

Déployer le pare-feu CN-Series dans le cloud et sur site

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

Déployer le pare-feu CN-Series dans GKE	5
Déploiement du pare-feu CN-Series en tant que service Kubernetes dans GKE	6
Déploiement du pare-feu CN-Series en tant que DaemonSet dans GKE	19
Déployer le pare-feu CN-Series dans OKE	31
Déployer le pare-feu CN-Series en tant que service Kubernetes dans OKE	33
Déployer le pare-feu CN-Series en tant que DaemonSet dans OKE	45
Déployer le pare-feu CN-Series dans EKS	57
Déploiement du pare-feu CN-Series en tant que service Kubernetes dans AWS EKS	58
Déploiement du pare-feu CN-Series en tant que DaemonSet dans AWS EKS	67
Déployer le pare-feu CN-Series à partir d'AWS Marketplace	76
Déployer le pare-feu CN-Series en tant que service Kubernetes sur	
AliCloud (ACK)	85
Déployer CN-Series sur OpenShift	.107
Déployer CN-Series sur le hub de l'opérateur OpenShift	. 109

TECH**DOCS**

Déployer le pare-feu CN-Series dans GKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?						
Déploiement CN-Series	• CN-Series 10.1.x or above Container Images						
	Panorama sous PAN-OS 10.1.x ou une version supérieure						
	Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm						

Après avoir examiné les blocs de construction CN-Series et la présentation générale du flux de travail dans Sécuriser les environnements Kubernetes avec CN-Series , vous pouvez commencer à déployer les pare-feu CN-Series sur la plate-forme GKE pour sécuriser le trafic entre les conteneurs au sein du même cluster, ainsi qu'entre les conteneurs et d'autres types de charges de travail tels que les machines virtuelles et les serveurs bare-metal.



Vous avez besoin d'outils Kubernetes standard tels que kubectl ou Helm pour déployer et gérer vos applications, vos services pare-feu et vos clusters Kubernetes.

Pour plus d'informations, consultez Déployer des pare-feu CN-Series avec des graphiques et des modèles Helm. Panorama n'est pas conçu pour être utilisé comme orchestrateur pour le déploiement et la gestion de clusters Kubernetes. Les modèles pour la gestion des clusters sont fournis par les fournisseurs de Kubernetes gérés. Palo Alto Networks fournit des modèles pris en charge par la communauté pour le déploiement CN-Series avec Helm et Terraform.

- Déploiement du pare-feu CN-Series en tant que service Kubernetes dans GKE
- Déploiement du pare-feu CN-Series en tant que DaemonSet dans GKE
 - Avant de passer du déploiement de CN-Series en tant que DaemonSet à CN-Series en tant que service ou vice versa, vous devez supprimer et réappliquer pluginserviceaccount.yaml. Pour plus d'informations, consultez Créer des comptes de service pour l'authentification des clusters.
 - Lorsque vous déployez CN-Series en tant que DaemonSet dans GKE, le pan-plugincluster-mode-secret ne doit pas exister.
 - Lorsque vous déployez CN-Series en tant que service Kubernetes dans GKE, le panplugin-cluster-mode-secret doit être présent.

Déploiement du pare-feu CN-Series en tant que service Kubernetes dans GKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que service Kubernetes.

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans GKE, procédez comme suit :

1. Cliquez sur le menu de navigation, accédez à Kubernetes Engine (Moteur Kubernetes), puis sélectionnez clusters.

≡	Google Cloud Platform	n 🔹 gcp-pavmqa 👻			Q Sea	arch products and re	sources		~						
ŵ	Home >	ubernetes clus	sters 🖪 CF	REATE 🛃 DEPLOY	C REFRESH	DELETE									
PINN	ED														
	Billing	•	An optimized cluste	aucing Autopliot mode xperience. When you create a cluster in Autopliot mode, Google provisions and manages the entire cluster's underlying infrastructure,											
Θ	IAM & Admin	•	including nodes and Compare cluster me	g nodes and node pools. e cluster modes											
API	APIs & Services	•	✓ Get a productio	t a production-ready cluster based on your workload requirements											
<u>\</u>	Marketplace		 Eliminate the or Pay per Pod, or 	Eliminate the overhead of node management Pay per Pod, only for the resources that you use											
۲	Compute Engine		 Increase securi Gain higher work 	crease security with Google best practices built-in sain higher workload availability											
	Cloud Storage >														
11	VPC network		TRY THE DEMO	N THE DEMO											
)≽	Cloud Run	_													
())	SQL	OVERVIEW	COST OPTIMIZATIO	ON PREVIEW											
٢	Kubernetes Engine	Tilter Enterp	roperty name or value	eastion N	lumber of podes	Total uCDI la	Total memory	Notifications	() abala	III					
G,	BigQuery >	Workloads	andra-gke- u:	s-central1-c	0	0	0 GB	A Pods		:					
ALL F	RODUCTS 🗸	Services & Ingress Applications	oud-init- u: ak-cluster1	s-east1-c	0	0	0 GB	A Pods unschedulable	-	:					
		Configuration	oud- u	s-central1-c	0	0	0 GB	A Pods	-	:					
		Storage Object Browser	ak2					Node upgrade available							
		Migrate to containers Config Management	-cnseries-2 u	s-west2-a	3	24	96 GB	Eow resource requests	-	:					
			10.1.1					A 0.1							

- 2. Cliquez sur Create (Créer).
- **3.** Sélectionnez la **GKE Standard (Norme GKE)** comme mode de cluster que vous souhaitez utiliser, puis cliquez sur **Configure (Configurer)**.

← → C ☆ 🔒 co	nsole.cloud.google.com/kubern	etes/list/overview?pro	oject=gcp-pavmqa&is0	CreateAndRegister=fals	e	Ey 🧰 DAN P	SP Homenan 💙	Lab & Firewall Reco	2021-07-21 Mastin	Y Darbhoa	rd - Conflu 🗖 AEM STAC	TING	x *
Google Cloud I	Platform : gcp-pavmqa	 syle & mong dat. 	. 🖤 Pitewali as a Piauc	Q Seal	rch products and reso	ources	se nomepaga.	tao or mewail kes.		Cesnode	io Comu. Provinsia	2	0
Kubernetes Eng	ine Kubernetes o	lusters 🖪	CREATE 🖪 DEPLI	DY CREFRESH	DELETE						& C	PERATIONS +	HIDE
Custers Custers Custers Custers Custers Curdoads Curdoad		Introduciny An optimized clu including nodes <u>Compare cluste</u> C Get a produ Eliminate th Pay per Pool Eliminate th Pay per Pool Chicreses see Gain higher TRY THE DEMO	g Autopilot mod uster with a hands off ex and node pools. :remotes citcon ready cluster bases is overhead of node man d, only for the resources th workload aveitability) LEARN MORE	e e e e e e e e e e e e e e e e e e e	e a cluster in Autopilot n Ster ode that you want to use e cluster modes to learn r where you configure an	ode, Google prov	isions and manage differences.	COMPARE	s underlying infrastructure,	×	No clusters select	:ted sur resources (e. i selected	.g., cost_ce
	OVERVIEW Filter Ent Status © © © © ©	COST OPTIMIZA er property name or val Name ↑ chandra-gike- cluster cloud-init- soak-cluster1 cloud- initegration- soak2	ATION PREVIEW	GKE Autopilot A Kubernetes cluste configuration requir	rr where GKE manages y ed. <u>Learn more</u> 0	our nodes with mi 0 GB	unschedulable Pods unschedulable	CANCEL	e				
 Marketplace Release Notes 		hs-cnseries-2 k8s-plugin- testing1	us-west2-a us-west2-a	3	24	96 GB 0 GB	Low resource requests A Pods unschedulable	-		I I			

4. Saisissez les informations de base du cluster, notamment Nom, Version, Emplacement, Sous-réseau de nœud, puis cliquez sur Create (Créer).

=	Google Cloud Platform	s gcp-	pavmqa 👻 Q Search proc	
÷	Create a Kubernetes clust	ter	ADD NODE POOL	
•	Cluster basics		Cluster basics	
NODE	POOLS		The new cluster will be created with the name, version, and in the location you specify	
•	default-pool	\sim	here. After the cluster is created, name and location can't be changed.	
LUST	TER		To experiment with an affordable cluster, try My first cluster in the Cluster set-up quides	
•	Automation		oot op galaco	
0	Networking Some form fields are incorrect		Name cluster-1	
•	Security		Location type	
	Metadata		Zonal	
-	Metadata		O Regional	
•	Features		Zone us-central1-c 🗸 🗸 🖉	
			Current default node locations Current default us-central1-c Control plane version Control plane version Coose a release channel for automatic management of your cluster's version and upgrade cadence. Choose a static version for more direct management of your cluster's version. Learn more. Static version Release channel Regular channel (default)	
			Version 1.20.10-gke.301 (default)	
			СПЕАТЕ	CANCEL

Si votre cluster se trouve sur GKE, assurez-vous d'activer l'API Network Policy de Kubernetes pour permettre à l'administrateur du cluster d'indiquer quels pods sont autorisés à communiquer entre eux. Cette API est requise pour permettre aux pods CN-NGFW et CN-MGMT de communiquer.

		-
Auto-upgrade: On	← Create a Kubernetes d	cluster
More options		
		Networking
		VPC notive
+ Add node pool		 Ensure And classify mass (c) (c)
		Network ()
Eachie Cloud Due for Anthon		und t
Enable cloud Run for Antrios		Node subnet
		default (10.128 0 0/20) *
Availability, networking, security, and additional features and additionand additional features and	res	Zutomatically create secondary ranges
0		Pod address range (Optional)
		Expmple: 10.96.0.0/14
		Maximum peda per node (Dational)
		110
		Mask for Pod address range per node: /24
		Service address range (Opticnal)
		Example: 10.94.0.0/18
		 Enable Initiands visibility (i) Reveals your intranode traffic to Goog vis networking tables. To get logs, your need to enable VPE days log in the selected subpervork.
		Lood balancing
		C Enable HTTP load balancing 🛞
		Network accurity
		 Private cluster @
		 Enable master authorized networks

1. Vérifiez que le cluster dispose des ressources adéquates. La spécification par défaut du pool de nœuds GKE n'est pas adaptée au pare-feu CN-Series. Vous devez vous assurer que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu :

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et mise à l'échelle de CN-Series.

Assurez-vous d'avoir les informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Cluster Definitior	n			0
	Name	on_prem-clstr		
D	escription			
API serve	er address	10.2.		
	Туре	Native-Kubernet	es	~
Crede	ntials			Į.
Label Selector	abel Filte	er Custom C	ertificate	
Q.($_{0 \text{ items}} \rightarrow \times$
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	APPLY ON
Validate				OK Cancel

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe de collecteurs de journaux à partir de Panorama.

Collector Group	Device Log Forwarding L Collector Log Forwarding L Log Ingestion
Name	ro-ce1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	
	rosconew(RPGOOGGKEPRA1)
N	
15	
	(+) Add (-) Delete
	Enable log redundancy across collectors
	Enable secure inter LC Communication
	Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.



Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_IP sur votre fichier YAML correspond à votre adresse IP Panorama réelle, comme indiqué dans le diagramme ci-dessous :



Vous devez vous assurer que la valeur des paramètres de PAN_DEVICE_GROUP et PAN_TEMPLATE sur votre fichier YAML correspond au nom du groupe d'appareils et de la pile de modèles que vous avez créés sur Panorama, comme indiqué dans le diagramme ci-dessous :

← → C ▲ Not Secure 35.196.181.54/#panorama::dev-dg::panorama/device-groups										० 🛧 🔾 🙆 💩			
UPANORAMA	D	SHBOARD	ACC	MONITOR	C Device	Groups n OBJECTS	ر T NETWO	emplates ר RK DEVICE	PANORAMA		t, j t		
Panorama 🗸 🗸											5		
C Access Domain	Q										2 items		
Authentication Profile						AU	HORIZATION			DEVICES/VIRTUAL	REFEREN		
Authentication Sequence		NAME 🛋		DESCRIPTIO	N	co	DE	SW VERSION	MASTER DEVICE	SYSTEM	TEMPLAT		
Data Redictribution		Shared											
Device Quarantine		Co. day	da								k8s-stack		
Managed Devices		le dev	-og										
Templates													
Device Groups													
Managed Collectors	1												
Collector Groups													
Certificate Management													
Certificates													
Certificate Profile													
SSL/TLS Service Profile													
SSH Service Profile													
Log Ingestion Profile													
Log Settings													
Server Profiles													
SNMP Trap													
Syslog													
Email													
В НТТР													
RADIUS													
LD SCP	-		-										

Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_CG_NAME est identique au nom du collecteur de journaux que vous avez créé.

	DA	SHBOARD	ACC	MONITOR	C Device	Groups 7 OBJECT	r Temp NETWORK	lates – DEVIC	PANORAMA	₽ ~ ⊕
Panorama										
C Access Domain	0									1 it
Authentication Profile		NAME		REDUI	DANCY ENABLE	D I	ORWARD TO ALL CO	DLLECTORS	COLLECTORS	LOG REDISTRIBUTIO
User Identification		rp-cg1							demo-panorama	none
Data Redistribution										
B Device Quarantine										
Managed Devices										
Templates										
Device Groups										
Managed Collectors										
Collector Groups										
Certificate Management										
Certificates										
Certificate Profile	4									
SSL/TLS Service Profile										
SCEP										
SSH Service Profile										
Log Ingestion Profile										
Log Settings										
Server Profiles										
SNMP Trap										
Syslog										
Email										
• НТТР										
RADIUS										
C) SCP										

Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.

STEP 4 | Si vous utilisez la mise à l'échelle automatique dans votre environnement Kubernetes, consultez Activer la mise à l'échelle horizontale du pod.



STEP 5 | Déployez le service CN-NGFW. Effectuez les étapes suivantes :

Lorsqu'elles sont déployées en tant que service Kubernetes, les instances du pod CN-NGFW peuvent être déployées sur des nœuds de sécurité et le trafic du pod d'application est redirigé vers une instance CN-NGFW disponible pour inspection et application.



- Vérifiez que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml.
 Consultez Création de comptes de service pour l'authentification des clusters.
- 2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez kubectl pour exécuter le fichier pan-cn-ngfw-svc.yaml.

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

Ce fichier yaml doit être déployé avant pan-cni.yaml.

4. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 5. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 6. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	<pre>\$ kubect1</pre>	get pods	-n	kube-system	grep	pan-cni
pan-cni-nmqkf		Running	0	2m11s				
pan-cni-wjrkq		Running	0	2m11s				
pan-cni-xrc2z		Running	0	2m12s				i i
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(w	eries-mktplace)	\$					i i

STEP 6 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

- 1. (Requis uniquement pour les PV provisionnés statiquement) Déployez les volumes persistants (PV) pour le StatefulSet CN-MGMT.
 - 1. Créez les répertoires qui correspondent aux noms des volumes locaux définis dans le fichier pan-cn-pv-local.yaml.

Vous avez besoin de six (6) répertoires sur au moins 2 nœuds esclaves. Connectez-vous à chaque nœud esclave sur lequel le StatefulSet CN-MGMT sera déployé pour créer les répertoires. Par exemple, pour créer des répertoires nommés /mnt/pan-local1 vers /mnt/pan-local6, utilisez la commande :

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

2. Modifiez pan-cn-pv-local.yaml.

Faites correspondre le nom d'hôte sous **nodeaffinity**, et vérifiez que vous avez modifié les répertoires que vous avez créés ci-dessus dans **spec.local.path** puis déployez le fichier pour créer une nouvelle storage class pan-local-storage et des PV locaux.

2. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap

Exemple de pan-cn-mgmt-configmap de l'EKS.

apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmtconfig 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: "<panoramatemplate-stack>" PAN_CGNAME: "<panorama-collector-</pre> group>" # ctnr mode: "k8s-service", "k8s-ilbservice"
 PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER NAME: "<Cluster name>" #PAN PANORAMA IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN JUMBO FRAME ENABLED: "true" # Start MGMT pod with GTP enabled. For complete functionality, need GTP # enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. #PAN NGFW MEMORY="6Gi" #PAN NGFW MEMORY="40Gi" # For enabling faster datapath - AF_XDP, default is AF_PACKETV2. This requires kernel support. #PAN_DATA_MODE: "next-gen" #HPA params #PAN_CLOUD: "EKS" #PAN_NAMESPACE_EKS: "EKSNamespace" #PUSH INTERVAL: "15" #time interval to publish metrics to AWS cloudwatch

Exemple de pan-cn-mgmt.yaml

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

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

3. Utilisez Kubectl pour exécuter les fichiers yaml.

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

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de compte de service pour l'authentification de cluster.

