paloalto TECHDOCS

Déploiement du HSF de la série CN

docs.paloaltonetworks.com

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

Last Revised

December 13, 2021

Table of Contents

HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de la série CN	• CN-Series 11.0.x or above Container Images • Panorama sous PAN-OS 11.0.x ou version supérieure

Hyperscale Security Fabric (HSF) CN-Series 1.0 de Palo Alto Networks est un cluster de pare-feu conteneurisés de nouvelle génération qui offrent une solution de pare-feu de nouvelle génération hautement évolutive et résiliente pour les fournisseurs de services mobiles déployant des réseaux 5G.

La solution HSF CN-Series offre les avantages suivants :

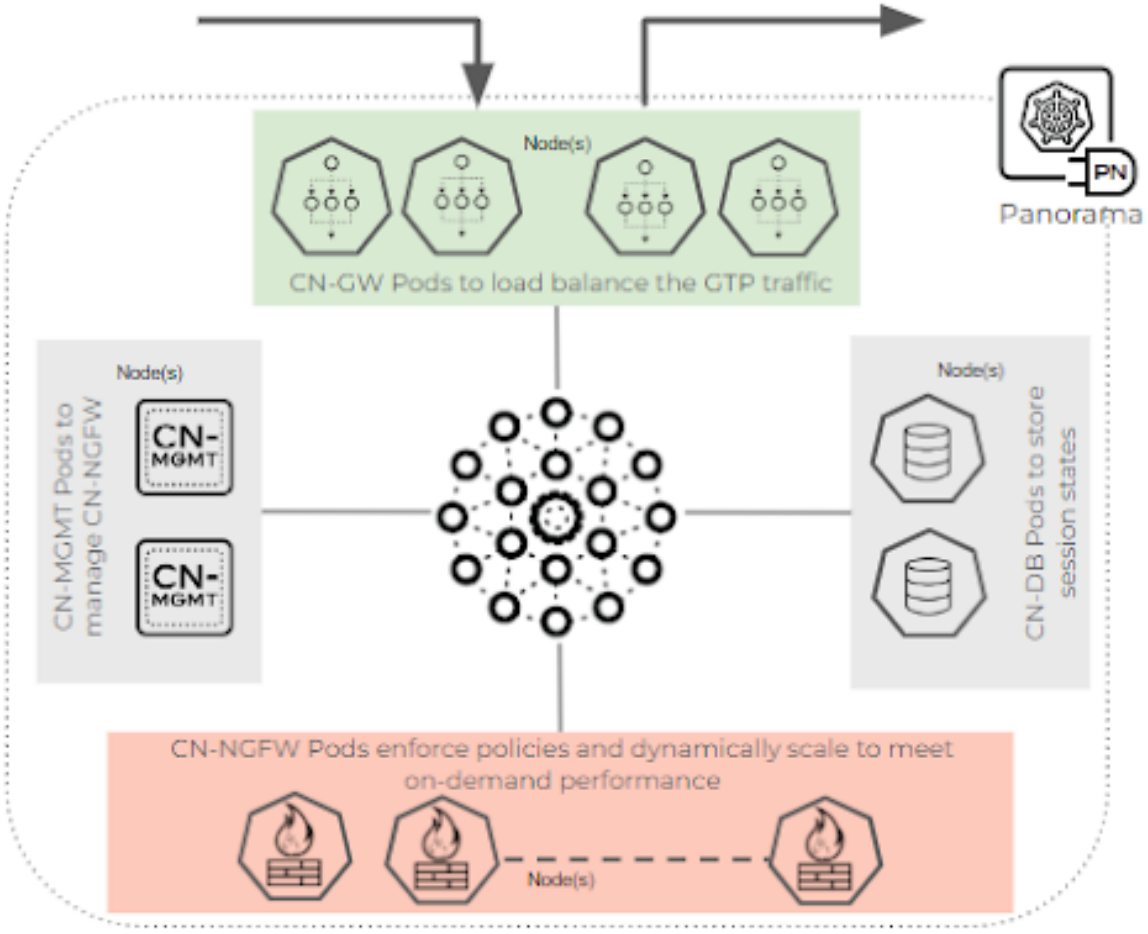
- **Hyper évolutivité avec NGFW conteneurisé** : augmente horizontalement les performances AppID et GTP à la demande.
- **Haute disponibilité et résilience** : assure une mise en cluster élastique qui agit dynamiquement en fonction du débit et de la session attendue, et garantit la continuité métier et la résilience des sessions sur les charges de travail.
- **Élimination de la dépendance de l’équilibreur de charge externe** : fournit une facilité de déploiement et un environnement convivial DevOps qui peut être entièrement orchestré par le biais des plug-ins Panorama.

La solution HSF CN-Series peut être déployée dans un environnement Kubernetes géré par le cloud public AWS EKS ou RedHat Openshift (sur site).

Architecture HSF CN-Series

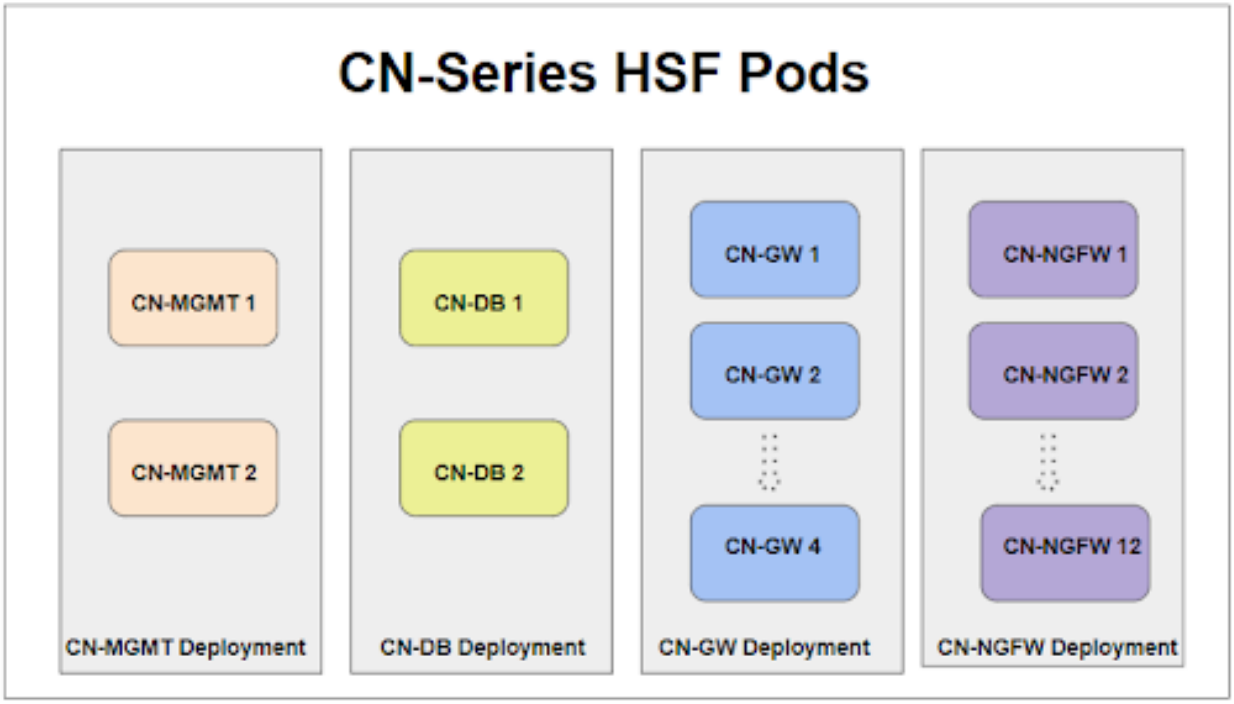
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de la série CN	• CN-Series 11.0.x or above Container Images • Panorama sous PAN-OS 11.0.x ou version supérieure

Le cluster HSF CN-Series se compose d'un pool de pods CN-MGMT (gestion), CN-NGFW (plan de données), CN-GW (passerelle) et CN-DB (base de données) connectés par des réseaux internes. Les pods CN-MGMT fournissent la fonctionnalité de plan de gestion du cluster. Les pods CN-NGFW fournissent la fonctionnalité de sécurité de plan de données du cluster. Les pods CN-GW sont le point d'entrée dans le cluster et répartissent le trafic entre les pods CN-NGFW. Les pods CN-DB fournissent le cache de session de cluster central utilisé par les pods CN-NGFW.



Le HSF CN-Series prend en charge deux conteneurs CN-MGMT qui assurent la redondance et la disponibilité. Cependant, seul l'un des deux conteneurs CN-MGMT peut recevoir des connexions de DP

CN-NGFW. Le CN-MGMT connecté s'exécute en tant que service StatefulSet pour permettre aux CN-NGFW de se connecter uniquement au CN-MGMT actif. L'autre conteneur CN-MGMT ne se connecte pas aux conteneurs CN-NGFW à moins que le CN-MGMT actuel tombe en panne.



Types de pods

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou version ultérieure

Il existe 3 types de pods de plan de données dans le HSF CN-Series. Tous utilisent la même image de pod de plan de données, mais ont des options configmap différentes. Le HSF CN-Series héberge deux pods de gestion.

Pods CN-GW – Le pod CN-GW est un type de pod de plan de données qui a accès au trafic réseau externe et gère l'équilibrage de charge du trafic entrant et du trafic sortant. Les nœuds extérieurs ne connaîtront que les pods CN-GW, leurs adresses IP, et tous les sous-réseaux de données pour le trafic sont attachés à ces pods par le biais d'interfaces Multus. Un minimum de 2 et un maximum de 4 pods CN-GW sont pris en charge dans le HSF CN-Series 1.0. Les pods CN-GW sont d'échelle statique jusqu'à la durée de vie du déploiement du cluster HSF. Par exemple, si vous possédez initialement 2 pods GW et que vous souhaitez procéder à une mise à l'échelle de diminution alors que les pods CN-NGFW peuvent procéder à une mise à l'échelle dynamique (diminution), vous devez redéployer le cluster HSF avec un nombre supplémentaire de pods CN-GW.

Pods CN-DB – Le pod CN-DB est un type de pod de plan de données qui peut interroger la propriété de la session/du flux sur les pods CN-NGFW. Les pods CN-DB prennent en charge la distribution de sessions à différents CN-NGFW en fonction de différents algorithmes, tels que ingress-slot, round-robin et session-load. Le HSF CN-Series prend en charge deux pods CN-DB. Les informations de session sont dupliquées entre les deux pods CN-DB avec l'un des deux pods CN-DB fonctionnant sur la recherche/liaison des flux.

Pods CN-NGFW – Le pod CN-NGFW traite le trafic réel pour les sessions C et U, applique des politiques de sécurité, et assure une mise à l'échelle séparée des pods CN-NGFW. Un minimum de 2 et un maximum de 12 pods CN-NGFW sont pris en charge dans le HSF CN-Series 1.0.

Pod CN-MGMT – Tous les pods NGFW (CN-GW, CN-DB et CN-NGFW) sont connectés à un seul pod CN-MGMT par le biais de IPSec sur eth0.

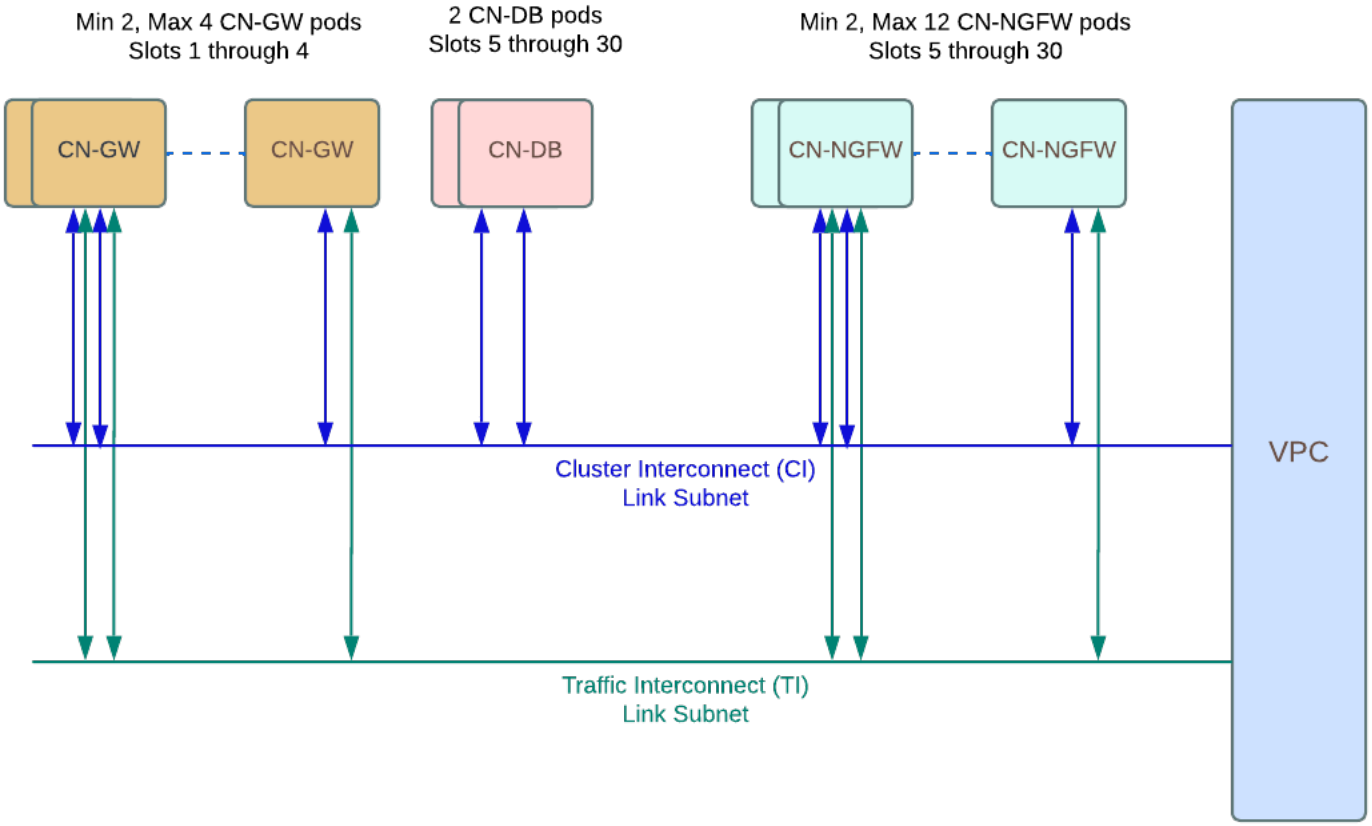
Liaisons d'interconnexion

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Tous les pods CN-GW, CN-DB et CN-NGFW sont connectés les uns aux autres par le biais de la liaison d'interconnexion du cluster (CI), qui est une interface Multus. La liaison CI est un port de données réservé à des fins de communication du cluster et de transfert de paquets entre les membres du cluster. Ethernet x/1 est utilisé pour les liaisons CI sur tous les pods pertinents. La liaison CI peut également être utilisée pour transférer le trafic d'un CN-NGFW à un autre.

Les pods CN-GW et CN-NGFW sont connectés les uns aux autres par le biais d'une liaison d'interconnexion du trafic (TI), qui est une interface Multus. La liaison TI est un port de données réservé au trafic interne au sein du cluster. Ethernet x/2 est utilisé pour les liaisons TI sur tous les pods pertinents.

Sur les pods CN-GW, Ethernet x/3 et ceux qui suivent sont utilisés comme interfaces externes de connexion au réseau du client.



Le HSF CN-Series ne prend en charge que le protocole IPv4.

Pour un environnement sur site, un serveur DHCP ou IPAM est nécessaire pour attribuer des adresses IP aux interfaces CI et TI. Pour AWS EKS, le serveur DHCP fait partie de l'infrastructure sous-jacente. Par conséquent, les adresses IP sont automatiquement attribuées aux interfaces CI et TI dans les environnements cloud.

Mettre sous licence le HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de la série CN	• CN-Series 11.0.x or above Container Images • Panorama sous PAN-OS 11.0.x ou version supérieure

La mise sous licence du pare-feu CN-Series est gérée par le plug-in Kubernetes sur Panorama. Les pare-feu CN-Series sont concédés sous licence en fonction du nombre total de vCPU (cœurs) utilisés par les pods CN-NGFW, CN-GW et CN-DB déployés dans votre environnement Kubernetes. Un jeton est consommé pour chaque vCPU utilisé par ces pods.

- Activer des crédits
- Créer un profil de déploiement HSF CN-Series
- Gérer les profils de déploiement

Activer des crédits

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• CN-Seriesdéploiement	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou version supérieure • Helm 3.6 or above version client

Au sein de votre organisation, vous pouvez créer de nombreux comptes ayant chacun un objectif différent. Pendant l'activation, vous ne pouvez choisir qu'un seul compte par pool de crédits par défaut. Une fois que le pool de crédits est actif, les utilisateurs qui se voient attribuer le rôle d'administrateur de crédits peuvent allouer des crédits pour les déploiements, et même transférer des crédits vers d'autres pools.

Si vous avez un compte CSP existant et que vous êtes un super utilisateur ou un administrateur, le système ajoute automatiquement le rôle d'administrateur de crédits à votre profil. Si vous n'avez pas de compte existant, le CSP crée automatiquement un compte pour vous et ajoute le rôle d'administrateur de crédits à votre profil.

Vous (l'acheteur) recevez un e-mail détaillant l'abonnement, l'ID du pool de crédits, la date de début et de fin de l'abonnement, le montant des crédits achetés et la description du pool de crédits par défaut (le pool de crédits créé quand vous activez vos crédits).

Conservez cet e-mail pour référence ultérieure.

STEP 1 | Dans l'e-mail, cliquez sur **Start Activation** (Démarrer l'activation) pour afficher vos pools de crédits disponibles.

STEP 2 | Sélectionnez le pool de crédits que vous souhaitez activer. Vous pouvez utiliser le champ de recherche pour filtrer votre liste de comptes par numéro ou par nom.

Si vous avez acheté plusieurs pools de crédit, les deux sont automatiquement sélectionnés. Les coches représentent les liens d'activation pour les crédits d'intégration.

Vous êtes invité à vous authentifier ou à vous connecter.

Si vous désélectionnez un pool de crédits, un rappel s'affiche pour indiquer que si vous souhaitez activer ces crédits, vous devez revenir à l'e-mail et cliquer sur le lien ***Start Activation*** *(Démarrer l'activation).*

STEP 3 | Sélectionnez **Start Activation** (Démarrer l'activation).

STEP 4 | Sélectionnez le compte d'assistance (vous pouvez effectuer une recherche par numéro de compte ou par nom).

STEP 5 | Sélectionnez le pool de crédits par défaut.

STEP 6 | Sélectionnez **Deposit Credits** (Déposer des crédits).

Un message indique que le dépôt a réussi.

STEP 7 | (facultatif) S'il s'agit de votre première activation de crédit, la boîte de dialogue Créer un profil de déploiement s'affiche.

Créer un profil de déploiement HSF CN-Series

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de Série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou version ultérieure

Utilisez la procédure suivante pour créer un profil de déploiement CN-Series.

STEP 1 | Si vous disposez déjà d'un pool de crédits, connectez-vous au compte et, à partir du tableau de bord, sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** > **Prisma NGFW Credits (Crédits NGFW Prisma)** > **Create New Profile (Créer un nouveau profil)**.

Si vous venez d'activer un pool de crédits, l'écran **Create Deployment Profile** (Créer un profil de déploiement) s'affiche.

1. Sélectionnez le type de pare-feu **CN-Series**.
2. Sélectionnez le **PAN-OS 11.0**.
3. Cliquez sur **Next (Suivant)**.

STEP 2 | Profil CN-Series.

1. **Profile Name** (Nom du profil).

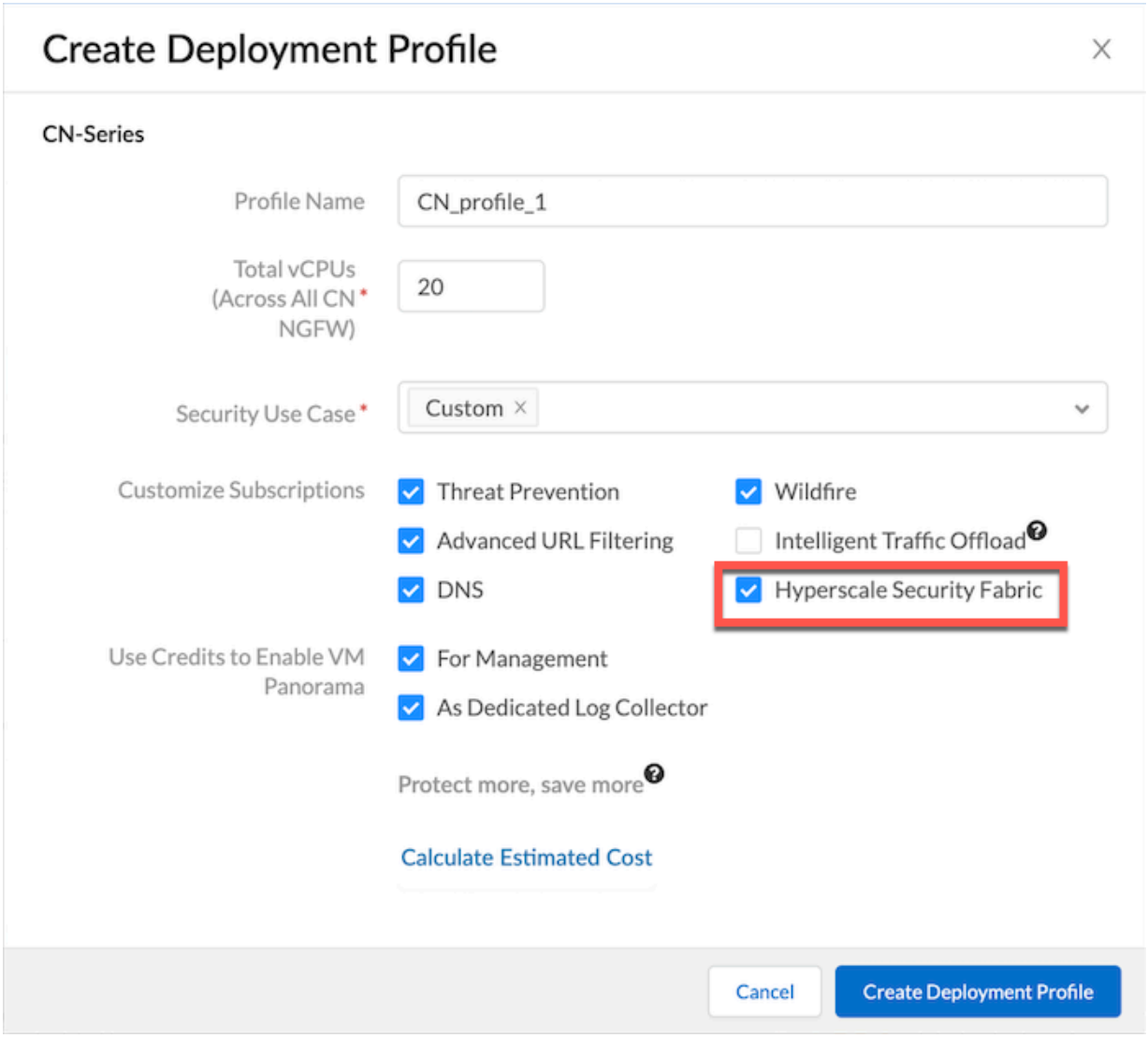
   Nommez le profil.

2. **Total vCPUs** (Total des vCPU).

   Saisissez le nombre total de vCPU nécessaires dans tous les pods (CN-NGFW, CN-GW et CN-DB).

3. Sélectionnez un cas d'utilisation de sécurité dans la liste déroulante. Chaque cas d'utilisation de sécurité dans la liste déroulante sélectionne automatiquement un certain nombre de descriptions recommandées pour le cas d'utilisation choisi. Si vous sélectionnez Custom (Personnalisé), vous pouvez spécifier les abonnements que vous souhaitez utiliser dans votre déploiement.
4. Sélectionnez **Hyperscale Security Fabric** sous **Customize Subscriptions (Personnaliser les abonnements)** pour activer HSF sur votre abonnement.
5. (facultatif) **Utilisez des crédits pour activer VM Panorama — Pour la gestion** ou **Collecteur de journaux dédié**.

STEP 3 | Cliquez sur **Calculate Estimated Cost** (Calculer le coût estimé) pour afficher le total des crédits et le nombre de crédits disponibles avant le déploiement.



Gérer les profils de déploiement

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Vous pouvez modifier, cloner ou supprimer des profils de déploiement CN-Series en fonction des exigences de votre déploiement CN-Series. De plus, vous pouvez ajouter ou supprimer des abonnements du profil de déploiement après sa création. Pour plus d’informations, reportez-vous à la section Gestion des profils de déploiement.

Configuration système requise pour le HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de la série CN	• CN-Series 11.0.x or above Container Images • Panorama sous PAN-OS 11.0.x ou version supérieure

Système HSF CN-Series recommandé et matrice de capacité

Voici notre configuration système recommandée pour le HSF CN-Series.

Le tableau suivant sépare les données par taille CN-Series : petite, moyenne et grande. L'inspection de débit que le HSF CN-Series peut assurer varie en fonction de la taille du cluster.

- **CN-Series pour HSF, taille petite**
- **CN-Series pour HSF, taille moyenne**
- **CN-Series pour HSF, taille grande**

Le HSF CN-Series nécessite deux groupes de nœuds : CN-MGMT et CN-DB avec deux nœuds chacun. Le nombre de nœuds nécessaires pour les groupes de nœuds CN-GW et CN-NGFW dépend du débit.

Version de cluster		Petite	Moyenne	Grande
CN-GW	Cœurs	24	24	24
	Mémoire	16 Go	20 Go	24 Go
	Bande passante	50 Gbit/s	100 Gbit/s	100 Gbit/s
	Type d'instance	c5n.9xlarge (36 vCPU, 96 Gi)	c5n.18xlarge	c5n.18xlarge
CN-DB	Cœurs	8	8	12
	Mémoire	0,64 x 12 x MaxSessions (en millions) Go	0,64 x 12 x MaxSessions (en millions) Go	0,64 x 10 x 10 Go
	Bande passante	10 GbE	25 GbE	25 GbE
	Type d'instance	c5n.4xlarge (16 vCPU, 42 Gi)	c5n.4xlarge	c5n.9xlarge

Version de cluster		Petite	Moyenne	Grande
CN-MGMT	Cœurs	4	12	12
	Mémoire	16 Go	16 Go – 24 Go	16 Go – 24 Go
	Bande passante	10 GbE	10 GbE	10 GbE
	Disque	56 Gi	80 Gi	80 Gi
	Type d’instance	c5n.4xlarge (8 vCPU, 21 Gi)	c5n.4xlarge ou c5d.9xlarge	c5n.4xlarge ou c5d.9xlarge
CN-NGFW	Cœurs	15	24	24 – 36
	Mémoire	20 Go	16 Go – 47 Go	48 Go (56 Go pour cœurs > 32)
	Bande passante	25 GbE	50 GbE	50 GbE
	Type d’instance	c5n.4xlarge (16 vCPU, 42 Gi)	c5n.9xlarge	c5n.9xlarge

Version HSF CN-Series recommandée

Version de cluster	Nombre de nœuds			Nombre total d’interfaces	Nombre minimal d’interfaces
	Petite	Moyenne	Grande		
CN-GW	2	3	4	4 – 15	4
CN-DB	2	2	2	2	2
CN-MGMT	2	2	2	1	1
CN-NGFW	6	8	10	3	3
CN-NGFW supplémentaire pour couvrir les pannes DP	2	2	2	-	-

Prise en charge du mode jumbo HSF CN-Series

Lorsque la prise en charge jumbo est activée, Panorama configure l’unité de transmission maximale (MTU) pour toutes les interfaces sur le non CN-MGMT à 8 744 octets.

