



逻辑设备

- [关于逻辑设备，第 1 页](#)
- [逻辑设备的要求和必备条件，第 9 页](#)
- [逻辑设备的准则和限制，第 17 页](#)
- [添加独立的逻辑设备，第 22 页](#)
- [添加高可用性对，第 33 页](#)
- [添加集群，第 34 页](#)
- [配置 Radware DefensePro，第 56 页](#)
- [配置 TLS 加密加速，第 61 页](#)
- [启用 FTD 链路状态同步，第 64 页](#)
- [管理逻辑设备，第 66 页](#)
- [“逻辑设备 \(Logical Devices\)” 页面，第 75 页](#)
- [站点间群集示例，第 78 页](#)
- [逻辑设备的历史记录，第 81 页](#)

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 FTD）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。



注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

独立和群集逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。
- 群集 - 群集逻辑设备允许您将多个单元集合在一起，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。Firepower 9300 等多模块设备支持机箱内群集。对于 Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。FDM 不支持集群。

逻辑设备应用程序实例：容器和本地

应用实例在以下类型部署中运行：

- 本地实例 - 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 - 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。仅使用 FMC 的 FTD 支持多实例功能；ASA 或使用 FDM 的 FTD 不支持。



注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全 FTD 功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。FTD 的多情景模式不可用。

对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

容器实例接口

要确保灵活使用容器实例的物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。本地实例不得使用 VLAN 子接口或共享接口。多实例集群不得使用 VLAN 子接口或共享接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。请参阅 [共享接口可扩展性](#) 和 [为容器实例添加 VLAN 子接口](#)。



注释 本文档仅讨论 FXOS VLAN 子接口。您还可以在 FTD 应用内单独创建子接口。有关详细信息，请参阅 [FXOS 接口与应用接口](#)。

机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。

- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一 MAC 地址的实例。在应用内配置每个接口时，您也可以手动设置 MAC 地址。

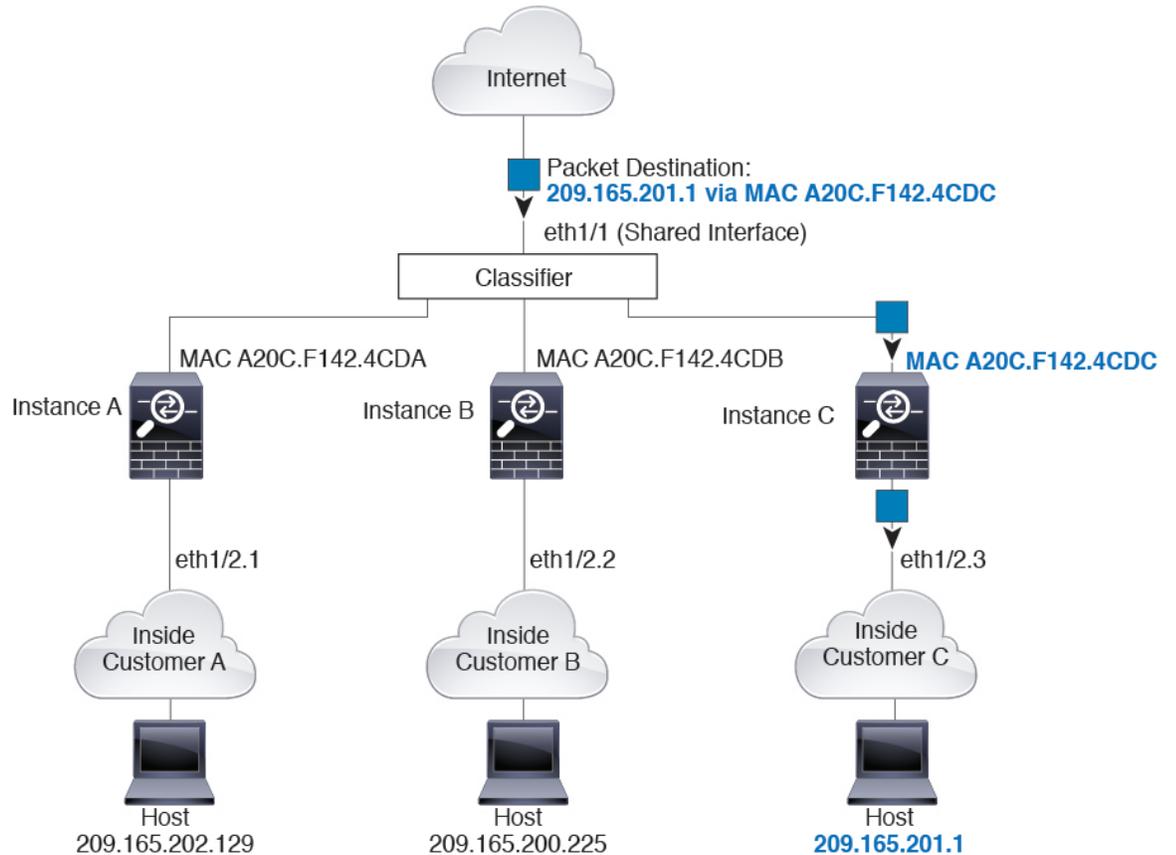


注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

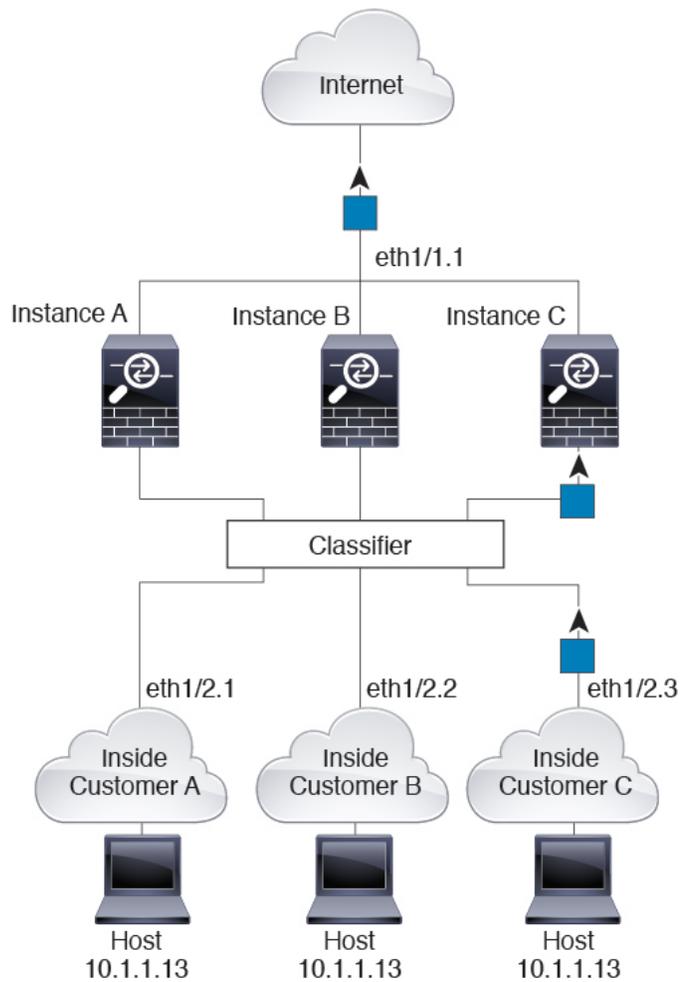
下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

图 1: 使用 MAC 地址通过共享接口进行数据包分类



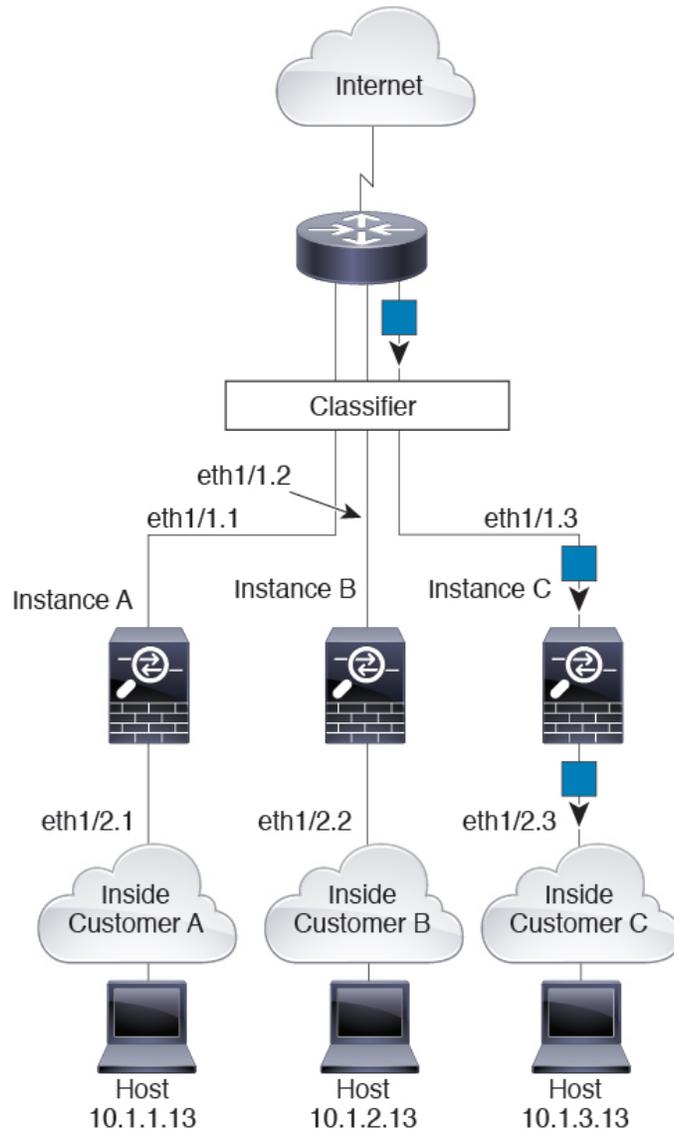
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 2: 来自内部网络的传入流量



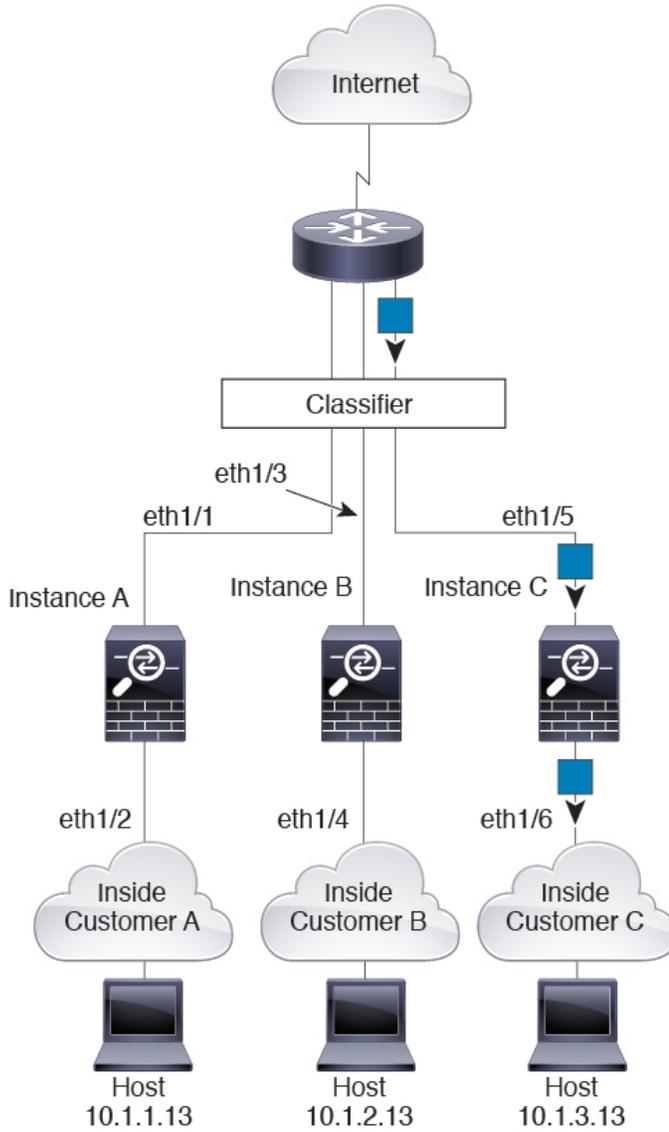
对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 3: 透明防火墙实例



对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 4: FTD 的内联集 FTD

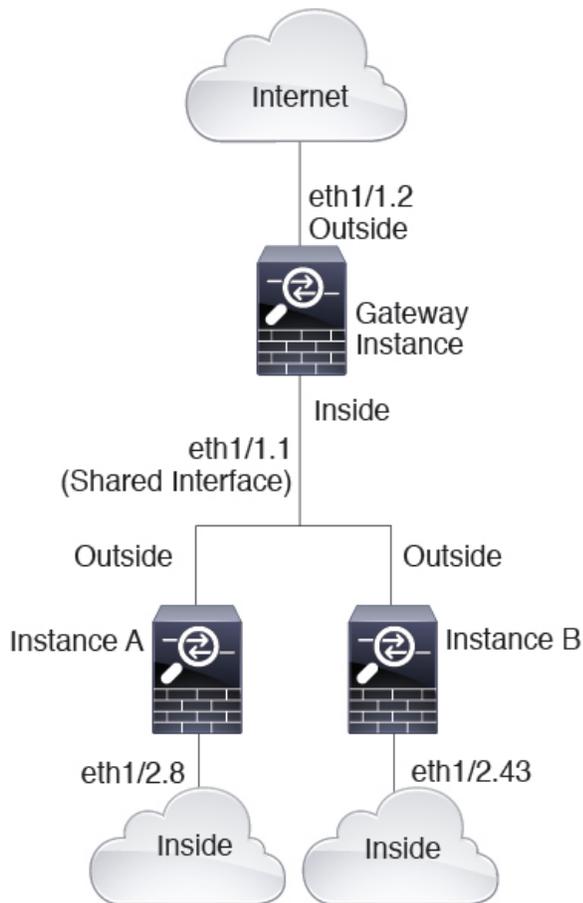


级联容器实例

直接在一个容器实例前面放置另一个实例的行为称为级联容器实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

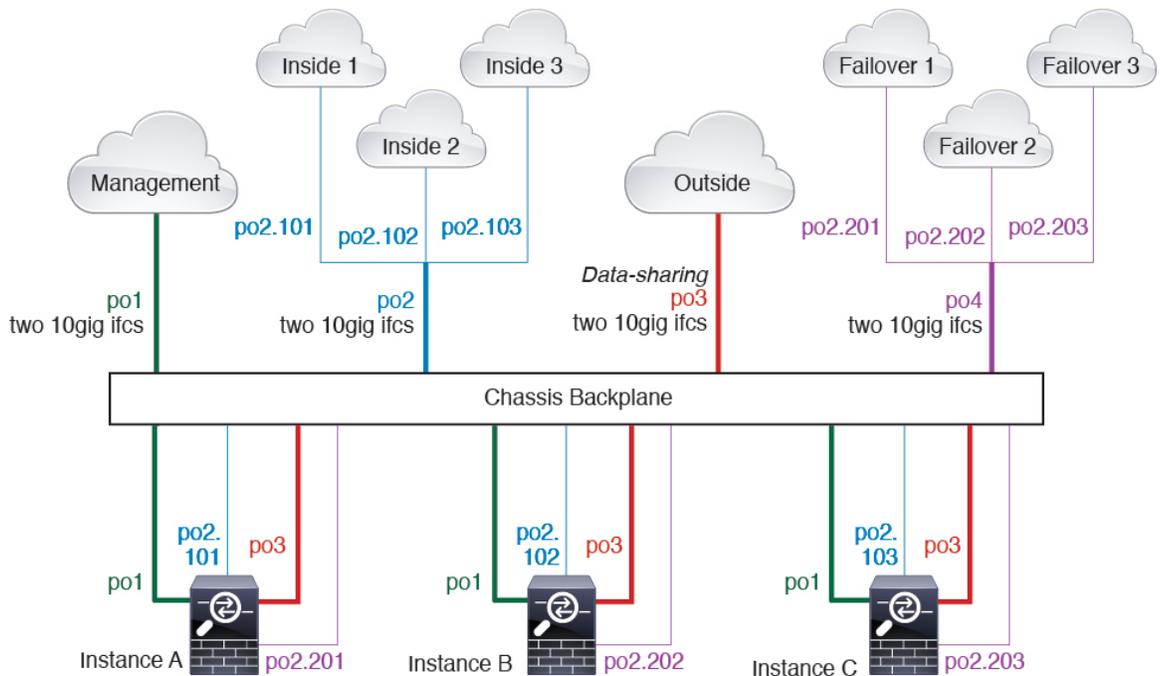
图 5: 级联容器实例



典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例都使用端口通道 1 接口（管理类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 2 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 3 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一外部网络上的唯一 IP 地址。
- 故障切换 - 每个实例都使用端口通道 4 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。



容器实例接口的自动 MAC 地址

FXOS 机箱会自动为容器实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一 MAC 地址。

如果您手动为应用中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在应用中为接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。

FXOS 机箱使用以下格式生成 MAC 地址：

A2xx.yyzz.zzzz

其中，xx.yy 是用户定义的前缀或系统定义的前缀，zz.zzzz 是由机箱生成的内部计数器。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (yyxx)。在 MAC 地址中使用时，该前缀会反转 (xxyy)，以便与机箱的本地形式匹配：

A24D.00zz.zzzz

对于前缀 1009 (03F1)，MAC 地址为：

A2F1.03zz.zzzz

容器实例资源管理

要指定每个容器实例的资源使用情况，请在 FXOS 中创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。要查看每个型号的可用资源，请参阅 [容器实例的要求和必备条件](#)，第 16 页。要添加资源配置文件，请参阅 [为容器实例添加资源配置文件](#)。

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数和 TLS 代理会话数）是为了得出本地实例的内存和 CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的容器实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但容器实例可用的吞吐量可能低于本地实例可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅 <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html>。

容器实例与高可用性

您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建 10 个高可用性对。请注意，不得在 FXOS 中配置高可用性；在应用管理器中配置每个高可用性对。

