

Configuración del clúster de Kubernetes mediante el servicio Intersight Kubernetes

Contenido

[Introducción](#)

[Antecedentes](#)

[Descripción general de la solución](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Suposición](#)

[Configuración](#)

[Paso 1. Configurar políticas](#)

[Paso 2. Configurar perfil](#)

[Verificación](#)

[Conéctese al clúster de Kubernetes](#)

[Verificar con CLI](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración para aprovisionar un clúster de Kubernetes de producción desde Cisco Intersight (SaaS) con el uso de Cisco Intersight™ Kubernetes Service (IKS).

Antecedentes

Kubernetes, en tiempos recientes, se ha convertido en una herramienta de gestión de contenedores de facto, ya que las organizaciones tienden a invertir más en la modernización de aplicaciones con soluciones Containerized. Con Kubernetes, los equipos de desarrollo pueden implementar, administrar y ampliar sus aplicaciones en contenedores con facilidad, lo que hace que las innovaciones sean más accesibles para sus sistemas de suministro continuo.

Sin embargo, Kubernetes se enfrenta a retos operativos, ya que se necesita tiempo y experiencia técnica para instalar y configurar.

La instalación de Kubernetes y los diferentes componentes de software necesarios, la creación de clústeres, la configuración del almacenamiento, las redes y la seguridad, junto con las operaciones (por ejemplo, la actualización, actualización y corrección de errores de seguridad críticos) requieren una importante inversión continua en capital humano.

Ingresa a IKS, una solución SaaS llave en mano para administrar Kubernetes uniformes y de calidad de producción en cualquier lugar. Para obtener más información sobre las capacidades de IKS, consulte este enlace [aquí](#).

Descripción general de la solución

Para este documento, la idea es mostrar la capacidad de IKS para integrarse sin problemas con su infraestructura in situ, ejecutando VMware ESXi y vCenter.

Con unos pocos clics, puede implementar un clúster de Kubernetes de grado de producción en su infraestructura VMware.

Pero para ello, debe integrar su vCenter in situ con Intersight, conocido como "reclamar un objetivo", ya que vCenter es el objetivo aquí.

Necesitaría un dispositivo virtual Cisco Intersight Assist, que ayude a agregar objetivos de terminales a Cisco Intersight. Puede instalar Intersight Assist usando el bootstrap OVA disponible en el sitio web oficial de Cisco.

Para limitar el alcance de este documento, no nos centraríamos en la instalación de Cisco Intersight Assist Virtual Appliance. Pero, puede echar un vistazo al proceso [aquí](#)

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cuenta de Intersight: Necesita una ID de Cisco y una cuenta de Intersight válidas. Puede crear una ID de Cisco en el sitio web de Cisco si no la tiene. A continuación, haga clic en el enlace Crear una cuenta en [Intersight](#).
- Cisco Intersight Assist: Cisco Intersight Assist le ayuda a agregar vCenter/ESXi como objetivo de terminales a Cisco Intersight.
- Conectividad: Si su entorno admite un proxy HTTP/S, puede utilizarlo para conectar su dispositivo Cisco Intersight Assist Appliance a Internet. Alternativamente, debe abrir puertos para las URL de interconexión. Verifique este [link](#) para conocer los requisitos de conectividad de red detallados :
- Credenciales de vCenter para reclamarlo en Intersight.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Suposición

Dado que la implementación de Cisco Intersight Appliance está fuera del alcance de este documento.

Suponemos que ya dispone de una cuenta de Intersight en funcionamiento y que ha solicitado con éxito un vCenter/Esxi in situ.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

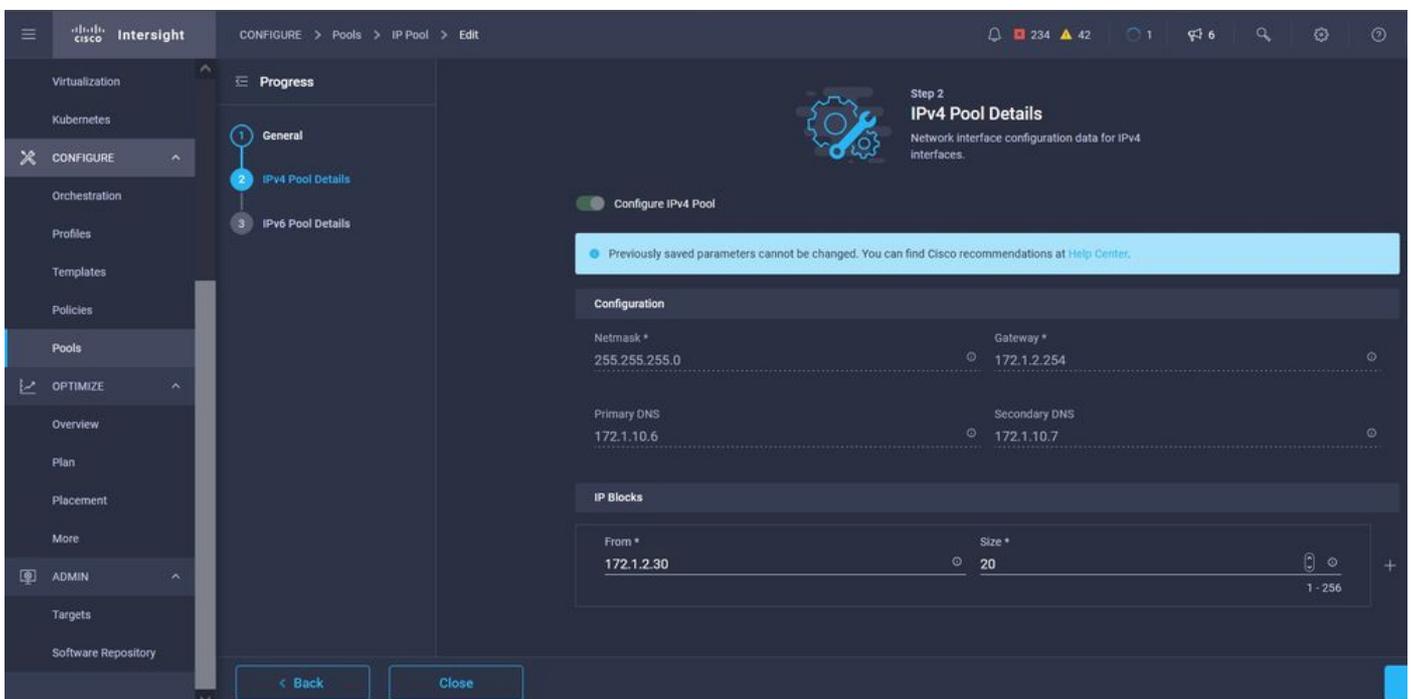
Paso 1. Configurar políticas

Las políticas permiten una gestión simplificada, ya que abstraen la configuración en plantillas reutilizables.

