paloalto TECHDOCS

Dépannage CN-Series

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

Dépannage CN-Series

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

Table 1: Définitions des termes :

Terme	Définitions
MP	CN-MGMT
DP	CN-NGFW

Connectez-vous à MP ou DP

Exécutez la commande suivante pour connaître le nom de votre pod MP ou DP :

kubectl get pods -n=<namespace>

Exécutez la commande suivante pour vous connecter aux pods MP ou DP :

Kubectl -n kube-system exec -it <mp-pod-name> -- su admin

Kubectl -n kube-system exec -it <mp/dp-pod-name> -- bash

Les pods ne parviennent pas à extraire l'image avec une erreur

x509 : certificat signé par une autorité inconnue (principalement observé avec les clusters k8 natifs/ onprem)

Sur tous les nœuds de travail, mettez à jour **/etc/docker/daemon.json** avec le référentiel d'images que vous extrayez. Créez un fichier daemon.json s'il n'existe pas

```
root@ctnr-debug-worker-2:~# cat /etc/docker/daemon.json { "insecure-
registries" : ["docker-panos-ctnr.af.paloaltonetworks.local",
 "panos-cntr-engtools.af.paloaltonetworks.local",
 "docker-public.af.paloaltonetworks.local", "panos-cntr-
engtools-releng.af.paloaltonetworks.local", "docker-qa-
pavm.af.paloaltonetworks.local"] } root@ctnr-debug-worker-2:~#
```

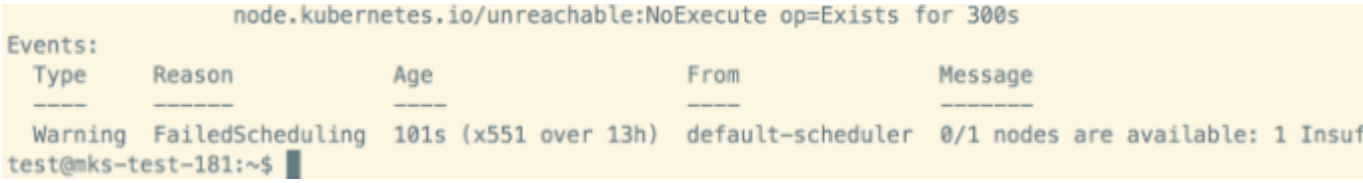
Redémarrage de Docker avec la commande "**systemctl restart docker.service**".

MP reste en attente

Vérifiez les éléments suivants :

1. Les ressources requises (nœud/mémoire/cpu) sont disponibles pour MP. Nous pouvons nous en assurer en vérifiant la sortie de la commande pour

   kubectl -n kube-system describe <mp-pod-name>



2. Un volume persistant (PV) est un élément de stockage dans le cluster qui a été provisionné par l'administrateur du serveur/stockage/cluster ou provisionné dynamiquement à l'aide de classes de stockage. Il s'agit d'une ressource du cluster, au même titre qu'un nœud. Une demande de volume persistant (PVC) est une requête de stockage formulée par un utilisateur qui peut être obtenue à partir de PV.

   Les PVC sont liés au PV (`kubectl -n kube-system get pvc`). Si ce n'est pas le cas, supprimez les anciennes PVC en exécutant la commande suivante :

   ```
   "kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts-<whatever>"
   ```

3. Vérifiez si les répertoires requis (pan-local1, pan-local2, pan-local3, pan-local4, pan-local5, pan-local6 sous /mnt) sont créés sur au moins deux nœuds de travail pour les configurations sur site.

   Les `pan-local1, pan-local2, pan-local3, pan-local4, pan-local5, pan-local6` sous `/mnt` ne sont pas requis pour le provisionnement dynamique de volumes. Le pilote EBS CSI manquant sur AWS EKS est l'une des raisons pour lesquelles le MP reste en attente. Vous devez vous assurer que le pilote EBS CSI est activé dans le cluster, vérifier le rôle et identifier le fournisseur du cluster. Pour plus d'informations, consultez Gestion du pilote Amazon EBS CSI en tant que module complémentaire Amazon EKS.

4. Si le message d'erreur « `pan-mgmt-sts-0` » : le pod comprend des demandes de volume persistant immédiates non liées » s'affiche, exécutez « **kubectl get pvcs -o wide** » et « **kubectl get pv -o wide** ». Les PVC qui n'ont pas réussi à se lier devraient s'afficher.

   La solution serait de supprimer les anciennes PVC à l'aide de la commande **kubectl -n kube-system delete pvc/<pvc-name>** ou de les nettoyer. Supprimez l'ensemble des PVC et des PV. Déployez de nouveaux PV et déployez les MP.

5. Si le message d'erreur**« k8 décrit le pod <mp-pod>»** s'affiche ci-dessous, vérifiez que les PV ont été créés. Sinon, déployez pan-cn-pv-local.yaml (avec les noms de nœuds où les répertoires sont configurés)

   Plug-in de filtre **« VolumeBinding »** pour le pod **« pan-mgmt-sts-0 »** : le pod comprend des demandes de volume persistant illimitées

   Avertissement Échec de la Planification <unknown> planificateur par défaut exécutant le plug-in de filtre **« VolumeBinding »** pour le pod**« pan-mgmt-sts-0 »** : le pod présente des demandes de volume persistant illimitées

6. ```
   lnehru@lnehru-parts-vm:~/cnv1/Kubernetes/pan-cn-k8s-daemonset/eks$
    k8l pan-mgmt-sts-0
   ```

   ```
   12-22-2021 11:34:36.961697 PST INFO : Conteneur de gestion
    commençant à s'exécuter sous la version PanOS 10.1.3-c47
   ```

   12-22-2021 11:34:41.335521 PST ERREUR : Failed to start pansw: 2

   Le problème pourrait être que **« pan-cn-mgmt-configmap.yaml »** ne présente pas de valeurs obligatoires.


   ```

# MP continue de planter

Connectez-vous à la racine MP et accédez à **/var/cores** pour voir le processus à l'origine du plantage.

# Les journaux K8 MP affichent l'erreur suivante

**La demande d'enregistrement du périphérique a échoué : Échec d'envoi de requête au serveur CSP**

Vérifiez les éléments suivants :

1. « Pan-cn-mgmt-secret.yaml » doit comprendre des valeurs correctes pour les deux champs ci-dessous CN-SERIES-AUTO-REGISTRATION-PIN-ID : « <PIN Id> »

   CN-SERIES-AUTO-REGISTRATION-PIN-VALUE : « <PIN-Value> »
2. Si les valeurs ci-dessus sont correctes, assurez-vous que le PinID et la valeur n'ont pas expiré depuis CSP

# Échec de connexion de MP à Panorama ou échec CommitAll MP

1. Vérifiez que MP peut atteindre/ping l'IP de Panorama. Pour les clouds publics, assurez-vous que les politiques de sécurité requises sont configurées pour permettre l'accessibilité entre Panorama et les clusters K8

   Connectez-vous à mp :

   - 1. Kubectl -n kube-system exec -it <mp-pod-name> -- su admin
     2. « Afficher l'état du panorama » pour obtenir l'adresse IP du panorama
     3. hôte ping <panorama-ip>
     4. Si le ping fonctionne, poursuivez les vérifications ci-dessous
2. Vérifiez que la clé « bootstrap-auth-key » fournie dans mgmt-secret.yaml est présente sur Panorama et n’a pas expiré.
   1. Pour vérifier bootstrap-auth-key, connectez-vous à Panorama et exécutez la commande « request bootstrap vm-auth-key show » # Cela devrait être valide (non expiré)
   2. Si elle n'est pas disponible, générez-la à l'aide de « request bootstrap vm-auth-key generate lifetime 8760 » et mettez-la à jour dans le pan-mgmt-secret.yaml. Annulez le déploiement de tous les yamls, effacez le PV, les PVC et redéployez.
3. Vérifiez que le DG, le TS et le groupe de collecteurs (CG) configurés dans mgmt-configmap.yaml ne sont pas mal orthographiés, et configurés+validés sur Panorama
4. Vérifiez que pan-mgmt-configmap et les yamls secrets sont déployés avant mgmt.yam. Vérifiez que pan-mgmt-configmap et les yamls secrets sont déployés avant mgmt.yaml.
5. Vérifiez si l’opération CommitAll (Valider tout) de Panorama sur MP a réussi à l’aide des commandes « afficher tous les travaux » et « afficher les ID des travaux <id>» pour consulter les échecs et corriger les configurations sur Panorama, puis procédez à nouveau à l’opération Valider tout/forcer.
6. La configuration Panorama est poussée sur MP « show config push-shared-policy
7. Recherchez « configd.log » sur Panorama à partir de la racine en entrant la commande « tac-login response » et recherchez avec le numéro de série MP. Il doit y avoir une raison pour laquelle la connexion échoue.

   **vi /var/log/pan/configd.log**

   **Exemple** :

   ```
   15/03/2021 14:19:49.213 -0700 Erreur :
    pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4085) :
    bootstrap : pile de modèles cnv2-template-stack
    introuvable, série=8CABD801686AD2021-04-15
    14:19:49.213 -0700 démarrage : candidat cfg ch Erreur :
    pan_cfg_bootstrap_vm_auth_key_verify(pan_cfg_bootstrap_mgr.c:3822) :
    Échec de la recherche vm_auth_key 923688689426978, vm_auth _key
    invalide
   ```

Impossible de lancer « Valider tout » sur MP

Vérifiez sur Panorama si les tâches CommitAll (Valider tout) sont bloquées ou en état ACT.

