Configurar o cluster Kubernetes usando o Intersight Kubernetes Service

Contents

[Introduction](#)
[Informações de Apoio](#)
[Visão geral da solução](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Hipóteses](#)
[Configuração](#)
[Etapa 1. Configurar políticas](#)
[Etapa 2. Configurar perfil](#)
[Verificar](#)
[Conectar-se ao cluster Kubernetes](#)
[Verificar com CLI](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve a configuração para provisionar um cluster Kubernetes de nível de produção do Cisco Intersight (SaaS) com o uso do Cisco Intersight™ Kubernetes Service (IKS).

Informações de Apoio

Kubernetes, nos últimos tempos, se tornou uma ferramenta de gerenciamento de contêineres de fato, já que as empresas tendem a investir mais na modernização de aplicativos com soluções contaminadas. Com os Kubernetes, as equipes de desenvolvimento podem implantar, gerenciar e dimensionar seus aplicativos contidos com facilidade, tornando as inovações mais acessíveis a seus pipelines de entrega contínua.

Entretanto, o Kubernetes vem com desafios operacionais, pois requer tempo e experiência técnica para instalar e configurar.
A instalação de Kubernetes e dos diferentes componentes de software necessários, a criação de clusters, a configuração de armazenamento, rede e segurança, juntamente com operações (por exemplo, atualização, atualização e correção de bugs de segurança críticos) exigem um investimento contínuo e significativo em capital humano.

Entre no IKS, uma solução de SaaS pronta para uso para gerenciar Kubernetes consistentes e de produção em qualquer lugar. Para ler mais sobre os recursos do IKS, verifique este link aqui.

Visão geral da solução

Para este documento, a ideia é mostrar a capacidade da IKS de se integrar perfeitamente à sua infraestrutura no local, executando o VMware ESXi e o vCenter.
Com alguns cliques, você pode implantar um cluster Kubernetes de produção na sua infraestrutura VMware.

Mas, para fazer isso, você precisa integrar seu vCenter no local com a Intersight, conhecida como "reivindicação de um alvo", sendo que o vCenter é o alvo aqui.
Você precisaria de um Cisco Intersight Assist Virtual Appliance, que ajude a adicionar destinos de endpoint ao Cisco Intersight. Você pode instalar o Intersight Assist usando o bootstrap OVA disponível no site oficial da Cisco.

Para limitar o escopo deste documento, não nos concentramos na instalação do Cisco Intersight Assist Virtual Appliance. Mas, você pode dar uma olhada no processo aqui

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conta do Intersight: Você precisa de uma ID da Cisco válida e uma conta do Intersight. Você pode criar uma ID da Cisco no site da Cisco se não tiver uma. Em seguida, clique no link Create an Account (Criar uma conta) no Intersight.
- Cisco Intersight Assist: O Cisco Intersight Assist ajuda você a adicionar o vCenter/ESXi como um destino de endpoint ao Cisco Intersight.
- Conectividade: Se o seu ambiente suportar um proxy HTTP/S, você poderá usá-lo para conectar o Cisco Intersight Assist Appliance à Internet. Como alternativa, você precisa abrir portas para entrevistar URLs. Verifique este link para obter os requisitos detalhados de conectividade de rede:
- Credenciais do vCenter para reivindicar no Intersight.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Hipóteses

Como a implantação de um Cisco Intersight Appliance está fora do escopo deste documento.

Pressupomos que você já tem uma conta do Intersight em funcionamento e já reivindicou com êxito um vCenter/Esxi no local.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

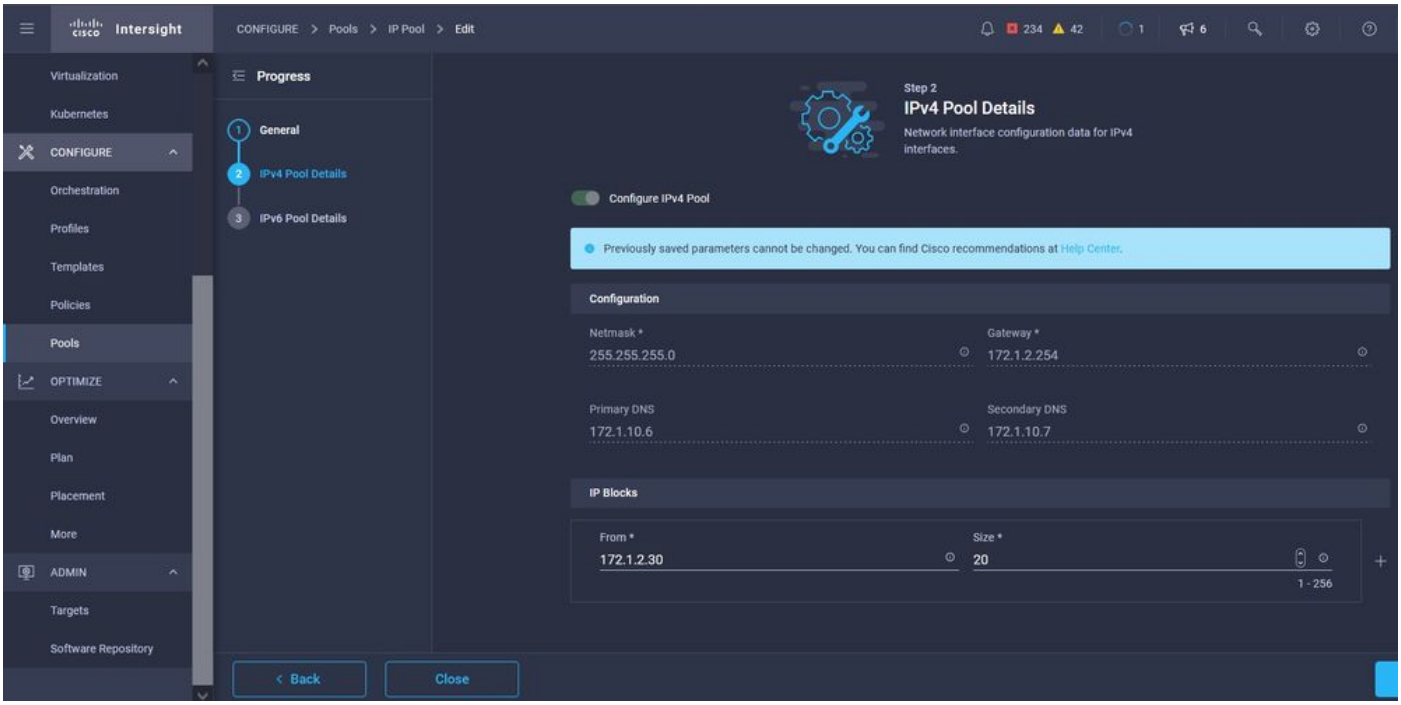
Etapa 1. Configurar políticas

As políticas permitem um gerenciamento simplificado à medida que abstraem a configuração em modelos reutilizáveis.

