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

Table des matières

Introduction

Ce document décrit la configuration pour provisionner un cluster Kubernetes de production à partir de Cisco Intersight (SaaS) avec l'utilisation de Cisco Intersight™ Kubernetes Service (IKS).

Informations générales

Kubernetes, ces derniers temps, est devenu un outil de gestion de conteneurs de facto, car les entreprises ont tendance à investir davantage dans la modernisation des applications avec des solutions conteneurisées. Avec Kubernetes, les équipes de développement peuvent déployer, gérer et faire évoluer leurs applications conteneurisées en toute simplicité, rendant ainsi les innovations plus accessibles à leurs réseaux de livraison continus.

Cependant, Kubernetes est livré avec des défis opérationnels, parce qu'il nécessite du temps et une expertise technique pour installer et configurer.
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 (par exemple, la mise à niveau, la mise à jour et la correction des bogues de sécurité critiques) nécessitent un investissement important en capital humain.

Découvrez IKS, une solution SaaS clé en main permettant de gérer des réseaux Kubernetes homogènes et de production, où que vous soyez. Pour en savoir plus sur les capacités d'IKS, cliquez 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, exécutant VMware ESXi et vCenter.
En quelques clics, vous pouvez déployer un cluster Kubernetes de production sur votre infrastructure VMware.

Mais, pour ce faire, vous devez intégrer votre vCenter sur site avec Intersight, connu sous le nom de « demande de cible », vCenter étant la cible ici.
Vous avez besoin d'une appliance virtuelle Cisco Intersight Assist, qui vous aide à ajouter des cibles de point de terminaison à Cisco Intersight. Vous pouvez installer Intersight Assist à l'aide du 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 l'appliance virtuelle Cisco Intersight Assist. Mais, vous pouvez jeter un oeil au processus ici

Conditions préalables

Exigences

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. Puis, cliquez sur le lien Créer un compte dans Intersight.
- Assistance Cisco Intersight : Cisco Intersight Assist vous aide à ajouter vCenter/ESXi en tant que cible de point de terminaison 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 vers des URL d'aperçu. Consultez ce lien pour connaître les exigences détaillées de connectivité réseau :
- Identifiants vCenter pour le réclamer sur Intersight.

Composants utilisés

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

Hypothèses

Le déploiement d'une appliance Cisco Intersight n'est pas traité dans ce document.

Nous supposons que vous disposez déjà d'un compte Intersight opérationnel et que vous avez demandé à bénéficier d'un vCenter/Exxi 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

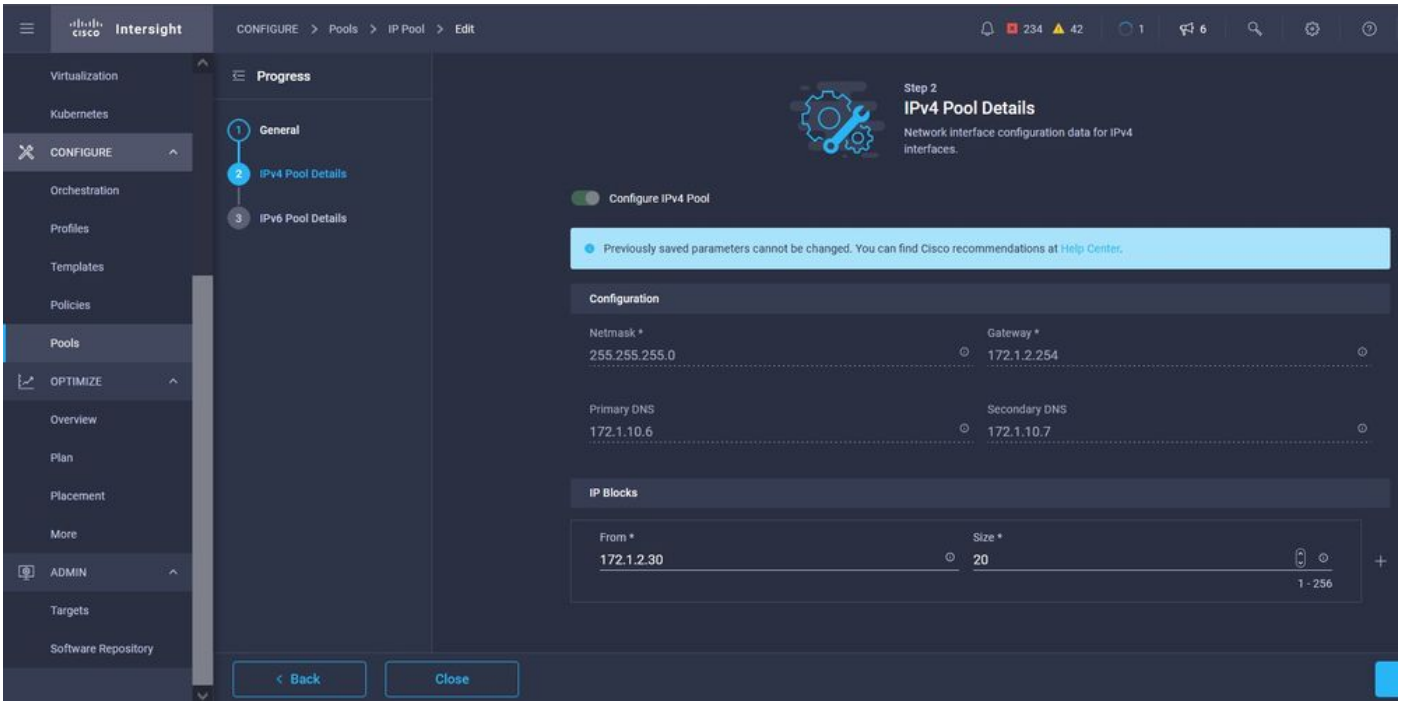
Étape 1 : configuration des stratégies

Les politiques simplifient la gestion en convertissant la configuration en modèles réutilisables.