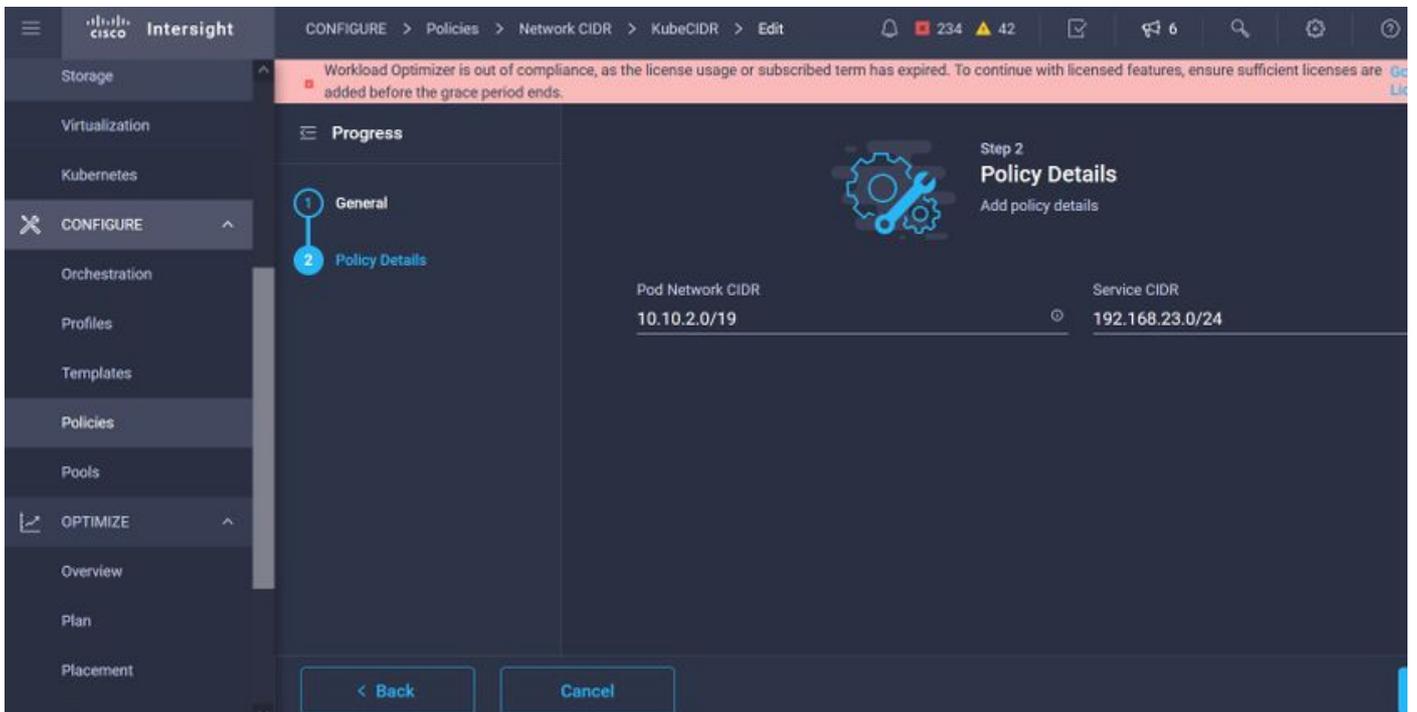
A continuación se enumeran algunas de las políticas que debemos configurar. Tenga en cuenta que todas estas políticas se crearán en la sección Configurar >> Políticas y Configurar >> Pools en Intersight.

También puede ver la ruta de la política encima de cada captura de pantalla, que se muestra a continuación.

Este grupo IP se utilizará para las direcciones IP de sus máquinas virtuales de control y nodos de trabajo cuando se inicie en el host ESXi.

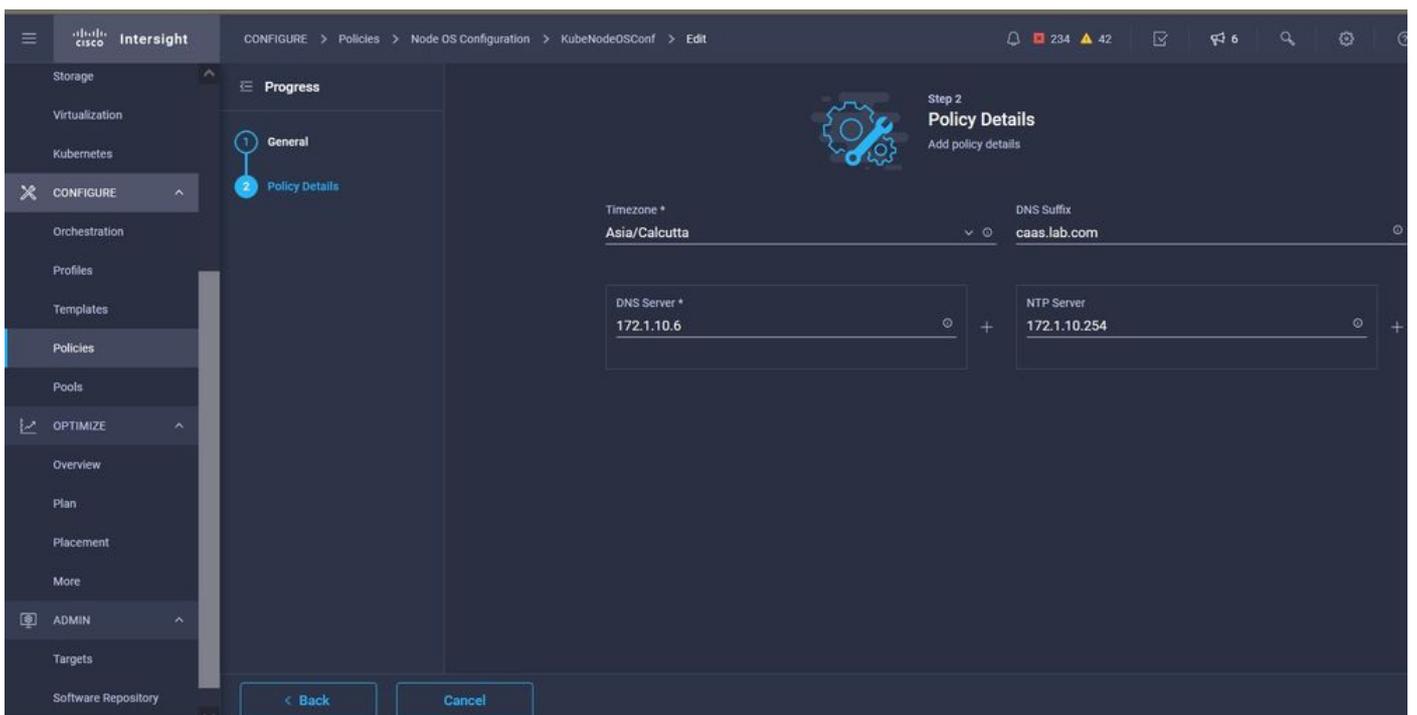


Aquí define el CIDR de red de Pod y servicios para redes internas dentro del clúster de Kubernetes.



