Konfigurieren des Kuberneten-Clusters mithilfe des Intersight KubertributeService

Inhalt

Einleitung
Hintergrundinformationen
Lösungsüberblick
Voraussetzungen
Anforderungen
Verwendete Komponenten
Annahmen
Konfiguration
Schritt 1: Richtlinien konfigurieren
Schritt 2: Profil konfigurieren
Überprüfung
Herstellen einer Verbindung zum Kuberneten-Cluster
Verifizieren mit CLI
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration zur Bereitstellung eines in der Produktion betriebenen Kuberneten-Clusters von Cisco Intersight (SaaS) mithilfe des Cisco Intersight™ Kuberettservice (IKS) beschrieben.

Hintergrundinformationen

Kubernete hat sich in jüngster Zeit zu einem de-facto-Containermanagement-Tool entwickelt, da Unternehmen tendenziell mehr in die Anwendungsmodernisierung mit Containerized-Lösungen investieren. Mit Kubernets können Entwicklungsteams ihre containerisierten Anwendungen ganz einfach bereitstellen, verwalten und skalieren. So wird der Zugriff auf Innovationen für die kontinuierliche Bereitstellung erleichtert.

Kubernetes bringt jedoch betriebliche Herausforderungen mit sich, da Installation und Konfiguration zeitaufwendig und technisches Know-how erfordern.
Die Installation von Kuberneten und den verschiedenen erforderlichen Softwarekomponenten, die Erstellung von Clustern, die Konfiguration von Storage, Netzwerk und Sicherheit sowie die Durchführung von Abläufen (z. B. Upgrades, Updates und Patches für kritische Sicherheitslücken) erfordern fortlaufend erhebliche Investitionen in Humankapital.

Die Einstiegslösung IKS, eine sofort einsatzbereite SaaS-Lösung für die Verwaltung konsistenter, produktionssicherer Kubernete an jedem Ort. Weitere Informationen zu den Funktionen von IKS finden Sie hier.

Lösungsüberblick

In diesem Dokument soll gezeigt werden, dass IKS nahtlos in Ihre Infrastruktur vor Ort integriert werden kann, wobei VMware ESXi und vCenter ausgeführt werden.
Mit wenigen Klicks können Sie ein kubernetes Cluster der Produktionsklasse auf Ihrer VMware-Infrastruktur bereitstellen.

Dazu müssen Sie jedoch Ihr Vor-Ort-vCenter mit Intersight integrieren, das als "Anfechten eines Ziels" bekannt ist, wobei vCenter hier das Ziel ist.
Sie benötigen eine Cisco Intersight Assist Virtual Appliance, mit der Sie Endgeräte-Ziele zu Cisco Intersight hinzufügen können. Sie können Intersight Assist mithilfe der Bootstrap-OVA installieren, die auf der offiziellen Website von Cisco verfügbar ist.

Um den Umfang dieses Dokuments zu begrenzen, sollten wir uns nicht auf die Installation der Cisco Intersight Assist Virtual Appliance konzentrieren. Aber Sie können sich den Prozess hier ansehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Intersight-Konto: Sie benötigen eine gültige Cisco ID und ein Intersight-Konto.
  Wenn Sie keine Cisco ID haben, können Sie auf der Cisco Website eine Cisco ID erstellen.
  Klicken Sie anschließend auf Intersight auf den Link Create an Account (Konto erstellen).
- Cisco Intersight-Unterstützung: Cisco Intersight Assist unterstützt Sie beim Hinzufügen von vCenter/ESXi als Endgeräteziel zu Cisco Intersight.
- Konnektivität: Wenn Ihre Umgebung einen HTTP/S-Proxy unterstützt, können Sie diese verwenden, um Ihre Cisco Intersight Assist Appliance mit dem Internet zu verbinden.
  Alternativ müssen Sie Ports öffnen, um URLs anzuzeigen. Bitte überprüfen Sie diesen Link für detaillierte Netzwerkanbindungsanforderungen:
- vCenter-Anmeldeinformationen, um diese bei Intersight anzufordern.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Annahmen

Da die Bereitstellung einer Cisco Intersight Appliance nicht im Umfang dieses Dokuments enthalten ist.

Wir gehen davon aus, dass Sie bereits über ein funktionierendes Intersight-Konto verfügen und erfolgreich ein Vor-Ort-vCenter/ESXi-Konto angefordert haben.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

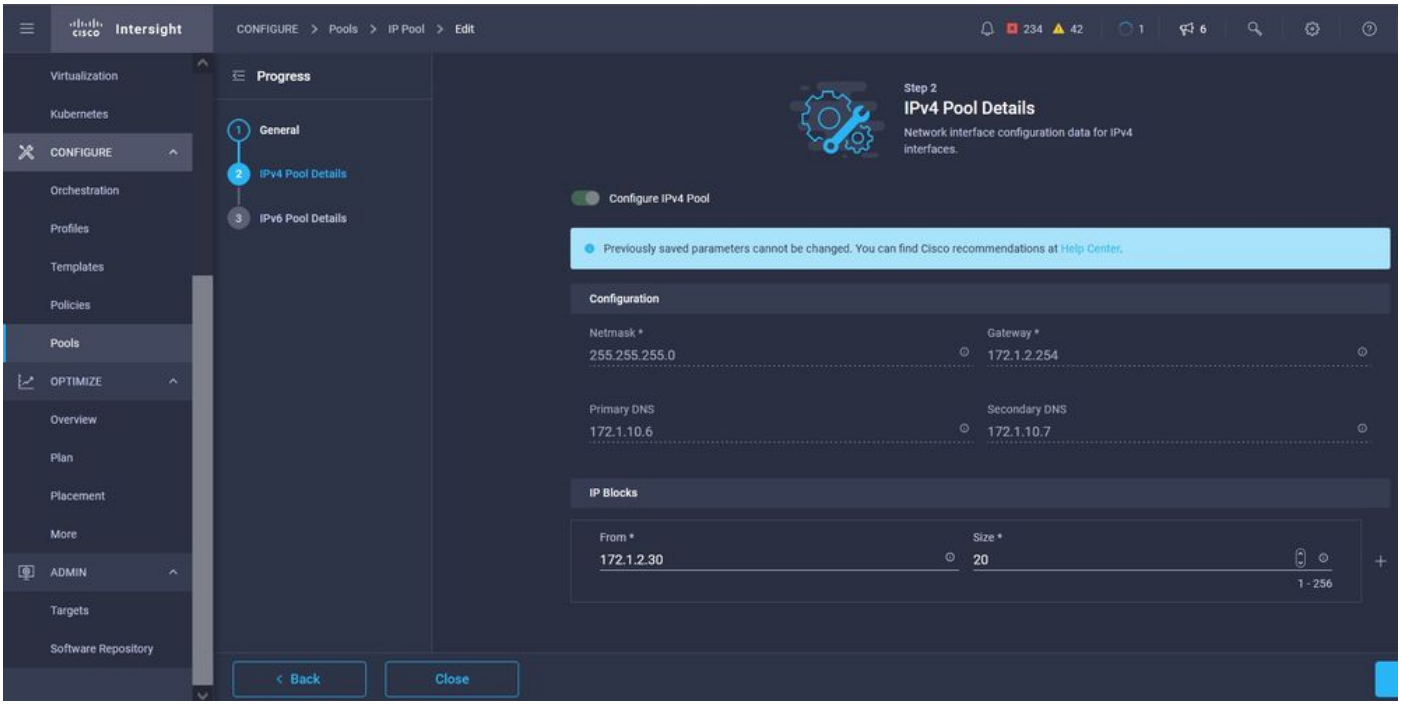
Schritt 1: Richtlinien konfigurieren

Richtlinien ermöglichen eine vereinfachte Verwaltung, da sie die Konfiguration in wiederverwendbare Vorlagen abstrahieren.

