paloalto TECHDOCS

CN-Series 故障排除

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 故障排除

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama

表 **1:** 术语定义：

术语	定义
MP	CN-MGMT
DP	CN-NGFW

连接到 MP 或 DP

运行以下命令可了解您的 MP 或 DP Pod 名称：

kubectl get pods -n=<namespace>

运行以下命令可连接到 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 无法拉取映像，并且包含错误

x509：由未知授权机构签名的证书（主要出现在本机/本地 **k8** 集群中）

在所有工作节点上，使用从中提取的映像存储库更新 **/etc/docker/daemon.json**。如果不存在，则创建一个 daemon.json 文件

```
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"** 重新启动 Docker。

MP 处于“待处理”状态

验证以下内容：

1. 所需的资源（节点/内存/CPU）可用于 MP。我们可以通过检查命令输出来验证这一点：

   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. PersistentVolume (PV) 是集群中的一段存储空间，由服务器/存储/集群管理员配置或使用存储类动态配置。它是集群中的资源，就像节点一样。PersistentVolumeClaim (PVC) 是用户提出的存储请求，可以从 PV 中获得。

   PVC 绑定到 PV (`kubectl -n kube-system get pvc`)。如果不是，请使用以下命令删除旧 PVC：

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

3. 检查是否在至少 2 个工作节点上为本地设置创建了所有必需的目录（/mnt 下的 pan-local1、pan-local2、pan-local3、pan-local4、pan-local5、pan-local6）。

   动态卷配置不需要 */mnt* 下的 *pan-local1*、*pan-local2*、*pan-local3*、*pan-local4*、*pan-local5*、*pan-local6*。*AWS EKS* 上缺少 *EBS CSI* 驱动程序是 *MP* 处于待处理状态的原因之一。您必须确保在集群中启用 *EBS CSI* 驱动程序，检查角色并确定集群的提供商。有关更多信息，请参阅将 Amazon EBS CSI 驱动程序作为 Amazon EKS 插件进行管理。

4. 如果错误是“`pan-mgmt-sts-0`”：Pod 已立即接触绑定 PersistentVolumeClaims” exec “**kubectl get pvcs -o wide**” 和 “**kubectl get pv -o wide**”。这应该显示哪些 pvc 绑定失败。

   解决方案是使用命令 **kubectl-n kube-system delete pvc/<pvc-name>** 删除旧的 PVC 或进行清理。删除所有的 PVC、PV。部署新的 PV 并部署 MP。

5. 如果出现下面的错误 **"k8 describe pod <mp-pod>"**，请确保已创建 PV。如果没有，请部署 pan-cn-pv-local.yaml（使用配置目录的节点名称）

   Pod ""**pan-mgmt-sts-0**"" 的 **"VolumeBinding"** 过滤器插件：Pod 已取消绑定 PersistentVolumeClaims

   Warning FailedScheduling <unknown> default-scheduler running **"VolumeBinding"** filter plugin for pod ""**pan-mgmt-sts-0**""：Pod 已取消绑定 PersistentVolumeClaims

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:Management container starting
    running PanOS version 10.1.3-c47
   ```

