公共云中的威胁防御虚拟部署集群

通过集群，您可以将多台 Threat Defense Virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。使用以下公共云频台，您可以在公共云中部署 Threat Defense Virtual 集群：

- Amazon Web Services (AWS)
- Google 云平台 (GCP)

目前仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅不支持的功能和群集，第 39 页。

关于公共云中的 Threat Defense Virtual 群集

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 Threat Defense Virtual 能够通过集群控制链路发送广播/组播消息。
- 负载均衡器 - 对于外部负载均衡，您有以下选择（具体取决于公共云）：
  - AWS 网关负载均衡器

    AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Threat Defense Virtual 支持使用 Geneve 接口单臂代理且具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。
  - 本地 GCP 负载均衡器，内部和外部
  - 使用内部和外部路由器（例如思科云服务路由器）的等价多路径路由 (ECMP)

    ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 威胁防御 故障会导致问题；如果继续使用该路由，发往故障 威胁防御 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 威胁防御 使之加入动态路由。

注释 负载均衡不支持第 2 层跨区以太网通道。

单个接口

您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的本地 IP 地址。必须仅在控制节点上配置接口配置，并且每个接口都要使用 DHCP。

注释 不支持第 2 层跨区以太网通道。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 首次创建集群时，您可以指定要成为控制节点的节点，因为它是添加到集群的第一个节点，所以它将成为控制节点。

集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅配置 VXLAN 接口。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规threat defense virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，threat defense virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

管理网络

您必须使用管理接口来管理每个节点；集群不支持从数据接口进行管理。

Threat Defense Virtual 集群的许可证

每个 threat defense virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 管理中心时，您可以指定要用于该集群的功能许可证。您可以在 **设备** > **设备管理** > **集群** > **许可证** 区域中修改集群的许可证。

注释 如果在 管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

Threat Defense Virtual 群集的要求和必备条件

型号要求

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100

注释 FTDv5 和 FTDv10 不支持 Amazon Web 服务 (AWS) 网关负载均衡器。

- 以下公共云服务：
  - Amazon Web Services (AWS)
  - Google 云平台 (GCP)
- 最多 16 个节点

另请参阅 Cisco Secure Firewall Threat Defense Virtual 入门指南中的 Threat Defense Virtual 一般要求。

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件和软件要求

集群中的所有设备：

- 必须在同一个性能层。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 必须从管理接口访问 管理中心；不支持数据接口管理。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。
- 集群中的所有设备都必须部署在同一可用性区域中。
- 所有设备的集群控制链路接口必须位于同一子网中。

MTU

确保连接到集群控制链路的端口配置了正确（更高）的 MTU。如果存在不匹配的 MTU，则集群形成将失败。默认情况下，集群控制链路 MTU 会被设置为比数据接口高 154 字节。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）加上 VXLAN 开销（54 字节）。

对于具有 GWLB 的 AWS，数据接口使用 Geneve 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将源接口 MTU 设置为网络 MTU + 306 字节。因此，对于标准的 1500 MTU 网络路径，源接口 MTU 应为 1806，而集群控制链路 MTU 应为 +154, 1960。

下表显示了集群控制链路 MTU 和数据接口 MTU 的默认值。

表 *1:* 默认 *MTU*

公共云	集群控制链路 MTU	数据接口 MTU
具有 GWLB 的 AWS	1960 年	1806
AWS	1654	1500
GCP	1554	1400

Threat Defense Virtual 群集的准则

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

其他准则

- 将节点添加到现有集群时或重新加载节点时，会有限地暂时丢弃数据包/断开连接；这是预期的行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 请勿在节点上禁用集群之前关闭该节点。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要与新节点建立新的连接。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。
- 不支持动态扩展。
- 则在 AWS 上部署集群时不支持状态目标故障切换。
- 在每个维护窗口完成后执行全局部署。
- 确保不要一次从自动扩展组 (AWS)/实例组 (GCP)中删除多个设备。我们还建议您先在设备上运行 **cluster disable** 命令，然后再从组东扩展组 (AWS) / 实例组 (GCP)中删除设备。
- 如果要禁用集群中的数据节点和控制节点，我们建议您在禁用控制节点之前禁用数据节点。如果在集群中有其他数据节点时禁用了某个控制节点，则必须将其中一个数据节点升级为控制节点。请注意，角色更改可能会干扰集群。
- 在本指南中提供的自定义 Day 0 配置脚本中，您可以根据需要更改 IP 地址，提供自定义接口名称，并更改 CCL-Link 接口的顺序。
- 为管理中心虚拟配置安全防火墙规则或安全组时，必须在源 IP 地址范围中包括 Threat Defense Virtual 的专用和公共 IP 地址。此外，请确保在 Threat Defense Virtual的安全防火墙规则或安全组中指定 Management Center Virtual 的专用和公共 IP 地址。这对于确保在集群部署期间正确注册节点非常重要。

集群默认设置

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。

- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

在 AWS 中部署集群

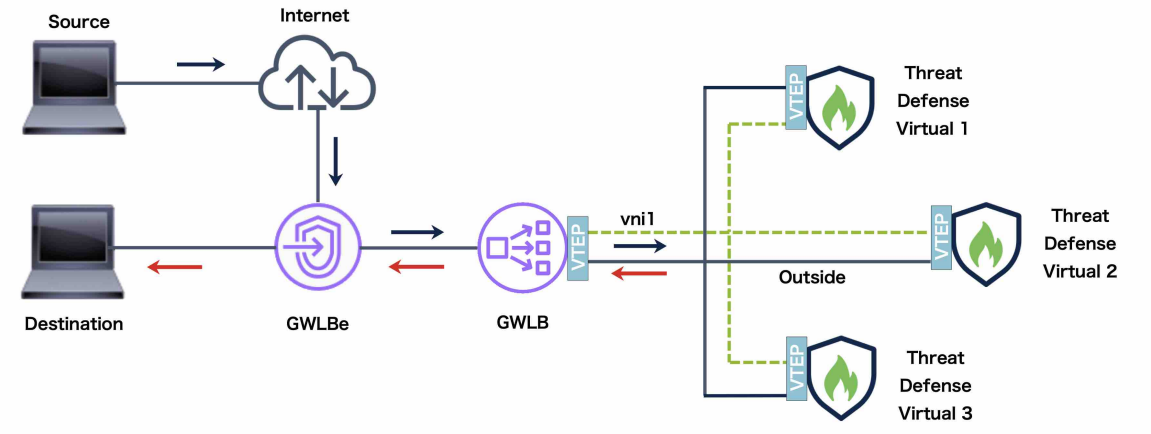
要在 AWS 中部署集群，您可以手动部署或使用 CloudFormation 模板来部署堆栈。您可以将集群与 AWS 网关负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

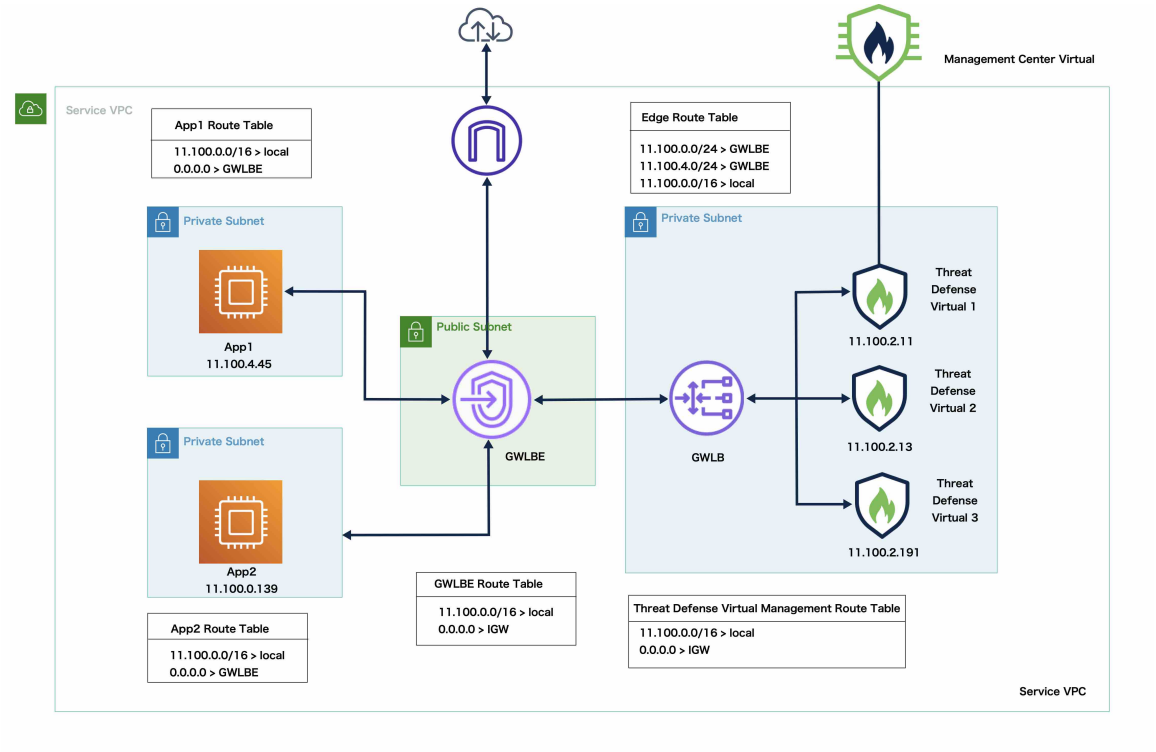
AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Threat Defense Virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个 Threat Defense Virtual 流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *1: Geneve* 单臂代理



拓扑示例

下面给出的拓扑描述了入站和出站流量。集群中有三个连接到 GWLB 的 Threat Defense Virtual 实例。Management Center Virtual 实例用于管理集群。



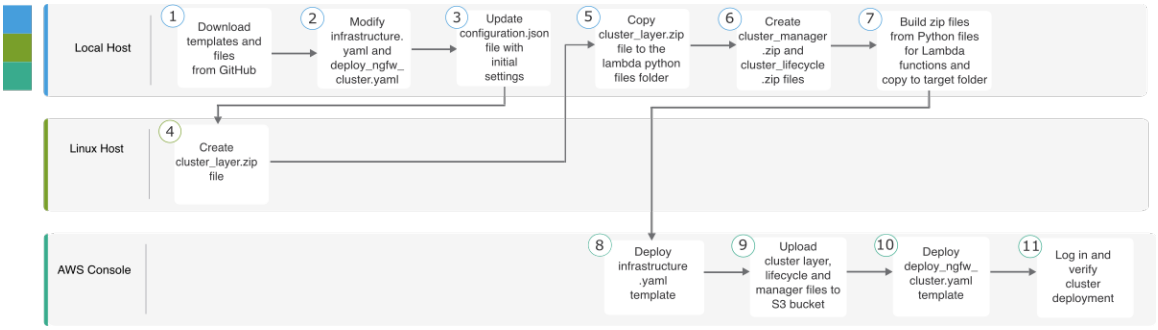
来自互联网的入站流量进入 GWLB 终端，然后由 GWLB 终端将流量传输到 GWLB。然后，流量被转发到威胁防御虚拟集群。集群中的 Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机 App1/App2。

