paloalto TECHDOCS

CN 系列 HSF 部署

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 系列 HSF

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

Palo Alto Networks **CN** 系列超大规模安全结构 (HSF) 1.0 是新一代容器化防火墙集群，可为部署 5G 网络的移动服务提供商提供高度可扩展且具有弹性的新一代防火墙解决方案。

CN 系列 HSF 解决方案提供：

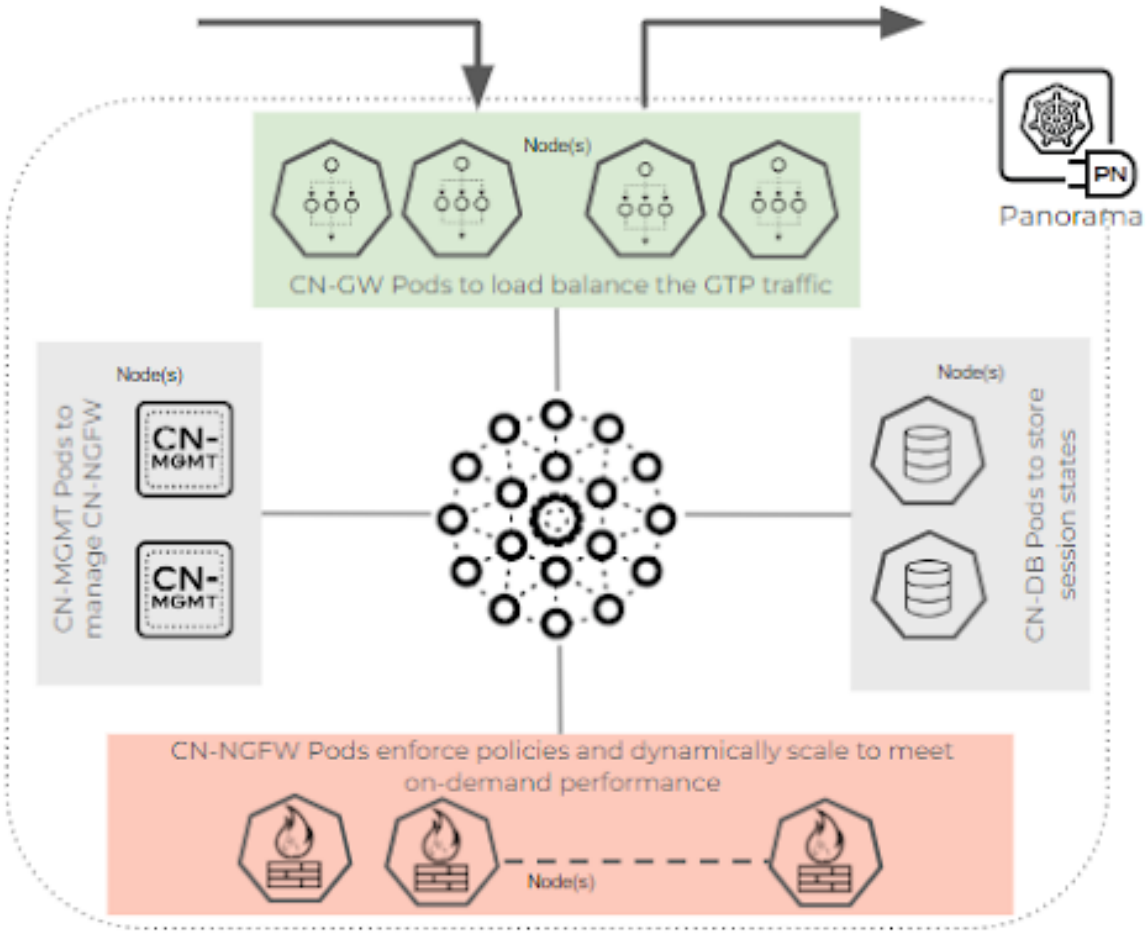
- 容器化 **NGFW** 实现的高度可扩展性：按需水平扩展 AppID 和 GTP 性能。
- 高可用性和弹性：提供弹性集群，该集群根据吞吐量和预期的会话动态运行，并保证跨工作负载的业务连续性和会话弹性。
- 消除对外部负载均衡器的依赖：提供可通过 Panorama 插件完全编排的易于部署和 DevOps 友好的环境。

CN 系列 HSF 解决方案可部署在 RedHat Openshift（内部部署）或 AWS EKS 公共云托管的 Kubernetes 环境中。

CN 系列 HSF 架构

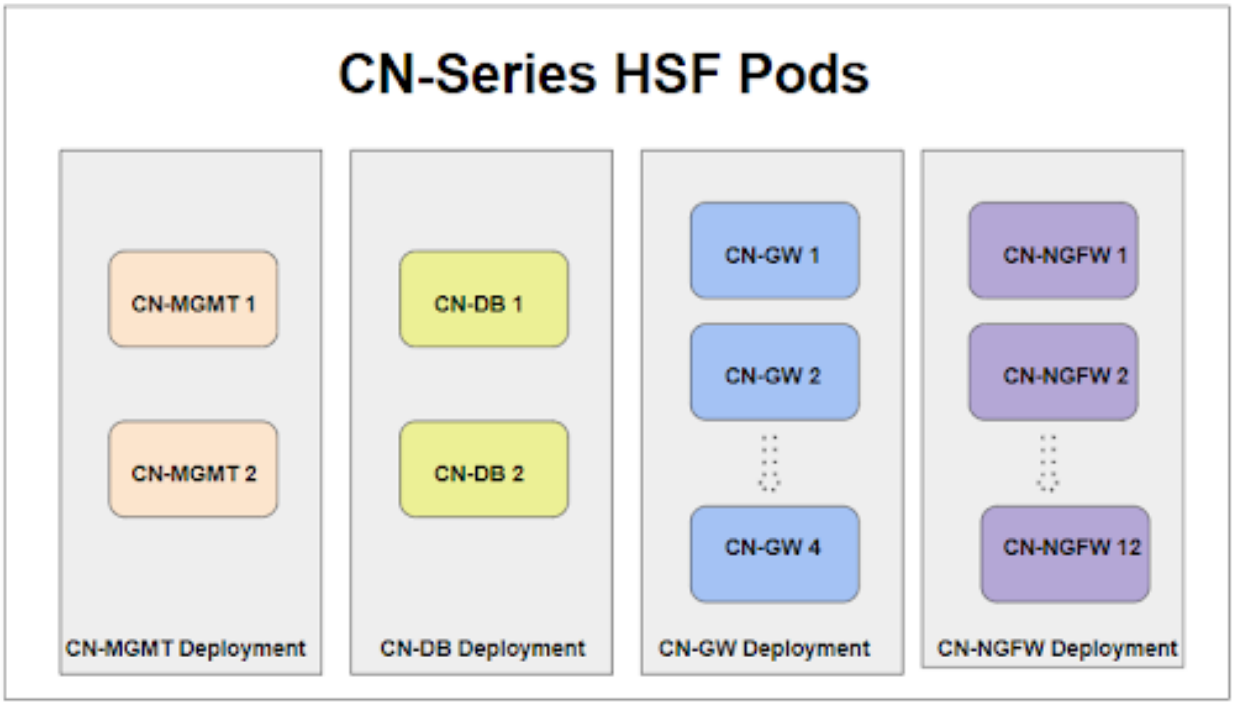
在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

CN 系列 HSF 集群由通过内部网络连接的 CN-MGMT（管理）、CN-NGFW（数据平面）、CN-GW（网关）和 CN-DB（数据库）Pod 池组成。CN-MGMT Pod 提供集群管理平面功能。CN-NGFW Pod 提供集群数据平面安全功能。CN-GW Pod 是集群的入口点，并在 CN-NGFW Pod 之间分配流量。CN-DB Pod 提供 CN-NGFW Pod 使用的中心集群会话缓存。



CN 系列 HSF 支持两个提供冗余和可用性的 CN-MGMT 容器。但是，两个 CN-MGMT 容器中只有一个可以接受来自 CN-NGFW DP 的连接。连接的 CN-MGMT 将作为 StatefulSet 服务运行，以允许

CN-NGFW 仅连接到活动的 CN-MGMT。另一个 CN-MGMT 容器不会连接到 CN-NGFW 容器，除非当前 CN-MGMT 连接失败。



Pod 的类型

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

CN 系列 HSF 中有 3 种类型的数据平面 Pod，它们都使用相同的数据平面 Pod 映像，但会有不同的配置映射选项。CN 系列 HSF 托管两个管理 Pod。

CN-GW Pod — CN-GW Pod 是一种数据平面 Pod，它可以访问外部网络流量并管理入口和出口流量的负载平衡。外部节点将只知道 CN-GW Pod、它们的 IP，并且所有用于流量的数据子网都通过 Multus 接口连接到这些 Pod。CN 系列 HSF 1.0 支持最少 2 个和最多 4 个 CN-GW Pod。在 HSF 集群部署的生命周期之前，CN-GW Pod 是静态规模的。例如，如果最初有 2 个 GW Pod，并且您希望横向扩展，而 CN-NGFW Pod 可以动态横向扩展，则必须重新部署具有额外数量的 CN-GW Pod 的 HSF 集群。

CN-DB Pod — CN-DB Pod 是一种数据平面 Pod，可以跨 CN-NGFW Pod 查询会话/流量所有权。CN-DB 支持基于不同的算法将会话分发到不同的 CN-NGFW，例如 ingress-slot、round-robin

和 session-load。CN 系列 HSF 支持两个 CN-DB Pod，并且在两个 CN-DB Pod 之间复制会话信息，流量的查找/绑定上可以运行这两个 CN-DB Pod 中的任何一个。

CN-NGFW Pod — CN-NGFW Pod 处理 C 和 U 会话的实际流量，应用安全策略，并允许单独扩展 CN-NGFW Pod。CN 系列 HSF 1.0 支持最少 2 个和最多 12 个 CN-NGFW Pod。

CN-MGMT Pod — 所有 NGFW Pod（CN-GW、CN-DB 和 CN-NGFW）都通过 eth0 上的 IPsec 连接到单个 CN-MGMT Pod。

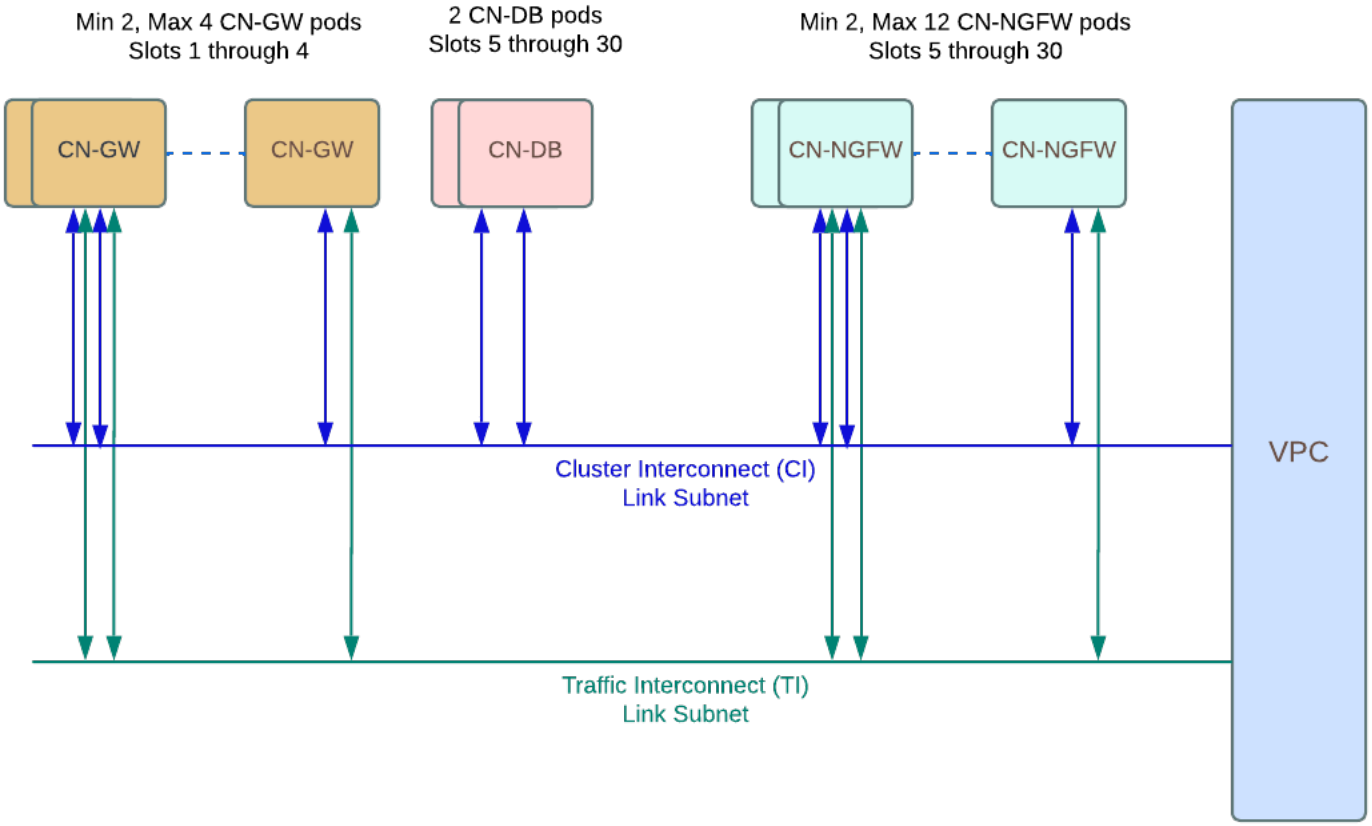
互连链路

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

所有 CN-GW、CN-DB 和 CN-NGFW Pod 都将通过集群互连 (CI) 链路（Multus 接口）相互连接。CI 链路是为集群成员之间的集群通信和转发数据包保留的数据端口。Ethernet x/1 用于所有相关 Pod 上的 CI 链路。CI 链路还可用于将流量从一个 CN-NGFW 转发到另一个。

CN-GW 和 CN-NGFW Pod 通过流量互连 (TI) 链路（Multus 接口）相互连接。TI 链路是为集群的内部流量保留的数据端口。以太网 x/2 用于所有相关 Pod 上的 TI 链路。

在 CN-GW Pod 上，以太网 x/3 以后将用作连接到客户网络的外部接口。



CN 系列 *HSF* 仅支持 *IPv4* 协议。

对于本地环境，需要 *DHCP* 服务器或 *IPAM* 来为 *CI* 和 *TI* 接口分配 *IP* 地址。对于 *AWS EKS*，*DHCP* 服务器是底层基础设施的一部分。因此，*IP* 地址会自动分配给云环境中的 *CI* 和 *TI* 接口。

为 CN 系列 HSF 授予许可

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

CN 系列防火墙许可由 Panorama 上的 Kubernetes 插件管理。CN 系列防火墙的许可基于部署在 Kubernetes 环境中的 CN-NGFW、CN-GW 和 CN-DB 使用的 vCPU（核心）总数。每个使用 CN-NGFW 的 vCPU 消耗一个令牌。

- 激活积分
- 创建 CN 系列 HSF 部署配置文件
- 管理部署配置文件

激活积分

在何处可以使用？	需要提供什么？
• CN-Series	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • Helm 3.6 or above version client

在贵组织内，您可以创建多个帐户，每个帐户都有不同的用途。在激活过程中，您只能为每个默认积分池选择一个帐户。一旦积分池处于活动状态，则授予积分管理员角色的用户就可以为部署分配积分，甚至可以将积分传输到其他积分池。

如果您有现有 CSP 帐户并且是超级用户或管理员，系统会自动将积分管理员角色添加到您的配置文件中。如果您没有现有帐户，CSP 会自动为您创建一个帐户，并将积分管理员角色添加到您的配置文件中。

您（购买者）会收到一封电子邮件，其中详细说明了订阅、积分池 ID、订阅的开始和结束日期、购买的积分金额以及默认积分池（激活积分时创建的积分池）的描述。

保护此电子邮件以备将来参考。

STEP 1 | 在电子邮件中，单击 **Start Activation**（开始激活）以查看可用的积分池。

STEP 2 | 选择要激活的积分池。您可以使用搜索字段按帐号或用户名筛选帐户列表。

如果您已购买多个积分池，系统会自动将其选定。复选标记表示登录积分的激活链接。

系统会提示您进行身份验证或登录。

如果您取消选择积分池，您会看到一个提醒，提示您如果要激活这些积分，则必须返回电子邮件并单击 ***Start Activation***（开始激活）链接。

STEP 3 | 选择 **Start Activation**（开始激活）。

STEP 4 | 选择支持帐户（您可以按帐号或姓名进行搜索）。

STEP 5 | 选择默认积分池。

STEP 6 | 选择 **Deposit Credits**（存款积分）。

您会看到一条提示存款成功的消息。

STEP 7 | （可选）如果这是您第一次激活积分，则系统会显示 Create Deployment Profile（创建部署配置文件）对话框。

创建 CN 系列 HSF 部署配置文件

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • 运行 PAN-OS 11.0.x 或更高版本的 Panorama

按照以下过程创建 CN 系列部署配置文件。

STEP 1 | 如果您已有积分池，请登录帐户，然后从指示板中选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分） > **Prisma NGFW Credits**（**Prisma NGFW** 积分） > **Create New Profile**（新建配置文件）。

如果您刚才已激活积分池，则会看到 **Create Deployment Profile**（创建部署配置文件）表单。

1. 选择 **CN-Series**（**CN** 系列）防火墙类型。
2. 选择 **PAN OS 11.0**。
3. 单击 **Next**（下一步）。

STEP 2 | CN 系列配置文件。

1. **Profile Name**（配置文件名称）。

   为配置文件命名。

2. 总 **vCPU** 数量

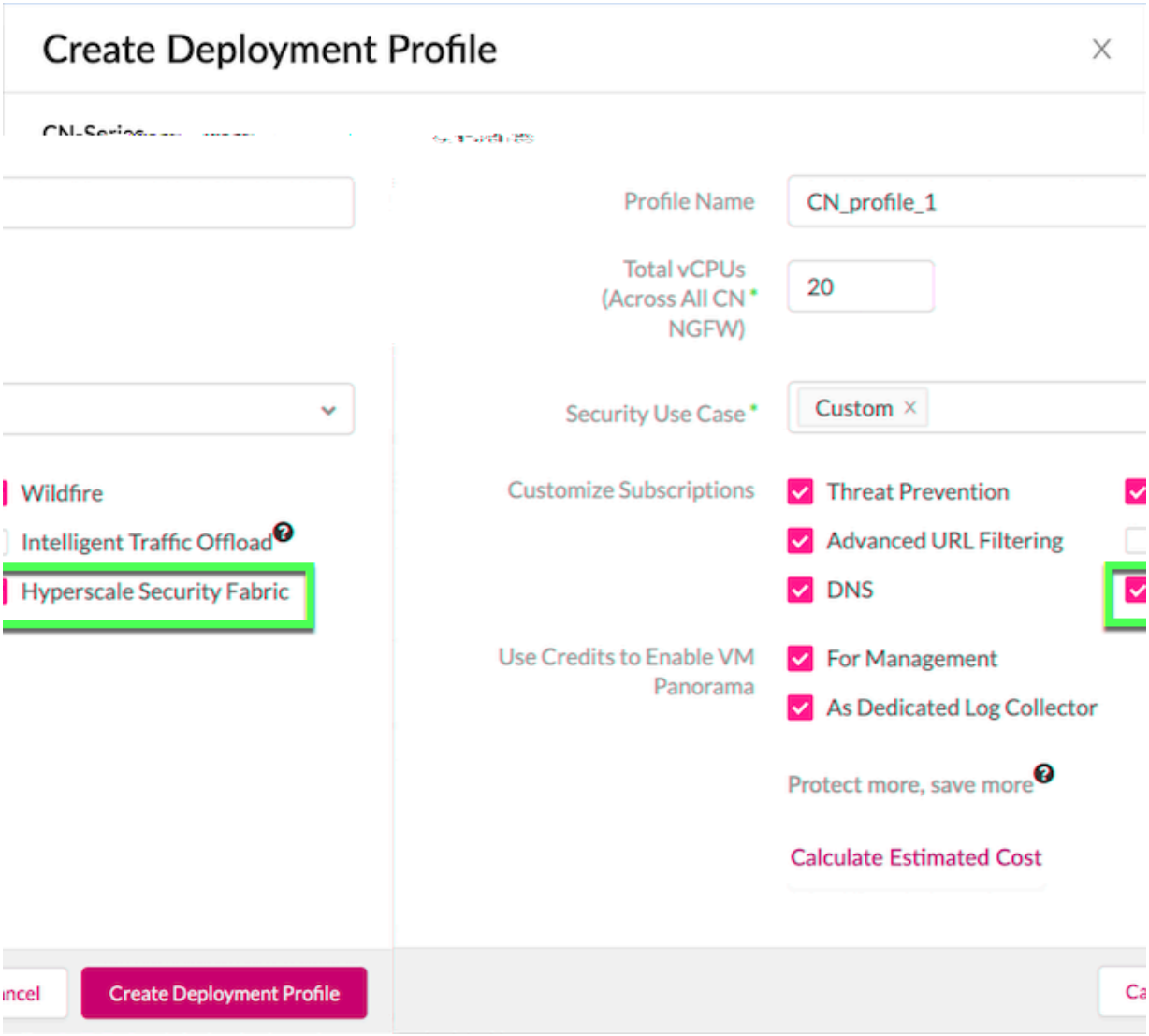
   输入所有 Pod（CN-NGFW、CN-GW 和 CN-DB）所需的 vCPU 总数。

3. 从下拉列表中选择一个安全用例。下拉列表中的每个安全用例都会自动选择一些建议用于所选用例的描述。如果选择自定义，则可以指定要在部署中使用的订阅。

4. 在 **Customize Subscriptions**（自定义订阅）下选择 **Hyperscale Security Fabric**（超大规模安全结构），以便在订阅上启用 HSF。

5. （可选）使用积分启用 **VM Panorama** — **For Management**（用于管理）或 **Dedicated Log Collector**（专用日志收集器）。

STEP 3 | 单击 **Calculate Estimated Cost**（计算估计成本）以查看积分总数和部署前可用的积分数量。



管理部署配置文件

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

您可以根据 CN 系列部署的要求编辑、克隆或删除 CN 系列部署配置文件。此外，您可以在创建部署配置文件后添加或删除订阅。有关详细信息，请参阅管理部署配置文件。

CN 系列 HSF 系统要求

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

- 推荐的 CN 系列系统和容量矩阵
- 推荐的 CN-系列 HSF 版本
- CN 系列 HSF Jumbo 模式支持

推荐的 CN 系列系统和容量矩阵

以下是我们对 CN 系列 HSF 的推荐系统要求。

下表按 CN 系列的大小（大、中、小）分别列出数据。CN 系列 HSF 可以执行的吞吐量检查因集群的大小而异。

- 适用于 **HSF** 的 **CN** 系列小型版
- 适用于 **HSF** 的 **CN** 系列中型版
- 适用于 **HSF** 的 **CN** 系列大型版

