paloalto TECHDOCS

Implementación de CN-Series HSF

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 13, 2021

Table of Contents

CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

CN-Series Hyperscale Security Fabric (HSF) 1.0 de Palo Alto Networks es un grupo de cortafuegos de nueva generación en contenedores que ofrece una solución de cortafuegos de nueva generación altamente escalable y resistente para proveedores de servicios móviles que implementan redes 5G.

La solución HSF de la CN-Series ofrece:

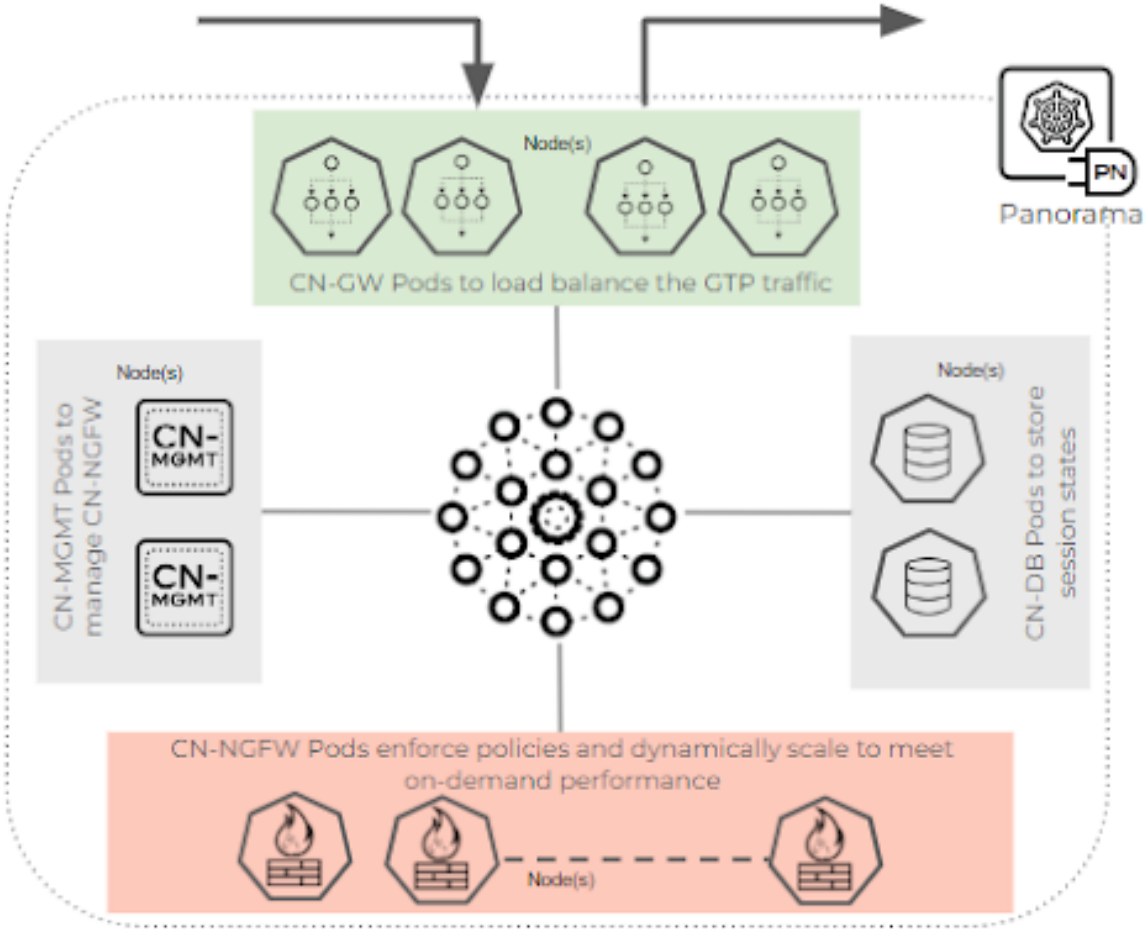
- **Hiperescalabilidad con NGFW en contenedores**: Amplía horizontalmente el rendimiento de AppID y GTP bajo demanda.
- **Altamente disponible y resistente**: Ofrece Agrupación en clústeres elástica que actúa dinámicamente en función del rendimiento y la sesión prevista, y garantiza la continuidad del negocio y la resiliencia de la sesión en todas las cargas de trabajo.
- **Elimina la dependencia del balanceador de carga externo**: Proporciona facilidad de implementación y un entorno compatible con DevOps que se puede organizar completamente a través de los complementos de Panorama.

La solución de CN-Series HSF se puede implementar en RedHat Openshift (en las instalaciones) o en un entorno de Kubernetes gestionado en la nube pública de AWS EKS.

Arquitectura de CN-Series HSF

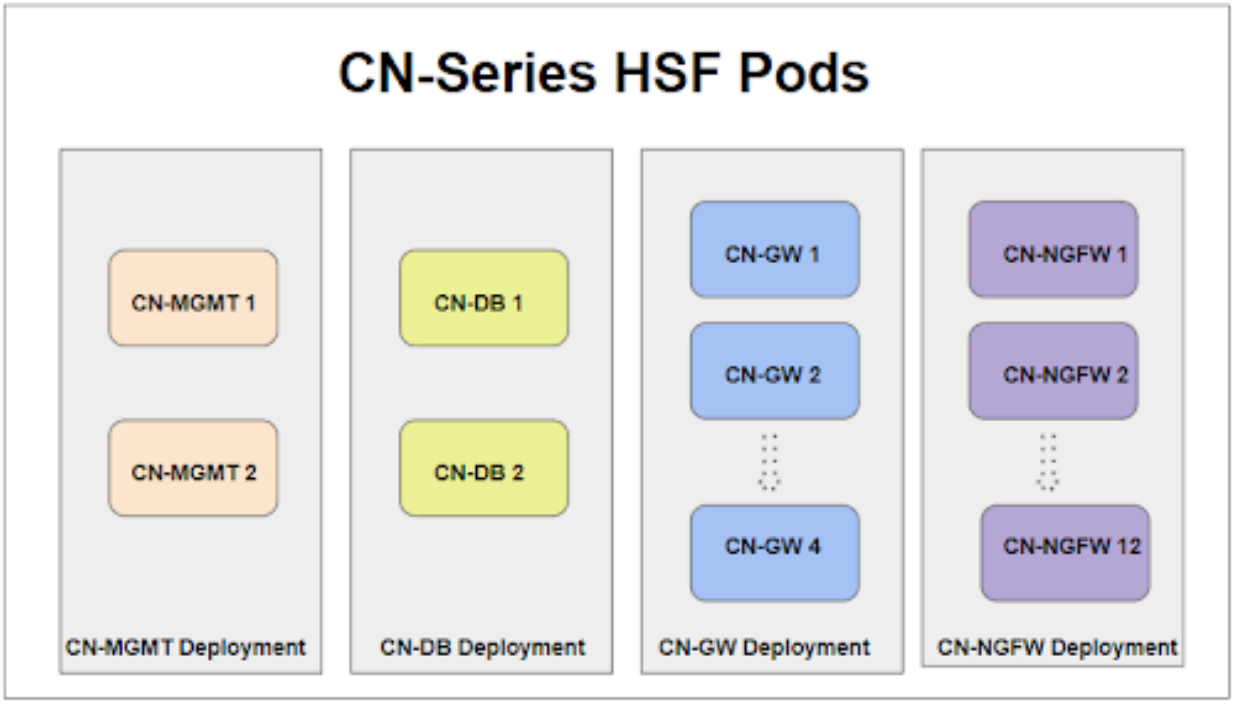
¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

El clúster de la serie CN-Series HSF consiste en un conjunto de pods CN-MGMT (gestión), CN-NGFW (plano de datos), CN-GW (puerta de enlace) y CN-DB (base de datos) conectados por redes internas. Los pods CN-MGMT proporcionan la funcionalidad del plano de gestión del clúster. Los pods CN-NGFW proporcionan la funcionalidad de seguridad del plano de datos del clúster. Los pods CN-GW son el punto de entrada al clúster y distribuyen el tráfico entre los pods CN-NGFW. Los pods CN-DB proporcionan la caché de sesión de clúster central utilizada por los pods CN-NGFW.



La CN-Series HSF admite dos contenedores CN-MGMT que proporcionan redundancia y disponibilidad. Sin embargo, solo uno de los dos contenedores CN-MGMT puede tomar conexiones de los PD de

CN-NGFW. El CN-MGMT conectado se ejecutará como un servicio StatefulSet para permitir que los CN-NGFW se conecten solo al CN-MGMT activo. El otro contenedor CN-MGMT no se conectará a contenedores CN-NGFW a menos que el CN-MGMT actual falle.



Tipos de pods

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Hay 3 tipos de pods de plano de datos en el CN-Series HSF y todos usan la misma imagen de pod de plano de datos, pero tendrán diferentes opciones de mapa de configuración. El CN-Series HSF alberga dos pods de gestión.

Pods CN-GW: el pod CN-GW es un tipo de pod de plano de datos que tiene acceso al tráfico de la red externa y gestiona el balanceo de carga del tráfico de entrada y salida. Los nodos externos solo conocerán los pods CN-GW, sus direcciones IP, y todas las subredes de datos para el tráfico están conectadas a estos pods a través de interfaces multus. El CN-Series HSF 1.0 admite un mínimo de 2 y un máximo de 4 pods CN-GW. Los pods CN-GW son de escalado estático hasta el final de la vida útil de la implementación del clúster HSF. Por ejemplo, si tenía 2 pods GW inicialmente y desea ampliar horizontalmente, mientras que los pods CN-NGFW pueden ampliar dinámicamente, tendrá que volver a implementar el clúster HSF con un número adicional de pods CN-GW.

Pods CN-DB: el pod CN-DB es un tipo de pod de plano de datos que puede consultar la propiedad de la sesión/flujo en los pods de CN-NGFW. Los pods CN-DB admiten la distribución de sesiones a diferentes CN-NGFW en base a diferentes algoritmos, como ingress-slot, round-robin y session-load. El CN-Series HSF admite dos pods CN-DB y la información de la sesión se duplica entre los dos pods CN-DB con cualquiera de los dos pods CN-DB funcionando en la consulta/enlace de flujos.

Pods CN-NGFW: el pod CN-NGFW procesa el tráfico real para las sesiones C y U, aplica políticas de seguridad y permite el escalado por separado de los pods CN-NGFW. El CN-Series HSF 1.0 admite un mínimo de 2 y un máximo de 12 pods CN-NGFW.

Pod CN-MGMT: todos los pods NGFW (CN-GW, CN-DB y CN-NGFW) están conectados a un solo pod CN-MGMT a través de IPsec en eth0.

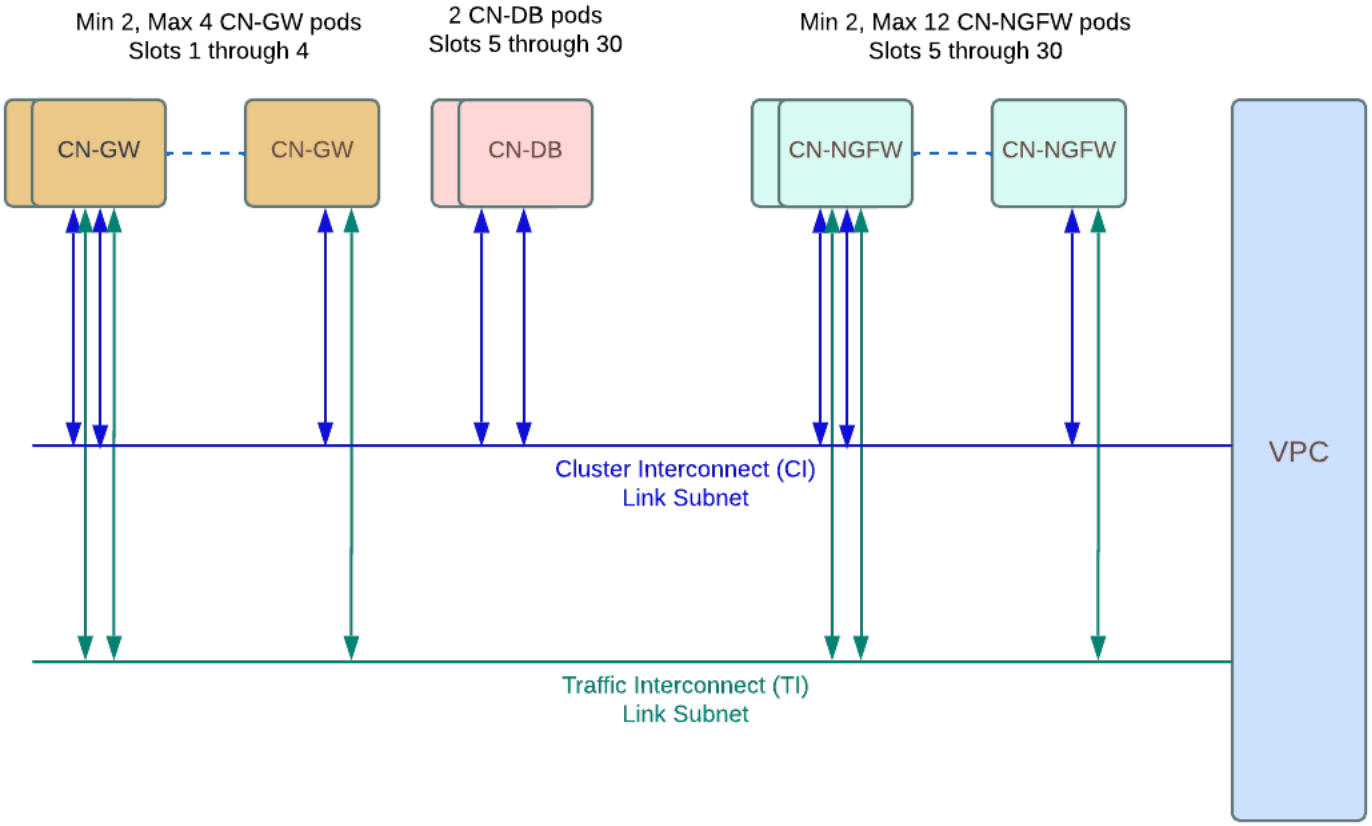
Enlaces de interconexión

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Todos los pods CN-GW, CN-DB y CN-NGFW se conectarán entre sí a través del enlace de Interconexión de clúster (CI), el cual es una interfaz multus. El enlace CI es un puerto de datos reservado para la comunicación del clúster y el reenvío de paquetes entre los miembros del clúster. Ethernet x/1 se utiliza para los enlaces de CI en todos los pods relevantes. El enlace CI también se puede utilizar para reenviar tráfico de un CN-NGFW a otro.

Los pods CN-GW y CN-NGFW están conectados entre sí a través del enlace Interconexión de tráfico (TI), el cual es una interfaz múltiple. El enlace TI es un puerto de datos reservado para el tráfico interno dentro del clúster. Ethernet x/2 se usa para los enlaces de TI en todos los pods relevantes.

En los pods CN-GW, Ethernet x/3 se utilizará en adelante como interfaces externas que se conectan a la red del cliente.



El CN-Series HSF solo admite el protocolo IPv4.

Para el entorno local, se necesita un servidor DHCP o IPAM para asignar direcciones IP a las interfaces CI y TI. Para AWS EKS, el servidor DHCP es parte de la infraestructura subyacente. Por lo tanto, las direcciones IP se asignan automáticamente a las interfaces de CI y TI en entornos de nube.

Autorización de licencia para el CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

El complemento de Kubernetes en Panorama gestiona la concesión de licencias del cortafuegos CN-Series. Las licencias de los cortafuegos de la serie CN-Series se basan en el número total de vCPU (núcleos) utilizadas por los pods CN-NGFW, CN-GW y CN-DB implementados en su entorno de Kubernetes. Se consume un token por cada vCPU utilizada por estos pods.

- Activación de créditos
- Creación de un perfil de implementación del CN-Series HSF
- Gestión de perfiles de implementación

Activación de créditos

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versiones superiores • Helm 3.6 or above version client

Dentro de su organización puede crear muchas cuentas, cada una con un propósito distinto. Durante la activación, solo puede elegir una cuenta por grupo de crédito predeterminado. Una vez que el grupo de créditos está activo, los usuarios a los que se les concedió la función de administrador de créditos pueden asignar los créditos para las implementaciones e incluso transferir créditos a otros grupos.

Si tiene una cuenta CSP existente y es un superusuario o un administrador, el sistema añade automáticamente la función de administrador de crédito a su perfil. Si no tiene una cuenta existente, el CSP crea automáticamente una cuenta para usted y añade la función de administrador de crédito a su perfil.

Usted (el comprador) recibe un correo electrónico detallando la suscripción, el ID del grupo de créditos, la fecha de inicio y finalización de la suscripción, la cantidad de créditos comprados y la descripción del grupo de créditos predeterminado (el grupo de créditos creado cuando activa sus créditos).

Guarde este correo electrónico en un sitio seguro para futuras referencias.

STEP 1 | En el correo electrónico, haga clic en **Start Activation (Iniciar activación)** para ver los grupos de crédito disponibles.

STEP 2 | Seleccione el grupo de créditos que desea activar. Puede usar el campo de búsqueda para filtrar su lista de cuentas por número o nombre.

Si ha comprado varios grupos de crédito, ambos se seleccionan automáticamente. Las marcas de verificación representan los enlaces de activación para los créditos de incorporación.

Se le solicitará una autenticación o inicio de sesión.

Si anula la selección de un grupo de créditos, verá un recordatorio que le pregunta si desea activar esos créditos, debe volver al correo electrónico y hacer clic en el vínculo ***Start Activation (Iniciar activación)****.*

STEP 3 | Seleccione **Start Activation (Iniciar activación)**.

STEP 4 | Seleccione la cuenta de soporte (puede buscar por número de cuenta o nombre).

STEP 5 | Seleccione el grupo de créditos predeterminado.

STEP 6 | Seleccione **Deposit Credits (Depositar créditos)**.

Verá un mensaje que indica que el depósito se realizó correctamente.

STEP 7 | (opcional) Si esta es su primera activación de crédito, verá el cuadro de diálogo Create Deployment Profile (Crear perfil de implementación).

Creación de un perfil de implementación del CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Utilice el siguiente procedimiento para crear un perfil de implementación de CN-Series.

STEP 1 | Si ya tiene un grupo de créditos, inicie sesión en la cuenta y, desde el panel de control, seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de software de NGFW)** > **Prisma NGFW Credits (Créditos de NGFW Prisma)** > **Create New Profile (Crear nuevo perfil)**.

Si acaba de activar un grupo de créditos, verá el formulario **Create Deployment Profile (Crear perfil de implementación)**.

1. Seleccione el tipo de cortafuegos **CN-Series**.
2. Seleccione el **PAN-OS 11.0**.
3. Haga clic en **Next (Siguiente)**.

STEP 2 | Perfil de la serie CN-Series.

1. **Nombre de perfil**.

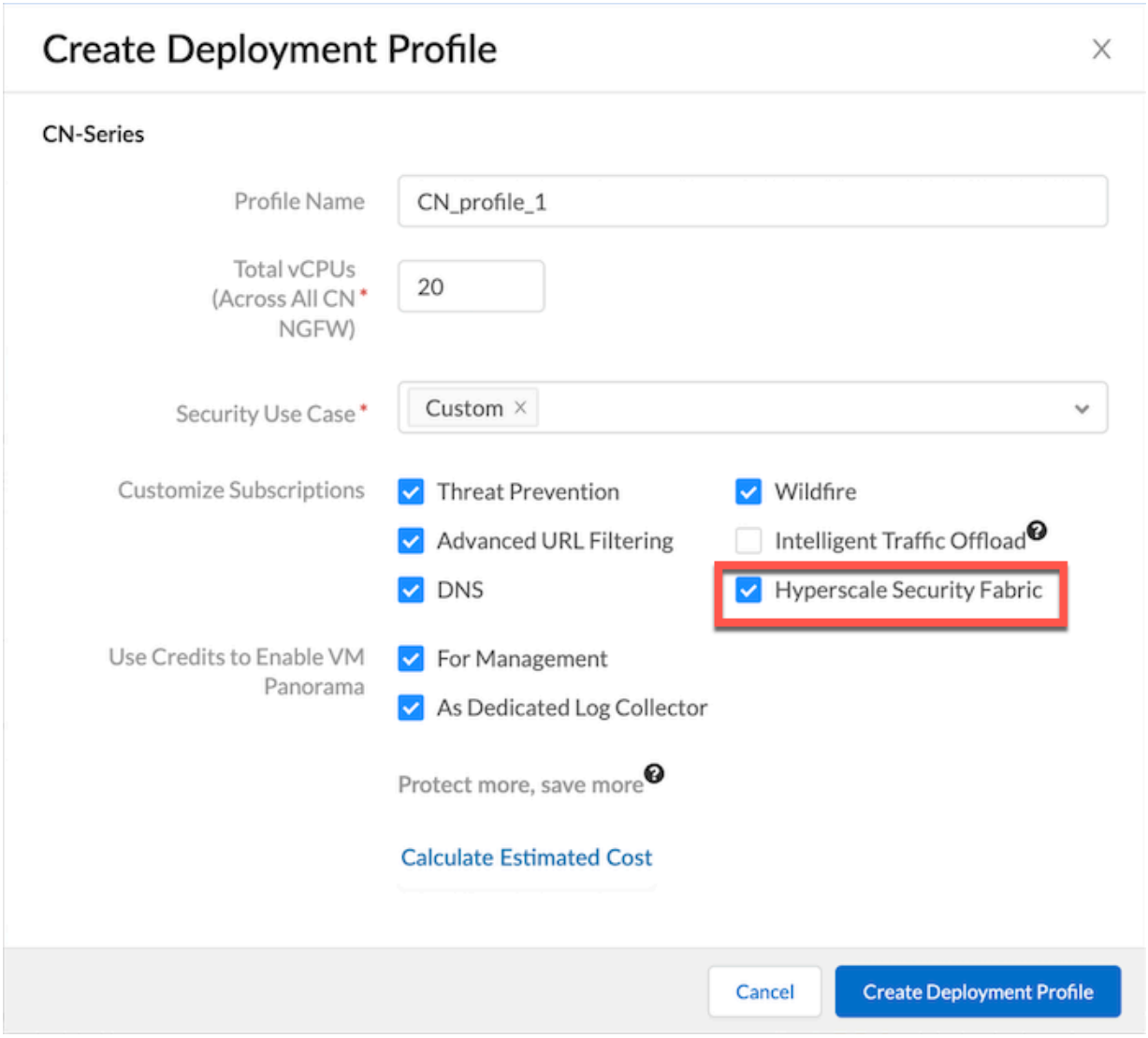
   Asigne un nombre al perfil.

2. **vCPU totales**

   Introduzca el número total de CPU virtuales necesarias en todos los pods (CN-NGFW, CN-GW y CN-DB).

3. Seleccione un caso de uso de seguridad en el menú desplegable. Cada caso de uso de seguridad en el menú desplegable selecciona automáticamente una serie de descripciones que se recomiendan para el caso de uso seleccionado. Si selecciona Personalizado, puede especificar las suscripciones que desea usar en su implementación.
4. Seleccione **Hyperscale Security Fabric** en **Customize Subscriptions (Personalizar suscripciones)** para habilitar HSF en su suscripción.
5. (opcional) **Use Credits to Enable VM Panorama (Utilice Créditos para habilitar VM Panorama)**: Para **Management (Administración)** o **Dedicated Log Collector (Recopilador de logs dedicado)**.

STEP 3 | Haga clic en **Calculate Estimated Cost (Calcular coste estimado)** para ver el total de crédito y el número de créditos disponibles antes de la implementación.



Gestión de perfiles de implementación

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Puede editar, clonar o eliminar perfiles de implementación de CN-Series en función de los requisitos de su implementación de la serie CN-Series. Además, puede añadir o quitar suscripciones del perfil de implementación una vez creado. Para obtener más información, consulte Gestión de perfiles de implementación.

Requisitos del sistema de CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

- Matriz de capacidad y sistema de CN-Series HSF recomendados
- Tipo CN-Series HSF recomendado
- Compatibilidad con el modo jumbo de la serie CN-Series HSF

Matriz de capacidad y sistema de CN-Series HSF recomendados

Estos son nuestros requisitos de sistema recomendados para el CN-Series HSF.

La siguiente tabla separa los datos por tamaños de CN-Series: pequeño, mediano y grande. La inspección de rendimiento que puede realizar el CN-Series HSF varía según el tamaño del clúster.

- **CN-Series pequeño para HSF**
- **CN-Series Mediano para HSF**
- **CN-Series grande para HSF**

El CN-Series HSF de la serie CN-Series requiere dos grupos de nodos: CN-MGMT y CN-DB con dos nodos cada uno. El número de nodos necesarios para los grupos de nodos CN-GW y CN-NGFW depende del rendimiento.

Tipo de clúster		Pequeño	Intermedia	Grande
CN-GW	Núcleos	24	24	24
	Memoria	16 GB	20 GB	24 GB
	Ancho de banda	50 Gbps	100 Gbps	100 Gbps
	Tipo de instancias	c5n.9xlarge (36vCPU, 96Gi)	c5n.18xlarge	c5n.18xlarge
CN-DB	Núcleos	8	8	12
	Memoria	0,64 x 12 x MaxSession (en millones) GB	0,64 x 12 x MaxSession (en millones) GB	0,64 x 10 x 10 GB
	Ancho de banda	10 GbE	25 GbE	25 GbE

Tipo de clúster		Pequeño	Intermedia	Grande
	Tipo de instancias	c5n.4xlarge (16vCPU, 42Gi)	c5n.4xlarge	c5n.9xlarge
CN-MGMT	Núcleos	4	12	12
	Memoria	16 GB	16 GB - 24 GB	16 GB - 24 GB
	Ancho de banda	10 GbE	10 GbE	10 GbE
	Disco	56 Gi	80 Gi	80 Gi
	Tipo de instancias	c5n.4xlarge (8vCPU, 21Gi)	c5n.4xlarge o c5d.9xlarge	c5n.4xlarge o c5d.9xlarge
CN-NGFW	Núcleos	15	24	24 - 36
	Memoria	20 GB	16 GB - 47 GB	48 GB (56 GB para núcleos > 32)
	Ancho de banda	25 GbE	50 GbE	50 GbE
	Tipo de instancias	c5n.4xlarge (16vCPU, 42Gi)	c5n.9xlarge	c5n.9xlarge

Tipo CN-Series HSF recomendado

Tipo de clúster	Número de nodos			Número total de interfaces	Número mínimo de interfaces
	Pequeño	Intermedia	Grande		
CN-GW	2	3	4	4-15	4
CN-DB	2	2	2	2	2
CN-MGMT	2	2	2	1	1
CN-NGFW	6	8	10	3	3
CN-NGFW adicional para cubrir el fallo de DP	2	2	2	-	-

Compatibilidad con el modo jumbo de la serie CN-Series HSF

Cuando la compatibilidad con jumbo está habilitada, Panorama configura la unidad de transmisión máxima (MTU) para todas las interfaces en el no CN-MGMT a 8744 bytes.