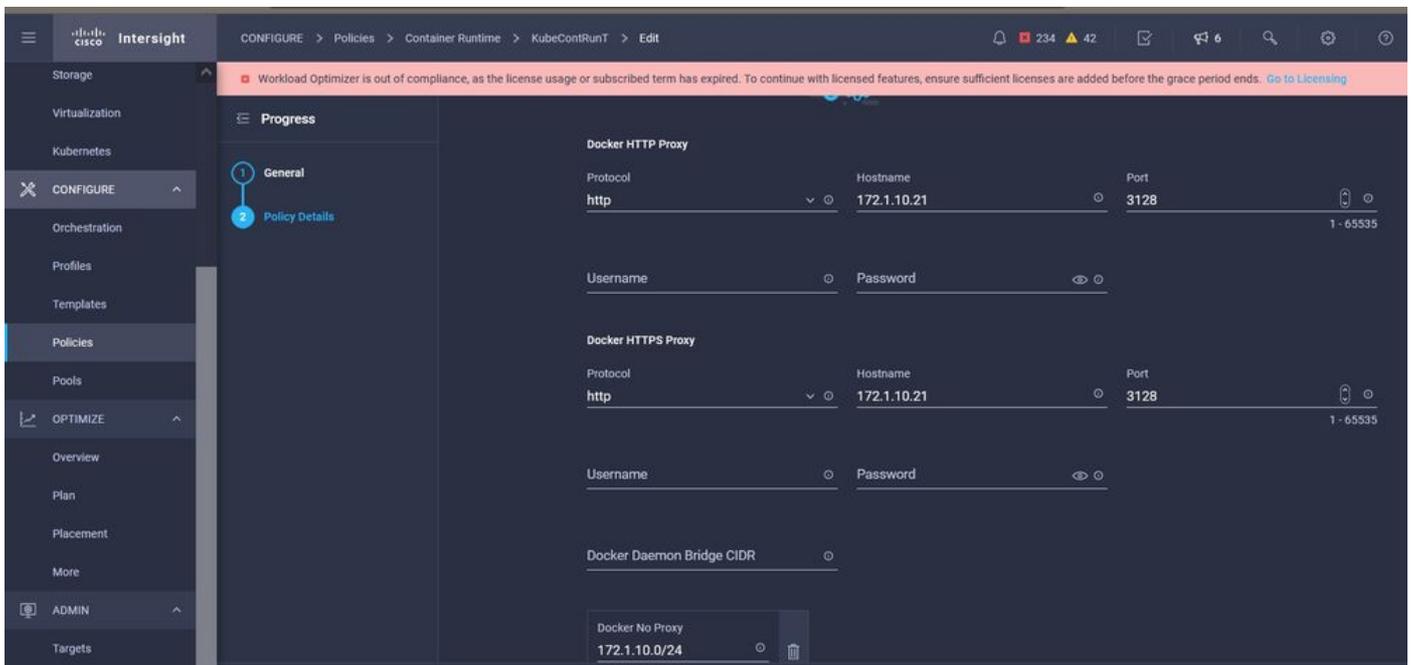
CIDR de red y servicios

Esta política define su configuración de NTP y DNS.



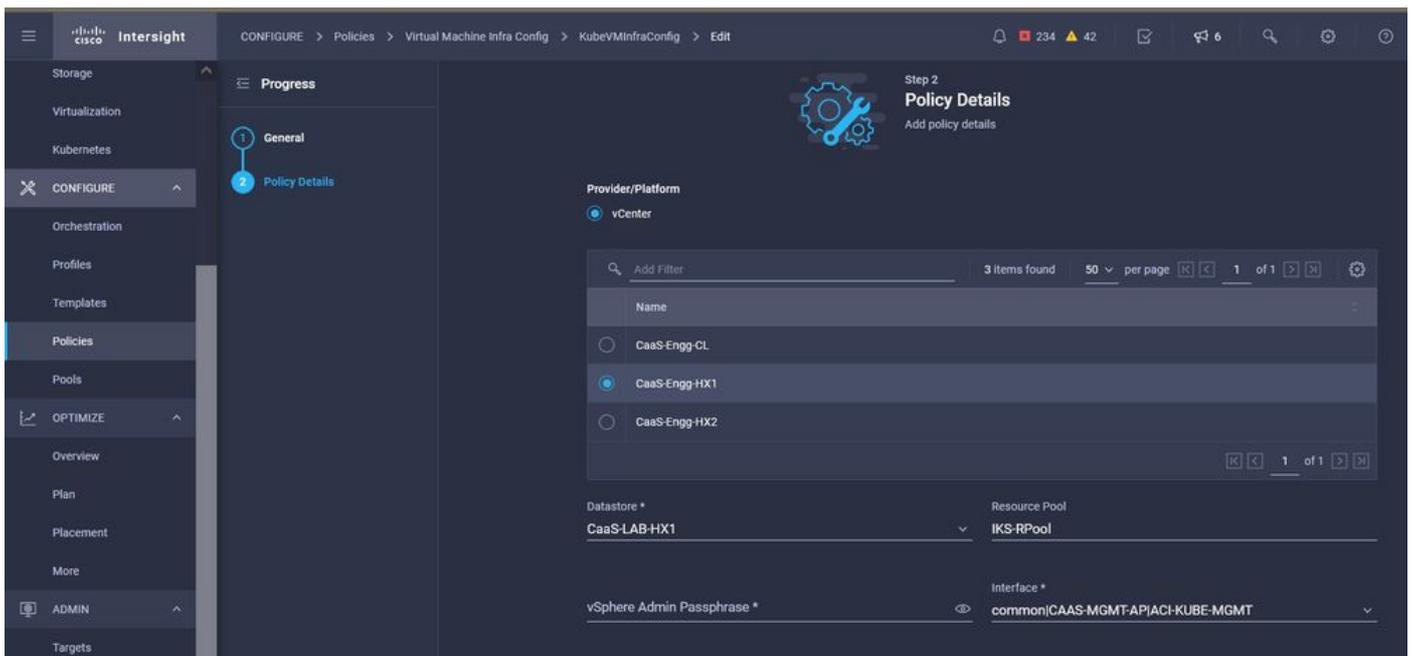
Configuración de NTP y DNS

Con esta política, puede definir la configuración de proxy para el motor en tiempo de ejecución del contenedor de docker.



Configuración de proxy para Docker

En esta política, definirá la configuración necesaria en las máquinas virtuales implementadas como nodos Master y Worker.



Configuración de VM utilizadas

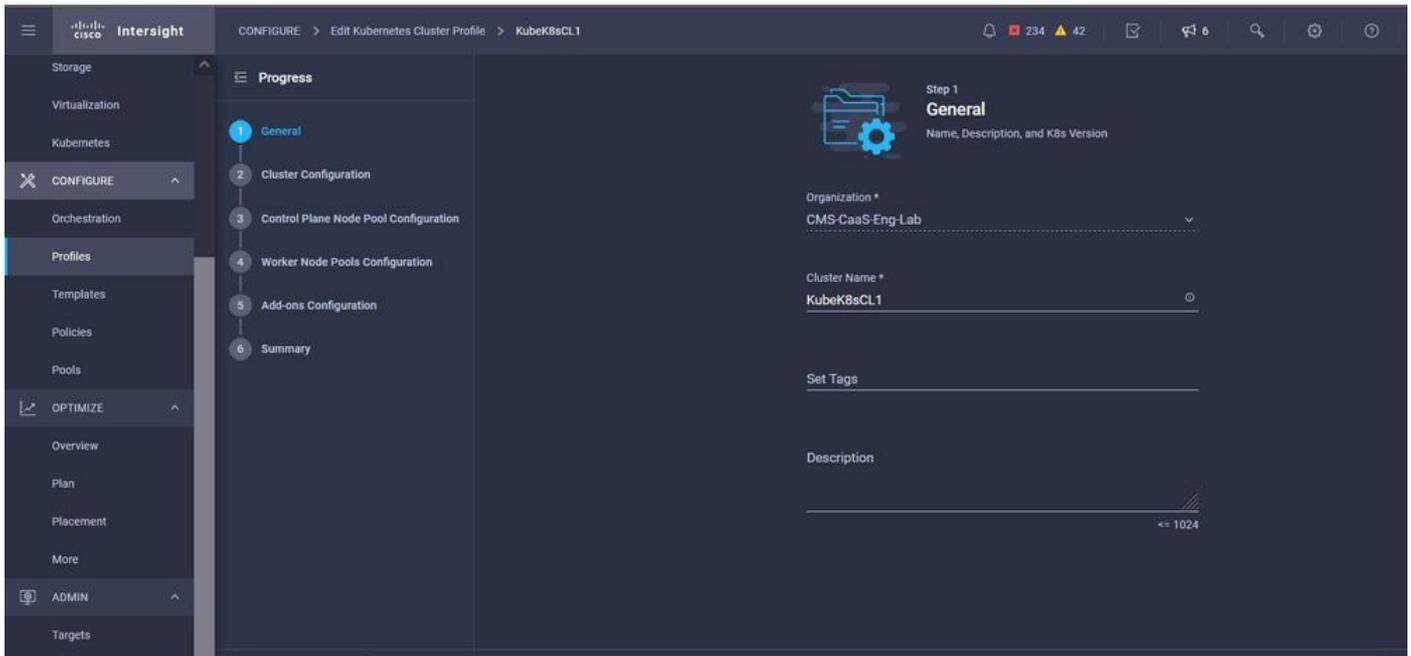
Paso 2. Configurar perfil

Una vez creadas las políticas anteriores, las enlazaríamos a un perfil que luego podemos implementar.

