paloalto TECHDOCS

CN-Series 疑難排解

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

CN-Series 疑難排解

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • Panorama 執行 PAN-OS 10.1.x 或更高版本

表 **1:** 詞彙定義：

詞彙	定義
MP	CN-MGMT
DP	CN-NGFW

連線至 MP 或 DP

執行以下命令以了解您的 MP 或 DP Pod 名稱：

kubectl get pods -n=<namespace>

執行以下命令以連線至 MP 或 DP Pod：

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

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

Pod 無法提取錯誤映像

x509：由未知授權單位簽署的憑證（主要出現在原生/內部部署 **k8** 叢集）

在所有工作節點上，使用您要從中提取的映像儲存庫來更新 **/etc/docker/daemon.json**。如果 daemon.json 檔案不存在，請建立該檔案

```
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:~#
```

使用命令 **"systemctl restart docker.service"** 重新啟動 Docker。

MP 處於擱置中狀態

驗證下列事項：

1. MP 可以使用節點、記憶體和 CPU 等必要資源。我們可以檢查命令輸出加以確認

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

```
                node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:
  Type     Reason            Age                  From               Message
  ----     ------            ----                 ----               -------
  Warning  FailedScheduling  101s (x551 over 13h)  default-scheduler  0/1 nodes are available: 1 Insuf
test@mks-test-181:~$
```

2. 永久性磁碟區 (PV) 是叢集中的儲存區，由伺服器/儲存區/叢集管理員佈建或使用儲存區類別進行動態佈建。它與節點一樣是叢集中的資源。永久性磁碟區宣告 (PVC) 是使用者對儲存區發出的要求，可以從 PV 中取得。

   PVC 會繫結至 PV (`kubectl -n kube-system get pvc`)。如果未繫結，請執行以下命令以刪除舊 PVC：

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

3. 檢查是否至少在 2 個工作節點上針對內部部署設定建立必需的目錄（/mnt 下方的 pan-local1、pan-local2、pan-local3、pan-local4、pan-local5、pan-local6）。

   `/mnt` 下方的 `pan-local1`、`pan-local2`、`pan-local3`、`pan-local4`、`pan-local5`、`pan-local6` 不需要動態磁碟區佈建。AWS EKS 上缺少 EBS CSI 驅動程式是 MP 處於擱置中狀態的原因之一。您必須確認啟用叢集中的 EBS CSI 驅動程式，檢查角色並確認叢集的提供者。如需更多詳細資訊，請參閱將 Amazon EBS CSI 驅動程式作為 Amazon EKS 附加元件進行管理。

4. 如果錯誤是「`pan-mgmt-sts-0`：Pod 具有未繫結的立即永久性磁碟區宣告」請執行「**kubectl get pvcs -o wide**」和「**kubectl get pv -o wide**」。其中應顯示哪些 PVC 繫結失敗。

   解決方案是使用命令 **kubectl -n kube-system delete pvc/<pvc-name>** 刪除或清理舊 PVC。刪除所有 PVC、PV。部署新的 PV 並部署 MP。

5. 如果 **"k8 describe pod <mp-pod>"** 出現以下錯誤，請確認已建立 PV。如果尚未建立，則請部署 pan-cn-pv-local.yaml（使用設定目錄的節點名稱）

   Pod「**"pan-mgmt-sts-0"**」：Pod 具有未繫結的永久性磁碟區宣告的 **"VolumeBinding"** 篩選器外掛程式

   警告排程失敗 <unknown> 執行 Pod「**"pan-mgmt-sts-0"**」：Pod 具有未繫結的永久性磁碟區宣告的 **"VolumeBinding"** 篩選器外掛程式的預設排程器

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:管理開始執行 PanOS 版本 10.1.3-
   c47 的容器
   ```

   12-22-2021 11:34:41.335521 PST ERROR:啟動 **pansw** 失敗：**2**

   問題可能是 “**pan-cn-mgmt-configmap.yaml**” 沒有必填值。
   ```

MP 不斷當機

登入 MP root 並前往 **/var/cores** 以查看當機程序。

K8 MP 日誌會顯示以下錯誤

裝置註冊要求失敗：無法向 **CSP** 伺服器傳送要求

驗證下列事項：

1. 「Pan-cn-mgmt-secret.yaml」應具有下列兩個欄位的正確值 CN-SERIES-AUTO-REGISTRATION-PIN-ID：「<PIN Id>」

   CN-SERIES-AUTO-REGISTRATION-PIN-VALUE：「<PIN-Value>」
2. 如果以上值正確無誤，請確認 PinID 和值未從 CSP 到期

MP 無法連線至 Panorama 或 MP CommitAll 失敗

1. 確認 MP 可以到達/偵測 Panorama IP。針對公共雲端，確定已設定所需的安全性政策，以啟用 Panorama 與 K8 叢集之間的連線性

   登入 MP：

   - 1. Kubectl -n kube-system exec -it <mp-pod-name> -- su admin
     2. 「顯示 Panorama 狀態」以取得 Panorama IP 位址
     3. 偵測主機 <panorama-ip>
     4. 如果偵測有效，請繼續進行以下驗證動作
2. 確認 mgmt-secret.yaml 所提供的「bootstrap-auth-key」存在於 Panorama 且未到期。
   1. 若要驗證 bootstrap-auth-key，請登入 Panorama 並執行命令「request bootstrap vm-auth-key show」→ 這應該有效（未到期）
   2. 如果不可行，請以「request bootstrap vm-auth-key generate lifetime 8760」產生並在 pan-mgmt-secret.yaml 中更新。取消部署所有 yaml，並清除 PV、PVC，然後重新部署。
3. 確認 mgmt-configmap.yaml 中所設定 DG、TS 和收集器群組 (CG) 有無拼寫錯誤，且在 Panorama 上設定和提交
4. 確認在 mgmt.yam 之前部署 pan-mgmt-configmap 和密碼 yamls；確認在 mgmt.yaml 之前部署 pan-mgmt-configmap 和密碼 yamls。
5. 執行 CMD「顯示所有工作」和「顯示工作 ID <id>」，檢查 MP 上 Panorama 的 commit-all 是否成功，並檢視是否有任何失敗、修正 Panorama 上的任何設定，然後再次執行 commit all/force。
6. Panorama 設定已推送到 MP「show config Pushed-shared-policy」
7. 請輸入 CMD「debug tac-login response」並以 MP 序號進行搜尋，從根目錄中尋找 Panorama 的 configd.log。其中應會說明連線失敗的原因。

   vi /var/log/pan/configd.log

   Example（範例）：

```
2021-03-15 14:19:49.213 -0700 Error:
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4085):
 bootstrap: template stack cnv2-template-stack
 not found, serial=8CABD801686AD2021-04-15
 14:19:49.213 -0700 bootstrap: candidate cfg ch Error:
 pan_cfg_bootstrap_vm_auth_key_verify(pan_cfg_bootstrap_mgr.c:3822):找不到 vm_auth_key 923688689426978；vm_auth _key 無效
```