有关详细要求，请参阅 [高可用性的要求和前提条件](#)，第 15 页和 [添加高可用性对](#)，第 33 页。

容器实例和集群

您可以每个安全模块/引擎各使用一个容器实例创建容器实例集群。有关详细要求，请参阅 [集群要求和必备条件](#)，第 11 页。

逻辑设备的要求和必备条件

有关要求和必备条件，请参阅以下章节。

硬件和软件组合的要求与前提条件

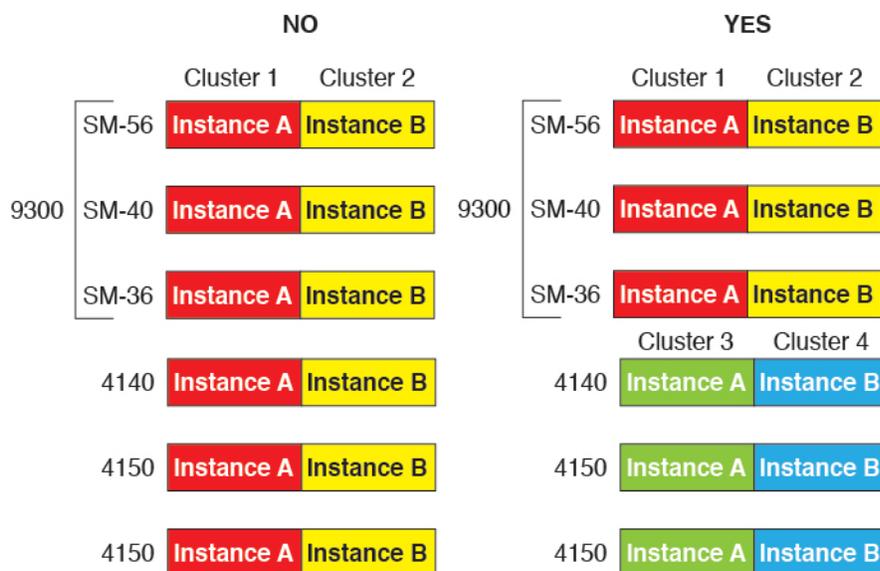
Firepower 4100/9300 支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-36 作为模块 1、SM-40 作为模块 2、SM-44 作为模块 3 安装。

- 本地和容器实例 - 在安全模块上安装容器实例时，该模块只能支持其他容器实例。本地实例将使用模块的所有资源，因此只能在模块上安装一个本地实例。可以在某些模块上使用本地实例，在其他模块上使用容器实例。例如，您可以在模块 1 和模块 2 上安装本地实例，但在模块 3 上安装容器实例。
- 本地实例 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。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。例如，您可以在机箱 1 中安装 2 个 SM-36，在机箱 2 中安装 3 个 SM-36。如果在同一机箱中安装了 1 个 SM-24 和 2 个 SM-36，则无法使用集群。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 9300 SM-56、SM-40 和 SM-36 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



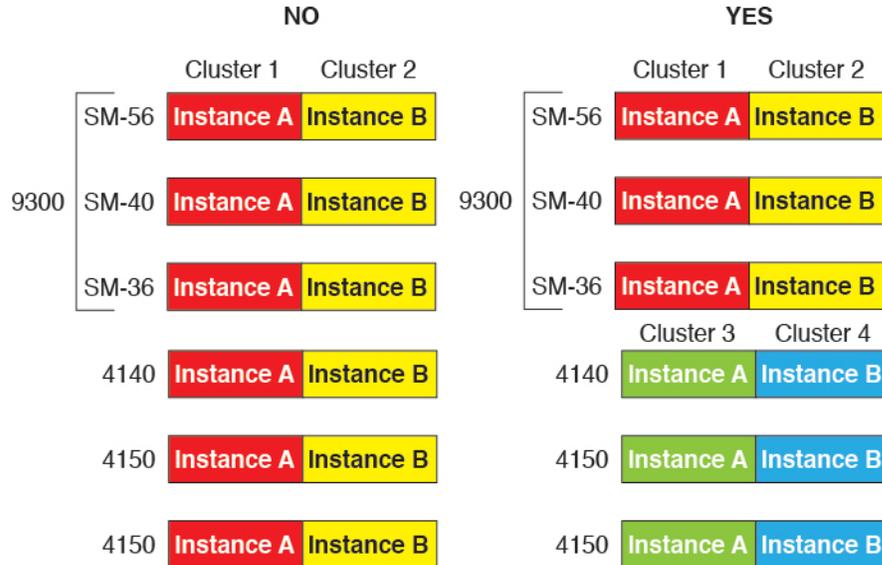
- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-36、SM-40 和 SM-44。可以在 SM-36 模块之间、SM-40 模块之间和 SM-44 模块之间创建高可用性对。
- ASA 和 FTD 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 FTD。
- ASA 或 FTD 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 FTD 6.3，在模块 2 上安装 FTD 6.4，在模块 3 上安装 FTD 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。

- 本地实例 集群 - 集群内的所有机箱都必须为同一型号。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，可以使用 Firepower 4140 和 4150 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 FTD 应用类型 - Firepower 4100 只能运行一种应用类型。
- FTD 容器实例版本 - 您可以在同一模块上将不同版本的 FTD 作为单独的容器实例运行。

群集要求和必备条件

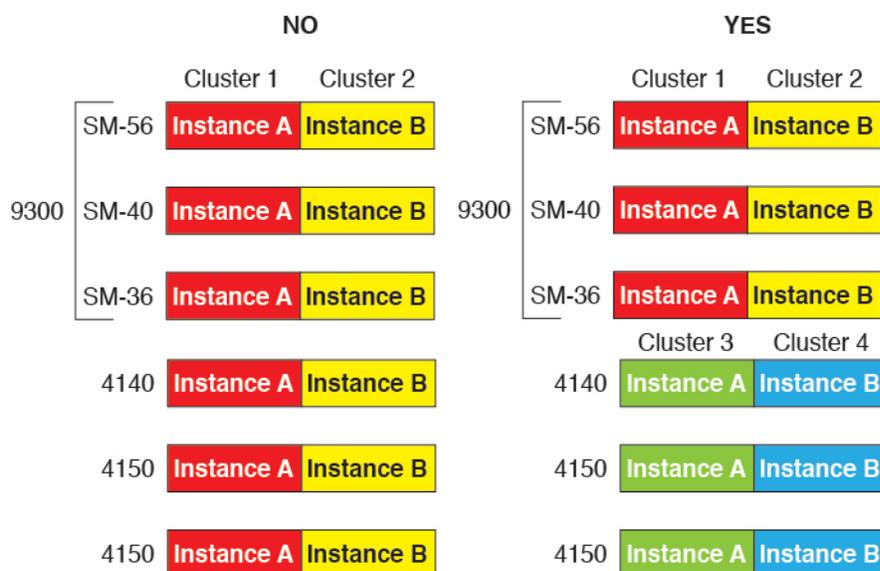
群集型号支持

- Firepower 9300 上的 ASA - 最多 16 个模块。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。请注意，机箱中的所有模块都必须属于该集群。支持机箱内、机箱间和站点间群集。
- Firepower 4100 系列上的 ASA - 最多 16 个机箱。支持机箱间和站点间群集。
- FTD 在使用 FMC 的 Firepower 9300 上 - 6 个模块。例如，您可以在 3 个机箱中使用 2 个模块，或者在 2 个机箱中使用 3 个模块，或者最多提供 6 个模块的任意组合。请注意，机箱中的所有模块都必须属于该集群。支持机箱内和机箱间群集。
- 在使 Firepower 4100 系列用 FMC 的 FTD 上 - 最多 6 个机箱。支持机箱间群集。
- Radware DefensePro - 对于包含 ASA 的机箱内群集受支持。
- Radware DefensePro - 支持包含 FTD 的机箱内群集。不支持多实例集群。

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-40 和 SM-36 上的实例创建集群。或者，可以在 Firepower 4140 和 4150 上创建集群。



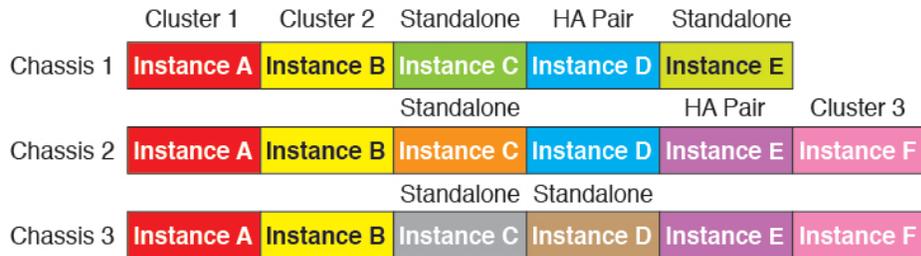
- 除进行映像升级外，必须运行完全相同的 FXOS 软件。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。对于 FTD，FMC 必须使用同一台 NTP 服务器。请勿手动设置时间。
- ASA：每个 FXOS 机箱都必须注册到许可证颁发机构或卫星服务器。数据节点没有额外的成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。对于 FTD，所有许可由 FMC 处理。

多实例集群要求

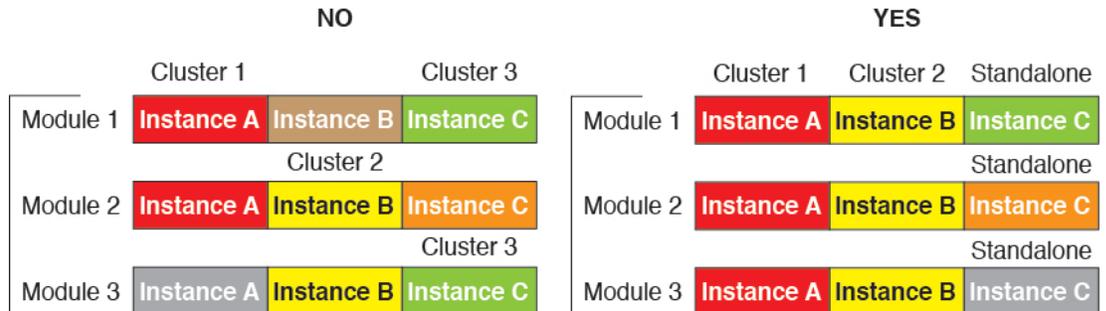
- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。



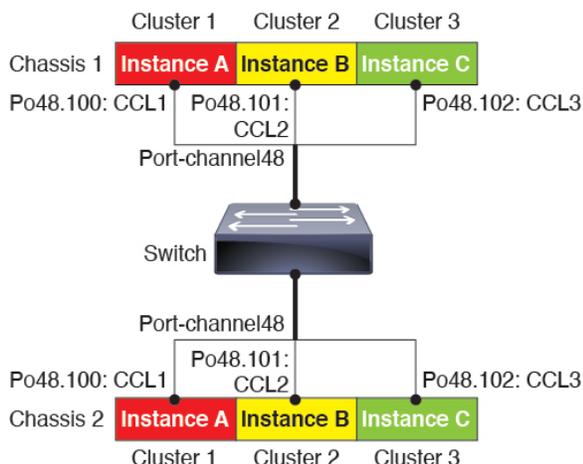
- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。



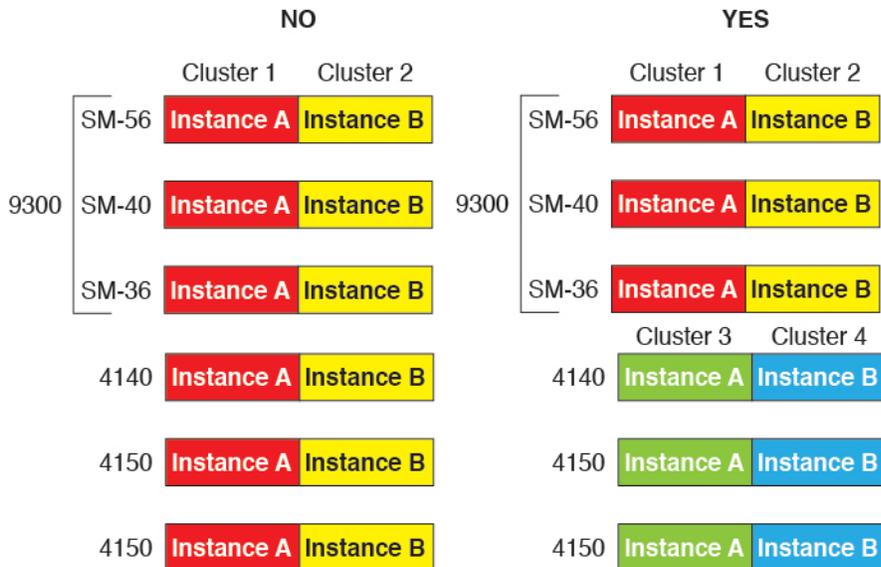
- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。



- 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 - 对于机箱间集群，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-40 和 SM-36 上的实例创建集群。或者，可以在 Firepower 4140 和 4150 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。

机箱间群集交换机必备条件

- 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](#)。

调整站点间群集的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：
 - 总共 4 个集群成员
 - 每个站点 2 个成员
 - 每个成员 5 Gbps 集群控制链路

保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。

- 对位于 3 个站点的 6 个成员而言，规格加大：
 - 总共 6 个集群成员
 - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
 - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。

- 位于 2 个站点的 2 个成员：
 - 总共 2 个集群成员
 - 每个站点 1 个成员
 - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps))。

高可用性的要求和前提条件

- 高可用性故障切换配置中的两个设备必须：
 - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
 - 型号相同。

- 将同一接口分配至高可用性逻辑设备。
- 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-36、SM-40 和 SM-44。可以在 SM-36 模块之间、SM-40 模块之间和 SM-44 模块之间创建高可用性对。
- 对于容器实例，每个单元必须使用相同的资源配置文件属性。
- 有关其他高可用性系统要求，请参阅“高可用性”的应用配置指南一章。

容器实例的要求和必备条件

受支持应用类型

- 使用 FMC 的 FTD

每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的 CPU 核心数量。系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

表 1: 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 安全模块	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 安全模块	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 安全模块	13	78	334 GB	1359 GB

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 9300 SM-44 安全模块	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 安全模块	15	94	334 GB	1341 GB
Firepower 9300 SM-56 安全模块	18	110	334 GB	1314 GB

FMC 要求

对于在 Firepower 4100 机箱或 Firepower 9300 模块上的所有情况下，由于许可实施，您必须使用相同 FMC。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

一般准则和限制

防火墙模式

您可以在 FTD 和 ASA 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障切换和状态链路。不支持数据共享接口。

多实例和情景模式

- 仅 ASA 支持多情景模式。
- 部署后，请在 ASA 中启用多情景模式。
- 包含容器实例的多实例功能仅适用于使用 FMC 的 FTD。
- 对于 FTD 容器实例，单个 FMC 必须管理安全模块/引擎上的所有实例。
- 您可以在最多 16 个容器实例上启用 TLS 加密加速。
- 对于 FTD 容器实例，不支持以下功能：
 - Radware DefensePro 链路修饰器
 - FMC UCAPL/CC 模式