La MTU système s’élève à 9 000 octets en mode jumbo et les interfaces héritent de la MTU système si la MTU n’est pas spécifiée.

Dans les hôtes EKS, la valeur MTU par défaut pour les instances AWS EC2 s’élève à 9 000. Par conséquent, aucune configuration n’est nécessaire côté hôte.

Lorsque la prise en charge jumbo est désactivée, Panorama configure l’unité de transmission maximale (MTU) pour toutes les interfaces sur le non CN-MGMT à 1 756 octets.

Vous devez faire correspondre vos valeurs MTU jumbo et non-jumbo sur vos environnements EKS avec les valeurs MTU Panorama.

Mode	MTU (octets)
Jumbo	EKS – 9 000 octets
Non-jumbo	1 756 octets pour toutes les interfaces

Conditions préalables pour déployer le HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Voici les conditions préalables au déploiement du HSF CN-Series :

- Exigences en matière de clusters
- Préparer le cluster
- Préparer Panorama pour le déploiement HSF CN-Series

Exigences en matière de clusters

Vous avez besoin d'un cluster Kubernetes doté des autorisations nécessaires pour créer et gérer des groupes de nœuds. Vous avez également besoin des ressources requises pour que le plug-in Kubernetes fasse apparaître le cluster CN-Series.

Configurez les éléments suivants en tant que conditions préalables du cluster :

- Cluster EKS ou Openshift (4.10), selon l'environnement dont vous disposez. Vous devez créer les VPC et sous-réseaux et configurer le rôle IAM nécessaire pour faire apparaître le cluster EKS.

  Pour plus d'informations sur la création d'un cluster EKS, reportez-vous à la section Création d'un cluster Amazon EKS.

  Pour plus d'informations sur la création d'un cluster Openshift, reportez-vous à la section Installation d'un cluster Openshift.
- Kubernetes version 1.22 ou ultérieure.

  Pour plus d'informations, reportez-vous à la section Installation de Kubernetes avec des outils de déploiement.
- CNI Multus afin de pouvoir attacher plusieurs interfaces réseau aux pods dans Kubernetes.

  Pour plus d'informations, reportez-vous à la section Installation d'un CNI Multus.
- Quatre groupes de nœuds avec la configuration minimale requise mentionnée dans la configuration système requise pour la série CN.

Préparer le cluster

Vous devrez configurer les éléments suivants :

- Groupe de nœuds et nœuds
- Étiquettes de nœuds
- Compte de service
- Interfaces

Groupe de nœuds et nœuds

Vous aurez besoin d'un minimum de 8 nœuds pour gérer la topologie et prendre en charge tous les pods dans la solution. Palo Alto Networks recommande 4 ensembles de groupes de nœuds avec un minimum de deux nœuds chacun. Veillez à ne pas autoriser le groupe de nœuds MP à chevaucher le reste des 3 groupes de nœuds.

Si vous souhaitez utiliser DPDK, vous devez avoir une AMI sur laquelle des pilotes DPDK sont configurés. Pour plus d'informations, reportez-vous à la section Configuration de DPDK sur AWS EKS.

Une fois le cluster EKS en cours d'exécution, utilisez le modèle CloudFormation avec Multus pour afficher les instances de groupe de nœuds et EC2 avec les types de nœuds.

```
lnehru@lnehru-parts-vm:~/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common$ kubectl get nodes
NAME                                          STATUS   ROLES    AGE     VERSION
ip-10-101-201-125.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-204.us-west-1.compute.internal   Ready    <none>   3d23h   v1.22.12-eks-ba74326
ip-10-101-201-223.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-226.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-81.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-159.us-west-1.compute.internal   Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-163.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-21.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-51.us-west-1.compute.internal    Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-66.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-221-78.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-90.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-222-149.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-175.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-176.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-213.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-38.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-6.us-west-1.compute.internal     Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-77.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-96.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
```

Étiquettes de nœuds

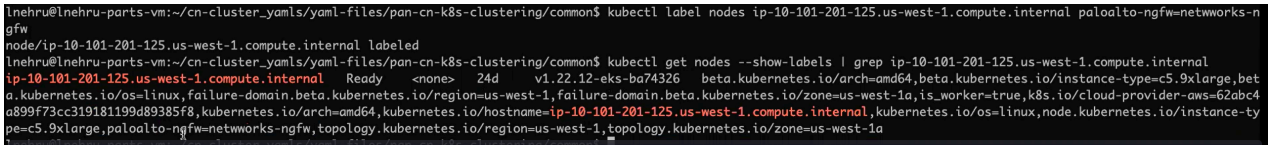
Utilisez les commandes suivantes pour étiqueter tous les nœuds :

```
kubectl label node (MP_node_name) Panw-mp=Panw-mp
kubectl label node (DB_node_name) Panw-db=Panw-db
kubectl label node (GW_node_nam) Panw-gw=Panw-gw
kubectl label node (NGFW_node_name) Panw-ngfw=Panw-ngfw
```

Voici des exemples d'étiquettes de nœuds :

```
CN-NGFW – paloalto-ngfw: networks-ngfw
CN-MGMT – paloalto-mgmt: networks-mgmt
CN-GW – paloalto-gw: networks-gw
CN-DB – paloalto-db: networks-db
```


Une paire clé-valeur doit être fournie pour chaque type de nœud. En outre, une valeur par défaut des réseaux clés paloalto et de valeur est recommandée. Toutefois, si vous choisissez de modifier les étiquettes de nœuds, vous devez apporter les modifications correspondantes à la configuration.



Après avoir étiqueté les nœuds, téléchargez les YAML nécessaires pour afficher le cluster.

Compte de service

Les autorisations étendues pour les déploiements sont fournies à l’aide d’un compte de service yaml. Pour créer les comptes de service, votre cluster Kubernetes doit être prêt.

1. Exécutez le compte de service YAML pour le `plugin-deploy-serviceaccount.yaml`.

   Le compte de service permet d’obtenir les autorisations dont Panorama a besoin pour s’authentifier auprès du cluster afin de récupérer les étiquettes Kubernetes et les informations sur les ressources. Ce compte de service est nommé pan-plugin-user par défaut.
2. Accédez à yaml-files/clustering folder/common et déployez les éléments suivants :

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

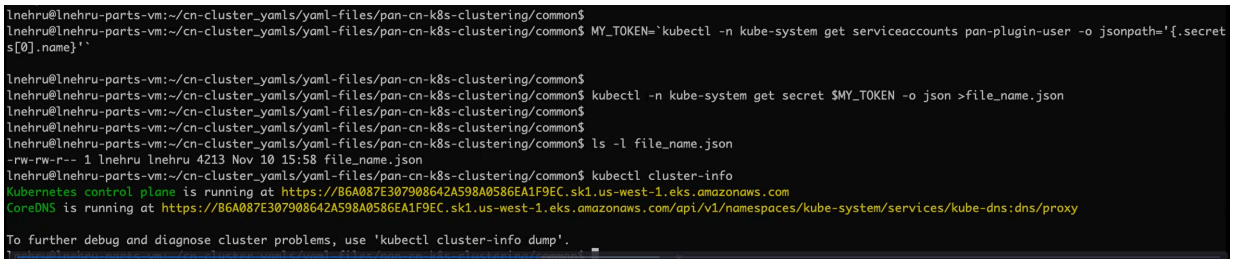
   ```
   kubectl apply -f pan-mgmt-serviceaccount.yaml
   ```

   ```
   kubectl -n kube-system get secrets | grep pan-plugin-user-token
   ```

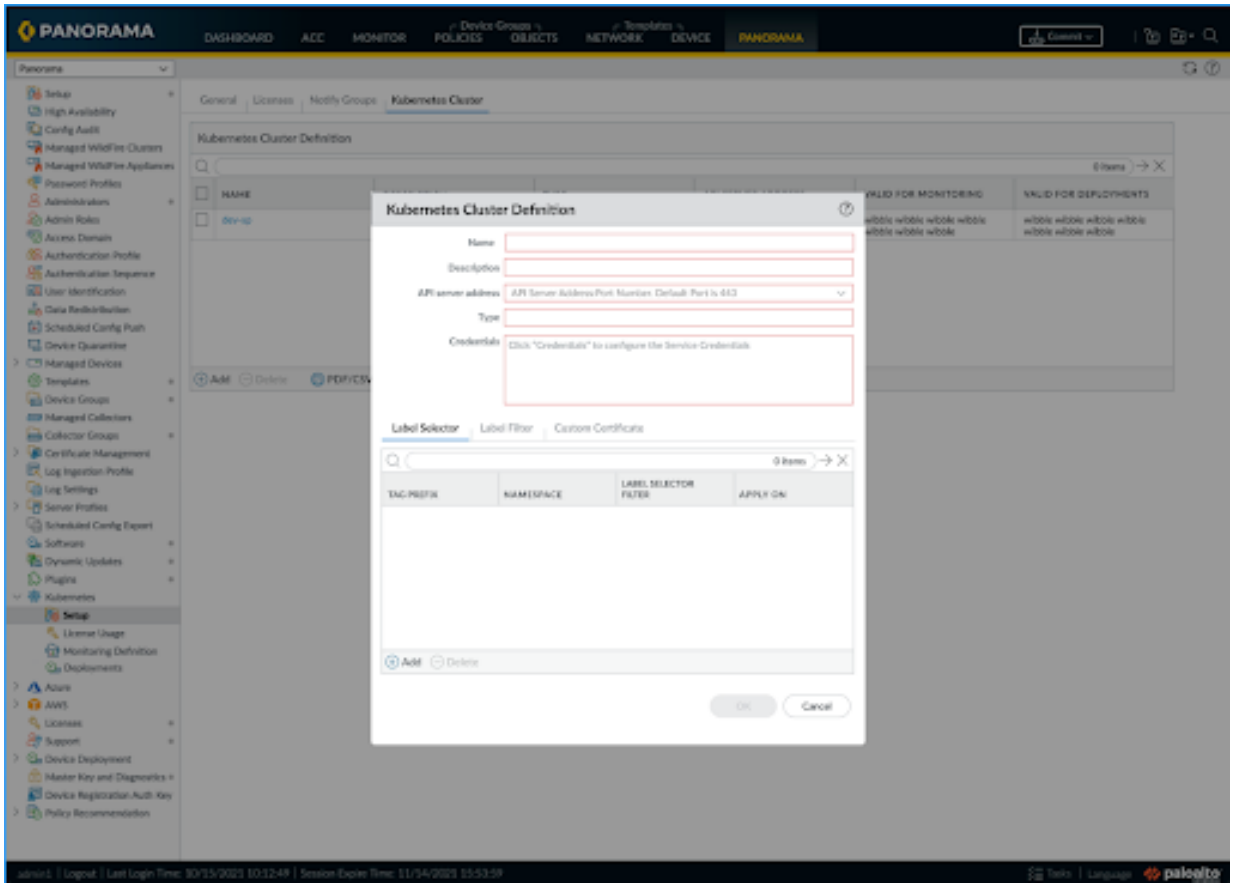
   Créez le fichier d’informations d’identification contenant les secrets, appelé cred.json par exemple, puis enregistrez ce fichier. Vous devez télécharger ce fichier sur Panorama afin de configurer le plug-in Kubernetes pour la surveillance des clusters.

3. Pour consulter les secrets associés à ce compte de service.

```
kubectl -n kube-system get secrets (secrets-from-above-command) -o
json >> cred.json
```



4. Téléchargez le fichier cred.json sur le plug-in Kubernetes et vérifiez l’état de validation.



Après la première opération validation/publication/validation sur Panorama, le plug-in continue à appeler la logique de validation à intervalles réguliers et à mettre à jour l’état de validation sur l’interface utilisateur.

Interfaces

Vous devrez créer les ENI nécessaires pour CN-DB, CN-NGFW et CN-GW. Identifiez les ID de bus PCI de ces interfaces qui seront ensuite utilisés pour créer des définitions de pièce jointe réseau pour l’interconnexion des pods.

1. SSH dans le nœud à l’aide de la clé ou de l’utilisateur que vous avez créé lors de la création d’un cluster.

   ```
   ssh ec2-user@(node_ip) -i private_(key)
   ```

2. Installez le package ethtool.

   ```
   Sudo yum install ethtool
   ```

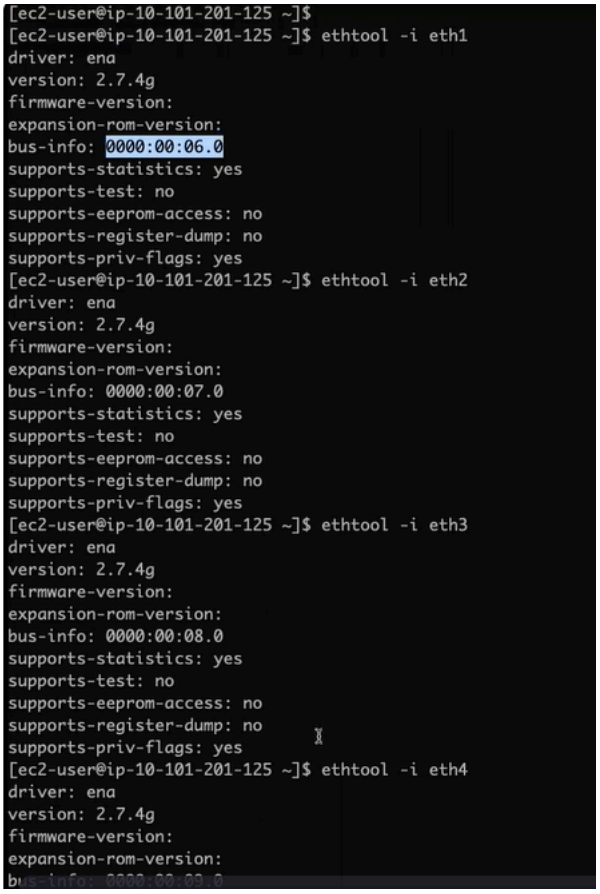
   ```
   sudo yum update -y && sudo yum install ethtool -y
   ```


3. Identifiez le nom de l’interface.

   ```
   ifconfig
   ```

4. Identifiez l’ID de bus PCI de l’interface pour déployer la connectivité réseau sur les pods.

   ```
   ethtool -i (i/f)
   ```



Ici, eth0 est l’interface de gestion des nœuds, eth1 est l’interface CI, eth2 est TI, eth3 est l’interface externe 1, eth4 est l’interface externe 2. Dans le nœud étiqueté pour CN-MGMT, vous ne trouverez que l’interface eth0 pour la gestion. Pour CN-DB, vous bénéficierez de eth1. Pour CN-NGFW, vous bénéficierez de eth1, eth2, et pour CN-GW, vous bénéficierez de eth1, eth2, et d’autant d’interfaces externes que vous avez créées dans votre environnement.

```
    net-attach-1 - 0000:00:08.0 net-attach-2 - 0000:00:09.0 net-
attach-def-ci-db - 0000:00:06.0 net-attach-def-ci-gw - 0000:00:06.0
 net-attach-def-ci-ngfw - 0000:00:06.0 net-attach-def-ti-gw -
 0000:00:07.0 net-attach-def-ti-ngfw - 0000:00:07.0
```

Tous les pods d’un déploiement doivent se trouver sur des nœuds différents, car ils utilisent les mêmes définitions de pièce jointe réseau. Par conséquent, chaque pod doit accéder au même ID de bus PCI. Par exemple, si le net-attach utilise l’ID PCI 6 pour la liaison CI de pod C/U, chaque pod C/U doit être placé sur un nœud doté d’une interface d’ID PCI 6 à partir du même sous-réseau.

5. Modifiez l’ID de bus PCI sur la définition de pièce jointe réseau YAML.

```
   { "cniVersion": "0.3.1", "type": "host-device", "pciBusID":
"0000:00:07.0" }
```

Ici, la première liaison eth1 est utilisée en tant que CI, eth2 est utilisé en tant que TI, et eth3 et ceux qui suivent sont utilisés pour les liaisons externes.

6. Appliquez les fichiers YAML prérequis.

```
kubectl apply -f pan-mgmt-serviceaccount.yaml
kubectl apply -f net-attach-def-1.yaml
kubectl apply -f net-attach-def-2.yaml
kubectl apply -f net-attach-def-ci-db.yaml
kubectl apply -f net-attach-def-ci-gw.yaml
kubectl apply -f net-attach-def-ci-ngfw.yaml
kubectl apply -f net-attach-def-ti-gw.yaml
kubectl apply -f net-attach-def-ti-ngfw.yaml
```

Dans Openshift, appliquez `Kubectl apply -f ctrcfg-pidslimit.yaml`. Pour plus d’informations sur pidlimit, reportez-vous à la section Tâches de configuration.

Si des PV statiques sont utilisés, créez les volumes de montage de PV statiques sur les nœuds étiquetés pour les pods CN-MGMT.


```
/mnt/pan-local1, /mnt/pan-local2, /mnt/pan-local3, /mnt/pan-local4, /
mnt/pan-local5, /mnt/pan-local6
```

Préparer Panorama pour le déploiement HSF CN-Series

La configuration et le déploiement HSF CN-Series sont effectués via Panorama. Avant de déployer le HSF CN-Series, veillez à avoir bien rempli les conditions préalables suivantes.

STEP 1 | Déployez un Panorama avec la version 11.0 du logiciel et installez la version de contenu minimale.

1. Cliquez sur **Panorama** > **Dynamic Updates (Mises à jour dynamiques)** pour connaître la version minimale du contenu sur PAN-OS 11.0.

   Consultez PAN-OS Release Notes (Notes de version PAN-OS).

2. Accédez à **Panorama** > **Software (Logiciel)** pour connaître la version du logiciel.

   Localisez et téléchargez le fichier spécifique au modèle pour la version finale vers laquelle vous effectuez la mise à niveau. Par exemple, pour mettre à niveau un appareil M-Series vers Panorama 11.0.0, téléchargez l'image Panorama_m-11.0.0. Pour mettre à niveau un appareil virtuel Panorama vers Panorama 11.0.0, téléchargez l'image Panorama_pc-11.0.0.

   Après un téléchargement réussi, la colonne **Action** passe de Download (Télécharger) à Install (Installer) pour l'image téléchargée.

STEP 2 | Vérifiez que votre Panorama est en Panorama mode (Mode Panorama), si vous souhaitez que Panorama collecte les journaux du pare-feu.

STEP 3 | Installez la version 4.0 du plug-in Kubernetes sur Panorama. Si vos appareils Panorama sont déployés en tant que paire HA, vous devez d'abord installer le plug-in Kubernetes sur le pair principal (actif).

1. Connectez-vous à l'interface Web Panorama et sélectionnez **Panorama** > **Plugins (Plug-ins)** et cliquez sur **Check Now (Vérifier maintenant)** pour générer la liste des plug-ins disponibles.
2. Sélectionnez **Download (Télécharger)** et **Install (Installer)** pour installer la version 4.0 du plug-in Kubernetes.

   Une fois l'installation du plug-in réussie, Panorama s'actualise et le plug-in Kubernetes s'affiche sur l'onglet **Panorama**.

   Si Panorama est déployé dans une paire HA, installez le plug-in Kubernetes sur le Panorama secondaire (passif) à l'aide des étapes décrites à l'étape 3.

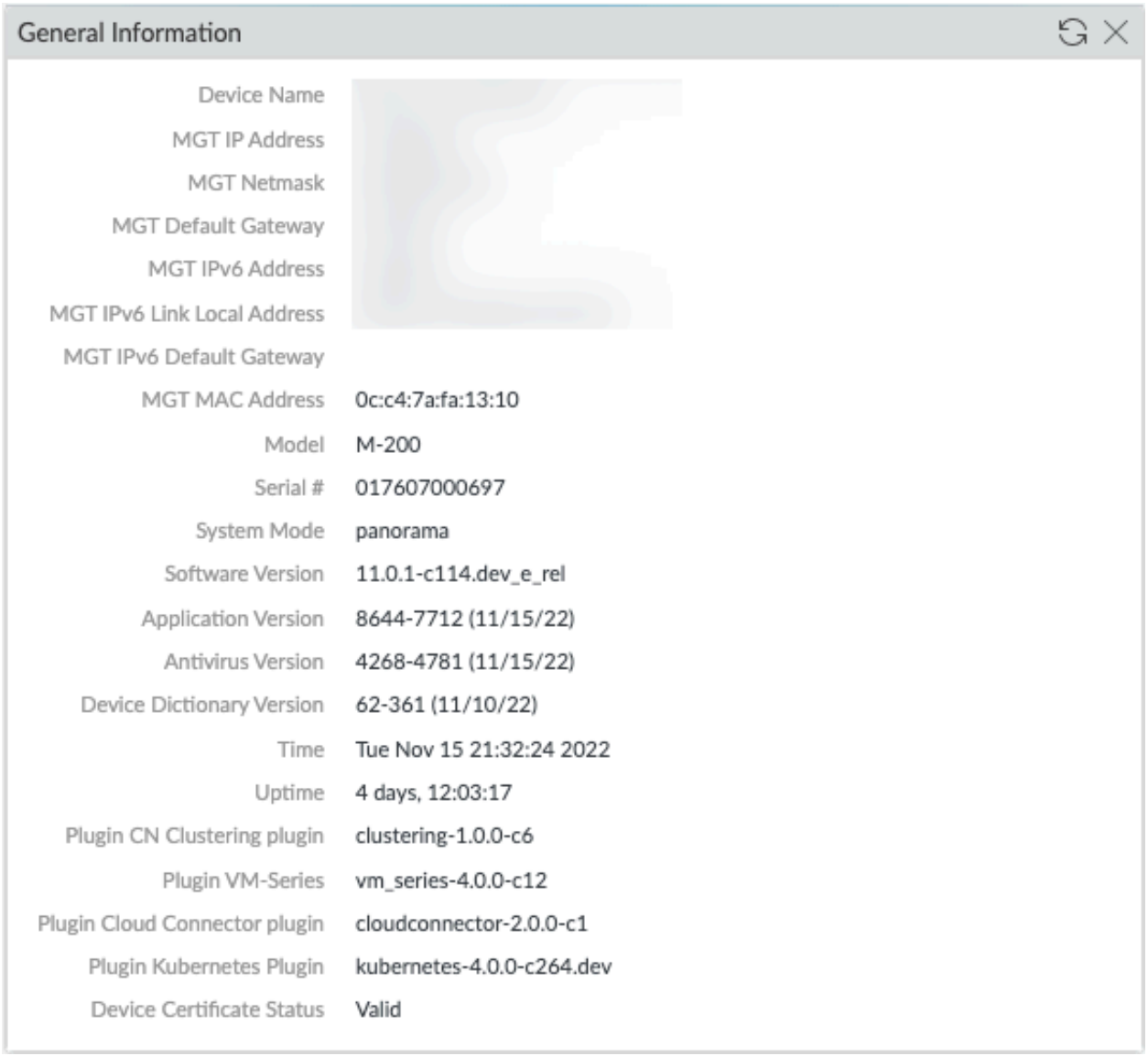
3. Cliquez sur **Commit to Panorama (Valider sur Panorama)**.

   La validation crée un modèle **K8S-CNF-Clustering-Readonly** à utiliser avec le HSF CN-Series. L'affichage des interfaces sur Panorama peut prendre jusqu'à une minute. Ce modèle possède la configuration réseau de la liaison d'interconnexion du cluster (CI) préconfigurée pour les pods CN-GW, CN-DB et CNNGFW et la liaison d'interconnexion du trafic (TI) pour les pods CN-GW et CN-NGFW. Le modèle **K8S-CNF-Clustering-Readonly** crée 30 routeurs logiques et

deux interfaces par routeur logique. Les ethernet x/1 sont des liaisons d'interconnexion du cluster (CI) tandis que les ethernet x/2 sont des liaisons d'interconnexion du trafic (TI).

*Veillez à ne pas renommer le modèle **K8S-CNG-Clustering-Readonly**.*

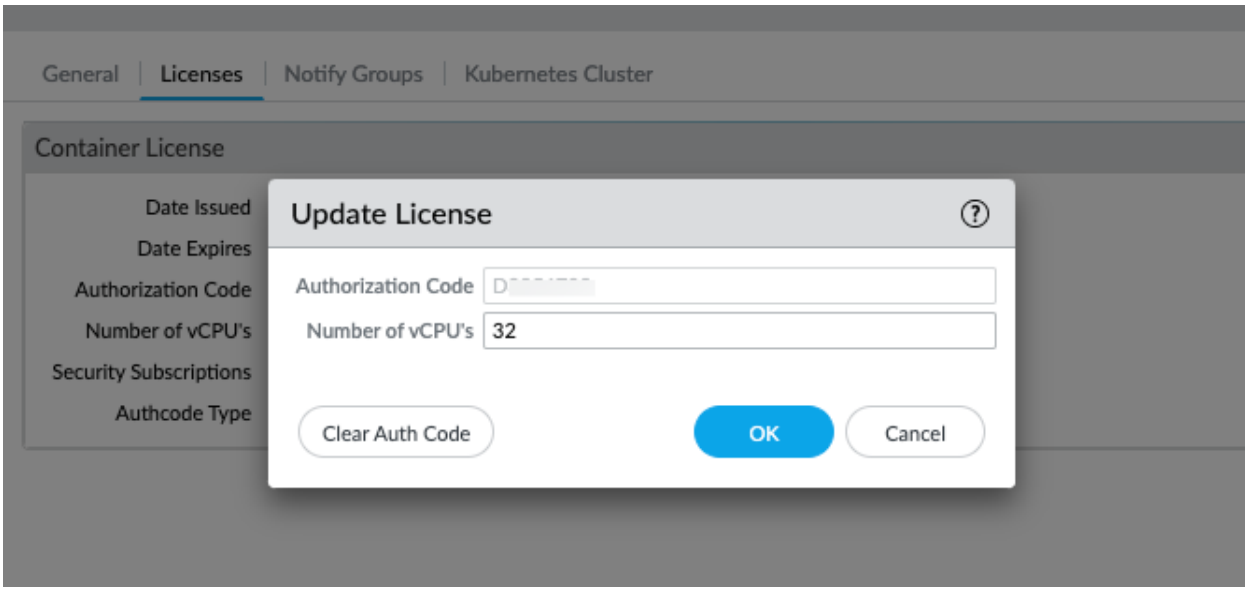
Vous pouvez vérifier le widget General Information (Informations générales) sur **Dashboard (Tableau de bord)** > **General Information (Informations générales)** de Panorama.