CommitAll 不會在 MP 上啟動

在 Panorama 上確認 CommitAll 工作是否處於停滯/ACT 狀態。

發生這種情況的原因可能是 MP 和 Panorama 之間的網路連線問題。

在實驗室中，將 MP/工作節點和 Panorama 置於同一子網路中可以解決此問題。

如果遇到上述問題，您可以看到以下 Panorama 日誌。

```
2023-01-19 09:13:51.788 -0800 錯
誤：device_needs_bkup(pan_bkup_mgr.c:323): failed to check out /opt/
pancfg/mgmt/devices/8B8AE8CB506CF09/running-config.xml 2023-01-19
 09:13:51.938 -0800 Panorama push device-group cn-dg-12c13c51-1
 for device 8B8AE8CB506CF09 with merge-with-candidate-cfg include-
template flags set.JobId=50860.User=pano rama.Dequeue time=2023/01/19
 09:13:51. 2023-01-19 09:13:52.812 -0800 Preference list thread was
 spawned to send to device 8B8AE8CB506CF09 in group CG 2023-01-19
 09:13:52.812 -0800 Preference list thread was sent to device
 8B8AE8CB506CF09 2023-01-19 09:13:52.813 -0800 DAU2:系統將清除
 dev:8B8AE8CB506CF09 上的所有位址。2023-01-19 09:14:35.061 -0800 錯
誤：pan_conn_mgr_callback_expiry_async(cs_conn.c:8781): connmgr:到期的
要求。entry:916, msgno=3 devid=8B8AE8CB506CF09 2023-01-19 09:14:35.061
 -0800 錯誤：pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:到期的要求。entry:916, msgno=6 devid=8B8AE8CB506CF09
 2023-01-19 09:14:35.061 -0800 錯
誤：pan_conn_mgr_callback_expiry_async(cs_conn.c:8781): connmgr:到期的
要求。entry:916, msgno=4 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060
 -0800 錯誤：pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:到期的要求。entry:916, msgno=0 devid=8B8AE8CB506CF09
 2023-01-19 09:15:05.060 -0800 錯
誤：pan_conn_mgr_callback_expiry_async(cs_conn.c:8781): connmgr:到期的
要求。entry:916, msgno=5 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060
 -0800 copy-lcs-pref-list:回應處理器：複製 lcs pref 工作從 cookie 2407 的
裝置 8B8AE8CB506CF09 接收到的回應。目前的 Cookie 是 2408。Remaini ng:1
 2023-01-19 09:15:05.060 -0800 copy-lcs-pref-list:回應處理器：複製
 lcs pref 工作從 cookie 2408 的裝置 8B8AE8CB506CF09 接收到的回應。目
前的 Cookie 是 2408。Remaini ng:1 2023-01-19 09:15:05.060 -0800 錯
誤：pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761):2023-01-19
 09:15:05.060 -0800 copy-lcs-pref-list:Failed to receive
 response fro m device 8B8AE8CB506CF09.錯誤 - 逾時傳送/接收訊息錯
誤：pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761):
 copy-lcs-pref-list:無法從裝置 8B8AE8CB506CF09 接收回應。錯誤 - 逾時傳
送/接收訊息 2023-01-19 09:15:08.545 -0800 connmgr: received disconnect
 cb from ms for 8B8AE8CB506CF09(1020484) 2023-01-19 09:15:08.545
 -0800 connmgr: connection entry removed. devid=8B8AE8CB506CF09
 sock=4294967295 result=0 2023-01-19 09:15:08.545 -0800 Handling
 device conn update [disconnection][activated:1] for 8B8AE8CB506CF09:
 "server: client is device" 2023-01-19 09:15:08.545 -0800 錯
誤：pan_bkupjobmgr_process_async_result(pan_bkup_mgr.c:208):無
法從裝置 8B8AE8CB506CF09 接收回應。錯誤 - 無
法傳送訊息 2023-01-19 09:15:08.545 -0800 錯
```

```
誤：pan_async_lcs_pref_list_result(pan_comp_collector.c:2681):
 lcs-pref-list:無法從裝置 8B8AE8CB506CF09 接收回應。錯誤
 - 無法傳送訊息 2023-01-19 09:15:08.546 -0800 Panorama HA
 feedback:8B8AE8CB506CF09 disconnected 2023-01-19 09:15:08.547
 -0800 connmgr: connection entry removed. devid=8B8AE8CB506CF09
 (1020484) 2023-01-19 09:15:41.212 -0800 Warning:
 _register_ext_validation(pan_cfg_mgt_handler.c:4418): reg: device
 '8B8AE8CB506CF09' not using issued cert.2023-01-19 09:15:41.213
 -0800 警告：pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4737):SC3:
 device '8B8AE8CB506CF09' is not SC3 capable 2023-01-19
 09:15:41.213 -0800 SVM registration.Serial: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:8410079617204080582: svm_id:2023-01-19 09:15:41.213 -0800 錯
誤：pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4020):
 bootstrap:8B8AE8CB506CF09 已新增至 mgd 裝置
```

DP Pod 處於擱置中或容器建立狀態

執行以下命令並確認和修復相應命令的輸出錯誤

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

   如果上述命令出現下列錯誤，請繼續尋找 CNI 日誌以及 CNI 是否正在使用 Multus。

   ```
   MountVolume.SetUp failed for volume "pan-cni-ready" : hostPath
    type check failed: /var/log/pan-appinfo/pan-cni-ready is not a
    directory
   ```

2. Kubectl -n kube-system 日誌 <dp-pod-name>
3. Kubectl -n kube-system 描述 Pod <cni-name-on-same-node>
4. Kubectl -n kube-system 日誌 <cni-name-on-same-node>
5. 如果 kubectl CNI 日誌如下，請確認 CNI 正在每個節點上執行。（GKE 叢集上需啟用預設 CNi 的網路政策才能執行）：

