Firepower 4100/9300 的 ASA 集群

通过集群，您可以将多台Firepower 4100/9300 机箱 ASA 组合成单个逻辑设备。Firepower 4100/9300 机箱 系列包括 Firepower 9300 和 Firepower 4100 系列。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 74 页。

关于 Firepower 4100/9300 机箱上的集群

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

- 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）。

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

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

- 在应用中创建集群引导程序配置。

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

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

注释 除管理接口以外，不支持独立接口。

- 向集群中的所有设备分配管理接口。

有关集群的详细信息，请参阅以下各节：

引导程序配置

在部署集群时，Firepower 4100/9300 机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。 如果您需要自定义集群环境，则用户可以配置引导程序配置的某些部分。

集群成员

集群成员协调工作来实现安全策略和流量的共享。

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

您必须仅在控制设备上执行所有配置；然后，配置将复制到数据设备。

有些功能在集群中无法扩展，控制设备将处理这些功能的所有流量。请参阅集群集中化功能，第 75 页。

集群控制链路

集群控制链路是用于设备到设备通信的 EtherChannel（端口通道 48）。对于机箱内集群，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 Firepower 4100/9300 机箱 上的此 EtherChannel 以进行机箱间通信。

对于有 2 个机箱的机箱间集群，请勿将集群控制链路从一机箱直接连接至另一机箱。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。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

有关集群控制链路的详细信息，请参阅以下部分。

确定集群控制链路规格

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

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

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 用于网络访问的 AAA 是集中功能，因此所有流量都会转发到控制设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

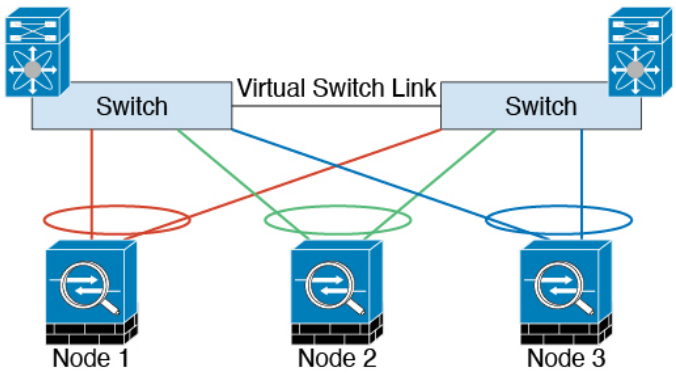
带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

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

集群控制链路冗余

我们建议将 EtherChannel 用于集群控制链路，以便在 EtherChannel 中的多条链路上传输流量，同时又仍能实现冗余。

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



机箱间集群的集群控制链路可靠性

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

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

集群控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。当您部署集群时，您可以自定义此 IP 地址。集群控制链路网络不能包括设备之间的任何路由器；仅可执行第 2 层交换。 对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

集群接口

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

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

除管理接口以外，不支持独立接口。

连接到冗余交换机系统

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

配置复制

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

Cisco Secure Firewall ASA集群管理

使用 ASA集群的一个好处可以简化管理。本节介绍如何管理集群。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

必须为集群分配管理类型的接口。此接口是与跨网络接口相对立的一种特殊接口。通过管理接口，可以直接连接到每个设备。

集群的主集群 IP 地址是集群的固定地址，始终属于当前的控制单元。您也可以配置一个地址范围，使每个设备（包括当前控制单元在内）都能使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。

例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制设备。要管理单个成员，您可以连接到本地 IP 地址。

注释 传入设备的流量必须指向节点的管理 IP 地址；传入设备的流量不会通过群集控制链路转发到任何其他节点。

对于 TFTP 或系统日志等出站管理流量，包括控制设备在内的每台设备都使用本地 IP 地址连接到服务器。

控制设备管理与数据设备管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

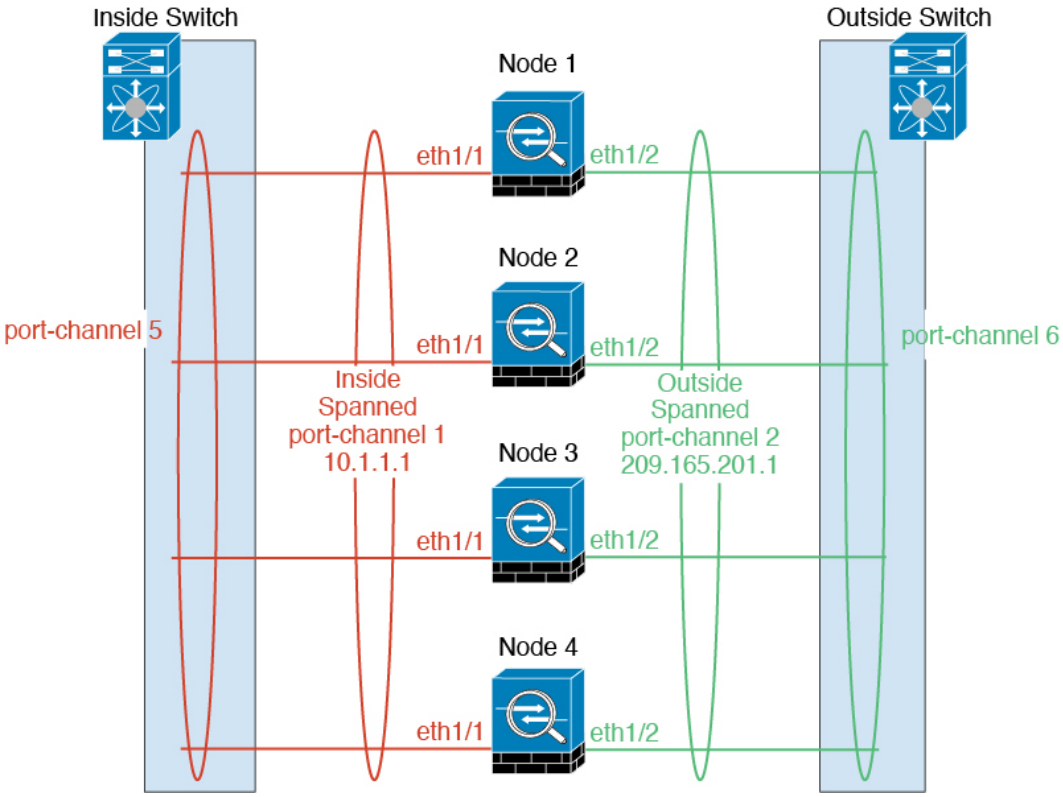
默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