La MTU del sistema es de 9000 bytes en modo jumbo y las interfaces heredarán la MTU del sistema si no se especifica la MTU.

En los hosts de EKS, el valor de MTU predeterminado para las instancias de AWS EC2 es 9000. Por lo tanto, no se necesita una configuración en el lado del host.

Cuando la compatibilidad con jumbo está deshabilitada, Panorama configura la unidad de transmisión máxima (MTU) para todas las interfaces en el no CN-MGMT a 1756 bytes.

Debe hacer coincidir sus valores de MTU jumbo y no jumbo en sus entornos EKS con los valores de MTU de Panorama.

Modo	MTU (bytes)
Jumbo	EKS—9000 bytes
No Jumbo	1756 bytes para todas las interfaces

Requisitos previos para implementar el CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Los siguientes son los requisitos previos para implementar el CN-series HSF:

- Requisitos del clúster
- Preparación del clúster
- Preparación de Panorama para la implementación de CN-Series HSF

Requisitos del clúster

Necesitará un clúster de Kubernetes con los permisos necesarios para crear y gestionar grupos de nodos. También necesitará los recursos necesarios para que el complemento Kubernetes abra el clúster CN-Series.

Debe configurar lo siguiente como requisitos previos del clúster:

- Clúster de EKS u Openshift (4.10), dependiendo del entorno que tenga, deberá crear las VPC y las subredes y configurar la función de IAM necesaria para abrir el clúster de EKS.

  Para obtener información sobre cómo crear un clúster de EKS, consulte Creación de un clúster de Amazon EKS.

  Para obtener información sobre la creación de un clúster de Openshift, consulte Instalación de un clúster de Openshift.
- Kubernetes versión 1.22 o posterior.

  Para obtener información, consulte Instalación de Kubernetes con herramientas de implementación.
- Multus CNI para permitir la conexión de múltiples interfaces de red a pods en Kubernetes.

  Para obtener más información, consulte Instalación de Multus CNI.
- Cuatro grupos de nodos con los requisitos mínimos como se indica en los Requisitos del sistema de CN-Series.

Preparación del clúster

Deberá configurar lo siguiente:

- Grupo de nodos y nodos
- Etiquetas de nodo
- Cuenta de servicio
- Interfaces

Grupo de nodos y nodos

Necesitará un mínimo de 8 nodos para gestionar la topología y acoplar todos los pods en la solución. Palo Alto Networks recomienda 4 conjuntos de grupos de nodos con un mínimo de dos nodos cada uno. Asegúrese de no permitir que el grupo de nodos MP se superponga con el resto de los 3 grupos de nodos.

Si desea utilizar DPDK, debe tener una AMI con los controladores DPDK configurados. Para obtener más información, consulte Configuración de DPDK en AWS EKS.

Una vez que tenga el clúster de EKS en ejecución, utilice la plantilla de CloudFormation con Multus para mostrar el grupo de nodos y las instancias EC2 con tipos de nodos.

```
lnehru@lnehru-parts-vm:~/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common$ kubectl get nodes
NAME                                          STATUS   ROLES    AGE     VERSION
ip-10-101-201-125.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-204.us-west-1.compute.internal   Ready    <none>   3d23h   v1.22.12-eks-ba74326
ip-10-101-201-223.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-226.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-81.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-159.us-west-1.compute.internal   Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-163.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-21.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-51.us-west-1.compute.internal    Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-66.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-221-78.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-90.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-222-149.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-175.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-176.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-213.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-38.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-6.us-west-1.compute.internal     Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-77.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-96.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
```

Etiquetas de nodo

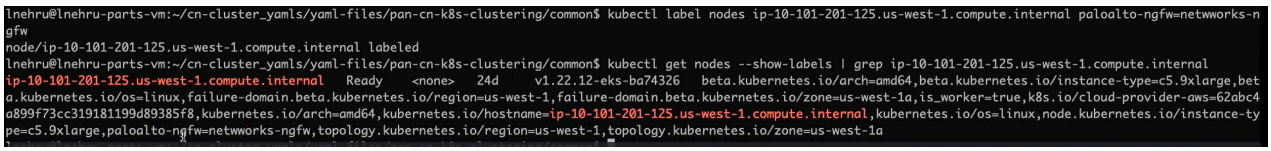
Utilice los siguientes comandos para etiquetar todos los nodos:

```
kubectl label node (MP_node_name) Panw-mp=Panw-mp
kubectl label node (DB_node_name) Panw-db=Panw-db
kubectl label node (GW_node_nam) Panw-gw=Panw-gw
kubectl label node (NGFW_node_name) Panw-ngfw=Panw-ngfw
```

Los siguientes son ejemplos de etiquetas de nodo:

```
CN-NGFW - paloalto-ngfw: networks-ngfw
CN-MGMT - paloalto-mgmt: networks-mgmt
CN-GW - paloalto-gw: networks-gw
CN-DB - paloalto-db: networks-db
```

Se espera que se proporcione un par clave-valor para cada tipo de nodo. Además, se recomienda un valor de clave paloalto y valor networks. Sin embargo, si elige cambiar las etiquetas de los nodos, también deberá realizar los cambios correspondientes en la configuración.



Después de etiquetar los nodos, descargue los YAML necesarios para activar el clúster.

Cuenta de servicio

Los permisos extendidos para implementaciones se proporcionan mediante una cuenta de servicio yaml. Para crear las cuentas de servicio, su clúster de Kubernetes debería estar listo.

1. Ejecute la cuenta de servicio YAML para `plugin-deploy-serviceaccount.yaml`.

   La cuenta de servicio habilita los permisos que Panorama requiere para autenticarse en el clúster para recuperar las etiquetas de Kubernetes y la información de recursos. Esta cuenta de servicio se denomina pan-plugin-user de forma predeterminada.
2. Vaya a yaml-files/clustering folder/common e implemente lo siguiente:

   ```
   kubectl apply -f plugin-deploy-serviceaccount.yaml
   ```

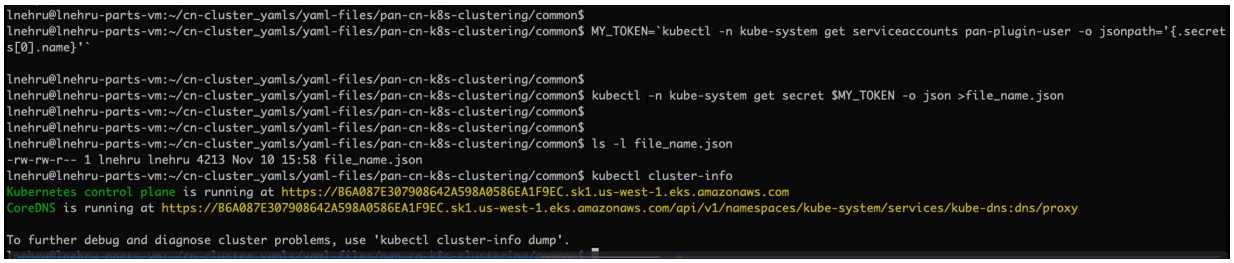
   ```
   kubectl apply -f pan-mgmt-serviceaccount.yaml
   ```

   ```
   kubectl -n kube-system get secrets | grep pan-plugin-user-token
   ```

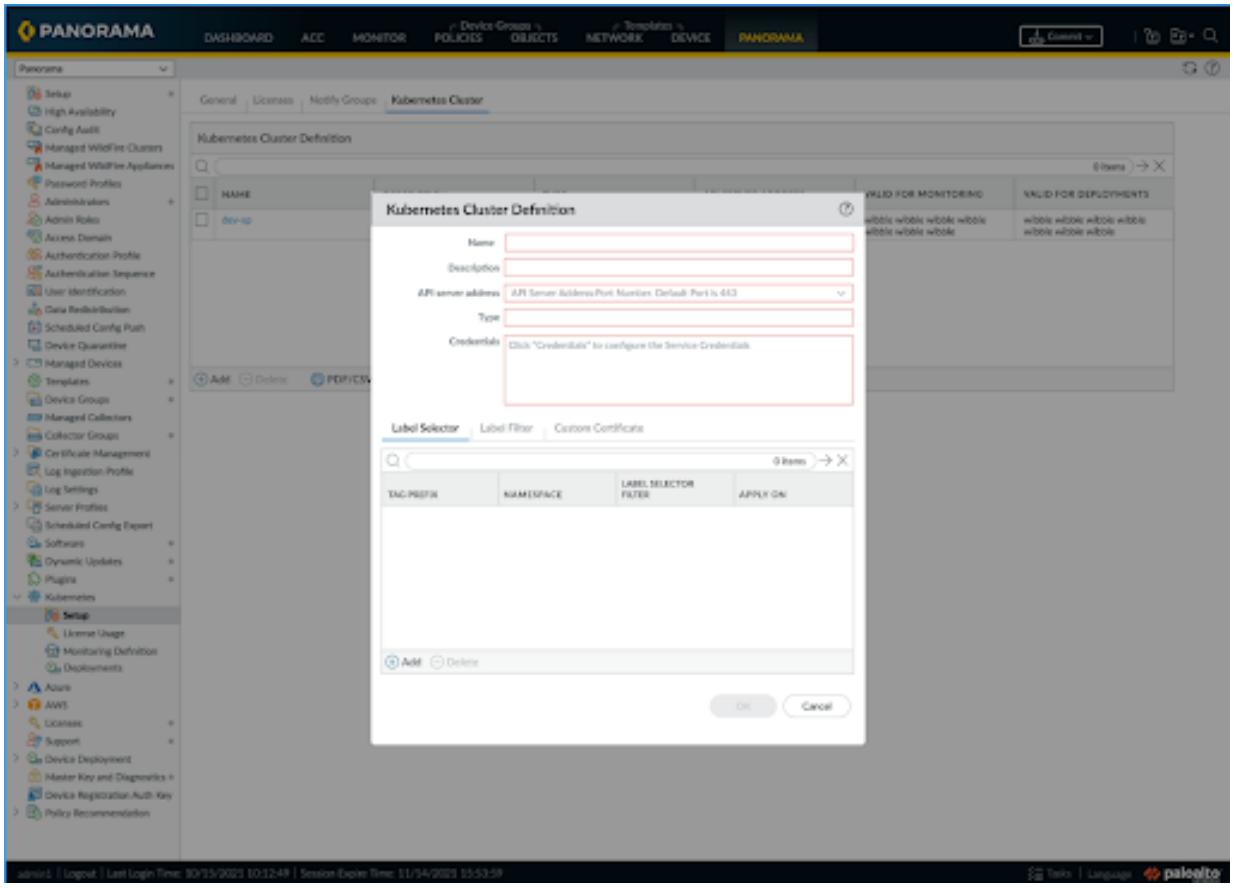
   Cree el archivo de credenciales, cred.json, por ejemplo, que incluye los secretos y guarde este archivo. Debe cargar este archivo en Panorama para configurar el complemento de Kubernetes para supervisar los clústeres.

3. Para ver los secretos asociados con esta cuenta de servicio.

```
kubectl -n kube-system get secrets (secrets-from-above-command) -o
json >> cred.json
```



4. Cargue cred.json en el complemento de kubernetes y verifique el estado de validación.



Después de la primera confirmación de publicación de validación en Panorama, el complemento continuará invocando la lógica de validación a intervalos regulares y actualizará el estado de validación en la interfaz de usuario.

Interfaces

Deberá crear los ENI necesarios para CN-DB, CN-NGFW y CN-GW. Identifique los ID de bus PCI de estas interfaces que luego se utilizarán para crear definiciones de adjuntos de red para interconectar los pods.

1. Acceda con SSH en el nodo usando la clave/usuario que creó al crear un clúster.

   ```
   ssh ec2-user@(node_ip) -i private_(key)
   ```

2. Instale el paquete ethtool.

   ```
   Sudo yum install ethtool
   ```

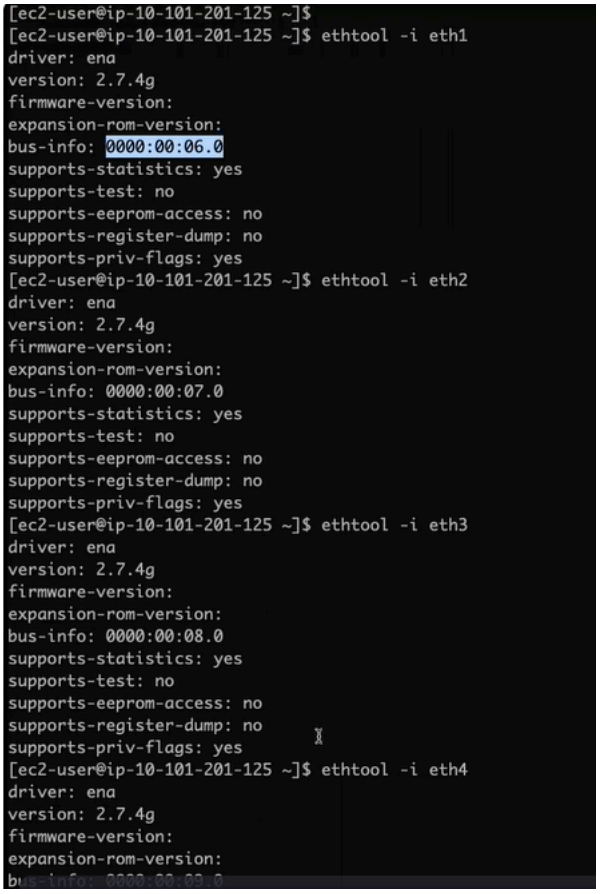
   ```
   sudo yum update -y && sudo yum install ethtool -y
   ```


3. Identifique el nombre de la interfaz.

   ```
   ifconfig
   ```

4. Identifique el ID de bus PCI de la interfaz para implementar la conectividad de red en los pods.

   ```
   ethtool -i (i/f)
   ```



Aquí eth0 es la interfaz de gestión del nodo, eth1 es la interfaz CI, eth2 es TI, eth3 Interfaz externa 1, eth4 Interfaz externa 2. En el nodo etiquetado para CN-MGMT, encontrará solo la interfaz eth0 para gestión. Para CN-DB, tendrá eth1, para CN-NGFW, tendrá eth1, eth2 y para CN-GW tendrá eth1, eth2 y tantas interfaces externas como haya creado en su entorno.

```
    net-attach-1 - 0000:00:08.0 net-attach-2 - 0000:00:09.0 net-
attach-def-ci-db - 0000:00:06.0 net-attach-def-ci-gw - 0000:00:06.0
 net-attach-def-ci-ngfw - 0000:00:06.0 net-attach-def-ti-gw -
 0000:00:07.0 net-attach-def-ti-ngfw - 0000:00:07.0
```

Todos los pods de una implementación deben estar en nodos diferentes, ya que usarían las mismas definiciones de conexión de red y, por lo tanto, cada pod necesita acceso a la misma ID de bus PCI. Por ejemplo, si net-attach utiliza PCI ID 6 para el enlace de CI del pod C/U, entonces cada pod C/U debe colocarse en un nodo que tenga una interfaz PCI ID 6 de la misma subred.

5. Modifique el ID de bus PCI en el YALM de definición de adjunto de red.

```
   { "cniVersion": "0.3.1", "type": "host-device", "pciBusID":
"0000:00:07.0" }
```

Aquí, el primer enlace eth1 se usa como CI, eth2 se usa como TI y eth3 en adelante se usa para enlaces externos.

6. Aplique los archivos YAML de requisitos previos.

```
kubectl apply -f pan-mgmt-serviceaccount.yaml
kubectl apply -f net-attach-def-1.yaml
kubectl apply -f net-attach-def-2.yaml
kubectl apply -f net-attach-def-ci-db.yaml
kubectl apply -f net-attach-def-ci-gw.yaml
kubectl apply -f net-attach-def-ci-ngfw.yaml
kubectl apply -f net-attach-def-ti-gw.yaml
kubectl apply -f net-attach-def-ti-ngfw.yaml
```

En Openshift, aplique `Kubectl apply -f ctrcfg-pidslimit.yaml`. Para obtener más información sobre pidlimit, consulte Tareas de configuración.

Si se utilizan PV estáticos, cree los volúmenes de montaje de PV estáticos en nodos etiquetados para pods CN-MGMT.


```
/mnt/pan-local1, /mnt/pan-local2, /mnt/pan-local3, /mnt/pan-local4, /
mnt/pan-local5, /mnt/pan-local6
```

Preparación de Panorama para la implementación de CN-Series HSF

La configuración y la implementación del CN-Series HSF se realizan a través de Panorama. Antes de implementar el CN-Series HSF, asegúrese de haber completado los siguientes requisitos previos.

STEP 1 | Implemente un Panorama con la versión de software 11.0 e instale la versión mínima de contenido.

1. Vaya a **Panorama** > **Dynamic Updates (Actualizaciones dinámicas)** para ver la versión mínima de lanzamiento de contenido en PAN-OS 11.0.

   Consulte Notas de la versión de PAN-OS .

2. Vaya a **Panorama** > **Software** para obtener la versión del software.

   Localice y descargue el archivo específico del modelo para la versión de lanzamiento a la que está actualizando. Por ejemplo, para actualizar un dispositivo M-Series a Panorama 11.0.0, descargue la imagen Panorama_m-11.0.0; para actualizar un dispositivo virtual Panorama a Panorama 11.0.0, descargue la imagen Panorama_pc-11.0.0.

   Después de una descarga correcta, la columna **Acción** cambia de Descargar a Instalar para instalar la imagen descargada.

STEP 2 | Compruebe que su Panorama está en Modo Panorama si desea que Panorama recopile los logs del cortafuegos.

STEP 3 | Instale la versión 4.0 del complemento de Kubernetes en Panorama. Si los dispositivos Panorama se implementan como una pareja de alta disponibilidad (HA), primero se debe instalar el complemento de Kubernetes en el equipo principal (activo).

1. Inicie sesión en la interfaz web de Panorama y seleccione **Panorama** > **Plugins (Complementos)** y haga clic en **Check Now (Comprobar ahora)** para obtener la lista de complementos disponibles.
2. Seleccione **Download (Descargar)** e **Install (Instalar)** para instalar la versión 4.0 del complemento de Kubernetes.

   Después de realizar la instalación del complemento correctamente, Panorama se actualiza y el complemento de Kubernetes aparece en la pestaña **Panorama**.

   Si Panorama se implementa en un par de alta disponibilidad, instale el complemento de Kubernetes en el Panorama secundario (pasivo) mediante los pasos anteriores descritos en el Paso 3.

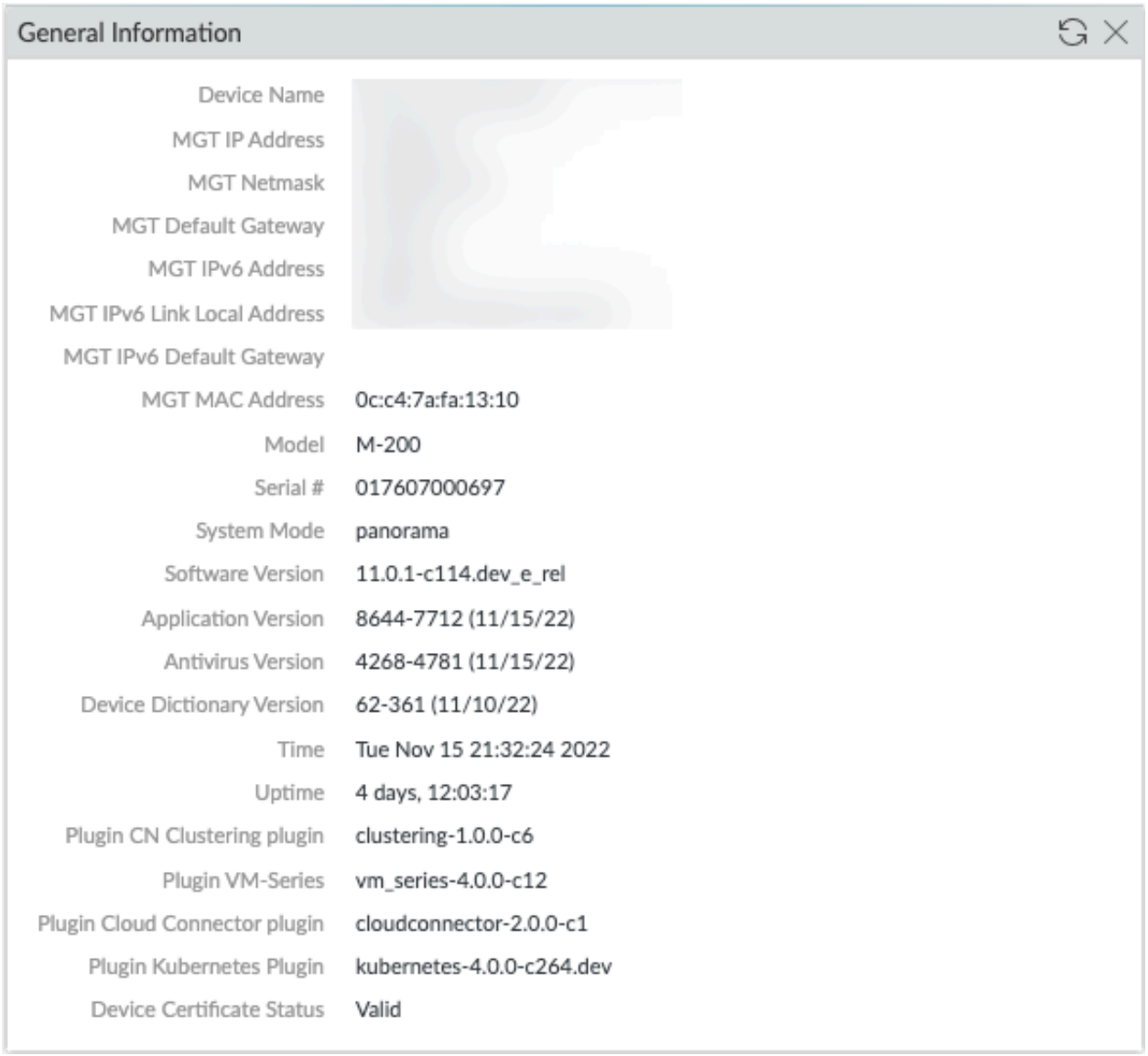
3. Haga clic en**Commit to Panorama (Confirmar en Panorama)**.

   La confirmación crea una plantilla **K8S-CNF-Clustering-Readonly** para usar con el CN-Series HSF. Las interfaces pueden tardar hasta un minuto en mostrarse en Panorama. Esta plantilla tiene la configuración de red del enlace de interconexión de clúster (CI) preconfigurado para los pods CN-GW, CN-DB y CNNGFW y el enlace de interconexión de tráfico (TI) para los pods CN-GW y CN-NGFW. **K8S-CNF-Clustering-Readonly** crea 30 enrutadores lógicos y dos interfaces por

cada enrutador lógico. Ethernet x/1 son enlaces de interconexión de clúster (CI), mientras que Ethernet x/2 son enlaces de interconexión de clúster (TI).

*Asegúrese de no cambiar el nombre de la plantilla **K8S-CNG-Clustering-Readonly** .*

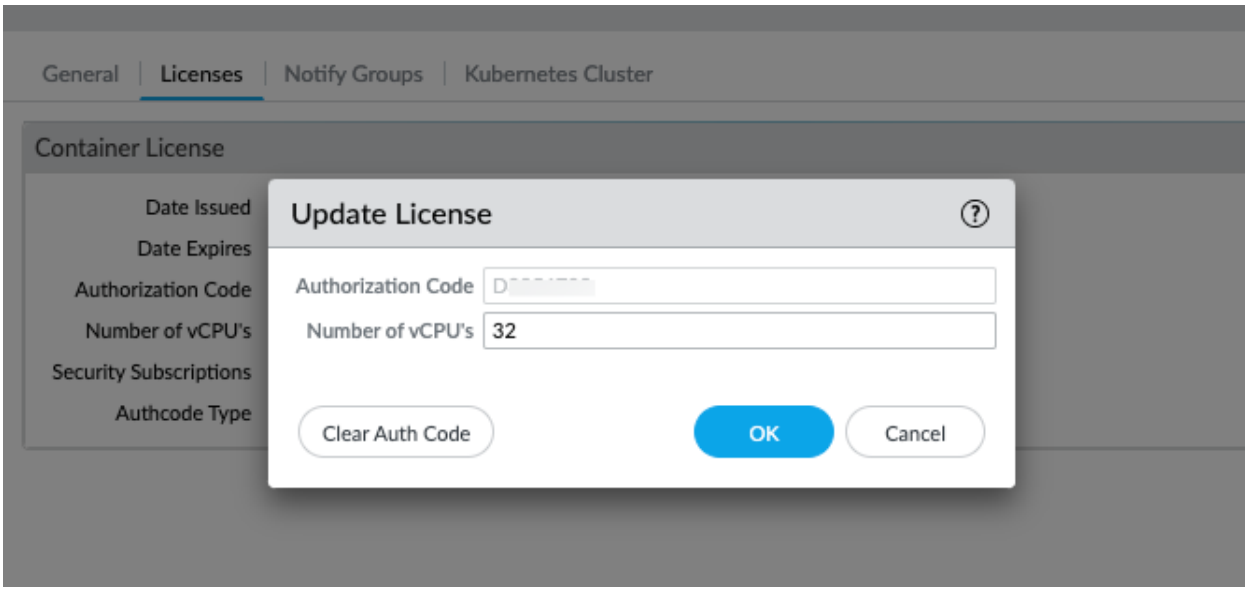
También puede comprobar el widget de Información general en el **Dashboard (Panel)** > **General Information (Información General)** de Panorama.