   ```
   08-18-2022 23:55:07.397661 UTC DEBUG:PAN CNI config: { "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" ] }} 08-18-2022
    23:55:07.402812 UTC DEBUG:在 FW 服務模式中執行的 CNI。您可以在應用程
   式 Pod 上啟用繞過防火牆 08-18-2022 23:55:07.454392 UTC CRITICAL:偵測
   到 Multus 作為主要 CNI（CONF 檔案 00-multus.conf）；正在等待非 Multus
    CNI 成為主要 CNI。root@manojmaster:~/pan-cn-k8s-service/native#
   ```

   如果出現上述錯誤，請嘗試取消部署 Multus 並從部署此 CNI 和 DP 的工作節點中刪除檔案 00-multus.conf

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

MP：不顯示 Panorama 詳細資料/狀態

```
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. pan-cn-mgmt-configmap 可能部署在 pan-cn-mgmt.yaml 之後
2. pan-cn-mgmt-secret 部署可能失敗（可能因為 bootstrap-auth-key 以“0”開頭）→ 從 Panorama 刪除並重新建立驗證金鑰，確保它不以“0”開頭

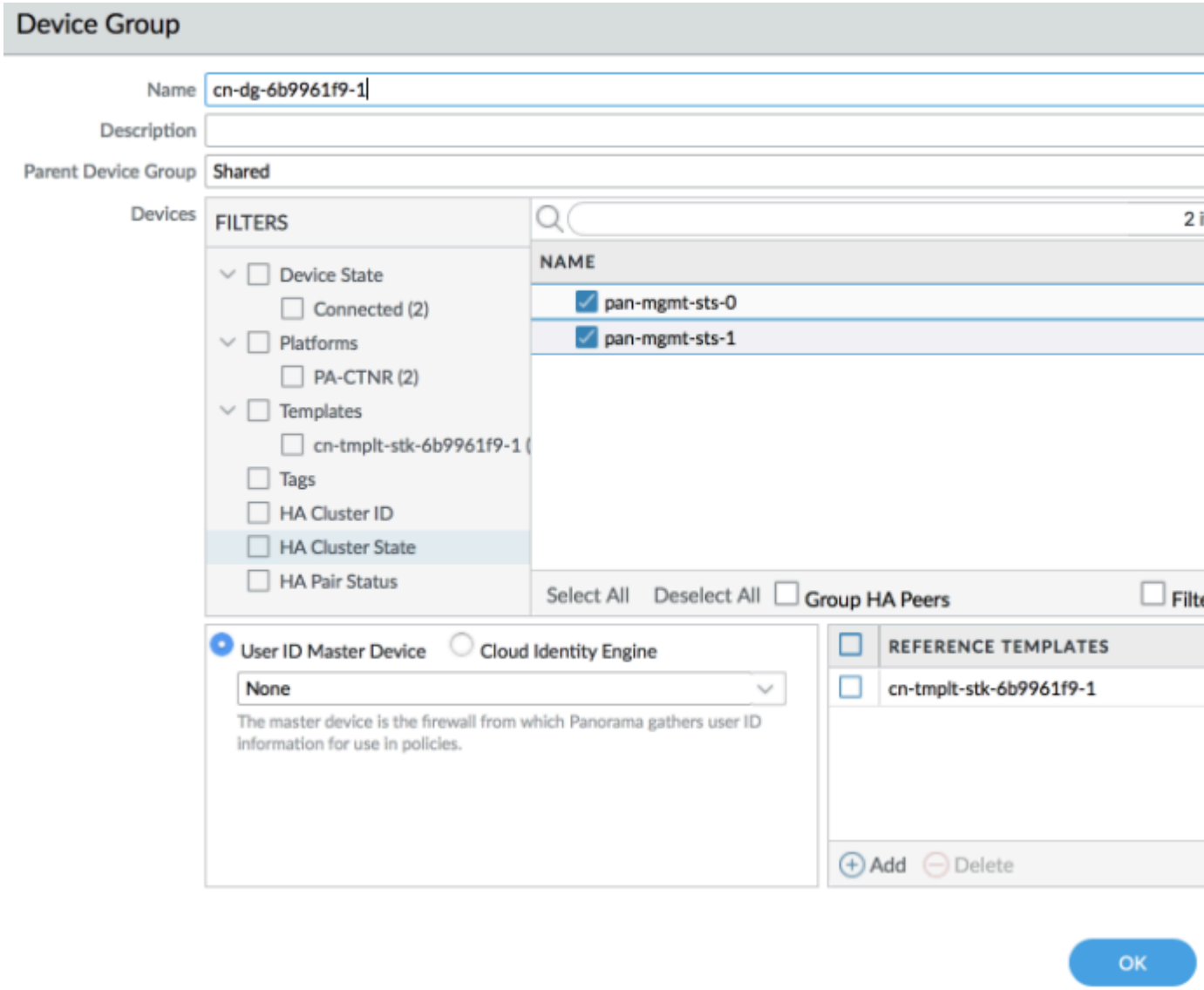
若要解決此問題，請取消部署 MP、刪除 PVC、PV、重新部署 mp-configmap，然後再部署 MP。

如果使用 HELM 圖表進行部署：

若要解決此問題，請取消部署 HELM 圖表、刪除 CN-Series PVC/PV，然後重新部署 HELM。

Panorama 未將 MP 顯示為受管理的裝置

1. 請確認 MP 和 DP 的軟體版本相同。「MP 上的 K8 日誌如果沒有相同的版本，則可能產生錯誤日誌。
2. 如果部署了 mgmt-slot-crd 和 mgmt-slot-cr.yaml。
3. 如果此 DP 已與任何 MP 建立 IPSec（使用根登入 MP 並使用 cmd “ipsec status” 進行檢查。
4. 自動認可和 CommitAll 應已傳遞此 DP 連接到的 MP。如果沒有，請檢查 MP，瞭解 CommitAll 或自動認可的失敗原因並進行相應修復。請參考上述步驟（MP 無法連線至 Panorama 或 MP CommitAll 失敗）以解決問題。
5. admin@pan-mgmt-sts-0> debug 會顯示所有內部介面 → 應顯示介面設定，如果沒有，請確認 DG 中參考範本堆疊。也要確認 K8S 網路範本具介面設定。



6. 如果 DP 有 4Gig 記憶體（檢查 ngfw.yaml）

7. 執行「masterd all status」cmd 來檢查 Masterd 所有程序是否正在執行。
8. 「Ps -aef」會檢查程序是否正常執行。
9. 請檢查以下命令的輸出並確認是否發現 DP 插槽註冊失敗：