跨网络 EtherChannel（推荐）

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。



站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥 ASA 集群的优势。

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。

有关站点间集群的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - Firepower 4100/9300 机箱上的集群要求和前提条件， 第 7 页
- 站点间准则 - 集群准则和限制， 第 10 页
- 配置集群流移动性 -配置集群流移动性， 第 38 页
- 启用导向器本地化 - 启用导向器本地化， 第 36 页
- 启用站点冗余 - 启用导向器本地化， 第 36 页

Firepower 4100/9300 机箱上的集群要求和前提条件

每个模型的最大集群单位

- Firepower 4100 机箱 — 16 机箱
- Firepower 9300 — 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。

机箱间集群的硬件和软件要求

集群中的所有机箱：

- 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。
- 除进行映像升级外，必须运行完全相同的 FXOS 和应用软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据

接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。 请注意，如果您要删除 FXOS 中的接口，ASA 配置将保留相关命令，以便您可以进行任何必要的调整；从配置中删除接口可能具有广泛影响。您可以手动删除旧的接口配置。

- 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 防火墙威胁防御，所有许可由防火墙管理中心处理。

交换机要求

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

调整站点间集群的数据中心互联

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)）。

集群许可证 Firepower 4100/9300 机箱

智能软件管理器常规版和本地版

集群功能本身不需要任何许可证。要使用强加密和其他可选许可证，每个 Firepower 4100/9300 机箱都必须注册到许可证颁发机构或智能软件管理器常规版和本地版中。数据设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，两个设备都可以使用标准许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 10 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 集群中有 6 个 Firepower 9300 模块。基础许可证包括 10 个情景；对于 6 台设备，这些许可证相加之和为 60 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括 80 个情景。由于一个模块的平台限制为 250，因此聚合后的许可证最多允许 250 个情景；80 个情景没有超出此限制。因此，您可以在控制设备上配置最多 80 个情景；每台数据设备通过配置复制也将拥有 80 个情景。
  - 集群中有 3 台 Firepower 4112 设备。基础许可证包括 10 个情景；对于 3 台设备，这些许可证相加之和为 30 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的集群许可证包括 280 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；280 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 220 个情景。
- 运营商 - 分布式站点间 VPN 所需。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

- 强加密 (3DES) - 对于 2.3.0 前 Cisco Software Manager 本地部署；或如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新的主用设备每12小时发送一次权利授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

集群准则和限制

集群的交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **src-dst-mixed-ip-port**（请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。请勿 更改集群设备上默认的负载均衡算法。
- 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-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。

- 与 ASA 硬件集群不同，Firepower 4100/9300 集群支持 LACP 正常融合。因此， 对于平台， 您可以在连接的 Cisco Nexus 交换机上启用 LACP 正常融合。

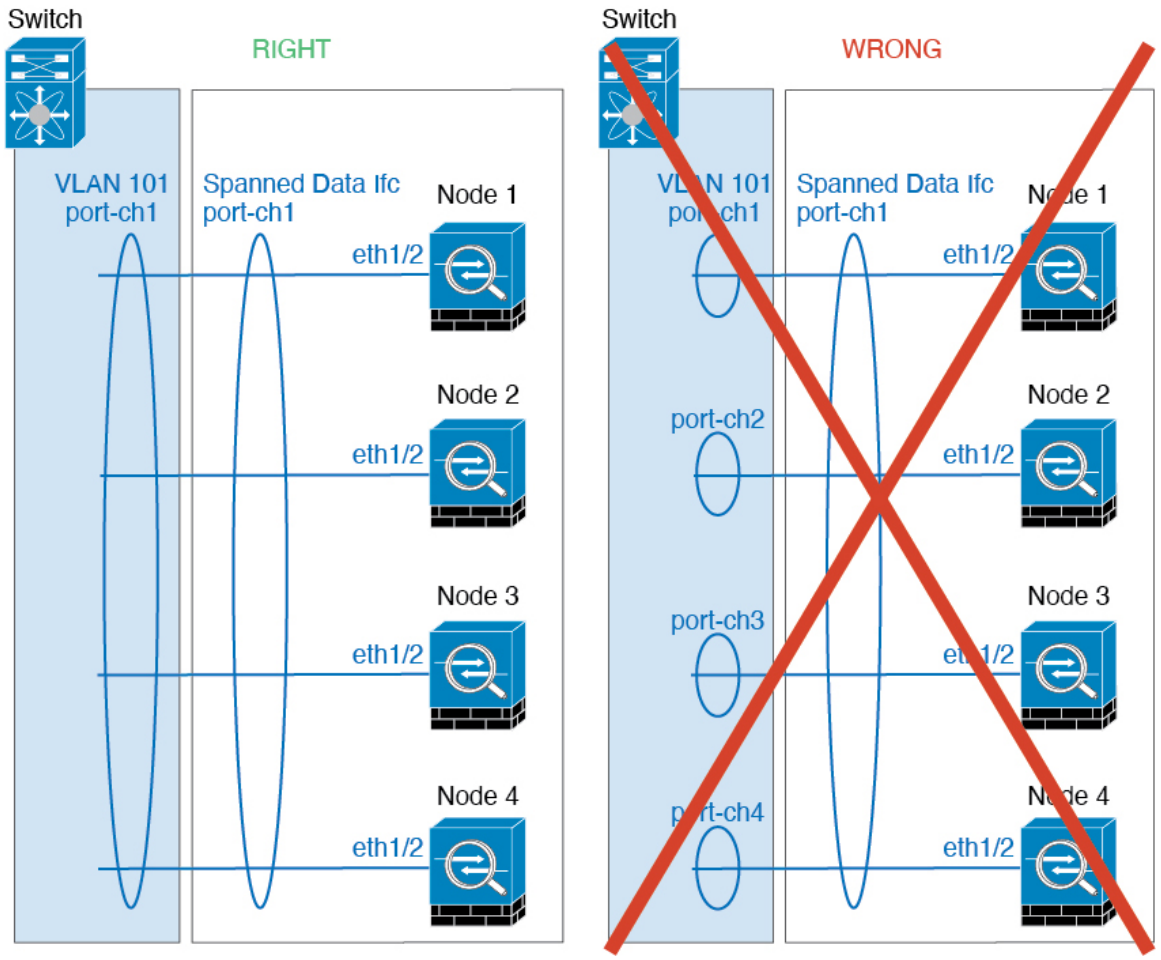
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

