paloalto TECHDOCS

Implemente el cortafuegos CN-Series en la nube y en las instalaciones

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

Implementación de los cortafuegos CN-Series en GKE.

¿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 versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Después de revisar los Componentes básicos de la serie CN-Series y la descripción general de alto nivel del flujo de trabajo en Protección de los entornos de Kubernetes con CN-Series, puede comenzar a implementar el cortafuegos CN-Series en la plataforma GKE para proteger el tráfico entre contenedores dentro del mismo clúster, así como entre contenedores y otros tipos de cargas de trabajo, como máquinas virtuales y servidores bare-metal.

Necesita herramientas estándar de Kubernetes, como kubectl o Helm, para implementar y gestionar sus clústeres, aplicaciones y servicios de cortafuegos de Kubernetes.

Para obtener más información, consulte Implementación de cortafuegos CN-Series con gráficos y plantillas de Helm.*. Panorama no está diseñado para ser un orquestador para la implementación y gestión de clústeres de Kubernetes. Los proveedores gestionados de Kubernetes proporcionan las plantillas para la gestión de clústeres. Palo Alto Networks proporciona plantillas compatibles con la comunidad para implementar CN-Series con* Helm *y* Terraform.

- Implementación del cortafuegos CN-Series como servicio de Kubernetes en GKE
- Implementación del cortafuegos CN-Series como un DaemonSet en GKE

Antes de pasar de implementar CN-Series como un DaemonSet a CN-Series como servicio o viceversa, debe eliminar y volver a aplicar `plugin-serviceaccount.yaml`*. Para obtener más información, consulte* Crear cuentas de servicio para la autenticación de clúster*.*

- *Cuando implementa el CN-Series como un DaemonSet en GKE,* `pan-plugin-cluster-mode-secret` *no debe existir.*
- *Cuando implementa el CN-Series como un servicio de Kubernetes GKE,* `pan-plugin-cluster-mode-secret` *debe estar presente.*

Implementación del cortafuegos CN-Series como servicio de Kubernetes en GKE

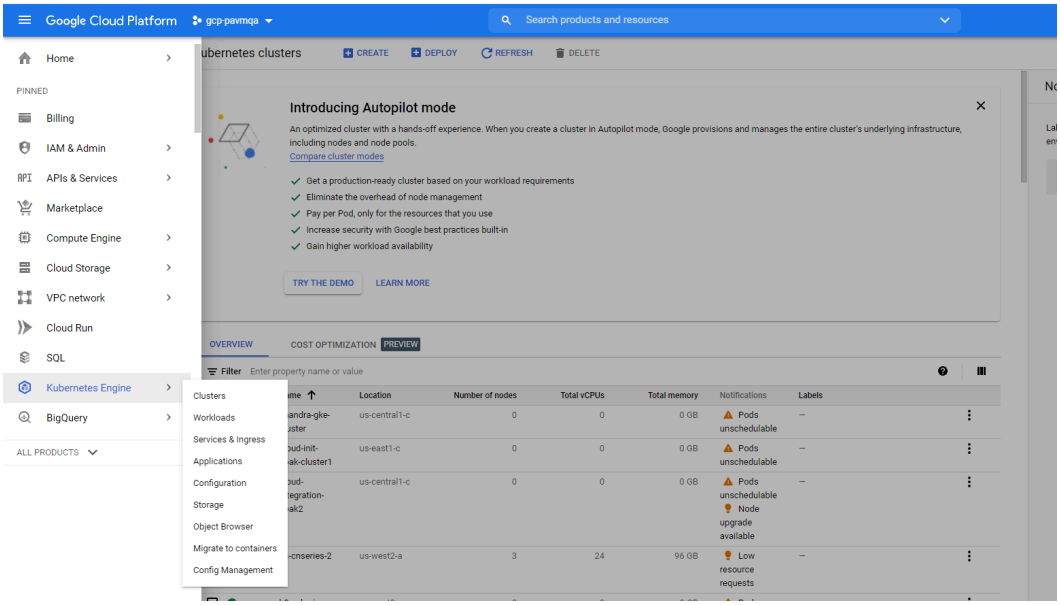
¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series Implementación	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como un servicio de Kubernetes en la plataforma GKE.

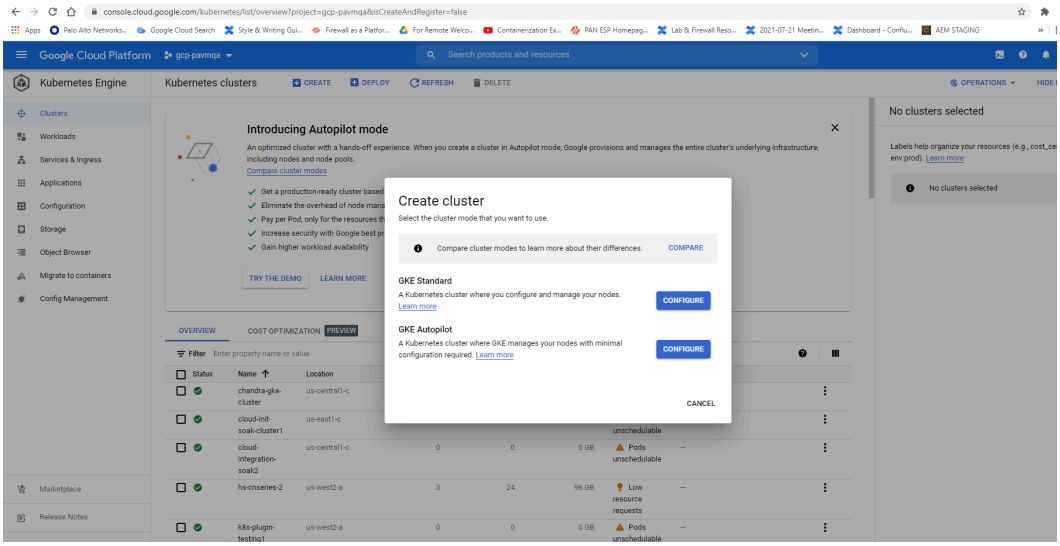
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en GKE, haga lo siguiente:

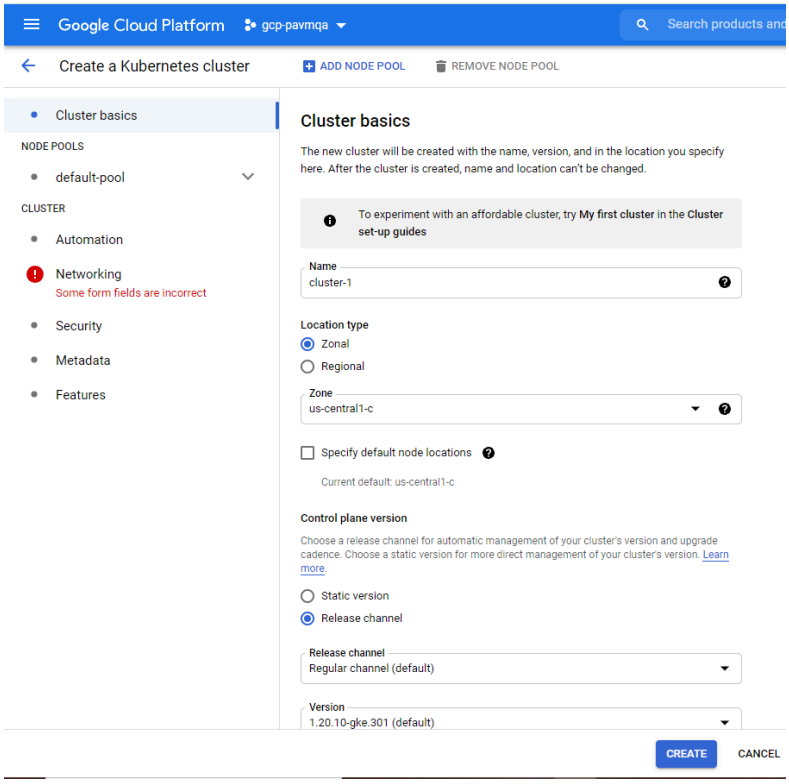
1. Haga clic en el menú de navegación, vaya a **Kubernetes Engine**, y, a continuación, seleccione **clústeres**.



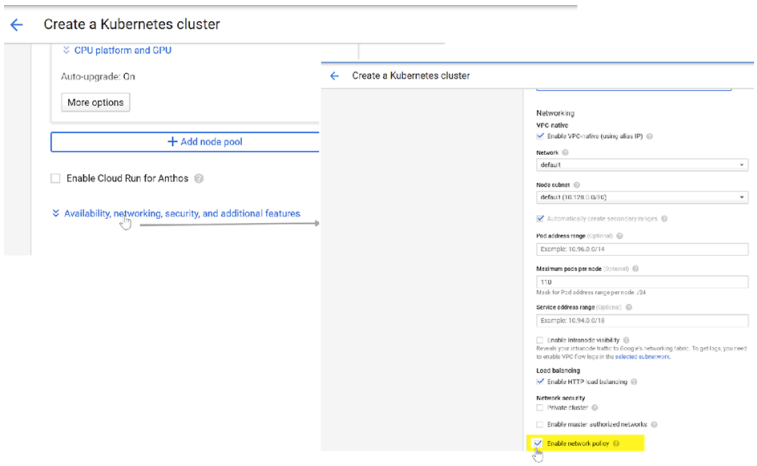
2. Haga clic en **Create (Crear)**.
3. Seleccione **GKE Standard** como el modo de clúster que desea usar y, a continuación, haga clic en **Configure (Configurar)**.



4. Escriba la información básica del clúster, incluidos Nombre, Versión, Ubicación, Subred de nodo y, a continuación, haga clic en **Create (Crear)**.



Si su clúster está en GKE, asegúrate de habilitar la API de política de red de Kubernetes para permitir que el administrador del clúster especifique qué pods pueden comunicarse entre sí. Esta API es necesaria para que los pods CN-NGFW y CN-MGMT se comuniquen.



1. Verifique que el clúster tenga los recursos adecuados. La especificación predeterminada del grupo de nodos de GKE no es adecuada para el cortafuegos CN-Series. Debe asegurarse de que

ese clúster tenga los recursos de Requisitos previos del modelo CN-Series compatibles con el cortafuegos.

```
kubectl get nodes
```

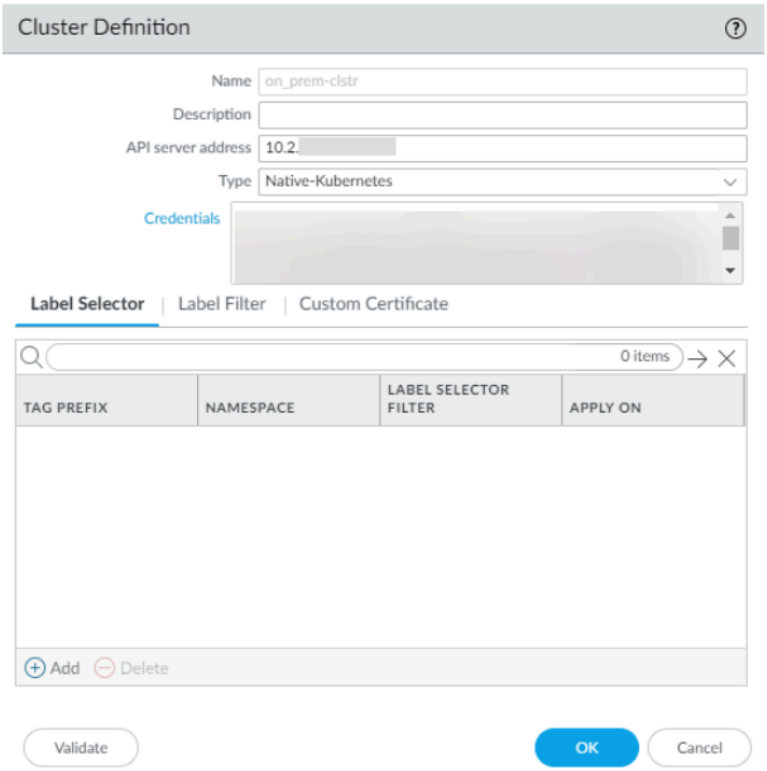
```
kubectl describe node <node-name>
```

Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series

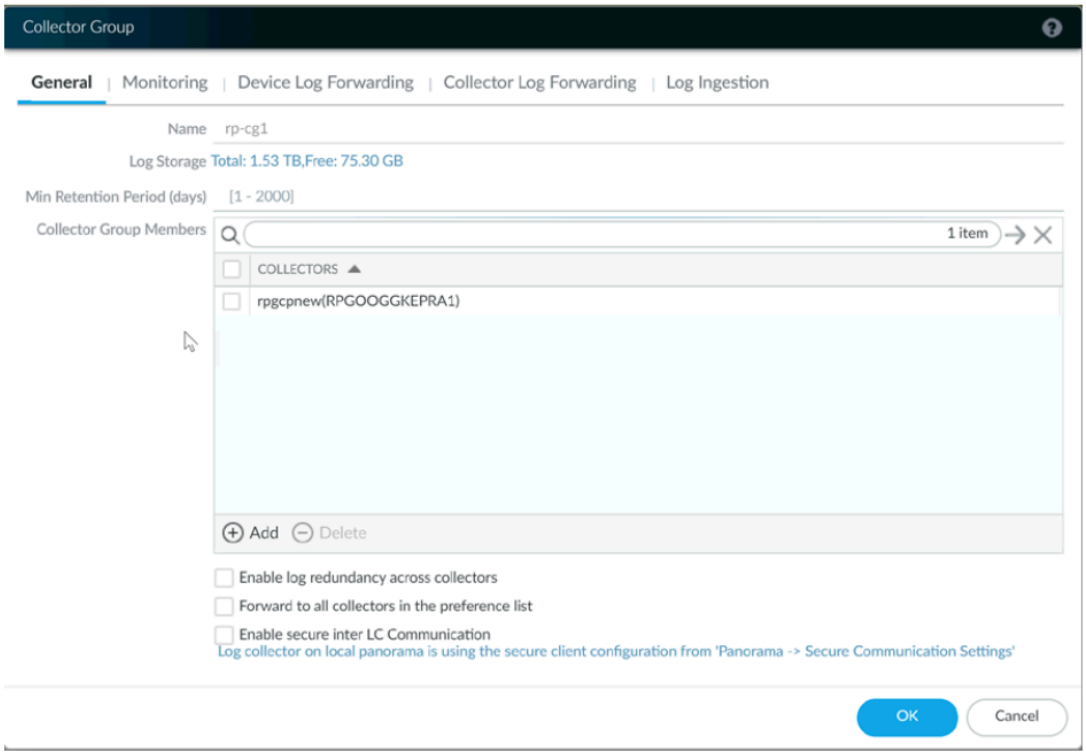
Asegúrese de tener la siguiente información:

- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



  Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

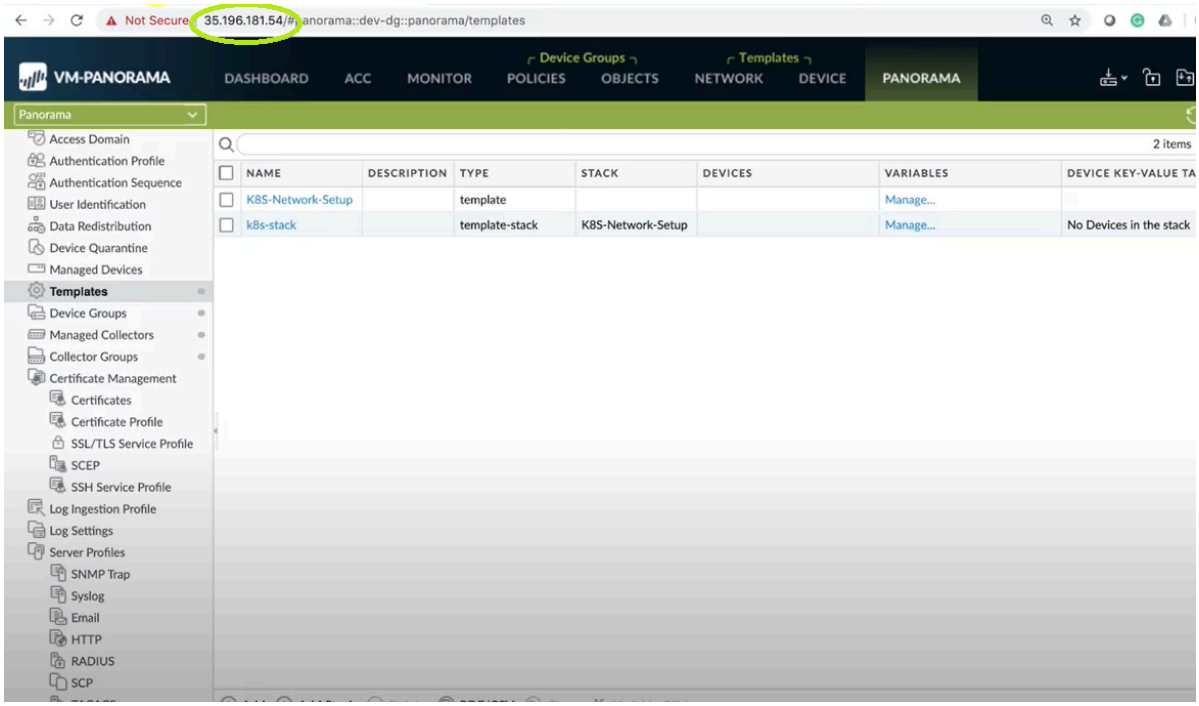
STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

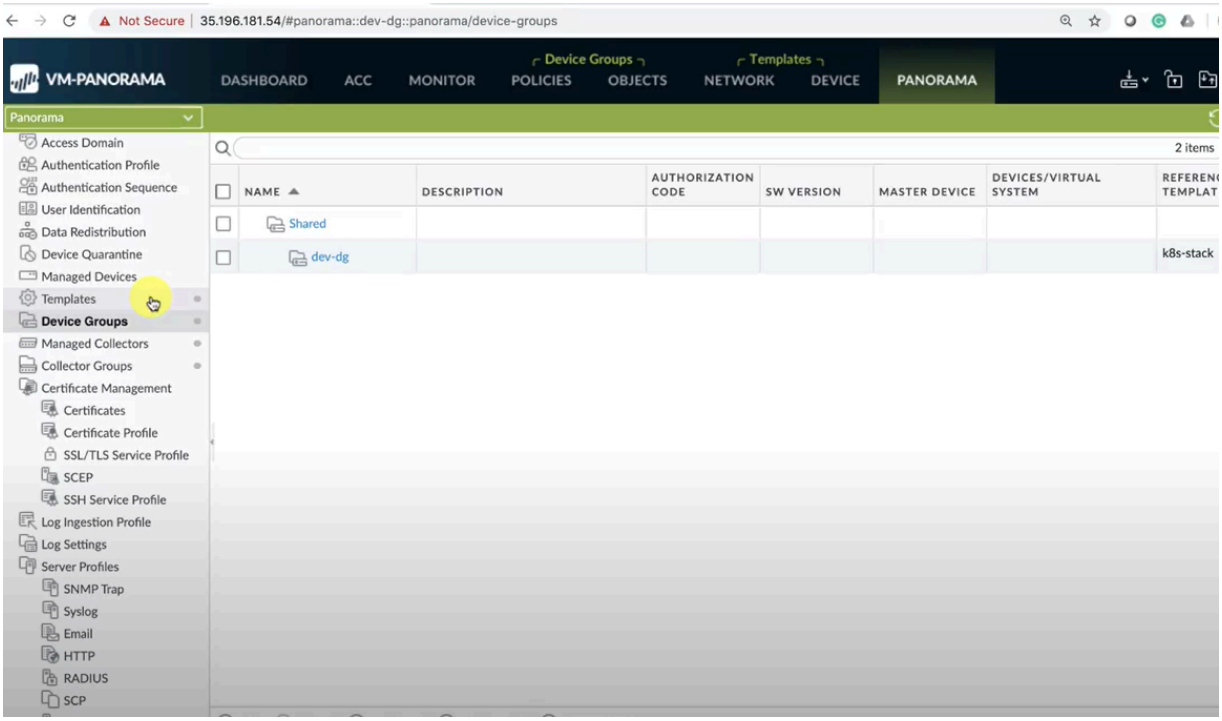

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-mgmt-config
  namespace: kube-system
data:
  PAN_OPERATION_MODE: "daemonset"
  PAN_SERVICE_NAME: "pan-mgmt"
  # Panorama settings
  PAN_PANORAMA_IP: "35.196.181.54"
  PAN_PANORAMA_AUTH_KEY: [redacted]
  PAN_DEVICE_GROUP: "dev-dg"
  PAN_TEMPLATE: "k8s-stack"
#Non-mandatory parameters
  PAN_PANORAMA_CGNAME: "rp-cg1"
  #PAN_CERTIFICATE: ""
  #PAN_CERTKEYFILE: ""
  #PAN_CERTPASSPHRASE: ""
```

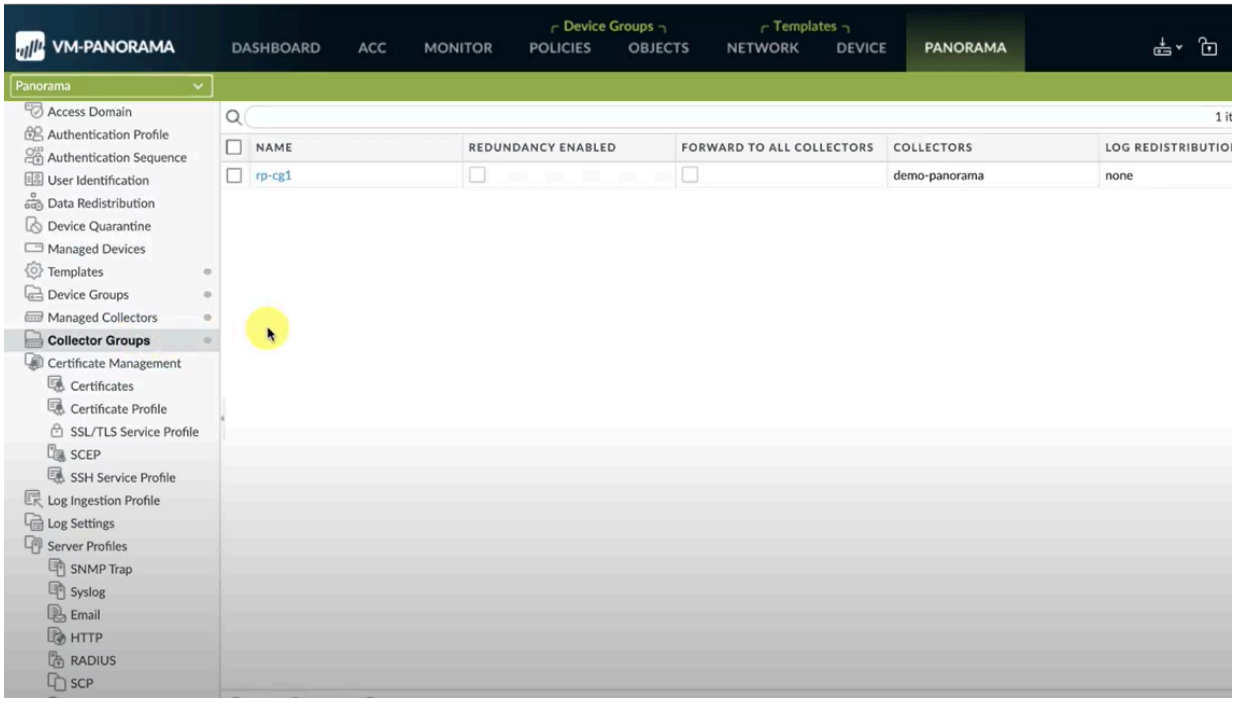
Debe asegurarse de que el valor del parámetro `PAN_PANORAMA_IP` en su archivo YAML coincida con su dirección IP de Panorama real, como se muestra en el siguiente diagrama:



Debe asegurarse de que el valor del parámetro de `PAN_DEVICE_GROUP` y `PAN_TEMPLATE` en su archivo YAML coincida con el nombre del grupo de dispositivos y la pila de plantillas que creó en Panorama, como se muestra en el siguiente diagrama:



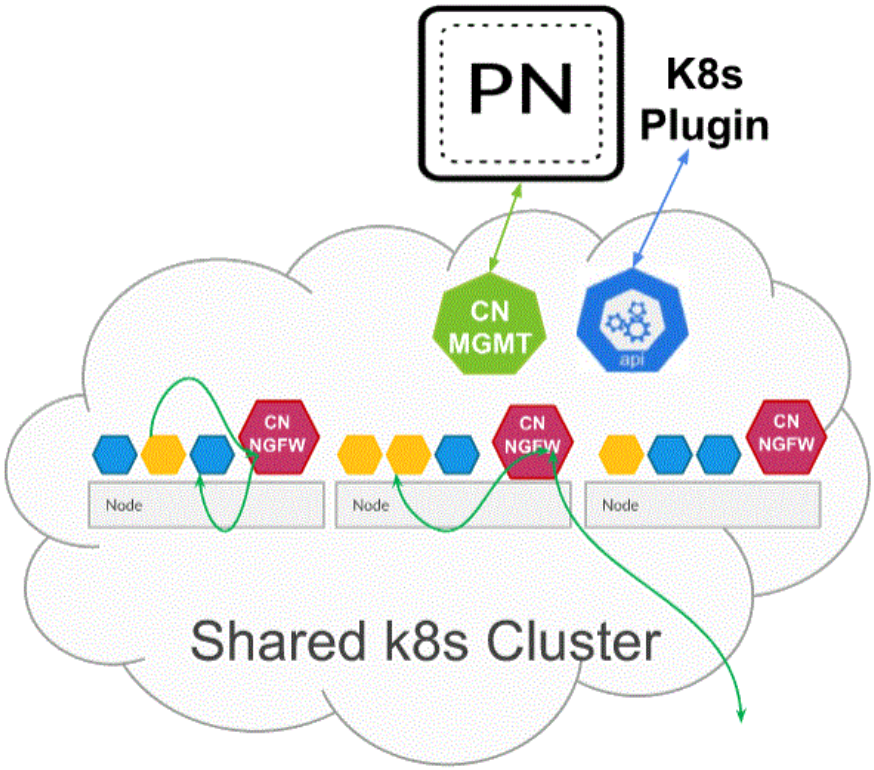
Debe asegurarse de que el valor del parámetro de `PAN_PANORAMA_CG_NAME` sea el mismo que el nombre del colector de logs que creó.



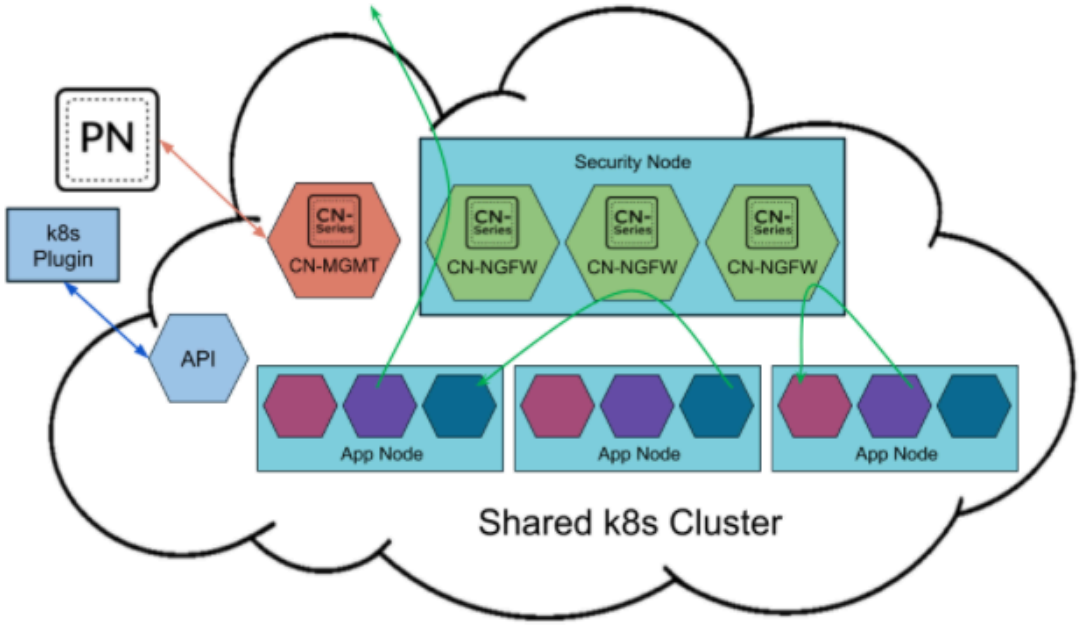
Para obtener más información, consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Si usa el ajuste de escalado automático en su entorno de Kubernetes, consulte Habilitar escalado de pod horizontal.

STEP 5 | Implemente el servicio CN-NGFW. Realice los siguientes pasos:



Cuando se implementa como un servicio de Kubernetes, las instancias de CN-NGFW se pueden implementar en nodos de seguridad y el tráfico de pods de aplicaciones se redirige a una instancia CN-NGFW disponible para su inspección y aplicación.



1. Verifique que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

   Consulte Creación de cuentas de servicio para la autenticación de clúster.
2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.


```
kubectl apply -f pan-cni-configmap.yaml
```

3. Utilice kubectl para ejecutar pan-cn-ngfw-svc.yaml.

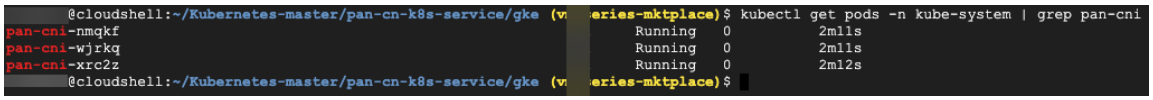
```
kubectl apply -f pan-cn-ngfw-svc.yaml
```

Este yaml debe implementarse antes de pan-cni.yaml.

4. Utilice Kubectl para ejecutar pan-cni.yaml.

