私有云中威胁防御虚拟的群集

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。您可以使用VMware和 KVM 在私有云中部署 threat defense virtual 集群。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 27 页。

- 关于私有云中的 Threat Defense Virtual 群集，第 1 页
- 威胁防御虚拟群集的许可证，第 5 页
- Threat Defense Virtual 群集的要求和必备条件，第 5 页
- Threat Defense Virtual 群集的准则，第 6 页
- 配置威胁防御虚拟群集，第 7 页
- 管理集群节点，第 15 页
- 监控集群，第 25 页
- 集群参考，第 27 页
- 私有云中 Threat Defense Virtual 群集的历史记录，第 38 页

关于私有云中的 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。
- 对每台防火墙的管理访问权限，用于进行配置和监控。threat defense virtual 部署包括用于管理集群节点的 Management 0/0 接口。

将集群接入网络中时，上游和下游路由器需要能够使用第 3 层单独接口和以下方法之一使出入集群的数据实现负载均衡：

- 策略型路由 - 上游和下游路由器使用路由映射和 ACL 在节点之间执行负载均衡。
- 等价多路径路由 - 上游和下游路由器使用等价静态或动态路由在节点之间执行负载均衡。

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。

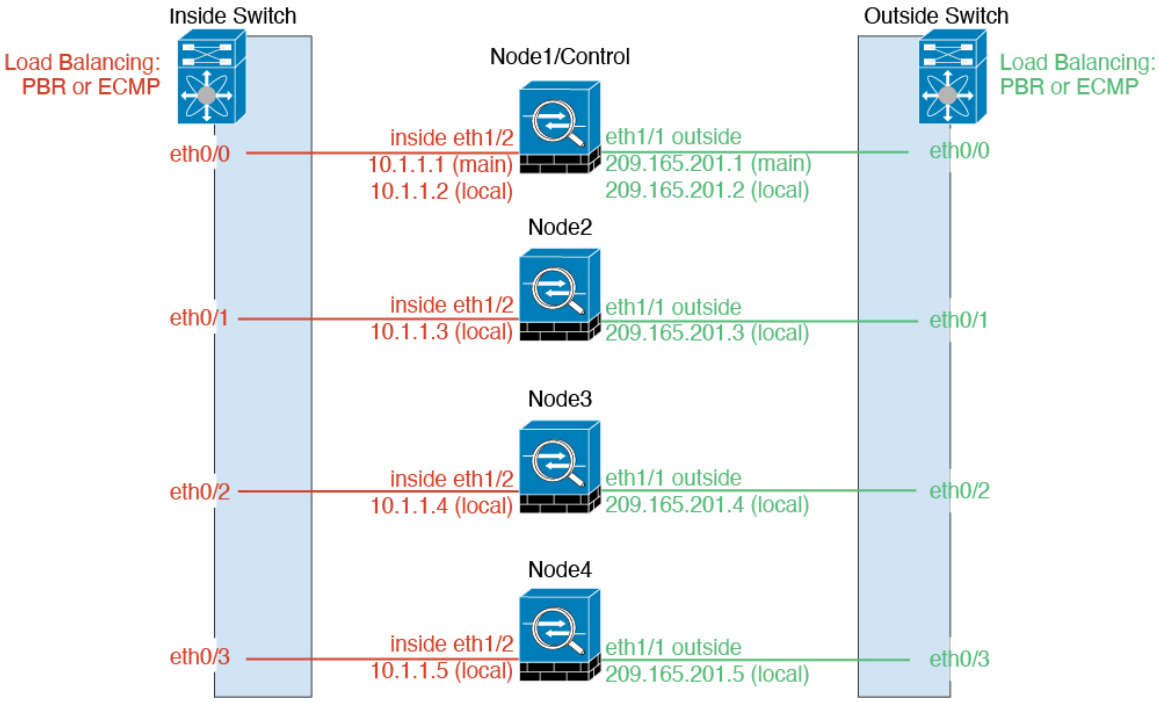
集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

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。

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。由于接口配置只能在控制节点上配置，因此您可以通过接口配置设置一个 IP 地址池，供集群节点上的给定接口（包括控制节点上的一个接口）使用。集群的主集群 *IP* 地址是集群的固定地址，始终属于当前的控制节点。本地 IP 地址始终是路由的控制节点地址。主集群 IP 地址提供对地址的统一管理访问；当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。不过，在此情况下必须在上游交换机上分别配置负载均衡。



注释 不支持第 2 层跨区以太网通道。

基于策略的路由

使用独立接口时，每个 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。基于策略的路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，我们建议使用此方法。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 威胁防御 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。为了获得最佳性能，建议您配置 PBR 策略，以便连接的转发数据包和返回数据包定向到同一个 威胁防御。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 威胁防御。然后，PBR 可根据特定 威胁防御 的可访问性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

同等成本的多路径路由

使用独立接口时，每个 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，我们建议使用此方法。

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。

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。

威胁防御虚拟群集的许可证

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。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。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
- VMware 或 KVM
- 在 2x2 部署配置中， 两 个主机上的集群最多有 四 个节点。我们建议您在 两 台主机 (2x2) 上最多部署 两 台threat defense virtual ，这会形成一个包含 四 个节点的集群。

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：

- 必须为集群控制链路启用巨帧预留。部署 threat defense virtual 时，可以通过设置 `"DeploymentType": "Cluster"`在 Day 0 配置中启用巨帧预留。否则，在集群形成且运行状况正常后，您需要重新启动每个节点才能启用巨帧。
- 对于 KVM，必须使用 CPU 硬分区（CPU 固定）。
- 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。
- 必须在同一域中。
- 必须在同一组中。
- 不得有任何待处理或进行中的部署。
- 控制节点不得配置任何不受支持的功能（请参阅不支持的功能和群集，第 27 页）。
- 数据节点不得配置任何 VPN。控制节点可以配置站点间 VPN。

管理中心 要求

- 确保 管理中心 NTP 服务器设置为所有集群节点均可访问的可靠服务器。默认情况下， threat defense virtual 使用与 管理中心相同的 NTP 服务器。如果未将所有集群节点上的时间设置为相同，则可以将其从集群中删除。

交换机要求

- 请务必完成交换机配置后再配置集群。确保连接到集群控制链路的端口配置了正确（更高）的 MTU。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。如果交换机的 MTU 不匹配，则集群形成将失败。

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

- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。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。
- 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。需要建立新连接以连通新设备。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。
- 我们不支持数据接口的 VXLAN；只有集群控制链路支持 VXLAN。

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。

配置威胁防御虚拟群集

要在部署 threat defense virtual 后配置集群，请执行以下任务。

将设备添加到管理中心

在配置集群之前部署每个集群节点，然后将设备添加为 管理中心 上的独立设备。

过程

步骤 1 根据 Cisco Secure Firewall Threat Defense Virtual 入门指南部署每个集群节点。

集群中的所有设备：

- 必须为集群控制链路启用巨帧预留。部署 threat defense virtual 时，可以通过设置 `"DeploymentType": "Cluster"`在 Day 0 配置中启用巨帧预留。否则，在集群形成且运行状况正常后，您需要重新启动每个节点才能启用巨帧。
- 对于 KVM，必须使用 CPU 硬分区（CPU 固定）。

步骤 2 将每个节点作为同一域和组中的独立设备添加到 管理中心。

请参阅将设备添加到 管理中心。您可以创建包含单个设备的集群，然后稍后添加更多节点。您在添加设备时设置的初始设置（许可、访问控制策略）将被控制节点的所有集群节点继承。您将在形成集群时选择控制节点。