```
“kubectl get panslotconfigs -n kube-system --insecure-skip-tls-
verify -o yaml”
```

DP 插槽註冊失敗

1. 確認是否已部署 pan-cn-mgmt-slot-cr and crd.yamls。
2.
```
[root@rk-cl3-master-1 native-2]# k8sys get PanSlotConfig NAME 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 get crd | grep
 pan NAME CREATED AT panslotconfigs.paloaltonetworks.com
 2022-11-10T04:18:13Z [root@rk-cl3-master-1 native-2]#
```

```
11-21-2022 20:54:31.783302 UTC INFO:Masterd Started 11-21-2022
 20:54:40.050008 UTC INFO:IPSec up-client event with 169.254.202.2
 11-21-2022 20:54:40.121502 UTC INFO:Calling dp slot register
 script 11-21-2022 20:54:40.323061 UTC WARNING:Readiness:尚
未準備好。Panorama 設定未推送。pan_task 未執行。11-21-2022
 20:54:40.486734 UTC INFO:Strongswan 精靈已啟動。正在嘗試達到管理平
面..11-21-2022 20:54:41.623966 UTC INFO:已建立管理平面連線。11-21-2022
 20:54:42.700770 UTC ERROR:註冊/重新註冊失敗：USER 11-21-2022
 20:54:42.818729 UTC WARNING: dp slot register failed.重複嘗試
幾次 11-21-2022 20:54:44.265372 UTC ERROR:註冊/重新註冊失敗：USER
 11-21-2022 20:54:45.759982 UTC ERROR:註冊/重新註冊失敗：USER
 11-21-2022 20:54:47.256744 UTC ERROR:註冊/重新註冊失敗：USER
 11-21-2022 20:54:48.768491 UTC ERROR:註冊/重新註冊失敗：USER
 11-21-2022 20:54:50.272969 UTC ERROR:註冊/重新註冊失敗：USER
 11-21-2022 20:54:51.390138 UTC CRITICAL:註冊 MP 失敗。關閉 DP
```

執行「k8 get pods -n kube-system」時，MP/DP/CNI Pod 不會顯示

1. 因為未部署 sa.yaml，請確認是否未建立服務帳戶。
2. 使用命令「k8 -n kube-system get svc」確認 MP 服務正常執行
3. 使用命令「k8 -n kube-system get sts」確認 MP 具狀態集正常執行，且 k8n -n 描述 sts/pan-mgmt-sts → 如果 pvc/pv 出現任何問題，這將進行列印

來自未透過 DP/防火牆傳送的安全應用程式 Pod 的流量

1. 確認所有工作節點是否正在執行最低 5.4 核心版本（使用 cmd “kubectl getnodes -o Wide）

```
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. （僅適用於 CNv2）確認是否在安全應用程式 Pod 上建立「vxlan」介面，並透過此 vxlan 介面建立了預設路由

```
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. 如果 DP 處於活動/執行狀態，但 IPSec 已終止，請確認 DP 是否正在執行並使用 IPSec 連接到 MP

4. 確認 DP 授權是否在 DP 啟動 4 小時後因為沒有驗證碼或群集未連接到 Panorama - k8 外掛程式而失敗

```
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. 確認 Panorama 中 kubernets 外掛程式的驗證碼尚未到期

   admin@Panorama> request plugins kubernetes get-license-tokens

   安全性訂閱：Wildfire、威脅防禦、DNS、URL 篩選

   授權碼類型：SW-NGFW 積分

   授權碼：D2962989

   已到期：無

   到期日期：2022 年 12 月 31 日

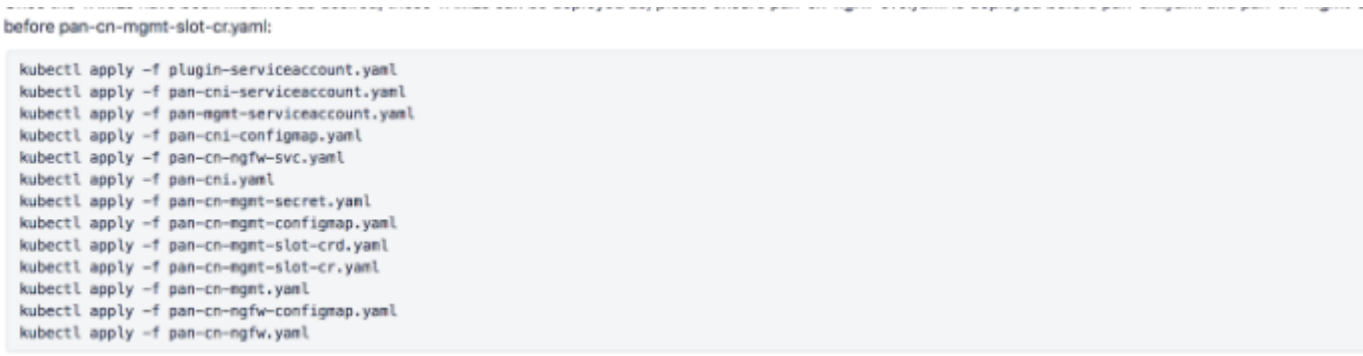
   已發布的 vCPU：50

   已使用的 vCPU：0

   發布日期：2022 年 12 月 31 日

   admin@Panorama-49.88>

6. 確認是否在 CNI.yaml 前面部署 ngfw-svc.yaml，且 NGFW svc 具 ClusterIP 並正在執行。


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. 登入 /var/log/pan/pan-cni.log ([ec2-user@ip-12-12-12-184 ~]$ vi /var/log/pan-appinfo/pan-cni.log) 下的節點，以確認 CNI 日誌
8. 應該在 CNI 和 ngfw svc 執行之後建立應用程式 Pod，您可以重新啟動 Pod 以解決問題
9. 應該在 CNI 和 ngfw svc 執行之後建立應用程式 Pod，您可以重新啟動 Pod 以解決問題
10. 在 MP Pod 上使用命令「debug show internal interface all」檢查介面設定是否推送到 DP
11. 使用「“show rule-hit-count vsys vsys-name vsys1 rule-base security rules all」以查看命中哪個安全性規則並相應修改安全性政策。

如何確認哪個 DP Pod 正在處理流量

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. 在 Panorama 上 > 監控日誌，新增 [Container ID（容器 ID）]欄，然後您將看到上面的容器 ID。

