Configurazione del cluster Kubernetes mediante Intersight Kubernetes Service

Sommario

Introduzione

Questo documento descrive la configurazione per il provisioning di un cluster Kubernetes di produzione da Cisco Intersight (SaaS) con l'utilizzo di Cisco Intersight™ Kubernetes Service (IKS).

Premesse

Kubernetes, in tempi recenti, è diventato di fatto uno strumento di gestione dei contenitori, in quanto le organizzazioni tendono ad investire maggiormente nella modernizzazione delle applicazioni con soluzioni container. Con Kubernetes, i team di sviluppo possono distribuire, gestire e scalare le applicazioni in container con facilità, rendendo le innovazioni più accessibili alle pipeline di distribuzione continua.

Kubernetes, tuttavia, si trova ad affrontare sfide operative, in quanto richiede tempo e competenze tecniche per l'installazione e la configurazione.
L'installazione di Kubernetes e dei diversi componenti software richiesti, la creazione di cluster, la configurazione di storage, reti e sicurezza, nonché le operazioni (ad esempio l'aggiornamento, l'aggiornamento e l'applicazione di patch ai bug critici relativi alla sicurezza) richiedono un investimento significativo in capitale umano.

IKS è una soluzione SaaS chiavi in mano per la gestione di Kubernetes coerenti e di livello produttivo ovunque. Per ulteriori informazioni sulle funzionalità di IKS, fare clic qui su questo collegamento.

Panoramica della soluzione

Per questo documento, l'idea è quella di mostrare la capacità di IKS di integrarsi perfettamente con l'infrastruttura locale, eseguendo VMware ESXi e vCenter.
Con pochi clic è possibile installare un cluster Kubernetes di livello produzione nell'infrastruttura VMware.

Tuttavia, per fare ciò è necessario integrare il vCenter locale con Intersight, noto come 'claim a target', dove vCenter è l'obiettivo.
Ènecessaria un'appliance virtuale Cisco Intersight Assist, che consente di aggiungere destinazioni endpoint a Cisco Intersight. È possibile installare Intersight Assist utilizzando l'OAV bootstrap disponibile sul sito Web ufficiale di Cisco.

Per limitare l'ambito di questo documento, non ci concentreremo sull'installazione di Cisco Intersight Assist Virtual Appliance. Ma qui potete dare un'occhiata al processo

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Account Intersight: Hai bisogno di un ID Cisco valido e di un account Intersight.
  Se non ne disponi, puoi creare un ID Cisco sul sito Web di Cisco. Quindi clicca sul link Crea un account su Intersight.
- Cisco Intersight Assist: Cisco Intersight Assist consente di aggiungere vCenter/ESXi come destinazione endpoint a Cisco Intersight.
- Connettività: Se l'ambiente supporta un proxy HTTP/S, è possibile utilizzarlo per connettere Cisco Intersight Assist Appliance a Internet. In alternativa, è necessario aprire le porte agli URL di intervista. Per informazioni dettagliate sui requisiti di connettività di rete, controllare questo collegamento:
- Credenziali vCenter per rivendicarlo su Intersight.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Presupposti

Poiché l'implementazione di un'appliance Cisco Intersight non rientra nell'ambito di questo documento.

Si presume che l'utente disponga già di un account Intersight funzionante e che abbia richiesto un vCenter/Esxi locale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

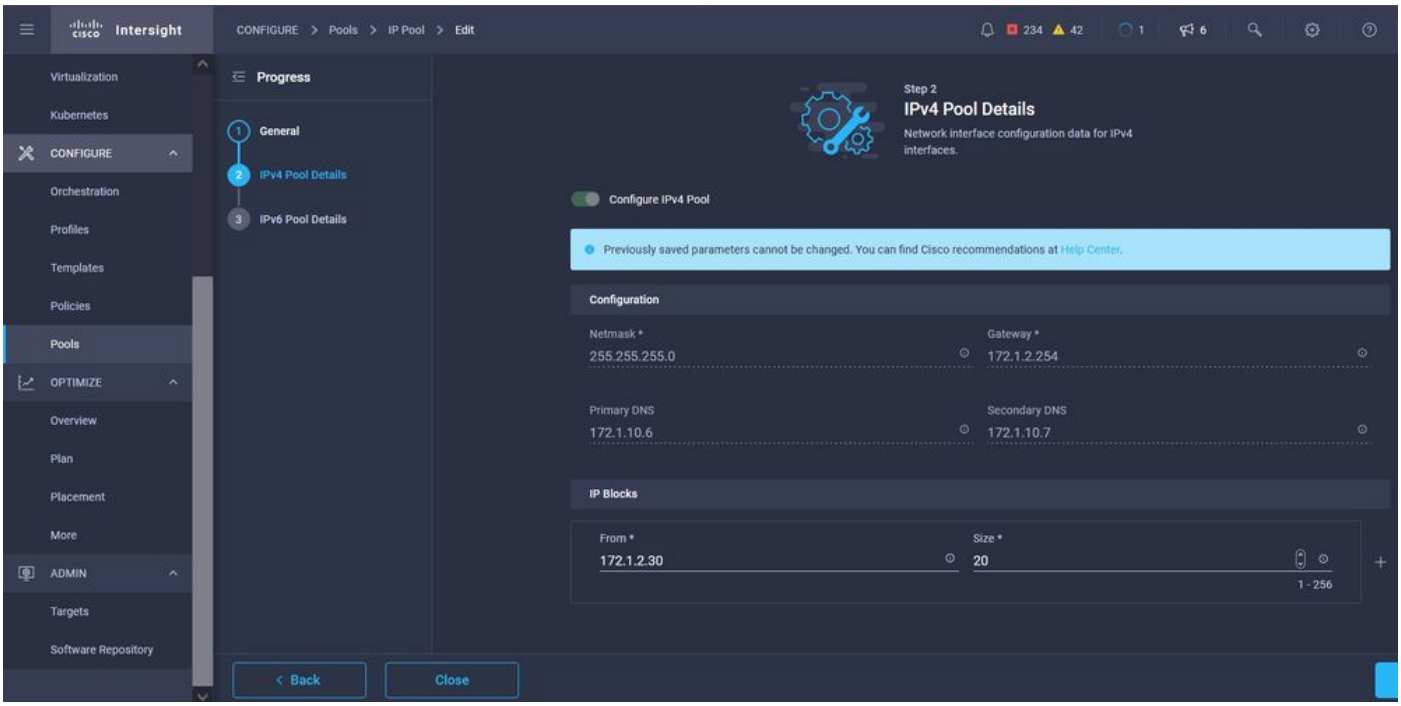
Passaggio 1. Configurare i criteri

Le regole consentono una gestione semplificata in quanto astraggono la configurazione in modelli riutilizzabili.