```
kubectl apply -f pan-cni.yaml
```

5. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
6. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.



STEP 6 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. (Requerido solo para los volúmenes persistentes aprovisionados estáticamente) Implemente los volúmenes persistentes (PV) para el StatefulSet de CN-MGMT.

   1. Cree los directorios para que coincidan con los nombres de los volúmenes locales definidos en pan-cn-pv-local.yaml.

   Necesita seis (6) directorios en al menos 2 nodos de trabajo. Inicie sesión en cada nodo de trabajo en el que se implementará el StatefulSet de CN-MGMT para crear los directorios. Por ejemplo, para crear directorios llamados / mnt / pan-local1 a / mnt / pan-local6, use el comando:

   ```
   mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
   mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
   ```

   2. Modifique pan-cn-pv-local.yaml.

   Haga coincidir el nombre de host en `nodeaffinity` y verifique que haya modificado los directorios que creó anteriormente en `spec.local.path`, luego implemente el archivo para crear una nueva clase de almacenamiento pan-local-storage y volúmenes persistentes locales.

2. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

   Ejemplo de pan-cn-mgmt-configmap de EKS.

   ```
   apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-
   config namespace: kube-system data: PAN_SERVICE_NAME:
   pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama
   settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:
   ```



```
 "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-
template-stack>" PAN_CGNAME: "<panorama-collector-
group>" # ctnr mode: "k8s-service", "k8s-ilbservice"
 PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters #
 Recommended to have same name as the cluster name provided in
 Panorama Kubernetes plugin - helps with easier identification
 of pods if managing multiple clusters with same Panorama
 #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" #
 Comment out to use CERTs otherwise PSK for IPSec between pan-
mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed
 # Override auto-detect of jumbo-frame mode and force enable
 system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT
 pod with GTP enabled. For complete functionality, need GTP #
 enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable
 high feature capacities. These need high memory for MGMT pod
 and # higher/matching memory than specified below for NGFW
 pod. #PAN_NGFW_MEMORY="6Gi" #PAN_NGFW_MEMORY="40Gi" # For
 enabling faster datapath - AF_XDP, default is AF_PACKETV2.
 This requires kernel support. #PAN_DATA_MODE: "next-gen" #HPA
 params #PAN_CLOUD: "EKS" #PAN_NAMESPACE_EKS: "EKSNamespace"
 #PUSH_INTERVAL: "15" #time interval to publish metrics to AWS
 cloudwatch
```

Ejemplo de pan-cn-mgmt.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

```
 containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

3. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-slot-crd.yaml

   kubectl apply -f pan-cn-mgmt-slot-cr.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente Crear cuenta de servicio para la autenticación de clúster.

4. Verifique que los pods CN-MGMT estén activos ejecutando el siguiente comando:

   kubectl get pods -l app=pan-mgmt -n kube-system

   Tarda unos 5 y 6 minutos.

STEP 7 | Implemente los pods CN-NGFW.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que los pods CN-NGFW se están ejecutando.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 8 | Habilite el ajuste de escalado automático de pod horizontal realizando los siguientes pasos:

1. Implemente el Adaptador de controlador de pila de métricas personalizadas en el clúster CN-Series. El nombre del clúster debe proporcionarse a través de un secreto K8s.
2. Descargue los archivos yaml de HPA específicos de GKE del Repositorio de GitHub de Palo Alto Networks.
3. Si su CN-MGMT se implementa en un espacio de nombres personalizado, actualice pan-cn-adapater.yaml con el espacio de nombres personalizado. El espacio de nombres predeterminado es **kube-system**.
4. Actualice los parámetros de HPA en el archivo pan-cn-mgmt-configmap.yaml específico de GKE.

   ```
   #PAN_CLOUD: "GKE"
   ```

   ```
   #HPA_NAME: "<name>" #unique name to identify hpa resource per
    namespace or per tenant
   ```

   ```
   #PUSH_INTERVAL: "15" #time interval to publish metrics to
    stackdriver
   ```

5. Modifique **`pan-cn-hpa-dp.yaml`** y **`pan-cn-hpa-mp.yaml`** con HPA_NAME (sustituya con el nombre) como se actualizó en el archivo pan-cn-mgmt-configmap.yaml anterior y actualice la métrica según qué HPA se debe activar.
   1. Introduzca el número mínimo y máximo de réplicas.
   2. (Opcional) Cambie los valores de frecuencia de ampliación o reducción para adaptarlos a su implementación. Si no cambia estos valores, se utilizan los valores predeterminados.
   3. (Opcional) Cambie el valor de umbral para cada métrica que desee utilizar para el escalado. Si no cambia estos valores, se utilizan los valores predeterminados.
   4. Seleccione Guardar los cambios.
6. Implemente los archivos yaml de HPA. Los archivos deben implementarse en el orden que se describe a continuación.
   1. Utilice Kubectl para ejecutar pan-cn-adapter.yaml

      ```
      kubectl apply -f pan-cn-adapter.yaml
      ```

   2. Utilice Kubectl para ejecutar pan-cn-crole.yaml

      ```
      kubectl apply -f pan-cn-crole.yaml
      ```

   3. Utilice Kubectl para ejecutar pan-cn-hpa-dp.yaml

      ```
      kubectl apply -f pan-cn-hpa-dp.yaml
      ```

   4. Utilice Kubectl para ejecutar pan-cn-hpa-mp.yaml

      ```
      kubectl apply -f pan-cn-hpa-mp.yaml
      ```

7. Compruebe la implementación.
   - Utilice kubectl para comprobar el pod del adaptador de métricas personalizadas en el espacio de nombres de métricas personalizadas.

     ```
     kubectl get pods -n custom-metrics
     ```


- Utilice kubectl para comprobar el recurso HPA.

  ```
  kubectl get hpa -n kube-system
  ```

  ```
  kubectl describe hpa <hpa-name> -n kube-system
  ```

Para obtener más información, consulte Habilitar el escalado automático de pod horizontal en la CN-Series.

STEP 9 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

```
kubectl -n kube-system get pods
```

STEP 10 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 11 | Implemente su aplicación en el clúster.

Implementación del cortafuegos CN-Series como un DaemonSet en GKE

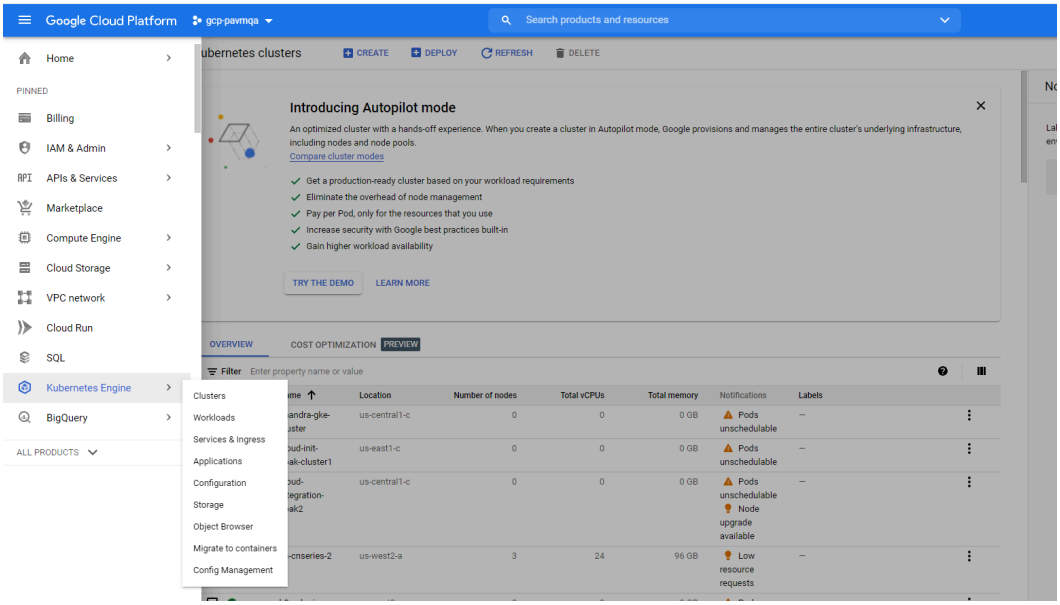
¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series Implementación	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como Daemonset en la plataforma GKE.

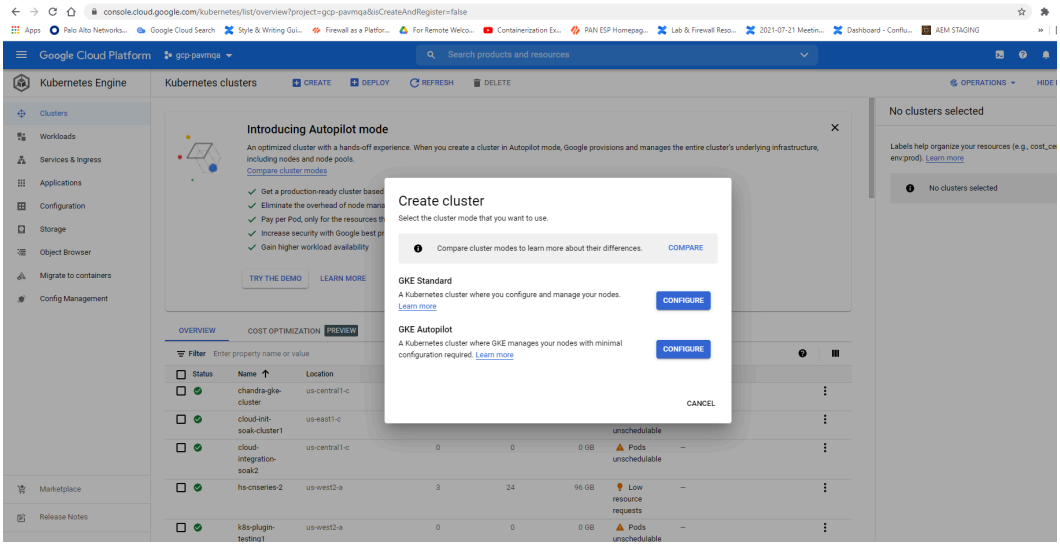
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en GKE, haga lo siguiente:

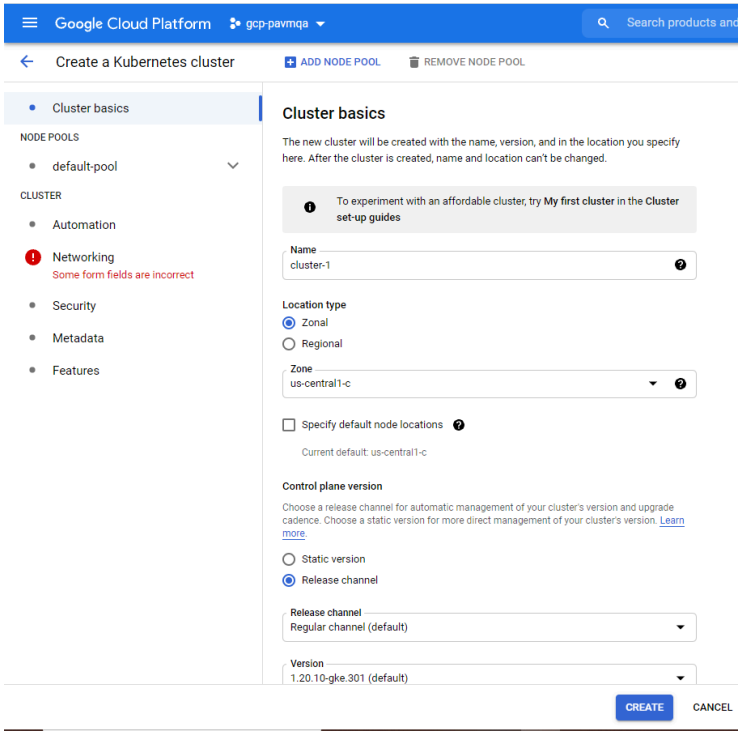
1. Haga clic en el menú de navegación, vaya a **Kubernetes Engine**, y, a continuación, seleccione **clústeres**.



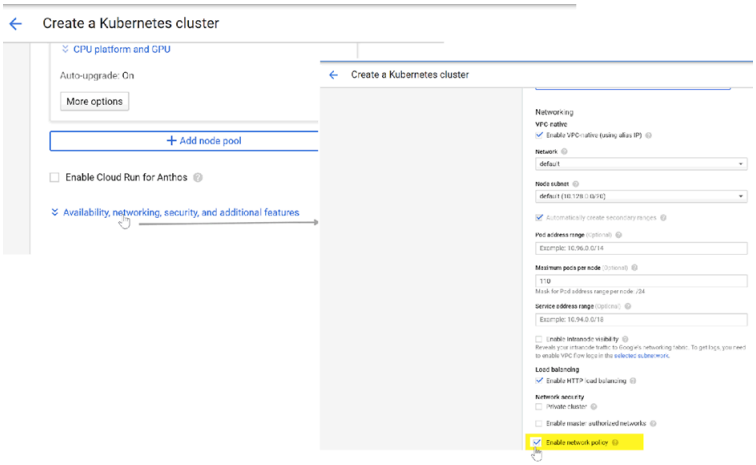
2. Haga clic en **Create (Crear)**.
3. Seleccione **GKE Standard** como el modo de clúster que desea usar y, a continuación, haga clic en **Configure (Configurar)**.



4. Escriba la información básica del clúster, incluidos Nombre, Versión, Ubicación, Subred de nodo y, a continuación, haga clic en **Create (Crear)**.



Si su clúster está en GKE, asegúrate de habilitar la API de política de red de Kubernetes para permitir que el administrador del clúster especifique qué pods pueden comunicarse entre sí. Esta API es necesaria para que los pods CN-NGFW y CN-MGMT se comuniquen.



Verifique que el clúster tenga los recursos adecuados. Asegúrese de que ese clúster tenga los requisitos del sistema CN-Series para admitir el cortafuegos.

```
kubectl get nodes
```

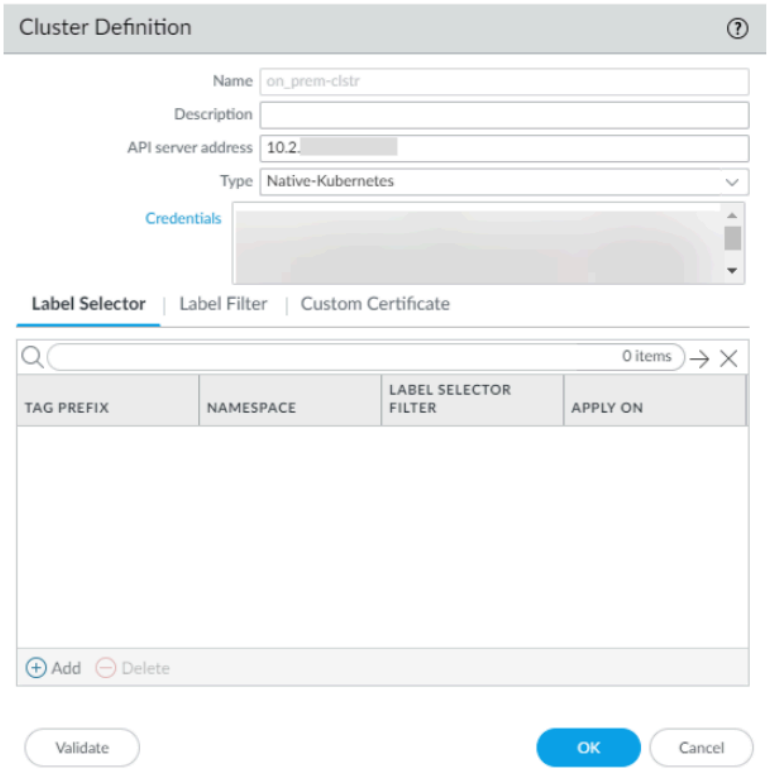
```
kubectl describe node <node-name>
```

Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series.

Asegúrese de tener la siguiente información:

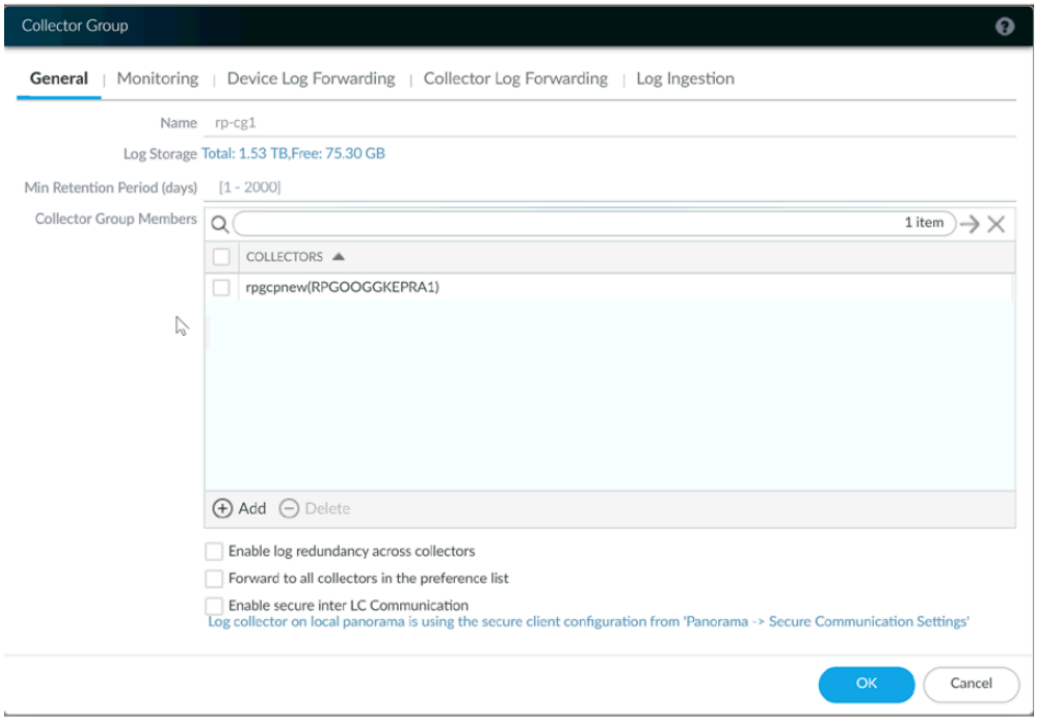
- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



  Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

  Para obtener más información, consulte Configurar el complemento de Kubernetes para supervisar los clústeres.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

Debe sustituir la ruta de la imagen en los archivos YAML para incluir la ruta a su registro privado de contenedor de Google y proporcionar los parámetros requeridos. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Implementación de CNI DaemonSet.

El contenedor CNI se implementa como un DaemonSet (un pod por nodo) y crea dos interfaces en el pod CN-NGFW para cada aplicación implementada en el nodo. Cuando utilice los comandos kubectl para ejecutar los archivos pan-cni YAML, se convierte en parte de la cadena de servicios en cada nodo.

1. El cortafuegos CN-Series requiere tres cuentas de servicio con los permisos mínimos que le autorizan a comunicarse con los recursos del clúster de Kubernetes. Deberá Crear una cuenta de

servicio para la autenticación de clúster CN-Series y verificar que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

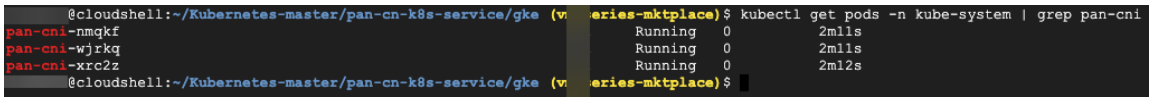
2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   ```
   kubectl apply -f pan-cni-configmap.yaml
   ```

3. Utilice Kubectl para ejecutar pan-cni.yaml.

   ```
   kubectl apply -f pan-cni.yaml
   ```

4. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
5. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.



STEP 5 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

Ejemplo pan-cn-mgmt-configmap

```
name: pan-mgmt-config
```

```
metadata:
```

```
espacio de nombre: kube-system
```

```
data:
```

```
PAN_SERVICE_NAME: pan-mgmt-svc
```

```
PAN_MGMT_SECRET: pan-mgmt-secret
```

```
# Panorama settings
```

```
PAN_PANORAMA_IP: "x.y.z.a"
```

```
PAN_DEVICE_GROUP: "dg-1"
```

```
PAN_TEMPLATE_STACK: "temp-stack-1"
```

```
PAN_CGNAME: "CG-GKE"
```

```
Parámetros no obligatorios
```

```
#Recommended to have same name as the cluster name provided in
 Panorama Kubernetes plugin - helps with easier identification
 of pods if managing multiple clusters with same Panorama
```

```
#CLUSTER_NAME: "<Cluster name>"
```

```
#PAN_PANORAMA_IP2: ""
```

```
#Comment usar CERT, de lo contrario, PSK para IPSec entre pan-
mgmt y pan-ngfw
```

```
#IPSEC_CERT_BYPASS: ""
```

```
#No requiere valores
```

```
#Override auto-detect of jumbo-frame mode and force enable
 system-wide#PAN_JUMBO_FRAME_ENABLED: "true"
```

```
#Start MGMT pod with GTP enabled. For complete functionality,
 need GTP enable at Panorama as well.
```

```
#PAN_GTP_ENABLED: "true"
```

```
#Enable high feature capacities. Estos necesitan una memoria
```


Ejemplo de pan-cn-mgmt.yaml

```
initContainers:
```

```
 - nombre: pan-mgmt-init
```

```
image: <your-private-registry-image-path>
```

```
containers: - name: pan-mgmt
```

```
image: <your-private-registry-image-path>
```

```
terminationMessagePolicy: FallbackToLogsOnError
```

2. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente la Creación de cuentas de servicio para la autenticación de clúster.

3. Verifique que los pods CN-MGMT estén activos.

   Tarda unos 5 y 6 minutos.

   Utilice **kubectl get pods -l app=pan-mgmt -n kube-system**

   ```
   NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1
   ```

   ```
   Ejecutando 0 27hpan-mgmt-sts-1 1/1 Ejecutando 0 27h
   ```

STEP 6 | Implemente los pods CN-NGFW.

De forma predeterminada, el pod CN-NGFW del plano de datos del cortafuegos se implementa como un DaemonSet. Una instancia del pod CN-NFGW puede proteger el tráfico de hasta 30 pods de aplicaciones en un nodo.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que todos los pods CN-NGFW se están ejecutando. (uno por nodo en su clúster)

   Este es un resultado de muestra de un clúster local de 4 nodos.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

   ```
   NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

   pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>

   pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>

   pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>

   pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
   ```

STEP 7 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 En ejecución
0 27hpan-cni-9j4rs 1/1 En ejecución
0 27hpan-cni-ddwb4 1/1 En ejecución
0 27hpan-cni-fwfrk 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-j62rk 1/1 En ejecución
0 27hpan-cni-lmxdz 1/1 En ejecución
0 27hpan-mgmt-sts-0 1/1 En ejecución
0 27hpan-mgmt-sts-1 1/1 En ejecución
0 27hpan-ngfw-ds-8g5xb 1/1 En ejecución
27hpan-ngfw-ds-qsrm6 1/1 En ejecución
0 27hpan-ngfw-ds-vqk7z 1/1 En ejecución
0 27hpan-ngfw-ds-zncqg 1/1 En ejecución
```

STEP 8 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 9 | Implemente su aplicación en el clúster.

Implementación de los cortafuegos CN-Series en OKE.

¿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 versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Oracle Kubernetes Engine (OKE) es un servicio de OCI que le permite implementar un clúster de kubernetes. Ahora puede implementar el cortafuegos CN-Series en el clúster de OKE como un daemonset o como un kubernetes como servicio.

Después de revisar los Componentes básicos de la serie CN-Series y la descripción general de alto nivel del flujo de trabajo en Protección de los entornos de Kubernetes con CN-Series, puede comenzar a implementar el cortafuegos CN-Series en la plataforma OKE para proteger el tráfico entre contenedores dentro del mismo clúster, así como entre contenedores y otros tipos de cargas de trabajo, como máquinas virtuales y servidores bare-metal.

Necesita herramientas estándar de Kubernetes, como kubectl o Helm, para implementar y gestionar sus clústeres, aplicaciones y servicios de cortafuegos de Kubernetes.

Para obtener más información, consulte Implementación de cortafuegos CN-Series con gráficos y plantillas de Helm.*. Panorama no está diseñado para ser un orquestador para la implementación y gestión de clústeres de Kubernetes. Los proveedores gestionados de Kubernetes proporcionan las plantillas para la gestión de clústeres. Palo Alto Networks proporciona plantillas compatibles con la comunidad para implementar CN-Series con* Helm *y* Terraform.

- Implementación del cortafuegos CN-Series como servicio de Kubernetes en OKE
- Implementación del cortafuegos CN-Series como un DaemonSet en OKE

Antes de pasar de implementar CN-Series como un DaemonSet a CN-Series como servicio o viceversa, debe eliminar y volver a aplicar `plugin-serviceaccount.yaml`. *Para obtener más información, consulte* Crear cuentas de servicio para la autenticación de clúster.

- *Cuando implemente el CN-Series como un DaemonSet en OKE,* `pan-plugin-cluster-mode-secret` *no debe existir.*
- *Cuando implementa el CN-Series como un servicio de Kubernetes OKE,* `pan-plugin-cluster-mode-secret` *debe estar presente.*

Implementación del cortafuegos CN-Series como servicio de Kubernetes en OKE

¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series Implementación	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

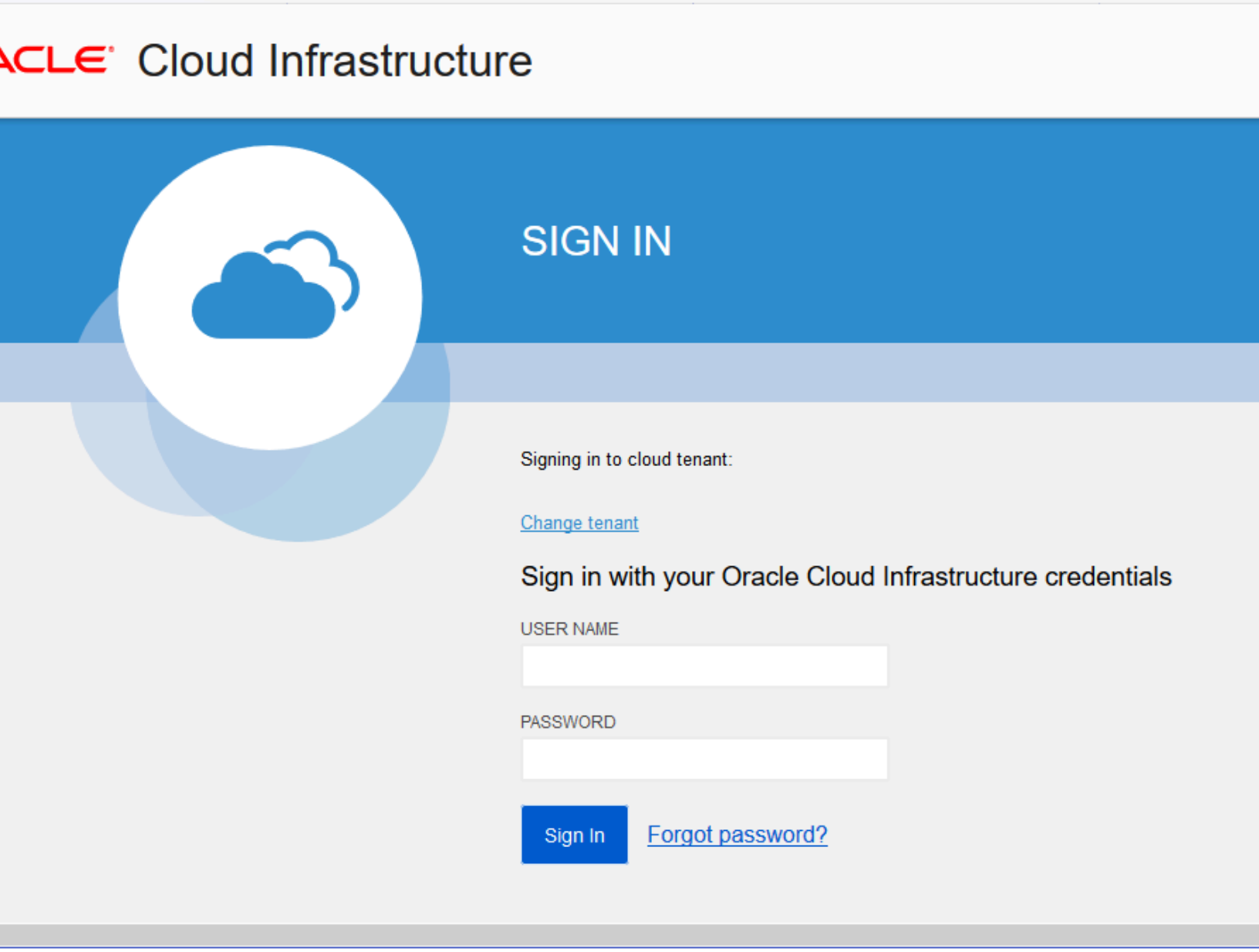
Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como un servicio de Kubernetes en la plataforma OKE.

Oracle Linux 8.5 OS es el único entorno cualificado para implementar el cortafuegos CN-Series en OKE.