CN 系列 HSF 需要两个节点组 — CN-MGMT 和 CN-DB，每个节点组有两个节点。CN-GW 和 CN-NGFW 节点组所需的节点数量取决于吞吐量。

集群版本		小	中	大
CN-GW	内核	24	24	24
	内存	16 GB	20 GB	24 GB
	带宽	50 Gbps	100 Gbps	100 Gbps
	实例类型	c5n.9xlarge（36vCPU、96GiB）	c5n.18xlarge	c5n.18xlarge
CN-DB	内核	8	8	12
	内存	0.64 x 12 x MaxSession（以百万计）GB	0.64 x 12 x MaxSession（以百万计）GB	0.64 x 10 x 10 GB
	带宽	10 GbE	25 GbE	25 GbE

集群版本		小	中	大
	实例类型	c5n.4xlarge（16vCPU、42GiB）	c5n.4xlarge	c5n.9xlarge
CN-MGMT	内核	4	12	12
	内存	16 GB	16 GB - 24 GB	16 GB - 24 GB
	带宽	10 GbE	10 GbE	10 GbE
	磁盘	56 Gi	80 Gi	80 Gi
	实例类型	c5n.4xlarge（8vCPU、21GiB）	c5n.4xlarge 或 c5d.9xlarge	c5n.4xlarge 或 c5d.9xlarge
CN-NGFW	内核	15	24	24 - 36
	内存	20 GB	16 GB - 47 GB	48 GB（如果内核数量超过 32 个，则为 56 GB）
	带宽	25 GbE	50 GbE	50 GbE
	实例类型	c5n.4xlarge（16vCPU、42GiB）	c5n.9xlarge	c5n.9xlarge

推荐的 CN-系列 HSF 版本

集群版本	节点数			接口总数	最少接口数
	小	中	大		
CN-GW	2	3	4	4-15	4
CN-DB	2	2	2	2	2
CN-MGMT	2	2	2	1	1
CN-NGFW	6	8	10	3	3
用于防止 DP 发生故障的额外 CN-NGFW	2	2	2	-	-

CN 系列 HSF Jumbo 模式支持

启用 Jumbo 支持后，Panorama 会将非 CN-MGMT 上所有接口的最大传输单位 (MTU) 配置为 8744 字节。

在 *Jumbo* 模式下，系统 *MTU* 为 *9000* 字节，如果未指定 *MTU*，接口将继承系统 *MTU*。

在 *EKS* 主机中，*AWS EC2* 实例的默认 *MTU* 值为 *9000*。因此，无需在主机端进行配置。

禁用 Jumbo 支持时，Panorama 会将非 CN-MGMT 上所有接口的最大传输单位 (MTU) 配置为 1756 字节。

您必须将 EKS 环境中的 Jumbo 和非 Jumbo MTU 值与 Panorama MTU 值相匹配。

模式	**MTU**（字节数）
Jumbo	EKS—9000 字节
非 Jumbo 模式	所有接口均为 1756 字节

部署 CN 系列 HSF 的先决条件

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

以下是部署 CN 系列 HSF 的先决条件：

- 集群要求
- 准备集群
- 为 CN 系列 HSF 部署准备 Panorama

集群要求

您需要一个具有必要权限的 Kubernetes 集群来创建和管理节点组。您还需要 Kubernetes 插件所需的资源来启动 CN 系列集群。

作为集群先决条件，您需要执行以下配置：

- EKS 或 Openshift (4.10) 集群，具体取决于您的环境。您需要创建 VPC 和子网并配置启动 EKS 集群所需的 IAM 角色。

  有关创建 EKS 集群的信息，请参阅创建 Amazon EKS 集群。

  有关创建 Openshift 集群的信息，请参阅安装 Openshift 集群。
- Kubernetes 版本 1.22 或更高版本。

  有关信息，请参阅使用部署工具安装 Kubernetes。
- Multus CNI，从而支持将多个网络接口附加到 Kubernetes 中的 Pod。

  有关详细信息，请参阅安装 Multus CNI。
- 四个节点组，具有 CN 系列系统要求中所述的最低要求。

准备集群

您需要配置以下各项：

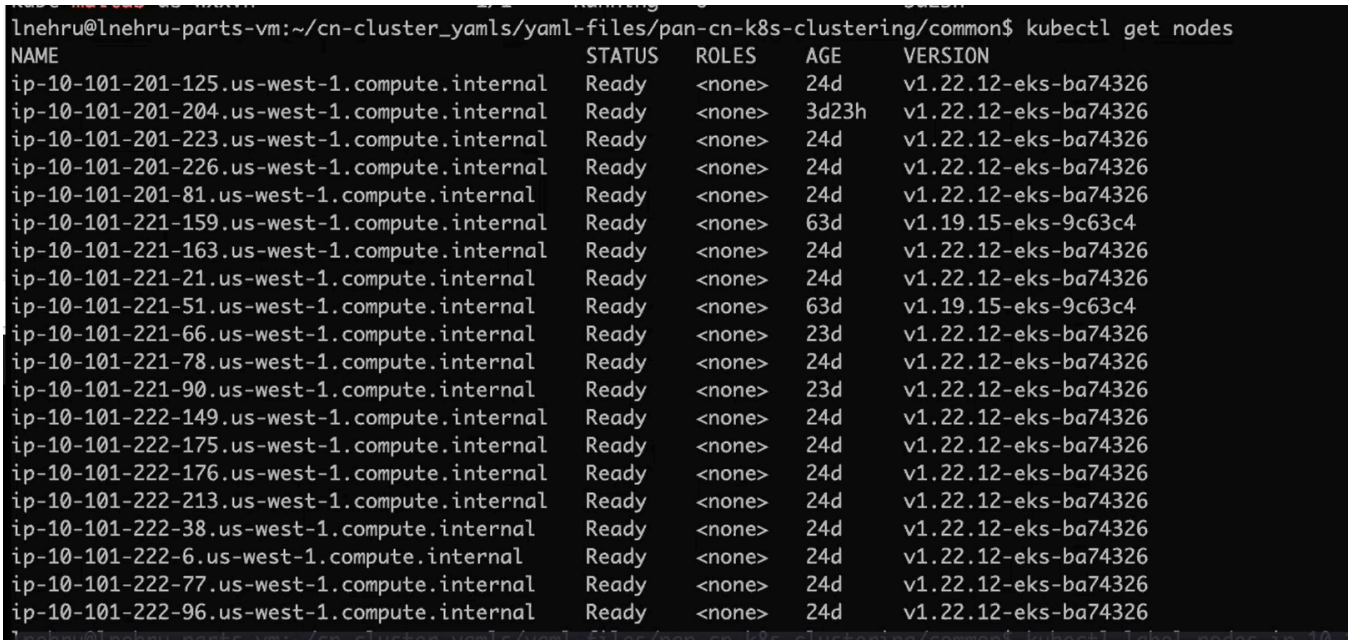
- 节点组和节点
- 节点标签
- 服务帐户
- 接口

节点组和节点

您需要至少 8 个节点来处理拓扑结构和容纳解决方案中的所有 Pod。Palo Alto Networks 推荐 4 组节点组，每组至少有两个节点。确保不允许 MP 节点组与其余 3 个节点组重叠。

如果您想使用 DPDK，则需要有一个配置了 DPDK 驱动程序的 AMI。有关更多信息，请参阅在 AWS EKS 上设置 DPDK。

运行 EKS 集群后，将 CloudFormation 模板与 Multus 结合使用，以便启动具有节点类型的节点组和 EC2 实例。



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

节点标签

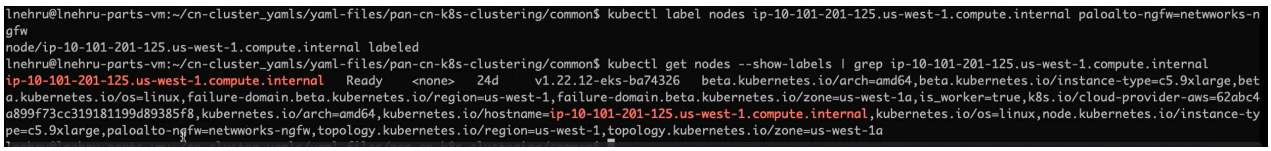
使用以下命令标记所有节点：

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

以下是节点标签的示例：

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

预计将为每个节点类型提供一个键值对。此外，建议为键使用默认值 paloalto，为值使用默认值 networks。但是，如果您选择更改节点标签，则需要在配置中进行相应的更改。



标记节点后，下载启动集群所需的 YAML。

服务帐户

部署的扩展权限使用服务帐户 yaml 提供。要创建服务帐户，Kubernetes 集群应该准备就绪。

1. 为 `plugin-serviceaccount.yaml` 文件运行服务帐户的 YAML 文件。

   该服务帐户可启用 Panorama 要求对 GKE 集群进行身份验证所需的权限，从而检索 Kubernetes 标签和资源信息。默认情况下，将该服务帐户命名为 pan-plugin-user。

2. 导航到 yaml-files/clustering folder/common 并部署以下各项：

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

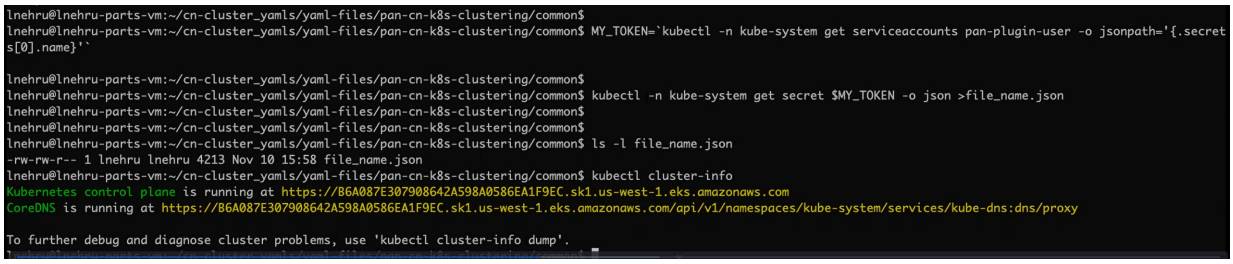
   ```
   kubectl apply -f pan-mgmt-serviceaccount.yaml
   ```

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

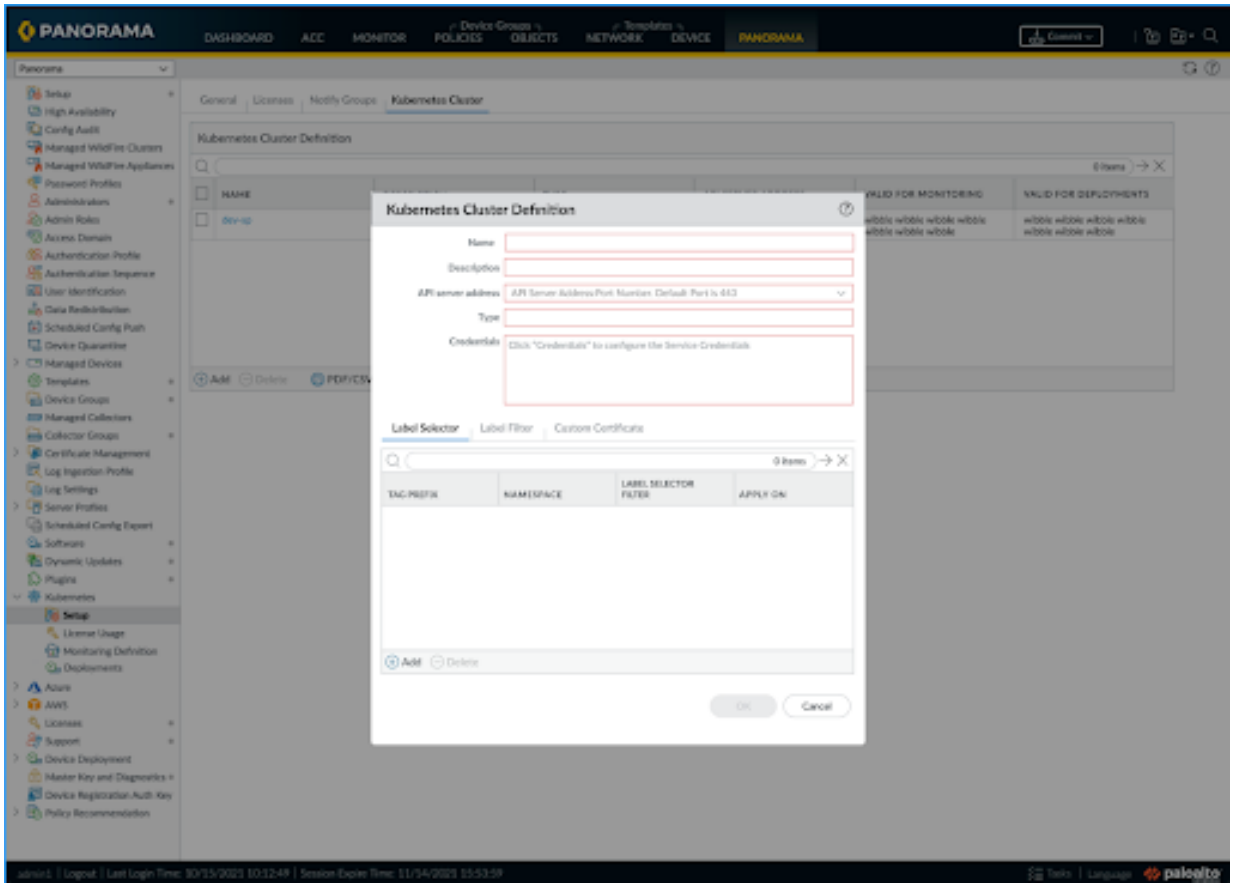
   例如，创建一个凭据文件，将其命名为 cred.json，其中包括密钥，然后保存该文件。您需要将此文件上传到 Panorama，以设置用于监控集群的 Kubernetes 插件。

3. 查看与该服务帐户相关联的密钥。

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



4. 将 cred.json 上传到 Kubernetes 插件并验证其状态。



在 Panorama 上提交第一次验证后，插件将继续定期调用验证逻辑并更新 UI 上的验证状态。

接口

您需要创建 CN-DB、CN-NGFW 和 CN-GW 所需的 ENI。识别这些接口的 PCI 总线 ID，这些接口随后将用于创建用于互连 Pod 的网络连接定义。

1. 使用在创建集群时创建的密钥/用户，通过 SSH 连接到节点。

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

2. 安装 ethtool 软件包。

   ```
   Sudo yum install ethtool
   ```

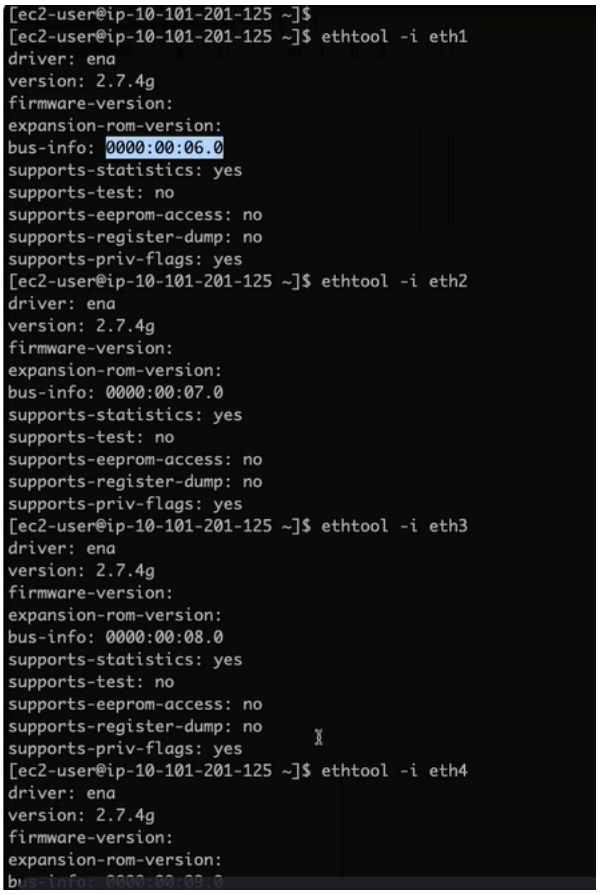
   ```
   sudo yum update -y && sudo yum install ethtool -y
   ```

3. 识别接口名称。

   ```
   ifconfig
   ```

4. 识别接口的 PCI 总线 ID，以便在 Pod 上部署网络连接。

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



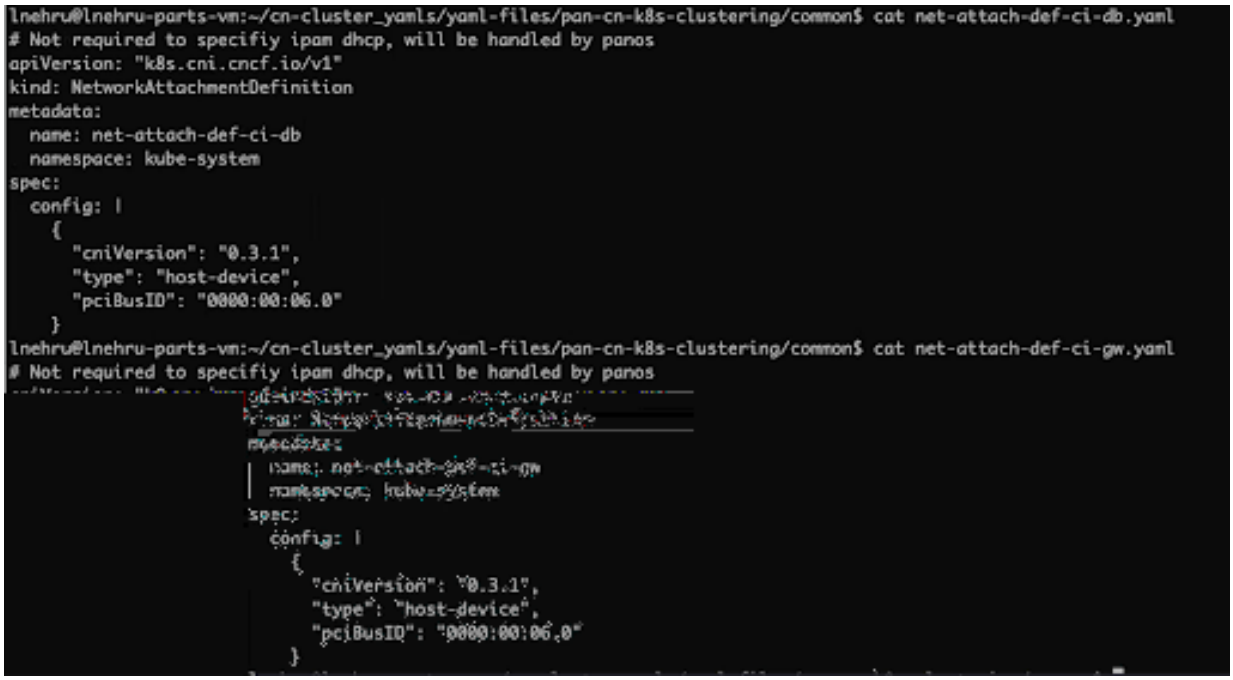
这里的 eth0 是节点管理接口，eth1 是 CI 接口，eth2 是TI，eth3 是外部接口 1，eth4 是外部接口 2。在标记为 CN-MGMT 的节点中，您只会找到用于管理的 eth0 接口。对于 CN-DB，您将拥有 eth1，对于 CN-NGFW，您将拥有 eth1、eth2，对于 CN-GW，您将拥有 eth1、eth2 以及在环境中创建的尽可能多的外部接口。

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

部署的所有 Pod 都需要位于不同的节点上，因为它们将使用相同的网络连接定义，因此，每个 Pod 都需要访问相同的 PCI 总线 ID。例如，如果网络连接使用用于 C/U Pod CI 链路的 PCI ID 6，则每个 C/U Pod 需要放置在具有来自同一子网的 PCI ID 6 接口的节点上。

5. 修改网络附件定义 YAML 上的 PCI 总线 ID。

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

这里的第一个链路 eth1 用于 CI，eth2 用于 TI，以此类推，eth3 用于外部链路。

6. 应用先决条件 YAML 文件。

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

在 Openshift 中，应用 `Kubectl apply -f ctrcfg-pidslimit.yaml`。有关 pidlimit 的详细信息，请参阅配置任务。

如果使用静态 PV，请在标记为 CN-MGMT Pod 的节点上创建静态 PV 安装卷。

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

为 CN 系列 HSF 部署准备 Panorama

CN 系列 HSF 配置和部署通过 Panorama 完成。在部署 CN 系列 HSF 之前，请确保已完成以下先决条件。

STEP 1 | 部署软件版本为 11.0 的 Panorama，并安装最低内容版本。

1. 有关 PAN-OS 11.0 上的最低内容发布版本，请转到 **Panorama** > **Dynamic Updates**（动态更新）。

   请参阅 PAN-OS 发行说明。

2. 对于软件版本，请转到 **Panorama** > **Software**（软件）。

   找到并下载您正在升级的发行版本的型号特定文件。例如，要将 M 系列设备升级到 Panorama 11.1.0，请下载 Panorama_m-11.0.0 映像；要将 Panorama 虚拟设备升级到 Panorama 11.0.0，请下载 Panorama_pc-11.0.0 映像。

   成功下载后，已下载映像的 **Action**（操作）列将从 Download（下载）更改为 Install（安装）。

STEP 2 | 如果您希望 Panorama 收集防火墙日志，请验证 Panorama 是否处于 Panorama 模式。

STEP 3 | 在 Panorama 上安装 Kubernetes 插件 4.0 版本。如果 Panorama 设备部署为 HA 对，则必须先在主要（活动）对端上安装 Kubernetes 插件。

1. 登录到 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以获取可用的插件列表。
2. 选择 **Download**（下载），然后 **Install**（安装）Kubernetes 4.0 插件。