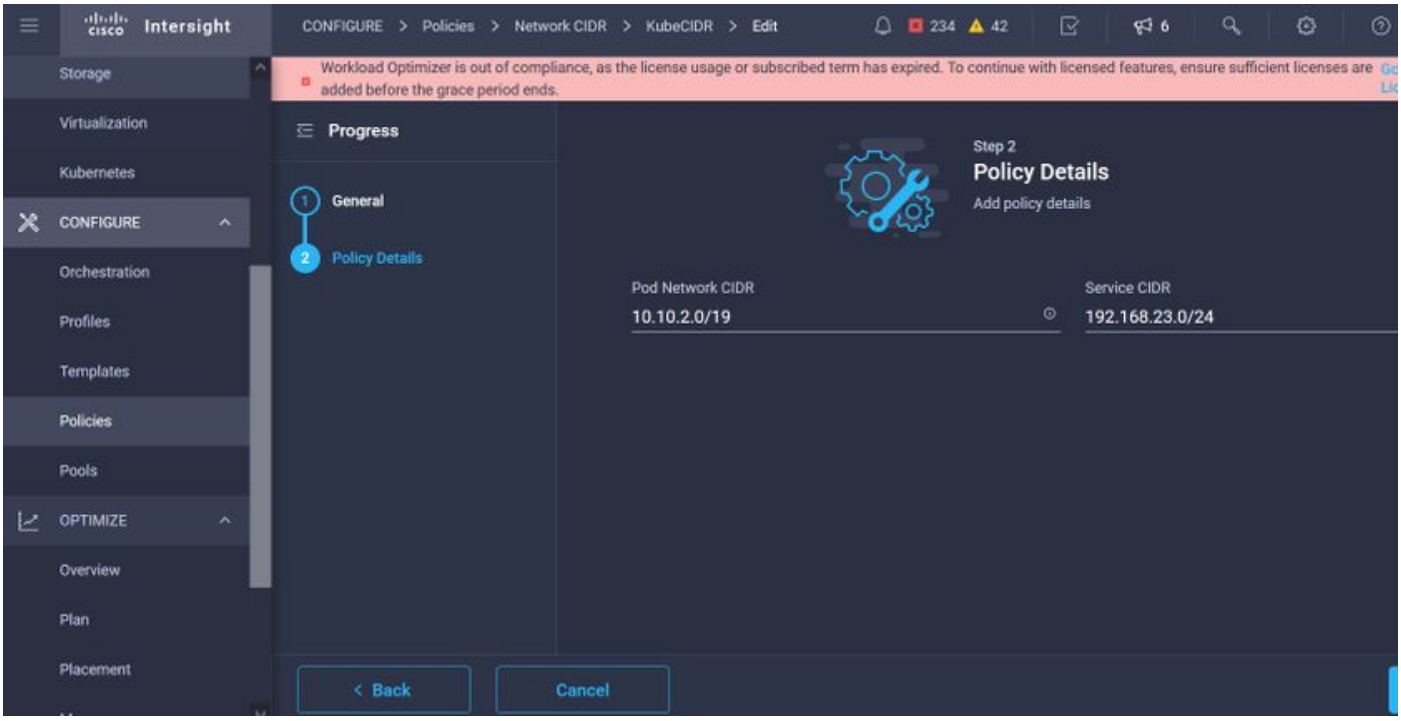
Di seguito sono elencati alcuni dei criteri da configurare. Tutte queste policy verrebbero create nella sezione Configura >> Criteri e configura >> Pool in Intersight.

Puoi vedere il percorso del criterio anche sopra ogni schermata, indicato di seguito.

Questo pool IP verrà utilizzato per gli indirizzi IP sui sistemi virtuali dei nodi di controllo e di lavoro, quando viene avviato sull'host ESXi.

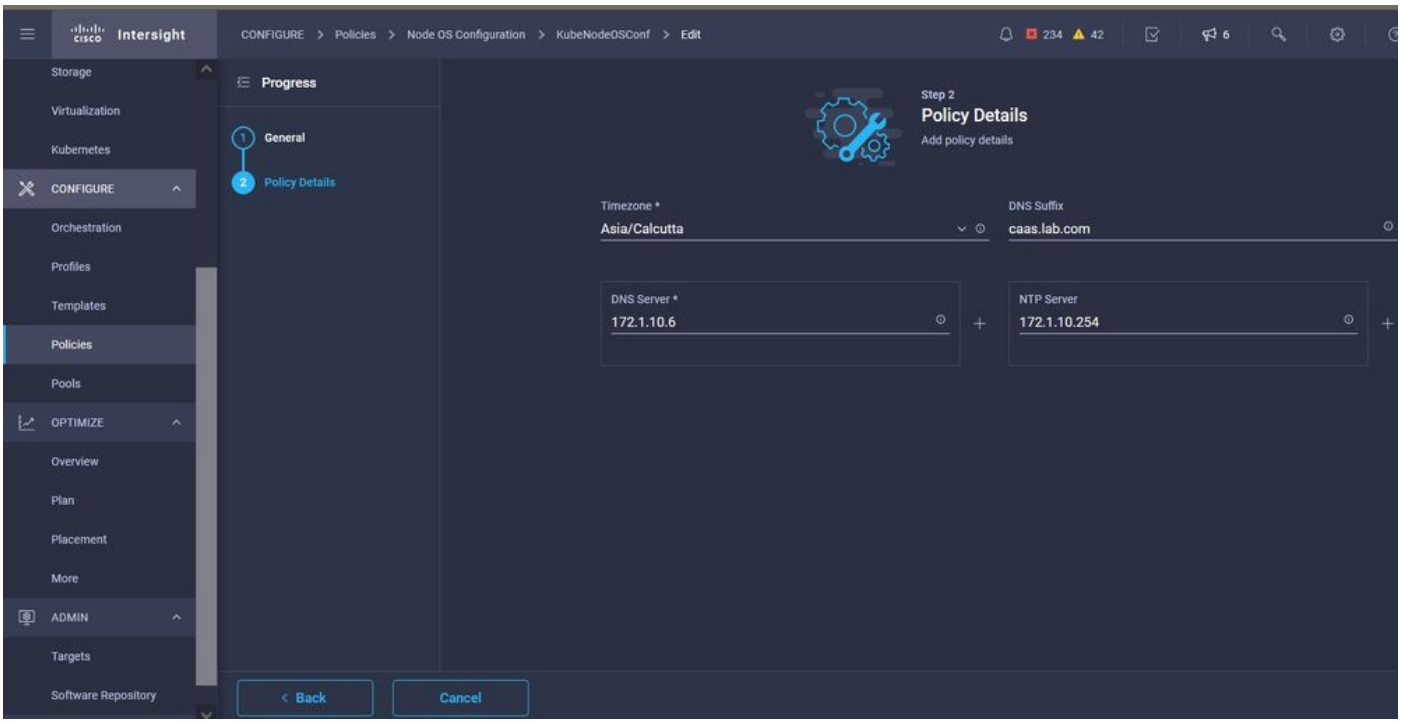


Qui si definisce il POD e la rete di servizi CIDR, per le reti interne all'interno del cluster Kubernetes.