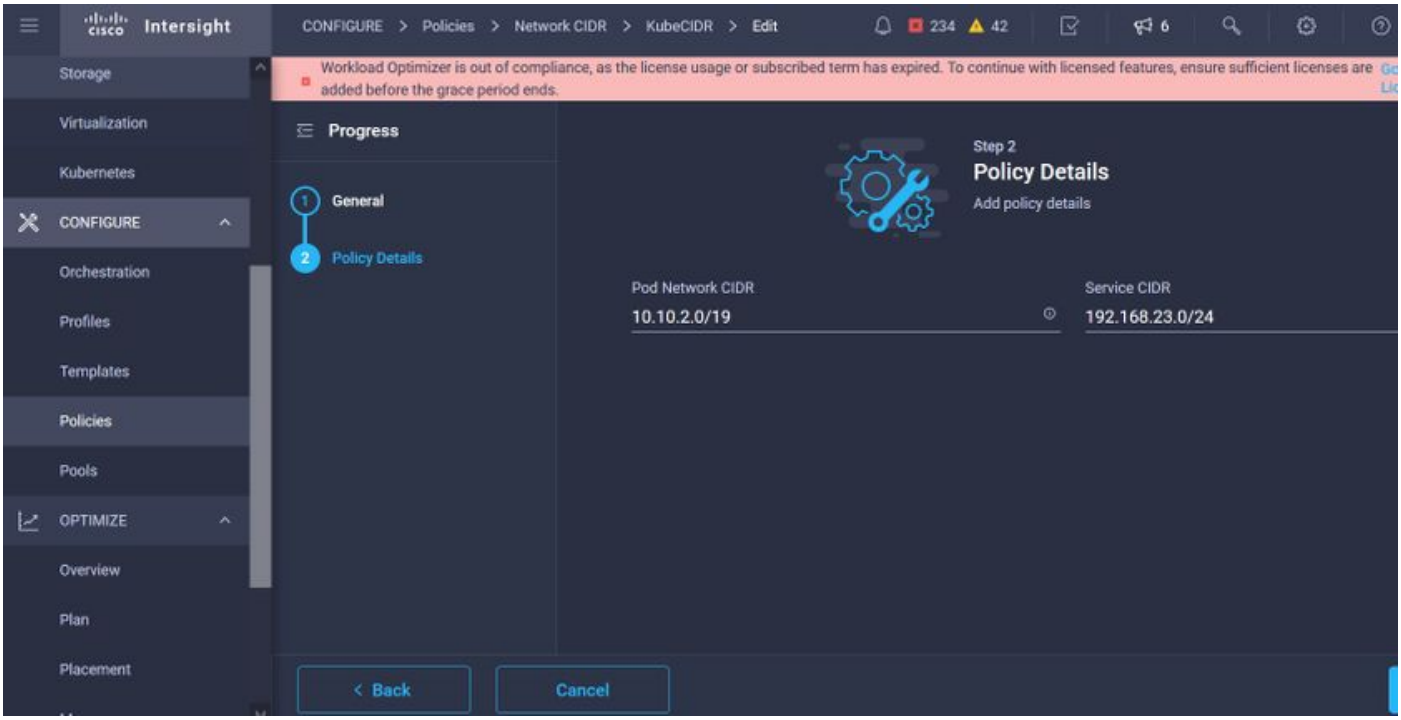
Algumas das políticas que precisamos configurar estão listadas abaixo. Observe que todas essas políticas seriam criadas na seção Configurar >> Políticas e Configurar >> Pools no Intersight.

Você também pode ver o caminho da política em cima de cada captura de tela, apresentado abaixo.

Esse pool de IPs será usado para endereços IP em suas máquinas virtuais de controle e nós de trabalho, quando iniciado no host ESXi.

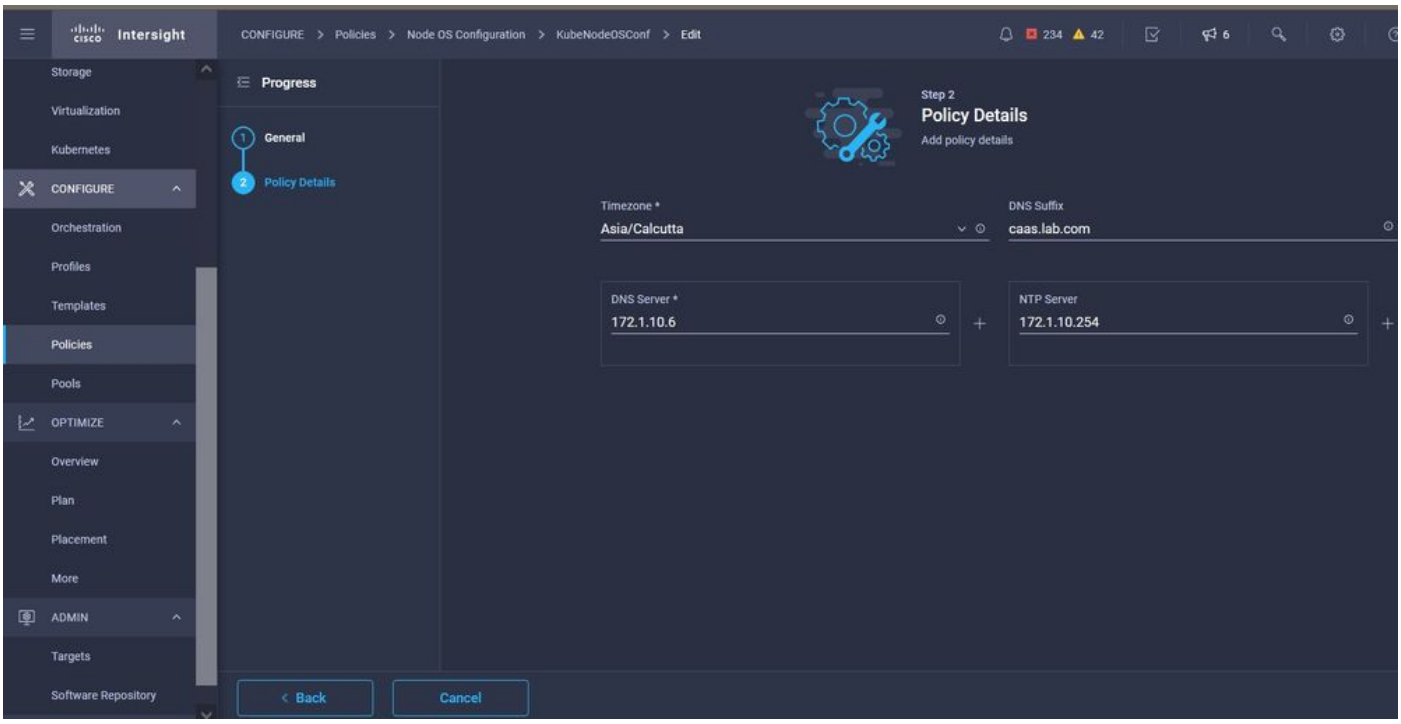


Aqui você define o CIDR da rede Pod and Services para redes internas no cluster Kubernetes.