来自 App1/App2 的出站流量将传输到 GWLB 终端，然后由 GWLB 终端发送到互联网。

在 AWS 上部署威胁防御虚拟集群的端到端流程

基于模板的部署

以下流程图说明了在 AWS 上基于模板部署威胁防御虚拟集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	修改 *infrastructure.yaml* 和 *deploy_ngfw_cluster.yaml* 模板。
3	本地主机	使用初始设置来更新 *Configuration.json* 文件。
4	Linux 主机	创建 *cluster_layer.zip* 文件。
5	本地主机	将 *cluster_layer.zip* 文件复制到 Lambda python files 文件夹。
6	本地主机	创建 *cluster_manager.zip* 和 *cluster_lifecycle.zip* 文件。
7	本地主机	从 Python 文件为 Lambda 函数构建 zip 文件，并复制到目标文件夹。
8	AWS 控制台	部署 *Infrastructure.yaml* 模板。
9	AWS 控制台	将 cluster_layer.zip、cluster_lifecycle.zip 和 cluster_manager.zip 上传 S3 存储桶。
10	AWS 控制台	部署 *deploy_ngfw_cluster.yaml* 模板。
11	AWS 控制台	登录并验证集群部署。

手动部署

以下流程图说明了在 AWS 上手动部署威胁防御虚拟集群的工作流程。

	工作空间	步骤
1	本地主机	创建 AWS 的 Day0 配置
2	AWS 控制台	部署威胁防御虚拟实例。
3	AWS 控制台	将接口连接到实例。
4	AWS 控制台	验证节点是否已加入集群。
5	AWS 控制台	创建目标组和 GWLB；将目标组附加到 GWLB。
6	AWS 控制台	使用数据接口 IP 向目标组注册实例。
7	管理中心	注册控制节点。

模板

以下提供的模板可在GitHub中获取。参数值一目了然，包括模板中给出的参数名称、默认值、允许值和说明。

- Infrastructure.yaml - 基础设施部署模板。
- deploy_ngfw_cluster.yaml - 用于集群部署的模板。

注释 在部署集群节点之前，请确保检查支持的 AWS 实例类型列表。此列表可在 *deploy_ngfw_cluster.yaml* 模板中的参数 InstanceType 的允许值下找到。

使用 CloudFormation 模板在 AWS 中部署堆栈

使用自定义 CloudFormation 模板在 AWS 中部署堆栈。

开始之前

- 您需要一台安装了 Python 3 的 Linux 计算机。
- 要允许集群自动注册到 管理中心，您需要在 管理中心 上创建一个具有管理权限且可以使用 REST API 的用户。请参阅《Cisco Secure Firewall Management Center 管理指南》。
- 在 管理中心 中添加与您在 Configuration.JSON 中指定的策略名称匹配的访问策略。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws。

b) 使用所需的参数修改 **infrastructure.yaml** 和 **deploy_ngfw_cluster.yaml**。

c) 使用初始设置修改 **cloud-clustering/ftdv-cluster/lambda-python-files/Configuration.json**。

例如：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- 将 fmcIpforDeviceReg 设置保留为 DONTRESOLVE。
- fmcAccessPolicyName 需要与 管理中心 上的访问策略匹配。

注释 不支持 FTDv5 和 FTDv10 层。

d) 创建名为 **cluster_layer.zip** 的文件，为 Lambda 函数提供必要的 Python 库。

您可以在 Linux 环境中创建 cluster_layer.zip 文件 - 安装了 Python 3.9 的 Ubuntu 18.04。

运行以下 shell 脚本以创建 cluster_layer.zip：

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install pycryptodome==3.17.0
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install cffi==1.15.1
pip3 install zipp==3.1.0
pip3 install importlib-metadata==1.6.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r cluster_layer.zip ./python
deactivate
```

e) 将生成的 cluster_layer.zip 文件复制到 lambda python files 文件夹。

f) 创建 **cluster_manager.zip** 和 **cluster_lifecycle.zip** 文件。

可以在克隆存储库中找到 **make.py** 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。

```
python3 make.py build
```

步骤 2 部署 **Infrastructure.yaml** 并记下集群部署的输出值。

a) 在 AWS 控制台上，转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **infrastructure.yaml**。

c) 点击**下一步 (Next)** 并提供所需的信息。

d) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

e) 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **BucketName**。

图 *2: infrastructure.yaml* 的输出

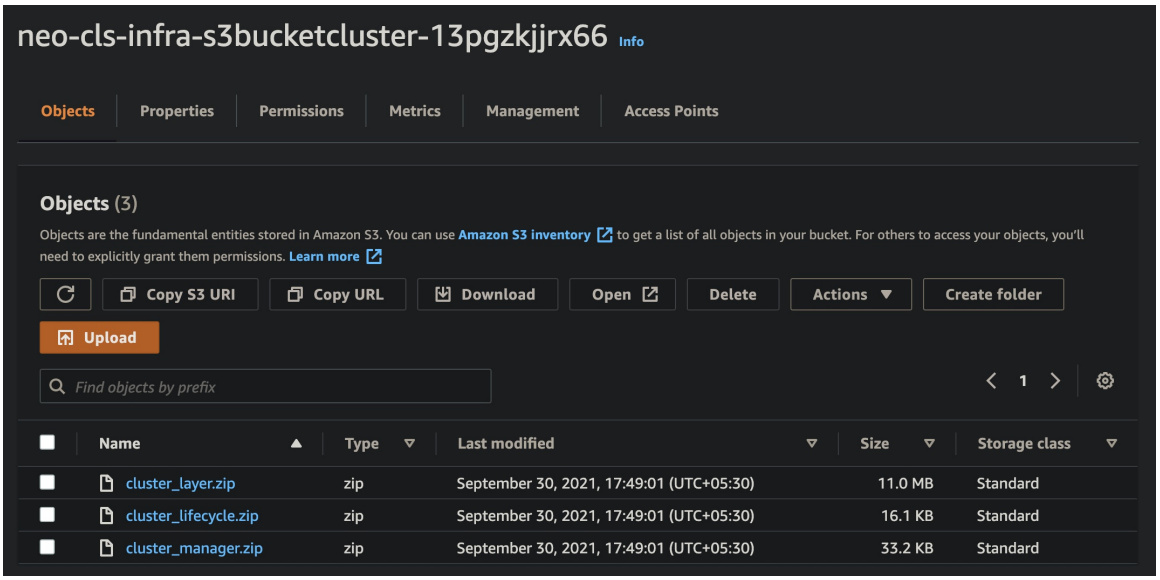
Outputs (16)

Search outputs

Key	Value	Description	Export name
AZ	me-south-1a	Availability zone	-
AppInstanceSGId	sg-02b07af19c3e746d9	Security Group ID for Application Instances	-
ApplicationSubnetIds	subnet-03217efc6049e5fee	Application subnet ID	-
BucketName	neo-cls-infra-s3bucketcluster-13pgzkjjrx66	Name of the sample Amazon S3 bucket with Private Static Web hosting Configuration	-
BucketUrl	http://neo-cls-infra-s3bucketcluster-13pgzkjjrx66.s3-website.me-south-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetId	subnet-0caf6c4801922d8b1	CCL subnet ID	-
EIPforNATgw	15.184.208.231	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-0a0d3797b04370aa3	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-0522ebe5acb8a2827	Security Group ID for Instances Inside Interface	-
InsideSubnetIds	subnet-056fdc9fe5389bf88	Inside subnet ID	-
InstanceSGId	sg-0be5b62647eb53dec	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-0347d191d724b2574	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-0989fbaeb522a906c,subnet-0c7a9b649d506f930	List of lambda subnet IDs (comma seperated)	-
MgmtSubnetIds	subnet-08c386d4b06890532	Mangement subnet ID	-
UseGWLB	Yes	Use Gateway Load Balancer	-
VpcName	vpc-0d94d3eaaa1f1354d	Name of the VPC created	-

步骤 3 将 **cluster_layer.zip**、**cluster_lifecycle.zip** 和 **cluster_manager.zip** 上传到通过 infrastructure.yaml 创建的 S3 存储桶。

图 *3: S3* 桶



步骤 4 部署 **deploy_ngfw_cluster.yaml**。

a) 转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

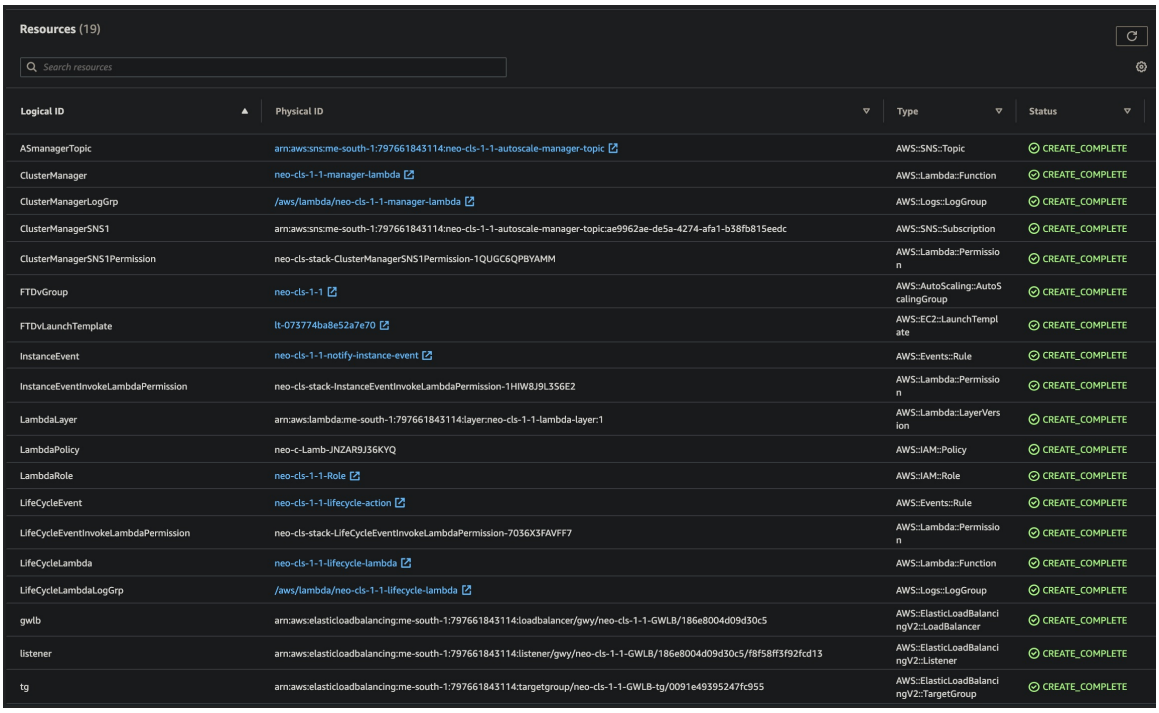
b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **deploy_ngfw_cluster.yaml**。

c) 点击**下一步 (Next)** 并提供所需的信息。

d) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

Lambda 函数将管理该过程的其余部分，并且 threat defense virtual 将自动注册到 管理中心。

图 *4:* 已部署的资源



步骤 5 通过登录到任何一个节点并使用 **show cluster info** 命令来验证集群部署。

图 *5:* 集群节点

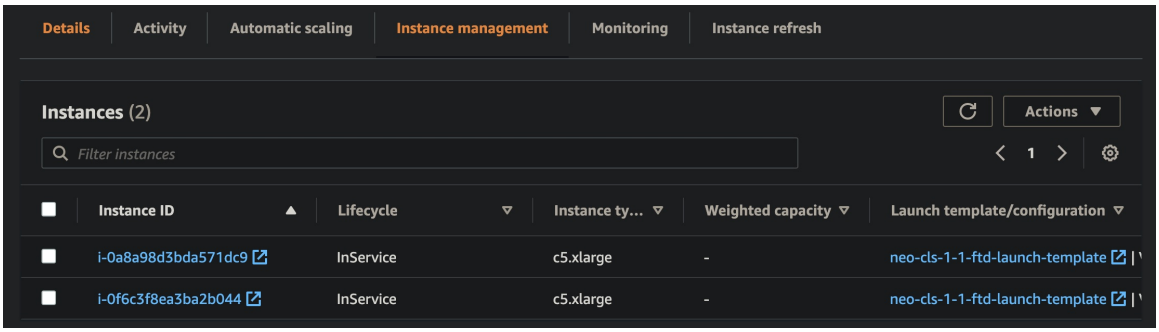


图 *6: show cluster info*

在 AWS 中手动部署集群

要手动部署集群，请准备 day 0 配置，部署每个节点，然后将控制节点添加到 管理中心。

创建 AWS 的 Day0 配置

您可以使用固定配置或自定义配置。我们建议使用固定配置。

使用 AWS 的固定配置创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
```

```
    }
}
```

