为 Firepower 威胁防御部署集群

首次发布日期: 2017 年 05 月 01 日

上次修改日期: 2017 年 07 月 10 日

为 Firepower 威胁防御部署集群

集群允许您将多个 Firepower 威胁防御设备作为单一逻辑设备组合到一起。仅 Firepower 9300 和 Firepower 4100 系列 上的 Firepower 威胁防御设备支持集群。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 9 页。

关于 Firepower 4100/9300 机箱上的集群

集群由充当单一逻辑单元的多个设备组成。在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 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，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。
- 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。
- 向集群中的所有设备分配管理接口。

以下部分提供有关集群概念和实施的更多详细信息。

性能度量因素

当您将多个设备合并成一个集群时，可以期待总体集群性能约为：

- TCP 或 CPS 吞吐量 - 0.8 x *number_of_units*
- UDP 吞吐量 - 0.9 x *number_of_units*
- 以太网混合 (EMIX) 吞吐量 - 0.6 x *number_of_units*，取决于流量混合情况

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

集群成员共同作用来实现安全策略和流量的共享。本节介绍每种成员角色的性质。

主设备角色和辅助设备角色

集群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。

有些功能在集群中不会扩展，主设备会处理这些功能的所有流量。请参阅集群集中式功能，第 10 页。

主设备选举

集群成员通过集群控制链路通信，如下选举主设备：

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，则该设备会成为主设备。
4. 如果稍后有优先级更高的设备加入集群，则该设备不会自动成为主设备；现有主设备将一直作为主设备，除非它停止响应，届时将选举新的主设备。

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

群集控制链接

集群控制链路使用端口通道48接口自动进行创建。对于机箱内集群，此接口没有成员接口。对于机箱间集群，必须将一个或多个接口添加到 EtherChannel。此集群类型 EtherChannel 利用 Firepower 9300 背板进行机箱内集群的集群通信。

对于包含 2 个成员的机箱间集群，请勿直接将集群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。

集群控制链路流量包括控制流量和数据流量。

设定机箱间集群的集群控制链路大小

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：

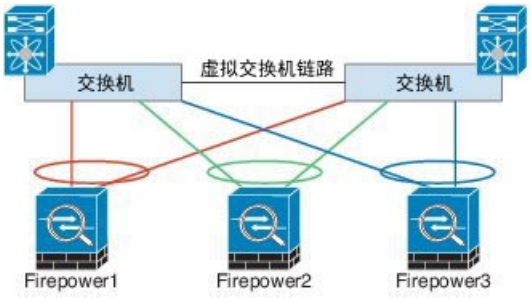
- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

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非对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

机箱间集群的集群控制链路冗余

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 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。当交换机是 VSS 或 vPC 的一部分时，您可以将同一 EtherChannel 中的 Firepower 4100/9300 机箱接口连接到 VSS 或 vPC 中不同的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独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：127.2.*chassis_id*.*slot_id*。无论在 FXOS 中还是在应用中，您都无法手动设置此 IP 地址。集群控制链路网络不能包含设备之间的任何路由器；仅允许第 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。

管理界面

对于集群，必须分配一个管理接口。此接口是与跨网络接口相对的特殊单个接口。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 Firepower 管理中心。并使用自己的逻辑身份验证、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主设备的集群固定地址。请始终配置一个地址范围，以便包括当前主设备在内的每个设备都可以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；当主设备更改时，主集群 IP 地址会移到新的主设备上，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。

集群接口

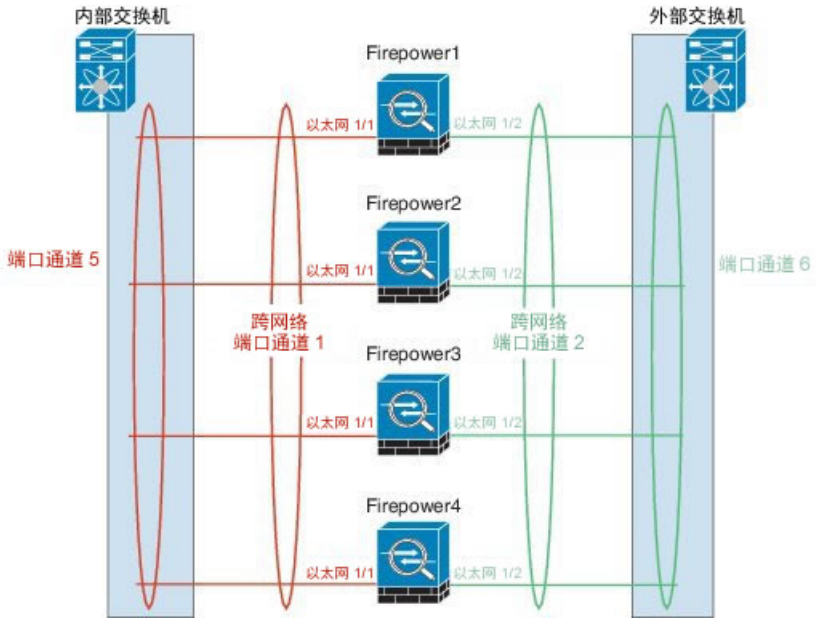
对于机箱内集群，可以向集群分配物理接口或 EtherChannel（亦称为端口通道）。分配至集群的接口为跨网络接口，它们可在集群的所有成员之间均衡流量负载。