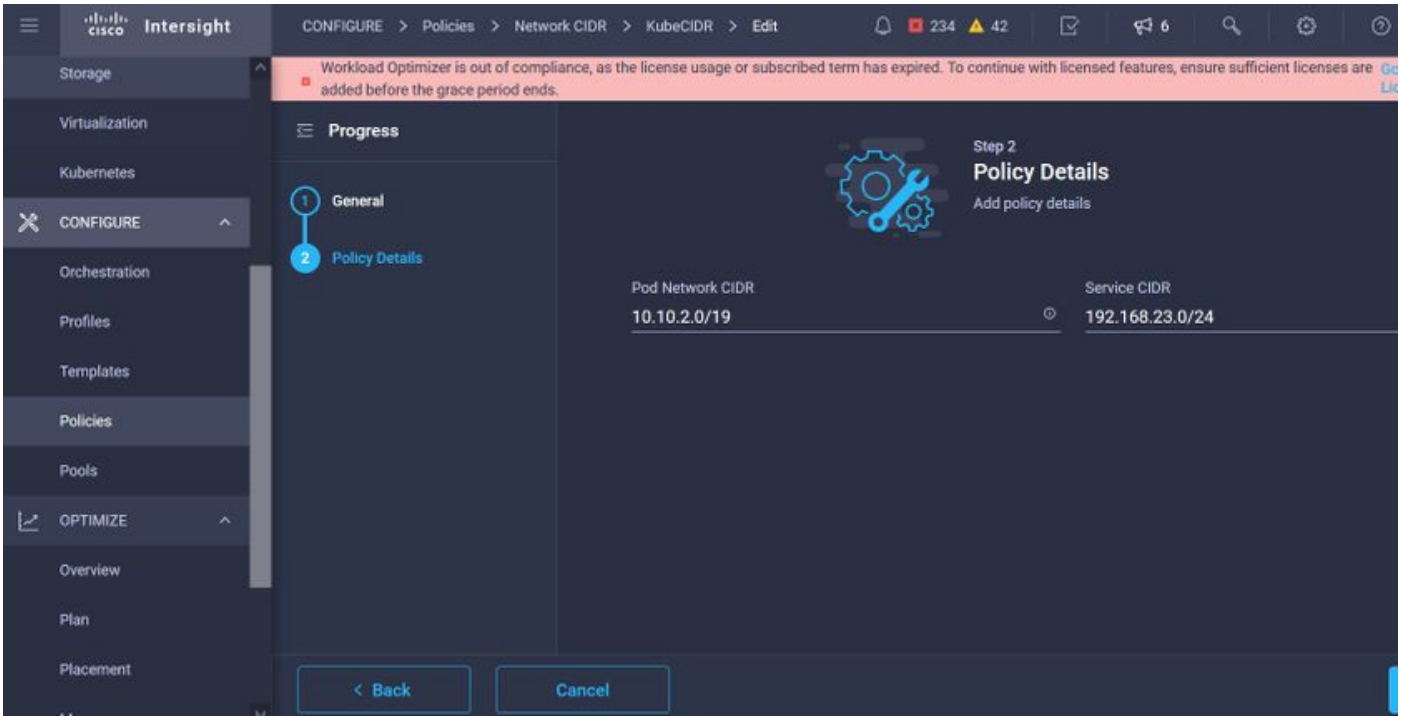
Einige der Richtlinien, die wir konfigurieren müssen, sind nachfolgend aufgeführt. Bitte beachten Sie, dass alle diese Richtlinien im Abschnitt Konfigurieren >> Richtlinien & Konfigurieren >> Pools unter "Intersight" erstellt werden.

Sie können den Pfad der Richtlinie auch oben in jedem Screenshot sehen, wie unten dargestellt.

Dieser IP-Pool wird für IP-Adressen auf Ihren virtuellen Systemen mit Steuerungs- und Arbeitsknoten verwendet, wenn er auf dem ESXi-Host gestartet wird.

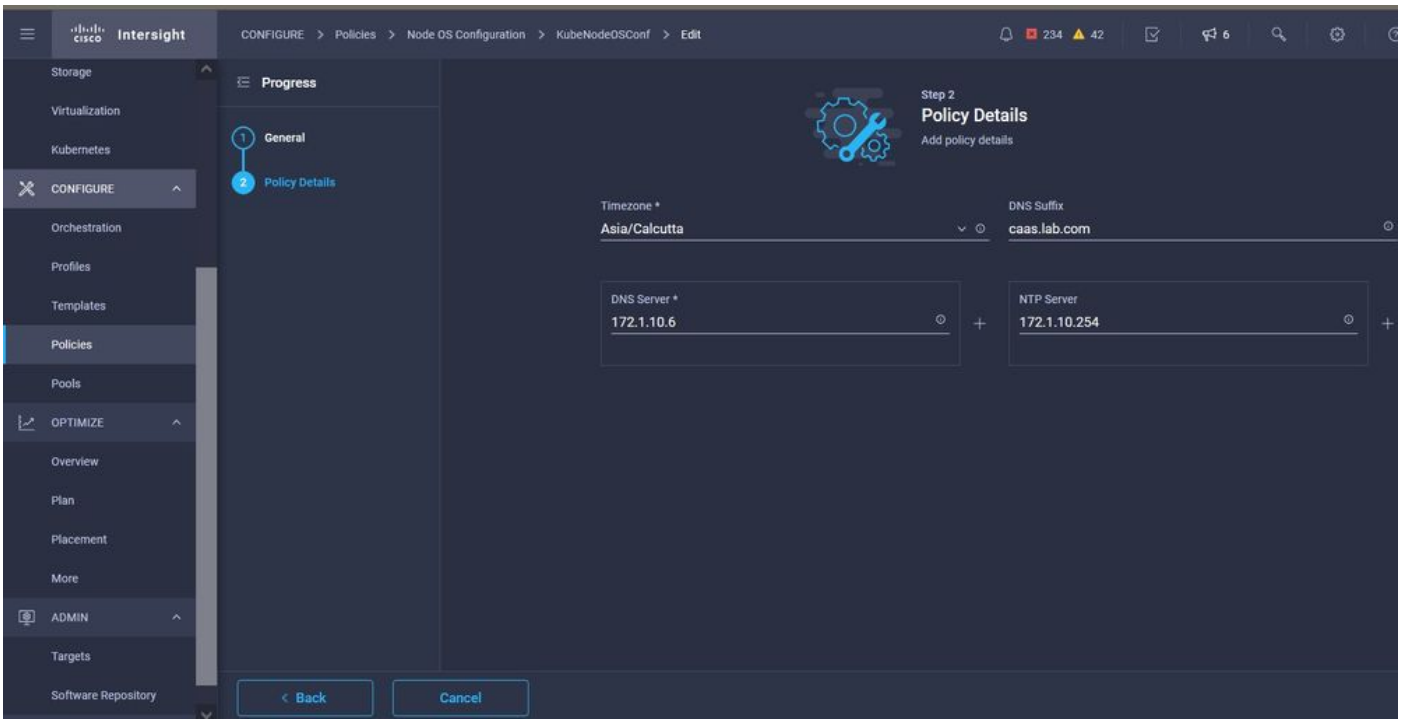


Hier definieren Sie den Pod and Services Network CIDR für interne Netzwerke im Kuberneten Cluster.



