用于 Firepower 4100/9300 的集群

通过集群，您可以将多个威胁防御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。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 46 页。

关于 Firepower 4100/9300 机箱上的集群

在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 对于本地实例集群： 为设备间通信创建 集群控制链路 （默认情况下，使用端口通道 48）。

  对于多实例集群：您应该在一个或多个集群类型 Etherchannel 上预配置子接口；每个实例都需要自己的集群控制链路。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，此链路利用 Firepower 9300 背板进行集群通信。

  对于多机箱集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。

- 在应用中创建集群引导程序配置。

在部署集群时，机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。

- 将数据接口作为跨网络 接口分配给集群。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，跨网络接口不限于 EtherChannel，就像用于多个机箱的集群一样。 Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。 对于多机箱集群，必须对所有数据接口使用跨网络 EtherChannel。

注释 除管理接口以外，不支持单个接口。

- 向集群中的所有设备分配管理接口。

有关集群的详细信息，请参阅以下各节：

引导程序配置

在部署集群时，Firepower 4100/9300 机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。

集群成员

集群成员协调工作来实现安全策略和流量的共享。

一个集群成员是**控制**设备。系统自动确定控制设备。所有其他成员都是**数据**设备。

您必须仅在控制设备上执行所有配置；然后，配置将复制到数据设备。

有些功能在集群中无法扩展，控制设备将处理这些功能的所有流量。。

集群控制链路

对于本地实例集群：使用端口通道 48 接口自动创建集群控制链路。

对于多实例群集：您应该在一个或多个集群类型 Etherchannel 上预配置子接口；每个实例都需要自己的集群控制链路。

对于与一个 Firepower 9300 机箱内的安全模块隔离的集群，此接口没有成员接口。此群集类型 EtherChannel 利用 Firepower 9300 背板进行集群通信。 对于多机箱群集，必须将一个或多个接口添加到 EtherChannel。

对于 2 个机箱群集，请勿直接将群集控制链路从一个机箱连接到另一个机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

群集控制链路流量包括控制流量和数据流量。

确定集群控制链路规格

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

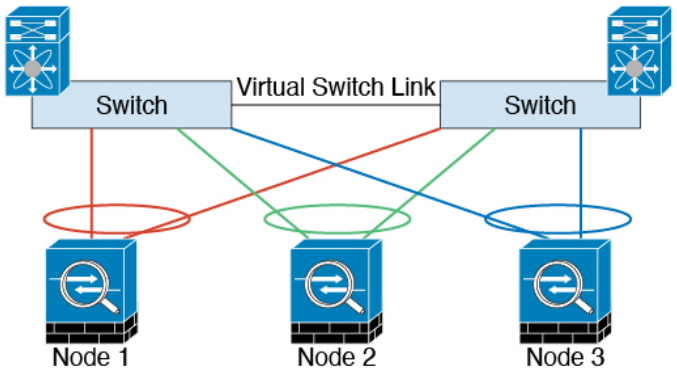
- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS)、虚拟端口通道 (vPC)、StackWise 或 StackWise Virtual 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是冗余系统的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到冗余系统中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。 对于多实例集群（通常使用同一 EtherChannel 的不同 VLAN 子接口），由

于 VLAN 分离，同一 IP 地址可用于不同的集群。集群控制链路网络不能包括设备之间的任何路由器；仅可执行第 2 层交换。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

必须为集群分配管理类型的接口。此接口是与跨网络接口相对立的一种特殊接口。通过管理接口，可以直接连接到每个设备。此管理接口不同于设备上的其他接口。它用于设置设备并将其注册到 Cisco Secure Firewall Management Center。它会使用自己的本地身份验证、IP 地址和静态路由。每个集群成员都使用您作为部分引导程序配置的管理网络中的独立 IP 地址。

管理逻辑接口与诊断逻辑接口之间共用管理接口。诊断逻辑接口是可选的，不能作为引导程序配置的一部分进行配置。诊断接口可随同其余数据接口一起进行配置。如果选择配置诊断接口，请将主集群 IP 地址配置为始终属于当前控制单元的集群固定地址。您也可以配置一个地址范围，使每个设备（包括当前控制单元在内）都能使用该范围内的本地地址。主集群 IP 地址可一致地诊断访问地址；当控制单元更改时，主集群 IP 地址会移到新的控制单元上，从而继续无缝地访问集群。对于 TFTP 或系统日志等出站管理流量，包括控制设备在内的每台设备都使用本地 IP 地址连接到服务器。

集群接口

对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，可以为集群分配物理接口或 EtherChannel 接口（也称为端口通道）。分配给集群的接口是对集群各个成员间的流量进行负载均衡的跨网络接口。

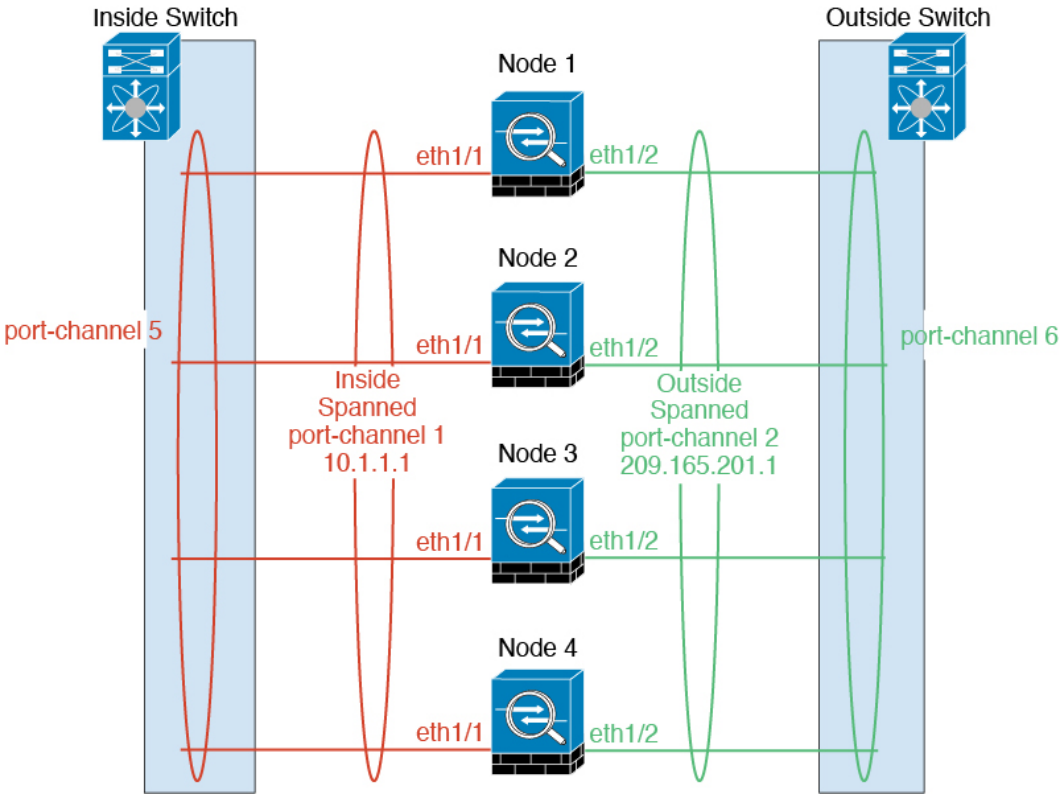
对于多机箱集群，只能为集群分配数据 EtherChannel 接口。这些跨网络 EtherChannel 在每个机箱上都包括相同的成员接口；在上游交换机上，所有这些接口都包括在一个 EtherChannel 内，因此交换机不知道它连接到多台设备。

除管理接口以外，不支持单个接口。

跨网络 EtherChannel

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。在路由模式和透明防火墙模式下均可配置跨区以太网通道。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。负载均衡属于 EtherChannel 固有的基本操作。

对于多实例集群，每个集群都需要专用数据 Etherchannel，不能使用共享接口或 VLAN 子接口。



连接到冗余交换机系统

我们建议将 EtherChannel 连接到冗余交换机系统（例如 VSS、vPC、StackWise 或 StackWise Virtual 系统），以便为接口提供冗余。

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。

集群许可证

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。

在将集群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。

集群要求和必备条件

群集型号支持

威胁防御 在以下型号上支持群集：

- Firepower 9300-您可以在集群中包含最多 16 个节点。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。支持多个机箱的集群，以及与一个机箱内的安全模块隔离的集群。
- Firepower 4100-使用多机箱集群时，最多支持 16 个节点。

用户角色

- 管理员
- 访问管理员
- 网络管理员

集群硬件和软件要求

集群中的所有机箱：

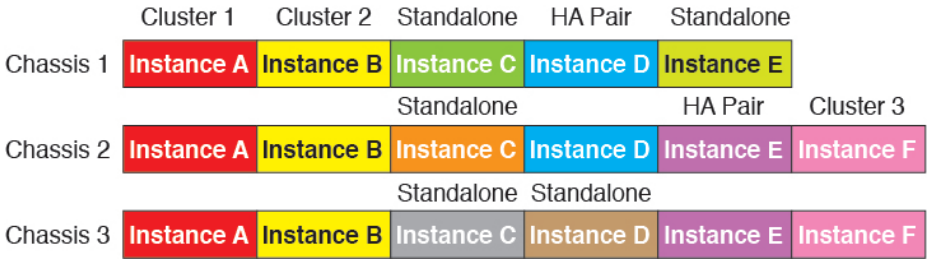
- 本地实例集群 -对于 Firepower 4100：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 容器实例集群 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。

- 除进行映像升级外，必须运行完全相同的 FXOS 和应用程序软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。 对于 威胁防御， 管理中心 必须使用同一台 NTP 服务器。请勿手动设置时间。

多实例集群要求

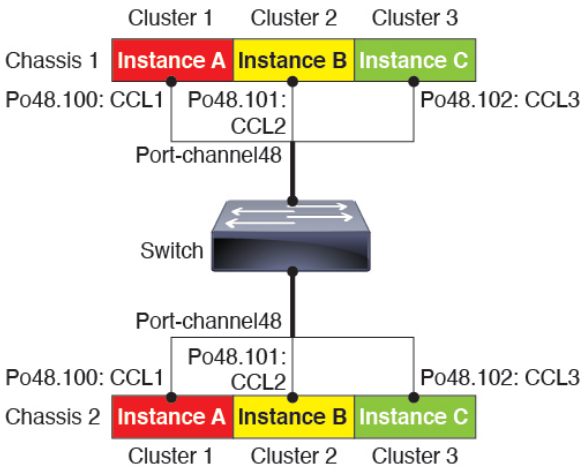
- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。

- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。



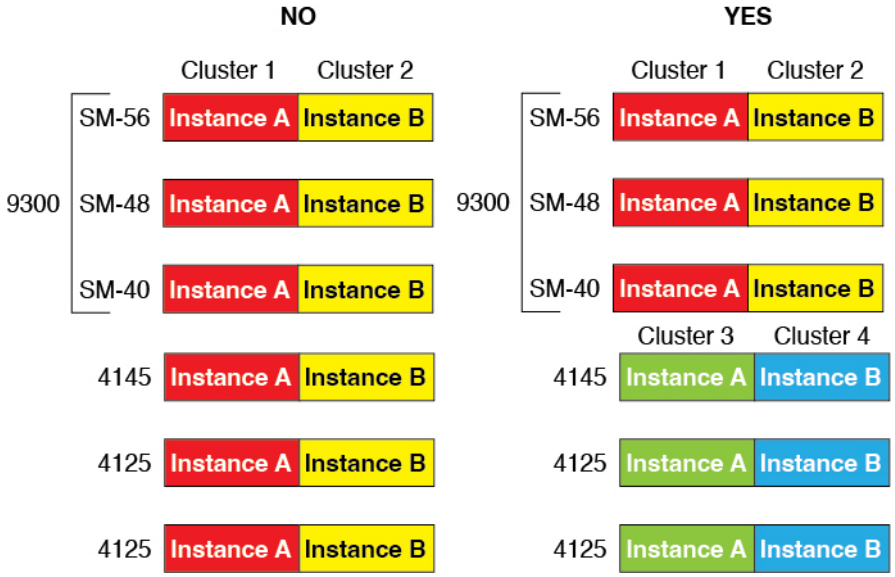
- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。

- 匹配资源配置文件 - 建议集群中的每个节点都使用相同的资源配置文件属性；但是，在将集群节点更改为使用其他资源配置文件或使用不同型号时，允许使用不匹配的资源。
- 专用集群控制链路 - 对于具有多个机箱的集群，每个集群都需要专用的集群控制链路。例如，每个集群可以在同一集群类型 EtherChannel 上使用单独的子接口，也可以使用单独的 Etherchannel。



- 无共享接口 - 集群不支持共享类型接口。但是，多个集群可以使用相同的管理接口和事件接口。
- 无子接口 - 多实例集群无法使用 FXOS 定义的 VLAN 子接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。
- 混合机箱型号 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器

实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



- 最多 6 个节点 - 在一个集群中最多可以使用六个容器实例。

交换机要求

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机的特性，请参阅思科 FXOS 兼容性。

集群准则和限制

集群的交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。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。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。

- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port** （请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

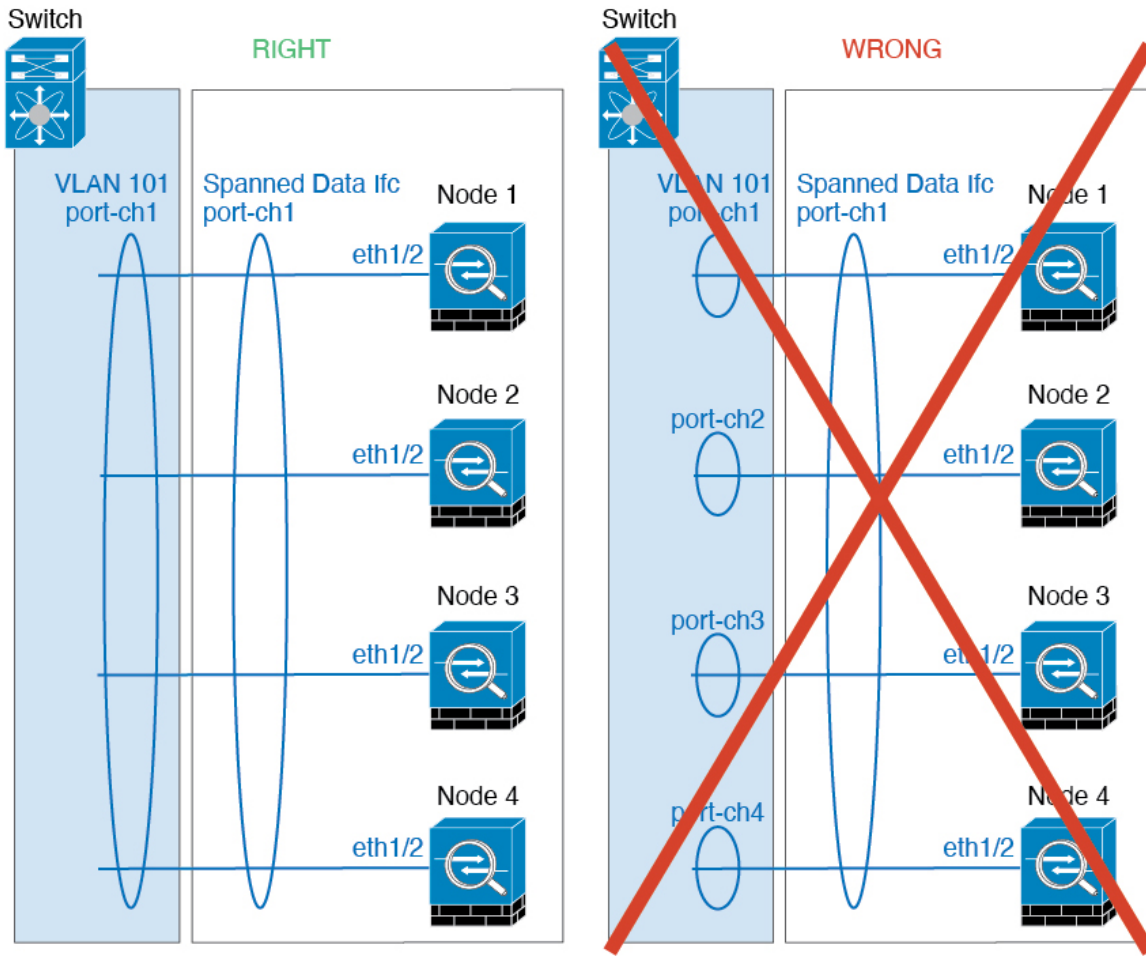
  router(config)# **port-channel** *id* **hash-distribution fixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