创建集群

从 管理中心 中的一个或多个设备组成集群。

开始之前

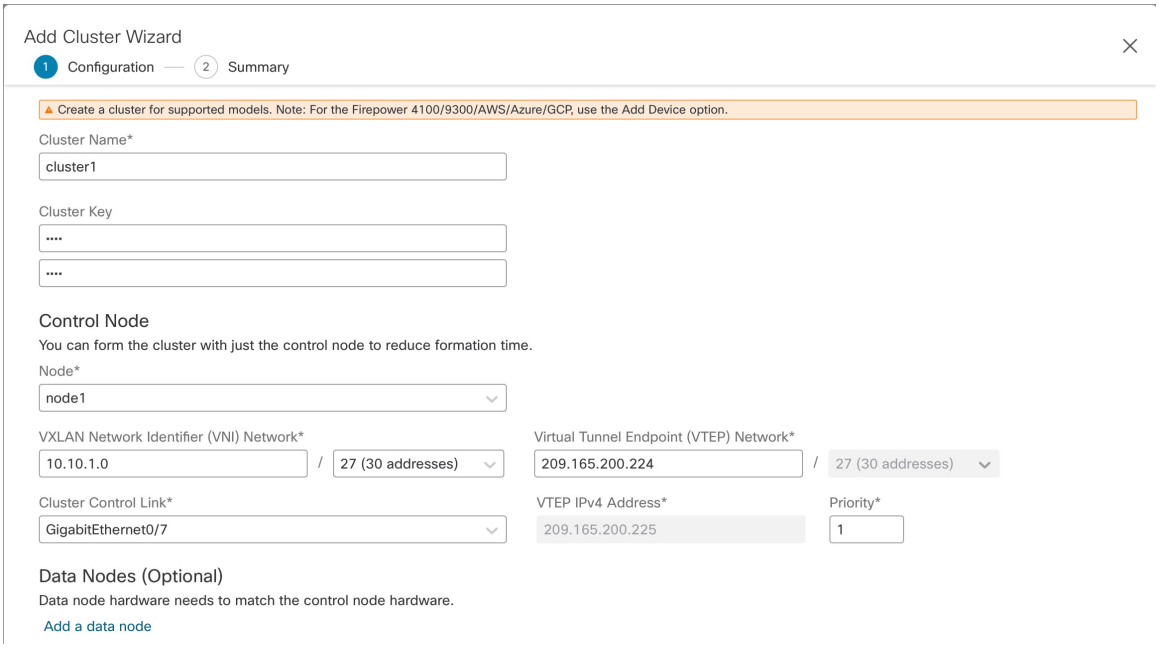
某些功能与集群不兼容，因此应等到启用集群后再执行配置。如果已配置某些功能，则会阻止集群的创建。例如，不要在接口或不支持的接口类型（例如 BVI）上配置任何 IP 地址。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后选择**添加 (Add)** > **添加集群 (Add Cluster)**。

出现**添加集群向导 (Add Cluster Wizard)**。

图 *1:* 添加集群向导



步骤 2 为控制流量指定**集群名称 (Cluster Name)** 和身份验证**集群密钥 (Cluster Key)**。

- **集群名称 (Cluster Name)** - 1 到 38 个字符的 ASCII 字符串。

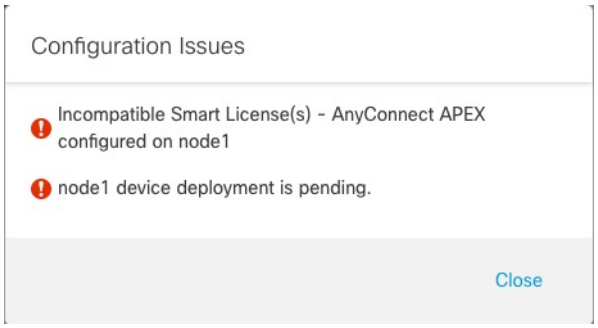
- **集群密钥 (Cluster Key)** - 1 到 63 个字符的 ASCII 字符串。 **集群密钥 (Cluster Key)** 值用于生成加密密钥。此加密不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 3 对于**控制节点**，请进行以下设置：

- **节点 (Node)** - 选择一开始要作为控制节点的设备。当 管理中心 形成集群时，它会首先将此节点添加到集群，因此它将成为控制节点。

  注释 如果您在节点名称旁边看到一个 **错误**（  ）图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。例如：

  图 *2:* 配置问题

  要解决上述问题，请删除不支持的 VPN 许可证，并将待处理的配置更改部署到设备。

- **VXLAN 网络标识符 (VNI) 网络 (VXLAN Network Identifier [VNI] Network)** - 为 VNI 网络指定 IPv4 子网；该网络不支持 IPv6。指定 **24**、**25**、**26** 或 **27** 子网。IP 地址将被自动分配给此网络上的每个节点。VNI 网络是在物理 VTEP 网络上运行的加密虚拟网络。
- **集群控制链路 (Cluster Control Link)** - 选择要用于集群控制链路的物理接口。
- **虚拟隧道终端 (VTEP) 网络 (Virtual Tunnel Endpoint [VTEP] Network)** - 为物理接口网络指定 IPv4 子网；该网络不支持 IPv6。VTEP 网络与 VNI 网络不同，它被用于物理集群控制链路。
- **VTEP IPv4 地址 (VTEP IPv4 Address)** - 此字段将自动填充 VTEP 网络上的第一个地址。
- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。即使您将优先级设置为低于其他节点，在首次建立集群时，此节点仍将作为控制节点。

步骤 4 对于**数据节点（可选）**，点击**添加数据节点 (Add a data node)** 以便将节点添加到集群。

您可以仅使用控制节点建立集群，以便加快集群建立的速度，也可以立即添加所有节点。为每个数据节点设置以下内容：

- **节点 (Node)** - 选择要添加的设备。

注释 如果您在节点名称旁边看到一个**错误**（）图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。

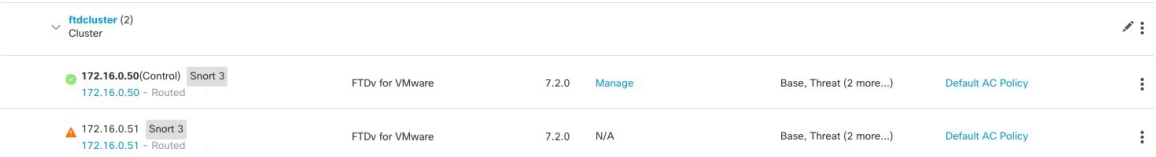
- **VTEP IPv4 地址 (VTEP IPv4 Address)** - 此字段将自动填充 VTEP 网络上的下一个地址。
- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。

步骤 5 点击**继续**。查看**摘要 (Summary)**，然后点击**保存 (Save)**。

集群引导程序配置会被保存到集群节点。引导程序配置包括用于集群控制链路的 VXLAN 接口。

集群名称显示在 **设备 (Save)** > **设备管理 (Device Management)**页面上；展开集群可查看集群节点。

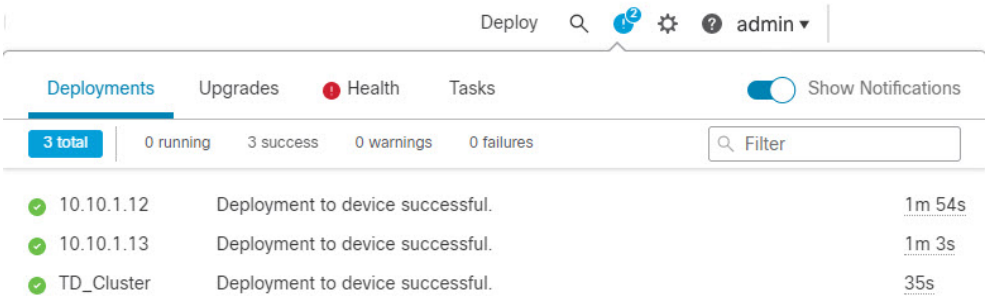
图 *3:* 集群管理



当前正在注册的节点会显示加载图标。

图 *4:* 节点注册

您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。管理中心 会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