   插件安装成功后，Panorama 将刷新，**Panorama** 选项卡上会显示 Kubernetes 插件。

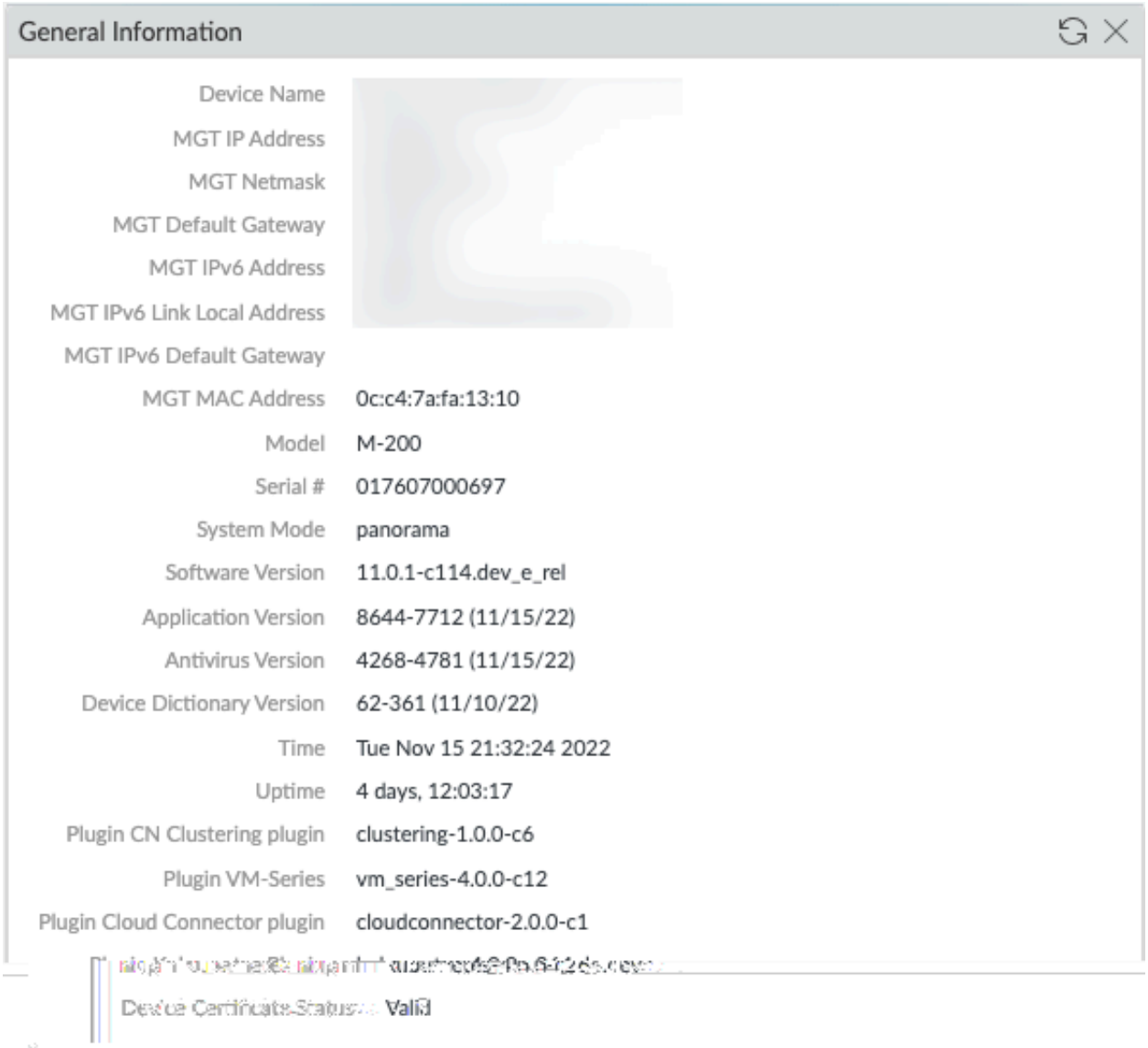
   如果 Panorama 部署在 HA 对中，请按步骤 3 中所述的步骤在辅助（被动）Panorama 上安装 Kubernetes 插件。
3. 单击 **Commit to Panorama**（提交到 **Panorama**）。

   该提交将创建一个用于 CN 系列 HSF 的 **K8S-CNF-Clustering-Readonly** 模板。这些接口显示在 Panorama 上最多可能需要一分钟的时间。此模板具有用于 CN-GW、CN-DB 和 CNNGFW Pod 的预配置集群互连 (CI) 链路以及用于 CN-GW 和 CN-NGFW Pod 的流量互连 (TI) 链路的网络配置。**K8S-CNF-Clustering-Readonly** 用于创建 30 个逻辑路由器和每

个逻辑路由器两个接口。以太网 x/1 是集群互连 (CI) 链路，而以太网 x/2 是集群互连 (TI) 链路。

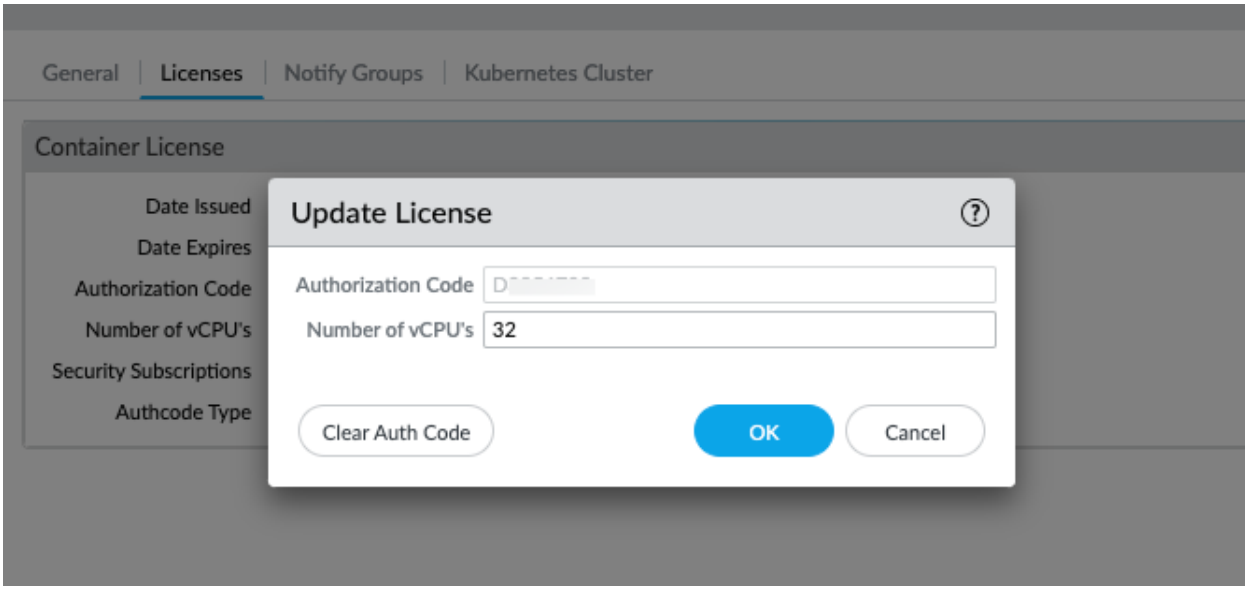
确保不重命名 ***K8S-CNG-Clustering-Readonly*** 模板。

您还可以在 Panorama **Dashboard**（指示板） > **General Information**（常规信息）小部件。



STEP 4 | 在 Panorama 上获取 CN 系列许可证积分。

1. 选择 **Panorama** > **Plugins**（插件） > **Kubernetes** > **Setup**（设置） > **Licenses**（许可证）。
2. 选择**Activate/update using authorization code**（使用授权代码激活/更新），然后输入授权代码和所需的 vCPU 总数。您必须创建部署配置文件才能获取 CN 系列授权代码。



使用 *HSF* 部署 *CN* 系列时，如果部署的 *Pod*（*CN-NGFW*、*CN-GW* 和 *CN-DB*）数量超过分配的 *vCPU* 数量，您将有四小时的宽限期来将更多 *vCPU* 添加到部署配置文件或删除足够多的 *Pod*。如果未在四小时宽限期内分配额外的 *vCPU* 或删除未获得许可的 *Pod*，则未许可的 *Pod* 将停止处理流量。已获得许可的 *Pod* 可保持许可状态。

3. 验证可用许可证积分的数量是否已更新。

STEP 5 | 创建父设备组。

您必须创建一个设备组，其中包含 CN 系列 HSF 所需的必要策略和对象。部署 CN 系列 HSF 时必须引用此设备组。

1. 转到 **Panorama** > **Device Groups**（设备组），然后单击 **Add**（添加）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。
3. 选择将处于您在设备组层次结构中所创建的设备组正上方的 **Parent Device Group**（父设备组）（默认为 **Shared**（共享））。
4. 单击 **OK**（确定）。

   将设备组名称引导至集群中的 CN-MGMT Pod。当 CN-MGMT Pod 使用这些引导参数连接到 Panorama 时，设备组将与集群配置中的集群名称相关联。对于 Panorama 高可用性

(HA)，CN-MGMT Pod 会将更新发送到主动和被动 Panorama。当 CN-NGFW、CN-DB 和 CN-GW Pod 处于活动状态时，会自动填充集群信息。

5. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），以提交设备组配置并将其推送到 Panorama。

STEP 6 | 创建变量模板以启用流量。

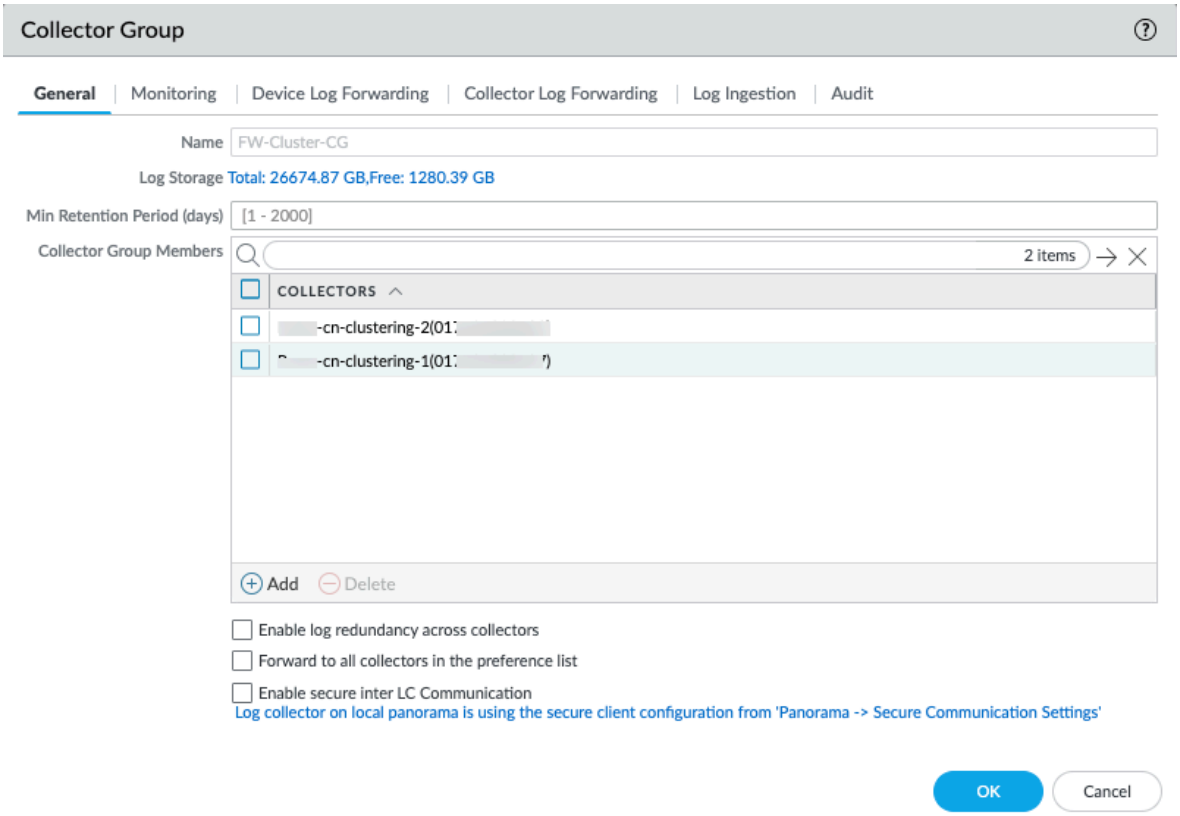
1. 转到 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 为模板输入一个唯一的 **Name**（名称）。
3. 输入可选 **Description**（说明）。
4. 配置变量模板以启用流量。

   在部署 *CN* 系列 *HSF* 之前或之后都可以配置此模板。

STEP 7 | 创建日志收集器并将其添加到日志收集器组。

1. 转到 **Panorama** > **Collector Groups**（收集器组），然后 **Add**（添加）收集器组。
2. 输入日志收集器的 **Name**（名称）。
3. 输入收集器组将保留防火墙日志的**Minimum Retention Period**（最小保留期）天数（范围为 1 至 2,000）。

   默认情况下，该字段为空，这表示收集器组无限期地保留日志。
4. 将日志收集器（1 至 16 个）**Add**（添加）到收集器组成员列表。



5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），以便将更改提交并推送到 Panorama 和配置的收集器组。

Panorama authkey 将由 *Kubernetes* 插件创建和管理。

部署 HSF 集群

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

确保满足将 CN 系列防火墙部署为 HSF 的先决条件后，导航到 **Kubernetes** > **Deployments**（部署）并单击 **Add**（添加）。

您需要配置以下选项卡才能部署 HSF 集群。

- General（常规）
- 节点数据
- 映像和存储
- CN 配置
- 自动扩展

General（常规）

在 **Deployments**（部署）弹出窗口的 **General**（常规）选项卡部分输入以下详细信息。

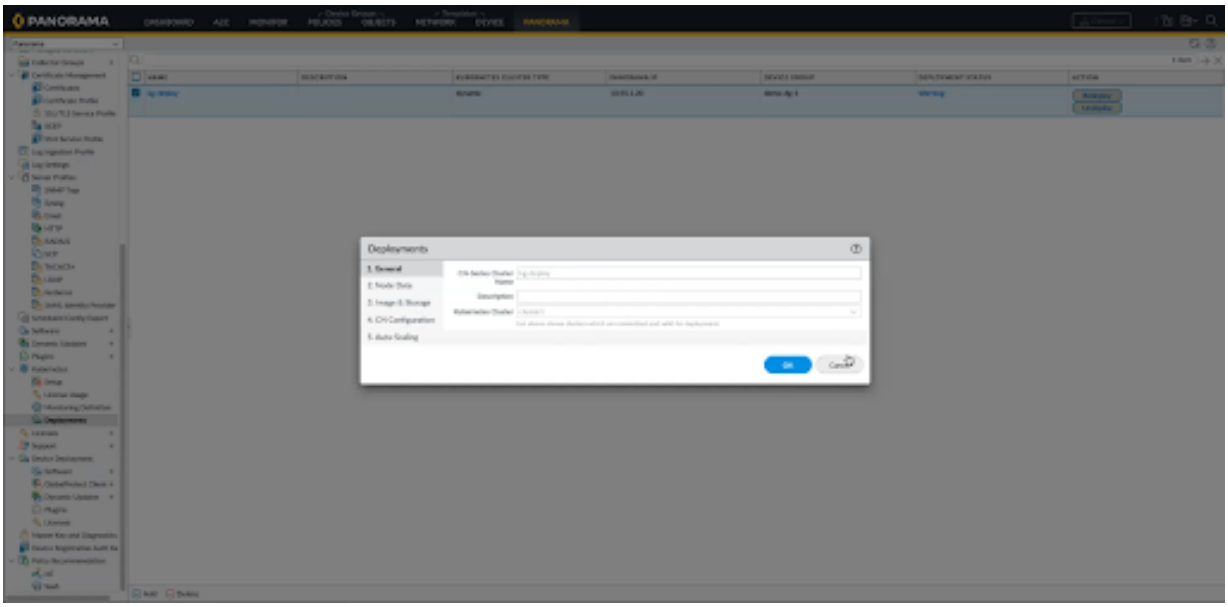
STEP 1 | **CN-Series Cluster Name**（**CN** 系列集群名称）— CN 系列 HSF 的名称。

STEP 2 | （可选）**Description**（说明）— 描述 HSF 集群的文本字符串。

STEP 3 | **Kubernetes Cluster**（**Kubernetes** 集群）— 集群的条目列表在插件的 **Setup**（设置）部分下创建。从下拉列表中选择创建的相关集群。

仅当已提交详细信息且对部署有效时，才会显示 *Kubernetes* 集群。

STEP 4 | **CN-Series Cluster Name**（**CN** 系列集群名称）— CN 系列 HSF 的名称。

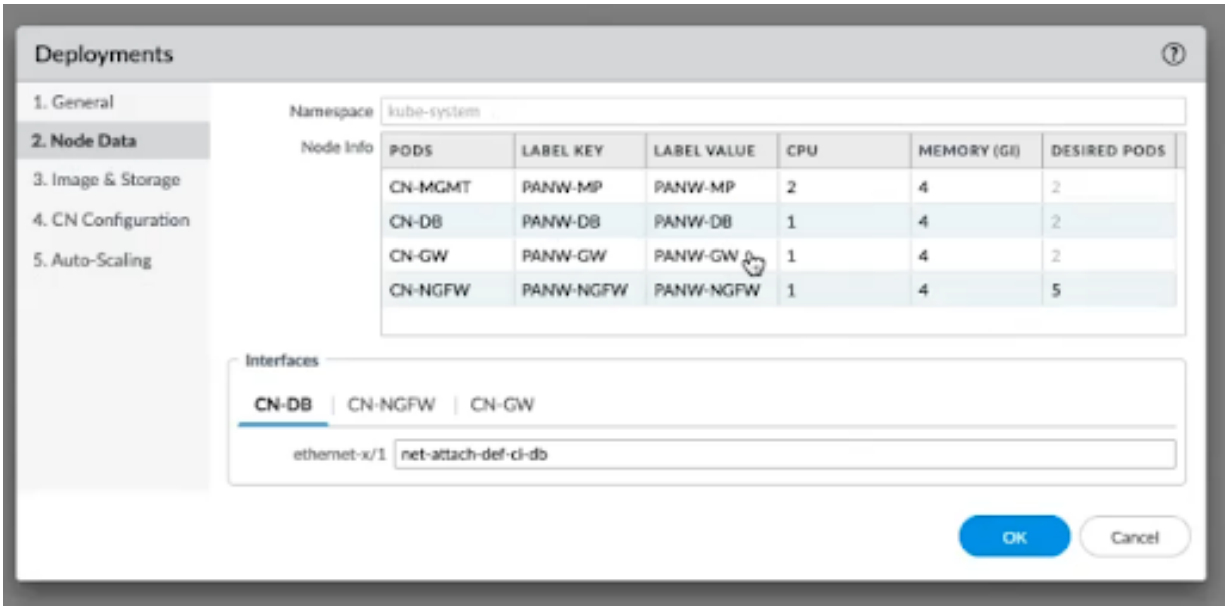


节点数据

在 **Deployments**（部署）弹出窗口的 **Node Data**（节点数据）选项卡部分输入以下详细信息。

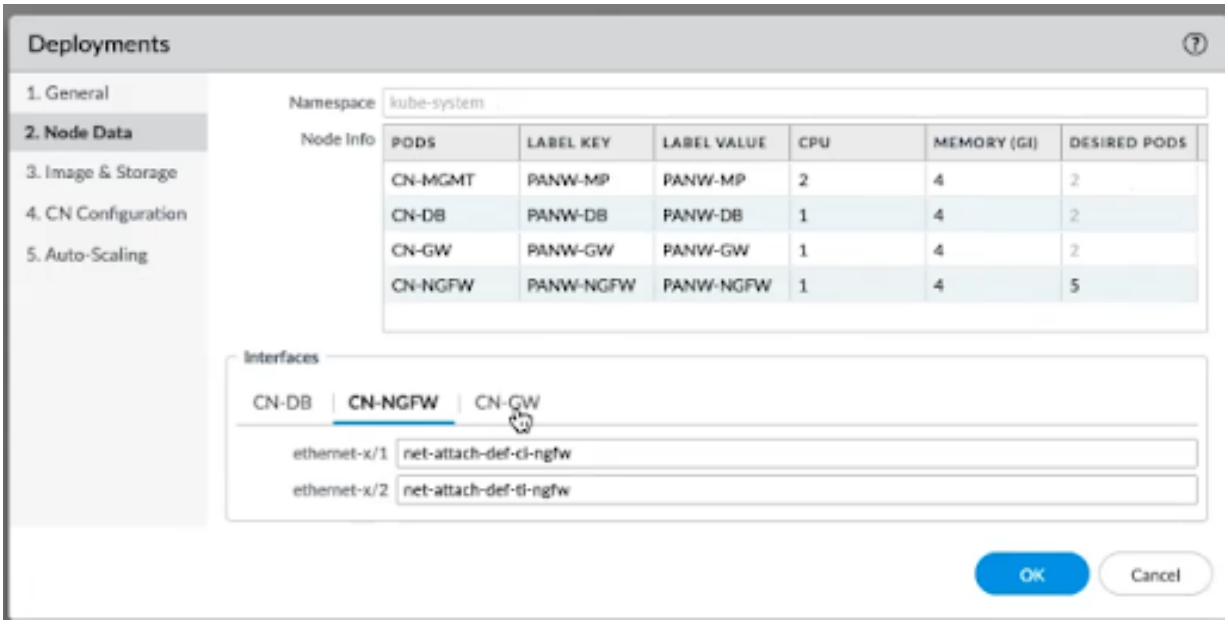
STEP 1 | **Namespace**（命名空间）— 现有 Kubernetes 集群中将部署 CN 系列 HSF 的命名空间。

STEP 2 | **Node Info**（节点信息）— 节点池标签用于部署各种类型的 CN Pod。您需要根据节点上的可用性为各种 Pod 类型指定 CPU、内存和所需 Pod。标签和标签值对是存在于节点上的先决条件值，您必须添加用于标记节点的相同键值对。



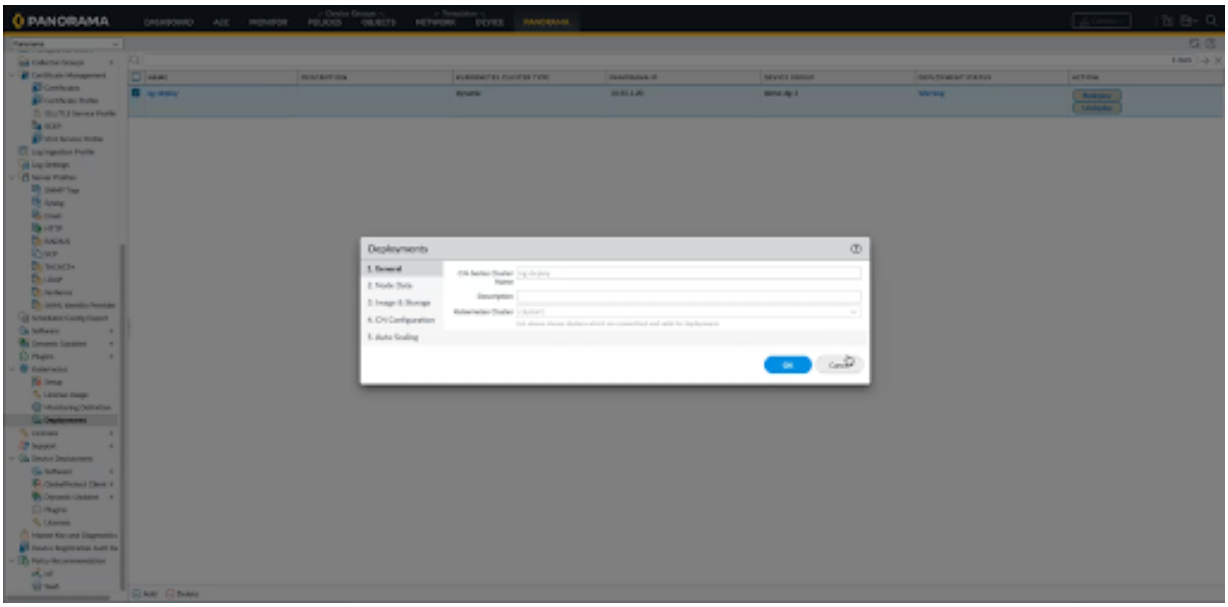
STEP 3 | **Interfaces**（接口）— 需要添加 CN-DB、NGFW、CN-GW Pod 的接口名称。每个接口都需要在 Kubernetes 集群上应用特定的 net-attach-def。默认情况下，插件将命名为 Ethernet x/1 和