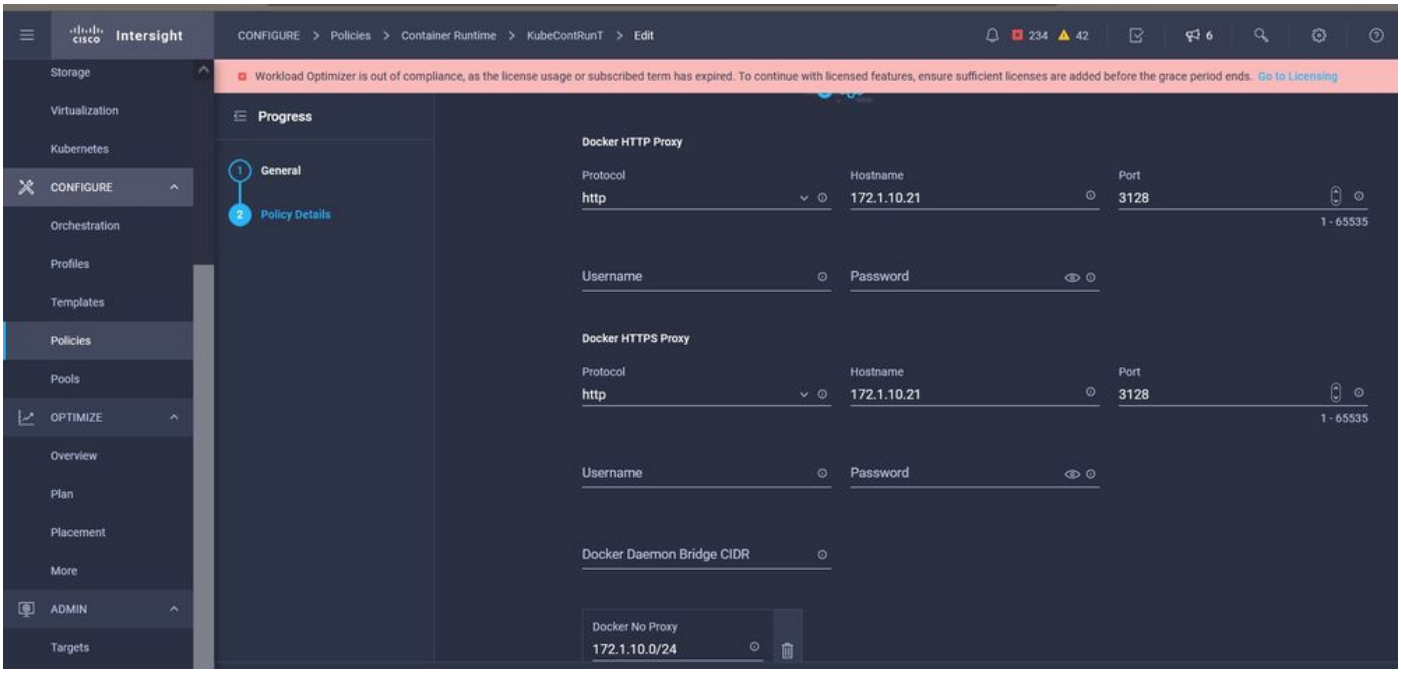
Services and Network CIDR

Questo criterio definisce la configurazione NTP e DNS.



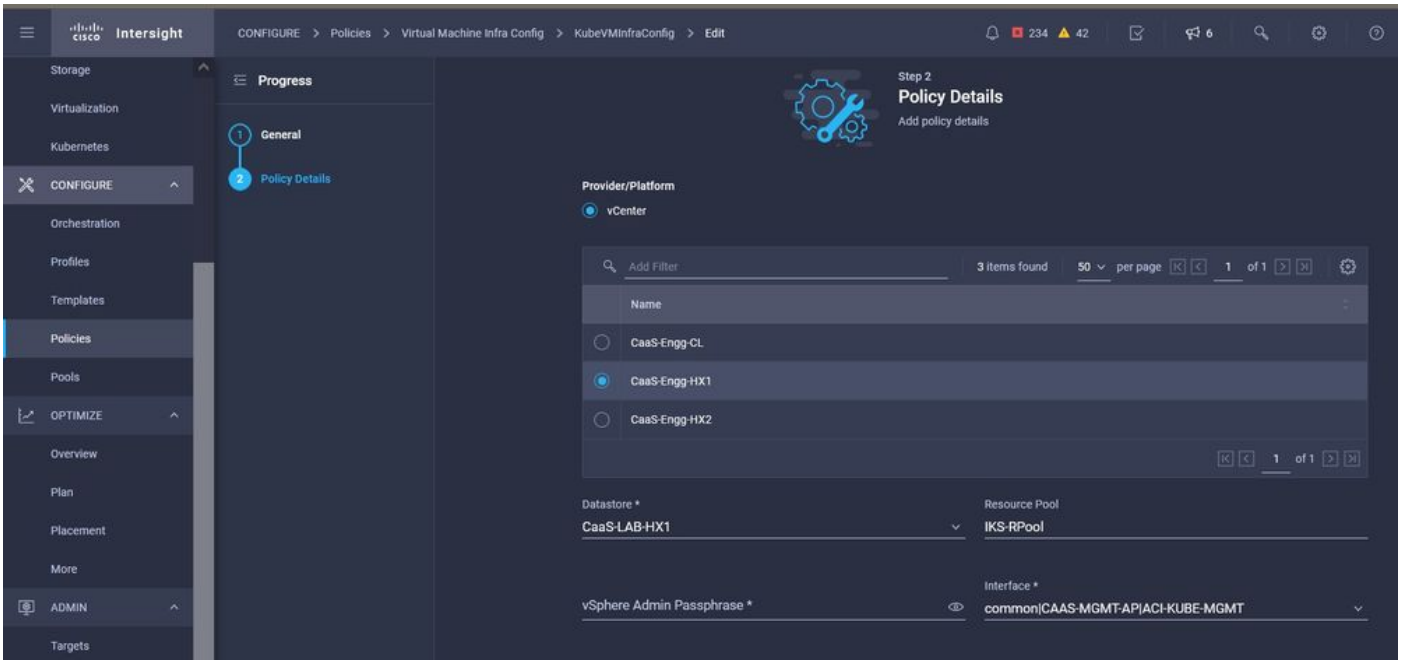
Configurazione NTP e DNS

Con questo criterio è possibile definire la configurazione proxy per il runtime del contenitore docker.



Configurazione proxy per Docker

In questo criterio viene definita la configurazione necessaria sulle macchine virtuali distribuite come nodi Master e Worker.