集群的 EtherChannel

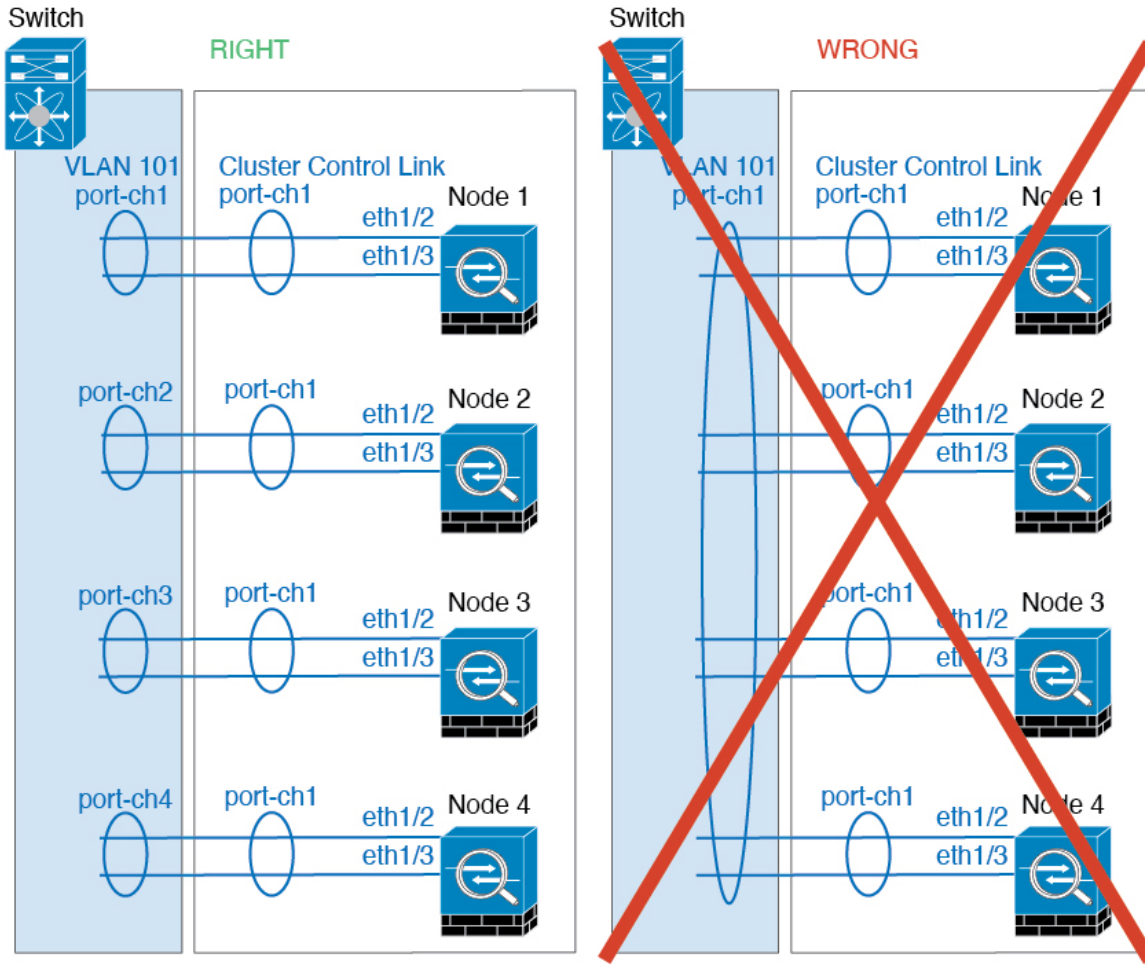
- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。

  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



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



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。
- ASA 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

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。
- 对于南北部署中的UDP长期流，如果原流所有者站点的节点出现故障，然后又恢复正常，那么流就会被引导回原站点，从而出现路由循环。如果另一个站点的新所有者没有通往目的地的路由，它就会将流路由回互联网，从而导致环路。在这种情况下，请对新的所有者使用 **clear conn** 命令强制重新建立流。
- 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，则您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 ASA 上将路由器 HSRP MAC 地址添加为静态 MAC 地址表条目（请参阅 为网桥组添加静态 MAC 地址）。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，ASA MAC 地址表通常仅在 HSRP IP 地址的 ASA ARP 表条目到期时更新，并且 ASA 发送 ARP 请求并接收应答。由于 ASA 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地址表到期流量丢弃。
- 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，则您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。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firepower 4100/9300 机箱 或交换机上的接口、添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。在某些情况下，丢弃的数据包可能会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包会使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。

