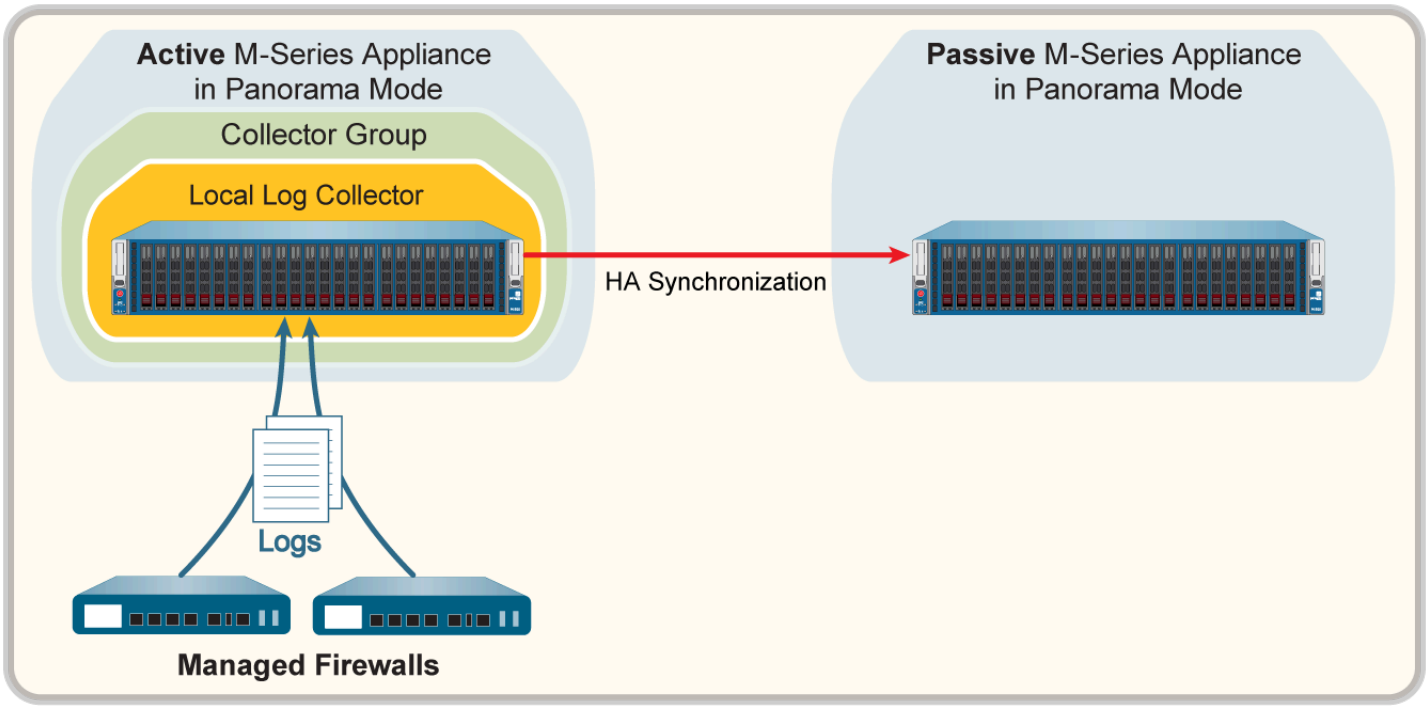


Figure 29: Peer HA de Panorama con grupo de recopiladores

- Ambos peers de HA de Panorama tienen recopiladores gestionados que pertenecen a un único grupo de recopiladores. Para obtener más detalles, consulte Varios recopiladores de logs locales por grupo de recopiladores.
- Ambos peers de HA de Panorama tienen un recopilador gestionado y cada uno de ellos está asignado a un grupo de recopiladores diferente. Para obtener más detalles, consulte Recopilador de logs local único por grupo de recopiladores.

STEP 1 | Reenvíe los logs que están en el SSD del dispositivo anterior de la serie M a un destino externo si desea conservarlos.

El SSD almacena los logs de sistema y configuración que Panorama y los recopiladores de logs generan. No puede mover el SSD entre dispositivos de la serie M.

Configuración del reenvío de logs desde Panorama a destinos externos.

STEP 2 | (RMA del peer de HA principal activo solamente) Reconfigure la configuración de alta disponibilidad de los peers de HA de Panorama para hacer que el peer de HA `secundario` sea el peer de HA `principal` durante el proceso de RMA.

Este paso es necesario si está reemplazando el peer de HA `principal` en una configuración de HA A/P para ayudar a garantizar que el estado de restablecimiento de comunicación segura y la entidad de certificación (CA) del nuevo dispositivo M-Series no se sincronicen involuntariamente con el peer existente en la configuración de HA. Al reemplazar el peer de HA `principal`, la reconfiguración de los ajustes de elección de alta disponibilidad garantiza que la administración de dispositivos de Panorama permanezca ininterrumpida durante el proceso de RMA.

Omita este paso si está reemplazando el peer de HA `secundario` en una configuración de HA A/P.

1. Inicio de sesión en la interfaz web de Panorama del peer de HA `principal`.

 ©2023 Palo Alto Networks, Inc.

2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección Election Settings (Ajustes de elección).
3. Para Priority (Prioridad), seleccione **secondary (secundario)** y haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.
   El par de HA de Panorama que está reemplazando ahora es el par de HA `secundario`.
5. Inicio de sesión en la interfaz web de Panorama del peer de HA `secundario`.
6. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección Election Settings (Ajustes de elección).
7. Para Priority (Prioridad), seleccione **primary (principal)** y haga clic en **OK (Aceptar)**.
8. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.
   El Panorama `secundario` anterior ahora es el peer de HA `principal`.

STEP 3 | Suspenda la funcionalidad de HA en el peer de HA de Panorama que está reemplazando.

Este paso es necesario para ayudar a garantizar que el estado de restablecimiento de comunicación segura y la entidad de certificación (CA) del nuevo dispositivo M-Series no se sincronicen involuntariamente con el peer existente en la configuración de HA durante el proceso de RMA. Esto pone al peer de HA de Panorama en un estado `suspendido`.

1. Inicio de sesión en la interfaz web de Panorama del peer de HA de Panorama que está reemplazando.
2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y **Suspend local Panorama (Suspender Panorama local) para alta disponibilidad**.
3. Haga clic en **OK (Aceptar)** para confirmar la suspensión de HA en el peer de HA de Panorama.

STEP 4 | Restablezca la configuración de conexión segura en el peer de HA de Panorama que está reemplazando.

1. Inicio de sesión en la CLI de Panorama del peer de HA de Panorama que está reemplazando.
2. Restablezca el estado de conexión segura.

   Este comando restablece todas las conexiones de dispositivos administrados y es irreversible.

   ```
   admin> request sc3 reset
   ```

3. Reinicie el servidor de gestión en el peer de HA de Panorama que está reemplazando.

   ```
   admin> debug software restart process management-server
   ```

STEP 5 | Retire los discos RAID del dispositivo anterior de la serie M.

1. Apague el dispositivo anterior de la serie M presionando el botón de encendido hasta que el sistema se apague.
2. Retire los pares de discos. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Lleve a cabo la configuración inicial del nuevo dispositivo de la serie M.

1. Monte en rack el dispositivo de la serie M. Consulte las Guías de referencia de hardware del dispositivo serie M para obtener instrucciones.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M.

   *Si el dispositivo serie M anterior utilizaba interfaces diferentes a la interfaz de MGT para los servicios de Panorama (como la recopilación de logs), debe definir estas interfaces durante la configuración inicial del nuevo dispositivo serie M (**Panorama** > **Setup [Configuración]** > **Interfaces [Interfaces]**).*
3. Registre Panorama.
4. Compre y active una licencia de asistencia técnica de Panorama o transfiera las licencias de la siguiente manera solamente si el nuevo dispositivo serie M es del mismo modelo de hardware que el dispositivo serie M anterior. Si el nuevo dispositivo M-Series es un modelo diferente al antiguo dispositivo M-Series, debe comprar nuevas licencias.
   1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
   2. Seleccione la pestaña **Assets (Activos)** y haga clic en el enlace **Spares (Repuestos)**.
   3. Haga clic en el número de serie del dispositivo nuevo de la serie M.
   4. Haga clic en **Transfer Licenses (Transferir licencias)**.
   5. Haga clic en **Select (Seleccionar)** para elegir el dispositivo anterior de la serie M y, luego, haga clic en **Submit (Enviar)**.
5. Active una licencia de gestión de cortafuegos. Si migra de un dispositivo M-100 a un dispositivo M-500, introduzca el código de autorización asociado con la licencia de migración.
6. Instale las actualizaciones de contenido y software de Panorama. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire.
7. Realice todos los demás cambios en la configuración que sean necesarios.

   *Si el anterior dispositivo M-Series utilizaba otras interfaces aparte de la MGT para los servicios de Panorama (como la recopilación de logs), debe definir esas interfaces en el nuevo dispositivo M-Series (**Panorama** > **Setup [Configuración]** > **Interfaces [Interfaces]**).*
8. Configuración de HA en Panorama. El nuevo dispositivo de la serie M debe tener la misma prioridad que el peer de HA que sustituya.

   El nuevo dispositivo M-Series debe añadirse a la configuración de HA como peer de HA `secundario`. La adición de la nueva M-Series como peer de HA `principal` fuerza la sincronización del estado de configuración de restablecimiento de comunicación segura con el dispositivo M-Series existente, lo que da como resultado la interrupción de la gestión de dispositivos de Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Inserte los discos en el nuevo dispositivo de la serie M. Para obtener más detalles, consulte el procedimiento de sustitución de discos en las Guías de referencia de hardware del dispositivo serie M.

> ***Los portadores de disco del dispositivo M-100 no son compatibles con aquellos del dispositivo M-500. Por lo tanto, cuando se realiza una migración entre estos modelos de hardware, debe desatornillar cada disco de su portador anterior e insertarlo en el nuevo portador antes de insertar el disco en el nuevo dispositivo.***

Debe mantener la asociación de pares de discos. A pesar de que puede colocar un par de discos de la ranura A1/A2 del dispositivo anterior en la ranura B1/B2 del dispositivo nuevo, debe mantener los discos juntos en la misma ranura; de lo contrario, es posible que Panorama no restaure los datos correctamente.