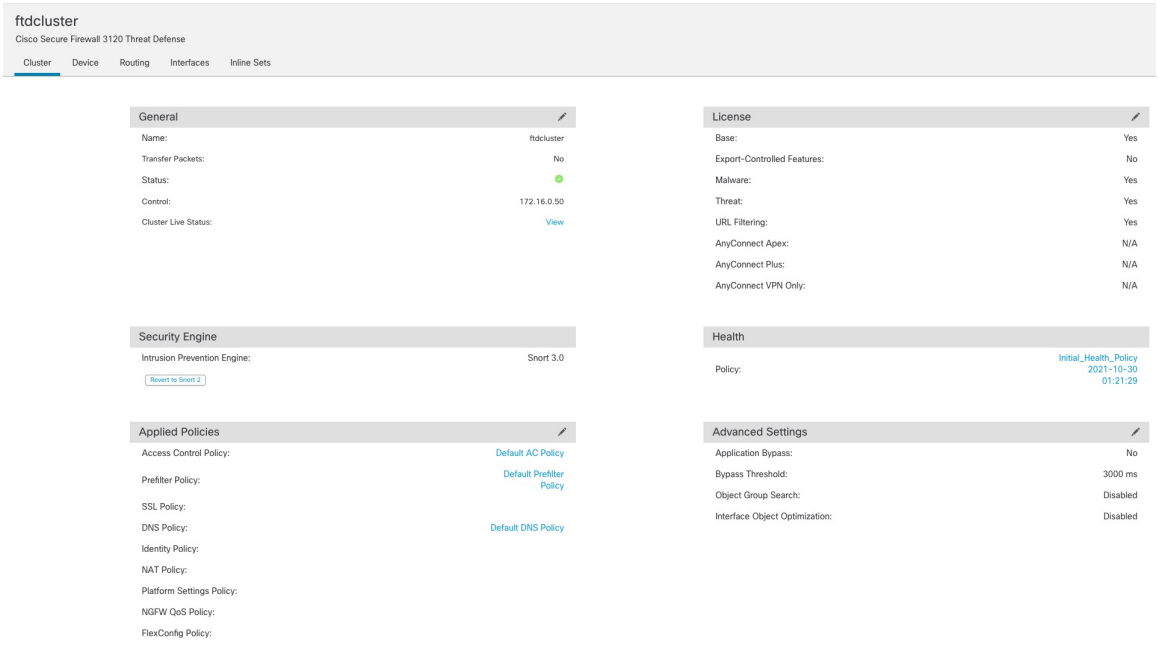


步骤 6 通过点击集群的 **编辑**（）， 配置设备特定设置。

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。

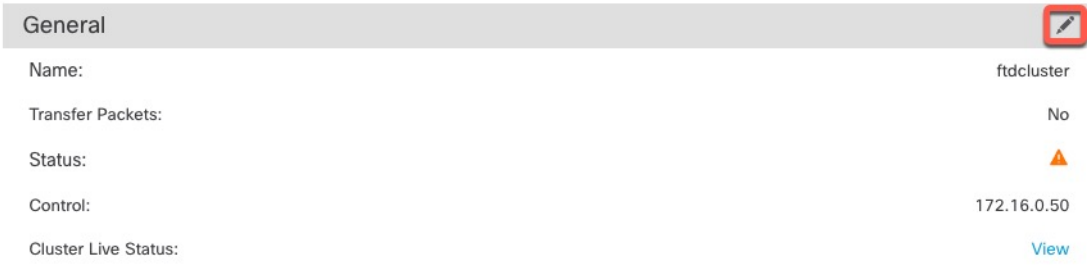
步骤 7 在 **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 屏幕中，可以查看集群的**常规 (General)** 和其他设置。

图 *5:* 集群设置

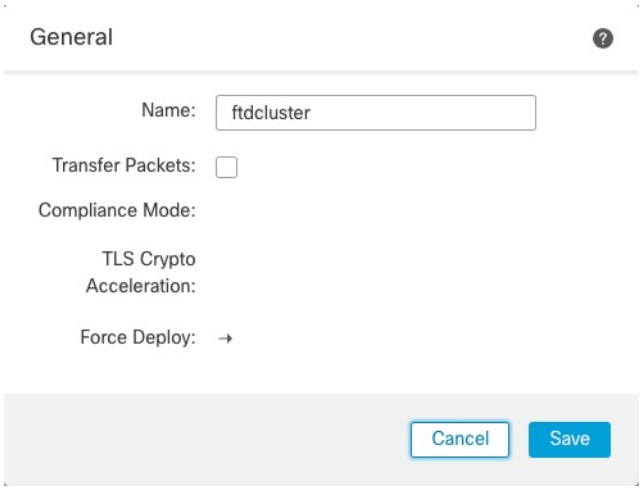


请参阅**常规 (General)** 区域中的以下集群特定项：

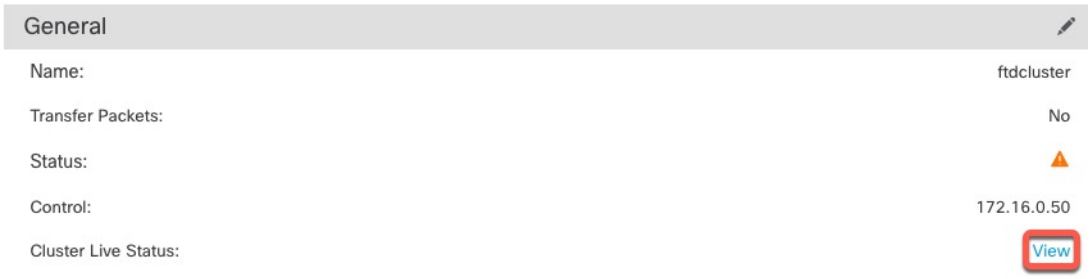
- **常规 > 名称**-通过点击 **编辑**（ ）更改集群显示名称。



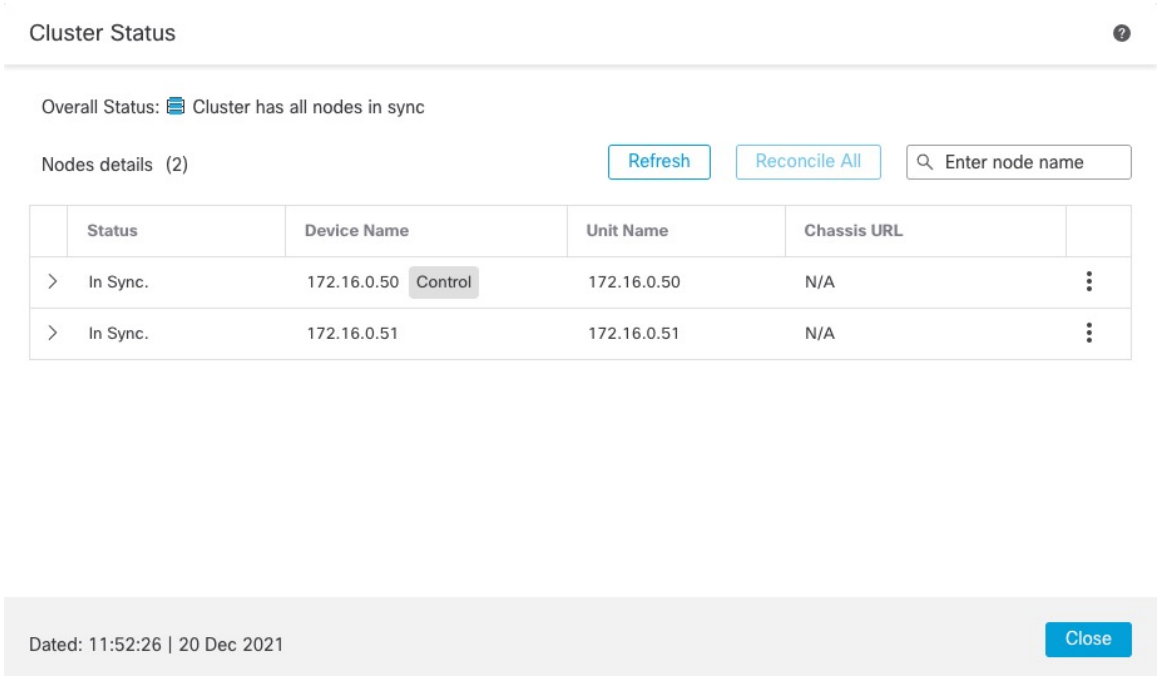
然后设置 **名称** 字段。



- **常规 (General) > 查看 (View) -** 点击**查看 (View)** 链接以打开**集群状态 (Cluster Status)** 对话框。