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

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。
- 默认情况下，连接再均衡处于禁用状态。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。
- 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。本节介绍可在 ASA 上执行的默认引导程序配置和可选定制。本节还将介绍如何从 ASA 中管理集群成员。您还可以通过 Firepower 4100/9300 机箱管理集群成员关系。有关详细信息，请参阅 Firepower 4100/9300 机箱文档。

过程

步骤 1 FXOS：添加 ASA 集群，第 16 页
步骤 2 ASA：配置防火墙模式和情景模式，第 26 页
步骤 3 ASA：配置数据接口，第 26 页
步骤 4 ASA：自定义集群配置，第 29 页
步骤 5 ASA：管理集群成员，第 50 页

FXOS：添加 ASA 集群

您可以将单个 Firepower 9300 机箱添加为机箱内集群，或添加多个机箱以实现机箱间集群。 对于机箱间集群，您必须单独配置每个机箱。在一个机箱上添加集群；然后，您可以在下一个机箱上输入基本相同的设置。

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。

对于多机箱集群，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）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。

在部署集群时，Firepower 4100/9300 机箱管理引擎将使用以下引导程序配置对每个 ASA 应用进行配置。以后如果需要，可以通过 ASA 修改引导程序配置的组成部分（以**粗体**文字显示）。

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

注释　如果禁用集群，则只能更改 **local-unit** 名称。

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。

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

对于多机箱集群，所有数据接口必须为至少带有一个成员接口的跨区以太网通道。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 10 页。

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

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

对于多机箱集群，在各机箱上添加相同的管理接口。

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

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

在各机箱上添加相同的成员接口。　集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 10 页。

步骤 2 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 3 设置应用实例参数，包括映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
```

```
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为映像版本。

scope app asa *application_version*

示例：

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) 将此版本设置为默认版本。

set-default

示例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

步骤 4 创建集群。

enter logical-device *device_name* **asa** *slots* **clustered**

- *Device_name* - 由 Firepower 4100/9300 机箱管理引擎用于配置集群设置以及分配接口；它不是在安全模块配置中使用的集群名称。必须指定全部三个安全模块，即使尚未安装硬件也是如此。
- *slots* - 将机箱模块分配给集群。对于 Firepower 4100，指定 **1**。对于 Firepower 9300，指定 **1,2,3**。您必须启用对 Firepower 9300 机箱中全部 3 个模块插槽的启用集群，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。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

步骤 5 配置集群引导程序参数。

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。

a) 创建集群引导程序对象。

enter cluster-bootstrap

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) 设置机箱 ID。

set chassis-id *id*

集群中的每个机箱都需要唯一 ID。

c) 对于站点间集群，请将站点 ID 设置为 1 到 8 之间的值。

set site-id *number*。

要删除站点 ID，请将值设为 **0**。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) 为集群控制链路上的控制流量配置身份验证密钥。

set key

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

系统将提示您输入共享密钥。

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) 设置集群接口模式。

set mode spanned-etherchannel

跨区以太网通道模式是唯一支持的模式。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) 在安全模块配置中设置集群组名称。

set service-type *cluster_name*

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （可选） 设置　集群控制链路 IP 网络。

set cluster-control-link network *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，您可以对集群指定唯一网络上的 /16 地址。

- *a*.*b*.**0.0** - 指定任意 /16 网络地址，环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外。如果将该值设置为 0.0.0.0，则使用默认网络：127.2.0.0。

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*。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

h) 配置管理 IP 地址信息。

此信息用于配置安全模块配置中的管理接口。

1. 配置本地 IP 地址池，其中一个地址将被分配到接口的每个集群设备。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   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。

2. 为管理接口配置主集群 IP 地址。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   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。

3. 输入网络网关地址。

set ipv4 gateway *ip_address*

set ipv6 gateway *ip_address*

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) 退出集群引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

步骤 6 配置管理引导程序参数。

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。

a) 创建管理引导程序对象。

enter mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

预配置的 ASA 管理员用户和启用密码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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 7 保存配置。

commit-buffer

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。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
```

```
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ ---------------- ------------
ftd        cluster1   1          Enabled     Online           7.3.0.49        7.3.0.49
    Native                    In Cluster      Data Node
ftd        cluster1   2          Enabled     Online           7.3.0.49        7.3.0.49
    Native                    In Cluster      Control Node
ftd        cluster1   3          Disabled    Not Available                    7.3.0.49
    Native                    Not Applicable  None
```

步骤 8 要向集群添加其他机箱，请重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**；否则，请对两个机箱使用同一配置。

请确保新机箱上的接口配置相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

步骤 9 连接到控制设备 ASA 以自定义集群配置。

示例

对于机箱 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
```

```
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

对于机箱 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
```

```
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

添加更多集群成员

添加或替换 ASA 集群成员。

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集群的Firepower 9300，则该模块将自动添加。

开始之前

- 确保现有集群在此新成员的管理 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集群引导程序配置，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，在第一个集群成员上的ASA应用中启用多情景模式；其他集群成员将自动继承多情景模式配置。

过程

步骤 1 确定。

步骤 2 要向集群添加其他机箱，请在创建 ASA 集群，第 16 页中重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**；否则，请对两个机箱使用同一配置。

ASA：配置防火墙模式和情景模式

默认情况下，FXOS 机箱在路由防火墙模式和单情景模式下部署集群。

- 更改防火墙模式 - 要在部署后更改模式，请更改控制设备上的模式；数据设备上的模式将自动更改以实现匹配。请参阅设置防火墙模式。在多情景模式下，应逐个情景设置防火墙模式。
- 更改为多情景模式 - 要在部署后更改为多情景模式，请更改控制设备上的模式；数据设备上的模式将自动更改以实现匹配。请参阅启用多情景模式。

ASA：配置数据接口

此程序配置您在 FXOS 中部署集群时为其分配的每个数据接口的基本参数。对于多机箱集群，数据接口始终是跨区以太网通道接口。

注释 管理接口在您部署集群时预先配置。您还可以在ASA中更改管理接口参数，但此程序侧重于数据接口。管理接口是一个单独的接口，而不是跨网络接口。有关详细信息，请参阅管理接口，第 5 页。

开始之前

- 对于多情景模式，请在系统执行空间中开始本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。
- 对于透明模式，请配置网桥组。请参阅配置网桥虚拟接口 (BVI)。
- 在将跨区以太网通道用于具有多机箱的集群时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的节点。

过程

步骤 1 指定接口 ID。

interface *id*

有关分配给此集群的接口，请参考 FXOS 机箱。接口 ID 可以是：

- **port-channel** *integer*
- **ethernet** *slot/port*

示例：