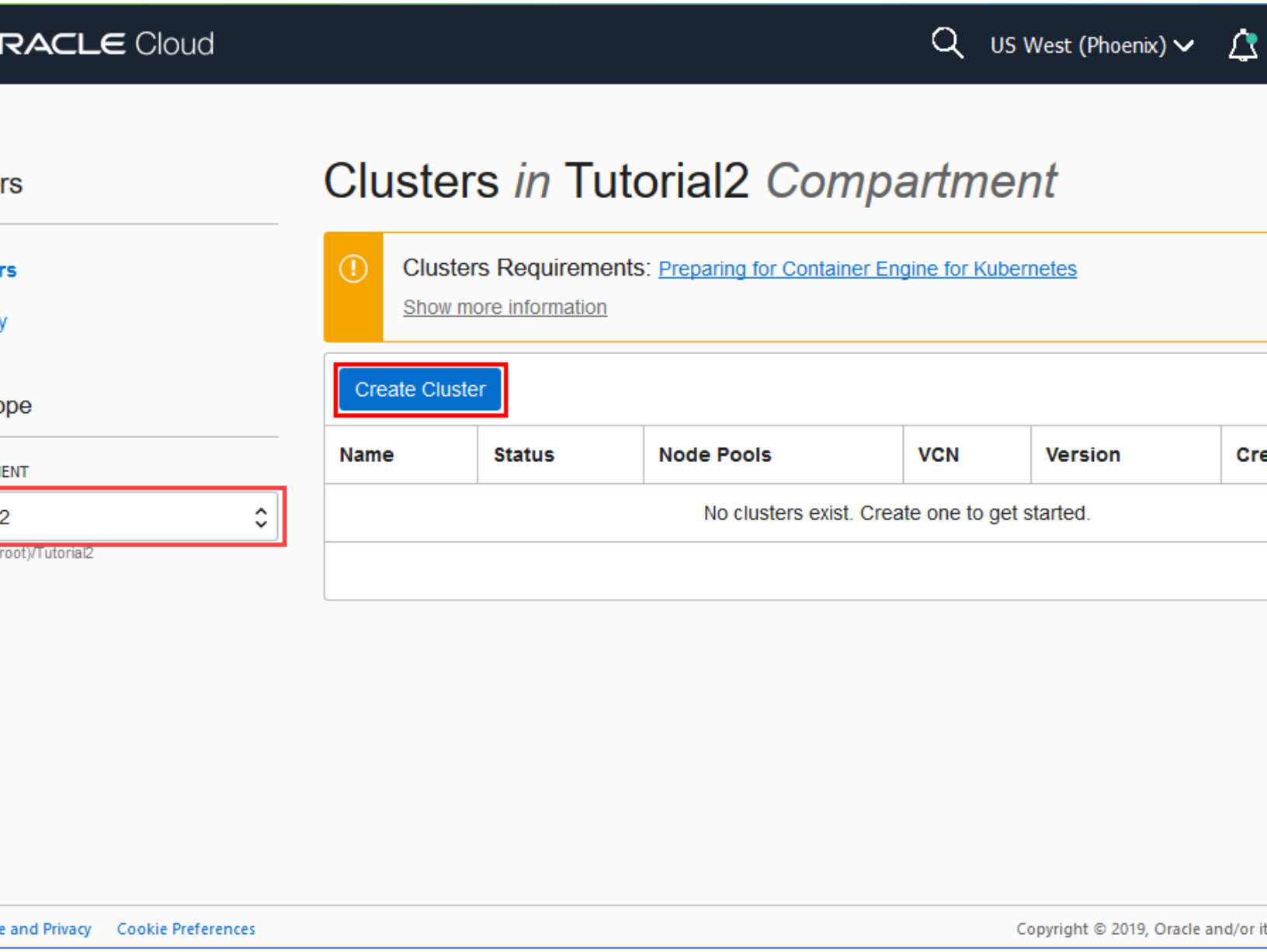
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en OKE, haga lo siguiente:

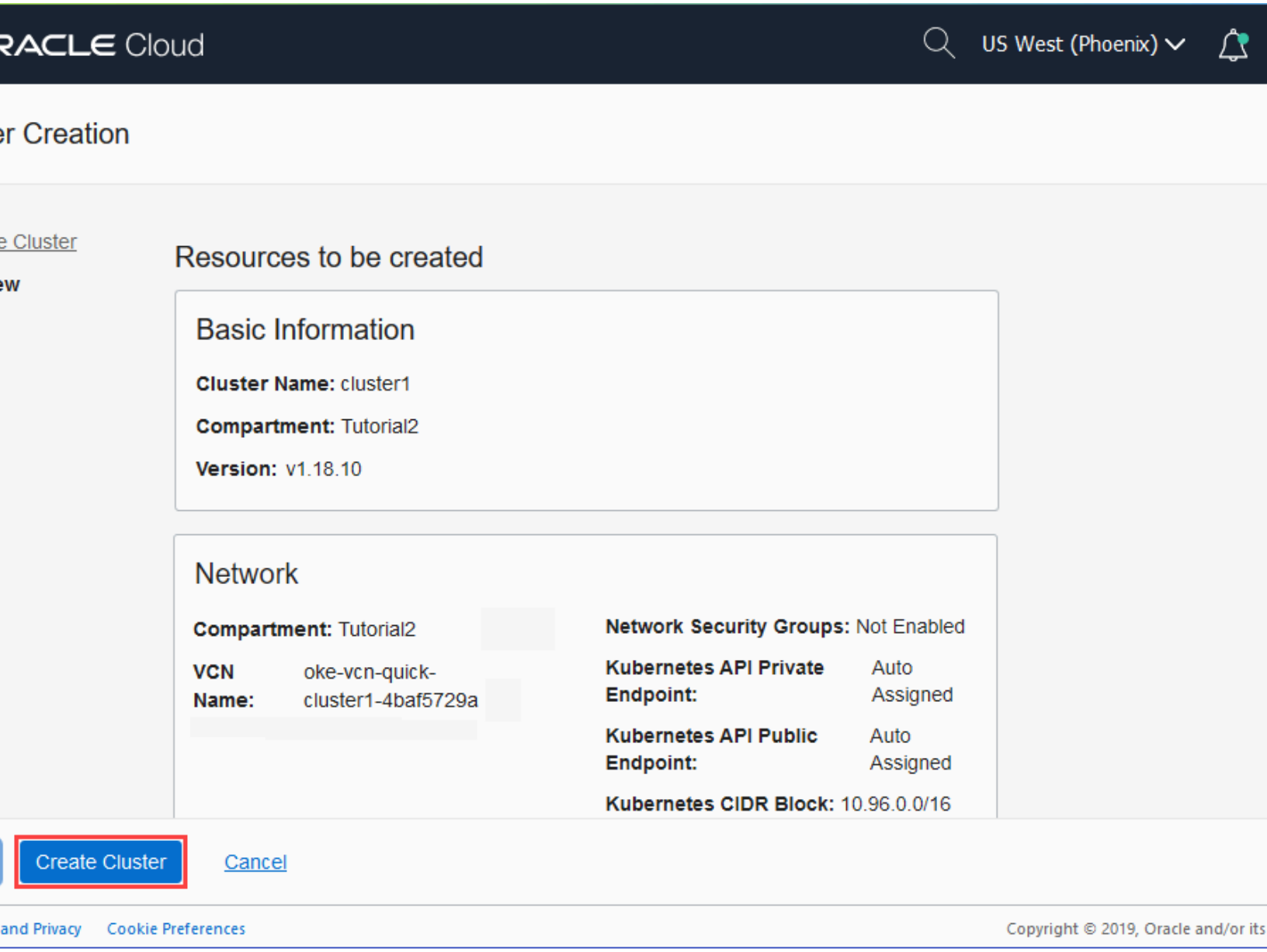
1. Inicie sesión en Oracle Cloud Infrastructure.



2. Haga clic en el menú de navegación, vaya a **En Soluciones y plataforma**, y haga clic en **Servicios para desarrolladores**.
3. Haga clic en **Clústeres de Kubernetes**.
4. Seleccione un compartimento y haga clic en **Crear clúster**.



5. En el cuadro de diálogo Crear clúster, haga clic en **Custom Create (Creación personalizada)** y, a continuación, haga clic en **Launch Workflow (Iniciar flujo de trabajo)**.
6. En la página **Crear clúster** escriba el **nombre** del clúster y otros detalles.
7. Haga clic en **Siguiente** para revisar los detalles especificados para el nuevo clúster.
8. En la página Revisar, haga clic en **Crear clúster**.



1. Debe asegurarse de que ese clúster tenga los recursos de Requisitos previos del modelo CN-Series compatibles con el cortafuegos.

   `kubectl get nodes`

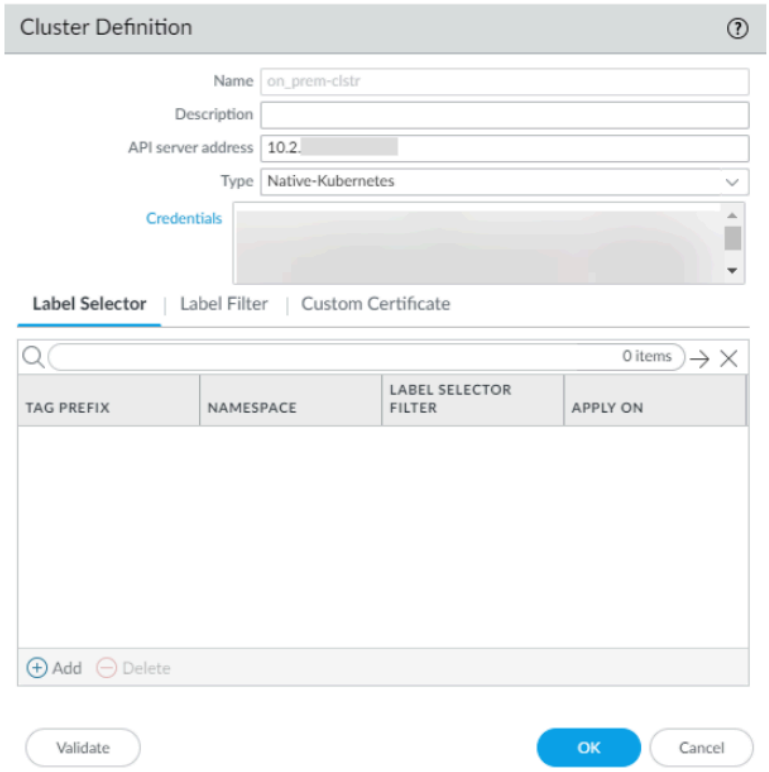
   `kubectl describe node <node-name>`

   Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

   La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series

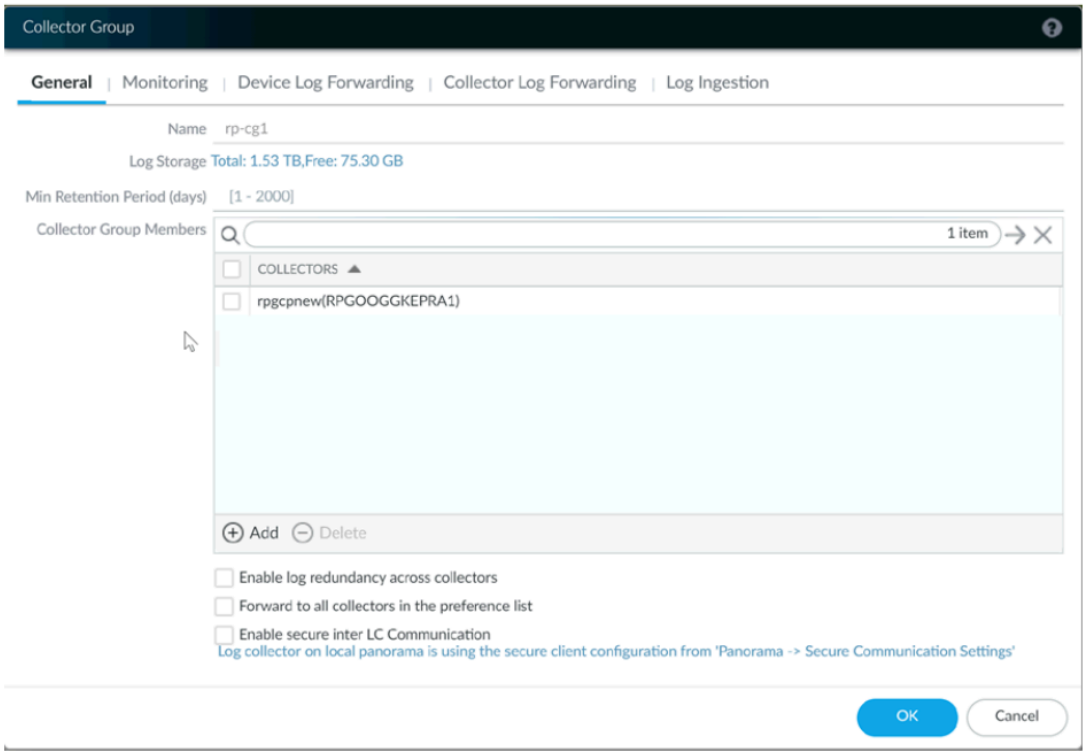
   Asegúrese de tener la siguiente información:

   - Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- Tenga lista la ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

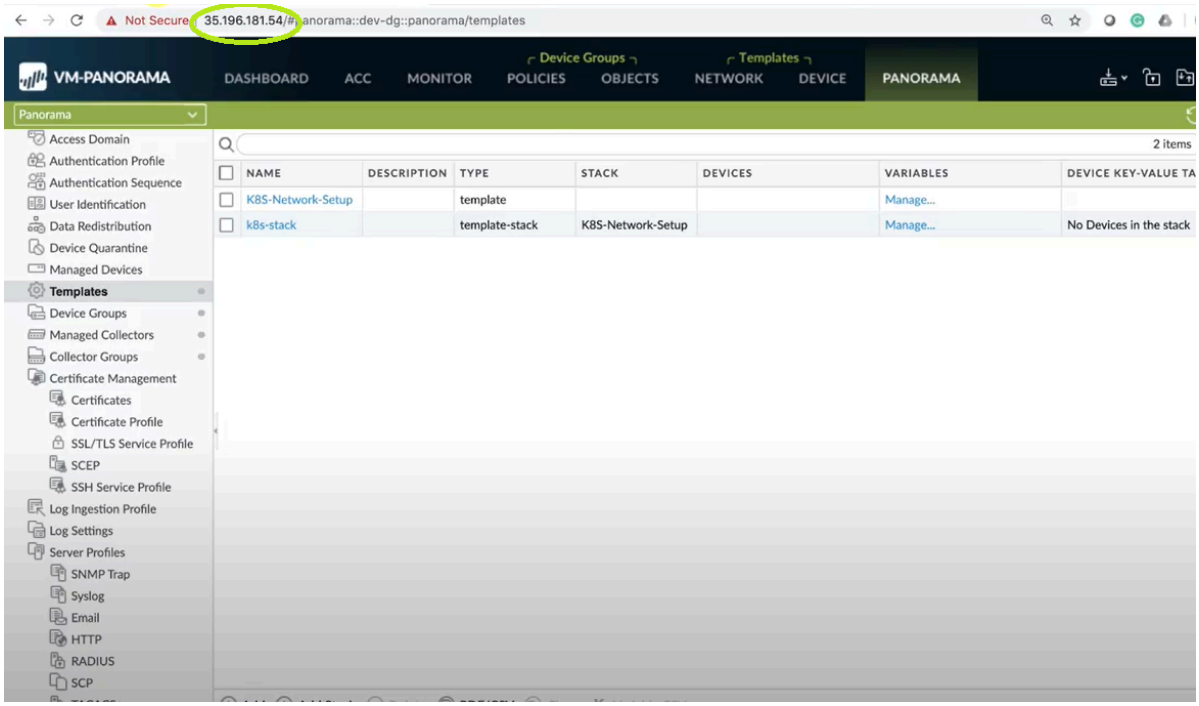
STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt-dynamic-pv.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

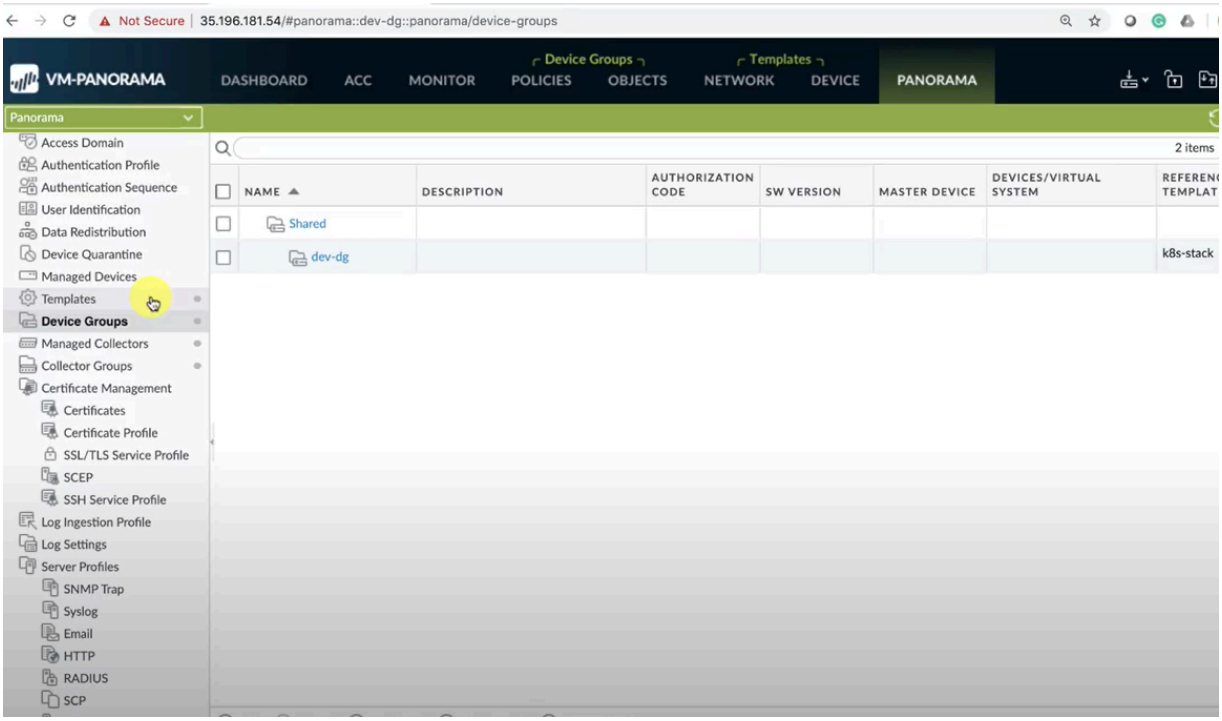
STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-mgmt-config
  namespace: kube-system
data:
  PAN_OPERATION_MODE: "daemonset"
  PAN_SERVICE_NAME: "pan-mgmt"
  # Panorama settings
  PAN_PANORAMA_IP: "35.196.181.54"
  PAN_PANORAMA_AUTH_KEY:
  PAN_DEVICE_GROUP: "dev-dg"
  PAN_TEMPLATE: "k8s-stack"
#Non-mandatory parameters
  PAN_PANORAMA_CGNAME: "rp-cg1"
  #PAN_CERTIFICATE: ""
  #PAN_CERTKEYFILE: ""
  #PAN_CERTPASSPHRASE: ""
```

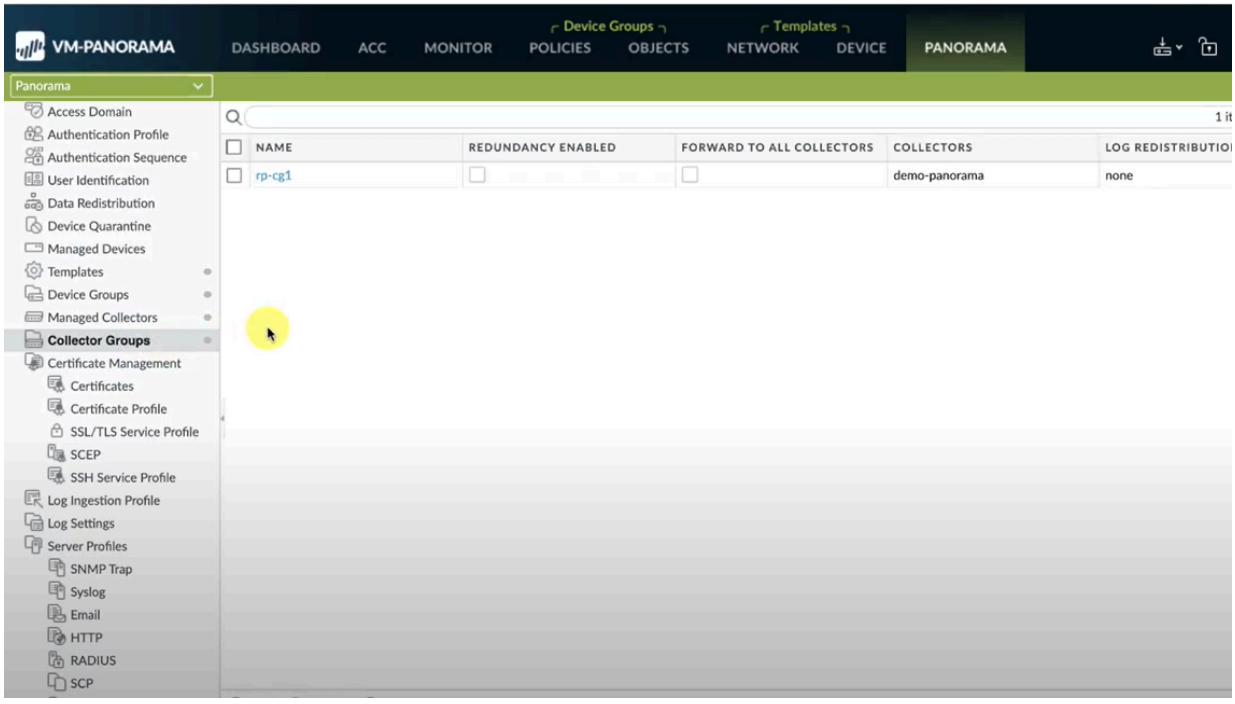
Debe asegurarse de que el valor del parámetro `PAN_PANORAMA_IP` en su archivo YAML coincida con su dirección IP de Panorama real, como se muestra en el siguiente diagrama:



Debe asegurarse de que el valor del parámetro de `PAN_DEVICE_GROUP` y `PAN_TEMPLATE` en su archivo YAML coincida con el nombre del grupo de dispositivos y la pila de plantillas que creó en Panorama, como se muestra en el siguiente diagrama:

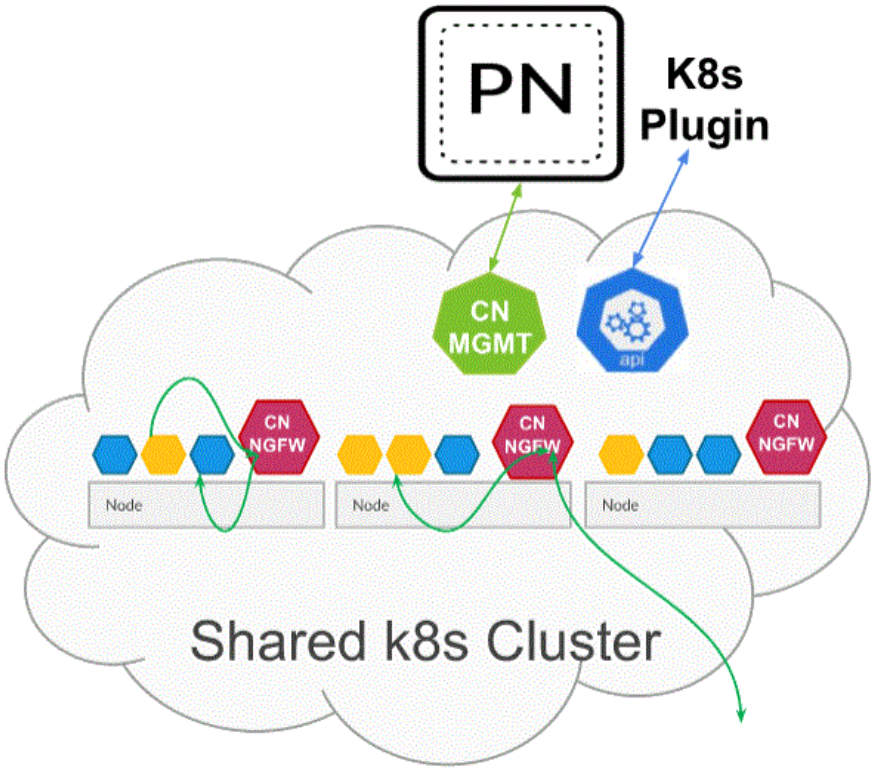


Debe asegurarse de que el valor del parámetro de `PAN_PANORAMA_CG_NAME` sea el mismo que el nombre del colector de logs que creó.



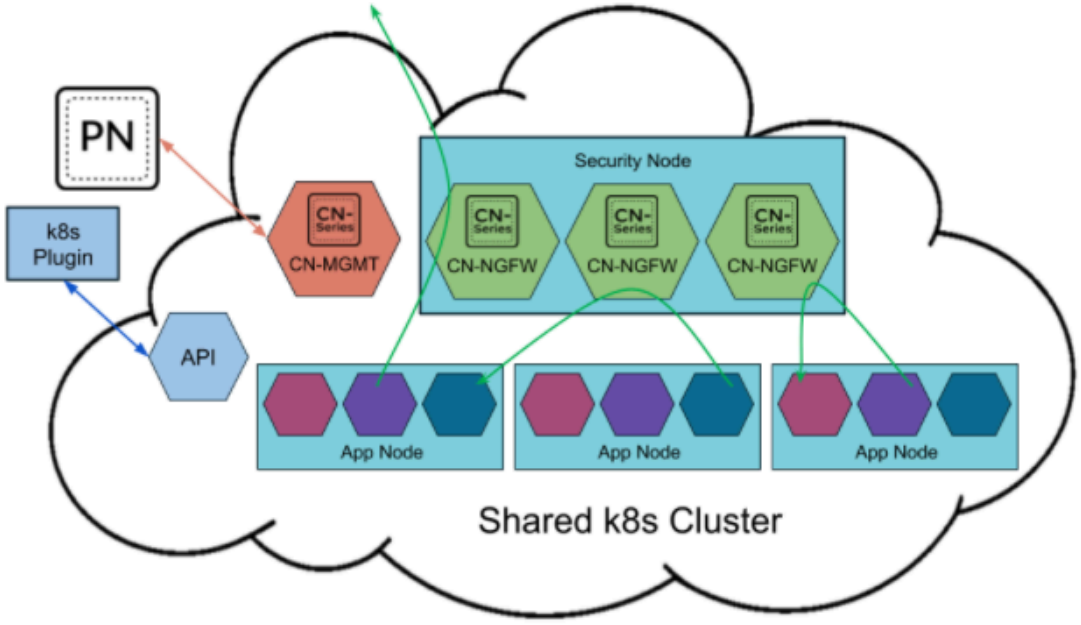
Para obtener más información, consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Implemente el servicio CN-NGFW. Realice los siguientes pasos:



Cuando se implementa como un servicio de Kubernetes, las instancias de CN-NGFW se pueden implementar en nodos de seguridad y el tráfico de pods de aplicaciones se redirige a una instancia CN-NGFW disponible para su inspección y aplicación.

Al implementar el cortafuegos CN-Series en OKE como un servicio de Kubernetes, puede usar los archivos yaml de la carpeta nativa pan-cn-k8s-service.



1. Verifique que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

   Consulte Creación de cuentas de servicio para la autenticación de clúster.

2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   kubectl apply -f pan-cni-configmap.yaml

3. Utilice kubectl para ejecutar pan-cn-ngfw-svc.yaml.

   kubectl apply -f pan-cn-ngfw-svc.yaml

   Este yaml debe implementarse antes de pan-cni.yaml.

4. Utilice Kubectl para ejecutar pan-cni.yaml.

   kubectl apply -f pan-cni.yaml

5. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
6. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.

STEP 5 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

   Ejemplo de pan-cn-mgmt-configmap de OKE.