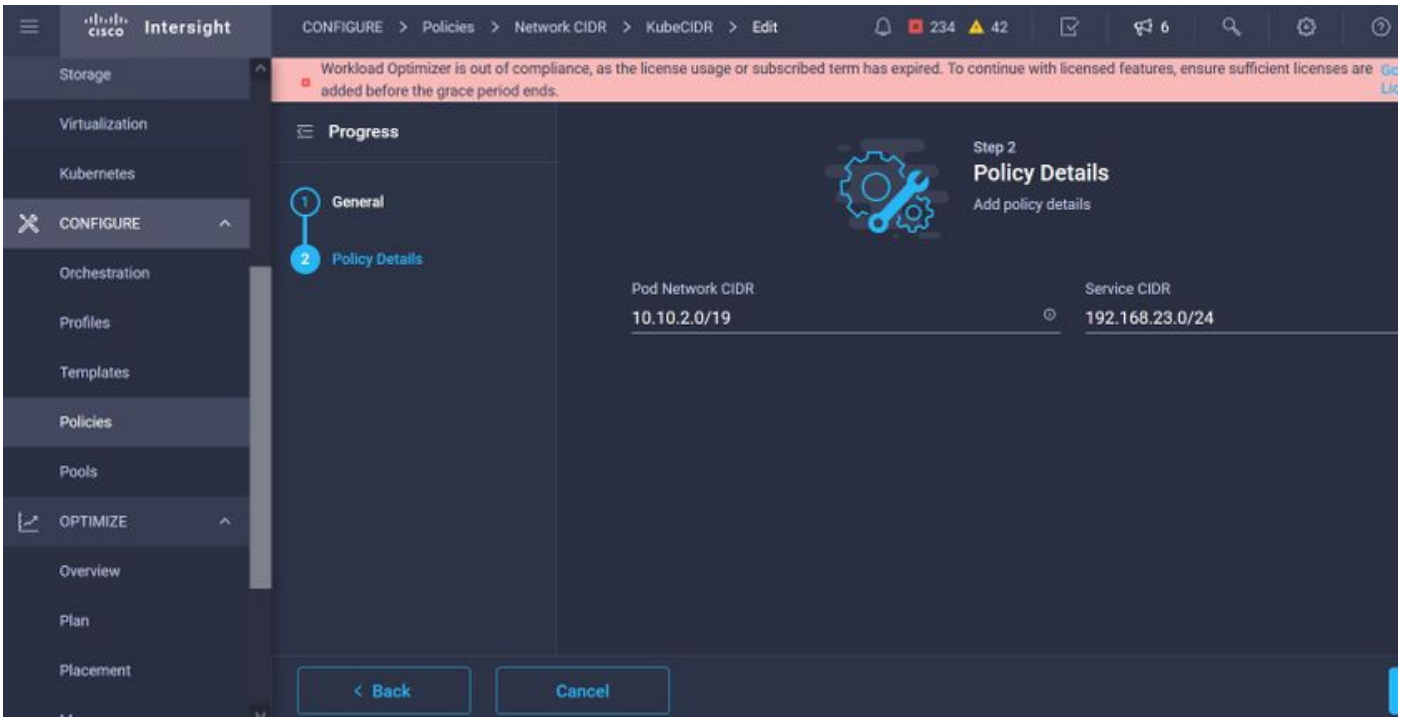
Certaines des politiques que nous devons configurer sont répertoriées ci-dessous. Veuillez noter que toutes ces stratégies seront créées dans Configurer >> Stratégies et Configurer >> Pools sur Intersight.

Vous pouvez également voir le chemin de la stratégie en haut de chaque capture d'écran, donnée ci-dessous.

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

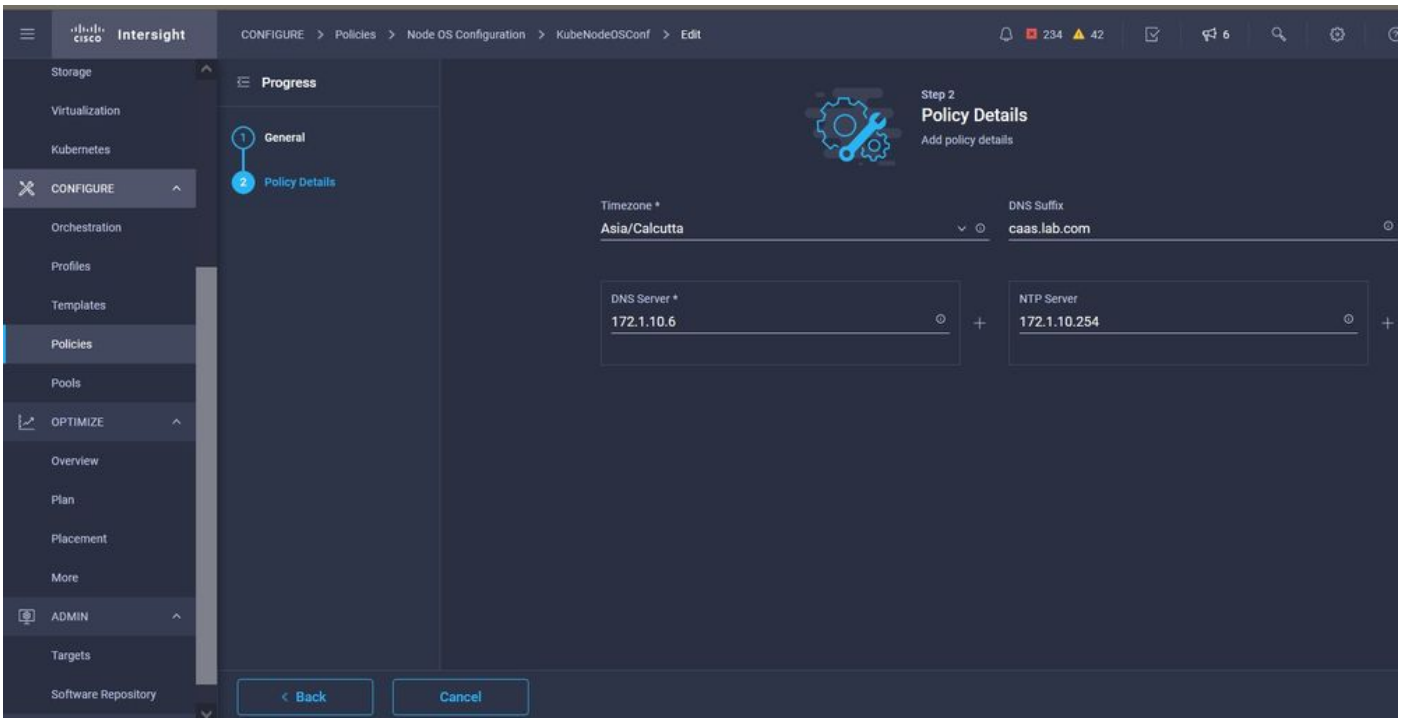


Vous définissez ici le CIDR du réseau de pods et de services, pour la mise en réseau interne au sein du cluster Kubernetes.