- 到硬件的流负载分流

集群准则和限制

机箱间集群的交换机

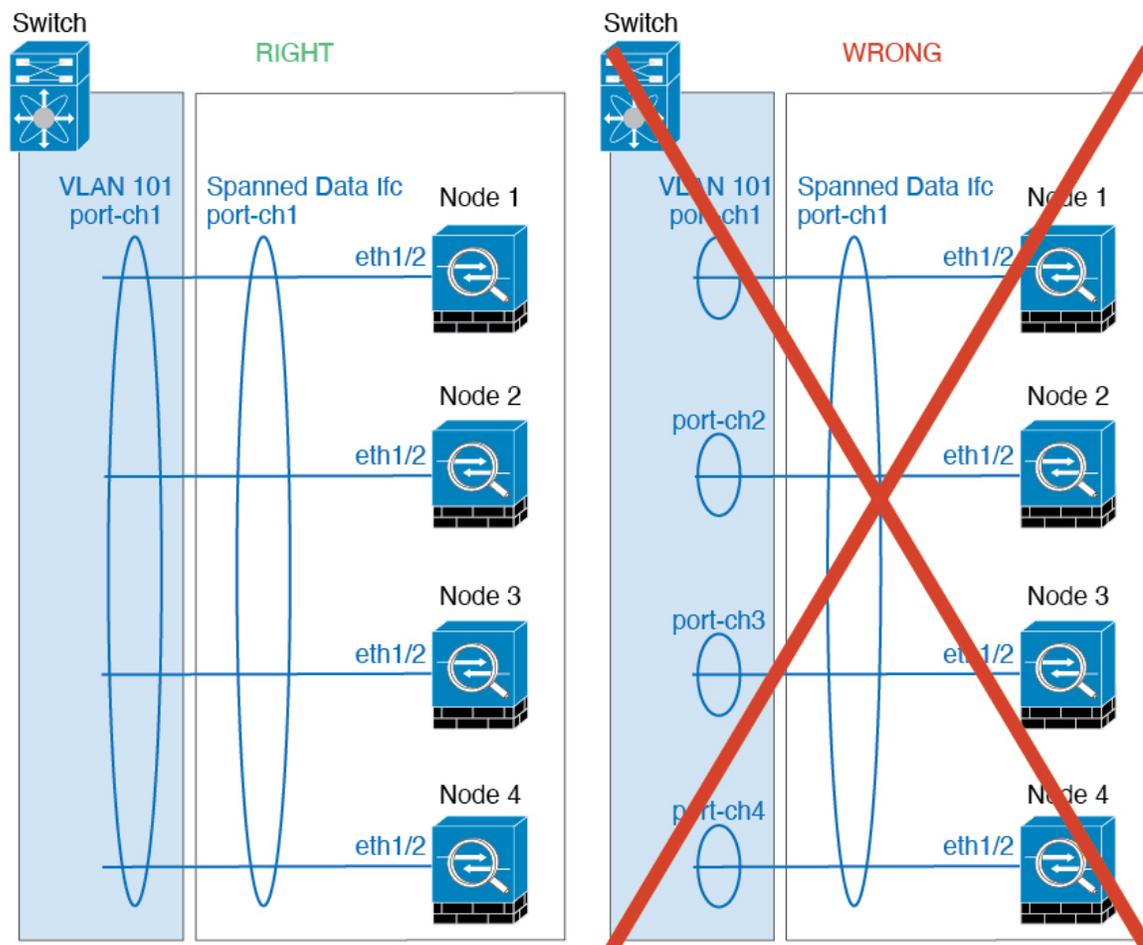
- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS IPv4 MTU 匹配。Cisco Catalyst 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 **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。
- 有些交换机不支持 LACP 动态端口优先级（活动链路和备用链路）。您可以禁用动态端口优先级，使跨区以太网通道具有更高兼容性。
- 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
```

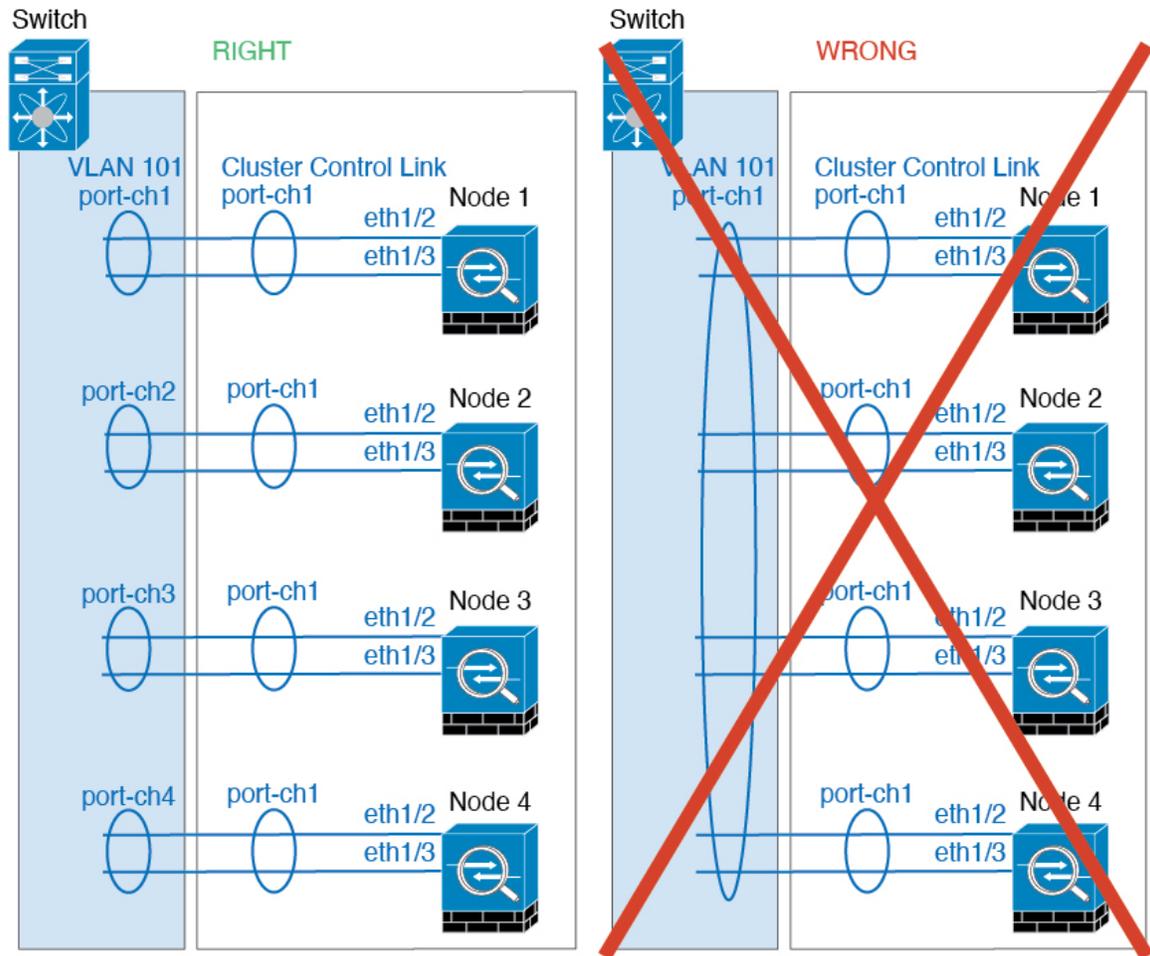
请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。
- Firepower 4100/9300 集群支持 LACP 正常融合。因此，您可以在连接的 Cisco Nexus 交换机上启用 LACP 正常融合。
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

机箱间集群的 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。



站点间集群

请参阅有关站点间集群的以下准则：

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。
- 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，您应使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- 不会加密集群控制链路上转发的数据流量，因为它是专用链接，即使在数据中心互连 (DCI) 上使用也是如此。如果您使用重叠传输虚拟化 (OTV) 或将集群控制链路扩展到本地管理域外部，可以在边界路由器（例如基于 OTV 的 802.1AE MacSec）上配置加密。
- 对于传入连接而言，位于多个站点的成员之间的集群实施没有区别；因此，给定连接的连接角色可以跨越所有站点。这是预期行为。但是，如果您启用导向器本地化，系统将始终从连接所有者所在同一站点选择本地导向器角色（根据站点 ID）。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者（注意：如果不同站点间的流量非对称，且原始所

所有者发生故障后远程站点继续发出流量，则远程站点节点可能成为新的所有者，但条件是该设备在重新托管期间接收到数据包。)

- 对于导向器本地化，以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。
- 对于透明模式，如果集群布置于内部和外部路由器对之间（AKA 南北插入），您必须确保两个内部路由器共享一个 MAC 地址，两个外部路由器共享一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目标 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于透明模式，如果集群布置于每个站点上的数据网络和网关路由器之间，用作内部网络之间的防火墙（AKA 东西插入），则每个网关路由器都应使用 HSRP 等第一跳冗余协议 (FHRP) 在每个站点提供相同的虚拟 IP 和 MAC 地址目标。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术扩展到多个站点。您需要创建过滤器，阻止发往本地网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则需要删除所有过滤器，使流量能够成功到达另一站点的网关。
- 对于透明模式，如果集群连接到 HSRP 路由器，则必须在。当邻接路由器使用 HSRP 时，发往 HSRP IP 地址的流量将发送到 HSRP MAC 地址，但返回流量将来自 HSRP 对中特定路由器接口的 MAC 地址。因此，MAC 地址表通常仅在 HSRP IP 地址的 ARP 表条目到期时更新，并且发送 ARP 请求并接收应答。由于的 ARP 表条目默认在 14400 秒后到期，但 MAC 地址表条目默认在 300 秒后到期，因此需要添加静态 MAC 地址条目来避免 MAC 地址表到期流量丢失。
- 对于使用跨区以太网通道的路由模式，请配置站点特定的 MAC 地址。使用 OTV 或类似技术跨站点扩展数据 VLAN。您需要创建过滤器，阻止发往全局 MAC 地址的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群，则需要删除所有过滤器，使流量能够成功到达另一站点的集群节点。当站点间集群作为扩展网段的第一跳路由器时，不支持动态路由。

其他规定

- 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 或 vPC，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。

添加独立的逻辑设备

独立逻辑设备可以单独或作为高可用性单元使用。有关高可用性的详细信息，请参阅[添加高可用性对](#)，第 33 页。

添加独立 ASA

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

您可以通过 Firepower 4100/9300 机箱部署一个路由或透明防火墙模式的 ASA。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300 机箱。



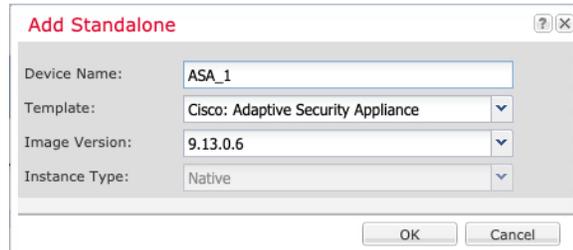
注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（并且在[接口](#)选项卡的顶部显示为 **MGMT**）。
- 收集以下信息：
 - 此设备的接口 ID
 - 管理接口 IP 地址和网络掩码
 - 网关 IP 地址

过程

步骤 1 选择逻辑设备。

步骤 2 点击添加 > 独立设备，并设置以下参数：



a) 提供设备名称。

此名称由机箱管理引擎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。

b) 对于模板，请选择思科：自适应安全设备。

c) 选择映像版本。

d) 单击确定 (OK)。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开数据端口区域，然后点击要分配给设备的每个端口。

仅可分配先前在接口页面上启用的数据接口。稍后您将在 ASA 上启用和配置这些接口，包括设置 IP 地址。

步骤 4 单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 5 在一般信息页面上，完成下列操作：

a) （对于 Firepower 9300）在安全模块选择下，点击您想用于此逻辑设备的安全模块。

b) 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。

c) 选择管理接口地址类型：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。

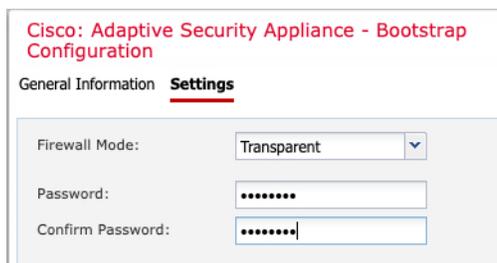
d) 配置管理 IP 地址。

设置用于此接口的唯一 IP 地址。

e) 输入网络掩码或前缀长度。

f) 输入网络网关地址。

步骤 6 点击设置选项卡。



步骤 7 选择防火墙模式：路由式或透明。

在路由模式下，ASA 被视为网络中的一个路由器跃点。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。

步骤 8 输入并确认管理员用户和启用密码的密码。

预配置的 ASA 管理员用户/密码和启用密码在进行密码恢复时非常有用；如果有 FXOS 访问权限，在忘记管理员用户密码/启用密码时，可以将其重置。

步骤 9 单击确定关闭配置对话框。

步骤 10 点击保存。

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，可以开始在应用中配置安全策略。



步骤 11 请参阅 ASA 配置指南，以开始配置安全策略。

为 FMC 添加独立 FTD

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

可以在某些模块上使用本地实例，在其他模块上使用容器实例。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300 机箱。



注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（并且在接口选项卡的顶部显示为 **MGMT**）。
- 您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关详细信息，请参阅 [FTD 命令参考](#) 中的 **configure network management-data-interface** 命令。
- 您还必须至少配置一个数据类型的接口。或者，您也可以创建 Firepower 事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅 [接口类型](#)。
- 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](#) 或 [安全引擎](#)，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。有关详细信息，请参阅 [重新初始化安全模块/引擎](#)。
- 收集以下信息：
 - 此设备的接口 ID
 - 管理接口 IP 地址和网络掩码
 - 网关 IP 地址
 - FMC 您选择的 IP 地址和/或 NAT ID
 - DNS 服务器 IP 地址
 - FTD 主机名和域名

过程

- 步骤 1** 选择逻辑设备。
- 步骤 2** 点击添加 > 独立设备，并设置以下参数：



a) 提供设备名称。

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

b) 对于模板，请选择 **Cisco Firepower 威胁防御**。

c) 选择映像版本。

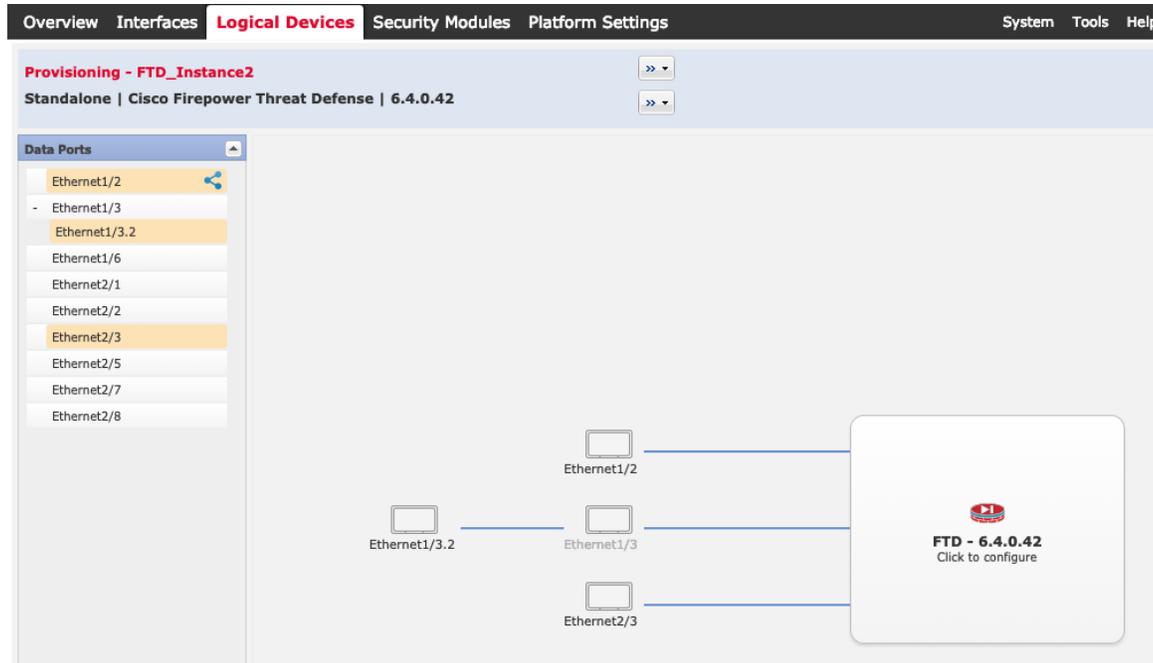
d) 选择实例类型：容器或本地。

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

e) 单击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开数据端口区域，然后单击要分配给设备的每个接口。



您仅可分配先前在接口页面上启用的数据和数据共享接口。稍后您需要在 FMC 中启用和配置这些接口，包括设置 IP 地址。

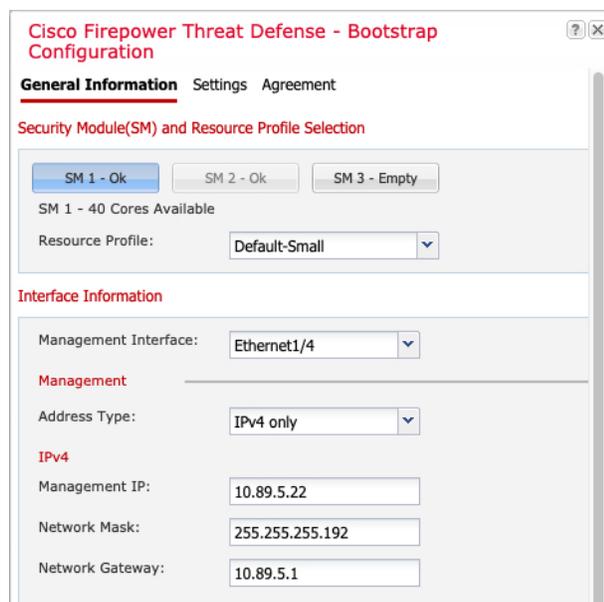
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（）表示。

具有硬件旁路功能的端口使用以下图标显示：。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能（请参阅 FMC 配置指南）。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 单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 配置中的大多数数值。

步骤 5 在一般信息页面上，完成下列操作：



The image shows a web-based configuration interface for Cisco Firepower Threat Defense. The title is "Cisco Firepower Threat Defense - Bootstrap Configuration". There are three tabs: "General Information", "Settings", and "Agreement", with "General Information" selected. The main content area is titled "Security Module(SM) and Resource Profile Selection". It contains three buttons: "SM 1 - Ok" (highlighted in blue), "SM 2 - Ok", and "SM 3 - Empty". Below these buttons, it says "SM 1 - 40 Cores Available" and "Resource Profile: Default-Small" with a dropdown arrow. The next section is "Interface Information", which includes a "Management Interface:" dropdown set to "Ethernet1/4". Below that is a "Management" section with "Address Type:" dropdown set to "IPv4 only". Underneath is an "IPv4" section with input fields for "Management IP:" (10.89.5.22), "Network Mask:" (255.255.255.192), and "Network Gateway:" (10.89.5.1).

- a) （对于 Firepower 9300）在安全模块选择下，点击您想用于此逻辑设备的安全模块。
- b) 对于容器实例，指定资源配置文件。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。请注意，对于已建立的高可用性对，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

- c) 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。

- d) 选择管理接口地址类型：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- e) 配置管理 IP 地址。

设置用于此接口的唯一 IP 地址。

- f) 输入网络掩码或前缀长度。

g) 输入网络网关地址。

步骤 6 在设置选项卡上，完成下列操作：

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

Management type of application instance:	FMC
Firepower Management Center IP:	10.89.5.35
Search domains:	cisco.com
Firewall Mode:	Routed
DNS Servers:	10.89.5.67
Firepower Management Center NAT ID:	test
Fully Qualified Hostname:	ftd2.cisco.com
Registration Key:
Confirm Registration Key:
Password:
Confirm Password:
Eventing Interface:	

a) 对于本地实例，在应用实例的管理类型下拉列表中，选择 **FMC**。

本地实例还支持 FDM 作为管理器。部署逻辑设备后，无法更改管理器类型。

b) 输入管理 FMC 的 **Firepower 管理中心 IP**。如果您不知道 FMC 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。

c) 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 FTD 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 FTD CLI 中使用 **expert** 命令。

d) 输入逗号分隔列表形式的搜索域。

e) 选择防火墙模式：透明或路由式。

在路由模式中，FTD 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。

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 FMC 主机名，则 FTD 使用 DNS。

- g) 输入 FTD 的完全限定主机名。
- h) 输入注册期间要在 FMC 和设备之间共享的注册密钥。
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 FTD 时，需要在 FMC 上输入相同的密钥。
- i) 输入供 FTD 管理员用户用于 CLI 访问的密码。
- j) 选择应该发送事件的事件接口。如果未指定，系统将使用管理接口。
此接口必须定义为 Firepower 事件接口。
- k) 对于容器实例，请将硬件加密设置为已启用或已禁用。
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。始终为本地实例启用此功能。要查看分配给该实例的硬件加密资源百分比，请输入 `show hw-crypto` 命令。

步骤 7 在协议选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 单击确定关闭配置对话框。

步骤 9 点击保存。

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，可以开始在应用中配置安全策略。



步骤 10 请参阅 FMC 配置指南，将 FTD 添加为受管设备，并开始配置安全策略。

为 FDM 添加独立的 FTD

可以将 FDM 与本地实例结合使用。不支持容器实例。独立逻辑设备可单独使用，也可在高可用性对中使用。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300 机箱。



注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（并且在**接口**选项卡的顶部显示为 **MGMT**）。
- 您还必须至少配置一个数据类型的接口。
- 收集以下信息：
 - 此设备的接口 ID
 - 管理接口 IP 地址和网络掩码
 - 网关 IP 地址
 - DNS 服务器 IP 地址
 - FTD 主机名和域名

过程

步骤 1 选择逻辑设备。

步骤 2 点击添加 > 独立设备，并设置以下参数：

a) 提供设备名称。

此名称由机箱管理引擎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。

b) 对于模板，请选择 **Cisco Firepower 威胁防御**。

c) 选择映像版本。

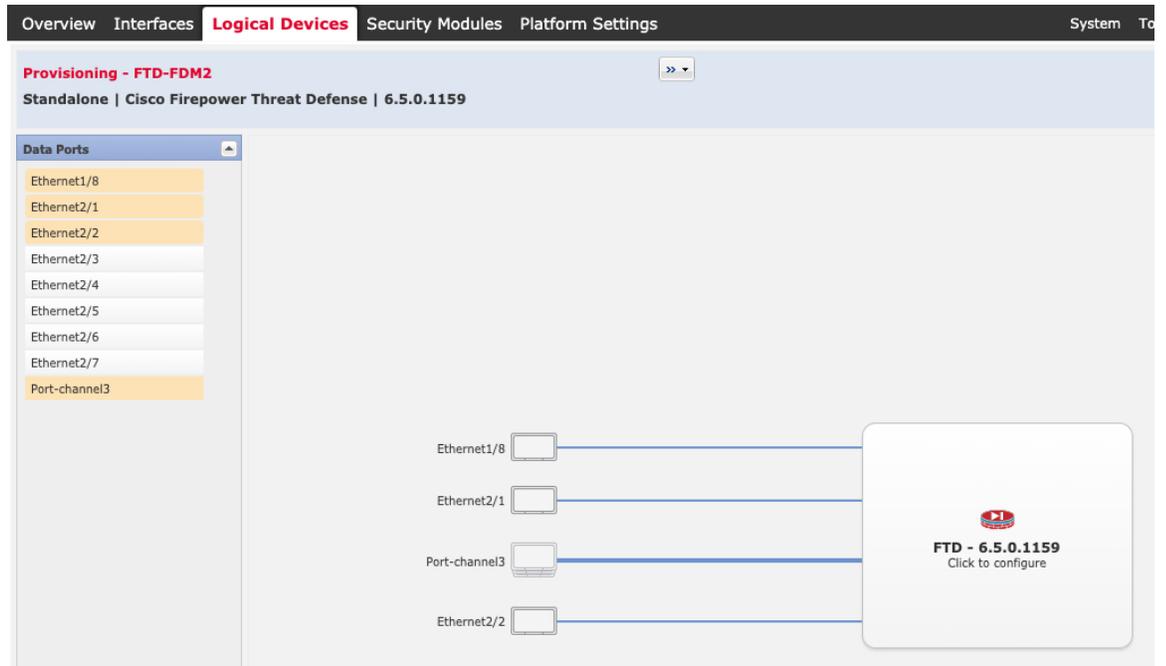
d) 选择实例类型：**本地**。

FDM不支持容器实例。

e) 单击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开数据端口区域，然后点击要分配给设备的每个接口。

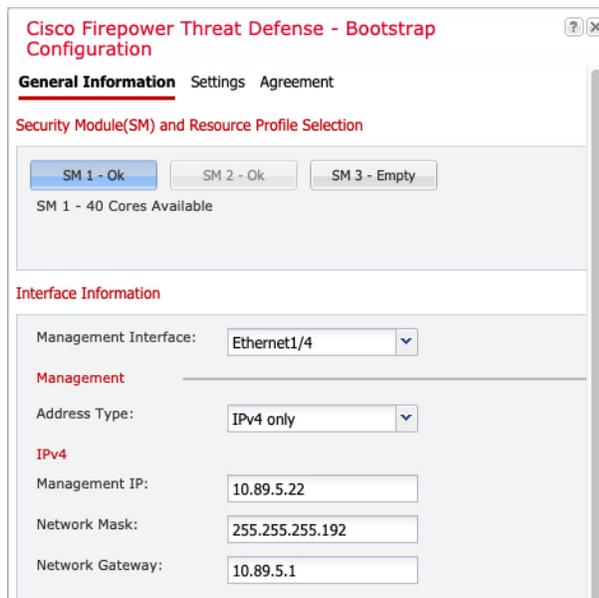


仅可分配先前在接口页面上启用的数据接口。稍后您需要在 FDM 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 单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 5 在一般信息页面上，完成下列操作：



a) （对于 Firepower 9300）在安全模块选择下，点击您想用于此逻辑设备的安全模块。

- b) 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。
- c) 选择**管理接口地址类型**：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- d) 配置**管理 IP 地址**。
设置用于此接口的唯一 IP 地址。
- e) 输入**网络掩码或前缀长度**。
- f) 输入**网络网关地址**。

步骤 6 在**设置选项卡**上，完成下列操作：

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The configuration fields are as follows:

- Management type of application instance: **LOCALLY_MANAGED** (dropdown)
- Firepower Management Center IP: (empty text field)
- Search domains: **cisco.com** (text field)
- Firewall Mode: **Routed** (dropdown)
- DNS Servers: **10.8.9.6** (text field)
