

TECHDOCS

CN-Seriesファイアウォールのクラウド およびオンプレミスへのデプロイメン ト

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 13, 2021

Table of Contents

CN-Series ファイアウォールを GKE にデプロイする.....	5
CN-Series ファイアウォールを Kubernetes サービスとして GKE に デプロイす る.....	7
CN-Series ファイアウォールを GKE に DaemonSet としてデプロイする.....	20
CN-Series ファイアウォールを OKE にデプロイする.....	33
CN-Series ファイアウォールを OKE に Kubernetes サービスとしてデプロイす る.....	35
CN-Series ファイアウォールを OKE に DaemonSet としてデプロイする.....	48
CN-Series ファイアウォールを EKS にデプロイする.....	61
CN-Series ファイアウォールを AWS EKS に Kubernetes サービスとしてデプロイす る.....	63
CN-Series ファイアウォールを AWS EKS に DaemonSet としてデプロイする.....	72
AWS Marketplace から CN-Seriesをデプロイする.....	82
CN-Series ファイアウォールを AliCloud (ACK) に Kubernetes サービ スとしてデプロイする.....	89
CN-Series を OpenShift にデプロイする.....	111
CN-Series を OpenShift にデプロイする.....	113

CN-Series ファイアウォールを GKE にデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Seriesデプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.x以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CNシリーズ ビルディング ブロックとCNシリーズ ファイアウォールによるKubernetesの安全な環境内のワークフローの概要を確認したら、同じクラスタ内のコンテナ間やコンテナと他のワークロード タイプ(仮想マシンやベアメタル サーバーなど)間のトラフィックを保護するためのGKE プラットフォームにおけるCN-Series ファイアウォールのデプロイから始めることができます。



Kubernetes クラスタ、アプリケーション、およびファイアウォール サービスをデプロイして管理するためには、*kubectl* や *Helm* などの標準の *Kubernetes* ツールが必要です。

詳細については、「*Helm* チャートとテンプレートを使用した [CN-Series ファイアウォールのデプロイ](#)」を参照してください。*Panorama* は、*Kubernetes* クラスタのデプロイメントと管理用のオーケストレーターになるようには設計されていません。クラスタ管理用のテンプレートがマネージド *Kubernetes* プロバイダから提供されています。*Palo Alto Networks* は、*Helm* および *Terraform* で *CN-Series* をデプロイするためのコミュニティサポートのテンプレートを提供しています。

- [CN-Series ファイアウォールを Kubernetes サービスとして GKE に デプロイする](#)
- [CN-Series ファイアウォールを GKE に DaemonSet としてデプロイする](#)



CN-Series を *DaemonSet* としての *CN-Series* からサービスとしての *CN-Series*、またはその逆に移行する前に、*plugin-serviceaccount.yaml* を削除して再適用する必要があります。詳細については、「[クラスタ認証用サービスアカウントの作成](#)」を参照してください。

- *CN-Series* を *DaemonSet* として *GKE* にデプロイする場合、*pan-plugin-cluster-mode-secret* が存在してはいけません。
- *CN-Series* を *Kubernetes* サービスとして *GKE* にデプロイする場合、*pan-plugin-cluster-mode-secret* が存在する必要があります。

CN-Series ファイアウォールを Kubernetes サービスとして GKE に デプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Seriesデプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.x以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

以下の手順を実行して、CN-Series ファイアウォールを Kubernetes サービスとして GKE プラットフォームにデプロイします。

STEP 1 | Kubernetes クラスタをセットアップします。

GKEでクラスタを作成するには、次のようにします。

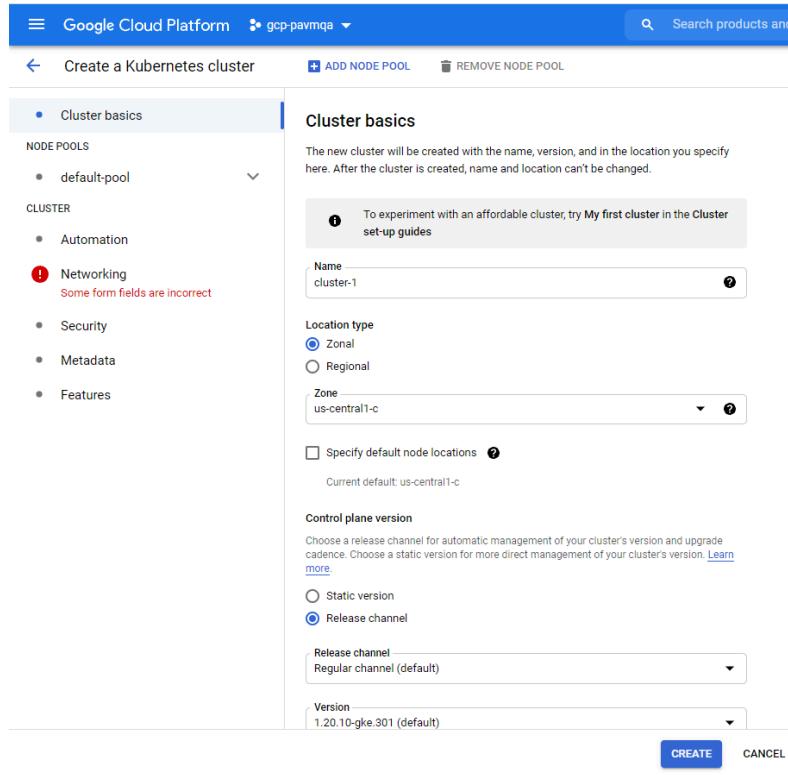
- ナビゲーションメニューをクリックし、**Kubernetes Engine**に移動してから、クラスターを選択します。

Name	Location	Number of nodes	Total vCPUs	Total memory	Notifications	Labels
chandra-gke-cluster	us-central1-c	0	0	0 GB	⚠️ Pods unschedulable	—
cloud-init-soak-cluster1	us-east1-c	0	0	0 GB	⚠️ Pods unschedulable	—
cloud-integration-soak2	us-central1-c	0	0	0 GB	⚠️ Pods unschedulable	—
hs-cnseries-2	us-west2-a	3	24	96 GB	⚠️ Low resource requests	—

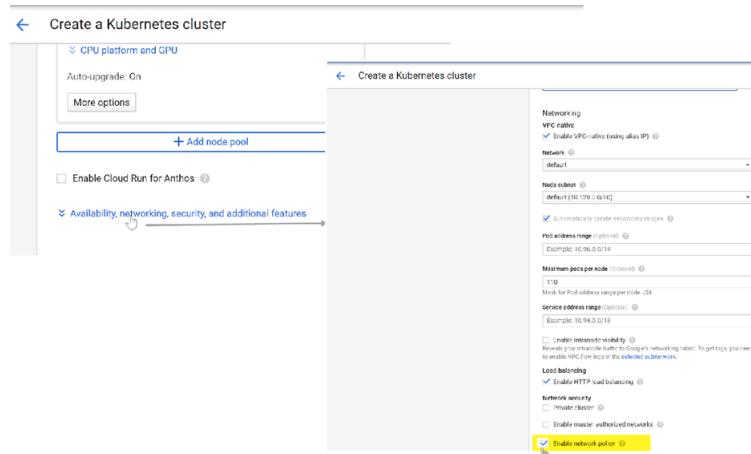
- 作成をクリックします。

- 使用するクラスタモードとして **GKE 標準** を選択し、設定をクリックします。

- 名前、バージョン、場所、ノードサブネットなどのクラスタの基本情報を入力し、作成をクリックします。



クラスタが GKE 上に存在する場合は、*Kubernetes* ネットワーク ポリシー API を有効にして、クラスタ管理者が相互に通信可能なポッドを指定できることを確認してください。この API は、CN-NGFW ポッドと CN-MGMT ポッドが通信するために必要です。



1. クラスタのリソースが適切であることを確認します。デフォルトのGKE ノードプール仕様は、CN-Series ファイアウォールには適していません。クラスタにファイアウォール

ルをサポートするためのCN-Series前提条件リソースがあることを確認する必要があります。

kubectl get nodes

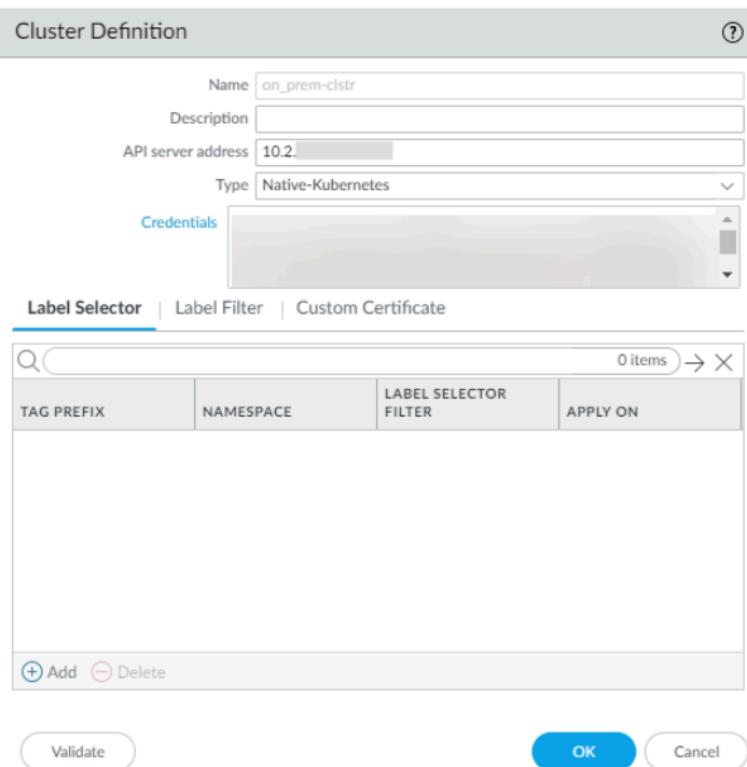
kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能なCPUとメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。CNシリーズのパフォーマンスとスケーリングを参照してください。

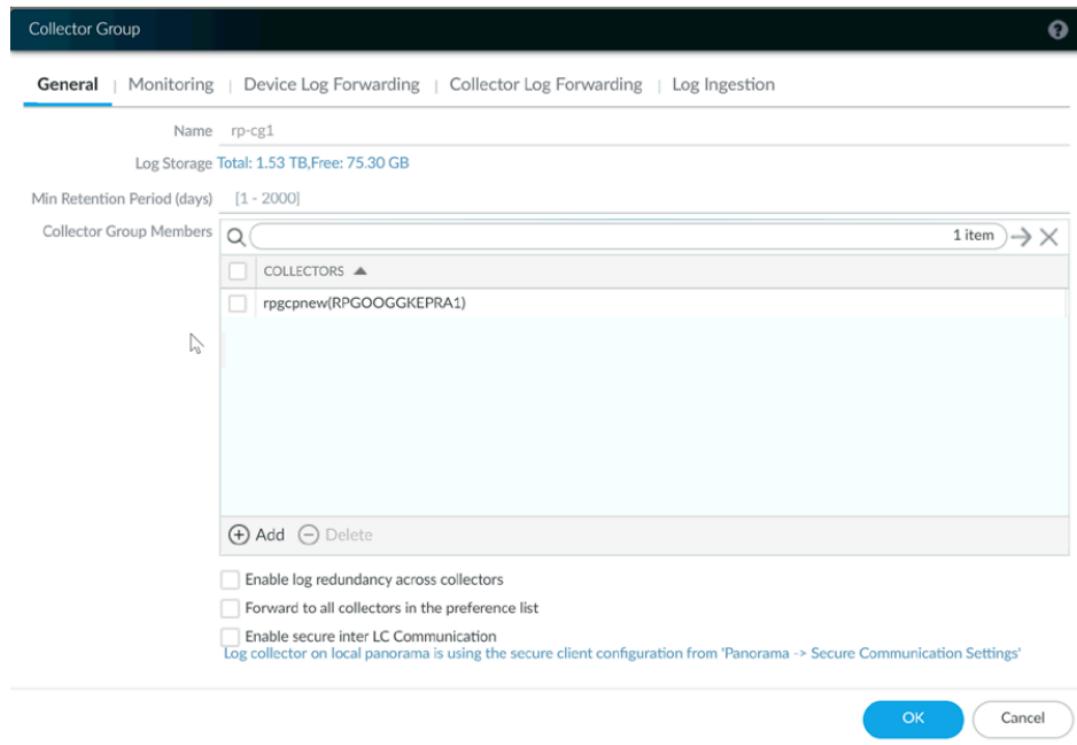
以下の情報があることを確認してください。

- PanoramaにAPIサーバーを設定するためのエンドポイントIPアドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

- テンプレートスタック名、デバイスグループ名、Panorama IP アドレス、およびオプションでログコレクタグループ名をPanorama から収集します。



詳細については、[親デバイスグループとテンプレートスタックの作成](#)を参照してください。

- [認証コードと自動登録の PIN ID と値](#)を収集します。
- イメージをダウンロードしたコンテナイメージリポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

```
kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt
```

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

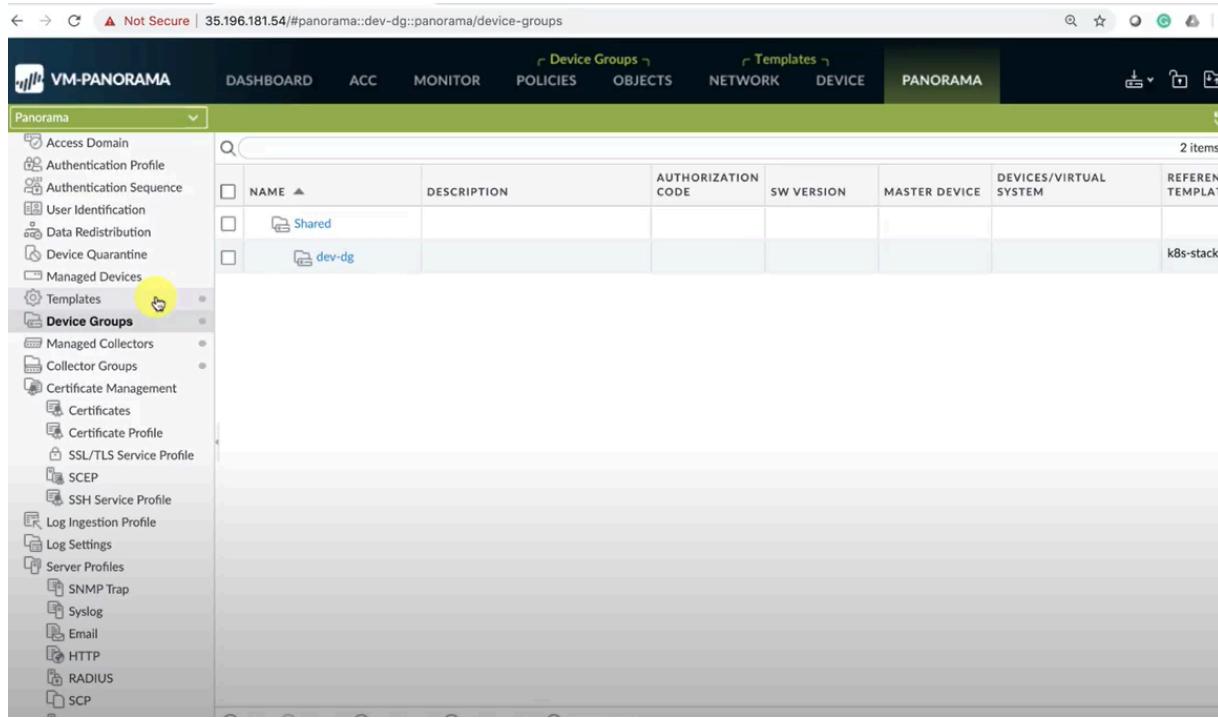
```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-mgmt-config
  namespace: kube-system
data:
  PAN_OPERATION_MODE: "daemonset"
  PAN_SERVICE_NAME: "pan-mgmt"
  # Panorama settings
  PAN_PANORAMA_IP: "35.196.181.54"
  PAN_PANORAMA_AUTH_KEY: [REDACTED]
  PAN_DEVICE_GROUP: "dev-dg"
  PAN_TEMPLATE: "k8s-stack"
  #Non-mandatory parameters
  PAN_PANORAMA_CGNAME: "rp-cg1"
  #PAN_CERTIFICATE: ""
  #PAN_CERTKEYFILE: ""
  #PAN_CERTPASSPHRASE: ""
```

以下の図に示すように、YAML ファイルの PAN_PANORAMA_IP パラメータの値が実際の Panorama IP アドレスと一致していることを確認する必要があります。

NAME	DESCRIPTION	TYPE	STACK	DEVICES	VARIABLES	DEVICE KEY-VALUE TA
K8S-Network-Setup		template			Manage...	
k8s-stack		template-stack	K8S-Network-Setup		Manage...	No Devices in the stack

以下の図に示すように、YAML ファイルの PAN_DEVICE_GROUP と PAN_TEMPLATE のパラメータ値が、Panorama で作成したデバイスグループとテンプレートスタックの名前と一致していることを確認する必要があります。

CN-Series ファイアウォールを GKE にデプロイする



NAME	DESCRIPTION	AUTHORIZATION CODE	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM	REFERENCE
Shared						
dev-dg						k8s-stack

PAN_PANORAMA(CG_NAME) のパラメータ値が、作成したログコレクターネームと同じであることを確認する必要があります。

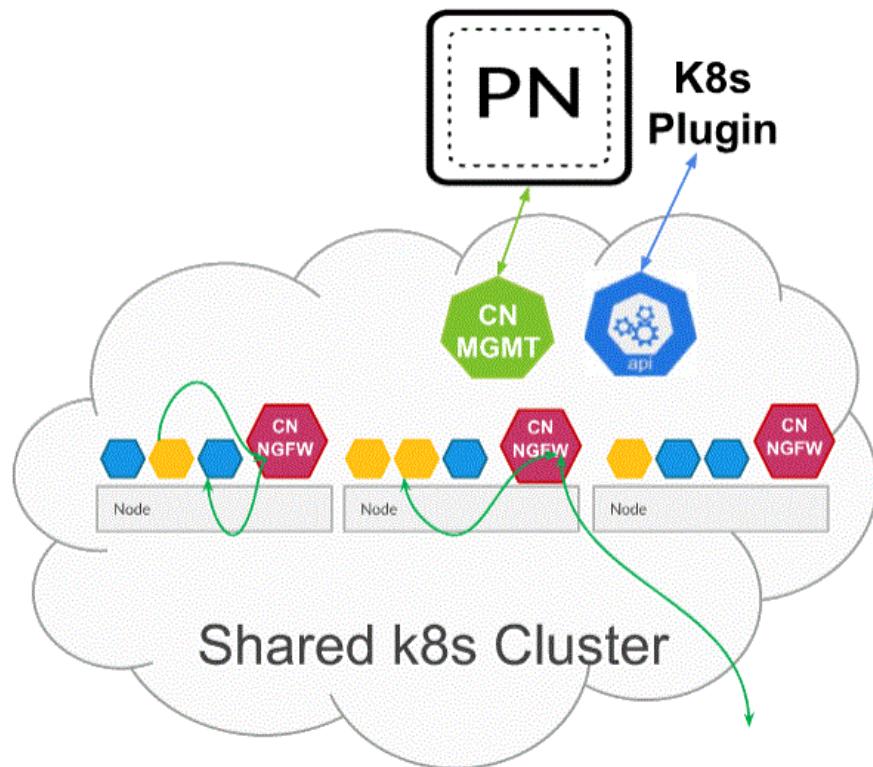


NAME	REDUNDANCY ENABLED	FORWARD TO ALL COLLECTORS	COLLECTORS	LOG REDISTRIBUTION
rp-cg1			demo-panorama	none

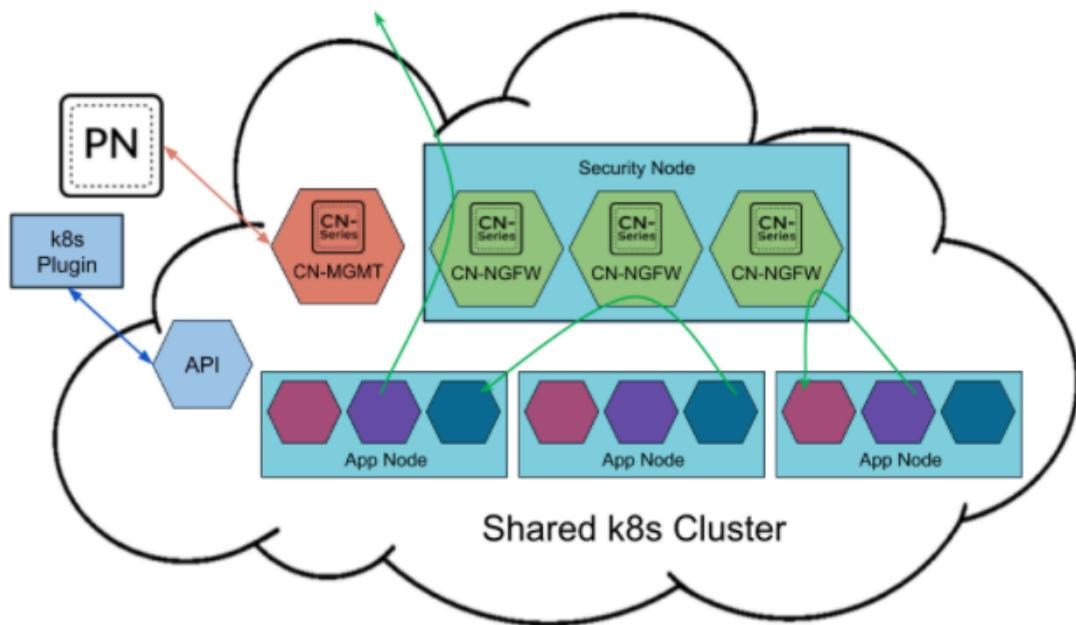
詳細については、[Editable parameters in CN-Series deployment yaml files \(CN-Series デプロイメント yaml ファイルの編集可能なパラメーター\)](#)を参照してください。

STEP 4 | Kubernetes 環境でオートスケーリングを使用している場合は、[Enable Horizontal Pod scaling \(Horizontal Pod のスケーリング\)](#)を参照してください。

STEP 5 | CN-NGFW サービスをデプロイします。次の手順を実行します。



Kubernetesサービスとしてデプロイすると、CN-NGFW のインスタンスをセキュリティノードにデプロイでき、アプリケーションポッドトラフィックは、検査と執行のために利用可能な CN-NGFW インスタンスにリダイレクトされます。



1. `pan-cni-serviceaccount.yaml` を使用してサービス アカウントが作成されたことを確認します。

クラスタ認証用のサービスアカウントの作成を参照してください。

2. Kubectl を使用して pan-cni-configmap.yaml を実行します。

```
kubectl apply -f pan-cni-configmap.yaml
```

3. `kubectl` を使用して `pan-cn-ngfw-svc.yaml` を実行します。

```
kubectl apply -f pan-cn-nqfw-svc.yaml
```



この `yaml` は `pan-cni.yaml` の前にデプロイする必要があります。

4. Kubectl を使用して pan-cni.yaml を実行します。

```
kubectl apply -f pan-cni.yaml
```

5. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。
 6. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
[root@cloudshell-192-168-1-10 ~]# gcloud container clusters get-credentials k8s-test-cluster --region=us-central1 --project=pan-cn-k8s-service
```

```
pan-chi-imqxi Running 0 2m11s
pan-chi-wjrkq Running 0 2m11s
pan-chi-xrc2z Running 0 2m12s
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v1.18.10-crio-4.10.2-0-gf333333-series-mktplace)$
```

STEP 6 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. (静的にプロビジョニングされた PV のみに必要) CN-MGMT StatefulSet 用の永続ボリューム (PV) をデプロイします。

1. `pan-cn-pv-local.yaml` で定義されたローカル ボリューム名と一致するディレクトリを作成します。

少なくとも 2 つのワーカー ノード上に 6 つのディレクトリが必要です。CN-MGMT StatefulSet をデプロイする各ワーカー ノードにログインして、ディレクトリを作成

します。たとえば、/mnt/pan-local1 から /mnt/pan-local6 という名前のディレクトリを作成するには、次のコマンドを使用します。

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /  
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. pan-cn-pv-local.yaml を変更します。

`nodeaffinity` の下でホスト名を一致させ、上記で `spec.local.path` に作成したディレクトリが変更されたことを確認してから、そのファイルをデプロイして、新しいストレージクラス `pan-local-storage` とローカル PV を作成します。

2. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

EKS から pan-cn-mgmt-configmap をサンプリングします。

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-  
config namespace: kube-system data:PAN_SERVICE_NAME: pan-  
mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama 設  
定 PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:  
"<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-  
template-stack>" PAN_CNAME: "<panorama-collector-  
group>" # ctnr mode: "k8s-service", "k8s-ilbservice"  
PAN_CTNR_MODE_TYPE: "k8s-service" #必須でないパラメータ #  
Panorama Kubernetes プラグインで提供されるクラスタ名と同じ名前  
を持つことを推奨 - 同じ Panorama で複数のクラスタを管理する場合、  
ポッドの識別が容易になります #CLUSTER_NAME: "<Cluster name>"  
#PAN_PANORAMA_IP2: "" # CERT を使用する場合はコメントアウト  
します。それ以外の場合は、pan-mgmt と pan-ngfw 間の IPsec 用に  
PSK を使用します #IPSEC_CERT_BYPASS: "" # 値は不要 # jumbo-  
frame モードの自動検出をオーバーライドし、システム全体を強制的に有  
効にします #PAN_JUMBO_FRAME_ENABLED: "true" # GTP を有効にし  
て MGMT を起動します。完全な機能を実現するには、Panorama でも GTP  
# を有効にする必要があります。#PAN_GTP_ENABLED: "true" # 高い  
機能容量を有効にします。これらは MGMT ポッドには高いメモリを必要と  
し、NGFW ポッドには以下の指定以上のメモリが必要です。#PAN_NGFW_MEMORY =  
"6Gi" #PAN_NGFW_MEMORY = "40Gi" # より高速なデータパス-AF_XDP を有  
効にするには、デフォルトは AF_PACKETV2 です。これにはカーネルのサポート  
が必要です。#PAN_DATA_MODE: "次世代" #HPA params #PAN_CLOUD: "EKS"  
#PAN_NAMESPACE_EKS: "EKSNamespace" #PUSH_INTERVAL: "15" #AWS  
cloudwatch にメトリクスを発行する間隔
```

pan-cn-mgmt.yaml のサンプル

```
initContainers: - name: pan-mgmt-init image: <your-private-  
registry-image-path>
```

```
containers: - name: pan-mgmt image: <your-private-registry-  
image-path> terminationMessagePolicy:FallbackToLogsOnError
```

3. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml  
kubectl apply -f pan-cn-mgmt-slot-crd.yaml  
kubectl apply -f pan-cn-mgmt-slot-cr.yaml  
kubectl apply -f pan-cn-mgmt-secret.yaml  
kubectl apply -f pan-cn-mgmt.yaml
```

pan-mgmt-serviceaccount.yaml は、[クラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

4. 次のコマンドを実行して、CN-MGMT ポッドが起動していることを確認します。

```
kubectl get pods -l app = pan-mgmt -n kube-system
```

これには、5 ~ 6 分かかります。

STEP 7 | CN-NGFW ポッドをデプロイします。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-  
registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. CN-NGFW ポッドがデプロイされたことを確認します。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
```

STEP 8 | 次の手順を実行して、Horizontal podのオートスケーリングを有効にします。

1. CN-Series クラスターに [カスタム メトリックスタック ドライバーアダプター](#)をデプロイします。クラスター名は K8s シークレットを通じて指定する必要があります。
2. GKE 固有の HPA yaml ファイルを [Palo Alto Networks GitHub リポジトリ](#)からダウンロードします。
3. CN-MGMT がカスタム名前空間にデプロイされている場合は、カスタム名前空間を使用して pan-cn-adapater.yaml を更新します。デフォルトの名前空間は **kube-system** です。
4. GKE-specificの pan-cn-mgmt-configmap.yaml で HPA パラメータを更新します。

```
#PAN_CLOUD:"GKE"
```

```
#HPA_NAME: 「<name>」 #ネームスペースごと、またはテナントごとに hpa リソースを識別するための固有名称
```

```
#PUSH_INTERVAL: 「15」 #Stackdriver にメトリクスを発行するための時間間隔
```

5. 上記の pan-cn-mgmt-configmap.yaml ファイルで更新された HPA_NAMEで **pan-cn-hpa-dp.yaml** と **pan-cn-hpa-mp.yaml** を変更し (nameに置き換え)、トリガーする HPA に基づいてメトリックを更新します。
 1. レプリカの最小数と最大数を入力します。
 2. (任意) スケールダウンを変更し、デプロイメントに合わせて頻度値をスケールアップします。これらの値を変更しない場合は、デフォルト値が使用されます。
 3. (任意) スケーリングに使用する各メトリックのしきい値を変更します。これらの値を変更しない場合は、デフォルト値が使用されます。
 4. 変更を保存します。
6. HPA yaml ファイルをデプロイします。ファイルは、以下に説明する順序でデプロイする必要があります。
 1. Kubectl を使用して pan-cn-adapter.yaml を実行します
kubectl apply -f pan-cn-adapter.yaml
 2. Kubectl を使用して pan-cn-crole.yaml を実行します
kubectl apply -f pan-cn-crole.yaml
 3. Kubectl を使用して pan-cn-hpa-dp.yaml を実行します
kubectl apply -f pan-cn-hpa-dp.yaml
 4. Kubectl を使用して pan-cn-hpa-mp.yaml を実行します
kubectl apply -f pan-cn-hpa-mp.yaml
7. デプロイメントを確認します。

- kubectl を使用して、カスタム メトリックス名前空間内のカスタム メトリック アダプター ポッドを確認します。

kubectl get pods -n custom-metrics

- kubectl を使用して、HPA リソースを確認します。

kubectl get hpa -n kube-system

kubectl describe hpa <hpa-name> -n kube-system

詳細については、「[Enable Horizontal Pod Autoscaling on the CN-Series \(CN-Seriesでの水平ポッド自動スケーリングの有効化\)](#)」を参照してください。

STEP 9 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

kubectl -n kube-system get pods

STEP 10 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

annotations : paloaltonetworks.com/firewall : pan-fw

たとえば、「default」名前空間のすべての新しいポッドの場合：

kubectl annotate namespace default paloaltonetworks.com/firewall=pan-fw



一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

volumes: - name: pan-cni-ready hostPath: path: /var/log/pan-appinfo/pan-cni-ready type: ディレクトリ

STEP 11 | クラスタでアプリケーションをデプロイします。

CN-Series ファイアウォールを GKE に DaemonSet としてデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Seriesデプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.x以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォールを GKE プラットフォームに Daemonset としてデプロイするには、次の手順を実行します。

STEP 1 | Kubernetes クラスタをセットアップします。

GKEでクラスタを作成するには、次のようにします。

- ナビゲーションメニューをクリックし、**Kubernetes Engine**に移動してから、クラスターを選択します。

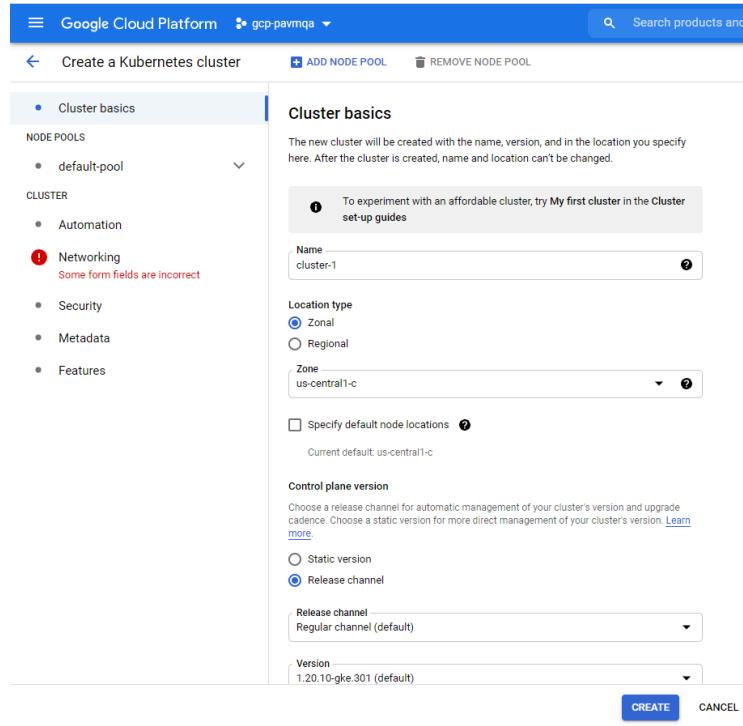
Name	Location	Number of nodes	Total vCPUs	Total memory	Notifications	Labels
chandra-gke-cluster	us-central1-c	0	0	0 GB	⚠️ Pods unschedulable	—
cloud-init-soak-cluster1	us-east1-c	0	0	0 GB	⚠️ Pods unschedulable	—
cloud-integration-soak2	us-central1-c	0	0	0 GB	⚠️ Pods unschedulable	—
hs-cnseries-2	us-west2-a	3	24	96 GB	⚠️ Low resource requests	—

- 作成をクリックします。

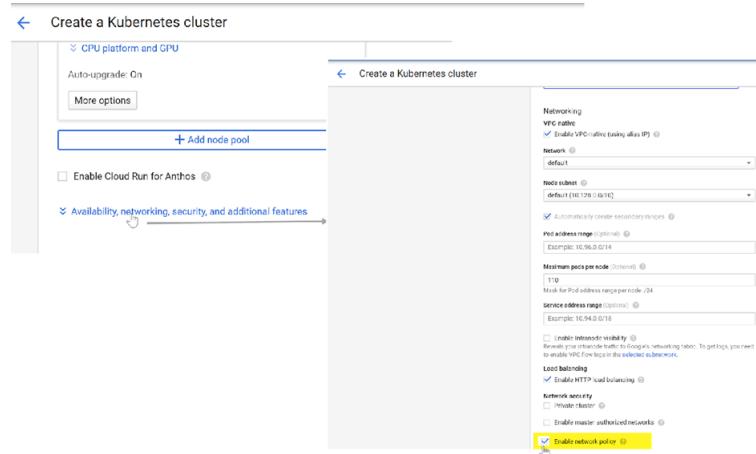
- 使用するクラスタモードとして **GKE 標準** を選択し、設定をクリックします。

- 名前、バージョン、場所、ノードサブネットなどのクラスタの基本情報を入力し、作成をクリックします。

CN-Series ファイアウォールを GKE にデプロイする



 クラスタが GKE 上に存在する場合は、*Kubernetes* ネットワーク ポリシー API を有効にして、クラスタ管理者が相互に通信可能なポッドを指定できることを確認してください。この API は、CN-NGFW ポッドと CN-MGMT ポッドが通信するために必要です。



クラスタのリソースが適切であることを確認します。クラスタがファイアウォールをサポートするための [CN-Series システム要件](#)を持っていますことを確認します。

kubectl get nodes

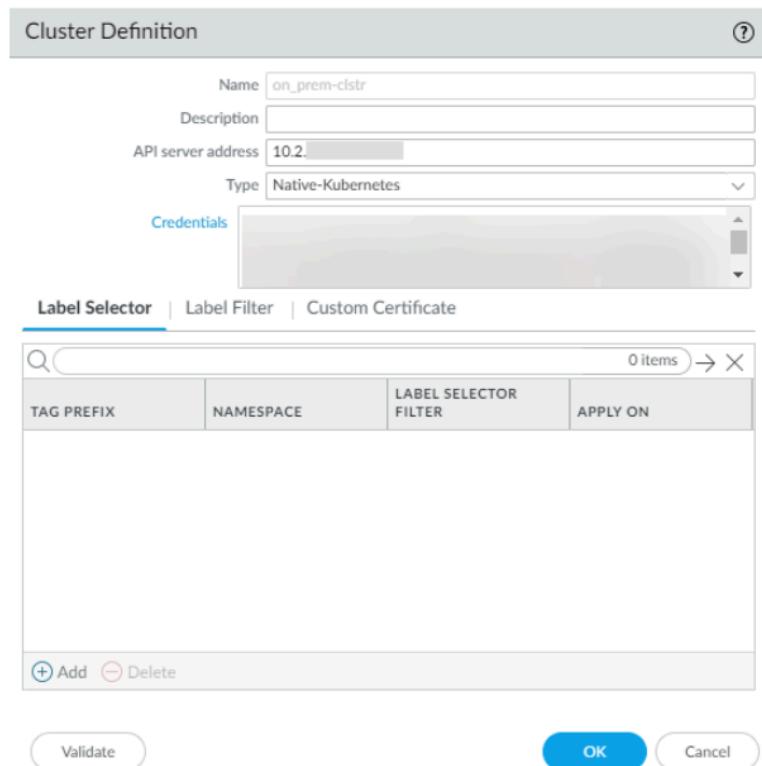
kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能な CPU とメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。 「[CN シリーズのパフォーマンスとスケーラビリティ](#)」を参照してください。

以下の情報があることを確認してください。

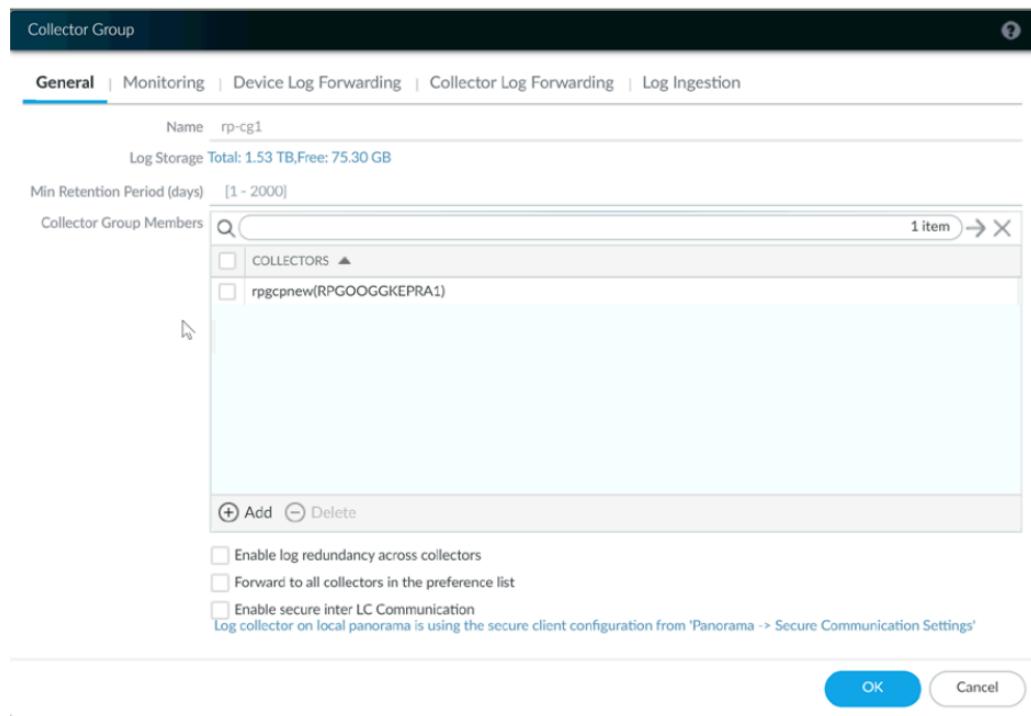
- Panorama 上で API サーバーをセットアップするためのエンドポイント IP アドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

詳細については、[クラスタをモニタリングするための Kubernetes プラグインの設定](#)をご覧ください。

- テンプレート スタック名、デバイス グループ名、Panorama IP アドレス、およびオプションで Panorama からログコレクタ グループ名を収集します。



詳細については、[親デバイス グループとテンプレート スタックの作成](#)を参照してください。

- [認証コード](#)と[自動登録の PIN ID](#)と値を収集します。
- イメージをダウンロードしたコンテナイメージリポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

非公開の Google Container レジストリへのパスを含め、必要なパラメータを提供するには、YAML ファイル内のイメージパスを置き換える必要があります。詳細は、「[CN-Series 配置の yaml ファイルで編集可能なパラメータ](#)」を参照してください。

STEP 4 | CNI DaemonSet をデプロイします。

CNI コンテナは、DaemonSet(ノードあたり 1 つのポッド)としてデプロイされ、ノード上にデプロイされたアプリケーションごとに 2 つずつのインターフェースを CN-NGFW ポッド上

を作成します。kubectl コマンドを使用して pan-cni YAML ファイルを実行すると、それが各ノード上のサービス チェーンに組み込まれます。

1. CN-Series ファイアウォールには、Kubernetes クラスタリソースと通信することを許可する最小権限を備えた 3 つのサービス アカウントが必要です。CN シリーズ クラスタ認証用サービスアカウントを作成し、pan-cni-serviceaccount.yaml を使用してサービスアカウントを作成したことを確認する必要があります。
2. Kubectl を使用して pan-cni-configmap.yaml を実行します。
kubectl apply -f pan-cni-configmap.yaml
3. Kubectl を使用して pan-cni.yaml を実行します。
kubectl apply -f pan-cni.yaml
4. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。
5. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v...@series-mktplace)$ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkf
pan-cni-wjrkq
pan-cni-xrc22
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v...@series-mktplace)$
```

STEP 5 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1 つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

pan-cn-mgmt-configmap のサンプル

```
name: pan-mgmt-config

metadata:

namespace: kube-system

data:

PAN_SERVICE_NAME: pan-mgmt-svc

PAN_MGMT_SECRET: pan-mgmt-secret

# Panorama の設定

PAN_PANORAMA_IP: "x.y.z.a"

PAN_DEVICE_GROUP: "dg-1"

PAN_TEMPLATE_STACK: "temp-stack-1"

PAN_CGNAME: "CG-GKE"

必須ではないパラメータ

#Panorama Kubernetes プラグインで提供されるクラスタ名と同じ名前にするこ
とを推奨。同じ Panorama で複数のクラスタを管理する場合、ポッドの識別が容
易になります

#CLUSTER_NAME: "<Cluster name>"

#PAN_PANORAMA_IP2: ""

#Pan-mgmt と pan-ngfw の間で IPSec の PSK を使用しない場合
は、CERT を使用するようにコメントアウトします

#IPSEC_CERT_BYPASS: ""

#値は不要です

#ジャンボフレームモードの自動検出をオーバーライドし、システム全体で強制的に
有効化#PAN_JUMBO_FRAME_ENABLED: "true"

#GTPを有効にして MGMT ポッドを開始します。完全な機能を得るに
は、Panorama でも GTP の有効化が必要
#PAN_GTP_ENABLED: "true"
```

pan-cn-mgmt.yaml のサンプル

```
initContainers:  
  
  - name: pan-mgmt-init  
  
    image: <your-private-registry-image-path>  
  
  containers: - name: pan-mgmt  
  
    image: <your-private-registry-image-path>  
  
    terminationMessagePolicy: FallbackToLogsOnError
```

2. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml  
kubectl apply -f pan-cn-mgmt-secret.yaml  
kubectl apply -f pan-cn-mgmt.yaml
```

pan-mgmt-serviceaccount.yamlは、[クラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

3. CN-MGMT ポッドが起動していることを確認します。

これには、5～6 分かかります。

```
kubectl get pods -l app=pan-mgmt -n kube-system を使用します。
```

```
NAME READY STATUS RESTARTS AGE  
pan-mgmt-sts-0 1/1 27h  
pan-mgmt-sts-1 1/1 Running 0 27h
```

STEP 6 | CN-NGFW ポッドをデプロイします。

デフォルトで、ファイアウォールデータプレーン CN-NGFW ポッドは DaemonSet としてデプロイされます。CN-NGFW ポッドのインスタンスは、1 つのノード上で最大 30 個のアプリケーション ポッドのトラフィックを保護することができます。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. すべての CN-NGFW ポッド (クラスタ内のノードあたり 1 つずつ) が実行していることを確認します。

これは、4 ノード オンプレミス クラスタからの出力例です。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES
pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>
pan-ngfw-ds-qsrn6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>
pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
```

STEP 7 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 Running
0 27hpan-cni-9j4rs 1/1 Running
0 27hpan-cni-ddwb4 1/1 Running
0 27hpan-cni-fwfrk 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-j62rk 1/1 Running
0 27hpan-cni-lmxdz 1/1 Running
0 27hpan-mgmt-sts-0 1/1 Running
0 27hpan-mgmt-sts-1 1/1 Running
0 27hpan-ngfw-ds-8g5xb 1/1 Running
27hpan-ngfw-ds-qsrn6 1/1 Running
0 27hpan-ngfw-ds-vqk7z 1/1 Running
0 27hpan-ngfw-ds-zncqg 1/1 Running
```

STEP 8 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```



一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

```
volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: ディレクトリ
```

STEP 9 | クラスタでアプリケーションをデプロイします。

CN-Series ファイアウォールを OKE にデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> • CN-Series デプロイメント 	<ul style="list-style-type: none"> • CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x 以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

Oracle Kubernetes Engine (OKE) は、kubernetes クラスタをデプロイできる OCI サービスです。CN-Series ファイアウォールを Daemonset または Kubernetes サービスとして OKE クラスタにデプロイできるようになりました。

CNシリーズ ビルドイング ブロックと CNシリーズ ファイアウォールによる Kubernetes の安全な環境内のワークフローの概要を確認したら、同じクラスタ内のコンテナ間やコンテナと他のワークロード タイプ(仮想マシンやベアメタル サーバーなど)間のトラフィックを保護するための OKE プラットフォームにおける CN-Series ファイアウォールのデプロイから始めることができます。



Kubernetes クラスタ、アプリケーション、およびファイアウォール サービスをデプロイして管理するためには、*kubectl* や *Helm* などの標準の *Kubernetes* ツールが必要です。

詳細については、「*Helm* チャートとテンプレートを使用した CN-Series ファイアウォールのデプロイ」を参照してください。*Panorama* は、*Kubernetes* クラスタのデプロイメントと管理用のオーケストレーターになるようには設計されていません。クラスタ管理用のテンプレートがマネージド *Kubernetes* プロバイダから提供されています。*Palo Alto Networks* は、*Helm* および *Terraform* で CN-Series をデプロイするためのコミュニティサポートのテンプレートを提供しています。

- CN-Series ファイアウォールを OKE に Kubernetes サービスとしてデプロイする
- CN-Series ファイアウォールを OKE に DaemonSet としてデプロイする



CN-Series を *DaemonSet* としての *CN-Series* からサービスとしての *CN-Series*、またはその逆に移行する前に、*plugin-serviceaccount.yaml* を削除して再適用する必要があります。詳細については、「[クラスタ認証用サービスアカウントの作成](#)」を参照してください。

- *CN-Series* を *DaemonSet* として *OKE* にデプロイする場合、*pan-plugin-cluster-mode-secret* が存在してはいけません。
- *CN-Series* を *Kubernetes* サービスとして *OKE* にデプロイする場合、*pan-plugin-cluster-mode-secret* が存在する必要があります。

CN-Series ファイアウォールを OKE に Kubernetes サービスとしてデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Series デプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

以下の手順を実行して、CN-Series ファイアウォールを OKE プラットフォームに Kubernetes サービスとしてデプロイします。



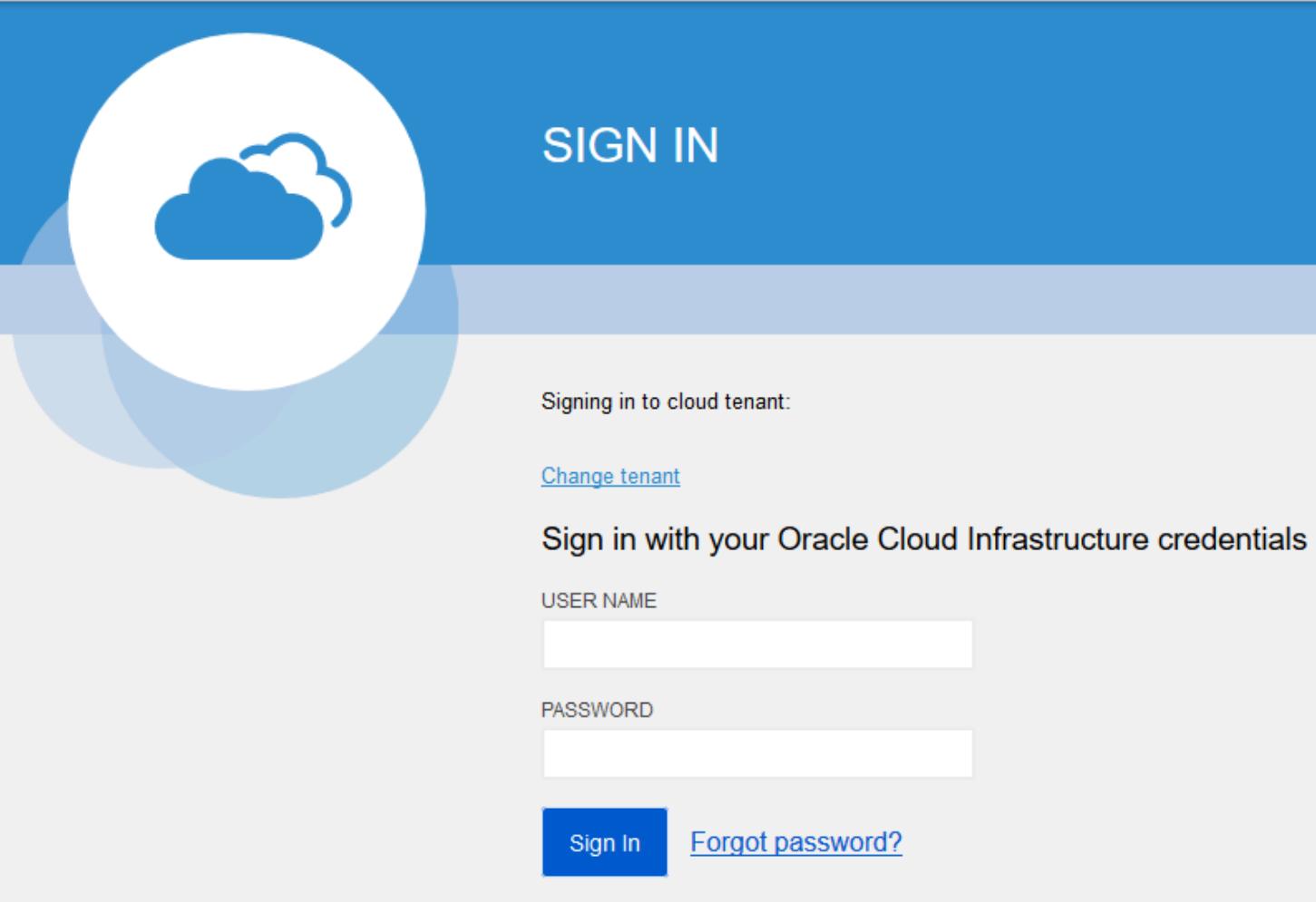
*Oracle Linux 8.5 OS*は、OKE に CN-Series ファイアウォールをデプロイするための唯一認定された環境です。

STEP 1 | Kubernetes クラスタをセットアップします。

OKE でクラスタを作成するには、次のように実施します。

1. Oracle Cloud Infrastructure にログインします。

ACLE® Cloud Infrastructure



2. ナビゲーションメニューをクリックし、**Under Solutions and Platform**に移動して、**Developer Services**をクリックします。
3. **Kubernetes Clusters**をクリックします。
4. コンパートメントを選択し、クラスタの作成をクリックします。

Clusters in Tutorial2 Compartment

Clusters Requirements: [Preparing for Container Engine for Kubernetes](#)
[Show more information](#)

Create Cluster

Name	Status	Node Pools	VCN	Version	Created
No clusters exist. Create one to get started.					