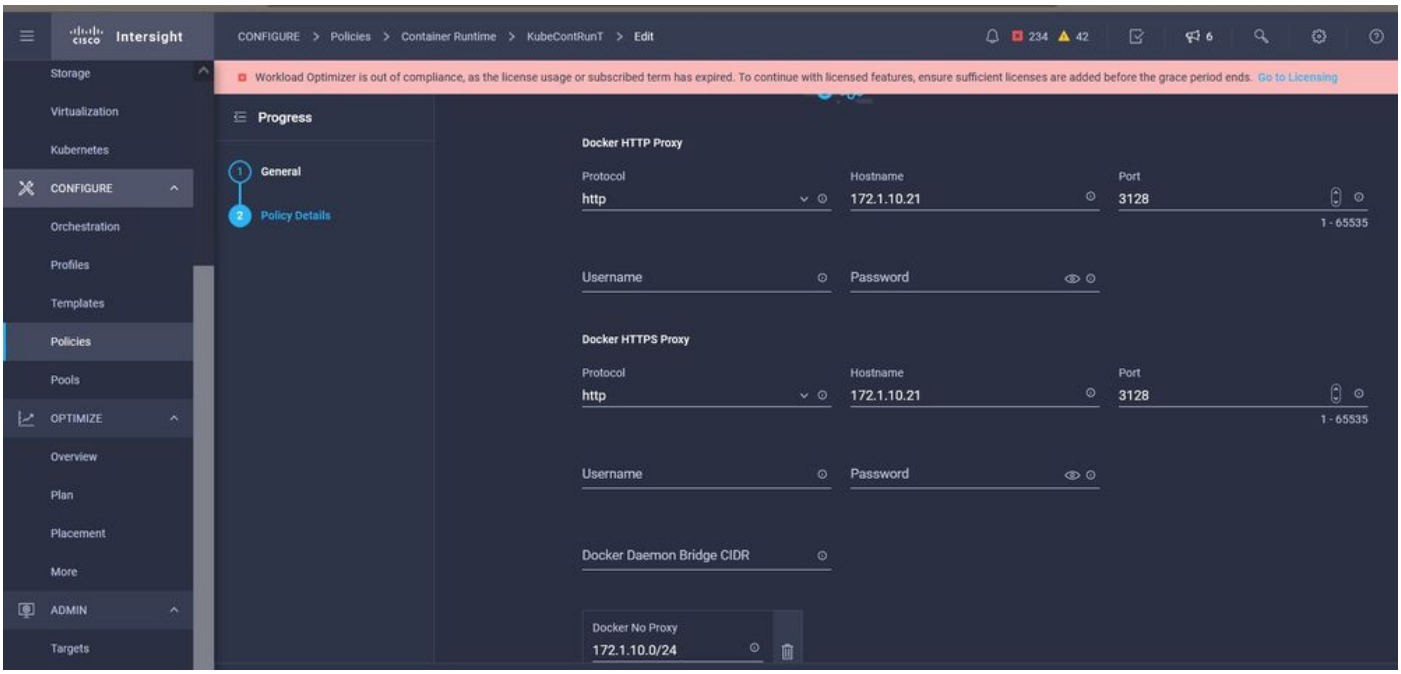
Services et réseau CIDR

Cette stratégie définit votre configuration NTP et DNS.



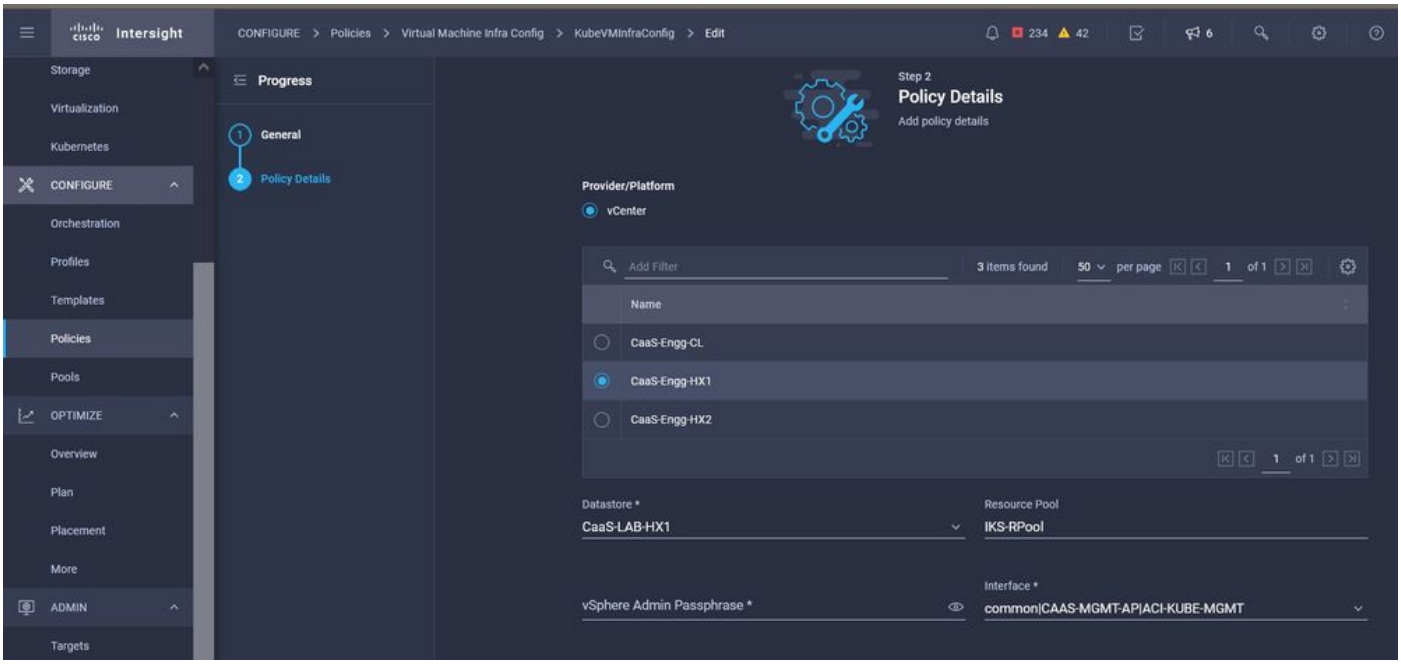
Configuration NTP et DNS

Avec cette stratégie, vous pouvez définir la configuration proxy pour l'exécution 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 : configuration du profil

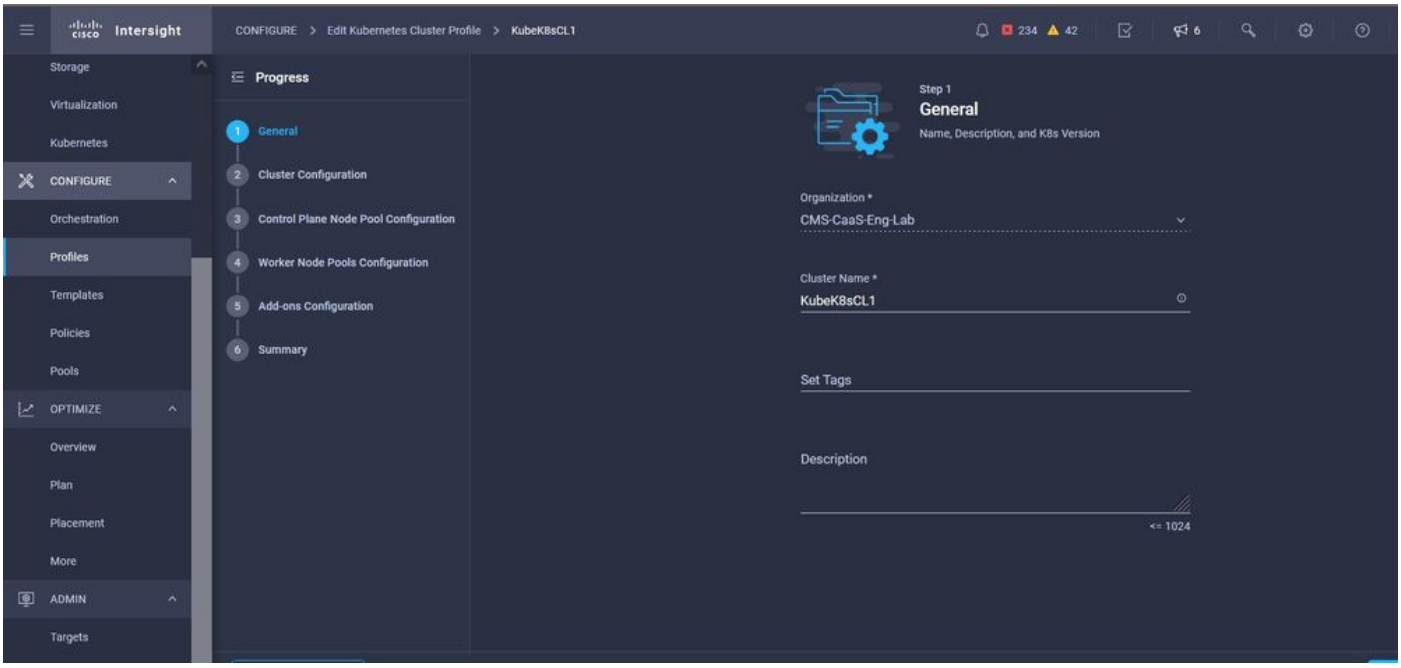
Une fois que nous aurons créé les politiques ci-dessus, nous les lierons dans un profil que nous pourrons ensuite déployer.