STEP 8 | Si el dispositivo M-Series formaba parte de un grupo de recopiladores, verifique que el número de serie del dispositivo M-Series fuera de servicio todavía sea parte del grupo de recopiladores correcto:

```
debug log-collector-group show name <Log CollectorGroup name>
```

STEP 9 | Prepare los discos para la migración.

> ***La generación de metadatos para cada par de discos reconstruye los índices. Por lo tanto, dependiendo del tamaño de los datos, este proceso puede tardar mucho tiempo en realizarse. Para acelerar el proceso, puede iniciar múltiples sesiones CLI y ejecutar el comando de regeneración de metadatos en cada sesión para completar el proceso simultáneamente para cada par. Para obtener más detalles, consulte*** Regeneración de metadatos para pares de RAID de un dispositivo de la serie M.

1. Habilite los pares de discos ejecutando el siguiente comando de la CLI para cada par:

   ```
   admin> request system raid add <slot> force no-format
   ```

   Por ejemplo:

   ```
   admin> request system raid add A1 force no-format
    admin> request system raid add A2 force no-format
   ```

   Los argumentos **force** y **no-format** son obligatorios. El argumento **force** asocia el par de discos con el nuevo dispositivo. El argumento **no-format** evita la aplicación de formato de las unidades y mantiene almacenados los logs en los discos.
2. Genere los metadatos para cada par de discos.

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   Por ejemplo:

   ```
   admin> request metadata-regenerate slot 1
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 10 | Configure el recopilador de logs local en el nuevo dispositivo de la serie M.

> ***Para todos los pasos con comandos que requieran un número de serie, debe introducir el número de serie completo; pulsar la tecla Tab no completará un número de serie parcial.***

No habilite los discos en el nuevo dispositivo de la serie M en este punto. Cuando migre correctamente los logs, Panorama habilitará los discos de manera automática.

1. Configure el recopilador de logs local como un recopilador gestionado mediante la interfaz web de Panorama o mediante los siguientes comandos de la CLI:

```
admin> configure admin# set log-collector <log-collector_SN>
 deviceconfig system hostname <log-collector-hostname>
 admin# exit
```

2. Compile los cambios realizados en Panorama. No compile los cambios en el grupo de recopiladores aún.

```
admin> configure admin# commit
```

3. Verifique que el recopilador de logs local esté conectado a Panorama y que el estado de sus pares de discos sea presente o disponible.

```
admin> show log-collector serial-number <log-collector_SN>
```

   Los pares de discos se mostrarán como desactivados en esta etapa del proceso de restauración.

STEP 11 | Añada un recopilador de logs sin discos a un grupo de recopiladores.

> ***Desde este punto, solo las confirmaciones que son necesarios para completar el proceso de migración en Panorama y los recopiladores de logs. No realice ningún otro cambio.***

1. Acceda a la CLI de Panorama.
2. Sobrescriba la restricción de Panorama para permitir que el recopilador de logs sin disco se añada a un grupo de recopiladores: **request log-migration-set-start**
3. Confirme la restricción sobrescrita:

```
admin> configure admin# commit force
```

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Migre los logs.

1. Acceda a la CLI de Panorama.
2. Añada el nuevo recopilador de logs local como miembro del grupo de recopiladores y compile sus cambios en Panorama.

   ```
   admin# set log-collector-group <collector_group_name> logfwd-
   setting collectors <SN_managed_collector> admin# commit
    admin# exit
   ```

   El recopilador de logs local anterior seguirá apareciendo en la lista de miembros, ya que todavía no lo ha eliminado de la configuración.
3. Para cada par de discos, migre los logs al nuevo dispositivo.

   ```
   admin> request log-migration from <old_LC_serial_number> old-
   disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
   pair <log_disk_pair>
   ```

   Por ejemplo:

   ```
   admin> request log-migration from 003001000010 old-disk-pair A
    to 00300100038 new-disk-pair A
   ```
4. Compile los cambios realizados en Panorama.

   ```
   admin> configure admin# commit
   ```

STEP 13 | Vuelva a configurar el grupo de recopiladores.

1. Utilice la interfaz de usuario para asignar el nuevo recopilador de logs a los cortafuegos que reenvían logs (**Panorama** > **Collector Groups [Grupos de recopiladores]** > **Device Log**

 ©2023 Palo Alto Networks, Inc.

Forwarding [Reenvío de logs del dispositivo]). Conceda al recopilador de logs la misma prioridad en las listas de preferencia del cortafuegos que el recopilador de logs anterior.

No puede usar la CLI para cambiar las asignaciones de prioridad de las listas de preferencia del cortafuegos.

2. Elimine el recopilador de logs anterior del grupo de recopiladores.

```
admin# delete log-collector-group <group_name> logfwd-setting
 collectors <old_LC_serial_number>
```

Por ejemplo:

```
admin# delete log-collector-group DC-Collector-Group logfwd-
setting collectors 003001000010
```

3. Elimine el Recopilador de logs anterior de la configuración de Panorama y compile sus cambios en Panorama.

```
admin# delete log-collector <old_LC_serial_number>
 admin# commit admin# exit
```

4. Sincronice la configuración de los peers de HA del dispositivo de la serie M.

```
admin> request high-availability sync-to-remote running-config
```

5. Compile los cambios del grupo de recopiladores de modo que los cortafuegos gestionados puedan enviar logs al nuevo recopilador de logs.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Por ejemplo:

```
admin> commit-all log-collector-config log-collector-group DC-
Collector-Group
```

 ©2023 Palo Alto Networks, Inc.

STEP 14 | Genere nuevas claves en el nuevo recopilador de logs.

Este comando es necesario para añadir el nuevo recopilador de logs al grupo de recopiladores y solo debe ejecutarse para el grupo de recopiladores del recopilador de logs que se está reemplazando. Este paso elimina las claves RSA existentes y permite que Panorama cree nuevas claves RSA.

1. Acceda a la CLI de Panorama.
2. Elimine todas las claves RSA en el nuevo recopilador de logs:

   request logdb update-collector-group-after-replacecollector-group *<collector-group-name>*

   El proceso puede tomar hasta 10 minutos para completarse.

STEP 15 | Confirme que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores.

No continúe hasta que el estado de SearchEngine esté activo para todos los recopiladores de logs en el grupo de recopiladores. Esto dará como resultado la purga de los logs del recopilador de logs que se está sustituyendo.

1. Acceda a la CLI de Panorama.
2. Muestre los detalles del recopilador de logs ejecutando los siguientes comandos en:
   - Panorama para todos los recopiladores de logs:

     show log-collector all

     Alternativamente, puede ejecutar el siguiente comando en cada recopilador de logs dedicado:

     ```
     show log-collector detail
     ```
3. Confirme que el estado de SearchEngine es activo.

```
Estado de redistribución: ninguno
```

```
Última compilación de todo: compilación exitosa, versión
 actual del anillo 1
```

