paloalto TECHDOCS

Resolución de problemas de CN-series

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

Resolución de problemas de CN-series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior

Table 1: Definiciones de términos:

Término	Definiciones
MP	CN-MGMT
DP	CN-NGFW

Conexión a MP o DP

Ejecute el siguiente comando para conocer el nombre de su módulo MP o DP:

kubectl get pods -n=<namespace>

Ejecute el siguiente comando para conectarse a pods MP o DP:

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

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

Los pods no consiguen extraer la imagen con error

x509: certificado firmado por una autoridad desconocida (visto generalmente con clústeres nativos/ onprem k8)

En todos los nodos trabajadores, actualice **/etc/docker/daemon.json** con el repositorio de imágenes del que está extrayendo. Cree un archivo daemon.json si no existe

```
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:~#
```

Reinicio del docker con el comando "**systemctl restart docker.service**".

MP permanece en estado Pendiente

Verifique lo siguiente:

1. Los recursos necesarios (nodo/memoria/cpu) están disponibles para MP. Podemos verificarlo esto comprobando la salida del comando para

   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. Un volumen persistente, PersistentVolume, (PV) es un fragmento de almacenamiento en el clúster que ha aprovisionado el administrador del servidor/almacenamiento/clúster o se ha aprovisionado dinámicamente mediante clases de almacenamiento. Es un recurso en el clúster al igual que el nodo. Una PersistentVolumeClaim (PVC) es una solicitud de almacenamiento realizada por un usuario que se puede obtener de PV.

   Las PVC están unidas al PV (`kubectl -n kube-system get pvc`). Si no es así, borre las pvc antiguas que ejecuten el siguiente comando:

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

3. Compruebe si todos los directorios necesarios (pan-local1, pan-local2, pan-local3, pan-local4, pan-local5, pan-local6 en /mnt) se crean en al menos 2 nodos trabajadores para las configuraciones locales.

   Los directorios `panlocal1, panlocal2, panlocal3, panlocal4, panlocal5, panlocal6` *en* `/ mnt` *no son necesarios para el aprovisionamiento dinámico por volumen. La falta del controlador EBS CSI en AWS EKS es una de las razones por las que el MP permanece en estado pendiente. Debe asegurarse de que el controlador CSI de EBS esté habilitado en el clúster, comprobar la función e identificar el proveedor del clúster. Para obtener más información, consulte* Gestión del controlador de CSI de Amazon EBS como complemento de Amazon EKS.

4. Si el error es “`pan-mgmt-sts-0`”: pod tiene PersistentVolumeClaims inmediatas ilimitadas” ejec. “**kubectl get pvcs -o wide**” y “**kubectl get pv -o wide**”. Esto debería mostrar cuáles pvc fallaron en unirse.

   La solución sería borrar las PVC antiguas usando el comando **kubectl -n kube-system delete pvc/ <pvc-name>** o eliminar. Eliminar todas las PVC, PV. Implemente nuevos PV e implemente MP.

5. Si **"k8 describe pod <mp-pod>"** falla con el error a continuación, asegúrese de que los PV estén creados. Si no es así, implemente pan-cn-pv-local.yaml (con los nombres de los nodos donde están configurados los directorios)

   Complemento de filtro **"VolumeBinding"** para pod ""**pan-mgmt-sts-0**"": pod tiene PersistentVolumeClaims ilimitados

   Advertencia FailedScheduling <unknown> default-scheduler ejecutando el complemento de filtro **"VolumeBinding"** para pod ""**pan-mgmt-sts-0**"": pod tiene PersistentVolumeClaims ilimitados

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: El contenedor de gestión
    comienza a ejecutar PanOS versión 10.1.3-c47
   ```

   12-22-2021 11:34:41.335521 PST ERROR: No se pudo iniciar pansw: 2

   El problema puede ser que **“pan-cn-mgmt-configmap.yaml”** no tenga valores obligatorios.


   ```

# MP sigue colapsándose

Inicie sesión en la raíz de MP y vaya a **/var/cores** para ver el proceso que se está bloqueando.