4. Vérifiez que les pods CN-MGMT sont opérationnels en exécutant la commande suivante :

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

Cela prend environ 5-6 minutes.

- **STEP 7** | Déployez les pods CN-NGFW.
 - 1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

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

4. Vérifiez que les pods CN-NGFW sont en cours d'exécution.

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

- **STEP 8** | Activez l'autoscaling horizontal des pods en procédant comme suit :
 - 1. Déployez l'adaptateur de pilote de pile de mesures personnalisées dans votre cluster CN-Series. Le nom du cluster doit être fourni via un secret K8s.
 - 2. Téléchargez les fichiers yaml HPA spécifiques à GKE à partir du référentiel GitHub de Palo Alto Networks.
 - 3. Si votre CN-MGMT est déployé dans un espace de noms personnalisé, mettez à jour pan-cnadapater.yaml avec l'espace de noms personnalisé. L'espace de noms par défaut est **kube**system.
 - 4. Mettez à jour les paramètres HPA dans le fichier pan-cn-mgmt-configmap.yaml spécifique à GKE.

#PAN_CLOUD: "GKE"

#HPA_NAME: "<name>" #nom unique pour identifier la ressource hpa par espace de noms ou par locataire

#PUSH_INTERVAL: "15" #intervalle de temps pour publier les métriques sur stackdriver

- 5. Modifiez les fichiers **pan-cn-hpa-dp.yaml** et **pan-cn-hpa-mp.yaml** avec HPA_NAME (remplacez par le nom) tel que mis à jour dans le fichier pan-cn-mgmtconfigmap.yaml ci-dessus et mettez à jour la métrique en fonction de quel HPA doit être déclenché.
 - 1. Entrez le nombre minimal et maximal de réplicas.
 - 2. (Facultatif) Modifiez les valeurs de fréquence de mise à l'échelle et de montée en puissance en fonction de votre déploiement. Si vous ne modifiez pas ces valeurs, les valeurs par défaut sont utilisées.
 - **3.** (Facultatif) Modifiez la valeur de seuil pour chaque métrique que vous souhaitez utiliser pour la mise à l'échelle. Si vous ne modifiez pas ces valeurs, les valeurs par défaut sont utilisées.

- **4.** Enregistrez les modifications.
- 6. Déployez les fichiers yaml HPA. Les fichiers doivent être déployés dans l'ordre décrit cidessous.
 - 1. Utiliser Kubectl pour exécuter le fichier pan-cn-adapter.yaml

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

2. Utiliser Kubectl pour exécuter le fichier pan-cn-crole.yaml

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

3. Utiliser Kubectl pour exécuter le fichier pan-cn-hpa-dp.yaml

```
kubectl apply -f pan-cn-hpa-dp.yaml
```

4. Utiliser Kubectl pour exécuter le fichier pan-cn-hpa-mp.yaml

```
kubectl apply -f pan-cn-hpa-mp.yaml
```

- 7. Vérifiez votre déploiement.
 - Utilisez kubectl pour vérifier que le pod d'adaptateur de mesures personnalisées dans l'espace de noms de mesures personnalisées.

```
kubectl get pods -n custom-metrics
```

• Utilisez kubectl pour rechercher la ressource HPA.

```
kubectl get hpa -n kube-system
```

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

Pour plus d'informations, consultez Activer la mise à l'échelle automatique horizontale du pod sur CN-Series.

STEP 9 | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

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

STEP 10 | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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



Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire **STEP 11** | Déployez votre application dans le cluster.

Déploiement du pare-feu CN-Series en tant que DaemonSet dans GKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que Daemonset dans la plateforme GKE :

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans GKE, procédez comme suit :

1. Cliquez sur le menu de navigation, accédez à Kubernetes Engine (Moteur Kubernetes), puis sélectionnez clusters.

≡	Google Cloud Platfo	orm	🕈 gcp-pavmqa 👻			Q Se	arch products and re	sources			~		
ŵ	Home	>	ubernetes clus	ters	🖶 CREATE 🛛 🗄 D	EPLOY C REFRESH	DELETE						
PINN	ED												1
	Billing		•	Introduci	ng Autopilot n	10de	iste a cluster in Autonilo	t mode. Google prov	isions and manages	the entire cluster's underlying infrastra	icture	×	
Θ	IAM & Admin	>	• 🐥	including node	es and node pools. ter modes	n experience. Then you de	are a claster in Autopilo	emote, obogie prof	isions and manages	the entire cluster s underlying infusite	iciure,		
API	APIs & Services	>	•	🗸 Get a pror	duction-ready cluster t	ased on your workload requ	uirements						
Ŷ	Marketplace			 Eliminate Pay per P 	the overhead of node od, only for the resour	management ces that you use							
۲	Compute Engine	>		 Increase : Gain high 	security with Google b er workload availabilit	est practices built-in v							
	Cloud Storage	>											
11	VPC network	>		TRY THE DEM	LEARN MORE								
)≽	Cloud Run												
\$	SQL		OVERVIEW	COST OPTIMI	IZATION PREVIEW						•		
٢	Kubernetes Engine	>	Clusters	me 个	Location	Number of nodes	Total vCPUs	Total memory	Notifications	Labels	U	-	
Ð,	BigQuery	>	Workloads	andra-gke-	us-central1-c	0	0	0 GB	A Pods	-		:	
ALL F	RODUCTS V		Services & Ingress	oud-init-	us-east1-c	0	0	0 GB	A Pods	-		:	
			Configuration	bud-	us-central1-c	0	0	0 GB	A Pods	-		:	
			Storage	ak2					• Node • Node				
			Object Browser						available				
			Config Management	-cnseries-2	us-west2-a	3	24	96 GB	Eow resource	-		:	
									requests				

- 2. Cliquez sur Create (Créer).
- **3.** Sélectionnez la **GKE Standard (Norme GKE)** comme mode de cluster que vous souhaitez utiliser, puis cliquez sur **Configure (Configurer)**.

← → C ☆ 🔒 co	nsole.cloud.google.com/kubern	etes/list/overview?pro	oject=gcp-pavmqa&is0	CreateAndRegister=fals	e	Ey MA DAN P	SP Homenan 💙	Lab & Firewall Reco	2021-07-21 Mastin	Y Darbhoa	rd - Conflu 🗖 AEM STAC	TING	x *
Google Cloud I	Platform : gcp-pavmqa	 syle & mong dat. 	. 🖤 Pitewali as a Piauc	Q Seal	rch products and reso	ources	se nomepaga.	tao or mewail kes.		Cesnode	io Comu. Provinsia	2	0
Kubernetes Eng	ine Kubernetes o	lusters 🖪	CREATE 🖪 DEPLI	DY CREFRESH	DELETE						& C	PERATIONS +	HIDE
Custers Custers Custers Custers Custers Curdoads Curdoad		Introducing Autopilot mode Ar optimized dustre with a hands of it spremeres including nodes and node poils. Correct custor mode Set a production ready cluster base Correct custor mode Set a production ready cluster base Correct custor mode Correct custor mo			terce: When you create a cluster in Autoplot mode, Google provisions and manages the entre cluster's unde Create Cluster Belect the cluster mode that you want to use. Compare cluster modes to learn more about their differences. COMPARE CRE Standard					×	No clusters selected Labels help signing your resources (e.g. enrystod), Labels help signing your resources (e.g. No clusters selected No clusters selected		.g., cost_ce
	OVERVIEW Filter Ent Status © © © © ©	COST OPTIMIZA er property name or val Name ↑ chandra-gik- cluster cloud-init- soak-cluster1 cloud- initegration- soak2	ATION PREVIEW	GKE Autopilot A Kubernetes cluste configuration requir	rr where GKE manages y ed. <u>Learn more</u> 0	our nodes with mi 0 GB	unschedulable Pods unschedulable	CANCEL	e				
 Marketplace Release Notes 		hs-cnseries-2 k8s-plugin- testing1	us-west2-a us-west2-a	3	24	96 GB 0 GB	Low resource requests A Pods unschedulable	-		I I			

4. Saisissez les informations de base du cluster, notamment Nom, Version, Emplacement, Sous-réseau de nœud, puis cliquez sur Create (Créer).



Si votre cluster se trouve sur GKE, assurez-vous d'activer l'API Network Policy de Kubernetes pour permettre à l'administrateur du cluster d'indiquer quels pods sont autorisés à communiquer entre eux. Cette API est requise pour permettre aux pods CN-NGFW et CN-MGMT de communiquer.

CPU platform and GPU		
Auto-upgrade: On	← Create a Kubernetes cluster	
More options		
		Networking
		VPC native
+ Add node pool		
		Network ()
		default
Enable Cloud Run for Anthos 10		Node subnet
		default (10.128.0 0/20)
Security, and additional fea	ures	Automatically create secondary ranges
Ŭ		Pod address range (Optional)
		Experiple: 10,96,0.0/14
		Masimum pods per node (3ptions)) 🛞
		110
		Mask for Pod address range per node: /24
		Service address range (Opticnal)
		Example: 10.94.0.0/18
		 Installe Instance's withinkity (i) Reveality your instance's traffects a Googie's networking status: To get logis, yo to enable VPC flow logis in the selected subnetwork.
		Lood balancing
		Enable HTTP load balancing (i)
		Network accurity
		 Private cluster
		Drable marter authorized networks. (D)

Vérifiez que le cluster dispose des ressources adéquates. Assurez-vous que ce cluster dispose des exigences système de CN-Series pour prendre en charge le pare-feu.

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et évolutivité de CN-Series.

Assurez-vous d'avoir les informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Na Descript API server addr Tr Credentials Label Selector Label F Credentials	ame on_p tion ress 10.2 Type Nativ	ve-Kubernet Custom C	tes Certificate		
Descript API server addr Tr Credentials	tion ress 10.2 Type Nativ	ve-Kubernet Custom C	tes Certificate		
API server addr Tr Credentials Label Selector Label F C TAG PREFIX NA	ress 10.2 Type Nativ	ve-Kubernet Custom C	tes Certificate		
Tr Credentials	ype Nativ	ve-Kubernet Custom C	tes Certificate		
Credentials Label Selector Label R C TAG PREFIX NAI	Filter	Custom C	Certificate		
Label Selector Label I C	Filter	Custom C	Certificate		
Q TAG PREFIX NAI					
TAG PREFIX NA					$0 \text{ items} \rightarrow \times$
	MESPACE		LABEL SELECTOR FILTER	A	APPLY ON
0					
(+) Add (-) Delete					

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

Pour plus d'informations, consultez Configurer le plug-in Kubernetes pour la surveillance des clusters.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe du collecteur de journaux à partir de Panorama.

Collector Group	0
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item)→X
	COLLECTORS
	rpgcpnew(RPGOOGGKEPRA1)
6	
	(+) Add (-) Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.

Vous devez remplacer le chemin d'accès de l'image dans les fichiers YAML pour inclure le chemin d'accès à votre répertoire privé Google Container et fournir les paramètres requis. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.

STEP 4 | Déployez le DaemonSet CNI.

Le conteneur CNI est déployé comme un DaemonSet (un pod par nœud) et il crée deux interfaces sur le pod CN-NGFW pour chaque application déployée sur le nœud. Lorsque vous utilisez les commandes kubectl pour exécuter les fichiers YAML pan-cni, il devient une partie de la chaîne de service sur chaque nœud.

1. Le pare-feu CN-Series nécessite trois comptes de service avec les autorisations minimales qui l'autorisent à communiquer avec les ressources de votre cluster Kubernetes. Vous devez créer

Création d'un compte de service pour l'authentification du cluster CN-Series et vérifier que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml.

2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 4. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 5. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	\$ kubectl get pods	-n	kube-system	grep	pan-cni
-nmqkf		Running	2m11s				
-wjrkq		Running	2m11s				
-xrc2z		Running	2m12s				
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	\$				
	· ·	-					

STEP 5 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

1. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt-configmap

name: pan-mgmt-config

metadata:

namespace: kube-system

data:

PAN_SERVICE_NAME: pan-mgmt-svc

PAN_MGMT_SECRET: pan-mgmt-secret

#Paramètres de Panorama :

PAN_PANORAMA_IP: "x.y.z.a"

PAN DEVICE GROUP: "dg-1"

PAN_TEMPLATE_STACK: "temp-stack-1"

PAN_CGNAME: "CG-GKE"

Paramètres non obligatoires

#Il est recommandé d'avoir le même nom que le nom du cluster fourni dans l'extension Kubernetes de Panorama. L'identification des pods sera plus facile en cas de gestion de plusieurs clusters avec le même Panorama

#CLUSTER NAME: "<Cluster name>"

#PAN PANORAMA IP2: ""

#Commentaire pour utiliser les CERT sinon PSK pour IPSec entre pan-mgmt et pan-ngfw

#IPSEC_CERT_BYPASS: ""

#Aucune valeur nécessaire

#Remplacer la détection automatique du mode
 jumbo-frame et forcer l'activation à l'échelle du
 système#PAN_JUMBO_FRAME_ENABLED: "true"

#Démarrer le pod MGMT avec GTP activé. Pour une fonctionnalité complète, vous devez également activer GTP dans Panorama.

#PAN GTP ENABLED: "true"

#Activer les capacités de fonctionnalités élevées. Cellesci nécessitent une mémoire élevée pour le pod MGMT et une mémoire supérieure/correspondant à celle spécifiée ci-dessous pour le pod NGFW.

#Ceci nécessite la prise en charge du noyau et le pod NGFW
s'exécutant avec des privilèges : true

#PAN NGFW MEMORY: "42Gi"

Exemple de pan-cn-mgmt.yaml

initContainers:

- name: pan-mgmt-init

image : <your-private-registry-image-path>

conteneurs : - nom : pan-mgmt

image : <your-private-registry-image-path>

terminationMessagePolicy: FallbackToLogsOnError

2. Utilisez Kubectl pour exécuter les fichiers yaml.

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

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de comptes de service pour l'authentification de cluster.

3. Vérifiez que les pods CN-MGMT sont activés.

Cela prend environ 5-6 minutes.

Utilisez kubectl get pods -l app=pan-mgmt -n kube-system NOM PRÊT ÉTAT REDÉMARRE AGEpan-mgmt-sts-0 1/1 Fonctionnement 0 27hpan-mgmt-sts-1 1/1 Exécution 0 27h

STEP 6 | Déployez les pods CN-NGFW.

Par défaut, le pod CN-NGFW du plan de données du pare-feu est déployé comme un DaemonSet. Une instance du pod CN-NFGW peut sécuriser le trafic pour un maximum de 30 pods d'application sur un nœud.

1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

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

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

kubectl apply -f pan-cn-ngfw.yaml

4. Vérifiez que tous les pods CN-NGFW sont en cours d'exécution (un par nœud dans votre cluster)

Il s'agit d'un exemple de résultat provenant d'un cluster de 4 nœuds sur site.

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-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none> **STEP 7** | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

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

- 0 27hpan-cni-5fhbg 1/1 En cours d'exécution
- 0 27hpan-cni-9j4rs 1/1 En cours d'exécution
- 0 27hpan-cni-ddwb4 1/1 En cours d'exécution
- 0 27hpan-cni-fwfrk 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-j62rk 1/1 En cours d'exécution
- 0 27hpan-cni-lmxdz 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-0 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-1 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-8g5xb 1/1 En cours d'exécution
- 27hpan-ngfw-ds-qsrm6 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-vqk7z 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-zncqg 1/1 En cours d'exécution
- **STEP 8** | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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

Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire

STEP 9 | Déployez votre application dans le cluster.

TECH**DOCS**

Déployer le pare-feu CN-Series dans OKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure
	 Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Oracle Kubernetes Engine (OKE) est un service OCI qui vous permet de déployer un cluster Kubernetes. Vous pouvez désormais déployer le pare-feu CN-Series dans le cluster OKE en tant que daemonset et en kubernetes en tant que service.

Après avoir examiné les blocs de construction CN-Series et la présentation générale du flux de travail dans Sécuriser les environnements Kubernetes avec CN-Series , vous pouvez commencer à déployer les pare-feu CN-Series sur la plate-forme OKE pour sécuriser le trafic entre les conteneurs au sein du même cluster, ainsi qu'entre les conteneurs et d'autres types de charges de travail tels que les machines virtuelles et les serveurs bare-metal.

Vous avez besoin d'outils Kubernetes standard tels que kubectl ou Helm pour déployer et gérer vos applications, vos services pare-feu et vos clusters Kubernetes.

Pour plus d'informations, consultez Déployer des pare-feu CN-Series avec des graphiques et des modèles Helm. Panorama n'est pas conçu pour être utilisé comme orchestrateur pour le déploiement et la gestion de clusters Kubernetes. Les modèles pour la gestion des clusters sont fournis par les fournisseurs de Kubernetes gérés. Palo Alto Networks fournit des modèles pris en charge par la communauté pour le déploiement CN-Series avec Helm et Terraform.