```
Estado de SearchEngine: Activo
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 actualizado en
 2017/06/14 09:58:19
```

 ©2023 Palo Alto Networks, Inc.

STEP 16 | En el nuevo recopilador de logs, reemplace el número de serie del recopilador de logs anterior con el número de serie del nuevo recopilador de logs.

Debe reemplazar el antiguo número de serie del recopilador de logs con el número de serie del nuevo recopilador de logs para que el nuevo recopilador de logs no se ejecute para purgar problemas, lo que evitaría que el recopilador de logs pueda purgar los datos antiguos de los logs migrados cuando sea necesario.

1. Acceda a la CLI del recopilador de logs.
2. Reemplace el número de serie de recopilador de logs antiguo con el número de serie de nuevo recopilador de logs:

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

STEP 17 | Restaure la funcionalidad de HA para el peer de HA de Panorama `suspendido` para forzar el restablecimiento de los cambios de estado de comunicación segura en el peer de HA secundario.

1. Inicio de sesión en la interfaz web de Panorama del nuevo peer de HA de Panorama (`secundario`).
2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y **Make local Panorama functional (Hacer que la instancia local de Panorama sea funcional) para alta disponibilidad**.
3. Haga clic en **OK (Aceptar)** para confirmar la restauración de la funcionalidad de HA en el nuevo peer de HA de Panorama.

STEP 18 | Reinicie el servidor de gestión en el nuevo peer de HA de Panorama.

1. Inicio de sesión en la CLI de Panorama del nuevo peer de HA de Panorama (`secundario`).
2. Reinicie el servidor de gestión.

   ```
   admin> debug software restart process management-server
   ```

STEP 19 | (RMA del peer de HA principal activo solamente) Restaure la configuración de alta disponibilidad de los peer de HA de Panorama.

Omita este paso si reemplazó el peer de HA `secundario` en una configuración de HA A/P.

1. Inicio de sesión en la interfaz web de Panorama del peer de HA `principal`.
2. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección Election Settings (Ajustes de elección).
3. Para Priority (Prioridad), seleccione **secondary (secundario)** y haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.
5. Inicio de sesión en la interfaz web de Panorama del peer de HA `secundario`.
6. Seleccione **Panorama** > **High Availability (Alta disponibilidad)** y edite la sección Election Settings (Ajustes de elección).
7. Para Priority (Prioridad), seleccione **primary (principal)** y haga clic en **OK (Aceptar)**.
8. Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

 ©2023 Palo Alto Networks, Inc.

Migración de recopiladores de logs después de un error o RMA de un Panorama que no es de HA

Si se produce un fallo de sistema en un servidor de gestión de Panorama que no está implementado en una configuración de alta disponibilidad (high availability, HA), realice este procedimiento para restaurar la configuración en el Panorama de sustitución y restaure el acceso a los logs de los recopiladores de logs dedicados que gestiona. Los casos de migración permitidos varían de acuerdo al modelo del servidor de gestión de Panorama:

Panorama antiguo o con errores	Panorama nuevo o de reemplazo
Dispositivo virtual Panorama	• Dispositivo virtual Panorama • Dispositivo M-200 • Dispositivo M-500 • Dispositivo M-600
Dispositivo M-100	• Dispositivo virtual Panorama • Dispositivo M-200 • Dispositivo M-500 • Dispositivo M-600
Dispositivo M-500	• Dispositivo virtual Panorama • Dispositivo M-200 • Dispositivo M-500 • Dispositivo M-600

Panorama mantiene un archivo en anillo que asigna los segmentos y las particiones que los recopiladores de logs dedicados usan para almacenar los logs. Un dispositivo de la serie M en modo Panorama almacena el archivo en anillo en su SSD interno; un dispositivo virtual Panorama almacena el archivo en anillo en su disco interno. Cuando se produce un fallo del sistema, un Panorama que no es de HA no puede recuperar automáticamente el archivo en anillo. Por lo tanto, cuando sustituye Panorama, debe restaurar el archivo en anillo para acceder a los logs de los recopiladores de logs dedicados.

Este procedimiento requiere que** haya realizado una copia de seguridad y exportado la configuración de Panorama **antes de que se produzca el error del sistema.

Palo Alto Networks recomienda implementar Panorama en una configuración de HA. El peer activo de Panorama sincroniza automáticamente el archivo de portacertificados con el peer pasivo en una configuración de HA, con lo que se mantiene el acceso a los logs de los recopiladores de logs dedicados aunque deba reemplazar uno de los peers.

©2023 Palo Alto Networks, Inc.

STEP 1 | Lleve a cabo la configuración inicial del nuevo dispositivo Panorama.

1. Realice la Configuración del dispositivo serie M o la Configuración del dispositivo virtual Panorama según sus necesidades. Si está configurando un nuevo dispositivo serie M, consulte las Guías de referencia de hardware del dispositivo serie M para obtener instrucciones sobre cómo montar el nuevo dispositivo serie M en bastidores.
2. Lleve a cabo la configuración inicial del dispositivo de la serie M o lleve a cabo la configuración inicial del dispositivo virtual Panorama.

   *Si el dispositivo serie M anterior utilizaba interfaces diferentes a la interfaz de MGT para los servicios de Panorama (como la recopilación de logs), debe definir estas interfaces durante la configuración inicial del nuevo dispositivo serie M (**Panorama** > **Setup [Configuración]** > **Interfaces [Interfaces]**). El dispositivo virtual Panorama solo admite interfaces MGT.*
3. Registre Panorama.
4. Transfiera las licencias de la siguiente manera solamente si el nuevo dispositivo Panorama es del mismo modelo que el dispositivo anterior. De lo contrario, debe comprar licencias nuevas.
   1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
   2. Seleccione la pestaña **Assets (Activos)** y haga clic en el enlace **Spares (Repuestos)**.
   3. Haga clic en el número de serie del dispositivo nuevo de la serie M.
   4. Haga clic en **Transfer Licenses (Transferir licencias)**.
   5. Haga clic en **Select (Seleccionar)** para elegir el dispositivo anterior y, luego, haga clic en **Submit (Enviar)**.
5. Active una licencia de asistencia técnica de Panorama.
6. Active una licencia de gestión de cortafuegos.
7. Instale las actualizaciones de contenido y software de Panorama.

   El dispositivo M-500 requiere Panorama 7.0 o una versión posterior. Los dispositivos M-200 y M-600 requieren Panorama 8.1. Para obtener detalles importantes sobre las versiones de software, consulte Compatibilidad de versiones de Panorama, recopilador de logs, cortafuegos y WildFire**.**

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Restaure la configuración desde el Panorama anterior en este Panorama de sustitución.

1. Inicie sesión en el nuevo Panorama y seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Import named Panorama configuration snapshot (Importar instantánea de configuración de Panorama con nombre)**, haga clic en **Browse (Explorar)** para localizar el archivo de configuración con copia de seguridad y, luego, haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el **Name (Nombre)** del archivo que acaba de importar, y haga clic en **OK (Aceptar)**.

   *Si desea sustituir una instancia de Panorama con una autorización para la devolución de bienes (return merchandise authorization, RMA), no olvide marcar **Retain Rule UUIDs (Conservar UUID de reglas)** cuando cargue la instantánea de la configuración con nombre de Panorama. Si no lo hace, Panorama elimina todos los UUID anteriores de la instantánea de configuración y asigna UUID nuevos a las reglas en Panorama. Eso implica que no se conserva la información asociada a los antiguos UUID, por ejemplo, el recuento de resultados de las reglas de las políticas.*
4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.
5. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y compruebe que la columna Conectado muestra una marca de verificación para el recopilador de logs dedicado.

   Si el recopilador de logs dedicado no aparece, debe volver a configurar el recopilador de logs y el grupo de recopiladores como se describe en el siguiente paso. De lo contrario, omita el siguiente paso y continúe al paso Recupere el archivo en anillo para restaurar el acceso a los logs almacenados en los recopiladores de logs dedicados..

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Vuelva a configurar el recopilador de logs dedicado y el grupo de recopiladores si no aparecen en Panorama.

1. Acceda a la CLI del recopilador de logs dedicado e introduzca los siguientes comandos para mostrar el nombre de su grupo de recopiladores.

   1. Introduzca el comando:

   ```
   > request fetch ring from log-collector <serial_number>
   ```

   Aparecerá el siguiente error:

   ```
   Server error: (Error del servidor) Failed to fetch
    ring info from (Error al obtener información de anillo
    de) <serial_number>
   ```

   2. Introduzca el comando:

   ```
   > less mp-log ms.log
   ```

   Aparecerá el siguiente error:

   ```
   Dec04 11:07:08 Error:
    pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): La
    configuración actual no contiene el grupo CA-Collector-
   Group
   ```

   En este ejemplo, el mensaje de error indica que el grupo de recopiladores que falta tiene el nombre CA-Collector-Group.

2. Configure el grupo de recopiladores y asigne el recopilador de logs dedicado a este.

   ```
   > configure # set log-collector-group <collector-group-name>
    # set log-collector-group <collector-group-name> logfwd-
   setting collector <serial-number>
   ```

3. Compile los cambios en Panorama pero no en el grupo de recopiladores.

   ```
   # commit # exit
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Recupere el archivo en anillo para restaurar el acceso a los logs almacenados en los recopiladores de logs dedicados.

1. Acceda a la CLI del nuevo Panorama.
2. Recupere el archivo en anillo:

```
> request fetch ring from log-collector <serial-number>
```

Por ejemplo:

```
> request fetch ring from log-collector 009201000343
```

Si no conoce el número de serie del recopilador de logs dedicado, inicie sesión en su CLI e introduzca el comando de operación ***show system info****.*

3. Compile los cambios en el grupo de recopiladores.

```
> commit-all log-collector-config log-collector-
group <collector-group-name>
```

Regeneración de metadatos para pares de RAID para un dispositivo serie M

Cuando se produce un fallo de sistema en el dispositivo M-700, M-600, M-500 o M-300 o M-200, y tiene que trasladar físicamente los discos de un dispositivo y colocarlos en otro, es necesario volver a generar los metadatos. Los metadatos son necesarios para localizar los logs en el disco; cuando un usuario realiza una consulta de log, la consulta mira los metadatos para acceder a los datos de log solicitados.

Para cada par de discos RAID configurado en el dispositivo de la serie M, debe acceder al dispositivo CLI y ejecutar el siguiente comando para volver a generar los metadatos:

```
> request metadata-regenerate slot <slot_number>
```

Por ejemplo:

```
> request metadata-regenerate slot 1
```

El tamaño de los discos RAID determina cuánto tiempo llevará la regeneración de metadatos. En promedio, llevará una hora por cada 100 GB. Cuando ejecuta el comando, la sesión de CLI se bloquea hasta que el comando se ejecuta por completo. Puede usar varias sesiones de CLI para ahorrar tiempo. Por ejemplo, para reemplazar cuatro pares RAID de 1 TB con un total de 4 TB de datos de logs, inicie cuatro sesiones de CLI y ejecute el comando en cada sesión para volver a generar los metadatos de manera simultánea para todos los pares o ranuras en aproximadamente 10 horas.

Durante la regeneración de los metadatos, el grupo de recopiladores al que pertenecen estos discos no está disponible y el par de discos no está disponible para ninguna operación de recopilación de creación de logs o informes (escrituras/consultas). Sin embargo, puede realizar otras tareas como

 ©2023 Palo Alto Networks, Inc.

la gestión de nuevas conexiones de cortafuegos o de cambios de configuración en los cortafuegos gestionados. El resto de los grupos de recopiladores que Panorama gestiona y que no forman parte de este proceso de RMA pueden realizar las tareas de creación de logs e informes asignadas de forma normal.

Visualización de trabajos de consulta de logs

Puede ver sus trabajos de consulta de logs para investigar y comprender mejor por qué la consulta de datos de logs tarda más de lo esperado. Para comenzar, primero debe mostrar todos los trabajos de consulta de logs que se ejecutan en Panorama. Después de identificar el trabajo de consulta de log que necesite investigar, use el ID de trabajo para ver información detallada sobre la consulta y comprender mejor por qué su consulta de logs tiene problemas. Al consultar datos de logs en Panorama, la información detallada de la identificación del trabajo se sobrescribe a medida que se ejecutan nuevos trabajos de consulta de logs.

STEP 1 | Inicio de sesión en la CLI de Panorama.

STEP 2 | Vea los trabajos de consulta de logs ejecutados en Panorama.

La salida de la CLI incluye información general sobre cada consulta de log ejecutada, como el ID de trabajo, cuándo se ejecutó la consulta, el estado de la consulta, la base de datos de logs que se consultó, el número de logs consultados, cuánto tiempo (en ms) tardó la consulta en devolver resultados, el administrador que ejecutó la consulta y cualquier filtro aplicado a la consulta.

```
admin@Panorama> show query jobs
```

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
------------------------------------------------------------------------------
------------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Consulte información de consulta de logs de detalles sobre un trabajo específico mediante el ID del trabajo.

```
admin@Panorama> show query jobid
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                              Last Update Time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                           2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                       2020/01/02 14:35:46
```

 ©2023 Palo Alto Networks, Inc.