对于机箱间集群，只能向集群分配数据 EtherChannel。这些跨网络 EtherChannel 在每个机箱上包括相同的成员接口；在上游交换机中，所有这些接口都包含在单个 EtherChannel 中，所以交换机不知道它已连接至多个设备。

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都可以配置跨网络 EtherChannel。在路由模式下，EtherChannel 被配置为只有一个 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。



连接到 VSS 或 vPC

我们建议将 EtherChannel 连接到 VSS 或 vPC，以便为接口提供冗余保障。

集群内的高可用性

集群通过监控机箱、设备和接口运行状况以及复制设备之间的连接状态提供高可用性。

机箱-应用监控

机箱-应用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 Firepower 威胁防御应用（每秒）。如果 Firepower 威胁防御设备已开启但 3 秒内无法与 Firepower 4100/9300 机箱管理引擎通信，则 Firepower 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 秒后无法与应用通信，则会重新加载 Firepower 威胁防御设备。如果 Firepower 威胁防御设备无法与管理引擎通信，则它会退出集群。

设备运行状况监控

主设备通过在集群控制链路上定期发送 keepalive 消息来监控每台从属设备。每台从属设备也使用相同的机制来监控主设备。如果设备运行状况检查失败，系统将从集群中删除该设备。

接口监控

每个设备都会监控使用中的所有硬件接口的链路状态，并向主设备报告状态变更情况。对于机箱间集群，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 Firepower 威胁防御应用。当启用运行状况监控时，默认情况下监控所有物理接口（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。

如果监控的某个端口在特定设备上出现故障，但在其他设备上处于活动状态，则会从集群中删除该特定设备。Firepower 威胁防御设备从集群中删除成员之前允许的时间取决于该设备是确定的成员还是要加入集群。Firepower 威胁防御设备 在设备加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 Firepower 威胁防御设备 从集群中删除。对于确定的成员，该设备会在 500 ms 后被删除。

对于机箱间集群，如果在集群中添加或删除 EtherChannel，接口运行状况监控会暂停 95 秒，以确保您有时间在每个机箱上进行相应的更改。

装饰器应用监控

在接口上安装装饰器（例如 Radware DefensePro 应用）应用时，Firepower 威胁防御设备和装饰器应用必须处于运行状态，才能保留在集群中。在两个应用运行之前，设备不会加入集群。加入集群后，设备会每 3 秒监控一次装饰器应用运行状态。如果装饰器应用关闭，则集群中会删除该设备。

发生故障后的状态

当集群中的设备发生故障时，该设备承载的连接将无缝转移到其他设备；流量的状态信息将通过集群控制链路共享。

如果主设备发生故障，则优先级最高（数字最小）的另一个集群成员将成为主设备。

Firepower 威胁防御设备 将自动尝试重新加入集群，具体取决于故障事件。

注释 当Firepower威胁防御设备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：

- 集群控制链路出现故障 - 解决集群控制链路的问题后，必须通过重新启用集群手动重新加入集群。
- 数据接口出现故障 - Firepower 威胁防御应用会在 5 分钟、10 分钟及 20分钟时自动尝试重新加入集群。如果在 20 分钟后未成功加入，则 Firepower 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。
- 设备发生故障 - 如果设备因设备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设备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。Firepower 威胁防御应用会每隔 5 秒尝试一次重新加入集群。
- 机箱-应用通信故障 - 当 Firepower 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。

如果所有者处于不可用状态，则系统会从该连接接收数据包的第一台设备（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。

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	-
VPN（站点到站点）	否	如果主设备发生故障，VPN 会话将断开连接。

配置复制

集群中的所有设备共享一个配置。您只能在主设备上进行配置更改，这些更改将自动同步到集群中的所有其他设备。

集群管理连接的方式

可以将连接负载均衡到多个集群成员。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

每个连接定义有 3 种不同角色：

- 所有者 - 最初接收连接的设备。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，则当新设备从连接接收到数据包时，导向器会从这些设备中选择新的所有者。
- 导向者 - 处理来自转发者的所有者查找请求，同时也维护连接状态，在所有者发生故障时作为备用设备。当所有者收到新连接时，会根据源/目标 IP 地址和 TCP 端口的散列值选择导向者，然后向导向者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设备，该设备会向导向者查询哪一台设备是所有者，以便转发数据包。一个连接只有一个导向者。如果导向器发生故障，所有者会选择一个新的导向器。
- 转发者 - 向所有者转发数据包的设备。如果转发者收到并非其所有的连接的数据包，则会向导向者查询所有者，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。导向者也可以是转发者。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，因此无需向导向者查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向者查询。）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者，然后由其发送到所有者。一个连接了可以有多个转发者；采用良好的负载均衡方法可以做到没有转发者，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。