# Los logs de K8 MP muestran el siguiente error

**La solicitud de registro del dispositivo falló: No fue posible enviar la solicitud al servidor CSP**

Verifique lo siguiente:

1. “Pan-cn-mgmt-secret.yaml” debería tener valores correctos para los siguientes 2 campos CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN Id>"

   CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<PIN-Value>"
2. Si los valores anteriores son correctos, asegúrese de que PinID y Value (Valor) no hayan caducado desde CSP

# MP no se puede conectar a Panorama o fallo de MP CommitFall

1. Verifique que MP puede alcanzar o hacer ping a la IP de Panorama. Para las nubes públicas, asegúrese de que las políticas de seguridad requeridas estén configuradas para habilitar la conectividad entre Panorama y los clústeres K8.

   Iniciar sesión en mp:

   - 1. Kubectl -n kube-system exec -it <mp-pod-name> -- su admin
     2. “Mostrar estado del panorama” para obtener la dirección IP del panorama
     3. Haga ping al host <panorama-ip>
     4. Si el ping funciona, continúe con las verificaciones a continuación
2. Verifique que “bootstrap-auth-key” proporcionado en mgmt-secret.yaml esté presente en Panorama y no haya caducado.
   1. Para verificar bootstrap-auth-key, inicie sesión en panorama y ejecute el comando “request bootstrap vm-auth-key show” # Este debería ser válido(no caducado)
   2. Si no está disponible, genérelo usando “request bootstrap vm-auth-key generate life 8760” y actualice en pan-mgmt-secret.yaml. Eliminar implementación de todos los yamls, borre PV, PVC y vuelva a implementar.
3. Verifique que el DG, TS y el grupo de recopiladores (CG) configurados en mgmt-configmap.yaml no estén mal escritos, configurados y confirmados en Panorama
4. Verifique que pan-mgmt-configmap y yamls secretos se implementen antes de mgmt.yam.
5. Verifique si commit-all de Panorama en MP es correcta usando el comando “show jobs all” y “show job id <id>” para ver si hay fallos y corregir cualquier configuración en panorama, y vuelva a confirmar todo/forzar.
6. La configuración de Panorama se envía a MP “show config push-shared-policy”
7. Busque configd.log en Panorama desde la raíz introduciendo cmd “debug tac-login response” y busque con el número de serie de MP. Debería indicar la razón por la que falla la conexión.

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

   **Ejemplo**:

```
2021-03-15 14:19:49.213 -0700 Error:
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4085):
 bootstrap: pila de plantillas 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):
 Error al encontrar vm_auth_key 923688689426978, vm_auth _key no
 válido
```

Commit All no se inicia en el MP

Verifique en Panorama si los trabajos de CommitAll están en el estado atascados/ACT.

Esto puede suceder debido a problemas de conectividad de red entre el MP y Panorama.

En el Lab, este problema se resuelve teniendo el MP/worker-node y Panorama en la misma subred.