Cela peut se produire en cas de problèmes de connectivité réseau entre MP et Panorama.

Dans Lab, le problème peut être résolu en mettant MP/le nœud de travail et Panorama dans le même sous-réseau.

Consultez les journaux de Panorama ci-dessous si vous rencontrez ce type de problème.

```
19/01/2023 09:13:51.788 -0800 Erreur :
 device_needs_bkup(pan_bkup_mgr.c:323) : échec de l'extraction
 de /opt/pancfg/mgmt/devices/8B8AE8CB506CF09/running-config.xml
 19/01/2023 09 : 13:51.938 -0800 Groupe de périphériques Push
 Panorama cn-dg-12c13c51-1 pour le périphérique 8B8AE8CB506CF09
 avec les indicateurs de modèle d'inclusion de fusion avec
 candidat-cfg définis.JobId=50860.User=pano rama. Temps de
 sortie de la file d'attente = 19/01/2023 09:13:51. 19/01/2023
 09:13:52.812 -0800 Le fil de liste de préférences a été
 généré pour être envoyé au périphérique 8B8AE8CB506CF09 dans
 le groupe CG 19/01/2023 09:13:52.812 -0800 Le fil de liste
 de préférences a été envoyé au périphérique 8B8AE8CB506CF09
 19/01/2023 09:13:52.813 -0800 JAU2 : Efface toutes les
 adresses sur dev:8B8AE8CB506CF09. 19/01/2023 09:14:35.061 -0800
 Erreur : pan_conn_mgr_callback_expiry_async(cs_conn.c:8781) :
 connmgr : Demande expirée. entrée : 916, msgno=3
 devid=8B8AE8CB506CF09 19/01/2023 09:14:35.061 -0800 Erreur :
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781) :
 connmgr : Demande expirée. entrée : 916, msgno=6
 devid=8B8AE8CB506CF09 19/01/2023 09:14:35.061 -0800 Erreur :
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781) :
 connmgr : Demande expirée. entrée : 916, msgno=4
 devid=8B8AE8CB506CF09 19/01/2023 09:15:05.060 -0800 Erreur :
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781) :
 connmgr : Demande expirée. entrée : 916, msgno=0
 devid=8B8AE8CB506CF09 19/01/2023 09:15:05.060 -0800 Erreur :
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781) : connmgr :
 Demande expirée. entrée : 916, msgno=5 devid=8B8AE8CB506CF09
 19/01/2023 09:15:05.060 -0800 copy-lcs-pref-list : Processeur
 de réponse : la tâche de copie de la préférence lcs a reçu
 la réponse du périphérique 8B8AE8CB506CF09 du cookie 2407. Le
 cookie actuel est 2408. Restant : 1 19/01/2023 09:15:05.060
 -0800 copie-lcs-pref-list : Processeur de réponse : la
 tâche de copie de la préférence lcs a reçu la réponse du
 périphérique 8B8AE8CB506CF09 du cookie 2408. Le cookie actuel
 est 2408. Restant : 1 19/01/2023 09:15:05.060 -0800 Erreur :
 pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761) :
 19/01/2023 09:15:05.060 -0800 copy-lcs-pref-list : Échec de la
 réception de la réponse du périphérique 8B8AE8CB506CF09. Erreur
 - délai d'expiration de l'envoi/réception du message Erreur :
 pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761) :
 copy-lcs-pref-list : échec de la réception de la réponse du
 périphérique 8B8AE8CB506CF09. Erreur - délai d'expiration de
 l'envoi/réception du message 2023-01-19 09:15:08.545 -0800 connmgr :
```



```
 réception de déconnexion cb de ms pour 8B8AE8CB506CF09(1020484)
 2023-01-19 09:15:08.545 -0800 connmgr : entrée de connexion
 supprimée. devid=8B8AE8CB506CF09 sock=4294967295 result=0 2023-01-19
 09:15:08.545 -0800 Mise à jour de la connexion du périphérique de
 gestion [déconnexion][activé :1] pour 8B8AE8CB506CF09 : « serveur :
 le client est le périphérique » 2023-01-19 09:15:08.545 -0800
 Erreur : pan_bkupjobmgr_process_async_result(pan_bkup_mgr.c:208) :
 Échec de la réception de la réponse du périphérique 8B8AE8CB506CF09.
 Erreur - échec de l'envoi du message 19/01/2023 09:15:08.545 -0800
 Erreur : pan_async_lcs_pref_list_result(pan_comp_collector.c:2681) :
 lcs-pref-list : échec de la réception de la réponse du
 périphérique 8B8AE8CB506CF09. Erreur - échec de l'envoi du
 message 19/01/2023 09:15:08.546 -0800 Commentaires Panorama
 HA : 8B8AE8CB506CF09 déconnecté 19/01/2023 09:15:08.547 -0800
 connmgr : entrée de connexion supprimée. devid=8B8AE8CB506CF09
 (1020484) 19/01/2023 09:15:41.212 -0800 Avertissement :
 _register_ext_validation(pan_cfg_mgt_handler.c:4418) :
 reg : le périphérique « 8B8AE8CB506CF09 » n'utilise pas le
 certificat émis. 19/01/2023 09:15:41.213 -0800 Avertissement :
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4737) : SC3 :
 le périphérique « 8B8AE8CB506CF09 » n'est pas compatible
 avec SC3 19/01/2023 09:15:41.213 -0800 Enregistrement SVM.
 Série : 8B8AE8CB506CF09 DG : cn-dg-12c13c51-1 TPL : cn-
tmplt-stk-12c13c51-1 vm-mode : 0 uuid : 4b96eccd-9d66-43b1-
a3f3-2318f3e5b2fd cpuid : K8SM P : A6D64F : 8410079
 617204080582 : svm_id : 2023-01-19 09:15:41.213 -0800 Erreur :
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4020) :
 bootstrap : 8B8AE8CB506CF09 déjà ajouté aux périphériques mgd
```


Les pods DP restent à l’état « En attente » ou « Création de conteneur »

Exécutez les commandes suivantes et vérifiez les erreurs mentionnées dans le résultat de chaque commande et corrigez-les

1. kubectl -n kube-system describe pod/<dp-pod-name>.

   Si le message d'erreur suivant s'affiche dans le cadre de la commande ci-dessus, continuez à rechercher les journaux CNI et à vérifier si CNI utilise multus.

   ```
   MountVolume.Échec de la configuration pour le volume « pan-cni-
   ready » : échec de la vérification du type hostPath : /var/log/pan-
   appinfo/pan-cni-ready n'est pas un répertoire
   ```

2. Journaux systèmes kubectl -n kube <dp-pod-name>
3. Kubectl -n kube-system describe pod <cni-name-on-same-node>
4. Journaux systèmes kubectl -n kube <cni-name-on-same-node>
5. Si kubectl CNI affiche le message suivant, assurez-vous que CNI est exécuté sur chaque nœud. (Sur le cluster GKE, nous devons activer la politique réseau pour exécuter CNi par défaut) :

   ```
   18/08/2022 23:55:07.397661 UTC DÉBOGAGE : Configuration PAN CNI :
    { "name": "pan-cni", "type": "pan-cni", "log_level": "debug",
    "appinfo_dir": "/var/log/pan-appinfo", "mode" : "service",
    "dpservicename": "pan-ngfw-svc", "dpservicenamespace": "kube-
   system", "firewall": [ "pan-fw" ], "interfaces": [ "eth0" ],
    "interfacesip": [ "" ], "interfacesmac": [ "" ], "override_mtu":
    "", "kubernetes": { "kubeconfig": "/etc/cni/net.d/ZZZ-pan-cni-
    kubeconfig", "cni_bin_dir": "/opt/cni/bin", "exclude_namespaces":
    [], "security_namespaces": [ "kube-system" ] }} 18/08/2022
    23:55:07.402812 UTC DÉBOGAGE : CNI fonctionnant en mode FW
    Service. Le contournement du pare-feu peut être activé sur les
    pods d'application 18/08/2022 23:55:07.454392 UTC CRITIQUE :
    Multus détecté en tant que CNI primaire (fichier CONF 00-
   multus.conf) ; en attendant que les CNI non multus deviennent des
    CNI primaires. root@manojmaster:~/pan-cn-k8s-service/native#
   ```

   Si le message d'erreur ci-dessus apparaît, essayez d'annuler le déploiement de Multus et supprimez le fichier 00-multus.conf des nœuds de travail sur lesquels ce CNI et ces DP sont déployés

   ```
   root@manojworker1:/etc/cni/net.d# pwd /etc/cni/net.d
    root@manojworker1:/etc/cni/net.d# rm 00-multus.conf
   ```


MP : Ne pas afficher les détails/l'état de Panorama

```
admin@PA-CTNR> show panorama-status admin@PA-CTNR> [root@PA-CTNR /]#
 cat /opt/pancfg/mgmt/bootstrap/init-cfg.txt.20210527 type=static
 netmask=255.255.255.0 cgname=CG tplname=10_3_252_62-CNv2 ip-
address=10.233.99.17 default-gateway=10.233.99.1 dgname=10_3_252_62-
CNv2 panorama-server=107.21.240.64 hostname=pan-mgmt-sts-0 vm-auth-
key=158251502922307 [root@PA-CTNR /]#
```