例如：

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
  "CclSubnetRange": "10.10.55.4 10.10.55.30",     //mandatory user input
  "ClusterGroupName": "ftdv-cluster",             //mandatory user input
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input** 。

对于 **CclSubnetRange** 变量，请指定从 xxx4 开始的 IP 地址范围。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始 (*ip_address_start*) 和结束 (*ip_address_end*) IP 地址的一些示例。

表 *2:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254
10.1.1.0/24	10.1.1.4	10.1.1.254

使用 AWS 的自定义配置创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
```

```
"run_config": [comma_separated_threat_defense_configuration]
}
```

网关负载均衡器示例

以下示例会为网关负载均衡器创建一个配置，其中一个用于掉头流量的Geneve接口和一个用于集群控制链路的 VXLAN 接口。请注意，每个节点需要设置唯一的粗体值。

```
{
 "AdminPassword": "Sam&Dean",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface TenGigabitEthernet0/0",
  "nameif geneve-vtep-ifc",
  "ip address dhcp",
  "no shutdown",
  "interface TenGigabitEthernet0/1",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy single-arm",
  "nameif uturn-ifc",
  "vtep-nve 2",
  "object network ccl_link",
  "range 10.1.90.4 10.1.90.19",
  "object-group network cluster_group",
  "network-object object ccl_link",
  "nve 2",
  "encapsulation geneve",
  "source-interface geneve-vtep-ifc",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster_group",
  "jumbo-frame reservation",
  "mtu geneve-vtep-ifc 1806",
  "mtu ccl_link 1960",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "aaa authentication listener http geneve-vtep-ifc port 7777"
 ]
}
```

注释 对于 CCL 子网范围，请指定 CCL 子网 CIDR 中的 IP 地址，不包括保留的 IP 地址。有关示例，请参阅上 表 2: 开始和结束 IP 地址示例 。

对于 AWS 运行状况检查设置，请确保指定您在此处设置的 **aaa authentication listener http** 端口。

非本地负载均衡器示例

以下示例会创建一个配置，用于具有管理接口、内部接口和外部接口的非本地负载均衡器，以及用于集群控制链路的 VXLAN 接口。请注意，每个节点需要设置唯一的粗体值。

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "jumbo-frame reservation",
  "mtu ccl_link 1654",
  "object network ccl_link",
  "range 10.1.90.4 10.1.90.19",          //mandatory user input
  "object-group network cluster_group",
  "network-object object ccl_link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster_group",
  "cluster group ftdv-cluster",          //mandatory user input
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable"
 ]
}
```

对于集群控制链路网络对象，仅指定所需数量的地址（最多16个）。较大的范围可能会影响性能。

注释　如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input**。

部署集群节点

部署集群节点，以便它们形成集群。

过程

步骤 1 使用具有所需数量的接口的集群 Day 0 配置部署威胁防御虚拟实例 - 如果使用网关负载均衡器 (GWLB)，则为四个接口；如果使用非本地负载均衡器，则为五个接口。在 **配置实例详细信息 > 高级详细信息** 部分中，粘贴您的 day0 配置。

注释 确保按以下顺序将接口连接到实例。

- AWS 网关负载均衡器 - 四个接口 - 管理、诊断、内部和集群控制链路。
- 非本地负载均衡器 - 五个接口 - 管理、诊断、内部、外部和集群控制链路。

有关在 AWS 上部署 Threat Defense Virtual 的更多信息，请参阅 在 AWS 上部署威胁繁育虚拟。

步骤 2 重复步骤 1 以部署所需数量的其他节点。

步骤 3 使用威胁防御虚拟控制台上的 **show cluster info** 命令验证是否所有节点都已成功加入集群。

步骤 4 配置 AWS 网关负载均衡器。

a) 创建目标组和 GWLB。

b) 将目标组连接到 GWLB。

注释 确保将 GWLB 配置为使用正确的安全组、侦听程序配置和运行状况检查设置。

c) 使用 IP 地址向目标组注册数据接口（内部接口）。

有关详细信息，请参阅 创建网关负载均衡器。

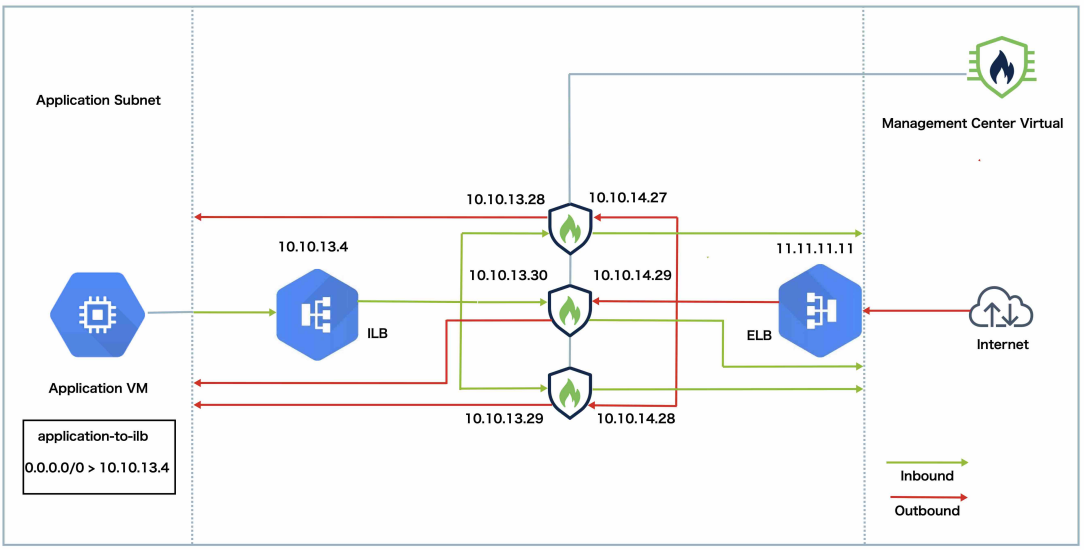
步骤 5 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 27 页。

在 GCP 中部署集群

要在 GCP 中部署集群，您可以手动部署，或者使用实例模板来部署实例组。您可以将集群与本地 GCP 负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

注释 出站流量需要使用接口 NAT 并被限制为 64K 连接。

拓扑示例



此拓扑同时描述了入站和出站流量。Threat Defense Virtual 集群夹在内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。

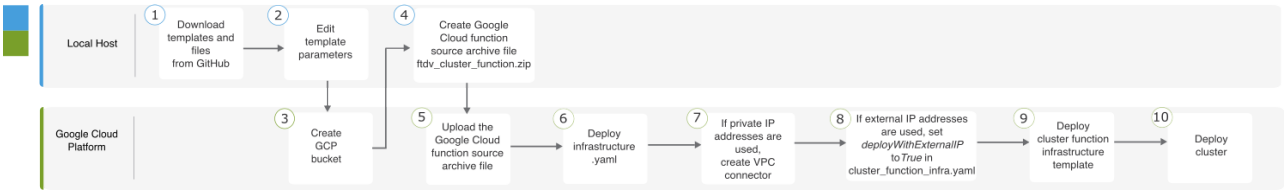
来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。集群中的 Threat Defense Virtual 实例检测到流量后，这些流量会被转发到应用 VM。