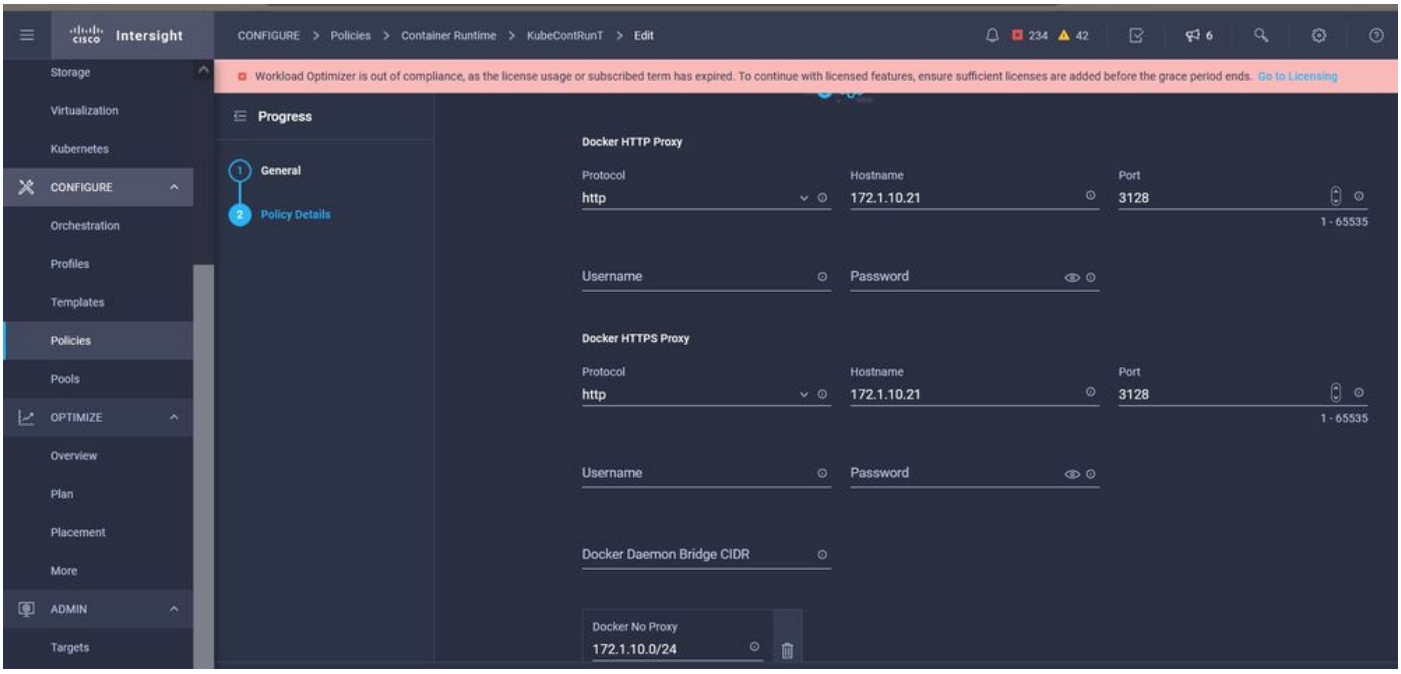
Services und Netzwerk-CIDR

Diese Richtlinie definiert Ihre NTP- und DNS-Konfiguration.



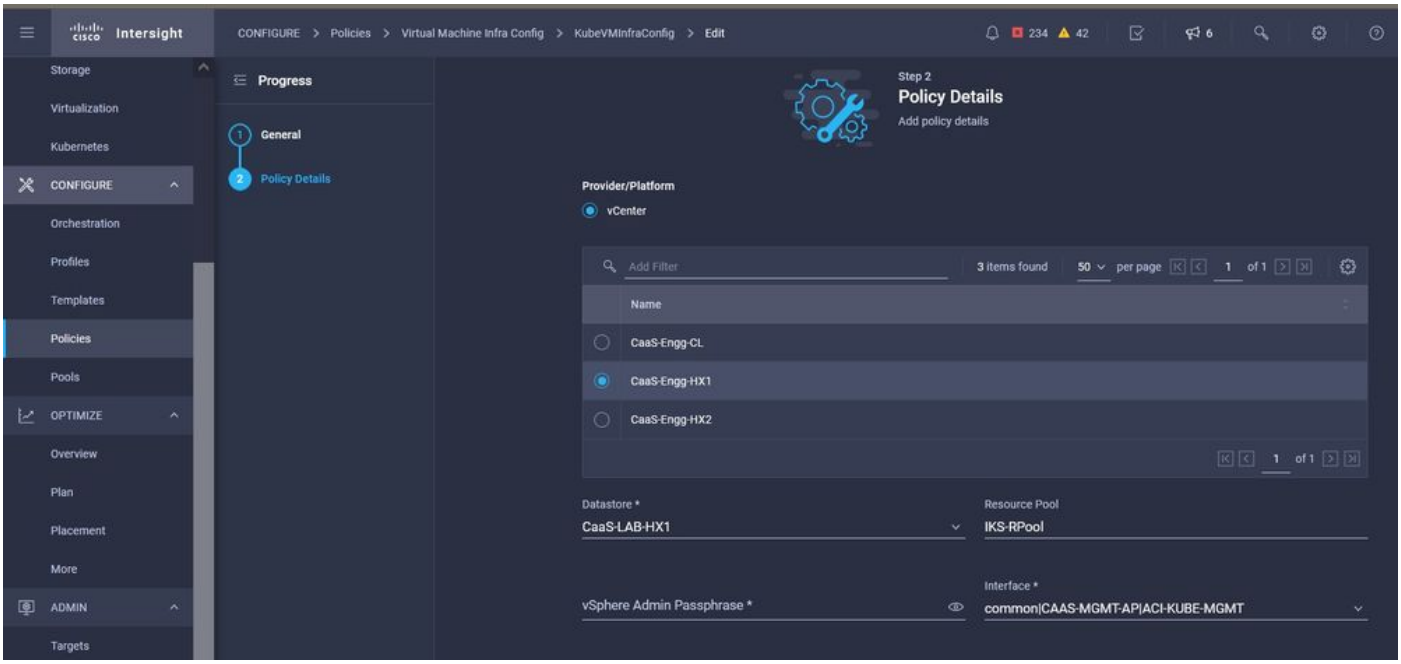
NTP- und DNS-Konfiguration

Mit dieser Richtlinie können Sie die Proxykonfiguration für die Laufzeit des Dockers-Containers definieren.



Proxy-Konfiguration für Docker

In dieser Richtlinie definieren Sie die erforderliche Konfiguration für die als Master- und Worker-Knoten bereitgestellten virtuellen Systeme.