5. [クラスタを作成] ダイアログ ボックスにて、カスタム作成をクリックし、ワークフローを起動をクリックします。
6. **Create Cluster**ページで、クラスタ名とその他の詳細を入力します。
7. 次へをクリックして、新しいクラスタについて入力した詳細を確認します。
8. 確認ページで、**Create Cluster**をクリックします。

Cluster Creation

[Create Cluster](#)

NEW

Resources to be created

Basic Information

Cluster Name: cluster1**Compartment:** Tutorial2**Version:** v1.18.10

Network

Compartment: Tutorial2**VCN Name:** oke-vcn-quick-cluster1-4baf5729a**Network Security Groups:** Not Enabled**Kubernetes API Private Endpoint:** Auto Assigned
Kubernetes API Public Endpoint: Auto Assigned**Kubernetes CIDR Block:** 10.96.0.0/16[Create Cluster](#)[Cancel](#)

1. クラスタにファイアウォールをサポートするためのCN-Series前提条件リソースがあることを確認する必要があります。

```
kubectl get nodes
```

```
kubectl describe node <node-name>
```

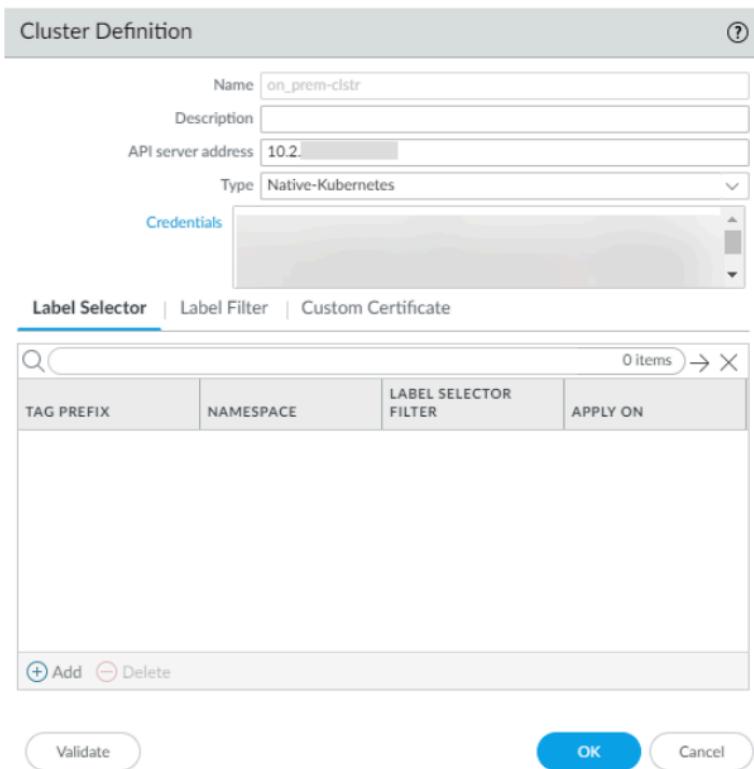
コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能なCPUとメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。CNシリーズのパフォーマンスとスケーリングを参照してください。

以下の情報があることを確認してください。

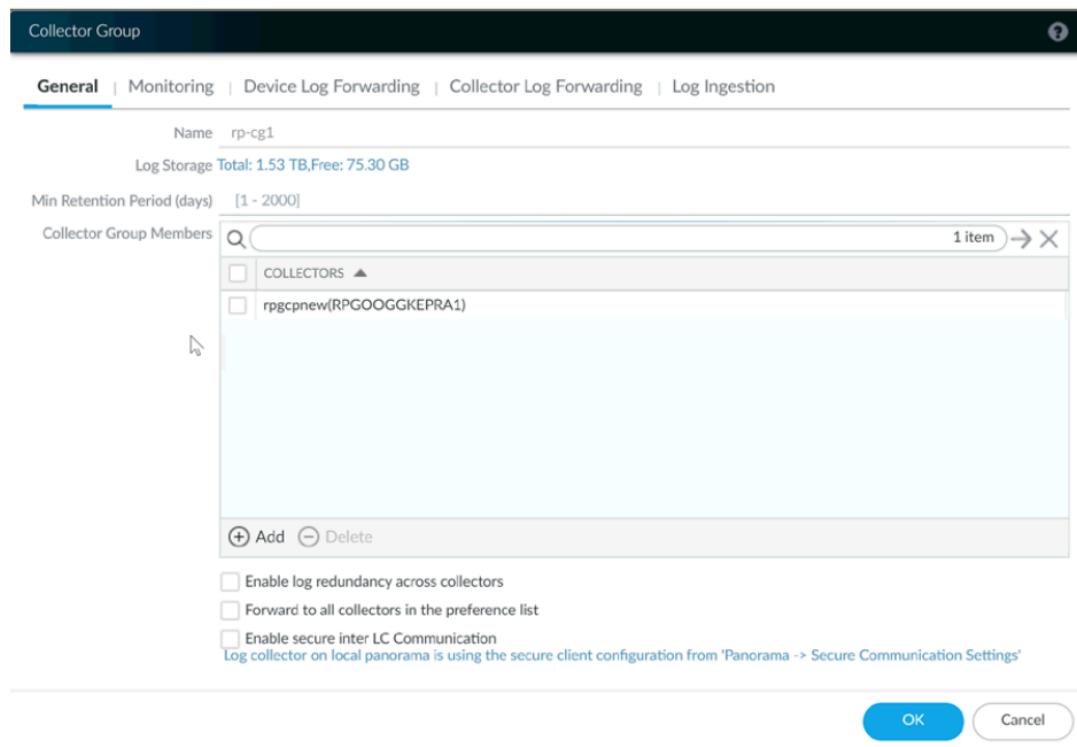
CN-Series ファイアウォールを OKE にデプロイする

- PanoramaにAPI サーバーを設定するためのエンドポイント IP アドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

- テンプレートスタック名、デバイス グループ名、Panorama IP アドレス、およびオプションでログコレクタグループ名をPanorama から収集します。



詳細については、[親デバイスグループとテンプレートスタックの作成](#)を参照してください。

- [認証コードと自動登録の PIN ID と値](#)を収集します。
- イメージをダウンロードしたコンテナイメージリポジトリの場所を用意します。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt-dynamic-pv.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

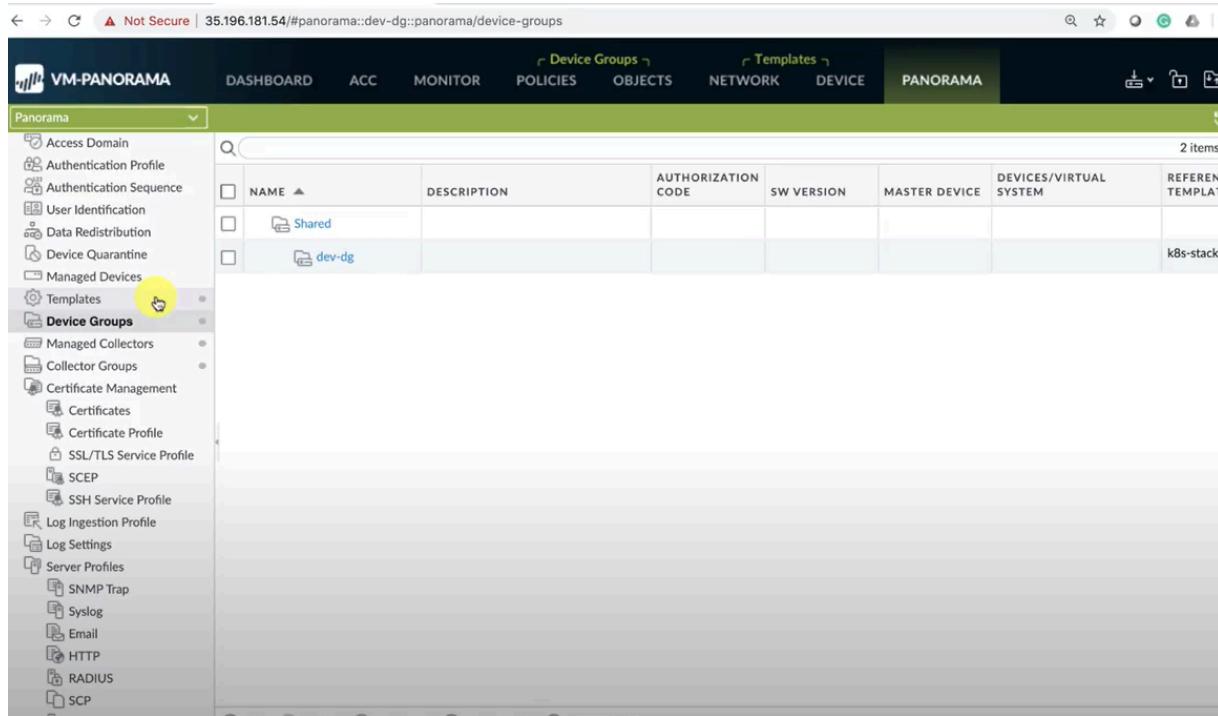
```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-mgmt-config
  namespace: kube-system
data:
  PAN_OPERATION_MODE: "daemonset"
  PAN_SERVICE_NAME: "pan-mgmt"
  # Panorama settings
  PAN_PANORAMA_IP: "35.196.181.54"
  PAN_PANORAMA_AUTH_KEY: [REDACTED]
  PAN_DEVICE_GROUP: "dev-dg"
  PAN_TEMPLATE: "k8s-stack"
#Non-mandatory parameters
  PAN_PANORAMA_CGNAME: "rp-cg1"
  #PAN_CERTIFICATE: ""
  #PAN_CERTKEYFILE: ""
  #PAN_CERTPASSPHRASE: ""
```

以下の図に示すように、YAML ファイルの PAN_PANORAMA_IP パラメータの値が実際の Panorama IP アドレスと一致していることを確認する必要があります。

NAME	DESCRIPTION	TYPE	STACK	DEVICES	VARIABLES	DEVICE KEY-VALUE TA
K8S-Network-Setup		template			Manage...	
k8s-stack		template-stack	K8S-Network-Setup		Manage...	No Devices in the stack

以下の図に示すように、YAML ファイルの PAN_DEVICE_GROUP と PAN_TEMPLATE のパラメータ値が、Panorama で作成したデバイスグループとテンプレートスタックの名前と一致していることを確認する必要があります。

CN-Series ファイアウォールを OKE にデプロイする



NAME	DESCRIPTION	AUTHORIZATION CODE	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM	REFERENCE
Shared						
dev-dg						k8s-stack

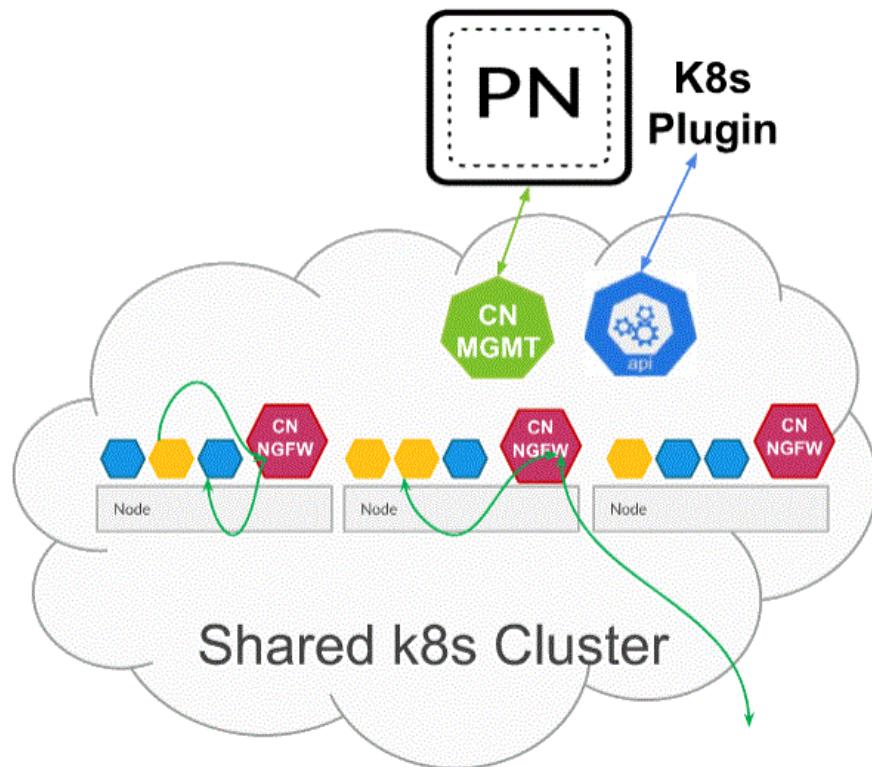
PAN_PANORAMA(CG_NAME) のパラメータ値が、作成したログコレクターネームと同じであることを確認する必要があります。



NAME	REDUNDANCY ENABLED	FORWARD TO ALL COLLECTORS	COLLECTORS	LOG REDISTRIBUTION
rp-cg1	<input type="checkbox"/>	<input type="checkbox"/>	demo-panorama	none

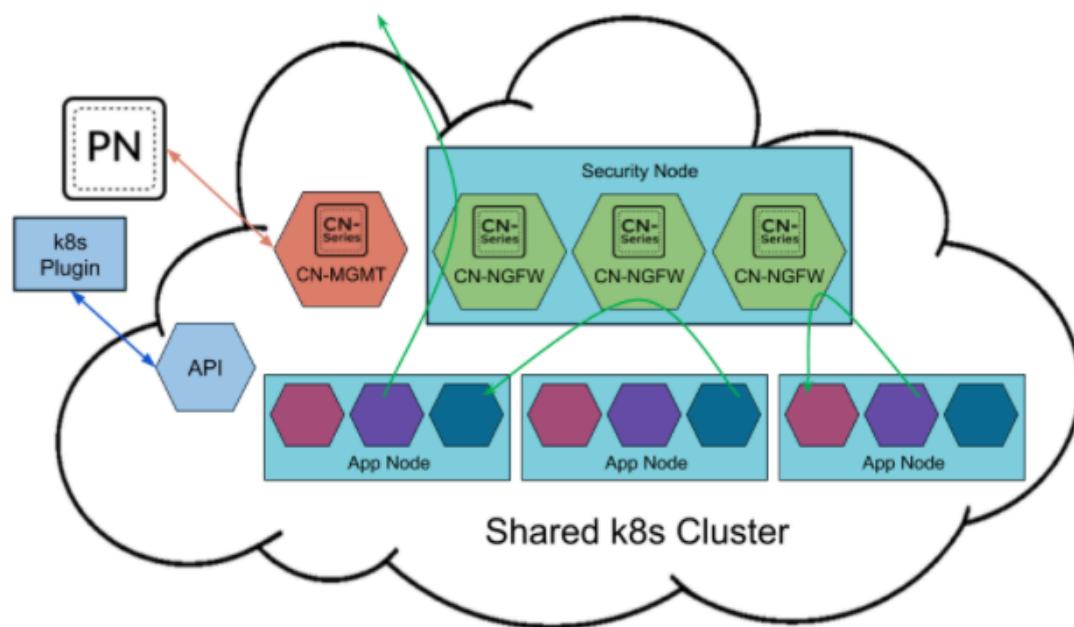
詳細については、[Editable parameters in CN-Series deployment yaml files \(CN-Series デプロイメント yaml ファイルの編集可能なパラメーター\)](#)を参照してください。

STEP 4 | CN-NGFW サービスをデプロイします。次の手順を実行します。



Kubernetes サービスとしてデプロイすると、CN-NGFW のインスタンスをセキュリティノードにデプロイでき、アプリケーションポッドトラフィックは、検査と適用のために利用可能な CN-NGFW インスタンスにリダイレクトされます。

-  *CN-Series ファイアウォールを Kubernetes サービスとして OKE にデプロイする場合、pan-cn-k8s-service ネイティブフォルダーの yaml ファイルを使用できます。*



1. `pan-cni-serviceaccount.yaml` を使用してサービス アカウントが作成されたことを確認します。

[クラスタ認証用のサービス アカウントの作成](#)を参照してください。

2. Kubectl を使用して `pan-cni-configmap.yaml` を実行します。

`kubectl apply -f pan-cni-configmap.yaml`

3. `kubectl` を使用して `pan-cn-ngfw-svc.yaml` を実行します。

`kubectl apply -f pan-cn-ngfw-svc.yaml`



この `yaml` は `pan-cni.yaml` の前にデプロイする必要があります。

4. Kubectl を使用して `pan-cni.yaml` を実行します。

`kubectl apply -f pan-cni.yaml`

5. `pan-cni-configmap` YAML ファイルと `pan-cni` YAML ファイルが変更されたことを確認します。

6. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
@cloudshell:~/Kubernetes-master/pan-cni-k8s-service/gke (v1.22.11-20240111T1445Z-001) $ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkf
pan-cni-wjrkq
pan-cni-xrc22
@cloudshell:~/Kubernetes-master/pan-cni-k8s-service/gke (v1.22.11-20240111T1445Z-001) $ kubectl get pods -n kube-system | grep pan-cni
  Running  0          2m11s
  Running  0          2m11s
  Running  0          2m12s
@cloudshell:~/Kubernetes-master/pan-cni-k8s-service/gke (v1.22.11-20240111T1445Z-001) $
```

STEP 5 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

OKE から pan-cn-mgmt-configmap をサンプリングします。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-mgmt-config
  namespace: kube-system
data:
  PAN_SERVICE_NAME: pan-mgmt-svc
  PAN_MGMT_SECRET: pan-mgmt-secret # パノラマ設定
  PAN_PANORAMA_IP: "<panorama-IP>" # PAN_DEVICE_GROUP: "<panorama-device-group>" # PAN_TEMPLATE_STACK: "<panorama-template-stack>" # PAN_CNAME: "<panorama-collector-group>" # PAN_CTNR_MODE_TYPE: "k8s-service" # 必須ではないパラメーター # Panorama Kubernetes プラグインで提供されるクラスター名と同じ名前にすることをお勧めします - 同じ Panorama で複数のクラスターを管理する場合、ポッドを簡単に識別できます
  #CLUSTER_NAME: "<Cluster name>" # PAN_PANORAMA_IP2: "" # CERT を使用する場合はコメント アウトします。それ以外の場合は、pan-mgmt と pan-ngfw の間で IPSec の PSK を使用します
  #IPSEC_CERT_BYPASS: "" # 値は必要ありません # ジャンボ フレーム モードの自動検出をオーバーライドし、システム全体で強制的に有効にします #
  PAN_JUMBO_FRAME_ENABLED: "true" # GTP を有効にして MGMT ポッドを開始します。完全な機能を実現するには、Panorama でも GTP # を有効にする必要があります。#PAN_GTP_ENABLED: 「true」 # 高い機能容量を有効にします。これらには、MGMT ポッド用に大量のメモリが必要であり、NGFW ポッド用に以下で指定されている # 以上のメモリが必要です。 # システム要件のドキュメントを参照して、各メモリ プロファイルでサポートされている # サポートされている NGFW CPU の最大サイズを確認してください。 #PAN_NGFW_MEMORY: "6.5Gi" #PAN_NGFW_MEMORY: "48Gi" #PAN_NGFW_MEMORY: "56Gi"
```

pan-cn-mgmt-dynamic-pv.yaml のサンプル

```
initContainers:
- name: pan-mgmt-init
  image: <your-private-registry-image-path>
  command: ["/usr/bin/pan_start.sh"]
  imagePullPolicy: Always
```

```
containers:
- name: pan-mgmt
  image: <your-private-registry-image-path>
  terminationMessagePolicy: FallbackToLogsOnError
```

2. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml  
kubectl apply -f pan-cn-mgmt-slot-crd.yaml  
kubectl apply -f pan-cn-mgmt-slot-cr.yaml  
kubectl apply -f pan-cn-mgmt-secret.yaml  
kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml
```

pan-mgmt-serviceaccount.yaml は、[クラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

3. 次のコマンドを実行して、CN-MGMT ポッドが起動していることを確認します。

```
kubectl get pods -l app = pan-mgmt -n kube-system
```

これには、5 ~ 6 分かかります。

STEP 6 | CN-NGFW ポッドをデプロイします。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. CN-NGFW ポッドがデプロイされたことを確認します。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
```

STEP 7 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
```

STEP 8 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

 一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