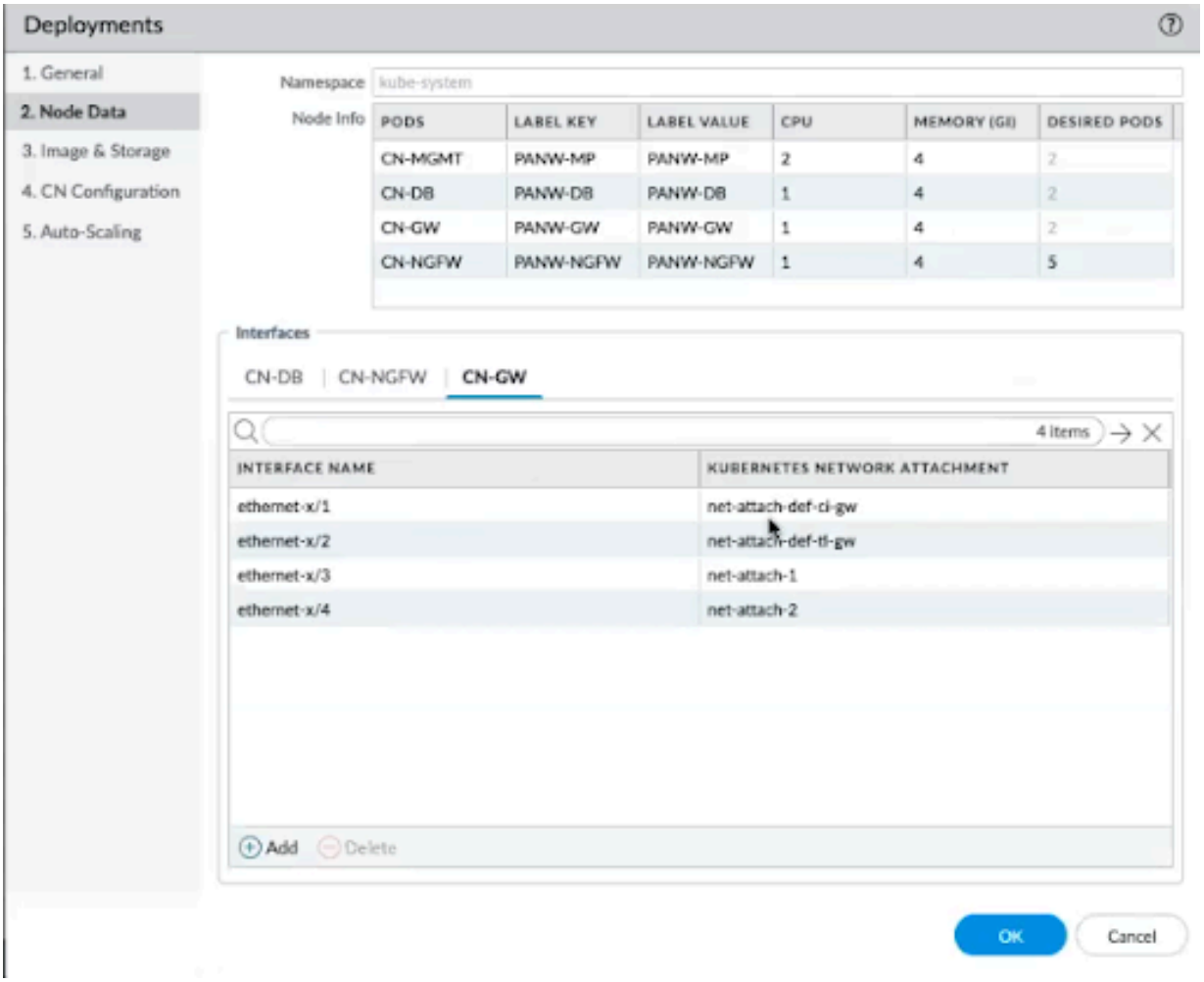
Ethernet x/2。如果更改以太网 x/1 和以太网 x/2 的接口名称，则还需要在网络附件部分进行更改。对于 CN-GW Pod，最多可添加 12 个接口（不包括 CI 和 TI 接口）。



仅当已提交详细信息且对部署有效时，才会显示 *Kubernetes* 集群。

STEP 4 | **CN-Series Cluster Name**（**CN** 系列集群名称）— CN 系列 HSF 的名称。





映像和存储

在 **Deployments**（部署）弹出窗口的 **Image & Storage**（映像和存储）选项卡部分输入以下详细信息。

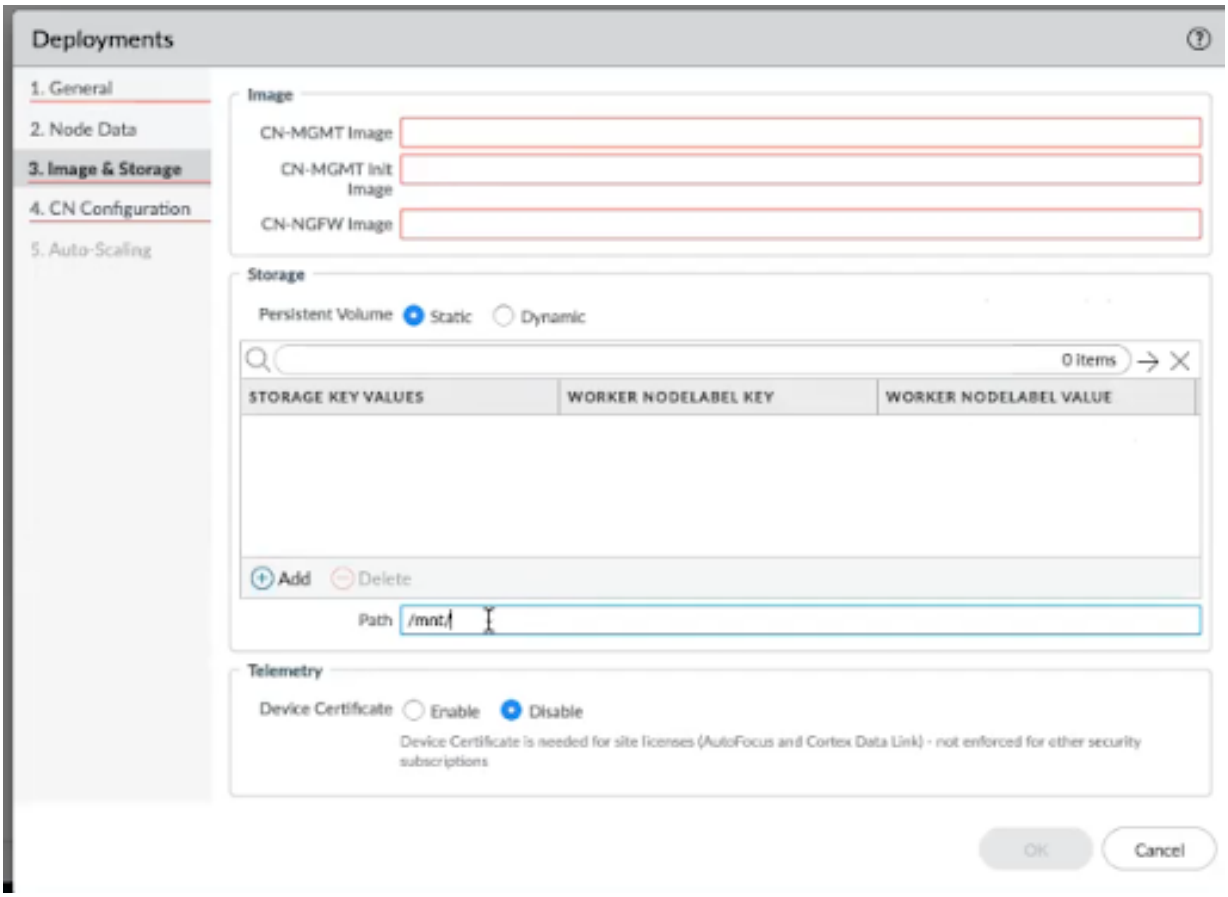
STEP 1 | **Image**（映像）— 您需要将映像存储在本地或 AWS 存储库中，而这无法通过 Panorama 进行验证。但是，Kubernetes 集群可以连接到存储映像的存储库。

1. **CN-MGMT** 映像：来自存储库的完整 URI，其中映像将由 Kubernetes 环境访问以部署 CN-MGMT Pod。
2. **CN-MGMT** 初始化映像：CN-MGMT Pod 所需的初始映像。
3. **CN-NGFW** 映像：来自存储库的完整 URI，其中映像将由 Kubernetes 环境访问以部署 CN-NGFW Pod。

STEP 2 | **Storage**（存储）— 如果您想配置独占存储，请在 EKS 环境的存储部分中单击动态，在 Openshift 环境中单击“静态”或“动态”，随后插件将配置云存储。如果选择静态，则需要

输入“存储密钥值”、“工作进程节点标签密钥”和“工作进程节点标签值”。您还需要输入安装存储的路径。

您必须在 *Kubernetes* 环境的命名空间中添加一个有效的非默认存储类。否则，如果选择动态存储选项，但未提供存储类名称，则将选择命名空间中存在的默认存储类。



STEP 3 | **Certificates**（证书）— 这是用于启用或禁用许可等信息的设备证书信息，如果启用，则需要提供 PIN ID 和 PIN 值。

CN 配置

在**Deployments**（部署）弹出窗口的 **CN Configuration**（**CN** 配置）选项卡部分中输入以下详细信息：

STEP 1 | **Primary Panorama IP**（主 **Panorama IP**）— 显示安装插件的 Panorama 的公共和私有 IP 地址的值。

STEP 2 | **Secondary Panorama IP**（辅助 **Panorama IP**）— 显示安装插件的辅助 Panorama（在 HA 的情况下）的公共和私有 IP 地址的值。

STEP 3 | **Device Group**（设备组）— 您需要在配置部署之前创建一个 DG，如先决条件部分所述。设备组下拉列表中列出了当前 Panorama 上的所有 DG，您需要选择一个有效的 DG。CN-MGMT Pod 将在该 DG 下注册。有关创建设备组的步骤，请参阅第 5 步为 CN 系列 HSF 部署准备 Panorama。

STEP 4 | **Template**（模板）— 在配置部署之前，您需要为 CN-GW 的特定详细信息创建一个模板 (variable_template)，如先决条件部分所述。模板下拉列表中列出了当前 Panorama 上的所有模板。您需要选择适合当前部署的模板。部署 HSF 后，插件会将该模板和 K8S-CNF-Clustering-Readonly 模板一起添加到模板堆栈中，后者可处理 CN-DB 和 CN-NGFW Pod 的基本配置。它还会在 CN-GW Pod 上配置 CI 和 TI 链接。CN-MGMT Pod 从模板堆栈获取配置。有关创建变量模板的步骤，请参阅第 6 步为 CN 系列 HSF 部署准备 Panorama。

STEP 5 | 日志收集器组 **(LCG)**— 此下拉列表中列出了当前 Panorama 上的所有日志收集器组，您需要选择合适的 LCG。它还会配置 CN-GW Pod 的 CI 和 TI 链接。有关创建 LCG 的步骤，请参阅第 7 步为 CN 系列 HSF 部署准备 Panorama。

STEP 6 | **Jumbo Frame**（巨型帧）— 巨型帧下拉列表中列出了以下值 —**Enable**（启用）、**Disable**（禁用）和 **AutoDetect**（自动检测）。此配置适用于 CN 系列 HSF 中的所有 Pod。

STEP 7 | **5G Enabled**（已启用 **5G**）— 这是一个包含 **Enable**（启用）和 **Disable**（禁用）选项的单选按钮，用于启用或禁用 CN 系列 HSF 上所需的 GTP 配置。

> 您需要在 ***variable_template*** 文件中处理模板所需的其他设置。

STEP 8 | **DPDK** — 这是一个包含 **Enable**（启用）和 **Disable**（禁用）选项的单选按钮。如果底层资源不支持 DPDK，则 CN 系列 HSF 默认会使用 packetmmap。

> 在 *EKS* 上，如果您想使用 *DPDK*，则需要有一个已配置 *DPDK* 驱动程序的 *AMI*。有关详细信息，请参阅在 AWS EKS 上设置 DPDK。

要在 Openshift 上启用 DPDK，您需要在工作节点上启用大页面。有关详细信息，请参阅配置大页面。

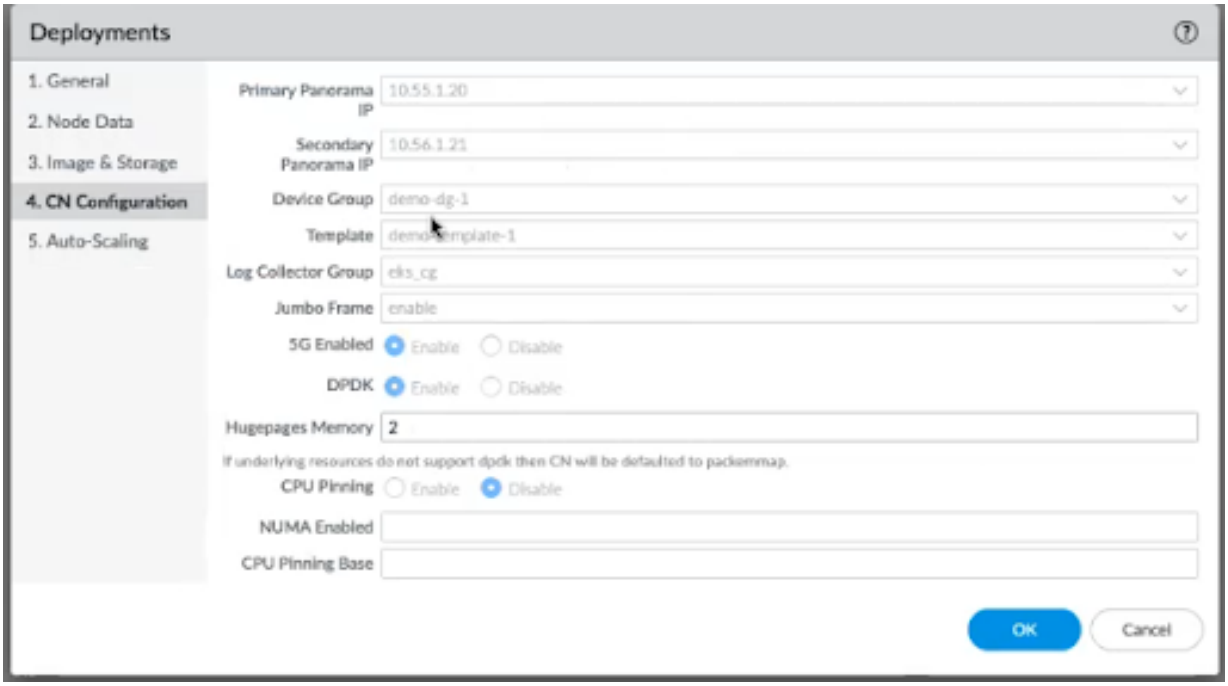
您还需要在工作节点上启用 VFIO PCI 驱动程序。

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

STEP 9 | **CPU Pinning**（**CPU** 固定）— 选择启用或禁用 CPU 固定。

STEP 10 | **Numa Enabled**（已启用 **Numa**）— 提供 NUMA 的节点编号。

STEP 11 | **CPU Pinning Base**（**CPU** 固定库）— 提供您希望从中开始转发进程的 CPU 固定并跳过编号较低的 CPU 的 CPU 编号。



自动扩展

在 **Deployments**（部署）弹出窗口的 **Auto-Scaling**（自动扩展）选项卡部分输入以下详细信息。

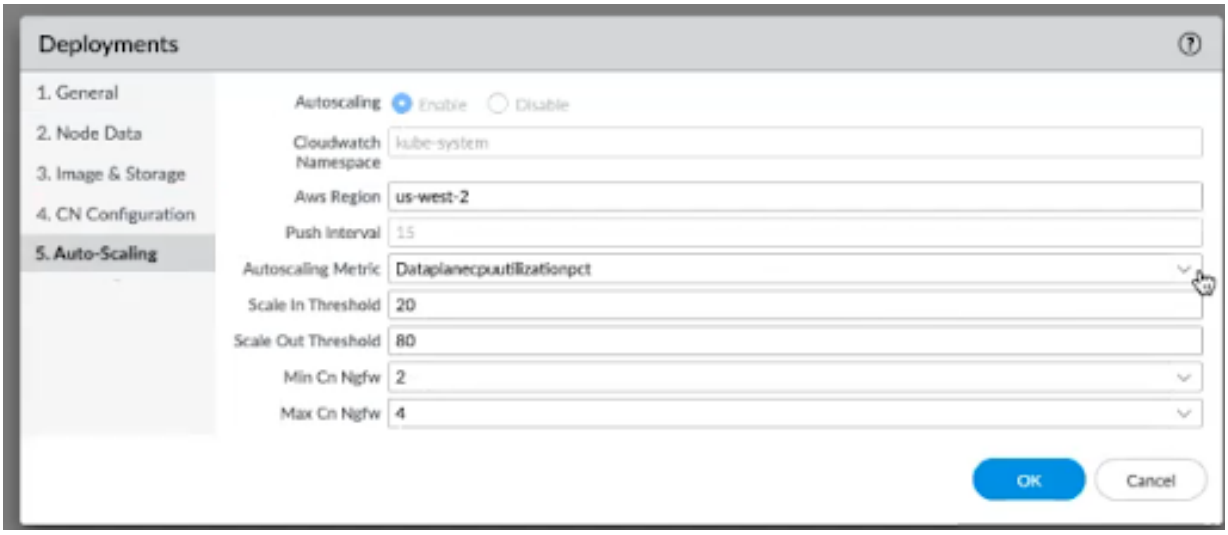
- 自动扩展仅在具有 *EKS Kubernetes 1.22* 版本的 *EKS* 环境中受支持。其他 *Kubernetes* 系统的自动扩展选项卡是灰色的。
- 您需要部署EKS 环境中使用 KEDA 的基于自定义指标的 HPA，自动扩展功能才会生效。

STEP 1 | 在 **Autoscaling**（自动扩展）部分输入 **Autoscaling Metric**（自动扩展指标）、**Scale In Threshold**（缩小阈值）和 **Scale Out Threshold**（扩展阈值）。

STEP 2 | 单击 **OK**（确定）以提交部署。

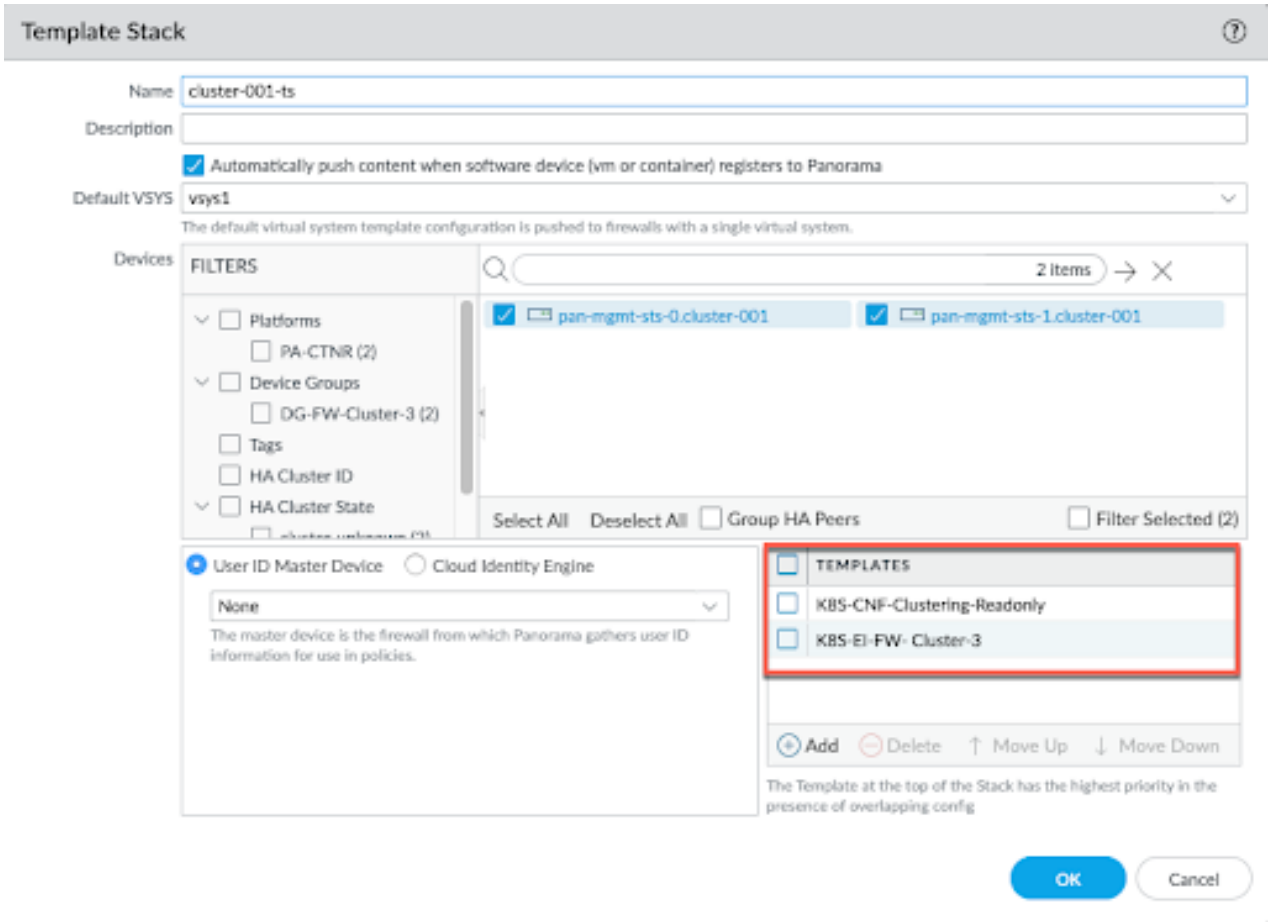
以下是自动扩展支持的指标。

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



输入所有配置详细信息后，“部署”选项卡会显示存储的各个部署的详细信息。单击 **Commit**（提交）以继续部署。提交完成后，插件会显示“部署”按钮。单击 **Deploy**（部署）按钮以部署 CN 系列 HSF。