Configurazione delle VM utilizzate

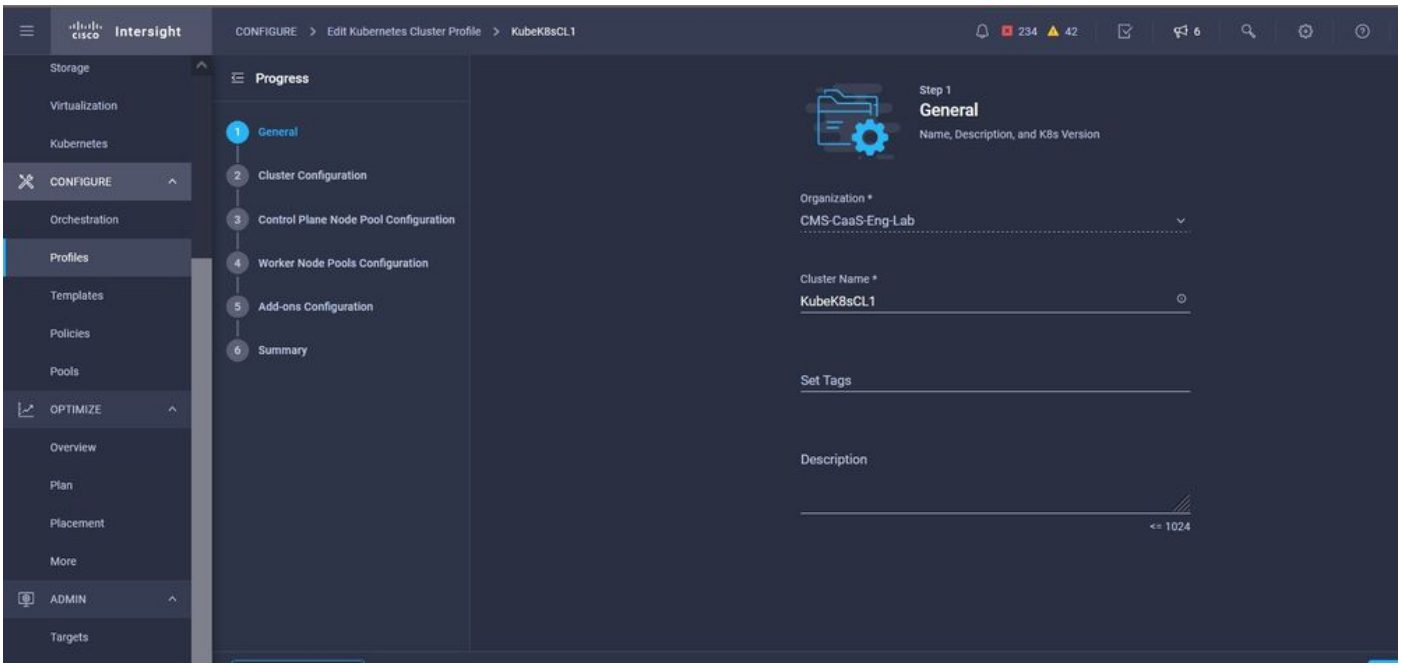
Passaggio 2. Configurare il profilo

Una volta create le politiche sopra descritte, le vincoleremmo in un profilo che potremo poi distribuire.

La distribuzione della configurazione mediante criteri e profili astrae il livello di configurazione in modo che possa essere distribuito più volte e rapidamente.

In pochi minuti è possibile copiare questo profilo e crearne uno nuovo con poche o più modifiche ai criteri sottostanti, in uno o più cluster Kubernetes attivi in una frazione di tempo necessaria con un processo manuale.

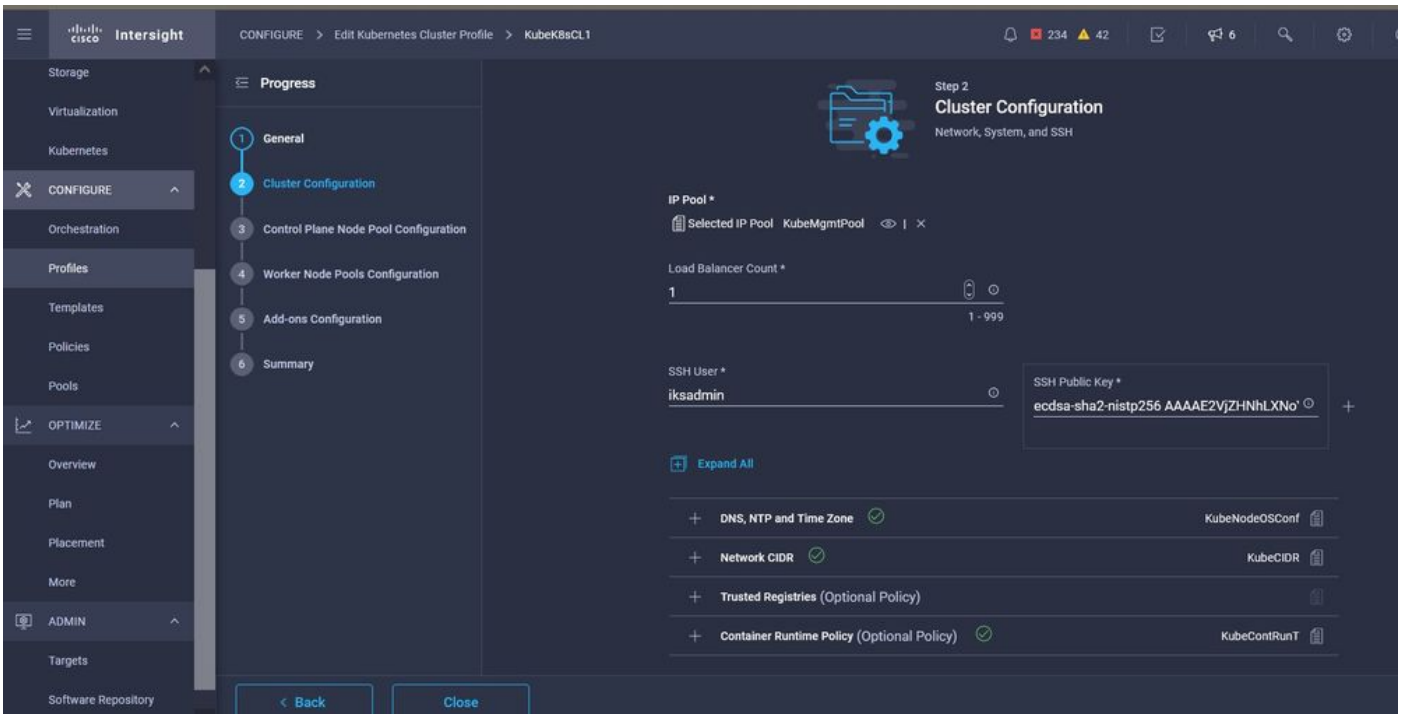
Visualizzare in Nome e impostare Tag.