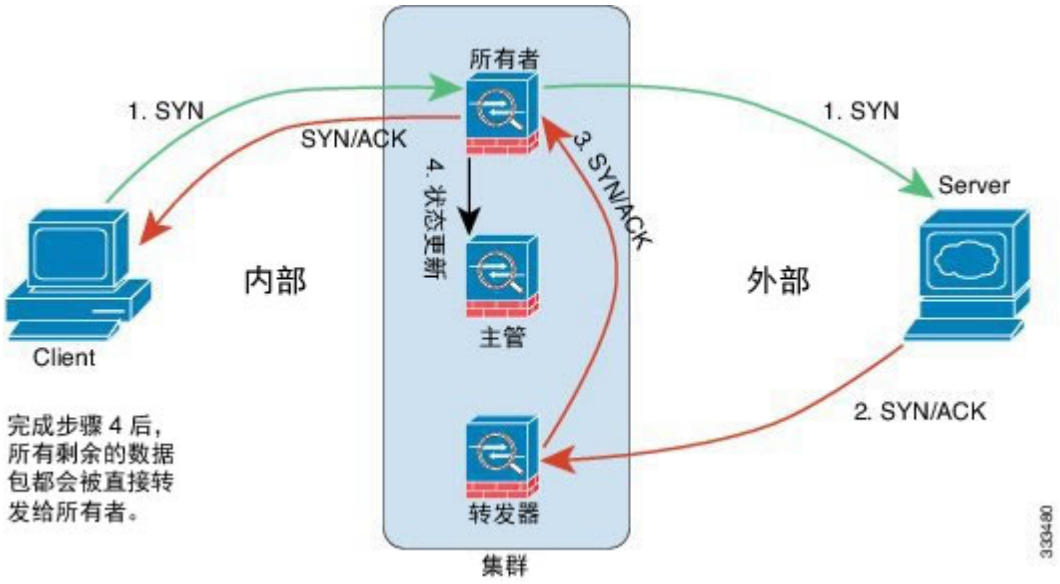
对于机箱间集群，如果流量的导向器与所有者位于同一个机箱中，则系统会选择不同机箱上的其他导向器作为导向器备份，以防所有者的机箱出现故障。如果导向器已位于不同的机箱，则无需额外的导向器。

新连接所有权

通过负载均衡将新连接定向到集群成员时，该连接的两个方向都由此设备所有。如果该连接有任何数据包到达其他设备，这些数据包都会通过集群控制链路被转发到所有者设备。如果反向流量到达其他设备，会被重定向回原始设备。

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 Firepower 威胁防御设备（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 Firepower 威胁防御设备（基于负载均衡方法）。此 Firepower 威胁防御设备 是转发者。
3. 由于转发者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者，然后将 SYN-ACK 数据包转发到客户端。
5. 导向者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。导向者将充当该连接的备用所有者。
6. 传送到转发者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设备，它将向导向者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者发送状态更新。

Firepower 威胁防御功能和集群

有些 Firepower 威胁防御功能在集群中不受支持，有些功能仅在主设备上受支持。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。