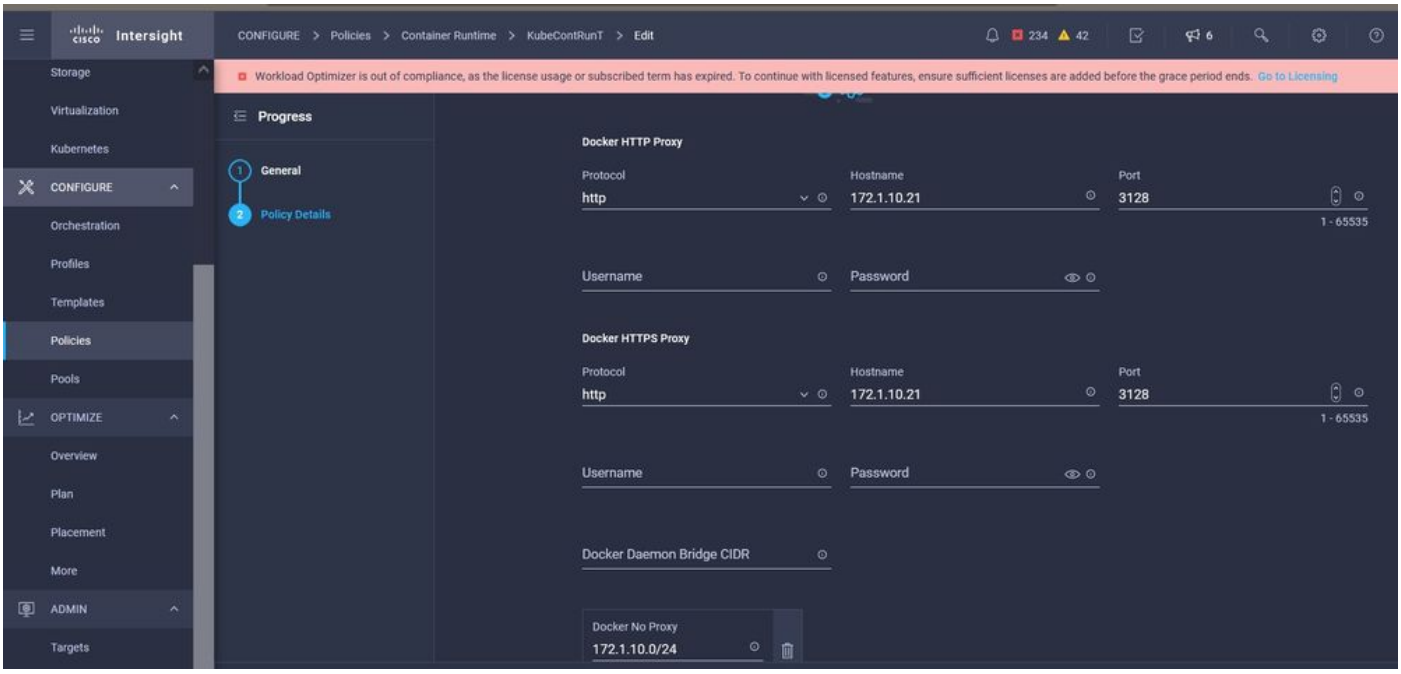
CIDR de serviços e rede

Essa política define sua configuração de NTP e DNS.



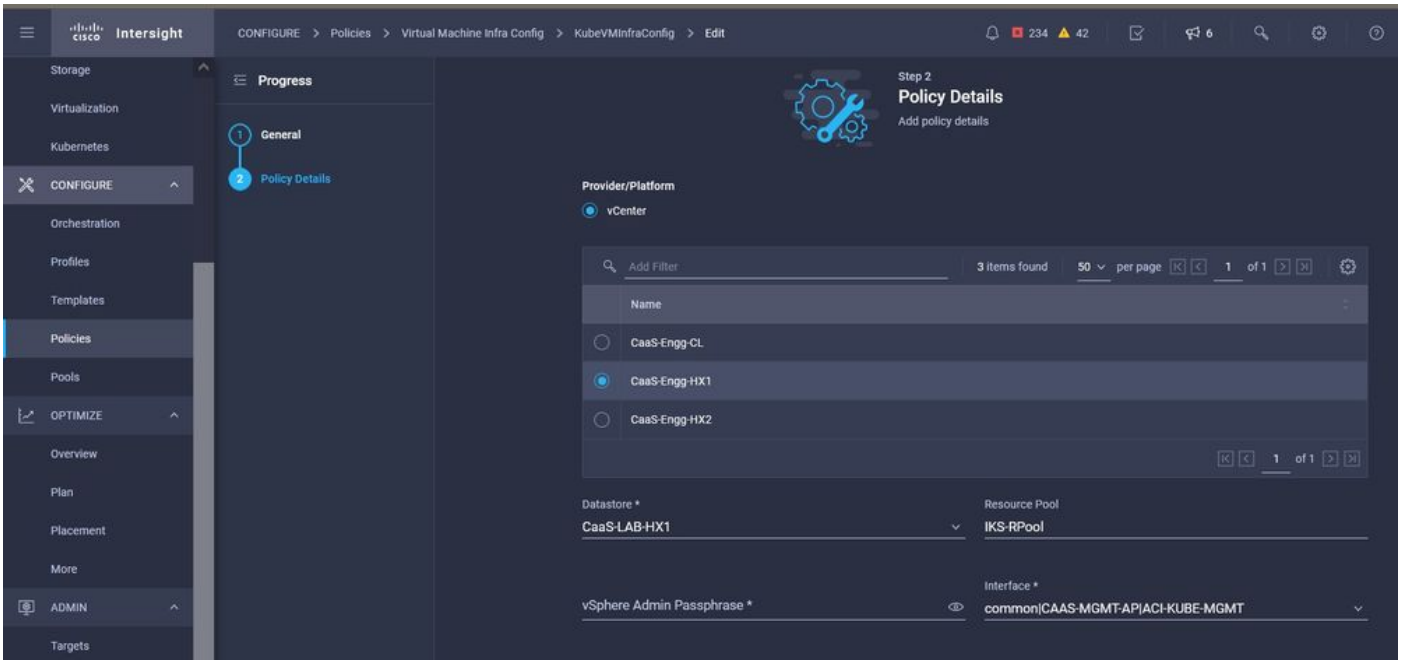
Configuração de NTP e DNS

Com essa política, você pode definir a configuração de proxy para o tempo de execução do contêiner do docker.



Configuração de proxy para Docker

Nesta política, você definirá a configuração necessária nas Máquinas virtuais implantadas como nós Master e Worker.