   12-22-2021 11:34:41.335521 PST ERROR:无法启动 **pansw：2**

   问题可能是 “**pan-cn-mgmt-configmap.yaml**” 没有强制值。
   ```

MP 一直崩溃

登录 MP 根目录并导航至 **/var/cores** 以查看崩溃的进程。

K8 MP 日志显示以下错误

设备注册请求失败：无法向 **CSP** 服务器发送请求

验证以下内容：

1. “Pan-cn-MGMT-Secret.YAML”的以下 2 个字段应该有正确的值 CN-SERIES-AUTO-REGISTRATION-PIN-ID："<PIN Id>"

   CN-SERIES-AUTO-REGISTRATION-PIN-VALUE："<PIN-Value>"
2. 如果以上值正确，请确保 CSP 的 PINID 和值未过期

MP 无法连接到 Panorama 或 MP CommitAll 失败

1. 验证 MP 可以访问/Ping Panorama IP。对于公有云，请确保已配置所需的安全策略，以启用 Panorama 和 K8 集群之间的可访问性

   登录 MP：

   - 1. Kubectl -n kube-system exec -it <mp-pod-name> -- su admin
     2. “Show panorama status”以获取 Panorama IP 地址
     3. Ping 主机 <panorama-ip>
     4. 如果 Ping 有效，请继续进行以下验证
2. 验证 Panorama 上有在 mgmt-secret.yaml 中提供的“bootstrap-auth-key”且未过期。
   1. 要验证 bootstrap-auth-key，请登录 Panorama 并执行命令 “request bootstrap vm-auth-key show”→ 这应该是有效的（未过期）
   2. 如果不可用，请使用“request bootstrap vm-auth-key generate lifetime 8760”生成，然后在 pan-mgmt-secret.yaml 中更新。取消部署所有 yaml，清除 PV、PVC 并重新部署。
3. 验证在 mgmt-configmap.yaml 中配置的 DG、TS 和 Collector 组 (CG) 是否有拼写错误，并在 Panorama 上配置和提交。
4. 验证在 mgmt.yaml 之前部署的 pan-mgmt-configmap 和 secret yaml。
5. 通过执行命令“show jobs all”和“show job id <id>，检查 MP 上 Panorama 的 commit-all 是否成功，从而查看失败的提交并修复 Panorama 上的配置，然后重新执行“Commit All/Force”。
6. Panorama 配置已在 MP 上推送“show config pushed-shared-policy”
7. 输入命令“调试 tac-login 响应”，然后使用 MP 序列号进行搜索，在 Panorama 上的根目录中查找 configd.log。它应该会提供连接失败的原因。

   vi /var/log/pan/configd.log

   示例：

```
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):Failed
 to find vm_auth_key 923688689426978, vm_auth _key invalid
```

Commit All 无法在 MP 上启动

在 Panorama 上验证 Commit All 任务是否处于“Stuck/ACT”状态。

这可能是由于 MP 和 Panorama 之间的网络连接问题而发生的。

在实验室中，通过将 MP/Worker-Node 和 Panorama 置于同一个子网中，可以解决此问题。

如果遇到上述问题，可以看到下面的 Panorama 日志。

```
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
```

DP Pod 处于“待处理”或“正在创建容器”状态

运行以下命令并验证相应命令的输出中提到的错误，并修复错误

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

   如果以下错误被视为上述命令的一部分，请继续查找 CNI 日志，以及 CNI 是否在使用 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 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. 如果 kubectl CNI 日志如下所示，请确保 CNI 正在每个节点上运行。（在 GKE 集群上，我们需要启用网络策略才能运行默认 CNI）：

   ```
   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 running in FW Service
    mode.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#
   ```

   如果出现上述错误，请尝试取消部署 Multus 并从部署此 CNI 和 DP 的工作节点中删除 00-multus.conf 文件

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

MP：未显示 Panorama 详细信息/状态

```
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 可能在 pan-cn-mgmt.yaml 之后显示
2. pan-cn-mgmt-secret 可能部署失败（可能是因为 bootstrap-auth-key 以“0”开头）→ 从 Panorama 中删除并重新创建身份验证密钥，以确保它不是以“0”开头