还可在**集群状态 (Cluster Status)** 对话框中点击**协调全部 (Reconcile All)**以重新注册数据单元。



步骤 8 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。

图 *6:* 设备设置

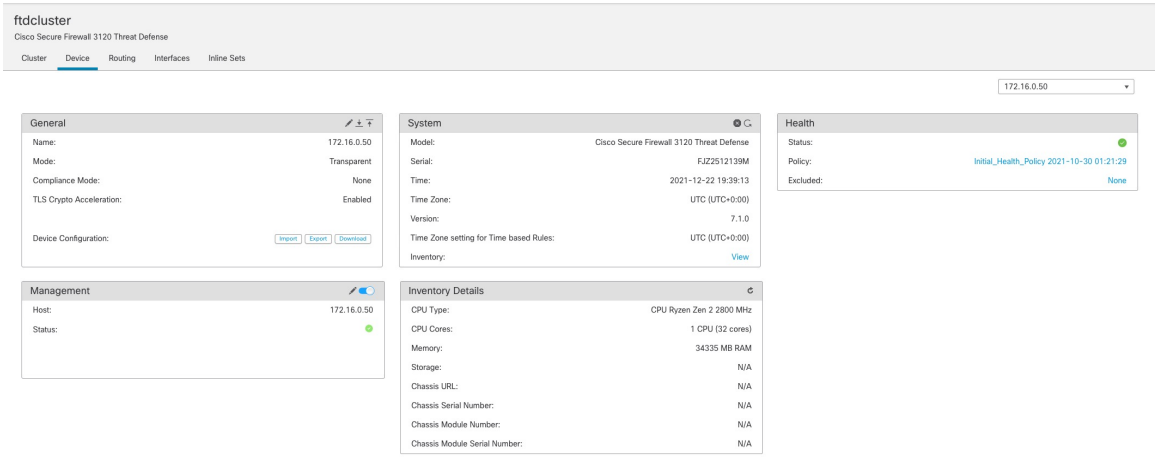
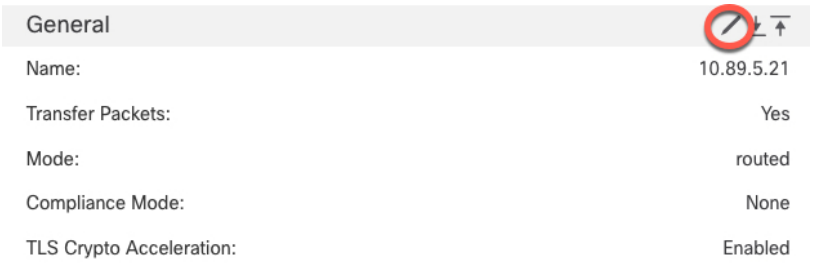
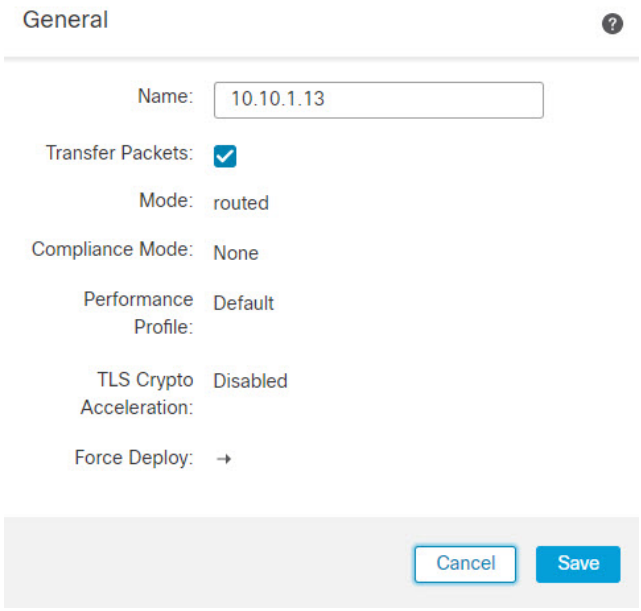


图 *7:* 选择节点

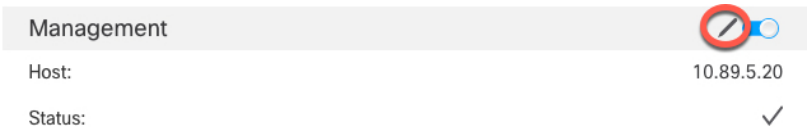
- **常规** > **名称**-通过点击 **编辑**（）更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理 (Management) > 主机 (Host)**-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。首先禁用连接，编辑**管理 (Management)** 区域中的**主机 (Host)** 地址，然后重新启用连接。



步骤 9 如果在未启用极大帧预留的情况下部署集群节点，则重新启动所有集群节点，以便启用集群控制链路所需的极大帧。请参阅关闭或重新启动设备。

如果您之前启用了极大帧预留，则可以跳过这一步。

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）和 VXLAN 开销（54 字节）。创建集群时，MTU 会被设置为比最高数据接口 MTU（默认为 1654）高 154 个字节。如果后来增加数据接口 MTU，请务必同时增大集群控制链路 MTU。例如，由于最大 MTU 为 9198 字节，因此最高的数据接口 MTU 可以是 9044，而集群控制链路则可以设置为 9198。请参阅配置 MTU。

注释 确保将连接到集群控制链路的交换机配置为正确（更高）的 MTU；否则，建立集群将失败。

配置接口

本节介绍如何将接口配置为与集群兼容的独立接口。独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于当前的控制节点。所有数据接口都必须是独立接口。

对于诊断接口，您可以配置 IP 地址池，也可以使用 DHCP；只有诊断接口支持从 DHCP 获取地址。要使用 DHCP，请勿使用此程序；而是照常配置（请参阅配置路由模式接口）。

注释 您不能使用子接口。

过程

步骤 1 选择 **对象** > **对象管理** > **地址池** 来添加 IPv4 和/或 IPv6 地址池。请参阅地址池。

至少包含与集群中的设备数量相同的地址。虚拟 IP 地址不属于此池，但需要位于同一网络中。无法提前确定分配到每台设备的确切本地地址。

步骤 2 选择 **设备** > **设备管理**，然后点击集群旁边的 **编辑**（ ）。

步骤 3 点击**接口 (Interfaces)**，然后点击一个数据接口的 **编辑**（ ）。

步骤 4 在 **IPv4**上，输入 **IP 地址** 和掩码。此 IP 地址是集群的固定地址，始终属于当前的控制设备。

步骤 5 从 **IPv4 地址池 (IPv4 Address Pool)** 下拉列表中，选择您创建的地址池。

注释 如果要手动将 MAC 地址分配给此接口，则需要使用 FlexConfig 来创建一个 **mac-address pool**。

步骤 6 在 **IPv6 > 基本 (Basic)** 中，从 **IPv6 地址池 (IPv6 Address Pool)** 下拉列表中，选择您创建的地址池。

步骤 7 按正常方式配置其他接口设置。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

管理集群节点

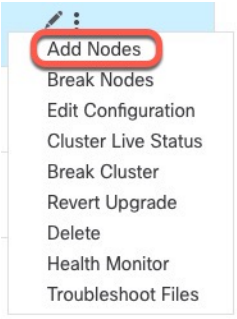
添加新的集群节点

您可以将一个或多个新的集群节点添加到现有的集群。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，点击集群的 **更多**（⋮），然后选择**添加节点 (Add Nodes)**。