- 站点到站点 VPN

- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 高可用性
- 集成路由和桥接

集群集中式功能

以下功能仅在主设备上受支持，不能扩展用于集群。

注释 集中式功能的流量将通过集群控制链路从成员设备转发到主设备。

如果使用重新均衡功能，在将流量归类为集中式功能之前，集中式功能的流量可能会被重新均衡到非主设备；如果出现这种情况，流量接下来会被发回主设备。

对于集中式功能，如果主设备出现故障，所有连接会被丢弃，而您必须在新的主设备上重新建立连接。

- 以下应用检查：

  DCERPC

  NetBIOS

  RSH

  SUNRPC

  TFTP

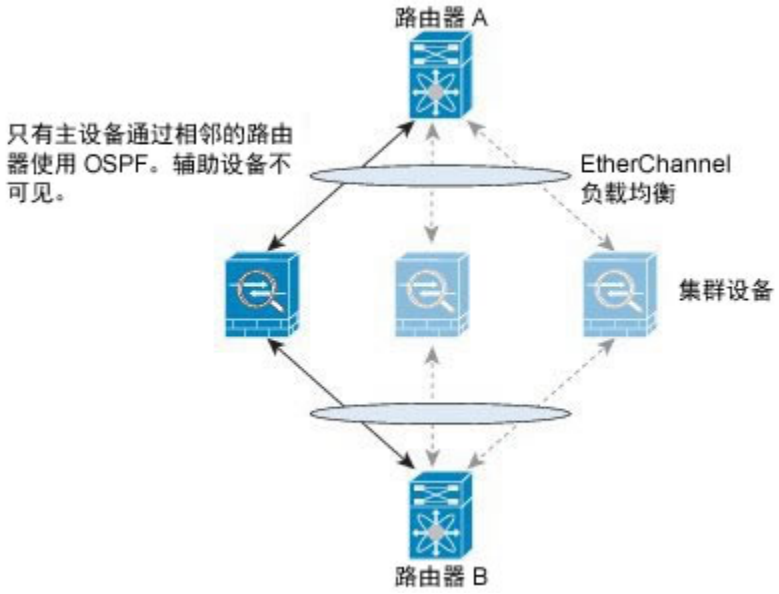
  XDMCP

- 动态路由
- 静态路由监控

动态路由和集群

路由进程仅在主设备上运行，路由通过主设备获知并复制到从属设备。如果路由数据包到达从属设备，会被重定向到主设备。

图 *1*：动态路由



当从属设备成员从主设备获知路由后，每台设备将独立作出转发决策。

OSPF LSA 数据库不会从主设备同步到从属设备。如果发生主设备切换，邻居路由器将检测到重新启动；切换过程不透明。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 无中断转发功能，解决中断问题。

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 Firepower 威胁防御设备，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。当数据包到达并非连接所有者的 Firepower 威胁防御设备 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。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 对动态 PAT 使用 NAT 池地址分配 - 主设备在整个集群中预先平均分配地址。如果成员收到连接却没有剩余的地址，则即使其他成员仍有可用地址，该连接仍会断开。因此，请确保至少包含与集群中的设备数量相同的 NAT 地址，务必让每台设备都收到一个地址。
- 不使用轮询 - 集群不支持 PAT 池轮询。

- 主设备管理的动态 NAT 转换项 - 主设备负责维护转换表并将其复制到从属设备。当从属设备收到需要动态 NAT 的连接而转换项不在表中时，从属设备将向主设备请求该转换项。从属设备是该连接的所有者。
- 对以下检查不使用静态 PAT -

  FTP

  RSH

  SQLNET

  TFTP

  XDMCP

  SIP

SIP 检测和集群

控制流可以在任何设备上创建（由于负载均衡），但其子数据流必须位于同一设备上。

系统日志 和集群

- 集群中的每台设备都会生成自己的系统日志消息。您可以配置日志记录，使每台设备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，集群中的所有设备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，则所有设备生成的系统日志消息都会看似来自一台设备。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设备名称作为设备 ID，系统日志消息就会看似来自不同设备。

SNMP 和集群

SNMP 代理按照诊断接口本地 IP 地址轮询每一台 Firepower 威胁防御设备。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，则当选举出新的主设备时，对新的主设备的轮询将失败。

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。

思科 TrustSec 和集群

只有主设备可获知安全组标签 (SGT) 信息。然后，主设备将向从属设备提供 SGT，从属设备可根据安全策略为 SGT 作出匹配决策。

VPN 和集群

站点到站点 VPN 是一项集中式功能；仅主设备支持 VPN 连接。

VPN 功能仅限于主设备，不会利用集群高可用性功能。如果主设备出现故障，所有现有的 VPN 连接都会丢失，并且 VPN 用户会看到服务中断。在选择新主设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨接口地址时，系统会自动将连接转发到主设备。

与 VPN 相关的密钥和证书将被复制到所有设备。

集群必备条件

机箱间硬件和软件要求

集群中的所有机箱：

- 对于 Firepower 4100 系列：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。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。
- 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网络 EtherChannel 中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。
- 必须使用同一台 NTP 服务器。对于 Firepower 威胁防御，Firepower 管理中心也必须使用同一 NTP 服务器。请勿手动设置时间。

机箱间集群交换机必备条件

- 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列表，请参阅《Cisco FXOS 兼容性》。

面向集群的指导原则

模式

- Firepower 9300 上的 Firepower 威胁防御 - 支持机箱内和机箱间集群。
- Firepower 4100 系列 上的 Firepower 威胁防御 - 支持机箱间集群。
- Radware DefensePro - 支持配备 Firepower 威胁防御的机箱内集群。

机箱间集群的交换机

- 对于 ASR 9006，如果要设置非默认 MTU，请将 ASR 接口 MTU 设置为高于集群设备 MTU 14 个字节。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 ASR *IPv4* MTU 匹配。
- 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。
- 当发现交换机上跨网络 EtherChannel 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。
- 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。切勿更改集群设备上的默认负载均衡算法。
- 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-distributionfixed**