```
ciscoasa(config)# interface port-channel 1
```

步骤 2 启用接口：

no shutdown

步骤 3 （可选）如果准备在此接口上创建 VLAN 子接口，请立即执行此操作。

示例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

本程序的其余部分适用于子接口。

步骤 4 （多情景模式下）将接口分配到情景，然后使用 changeto 命令进入情景和接口模式。

示例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

对于多情景模式，其余的接口配置将在每个情景中完成。

步骤 5 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 6 根据防火墙模式，执行以下其中一项操作。

- 路由模式 - 设置 IPv4 和/或 IPv6 地址：

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

示例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

不支持 DHCP、PPPoE 和 IPv6 自动配置。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在此情况下，不会为网络或广播地址保留 IP 地址。也不支持手动配置链路本地地址。

- 透明模式 - 将接口分配到网桥组：

  bridge-group *number*

  示例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number 为 1 到 100 之间的整数。最多可将 64 个接口分配到网桥组。您不能将同一接口分配至多个网桥组。请注意，BVI 配置包含 IP 地址。

步骤 7 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

步骤 8 （多机箱集群）为跨区以太网通道配置全局 MAC 地址，以避免潜在的网络连接问题。

mac-address *mac_address*

- *Mac_address* - 采用 H.H.H 格式的 MAC 地址，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

您必须配置网络中当前未使用的唯一 MAC 地址。如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的 MAC 地址用于该接口，而这可能导致临时网络故障。

在多情景模式下，如果您在情景之间共享接口，则应改为启用自动生成 MAC 地址，这样就无需手动设置 MAC 地址。请注意，您必须使用此命令为非共享 接口手动配置 MAC 地址。

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

步骤 9 （站点间集群）为每个站点配置一个站点特定的 MAC 地址和 IP 地址（对于路由模式）：

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

示例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

站点特定的 IP 地址必须与全局 IP 地址位于同一子网。供设备使用的站点特定的 MAC 地址和 IP 地址取决于您在每台设备的引导程序配置中指定的站点 ID。

ASA：自定义集群配置

如果您在部署集群或配置其他选项（例如集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化）后想要更改引导程序设置，您可以在控制设备上执行此操作。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

开始之前

- 对于多情景模式，请在控制单元的系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入 **changeto system** 命令。
- 本地设备 name 和多个其他选项只能在 FXOS 机箱上设置，或者只能在禁用集群的情况下才能在 ASA 上进行更改，因此以下程序未包括这些选项。

过程

步骤 1 确认此设备是控制单元：

show cluster info

示例：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state CONTROL_NODE
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
```

```
Unit "unit-1-3" in state DATA_NODE
    ID        : 4
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.1.3
    CCL MAC   : 0015.c500.018f
    Last join : 20:29:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-1-1" in state DATA_NODE
    ID        : 1
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.1.1
    CCL MAC   : 0015.c500.017f
    Last join : 20:20:53 UTC Nov 4 2015
    Last leave: 20:18:15 UTC Nov 4 2015
Unit "unit-2-1" in state DATA_NODE
    ID        : 3
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.2.1
    CCL MAC   : 0015.c500.020f
    Last join : 20:19:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
```

如果其他设备才是控制设备，请退出当前连接，并连接到正确的设备。

步骤 2 指定集群控制链路接口的最大传输单位至少比数据接口的最高 MTU 高 100 字节。

mtu cluster 字节

示例：

```
ciscoasa(config)# mtu cluster 9184
```

我们建议将 MTU 设置为最大；最小值为 1400 个字节。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。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。例如，由于最大 MTU 为 9184，因此最高的数据接口 MTU 可以是 9084，而集群控制链路则可以设置为 9184。

步骤 3 进入集群配置模式：

cluster group *name*

步骤 4 （可选） 启用数据单元到控制单元的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据设备会将控制台消息发送到控制设备，因此您只需要监控集群的一个控制台端口。

步骤 5 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical** - 重要事件（严重性=1）
- **warning** - 警告（严重性 = 2）
- **informational** - 信息事件（严重性=3）
- **debug** - 调试事件（严重性=4）

步骤 6 （可选）（仅限 Firepower 9300）确保机箱中的安全模块同时加入集群，以便在模块之间均匀分配流量。如果某个模块先于其他模块很早加入，它可能会收到超过所需的流量，因为其他模块还无法分担负载。