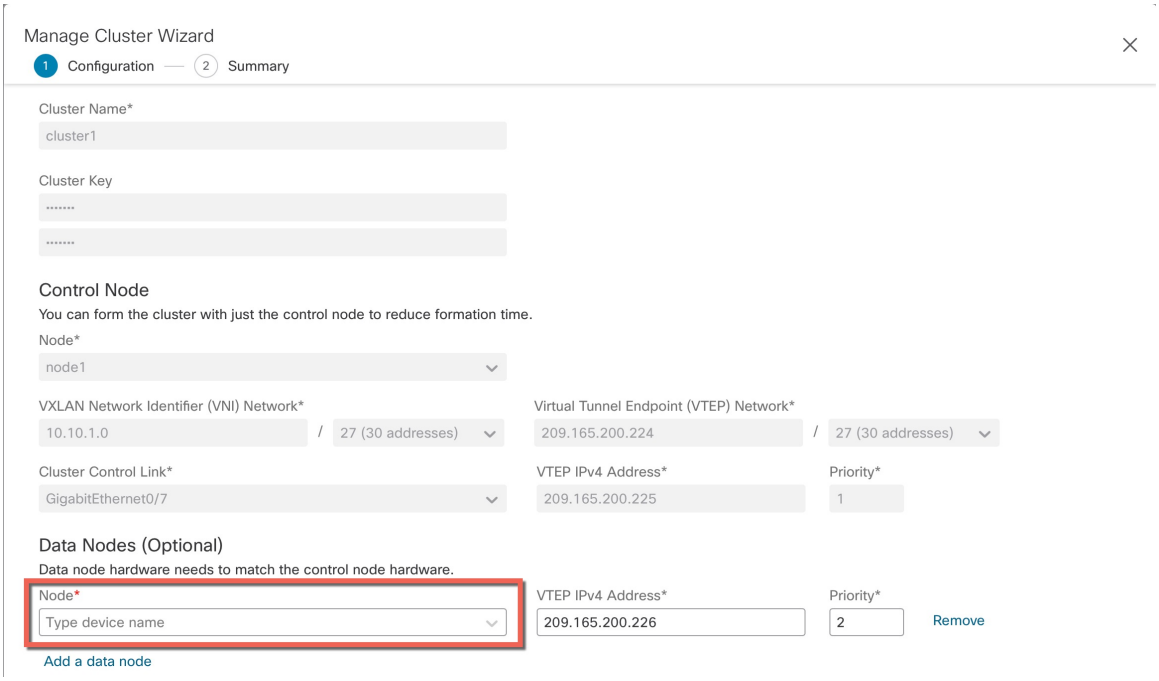
图 *8:* 添加节点



系统将显示**管理集群向导 (Manage Cluster Wizard)**。

步骤 2 从**节点 (Node)** 菜单中选择设备，然后根据需要调整 IP 地址和优先级。

图 *9:* 管理集群向导

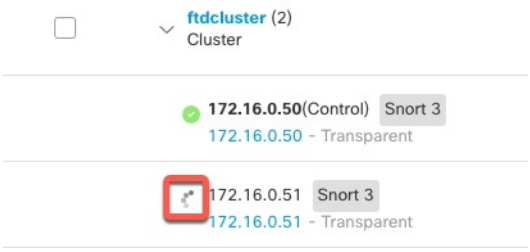


步骤 3 要添加其他节点，请点击**添加数据节点 (Add a data node)**。

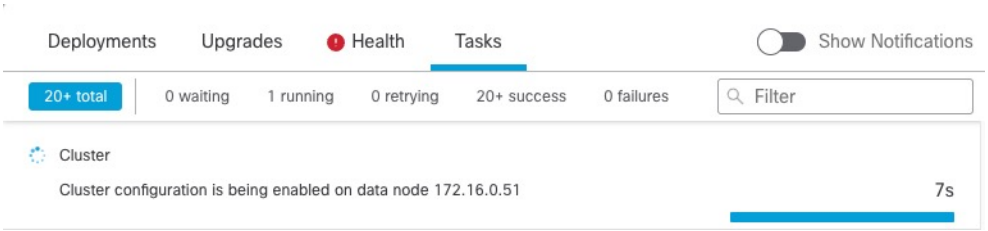
步骤 4 点击**继续**。查看**摘要 (Summary)**，然后点击**保存 (Save)**

当前正在注册的节点会显示加载图标。

图 *10:* 节点注册



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。



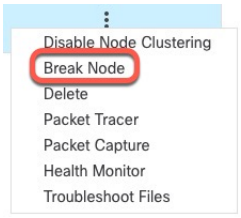
中断节点

您可以从集群中删除节点，使其成为一个独立设备。除非中断整个集群，否则您无法中断控制节点。数据节点的配置已被清除。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，点击您要中断的节点的 **更多**（⋮），然后选择**中断节点 (Break Node)**。

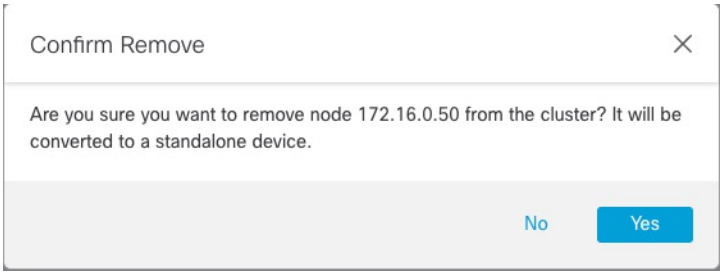
图 *11:* 中断节点



您可以选择通过选择**中断节点 (Break Nodes)** 从集群的“更多”(More) 菜单中断一个或多个节点。

步骤 2 系统会提示您确认中断；点击**是 (Yes)**。

图 *12:* 确认中断



您可以通过点击**通知 (Notifications)** 图标并选择**任务 (Tasks)** 来监控集群节点中断。

中断集群

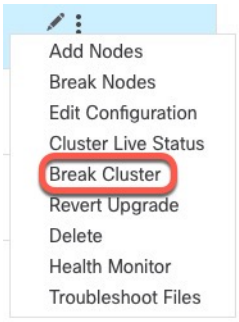
您可以中断集群并将所有节点都转换为独立设备。控制节点会保留接口和安全策略配置，而数据节点则会清除其配置。

过程

步骤 1 确保所有集群节点都由 管理中心 通过协调节点来管理。请参阅调整集群节点，第 22 页。

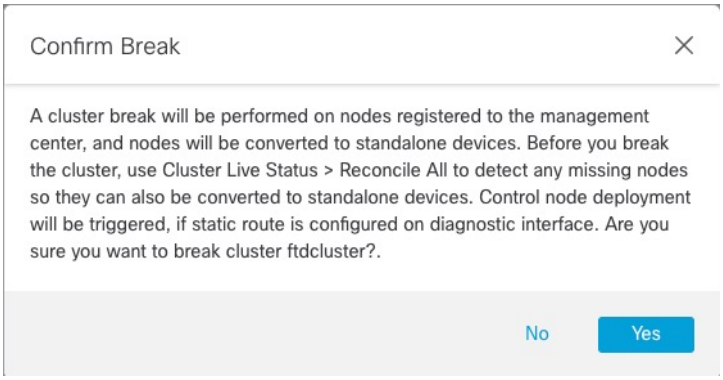
步骤 2 选择**设备 (Devices)** > **设备管理 (Device Management)**，点击集群的 **更多**（⋮），然后选择**中断集群 (Break Cluster)**。

图 *13:* 中断集群



步骤 3 系统会提示您断开集群；点击**是 (Yes)**。

图 *14:* 确认中断



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群中断。

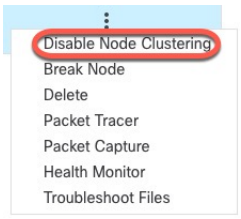
禁用集群

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。

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)**。

图 *15:* 禁用集群



如果在控制节点上禁用集群，则其中一个数据节点将成为新的控制节点。请注意，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。如果控制节点是集群中的唯一节点，则无法在该控制节点上禁用集群。

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 20 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 33 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。

