Configurer le cluster Kubernetes à l'aide du service Intersight Kubernetes

Contenu

Introduction

Ce document décrit la configuration permettant de provisionner un cluster Kubernetes de qualité production à partir de Cisco Intersight (SaaS) à l'aide du service Cisco Intersight™ Kubernetes (IKS).

Informations générales

Ces derniers temps, Kubernetes est devenu un outil de gestion des conteneurs de facto, les entreprises ayant tendance à investir davantage dans la modernisation des applications grâce aux solutions conteneurisées. Grâce à Kubernetes, les équipes de développement peuvent déployer, gérer et faire évoluer leurs applications conteneurisées en toute simplicité, rendant les innovations plus accessibles à leurs pipelines de livraison continue.

Cependant, Kubernetes est confronté à des défis opérationnels, car l'installation et la configuration nécessitent du temps et une expertise technique.
L'installation de Kubernetes et des différents composants logiciels requis, la création de clusters, la configuration du stockage, de la mise en réseau et de la sécurité, ainsi que les opérations (mise à niveau, mise à jour et correction des bogues de sécurité critiques, par exemple) nécessitent un investissement important en capital humain continu.

Saisissez IKS, une solution SaaS clé en main pour gérer des Kubernetes homogènes et de qualité production partout. Pour en savoir plus sur les fonctionnalités d'IKS, cliquez sur ce lien ici.

Présentation de la solution

Pour ce document, l'idée est de présenter la capacité d'IKS à s'intégrer de manière transparente à votre infrastructure sur site, en exécutant VMware ESXi et vCenter.
En quelques clics, vous pouvez déployer un cluster Kubernetes de qualité production sur votre infrastructure VMware.

Mais pour ce faire, vous devez intégrer votre vCenter sur site à Intersight, connu sous le nom de 'revendication d'une cible', vCenter étant la cible ici.
Vous avez besoin d'un appareil virtuel Cisco Intersight Assist, qui permet d'ajouter des cibles de terminaux à Cisco Intersight. Vous pouvez installer Intersight Assist à l'aide de la bootstrap OVA disponible sur le site Web officiel de Cisco.

Pour limiter la portée de ce document, nous ne nous concentrerons pas sur l'installation de Cisco Intersight Assist Virtual Appliance. Mais vous pouvez jeter un coup d'oeil au processus ici

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compte Intersight : Vous avez besoin d'un ID Cisco valide et d'un compte Intersight.
  Vous pouvez créer un ID Cisco sur le site Web de Cisco si vous n'en avez pas. Ensuite, cliquez sur le lien Créer un compte dans Intersight.
- Cisco Intersight Assist : Cisco Intersight Assist vous aide à ajouter vCenter/ESXi en tant que cible de terminaux à Cisco Intersight.
- Connectivité : Si votre environnement prend en charge un proxy HTTP/S, vous pouvez l'utiliser pour connecter votre appareil Cisco Intersight Assist à Internet. Vous pouvez également ouvrir des ports sur des URL d'analyse. Veuillez consulter ce lien pour connaître les exigences détaillées en matière de connectivité réseau :
- Informations d'identification vCenter pour le réclamer sur Intersight.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Hypothèses

Puisque le déploiement d'un appareil Cisco Intersight n'est pas couvert par ce document.

Nous supposons que vous disposez déjà d'un compte Intersight fonctionnel et que vous avez réussi à lui demander un vCenter/Esxi sur site.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

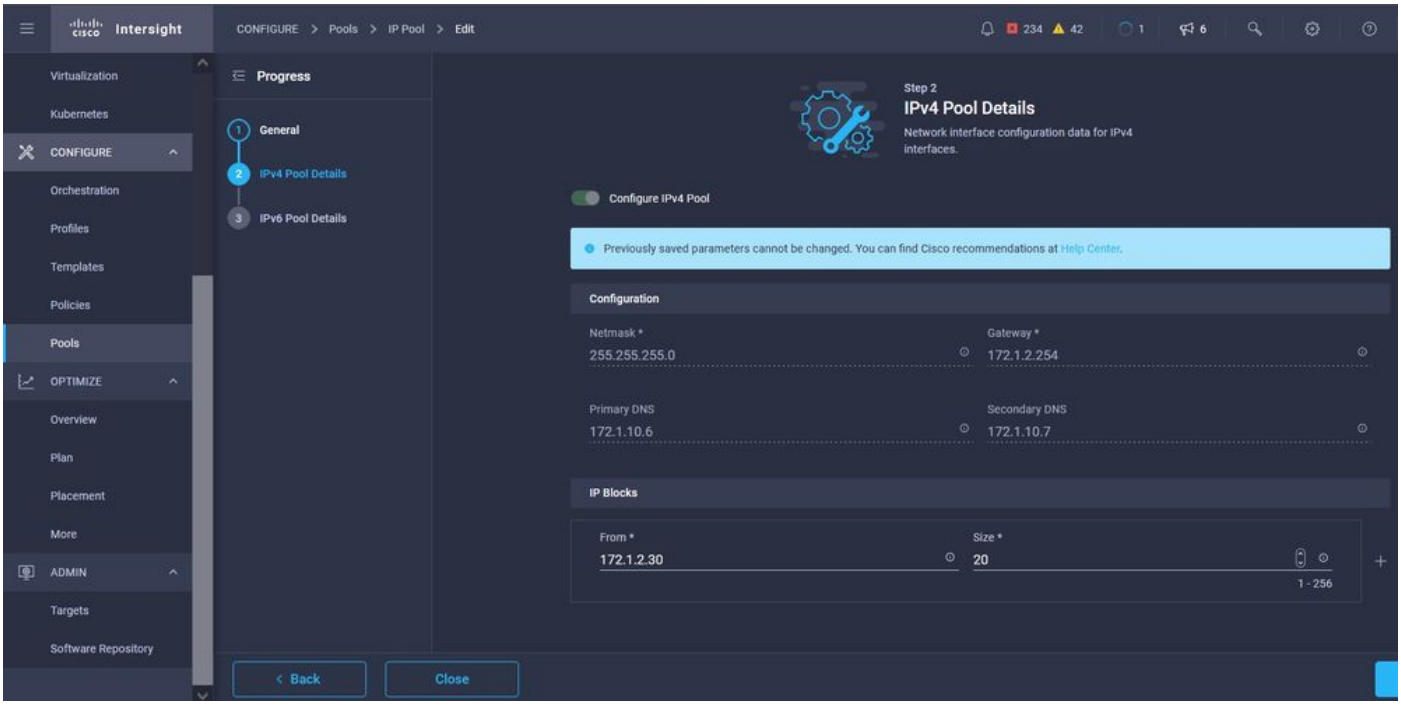
Étape 1. Configurer les stratégies

Les politiques simplifient la gestion car elles transforment la configuration en modèles réutilisables.