1. Il est possible que pan-cn-mgmt-configmap soit déployé après pan-cn-mgmt.yaml
2. Possible échec du déploiement de pan-cn-mgmt-secret (possiblement car bootstrap-auth-key commence par « 0 ») # Supprimez la clé d'authentification de Panorama et recréez-la en vérifiant qu'elle ne commence pas par « 0 »

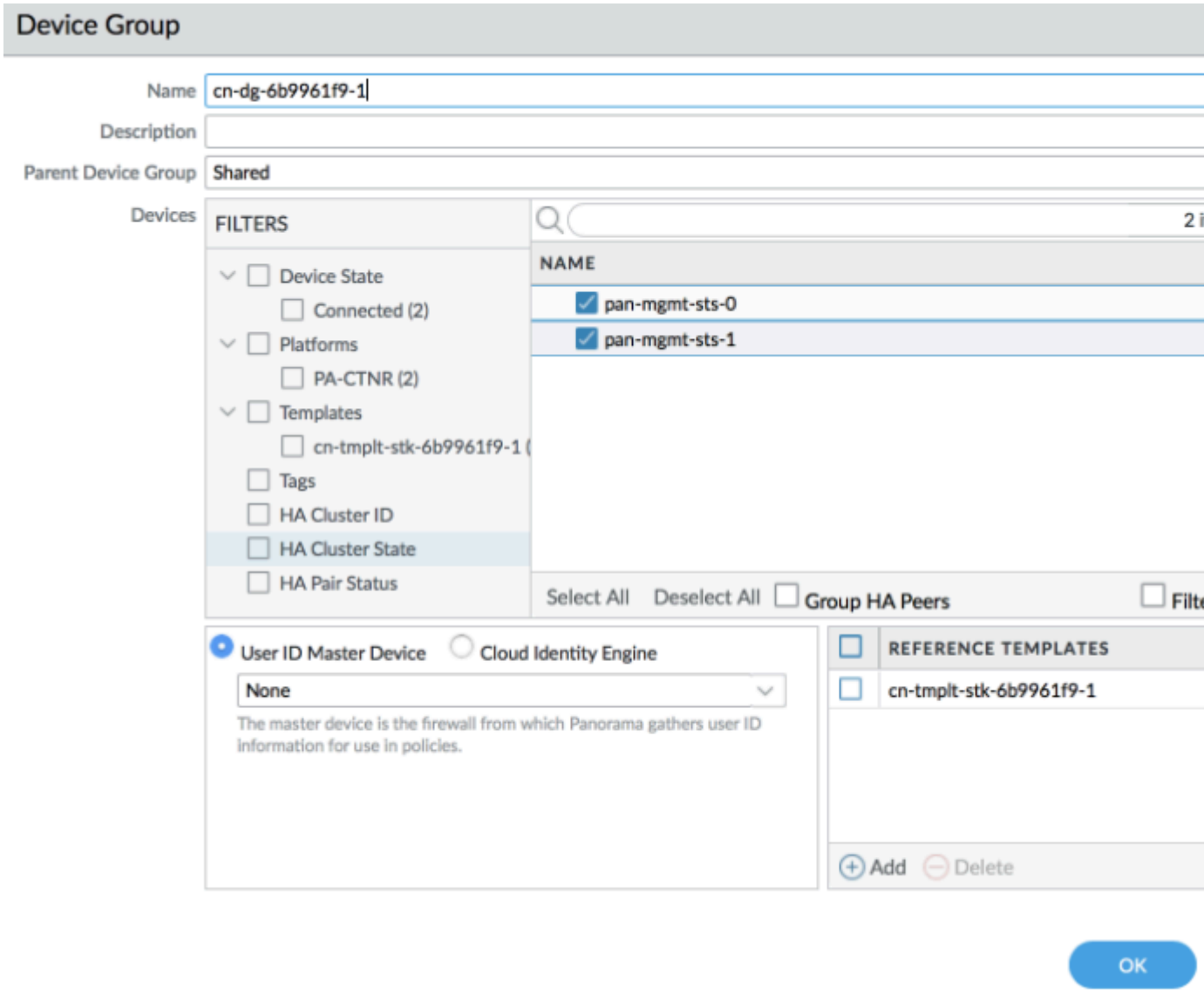
Pour résoudre le problème, annulez le déploiement de MP, supprimez les PVC, les PV, redéployez mp-configmap, suivi de MP.

En cas de déploiement à l'aide du graphique HELM :

Pour résoudre le problème, annulez le déploiement du graphique HELM, supprimez les PVC/PV CN-Series, puis redéployez le HELM.

Panorama n'affiche pas MP en tant qu'appareil géré

1. Assurez-vous que MP et DP sont sur la même version logicielle. « Les journaux K8 sur MP généreraient des journaux d'erreurs s'ils n'étaient pas sur la même version.
2. Si mgmt-slot-crd et mgmt-slot-cr.yaml sont déployés.
3. Si ce DP a établi une connexion IPSec sur l'un des MP (connectez-vous au MP via la racine et vérifiez avec la commande « ipsec status ».
4. Valider tout et Validation automatique devraient passer sur le MP auquel ce DP est connecté. Si ce n'est pas le cas, vérifiez sur MP pourquoi Valider tout ou Validation automatique a échoué et corrigez en conséquence. Reportez-vous à l'étape ci-dessus (échec de la connexion de MP à Panorama ou échec de MP Valider tout) pour résoudre le problème.
5. admin@pan-mgmt-sts-0> debug show internal interface all # devrait afficher la configuration de l'interface, si ce n'est pas le cas, assurez-vous que la pile de modèles est référencée dans le DG. Assurez-vous également que K8S-Network-template dispose de la configuration de l'interface.



6. Si DP possède un mémoire de 4 Go (vérifiez dans ngfw.yaml)
7. Tous les processus Masterd sont en cours d'exécution en exécutant la commande « masterd all status ».
8. « Ps -aef » vérifie le fonctionnement du processus.
9. Vérifiez le résultat de la commande suivante et vérifiez si des échecs d'enregistrement de l'emplacement DP sont observés :

```
 « kubectl get panslotconfigs -n kube-system --insecure-skip-tls-
verify -o yaml »
```


Échec de l'enregistrement de l'emplacement DP

1. Vérifiez que pan-cn-mgmt-slot-cr et crd.yamls sont déployés.
2.
```
[root@rk-cl3-master-1 native-2]# k8sys obtient PanSlotConfig NOM
 AGE pan-mgmt-svc-2-slots 13s pan-mgmt-svc-slots 11d [root@rk-cl3-
master-1 native- 2]#
```
3.
```
[root@rk-cl3-master-1 native-2]# k8sys obtient crd | grep pan NOM
 CRÉÉ SUR panslotconfigs.paloaltonetworks.com 10/11/2022T04:18:13Z
 [root@rk-cl3-master-1 native-2]#
```

```
21/11/2022 20:54:31.783302 UTC INFO : Masterd démarré le
 21/11/2022 20:54:40.050008 UTC INFO : Événement IPSec up-
client avec 169.254.202.2 21/11/2022 20:54:40.121502 UTC INFO :
 Appel du script du registre des emplacements dp 21/11/2022
 20:54:40.323061 UTC AVERTISSEMENT : Readiness: Pas prêt. La
 configuration Panorama n'est pas poussée. pan_task n'est pas
 en cours d'exécution. 21/11/2022 20:54:40.486734 UTC INFO : Le
 démon Strongswan est opérationnel. Essayer d'accéder au plan de
 gestion. 21/11/2022 20:54:41.623966 UTC INFO : Connectivité du
 plan de gestion établie. 21/11/2022 20:54:42.700770 UTC ERREUR :
 Échec de l'enregistrement/du réenregistrement : UTILISATEUR
 21/11/2022 20:54:42.818729 UTC AVERTISSEMENT : le registre
 des emplacements dp a échoué. Réessayer plusieurs fois le
 21/11/2022 20:54:44.265372 UTC ERREUR : Échec de l'enregistrement/
du réenregistrement : UTILISATEUR 21/11/2022 20:54:45.759982
 UTC ERREUR : Échec de l'enregistrement/du réenregistrement :
 UTILISATEUR 21-11-2022 20:54:47.256744 UTC ERREUR : Échec de
 l'enregistrement/du réenregistrement : UTILISATEUR 21/11/2022
 20:54:48.768491 UTC ERREUR : Échec de l'enregistrement/du
 réenregistrement : UTILISATEUR 21/11/2022 20:54:50.272969
 UTC ERREUR : Échec de l'enregistrement/du réenregistrement :
 UTILISATEUR 21/11/2022 20:54:51.390138 UTC CRITIQUE : Échec de
 l'enregistrement au MP. Arrêter DP
```


Les pods MP/DP/CNI ne sont pas affichés lors de l'exécution de la commande « k8 get pods -n kube-system »