Sustitución de un cortafuegos con una autorización de devolución de mercancía

Para reducir al mínimo el esfuerzo necesario para restablecer la configuración de un cortafuegos gestionado con una Autorización de devolución de mercancía (Return Merchandise Authorizatio, RMA), sustituya el número de serie del cortafuegos anterior por el del cortafuegos nuevo en Panorama. Para restablecer la configuración en el cortafuegos de sustitución a continuación, importe un estado de cortafuegos que haya generado y exportado anteriormente del cortafuegos o utilice Panorama para generar un ***estado de dispositivo parcial*** para cortafuegos gestionados que ejecuten PAN-OS 5.0 y versiones posteriores. Cuando sustituye el número de serie e importa el estado del cortafuegos, puede volver a utilizar Panorama para gestionar el cortafuegos.

- Generación de estado de dispositivo parcial para cortafuegos
- Antes de iniciar una sustitución de un cortafuegos con RMA
- Restablecimiento de la configuración del cortafuegos tras su sustitución

Generación de estado de dispositivo parcial para cortafuegos

Cuando utiliza Panorama para generar un estado de dispositivo parcial, replica la configuración de los cortafuegos gestionados con un par de excepciones para configuraciones de VPN a gran escala (LSVPN). Cree el estado de dispositivo parcial combinando dos facetas de la configuración del cortafuegos:

- Configuración centralizada gestionada por Panorama: Panorama mantiene una instantánea de las reglas de políticas y plantillas compartidas que introduce en los cortafuegos.
- Configuración local en el cortafuegos: cuando compila un cambio de configuración en un cortafuegos, se envía una copia de su archivo de configuración local en Panorama. Panorama almacena este archivo y lo utiliza para compilar el lote del estado de dispositivo parcial.



En una configuración de LSVPN, el lote del estado de dispositivo parcial que genera en Panorama no es el mismo que la versión que puede exportar desde un cortafuegos (seleccionando ***Device [Dispositivo] > Setup [Configuración] > Operations [Operaciones]*** *y haciendo clic en* ***Export device state [Exportar estado de dispositivo]****). Si ha ejecutado manualmente la exportación de estado de dispositivo o ha programado un comando API XML para exportar el archivo a un servidor remoto, puede utilizar el estado de dispositivo exportado de su flujo de trabajo de sustitución de cortafuegos.*

Si no ha exportado el estado de dispositivo, el estado de dispositivo que genere en este flujo de trabajo de sustitución no incluirá la información de configuración dinámica, como la información detallada de certificado y los cortafuegos registrados, que es necesaria para restablecer la configuración completa de un cortafuegos que funcione como portal de LSVPN. Consulte Antes de iniciar una sustitución de un cortafuegos con RMA *para obtener más información.*

Panorama no almacena el estado de dispositivo; se genera tras solicitarlo mediante los comandos de la CLI indicados en Restablecimiento de la configuración del cortafuegos tras su sustitución.

 ©2023 Palo Alto Networks, Inc.

Antes de iniciar una sustitución de un cortafuegos con RMA

- El cortafuegos que se reemplazará debe ejecutar PAN-OS 5.0.4 o una versión posterior. Panorama no puede generar el ***estado de dispositivo*** para cortafuegos que ejecuten versiones anteriores de PAN-OS.
- Registre los siguientes detalles sobre el cortafuegos que reemplazará:
  - **Número de serie**: Debe introducir el número de serie en el sitio web de Atención al cliente de Palo Alto Networks para transferir las licencias del cortafuegos anterior al cortafuegos de sustitución. También deberá introducir esta información en Panorama para sustituir todas las referencias al número de serie anterior por el nuevo número de serie del cortafuegos de sustitución.
  - (Recomendado) **Versión de PAN-OS y versión de la base de datos de contenido**: La instalación de las mismas versiones de software y base de datos de contenido, incluido el proveedor de base de datos de URL, le permite crear el mismo estado en el cortafuegos de sustitución. Si decide instalar la versión más reciente de la base de datos de contenido, puede que observe diferencias debido a actualizaciones y adiciones a la base de datos. Para determinar las versiones instaladas en el cortafuegos, acceda a los logs de sistema del cortafuegos almacenados en Panorama.
- Prepare el cortafuegos de sustitución para su implementación. Antes de importar el lote del estado de dispositivo y restablecer la configuración, debe hacer lo siguiente:
  - Verifique que el cortafuegos de sustitución es del mismo modelo que el anterior y está habilitado para una capacidad operativa similar. Considere las siguientes funciones operativas: ¿el cortafuegos de sustitución debe tener múltiples sistemas virtuales, admitir Jumbo Frames o habilitarse para funcionar en modo CC o FIPS?
  - Configure el acceso de red, transfiera las licencias e instale la versión de PAN-OS y la versión de la base de datos de contenido adecuadas.
- Debe utilizar la CLI de Panorama para completar este proceso de sustitución del cortafuegos. Para ello, la cuenta de administrador debe tener la función de usuario de superusuario o administrador de Panorama.
- Si tiene una configuración de LSVPN y está sustituyendo un cortafuegos de Palo Alto Networks implementado como satélite o portal de LSVPN, la información de configuración dinámica necesaria para restablecer la conectividad de LSVPN no estará disponible cuando restablezca el estado de dispositivo parcial generado en Panorama. Si siguió la recomendación de generar y exportar frecuentemente el estado de dispositivo de los cortafuegos de una configuración de LSVPN, utilice el estado de dispositivo que había exportado anteriormente desde el propio cortafuegos en lugar de generar uno en Panorama.

  Si no ha exportado manualmente el estado de dispositivo desde el cortafuegos y necesita generar un estado de dispositivo parcial en Panorama, la configuración dinámica que falta afectará al proceso de sustitución del cortafuegos del modo siguiente:

  - **Si el cortafuegos que está sustituyendo es un portal GlobalProtect** que está configurado explícitamente con el número de serie de los satélites (**Network [Red]** > **GlobalProtect** > **Portals [Portales]** > **Satellite Configuration [Configuración de satélite]**), al restablecer la configuración del cortafuegos, aunque se haya perdido la configuración dinámica, el cortafuegos de portal podrá autenticar los satélites correctamente. La autenticación correcta añadirá la información de configuración dinámica y la conectividad de LSVPN volverá a establecerse.

 ©2023 Palo Alto Networks, Inc.

- **Si está sustituyendo un cortafuegos satélite**, este no podrá conectarse ni realizar la autenticación en el portal. Esta falla se produce porque el número de serie no se configuró explícitamente en el cortafuegos (**Network [Red]** > **GlobalProtect** > **Portals [Portales]** > **Satellite Configuration [Configuración de satélite]**) o porque, aunque el número de serie se configuró explícitamente, el número de serie del cortafuegos sustituido no coincide con el del cortafuegos anterior. Para restablecer la conectividad, después de importar el lote del estado de dispositivo, el administrador del satélite debe iniciar sesión en el cortafuegos e introducir las credenciales (nombre de usuario y contraseña) para realizar la autenticación en el portal. Después de la autenticación, la configuración dinámica necesaria para la conectividad de LSVPN se generará en el portal.

Sin embargo, si el cortafuegos tiene una configuración de alta disponibilidad, después de restablecer la configuración, el cortafuegos sincronizará automáticamente la configuración que se está ejecutando con su peer y obtendrá la configuración dinámica más reciente necesaria para funcionar sin problemas.

Restablecimiento de la configuración del cortafuegos tras su sustitución

Para restaurar la configuración del cortafuegos en el nuevo cortafuegos, primero debe realizar la configuración inicial en el nuevo cortafuegos, incluida la configuración del modo operativo, la actualización del software de PAN-OS y la versión de publicación de contenido para que coincida con lo que se instaló en el cortafuegos anterior. Luego, exporte el estado del dispositivo del cortafuegos anterior desde Panorama e impórtelo en el nuevo cortafuegos. Por último, vuelva a Panorama para validar que el nuevo cortafuegos se haya conectado y sincronizado con Panorama.

STEP 1 | Lleve a cabo la configuración inicial en el nuevo cortafuegos y verifique la conectividad de red.

Utilice una conexión de puerto de serie o una conexión de shell seguro (Secure Shell, SSH) para añadir una dirección IP y una dirección IP de un servidor DNS, y para verificar que el nuevo cortafuegos pueda acceder al servidor de actualizaciones de Palo Alto Networks.

STEP 2 | (Opcional) Establezca el modo operativo del cortafuegos nuevo para que coincida con el del cortafuegos anterior.

Se requiere una conexión de puerto de serie para esta tarea.

1. Introduzca el siguiente comando de la CLI para acceder al modo de mantenimiento del cortafuegos:

```
> debug system maintenance-mode
```

2. Para el modo operativo, seleccione **Set FIPS Mode** o **Set CCEAL 4 Mode** desde el menú principal.

STEP 3 | Recupere las licencias del nuevo cortafuegos.

Introduzca el siguiente comando para recuperar las licencias:

```
> request license fetch
```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Haga coincidir el estado operativo del nuevo cortafuegos con el del cortafuegos anterior. Por ejemplo, habilite la capacidad de varios sistemas virtuales (VSYS múltiple) para un cortafuegos que tuviera esta capacidad habilitada.

Introduzca los comandos relativos a sus ajustes de cortafuegos:

```
> set system setting multi-vsys on > set system setting jumbo-frame
 on
```

STEP 5 | Actualice la versión de PAN-OS en el cortafuegos nuevo.

Debe realizar la actualización a las mismas versiones de PAN-OS instaladas en el cortafuegos anterior. Debe actualizar las versiones de contenido a la misma o a una versión posterior a la que está instalada en el cortafuegos anterior.