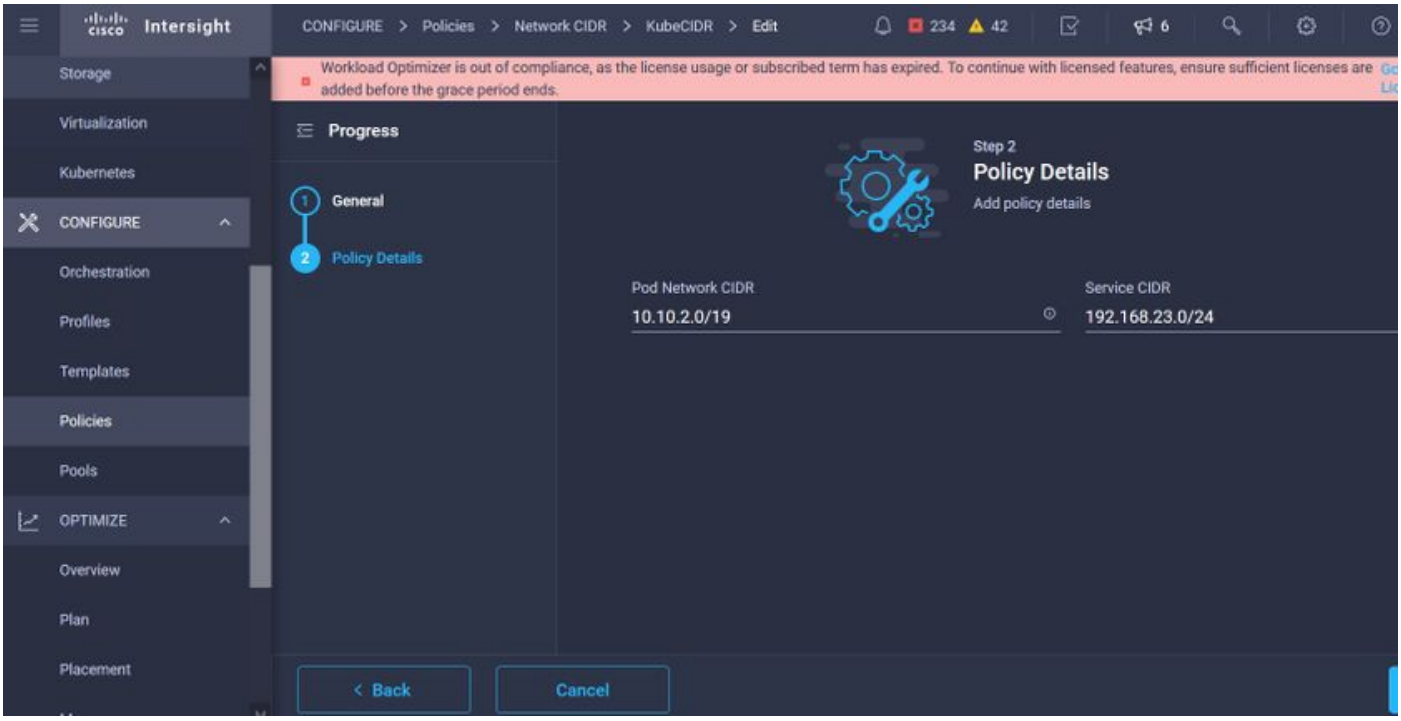
Certaines des stratégies que nous devons configurer sont répertoriées ci-dessous. Notez que toutes ces stratégies seront créées dans la section Configurer » Politiques et configuration » Pools sur Intersight.

Vous pouvez également voir le chemin d'accès de la politique au-dessus de chaque capture d'écran, comme indiqué ci-dessous.

Ce pool d'adresses IP sera utilisé pour les adresses IP de vos machines virtuelles de noeuds de contrôle et de travail, lorsqu'il sera lancé sur l'hôte ESXi.

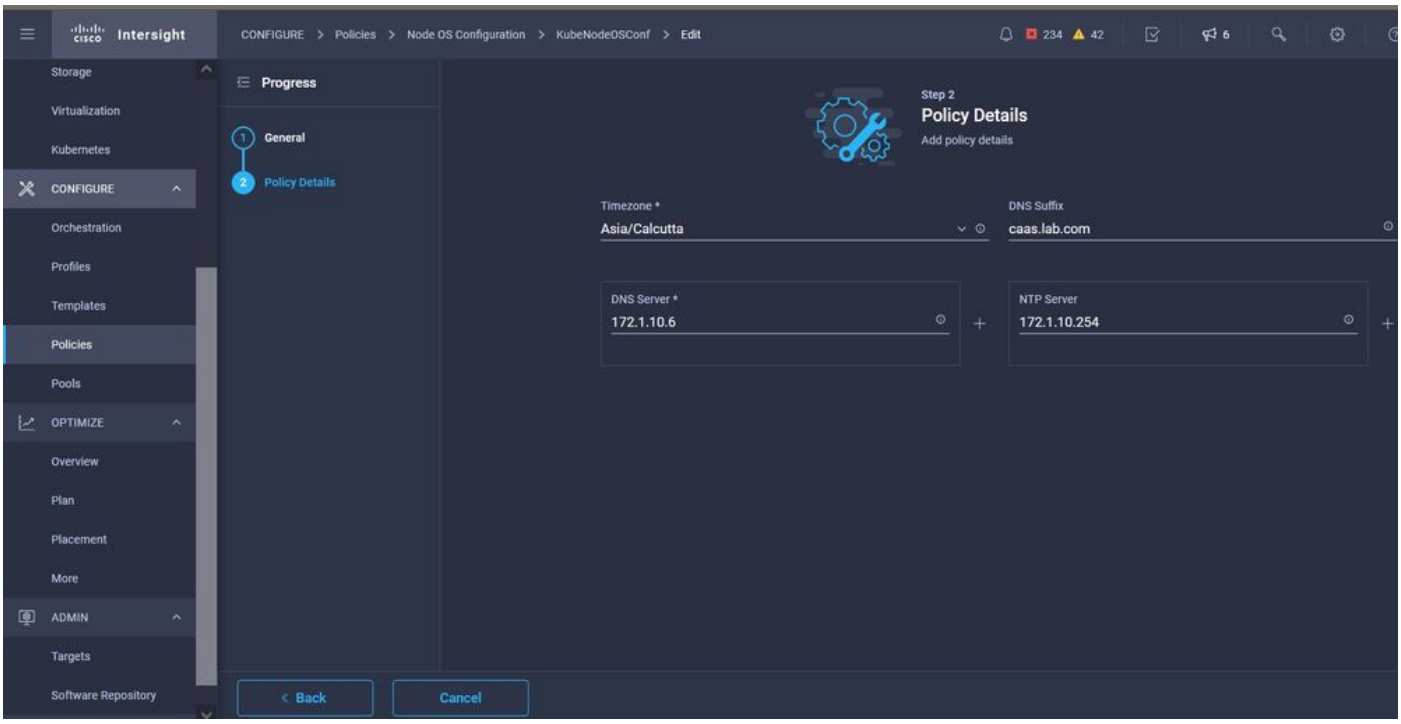


Vous définissez ici le CIDR du réseau Pod and Services, pour les réseaux internes au sein du cluster Kubernetes.