1. Vérifiez s'il est possible que le « compte de service » ne soit pas créé car « sa.yaml » n'est pas déployé.
2. Vérifiez si le service mp est en cours d'exécution à l'aide de la commande « k8 -n kube-system get svc »
3. Vérifiez que mp stateful set est en cours d'exécution à l'aide des commandes « k8 -n kube-system get sts » et « k8n -n describe sts/pan-mgmt-sts » # cela s'imprimerait en cas de problème avec pvc/pv

Le trafic des pods d'applications sécurisés n'est pas envoyé via DP/Pare-feu

1. Vérifiez si tous les nœuds de travail exécutent la version minimale 5.4 du noyau (en utilisant la commande « kubectl get nodes -owide)

```
test@mks-test-181:~$ k8getnodes
NAME                          STATUS   ROLES    AGE   VERSION              INTERNAL-IP   EXTERNAL-IP    OS-IMAGE         KERNEL-VERSION
ip-12-12-12-23.ec2.internal   Ready    <none>   14h   v1.19.6-eks-49a6c0   12.12.12.23   3.239.70.160   Amazon Linux 2   5.4.95-42.163.amzn2.x86_64
test@mks-test-181:~$
```

2. (uniquement pour CNv2) Vérifiez si l'interface « vxlan » est créée sur le pod d'application sécurisé et si un itinéraire par défaut est créé par le biais de cette interface vxlan

```
root@vn-cl1-master1:~# k8getpods
NAME                                READY   STATUS    RESTARTS   AGE     IP               NODE             NOMINATED NODE   READ
lighttpd-dep-68bb6f4fbb-wwx24       1/1     Running   0          3d20h   10.233.124.128   vn-cl1-worker3   <none>           <non
wrk2-55f6f4ff85-bwrb2               1/1     Running   0          3d20h   10.233.87.141    vn-cl1-worker2   <none>           <non
root@vn-cl1-master1:~# k8 exec -it lighttpd-dep-68bb6f4fbb-wwx24 -- bash
root@lighttpd-dep-68bb6f4fbb-wwx24:/# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
4: eth0@if150: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT group default qlen 1000
    link/ether 5e:c5:45:a0:b6:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
5: vxlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/ether 5e:c5:45:a0:b6:07 brd ff:ff:ff:ff:ff:ff
root@lighttpd-dep-68bb6f4fbb-wwx24:/#
```

```
root@lighttpd-dep-68bb6f4fbb-wwx24:/# ip r
default via 169.254.1.1 dev vxlan0
10.233.20.139 dev eth0  scope link
169.254.1.1 dev vxlan0  scope link
root@lighttpd-dep-68bb6f4fbb-wwx24:/#
```

3. Vérifiez si les DP sont en cours d'exécution et sont connectés au MP en utilisant IPSec. Si les DP sont actifs/en cours d'exécution, mais que IPSec est terminé

4. Vérifiez si la mise sous licence DP a échoué après 4 heures d'affichage DP en raison de l'absence de code d'authentification ou d'un cluster non connecté au panorama - plug-in k8

```
test2@mks-test-181:~$ k8l pan-ngfw-dep-694797597c-dcxkv
03-30-2021 16:58:19.997929 UTC INFO: DP container starting running PanOS version 10.1.0-c209.dev_s_rel
03-30-2021 16:58:20.048545 UTC INFO: Starting DP in k8s-service mode.
RTNETLINK answers: Network is unreachable
RTNETLINK answers: File exists
03-30-2021 16:58:20.645946 UTC INFO: CPU pinning is not enabled for the pan_tasks
03-30-2021 16:58:21.187358 UTC DEBUG: Using network namespace nspan-fw.
03-30-2021 16:58:21.729211 UTC DEBUG: IPsec nat port range is not specified in configmap, defaulting to port 4500.
2021-03-30 16:58:25.131 +0000 Changing python default from NONE to /etc/masterd.d/runtime/default.py
03-30-2021 16:58:25.606757 UTC INFO: Masterd Started
03-30-2021 16:58:26.646909 UTC INFO: Strongswan daemon is up. Trying to reach Management Plane..
03-30-2021 16:58:34.629870 UTC WARNING: Readiness: Not Ready. Panorama config is not pushed. pan_task is not running.
03-30-2021 17:01:33.060768 UTC INFO: IPSec up-client event with 169.254.202.2
03-30-2021 17:01:33.118831 UTC INFO: Calling dp slot register script
03-30-2021 17:01:33.624694 UTC INFO: Successfully registered with MP (slot s6). Triggering sysd daemon connect...
03-30-2021 17:01:33.902867 UTC INFO: sysd daemon connect event done
03-30-2021 17:01:34.339245 UTC INFO: Management Plane connectivity established.
03-30-2021 17:01:36.201567 UTC INFO: DP Container bringing up rest of the services.
03-30-2021 10:01:54.575489 PST WARNING: Readiness: Not Ready. Panorama config is not pushed. pan_task is running.
03-30-2021 10:02:36.993758 PST INFO: Port configuration received.
03-30-2021 10:02:38.113636 PST INFO: Phase2 commit succeeded with port config.
03-30-2021 10:02:38.572140 PST WARNING: Readiness: Ready now. Panorama config is pushed. pan_task is running.
03-30-2021 14:01:48.157911 PST CRITICAL: Failed to obtain license in predefined time.
03-30-2021 14:01:48.205252 PST CRITICAL: The system is toggling loopback state due to license fail.
test2@mks-test-181:~$
```

5. Vérifiez si le code d'authentification sur le plug-in kubernets dans Panorama n'a pas expiré

   admin@Panorama> requête de plug-ins kubernetes get-license-tokens

   Abonnements de sécurité : Wildfire, prévention des menaces, DNS, filtrage d'URL

   Type de code d'authentification : Crédits SW-NGFW

   Code d'authentification : D2962989

   Expiré : non

   Date d'expiration : 31 décembre 2022

   vCPU émis : 50

   vCPU utilisé : 0

   Date d'émission : 31 décembre 2022

   admin@Panorama-49.88>

6. Vérifiez si « ngfw-svc.yaml » est déployé avant CNI.yaml et si NGFW svc possède ClusterIP et est en cours d’exécution.

before pan-cn-mgmt-slot-cr.yaml:

```
kubectl apply -f plugin-serviceaccount.yaml
kubectl apply -f pan-cni-serviceaccount.yaml
kubectl apply -f pan-mgmt-serviceaccount.yaml
kubectl apply -f pan-cni-configmap.yaml
kubectl apply -f pan-cn-ngfw-svc.yaml
kubectl apply -f pan-cni.yaml
kubectl apply -f pan-cn-mgmt-secret.yaml
kubectl apply -f pan-cn-mgmt-configmap.yaml
kubectl apply -f pan-cn-mgmt-slot-crd.yaml
kubectl apply -f pan-cn-mgmt-slot-cr.yaml
kubectl apply -f pan-cn-mgmt.yaml
kubectl apply -f pan-cn-ngfw-configmap.yaml
kubectl apply -f pan-cn-ngfw.yaml
```

7. Vérifiez les journaux CNI en vous connectant au nœud sous /var/log/pan/pan-cni.log ([ec2-user@ip-12-12-12-184 ~]$ vi /var/log/pan-appinfo/pan -cni.log)
8. Le pod d'application doit être créé après l'exécution de CNI et ngfw svc - le redémarrage du pod peut aider
9. Le pod d'application doit être créé après l'exécution de CNI et ngfw svc - le redémarrage du pod peut aider
10. Vérifiez que la configuration de l'interface est poussée vers DP à l'aide de la commande « debug show internal interface all » sur le pod MP
11. « show rule-hit-count vsys vsys-name vsys1 rule-base security rules all » pour voir quelle règle de sécurité est touchée et modifier la politique de sécurité en conséquence.

Comment vérifier quel pod DP traite le trafic

1. kubectl -n kube-system get pods -l app=pan-ngfw -o wide
2. kubectl -n kube-system describe pod <dp-pod-name> | grep "Container ID"
3. Sur Panorama, accédez à « Surveiller les journaux », ajoutez la colonne « ID de conteneur » et vous verrez apparaître l’ID de conteneur ci-dessus

Journalisation : Panorama n'affiche pas les journaux de trafic/des menaces

Voici les étapes de dépannage :

1. Vérifiez si les journaux sont générés sur le MP à l'aide de la commande « show log traffic/threat direction equal backward ». Si les journaux ne sont pas visibles sur MP, vérifiez si le même MP traite le trafic en utilisant « afficher tout la session », tout en envoyant un ping continu depuis le pod sécurisé
2. Assurez-vous que DP dispose d'une licence à l'aide des commandes :
    1. Sur MP « request plugins vm_series list-dp-pods »
    2. Les journaux K8 sur DP devraient le confirmer.
3. « debug log-receiver statistics » affiche le taux d'entrée des journaux de DP vers MP.
4. Vérifiez que le trafic respecte la politique attendue configurée avec le transfert des journaux à l'aide de « afficher toute la session » et « afficher l'identifiant de session <id>»
5. Vérifiez si la configuration est reçue sur MP exécutant les commandes « show config pushed-shared-policy » et « show running security-policy »
6. Assurez-vous que les « collecteurs gérés » sont synchronisés et connectés sur Panorama.
7. « état masterd elasticsearch » sur Panorama # devrait être en cours d'exécution. Si ce n'est pas le cas, exécutez « es_restart.py -e »
8. ```
   [root@cnsmokepanorama ~]# sdb cfg.es.* cfg.es.acache-update:
    cfg.es.enable : 0x0
   ```
9. es_cluster.sh health
10. « debug log-collector log-collection-stats show incoming-logs » sur Panorama
11. **pan_logquery -t traffic -i bwd -n 50**
   ```