  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。

机箱间集群的 EtherChannel

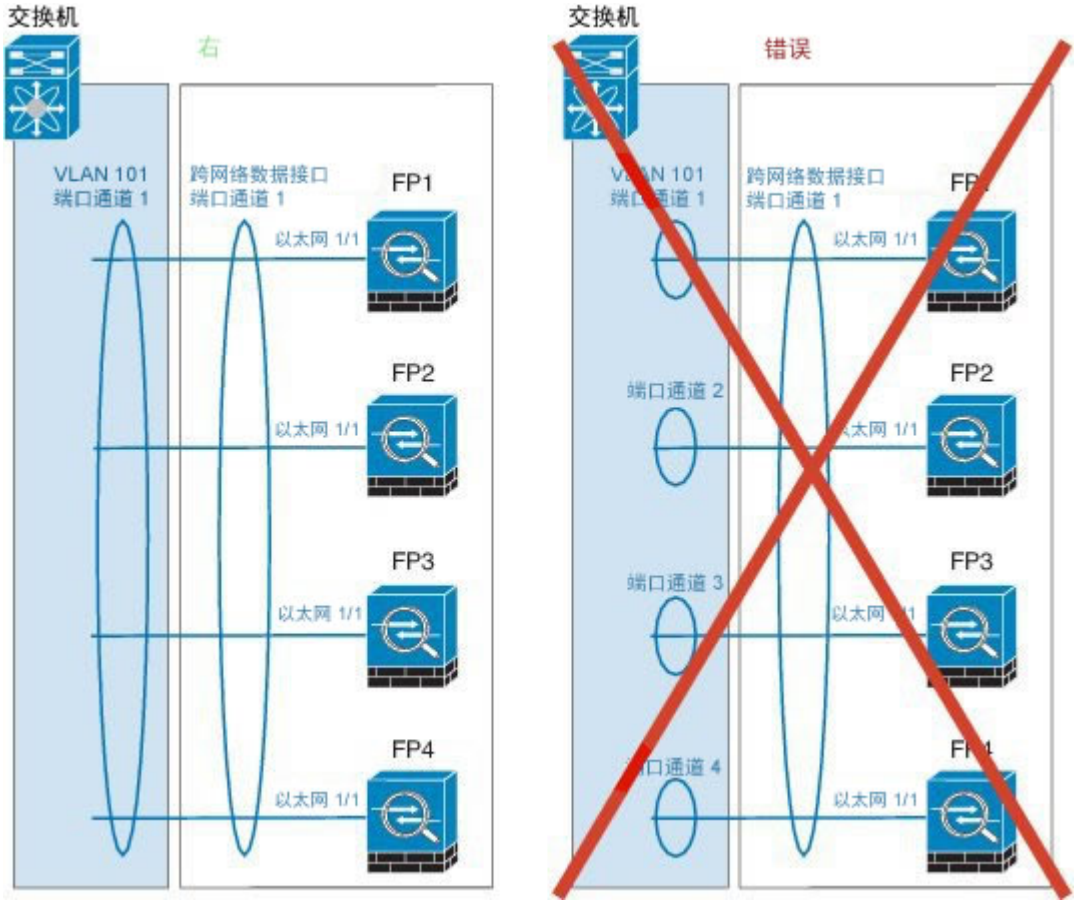
- 为了连接交换机，请将 EtherChannel 模式设置为 Active；Firepower 4100/9300 机箱 不支持 ON 模式，甚至对于集群控制链路也是如此。
- 默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为正常。此设置可能使端口通道成员的捆绑时间超过 30 秒，从而导致集群接口运行状况检查失败，这会让设备从集群中删除。我们建议您在 FXOS CLI 中将 LACP 速率更改为快速。以下示例修改“默认”LACP 策略：

```
firepower# scope org
firepower /org # scope lacppolicy default
firepower /org/lacppolicy# set lacp-rate fast
firepower /org* # commit-buffer
```