Le déploiement de la configuration à l'aide de stratégies et de profils permet d'extraire la couche de configuration afin de la déployer rapidement et de manière répétée.

Vous pouvez copier ce profil et en créer un nouveau avec peu ou plus de modifications sur les

politiques sous-jacentes en quelques minutes, vers un ou plusieurs clusters Kubernetes en une fraction de temps nécessaire avec un processus manuel.

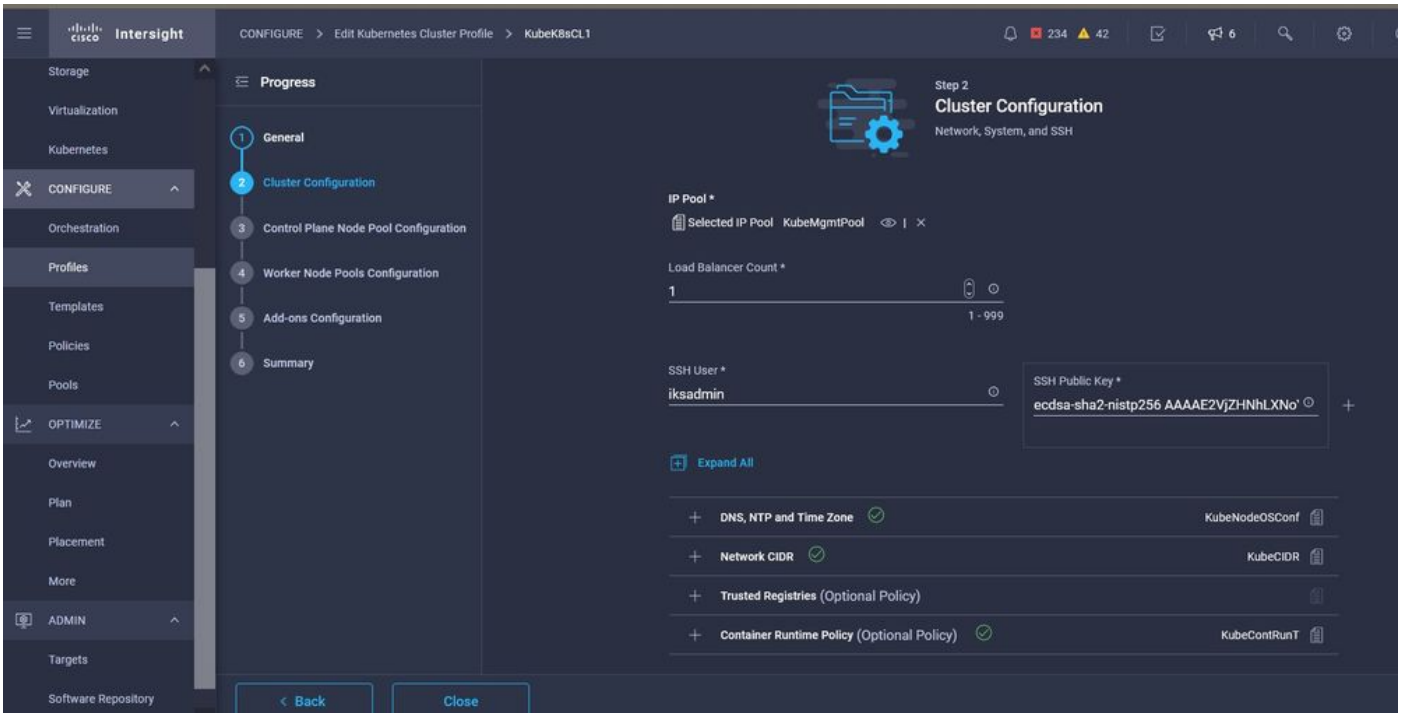
Entrez le nom et définissez les balises.



Configuration du profil avec nom et balises

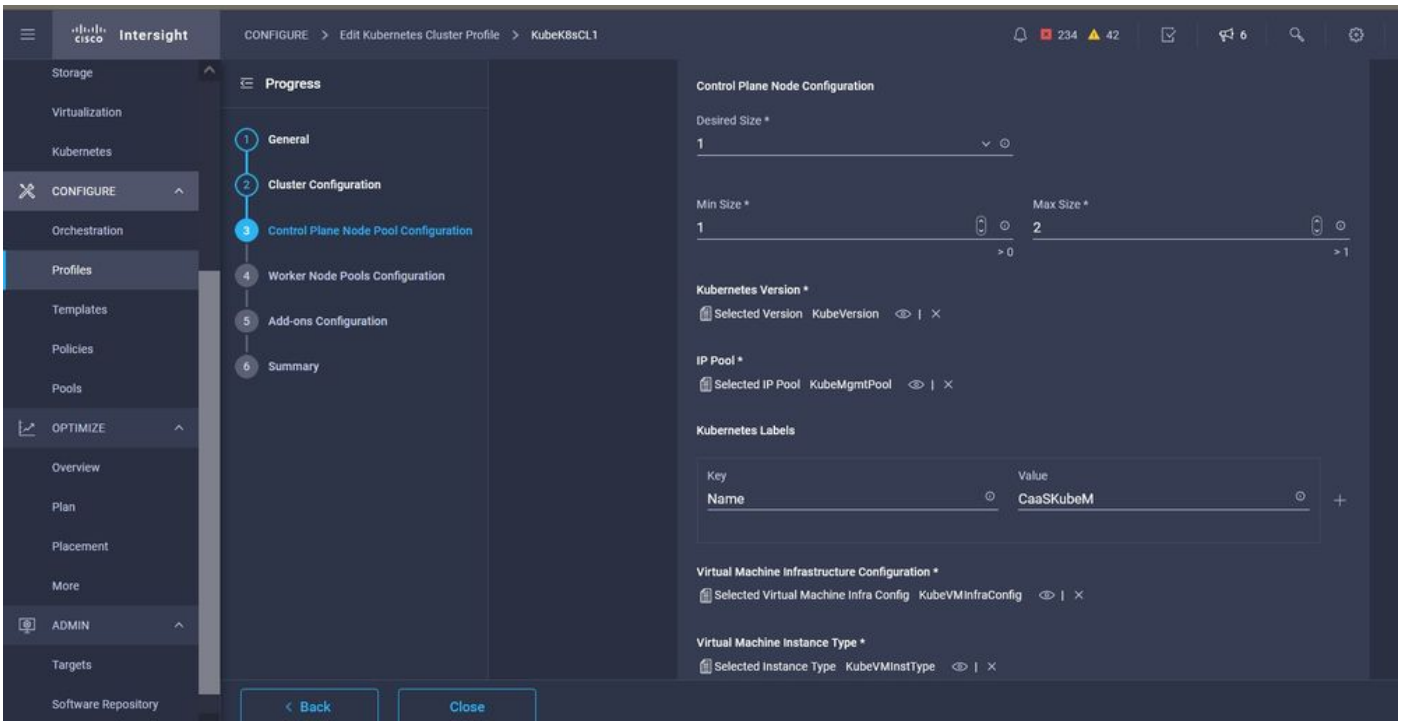
Définissez les stratégies Pool, Node OS et Network CIDR. Vous devez également configurer un ID utilisateur et une clé SSH (publique).