- Déployer le pare-feu CN-Series en tant que service Kubernetes dans OKE
- Déployer le pare-feu CN-Series en tant que DaemonSet dans OKE



Avant de passer du déploiement de CN-Series en tant que DaemonSet à CN-Series en tant que service ou vice versa, vous devez supprimer et réappliquer pluginserviceaccount.yaml. Pour plus d'informations, consultez Créer des comptes de service pour l'authentification des clusters.

- Lorsque vous déployez CN-Series en tant que DaemonSet dans OKE, le pan-plugincluster-mode-secret ne doit pas exister.
- Lorsque vous déployez CN-Series en tant que service Kubernetes, lepan-plugincluster-mode-secret doit être présent.

Déployer le pare-feu CN-Series en tant que service Kubernetes dans OKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	• CN-Series 10.1.x or above Container Images
	Panorama sous PAN-OS 10.1.x ou une version supérieure
	• Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que service Kubernetes dans la plateforme OKE.



Le système d'exploitation Oracle Linux 8.5 est le seul environnement qualifié pour le déploiement du pare-feu CN-Series dans OKE.

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans OKE, procédez comme suit :

1. Connectez-vous à Oracle Cloud Infrastructure.

CLE Cloud Infrastructure

SIGN IN
Signing in to cloud tenant: <u>Change tenant</u> Sign in with your Oracle Cloud Infrastructure credentials
USER NAME
PASSWORD
Sign In Forgot password?

- 2. Cliquez sur le menu de navigation, accédez à Under Solutions and Platform (Solutions et plateforme inférieures), puis cliquez sur Developer Services (Services aux développeurs).
- 3. Cliquez sur Kubernetes Clusters (Clusters Kubernetes).
- 4. Sélectionnez un compartiment et cliquez sur Create Cluster (Créer un cluster).

RACLE Cloud

ſS	Clusters in Tutorial2 Compartment						
' S	()	Clusters Requirements	ents: <u>Preparing for Contain</u>	ier Engine for Kut	ernetes		
ре	Crea	ate Cluster					
ENT	Name	Status	Node Pools	VCN	Version	Cre	
2 \$		No clusters exist. Create one to get started.					
oot)/Tutorial2							

and Privacy	Cookie Preferences	Copyright © 2019, Oracle and/or it
	5 Dans la haîte de diele sur Create Chuster (Créanum shute) aligner our Creatory Create (Création

- 5. Dans la boîte de dialogue Create Cluster (Créer un cluster), cliquez sur Custom Create (Création personnalisée), puis sur Launch Workflow (Lancer le flux de production).
- 6. Sur la page Create Cluster (Créer un cluster), entrez le Name (Nom) du cluster et d'autres détails.
- 7. Cliquez sur Next (Suivant) pour vérifier les détails que vous avez saisis pour le nouveau cluster.
- 8. Sur la page Réviser, cliquez sur Create Cluster (Créer un cluster).

RACLE Cloud

er Creation

	Basic Information Cluster Name: cluster1				
	Version: v1.18.10				
	Networ	rk			
	Compartment: Tutorial2		Network Security Groups: Not Enabled		
	VCN Name:	oke-vcn-quick- cluster1-4baf5729a	Kubernetes API Private Endpoint:	Auto Assigned	
			Kubernetes API Public Endpoint:	Auto Assigned	
				Kubernetes CIDR Block: 10.96.0.0/16	

1. Vous devez vous assurer que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu :

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et mise à l'échelle de CN-Series.

Assurez-vous d'avoir les informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Q US West (Phoenix) ✓

<u>^</u>
Cluster Definition					0				
	Name	on_prem-clstr							
De	scription								
API server	API server address 10.2.								
Type Native-Kubernetes									
Credentials									
Label Selector La	bel Filte	er Custom C	ertificate						
Q					$_{0 \text{ items}} \rightarrow \times$				
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER		APPLY ON				
(+) Add (-) Delete									

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe de collecteurs de journaux à partir de Panorama.

Collector Group	0									
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion									
Name rp-cg1										
Log Storage	Log Storage Total: 1.53 TB,Free: 75.30 GB									
Min Retention Period (days)	veriod (days) [1 - 2000]									
Collector Group Members	Q(1item) → X									
	rpgcpnew(RPGOOGGKEPRA1)									
5										
	O 111 O 211									
	+ Add - Delete									
	Enable log redundancy across collectors									
	Forward to all collectors in the preference list									
	Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'									
	OK Cancel									

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- Préparez l'emplacement du répertoire du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.



Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_IP sur votre fichier YAML correspond à votre adresse IP Panorama réelle, comme indiqué dans le diagramme ci-dessous :



Vous devez vous assurer que la valeur des paramètres de PAN_DEVICE_GROUP et PAN_TEMPLATE sur votre fichier YAML correspond au nom du groupe d'appareils et de la pile de modèles que vous avez créés sur Panorama, comme indiqué dans le diagramme ci-dessous :

← → C ▲ Not Secure 38	5.196	.181.54/#panora	ima::dev-dg	::panorama/dev	ice-groups					© ☆	0 6 6
UM-PANORAMA	DA	SHBOARD	ACC	MONITOR	C Device	Groups n OBJECTS	ر T NETWO	emplates – RK DEVICE	PANORAMA		t, j t
Panorama 🗸											5
C Access Domain	9										2 items
Authentication Profile						AU	THORIZATION			DEVICES/VIRTUAL	REFEREN
Authentication Sequence		NAME 🛋		DESCRIPTIO	N	co	DE	SW VERSION	MASTER DEVICE	SYSTEM	TEMPLAT
Data Redistribution		Shared									
Device Quarantine		C dev	-dø								k8s-stack
Managed Devices		(E) der	~ 6								
💮 Templates 🛛 😓 🔹											
Device Groups											
Managed Collectors											
Collector Groups											
Certificate Management											
Certificate Profile											
SSL/TLS Service Profile	¢										
SCEP											
SSH Service Profile											
R Log Ingestion Profile											
Log Settings											
Server Profiles											
SNMP Trap											
Email											
HTTP											
RADIUS											
C SCP											

Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_CG_NAME est identique au nom du collecteur de journaux que vous avez créé.

	DASHBOA	RD ACC	MONITOR	C Device	Groups n OBJECTS	C Templates		PANORAMA	्≢ र क
Panorama 🗸									
C Access Domain	0								1 i
Re Authentication Profile							In the second	Lavi Faranz	
Authentication Sequence			REDUI	NDANCY ENABLE	FOI	KWARD TO ALL COLLE	ECTORS 0	COLLECTORS	LOG REDISTRIBUTIO
User Identification	rp-cg1							demo-panorama	none
Data Redistribution									
B Device Quarantine									
Managed Devices									
Templates									
Device Groups									
Managed Collectors									
Collector Groups									
Certificate Management									
Certificates									
Certificate Profile									
SSL/TLS Service Profile									
SCEP									
SSH Service Profile									
Log Ingestion Profile									
Log Settings									
Server Profiles									
SNMP Trap									
Syslog									
Email									
B HTTP									
Th RADIUS									
ID SCP									

Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.



STEP 4 | Déployez le service CN-NGFW. Effectuez les étapes suivantes :

Lorsqu'elles sont déployées en tant que service Kubernetes, les instances du pod CN-NGFW peuvent être déployées sur des nœuds de sécurité et le trafic du pod d'application est redirigé vers une instance CN-NGFW disponible pour inspection et application.



Lors du déploiement du pare-feu CN-Series dans OKE en tant que service Kubernetes, vous pouvez utiliser les fichiers yaml du dossier natif pan-cn-k8s-service.



- Vérifiez que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml. Consultez Création de comptes de service pour l'authentification des clusters.
- 2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez kubectl pour exécuter le fichier pan-cn-ngfw-svc.yaml.

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



Ce fichier yaml doit être déployé avant pan-cni.yaml.

4. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 5. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 6. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)\$	kubectl get pods	-n kube-system	grep pan-cni
pan-cni-nmqkf		Running 0	2m11s		
pan-cni-wjrkq		Running 0	2m11s		
pan-cni-xrc2z		Running 0	2m12s		
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(v	eries-mktplace)\$			

STEP 5 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

1. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt-configmap d'OKE.

apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmtconfig 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-</pre> template-stack>" PAN CGNAME: "<panorama-collector-group>" PAN CTNR MODE TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER NAME: "<Cluster name>" #PAN PANORAMA IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between panmgmt and pan-ngfw #IPSEC CERT BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT pod with GTP enabled. For complete functionality, need GTP # enable at Panorama as well. #PAN GTP ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. # Refer to the system requirements documentation to see the max supported NGFW CPU size # supported for each memory

profile. #PAN_NGFW_MEMORY: "6.5Gi" #PAN_NGFW_MEMORY: "48Gi"
#PAN_NGFW_MEMORY: "56Gi"

Exemple pan-cn-mgmt-dynamic-pv.yaml

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

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

2. Utilisez Kubectl pour exécuter les fichiers yaml.

```
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
```

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de compte de service pour l'authentification de cluster.

3. Vérifiez que les pods CN-MGMT sont opérationnels en exécutant la commande suivante :

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

Cela prend environ 5-6 minutes.

- **STEP 6** | Déployez les pods CN-NGFW.
 - 1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

kubectl apply -f pan-cn-ngfw.yaml

4. Vérifiez que les pods CN-NGFW sont en cours d'exécution.

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

STEP 7 | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

kubectl -n kube-system get pods

STEP 8 | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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



Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire

STEP 9 | Déployez votre application dans le cluster.

Déployer le pare-feu CN-Series en tant que DaemonSet dans OKE

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.2.x or above Container Images Panorama sous PAN-OS 10.2.x ou version supérieure Helm 3.6 or above version client pour le déploisement CN Series à l'aide de Helm

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que Daemonset dans la plateforme OKE :



Le système d'exploitation Oracle Linux 8.5 est le seul environnement qualifié pour le déploiement du pare-feu CN-Series dans OKE.

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans OKE, procédez comme suit :

1. Connectez-vous à Oracle Cloud Infrastructure.

CLE Cloud Infrastructure

SIGN IN
Signing in to cloud tenant: Change tenant
Sign in with your Oracle Cloud Infrastructure credentials
USER NAME
PASSWORD
Sign In Forgot password?

- 2. Cliquez sur le menu de navigation, accédez à Under Solutions and Platform (Solutions et plateforme inférieures), puis cliquez sur Developer Services (Services aux développeurs).
- 3. Cliquez sur Kubernetes Clusters (Clusters Kubernetes).
- 4. Sélectionnez un compartiment et cliquez sur Create Cluster (Créer un cluster).

RACLE Cloud

ſS	Clusters in Tutorial2 Compartment									
' S	() S	Clusters Requiremen	ts: Preparing for Contain	ner Engine for Kut	ernetes					
ре	Create	e Cluster								
ENT	Name	Status	Node Pools	VCN	Version	Cre				
2			No clusters exis	t. Create one to ge	et started.					
oot)/Tutomaiz										

and Privacy	Cookie Preferences	Copyright © 2019, Oracle and/or it

- 5. Dans la boîte de dialogue Create Cluster (Créer un cluster), cliquez sur Custom Create (Création personnalisée), puis sur Launch Workflow (Lancer le flux de production).
- 6. Sur la page Create Cluster (Créer un cluster), entrez le Name (Nom) du cluster et d'autres détails.
- 7. Cliquez sur Next (Suivant) pour vérifier les détails que vous avez saisis pour le nouveau cluster.
- 8. Sur la page Réviser, cliquez sur Create Cluster (Créer un cluster).

RACLE Cloud

er Creation

Reso	ources	s to be created		
Ba	sic Inf	ormation		
Clus	ster Na	me: cluster1		
Con	npartme	ent: Tutorial2		
Vers	sion: v1	.18.10		
Ne	twork			
Com	npartme	nt: Tutorial2	Network Security Groups:	Not Enabled
VCN Nam	l le:	oke-vcn-quick- cluster1-4baf5729a	Kubernetes API Private Endpoint:	Auto Assigned
			Kubernetes API Public	Auto
			Enupoint.	

and Privacy Cookie Preferences

Copyright © 2019, Oracle and/or its

 \bigcirc US West (Phoenix) \checkmark

<u>ل</u>ً



Si votre cluster se trouve sur OKE, assurez-vous d'activer l'API Network Policy de Kubernetes pour permettre à l'administrateur du cluster d'indiquer quels pods sont autorisés à communiquer entre eux. Cette API est requise pour permettre aux pods CN-NGFW et CN-MGMT de communiquer.

create a Rubernetes cluster		
CPU platform and GPU		
Auto-upgrade: On	← Create a Kubernetes	s cluster
More options		Hotematica
		VPC cative
L data a da se d		Enable VPC-native (using alias IP) (i)
+ Add node pool		Betanti 💮
		default
Enable Cloud Run for Anthos		
		Noda subnet iii
➢ Availability, networking, security, and additional fea	tures	Automatically create secondary ranges
		Exemple: 10.96.0.0/14
		Maximum peca per node (Dational)
		110
		Mask for Pod address range per node: 724
		Service address range (Opticna)
		Example: 10.94.0.0/18
		Cnable Intransite visibility @ Breveals your intransite to Society in setunding table: To get logs, your even to enable VPC For Work and the Society in t
		Lood balancing
		C Enable HTTP icad bulancing 🛞
		Network acounty
		 Private cluster
		 Enable master authorized networks
		Z Englis options policy ()

Vérifiez que le cluster dispose des ressources adéquates. Assurez-vous que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu.

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et évolutivité de CN-Series.

Assurez-vous d'avoir les informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Cluster Definition				?				
	Name	on_prem-clstr						
Des	cription							
API server	r address 10.2.							
Type Native-Kubernetes								
Credent	ials			i.				
Label Selector La	bel Filte	r Custom C	ertificate					
Q				$_{0 \text{ items}} \rightarrow \times$				
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	APPLY ON				
+ Add - Delete								
Validate				OK Cancel				

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

Pour plus d'informations, consultez Configurer le plug-in Kubernetes pour la surveillance des clusters.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe du collecteur de journaux à partir de Panorama.

Collector Group		0
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion	
Name	rp-cg1	
Log Storage	Total: 1.53 TB,Free: 75.30 GB	
Min Retention Period (days)	[1 - 2000]	
Collector Group Members	Q(1item →	\times
	COLLECTORS	
	rpgcpnew(RPGOOGGKEPRA1)	
\sim		
	↔ Add	
	Enable log redundancy across collectors	
	Forward to all collectors in the preference list	
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'	
	OK Cance	el

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.

Vous devez remplacer le chemin d'accès de l'image dans les fichiers YAML pour inclure le chemin d'accès à votre répertoire privé Google Container et fournir les paramètres requis. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.

STEP 4 | Déployez le DaemonSet CNI.

Le conteneur CNI est déployé comme un DaemonSet (un pod par nœud) et il crée deux interfaces sur le pod CN-NGFW pour chaque application déployée sur le nœud. Lorsque vous utilisez les commandes

kubectl pour exécuter les fichiers YAML pan-cni, il devient une partie de la chaîne de service sur chaque nœud.



- 1. Le pare-feu CN-Series nécessite trois comptes de service avec les autorisations minimales qui l'autorisent à communiquer avec les ressources de votre cluster Kubernetes. Vous devez créer des comptes de service pour l'authentification de cluster avec CN-Series et vérifier que vous avez créé le compte de service à l'aide de pan-cni-serviceaccount.yaml.
- 2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 4. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 5. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	<pre>\$ kubect1</pre>	get pods	-n kul	be-system	grep	pan-cni
pan-cni-nmqkf		Running	0	2m11s				
pan-cni-wjrkq		Running	0	2m11s				
pan-cni-xrc2z		Running	0	2m12s				
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	\$					

STEP 5 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

1. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt-configmap

apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmtconfig 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-</pre> template-stack>" PAŇ CGNAME: "<panorama-collector-group>"#Nonmandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #IPSEC CERT BYPASS: "" # No values needed # Override autodetect of jumbo-frame mode and force enable system-wide #PAN JUMBO FRAME ENABLED: "true" # Start MGMT pod with GTP enabled. For complete functionality, need GTP # enable at
Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. # Refer to the system requirements documentation to see

the max supported NGFW CPU size # supported for each memory
profile. #PAN_NGFW_MEMORY: "6.5Gi" #PAN_NGFW_MEMORY: "48Gi"
#PAN_NGFW_MEMORY: "56Gi"

Exemple pan-cn-mgmt-dynamic-pv.yaml

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

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

2. Utilisez Kubectl pour exécuter les fichiers yaml.

```
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
```

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de comptes de service pour l'authentification de cluster avec CN-Series.