更改控制节点

⚠

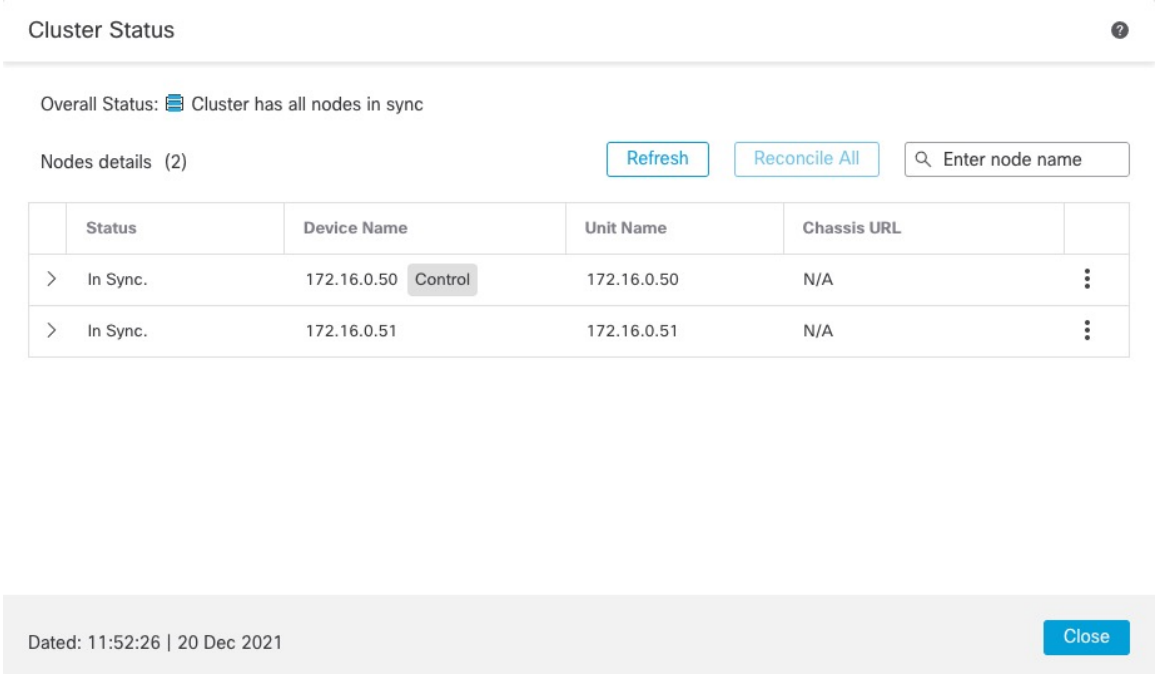
注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体单元，请使用本节中的程序。请注意，对集中功能而言，如果使用任何一种方法来强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

过程

步骤 1 通过依次选择 **设备** > **设备管理** > **更多**（⋮） >**集群实时状态**，打开 **集群状态** 对话框。

图 *16:* 集群状态



步骤 2 对于要成为控制设备的设备，请选择 **更多**（⋮） > **将角色更改为控制**。

步骤 3 系统将提示您确认角色更改。选中该复选框，然后点击 **确定**。

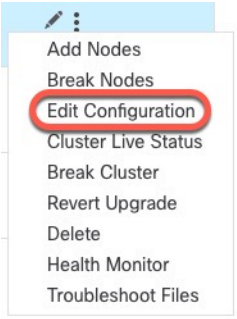
编辑集群配置

您可以编辑集群配置。如果您更改节点或节点优先级的 VTEP IP 地址之外的任何值，则集群将被自动中断和重组。在重组集群之前，您可能会遇到流量中断。如果您更改节点或节点优先级的 VTEP IP 地址，则只有受影响的节点会中断并重新添加到集群。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，点击集群的 **更多**（⋮），然后选择**编辑配置 (Edit Configuration)**。

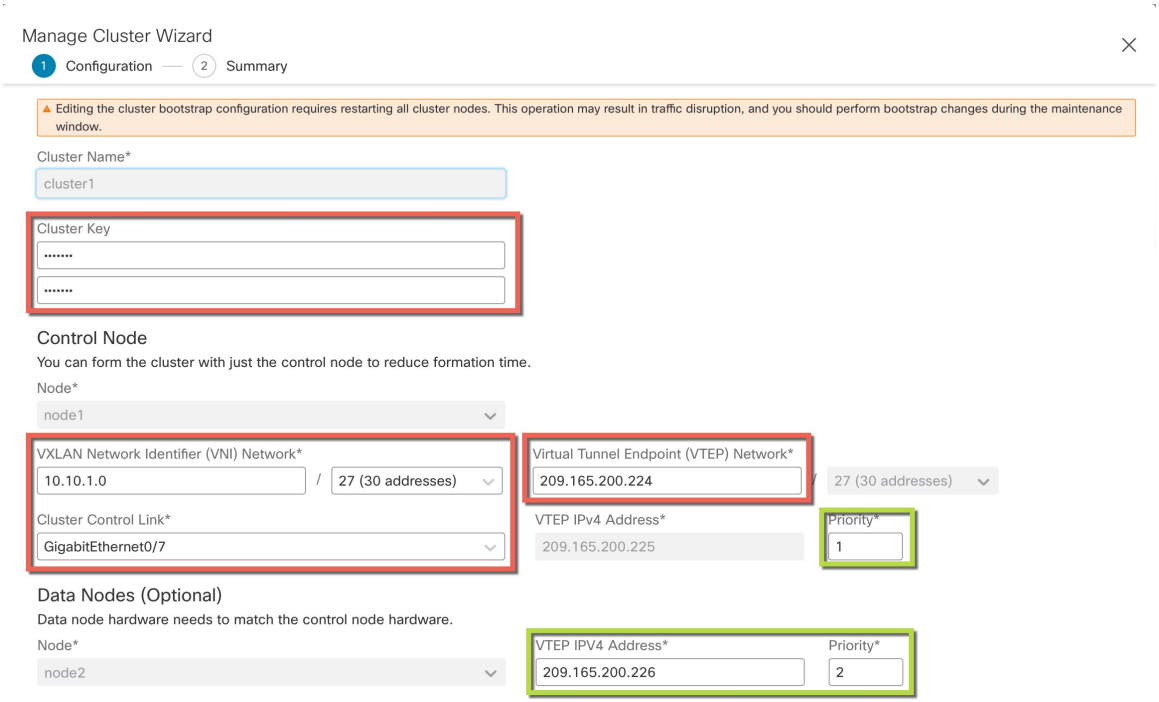
图 *17:* 编辑配置



系统将显示管理集群向导 **(Manage Cluster Wizard)**。

步骤 2 更新集群配置。

图 *18:* 管理集群向导



步骤 3 点击继续。查看摘要 **(Summary)**，然后点击保存 **(Save)**

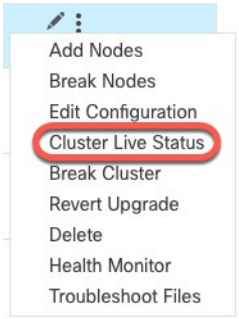
调整集群节点

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

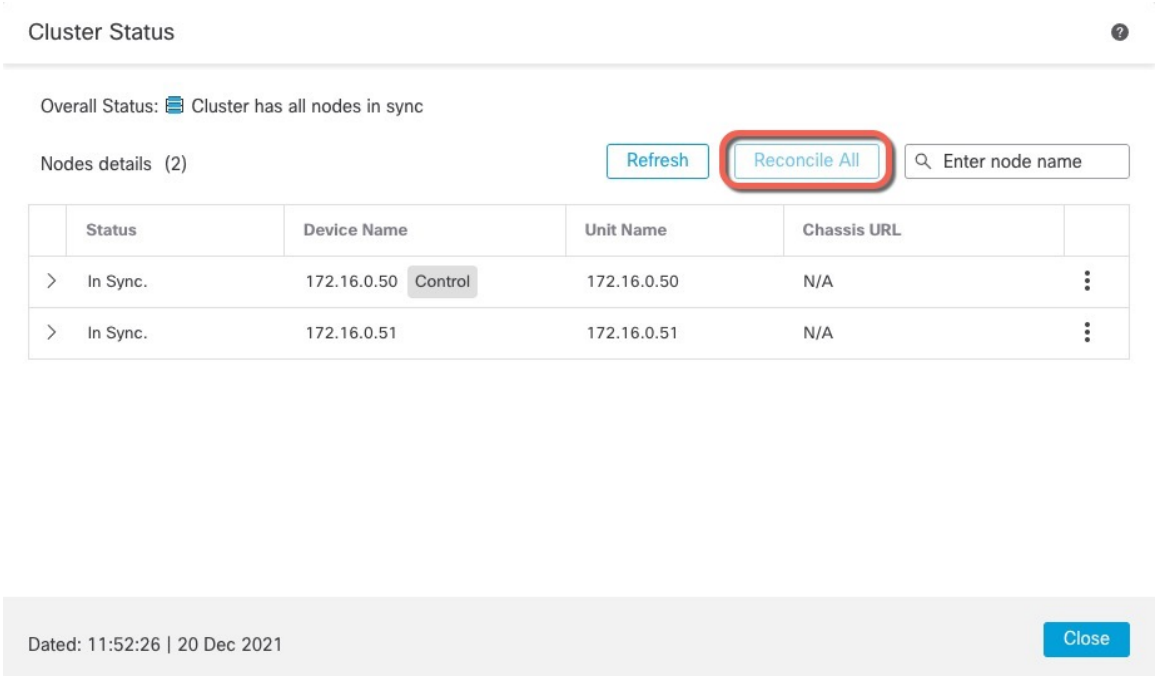
步骤 1 选择集群的 **设备** > **设备管理** > **更多**（⋮），然后选择 **集群实时状态** 来打开 **集群状态** 对话框。