来自应用虚拟机的出站流量会被传输到内部负载均衡器。然后，流量被转发到 Threat Defense Virtual 集群，然后发送到互联网。

在 GCP 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

以下流程图说明了在 GCP 上基于模板部署 Threat Defense Virtual 集群的工作流程。

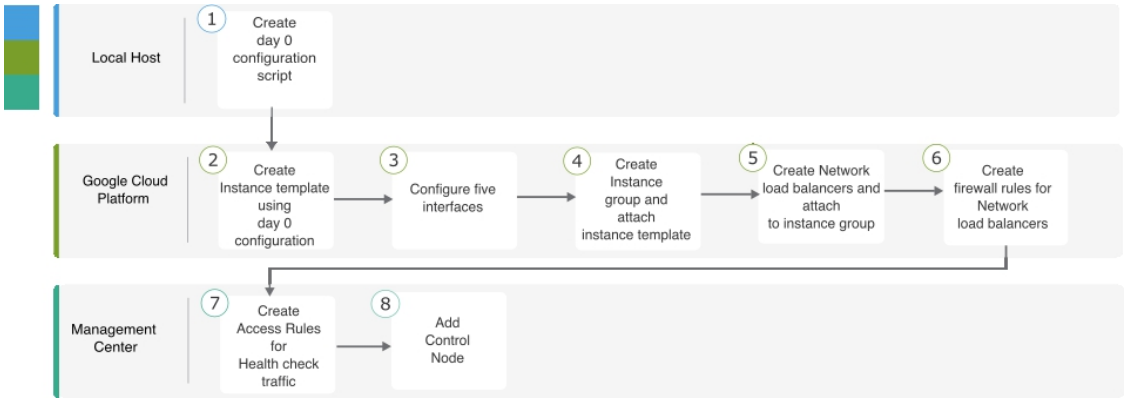


	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	编辑模板参数。

	工作空间	步骤
3	Google 云平台	创建 GCP 存储桶。
4	本地主机	创建 Google Cloud 函数源存档文件 *ftdv_cluster_function.zip*。
5	Google 云平台	上传 Google 函数源存档文件。
6	Google 云平台	部署 infrastructure.yaml。
7	Google 云平台	如果使用私有 IP 地址，请创建 VPC 连接器。
8	Google 云平台	如果使用外部 IP 地址，请在 *cluster_function_infra.yaml* 中将 *deployWithExternalIP* 设置为 *True*。
9	Google 云平台	部署集群功能基础设施模板。
10	Google 云平台	部署集群。

手动部署

以下流程图说明了在 GCP 上手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	为 GCP 创建 Day0 配置
2	Google 云平台	使用 Day 0 配置来创建实例模板。
3	Google 云平台	配置接口。
4	Google 云平台	创建实例组并附加实例模板。

	工作空间	步骤
5	Google 云平台	创建 NLB 并附加到实例组。
6	Google 云平台	创建 NLB 的防火墙规则。
7	管理中心	创建运行状况检查流量的访问规则。
8	管理中心	添加控制节点。

模板

以下给出的模板可在 GitHub 中获取。参数值与模板中给出的参数名称和值不言自明。

- 东西流量的集群部署模板 - *deploy_ngfw_cluster_yaml*
- 南北流量的集群部署模板 - deploy_ngfw_cluster.yaml

使用实例模板在 GCP 中部署实例组

使用实例模板在 GCP 中部署实例组。

开始之前

- 使用 Google Cloud Shell 进行部署。或者，您可以在任何 macOS/Linux/Windows 计算机上使用 Google SDK。
- 要允许集群自动向管理中心注册，您需要在管理中心创建一个具有管理权限的用户，该用户可以使用 REST API。请参阅《Cisco Secure Firewall Management Center 管理指南》。
- 在管理中心中添加与您在 *cluster_function_infra.yaml* 中指定的策略名称匹配的访问策略。

过程

步骤 1 将模板从 GitHub 下载到本地文件夹。

步骤 2 使用所需的 *resourceNamePrefix* 参数（例如 ngfwvcls）和其他所需的用户输入来编辑 **infrastructure.yaml**、**cluster_function_infra.yaml** 和 **deploy_ngfw_cluster.yaml**。

请注意，GitHub 的 **east-west** 和 **north-south** 文件夹中都有一个 *deploy_ngfw_cluster.yaml* 文件。根据流量要求下载相应的模板。

步骤 3 使用 Google Cloud Shell 创建存储桶，以上传 Google 云函数源存档文件 *ftdv_cluster_function.zip*。

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

确保此处的 *resourceNamePrefix* 变量与您在 **cluster_function_infra.yaml** 中指定的 *resourceNamePrefix* 变量匹配。

步骤 4 为集群基础设施创建一个存档文件。

示例：

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

步骤 5 上传您之前创建的 Google 源存档。

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

步骤 6 部署集群的基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

步骤 7 如果您使用的是专用 IP 地址，请执行以下步骤：

a) 使用 Threat Defense Virtual 管理 VPC 来启动和设置管理中心。

b) 创建 VPC 连接器，以便将 Google Cloud 功能与 Threat Defense Virtual 管理 VPC 连接。

gcloud compute networks vpc-access connectors create *vpc-connector-name* **--region us-central1 --subnet** *resourceNamePrefix***-ftdv-mgmt-subnet28**

步骤 8 如果管理中心相对于 Threat Defense Virtual 是远程，并且 Threat Defense Virtual 需要外部 IP 地址，请确保在 **cluster_function_infra.yaml** 中将 **deployWithExternalIP** 设置为 **True**。

步骤 9 部署集群功能基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

步骤 10 部署集群。

1. 对于北-南拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

2. 对于东-西拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

在 GCP 中手动部署集群

要手动部署集群，请准备 day0 配置，部署每个节点，然后将控制节点添加到 管理中心。

为 GCP 创建 Day0 配置

您可以使用固定配置或自定义配置。

使用 GCP 的固定配置来创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
    }
}
```

例如：

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",      //mandatory user input
        "ClusterGroupName": "ftdv-cluster"                //mandatory user input
    }
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input**。

请注意，对于 **CclSubnetRange** 变量，不能使用子网中的前两个 IP 地址和后两个 IP 地址。有关详细信息，请参阅 IPv4 子网中的保留 IP 地址。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始和结束 IP 地址的一些示例。

表 *3:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253
10.1.1.0/24	10.1.1.2	10.1.1.253

使用 GCP 的自定义配置来创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
    }
```

以下是为集群控制链路创建包含管理接口、内部接口和外部接口的配置的示例。请注意，每个节点需要设置唯一的粗体值。

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "object network ccl_link",
  "range 10.1.90.2 10.1.90.17",
  "object-group network cluster_group",
  "network-object object ccl_link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster_group",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu outside 1400",
  "mtu inside 1400"
 ]
}
```

注释 对于集群控制链路网络对象，仅指定所需数量的地址（最多16个）。较大的范围可能会影响性能。

手动部署集群节点

部署集群节点，以便它们形成集群。对于 GCP 上的集群，您不能使用 4 vCPU 机器类型。4 vCPU 机器类型仅支持 4 个接口，但需要 5 个接口。请使用支持五个接口的机器类型，例如 c2-standard-8。

过程

步骤 1 使用 day 0 配置（在**元数据 (Metadata) > 启动脚本 (Startup Script)** 部分中）创建具有 5 个接口的实例模板：外部、内部、管理、诊断和集群控制链路。

请参阅Cisco Secure Firewall Threat Defense Virtual 入门指南。

步骤 2 创建实例组，然后附加实例模板。

步骤 3 创建 GCP 网络负载均衡器（内部和外部），然后附加实例组。

步骤 4 对于GCP网络负载均衡器，允许在管理中心上的安全策略中进行运行状况检查。请参阅 允许对 GCP 网络负载均衡器进行运行状况检查，第 26 页。

步骤 5 将控制节点添加到 Management Center。请参阅将集群添加到管理中心（手动部署），第 27 页。

允许对 GCP 网络负载均衡器进行运行状况检查

Google Cloud 可提供运行状况检查，以确定后端是否对流量做出响应。

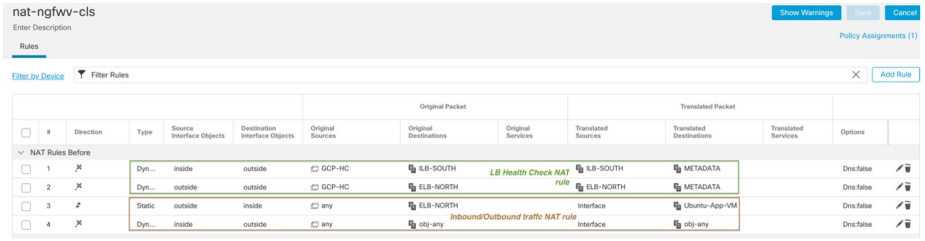
请参阅https://cloud.google.com/load-balancing/docs/health-checks，以便为网络负载均衡器创建防火墙规则。然后，在管理中心中创建访问规则以允许运行状况检查流量。有关所需的网络范围，请参阅https://cloud.google.com/load-balancing/docs/health-check-concepts。请参阅访问控制规则。

您还需要配置动态手动NAT规则，以便将运行状况检查流量重定向到位于169.254.169.254的Google元数据服务器。请参阅配置动态手动 NAT。

北-南 NAT 规则示例配置

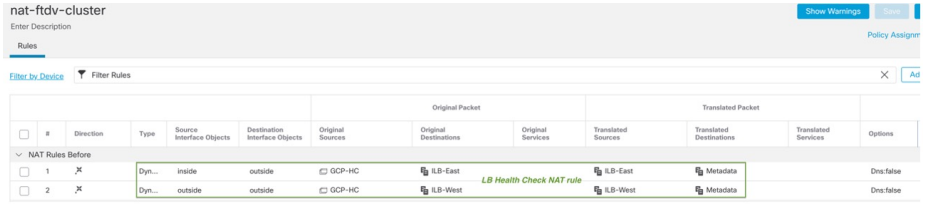
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
```

```
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



东西 NAT 规则示例配置