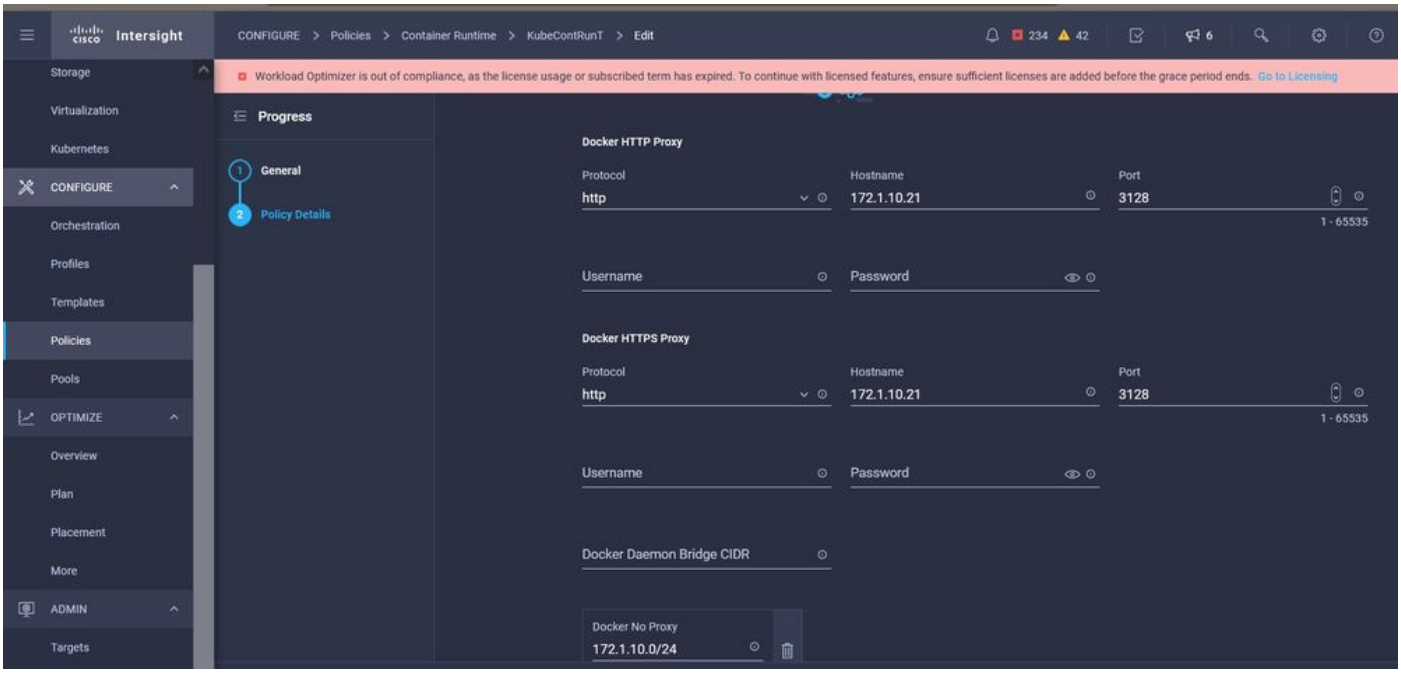
Services et CIDR réseau

Cette stratégie définit votre configuration NTP et DNS.



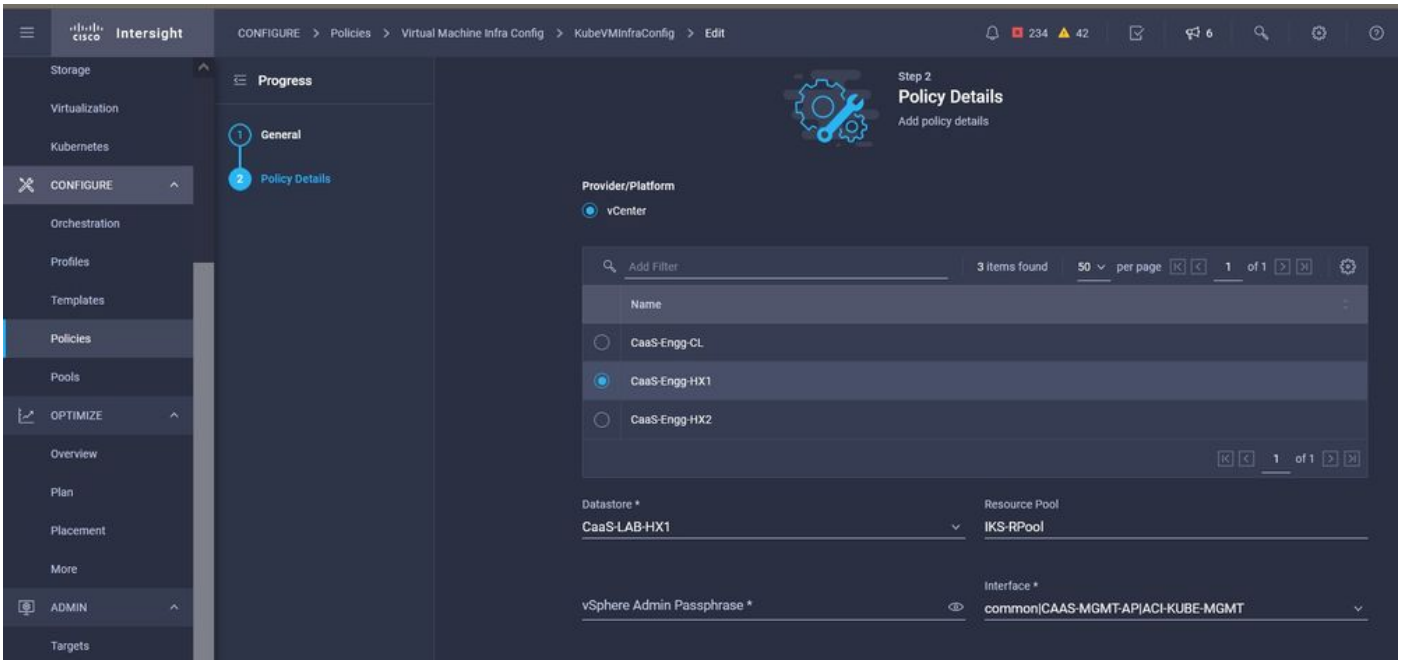
Configuration NTP et DNS

Avec cette stratégie, vous pouvez définir la configuration du proxy pour le runtime de votre conteneur docker.



Configuration du proxy pour Docker

Dans cette stratégie, vous allez définir la configuration requise sur les machines virtuelles déployées en tant que noeuds Master et Worker.