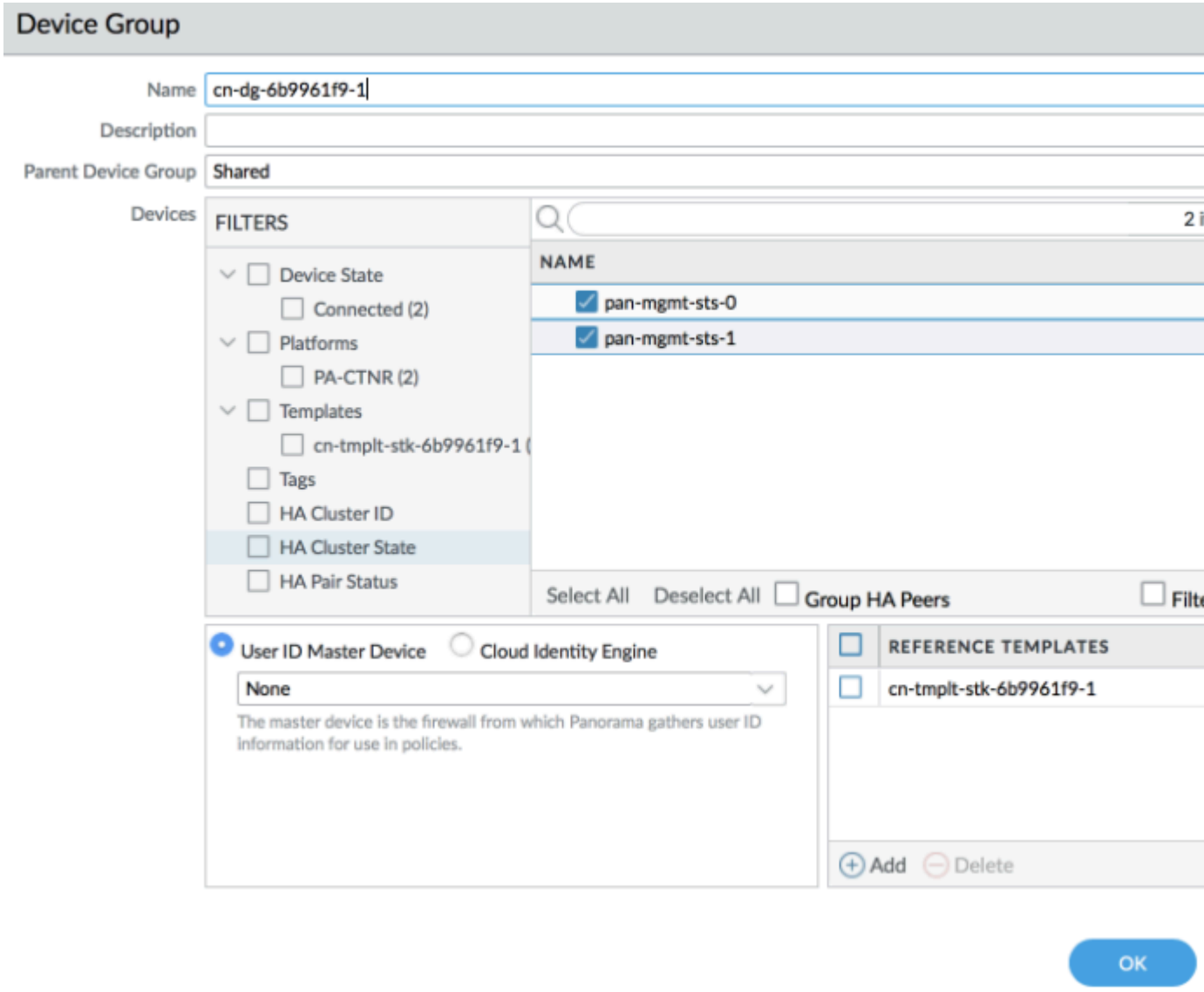
要解决问题，请取消部署 MP，删除 PVC、PV，重新部署 mp-configmap，然后再重新部署 MP。