Journalisation : Panorama n'affiche pas les journaux lors du filtrage avec le nom de la règle

Un problème peut survenir lorsque Panorama ne charge pas correctement les modèles ES. Essayez de redémarrer ES avec la commande « es_restart.py -t » à partir du mode racine de Panorama. Envoyez un nouveau trafic/de nouveaux journaux et vérifiez que les journaux sont visibles :

```
[root@sjc-bld-smk01-esx12-t4-pano-02 ~]# es_restart.py -t ====== /
opt/pancfg/mgmt/factory/es/templates/urlsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/sctpsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/iptag.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100004.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/sctp.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/extpcap.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/system.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/wfr.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/gtpsum.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100006.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/decryption.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/thsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/globalprotect.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/hipmatch.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/desum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/userid.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100007.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/trace.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/threat.tpl ==== ====== /opt/pancfg/mgmt/
factory/es/templates/auth.tpl ==== ====== /opt/pancfg/mgmt/factory/
es/templates/config.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/panflex0000100003.tpl ==== ====== /opt/pancfg/mgmt/
factory/es/templates/gtp.tpl ==== ====== /opt/pancfg/mgmt/factory/
es/templates/trsum.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/traffic.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/panflex0000100005.tpl ==== [root@sjc-bld-smk01-esx12-t4-
pano-02 ~]#
```


Échec de reconnexion de MP à Panorama

```
pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105): This device or
 log collector or wf appliance (devid 892A1C93EF280D0) is not managed
```

Le message d’erreur ci-dessus signifie que le périphérique est en train de se réenregistrer. Comme il s’est déjà enregistré, il ne passe pas par le workflow d'amorçage où il s’ajoute à la configuration du panorama.

Cela peut se produire dans le scénario suivant : le périphérique s'est déjà enregistré et connecté, mais aucune validation n'a été effectuée sur Panorama pour enregistrer cette configuration. Ensuite, Panorama a été redémarré ou relancé, ce qui a effacé la configuration. À présent; lorsque le périphérique tente de se connecter, Panorama ne le reconnaît pas et la connexion est rompue.

Ci-dessous les journaux de `configd.log` sur Panorama :

```
03/02/2021 11:48:00.436 -0800 Traitement du message lcs-register
 du périphérique « 8B1EB1ADC72B44E » 03/02/2021 11:48:00.436 -0800
 Avertissement : _get_current_cert(sc3_utils.c:84) : nœud sdb « cfg.
 ms.ak » n'existe pas. 03/02/2021 11:48:04.425 -0800 logbuffer :
 aucune connexion active à cms0 03/02/2021 11:48:24.425 -0800
 logbuffer : aucune connexion active à cms0 03/02/2021 11:48:44.425
 -0800 logbuffer : aucune connexion active à cms0 03/02/2021
 11:48:57.751 -0800 Avertissement : sc3_register(sc3_register.c:90) :
 SC3: Désactivé - Ignorer le registre. 03/02/2021 11:48:57.752 -0800
 Avertissement : pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645) :
 SC3 : le dispositif « 892A1C93EF280D0 » n’est pas
 compatible avec SC3 03/02/2021 11:48:57.752 -0800
 enregistrement SVM. Serial:892A1C93EF280D0 DG: TPL :
 vm-mode:0 uuid:481a70f4-1647-426c-954a-a003ec60943f
 cpuid:K8SMP:A6D64F:84100796172040 80581 : svm_id:2021-02-03
 11:48:57.752 -0800 traitement d'un message d'enregistrement
 issu de 892A1C93EF280D0-2021-02-03 11:48:57.752 -0800 Erreur :
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105): Ce
 périphérique ou collecteur de journaux ou appareil wf (devid
 892A1C93EF280D0) n'est pas géré 03/02/202111:49:04.426 -0800
 logbuffer :pas de connexion active à cms0 03/02/2021 11:49:06.015
 -0800 Avertissement : sc3_register(sc3_register.c:90) : SC3:
 Désactivé - Ignorer le registre. 03/02/2021 11:49:06.015 -0800
 Avertissement : pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645) :
 SC3 : le périphérique « 8B1EB1ADC72B44E » n'est pas
 compatible avec SC3 03/02/2021-2021 11:49:06.015 -0800
 enregistrement SVM. Serial:8B1EB1ADC72B44E DG: TPL :
 vm-mode:0 uuid:731de362-59ed-45a0-9fdd-7e642626f187
 cpuid:K8SMP:A6D64F:84100796172040 80581: svm_id:2021-02-03
 11:49:06.015 -0800 traitement d'un message de registre issu
 de 8B1EB1ADC72B44E-2021-02-03 11:49:06.015 -0800 Error :
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105) : This device or
 log collector or wf app
```


MP et DP sont actifs et en cours d'exécution, mais IPsec est terminé entre MP et DP

Vérifiez les journaux kubectl sur MP, voyez si les emplacements sont libérés après 4 heures comme ci-dessous :

```
(pièces) root@test-virtual-machine : ~# journaux k8sys pan-mgmt-
sts-0 09/03/2021 01:07:36.508002 PST INFO : Conteneur de gestion
 fonctionnant sous la version 10.1 de PanOS.0-c182.dev_s_rel
 Démarrage du logiciel PAN : 03-09-2021 01:08:07.460287 PST WARNING:
 Readiness: Pas prêt. slotd pour l'enregistrement du plan de
 données en cours d'exécution. IPSec pour les connexions au plan de
 données n'est pas en cours d'exécution.09/03/2021 01:10:54.558525
 PST INFO : Échec de l'exécution de cmd:dpdk-devbind --status
 [ OK ] 09/03/2021 01:09:43.043467 PST INFO : Masterd démarré le
 09/03/2021 01:10:53.453639 PST AVERTISSEMENT : Readiness: Prêt
 maintenant. slotd pour l'enregistrement du plan de données en
 cours d'exécution. IPSec pour les connexions au plan de données
 en cours d'exécution. 03-09-2021 01:10:54.558525 PST INFO: Le
 démon Strongswan est opérationnel. 03-09-2021 01:10:56.286104 PST
 INFO : La version logicielle correspond, les versions logicielles
 MP et DP sont 10.1.0-c182.dev_s_rel 03-09-2021 01:10:56.346162
 PST INFO : Inscrivez-vous avec l'uid pan-ngfw-ds-4lhhc, sw_ver
 10.1.0-c182.dev_s_rel, emplacement 0, dp_ip 169.254.202.2 09/03/2021
 01:10:56.453298 PST INFO : Emplacement 1 alloué pour l’uid pan-
ngfw-ds-4lhhc 169.254.202.2 03-09-2021 01:10:57.131769 PST INFO :
 La version logicielle correspond, les versions logicielles MP
 et DP sont 10.1.0-c182.dev_s_rel 09/03/2021 01:10:57.198584 PST
 INFO : Inscrivez-vous avec l'uid pan-ngfw-ds-9pj2f, sw_ver 10.1.0-
c182.dev_s_rel, emplacement 0, dp_ip 169.254.202.3 09/03/2021
 01:10:57.288892 PST INFO : Emplacement 2 alloué pour l'uid pan-
ngfw-ds-9pj2f 169.254.202.3 09/03/2021 01:12:02.279032 PST INFO :
 Installation de la licence AutoFocus. 03-09-2021 01:12:02.362417
 PST INFO : Installation de la licence LoggingServices. 03-09-2021
 05:13:01.521227 PST INFO : La version logicielle correspond, les
 versions logicielles MP et DP sont 10.1.0-c182.dev_s_rel 09/03/2021
 05:13:01.597810 PST INFO : Libération de l'emplacement 2, uid pan-
ngfw-ds-9pj2f avec Force 09/03/2021 05:13:01.694588 PST INFO : La
 version logicielle correspond, les versions logicielles MP et DP
 sont 10.1.0-c182.dev_s_rel 09/03/2021 05:13:01.764245 PST INFO :
 Libération de l'emplacement 1, uid pan-ngfw-ds-4lhhc avec Force
 09/03/2021 05:13:02.100376 PST INFO : IPSec a reçu un événement
 client pour 169.254.202.2 09/03/2021 05:13:02.707976 PST INFO :
 IPSec got down-client event for 169.254.202.3
```


ImagePullBackOff

Vérifiez les éléments suivants :

1. Image non disponible sur le dépôt ou le nœud n'a pas accès au dépôt
2. x509 : certificat signé par une autorité inconnue. Si c'est le cas, procédez ainsi :

   ajoutez/Modifiez le fichier /etc/docker/daemon.json avec des dépôts privés :