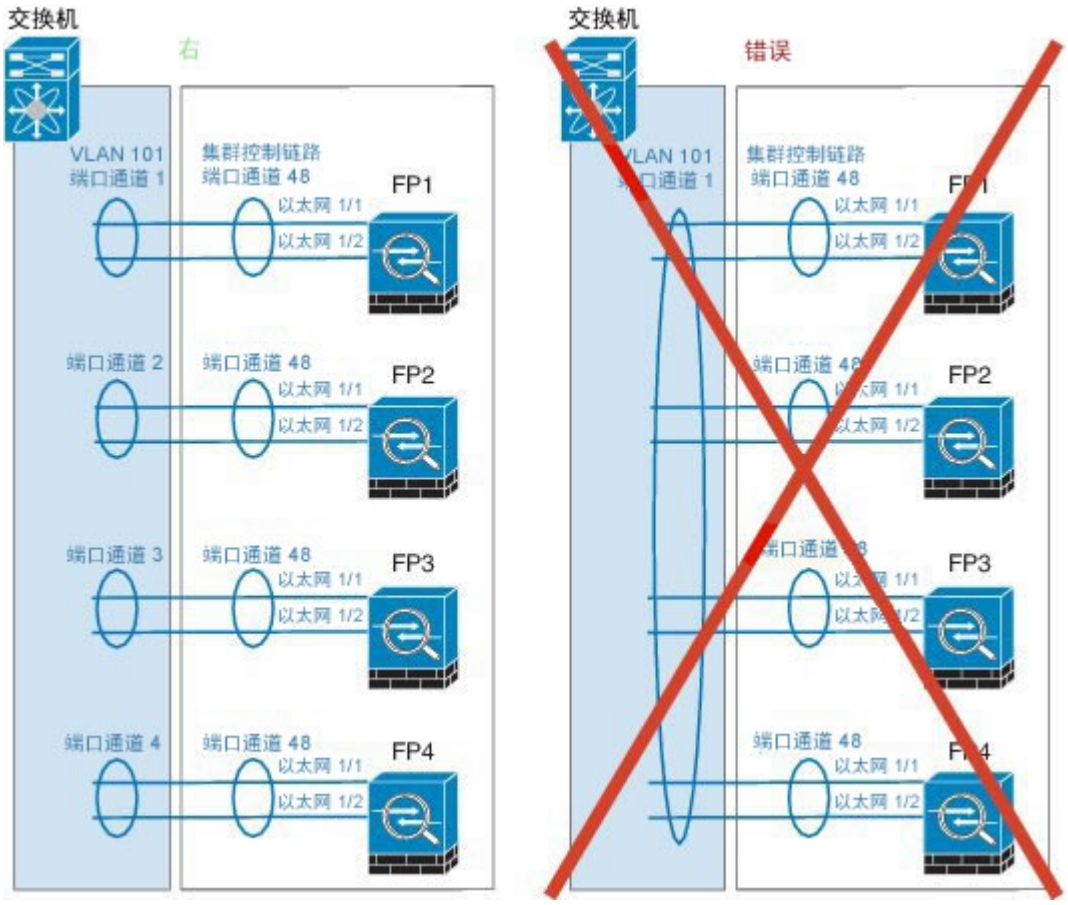
- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接集群设备 EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为一个足够大的值，以考虑重新加载时间；例如，8 分钟或无限接近 0。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨网络 EtherChannel 和设备本地 EtherChannel 适当地配置交换机。

  跨网络 EtherChannel - 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。



其他规定

- 最多可在 6 个机箱中包括多达 6 个模块。
- 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。
- 如果使用连接到跨网络接口的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器不限制 ICMP 错误消息时，会有大量 ICMP 消息被发回集群。这些消息可能导致集群的某些设备 CPU 使用率极高，进而影响性能。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，也不能在独立模式下运行其他安全模块；必须将所有安全模块都包括在集群中，包括空插槽。

Firepower 4100/9300 机箱上的集群默认设置

- 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。

在 Firepower 4100/9300 机箱上配置集群

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。然后，可将设备添加到管理中心，再将它们组合成一个集群。

在 FXOS 机箱管理引擎中部署集群

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。

开始之前

- 您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，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。
- 在**接口 (Interfaces)** 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 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。
部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加同一 EtherChannel。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。
对于机箱间集群，在各机箱上添加相同的“管理 (Management)”接口。

步骤 3 对于机箱间集群，向端口通道 48 添加成员接口，用作集群控制链路。
如果不包含成员接口，那么当您部署逻辑设备时，Firepower 机箱管理器 会认为此集群为机箱内集群，并且不显示**机箱 ID (Chassis ID)** 字段。在各机箱上添加相同的成员接口。

步骤 4 （可选） 添加 Firepower 事件接口。
此接口是 Firepower 威胁防御设备的二级管理接口。要使用此接口，您必须在 Firepower 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 Firepower 威胁防御命令参考中的 **configure network** 命令。

对于机箱间集群，在各机箱上添加相同的事件接口。

步骤 5 选择**逻辑设备 (Logical Devices)** 以打开**逻辑设备 (Logical Devices)** 页面。
逻辑设备 (Logical Devices) 页面显示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 6 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。
如果存在现有逻辑设备，系统会提示您删除该设备并添加新的逻辑设备。设备上的所有配置都将替换为新的信息。

步骤 7 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。Firepower 4100/9300 机箱管理引擎使用此名称来配置集群/管理设置以及分配接口；该名称不是逻辑设备配置中使用的集群名称。

步骤 8 对于**模板 (Template)**，请选择**思科 Firepower 威胁防御 (Cisco Firepower Threat Defense)**。