Configuração de VMs usadas

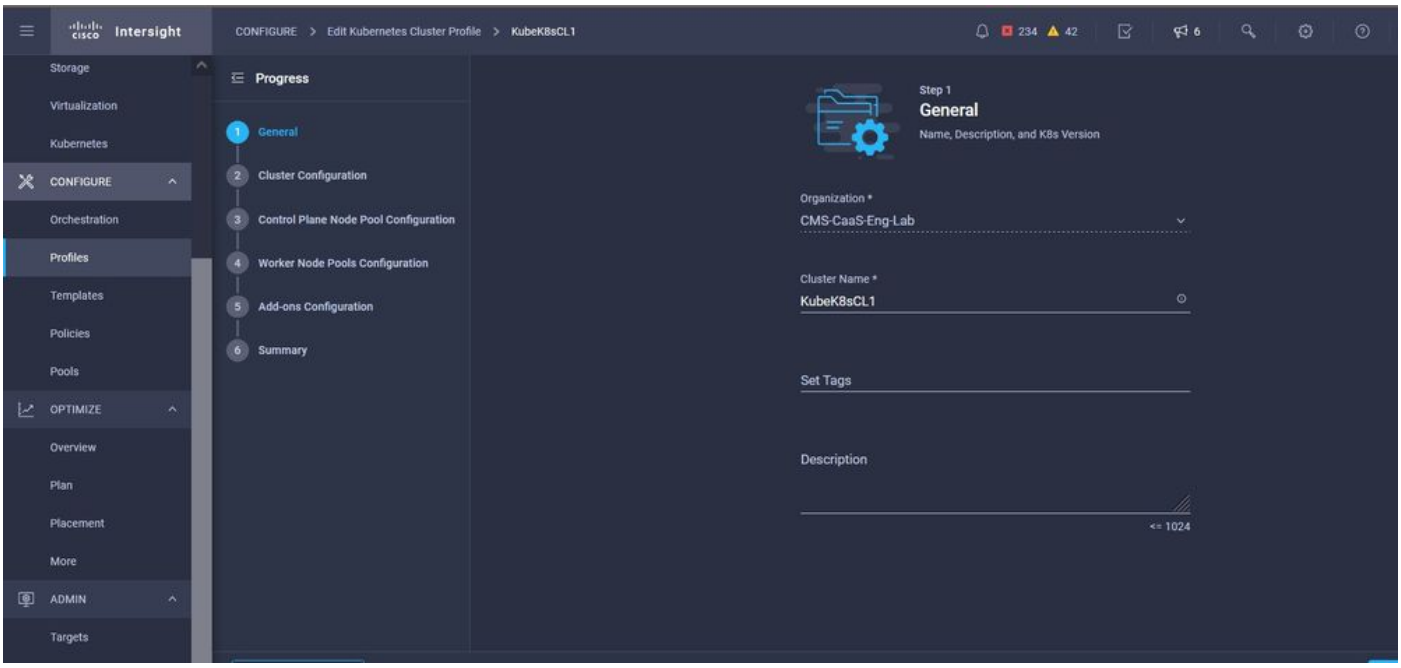
Etapa 2. Configurar perfil

Depois de criarmos as políticas acima, as vincularíamos a um perfil que poderíamos implantar.

A implantação da configuração usando políticas e perfis abstrai a camada de configuração para que ela possa ser implantada repetidamente rapidamente.

Você pode copiar esse perfil e criar um novo com pequenas ou mais modificações nas políticas subjacentes em minutos, para um ou mais clusters de Kubernetes em uma fração de tempo necessário com um processo manual.

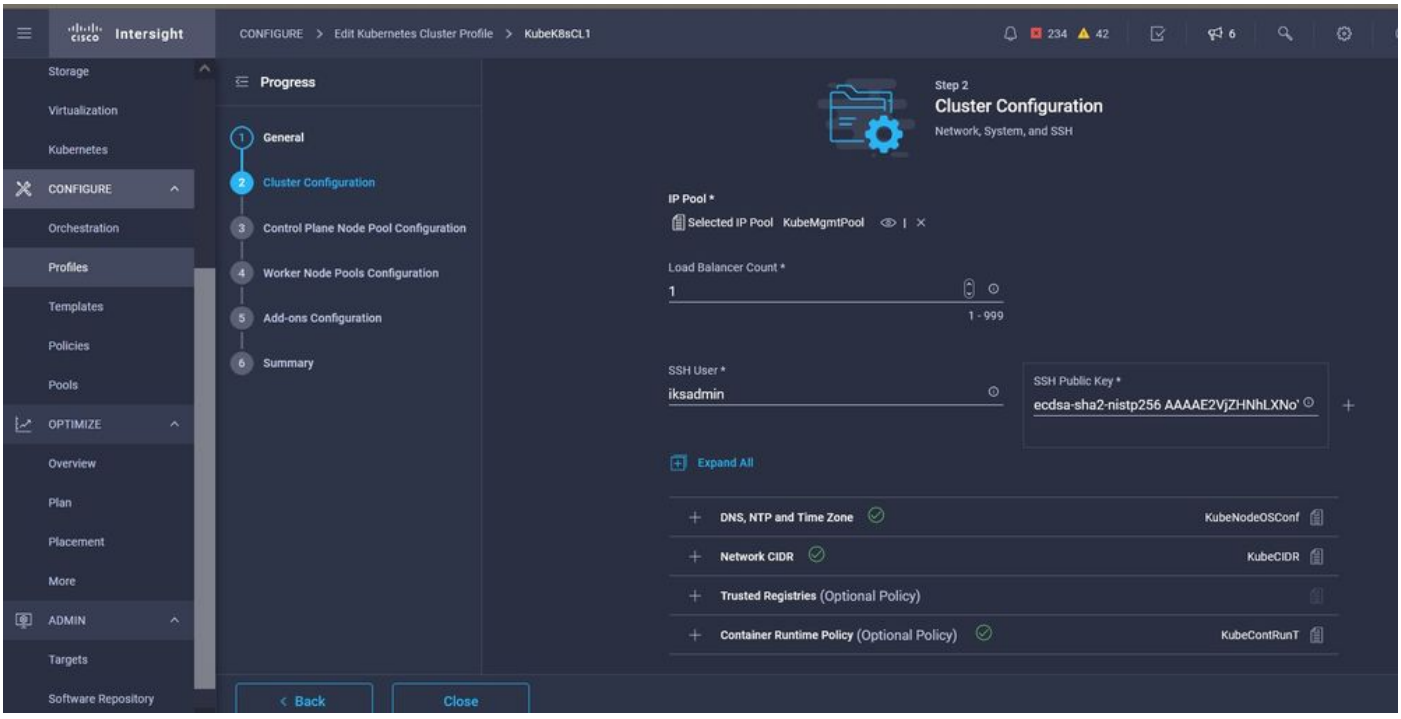
Ilustre o nome e defina marcas.