A continuación se pueden ver los logs de panorama si se encuentra el problema anterior.

```
2023-01-19 09:13:51.788 -0800 Error:
 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: Will
 clear all addresses on dev:8B8AE8CB506CF09. 2023-01-19 09:14:35.061
 -0800 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr: Expired Request. entry:916, msgno=3
 devid=8B8AE8CB506CF09 2023-01-19 09:14:35.061 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr: Expired Request. entry:916, msgno=6
 devid=8B8AE8CB506CF09 2023-01-19 09:14:35.061 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr: Expired Request. entry:916, msgno=4
 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr: Expired Request. entry:916, msgno=0
 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060 -0800 Error:
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781): connmgr:
 Expired Request. entry:916, msgno=5 devid=8B8AE8CB506CF09
 2023-01-19 09:15:05.060 -0800 copy-lcs-pref-list: Response
 Processor: copy lcs pref job received response from device
 8B8AE8CB506CF09 of cookie 2407. Current cookie is 2408.
 Remaini ng: 1 2023-01-19 09:15:05.060 -0800 copy-lcs-pref-
list: Response Processor: copy lcs pref job received response
 from device 8B8AE8CB506CF09 of cookie 2408. Current cookie
 is 2408. Remaini ng: 1 2023-01-19 09:15:05.060 -0800 Error:
 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.
 Error - time out sending/receiving message Error:
 pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761):
 copy-lcs-pref-list:Failed to receive response from device
 8B8AE8CB506CF09. Error - time out sending/receiving message
 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
 Error: pan_bkupjobmgr_process_async_result(pan_bkup_mgr.c:208):
```



```
 Failed to receive response from device 8B8AE8CB506CF09. Error
 - failed to send message 2023-01-19 09:15:08.545 -0800 Error:
 pan_async_lcs_pref_list_result(pan_comp_collector.c:2681): lcs-pref-
list:Failed to receive response from device 8B8AE8CB506CF09. Error
 - failed to send message 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 Warning: 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 Error:
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4020):
 bootstrap: 8B8AE8CB506CF09 already adde d to mgd devices
```


Los pods DP permanecen en estado Pendiente o Contenedor

Ejecute los siguientes comandos, verifique los errores mencionados en el resultado obtenido del respectivo comando y corrija

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

   Si el siguiente error se ve como parte del comando anterior, continúe buscando logs de CNI y si CNI está usando 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 logs <dp-pod-name>
3. Kubectl -n kube-system describe pod <cni-name-on-same-node>
4. Kubectl -n kube-system logs <cni-name-on-same-node>
5. Si kubectl CNI registra como a continuación, asegúrese de que CNI se ejecuta en cada nodo. (En el clúster GKE, necesitamos habilitar la política de red para que se ejecute la CNI predeterminada):

   ```
   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: CNI que se ejecuta en modo de
    servicio de FW. Bypassfirewall can be enabled on application
    pods 08-18-2022 23:55:07.454392 UTC CRITICAL: Detected Multus as
    primary CNI (CONF file 00-multus.conf); waiting for non-multus
    CNI to become primary CNI. root@manojmaster:~/pan-cn-k8s-service/
   native#
   ```

   Si se ve el error anterior, Pruebe a quitar la implementación de Multus y elimine el archivo 00-multus.conf de los nodos trabajadores donde se implementan los DP y CNI

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


MP: No muestra detalles/estado del 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. Es posible que pan-cn-mgmt-configmap se implemente después de pan-cn-mgmt.yaml
2. Es posible que la implementación de pan-cn-mgmt-secret falló (posiblemente porque bootstrap-auth-key empieza con ‘0’) # Elimine la clave de autenticación de panorama y recree para asegurarse de que no comience con ‘0’