3. ```
   root@vn-cl1-master1:~# cat /etc/docker/daemon.json
    {"insecure-registries" : ["panos-cntr-engtools-
   releng.af.paloaltonetworks.local", "panos-cntr-
   engtools. af.paloaltonetworks.local", "docker-
   public.af.paloaltonetworks.local", "panos-cntr-
   engtools-releng.af.paloaltonetworks.local", "docker-qa-
   pavm.af.paloaltonetworks.local"]} root@vn-cl1-master1 :~#
   ```

   Événements :

   ```
    Type Raison Âge À partir du message ---- ------ ---- ----
    ------- Normal Planifié 64 s default-scheduler Affecté avec
    succès kube-system/pan-cni-4jbpl à qalab- machine virtuelle
    Extraction normale 23 s (x3 sur 63 s) kubelet Extraction de
    l'image "docker-panos-ctnr.af.paloaltonetworks.local/pan-
   cni/develop/pan-cni-1.0.0:10_a26df862ed" Avertissement Échec
    23 s (x3 sur 63 s ) Kubelet Échec de l'extraction de l'image
    "docker-panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/
   pan-cni-1.0.0:10_a26df862ed" : erreur rpc : code = Inconnu desc
    = Réponse d'erreur du démon : Obtenez https://docker-panos-
   ctnr.af.paloaltonetworks.local/v2/ : x509 : certificat signé par
    une autorité inconnue Avertissement Échec 23s (x3 sur 63 s) Erreur
    kubelet : ErrImagePull Avertissement DNSConfigForming 8s (x7 sur
    63s) Les limites du serveur de noms kubelet ont été dépassées,
    certains serveurs de noms ont été omis, la ligne du serveur
    de noms appliquée est : 8.8.8.8 8.8.4.4 2620:130:800a:14::53
    BackOff normal 8s (x3 sur 63s) kubelet Back-off tirant l'image
    "docker-panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/
   pan -cni-1.0.0:10_a26df862ed" Avertissement Échec 8s (x3 sur 63
    s) Erreur kubelet : ImagePullBackOff qalab@master-node :~/cnv2/
   Kubernetes/pan-cn-k8s-service/native$
   ```


   ```

# Connectez-vous à DP à partir du nœud de travail exécuté dans l'espace de noms ns-panw

Accédez au répertoire /var/log/pan-appinfo et exécutez la commande **cat pan-cmdmap** et copiez le journal pour vous connecter à DP dans l'espace de noms nspan-fw

```
root@pv-k8-vm-worker-2:/var/log/pan-appinfo# cat pan-cmdmap
 02-07-2022 17:39:54.079133 PST : kube-system/pan-ngfw-ds-ql4q9 : ' /
usr/bin/nsenter -t 15872 -m -p --ipc -u --net=/var/run/netns/nspan-
fw -- /bin/bash' 02-07-2022 17:43:08.976154 PST : kube-system/pan-
ngfw-ds-zbt54 : '/usr/bin/nsenter -t 28308 -m -p --ipc -u --net=/var/
run/netns/nspan-fw -- /bin /bash' root@pv-k8-vm-worker-2:/var/log/
pan-appinfo# root@pv-k8-vm-worker-2:/var/log/pan-appinfo# /usr/bin/
 nsenter -t 28308 -m -p --ipc -u --net=/var/run/netns/nspan-fw -- /
bin/bash [root@pan-ngfw-ds-zbt54 /]# —--- -->>>>>
```

Vous pouvez vous connecter à DP et exécuter masterd all status à partir d'ici.

Les pods DP restent dans l'état **Création de conteneur** avec les journaux kubectl ci-dessous

“MountVolume.SetUp failed for volume "pan-cni-ready"

Échec de la vérification du type hostPath : **/var/log/pan-appinfo/pan-cni-ready** n'est pas un répertoire

```
Événements : Type Raison Âge À partir du message ---- ------ ----
 ---- ------- Normal Planifié 98 s default-scheduler Attribué
 avec succès kube-system/pan-ngfw-dep-7569f69d8- j4hfp vers ctnr-
debug-worker-3 Avertissement FailedMount 34s (x8 sur 98s) kubelet
 MountVolume.SetUp a échoué pour le volume "pan-cni-ready" : échec
 de la vérification du type hostPath : /var/log/pan-appinfo/pan-cni-
 ready n'est pas un répertoire test@msatane-182:~/scripts$
```

Solution :

1. consultez le journal kubectl du pod pan-cni. Assurez-vous que multus, non-multus et yaml sont correctement déployés.
2. Si multus est déployé, annulez le déploiement de multus et supprimez le fichier 00-multus.conf du répertoire /etc/cni/net.d/. Suivi du déploiement et du redéploiement de CNI et DP

Ci-dessous, les journaux k8 sur pan-cni montrent que multus est détecté. Vous devez donc suivre les étapes ci-dessus.

```
test@msatane-182:~/results/job_vm_series_72342/cn-sanity/cntr_deploy/
kube-system$ k8l pan-cni-csqt4 29/09/2021 04:07:22.495812 UTC
 DÉBOGAGE : CNI_CONF_NAME = 29/09/2021 04:07:22.498585 UTC DÉBOGAGE
 réussi : Utilisation du modèle de configuration CNI à partir
 de la variable d'environnement CNI_NETWORK_CONFIG. 29/09/2021
 04:07:22.633416 UTC DÉBOGAGE : Suppression des binaires existants
 29/09/2021 04:07:22.731559 UTC DÉBOGAGE : Binaires PAN CNI écrits
 dans /host/opt/cni/bin le 29/09/2021 04:07:22.734940 UTC DEBUG : /
host/secondary-bin-dir n'est pas accessible en écriture, saut le
 29/09/2021 04:07:22.752094 UTC DÉBOGAGE : Configuration PAN CNI :
 { "name": "pan-cni", "type": "pan-cni", "log_level": "debug",
 "appinfo_dir": "/var/log/pan-appinfo", "mode " : "service",
 "dpservicename": "pan-ngfw-svc", "dpservicenamespace": "kube-
system", "firewall": [ "pan-fw" ], "interfaces": [ "eth0" ],
 "interfacesip": [ "" ], "interfacesmac": [ "" ], "override_mtu":
 "", "kubernetes": { "kubeconfig": "/etc/cni/net.d/ZZZ-pan-cni-
 kubeconfig", "cni_bin_dir": "/opt/cni/bin", "exclude_namespaces":
 [], "security_namespaces": [ "kube-system" ] }} 29/09/2021
 04:07:22.756725 UTC DÉBOGAGE : CNI fonctionnant en mode FW
 Service. Le contournement du pare-feu peut être activé sur les
 pods d'application 29/09/2021 04:07:22.796082 UTC CRITIQUE : Multus
 détecté en tant que CNI primaire (fichier CONF 00-multus.conf) ;
 en attendant que les CNI non multus deviennent des CNI primaires.
 test@msatane-182 :~/results/job_vm_series_72342/cn-sanity/
cntr_deploy/kube-system$
```

État du lien sur le pod d'application sécurisé par CNv2 (à l'aide de vxlan)

root@testapp-secure-deployment-86f9f95b5-q5nxt:/# ip link show

lo : <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc retiré de la file d'attente état INCONNU mode PAR DÉFAUT groupe par défaut qlen 1000

lien/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

tunl0@AUCUN : <NOARP> mtu 1480 qdisc noop état INACTIF mode PAR DÉFAUT groupe par défaut qlen 1000

lien/ipip 0.0.0.0 brd 0.0.0.0

eth0@if227 : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1480 qdisc état retiré de la file d'attente UP mode PAR DÉFAUT groupe par défaut qlen 1000

lien/ether 26:54:8f:43:44:3f brd ff:ff:ff:ff:ff:ff lien-netnsid 0

vxlan0 : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1430 qdisc noqueue état INCONNU mode PAR DÉFAUT groupe par défaut qlen 1000

lien/ether 26:54:8f:43:44:3f brd ff:ff:ff:ff:ff:ff

root@testapp-secure-deployment-86f9f95b5-q5nxt:/#

Capturez l'assistance technique de MP

Sur MP :

1. admin@pan-mgmt-sts-0> demander un vidage de l'assistance technique

```
Travail d'exécution mis en file d'attente avec l'ID
 de travail 4 4 admin@pan-mgmt-sts-0> show jobs id 4
 Mis en file d'attente ID retiré de la file d'attente
 Type Statut Résultat Terminé ----------------------
 ------------------------------------------------
 ------------------------------------------------- ---- 15/02/2022
 12:46:50 12:46:51 4 Exec FIN OK 12:47:36
```

2. Connectez-vous à la racine MP pour copier le nom TSF stocké sur

   praveena@praveena : ~$ kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash

   Conteneur par défaut « pan-mgmt » parmi : pan-mgmt, pan-mgmt-init (init)

   [root@pan-mgmt-sts-0 /]#

   [root@pan-mgmt-sts-0 techsupport]# pwd

   /opt/pancfg/tmp/techsupport

   [root@pan-mgmt-sts-0 techsupport]# ls

   PA_878C48E8DDCFA5B_ts_102.0-c55_20220215_1246.tar.gz

3. Copiez le TSF du MP vers le contrôleur local en utilisant

   praveena@praveena : ~$ kubectl -n kube-system cp pan-mgmt-sts-0:/opt/pancfg/tmp/techsupport/PA_878C48E8DDCFA5B_ts_102.0-c55_20220215_1246.tar.gz PA_878C48E8DDCFA5B_ts_102.0-c55 _20220215_1246.tar.gz

HPA ne fonctionne pas

1. Vérifiez « k8sys get hpa » et « k8sys describe hpa »
2. Vérifiez l'outil de surveillance (cloudwatch/GCP stackdriver/Azure Application Insights) pour voir si les métriques personnalisées sont visibles.
3. Vérifiez /var/log/pan/pan_vm_plugin.log pour toute erreur si les métriques personnalisées sur l'outil de surveillance ne sont pas visibles

   test2@mks-test-181 :~/cnv2/yaml-files/CNSeries_V2/eks/HPA$ k8 obtenir des pods -n métriques personnalisées

   NAME READY STATUS RESTARTS AGE

   k8s-cloudwatch-adapter-6647595dfd-qhbtd 1/1 En cours d'exécution 0 42m

   test2@mks-test-181:~/cnv2/yaml-files/CNSeries_V2/eks/HPA$ journaux k8 k8s-cloudwatch-adapter-6647595dfd-qhbtd -n métriques personnalisées

Comment contrôler l'accès entrant aux applications sur OpenShift ?