3. Vérifiez que les pods CN-MGMT sont activés.

Cela prend environ 5-6 minutes.

Utilisez kubectl get pods -l app=pan-mgmt -n kube-system NOM PRÊT ÉTAT REDÉMARRE AGEpan-mgmt-sts-0 1/1 Fonctionnement 0 27hpan-mgmt-sts-1 1/1 Exécution 0 27h

STEP 6 | Déployez les pods CN-NGFW.

Par défaut, le pod CN-NGFW du plan de données du pare-feu est déployé comme un DaemonSet. Une instance du pod CN-NFGW peut sécuriser le trafic pour un maximum de 30 pods d'application sur un nœud.

1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

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

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

kubectl apply -f pan-cn-ngfw.yaml

4. Vérifiez que tous les pods CN-NGFW sont en cours d'exécution (un par nœud dans votre cluster)

Il s'agit d'un exemple de résultat provenant d'un cluster de 4 nœuds sur site.

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>

pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none> **STEP 7** | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

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

- 0 27hpan-cni-5fhbg 1/1 En cours d'exécution
- 0 27hpan-cni-9j4rs 1/1 En cours d'exécution
- 0 27hpan-cni-ddwb4 1/1 En cours d'exécution
- 0 27hpan-cni-fwfrk 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-j62rk 1/1 En cours d'exécution
- 0 27hpan-cni-lmxdz 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-0 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-1 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-8g5xb 1/1 En cours d'exécution
- 27hpan-ngfw-ds-qsrm6 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-vqk7z 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-zncqg 1/1 En cours d'exécution
- **STEP 8** | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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

Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire

STEP 9 | Déployez votre application dans le cluster.

TECH**DOCS**

Déployer le pare-feu CN-Series dans EKS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?				
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version 				
	supérieure				
	Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm				

Après avoir examiné les blocs de construction CN-Series et la présentation générale du flux de travail dans Sécuriser les environnements Kubernetes avec CN-Series , vous pouvez commencer à déployer les pare-feu CN-Series sur la plate-forme AWS EKS pour sécuriser le trafic entre les conteneurs au sein du même cluster, ainsi qu'entre les conteneurs et d'autres types de charges de travail tels que les machines virtuelles et les serveurs bare-metal.



Vous avez besoin d'outils Kubernetes standard tels que kubectl ou Helm pour déployer et gérer vos applications, vos services pare-feu et vos clusters Kubernetes.

Pour plus d'informations, consultez Déployer des pare-feu CN-Series avec des graphiques et des modèles Helm. Panorama n'est pas conçu pour être utilisé comme orchestrateur pour le déploiement et la gestion de clusters Kubernetes. Les modèles pour la gestion des clusters sont fournis par les fournisseurs de Kubernetes gérés. Palo Alto Networks fournit des modèles pris en charge par la communauté pour le déploiement CN-Series avec Helm et Terraform.

- Déploiement du pare-feu CN-Series en tant que service Kubernetes dans AWS EKS
- Déploiement du pare-feu CN-Series en tant que DaemonSet dans AWS EKS
- Déployer le pare-feu CN-Series à partir d'AWS Marketplace



Avant de passer du déploiement de CN-Series en tant que DaemonSet à CN-Series en tant que service ou vice versa, vous devez supprimer et réappliquer pluginserviceaccount.yaml. Pour plus d'informations, consultez Créer des comptes de service pour l'authentification des clusters.

- Lorsque vous déployez CN-Series en tant que DaemonSet dans EKS, lepan-plugincluster-mode-secret ne doit pas exister.
- Lorsque vous déployez CN-Series en tant que service Kubernetes dans EKS, lepanplugin-cluster-mode-secret doit être présent.

Déploiement du pare-feu CN-Series en tant que service Kubernetes dans AWS EKS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que service Kubernetes.

Avant de commencer, assurez-vous que la version du fichier YAML CN-Series est compatible avec la version PAN-OS.

- PAN-OS 10.1.2 ou version ultérieure nécessite YAML 2.0.2
- PAN-OS 10.1.0 et 10.1.1 nécessitent YAML 2.0.0 ou 2.0.1

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans AWS EKS, procédez comme suit :

1. Cliquez sur le menu de navigation Services, accédez à Containers (Conteneurs)->Elastic Kubernetes Service (Service Elastic Kubernetes).



- 2. Cliquez sur Create Cluster (Créer un cluster).
- 3. Renseignez les détails requis, puis cliquez sur Create (Créer).

configure cluster	configure cluster
Step 2 Specify networking	Cluster configuration Info
Step 3 Configure logging	Name - Net-effloble after creation. Enter a unique name for this cluster.
Step 4 Review and create	Kubernetes version infe Setext the Kubernetes wersion for this cluster. 1.21 Cluster Service Role info - Net edition after crossion. Setext the IAM Mate to allow the Kubernetes control plane to manage AWS resources on your behalf. To cruste a new role, go to the IAM console. To cruste a new role, go to the IAM console. To cruste a new role, go to the IAM console. To cruste a new role, go to the IAM console. The material method, scorets encryption nember Conservation of Kubernetes scorets using KMS Enable envelope encryption of Kubernetes scorets using KMS Enable envelope encryption of Kubernetes scorets using KMS Enable envelope and additional lips of encryption for your Kubernetes scorets.
	Tags (0) into This cluster does not have any tags. Add tag
	This duster does not have any tags. Add tag

1. Vérifiez que le cluster dispose des ressources adéquates. Assurez-vous que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu :

kubectl	get nodes
kubectl	<pre>describe node <node-name></node-name></pre>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et mise à l'échelle de CN-Series.

Assurez-vous d'avoir les informations suivantes :

- Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama. Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.
- Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe du collecteur de journaux à partir de Panorama.
- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- **STEP 2** (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.

Vous devez remplacer le chemin d'accès de l'image dans les fichiers YAML pour inclure le chemin d'accès à votre registre privé et fournir les paramètres requis. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.

- **STEP 4** | Mettez à jour la classe de stockage. Pour prendre en charge CN-Series déployé sur AWS Outpost, vous devez utiliser le pilote de stockage aws-ebs-csi-driver, qui garantit qu'Outpost extrait les volumes d'Outpost lors de la création dynamique de volume persistant (PV).
 - 1. Appliquez le yaml suivant.

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

2. Vérifiez que le contrôleur ebs-sc est en cours d'exécution.

kubectl -n kube-system get pods

3. Mettez à jour pan-cn-storage-class.yaml pour qu'il corresponde à l'exemple ci-dessous.

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

4. Ajoutez **storageClassName: ebs-sc** à pan-cn-mgmt.yaml aux emplacements indiqués ci-dessous.

```
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 # change this to 200Gi while using storageClassName for better disk iops - metadata: name: varlogpan spec: #storageClassName: pan-cn-storage-class //For better disk iops performance for dp logs accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage: 20Gi # change this to 200Gi while using storageClassName for better disk iops - 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 | Si vous utilisez l'autoscaling dans votre environnement Kubernetes, procédez comme suit :

- Déployez l'adaptateur Amazon CloudWatch Metrics pour Kubernetes dans votre cluster CN-Series en tant que service. Vous devez autoriser CloudWatch à accéder complètement aux deux rôles IAM associés à vos pods et clusters Kubernetes. Pour publier les métriques personnalisées dans CloudWatch, le rôle des nœuds esclaves doit disposer de la politique gérée par AWS CloudWatchAgentServerPolicy afin que la fonction HPA puisse les récupérer.
- **2.** Téléchargez les fichiers yaml HPA spécifiques à EKS à partir du référentiel GitHub de Palo Alto Networks.
- **3.** Si votre CN-MGMT est déployé dans un espace de noms personnalisé, mettez à jour pan-cnadapater.yaml avec l'espace de noms personnalisé. L'espace de noms par défaut est **kube-system**.

- 4. Modifiez pan-cn-hpa-dp.yaml et pan-cn-hpa-mp.yaml.
 - 1. Entrez le nombre minimal et maximal de réplicas.
 - 2. (Facultatif) Modifiez les valeurs de fréquence de mise à l'échelle et de montée en puissance en fonction de votre déploiement. Si vous ne modifiez pas ces valeurs, les valeurs par défaut sont utilisées.
 - **3.** Copiez la section suivante pour chaque métrique que vous souhaitez utiliser pour la mise à l'échelle.

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

- 4. Modifiez le nom de la métrique que vous souhaitez utiliser et définissez **averageValue** sur le seuil décrit dans le tableau ci-dessus. Si vous ne modifiez pas ces valeurs, les valeurs par défaut sont utilisées.
- 5. Enregistrez vos modifications.

Pour plus d'informations, consultez Autoscaling horizontal des pods.

- 5. Déployez les fichiers yaml HPA. Les fichiers doivent être déployés dans l'ordre décrit ci-dessous.
 - 1. Utiliser Kubectl pour exécuter le fichier pan-cn-adapter.yaml

kubectl apply -f pan-cn-adapter.yaml

2. Utiliser Kubectl pour exécuter le fichier pan-cn-externalmetrics.yaml

kubectl apply -f pan-cn-externalmetrics.yaml

3. Utiliser Kubectl pour exécuter le fichier pan-cn-hpa-dp.yaml

kubectl apply -f pan-cn-hpa-dp.yaml

4. Utiliser Kubectl pour exécuter le fichier pan-cn-hpa-mp.yaml

kubectl apply -f pan-cn-hpa-mp.yaml

6. Vérifiez votre déploiement.

Utilisez kubectl pour vérifier que le pod d'adaptateur de mesures personnalisées dans l'espace de noms de mesures personnalisées.

kubectl get pods -n custom-metrics

Utilisez kubectl pour rechercher la ressource HPA.

kubectl get hpa -n kube-system

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

STEP 6 | Déployez le service CN-NGFW.

- Vérifiez que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml. Consultez Création de comptes de service pour l'authentification des clusters.
- 2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

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

3. Utilisez kubectl pour exécuter le fichier pan-cn-ngfw-svc.yaml.

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

Ce fichier yaml doit être déployé avant pan-cni.yaml.

4. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 5. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 6. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

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



STEP 7 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

- 1. (Requis uniquement pour les PV provisionnés statiquement) Déployez les volumes persistants (PV) pour le StatefulSet CN-MGMT.
 - 1. Créez les répertoires qui correspondent aux noms des volumes locaux définis dans le fichier pan-cn-pv-local.yaml.

Vous avez besoin de six (6) répertoires sur au moins 2 nœuds esclaves. Connectez-vous à chaque nœud esclave sur lequel le StatefulSet CN-MGMT sera déployé pour créer les

répertoires. Par exemple, pour créer des répertoires nommés /mnt/pan-local1 vers /mnt/pan-local6, utilisez la commande :

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

2. Modifiez pan-cn-pv-local.yaml.

Faites correspondre le nom d'hôte sous **nodeaffinity**, et vérifiez que vous avez modifié les répertoires que vous avez créés ci-dessus dans **spec.local.path** puis déployez le fichier pour créer une nouvelle storage class pan-local-storage et des PV locaux.

2. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt-configmap de l'EKS.

apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmtconfig 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-</pre> template-stack>" PAN_CGNAME: "<panorama-collector-group>" # ctnr mode: "k8s-service", "k8s-ilbservice" PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME: "<Cluster name>" #PAN PANORAMA IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between panmgmt and pan-ngfw #IPSEC_CERT BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT pod with GTP enabled. For complete functionality, need GTP # enable at Panorama as well. #PAN GTP ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. #PAN_NGFW_MEMORY="6Gi" #PAN_NGFW_MEMORY="40Gi" # For enabling faster datapath - AF_XDP, default is AF_PACKETV2. This requires kernel support. #PAN DATA MODE: "next-gen" #HPA params #PAN CLOUD: "EKS" #PAN NAMESPACE EKS: "EKSNamespace" #PUSH INTERVAL: "15" #time interval to publish metrics to AWS cloudwatch

Exemple de pan-cn-mgmt.yaml

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

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy: FallbackToLogsOnError 3. Utilisez Kubectl pour exécuter les fichiers yaml.

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

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de compte de service pour l'authentification de cluster.

4. Vérifiez que les pods CN-MGMT sont activés.

Cela prend environ 5-6 minutes.

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

- **STEP 8** | Déployez les pods CN-NGFW.
 - 1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

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

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

kubectl apply -f pan-cn-ngfw.yaml

4. Vérifiez que les pods CN-NGFW sont en cours d'exécution.

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

- **STEP 9** Activer la mise à l'échelle automatique horizontale du pod sur CN-Series.
- **STEP 10** | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

kubectl -n kube-system get pods

STEP 11 | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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



Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire

STEP 12 | Déployez votre application dans le cluster.

Déploiement du pare-feu CN-Series en tant que DaemonSet dans AWS EKS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?				
CN-Series déploiement	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm 				

Procédez comme suit pour déployer le pare-feu CN-Series en tant que dameonset dans AWS EKS :

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans AWS EKS, procédez comme suit :

1. Cliquez sur le menu de navigation Services, accédez à Containers (Conteneurs)->Elastic Kubernetes Service (Service Elastic Kubernetes).



- 2. Cliquez sur Create Cluster (Créer un cluster).
- 3. Renseignez les détails requis, puis cliquez sur Create (Créer).

Configure cluster	Configure cluster
Step 2 Specify networking	Cluster configuration Info
Step 3 Configure logging	Name - Not editable after creation. Enter a unique name for this cluster.
Step 4 Review and create	LutaterES1 Kubernets version info Seter the Kubernets version for this duster. 1.21 Cluster Service Role Info- Not estable ofter creation. Seter the WA Role Info- Not estable of the create in the WA resources on your behalf. Seter the WA Role Info- Not estable of the Complex. Seter the WA Role Info- Not estable of the VA resources on your behalf. Seter the WA Role Info- Not estable of the VA resources on your behalf. Seter the WA Role Info- Not estable of the VA resources on your behalf.
	One enabled, sovets encryption cannot be modified or removed.
	Tags (0) Info
	Add tag Remaining tags available to add: 50

Vérifiez que le cluster dispose des ressources adéquates. Assurez-vous que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu.

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et mise à l'échelle de CN-Series.

Assurez-vous d'avoir les informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Cluster Definition					0
	Name	on_prem-clstr			
Des	cription				
API server	address	10.2.			
	Туре	Native-Kubernet	es		
Credent	ials				Î.
Label Selector La	bel Filte	er Custom C	ertificate		
Q					$_{0 \text{ items}} \rightarrow \times$
TAG PREFIX NAMES		PACE	LABEL SELECTOR ACE FILTER		APPLY ON
(+) Add (-) Delete					
Validate					OK Cancel

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

Pour plus d'informations, consultez Configurer le plug-in Kubernetes pour la surveillance des clusters.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe du collecteur de journaux à partir de Panorama.

Collector Group	0
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item)→X
	COLLECTORS
	rpgcpnew(RPGOOGGKEPRA1)
Le.	
	↔ Add ⊖ Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list Frable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez le code d'autorisation et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.

Vous devez remplacer le chemin d'accès de l'image dans les fichiers YAML pour inclure le chemin d'accès à votre répertoire privé Google Container et fournir les paramètres requis. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml de déploiement CN-Series.

STEP 4 | Déployez le DaemonSet CNI.

Le conteneur CNI est déployé comme un DaemonSet (un pod par nœud) et il crée deux interfaces sur le pod CN-NGFW pour chaque application déployée sur le nœud. Lorsque vous utilisez les commandes kubectl pour exécuter les fichiers YAML pan-cni, il devient une partie de la chaîne de service sur chaque nœud.

1. Le pare-feu CN-Series nécessite trois comptes de service avec les autorisations minimales qui l'autorisent à communiquer avec les ressources de votre cluster Kubernetes. Vous devez créer

Création d'un compte de service pour l'authentification du cluster et vérifier que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml.

2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 4. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 5. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)	<pre>\$ kubect1</pre>	. get pods	-n kube-syste	em gre	p pan-cni
pan-cni-nmqkf		Running	0	2m11s			
pan-cni-wjrkq		Running	0	2m11s			
pan-cni-xrc2z		Running	0	2m12s			
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	eries-mktplace)	\$					

- **STEP 5** | Mettez à jour la classe de stockage. Pour prendre en charge CN-Series déployé sur AWS Outpost, vous devez utiliser le pilote de stockage aws-ebs-csi-driver, qui garantit qu'Outpost extrait les volumes d'Outpost lors de la création dynamique de volume persistant (PV).
 - 1. Appliquez le yaml suivant.

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

2. Vérifiez que le contrôleur ebs-sc est en cours d'exécution.

kubectl -n kube-system get pods

3. Mettez à jour pan-cn-storage-class.yaml pour qu'il corresponde à l'exemple ci-dessous.

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

4. Ajoutez **storageClassName: ebs-sc** à pan-cn-mgmt.yaml aux emplacements indiqués ci-dessous.