Introduzca los siguientes comandos:

1. Para actualizar la versión de publicación de contenido:

   ```
   > request content upgrade download latest > request content
    upgrade install version latest
   ```

2. Para actualizar la versión de publicación de antivirus, realice el siguiente procedimiento:

   ```
   > request anti-virus upgrade download latest > request anti-
   virus upgrade install version latest
   ```

3. Para actualizar la versión del software PAN-OS:

   ```
   > request system software download version <version> > request
    system software install version <version>
   ```

STEP 6 | Vaya a la CLI de Panorama y exporte el lote del estado del dispositivo del antiguo cortafuegos a un ordenador con Secure Copy (SCP) or TFTP (no puede hacer esto desde la interfaz web).

Si exportó manualmente el estado del dispositivo desde el cortafuegos, puede omitir este paso.

El comando de exportación genera el lote del estado de dispositivo como un archivo comprimido tar y lo exporta a la ubicación especificada. Este estado de dispositivo no incluirá la configuración dinámica de LSVPN (información de satélite e información detallada de certificado).

Introduzca uno de los siguientes comandos:

```
> scp export device-state device <old serial#> to <login>
 @ <serverIP>: <path>
```

O

```
> tftp export device-state device <old serial#> to <serverIP>
```

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Sustituya el número de serie del cortafuegos anterior por el del nuevo cortafuegos de sustitución en Panorama.

Al sustituir el número de serie en Panorama permite que el nuevo cortafuegos se conecte a Panorama después de restablecer la configuración en el cortafuegos.

1. Introduzca el siguiente comando en el modo operativo:

```
> replace device old <old SN#> new <new SN#>
```

2. Introduzca el modo de configuración y compile los cambios.

```
> configure # commit
```

3. Salga del modo de configuración.

```
# exit
```

 ©2023 Palo Alto Networks, Inc.

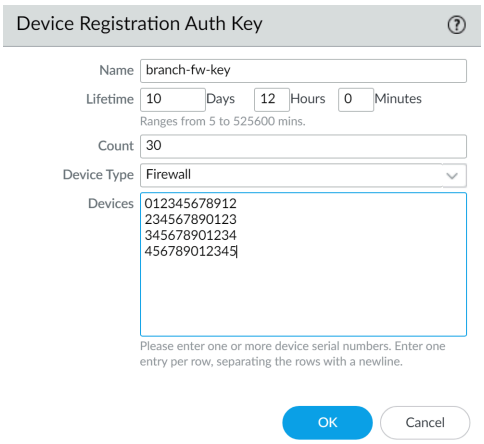
STEP 8 | (Opcional) Cree una clave de autenticación de registro de dispositivo en Panorama.

Este paso es necesario si no se crea una clave válida de autenticación de registro de dispositivo en Panorama. Omita este paso si ya se creó una clave válida de autenticación de registro de dispositivo en Panorama.

La exportación del paquete de estado del dispositivo no exporta la clave de autenticación de registro del dispositivo utilizada para agregar el cortafuegos a la administración de Panorama. Cuando restaura la configuración del cortafuegos después del reemplazo, debe crear una nueva clave de autenticación de registro del dispositivo para agregar el nuevo cortafuegos a Panorama.

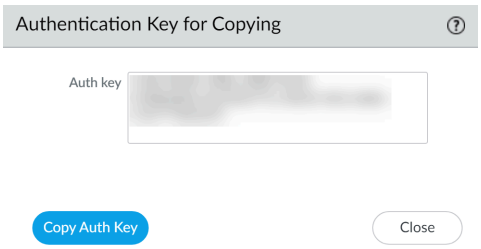
1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Device Registration Auth Key (Clave de autenticación de registro del dispositivo)** y haga clic en **Add (Añadir)** para agregar una nueva clave de autenticación.
3. Configure la clave de autenticación.
   - **Name (Nombre)**: ingrese un nombre descriptivo para la clave de autenticación.
   - **Lifetime (Duración)**: ingrese la duración de la clave a fin de especificar durante cuánto tiempo se puede utilizar la clave de autenticación para incorporar nuevos cortafuegos.
   - **Count (Conteo)**: especifique cuántas veces se puede utilizar la clave de autenticación para incorporar nuevos cortafuegos.
   - **Device Type (Tipo de dispositivo)**: especifique que esta clave de autenticación se utiliza para autenticar un **Firewall (Cortafuegos)**.

     *Seleccione **Any (Cualquiera)** para usar la clave de autenticación de registro del dispositivo para incorporar cortafuegos y recopiladores de logs.*
   - (Opcional) **Devices (Dispositivos)**: introduzca uno o más números de serie de dispositivo para especificar para qué cortafuegos es válida la clave de autenticación.
4. Haga clic en **OK (Aceptar)**.



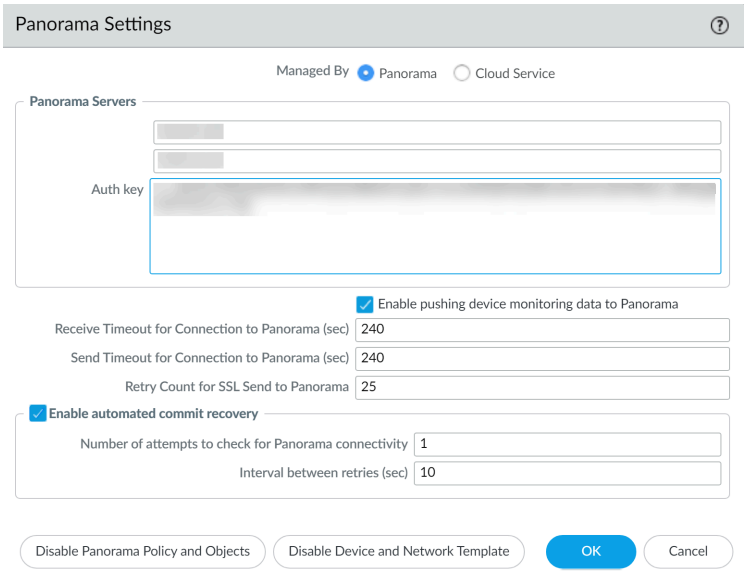
5. Seleccione **Copy Auth Key (Copiar la clave de autenticación)** y **Close (Cerrar)**.

 ©2023 Palo Alto Networks, Inc.



STEP 9 | En el nuevo cortafuegos, importe el estado del dispositivo y agregue la clave de autenticación de registro del dispositivo.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en el enlace **Import Device State (Importar estado del dispositivo)** en la sección Gestión de configuración.
3. Navegue para ubicar el archivo y haga clic en **OK (Aceptar)**.
4. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
5. Introduzca la **Auth key (Clave de autenticación)** que creó en Panorama y haga clic en **OK (Aceptar)**.



6. Seleccione **Commit (Confirmar)** sus políticas en la configuración que se esté ejecutando en el cortafuegos.

STEP 10 | Desde Panorama, verifique que restauró correctamente la configuración del cortafuegos.

1. Acceda a la interfaz web de Panorama y seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)**.
2. Verifique que la columna Conectado del cortafuegos nuevo tenga una marca de verificación.

 ©2023 Palo Alto Networks, Inc.

STEP 11 | Sincronice el cortafuegos con Panorama.

1. Acceda a la interfaz web de Panorama, seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Device Groups (Grupos de dispositivos)**, seleccione el grupo de dispositivos que contiene el cortafuegos e seleccione **Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
3. Seleccione **Collector Groups (Grupos de recopiladores)** y seleccione el Grupo de recopiladores que contiene el cortafuegos.
4. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
5. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.



Si necesita generar informes para un periodo durante el cual el cortafuegos anterior era funcional después de haber instalado el cortafuegos nuevo, debe generar una consulta independiente para cada número de serie de cortafuegos, ya que sustituir el número de serie en Panorama no sobrescribe la información en los logs.

 ©2023 Palo Alto Networks, Inc.

Solución de problemas de fallos de compilación

Si se producen fallos de confirmación o envío en Panorama, verifique las siguientes condiciones:

Síntoma	Condición	Solución
Fallo de envío de grupo de dispositivos o plantillas	La capacidad de recibir cambios de configuración en las plantillas y en los grupos de dispositivos se deshabilitó en el cortafuegos.	Acceda a la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)**, edite la configuración de Panorama y luego haga clic en **Enable Device and Network Template (Habilitar plantilla de dispositivo y red)** y **Enable Panorama Policy and Objects (Habilitar objetos y política de Panorama)**.
Fallo de confirmación de Panorama o fallo de envío de plantilla, grupo de dispositivos o grupo de recopiladores	El servidor de gestión de Panorama posee una versión de software anterior a la de los recopiladores de logs dedicados o cortafuegos que gestiona.	Actualice el servidor de gestión de Panorama a la misma versión de software o una más alta que los cortafuegos gestionados, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire. Para obtener más información, consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.

©2023 Palo Alto Networks, Inc.

Solución de problemas de errores de registro o números de serie

En el dispositivo M-700, M-600, M-500, M-300 o M-200, si la página **Panorama** > **Support (Asistencia técnica)** no muestra los detalles de la licencia de asistencia técnica o la página **Panorama** > **Setup (Configuración)** > **Management (Gestión)** muestra el mensaje Unknown (Desconocido) en **Serial Number (Número de serie)** incluso después de realizar el Registro de Panorama, lleve a cabo estos pasos:

STEP 1 | Registre el número de serie de Panorama del correo electrónico de procesamiento del pedido que le envió Palo Alto Networks cuando realizó su pedido de Panorama.

STEP 2 | Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y edite la Configuración general.

STEP 3 | Introduzca **Serial Number** y haga clic en **OK**.

STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

 ©2023 Palo Alto Networks, Inc.

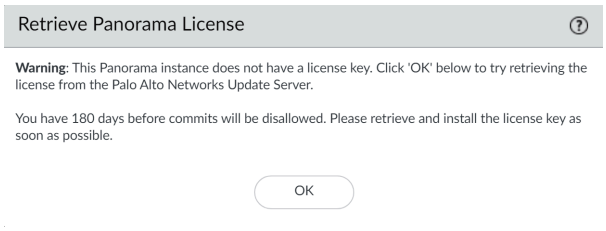
Solución de problemas de errores de creación de informes

Si Panorama falla al generar un informe o faltan los datos esperados en un informe, sus versiones de contenido (por ejemplo, la base de datos de aplicaciones) podrían ser diferentes de aquellas de los cortafuegos y recopiladores gestionados. Las versiones de contenido de Panorama deben ser iguales o inferiores a las versiones de contenido de los cortafuegos y recopiladores gestionados. Para obtener más información, consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.