Pour l'accès entrant aux applications :

1. Demandez au client d'activer la protection pour haproxy/router en utilisant l'annotation dans les fichiers yaml. Cela garantit que tout le trafic entrant et sortant de haproxy passe par CN-Series.
2. Demandez-lui d’utiliser les règles personnalisées basées sur les URL (destination) avec les adresses IP sources pour déterminer qui est autorisé à accéder à une application donnée. Les URL personnalisées telles que osecluster/payments doivent être définies pour les terminaux des applications. Cela leur permet d’autoriser ou de refuser l’accès à ces applications sans avoir à se soucier de la NAT.
3. En cas d'utilisation d'un équilibreur de charge externe (par exemple, F5) devant le cluster OSE, il est possible d'utiliser l'en-tête XFF pour appliquer une granularité plus poussée sur les personnes autorisées à accéder à une application donnée.

Annuler le déploiement de CN-Series

Exécutez les commandes suivantes :

1. kubectl delete -f pan-cn-mgmt.yaml
2. kubectl delete -f pan-cn-mgmt-configmap.yaml
3. kubectl delete -f pan-cn-mgmt-secret.yaml
4. Supprimer les PVC :

   kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts
5. kubectl delete -f . # annule le déploiement de tous les objets définis dans les yamls dans ce répertoire (CELA DÉTRUIT TOUT !!)

Activer le diagnostic de paquets sur CN

1. Exécutez dans le pod MP auquel est connecté le pod DP spécifique qui inspecte le trafic à partir du pod d'application.
2. Exécutez la commande suivante :

   ```
   > déboguer la source de correspondance du filtre défini par le
    diagnostic de paquets du plan de données <src> destination <> … >
    Vérifiez le filtre à l'aide de « debug dataplane packet-diag show
    settings » > debug dataplane packet-diag set capture on > Une fois
    les paquets capturés, exécutez « debug dataplane packet-diag set
    capture off »
   ```

3. Une fois le paquet capturé, recherchez le fichier sous :

   /opt/panlogs/session/pan/filters/

IPSec entre MP et DP échoue avec un état d'erreur asymétrique

Cela peut se produire dans les scénarios suivants :