STEP 4 | Obtenez les crédits de licence HSF CN-Series sur Panorama.

1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Kubernetes** > **Setup (Configuration)** > **Licenses (Licences)**.
2. Sélectionnez **Activate/update using authorization code (Activer/mettre à jour à l'aide du code d'autorisation)**, puis saisissez le code d'autorisation et le nombre total de vCPU de plan

de données nécessaires. Vous devez créer un profil de déploiement pour obtenir votre code d'authentification de la série CN.



Lorsque CN-Series est déployé avec HSF, si le nombre de pods (CN-NGFW, CN-GW et CN-DB) déployés dépasse le nombre de vCPU alloués, vous disposez d'un délai de grâce de quatre heures pour ajouter d'autres vCPU à votre profil de déploiement ou supprimer suffisamment de pods. Si vous n'allouez pas de vCPU supplémentaires ou ne supprimez pas de pods sans licence dans le délai de grâce de quatre heures, les pods sans licence redémarrent et créent une perturbation du trafic. Les pods déjà sous licence restent sous licence.

3. Vérifiez que le nombre de crédits de licence disponibles est mis à jour.

STEP 5 | Créez un groupe d'appareils parent.

Vous devez créer un groupe d'appareils avec les politiques et les objets nécessaires requis pour le HSF CN-Series. Vous devez référencer ce groupe d'appareils lorsque vous déployez le HSF CN-Series.

1. Accédez à **Panorama** > **Device Groups (Groupes d'appareils)**, puis cliquez sur **Add (Ajouter)**.
2. Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.
3. Sélectionnez le **Parent Device Group (Groupe de périphériques Parent)** (la valeur par défaut est **Shared (partagé)**) qui sera juste au-dessus de l'ensemble d'appareils que vous créez dans la hiérarchie de groupes de périphériques.
4. Cliquez sur **OK**.

   Le nom du groupe d'appareils est amorcé dans le pod CN-MGMT du cluster. Lorsque les pods CN-MGMT se connectent à Panorama avec ces paramètres d'amorçage, le groupe d'appareils est associé au nom du cluster dans la configuration du cluster. Pour Panorama Haute Disponibilité (HA), le pod CN-MGMT envoie des mises à jour aux Panoramas actifs et passifs. Les informations de cluster sont automatiquement renseignées pour les pods CN-NGFW, CN-DB et CN-GW lorsqu'ils sont actifs.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider et appliquer la configuration du groupe d'appareils à Panorama.

STEP 6 | Créez un modèle de variable pour activer le flux de trafic.

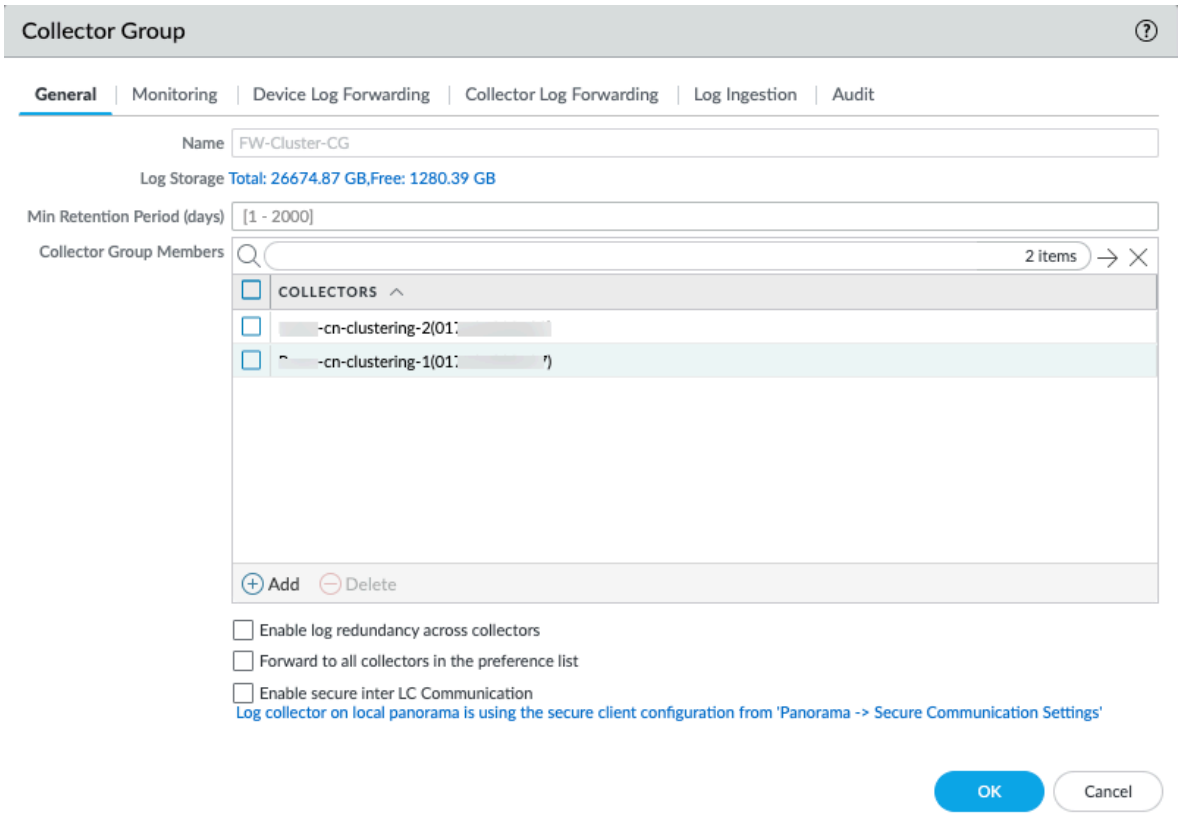
1. Accédez à **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** unique pour le modèle.
3. Ajoutez une **Description** facultative.
4. Configurez le modèle de variable pour activer le flux de trafic.

   Vous pouvez configurer ce modèle avant ou après le déploiement du HSF CN-Series.

STEP 7 | Créez un collecteur de journaux et ajoutez-le à un groupe de collecteurs de journaux.

1. Accédez à **Panorama** > **Collector Groups (Groupes de collecteurs)** et **Add (Ajoutez)** un groupe de collecteurs.
2. Saisissez un **Name (Nom)** pour identifier le groupe de collecteurs.
3. Entrez la **Minimum Retention Period (Période de conservation minimale)** en jours (1 à 2 000) pendant laquelle le groupe de collecteurs sera conservé pour les journaux de pare-feu.

   Par défaut, le champ est vide, ce qui signifie que le groupe de collecteurs conserve indéfiniment les journaux.
4. **Add (Ajoutez)** les collecteurs de journaux (1 à 16) à la liste des membres du groupe de collecteurs.



5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications à Panorama et au groupe de collecteurs que vous avez configuré.

La clé d'authentification Panorama sera créée et gérée par le plug-in Kubernetes.

Déployer le cluster HSF

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Après avoir vérifié que les conditions préalables au déploiement du pare-feu CN-Series en tant que HSF sont remplies, accédez à **Kubernetes** > **Deployments (Déploiements)** et cliquez sur **Add (Ajouter)**.

Vous devez configurer les onglets suivants pour déployer le cluster HSF.

- Général
- Données de nœud
- Image et stockage
- Configuration CN
- Mise à l'échelle automatique

Général

Saisissez les détails suivants dans la section de l'onglet **General (Général)** de la fenêtre contextuelle **Deployments (Déploiements)**.

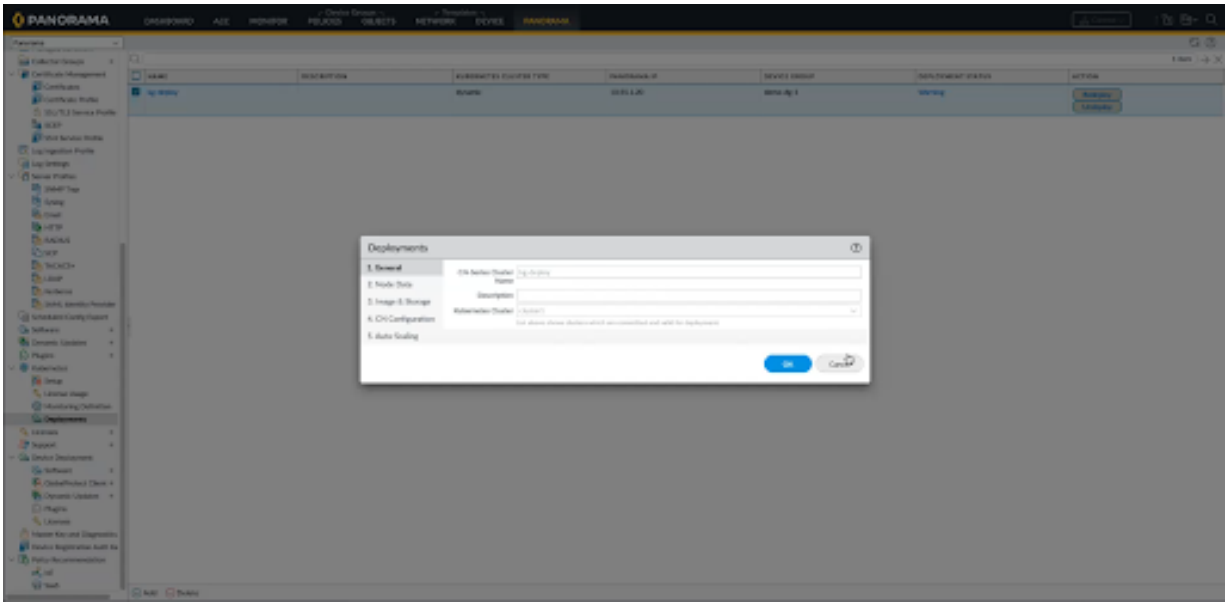
STEP 1 | **CN-Series Cluster Name (Nom du cluster CN-Series)** : nom du HSF CN-Series.

STEP 2 | (Facultatif)**Description** : chaîne de texte décrivant le cluster HSF.

STEP 3 | **Kubernetes Cluster (Cluster Kubernetes)** : une liste d'entrées pour les clusters est créée dans la section **Setup (Configuration)** du plug-in. Sélectionnez le cluster approprié que vous avez créé dans la liste déroulante.

Le cluster Kubernetes n'est affiché que si les détails sont validés et valides pour les déploiements.

STEP 4 | **CN-Series Cluster Name (Nom du cluster CN-Series)** : nom du HSF CN-Series.



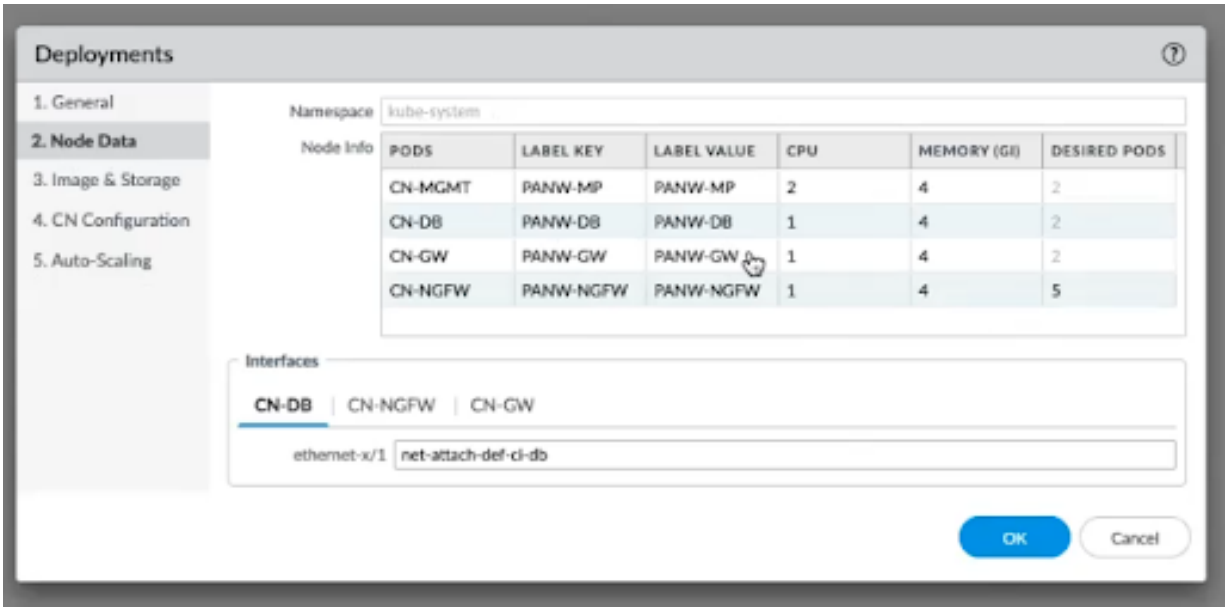
Données de nœud

Saisissez les détails suivants dans la section de l'onglet **Node Data (Données de nœud)** de la fenêtre contextuelle **Deployments (Déploiements)**.

STEP 1 | **Namespace (Espace de noms)** : espace de noms dans le cluster Kubernetes existant où le HSF CN-Series est déployé.

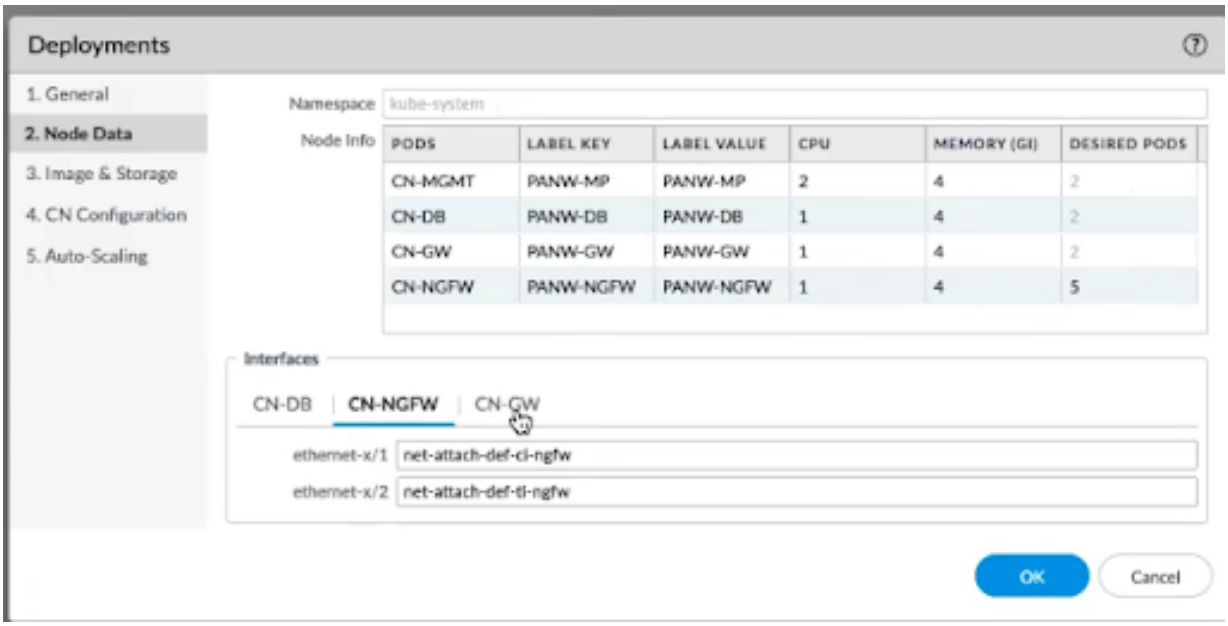
STEP 2 | **Node Info (Informations sur les nœuds)** : des étiquettes de pool de nœuds sont utilisées pour déployer chaque type de pod CN. Vous devez spécifier le processeur, la mémoire et les pods souhaités pour chacun des types de pods en fonction de la disponibilité sur les nœuds. Les paires

Labels (Étiquettes) et Label value (Valeur d’étiquette) sont des valeurs préalables devant exister sur le nœud ; vous devez ajouter la même paire clé-valeur utilisée pour étiqueter les nœuds.



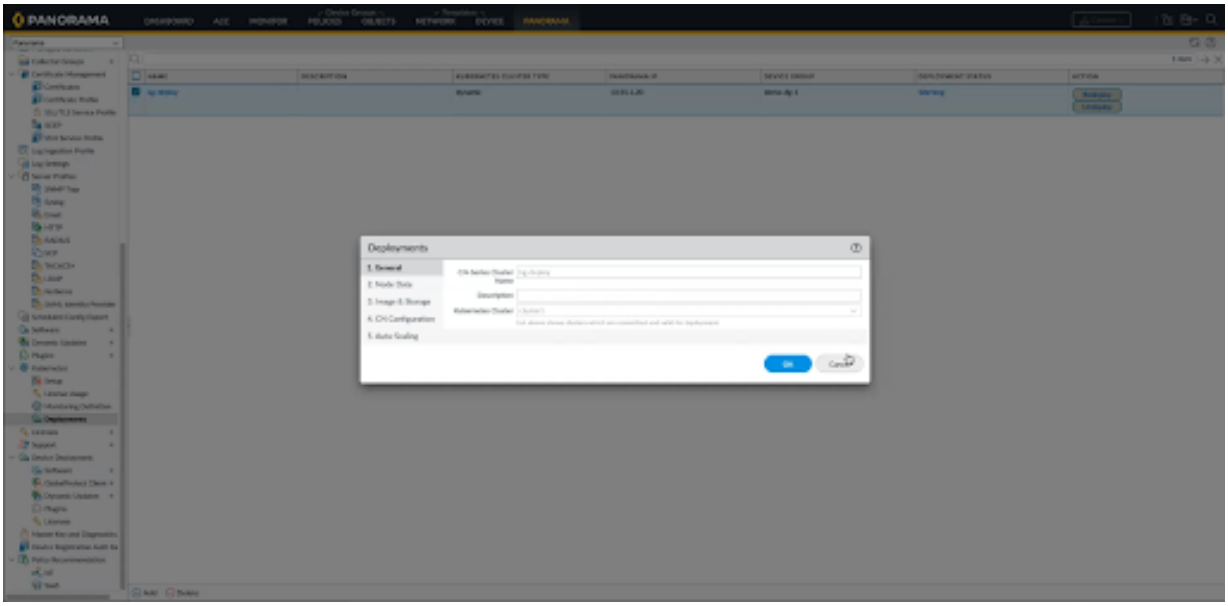
STEP 3 | **Interfaces** : des noms d’interface pour les pods CN-DB, NGFW, CN-GW doivent être ajoutés. Chaque interface nécessite l’application d’une net-attach-def spécifique sur le cluster Kubernetes. Le plug-in nomme Ethernet x/1 et Ethernet x/2 par défaut. Si vous modifiez les noms d’interface pour Ethernet x/1 et Ethernet x/2, vous devrez également effectuer la modification dans la section

relative aux pièces jointes réseau. Pour le pod CN-GW, vous pouvez ajouter jusqu'à 12 interfaces, à l'exclusion des interfaces CI et TI.



Le cluster Kubernetes n'est affiché que si les détails sont validés et valides pour les déploiements.

STEP 4 | **CN-Series Cluster Name (Nom du cluster CN-Series)** : nom du HSF CN-Series.



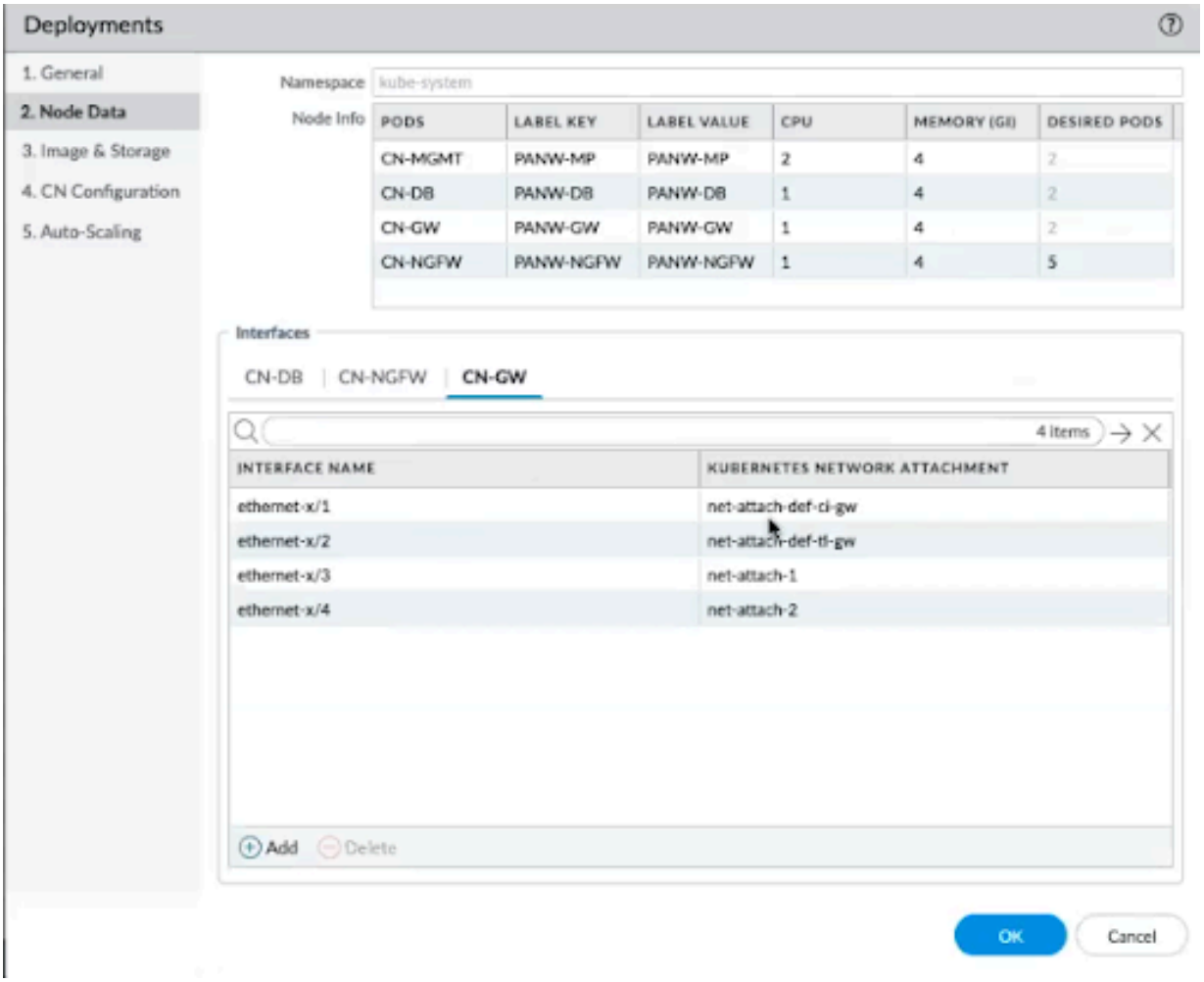


Image et stockage

Saisissez les détails suivants dans la section de l'onglet **Image & Storage (Image et stockage)** de la fenêtre contextuelle **Deployments (Déploiements)**.

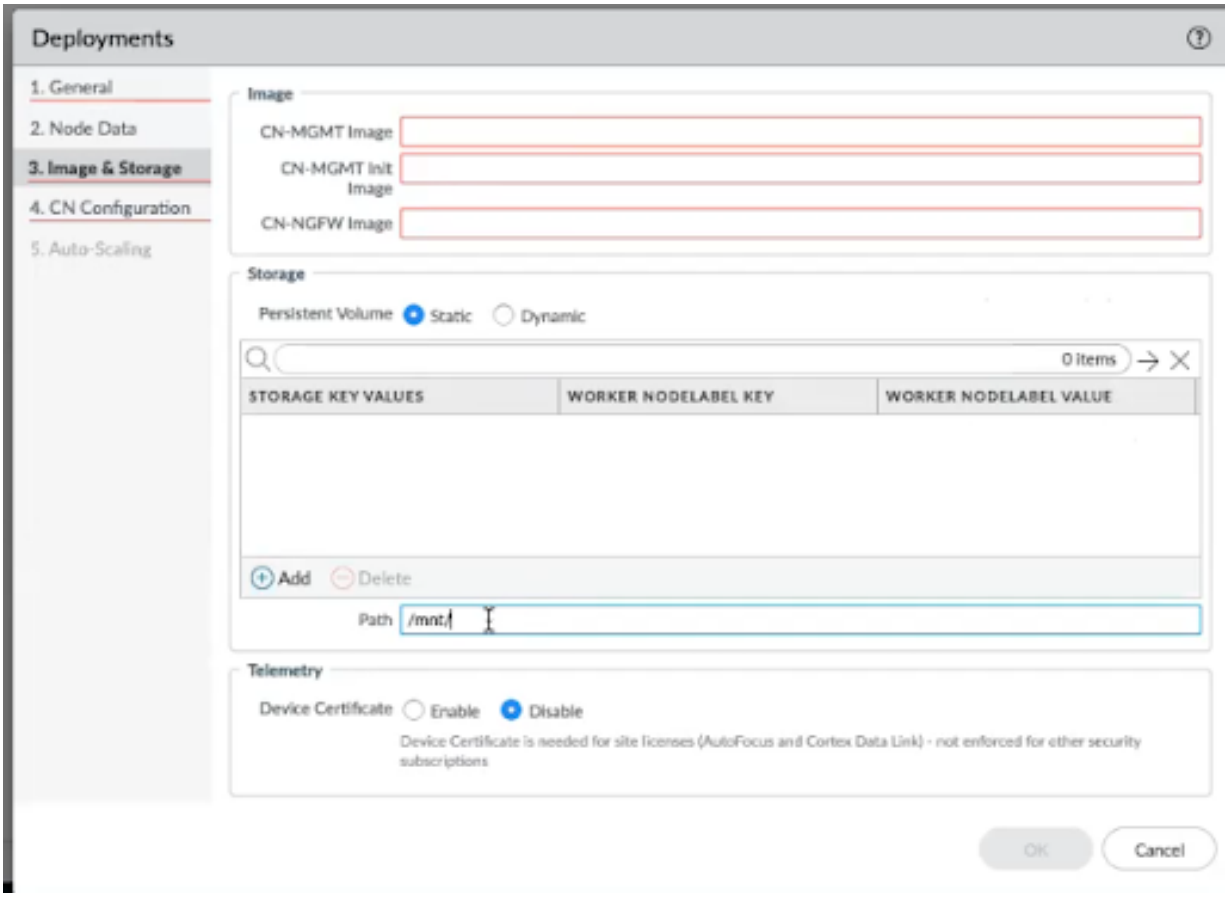
STEP 1 | **Image** : vous devez stocker les images dans le référentiel local ou AWS, ce qui ne peut pas être validé par Panorama. Toutefois, le cluster Kubernetes dispose d'une connectivité aux référentiels dans lesquels les images sont stockées.