Konfiguration der verwendeten VMs

Schritt 2: Profil konfigurieren

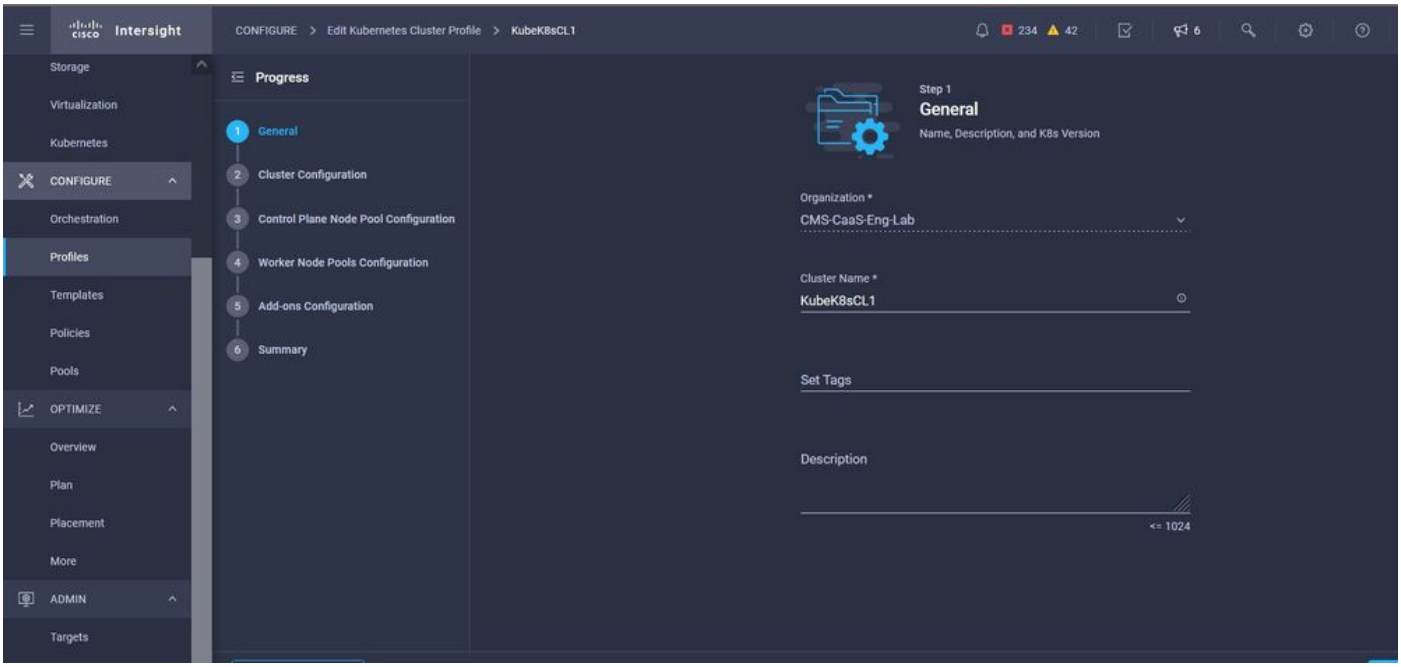
Sobald wir die oben genannten Richtlinien erstellt haben, werden sie in ein Profil gebunden, das wir dann bereitstellen können.

Durch die Bereitstellung von Konfigurationen mithilfe von Richtlinien und Profilen wird die Konfigurationsebene abstrahiert, sodass sie wiederholt und schnell bereitgestellt werden kann.

Sie können dieses Profil kopieren und innerhalb weniger Minuten ein neues Profil mit wenigen oder mehr Änderungen an den zugrunde liegenden Richtlinien erstellen, das in einem oder mehreren Kuberetteten-Clustern in einem Bruchteil der Zeit, die Sie mit einem manuellen Prozess

benötigen, erstellt wird.

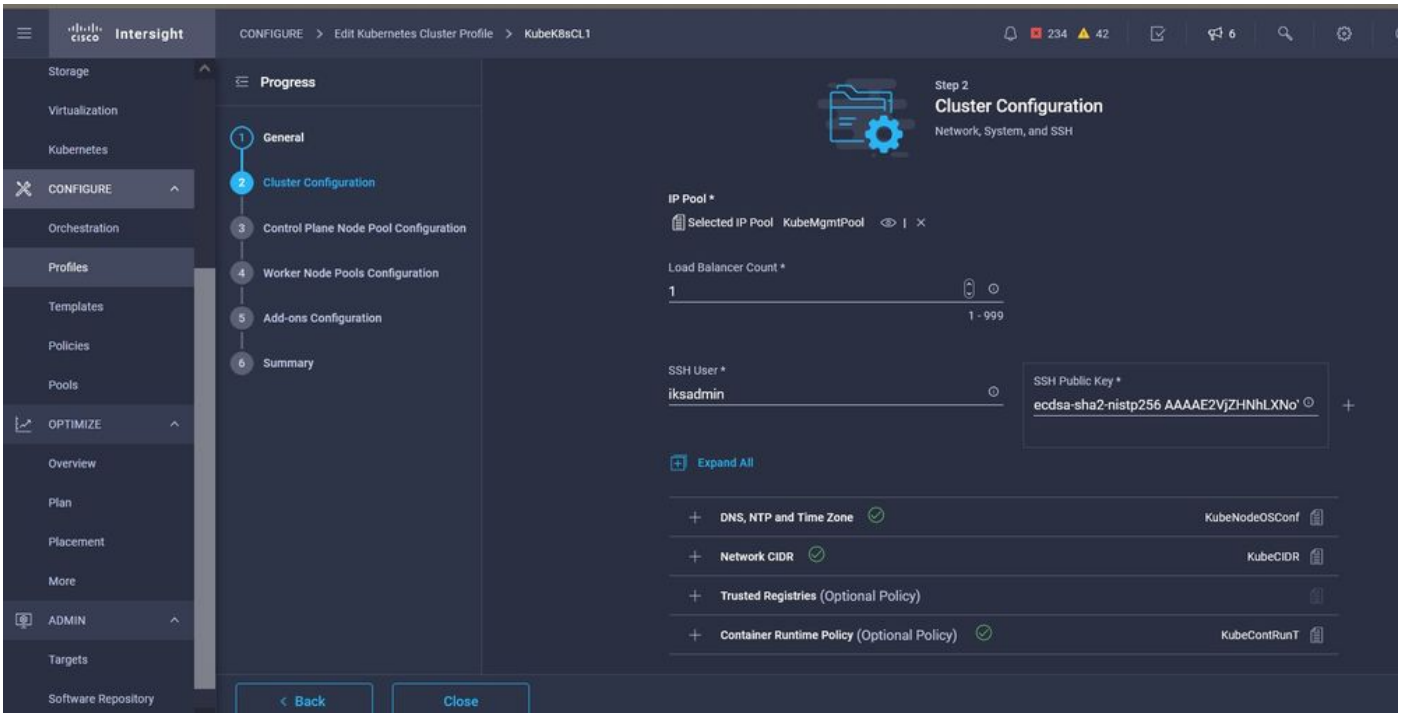
GIve in den Namen und setzen Tags.