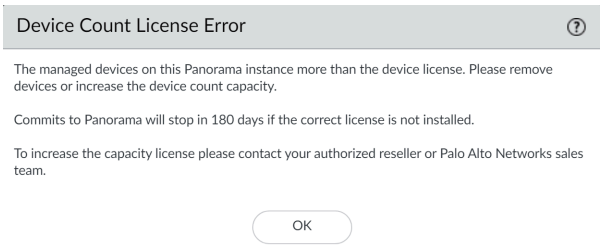
 ©2023 Palo Alto Networks, Inc.

Solución de problemas de errores de licencia de gestión de dispositivos

Después de actualizar a PAN-OS 8.1, el dispositivo virtual Panorama comprobará si se instaló correctamente una licencia de gestión de dispositivos. Si no se instaló correctamente una licencia de gestión de dispositivos o si el número de cortafuegos gestionados por el dispositivo virtual Panorama supera el límite de licencias de gestión de dispositivos, tendrá 180 días para instalar una licencia de gestión de dispositivos válida. Si no se instala una licencia de gestión de dispositivos válida, aparecerá la siguiente alerta cada vez que inicie sesión en la interfaz web de Panorama:



Si el número de cortafuegos gestionados por el dispositivo virtual Panorama supera el límite de licencias de gestión de dispositivos, aparecerán las siguientes alertas cada vez que inicie sesión en la interfaz web de Panorama:



Para solucionar el problema, instale una licencia de gestión de dispositivos válida:

STEP 1 | Póngase en contacto con su representante de ventas o distribuidor autorizado de Palo Alto Networks para adquirir la licencia de gestión de dispositivos adecuada.

STEP 2 | Inicio de sesión en la interfaz web de Panorama.

STEP 3 | Active/recupere una licencia de gestión de dispositivos en función de si el dispositivo virtual Panorama está conectado o no a internet.

- Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama está conectado a internet.
- Activación/recuperación de una licencia de gestión de cortafuegos cuando el dispositivo virtual Panorama no está conectado a internet.

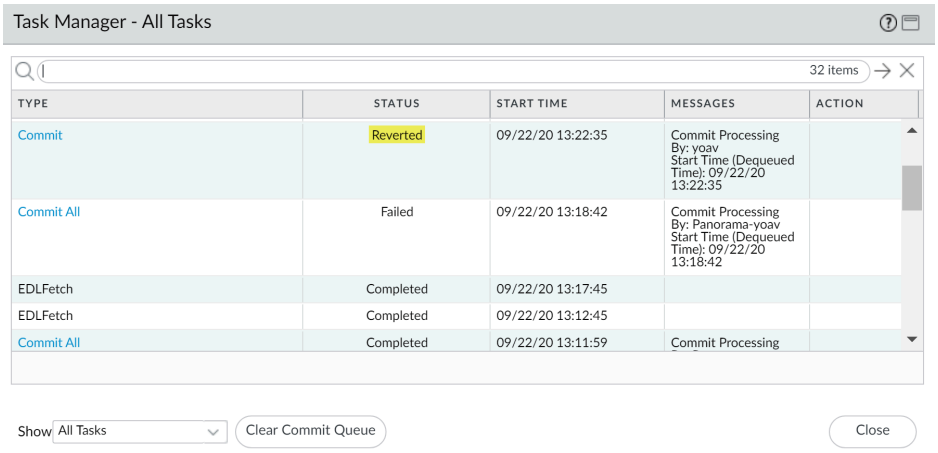
©2023 Palo Alto Networks, Inc.

Solución de problemas de las configuraciones del cortafuegos revertidas automáticamente

Si su cortafuegos gestionado revierte automáticamente su configuración debido a un cambio de configuración que provocó una interrupción de la conexión entre el servidor de gestión Panorama™ y el cortafuegos, puede solucionar los problemas de los cortafuegos no sincronizados para determinar qué cambios se realizaron y qué aspectos de ese último envío de configuración generó que el cortafuegos revirtiera su configuración

STEP 1 | Compruebe que el cortafuegos gestionado se haya revertido automáticamente a la última configuración en ejecución.

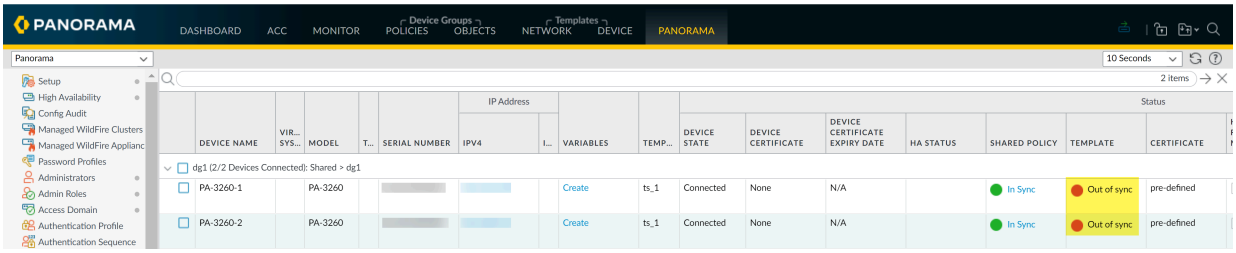
- En el cortafuegos:
  1. Inicie la interfaz web del cortafuegos.
  2. Haga clic en **Tasks (Tareas)** (esquina inferior derecha de la interfaz web).
  3. Compruebe que la última operación de confirmación (enviada desde Panorama o confirmada localmente) muestre el estado `Reverted (Revertido)`.



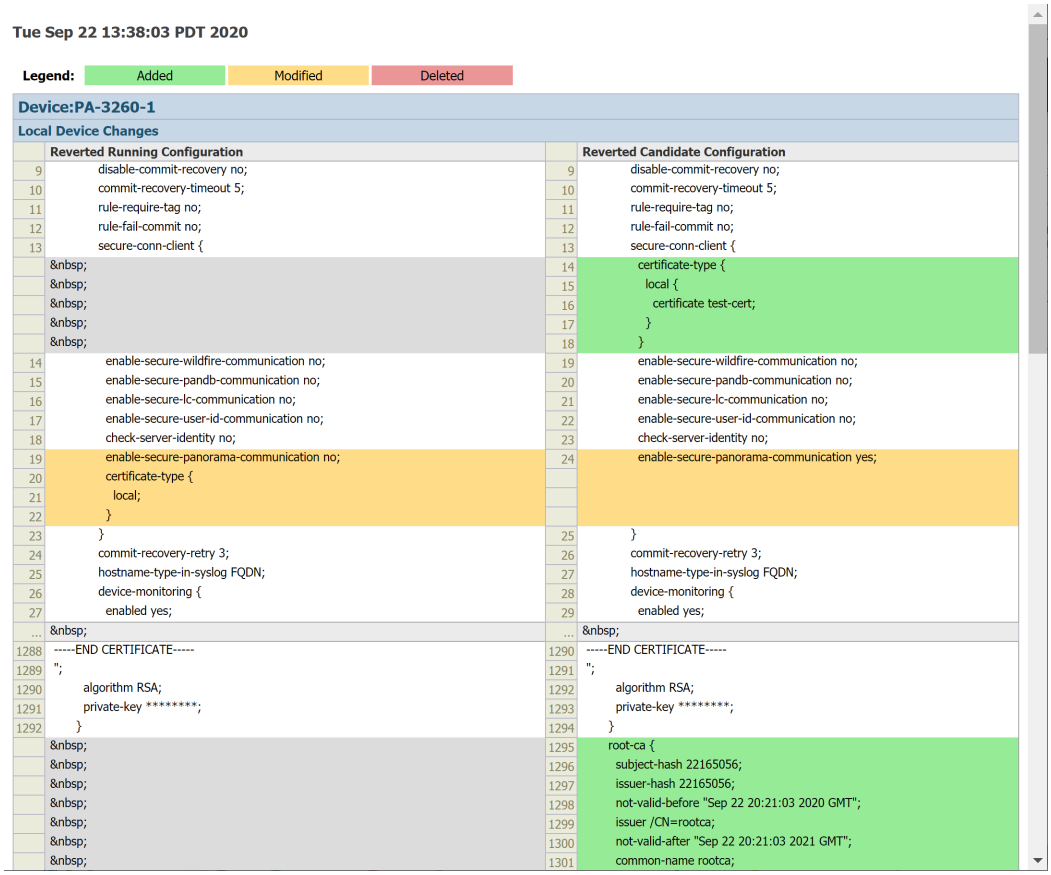
- En Panorama
  1. Inicio de sesión en la interfaz web de Panorama.
  2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
  3. Compruebe el estado de sincronización de la plantilla y la política compartida. Si ha insertado recientemente una configuración de Panorama en sus cortafuegos gestionados y

 ©2023 Palo Alto Networks, Inc.

se ha revertido, la política compartida o la plantilla deben aparecer con el estado **Out of Sync (Sin sincronización)** (según los cambios de configuración realizados).



STEP 2 | En la columna Last Merged Diff (Último diferencial combinado) para un cortafuegos gestionado, seleccione **Show Last Merged Config Diff (Mostrar último diferencial de configuración combinada)** ( ) para comparar la configuración actual en ejecución y la revertida. En este ejemplo, una regla de políticas enviada desde Panorama denegó todo el tráfico entre el cortafuegos gestionado y Panorama, lo que provocó que la configuración del cortafuegos se revirtiera automáticamente.



Tue Sep 22 13:38:03 PDT 2020

Legend: Added | Modified | Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | Modifique los objetos de configuración según sea necesario para no interrumpir la conexión entre los cortafuegos gestionados y Panorama antes de volver a enviar la configuración.

 ©2023 Palo Alto Networks, Inc.