Configuration des machines virtuelles utilisées

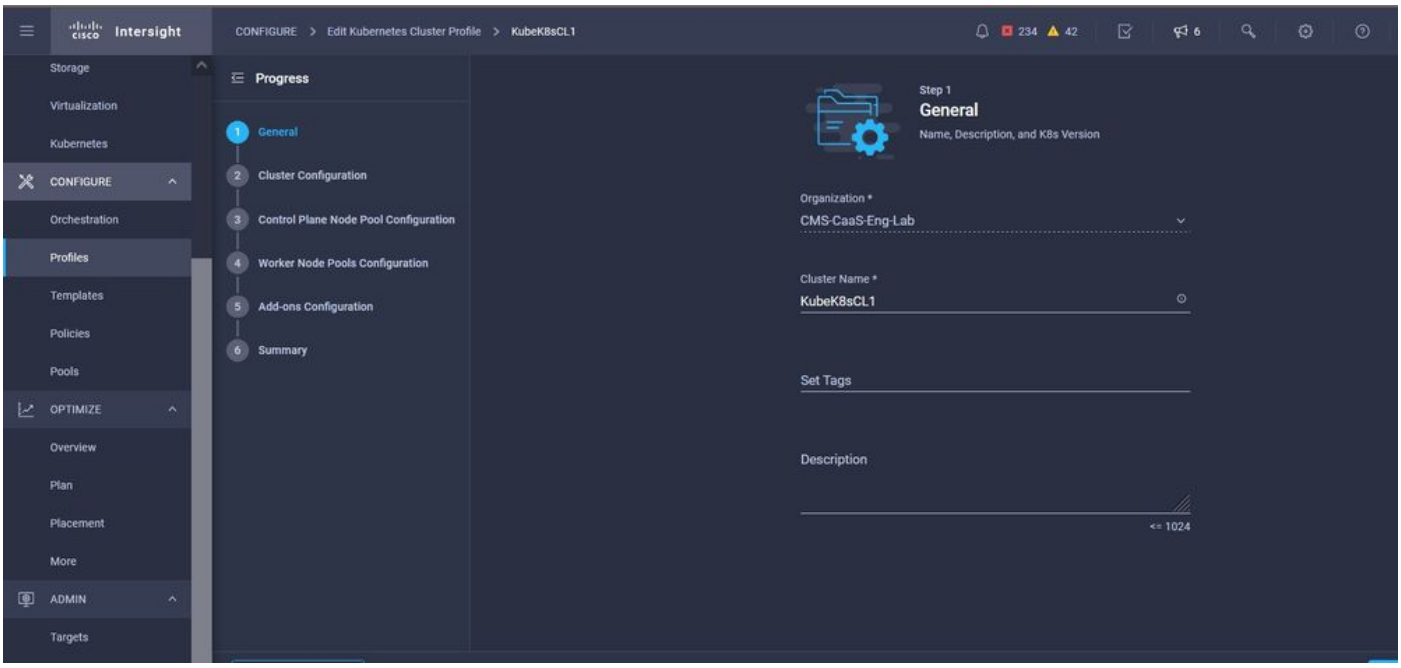
Étape 2. Configurer le profil

Une fois que nous avons créé les stratégies ci-dessus, nous les lions à un profil que nous pouvons ensuite déployer.

Le déploiement de la configuration à l'aide de stratégies et de profils extrait la couche de configuration afin qu'elle puisse être déployée à plusieurs reprises rapidement.

Vous pouvez copier ce profil et en créer un nouveau avec peu ou plus de modifications sur les stratégies sous-jacentes en quelques minutes, dans un ou plusieurs clusters Kubernetes en une fraction de temps nécessaire avec un processus manuel.

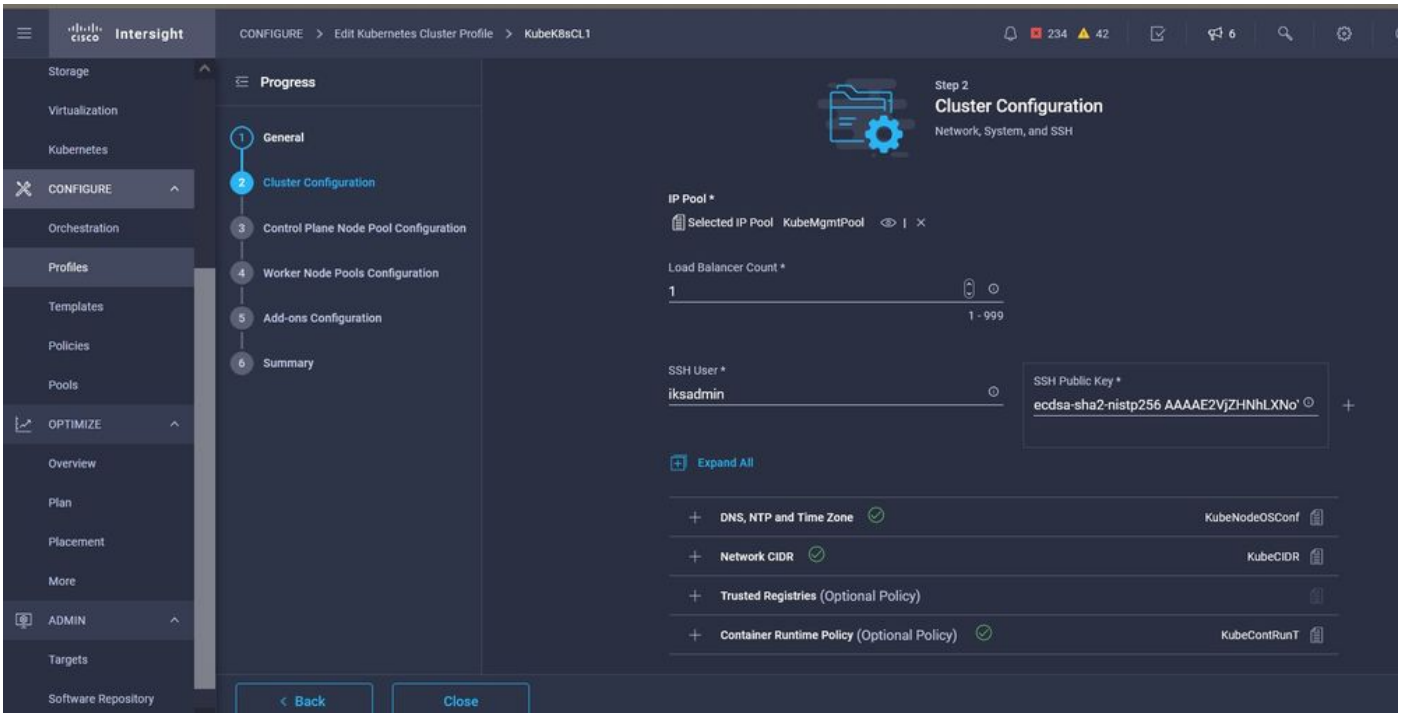
GIve dans le champ Nom et définir des balises.