La implementación de la configuración mediante políticas y perfiles abstrae la capa de configuración para que se pueda implementar repetidamente rápidamente.

Puede copiar este perfil y crear uno nuevo con pocas o más modificaciones en las políticas subyacentes en cuestión de minutos, para que uno o más grupos de Kubernetes se agrupen en una fracción de tiempo necesaria con un proceso manual.

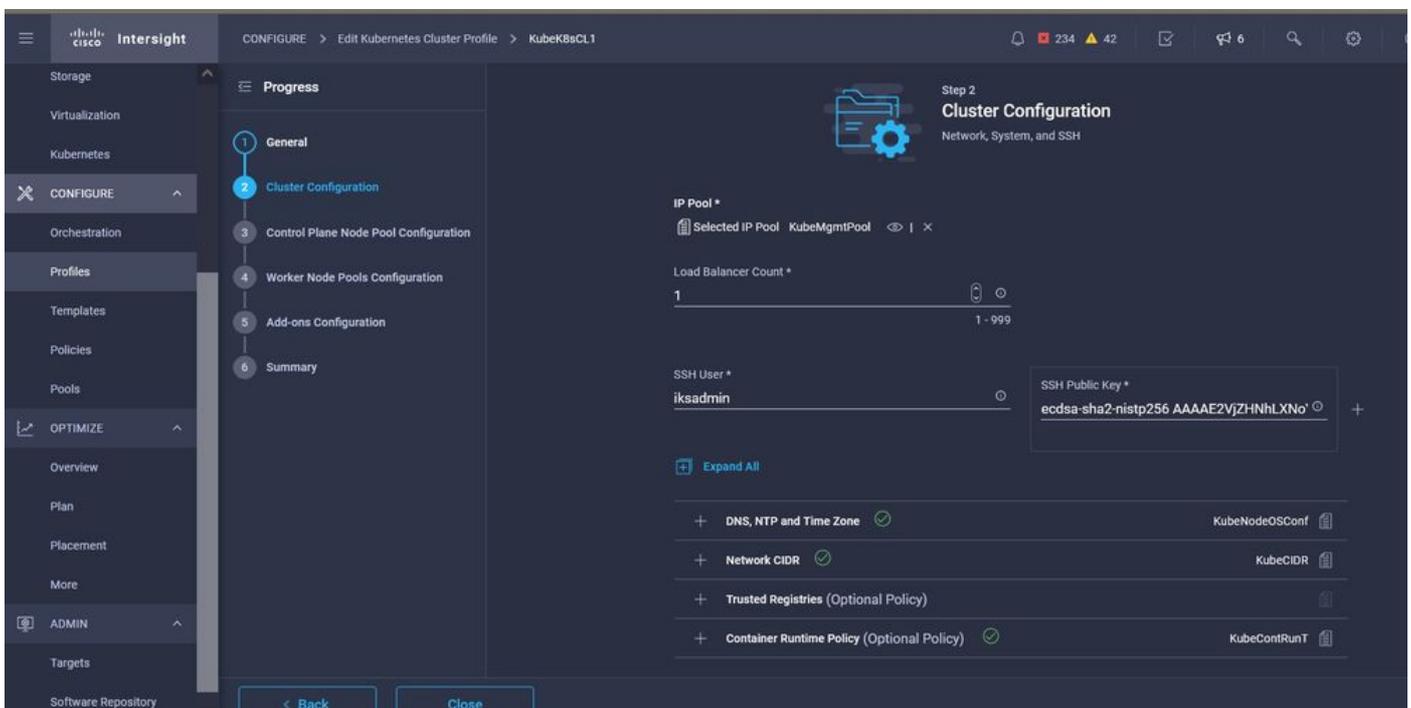
Give en el campo Nombre y establezca Etiquetas.



Configuración del perfil con nombre y etiquetas

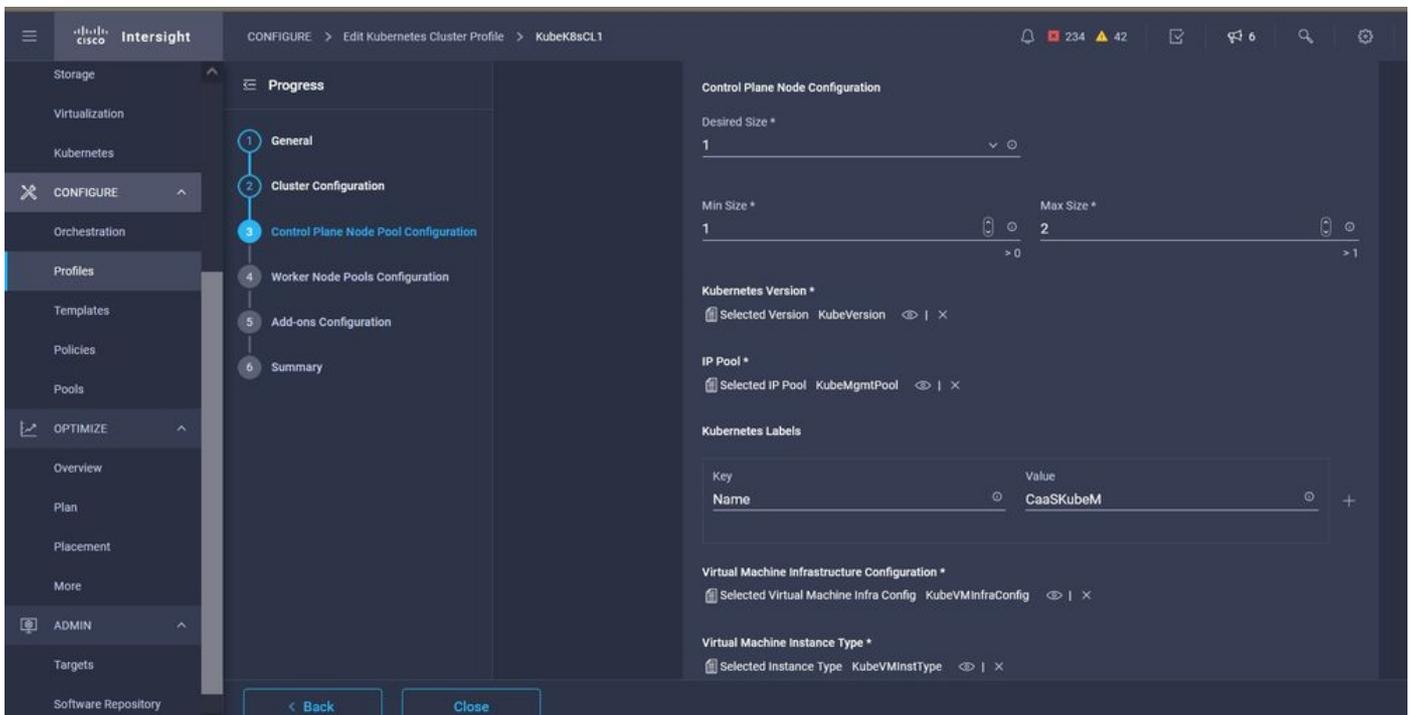
Establezca las políticas Pool, Node OS, Network CIDR. También debe configurar un ID de usuario y una clave SSH (pública).