```
apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-
config namespace: kube-system data: PAN_SERVICE_NAME:
 pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama
 settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:
 "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-
template-stack>" PAN_CGNAME: "<panorama-collector-group>"
 PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters #
 Recommended to have same name as the cluster name provided in
 Panorama Kubernetes plugin - helps with easier identification
 of pods if managing multiple clusters with same Panorama
 #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" #
 Comment out to use CERTs otherwise PSK for IPSec between pan-
mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed
 # Override auto-detect of jumbo-frame mode and force enable
 system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT
 pod with GTP enabled. For complete functionality, need GTP #
 enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable
 high feature capacities. Estos necesitan mucha memoria para
 el pod de MGMT y # una memoria superior/coincidente a la que
 se especifica a continuación para el pod NGFW. # Consulte la
 documentación de requisitos del sistema para ver el tamaño
```



```
de CPU de NGFW máximo admitido # admitido para cada perfil de
memoria. #PAN_NGFW_MEMORY: "6.5Gi" #PAN_NGFW_MEMORY: "48Gi"
#PAN_NGFW_MEMORY: "56Gi"
```

Sample pan-cn-mgmt-dynamic-pv.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path> command: ["/usr/bin/pan_start.sh"]
 imagePullPolicy: Siempre
```

```
 containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

2. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-slot-crd.yaml

   kubectl apply -f pan-cn-mgmt-slot-cr.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente Crear cuenta de servicio para la autenticación de clúster.

3. Verifique que los pods CN-MGMT estén activos ejecutando el siguiente comando:

   kubectl get pods -l app=pan-mgmt -n kube-system

   Tarda unos 5 y 6 minutos.

STEP 6 | Implemente los pods CN-NGFW.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que los pods CN-NGFW se están ejecutando.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 7 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

kubectl -n kube-system get pods

STEP 8 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 9 | Implemente su aplicación en el clúster.

Implementación del cortafuegos CN-Series como un DaemonSet en OKE

¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series Implementación	• CN-Series 10.2.x or above Container Images • Panorama con PAN-OS 10.2.x o versiones superiores • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

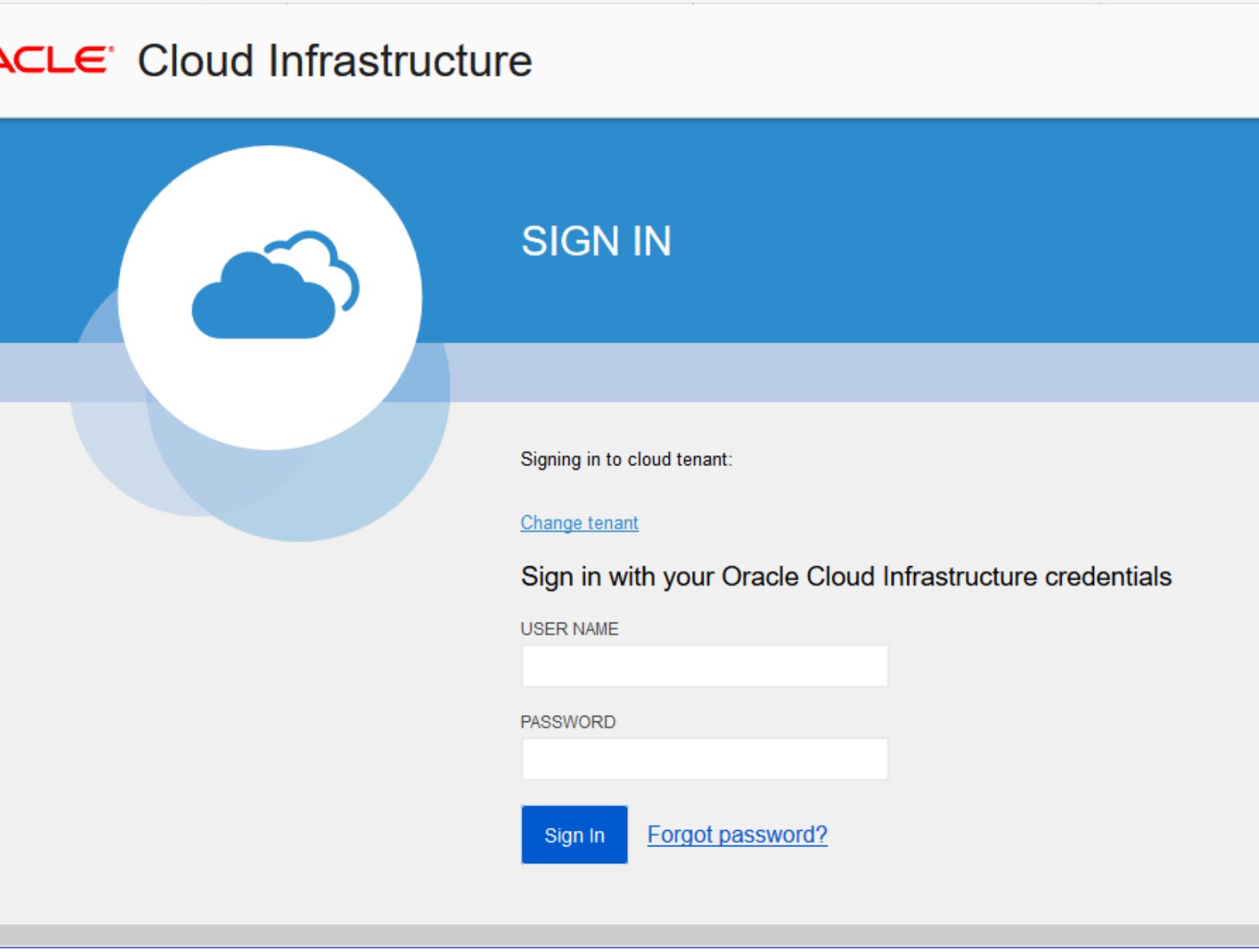
Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como Daemonset en la plataforma OKE:

Oracle Linux 8.5 OS es el único entorno cualificado para implementar el cortafuegos CN-Series en OKE.

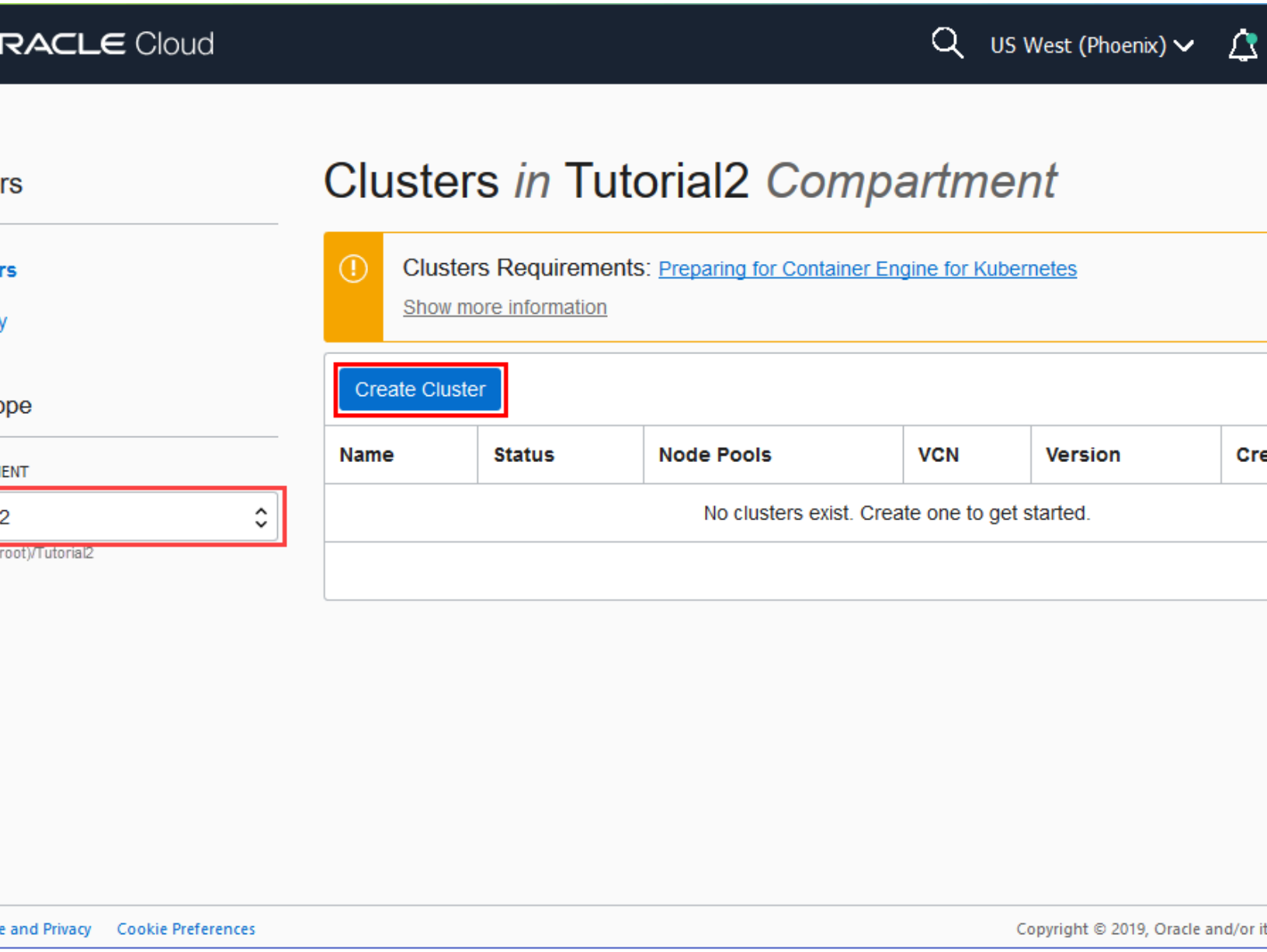
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en OKE, haga lo siguiente:

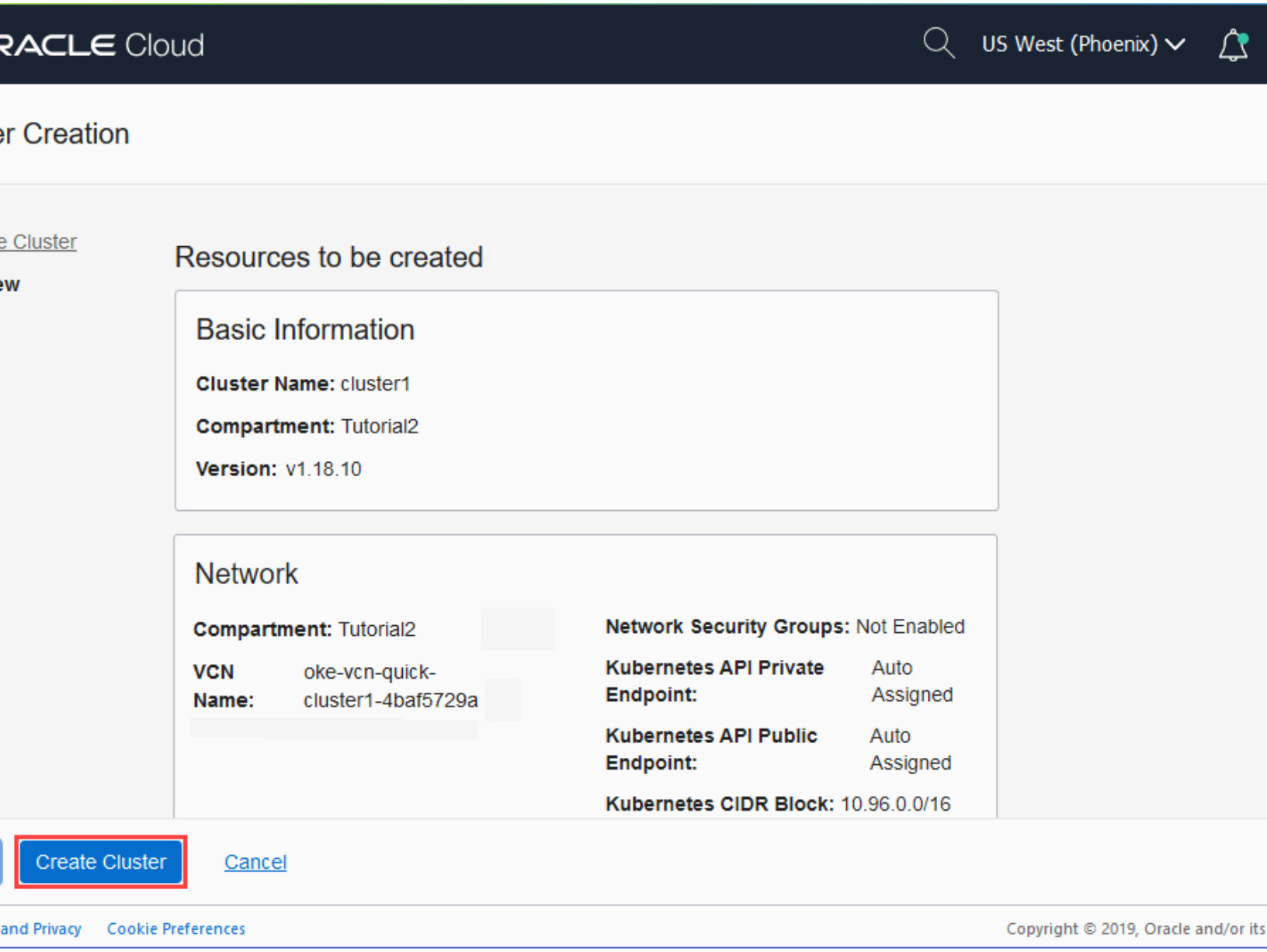
1. Inicie sesión en la infraestructura de Oracle Cloud.



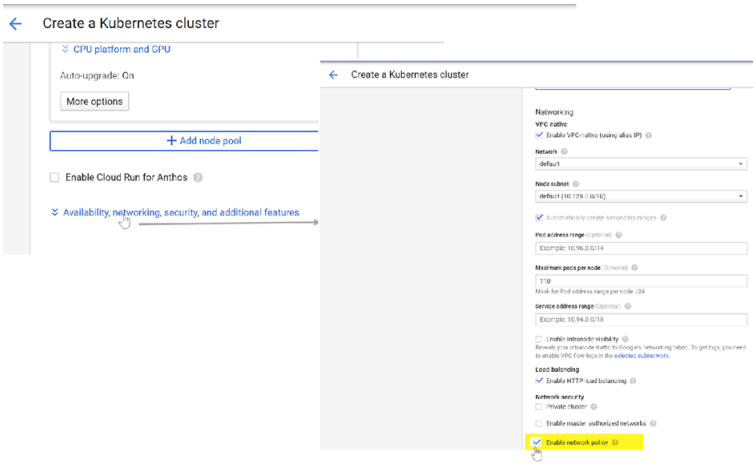
2. Haga clic en el menú de navegación, vaya a **En Soluciones y plataforma**, y, a continuación, haga clic en **Servicios para desarrolladores**.
3. Haga clic en **Clústeres de Kubernetes**.
4. Seleccione un compartimento y haga clic en **Crear clúster**.



5. En el cuadro de diálogo Crear clúster, haga clic en **Custom Create (Creación personalizada)** y, a continuación, haga clic en **Launch Workflow (Iniciar flujo de trabajo)**.
6. En la página **Crear clúster** escriba el **nombre** del clúster y otros detalles.
7. Haga clic en **Siguiente** para revisar los detalles especificados para el nuevo clúster.
8. En la página Revisar, haga clic en **Crear clúster**.



Si su clúster está en OKE, asegúrate de habilitar la API de política de red de Kubernetes para permitir que el administrador del clúster especifique qué pods pueden comunicarse entre sí. Esta API es necesaria para que los pods CN-NGFW y CN-MGMT se comuniquen.



Verifique que el clúster tenga los recursos adecuados. Asegúrese de que ese clúster tenga los recursos de Requisitos previos del modelo CN-Series para admitir el cortafuegos.

`kubectl get nodes`

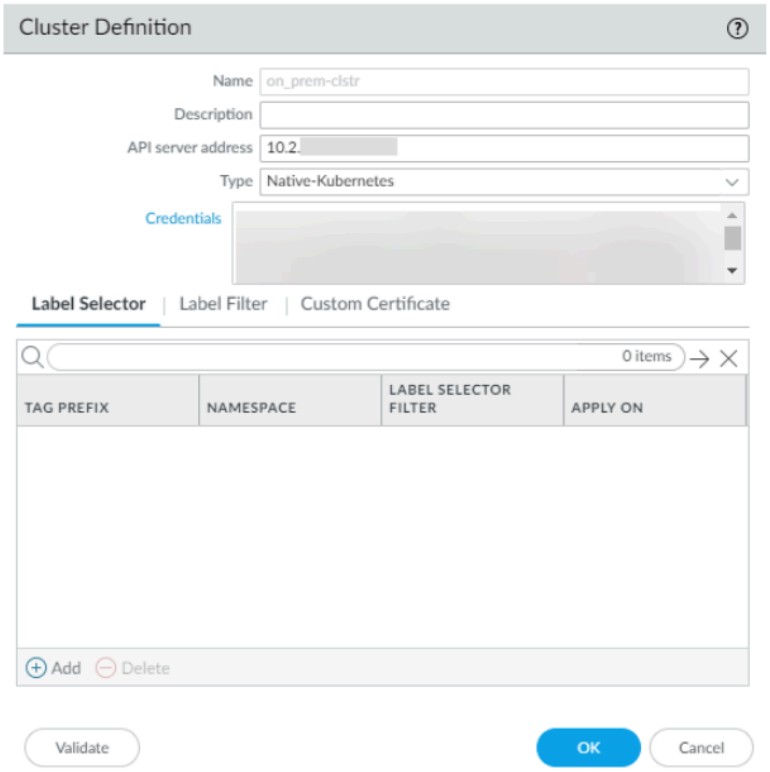
`kubectl describe node <node-name>`

Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series.

Asegúrese de tener la siguiente información:

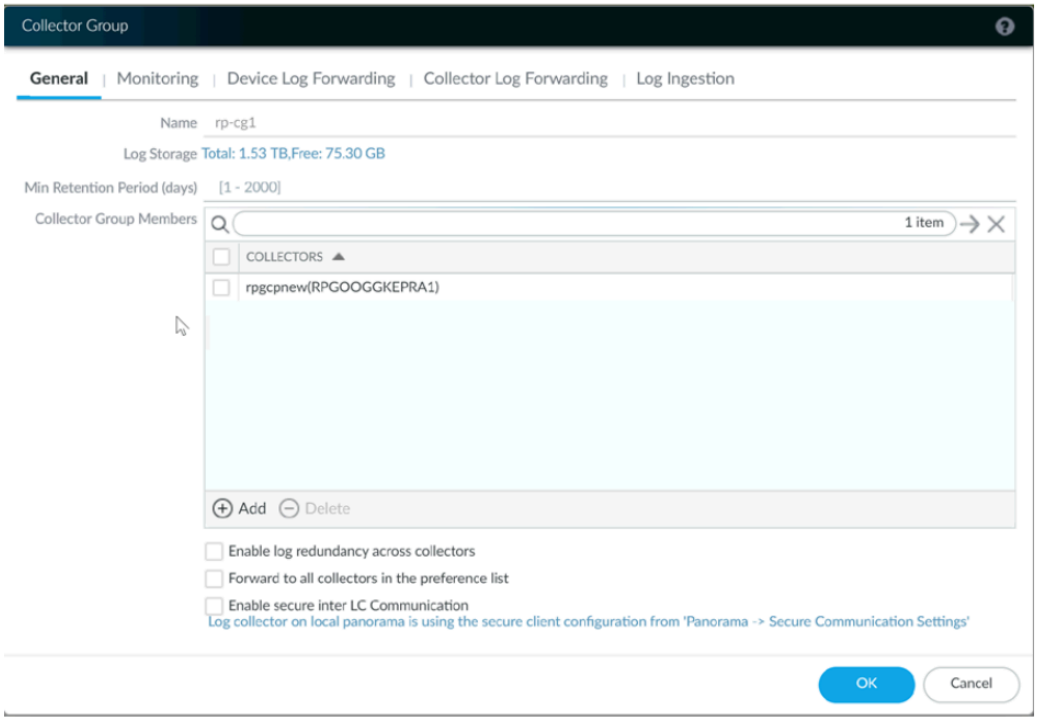
- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

Para obtener más información, consulte Configurar el complemento de Kubernetes para supervisar los clústeres.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt-dynamic-pv.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

Debe sustituir la ruta de la imagen en los archivos YAML para incluir la ruta a su registro privado de contenedor de Google y proporcionar los parámetros requeridos. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Implementación de CNI DaemonSet.

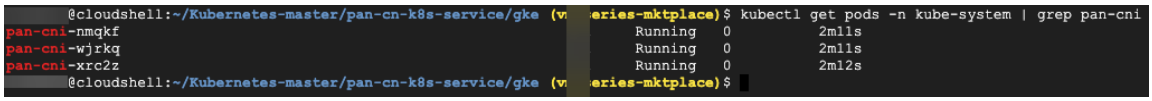
El contenedor CNI se implementa como un DaemonSet (un pod por nodo) y crea dos interfaces en el pod CN-NGFW para cada aplicación implementada en el nodo. Cuando utilice los comandos kubectl para ejecutar los archivos pan-cni YAML, se convierte en parte de la cadena de servicios en cada nodo.

Al implementar el cortafuegos CN-Series en OKE como un Daemonset, puede usar los archivos yaml de la carpeta nativa pan-cn-k8s-daemonset.

1. El cortafuegos CN-Series requiere tres cuentas de servicio con los permisos mínimos que le autorizan a comunicarse con los recursos del clúster de Kubernetes. Deberá Crear cuentas de servicio para la autenticación de clúster con CN-Series y verificar que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.
2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   kubectl apply -f pan-cni-configmap.yaml
3. Utilice Kubectl para ejecutar pan-cni.yaml.

   kubectl apply -f pan-cni.yaml
4. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
5. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.



STEP 5 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

   Ejemplo pan-cn-mgmt-configmap

```
apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-
config namespace: kube-system data: PAN_SERVICE_NAME:
 pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama
 settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:
 "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-
template-stack>" PAN_CGNAME: "<panorama-collector-group>"#Non-
mandatory parameters # Recommended to have same name as
 the cluster name provided in Panorama Kubernetes plugin
 - helps with easier identification of pods if managing
 multiple clusters with same Panorama #CLUSTER_NAME: "<Cluster
 name>" #PAN_PANORAMA_IP2: "" # Comment out to use CERTs
 otherwise PSK for IPSec between pan-mgmt and pan-ngfw
 #IPSEC_CERT_BYPASS: "" # No values needed # Override auto-
detect of jumbo-frame mode and force enable system-wide
 #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT pod with GTP
 enabled. For complete functionality, need GTP # enable at
```



```
 Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high
feature capacities. Estos necesitan mucha memoria para el
pod de MGMT y # una memoria superior/coincidente a la que
se especifica a continuación para el pod NGFW. # Consulte la
documentación de requisitos del sistema para ver el tamaño
de CPU de NGFW máximo admitido # admitido para cada perfil de
memoria. #PAN_NGFW_MEMORY: "6.5Gi" #PAN_NGFW_MEMORY: "48Gi"
#PAN_NGFW_MEMORY: "56Gi"
```

Sample pan-cn-mgmt-dynamic-pv.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

```
 containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

2. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente el paso Crear cuentas de servicio para la autenticación de clúster con CN-Series.

3. Verifique que los pods CN-MGMT estén activos.

   Tarda unos 5 y 6 minutos.

   Utilice **kubectl get pods -l app=pan-mgmt -n kube-system**

   ```
   NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1
   ```

   ```
   Ejecutando 0 27hpan-mgmt-sts-1 1/1 Ejecutando 0 27h
   ```

STEP 6 | Implemente los pods CN-NGFW.

De forma predeterminada, el pod CN-NGFW del plano de datos del cortafuegos se implementa como un DaemonSet. Una instancia del pod CN-NFGW puede proteger el tráfico de hasta 30 pods de aplicaciones en un nodo.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que todos los pods CN-NGFW se están ejecutando. (uno por nodo en su clúster)

   Este es un resultado de muestra de un clúster local de 4 nodos.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

   ```
   NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

   pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>

   pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>

   pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>

   pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
   ```

STEP 7 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 En ejecución
0 27hpan-cni-9j4rs 1/1 En ejecución
0 27hpan-cni-ddwb4 1/1 En ejecución
0 27hpan-cni-fwfrk 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-j62rk 1/1 En ejecución
0 27hpan-cni-lmxdz 1/1 En ejecución
0 27hpan-mgmt-sts-0 1/1 En ejecución
0 27hpan-mgmt-sts-1 1/1 En ejecución
0 27hpan-ngfw-ds-8g5xb 1/1 En ejecución
27hpan-ngfw-ds-qsrm6 1/1 En ejecución
0 27hpan-ngfw-ds-vqk7z 1/1 En ejecución
0 27hpan-ngfw-ds-zncqg 1/1 En ejecución
```

STEP 8 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 9 | Implemente su aplicación en el clúster.

Implementación de los cortafuegos CN-Series en EKS.

¿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 versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Después de revisar los Componentes básicos de la serie CN-Series y la descripción general de alto nivel del flujo de trabajo en Protección de los entornos de Kubernetes con CN-Series, puede comenzar a implementar el cortafuegos CN-Series en la plataforma AWS EKS para proteger el tráfico entre contenedores dentro del mismo clúster, así como entre contenedores y otros tipos de cargas de trabajo, como máquinas virtuales y servidores bare-metal.

Necesita herramientas estándar de Kubernetes, como kubectl o Helm, para implementar y gestionar sus clústeres, aplicaciones y servicios de cortafuegos de Kubernetes.

Para obtener más información, consulte Implementación de cortafuegos CN-Series con gráficos y plantillas de Helm.*. Panorama no está diseñado para ser un orquestador para la implementación y gestión de clústeres de Kubernetes. Los proveedores gestionados de Kubernetes proporcionan las plantillas para la gestión de clústeres. Palo Alto Networks proporciona plantillas compatibles con la comunidad para implementar CN-Series con* Helm *y* Terraform.

- Implementación del cortafuegos CN-Series como servicio de Kubernetes en AWS EKS
- Implementación del cortafuegos CN-Series como un DaemonSet en AWS EKS
- Implementación de la CN-Series desde AWS Marketplace

Antes de pasar de implementar CN-Series como un DaemonSet a CN-Series como servicio o viceversa, debe eliminar y volver a aplicar `plugin-serviceaccount.yaml`*. Para obtener más información, consulte* Crear cuentas de servicio para la autenticación de clúster.

- *Cuando implementa el CN-Series como un DaemonSe en EKS,* `pan-plugin-cluster-mode-secret` *no debe existir.*
- *Cuando implementa el CN-Series como un servicio de Kubernetes en EKS,* `pan-plugin-cluster-mode-secret` *debe estar presente.*

Implementación del cortafuegos CN-Series como servicio de Kubernetes en AWS EKS

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

Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como un servicio de Kubernetes.

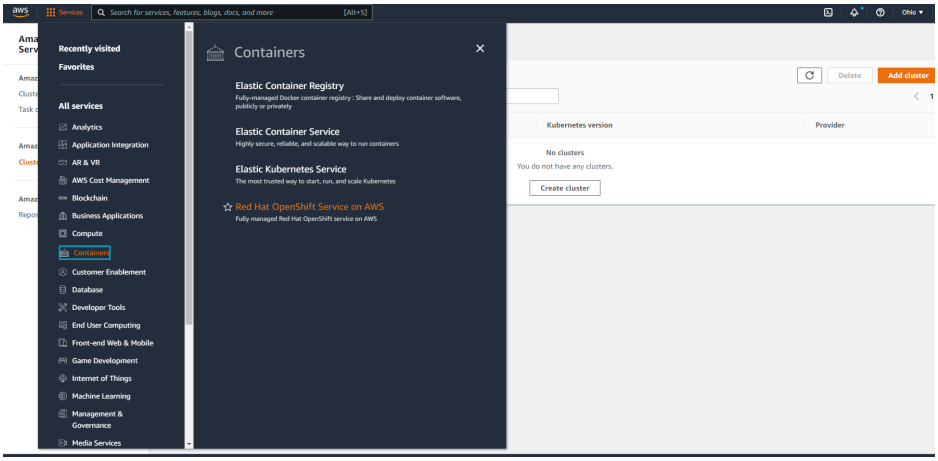
Antes de comenzar, asegúrese de que la versión del archivo YAML de la serie CN-Series sea compatible con la versión de PAN-OS.

- PAN-OS 10.1.2 o posterior requiere YAML 2.0.2
- PAN-OS 10.1.0 y 10.1.1 requieren YAML 2.0.0 o 2.0.1

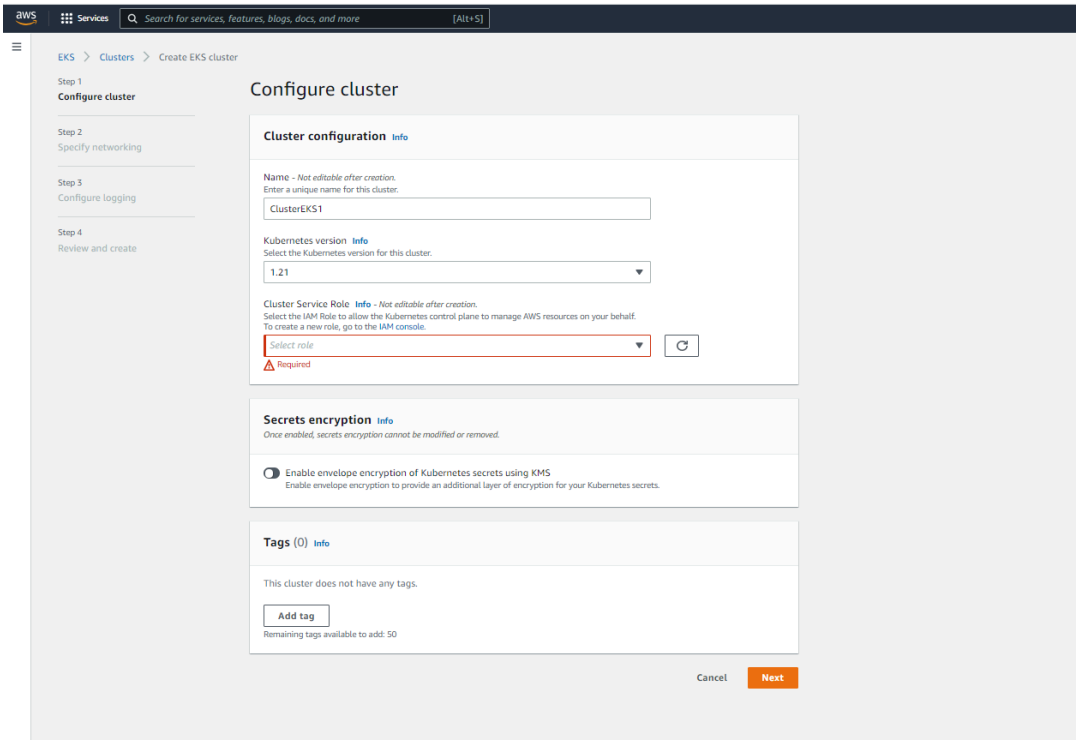
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en AWS EKS, haga lo siguiente:

1. Haga clic en el menú de navegación de **Servicios**, vaya a **Contenedores->Elastic Kubernetes Service**.



2. Haga clic en **Create Cluster (Crear clúster)**.
3. Rellene los detalles necesarios y, a continuación, haga clic en **Create (Crear)**.



1. Verifique que el clúster tenga los recursos adecuados. Asegúrese de que el clúster tenga los recursos de Requisitos previos del modelo CN-Series compatibles con el cortafuegos:

```
kubectl get nodes
```

```
kubectl describe node <node-name>
```


Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series

Asegúrese de tener la siguiente información:

- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama. Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.
- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.
- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

Debe reemplazar la ruta de la imagen en los archivos YAML para incluir la ruta a su registro privado y proporcionar los parámetros requeridos. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Actualice la clase de almacenamiento. Para ser compatible con la CN-Series implementada en AWS Outpost, debe utilizar el controlador de almacenamiento aws-ebs-csi-driver, que garantiza que

Outpost extrae los volúmenes de Outpost durante la creación dinámica de volúmenes persistentes (PV).

1. Aplicar el siguiente yaml.

   kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/deploy/kubernetes/overlays/stable/?ref=release-0.10"

2. Verifique que el controlador ebs-sc se esté ejecutando.

   kubectl -n kube-system get pods

3. Actualice pan-cn-storage-class.yaml para que coincida con el ejemplo siguiente.

```
apiVersion: v1 kind: StorageClass apiVersion: storage.k8s.io/
v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com
 volumeBindingMode: WaitForFirstConsumer parameters: type: gp2
```

4. Añada **storageClassName: ebs-sc** a pan-cn-mgmt.yaml en las ubicaciones que se muestran a continuación.