1. **CN-MGMT Image (Image CN-MGMT)** : URI complet du référentiel dans lequel l'environnement Kubernetes doit accéder à l'image pour déployer le pod CN-MGMT.
2. **CN-MGMT INIT Image (Image INIT CN-MGMT)** : image init nécessaire pour le pod CN-MGMT.
3. **CN-NGFW Image (Image CN-NGFW)** : URI complet du référentiel dans lequel l'environnement Kubernetes doit accéder à l'image pour déployer le pod CN-NGFW.

STEP 2 | **Storage (Stockage)** : si vous souhaitez configurer le stockage exclusif, cliquez sur **Dynamic (Dynamique)** dans la section Storage (Stockage) pour l'environnement EKS et Static (Statique) ou

Dynamic (Dynamique) pour les environnements Openshift. Le plug-in configure alors le stockage cloud. Si vous avez sélectionné **Static (Statique)**, vous devez saisir les valeurs Storage Key Values (Valeurs clés de stockage), Worker Nodelabel Key (Clé Nodelabel esclave) et Worker Nodelabel Value (Valeur Nodelabel esclave). Vous devez également saisir le **Path (Chemin d'accès)** où le stockage est monté.

Vous devez ajouter une classe de stockage valide autre que celle par défaut dans l'espace de noms de l'environnement Kubernetes. Sinon, si l'option de stockage Dynamic (Dynamique) est sélectionnée et qu'aucun nom de classe de stockage n'est fourni, la classe de stockage par défaut présente dans l'espace de noms est sélectionnée.



STEP 3 | **Certificates (Certificats)** : il s'agit des informations de certificat de périphérique permettant d'activer ou de désactiver des informations telles que les licences. Si elles sont activées, vous devez fournir le PIN ID (ID DE PIN) et la PIN VALUE (VALEUR DE PIN).

Configuration CN

Saisissez les détails suivants dans la section de l'onglet **CN Configuration (Configuration CN)** de la fenêtre contextuelle **Deployments (Déploiements)** :

STEP 1 | **Primary Panorama IP (IP Panorama primaire)** : affiche les valeurs des adresses IP publiques et privées du Panorama sur lequel le plug-in est installé.

STEP 2 | **Secondary Panorama IP (IP Panorama secondaire)** : affiche les valeurs des adresses IP publiques et privées du Panorama secondaire (dans le cas de HA) sur lequel le plug-in est installé.

STEP 3 | **Device Group (Groupe d'appareils)** : vous devez créer un DG avant de configurer le déploiement, comme indiqué dans la section relative aux conditions préalables. La liste déroulante Device Group (Groupe d'appareils) répertorie tous les DG sur le Panorama actuel. Vous devez sélectionner un DG valide. Le pod CN-MGMT est enregistré sous ce DG. Pour connaître la procédure de création d'un groupe d'appareils, reportez-vous à l'étape 5 de la section Préparer Panorama pour le déploiement HSF CN-Series.

STEP 4 | **Template (Modèle)** : vous devez créer un modèle (variable_template) pour les détails spécifiques à CN-GW avant de configurer le déploiement comme mentionné dans la section relative aux conditions préalables. La liste déroulante Template (Modèle) répertorie tous les modèles sur le Panorama actuel. Vous devez choisir un modèle adapté à votre déploiement actuel. Après le déploiement HSF, ce modèle est ajouté à une pile de modèles par le plug-in avec un modèle K8S-CNF-Clustering-Readonly qui gère la configuration de base pour les pods CN-DB et CN-NGFW. Il configure également les liaisons CI et TI sur le pod CN-GW. Le pod CN-MGMT reçoit les configurations de la pile de modèles. Pour connaître la procédure de création du modèle de variable, reportez-vous à l'étape 6 de la section Préparer Panorama pour le déploiement HSF CN-Series.

STEP 5 | **Log Collector Group (Groupe de collecteurs de journaux) (LCG)** : cette liste déroulante répertorie tous les groupes de collecteurs de journaux sur le Panorama actuel. Un LCG approprié doit être sélectionné. Il configure également les liaisons CI et TI du pod CN-GW. Pour connaître la procédure de création d'un LCG, reportez-vous à l'étape 7 de la section Préparer Panorama pour le déploiement HSF CN-Series.

STEP 6 | **Jumbo Frame (Trame Jumbo)** : la liste déroulante Jumbo Frame (Trame Jumbo) répertorie les valeurs **Enable (Activer)**, **Disable (Désactiver)** et **AutoDetect (Détection automatique)**. Cette configuration s'applique à tous les pods dans le HSF CN-Series.

STEP 7 | **5G Enabled (5G activé)** : il s'agit d'un bouton d'option comprenant les options **Enable (Activer)** et **Disable (Désactiver)**, et fait référence à la configuration GTP requise sur le HSF CN-Series.

Vous devez gérer d'autres paramètres nécessaires sur le modèle dans le fichier ***variable_template****.*

STEP 8 | **DPDK** : il s’agit d’un bouton d’option comprenant les options **Enable (Activer)** et **Disable (Désactiver)**. Si les ressources sous-jacentes ne prennent pas en charge DPDK, le HSF CN-Series est défini par défaut sur packetmmap.

Sur EKS, si vous souhaitez utiliser DPDK, vous devez avoir une AMI sur laquelle des pilotes DPDK sont configurés. Pour plus d’informations, reportez-vous à la section Configuration de DPDK sur AWS EKS.

Pour activer DPDK sur Openshift, vous devez activer HugePages sur les nœuds esclaves. Pour plus d’informations, reportez-vous à la section Configuration de HugePages.

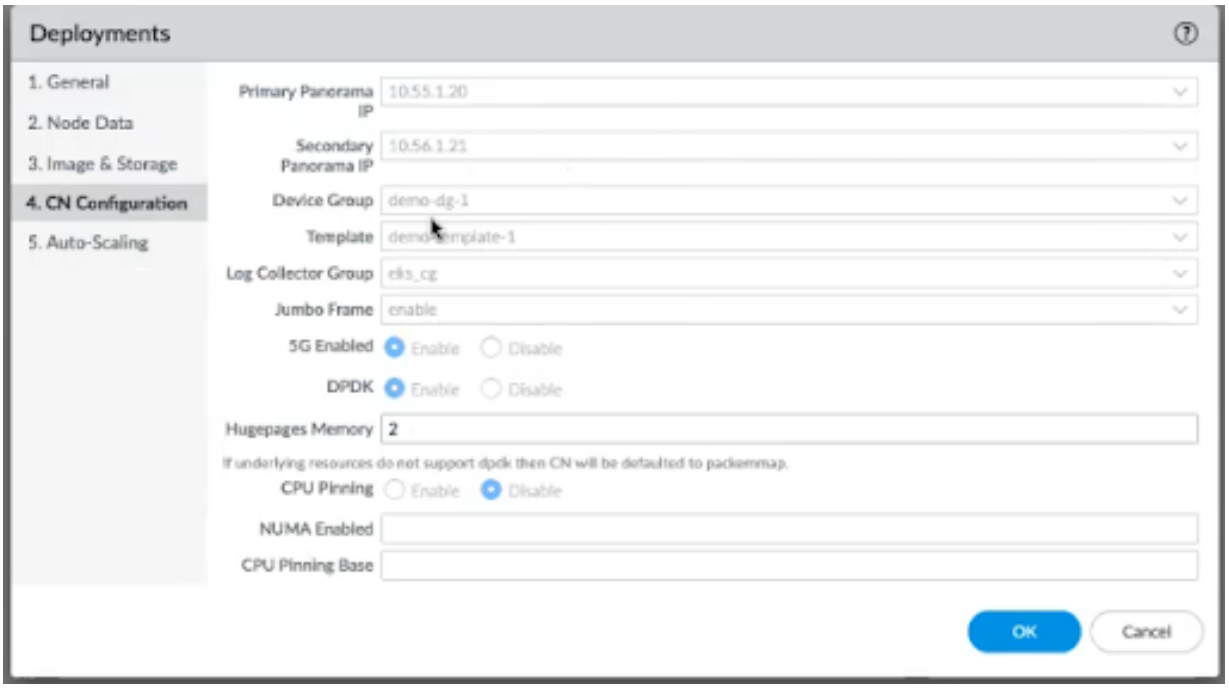
Vous devez également activer le pilote PCI VFIO sur les nœuds esclaves.

```
modprobe vfio-pci echo 1 > /sys/module/vfio/parameters/
enable_unsafe_noiommu_mode
```

STEP 9 | **CPU Pinning (Épinglage du processeur)** : choisissez d’activer ou de désactiver l’épinglage du processeur.

STEP 10 | **Numa Enabled (Numa activé)** : indiquez le numéro de nœud pour NUMA.

STEP 11 | **CPU Pinning Base (Base d’épinglage du processeur)** : indiquez le numéro du processeur à partir duquel vous souhaitez démarrer l’épinglage du processeur des processus de transfert et ignorez les processeurs dont le numéro est inférieur.



Mise à l’échelle automatique

Saisissez les détails suivants dans la section de l’onglet **Auto-Scaling (Mise à l’échelle automatique)** de la fenêtre contextuelle **Deployments (Déploiements)**.

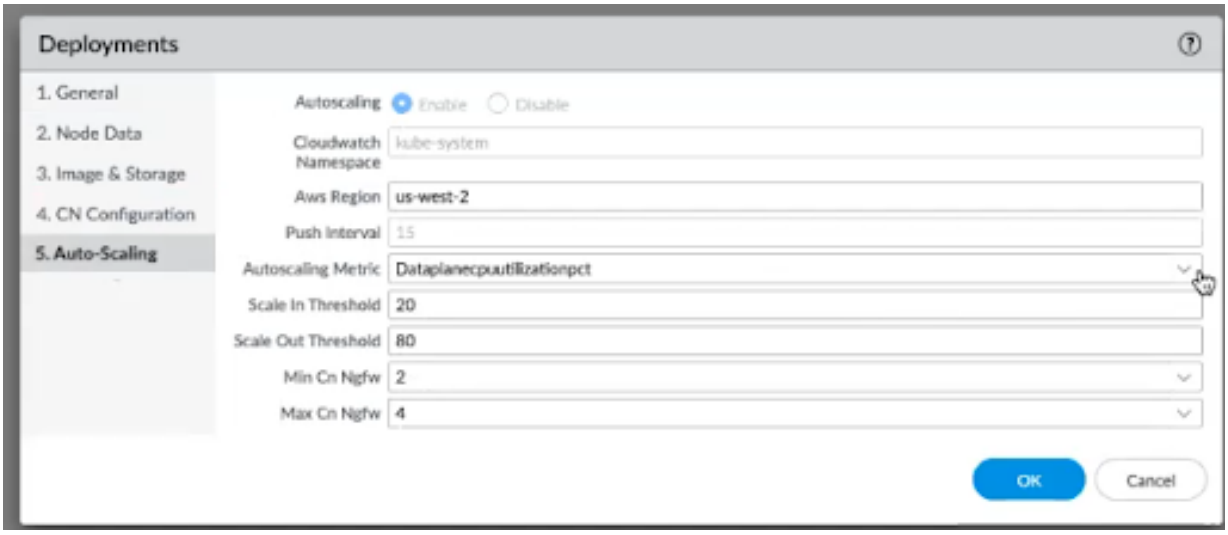
- *La mise à l'échelle automatique est prise en charge uniquement sur les environnements EKS avec EKS Kubernetes version 1.22. L'onglet Auto-Scaling (Mise à l'échelle automatique) est grisé pour les autres systèmes Kubernetes.*
- *Vous devez effectuer un déploiement de HPA basé sur des métriques personnalisées utilisant KEDA au sein d'environnements EKS pour que la mise à l'échelle automatique fonctionne.*

STEP 1 | Saisissez les valeurs **Autoscaling Metric (Métrique de mise à l'échelle automatique)**, **Scale In Threshold (Seuil de mise à l'échelle [augmentation])** et **Scale Out Threshold (Seuil de mise à l'échelle [diminution])** dans la section **Autoscaling (Mise à l'échelle automatique)**.

STEP 2 | Cliquez sur **OK** pour valider le déploiement.

Voici les métriques prises en charge pour la mise à l'échelle automatique.

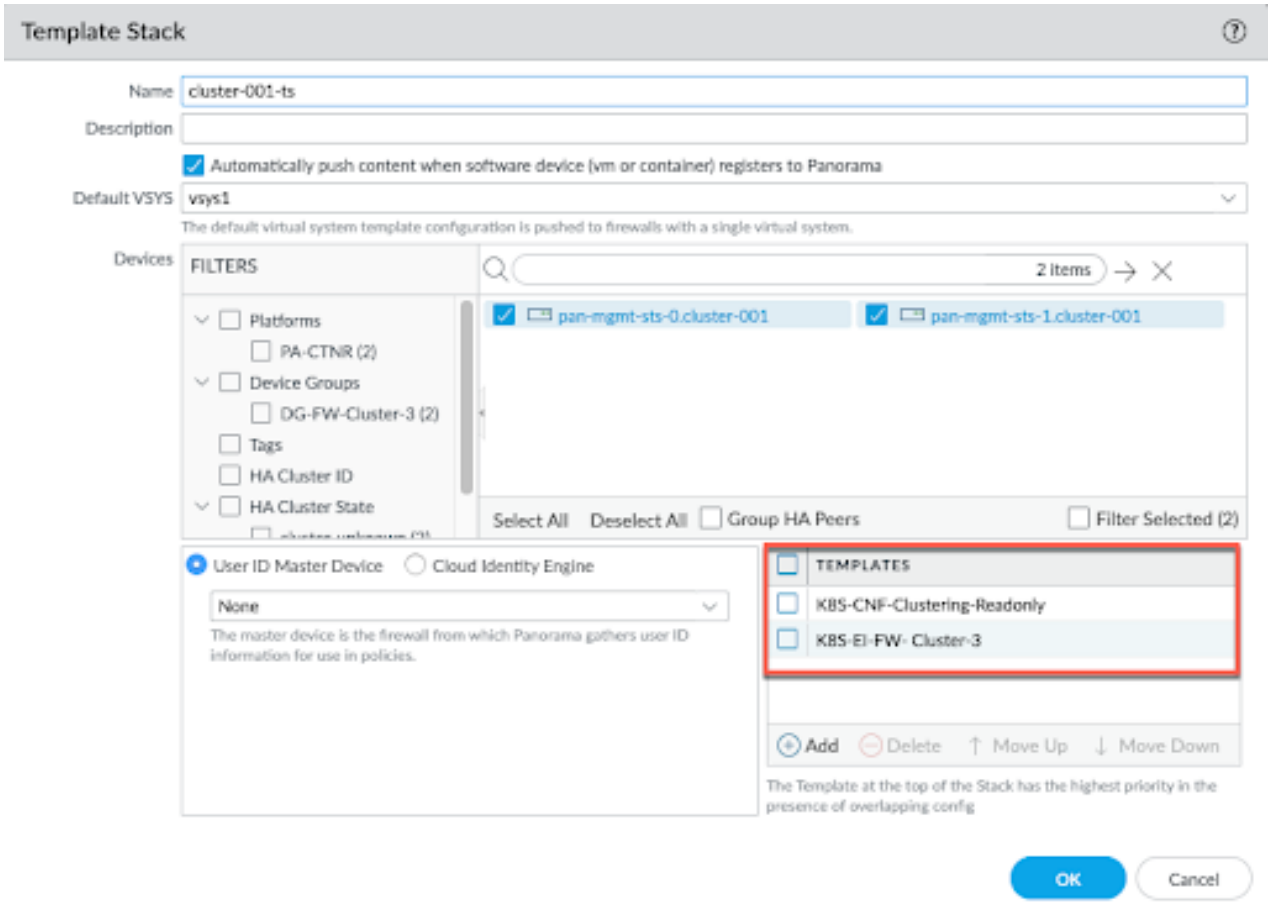
- `dataplanecpuutilizationpct`
- `dataplanepacketbufferutilization`
- `pansessionactive`
- `pansessionutilization`
- `pansessionsslproxyutilization`
- `panthroughput`
- `panpacketrate`
- `panconnectionspersecond`



Après avoir saisi tous les détails de configuration, l'onglet Deployments (Déploiements) affiche les détails d'un déploiement unique stocké. Cliquez sur **Commit (Valider)** pour poursuivre le déploiement. Une

fois la validation terminée, le plug-in affiche le bouton Deploy (Déployer). Cliquez sur le bouton **Deploy (Déployer)** pour déployer le HSF CN-Series.

Après le déploiement HSF CN-Series, le cluster crée une pile de modèles, `<cluster-name>-ts` avec le modèle K8S-CNF-Clustering-Readonly et le modèle de variable que vous avez créé à l'étape 6 de la section Préparer Panorama pour le déploiement HSF CN-Series.



Le groupe d'appareils que vous avez référencé lors de la configuration du déploiement HSF (créé à l'étape 5 de la section Préparer Panorama pour le déploiement HSF CN-Series) et la pile de modèles créée automatiquement après le déploiement HSF sont amorcés dans le pod CN-MGMT. Lorsque le pod CN-MGMT se connecte à Panorama, le groupe d'appareils et la pile de modèles sont automatiquement associés au nom HSF.

Les informations HSF pour les pods CN-DB, CN-GW et CN-NGFW sont renseignées automatiquement lorsqu'elles sont actives. Lorsque ces pods sont opérationnels, le pod CN-MGMT envoie des détails tels que l'adresse IP CI, les détails du pod, l'ID de périphérique et la version logicielle à Panorama.

Pour Panorama Haute Disponibilité (HA), le pod CN-MGMT envoie des mises à jour aux Panoramas actifs et passifs.

Différents états de déploiement

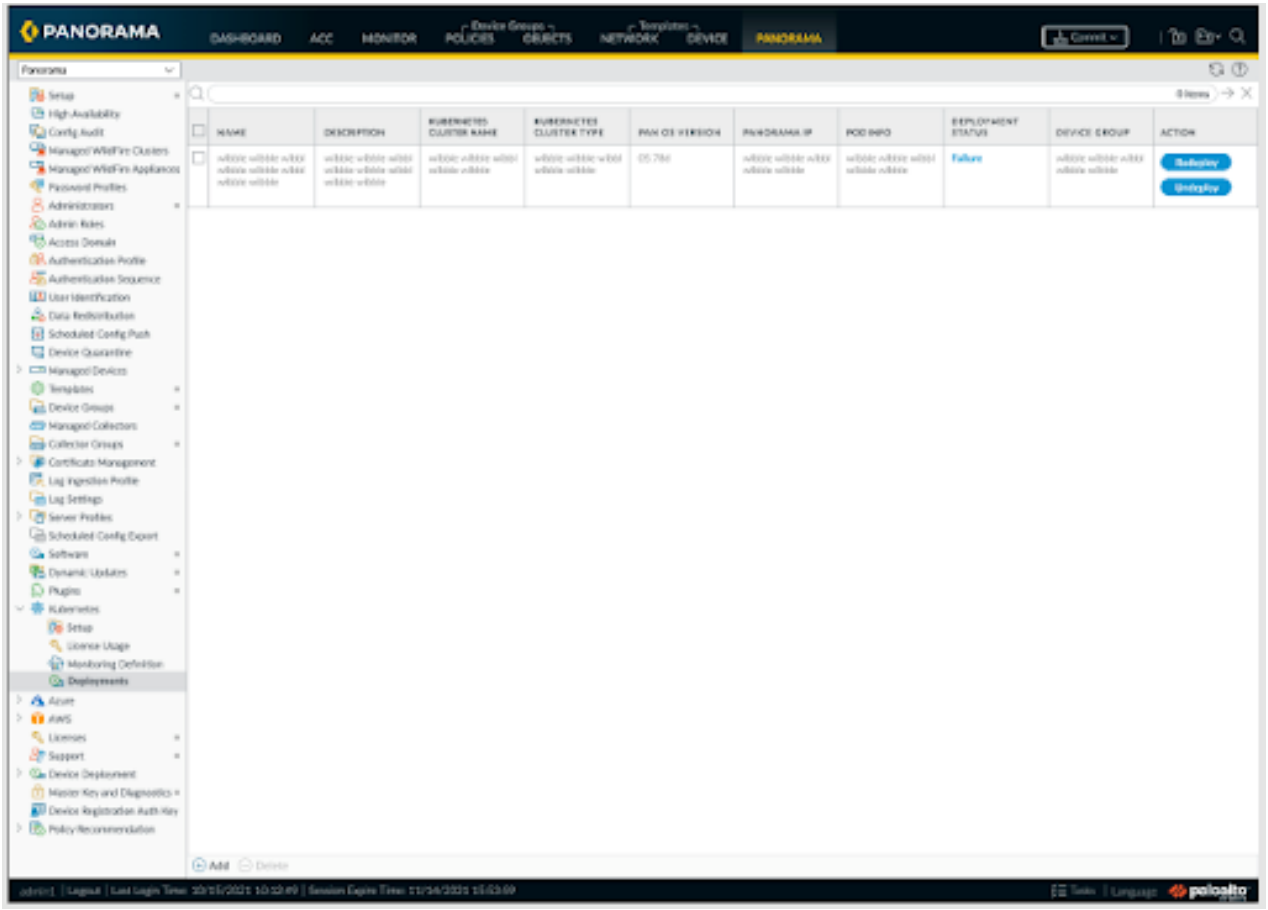
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Après avoir saisi tous les détails de configuration, l'onglet Deployments (Déploiements) affiche les détails d'un déploiement unique stocké. Un déploiement est composé de 5 étapes :

1. Validation requise
2. Non déployé
3. Déploiement
4. Avertissement
5. Réussite/Échec

1. Cliquez sur **Commit (Valider)** pour poursuivre le déploiement. Vous remarquerez peut-être que le bouton Deploy (Déployer) est désactivé et que l'état du déploiement passe à **Not Deployed (Non déployé)** une fois que vous avez cliqué sur Commit (Valider). Le bouton Deploy (Déployer) est activé une fois la validation terminée.
2. Cliquez sur Deploy (Déployer) pour poursuivre le déploiement du CNF CN-Series. L'état de déploiement passe à Deploying (Déploiement). Au cours de cette étape, les configurations Panorama sont créées. Les CN-GW sont alors générés et le plug-in commence à effectuer des appels d'API pour déployer le HSF CN-Series.
3. L'état Deploying (Déploiement) passe ensuite à **Warning (Avertissement)**, **Success (Réussite)**, ou **Failure (Échec)** en fonction de la disponibilité des ressources et des détails de configuration. Les boutons Redeploy (Redéployer) et Undeploy (Annuler le déploiement) sont alors activés.
4. Cliquez sur Redeploy (Redéployer) pour apporter des modifications aux paramètres activés et validez les modifications avant de cliquer sur Redeploy (Redéployer).
5. Cliquez sur **Undeploy (Annuler le déploiement)** pour supprimer tous les pods HSF CN-Series créés dans le cadre de ce déploiement.

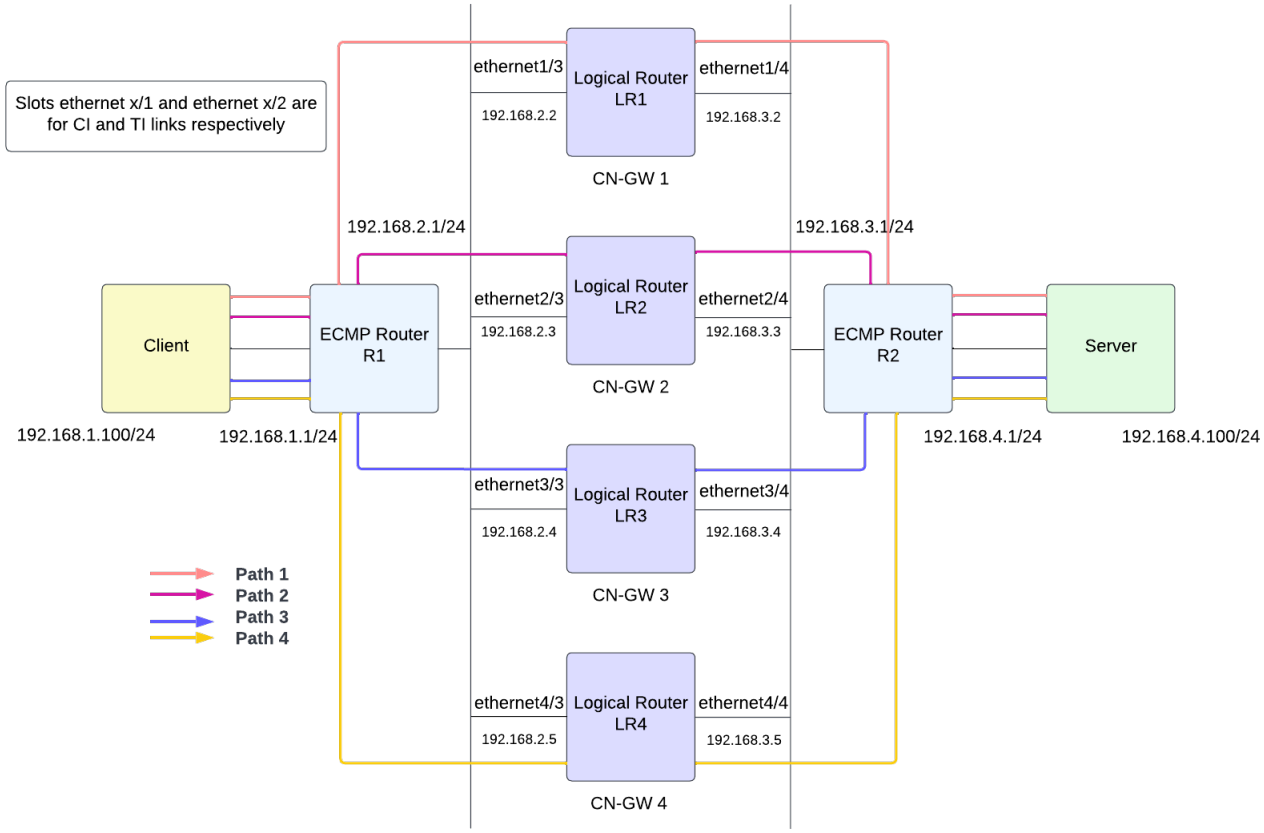
Toutes les configurations Panorama sont toujours conservées après la suppression de tous les pods HSF CN-Series.