Su clave privada correspondiente se utilizaría para enviar a los nodos Master y Worker.



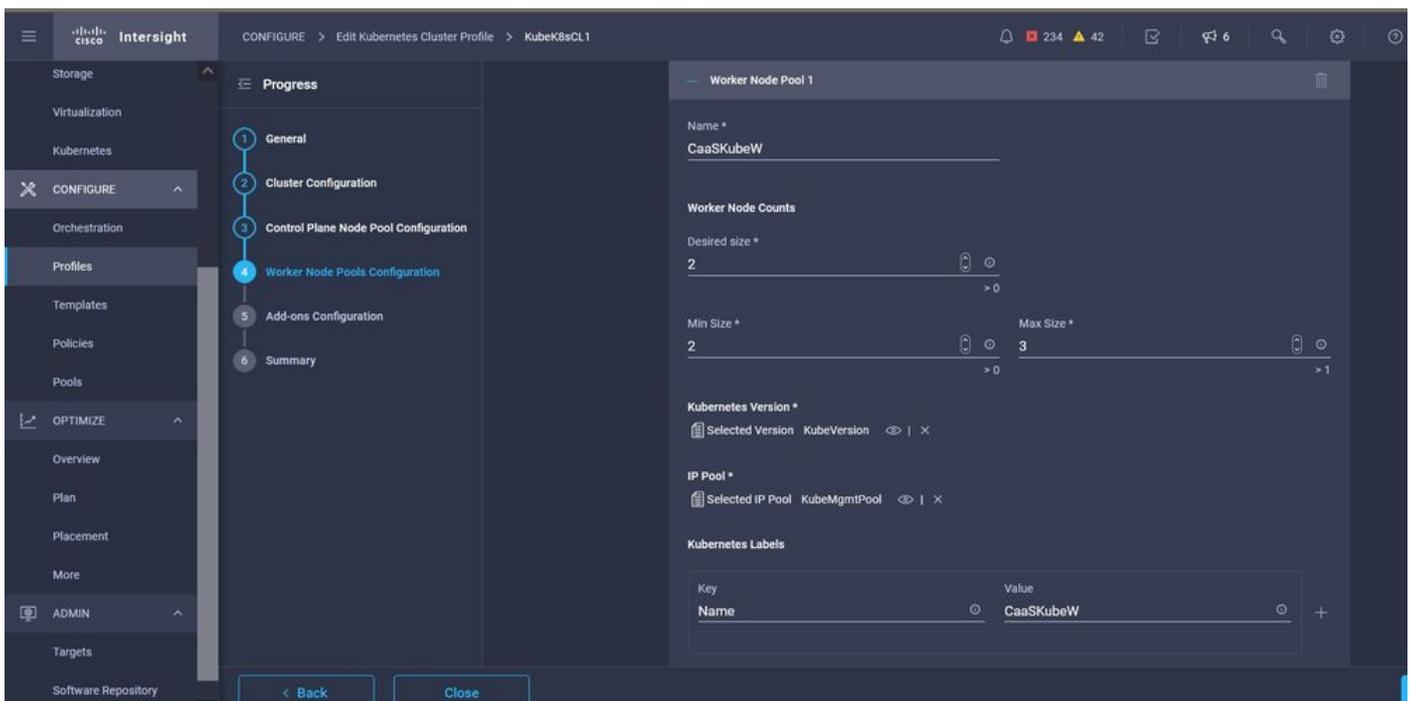
Configuración de perfiles con políticas asignadas

Configure el plano de control: Puede definir cuántos nodos principales necesitará en el plano de control.



Configuración del nodo maestro

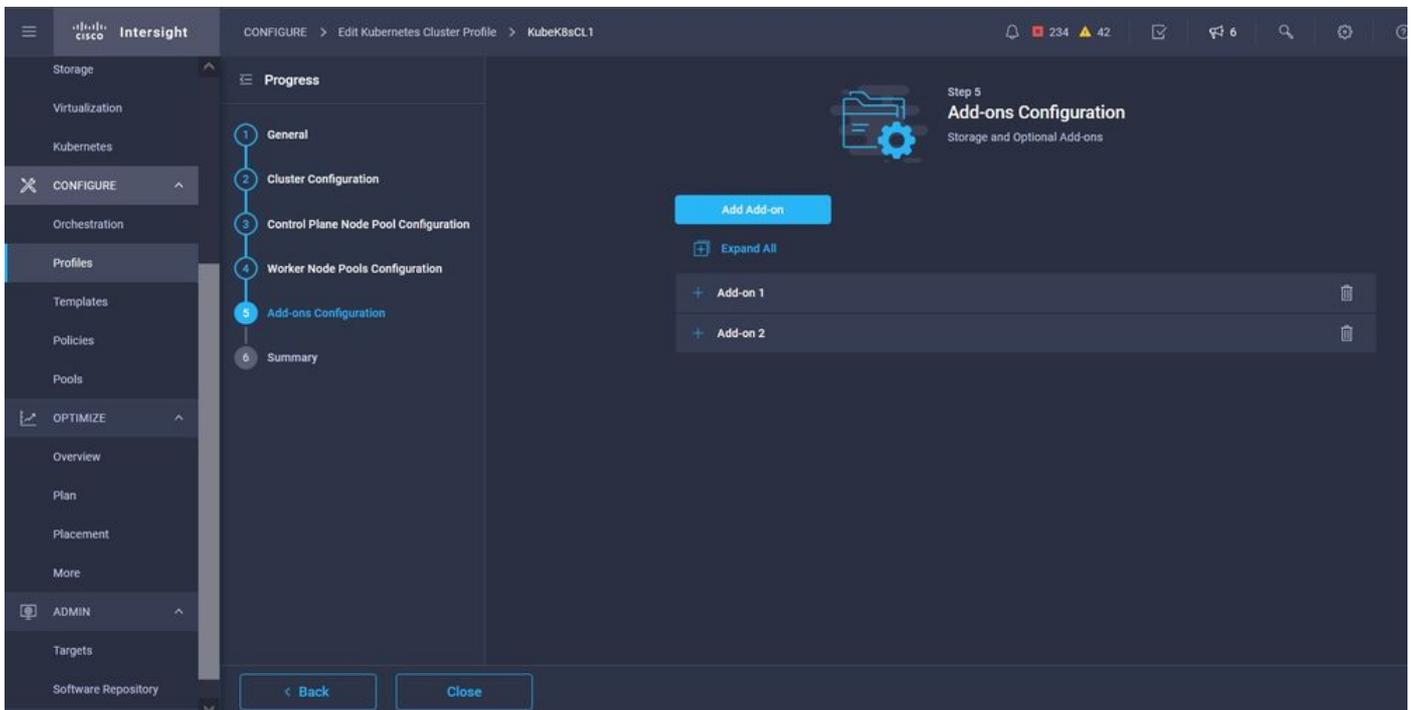
Configure los nodos Worker: En función de los requisitos de la aplicación, puede ampliar o reducir los nodos de los trabajadores.