部署 CN 系列 HSF 后，集群会创建模板堆栈，<cluster-name>`-ts` 会使用 K8S-CNF-Clustering-Readonly 模板和在第 6 步为 CN 系列 HSF 部署准备 Panorama中创建的变量模板。



在 HSF 部署配置期间引用的设备组（在第 5 步为 CN 系列 HSF 部署准备 Panorama中创建）和在 HSF 部署引导到 CN-MGMT Pod 后自动创建的模板堆栈。当 CN-MGMT Pod 连接到 Panorama 时，设备组和模板堆栈会自动与 HSF 名称相关联。

CN-DB、CN-GW 和 CN-NGFW Pod 的 HSF 信息在它们处于活动状态时会自动填充。当这些 Pod 启动并运行时，CN-MGMT Pod 会将 CI IP 地址、Pod 详细信息、设备 ID 和软件版本等详细信息发送到 Panorama。

对于 Panorama 高可用性 (HA)，CN-MGMT Pod 会将更新发送到主动和被动 Panorama。

不同的部署状态

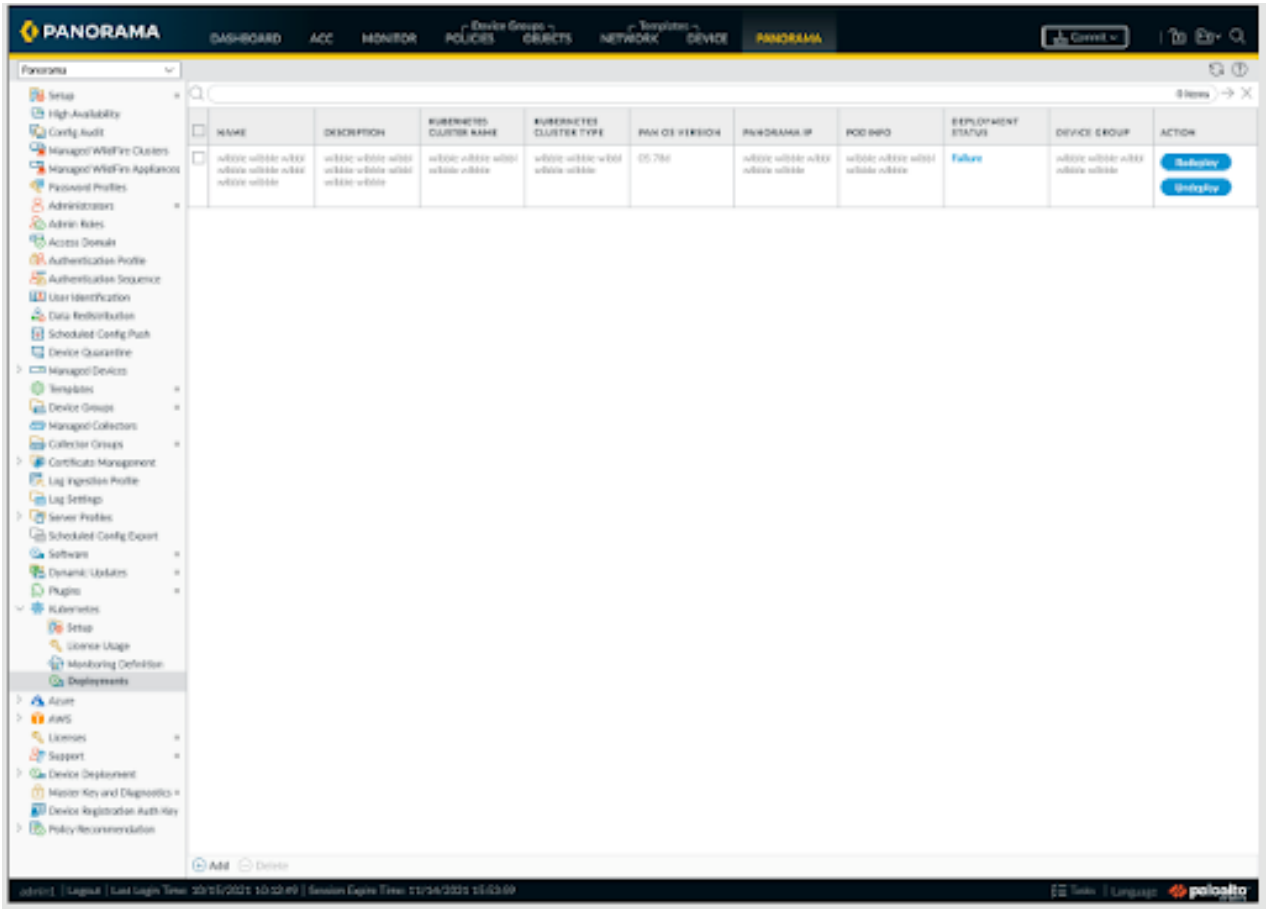
在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

输入所有配置详细信息后，“部署”选项卡会显示存储的各个部署的详细信息。部署包含 5 个阶段：

1. 需要提交
2. 未部署
3. 正在部署
4. 警告
5. 成功/失败

1. 单击提交以继续部署。您可能会发现，单击“提交”后会禁用“部署”按钮，部署状态将变成未部署。完成提交后，“部署”按钮处于启用状态。
2. 单击“部署”以继续部署 CNC 系列 CNF。部署状态将变成“正在部署”。在此阶段，创建 Panorama 配置并生成 CN-GW，插件会开始调用 API 来部署 CN 系列 HSF。
3. 然后，根据资源可用性和配置详细信息，部署状态将变成警告、成功或失败。接着会启用“重新部署”和“取消部署”按钮。
4. 单击“重新部署”，更改启用的参数并提交更改，然后单击“重新部署”。
5. 单击取消部署可删除在此部署中创建的所有 CN 系列 HSF 容器。

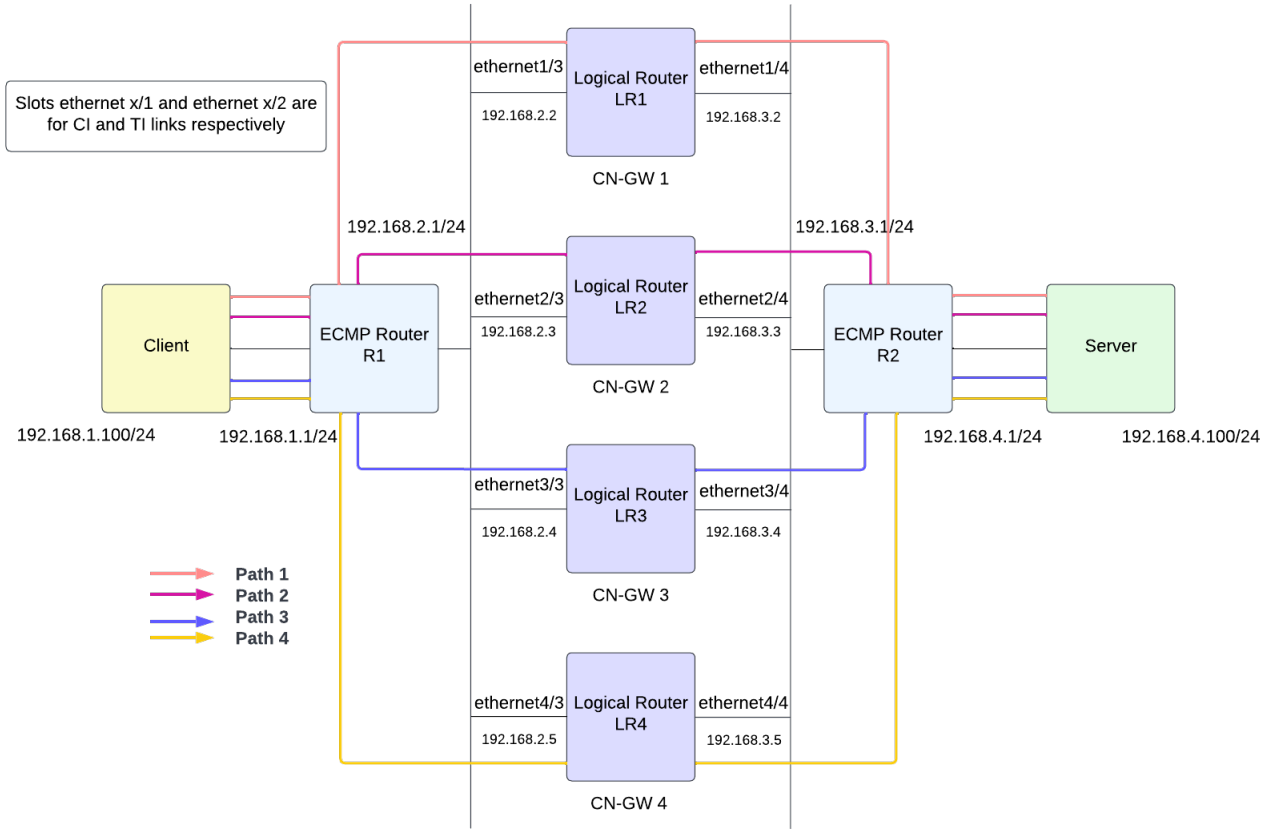
删除所有 *CN* 系列 *HSF Pod* 后仍会保留所有 *Panorama* 配置。



配置流向 CN 系列 HSF 的流量

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

上游/下游路由器使用基于流的 ECMP 算法。当流量到达 CN-GW 时，它将使用对称哈希算法，通过流量互连 (TI) 链路将流量分配到可用的一个 CN-NGFW。从两个方向（客户端到服务器和服务器到客户端）匹配会话的流量将始终通过相同的 CN-NGFW。CN-NGFW 处理流量后，如果您设置了 **Allow**（允许）流量的策略，则会将流量数据包发送回 CN-GW 以使其到达服务器。



STEP 1 | 在防火墙上创建逻辑路由器以参与第 3 层路由。

1. 转到 **Network**（网络）> **Routing**（路由）> **Logical Router**（逻辑路由器），然后从 **Template**（模板）下拉列表中选择变量模板。
2. 选择默认虚拟路由器或为新逻辑路由器添加 **Name**（名称）。
3. 选择 **General**（常规），然后添加一个已定义的 **Interface**（接口）。

   重复此步骤以添加要添加到逻辑路由器的所有接口。

   ethernetX/1 和 *etehrnetX/2* 接口分别保留给 *CI* 和 *TI* 链路。选择 ***ethernet1/3*** 和 ***ethernet1/14*** 之间的接口。
4. 单击 **OK**（确定）。
5. 设置静态路由的管理距离。范围是 10 到 240；默认值是 10。

   根据您的网络需要设置各种类型的路由的管理距离。当虚拟路由器有两个或两个以上前往同一目标的路由时，可使用管理距离从不同的路由协议和静态路由中选择最佳路径，优先选择较短的距离。
6. 让 ECMP 能够利用多个等价路径进行转发。
7. 单击 **OK**（确定）。

STEP 2 | 配置第 3 层接口，从而使流量可以传输。

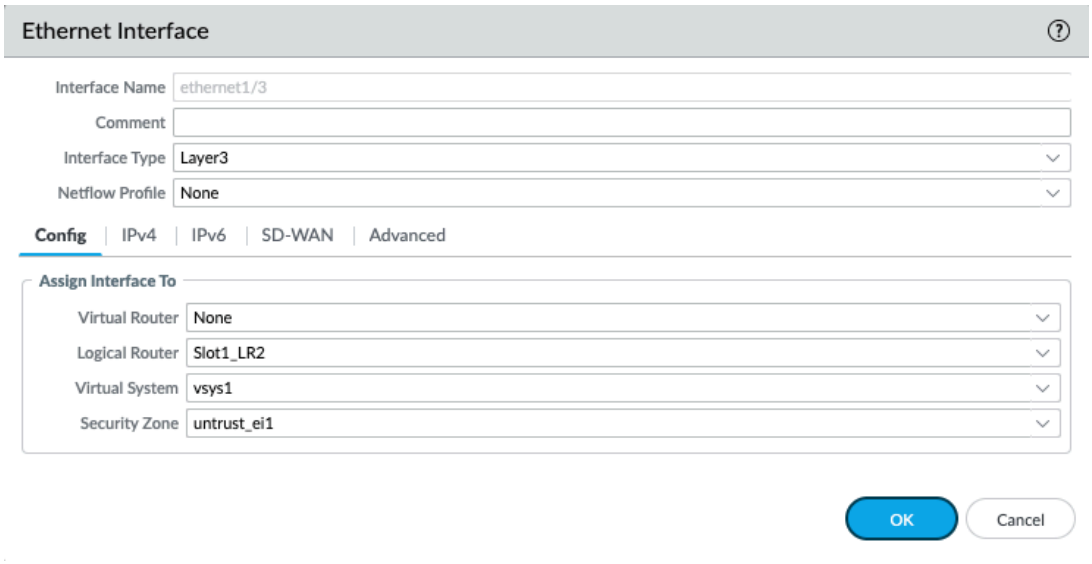
为 CN 系列 HSF 部署准备 Panorama时，您可能已经创建了一个变量模板。要让流量通过集群网络传输，您必须使用必要的网络和流量配置来配置变量模板，从而平衡 CN 系列 HSF 的负载。

您必须使用 IPv4 地址配置第 3 层以太网接口，以便让防火墙在这些接口上执行路由。通常，您可以使用以下步骤来配置连接到互联网的外部接口和内网接口。

您可以在部署 *CN* 系列 *HSF* 之前或之后配置此模板。

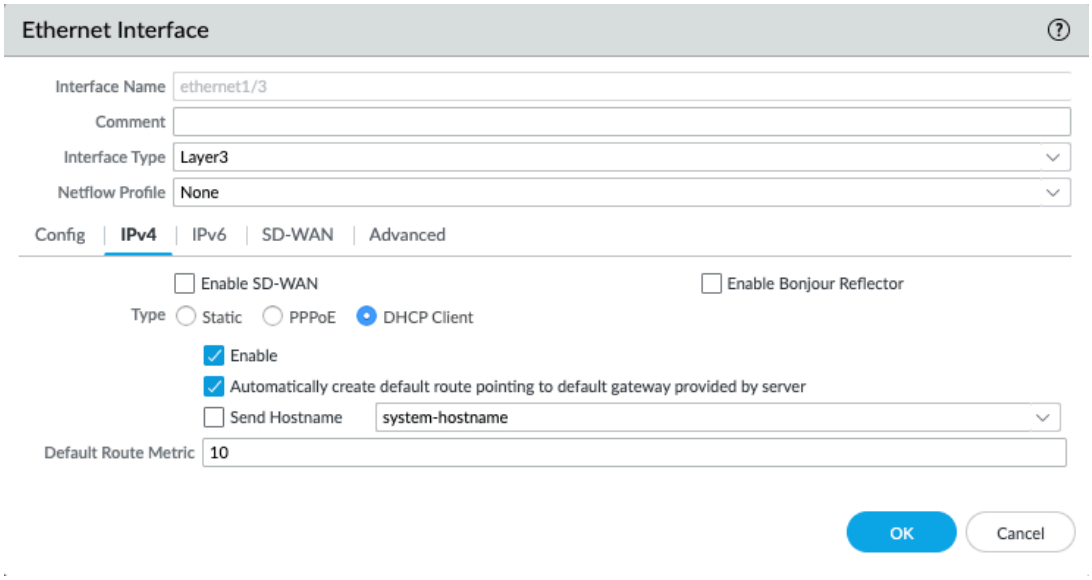
确保不要让此模板的配置与在 *Kubernetes* 插件安装期间自动创建的 ***K8S-CNF-Clustering-Readonly*** 模板发生重叠。

1. 转到 **Network**（网络） > **Interfaces**（接口），然后从 **Template**（模板）下拉列表中选择变量模板。
2. 选择 **Ethernet**（以太网）接口以 **Add Interface**（添加接口）。
3. 选择 1 到 30 之间的 **Slot**（插槽）。
4. 输入 **`ethernet1/3`** 和 **`ethernet1/14`** 之间的 **Interface Name**（接口名称）。
5. 对于 **Interface Type**（接口类型），请选择 **Layer 3**（第 **3** 层）。
6. 选择 **Config**（配置）选项卡：
   - 对于 **Logical Router**（逻辑路由器），请选择在第 1 步中配置的逻辑路由器。
   - 对于 **Virtual System**（虚拟系统），如果是多虚拟系统防火墙，请选择正在配置的虚拟系统。
   - 对于 **Security Zone**（安全区域），选择接口所属的区域或创建 **New Zone**（新区域）。



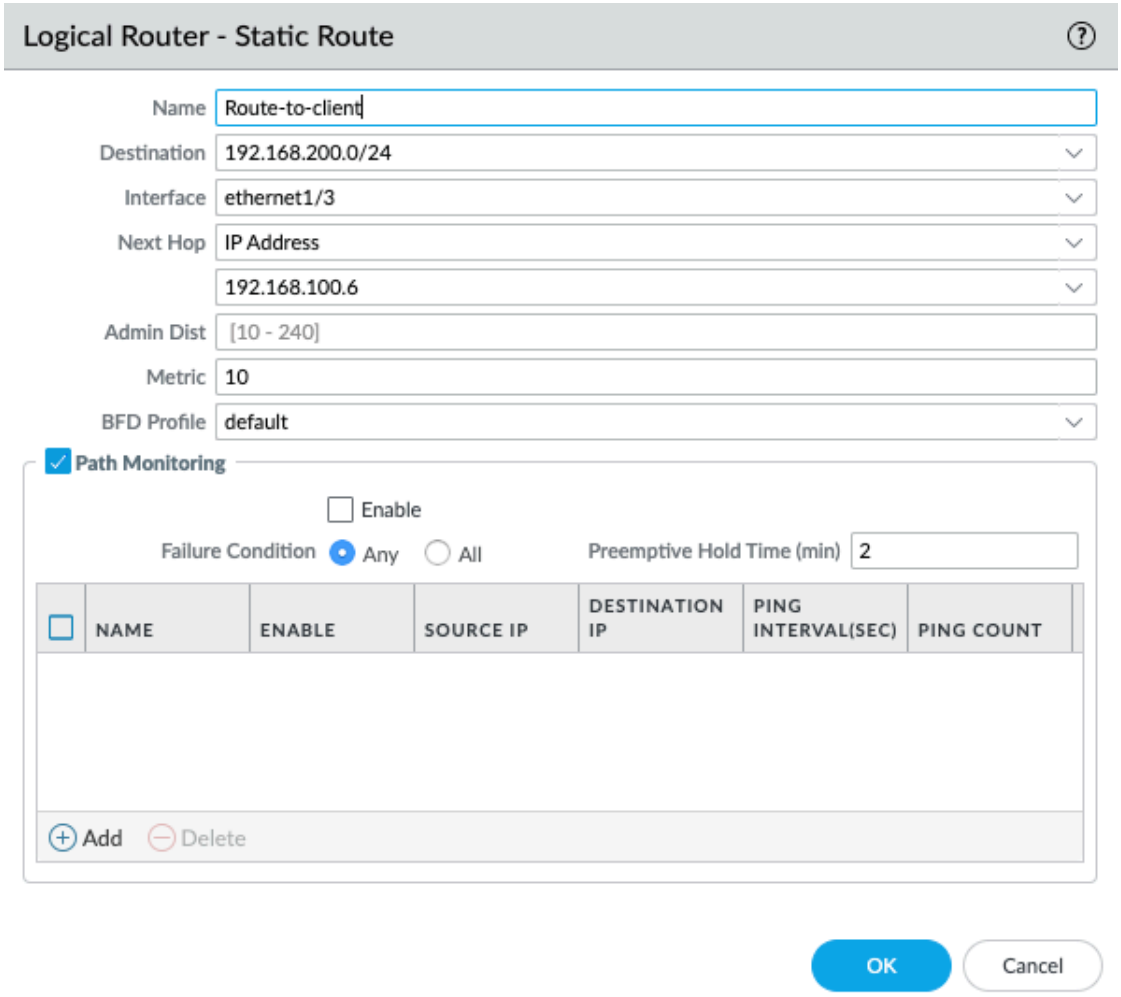
7. 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）。

   防火墙接口充当 DHCP 客户端，并接收动态分配的 IP 地址。防火墙还可以将 DHCP 客户端接口收到的设置传播到在防火墙上运行的 DHCP 服务器中。有关详细信息，请参阅将接口配置为 DHCP 客户端。
8. 单击 **OK**（确定）。



STEP 3 | 为逻辑路由器配置静态路由。

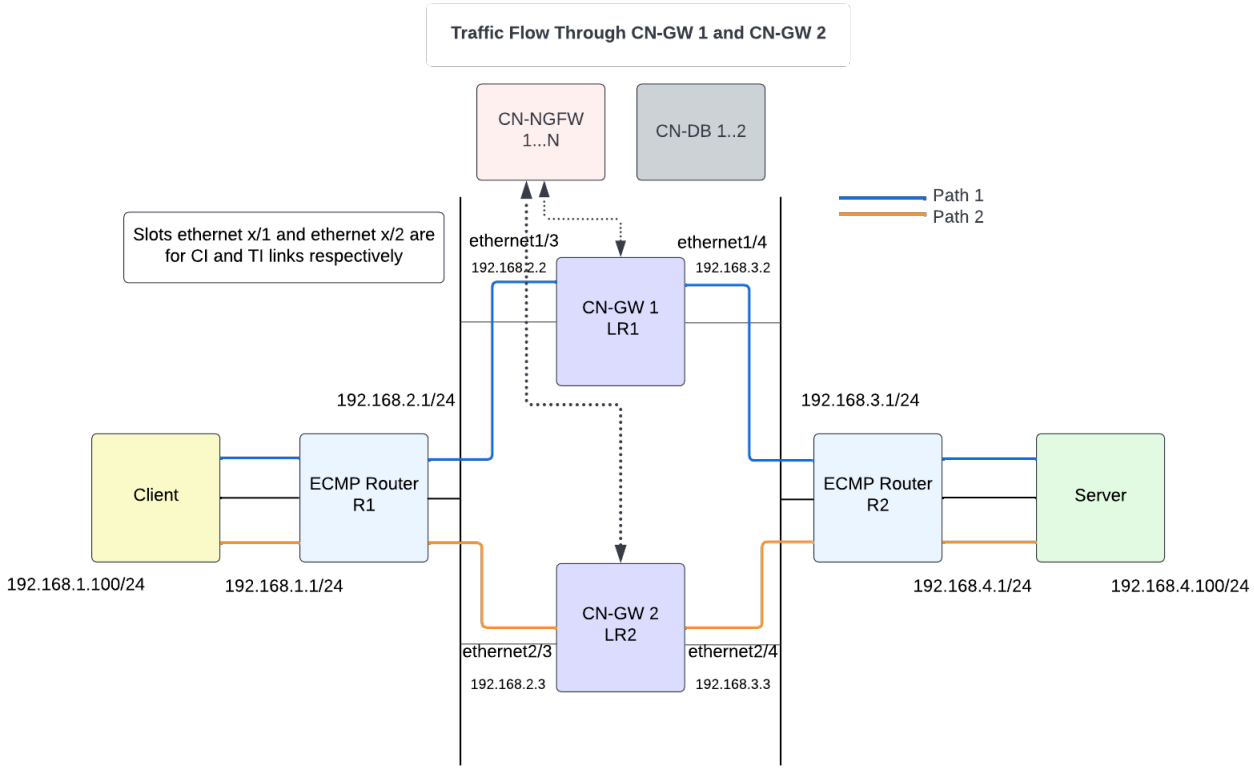
1. 转到 **Network**（网络）> **Routing**（路由）> **Logical Router**（逻辑路由器），然后从 **Template**（模板）下拉列表中选择变量模板。
2. 选择 **Static**（静态）> **IPv4**，然后单击 **Add**（添加）。
3. 输入静态路由的 **Name**（名称）。
4. 输入 **Destination**（目标）路由和网络掩码。例如，192.168.200.0/24。
5. 选择要用于下一个跃点的数据包的出站接口。
6. 对于 **Next Hop**（下一个跃点），请选择 **ip-address** 并输入内部网关的 IP 地址。例如，192.168.100.2。
7. 为路由输入 **Admin Distance**（管理距离），以覆盖此逻辑路由器为静态路由设置的默认管理距离（范围为 10-240；默认值为 10）。
8. 输入路由 **Metric**（跃点数）（范围为 1-65,535）。
9. 将 **BFD Profile**（**BFD** 配置文件）应用到静态路由，以便在静态路由失败时，防火墙可以删除该路由并使用备用路由。默认为 **None**（无）。
10. 单击 **OK**（确定）。