Configurazione profilo con nome ed etichette

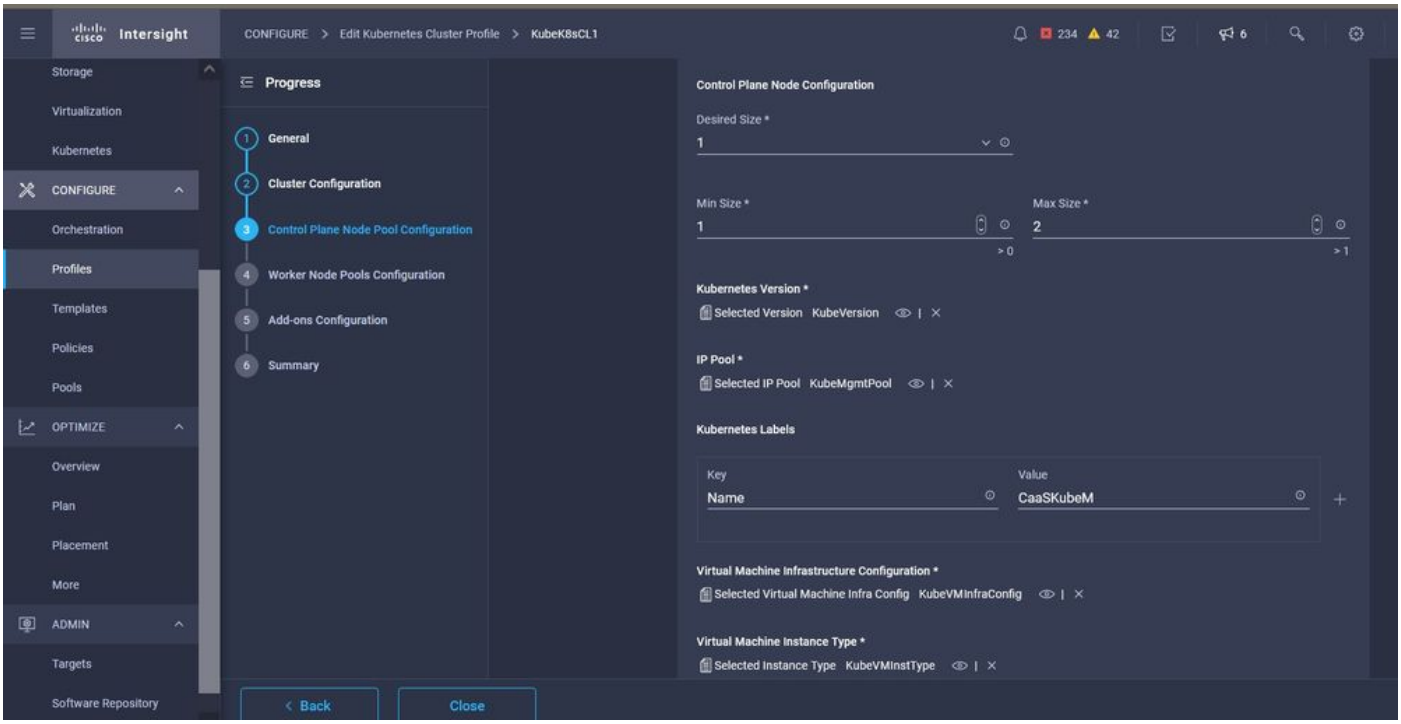
Impostare il pool, il sistema operativo dei nodi e i criteri CIDR di rete. Inoltre, è necessario configurare un ID utente e una chiave SSH (pubblica).

La chiave privata corrispondente verrebbe utilizzata per eseguire il protocollo ssh nei nodi Master & Worker.



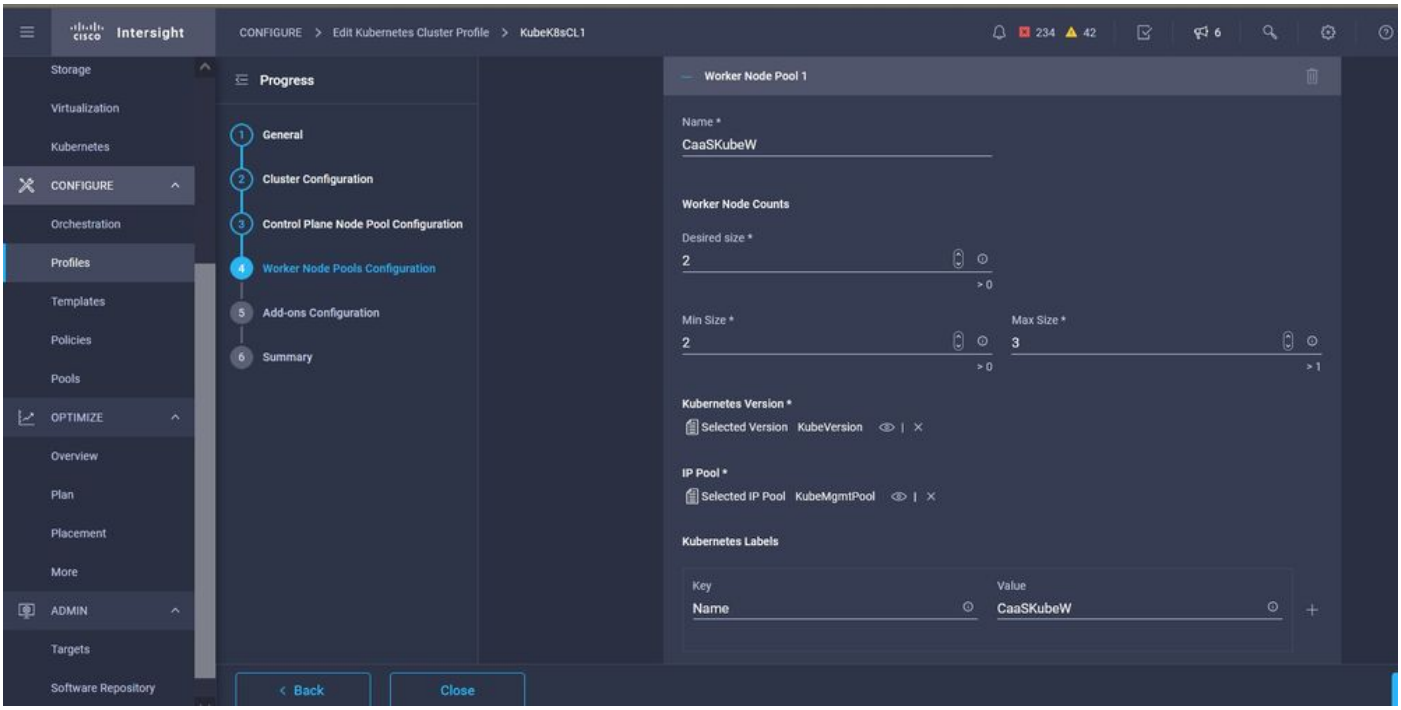
Configurazione profilo con criteri assegnati

Configurare il Control Plane: È possibile definire il numero di nodi principali necessari sul piano di controllo.