图 *19:* 集群实时状态



步骤 2 点击**协调全部 (Reconcile All)**。

图 *20:* 协调全部



有关集群状态的详细信息，请参阅监控集群，第 25 页。

删除（注销）集群或节点并注册到新集群 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。

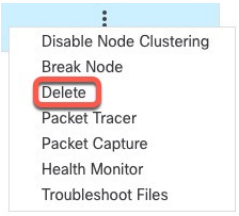
开始之前

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)**。

图 *21:* 删除集群或节点



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。请参阅在 CLI 中修改 威胁防御 管理接口。

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。

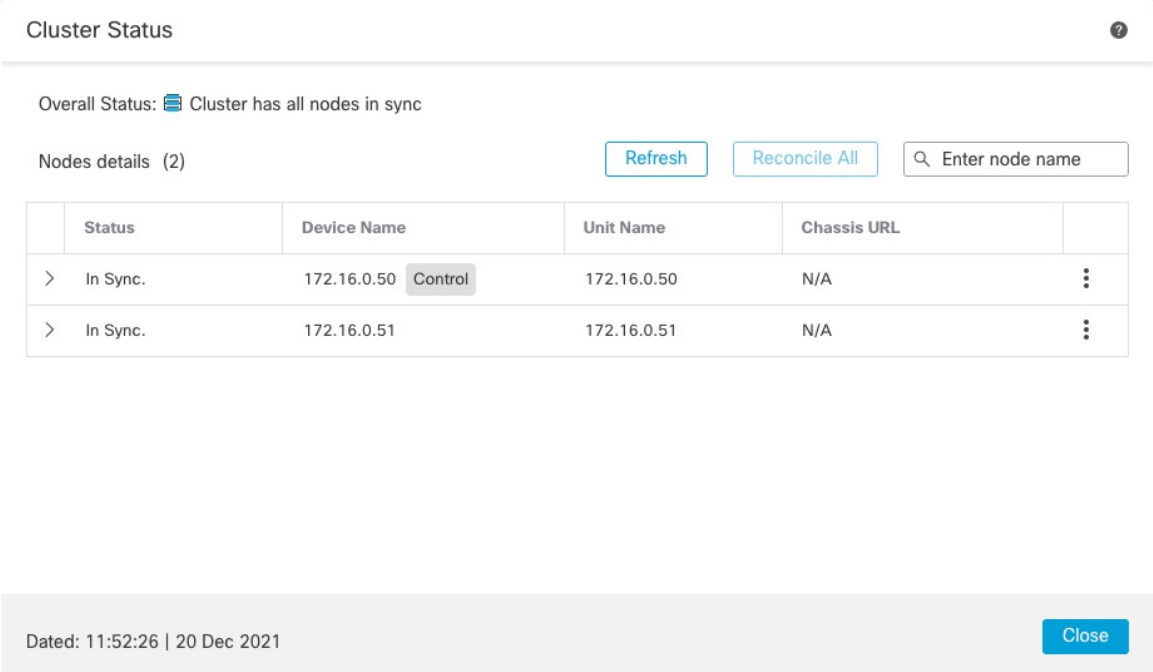
步骤 4 要重新添加已删除的节点，请参阅调整集群节点 ， 第 22 页。

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 *22:* 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 ***23:*** 节点摘要

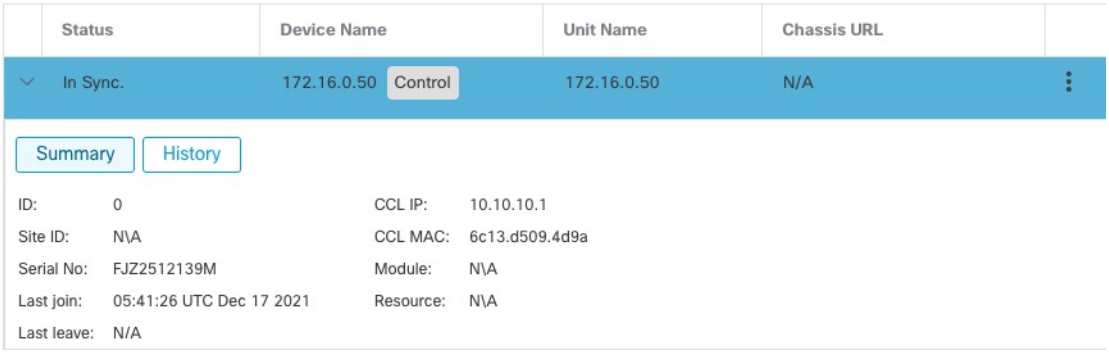
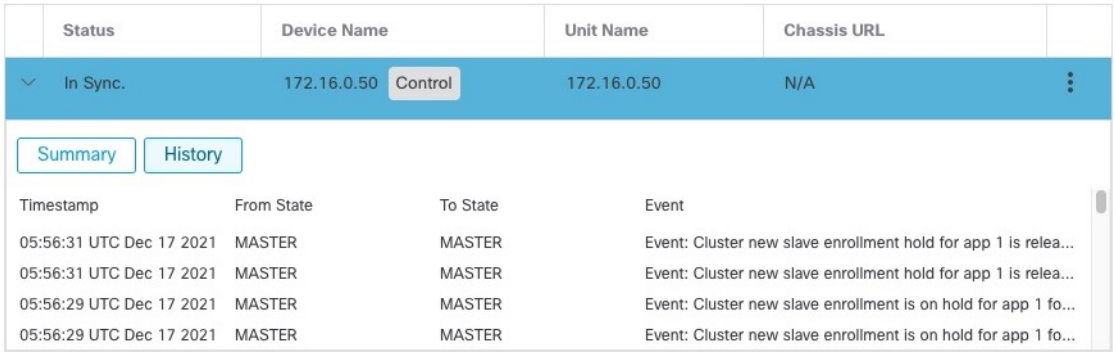