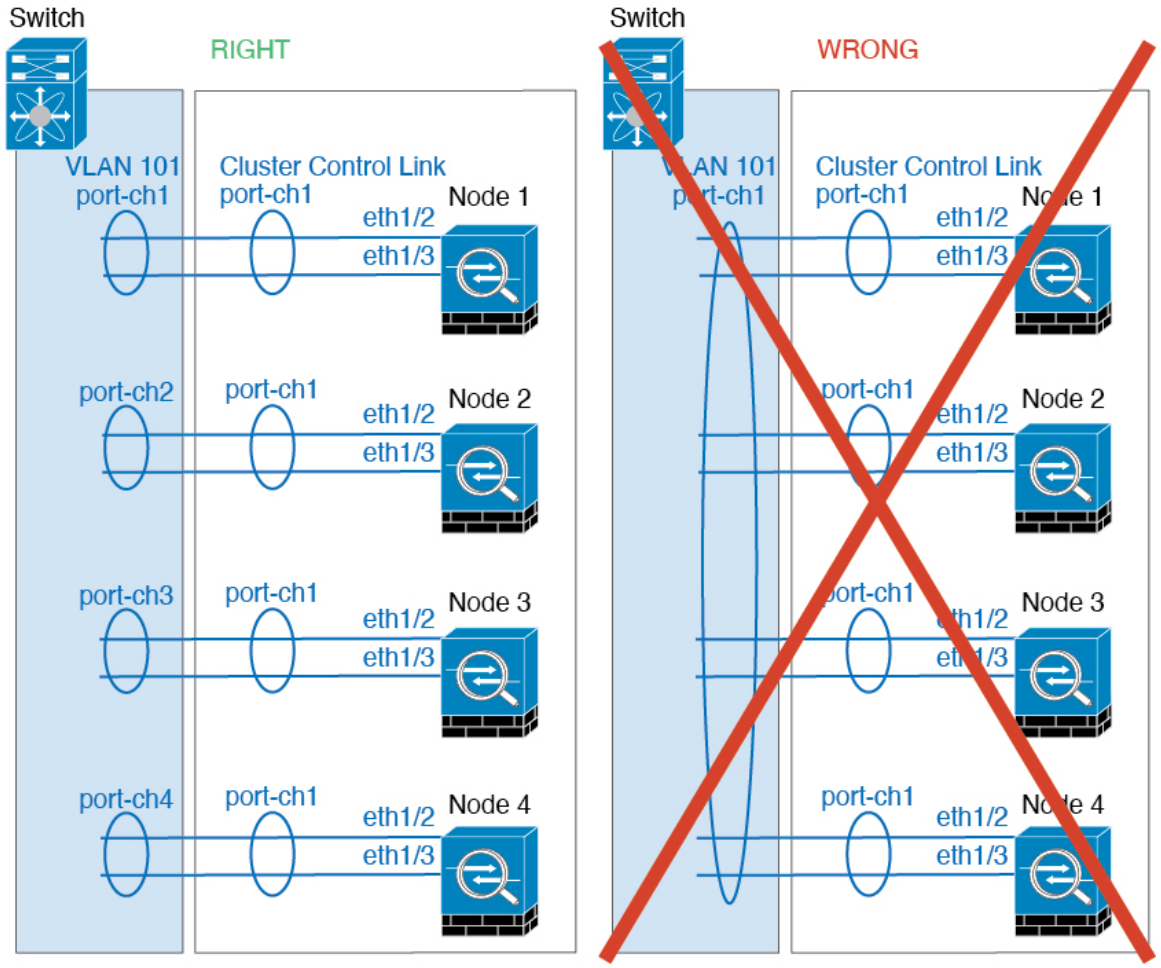
- Firepower 4100/9300 集群支持 LACP 正常融合。因此， 您可以在连接的 Cisco Nexus 交换机上启用 LACP 正常融合。
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

集群的 EtherChannel

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。
  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



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。在某些情况下，丢弃的数据包可能会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包会使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨区以太网通道接口的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器未限制 ICMP 错误消息时，会有大量 ICMP 消息被发回集群。这些消息可能会导致集群的某些设备出现高 CPU 问题，从而可能影响性能。因此，我们建议您限制 ICMP 错误信息。
- 我们建议将 EtherChannel 连接到 VSS、vPC、StackWise 或 StackWise Virtual，以实现冗余。
- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。
- 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。

默认值

- 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。
- 出现故障的集群控制链路的集群自动重新加入功能设置为无限次尝试，每隔 5 分钟进行一次。
- 出现故障的数据接口的集群自动重新加入功能设置为尝试 3 次，每 5 分钟一次，递增间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

配置集群

您可以从 Firepower 4100/9300管理引擎轻松部署集群。自动为每台设备生成所有初始配置。然后，可将设备添加到管理中心，再将它们组合成一个集群。

FXOS： 添加 威胁防御 群集

在本地模式下： 可以将集群添加到与机箱内的安全模块隔离的单个 Firepower 9300 机箱，也可以使用多个机箱。

在多实例模式下：您可以将一个或多个集群添加到与机箱内的安全模块隔离的单个 Firepower 9300 机箱（必须在每个模块上包含一个实例），或者在多个机箱上添加一个或多个集群。

对于多机箱群集，您必须单独配置每个机箱。在一个机箱上添加群集；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署

创建 威胁防御 集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。

对于多机箱群集，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

在 Firepower 9300 机箱中，必须对全部 3 个模块插槽或容器实例（每个插槽中有一个容器实例）启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传至 Firepower 4100/9300 机箱。
- 对于容器实例，如果您不想使用默认配置文件，则请根据为容器实例添加资源配置文件添加资源配置文件。
- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择**安全模块 (Security Modules)** 或**安全引擎 (Security Engine)**，然后点击重新初始化图标（）。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用

配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。

- 收集以下信息：
  - 管理接口 ID、IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址
  - 威胁防御 主机名和域名

过程

步骤 1 配置接口。

a) 部署集群之前，至少添加一个“数据”类型接口或 EtherChannel（也称为端口通道）。请参阅添加 EtherChannel（端口通道）或配置物理接口。

对于多机箱群集，所有数据接口必须为至少带有一个成员接口的跨区以太网通道。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关 EtherChannel 的详细信息，请参阅 集群准则和限制，第 9 页。

对于多实例集群，禁止在集群中使用 FXOS 定义的 VLAN 子接口或数据共享接口。仅支持应用定义的子接口。有关详细信息，请参阅FXOS 接口与应用接口。

b) 添加“管理”类型接口或 EtherChannel。请参阅添加 EtherChannel（端口通道）或配置物理接口。

管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口不同（在 FXOS 中，您可能会看到机箱管理接口显示为 MGMT、management0 或其他类似名称）。

对于多机箱集群，在各机箱上添加相同的管理接口。

对于多实例集群，可以在同一机箱上的多个集群之间或与独立实例共享同一管理接口。

c) 对于多机箱集群，将成员接口添加到集群控制链路 EtherChannel（默认情况下为端口通道 48）。请参阅 添加 EtherChannel（端口通道）。

请勿为与一个 Firepower 9300 机箱内的安全模块隔离的集群添加成员接口。例如，如果添加成员，则机箱假设此集群将使用多机箱，且将仅允许您使用跨区以太网通道。

在**接口**选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态**将显示为**失败**。对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，此 EtherChannel 无需任何成员接口，您可忽略此运行状态。

在各机箱上添加相同的成员接口。　集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关 EtherChannel 的详细信息，请参阅 集群准则和限制，第 9 页。

对于多实例集群，可以创建其他集群类型 Etherchannel。与管理接口不同，集群控制链路不可在多台设备之间共享，因此每个集群都需要一个集群接口。但是，建议使用 VLAN 子接口而不是多个 EtherChannel；请参阅下一步，将 VLAN 子接口添加到集群接口。

d) 对于多实例集群，将 VLAN 子接口添加到集群 EtherChannel，以便每个集群都有一个子接口。请参阅 为容器实例添加 VLAN 子接口。

如果向某个集群接口添加子接口，则不能将该接口用于本地集群。

e) （可选） 添加事件接口。请参阅添加 EtherChannel（端口通道）或配置物理接口。

此接口是 威胁防御 设备的辅助管理接口。要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅 威胁防御 命令参考中的 **configure network** 命令。

对于多机箱集群，在各机箱上添加相同的事件接口。

步骤 2 选择**逻辑设备 (Logical Devices)**。

步骤 3 依次点击**添加 (Add)** > **集群 (Cluster)**，并设置以下参数：

图 *1:* 本地集群

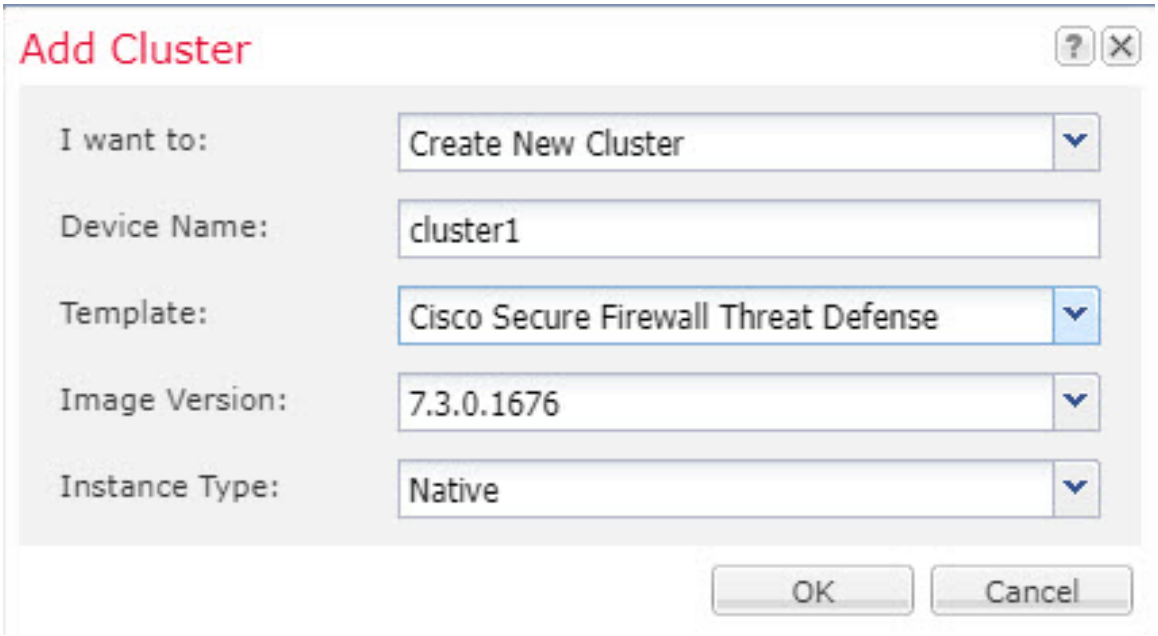
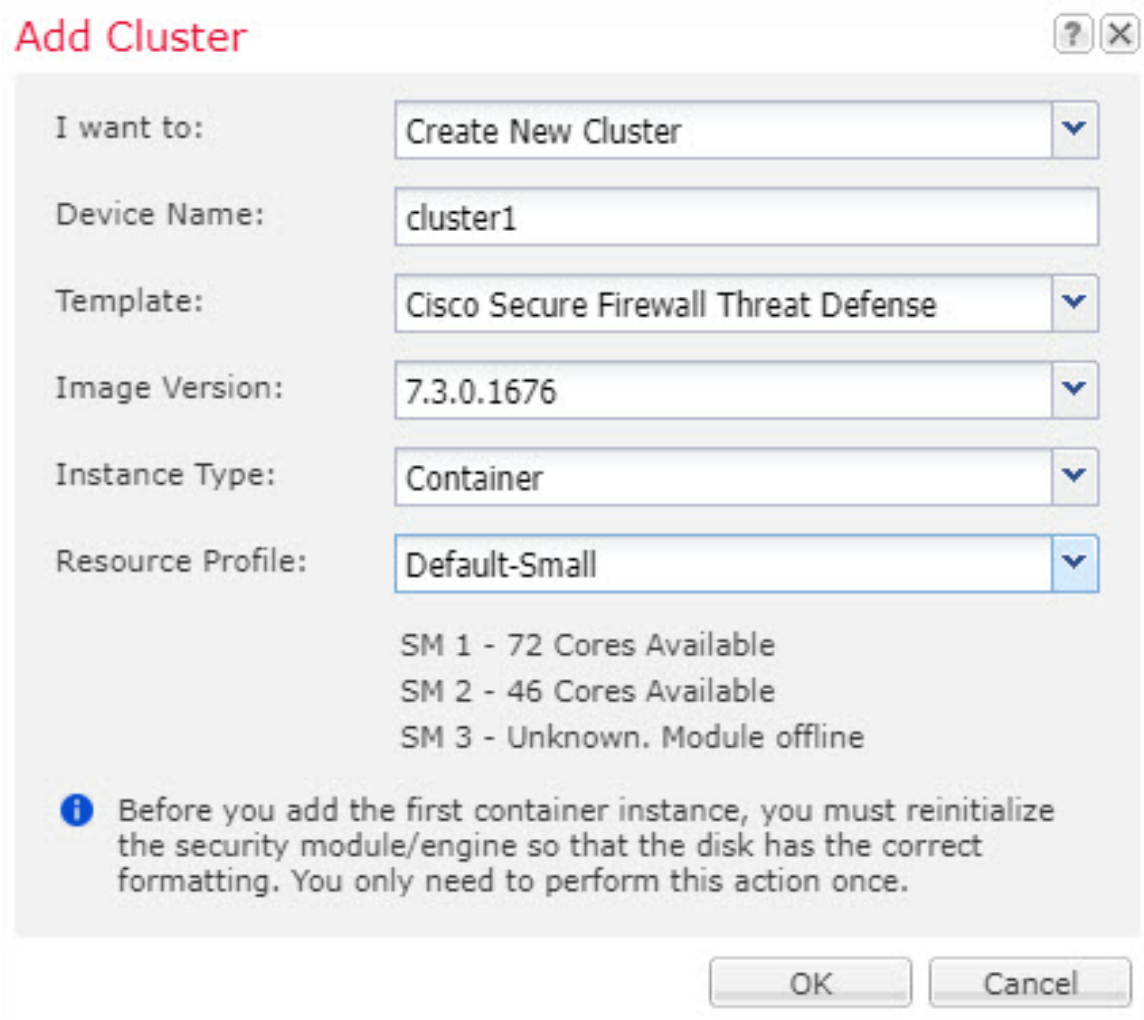