```
volumeClaimTemplates: - metadata: name: panlogs spec:
 #storageClassName: pan-cn-storage-class //For better disk
 iops performance for logging accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc // resources: requests: storage:
 20Gi # change this to 200Gi while using storageClassName
 for better disk iops - metadata: name: varlogpan spec:
 #storageClassName: pan-cn-storage-class //For better disk
 iops performance for dp logs accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc resources: requests: storage: 20Gi #
 change this to 200Gi while using storageClassName for better
 disk iops - metadata: name: varcores spec: accessModes:
 [ "ReadWriteOnce" ] storageClassName: ebs-sc resources:
 requests: storage: 2Gi - metadata: name: panplugincfg spec:
 accessModes: [ "ReadWriteOnce" ] storageClassName: ebs-sc
 resources: requests: storage: 1Gi - metadata: name: panconfig
 spec: accessModes: [ "ReadWriteOnce" ] storageClassName:
 ebs-sc resources: requests: storage: 8Gi - metadata:
 name: panplugins spec: accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc resources: requests: storage: 200Mi
```

STEP 5 | Si está utilizando el escalado automático en su entorno de Kubernetes, haga lo siguiente:

1. Implemente el adaptador de métricas de Amazon CloudWatch para Kubernetes en su clúster de CN-Series como servicio. Debe permitir que CloudWatch tenga acceso completo a las dos funciones de IAM asociadas a los pods y clústeres de Kubernetes. Para publicar las métricas personalizadas en CloudWatch, la función de los nodos de trabajo debe tener la política gestionada de AWS **CloudWatchAgentServerPolicy** para que la HPA pueda recuperarlas.
2. Descargue los archivos yaml de HPA específicos de EKS del Repositorio de GitHub de Palo Alto Networks.
3. Si su CN-MGMT se implementa en un espacio de nombres personalizado, actualice pan-cn-adapater.yaml con el espacio de nombres personalizado. El espacio de nombres predeterminado es **kube-system**.

4. Modifique **pan-cn-hpa-dp.yaml** y **pan-cn-hpa-mp.yaml**.
   1. Introduzca el número mínimo y máximo de réplicas.
   2. (Opcional) Cambie los valores de frecuencia de ampliación o reducción para adaptarlos a su implementación. Si no cambia estos valores, se utilizan los valores predeterminados.
   3. Copie la siguiente sección para cada métrica que desee utilizar para el escalado.

      ```
      - type: Pods pods: metric: name: pansessionactive target: type:
       AverageValue averageValue: 30
      ```

   4. Cambie el nombre de la métrica que desea usar y establezca el **averageValue** en el umbral descrito en la tabla anterior. Si no cambia estos valores, se utilizan los valores predeterminados.
   5. Guarde los cambios.

      Para obtener más información, consulte Escalado automático de pod horizontal.
5. Implemente los archivos yaml de HPA. Los archivos deben implementarse en el orden que se describe a continuación.
   1. Utilice Kubectl para ejecutar pan-cn-adapter.yaml

      ```
      kubectl apply -f pan-cn-adapter.yaml
      ```
   2. Utilice Kubectl para ejecutar pan-cn-externalmetrics.yaml

      ```
      kubectl apply -f pan-cn-externalmetrics.yaml
      ```
   3. Utilice Kubectl para ejecutar pan-cn-hpa-dp.yaml

      ```
      kubectl apply -f pan-cn-hpa-dp.yaml
      ```
   4. Utilice Kubectl para ejecutar pan-cn-hpa-mp.yaml

      ```
      kubectl apply -f pan-cn-hpa-mp.yaml
      ```
6. Compruebe la implementación.

   Utilice kubectl para comprobar el pod del adaptador de métricas personalizadas en el espacio de nombres de métricas personalizadas.

   ```
   kubectl get pods -n custom-metrics
   ```

   Utilice kubectl para comprobar el recurso HPA.

   ```
   kubectl get hpa -n kube-system
   ```

   ```
   kubectl describe hpa <hpa-name> -n kube-system
   ```


STEP 6 | Implemente el servicio CN-NGFW.

1. Verifique que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

   Consulte Creación de cuentas de servicio para la autenticación de clúster.

2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   kubectl apply -f pan-cni-configmap.yaml

3. Utilice kubectl para ejecutar pan-cn-ngfw-svc.yaml.

   kubectl apply -f pan-cn-ngfw-svc.yaml

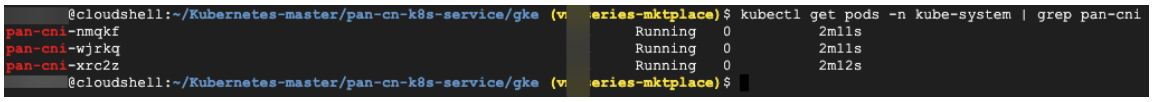
   Este yaml debe implementarse antes de pan-cni.yaml.

4. Utilice Kubectl para ejecutar pan-cni.yaml.

   kubectl apply -f pan-cni.yaml

5. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
6. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.

   kubectl get pods -n kube-system | grep pan-cni



STEP 7 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. (Requerido solo para los volúmenes persistentes aprovisionados estáticamente) Implemente los volúmenes persistentes (PV) para el StatefulSet de CN-MGMT.

   1. Cree los directorios para que coincidan con los nombres de los volúmenes locales definidos en pan-cn-pv-local.yaml.

   Necesita seis (6) directorios en al menos 2 nodos de trabajo. Inicie sesión en cada nodo de trabajo en el que se implementará el StatefulSet de CN-MGMT para crear los directorios. Por ejemplo, para crear directorios llamados / mnt / pan-local1 a / mnt / pan-local6, use el comando:

   ```
   mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
   mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
   ```

   2. Modifique pan-cn-pv-local.yaml.

   Haga coincidir el nombre de host en `nodeaffinity` y verifique que haya modificado los directorios que creó anteriormente en `spec.local.path`, luego implemente el archivo

para crear una nueva clase de almacenamiento pan-local-storage y volúmenes persistentes locales.

2. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

   Ejemplo de pan-cn-mgmt-configmap de EKS.

```
 apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-
config namespace: kube-system data: PAN_SERVICE_NAME:
 pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama
 settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:
 "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-
template-stack>" PAN_CGNAME: "<panorama-collector-
group>" # ctnr mode: "k8s-service", "k8s-ilbservice"
 PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters #
 Recommended to have same name as the cluster name provided in
 Panorama Kubernetes plugin - helps with easier identification
 of pods if managing multiple clusters with same Panorama
 #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" #
 Comment out to use CERTs otherwise PSK for IPSec between pan-
mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed
 # Override auto-detect of jumbo-frame mode and force enable
 system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT
 pod with GTP enabled. For complete functionality, need GTP #
 enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable
 high feature capacities. These need high memory for MGMT pod
 and # higher/matching memory than specified below for NGFW
 pod. #PAN_NGFW_MEMORY="6Gi" #PAN_NGFW_MEMORY="40Gi" # For
 enabling faster datapath - AF_XDP, default is AF_PACKETV2.
 This requires kernel support. #PAN_DATA_MODE: "next-gen" #HPA
 params #PAN_CLOUD: "EKS" #PAN_NAMESPACE_EKS: "EKSNamespace"
 #PUSH_INTERVAL: "15" #time interval to publish metrics to AWS
 cloudwatch
```

   Ejemplo de pan-cn-mgmt.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

```
 containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

3. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-slot-crd.yaml

   kubectl apply -f pan-cn-mgmt-slot-cr.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente Crear cuenta de servicio para la autenticación de clúster.

4. Verifique que los pods CN-MGMT estén activos.

   Tarda unos 5 y 6 minutos.

   Utilice **`kubectl get pods -l app=pan-mgmt -n kube-system`**

STEP 8 | Implemente los pods CN-NGFW.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   `containers: - name: pan-ngfw-container image: <your-private-registry-image-path>`

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   `kubectl apply -f pan-cn-ngfw-configmap.yaml`

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   `kubectl apply -f pan-cn-ngfw.yaml`

4. Compruebe que los pods CN-NGFW se están ejecutando.

   `kubectl get pods -n kube-system -l app=pan-ngfw -o wide`

STEP 9 | Habilitación del escalado automático de pod horizontal en la CN-Series.

STEP 10 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

```
kubectl -n kube-system get pods
```

STEP 11 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 12 | Implemente su aplicación en el clúster.

Implementación del cortafuegos CN-Series como un DaemonSet en AWS EKS

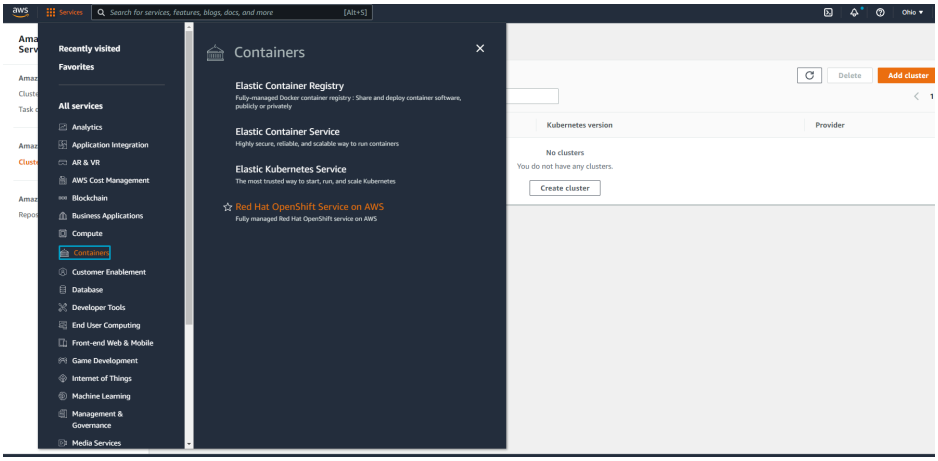
¿Dónde puedo usar esto?	¿Qué necesito?
• CN-SeriesImplementación	• CN-Series 10.1.x or above Container Images • Panoramaque ejecuta PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Complete los siguientes pasos para implementar el cortafuegos CN-Series como un daemonset en AWS EKS:

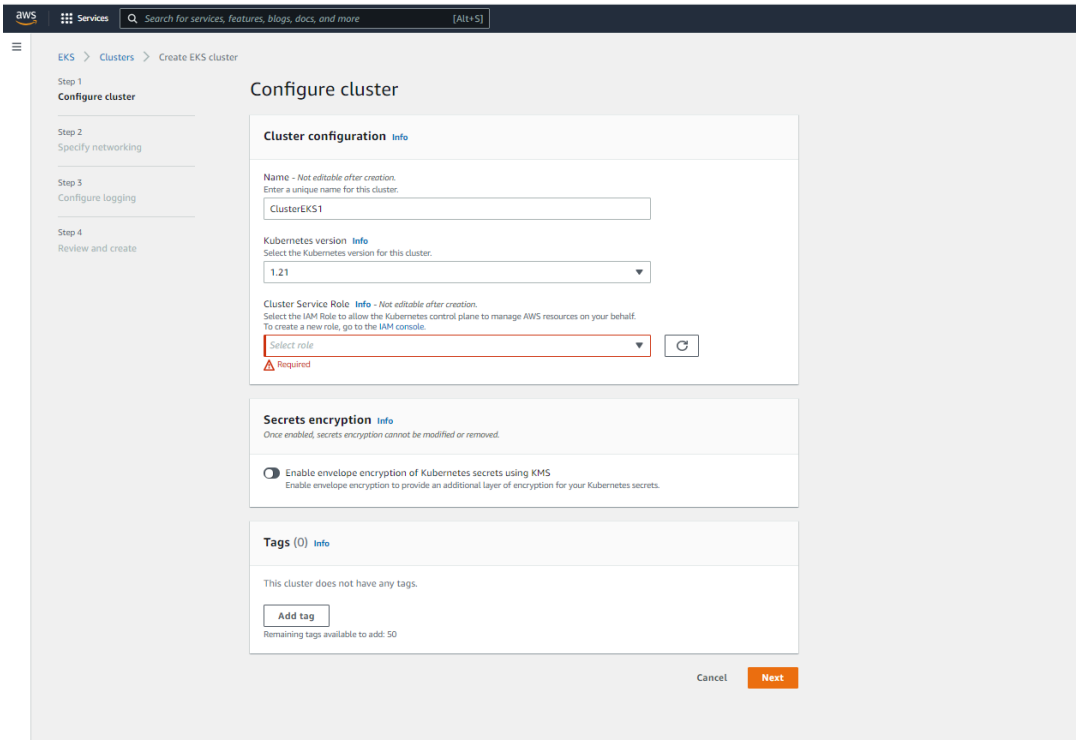
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en AWS EKS, haga lo siguiente:

1. Haga clic en el menú de navegación de **Servicios**, vaya a **Contenedores->Elastic Kubernetes Service**.



2. Haga clic en **Create Cluster (Crear clúster)**.
3. Rellene los detalles necesarios y, a continuación, haga clic en **Create (Crear)**.



Verifique que el clúster tenga los recursos adecuados. Asegúrese de que ese clúster tenga los recursos de Requisitos previos del modelo CN-Series para admitir el cortafuegos.

```
kubectl get nodes
```

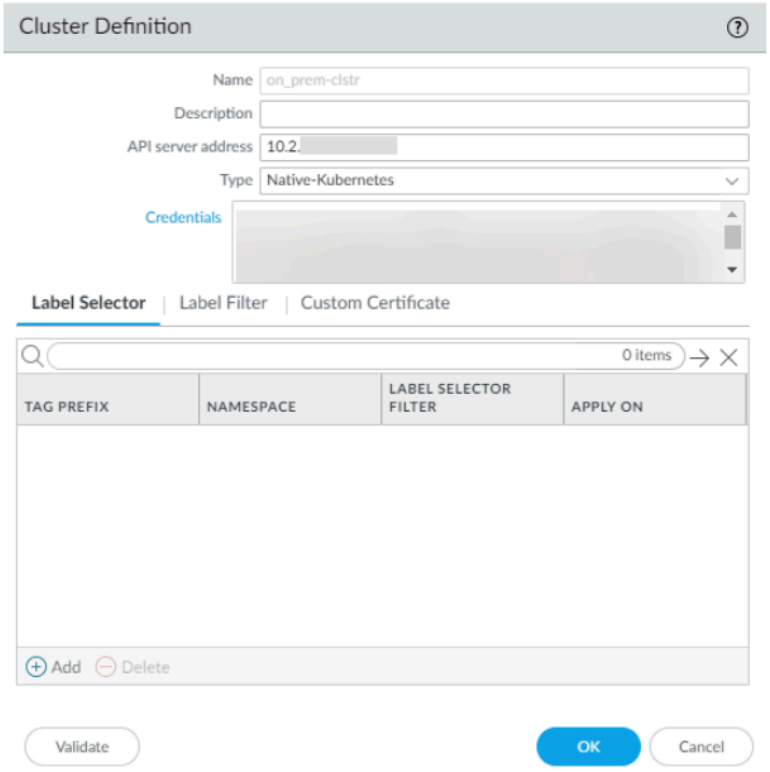
```
kubectl describe node <node-name>
```


Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series

Asegúrese de tener la siguiente información:

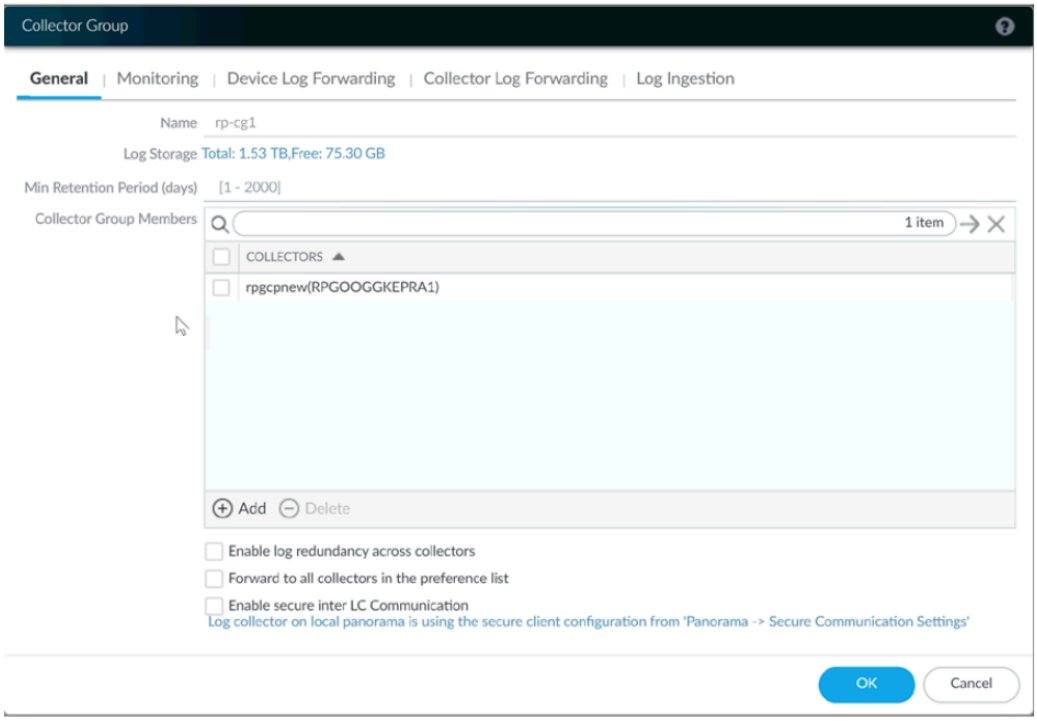
- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



  Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

  Para obtener más información, consulte Configurar el complemento de Kubernetes para supervisar los clústeres.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile el código de autorización y el ID y valor del ID de PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

Debe sustituir la ruta de la imagen en los archivos YAML para incluir la ruta a su registro privado de contenedor de Google y proporcionar los parámetros requeridos. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.

STEP 4 | Implementación de CNI DaemonSet.

El contenedor CNI se implementa como un DaemonSet (un pod por nodo) y crea dos interfaces en el pod CN-NGFW para cada aplicación implementada en el nodo. Cuando utilice los comandos kubectl para ejecutar los archivos pan-cni YAML, se convierte en parte de la cadena de servicios en cada nodo.

1. El cortafuegos CN-Series requiere tres cuentas de servicio con los permisos mínimos que le autorizan a comunicarse con los recursos del clúster de Kubernetes. Deberá Crear cuentas de

servicio para la autenticación de clúster y verificar que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

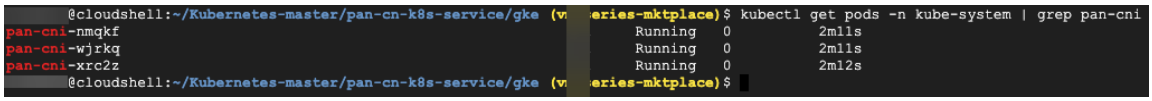
2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   kubectl apply -f pan-cni-configmap.yaml

3. Utilice Kubectl para ejecutar pan-cni.yaml.

   kubectl apply -f pan-cni.yaml

4. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
5. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.



STEP 5 | Actualice la clase de almacenamiento. Para ser compatible con la CN-Series implementada en AWS Outpost, debe utilizar el controlador de almacenamiento aws-ebs-csi-driver, que garantiza que Outpost extrae los volúmenes de Outpost durante la creación dinámica de volúmenes persistentes (PV).

1. Aplicar el siguiente yaml.

   kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/deploy/kubernetes/overlays/stable/?ref=release-0.10"

2. Verifique que el controlador ebs-sc se esté ejecutando.

   kubectl -n kube-system get pods

3. Actualice pan-cn-storage-class.yaml para que coincida con el ejemplo siguiente.

```
apiVersion: v1 kind: StorageClass apiVersion: storage.k8s.io/
v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com
 volumeBindingMode: WaitForFirstConsumer parameters: type: gp2
```

4. Añada **storageClassName: ebs-sc** a pan-cn-mgmt.yaml en las ubicaciones que se muestran a continuación.

```
volumeClaimTemplates: - metadata: name: panlogs spec:
 #storageClassName: pan-cn-storage-class //For better disk
 iops performance for logging accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc // resources: requests: storage:
 20Gi # change this to 200Gi while using storageClassName
 for better disk iops - metadata: name: varlogpan spec:
 #storageClassName: pan-cn-storage-class //For better disk
 iops performance for dp logs accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc resources: requests: storage: 20Gi #
 change this to 200Gi while using storageClassName for better
 disk iops - metadata: name: varcores spec: accessModes:
 [ "ReadWriteOnce" ] storageClassName: ebs-sc resources:
 requests: storage: 2Gi - metadata: name: panplugincfg spec:
 accessModes: [ "ReadWriteOnce" ] storageClassName: ebs-sc
 resources: requests: storage: 1Gi - metadata: name: panconfig
 spec: accessModes: [ "ReadWriteOnce" ] storageClassName:
 ebs-sc resources: requests: storage: 8Gi - metadata:
```



```
 name: panplugins spec: accessModes: [ "ReadWriteOnce" ]
 storageClassName: ebs-sc resources: requests: storage: 200Mi
```

STEP 6 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. (Requerido solo para los volúmenes persistentes aprovisionados estáticamente) Implemente los volúmenes persistentes (PV) para el StatefulSet de CN-MGMT.

   1. Cree los directorios para que coincidan con los nombres de los volúmenes locales definidos en pan-cn-pv-local.yaml.

   Necesita seis (6) directorios en al menos 2 nodos de trabajo. Inicie sesión en cada nodo de trabajo en el que se implementará el StatefulSet de CN-MGMT para crear los directorios. Por ejemplo, para crear directorios llamados / mnt / pan-local1 a / mnt / pan-local6, use el comando:

   ```
   mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
   mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
   ```

   2. Modifique pan-cn-pv-local.yaml.

   Haga coincidir el nombre de host en `nodeaffinity` y verifique que haya modificado los directorios que creó anteriormente en `spec.local.path`, luego implemente el archivo para crear una nueva clase de almacenamiento pan-local-storage y volúmenes persistentes locales.

2. Verifique que haya modificado los archivos YAML pan-cn-mgmt-configmap y pan-cn-mgmt.

   Ejemplo de pan-cn-mgmt-configmap de EKS.

   ```
    Session Contents Restored apiVersion: v1 kind: ConfigMap
    metadata: name: pan-mgmt-config namespace: kube-system
    data: PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-
   mgmt-secret # Panorama settings PAN_PANORAMA_IP: "x.y.z.a"
    PAN_DEVICE_GROUP: "dg-1" PAN_TEMPLATE_STACK: "temp-stack-1"
    PAN_CGNAME: "CG-EKS" # Intended License Bundle type - "CN-
   X-BASIC", "CN-X-BND1", "CN-X-BND2" # based on the authcode
    applied on the Panorama K8S plugin" PAN_BUNDLE_TYPE: "CN-X-
   BND2" #Non-mandatory parameters # Recommended to have same
    name as the cluster name provided in Panorama Kubernetes
    plugin - helps with easier identification of pods if managing
    multiple clusters with same Panorama #CLUSTER_NAME: "Cluster-
   name" #PAN_PANORAMA_IP2: "passive-secondary-ip" # Comment
    out to use CERTs otherwise bypass encrypted connection to
    etcd in pan-mgmt. # Not using CERTs for etcd due to EKS bug
    ETCD_CERT_BYPASS: "" # No value needed # Comment out to use
   ```



```
 CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #
 IPSEC_CERT_BYPASS: "" # No values needed
```

Ejemplo de pan-cn-mgmt.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

```
 containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

3. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   kubectl apply -f pan-cn-mgmt-configmap.yaml

   kubectl apply -f pan-cn-mgmt-slot-crd.yaml

   kubectl apply -f pan-cn-mgmt-slot-cr.yaml

   kubectl apply -f pan-cn-mgmt-secret.yaml

   kubectl apply -f pan-cn-mgmt.yaml

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente Crear cuentas de servicio para la autenticación de clúster con un cortafuegos CN-Series.

4. Verifique que los pods CN-MGMT estén activos.

   Tarda unos 5 y 6 minutos.

   Utilice **kubectl get pods -l app=pan-mgmt -n kube-system**

   ```
   NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1 Running 0
   27hpan-mgmt-sts-1 1/1 Running 0 27h
   ```

STEP 7 | Implemente los pods CN-NGFW.

De forma predeterminada, el pod CN-NGFW del plano de datos del cortafuegos se implementa como un DaemonSet. Una instancia del pod CN-NFGW puede proteger el tráfico de hasta 30 pods de aplicaciones en un nodo.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que todos los pods CN-NGFW se están ejecutando. (uno por nodo en su clúster)

   Este es un resultado de muestra de un clúster local de 4 nodos.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

   ```
   NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

   pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>

   pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>

   pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>

   pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
   ```

STEP 8 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 En ejecución
0 27hpan-cni-9j4rs 1/1 En ejecución
0 27hpan-cni-ddwb4 1/1 En ejecución
0 27hpan-cni-fwfrk 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-h57lm 1/1 En ejecución
0 27hpan-cni-j62rk 1/1 En ejecución
0 27hpan-cni-lmxdz 1/1 En ejecución
0 27hpan-mgmt-sts-0 1/1 En ejecución
0 27hpan-mgmt-sts-1 1/1 En ejecución
0 27hpan-ngfw-ds-8g5xb 1/1 En ejecución
27hpan-ngfw-ds-qsrm6 1/1 En ejecución
0 27hpan-ngfw-ds-vqk7z 1/1 En ejecución
0 27hpan-ngfw-ds-zncqg 1/1 En ejecución
```

STEP 9 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

En algunas plataformas, los pods de aplicaciones pueden iniciarse cuando pan-cni no está activo en la cadena del complemento CNI. Para evitar estos escenarios, debe especificar los volúmenes como se muestra aquí en el pod de aplicación YAML.

```
 volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: Directory
```

STEP 10 | Implemente su aplicación en el clúster.

Implementación de la CN-Series desde AWS Marketplace

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

Puede dar licencia a su cortafuegos CN-Series como un servicio de Kubernetes implementado en AWS EKS a través de AWS Marketplace. La CN-Series se puede licenciar por un mes, un año, dos años o tres años e implementarse en EKS 1.19 y posteriores o Redhat Openshift 4.7 y posteriores.

Este producto está en versión preliminar.

El uso de esta licencia requiere que actualice la política de IAM adjunta al nodo de trabajo de Kubernetes.

Si utiliza una licencia PAYG adquirida a través de AWS Marketplace para su implementación de CN-Series, no añada un código de autorización al complemento Panorama para Kubernetes.

STEP 1 | Complete los siguientes requisitos previos.

1. Cree su clúster EKS o Redhat OpenShift.
2. Implemente Panorama e instale el complemento de Kubernetes.

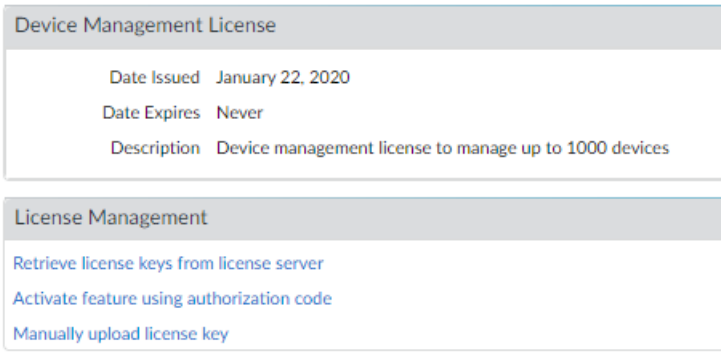
   Omita estos pasos si ya tiene una instancia de Panorama con licencia implementada en AWS.

   1. Instalar Panorama en una instancia Amazon EC2.
   2. Instale el complemento Kubernetes para CN-Series.
   3. Una vez que Panorama esté instalado, envíe un correo electrónico al equipo de CN-Series a **cn-series-aws-marketplace@paloaltonetworks.com** para solicitar una licencia para su Panorama. Incluya su nombre completo, correo electrónico de la empresa, nombre de la empresa, número de pedido de compra, nombre de cuenta de AWS e ID de cuenta de AWS.

STEP 2 | Aplique su número de serie y licencia a Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** y haga clic en el icono de edición .
3. Introduzca el **Serial Number (Número de serie)** de Panorama (incluido en el correo electrónico de procesamiento del pedido) y haga clic en **OK (Aceptar)**.
4. Seleccione **Panorama** > **Licenses (Licencias).**
5. Haga clic en **Activate feature using authorization code (Activar la funcionalidad mediante código de autorización)**.
6. Introduzca el código de autorización de licencia de gestión del cortafuegos y haga clic en **OK (Aceptar)** para activar la licencia.
7. Verifique que la licencia de gestión de cortafuegos está activada.

   Ahora debe aparecer la sección Device Management License (Licencia de gestión de dispositivos) con la fecha de emisión, la fecha de vencimiento y la descripción.



STEP 3 | Actualice las políticas de IAM y adjunte la política al nodo de trabajo de Kubernetes.

1. Inicie sesión en la Consola de administración de AWS y abra la consola IAM.
1. Seleccione **Policies (Políticas)**.
2. En la lista de políticas, seleccione **AWSLicenseManagerConsumptionPolicy** y **AWSMarketplaceMeteringRegisterUsage**.
3. Seleccione **Actions (Acciones)** y a continuación, elija **Attach (Adjuntar)**.
4. Seleccione la identidad del nodo de trabajo al que desea adjuntar la política. Después de seleccionar la identidad, haga clic en **Attach policy (Adjuntar política)**.

STEP 4 | Descargue el **`plugin-serviceaccount.yaml`** y aplique el yaml antes de implementar los gráficos de Helm.

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

STEP 5 | Acceda a AWS Marketplace y localice la lista. de **CN-Series for AWS Marketplace (CN-Series para AWS Marketplace)**.

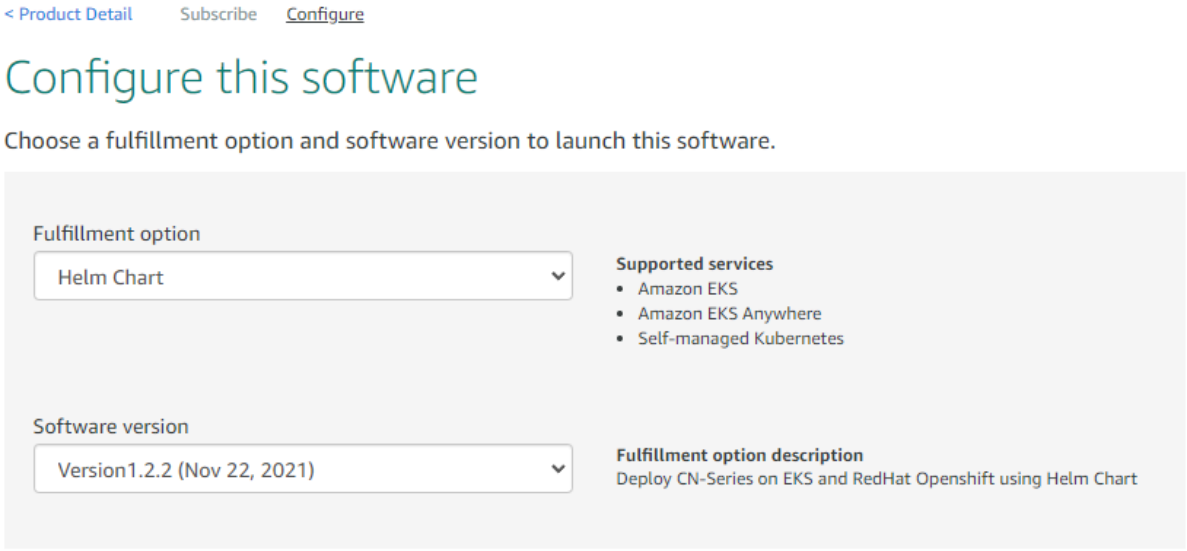
STEP 6 | Haga clic en **Continue to Subscribe (Continuar para suscribirse)**.