Configuración de nodos de trabajo

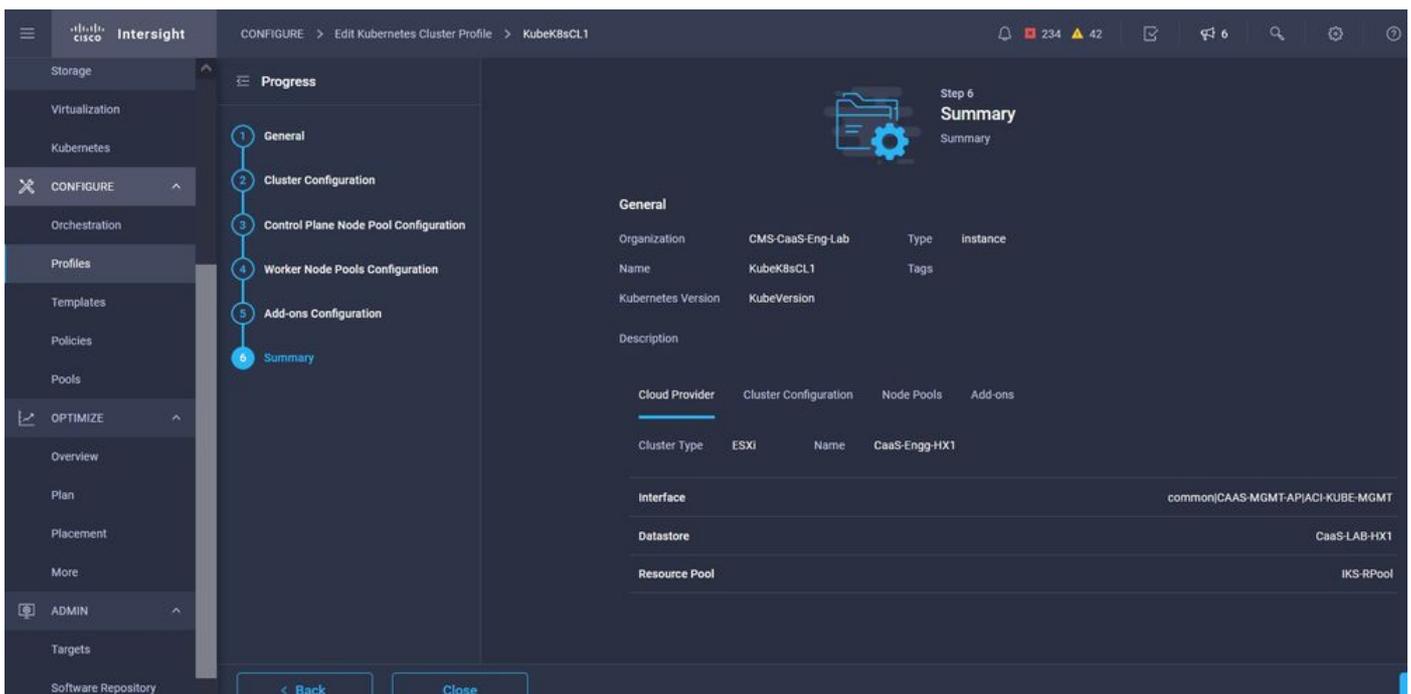
Configurar el complemento. A partir de ahora, puede implementar automáticamente el panel de Kubernetes y Grafana con supervisión Prometheus.

En el futuro, puede agregar más complementos que puede implementar automáticamente con IKS.



Agregar complementos, si los hubiera

Verifique el Resumen y haga clic en **Implementar**.