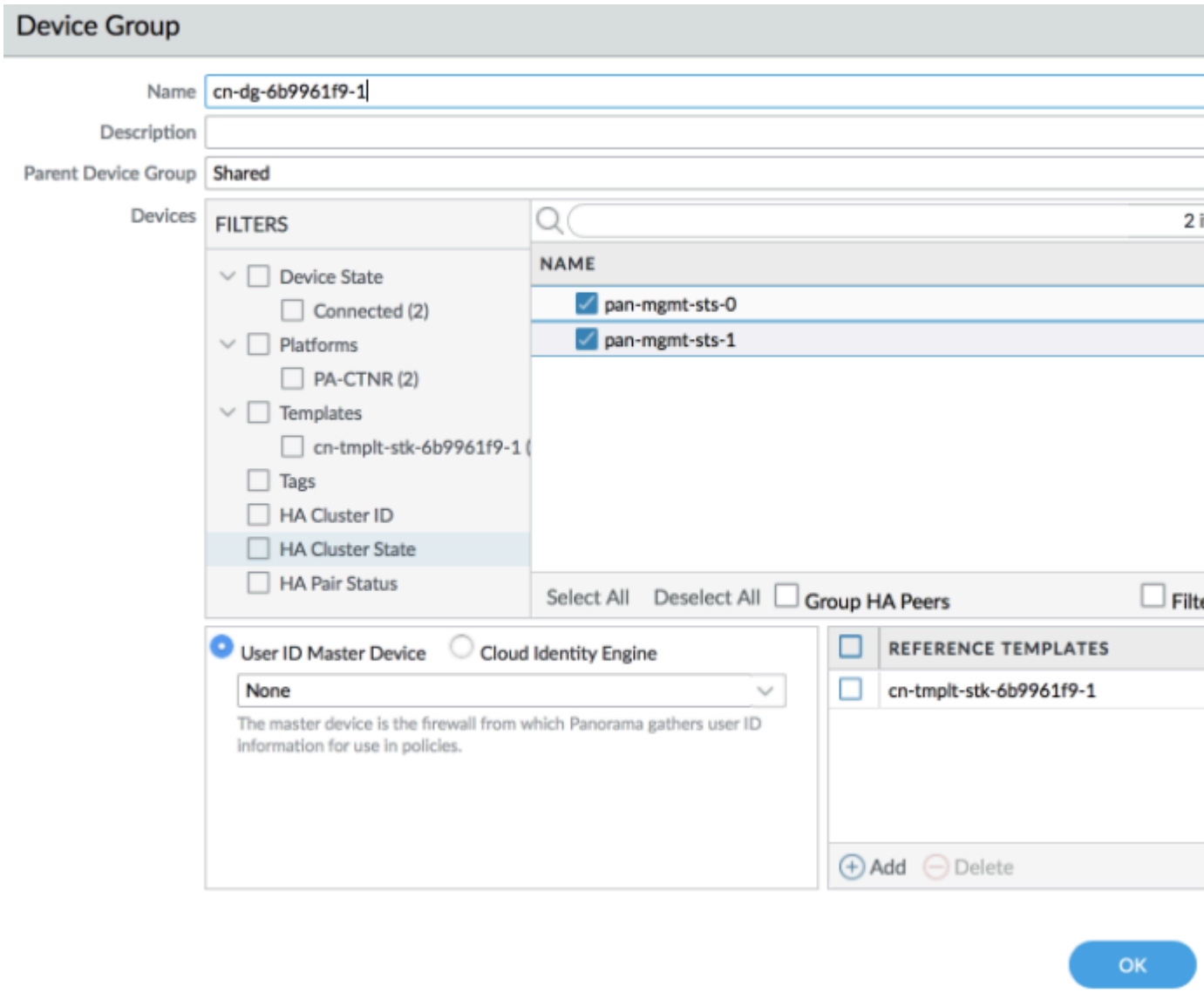
Para resolver, elimine la implementación de MP, elimine las PVC, los PV, vuelva a implementar mp-configmap, seguido de MP.

En caso de implementación utilizando el gráfico HELM:

Para resolver el problema, quite la implementación del gráfico HELM, elimine los PVC/PV de CN-series y, a continuación, vuelve a implementar el HELM.

Panorama no muestra MP como dispositivo gestionado

1. Asegúrese de que MP y DP estén en la misma versión de sw. “Los logs K8 en MP arrojarían logs de error si no están en la misma versión.
2. Si mgmt-slot-crd y mgmt-slot-cr.yaml están implementados.
3. Si este DP ha establecido IPSec en cualquiera de los MP (inicie sesión en MP usando raíz y compruebe con cmd “ipsec status” (estado de ipsec).
4. AutoCommit y CommitAll deberían haber transmitido el MP al que está conectado este DP. Si no, compruebe en MP por qué CommitAll o AutoCommit ha fallado y corrija en consecuencia. Consulte el paso anterior (MP falla al conectarse a Panorama o fallo de MP CommitAll) para resolver.
5. admin@pan-mgmt-sts-0> debug show internal interface all # debería mostrar la config de interfaz, si no lo hace, asegúrese de que se hace referencia a la pila de plantillas en el DG. Asegúrese también de que K8S-Network-template tenga la configuración de la interfaz.