```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



将集群添加到管理中心（手动部署）

如果您手动部署了集群，请使用此程序将集群添加到管理中心。如果您使用模板，则集群会自动注册到 管理中心。

将集群设备之一作为新设备添加到 管理中心；管理中心 会自动检测所有其他集群成员。

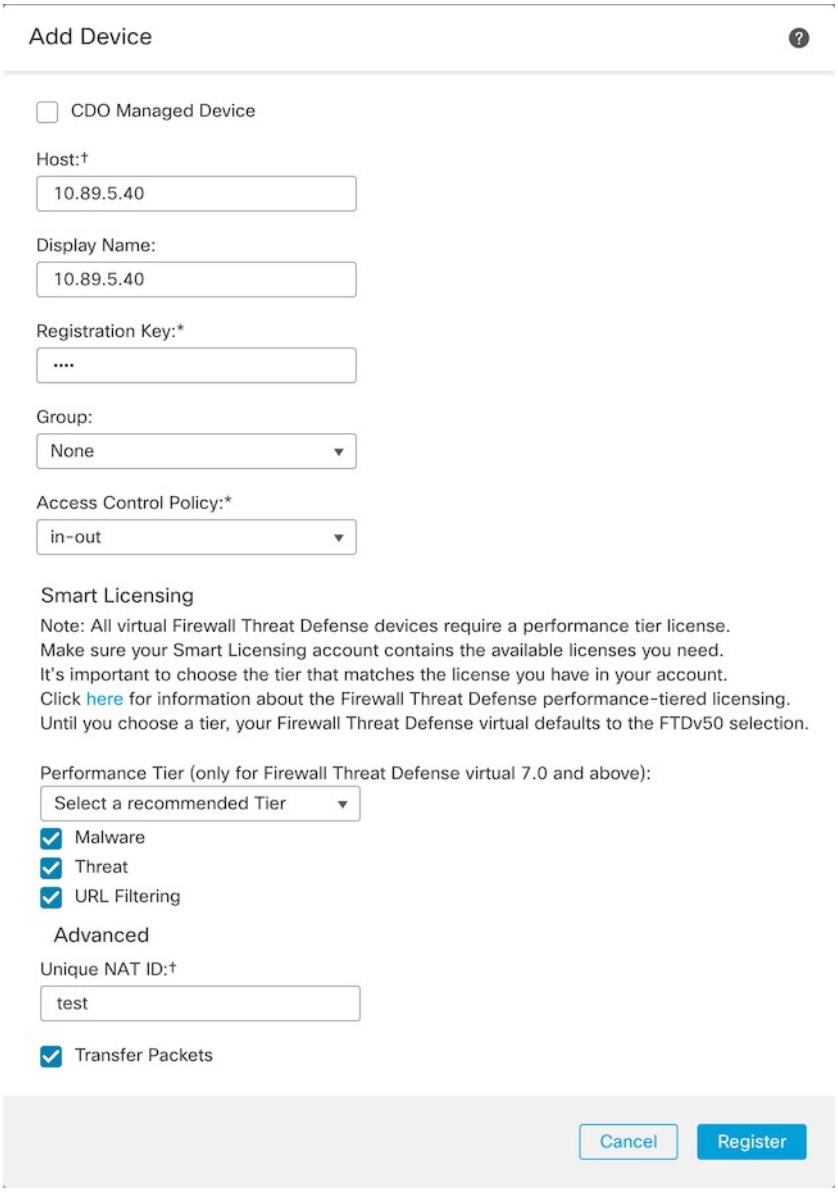
开始之前

- 所有集群设备必须位于成功建立的集群中，才能将集群添加到 管理中心。还应检查哪个是控制单元。使用 威胁防御 **show cluster info** 命令。

过程

步骤 1 在 管理中心中，选择 **设备 (Devices)** > **设备管理 (Device Management)**，然后选择 **添加 (Add)** > **添加设备 (Add Device)** 以使用管理 IP 来添加控制设备。

图 *7:* 添加设备



a) 在 **主机** 字段中，输入控制单元的 IP 地址或主机名。

虽然您可以添加任何集群单元，但我们建议添加控制单元备以获得最佳性能。

如果在设备设置期间使用了 NAT ID，则可能不需要输入此字段。有关详细信息，请参阅NAT 环境。

b) 在 **显示名称** 字段中，输入要在 管理中心中显示的控制单元名称。

此显示名称不适用于集群；它仅适用于要添加的控制单元。您可以稍后更改其他集群成员的名称和集群显示名称。

c) 在**注册密钥 (Registration Key)** 字段中，输入在设备设置时所使用的同一注册密钥。注册密钥是一个一次性的共享密钥。

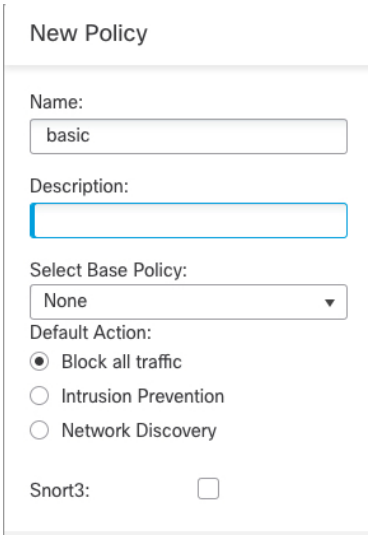
d) 在多域部署中，无论当前的域是什么，都将该设备分配给叶**域**。

如果当前域是叶域，设备会自动添加到当前域。如果当前域不是叶域，则注册后必须切换到叶域才能配置设备。

e) （可选） 将设备添加到设备 **组**。

f) 选择初始**访问控制策略**以在注册时部署到设备，或创建一个新策略。

如果创建新策略，则仅创建基本策略。您可以稍后根据需要自定义策略。



g) 选择要应用到设备的许可证。

h) 如果在设备安装过程中使用了 NAT ID，请展开**高级**部分，并在**唯一 NAT ID** 字段中输入相同的 NAT ID。

i) 选中**传输数据包**复选框以允许设备将数据包传输到 管理中心。

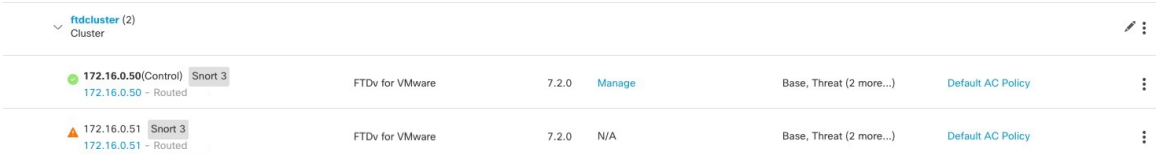
默认情况下，此选项已启用。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 管理中心进行检测。如果禁用此选项，则仅发送事件信息到管理中心，不发送数据包数据。

j) 点击 **Register**。

管理中心会识别并注册控制单元，接着注册所有数据单元。如果控制单元未注册成功，则不会添加集群。如果集群未运行或存在其他连接问题，则注册会失败。在这种情况下，我们建议尝试重新添加集群设备。

集群名称显示在 **设备** > **设备管理**页面上；展开集群可查看集群设备。

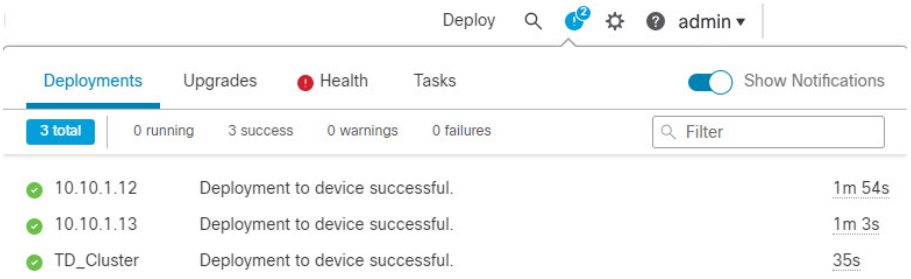
图 8: 集群管理



当前正在注册的设备会显示加载图标。

图 9: 节点注册

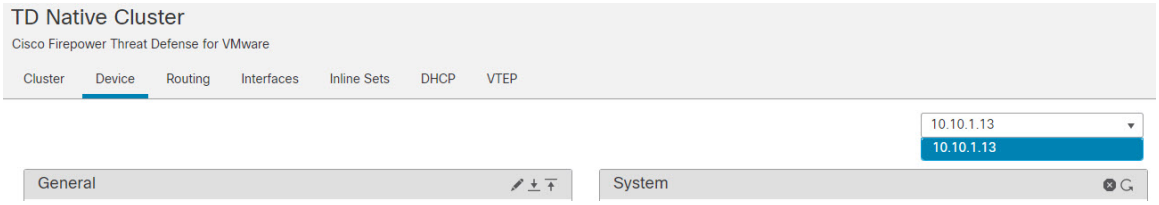
您可以通过点击 **通知** 图标并选择 **任务** 来监控集群设备的注册情况。管理中心 会在每个设备注册时更新“集群注册”任务。如有任何设备无法注册，请参阅调整集群节点，第 34 页。



步骤 2 通过点击集群的 **编辑**（✎），配置设备特定设置。

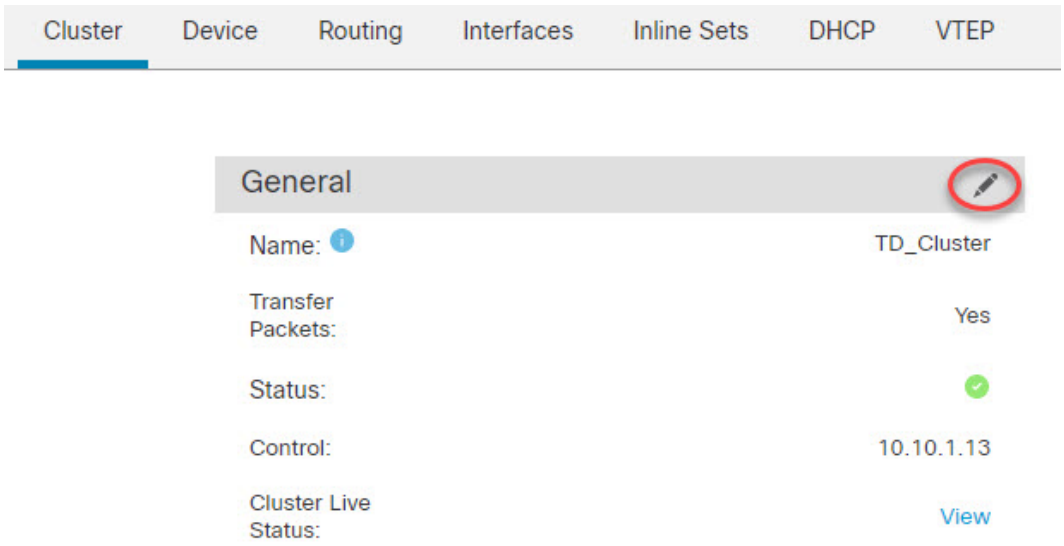
大多数配置可以应用于整个集群，而不适用于集群中的节点。例如，可以更改每个节点的显示名称，但只能配置整个集群的接口。