图 2: 多实例集群



a) 选择**我想：(I want to:)** > **新建集群 (Create New Cluster)**

b) 提供**设备名称**。

此名称由机箱管理引擎在内部用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

c) 对于**模板**，请选择 **Cisco Firepower 威胁防御**。

d) 选择**映像版本 (Image Version)**。

e) 对于**实例类型 (Instance Type)**， 类型选择**本地 (Native)** 或**容器 (Container)**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此您仅可安装一个本地实例。容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。

f) （仅限容器实例）对于**资源类型 (Resource Type)**，请从下拉列表中选择一个资源配置文件。

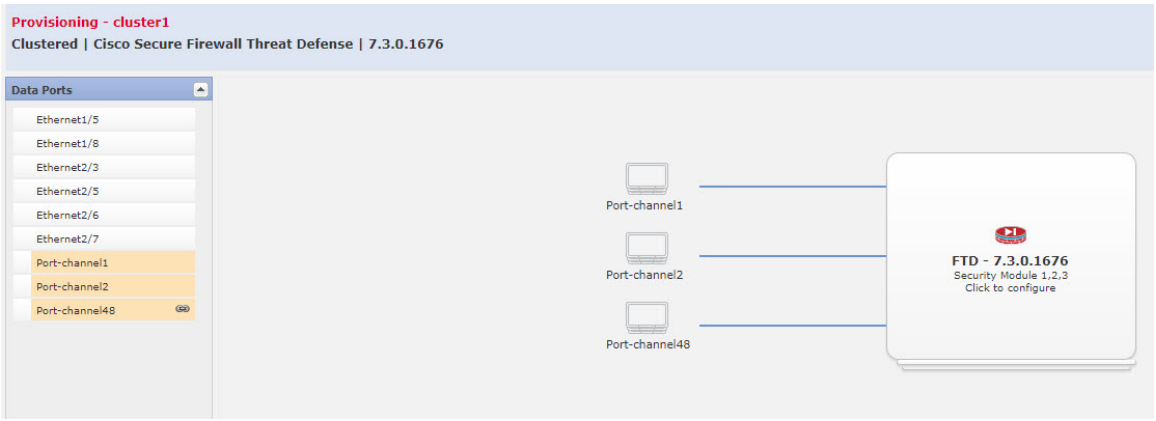
对于 Firepower 9300，此配置文件将应用于每个安全模块上的每个实例。例如，如果您使用的是不同的安全模块类型，并且想要在更低端型号上使用更多 CPU 时，可以稍后在此过程中为每个

安全模块设置不同的配置文件。建议您在创建集群之前选择正确的配置文件。如果您需要创建新配置文件，请取消集群创建操作，然后使用 为容器实例添加资源配置文件添加一个配置文件。

g) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 4 选择要分配给此集群的接口。



对于本地模式集群：默认情况下会分配所有有效接口。 如果定义了多个集群类型接口，请取消选中除一个接口外的所有接口。

对于多实例集群：选择要分配到集群的每个数据接口，并选择集群类型端口-通道或端口-通道子接口。

步骤 5 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 6 在**集群信息 (Cluster Information)** 页面上，完成以下操作。

图 *3:* 本地集群

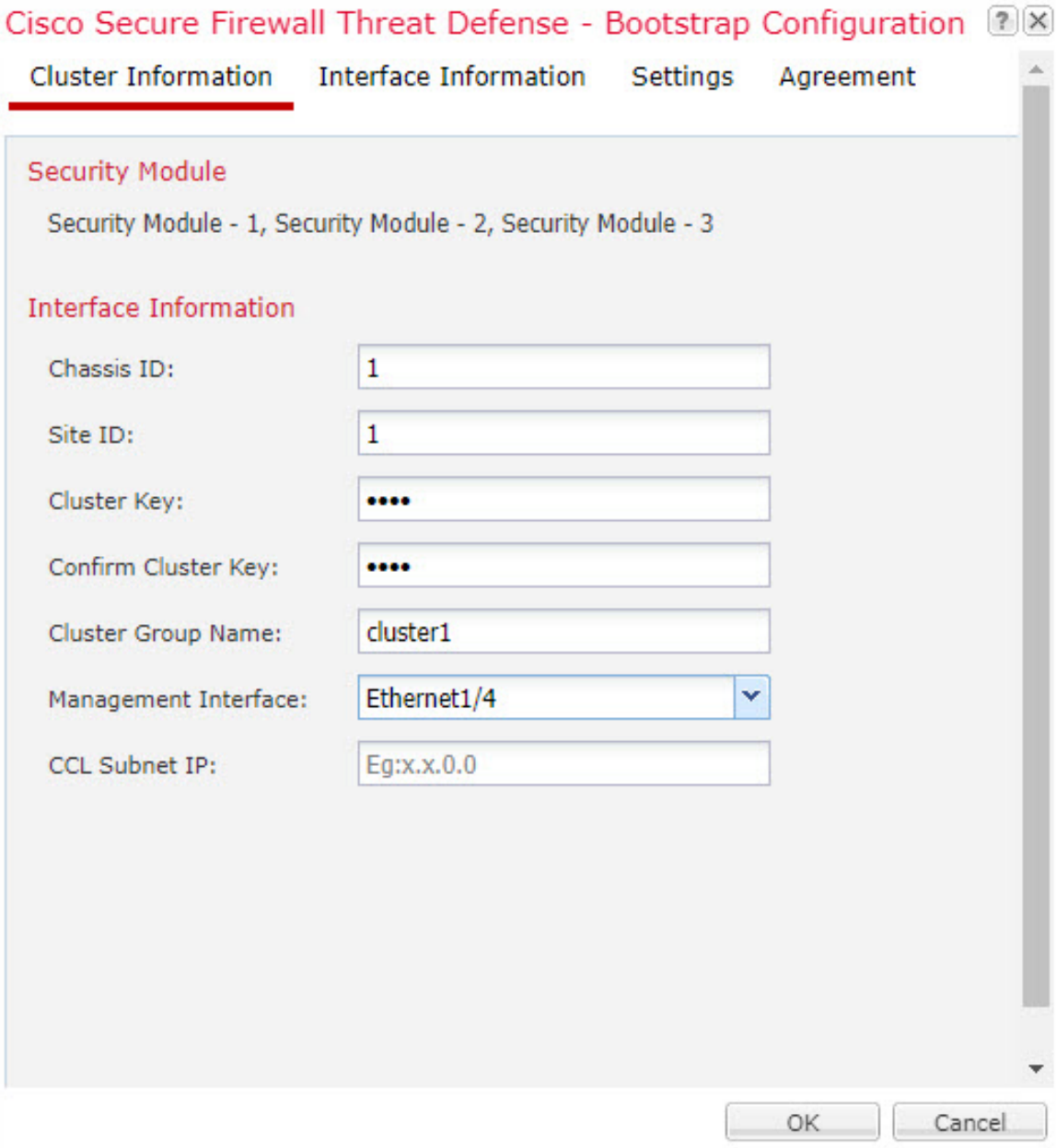
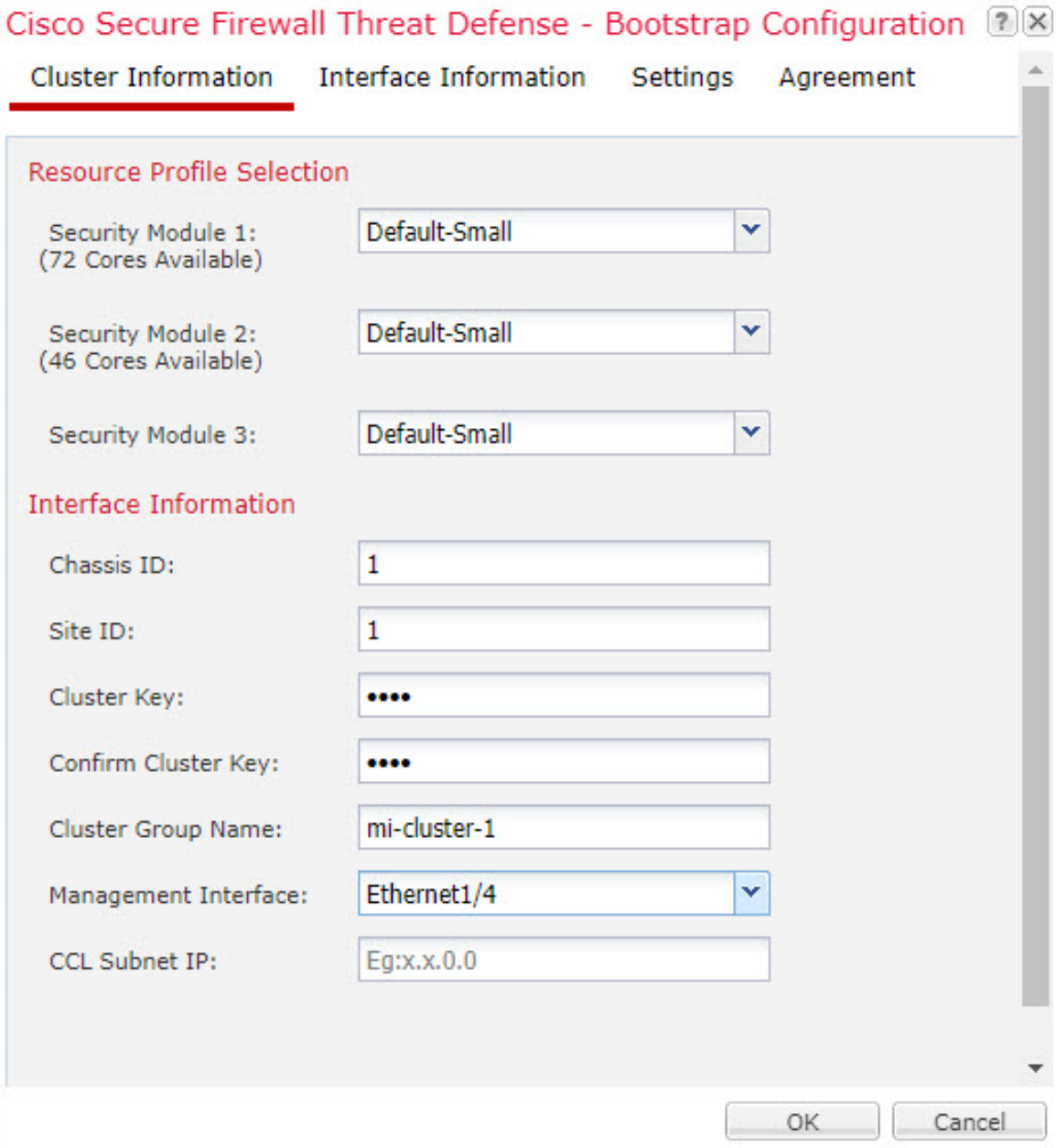

Cisco Secure Firewall Threat Defense - Bootstrap Configuration
Cluster Information
Interface Information
Settings
Agreement
Security Module
Security Module - 1, Security Module - 2, Security Module - 3
Interface Information
Chassis ID:
1
Site ID:
1
Cluster Key:
Confirm Cluster Key:
Cluster Group Name:
cluster1
Management Interface:
Ethernet1/4
CCL Subnet IP:
Eg:x.x.0.0
OK
Cancel

图 *4:* 多实例集群



a) （仅适用于 Firepower 9300 的容器实例）在**安全模块 (SM) 和资源配置文件选择 (Security Module (SM) and Resource Profile Selection)** 区域中，例如，如果您使用的是不同的安全模块类型，并且想要在更低端型号上使用更多 CPU 时，可以为每个模块设置不同的资源配置文件。

b) 对于多机箱集群，在 **机箱 ID** 中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

仅当向集群控制链路端口通道 48 添加成员接口时，才会显示此字段。

c) 对于站点间集群，在**站点 ID (Site ID)** 字段中输入此机箱的站点 ID（1 和 8 之间的整数）。FlexConfig 功能。仅可通过使用 管理中心 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。

d) 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项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。

e) 设置**集群组名称**，即逻辑设备配置中的集群组名称。

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

f) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

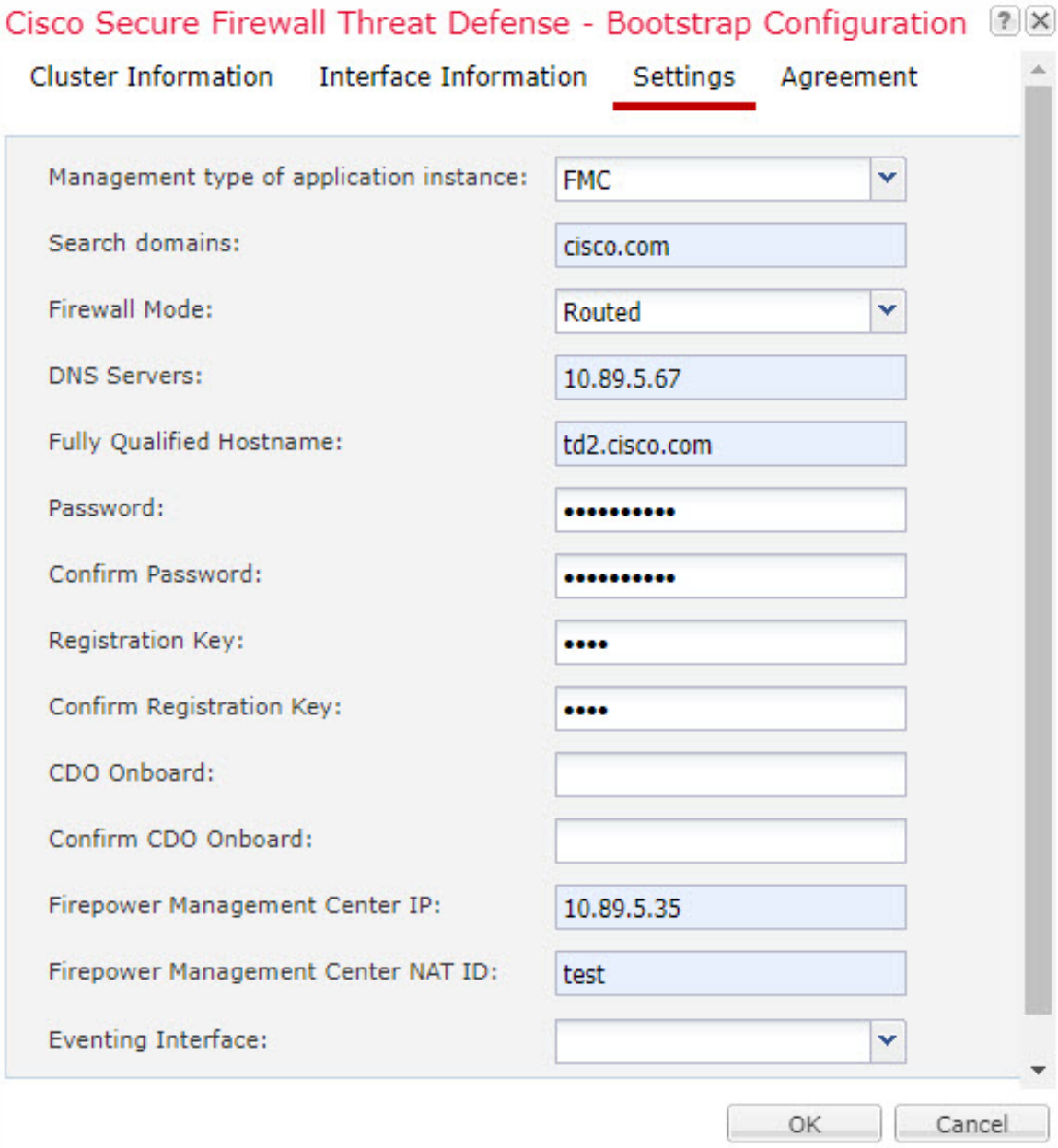
如果您分配一个支持硬件旁路功能的接口作为管理接口，则会收到一条警告消息，确认您是故意这样分配。

g) （可选） 将 **CCL 子网 IP** 设为 ***a.b*.0.0**。

默认情况下， 集群控制链路使用 127.2.0.0/16 网络。但是，某些网络部署不允许 127.2.0.0/16 流量通过。在这种情况下，请对集群指定唯一网络上的任意 /16 网络地址，环回 (127.0.0.0/8)、组播 (224.0.0.0/4) 和内部 (169.254.0.0/16) 地址除外。如果将该值设置为 0.0.0.0，则系统会使用默认网络。

机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：*a.b.chassis_id.slot_id*。

步骤 7 在**设置 (Settings)** 页面上，执行以下操作。



a) 在 **注册密钥** 字段中，输入注册期间 管理中心 与集群成员之间要共享的密钥。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加威胁防御时，需要在管理中心上输入相同的密钥。

b) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。

c) 在 **Firepower 管理中心 IP** 字段中，输入执行管理 管理中心的 IP 地址。如果您不知道 管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中输入口令。

d) （可选）对于容器实例，选择**是否允许 FTD SSH 会话专家模式 (Permit Expert mode from FTD SSH sessions)**：**是 (Yes)** 或**否 (No)**。专家模式提供 威胁防御 shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择**是 (Yes)**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否 (No)**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否 (No)** 以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 威胁防御 CLI 中使用 **expert** 命令。

e) （可选）在**搜索域 (Search Domains)** 字段中，输入管理网络的搜索域逗号分隔列表。

f) （可选）从**防火墙模式**下拉列表中选择**透明**或**路由**。

在路由模式中，威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

g) （可选）在 **DNS 服务器 (DNS Servers)** 字段中，输入用逗号分隔的 DNS 服务器列表。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

h) （可选）在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中，输入在添加集群作为新设备时还将在 管理中心 上输入的口令。