Configuração de perfil com nome e marcas

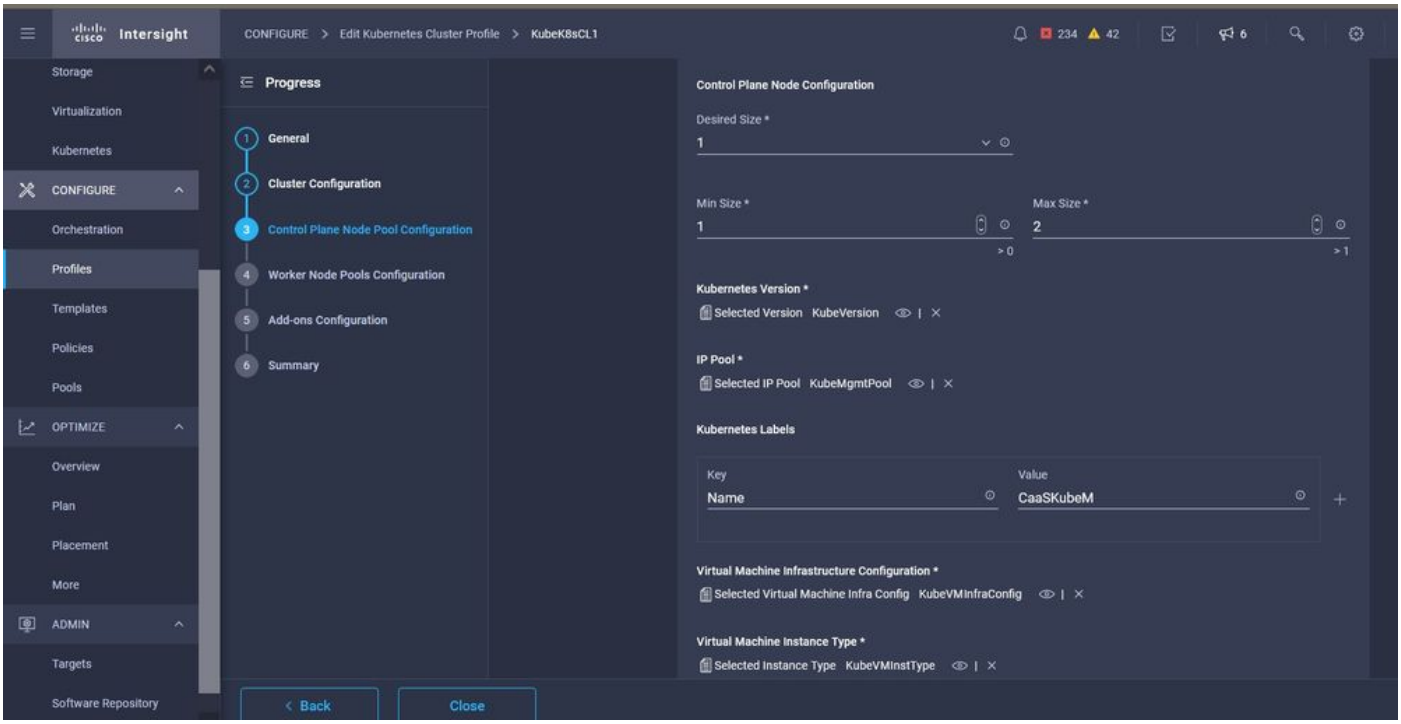
Defina as políticas de pool, SO de nó e CIDR de rede. Você também precisa configurar um ID de usuário e uma chave SSH (pública).

Sua chave privada correspondente seria usada para ssh nos nós Master & Worker.



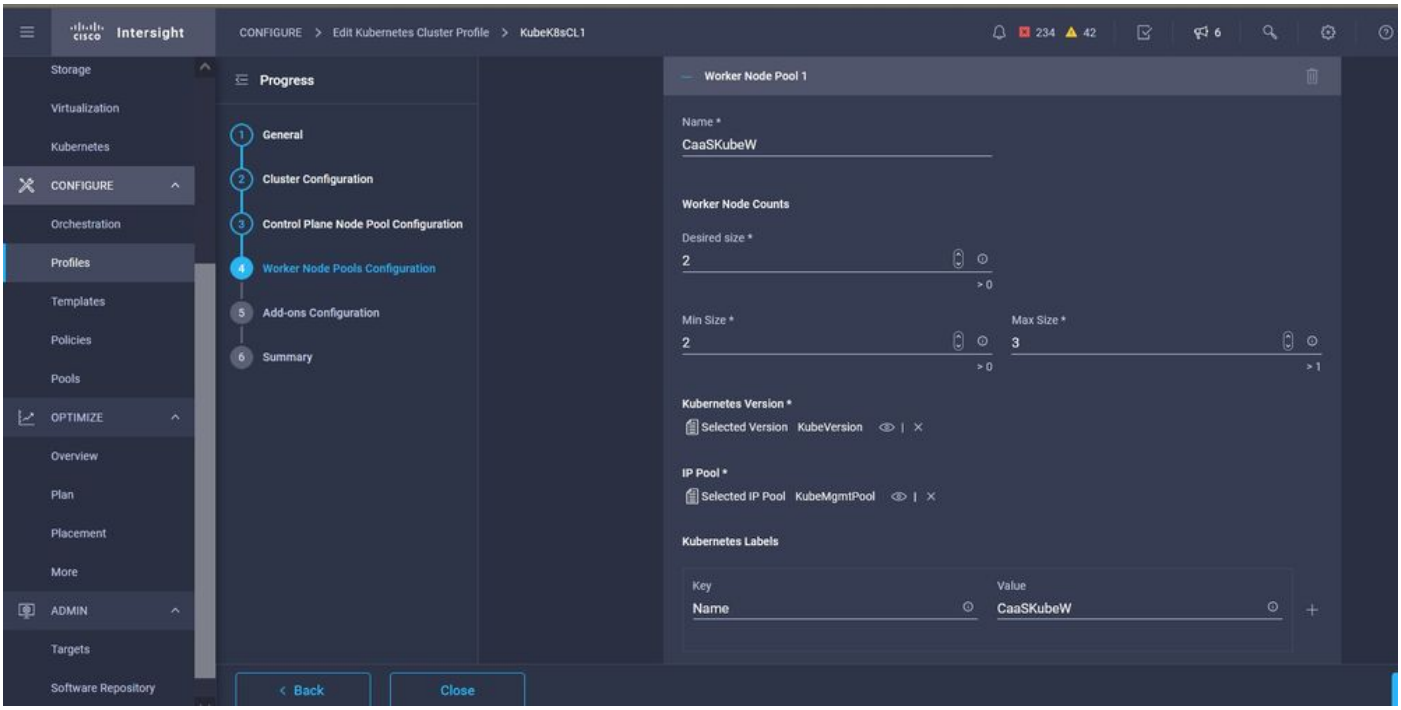
Configuração de perfil com políticas atribuídas

Configurar o plano de controle: Você pode definir quantos nós Master você precisaria no plano de controle.