Profilkonfiguration mit Namen und Tags

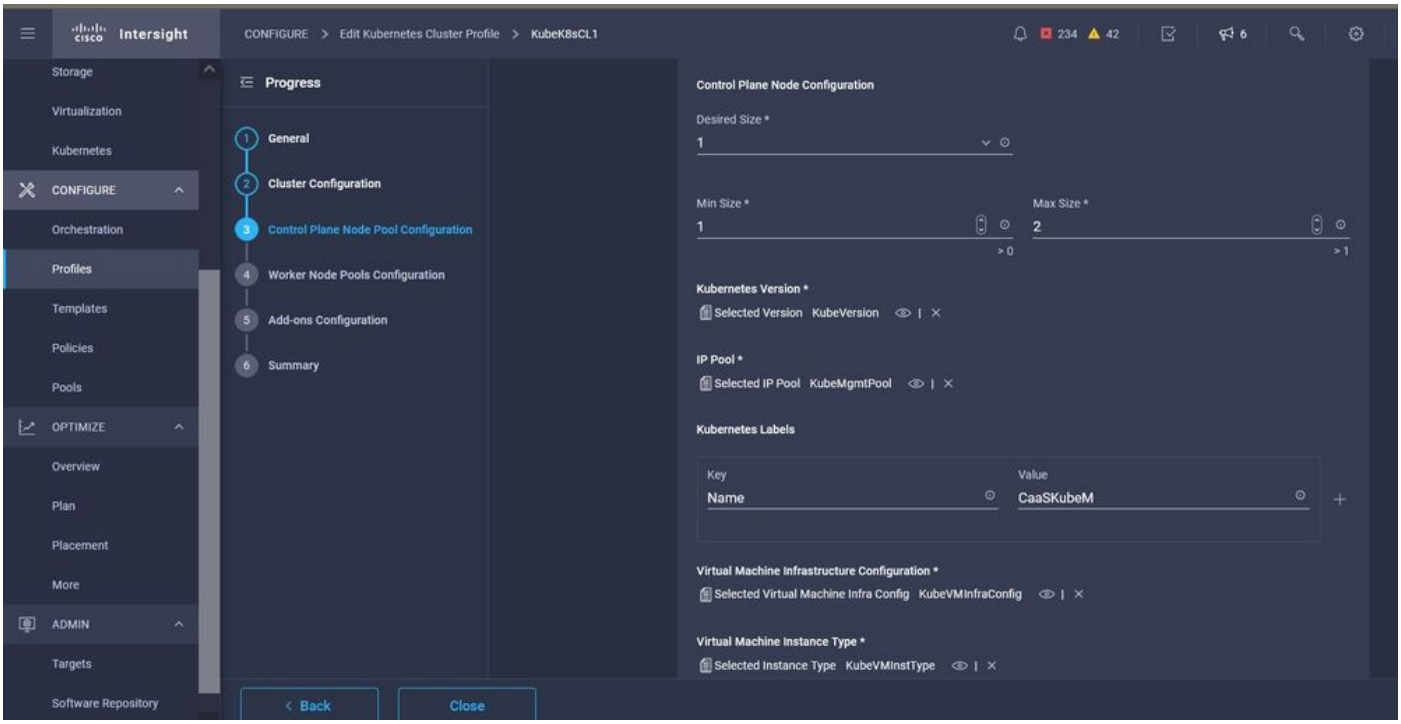
Legen Sie die Richtlinien für Pool, Node-Betriebssystem, Network CIDR fest. Sie müssen auch eine Benutzer-ID und einen SSH-Schlüssel (öffentlich) konfigurieren.

Der entsprechende private Schlüssel wird zum SSH in Master- und Worker-Knoten verwendet.



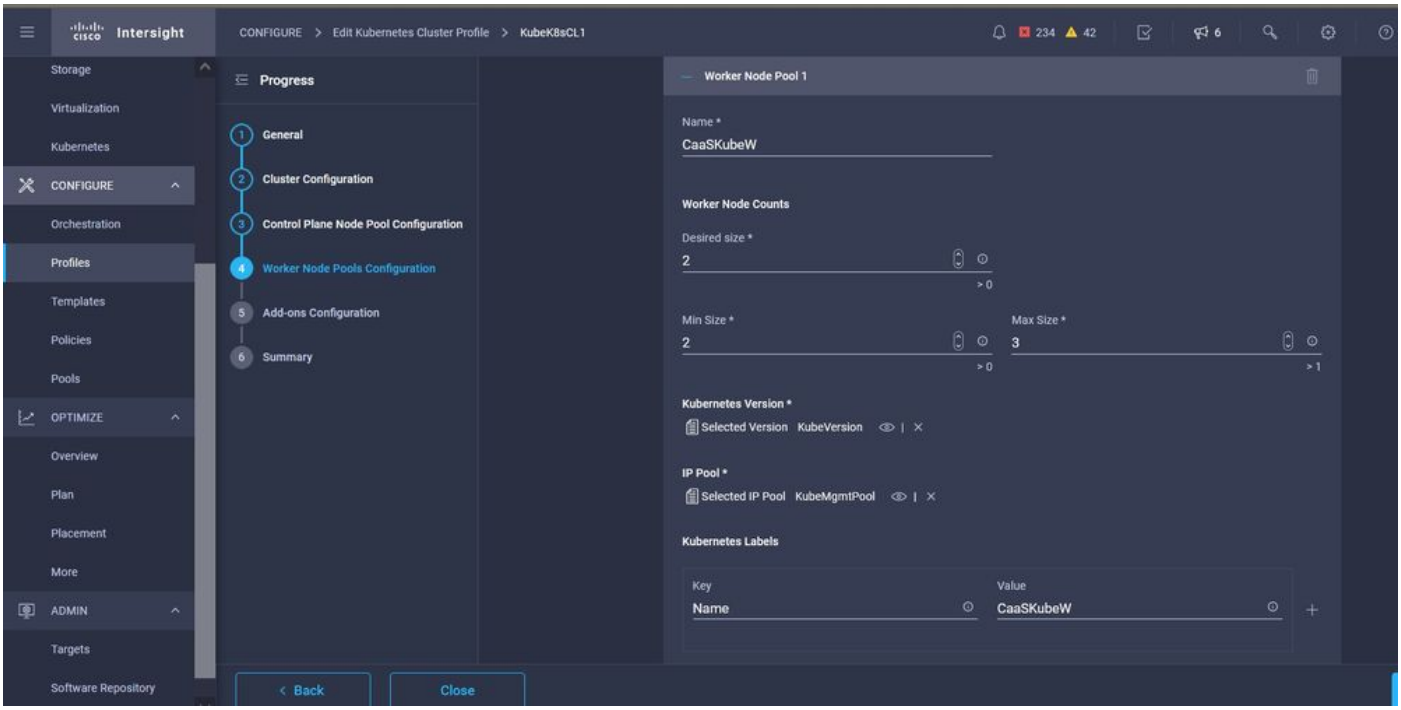
Profilkonfiguration mit zugewiesenen Richtlinien

Konfigurieren Sie die Kontrollebene: Sie können festlegen, wie viele Master-Knoten Sie auf der Kontrollebene benötigen.