通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同一个注册密钥）：管理中心指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。您可以将长度介于 1 到 37 个字符之间的任意文本字符串指定为 NAT ID。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

i) （可选）在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入 威胁防御设备的完全限定名称。

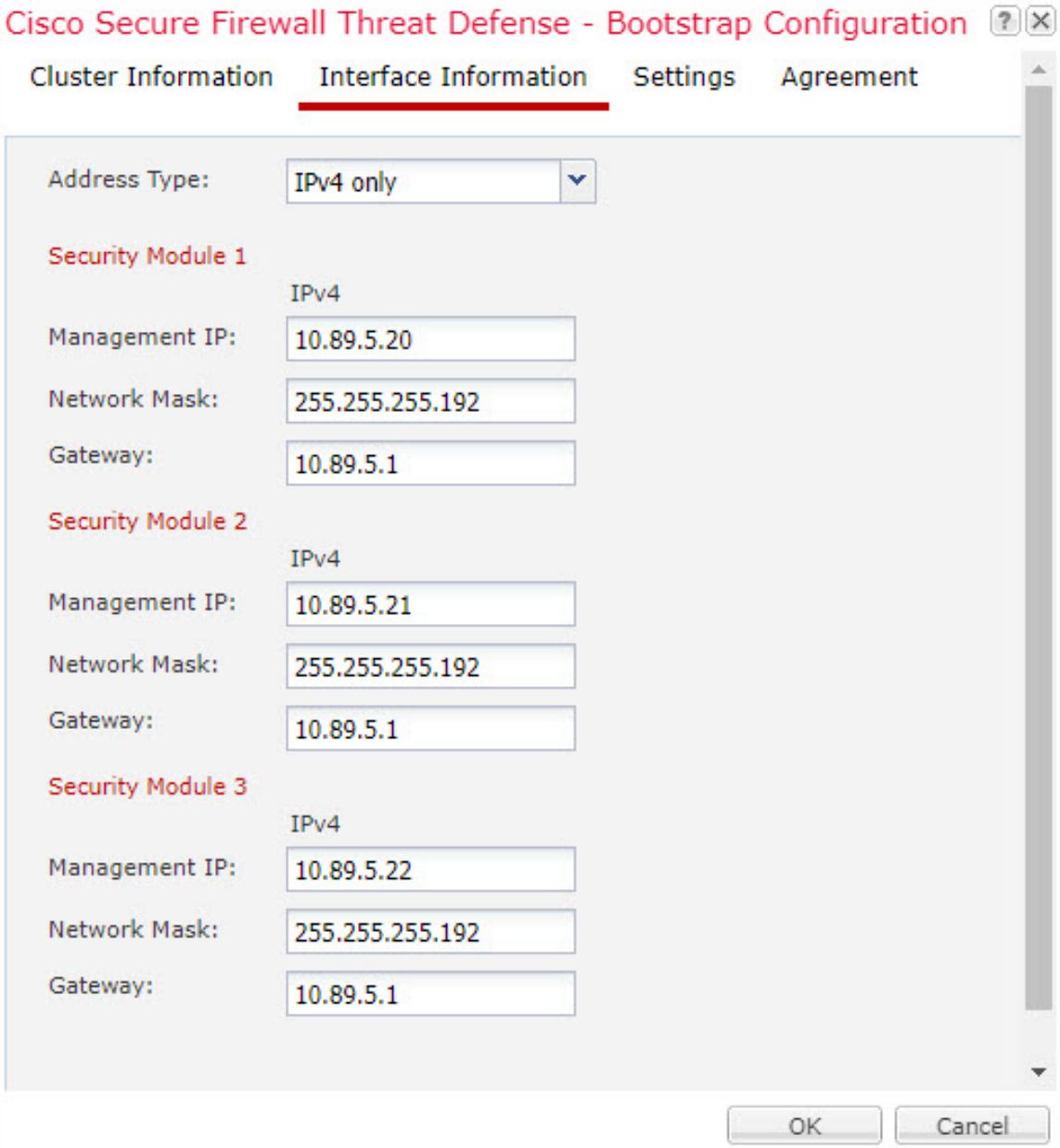
有效字符是从 a 到 z 的字母、从 0 到 9 的数字、点 (.) 和连字符(-)；最大字符数为 253。

j) （可选）从 **事件接口** 下拉列表中，选择发送事件时应当使用的接口。如果未指定，系统将使用管理接口。

要指定发送事件所用的独立接口，必须将接口配置为 *firepower-eventing* 接口。如果您分配一个支持硬件旁路功能的接口作为事件接口，则会收到一条警告消息，以确认您是故意这样分配的。

步骤 8 在**接口信息 (Interface Information)** 页面上，为集群中的每个安全模块配置一个管理 IP 地址。从**地址类型 (Address Type)** 下拉列表中选择地址类型，然后为每个安全模块填写以下字段。

注释 您必须为机箱中全部 3 个模块插槽设置 IP 地址，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。



a) 在**管理 IP (Management IP)** 字段中，配置 IP 地址。

在同一网络上为每个模块指定唯一 IP 地址。

b) 输入**网络掩码**或**前缀长度**。

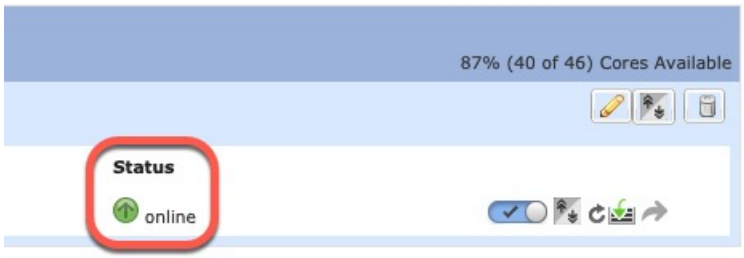
c) 输入**网络网关**地址。

步骤 9 在**协议**选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 10 点击**确定 (OK)** 关闭配置对话框。

步骤 11 单击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其 **状态** 显示为 **在线** 时，您可以 添加剩余的集群机箱；或对于同一个 Firepower 9300 机箱内的安全模块隔离的集群， 则可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。



步骤 12 对于多机箱集群，将下一个机箱添加到集群中：

a) 在第一个 机箱管理器机箱上，点击右上角的 **显示配置图标** ，复制显示的集群配置

b) 连接到下一个机箱上的 机箱管理器，然后按照此程序添加逻辑设备。

c) 选择**我想要：(I want to:) > 加入现有集群 (Join an Existing Cluster)**。

d) 点击**确定 (OK)**。

e) 在**复制集群详细信息**对话框中，粘贴第一个机箱的集群配置，然后点击**确定**。

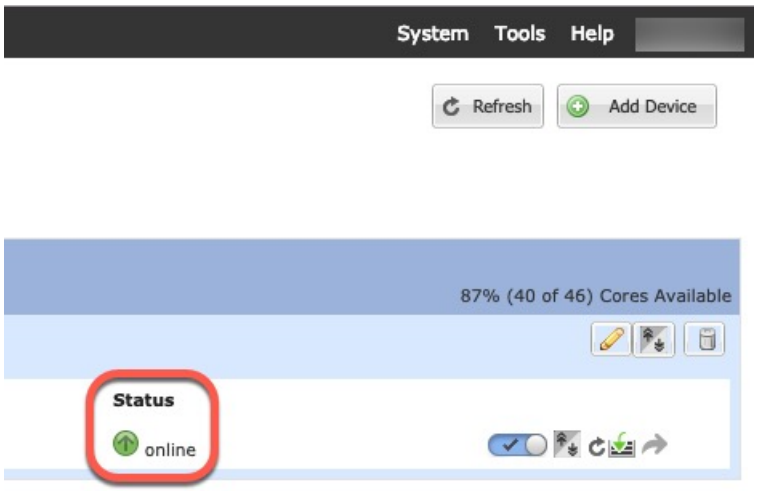
f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- **机箱 ID** - 输入唯一的机箱 ID。
- **站点 ID** - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。仅可通过使用 管理中心 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。
- **集群密钥** -（未预填充）输入相同的集群密钥。
- **管理 IP** - 将每个模块的管理地址更改为与其他集群成员位于同一网络中的唯一 IP 地址。

点击**确定 (OK)**。

g) 单击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在每个集群成员的**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当每个集群成员的逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。



步骤 13 使用管理 IP 地址将控制设备添加到 管理中心。

所有集群设备必须位于 FXOS 上成功建立的集群中，才能将它们添加到 管理中心。

然后，管理中心 会自动检测数据设备。

添加更多集群节点

在现有集群中添加或替换 威胁防御 集群节点。 在 FXOS 中添加新的集群节点时， 管理中心 会自动添加该节点。

注释 此程序中的 FXOS 步骤仅适用于添加新机箱；如果将新模块添加或替换到已启用群集的 Firepower 9300，则该模块将自动添加。

开始之前

- 如果是替换，则必须从 管理中心中删除旧的集群节点。当您将其替换为一台新节点时，它将被视为 管理中心上的一个新设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

过程

步骤 1 如果之前使用 管理中心升级了 威胁防御 映像，请在集群中 的每个机箱上执行以下步骤。

当您从 管理中心升级时，FXOS 配置中的启动版本未更新，并且机箱上未安装独立软件包。这两个项目都需要手动设置，以便新节点可以使用正确的映像版本加入集群。

注释 如果仅应用了补丁版本，则可以跳过此步骤。Cisco 不为补丁提供独立软件包。

a) 使用 **系统** > **更新** 页面在机箱上安装运行 威胁防御 映像。
b) 点击 **逻辑设备**，然后点击 设置版本图标（）。对于具有多个模块的 Firepower 9300，请设置每个模块的版本。

   启动版本 显示您部署时使用的原始软件包。**当前版本** 显示升级到的版本。

c) 在 **新版本** 下拉菜单中，选择您上传的版本。此版本应与显示的 **当前版本** 匹配，并将启动版本设置为与新版本匹配。
d) 在新机箱上，确保安装了新映像包。

步骤 2 在现有集群机箱 机箱管理器上，点击 **逻辑设备**。

步骤 3 单击右上角的**显示配置图标**；复制显示的集群配置。

步骤 4 连接到新机箱上的 机箱管理器，然后单击 **添加** > **群集**。

步骤 5 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

步骤 6 点击**确定 (OK)**。

步骤 7 在**复制集群详细信息**对话框中，粘贴第一个机箱的集群配置，然后点击**确定**。

步骤 8 点击屏幕中心的设备图标。集群信息已部分预填充，但您必须填写以下设置：

图 *5:* 集群信息

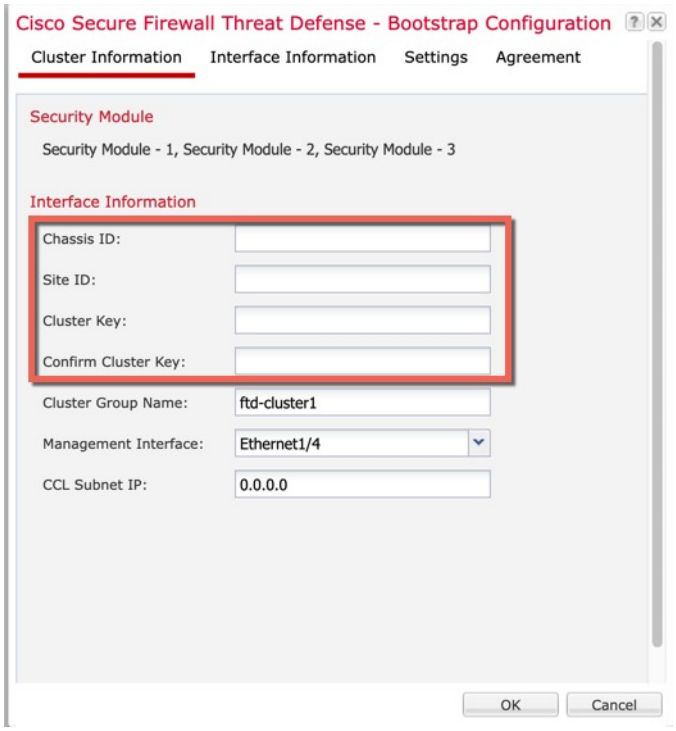


图 *6:* 接口信息

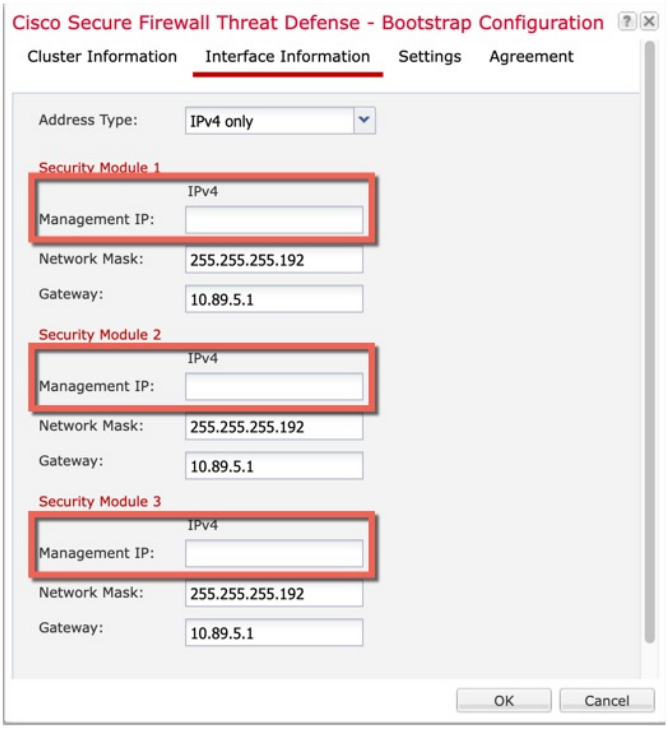
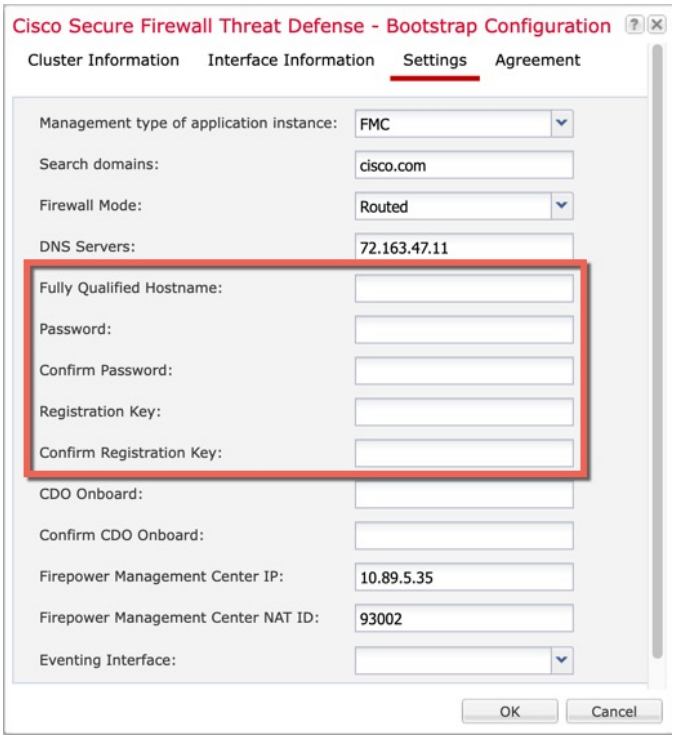

Cisco Secure Firewall Threat Defense - Bootstrap Configuration
Cluster Information
Interface Information
Settings
Agreement
Address Type:
IPv4 only
Security Module 1
IPv4
Management IP:
Network Mask:
255.255.255.192
Gateway:
10.89.5.1
Security Module 2
IPv4
Management IP:
Network Mask:
255.255.255.192
Gateway:
10.89.5.1
Security Module 3
IPv4
Management IP:
Network Mask:
255.255.255.192
Gateway:
10.89.5.1
OK
Cancel