Configurazione nodo master

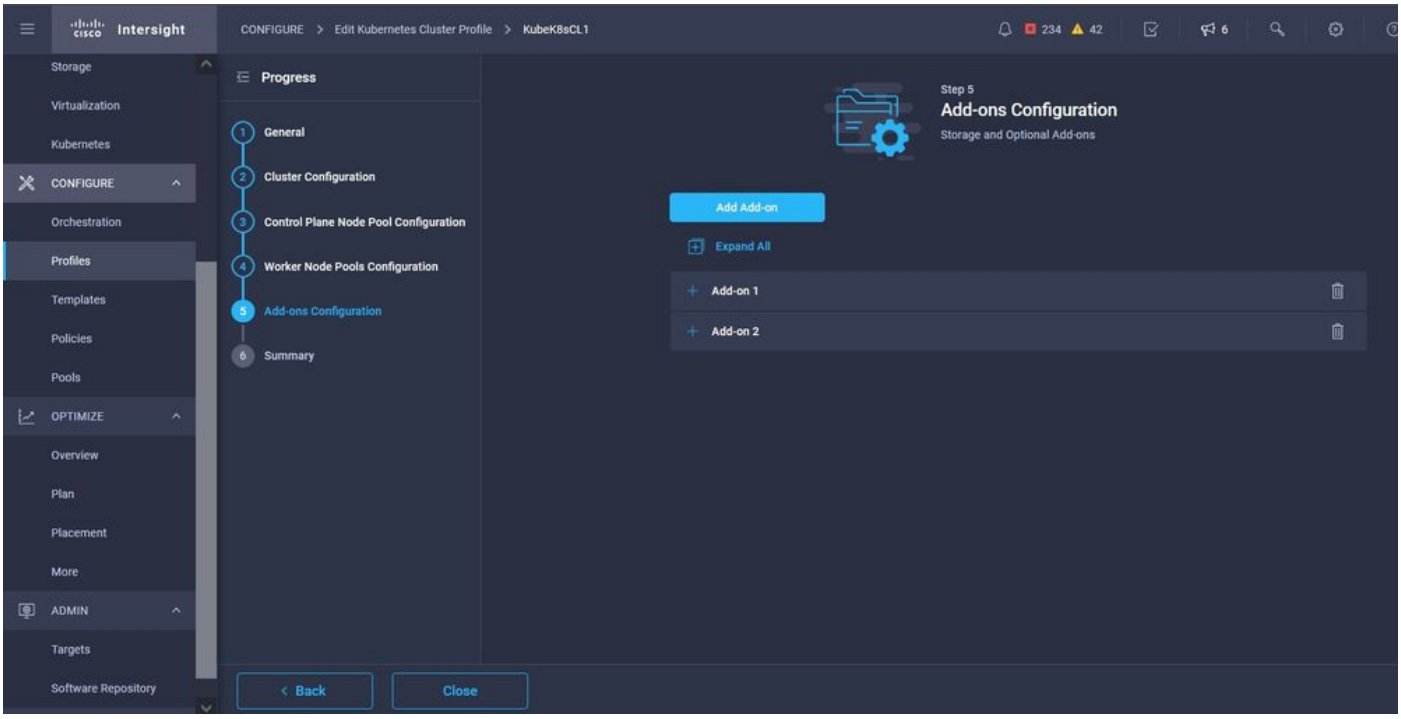
Configurare i nodi Worker: A seconda dei requisiti dell'applicazione, è possibile aumentare o ridurre la scalabilità dei nodi di lavoro.



Configurazione nodi Worker

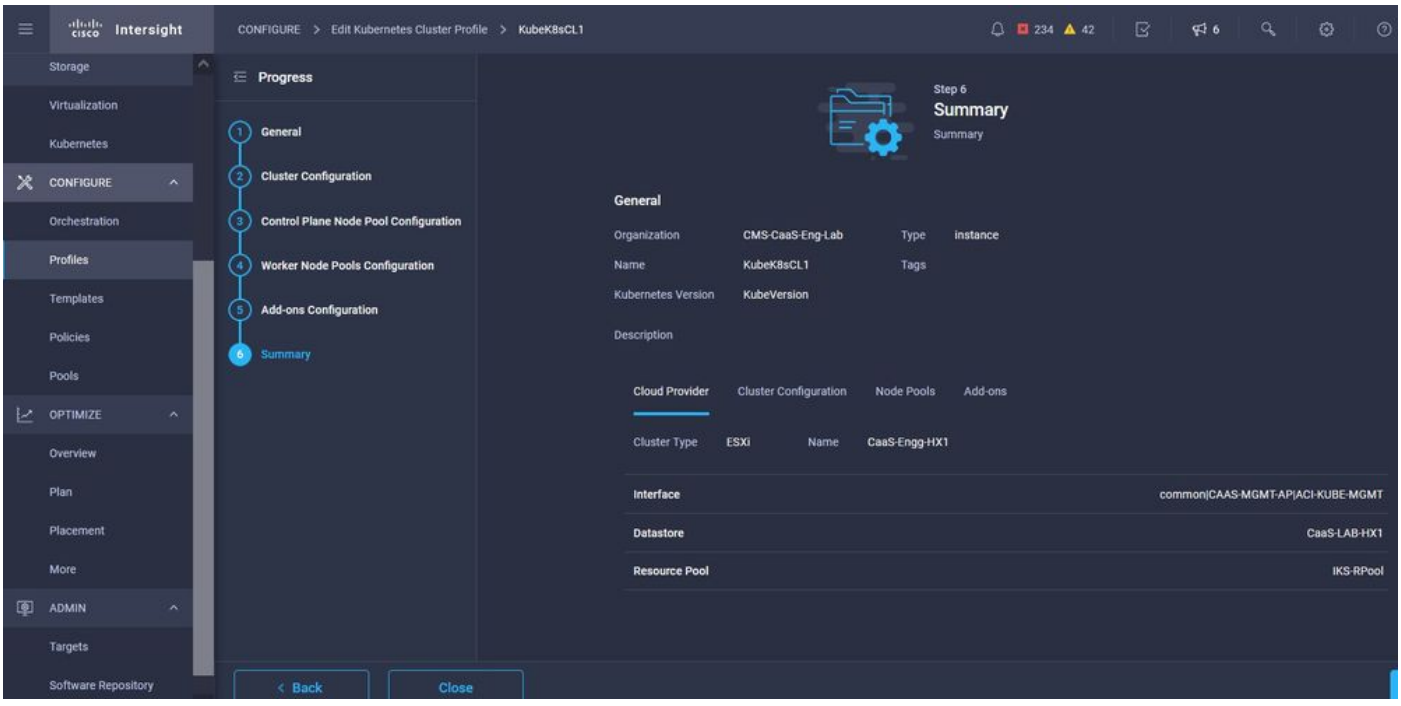
Configurare il componente aggiuntivo. Da ora, è possibile installare automaticamente, Kubernetes Dashboard e Graffana con monitoraggio Prometheus.

In futuro, sarà possibile aggiungere altri componenti aggiuntivi da distribuire automaticamente utilizzando IKS.



Aggiungi eventuali componenti aggiuntivi

Controllare il riepilogo e fare clic su **Distribuisci**.