测试用例：基于第 3 层 BFD 的 CN-GW 故障处理

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

该测试评估了处理 CN-GW 故障所需的 BFD 配置。BFD 配置文件处理上游/下游路由器上的 CN-GW 故障。



对称通信流量

- 如果入口流量接口是 CN-GW 1，则在 LR1 上查找路由以找到出口接口。
  - 路由 1：目标：客户端子网；下一跃点：R1
  - 路由 2：目标：服务器子网；下一跃点：LR2
- 如果入口流量接口是 CN-GW 2，则在 LR2 上查找路由以查找出口接口。
  - 路由 1：目标：客户端子网；下一跃点：R1
  - 路由 2：目标：服务器子网；下一跃点：R2

非对称通信流量

CN 系列 HSF 也支持非对称通信流量。例如，客户端到服务器的流量匹配会话 1 流经 CN-GW 1，服务器到客户端的流量匹配会话 1 流经 CN-GW 2。对于非对称通信流量，面向 R1 的所有接口必须位于同一个区域内。同样，面向 R2 的所有接口必须位于同一个区域内。

Inter LR 路由

例如，如果入口流量接口是 CN-GW 1，则在 LR1 上查找路由以查找出口接口。如果有一条到达服务器的路由，下一跃点为 LR2，则 CN-NGFW 会将流量发送到 LR2。根据 CN-GW 2 LR2 路由查询，数据包将发送到服务器。

STEP 1 | 转到 **Network**（网络）> **Routing**（路由）> **Routing Profiles**（路由配置文件）> **BFD**，然后从 **Template**（模板）下拉列表中选择变量模板。

您必须在外部路由器和逻辑路由器上启用 BFD。

STEP 2 | 单击 **Add**（添加），为 BFD 配置文件添加。

STEP 3 | 输入 **Name**（名称）。

STEP 4 | 选择 BFD 运行的 **Mode**（模式）：

- **Active**（主动）— BFD 发起控制数据包的发送（默认）。BFD 对端设备中至少有一个要为主动；两个对端设备可同时为主动。
- **Passive**（被动）— BFD 等待对端发送控制数据包，并在必要时作出响应。

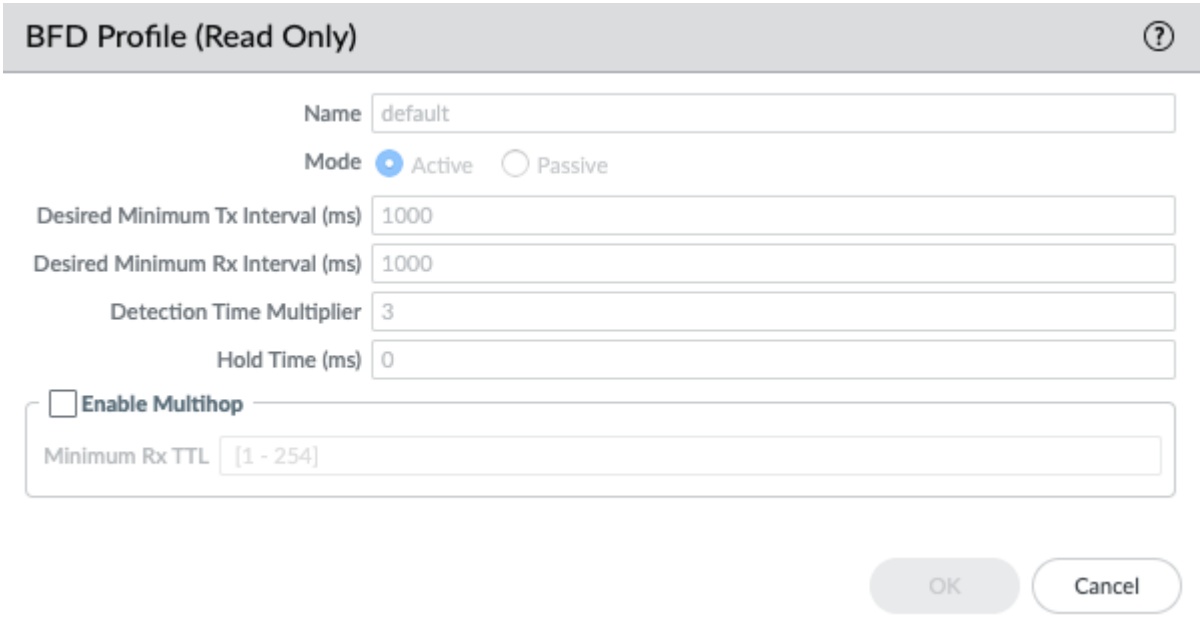
STEP 5 | 输入 **Desired Minimum Tx Interval (ms)**（理想最短传输间隔时间（毫秒））。这是您希望 BFD 协议（简称为 BFD）发送 BFD 控制数据包的最短间隔时间（毫秒）；因此您与对端设备协商传输间隔。

STEP 6 | 输入 **Detection Time Multiplier**（检测时间乘数）。本地系统计算检测时间的方式如下：用从远程系统接获取的 **Detection Time Multiplier**（检测时间乘数）乘以远程系统的约定传输间隔（**Required Minimum Rx Interval**（所需最小 **Rx** 间隔时间）越大，获得 **Desired Minimum Tx Interval**（理想最小 **Tx** 间隔时间）越晚。）。如果在检测时间耗尽前，BFD 未从其对等接收到 BFD 控制数据包，则会出现故障。范围为 2 至 50，默认为 3。

STEP 7 | 输入 **Hold Time (ms)**（保持时间（毫秒））。BFD 传输 BFD 控制数据包之前，链路启用后的延迟时间（毫秒）。**Hold Time**（保持时间）仅适用于 BFD Active（BFD 活动）模式。如果 BFD 在 **Hold Time**（保持时间）内收到 BFD 控制数据包，则它会忽略这些数据包。范围为 0-120000，默认值为 0。

STEP 8 | 选择 **Multihop**（多跃点）通过 BGP 启用 BFD 多跃点。输入 **Minimum Rx TTL**（最短接收 **TTL**）。这是 BFD 会在支持多跃点 BFD 时在 BFD 控制数据包中接受（接收）的最小生存时间 (TTL) 值（跃点数）。（范围为 1-254；没有默认设置）。

STEP 9 | 单击 **OK**（确定），保存 BFD 配置文件。



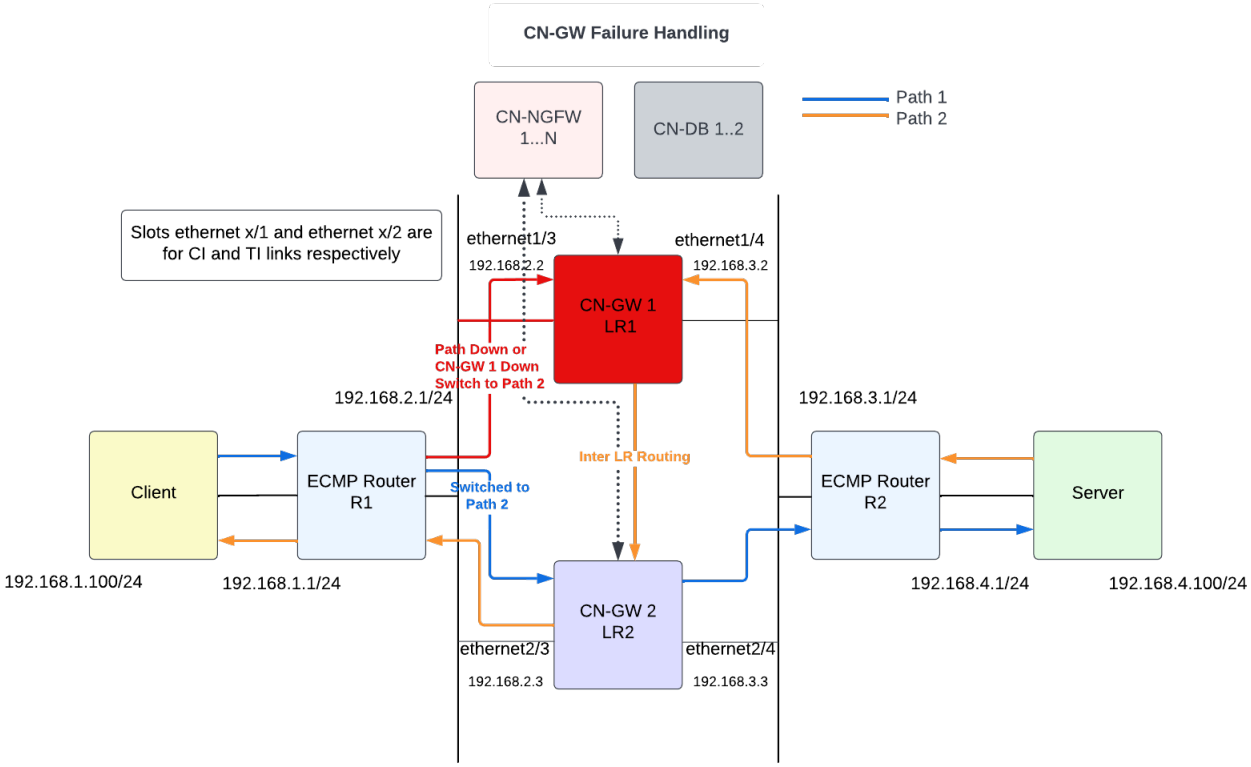
STEP 10 | 为逻辑路由器配置静态路由。

1. 转到 **Network**（网络）> **Routing**（路由）> **Logical Router**（逻辑路由器），然后从 **Template**（模板）下拉列表中选择变量模板。
2. 选择 **Static**（静态）> **IPv4**，然后单击 **Add**（添加）。
3. 输入静态路由的 **Name**（名称）。
4. 输入 **Destination**（目标）路由和网络掩码。例如，192.168.200.0/24。
5. 选择要用于下一个跃点的数据包的出站接口。
6. 对于 **Next Hop**（下一个跃点），请选择 **ip-address** 并输入内部网关的 IP 地址。例如，192.168.100.2。
7. 为路由输入 **Admin Distance**（管理距离），以覆盖此逻辑路由器为静态路由设置的默认管理距离（范围为 10-240；默认值为 10）。
8. 输入路由 **Metric**（跃点数）（范围为 1-65,535）。
9. 将前述步骤中创建的 **BFD Profile**（**BFD** 配置文件）应用到静态路由，这样，如果静态路由失败，防火墙就会删除路由并使用备用路由。
10. 单击 **OK**（确定）。

BFD 配置负责处理 CN-GW 和路径故障。在以下流量流图中，考虑客户端和服务器之间的两个 SSH 会话。会话 1 流经路径 1，会话 2 流经路径 2。如果 CN-GW 1 或路径 1 出现故障，则 R1 和 CN-GW 1、R2 和 CN-GW 1 之间的 BFD 配置可帮助 R1 识别路径故障并通过路径 2 发送流量。面向 R1 的接口必须位于同一个区域中。同样，面向 R2 的接口必须位于同一个区域中。

路由 1：目标：客户端子网；下一跃点是 R1，指标 10

路由 2：目标：服务器子网；下一跃点是 LR2，指标 11

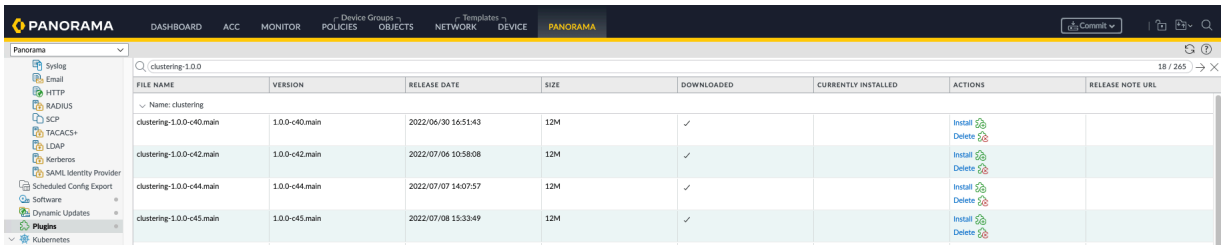


查看 CN 系列 HSF 摘要和监控信息

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

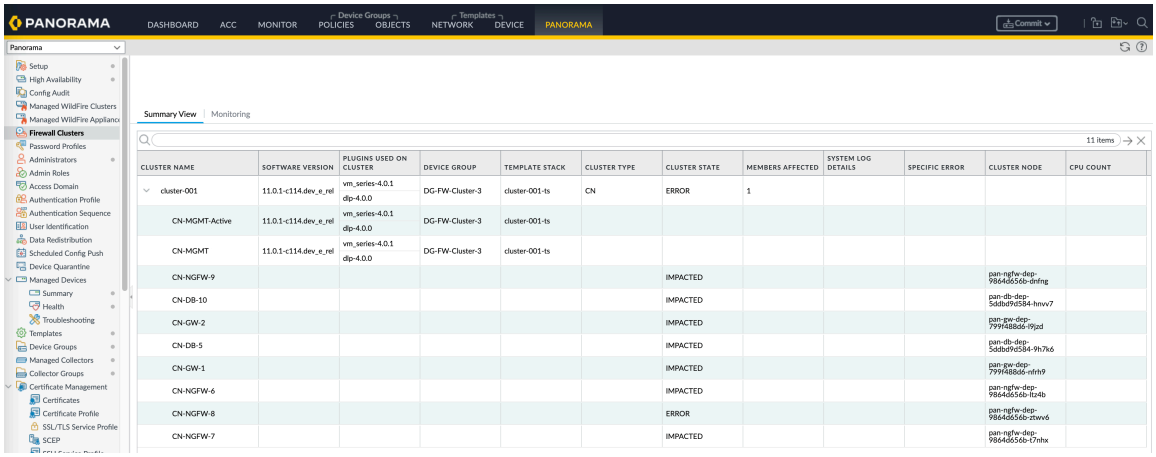
您可以在 Panorama Web 界面的 **Firewall Clusters**（防火墙集群）选项卡下查看 CN 系列 HSF 的摘要和监控信息。要查看和访问防火墙集群，您必须从 **Panorama** > **Admin Roles**（管理角色）**Web UI** > **Enable**（启用） > **Firewall Clusters**（防火墙集群）。有关详细信息，请参阅配置管理员角色配置文件。

您必须从 **Panorama** > **Plugins**（插件）安装 Clustering 1.0.0 插件才能在 **Firewall Clusters**（防护墙集群）下查看集群详细信息。



摘要视图

查看最近五分钟内防火墙获取的 CN 系列集群信息。单击刷新按钮以加载最新的详细信息。

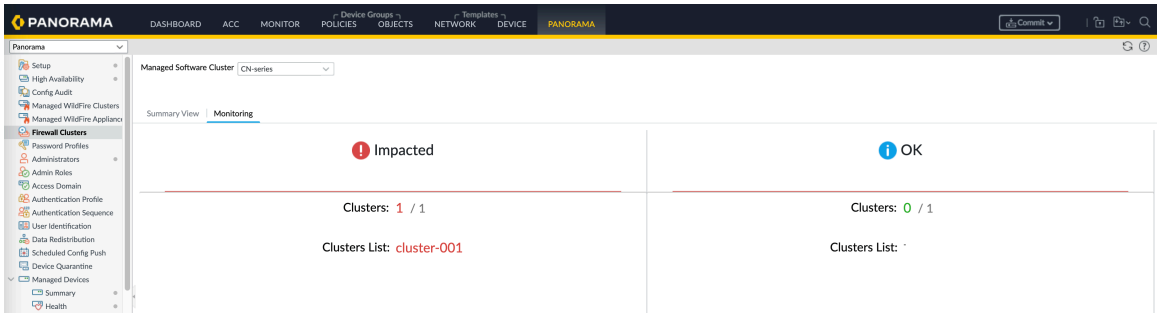


字段	说明
群集名称	防火墙集群的名称。

字段	说明
软件版本	PAN-OS 版本。
集群上使用的插件	集群上使用的插件列表。 仅支持 *CN* 系列防火墙插件。
模板堆栈	与集群关联的模板堆栈的名称。
设备组	与集群关联的设备组的名称。
集群状态	显示集群是否受影响。
群集类型	集群的类型。 仅支持 *CN* 系列防火墙集群类型。
受影响的成员	受影响的集群成员数量及其名称。
系统日志详细信息	显示系统事件的详细信息。
具体错误	集群中特定错误的列表。在 **Monitor**（监控）> **Logs**（日志）> **System**（系统）下单击链接以查看有关错误的更多详细信息，其中可以查看日志。
集群节点	对等的名称。
CPU 计数	使用的 CPU 数量。

监控

查看 CN 系列防火墙集群运行状况信息。



字段	说明
托管软件群集	选择防火墙集群。 仅支持 *CN* 系列防火墙集群类型。
受影响	受影响防火墙集群的列表。 • **CN-Clusters**（**CN** 集群） — 受影响 CN 系列防火墙集群的数量。 • **Clusters Impacted**（受影响的集群）— 显示受影响集群的列表。 单击可在 **Interconnect Status**（互连状态）和 **Cluster Utilization**（集群利用率）指示板中查看有关集群的详细信息。
正常	未受影响的防火墙集群的列表。 • **Clusters**（集群）— 未受影响的 CN 系列防火墙集群的数量。 • **Clusters List**（集群列表）— 显示未受影响的集群的列表。 单击可在 **Interconnect Status**（互连状态）和 **Cluster Utilization**（集群利用率）指示板中查看有关集群的详细信息。

互连状态	查看所选时间范围内的集群互连详细信息。
	选择 **Last 5 Mins**（过去 **5** 分钟）以查看以下详细信息。
	• **Cluster Name**（集群名称）— 防火墙集群的名称。
	• **Cluster Type**（集群类型）— 集群的类型。
	仅支持 *CN* 系列防火墙集群类型。
	• **Cluster Creation Time**（集群创建时间）— 集群创建时间。
	• **Current Cluster State**（当前集群状态）— 显示集群是否受影响。
	  • **Current Cluster Detail**（当前集群详细信息）— 单击当前集群状态链接可查看有关受影响集群的更多详细信息。
	• **Cluster Interconnect Status**（集群互连状态）— 显示集群相互连接性。
	  • **Current Cluster Detail**（当前集群详细信息）— 单击当前互连状态链接可查看有关受影响集群的更多详细信息。
	• **Traffic Interconnect**（流量互连）— 流量互连的状态。
	• **External Connection**（外部连接）— 外部连接的状态。
	• **Impacted Links**（受影响的链接）— 受影响的链接数。
	• **Management Connectivity**（管理连接）— 管理连接数。

字段	说明
	• **Impacted Cluster Member**（受影响的集群成员）— 受影响的集群成员列表。 • **Time Stamp Hi-Res Uptime**（时间戳高解析度正常运行时间）— 正常运行时间时间戳。 • **Time Stamp Hi-Res Downtime**（时间戳高解析度停机时间）— 停机时间戳。 如果选择任何其他时间范围，则仅显示以下信息。 • 群集名称 • 群集类型 • 群集创建时间 • 当前集群状态 • 集群互连状态 • 流量互连 • 外部连接
群集利用率	查看整个防火墙集群、内存和数据利用率。 • **Cluster Name**（集群名称）— 防火墙集群的名称。展开集群名称会显示集群中所有 Pod 的详细信息。 • **Cluster Details**（集群详细信息）— 单击集群名称链接可查看所选集群的吞吐量、内存和数据利用率详细信息。 • **Cluster Type**（集群类型）— 集群的类型。 仅支持 *CN* 系列防火墙集群类型。 • **Cluster State**（集群状态）— 显示集群的运行状况。 • **Cluster Throughput (gbps)**（集群吞吐量 **(gbps)**）— 防火墙集群的吞吐量 (Gbps)。 • **CPS** — 每秒连接数。 • **Session Count (Sessions)**（会话计数）— 会话数。 • **Average Data Plane (%) Within Health Threshold**（运行状况阈值内的平均数据平面百分比）— 以百分比表示的平均数据平面阈值。 • **Management Plane CPU (%)**（管理平面 **CPU** 百分比）— 管理平面 CPU 利用率的百分比。 • **Management Plane Mem (%)**（管理平面内存百分比）— 管理平面内存利用率的百分比。