步骤 3 在 **设备** > **设备管理** > **集群** 屏幕上，可以查看 **常规**、**许可证**、**系统** 和 **运行状况** 设置。

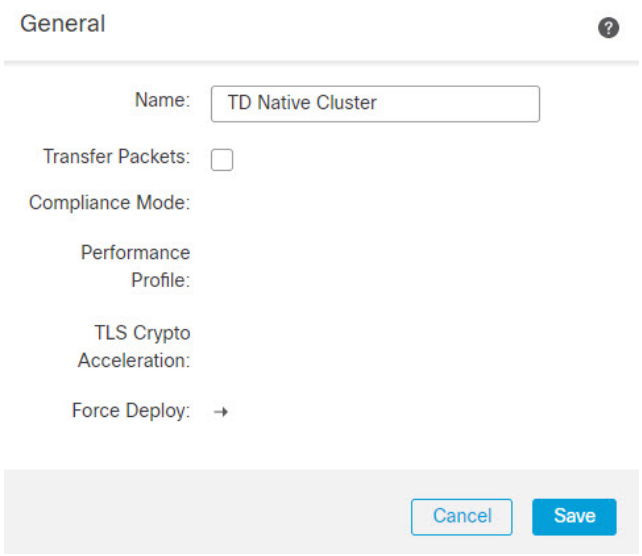


请参阅以下集群特定项：

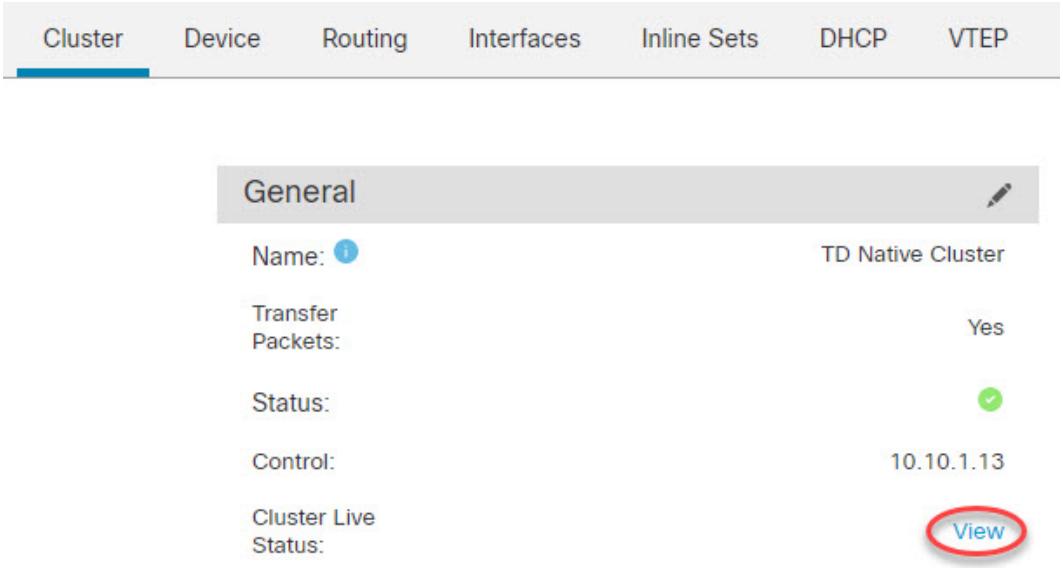
- **常规** > **名称**-通过点击 **编辑**（✎）更改集群显示名称。



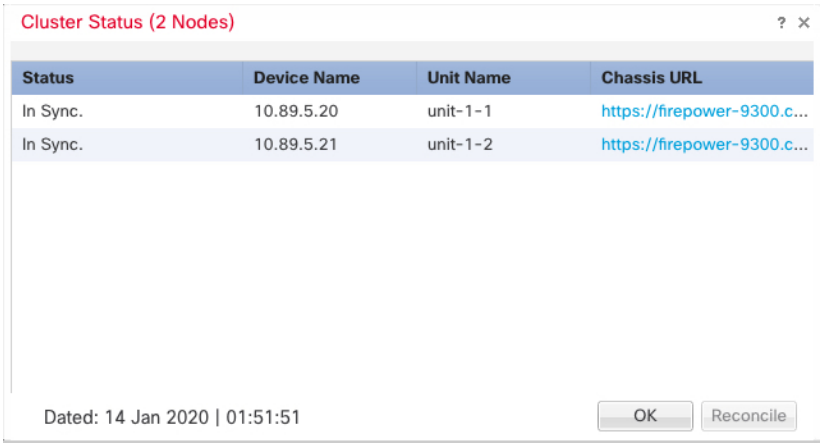
然后设置 **名称** 字段。



- **常规 > 查看集群状态**—点击 **查看集群状态** 链接来打开 **集群状态** 对话框。



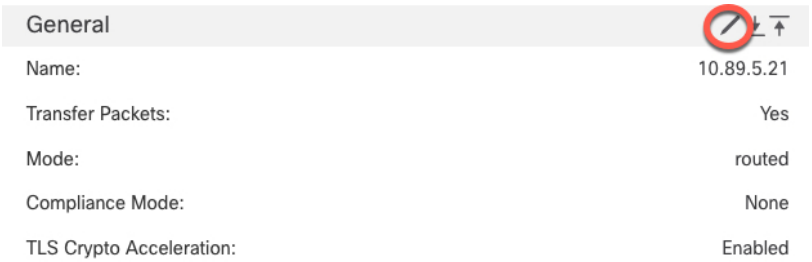
还可在 **集群状态** 对话框中点击 **协调**以重新注册数据单元。



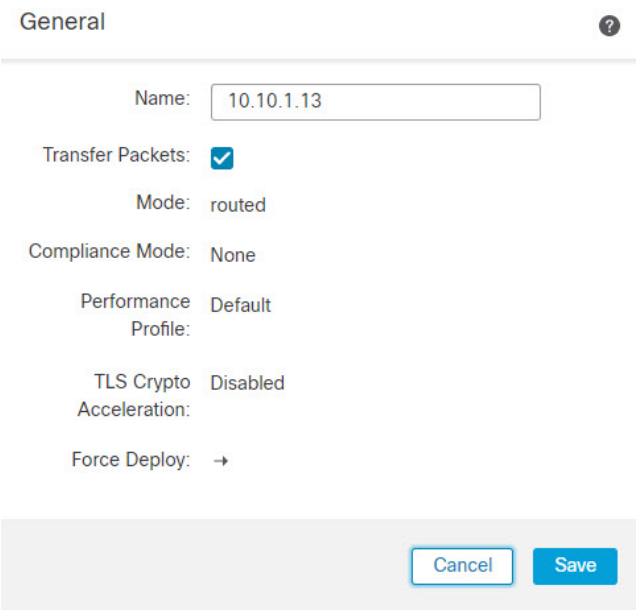
- **许可证**-点击 **编辑**（ ）可设置许可证授权。

步骤 4 在 **设备** > **设备管理** > **设备**上，可从右上方的下拉菜单中选择集群中的每个成员并配置以下设置。

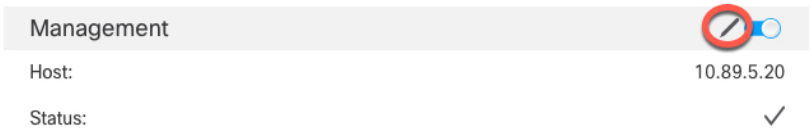
- **常规** > **名称**-通过点击 **编辑**（ ）更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理 > 主机**-如果在设备配置中更改了管理 IP 地址，则必须在 管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备；编辑 **管理** 区域中的 **主机** 地址。



管理集群节点

-

禁用集群

您可能需要停用节点，以准备删除节点，或临时进行维护。此程序旨在暂时停用节点；节点仍将显示在 管理中心 设备列表中。当节点变为非活动状态时，所有数据接口都将关闭。

注释 在禁用集群之前，请勿关闭节点。

过程

步骤 1 对于要禁用的设备，请选择**设备 (Devices)** > **设备管理 (Device Management)**，点击 **更多**（⋮），然后选择**禁用节点集群 (Disable Node Clustering)**。

步骤 2 确认要在节点上禁用集群。

节点将在**设备 (Devices)** > **设备管理 (Device Management)** 列表中的节点名称旁边显示（**已禁用**）**([Disabled])**。

步骤 3 重新启用集群，请参阅 重新加入集群，第 34 页。

重新加入集群

如果从集群中删除了某个节点（例如对于出现故障的接口），或者如果您手动禁用集群，必须手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除节点的原因的更多信息，请参阅重新加入集群，第 45 页。

过程

步骤 1 对于要重新激活的设备，请选择**设备 (Devices)** > **设备管理 (Device Management)**，点击 **更多**（⋮），然后选择**启用节点集群 (Enable Node Clustering)**。

步骤 2 确认要在节点上启用集群。

调整集群节点

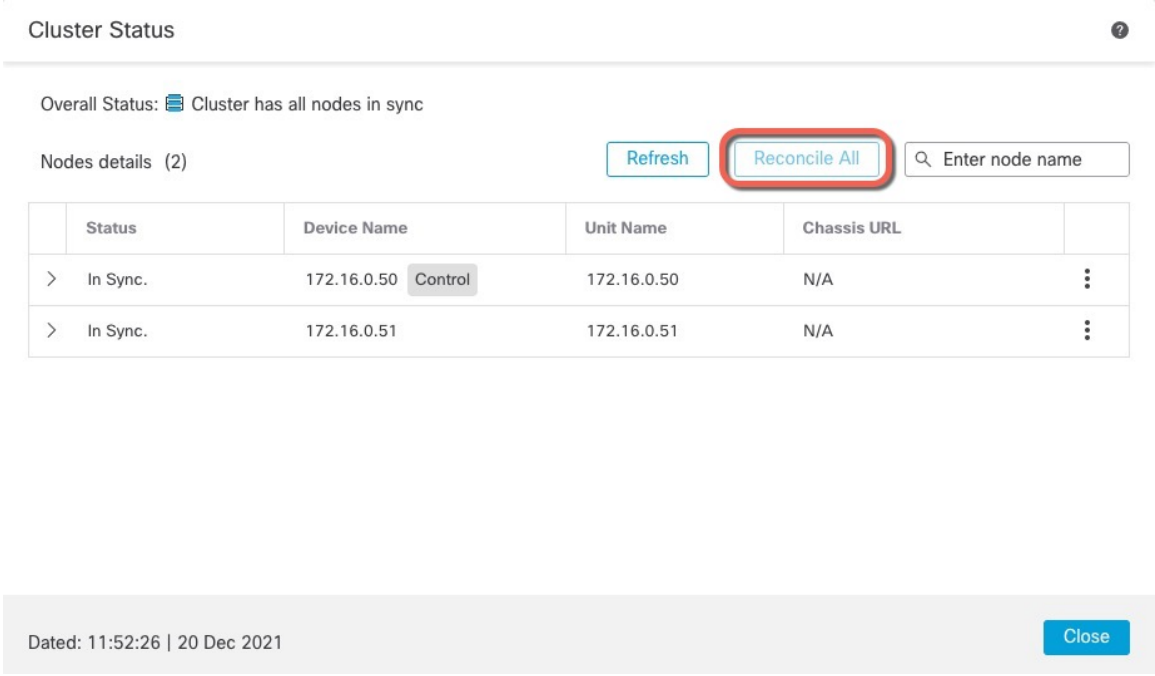
如果集群节点注册失败，则可将集群成员身份从设备协调至管理中心。例如，数据节点在管理中心被占用或存在网络问题时注册失败的情况下。