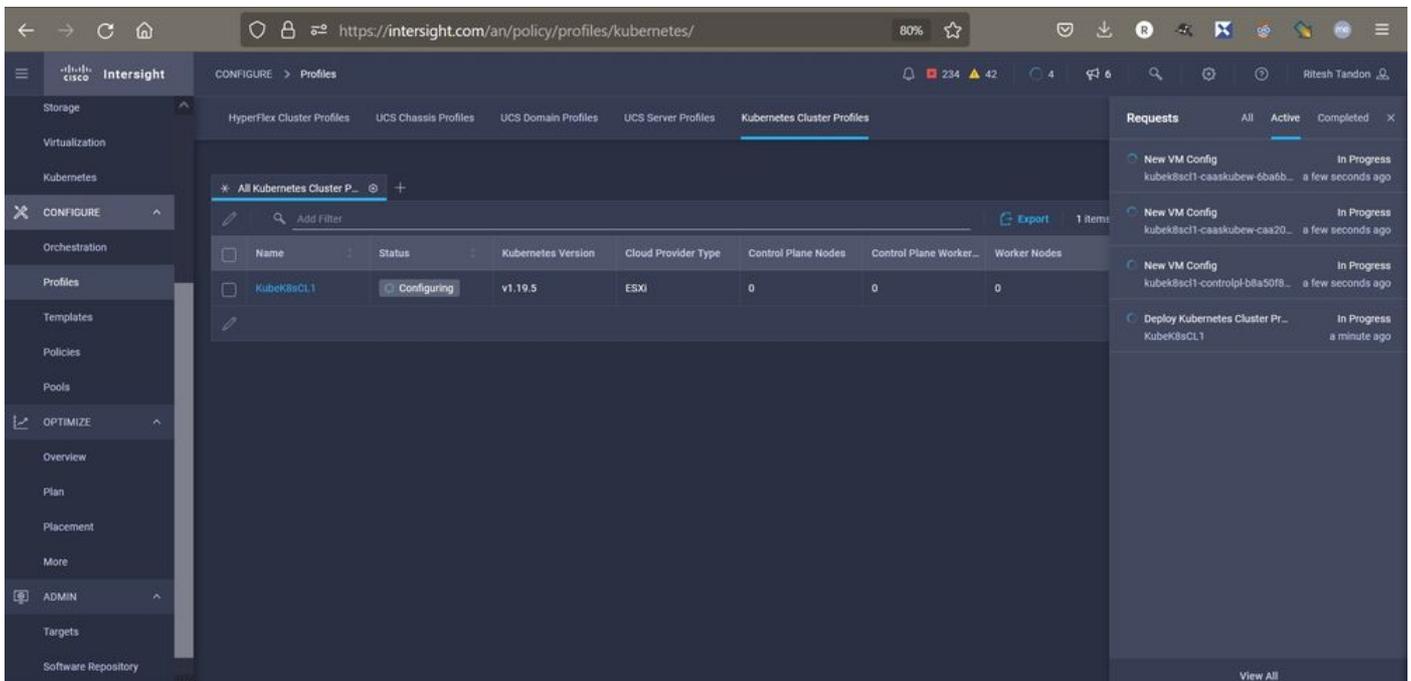


Pantalla Resumen de creación de perfiles

Verificación

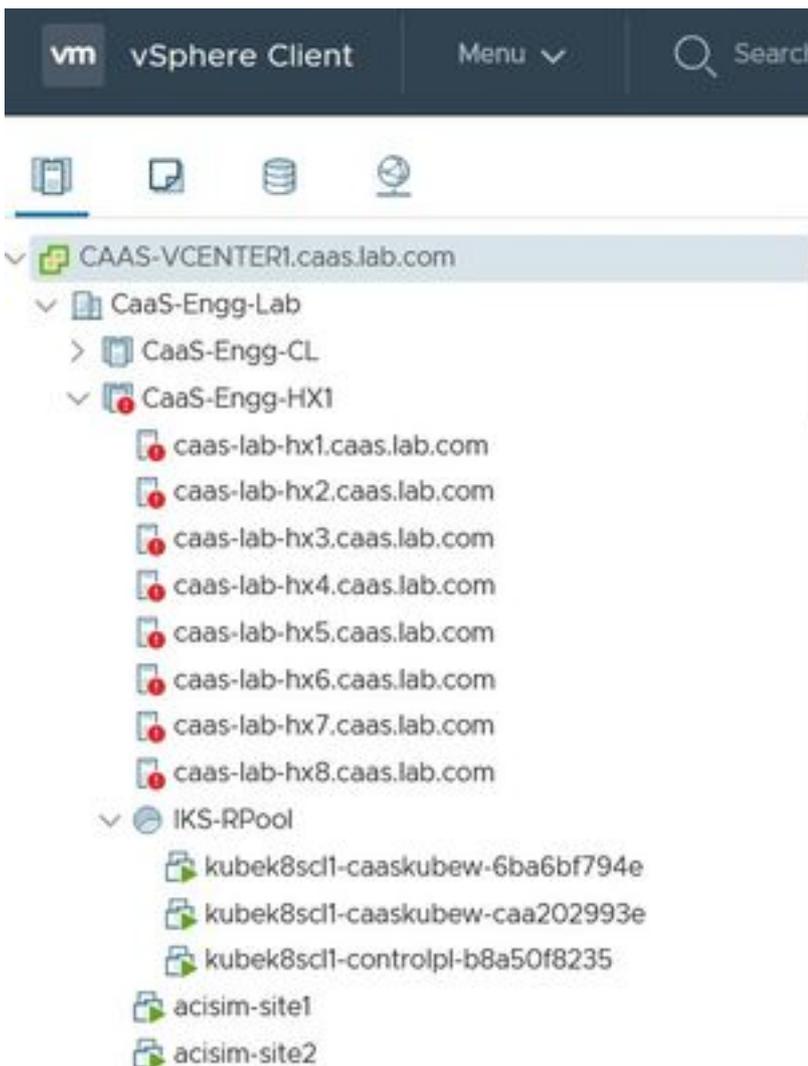
Use esta sección para confirmar que su configuración funciona correctamente.

En la parte superior derecha, puede realizar un seguimiento del progreso de la implementación.



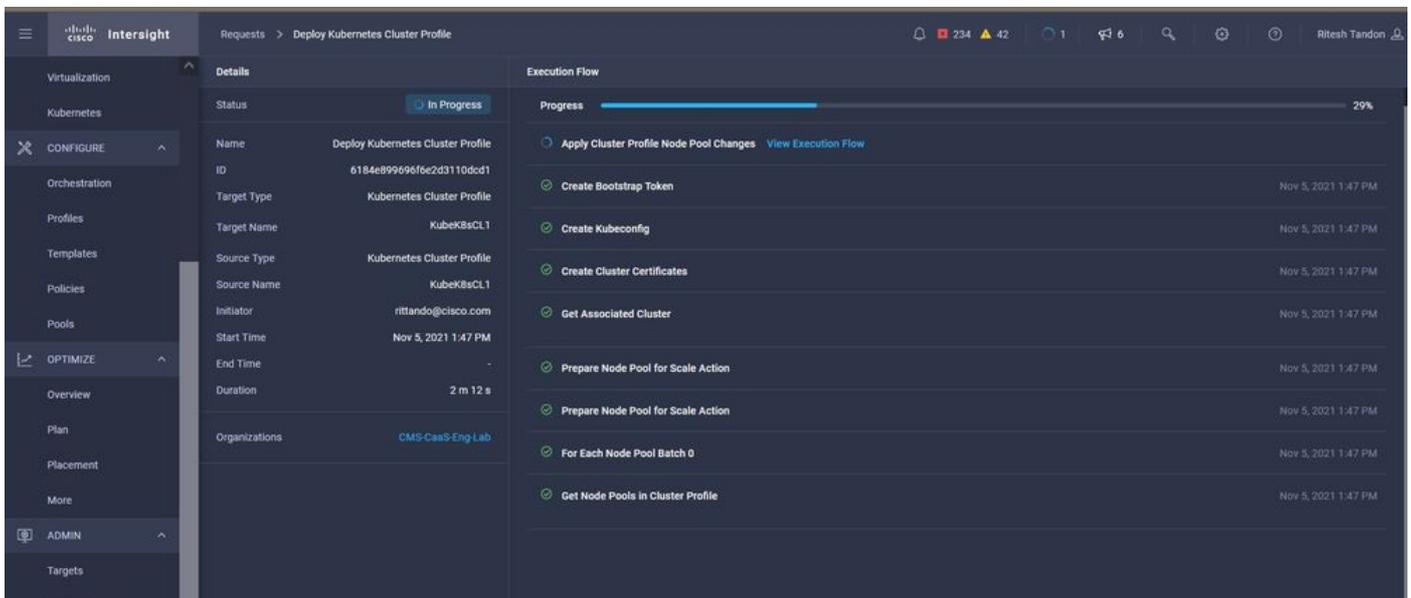
Verificar mediante la GUI de IKS

A medida que avanza la implementación, puede ver los nodos maestro y de trabajo de Kubernetes en el vCenter.



Se acerca el clúster IKS en vCenter

Si necesita ver los pasos detallados para la implementación, puede profundizar en la ejecución.



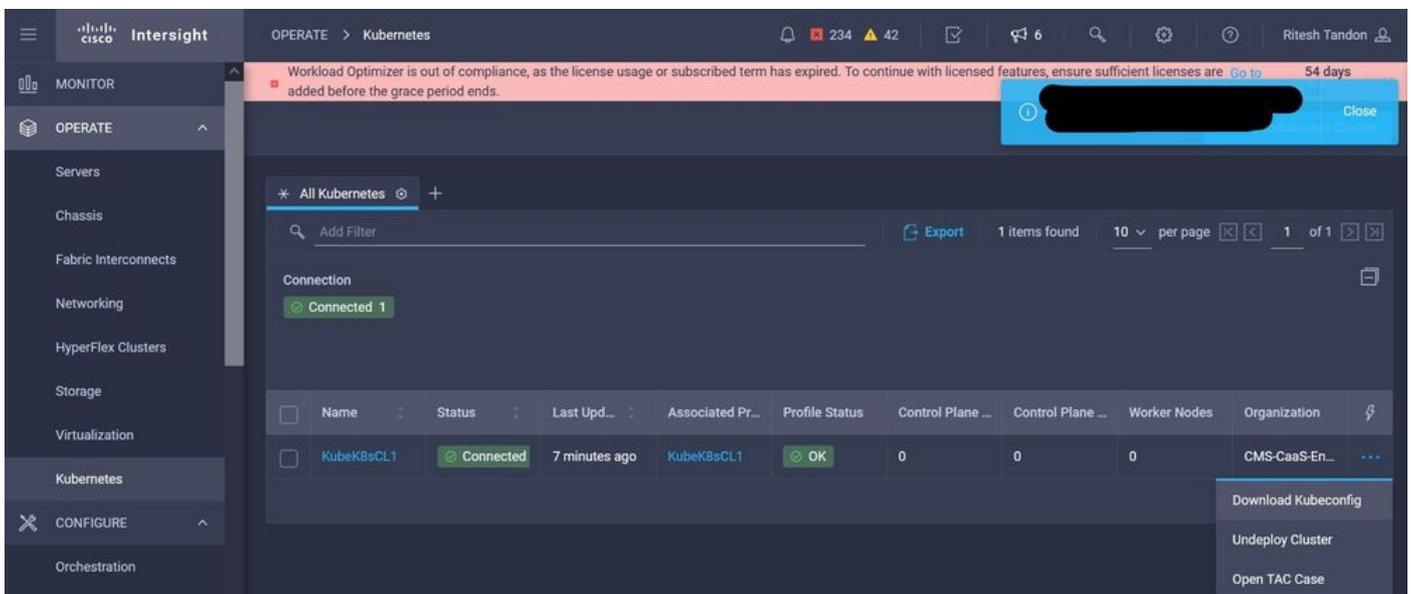
Ejecución de creación de perfiles

Conéctese al clúster de Kubernetes

Puede conectarse al clúster de Kubernetes de las siguientes maneras:

Utilizando el archivo KubeConfig, que puede descargar desde **Operate > Kubernetes > Seleccione las opciones en el extremo derecho.**

Debe tener instalado KubeCtl en la estación de trabajo de administración, desde donde desea acceder a este clúster.