图 *7:* 设置

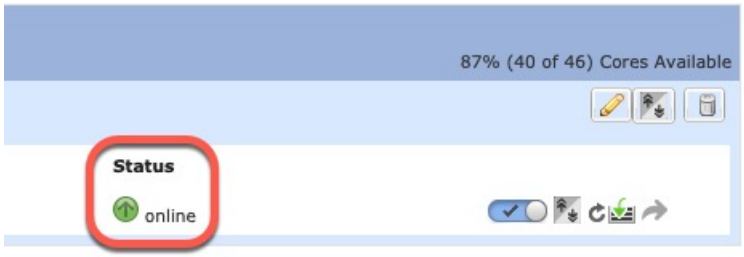

Cisco Secure Firewall Threat Defense - Bootstrap Configuration
Cluster Information
Interface Information
Settings
Agreement
Management type of application instance:
FMC
Search domains:
cisco.com
Firewall Mode:
Routed
DNS Servers:
72.163.47.11
Fully Qualified Hostname:
Password:
Confirm Password:
Registration Key:
Confirm Registration Key:
CDO Onboard:
Confirm CDO Onboard:
Firepower Management Center IP:
10.89.5.35
Firepower Management Center NAT ID:
93002
Eventing Interface:
OK
Cancel

- **机箱 ID**-输入 唯一 机箱 ID。
- **站点 ID** - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。此功能仅可使用 管理中心 FlexConfig 功能进行配置。
- **集群密钥**-输入 相同 集群密钥。
- **管理 IP**-将每个模块的管理地址更改为与其他集群成员位于同一网络中的 唯一 IP 地址。
- **完全限定主机名**-使用 相同 主机名。
- **密码**-输入 相同 密码。
- **注册密钥**-输入 相同 注册密钥。

点击**确定 (OK)**。

步骤 9 单击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在每个集群成员的**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当每个集群成员的逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。



管理中心：添加集群

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

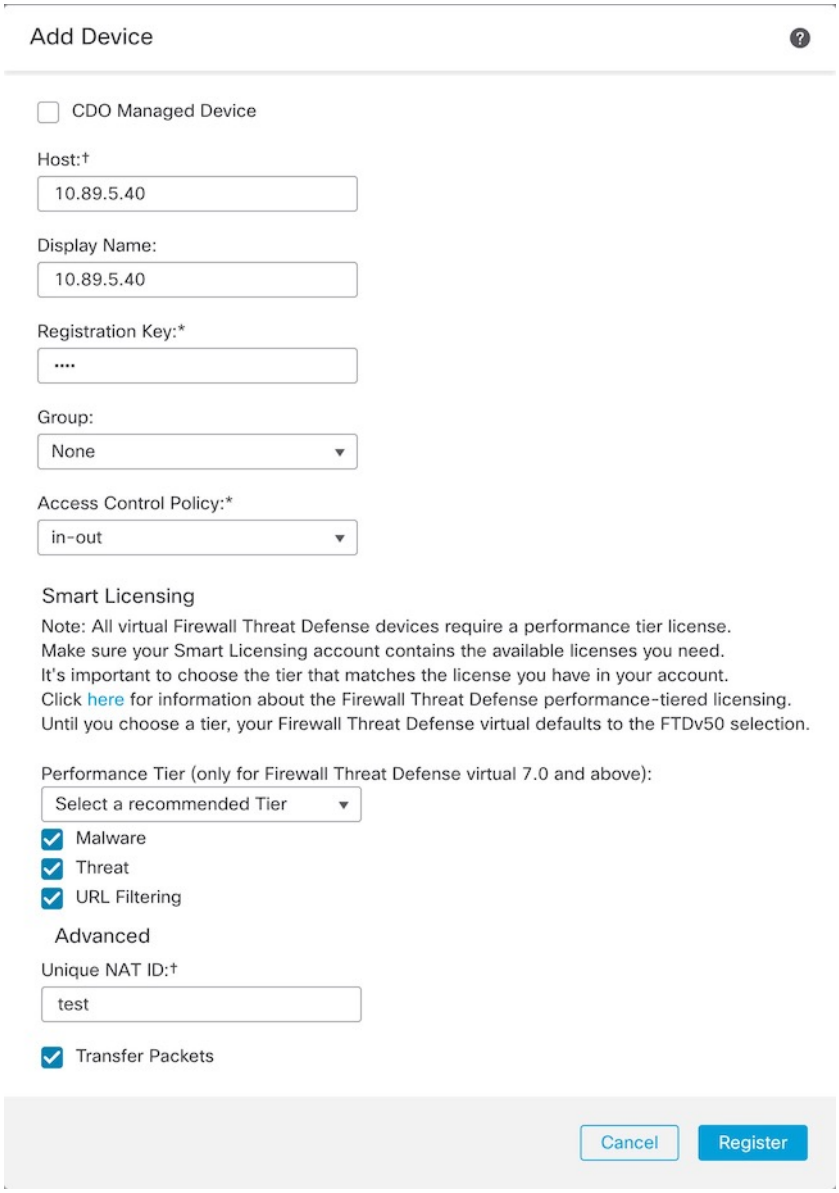
开始之前

- 所有集群设备必须位于 FXOS 上成功建立的集群中，才能将集群添加到 管理中心。还应检查哪个是控制单元。请参阅机箱管理器 **逻辑设备 (Logical Devices)** 屏幕或使用 威胁防御 **show cluster info** 命令。

过程

步骤 1 在 管理中心中，选择 **设备** > **设备管理**，然后选择 **添加** > **添加设备** 以使用部署该集群时分配的管理 IP 添加其中一个集群单元。

图 *8:* 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** 字段中，输入在 FXOS 中部署集群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。

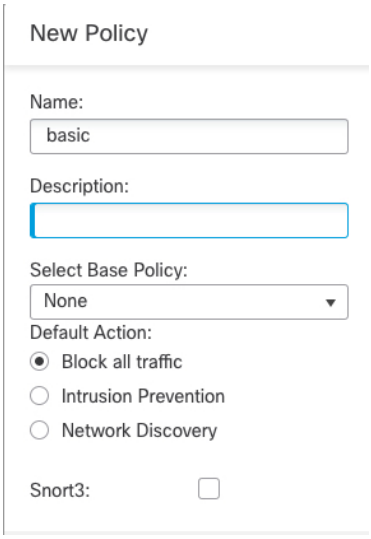
d) 在多域部署中，无论当前的域是什么，都将该设备分配给叶**域**。

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。

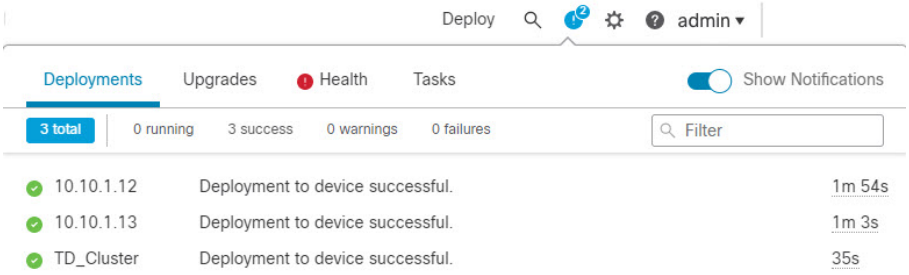
j) 点击 **Register**。

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。如果集群未在机箱上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。

当前正在注册的设备会显示加载图标。

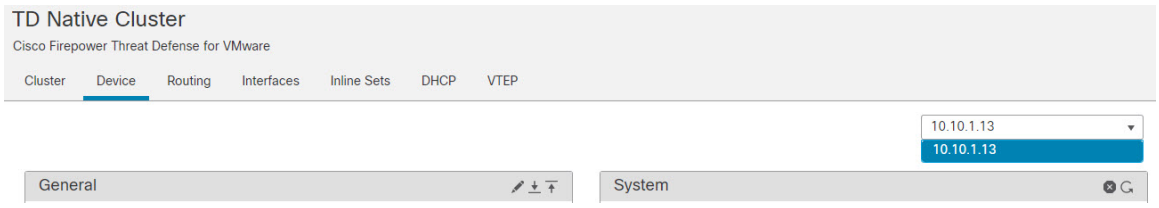
您可以通过点击 **通知** 图标并选择 **任务**来监控集群设备的注册情况。管理中心 会在每个设备注册时更新“集群注册”任务。如有任何设备无法注册，请参阅调整集群成员， 第 42 页。



步骤 2 通过点击集群的 **编辑**（ ），配置设备特定设置。

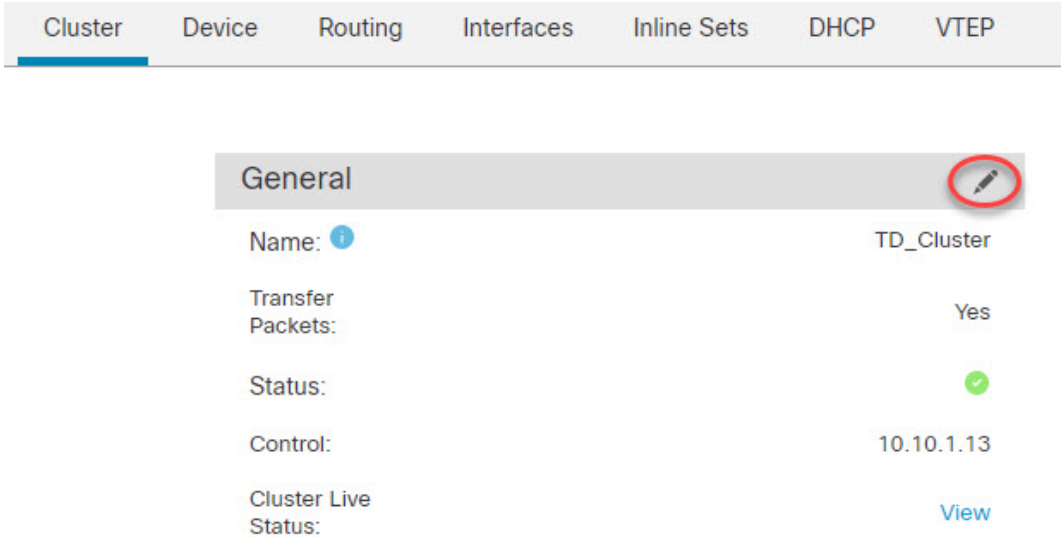
大多数配置可以应用于整个集群，而不适用于集群中的成员设备。例如，可以更改每台设备的显示名称，但只能配置整个集群的接口。

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。

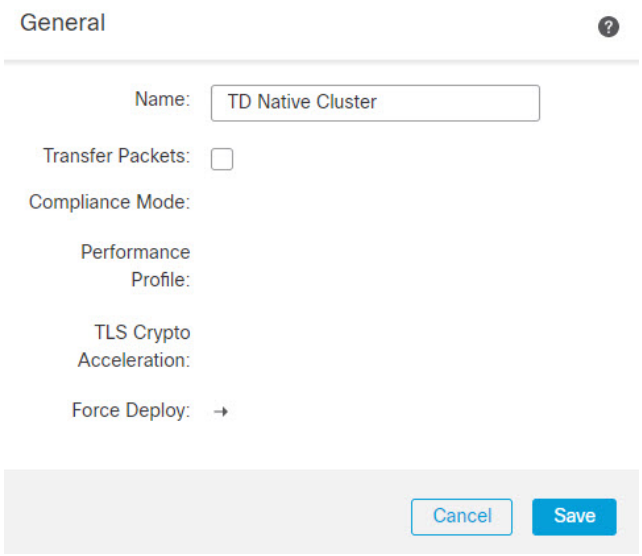


请参阅以下集群特定项：

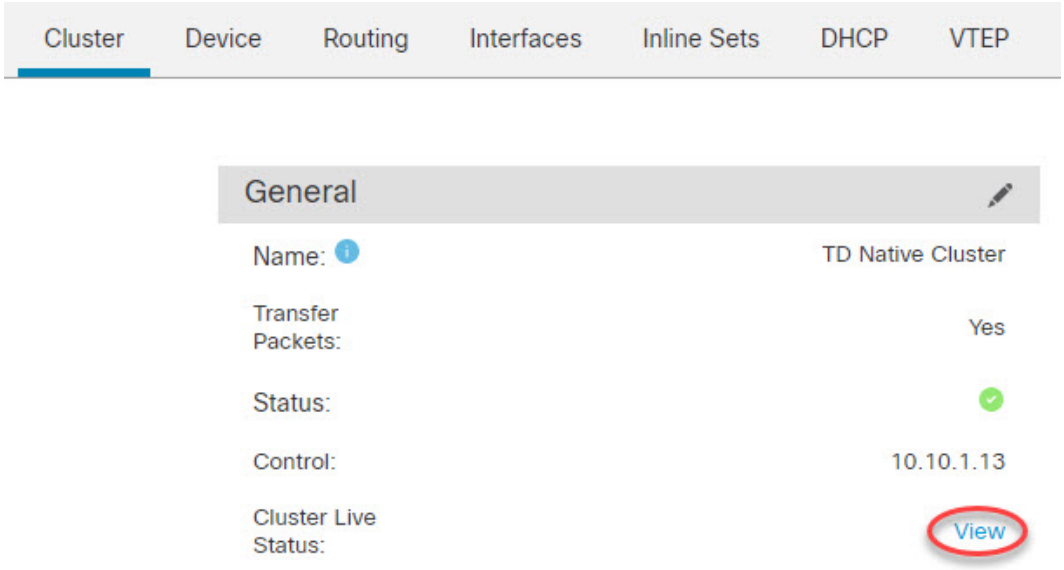
- **常规 > 名称**-通过点击 **编辑**（）更改集群显示名称。



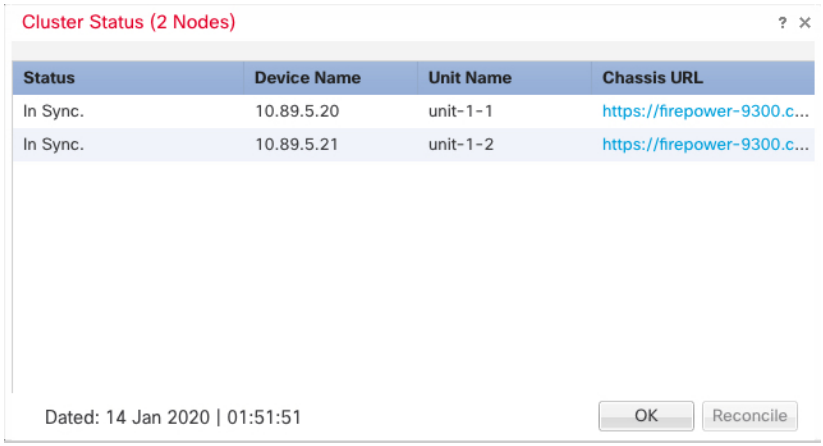
然后设置 **名称** 字段。



- **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。



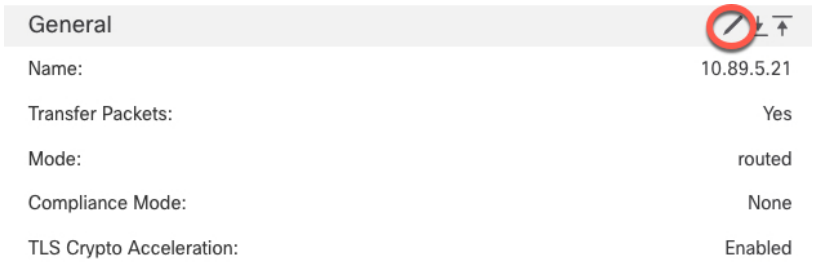
还可在 **集群状态** 对话框中点击 **协调**以重新注册数据单元。



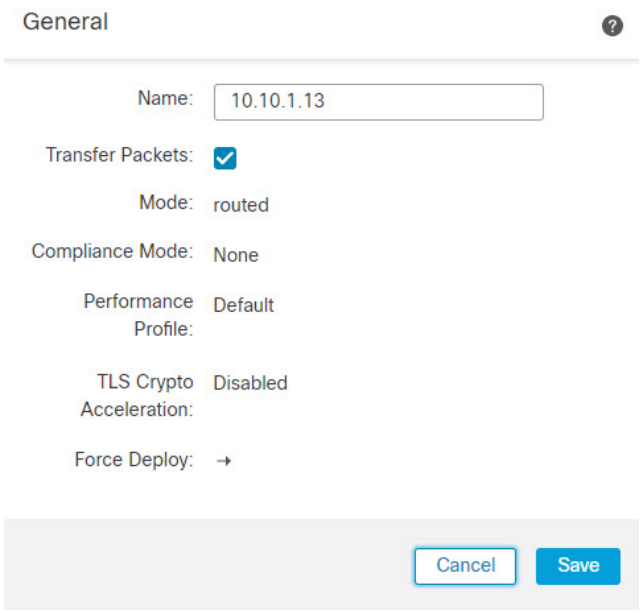
- **许可证**-点击 **编辑**（）可设置许可证授权。

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。

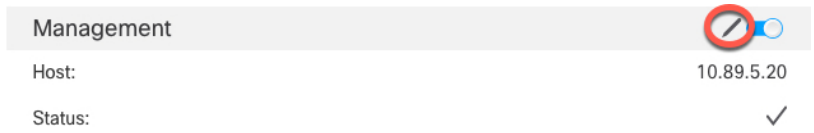
- **常规** > **名称**-通过点击 **编辑**（）更改集群成员显示名称。