Configuração do nó mestre

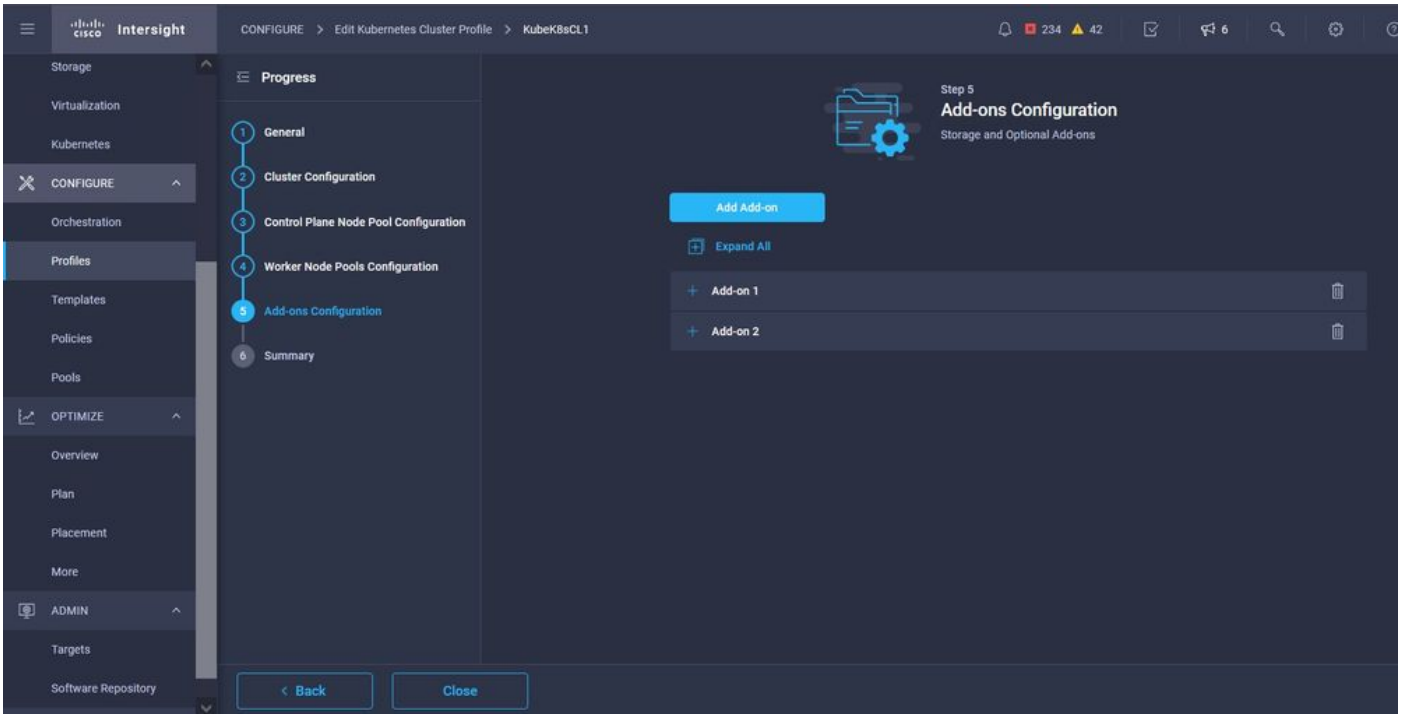
Configure os nós do Worker: Dependendo dos requisitos do aplicativo, você pode escalar ou escalar seus nós de trabalho.



configuração de nós de trabalhador

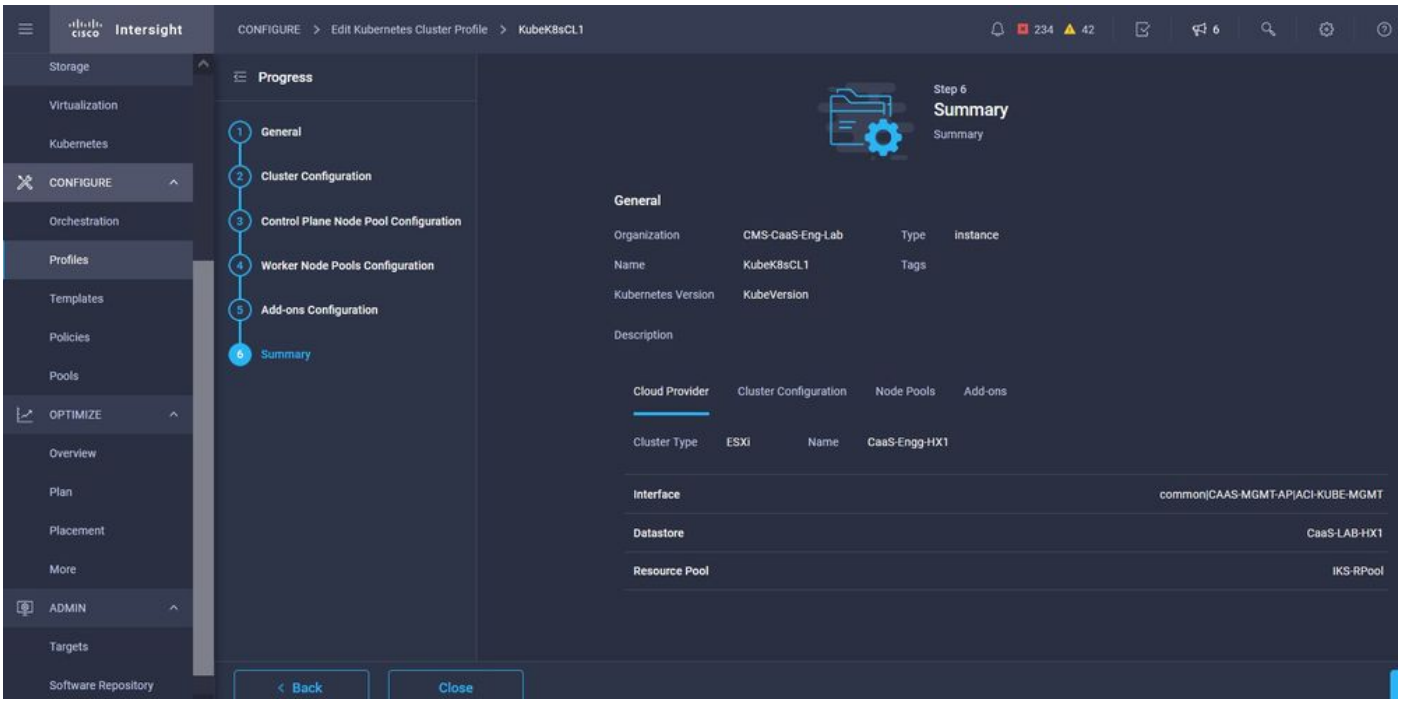
Configure o complemento. A partir de agora, você pode implantar automaticamente o Kubernetes Dashboard e o Graffana com monitoramento Prometheus.

No futuro, você pode adicionar mais complementos que podem ser implantados automaticamente usando o IKS.



Adicionar complementos se houver

Marque Resumo e clique em **Implantar**.