步骤 9 对于**映像版本 (Image Version)**，请选择 Firepower 威胁防御软件版本。确保此版本与您的 FXOS 版本及 Firepower 管理中心版本兼容。

步骤 10 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。

步骤 11 点击**创建新集群 (Create New Cluster)** 单选按钮。

步骤 12 点击**确定 (OK)**。
如果您配置了任何独立设备，系统将提示您用新集群替代它们。您会看到**调配-设备名称 (Provisioning -** *device name)* 窗口。

默认情况下，所有接口都会分配给集群。具有硬件绕行功能的端口使用以下图标显示：  。如果您未同时分配一个硬件绕行对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件绕行功能，因此如果您愿意，可以分配单个接口。机箱间集群不支持硬件旁路端口，因为不支持将其作为 EtherChannel 成员。

步骤 13 点击屏幕中心的设备图标。
此时将显示**思科 Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration)** 对话框。

步骤 14 在**集群信息 (Cluster Information)** 选项卡上，填写以下字段：

a) 在**机箱 ID (Chassis ID)** 字段中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

b) 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。
共享密钥是长度为 1 到 63 个字符的 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。

c) 设置**集群组名称 (Cluster Group Name)**，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。

d) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。
如果您分配一个支持硬件绕行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。

步骤 15 在**设置 (Settings)** 选项卡上，完成下列操作：

a) 在**注册密钥 (Registration Key)** 字段中，输入注册期间 Firepower 管理中心与集群成员之间要共享的密钥。
b) 在**密码 (Password)** 字段中，输入集群中管理员用户的密码。
c) 在 **Firepower 管理中心 IP (Firepower Management Center IP)** 字段中，输入执行管理的 Firepower 管理中心的 IP 地址。
d) 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。
e) 从**防火墙模式 (Firewall Mode)** 下拉列表中选择**透明 (Transparent)** 或**路由 (Routed)**。
f) 在 **DNS 服务器 (DNS Servers)** 字段中，输入 Firepower 威胁防御设备应在管理网络中使用的 DNS 服务器逗号分隔列表。
g) 在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入 Firepower 威胁防御设备的完全限定名称。
h) 从**事件接口 (Eventing Interface)** 下拉列表中，选择发送 Firepower 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 Firepower 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 硬件绕行功能的接口作为事件接口，则会收到一条警告消息，确认您是故意这样分配的。

步骤 16 在**接口信息 (Interface Information)** 选项卡中，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 IP 地址。
b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
c) 输入**网络网关 (Network Gateway)** 地址。

步骤 17 在**协议 (Agreement)** 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 18 点击**确定 (OK)** 以关闭**思科 Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration)** 对话框。

步骤 19 点击**保存 (Save)**。
Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 20 对于机箱间集群，将下一个机箱添加到集群中：

a) 在第一个机箱 Firepower 机箱管理器上，点击右上角的**显示集群详细信息 (Show Cluster Details)** 图标；复制显示的集群配置。
b) 连接到下一机箱上的 Firepower 机箱管理器，并按照此程序添加逻辑设备。
c) 选择**加入现有集群 (Join an Existing Cluster)**。
d) 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
e) 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。
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 (Chassis ID)** - 输入唯一的机箱 ID。
- **集群密钥 (Cluster Key)** -（未预填充）输入相同的集群密钥。

- **管理 IP (Management 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) 点击 **保存 (Save)**。

步骤 21 使用管理 IP 地址将每台设备单独添加到 Firepower 管理中心，然后在 Web 界面上将它们组成集群。所有集群设备必须在 FXOS 上已成功建立的集群中，然后才可将其添加到 Firepower 管理中心 中。

将集群添加到管理中心

智能许可证	经典许可证	支持的设备	支持的域	访问
任意	不适用	Firepower 4100 和 9300上的 Firepower 威胁防御	任意	访问管理员 管理员 网络管理员

将逻辑设备添加到管理中心，再将它们组合成集群。

开始之前

- 请参阅 Firepower 机箱管理器**逻辑设备 (Logical Devices)** 屏幕，了解哪台设备是主设备。
- 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。

步骤 1 在管理中心中，依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并选择**添加 (Add)** > **添加设备 (Add Device)** 以使用部署该集群时分配的管理 IP 地址将每台设备添加为独立的受管设备。

注释 如果使用管理中心高可用性，请确保备用管理中心也可成功注册每台设备，再在活动管理中心上继续建立集群：登录到备用管理中心可检查每台设备的注册状态。

步骤 2 依次选择**添加 (Add)** > **添加集群 (Add Cluster)** 以将设备组合成集群。

a) 从下拉列表中选择**主 (Primary)** 设备。
所有其他符合条件的成员都会添加到**辅助设备 (Secondary Devices)** 框中。

b) 为集群指定**名称 (Name)**。

c) 点击**确定 (OK)**。
集群对象将被添加到**设备 (Devices)** 屏幕，其下面是成员设备。当前主设备的设备名称后面标有“主 (primary)”。