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。



管理中心：配置集群、数据和诊断 接口

此程序配置您在 FXOS 中部署集群时为其分配的每个数据接口的基本参数。对于多机箱集群，数据接口始终是跨网络的 EtherChannel 接口。对于与一个 Firepower 9300 机箱内的安全模块隔离的集群控制链路接口，必须将 MTU 从默认值增加。 您还可以配置诊断接口，它是唯一可在单个接口模式下运行的接口。

注释 将跨网络 EtherChannel 用于多机箱集群时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的设备。

过程

步骤 1 选择 **设备** > **设备管理**，然后点击集群旁边的 **编辑**（ ）。

步骤 2 点击**接口 (Interfaces)**。

步骤 3 配置群集控制链路。

对于多机箱集群，将集群控制链路 MTU 设置为比数据接口的最高 MTU 至少高 100 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。我们建议将 MTU 设置为最大 9184；最小值为 1400 个字节。例如，由于最大 MTU 为 9184，因此最高的数据接口 MTU 可以是 9084，而群集控制链路则可以设置为 9184。

对于本地集群：默认情况下，集群控制链路接口为端口通道48。如果您不知道哪个接口是集群控制链路，请为分配给集群的集群类型接口检查机箱的 FXOS 配置。

a) 点击 **编辑**（ ） 以打开集群控制链路接口。
b) 在常规页面的MTU字段中，输入1400和9184之间的值。我们建议使用最大值 9184。
c) 单击**确定 (OK)**。

步骤 4 配置数据接口。

a) （可选） 在数据接口上配置 VLAN 子接口。本程序的其余部分适用于子接口。请参阅添加子接口。
b) 点击数据接口的 **编辑**（ ） 。
c) 根据 配置路由模式接口或 配置网桥组接口，配置名称、IP 地址和其他参数 。

注释 如果集群控制链路接口 MTU 不比数据接口 MTU 高出至少 100 个字节，您将看到必须降低数据接口 MTU 的错误。请参阅步骤 步骤 3 ， 第 35 页 以增加集群控制链路 MTU，之后您可以继续配置数据接口。

d) 对于多机箱集群，请为 EtherChannel 设置手动全局 MAC 地址。点击 **高级**， 在 **主用 Mac 地址** 字段，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

请勿设置 **备用 Mac 地址**；它会被忽略。

您必须为跨网络 EtherChannel 配置全局 MAC 地址，以避免潜在的网络连接问题：如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的MAC 地址用于该接口，而这可能导致临时网络故障。

e) 点击**确定**。对其他数据接口重复上述步骤。

步骤 5 （可选） 配置诊断接口。

诊断接口是唯一可在单个接口模式下运行的接口。例如，对于系统日志消息或 SNMP 可以使用此接口。

a) 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。

b) 在 **设备** > **设备管理** > **接口**上，点击诊断接口的 **编辑**（ ） 。
c) 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。

d) 从 **IPv4 地址池**下拉列表中，选择您创建的地址池。
e) 在 **IPv6 > 基本**， **IPv6 地址池** 下拉列表中，选择您创建的地址池。
f) 按正常方式配置其他接口设置。

步骤 6 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。

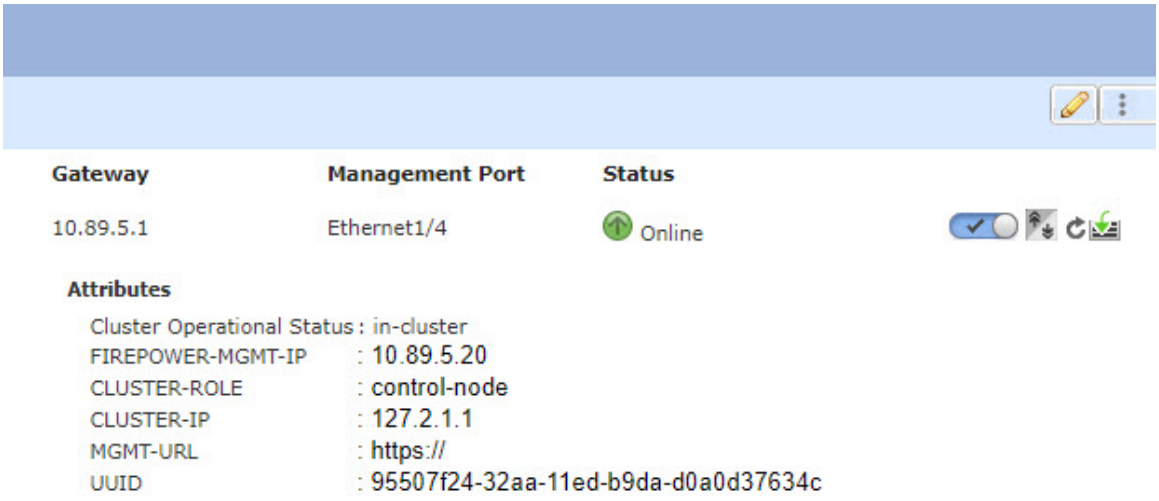
FXOS： 删除集群设备

以下部分介绍如何临时或永久删除集群中的节点。

临时删除

例如，出现硬件或网络故障时，集群节点会自动从集群中删除。此删除是临时的，故障消除后，它们可以重新加入集群。您也可以手动禁用集群。

要检查设备当前是否在集群中，登录 机箱管理器 **逻辑设备**页面查看集群状态：



对于使用 管理中心 的 威胁防御，应该将设备留在 管理中心 设备列表中，以便在重新启用集群后，它可以恢复全部功能。

- 在应用程序中禁用集群 - 您可以使用应用程序 CLI 禁用集群。输入 **cluster remove unit** 名称 命令删除除您登录的设备以外的所有节点。引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

  当设备处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从引导程序配置接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态 ，管理接口将被禁用。

  要重新启用集群，请在 威胁防御 上输入 **cluster enable**。

- 禁用应用程序实例 -在 机箱管理器 的 **逻辑设备** 页面，点击 **滑块已启用**（ ）。您可以稍后使用 **滑块已禁用**（ ） 重新启用它。
- 关闭 安全模块/引擎 - 在 机箱管理器 的**安全模块/引擎**页面，点击**关闭电源图标**。
- 关闭机箱 -在 机箱管理器 的 “**概览**” 页面，点击 **关机图标**。

永久删除

您可以使用以下方法永久删除集群节点。

对于使用 管理中心 的 威胁防御，确保在机箱上禁用集群后，从 管理中心 设备列表删除节点。

- 删除逻辑设备 -在 机箱管理器 的 “**逻辑设备**” 页面，点击 **删除**（ ）。然后，您可以部署独立的逻辑设备、新的集群，还可以在同一集群中添加新的逻辑设备。
- 从服务中删除机箱或安全模块 - 如果从服务中删除设备，则可以将替换硬件添加为集群的新节点。

FMC：管理群集成员

部署集群后，您可以更改配置和管理集群成员。

添加新的集群成员

在 FXOS 中添加新的集群成员时，Cisco Secure Firewall Management Center会自动添加该成员。

开始之前

- 请确保其他机箱的替换设备上的接口配置相同。

过程

步骤 1 在 FXOS 中将新设备添加到集群。请参阅《FXOS 配置指南》。

等待新设备添加到集群。请查看 Firepower 机箱管理器**逻辑设备**菜单项或使用 Firepower 威胁防御 **show cluster info** 命令来查看集群状态。

步骤 2 新集群成员将自动添加。要监控替换设备的注册情况，请查看以下信息：

- **集群状态** 对话框 (从以下可用 **设备** > **设备管理** **更多**（ ） 图标或从 **设备** > **设备管理** > **集群** 选项卡 > **常规** 区域 > **集群实时状态** 链接)—在正在加入机箱上集群的设备显示为“正在加入集群...”设备加入集群后，管理中心 会尝试注册该设备，状态会更改为“可供注册”。完成注册后，状态会更改为“正在同步”。如果注册失败，设备将停留在“可供注册”状态。此时，通过点击 **协调**可强制重新注册。

- 系统状态 > **任务** - 管理中心 显示所有注册事件和失败情况。
- **设备** > **设备管理** - 展开设备列表页面上的集群时，可以看到左侧显示加载图标的设备正在进行注册。

替换集群成员

您可以替换现有集群中的集群成员。管理中心会自动检测替换设备。但是，您必须在 管理中心中手动删除旧集群成员。此程序也适用于已重新初始化的设备；此时，虽然硬件未发生变动，但会显示为新成员。

开始之前

- 请确保其他机箱的替换设备上的接口配置相同。

过程

步骤 1 如果可能的话，对于新机箱，请在 FXOS 中从旧机箱备份配置并予以恢复。

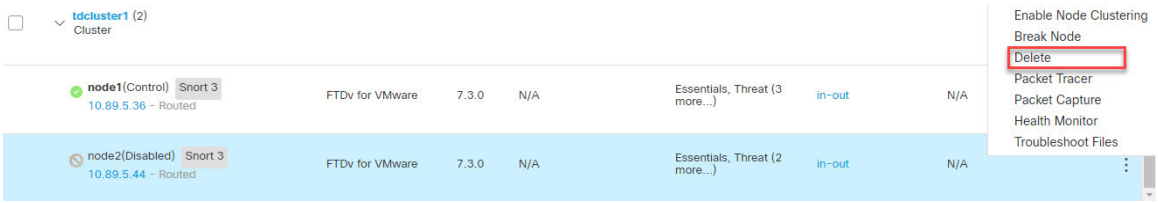
如要更换 Firepower 9300 中的模块，则无需执行这些步骤。

如果没有旧机箱的 FXOS 备份配置，请首先执行添加新的集群成员 ， 第 37 页中的步骤。

有关以下所有步骤的信息，请参阅《FXOS 配置指南》。

a) 使用配置导出功能导出包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件。
b) 将配置文件导入替换机箱。
c) 接受许可协议。
d) 如有必要，可升级逻辑设备应用实例版本以配合集群其余成员。

步骤 2 在旧设备的 管理中心 ， 选择 **设备** > **设备管理** > **更多**（⋮） > **删除** 。



步骤 3 确认要删除该设备。

集群和管理中心设备列表中将删除该设备。

步骤 4 新的或已重新初始化的集群成员将自动添加。要监控替换设备的注册情况，请查看以下信息：

- **集群状态** 对话框 (**设备** > **设备管理** **更多**（⋮） 图标或 **设备** > **设备管理** > **集群** 页面 > **常规** 区域 > **集群实时状态** 链接)—在正在加入机箱上集群的设备显示为“正在加入集群...” 设备加入集群

后，管理中心 会尝试注册该设备，状态会更改为“可供注册”。完成注册后，状态会更改为“正在同步”。如果注册失败，设备将停留在“可供注册”状态。此例中，通过点击 **协调所有** 可强制重新注册。

- **系统**（⚙）> **任务** - 管理中心 显示所有注册事件和失败情况。
- **设备** > **设备管理** - 展开设备列表页面上的集群时，可以看到左侧显示加载图标的设备正在进行注册。

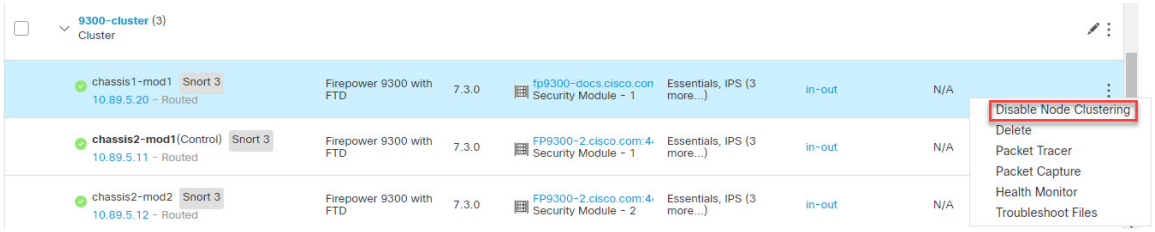
停用成员

您可能需要停用成员，以准备删除设备，或临时进行维护。此程序旨在暂时停用成员；设备仍将显示在 管理中心 设备列表中。

注释 当单元处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用设备从引导程序配置接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台来进行任何进一步配置。

过程

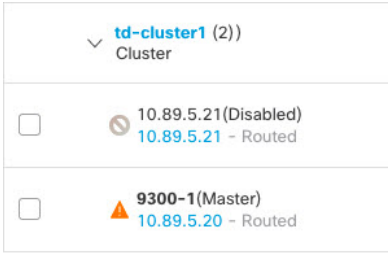
步骤 1 对于要停用的设备，依次选择 **设备** > **设备管理** > **更多**（⋮）> **禁用集群**。



您还可以从 **集群状态** 对话框 （**设备** > **设备管理** > **更多**（⋮）> **集群实时状态** ）停用设备。

步骤 2 确认要在设备上禁用集群。

设备将在**设备** > **设备管理**列表中的设备名称旁边显示 （**已禁用**） 。



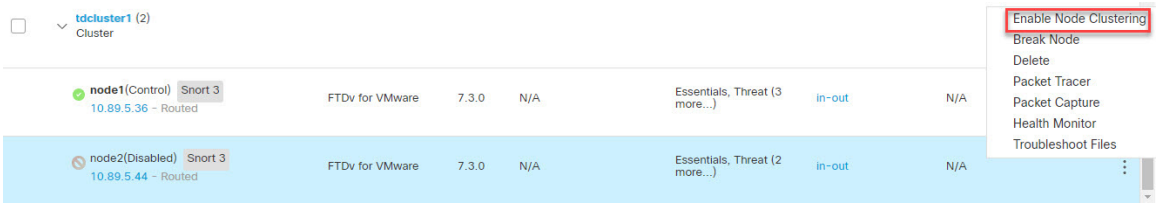
步骤 3 重新启用集群，请参阅 重新加入集群，第 40 页。

重新加入集群

如果从集群中删除了某个设备（例如对于出现故障的接口），或者如果您手动禁用集群，必须通过访问设备 CLI 。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设备的原因的更多信息，请参阅 重新加入集群，第 53 页。