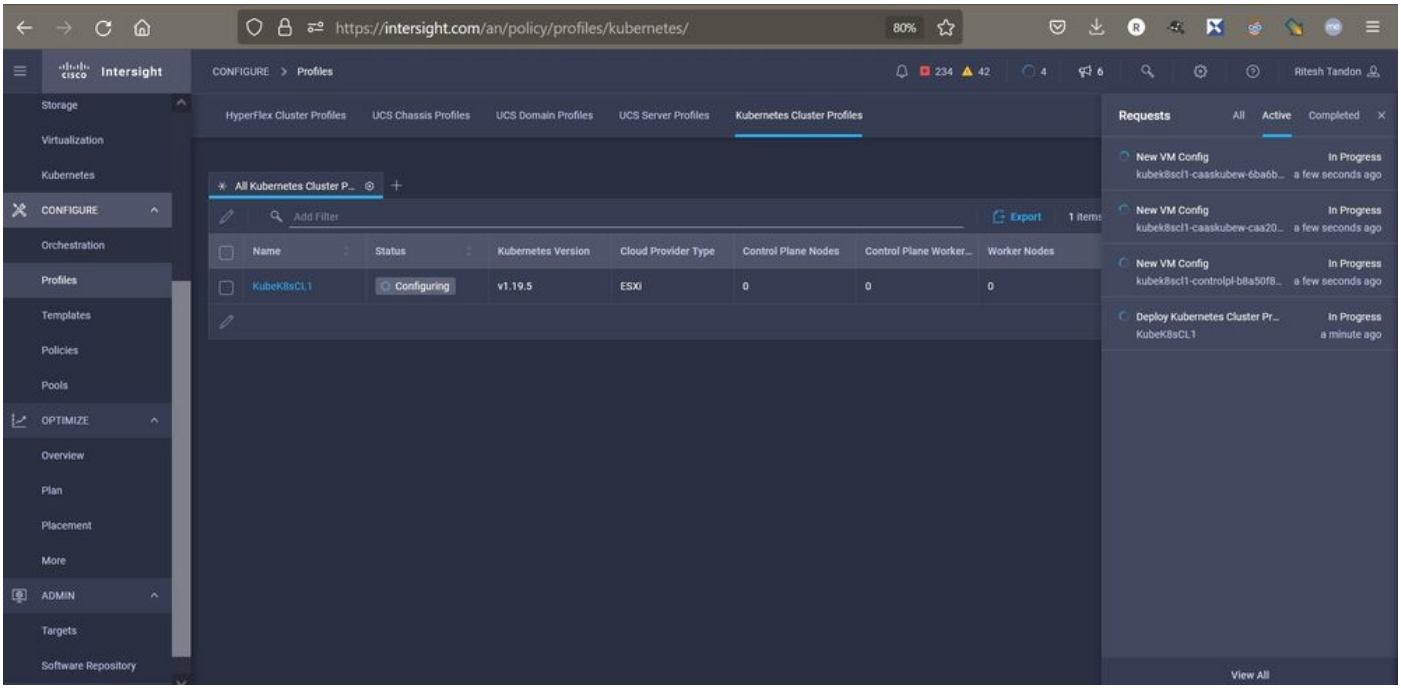


Tela Resumo da criação do perfil

Verificar

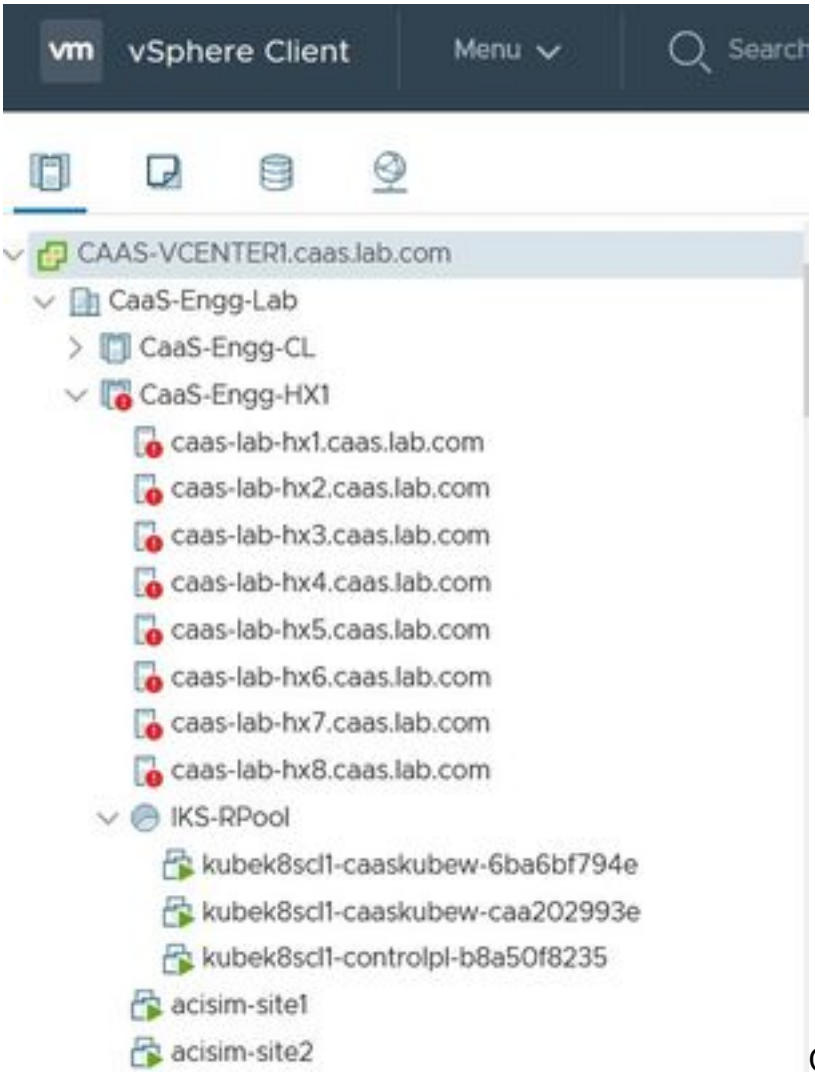
Use esta seção para confirmar se a sua configuração funciona corretamente.

No lado superior direito, você pode acompanhar o progresso da implantação.