Descargue el archivo KubeConfig de IKS

También puede ingresar directamente SSH en el nodo maestro, utilizando aplicaciones SSH como Putty con las credenciales y la clave privada configuradas en el momento de la implementación

Si implementa 'Panel de Kubernetes' como complemento, también puede utilizarlo para implementar aplicaciones directamente mediante la GUI.

Para ver más detalles, por favor consulte la sección 'Acceso a los clústeres de Kubernetes', [aquí](#) :

Verificar con CLI

Una vez que pueda conectarse al clúster de Kubernetes, utilizando kubeCtl, puede utilizar los siguientes comandos para verificar si el clúster tiene todos los componentes instalados y en ejecución.

Verifique que los nodos del clúster estén en estado 'preparado'.

```
iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ kubectl get nodes NAME STATUS ROLES AGE VERSION kubek8scl1-caaskubew-6ba6bf794e Ready
```

Verifique el estado de los grupos de dispositivos que se crearon en el momento de la instalación de los componentes esenciales en el clúster.

```
iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ kubectl get pod -n iks | grep apply- apply-ccp-monitor-2b7tx 0/1 Completed 0 6d3h apply-cloud-provider-qczsj 0/1 Completed 0 6d3h apply-cni-g7dcc 0/1 Completed 0 6d3h apply-essential-cert-ca-jwdtk 0/1 Completed 0 6d3h apply-essential-cert-manager-bg5fj 0/1 Completed 0 6d3h apply-essential-metallb-nzj7h 0/1 Completed 0 6d3h apply-essential-nginx-ingress-8qrnq 0/1 Completed 0 6d3h apply-essential-registry-f5wn6 0/1 Completed 0 6d3h apply-essential-vsphere-csi-tjfnq 0/1 Completed 0 6d3h apply-kubernetes-dashboard-rslt4 0/1 Completed 0 6d3h
```

Verifique el estado del ccp-helm-operator pod que administra el casco que se ejecuta localmente e instala los complementos.

```
iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ kubectl get helmcharts.helm.ccp.----.com -A NAMESPACE NAME STATUS VERSION INSTALLED VERSION SYNCED iks ccp-monitor INSTALLED 0.2.61-helm3 iks essential-cert-ca INSTALLED 0.1.1-helm3 iks essential-cert-manager INSTALLED v1.0.2-cisco1-helm3 iks essential-metallb INSTALLED 0.12.0-cisco3-helm3 iks essential-nginx-ingress INSTALLED 2.10.0-cisco2-helm3 iks essential-registry INSTALLED 1.8.3-cisco10-helm3 iks essential-vsphere-csi INSTALLED 1.0.1-helm3 iks kubernetes-dashboard INSTALLED 3.0.2-cisco3-helm3 iks vsphere-cpi INSTALLED 0.1.3-helm3 iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ helm ls -A WARNING: Kubernetes configuration file is group-readable. This is insecure. Location: /home/iksadmin/.kube/config NAME NAMESPACE REVISION UPDATED STATUS CHART APP VERSION addon-operator iks 1 2021-11-05 07:45:15.44180913 +0000 UTC deployed ccp-helm-operator-9.1.0-alpha.44.g415a48c4be1.0 ccp-monitor iks 1 2021-11-05 08:23:11.309694887 +0000 UTC deployed ccp-monitor-0.2.61-helm3 essential-cert-ca iks 1 2021-11-05 07:55:04.409542885 +0000 UTC deployed cert-ca-0.1.1-helm3 0.1.0 essential-cert-manager iks 1 2021-11-05 07:54:41.433212634 +0000 UTC deployed cert-manager-v1.0.2-cisco1-helm3 v1.0.2 essential-metallb iks 1 2021-11-05 07:54:48.799226547 +0000 UTC deployed metallb-0.12.0-cisco3-helm3 0.8.1 essential-nginx-ingress iks 1 2021-11-05 07:54:46.762865131 +0000 UTC deployed ingress-nginx-2.10.0-cisco2-helm3 0.33.0 essential-registry iks 1 2021-11-05 07:54:36.734982103 +0000 UTC deployed docker-registry-1.8.3-cisco10-helm3 2.7.1 essential-vsphere-csi kube-system 1 2021-11-05 07:54:58.168305242 +0000 UTC deployed vsphere-csi-1.0.1-helm3 v2.0.0 kubernetes-dashboard iks 1 2021-11-05 07:55:10.197905183 +0000 UTC deployed kubernetes-dashboard-3.0.2-cisco3-helm3 2.1.0 vsphere-cpi kube-system 1 2021-11-05 07:54:38.292088943 +0000 UTC deployed vsphere-cpi-0.1.3-helm3 1.1.0
```

Verifique el estado de los grupos de dispositivos esenciales* que administran los complementos Essential (core), instalados de forma predeterminada, en cada clúster de arrendatarios IKS.

```
iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ kubectl get pod -n iks | grep ^essential- essential-cert-manager-6bb7d776d-tpkhj 1/1 Running 0 6d4h essential-cert-manager-cainjector-549c8f74c-x5sjp 1/1 Running 0 6d4h essential-cert-manager-webhook-76f596b686-drf79 1/1 Running 0 6d4h essential-metallb-controller-6557847d57-djs9b 1/1 Running 0 6d4h essential-metallb-speaker-7t54v 1/1 Running 0 6d4h essential-metallb-speaker-ggmbn 1/1 Running 0 6d4h essential-metallb-speaker-
```

```
mwmfg 1/1 Running 0 6d4h essential-nginx-ingress-ingress-nginx-controller-k2hsw 1/1 Running 0
6d4h essential-nginx-ingress-ingress-nginx-controller-kfkm9 1/1 Running 0 6d4h essential-nginx-
ingress-ingress-nginx-defaultbackend-695fbj4mnd 1/1 Running 0 6d4h essential-registry-docker-
registry-75b84457f4-4fmlh 1/1 Running 0 6d4h
```

Verifique el estado de los servicios y el equilibrador de carga implementado en el espacio de nombres IKS.

```
iksadmin@kubek8scl1-controlpl-b8a50f8235:~$ kubectl get svc -n iks NAME TYPE CLUSTER-IP
EXTERNAL-IP PORT(S) AGE ccp-monitor-grafana ClusterIP 192.168.23.161
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

En caso de que no aparezca un grupo de dispositivos determinado, puede utilizar estos comandos para profundizar en la causa.

Syntax : `kubectl describe pod`

Información Relacionada

- Consulte el resumen de servicio de IKS [aquí](#).
- Consulte la guía del usuario [aquí](#).
- Compruebe la demostración del servicio Intersight Kubernetes [aquí](#).
- [Soporte Técnico y Documentación - Cisco Systems](#)