Configurer le flux de trafic vers le HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF de la série CN	• CN-Series 11.0.x or above Container Images • Panorama sous PAN-OS 11.0.x ou version supérieure

Le routeur amont/aval utilise un algorithme ECMP basé sur le flux. Lorsque le trafic atteint CN-GW, il distribue le trafic à l'un des CN-NGFW disponibles par l'intermédiaire de la liaison d'interconnexion du trafic (TI) à l'aide d'un algorithme de hachage symétrique. Le trafic correspondant à une session dans les deux directions (client à serveur et serveur à client) passe toujours par le même CN-NGFW. Une fois que le CN-NGFW traite le trafic, et si vous avez défini une politique pour **Allow (Autoriser)** le trafic, le paquet de trafic est renvoyé au CN-GW pour atteindre le serveur.



STEP 1 | Créez un routeur logique sur le pare-feu pour participer au routage de couche 3.

1. Accédez à **Network (Réseau)** > **Routing (Routage)** > **Logical Router (Routeur logique)** et sélectionnez le modèle de variable dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez un routeur virtuel par défaut ou ajoutez un **Name (Nom)** pour le nouveau routeur logique.
3. Sélectionnez **General (Général)**, puis ajoutez une **Interface** déjà définie.

   Répétez cette étape pour ajouter toutes les interfaces que vous souhaitez ajouter au routeur logique.

   *Les interfaces ethernetX/1 et etehrnetX/2 sont réservées aux liaisons CI et TI, respectivement. Sélectionnez une interface entre **ethernet1/3** et **ethernet1/14**.*
4. Cliquez sur **OK**.
5. Définissez la distance administrative pour le routage statique. La plage est comprise entre 10 et 240 ; la valeur par défaut est 10.

   Définissez les distances administratives pour les types d'itinéraires nécessaires à votre réseau. Lorsque le routeur virtuel a deux itinéraires ou plus vers la même destination, il utilise la distance administrative pour choisir le meilleur chemin entre des protocoles de routage et itinéraires statiques différents en favorisant une distance plus courte.
6. Activez ECMP pour exploiter plusieurs chemins à coût égal pour le transfert.
7. Cliquez sur **OK**.

STEP 2 | Configurez l’interface de couche 3 pour activer le flux de trafic.

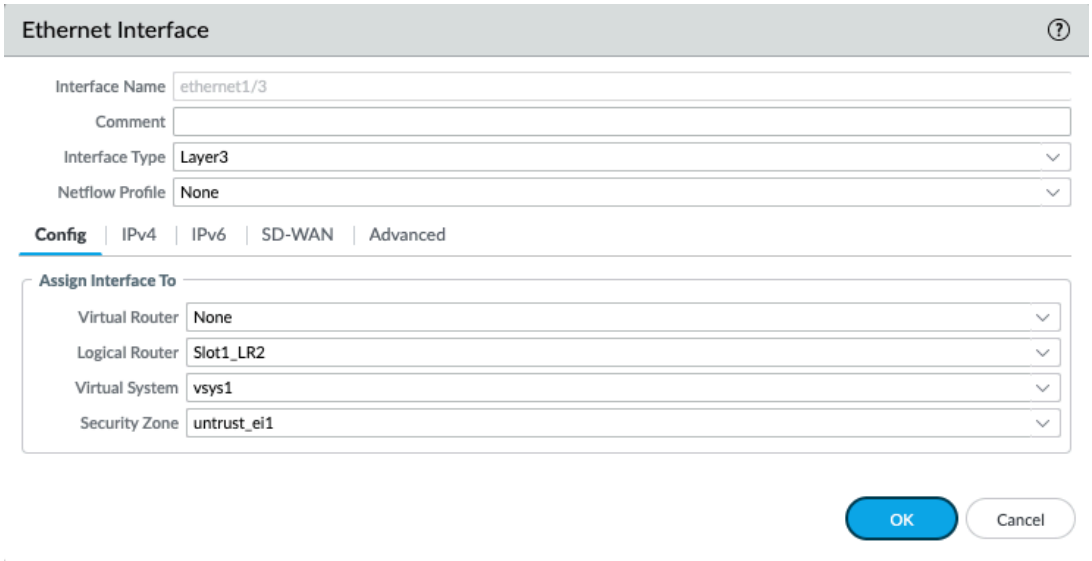
Lorsque vous procédez à l’étape Préparer Panorama pour le déploiement HSF CN-Series, il se peut que vous ayez créé un modèle de variable. Pour activer le flux de trafic par le réseau en cluster, vous devez configurer le modèle de variable avec la configuration de réseau et de trafic nécessaire à l’équilibrage de charge du HSF CN-Series. Vous devez configurer l’interface Ethernet de couche 3 avec des adresses IPv4 afin que le pare-feu puisse effectuer le routage sur ces interfaces. En général, vous utiliserez cette procédure pour configurer une interface externe qui se connecte à l'Internet et une interface pour votre réseau interne.

Vous pouvez configurer ce modèle avant ou après le déploiement du HSF CN-Series.

*Veillez à ne pas chevaucher la configuration de ce modèle avec le modèle **K8S-CNF-Clustering-Readonly** créé automatiquement lors de l’installation du plug-in Kubernetes.*

1. Accédez à **Network (Réseau)** > **Interfaces**, puis sélectionnez le modèle de variable dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez l’interface **Ethernet** pour **Add Interface (Ajouter une interface)**.
3. Sélectionnez un **Slot (Emplacement)** entre 1 et 30.
4. Saisissez un **Interface Name (Nom d’interface)** entre **`ethernet1/3`** et **`ethernet1/14`**.
5. Sous **Interface Type (Type d’interface)**, sélectionnez **Layer 3 (Couche 3)**.

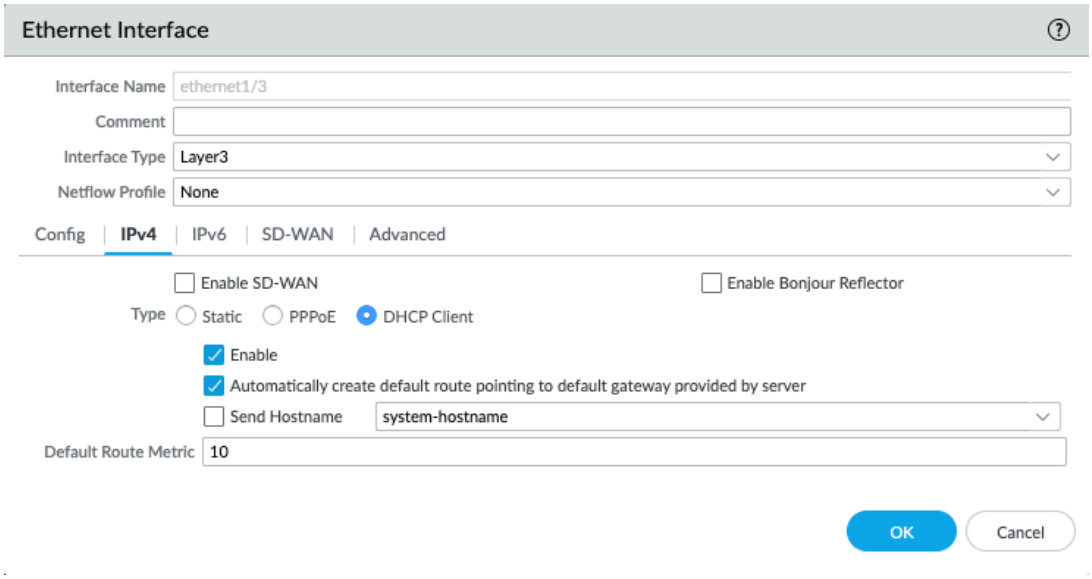
6. Sur l’onglet **Config (Configuration)** :
   - Pour **Logical Router (Routeur logique)**, sélectionnez le routeur logique configuré à l’étape 1.
   - Sous **Virtual System (Système virtuel)**, sélectionnez le système virtuel que vous configurez s'il se trouve sur un pare-feu de systèmes virtuels multiples.
   - Sous **Security Zone (Zone de sécurité)**, sélectionnez la zone à laquelle l'interface appartient ou créez une **New Zone (Nouvelle zone)**.



7. Dans l’onglet **IPv4**, sélectionnez **DHCP Client (Client DHCP)**.

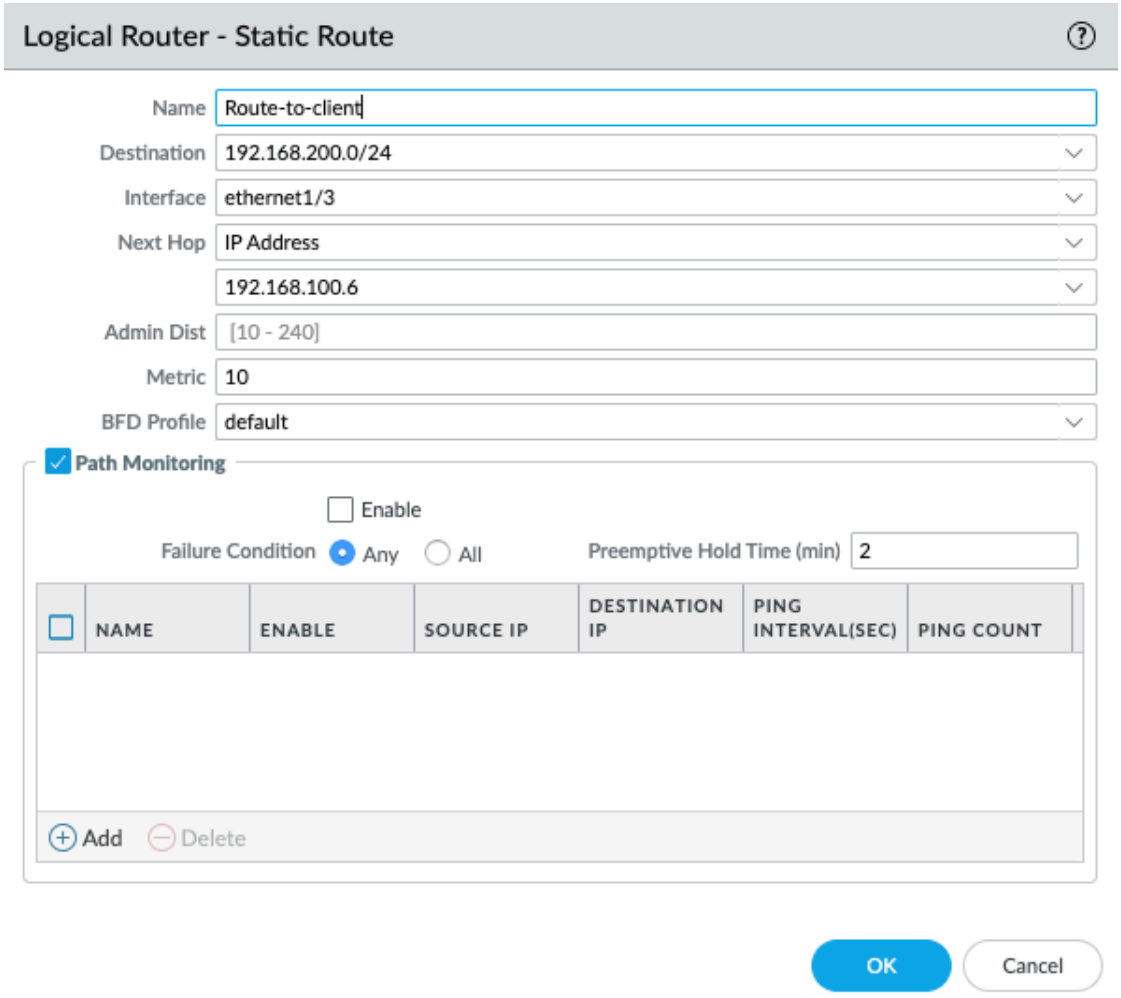
   L’interface du pare-feu agit en tant que client DHCP et reçoit une adresse IP affectée de façon dynamique. Le pare-feu permet également de propager les paramètres reçus par l'interface du client DHCP dans un serveur DHCP actif sur le pare-feu. Pour plus d’informations, reportez-vous à la section Configuration d’une interface en tant que client DHCP.

8. Cliquez sur **OK**.



STEP 3 | Configurez des itinéraires statiques pour le routeur logique.

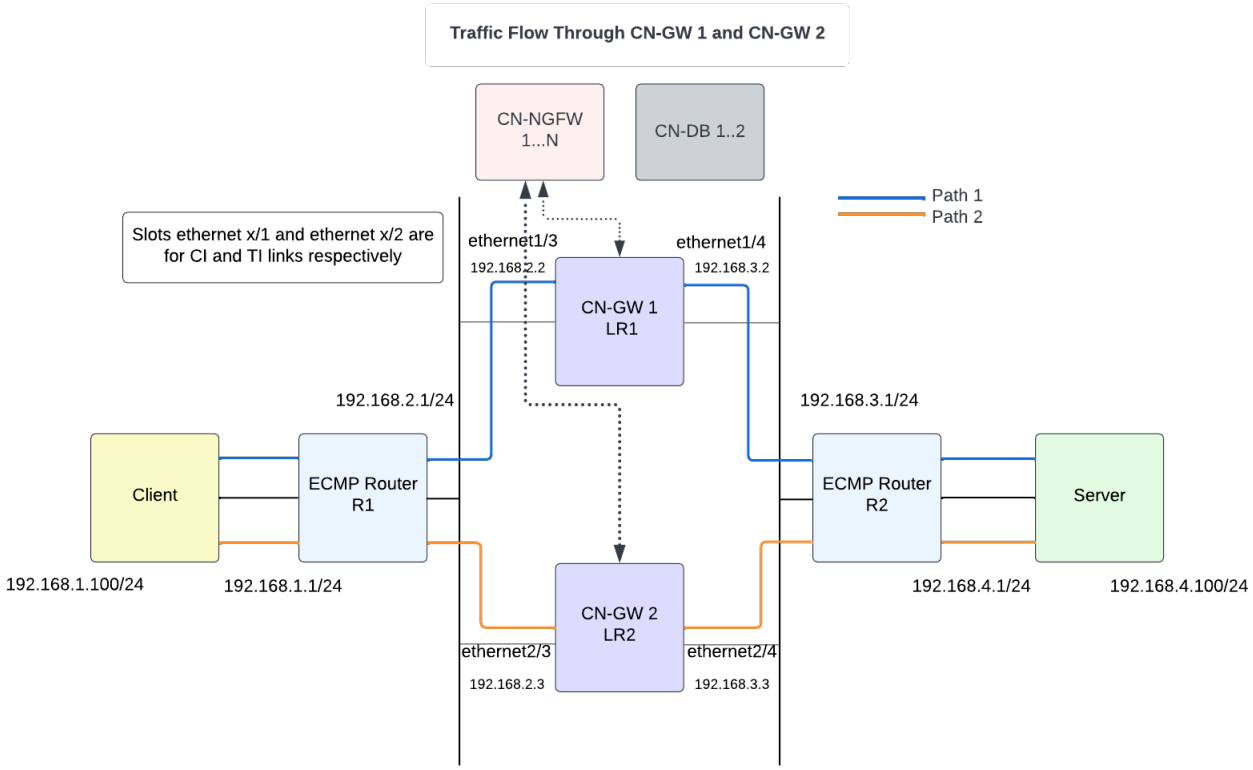
1. Accédez à **Network (Réseau)** > **Routing (Routage)** > **Logical Router (Routeur logique)**, puis sélectionnez le modèle de variable dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez l'onglet **Static (Statique)** > **IPv4** et cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name (Nom)** pour l'itinéraire statique.
4. Saisissez l'itinéraire de **Destination** et le masque réseau. Par exemple, 192.168.200.0/24.
5. Sélectionnez l'interface sortante que les paquets doivent utiliser pour atteindre le saut suivant.
6. Pour **Next Hop (Saut suivant)**, sélectionnez **ip-address** et saisissez l'adresse IP de votre passerelle interne. Par exemple, 192.168.100.2.
7. Saisissez une **Admin Distance (Distance admin)** si vous souhaitez que l'itinéraire remplace la distance administrative par défaut qui a été définie pour les itinéraires statiques de ce routeur logique (plage comprise entre 10 et 240 ; valeur par défaut : 10).
8. Saisissez une **Metric (Mesure)** pour l'itinéraire (plage comprise entre 1 et 65 535).
9. Appliquez un **BFD Profile (Profil BFD)** à l'itinéraire statique. Ainsi, en cas d'échec de l'itinéraire statique, le pare-feu supprime l'itinéraire et utilise un autre itinéraire. Valeur par défaut : **Aucune**.
10. Cliquez sur **OK**.



Scénario de test : gestion des pannes CN-GW basée sur une BFD de couche 3

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Ce test évalue la configuration BFD requise pour gérer les pannes CN-GW. Un profil BFD gère les pannes CN-GW sur les routeurs amont/aval.



Flux de trafic symétrique

- Si l’interface de trafic d’entrée est CN-GW 1, la recherche d’itinéraire pour trouver l’interface de sortie se trouve sur LR1.
  - Itinéraire 1 : destination : sous-réseau client ; saut suivant : R1
  - Itinéraire 2 : destination : sous-réseau du serveur ; saut suivant : LR2

- Si l’interface de trafic d’entrée est CN-GW 2, la recherche d’itinéraire pour trouver l’interface de sortie se trouve sur LR2.
  - Itinéraire 1 : destination : sous-réseau client ; saut suivant : R1
  - Itinéraire 2 : destination : sous-réseau du serveur ; saut suivant : R2

Flux de trafic asymétrique

Le HSF CN-Series prend également en charge le flux de trafic asymétrique. Par exemple, la session 1 de correspondance de trafic client à serveur passant par CN-GW 1 et la session 1 de correspondance de trafic serveur à client passant par CN-GW 2. Pour un flux de trafic asymétrique, toutes les interfaces faisant face à R1 doivent se trouver dans la même zone. De même, toutes les interfaces faisant face à R2 doivent se trouver dans la même zone.

Routage inter-LR

Par exemple, si l’interface de trafic d’entrée est CN-GW 1, la recherche d’itinéraire pour trouver l’interface de sortie se trouve sur LR1. S’il existe un itinéraire pour atteindre le serveur avec le saut suivant étant LR2, CN-NGFW envoie alors le trafic à LR2. Sur la base de la recherche d’itinéraire LR2 CN-GW 2, le paquet est envoyé au serveur.

STEP 1 | Accédez à **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **BFD**, puis sélectionnez le modèle de variable dans la liste déroulante **Template (Modèle)**.

Vous devez activer BFD sur les routeurs externes et les routeurs logiques.

STEP 2 | Cliquez sur **Add (Ajouter)** pour ajouter le profil BFD.

STEP 3 | Saisissez un **Name (Nom)**.

STEP 4 | Sélectionnez le **Mode (Mode)** sous lequel la BFD fonctionne :

- **Active (Actif)** : la BFD initie l'envoi de paquets de contrôle vers l'homologue (par défaut). Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux.
- **Passive (Passif)** : la BFD attend que l'homologue envoie des paquets de contrôles et réponde comme il se doit.

STEP 5 | Saisissez le **Desired Minimum Tx Interval (ms) (Intervalle de transmission minimum souhaité (ms))**. Il s'agit de l'intervalle minimal, en millisecondes, auquel vous voulez que le protocole BFD (appelé BFD) envoie des paquets de contrôles BFD ; vous négociez ainsi l'intervalle de transmission avec l'homologue.

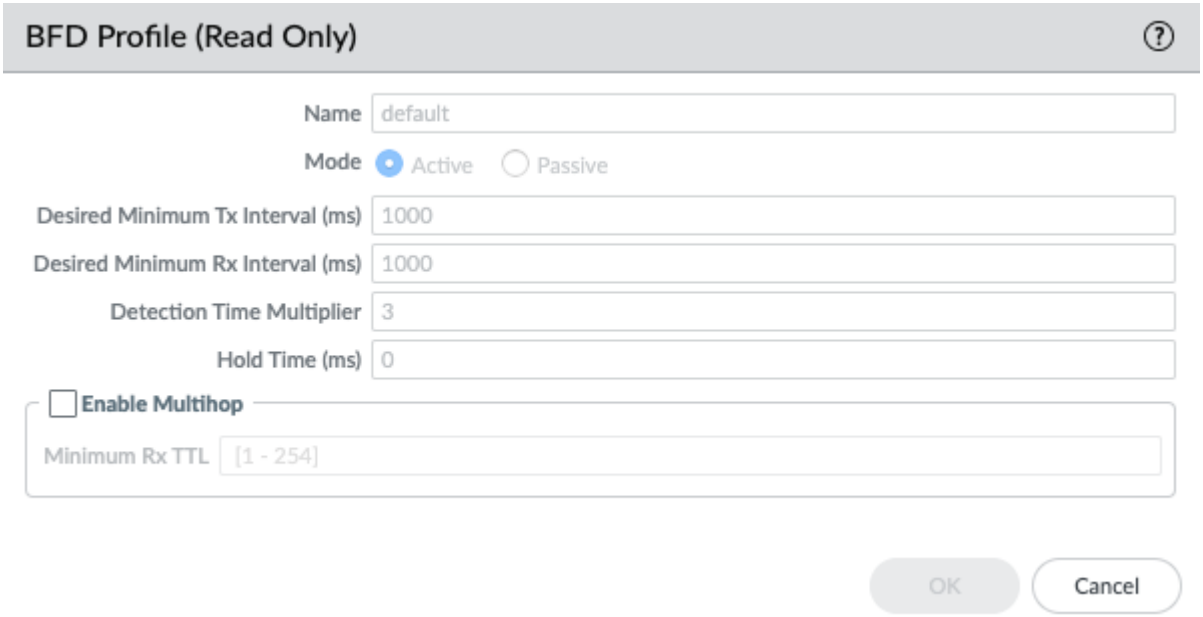
STEP 6 | Saisissez le **Detection Time Multiplier (Multiplicateur de délai de détection)**. Le système local calcule le délai de détection en tant que **Detection Time Multiplier (Multiplicateur de délai de détection)** reçu du système distant multiplié par l’intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Required Minimum Rx Interval (Intervalle de réception minimum requis)** et le dernier **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu. La plage est comprise entre 2 et 50 ; la valeur par défaut est 3.

STEP 7 | Saisissez le **Hold Time (ms) (Temps d'attente (ms))**. Il s'agit du délai, en millisecondes, entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par la BFD. Le **Hold Time (Temps d'attente)** ne s'applique qu'au mode Actif de la BFD. Si la BFD reçoit des paquets de

contrôles BFD pendant le **Hold Time (Temps d'attente)**, ceux-ci sont ignorés. La plage est comprise entre 0 et 120 000 ; la valeur par défaut est 0.

STEP 8 | Sélectionnez **Multihop (Multi-sauts)** pour activer la BFD pour le protocole BGP à sauts multiples. Saisissez la **Minimum Rx TTL (TTL de réception minimum)**. Il s'agit de la valeur Time-to-Live (Durée de vie ; TTL) minimale (nombre de sauts) que la BFD acceptera (recevra) dans un paquet de contrôles BFD lorsque le protocole BGP prend en charge la BFD à sauts multiples. (Plage comprise entre 1 et 254 ; aucune valeur par défaut).

STEP 9 | Cliquez sur **OK** pour enregistrer le profil BFD.



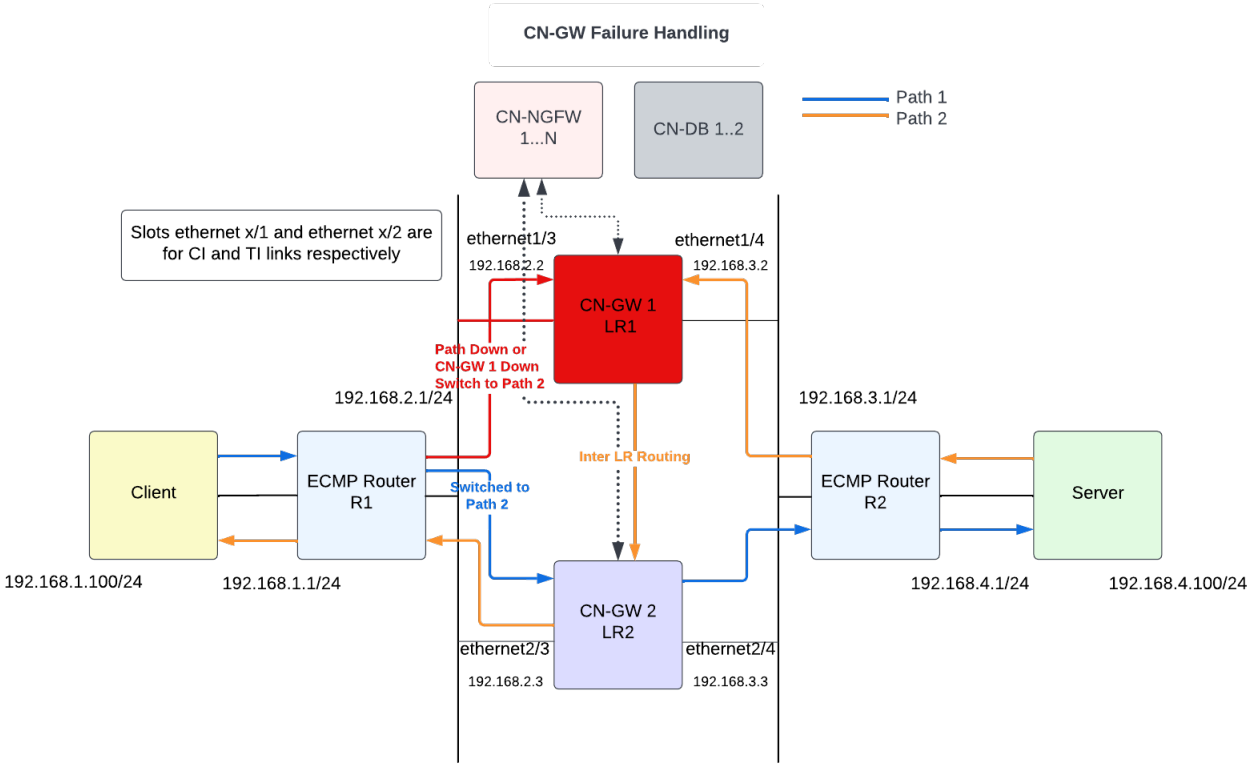
STEP 10 | Configurez des itinéraires statiques pour le routeur logique.

1. Accédez à **Network (Réseau)** > **Routing (Routage)** > **Logical Router (Routeur logique)**, puis sélectionnez le modèle de variable dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez l'onglet **Static (Statique)** > **IPv4** et cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name (Nom)** pour l'itinéraire statique.
4. Saisissez l'itinéraire de **Destination** et le masque réseau. Par exemple, 192.168.200.0/24.
5. Sélectionnez l'interface sortante que les paquets doivent utiliser pour atteindre le saut suivant.
6. Pour **Next Hop (Saut suivant)**, sélectionnez **ip-address** et saisissez l'adresse IP de votre passerelle interne. Par exemple, 192.168.100.2.
7. Saisissez une **Admin Distance (Distance admin)** si vous souhaitez que l'itinéraire remplace la distance administrative par défaut qui a été définie pour les itinéraires statiques de ce routeur logique (plage comprise entre 10 et 240 ; valeur par défaut : 10).
8. Saisissez une **Metric (Mesure)** pour l'itinéraire (plage comprise entre 1 et 65 535).
9. Appliquez le **BFD Profile (Profil BFD)** créé lors des étapes précédentes à l'itinéraire statique. Ainsi, en cas d'échec de l'itinéraire statique, le pare-feu supprime l'itinéraire et utilise un autre itinéraire.
10. Cliquez sur **OK**.