- Firepower Management Center NAT ID: (empty text field)
- Fully Qualified Hostname: **ftd.example.cisco.com** (text field)
- Registration Key: (empty text field)
- Confirm Registration Key: (empty text field)
- Password: ********* (password field)
- Confirm Password: ********* (password field)
- Eventing Interface: (empty dropdown)

Buttons at the bottom: **OK** and **Cancel**.

- a) 在**应用实例的管理类型**下拉列表中，选择 **LOCALLY_MANAGED**。
本地实例还支持 Firepower Management Center 作为管理器。如果在部署逻辑设备后更改管理器，则系统会清除您的配置，并重新初始化设备。
- b) 输入逗号分隔列表形式的**搜索域**。
- c) **防火墙模式**仅支持路由式。
- d) 输入逗号分隔列表形式的 **DNS 服务器**。
- e) 输入FTD的**完全限定主机名**。
- f) 输入供FTD管理员用户用于 CLI 访问的**密码**。

步骤 7 在**协议选项卡**上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 单击**确定**关闭配置对话框。

步骤 9 点击保存。

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**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，可以开始在应用中配置安全策略。

**步骤 10** 请参阅《FDM 配置指南》，以开始配置安全策略。

添加高可用性对

FTD 或 ASA 高可用性（也称为故障切换）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅[高可用性的要求和前提条件](#)，第 15 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障切换和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障切换和状态链路。如果您有可用的接口，可以使用单独的故障切换和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障切换或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障切换接口。

对于容器实例，故障切换链路不支持数据共享接口。我们建议您在父接口或 EtherChannel 上创建子接口，并为每个实例分配子接口以用作故障切换链路。请注意，您必须将同一父接口上的所有子接口用作故障切换链路。不得将一个子接口用作故障切换链路，然后将其他子接口（或父接口）用作常规数据接口。

步骤 3 在逻辑设备上启用高可用性。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

注释 对于 ASA，如果在 FXOS 中移除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

添加集群

通过集群，您可以将多台设备组合成单个逻辑设备。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。包含多个模块的 Firepower 9300 支持机箱内集群，在此，即您可以将单个机箱中的所有模块分组到一个群集中。您还可使用将多个机箱组合在一起的机箱间集群；机箱间集群是单模块设备（例如 Firepower 4100 系列）的唯一选择。

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。
 - 对于机箱内集群（仅限 Firepower 9300），此链路利用 Firepower 9300 背板进行集群通信。
 - 对于机箱间集群，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。如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。
- 将数据接口作为跨网络接口分配给集群。
 - 对于机箱内集群，跨网络接口不仅限于 EtherChannel，与机箱间集群类似。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。对于机箱间集群，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。

- 向群集中的所有设备分配管理接口。

主设备角色和辅助设备角色

群集的一个成员是主设备。系统自动确定主设备。所有其他成员都是辅助设备。

您必须仅在主设备上执行所有配置；然后，配置将复制到辅助设备。

群集控制链接

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。

对于机箱内群集，此接口未设任何成员接口。此集群类型 EtherChannel 利用 Firepower 9300 背板进行机箱内群集的群集通信。对于机箱间群集，必须将一个或多个接口添加到 EtherChannel。

对于包含 2 个成员的机箱间群集，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，群集控制链路失效，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群集控制链路，则群集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。

设定机箱间群集的群集控制链路大小

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

群集控制链路流量主要由状态更新和转发的数据包组成。群集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，群集需要对大量连接进行再均衡，因此会暂时耗用大量群集控制链路带宽。

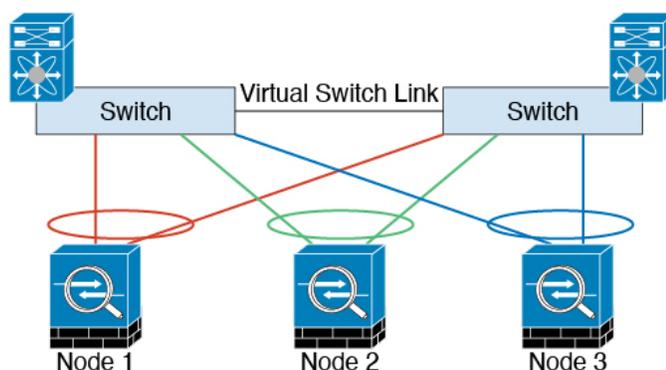
带宽较高的群集控制链路可以帮助群集在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。



注释 如果群集中存在大量不对称（再均衡）流量，应增加群集控制链路的吞吐量大小。

机箱间群集的群集控制链路冗余

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为群集控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是 VSS 或 vPC 的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到 VSS 或 vPC 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。



机箱间群集的群集控制链路可靠性

为了确保群集控制链路的功能，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群集成员的兼容性。要检查延迟，请在设备之间的群集控制链路上执行 ping 操作。

群集控制链路必须可靠，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。

群集控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成群集控制链路接口 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。当您部署群集时，您可以自定义此 IP 地址。群集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。对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与群集控制链路分隔开来。

管理接口

必须为群集分配管理类型的接口。此接口是相对于跨网络 (Spanned) 接口的特殊单独接口。通过管理接口，可以直接连接到每个设备。

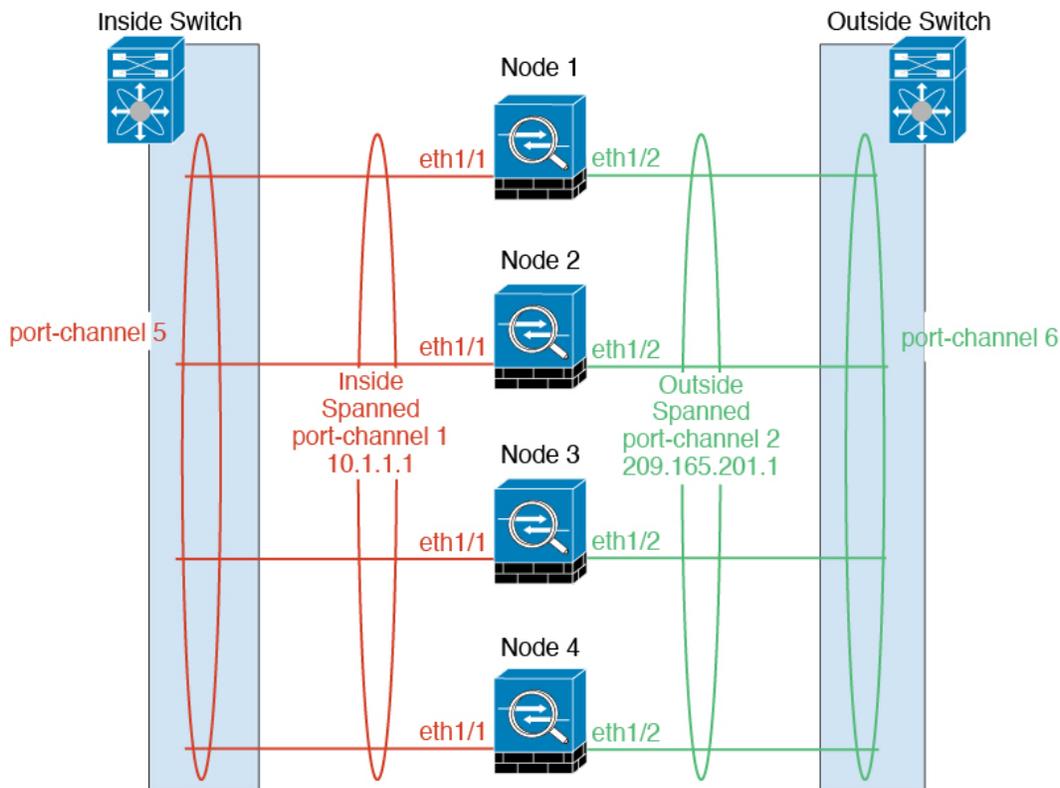
对于 ASA，主群集 IP 地址是始终属于当前主设备的群集的固定地址。您必须配置一个地址范围，使每个设备（包括当前主设备在内）都能使用该范围内的本地地址。主群集 IP 地址提供对地址的统一管理访问权限；当主设备更改时，主群集 IP 地址将转移给新的主设备，使群集管理可以无缝衔接。本地 IP 地址用于路由，在排除故障时也非常有用。例如，可以通过连接到主群集 IP 地址来管理群集，该地址始终连接到当前主设备。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每个设备都使用本地 IP 地址来连接到服务器。

对于 FTD，请向同一网络上的每个设备分配管理 IP 地址。将每个设备连接到 FMC 时，请使用这些 IP 地址。

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。



站点间群集

对于站点间安装，您只要遵循建议的准则即可充分发挥群集的作用。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发出的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨区以太网通道的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟以及连接的站点冗余，其中流量流的备用所有者始终位于与所有者不同的站点上。

有关站点间群集的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - [群集要求和必备条件](#)，第 11 页

- 站点间准则 -[集群准则和限制](#)，第 18 页
- 站点间示例：[站点间群集示例](#)，第 78 页

添加 ASA 群集

您可以将单个 Firepower 9300 机箱添加为机箱内群集，或添加多个机箱以实现机箱间群集。对于机箱间群集，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 ASA 集群

将范围设置为映像版本。

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。

对于机箱间集群，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。

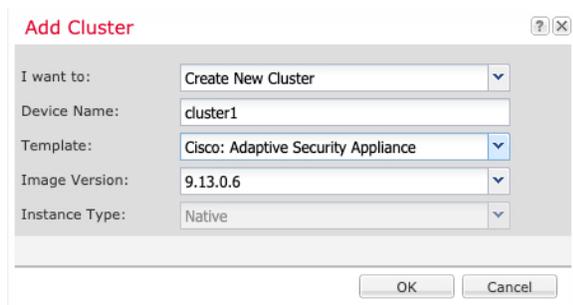
对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

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。
- 收集以下信息：
 - 管理接口 ID、IP 地址和网络掩码
 - 网关 IP 地址

过程

- 步骤 1** 配置接口。
- 步骤 2** 选择逻辑设备 (**Logical Devices**)。
- 步骤 3** 依次单击添加 > 集群，并设置以下参数：



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，请选择思科自适应安全设备。

d) 选择映像版本 (Image Version)。

e) 对于实例类型，仅支持本地类型。

f) 单击确定 (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。

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。

步骤 5 单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 在集群信息页面上，完成以下操作。

Cisco: Adaptive Security Appliance - Bootstrap Configuration

Cluster Information Settings

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: asa_cluster

Management Interface: Ethernet1/4

CCL Subnet IP: Eg:x.x.0.0

DEFAULT

Address Type: IPv4 only

IPv4

Management IP Pool: 10.89.5.10 - 10.89.5.22

Virtual IPv4 Address: 10.89.5.25

Network Mask: 255.255.255.192

Network Gateway: 10.89.5.1

OK Cancel

- a) 对于机箱间集群，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。
- b) 对于站点间集群，在**站点 ID**字段中输入此机箱的站点 ID（1 和 8 之间的整数）。
- c) 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。
- d) 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。
- e) 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。

- f) (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。

- g) 选择管理接口的地址类型。

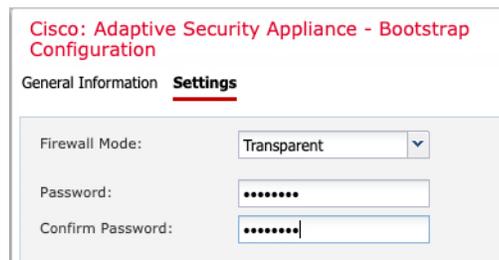
此信息用于配置 ASA 配置中的管理接口。设置以下信息：

- **管理 IP 池** - 配置本地 IP 地址池，其中一个地址将分配给接口的每个集群设备，方法是输入以连字符分隔的起始地址和结束地址。

至少包含与集群中的设备数量相同的地址。请注意，对于 Firepower 9300，每台机箱必须包括 3 个地址，即使未填满所有模块插槽。如果计划扩展集群，则应包含更多地址。属于当前控制设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

- **网络掩码或前缀长度**
- **网络网关**
- **虚拟 IP 地址** - 设置当前控制设备的管理 IP 地址。此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。

步骤 7 在设置页面上，执行以下操作。



The screenshot shows the 'Settings' tab in the 'Cisco: Adaptive Security Appliance - Bootstrap Configuration' interface. Under the 'Firewall Mode' section, a dropdown menu is set to 'Transparent'. Below it are two password fields: 'Password' and 'Confirm Password', both containing masked characters (dots).

- a) 从防火墙模式下拉列表中选择透明或路由。

在路由模式中，FTD 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。

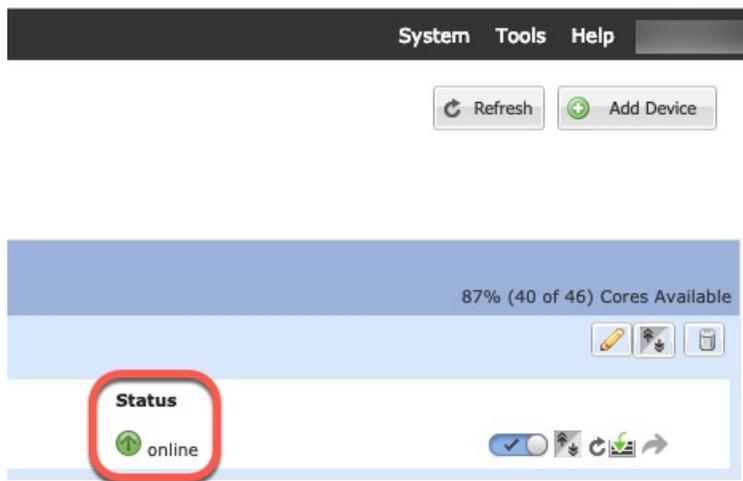
- b) 输入并确认管理员用户和启用密码的密码。

预配置的 ASA 管理员用户在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

步骤 8 单击确定关闭配置对话框。

步骤 9 点击保存。

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**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；对于机箱内集群，则可以开始在空中配置集群。您可能在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。

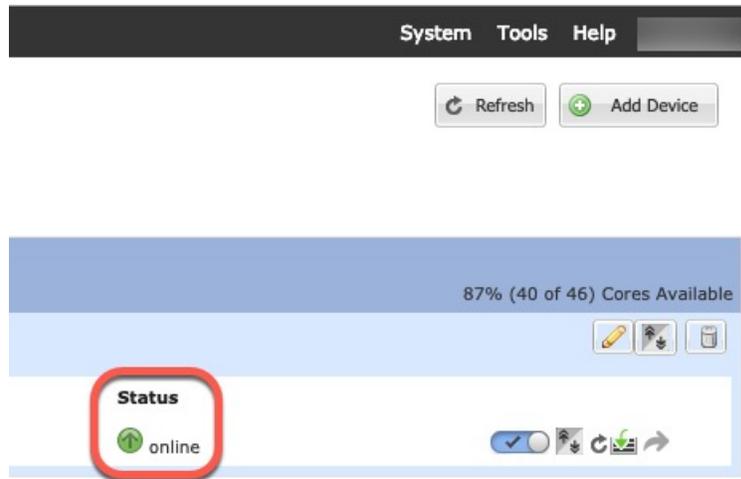
**步骤 10** 对于机箱间集群，将下一个机箱添加到集群中：

- 在第一个 Firepower 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
- 连接到下一个机箱上的 Firepower 机箱管理器，然后按照此程序添加逻辑设备。
- 选择我想要：(**I want to:**) > **加入现有集群 (Join an Existing Cluster)**。
- 单击确定。
- 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，然后单击**确定**。
- 单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** - 输入正确的站点 ID。
 - **集群密钥** - (未预填充) 输入相同的集群密钥。

单击**确定 (OK)**。

g) 点击保存。

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**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，可以开始在空中配置集群。您可能在此过程中看到“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 11 连接到控制设备 ASA 以自定义集群配置。

添加更多群集成员

添加或替换 ASA 群集成员。



注释 此程序仅适用于添加或替换机箱；如果将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

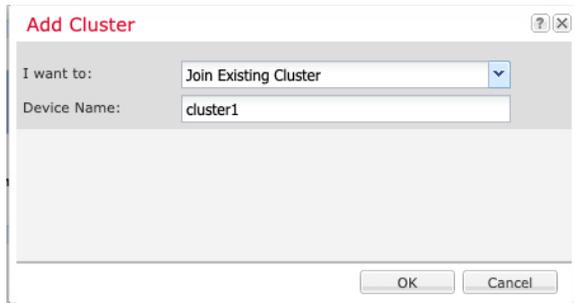
- 确保现有群集在此新成员的管理 IP 地址池中有足够的 IP 地址。如果没有，您需要在每个机箱上编辑现有群集引导程序配置，然后才可添加此新成员。此更改将导致重新启动逻辑设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。
- 对于多情景模式，在第一个群集成员上的 ASA 应用中启用多情景模式；其他群集成员将自动继承多情景模式配置。

过程

步骤 1 在现有群集 Firepower 机箱管理器上，选择**逻辑设备**打开**逻辑设备**页面。

步骤 2 单击右上角的显示配置图标 ()；复制显示的群集配置。

步骤 3 连接到新机箱上的 Firepower 机箱管理器，然后单击**添加 > 群集**。



步骤 4 选择我想要： > 加入现有群集

步骤 5 对于设备名称，请为逻辑设备提供一个名称。

步骤 6 确定。

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。

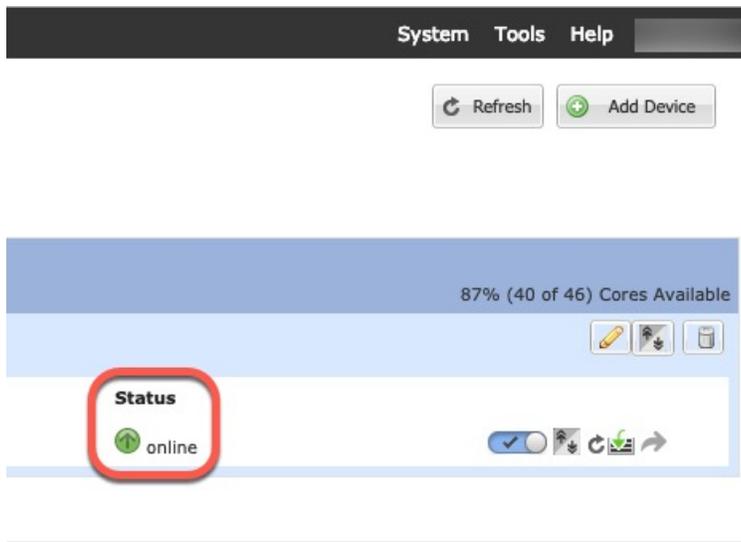
步骤 8 单击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- 机箱 ID - 输入唯一的机箱 ID。
- 站点 ID - 输入正确的站点 ID。
- 集群密钥 - (未预填充) 输入相同的集群密钥。

单击确定 (OK)。

步骤 9 单击保存 (Save)。

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。



添加 FTD 群集

在原生模式下：您可以将单个 Firepower 9300 机箱添加为机箱内群集，或添加多个机箱以实现机箱间群集。

在多实例模式下：您可以在单个 Firepower 9300 机箱上添加一个或多个群集作为机箱内群集（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群集以用于机箱间群集。

对于机箱间群集，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 FTD 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。

对于机箱间群集，您必须单独配置每个机箱。在一个机箱上部署群集；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。

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）启用群集，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)，然后单击重新初始化图标 (Ⓢ)。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。有关详细信息，请参阅[重新初始化安全模块/引擎](#)。
- 收集以下信息：
 - 管理接口 ID、IP 地址和网络掩码
 - 网关 IP 地址
 - FMC 您选择的 IP 地址和/或 NAT ID
 - DNS 服务器 IP 地址