Master Node-Konfiguration

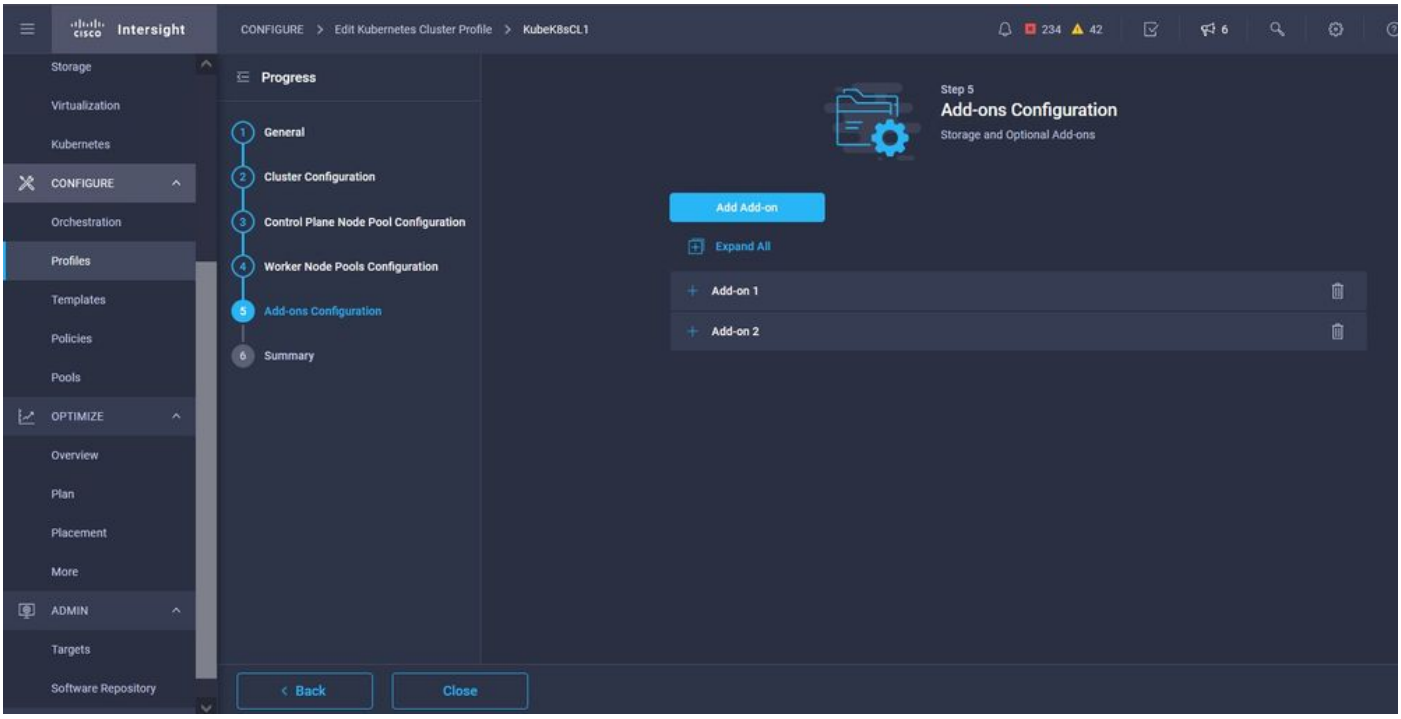
Konfigurieren der Arbeitsknoten: Je nach Anwendungsanforderungen können Sie die Knoten Ihrer Mitarbeiter nach oben oder unten skalieren.



Konfiguration von Arbeitsknoten

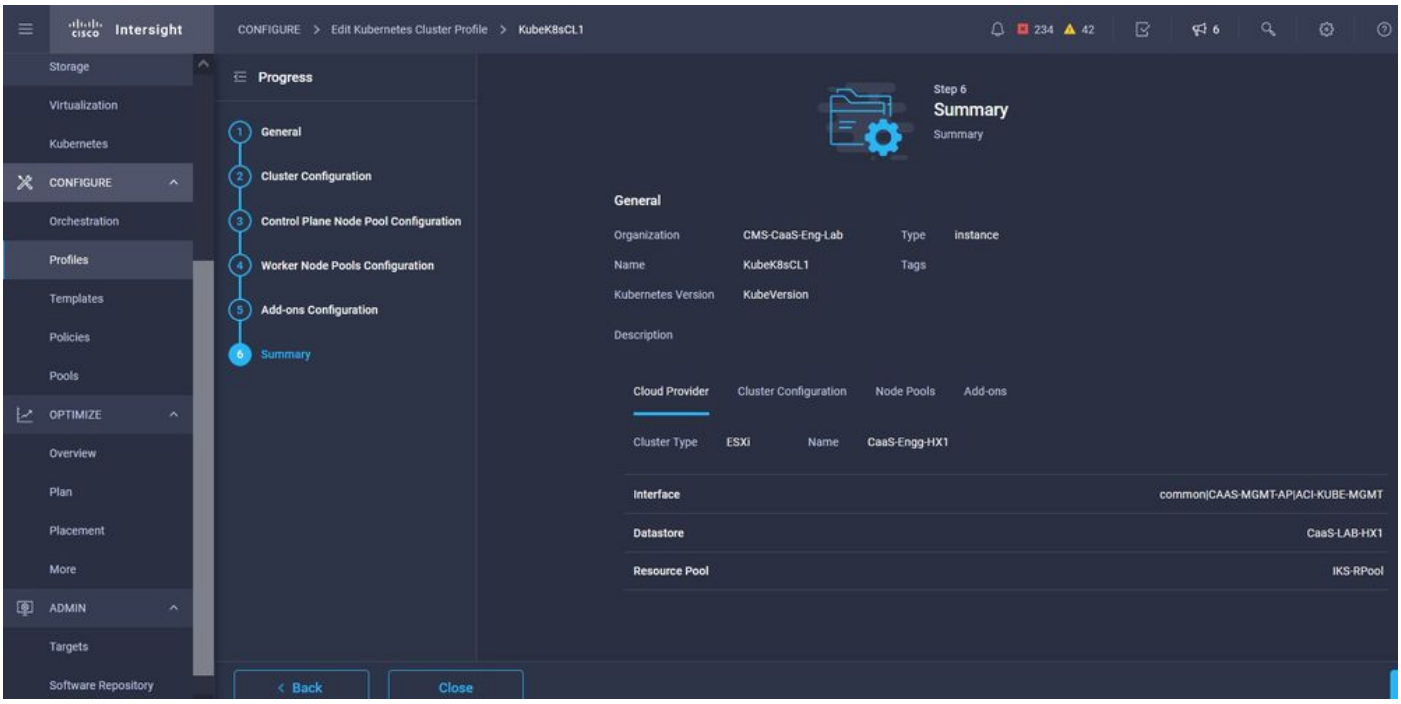
Konfigurieren Sie das Add-on. Ab sofort können Sie mit Prometheus Monitoring automatisch Kubernetes Dashboard und Graffana bereitstellen.

In Zukunft können Sie weitere Add-ons hinzufügen, die Sie automatisch mithilfe von IKS bereitstellen können.



Add-ONs (falls vorhanden)

Überprüfen Sie die Übersicht, und klicken Sie auf **Bereitstellen**.