Sa clé privée correspondante serait utilisée pour établir une connexion SSH dans les noeuds Master et Worker.



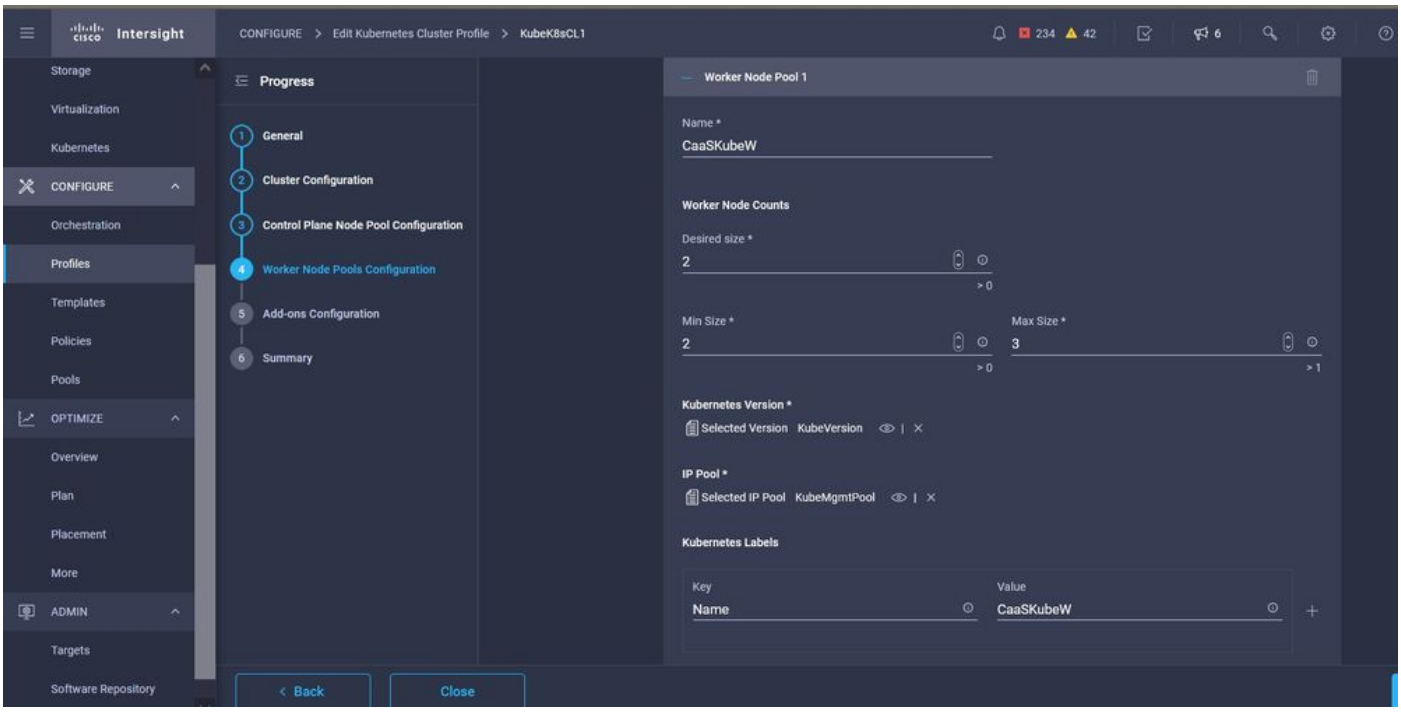
Configuration du profil avec stratégies attribuées

Configurez le plan de contrôle : Vous pouvez définir le nombre de noeuds maîtres nécessaires sur le plan de contrôle.



Configuration du noeud maître

Configurez les noeuds Worker : En fonction des besoins de l'application, vous pouvez augmenter ou diminuer le nombre de noeuds de vos collaborateurs.