如果使用 HELM 图表进行部署：

要解决此问题，请取消部署 HELM 图表，删除 CN-Series PVCS/PV，然后重新部署 HELM。

Panorama 未将 MP 显示为托管设备

1. 确保 MP 和 DP 的软件版本相同。“如果版本不同，MP 上的 K8 日志可能会抛出错误日志。
2. 如果部署了 mgmt-slot-crd 和 mgmt-slot-cr.yaml。
3. 如果此 DP 已与任何 MP 建立 IPsec（使用 root 登录到 MP），然后使用命令检查“ipsec 状态”。
4. AutoCommit 和 CommitAll 应该已经传递了此 DP 所连接的 MP。如果不是，请在 MP 上查看 CommitAll 或 AutoCommit 失败的原因，并进行相应的修复。请参考上述步骤（MP 无法连接到 Panorama 或 MP CommitAll 故障）来解决。
5. admin@pan-mgmt-sts-0> debug show internal interface all → 应显示接口配置，如果没有，请确保 DG 中引用了模板堆栈。还要确保 K8S-Network-template 具有接口配置。



6. 如果 DP 有 4Gig 内存（在 ngfw.yaml 中查看）

7. 通过运行“masterd all status”命令来运行所有 Masterd 进程。
8. “ps-aef”检查进程是否正常。
9. 检查以下命令的输出并验证是否出现 DP 插槽注册失败：

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

DP 插槽注册失败

1. 验证 pan-cn-mgmt-slot-cr 和 crd.yamls 已部署。
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.关闭 DP
```

当我们执行“k8 get pods -n kube-system”时，MP/DP/CNI Pod 不显示

1. 验证是否未创建“Service-account”，因为未部署“sa.yaml”。
2. 使用命令“k8 -n kube-system get svc”验证 mp 服务是否正在运行
3. 使用命令“k8-n kube-system get sts”和 k8n -n describe sts/pan-mgmt-sts 来验证 mp 状态集是否正在运行 → 如果 pvc/pv 出现任何问题，则会打印出来

来自安全应用 Pod 的流量未通过 DP/防火墙发送

1. 验证所有工作节点是否都在运行最低的 5.4 内核版本（使用命令“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. （仅适用于 CNv2）验证是否已在安全应用 Pod 上创建“vxlan”接口，以及是否已通过此 vxlan 接口创建默认路由

```
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. 验证 DP 是否正在运行并使用 IPsec 连接到 MP，DP 是否处于活动/运行状态，但是 IPsec 已终止