 - FTD 主机名和域名

过程

- 步骤 1 配置接口。
- 步骤 2 选择逻辑设备 (Logical Devices)。

步骤 3 依次单击添加 > 集群，并设置以下参数：

图 6: 本地集群

图 7: 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。

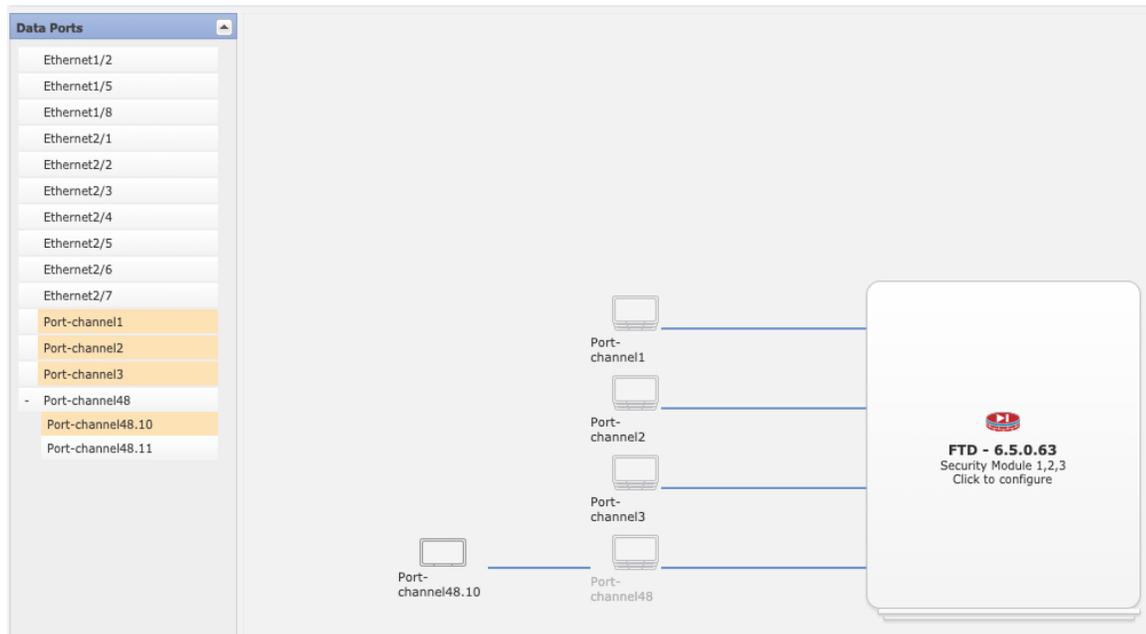
- f) (仅限容器实例) 对于资源类型 (Resource Type)，请从下拉列表中选择一个资源配置文件。

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) 单击确定 (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。

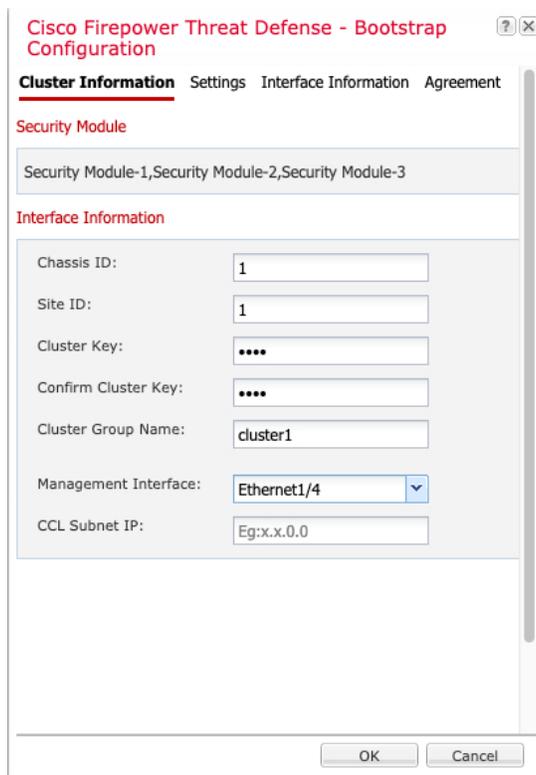
对于多实例集群：选择要分配到集群的每个数据接口，并选择集群类型端口-通道或端口-通道子接口。

步骤 5 单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 在集群信息页面上，完成以下操作。

图 8: 本地集群



The image shows a configuration window titled "Cisco Firepower Threat Defense - Bootstrap Configuration". The window has a tabbed interface with the following tabs: "Cluster Information" (selected), "Settings", "Interface Information", and "Agreement".

Under the "Cluster Information" tab, there are two main sections:

- Security Module:** A text box containing "Security Module-1, Security Module-2, Security Module-3".
- Interface Information:** A form with the following fields:
 - Chassis ID:
 - Site ID:
 - Cluster Key:
 - Confirm Cluster Key:
 - Cluster Group Name:
 - Management Interface: - CCL Subnet IP:

At the bottom of the window, there are two buttons: "OK" and "Cancel".

图 9: 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) 对于机箱间集群, 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 FMC 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 在设置页面上，执行以下操作。

- 在 **注册密钥** 字段中，输入注册期间 FMC 与集群成员之间要共享的密钥。
可以为该密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加 FTD 时，需要在 FMC 上输入相同的密钥。
- 输入供 FTD 管理员用户用于 CLI 访问的密码。
- 在 **Firepower 管理中心 IP** 字段中，输入执行管理 FMC 的 IP 地址。如果您不知道 FMC 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。
- (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 FTD 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 FTD 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，FTD 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 FMC 主机名，则 FTD 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 FMC 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（连同注册密钥）：FMC 指定设备 IP 地址，设备指定 FMC 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。FMC 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 FTD 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**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。

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Settings **Interface Information** Agreement

Address Type: IPv4 only

Security Module 1
IPv4
Management IP: 10.89.5.20
Network Mask: 255.255.255.192
Gateway: 10.89.5.1

Security Module 2
IPv4
Management IP: 10.89.5.21
Network Mask: 255.255.255.192
Gateway: 10.89.5.1

Security Module 3
IPv4
Management IP: 10.89.5.22
Network Mask: 255.255.255.192
Gateway: 10.89.5.1

OK Cancel

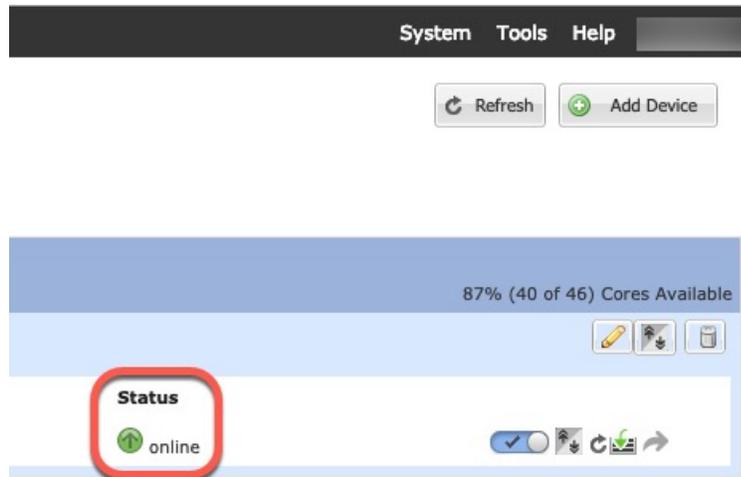
- a) 在**管理 IP (Management IP)** 字段中，配置 IP 地址。
在同一网络上为每个模块指定唯一 IP 地址。
- b) 输入网络掩码或前缀长度。
- c) 输入网络网关地址。

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 单击确定关闭配置对话框。

步骤 11 点击保存。

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**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；对于机箱内集群，则可以开始在应用中配置集群。您可能在此过程中看到“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 对于机箱间集群，将下一个机箱添加到集群中：

- a) 在第一个 Firepower 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 Firepower 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) 单击**确定**。
- 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，然后单击**确定**。
- f) 单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 FMC 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。

单击**确定**。

- 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**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 FMC。

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 FMC。

然后，FMC 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 FTD 集群节点。在 FXOS 中添加新的集群节点时，FMC 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 FMC 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 FMC 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 FMC 升级了 FTD 映像，请在集群中的每个机箱上执行以下步骤。

当您从 FMC 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 FTD 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 Firepower 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 Firepower 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 单击**确定**。

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**。

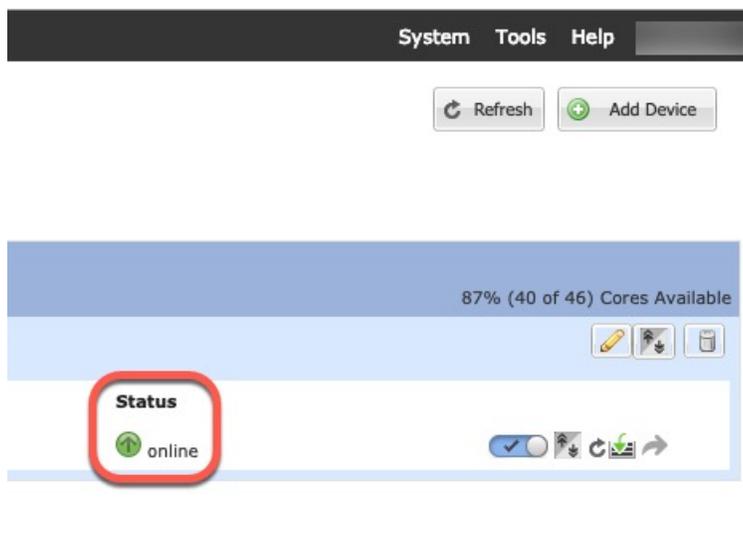
步骤 8 单击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- **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）。此功能仅可使用 FMC FlexConfig 功能进行配置。
- **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。

单击**确定 (OK)**。

步骤 9 单击**保存 (Save)**。

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**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。



配置 Radware DefensePro

思科 Firepower 4100/9300 机箱可在单个刀片上支持多个服务（例如防火墙和第三方 DDoS 应用）。这些应用和服务可以链接在一起形成服务链。

关于 Radware DefensePro

在当前支持的服务链配置中，可以安装第三方 Radware DefensePro 虚拟平台以在 ASA 防火墙前面或在 FTD 前面运行。Radware DefensePro 是基于 KVM 的虚拟平台，可在 Firepower 4100/9300 机箱上提供分布式拒绝服务 (DDoS) 检测和缓解功能。当在 Firepower 4100/9300 机箱上启用服务链时，来自网络的流量必须先通过 DefensePro 虚拟平台，然后再到达主要 ASA 或 FTD 防火墙。



注释

- Radware DefensePro 虚拟平台可以称为 *Radware vDP*（虚拟 DefensePro），或者简称为 *vDP*。
- Radware DefensePro 虚拟平台有时可能是指链路修饰器。

Radware DefensePro 的必备条件

在 Firepower 4100/9300 机箱上部署 Radware DefensePro 之前，必须将 Firepower 4100/9300 机箱配置为使用 **etc/UTC** 时区的 NTP 服务器。有关设置 Firepower 4100/9300 机箱日期与时间的详细信息，请参阅[设置日期和时间](#)。

服务链准则

模式

- ASA - 以下型号的 ASA 支持 Radware DefensePro (vDP) 平台：

- Firepower 9300
- Firepower 4115
- Firepower 4120
- Firepower 4125
- Firepower 4140
- Firepower 4145
- Firepower 4150



注释 在 Firepower 4110 设备上，当前不支持 Radware DefensePro 平台用于 ASA。

- FTD - 以下型号的 FTD 支持 Radware DefensePro 平台：

- Firepower 9300
- Firepower 4110 - 请注意，还必须同时部署修饰器与逻辑设备。在设备上配置了逻辑设备后，无法安装修饰器。
- Firepower 4112
- Firepower 4115
- Firepower 4120 - 请注意，还必须同时部署修饰器与逻辑设备。在设备上配置了逻辑设备后，无法安装修饰器。
- Firepower 4125
- Firepower 4140
- Firepower 4145
- Firepower 4150



注释 您必须使用 CLI 在所有 FTD 平台上部署 Radware DefensePro；Firepower 机箱管理器 尚不支持此功能。

其他规定

- 服务链在机箱间群集配置中不受支持。但是，在机箱间群集场景中，可采用独立配置部署 Radware DefensePro (vDP) 应用。

在独立逻辑设备上配置 Radware DefensePro

以下程序显示如何在独立 ASA 或 FTD 逻辑设备前面的单个服务链中安装 Radware DefensePro。



注释 设置 vDP 应用并在此程序结束时提交更改后，逻辑设备（ASA 或 FTD）将重新启动。

如果要在 Firepower 4120 或 4140 安全设备上的 ASA 前面安装 Radware vDP，则必须使用 FXOS CLI 部署修饰器。有关如何在 Firepower 4100 设备上在 ASA 前面的服务链中安装和配置 Radware DefensePro 的完整 CLI 说明，请参阅 FXOS CLI 配置指南。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅[从 Cisco.com 下载映像](#)），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅[将映像上传到安全设备](#)）。
- 您可以在机箱内集群的独立配置中部署 Radware DefensePro 应用；对于机箱内集群，请参阅在[机箱内集群上配置 Radware DefensePro](#)，第 59 页。

过程

- 步骤 1** 如果要将单独的管理接口用于 vDP，请启用该接口并根据[配置物理接口](#)将其设置为管理类型。否则，您可以共享应用管理接口。
- 步骤 2** 选择**逻辑设备**打开“逻辑设备”页面。

“逻辑设备”页面显示在机箱上配置的逻辑设备列表。如果尚未配置逻辑设备，系统将显示一条消息，要求您配置逻辑设备。
- 步骤 3** 创建独立的 ASA 或 FTD 逻辑设备（请参阅[添加独立 ASA](#)，第 22 页 或为 [FMC 添加独立 FTD](#)，第 24 页）。
- 步骤 4** 在**修饰器**区域中，选择 vDP。系统将显示“Radware: 虚拟 DefensePro - 配置”窗口。在**一般信息**选项卡下配置以下字段。
- 步骤 5** 如果您已将多个 vDP 版本上传到 Firepower 4100/9300 机箱，请在**版本**下拉列表中选择要使用的版本。
- 步骤 6** 如果您有一个资源可配置的 Radware DefensePro 应用，则**资源配置文件**下拉列表下会显示支持的资源配置文件列表。选择要分配给设备的资源配置文件。如果未选择资源配置文件，则使用默认设置。
- 步骤 7** 在**管理接口**下拉列表下，选择在此操作步骤的步骤 1 中创建的管理接口。
- 步骤 8** 选择默认**地址类型**：仅 IPv4、仅 IPv6，或者 IPv4 和 IPv6。

步骤 9 根据在上一步中选择的地址类型，配置以下字段。

- a) 在**管理 IP** 字段中，配置本地 IP 地址。
- b) 仅 IPv4：输入**网络掩码**。
仅 IPv6：输入**前缀长度**。
- c) 输入**网络网关地址**。

步骤 10 点击您想要分配给设备的每个数据端口旁边的复选框。

步骤 11 单击**确定 (OK)**。

步骤 12 单击**保存 (Save)**。

FXOS通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定安全模块来部署逻辑设备。

下一步做什么

为 DefensePro 应用设置密码。请注意，在您完成密码设置之前，DefensePro 应用无法联网。有关更多信息，请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。

在机箱内集群上配置 Radware DefensePro

以下程序显示如何安装 Radware DefensePro 映像、如何在 ASA 或 FTD 机箱内集群前面的服务链中配置此映像。



注释 服务链在机箱间集群配置中不受支持。但是，Radware DefensePro 应用可在机箱间集群情景的独立配置中进行部署。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅[从 Cisco.com 下载映像](#)），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅[将映像上传到安全设备](#)）。

过程

步骤 1 如果要将单独的管理接口用于 vDP，请启用该接口并根据[配置物理接口](#)将其设置为管理类型。否则，您可以共享应用管理接口。

步骤 2 配置 ASA 或 FTD 机箱内集群（请参阅[创建 ASA 集群](#)，第 38 页 或 [创建 FTD 集群](#)，第 45 页）。

请注意，在配置机箱内集群的程序结束时单击**保存**之前，必须首先按照以下步骤将 vDP 修饰器添加到集群。

- 步骤 3** 在修饰器区域中，选择 vDP。系统将显示 **Radware: 虚拟 DefensePro - 配置对话框**。在一般信息选项卡下配置以下字段。
- 步骤 4** 如果已将多个 vDP 版本上传到 Firepower 4100/9300 机箱，请在版本下拉列表中选择要使用的 vDP 版本。
- 步骤 5** 如果您有一个资源可配置的 Radware DefensePro 应用，则“资源配置文件”下拉列表下会显示支持的资源配置文件列表。选择要分配给设备的资源配置文件。如果未选择资源配置文件，则使用默认设置。
- 步骤 6** 在管理接口下拉列表下，选择管理接口。
- 步骤 7** 点击您想分配给 vDP 修饰程序的每个数据端口旁边的复选框。
- 步骤 8** 点击接口信息选项卡。
- 步骤 9** 选择要使用的地址类型，仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- 步骤 10** 为每个安全模块配置以下字段。请注意，显示的字段取决于您在上一步中选择的地址类型。
- a) 在管理 IP 字段中，配置本地 IP 地址。
 - b) 仅 IPv4: 输入网络掩码。
仅 IPv6: 输入前缀长度。
 - c) 输入网络网关地址。
- 步骤 11** 单击确定 (OK)。
- 步骤 12** 单击保存 (Save)。

FXOS通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定安全模块来部署逻辑设备。

- 步骤 13** 选择逻辑设备打开“逻辑设备”页面。
- 步骤 14** 滚动已配置的逻辑设备列表至 vDP 条目。验证管理 IP 列中列出的属性。
- 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为未知，必须进入 DefensePro 应用，配置控制设备 IP 地址，完成 vDP 集群创建。
 - 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为 *primary* 或 *secondary*，则说明应用在线，并且已在集群中形成。

下一步做什么

为 DefensePro 应用设置密码。请注意，在您完成密码设置之前，DefensePro 应用无法联网。有关更多信息，请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。

开放 UDP/TCP 端口和启用 vDP Web 服务

Radware APSolute Vision 管理器接口可使用各种 UDP/TCP 端口与 Radware vDP 应用进行通信。为使 vDP 应用与 APSolute Vision 管理器进行通信，您必须确保这些端口可访问及未被防火墙阻止。有关哪些特定接口可开放的详细信息，请参阅《APSolute Vision 用户指南》中的以下表格：

- APSolute Vision 服务器端口 - WBM 通信和操作系统
- 带 Radware 设备的 APSolute Vision 服务器的通信端口

为使 Radware APSolute Vision 管理部署在 FXOS 机箱上的虚拟 DefensePro 应用，您必须使用 FXOS CLI 启用 vDP Web 服务。

过程

步骤 1 从 FXOS CLI 连接到 vDP 应用实例。