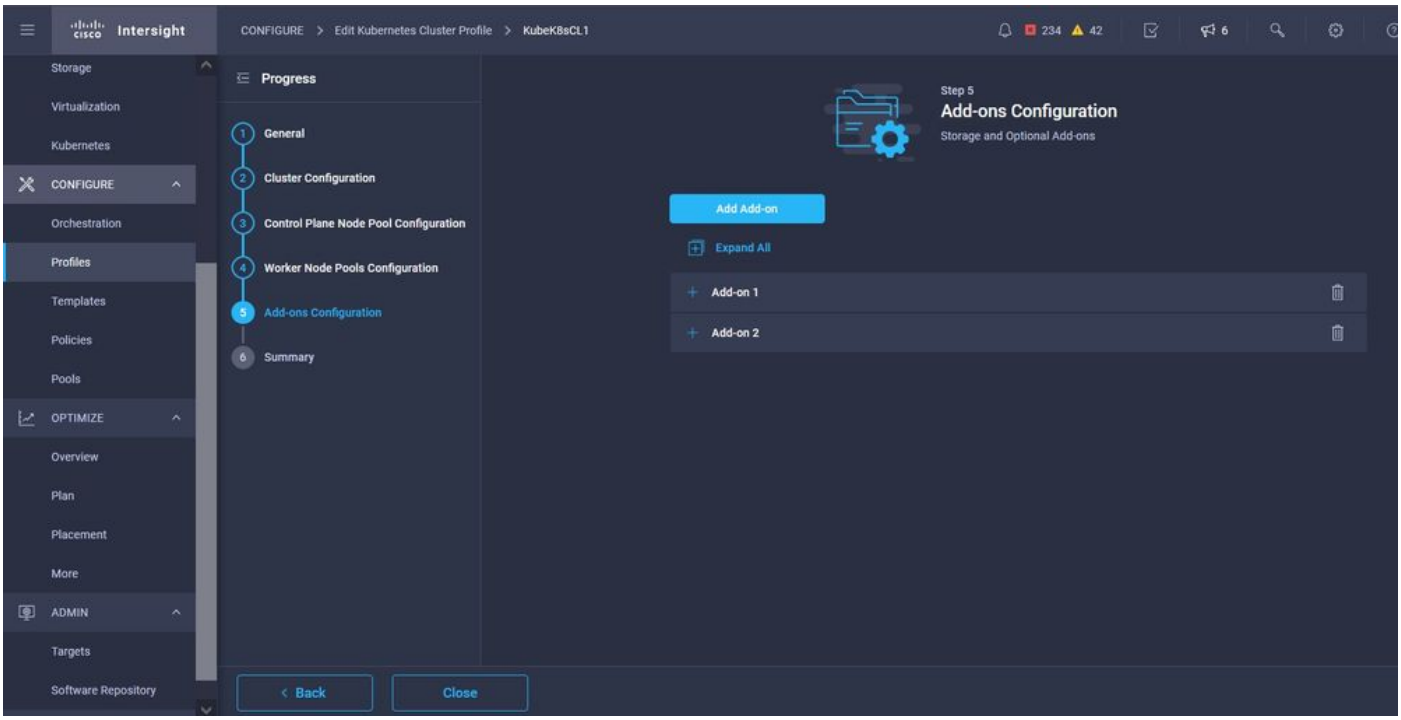


Configuration des noeuds de travail

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

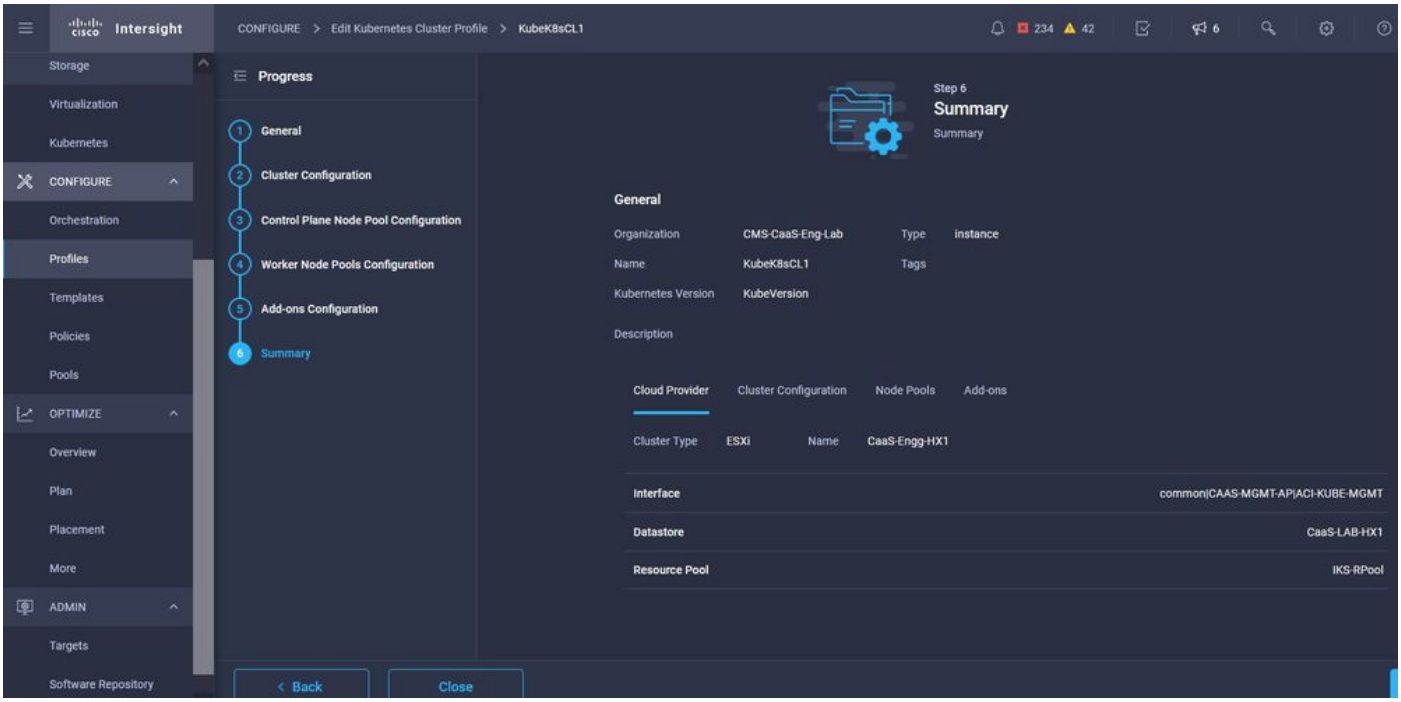
À l'avenir, vous pourrez ajouter d'autres modules complémentaires que vous pourrez déployer

automatiquement à l'aide d'IKS.



Ajoutez des modules d'extension, le cas échéant

Cochez la case Summary, puis cliquez sur Deploy.