```
volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: ディレクトリ
```

STEP 9 | クラスタでアプリケーションをデプロイします。

CN-Series ファイアウォールを OKE に DaemonSet としてデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Series デプロイメント	<ul style="list-style-type: none">• CN-Series 10.2.x or above Container Images• PanoramaPAN-OS 10.2.x 以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォールを OKE プラットフォームに Daemonset としてデプロイするには、次の手順を実行します。



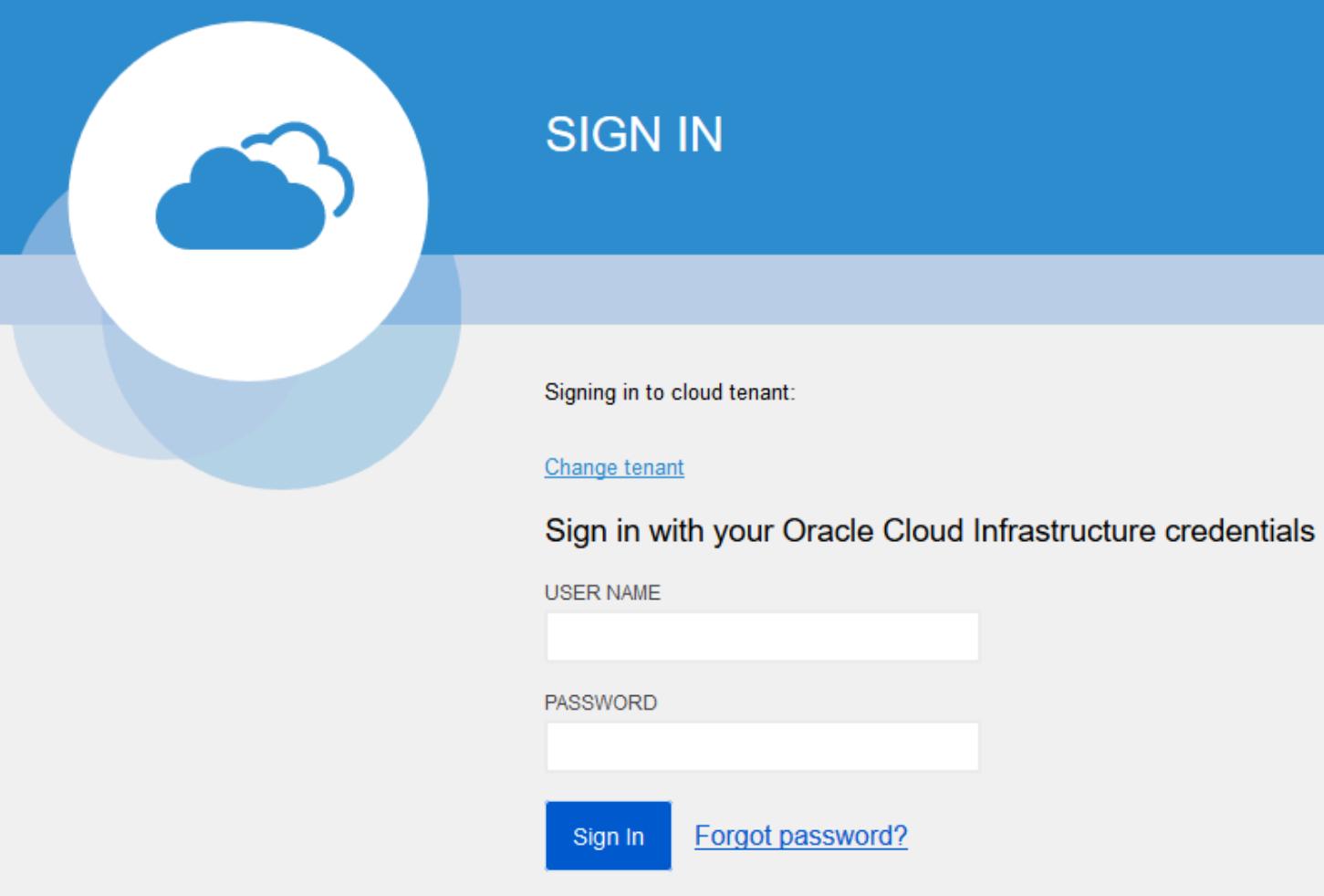
*Oracle Linux 8.5 OS*は、OKE に CN-Series ファイアウォールを導入するための唯一の認定環境です。

STEP 1 | Kubernetes クラスタをセットアップします。

OKE でクラスタを作成するには、次のように実施します。

1. Oracle Cloud Infrastructure にログインします。

ORACLE® Cloud Infrastructure



2. ナビゲーションメニューをクリックし、ソリューションとプラットフォームに移動して、開発者サービスをクリックします。
3. **Kubernetes Clusters**をクリックします。
4. コンパートメントを選択し、クラスタの作成をクリックします。

Clusters in Tutorial2 Compartment

Clusters Requirements: [Preparing for Container Engine for Kubernetes](#)
[Show more information](#)

Create Cluster

Name	Status	Node Pools	VCN	Version	Cre
No clusters exist. Create one to get started.					

5. [クラスタを作成] ダイアログ ボックスにて、カスタム作成をクリックし、ワークフローを起動をクリックします。
6. **Create Cluster**ページで、クラスタ名とその他の詳細を入力します。
7. 次へをクリックして、新しいクラスタについて入力した詳細を確認します。
8. レビューページで、**Create Cluster**をクリックします。

Cluster Creation

[Create Cluster](#)

NEW

Resources to be created

Basic Information

Cluster Name: cluster1**Compartment:** Tutorial2**Version:** v1.18.10

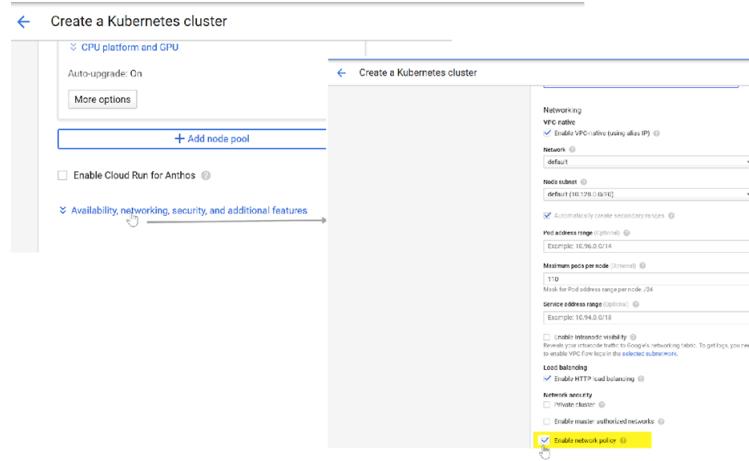
Network

Compartment: Tutorial2

VCN Name: oke-vcn-quick-cluster1-4baf5729a

Network Security Groups: Not Enabled**Kubernetes API Private Endpoint:** Auto Assigned**Kubernetes API Public Endpoint:** Auto Assigned**Kubernetes CIDR Block:** 10.96.0.0/16[Create Cluster](#)[Cancel](#)

自 クラスタが *GKE* 上に存在する場合は、クラスタ管理者が相互通信を許可するポッドを指定できるように、*Kubernetes* ネットワーク ポリシー API を有効にしてください。この API は、*CN-NGFW* ポッドと *CN-MGMT* ポッドが通信するために必要です。



クラスタのリソースが適切であることを確認します。ファイアウォールをサポートするための [CN シリーズの前提条件](#) リソースがクラスタにあることを確認します。

kubectl get nodes

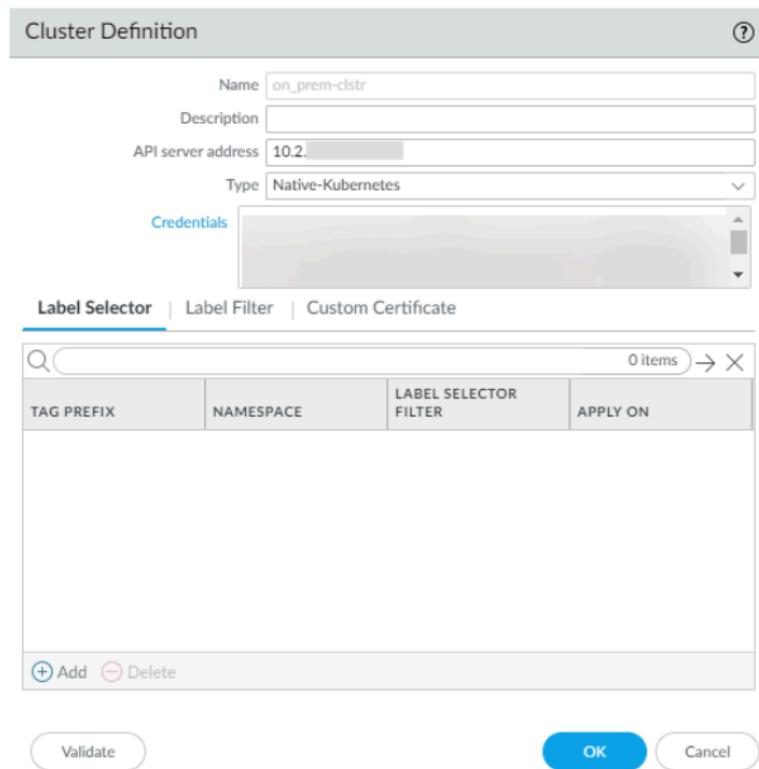
kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能な CPU とメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。 [「CN シリーズのパフォーマンスとスケーラビリティ」](#) を参照してください。

以下の情報があることを確認してください。

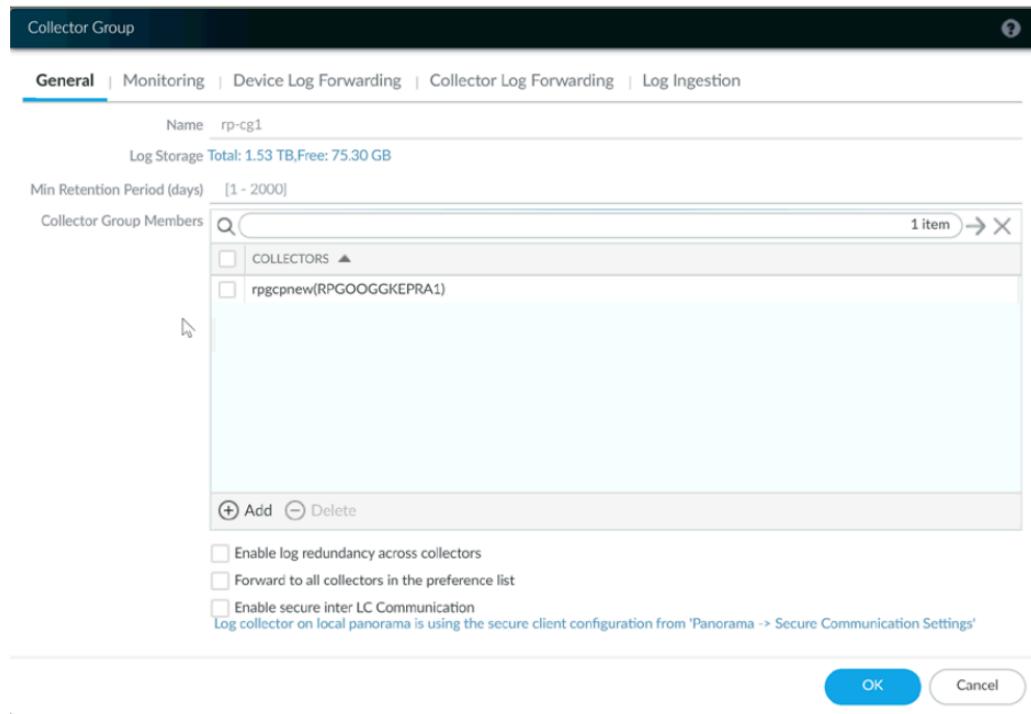
- Panorama 上で API サーバーをセットアップするためのエンドポイント IP アドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

詳細については、[クラスタをモニタリングするための Kubernetes プラグインの設定](#)をご覧ください。

- テンプレート スタック名、デバイス グループ名、Panorama IP アドレス、およびオプションで Panorama からログ コレクタ グループ名を収集します。



詳細については、[親デバイスグループとテンプレートスタックの作成](#)を参照してください。

- 認証コードと自動登録の PIN ID と値を収集します。
- イメージをダウンロードしたコンテナイメージリポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt-dynamic-pv.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

```
kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt
```

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

非公開の Google Container レジストリへのパスを含め、必要なパラメータを提供するには、YAML ファイル内のイメージパスを置き換える必要があります。詳細は、「[CN-Series 配置の yaml ファイルで編集可能なパラメータ](#)」を参照してください。

STEP 4 | CNI DaemonSet をデプロイします。

CNI コンテナは、DaemonSet(ノードあたり 1 つのポッド)としてデプロイされ、ノード上にデプロイされたアプリケーションごとに 2 つずつのインターフェースを CN-NGFW ポッド上

を作成します。kubectl コマンドを使用して pan-cni YAML ファイルを実行すると、それが各ノード上のサービス チェーンに組み込まれます。

💡 *CN-Series ファイアウォールを Kubernetes サービスとして OKE にデプロイする場合、pan-cni-k8s-daemonset ネイティブフォルダーの yaml ファイルを使用できます。*

1. CN-Series ファイアウォールには、Kubernetes クラスタリソースと通信することを許可する最小権限を備えた 3 つのサービス アカウントが必要です。[Create Service Accounts for Cluster Authentication with CN-Series\(CN-Seriesを使用したクラスタ認証用サービスアカウントの作成\)](#)を作成し、pan-cni-serviceaccount.yamlを使用してサービスアカウントを作成したことを確認します。
2. Kubectl を使用して pan-cni-configmap.yaml を実行します。
kubectl apply -f pan-cni-configmap.yaml
3. Kubectl を使用して pan-cni.yaml を実行します。
kubectl apply -f pan-cni.yaml
4. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。
5. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v    series-mktplace)$ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkf
pan-cni-wjrkq
pan-cni-xrc2z
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v    series-mktplace)$
```

STEP 5 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1 つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

pan-cn-mgmt-configmap のサンプル

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-config
namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-svc
PAN_MGMT_SECRET: pan-mgmt-secret # パノラマ設定 PAN_PANORAMA_IP:
"<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>"
PAN_TEMPLATE_STACK: "<panorama-template-stack>" PAN_CGNAME:
"<panorama-collector-group>" #必須ではないパラメーター # Panorama
Kubernetes プラグインで提供されるクラスター名と同じ名前にするこ
とをお勧めします - 同じ Panorama #CLUSTER_NAME で複数のクラス
ターを管理する場合、ポッドを簡単に識別できます: "<Cluster name>"#
#PAN_PANORAMA_IP2: "" # CERT を使用する場合はコメント アウトし
ます。それ以外の場合は、pan-mgmt と pan-ngfw の間の IPSec の PSK
```

```

#IPSEC_CERT_BYPASS: "" # 値は必要ありません # ジャンボ フレーム モードの自動検出をオーバーライドし、システム全体で強制的に有効にします #
PAN_JUMBO_FRAME_ENABLED: "true" # GTP を有効にして MGMT ポッドを開始します。完全な機能を実現するには、Panorama でも GTP # を有効にする必要があります。#PAN_GTP_ENABLED:「true」# 高い機能容量を有効にします。これらには、MGMT ポッド用に大量のメモリが必要であり、NGFW ポッド用に以下で指定されている # 以上のメモリが必要です。 # システム要件のドキュメントを参照して、各メモリ プロファイルでサポートされている # サポートされている NGFW CPU の最大サイズを確認してください。 #PAN_NGFW_MEMORY:"6.5Gi"
#PAN_NGFW_MEMORY:"48Gi" #PAN_NGFW_MEMORY:"56Gi"

```

pan-cn-mgmt-dynamic-pv.yaml のサンプル

```

initContainers: - name: pan-mgmt-init image: <your-private-registry-image-path>

```

```

  containers: - name: pan-mgmt image: <your-private-registry-image-path> terminationMessagePolicy:FallbackToLogsOnError

```

2. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml
```

```
kubectl apply -f pan-cn-mgmt-secret.yaml
```

```
kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml
```

[CN-Seriesを使用したクラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ、pan-mgmt-serviceaccount.yaml を実行する必要があります。

3. CN-MGMT ポッドが起動していることを確認します。

これには、5 ~ 6 分かかります。

```
kubectl get pods -l app=pan-mgmt -n kube-system を使用します。
```

```
NAME READY STATUS RESTARTS AGE
pan-mgmt-sts-0 1/1
Running 0 27h
pan-mgmt-sts-1 1/1 Running 0 27h
```

STEP 6 | CN-NGFW ポッドをデプロイします。

デフォルトで、ファイアウォールデータプレーン CN-NGFW ポッドは DaemonSet としてデプロイされます。CN-NGFW ポッドのインスタンスは、1 つのノード上で最大 30 個のアプリケーション ポッドのトラフィックを保護することができます。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. すべての CN-NGFW ポッド (クラスタ内のノードあたり 1 つずつ) が実行していることを確認します。

これは、4 ノード オンプレミス クラスタからの出力例です。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide  
NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES  
pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>  
pan-ngfw-ds-qsrn6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>  
pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>  
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
```

STEP 7 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 Running
0 27hpan-cni-9j4rs 1/1 Running
0 27hpan-cni-ddwb4 1/1 Running
0 27hpan-cni-fwfrk 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-j62rk 1/1 Running
0 27hpan-cni-lmxdz 1/1 Running
0 27hpan-mgmt-sts-0 1/1 Running
0 27hpan-mgmt-sts-1 1/1 Running
0 27hpan-ngfw-ds-8g5xb 1/1 Running
27hpan-ngfw-ds-qsrn6 1/1 Running
0 27hpan-ngfw-ds-vqk7z 1/1 Running
0 27hpan-ngfw-ds-zncqg 1/1 Running
```

STEP 8 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```



一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

```
volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: ディレクトリ
```

STEP 9 | クラスタでアプリケーションをデプロイします。

CN-Series ファイアウォールを EKS にデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> • CN-Seriesデプロイメント 	<ul style="list-style-type: none"> • CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CNシリーズ ビルディング ブロックとCNシリーズ ファイアウォールによるKubernetesの安全な環境内のワークフローの概要を確認したら、同じクラスタ内のコンテナ間やコンテナと他のワークロード タイプ(仮想マシンやベアメタル サーバーなど)間のトラフィックを保護するためのAWS EKS プラットフォームにおけるCN-Series ファイアウォールのデプロイから始めることができます。



Kubernetes クラスタ、アプリケーション、およびファイアウォール サービスをデプロイして管理するためには、*kubectl* や *Helm* などの標準の *Kubernetes* ツールが必要です。

詳細については、「*Helm* チャートとテンプレートを使用した [CN-Series ファイアウォールのデプロイ](#)」を参照してください。*Panorama* は、*Kubernetes* クラスタのデプロイメントと管理用のオーケストレーターになるようには設計されていません。クラスタ管理用のテンプレートがマネージド *Kubernetes* プロバイダから提供されています。*Palo Alto Networks* は、*Helm* および *Terraform* で *CN-Series* をデプロイするためのコミュニティサポートのテンプレートを提供しています。

- CN-Series ファイアウォールを AWS EKS に Kubernetes サービスとしてデプロイする
- CN-Series ファイアウォールを AWS EKS に DaemonSet としてデプロイする
- AWS Marketplace から CN-Seriesをデプロイする



CN-Series を *DaemonSet* としての *CN-Series* からサービスとしての *CN-Series*、またはその逆に移行する前に、*plugin-serviceaccount.yaml* を削除して再適用する必要があります。詳細については、「[クラスタ認証用サービスアカウントの作成](#)」を参照してください。

- *CN-Series* を *EKS* 上の *DaemonSet* としてデプロイする場合、*pan-plugin-cluster-mode-secret* が存在してはいけません。
- *CN-Series* を *EKS* 上の *Kubernetes* サービスとしてデプロイする場合は、*pan-plugin-cluster-mode-secret* が存在する必要があります。

CN-Series ファイアウォールを AWS EKS に Kubernetes サービスとしてデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Series デプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している• Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

以下の手順を実行して、CN-Series ファイアウォールを Kubernetes サービスとしてデプロイします。

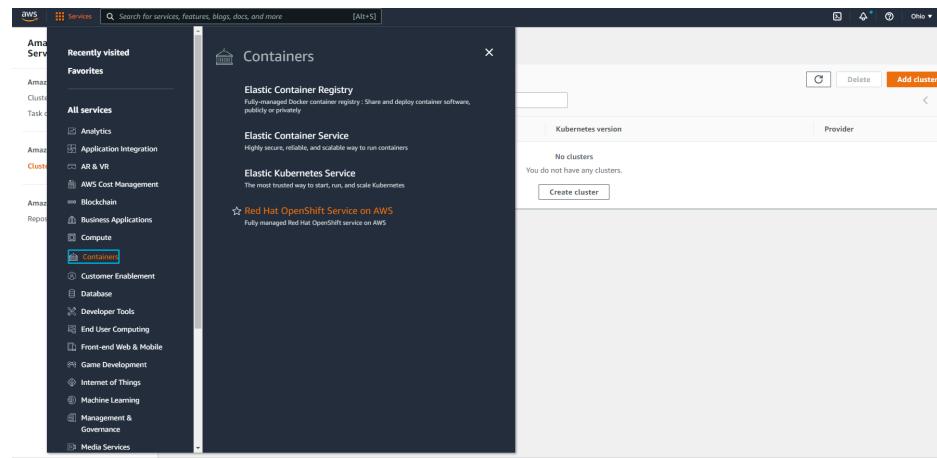
開始する前に、CN-Series YAML ファイルのバージョンが PAN-OS バージョンと互換性があることを確認します。

- PAN-OS 10.1.2 以降には YAML 2.0.2 が必要です
- PAN-OS 10.1.0 および 10.1.1 には YAML 2.0.0 または 2.0.1 が必要です

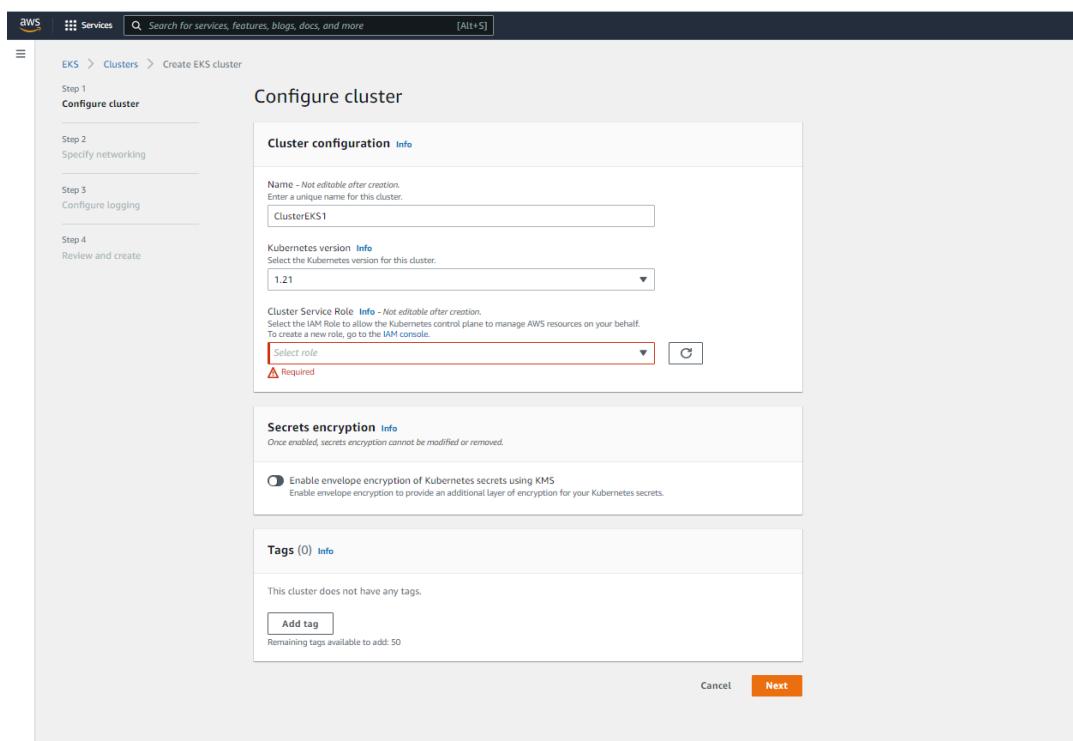
STEP 1 | Kubernetes クラスタをセットアップします。

AWS EKS でクラスターを作成するには、次の手順を実行します。

- サービスナビゲーションメニューをクリックし、コンテナ->**Elastic Kubernetes Service**に移動します。



- [クラスタの作成]をクリックします。
- 必要な詳細を入力し、 [作成] をクリックします。



- クラスタのリソースが適切であることを確認します。クラスタにファイアウォールをサポートするための**CNシリーズの前提条件**のリソースが含まれていることを確認します。

kubectl get nodes

kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能な CPU とメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。CNシリーズのパフォーマンスとスケーリングを参照してください。

以下の情報があることを確認してください。

- Panorama 上で API サーバーをセットアップするためのエンドポイント IP アドレスを収集します。Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。
- テンプレート スタック名、デバイス グループ名、Panorama IP アドレス、およびオプションで Panorama からログ コレクタ グループ名を収集します。
- 認証コードと自動登録の PIN ID と値を収集します。
- イメージをダウンロードしたコンテナ イメージ リポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

プライベート レジストリへのパスを含み、必要なパラメータを提供するように YAML ファイル内のイメージパスを置き換える必要があります。詳細は、「CN-Series 配置の yaml ファイルで編集可能なパラメータ」を参照してください。

STEP 4 | ストレージクラスを更新します。AWS Outpost にデプロイされた CN-Series をサポートするには、ストレージドライバー aws-ebs-csi-driver を使用する必要があります。これにより、動的永続ボリューム (PV) の作成中に Outpost が Outpost からボリュームをプルします。

1. 以下の yaml を適用します。

```
kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/
deploy/kubernetes/overlays/stable/?ref=release-0.10"
```

2. ebs-sc コントローラーが実行されていることを確認します。

```
kubectl -n kube-system get pods
```

3. 以下の例に一致するように pan-cn-storage-class.yaml を更新します。

```
apiVersion: v1 kind:StorageClass apiVersion: storage.k8s.io/
v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com
volumeBindingMode:WaitForFirstConsumer parameters: type: gp2
```

4. 以下に示す場所で、**storageClassName : ebs-sc** を pan-cn-mgmt.yaml に追加します。

```
volumeClaimTemplates: - metadata: name: panlogs spec:
  #storageClassName: pan-cn-storage-class //For better disk
  iops performance for logging accessModes: [ "ReadWriteOnce" ]
  storageClassName: ebs-sc // resources: requests: storage:20Gi
  # ディスク IOPS を向上させるためにstorageClassName を使用
  しているときにこれを 200Gi に変更します - metadata: name:
  varlogpan spec: #storageClassName: pan-cn-storage-
  class // dp ログのディスク IOPS パフォーマンスを向上させるため
  accessModes: [ "ReadWriteOnce" ] storageClassName: ebs-
  sc resources: requests: storage:20Gi # ディスク IOPS 向
  上のために storageClassName を使用している間、これを 200Gi に
  変更します - metadata: name: varcores spec: accessModes:
  [ "ReadWriteOnce" ] storageClassName: ebs-sc resources:
  requests: storage:2Gi - metadata: name: panplugincfg spec:
  accessModes: [ "ReadWriteOnce" ] storageClassName: ebs-sc
  resources: requests: storage:1Gi - metadata: name: panconfig
  spec: accessModes: [ "ReadWriteOnce" ] storageClassName:
  ebs-sc resources: requests: storage:8Gi - metadata:
  name: panplugins spec: accessModes: [ "ReadWriteOnce" ]
  storageClassName: ebs-sc resources: requests: storage:200Mi
```

STEP 5 | Kubernetes 環境でオートスケーリングを使用している場合は、次の手順を実行します。

1. CN-Series で、[Kubernetes 用 Amazon CloudWatch メトリクスアダプター](#)をサービスクラス ターとしてデプロイします。CloudWatch に、Kubernetes ポッドとクラスターに関連付けられた両方の IAM ロールへの完全なアクセスを許可する必要があります。カスタムメトリクスを CloudWatch に公開するには、HPA がそれらを取得できるように、ワーカーノードのロールに AWS 管理ポリシー **CloudWatchAgentServerPolicy** が必要です。
2. [Palo Alto Networks GitHub リポジトリ](#)から EKS 固有の HPA yaml ファイルをダウンロードします。

3. CN-MGMT がカスタム名前空間にデプロイされている場合は、カスタム名前空間を使用して pan-cn-adapater.yaml を更新します。デフォルトの名前空間は **kube-system** です。
4. **pan-cn-hpa-dp.yaml** と **pan-cn-hpa-mp.yaml** を変更します。
 1. レプリカの最小数と最大数を入力します。
 2. (任意) スケールダウンを変更し、デプロイメントに合わせて頻度値をスケールアップします。これらの値を変更しない場合は、デフォルト値が使用されます。
 3. スケーリングに使用する各メトリックについて、以下のセクションをコピーします。

```
- type: Pods pods: metric: name: pansessionactive target:
  type: AverageValue averageValue:30
```

4. 使用するメトリックの名前を変更し、**averageValue** を上記の表で説明したしきい値に設定します。これらの値を変更しない場合は、デフォルト値が使用されます。
 5. 変更を保存します。
- 詳細については、Horizontal Pod Autoscalingを参照してください。
5. HPA yaml ファイルをデプロイします。ファイルは、以下に説明する順序でデプロイする必要があります。
 1. Kubectl を使用して pan-cn-adapter.yaml を実行します
`kubectl apply -f pan-cn-adapter.yaml`
 2. Kubectl を使用して pan-cn-externalmetrics.yaml を実行します
`kubectl apply -f pan-cn-externalmetrics.yaml`
 3. Kubectl を使用して pan-cn-hpa-dp.yaml を実行します
`kubectl apply -f pan-cn-hpa-dp.yaml`
 4. Kubectl を使用して pan-cn-hpa-mp.yaml を実行します
`kubectl apply -f pan-cn-hpa-mp.yaml`
 6. デプロイメントを確認します。

kubectl を使用して、カスタム メトリックス名前空間内のカスタム メトリック アダプター ポッドを確認します。

`kubectl get pods -n custom-metrics`

kubectl を使用して、HPA リソースを確認します。

`kubectl get hpa -n kube-system`

`kubectl describe hpa <hpa-name> -n kube-system`

STEP 6 | CN-NGFW サービスをデプロイします。

1. pan-cni-serviceaccount.yaml を使用してサービス アカウントが作成されたことを確認します。

[クラスタ認証用のサービス アカウントの作成](#)を参照してください。

2. Kubectl を使用して pan-cni-configmap.yaml を実行します。

kubectl apply -f pan-cni-configmap.yaml

3. kubectl を使用して pan-cn-ngfw-svc.yaml を実行します。

kubectl apply -f pan-cn-ngfw-svc.yaml



この yaml は pan-cni.yaml の前にデプロイする必要があります。

4. Kubectl を使用して pan-cni.yaml を実行します。

kubectl apply -f pan-cni.yaml

5. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。

6. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

kubectl get pods -n kube-system | grep pan-cni

```
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v) [series-mktplace]$ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkt
pan-cni-wjrkq
pan-cni-xrc2z
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v) [series-mktplace]$
```