STEP 4 | Obtenga los créditos de licencia de la serie CN-Series HSF en Panorama.

1. Seleccione **Panorama** > **Plugins (Complementos)** > **Kubernetes** > **Setup (Configuración)** > **Licenses (Licencias)**.
2. Seleccione **Activate/update using authorization code (Activar/actualizar mediante el código de autorización)** e introduzca el código de autorización y el número total de vCPU de

plano de datos necesarias. Debe Crear un perfil de implementación para obtener su código de autenticación de CN-Series.



Cuando la serie CN-Series se implementa con HSF, si el número de pods (CN-NGFW, CN-GW y CN-DB) implementados supera el número de CPU virtuales asignadas, tiene un período de gracia de cuatro horas para añadir más CPU virtuales a su perfil de implementación o eliminar suficientes pods. Si no asigna vCPU adicionales ni elimina pods sin licencia dentro del período de gracia de cuatro horas, los pods se reiniciarán y crearán una interrupción del tráfico. Los pods que ya tienen licencia siguen teniendo licencia.

3. Verifique que el número de créditos de licencia disponibles esté actualizado.

STEP 5 | Cree un Grupo de dispositivos principal.

Debe crear un grupo de dispositivos con las políticas y los objetos necesarios para el CN-Series HSF. Debe hacer referencia a este grupo de dispositivos cuando implemente el CN-Series HSF.

1. Vaya a **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.
3. 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.
4. Haga clic en **OK (Aceptar)**.

   El nombre del grupo de dispositivos se carga en el pod CN-MGMT en el clúster. Cuando los pods CN-MGMT se conectan a Panorama con estos parámetros de arranque, el grupo de dispositivos se asocia con el nombre del clúster en la configuración del clúster. Para Alta disponibilidad (HA) de Panorama, el pod CN-MGMT envía actualizaciones a los Panorama activos y pasivos. La información del clúster se completa automáticamente para los pods CN-NGFW, CN-DB y CN-GW cuando estos están activos.
5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar y enviar la configuración del grupo de dispositivos a Panorama.

STEP 6 | Cree una plantilla variable para habilitar el flujo de tráfico.

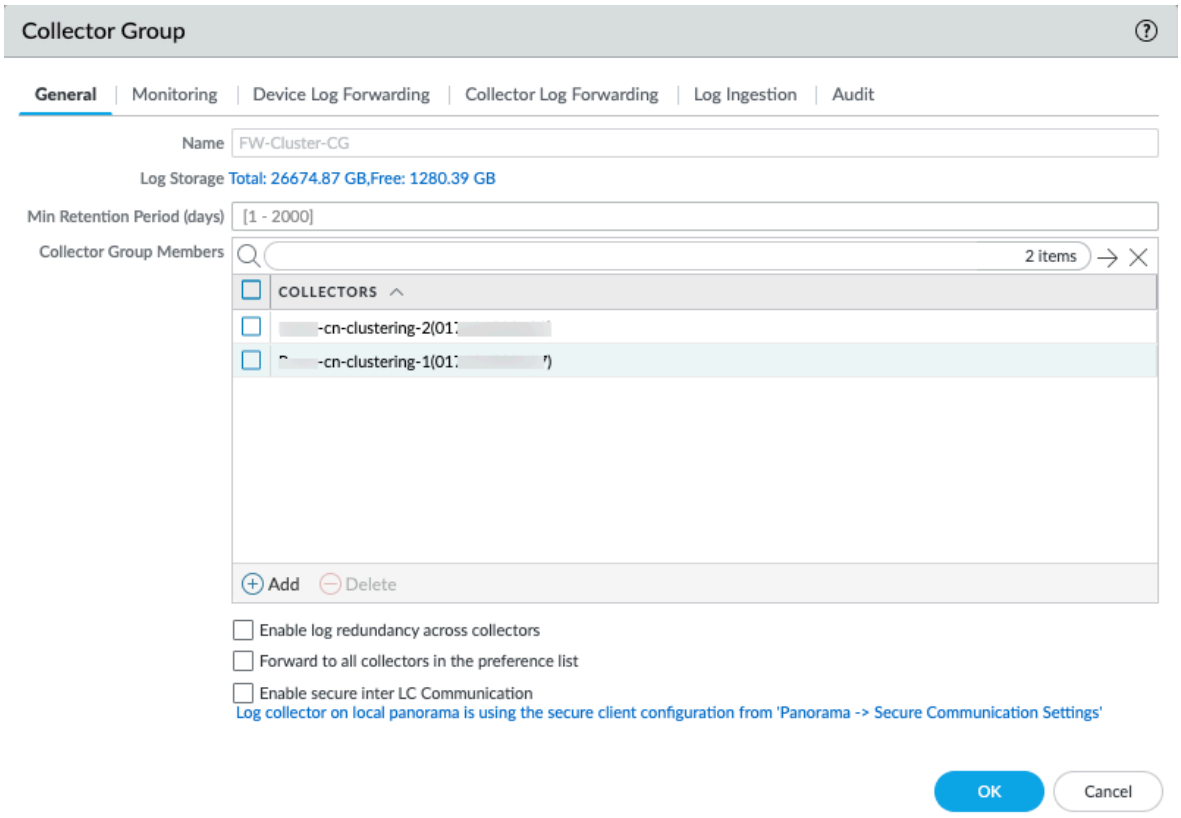
1. Vaya a **Panorama** > **Templates (Plantillas)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** único para la plantilla.
3. Introduzca una **Description (Descripción)** opcional.
4. Configure la plantilla variable para habilitar el flujo de tráfico.

Puede configurar esta plantilla antes o después de implementar el CN-Series HSF.

STEP 7 | Cree un Recopilador de log y añádalo a un Grupo de recopiladores de logs.

1. Vaya a **Panorama** > **Collector Groups (Grupos de recopiladores)** y haga clic en **Add (Añadir)** para añadir un grupo de recopiladores.
2. Introduzca un nombre en **Name (Nombre)** para el grupo de recopiladores.
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. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y al Grupo de recopiladores que configuró.

El complemento de Kubernetes creará y gestionará la clave de autenticación de Panorama.

Implementación del clúster HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Después de asegurarse de que se cumplen los requisitos previos para implementar el cortafuegos CN-Series como un HSF, vaya a **Kubernetes** > **Deployments (Implementaciones)** y haga clic en **Add (Añadir)**.

Deberá configurar las siguientes pestañas para implementar el clúster HSF.

- General
- Datos del nodo
- Imagen y almacenamiento
- Configuración CN
- Escalado automático

General

Introduzca los siguientes detalles en la sección de la pestaña **General** de la ventana emergente **Deployments (Implementaciones)** .

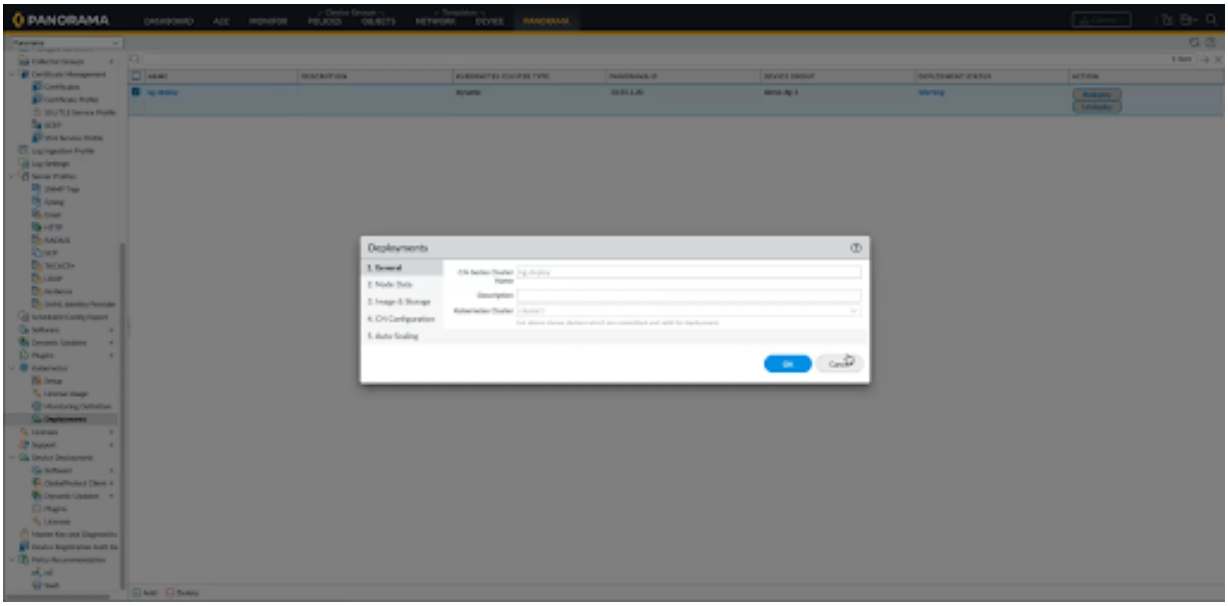
STEP 1 | **CN-Series Cluster Name (Nombre del clúster de CN-Series)**: nombre del CN-Series HSF.

STEP 2 | (Opcional)**Description (Descripción)**: una cadena de texto para describir el clúster HSF.

STEP 3 | **Kubernetes Cluster (Clúster de Kubernetes)**: se crea una lista de entradas para los clústeres en la sección **Setup (Configuración)** del complemento. Elija el clúster relevante que creó en el menú desplegable.

El clúster de Kubernetes se mostrará solo si los detalles están confirmados y son válidos para las implementaciones.

STEP 4 | **CN-Series Cluster Name (Nombre del clúster de CN-Series)**: nombre del CN-Series HSF.



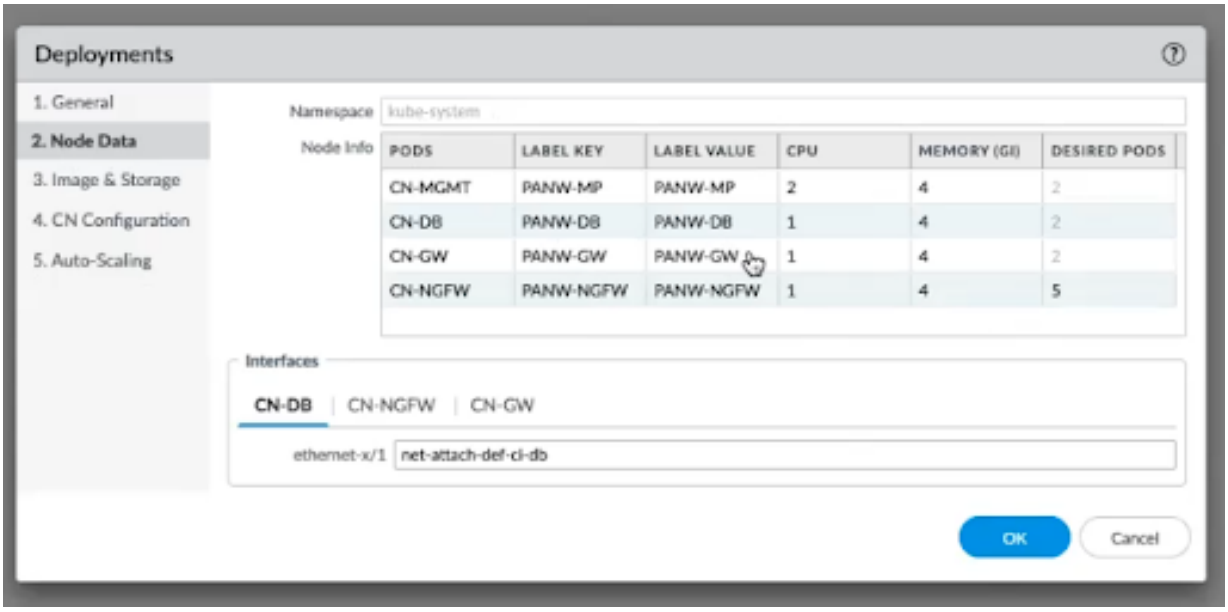
Datos del nodo

Introduzca los siguientes detalles en la sección de la pestaña **Node Data (Datos del nodo)** de la ventana emergente **Deployments (Implementaciones)** .

STEP 1 | **Namespace (Espacio de nombres)**: espacio de nombres en el clúster de Kubernetes existente donde se implementará el CN-Series HSF.

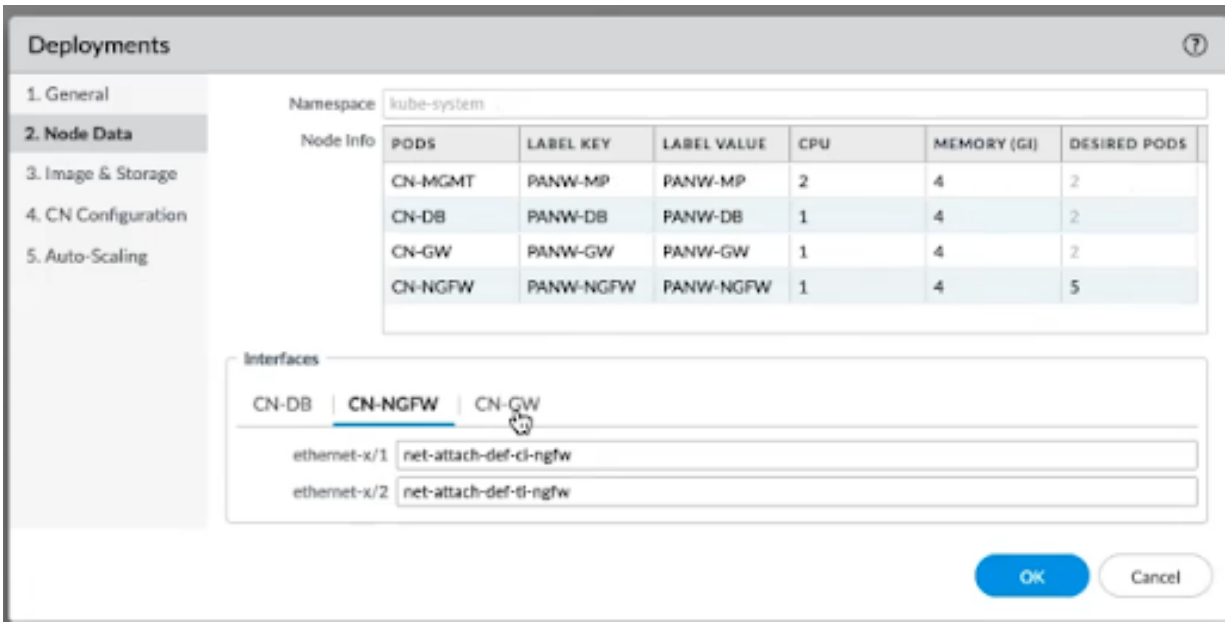
STEP 2 | **Node Info (Información del nodo)**: las etiquetas del grupo de nodos se utilizan para implementar cada tipo de pod de CN. Debe especificar la CPU, la memoria y los Pods deseados para cada uno de los tipos de pods en base a la disponibilidad en los nodos. Los pares de etiquetas y valores de etiqueta

son valores de requisito previo para existir en el nodo y debe añadir el mismo par de valores de clave que se usa para etiquetar los nodos.



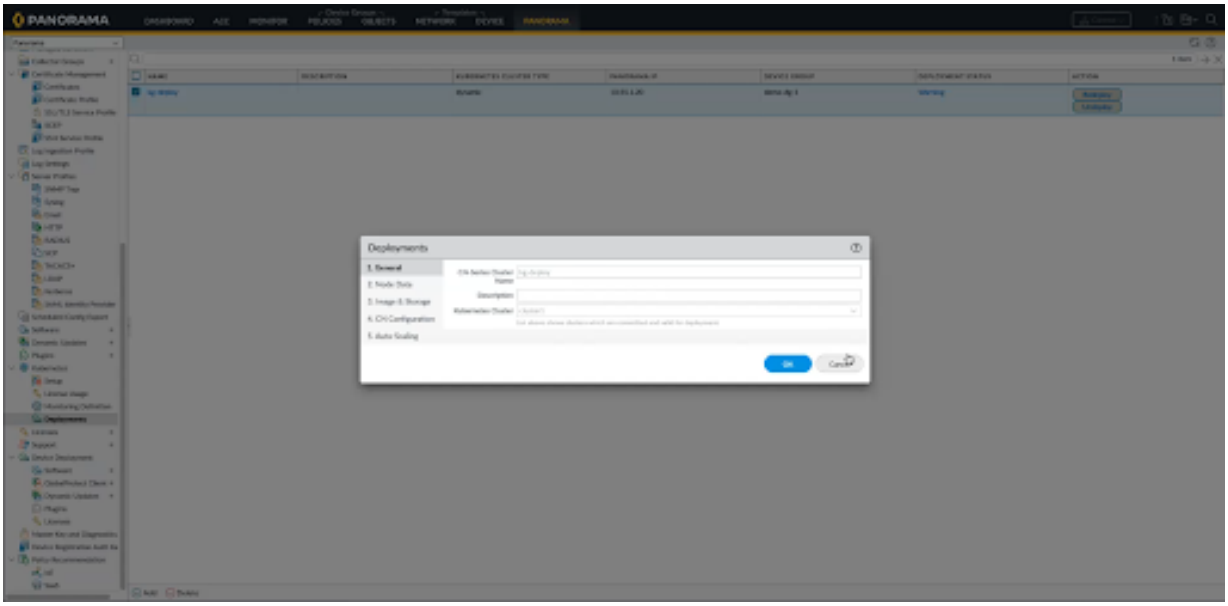
STEP 3 | **Interfaces:** se deben añadir los nombres de interfaz para los pods CN-DB, NGFW y CN-GW. Cada interfaz requiere que se aplique una net-attach-def específica en el clúster de Kubernetes. El complemento nombrará Ethernet x/1 y Ethernet x/2 de forma predeterminada. Si cambia los nombres de interfaz para Ethernet x/1 y Ethernet x/2, también deberá realizar el cambio en la sección de

conexiones de red. Para el pod CN-GW, puede añadir hasta 12 interfaces, sin incluir las interfaces CI y TI.



El clúster de Kubernetes se mostrará solo si los detalles están confirmados y son válidos para las implementaciones.

STEP 4 | **CN-Series Cluster Name (Nombre del clúster de CN-Series)**: nombre del CN-Series HSF.



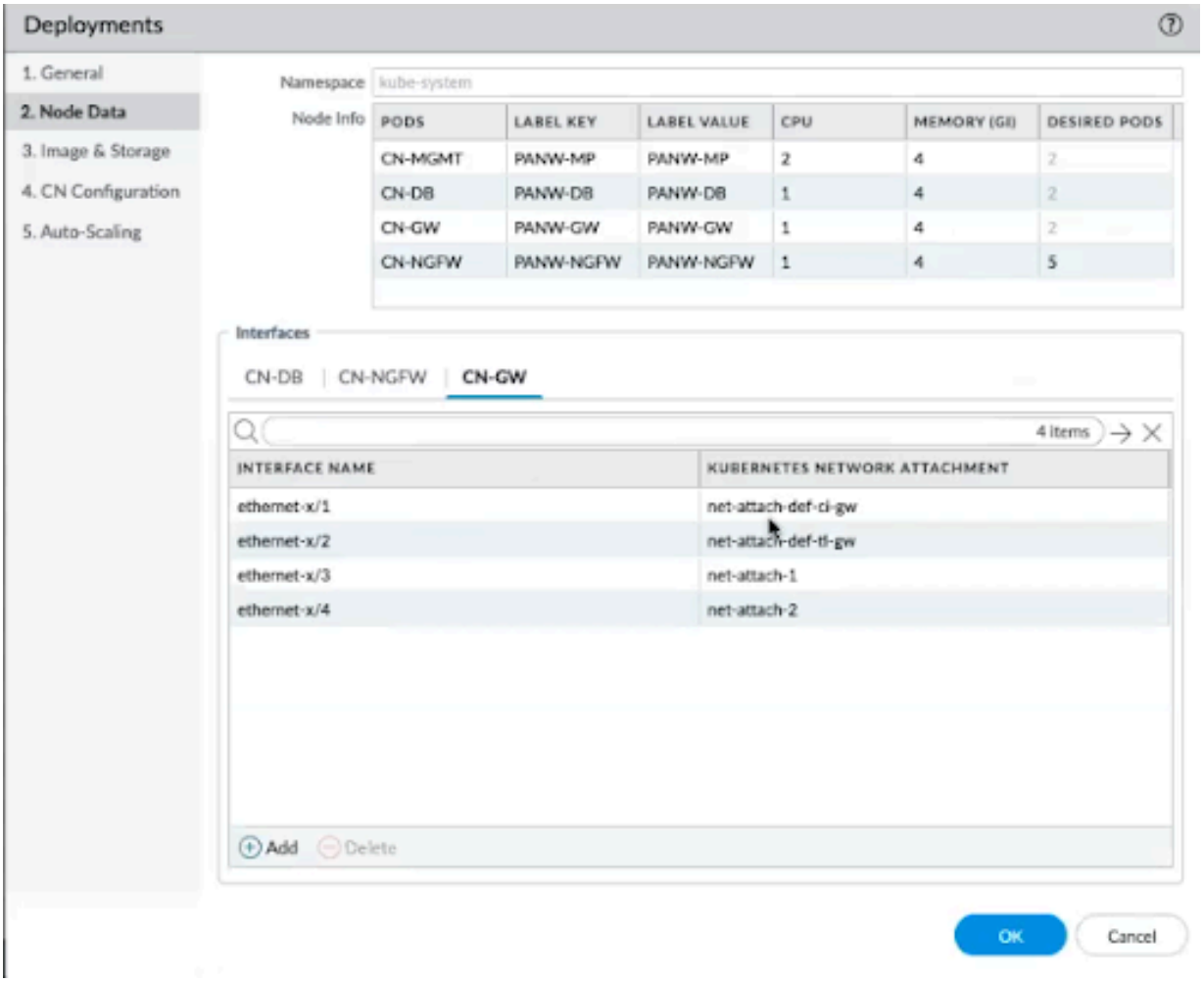


Imagen y almacenamiento

Introduzca los siguientes detalles en la sección de la pestaña **Image & Storage (Imagen y almacenamiento)** de la ventana emergente **Deployments (Implementaciones)**.

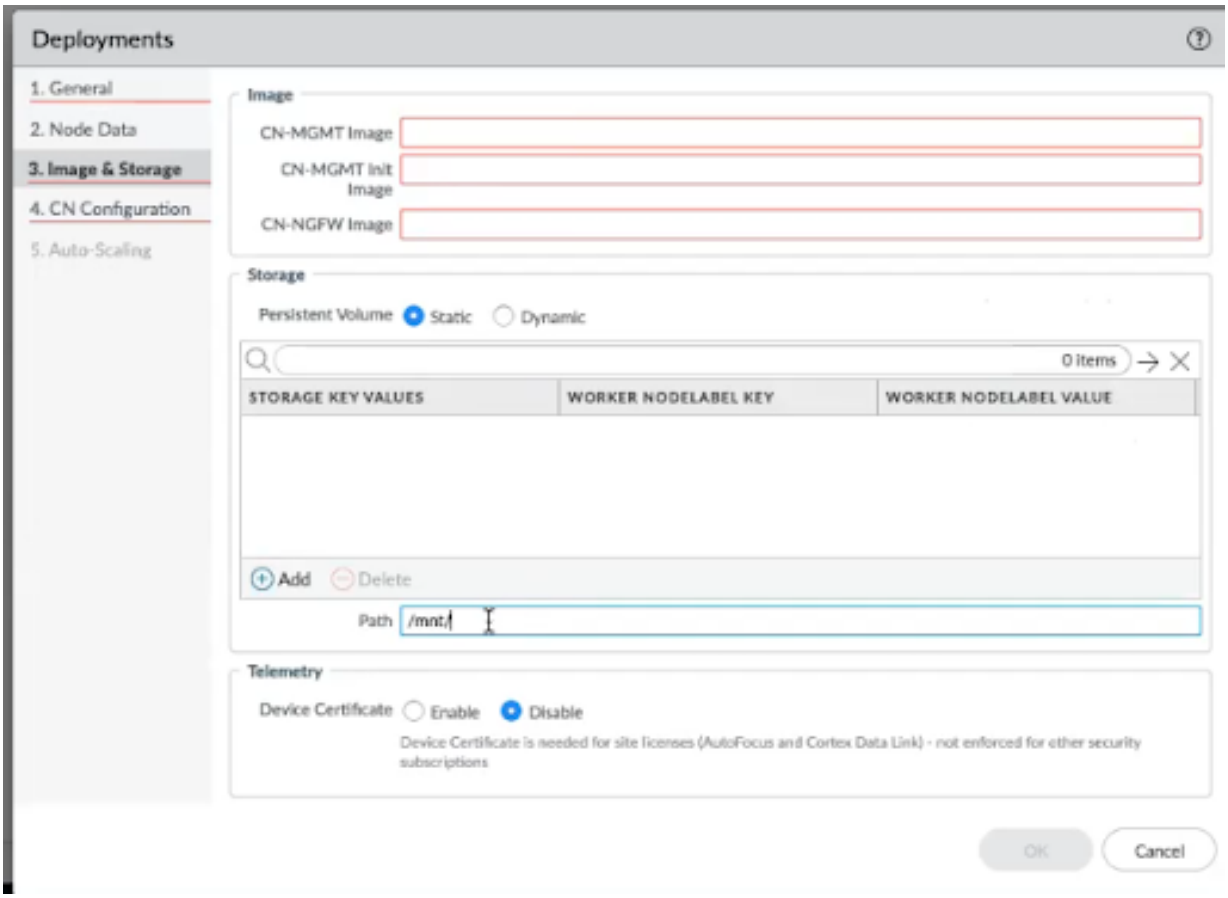
STEP 1 | **Image (Imagen)**: debe almacenar las imágenes en el repositorio local o de AWS, y Panorama no puede validarlo. Sin embargo, el clúster de Kubernetes tiene conectividad con los repositorios donde se almacenan las imágenes.