图 ***24:*** 节点历史记录



- **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。

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

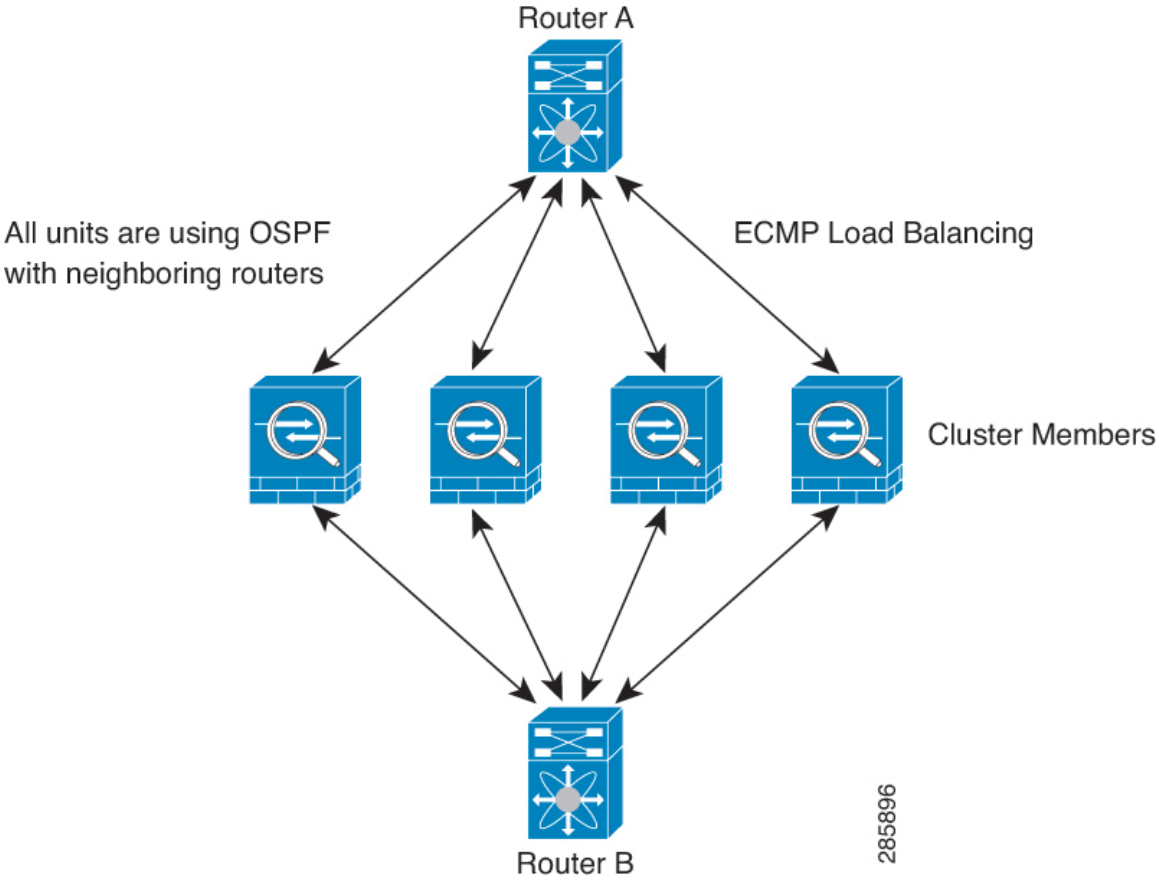
连接设置和集群

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 *25:* 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

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。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- 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。

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。

VPN 和集群

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。

注释 集群不支持远程接入 VPN。

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

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

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 *1:* 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。

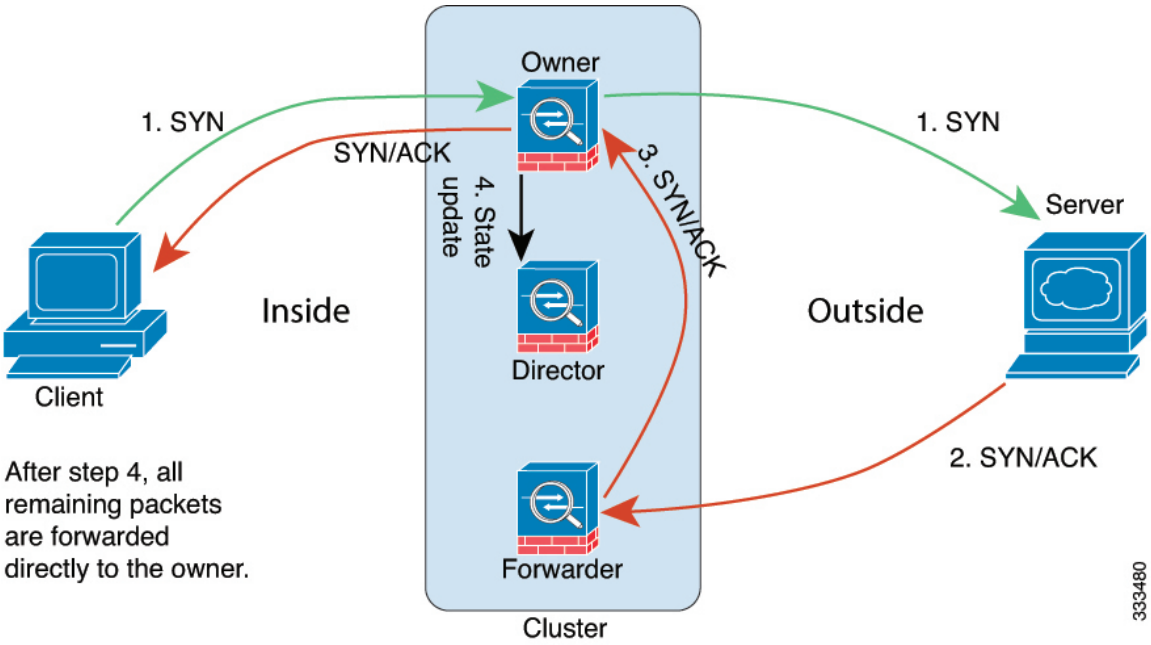
- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

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。

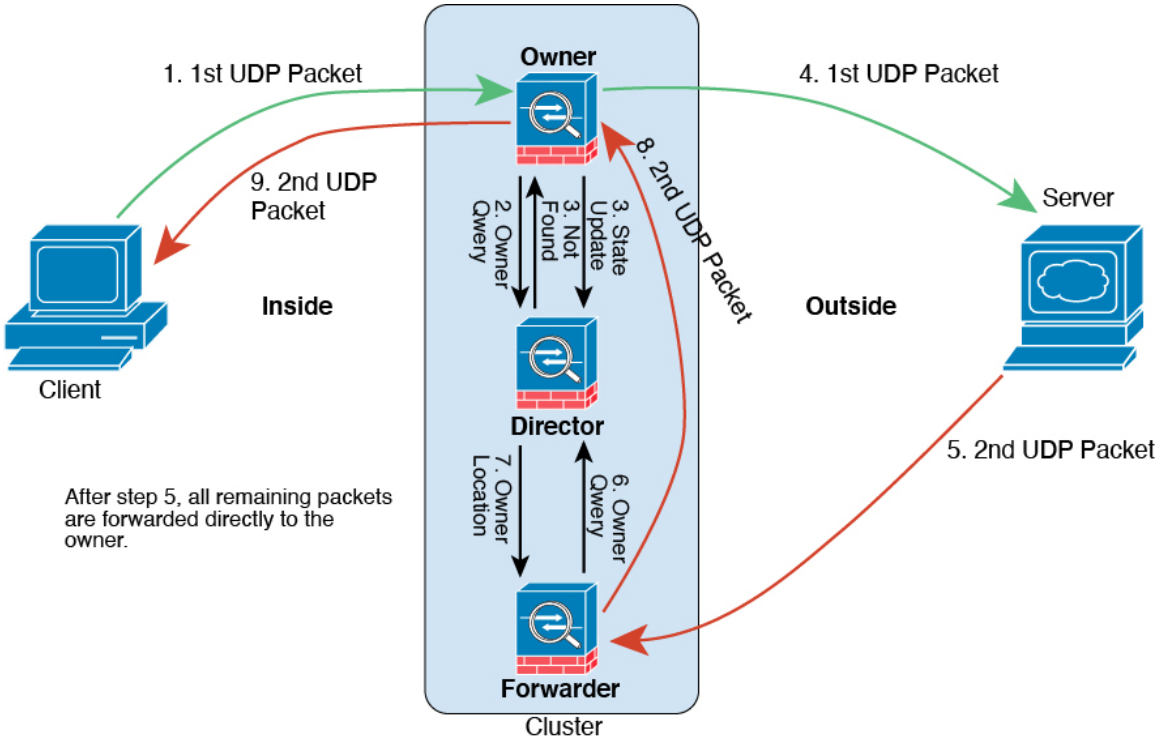


1. SYN 数据包从客户端发出，被传送到一台 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 威胁防御（基于负载均衡方法）。此 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，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 *26: 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。

私有云中 **Threat Defense Virtual** 群集的历史记录

特性	**Version**	详细信息
VMware 和 KVM 上 Threat Defense Virtual 的集群	7.2	threat defense virtual 支持 VMware 和 KVM 上最多 4 个节点的单个接口集群。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **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：VMware 和 KVM 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。