```
connect module slot console
```

```
connect vdp
```

步骤 2 启用 vDP Web 服务。

```
manage secure-web status set enable
```

步骤 3 退出 vDP 应用控制台并返回 FXOS 模块 CLI。

```
Ctrl ]
```

配置 TLS 加密加速

以下主题讨论 TLS 加密加速、如何启用它，以及如何使用 FMC 查看其状态。

下表会将 FTD 和 FXOS 版本与所需的 TSL 加密进行映射：



注释 当 FXOS 2.6.1 升级到 FXOS 2.7.x 及更高版本时，FTD 6.4 不会自动启用加密，因为 6.4 与 TLS 加密不兼容。

FTD	FXOS	加密
6.4	2.6	仅支持一个容器实例（第 1 阶段）
6.4	2.7 及更高版本	不适用
6.5 及更高版本	2.7 及更高版本	支持最多 16 个容器实例（第 2 阶段）

关于 TLS 加密加速

The Firepower 4100/9300 支持传输层安全加密加速，它在硬件中执行传输层安全/安全套接层 (TLS/SSL) 加密和解密，这极大地改进了以下方面的性能：

- TLS/SSL 加密和解密。
- VPN，包括 TLS/SSL 和 IPsec

TLS 加密加速功能在本地实例上自动启用，无法禁用。您还可以在每个安全引擎/模块上的最多 16 个 FTD 容器实例上启用 TLS 加密加速。

TLS 加密加速的准则和限制

如果 FTD 启用了 TLS 加密加速，请记住以下几点。

检测引擎故障

如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL 流量将被丢弃，直到引擎重启。

此行为由 FTD **configure snort preserve-connection {enable | disable}** 命令控制。

仅 HTTP 性能

在不解密流量的 FTD 容器实例上使用 TLS 加密加速可能会影响性能。我们建议 TLS 加密加速仅在解密 TLS/SSL 流量的 FTD 容器实例上启用。

联邦信息处理标准 (FIPS)

如果同时启用了 TLS 加密加速和联邦信息处理标准 (FIPS)，则与以下选项的连接会失败：

- 大小小于 2048 字节的 RSA 密钥
- Rivest 密码 4 (RC4)
- 单一数据加密标准 (单一 DES)
- Merkle - Damgard 5 (MD5)
- SSL v3

当您 FMC 和 FTD 配置为以安全认证合规模式运行时，FIPS 会被启用。在这些模式下运行时，要允许连接，可以在 FTD 容器实例上禁用 TLS 加密加速，或者可以配置 Web 浏览器以接受更为安全的选项。

更多详情：

- [通用标准](#)。

高可用性 (HA) 和集群

如果有高可用性 (HA) 或集群 FTD，则必须分别在每个 FTD 上启用 TLS 加密加速。一个设备的 TLS 加密加速配置不与 HA 对或集群中的其他设备共享。

TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 TLS 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速的受 FMC 管理的 FTD 遇到使用 TLS 心跳扩展的数据包时，该 FTD 将执行 SSL 策略的无法解密的操作中解密错误 FMC 设置所指定的操作：

- 阻止
- 阻止并重置

要确定应用程序是否使用 TLS 心跳，请参阅《Firepower 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

如果在 FTD 容器实例上禁用 TLS 加密加速，则可以在 FMC 中的网络分析策略 (NAP) 中配置最大心跳长度，以便确定如何处理 TLS 心跳。

有关 TLS 心跳的详细信息，请参阅《Firepower 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

TLS/SSL 超订用

TLS/SSL 超订用指 FTD 的 TLS/SSL 流量过载的状态。任何 FTD 都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速的 FTD 才提供可配置的方式对其进行处理。

当启用了 TLS 加密加速的 FMC 管理的 FTD 发生超订用时，对于该 FTD 接收的任何数据包，都将根据 SSL 策略无法解密的操作中握手错误设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 SSL 策略无法解密的操作中握手错误的设置为不解密，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密不会发生。

如果出现大量超订用，有以下选项可供选择：

- 升级到具有更多 TLS/SSL 处理能力的 FTD。
- 更改您的 SSL 策略，为不具有较高解密优先级的流量添加不解密规则。

有关 TLS 超订用的详细信息，请参阅《Firepower 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

不支持被动和内联轻触设置

启用 TLS 加密加速后，无法在被动或内联轻触设置接口上解密 TLS/SSL 流量。

启用容器实例的 TLS 加密加速

当按照为 [FMC 添加独立 FTD](#)，第 24 页中所述部署逻辑实例时，将自动启用 TLS 加密加速。

TLS 加密加速将在所有本地实例上自动启用，并且无法禁用。

查看 TLS 加密加速的状态

本主题讨论如何确定是否已启用 TLS 加密加速。

请执行 FMC 中的下列任务。

过程

步骤 1 登录 FMC。

步骤 2 点击设备 > 设备管理。

步骤 3 点击 **编辑** () 以编辑受管设备。

步骤 4 单击设备 (**Device**) 页面。TLS 加密加速 状态显示在“常规” (General) 部分中。

启用 FTD 链路状态同步

机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动 FTD 关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。

该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。此功能不会影响非数据接口（例如管理接口或集群接口）。

当您启用 FTD 链路状态同步时，FXOS 中接口的 **服务状态** 将与 FTD 中此接口的管理状态同步。例如，如果关闭 FTD 中的接口，“服务状态”将显示为“已禁用”。如果关闭 FTD 应用，所有接口将显示为“已禁用”。对于硬件旁路接口，以管理方式关闭 FTD 中的接口会将“服务状态”设置为“已禁用”；但关闭 FTD 应用或执行其他机箱级别的关闭（包括关闭电源）会使接口保持“已启用”状态。

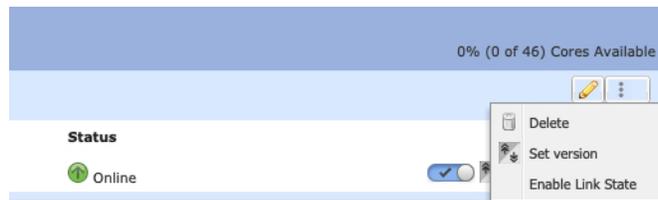
如果禁用 FTD 链路状态同步，则“服务状态”将始终显示为“已启用”。



注释 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。

过程

步骤 1 选择逻辑设备 (**Logical Devices**)，然后为 FTD 逻辑设备从下拉列表中选择启用链路状态 (**Enable Link State**)。



要禁用该功能，选择禁用链路状态 (**Disable Link State**)。

步骤 2 查看当前接口状态，以及上次关闭原因。

show interface expand detail

示例：

```
Firepower # scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface expand detail
Interface:
  Port Name: Ethernet1/2
  User Label:
  Port Type: Data
  Admin State: Enabled
  Oper State: Up
  State Reason:
  flow control policy: default
  Auto negotiation: Yes
  Admin Speed: 1 Gbps
  Oper Speed: 1 Gbps
  Admin Duplex: Full Duplex
  Oper Duplex: Full Duplex
  Ethernet Link Profile name: default
  Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
  Uddl Oper State: Admin Disabled
  Inline Pair Admin State: Enabled
  Inline Pair Peer Port Name:
  Service State: Enabled
  Last Service State Down Reason: None
  Allowed Vlan: All
  Network Control Policy: default
  Current Task:
  <...>
```

管理逻辑设备

您可以删除逻辑设备、将ASA转换为透明模式、更改接口配置并在现有逻辑设备上执行其他任务。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module slot_number { console | telnet }

要连接至不支持多个安全模块的设备的引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。为您的设备输入适当的命令。

connect asa name

connect ftd name

connect vdp name

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect asa asal
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
```

>

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- ASA - 输入 **Ctrl-a, d**
- FTD - 输入 **exit**
- vDP - 输入 **Ctrl-], .**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

- 输入 ~
您将退出至 Telnet 应用。
- 要退出 Telnet 应用，请输入：
telnet>quit

退出 Telnet 会话：

- 输入 **Ctrl-], .**

示例

以下示例连接至安全模块 1 上的 ASA，然后退回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

删除逻辑设备

过程

步骤 1 选择逻辑设备打开“逻辑设备”页面。

“逻辑设备”页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。

步骤 2 单击想要删除的逻辑设备所对应的删除 (**Delete**)。

步骤 3 单击是 (**Yes**) 确认想要删除此逻辑设备。

步骤 4 单击是 (**Yes**) 确认想要删除应用配置。

删除集群设备

以下部分介绍如何临时或永久删除群集中的设备。

临时删除

例如，出现硬件或网络故障时，集群设备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群集中，登录 Firepower 机箱管理器 **逻辑设备** 页面查看群集状态：

Management Port	Status
Ethernet1/4	online

Attributes

- Cluster Operational Status : not-in-cluster
- FIREPOWER-MGMT-IP : 10.89.5.20
- CLUSTER-ROLE : none
- CLUSTER-IP : 127.2.1.1
- MGMT-URL : https://10.89.5.35/
- UUID : 8e459170-451d-11e9-8475-f22f06c32630

对于使用 FMC 的 FTD，应该将设备留在 FMC 设备列表中，以便在重新启用群集后，它可以恢复全部功能。

- 在应用程序中禁用群集 - 您可以使用应用程序 CLI 禁用群集。输入 **cluster remove unit name** 命令删除除您登录的设备以外的所有设备。引导程序配置保持不变，从控制设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在数据设备上输入此命令来删除控制设备，将会选举新的控制设备。

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，请重新启用群集。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。但如果您重新加载，而设备仍在群集中处于非主用状态，则管理接口将被禁用。

要重新启用群集，请在 ASA 上输入 **cluster group name**，然后输入 **enable**。要重新启用群集，请在 FTD 上输入 **cluster enable**。

- 禁用应用程序实例 - 在 Firepower 机箱管理器的 **逻辑设备** 页面，单击 **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 Firepower 机箱管理器的 安全模块/引擎 页面，单击 关闭电源 图标。
- 关闭机箱 - 在 Firepower 机箱管理器的 “概览” 页面，单击 关机 图标。