1. **Imagen de CN-MGMT**: El URI completo del repositorio donde el entorno de Kubernetes accederá a la imagen para implementar el pod CN-MGMT.
2. **Imagen INIT de CN-MGMT**: La imagen inicial necesaria para el pod CN-MGMT.
3. **Imagen de CN-NGFW**: El URI completo del repositorio donde el entorno de Kubernetes accederá a la imagen para implementar el pod de CN-NGFW.

STEP 2 | **Storage (Almacenamiento)**: si desea configurar almacenamiento exclusivo, haga clic en **Dynamic (Dinámico)** en la sección Almacenamiento para el entorno EKS y Estático o Dinámico para entornos Openshift, y el complemento configurará el almacenamiento en la nube. Si ha elegido **Estático**,

debe introducir los valores de clave de almacenamiento, la clave de etiqueta de nodo de trabajador y el valor de etiqueta de nodo de trabajador. También debe introducir la **ruta** donde está montado el almacenamiento.

Debe añadir una clase de almacenamiento no predeterminada válida en el espacio de nombres del entorno de kubernetes. De lo contrario, si se selecciona la opción de almacenamiento dinámico y no se proporciona ningún nombre de clase de almacenamiento, se seleccionará la clase de almacenamiento predeterminada presente en el espacio de nombres.



STEP 3 | **Certificates (Certificados)**: esta es la información del certificado del dispositivo para Habilitar o Deshabilitar la información, como la licencia y, si está habilitado, deberá proporcionar el ID del PIN y el VALOR DEL PIN.

Configuración CN

Introduzca los siguientes detalles en la sección de la pestaña **CN Configuration (Configuración CN)** de la ventana emergente **Deployments (Implementaciones)**.

STEP 1 | **Primary Panorama IP (IP principal de Panorama)**: muestra los valores de las direcciones IP públicas y privadas del Panorama en el que está instalado el complemento.

STEP 2 | **Secondary Panorama IP (IP secundaria de Panorama)**: muestra los valores de las direcciones IP públicas y privadas del Panorama secundario (en el caso de HA) en el que está instalado el complemento.

STEP 3 | **Device Group (Grupo de dispositivos)**: debe crear un DG antes de configurar la implementación como se menciona en la sección de requisitos previos. El menú desplegable Grupo de dispositivos enumera todos los DG en el panorama actual y debe elegir un DG válido. El pod CN-MGMT se registrará bajo este DG. Para conocer los pasos para crear un grupo de dispositivos, consulte el Paso 5 de Preparación de Panorama para la implementación de CN-Series HSF.

STEP 4 | **Template (Plantilla)**: debe crear una plantilla (variable_template) para los detalles específicos de CN-GW antes de configurar la implementación como se menciona en la sección de requisitos previos. El menú desplegable Plantilla enumera todas las plantillas en el Panorama actual. Debe elegir una plantilla adecuada para su implementación actual. Después de la implementación de HSF, el complemento añadirá esta plantilla a una pila de plantillas junto con una plantilla K8S-CNF-Clustering-Readonly que gestiona la configuración básica para los pods CN-DB y CN-NGFW. También configura los enlaces CI y TI en el pod CN-GW. El pod CN-MGMT obtiene configuraciones de la pila de plantillas. Para conocer los pasos para crear la plantilla variable, consulte el Paso 6 de Preparación de Panorama para la implementación de CN-Series HSF.

STEP 5 | **Log Collector Group (LCG) [Grupo de recopiladores de logs (LCG)]**: este menú desplegable enumera todos los grupos de recopiladores de logs en el Panorama actual y se debe elegir un LCG adecuado. También configura los enlaces CI y TI del pod CN-GW. Para ver los pasos para crear LCG, consulte el Paso 7 de Preparación de Panorama para la implementación de CN-Series HSF.

STEP 6 | **Jumbo Frame (Trama gigante)**: el menú desplegable Trama gigante enumera los valores: **Enable (Habilitar)**, **Disable (Deshabilitar)**y **AutoDetect (Detectar automáticamente)**. Esta configuración se aplica a todos los pods del CN-Series HSF.

STEP 7 | **5G Enabled (5G habilitado)**: este es un botón de radio con opciones **Enable (Habilitar)** y **Disable (Deshabilitar)** y se refiere a la configuración de GTP necesaria en el CN-Series HSF.

Debe gestionar más configuraciones necesarias en la plantilla en el archivo ***variable_template****.*

STEP 8 | **DPDK**: este es un botón de opción con opciones **Enable (Habilitar)** y **Disable (Deshabilitar)**. Si los recursos subyacentes no son compatibles con DPDK, entonces, de forma predeterminada, el CN-Series HSF se configurará como packetmmap de forma predeterminada.

En EKS, si desea utilizar DPDK, debe tener una AMI con controladores DPDK configurados. Para obtener más información, consulte Configuración de DPDK en AWS EKS.

Para habilitar DPDK en Openshift, debe habilitar páginas grandes en los nodos trabajadores. Para obtener más información, consulte Configuración de hugepages.

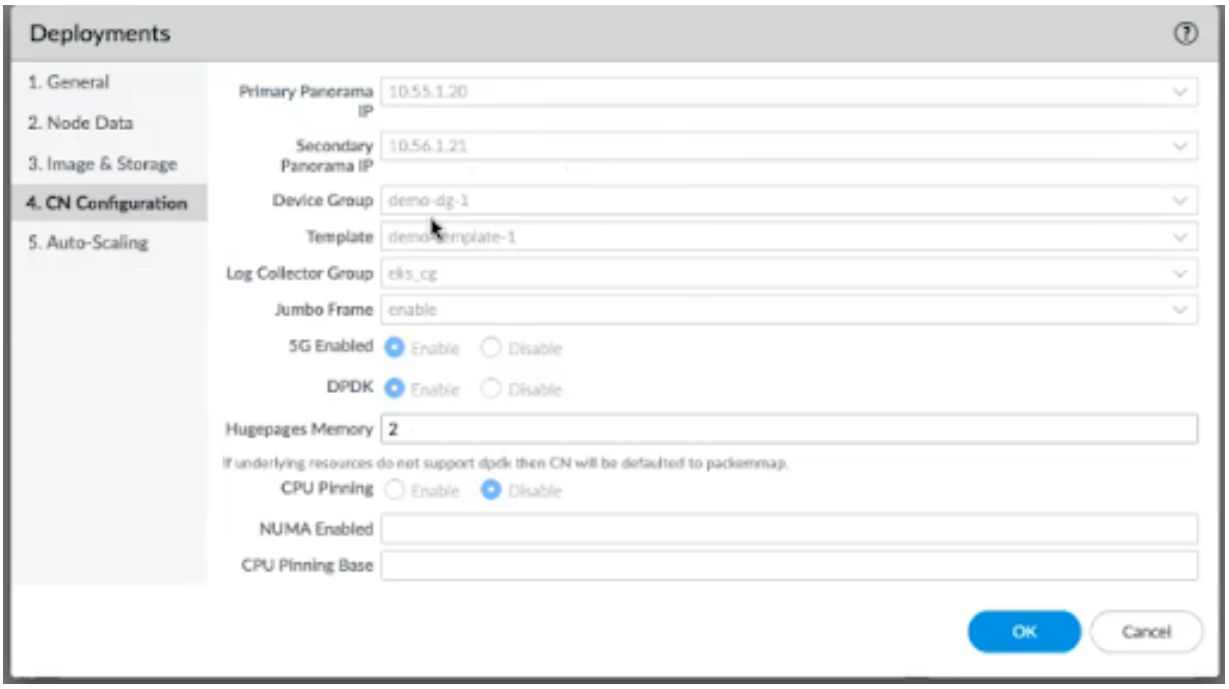
También deberá habilitar el controlador PCI VFIO en los nodos trabajadores.

```
modprobe vfio-pci echo 1 > /sys/module/vfio/parameters/
enable_unsafe_noiommu_mode
```

STEP 9 | **CPU Pinning (Fijación de CPU)**: elija habilitar o deshabilitar la fijación de CPU.

STEP 10 | **Numa Enabled (Numa habilitado)**: proporcione el número de nodo para NUMA.

STEP 11 | **CPU Pinning Base (Base de fijación de CPU)**: proporcione el número de CPU desde donde desea iniciar la fijación de CPU de los procesos de reenvío y omita las CPU con números más bajos.



Escalado automático

Introduzca los siguientes detalles en la sección de la pestaña **Node Data (Datos del nodo)** de la ventana emergente **Auto-Scaling (Escalado automático)**.

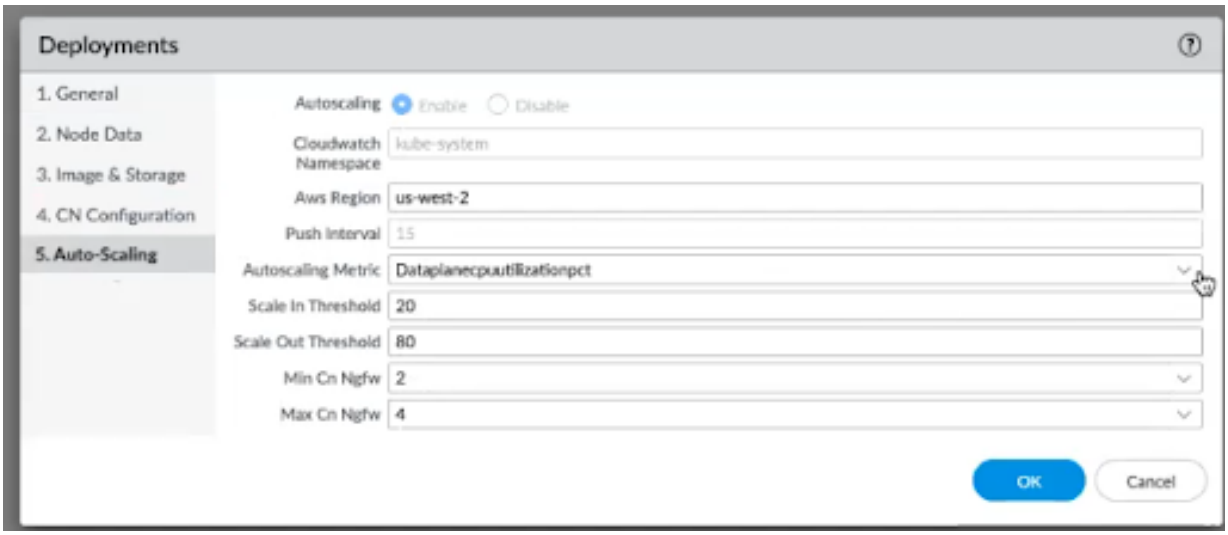
- *El Escalado automático solo se admite en entornos EKS con EKS Kubernetes versión 1.22. La pestaña Escalado automático está atenuada para otros sistemas de Kubernetes.*
- *Tendrá que implementar* HPA basado en métricas personalizadas mediante KEDA en entornos EKS *para que funcione el escalado automático.*

STEP 1 | Introduzca la **Autoscaling Metric (Métrica de escalado automático)**, el **Scale In Threshold (Umbral de reducción horizontal)** y el **Scale Out Threshold (Umbral de escalado horizontal)** en la sección **Autoscaling (Escalado automático)**.

STEP 2 | Haga clic en **OK (Aceptar)** para confirmar la implementación.

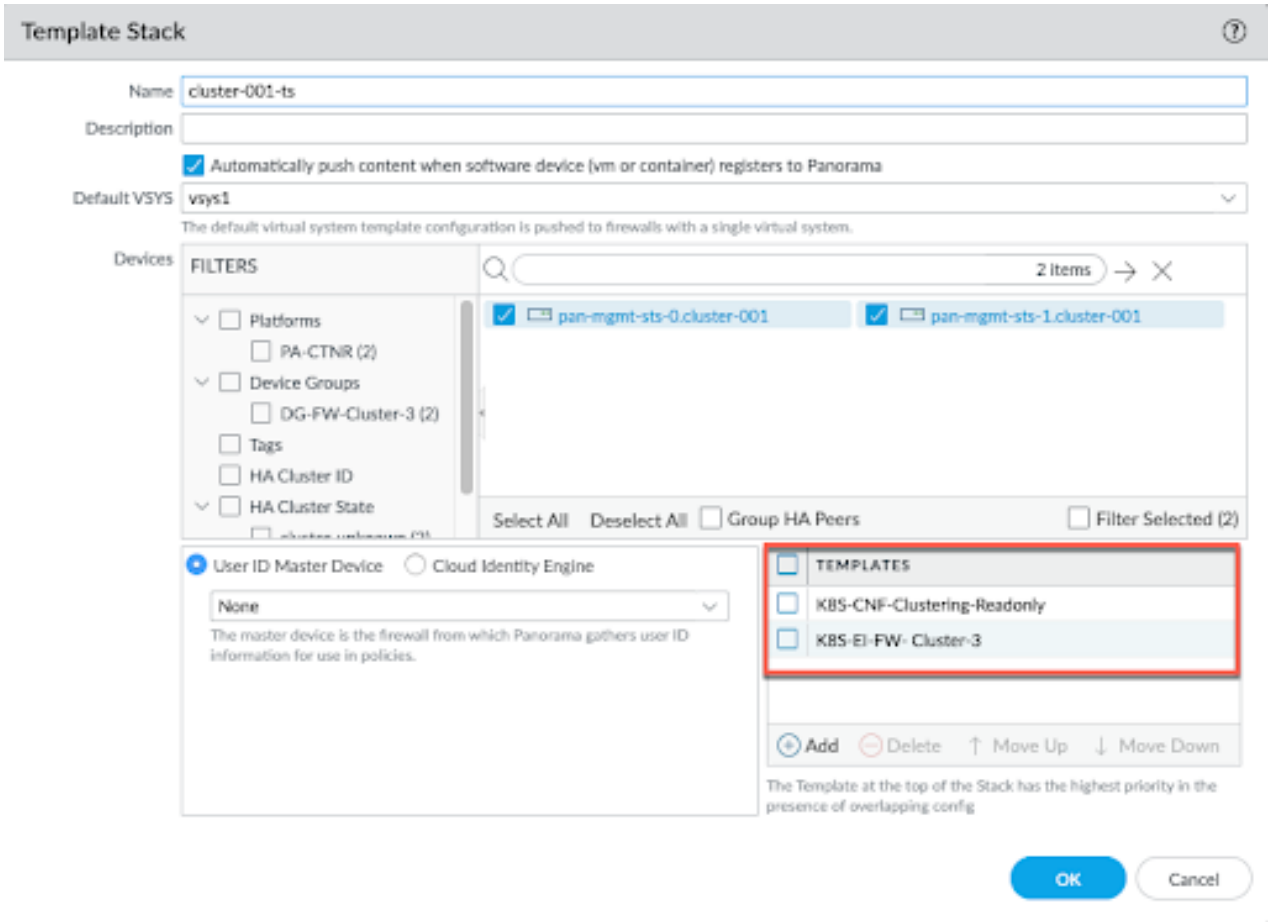
Las siguientes son las métricas compatibles con el ajuste de Escalado automático.

- `dataplanecpuutilizationpct`
- `dataplanepacketbufferutilization`
- `pansessionactive`
- `pansessionutilization`
- `pansessionsslproxyutilization`
- `panthroughput`
- `panpacketrate`
- `panconnectionspersecond`



Una vez que haya introducido todos los detalles de configuración, la pestaña Implementaciones muestra los detalles de una única implementación que está almacenada. Haga clic en **Commit (Confirmar)** para continuar con la implementación. Después de completar la confirmación, el complemento muestra el botón Implementar. Haga clic en el botón **Deploy (Implementar)** para implementar el CN-Series HSF.

Después de la implementación del CN-Series HSF, el clúster crea una pila de plantillas,`<cluster-name>-ts` con la plantilla K8S-CNF-Clustering-Readonly y la plantilla variable que creó en el Paso 6 de Preparación de Panorama para la implementación de CN-Series HSF.



El grupo de dispositivos al que hizo referencia durante la configuración de implementación de HSF (creado en el Paso 5 de Preparación de Panorama para la implementación de CN-Series HSF) y la Pila de plantillas crea da automáticamente después de que la implementación de HSF se inicia en el pod CN-MGMT. Cuando el pod CN-MGMT se conecta a Panorama, el grupo de dispositivos y la pila de plantillas se asocian automáticamente con el nombre del HSF.

La información de HSF para los pods CN-DB, CN-GW y CN-NGFW se completa automáticamente cuando están activos. Cuando estos pods están en funcionamiento, el pod CN-MGMT envía a Panorama detalles como la dirección IP de CI, los detalles del pod, el ID del dispositivo y la versión del software.

Para Alta disponibilidad (HA) de Panorama, el pod CN-MGMT envía actualizaciones a los Panorama activos y pasivos.

Diferentes estados de implementación

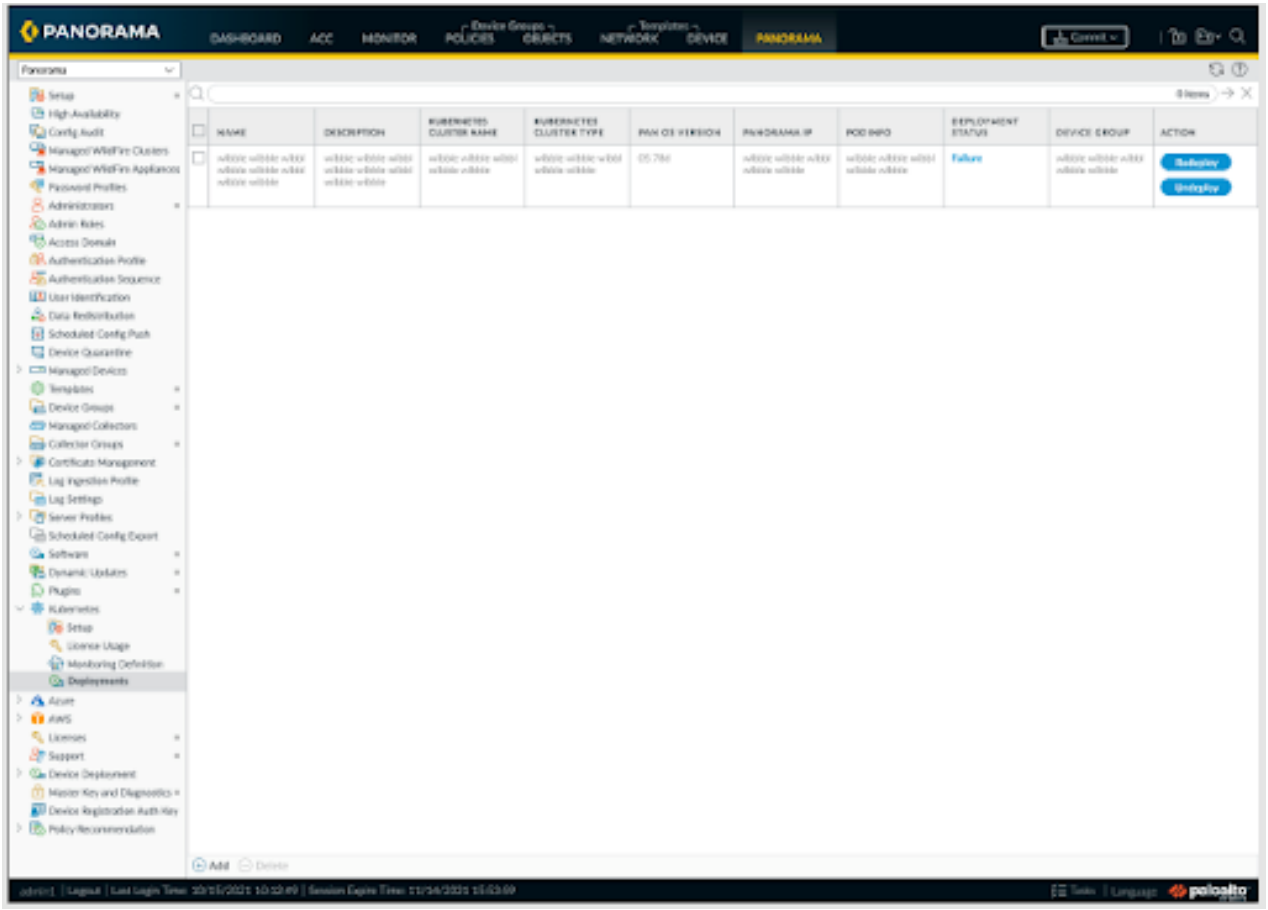
¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Una vez que haya introducido todos los detalles de configuración, la pestaña Implementaciones muestra los detalles de una única implementación que está almacenada. Hay 5 etapas en una implementación:

1. Confirmación requerida
2. No implementado
3. Implementando
4. Warning (Advertencia)
5. Correcto/fallo

1. Haga clic en **Commit (Confirmar)** para continuar con la implementación. Puede notar que el botón Implementar está deshabilitado y el estado de implementación se cambia a **Not Deployed (No implementado)** después de hacer clic en Confirmar. El botón Implementar se habilita después de completar la confirmación.
2. Haga clic en Implementar para continuar con la implementación de la CNF del CN-Series. El estado de implementación cambia a Implementando. Durante esta etapa se crean las configuraciones de Panorama y se generan CN-GWs, y el complemento comienza a hacer llamadas a la api para implementar el CN-Series HSF.
3. El estado de Implementación luego cambia a **Advertencia**, **Correcto** o **Fallo** según la disponibilidad de recursos y los detalles de configuración. Los botones Volver a implementar e Implementar están habilitados.
4. Haga clic en Volver a implementar para realizar cambios en los parámetros habilitados y confirmar los cambios antes de hacer clic en Volver a implementar.
5. Haga clic en **Undeploy (Eliminar implementación)** para eliminar todos los pods de CN-Series HSF creados como parte de esta implementación.

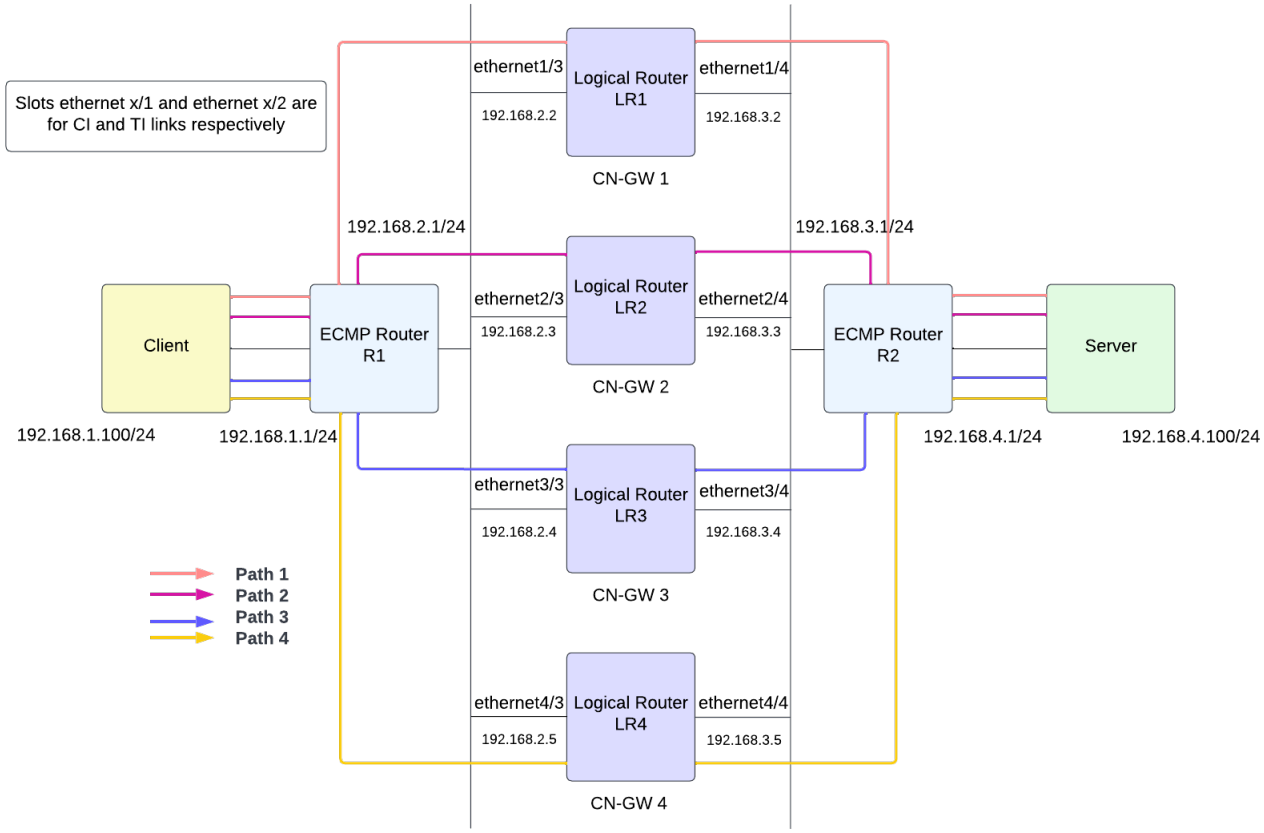
Todas las configuraciones de Panorama aún se conservan después de eliminar todos los pods de CN-Series HSF.



Configuración del flujo de tráfico hacia el CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

El enrutador de subida/bajada utiliza un algoritmo ECMP basado en flujo. Cuando el tráfico llega a CN-GW, este distribuirá el tráfico a uno de los CN-NGFW disponibles a través del enlace de Interconexión de tráfico (TI) utilizando un algoritmo hash simétrico. El tráfico que coincide con una sesión desde ambas direcciones (cliente a servidor y servidor a cliente) siempre pasará por el mismo CN-NGFW. Una vez que el CN-NGFW procese el tráfico, y si ha establecido una política para **Allow (Permitir)** el tráfico, el paquete de tráfico se enviará de vuelta al CN-GW para llegar al servidor.



STEP 1 | Cree un enrutador lógico en el cortafuegos para que participe en el enrutamiento de capa 3.