記錄：Panorama 不會顯示流量/威脅日誌

以下是疑難排解步驟：

1. 使用命令「show log traffic/threat direction equal backward」確認 MP 是否產生日誌。如果在 MP 上未看到日誌，請使用「show session all」確認相同的 MP 是否正在處理流量，同時從安全 Pod 傳送連續偵測
2. 使用命令確保 DP 已獲授權：
    1. 在 MP 上「request plugins vm_series list-dp-pods」
    2. DP 上的 K8 日誌應予以確認。
3. 「debug log-receiver statistics」會顯示從 DP 到 MP 的日誌傳入速率。
4. 使用「show session all」和「show session id <id>」，以檢查流量是否符合已設定日誌轉送的預期政策。
5. 使用 CMD「show config pushed-shared-policy」和「show running security-policy」，以檢查 MP 上是否收到設定
6. 確定受管理的收集器在 Panorama 上同步且處於已連線狀態。
7. Panorama 上的「masterd elasticsearch status」→ 應該正在執行。如果尚未執行，則請執行「es_restart.py -e」
8. ```
   [root@cnsmokepanorama ~]# sdb cfg.es.* cfg.es.acache-update:1
    cfg.es.enable:0x0
   ```
9. es_cluster.sh health
10. “debug log-collector log-collection-stats show incoming-logs” on the panorama
11. **pan_logquery -t traffic -i bwd -n 50**
   ```

記錄：使用規則名稱篩選時 Panorama 不會顯示日誌

當 Panorama 無法正確載入 ES 範本時，可能會發生錯誤。請嘗試在 Panorama 根模式下透過命令「es_restart.py -t」重新啟動 ES。傳送新的流量/日誌並確認系統是否顯示日誌：

```
[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 ~]#
```

MP 無法重新連線至 Panorama

```
pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105):此裝置或日誌收集器或
 wf 設備 (devid 892A1C93EF280D0) 不受管理
```

以上錯誤訊息表示裝置正在重新註冊，因為之前已進行註冊，所以它不會透過啟動工作流程將自己新增至 Panorama 設定。

如果裝置先前已註冊和連接但未在 Panorama 上提交以儲存該設定，然後 Panorama 經重新啟動、清除設定，並當裝置嘗試連線時，Panorama 無法識別該裝置而中斷連線，就可能發生這種情況。

以下是 Panorama 上 `configd.log` 的日誌：

```
2021-02-03 11:48:00.436 -0800 Processing lcs-register message
 from device '8B1EB1ADC72B44E' 2021-02-03 11:48:00.436 -0800 警
告：_get_current_cert(sc3_utils.c:84): sdb 節點「cfg.ms.ak」不
存在。2021-02-03 11:48:04.425 -0800 logbuffer: 無主動連線至 cms0
 2021-02-03 11:48:24.425 -0800 logbuffer:無主動連線至 cms0 2021-02-03
 11:48:44.425 -0800 logbuffer: 無主動連線至 cms0 2021-02-03
 11:48:57.751 -0800 警告：sc3_register(sc3_register.c:90):SC3:已
停用 - 略過註冊。2021-02-03 11:48:57.752 -0800 警
告：pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645):SC3:
 device '892A1C93EF280D0' is not SC3 capable 2021-02-03
 11:48:57.752 -0800 SVM registration.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 processing a register message
 from 892A1C93EF280D0 2021-02-03 11:48:57.752 -0800 錯
誤：pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105):此裝置或
日誌收集器或 wf 設備 (devid 892A1C93EF280D0) 不受管理 2021-02-03
 11:49:04.426 -0800 logbuffer：無主動連線至 cms0 2021-02-03
 11:49:06.015 -0800 警告：sc3_register(sc3_register.c:90):SC3:已
停用 - 略過註冊。2021-02-03 11:49:06.015 -0800 警
告：pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645):SC3:
 device '8B1EB1ADC72B44E' is not SC3 capable 2021-02-03
 11:49:06.015 -0800 SVM registration.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 processing a register message
 from 8B1EB1ADC72B44E 2021-02-03 11:49:06.015 -0800 錯
誤：pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105):此裝置或日誌收集器
或 wf 應用程式
```

MP 和 DP 處於活動且執行狀態，但 IPsec 在 MP 和 DP 之間遭終止

確認 MP 上的 kubectl 日誌，檢查是否在 4 個小時後釋出插槽，如下所示：

```
（部分）root@test-virtual-machine:~# k8sys logs pan-mgmt-sts-0
 03-09-2021 01:07:36.508002 PST INFO:管理容器開始執行 PanOS
 version 10.1.0-c182.dev_s_rel Starting PAN Software:03-09-2021
 01:08:07.460287 PST WARNING:Readiness:尚未準備就緒。資料平面註冊的
插槽未執行。資料平面連線的 ipsec 正在執行。無法執行 cmd:dpdk-devbind --
status [ OK ] 03-09-2021 01:09:43.043467 PST INFO:Masterd Started
 03-09-2021 01:10:53.453639 PST WARNING:Readiness:準備就緒。資料平面註
冊的插槽正在執行。資料平面連線的 ipsec 正在執行。03-09-2021 01:10:54.558525
 PST INFO:Strongswan 精靈已啟動。03-09-2021 01:10:56.286104 PST
 INFO:SW 版本相符，MP 和 DP 軟體版本為 10.1.0-c182.dev_s_rel 03-09-2021
 01:10:56.346162 PST INFO:Get registration with uid pan-ngfw-
ds-4lhhc, sw_ver 10.1.0-c182.dev_s_rel, slot 0, dp_ip 169.254.202.2
 03-09-2021 01:10:56.453298 PST INFO:Allocated slot 1 for uid
 pan-ngfw-ds-4lhhc 169.254.202.2 03-09-2021 01:10:57.131769 PST
 INFO:SW 版本相符，MP 和 DP 軟體版本為 10.1.0-c182.dev_s_rel 03-09-2021
 01:10:57.198584 PST INFO:Get registration with uid pan-ngfw-
ds-9pj2f, sw_ver 10.1.0-c182.dev_s_rel, slot 0, dp_ip 169.254.202.3
 03-09-2021 01:10:57.288892 PST INFO:Allocated slot 2 for uid pan-
ngfw-ds-9pj2f 169.254.202.3 03-09-2021 01:12:02.279032 PST INFO:正在安
裝 AutoFocus 授權。03-09-2021 01:12:02.362417 PST INFO:正在安裝記錄日誌服
務授權。03-09-2021 05:13:01.521227 PST INFO:SW 版本相符，MP 和 DP 軟體版本
為 10.1.0-c182.dev_s_rel 03-09-2021 05:13:01.597810 PST INFO:Freeing
 slot 2, uid pan-ngfw-ds-9pj2f with Force 03-09-2021 05:13:01.694588
 PST INFO:SW 版本相符，MP 和 DP 軟體版本為 10.1.0-c182.dev_s_rel
 03-09-2021 05:13:01.764245 PST INFO:Freeing slot 1, uid pan-ngfw-
ds-4lhhc with Force 03-09-2021 05:13:02.100376 PST INFO:IPSec got
 down-client event for 169.254.202.2 03-09-2021 05:13:02.707976 PST
 INFO:IPSec got down-client event for 169.254.202.3
```