6. Si DP tiene 4Gig de memoria (compruebe en ngfw.yaml).

7. Compruebe si el proceso Masterd all se está ejecutando mediante la ejecución del comando “masterd all status”.
8. “Ps-aef” comprueba el funcionamiento del proceso.
9. Compruebe el resultado del siguiente comando y verifique si se ven fallos en el registro de ranuras DP:

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


Fallo en el registro de DP Slot

1. Verifique que los pan-cn-mgmt-slot-cr y crd.yamls estén desplegados.
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: Not
 Ready. Panorama config is not pushed. pan_task is not running.
 11-21-2022 20:54:40.486734 UTC INFO: Strongswan daemon is up.
 Trying to reach Management Plane.. 11-21-2022 20:54:41.623966
 UTC INFO: Management Plane connectivity established. 11-21-2022
 20:54:42.700770 UTC ERROR: Registration/Re-registration failed:
 USER 11-21-2022 20:54:42.818729 UTC WARNING: dp slot register
 failed. Retrying a few times 11-21-2022 20:54:44.265372 UTC
 ERROR: Registration/Re-registration failed: USER 11-21-2022
 20:54:45.759982 UTC ERROR: Registration/Re-registration failed:
 USER 11-21-2022 20:54:47.256744 UTC ERROR: Registration/
Re-registration failed: USER 11-21-2022 20:54:48.768491 UTC
 ERROR: Registration/Re-registration failed: USER 11-21-2022
 20:54:50.272969 UTC ERROR: Registration/Re-registration failed:
 USER 11-21-2022 20:54:51.390138 UTC CRITICAL: Failed to register
 to MP. Shutting down DP
```


Los pods MP/DP/CNI no se muestran cuando hacemos “k8 get pods -n kube-system”

1. Verifique si posiblemente la ‘Service-account’ no se ha creado porque “sa.yaml” no se ha implementado.
2. Verifique que el servicio mp se esté ejecutando usando el comando “k8 -n kube-system get svc”
3. Verifique que mp stateful set se esté ejecutando usando el comando “k8 -n kube-system get sts” y k8n -n describe sts/pan-mgmt-sts # esto se imprimiría si hubiera algún problema con pvc/pv

El tráfico de los pods de aplicaciones seguras no se envía a través de DP/Cortafuegos

1. Verifique si todos los nodos trabajadores están funcionando con las versión 5.4 mín. del kernel (usando el comando “kubectl get nodes -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. (sólo para CNv2) Compruebe si la interfaz ‘vxlan’ se crea en el pod de la aplicación segura y si se crea una ruta predeterminada a través de esta interfaz 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. Verifique si los DP se están ejecutando y están conectados a MP usando IPSec, si los DP están activos/en ejecución, pero IPSec ha finalizado

4. Verifique si la licencia de DP falló después de 4 horas de inicio de DP debido a que no hay código de autenticación o el clúster no está conectado a panorama - k8 plugin

```
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. Verifique si el complemento auth-code on kubernets en Panorama no está caducado

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

   Suscripciones de seguridad: Wildfire, Threat Prevention, DNS, URL Filtering

   Tipo de código de autenticación: Créditos SW-NGFW

   Código de autenticación: D2962989

   Caducado: no

   Fecha de caducidad: 31 de diciembre de 2022

   vCPU emitidas: 50

   vCPU usadas: 0

   Fecha de emisión: 31 de diciembre de 2022

   admin@Panorama-49.88>

6. Verifique si ‘ngfw-svc.yaml' está implementado antes de que CNI.yaml y NGFW svc tengan ClusterIP y se estén ejecutando.