1. Vaya a **Network (Red)** > **Routing (Enrutamiento)** > **Logical Router (Enrutador lógico)** y luego seleccione la plantilla variable del menú desplegable **Template (Plantilla)**.
2. Seleccione un enrutador virtual predeterminado o añada un **Name (Nombre)** para el nuevo enrutador lógico.
3. Seleccione **General**, luego añada una **Interface (Interfaz)** ya definida.

   Repita este paso para añadir todas las interfaces que desee añadir al enrutador lógico.

   *Las interfaces ethernetX/1 y ethernetX/2 están reservadas para enlaces CI y TI respectivamente. Seleccione una interfaz entre **ethernet1/3** y **ethernet1/14**.*
4. Haga clic en **OK (Aceptar)**.
5. Establezca la distancia administrativa para el enrutamiento estático. El rango es de 10 a 240, el valor predeterminado es 10.

   Establezca las distancias administrativas para los tipos de rutas como sea necesario para su red. Cuando el enrutador virtual tiene dos o más rutas diferentes hacia el mismo destino, utiliza la distancia administrativa para seleccionar la mejor ruta de diferentes protocolos de enrutamiento y rutas estáticas mediante la elección de una distancia menor.
6. Habilite ECMP para aprovechar varias rutas de igual coste para el reenvío.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure la interfaz de Capa 3 para habilitar el flujo de tráfico.

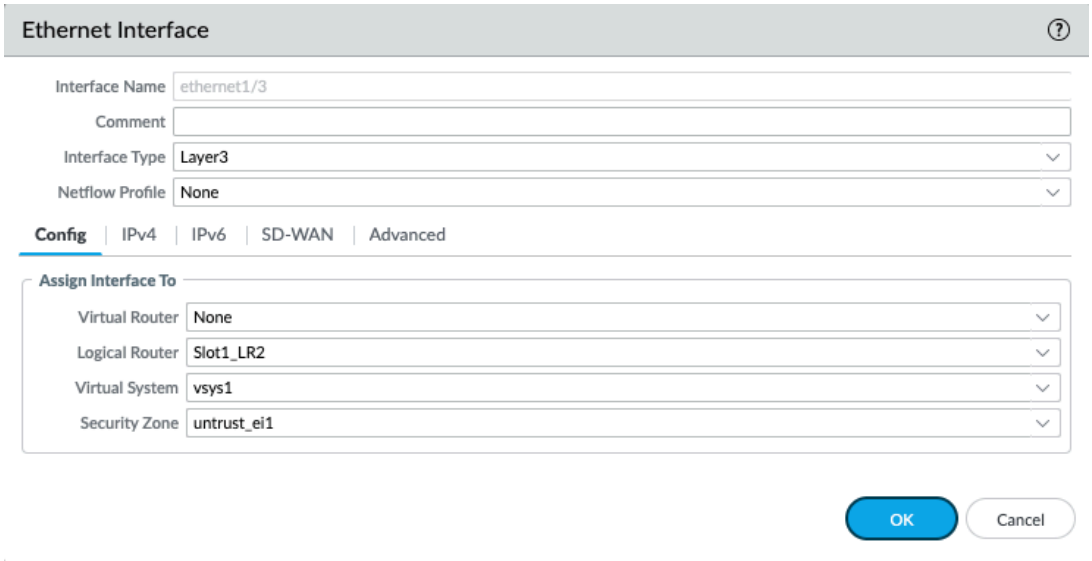
Cuando usted Preparación de Panorama para la implementación de CN-Series HSF, es posible que haya creado una Plantilla variable. Para habilitar el flujo de tráfico a través de la red del clúster, debe configurar la plantilla variable con la red necesaria y la configuración de tráfico necesaria para balancear la carga del CN-Series HSF. Debe configurar la interfaz Ethernet de capa 3 con direcciones IPv4 para que el cortafuegos pueda realizar el enrutamiento en dichas interfaces. Habitualmente usaría el siguiente procedimiento para configurar una interfaz externa que se conecte con Internet y una interfaz para su red interna.

Puede configurar esta plantilla antes o después de implementar el CN-Series HSF.

*Asegúrese de no superponer la configuración de esta plantilla con la plantilla **K8S-CNF-Clustering-Readonly** creada automáticamente durante la instalación del complemento de Kubernetes.*

1. Vaya a **Network (Red)** > **Interfaces**, luego seleccione la plantilla variable del menú desplegable **Template (Plantilla)**.
2. Seleccione la interfaz **Ethernet** para **Add Interface (Añadir interfaz)**.
3. Seleccione una **Slot (Ranura)** entre 1 y 30.
4. Introduzca un **Interface Name (Nombre de interfaz)** entre **`ethernet1/3`** y **`ethernet1/14`**.
5. En **Interface Type (Tipo de interfaz)**, seleccione **Layer3 (Capa3)**.

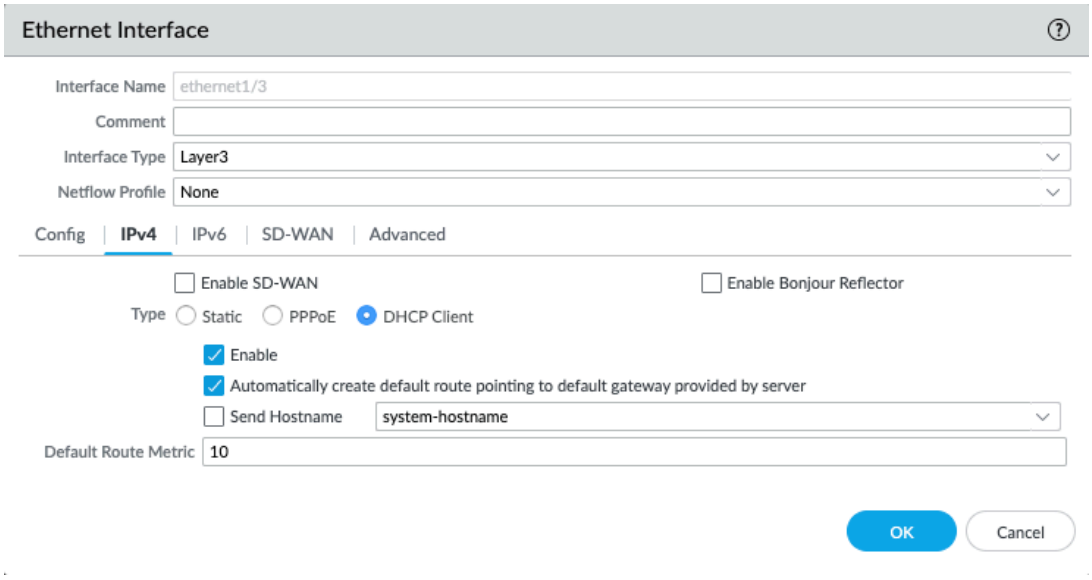
6. En la pestaña **Config (Configurar)**:
   - Para **Logical Router (Enrutador lógico)**, seleccione el enrutador lógico que configuró en el Paso 1.
   - Para **Virtual System (Sistema virtual)**, seleccione el sistema virtual que está configurando, en el caso de un cortafuegos de sistema virtual múltiple.
   - Para **Security Zone (Zona de seguridad)**, seleccione la zona a la cual pertenece la interfaz o cree una **New Zone (Zona nueva)**.



7. En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.

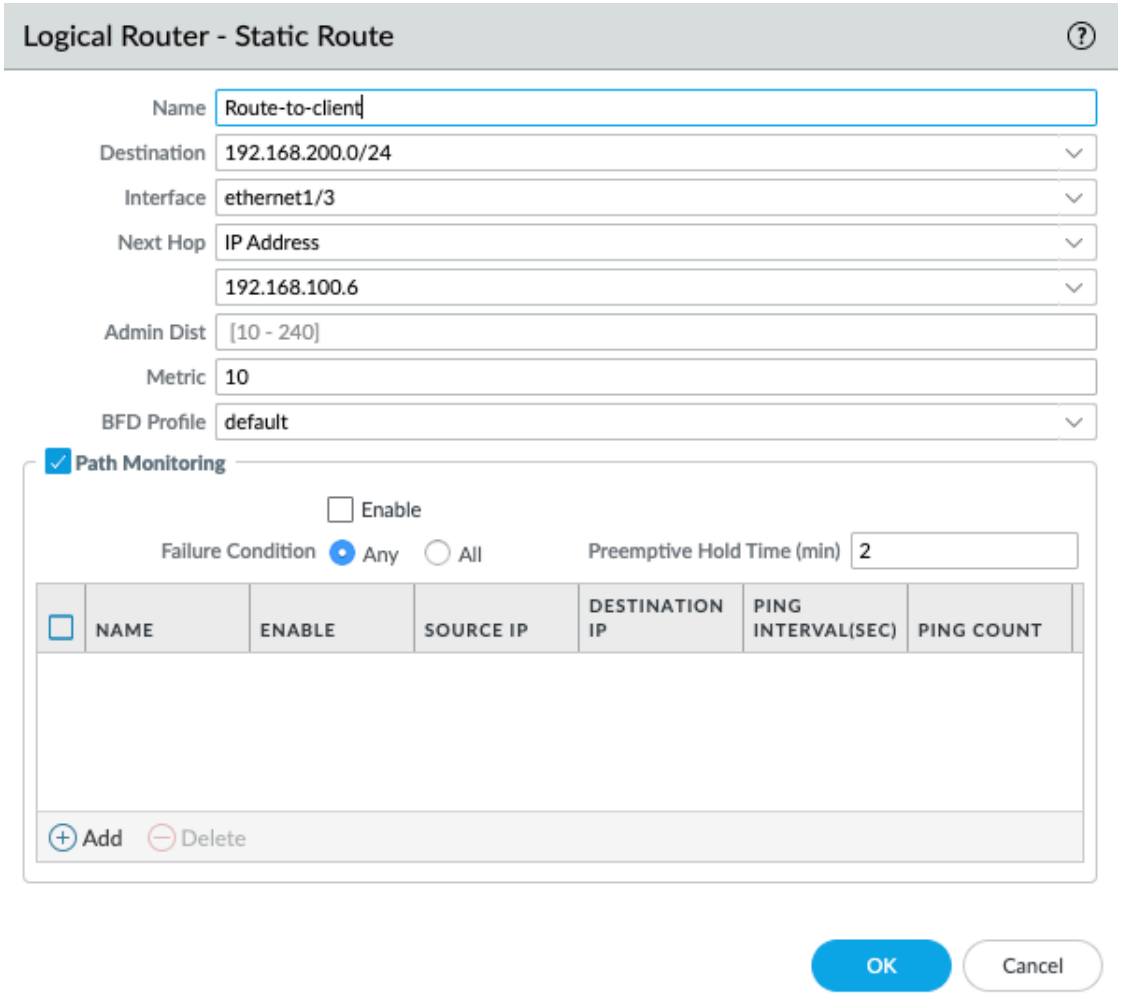
   La interfaz del cortafuegos funciona como un cliente DHCP y recibe una dirección IP asignada dinámicamente. El cortafuegos también permite propagar los ajustes recibidos mediante la interfaz del cliente DHCP a un servidor DHCP activo en el cortafuegos. Para obtener más información, consulte Configurar una interfaz como cliente DHCP.

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



STEP 3 | Configure rutas estáticas para el enrutador lógico.

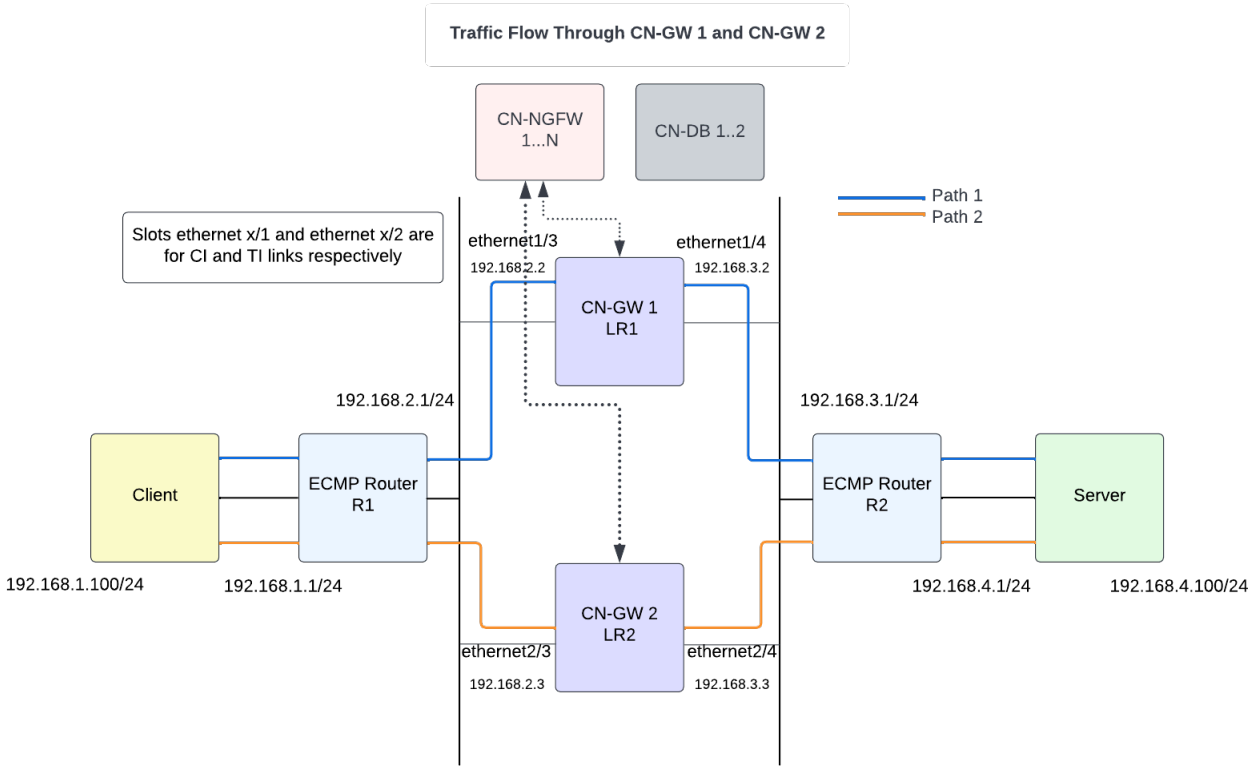
1. Vaya a **Network (Red)** > **Routing (Enrutamiento)** > **Logical Router (Enrutador lógico)**, luego seleccione la plantilla variable del menú desplegable **Template (Plantilla)**.
2. Seleccione la pestaña **Static (Estática)** > **IPv4** y haga clic en **Add (Añadir)**.
3. Introduzca un nombre en **Name (Nombre)** para la ruta estática.
4. Introduzca la ruta de **Destination (Destino)** y la máscara de red. Por ejemplo, 192.168.200.0/24.
5. Seleccione la interfaz de salida que utilizarán los paquetes para ir al siguiente salto.
6. Para **Next Hop (Siguiente salto)**, seleccione **ip-address (dirección IP)** e introduzca la dirección IP de su puerta de enlace interna. Por ejemplo, 192.168.100.2.
7. Introduzca una **Admin Distance (Distancia administrativa)** para que la ruta anule la distancia administrativa predeterminada establecida para las rutas estáticas en este enrutador lógico (intervalo de 10 a 240; valor predeterminado: 10).
8. Introduzca una **Metric (Métrica)** para la ruta (el intervalo es de 1 a 65 535).
9. Aplique un **BFD Profile (Perfil BFD)** a la ruta estática para que, si la ruta estática falla, el cortafuegos elimine la ruta y utilice una ruta alternativa. El valor predeterminado es **None (Ninguna)**.
10. Haga clic en **OK (Aceptar)**.



Caso de prueba: Gestión de fallos de CN-GW basado en BFD de capa 3

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Esta prueba evalúa la configuración de BFD necesaria para gestionar fallos de CN-GW. Un perfil BFD gestiona fallos de CN-GW en los enrutadores de subida/bajada.



Flujo de tráfico simétrico

- Si la interfaz de tráfico de entrada es CN-GW 1, la consulta de ruta para encontrar la interfaz de salida está en LR1.
  - Ruta 1: Destino: Subred del cliente; Siguiente salto: R1
  - Ruta 2: Destino: Subred del servidor; Siguiente salto: LR2

- Si la interfaz de tráfico de entrada es CN-GW 2, la consulta de ruta para encontrar la interfaz de salida está en LR2.
  - Ruta 1: Destino: Subred del cliente; Siguiente salto: R1
  - Ruta 2: Destino: Subred del servidor; Siguiente salto: R2

Flujo de tráfico asimétrico

El CN-Series HSF también admite flujos de tráfico asimétricos. Por ejemplo, la sesión de coincidencia de tráfico de cliente a servidor 1 que fluye a través de CN-GW 1 y la sesión de coincidencia de tráfico de servidor a cliente 1 que fluye a través de CN-GW 2. Para el flujo de tráfico asimétrico, todas las interfaces orientadas a R1 deben estar en la misma zona. Igualmente, todas las interfaces orientadas hacia R2 deben estar en la misma zona.

Enrutamiento Inter LR

Por ejemplo, si la interfaz de tráfico de entrada es CN-GW 1, la consulta de ruta para encontrar la interfaz de salida está en LR1. Si hay una ruta para llegar al servidor con el siguiente salto como LR2, entonces CN-NGFW enviará el tráfico a LR2. Basado en la consulta de rutas LR2 de CN-GW 2, el paquete se enviará al servidor.

STEP 1 | Vaya a **Network (Red)** > **Routing (Enrutamiento)** > **Routing Profiles (Perfiles de enrutamiento)** > **BFD**, luego seleccione la plantilla variable en el menú desplegable **Template (Plantilla)**.

Debe habilitar BFD en enrutadores externos y enrutadores lógicos.

STEP 2 | Haga clic en **Add (Añadir)** para añadir al perfil de BFD.

STEP 3 | Introduzca un **Name (Nombre)**.

STEP 4 | Seleccione el **Mode (Modo)** en el que BFD operará:

- **Active**: BFD inicia el envío de los paquetes de control (por defecto). Al menos uno de los peers de BFD debe estar activo; ambos pueden estar activos.
- **Passive**: BFD espera que el peer envíe los paquetes de control y responde según corresponda.

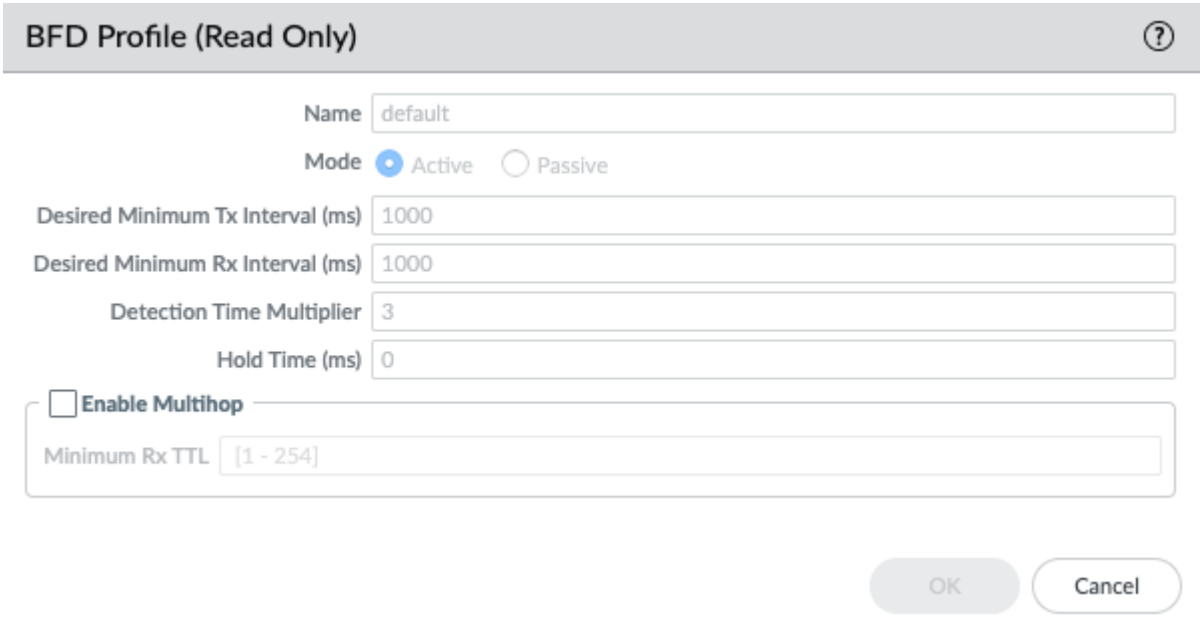
STEP 5 | Introduzca el **Desired Minimum Tx Interval (ms)**. Este es el intervalo mínimo, en milisegundos, con el cual usted desea que el protocolo BFD (denominad BFD) envíe paquetes de control BFD; con lo cual usted está negociando el intervalo de transmisión con el peer.

STEP 6 | Introduzca el **Detection Time Multiplier**. El sistema local calcula el tiempo de detección como el **Detection Time Multiplier (Multiplicador de tiempo de detección)** recibido del sistema remoto, multiplicado por el intervalo de transmisión acordado del sistema remoto (el valor más alto de **Required Minimum Rx Interval [Intervalo Rx mínimo necesario]** y el último **Desired Minimum Tx Interval [Intervalo Tx mínimo deseado]** recibido). Si BFD no recibe un paquete de control BFD desde su peer antes de que se agote el tiempo de detección, se produjo un fallo. El intervalo va de 2 a 50 y el valor predeterminado es 3.

STEP 7 | Introduzca el **Hold Time (ms)**. Esta es la demora, en milisegundos, una vez que un enlace se activa antes de que BFD transmita los paquetes de control de BFD. **Hold Time (Tiempo de espera)** se aplica al modo activo de BFD únicamente. Si el BFD recibe paquetes de control BFD durante el **tiempo de espera**, los ignora. El intervalo es 0-120000; el valor por defecto es 0.

STEP 8 | Seleccione **Multihop (Múltiples pasos)** para habilitar BFD en varios saltos de BGP. Introduzca el **Minimum Rx TTL**. Este es el valor mínimo de período de vida (cantidad de saltos) que BFD aceptará (recibirá) en un paquete de control de BFD cuando BGP admite varios saltos de BFD. (El intervalo es 1-254; no hay valor por defecto).

STEP 9 | Haga clic en **OK (Aceptar)** para guardar el perfil BFD.



STEP 10 | Configure rutas estáticas para el enrutador lógico.

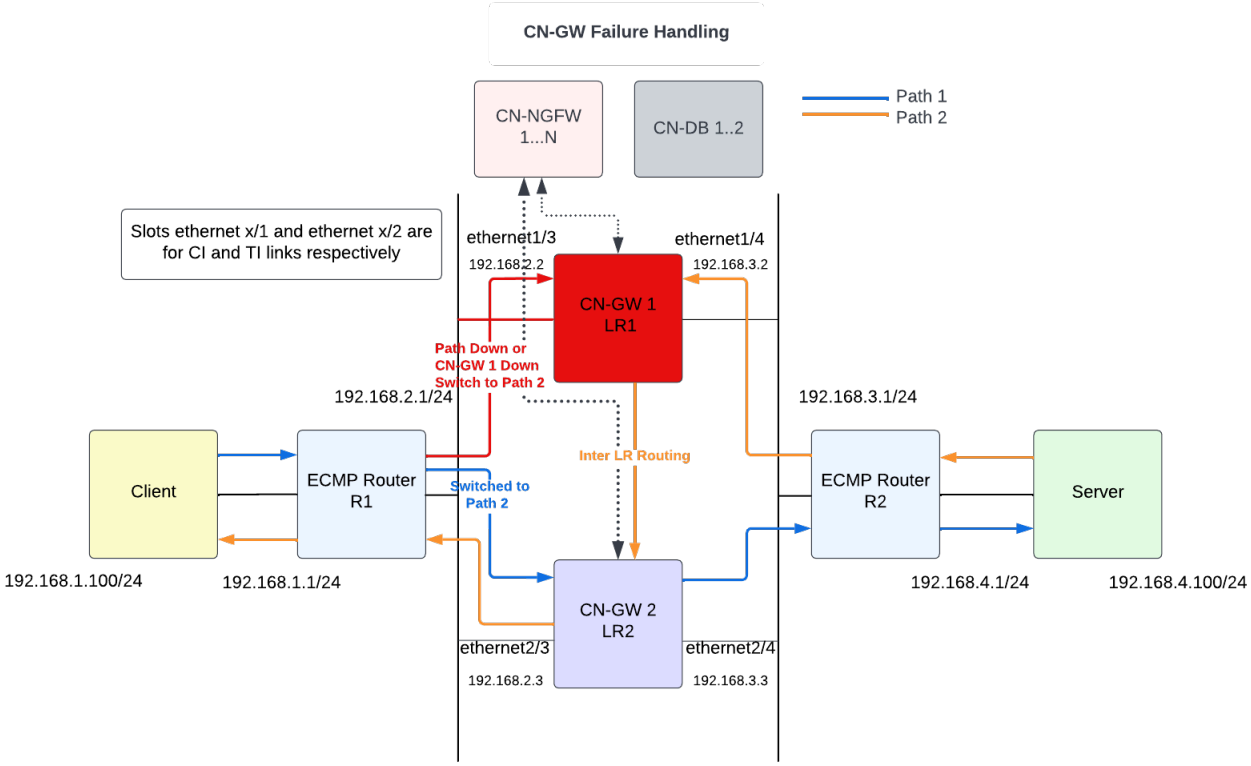
1. Vaya a **Network (Red)** > **Routing (Enrutamiento)** > **Logical Router (Enrutador lógico)**, luego seleccione la plantilla variable del menú desplegable **Template (Plantilla)**.
2. Seleccione la pestaña **Static (Estática)** > **IPv4** y haga clic en **Add (Añadir)**.
3. Introduzca un nombre en **Name (Nombre)** para la ruta estática.
4. Introduzca la ruta de **Destination (Destino)** y la máscara de red. Por ejemplo, 192.168.200.0/24.
5. Seleccione la interfaz de salida que utilizarán los paquetes para ir al siguiente salto.
6. Para **Next Hop (Siguiente salto)**, seleccione **ip-address (dirección IP)** e introduzca la dirección IP de su puerta de enlace interna. Por ejemplo, 192.168.100.2.
7. Introduzca una **Admin Distance (Distancia administrativa)** para que la ruta anule la distancia administrativa predeterminada establecida para las rutas estáticas en este enrutador lógico (intervalo de 10 a 240; valor predeterminado: 10).
8. Introduzca una **Metric (Métrica)** para la ruta (el intervalo es de 1 a 65 535).
9. Aplique el **BFD Profile (Perfil BFD)** creado en pasos anteriores a la ruta estática de modo que si la ruta estática falla, el cortafuegos elimine la ruta y utilice una ruta alternativa.
10. Haga clic en **OK (Aceptar)**.