```
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 # change this to 200Gi while using storageClassName
for better disk iops - metadata: name: varlogpan spec:
#storageClassName: pan-cn-storage-class //For better disk
iops performance for dp logs accessModes: [ "ReadWriteOnce" ]
storageClassName: ebs-sc resources: requests: storage: 20Gi #
change this to 200Gi while using storageClassName for better
disk iops - 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 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

- 1. (Requis uniquement pour les PV provisionnés statiquement) Déployez les volumes persistants (PV) pour le StatefulSet CN-MGMT.
 - 1. Créez les répertoires qui correspondent aux noms des volumes locaux définis dans le fichier pan-cn-pv-local.yaml.

Vous avez besoin de six (6) répertoires sur au moins 2 nœuds esclaves. Connectez-vous à chaque nœud esclave sur lequel le StatefulSet CN-MGMT sera déployé pour créer les répertoires. Par exemple, pour créer des répertoires nommés /mnt/pan-local1 vers /mnt/pan-local6, utilisez la commande :

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

2. Modifiez pan-cn-pv-local.yaml.

Faites correspondre le nom d'hôte sous **nodeaffinity**, et vérifiez que vous avez modifié les répertoires que vous avez créés ci-dessus dans **spec.local.path** puis déployez le fichier pour créer une nouvelle storage class pan-local-storage et des PV locaux.

2. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt-configmap de l'EKS.

Session Contents Restored apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmt-config namespace: kube-system data: PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: panmgmt-secret # Panorama settings PAN_PANORAMA_IP: "x.y.z.a" PAN_DEVICE_GROUP: "dg-1" PAN_TEMPLATE_STACK: "temp-stack-1" PAN_CGNAME: "CG-EKS" # Intended License Bundle type - "CN-X-BASIC", "CN-X-BND1", "CN-X-BND2" # based on the authcode applied on the Panorama K8S plugin" PAN_BUNDLE_TYPE: "CN-X-BND2" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME: "Clustername" #PAN_PANORAMA_IP2: "passive-secondary-ip" # Comment out to use CERTs otherwise bypass encrypted connection to etcd in pan-mgmt. # Not using CERTs for etcd due to EKS bug ETCD_CERT_BYPASS: "" # No value needed # Comment out to use
CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw # IPSEC_CERT_BYPASS: "" # No values needed

Exemple de pan-cn-mgmt.yaml

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

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

3. Utilisez Kubectl pour exécuter les fichiers yaml.

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

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de comptes de service pour l'authentification de cluster avec le pare-feu CN-Series.

4. Vérifiez que les pods CN-MGMT sont activés.

Cela prend environ 5-6 minutes.

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

NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1 Running 0 27hpan-mgmt-sts-1 1/1 Running 0 27h

STEP 7 | Déployez les pods CN-NGFW.

Par défaut, le pod CN-NGFW du plan de données du pare-feu est déployé comme un DaemonSet. Une instance du pod CN-NFGW peut sécuriser le trafic pour un maximum de 30 pods d'application sur un nœud.

1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

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

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

kubectl apply -f pan-cn-ngfw.yaml

4. Vérifiez que tous les pods CN-NGFW sont en cours d'exécution (un par nœud dans votre cluster)

Il s'agit d'un exemple de résultat provenant d'un cluster de 4 nœuds sur site.

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>

pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none> **STEP 8** | Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

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

- 0 27hpan-cni-5fhbg 1/1 En cours d'exécution
- 0 27hpan-cni-9j4rs 1/1 En cours d'exécution
- 0 27hpan-cni-ddwb4 1/1 En cours d'exécution
- 0 27hpan-cni-fwfrk 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-h57lm 1/1 En cours d'exécution
- 0 27hpan-cni-j62rk 1/1 En cours d'exécution
- 0 27hpan-cni-lmxdz 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-0 1/1 En cours d'exécution
- 0 27hpan-mgmt-sts-1 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-8g5xb 1/1 En cours d'exécution
- 27hpan-ngfw-ds-qsrm6 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-vqk7z 1/1 En cours d'exécution
- 0 27hpan-ngfw-ds-zncqg 1/1 En cours d'exécution
- **STEP 9** Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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

Sur certaines plateformes, les pods de l'application peuvent démarrer lorsque le pan-cni n'est pas actif dans la chaîne de plug-ins CNI. Pour éviter de tels scénarios, vous devez spécifier les volumes comme indiqué ici dans le pod d'application YAML.

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type: Répertoire

STEP 10 | Déployez votre application dans le cluster.

Déployer le pare-feu CN-Series à partir d'AWS Marketplace

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?							
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure Helm 3.6 or above version client pour le déploiement CN-Series avec Helm 							

Vous pouvez concéder sous licence votre pare-feu CN-Series en tant que service Kubernetes déployé dans AWS EKS via AWS Marketplace. La CN-Series peut être concédée sous licence pour un mois, un an, deux ans ou trois ans et déployée dans EKS 1.19 et versions ultérieures ou Redhat Openshift 4.7 et versions ultérieures.



Ce produit est en avant-première.

L'utilisation de cette licence nécessite que vous mettiez à jour la politique IAM attachée à votre nœud de travail Kubernetes.



Si vous utilisez une licence PAYG achetée via AWS Marketplace pour votre déploiement CN-Series, n'ajoutez pas de code d'autorisation au plug-in Panorama pour Kubernetes.

STEP 1 | Remplissez les conditions préalables suivantes.

- 1. Créez votre cluster EKS ou Redhat OpenShift.
- 2. Déployez Panorama et installez le plug-in Kubernetes.



Ignorez ces étapes si vous disposez déjà d'une instance Panorama sous licence déployée dans AWS.

- 1. Installez Panorama sur une instance Amazon EC2.
- 2. Installez le plug-in Kubernetes pour le CN-Series.
- **3.** Une fois Panorama installé, veuillez envoyer un e-mail à l'équipe CN-Series à **cn-series-aws-marketplace@paloaltonetworks.com** pour demander une licence pour votre Panorama. Veuillez inclure votre nom complet, l'adresse e-mail de votre entreprise, le nom de votre entreprise, votre numéro de bon de commande, votre nom de compte AWS et votre identifiant de compte AWS.

- **STEP 2** | Appliquez votre numéro de série et votre licence à Panorama.
 - 1. Connectez-vous à l'interface Web Panorama.
 - 2. Sélectionnez **Panorama** > **Setup** (**Configuration**) > **Management** (**Gestion**) et cliquez sur l'icône de modification ③.
 - 3. Saisissez le **Serial Number (Numéro de série)** de Panorama (fourni dans l'e-mail de confirmation de commande), puis cliquez sur **OK**.
 - 4. Sélectionnez Panorama > Licenses (Licences).
 - 5. Cliquez sur Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation.
 - 6. Saisissez le code d'autorisation de licence de gestion du pare-feu et cliquez sur **OK** pour activer la licence.
 - 7. Vérifiez que la licence de gestion du pare-feu est activée.

La section Device Management License (Licence de gestion du périphérique) apparaît et affiche la date d'émission de la licence, la date d'expiration de la licence et une description de la licence de gestion du pare-feu.

Device Management License								
Date Issued Date Expires Description	January 22, 2020 Never Device management license to manage up to 1000 devices							
License Management								
Retrieve license keys from license server Activate feature using authorization code Manually upload license key								

- **STEP 3** | Mettez à jour vos politiques IAM et associez la politique à votre nœud de travail Kubernetes.
 - 1. Connectez-vous à AWS Management Console et ouvrez la console IAM.
 - 1. Sélectionnez Policies (Politiques).
 - 2. Dans la liste des politiques, sélectionnez AWSLicenseManagerConsumptionPolicy et AWSMarketplaceMeteringRegisterUsage.
 - 3. Sélectionnez Actions puis choisissez Attach (Associer).
 - 4. Sélectionnez l'identité de votre nœud de travail à laquelle associer la politique. Après avoir sélectionné l'identité, cliquez sur **Attach policy** (**Associer la politique**).
- **STEP 4** | **Téléchargez** le **plugin-serviceaccount.yaml** et appliquez le yaml avant de déployer les graphiques Helm.

kubectl apply -f plugin-serviceaccount.yaml

- **STEP 5** | Accédez à AWS Marketplace et recherchez la liste CN-Series pour AWS Marketplace .
- **STEP 6** | Cliquez sur **Continue to Subscribe** (**Continuer pour vous abonner**).

STEP 7 | Saisissez le nombre de licences que vous souhaitez acheter. Chaque droit de licence équivaut à un vCPU utilisé par votre déploiement CN-Series.

Reportez-vous aux Exigences du système CN-Series et aux Performances et mise à l'échelle CN-Series pour obtenir des conseils sur le nombre de vCPU requis pour répondre aux besoins de votre déploiement.

- **STEP 8** | Cliquez sur **Continue to Configuration** (**Continuer la configuration**). Cela ajoute les licences à votre compte AWS.
 - 1. Sélectionnez Helm Chart (Graphique Helm) comme Fulfillment option (Option d'exécution).
 - 2. Sélectionnez la dernière version pour Software version (Version du logiciel).

< Product Detail Subscribe Configure

Configure this software

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

Helm Chart	*	Supported services Amazon EKS Amazon EKS Anywhere Self-managed Kubernetes
oftware version		

STEP 9 | Cliquez sur **Continue to Launch** (**Continuer pour lancer**).

- 1. Sélectionnez votre Launch target (Cible de lancement) : Kubernetes géré par Amazon ou Kubernetes autogéré. Le mode autogéré est déployé dans Redhat OpenShift.
- 2. Suivez les Launch instruction (Instructions de lancement) affichées dans la liste AWS Marketplace. Les instructions diffèrent en fonction de votre cible de lancement.
 - Kubernetes géré par Amazon
 - **1.** Copiez les commandes de l'étape 1 des Launch instructions (instructions de lancement).
 - 2. Mettez à jour les commandes copiées pour ajouter le nom de votre cluster.

--cluster <ENTER_YOUR_CLUSTER_NAME_HERE>

3. Exécutez la commande copiée sur votre cluster EKS.

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	1	🗇 Сору							
eksctl create iamserviceaccount \ name my-service-account \ namespace kube-system \	Ţ								

- **4.** Copiez les commandes du graphique Helm à partir de l'étape 2 des Launch instructions (Instructions de lancement).
- 5. Mettez à jour les informations d'installation de Helm pour inclure votre adresse IP Panorama, votre clé d'authentification Panorama, le nom du groupe d'appareils, le nom de la pile de modèles et le nom du groupe de collecte. Définissez cluster.deployTo sur eks.

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

- 6. Exécutez la commande d'installation helm sur votre cluster EKS après avoir mis à jour les valeurs répertoriées ci-dessus.
- Kubernetes autogéré
 - 1. Effectuez l'étape 1 des instructions de lancement pour créer un jeton de licence et un rôle IAM.

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.								
Create token								

- 2. Copiez les commandes de l'étape 2 des Launch instructions (Instructions de lancement).
- 3. Mettez à jour les commandes copiées pour ajouter la valeur du jeton.

AWSMP_TOKEN=<CREATE_TOKEN_ABOVE>

4. Exécutez la commande copiée sur votre cluster OpenShift.



- 5. Copiez les commandes du graphique Helm à partir de l'étape 3 des Launch instructions (Instructions de lancement).
- 6. Mettez à jour les informations d'installation de Helm pour inclure votre adresse IP Panorama, votre clé d'authentification Panorama, le nom du groupe