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units*- - 指定在模块可加入集群之前同一机箱中需要就绪的最小模块数（介于 1 到 3 之间）。默认值为 1，这意味着模块在加入集群之前不会等待其他模块准备就绪。例如，如果将值设置为3，则每个模块将会等待*max_delay_time*或者直到全部3个模块都就绪后才加入集群。所有 3 个模块将大致同时请求加入集群，并几乎同时开始接收流量。
- *max_delay_time* - 指定在某个模块停止等待其他模块就绪后才加入集群之前的最大延迟时间（以秒为单位），范围介于 0 到 30 分钟之间。默认值为 0，这意味着模块在加入集群之前不会等待其他模块准备就绪。如果将 *num_of_units* 设置为 1，则该值必须为 0。如果将 *num_of_units* 设置为 2 或 3，则该值必须为 1 或更大值。此计时器按模块执行，但当第一个模块加入集群时，则所有其他模块计时器将会结束，并且其余模块也会加入集群。

例如，您将 *num_of_units* 设置为 3，并将 *max_delay_time* 设置为 5 分钟。当模块 1 启动时，会开始其 5 分钟计时器。模块 2 在 2 分钟后启动，并启动其 5 分钟计时器。模块 3 在 1 分钟后启动，因此所有模块现在将在 4 分钟时加入集群；它们不会等待计时器完成。如果模块 3 一直没有启动，则模块 1 将在 5 分钟计时器结束时加入集群，模块 2 也会加入，尽管其计时器还剩余 2 分钟；它不会等待其计时器完成。

步骤 7 配置最大集群成员数。

cluster-member-limit 编号

- *number* - 2 到 16。默认值为 16。

如果您明确知道集群中的设备数少于最大设备数（即16台），建议您设置实际计划的设备数。设置最大单位可让集群更好地管理资源。例如，如果您使用端口地址翻译 (PAT)，则控制设备可以将端口块分配给计划的成员数，并且不必为您不打算使用的额外设备预留端口。

步骤 8 设置从流所有者到导向器和备份所有者的流状态刷新消息（clu_keepalive 和 clu_update 消息）的保持连接间隔。

clu-keepalive-interval 秒

- 秒 - 15 到 55。默认值为 15。

您可能想将间隔设置为比默认值更长的时间，以减少集群控制链路上的流量。

配置运行状态监控并自动重新加入设置

此程序可以配置设备和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。您可以监控任何端口通道ID或单一物理接口ID。运行状况监控不在VLAN子接口或虚拟接口（例如，VNI或BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 自定义集群设备运行状态检查功能：

health-check [**holdtime** *timeout*]

holdime 用于确定两次设备 heartbeat 状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。

为了确定设备运行状况，ASA 集群设备会在集群控制链路上将 heartbeat 消息发送到其他设备。如果设备在保持期内未接收到来自对等设备的任何heartbeat消息，则对等设备被视为无响应或无法工作。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、Firepower 4100/9300 机箱 或交换机上的接口、或者添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能 (**no health-check monitor-interface**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状态检查：

no health-check monitor-interface [*interface_id* | **service-application**]

接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定设备上发生故障，但在其他设备上的同一逻辑接口下仍有活动端口，则会从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于接口的类型以及该设备是既定成员还是正在加入集群的设备。

默认情况下，为所有接口启用运行状况检查。您可以使用此命令的 **no** 形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。指定 **service-application** 以禁用对修饰器应用程序的监控。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、Firepower 4100/9300 机箱 或交换机上的接口、或者添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能 (**no health-check**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

步骤 4 自定义在运行状态检查发生故障后的自动重新加入集群设置：

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。设备尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- *Auto_rejoin_interval_variation* - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。对于集群接口，默认值为 **1**；对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 设置机箱重新加入，以匹配机箱心跳故障的 **health-check system auto-rejoin** 命令。

health-check chassis-heartbeat-delay-rejoin

默认情况下，如果机箱心跳失败然后恢复，则节点会立即重新加入集群。但是，如果配置 **health-check chassis-heartbeat-delay-rejoin** 命令，则它将根据 **health-check system auto-rejoin** 命令的设置重新加入。

步骤 6 配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。 对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群上的接口仅仅因为另一个集群设备在绑定端口时的速度更快便显示为故障状态。

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

步骤 7 配置机箱运行状况检查间隔：

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms* - 设置检测信号之间的时间量，介于 100 和 6000 毫秒之间（100 的倍数）。默认值为 1000 毫秒。
- **retry-count** *Number* - 设置重试次数，介于 1 和 30 之间。默认值为 3 次重试。

ASA 将会检查其能否通过背板与主机机箱通信。

最小组合时间（间隔x重试计数）不能小于 600 毫秒。例如，如果将时间间隔设置为 100，将重试次数设置为 3，则总合并时间为 300 毫秒，这是不受支持的。例如，您可以将间隔设置为 100，将重试计数设置为 6 以满足最短时间（600 毫秒）。

示例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 1000 retry-count 10
```

步骤 8 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的设备可以处理负载，您可以选择在设备上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。例如，对于每个机箱中具有 3 个安全模块的 Firepower 9300 上的机箱间集群，如果机箱中的 2 个安全模块离开集群，则与该机箱的相同数量的流量将被发送到剩余的模块，并可能压垮它。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用设备上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
```

```
1           0           0           13              27
```

配置连接再均衡和集群 TCP 复制延迟

可以配置连接再均衡。 您可以为 TCP 连接启用集群复制中继，以延迟导向器/备份流的创建，从而帮助消除与短期流量相关的“不必要的工作”。请注意，如果某个设备在创建导向器/备份数据流前出现故障，则无法恢复这些数据流。同样，如果流量在创建数据流前再均衡到其他设备，则无法恢复该数据流。您不应为禁用了 TCP 随机化的流量启用 TCP 复制中继。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选）为 TCP 流量启用连接再均衡：

conn-rebalance [**frequency** *seconds*]