过程

步骤 1 对于要重新激活的设备，请选择 **设备** > **设备管理** > **更多**（⋮） > **启用集群**。



您还可以从 **集群状态** 对话框 （**设备** > **设备管理** > **更多**（⋮） > **集群实时状态**）重新激活设备。

步骤 2 确认要在设备上启用集群。

删除（取消注册）数据节点

如果需要永久删除集群节点（例如，如果您删除 Firepower 9300上的模块，或删除机箱），应从 管理中心将其取消注册。

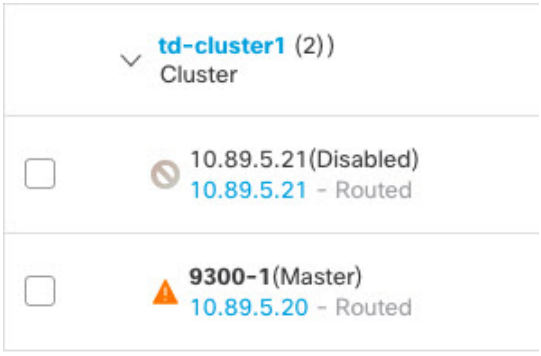
如果该节点仍然是集群的正常运行部分，或者如果您只想临时禁用该成员，请不要删除该节点。要从 FXOS 中的集群中永久删除，请参阅 FXOS： 删除集群设备，第 36 页。如果将其从 管理中心中取消注册，并且它仍然是集群的一部分，它将继续传递流量，甚至可能成为控制节点- 管理中心 不再能够管理的控制节点。

开始之前

要手动停用节点，请参阅 停用成员 ， 第 39 页。在取消注册节点之前，节点必须处于手动或由于运行状况故障而处于非活动状态。

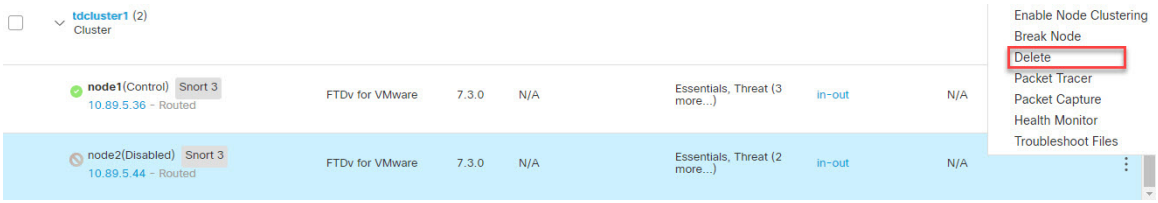
过程

步骤 1 确保准备好从 管理中心取消注册节点。 在 **设备** > **设备管理**，确保节点显示 （**已禁用**）。



您还可从 **更多** （⋮）的 **集群状态** 对话框中查看每个节点的状态。如果状态过时，请点击 **集群状态** 对话框上的 **协调全部** 进行强制更新。

步骤 2 在您想要删除的数据节点的 管理中心 ， 选择 **设备** > **设备管理** > **更多** （⋮） > **删除** 。



步骤 3 确认要删除该节点。

从集群和 管理中心 设备列表中将删除该节点。

变更控制单元

⚠

注意 要更改控制单元，最好的方法是在控制单元上禁用群集，等到新的控制选举后再重新启用群集。如果必须指定要成为控制单元的具体单元，请使用本节中的程序。请注意，对集中功能而言，如果强制更改控制设备，则所有连接都将断开，而您必须在新的控制设备上重新建立连接。

要更改控制单元，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。

您还可以从 **设备** > **设备管理** > **集群** 页面 > **常规** 区域 > **集群实时状态** 链接访问 **集群状态** 对话框。

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**。

调整集群成员

如果集群成员注册失败，则可将集群成员身份从机箱协调至 Cisco Secure Firewall Management Center。例如，数据单元在 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。

您还可以从 **设备** > **设备管理** > **集群** 页面 > **常规** 区域 > **集群实时状态** 链接打开 **集群状态** 对话框。

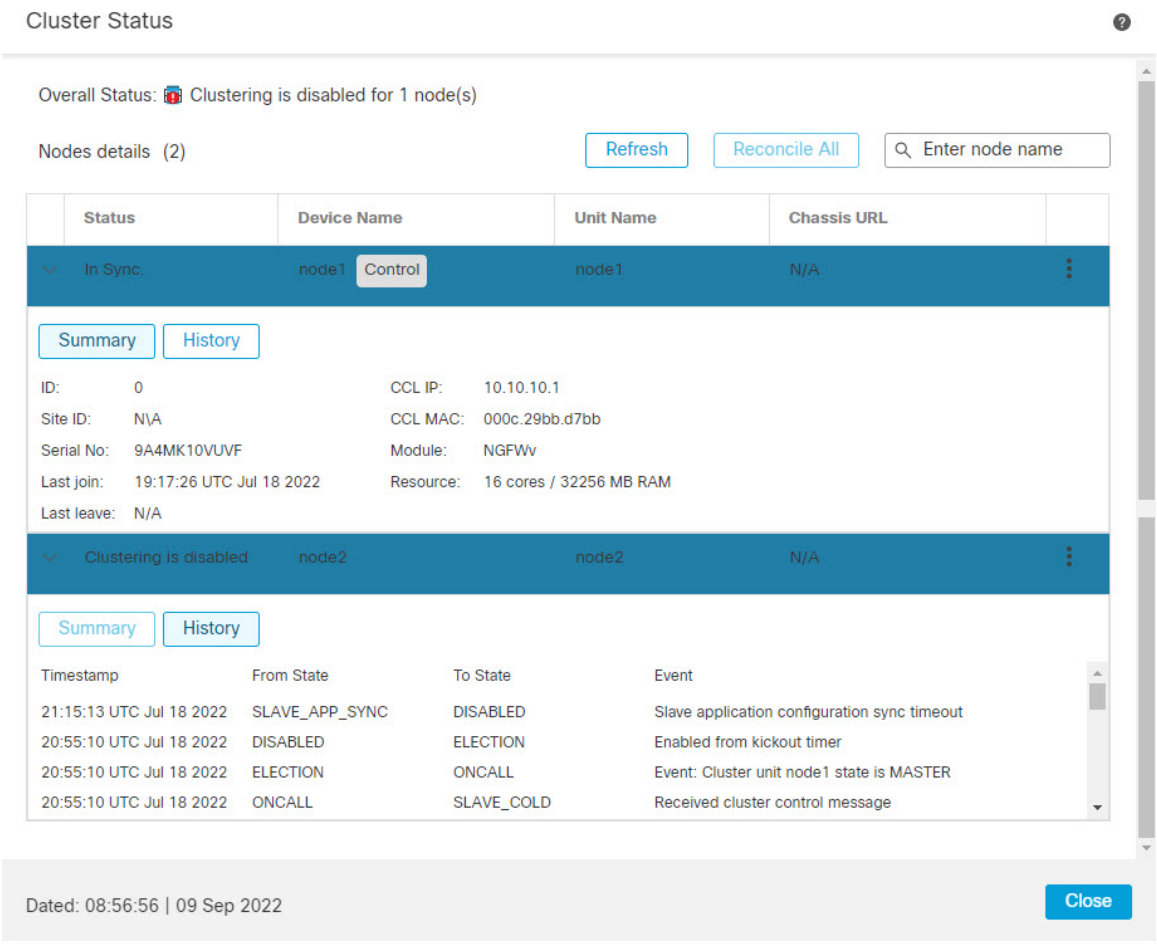
步骤 2 点击 **协调 所有**。

有关集群状态的详细信息，请参阅管理中心：监控集群，第 42 页。

管理中心：监控集群

您可以监控 Cisco Secure Firewall Management Center 中和 威胁防御 CLI 上的集群。

- **集群状态** 对话框 (**设备** > **设备管理** **更多**（⋮） 图标或 **设备** > **设备管理** > **集群** 页面 > **常规** 区域 > **集群实时状态** 链接。



控制单元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 - 设备已向 管理中心 注册。
- 待定注册-设备属于集群，但尚未向 管理中心注册。如果设备注册失败，则可点击 **协调 所有**以重试注册。
- 集群已禁用可供删除-设备已向注册，但是集群的非活动成员。管理中心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设备。
- 正在加入集群... - 设备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。

对于每台设备，您可以查看 **摘要** 或 **历史记录**。

对于 **更多**（⋮）菜单中的每台设备，您可以执行以下状态更改：

- **禁用集群**
- **启用集群**

- 将角色更改为控制角色

- **系统**（⚙）> **任务** 页面。

  任务 页面会在每个设备注册时更新“集群注册”任务。

- **设备** > **设备管理** > *cluster_name*。

  展开设备列表页面上的集群时，可看到所有成员设备，包括 IP 地址旁显示的设备。对于仍在注册的设备，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。

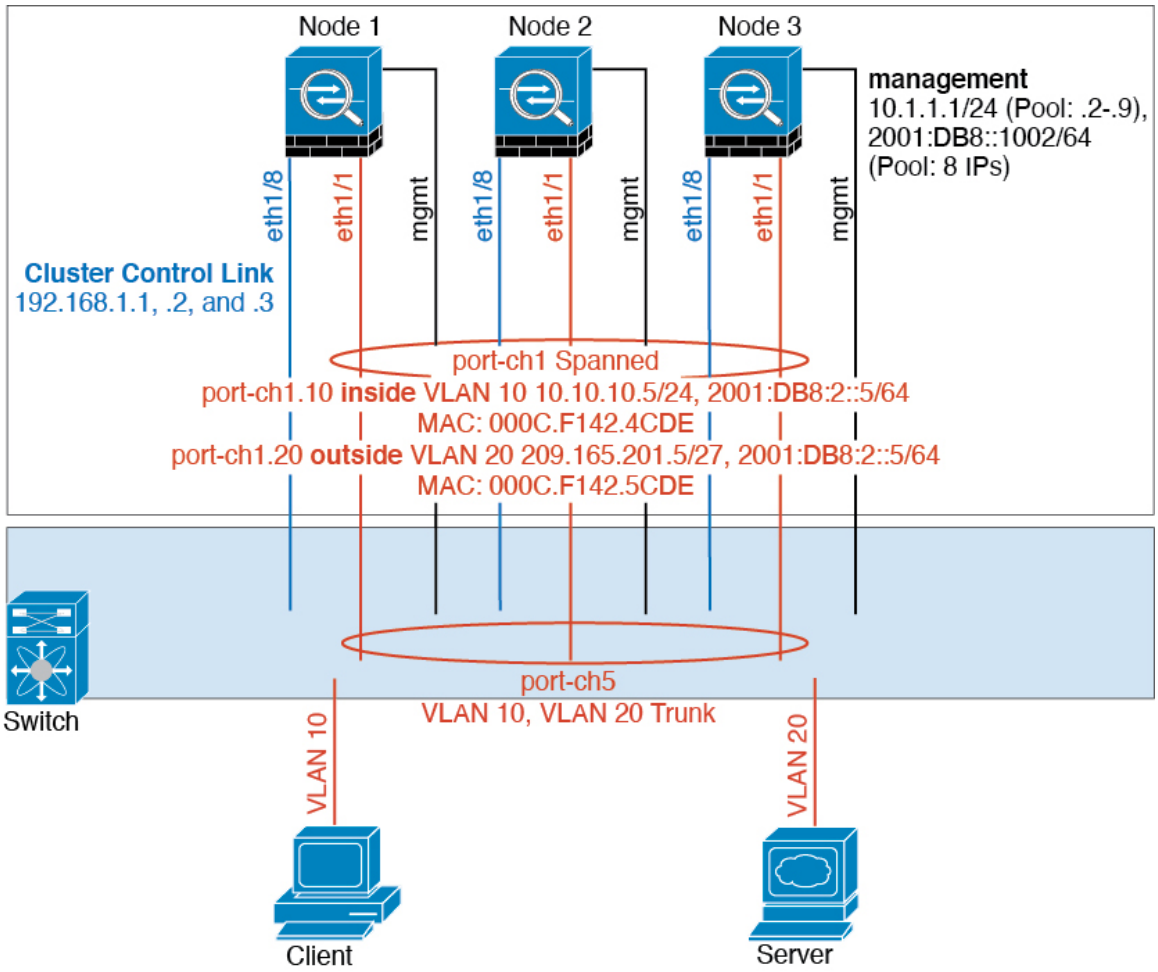
- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

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

集群示例

这些示例包含典型部署。

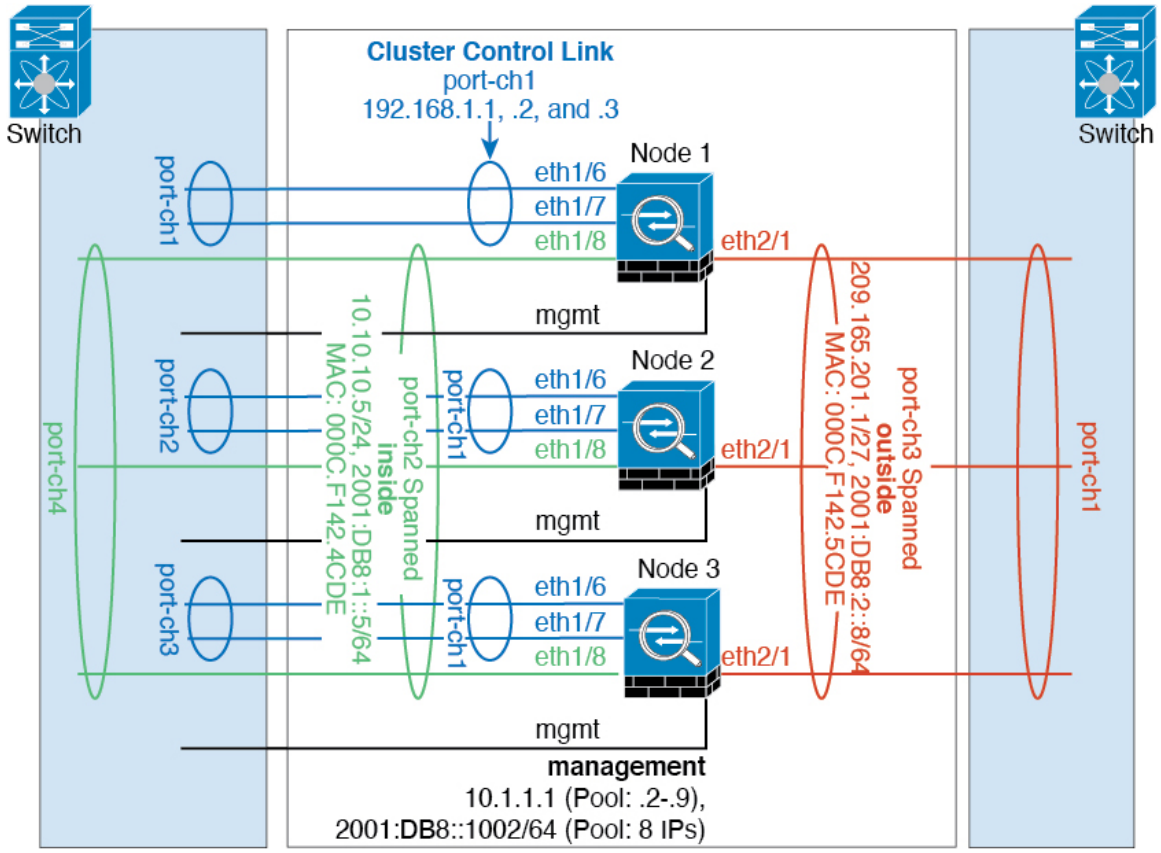
单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如，VLAN 10 用于内部网络，而 VLAN 20 用于外部网络。每台 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机侧分组为一个 EtherChannel。如果一台 变得不可用，交换机将在其余设备之间再均衡流量。

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

集群参考

本部分包括有关集群工作原理的详细信息。

威胁防御功能和集群

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。

集群不支持的功能

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
- 站点到站点 VPN
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由