ImagePullBackOff

檢查以下內容：

1. 映像在儲存庫上不可使用或節點無權存取儲存庫
2. x509：由未知授權單位簽署的憑證..若是此情況，請執行以下操作：

   add/Modify the file /etc/docker/daemon.json with private repos:

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:~#
   ```

   Events:

   ```
    Type Reason Age From Message ---- ------ ---- ---- -------
    Normal Scheduled 64s default-scheduler Successfully assigned
    kube-system/pan-cni-4jbpl to qalab-virtual-machine Normal
    Pulling 23s (x3 over 63s) kubelet Pulling image "docker-
   panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/pan-
   cni-1.0.0:10_a26df862ed" Warning Failed 23s (x3 over 63s) kubelet
    Failed to pull image "docker-panos-ctnr.af.paloaltonetworks.local/
   pan-cni/develop/pan-cni-1.0.0:10_a26df862ed": rpc error: code =
    Unknown desc = Error response from daemon:取得 https://docker-
   panos-ctnr.af.paloaltonetworks.local/v2/: x509：由未知授權單位簽署的憑
   證警告 Failed 23s (x3 over 63s) kubelet Error:ErrImagePull Warning
    DNSConfigForming 8s (x7 over 63s) kubelet 名稱伺服器限制已超過，部分名
   稱伺服器遭省略，使用的名稱伺服器列為：8.8.8.8 8.8.4.4 2620:130:800a:14::53
    Normal BackOff 8s (x3 over 63s) kubelet Back-off pulling image
    "docker-panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/pan-
   cni-1.0.0:10_a26df862ed" Warning Failed 8s (x3 over 63s) kubelet
    Error:ImagePullBackOff qalab@master-node:~/cnv2/Kubernetes/pan-cn-
   k8s-service/native$
   ```
   ```

從在 ns-panw 命名空間中執行的工作節點登入 DP

前往 /var/log/pan-appinfo 目錄、執行命令 **cat pan-cmdmap** 並複製日誌以登入 nspan-fw 命名空間中的 DP

```
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 /]# —------>>>>>
```

您可以登入 DP 並從這裡執行 masterd 所有狀態。

DP Pod 仍處於 **ContainerCreating** 狀態，並具有以下 kubectl 日誌

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

hostPath 類型檢查失敗：**/var/log/pan-appinfo/pan-cni-ready** 不是目錄

```
事件：Type Reason Age From Message ---- ------ ---- ---- -------
 Normal Scheduled 98s default-scheduler Successfully assigned kube-
system/pan-ngfw-dep-7569f69d8-j4hfp to ctnr-debug-worker-3 Warning
 FailedMount 34s (x8 over 98s) kubelet MountVolume.SetUp failed for
 volume "pan-cni-ready" : hostPath type check failed: /var/log/pan-
appinfo/pan-cni-ready is not a directory test@msatane-182:~/scripts$
```

解決方案：

1. 檢查 pan-cni Pod 的 kubectl 日誌。確保 Multus 與非 Multus 部署正確的 yaml。
2. 如果已部署 Multus，請取消部署 Multus 並從 /etc/cni/net.d/ 目錄中移除 00-multus.conf。然後取消部署並重新部署 CNI 和 DP

以下 pan-cni 的 k8 日誌會顯示偵測到 Multus。因此您應遵循上述步驟。

```
test@msatane-182:~/results/job_vm_series_72342/cn-sanity/cntr_deploy/
kube-system$ k8l pan-cni-csqt4 09-29-2021 04:07:22.495812 UTC
 DEBUG:Passed CNI_CONF_NAME= 09-29-2021 04:07:22.498585 UTC
 DEBUG:請使用 CNI_NETWORK_CONFIG 環境變數中的 CNI 設定範本。09-29-2021
 04:07:22.633416 UTC DEBUG:刪除現有二進位檔 09-29-2021 04:07:22.731559
 UTC DEBUG:將 PAN CNI 二進位檔寫入 /host/opt/cni/bin 09-29-2021
 04:07:22.734940 UTC DEBUG: /host/secondary-bin-dir is non-
writeable, skipping 09-29-2021 04:07:22.752094 UTC DEBUG:PAN CNI
 config: { "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" ] }} 09-29-2021
 04:07:22.756725 UTC DEBUG:在 FW 服務模式中執行的 CNI。您可以在應用程式
 Pod 上啟用繞過防火牆 09-29-2021 04:07:22.796082 UTC CRITICAL:檢測到
 Multus 作為主要 CNI（CONF 檔案 00-multus.conf）；正在等待非 Multus CNI 成
為主要 CNI。test@msatane-182:~/results/job_vm_series_72342/cn-sanity/
cntr_deploy/kube-system$
```

由 CNv2 保護（使用 vxlan）的應用程式 Pod 上的連線狀態

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

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

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

eth0@if227: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1480 qdisc noqueue state UP mode DEFAULT group default qlen 1000

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

vxlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1430 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000

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

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

擷取 MP 的技術支援

在 MP 上：

1. admin@pan-mgmt-sts-0> request tech-support dump

```
Exec job enqueued with jobid 4 4 admin@pan-mgmt-sts-0> show
 jobs id 4 Enqueued Dequeued ID Type Status Result Completed
 ------------------------------------------------------------------------------
 2022/02/15 12:46:50 12:46:51 4 Exec FIN OK 12:47:36
```

2. 登入 MP 根以複製儲存在以下位置的 TSF 名稱

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

   Defaulted container "pan-mgmt" out of: 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. 請使用以下命令，將 TSF 從 MP 複製到本機控制器

   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 無法正常運作

1. 驗證「k8sys get hpa」和「k8sys describe hpa」
2. 確認監控工具 (cloudwatch/GCP stackdriver/Azure App Insights) 以查看系統是否顯示自訂指標。
3. 如果未看到監控工具上的自訂指標，請確認 /var/log/pan/pan_vm_plugin.log 是否有任何錯誤

   test2@mks-test-181:~/cnv2/yaml-files/CNSeries_V2/eks/HPA$ k8 get pods -n custom-metrics