4. 验证 DP 启动 4 小时后是否因为没有验证码或集群未连接到 Panorama-k8 插件而失败

```
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. 验证 Panorama 中 Kubernets 插件的身份验证代码是否未过期

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

   安全订阅：Wildfire、威胁防御、DNS、URL 过滤

   身份验证代码类型：SW-NGFW 积分

   身份验证代码：D2962989

   过期：否

   到期日期：2022 年 12 月 31 日

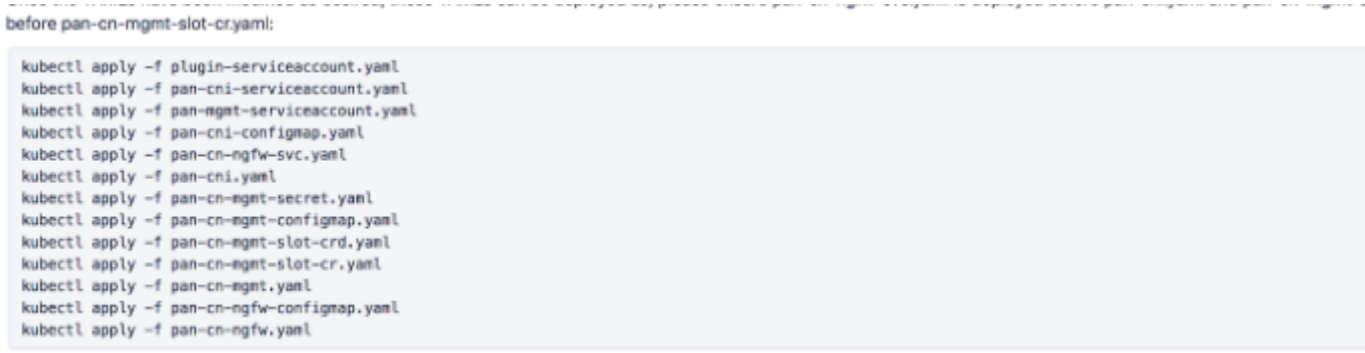
   发行的 vCPU：50

   使用的 vCPU：0

   发行日期：2022 年 12 月 31 日

   admin@Panorama-49.88>

6. 验证“ngfw-svc.yaml”是否在 CNI.yaml 文件之前部署，以及 ngfw svc 是否具有 ClusterIP 且正在运行。


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. 登录 /var/log/pan/pan-cni.log 下的节点以查看 CNI 日志 ([ec2-user@ip-12-12-12-184 ~]$ vi /var/log/pan-appinfo/pan-cni.log)
8. 应用 Pod 应在 CNI 和 ngfw svc 运行后创建 - 重启 Pod 会有帮助
9. 应用 Pod 应在 CNI 和 ngfw svc 运行后创建 - 重启 Pod 会有帮助
10. 在 MP Pod 上使用“debug show internateal all”命令检查接口配置是否已推送到 DP
11. “show rule-hit-count vsys vsys-name vsys1 rule-base security rules all”以查看匹配的安全规则并相应地修改安全策略。

如何验证哪个 DP Pod 正在处理流量

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 上转到“监控日志”，然后添加“容器 ID”列，您会看到上述容器 ID。

日志记录：Panorama 未显示流量/威胁日志

下面是故障排除步骤：

1. 使用命令“show log traffic/threat direction equal backward”验证是否在 MP 上生成日志。如果在 MP 上看不到日志，则使用“show session all”来验证同一 MP 是否正在处理流量，同时从安全 Pod 发送持续的 Ping 信号
2. 使用以下命令确保 DP 已获得许可：
    1. 在 MP 上“request plugins vm_series list-dp-pods”
    2. DP 上的 K8 日志应该证实了这一点。
3. “debug log-receiver statistics”将显示从 DP 到 MP 的日志传入速率。
4. 检查流量是否符合使用“show session all”和“show session id <id>”的日志转发配置的预期策略
5. 检查是否已在运行命令“show config pushed-shared-policy”和“show running security-policy”的 MP 上收到配置。
6. 确保“托管收集器”已在 Panorama 上同步且处于连接状态。
7. 在 Panorama 上运行命令“masterd elasticsearch status”→ 它应该正在运行。如果未运行，请执行“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. 在 Panorama 上运行“debug log-collector log-collection-stats show incoming-logs”
11. **pan_logquery -t traffic -i bwd -n 50**
   ```

日志记录：使用 rule-name 筛选时，Panorama 不显示日志

当 Panorama 无法正确加载 ES 模板时，可能会出现问题。尝试通过命令“es_restart.py-t”从 Panorama 根模式重启 ES。发送新的流量/日志并验证是否看到日志：

```
[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 无法重新连接到 Panorama

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

上述错误消息表示设备正在重新注册。由于它之前已注册过，因此它没有通过引导工作流程将自己添加到 Panorama 配置中。

如果设备先前已注册和连接过，但未在 Panorama 上进行提交以保存配置，然后 Panorama 重新启动或重新引导，清除配置时，可能会发生这种情况；当设备尝试连接时，Panorama 无法识别该设备，因此连接被切断。

以下是 Panorama 上来自 `configd.log` 的日志：

```
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):This device or
 log collector or wf app
```

MP 和 DP 处于活动状态和运行状态，但是 IPsec 在 MP 和 DP 之间终止

验证 MP 上的 kubectl 日志，查看插槽是否在 4 小时后被释放，如下所示：

```
(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

检查以下内容：

1. 影响在存储库上不可用或节点无法访问存储库
2. x509：证书由未知证书签发机构签名...如果是这样，请执行以下操作：

   使用专用存储库添加/修改文件 /etc/docker/daemon.json：

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:~#
   ```

   :

   ```
    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$
   ```
   ```