La configuration BFD prend en charge les pannes CN-GW et de chemin d'accès. Dans le diagramme de flux de trafic suivant, tenez compte de la présence de deux sessions SSH entre le client et le serveur. La session 1 passe par le chemin 1 et la session 2 passe par le chemin 2. Si le pod CN-GW 1 ou le chemin 1 est en panne, la configuration BFD entre R1 et le pod CN-GW 1, R2 et le pod CN-GW 1 aide R1 à identifier la panne du chemin et envoie le trafic par le biais du chemin 2. Les interfaces faisant face à R1 doivent se trouver dans la même zone. De même, les interfaces faisant face à R2 doivent se trouver dans la même zone.

Itinéraire 1 : destination : sous-réseau client ; le saut suivant est R1, métrique 10

Itinéraire 2 : destination : sous-réseau du serveur ; le saut suivant est LR2, métrique 11

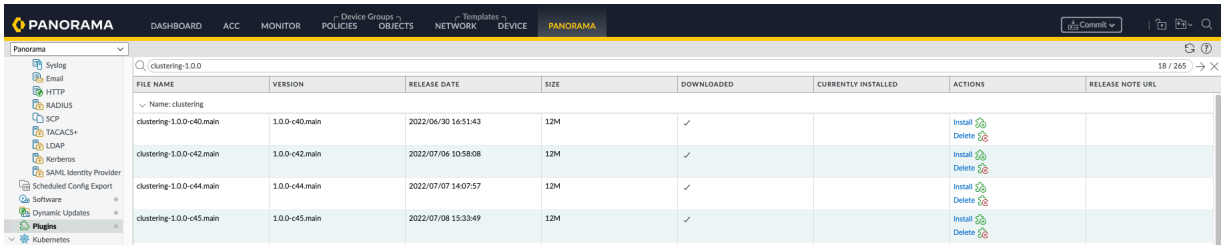


Afficher le résumé et la surveillance du HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

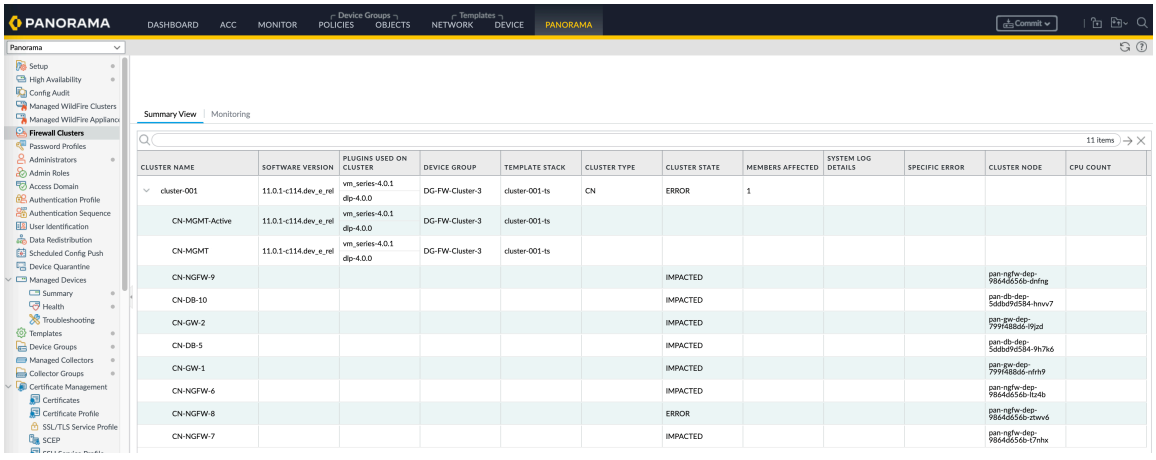
Vous pouvez afficher les informations de résumé et de surveillance du HSF CN-Series sous l'onglet **Firewall Clusters (Clusters de pare-feu)** dans l'interface Web Panorama. Pour afficher les clusters de pare-feu et y accéder, vous devez **Enable (Activer)** > **Firewall Clusters (Clusters de pare-feu)** depuis la liste **Panorama** > **Admin Roles (Rôles admin)** > **Web UI (Interface utilisateur Web)**. Pour plus d'informations, reportez-vous à la section Configuration d'un profil de rôle admin.

Vous devez installer le plug-in Clustering 1.0.0 à partir de **Panorama** > **Plugins (Plug-ins)** pour afficher les détails de cluster sous **Firewall Clusters (Clusters de pare-feu)**.



Vue récapitulative

Affichez les informations concernant les clusters CN-Series capturés par le pare-feu au cours des cinq dernières minutes. Cliquez sur le bouton d'actualisation pour charger les derniers détails.

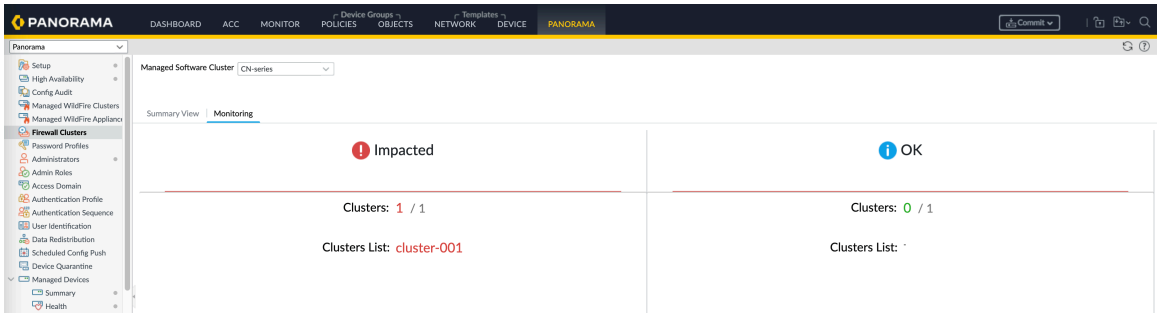


Champ	Description
Nom du cluster	Nom du cluster de pare-feu.

Champ	Description
Version du logiciel	Version PAN-OS.
Plug-ins utilisés sur le cluster	Liste des plugins utilisés sur le cluster.  *Seuls les plug-ins de pare-feu CN-Series sont pris en charge.*
Pile de modèles	Nom de la pile de modèles associée au cluster.
Groupe de périphériques	Nom du groupe de périphériques associé au cluster.
État du cluster	Indique si le cluster est affecté ou non.
Type de cluster	Type de cluster.  *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.*
Membres touchés	Nombre de membres du cluster affectés et leurs noms.
Détails du journal système	Affiche les détails des événements système.
Erreur spécifique	Liste des erreurs spécifiques dans le cluster. Cliquez sur le lien pour afficher davantage de détails sur l'erreur sous **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)**, où vous pouvez afficher les journaux.
Nœud de cluster	Nom du pod.
Nombre de CPU	Nombre de processeurs utilisés.

Surveillance

Affichez les informations sur l'état de santé du cluster de pare-feu CN-Series.



Champ	Description
Cluster de logiciels gérés	Sélectionnez un cluster de pare-feu. *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.*
Touchés	Liste des clusters de pare-feu affectés. • **CN-Clusters (Clusters CN)** – Nombre de clusters de pare-feu CN-Series affectés. • **Clusters Impacted (Clusters affectés)** – Affiche la liste des clusters affectés. Cliquez pour afficher des informations détaillées sur les clusters dans les tableaux de bord **Interconnect Status (État de l'interconnexion)** et **Cluster Utilization (Utilisation du cluster)**.
OK	Liste des clusters de pare-feu qui ne sont pas affectés. • **Clusters** – Nombre de clusters de pare-feu CN-Series qui ne sont pas affectés. • **Clusters List (Liste des clusters)** – Affiche la liste des clusters qui ne sont pas affectés. Cliquez pour afficher des informations détaillées sur les clusters dans les tableaux de bord **Interconnect Status (État de l'interconnexion)** et **Cluster Utilization (Utilisation du cluster)**.
État de l'interconnexion	Affichez les détails d'interconnexion du cluster pour une période sélectionnée. Sélectionnez **Last 5 Mins (5 dernières minutes)** pour afficher les détails suivants. • **Cluster Name (Nom du cluster)** – Nom du cluster de pare-feu. • **Cluster Type (Type de cluster)** – Type de cluster. *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.* • **Cluster Creation Time (Heure de création du cluster)** – Heure de création du cluster.

Champ	Description

	• **Current Cluster State (État actuel du cluster)** – Indique si le cluster est affecté ou non.
	  • **Current Cluster Detail (Détails actuels du cluster)** – Cliquez sur le lien de l'état actuel du cluster pour afficher davantage de détails sur le cluster affecté.
	• **Cluster Interconnect Status (État de l'interconnexion du cluster)** – Affiche l'interconnectivité du cluster.
	  • **Current Cluster Detail (Détails actuels du cluster)** – Cliquez sur le lien de l'état actuel de l'interconnexion pour afficher davantage de détails sur le cluster affecté.
	• **Traffic Interconnect (Interconnexion du trafic)** – État de l'interconnectivité du trafic.
	• **External Connection (Connexion externe)** – État de la connectivité externe.
	• **Impacted Links (Liaisons affectées)** – Nombre de liaisons affectées.
	• **Management Connectivity (Connectivité de gestion)** – Nombre de connexions de gestion.
	• **Impacted Cluster Member (Membre de cluster affecté)** – Liste des membres de cluster affectés.
	• **Time Stamp Hi-Res Uptime (Horodatage haute résolution du temps de disponibilité)** – Horodatage du temps de disponibilité.
	• **Time Stamp Hi-Res Downtime (Horodatage haute résolution du temps d'interruption)** – Horodatage du temps d'interruption.
	En cas de sélection de toute autre période, seules les informations suivantes apparaissent.
	• **Nom du cluster**
	• **Type de cluster**
	• **Temps de création du cluster**
	• **État actuel du cluster**
	• **État de l'interconnexion du cluster**
	• **Interconnexion du trafic**
	• **Connexion externe**

Utilisation du cluster	Affichez le débit, la mémoire et l'utilisation des données du cluster de pare-feu. • **Cluster Name (Nom du cluster)** – Nom du cluster de pare-feu. Le développement du nom du cluster affiche les détails de tous les pods de ce cluster. • **Cluster Details (Détails du cluster)** – Cliquez sur le lien du nom du cluster pour afficher les détails relatifs au débit, à la mémoire et à l'utilisation des données du cluster sélectionné.

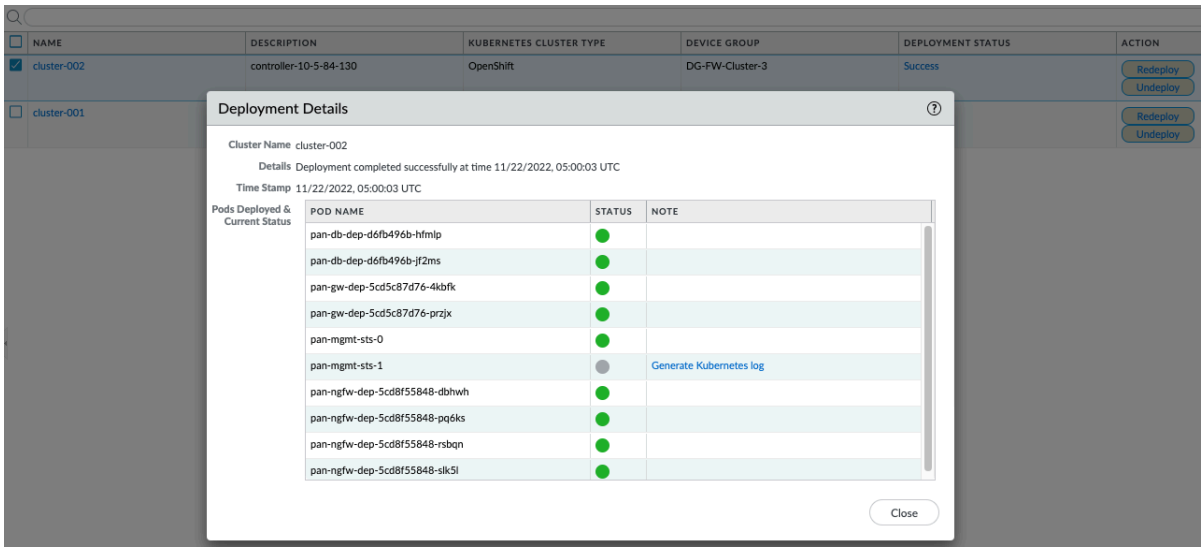
Champ	Description
	• **Cluster Type (Type de cluster)** – Type de cluster. *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.* • **Cluster State (État du cluster)** – Affiche l'état de santé du cluster. • **Cluster Throughput (gbps) (Débit du cluster [Gbit/s])** – Débit du cluster de pare-feu en Gbit/s. • **CPS** – Nombre de connexions par seconde. • **Session Count (Sessions) (Nombre de sessions [Sessions])** – Nombre de sessions. • **Average Data Plane (%) Within Health Threshold (Plan de données moyen [%] dans le seuil de santé)** – Seuil moyen du plan de données en pourcentage. • **Management Plane CPU (%) (Processeur du plan de gestion [%])** – Utilisation du processeur du plan de gestion en pourcentage. • **Management Plane Mem (%) (Mémoire du plan de gestion [%])** –Utilisation de la mémoire du plan de gestion en pourcentage. • **Logging Rate (Log/Sec) (Taux de journalisation [Journaux/s])** – Taux auquel les journaux sont générés sur le cluster. • **DP Auto-Scale Status (État de mise à l'échelle automatique DP)** – Détails de la mise à l'échelle automatique du plan de données.

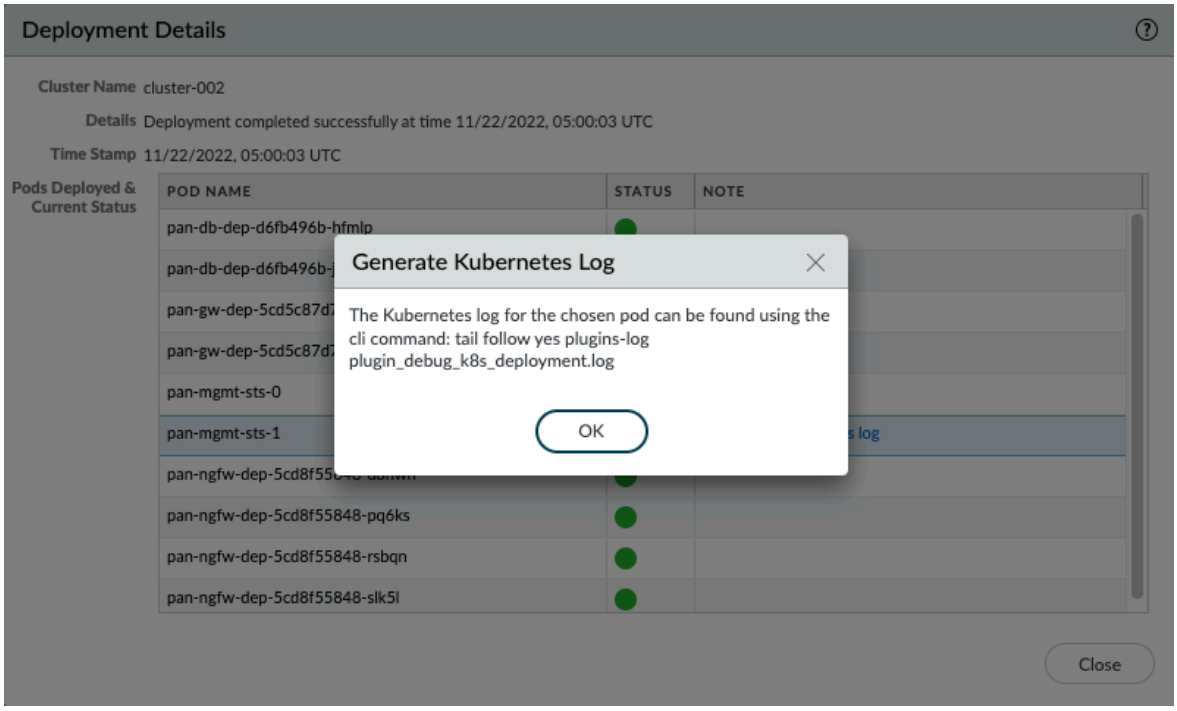
Validation du déploiement HSF CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Vous pouvez valider les déploiements HSF CN-Series dans la section **Deployment (Déploiement)**, sous **Panorama** > **Kubernetes**. Cliquez sur le lien sous **Deployment Status (État du déploiement)** pour afficher les détails du déploiement.

Les pods déployés et leur état actuel sont codés par couleur et affichés dans la section **Deployment Status (État du déploiement)**. Vous pouvez cliquer sur le lien sous la **Note (Remarque)** en lien avec le déploiement de pod échoué pour afficher davantage de détails.





Utilisez les commandes suivantes dans la CLI Panorama pour générer des journaux.

```
debug plugins kubernetes generate-pod-log deployment_name pod_name
 <value> Name of the pod
```

```
show plugins kubernetes deployment-status
```

```
show plugins kubernetes deployment-details name
```

Débogage des problèmes de synchronisation entre le plug-in Kubernetes et le HSF CN-Series

Le plug-in Kubernetes collecte des informations sur le HSF CN-Series à partir de pods, de services et de nœuds à l'aide d'API Watch. L'API Watch est une API basée sur les notifications qui envoie des mises à jour lorsque l'état d'un cluster change. Pour veiller à ce que le plug-in et le HSF CN-Series déployé soient synchronisés, le plug-in écoute les notifications et affiche les notifications HPA et d'événements de mise à niveau/rétrogradation.

Le plug-in utilise les commandes de débogage suivantes pour déboguer un nœud spécifique en fonction de l'état du plug-in.

```
debug plugin kubernetes kubectl-logs pod <pod-name>
```

Cette commande debug génère un fichier journal qui contient les journaux `kubectl` describe pour le nœud transmis dans la commande, et est enregistrée dans le fichier de journaux du plug-in.

HPA basé sur des métriques personnalisées utilisant KEDA au sein d'environnements EKS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

L'implémentation HPA dans les environnements EKS nécessite l'utilisation du module KEDA (Kubernetes-based Event Driven Autoscaler). Les conditions préalables à l'implémentation HPA basée sur des métriques personnalisées sont les suivantes :

- Activez HPA pour la mise en cluster à partir de YAML.
  - Vérifiez que les paramètres HPA sont remplis dans le fichier pan-cn-mgmt-configmap.yaml.
  - Vérifiez que le champ `PAN_NAMESPACE_EKS` possède un nom unique dans votre compte AWS au sein de votre région. Cela évite d'écraser les métriques de différents clusters CN avec le même espace de noms EKS.
- Publication par CN-MGMT de métriques sur Cloudwatch.

  Le pod CN-MGMT requiert les autorisations nécessaires pour accéder à la ressource Cloudwatch, collecter des métriques CN-NGFW et publier des métriques personnalisées sur Cloudwatch. Pour ce faire, ajoutez la politique `CloudWatchFullAccess` au rôle IAM de nœud que vous avez spécifié lors de la création du groupe de nœuds.
- Déployez le module de mise à l'échelle automatique de cluster à partir d'AWS. Pour plus d'informations, reportez-vous à la section Module de mise à l'échelle automatique de cluster.

Authentifier KEDA avec AWS

Pour authentifier KEDA, vous pouvez associer un rôle IAM au compte de service opérateur KEDA en annotant le role-arn dans le compte de service KEDA. Cette étape est recommandée, car elle évite d'ajouter un accès Cloudwatch au rôle IAM de nœud et permet uniquement au compte de service KEDA d'accéder à Cloudwatch et non au nœud entier sur lequel KEDA s'exécute.

Pour associer un rôle IAM au compte de service opérateur KEDA :

1. Créez un fournisseur OIDC IAM pour votre cluster : vous ne devez créer un fournisseur OIDC IAM qu'une seule fois pour un cluster.
2. Créez un rôle IAM et attachez-y une politique IAM avec les autorisations dont vos comptes de service ont besoin. Veillez à fournir la politique d'accès Cloudwatch lors de l'exécution de cette étape.
3. Associez un rôle IAM à un compte de service : effectuez cette tâche pour chaque compte de service Kubernetes qui a besoin d'accéder à des ressources AWS.
4. Déployez le module de mise à l'échelle automatique de cluster à partir d'AWS. Pour plus d'informations, reportez-vous à la section Module de mise à l'échelle automatique de cluster.

Déployer les pods KEDA

Pour déployer les pods Keda, téléchargez les derniers fichiers KEDA.

```
kubectl apply -f keda-2.7.1.yaml
```

Le plug-in modifie et applique le yaml en fonction des entrées que vous fournissez selon vos exigences en matière de mise à l’échelle.

Observez les valeurs dans la console Cloudwatch et vérifiez la manière dont les pods cibles augmentent et diminuent.

Configurer le routage dynamique dans le HSF série CN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• Panorama fonctionnant avec la version minimale de PAN-OS 11.1

Hyperscale Security Fabric (HSF) de la série CN introduit désormais le routage dynamique via les protocoles BGP et BGP sur BFD. Grâce au routage dynamique, vous pouvez obtenir un routage de couche 3 stable, performant et hautement disponible grâce à des listes de filtrage basées sur les profils et des cartes de routage conditionnelles qui peuvent être utilisées sur les routeurs logiques. Ces profils fournissent une granularité plus fine pour filtrer les routes pour chaque protocole de routage dynamique et améliorent la redistribution des routes sur plusieurs protocoles.

BGP recherche les chemins disponibles que les données pourraient emprunter et sélectionne le meilleur itinéraire, en fonction des préfixes IP disponibles dans les systèmes autonomes. La configuration BFD (Bidirectionnel Forwarding Detection) gère les pods CN-GW et les échecs de chemin.

Pour activer le routage dynamique, vous devrez configurer le cluster Panorama et CN-Series HSF. Vous aurez besoin d'au moins 2 CN-MGMT, 2 CN-NGFW, 2 CN-DB et 1 CN-GW dans le cluster. L'appairage BGP est configuré entre le cluster CN et le routeur externe.

Sur le HSF de la série CN, le routage dynamique sera pris en charge sur PANOS 11.xx Pour plus d'informations sur l'obtention de PAN-OS 11.0, consultez Obtenir les images et les fichiers pour le déploiement de la série CN.

Dans Panorama, vous devrez configurer les groupes de périphériques et gérer le cluster HSF via le groupe d'appareils. Pour configurer le cluster HSF, consultez Déployer le cluster HSF.

Pour configurer BGP sur le cluster HSF, vous devrez effectuer les étapes suivantes :

1. Activer le module de routage avancé.
2. Configurer un routeur logique.
3. Créez une route statique pour l'interface de bouclage CN-GW.
4. Configurer BGP sur un moteur de routage avancé.

   1. *Actuellement, seul IPv4 est pris en charge sur le routage BGP.*
   2. *Lors de la création d'un homologue, assurez-vous de créer une session de bouclage et de fournir une adresse IP de bouclage pour chaque CN-GW dans l'onglet* ***Adressage*** .
5. (facultatif) Créez des profils de routage BGP pour l'authentification, les minuteries, les familles d'adresses, l'amortissement, la redistribution des routes vers BGP et le filtrage BGP.
6. (facultatif) Créez des filtres pour le moteur de routage avancé, tels que des listes d'accès, des listes de préfixes, des listes d'accès AS Path, des listes de communauté et des cartes de routage.
7. Cliquez sur **Commit to Panorama (Valider sur Panorama)**. Une fois la configuration validée dans Panorama, BGP sera configuré sur chaque CN-GW.