d'appareils, le nom de la pile de modèles et le nom du groupe de collecte. Définissez **cluster.deployTo** sur **openshift**.

```
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).



7. Exécutez la commande d'installation helm sur votre cluster OpenShift après avoir mis à jour les valeurs répertoriées ci-dessus.

STEP 10 | Vérifiez que la licence a été ajoutée avec succès à votre compte.

- 1. Accédez à AWS License Manager.
- 2. Sélectionnez **Granted Licenses (Licences accordées)** et recherchez la liste CN-Series pour AWS Marketplace.
- 3. Sous **Entitlements** (**Droits**), vous pouvez voir le nombre total de licences et le nombre de licences consommées.

Entitlements An entitlement is a right to use, access, or consume a	n application or resource.				
Q Search				< 1 > 🐵	
Name 🔻	Value 🗢 Max count	⊽ Usage	⊽ Units ⊽	Overages	
vCPU	-	1000	5 Count	Not Allowed	Allowed
AWS::Marketplace::Usage	Enabled	-	- None	-	Not Allowed

STEP 11 | Vérifiez que les pare-feu CN-Series apparaissent dans Panorama.

- 1. Connectez-vous à Panorama.
- 2. Pour afficher les pods CN-MGMT, sélectionnez **Panorama** > **Managed Devices** (Appareils gérés) > Summary (Résumé).

DASHBOARD A		C MONITOR	r Device POLICIES	Groups _¬ OBJECTS	Templates ر NETWORK	DEVICE PAI	E PANORAMA		Commit		
										M	1anual 🗸
Q	λ(
						IP.	IP Address				
	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IPV4			BLES	TEMPLATE	DEVICE STATE
\sim	vrp-gke5-dg (1/2 De	vices Connected): Sha	ared > vrp-gke5-dg								
	mp1 pan-mgmt-sts-0		PA-CTNR		805(10.12.0.17		Create		vrp-gke5-ts	Connected
	mp2 pan-mgmt-sts-1				8661	10.12.2.20		Create		vrp-gke5-ts	Connected

 Pour vérifier que les pods CN-NGFW sont sous licence, sélectionnez Panorama > Plugins (Plug-ins) > Kubernetes > License Usage (Utilisation de licence) et vérifiez que chaque pod a reçu un jeton de licence.

C Device Gro DASHBOARD ACC MONITOR POLICIES (IPS T Templates T DBJECTS NETWORK DEVICE PANORAMA							
Q(
NODE ID	FIREWALL POD NAME	LICENSE STATUS	NODE STATUS					
v rr-cluster-1 (3 Nodes, 3/3 Licensed)								
-rr-cluster-1-default-pool-e2d3de37-1jfz	pan-ngfw-ds-4qflb		Successfully licensed.					
			Created at: -06-11 22:30:37 UTC					
-rr-cluster-1-default-pool-e2d3de37-xhq5	pan-ngfw-ds-z5z8k		Successfully licensed.					
			Created at: -06-11 22:30:37 UTC					
-rr-cluster-1-default-pool-e2d3de37-jn8z	pan-ngfw-ds-vr8hx	✓ Successful						
			Created at: -06-11 22:30:36 UTC					

TECH**DOCS**

Déployer le pare-feu CN-Series en tant que service Kubernetes sur AliCloud (ACK)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
Déploiement CN-Series	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou PAN-OS 10.2.x

Après avoir examiné les blocs de construction principaux CN-Series et la présentation générale du flux de travail dans Sécuriser les charges de travail Kubernetes avec CN-Series , vous pouvez commencer à déployer le pare-feu CN-Series sur la plate-forme AliCloud ACK pour sécuriser le trafic entre les conteneurs au sein du même cluster, ainsi qu'entre les conteneurs et d'autres types de charges de travail tels que les machines virtuelles et les serveurs bare-metal.

Vous devez vous assurer que vous appliquez le fichier plugin-serviceaccount.yaml. Pour plus d'informations, consultez Créer des comptes de service pour l'authentification des clusters.



Lorsque vous déployez le pare-feu CN-Series en tant que service Kubernetes sur ACK, le pan-plugin-cluster-mode-secret doit être présent.

Avant de commencer, assurez-vous que la version du fichier YAML CN-Series est compatible avec la version PAN-OS. Pour plus d'informations, consultez YAML CN-Series.

Effectuez la procédure suivante pour déployer le pare-feu CN-Series en tant que service Kubernetes sur la plateforme ACK :

STEP 1 | Configurez votre cluster Kubernetes.

Pour créer un cluster dans ACK, procédez comme suit :

1. Connectez-vous à la connexion utilisateur RAM à l'aide de vos informations de connexion RAM.

RAM User Logon	
* Username	
<user>@<domain> or <user>@<alias> X Example: username@company.onaliyun.com or username@company-alias.</alias></user></domain></user>	
Next	
Logon with Alibaba Cloud Account	

- 2. Dans la barre de navigation supérieure, sélectionnez la région dans laquelle vous souhaitez créer un cluster et sélectionnez un groupe de ressources en fonction des besoins de votre entreprise.
 - La région d'un cluster ne peut pas être modifiée une fois le cluster créé.
 - Tous les groupes de ressources de votre compte sont affichés par défaut.
- 3. Recherchez Container Service pour Kubernetes dans le menu de la barre de recherche.

Ε	E C-J Alibaba Cloud 🔿 Workbench								0	Expenses	ICP	Enterprise	Support	Tickets	Ð	> <u>_</u>	٥	Ä
							1) >					Resources 3	,					
	分 Overview	Resource Manager Operation & Monitor				Container R	egistry		_									
						Container S	ervice for K	lubernetes	5			ing Found no						
						Elastic Con	tainer Instar	nce										
	My Navigation					Serverless	Container S	ervice				Quick Acces	s>					
	Recent - Cloud Service																	
	Home Console	Container Service fo	Elastic I	IP Address	Elasti	Documenta	tion (1027)	>				Poond no						
	Pesource Access M	Cloud Enterprise Ne	Contain	er Registry	File S	Container	情	Applicatio	n Real	Time Monitor								
	Resource Access m	cious cherphae real	Contain	ler negistry	rife a	Custom Co	ntainer简介				pute							
	Custom Shortcuts					容器(Cont	ainer)											
	Add Shortcut					创建Custom	Container	函数			pute							
						创建Custon	Containeri	函数		Function Com	pute							
	Cloud Architecture					API (249)												
	Generate My Architecture			ExecContai	ExecContainerCommand Elastic Container Instance													
		•				DeleteCont	ainerGroup		lastic (Container Inst	ance							
	Recommended Architecture Te	emplates				DescribeCo	ntainerLog	E	lastic (Container Inst	ance							
						RestartCon	tainer Group	E	lastic (Container Inst	ance							

4. Cliquez sur Créer un cluster Kubernetes.



5. Pour créer un cluster, vous devez configurer les paramètres logiciels, les paramètres matériels et les paramètres de base en suivant le guide de l'assistant. Pour plus d'informations sur la configuration

de ces paramètres requis, consultez Créer un cluster sur ACK. Les étapes suivantes représentent un exemple de création de cluster sur la plateforme ACK :



CN-Series sur le cloud Alibaba ACK prend en charge uniquement le plug-in réseau Terway.

• Sélectionnez VPC, plug-in réseau et vSwitch.

VPC	vpc-xiaofang (vpc-2zewk	drmhjezfcm2ibotn, 10.1 👻 💭			
	🔗 Create VPC 🔗 Plan Kub	ernetes CIDR blocks in VPC networks			
Network Plug-in	Flannel	Terway You carnot chang	e the network plug-in after	the cluster is created. 💰	How to select a network plug-i
	Kubernetes cluster				
	IPVLAN (The inclusive E	NI mode uses a combination of IPVLAN and e	BPF as the virtualization tec	hnology. Only Alibaba Clo	oud Linux is supported)
	Support for NetworkPoli	cy Policy-based network traffic control is pro			
vSwitch	Select 1~5 vSwitches. We r	ecommend that you select vSwitches in differ	rent zones to ensure high av	ailability for the cluster.	
	puir court		sogning content		10. OF 10.
	inside	vsw-2zej8ngtuyp6r6qy1eoil	Beijing Zone C	10.101.2.0/24	252
	outside	vsw-2zerc7sn6emhk9mq4lzy7	Beijing Zone C	10.101.1.0/24	252
	mgmt	vsw-2zepoq1k3a7zx1pk2iafs	Beijing Zone C	10.101.0.0/24	252
	cn-pod2	vsw-2ze5v4zny1j58rzzdd19t	Beijing Zone A	10.101.102.0/24	243

• Sélectionnez POD contre Switch.

Pod vSwitch	All Z	oneA (2 / 1)									
		protect as served									
		inside	vsw-2zej8ngtuyp6r6qy1eoil	Beijing Zone C	10.101.2.0/24	252					
		outside	vsw-2zerc7sn6emhk9mq4lzy7	Beijing Zone C	10.101.1.0/24	252					
		mgmt	vsw-2zepoq1k3a7zx1pk2iafs	Beijing Zone C	10.101.0.0/24						
	~	cn-pod2	vsw-2ze5v4zny1j58rzzdd19t	Beijing Zone A	10.101.102.0/24	252					
	~	cn-pod1	vsw-2zex1z33iu6ffu72ko5ry	Beijing Zone A	10.101.101.0/24	252					
		cn-node-ip	vsw-2ze5nzjrkzio4sbf5d2n9	Beijing Zone A	10.101.10.0/24						
	🔗 Crea	ate vSwitch									
	The prefix length of the VSwitch address is recommended to be no greater than 19 bits.										
Service CIDR	192.168	3.0.0/16	 Recommended Value:192.168.0.0/16 								
	Valid val	lues: 10.0.0.0/16-24. 1	72.16-31.0.0/16-24. and 192.168.0.0/16-24.								

• Sélectionnez Configurer SNAT, Accès au serveur API, Groupes de sécuritéet Groupe de ressources.

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 Intern
	VPC does not have a NAT gateway, ACK automatically creates a NAT gateway and configures SNAT rules. For more information, see NAT Gateway bill
Access to API Server	slb.s1.small 🗸 🖉 SLB Instance Specifications
	By default, an internal-facing SLB instance is created for the API server. You can modify the specification of the SLB instance. If you delete the SLB in
	access the API server.
	✓ 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
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. (
	PDS inclance is not in the sunning 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 r
	advanced security group. Security group overview
Deletion Protection	Enable
	Cluster Cannot Be Deleted in Console or by Calling API
Resource Group 📀	default resource group 🗾 💭
	To create a resource group, click here.

• Sélectionnez **Quantité**, **Système d'exploitation** et **Type de connexion** pour les configurations de pool de nœuds.

_												
	instance type is used. The	actual instance types used	d to create nodes are subj	ect to inventory availability	<i>ι</i> .							
	ecs.sn2nec.xlarge sn2nec)	(4 vCPU 16 GiB, General p	nce Move Up Move Down									
Quantity	2 unit(s) 🜲											
_	Nodes will be evenly assig	ned to your selected vSwit	cnes.									
	A standard managed clust	er can contain up to 100 n	odes. To use a larger clust	er, create a professional n								
System Disk	SSD Disk	▼ 120 GiB	*									
Mount Data Disk	You have selected 0 disks and can select 10 more.											
🔗 Disk Parameters and												
Performance	Add Data Disk 10	Recommended										
Operating System	Alibaba Cloud Linux 3.2	104	•									
Security	Disable	Reinforcement based o	on classified protection	CIS Reinforcement	0							
Reinforcement	1											
Logon Type	Key Pair	Password	Later									
Key Pair	key-par-Alibaba		• 0									
	You can log on to the ECC	console to create a key pa	ie.									

SACK Billing SLB Price: ¥ 0.100 /Hours EIP Price: ¥ 0.800 /GB ECS Price: ¥ 4.91 /Hours Prev:Cluster Configurations Next:Configurations

• Accédez à l'onglet Réseau public, décochez les casesDécouverte des services, Plug-in de volume et Agents de surveillance.



ACK Billing SLB Price: 0.800 m EIP Price: ¥ 0.800 /GB ECS Price: ¥ 4.91 /Hours Prev:Node Pool Confi

6. Cochez la case Conditions d'utilisation.

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 Account Balance Check Passed Account Balance Check Passed Account Balance Check Passed Service During the cluster creation process, the following operations may be performed depending on cluster configurations: • Create SCB instances, configure a public key to enable SSH logon from master nodes to other nodes, and configure the Kubernetes cluster through Cloudinit. • Create ARM role and grant Lit the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and all permissions on SLB instances. Clouddisks, Cluster and grant Lit the following permission: query, create, and delete ECS instances, cloud disks, and all permissions on SLB instances. Clouddisks, Cluster and an PAS. The Kubernetes cluster dynamically creates SLB instances, and VPC entimissions on SLB instance. • Create a RAM role and grant Lit the following permission: query, create, and delete ECS instances, cloud disks, with all permissions on SLB instances. • Create a RAM role and grant Lit the following permission: query, create, and delete cloud disks, and all permissions on SLB instances. • Creat						
bependent Service Activation Status Passed Auto Scaling Status Check Passed System Disk Size Check Passed Data Disk Size Check Passed Account Balance Check Passed Data Disk Size Check Passed Account Balance Check Passed Data Disk Size Check Passed Account Balance Check Passed Data Disk Size Check Passed <t< td=""><th></th><td>RAM Role Authorization Check</td><td>Passed</td><td></td><th></th><td></td></t<>		RAM Role Authorization Check	Passed			
Auto Scaling Status Check Passed System Disk Size Check Passed Data Disk Size Check Passed Account Balance Check Passed Balance Check Passed Account Balance Check Passed Balance Check Passed Account Passe Data Balance Check Passed Balance Check		Dependent Service Activation Status	Passed			
Service Quota Check Passed System Disk Size Check Passed Data Disk Size Check Passed Account Balance Check Passed Account Selance Check Passed Account Selance Check Passed Account Selances, configure a public key to enable SM logon from master nodes to other nodes, and configure the Kubernetes cluster through Cloudints. ************************************		Auto Scaling Status Check	Passed			
System Disk Size Check Passed Data Disk Size Check Passed Account Balance Check Passed Account Balance Check Passed as of Service During the cluster creation process, the following operations may be performed depending on cluster configurations: as of Service Create as courty group that allows access to the VPC network over ICMP. ************************************		Service Quota Check	Passed			
Data Disk Size Check Passed Account Bilance Check Passed as of Service During the cluster creation process, the following operations may be performed depending on cluster configurations: as of Service Create a Security group that allows access to the VPC network over CMM: • Create a Security group that allows access to the VPC network over CMM: • Create a Security group that allows access to the VPC network over CMM: • Create a Security group that allows access to the VPC network over CMM: • Create a Security group that allows access to the VPC network over CMM: • Create a Security group that allows access to the VPC network over CMM: • Create a Security and the dupt gremissions: cuery, create, and delete ECS instances, create and delete cloud disks, and 4D permissions on SLB instances, cloud disks, and VPC routing rules based on your creates and instances, cloud disks, and VPC routing rules based on your creates and instances and open port 644. • The cluster creation talls, the created resources will be charged. we recommend that you delete undisk resources at the trainest of nortunity. • The cluster creation talls, the created resources will be charged. we recommend that you delete undisk resources at the trainest of nortunity. • The cluster creation talls, the created resources will be charged. we recommend that you delete undisk and Disclaimer. • The cluster creation talls, the created resources will be charged. We recommend that you delete undisk for a Disclaimer.		System Disk Size Check	Passed			
Accurate Balance Check Passed as of Service Turing the cluster creation process, the following operations may be performed depending on cluster configurations: as of Service There LCSS instances, configure a public key to enable SSH logon form master nodes to other nodes, and configure the Kubernetes cluster through CloudInit. • Create ACS instances, configure a public key to enable SSH logon form master nodes to other nodes, and configure the Kubernetes cluster through CloudInit. • Create ACS instances, configure a public key to enable SSH logon form master nodes to other nodes, and configure the Kubernetes cluster through CloudInit. • Create ACM role and grant it the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and VPC routing rules based on your strateging. • Create a RSH role and grant it the following permissions: query, create, and delete ECS instances, cloud disks, and VPC routing rules based on your strateging. • Create a RSH role and grant it the following permissions: query, create, and delete ECS instances, cloud disks, and VPC routing rules based on your strateging. • Create a RSH role and grant it the following permissions: query, create, and delete ECS instances, cloud disks, and VPC routing rules based on your strateging. • Other CloudNonitor, VPC, Log Service, and NAS. The Kubernetes cluster the system collects log and monitoring information about control components on master nodes to help ensceive stability. • The clouder cleation tam, the created resources will be charged, we recommend that you devede unused resources at the clainest. • The clouder cleation tam, the created resources wi		Data Disk Size Check	Passed			
 In a of Service During the cluster creation process, the following operations may be performed depending on cluster configurations: Create a security group that allows access to the VPC network over ICM. Create a security group that allows access to the VPC network over ICM. Create a Security group that allows access to the VPC network over ICM. Create a Security group that allows access to the VPC network over ICM. Create a AAM role and grant it the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and all permissions on SLB instances, clouddholitor, VPC, Log Service, and NAS. The Kubernetes cluster dynamically creates SLB instances, cloud disks, and VPC routing rules based on your serving. Create an internal SLB instance and open port 6443. The routewer stability. If the cluster creation tails, the created resources will be charged. we recommend that you delete undeet resources at the transet of nortunity. If the cluster creation tails, the created resources will be charged. we recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the created resources will be charged. We recommend that you delete undeet account alls, the stability of th		Account Balance Check	Passed			