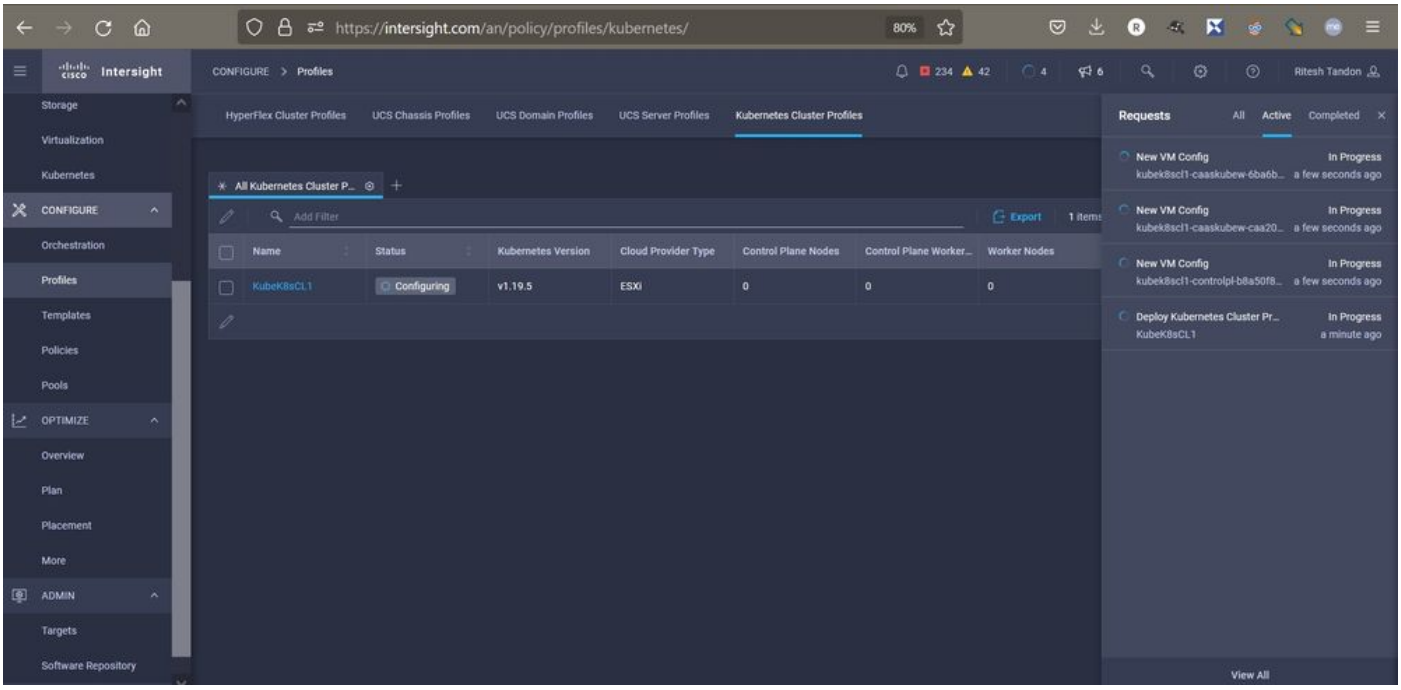


Bildschirm "Übersicht über die Erstellung von Profilen"

Überprüfung

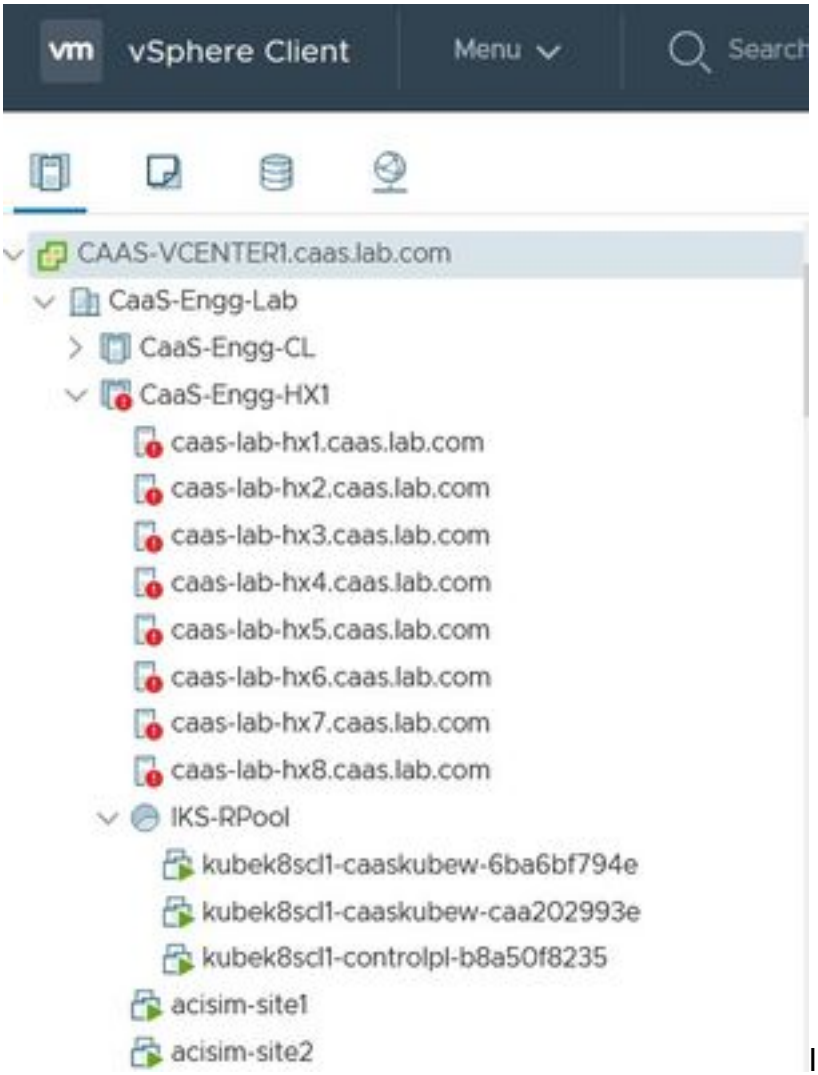
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Oben rechts können Sie den Fortschritt der Bereitstellung verfolgen.