永久删除

您可以使用以下方法永久删除群集成员。

对于使用 FMC 的 FTD，确保在机箱上禁用群集后，从 FMC 设备列表删除设备。

- 删除逻辑设备 - 在 Firepower 机箱管理器的 “逻辑设备” 页面，单击 删除 ()。然后，您可以部署独立的逻辑设备、新的群集，还可以在同一个群集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群集的新成员。

删除与逻辑设备不关联的应用实例

删除逻辑设备后，系统将提示您是否要删除逻辑设备的应用配置。如果不删除应用配置，则在删除该应用实例之前，将无法使用其他应用创建逻辑设备。当应用实例不再与逻辑设备关联时，可使用以下程序步骤从 安全模块/引擎 中删除应用实例。

过程

步骤 1 选择逻辑设备打开 “逻辑设备” 页面。

“逻辑设备” 页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。在逻辑设备列表下方，您可以看到与逻辑设备不关联的应用实例列表。

步骤 2 单击想要删除的应用实例所对应的删除 (Delete)。

步骤 3 单击是 (Yes) 确认想要删除应用实例。

更改 FTD 逻辑设备上的接口

可以在 FTD 逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 FMC 或 FDM 中同步接口配置。

添加新接口或删除未使用接口对 FTD 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 FTD 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 FMC 或 FDM 上进行同步。

对于 FMC：删除接口将删除与该接口相关的任何配置。

对于 FDM：可以在删除旧接口前，将配置从一个接口迁移至另一个接口。

开始之前

- 根据配置物理接口和添加 EtherChannel（端口通道）配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。FTD 重新启动（管理接口更改导致重新启动），并且在 FMC 或 FDM 中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在 FMC 或 FDM 中同步配置。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

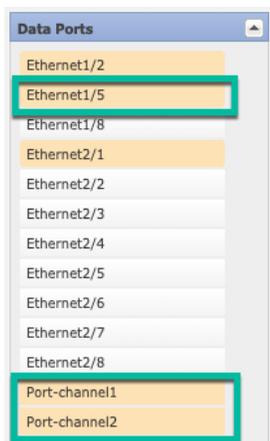
过程

步骤 1 在 Firepower 机箱管理器中，选择逻辑设备。

步骤 2 点击右上角的编辑图标以编辑逻辑设备。

步骤 3 通过在数据端口区域中选择新的数据接口来分配该接口。

请勿删除任何接口。



步骤 4 替换管理或事件接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

- 点击页面中心的设备图标。
- 在常规或集群信息选项卡上，从下拉列表中选择新的管理接口。
- 在设置选项卡上，从下拉列表中选择新的事件接口。
- 点击确定。

如果更改管理接口的 IP 地址，则还必须更改 FMC 中设备的 IP 地址：转到设备 > 设备管理 > 设备/集群。在管理区域中，设置 IP 地址以匹配引导程序配置地址。

步骤 5 单击保存 (Save)。

步骤 6 同步 FMC 中的接口。

- a) 登录至 FMC。
- b) 依次选择设备 (Devices) > 设备管理 (Device Management)，并单击 FTD 设备的编辑 (✎)。系统默认选择接口 (Interfaces) 页面。
- c) 单击接口页面左上方的同步设备按钮。
- d) 检测到更改后，可以在接口页面上看到红色横幅，表明接口配置已发生更改。单击[单击了解详情](#)链接以查看接口更改。
- e) 如果计划删除接口，请手动将任何接口配置从旧接口传输至新接口。

由于尚未删除任何接口，因此可以引用现有配置。在删除旧接口并重新运行验证后，将有额外的机会来修复配置。验证将显示仍在使用旧接口的所有位置。

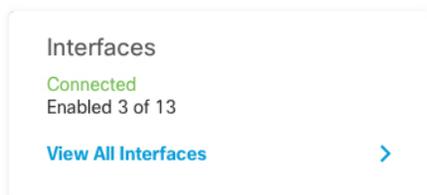
- f) 单击验证更改 (Validate Changes) 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

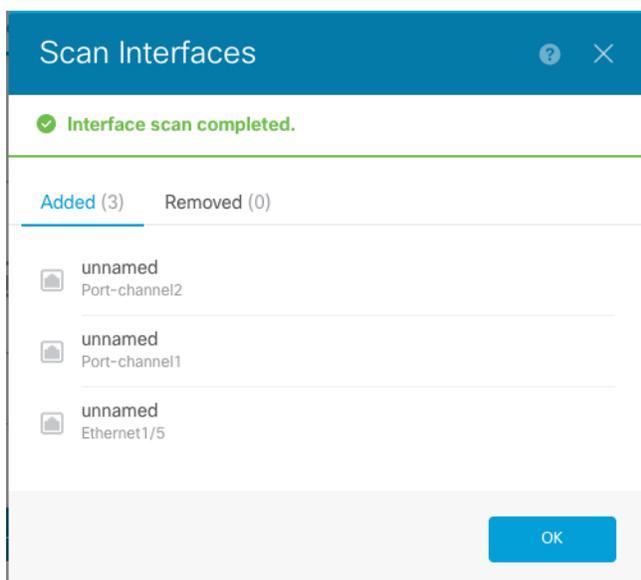
- g) 单击保存。
- h) 选择设备然后单击部署，以将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 7 同步和迁移 FDM 中的接口。

- a) 登录至 FDM。
- b) 单击设备 (Device)，然后单击接口 (Interfaces) 摘要中的[查看所有接口 \(View All Interfaces\)](#) 链路。



- c) 单击扫描接口图标。
- d) 等待接口扫描，然后单击确定。



- e) 使用名称、IP 地址等配置新接口。

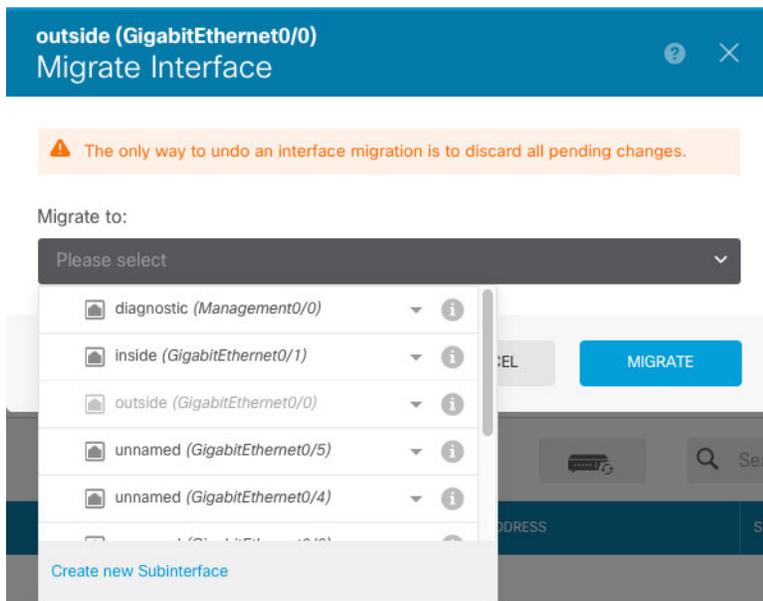
如果要使用待删除接口的现有 IP 地址和名称，则需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

- f) 要将旧接口替换为新接口，请点击旧接口的“替换”图标。

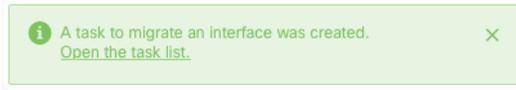
替换图标

此过程会将旧接口替换为引用该接口的所有配置设置中的新接口。

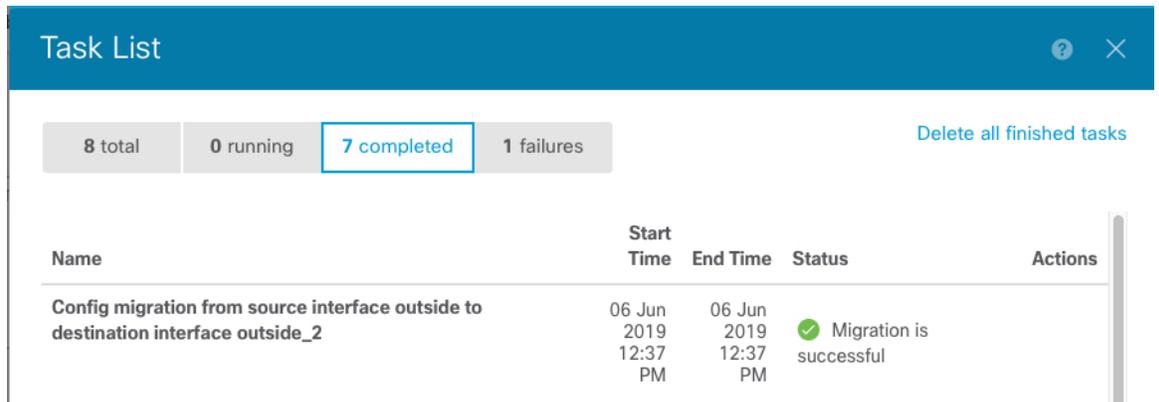
- g) 从替换接口下拉列表中选择新接口。



- h) 一则消息将显示在接口页面上。点击消息中的链接。



i) 检查任务列表，以确保迁移成功。



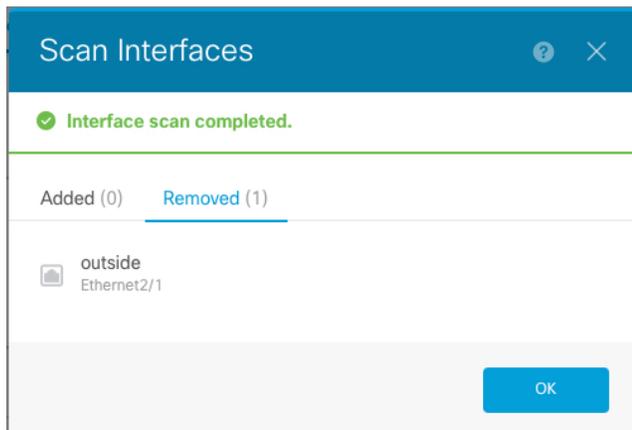
步骤 8 在 Firepower 机箱管理器 中，通过在数据端口 (Data Ports) 区域中取消选择数据接口来取消分配该接口。



步骤 9 点击保存。

步骤 10 再次在 FMC或 FDM 中同步接口。

图 10: FDM 扫描接口



更改 ASA 逻辑设备上的接口

可以在 ASA 逻辑设备上分配、取消分配或替换管理接口。ASDM 会自动发现新接口。

添加新接口或删除未使用的接口对 ASA 配置的影响很小。但是，如果在 FXOS 中删除已分配的接口（例如，如果删除网络模块、删除 EtherChannel，或将分配的接口重新分配给 EtherChannel），并且在安全策略中使用该接口，则删除操作会影响 ASA 配置。在这种情况下，ASA 配置会保留原始命令，以便您可以进行任何必要的调整。您可以在 ASA OS 中手动移除旧的接口配置。



注释 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。

开始之前

- 根据[配置物理接口](#)和[添加 EtherChannel（端口通道）](#)配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。在 ASA 重新加载（管理接口更改导致重新加载）后，您还可以将（当前取消分配的）管理接口添加到 EtherChannel。
- 对于群集或故障切换，请确保添加或移除所有设备上的接口。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。新的接口在管理性关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 在 Firepower 机箱管理器中，选择逻辑设备。

步骤 2 点击右上角的编辑图标以编辑逻辑设备。

步骤 3 通过在数据端口 (**Data Ports**) 区域中取消选择数据接口来取消分配该接口。

步骤 4 通过在数据端口 (**Data Ports**) 区域中选择新的数据接口来分配该接口。

步骤 5 替换管理接口：

对于此类型的接口，在您保存更改后，设备会重新加载。

a) 单击页面中心的设备图标。

b) 在常规/群集信息 (**General/Cluster Information**) 选项卡上，从下拉列表中选择新的管理接口 (**Management Interface**)。

c) 单击确定 (**OK**)。

步骤 6 单击保存 (**Save**)。

修改或恢复逻辑设备的引导程序设置

您可以修改逻辑设备的引导程序设置。然后可以立即使用这些新设置重启应用实例，或者保存更改，稍后再使用这些新设置重启应用实例。

过程

步骤 1 在 Firepower 机箱管理器中，选择逻辑设备。

步骤 2 点击右上角的编辑图标以编辑逻辑设备。

步骤 3 单击页面中心的设备图标。

步骤 4 根据需要修改逻辑设备设置。

步骤 5 单击 **OK**。

步骤 6 单击**立即重启**，以保存更改并立即重启应用实例。单击**稍后重启**，以保存更改而不重启应用实例。

注释 如果您选择**稍后重启**，您可以在准备好时，通过单击“逻辑设备”页面中的**重启实例**来重启应用实例。

“逻辑设备 (Logical Devices)” 页面

使用 Firepower 机箱管理器的逻辑设备页面创建、编辑和删除逻辑设备。逻辑设备页面包含每个 Firepower 4100/9300 机箱 安全模块/引擎上安装的逻辑设备的信息区域。

每个逻辑设备区域的标头均提供以下信息：

- 逻辑设备的唯一名称。
- 逻辑设备模式，即“独立 (Standalone)”或“群集 (Clustered)”。
- 状态 - 显示逻辑设备的状态：
 - ok - 逻辑设备配置完成。
 - incomplete-configuration - 逻辑设备配置未完成。

每个逻辑设备区域均提供以下信息：

- 应用 - 显示安全模块上运行的应用。
- 版本 - 显示安全模块上运行的应用的软件版本号。



注释 对逻辑设备FTD进行的更新是通过FMC完成的，而且所做的更新并未反映在Firepower 机箱管理器中的**逻辑设备编辑 (Logical Devices > Edit)** 和**系统更新 (System > Updates)** 页面上。这些页面中显示的版本是指创建 FTD逻辑设备所用的软件版本（CSP 映像）。

- 资源配置文件 - 显示分配给逻辑设备/应用程序实例的资源配置文件。
- 管理 IP - 显示分配作为逻辑设备管理 IP 的本地 IP 地址。
- 网关 - 显示分配给应用实例的网络网关地址。
- 管理端口 - 显示分配给应用实例的管理端口。
- 状态 - 显示应用实例的状态：
 - 在线 (Online) - 应用正在运行和工作。
 - 离线 (Offline) - 应用已停止并且不可操作。
 - 正在安装 (Installing) - 应用安装正在进行。
 - 未安装 (Not Installed) - 应用未安装。
 - 安装失败 (Install Failed) - 应用安装失败。
 - 正在启动 (Starting) - 应用正在启动。
 - 启动失败 (Start Failed) - 应用启动失败。
 - 已启动 (Started) - 应用成功启动，正在等待应用代理心跳。
 - 正在停止 (Stopping) - 应用正在停止。
 - 停止失败 (Stop Failed) - 应用无法进入离线状态。
 - 未响应 (Not Responding) - 应用未响应。

- 正在更新 - 应用软件正在更新。
- 更新失败 - 应用软件更新失败。
- 更新成功 - 应用软件更新成功。
- 不支持 - 不支持安装的应用程序。

如果安全模块不存在或处于故障状态，该信息将显示在状态字段中。您可以将鼠标悬停在信息图标上，以查看故障的其他信息。有关安全模块故障的详细信息，请参阅[关于 FXOS 安全模块/安全引擎](#)。

- **扩展的信息区域** - 显示当前正在运行的应用程序实例的其他属性。



注释 如果修改了应用的引导程序设置而未立即重启应用实例，则在应用重启之前，属性字段将显示当前正在运行的应用的信息，而不会反映所做的更改。

- **端口** - 显示分配给应用程序实例的接口名称和类型。
- **群集操作状态** - 显示分配给应用实例的管理 URL。
- **管理 IP/Firepower 管理 IP** - 显示分配给应用实例的管理 IP 地址。
- **集群角色** - 显示应用实例、控制或数据的集群角色。
- **群集 IP** - 显示分配给应用程序实例的 IP 地址。
- **HA 角色** - 显示应用实例的高可用性角色：主用或备用。
- **管理 URL** - 显示分配给应用实例的管理应用 URL。
- **UUID** - 显示应用实例的全局唯一标识符。

从 Firepower 机箱管理器的**逻辑设备**页面，可以在逻辑设备上执行以下功能：

- **刷新** - 刷新“逻辑设备”页面上的信息。
- **添加设备** - 允许您创建逻辑设备。
- **编辑** - 允许您编辑现有逻辑设备。
- **设置版本** - 用于升级或降级逻辑设备上的软件。
- **删除** - 删除逻辑设备。
- **显示配置** - 打开对话框，以 JSON 格式显示逻辑设备或群集的配置信息。您可以复制配置信息，并在创建作为群集一部分的更多设备时使用此配置信息。
- **启用/禁用** - 启用或禁用应用实例。
- **升级/降级** - 允许您升级或降级应用实例。

- **重启实例** - 允许您重启应用实例。如果您已修改设备引导程序信息，但尚未重新启动应用实例，您可以单击“重新启动实例”，以清除现有的管理引导程序信息，并使用新的引导程序信息重新启动应用实例。
- **重新安装实例** - 用于重新安装应用程序实例。
- **转到设备管理器** - 提供指向为应用实例所定义的 FMC 或 ASDM 的链接。
- **启用/禁用链路状态** - 启用或禁用 FTD 链路状态同步。有关详细信息，请参阅[启用 FTD 链路状态同步](#)，第 64 页。