Visualización de tareas que se realizaron correctamente o tienen errores

Haga clic en el icono del Gestor de tareas 

de la parte inferior derecha de la interfaz web de Panorama para ver si una tarea se ha realizado correctamente o no. El Gestor de tareas también muestra un mensaje detallado que ayuda a depurar un problema. Para obtener más detalles, consulte Uso del gestor de tareas de Panorama.

©2023 Palo Alto Networks, Inc.

Pruebas de coincidencia con políticas y conectividad de dispositivos gestionados

Tras enviar las configuraciones de los grupos de dispositivos y de la pila de plantillas a los cortafuegos, los recopiladores de logs y los dispositivos WF-500, compruebe que el tráfico coincide con las reglas de políticas enviadas a los dispositivos gestionados y que los cortafuegos se pueden conectar a todos los recursos de red pertinentes.

- Solución de problemas de coincidencias del tráfico con las reglas de políticas
- Solución de problemas de conectividad a recursos de red

Solución de problemas de coincidencias del tráfico con las reglas de políticas

Compruebe la configuración de las reglas de políticas aplicables a los dispositivos gestionados mediante pruebas de coincidencia para garantizar que la configuración activa ofrece la protección adecuada a la red permitiendo o denegando el tráfico correcto. Una vez generados los resultados sobre el tráfico que coincide con las reglas configuradas, haga clic en **Export to PDF (Exportar a PDF)** para guardarlos con fines de auditoría.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Troubleshooting (Solución de problemas)** para ejecutar una prueba de coincidencia con políticas.

*También puede ejecutar pruebas de coincidencia con políticas en la pestaña **Policies (Políticas)**.*

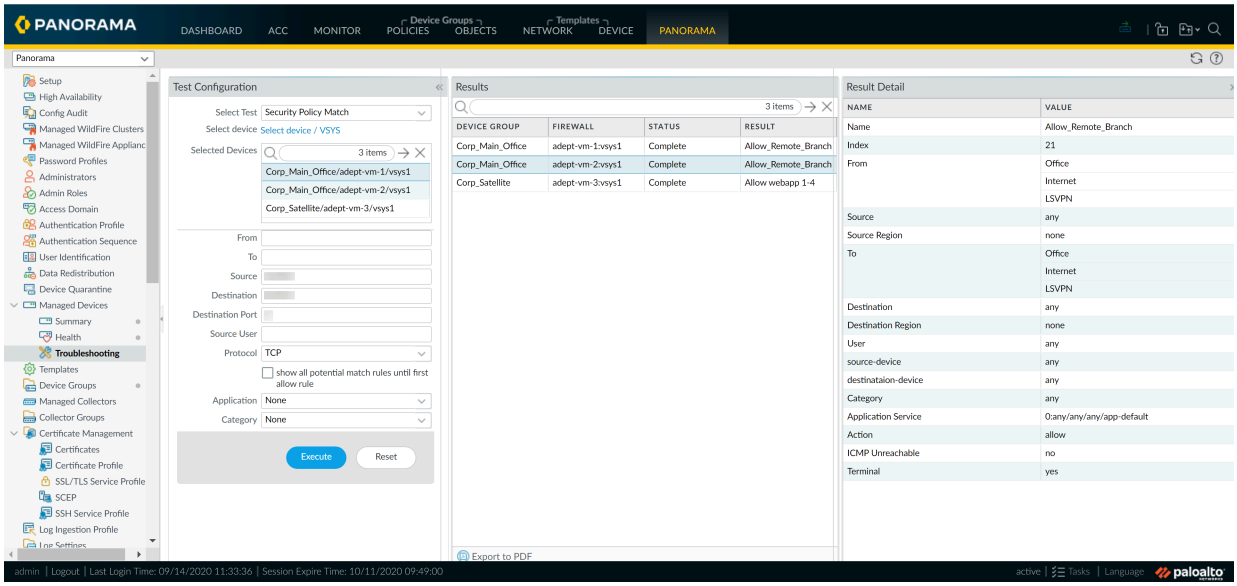
STEP 3 | Introduzca los datos precisos para ejecutar la prueba de coincidencia con políticas, en este ejemplo, con la política de seguridad.

1. Seleccione **Security Policy Match (Coincidencia con política de seguridad)** en el menú desplegable **Select Test (Seleccionar prueba)**.
2. Haga clic en **Select device / VSYS (Seleccionar dispositivo o sistema virtual)** y seleccione los cortafuegos gestionados que se deben comprobar.
3. Introduzca la dirección IP en la que se origina el tráfico.
4. Introduzca la dirección IP del dispositivo de destino del tráfico.
5. Introduzca el protocolo IP que se usa para el tráfico.
6. Si es preciso, introduzca cualquier otro dato pertinente para comprobar las reglas de la política de seguridad.

STEP 4 | Haga clic en **Execute (Ejecutar)** para comprobar la coincidencia con la política de seguridad.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | En Results (Resultados), seleccione la prueba para comprobar las reglas de la política que coinciden con los criterios especificados.



Solución de problemas de conectividad a recursos de red

Ejecute pruebas de conectividad en los cortafuegos gestionados para asegurarse de que se pueden conectar a todos los recursos de red pertinentes. Para garantizar que la red dispone de la protección adecuada, compruebe si la configuración activa que se envía a los dispositivos gestionados les permite conectarse a los recursos, por ejemplo, los recopiladores de logs, las listas dinámicas externas configuradas o el servidor de actualizaciones de Palo Alto Networks. También puede ejecutar pruebas de enrutamiento, de WildFire®, de la base de datos de amenazas, de ping y de traceroute para verificar que Panorama™ y los dispositivos gestionados tienen acceso a todos los recursos de red externos que resultan esenciales para el funcionamiento y la seguridad de la red. Una vez generados los resultados, haga clic en **Export to PDF (Exportar a PDF)** para guardarlos con fines de auditoría.

La prueba de conectividad con ping solo se admite en los cortafuegos que ejecutan PAN-OS 9.0 o versiones posteriores.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Troubleshooting (Solución de problemas)** para ejecutar una prueba de conectividad.

*También puede ejecutar pruebas de coincidencia con políticas en la pestaña **Policies (Políticas)**.*

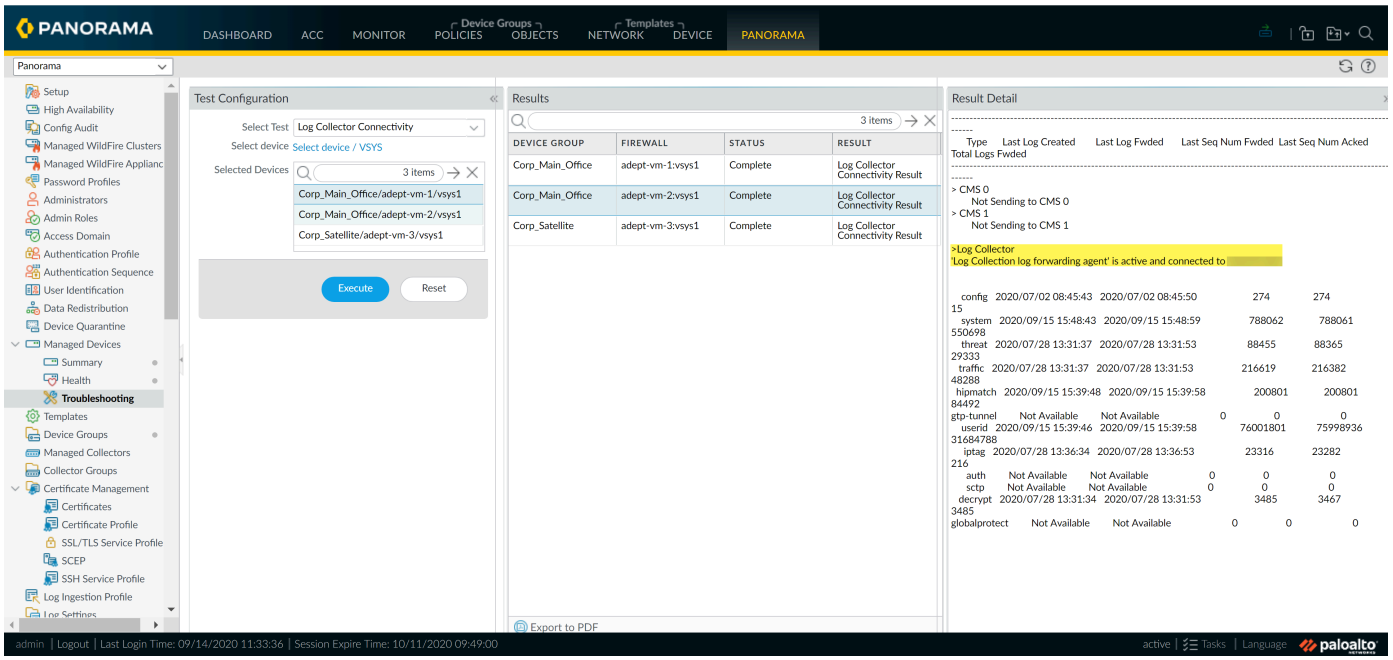
 ©2023 Palo Alto Networks, Inc.

STEP 3 | Introduzca los datos precisos para ejecutar la prueba de conectividad, en este ejemplo, de los recopiladores de logs.

1. Seleccione **Log Collector Connectivity (Conectividad de recopiladores de logs)** en el menú desplegable **Select Test (Seleccionar prueba)**.
2. Haga clic en **Select device / VSYS (Seleccionar dispositivo o sistema virtual)** y seleccione los cortafuegos gestionados que se deben comprobar.
3. Si es preciso, introduzca cualquier otro dato pertinente para comprobar la conectividad.

STEP 4 | Haga clic en **Execute (Ejecutar)** para comprobar la conectividad de los recopiladores de logs.

STEP 5 | En Results (Resultados), seleccione la prueba para comprobar el estado de conectividad de los dispositivos seleccionados.



 ©2023 Palo Alto Networks, Inc.