Überprüfen der IKS-GUI

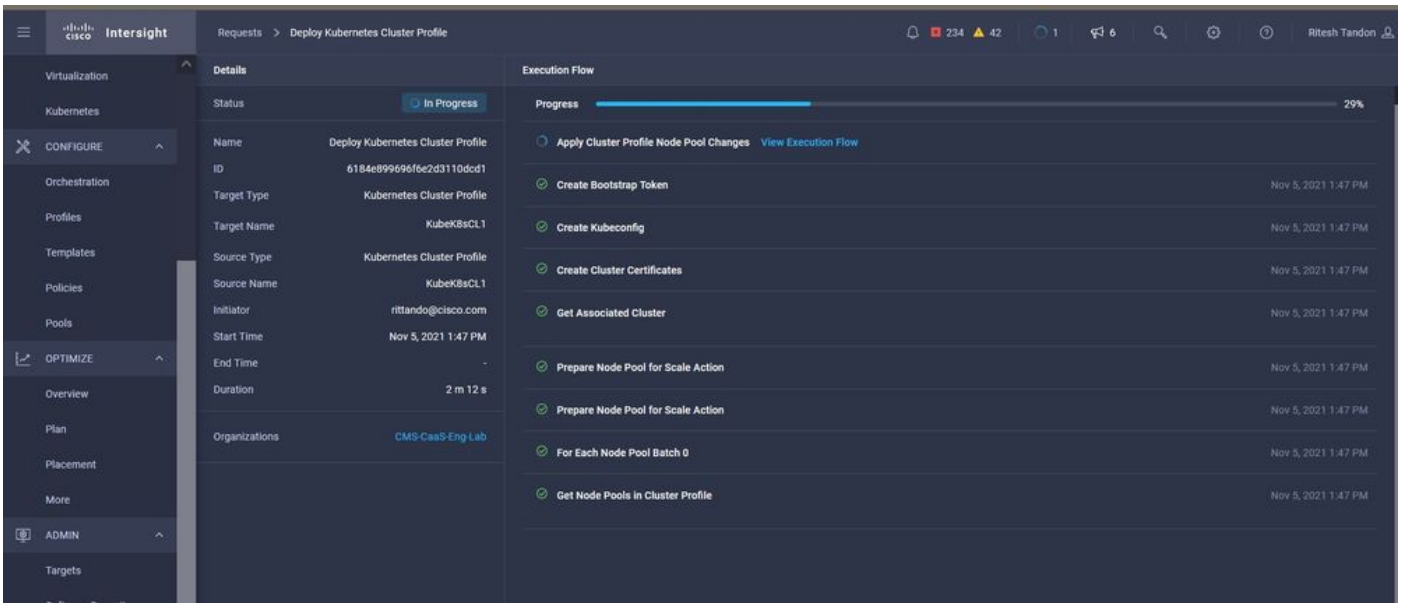
Im Verlauf der Bereitstellung werden die Kubernet Master- und Worker-Knoten im vCenter angezeigt.



IKS-Cluster kommt in vCenter auf

Wenn Sie detaillierte Schritte für die Bereitstellung sehen müssen, können Sie die Ausführung

genauer untersuchen.



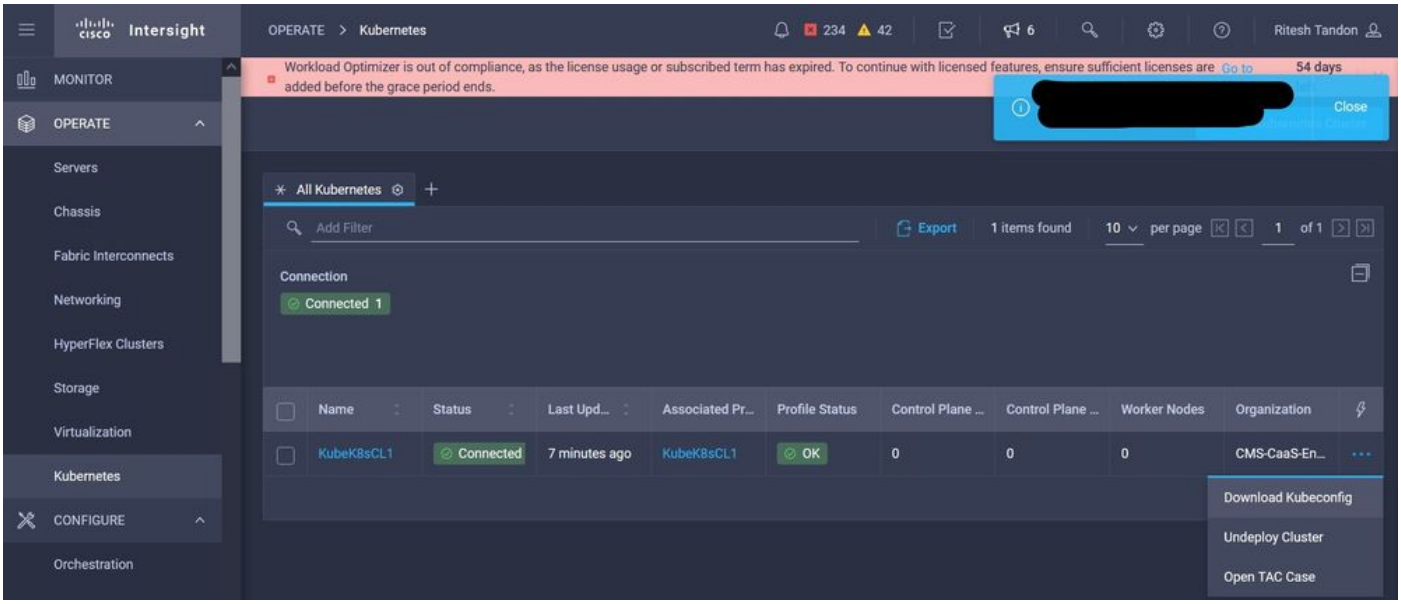
Erstellung von Profilen

Herstellen einer Verbindung zum Kuberneten-Cluster

Es gibt folgende Möglichkeiten, eine Verbindung zum Kuberneten-Cluster herzustellen:

Verwenden Sie die KubeConfig-Datei, die Sie von **Operate > Kuberettes > Wählen Sie die Optionen ganz rechts aus**.

KubeCtl muss auf der Management-Workstation installiert sein, von wo aus Sie auf diesen Cluster zugreifen möchten.



KubeConfig-Datei von IKS herunterladen

Sie können SSH auch direkt in den Master-Knoten eingeben, indem Sie SSH-Anwendungen wie Putty verwenden, für die die Anmeldeinformationen und der private Schlüssel zum Zeitpunkt der Bereitstellung konfiguriert sind.

Wenn Sie "Kubernetes Dashboard" als Add-on bereitstellen, können Sie dies auch verwenden, um

Anwendungen direkt über die Benutzeroberfläche bereitzustellen.

Weitere Einzelheiten finden Sie im Abschnitt "Zugriff auf kubernete Cluster" hier:

Verifizieren mit CLI

Wenn Sie mit kubeCtl eine Verbindung zum Kuberneten-Cluster herstellen können, können Sie mithilfe der folgenden Befehle überprüfen, ob alle Komponenten im Cluster installiert und ausgeführt sind.

Stellen Sie sicher, dass die Knoten im Cluster den Status 'ready' haben.

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

Überprüfen Sie den Status der PODs, die zum Zeitpunkt der Installation der wesentlichen Komponenten auf dem Cluster erstellt wurden.

```
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
```

Überprüfen Sie den Status des ccp-helm-operator-POD, der den lokal laufenden Helm verwaltet und Add-ons installiert.

```
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
```

Überprüfen Sie den Status der unverzichtbaren* PODs, die die standardmäßig installierten Essential (Core)-Add-ons auf jedem IKS-Tenant-Cluster verwalten.

```
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
```

Überprüfen Sie den Status der Dienste und des im IKS-Namespace bereitgestellten Load Balancers.

```
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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Falls ein bestimmter POD nicht hochgefahren wird, können Sie diese Befehle verwenden, um die Ursache zu ermitteln.

```
Syntax : kubectl describe pod
```

Zugehörige Informationen

- Siehe IKS-Servicebeschreibung hier.
- Überprüfen Sie hier das Benutzerhandbuch.
- Informieren Sie sich hier über die Intersight-Servicedemo.
- Technischer Support und Dokumentation für Cisco Systeme