示例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

此命令默认禁用。如果启用，ASA 会定期交换有关每秒连接数的信息，并将新连接从每秒连接数较多的设备分流到负载较低的设备。现有连接永远不会移动。此外，由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。此频率的值为 1 到 360 秒，用于指定多长时间交换一次负载信息。默认值为 5 秒。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

步骤 3 为 TCP 连接启用集群复制延迟：

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

示例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

将 *seconds* 设置为介于 1 到 15 之间的值。默认启用 **http** 延迟，时间为 5 秒。

配置站点间功能

对于站点间集群，您可以自定义配置，以提高冗余性和稳定性。

启用导向器本地化

为了提高性能并缩短数据中心的站点间集群的往返时间延迟，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。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。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。

开始之前

- 在Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。
- 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。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用导向器本地化：

director-localization

启用站点冗余

为保护流量免受站点故障的影响，您可以启用站点冗余。如果连接的备份所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备份所有者来保护流量免受站点故障的影响。

开始之前

- 在Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用站点冗余。

site-redundancy

配置每站点免费 ARP

ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。

当使用来自集群的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，集群接收的数据包使用全局 MAC 地址和 IP 地址。如果流量不是定期从全局 MAC 地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。

当您为每台设备设置站点 ID 和为每个跨区以太网通道设置站点 MAC 地址时，默认情况下会启用 GARP。您可以自定义 GARP 间隔，也可以禁用 GARP。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。
- 在控制设备配置中为跨区以太网通道设置每站点 MAC 地址。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 自定义 GARP 间隔。