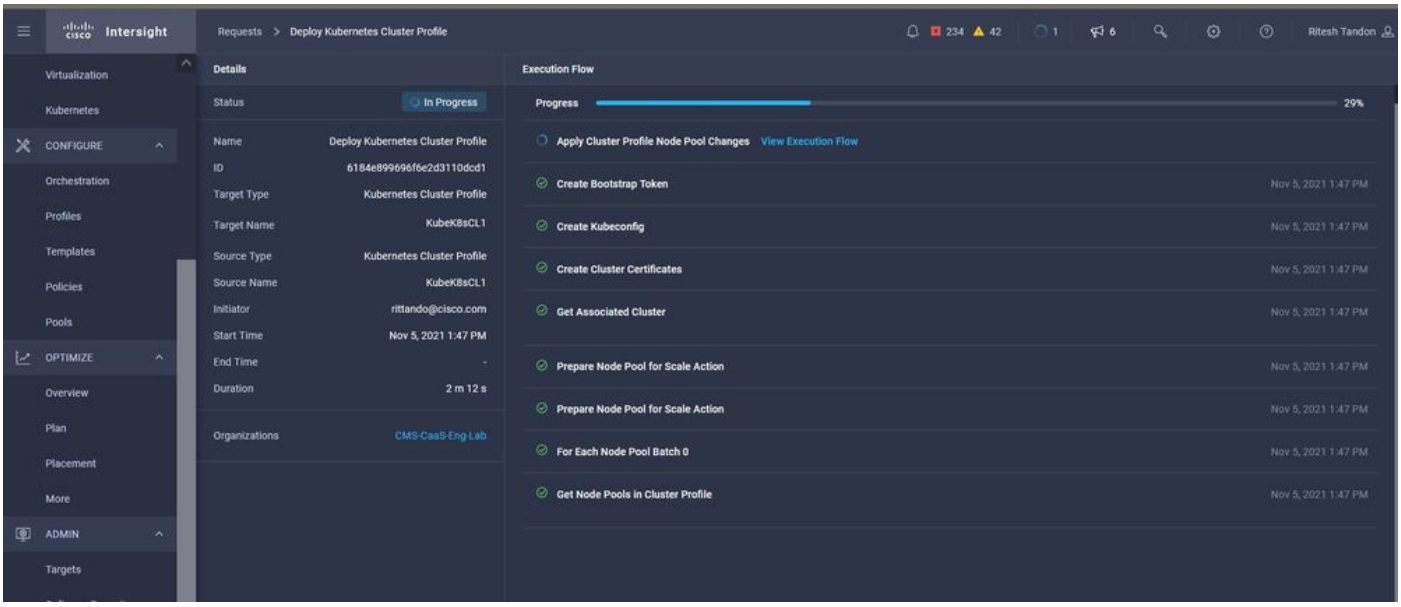
Verificar usando a GUI do IKS

Àmedida que a implantação progride, você pode ver seus nós Kubernetes Master e Worker surgindo no vCenter.



Cluster IKS no vCenter

Caso precise ver as etapas detalhadas para a implantação, você pode detalhar a execução.



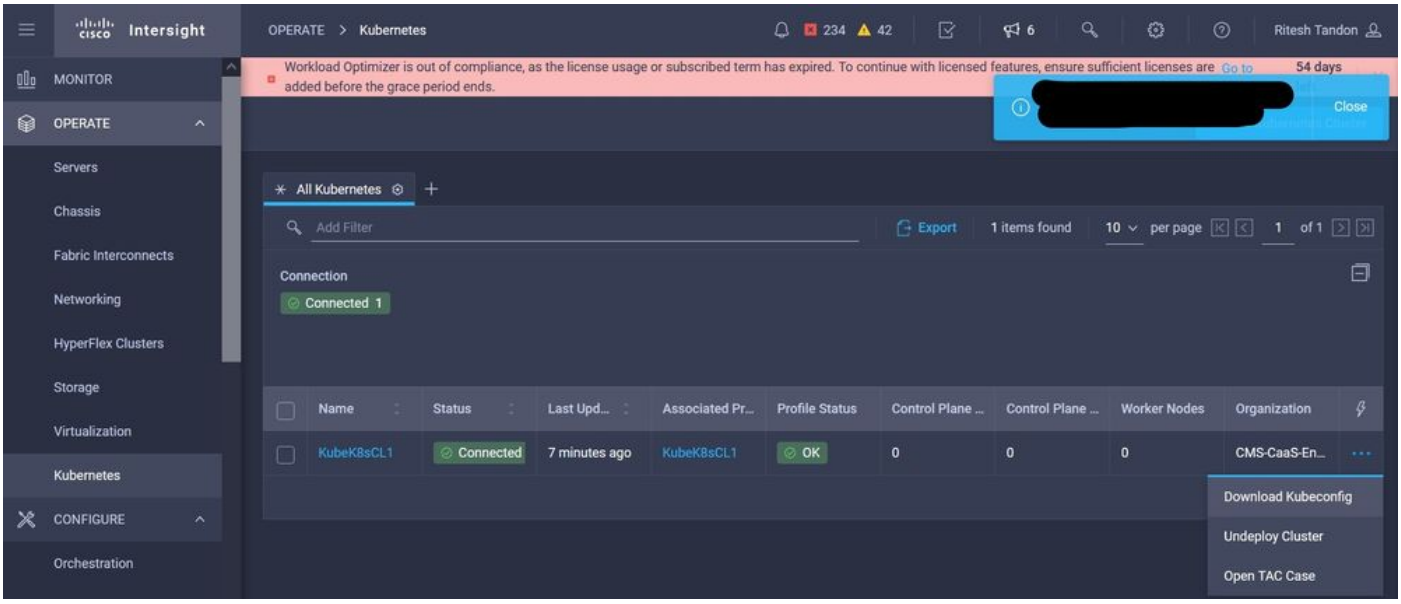
Execução de criação de perfil

Conectar-se ao cluster Kubernetes

Você pode se conectar ao cluster Kubernetes das seguintes maneiras:

Usando o arquivo KubeConfig, que você pode baixar de **Operate > Kubernetes > Selecione as opções na extrema direita**.

Você precisa ter o KubeCtl instalado na estação de trabalho Management, de onde deseja acessar esse cluster.



Baixar arquivo KubeConfig do IKS

Você também pode fazer SSH diretamente no nó mestre, usando aplicativos SSH como Putty com as credenciais e chave privada configuradas no momento da implantação

Se você implantar o 'Painel de Kubernetes' como um complemento, você também poderá usá-lo para implantar aplicativos diretamente usando a GUI.

Para verificar mais detalhes, consulte a seção 'Acessando clusters de Kubernetes', aqui:

Verificar com CLI

Depois de conseguir se conectar ao cluster Kubernetes, usando o kubeCtl, você poderá usar os seguintes comandos para verificar se o cluster tem todos os componentes instalados e em execução.

Verifique se os nós no cluster estão em um estado 'pronto'.

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

Verifique o status dos pods criados no momento da instalação dos componentes essenciais no cluster.

```
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 o status do pod do operador ccp-helm que gerencia o helm que está executando localmente e instala 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 o status dos pods Essential* que gerenciam os complementos Essential (core), instalados por padrão, em cada cluster de espaço 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 o status dos serviços e do balanceador de carga implantados no namespace 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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Caso um pod específico não esteja sendo exibido, você pode usar esses comandos para detalhar a causa.

```
Syntax : kubectl describe pod
```

Informações Relacionadas

- Verifique o resumo do serviço IKS aqui.
- Verifique o Guia do usuário aqui.
- Verifique a demonstração do Intersight Kubernetes Service aqui.
- Suporte Técnico e Documentação - Cisco Systems