   NAME READY STATUS RESTARTS AGE

   k8s-cloudwatch-adapter-6647595dfd-qhbtd 1/1 Running 0 42m

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

如何控制 - OpenShift 上應用程式的輸入存取？

針對應用程式的輸入存取：

1. 讓客戶使用 yaml 檔案中的註釋來啟用對 haproxy/路由器的保護。這將確保所有進出 haproxy 的流量都會通過 CN-Series。
2. 讓他們搭配使用自訂 URL 型規則（目的地）與來源 IP，以強制執行允許誰存取給定的應用程式。需要針對應用程式的端點定義自訂 URL，例如 osecluster/payments。這將可讓其允許/拒絕這些應用程式的存取，而不需要擔心 NAT。
3. 如果他們要在 OSE 叢集前面使用 F5 這類外部負載平衡器，則他們應該使用 XFF 標頭，以針對允許誰存取給定應用程式來進一步細化。

取消部署 CN-series

執行下列命令：

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. 刪除 PVC：

   kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts
5. kubectl delete -f . → undeploys all objects defined in the yamls in that dir

   （此動作將銷毀一切內容#）

在 CN 上啟用 packet-diag

1. 執行到特定 DP Pod 的 MP Pod，該 DP Pod 會檢查來自應用程式 Pod 的流量。
2. 執行下列命令：

```
> debug dataplane packet-diag set filter match source <src>
 destination <> ⋯ > Verify the filter using “debug dataplane
 packet-diag show setting” > debug dataplane packet-diag set
 capture on > After packets are captured execute “debug dataplane
 packet-diag set capture off”
```