Configuration du profil avec nom et balises

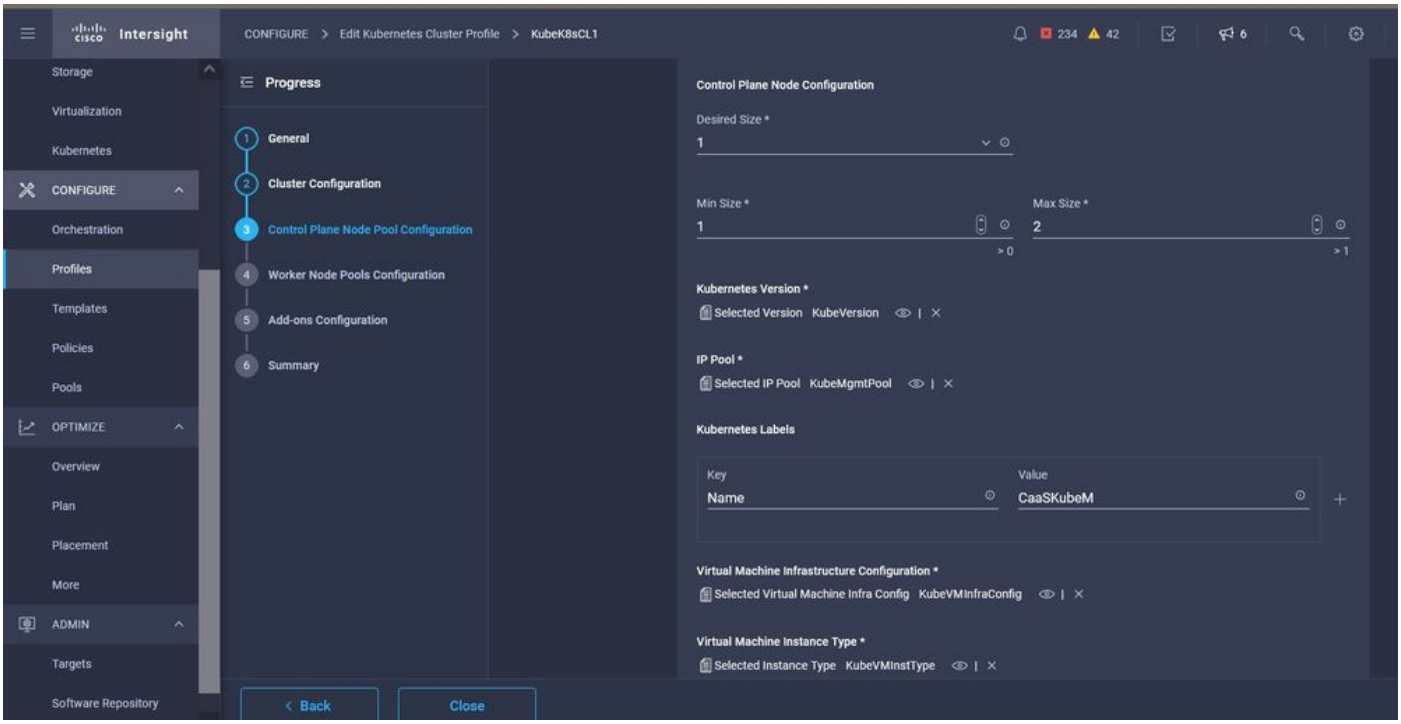
Définissez les stratégies Pool, Node OS et Network CIDR. Vous devez également configurer un ID utilisateur et une clé SSH (publique).

Sa clé privée correspondante serait utilisée pour ssh dans les noeuds Master & Worker.



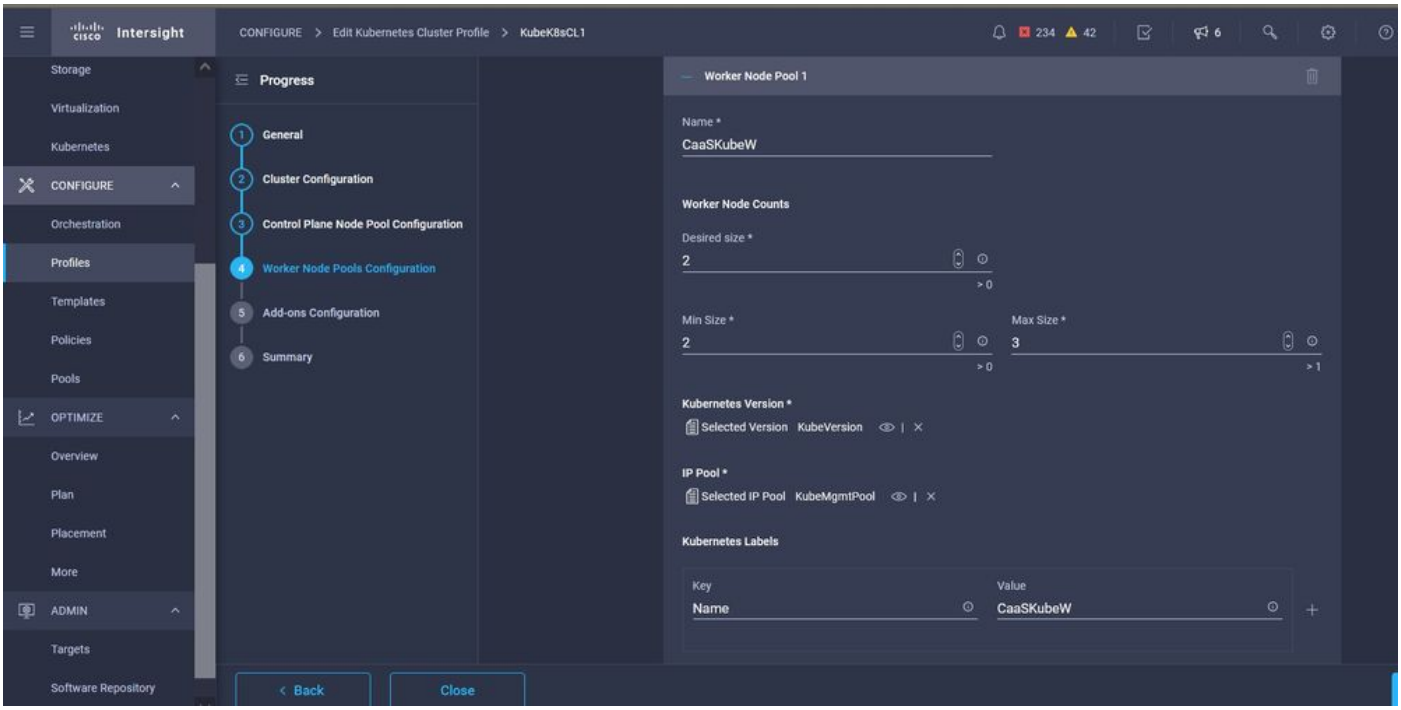
Configuration du profil avec les stratégies affectées

Configurez le plan de contrôle : Vous pouvez définir le nombre de noeuds maîtres dont vous avez besoin sur le plan de contrôle.