STEP 7 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1 つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. (静的にプロビジョニングされた PV のみに必要) CN-MGMT StatefulSet 用の永続ボリューム (PV) をデプロイします。

1. pan-cn-pv-local.yaml で定義されたローカル ボリューム名と一致するディレクトリを作成します。

少なくとも 2 つのワーカー ノード上に 6 つのディレクトリが必要です。CN-MGMT StatefulSet をデプロイする各ワーカー ノードにログインして、ディレクトリを作成

します。たとえば、/mnt/pan-local1 から /mnt/pan-local6 という名前のディレクトリを作成するには、次のコマンドを使用します。

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /  
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. pan-cn-pv-local.yaml を変更します。

`nodeaffinity` の下でホスト名を一致させ、上記で `spec.local.path` に作成したディレクトリが変更されたことを確認してから、そのファイルをデプロイして、新しいストレージクラス `pan-local-storage` とローカル PV を作成します。

2. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

EKS から pan-cn-mgmt-configmap をサンプリングします。

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-  
config namespace: kube-system data:PAN_SERVICE_NAME: pan-  
mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama 設  
定 PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP:  
"<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-  
template-stack>" PAN_CNAME: "<panorama-collector-  
group>" # ctnr mode: "k8s-service", "k8s-ilbservice"  
PAN_CTNR_MODE_TYPE: "k8s-service" #必須でないパラメータ #  
Panorama Kubernetes プラグインで提供されるクラスタ名と同じ名前  
を持つことを推奨 - 同じ Panorama で複数のクラスタを管理する場合、  
ポッドの識別が容易になります #CLUSTER_NAME: "<Cluster name>"  
#PAN_PANORAMA_IP2: "" # CERT を使用する場合はコメントアウト  
します。それ以外の場合は、pan-mgmt と pan-ngfw 間の IPsec 用に  
PSK を使用します #IPSEC_CERT_BYPASS: "" # 値は不要 # jumbo-  
frame モードの自動検出をオーバーライドし、システム全体を強制的に有  
効にします #PAN_JUMBO_FRAME_ENABLED: "true" # GTP を有効にし  
て MGMT を起動します。完全な機能を実現するには、Panorama でも GTP  
# を有効にする必要があります。#PAN_GTP_ENABLED: "true" # 高い  
機能容量を有効にします。これらは MGMT ポッドには高いメモリを必要と  
し、NGFW ポッドには以下の指定以上のメモリが必要です。#PAN_NGFW_MEMORY =  
"6Gi" #PAN_NGFW_MEMORY = "40Gi" # より高速なデータパス-AF_XDP を有  
効にするには、デフォルトは AF_PACKETV2 です。これにはカーネルのサポート  
が必要です。#PAN_DATA_MODE: "次世代" #HPA params #PAN_CLOUD: "EKS"  
#PAN_NAMESPACE_EKS: "EKSNamespace" #PUSH_INTERVAL: "15" #AWS  
cloudwatch にメトリクスを発行する間隔
```

pan-cn-mgmt.yaml のサンプル

```
initContainers: - name: pan-mgmt-init image: <your-private-  
registry-image-path>
```

```
containers: - name: pan-mgmt image: <your-private-registry-  
image-path> terminationMessagePolicy:FallbackToLogsOnError
```

3. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml
kubectl apply -f pan-cn-mgmt-slot-crd.yaml
kubectl apply -f pan-cn-mgmt-slot-cr.yaml
kubectl apply -f pan-cn-mgmt-secret.yaml
kubectl apply -f pan-cn-mgmt.yaml
```

pan-mgmt-serviceaccount.yaml は、[クラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

4. CN-MGMT ポッドが起動していることを確認します。

これには、5 ~ 6 分かかります。

```
kubectl get pods -l app=pan-mgmt -n kube-system
```

を使用します。

STEP 8 | CN-NGFW ポッドをデプロイします。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. CN-NGFW ポッドがデプロイされたことを確認します。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
```

STEP 9 | CN-Series で水平ポッド自動スケーリングを有効にします。

STEP 10 | Kubernetes クラスタ上での CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
```

STEP 11 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```

 一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

```
volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: ディレクトリ
```

STEP 12 | クラスタでアプリケーションをデプロイします。

CN-Series ファイアウォールを AWS EKS に DaemonSet としてデプロイする

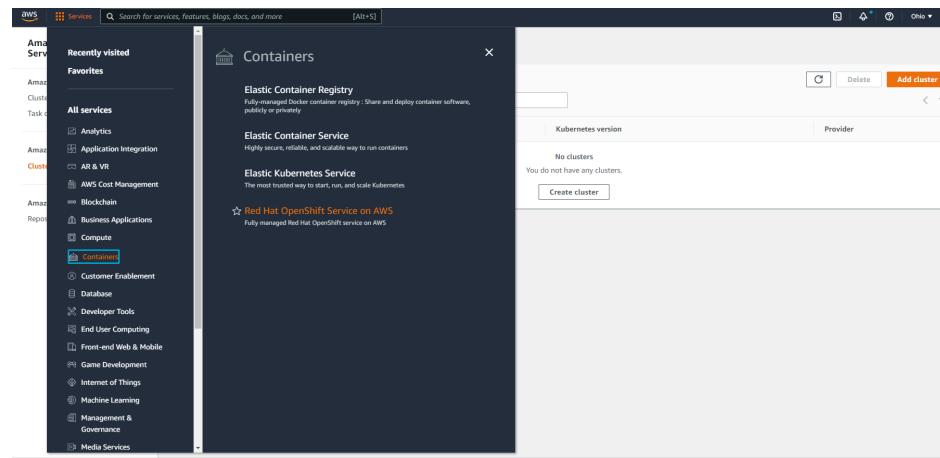
どこで使用できますか?	何が必要か?
<ul style="list-style-type: none">• CN-Seriesデプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaHelmを使用してCN-SeriesをデプロイするためのPAN-OS 10.1.xまたはそれ以上のバージョンを実行している場合• Helm 3.6 or above version client 以下の手順を完了し、

CN-Series ファイアウォールを AWS EKS 上の daemonset としてデプロイします。

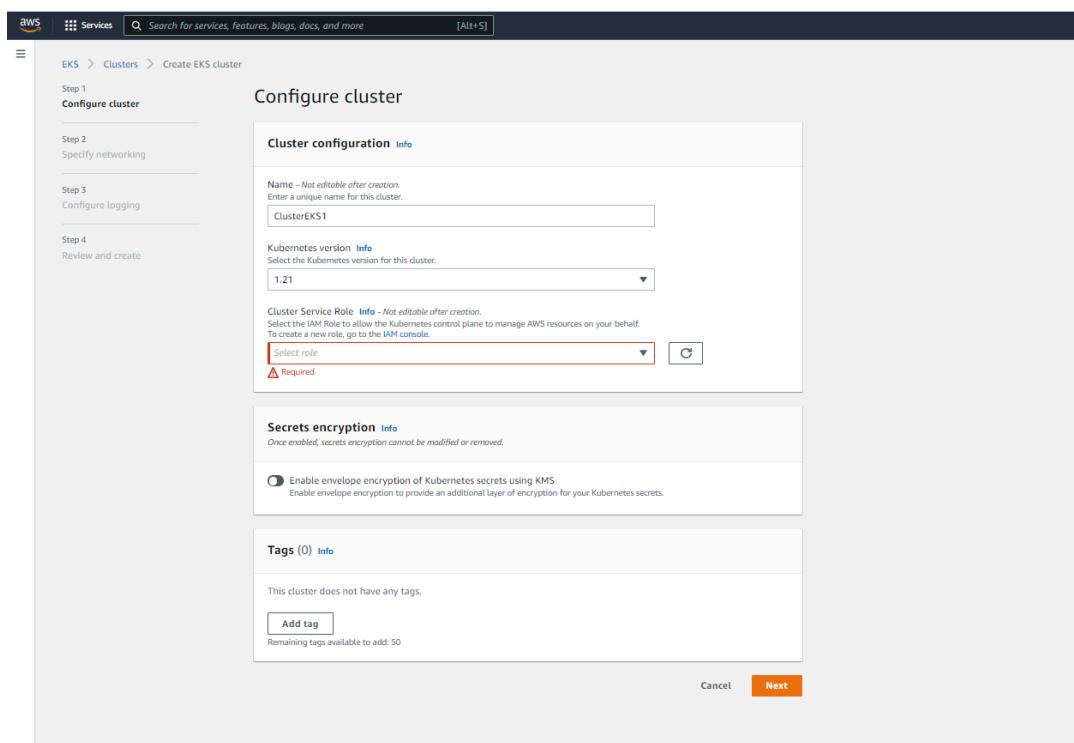
STEP 1 | Kubernetes クラスタをセットアップします。

AWS EKS でクラスターを作成するには、次の手順を実行します。

- サービスナビゲーションメニューをクリックし、コンテナ->**Elastic Kubernetes Service**に移動します。



- [クラスタの作成]をクリックします。
- 必要な詳細を入力し、 [作成] をクリックします。



クラスタのリソースが適切であることを確認します。クラスタにファイアウォールをサポートするためのCNシリーズの前提条件のリソースが含まれていることを確認します。

kubectl get nodes

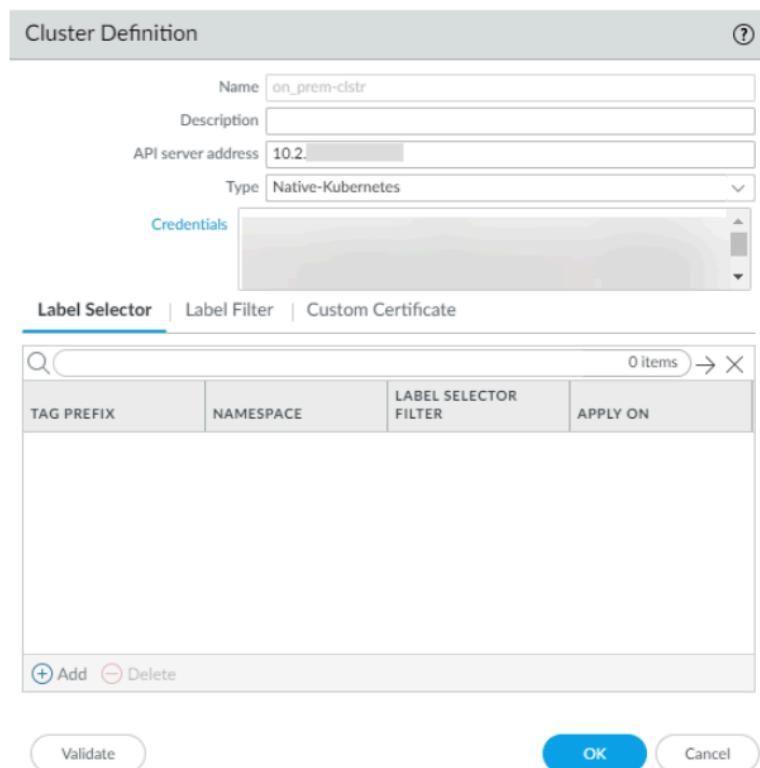
kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能な CPU とメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。CN シリーズの [パフォーマンスとスケーリング](#) を参照してください。

以下の情報があることを確認してください。

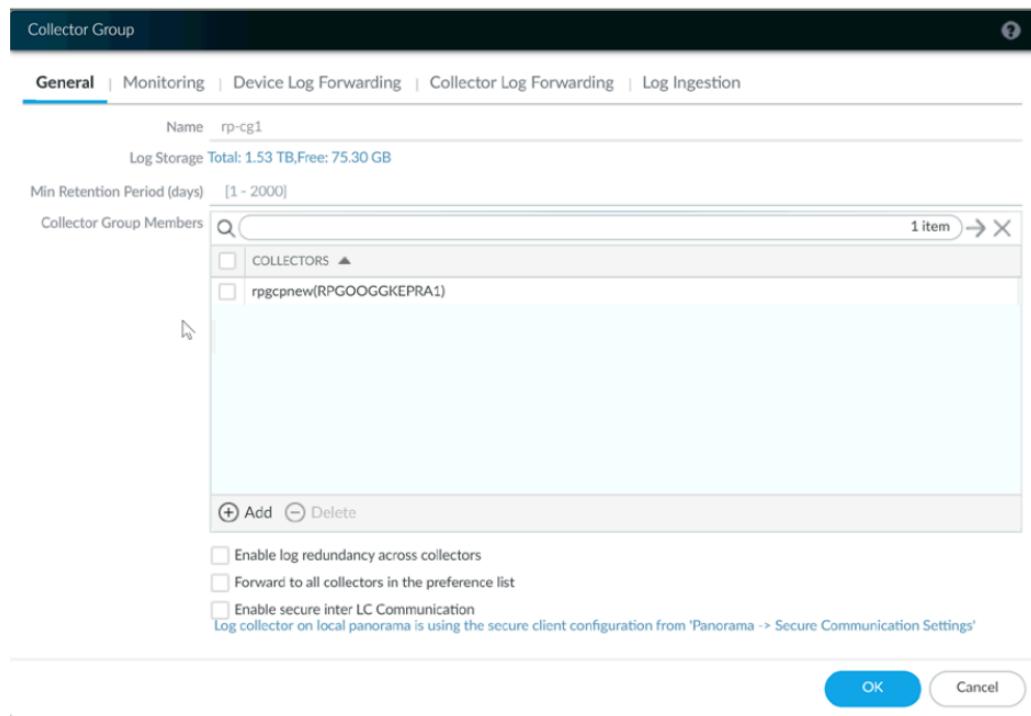
- Panorama 上で API サーバーをセットアップするためのエンドポイント IP アドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

詳細については、[クラスタをモニタリングするための Kubernetes プラグインの設定](#)をご覧ください。

- テンプレート スタック名、デバイス グループ名、Panorama IP アドレス、およびオプションで Panorama からログコレクタ グループ名を収集します。



詳細については、[親デバイスグループとテンプレートスタックの作成](#)を参照してください。

- [認証コード](#)と[自動登録の PIN ID](#)と値を収集します。
- イメージをダウンロードしたコンテナイメージリポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

非公開の Google Container レジストリへのパスを含め、必要なパラメータを提供するには、YAML ファイル内のイメージパスを置き換える必要があります。詳細は、「[CN-Series 配置の yaml ファイルで編集可能なパラメータ](#)」を参照してください。

STEP 4 | CNI DaemonSet をデプロイします。

CNI コンテナは、DaemonSet(ノードあたり 1 つのポッド)としてデプロイされ、ノード上にデプロイされたアプリケーションごとに 2 つずつのインターフェースを CN-NGFW ポッド上

を作成します。kubectl コマンドを使用して pan-cni YAML ファイルを実行すると、それが各ノード上のサービス チェーンに組み込まれます。

1. CN-Series ファイアウォールには、Kubernetes クラスタリソースと通信することを許可する最小権限を備えた 3 つのサービス アカウントが必要です。Create Service Accounts for Cluster Authentication (クラスタ認証用サービスアカウントの作成) を作成し、pan-cni-serviceaccount.yaml を使用してサービスアカウントを作成したことを確認します。
2. Kubectl を使用して pan-cni-configmap.yaml を実行します。
kubectl apply -f pan-cni-configmap.yaml
3. Kubectl を使用して pan-cni.yaml を実行します。
kubectl apply -f pan-cni.yaml
4. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。
5. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v...@series-mktplace) $ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkf
pan-cni-wjrkq
pan-cni-xrc22
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v...@series-mktplace) $
```

STEP 5 |ストレージクラスを更新します。AWS Outpost にデプロイされた CN-Series をサポートするには、ストレージドライバー aws-ebs-csi-driver を使用する必要があります。これにより、動的永続ボリューム (PV) の作成中に Outpost が Outpost からボリュームをプルします。

1. 以下の yaml を適用します。

```
kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/
deploy/kubernetes/overlays/stable/?ref=release-0.10"
```

2. ebs-sc コントローラーが実行されていることを確認します。

```
kubectl -n kube-system get pods
```

3. 以下の例に一致するように pan-cn-storage-class.yaml を更新します。

```
apiVersion: v1 kind:StorageClass apiVersion: storage.k8s.io/
v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com
volumeBindingMode:WaitForFirstConsumer parameters: type: gp2
```

4. 以下に示す場所で、**storageClassName : ebs-sc** を pan-cn-mgmt.yaml に追加します。

```
volumeClaimTemplates: - metadata: name: panlogs spec:
#storageClassName: pan-cn-storage-class //For better disk
iops performance for logging accessModes: [ "ReadWriteOnce" ]
storageClassName: ebs-sc // resources: requests: storage:20Gi
# ディスク IOPS を向上させるためにstorageClassName を使用
しているときにこれを 200Gi に変更します - metadata: name:
varlogpan spec: #storageClassName: pan-cn-storage-
class // dp ログのディスク IOPS パフォーマンスを向上させるため
```

```

accessModes: ["ReadWriteOnce"] storageClassName: ebs-
sc resources: requests: storage:20Gi # ディスク IOPS 向
上のため storageClassName を使用している間、これを 200Gi に
変更します - metadata: name: varcores spec: accessModes:
[ "ReadWriteOnce" ] storageClassName: ebs-sc resources:
requests: storage:2Gi - metadata: name: panplugincfg spec:
accessModes: [ "ReadWriteOnce" ] storageClassName: ebs-sc
resources: requests: storage:1Gi - metadata: name: panconfig
spec: accessModes: [ "ReadWriteOnce" ] storageClassName:
ebs-sc resources: requests: storage:8Gi - metadata:
name: panplugins spec: accessModes: [ "ReadWriteOnce" ]
storageClassName: ebs-sc resources: requests: storage:200Mi

```

STEP 6 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1 つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. (静的にプロビジョニングされた PV のみに必要) CN-MGMT StatefulSet 用の永続ボリューム (PV) をデプロイします。
2. pan-cn-pv-local.yaml で定義されたローカル ボリューム名と一致するディレクトリを作成します。

少なくとも 2 つのワーカー ノード上に 6 つのディレクトリが必要です。CN-MGMT StatefulSet をデプロイする各ワーカー ノードにログインして、ディレクトリを作成します。たとえば、/mnt/pan-local1 から /mnt/pan-local6 という名前のディレクトリを作成するには、次のコマンドを使用します。

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. pan-cn-pv-local.yaml を変更します。

nodeaffinity の下でホスト名を一致させ、上記で spec.local.path に作成したディレクトリが変更されたことを確認してから、そのファイルをデプロイして、新しいストレージ クラス pan-local-storage とローカル PV を作成します。

2. pan-cn-mgmt-configmap YAML ファイルと pan-cn-mgmt YAML ファイルが変更されたことを確認します。

EKS から pan-cn-mgmt-configmap をサンプリングします。

```

復元されたセッション コンテンツ apiVersion: v1 kind:ConfigMap
metadata: name: pan-mgmt-config namespace: kube-system
data:PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-
mgmt-secret # Panorama 設定 PAN_PANORAMA_IP: "x.y.z.a"
PAN_DEVICE_GROUP: "dg-1" PAN_TEMPLATE_STACK: "temp-stack-1"
PAN_CGNAME:"CG-EKS" # 意図されたライセンス バンドル タイプ - "CN-
X-BASIC", "CN-X-BND1", "CN-X-BND2" # Panorama K8S プラグインに適
用された認証コードに基づく" PAN_BUNDLE_TYPE:"CN-X-BND2"# 必須ではな

```

いパラメーター # Panorama Kubernetes プラグインで提供されるクラスター名と同じ名前にすることをお勧めします-同じ Panorama #CLUSTER_NAME で複数のクラスターを管理する場合、ポッドを簡単に識別できます。"Cluster-name" #PAN_PANORAMA_IP2: "passive-secondary-ip" # CERT を使用する場合はコメントアウトします。それ以外の場合は、pan-mgmt の etcd への暗号化された接続をバイパスします。# EKS バグのために etcd に CERT を使用しない ETCD_CERT_BYPASS: "" # 値は必要ありません # CERT を使用するようにコメントアウトしてください。それ以外の場合は、pan-mgmt と pan-ngfw 間の IPSec に PSK を使用します。# IPSEC_CERT_BYPASS: "" # 値は必要ありません

pan-cn-mgmt.yaml のサンプル

```
initContainers: - name: pan-mgmt-init image: <your-private-registry-image-path>
```

```
  containers: - name: pan-mgmt image: <your-private-registry-image-path> terminationMessagePolicy: FallbackToLogsOnError
```

3. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml  
kubectl apply -f pan-cn-mgmt-slot-crd.yaml  
kubectl apply -f pan-cn-mgmt-slot-cr.yaml  
kubectl apply -f pan-cn-mgmt-secret.yaml  
kubectl apply -f pan-cn-mgmt.yaml
```

pan-mgmt-serviceaccount.yaml は、[CN-Series ファイアウォールを使用したクラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

4. CN-MGMT ポッドが起動していることを確認します。

これには、5 ~ 6 分かかります。

```
kubectl get pods -l app=pan-mgmt -n kube-system
```

を使用します。

```
NAME READY STATUS RESTARTS AGE  
pan-mgmt-sts-0 1/1 Running 0  
pan-mgmt-sts-1 1/1 Running 0 27h
```

STEP 7 | CN-NGFW ポッドをデプロイします。

デフォルトで、ファイアウォールデータプレーン CN-NGFW ポッドは DaemonSet としてデプロイされます。CN-NGFW ポッドのインスタンスは、1 つのノード上で最大 30 個のアプリケーション ポッドのトラフィックを保護することができます。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. すべての CN-NGFW ポッド (クラスタ内のノードあたり 1 つずつ) が実行していることを確認します。

これは、4 ノード オンプレミス クラスタからの出力例です。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES
pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1 <none> <none>
pan-ngfw-ds-qsrn6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-worker-1 <none> <none>
pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vm-worker-3 <none> <none>
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-worker-2 <none> <none>
```

STEP 8 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
0 27hpan-cni-5fhbg 1/1 Running
0 27hpan-cni-9j4rs 1/1 Running
0 27hpan-cni-ddwb4 1/1 Running
0 27hpan-cni-fwfrk 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-h57lm 1/1 Running
0 27hpan-cni-j62rk 1/1 Running
0 27hpan-cni-lmxdz 1/1 Running
0 27hpan-mgmt-sts-0 1/1 Running
0 27hpan-mgmt-sts-1 1/1 Running
0 27hpan-ngfw-ds-8g5xb 1/1 Running
27hpan-ngfw-ds-qsrn6 1/1 Running
0 27hpan-ngfw-ds-vqk7z 1/1 Running
0 27hpan-ngfw-ds-zncqg 1/1 Running
```

STEP 9 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw
```



一部のプラットフォームでは、CNI プラグイン チェーン内で *pan-cni* がアクティブになっていない状態でアプリケーション ポッドが開始する可能性があります。このようなシナリオを回避するには、アプリケーション ポッド YAML にここに示すようにボリュームを指定する必要があります。

```
volumes: - name: pan-cni-ready hostPath: path: /var/log/
pan-appinfo/pan-cni-ready type: ディレクトリ
```

STEP 10 | クラスタでアプリケーションをデプロイします。

AWS Marketplace から CN-Seriesをデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> • CN-Seriesデプロイメント 	<ul style="list-style-type: none"> • CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォールは、[AWS Marketplace](#)を通じて AWS EKS にデプロイされた Kubernetes サービスとしてライセンスを取得できます。CNシリーズは、1か月、1年、2年、または3年のライセンスを取得し、EKS 1.19以降または Redhat Openshift 4.7 以降にデプロイできます。



この製品はプレビュー版です。

このライセンスを使用するには、Kubernetes ワーカーノードに添付されている IAM ポリシーを更新する必要があります。



– CN-Series のデプロイにAWS Marketplaceから購入した PAYG ライセンスを使用している場合は、KubernetesのPanorama プラグインに認証コードを追加しないでください。

STEP 1 | 次の前提条件を完了します。

1. EKS または Redhat OpenShift クラスターを作成します。
2. Panorama をデプロイし、Kubernetes プラグインをインストールします。



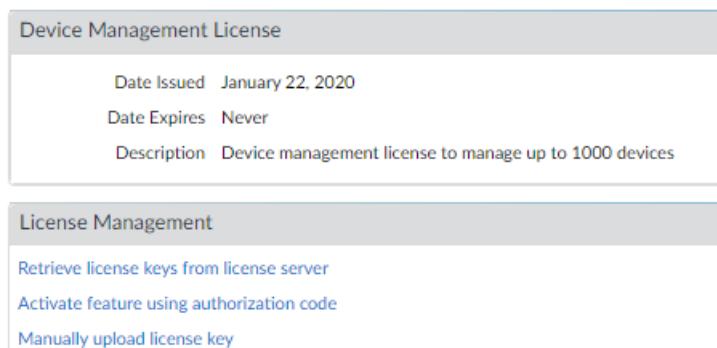
ライセンスされた Panorama インスタンスがすでに AWS にデプロイされている場合は、この手順をスキップしてください。

1. Amazon EC2インスタンスに[Panoramaをインストール](#)します。
2. [CNシリーズ用Kubernetesプラグインをインストール](#)します。
3. Panorama がインストールされたら、CN-Series チーム（cn-series-aws-marketplace@paloaltonetworks.com）に電子メールを送信して、Panoramaのライセンスをリクエストしてください。フルネーム、会社の電子メール、会社名、発注書番号、AWS アカウント名、および AWS アカウント ID を含めてください。

STEP 2 | シリアル番号とライセンスを Panorama に適用します。

1. Panorama Web インターフェイスにログインします。
2. [Panorama] > [Setup (セットアップ)] > [Management (管理)] を選択し、編集  アイコンをクリックします。
3. Panorama の **Serial Number** (シリアル番号) (受注完了電子メールに記載) を入力し、**OK** をクリックします。
4. **Panorama** > ライセンスを選択します。
5. **Activate feature using authorization code** (認証コードを使用した機能のアクティベーション) をクリックします。
6. ファイアウォール管理ライセンス認証コードを入力し、**OK** をクリックしてライセンスをアクティブ化します。
7. ファイアウォール管理ライセンスがアクティブ化されていることを確認します。

デバイス管理ライセンスセクションが表示され、ライセンスの発行日、ライセンスの有効期限、およびファイアウォール管理ライセンスの説明が表示されます。

**STEP 3 |** IAM ポリシーを更新し、そのポリシーを Kubernetes ワーカーノードに添付します。

1. AWS 管理コンソールにログインして IAM コンソールを開きます。
2. **Policies (ポリシー)** を選択します。
3. ポリシーリストから、**AWSLicenseManagerConsumptionPolicy** および **AWSMarketplaceMeteringRegisterUsage** を選択します。
4. アクションを選択してから、添付を選択します。
5. ポリシーを添付するワーカーノード ID を選択します。ID を選択したら、ポリシーの添付をクリックします。

STEP 4 | `plugin-serviceaccount.yaml` をダウンロードし、Helm チャートをデプロイする前に `yaml` を適用します。