STEP 7 | Introduzca el número de licencias que desea comprar. Cada derecho de licencia es equivalente a una vCPU utilizada por su implementación de CN-Series.

Consulte Requisitos del sistema de la CN-Series y Rendimiento y escalado de la CN-Series para obtener orientación sobre el número de vCPU necesarias para satisfacer las necesidades de la implementación.

STEP 8 | Haga clic en **Continue to Configuration (Continuar a la configuración)**. Esto añade las licencias a su cuenta de AWS.

1. Seleccione **Helm Chart (Gráfico Helm)** como la **Fulfillment option (Opción de cumplimiento)**.
2. Seleccione la versión más reciente para **Software version (Versión de software)**.



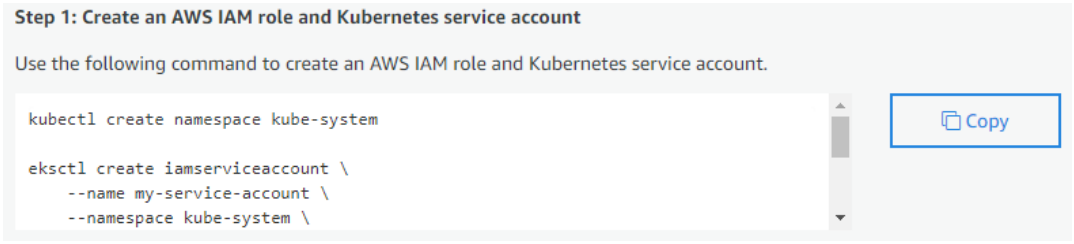
STEP 9 | Haga clic en **Continue to Launch (Continuar para iniciar)**.

1. Seleccione su **Launch target (Destino de lanzamiento)**:**Amazon-managed Kubernetes (Kubernetes gestionado por Amazon)** o **Self-managed Kubernetes (Kubernetes autogestionado)**. El modo autogestionado se implementa en Redhat OpenShift.
2. Siga las **Launch Instruction (Instrucciones de lanzamiento)** se muestran en la lista de AWS Marketplace. Las instrucciones difieren según el objetivo de lanzamiento.

   - **Kubernetes gestionado por Amazon**

     1. Copie los comandos del **Step 1 (Paso 1)** de las **Launch instructions (Instrucciones de inicio)**.
     2. Actualice los comandos copiados para añadir el nombre del clúster.

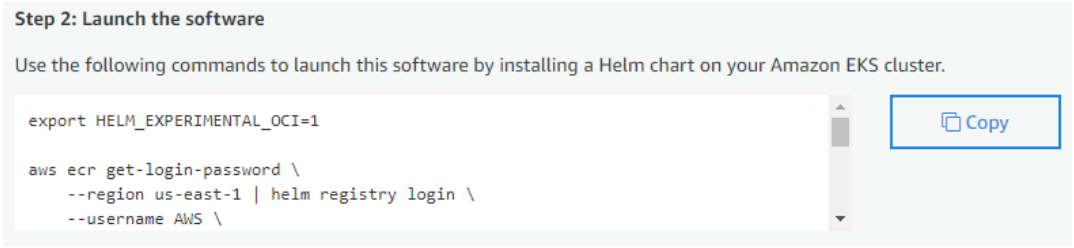
        `--cluster <ENTER_YOUR_CLUSTER_NAME_HERE>`
     3. Ejecute el comando copiado en el clúster de EKS.

     4. Copie los comandos del gráfico Helm del **Step 2 (Paso 2)** de las **Launch instructions (Instrucciones de inicio)**.
     5. Actualice la información de instalación de Helm para incluir su IP de Panorama, clave de autenticación de Panorama, nombre de grupo de dispositivos, nombre de pila de plantilla y nombre de grupo de recopilación. Establezca el **`cluster.deployTo`** en **`eks`**.

        ```
        helm install cn-series-helm \ --namespace kube-system ./
        awsmp-chart/* \ --set serviceAccount.create=false
         \ --set serviceAccount.name=my-service-
        account \ --set cluster.deployTo=eks \ --set
         panorama.ip=Panorama-IP \ --set panorama.ip2=Panorama-
        IP2 \ --set panorama.authKey=000xxxxxxx
         \ --set panorama.deviceGroup=Panorama-DG
         \ --set panorama.template=Panorama-TS \
        ```

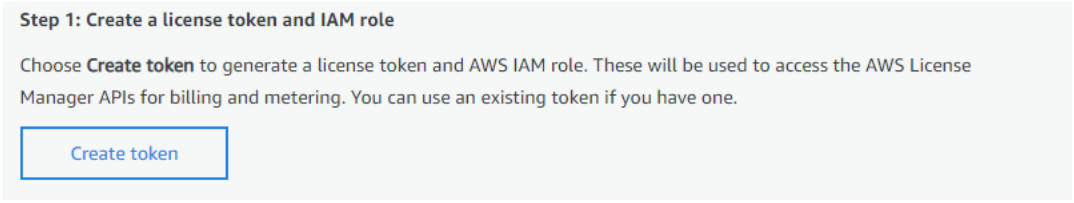
```
--set panorama.cgName=Panorama-CG \ --set
imagePullSecrets=awsmp-image-pull-secret
```



6. Ejecute el comando de instalación helm en el clúster de EKS después de actualizar los valores enumerados anteriormente.

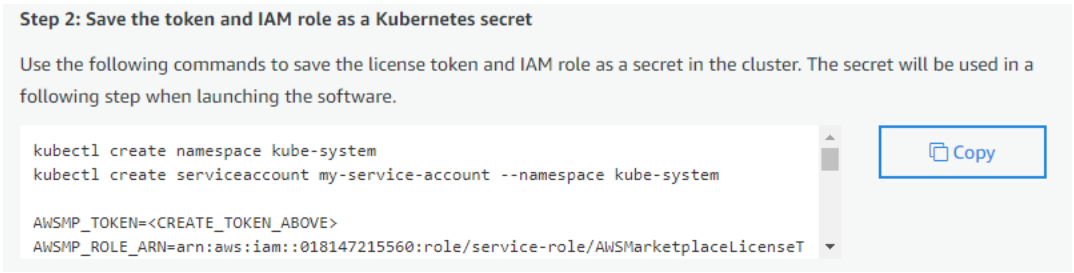
- **Kubernetes autogestionado**

1. Complete el Paso 1 de las instrucciones de inicio para crear un token de licencia y una función de IAM.



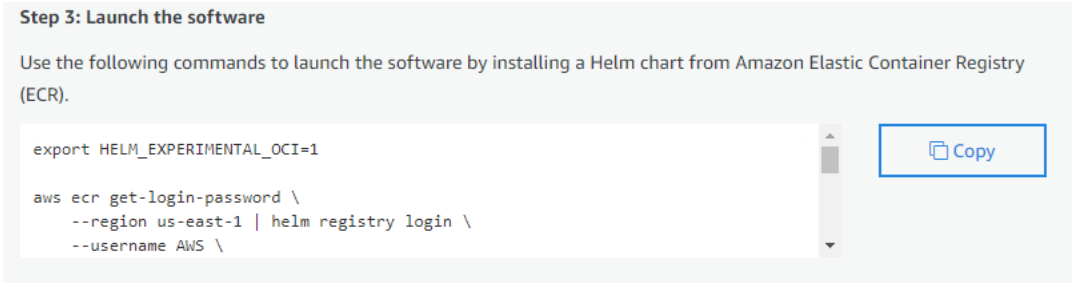
2. Copie los comandos del **Step 2 (Paso 1)** de las **Launch instructions (Instrucciones de inicio)**.
3. Actualice los comandos copiados para añadir el valor del token.

   `AWSMP_TOKEN=<CREATE_TOKEN_ABOVE>`
4. Ejecute el comando copiado en el clúster de OpenShift.



5. Copie los comandos del gráfico Helm del **Step 3 (Paso 3)** de las **Launch instructions (Instrucciones de inicio)**.
6. Actualice la información de instalación de Helm para incluir su IP de Panorama, clave de autenticación de Panorama, nombre de grupo de dispositivos, nombre de pila de plantilla y nombre de grupo de recopilación. Establezca **`cluster.deployTo`** en **`openshift`**.

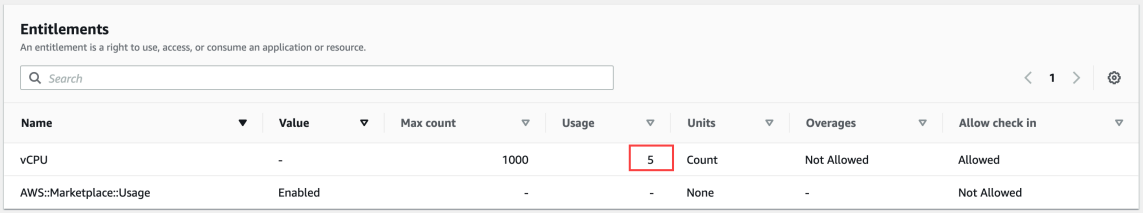
```
helm install cn-series-helm \ --namespace kube-system ./
awsmp-chart/* \ --set serviceAccount.create=false
 \ --set serviceAccount.name=my-service-account
 \ --set cluster.deployTo=eks|openshift \ --set
 panorama.ip=Panorama-IP \ --set panorama.ip2=Panorama-
IP2 \ --set panorama.authKey=000xxxxxxx
 \ --set panorama.deviceGroup=Panorama-DG
 \ --set panorama.template=Panorama-TS \
 --set panorama.cgName=Panorama-CG \ --set
 imagePullSecrets=awsmp-image-pull-secret
```



7. Ejecute el comando de instalación helm en el clúster de OpenShift después de actualizar los valores enumerados anteriormente.

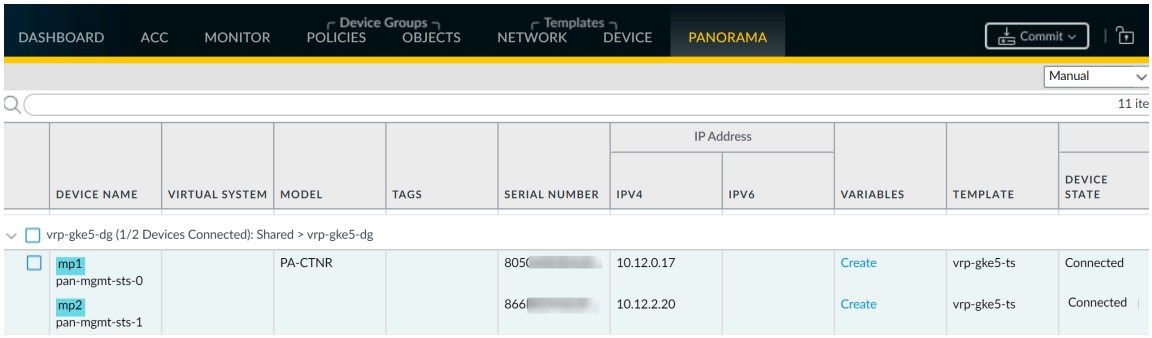
STEP 10 | Compruebe que la licencia se ha añadido correctamente a su cuenta.

1. Vaya a AWS License Manager.
2. Seleccione **Granted Licenses (Licencias concedidas)** y busque la lista de CN-Series para AWS Marketplace.
3. En **Entitlements (Derechos)**, puede ver el número total de licencias y el número de licencias consumidas.

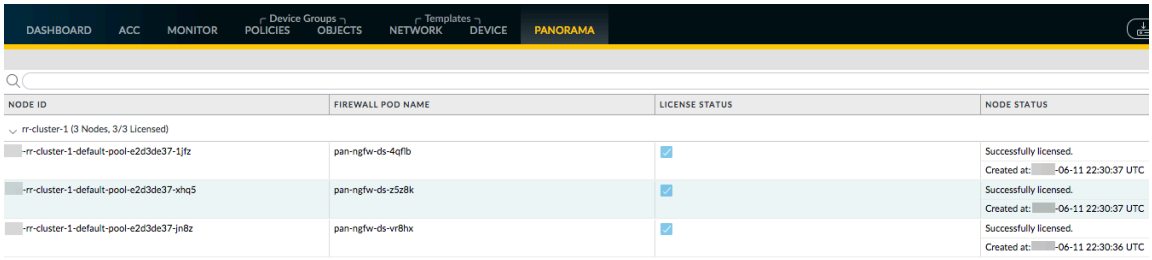


STEP 11 | Compruebe que los cortafuegos CN-Series aparecen en Panorama.

1. Inicie sesión en Panorama.
2. Para ver los pods CN-MGMT, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.



3. Para comprobar que los pods CN-NGFW tienen licencia, seleccione **Panorama** > **Plugins (Complementos)** > **Kubernetes** > **License Usage (Uso de la licencia)** y compruebe que a cada pod se le ha asignado un token de licencia.



Implementación del cortafuegos CN-Series como un servicio de Kubernetes en AliCloud (ACK)

¿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 la versión PAN-OS 10.2.x

Después de revisar los componentes básicos de la serie CN-Series y la descripción general de alto nivel del flujo de trabajo en Protección de las cargas de trabajo de Kubernetes con CN-Series, puede comenzar a implementar el cortafuegos CN-Series en la plataforma AliCloud ACK para proteger el tráfico entre contenedores dentro del mismo clúster, así como entre contenedores y otros tipos de carga de trabajo, como máquinas virtuales y servidores bare-metal.

Debe asegurarse de aplicar el archivo `plugin-serviceaccount.yaml`. Para obtener más información, consulte Crear cuenta de servicio para la autenticación de clúster.

- *Cuando implementa el cortafuegos CN-Series como un servicio de Kubernetes ACK,* `pan-plugin-cluster-mode-secret` *debe estar presente.*

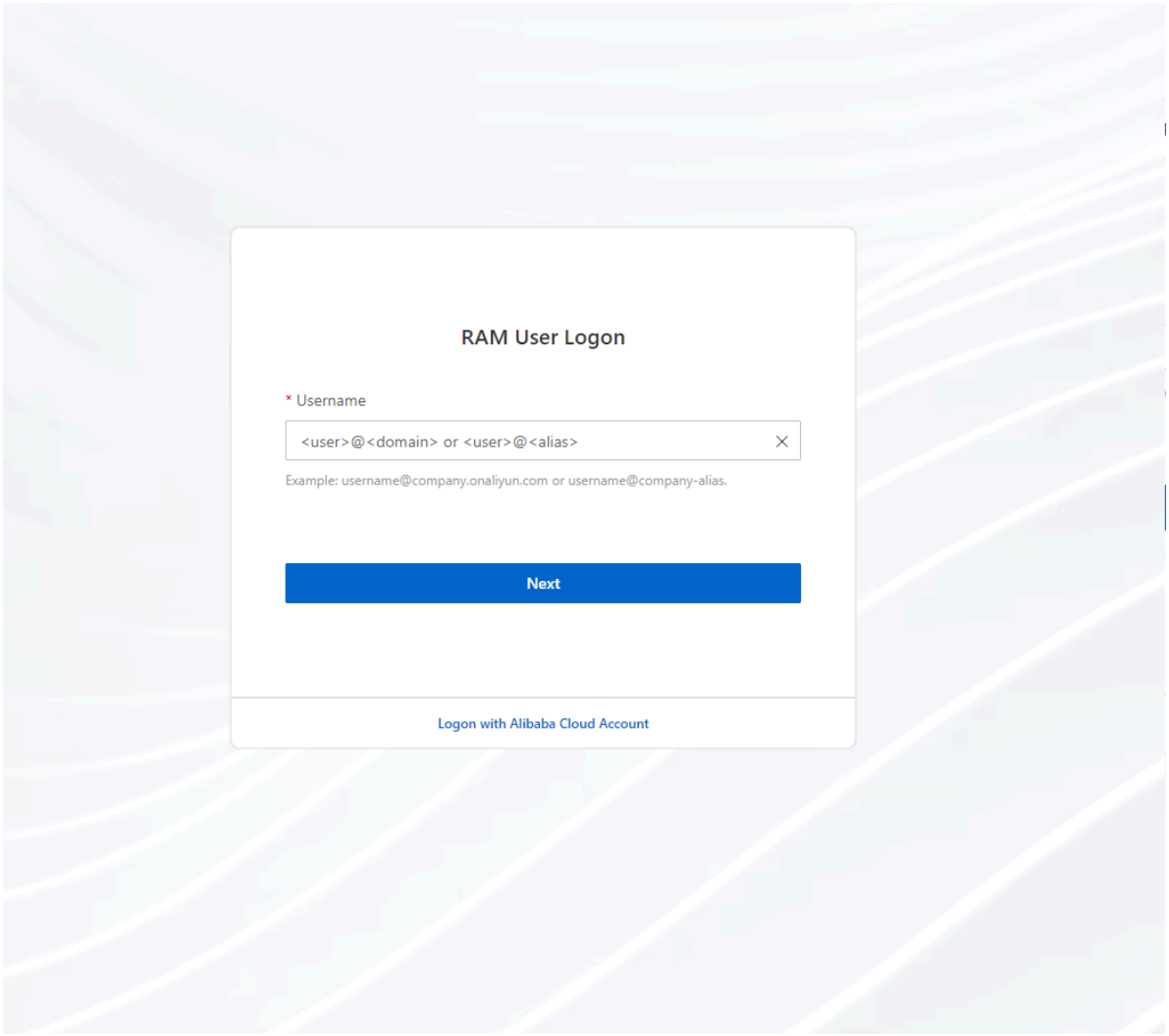
Antes de comenzar, asegúrese de que la versión del archivo YAML de la serie CN-Series sea compatible con la versión de PAN-OS. Para obtener más información, consulte YALM de CN-Series.

Complete el siguiente procedimiento para implementar el cortafuegos CN-Series como un servicio de Kubernetes en la plataforma ACK.

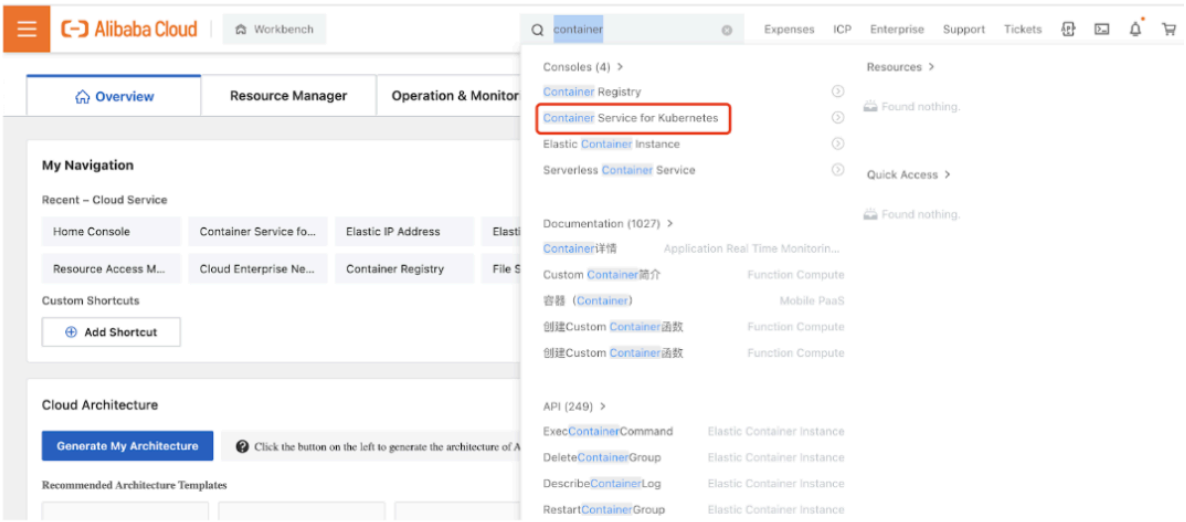
STEP 1 | Configure su clúster de Kubernetes.

Para crear un clúster en ACK, haga lo siguiente:

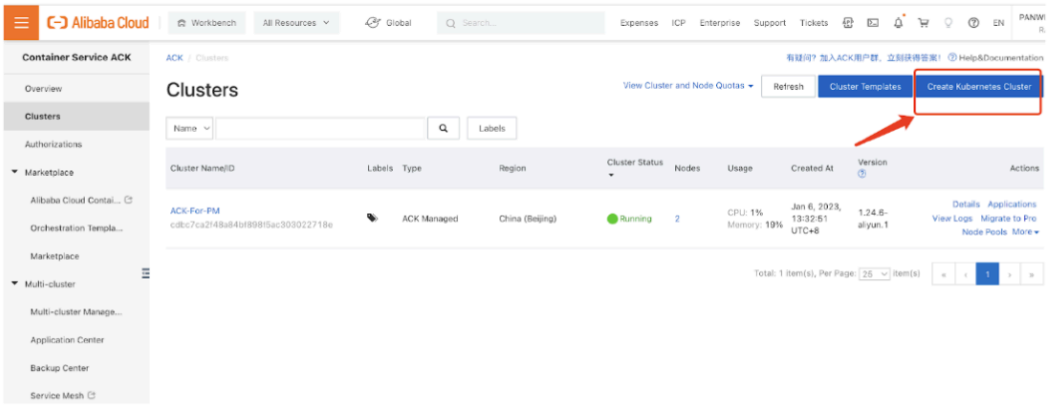
1. Inicie sesión en el Inicio de sesión de usuario de RAM con sus credenciales de inicio de sesión de RAM.



2. En la barra de navegación superior, seleccione la región donde desea crear un clúster y seleccione un grupo de recursos en función de sus requisitos empresariales.
   - La región de un clúster no se puede cambiar después de crear el clúster.
   - Todos los grupos de recursos de tu cuenta se muestran de forma predeterminada.
3. Busque **Servicio de contenedores para Kubernetes** en el menú de la barra de búsqueda.



4. Haga clic en **Crear clúster de Kubernetes**.

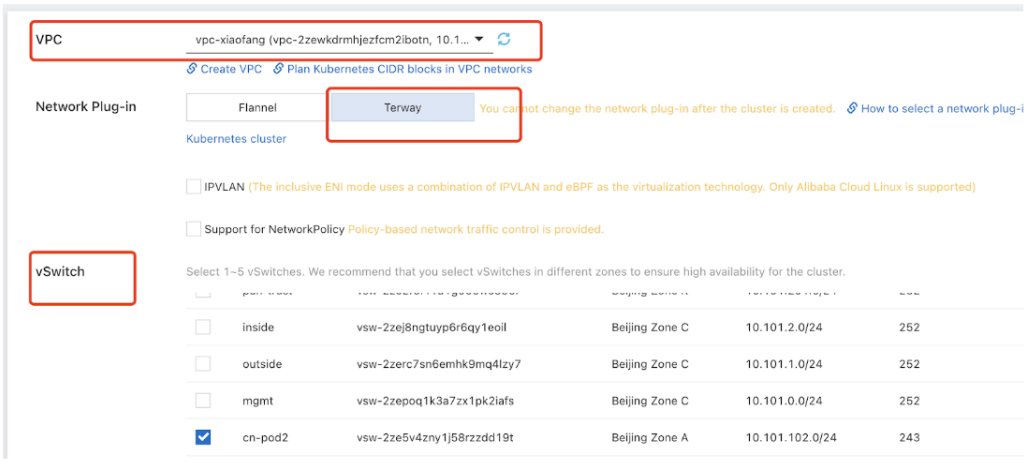


5. Para crear un clúster, debe configurar parámetros de software, parámetros de hardware y parámetros básicos según las instrucciones del asistente. Para obtener más información sobre la configuración

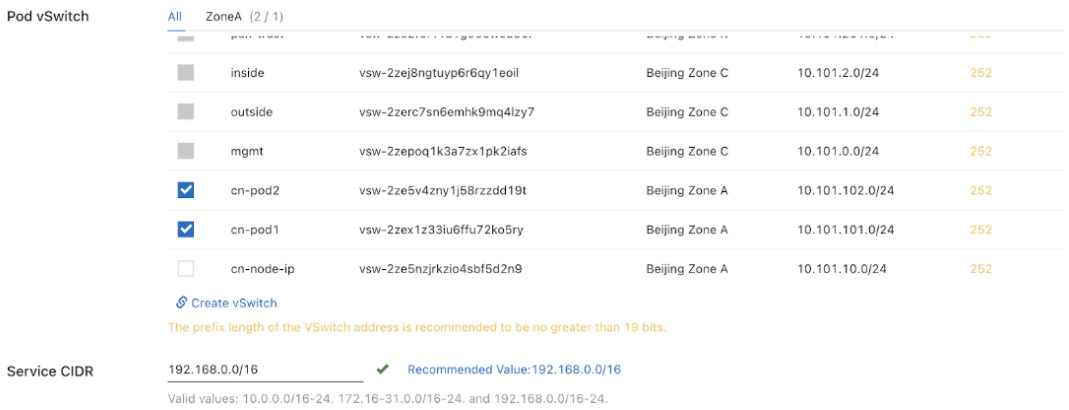
de estos parámetros necesarios, consulte Crear un clúster en ACK. Los siguientes pasos representan un ejemplo de una creación de clúster en la plataforma ACK:

CN-Series en Alibaba cloud ACK solo es compatible con el complemento Terway Network.

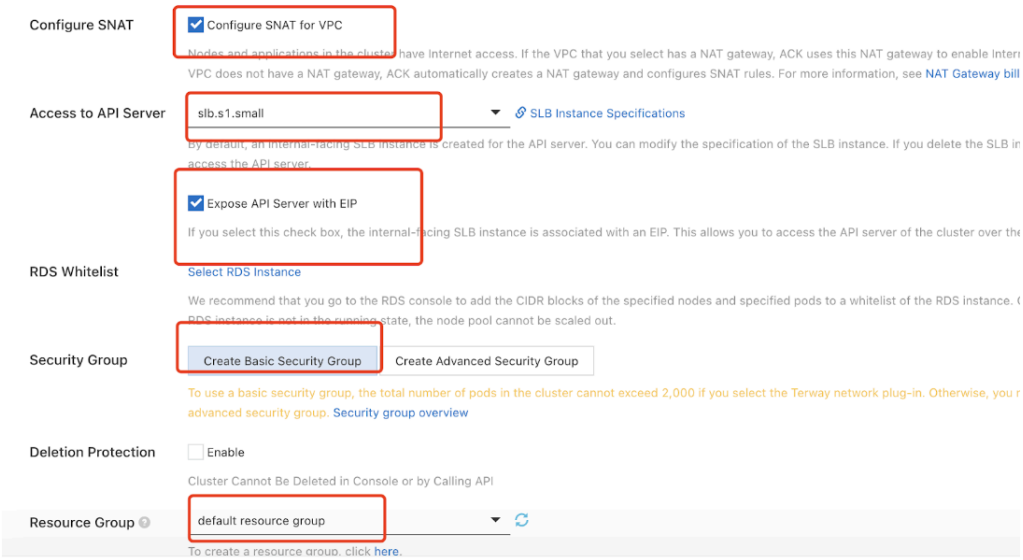
- Seleccione **VPC, complemento de red** y **vSwitch**.



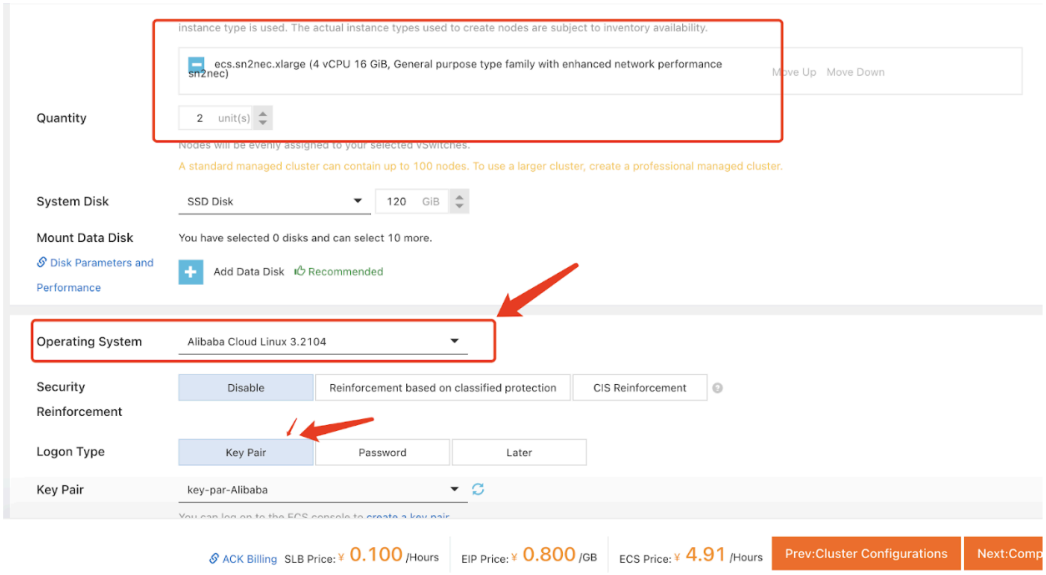
- Seleccione **POD v Switch**.