Configuration du noeud maître

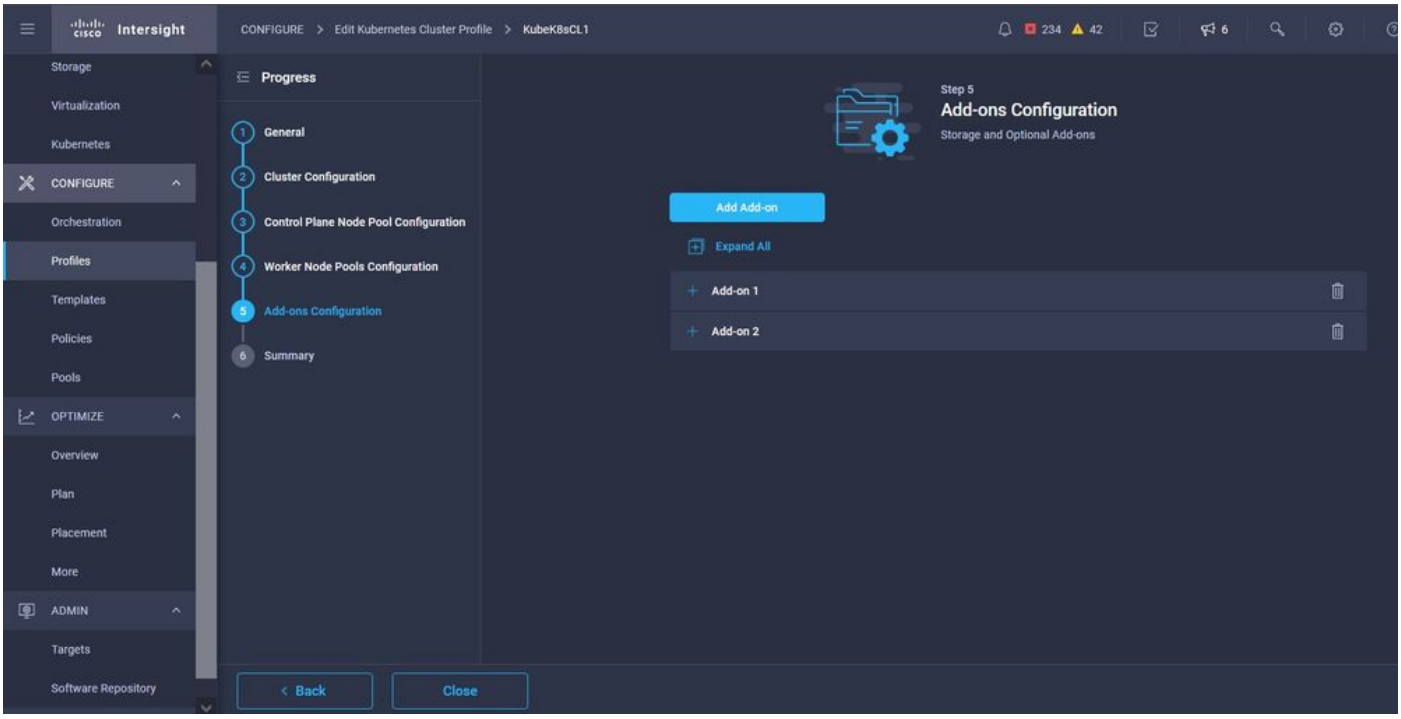
Configurez les noeuds Worker : En fonction des besoins des applications, vous pouvez augmenter ou réduire vos noeuds de travail.



Configuration des noeuds de travail

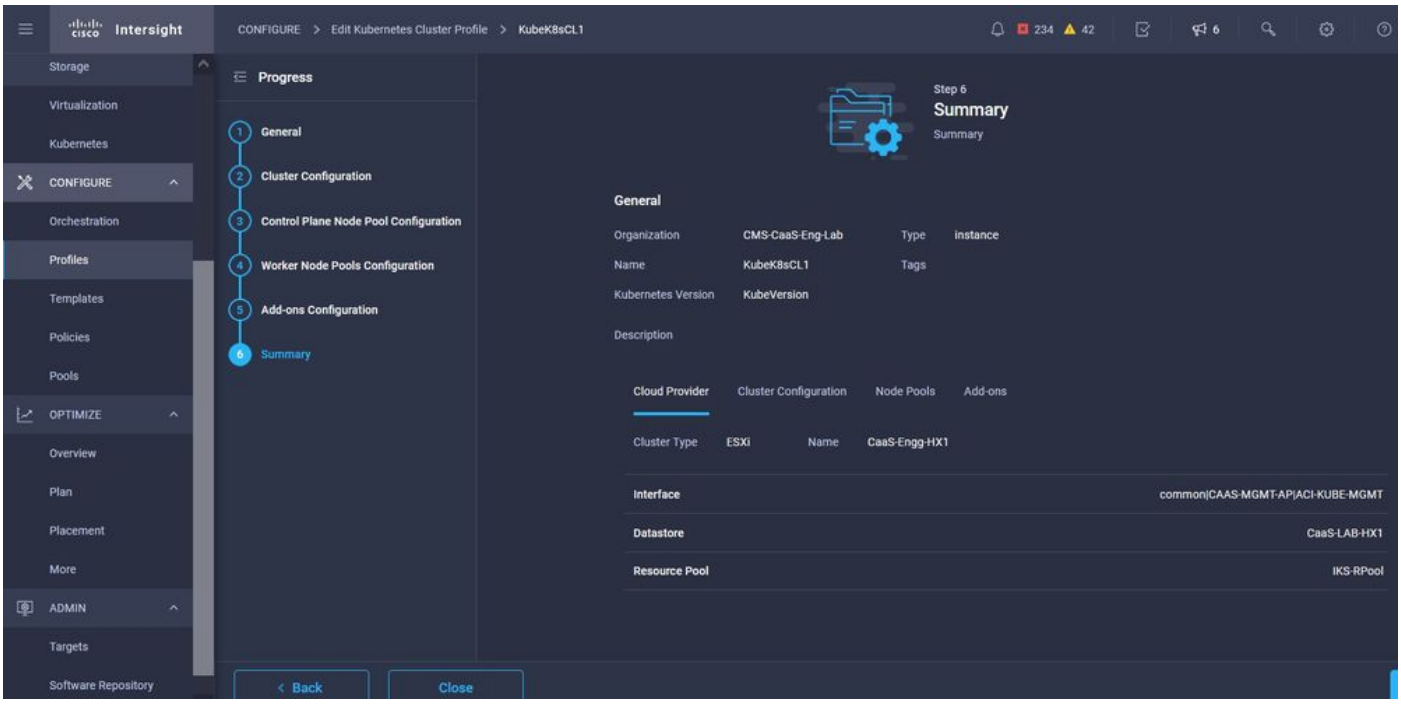
Configurer le module complémentaire. À partir de maintenant, vous pouvez déployer automatiquement, Kubernetes Dashboard et Graffana avec la surveillance Prometheus.

Àl'avenir, vous pouvez ajouter des modules complémentaires que vous pouvez déployer automatiquement à l'aide d'IKS.



Ajouter des compléments, le cas échéant

Cochez la case Résumé, puis cliquez sur **Déployer**.