过程

步骤 1 选择集群的 **设备** > **设备管理** > **更多**（⋮），然后选择 **集群实时状态** 来打开 **集群状态** 对话框。

步骤 2 点击**协调全部 (Reconcile All)**。

图 *10:* 协调全部



有关集群状态的详细信息，请参阅监控集群，第 36 页。

删除（注销）集群或节点并注册到新的管理中心

您可以从 管理中心 中取消注册集群，从而使集群保持不变。如果要将集群添加到新的 管理中心，则可能需要取消注册该集群。

您还可以从 管理中心 取消注册节点，而不会中断集群中的节点。虽然该节点不会显示在 管理中心 中，但它仍然是集群的一部分，并且它会继续传递流量，甚至可能成为控制节点。您无法取消注册当前的控制节点。如果无法再从管理中心访问该节点，您可能会希望将其取消注册，但在排除管理连接故障时，您仍希望将其作为群集的一部分。

取消注册集群：

- 会切断 管理中心和该集群之间的所有通信。
- 从**设备管理 (Device Management)** 页面删除集群。
- 如果集群的平台设置策略配置为使用NTP从 管理中心 接收时间，则将集群返回本地时间管理。
- 让配置保持不变，以便集群继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将集群再次注册到相同或不同的管理中心会导致配置被删除，因此集群将在该点停止处理流量；集群配置将保持不变，因此您可以将集群作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

开始之前

此过程需要 CLI 对一个节点拥有访问权限。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，点击集群或节点的 **更多**（⋮），然后选择**删除 (Delete)**。

步骤 2 系统会提示您删除集群或节点；点击**是 (Yes)**。

步骤 3 您可以通过将其中一个集群成员添加为新设备来将集群注册到新的（或相同的）管理中心。

a) 连接到一个集群节点的 CLI，并使用 **configure manager add** 命令来识别新的管理中心。

b) 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击**添加设备 (Add Device)**。

您只用将其中一个集群节点添加为设备，然后便可发现其余集群节点。

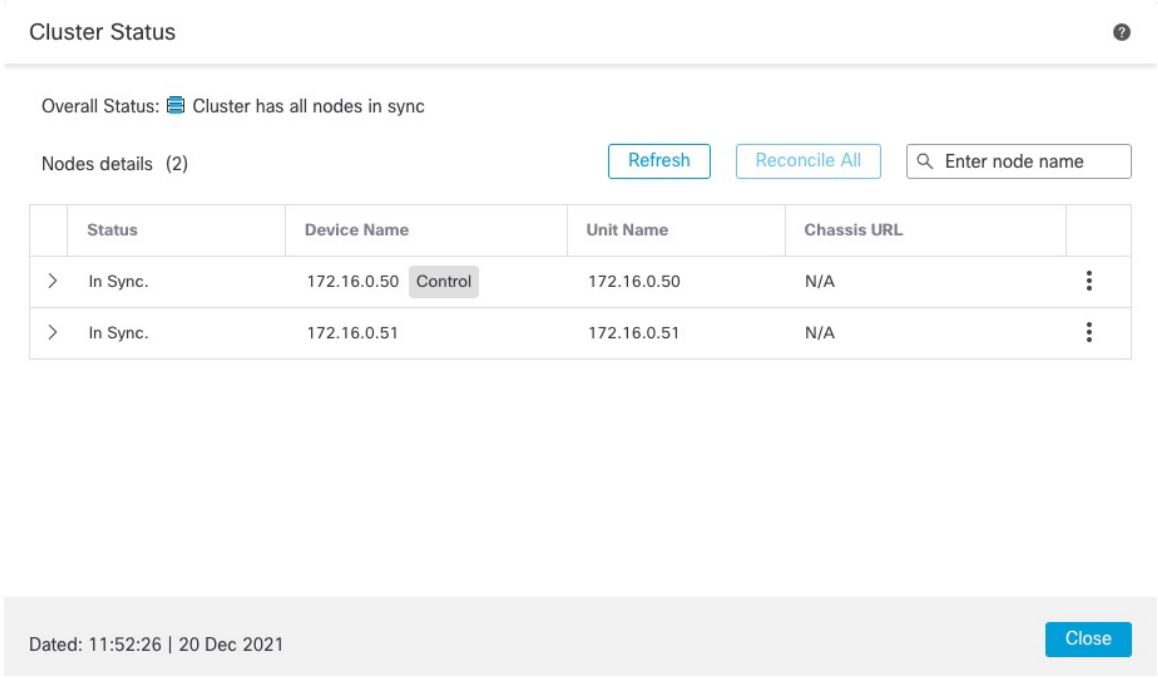
步骤 4 要重新添加已删除的节点，请参阅调整集群节点，第 34 页。

监控集群

您可以在 管理中心 中和 威胁防御 CLI 上监控集群。

- **集群状态 (Cluster Status)** 对话框，可通过**设备 (Devices)** > **设备管理 (Device Management)** > **更多**（⋮）图标或从**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 页面 > **常规 (General)** 区域 > **集群实时状态 (Cluster Live Status)** 链接打开。

图 *11:* 集群状态



控制节点有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 (In Sync.) - 节点已向 管理中心 注册。
- 待处理注册 (Pending Registration) - 节点是集群的一部分，但尚未向 管理中心 注册。如果节点注册失败，则可点击**协调所有 (Reconcile All)** 以重试注册。
- 集群已禁用 (Clustering is disabled) - 节点已向 管理中心 注册，但它是集群的非活动成员。如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除节点。
- “正在加入集群...”(Joining cluster...) - 节点正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 管理中心 注册。

对于每个节点，您可以查看**摘要 (Summary)** 或**历史记录 (History)**。

图 *12:* 节点摘要

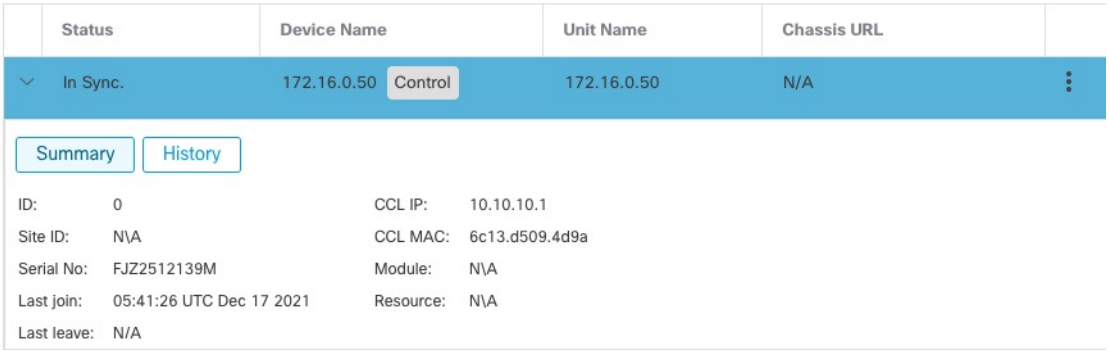
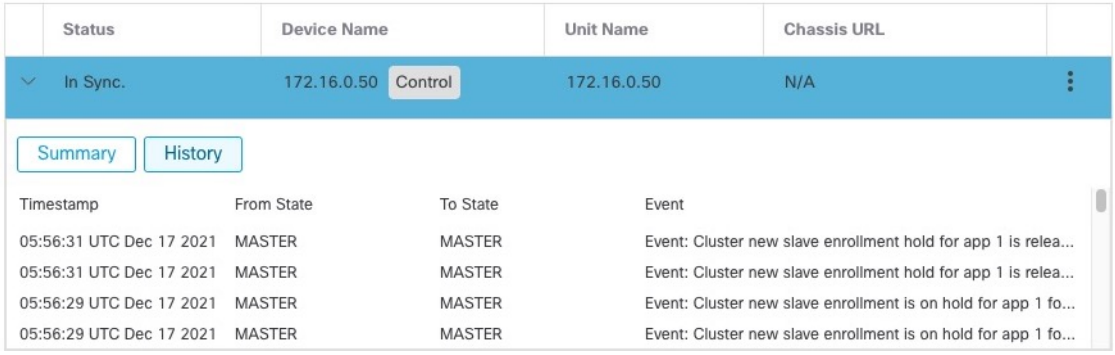


图 *13:* 节点历史记录



- **系统**（⚙）> **任务** 页面。

  任务 (Tasks) 页面会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

- **设备 (Devices)** > **设备管理 (Device Management)** > *cluster_name*。

  展开设备列表页面上的集群时，您可以看到所有成员节点，包括 IP 地址旁显示其角色的控制节点。对于仍在注册的节点，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

升级集群

要升级 threat defense virtual 集群，请执行以下步骤。

过程

步骤 1 将目标映像版本上传到云映像存储。

步骤 2 使用更新后的目标映像版本来更新集群的云实例模板。

a) 使用目标映像版本来创建实例模板的副本。

b) 将新创建的模板附加到集群实例组。

步骤 3 将目标映像版本升级包上传到 管理中心。

步骤 4 对要升级的集群执行就绪性检查。

步骤 5 成功进行就绪性检查后，开始安装升级包。

步骤 6 管理中心 会一次升级一个集群节点。

步骤 7 成功升级集群后，管理中心 会显示通知。

升级后，实例的序列号和 UUID 不会变化。

注释

- 如果从管理中心启动集群升级，请确保在升级后重新启动过程中没有 Threat Defense Virtual 设备意外终止或被 Auto Scaling 组替换。要防止这种情况发生，请转到 AWS 控制台，点击 **自动扩展组 (Auto scaling group) -> 高级配置 (Advanced configurations)**，然后暂停运行状况检查和替换不正常的进程。升级完成后，再次转至**高级配置 (Advanced configurations)** 并删除所有暂停的进程，以检测运行状况不佳的实例。
- 如果将 AWS 上部署的集群从主要版本升级到补丁版本，然后向上扩展集群，则新节点将提供主要发行版本而不是修补程序版本。然后，您必须从管理中心手动将每个节点升级到修补程序版本。