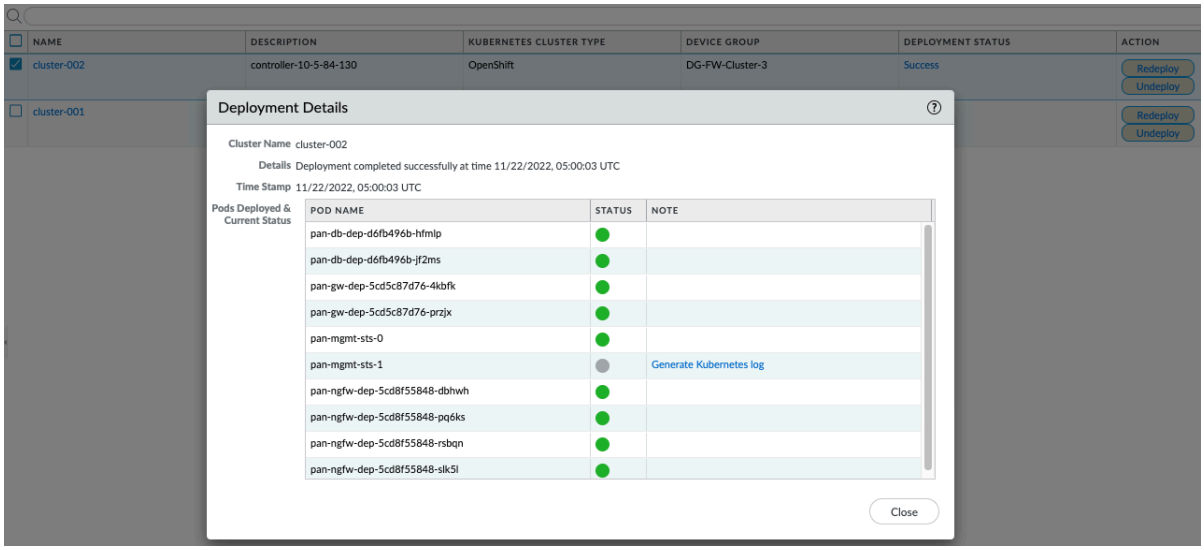
字段	说明
	• **Logging Rate (Log/Sec)**（以日志数/秒为单位的日志记录速率）— 集群上生成日志的速率。 • **DP Auto-Scale Status**（**DP** 自动缩放状态）— 数据平面自动缩放详细信息。

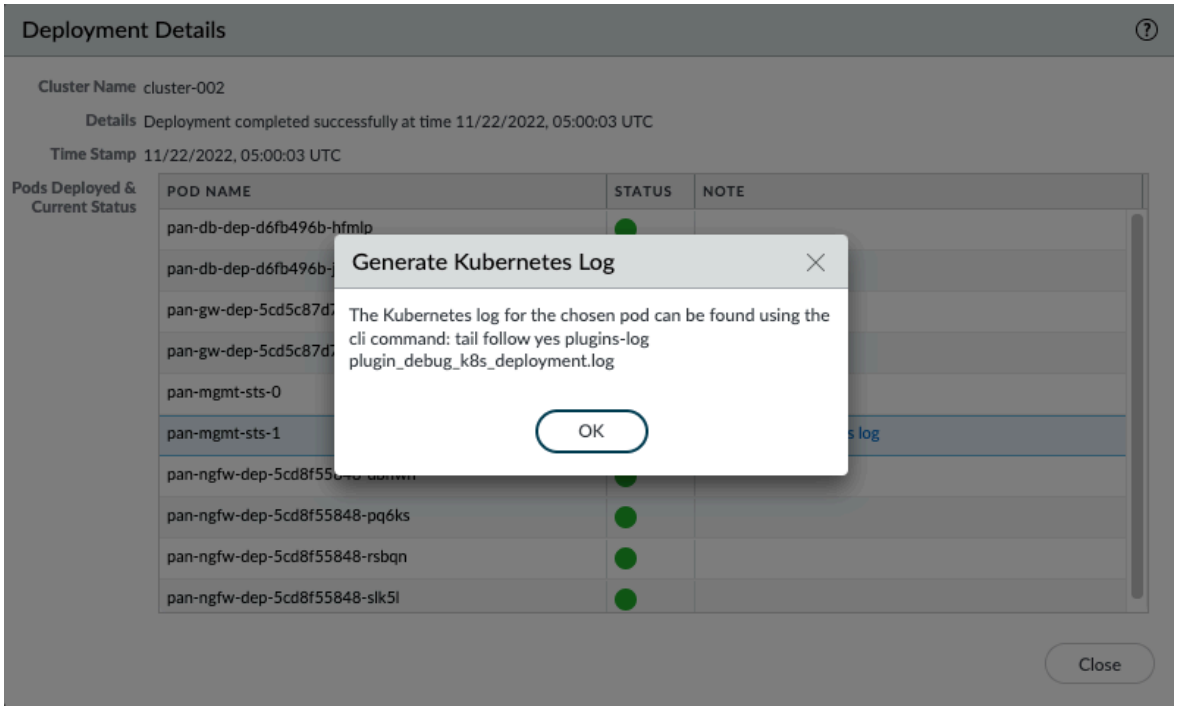
验证 CN 系列 HSF 部署

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

您可以在 **Panorama** > **Kubernetes** 下的 **Deployment**（部署）部分验证 CN 系列 HSF 部署。单击 **Deployment Status**（部署状态）下的链接以查看部署的详细信息。

已部署的 Pod 及其当前状态以颜色编码并显示在 **Deployment Status**（部署状态）部分。在 **Note**（注释）下，您可以单击失败的 Pod 部署的链接以查看更多详细信息。





在 Panorama CLI 中使用以下命令生成日志。

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

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

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

调试 **Kubernetes** 插件和 **CN** 系列 **HSF** 之间的同步问题

Kubernetes 插件使用 Watch API 从 Pod、服务和节点收集有关 CN 系列 HSF 的信息。Watch API 是一种基于通知的 API，它会在集群状态发生变化时发送更新。为确保插件和部署的 CN 系列 HSF 同步，插件会监听通知并显示 HPA 和升级/降级事件通知。

该插件使用以下调试命令，根据插件状态来调试特定节点。

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

该调试命令会生成一个日志文件，其中包含在命令中传递的节点的 `kubectl` 描述日志。该日志保存在插件日志文件中。

EKS 环境中使用 KEDA 的基于自定义指标的 HPA

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

EKS 环境中的 HPA 实施需要使用 KEDA（基于 Kubernetes 的事件驱动 Autoscaler）。以下是基于自定义指标的 HPA 实施的先决条件：

- 从 YAML 为集群启用 HPA。
  - 确保将 HPA 参数填写在 pan-cn-mgmt-configmap.yaml 文件中。
  - 确保 `PAN_NAMESPACE_EKS` 字段在您所在区域的 AWS 帐户中具有唯一名称。这样可以避免覆盖不同 CN 集群中具有相同 EKS 命名空间的指标。
- CN-MGMT 向 Cloudwatch 发布指标。

  CN-MGMT Pod 需要必要的权限才能访问 Cloudwatch 资源、收集 CN-NGFW 指标并将自定义指标发布到 Cloudwatch。这是通过将 `CloudWatchFullAccess` 策略添加到创建节点组时指定的节点 IAM 角色来完成的。
- 从 AWS 部署 Cluster Autoscaler。有关详细信息，请参阅集群 Autoscaler。

使用 AWS 对 KEDA 进行身份验证

要对 KEDA 进行身份验证，您可以通过在 KEDA 服务帐户中注释 role-arn 来将 IAM 角色与 KEDA 操作员服务帐户相关联。建议执行此步骤，因为这这样可以避免向节点 IAM 角色添加 Cloudwatch 访问权限，并且仅允许 KEDA 服务帐户访问 Cloudwatch，而不是运行 KEDA 的整个节点。

将 IAM 角色与 KEDA 操作员服务帐户相关联：

1. 为集群创建一个 IAM OIDC 提供程序 — 只需为一个集群创建一次 IAM OIDC 提供程序。
2. 创建 IAM 角色并使用服务帐户所需的权限将 IAM 策略附加到该角色。确保在执行此步骤时提供 Cloudwatch 访问策略。
3. 将 IAM 角色与服务帐户相关联 — 为需要访问 AWS 资源的每个 Kubernetes 服务帐户完成此任务。
4. 从 AWS 部署 Cluster Autoscaler。有关详细信息，请参阅集群 Autoscaler。

部署 KEDA Pod

要部署 KEDA Pod，请下载最新的 KEDA 文件。

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

该插件根据您视扩展需求而提供的输入修改并应用 yaml。

观察 Cloudwatch 控制台中的值，并检查目标 Pod 如何扩展和缩小。

在 CN 系列 HSF 中配置动态路由

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• 最低运行 PAN-OS 11.1 版本的 Panorama

CN 系列超大规模安全结构 **(HSF)** 现在通过 BGP 和 BGP over BFD 协议引入了动态路由。使用动态路由，您可以通过可跨逻辑路由器使用的基于配置文件的过滤列表和条件路由图实现稳定、高性能和高可用性的第 3 层路由。这些配置文件的粒度更精细，可以筛选每个动态路由协议的路由、改进跨多个协议的路由重新分发。

BGP 寻找可传输数据的可用路径并根据自治系统内可用的 IP 前缀选择最佳路由。双向转发检测 (BFD) 配置管理 CN-GW Pod 和路径故障。

要启用动态路由，您需要配置 Panorama 和 CN-Series HSF 集群。集群中至少需要 2 个 CN-MGMT、2 个 CN-NGFW、2 个 CN-DB 和 1 个 CN-GW。在 CN 集群和外部路由器之间配置 BGP 对等连接。

在 *CN* 系列 *HSF* 上，*PANOS 11.xx* 将支持动态路由有关获取 *PAN-OS 11.0* 的信息，请参阅获取 CN 系列部署的映像和文件。

在 Panorama 中，您需要配置设备组并通过设备组管理 HSF 集群。要配置 HSF 集群，请参阅部署 HSF 集群。

要在 HSF 集群上配置 BGP，您需要执行以下步骤：

1. 启用高级路由。
2. 配置逻辑路由器。
3. 为 CN-GW 环回接口创建静态路由。
4. 在高级路由引擎上配置 BGP。

   1. 目前，*BGP* 路由仅支持 *IPv4*。
   2. 创建对等时，请确保创建环回会话并在寻址选项卡中为每个 *CN-GW* 提供一个环回 *IP* 地址。
5. （可选）为身份验证、计时器、地址系列、抑制、路由重新分配到 BGP 以及 BGP 过滤创建 BGP 路由配置文件。
6. （可选）为高级路由引擎创建过滤器，例如访问列表、前缀列表、AS 路径访问列表、社区列表和路由图。
7. 单击 **Commit to Panorama**（提交到 **Panorama**）。将配置提交给 Panorama 后，BGP 将配置到每个 CN-GW。

要检查 BGP 状态，请登录 CN-MGMT 并执行以下命令：

- 显示高级路由 BGP 摘要

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

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

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

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

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



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

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

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

- 显示高级路由 BGP 对等状态

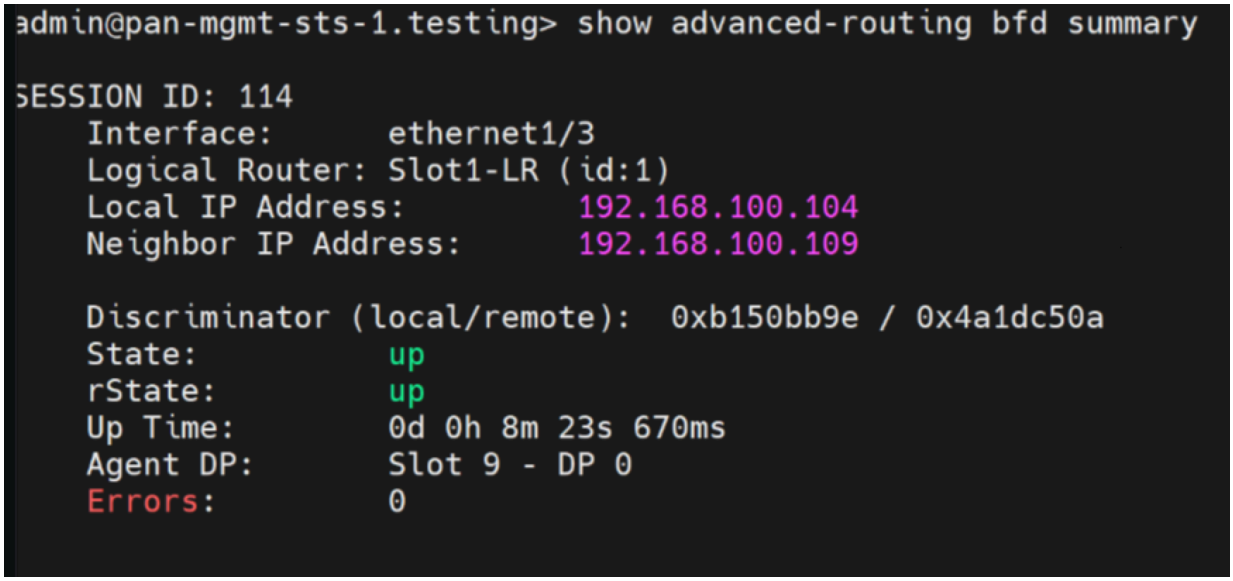
```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer status peer-name DHCP-PEER

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

- 显示高级路由 BGP 对等体详细信息

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

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

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

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

要从 CN-MGMT 检查 BFD 状态，请执行以下命令

- 显示高级路由 BFD 摘要



- 显示高级路由 BFD 详细信息

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

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

    BFD profile:                default

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

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

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

CN 系列 HSF：用例

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

以下是 CN-系列 HSF 的用例：

- 5G 流量测试
  - 具有 N3+N4 可见性和关联策略的 5G 安全性
  - 通过应用程序识别和威胁检查实现入站/出站保护
- 支持基于自定义指标横向扩展防火墙
- 测试用例：CN-MGMT 故障处理
- 测试用例：CN-NGFW 故障处理
- 测试用例：CN-DB 故障处理

5G 流量测试

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 • Helm 3.6 or above version client

保护网络边缘需要对流量检查和控制（安全要求）与高带宽、低延迟和实时访问（用户体验）进行平衡。如果流量由许多防火墙进行处理，应用程序托管在边缘站点上，或者网络边缘是 IoT 数据的聚合点，那么这些问题将变得更加难以解决。此外，5G 网络中用户和控制平面的分离导致难以在用户或设备级别应用安全策略，而且缺乏基于上下文的威胁可见性。使用 N3 和 N4 接口部署的防火墙提供：

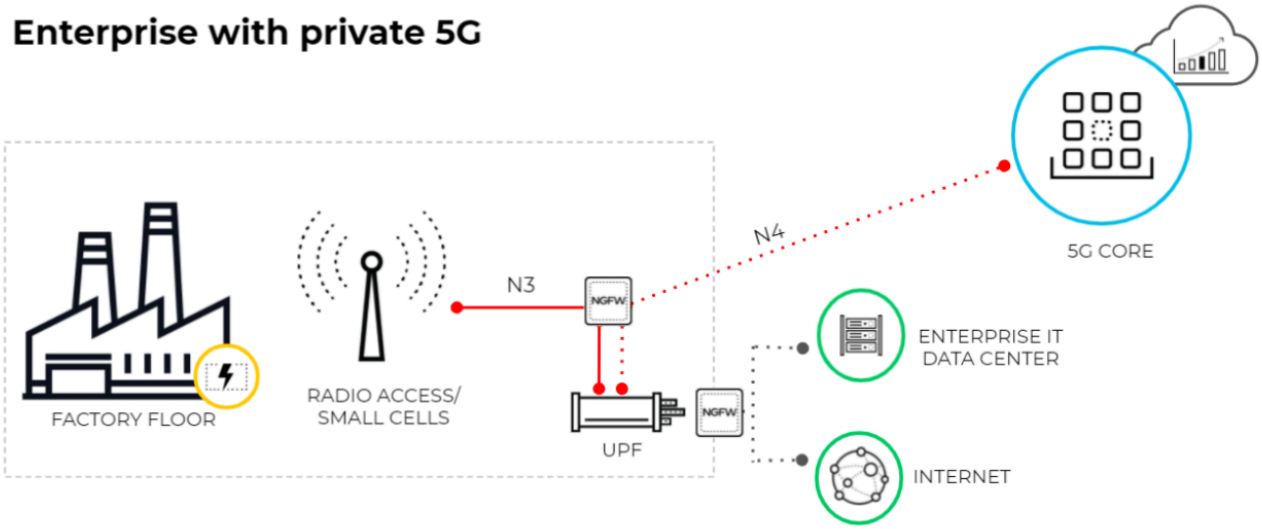
- 相互连接的设备之间的信号级别可见性
- PFCP 和 GTP-U 状态检查
- 将订户 ID/设备 ID /切片 ID 与 GTP-U 流量漏洞相关联

以下是 CN 系列 HSF 的 5G 流量用例：

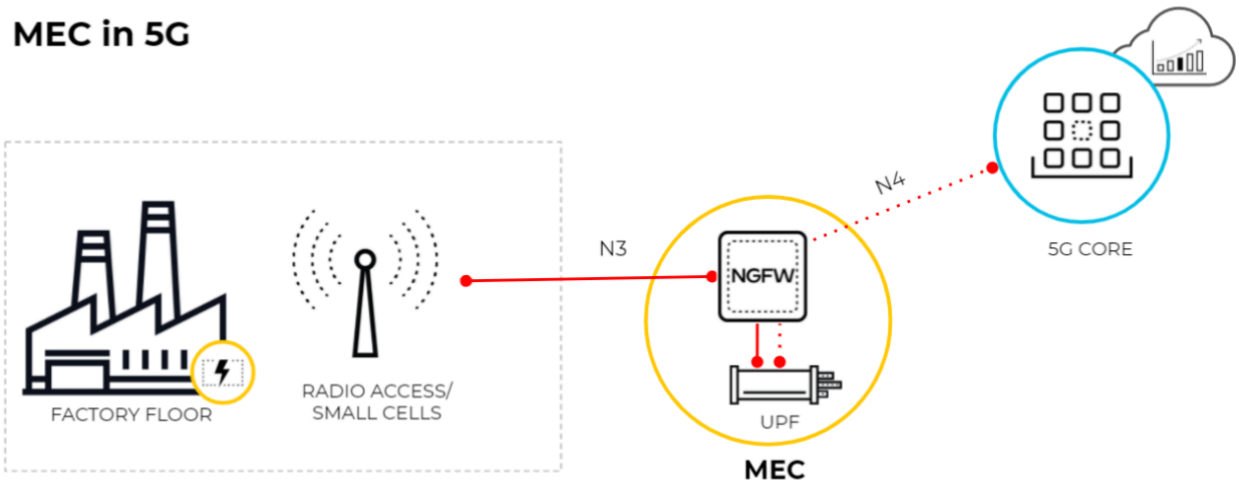
- 具有 N3+N4 可见性和关联策略的 5G 安全性

- 通过应用程序识别和威胁检查实现入站/出站保护

下图说明了使用私有 5G 网络的企业。5G 核心功能基于云或在服务提供商的中心站点。5G 接入与 UPF 之间的连接使用 N3 接口。GTP-U 隧道承载 N3 接口上的用户平面流量。UPF 与会话管理功能 (SMF) 之间的连接使用 N4 接口。PFCP 协议在 N4 接口上使用 UDP 交换来交换数据包转发规则。



上图说明了 5G 网络中的 MEC，其中用户平面功能 (UPF) 位于边缘或 MEC 位置，而 5G 核心功能基于云或服务提供商的中心站点。5G 接入与 UPF 之间的连接使用 N3 接口，GTP-U 隧道通过 N3 接口承载用户平面流量。UPF 和 SMF 之间的连接使用 N4 接口，PFCP 协议通过 N4 接口使用 UDP 交换数据包转发规则。



具有 N3+N4 可见性和关联策略的 5G 安全性

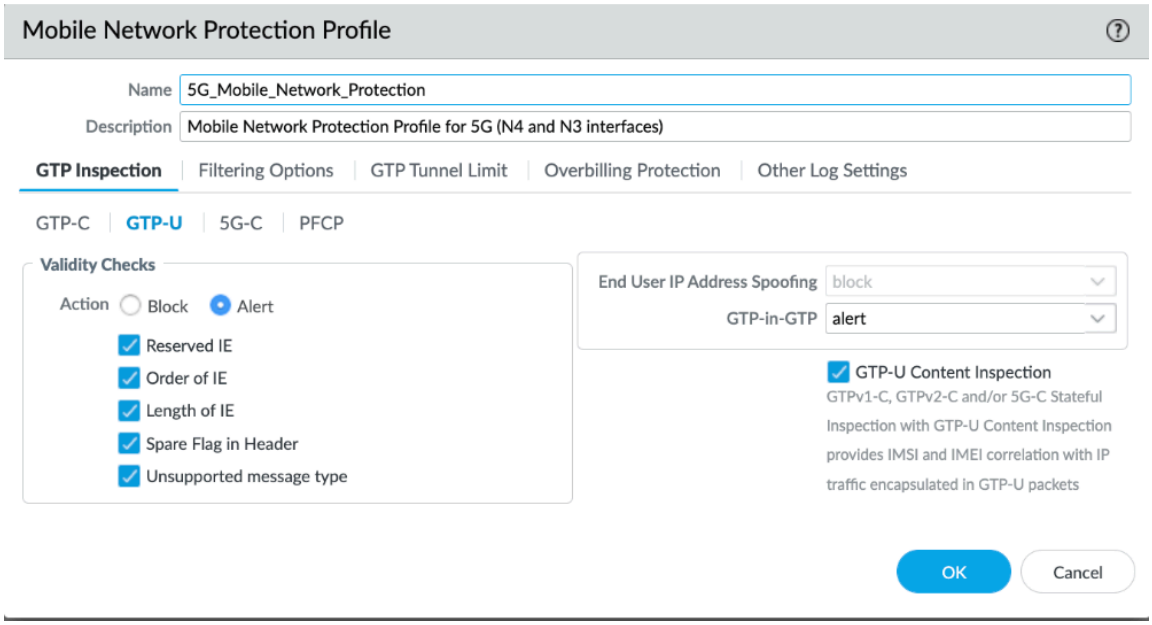
此测试用例评估 CNF 集群检查和保护来自 N3+N4 接口的流量的能力。

STEP 1 | 要检查和保护来自 N3+N4 接口的流量，首先，您需要启用 GTP 安全。

1. 登录到防火墙 Web 界面。
2. 选择 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **General Settings**（常规设置），然后选择 **GTP-U Security**（**GTP-U** 安全）。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。
5. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后选择 **Reboot Device**（重启设备）。

STEP 2 | 创建移动网络保护配置文件并启用 GTP-U 检查。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Mobile Network Protection**（移动网络保护）。
2. **Add**（添加）配置文件并输入 **Name**（名称），如 **`5G_Mobile_Network_Protection`**。
3. 在 **PFCP** 选项卡上，启用 **Stateful Inspection**（状态检查）。



STEP 3 | 选择您希望防火墙对 PFCP 流量执行的状态检查以及防火墙在状态检查不成功时采取的操作。

1. 确定要使用的状态检查。
   - **Check Association Messages**（检查关联消息）— 检查是否存在任何错误或已被拒绝的 PFCP 关联消息。
   - **Check Session Messages**（检查会话消息）— 检查任何无序或被拒绝的 PFCP 会话消息；验证所有 PFCP 会话消息是否匹配现有 PFCP 关联；警告或丢弃在 PFCP 关联建立之前收到的 PFCP 会话消息。
   - **Check Sequence Number**（检查序列号）— 确认 PFCP 响应中的序列号与先前 PFCP 请求消息中的序列号匹配。
2. 如果状态检查不成功，请选择您希望防火墙采取的操作。
   - **Allow**（允许）— 允许流量且不在 GTP 日志中生成日志条目。
   - **Block**（阻止）— 阻止流量并在 GTP 日志中生成高严重性日志条目。
   - **Alert**（报警）—（默认）允许流量并在 GTP 日志中生成高严重性日志条目。

STEP 4 | （可选）为 PFCP 检查配置日志记录。

1. 选择您希望防火墙何时生成日志条目。
   - 在 **PFCP** 关联开始时记录
   - 在 **PFCP** 关联结束时记录
   - 在 **PFCP** 会话开始时记录
   - 在 **PFCP** 会话结束时记录

STEP 5 | 为 PFCP 和 GTP-U 消息启用其他日志设置

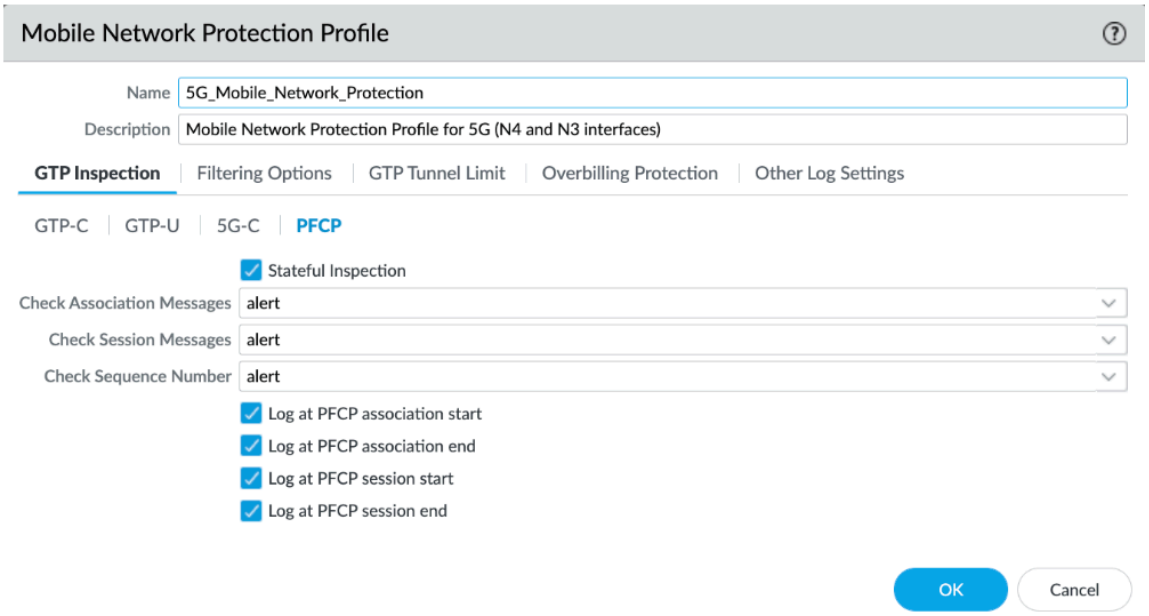
1. 在 **Other Log Settings**（其他日志设置）选项卡上，选择要包含在日志中的 **PFCP Allowed Messages**（**PFCP** 允许的消息）的类型。

   只能为故障排除启用这些选项。

   - **Session Establishment**（会话建立）— 这些 PFCP 消息设置会话，包括建立 GTP-U 隧道。
   - **Session Modification**（会话修改）— 如果会话 ID 或 PDR ID 发生变化（例如，由于从 4G 网络迁移到 5G 网络而发生变化），则会发送这些 PFCP 消息。它包括 PFCP

Session Modification Request（PFCP 会话修改请求）和 PFCP Session Modification Response（PFCP 会话修改响应）之类的消息。

- **Session Deletion**（会话删除）— 这些 PFCP 消息终止 PFCP 会话，包括释放关联的资源。



STEP 6 | 创建两条安全策略，其中源和目的分别为 N3 和 N4 接口，应用程序分别为 GTP-U 和 PFCP。

1. 选择 **Policies**（策略）> **Security**（安全）并按**Name**（名称） **Add**（添加）安全策略规则。
2. 选择 **Source**（源）选项卡并 **Add**（添加） **Source Zone**（源区域）或选择 **Any**（任何）。
3. 对于 **Source Address**（源地址），为 N3 接口上的 5G 元素端点 **Add**（添加）地址对象。
4. 对于 **Destination**（目标），为 N3 接口上的 5G 元素端点 **Add**（添加）**Destination Address**（目标地址）对象。
5. **Add**（添加）要允许的 **Applications**（应用程序），如用户平面，即 **GTP-U** 和 **PFCP**。
6. 在 **Actions**（操作）选项卡上，选择 **Action**（操作），如 **Allow**（允许）。
7. 选择创建的 **Mobile Network Protection**（移动网络保护）配置文件。
8. 选择要应用的其他配置文件，例如 **Vulnerability Protection**（漏洞防护）。
9. 选择日志设置，例如 **Log at Session Start**（会话启动时的日志）和 **Log at Session End**（会话结束时的日志）。
10. 单击 **OK**（确定）。
11. 同样，为 N4 接口创建另一条安全策略。

STEP 7 | （可选）创建另一条基于设备 ID/用户 ID/网络切片 ID 的安全策略规则，通过在源中输入 EDL 信息创建基于保护的安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），并按 **Name**（名称）（如“设备 ID 安全”）**Add**（添加）安全策略规则。
2. 选择 **Source**（源）选项卡并 **Add**（添加） **Source Zone**（源区域）或选择 **Any**（任何）。
3. **Add**（添加）以下任一格式的一个或多个 **Source Equipment**（源设备）ID：
   - 5G 永久性设备标识符 (PEI)，包括 IMEI
   - IMEI（15 或 16 位数字）
   - IMEI 前缀为 8 位数的类型分配代码 (TAC)
   - 用于指定 IMEI 的 EDL
4. （可选）您可以将 **Source Subscriber**（源订户）和 **Network Slice**（网络切片）名称添加到此安全策略规则中，从而进一步细化规则的限制性。
5. 将 **Destination Zone**（目标区域）、**Destination Address**（目标地址）和 **Destination Device**（目标设备）指定为 **Any**（任何）。
6. **Add**（添加）要允许的 **Applications**（应用程序），例如，**ssh**、**ssl**、**radmin** 和 **telnet**。
7. 在 **Actions**（操作）选项卡上，选择 **Action**（操作），如 **Allow**（允许）。
8. 选择要应用的配置文件，例如 **Antivirus**（防病毒）、**Vulnerability Protection**（漏洞防护）和 **Anti-Spyware**（防间谍软件）。
9. 选择日志设置，例如 **Log at Session Start**（会话启动时的日志）和 **Log at Session End**（会话结束时的日志）。
10. 单击 **OK**（确定）。

    预期测试结果：
    - 验证监控部分的 GTP-U 日志。
    - 验证日志的详细信息部分，以查看订户、设备、网络切片信息。
    - 观察规则匹配数的增加。

通过应用程序识别和威胁检查实现入站/出站保护

该测试用例评估 CNF 集群检查和保护 N6 接口上的入站和出站流量的能力。

N6 接口通过 TCP/UDP 向互联网传输明文流量。现在，通过部署在 N6 接口上的 VM 系列防火墙，您可以全面了解应用程序的使用情况。防火墙可以通过 CDSS 订阅实现安全性，如 TP、Adv-URL 过滤、Wildfire 以及针对允许流量的 DNS 安全。

以下步骤是执行此测试用例的概要。有关执行各个步骤的详细信息，请参阅具有 N3+N4 可见性和关联策略的 5G 安全性。

STEP 1 | 使用适当的区域和接口为 N6 接口创建安全策略。

STEP 2 | 使用默认安全配置文件或为 URL 过滤、WildFire、漏洞保护等创建自定义类别。

STEP 3 | （可选）在 URL 类别下为允许的 URL 创建自定义配置文件。

STEP 4 | （可选）创建多个符合不同条件的安全策略。创建安全策略时，选择在步骤 3 中创建的配置文件。

STEP 5 | 发送流量。

STEP 6 | 在入站/出站方向发送恶意流量并验证是否会阻止流量。

预期结果：

- 策略的匹配数增加。
- 检查 URL 过滤、流量和威胁的相应日志。

支持基于自定义指标横向扩展防火墙

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

此测试有助于验证 CN 系列 HSF 集群根据自动扩展中指定的自定义指标值目标进行自动扩展的能力。

STEP 1 | 在创建 CN 系列 HSF 集群时启用自动扩展，以根据自动扩展中指定的自定义指标目标值自动扩展。有关更多信息，请参阅 部署 HSF 集群

STEP 2 | 输入 CloudWatch 命名空间以将指标推送到 AWS CloudWatch。

STEP 3 | 输入 EKS 集群的区域。

STEP 4 | 输入推送时间间隔。

STEP 5 | 选择“自动扩展指标”。在此示例中，您可能希望选择 PansessionActive。

STEP 6 | 指定扩展阈值和缩小阈值。例如，如果您有 2 个 NGFW Pod 正在运行且当前防火墙上的会话总数为 1000，则云监视指标将显示 500（每个 NGFW Pod）。

STEP 7 | 您可以将扩展阈值设置为 250，自动扩展应再增加 2 个 NGFW Pod。

STEP 8 | 在 MGMT Pod 上使用 show session info 命令获取会话信息

STEP 9 | 您可以指定可以自动扩展的最大和最小 NGFW Pod 数。

预期结果：NGFW Pod 应根据扩展阈值自动扩展

测试用例：CN-MGMT 故障处理

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

此测试评估 CN-NGMT 故障处理。

CN 系列 HSF 部署所需的最小 CN-MGMT Pod 数量为两个，以确保进行故障处理。完成部署后，第一个激活的 CN-MGMT Pod 成为 Leader，第二个 CN-MGMT 成为 Follower。两个 CN-MGMT Pod 具有相同的配置。在任何情况下，一个 CN-MGMT Pod 处于“就绪”状态。CN-DB、CN-GW 和 CN-NGFW Pod 通过流量互连 (TI) 链路连接到处于“就绪”状态的 CN-MGMT Pod。

两个 *CN-MGMT Pod* 不处于“*HA* 主动-被动”或“*HA* 主动-主动”模式。两个 *Pod* 具有相同的配置，并使用 *Panorama* 配置。

CN-MGMT Pod 故障是由于以下情况之一而发生的。

- 活性检查失败
  - 如果 `slotd` 关闭
  - 如果 `ipsec` 或 `strongswan` 关闭
- CN-MGMT Pod 崩溃并重新启动

STEP 1 | 在 Panorama CLI 中，输入 `show clusters name`<cluster-name>以查看 Leader 和 Follower CN-MGMT Pod。

以下输出显示 **`pan-mgmt-sts-1`** Pod 处于活动状态。

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

STEP 2 | 从 Kubernetes 控制器 CLI 查看 **pan-mgmt-sts-1** Pod 的集群成员以及 CN-DB、CN-GW 和 CN-NGFW Pod 的状态。

1. 输入 `kubectl get pods -n kube-system` 以查看所有 Pod 的状态。

   输出：

   pan-mgmt-sts-1 处于活动状态。所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已连接到 **pan-mgmt-sts-1**。

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

2. 从 **pan-mgmt-sts-1** 检查集群成员关系。

   进入 **pan-mgmt-sts-1** Pod。

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

   ```
   su - admin
   ```

   使用以下命令检查是否所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已连接到 Leader CN-MGMT Pod。

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

   Output:

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

3. 从 **pan-mgmt-sts-0** 检查集群成员关系。

   进入 **pan-mgmt-sts-0** Pod。

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

   ```
   su - admin
   ```

   使用以下命令检查是否有任何 CN-DB、CN-GW 和 CN-NGFW Pod 连接到 Follower CN-MGMT Pod。

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

   输出：

   ```
   No members info present
   ```


STEP 3 | 测试 CN-MGMT Pod 故障处理。

1. 在 Kubernetes 控制器 CLI 中，输入以下命令以删除 Leader **pan-mgmt-sts-1** Pod。

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

2. 在 Panorama CLI 中，输入 `show clusters name`<cluster-name> 以查看新的 Leader 和 Follower CN-MGMT Pod。

   以下输出显示 **pan-mgmt-sts-0** Pod 现在处于活动状态。

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

STEP 4 | 从 Kubernetes 控制器 CLI 查看 **pan-mgmt-sts-0** Pod 的集群成员以及 CN-DB、CN-GW 和 CN-NGFW Pod 的状态。

1. 输入 `kubectl get pods -n kube-system` 以查看所有 Pod 的状态。

   输出：

   pan-mgmt-sts-0 处于活动状态。所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已连接到 **pan-mgmt-sts-1**。

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

2. 从 **pan-mgmt-sts-0** 检查集群成员关系。

   进入 **pan-mgmt-sts-0** Pod。

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