 as of Service During the cluster creation process, the following operations may be performed depending on cluster configurations: Create a Security group that allows access to the VPC network over ICMP. Create a Security group that allows access to the VPC network over ICMP. Create a Security group that allows access to the VPC network over ICMP. Create a Security group that allows access to the VPC network over ICMP. Create a Security group that allows access to the VPC network over ICMP. Create a Security group that allows access to the VPC network over ICMP. Create a NAT giteway and Elastic IP addresses. Create an internal SLB instances, individuel grant the forwing persistions: super, create, and delete ECS instances, cloud disks, and VPC routing rules based on your setting. Create an internal SLB instance and open port 6443. Phon 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 take, the Created resources will be charged. we recommend what you dealed ensure cluster of components on master nodes to help ensure cluster stability. If have read and understand the preceding statement. I also have read and accept the Terms of Service and Disclaimer. Max CK Billing SLB Price: V 0.8000 /rsB ECS Price: V 4.91 /Hours Prevs (0.8000 /rsB) 						
CCS Price: ¥ 4.91 /Hours Prov.	[Create VPC routing rules. Create ANT gateway and Elastic IP address Create a RAM role and grant it the following instances, CloudMonitor, VPC, Log Service, settings. Create an internal SLB instance and open pu When you use a dedicated or managed Kub ensure cluster stability. I the cluster creation tails, the created reso I have read and understand the preceding s	ses. permissions: query, create, a and NAS. The Kubernetes clu rrf 6443. rrnetes cluster, the system cc arces win ce charged. We rec tatement. I also have read an	d delete ECS instances, create and delete cloud ter dynamically creates SLB instances, cloud dis lects log and monitoring information about contro mmeno mat you delete unused resources at the laccept the Terms of Service and Disclaimer.	disks, and all permissions on SLB ks, and VPC routing rules based on your of components on master nodes to help earnest opportunity.	
O.220 /mext O.300 /me	_					
ACK Billing SLB Price: 0.800 / GB ECS Price: 4.91 / Hours Prev: 0.800 / GB ECS Price: 4.91 / Hours				0.220		
			& ACK Billing SLB Pric	EIP Price: ¥ 0.800 /GB	ECS Price: ¥ 4.91 /Hours Prev:	Com
· ····						

- 7. Cliquez sur Create Cluster (Créer un cluster).
- 8. Vérifiez la clé du serveur API pour vous connecter au cluster ACK et copiez le contenu suivant dans \$HOME/.kube/config sur votre ordinateur local.

_	_	
	< ACK-For-PM -	All Clusters / ACK-Fon-PM
	Cluster Information	ACK-For-PM
•	Nodes	
	Node Pools	Overview Basic Information Connection Information Cluster Resources Cluster Logs Cluster Tasks
	Nodes	Connect to a Kubernetes cluster using kubectl I lontal and configure lubbett. For more information, see lottell and configure lubbett
	Namespaces and Quota	2. Configure cluster credentials:
•	Workloads	Public Access Internal Access Ganerate Temporary Kubeconfig Revoke KubeCont
	Deployments	Copy the following content to \$HOME/kube/config on your local computer.
	StatefulSets	Gredentials Excite At: Jan 5. 2026. 13:32:51 UTC+8
	DaemonSets	apiVersion: v1 Cccy clusters:
	Jobs	- cluster:
	CronJobs	server: https://47.93.191.191:6443 certificate-authority-data:
	Pods	LSØELSICRUdJTIBDRVJUSUZJQØFURSØELSØECKIJSURUaKNDQWphSØF3SUJBZØIVRDUINDJE7mRRYmIIeThEQ3ByQnhLQIUJRXIZdØRRWUpLbipJaHZjTKFRRUwKQIFBdIBqRW5NQThHG
	Custom Resources	TTVRUNGTUINRUZ MYNMAZIZYXGGQYLEVIFRSUV.MMAIRAXDWYGKAZIHTININIZTV/NGMPFUVLEVIFRREVGEDJRUDBYZUIGGREWNDNQUFFRFOGEIEKGGAREXTMDHOUGDIEGEIST RJEEIGSTVNRFV5CH9EQXdXaKE:TVNjdOR3WURWUVFLRXdobllXNM51bwh2ZFRBVUJnT1ZcQM9URPGc2EXSmh2biVnWT1dmRXUXgKRXpBUKJnT1ZcQU1Q210MV1tVnlibVYwN1hNd2c
٠	Network	nRW1N97BEQ1NxR1NJYjNEUUVCQVFVQUEOSUJEdOFJ22dFSwpBb01CgvFDGGoxcsVFVVQvTn1xdXBidkloUEtRNmCoXBayjJ4VHB32lFUTe72dmFN3U0OCLMS2JmvDnNvEdtC11yYUMa akFhQVVV2GhPcTBNaklLb2xpU1RQOTBLRWQyZnVP2EU4RXE2U1p5WE11UU1xVBp2c2VNR1hYvm1x80oKNjVBWjmQsk0gXVycWF4SjJvbUJyVTmrSNxR2VQ0LytjYU1vZ09ABU5KUjhxc
•	Configurations	mniumaji karea pravima u ravo prava na karveni vysoko v na sa karveni vysoko na karveni vysoko na karveni na karveni

9. Obtenez l'adresse du terminal public du serveur API du cluster ACK.

	C-) Alibaba Cloud	යි Workbe	nch All Resources 🗸	🧬 Global 📿		Exper	ises ICP Enterpris	se Support	Tickets	₽ <u>₽</u> >_	
	< ACK-For-PM +	All Clusters /	ACK-For-PM								
	Cluster Information	ACK-F	or-PM								
•	Nodes Node Pools	Overview	Basic Information	Connection Information	Cluster Logs	Cluster Tasks					
	Nodes	Basic Info	ormation	nation							
Dra	Namespaces and Qu	uota	ClosteriDize6507ca2148a	CIRSter: D_cs577c82748a845698856383098227218a Begions-China (Beijing) Time-Sorie: Ar							
	 Workloads 		Cluster Information	Cluster Information							
	Deployments	Ξ	API Server Public Endpoir	nt	https://47.93.191	1.191:6443 Cł	hange EIP Unbind E	IP			
	StatefulSets		API Server Internal Endpo	https://10.101.10	https://10.101.10.169:6443 Set access control 🔗 Troubleshoot connection issues						
	Jobs		Service CIDR	192.168.0.0/16	192.168.0.0/16						
ds	CronJobs		RRSA OIDC		Enable RRSA	Enable RRSA SC Configure RAM permissions for service accounts to isolate permissions among					
	Pods		Kube-proxy Mode	ipvs	ipvs						
	Custom Resources		Network Plug-in	terway-eniip	terway-eniip						
	Network		Custom Certificate SANs		Update	Update					
	 Configurations 		Testing Domain		*.cdbc7ca2f48a8	*.cdbc7ca2f48a84bf898f5ac303022718e.cn-beijing.alicontainer.com Rebind Domain Name					



Vérifiez que le cluster dispose des ressources adéquates. La spécification par défaut du pool de nœuds GKE n'est pas adaptée au pare-feu CN-Series. Vous devez vous assurer que ce cluster dispose des conditions préalables de CN-Series pour prendre en charge le pare-feu :

kubectl get nodes

kubectl describe node <node-name>

Affichez les informations sous l'en-tête Capacity (Capacité) dans la sortie de la commande pour voir le processeur et la mémoire disponibles sur le nœud spécifié.

L'allocation du processeur, de la mémoire et du stockage sur disque dépendra de vos besoins. Voir Performances et évolutivité de CN-Series.

Vous devez vous assurer que vous disposez des informations suivantes :

• Collectez l'adresse IP du terminal pour configurer le serveur API sur Panorama.

Cluster Definiti	on			?
	Name	on_prem-clstr		
	Description			
API se	erver address	10.2.		
	Туре	Native-Kubernet	es	~
Cre	dentials			Â.
Label Selector	Label Filte	er Custom C	ertificate	
Q				0 items \rightarrow X
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	APPLY ON
↔ Add — Delete	2			
Validate				OK Cancel

Panorama utilise cette adresse IP pour se connecter à votre cluster Kubernetes.

• Collectez le nom de la pile de modèles, le nom du groupe d'appareils, l'adresse IP Panorama et éventuellement le nom du groupe de collecteurs de journaux à partir de Panorama.

Name	rp-cg1
Log Storage	
Collector Group Members	[1-200]
concetor or oup ritempers	
Ν.	
10	
	(→ Add) Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication

Pour plus d'informations, consultez Créer un groupe d'appareils parents et une pile de modèles.

- Collectez la clé d'authentification VM et l'ID et la valeur du code PIN d'enregistrement automatique.
- L'emplacement du conteneur d'images dans lequel vous avez téléchargé les images.
- STEP 2 | (facultatif) Si vous avez configuré un certificat personnalisé dans le plug-in Kubernetes pour Panorama, vous devez créer le secret de certificat en exécutant la commande suivante. Ne modifiez pas le nom de fichier de ca.crt. Le volume des certificats personnalisés dans pan-cn-mgmt.yaml et pan-cn-ngfw.yaml est facultatif.

kubectl -n kube-system crée un secret générique custom-ca --fromfile=ca.crt

STEP 3 | Modifiez les fichiers YAML afin de fournir les détails nécessaires au déploiement des pare-feu CN-Series.

apiVersion: v1 kind: ConfigMap metadata: name: pan-mgmtconfig namespace: kube-system data: PAN_SERVICE_NAME: panmgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panoramadevice-group>" PAN_TEMPLATE_STACK: "<panorama-template-stack>" PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8sservice"

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>"

Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_IP sur votre fichier YAML correspond à votre adresse IP Panorama réelle, comme indiqué dans le diagramme ci-dessous :

← → C ▲ Not Secure	35.196	6.181.54/# anorama:	:dev-dg::panorar	na/templates					० 🛧 🛛 🕝 🗗
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	DA	ASHBOARD AG		COR POLICIES	e Groups ¬ OBJECTS	r Templates	DEVICE	PANORAMA	tr • €•
Panorama 🗸									ť
C Access Domain	Q	C							2 items
Authentication Profile		NAME	DESCRIPTION	TYPE	STACK	DEVICES		VARIABLES	DEVICE KEY-VALUE TA
Authentication Sequence		K9S-Network-Setup		template				Manago	
User Identification		Los stade		template	KOC Matural Catura			Managem	No Devices in the stands
Data Redistribution		K6S-STACK		template-stack	K85-INetwork-Setup			Manage	No Devices in the stack
Managed Devices									
Templates									
Device Groups									
Managed Collectors									
Collector Groups									
Certificate Management									
Certificates									
Certificate Profile	1								
SSL/TLS Service Profile	1								
C SCEP									
SSH Service Profile									
R Log Ingestion Profile									
Log Settings									
Server Profiles									
SNMP Trap									
Syslog									
Email									
HTTP									
RADIUS									
LD SCP	-		-						

La dernière version des fichiers YAML est disponible sur le référentiel de Palo Alto Networks Kubernetes Security - CN Series. Vous pouvez sélectionner les dernières branches ou balises dans le menu déroulant **Commutateurde branches/balises**.

Vous devez vous assurer que la valeur des paramètres de PAN_DEVICE_GROUP et PAN_TEMPLATE sur votre fichier YAML correspond au nom du groupe d'appareils et de la pile de modèles que vous avez créés sur Panorama, comme indiqué dans le diagramme ci-dessous :

← → C ▲ Not Secure 3	85.196	6.181.54/#panor	rama::dev-dg:	:panorama/devi	ce-groups					Q \$	0 0	0 0
UM-PANORAMA	DA	ASHBOARD	ACC	MONITOR	C Device	Groups – OBJECTS	r T NETWO	emplates – RK DEVICE	PANORAMA		÷	œ 🗄
Panorama 🗸 🗸												E
C Access Domain	Q											2 items
Authentication Frome		NAME 🛋		DESCRIPTION	N	AU	THORIZATION	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM		REFEREN
Data Redistribution		G Shared										
B Device Quarantine		Ga de	v-dg									k8s-stack
Managed Devices Managed Devices Device Groups Managed Collectors Collector Groups Collector Groups Certificate Certificates Certificates Certificates Scarper Scarper Scarper Scarper Scarper Scarper Scarper Scarper Collector Groups Certificate Profile Scarper Collector Groups Scarper Scarper Scarper Collector Groups Scarper Sc	-											
ER, Log Ingestion Profile Image: Log Settings Image: Server Profiles Image: System												
C) SCP												

Vous devez vous assurer que la valeur du paramètre PAN_PANORAMA_CG_NAME est identique au nom du collecteur de journaux que vous avez créé.

					C Device	Groups –	r Templates -			
W-PANORAMA	DA	SHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK D	DEVICE	PANORAMA	ta
Panorama 🗸										
C Access Domain	Q									11
Authentication Profile		NAME		REDUN	DANCY ENABLE	. 500	WARD TO ALL COLLECT	TORS	OLLECTORS	LOG REDISTRIBUTIO
Authentication Sequence				REDON	ETTER ETTABLE		TO ALL COLLEC	. ona i		LOG REDISTRIBUTIO
User Identification	U	rp-cg1						1	demo-panorama	none
Data Redistribution										
Device Quarantine										
Managed Devices										
Templates										
E Device Groups										
Managed Collectors										
Collector Groups	11									
Certificate Management										
Certificates										
Certificate Profile										
SSL/TLS Service Profile	-									
SCEP										
SSH Service Profile										
Log Ingestion Profile										
Can Log Settings										
Server Profiles										
SNMP Trap										
Svslog										
Email										
P RADIUC										
Co co										

Pour plus d'informations, consultez Paramètres modifiables dans les fichiers yaml CN-Series.

STEP 4 | Déployez le service CN-NGFW. Effectuez les étapes suivantes :

Lorsqu'elles sont déployées en tant que service Kubernetes, les instances du pod CN-NGFW peuvent être déployées sur des nœuds de sécurité et le trafic du pod d'application est redirigé vers une instance CN-NGFW disponible pour inspection et application.

1. Vérifiez que vous avez créé le compte de service à l'aide du fichier pan-cni-serviceaccount.yaml.

Consultez Création de comptes de service pour l'authentification des clusters.

2. Utilisez Kubectl pour exécuter le fichier pan-cni-configmap.yaml.

kubectl apply -f pan-cni-configmap.yaml

3. Utilisez kubectl pour exécuter le fichier pan-cn-ngfw-svc.yaml.

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



Ce fichier yaml doit être déployé avant pan-cni.yaml.

4. Utilisez Kubectl pour exécuter le fichier pan-cni.yaml.

kubectl apply -f pan-cni.yaml

- 5. Vérifiez que vous avez modifié les fichiers YAML pan-cni et pan-cni-configmap.
- 6. Exécutez la commande suivante et vérifiez que votre sortie est similaire à l'exemple suivant.

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace) \$ }	kubectl get pods	-n kube-system	grep pan-cni
pan-cni-nmqkf		Running 0	2m11s		
pan-cni-wjrkq		Running 0	2m11s		
pan-cni-xrc2z		Running 0	2m12s		
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace)\$			



Alicloud ACK prend en charge uniquement la mise à l'échelle automatique basée sur des métriques standard.

STEP 5 | Déployez le StatefulSet CN-MGMT.

Par défaut, le plan de gestion est déployé comme un StatefulSet qui garantie la tolérance aux pannes. Jusqu'à 30 pods pare-feu CN-NGFW peuvent se connecter à un StatefulSet CN-MGMT.

- 1. (Requis uniquement pour les PV provisionnés statiquement) Déployez les volumes persistants (PV) pour le StatefulSet CN-MGMT.
 - 1. Créez les répertoires qui correspondent aux noms des volumes locaux définis dans le fichier pan-cn-pv-local.yaml.

Vous avez besoin de six (6) répertoires sur au moins 2 nœuds esclaves. Connectez-vous à chaque nœud esclave sur lequel le StatefulSet CN-MGMT sera déployé pour créer les

répertoires. Par exemple, pour créer des répertoires nommés /mnt/pan-locall à /mnt/ pan-local6, utilisez la commande suivante :

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

2. Modifiez pan-cn-pv-local.yaml.

Faites correspondre le nom d'hôte sous **nodeaffinity**, et vérifiez que vous avez modifié les répertoires que vous avez créés ci-dessus dans **spec.local.path** puis déployez le fichier pour créer une nouvelle storage class pan-local-storage et des PV locaux.



Dans le fichier pan-cn-mgmt.yaml, vous devez ajouter le nom de la classe de stockage comme alicloud-disk-available lors de la création de volumeClaimTemplates.

Par exemple :

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

La taille de stockage doit être d'au moins 20 Go pour tous les PV.

2. Vérifiez que vous avez modifié les fichiers YAML pan-cn-mgmt et pan-cn-mgmt-configmap.

Exemple de pan-cn-mgmt.yaml

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

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

3. Utilisez Kubectl pour exécuter les fichiers yaml.

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.yaml

Vous devez exécuter pan-mgmt-serviceaccount.yaml, uniquement si vous n'aviez pas déjà terminé la création de compte de service pour l'authentification de cluster.

4. Vérifiez que les pods CN-MGMT sont opérationnels en exécutant la commande suivante :

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

Cela prend environ 5-6 minutes.

STEP 6 | Déployez les pods CN-NGFW.

1. Vérifiez que vous avez modifié les fichiers YAML comme indiqué dans PAN-CN-NGFW-CONFIGMAP et PAN-CN-NGFW.

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. Utilisez l'application Kubectl pour exécuter le fichier pan-cn-ngfw-configmap.yaml.

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

3. Utilisez l'application Kubectl pour exécuter le pan-cn-ngfw.yaml.

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

4. Vérifiez que les pods CN-NGFW sont en cours d'exécution.

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

STEP 7 Vérifiez que vous pouvez voir CN-MGMT, le CN-NGFW et le PAN-CNI sur le cluster Kubernetes.

kubectl -n kube-system get pods

STEP 8 | Annotez l'application yaml ou l'espace de noms afin que le trafic de leurs nouveaux pods soit redirigé vers le pare-feu.

Vous devez ajouter l'annotation suivante pour rediriger le trafic vers le CN-NGFW pour inspection :

annotations: paloaltonetworks.com/firewall: pan-fw

Par exemple, pour tous les nouveaux pods dans l'espace de noms « par défaut :

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

STEP 9 | Déployez votre application dans le cluster.

TECH**DOCS**

Déployer CN-Series sur OpenShift

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 Déploiement CN-Series sur un environnement OpenShift 	 CN-Series 10.1.x or above Container Images Panorama sous PAN-OS 10.1.x ou une version supérieure

Le fichier pan-cni sécurise le trafic sur l'interface par défaut « eth0 » du pod de l'application. Si vous avez des pods multi-hôtes, vous pouvez configurer le pod CN-NGFW afin de sécuriser des interfaces supplémentaires qui sont configurées avec une connexion basée sur un pont pour communiquer avec d'autres pods ou avec l'hôte. En fonction de l'annotation dans le YAML de l'application, vous pouvez configurer le pare-feu CN-Series pour inspecter le trafic de toutes les interfaces ou d'un nombre sélectionné d'interfaces attachées à chaque pod.