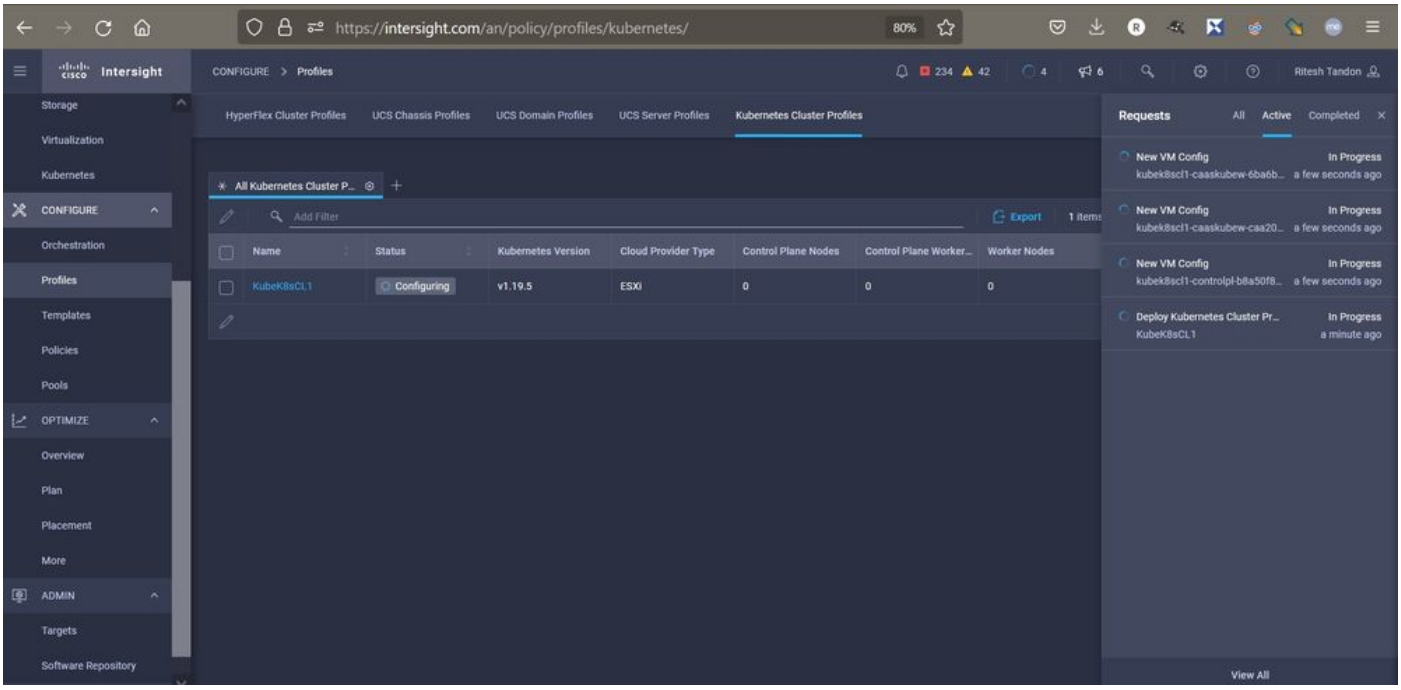


Ecran Résumé de la création du profil

Vérification

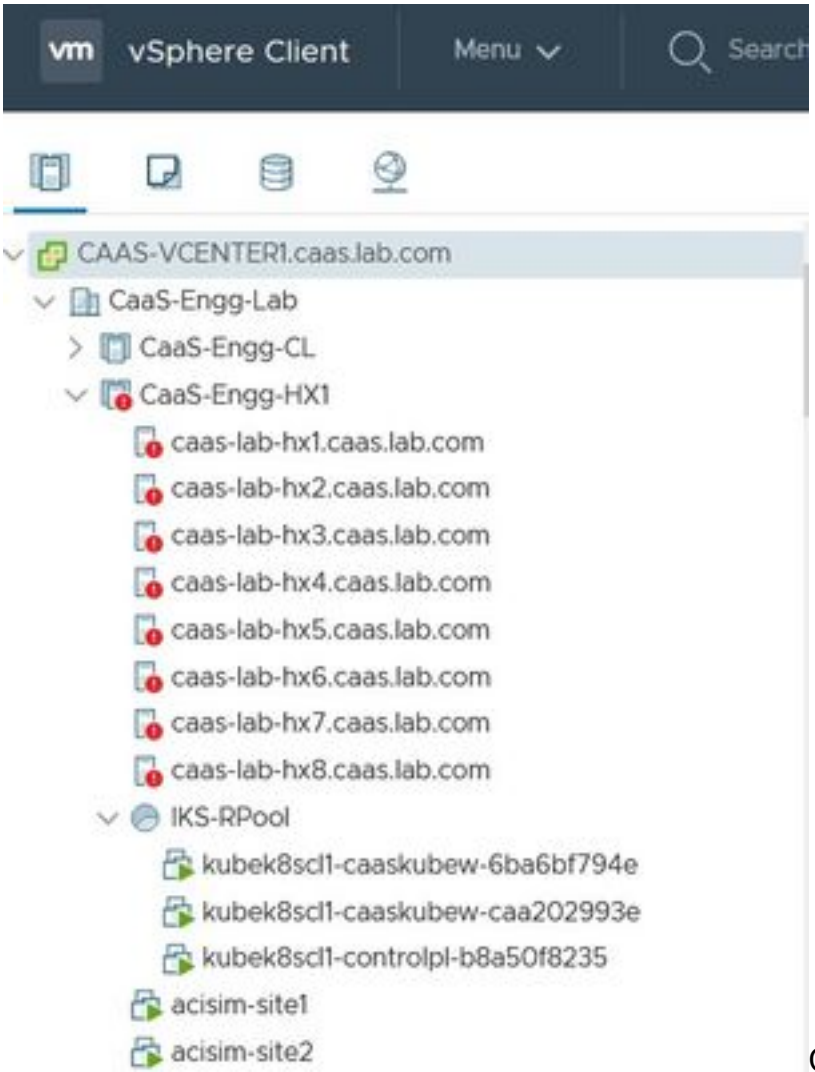
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

En haut à droite, vous pouvez suivre la progression du déploiement.