```
su - admin
```

   使用以下命令检查是否所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已连接到 Leader CN-MGMT Pod。

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

   Output:

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

3. 从 **pan-mgmt-sts-1** 检查集群成员关系。

   进入 **pan-mgmt-sts-1** Pod。

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

   ```
   su - admin
   ```

   使用以下命令检查是否有任何 CN-DB、CN-GW 和 CN-NGFW Pod 连接到 Follower CN-MGMT Pod。

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

   输出：

   ```
   No members info present
   ```

测试结果：当 Leader Pod `pan-mgmt-sts-1` 失败时，Follower Pod `pan-mgmt-sts-0` 会成为新的 Leader。这种 CN-MGMT 故障处理机制可确保通信流量不中断。对现有或新会话没有影响。

测试用例：CN-NGFW 故障处理

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

该测试评估 CN-NGFW 故障处理。

CN-NGFW 故障可能发生在以下情况。

- 节点问题
- CN-NGFW Pod 崩溃并重启
- 节点和 CN-NGFW Pod 没有问题，但 **pan_task** 崩溃了
- 在以下情况下，将从集群成员关系中删除 CN-NGFW：
  - 通过 Eth0 接口的 IPsec 监控失败
  - 集群互连 (CI) 链路已断开
  - 流量互连 (TI) 链路已断开

在此场景中，客户端和服务器之间的 SSH 会话安装在 CN-NGFW 1 上。如果 CN-NGFW 1 关闭，则 SSH 会话必须通过故障转移到另一个 CN-NGFW 来保持活动状态。

STEP 1 | 在 Panorama CLI 中，输入 `show clusters name`<cluster-name> 以查看连接到 CN-MGMT Pod 的 CN-NGFW、CN-DB 和 CN-GW Pod。

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

STEP 2 | 使用命令 `show cluster-membership show-slot-info slot all` 查看 CN-MGMT Pod `an-mgmt-sts-0` 的集群成员详细信息。

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

ethernetx/3 子网的所有接口必须在同一区域中。同样，ethernetx/4 子网的所有接口都必须在同一区域中。

STEP 3 | 使用 `show session all filter application ssh` 查看所有 SSH 会话。

每个会话都有两个流量，一个是从客户端到服务器方向的流量，另一个是从服务器到客户端方向的流量。

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

会话所有者为插槽 11。

You can view the filtered cluster flow details using the following example command.

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

输出：

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

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

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

输出：

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

STEP 4 | 使用命令 `kubectl -n kube-system delete Pod pan-ngfw-dep-5cd8f55848-rsbqn` 删除插槽 11 上的 Pod。

输出：

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

插槽 11 中 CN-NGFW Pod 的会话现在已标记为孤立。

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

STEP 5 | 使用命令 `show session all filter application ssh` 访问 SSH 会话。

防火墙将故障转移到可用的 CN-NGFW Pod 以处理孤立流量。新的会话所有者是插槽 7。

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 805306374 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 805306374 Session 805306374 c2s flow: source:192.168.200.100 [untrust_ei1]
 dst:192.168.250.100 proto:6 sport:48702 dport:22 state:ACTIVE type:FLOW src user: unknown
 dst user: unknown s2c flow: source:192.168.250.100 [trust_ei2] dst:192.168.200.100 proto:6
 sport:22 dport:48702 state:ACTIVE type:FLOW src user: unknown dst user: unknown Slot :7 DP :0
 index(local): :6 start time :Mon Nov 21 21:43:27 2022 timeout :3600 sec time to live :3581 sec
 total byte count(c2s) :1350 total byte count(s2c) :1506 layer7 packet count(c2s) :17 layer7
 packet count(s2c) :11 vsys : vsys1 application : ssh rule :Promoted-session service timeout
```

```
 override(index) :False session to be logged at end :True session in session ager :由 HA 对等
更新的真实会话：False layer7 processing : completed URL filtering enabled :True URL category :
 any session via syn-cookies :False session terminated on host :False session traverses
 tunnel :False session terminate tunnel :False captive portal session :False ingress interface :
 ethernet1/3 egress interface : ethernet1/4 session QoS rule :N/A (class 4) tracker stage
 l7proc : fastpath state none end-reason : unknown
```

集群流量中没有更改。

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

结果：

对现有或新会话没有影响。已在 Panorama 上更新集群成员身份。

测试用例：CN-DB 故障处理

在何处可以使用？	需要提供什么？
• CN 系列 HSF 防火墙部署	• CN-Series 11.0.x or above Container Images • Panorama 运行 PAN-OS 11.0.x 或更高版本

此测试评估 CN-DB 故障处理。CN 系列 HSF 部署的首选 CN-DB Pod 数量为两个。两个 CN-DB 具有相同的配置。

当 CN-DB 1 长时间停机时，CN-DB 2 会处理现有会话并建立新会话。当 CN-DB 1 再次启动时，它会检查现有会话的会话同步状态，查找并拆卸，然后设置新会话。

STEP 1 | 使用命令 `show cluster-membership show-slot-info slot all` 查看 CN-MGMT Pod 的集群成员详细信息。

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


STEP 2 | 删除插槽 6 中的 CN-DB Pod。

1. 使用命令 `show clusters name cluster-001` 从 Panorama CLI 获取插槽 6 上的 CN-DB Pod 名称。

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

2. 在控制器 CLI 中，输入命令 `kubectl delete pod pan-db-dep-7b6f6c5458-4tvpq -n kube-system` 以删除插槽 6 中的 CN-DB Pod。

   现在，插槽 6 中的 CN-DB Pod 已删除。

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

3. 使用命令 `show cluster-flow all` 检查集群流量。

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

   现在，带 CN-DB Pod 的插槽 6 处于 PREPARE 状态且 CI 链路已关闭。

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

STEP 3 | 输入 `show cluster-membership show-slot-info slot all`，直到 CN-DB Pod 再次激活。

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

STEP 4 | 使用命令 `show cluster-flow all` 再次检查集群流量。

```
------------------------------------------------------------------------------ Slot 5
 ------------------------------------------------------------------------------ Id State Type
```

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

- `show cluster-flow all filter count yes`

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

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

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

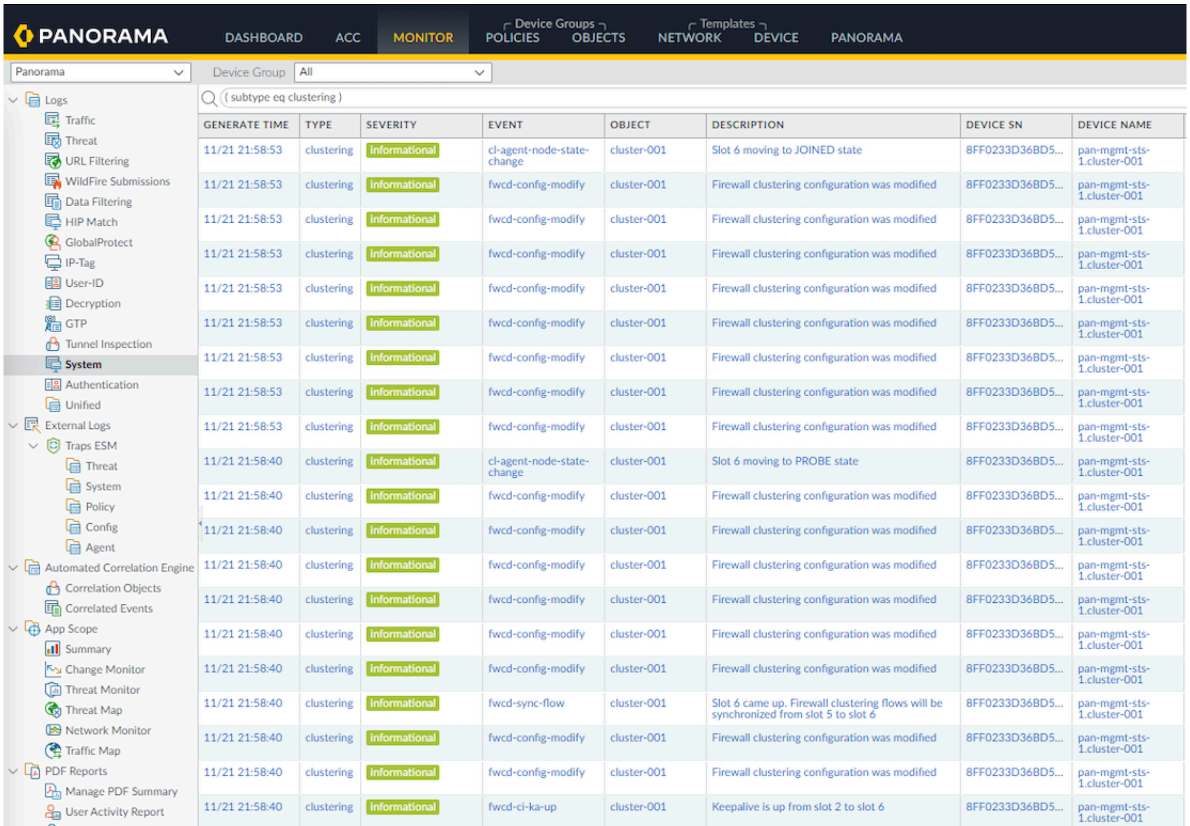
- 从 Panorama CLI

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

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

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

您可以在 **Monitor**（监视） > **Logs**（日志） > **System**（系统）下的 Panorama Web 界面中查看 CN-DB 更改



结果：

对现有或新会话没有影响。已在 Panorama 上更新集群成员身份。

CN 系列不支持的功能

除非下文另有说明，否则 PAN-OS 支持的以下功能不适用于 CN 系列：

功能	DaemonSet	K8s 服务	CNF 模式	HSF 模式
身份验证	否	否	否	否
将日志转发至 Cortex Data Lake	否	否	否	否
企业 DLP	否	否	否	否
非 vWire 接口	否	否	是	是
IoT Security	否	否	否	否
IPv6	是	否	是	否
NAT	否	否	是	否
基于策略的转发	否	否	是	否
QoS	否	否	否	否
SD-WAN	否	否	否	否
User-ID	否	否	否	否
WildFire Inline ML	否	否	否	否
SaaS 内联	否	否	否	否
IPSec	否	否	否	否
隧道内容检测	否	否	否	否