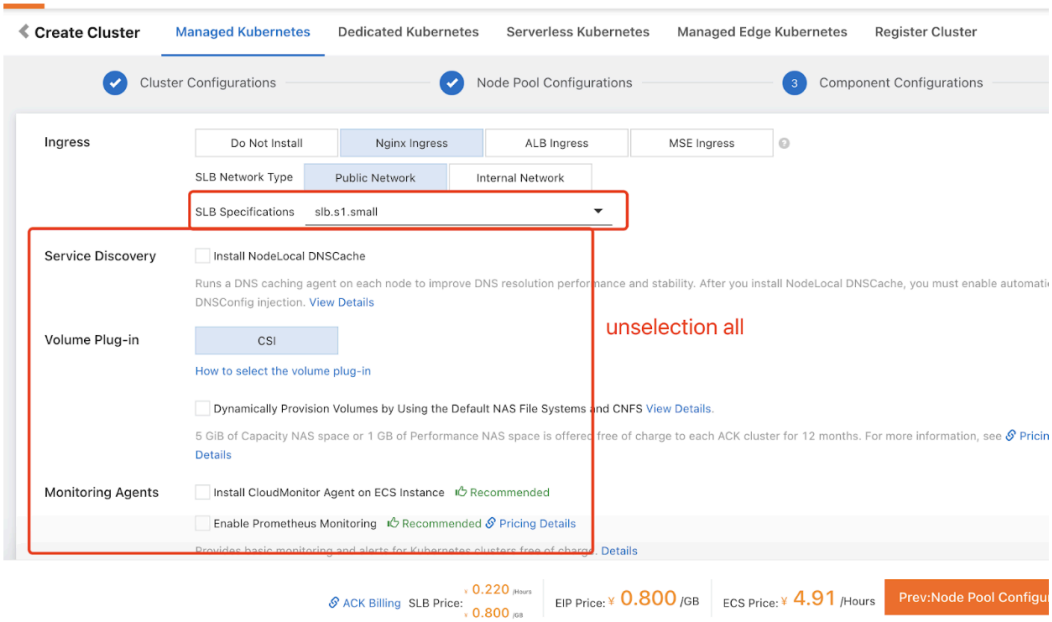
- Seleccione **Configurar SNAT, Acceso al servidor API, Grupos de seguridad** y **Grupo de recursos**.



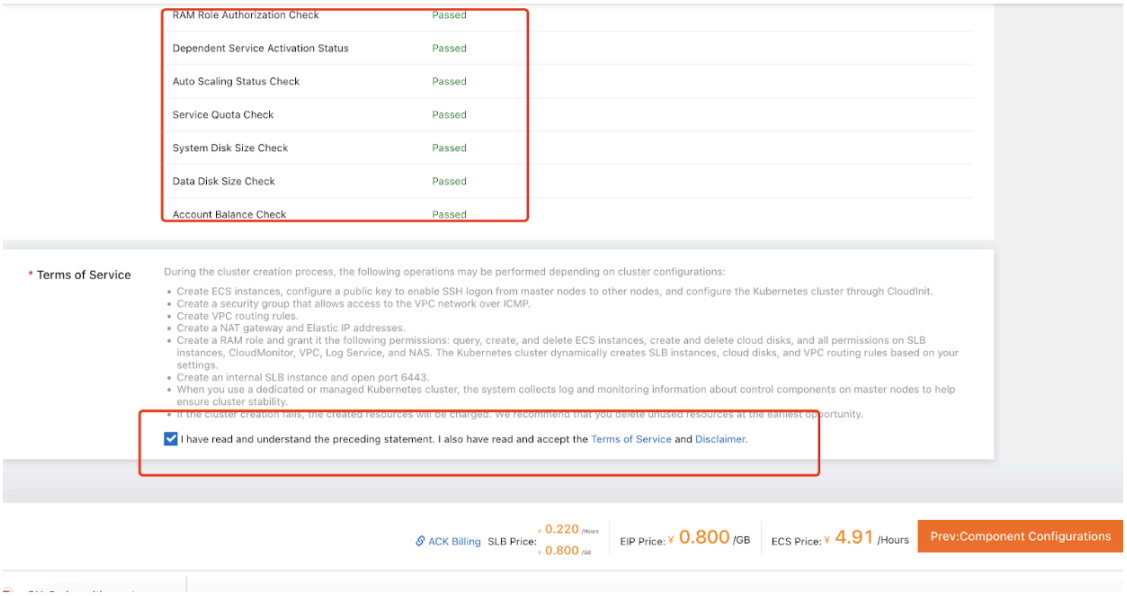
- Seleccione **Cantidad, Sistema operativo** y **Tipo de inicio de sesión** para las configuraciones del grupo de nodos.



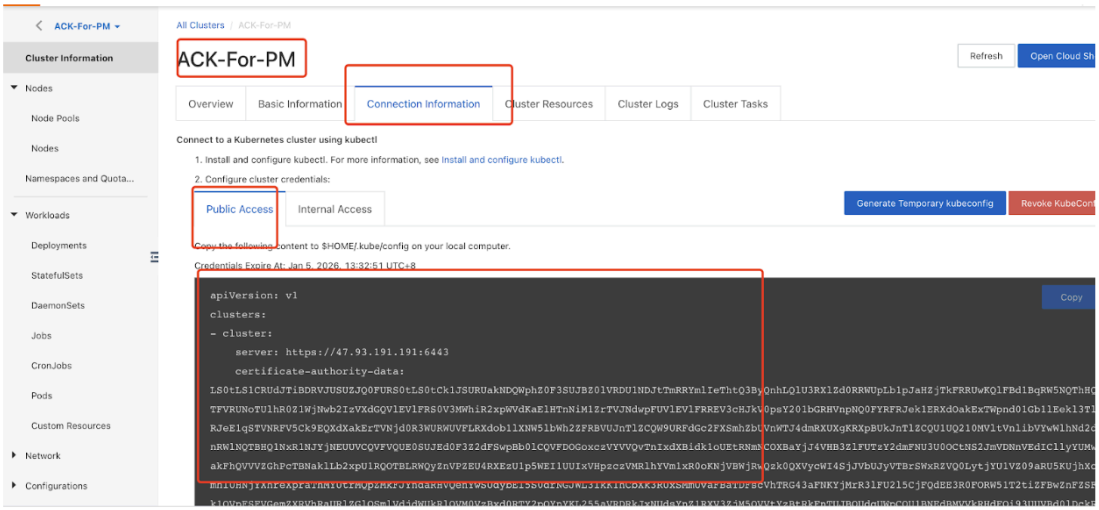
- Vaya a la **pestaña de Red pública**, desactive la casilla de verificación **Descubrimiento de servicios, Complemento de volumen** y la casilla **Agentes de supervisión**.



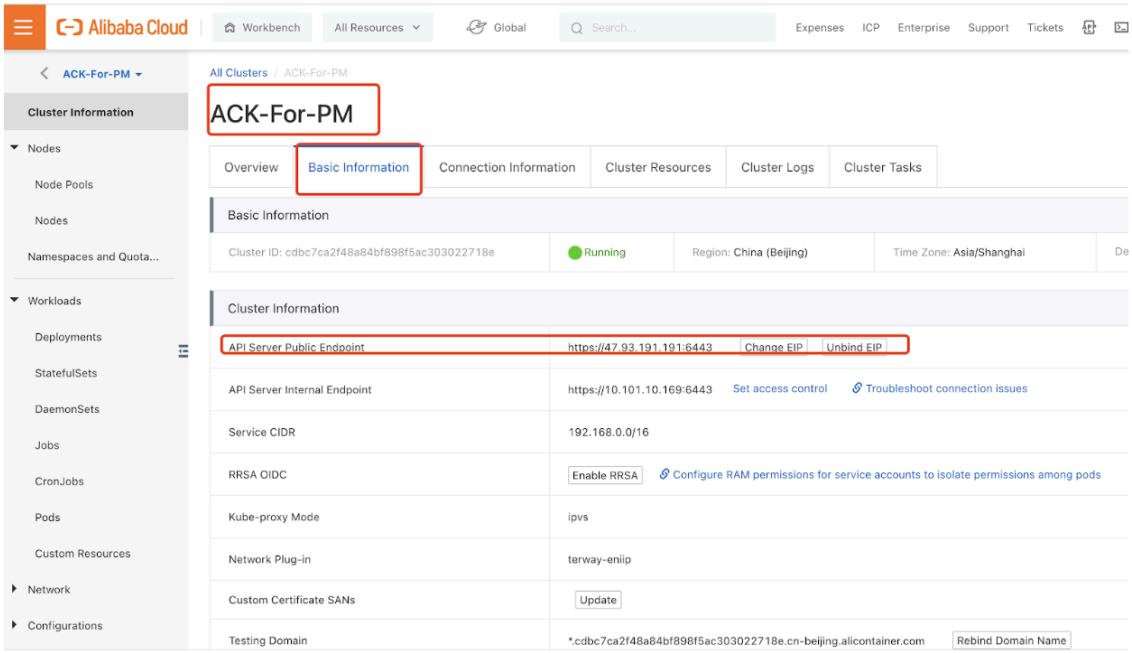
6. Seleccione la casilla **Condiciones de servicio**.

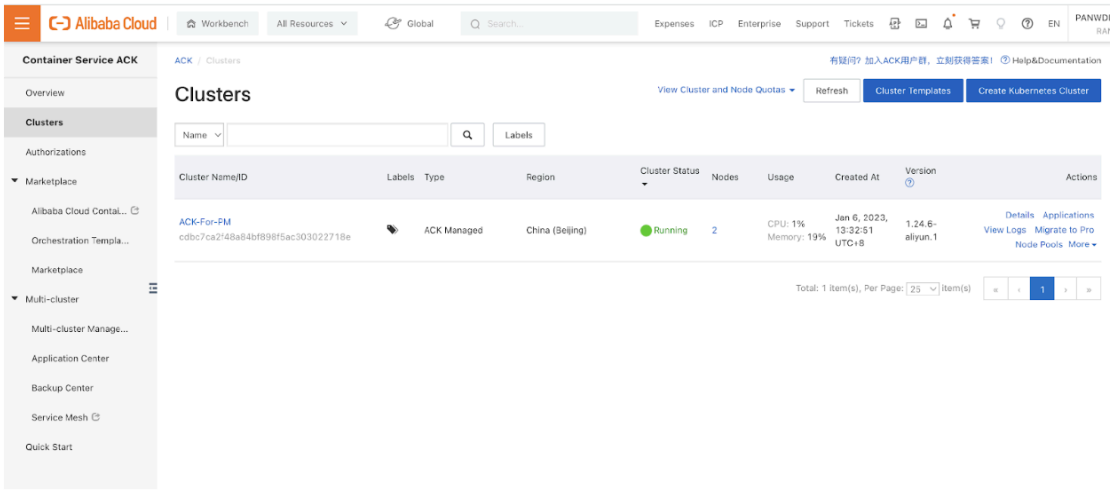


7. Haga clic en **Crear clúster**.
8. Compruebe la clave del servidor API para iniciar sesión en el clúster ACK y copie el contenido siguiente a `$HOME/.kube/config` en el equipo local.



9. Obtenga la dirección del endpoint público del servidor API del clúster ACK.





Verifique que el clúster tenga los recursos adecuados. La especificación predeterminada del grupo de nodos de GKE no es adecuada para el cortafuegos CN-Series. Debe asegurarse de que ese clúster tenga los recursos de Requisitos previos del modelo CN-Series compatibles con el cortafuegos.

`kubectl get nodes`

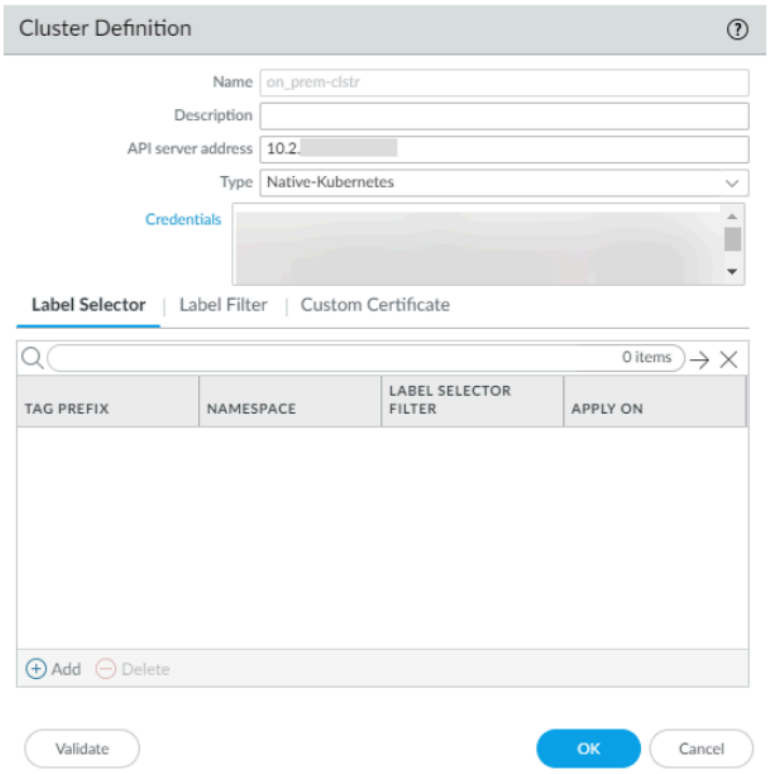
`kubectl describe node <node-name>`

Vea la información bajo el encabezado Capacidad en la salida del comando para ver la CPU y la memoria disponibles en el nodo indicado.

La asignación de CPU, memoria y almacenamiento en disco dependerá de sus necesidades. Consulte Rendimiento y ampliación de la CN-Series.

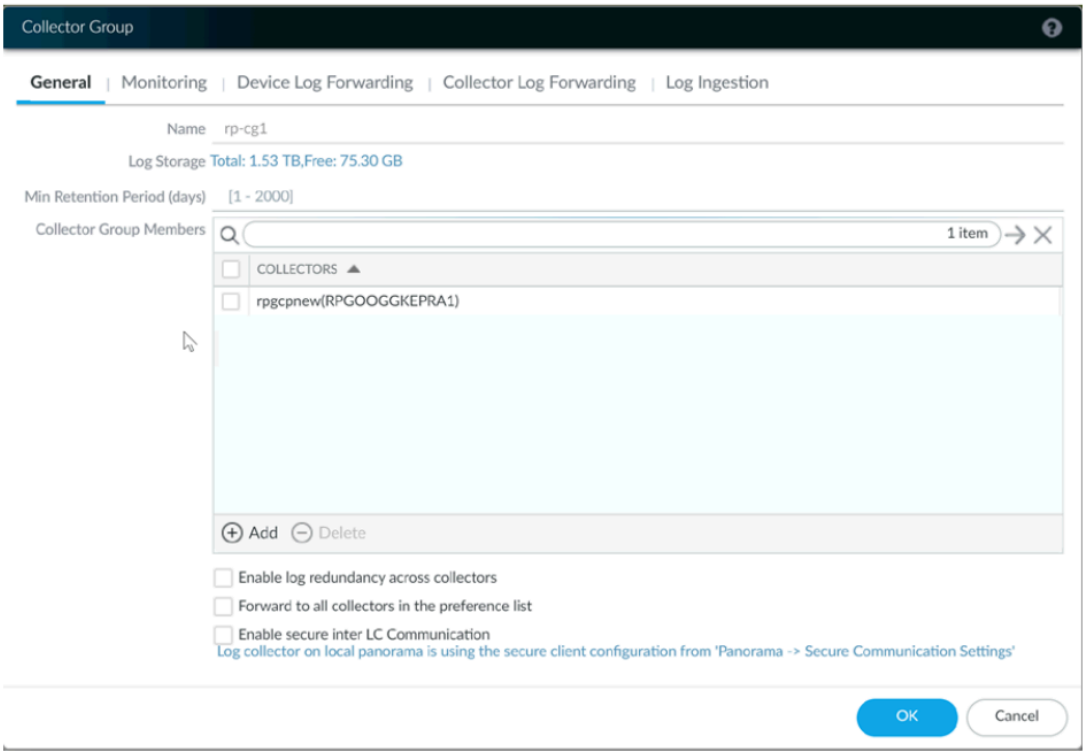
Debe asegurarse de tener la siguiente información:

- Recopile la dirección IP del endpoint para configurar el servidor API en Panorama.



  Panorama utiliza esta dirección IP para conectarse a su clúster de Kubernetes.

- Recopile el nombre de la pila de plantillas, el nombre del grupo de dispositivos, la dirección IP de Panorama y, opcionalmente, el Nombre del grupo del recopilador de registros de Panorama.



Para obtener más información, consulte Crear un grupo de dispositivos primario y una pila de plantillas.

- Recopile la Clave de autenticación de VM y el valor y el ID del PIN de registro automático.
- La ubicación del repositorio de imágenes del contenedor en el que descargó las imágenes.

STEP 2 | (opcional) Si configuró un certificado personalizado en el complemento de Kubernetes para Panorama, debe crear el secreto del certificado ejecutando el siguiente comando. No cambie el nombre del archivo de ca.crt. El volumen de certificados personalizados en pan-cn-mgmt.yaml y pan-cn-ngfw.yaml es opcional.

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | Edite los archivos YAML para proporcionar los detalles necesarios para implementar los cortafuegos CN-Series.

```
apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-config namespace: kube-system data: PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings
 PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-template-stack>"
 PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8s-service"
```

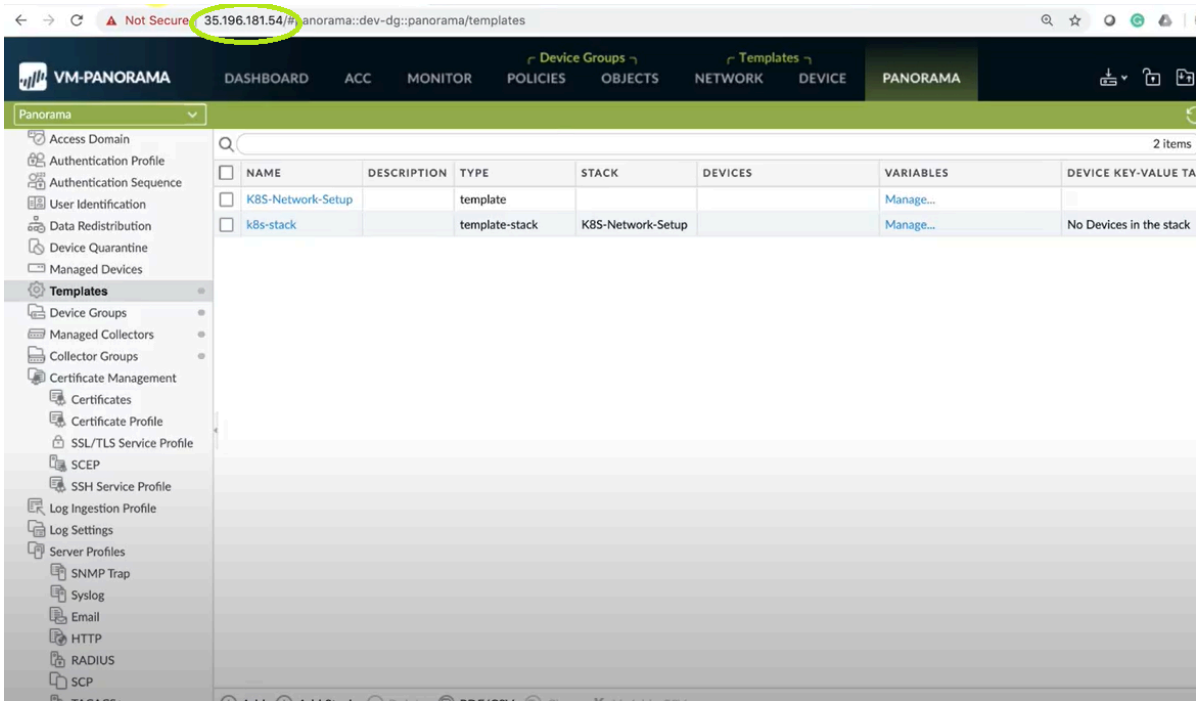
```
apiVersion: v1 kind: Secret metadata: name: pan-mgmt-secret
 namespace: kube-system type: Opaque stringData: # Panorama Auth
```



```
  Key PAN_PANORAMA_AUTH_KEY: "<panorama-auth-key>" # Thermite
```

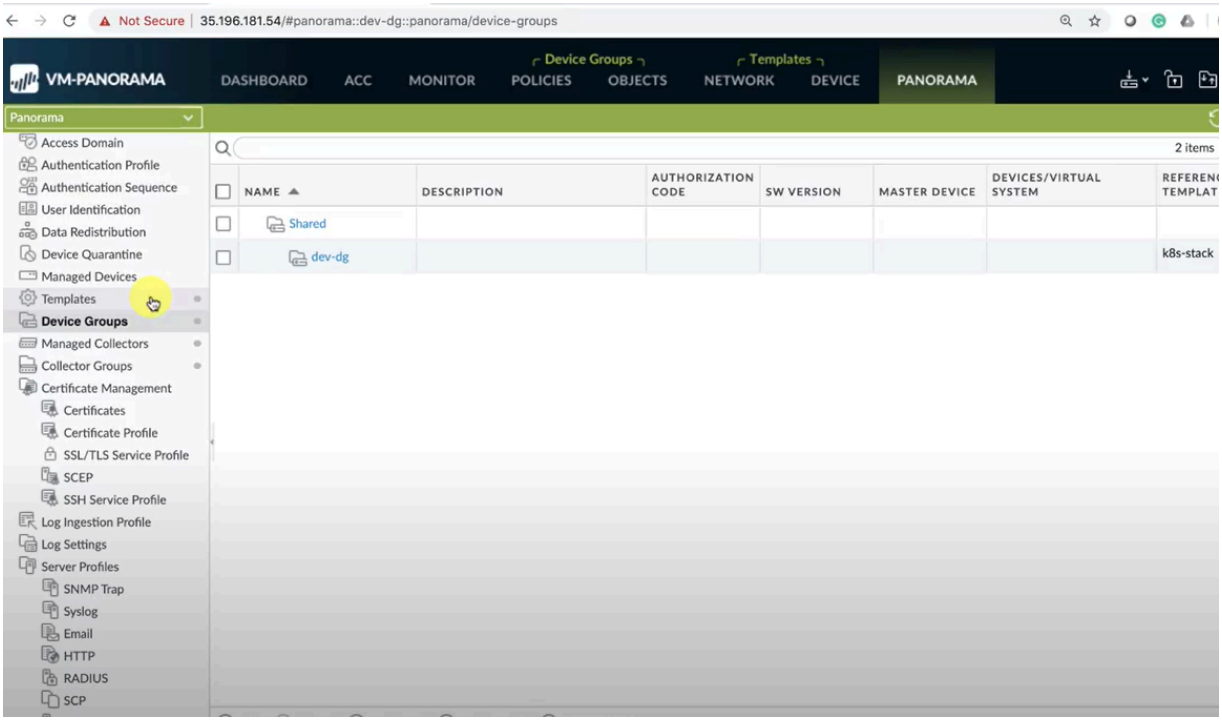
```
Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN
Id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<PIN-Value>"
```

Debe asegurarse de que el valor del parámetro `PAN_PANORAMA_IP` en su archivo YAML coincida con su dirección IP de Panorama real, como se muestra en el siguiente diagrama:

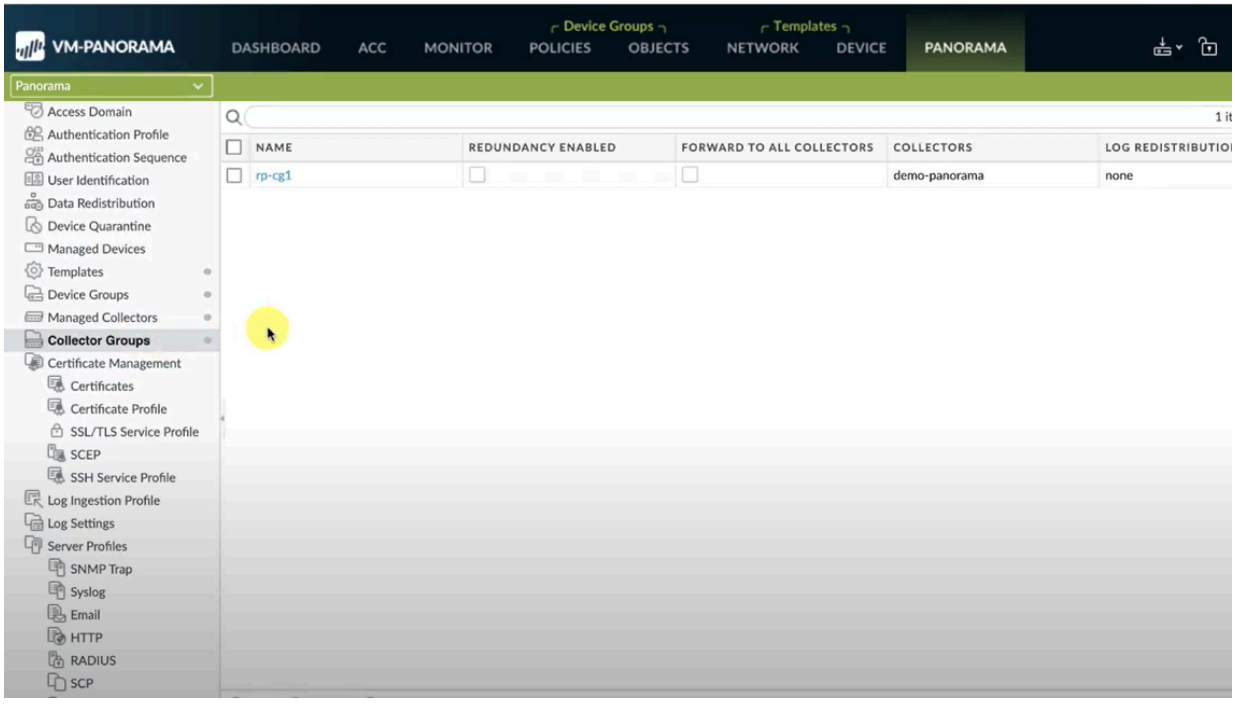


La última versión de los archivos YAML está disponible en el Repositorio para la seguridad de Kubernetes de Palo Alto Networks - CN Series*. Puede seleccionar las ramas o etiquetas más recientes en el menú desplegable* ***Switch*** *(Cambiar)* ***branches/tags*** *(ramas/etiquetas).*

Debe asegurarse de que el valor del parámetro de `PAN_DEVICE_GROUP` y `PAN_TEMPLATE` en su archivo YAML coincida con el nombre del grupo de dispositivos y la pila de plantillas que creó en Panorama, como se muestra en el siguiente diagrama:



Debe asegurarse de que el valor del parámetro de `PAN_PANORAMA_CG_NAME` sea el mismo que el nombre del colector de logs que creó.



Para obtener más información, consulte parámetros editables para archivos yaml de CN-Series.

STEP 4 | Implemente el servicio CN-NGFW. Realice los siguientes pasos:

Cuando se implementa como un servicio de Kubernetes, las instancias de CN-NGFW se pueden implementar en nodos de seguridad y el tráfico de pods de aplicaciones se redirige a una instancia CN-NGFW disponible para su inspección y aplicación.

1. Verifique que ha creado la cuenta de servicio con pan-cni-serviceaccount.yaml.

   Consulte Creación de cuenta de servicio para la autenticación de clúster.

2. Utilice Kubectl para ejecutar pan-cni-configmap.yaml.

   `kubectl apply -f pan-cni-configmap.yaml`

3. Utilice kubectl para ejecutar pan-cn-ngfw-svc.yaml.

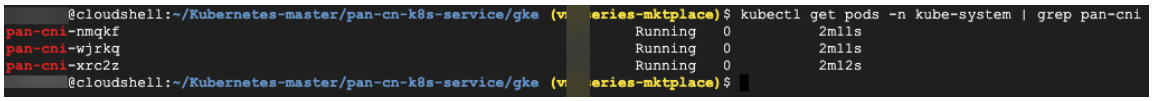
   `kubectl apply -f pan-cn-ngfw-svc.yaml`

   Este yaml debe implementarse antes de pan-cni.yaml.

4. Utilice Kubectl para ejecutar pan-cni.yaml.

   `kubectl apply -f pan-cni.yaml`

5. Verifique que haya modificado los archivos pan-cni-configmap y pan-cni YAML.
6. Ejecute el siguiente comando y verifique que su resultado sea similar al siguiente ejemplo.



Alicloud ACK solo es compatible con el escalado automático basado en métricas estándar.

STEP 5 | Implemente el StatefulSet de CN-MGMT.

De forma predeterminada, el plano de gestión se implementa como StatefulSet que proporciona tolerancia a fallos. Es posible conectar hasta 30 pods CN-NGFW de cortafuegos a un StatefulSet de CN-MGMT.

1. (Requerido solo para los volúmenes persistentes aprovisionados estáticamente) Implemente los volúmenes persistentes (PV) para el StatefulSet de CN-MGMT.

   1. Cree los directorios para que coincidan con los nombres de los volúmenes locales definidos en pan-cn-pv-local.yaml.

   Necesita seis (6) directorios en al menos 2 nodos de trabajo. Inicie sesión en cada nodo de trabajo en el que se implementará el StatefulSet de CN-MGMT para crear los directorios.

Por ejemplo, para crear directorios llamados `/mnt/pan-local1` a `/mnt/pan-local6`, utilice el comando a continuación:

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. Modifique pan-cn-pv-local.yaml.

   Haga coincidir el nombre de host en `nodeaffinity` y verifique que haya modificado los directorios que creó anteriormente en `spec.local.path`, luego implemente el archivo para crear una nueva clase de almacenamiento pan-local-storage y volúmenes persistentes locales.

   *En el archivo `pan-cn-mgmt.yaml` debe agregar el nombre de la clase de almacenamiento como `alicloud-disk disponible` al crear **volumeClaimTemplates**.*

   Por ejemplo:

   ```
   storageClassName: alicloud-disk-available
   ```

   El tamaño de almacenamiento debe ser como mínimo de 20G para todos los PV.

2. Verifique que haya modificado los archivos pan-cn-mgmt-configmap y pan-cn-mgmt YAML.

   Ejemplo de pan-cn-mgmt.yaml

   ```
   initContainers: - name: pan-mgmt-init image: <your-private-
   registry-image-path>
   ```

   ```
    containers: - name: pan-mgmt image: <your-private-registry-
   image-path> terminationMessagePolicy: FallbackToLogsOnError
   ```

3. Utilice Kubectl para ejecutar archivos pan-cni.yaml.

   `kubectl apply -f pan-cn-mgmt-configmap.yaml`

   `kubectl apply -f pan-cn-mgmt-slot-crd.yaml`

   `kubectl apply -f pan-cn-mgmt-slot-cr.yaml`

   `kubectl apply -f pan-cn-mgmt-secret.yaml`

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

   Debe ejecutar pan-mgmt-serviceaccount.yaml, solo si no ha completado previamente Crear cuenta de servicio para la autenticación de clúster.

4. Verifique que los pods CN-MGMT estén activos ejecutando el siguiente comando:

   `kubectl get pods -l app=pan-mgmt -n kube-system`

   Tarda unos 5 y 6 minutos.

STEP 6 | Implemente los pods CN-NGFW.