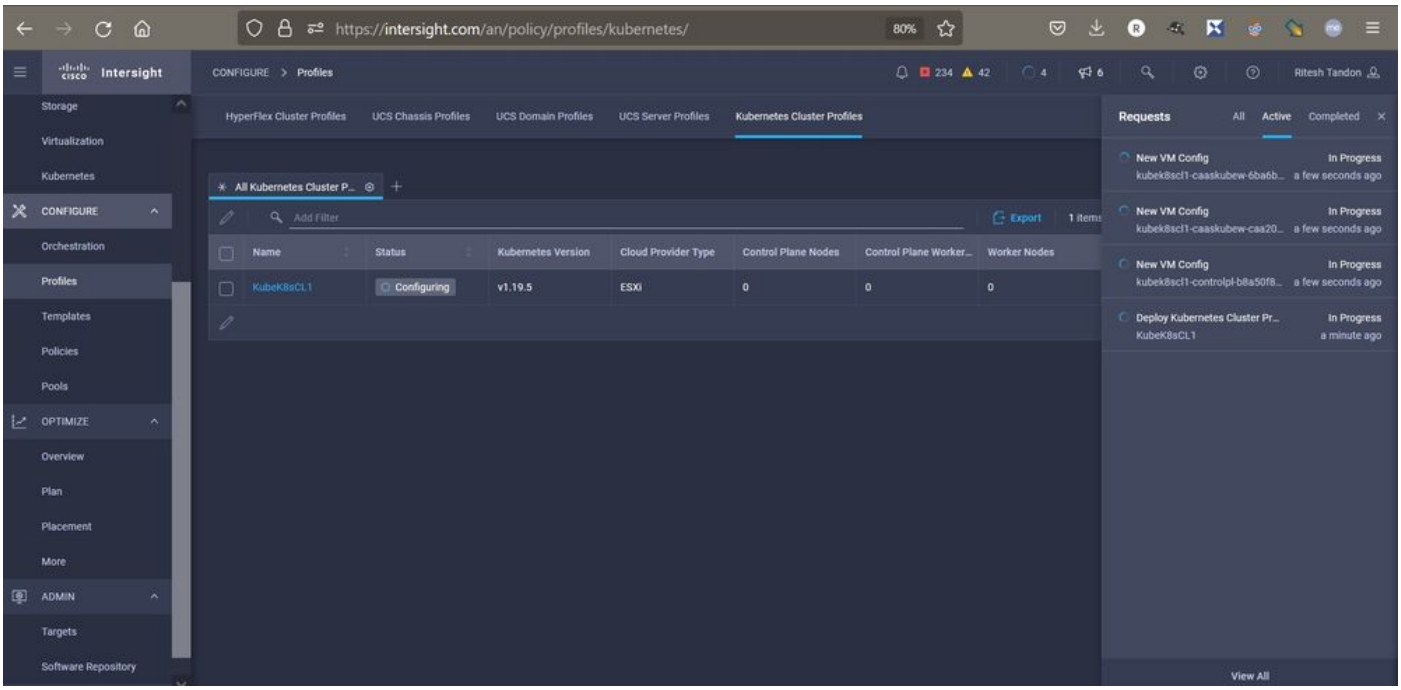


Écran Résumé de création de profil

Vérifier

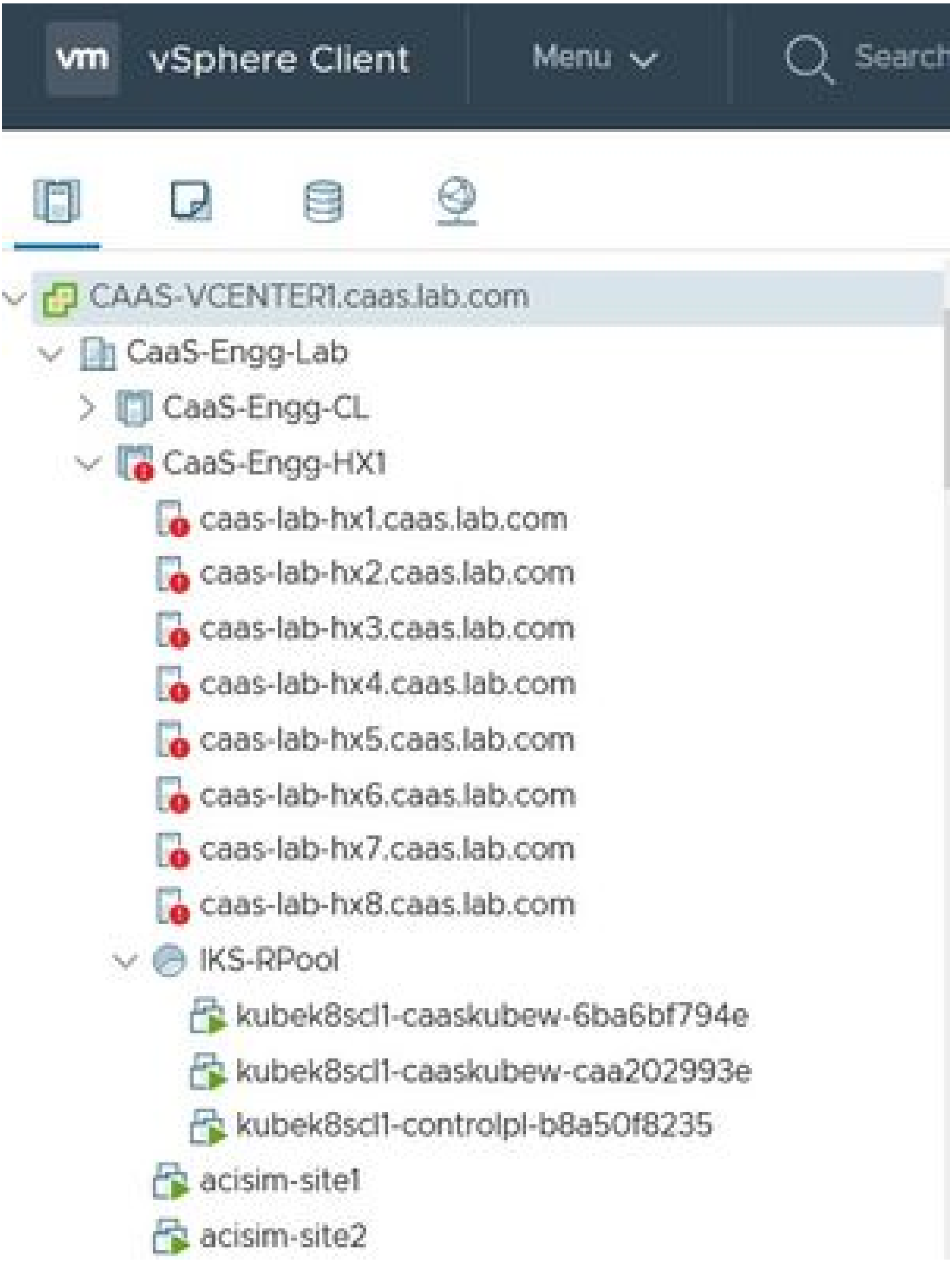
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Dans l'angle supérieur droit, vous pouvez suivre la progression du déploiement.



Vérification via l'interface utilisateur IKS

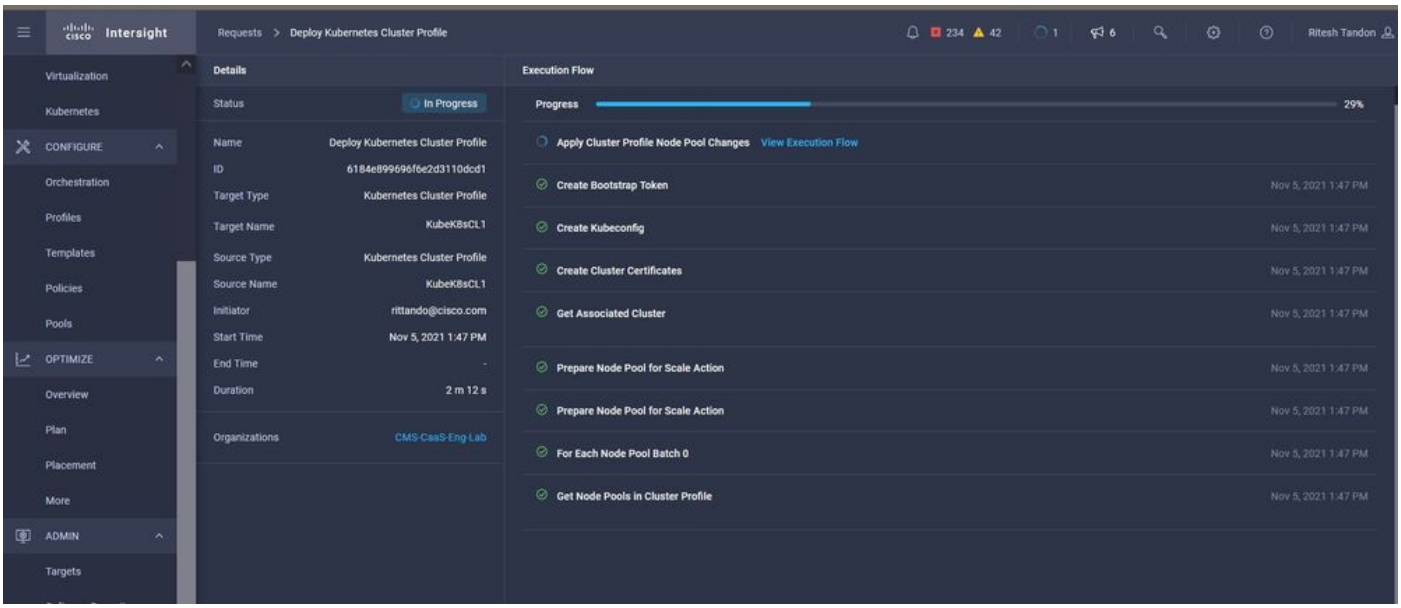
Au fur et à mesure du déploiement, vous pouvez voir vos noeuds Kubernetes Master et Worker apparaître sur le vCenter.



Cluster IKS bientôt disponible dans vCenter

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

l'exécution.