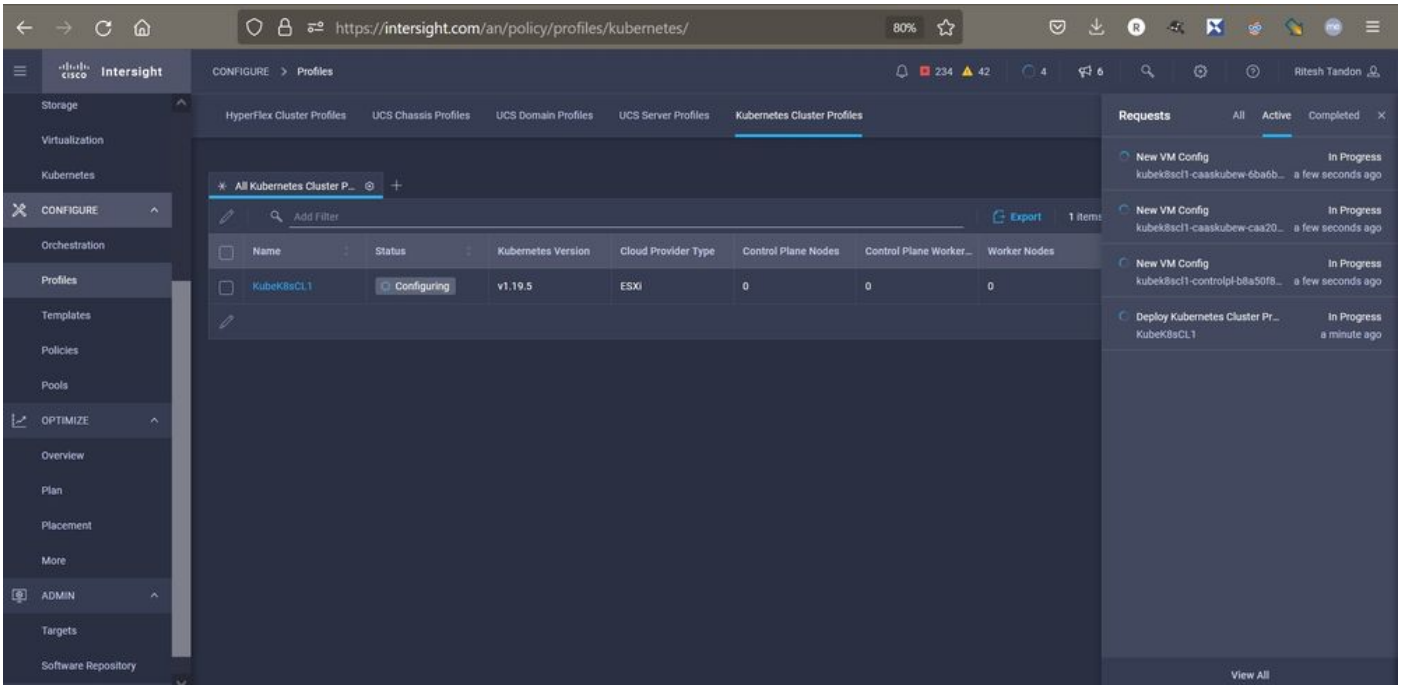


schermata Riepilogo creazione profilo

Verifica

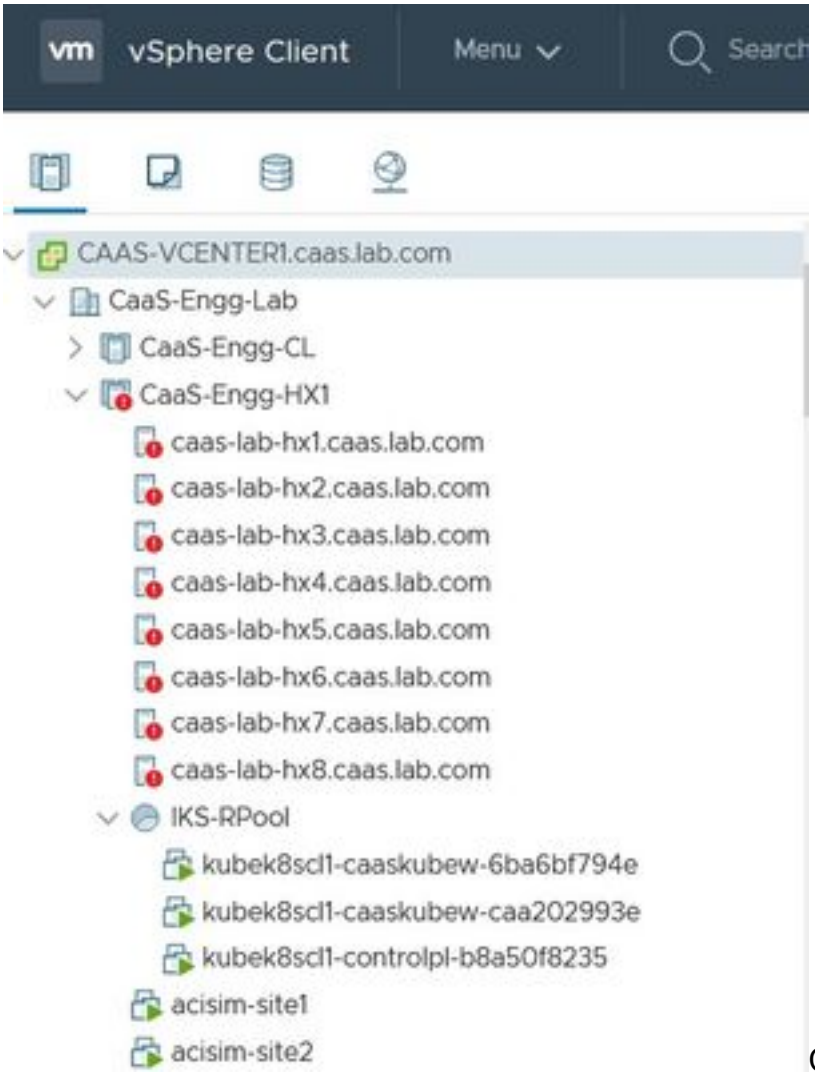
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Nella parte superiore destra è possibile tenere traccia dello stato di avanzamento dell'installazione.