Le pan-cni ne crée pas de réseau et n'a donc pas besoin d'adresses IP comme les autres plug-ins du CNI.



PAN-OS 10.1.3 ou version ultérieure est requis pour déployer CN-Series en tant que service Kubernetes sur OpenShift. De plus, CN-Series en tant que service Kubernetes sur OpenShift ne sécurise que l'interface **eth0**.

STEP 1 | Déployez votre cluster.

Consultez la documentation du fournisseur de la plateforme cloud et vérifiez que les versions OpenShift et CNI sont prises en charge pour CN-Series. Consultez Obtenir le fichier image pour le pare-feu CN-Series et Paramètres modifiables dans les fichiers yaml CN-Series.

STEP 2 | Utilisez le flux de travail inclus dans Sécuriser les charges de travail Kubernetes avec CN-Series.

Vous devez créer les identifiants du service, et déployer les YAML du pare-feu.



Remarque : Si votre fichier d'identification de service fait plus de 10 Ko, vous devez le compresser puis effectuer un encodage base64 du fichier compressé avant de télécharger ou de coller le contenu du fichier dans l'API ou le CLI Panorama.

STEP 3 | Configurez le plug-in PAN-CNI pour qu'il fonctionne avec le plug-in CNI Multus.

Le CNI Multus sur OpenShift fonctionne comme un « méta-plug-in » qui appelle d'autres plug-ins CNI. Pour chaque application, vous devez :

1. Déployer le PAN-CNI NetworkAttachmentDefinition dans chaque espace de noms de pod

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

2. Modifier le YAML de l'application.

Après avoir déployé le pan-cni-net-attach-def.yaml, ajoutez l'annotation dans le yaml du pod de l'application :

paloaltonetworks.com/firewall: pan-fw

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

Si vous avez d'autres réseaux dans l'annotation ci-dessus, ajoutez **pan-cni** après les réseaux qui doivent être inspectés. Les réseaux qui suivent **pan-cni** ne sont pas redirigés et inspectés.



Si votre pod possède plusieurs interfaces réseau, vous devez spécifier les noms des interfaces pour lesquelles vous souhaitez que le pod CN-NGFW inspecte le trafic, sous « interfaces » dans le fichier pan-cni-configmap.yaml.

Par exemple :

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



CN-Series prend désormais en charge le plug-in OVN-Kubernetes Container Network Interface (CNI) sur RedHat OpenShift version 4.13 et ultérieure, en mode de déploiement Kubernetes Service et en mode DaemonSet.
TECH**DOCS**

Déployer CN-Series sur le hub de l'opérateur OpenShift

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?						
Déploiement CN-Series	• CN-Series 10.1.x or above Container Images						
	Panorama sous PAN-OS 10.2.x et version supérieure						

Le pare-feu de conteneur CN-Series est maintenant disponible sur hub de l'opérateur de la plate-forme RedHat Openshift. Vous pouvez déployer, configurer et exploiter des pare-feu de conteneurs CN-Series directement depuis le hub de l'opérateur RedHat.

Prérequis pour CN-Series sur le hub de l'opérateur Openshift :

Voici les conditions préalables au déploiement du pare-feu CN-Series sur le hub de l'opérateur Openshift :

- Mettre sous licence le pare-feu CN-Series. La mise sous licence du pare-feu CN-Series est gérée par le plug-in Kubernetes sur Panorama. Générez votre code d'autorisation et gardez-le à portée de main lorsque vous êtes prêt à déployer le pare-feu CN-Series. Pour plus d'informations, voir Mettre sous licence le pare-feu CN-Series.
- Générez la clé d'authentification VM sur Panorama.
- Installez un certificat de périphérique sur le pare-feu CN-Series.
- Créez des comptes de service pour l'authentification des clusters.
- Déployer Panorama : vous devez utiliser Panorama pour configurer, déployer et gérer le déploiement de votre pare-feu CN-Series. Pour plus d'informations sur le déploiement et la configuration d'un appareil Panorama, voir Configurer Panorama.
- Installez le plug-in Kubernetes pour le pare-feu CN-Series.
- Le cluster OpenShift doit respecter les conditions préalables de CN-Series.
- Assurez-vous d'avoir accès au portail de service à la clientèle (CSP) de Palo Alto Networks et d'avoir des crédits Flex.
- Assurez-vous que vous êtes un client RedHat avec une licence OpenShift et un compte qui a les autorisations pour créer des ressources dans OpenShift.
- Assurez-vous que le cluster OpenShift respecte les conditions préalables de CN-Series.

Pour plus d'informations, voir Comment déployer facilement CN-Series sur le hub de l'opérateur RedHat Openshift.

Déployer CN-Series sur un hub de l'opérateur OpenShift :

Le fichier pan-cni sécurise le trafic sur l'interface par défaut **eth0** du pod de l'application. Si vous avez des pods multi-hôtes, vous pouvez configurer le pod CN-NGFW afin de sécuriser des interfaces supplémentaires qui sont configurées avec une connexion basée sur un pont pour communiquer avec d'autres pods ou avec l'hôte. En fonction de l'annotation dans le YAML de l'application, vous pouvez

configurer le pare-feu CN-Series pour inspecter le trafic de toutes les interfaces ou d'un nombre sélectionné d'interfaces attachées à chaque pod.

Le pan-cni ne crée pas de réseau et n'a donc pas besoin d'adresses IP comme les autres plug-ins du CNI.



Vous avez besoin de PAN-OS 10.2 ou version ultérieure pour déployer CN-Series sur le hub de l'opérateur OpenShift.

Voici les étapes à suivre pour déployer le pare-feu CN-Series sur votre hub de l'opérateur Redhat OpenShift :

STEP 1 | Connectez-vous à la console du conteneur Redhat OpenShift.

STEP 2 | Accédez à **Opérateurs**, puis cliquez sur **OperatorHub**.

Red Hat OpenShift Container Plat	form							\$ 3	Ð	Ø	kube:admin -				
S Administrator			You are logged in as a temporary administrative user. Update the <u>cluster OAuth configuration</u> to allow others to log in.												
Home	~	Overview													
Overview		Cluster													
Projects															
Search API Explorer		Getting started resourc													
Events		Set up your cluster			eg Build with guided documentation	Explore new admin features									
Operators	~	Finish setting up your cluster v Add identity providers →	with recommended configura	ations.	Follow guided documentation to build applications and familiarize yourself with key features.	Explore new features and resources within the admin perspective. API Explorer >									
OperatorHitto		Configure alert receivers →			Get started with Quarkus using a Helm Chart >			peratorHub →							
Installed Operators		View all steps in documenta	tion 🗗		View all quick starts	See what's new i	w in OpenShift 4.8 g			_					
Workloads	>														
Networking		Details	View settings	Status		View alerts	Activi	ty			View events				
Storage		Cluster API address https://api.cntest.danielma.i	nfo:6443	Cluster	ter Control Plane Coperators Idegraded Insights 2 issues found			Ongoing There are no ongoing activities.							
Builds		Cluster ID 02c8c2d4-48a8-4674-9be9-58bbb2cb5654			ter version update is available Update cluster		Recent events Pause		Pause						
Monitoring	\$	OpenShift Cluster Manager	G	Jan 18, 2	, 2022, 6:19 PM View details atial/Request(c) upphis to be fulfilled			11:09 AM P Stopping container registry >							
monitoring.		GCP		Jan 14, 2	4, 2022, 7:08 PM View details			11:09 AM (2) Started container registry-s >							

STEP 3 | Entrez **Palo Alto** dans la zone de recherche Opérateur.

STEP 4 | Cliquez sur **pan-cn-series-operator**.



La fenêtre d'installation s'ouvre lorsque vous cliquez sur la tuile **pan-cn-series-operator**.

STEP 5 Cliquez sur **Installer** pour installer l'opérateur pan-cn-series sur votre cluster OpenShift.



Terminez les étapes de pré-installation avant les étapes de déploiement suivantes indiquées ici.

Si votre fichier d'identification de service fait plus de 10 Ko, vous devez le compresser puis effectuer un encodage base64 du fichier compressé avant de télécharger ou de coller le contenu du fichier dans l'API ou le CLI Panorama.

STEP 6 | Dans le menu de navigation, accédez à **Opérateurs installés**, puis cliquez sur **pan-cn-series-operator** que vous avez installé.

Bed Hat OpenShift Container Platf	orm		🇱 🌲 3 🗢 😧 kube:admin -
🗱 Administrator		You are logged in as a temporary administrative user. Update the cluster OAuth configurat	ion to allow others to log in.
		Project: openshift-operators 🔹	
Home	*		
Overview		Installed Operators	
Projects		Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators do	cumentation g. Or create an Operator and ClusterServiceVersion using the
Search		Operator SDK g.	
API Explorer		Name Variable Search by name	
Events		Name † Managed Namespaces ‡ Status Last updat	ted Provided APIs
Operators	~	pan-cn-series-operator All Namespaces Succeeded S 1 minute 10.0 provided by Palo Alto Up to date	e ago PanCnSeriesFirewall
OperatorHub		INCLUSION AS	
Installed Operators			
Workloads	>		
Networking			
Storage			
Builds			
Monitoring			

STEP 7 Cliquez sur **Create Instance** (Créer une instance).

Red Hat OpenShift Container Platform		III 🔺 3 😋 😧
🎕 Administrator	You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in	
	Project: openshift-operators 👻	
Home	10.0 provided by Palo Alto Networks	
Overview	Details YAML Subscription Events PanCnSeriesFirewall	
Projects		
	Provided APIs	Provider
Search	Flowled Aris	Palo Alto Networks
API Explorer		
Events	(PCSF) PanCnSeriesFirewall	Created at
	Not available	1 minute ago
Operators		Links
Operators •		Pan Cn Series Operator
OperatorHub	Create justance	https://pan-cn-series-operator.doma
		Maintainers
Installed Operators		Not available
	Description	
Workloads >	Palo Alto CN-Series NGFW (container firewall)	
	Product Overview The CNI Social Republication for	
Networking 3	Product Overview: The Cre-series Intendities you to:	
	1. Gain Layer-7 traffic visibility and control within the cluster	
Storage >	2. Stop lateral movement of threats	
	 Prevent known and unknown indound attacks. A populy agrees filtering to a configuration and unwasted outbound connections. 	
Builds >	5. Dynamically scale security without compromising DevOps agility.	
	6. Ensure a frictionless CI/CD pipeline deployment.	
Monitoring >	7. Unify management across all your firewalls using Panorama.	
	Deploy CN-Series as-a-Kubernetes service and manage the fleet of firewalls from Panorama, alongside our hardware and VM-Series NGFW anniliances to ensure	

STEP 8 | Entrez un **Nom** d'opérande unique.

Project openations	
Name *	
ceselies-sample	
Labels	
app+footerd	
Minimum Replices for DP	
- 2 +	
Minimum Replicas for DP	
CPU Linit (DP)	
Desired number of CPUs for CP	
Meansy surve (OP)	
August namov for DP	
- 2 +	
Desired number of CPUs for MP	
Mensery Livit (MP)	
306	
Desired memory for MP	
Panarana IP Address	
Provine Pr	
Panorana IP Address	
Secondary Panorana IP Address (Optional)	
Secondary Panoaran IP Address for HA deployment	
vm-suff-key from Pancaraa	
removale autoremovale a	
Parantena Derica Graza	
Pareruna Device Group	
Parosrana Template Stack	

STEP 9 | Entrez les **Minimum Replicas for DP** (**Répliques minimales pour DP**), **Memory Unit (Unité mémoire)** et **vCPU Limit (Limite vCPU)** pour les pods DP et MP. Pour en savoir plus sur les limites du vCPU, consultez Indicateurs de performance clés CN-Series.

STEP 10 | Entrez l'adresse IP Panorama.

Panorama Template Stack
Panorama Log Collector Group Name
<pre><pre>capanorama-collector-group></pre></pre>
Panorama Log Collector Group Name
Customer Support Portal PIN ID (Optional)
Customer Support Portal PIN ID
Customer Support Portal PIN Value (Optional)
Customer Support Portal Value
Customer Support Portal Alternate URL (Optional)
Customer Support Portal Alternate URL
DP Image
gczio/pan-cn-series/panos_cn_ngfw
The docker image name and version of CN Series DP
DP Image Version
preferred-10.2
DP Image Version
MP Image
gczio/pan-cn-series/panos_cn_mgmt
The docker image name and version of CN Series MP
MP Image Version
preferred-10.2
MP Image Version
PAN CNI Image
gczio/pan-en-series/pan_eni
The docker image name and version of CN Series pan-cni
PAN CNI Image Version
preferred
PAN CNI Image Version
Create Cancel

- STEP 11 | Facultatif Entrez l'adresse IP Panorama secondaire pour votre déploiement HA.
- **STEP 12** | Entrez la clé d'authentification Panorama CN-Series.
- **STEP 13** | Accédez au groupe d'appareils Panorama.
- **STEP 14** | Accédez à la **pile de modèles Panorama**.
- **STEP 15** | Entrez le nom du groupe de collecteurs de journal Panorama.
- **STEP 16** | Facultatif Entrez l'**identifiant PIN**, la **valeur PIN** et l'**URL alternative** du portail d'assistance à la clientèle (CSP).
- STEP 17 | En fonction de votre version PAN-OS, liez les images appropriées pour DP, MP et CNI dans la console de registre de conteneur CN-Series.
- **STEP 18** | Cliquez sur **Create** (**Créer**).
- **STEP 19** | Dans le menu Navigation, accédez à **pods**.

STEP 20 | Sélectionnez les **OpenShift-operators** du projet, puis accédez à **kube-system** pour afficher le nom et l'état des pods CNI, de gestion et de plan de données que vous avez déployés dans le cadre de l'opérande.

E Red Hat OpenShift Container Platform						III 🌲 3	0 0
📽 Administrator 🗸 👻	-781	You are logged in as a temporary ad	ministrative user. Upda	ate the <u>cluster OAuth configuration</u> to	allow others to log in.		
Home 🗸	Project: openshift-operators Select Project. Create Project	7					I
Search API Explorer	All Projects default kube-node-lease	Ready 1	Restarts 1	Owner 1 RS pan-cn-series-operator-	Memory I 80.3 MiB	CPU 1	Created 3 minutes
Operators V	 kube-public kube-system openshift 			controller-manager- 596f79d5f9			
OperatorHub Installed Operators	openshift-apiserver openshift-apiserver-operator openshift-authentication						
Workloads 🛩	 openshift-authentication-operator openshift-cloud-credential-operator 						
Deployments DeploymentConfigs	 openshift-cluster-csi-drivers openshift-cluster-machine-approver 						
StatefulSets Secrets ConfigMaps							
CronJobs							

Vous pouvez vérifier l'état de déploiement du pare-feu sur Panorama. L'**état du périphérique** passera à Connected (Connecté) moins de 5 minutes après le déploiement.

🚺 PANORAMA	D	ASHBOARD		r Devi DR POLICIES	ce Groups – OBJECTS	r Template		PANORAMA							Commit ~) 10 🖽	+ Q
Panorama V															M	anual 🗸 🗄	S ()
Setup 0	QC															3 items	$\rightarrow \times$
High Availability								ID Address	на								
Config Audit								IF Poures	na								-
Managed WildFire Clusters												DEVICE	DEVICE	CERTIFICATE			
Managed WildFire Appliances		DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IPV4	IPV6	CLUSTER STATE	VARIABLES	TEMPLATE	STATE	CERTIFICATE	EXPIRY DATE	SHARED POLICY	TEMPLATE	CERTIF
Password Profiles	~ 🗆	rhos-clusters (0/4 D	evices Connected): Si	hared > rhos-cluster	s												
Administrators •		pan-mgmt-sts-0		PA-CTNR						Create	tp-stack1	Disconnected		N/A	Out of Sync	Out of sync	
Access Domain							-								Panorama pushed	Panorama pushed	
Authentication Profile															VEISION 12	VEISION 12	
Authentication Sequence		pan-mgmt-sts-1		PA-CTNR						Create	tp-stack1	Disconnected		N/A	Out of Sync	 Out of sync 	
User Identification															Panorama pushed version: 12	Panorama pushed version: 12	
🚵 Data Redistribution	-																
Scheduled Config Push	8	mp1 nan-memt-sts-1		PA-CTNR		-		•		Create	tp-stack1	Disconnected	Valid	2022/03/09 04:20:00 PST	In Sync Panorama pushed	Out of sync Panorama nushed	
Caracter Device Quarantine		part ingini sis i													version: 13	version: 14	
Managed Devices		mp2									tp-stack1	Disconnected	Valid	2022/03/09 04:02:52 PST			
Summary •		pan-mgmc-sis-0															
Texhistering																	
Co Termistes 0																	
Device Groups o	*																
Managed Collectors •																	
Collector Groups •																	
Certificate Management																	
Certificates																	
Certificate Profile																	
SSL/TLS Service Profile																	
SCEP																	
Los Insetion Profile																	
Log Settings																	
 Server Profiles 																	
SNMP Trap																	
Syslog																	
Email																	
B HTTP																	
RADIUS																	
U_ SCP																	

STEP 21 | Configurez le plug-in PALO ALTO NETWORKS-CNI pour qu'il fonctionne avec le plug-in Multus CNI.

Le CNI Multus sur OpenShift fonctionne comme un **méta-plug-in** qui appelle d'autres plug-ins CNI. Pour chaque application, vous devez :

1. Exécutez la commande suivante pour déployer le pan-cni-net-attach-def.yaml dans chaque espace de noms de pod :

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

2. Modifier le YAML de l'application.

Après avoir déployé le pan-cni-net-attach-def.yaml, ajoutez l'annotation suivante dans le yaml du pod de l'application :

paloaltonetworks.com/firewall: pan-fw

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

Si vous avez d'autres réseaux dans l'annotation ci-dessus, ajoutez **pan-cni** après les réseaux qui doivent être inspectés. Les réseaux qui suivent **pan-cni** ne sont pas redirigés et inspectés.



Si votre pod possède plusieurs interfaces réseau, vous devez spécifier les noms des interfaces pour lesquelles vous souhaitez que le pod CN-NGFW inspecte le trafic, sous la section **interfaces** dans le fichier pan-cni-configmap.yaml.

Par exemple :

template: metadata: annotations: paloaltonetworks.com/ firewall: pan-fw k8s.v1.cni.cncf.io/networks: pan-cni