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. Compruebe los registros de CNI iniciando sesión en el nodo en /var/log/pan/pan-cni.log ([ec2-user@ip-12-12-12-184 ~]$ vi /var/log/pan-appinfo/pan-cni.log)
8. El pod de la aplicación se debería crear después de que CNI y ngfw svc se estén ejecutando; reiniciar el pod puede ayudar.
9. El pod de la aplicación se debería crear después de que CNI y ngfw svc se estén ejecutando; reiniciar el pod puede ayudar.
10. Verifique que la configuración de la interfaz se envía a DP mediante el comando “debug show internal interface all” en el pod de MP
11. “show rule-hit-count vsys vsys-name vsys1 rule-base security rules all” para ver qué regla de seguridad se está alcanzando y modifique la política de seguridad en consecuencia.

¿Cómo verificar qué módulo DP está procesando el tráfico?

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. En Panorama-> Monitor logs (Supervisar logs), añada la columna “Container ID” (ID de contenedor) y verá el ID del contenedor anterior.

Creación de logs: Panorama no muestra logs de tráfico/amenazas

Los siguientes son los pasos de resolución de problemas:

1. Verifique si se generan logs en el MP usando el comando “show log traffic/threat direction equal backward”. Si los logs no se ven en MP, compruebe si el mismo MP está procesando tráfico usando “show session all”, mientras envía ping continuo desde el pod seguro
2. Asegúrese de que DP tiene licencia mediante los comandos:
    1. En MP “solicitar plugins vm_series list-dp-pods”
    2. Los logs K8 en DP deberían confirmarlo.
3. “debug log-receiver statistics” mostrará la tasa de entrada de logs de DP a MP.
4. Verifique si el tráfico está alcanzando la política prevista configurada con el reenvío de logs, log-forwarding, mediante “show session all” y “show session id <id>”
5. Verifique si la configuración se recibe en MP mediante los comandos “show config pushed-shared-policy” y “show running security-policy”
6. Asegúrese de que los “managed collectors”, recopiladores gestionados, estén sincronizados y en un estado conectado en panorama.
7. “masterd elasticsearch status” en panorama # debería estar ejecutándose. Si no está ejecutándose, ejecute “es_restart.py -e”
8.
```
[root@cnsmokepanorama ~]# sdb cfg.es.* cfg.es.acache-update: 1
 cfg.es.enable: 0x0
```
9. salud de es_cluster.sh
10. “debug log-collector log-collection-stats show incoming-logs” en panorama
11. **pan_logquery -t traffic -i bwd -n 50**

Creación de logs: Panorama no muestra logs al filtrar con nombre de regla, rule-name

El problema puede ocurrir cuando Panorama falla al cargar correctamente las plantillas ES. Pruebe a reiniciar ES mediante el comando “es_restart.py -t” desde el modo raíz de Panorama. Envíe nuevos logs de tráfico y verifique que se vean los logs:

```
[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 no logra reconectarse a panorama

```
pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105): Este dispositivo
 o recopilador de logs o dispositivo wf (devid 892A1C93EF280D0) no se
 gestiona
```

El mensaje de error anterior significa que el dispositivo se está volviendo a registrar. Dado que se registró anteriormente, no está pasando por el flujo de trabajo de arranque donde se añade a si mismo a la configuración de panorama.

Esto podría suceder cuando el dispositivo se registró y conectó previamente, pero no se realizó una confirmación en panorama para guardar esa configuración, luego panorama se reinició o volvió a arrancar borrando la configuración, y cuando el dispositivo intenta conectarse, panorama no reconoce el dispositivo por lo que la conexión se corta.

Los siguientes son los logs de `configd.log` en panorama:

```
2021-02-03 11:48:00.436 -0800 Processing lcs-register message
 from device '8B1EB1ADC72B44E' 2021-02-03 11:48:00.436 -0800
 Warning: _get_current_cert(sc3_utils.c:84): sdb node 'cfg.ms.ak'
 does not exist. 2021-02-03 11:48:04.425 -0800 logbuffer:
 no active connection to cms0 2021-02-03 11:48:24.425 -0800
 logbuffer: no active connection to cms0 2021-02-03 11:48:44.425
 -0800 logbuffer: no active connection to cms0 2021-02-03
 11:48:57.751 -0800 Warning: sc3_register(sc3_register.c:90):
 SC3: Disabled - Ignoring register. 2021-02-03 11:48:57.752 -0800
 Warning: 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 Error:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105): This
 device or log collector or wf appliance (devid 892A1C93EF280D0)
 is not managed 2021-02-03 11:49:04.426 -0800 logbuffer:
 no active connection to cms0 2021-02-03 11:49:06.015 -0800
 Warning: sc3_register(sc3_register.c:90): SC3: Disabled -
 Ignoring register. 2021-02-03 11:49:06.015 -0800 Warning:
 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 Error:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105): Este dispositivo
 o recopilador de logs o aplicación wf
```


MP y DP están en estado activo y en ejecución, pero IPsec se ha finalizado entre MP y DP

Verifique los logs de kubectl en MP, vea si las ranuras se liberan después de 4 horas como a continuación:

```
(parts) root@test-virtual-machine:~# k8sys logs pan-mgmt-sts-0
 03-09-2021 01:07:36.508002 PST INFO: Management container starting
 running PanOS version 10.1.0-c182.dev_s_rel Starting PAN Software:
 03-09-2021 01:08:07.460287 PST WARNING: Readiness: Not Ready.
 slotd for Data Plane registration is not running. ipsec for Data
 Plane connections is not running. Failed to execute 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: Ready
 now. slotd for Data Plane registration is running. ipsec for Data
 Plane connections is running. 03-09-2021 01:10:54.558525 PST INFO:
 Strongswan daemon is up. 03-09-2021 01:10:56.286104 PST INFO:
 SW version matches, both MP and DP software versions are 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 version matches, both
 MP and DP software versions are 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:
 Installing license AutoFocus. 03-09-2021 01:12:02.362417 PST INFO:
 Installing license LoggingServices. 03-09-2021 05:13:01.521227
 PST INFO: SW version matches, both MP and DP software versions are
 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 version matches, both MP and DP software versions are
 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

Compruebe lo siguiente:

1. La imagen no está disponible en el repositorio o el nodo no tiene acceso al repositorio
2. x509: certificado firmado por una autoridad desconocida. Si es así, haga lo siguiente:

   añadir/modificar el archivo /etc/docker/daemon.json con repositorios privados:

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:~#
   ```

   Eventos:

   ```
    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: Get https://docker-
   panos-ctnr.af.paloaltonetworks.local/v2/: x509: certificate signed
    by unknown authority Warning Failed 23s (x3 over 63s) kubelet
    Error: ErrImagePull Warning DNSConfigForming 8s (x7 over 63s)
    kubelet Nameserver limits were exceeded, some nameservers have
    been omitted, the applied nameserver line is: 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$
   ```


   ```

# Iniciar sesión en DP desde el nodo de trabajo, worker-node, que se ejecuta en el espacio de nombres ns-panw

Vaya al directorio /var/log/pan-appinfo y ejecute el comando **cat pan-cmdmap** y copie el log para iniciar sesión en DP en el espacio de nombres 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 /]# —------>>>>>
```

Puede iniciar sesión en DP y puede ejecutar el estado masterd all desde aquí.

Los pods DP permanecen en el estado **ContainerCreating** con los siguientes logs de kubectl

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

Falló de la comprobación del tipo hostPath: **/var/log/pan-appinfo/pan-cni-ready** no es un directorio

```
Eventos: 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$
```

Solución:

1. Verifique el log de Kubectl de pan-cni. Asegure multus vs no multus, corrija yaml implementado.
2. Si multus está implementado, deshaga implementación de multus y elimine el directorio 00-multus.conf de /etc/cni/net.d/. Seguido de la retirada de la implementación y vuelta a implementar de CNI y PD

A continuación logs k8 en pan-cni muestran que se detecta multus. Por lo tanto, los pasos anteriores se deberían seguir.