La configuración BFD se encarga de los fallos de ruta y de CN-GW. En el siguiente diagrama de flujo de tráfico, considere dos sesiones SSH entre cliente y servidor. La Sesión 1 está pasando a través de la ruta 1 y la Sesión 2 está pasando a través de la ruta 2. Si la CN-GW 1 o la ruta 1 están caídas, la configuración BFD entre R1 y CN-GW 1, R2 y CN-GW 1 ayuda a R1 a identificar el fallo de la ruta y envía el tráfico a

través de la ruta 2. Las interfaces orientadas hacia R1 deben estar en la misma zona. Del mismo modo, las interfaces orientadas hacia R2 deben estar en la misma zona.

Ruta 1: Destino: Subred del cliente; siguiente salto es R1, Métrica 10

Ruta 2: Destino: Subred del servidor; siguiente salto es LR2, Métrica 11

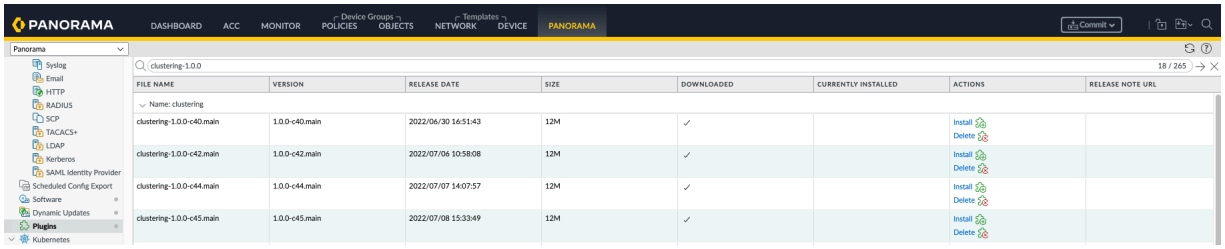


Ver el resumen y la supervisión de CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

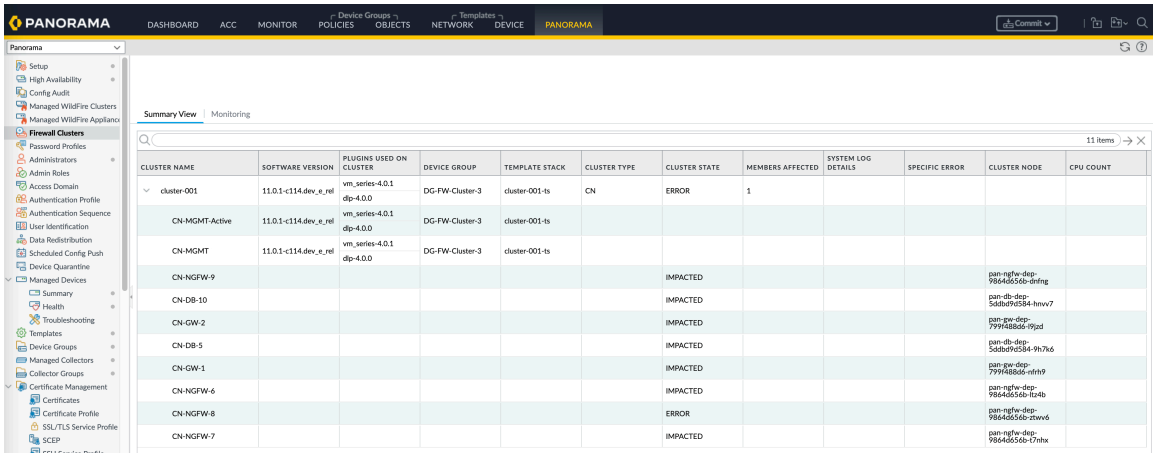
Puede ver la información de resumen y supervisión del HSF de la CN-Series en la pestaña **Firewall Clusters (Clústeres de cortafuegos)** en la interfaz web de Panorama. Para ver y acceder a los clústeres de cortafuegos, debe **Enable (Habilitar)** > **Firewall Clusters (Clústeres de cortafuegos)** de la lista **Panorama** > **Admin Roles (Funciones de administración)** > **Web UI (Interfaz web)**. Para obtener más información, consulte configurar un perfil de función de administración.

Debe instalar el complemento Clustering 1.0.0 de **Panorama** > **Plugins (Complementos)** para ver los detalles del clúster en **Firewall Clusters (Clústeres de cortafuegos)**.



Vista de resumen

Vea la información sobre los clústeres de la serie CN-Series capturados por el cortafuegos en los últimos cinco minutos. Haga clic en el botón actualizar para cargar los últimos detalles.

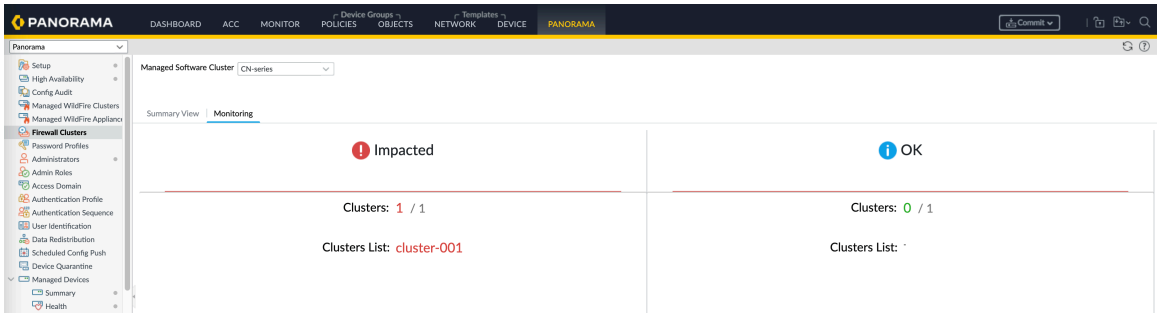


Campo	Description (Descripción)
Nombre de clústeres	Nombre del clúster de cortafuegos.

Campo	Description (Descripción)
Versión de software	La versión PAN-OS.
Complementos utilizados en el clúster	Lista de complementos utilizados en el clúster. *Solo compatible con los complementos de cortafuegos CN-Series.*
Pila de plantillas	Nombre de la pila de plantillas asociada con el clúster.
Grupo de dispositivos	Nombre del grupo de dispositivos asociado al clúster.
Estado de clúster	Muestra si el clúster está afectado o no.
Tipo de clúster	Tipo de clúster. *Solo se admiten los tipos de clúster de cortafuegos CN-Series.*
Miembros afectados	Número de miembros del clúster afectados y sus nombres.
Detalles del registro del sistema	Muestra los detalles de los eventos del sistema.
Error específico	Lista de errores específicos en el clúster. Haga clic en el enlace para ver más detalles sobre el error en **Monitor (Supervisar)** > **Logs** > **System (Sistema)** donde puede ver los logs.
Nodo de clúster	Nombre del pod.
Recuento de CPU	Número de CPU utilizadas.

Monitorización

Vea la información de estado del clúster de cortafuegos CN-Series.



Campo	Description (Descripción)
Clúster de software administrado	Seleccione un clúster de cortafuegos. *Solo se admiten los tipos de clúster de cortafuegos CN-Series.*
Impactado	Lista de clústeres de cortafuegos afectados. • **CN-Clusters (Clústeres CN)**: el número de clústeres de cortafuegos de la serie CN afectados. • **Clusters Impacted (Clústeres afectados)**: muestra la lista de clústeres afectados. Haga clic para ver información detallada sobre los clústeres en los paneles **Interconnect Status (Estado de interconexión)** y **Cluster Utilization (Utilización del clúster)**.
ACEPTAR	Lista de clústeres de cortafuegos que no se ven afectados. • **Clusters (Clústeres)**: el número de clústeres de cortafuegos CN-Series que no se ven afectados. • **Clusters List (Lista de clústeres)**: muestra la lista de clústeres que no se ven afectados. Haga clic para ver información detallada sobre los clústeres en los paneles **Interconnect Status (Estado de interconexión)** y **Cluster Utilization (Utilización del clúster)**.
Estado de interconexión	Vea los detalles de interconexión del clúster para un marco de tiempo seleccionado. Seleccione **Last 5 Mins (Últimos 5 minutos)** para ver los siguientes detalles. • **Cluster Name (Nombre del clúster)**: nombre del clúster de cortafuegos. • **Cluster Type (Tipo de clúster)**: el tipo de clúster. *Solo se admiten tipos de clúster de cortafuegos de la serie CN.* • **Cluster Creation Time (Hora de creación del clúster)**: la hora de creación del clúster.

Campo	Description (Descripción)

	• **Current Cluster State (Estado actual del clúster)**: muestra si el clúster se ve afectado o no.
	  • **Current Cluster Detail (Detalle del clúster actual)**: haga clic en el vínculo del estado del clúster actual para ver más detalles sobre el clúster afectado.
	• **Cluster Interconnect Status (Estado de la interconexión del clúster)**: muestra la interconectividad del clúster.
	  • **Current Cluster Detail (Detalle del clúster actual)**: haga clic en el enlace de estado de interconexión actual para ver más detalles sobre el clúster afectado.
	• **Traffic Interconnect (Interconexión de tráfico)**: estado de la interconexión de tráfico.
	• **External Connection (Conexión externa)**: estado de la conectividad externa.
	• **Impacted Links (Enlaces afectados)**: número de enlaces afectados.
	• **Management Connectivity (Conectividad de gestión)**: número de conexiones de gestión.
	• **Impacted Cluster Member (Miembro del clúster afectado)**: lista de miembros del clúster afectados.
	• **Time Stamp Hi-Res Uptime (Tiempo de actividad de alta resolución de la marca de tiempo)**: marca de tiempo del tiempo de actividad
	• **Time Stamp Hi-Res Downtime (Tiempo de inactividad de alta resolución de la marca de tiempo)**: marca de tiempo de tiempo de inactividad.
	Al seleccionar cualquier otro período de tiempo, solo se muestra la siguiente información.
	• **Nombre de clústeres**
	• **Tipo de clúster**
	• **Hora de creación del clúster**
	• **Estado del clúster actual**
	• **Estado de la interconexión del clúster**
	• **Interconexión de tráfico**
	• **Conexión externa**

Utilización del clúster	Vea el rendimiento del clúster de cortafuegos, la memoria y la utilización de datos. • **Cluster Name (Nombre del clúster)**: nombre del clúster de cortafuegos. Al expandir el nombre del clúster, se muestran los detalles de todos los pods en dicho clúster. • **Cluster Details (Detalles del clúster)**: haga clic en el enlace del nombre del clúster para ver los detalles de rendimiento, memoria y uso de datos del clúster seleccionado.

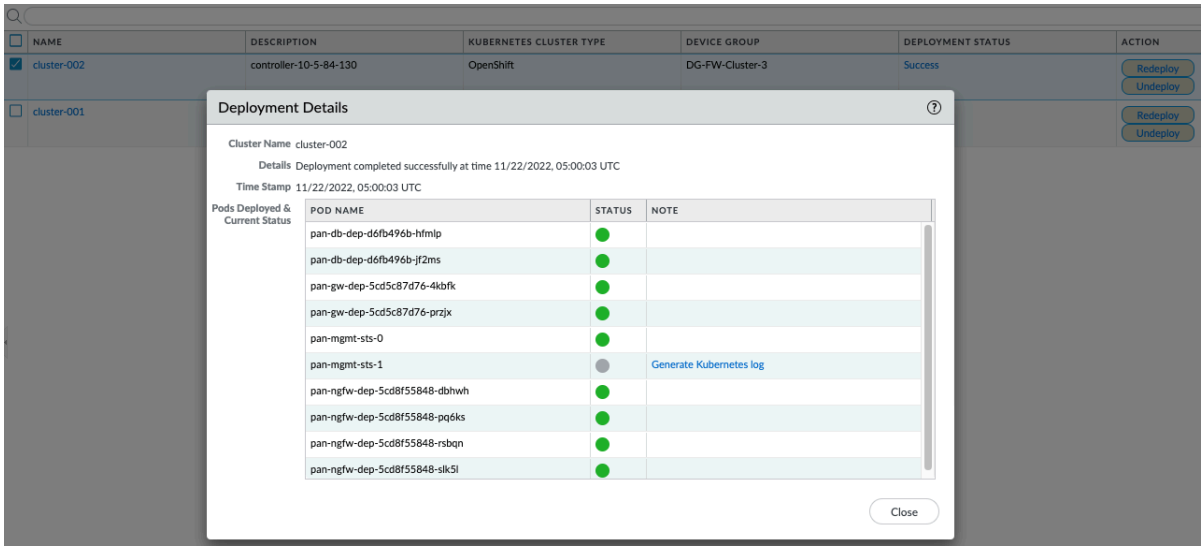
Campo	Description (Descripción)
	• **Cluster Type (Tipo de clúster)**: el tipo de clúster. *Solo compatible con los tipos de clúster de los cortafuegos CN-Series.* • **Cluster State (Estado del clúster)**: muestra el estado del clúster. • **Cluster Throughput (Gbps) [Rendimiento del clúster (Gbps)]**: rendimiento del clúster de cortafuegos en Gbps. • **CPS**: número de conexiones por segundo. • **Session Count (Sessions) [Recuento de sesiones (sesiones)]**: número de sesiones. • **Average Data Plane (%) Within Health Threshold [Plano de datos promedio (%) dentro del umbral de estado]**: el umbral del plano de datos promedio en porcentaje. • **Management Plane CPU (%) [CPU del plano de gestión (%)]**: utilización de la CPU del plano de gestión en porcentaje. • **Management Plane Mem (%) [Memoria del plano de gestión (%)]**: utilización de la memoria del plano de gestión en porcentaje. • **Logging Rate (Log/Sec) [Tasa de registro de logs (log/seg.)]**: tasa a la que se generan los logs en el clúster. • **DP Auto-Scale Status (Estado de escalado automático de DP)**: detalles de escalado automático del plano de datos.

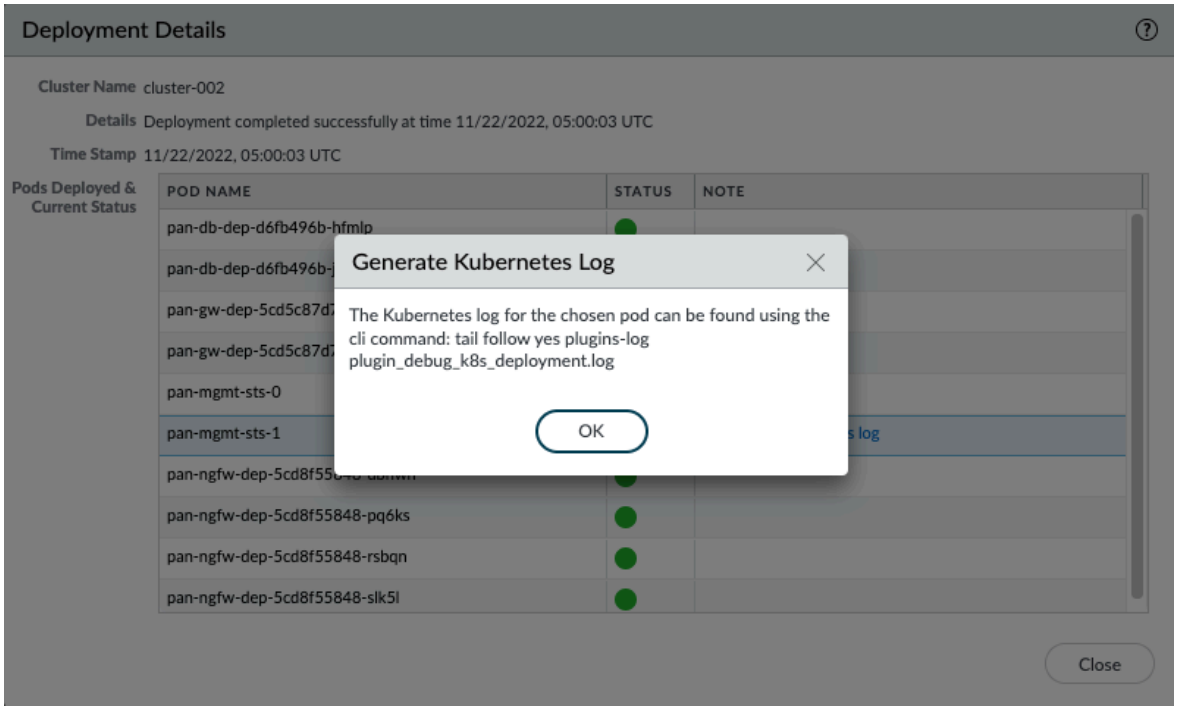
Validación de la implementación de CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Puede validar las implementaciones del CN-Series HSF en la sección **Deployment (Implementación)** en **Panorama** > **Kubernetes**. Haga clic en el vínculo situado en **Deployment Status (Estado de implementación)** para ver los detalles de la implementación.

Los pods implementados y su estado actual están codificados por colores y se muestran en la sección **Deployment Status (Estado de implementación)**. Puede hacer clic en el enlace en la **Note (Nota)** de la implementación fallida del pod para ver más detalles.





Utilice los siguientes comandos de la CLI de Panorama para generar logs.

```
debug plugins kubernetes generate-pod-log deployment_name pod_name
 <value> Name of the pod
```

```
show plugins kubernetes deployment-status
```

```
show plugins kubernetes deployment-details name
```

Problemas de sincronización de depuración entre el complemento de Kubernetes y el CN-series HSF

El complemento de Kubernetes recopila información sobre el CN-Series HSF de los pods, servicios y nodos mediante las API de Watch. La API de Watch es una API basada en notificaciones que envía actualizaciones cuando cambia el estado de un clúster. Para asegurarse de que el complemento y el CN-Series HSF implementado estén sincronizados, el complemento escucha las notificaciones y muestra las notificaciones de HPA y eventos de actualización/degradación.

El complemento utiliza los siguientes comandos de depuración para depurar un nodo específico en función del estado del complemento.

```
debug plugin kubernetes kubectl-logs pod <pod-name>
```

Este comando de depuración genera un archivo de log que contiene los logs de descripción `kubectl` para el nodo pasado en el comando, y se guarda en el archivo de logs del complemento.

HPA basado en métricas personalizadas mediante KEDA en entornos EKS

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

La implementación de HPA en entornos EKS requiere el uso de KEDA (Escalado automático controlado por eventos de Kubernetes). Los siguientes son requisitos previos para la implementación de HPA basada en métricas personalizadas:

- Habilite HPA para la agrupación en clústeres desde YAML.
  - Asegúrese de que los parámetros de HPA estén completos en el archivo pan-cn-mgmt-configmap.yaml.
  - Asegúrese de que el campo `PAN_NAMESPACE_EKS` tenga un nombre único en su cuenta de AWS en su región. Esto impide sobrescribir métricas de diferentes clústeres de CN con el mismo espacio de nombres EKS.
- Métricas de publicación de CN-MGMT en Cloudwatch.

  El pod de CN-MGMT requiere los permisos necesarios para acceder al recurso de Cloudwatch, recopilar métricas de CN-NGFW y publicar métricas personalizadas en Cloudwatch. Esto se hace añadiendo la política `CloudWatchFullAccess` a la función de IAM del nodo que especificó al crear el grupo de nodos.
- Implemente el escalador automático de clúster de AWS. Para obtener más información, consulte Escalador automático de clúster.

Autenticar KEDA con AWS

Para autenticar KEDA, puede asociar una función de IAM con la cuenta de servicio del operador de keda anotando el rol-arn en la cuenta de servicio de keda. Se recomienda este paso porque evita añadir el acceso de Cloudwatch a la función de IAM del nodo y permite que solo la cuenta de servicio de keda obtenga acceso a Cloudwatch y no todo el nodo en el que se ejecuta keda.

Para asociar una función de IAM con la cuenta de servicio del operador keda:

1. Cree un proveedor OIDC de IAM para su clúster: debe crear un proveedor OIDC de IAM solo una vez para un clúster.
2. Cree una función de IAM y adjúntelo a una política de IAM con los permisos que necesitan sus cuentas de servicio. Asegúrese de proporcionar la política de acceso de Cloudwatch mientras realiza este paso.
3. Asociar una función de IAM con una cuenta de servicio: complete esta tarea para cada cuenta de servicio de Kubernetes que necesite acceso a los recursos de AWS.
4. Implemente el escalador automático de clúster de AWS. Para obtener más información, consulte Escalador automático de clúster.

Implementación de los pods de KEDA

Para implementar los pods de Keda, descargue los archivos keda más recientes.

```
kubectl apply -f keda-2.7.1.yaml
```

El complemento modifica y aplica el yaml en función de las entradas que proporcione, según sus requisitos de escalado.

Observe los valores en la consola de Cloudwatch y verifique cómo los pods de destino aumentan o disminuyen.

Configurar enrutamiento dinámico en CN-Series HSF

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación del cortafuegos CN-Series HSF	• Panorama con la versión PAN-OS 11.1 como mínimo

CN-Series Hyperscale Security Fabric (HSF) ahora introduce el enrutamiento dinámico a través de protocolos BGP y BGP sobre BFD. Mediante el enrutamiento dinámico, puede lograr un enrutamiento de capa 3 estable, de alto rendimiento y altamente disponible a través de listas de filtrado basadas en perfiles y mapas de rutas condicionales que se pueden usar en enrutadores lógicos. Estos perfiles proporcionan una granularidad más detallada para filtrar rutas para cada protocolo de enrutamiento dinámico y mejorar la redistribución de rutas a través de varios protocolos.

BGP busca las rutas disponibles que los datos podrían recorrer y elige la mejor ruta, basándose en los prefijos IP que están disponibles dentro de los sistemas autónomos. La configuración de Detección de reenvío bidireccional (BFD) gestiona los pods CN-GW y los fallos de ruta.

Para habilitar el enrutamiento dinámico, deberá configurar el Panorama y el clúster CN-Series HSF. Necesitará en el clúster al menos 2 CN-MGMT, 2 CN-NGFW, 2 CN-DB y 1 CN-GW. El emparejamiento BGP se configura entre el clúster CN y el enrutador externo.

En el CN-Series HSF, el enrutamiento dinámico será compatible con PANOS 11.x.x. Para obtener información sobre la obtención de PAN-OS 11.0, consulte Obtener las imágenes y archivos para la implementación de la CN-Series.

En el Panorama, deberá configurar los grupos de dispositivos y gestionar el clúster HSF a través del grupo de dispositivos. Para configurar el clúster HSF, consulte Implementación del clúster HSF.

Para configurar BGP en el clúster HSF, deberá realizar los siguientes pasos:

1. Habilitar enrutamiento avanzado.
2. Configurar un enrutador lógico.
3. Cree una ruta estática para la interfaz de bucle invertido de CN-GW.
4. Configuración de BGP en un motor de enrutamiento avanzado.

   1. *Actualmente, solo IPv4 es compatible con el enrutamiento BGP.*
   2. *Al crear un par, asegúrese de crear una sesión de bucle invertido y proporcione una dirección IP de bucle invertido para cada CN-GW en la pestaña* ***Direccionamiento****.*
5. (opcional) Cree perfiles de enrutamiento BGP para autenticación, temporizadores, familias de direcciones, amortiguación, redistribución de rutas a BGP y filtrado BGP.
6. (opcional) Cree filtros para el motor de enrutamiento avanzado, como listas de acceso, listas de prefijos, listas de acceso de ruta AS, listas comunitarias y mapas de rutas.
7. Haga clic en**Commit to Panorama (Confirmar en Panorama)**. Después de que la configuración se confirme con Panorama, BGP se configurará para cada CN-GW.