Cómo generar un archivo de volcado de estadísticas para un cortafuegos gestionado

Genere un conjunto de informes XML que resuman el tráfico de red de los últimos siete días para un único cortafuegos gestionado por el servidor de gestión Panorama™ o para todos los cortafuegos gestionados por Panorama. Después de seleccionar un cortafuegos gestionado y generar el archivo de volcado de estadísticas, puede descargar el archivo de volcado de estadísticas localmente en su dispositivo.

El ingeniero de sistemas de Palo Alto Networks o el socio autorizado utiliza el archivo de volcado de estadísticas para crear una revisión del ciclo de vida de seguridad (SLR) y para realizar comprobaciones de seguridad después de implementar correctamente los cortafuegos gestionados para ayudar a fortalecer su estrategia de seguridad. La SLR destaca la actividad que se encuentra en la red y los riesgos comerciales o de seguridad asociados que pueden estar presentes. Para obtener más información sobre SRL, póngase en contacto con el ingeniero de sistemas de Palo Alto Networks o de un socio autorizado.

La generación de archivos de volcado de estadísticas para varios cortafuegos gestionados puede tardar varias horas en completarse. Durante este tiempo, no puede navegar desde la interfaz de usuario de generación de archivos de volcado de estadísticas, por lo que se recomienda generar el archivo de volcado de estadísticas desde la CLI de modo que pueda continuar utilizando la interfaz web de Panorama.

Palo Alto Networks recomienda generar un archivo de volcado de estadísticas para todos los cortafuegos gestionados desde la CLI de Panorama con el siguiente comando. Panorama debe poder llegar a su servidor SCP o TFTP para exportar correctamente el archivo de volcado de estadísticas.

- ***Servidor SCP***

```
admin> scp export stats-dump to
 <username@hostname:SCP_export_path>
```

- ***Servidor TFTP***

```
admin> tftp export stats-dump to <tftp_host_address>
```

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

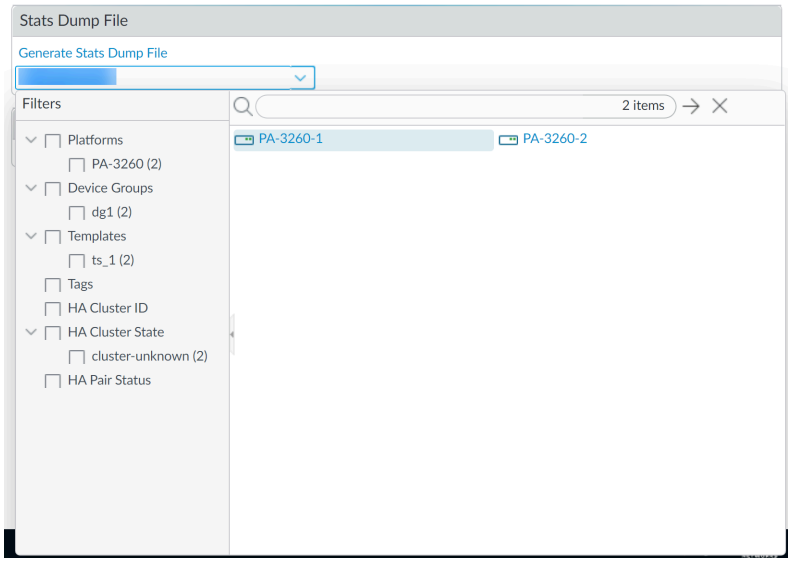
STEP 2 | Seleccione **Panorama** > **Support (Soporte)** y desplácese al **Stats Dump File (Archivo de volcado de estadísticas)**.

STEP 3 | Seleccione un cortafuegos gestionado para el cual generar un archivo de volcado de estadísticas.

Se recomienda generar un archivo de volcado de estadísticas para un único firewall administrado desde la interfaz web de Panorama.

 ©2023 Palo Alto Networks, Inc.

De forma predeterminada, se genera un archivo de volcado de estadísticas para **All devices (Todos los dispositivos)** si no selecciona un cortafuegos gestionado.



STEP 4 | **Generate Stats Dump File (Generar archivo de volcado de estadísticas)**.

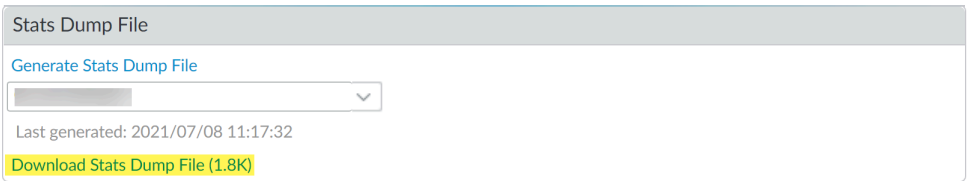
Haga clic en **Yes (Sí)** cuando se le pida que continúe generando el archivo de volcado de estadísticas.

Se muestra una barra de progreso del estado de generación del archivo de volcado de estadísticas.

La generación puede tardar hasta una hora para un único cortafuegos gestionado en función del volumen de datos de logs. No puede navegar desde la ventana de estado de generación de archivos de volcado de estadísticas durante este período.

STEP 5 | Haga clic en **Download Stats Dump File (Descargar archivo de volcado de estadísticas)** para descargar este archivo en su dispositivo local.

El archivo de volcado de estadísticas descargado está en un formato de archivo `tar.gz.`.



 ©2023 Palo Alto Networks, Inc.

Cómo recuperar la conectividad a Panorama en dispositivos gestionados

PAN-OS 10.2 introdujo la clave de autenticación de registro de dispositivos para incorporar de forma segura cortafuegos gestionados, recopiladores de logs dedicados y dispositivos WildFire al servidor de gestión Panorama™. Los pasos siguientes describen cómo recuperar la conectividad del dispositivo gestionado a Panorama en los siguientes casos:

- Si un dispositivo gestionado se desconecta de Panorama sin motivo y no puede volver a conectarse.
- Debe realizar la transición de la administración del cortafuegos de un Panorama que ejecute PAN-OS 10.2 o una versión posterior a un Panorama diferente que ejecute PAN-OS 10.2 o una versión posterior.
- Si restablece Panorama o el cortafuegos gestionado a la configuración predeterminada de fábrica, pero el cortafuegos gestionado no puede conectarse a Panorama.

La recuperación de la conectividad del dispositivo gestionado a Panorama solo se aplica a los dispositivos gestionados que ejecutan PAN-OS 10.2 cuando se incorporan a Panorama. El comportamiento descrito no se aplica a los dispositivos gestionados que ejecutan PAN-OS 10.0 y versiones anteriores o a los dispositivos gestionados que se actualizaron a PAN-OS 10.2 mientras ya estaban administrados por Panorama.

Las siguientes plataformas de cortafuegos no se ven afectadas por los problemas de conectividad descritos con Panorama.

- *Cortafuegos gestionados e integrados en Panorama con Zero Touch Provisioning (ZTP)*
- *Cortafuegos CN-Series*
- *Cortafuegos gestionados e implementados en VMware NSX*
- *Compras de cortafuegos VM-Series en un mercado de hipervisores público Consulte* cortafuegos PAYG *para obtener más información.*

©2023 Palo Alto Networks, Inc.

STEP 1 | Restablezca el estado de conexión segura del dispositivo gestionado.

1. Inicie sesión en la CLI del dispositivo gestionado.
   - Inicie sesión en la CLI del cortafuegos.
   - Inicie sesión en la CLI del recopilador de logs dedicado.
   - Inicie sesión en la CLI del dispositivo WildFire.
2. Restablezca el estado de conexión segura.

   Este comando restablece la conexión del dispositivo gestionado y es irreversible.

   ```
   admin> request sc3 reset
   ```
3. Reinicie el servidor de administración en el dispositivo gestionado.

   ```
   admin> debug software restart process management-server
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Borre el estado de conexión segura de un dispositivo gestionado en Panorama y genere una nueva clave de autenticación de registro de dispositivo.

Borrar el estado de conexión segura para un dispositivo gestionado en Panorama es irreversible. Esto significa que el dispositivo gestionado está desconectado y debe agregarse de nuevo a Panorama.

1. Inicio de sesión en la CLI de Panorama.
2. Restablezca el estado de conexión segura de un dispositivo gestionado en Panorama.

   Este comando restablece la conexión del dispositivo gestionado a Panorama y es irreversible.

   ```
   admin> clear device-status deviceid <device_SN>
   ```

   Donde **<device_SN>** es el número de serie del dispositivo gestionado para el que desea borrar el estado de conexión.
3. Cree una nueva clave de autenticación de registro de dispositivo en Panorama.

   ```
   admin> request authkey add devtype <fw_or_lc) count
    <device_count> lifetime <key_lifetime> name <key_name> serial
    <device_SN>
   ```

   *Los argumentos **devtype** y **serial** son opcionales. Omita estos dos argumentos para crear una clave de autenticación de registro de dispositivo de uso general que no sea específica de un tipo de dispositivo o número de serie de dispositivo.*
4. Compruebe que la clave de autenticación de registro de dispositivo se ha creado correctamente y copie el valor de `Key (Clave)`.

   ```
   admin> request authkey list <key_name>
   ```

STEP 3 | Añada la clave de autenticación de registro de dispositivo que creó al dispositivo gestionado.

1. Inicie sesión en la CLI del dispositivo gestionado.
   - Inicie sesión en la CLI del cortafuegos.
   - Inicie sesión en la CLI del recopilador de logs dedicado.
   - Inicie sesión en la CLI del dispositivo WildFire.
2. Añada la clave de autenticación de registro de dispositivos que creó en el paso anterior.

   ```
   admin> request authkey set <auth_key>
   ```

   En **<auth_key>**, escriba el valor de la `clave` que copió en el paso anterior.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Compruebe la conectividad del dispositivo gestionado a Panorama.

```
admin> show panorama-status
```

Compruebe que el estado `Connected (Conectado)` del servidor de Panorama muestra `yes (sí)`.

Si este procedimiento no resuelve el problema de conectividad para su dispositivo gestionado, debe ponerse en contacto con el servicio de atención al cliente de Palo Alto Networks para obtener más ayuda, ya que es posible que se requiera un restablecimiento completo de todas las conexiones de los dispositivos gestionados en Panorama.

 ©2023 Palo Alto Networks, Inc.