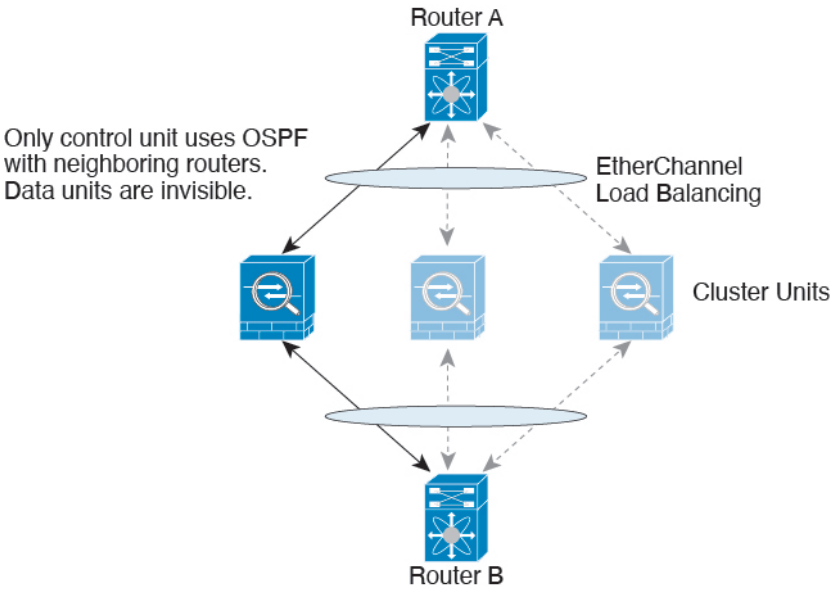
连接设置

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

路由进程仅在控制单元上运行，而路由通过控制单元获知并复制到从属设备。如果路由数据包到达数据设备，它将重定向到控制设备。

图 *9:* 动态路由



在数据设备向控制设备学习路线后，每个设备将单独做出转发决策。

OSPF LSA 数据库不会从控制设备同步到数据设备。如果切换了控制设备，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路

由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

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。

组播路由和集群

在建立快速路径转发之前，控制单元会处理所有的组播路由数据包和数据数据包。在连接建立之后，每台数据设备都可以转发组播数据包。

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：

- 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。

TLS / SSL 连接和群集

TLS/SSL 连接的解密状态不同步，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。

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

站点到站点 VPN 是集中功能；只有控制单元支持 VPN 连接。

注释 群集不支持远程接入 VPN。

VPN 功能仅限控制设备使用，且不能利用群集的高可用性功能。如果控制单元发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。

与 VPN 相关的密钥和证书将被复制到所有设备。

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。

以 TCP 吞吐量为例，含 3 个 SM-40 模块的 Firepower 9300 在单独运行时大约可处理 135 Gbps 的实际防火墙流量。2 个机箱的最大合并吞吐量约为 270 Gbps（2 个机箱 x 135 Gbps）的 80%：216 Gbps。

控制设备选择

集群成员通过集群控制链路通信，如下选举控制设备：

1. 当您部署集群时，每台设备会每隔 3 秒广播一次选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级在您部署集群时设置且不可配置。
3. 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为控制设备。

注释 如果多台设备并列获得最高优先级，则使用集群设备名称和序列号确定控制设备。

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设备；现有控制设备始终保持为控制设备，除非它停止响应，此时会选择新的控制设备。
5. 在“裂脑”场景中，当临时存在多个控制单元时，具有最高优先级的单元将会保留角色，其他单元则恢复为数据单元角色。

注释 您可以手动强制一台设备成为控制设备。对集中功能而言，如果强制更改控制设备，则所有连接都将断开，而您必须在新的控制设备上重新建立连接。

集群中的高可用性

集群通过监控机箱、设备和接口的运行状态并在设备之间复制连接状态来提供高可用性。

机箱应用程序监控

机箱应用程序运行状况监控始终处于启用状态。Firepower 4100/9300 机箱 管理引擎会定期检查 威胁防御应用程序（每秒）。如果 威胁防御设备已启动且无法与 Firepower 4100/9300 机箱管理引擎通信达到 3 秒，则 威胁防御设备会生成系统日志消息并离开集群。

如果 Firepower 4100/9300 机箱管理引擎在 45 秒后仍无法与应用程序通信，则会重新加载 威胁防御设备。如果 威胁防御设备无法与管理引擎通信，则会将自身从集群中删除。

设备运行状况监控

每台设备通过集群控制链路定期发送广播keepalive keepalive心跳数据包。如果控制节点在的超时期限内未从数据节点接收任何 keepaliveheartbeat 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。有关详细信息，请参阅控制设备选择，第 51 页。

接口监控

每个节点都会监控使用中的所有硬件接口的链路状态，并向控制节点报告状态更改。对于多机箱集群，跨网络 EtherChannel 使用集群链路汇聚控制协议 (cLACP)。每个机箱都会监控链路状态和 cLACP 协议消息，以确定端口在 EtherChannel 中是否仍处于活动状态，并在接口关闭时通知 威胁防御应用。所有物理接口（包括 EtherChannel 接口的主 EtherChannel）。仅可监控处于开启状态的命名接口。例如，只有 EtherChannel 的所有成员端口都出现故障时，才会从集群中删除指定的 EtherChannel。

如果受监控接口在特定节点上发生故障，但在其他节点上处于活动状态，则该节点将从集群中删除。威胁防御设备在多长时间后从集群中删除节点取决于该节点是既定成员还是正在加入集群的设备。

威胁防御设备 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 威胁防御设备从集群中删除。对于既定成员，节点将在 500 毫秒后删除。

对于多机箱集群，如果从集群添加或删除一个 EtherChannel，则接口运行状况监控将暂停 95 秒，以确保您有时间在每个机箱上进行更改。

修饰符应用监控

在接口上安装某种修饰符应用时，例如 Radware DefensePro 应用，威胁防御设备和该修饰符应用必须处于运行状态，以保留在集群中。只有两个应用都处于运行状态，设备才会加入集群。加入集群后，设备每 3 秒钟监控一次修饰符应用的运行状况。如果修饰符应用关闭，设备将从集群中移除。

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。

- 机箱-应用通信故障 - 当 威胁防御应用检测到机箱-应用运行状况恢复时，会自动尝试重新加入集群。

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。

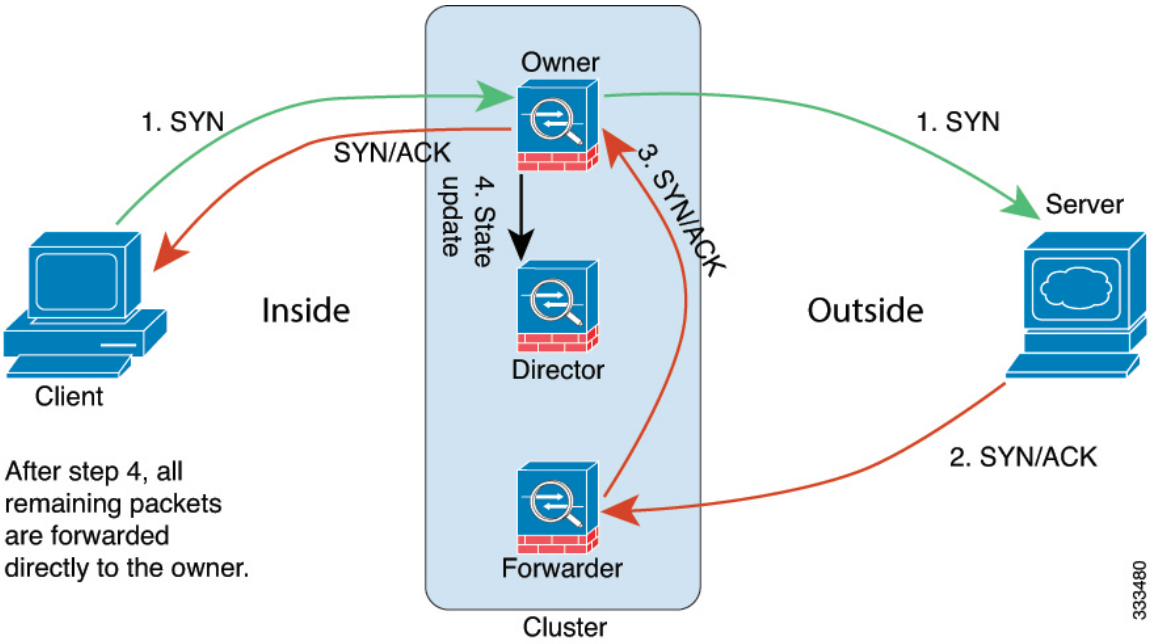
- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

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。

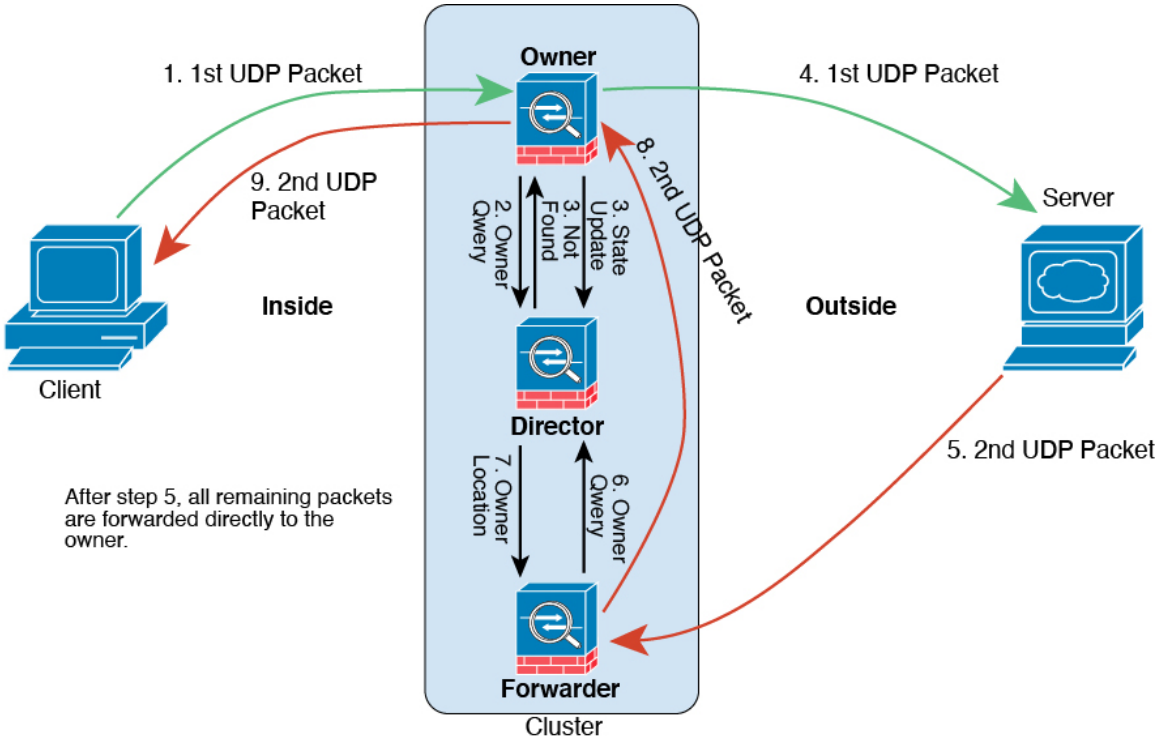


1. SYN 数据包从客户端发出，被传送到一台 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 威胁防御（基于负载均衡方法）。此 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，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 *10: 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。

集群历史记录

特性	Version	详细信息
支持 16 节点集群	7.2	您现在可以为 Firepower 4100/9300 配置 16 个节点集群。 新增/修改的屏幕：无。 支持的平台：Firepower 4100/9300
用于防火墙更改的集群部署更快完成	7.1	集群集群部署防火墙更改现在完成更快。 新增/修改的屏幕：无。
改进了集群的 PAT 端口块分配	7.0	改进的PAT端口块分配可确保控制设备保留端口以供加入节点，并主动回收未使用的端口。为了最好地优化分配，您可以使用 **cluster-member-limit** 命令和 FlexConfig 设置您计划在集群中拥有的最大节点数。然后，控制单元可以分配端口块到计划的节点数量，并且不必为您不打算使用的额外节点预留端口。默认值为 16 节点。您还可以监控系统日志 747046，以确保有足够的端口可用于新节点。 新增/经修改的命令： **cluster-member-limit** (FlexConfig)、 **show nat pool cluster summary**、 **show nat pool ip detail**
Snort 的集群部署更改完成得更快，并且在发生事件时失败更快	6.7	Snort 更改的集群部署现在可以更快完成。此外，当集群发生导致 管理中心 部署失败的事件时，故障现在会更快发生。 新增/修改的屏幕：无。
改进了 管理中心 中的集群管理	6.7	管理中心改进了以前只能使用CLI完成的集群管理功能，包括： • 启用和禁用集群设备 • 从设备管理页面显示集群状态，包括每台设备的历史记录和摘要 • 变更角色为控制单元 新建/修改的菜单项： • **设备** > **设备管理** > **更多** 菜单 • **设备** > **设备管理** > **集群** > **常规** 区域 > **集群实时状态** 链接 **集群状态** 支持的平台：Firepower 4100/9300

特性	Version	详细信息
多实例群集	6.6	您现在可以使用容器实例来创建集群。在 Firepower 9300 上，必须在集群中的每个模块上包含一个容器实例。不能为每个安全引擎/模块向集群添加多个容器实例。我们建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。 新增/修改的 FXOS 命令：**set port-type cluster** 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **添加集群** • **接口 (Interfaces)** > **所有接口 (All Interfaces)** > **新增 (Add New)**下拉菜单 > **子接口 (Subinterface)** > **类型 (Type)** 字段 支持的平台：Firepower 4100/9300 上的 威胁防御
并行配置同步到数据设备	6.6	控制设备现在默认将配置更改并行同步到数据设备。以前，同步是按顺序发生的。 新增/修改的屏幕：无。
集群加入失败或逐出的消息已添加到 **show cluster history**	6.6	关于集群设备无法加入集群或离开集群的新消息添加到了 **show cluster history** 命令。 新增/修改的命令：**show cluster history** 新增/修改的屏幕：无。
群集中的“死连接检测”(DCD) 支持的发起方和响应方信息。	6.5	如果启用死连接检测(DCD)，则可以使用该 **show conn detail** 命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 **show conn** 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出） 支持的平台：Firepower 4100/9300 上的 威胁防御

特性	Version	详细信息
管理中心 中添加了改进的 威胁防御 群集	6.3	现在可将群集中的任何设备添加到 管理中心，并会自动检测其他群集设备。以前，必须将每个集群设备作为独立设备予以添加，然后在管理中心中将其组合到集群中。现在也可以自动添加集群设备了。请注意，必须手动删除设备。 新增/修改的屏幕： **设备** > **设备管理** > **添加**下拉菜单 > **设备** > **添加设备**对话框 **设备** > **设备管理** > **集群**选项卡> **常规**区域 > **集群注册状态** > **当前集群摘要**链接 > **集群状态**对话框 支持的平台：Firepower 4100/9300 上的 威胁防御
支持将集群作为集中功能的站点到站点 VPN	6.2.3.3	现在可以配置使用群集的站点到站点 VPN。站点到站点 VPN 是集中功能；只有控制单元支持 VPN 连接。 支持的平台：Firepower 4100/9300 上的 威胁防御
内部故障后自动重新加入集群	6.2.3	过去，许多内部错误条件导致集群设备从集群中移除，并且在解决问题后需要手动重新加入集群。现在，设备将尝试以下列时间间隔自动重新加入群集：5 分钟、10 分钟以及 20 分钟。内部故障包括：应用程序同步超时、不一致的应用程序状态等。 新增/修改的命令：**show cluster info auto-join** 未修改任何屏幕。 支持的平台：Firepower 4100/9300 上的 威胁防御
6 个模块的多机箱集群；Firepower 4100 支持	6.2	使用 FXOS 2.1.1，您现在可以在 Firepower 9300 和 4100 上启用多机箱集群。对于 Firepower 9300，最多可以包含 6 个模块。例如，您可以在 6 个机箱中使用 1 个模块，或者在 3 个机箱中使用 2 个模块，也可以使用最多提供 6 个模块的任意组合。对于 Firepower 4100，最多可以包含 6 个机箱。 **注释** 也支持站点间群集。然而，仅可通过使用 FlexConfig 功能来配置用以增强冗余性和稳定性自定义功能，例如指定站点的 MAC 和 IP 地址、导向器本地化、站点冗余和集群流移动性。 未修改任何屏幕。 支持的平台：Firepower 4100/9300 上的 威胁防御

特性	Version	详细信息
使用一个 Firepower 9300 机箱在多个模块上集群	6.0.1	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **添加集群 (Add Cluster)** **设备** > **设备管理** > **集群** 支持的平台：Firepower 9300 上的 威胁防御

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。