Pour vérifier l'état BGP, connectez-vous à CN-MGMT et exécutez les commandes suivantes :

- `afficher le résumé BGP du routage avancé`


```
admin@pan-mgmt-sts-1.cluster-001> show advanced-routing bgp route logical-router slot1-LR-1

Status codes:  R removed, d damped, * valid, r ribFailure, S stale, = multipath,
               s suppressed, i internal, > best, h history
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  e egp, i igp, ? incomplete

Logical router: slot1-LR-1
BGP table version is 10, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24           0.0.0.0                  0    100  32768  i
*> 192.168.85.0/24      200.0.0.1                0    100      0 22 i
------------------------------------------------------------------------------
Displayed 2 route(s) 2 path(s)

Logical router: slot1-LR-1
BGP table version is 0, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
------------------------------------------------------------------------------
Displayed 0 route(s) 0 path(s)

admin@pan-mgmt-sts-1.cluster-001> show advanced-routing route type bgp logical-router slot1-LR-1



Logical Router: slot1-LR-1
==========================
flags: A:active, E:ecmp, Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext 1, O2:ospf ext 2

destination                             protocol        nexthop                                 distance  metric    flag      tag       age          inte
ace
192.168.85.0/24                         bgp             200.0.0.1                               20        0         A E               00:04:07

192.168.85.0/24                         bgp             2.2.2.222                               20        0         A E               00:04:07     ethe
et1/3
total route shown: 2
```

- afficher l’état du homologue BGP de routage avancé

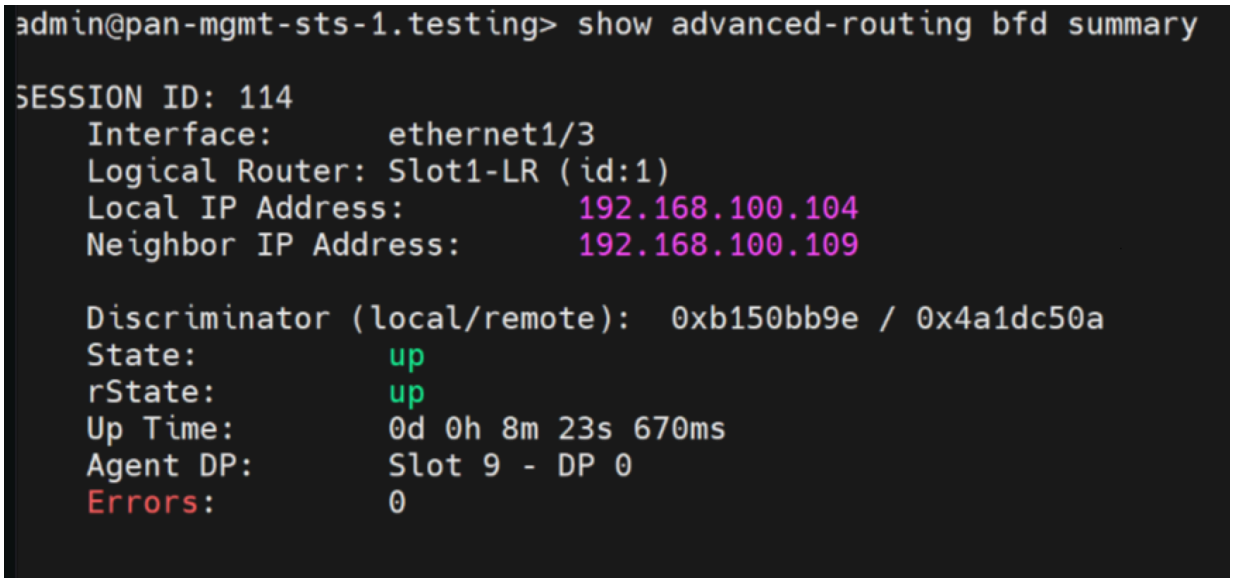
```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer status peer-name DHCP-PEER

Logical Router: Slot1-LR
==============
Peer Name:              DHCP-PEER
BGP State:              Established, up for 00:01:15
```


- afficher les détails du homologue BGP de routage avancé


```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer details

Peer: DHCP-PEER
==============
Peer name                   DHCP-PEER
Logical router:             Slot1-LR
Remote router ID:           11.11.11.1
Remote AS:                  65008
Remote address:             192.168.100.109:34986
Local address:              192.168.100.102:179
Peer group:                 DHCP-BGP
Peer status:                Established
Up time:                    188 s
Hold time:                  90 s (configured 90)
Keepalive interval:         30 s (configured 30)
Connection retry timer:     15 s
Estimated RTT:              3 ms
Last reset time:            222 s ago
Last reset reason:          No AFI/SAFI activated for peer
BGP connection:             sharedNetwork
Connection established:     2
Connection dropped:         1

Address family:             ipv4Unicast
  Packet queue length:      0
  Update group id:          2
  Sub group id:             2
  Prefix allowed Max:       1000 (warning-only)
  Prefix accepted:          2810
  Prefix Sent:              2920
  Prefix allowed Max warnning: True
  Prefix allowed warnning threshold: 100
  Inbound soft reconfiguration allowed: True

Neighbor capabilities:
  4byteAs                   advertisedAndReceived
  extendedMessage           advertisedAndReceived
  addPath                   {'ipv4Unicast': {'rxAdvertisedAndReceived': True}}
  routeRefresh              advertisedAndReceivedOldNew
  enhancedRouteRefresh      advertisedAndReceived
  multiprotocolExtensions   {'ipv4Unicast': {'advertisedAndReceived': True}}
  hostName                  {'advHostName': 'pan-mgmt-sts-1.testing', 'advDomainName': 'n/a', 'rcvHostName': 'vyos', 'rcvDomainName': 'n/
  gracefulRestart           advertisedAndReceived
admin@pan-mgmt-sts-1.testing>
```


Pour vérifier l'état du BFD depuis CN-MGMT, exécutez les commandes suivantes

- `afficher le résumé bfd du routage avancé`



- afficher les détails du bfd de routage avancé

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd details

BFD Session ID: 114
    Version:          1
    Interface:        ethernet1/3
    Protocol:         BGP
    Local IP Address:           192.168.100.104
    Neighbor IP Address:        192.168.100.109

    BFD profile:                default

    State (local/remote):             up / up
    Up Time:          0d 0h 8m 46s 650ms
    Discriminator (local/remote):  0xb150bb9e / 0x4a1dc50a
    Mode:             Active
    Demand Mode:      Disabled
    Poll Bit:         Disabled
    Multihop:         Disabled
    Multihop TTL:     255
    Local Diag Code:                  0 (No Diagnostic)
    Last Received Remote Diag Code:   0 (No Diagnostic)

    Transmit Hold Time:               0ms
    Desired Min Tx Interval:          1000ms
    Required Min Rx Interval:         1000ms
    Received Min Rx Interval:         1000ms
    Negotiated Transmit Interval:     1000ms
    Detect Multiplier:                3
    Received Multiplier:              3
    Detect time (exceeded):           3000ms (1)
    Tx Control Packets (last):        649 (861ms ago)
    Rx Control Packets (last):        604 (669ms ago)
    Agent DP:         Slot 9 - DP 0
    Errors:           0

    Last Recieved Packet:
        Version:          1
        My Discriminator:           0x4a1dc50a
        Your Discriminator:         0xb150bb9e
        Diag Code:        0 (No Diagnostic)
        Length:           24
        Demand bit:       0         Poll bit:         0
        Final bit:        0         Multipoint:       0
        Control Plane Independent:      0
        Authentication Present:         0
        Desired Min Tx Interval:        1000ms
        Required Min Rx Interval:       1000ms
        Detect Multiplier:              3
        Required Min Echo Rx Interval: 50ms
```


HSF CN-Series : Cas pratiques

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Voici les cas d'utilisation pour le HSF CN-Series :

- Test de trafic 5G
  - Sécurité 5G avec visibilité N3+N4 et politique de corrélation
  - Protection entrante/sortante avec identification des applications et inspection des menaces
- Mettre à l'échelle les pare-feu en fonction de métriques personnalisées prises en charge
- Scénario de test : gestion des pannes CN-MGMT
- Scénario de test : gestion des pannes CN-NGFW
- Scénario de test : gestion des pannes CN-DB

Test de trafic 5G

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

La sécurisation de la périphérie réseau implique d'équilibrer l'inspection et le contrôle du trafic (exigences de sécurité) avec une bande passante élevée, une faible latence et un accès en temps réel (expérience utilisateur). Ces problèmes sont exponentiellement plus difficiles si le trafic est traité par de nombreux pare-feu, si les applications sont hébergées sur des sites périphériques ou si la périphérie réseau est un point d'agrégation pour les données IoT. De plus, la séparation de l'utilisateur et du plan de contrôle dans les réseaux 5G complexifie l'application de la politique de sécurité au niveau de l'abonné ou du périphérique et manque de visibilité contextuelle pour les menaces. Les pare-feu placés avec les interfaces N3 et N4 fournissent les points suivants :

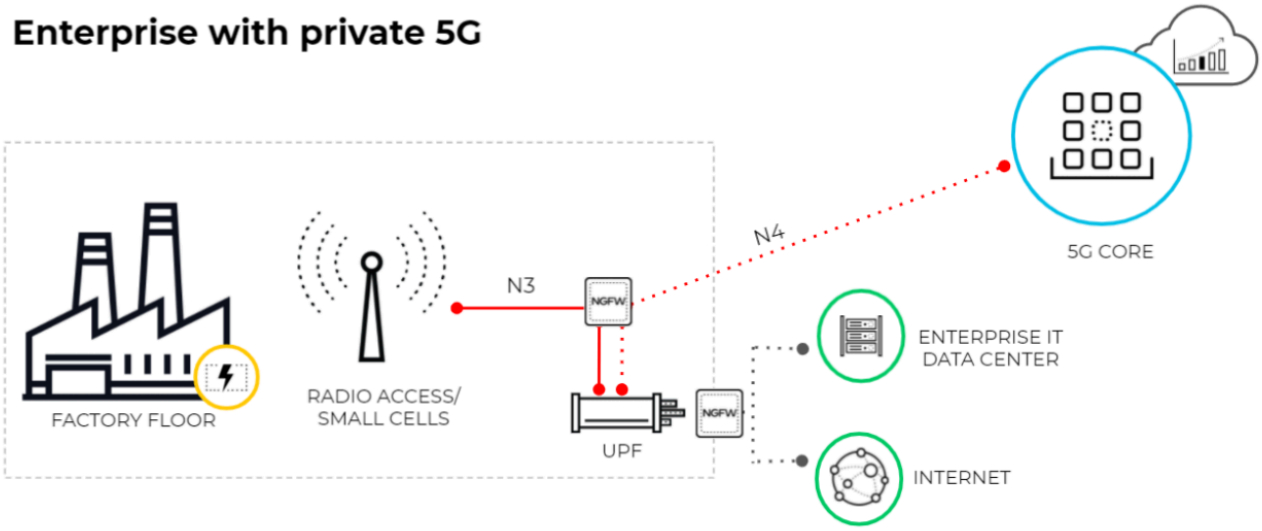
- Visibilité du niveau de signalisation entre les périphériques connectés
- Inspection d'état de PFCP et de GTP-U
- Corrélation de l'ID d'abonné/l'ID d'équipement/l'ID de tranche avec les vulnérabilités de trafic GTP-U

Voici les cas d'utilisation du trafic 5G pour le HSF CN-Series :

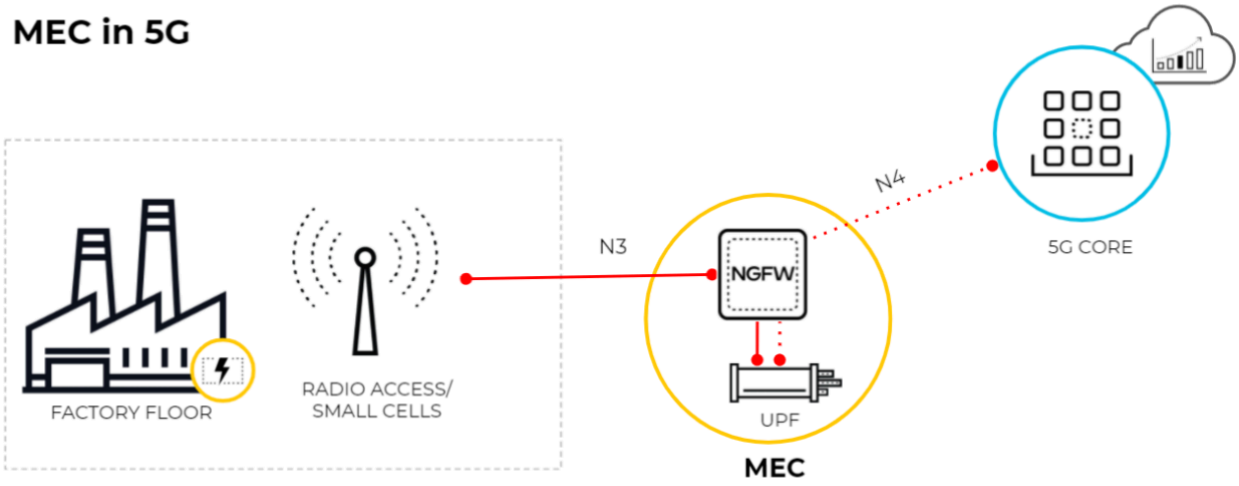
- Sécurité 5G avec visibilité N3+N4 et politique de corrélation

- Protection entrante/sortante avec identification des applications et inspection des menaces

Le diagramme suivant illustre une entreprise qui utilise un réseau 5G privé. Les fonctions de base de la 5G reposent sur le cloud ou sur le site central du fournisseur de services. La connexion entre l'accès 5G et l'UPF utilise l'interface N3. Les tunnels GTP-U acheminent le trafic du plan utilisateur sur l'interface N3. La connexion entre l'UPF et la fonction de gestion de session (SMF) utilise l'interface N4. Le protocole PFCP échange des règles de transfert de paquets à l'aide d'échanges UDP sur l'interface N4.



Ce diagramme illustre le MEC dans un réseau 5G où la fonction de plan utilisateur (UPF) se situe à la périphérie ou à l'emplacement MEC, les fonctions de base de la 5G reposant sur le cloud ou sur le site central du fournisseur de services. La connexion entre l'accès 5G et l'UPF utilise l'interface N3 et les tunnels GTP-U acheminent le trafic du plan utilisateur sur l'interface N3. La connexion entre l'UPF et le SMF utilise l'interface N4 et le protocole PFCP échange des règles de transfert de paquets à l'aide d'UDP sur l'interface N4.



Sécurité 5G avec visibilité N3+N4 et politique de corrélation

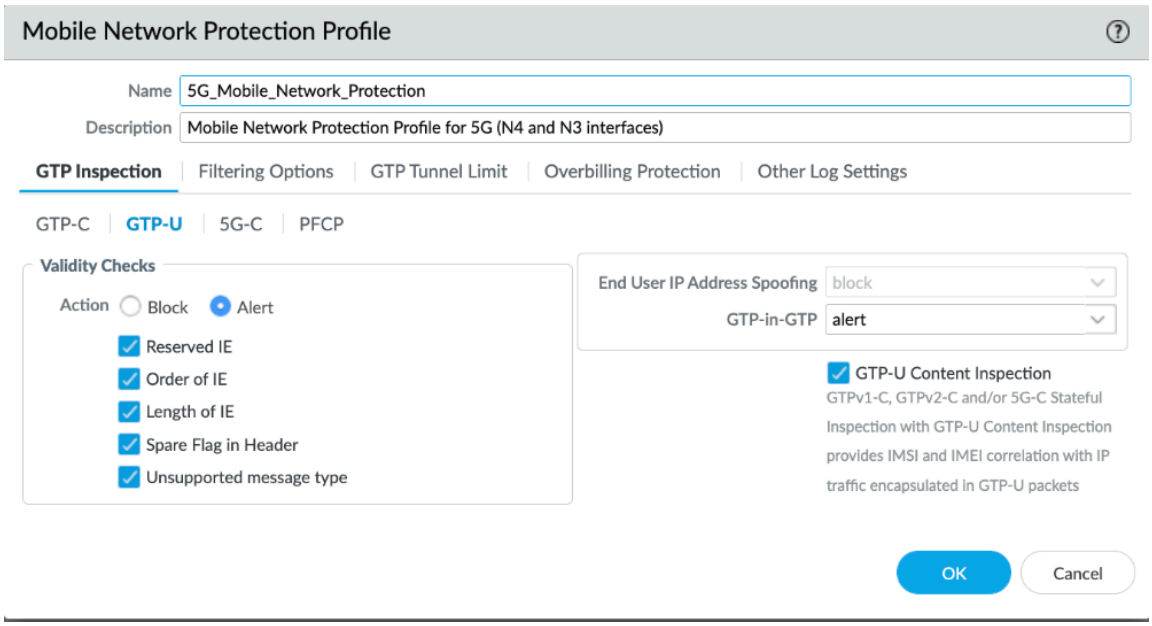
Ce scénario de test évalue la capacité du cluster CNF à inspecter et sécuriser le trafic des interfaces N3+N4.

STEP 1 | Comme première étape vers l'inspection et la sécurisation du trafic des interfaces N3+N4, vous devez activer la sécurité GTP.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)** et sélectionnez **GTP-U Security (Sécurité GTP-U)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** la modification.
5. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Device (Réamorcer l'appareil)**.

STEP 2 | Créez un profil de protection de réseau mobile et activez l’inspection GTP-U.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Mobile Network Protection (Protection de réseau mobile)**.
2. **Add (Ajoutez)** un profil et saisissez un **Name (Nom)**, tel que **`5G_Mobile_Network_Protection`**.
3. Dans l’onglet **PFCP**, activez **Stateful Inspection (Inspection d’état)**.



STEP 3 | Sélectionnez les vérifications d’état que vous souhaitez que le pare-feu effectue sur le trafic PFCP et l’action que vous souhaitez que le pare-feu entreprenne si une vérification d’état échoue.

1. Déterminez les vérifications d’état que vous souhaitez utiliser.
   - **Check Association Messages (Vérifier les messages d'association)** : vérifie les messages d'association PFCP qui sont en panne ou qui ont été rejetés.
   - **Check Session Messages (Vérifier les messages de session)** : vérifie les messages de session PFCP qui sont en panne ou qui ont été rejetés ; vérifie que tous les messages de session PFCP

correspondent à une association PFCP existante ; alerte ou abandonne les messages de session PFCP qui arrivent avant que l'association PFCP soit configurée.

- **Check Sequence Number (Vérifier le numéro de séquence)** : confirme que le numéro de séquence dans la réponse PFCP correspond au numéro de séquence dans le message de demande PFCP précédent.

2. Sélectionnez l'action que vous souhaitez que le pare-feu entreprenne si une vérification d'état échoue.
   - **allow (autoriser)** : autorisez le trafic et ne générez pas d'entrée de journal dans le journal GTP.
   - **block (bloquer)** : bloquez le trafic et générez une entrée de journal à haute gravité dans le journal GTP.
   - **alert (alerter)** : (par défaut) autorisez le trafic et générez une entrée de journal à haute gravité dans le journal GTP.

STEP 4 | (Facultatif) Configurez la journalisation à des fins d'inspection PFCP.

1. Sélectionnez le moment lors duquel vous souhaitez que le pare-feu génère une entrée de journal.
   - **Journaliser au début de l'association PFCP**
   - **Journaliser en fin d'association PFCP**
   - **Journaliser au début de la session PFCP**
   - **Journaliser en fin de session PFCP**

STEP 5 | Activez les autres paramètres des journaux pour les messages PFCP et GTP-U.

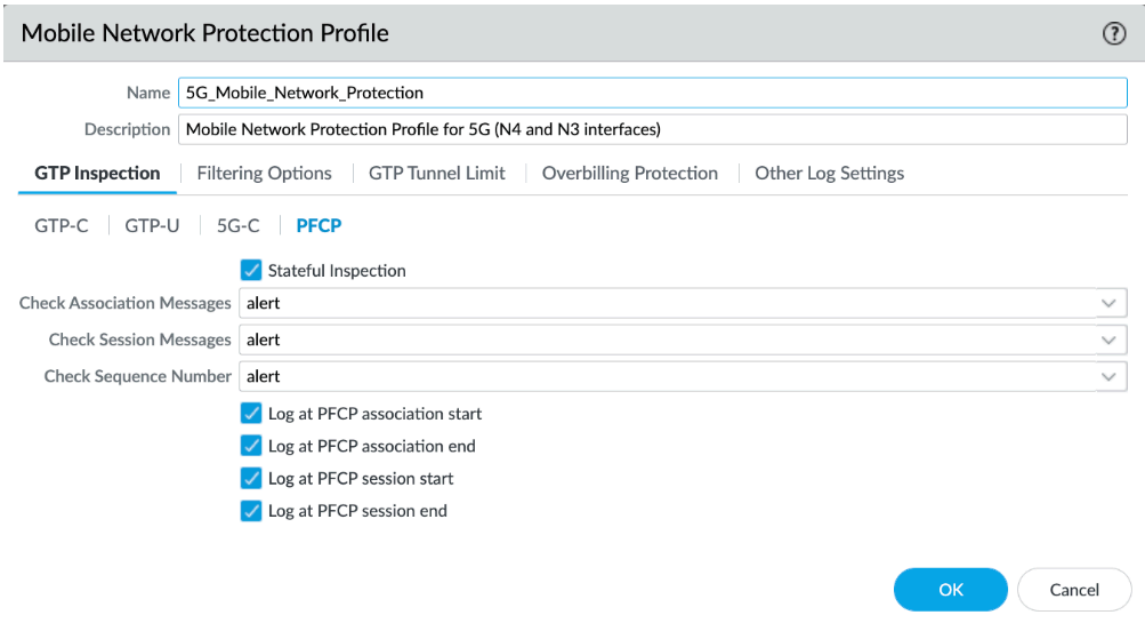
1. Dans l'onglet **Other Log Settings (Autres paramètres des journaux)**, sélectionnez le type de **PFCP Allowed Messages (Messages autorisés PFCP)** que vous souhaitez inclure dans les journaux.

   Activez ces options à des fins de dépannage uniquement.

   - **Session Establishment (Établissement de session)** : ces messages PFCP configurent la session, y compris l'établissement du tunnel GTP-U.
   - **Session Modification (Modification de session)** : ces messages PFCP sont envoyés si l'ID de session ou l'ID PDR change (par exemple, suite au passage d'un réseau 4G à un réseau 5G. Il

comprend des messages tels que la demande de modification de session PFCP et la réponse de modification de session PFCP.

- **Session Deletion (Suppression de session)** : ces messages PFCP mettent fin à la session PFCP, y compris la libération des ressources associées.



STEP 6 | Créez deux politiques de sécurité avec la source et la destination comme interfaces N3 et N4, l'application comme GTP-U et PFCP respectivement.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** une règle de politique de sécurité par **Name (Nom)**.
2. Sélectionnez l'onglet **Source** et **Add (Ajoutez)** une **Source Zone (Zone source)** ou sélectionnez **Any (Indifférent)**.
3. Pour **Source Address (Adresse source)**, **Add (Ajoutez)** les objets d'adresse pour les terminaux d'élément 5G sur l'interface N3.
4. Pour **Destination**, **Add (Ajoutez)** les objets d'adresse **Destination Address (Adresse de destination)** pour les terminaux d'élément 5G sur l'interface N3.
5. **Add (Ajoutez)** les **Applications** à autoriser, telles que le plan utilisateur, à savoir **GTP-U** et **PFCP**.
6. Dans l'onglet **Actions**, sélectionnez l'**Action**, telle que **Allow (Autoriser)**.
7. Sélectionnez le profil **Mobile Network Protection (Protection de réseau mobile)** que vous avez créé.
8. Sélectionnez les autres profils que vous souhaitez appliquer, tels que **Vulnerability Protection (Protection contre les vulnérabilités)**.
9. Sélectionnez les paramètres des journaux, tels que **Log at Session Start (Journaliser au début de la session)** et **Log at Session End (Journaliser en fin de session)**.
10. Cliquez sur **OK**.
11. De même, créez une autre politique de sécurité pour l'interface N4.

STEP 7 | (Facultatif) Créez une autre règle de politique de sécurité basée sur l'ID d'équipement/l'ID d'abonné/l'ID de tranche réseau, en fonction de la protection en saisissant les informations EDL dans la source.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** une règle de politique de sécurité par **Name (Nom)**, p. ex. Sécurité de l'ID d'équipement.
2. Sélectionnez l'onglet **Source** et **Add (Ajoutez)** une **Source Zone (Zone source)** ou sélectionnez **Any (Indifférent)**.
3. **Add (Ajoutez)** un ou plusieurs ID **Source Equipment (Équipement source)** dans l'un des formats suivants :
   - Identifiant d'équipement permanent (PEI) 5G, y compris IMEI
   - IMEI (15 ou 16 chiffres)
   - Préfixe IMEI de huit chiffres pour le Code d'attribution de type (TAC)
   - EDL qui spécifie les IMEI
4. (Facultatif) Vous pouvez ajouter des noms **Source Subscriber (Abonné source)** et **Network Slice (Tranche réseau)** à cette règle de politique de sécurité pour rendre la règle plus restrictive.
5. Spécifiez **Destination Zone (Zone de destination)**, **Destination Address (Adresse de destination)** et **Destination Device (Périphérique de destination)** sur **Any (Indifférent)**.
6. **Add (Ajoutez)** les **Applications** à autoriser, p. ex. **ssh**, **ssl**, **radmin** et **telnet**.
7. Dans l'onglet **Actions**, sélectionnez l'**Action**, telle que **Allow (Autoriser)**.
8. Sélectionnez les profils que vous souhaitez appliquer, tels que **Antivirus**, **Vulnerability Protection (Protection contre les vulnérabilités)**et **Anti-Spyware (Antispyware)**.
9. Sélectionnez les paramètres des journaux, tels que **Log at Session Start (Journaliser au début de la session)** et **Log at Session End (Journaliser en fin de session)**.
10. Cliquez sur **OK**.

    Résultat du test attendu :
    - Vérifiez les journaux GTP-U dans la section de surveillance.
    - Vérifiez la section des détails du journal, pour bénéficier d'une visibilité sur les informations relatives à l'abonné, l'équipement et à la tranche réseau.
    - Observez que le nombre de correspondances avec la règle augmente.

Protection entrante/sortante avec identification des applications et inspection des menaces

Ce scénario de test évalue la capacité du cluster CNF à inspecter et à sécuriser le trafic entrant et sortant sur l'interface N6.

L'interface N6 achemine le trafic en texte clair via TCP/UDP vers Internet. Désormais, avec le pare-feu VM-Series déployé sur l'interface N6, vous pouvez bénéficier d'une visibilité complète sur l'utilisation des applications. Le pare-feu peut implémenter la sécurité avec un abonnement CDSS tels que TP, filtrage avancé des URL, Wildfire, sécurité DNS sur le trafic autorisé.

Les étapes suivantes décrivent comment exécuter ce scénario de test. Pour plus de détails sur l'exécution des étapes individuelles, reportez-vous à la section Sécurité 5G avec visibilité N3+N4 et politique de corrélation.

STEP 1 | Créez une politique de sécurité pour l'interface N6 avec les zones et l'interface appropriées.

STEP 2 | Utilisez les profils de sécurité par défaut ou créez une catégorie personnalisée pour le filtrage des URL, Wildfire, la protection contre les vulnérabilités, etc.

STEP 3 | (Facultatif) Créez un profil personnalisé pour l'URL autorisée dans la catégorie URL.

STEP 4 | (Facultatif) Créez plusieurs politiques de sécurité correspondant à différents critères. Lors de la création de la politique de sécurité, sélectionnez les profils créés à l'étape 3.

STEP 5 | Envoyez le trafic.

STEP 6 | Envoyez le trafic malveillant dans les directions entrantes/sortantes et vérifiez si le trafic est bloqué.

Résultat attendu :

- Le nombre de correspondances de la politique augmente.
- Vérifiez les journaux appropriés pour le filtrage des URL, le trafic et les journaux de menaces.

Mettre à l'échelle les pare-feu en fonction de métriques personnalisées prises en charge

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Ce test permet de valider la capacité du cluster HSF CN-Series à procéder à une mise à l'échelle automatique, en fonction de la cible de valeur métrique personnalisée spécifiée dans la mise à l'échelle automatique.

STEP 1 | Activez la mise à l'échelle automatique pendant que vous créez le cluster HSF CN-Series pour la mise à l'échelle automatique en fonction de la valeur cible de métrique personnalisée spécifiée dans la mise à l'échelle automatique. Pour plus d'informations, consultez Déployer le cluster HSF

STEP 2 | Saisissez l'espace de noms CloudWatch pour transmettre des métriques à AWS CloudWatch.

STEP 3 | Saisissez la région du cluster EKS.

STEP 4 | Saisissez l'intervalle Push.

STEP 5 | Sélectionnez la métrique de mise à l'échelle automatique. Dans cet exemple, vous pouvez décider de sélectionner PansessionActive.

STEP 6 | Spécifiez le seuil de mise à l'échelle (augmentation) et le seuil de mise à l'échelle (diminution). Par exemple, si vous avez 2 pods NGFW en cours d'exécution et que le nombre total de sessions sur le pare-feu est actuellement de 1 000, la métrique de surveillance cloud affiche alors 500 (par pod NGFW).

STEP 7 | Vous pouvez définir le seuil de mise à l'échelle (diminution) à 250, et la mise à l'échelle automatique doit développer 2 pods NGFW supplémentaire.

STEP 8 | Utilisez la commande show session info sur le pod MGMT pour générer les informations de session.

STEP 9 | Vous pouvez spécifier les pods NGFW maximum et minimum pouvant procéder à une mise à l'échelle automatique.

Résultat attendu : le pod NGFW doit être mis à l'échelle automatiquement en fonction de la valeur de seuil de mise à l'échelle automatique (diminution).

Scénario de test : gestion des pannes CN-MGMT

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Ce test évalue la gestion des pannes CN-NGMT.

Le nombre minimal souhaité de pods CN-MGMT pour un déploiement HSF CN-Series est de deux afin d'assurer la gestion des pannes. Après le déploiement, le pod CN-MGMT qui devient actif devient le leader, tandis que le deuxième pod CN-MGMT devient le suiveur. Les deux pods CN-MGMT ont la même configuration. À un moment quelconque, un pod CN-MGMT se trouve à l'état READY (PRÊT). Les pods CN-DB, CN-GW et CN-NGFW se connectent au pod CN-MGMT à l'état READY (PRÊT) par le biais de liaisons d'interconnexion du trafic (TI).

Les deux pods CN-MGMT ne sont pas en mode HA active/passive ou HA active/active. Les deux pods ont la même configuration, et sont configurés à l'aide de Panorama.

La panne du CN-MGMT se produit en raison de l'une des conditions suivantes.

- La vérification de l'activité échoue
  - Si `slotd` est en panne
  - Si `ipsec` ou `strongswan` est en panne
- Le pod CN-MGMT plante et redémarre

STEP 1 | Depuis la CLI Panorama, saisissez `show clusters name <cluster-name>` pour afficher les pods CN-MGMT leader et suiveur.

La sortie suivante montre que le pod **`pan-mgmt-sts-1`** est actif.