Para comprobar el estado de BGP, inicie sesión en CN-MGMT y ejecute los siguientes comandos:

- Mostrar resumen bgp de enrutamiento avanzado


```
admin@pan-mgmt-sts-1.cluster-001> show advanced-routing bgp route logical-router slot1-LR-1

Status codes:  R removed, d damped, * valid, r ribFailure, S stale, = multipath,
               s suppressed, i internal, > best, h history
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  e egp, i igp, ? incomplete

Logical router: slot1-LR-1
BGP table version is 10, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24           0.0.0.0                  0    100  32768  i
*> 192.168.85.0/24      200.0.0.1                0    100      0 22 i
------------------------------------------------------------------------------
Displayed 2 route(s) 2 path(s)

Logical router: slot1-LR-1
BGP table version is 0, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
------------------------------------------------------------------------------
Displayed 0 route(s) 0 path(s)

admin@pan-mgmt-sts-1.cluster-001> show advanced-routing route type bgp logical-router slot1-LR-1



Logical Router: slot1-LR-1
==========================
flags: A:active, E:ecmp, Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext 1, O2:ospf ext 2

destination                             protocol        nexthop                                 distance  metric    flag      tag       age          inte
ace
192.168.85.0/24                         bgp             200.0.0.1                               20        0         A E               00:04:07

192.168.85.0/24                         bgp             2.2.2.222                               20        0         A E               00:04:07     ethe
et1/3
total route shown: 2
```

- Mostrar el estado del peer bgp de enrutamiento avanzado

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer status peer-name DHCP-PEER

Logical Router: Slot1-LR
==============
Peer Name:              DHCP-PEER
BGP State:              Established, up for 00:01:15
```


- Mostrar detalles del peer bgp de enrutamiento avanzado


```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer details

Peer: DHCP-PEER
==============
Peer name                   DHCP-PEER
Logical router:             Slot1-LR
Remote router ID:           11.11.11.1
Remote AS:                  65008
Remote address:             192.168.100.109:34986
Local address:              192.168.100.102:179
Peer group:                 DHCP-BGP
Peer status:                Established
Up time:                    188 s
Hold time:                  90 s (configured 90)
Keepalive interval:         30 s (configured 30)
Connection retry timer:     15 s
Estimated RTT:              3 ms
Last reset time:            222 s ago
Last reset reason:          No AFI/SAFI activated for peer
BGP connection:             sharedNetwork
Connection established:     2
Connection dropped:         1

Address family:             ipv4Unicast
  Packet queue length:      0
  Update group id:          2
  Sub group id:             2
  Prefix allowed Max:       1000 (warning-only)
  Prefix accepted:          2810
  Prefix Sent:              2920
  Prefix allowed Max warnning: True
  Prefix allowed warnning threshold: 100
  Inbound soft reconfiguration allowed: True

Neighbor capabilities:
  4byteAs                   advertisedAndReceived
  extendedMessage           advertisedAndReceived
  addPath                   {'ipv4Unicast': {'rxAdvertisedAndReceived': True}}
  routeRefresh              advertisedAndReceivedOldNew
  enhancedRouteRefresh      advertisedAndReceived
  multiprotocolExtensions   {'ipv4Unicast': {'advertisedAndReceived': True}}
  hostName                  {'advHostName': 'pan-mgmt-sts-1.testing', 'advDomainName': 'n/a', 'rcvHostName': 'vyos', 'rcvDomainName': 'n/
  gracefulRestart           advertisedAndReceived
admin@pan-mgmt-sts-1.testing>
```

Para comprobar el estado de BFD de CN-MGMT, ejecute los siguientes comandos

- `mostrar resumen de bfd de enrutamiento avanzado`

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd summary

SESSION ID: 114
    Interface:      ethernet1/3
    Logical Router: Slot1-LR (id:1)
    Local IP Address:          192.168.100.104
    Neighbor IP Address:       192.168.100.109

    Discriminator (local/remote):  0xb150bb9e / 0x4a1dc50a
    State:           up
    rState:          up
    Up Time:         0d 0h 8m 23s 670ms
    Agent DP:        Slot 9 - DP 0
    Errors:          0
```


- mostrar detalles de bfd de enrutamiento avanzado

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd details

BFD Session ID: 114
    Version:          1
    Interface:        ethernet1/3
    Protocol:         BGP
    Local IP Address:           192.168.100.104
    Neighbor IP Address:        192.168.100.109

    BFD profile:                default

    State (local/remote):             up / up
    Up Time:          0d 0h 8m 46s 650ms
    Discriminator (local/remote):  0xb150bb9e / 0x4a1dc50a
    Mode:             Active
    Demand Mode:      Disabled
    Poll Bit:         Disabled
    Multihop:         Disabled
    Multihop TTL:     255
    Local Diag Code:                  0 (No Diagnostic)
    Last Received Remote Diag Code:   0 (No Diagnostic)

    Transmit Hold Time:               0ms
    Desired Min Tx Interval:          1000ms
    Required Min Rx Interval:         1000ms
    Received Min Rx Interval:         1000ms
    Negotiated Transmit Interval:     1000ms
    Detect Multiplier:                3
    Received Multiplier:              3
    Detect time (exceeded):           3000ms (1)
    Tx Control Packets (last):        649 (861ms ago)
    Rx Control Packets (last):        604 (669ms ago)
    Agent DP:         Slot 9 - DP 0
    Errors:           0

    Last Recieved Packet:
        Version:          1
        My Discriminator:           0x4a1dc50a
        Your Discriminator:         0xb150bb9e
        Diag Code:        0 (No Diagnostic)
        Length:           24
        Demand bit:       0         Poll bit:         0
        Final bit:        0         Multipoint:       0
        Control Plane Independent:      0
        Authentication Present:         0
        Desired Min Tx Interval:        1000ms
        Required Min Rx Interval:       1000ms
        Detect Multiplier:              3
        Required Min Echo Rx Interval: 50ms
```


CN-Series HSF: Casos de uso

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Los siguientes son los casos de uso para CN-Series HSF:

- Pruebas de tráfico 5G
  - Seguridad 5G con política de correlación y visibilidad N3+N4
  - Protección de entrada/salida con identificación de aplicaciones e inspección de amenazas
- Ampliación de los cortafuegos en función de las métricas personalizadas compatibles
- Caso de prueba: Gestión de los fallos de CN-MGMT
- Caso de prueba: Gestión de los fallos de CN-NGFW
- Caso de prueba: Gestión de los fallos de CN-DB

Pruebas de tráfico 5G

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versiones superiores • Helm 3.6 or above version client

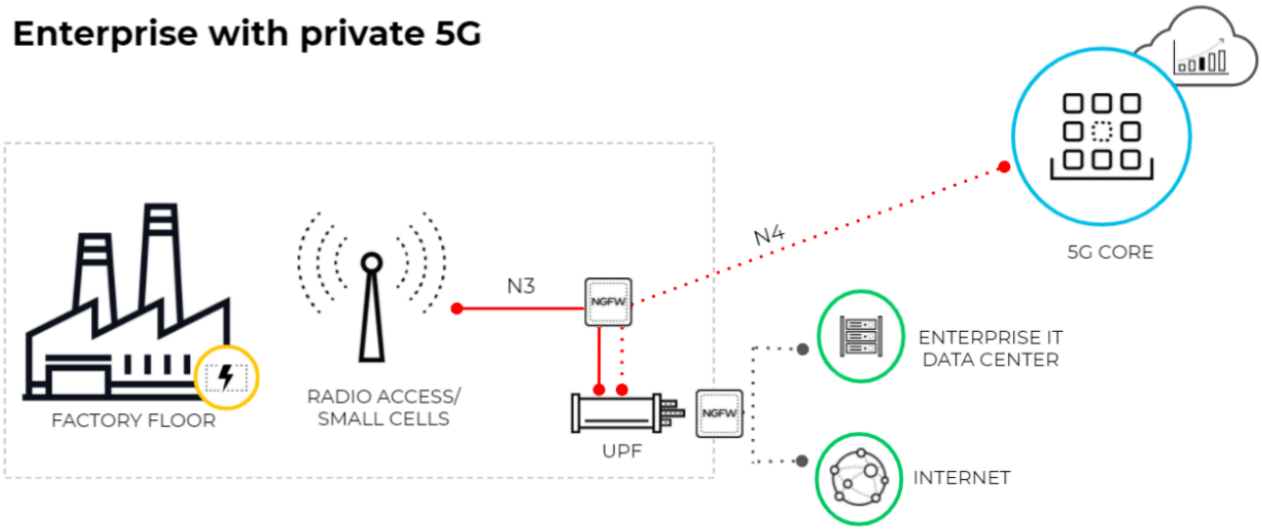
Proteger el borde de la red requiere equilibrar la inspección y el control del tráfico (requisitos de seguridad) con un ancho de banda alto, una latencia baja y acceso en tiempo real (experiencia del usuario). Estos problemas son exponencialmente más difíciles si muchos cortafuegos procesan el tráfico, si las aplicaciones se alojan en sitios perimetrales o si el perímetro de la red es un punto de agregación para datos de IoT. Además, la separación del usuario y el plano de control en las redes 5G dificulta la aplicación de políticas de seguridad a nivel de suscriptor o dispositivo, y carece de visibilidad basada en el contexto para las amenazas. Los cortafuegos colocados con la interfaz N3 y N4 proporcionan:

- Visibilidad del nivel de señalización entre dispositivos conectados
- Inspección de estado de PFCP y GTP-U
- Correlación de ID de suscriptor/ID de equipo/ID de segmento con vulnerabilidades de tráfico GTP-U

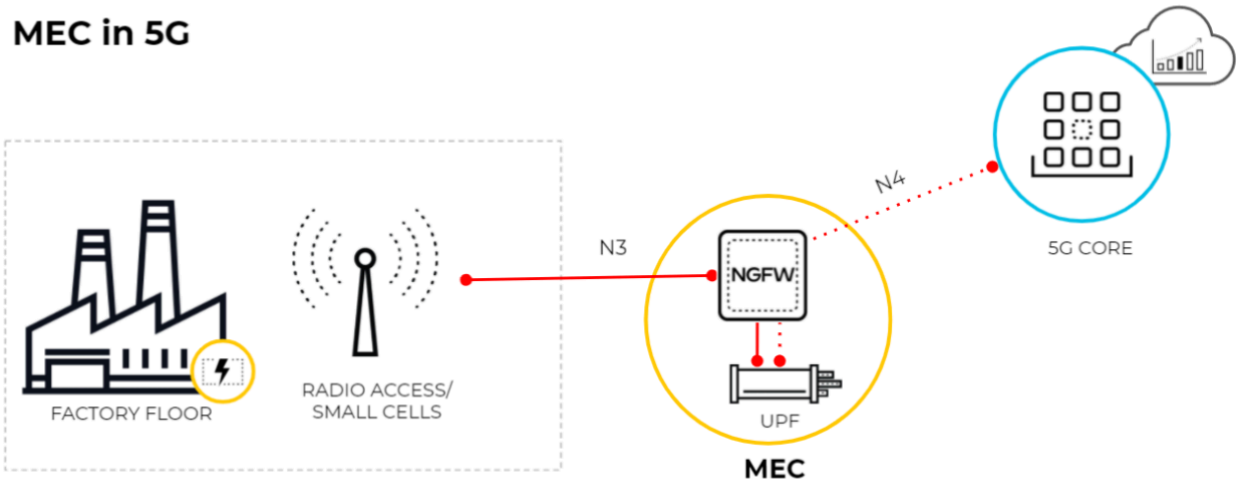
Los siguientes son los casos de uso de tráfico 5G para la serie CN-Series HSF:

- Seguridad 5G con política de correlación y visibilidad N3+N4
- Protección de entrada/salida con identificación de aplicaciones e inspección de amenazas

El siguiente diagrama ilustra una empresa que utiliza una red 5G privada. Las funciones principales de 5G están basadas en la nube o en el sitio central del proveedor de servicios. La conexión entre el acceso 5G y la UPF utiliza la interfaz N3. Los túneles GTP-U transportan el tráfico del plano de usuario en la interfaz N3. La conexión entre la UPF y la Función de gestión de sesiones (SMF) utiliza la interfaz N4. El protocolo PFCP intercambia reglas de reenvío de paquetes mediante intercambios UDP en la interfaz N4.



Este diagrama ilustra MEC en una red 5G donde la Función de plano de usuario (UPF) está en el borde o en la ubicación MEC y las funciones principales de 5G están basadas en la nube o en el sitio central del proveedor de servicios. La conexión entre el acceso 5G y la UPF utiliza la interfaz N3 y los túneles GTP-U transportan el tráfico del plano de usuario por la interfaz N3. La conexión entre UPF y SMF usa la interfaz N4 y el protocolo PFCP intercambia reglas de reenvío de paquetes usando UDP en la interfaz N4.



Seguridad 5G con política de correlación y visibilidad N3+N4

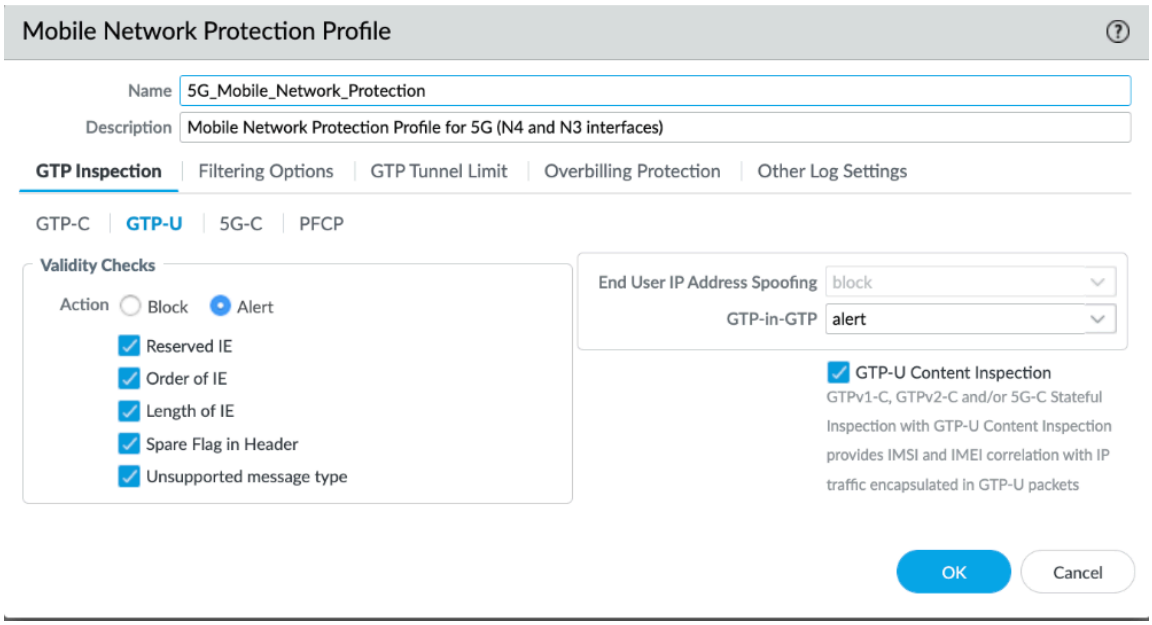
Este caso de prueba evalúa la capacidad del clúster CNF para inspeccionar y proteger el tráfico de las interfaces N3+N4.

STEP 1 | Como primer paso para inspeccionar y proteger el tráfico de las interfaces N3+N4, deberá habilitar GTP Security.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)** y seleccionar **GTP-U Security**.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** para confirmar el cambio.
5. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y **Reboot Device (Reiniciar dispositivo)**.

STEP 2 | Cree un perfil de protección de red móvil y habilite la inspección GTP-U.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Mobile Network Protection (Protección de red móvil)**.
2. Deberá **Add (Añadir)** un perfil e introducir un **Name (Nombre)**, como **`5G_Mobile_Network_Protection`**.
3. En la pestaña **PFCP** , habilite **Stateful Inspection (Inspección con estado)**.



STEP 3 | Seleccione las comprobaciones de estado que desea que realice el cortafuegos en el tráfico PFCP y la acción que desea que realice el cortafuegos si una comprobación de estado da error.

1. Determine las comprobaciones de estado que desea utilizar.
   - **Check Association Messages (Comprobar mensajes de asociación)**: comprueba si hay mensajes de asociación PFCP que estén fuera de servicio o que hayan sido rechazados.
   - **Check Session Messages (Comprobar mensajes de sesión)**: comprueba si hay mensajes de sesión PFCP que estén fuera de servicio o que se hayan rechazado; verifica que todos los mensajes de la sesión PFCP coincidan con una asociación PFCP existente; alerta o elimina los mensajes de sesión PFCP que llegan antes de que se configure la asociación PFCP.
   - **Check Sequence Number (Comprobar número de secuencia)**: confirma que el número de secuencia en la respuesta del PFCP coincide con el número de secuencia del mensaje de solicitud del PFCP anterior.
2. Seleccione la acción que desea que realice el cortafuegos si la comprobación de estado no es correcta.
   - **allow (permitir)**: permite el tráfico y no genera una entrada de log en el log de GTP.
   - **block (bloquear)**: bloquea el tráfico y genera una entrada de log de gravedad alta en el log de GTP.
   - **alert (alerta)**: (predeterminado) permite el tráfico y genera una entrada de log de gravedad alta en el log de GTP.

STEP 4 | (Opcional) Configure el registro para la inspección de PFCP.

1. Seleccione cuándo desea que el cortafuegos genere una entrada de log.
   - **Log al inicio de la asociación PFCP**
   - **Log al final de la asociación PFCP**
   - **Log al iniciar sesión PFCP**
   - **Log al finalizar sesión PFCP**

STEP 5 | Habilite la configuración de Otro log para mensajes PFCP y GTP-U

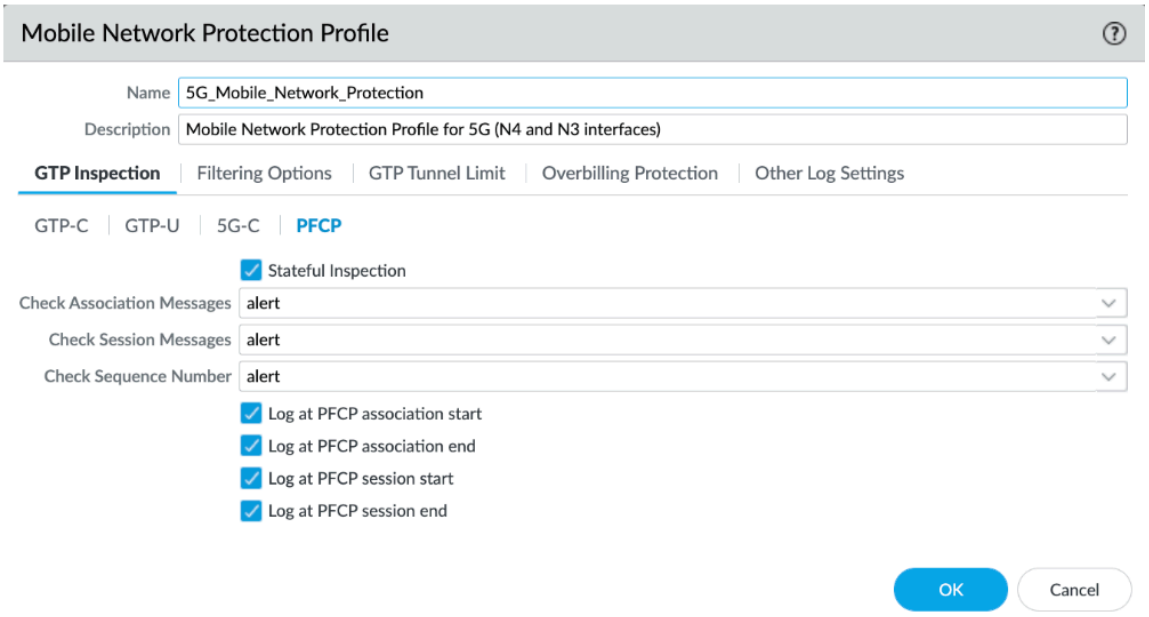
1. En la pestaña **Other Log Settings (Configuración de Otro log)**, seleccione el tipo de **PFCP Allowed Messages (Mensajes permitidos de PFCP)** que desea incluir en los logs.

   Habilite estas opciones solo para la resolución de problemas.

   - **Establecimiento de sesión**: estos mensajes de PFCP configuran la sesión, incluido el establecimiento del túnel GTP-U.
   - **Modificación de sesión**: estos mensajes de PFCP se envían si el ID de sesión o PDR ID cambia (por ejemplo, como resultado de pasar de una red 4G a una 5G. Incluye mensajes,

como la solicitud de modificación de sesión PFCP y la respuesta de modificación de sesión PFCP.

- **Eliminación de sesión**: estos mensajes de PFCP finalizan la sesión de PFCP, incluida la liberación de recursos asociados.



STEP 6 | Cree dos políticas de seguridad con origen y destino como interfaces N3 y N4, Aplicación como GTP-U y PFCP respectivamente.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** una regla de política de seguridad por **Name (Nombre)**
2. Seleccione la pestaña **Source (Origen** y elija **Add (Añadir)** una **Source Zone (Zona de origen)** o seleccione **Any (Cualquiera)**.
3. Para **Source Address (Dirección de origen)**, debe **Add (Añadir)** los objetos de dirección para los endpoints del elemento 5G en la interfaz N3.
4. Para **Destination (Destino)**, deberá **Add (Añadir)** los objetos de dirección de **Destination Address (Dirección de destino)** para los endpoints del elemento 5G en la interfaz N3.
5. **Add (Añadir)** las **Applications (Aplicaciones)** en permitir, como el plano de usuario, el cual es **GTP-U** y **PFCP**.
6. En la pestaña **Actions (Acciones)** , seleccione la **Action (Acción)**, como **Allow (Permitir)**.
7. Seleccione el perfil **Mobile Network Protection (Protección de red móvil)** que creó.
8. Seleccione otros perfiles que desee aplicar, como **Vulnerability Protection (Protección frente a vulnerabilidades)**.
9. Seleccione Log Settings (Configuración de log), como **Log at Session Start (Log al iniciar sesión)** y **Log at Session End (log al finalizar sesión)**.
10. Haga clic en **OK (Aceptar)**.
11. Del mismo modo, cree otra política de seguridad para la interfaz N4.

STEP 7 | (Opcional) Cree otra regla de política de seguridad basada en la protección basada en ID de equipo/ID de suscriptor/ID de segmento de red, introduciendo la información de EDL en la fuente.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** una regla de política de seguridad por **Name (Nombre)**, por ejemplo, Seguridad de ID de equipo.
2. Seleccione la pestaña **Source (Origen** y elija **Add (Añadir)** una **Source Zone (Zona de origen)** o seleccione **Any (Cualquiera)**.
3. **Add (Añadir)** uno o más ID de **Source Equipment (Equipo de origen)** en cualquiera de los siguientes formatos:
   - Identificador de equipo permanente (PEI) 5G, incluido IMEI
   - IMEI (15 o 16 dígitos)
   - Prefijo de IMEI de ocho dígitos para el código de asignación de tipo (TAC, Type Allocation Code).
   - EDL que especifica IMEI.
4. (Opcional) Puede añadir nombres de **Source Subscriber (Suscriptor de origen)** y **Network Slice (Segmento de red)** a esta regla de política de seguridad para que la regla sea más restrictiva.
5. Especifique la **Destination Zone (Zona de destino)**, la **Destination Address (Dirección de destino)** y el **Destination Device (Dispositivo de destino)** como **Any (Cualquiera)**.
6. **Add (Añadir)** las **Applications (Aplicaciones)** a permitir, por ejemplo, **ssh**, **ssl**, **radmin**y **telnet**.
7. En la pestaña **Actions (Acciones)** , seleccione la **Action (Acción)**, como **Allow (Permitir)**.
8. Seleccione los perfiles que desea aplicar, como **Antivirus**, **Vulnerability Protection (Protección frente a vulnerabilidades)**y **Anti-Spyware (Antispyware)**.
9. Seleccione Log Settings (Configuración de log), como **Log at Session Start (Log al iniciar sesión)** y **Log at Session End (log al finalizar sesión)**.
10. Haga clic en **OK (Aceptar)**.

    Resultado esperado de la prueba:
    - Verifique los logs de GTP-U en la sección del monitor.
    - Verifique la sección de detalles del log para ver la información del suscriptor, el equipo y la porción de la red.
    - Observe que el número de aciertos de la regla aumenta.

Protección de entrada/salida con identificación de aplicaciones e inspección de amenazas

Este caso de prueba evalúa la capacidad del clúster CNF para inspeccionar y proteger el tráfico de entrada y salida en la interfaz N6.

La interfaz N6 transporta tráfico de texto claro a través de TCP/UDP hacia Internet. Ahora, con el cortafuegos VM-series implementado en la interfaz N6, puede obtener una visibilidad completa del uso de la aplicación. El cortafuegos puede implementar seguridad con suscripción CDSS como - Prevención de amenazas (TP), Adv-URL Filtering, Wildfire, DNS Security en el tráfico permitido.

Los siguientes pasos son un esquema para ejecutar este caso de prueba. Para obtener detalles sobre la ejecución de pasos individuales, consulte Seguridad 5G con política de correlación y visibilidad N3+N4.

STEP 1 | Cree una política de seguridad para la interfaz N6 con las zonas y la interfaz adecuadas.

STEP 2 | Utilice los perfiles de seguridad predeterminados o cree una categoría personalizada para el filtrado de URL, Wildfire, protección frente a vulnerabilidades, etc.

STEP 3 | (Opcional) Cree un perfil personalizado para la URL permitida en la categoría de URL.

STEP 4 | (Opcional) Cree varias políticas de seguridad que coincidan con diferentes criterios. Al crear la política de seguridad, seleccione los perfiles creados en el paso 3.

STEP 5 | Envíe el tráfico.

STEP 6 | Envíe el tráfico malicioso en direcciones de entrada/salida y verifique si el tráfico está bloqueado.

Resultado previsto:

- El recuento de resultados de la política aumenta.
- Verifique los logs apropiados para el filtrado de URL, el tráfico y los logs de amenazas.

Ampliación de los cortafuegos en función de las métricas personalizadas compatibles

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Esta prueba ayuda a validar la capacidad del clúster del CN-Series HSF para el escalado automático, en función del objetivo de valor de métrica personalizado especificado en el escalado automático.

STEP 1 | Habilite el escalado automático mientras crea el clúster del CN-series HSF para el escalado automático en función del valor objetivo de la métrica personalizada especificado en el escalado automático. Para obtener más información, consulte Implementación del clúster HSF

STEP 2 | Introduzca el espacio de nombres de CloudWatch para enviar métricas a AWS CloudWatch.

STEP 3 | Introduzca la región del clúster de EKS.

STEP 4 | Introduzca el intervalo de envío.

STEP 5 | Seleccione la métrica de escalado automático. En este ejemplo, es posible que desee elegir PansessionActive.

STEP 6 | Especifique el umbral de reducción horizontal y el umbral de escalado horizontal Por ejemplo, si tiene 2 pods de NGFW en ejecución y el número total de sesiones en el cortafuegos actualmente es 1000, la métrica de vigilancia en la nube mostrará 500 (por pod de NGFW).

STEP 7 | Puede establecer el umbral de escalado horizontal en 250 y el escalado automático debería generar 2 pods de NGFW más.

STEP 8 | Use el comando show session info en el pod de MGMT para obtener la información de la sesión

STEP 9 | Puede especificar el número máximo y mínimo de pods de NGFW que pueden realizar un escalado automático.

Resultado previsto: El pod de NGFW debe realizar un escalado automático en función del valor de umbral de escalado horizontal

Caso de prueba: Gestión de los fallos de CN-MGMT

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Esta prueba evalúa la gestión de fallos de CN-NGMT.

El número mínimo deseado de pods CN-MGMT para una implementación de CN-Series HSF es dos para garantizar la gestión de fallos. Después de la implementación, el pod CN-MGMT que se activa primero se convierte en el Líder y el segundo CN-MGMT se convierte en Seguidor. Ambos pods CN-MGMT tienen la misma configuración. En cualquier instancia, un pod CN-MGMT está en estado LISTO. Los pods CN-DB, CN-GW y CN-NGFW se conectan al pod CN-MGMT en estado LISTO a través de enlaces de Interconexión de tráfico (TI).

Los dos pods CN-MGMT no están en modo HA activo-pasivo o HA activo-activo. Ambos pods tienen la misma configuración y se configuran mediante Panorama.

El fallo del pod CN-MGMT se produce debido a una de las siguientes condiciones.

- La comprobación de actividad falla
  - Si `slotd` está inactivo
  - Si `ipsec` o `strongswan` está inactivo
- El pod CN-MGMT se bloquea y se reinicia

STEP 1 | Desde la CLI de Panorama, introduzca `mostrar nombre de clústeres<cluster-name>` para ver el pod CN-MGMT líder y seguidor.

El siguiente resultado muestra que el pod **`pan-mgmt-sts-1`** está activo.