```
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:
 Using CNI config template from CNI_NETWORK_CONFIG environment
 variable. 09-29-2021 04:07:22.633416 UTC DEBUG: Removing existing
 binaries 09-29-2021 04:07:22.731559 UTC DEBUG: Wrote PAN CNI
 binaries to /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: CNI que se
 ejecuta en modo de servicio de FW. Bypassfirewall can be enabled on
 application pods 09-29-2021 04:07:22.796082 UTC CRITICAL: Detected
 Multus as primary CNI (CONF file 00-multus.conf); waiting for
 non-multus CNI to become primary CNI. test@msatane-182:~/results/
job_vm_series_72342/cn-sanity/cntr_deploy/kube-system$
```


Estado del enlace en pod de aplicación protegido por CNv2 (mediante vxlan)

Muestra enlace de IP 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:/#

Capture Techsupport de MP

En MP:

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. Inicie sesión en la raíz de MP para copiar el nombre TSF almacenado en

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

   Contenedor predeterminado "pan-mgmt" de: 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. Copie el TSF desde el MP al controlador local usando

   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 no funciona

1. Verificar “k8sys get hpa” y “k8sys describe hpa”
2. Verifique la herramienta de supervisión (cloudwatch/GCP stackdriver/Azure App Insights) para ver si se ven las métricas personalizadas.
3. Verifique si /var/log/pan/pan_vm_plugin.log tiene errores si no se ven métricas personalizadas en la herramienta de supervisión

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

   NOMBRE ESTADO LISTO REINICIOS ANTIGÜEDAD

   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

¿Cómo controlar - Acceso entrante a aplicaciones en OpenShift?

Para el acceso entrante a las aplicaciones:

1. Haga que el cliente habilite la protección para haproxy/router mediante la anotación en los archivos yaml. Esto garantizará que todo el tráfico que entra y sale del haproxy pase por el CN-Series.
2. Pídales que usen las reglas personalizadas basadas en URL (destino) con las IP de origen para hacer cumplir quién puede acceder a una aplicación determinada. Las URL personalizadas (como osecluster/payments) se deberán definir para los endpoints de las aplicaciones. Esto les permitirá permitir o denegar el acceso a estas aplicaciones sin tener que preocuparse por el NAT.
3. Si están usando un balanceador de carga externo (p. ej., F5) frente al clúster OSE, podrían usar el encabezado XFF para imponer un mayor detalle sobre quién puede tener acceso a una aplicación determinada.

Retirar la implementación de CN-series

Ejecute los siguientes comandos:

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. Elimine los PVC:

   kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts
5. kubectl delete -f . # quita la implementación de todos los objetos definidos en los yamls en ese directorio

   (ESTO LO DESHACE TODO!!)

Habilitar packet-diag en CN

1. Ejecute en el pod de MP al que pertenece el pod de DP específico que inspecciona el tráfico desde el pod de la aplicación.
2. Ejecute el siguiente comando:

```
> 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. Después de capturar el paquete, busque el archivo en:

   /opt/panlogs/session/pan/filters/

IPSec entre MP y DP fallan con error de estado asimétrico

Esto puede ocurrir en las siguientes situaciones:

1. MP y DP están en diferentes versiones de PanOS
2. “pan-cn-mgmt-slot-crd.yaml” and pan-cn-mgmt-slot-cr.yaml” no están implementados.

```
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
```


Las cápsulas de aplicaciones fallan en la resolución DNS (independientemente de su tiene cortafuegos o no)

Verifique lo siguiente:

1. Compruebe que los pods DNS se están ejecutando: “kubectl get pods --namespace=kube-system -l k8s-app=kube-dns”
2. Comprueba que se está ejecutando el servicio DNS: “kubectl get svc --namespace=kube-system”
3. Si el servicio DNS no se está ejecutando, exponga la implementación DNS como svc o use el yaml e implemente.
4. Una vez implementado SVC, verifique que los endpoints estén expuestos correctamente. “kubectl get endpoints coredns --namespace=kube-system”
5. Vuelva a implementar los pods de aplicaciones.