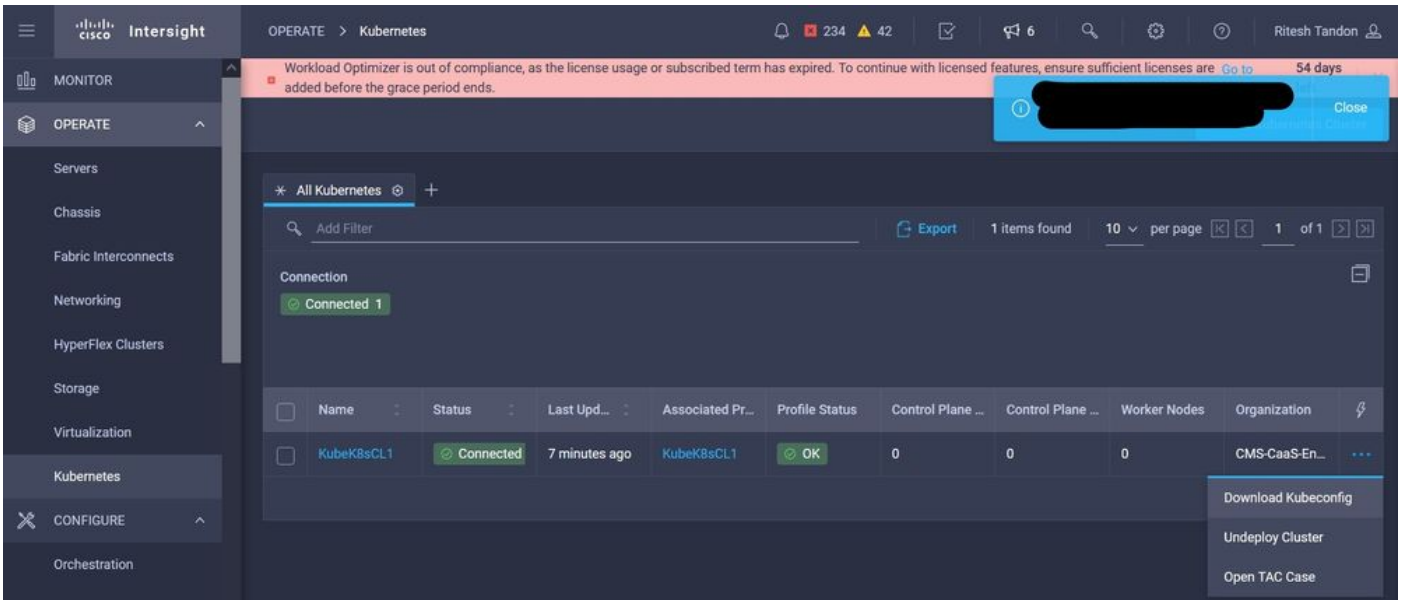
Exécution de création de profil

Se connecter au cluster Kubernetes

Vous pouvez vous connecter au cluster Kubernetes de l'une des manières suivantes :

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 utiliser SSH directement dans le noeud maître, en utilisant des applications SSH comme Putty avec les informations d'identification et la clé privée configurées au moment du déploiement

Si vous déployez 'Kubernetes Dashboard' comme Add-on, vous pouvez également l'utiliser pour déployer des applications directement à l'aide de l'interface graphique utilisateur.

Pour en savoir plus, consultez la section « Accès aux clusters Kubernetes », ici :

Vérifier avec CLI

Une fois que vous êtes en mesure de vous connecter au cluster Kubernetes, en utilisant kubeCtl, vous pouvez utiliser les commandes suivantes pour vérifier si le cluster a tous les composants installés et en cours d'exécution.

Vérifiez que les noeuds du cluster sont à l'état « Prêt ».

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



           6d4h   v1.19.5
kubek8scl1-caaskubew-caa202993e   Ready



            6d4h   v1.19.5
kubek8scl1-controlpl-b8a50f8235   Ready    master   6d4h   v1.19.5
```

Vérifiez l'état des pods qui ont été 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 ccp-helm-operator qui gère la barre en cours d'exécution locale 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/.k
NAME                    NAMESPACE       REVISION        UPDATED                                 STATUS
addon-operator          iks             1               2021-11-05 07:45:15.44180913 +0000 UTC  deploye
ccp-monitor             iks             1               2021-11-05 08:23:11.309694887 +0000 UTC deploye
essential-cert-ca       iks             1               2021-11-05 07:55:04.409542885 +0000 UTC deploye
essential-cert-manager  iks             1               2021-11-05 07:54:41.433212634 +0000 UTC deploye
essential-metallb       iks             1               2021-11-05 07:54:48.799226547 +0000 UTC deploye
essential-nginx-ingress iks             1               2021-11-05 07:54:46.762865131 +0000 UTC deploye
essential-registry      iks             1               2021-11-05 07:54:36.734982103 +0000 UTC deploye
essential-vsphere-csi   kube-system     1               2021-11-05 07:54:58.168305242 +0000 UTC deploye
kubernetes-dashboard    iks             1               2021-11-05 07:55:10.197905183 +0000 UTC deploye
vsphere-cpi             kube-system     1               2021-11-05 07:54:38.292088943 +0000 UTC deploye
```

Vérifiez l'état des modules complémentaires Essential-* qui gèrent les modules complémentaires Essential (principaux), 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   PO
ccp-monitor-grafana                                 ClusterIP      192.168.23.161


                80/TCP                      6d3h
```

```
ccp-monitor-prometheus-alertmanager                    ClusterIP      192.168.23.70

                 80/TCP                         6d3h
ccp-monitor-prometheus-kube-state-metrics              ClusterIP      None

                  80/TCP                        6d3h
ccp-monitor-prometheus-node-exporter                   ClusterIP      None

                 9100/TCP                       6d3h
ccp-monitor-prometheus-pushgateway                     ClusterIP      192.168.23.130

                  9091/TCP                      6d3h
ccp-monitor-prometheus-server                          ClusterIP      192.168.23.95

                  443/TCP                       6d3h
essential-cert-manager                                 ClusterIP      192.168.23.178

                  9402/TCP                      6d4h
essential-cert-manager-webhook                         ClusterIP      192.168.23.121

                  443/TCP                       6d4h
essential-nginx-ingress-ingress-nginx-controller       LoadBalancer   192.168.23.26    192.168.10.11
essential-nginx-ingress-ingress-nginx-defaultbackend   ClusterIP      192.168.23.205

                  80/TCP                        6d4h
essential-registry-docker-registry                     ClusterIP      192.168.23.12

                  443/TCP                       6d4h
kubernetes-dashboard                                   ClusterIP      192.168.23.203

                  443/TCP                       6d4h
```

Dépannage

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

Dans le cas où un pod particulier ne s'affiche pas, vous pouvez utiliser ces commandes pour explorer la cause vers le bas.

```
Syntax : kubectl describe pod


         -n




Example :
kubectl describe pod vsphere-csi-controller-7d56dc7c8-qgbhw -n kube-system
Name:         vsphere-csi-controller-7d56dc7c8-qgbhw
Namespace:    kube-system
Priority:     0
Node:         kubek8scl1-controlpl-eb44cf1bf3/192.168.58.11
Start Time:   Tue, 28 Sep 2021 02:39:41 +0000
Labels:       app=vsphere-csi-controller
              pod-template-hash=7d56dc7c8
              role=vsphere-csi
Annotations:




Status:       Running
IP:           192.168.58.11
IPs:
  IP:           192.168.58.11
Controlled By:  ReplicaSet/vsphere-csi-controller-7d56dc7c8
Containers:
  csi-attacher:
    Container ID:  docker://60002693136d00f3b61237304a1fbc033df92f86dc1352965328fe3c4d264fdb
    Image:         registry.ci.x----x.com/cpsg_kaas-images/quay.io/k8scsi/csi-attacher:v2.0.0
    Image ID:      docker-pullable://registry.ci.x------x.com/cpsg_kaas-images/quay.io/k8scsi/csi-attac
    Port:
```

```
    Host Port:



    Args:
      --v=4
      --timeout=300s
      --csi-address=$(ADDRESS)
      --leader-election
    State:          Running
      Started:      Thu, 30 Sep 2021 05:44:11 +0000
    Last State:     Terminated
      Reason:       Error
      Message:      Lost connection to CSI driver, exiting
      Exit Code:    255
      Started:      Thu, 30 Sep 2021 05:38:20 +0000
      Finished:     Thu, 30 Sep 2021 05:39:06 +0000
    Ready:          True
    Restart Count:  531

X---------------------- Log Text Omitted ---------X----------------------X--------------------X
```

Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.