1. MP et DP sont sur des versions PanOS différentes
2. « pan-cn-mgmt-slot-crd.yaml » et pan-cn-mgmt-slot-cr.yaml » ne sont pas déployés.

```
22/08/2022 -0700 11:46:35.208 16[NET] paquet reçu : de
 10.233.110.10[4500] à 10.233.96.7[4500] (464 octets) 22/08/2022-
 -0700 11:46:35.208 16 [ENC] a analysé la requête IKE_SA_INIT
 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG)
 N(REDIR_SUP) ] 22/08/2022 -0700 11:46:35.208 16[IKE] 10.233.
 110.10 lance une proposition sélectionnée IKE_SA 22/08/2022
 -0700 11:46:35.208 16[CFG] : IKE:AES_CBC_256/HMAC_SHA2_256_128/
PRF_HMAC_SHA2_256/MODP_2048 22/08/2022 -0700 11:46:35.229 16[IKE]
 l'hôte local est derrière NAT, envoyant des messages Keep
 Alive 2022-08-22 -0700 11:46:35.22 9 16[IKE] l'hôte distant
 est derrière NAT 2022-08-22 -0700 11:46:35.229 16[IKE] envoie
 une demande de certificat pour "CN=kubernetes" 2022-08-22
 -0700 11:46:35.229 16[ENC] génère une réponse IKE_SA_INIT
 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP)
 N(HASH_ALG) N(CHDLESS_SUP) ] 2022-08-22 -0700 11:46:35.229
 16[NET] envoi du paquet : à partir du 10.233.96.7[ 4500] à
 10.233.110.10[4500] (489 octets) 2022-08-22 -0700 11:46:35.274
 11[NET] paquet reçu : de 10.233.110.10[4500] à 10.233.96.7[4500]
 (1236 octets) 2022-08-22 -0700 11:46:35.274 11[ENC] a analysé la
 requête IKE_AUTH 1 [ EF(1/2) ] 2022-08-22-0 -0700 11:46:35.274
 11[ENC] a reçu le fragment n°1 sur 2 , en attente du message
 IKE complet 2022-08-22 -0700 11:46:35.274 12[NET] paquet
 reçu : de 10.233.110.10[4500] à 10.233.96.7[4500] (308 octets)
 2022-08-22 -0700 11:46:35.274 12[ENC] a analysé la requête
 IKE_AUTH 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.274 12[ENC] a
 reçu le fragment n° 2 sur 2, message IKE fragmenté réassemblé
 (1456 octets) 2022-08-22 -0700 11:46:35.274 12[ENC] analysé
 la requête IKE_AUTH 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr
 AUTH CPRQ(ADDR DNS) SA TSi TSr N(EAP_ONLY) N(MSG_ID_SYN_SUP)]
 2022-08-22 -0700 11:46:35.274 12[IKE] a reçu une demande de
 certificat pour "CN=kubernetes" 2022-08-22 -0700 11:46:35.274
 12[IKE] a reçu un certificat d'entité finale "CN=pan-fw .kube-
system.svc" 2022-08-22 -0700 11:46:35.274 12[CFG] recherche de
 configurations homologues correspondant à 10.233.96.7[CN=pan-
mgmt-svc.kube-system.svc]...10.233 .110.10[CN=pan-fw.kube-
system.svc] 22/08/2022 -0700 11:46:35.274 12[CFG] configuration
 homologue sélectionnée 'to-mp' 22/08/2022 -0700 11:46 : 35.274
 12[CFG] utilisant le certificat "CN=pan-fw.kube-system.svc"
 2022-08-22 -0700 11:46:35.275 12[CFG] utilisant le certificat
 CA de confiance "CN=kubernetes" 2022-08-22 -0700 11:46:35.275
 12[CFG] vérification de l'état du certificat de "CN=pan-fw.kube-
system.svc" 22/08/2022 -0700 11:46:35.275 12[CFG] l'état du
 certificat n'est pas disponible 2022 -08-22 -0700 11:46:35.275
 12[CFG] a atteint la racine auto-signée avec une longueur de
 chemin de 0 2022-08-22 -0700 11:46:35.275 12[IKE] authentification
```



```
 de 'CN=pan- fw.kube-system.svc' avec RSA_EMSA_PKCS1_SHA2_256
 réussie 2022-08-22 -0700 11:46:35.279 12[IKE] authentification
 de 'CN=pan-mgmt-svc.kube-system.svc' (moi-même) avec
 RSA_EMSA_PKCS1_SHA2_256 réussie 2022-08-22 -0700 11:46:35.279
 12[IKE] IKE_SA to-mp[2] établi entre 10.233.96.7[CN=pan-mgmt-
svc.kube-system.svc]...10.233.110.10[ CN=pan-fw.kube-system.svc]
 2022-08-22 -0700 11:46:35.279 12[IKE] envoi du certificat
 d'entité finale "CN=pan-mgmt-svc.kube-system.svc" 2022-08
 -22 -0700 11:46:35.279 12[IKE] un homologue a demandé une
 adresse IP virtuelle %any 2022-08-22 -0700 11:46:35.279 12[CFG]
 attribuant un nouveau bail à 'CN=pan-fw.kube-system. svc'
 2022-08-22 -0700 11:46:35.279 12[IKE] attribuant l'adresse IP
 virtuelle 169.254.202.2 à l'homologue 'CN=pan-fw.kube-system.svc'
 2022-08-22 -0700 11:46 : 35.279 12[CFG] proposition sélectionnée :
 ESP:AES_GCM_8_128/NO_EXT_SEQ 2022-08-22 -0700 11:46:35.279 12[IKE]
 CHILD_SA to-mp{1} établi avec les SPI 6d779dbe_i 0a178b55_o et
 TS 0.0.0.0/0 === 169.254.202.2 /32 2022-08-22 -0700 11:46:35.290
 12[ENC] générant la réponse IKE_AUTH 1 [ IDr CERT AUTH CPRP(ADDR)
 SA TSi TSr ] 2022-08-22 -0700 11:46:35.290 12[ENC] fractionnement
 d'IKE message (1392 octets) en 2 fragments 2022-08-22 -0700
 11:46:35.290 12[ENC] générant la réponse IKE_AUTH 1 [ EF(1/2) ]
 2022-08-22 -0700 11:46:35.290 12[ ENC] générant la réponse
 IKE_AUTH 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.291 12[NET]
 envoi du paquet : de 10.233.96.7[4500] à 10.233.110.10[4500] (1236
 octets ) 2022-08-22 -0700 11:46:35.291 12[NET] envoi du paquet :
 de 10.233.96.7[4500] à 10.233.110.10[4500] (228 octets) 2022-08-22
 -0700 11:46:35.345 09[NET] paquet reçu : de 10.233.96.9[4500]
 à 10.233.96.7[4500] (464 octets) 2022-08-22 -0700 11:46:35.346
 09[ENC] analysé la requête IKE_SA_INIT 0 [ SA KE No N (NATD_S_IP)
 N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ] 2022-08-22
 -0700 11:46:35.346 09[IKE] 10.233.96.9 lance un IKE_SA
 2022-08-22 -0700 11:46:35.346 09[CFG] proposition sélectionnée :
 IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
 2022-08-22 -0700 11:46:35.356 09[IKE] l'hôte local est derrière
 NAT, envoie des messages Keep Alive 2022-08-22 -0700 11:46:35.35
 6 09[IKE] l'hôte distant est derrière NAT 2022-08-22 -0700
 11:46:35.356 09[IKE] envoie une demande de certificat pour
 "CN=kubernetes" 2022-08-22 -0700 11:46:35.356 09[ENC] génère
 une réponse IKE_SA_INIT 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP)
 CERTREQ N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) ] 2022-08-22
 -0700 11:46:35.356 09[NET] envoi du paquet : à partir du
 10.233.96.7[ 4500] à 10.233.96.9[4500] (489 octets) 2022-08-22
 -0700 11:46:35.363 10[NET] paquet reçu : de 10.233.96.9[4500]
 à 10.233.96.7[4500] (1236 octets) 2022-08-22 -0700 11:46:35.364
 10[ENC] analysé la requête IKE_AUTH 1 [ EF(1/2) ] 2022-08-22
 -0700 11:46:35.364 10[ENC] a reçu le fragment n°1 sur 2 , en
 attente du message IKE complet 2022-08-22 -0700 11:46:35.364
 15[NET] paquet reçu : de 10.233.96.9[4500] à 10.233.96.7[4500]
 (308 octets) 2022-08-22 -0700 11:46:35.364 15[ENC] a analysé
 la requête IKE_AUTH 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.364
 15[ENC] a reçu le fragment n°2 sur 2, message IKE fragmenté
 réassemblé (1456 octets) 2022-08-22 -0700 11:46:35.364 15[ENC]
 analysé la requête IKE_AUTH 1 [ IDi CERT N(INIT_CONTACT) CERTREQ
 IDr AUTH CPRQ(ADDR DNS) SA TSi TSr N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
 2022 -08-22 -0700 11:46:35.364 15[IKE] a reçu une demande de
 certificat pour "CN=kubernetes" 2022-08-22 -0700 11:46:35.364
```



```
 15[IKE] a reçu un certificat d'entité finale "CN=pan-fw .kube-
system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] recherche de
 configurations homologues correspondant à 10.233.96.7[CN=pan-mgmt-
svc.kube-system.svc]...10.233 .96.9[CN=pan-fw.kube-system.svc]
 2022-08-22 -0700 11:46:35.364 15[CFG] configuration homologue
 sélectionnée 'to-mp' 2022-08-22 -0700 11:46 : 35.364 15[CFG]
 utilisant le certificat "CN=pan-fw.kube-system.svc" 2022-08-22
 -0700 11:46:35.364 15[CFG] utilisant le certificat CA de confiance
 "CN=kubernetes" 2022-08-22 -0700 11:46:35.364 15[CFG] vérification
 de l'état du certificat de "CN=pan-fw.kube-system.svc" 2022-08-22
 -0700 11:46:35.364 15[CFG] l'état du certificat n'est pas
 disponible 2022 -08-22 -0700 11:46:35.364 15[CFG] a atteint la
 racine auto-signée avec une longueur de chemin de 0 2022-08-22
 -0700 11:46:35.364 15[IKE] authentification de 'CN=pan- fw.kube-
system.svc' avec RSA_EMSA_PKCS1_SHA2_256 réussie 2022-08-22
 -0700 11:46:35.366 15[IKE] authentification de 'CN=pan-mgmt-
svc.kube-system.svc' (moi-même) avec RSA_EMSA_PKCS1_SHA2_256
 réussie 2022-08-22 -0700 11:46:35.366 15[IKE] IKE_SA
 to-mp[3] établi entre 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.96.9[ CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:35.366 15[IKE] envoi du certificat d'entité finale
 "CN=pan-mgmt-svc.kube-system.svc" 2022-08 -22 -0700 11:46:35.366
 15[IKE] un homologue a demandé une adresse IP virtuelle %any
 2022-08-22 -0700 11:46:35.366 15[CFG] attribuant un nouveau bail
 à 'CN=pan-fw.kube-system. svc' 2022-08-22 -0700 11:46:35.366
 15[IKE] attribuant l'adresse IP virtuelle 169.254.202.3 à
 l'homologue 'CN=pan-fw.kube-system.svc' 2022-08-22 -0700 11:46 :
 35.366 15[CFG] proposition sélectionnée : ESP:AES_GCM_8_128/
NO_EXT_SEQ 22/08/2022 -0700 11:46:35.366 15[IKE] CHILD_SA to-
mp{2} établi avec les SPI a97528ab_i f6667584_o et TS 0.0.0.0/0
 === 169.254.202.3/3 2 22/08/2022 -0700 11:46:35.372 15[CHD]
 vers le haut : SIOCADRT : Le fichier existe 2022-08-22 -0700
 11:46:35.373 15[ENC] générant la réponse IKE_AUTH 1 [ IDr CERT
 AUTH CPRP(ADDR) SA TSi TSr ] 2022-08-22 -0700 11:46:35.373
 15[ENC] diviser le message IKE (1392 octets) en 2 fragments
 2022-08-22 -0700 11:46:35.373 15[ENC] générer la réponse IKE_AUTH
 1 [ EF(1/2) ] 2022-08-22 -0700 11:46:35.373 15[ENC] générant
 la réponse IKE_AUTH 1 [ EF(2/2)] 2022-08-22 -0700 11:46:35.373
 15[NET] envoi du paquet : de 10.233.96.7[4500] à 10.233.96.9[4500]
 ( 1236 octets) 2022-08-22 -0700 11:46:35.373 15[NET] envoi
 du paquet : de 10.233.96.7[4500] à 10.233.96.9[4500] (228
 octets) 2022-08-22 -0700 11:46 :46.471 11[NET] paquet reçu :
 de 10.233.96.9[4500] à 10.233.96.7[4500] (80 octets) 2022-08-22
 -0700 11:46:46.471 11[ENC] requête INFORMATIONNELLE analysée
 2 [ D ] 2022-08-22 -0700 11:46:46.471 11[IKE] a reçu DELETE
 pour IKE_SA to-mp[3] entre 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.96.9[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:46.471 11[IKE] incapable de rétablir IKE_SA en raison
 d'une configuration asymétrique 2022-08-22 -0700 11:46:46.471
 11[IKE] IKE_SA supprimé 2022-08-22 -0700 11:46:46.751 11[ENC]
 générant une réponse INFORMATIONNELLE 2 [ ] 2022-08-22 -0700
 11:46:46.751 11[NET] envoi du paquet : de 10.233.96.7[4500] à
 10.233.96.9[4500] (80 octets) 2022-08-22 -0700 11:46 : 46.752
 11[CFG] bail 169.254.202.3 par 'CN=pan-fw.kube-system.svc'
 s'est déconnecté 2022-08-22 -0700 11:46:47.040 12[NET] paquet
 reçu : de 10.233.110.10[4500 ] à 10.233.96.7[4500] (80 octets)
```



```
2022-08-22 -0700 11:46:47.040 12[ENC] demande d'information
analysée 2 [ D ] 2022-08-22 -0700 11:46:47.040 12[IKE ] a reçu
DELETE pour IKE_SA to-mp[2] 2022-08-22 -0700 11:46:47.040 12[IKE]
supprimant IKE_SA to-mp[2] entre 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.110.10[CN=pan-fw.kube-system.svc] 2022-08-22
-0700 11:46:47.040 12[IKE] impossible de rétablir IKE_SA en raison
d'une configuration asymétrique 2022-08 -22 -0700 11:46:47.041
12[IKE] IKE_SA supprimé
```


Les pods d'application ne parviennent pas à résoudre les problèmes de DNS (qu'il y ait un pare-feu ou non)

Vérifiez les éléments suivants :

1. Vérifiez que les pods DNS sont en cours d'exécution : « kubectl get pods --namespace=kube-system -l k8s-app=kube-dns »
2. Vérifiez que le service DNS est en cours d'exécution : « kubectl get svc --namespace=kube-system »
3. Si le service DNS n'est pas en cours d'exécution, exposez le déploiement DNS en tant que svc ou utilisez le yaml et déployez.
4. Une fois le SVC déployé, vérifiez que les terminaux sont correctement exposés.« kubectl récupère les terminaux coredns --namespace=kube-system »
5. Redéployez les pods d’application.