```
Cluster: cluster-001 Creation time: 2022/11/30 03:23:50 CN-MGMT pods: 88C00D31E1FC86B
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196 (active,
 pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------- 5
 pan-db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW
 11.0.1-c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-
ngfw-dep-668965d598-s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW
 11.0.1-c183.dev_e_rel 9 pan-ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-
db-dep-6774cd774d-gjpkr CN-DB 11.0.1-c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-
c183.dev_e_rel
```


STEP 2 | Affichez l'appartenance au cluster pour le pod **pan-mgmt-sts-1**et l'état des pods CN-DB, CN-GW et CN-NGFW à partir de la CLI du contrôleur Kubernetes.

1. Saisissez `kubectl get pods -n kube-system` pour afficher l'état de tous les pods.

   Sortie :

   Le **pan-mgmt-sts-1** est actif. Tous les pods CN-DB, CN-GW et CN-NGFW sont connectés à **pan-mgmt-sts-1**.

   ```
   NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 69m
    pan-db-dep-6774cd774d-k49cm 1/1 Running 0 69m pan-gw-dep-d849c7df8-4sk54 1/1
    Running 0 69m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 69m pan-mgmt-sts-0
    0/1 Running 0 83m pan-mgmt-sts-1 1/1 Running 0 83m pan-ngfw-dep-668965d598-
   pmmjd 1/1 Running 0 69m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 69m pan-
   ngfw-dep-668965d598-s2zcc 1/1 Running 0 69m pan-ngfw-dep-668965d598-vf9l4 1/1
    Running 0 69m
   ```

2. Vérifiez l'appartenance au cluster à partir de **pan-mgmt-sts-1**.

   Accédez au pod **pan-mgmt-sts-1**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   Vérifiez si tous les pods CN-DB, CN-GW et CN-NGFW sont connectés au pod CN-MGMT leader à l'aide de la commande suivante.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Sortie :

   ```
   MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
    ================================================================================ 1 CN-GW
    192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 :: UP UP NA 2 CN-GW 192.168.23.100
    192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP
    UP 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9
    CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
   ```

3. Vérifiez l'appartenance au cluster à partir de **pan-mgmt-sts-0**.

   Accédez au pod **pan-mgmt-sts-0**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
   ```

   ```
   su - admin
   ```

   Vérifiez si des pods CN-DB, CN-GW et CN-NGFW sont connectés au pod CN-MGMT suiveur à l'aide de la commande suivante.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Sortie :

   ```
   No members info present
   ```


STEP 3 | Testez la gestion des pannes du pod CN-MGMT.

1. Depuis la CLI du contrôleur Kubernetes, saisissez la commande suivante pour supprimer le pod **pan-mgmt-sts-1** leader.

```
kubectl -n kube-system delete pod pan-mgmt-sts-1
```

2. Depuis la CLI Panorama, saisissez `show clusters name <cluster-name>` pour afficher les nouveaux pods CN-MGMT leader et suiveur.

   La sortie suivante montre que le pod **pan-mgmt-sts-0** est désormais actif.

```
Cluster: cluster-001 Creation time: 2022/11/30 03:23:50 CN-MGMT pods: 88C00D31E1FC86B
 (active, pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196
 (pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------ 5 pan-
db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW 11.0.1-
c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-ngfw-dep-668965d598-
s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW 11.0.1-c183.dev_e_rel 9 pan-
ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-db-dep-6774cd774d-gjpkr CN-DB 11.0.1-
c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-c183.dev_e_rel
```

STEP 4 | Affichez l'appartenance au cluster pour le pod **pan-mgmt-sts-0**et l'état des pods CN-DB, CN-GW et CN-NGFW à partir de la CLI du contrôleur Kubernetes.

1. Saisissez `kubectl get pods -n kube-system` pour afficher l'état de tous les pods.

   Sortie :

   Le **pan-mgmt-sts-0** est actif. Tous les pods CN-DB, CN-GW et CN-NGFW sont connectés à **pan-mgmt-sts-1**.

```
NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 76m
 pan-db-dep-6774cd774d-k49cm 1/1 Running 0 76m pan-gw-dep-d849c7df8-4sk54 1/1
 Running 0 76m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 76m pan-mgmt-sts-0
 1/1 Running 0 90m pan-mgmt-sts-1 0/1 Running 0 90m pan-ngfw-dep-668965d598-
pmmjd 1/1 Running 0 76m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 76m pan-
ngfw-dep-668965d598-s2zcc 1/1 Running 0 76m pan-ngfw-dep-668965d598-vf9l4 1/1
 Running 0 76m
```

2. Vérifiez l'appartenance au cluster à partir de **pan-mgmt-sts-0**.

   Accédez au pod **pan-mgmt-sts-0**.

```
kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
```

```
su - admin
```

   Vérifiez si tous les pods CN-DB, CN-GW et CN-NGFW sont connectés au pod CN-MGMT leader à l'aide de la commande suivante.

```
show cluster-membership show-slot-info slot all
```

   Sortie :

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 :: UP UP NA 2 CN-GW 192.168.23.100
 192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP
 UP 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9
 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```


3. Vérifiez l’appartenance au cluster à partir de **pan-mgmt-sts-1**.

   Accédez au pod **pan-mgmt-sts-1**.

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   Vérifiez si des pods CN-DB, CN-GW et CN-NGFW sont connectés au pod CN-MGMT suiveur à l’aide de la commande suivante.

   ```
   show cluster-membership show-slot-info slot all
   ```

   Sortie :

   ```
   No members info present
   ```

Résultat de test : lorsque le pod `pan-mgmt-sts-1` leader échoue, le pod suiveur `pan-mgmt-sts-0` devient le nouveau leader. Ce mécanisme de gestion des pannes CN-MGMT veille à ce que le flux de trafic soit ininterrompu. Aucune répercussion sur les sessions existantes ou nouvelles.

Scénario de test : gestion des pannes CN-NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Ce test évalue la gestion des pannes CN-NGFW.

Une panne CN-NGFW peut se produire dans les circonstances suivantes.

- Problèmes relatifs aux nœuds
- Le pod CN-NGFW plante et redémarre
- Le nœud et le pod CN-NGFW sont fonctionnels, mais **pan_task** plante
- CN-NGFW est retiré de l’appartenance au cluster lorsque :
  - La surveillance IPSec sur l’interface Eth0 échoue
  - La liaison d’interconnexion du cluster (CI) est interrompue
  - La liaison d’interconnexion du trafic (TI) est interrompue

Dans ce scénario, la session SSH entre le client et le serveur est installée sur CN-NGFW 1. Si le pod CN-NGFW 1 est en panne, la session SSH doit être maintenue active par basculement vers un autre CN-NGFW.

STEP 1 | Depuis la CLI Panorama, saisissez `show clusters name <cluster-name>` pour afficher les pods CN-NGFW, CN-DB et CN-GW connectés au pod CN-MGMT.

```
Cluster: cluster-002 Creation time: 2022/11/22 04:56:46 CN-MGMT pods: 87F87FE94CBBB03
 (active, pan-mgmt-sts-0.cluster-002, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------ 1
 pan-gw-dep-5cd5c87d76-przjx CN-GW 11.0.1-c156.dev_e_rel 6 pan-db-dep-d6fb496b-jf2ms CN-DB
 11.0.1-c156.dev_e_rel 5 pan-ngfw-dep-5cd8f55848-dbhwh CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-
ngfw-dep-5cd8f55848-slk5l CN-NGFW 11.0.1-c156.dev_e_rel 7 pan-db-dep-d6fb496b-hfmlp CN-DB
 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-5cd8f55848-pq6ks CN-NGFW 11.0.1-c156.dev_e_rel 2 pan-
gw-dep-5cd5c87d76-4kbfk CN-GW 11.0.1-c156.dev_e_rel 11 pan-ngfw-dep-5cd8f55848-rsbqn CN-NGFW
 11.0.1-c156.dev_e_rel
```

STEP 2 | Consultez les détails de l'appartenance au cluster du pod CN-MGMT `an-mgmt-sts-0` à l'aide de la commande `show cluster-membership show-slot-info slot all`.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 11 CN-NGFW 192.168.23.87 192.168.24.93 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 7 CN-DB 192.168.23.102 :: UP UP NA 6
 CN-DB 192.168.23.104 :: UP UP NA 5 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

Toutes les interfaces du sous-réseau ethernetx/3 doivent être dans la même zone. De même, toutes les interfaces du sous-réseau ethernetx/4 doivent se trouver dans la même zone.

STEP 3 | Utilisez `show session all filter application ssh` pour afficher toutes les sessions SSH.

Pour chaque session, il existe deux flux pour les directions client à serveur et serveur à client.

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 1342177294 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 1342177294 Session 1342177294 c2s flow: source: 192.168.200.100 [untrust_ei1]
 dst: 192.168.250.100 proto: 6 sport: 48702 dport: 22 state: Type ACTIF : FLOW utilisateur
 src : inconnu utilisateur dst : inconnu flux s2c : source : 192.168.250.100 [trust_ei2] dst:
 192.168.200.100 proto: 6 sport: 22 dport: 48702 state: Type ACTIF : FLOW src user: unknown
 dst user: unknown Slot : 11 DP : 0 index(local): : 14 start time : Mon Nov 21 21:30:02 2022
 timeout : 3600 sec time to live : 3542 sec total byte count(c2s) : 3887 total byte count(s2c) :
 4501 layer7 packet count(c2s) : 23 layer7 packet count(s2c) : 20 vsys : vsys1 application :
 ssh rule : allow_inside-to-outside service timeout override(index) : False session to be
 logged at end : Vrai session dans session ager : True session updated by HA peer : False
 layer7 processing : completed URL filtering enabled : True URL category : any session via syn-
cookies : Fausse session terminée sur l'hôte : La fausse session traverse le tunnel : False
 session terminate tunnel : False captive portal session : False ingress interface : ethernet1/3
 egress interface : ethernet1/4 session QoS rule : N/A (class 4) tracker stage l7proc : ctd
 decoder done end-reason : unknown
```

Le propriétaire de la session est l'emplacement 11.

Vous pouvez afficher les détails du flux de cluster filtré à l'aide de l'exemple de commande suivant.

```
show cluster-flow all filter source-port 22
```

Sortie :

```
--------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 --------------------------------------------------------------------------------
 536870940 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
 --------------------------------------------------------------------------------
```



```
 Slot 6
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------------
 671088668 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
```

```
show cluster-flow all filter destination-port 22
```

Sortie :

```
-------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------------
 536870939 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
 ------------------------------------------------------------------------------------
 Slot 6
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------------
 671088667 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
```

STEP 4 | Supprimez le pod sur l'emplacement 11 à l'aide de la commande `kubectl -n kube-system delete pod pan-ngfw-dep-5cd8f55848-rsbqn`.

Sortie :

```
pod "pan-ngfw-dep-5cd8f55848-rsbqn" deleted
```

La session appartenant au pod CN-NGFW dans l'emplacement 11 est maintenant marquée comme orpheline.

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s6dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id
 536870939 Flow 536870939 start time : Mon Nov 21 21:30:02 2022 timeout : 3600 sec
 source : 192.168.200.100 sport : 48702 dest : 192.168.250.100 dport : 22 proto :
 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 28 cid : 0 gft : 0 gft' : 1
 predict : 0 orphan : 1 flag_inager : 0 ager_thread : 3 flags : 0 flow-data : type:
 l7 app-id: 25 startlog: 1 endlog: 1 denied: 0 admin@pan-mgmt-sts-1.cluster-001>
 set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-
mgmt-sts-1.cluster-001> show cluster-flow id 671088667 Flow 671088667 start time :
 Mon Nov 21 21:30:02 2022 timeout : 3600 sec source : 192.168.200.100 sport : 48702
 dest : 192.168.250.100 dport : 22 proto : 6 zone : 1 type : FLOW state : ACTIVE
 ipver : 4 fidx : 28 cid : 0 gft : 1 gft' : 0 predict : 0 orphan : 1 flag_inager :
 0 ager_thread : 4 flags : 0 flow-data : type: l7 app-id: 25 startlog: 1 endlog: 1
 denied: 0
```

STEP 5 | Accédez à la session SSH à l'aide de la commande `show session all filter application ssh`.

Le pare-feu bascule vers un pod CN-NGFW disponible pour gérer le flux orphelin. Le propriétaire de la nouvelle session est l'emplacement 7.

```
------------------------------------------------------------------------------- ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 805306374 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 805306374 Session 805306374 c2s flow: source: 192.168.200.100 [untrust_ei1]
 dst: 192.168.250.100 proto: 6 sport: 48702 dport: 22 state: Type ACTIF : FLOW utilisateur
 src : inconnu utilisateur dst : inconnu flux s2c : source : 192.168.250.100 [trust_ei2] dst:
 192.168.200.100 proto: 6 sport: 22 dport: 48702 state: Type ACTIF : FLOW src user: unknown
```



```
 dst user: unknown Slot : 7 DP : 0 index(local): : 6 start time : Mon Nov 21 21:43:27 2022
 timeout : 3600 sec time to live : 3581 sec total byte count(c2s) : 1350 total byte count(s2c) :
 1506 layer7 packet count(c2s) : 17 layer7 packet count(s2c) : 11 vsys : vsys1 application :
 ssh rule : Promoted-session service timeout override(index) : False session to be logged
 at end : Vrai session dans session ager : True session updated by HA peer : False layer7
 processing : completed URL filtering enabled : True URL category : any session via syn-
cookies : Fausse session terminée sur l'hôte : La fausse session traverse le tunnel : False
 session terminate tunnel : False captive portal session : False ingress interface : ethernet1/3
 egress interface : ethernet1/4 session QoS rule : N/A (class 4) tracker stage l7proc : fastpath
 state none end-reason : unknown
```

Aucune modification dans le flux du cluster.

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s5dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id
 536870939 Flow 536870939 start time : Mon Nov 21 21:30:02 2022 timeout : 3600 sec
 source : 192.168.200.100 sport : 48702 dest : 192.168.250.100 dport : 22 proto :
 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 12 cid : 7 gft : 0 gft' : 1
 predict : 0 orphan : 0 flag_inager : 0 ager_thread : 3 flags : 0 flow-data : type:
 l7 app-id: 25 startlog: 1 endlog: 1 denied: 0 admin@pan-mgmt-sts-1.cluster-001>
 set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-
mgmt-sts-1.cluster-001> show session id 805306374 Session 805306374 Bad Key: c2s:
 'c2s' Bad Key: s2c: 's2c' index(local): : 6 admin@pan-mgmt-sts-1.cluster-001> show
 cluster-flow id 671088667 Flow 671088667 start time : Mon Nov 21 21:30:02 2022
 timeout : 3600 sec source : 192.168.200.100 sport : 48702 dest : 192.168.250.100
 dport : 22 proto : 6 zone : 1 type : FLOW state : ACTIVE ipver : 4 fidx : 12 cid :
 7 gft : 1 gft' : 0 predict : 0 orphan : 0 flag_inager : 0 ager_thread : 4 flags : 0
 flow-data : type: l7 app-id: 25 startlog: 1 endlog: 1 denied: 0
```

Résultats :

Aucune répercussion sur les sessions existantes ou nouvelles. Appartenance au cluster mise à jour sur Panorama.

Scénario de test : gestion des pannes CN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement du pare-feu HSF série CN	• CN-Series 11.0.x or above Container Images • Panorama exécutant PAN-OS 11.0.x ou une version supérieure

Ce test évalue la gestion des pannes CN-DB. Le nombre préféré de pods CN-DB pour un déploiement HSF CN-Series est de deux. Les deux pods CN-DB ont la même configuration.

Lorsque le pod CN-DB 1 est en panne pour une période prolongée, le pod CN-DB 2 s’occupe des sessions existantes et configure de nouvelles sessions. Lorsque le pod CN-DB 1 est à nouveau opérationnel, il vérifie la synchronisation des sessions, la recherche et l’arrêt des sessions existantes, ainsi que la configuration de nouvelles sessions.

STEP 1 | Consultez les détails de l’appartenance au cluster du pod CN-MGMT à l’aide de la commande `show cluster-membership show-slot-info slot all`.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ==========================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6
 CN-DB 192.168.23.104 :: UP UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```


STEP 2 | Supprimez le pod CN-DB dans l'emplacement 6.

1. Générez le nom du pod CN-DB sur l'emplacement 6 à l'aide de la commande `show clusters name cluster-001` depuis la CLI Panorama.

```
Cluster: cluster-001 Creation time: 2022/11/22 05:11:09 CN-MGMT pods: 8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------- 5 pan-
db-dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-
c156.dev_e_rel 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-
srmdt CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-
ngfw-dep-56cdfdd656-bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-
c156.dev_e_rel 6 pan-db-dep-7b6f6c5458-4tvpq CN-DB 11.0.1-c156.dev_e_rel
```

2. Depuis la CLI du contrôleur, saisissez la commande `kubectl delete pod pan-db-dep-7b6f6c5458-4tvpq -n kube-system` pour supprimer le pod CN-DB dans l'emplacement 6.

   Le pod CN-DB de l'emplacement 6 est désormais supprimé.

```
admin@pan-mgmt-sts-1.cluster-001> show cluster-membership show-slot-info slot
 all MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 7 CN-NGFW 192.168.23.103
 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82
 192.168.24.81 UP UP UP
```

3. Vérifiez le flux de trafic du cluster à l'aide de la commande `show cluster-flow all`.

```
Slot 5 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156]
 536870958 ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954
 ACTIVE FLOW 192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE
 FLOW 192.168.100.100[3784]/17 192.168.100.6[49153] 536870952 ACTIVE
 FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 536870951 ACTIVE FLOW
 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960 OPENING FLOW
 fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:2[0] 536870957 ACTIVE FLOW
 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW 192.168.250.100[22]/6
 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
 192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
 ------------------------------------------------------------------------------ Slot
 6 ------------------------------------------------------------------------------ No
 Active Flows
```

   L'emplacement 6 avec le pod CN-DB se trouve désormais à l'état PREPARE (PRÉPARATION) et la liaison CI est inactive.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-GW
 192.168.23.100 192.168.24.80 UP IMPACTED UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP IMPACTED UP 2
 CN-GW 192.168.23.101 192.168.24.100 UP IMPACTED UP 5 CN-DB 192.168.23.102 :: UP IMPACTED NA 6 CN-DB
 192.168.23.104 :: PREPARE DOWN NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP IMPACTED UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP IMPACTED UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP IMPACTED UP
```

STEP 3 | Saisissez `show cluster-membership show-slot-info slot all` jusqu'à ce que le pod CN-DB redevienne actif.

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP
 UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-
DB 192.168.23.104 :: PROBE UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```


STEP 4 | Vérifiez à nouveau le flux de trafic du cluster à l'aide de la commande `show cluster-flow all`.

```
-------------------------------------------------------------------------------- Slot 5
 -------------------------------------------------------------------------------- Id State Type
Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 536870958
ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954 ACTIVE FLOW
192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE FLOW 192.168.100.100[3784]/17
192.168.100.6[49153] 536870952 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784]
536870951 ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960
OPENING FLOW fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 536870957
ACTIVE FLOW 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW
192.168.250.100[22]/6 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
-------------------------------------------------------------------------------- Slot 6
 -------------------------------------------------------------------------------- Id State Type
Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
671088642 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 671088641 ACTIVE FLOW
192.168.200.100[48706]/6 192.168.250.100[22] 671088643 ACTIVE FLOW 192.168.100.6[49153]/17
192.168.100.100[3784] 671088645 ACTIVE FLOW 192.168.100.100[3784]/17 192.168.100.6[49153]
671088644 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 671088646
ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 671088647 ACTIVE FLOW
fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 671088648 ACTIVE FLOW
192.168.101.101[3784]/17 192.168.101.6[49155] 671088649 ACTIVE FLOW 192.168.250.100[22]/6
192.168.200.100[48706] 671088650 ACTIVE FLOW 192.168.100.6[49154]/17 192.168.100.101[3784]
671088651 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
```

- `show cluster-flow all filter count yes`

```
-------------------------------------------------------------------------------- Slot 5
 -------------------------------------------------------------------------------- Number of
 sessions that match filter: 11
 -------------------------------------------------------------------------------- Slot 6
 -------------------------------------------------------------------------------- Number of
 sessions that match filter: 11
```

- `show cluster-membership show-slot-info slot all`

```
MP leader status: Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 :: UP UP NA 6 CN-DB 192.168.23.104 :: UP UP
 NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-
NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

- Depuis la CLI Panorama

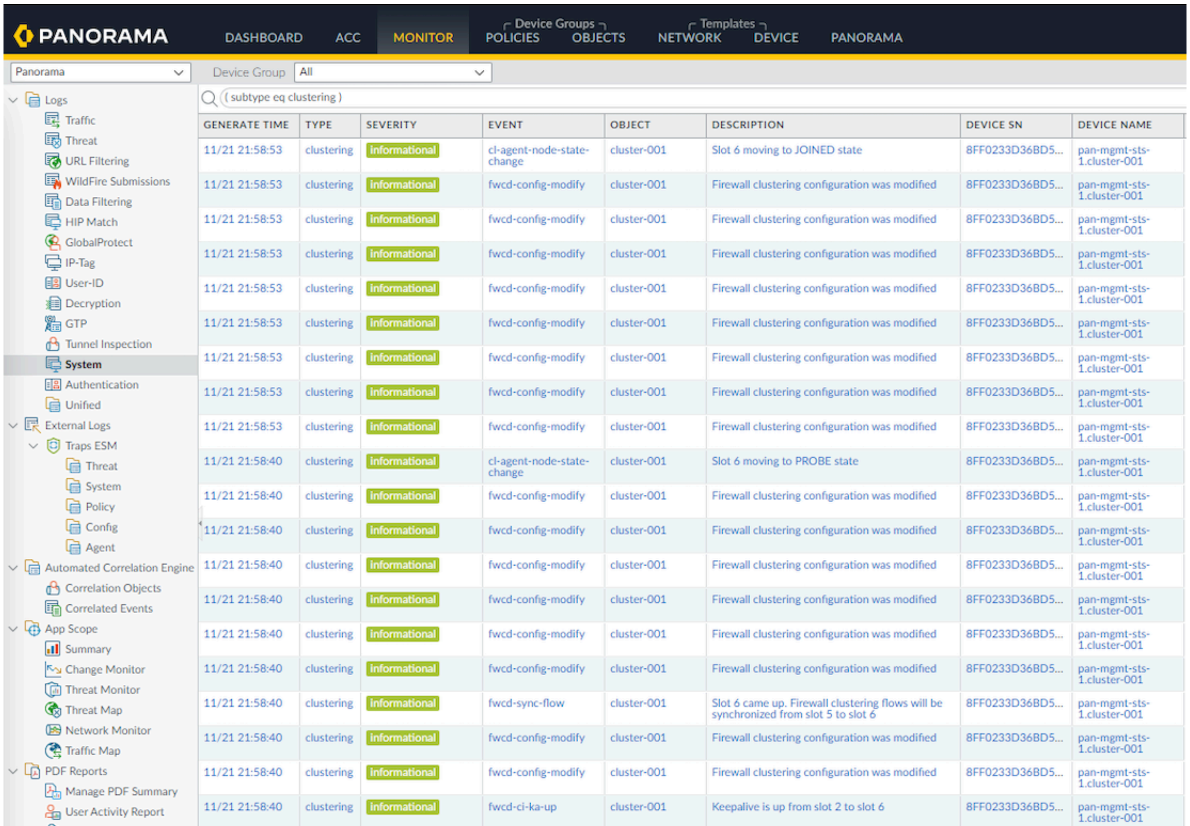
```
show clusters name cluster-001
```

```
Cluster: cluster-001 Creation time: 2022/11/22 05:11:09 CN-MGMT pods: 8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 -------------------------------------------------------------------------------- 5 pan-db-
dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-c156.dev_e_rel
 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-srmdt CN-NGFW 11.0.1-
c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-56cdfdd656-
```



```
bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-c156.dev_e_rel 6 pan-db-dep-7b6f6c5458-r449b CN-DB 11.0.1-c156.dev_e_rel
```

Vous pouvez consulter les changements CN-DB dans l’interface Web Panorama sous **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)**.



Résultats :

Aucune répercussion sur les sessions existantes ou nouvelles. Appartenance au cluster mise à jour sur Panorama.

Fonctionnalités non prises en charge par le pare-feu CN-Series

Les fonctionnalités suivantes prises en charge sur PAN-OS ne sont pas disponibles pour la série CN, sauf indication contraire ci-dessous :

Fonctionnalité	DaemonSet	Service K8s	Mode CNF	Mode HSF
Authentification	Non	Non	Non	Non
Journaux vers Cortex Data Lake	Non	Non	Non	Non
Enterprise DLP	Non	Non	Non	Non
Interfaces non-vWire	Non	Non	**Oui**	**Oui**
IoT Security	Non	Non	Non	Non
IPv6	**Oui**	Non	**Oui**	Non
NAT	Non	Non	**Oui**	Non
Transfert basé sur une politique	Non	Non	**Oui**	Non
QoS	Non	Non	Non	Non
SD-WAN	Non	Non	Non	Non
User-id	Non	Non	Non	Non
WildFire Inline ML	Non	Non	Non	Non
SaaS Inline	Non	Non	Non	Non
IPSec	Non	Non	Non	Non
Inspection du contenu du tunnel	Non	Non	Non	Non