```
kubectl apply -f plugin-serviceaccount.yaml
```

STEP 5 | AWS Marketplace にアクセスし、AWS Marketplace のリストから CN-Series を見つけます。

STEP 6 | Continue to Subscribe (続行して登録) をクリックします。

STEP 7 | 購入するライセンスの数を入力します。各ライセンス資格は、CN-Series のデプロイメントで使用される1つの vCPU と同等です。

デプロイメントのニーズを満たすために必要な vCPU の数については、[CN-Series のシステム要件](#)および[CN-Series のパフォーマンスとスケーリング](#)を参照してください。

STEP 8 | 設定に進むをクリックします。これにより、AWS アカウントにライセンスが追加されます。

1. フルフィルメントオプションとして**Helm**チャートを選択します。
2. ソフトウェアバージョンの最新バージョンを選択します。

[< Product Detail](#) [Subscribe](#) [Configure](#)

Configure this software

Choose a fulfillment option and software version to launch this software.

The screenshot shows a configuration interface for launching software. It includes a 'Fulfillment option' dropdown set to 'Helm Chart', a 'Software version' dropdown set to 'Version1.2.2 (Nov 22, 2021)', and a 'Supported services' list that includes 'Amazon EKS', 'Amazon EKS Anywhere', and 'Self-managed Kubernetes'. A 'Fulfillment option description' box contains the text: 'Deploy CN-Series on EKS and RedHat Openshift using Helm Chart'.

Fulfillment option	Supported services
Helm Chart	Amazon EKS Amazon EKS Anywhere Self-managed Kubernetes

Software version

Version1.2.2 (Nov 22, 2021)

Fulfillment option description

Deploy CN-Series on EKS and RedHat Openshift using Helm Chart

STEP 9 | [Continue to Launch (続行して起動)] をクリックします。

1. 起動ターゲット (Amazon が管理する **Kubernetes** または自己が管理する **Kubernetes**) を選択します。自己管理モードは、Redhat OpenShift にデプロイされます。
2. AWS Marketplace のリストに表示される起動手順に従ってください。この手順は、起動ターゲットによって異なります。

- **Amazon が管理する Kubernetes**

1. 起動手順のステップ 1 からコマンドをコピーします。
2. コピーしたコマンドを更新して、クラスター名を追加します。

--cluster<ENTER_YOUR_CLUSTER_NAME_HERE>

3. コピーしたコマンドをEKSクラスターで実行します。

Step 1: Create an AWS IAM role and Kubernetes service account

Use the following command to create an AWS IAM role and Kubernetes service account.

```
kubectl create namespace kube-system
eksctl create iamserviceaccount \
--name my-service-account \
--namespace kube-system \
```

 Copy

4. 起動手順のステップ 2 から Helm チャートコマンドをコピーします。
5. Helm のインストール情報を更新して、Panorama IP、Panorama 認証キー、デバイスグループ名、テンプレート名、および収集グループ名を含めます。**cluster.deployTo**を**eks**に設定します。

```
helm install cn-series-helm \
--namespace kube-system \
awsmp-chart/* \
--set serviceAccount.create=false \
--set serviceAccount.name=my-service-account \
--set cluster.deployTo=eks \
--set panorama.ip=Panorama-IP \
--set panorama.ip2=Panorama-IP2 \
--set panorama.authKey=000xxxxxxxx \
--set panorama.deviceGroup=Panorama-DG \
--set panorama.template=Panorama-TS \
```

```
--set panorama.cgName=Panorama-CG \
--set imagePullSecrets=awsmp-image-pull-secret
```

Step 2: Launch the software

Use the following commands to launch this software by installing a Helm chart on your Amazon EKS cluster.

```
export HELM_EXPERIMENTAL_OCI=1
aws ecr get-login-password \
--region us-east-1 | helm registry login \
--username AWS \
--password-stdin
```

6. 上記の値を更新した後、EKS クラスターにて helm install コマンドを実行します。
- セルフマネージド型 **Kubernetes**
 1. 起動手順のステップ 1を完了して、ライセンストークンと IAM ロールを作成します。

Step 1: Create a license token and IAM role

Choose **Create token** to generate a license token and AWS IAM role. These will be used to access the AWS License Manager APIs for billing and metering. You can use an existing token if you have one.

2. 起動手順のステップ 2からコマンドをコピーします。
3. コピーしたコマンドを更新して、トークン値を追加します。

AWSMP_TOKEN =<CREATE_TOKEN_ABOVE>

4. コピーしたコマンドを OpenShift クラスターで実行します。

Step 2: Save the token and IAM role as a Kubernetes secret

Use the following commands to save the license token and IAM role as a secret in the cluster. The secret will be used in a following step when launching the software.

```
kubectl create namespace kube-system
kubectl create serviceaccount my-service-account --namespace kube-system
AWSMP_TOKEN=<CREATE_TOKEN_ABOVE>
AWSMP_ROLE_ARN=arn:aws:iam::018147215560:role/service-role/AWSMarketplaceLicenseT
```

5. 起動手順のステップ 3から Helm チャートコマンドをコピーします。
6. Helmのインストール情報を更新して、Panorama IP、Panorama 認証キー、デバイスグループ名、テンプレートスタック名、および収集グループ名を含めます。cluster.deployToをopenshiftに設定します。

```
helm install cn-series-helm \
--namespace kube-system \
awsmp-chart/* \
--set serviceAccount.create=false
```

```
\ \ --set serviceAccount.name=my-service-account
  \ --set cluster.deployTo=eks|openshift \ --set
  panorama.ip=Panorama-IP \ --set panorama.ip2=Panorama-
  IP2 \ --set panorama.authKey=000xxxxxxxx
  \ --set panorama.deviceGroup=Panorama-DG
  \ --set panorama.template=Panorama-TS \
  --set panorama.cgName=Panorama-CG \ --set
  imagePullSecrets=awsmp-image-pull-secret
```

Step 3: Launch the software

Use the following commands to launch the software by installing a Helm chart from Amazon Elastic Container Registry (ECR).

```
export HELM_EXPERIMENTAL_OCI=1

aws ecr get-login-password \
  --region us-east-1 | helm registry login \
  --username AWS \
```

[Copy](#)

7. 上記の値を更新した後、OpenShift クラスターにてhelm installコマンドを実行します。

STEP 10 | ライセンスがアカウントに正常に追加されたことを確認します。

1. AWS License Manager に移動します。
2. **Granted Licenses** (付与されたライセンス)を選択し、CN-Series for AWS Marketplace のリストを見つけます。
3. **Entitlements** (資格)にて、ライセンスの総数と消費されたライセンスの数を確認できます。

Entitlements						
An entitlement is a right to use, access, or consume an application or resource.						
Name	Value	Max count	Usage	Units	Overages	Allow check in
vCPU	-	1000	5	Count	Not Allowed	Allowed
AWS::Marketplace::Usage	Enabled	-	-	None	-	Not Allowed

STEP 11 | CN-Series ファイアウォールが Panorama に表示されることを確認します。

1. Panorama にログインします。
2. CN-MGMT ポッドを表示するには、**Panorama** > 管理対象デバイス > サマリーを選択します。

DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address		VARIABLES	TEMPLATE	DEVICE STATE
					IPV4	IPV6			
mp1 pan-mgmt-sts-0		PA-CTNR		8050	10.12.0.17		Create	vRP-gke5-ts	Connected
mp2 pan-mgmt-sts-1				8661	10.12.2.20		Create	vRP-gke5-ts	Connected

3. CN-NGFW ポッドにライセンスが付与されていることを確認するには、**Panorama** > プラグイン > **Kubernetes** > ライセンス使用状況を選択し、各ポッドにライセンストークンが割り当てられていることを確認します。

NODE ID	FIREWALL POD NAME	LICENSE STATUS	NODE STATUS
rr-cluster-1 (3 Nodes, 3/3 Licensed)			
rr-cluster-1-default-pool-e2d3de37-1j1z	pan-ngfw-ds-4dfb	<input checked="" type="checkbox"/>	Successfully licensed. Created at: 06-11 22:30:37 UTC
rr-cluster-1-default-pool-e2d3de37-xhq5	pan-ngfw-ds-z5z8k	<input checked="" type="checkbox"/>	Successfully licensed. Created at: 06-11 22:30:37 UTC
rr-cluster-1-default-pool-e2d3de37-jn8z	pan-ngfw-ds-vr8hx	<input checked="" type="checkbox"/>	Successfully licensed. Created at: 06-11 22:30:36 UTC

CN-Series ファイアウォールを AliCloud (ACK) に Kubernetes サー ビスとしてデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none">• CN-Seriesデプロイメント	<ul style="list-style-type: none">• CN-Series 10.1.x or above Container Images• PanoramaPAN-OS 10.1.xまたはPAN-OS 10.2.xバージョンを実行している

[CNシリーズ コアビルディング ブロック](#)と[CNシリーズ ファイアウォールによるKubernetesの安全なワークフロー](#)による[Kubernetesの安全なワークフロー](#)の概要を確認したら、同じクラスタ内のコンテナ間やコンテナと他のワークフロー タイプ(仮想マシンやベアメタル サーバーなど)間のトラフィックを保護するためのCNシリーズ ファイアウォールのデプロイから始めることができます。

`plugin-serviceaccount.yaml` ファイルを確実に適用する必要があります。詳細については、「[クラスタ認証用サービスアカウントの作成](#)」を参照してください。



- CN-Series ファイアウォールを *Kubernetes* サービスとして ACK にデプロイする場合、`pan-plugin-cluster-mode-secret` が存在する必要があります。

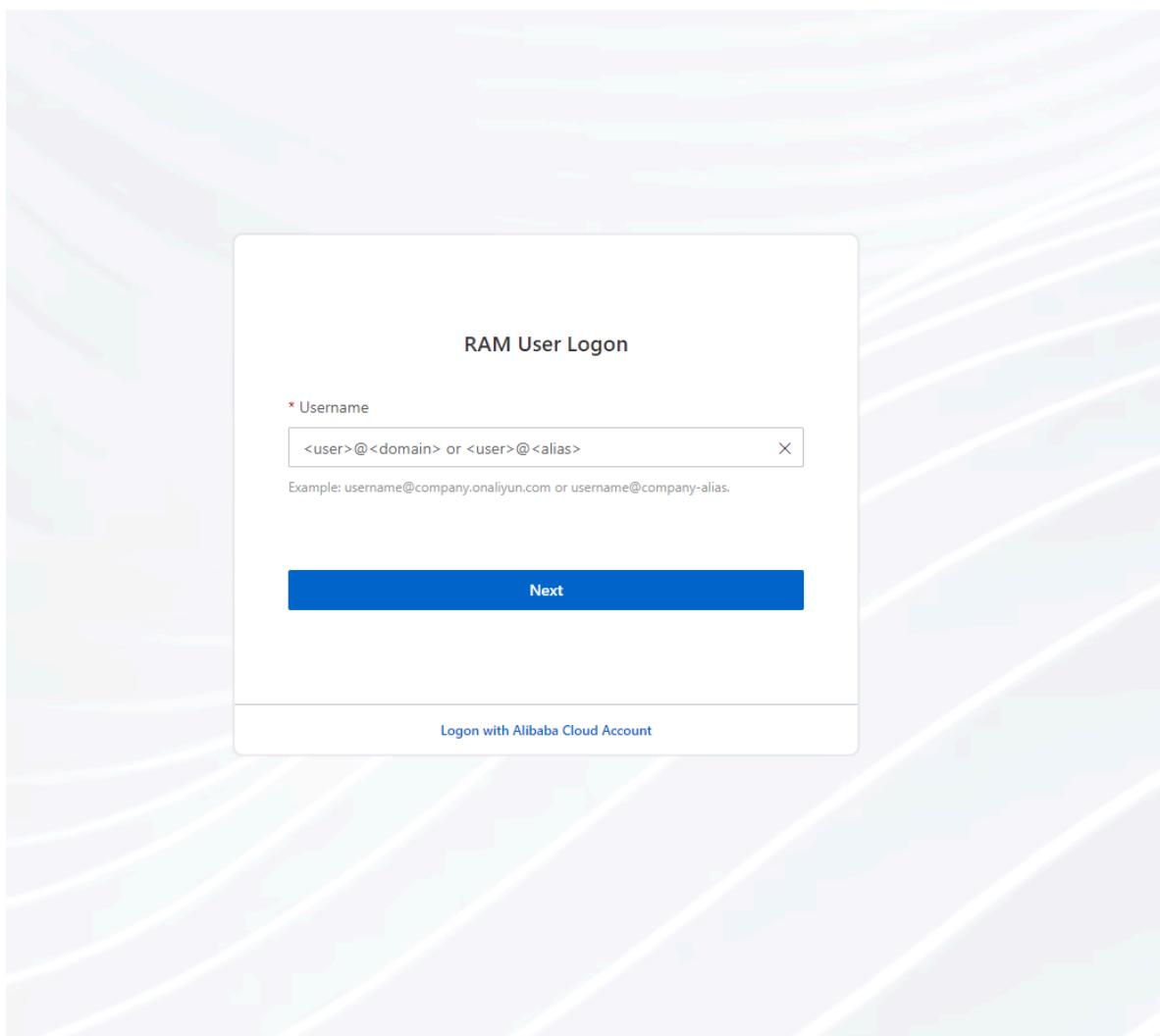
開始する前に、CN-Series YAML ファイルのバージョンが PAN-OS バージョンと互換性があることを確認します。詳細については、[CN-Series YAML](#)を参照してください。

以下の手順を実行して、CN-Series ファイアウォールを Kubernetes サービスとして ACK プラットフォームにデプロイします。

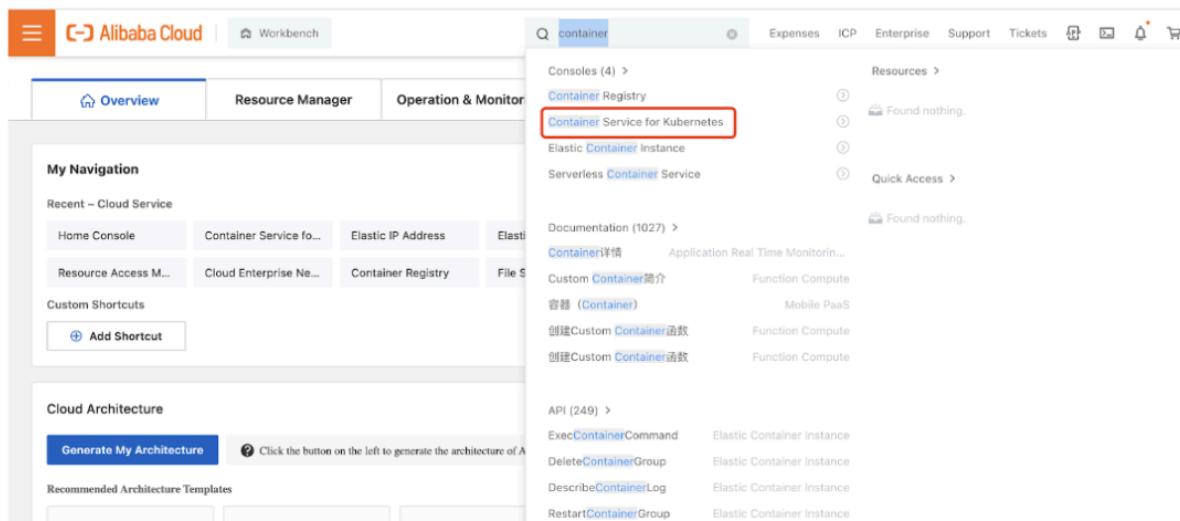
STEP 1 | Kubernetes クラスタをセットアップします。

ACKでクラスタを作成するには、次のようにします。

1. RAMログイン資格情報を使用して[RAM User Logon \(RAMユーザーログオン\)](#)にログオンします。



- 上部のナビゲーションバーで、クラスタを作成するリージョンを選択し、ビジネス要件に基づいてリソースグループを選択します。
 - クラスタのリージョンは、クラスタの作成後に変更できません。
 - デフォルトでは、アカウント内のすべてのリソースグループが表示されます。
- 検索バーで**Container Service for Kubernetes (Kubernetes向けコンテナサービス)**を検索します。



- [Create Kubernetes Cluster (Kubernetesクラスタの作成)]をクリックします。

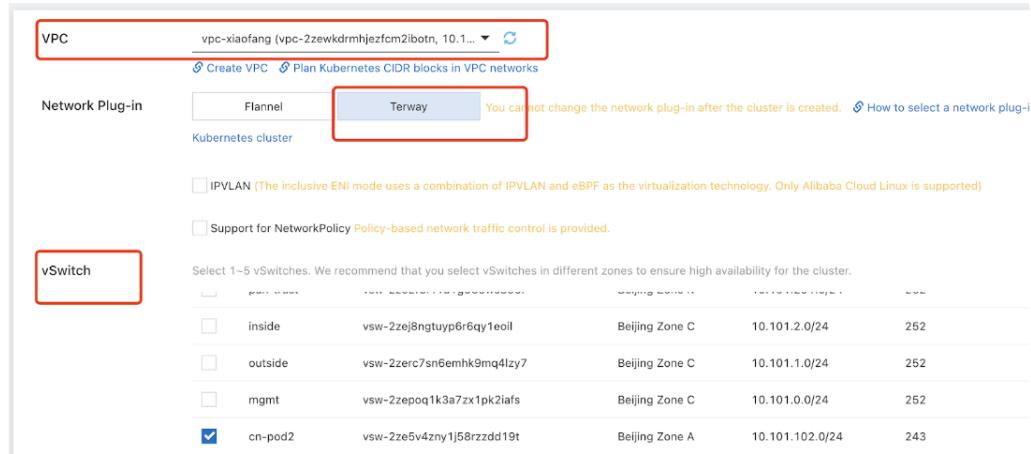
The screenshot shows the Alibaba Cloud Container Service ACK Clusters page. The left sidebar is for Container Service ACK, with 'Clusters' selected. The main area is titled 'Clusters' and shows a table with one item: 'ACK-For-PM'. The table columns include Cluster Name/ID, Labels, Type, Region, Cluster Status, Nodes, Usage, Created At, Version, and Actions. The 'Actions' column for the first item has options like 'Details', 'Applications', 'View Logs', 'Migrate to Pro', 'Node Pools', and 'More'. At the top right of the main area, there are buttons for 'View Cluster and Node Quotas', 'Refresh', 'Cluster Templates', and 'Create Kubernetes Cluster'. The 'Create Kubernetes Cluster' button is highlighted with a red box and an arrow pointing to it.

5. クラスタを作成するには、ウィザードの指示に従ってソフトウェアパラメータ、ハードウェアパラメータ、および基本パラメータを設定する必要があります。これらの必須パラメータの設定の詳細については、「[Create a Cluster on ACK \(ACKでクラスタを作成する\)](#)」

を参照してください。次の手順は、ACKプラットフォームでのクラスタ作成のサンプルを示しています。

 *CN-Series on Alibaba cloud ACK*は、*Terway Network*プラグインのみをサポートしています

- **[VPC]**、**[Network Plugin (ネットワークプラグイン)]**、**[vSwitch]**を選択します。



- **[POD v Switch]** を選択します。

Pod vSwitch

	All	ZoneA (2 / 1)			
<input type="checkbox"/>	inside	vsw-2zej8ngtuyp6qy1eoil	Beijing Zone C	10.101.2.0/24	252
<input type="checkbox"/>	outside	vsw-2zerc7sn6emhk9mq4lzy7	Beijing Zone C	10.101.1.0/24	252
<input type="checkbox"/>	mgmt	vsw-2zepoq1k3a7zx1pk2iafs	Beijing Zone C	10.101.0.0/24	252
<input checked="" type="checkbox"/>	cn-pod2	vsw-2ze5v4zny1j5brzzdd19t	Beijing Zone A	10.101.102.0/24	252
<input checked="" type="checkbox"/>	cn-pod1	vsw-2zex1z33iu6ffu72ko5ry	Beijing Zone A	10.101.101.0/24	252
<input type="checkbox"/>	cn-node-ip	vsw-2ze5nzjrkzio4sbf6d2n9	Beijing Zone A	10.101.10.0/24	252

[Create vSwitch](#)

The prefix length of the VSwitch address is recommended to be no greater than 19 bits.

Service CIDR

192.168.0.0/16	<input checked="" type="checkbox"/> Recommended Value: 192.168.0.0/16
----------------	---

Valid values: 10.0.0.0/16-24, 172.16-31.0.0/16-24, and 192.168.0.0/16-24.

- [Configure SNAT (SNATを設定)]、[Access to API Server (APIサーバーへアクセス)]、[Security Groups (セキュリティグループ)]、[Resource Group (リソースグループ)]を選択します。

Configure SNAT Configure SNAT for VPC
Nodes and applications in the cluster have Internet access. If the VPC that you select has a NAT gateway, ACK uses this NAT gateway to enable Internet access. If the VPC does not have a NAT gateway, ACK automatically creates a NAT gateway and configures SNAT rules. For more information, see [NAT Gateway](#).

Access to API Server [SLB Instance Specifications](#)
By default, an intermediate SLB instance is created for the API server. You can modify the specification of the SLB instance. If you delete the SLB instance, the API server is still accessible.

Expose API Server with EIP
If you select this check box, the internal-facing SLB instance is associated with an EIP. This allows you to access the API server of the cluster over the Internet.

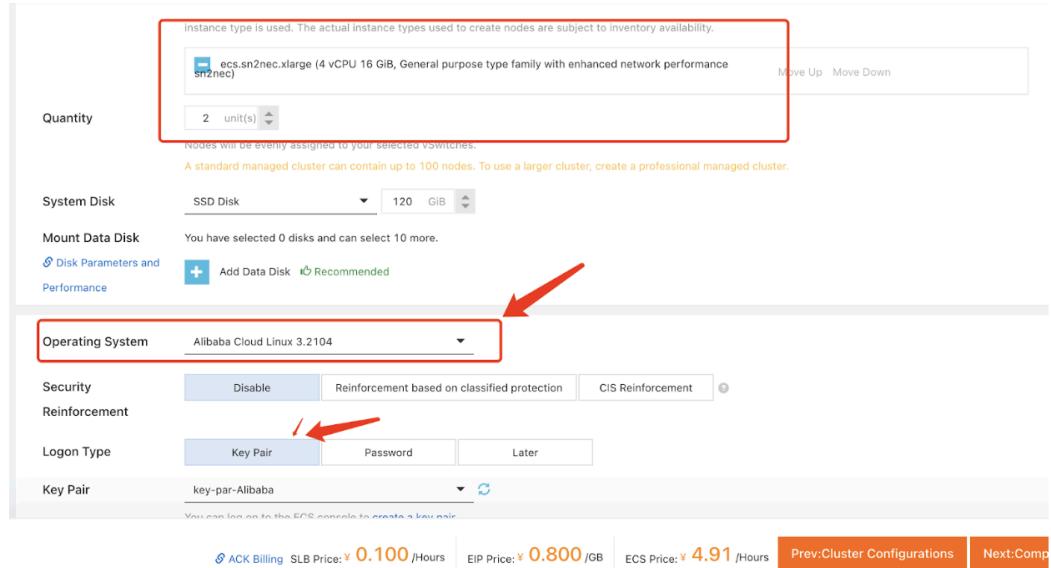
RDS Whitelist [Select RDS Instance](#)
We recommend that you go to the RDS console to add the CIDR blocks of the specified nodes and specified pods to a whitelist of the RDS instance. (The RDS instance is not in the running state, the node pool cannot be scaled out.)

Security Group [Create Basic Security Group](#) [Create Advanced Security Group](#)
To use a basic security group, the total number of pods in the cluster cannot exceed 2,000 if you select the Terway network plug-in. Otherwise, you must use an advanced security group. [Security group overview](#)

Deletion Protection Enable
Cluster Cannot Be Deleted in Console or by Calling API

Resource Group [default resource group](#) [Create](#)
To create a resource group, click [here](#).

- [Quantity (数量)]、[Operating System (オペレーティングシステム)]を選択し、次に[Node Pool Configurations (ノードプール構成)]の[Logon Type (ログオンタイプ)]を選択します。



- [Public Network (パブリックネットワーク)]タブに移動し、[Service Discovery (サービス検出)]、[Volume Plug-in (ボリュームプラグイン)]、[Monitoring Agents (監視エージェント)]のチェックボックスをオフにします。

Cluster Configurations Node Pool Configurations Component Configurations

Ingress: Nginx Ingress

SLB Network Type: Public Network

SLB Specifications: slb.s1.small

Service Discovery: Install NodeLocal DNSCache

Volume Plug-in: CSI

Monitoring Agents:

- Install CloudMonitor Agent on ECS Instance Recommended
- Enable Prometheus Monitoring Recommended Pricing Details

ACK Billing: SLB Price: 0.800 GB

EIP Price: 0.800 /GB

ECS Price: 4.91 /Hours

Prev:Node Pool Configu

6. 利用規約のチェックボックスを選択します。

The screenshot shows a step in the AliCloud ACK cluster creation process. At the top, a table lists several pre-deployment checks with 'Passed' results. Below this, a section titled 'Terms of Service' contains a list of actions performed during cluster creation and a checkbox for accepting the terms. The checkbox is checked, and the text indicates that resources will be charged if creation fails. At the bottom, there are price details for ACK Billing, SLB Price, EIP Price, and ECS Price, along with a 'Prev: Component Configurations' button.

RAM Role Authorization Check	Passed
Dependent Service Activation Status	Passed
Auto Scaling Status Check	Passed
Service Quota Check	Passed
System Disk Size Check	Passed
Data Disk Size Check	Passed
Account Balance Check	Passed

*** Terms of Service**

During the cluster creation process, the following operations may be performed depending on cluster configurations:

- Create ECS instances, configure a public key to enable SSH logon from master nodes to other nodes, and configure the Kubernetes cluster through CloudInit.
- Create a security group that allows access to the VPC network over ICMP.
- Create VPC routing rules.
- Create a NAT gateway and Elastic IP addresses.
- Create a RAM role and grant it the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and all permissions on SLB instances, CloudMonitor, VPC, Log Service, and NAS. The Kubernetes cluster dynamically creates SLB instances, cloud disks, and VPC routing rules based on your settings.
- Create an internal SLB instance and open port 6443.
- When you use a dedicated or managed Kubernetes cluster, the system collects log and monitoring information about control components on master nodes to help ensure cluster stability.

If the cluster creation fails, the created resources will be charged. We recommend that you delete unused resources at the earliest opportunity.

I have read and understand the preceding statement. I also have read and accept the [Terms of Service](#) and [Disclaimer](#).

ACK Billing: 0.220 Hours | SLB Price: 0.800 | EIP Price: 0.800 /GB | ECS Price: 4.91 /Hours | Prev: Component Configurations

7. [クラスタの作成]をクリックします。
8. API server KeyをチェックしてACKクラスタにログインし、以下のコンテンツをローカルコンピュータの\$HOME / . kube/configにコピーします。

Cluster Information

ACK-For-PM

Connection Information

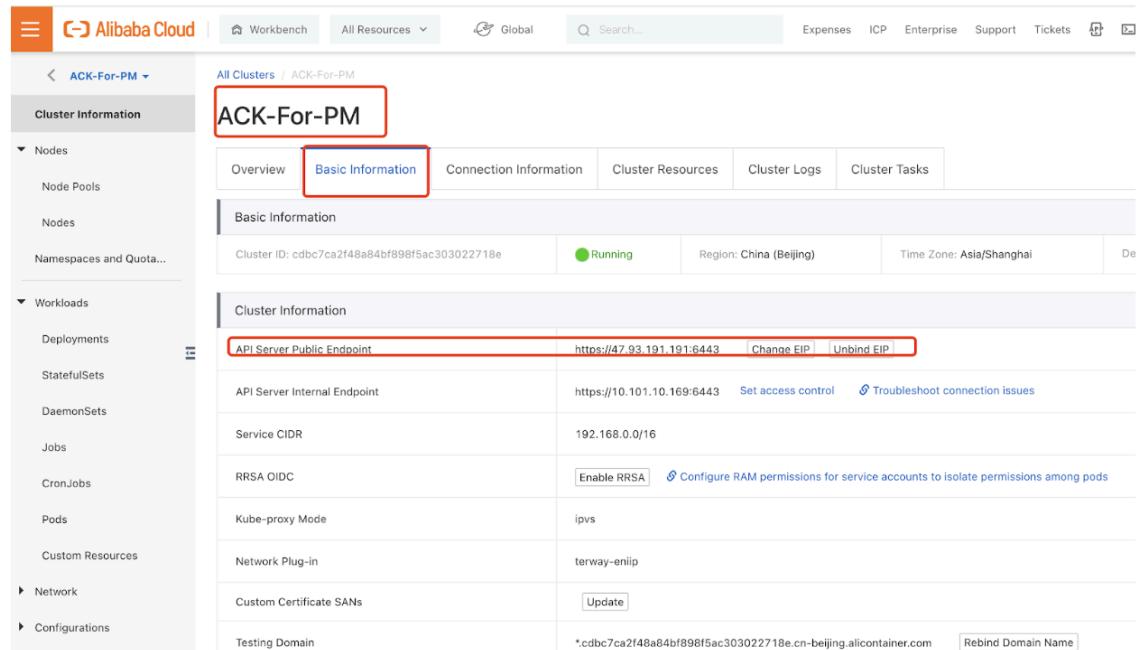
Public Access

Copy