从在 ns-panw 命名空间中运行的工作节点登录到 DP

导航到 /var/log/pan-appinfo 目录并运行命令 **cat pan-cmdmap**，同时将日志复制到 nspan-fw 命名空间中的 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 /]# —------>>>>>
```

您可以登录到 DP 并从该处运行 masterd all status。

DP Pod 保持 **ContainerCreating** 状态，并具有以下 kubectl 日志

卷“**pan-cni-ready**”的“**MountVolume.SetUp**”失败

hostPath 类型检查失败：**/var/log/pan-appinfo/pan-cni-ready** 不是目录

```
Events: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$
```

解决方案：

1. 查看 pan-cni Pod 的 kubectl 日志。确保 Multus 与非 Multus，正确部署 yaml。
2. 如果已部署 Multus，请取消部署 Multus 并从 /etc/cni/net.d/ 目录中删除 00-multus.conf。其次是取消部署并重新部署 CNI 和 DP

下面 pan-cni 上的 k8 日志显示已检测到 Multus。因此，应遵循上述步骤。

```
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 running in
 FW Service mode.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$
```

应用 Pod 上的链路状态由 CNv2 提供安全保护（使用 vxlan）

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:/#

获取 MP 的技术支持

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. 登录 MP 根目录以复制存储在以下位置的 TSF 名称

   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. 使用以下命令将 TSF 从 MP 复制到本地控制器

   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 无法运行

1. 验证“k8sys get hpa”和“k8sys describe hpa”
2. 验证监控工具 (cloudwatch/GCP stackdriver/Azure App Insights)，看看是否可以看到自定义指标。
3. 如果看不到监控工具上的自定义指标，请验证 /var/log/pan/pan_vm_plugin.log 是否存在任何错误

   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 上应用的入站访问权限？

对于应用的入站访问权限：

1. 让客户使用 yaml 文件中的注解启用对 haproxy/router 的保护。这将确保所有进出 HAProxy 的流量都会通过 CN 系列。
2. 让客户在源 IP 中使用基于 URL 的自定义规则（目标）来强制执行允许谁访问指定应用程序。需要为应用程序的端点定义自定义网址（例如 osecluster/payments）。这样，他们就可以允许/拒绝访问这些应用程序，而不必担心 NAT。
3. 如果客户在 OSE 集群前使用外部负载均衡器（例如 F5），则客户应使用 XFF 标头进一步详细设置允许谁访问指定应用程序。

取消部署 CN-Series

运行以下命令：

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. 删除 PVC：

   kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts
5. kubectl delete -f . → 取消部署在该目录下的 yaml 中定义的所有对象

   （这摧毁了一切##）

在 CN 上启用数据包诊断

1. 执行到 MP Pod 中，特定 DP Pod 会检查来自应用 Pod 的流量。
2. 执行以下命令：

```
> 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. 捕获数据包后，在下面找到该文件：

   /opt/panlogs/session/pan/filters/

MP 和 DP 之间的 IPsec 失败，出现错误不对称状态

这可能发生在以下情况下：

1. MP 和 DP 使用不同的 PanOS 版本
2. “pan-cn-mgmt-slot-crd.yaml” and pan-cn-mgmt-slot-cr.yaml” are not deployed.

```
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
```

应用 Pod 无法通过 DNS 解析（无论其是否已设置防火墙）

验证以下内容：

1. 检查 DNS Pod 是否在运行：“kubectl get pods --namespace=kube-system -l k8s-app=kube-dns”
2. 检查 DNS 服务是否正在运行：“kubectl get svc --namespace=kube-system”
3. 如果 DNS 服务未运行，请将 DNS 部署公开为 svc 或使用 yaml 进行部署。
4. 部署 SVC 后，验证端点是否已正确公开。“kubectl get endpoints coredns --namespace=kube-system”
5. 重新部署应用 Pod。