```
Cluster: cluster-001 Creation time: 2022/11/30 03:23:50 CN-MGMT pods: 88C00D31E1FC86B
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196 (active,
 pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------- 5
 pan-db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW
 11.0.1-c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-
ngfw-dep-668965d598-s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW
 11.0.1-c183.dev_e_rel 9 pan-ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-
db-dep-6774cd774d-gjpkr CN-DB 11.0.1-c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-
c183.dev_e_rel
```


STEP 2 | Vea la pertenencia del clúster para el pod **pan-mgmt-sts-1** y el estado de los pods CN-DB, CN-GW y CN-NGFW desde la CLI del controlador de Kubernetes.

1. Introduzca `kubectl get pods -n kube-system` para ver el estado de todos los pods.

   Resultado:

   El **pan-mgmt-sts-1** está activo. Todos los pods CN-DB, CN-GW y CN-NGFW están conectados a **pan-mgmt-sts-1**.

   ```
   NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 69m
    pan-db-dep-6774cd774d-k49cm 1/1 Running 0 69m pan-gw-dep-d849c7df8-4sk54 1/1
    Running 0 69m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 69m pan-mgmt-sts-0
    0/1 Running 0 83m pan-mgmt-sts-1 1/1 Running 0 83m pan-ngfw-dep-668965d598-
   pmmjd 1/1 Running 0 69m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 69m pan-
   ngfw-dep-668965d598-s2zcc 1/1 Running 0 69m pan-ngfw-dep-668965d598-vf9l4 1/1
    Running 0 69m
   ```

2. Compruebe la pertenencia al clúster desde **pan-mgmt-sts-1**.

   Entre en el pod **pan-mgmt-sts-1**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   Verifique si todos los pods CN-DB, CN-GW y CN-NGFW están conectados al pod líder CN-MGMT usando el siguiente comando.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Resultado:

   ```
   MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
    ================================================================================ 1 CN-GW
    192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 :: UP UP NA 2 CN-GW 192.168.23.100
    192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP
    UP 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9
    CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
   ```

3. Compruebe la pertenencia al clúster desde **pan-mgmt-sts-0**.

   Entre en el pod **pan-mgmt-sts-0**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
   ```

   ```
   su - admin
   ```

   Compruebe si algún pod CN-DB, CN-GW y CN-NGFW está conectado al pod CN-MGMT del seguidor usando el siguiente comando.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Resultado:

   ```
   No hay información de miembros presente
   ```


STEP 3 | Pruebe la gestión de fallos del pod CN-MGMT.

1. Desde la CLI del controlador de Kubernetes, introduzca el siguiente comando para eliminar el pod líder **pan-mgmt-sts-1** .

```
kubectl -n kube-system delete pod pan-mgmt-sts-1
```

2. Desde la CLI de Panorama, introduzca `mostrar nombre de clústeres<cluster-name>` para ver el nuevo pod CN-MGMT de líder y seguidor.

   El siguiente resultado muestra que el pod **pan-mgmt-sts-0** ahora está activo.

```
Cluster: cluster-001 Creation time: 2022/11/30 03:23:50 CN-MGMT pods: 88C00D31E1FC86B
 (active, pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196
 (pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------- 5 pan-
db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW 11.0.1-
c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-ngfw-dep-668965d598-
s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW 11.0.1-c183.dev_e_rel 9 pan-
ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-db-dep-6774cd774d-gjpkr CN-DB 11.0.1-
c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-c183.dev_e_rel
```

STEP 4 | Vea la pertenencia del clúster para el pod **pan-mgmt-sts-0** y el estado de los pods CN-DB, CN-GW y CN-NGFW desde la CLI del controlador de Kubernetes.

1. Introduzca `kubectl get pods -n kube-system` para ver el estado de todos los pods.

   Resultado:

   El **pan-mgmt-sts-0** está activo. Todos los pods CN-DB, CN-GW y CN-NGFW están conectados a **pan-mgmt-sts-1**.

```
NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 76m
 pan-db-dep-6774cd774d-k49cm 1/1 Running 0 76m pan-gw-dep-d849c7df8-4sk54 1/1
 Running 0 76m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 76m pan-mgmt-sts-0
 1/1 Running 0 90m pan-mgmt-sts-1 0/1 Running 0 90m pan-ngfw-dep-668965d598-
pmmjd 1/1 Running 0 76m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 76m pan-
ngfw-dep-668965d598-s2zcc 1/1 Running 0 76m pan-ngfw-dep-668965d598-vf9l4 1/1
 Running 0 76m
```

2. Compruebe la pertenencia al clúster desde **pan-mgmt-sts-0**.

   Entre en el pod **pan-mgmt-sts-0**.

```
kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
```

```
su - admin
```

   Verifique si todos los pods CN-DB, CN-GW y CN-NGFW están conectados al pod líder CN-MGMT usando el siguiente comando.

```
show cluster-membership show-slot-info slot all
```

   Resultado:

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ============================================================================== 1 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 :: UP UP NA 2 CN-GW 192.168.23.100
 192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP
 UP 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9
 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```


3. Compruebe la pertenencia al clúster desde **pan-mgmt-sts-1**.

   Entre en el pod **pan-mgmt-sts-1**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   Compruebe si algún pod CN-DB, CN-GW y CN-NGFW está conectado al pod CN-MGMT del seguidor usando el siguiente comando.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Resultado:

   ```
   No hay información de miembros presente
   ```

Resultado de la prueba: Cuando el pod líder `pan-mgmt-sts-1` falla, el pod seguidor `pan-mgmt-sts-0` se convierte en el nuevo líder. Este mecanismo de gestión de fallos de CN-MGMT garantiza que el flujo de tráfico no se interrumpa. Sin efecto en las sesiones existentes o nuevas.

Caso de prueba: Gestión de los fallos de CN-NGFW

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Esta prueba evalúa la gestión de fallos de CN-NGFW.

El fallo de CN-NGFW puede producirse en las siguientes circunstancias.

- Problemas de nodo
- El pod CN-NGFW se bloquea y se reinicia
- El nodo y el pod CN-NGFW están bien, pero **pan_task** se bloquea
- CN-NGFW se elimina de la pertenencia al clúster cuando:
  - La supervisión de IPsec en la interfaz Eth0 falla
  - El enlace de interconexión del clúster (CI) está roto
  - El enlace de interconexión del tráfico (TI) está roto

En este escenario, la sesión SSH entre el cliente y el servidor se instala en CN-NGFW 1. Si el CN-NGFW 1 está inactivo, la sesión SSH debe mantenerse activa mediante la conmutación por error a otro CN-NGFW.

STEP 1 | Desde la CLI de Panorama, introduzca `mostrar nombre de clústeres <cluster-name>` para ver los pods CN-NGFW, CN-DB y CN-GW conectados al pod CN-MGMT.

```
Cluster: cluster-002 Creation time: 2022/11/22 04:56:46 CN-MGMT pods: 87F87FE94CBBB03
 (active, pan-mgmt-sts-0.cluster-002, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------ 1
 pan-gw-dep-5cd5c87d76-przjx CN-GW 11.0.1-c156.dev_e_rel 6 pan-db-dep-d6fb496b-jf2ms CN-DB
 11.0.1-c156.dev_e_rel 5 pan-ngfw-dep-5cd8f55848-dbhwh CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-
ngfw-dep-5cd8f55848-slk5l CN-NGFW 11.0.1-c156.dev_e_rel 7 pan-db-dep-d6fb496b-hfmlp CN-DB
 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-5cd8f55848-pq6ks CN-NGFW 11.0.1-c156.dev_e_rel 2 pan-
gw-dep-5cd5c87d76-4kbfk CN-GW 11.0.1-c156.dev_e_rel 11 pan-ngfw-dep-5cd8f55848-rsbqn CN-NGFW
 11.0.1-c156.dev_e_rel
```

STEP 2 | Vea los detalles de pertenencia del clúster del pod CN-MGMT pod `an-mgmt-sts-0` mediante el comando `show cluster-membership show-slot-info slot all`.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 11 CN-NGFW 192.168.23.87 192.168.24.93 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 7 CN-DB 192.168.23.102 :: UP UP NA 6
 CN-DB 192.168.23.104 :: UP UP NA 5 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

Todas las interfaces de la subred ethernetx/3 deben estar en la misma zona. Igualmente, todas las interfaces de la subred ethernetx/4 deben estar en la misma zona.

STEP 3 | Utilice `show session all filter application ssh` para ver todas las sesiones SSH.

Para cada sesión, hay dos flujos para las direcciones de Cliente a Servidor y de Servidor a Cliente.

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 1342177294 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 1342177294 Session 1342177294 c2s flow: source: 192.168.200.100 [untrust_ei1]
 dst: 192.168.250.100 proto: 6 sport: 48702 dport: 22 state: ACTIVE type: FLOW src user:
 unknown dst user: unknown s2c flow: source: 192.168.250.100 [trust_ei2] dst: 192.168.200.100
 proto: 6 sport: 22 dport: 48702 state: ACTIVE type: FLOW src user: unknown dst user: unknown
 Slot : 11 DP : 0 index(local): : 14 start time : Mon Nov 21 21:30:02 2022 timeout : 3600 sec
 time to live : 3542 sec total byte count(c2s) : 3887 total byte count(s2c) : 4501 layer7
 packet count(c2s) : 23 layer7 packet count(s2c) : 20 vsys : vsys1 application : ssh rule :
 allow_inside-to-outside service timeout override(index) : False session to be logged at end :
 True session in session ager : True session updated by HA peer : False layer7 processing :
 completed URL filtering enabled : True URL category : any session via syn-cookies : False
 session terminated on host : False session traverses tunnel : False session terminate tunnel :
 False captive portal session : False ingress interface : ethernet1/3 egress interface :
 ethernet1/4 session QoS rule : N/A (class 4) tracker stage l7proc : ctd decoder done end-
reason : unknown
```

El propietario de la sesión es Ranura 11.

Puede ver los detalles del flujo del clúster filtrado con el siguiente comando de ejemplo.

```
show cluster-flow all filter source-port 22
```

Resultado:

```
--------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 --------------------------------------------------------------------------------
 536870940 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
 --------------------------------------------------------------------------------
 Slot 6
 ------------------------------------------------------------------------------ Id
```



```
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 671088668 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
```

```
show cluster-flow all filter destination-port 22
```

Resultado:

```
------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 536870939 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
 ------------------------------------------------------------------------------
 Slot 6
 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 671088667 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
```

STEP 4 | Elimine el pod en la ranura 11 con el comando `kubectl -n kube-system delete pod pan-ngfw-dep-5cd8f55848-rsbqn`.

Resultado:

```
pod "pan-ngfw-dep-5cd8f55848-rsbqn" deleted
```

La sesión propiedad del pod CN-NGFW en la ranura 11 ahora está marcada como huérfana.

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s6dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id
 536870939 Flow 536870939 start time : Mon Nov 21 21:30:02 2022 timeout : 3600 sec
 source : 192.168.200.100 sport : 48702 dest : 192.168.250.100 dport : 22 proto :
 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 28 cid : 0 gft : 0 gft' : 1
 predict : 0 orphan : 1 flag_inager : 0 ager_thread : 3 flags : 0 flow-data : type:
 l7 app-id: 25 startlog: 1 endlog: 1 denied: 0 admin@pan-mgmt-sts-1.cluster-001>
 set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-
mgmt-sts-1.cluster-001> show cluster-flow id 671088667 Flow 671088667 start time :
 Mon Nov 21 21:30:02 2022 timeout : 3600 sec source : 192.168.200.100 sport : 48702
 dest : 192.168.250.100 dport : 22 proto : 6 zone : 1 type : FLOW state : ACTIVE
 ipver : 4 fidx : 28 cid : 0 gft : 1 gft' : 0 predict : 0 orphan : 1 flag_inager :
 0 ager_thread : 4 flags : 0 flow-data : type: l7 app-id: 25 startlog: 1 endlog: 1
 denied: 0
```

STEP 5 | Acceda a la sesión SSH usando el comando `show session all filter application ssh`.

El cortafuegos conmutará por error a un pod CN-NGFW disponible para gestionar el flujo huérfano. El nuevo propietario de la sesión es Ranura 7.

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 805306374 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702]) vsys1
 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001> show
 session id 805306374 Session 805306374 c2s flow: source: 192.168.200.100 [untrust_ei1] dst:
 192.168.250.100 proto: 6 sport: 48702 dport: 22 state: ACTIVE type: FLOW src user: unknown
 dst user: unknown s2c flow: source: 192.168.250.100 [trust_ei2] dst: 192.168.200.100 proto:
 6 sport: 22 dport: 48702 state: ACTIVE type: FLOW src user: unknown dst user: unknown Slot :
 7 DP : 0 index(local): : 6 start time : Mon Nov 21 21:43:27 2022 timeout : 3600 sec time
 to live : 3581 sec total byte count(c2s) : 1350 total byte count(s2c) : 1506 layer7 packet
 count(c2s) : 17 layer7 packet count(s2c) : 11 vsys : vsys1 application : ssh rule : Promoted-
```



```
session service timeout override(index) : False session to be logged at end : True session
 in session ager : True session updated by HA peer : False layer7 processing : completed URL
 filtering enabled : True URL category : any session via syn-cookies : False session terminated
 on host : False session traverses tunnel : False session terminate tunnel : False captive
 portal session : False ingress interface : ethernet1/3 egress interface : ethernet1/4 session
 QoS rule : N/A (class 4) tracker stage l7proc : fastpath state none end-reason : unknown
```

Sin cambios en el flujo del clúster.

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s5dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id
 536870939 Flow 536870939 start time : Mon Nov 21 21:30:02 2022 timeout : 3600 sec
 source : 192.168.200.100 sport : 48702 dest : 192.168.250.100 dport : 22 proto :
 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 12 cid : 7 gft : 0 gft' : 1
 predict : 0 orphan : 0 flag_inager : 0 ager_thread : 3 flags : 0 flow-data : type:
 l7 app-id: 25 startlog: 1 endlog: 1 denied: 0 admin@pan-mgmt-sts-1.cluster-001>
 set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-
mgmt-sts-1.cluster-001> show session id 805306374 Session 805306374 Bad Key: c2s:
 'c2s' Bad Key: s2c: 's2c' index(local): : 6 admin@pan-mgmt-sts-1.cluster-001> show
 cluster-flow id 671088667 Flow 671088667 start time : Mon Nov 21 21:30:02 2022
 timeout : 3600 sec source : 192.168.200.100 sport : 48702 dest : 192.168.250.100
 dport : 22 proto : 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 12 cid :
 7 gft : 1 gft' : 0 predict : 0 orphan : 0 flag_inager : 0 ager_thread : 4 flags : 0
 flow-data : type: l7 app-id: 25 startlog: 1 endlog: 1 denied: 0
```

Resultados:

Sin efecto en las sesiones existentes o nuevas. Pertenencia del clúster actualizada en Panorama.

Caso de prueba: Gestión de los fallos de CN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de cortafuegos CN-Series HSF	• CN-Series 11.0.x or above Container Images • Panorama con PAN-OS 11.0.x o versiones superiores

Esta prueba evalúa la gestión de los fallos de CN-DB. El número preferido de pods CN-DB para una implementación CN-series HSF es dos. Ambos CN-DB tienen la misma configuración.

Cuando CN-DB 1 no está activo durante un período prolongado, CN-DB 2 se encarga de las sesiones existentes y configura nuevas sesiones. Cuando CN-DB 1 vuelve a estar ACTIVO, este comprueba la sincronización, la búsqueda y el desmontaje de las sesiones existentes y configura nuevas sesiones.

STEP 1 | Vea los detalles de pertenencia del clúster del pod CN-MGMT con el comando `show cluster-membership show-slot-info slot all`.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6
 CN-DB 192.168.23.104 :: UP UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```


STEP 2 | Elimine el pod CN-DB en la ranura 6.

1. Obtenga el nombre del pod de CN-DB en la ranura 6 mediante el comando `show clusters name cluster-001` de la CLI de Panorama.

```
Cluster: cluster-001 Creation time: 2022/11/22 05:11:09 CN-MGMT pods: 8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------ 5 pan-
db-dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-
c156.dev_e_rel 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-
srmdt CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-
ngfw-dep-56cdfdd656-bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-
c156.dev_e_rel 6 pan-db-dep-7b6f6c5458-4tvpq CN-DB 11.0.1-c156.dev_e_rel
```

2. Desde la CLI del controlador, introduzca el comando `kubectl delete pod pan-db-dep-7b6f6c5458-4tvpq -n kube-system` para eliminar el pod CN-DB en la ranura 6.

   El pod CN-DB en la ranura 6 ahora se ha eliminado.

```
admin@pan-mgmt-sts-1.cluster-001> show cluster-membership show-slot-info slot
 all MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 7 CN-NGFW 192.168.23.103
 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82
 192.168.24.81 UP UP UP
```

3. Verifique el flujo de tráfico del clúster con el comando `show cluster-flow all`.

```
Slot 5 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156]
 536870958 ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954
 ACTIVE FLOW 192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE
 FLOW 192.168.100.100[3784]/17 192.168.100.6[49153] 536870952 ACTIVE
 FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 536870951 ACTIVE FLOW
 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960 OPENING FLOW
 fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 536870957 ACTIVE FLOW
 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW 192.168.250.100[22]/6
 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
 192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
 ------------------------------------------------------------------------------ Slot
 6 ------------------------------------------------------------------------------ No
 Active Flows
```

   La ranura 6 con el pod CN-DB ahora está en estado PREPARAR y el enlace CI no está activo.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-GW
 192.168.23.100 192.168.24.80 UP IMPACTED UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP IMPACTED UP 2
 CN-GW 192.168.23.101 192.168.24.100 UP IMPACTED UP 5 CN-DB 192.168.23.102 :: UP IMPACTED NA 6 CN-DB
 192.168.23.104 :: PREPARE DOWN NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP IMPACTED UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP IMPACTED UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP IMPACTED UP
```

STEP 3 | Introduzca `show cluster-membership show-slot-info slot all` hasta que el pod CN-DB vuelva a estar activo.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP
 UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-
DB 192.168.23.104 :: PROBE UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

STEP 4 | Vuelva a verificar el flujo de tráfico del clúster con el comando `show cluster-flow all`.

```
------------------------------------------------------------------------------ Slot 5
 ------------------------------------------------------------------------------ Id State Type
 Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
```



```
536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 536870958
ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954 ACTIVE FLOW
192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE FLOW 192.168.100.100[3784]/17
192.168.100.6[49153] 536870952 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784]
536870951 ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960
OPENING FLOW fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 536870957
ACTIVE FLOW 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW
192.168.250.100[22]/6 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
-------------------------------------------------------------------------------- Slot 6
-------------------------------------------------------------------------------- Id State Type
Src[Sport]/Proto Dst[Dport]
--------------------------------------------------------------------------------
671088642 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 671088641 ACTIVE FLOW
192.168.200.100[48706]/6 192.168.250.100[22] 671088643 ACTIVE FLOW 192.168.100.6[49153]/17
192.168.100.100[3784] 671088645 ACTIVE FLOW 192.168.100.100[3784]/17 192.168.100.6[49153]
671088644 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 671088646
ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 671088647 ACTIVE FLOW
fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 671088648 ACTIVE FLOW
192.168.101.101[3784]/17 192.168.101.6[49155] 671088649 ACTIVE FLOW 192.168.250.100[22]/6
192.168.200.100[48706] 671088650 ACTIVE FLOW 192.168.100.6[49154]/17 192.168.100.101[3784]
671088651 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
```

- `show cluster-flow all filter count yes`

```
-------------------------------------------------------------------------------- Slot 5
 -------------------------------------------------------------------------------- Number of
 sessions that match filter: 11
 -------------------------------------------------------------------------------- Slot 6
 -------------------------------------------------------------------------------- Number of
 sessions that match filter: 11
```

- `show cluster-membership show-slot-info slot all`

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-DB 192.168.23.104 :: UP UP
 NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-
NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

- Desde el CLI de Panorama

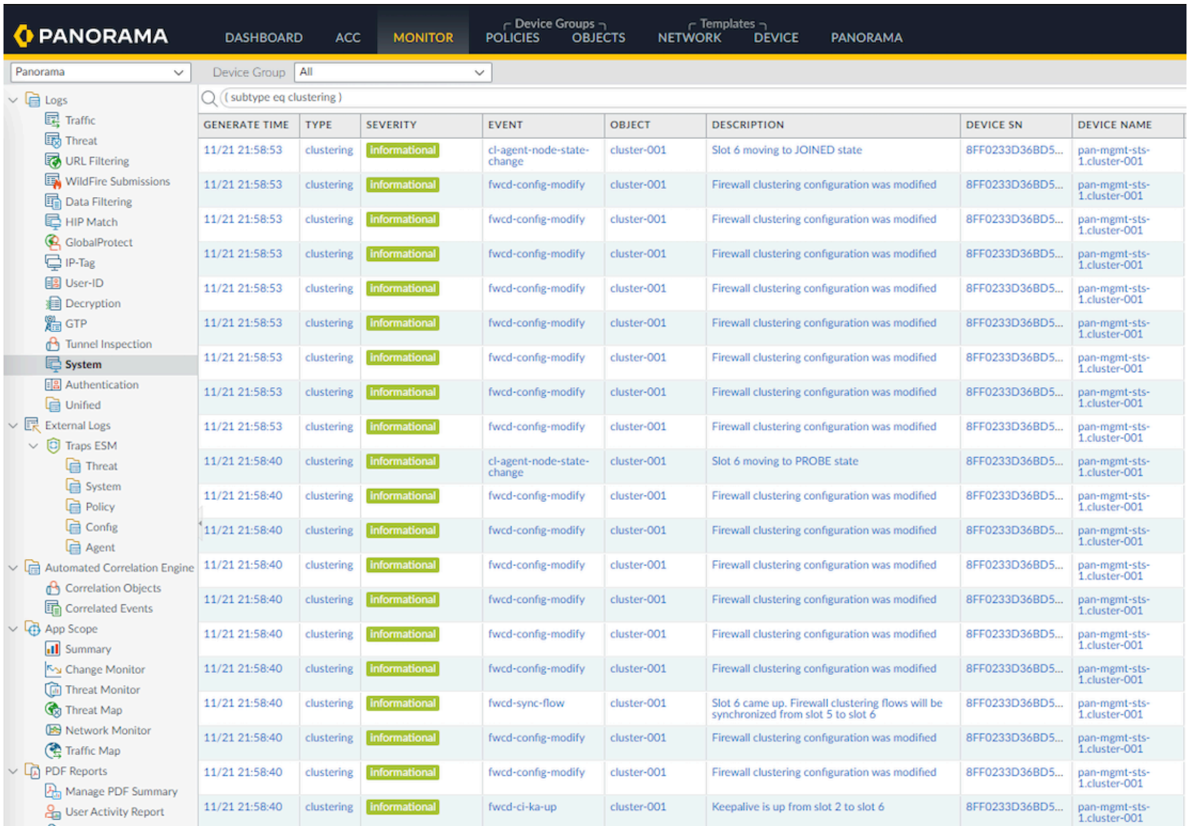
```
show clusters name cluster-001
```

```
Cluster: cluster-001 Creation time: 2022/11/22 05:11:09 CN-MGMT pods: 8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 -------------------------------------------------------------------------------- 5 pan-db-
dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-c156.dev_e_rel
 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-srmdt CN-NGFW 11.0.1-
c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-56cdfdd656-
```



```
bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-c156.dev_e_rel 6 pan-db-dep-7b6f6c5458-r449b CN-DB 11.0.1-c156.dev_e_rel
```

Puede ver los cambios de CN-DB en la interfaz web de Panorama en **Monitor (Supervisar)** > **Logs** > **System (Sistema)**



GENERATE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION	DEVICE SN	DEVICE NAME
11/21 21:58:53	clustering	informational	cl-agent-node-state-change	cluster-001	Slot 6 moving to JOINED state	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	cl-agent-node-state-change	cluster-001	Slot 6 moving to PROBE state	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-sync-flow	cluster-001	Slot 6 came up. Firewall clustering flows will be synchronized from slot 5 to slot 6	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001
11/21 21:58:40	clustering	informational	fwcd-ci-ka-up	cluster-001	Keepalive is up from slot 2 to slot 6	8FF0233D36BD5...	pan-mgmt-sts-1.cluster-001

Resultados:

Sin efecto en las sesiones existentes o nuevas. Pertenencia del clúster actualizada en Panorama.

Funciones no compatibles con el modelo CN-Series

Las siguientes capacidades compatibles con PAN-OS no están disponibles para la CN-Series a menos que se indique lo contrario a continuación:

Función	DaemonSet	Servicio K8s	Modo CNF	Modo HSF
Autenticación	No	No	No	No
Envío de logs a Cortex Data Lake	No	No	No	No
DLP empresarial	No	No	No	No
Interfaces que no son de vWire	No	No	**Sí**	**Sí**
IoT Security (Seguridad de IoT)	No	No	No	No
IPv6	**Sí**	No	**Sí**	No
NAT	No	No	**Sí**	No
Reenvío basado en políticas	No	No	**Sí**	No
QoS	No	No	No	No
SD-WAN	No	No	No	No
User-ID	No	No	No	No
WildFire Inline ML	No	No	No	No
SaaS en línea	No	No	No	No
IPSec	No	No	No	No
Inspección del contenido del túnel	No	No	No	No