```

apiVersion: v1
clusters:
- cluster:
    server: https://47.93.191.191:6443
    certificate-authority-data:
    LS0tLS1CR0dT1lDRVJUSUZJQ0FRS0tLS0tck1JSURUaKNDQWhpZ0F3SUJBZ0lVRDU1NDJtTmRRYmlIeThtQ3ByQnhLQlU3RX1zd0RNUpLb1pJaH2jTkFRRUwFQ1FBd1BgRW5NQThNC
    TTVRUNoTUhr0Z1WjNwb2IzVxdGQ1EV1FRS0V3MWhiR2xpVdKaElNTnNiM12rTVJNdpFUV1EV1FREV3cHJXpOpY201bGRHVnpNQ0YFRFJek1ERXdOakExTwpnd01gb1Eek13T1
    Rje1sQTVNRPV5c3PEQXaKetTNj0d83WUWUVEFLRXdob1lXNW1lWh2ZFRBVUJnT1ZCQWQURFdgC2FXshzb1VnWV4dnXUXgRxpBukJn1lCQU1UQ210W1tVn1l1VwVwWhhd2c
    nRW1nQTBBQ1NxR1nJYjNEUUVCQYFVQUE0S1J8dF322dFSwpBb01CQ/FEOGoxczYYVQvTn1xdB1dk1oJUERnmaCOKBxayjJ4VHb32lFUTz2dFnWU00CtNS2JmDnV9d1c1lyYUd
    akFhQVVVZGHPCTBNak1lB2xpU1RgOTBLRnQyznV2EUVRKEu1p5WE11U1xBpczVMR1hYVmIxR0oKNjV8WjRgQ2k0QxVycI4SjJVBu0jyVtBrsWxR2VQ0LyjyU1VZ0aR5KUjhx
    M11URhJ1An1reApkrBN11r1rNp2QKfJ1n0dRnRvvn1wSu0yDe1SSUGtNCJN51Kx1nCDAK3R0XSmuvaZea1uScVhTRG41aRHKYjMrR31FU21SC1F0d8E3R0FORw51T21z1F2BwZnZ2S
    k1Ou3nFSEFWGmZX9V9Ra1H121C1os1v1d1dwk1k1lQW0W0x2yv0dRtY2oYnYX1.25.5aUR0Rk1xN0deYn7.1kXV3.3.3MSOVtVt2ht5kPm7U1b0ndd0U0cCm11BNRd4BmVvV8RdP0i9uunnd01oex
  
```

9. ACKクラスタAPIサーバのパブリックエンドポイントアドレスを取得します。



The screenshot shows the Alibaba Cloud Workbench interface for managing Kubernetes clusters. The left sidebar shows the cluster navigation, and the main area displays the 'Basic Information' tab for the 'ACK-For-PM' cluster. The 'API Server Public Endpoint' is highlighted with a red box. The table below provides detailed configuration information for the cluster.

Setting	Value	Actions
API Server Public Endpoint	https://47.93.191.191:6443	Change EIP Unbind EIP
API Server Internal Endpoint	https://10.101.10.169:6443	Set access control Troubleshoot connection issues
Service CIDR	192.168.0.0/16	
RRSA OIDC	Enable RRSA Configure RAM permissions for service accounts to isolate permissions among pods	
Kube-proxy Mode	ipvs	
Network Plug-in	terway-enip	
Custom Certificate SANs	Update	
Testing Domain	*.cdbc7ca2f48a84bf898f5ac303022718e.cn-beijing.alicontainer.com	Rebind Domain Name

Cluster Name/ID	Labels	Type	Region	Cluster Status	Nodes	Usage	Created At	Version	Actions
ACK-For-FM cdbc7ca2f48a84bf898f5ac303022718e		ACK Managed	China (Beijing)	Running	2	CPU: 1% Memory: 19%	Jan 6, 2023, 13:32:51 UTC+8	1.24.6- aliyun.1	Details Applications View Logs Migrate to Pro Node Pools More

クラスタのリソースが適切であることを確認します。デフォルトのGKE ノードプール仕様は、CN-Series ファイアウォールには適していません。クラスタにファイアウォールをサポートするためのCN-Series前提条件リソースがあることを確認する必要があります。

kubectl get nodes

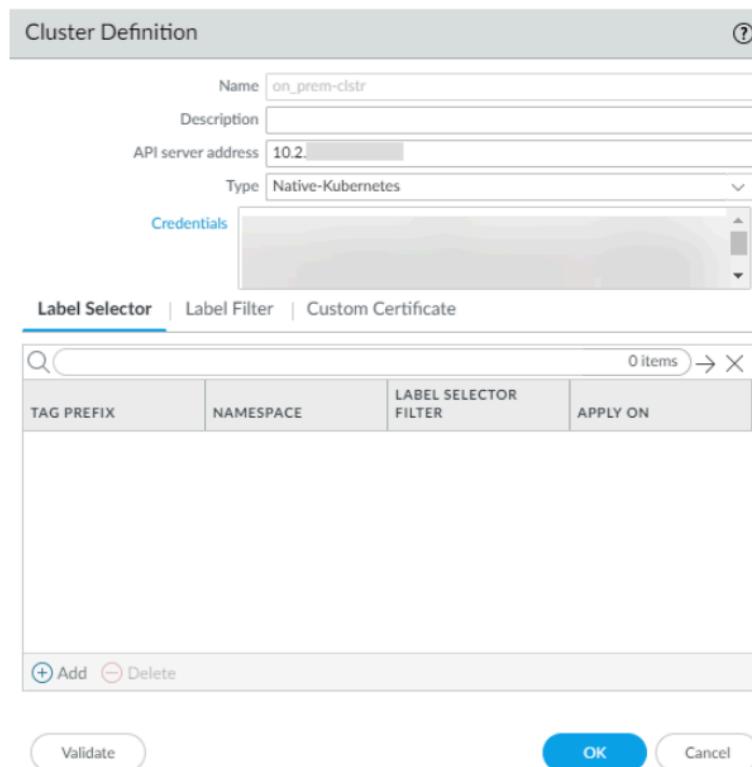
kubectl describe node <node-name>

コマンド出力の[容量]見出しの下にある情報を表示して、指定したノードで使用可能な CPU とメモリーを確認します。

CPU、メモリ、およびディスクストレージの割り当てはニーズによって異なります。CN-Seriesのパフォーマンスとスケーラビリティを参照してください。

次の情報があることを確認する必要があります。

- PanoramaにAPI サーバーを設定するためのエンドポイント IP アドレスを収集します。



Panorama は、この IP アドレスを使用して、Kubernetes クラスタに接続します。

- テンプレートスタック名、デバイス グループ名、Panorama IP アドレス、およびオプションで ログ コレクタグループ名をPanorama から収集します。
詳細については、[親デバイス グループとテンプレート スタックの作成](#)を参照してください。
- [VM 認証キーと自動登録の PIN ID と値](#)を収集します。
- イメージをダウンロードしたコンテナ イメージ リポジトリの場所。

STEP 2 | (任意) Panorama の Kubernetes プラグインでカスタム証明書を設定した場合は、次のコマンドを実行して証明書シークレットを作成する必要があります。ファイル名を ca.crt から変更しないでください。pan-cn-mgmt.yaml および pan-cn-ngfw.yaml のカスタム証明書のボリュームはオプションです。

kubectl -n kube-system create secret generic custom-ca --from-file = ca.crt

STEP 3 | YAML ファイルを編集して、CN-Series ファイアウォールをデプロイするために必要な詳細を記入します。

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-config
  namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-
  svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings
  PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-
  device-group>" PAN_TEMPLATE_STACK: "<panorama-template-stack>" PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8s-
  service"
```

```
apiVersion: v1 kind:Secret metadata: name: pan-mgmt-secret
  namespace: kube-system type:Opaque stringData: # Panorama Auth
  Key PAN_PANORAMA_AUTH_KEY: "<panorama-auth-key>" # Thermite
```

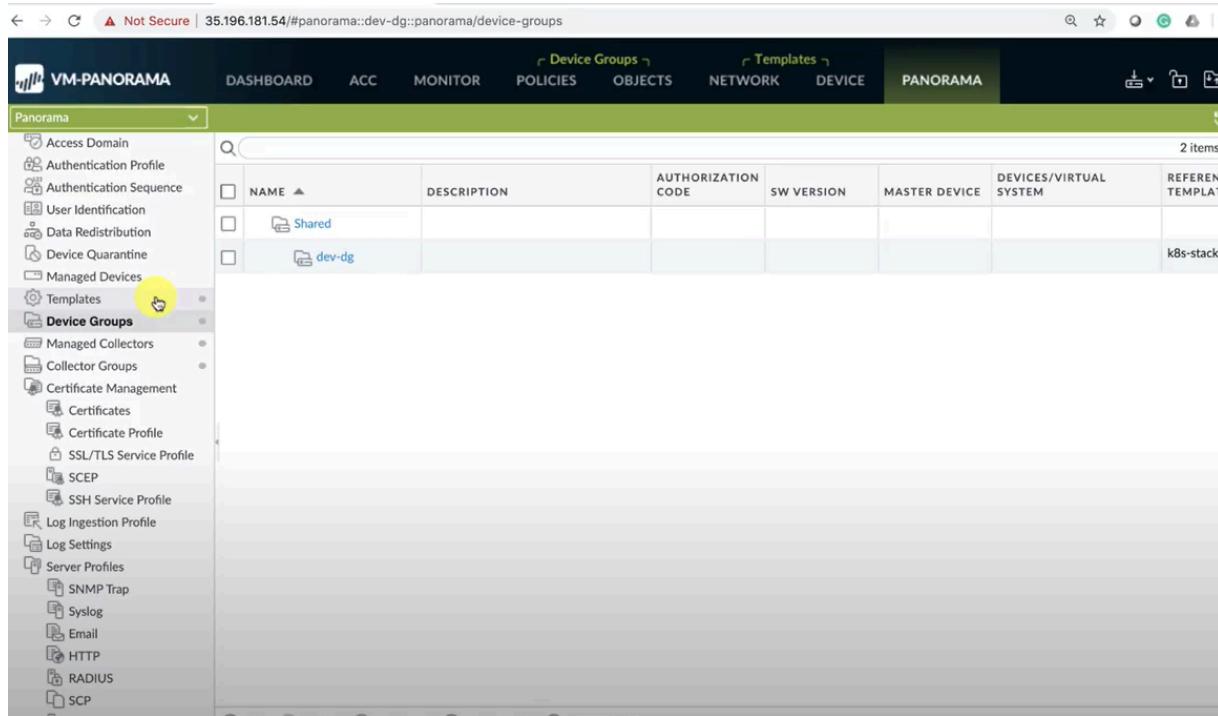
```
Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN
Id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<PIN-Value>"
```

以下の図に示すように、YAML ファイルの PAN_PANORAMA_IP パラメータの値が実際の Panorama IP アドレスと一致していることを確認する必要があります。

NAME	DESCRIPTION	TYPE	STACK	DEVICES	VARIABLES	DEVICE KEY-VALUE TA
K8S-Network-Setup		template			Manage...	No Devices in the stack
k8s-stack		template-stack	K8S-Network-Setup		Manage...	No Devices in the stack

 YAML ファイルの最新バージョンは、[Palo Alto Networks Kubernetes Security のリポジトリ - CN Series](#) で入手できます。「Switch branches/tags (分岐/タグの切り替え)」ドロップダウンメニューから、最新の分岐またはタグを選択できます。

以下の図に示すように、YAML ファイルの PAN_DEVICE_GROUP と PAN_TEMPLATE のパラメータ値が、Panorama で作成したデバイスグループとテンプレートスタックの名前と一致していることを確認する必要があります。



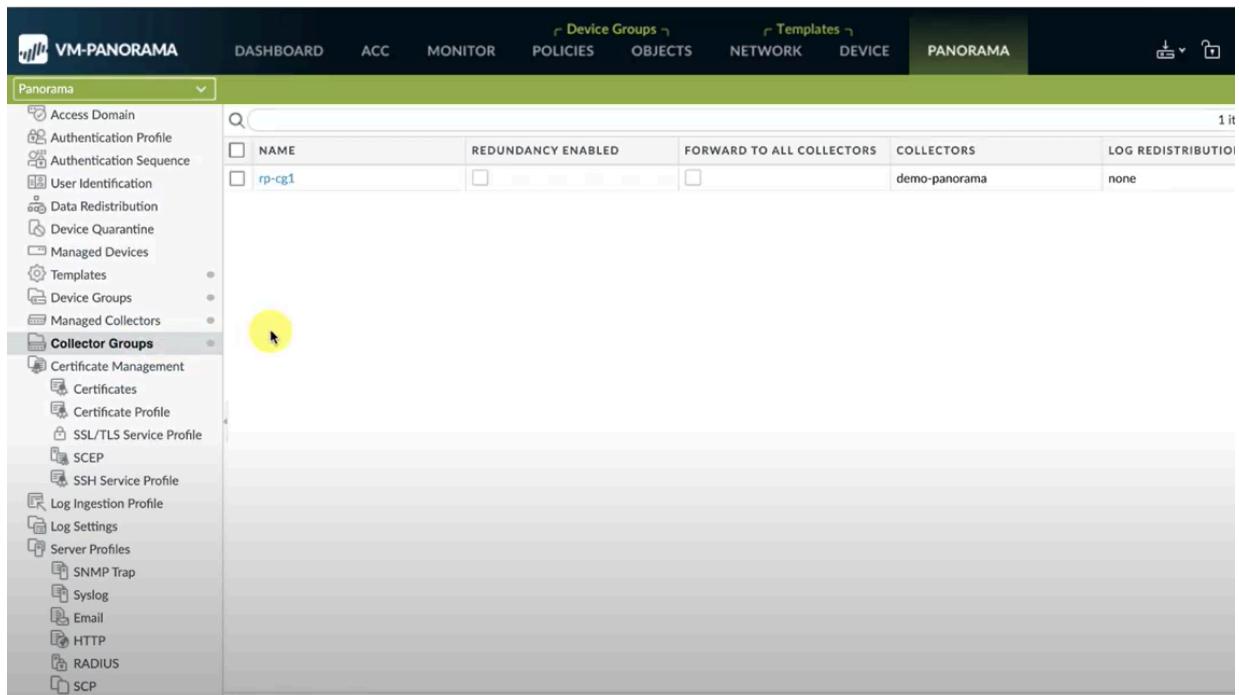
VM-PANORAMA

PANORAMA

Device Groups

NAME	DESCRIPTION	AUTHORIZATION CODE	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM	REFERENCE
Shared						
dev-dg						k8s-stack

PAN_PANORAMA(CG_NAME) のパラメータ値が、作成したログコレクターネームと同じであることを確認する必要があります。



VM-PANORAMA

PANORAMA

Collector Groups

NAME	REDUNDANCY ENABLED	FORWARD TO ALL COLLECTORS	COLLECTORS	LOG REDISTRIBUTION
rp-cg1			demo-panorama	none

詳細については、CN-Seriesの[yamlファイルの編集可能なパラメータ](#)を参照してください。

STEP 4 | CN-NGFW サービスをデプロイします。次の手順を実行します。

Kubernetes サービスとしてデプロイすると、CN-NGFW のインスタンスをセキュリティノードにデプロイでき、アプリケーションポッドトラフィックは、検査と執行のために利用可能な CN-NGFW インスタンスにリダイレクトされます。

1. pan-cni-serviceaccount.yaml を使用してサービス アカウントが作成されたことを確認します。

[クラスタ認証用のサービスアカウントの作成](#)を参照してください。

2. Kubectl を使用して pan-cni-configmap.yaml を実行します。

kubectl apply -f pan-cni-configmap.yaml

3. kubectl を使用して pan-cn-ngfw-svc.yaml を実行します。

kubectl apply -f pan-cn-ngfw-svc.yaml



この yaml は pan-cni.yaml の前にデプロイする必要があります。

4. Kubectl を使用して pan-cni.yaml を実行します。

kubectl apply -f pan-cni.yaml

5. pan-cni-configmap YAML ファイルと pan-cni YAML ファイルが変更されたことを確認します。

6. 以下のコマンドを実行して、出力が以下の例のようになっていることを確認します。

```
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v1.22.10-20230726T1045Z-001) [pan-cni-nmqkf] [pan-cni-wjrkq] [pan-cni-xrc2z] @cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v1.22.10-20230726T1045Z-001) [series-mktplace] $ kubectl get pods -n kube-system | grep pan-cni
  Running 0          2m11s
  Running 0          2m11s
  Running 0          2m12s
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v1.22.10-20230726T1045Z-001) [series-mktplace] $
```



AliCloud ACKは標準メトリックベースのオートスケーリングのみをサポートしています。

STEP 5 | CN-MGMT StatefulSet をデプロイします。

デフォルトで、管理プレーンは耐障害性を提供する StatefulSet としてデプロイされます。1 つの CN-MGMT StatefulSet に最大 30 個のファイアウォール CN-NGFW ポッドを接続できます。

1. (静的にプロビジョニングされた PV のみに必要) CN-MGMT StatefulSet 用の永続ボリューム (PV) をデプロイします。

1. pan-cn-pv-local.yaml で定義されたローカル ボリューム名と一致するディレクトリを作成します。

少なくとも 2 つのワーカー ノード上に 6 つのディレクトリが必要です。CN-MGMT StatefulSet をデプロイする各ワーカー ノードにログインして、ディレクトリを作成

します。たとえば、/mnt/pan-local1～/mnt/pan-local6 のディレクトリを作成するには、次のコマンドを実行します。

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /  
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. pan-cn-pv-local.yaml を変更します。

nodeaffinity の下でホスト名を一致させ、上記で `spec.local.path` に作成したディレクトリが変更されたことを確認してから、そのファイルをデプロイして、新しいストレージクラス `pan-local-storage` とローカル PV を作成します。



`pan-cn-mgmt.yaml` ファイルでは、`volumeClaimTemplates` の作成時にストレージクラス名を `alicloud-disk-available` として追加する必要があります。

以下に例を示します。

```
storageClassName: alicloud-disk-available
```

収納サイズは、すべての PV で 20G 以上が必要です。

2. `pan-cn-mgmt-configmap` YAML ファイルと `pan-cn-mgmt` YAML ファイルが変更されたことを確認します。

`pan-cn-mgmt.yaml` のサンプル

```
initContainers: - name: pan-mgmt-init image: <your-private-  
registry-image-path>
```

```
containers: - name: pan-mgmt image: <your-private-registry-  
image-path> terminationMessagePolicy: FallbackToLogsOnError
```

3. Kubectl を使用して yaml ファイルを実行します。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml  
kubectl apply -f pan-cn-mgmt-slot-crd.yaml  
kubectl apply -f pan-cn-mgmt-slot-cr.yaml  
kubectl apply -f pan-cn-mgmt-secret.yaml  
kubectl apply -f pan-cn-mgmt.yaml
```

`pan-mgmt-serviceaccount.yaml` は、[クラスター認証用のサービスアカウントの作成](#)を以前に完了していない場合にのみ実行する必要があります。

4. 次のコマンドを実行して、CN-MGMT ポッドが起動していることを確認します。

```
kubectl get pods -l app=pan-mgmt -n kube-system
```

これには、5～6分かかります。

STEP 6 | CN-NGFW ポッドをデプロイします。

1. PAN-CN-NGFW-CONFIGMAP と PAN-CN-NGFW に詳述されているように YAML ファイルが変更されたことを確認します。

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

2. Kubectl apply を使用して pan-cn-ngfw-configmap.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. Kubectl apply を使用して pan-cn-ngfw.yaml を実行します。

```
kubectl apply -f pan-cn-ngfw.yaml
```

4. CN-NGFW ポッドがデプロイされたことを確認します。

```
kubectl get pods -n kube-system -l app=pan-ngfw -o wide
```

STEP 7 | Kubernetes クラスタ上の CN-MGMT、CN-NGFW、および PAN-CNI が表示されていることを確認します。

```
kubectl -n kube-system get pods
```

STEP 8 | 新しいポッドからのトラフィックがファイアウォールにリダイレクトされるようにアプリケーション yaml または名前空間に注釈を付けます。

検査のためにトラフィックを CN-NGFW にリダイレクトするには、以下のアノテーションを追加する必要があります：

```
annotations: paloaltonetworks.com/firewall: pan-fw
```

たとえば、「default」名前空間のすべての新しいポッドの場合：