3. 擷取封包之後，請從以下位置找到檔案：

   /opt/panlogs/session/pan/filters/

MP 和 DP 之間的 IPSec 失敗，出現不對稱狀態

這可能發生在以下情況：

1. MP 和 DP 位於不同的 PanOS 版本
2. 未部署「pan-cn-mgmt-slot-crd.yaml」和「pan-cn-mgmt-slot-cr.yaml」。

```
2022-08-22 -0700 11:46:35.208 16[NET] received packet: from
 10.233.110.10[4500] to 10.233.96.7[4500] (464 bytes) 2022-08-22
 -0700 11:46:35.208 16[ENC] parsed IKE_SA_INIT request 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 11:46:35.208 16[IKE] 10.233.110.10 is initiating
 an IKE_SA 2022-08-22 -0700 11:46:35.208 16[CFG] selected
 proposal:IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/
MODP_2048 2022-08-22 -0700 11:46:35.229 16[IKE] local host is
 behind NAT, sending keep alives 2022-08-22 -0700 11:46:35.229
 16[IKE] remote host is behind NAT 2022-08-22 -0700 11:46:35.229
 16[IKE] sending cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.229 16[ENC] generating IKE_SA_INIT response
 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]
 sending packet: from 10.233.96.7[4500] to 10.233.110.10[4500]
 (489 bytes) 2022-08-22 -0700 11:46:35.274 11[NET] received
 packet: from 10.233.110.10[4500] to 10.233.96.7[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.274 11[ENC] parsed IKE_AUTH
 request 1 [ EF(1/2) ] 2022-08-22 -0700 11:46:35.274 11[ENC]
 received fragment #1 of 2, waiting for complete IKE message
 2022-08-22 -0700 11:46:35.274 12[NET] received packet: from
 10.233.110.10[4500] to 10.233.96.7[4500] (308 bytes) 2022-08-22
 -0700 11:46:35.274 12[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
 2022-08-22 -0700 11:46:35.274 12[ENC] received fragment #2 of
 2, reassembled fragmented IKE message (1456 bytes) 2022-08-22
 -0700 11:46:35.274 12[ENC] parsed IKE_AUTH request 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] received cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.274 12[IKE] received end entity cert "CN=pan-
fw.kube-system.svc" 2022-08-22 -0700 11:46:35.274 12[CFG] looking
 for peer configs matching 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 11:46:35.274 12[CFG] selected peer config 'to-mp' 2022-08-22
 -0700 11:46:35.274 12[CFG] using certificate "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.275 12[CFG] using trusted
 ca certificate "CN=kubernetes" 2022-08-22 -0700 11:46:35.275
 12[CFG] checking certificate status of "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.275 12[CFG] certificate
 status is not available 2022-08-22 -0700 11:46:35.275 12[CFG]
 reached self-signed root ca with a path length of 0 2022-08-22
 -0700 11:46:35.275 12[IKE] authentication of 'CN=pan-fw.kube-
system.svc' with RSA_EMSA_PKCS1_SHA2_256 successful 2022-08-22
 -0700 11:46:35.279 12[IKE] authentication of 'CN=pan-mgmt-
svc.kube-system.svc' (myself) with RSA_EMSA_PKCS1_SHA2_256
 successful 2022-08-22 -0700 11:46:35.279 12[IKE] IKE_SA to-
mp[2] established between 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] sending end entity cert "CN=pan-
mgmt-svc.kube-system.svc" 2022-08-22 -0700 11:46:35.279 12[IKE]
 peer requested virtual IP %any 2022-08-22 -0700 11:46:35.279
 12[CFG] assigning new lease to 'CN=pan-fw.kube-system.svc'
 2022-08-22 -0700 11:46:35.279 12[IKE] assigning virtual IP
 169.254.202.2 to peer 'CN=pan-fw.kube-system.svc' 2022-08-22
 -0700 11:46:35.279 12[CFG] selected proposal:ESP:AES_GCM_8_128/
NO_EXT_SEQ 2022-08-22 -0700 11:46:35.279 12[IKE] CHILD_SA to-mp{1}
 established with SPIs 6d779dbe_i 0a178b55_o and TS 0.0.0.0/0
 === 169.254.202.2/32 2022-08-22 -0700 11:46:35.290 12[ENC]
 generating IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR)
 SA TSi TSr ] 2022-08-22 -0700 11:46:35.290 12[ENC] splitting
 IKE message (1392 bytes) into 2 fragments 2022-08-22 -0700
 11:46:35.290 12[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
 2022-08-22 -0700 11:46:35.290 12[ENC] generating IKE_AUTH response
 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.291 12[NET] sending
 packet: from 10.233.96.7[4500] to 10.233.110.10[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.291 12[NET] sending packet:
 from 10.233.96.7[4500] to 10.233.110.10[4500] (228 bytes)
 2022-08-22 -0700 11:46:35.345 09[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (464 bytes) 2022-08-22
 -0700 11:46:35.346 09[ENC] parsed IKE_SA_INIT request 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 is initiating
 an IKE_SA 2022-08-22 -0700 11:46:35.346 09[CFG] selected
 proposal:IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/
MODP_2048 2022-08-22 -0700 11:46:35.356 09[IKE] local host is
 behind NAT, sending keep alives 2022-08-22 -0700 11:46:35.356
 09[IKE] remote host is behind NAT 2022-08-22 -0700 11:46:35.356
 09[IKE] sending cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.356 09[ENC] generating IKE_SA_INIT response
 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]
 sending packet: from 10.233.96.7[4500] to 10.233.96.9[4500]
 (489 bytes) 2022-08-22 -0700 11:46:35.363 10[NET] received
 packet: from 10.233.96.9[4500] to 10.233.96.7[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.364 10[ENC] parsed IKE_AUTH
 request 1 [ EF(1/2) ] 2022-08-22 -0700 11:46:35.364 10[ENC]
 received fragment #1 of 2, waiting for complete IKE message
 2022-08-22 -0700 11:46:35.364 15[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (308 bytes) 2022-08-22
 -0700 11:46:35.364 15[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
 2022-08-22 -0700 11:46:35.364 15[ENC] received fragment #2 of
 2, reassembled fragmented IKE message (1456 bytes) 2022-08-22
 -0700 11:46:35.364 15[ENC] parsed IKE_AUTH request 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] received cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.364 15[IKE] received end entity cert "CN=pan-
fw.kube-system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] looking
 for peer configs matching 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] selected peer config 'to-mp' 2022-08-22
 -0700 11:46:35.364 15[CFG] using certificate "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] using trusted
```

```
 ca certificate "CN=kubernetes" 2022-08-22 -0700 11:46:35.364
 15[CFG] checking certificate status of "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] certificate
 status is not available 2022-08-22 -0700 11:46:35.364 15[CFG]
 reached self-signed root ca with a path length of 0 2022-08-22
 -0700 11:46:35.364 15[IKE] authentication of 'CN=pan-fw.kube-
system.svc' with RSA_EMSA_PKCS1_SHA2_256 successful 2022-08-22
 -0700 11:46:35.366 15[IKE] authentication of 'CN=pan-mgmt-
svc.kube-system.svc' (myself) with RSA_EMSA_PKCS1_SHA2_256
 successful 2022-08-22 -0700 11:46:35.366 15[IKE] IKE_SA to-
mp[3] established between 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] sending end entity cert "CN=pan-
mgmt-svc.kube-system.svc" 2022-08-22 -0700 11:46:35.366 15[IKE]
 peer requested virtual IP %any 2022-08-22 -0700 11:46:35.366
 15[CFG] assigning new lease to 'CN=pan-fw.kube-system.svc'
 2022-08-22 -0700 11:46:35.366 15[IKE] assigning virtual IP
 169.254.202.3 to peer 'CN=pan-fw.kube-system.svc' 2022-08-22
 -0700 11:46:35.366 15[CFG] selected proposal:ESP:AES_GCM_8_128/
NO_EXT_SEQ 2022-08-22 -0700 11:46:35.366 15[IKE] CHILD_SA to-mp{2}
 established with SPIs a97528ab_i f6667584_o and TS 0.0.0.0/0
 === 169.254.202.3/32 2022-08-22 -0700 11:46:35.372 15[CHD]
 updown:SIOCADDRT:File exists 2022-08-22 -0700 11:46:35.373
 15[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR)
 SA TSi TSr ] 2022-08-22 -0700 11:46:35.373 15[ENC] splitting
 IKE message (1392 bytes) into 2 fragments 2022-08-22 -0700
 11:46:35.373 15[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
 2022-08-22 -0700 11:46:35.373 15[ENC] generating IKE_AUTH
 response 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.373 15[NET]
 sending packet: from 10.233.96.7[4500] to 10.233.96.9[4500]
 (1236 bytes) 2022-08-22 -0700 11:46:35.373 15[NET] sending
 packet: from 10.233.96.7[4500] to 10.233.96.9[4500] (228 bytes)
 2022-08-22 -0700 11:46:46.471 11[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (80 bytes) 2022-08-22
 -0700 11:46:46.471 11[ENC] parsed INFORMATIONAL request 2
 [ D ] 2022-08-22 -0700 11:46:46.471 11[IKE] received DELETE
 for IKE_SA to-mp[3] 2022-08-22 -0700 11:46:46.471 11[IKE]
 deleting IKE_SA to-mp[3] between 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] unable to reestablish
 IKE_SA due to asymmetric setup 2022-08-22 -0700 11:46:46.471
 11[IKE] IKE_SA deleted 2022-08-22 -0700 11:46:46.751 11[ENC]
 generating INFORMATIONAL response 2 [ ] 2022-08-22 -0700
 11:46:46.751 11[NET] sending packet: from 10.233.96.7[4500]
 to 10.233.96.9[4500] (80 bytes) 2022-08-22 -0700 11:46:46.752
 11[CFG] lease 169.254.202.3 by 'CN=pan-fw.kube-system.svc'
 went offline 2022-08-22 -0700 11:46:47.040 12[NET] received
 packet: from 10.233.110.10[4500] to 10.233.96.7[4500] (80 bytes)
 2022-08-22 -0700 11:46:47.040 12[ENC] parsed INFORMATIONAL
 request 2 [ D ] 2022-08-22 -0700 11:46:47.040 12[IKE] received
 DELETE for IKE_SA to-mp[2] 2022-08-22 -0700 11:46:47.040 12[IKE]
 deleting IKE_SA to-mp[2] between 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] unable to reestablish IKE_SA due to
 asymmetric setup 2022-08-22 -0700 11:46:47.041 12[IKE] IKE_SA
 deleted
```

應用程式 Pod 無法進行 DNS 解析（無論是否有防火牆）

驗證下列事項：

1. 檢查 DNS Pod 是否正在執行：「kubectl get pods --namespace=kube-system -l k8s-app=kube-dns」
2. 檢查 DNS 服務是否正在執行：「kubectl get svc --namespace=kube-system」
3. 如未執行 DNS 服務，請將 DNS 部署公開為 svc 或使用 yaml 並進行部署。
4. 部署 SVC 之後，請確認端點是否正確公開。「kubectl get endpoints coredns --namespace=kube-system」
5. 重新部署應用程式 Pod。