Verifica tramite interfaccia utente IKS

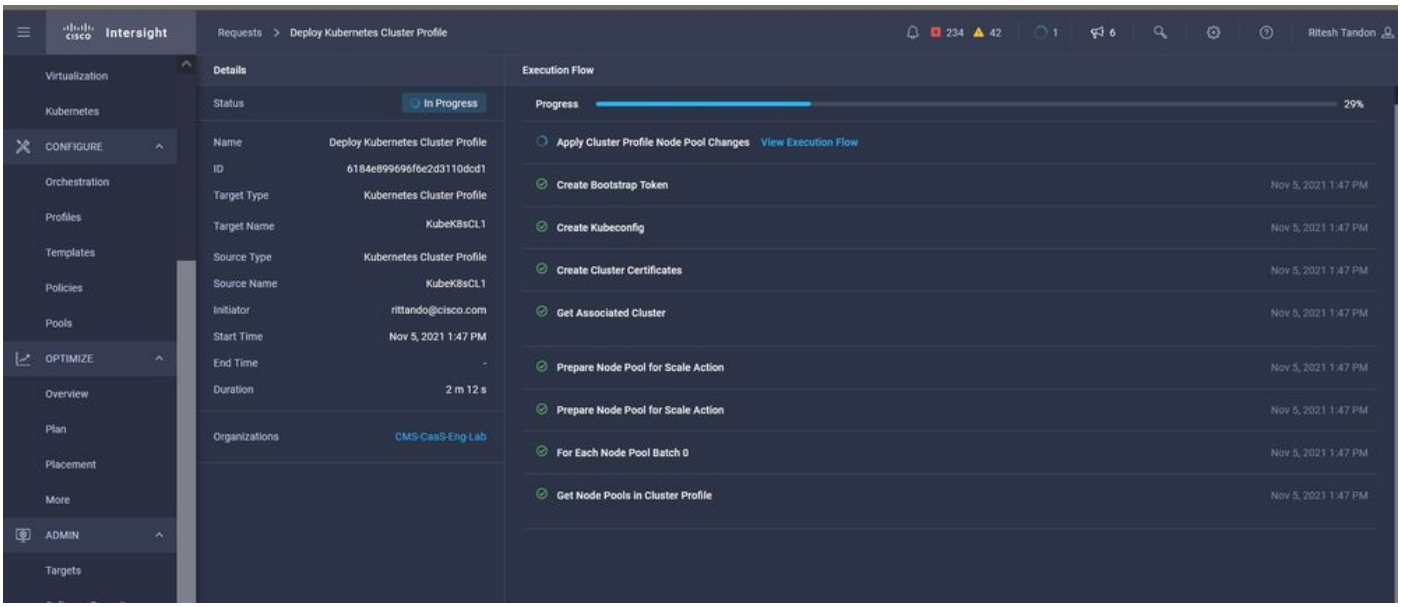
Man mano che l'implementazione procede, è possibile verificare che i nodi Kubernetes Master e Worker saranno disponibili su vCenter.



Cluster IKS in arrivo in vCenter

Se è necessario visualizzare i passaggi dettagliati per la distribuzione, è possibile eseguire il drill-

down più a fondo.



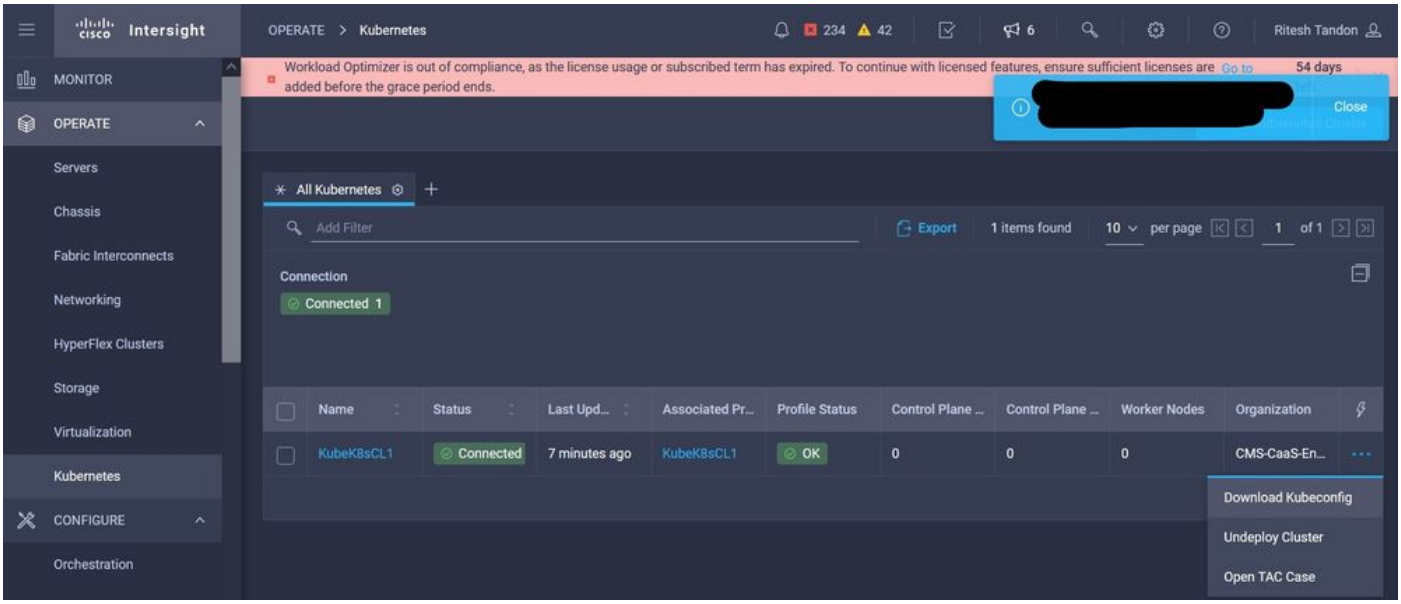
Esecuzione creazione profilo

Connessione al cluster Kubernetes

Èpossibile connettersi al cluster Kubernetes nei modi seguenti:

Utilizzando il file KubeConfig, scaricabile da **Operate > Kubernetes > Selezionare le opzioni all'estrema destra**.

Ènecessario che KubeCtl sia installato nella workstation di gestione dalla quale si desidera accedere al cluster.



Scarica il file KubeConfig da IKS

Èpossibile anche configurare SSH direttamente nel nodo master usando applicazioni SSH come Putty con le credenziali e la chiave privata configurate al momento della distribuzione

Se si distribuisce 'Kubernetes Dashboard' come componente aggiuntivo, è possibile utilizzare anche quello, per distribuire le applicazioni direttamente tramite GUI.

Per ulteriori informazioni, consultare la sezione 'Accesso ai cluster Kubernetes', qui:

Verifica con CLI

Una volta stabilita la connessione al cluster Kubernetes utilizzando kubeCtl, è possibile utilizzare i comandi seguenti per verificare se nel cluster sono installati e in esecuzione tutti i componenti.

Verificare che i nodi nel cluster siano nello stato 'ready'.

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

Verificare lo stato dei pod creati al momento dell'installazione dei componenti essenziali nel 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
```

Verificare lo stato dell'alloggiamento operatore ccp-helm che gestisce l'alloggiamento dell'alloggiamento in esecuzione localmente e installa i componenti aggiuntivi.

```
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
```

Verificare lo stato dei pod Essential-* che gestiscono i componenti aggiuntivi Essential (core), installati per impostazione predefinita, in ogni cluster tenant 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
```

Verificare lo stato dei servizi e del bilanciamento del carico distribuito nello spazio dei nomi 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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nel caso in cui un particolare pod non venga verso l'alto, è possibile utilizzare questi comandi per approfondire la causa.

```
Syntax : kubectl describe pod
```

Informazioni correlate

- Fare clic qui per leggere la descrizione del servizio IKS.
- Consultare qui la Guida per l'utente.
- Fare clic qui per visualizzare la demo del servizio Intersight Kubernetes.
- Documentazione e supporto tecnico – Cisco Systems