  或者，您也可以从已应用补丁且没有 Day 0 配置的独立 Threat Defense Virtual 实例的快照创建 Amazon 系统映像 (AMI)。在集群部署模板中使用此 AMI。扩展集群时出现的任何新节点都将具有修补程序版本。

集群参考

本部分包括有关集群工作原理的详细信息。

威胁防御功能和群集

部分威胁防御功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

不支持的功能和群集

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略。

- 远程接入 VPN（SSL VPN 和 IPsec VPN）
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- FMC UCAPL/CC 模式

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC

- TFTP
- XDMCP

- 静态路由监控

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

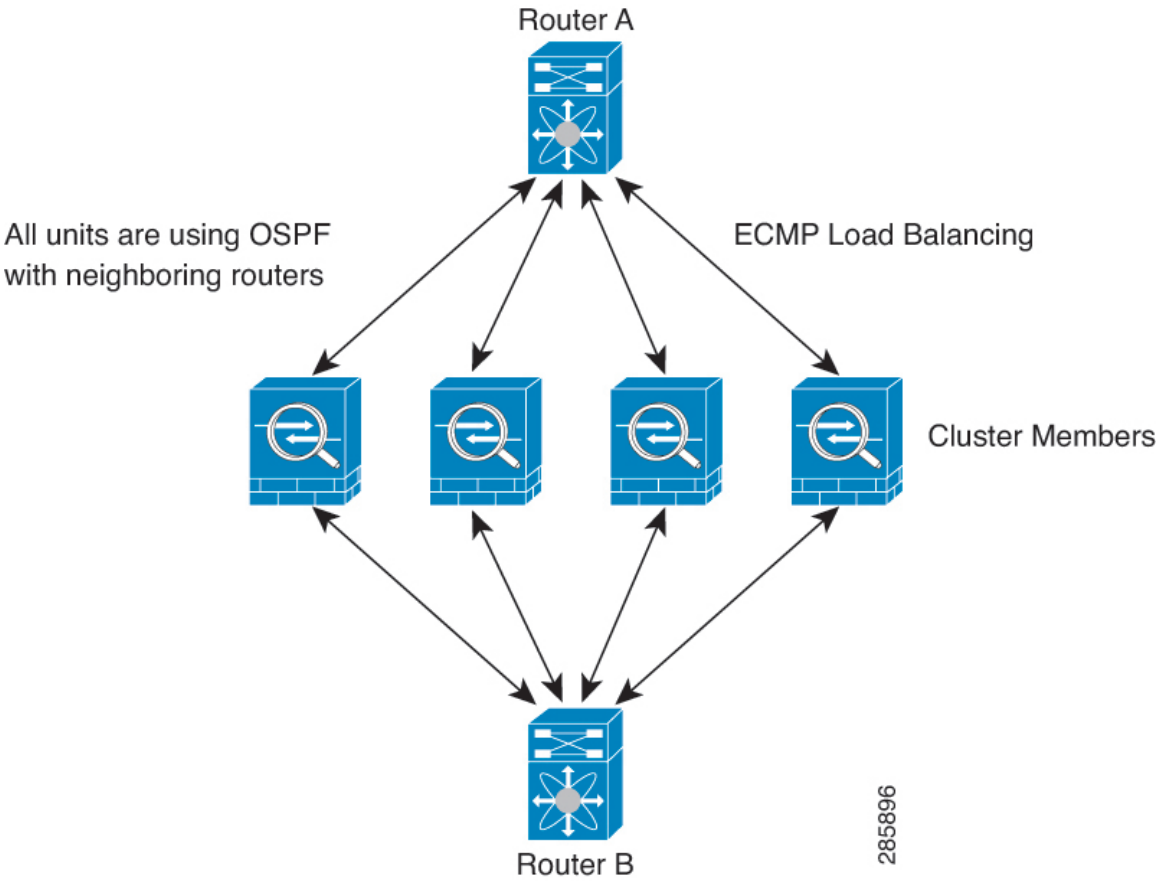
连接设置和集群

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *14:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

NAT 和集群

对于 NAT 用途，请参阅以下限制。

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为NAT所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。

- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT

连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。

- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

SNMP 代理按照诊断接口本地 IP 地址轮询每一个威胁防御。您无法轮询集群的合并数据。

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

VPN 和集群

站点到站点 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程接入 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。

注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。

5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

监控所有物理接口；只能监控已命名的接口。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。节点将在 500 毫秒后删除。

发生故障后的状态

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

威胁防御将自动尝试重新加入集群，具体取决于故障事件。

注释 当 威胁防御 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理/诊断接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。

- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - 威胁防御 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 威胁防御应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。威胁防御应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。
- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储 TCP/UDP 状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *4:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。
- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。
- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

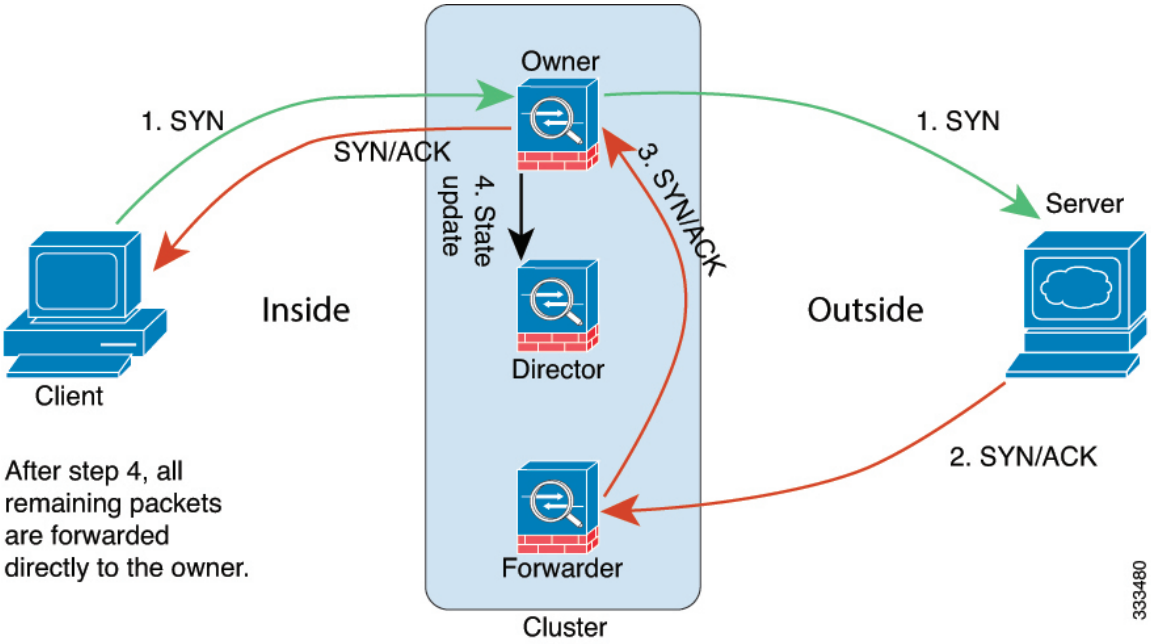
- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。



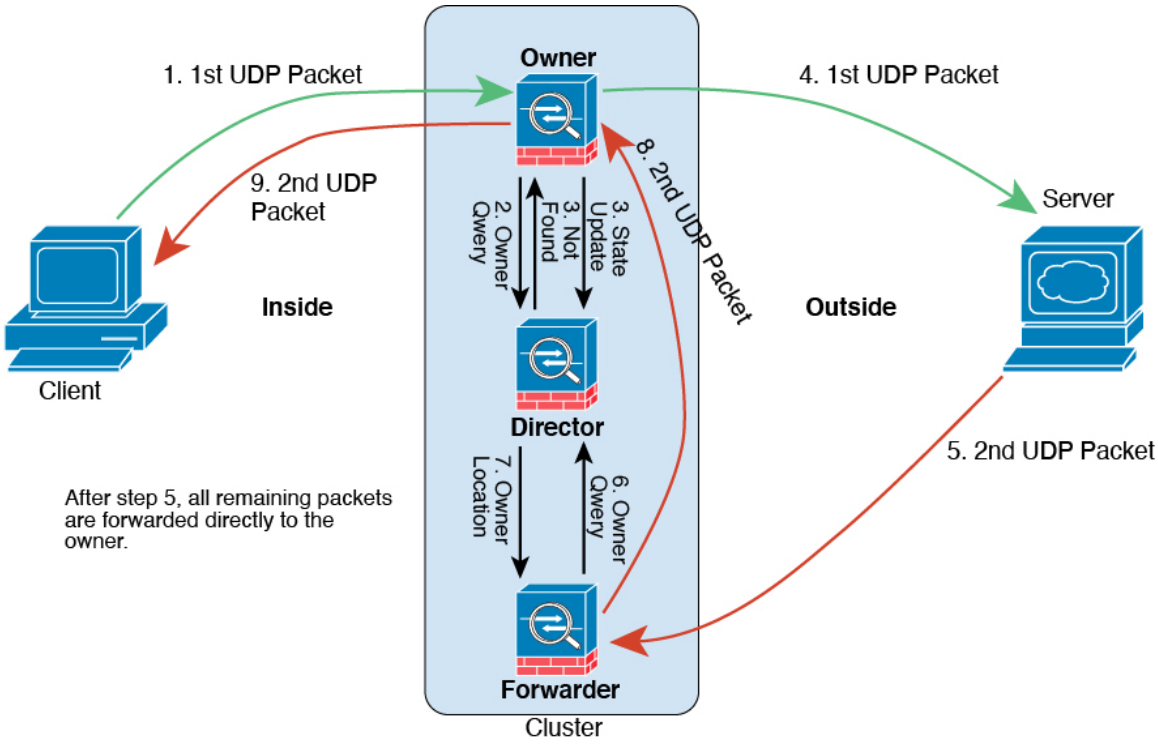
1. SYN 数据包从客户端发出，被传送到一台 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 威胁防御（基于负载均衡方法）。此 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。

5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *15: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。

7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

关于公共云中的 Threat Defense Virtual 群集的历史记录

特性	Version	详细信息
公共云（Amazon Web 服务和 Google 云平台）上 Threat Defense Virtual 的集群	7.2	threat defense virtual 支持公共云（AWS 和 GCP）上最多 16 个节点的单个接口集群。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加设备 (Add Device)** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：AWS 和 GCP 上的 Threat Defense Virtual

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。