1. Compruebe que haya modificado los archivos YAML como se detalla en PAN-CN-NGFW-CONFIGMAP y PAN-CN-NGFW.

   containers: - name: pan-ngfw-container image: <your-private-registry-image-path>

2. Utilice Kubectl apply para ejecutar pan-cn-ngfw-configmap.yaml.

   kubectl apply -f pan-cn-ngfw-configmap.yaml

3. Utilice Kubectl apply para ejecutar pan-cn-ngfw.yaml.

   kubectl apply -f pan-cn-ngfw.yaml

4. Compruebe que los pods CN-NGFW se están ejecutando.

   kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 7 | Compruebe que puede ver CN-MGMT, CN-NGFW y PAN-CNI en el clúster de Kubernetes.

kubectl -n kube-system get pods

STEP 8 | Anote el yaml de la aplicación o el espacio de nombres para que el tráfico de sus nuevos pods se redirija al cortafuegos.

Debe añadir la siguiente anotación para redirigir el tráfico al CN-NGFW para su inspección:

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

Por ejemplo, para todos los nuevos pods en el espacio de nombres "predeterminado":

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

STEP 9 | Implemente su aplicación en el clúster.

Implementación del CN-Series en OpenShift

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series en entorno OpenShift	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior

El pan-cni protege el tráfico en la interfaz predeterminada "eth0" del pod de la aplicación. Si tiene pods de múltiples hosts, puede configurar el pod CN-NGFW para proteger interfaces adicionales que están configuradas con una conexión basada en puente para comunicarse con otros pods o el host. Dependiendo de la anotación en la aplicación YAML, puede configurar el cortafuegos CN-Series para inspeccionar el tráfico de todas las interfaces o una cantidad seleccionada de interfaces adjuntas a cada pod.

El pan-cni no crea ninguna red y, por lo tanto, no necesita direcciones IP como otros complementos CNI.

*Se requiere PAN-OS 10.1.3 o posterior para implementar la serie CN-Series como servicio de Kubernetes en OpenShift. Además, la serie CN-Series como servicio de Kubernetes en OpenShift solo protege la interfaz **eth0**.*

STEP 1 | Implemente su clúster.

Consulte la documentación del proveedor de la plataforma en la nube y verifique que las versiones de OpenShift y CNI sean compatibles con la serie CN-Series. Revisar Obtener el archivo de imagen para el cortafuegos CN-Series y Parámetros editables en archivos yaml de CN-Series.

STEP 2 | Utilice el flujo de trabajo incluido en Protección de las cargas de trabajo de Kubernetes con CN-Series.

Debe crear las credenciales de servicio e implementar los YAML del cortafuegos.

Nota: Si su archivo de credenciales de servicio tiene más de 10 KB, debe comprimir con gzip el archivo y luego realizar una codificación base64 del archivo comprimido antes de cargar o pegar el contenido del archivo en la CLI o API de Panorama.

STEP 3 | Configure el complemento PAN-CNI para que funcione con el complemento Multus CNI.

Multus CNI en OpenShift funciona como un "meta-complemento" que llama a otros complementos CNI. Para cada aplicación debe:

1. Implementar la definición de adjunto de red PAN-CNI en cada espacio de nombres de pod

   `kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>`

2. Modifique la aplicación YAML.

   Después de implementar pan-cni-net-attach-def.yaml, en el pod de la aplicación yaml añada la anotación:

   `paloaltonetworks.com/firewall: pan-fw`

   `k8s.v1.cni.cncf.io/networks: pan-cni`

   Si tiene otras redes en la anotación anterior, añada **`pan-cni`** después de las redes que se deben inspeccionar. Las redes que siguen a **`pan-cni`** no se redirigen ni se inspeccionan.

   Si su pod tiene varias interfaces de red, debe especificar la interfaz para los que desea que el pod CN-NGFW inspeccione el tráfico, en "interfaces" en pan-cni-configmap.yaml.

   Por ejemplo:

```
        plantilla: metadatos: anotaciones: paloaltonetworks.com/
cortafuegos: pan-fw k8s.v1.cni.cncf.io/networks: bridge-conf,
 macvlan-conf, sriov-conf, pan-cni
```

CN-Series ahora es compatible con el complemento OVN-Kubernetes Container Network Interface (CNI) en RedHat OpenShift versión 4.13 y superior, en el modo de implementación de Kubernetes Service y el modo DaemonSet.

Implementación del CN-Series en el Operator Hub de OpenShift

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con la versión PAN-OS 10.2.x y superior

El cortafuegos para contenedores CN-Series ahora está disponible en Operator Hub de la plataforma RedHat Openshift. Puede implementar, configurar y operar cortafuegos para contenedores CN-Series directamente desde RedHat Operador Hub.

Requisitos previos para CN-Series en el Operador Hub de Openshift:

Los siguientes son los requisitos previos para implementar el cortafuegos CN-Series en el operator hub de Openshift:

- Autorizar la licencia para el cortafuegos CN-Series. El complemento de Kubernetes en Panorama gestiona las licencias del cortafuegos CN-Series. Generar su código de autorización y téngalo a mano cuando esté listo para implementar el cortafuegos CN-Series. Para obtener más información, consulte Autorización de licencia para el cortafuegos CN-Series.
- Generar la clave de autenticación de VM en Panorama.
- Instalar un certificado de dispositivo en el cortafuegos VM-Series.
- Crear cuentas de servicio para la autenticación de clúster
- Implementar Panorama: debe usar Panorama para configurar, implementar y gestionar la implementación de su cortafuegos CN-Series. Para obtener más información sobre cómo implementar y configurar un dispositivo Panorama, consulte Configurar Panorama.
- Instale el complemento de Kubernetes para el cortafuegos CN-Series.
- El clúster de OpenShift debe cumplir los requisitos previos de CN-Series.
- Asegúrese de tener acceso al Portal de atención al cliente (CSP) de Palo Alto Networks y tener créditos Flex.
- Asegúrese de ser cliente de RedHat con una licencia de OpenShift y una cuenta que tenga permisos para crear recursos en OpenShift.
- Asegúrese de que el clúster de OpenShift cumpla con los Requisitos previos de CN-Series.

Para obtener más información, consulte Cómo implementar fácilmente CN-Series en el Operador Hub de RedHat Openshift.

Implemente CN-Series en un operator hub de OpenShift:

El pan-cni protege el tráfico en la interfaz predeterminada **eth0** del pod de la aplicación. Si tiene pods de múltiples hosts, puede configurar el pod CN-NGFW para proteger interfaces adicionales que están configuradas con una conexión basada en puente para comunicarse con otros pods o el host. Dependiendo

de la anotación en la aplicación YAML, puede configurar el cortafuegos CN-Series para inspeccionar el tráfico de todas las interfaces o una cantidad seleccionada de interfaces adjuntas a cada pod.

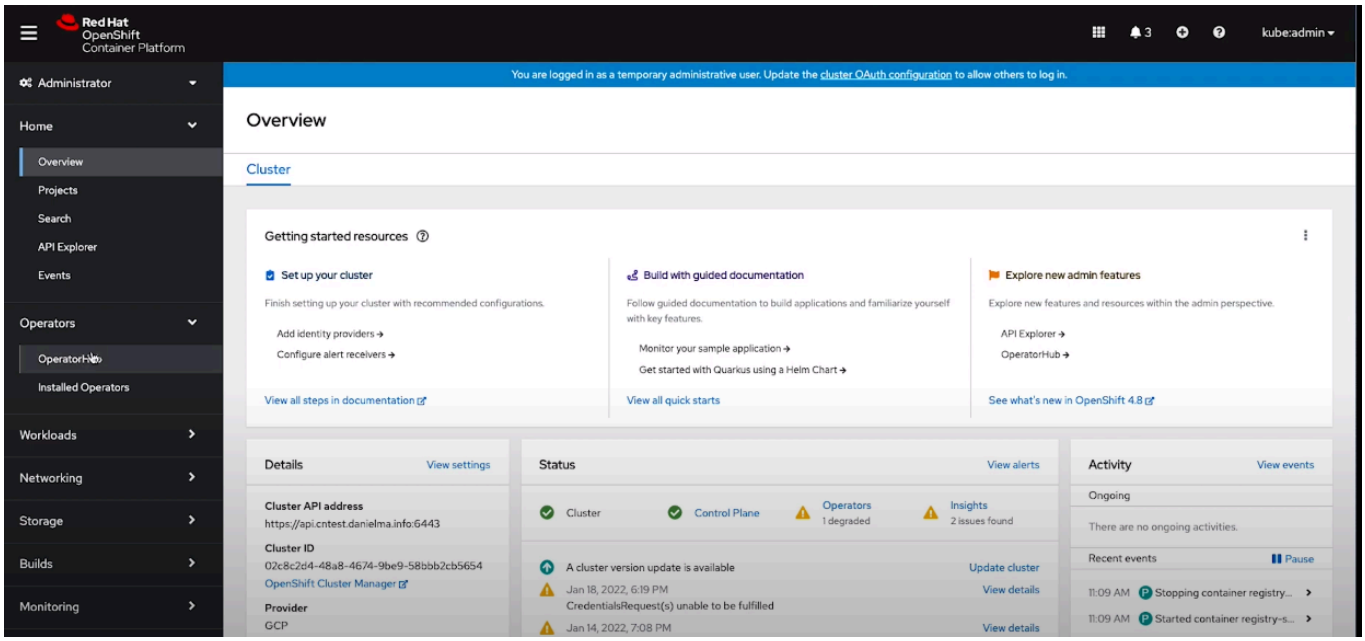
El pan-cni no crea una red y, por lo tanto, no necesita direcciones IP como otros complementos de CNI.

Necesita PAN-OS 10.2 o posterior para implementar CN-Series en el Operator Hub de OpenShift.

Los siguientes son los pasos para implementar el cortafuegos CN-Series en el Operator Hub de Redhat OpenShift:

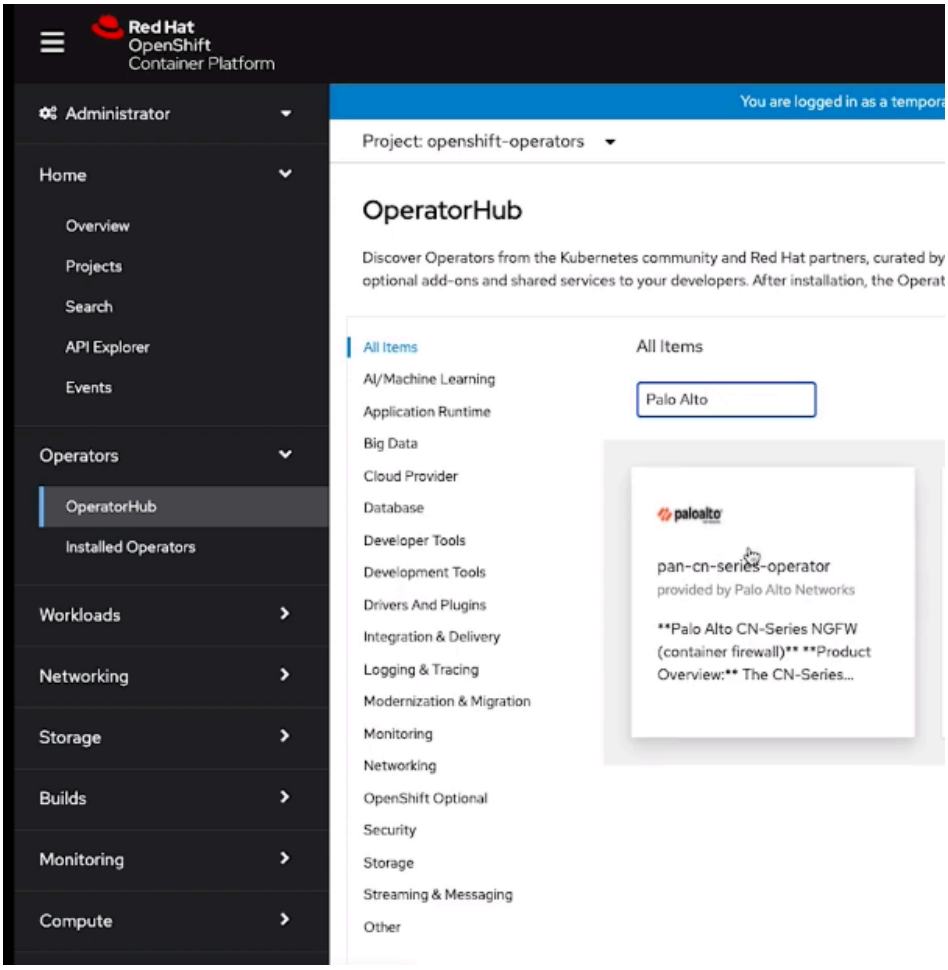
STEP 1 | Inicie sesión en la consola del contenedor OpenShift de Redhat.

STEP 2 | Vaya a **Operadores**y luego haga clic en **OperadorHub**.



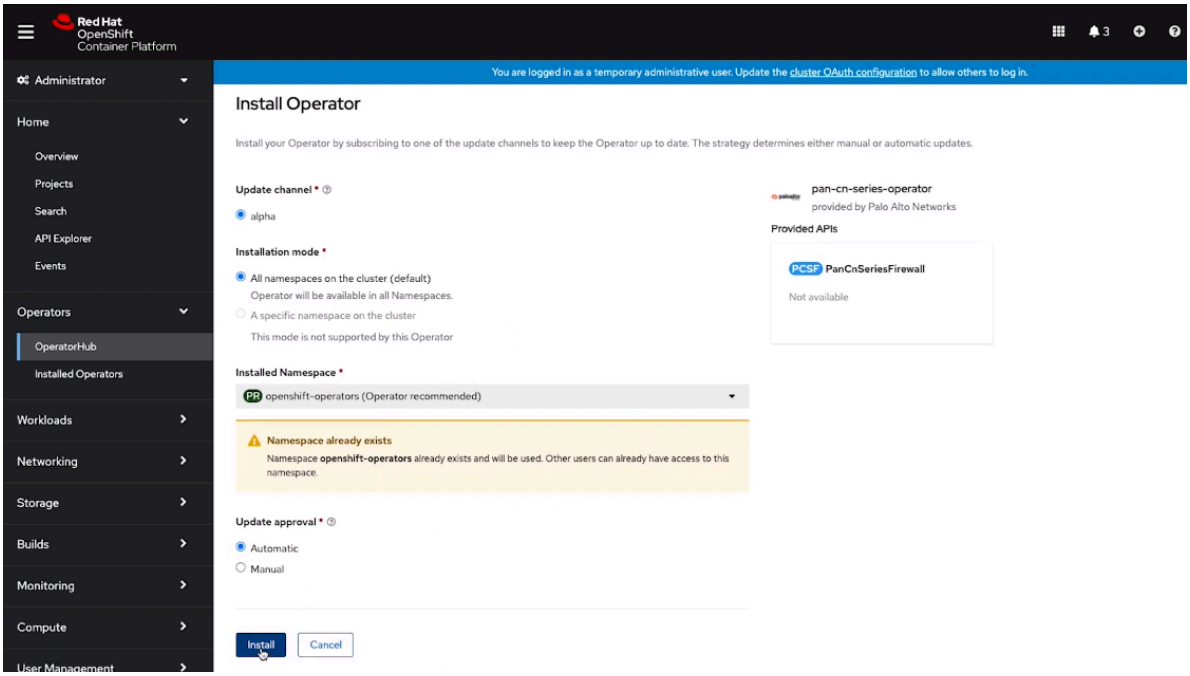
STEP 3 | Introduzca **Palo Alto** en el cuadro de búsqueda de Operador.

STEP 4 | Haga clic en **pan-cn-series-operator**.



La ventana de instalación se abre al hacer clic en el mosaico **pan-cn-series-operator**.

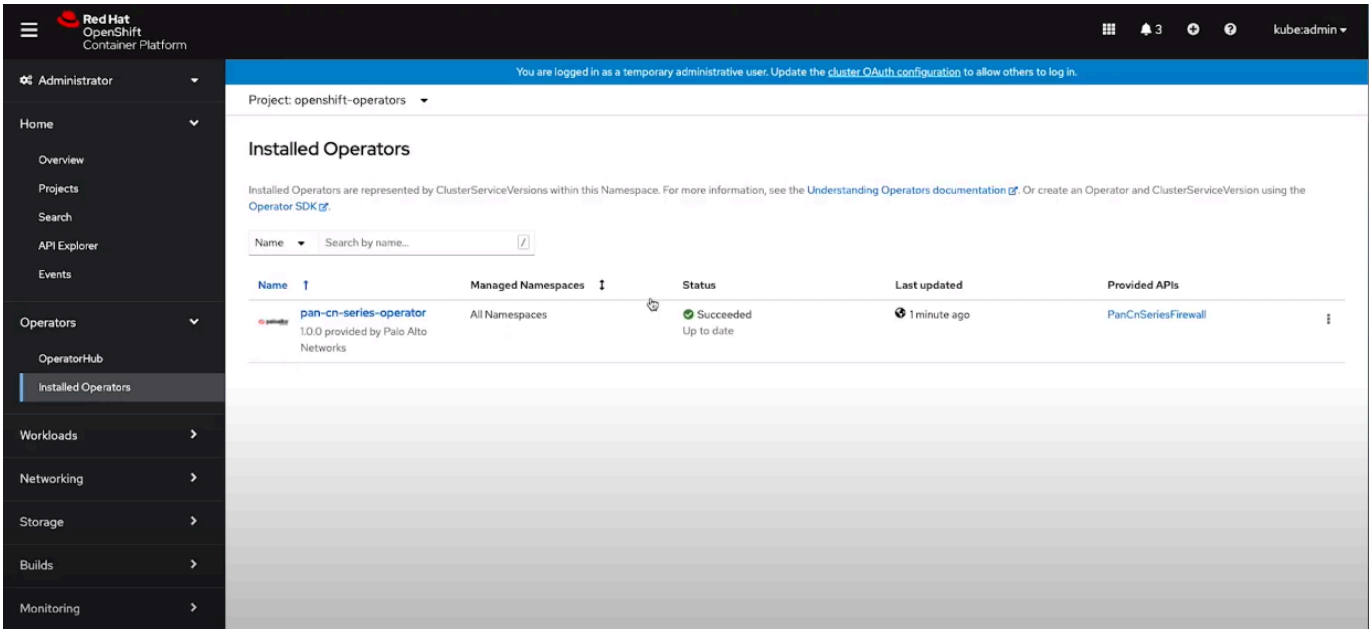
STEP 5 | Haga clic en **Instalar** para instalar el operador pan-cn-series en su clúster OpenShift.



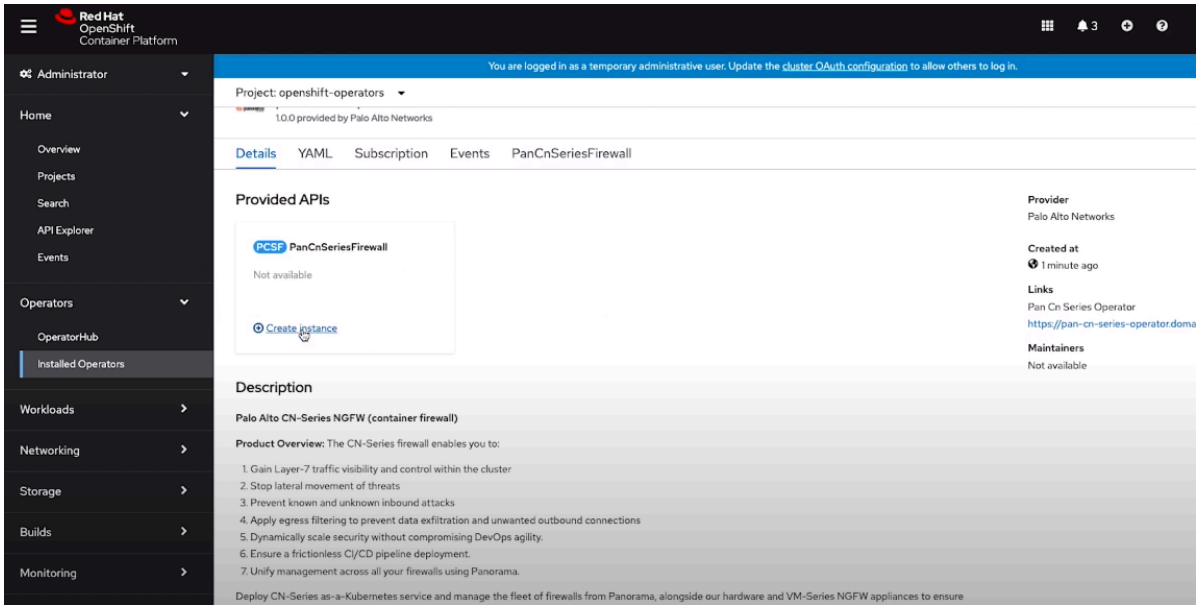
Complete los pasos previos a la instalación antes de los siguientes pasos de implementación que se indican aquí.

Si su archivo de credenciales de servicio tiene más de 10 KB, debe comprimir con gzip el archivo y luego realizar una codificación base64 del archivo comprimido antes de cargar o pegar el contenido del archivo en la CLI o API de Panorama.

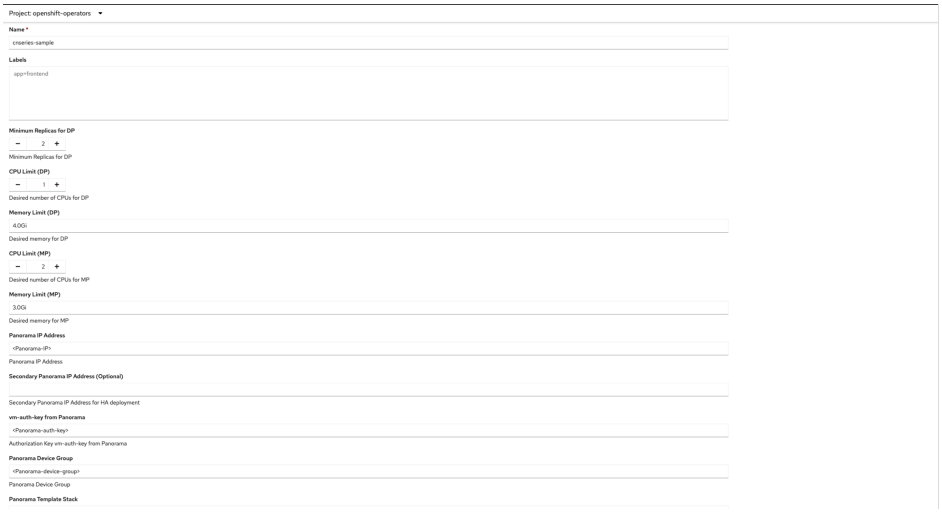
STEP 6 | En el menú de navegación, vaya a **Operadores instalados** y luego haga clic en el operador **pan-cn-series-operator** que ha instalado.



STEP 7 | Haga clic en **Crear instancia**.



STEP 8 | Introduzca un **nombre**de operando único.



STEP 9 | Introduzca el **número mínimo de réplicas para DP**, **la unidad de memoria**y **el límite de vCPU** para los pods de DP y MP. Para obtener información sobre los límites de vCPU, consulte Métricas clave de rendimiento de la CN-Series.

STEP 10 | Introduzca la **dirección IP de Panorama**.

STEP 11 | Opcional Introduzca la **dirección IP secundaria de Panorama** para su implementación de HA.

STEP 12 | Introduzca la **clave de autenticación** de Panorama para CN-Series.

STEP 13 | Introduzca el **Grupo de dispositivos de Panorama**.

STEP 14 | Introduzca la **Pila de plantillas de Panorama**.

STEP 15 | Introduzca el **nombre del grupo de recopiladores de logs de Panorama**.

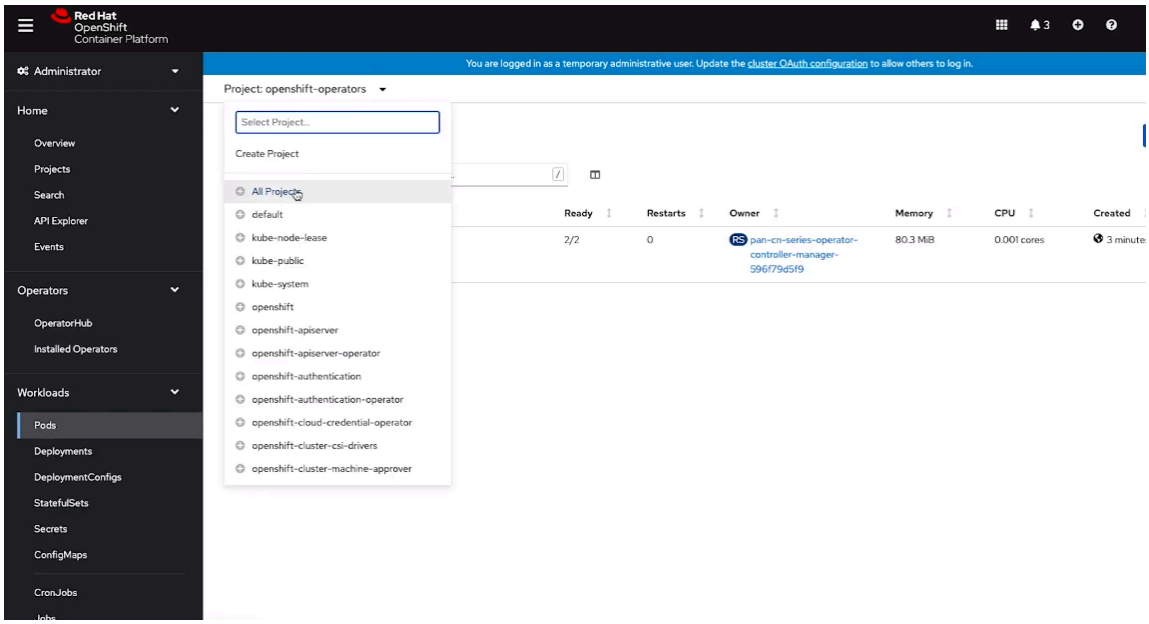
STEP 16 | Opcional Introduzca el **ID del PIN**, el **valor del PIN**y la **URL alternativa**del portal de atención al cliente (CSP).

STEP 17 | Según su versión de PAN-OS, vincule las imágenes apropiadas para DP, MP y CNI en la consola de registros contenedores de CN-Series.

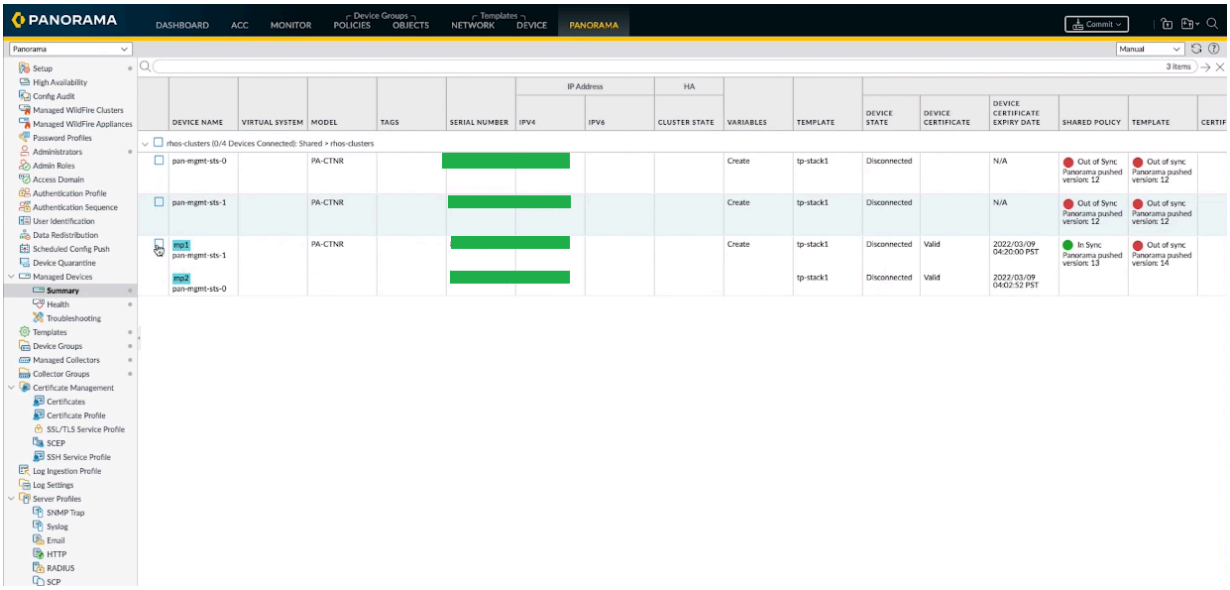
STEP 18 | Haga clic en **Create (Crear)**.

STEP 19 | En el menú de navegación, vaya a **pods**.

STEP 20 | Seleccione los **operadores OpenShift** del proyecto y luego vaya a **kube-system** para ver el nombre y el estado de los pods de CNI, gestión y plano de datos que implementó como parte del operando.



Puede verificar el estado de implementación del cortafuegos en Panorama. El **Estado del dispositivo** cambiará a Conectado en menos de 5 minutos después de la implementación.



STEP 21 | Configure el complemento PALO ALTO NETWORKS-CNI para que funcione con el complemento Multus CNI.

Multus CNI en OpenShift funciona como un **meta-plugin** que llama a otros complementos CNI. Para cada aplicación debe:

1. Ejecute el siguiente comando para implementar pan-cni-net-attach-def.yaml en cada espacio de nombres del pod:

   `kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>`

2. Modifique la aplicación YAML.

   Después de implementar pan-cni-net-attach-def.yaml en el yalm del pod de la aplicación añada la siguiente anotación:

   `paloaltonetworks.com/firewall: pan-fw`

   `k8s.v1.cni.cncf.io/networks: pan-cni`

   Si tiene otras redes en la anotación anterior, añada **`pan-cni`** después de las redes que necesitan inspección. Las redes que siguen a **`pan-cni`** no se redirigen ni se inspeccionan.

   Si su pod tiene varias interfaces de red, debe especificar los nombres de las interfaces para las cuales desea que el pod CN-NGFW inspeccione el tráfico, en la sección de ***interfaces*** *del archivo* `pan-cni-configmap.yaml` .

   Por ejemplo:

```
        template: metadata: annotations: paloaltonetworks.com/
firewall: pan-fw k8s.v1.cni.cncf.io/networks: pan-cni
```