Vérifier à l'aide de l'interface graphique IKS

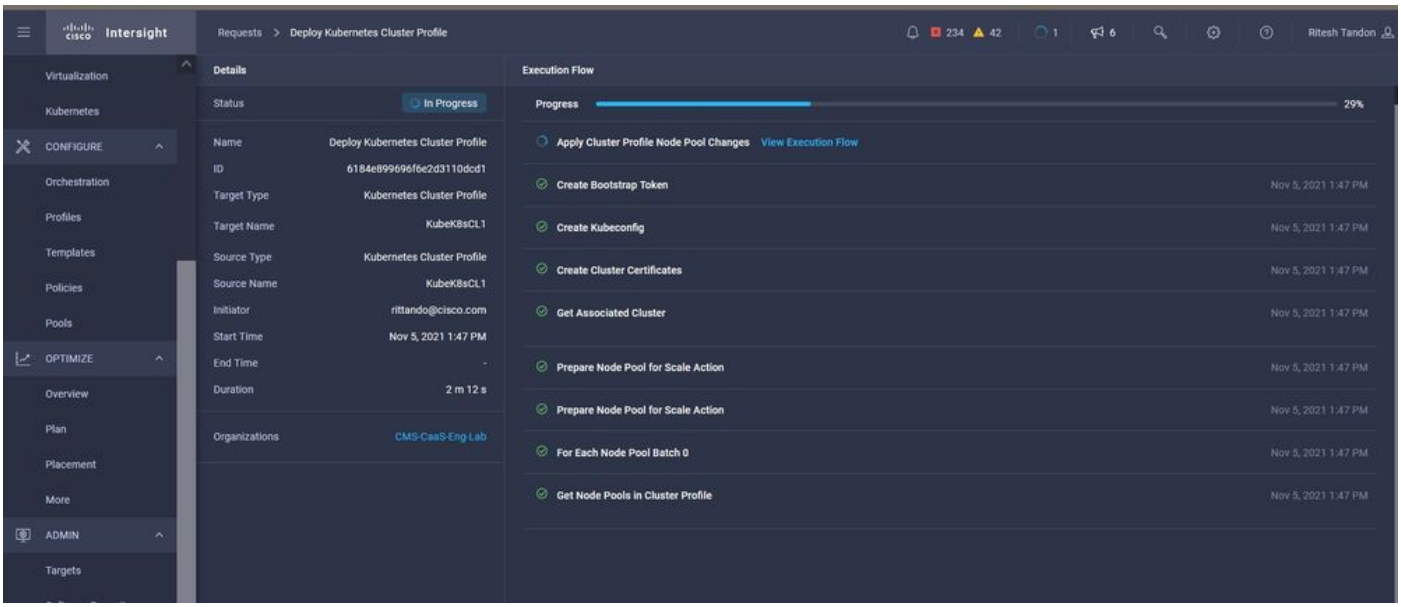
Au fur et à mesure que le déploiement progresse, vous pouvez voir vos noeuds maître et de travail Kubernetes apparaître sur vCenter.



Cluster IKS à venir dans vCenter

Si vous avez besoin de voir les étapes détaillées du déploiement, vous pouvez approfondir

l'exécution.



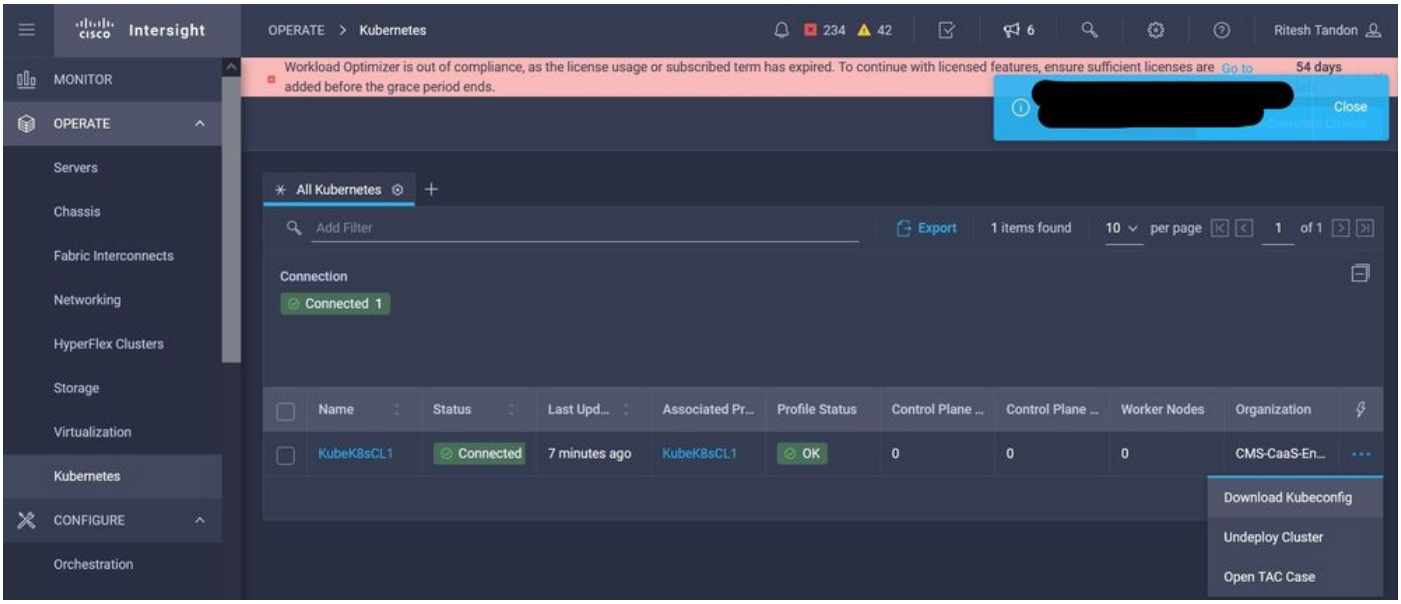
Exécution de la création de profil

Se connecter au cluster Kubernetes

Vous pouvez vous connecter au cluster Kubernetes de la manière suivante :

En utilisant le fichier KubeConfig, que vous pouvez télécharger à partir de **Operate > Kubernetes > Sélectionnez les options à l'extrême droite**.

KubeCtl doit être installé sur la station de travail Management, à partir de laquelle vous souhaitez accéder à ce cluster.



Télécharger le fichier KubeConfig depuis IKS

Vous pouvez également accéder directement à SSH dans le noeud maître, en utilisant des applications SSH telles que Putty avec les informations d'identification et la clé privée configurées au moment du déploiement

Si vous déployez 'Tableau de bord de Kubernetes' en tant que module complémentaire, vous

pouvez également l'utiliser pour déployer des applications directement à l'aide de l'interface utilisateur graphique.

Pour plus de détails, consultez la section 'Accès aux clusters Kubernetes', ici :

Vérifier avec CLI

Une fois que vous êtes en mesure de vous connecter au cluster Kubernetes à l'aide de kubeCtl, vous pouvez utiliser les commandes suivantes pour vérifier si tous les composants du cluster sont installés et en cours d'exécution.

Vérifiez que les noeuds du cluster sont prêts.

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

Vérifiez l'état des pods créés au moment de l'installation des composants essentiels sur le 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
```

Vérifiez l'état du pod de l'opérateur ccp-helm qui gère l'helm en cours d'exécution localement et installe les modules complémentaires.

```
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
```

Vérifiez l'état des pods essentiels* qui gèrent les modules complémentaires Essential (core), installés par défaut, sur chaque cluster de locataires 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
```

Vérifiez l'état des services et de l'équilibreur de charge déployés dans l'espace de noms 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si un pod particulier ne s'affiche pas, vous pouvez utiliser ces commandes pour analyser la cause.

```
Syntax : kubectl describe pod
```

Informations connexes

- Consultez la fiche de service IKS ici.
- Consultez le Guide de l'utilisateur ici.
- Consultez la démo du service Intersight Kubernetes ici .
- Support et documentation techniques - Cisco Systems