注释 如果稍后要在 FXOS 机箱上向集群中添加更多设备，必须先将每台设备添加到管理中心，再尽快将它们添加为集群的辅助节点。

步骤 3 要配置设备特定的设置，请点击集群的编辑图标 ( )；只能整体配置集群，而不能配置集群中的成员设备。

步骤 4 在**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 选项卡上，可以查看常规、许可证、系统和运行状况设置。设置许可证授权时，此选项非常有用。在**设备 (Devices)** 选项卡上，只能更改主设备的管理 IP 地址。

步骤 5 （可选） 如果要配置诊断接口，请执行以下步骤：
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) 添加 IPv4 和/或 IPv6 地址池。
b) 点击**接口 (Interfaces)** 选项卡以编辑诊断接口。
c) 在 **IPv4** 选项卡上，输入**虚拟 IP 地址 (Virtual IP Address)** 和掩码。此 IP 地址是集群的固定地址，始终属于当前的主设备。
d) 从 **IPv4 地址池 (IPv4 Address Pool)** 下拉列表中，选择您创建的地址池。
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。
e) 对于**掩码 (Mask)**，请输入集群 IP 池的子网掩码。
f) 在 **IPv6 > 基本 (Basic)** 选项卡的 **IPv6 地址池 (IPv6 Address Pool)** 下拉列表中，选择您创建的地址池。
g) 按正常方式配置其他接口设置。

步骤 6 根据需要配置其他设备级别设置。

步骤 7 点击**保存 (Save)**，然后点击**部署 (Deploy)**。

添加集群成员

智能许可证	经典许可证	支持的设备	支持的域	访问
任意	不适用	Firepower 4100 和 9300上的 Firepower 威胁防御	任意	访问管理员 管理员 网络管理员

可以向现有集群中添加新的集群成员，例如向 Firepower 9300 设备或其他机箱添加更多模块时。

开始之前

当您在 FXOS 机箱上向集群中添加更多设备时，必须将每个设备添加到管理中心，再尽快将它们添加为集群的辅助节点。

步骤 1 在管理中心中，依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并选择**添加 (Add)** > **添加设备 (Add Device)** 以添加新的逻辑设备。

步骤 2 依次选择**添加 (Add)** > **添加集群 (Add Cluster)**。

步骤 3 从下拉列表中选择当前的**主 (Primary)** 设备。
选择已在集群中的主设备时，系统会自动填充现有的集群名称，并且所有符合条件的辅助设备都会添加到**辅助设备 (Secondary Devices)** 框中，包括刚添加到管理中心的新设备。

步骤 4 点击**添加 (Add)**，然后点击**部署 (Deploy)**。
该集群将更新为包括新成员。

删除辅助成员

智能许可证	经典许可证	支持的设备	支持的域	访问
任意	不适用	Firepower 4100 和 9300上的 Firepower 威胁防御	任意	访问管理员 管理员 网络管理员

如果需要删除集群成员（例如，如果删除 Firepower 9300 上的某个模块或删除机箱），应从管理中心中将其删除。 如果根据 Firepower 机箱管理器，该成员仍是集群正常运行的一部分，请勿删除该成员；即便将其从管理中心中删除，它仍会是集群的运行部分，如果该设备变成主设备且管理中心不能再对其管理，则可能会导致出现问题。

步骤 1 在管理中心中，依次选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击辅助设备旁边的垃圾桶。

步骤 2 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。

重新加入集群

智能许可证	经典许可证	支持的设备	支持的域	访问
任意	不适用	Firepower 4100 和 9300上的 Firepower 威胁防御	任意	访问管理员 管理员 网络管理员

如果从集群中删除了某个设备（例如对于出现故障的接口），必须通过访问设备 CLI 手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除设备的原因的更多信息，请参阅重新加入集群，第 6 页。

步骤 1 从控制台端口或使用 SSH 连接到管理接口，访问需要重新加入集群的设备的 CLI。使用用户名 **admin** 和初始设置期间设定的密码登录。

步骤 2 启用集群：
cluster enable

集群历史记录

功能名称	平台版本	功能信息
对 Cisco ASA 进行机箱内集群	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建集群。 我们引入了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
对 6 个 ASA 模块进行机箱间集群	1.1.3	现在，您可以对 ASA 启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
支持在 Firepower 9300 上的 Firepower 威胁防御 上执行机箱内集群	1.1.4	Firepower 9300 支持使用 Firepower 威胁防御 应用执行机箱内集群。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	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)**

功能名称	平台版本	功能信息
对 6 个 Firepower 威胁防御 模块进行机箱间集群	2.1.1	现在，您可以对 Firepower 威胁防御启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**