```
kubectl annotate namespace default paloaltonetworks.com/firewall=pan-fw
```

STEP 9 | クラスタでアプリケーションをデプロイします。

CN-Series を OpenShift にデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> CN-Series OpenShift環境へのデプロイメント 	<ul style="list-style-type: none"> CN-Series 10.1.x or above Container Images PanoramaPAN-OS 10.1.x以降のバージョンを実行している

pan-cni は、アプリケーション ポッドのデフォルトの "eth0" インターフェース上のトラフィックを保護します。マルチホーム ポッドを使用している場合は、ブリッジベースの接続を使用して他のポッドやホストと通信するように設定された追加のインターフェースを保護するように CN-NGFW ポッドを設定できます。アプリケーション YAML 内の注釈に応じて、各ポッドに関連付けられたすべてのインターフェースまたは選択された数のインターフェースからのトラフィックを検査するように CN-Series ファイアウォールを設定できます。

pan-cni は、ネットワークを作成しないため、他の CNI プラグインのように IP アドレスを必要としません。



OpenShift で CN-Series を Kubernetes サービスとしてデプロイするには、PAN-OS 10.1.3 以降が必要です。さらに、OpenShift 上の Kubernetes サービスとしての CN-Series は、インターフェース eth0 のみを保護します。

STEP 1 | クラスタをデプロイします。

クラウド プラットフォーム ベンダーのドキュメントを参照し、OpenShift のバージョンと CNI が CN-Series に対してサポートされていることを確認してください。[CN シリーズ ファイアウォールのイメージファイルを取得し、CN-Series yaml ファイルで編集可能なパラメータを確認します。](#)

STEP 2 | CN-Series を使用した Secure Kubernetes ワークフローに含まれるワークフローを使用します。

サービス認証情報を作成し、ファイアウォール YAML をデプロイします。



注:サービス認証情報ファイルが 10KB を超えている場合は、ファイルを gzip で圧縮し、圧縮したファイルの base64 エンコーディングを実施してから、ファイルの内容を Panorama CLI または API にアップロードまたは貼り付ける必要があります。

STEP 3 | Multus CNI プラグインと連動するように PAN-CNI プラグインを設定します。

OpenShift 上の Multus CNI は、他の CNI プラグインを呼び出す「メタプラグイン」として機能します。アプリケーションごとに、以下の作業を行う必要があります。

- すべてのポッド名前空間で PAN-CNI NetworkAttachmentDefinition をデプロイします。

```
kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>
```

- アプリケーション YAML を変更します。

pan-cni-net-attach-def.yaml をデプロイしたら、アプリケーション ポッド yaml に注釈を追加します。

```
paloaltonetworks.com/firewall: pan-fw
```

```
k8s.v1.cni.cncf.io/networks: pan-cni
```

上記注釈内に他のネットワークが含まれている場合は、検査する必要のあるネットワークの後ろに **pan-cni** を追加します。**pan-cni** の後ろのネットワークは、リダイレクトされず、検査されません。



ポッドに複数のネットワークインターフェースが含まれている場合は、*pan-cni-configmap.yaml* の "interfaces" の下で、CN-NGFW ポッドがトラフィックを検査する対象のインターフェース名を指定する必要があります。

以下に例を示します。

```
template: metadata: annotations: paloaltonetworks.com/
firewall: pan-fw k8s.v1.cni.cncf.io/networks: bridge-conf,
macvlan-conf, sriov-conf, pan-cni
```



CNシリーズはRedHat OpenShiftバージョン4.13以上で、Kubernetes ServiceデプロイモードとDaemonSetモードでOVN-Kubernetes Container Network Interface (CNI) プラグインをサポートするようになりました。

CN-Series を OpenShift にデプロイする

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> • CN-Seriesデプロイメント 	<ul style="list-style-type: none"> • CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.2.xバージョン以降を実行している

[CN-Seriesコンテナファイアウォール](#)が、[RedHat Openshiftプラットフォーム](#)のOperator Hubで利用できるようになりました。RedHat Operator Hubから直接CN-Seriesのコンテナファイアウォールを導入、設定、運用できます。

Openshift Operator HubでのCN-Seriesの前提条件。

OpenshiftオペレータハブにCN-Seriesファイアウォールを導入するための前提条件は次のとおりです。

- CN-Series ファイアウォールのライセンス取得CN-Series ファイアウォール ライセンスは、Kubernetes plugin on Panorama によって管理されます。CN-Series ファイアウォールをデプロイする準備ができたら、認証コードを生成し、手元に置いておきます。詳細については、「[License the CN-Series Firewall \(CN-Series ファイアウォールのライセンス\)](#)」を参照してください。
- Panorama で VM 認証キーを生成します。
- VM-Seriesファイアウォールへのデバイス証明書のインストール
- クラスタ認証用にサービスアカウントを作成する
- Panorama のデプロイ-CN-Series ファイアウォールのデプロイメントを設定、デプロイ、および管理するには、Panorama を使用する必要があります。Panorama アプライアンスのデプロイとセットアップの詳細については、[Panorama の設定](#)を参照してください。
- [CN-Seriesファイアウォール用のKubernetesプラグインをインストールします。](#)
- OpenShiftクラスタは、[CN-Series前提条件](#)に準拠している必要があります。
- [Palo Alto Networks Customer Service Portal \(CSP\)](#)へのアクセスがあり、[Flexクレジット](#)を取得していることを確認します。
- OpenShiftライセンスとOpenShiftでリソースを作成する権限を持つアカウントを持つRedHatの顧客であることを確認します。
- OpenShiftクラスタが[CN-Series前提条件](#)に準拠していることを確認します。

詳しくは、[RedHat Openshift Operator HubでCN-Seriesを簡単に導入する方法](#)をご覧ください。

OpenShift OperatorハブにCN-Seriesをデプロイする。

pan-cni は、アプリケーション ポッドのデフォルトの **eth0** インターフェース上のトラフィックを保護します。マルチホーム ポッドを使用している場合は、ブリッジベースの接続を使用して他のポッドやホストと通信するように設定された追加のインターフェースを保護するように CN-NGFW ポッドを設定できます。アプリケーション YAML 内の注釈に応じて、各ポッドに関連付けられたすべてのインターフェースまたは選択された数のインターフェースからのトラフィックを検査するように CN-Series ファイアウォールを設定できます。

pan-cni はネットワークを作成しないため、他の CNI プラグインのように IP アドレスを必要としません。



OpenShift OperatorハブにCN-Seriesを導入するには、PAN-OS 10.2以降が必要です。

Redhat OpenShiftオペレーター ハブにCN-Series ファイアウォールを導入する手順は、次のとおりです。

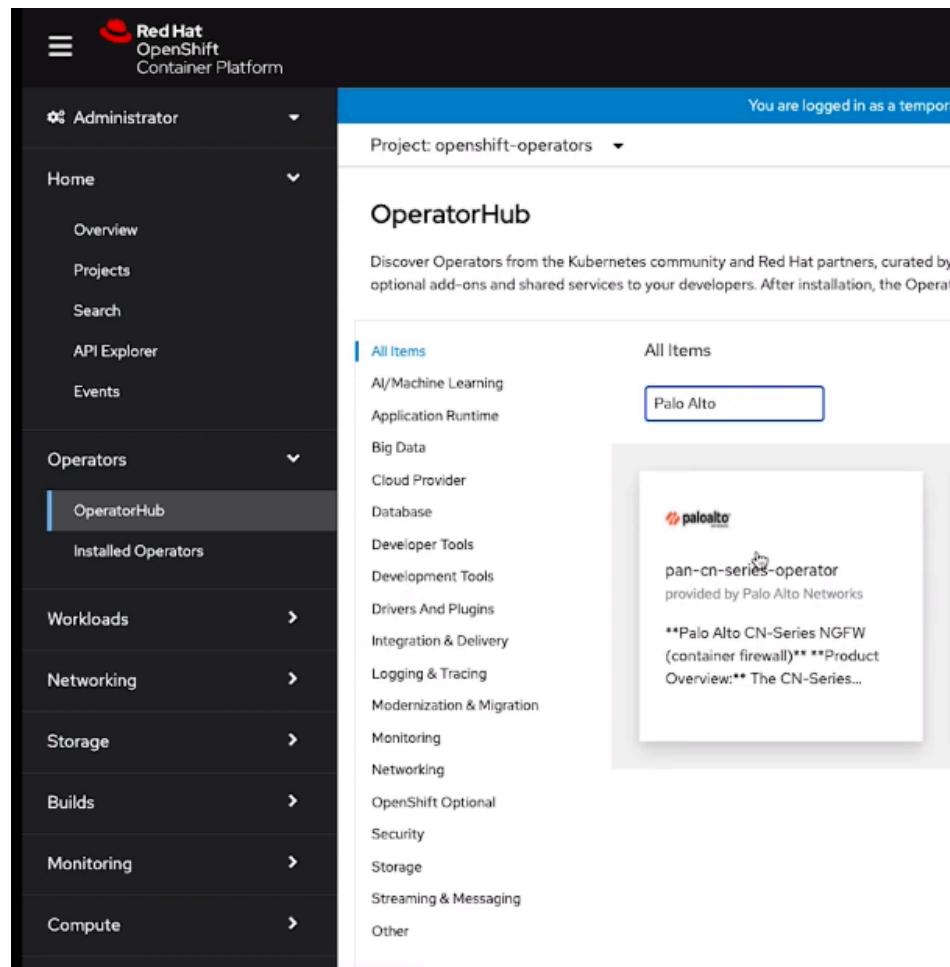
STEP 1 | Redhat OpenShiftコンテナコンソールにログインします。

STEP 2 | [Operators (オペレータ)]に移動し、[OperatorHub]をクリックします。

The screenshot shows the Red Hat OpenShift Container Platform interface. The left sidebar is open, showing categories like Home, Operators, Workloads, Networking, Storage, Builds, and Monitoring. Under Operators, 'OperatorHub' is selected. The main content area is titled 'Overview' and shows the 'Cluster' section. It includes 'Getting started resources' with links to 'Set up your cluster' and 'Build with guided documentation'. It also shows 'Status' with a green 'Cluster' icon, a green 'Control Plane' icon, a yellow 'Operators' icon (1 degraded), and a yellow 'Insights' icon (2 issues found). The 'Activity' section shows recent events: 'Recent events' (1 event: 'Stopping container registry...'), 'Update cluster' (1 event: 'A cluster version update is available'), 'View details' (1 event: 'Jan 18, 2022, 6:19 PM CredentialsRequest(s) unable to be fulfilled'), and 'View details' (1 event: 'Jan 14, 2022, 7:08 PM'). The top right corner shows the user is 'kube:admin'.

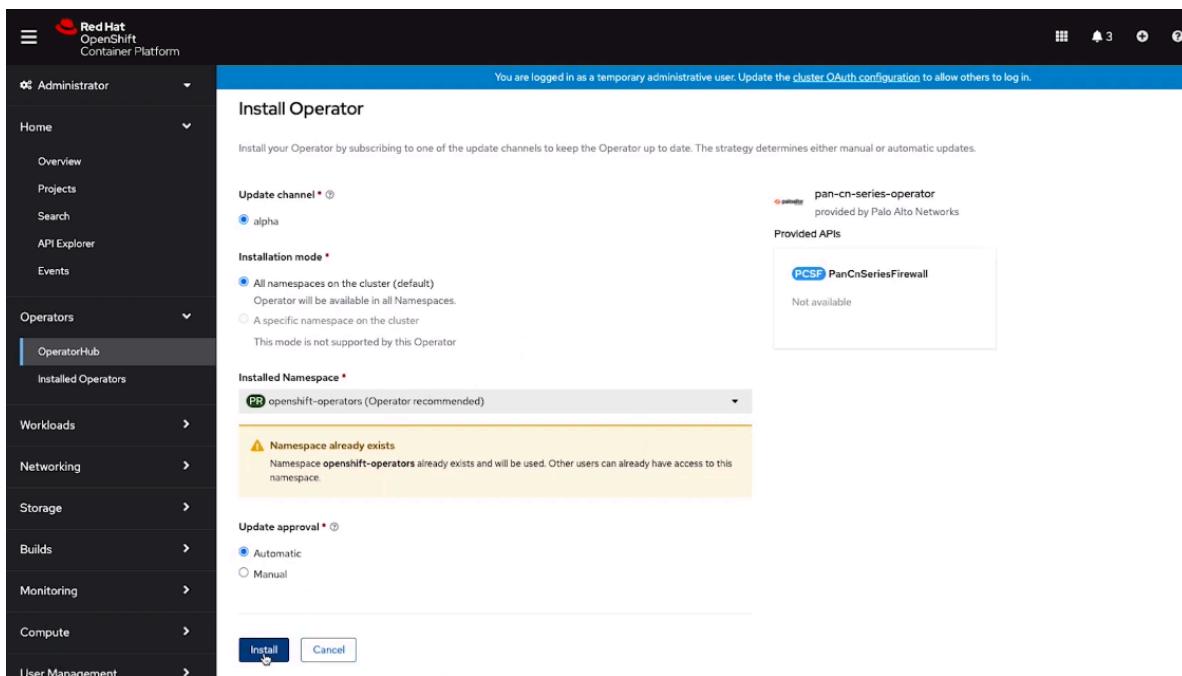
STEP 3 | [演算子]検索ボックスに「**Palo Alto**」と入力します。

STEP 4 | pan-cn-series-operator をクリックします。



pan-cn-series-operator タイルをクリックすると、インストールウィンドウが開きます。

STEP 5 | [Install (インストール)] をクリックして、OpenShiftクラスタにpan-cn-seriesオペレータをインストールします。



自 ここで示す次の展開手順の前に、[インストール前手順](#)を完了します。

自 サービス認証情報ファイルが 10KB を超えている場合は、ファイルを `gzip` で圧縮し、圧縮したファイルの `base64` エンコーディングを実施してから、ファイルの内容を *Panorama CLI* または *API* にアップロードまたは貼り付ける必要があります。

STEP 6 | 操作メニューで、[Installed Operators (インストール済オペレーター)]に移動し、インストールしたpan-cn-series-operatorをクリックします。

The screenshot shows the Red Hat OpenShift Container Platform interface. The left sidebar is titled 'Administrator' and includes 'Home', 'Overview', 'Projects', 'Search', 'API Explorer', 'Events', 'Operators' (selected), 'OperatorHub', and 'Installed Operators' (selected). The main content area is titled 'Installed Operators' and shows a table with one row. The row for 'pan-cn-series-operator' is highlighted with a blue border. The table columns are 'Name', 'Managed Namespaces', 'Status', 'Last updated', and 'Provided APIs'. The 'Name' column shows 'pan-cn-series-operator' with a small red icon. The 'Managed Namespaces' column shows 'All Namespaces'. The 'Status' column shows 'Succeeded' with a green circle icon and 'Up to date'. The 'Last updated' column shows '1 minute ago'. The 'Provided APIs' column shows 'PanCnSeriesFirewall'.

STEP 7 | Create Instance (インスタンスを作成) をクリックします。

The screenshot shows the Red Hat OpenShift Container Platform interface. The left sidebar is identical to the previous screenshot. The main content area shows the 'Details' tab for the 'PanCnSeriesFirewall' operator instance. The 'Provided APIs' section contains a box for 'PanCnSeriesFirewall' with a 'Not available' message and a blue 'Create instance' button. To the right, there is a 'Provider' section with 'Palo Alto Networks', a 'Created at' section with '1 minute ago', a 'Links' section with 'Pan Cn Series Operator' and a URL, and a 'Maintainers' section with 'Not available'. The 'Description' section contains a product overview and a list of 7 features. At the bottom, there is a note about deploying CN-Series as-a-Kubernetes service.

STEP 8 | 一意のオペランド名を入力します。

Project: openshift-operators

Name *: crosses-sample

Labels: app=frontend

Minimum Replicas for DP: 2

CPU Limit (DP): 1

Memory Limit (DP): 4.0Gi

CPU Limit (MP): 2

Memory Limit (MP): 3.0Gi

Secondary Panorama IP Address (Optional):

Secondary Panorama IP Address for HA deployment: vm-auth-key from Panorama

Customer Support Portal PIN ID (Optional):

Customer Support Portal PIN Value (Optional):

Customer Support Portal Value:

Customer Support Portal Alternate URL (Optional):

Customer Support Portal Alternate URL:

DP Image: gcr.io/pan-cn-series/panos_cn_ngfw

DP Image Version: preferred-10.2

MP Image: gcr.io/pan-cn-series/panos_cn_mgmt

MP Image Version: preferred-10.2

PAN CNI Image: gcr.io/pan-cn-series/pan_cni

PAN CNI Image Version: preferred

Create **Cancel**

STEP 9 | [Minimum Replicas for DP (DPの最小レプリカ数)]、[Memory Unit (メモリーユニット)]を入力し、DPとMPポッド用の[vCPU Limit]を入力します。vCPU の制限については、「[CN-Series Key Performance Metrics \(CNシリーズ主要パフォーマンス メトリクス\)](#)」を参照してください。

STEP 10 | Panorama IPアドレスを入力します。

Panorama Template Stack

Panorama Log Collector Group Name: <panorama-collector-group>

Customer Support Portal PIN ID (Optional):

Customer Support Portal PIN Value (Optional):

Customer Support Portal Value:

Customer Support Portal Alternate URL (Optional):

Customer Support Portal Alternate URL:

DP Image: gcr.io/pan-cn-series/panos_cn_ngfw

DP Image Version: preferred-10.2

MP Image: gcr.io/pan-cn-series/panos_cn_mgmt

MP Image Version: preferred-10.2

PAN CNI Image: gcr.io/pan-cn-series/pan_cni

PAN CNI Image Version: preferred

Create **Cancel**

STEP 11 | (任意)HA展開のセカンダリPanoramaIPアドレスを入力します。

STEP 12 | CN-Series PanoramaAuth Key (認証キー)を入力します。

STEP 13 | Panoramaデバイスグループを入力します。

STEP 14 | Panoramaテンプレートスタックを入力します。

STEP 15 | Panoramaログコレクタグループ名を入力します。

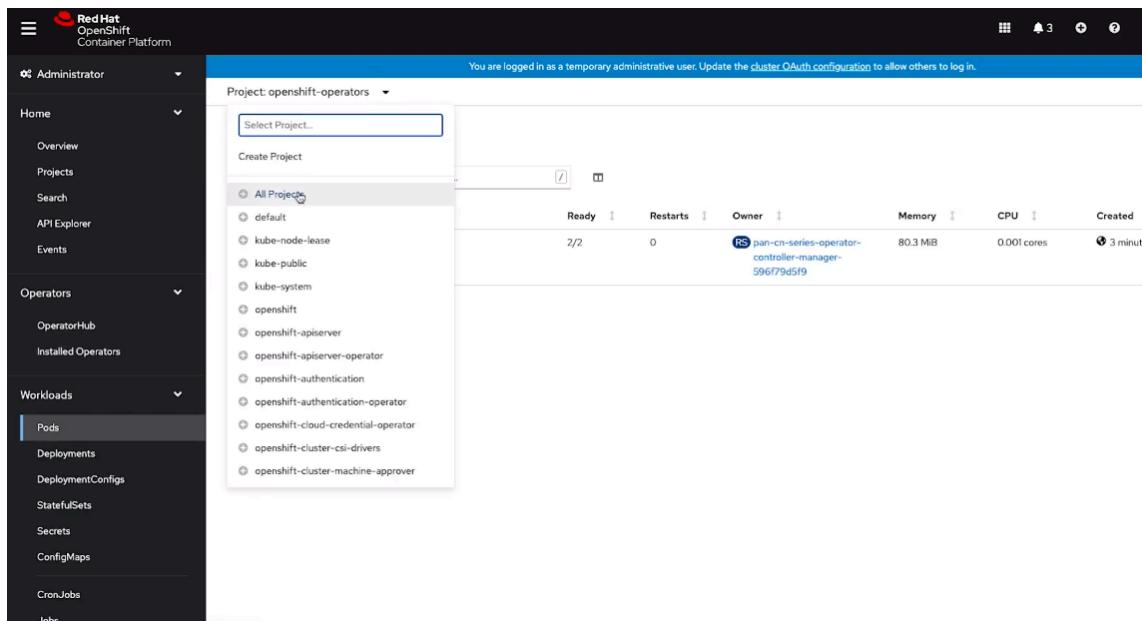
STEP 16 | (オプション)CSP(カスタマーサポートポータル)の**PIN ID**、**PIN**値、代替**URL**を入力します。

STEP 17 | PAN-OS のバージョンに基づいて、[CN シリーズ コンテナ レジストリ](#) コンソールで DP、MP、および CNI の適切なイメージにリンクします。

STEP 18 | 作成をクリックします。

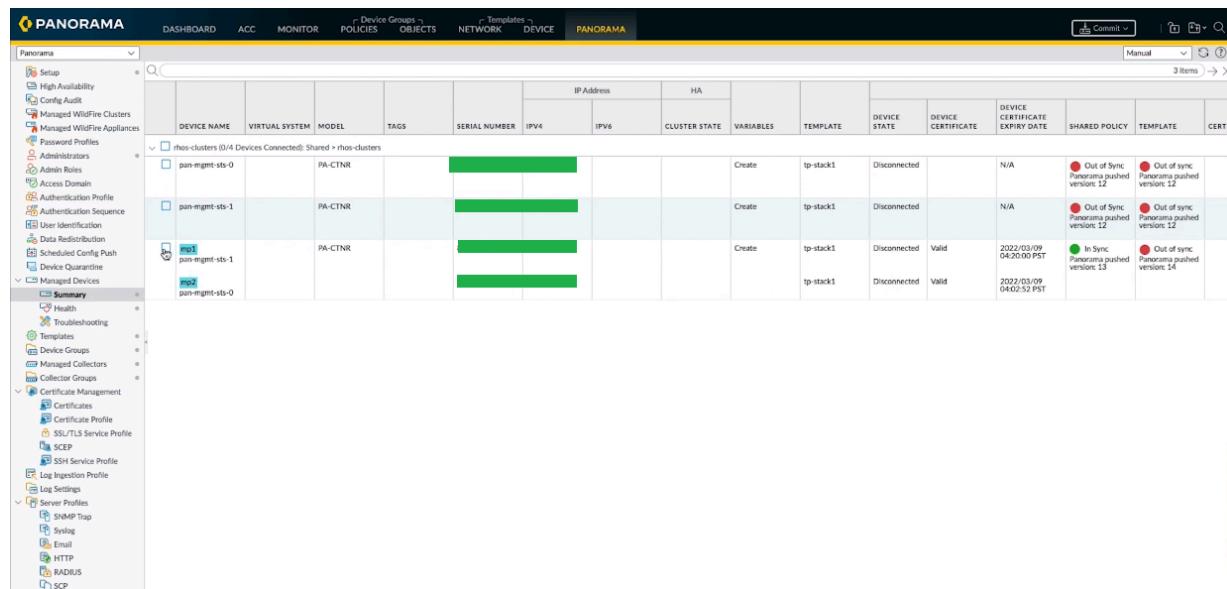
STEP 19 | ナビゲーションメニューで、ポッドに移動します。

STEP 20 | プロジェクト[OpenShift-operators]を選択してから[kube-system]に移動し、オペランドの一部としてデプロイしたCNI、管理、およびデータプレーンポッドの名前とステータスを表示します。



The screenshot shows the Red Hat OpenShift Container Platform interface. The left sidebar is the navigation menu. The main area is titled 'Project: openshift-operators'. A sub-menu 'Select Project...' is open, showing a list of projects including 'All Projects', 'default', 'kube-node-lease', 'kube-public', 'kube-system', 'openshift', 'openshift-apiserver', 'openshift-apiserver-operator', 'openshift-authentication', 'openshift-authentication-operator', 'openshift-cloud-credential-operator', 'openshift-cluster-csi-drivers', and 'openshift-cluster-machine-approver'. Below this, a table lists pods with columns: Ready, Restarts, Owner, Memory, CPU, and Created. One pod is visible: 'pan-cn-series-operator-controller-manager-99679d5f9' (Owner: RS), which is 'Ready' with 2/2, 0 restarts, and created 3 minutes ago.

Panorama上でファイアウォールの導入状況を確認できます。導入後5分以内にデバイス状態が「接続済み」に変わります。



The screenshot shows the Palo Alto Networks Panorama interface. The left sidebar contains navigation links for Setup, High Availability, Confire Audit, Managed WildFire Clusters, Managed WildFire Appliances, Password Profiles, Administrators, Access Domain, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Scheduled Config Push, Device Quarantine, and Managed Devices. The 'Managed Devices' section is expanded, showing a table of devices. The table has columns: DEVICE NAME, VIRTUAL SYSTEM, MODEL, TAGS, SERIAL NUMBER, IPV4, IPV6, CLUSTER STATE, VARIABLES, TEMPLATE, DEVICE STATE, DEVICE CERTIFICATE, EXPIRY DATE, SHARED POLICY, TEMPLATE, and CERTIF. Two devices are listed: 'pan-mgmt-sts-0' and 'pan-mgmt-sts-1', both of which are marked as 'Out of Sync' with 'Panorama pushed version 12'.

STEP 21 | Multus CNI プラグインと連動するように PALO ALTO NETWORKS-CNI プラグインを設定します。

OpenShift 上の Multus CNI は、他の CNI プラグインを呼び出す「メタプラグイン」として機能します。アプリケーションごとに、以下の作業を行う必要があります。

1. 次のコマンドを実行して、すべてのポッド名前空間に `pan-cni-net-attach-def.yaml` をデプロイします。

```
kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>
```

2. アプリケーション YAML を変更します。

`pan-cni-net-attach-def.yaml` をデプロイしたら、アプリケーション ポッド yaml に以下の注釈を追加します。

```
paloaltonetworks.com/firewall: pan-fw
```

```
k8s.v1.cni.cncf.io/networks: pan-cni
```

上記注釈内に他のネットワークが含まれている場合は、検査する必要のあるネットワークの後ろに `pan-cni` を追加します。`pan-cni` の後ろのネットワークは、リダイレクトされず、検査されません。



ポッドに複数のネットワークインターフェースが含まれている場合は、`pan-cni-configmap.yaml` の `interfaces` セクションの下で、`CN-NGFW` ポッドがトラフィックを検査する対象のインターフェース名を指定する必要があります。

以下に例を示します。

```
テンプレート: metadata: annotations: paloaltonetworks.com/
firewall: pan-fw k8s.v1.cni.cncf.io/networks: pan-cni
```