站点间群集示例

以下示例显示支持的群集部署。

具有站点特定的 MAC 地址的跨网络 EtherChannel 路由模式示例

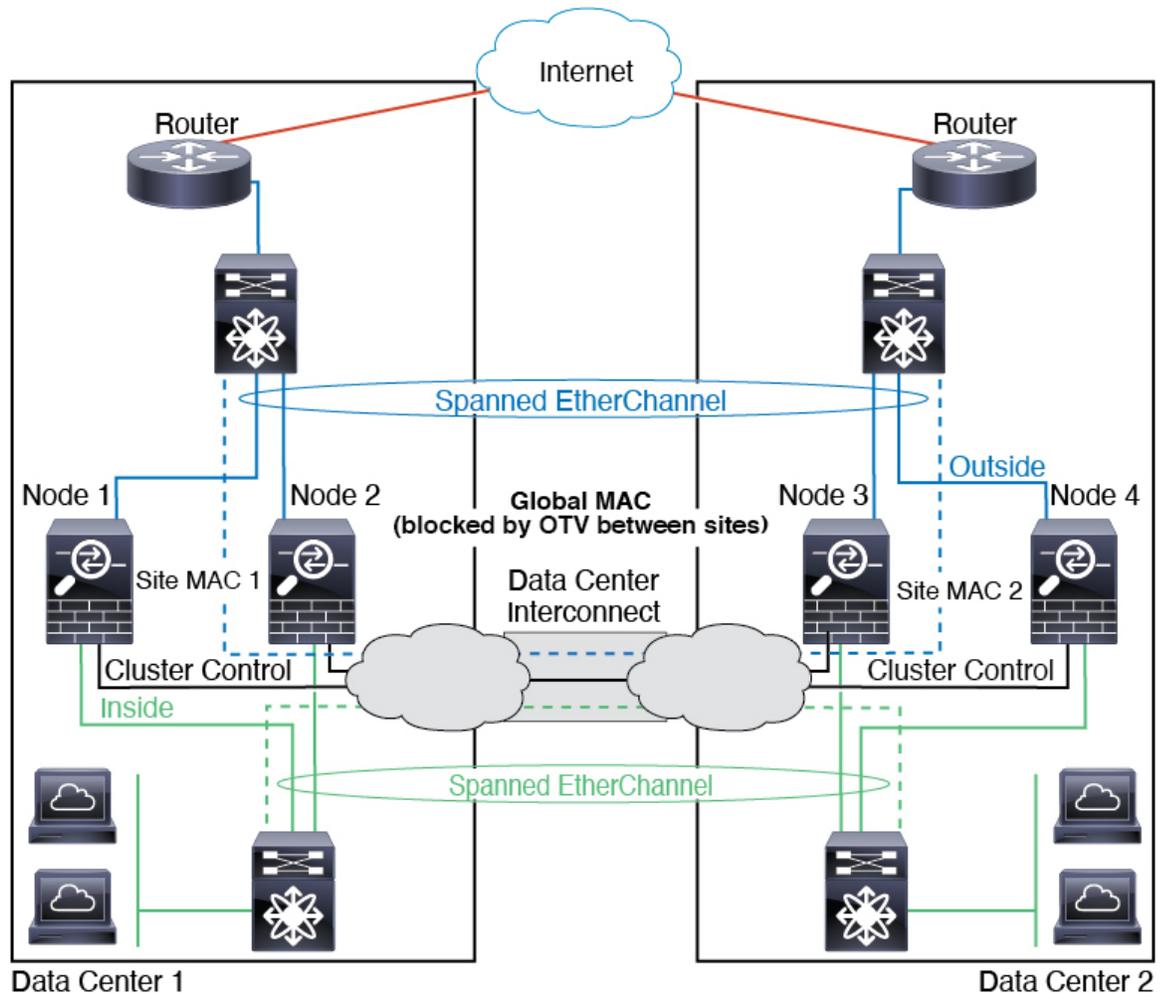
以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和内部网络之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集中的所有机箱。

数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加阻止全局 MAC 地址的过滤器，防止发往集群的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群节点，则您必须删除过滤器，使流量能够发送到另一站点的集群节点。您应使用 VACL 来过滤全局 MAC 地址。务必禁用 ARP 检查。

集群相当于内部网络的网关。所有集群节点共享的全局虚拟 MAC 仅用于接收数据包。传出数据包使用来自每个 DC 集群的站点特定的 MAC 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。

在此场景中：

- 从集群发送的所有出口数据包使用站点 MAC 地址，并在数据中心进行本地化。
- 发送到集群的所有入口数据包使用全局 MAC 地址发送，因此可以被两个站点的任何节点接收；OTV 的过滤器将数据中心内的流量本地化。



跨区以太网通道透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

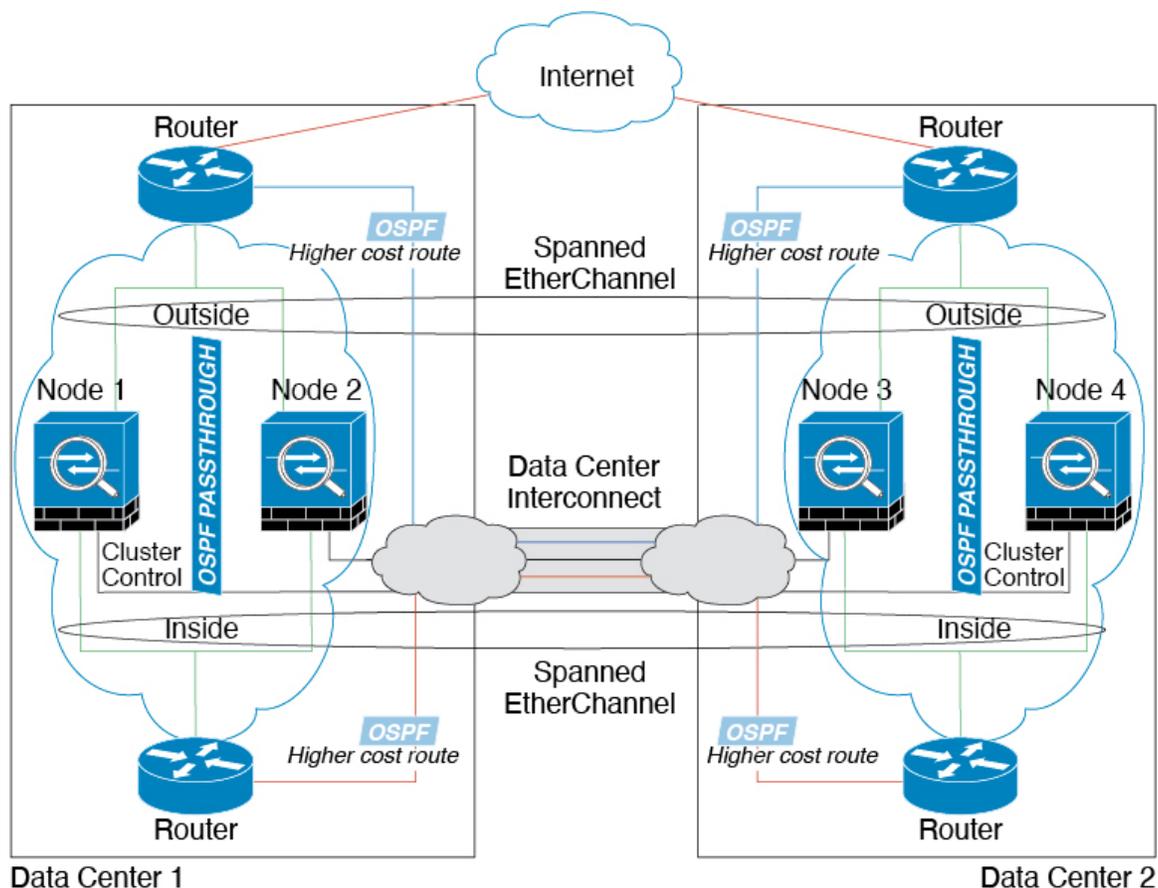
位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- 站点间 VSS/vPC - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群节点只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您

也可以选择将每个节点通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。

- 位于每个站点的本地 VSS/vPC - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管集群节点仍然有一个跨区以太网通道将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨区以太网通道本质上是“分离的”。每个本地 VSS/vPC 都会将跨区以太网通道视作站点本地的 EtherChannel。

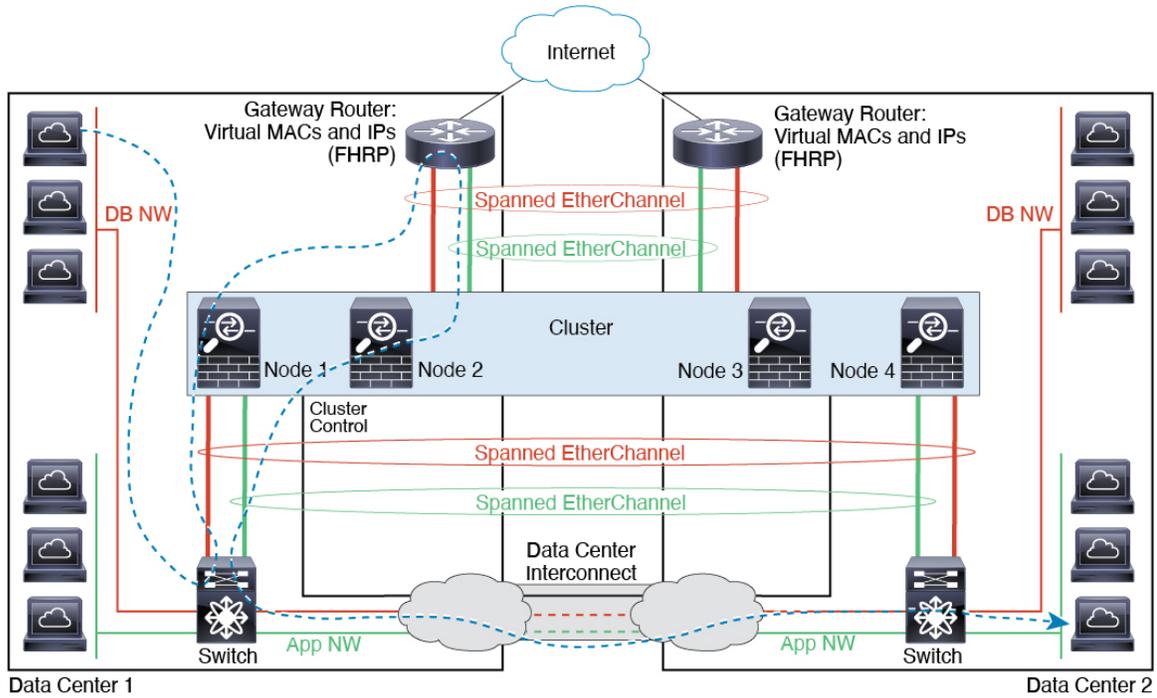


跨网络 EtherChannel 透明模式东西站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和两个内部网络（应用网络和数据库网络）之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。要避免 MAC 地址意外摆动，最好使用将网关路由器实际 MAC 地址静态添加到 ASA MAC 地址表。如果没有这些条目，当位于站点 1 的网关与位于站点 2 的网关通信时，流量可能通过 ASA 并尝试从内部接口到达站点 2，从而导致出现问题。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤器，阻止发往网关路由器的流量通过 DCI 发送到另一站点。如果

无法访问一个站点上的网关路由器，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



逻辑设备的历史记录

功能名称	平台版本	功能信息
FTD 运行链路状态与物理链路状态之间的同步	2.9.1	<p>机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动 FTD 关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。</p> <p>注释 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。</p> <p>新增/修改的 Firepower 机箱管理器 屏幕：逻辑设备 > 启用链路状态</p> <p>新增/修改的 FXOS 命令：set link-state-sync enabled、show interface expand detail</p>

功能名称	平台版本	功能信息
对容器实例使用 FMC 的 FTD 配置备份和恢复	2.9.1	<p>您现在可以在 FTD 容器实例上使用 FMC 备份/恢复工具。</p> <p>新增/修改的 FMC 屏幕：系统 (System) > 工具 (Tools) > 备份/恢复 (Backup/Restore) > 受管设备备份 (Managed Device Backup)</p> <p>新增/修改的 FTD CLI 命令：restore</p> <p>支持的平台：Firepower 4100/9300</p> <p>注释 需要使用 Firepower 6.7。</p>
多实例群集	2.8.1	<p>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。</p> <p>新增/修改的菜单项：</p> <ul style="list-style-type: none"> • 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 <p>注释 需要使用 Firepower 6.6 或更高版本。</p>
支持带有 FDM 的 FTD	2.7.1	<p>现在，您可以部署本地 FTD 实例并指定 FDM 管理。不支持容器实例。</p> <p>新增/修改的 Firepower 机箱管理器 菜单项：</p> <p>逻辑设备 > 添加设备 > 设置 > 应用程序实例的管理类型</p> <p>注释 需要 FTD 6.5 或更高版本。</p>
多个容器实例的 TLS 加密加速	2.7.1	<p>现在，在 Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。</p> <p>新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，请依次使用 enter hw-crypto 和 set admin-state enabled FXOS 命令。</p> <p>新增/修改的 Firepower 机箱管理器菜单项：</p> <p>逻辑设备 > 添加设备 > 设置 > 硬件加密下拉菜单</p> <p>注释 需要 FTD 6.5 或更高版本。</p>
Firepower 4115、4125 和 4145	2.6.1	<p>我们推出了 Firepower 4115、4125 和 4145。</p> <p>注释 要求 ASA 9.12(1)。Firepower 6.4.0 要求 FXOS 2.6.1.157。</p> <p>未修改任何菜单项。</p>

功能名称	平台版本	功能信息
Firepower 9300 SM-40、SM-48 和 SM-56 支持	2.6.1	<p>引入了以下三个安全模块：SM-40、SM-48 和 SM-56。</p> <p>注释 SM-40 和 SM-48 要求 ASA 9.12(1)。SM-56 要求 ASA 9.12(2) 和 FXOS 2.6.1.157。</p> <p>所有模块都要求 FTD6.4 和 FXOS 2.6.1.157。</p> <p>未修改任何菜单项。</p>
支持在同一个 Firepower 9300 上使用独立的 ASA 和 FTD 模块	2.6.1	<p>您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD 逻辑设备。</p> <p>注释 要求 ASA 9.12(1)。Firepower 6.4.0 要求 FXOS 2.6.1.157。</p> <p>未修改任何菜单项。</p>
对于 FTD 引导程序配置，您现在可以在 Firepower 机箱管理器 中设置 FMC 的 NAT ID	2.6.1	<p>您现在可以在 Firepower 机箱管理器 中设置 FMC NAT ID。以前，您只能在 FXOS CLI 或 FTD CLI 内设置 NAT ID。通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同同一个注册密钥）：FMC指定设备 IP 地址，设备指定 FMC 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。FMC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。</p> <p>新增/修改的屏幕： 逻辑设备 > 添加设备 > 设置 > Firepower 管理中心 NAT ID 字段</p>
支持将 SSL 硬件加速用于模块/安全引擎上的一个 FTD 容器实例	2.6.1	<p>您现在可以启用用于模块/安全引擎上的一个容器实例的 SSL 硬件加速。SSL 硬件加速禁用于其他容器实例，但启用于本地实例。有关详细信息，请参阅 FMC 配置指南。</p> <p>新增/修改的命令：<code>config hwCrypto enable</code>、<code>show hwCrypto</code></p> <p>未修改任何菜单项。</p>

功能名称	平台版本	功能信息
FTD 多实例功能	2.4.1	<p>您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 FTD 容器实例。以前，您仅可部署单个本地应用实例。此外，仍支持本地实例。对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。</p> <p>要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。部署容器实例时，必须指定分配的 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。此资源管理允许您自定义每个实例的性能。</p> <p>您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建 10 个高可用性对。不支持集群。</p> <p>注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全 FTD 功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。FTD 的多情景模式不可用。</p> <p>注释 要求使用 6.3 或更高版本的 FTD。</p> <p>新增/修改的 Firepower 机箱管理器菜单项： 概述 > 设备 接口 (Interfaces) > 所有接口 (All Interfaces) > 新增 (Add New) 下拉菜单 > 子接口 (Subinterface) 接口 > 所有接口 > 类型 逻辑设备 > 添加设备 平台设置 > Mac 池 平台设置 > 资源配置文件 新增/修改的 FMC 菜单项： 设备 > 设备管理 > 编辑图标 > 接口选项卡</p>
支持 ASA 逻辑设备的透明模式部署	2.4.1	<p>您现在可以在部署 ASA 时指定透明模式或路由模式。</p> <p>新增/修改的 Firepower 机箱管理器 菜单项： 逻辑设备 > 添加设备 > 设置 新增/修改的选项：防火墙模式下拉列表</p>

功能名称	平台版本	功能信息
群集控制链路可自定义 IP 地址	2.4.1	默认情况下，群集控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署群集时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的群集控制链路接口 IP 地址：127.2.chassis_id.slot_id。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的群集控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的菜单项： 逻辑设备 > 添加设备 > 群集信息 > CCL 子网 IP 字段
对于 FTD 引导程序配置，您现在可以在 FXOS CLI 中设置 FMC 的 NAT ID	2.4.1	您现在可以在 FXOS CLI 中设置 FMC NAT ID。以前，您只能在 FTD CLI 内设置 NAT ID。通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同同一个注册密钥）：FMC 指定设备 IP 地址，设备指定 FMC 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。FMC 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。 新增/修改的命令： enter bootstrap-key NAT_ID
ASA 的站点间群集改进	2.1.1	现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 我们修改了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)
Firepower 9300 上 6 个 FTD 模块的机箱内群集	2.1.1	现在，您可以对 Firepower 9300 上的 FTD 启用机箱内群集。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。 我们修改了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)
支持在 Firepower 4100 上执行 FTD 群集	2.1.1	在 FTD 群集中，最多可以群集 6 个机箱。
ASA 群集中，支持 16 个 Firepower 4100 机箱	2.0.1	在 ASA 群集中，最多可以群集 16 个机箱。
支持在 Firepower 4100 上执行 ASA 群集	1.1.4	在 ASA 群集中，最多可以群集 6 个机箱。
支持在 Firepower 9300 上的 FTD 上执行机箱内群集	1.1.4	Firepower 9300 支持使用 FTD 应用执行机箱内群集。 我们修改了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)

功能名称	平台版本	功能信息
Firepower 9300 上 16 个 ASA 模块的机箱内群集	1.1.3	<p>现在，您可以对 ASA 启用机箱间群集。最多可以包含 16 个模块。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。</p> <p>我们修改了以下屏幕：逻辑设备 (Logical Devices) > 配置 (Configuration)</p>
Firepower 9300 上 ASA 的机箱内群集	1.1.1	<p>您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建群集。</p> <p>我们引入了以下屏幕：逻辑设备 (Logical Devices) > 配置 (Configuration)</p>