site-periodic-garp interval 秒

- *seconds* — 设置 GARP 生成之间的时间（以秒为单位），介于 1 到 1000000 秒之间。默认值为 290 秒。

要禁用 GARP，请输入 **no site-periodic-garp interval**。

示例：

```
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

配置集群流移动性

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

关于 *LISP* 检测

可以检查 LISP 流量，以便在站点间启用流移动性。

关于 LISP

利用数据中心的虚拟机移动性（例如，VMware VMotion），服务器可以在数据中心之间迁移，同时维持与客户端的连接。为了支持此类数据中心服务器移动性，路由器需要能够在服务器移动时更新通往服务器的入口路由。思科定位/ID 分离协议 (LISP) 架构将设备身份或终端标识符 (EID) 与设备位置或路由定位符 (RLOC) 分离开，并分隔到两个不同的编号空间，实现服务器迁移对客户端的透明化。例如，当服务器迁移到新的站点并且客户端向服务器发送流量时，路由器会将流量重定向到新位置。

LISP 需要充当特定角色的路由器和服务器，例如 LISP 出口隧道路由器 (ETR)、入口隧道路由器 (ITR)、第一跳路由器、映射解析器 (MR) 和映射服务器 (MS)。当服务器的第一跳路由器检测到服务器连接了其他路由器时，它会更新所有其他路由器和数据库，以便连接到客户端的 ITR 可以拦截、封装流量并将流量发送到新的服务器位置。

Cisco Secure Firewall ASA LISP 支持

ASA 本身不运行 LISP；但是，它可以通过检查 LISP 流量确定位置更改，然后使用此信息进行无缝集群操作。如果不使用 LISP 集成，当服务器移动到新站点时，流量将到达位于新站点的 ASA 集群成员，而不是原始的流所有者。新 ASA将流量转发到旧站点的 ASA，然后旧 ASA必须将流量发回新站点，才能到达服务器。此类流量流并未处于最佳状态，称为“长号”或“发夹”。

如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

LISP 准则

- ASA 集群成员必须位于第一跳路由器和该站点的 ITR 或 ETR 之间。ASA 集群本身不能作为扩展网段的第一跳路由器。

- 仅支持全分布数据流；集中数据流、半分布数据流或属于单个节点的数据流不会移动到新的所有者。半分布数据流包括应用（例如 SIP），其中作为父数据流所有者的同一 ASA 拥有所有子数据流。
- 集群仅移动第 3 和第 4 层流状态；一些应用数据可能丢失。
- 对于持续时间极短的数据流或非关键业务数据流，移动所有者可能并非最佳选择。在配置检查策略时，您可以控制该功能支持的流量类型，并应只对必要流量限制流移动性。

ASA LISP 实施

此功能包含多种相互关联的配置（本章将逐一说明）：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。
2. LISP 流量检查 - ASA 检查 UDP 端口 4342 上的 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个将 EID 和站点 ID 相关联的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。请注意，没有为 LISP 流量分配导向器，并且 LISP 流量本身不参与集群状态共享。
3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。
4. 站点 ID - ASA 使用集群中每个节点的站点 ID 确定新的所有者。
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。

配置 *LISP* 检测

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

开始之前

- 在 Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。
- LISP 流量未包含在 default-inspection-traffic 类中，因此，您在此过程中必须为 LISP 流量配置单独的类。

过程

步骤 1 （可选） 配置 LISP 检测映射以根据 IP 地址限制检测的 EID，并配置 LISP 预共享密钥：

a) 创建扩展 ACL；仅目标 IP 地址与 EID 嵌入式地址匹配：

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 创建 LISP 检测映射，并进入参数模式：

policy-map type inspect lisp *inspect_map_name*

parameters

c) 通过识别您创建的 ACL 定义允许的 EID：

allowed-eid access-list *eid_acl_name*

第一跳路由器或 ITR/ETR 可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。

d) 如果需要，请输入预共享密钥：

validate-key 密钥

示例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

步骤 2 在端口 4342 上为第一跳路由器与 ITR 或ETR 之间的 UDP 流量配置 LISP检测：

a) 配置扩展 ACL 以识别 LISP 流量：

access list *eid_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

您必须 指定 UDP 端口 4342。接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 为 ACL 创建类映射：

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 使用可选 LISP 检测映射指定策略映射、类映射以及启用检测，然后将服务策略应用于接口（如果为新接口）：

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

如果您有现有服务策略，请指定现有策略映射名称。默认情况下，ASA 包括称为 **global_policy** 的全局策略，因此对于全局策略，请指定该名称。如果您希望全局应用该策略，还可以为每个接口创建一个服务策略。LISP 检测会双向应用于流量，因此您无需在源接口和目标接口上应用服

务策略；如果流量与两个方向的类映射都匹配，则进入或退出您应用策略映射的接口的所有流量都受影响。

示例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

步骤 3 为流量类启用流移动性：

a) 配置扩展 ACL 以在服务器更改站点时确定要重新分配至最佳站点的业务关键流量：

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。您应对业务关键流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。

b) 为 ACL 创建类映射：

class-map *flow_map_name*

match access-list *flow_acl_name*

c) 指定在其上启用了 LISP 检测的同一策略映射，再指定流类映射，然后启用流移动性：

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

示例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

步骤 4 进入集群组配置模式，并为集群启用流移动性：

cluster group *name*

flow-mobility lisp

此开/关使您可以轻松地启用或禁用流移动性。

示例

以下示例：

- 将 EID 限制为 10.10.10.0/24 网络上的 EID
- 检查位于 192.168.50.89 的 LISP 路由器（内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（在另一个 ASA 接口上）之间的 LISP 流量 (UDP 4342)
- 为使用 HTTPS 在 10.10.10.0/24 上进入服务器的所有内部流量启用流移动性。
- 为集群启用流移动性。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

配置分布式站点间 VPN

默认情况下，集群使用集中式站点间VPN模式。要利用集群的可扩展性，您可以启用分布式站点间 VPN 模式。

关于分布式站点间 VPN

在分布式模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群节点分发。在集群节点之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

分布式 *VPN* 连接角色

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。在分布式 VPN 模式下运行时，系统将为集群节点分配以下角色：

- 主用会话所有者 - 最初接收连接的节点，或将备份会话转换为主用会话的设备。所有者为完整的会话维护状态并处理数据包，包括 IKE 和 IPsec 隧道以及所有与之关联的流量。
- 备份会话所有者 - 正在处理现有主用会话的备份会话的节点。如果主用会话所有者发生故障，备份会话所有者将成为主用会话所有者，并在另一个节点上建立新的备份会话。
- 转发器 - 如果与某个 VPN 会话关联的流量被发送至一个未拥有该 VPN 会话的节点，该节点将使用集群控制链路 (CCL) 将流量转发到拥有该 VPN 会话的节点。
- 协调器 - 协调器（始终是集群的控制节点）负责计算将移动哪些会话，在哪里以及何时执行主用会话重新分发 (ASR)。它会向所有者节点 X 发送将 N 个会话移至节点 Y 的请求。成员 X 将在完成操作时向协调器发送回应，指定它已成功移动的会话数量。

分布式 *VPN* 会话的特征

分布式站点间 VPN 会话具有以下特征。否则，VPN 连接的行为与不在集群上时的行为相同。

- VPN 会话将在会话级别跨集群分布。这意味着同一集群节点将会处理 VPN 连接的 IKE 和 IPsec 隧道及其所有流量。如果 VPN 会话流量被发送至未拥有该 VPN 会话的集群节点，此流量将被转发至拥有该 VPN 会话的集群节点。
- VPN 会话拥有在整个集群内唯一存在的会话 ID。此会话 ID 将用于验证流量，做出转发决策和完成 IKE 协商。
- 在站点间VPN集线器和辐射配置中，当客户端通过集群连接（称为发夹）时，流入的会话流量和流出的会话流量可能在不同的集群节点上。
- 您可以要求将备份会话分配到另一个机箱内的安全模块上；这样可以防范机箱出现故障。或者，您可以选择在集群内的任意节点上分配备份会话；这样可以防范节点出现故障。当集群中有两个机箱时，强烈建议采用远程机箱备份。

集群事件的分布式 *VPN* 处理

事件	分布式 VPN
节点故障	此故障节点上所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并根据备份策略将备份会话重新分配到另一个节点上。
机箱故障	使用远程机箱备份策略时，故障机箱上所有主用会话的备份会话（位于另一机箱中的节点上）将变为主用状态。更换节点时，这些当前处于主用状态的会话的备份会话将被重新分配到更换机箱中的节点上。 使用平面备份策略时，如果主用会话和备份会话都在故障机箱上，则连接将会断开。在另一个机箱的节点上具有备份会话的所有主用会话将会回退到备份会话。新的备份会话将被分配到存活机箱中的另一个节点。

事件	分布式 VPN
停用集群节点	正在停用的集群节点上的所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并根据备份策略将备份会话重新分配到另一个节点上。
集群节点加入	如果新节点上的VPN集群模式未设置为分布式，则控制节点将请求更改模式。 在与 VPN 模式兼容后，集群节点将被分配正常操作流中的主用和备份会话。

IPsec IKEv2 修改

在分布式站点间 VPN 模式下，IKEv2 进行了以下方面的修改：

- 使用身份取代了 IP/端口元组。这将允许对数据包做出正确的转发决策，以及清理可能位于其他集群成员上的先前连接。
- 标识单个 IKEv2 会话的 (SPI) 标识符是在本地生成的 8 字节随机值，并且在整个集群中是唯一的。SPI 嵌入了时间戳和集群节点 ID。在收到 IKE 协商数据包时，如果时间戳或集群节点 ID 检查失败，则会丢弃数据包并记录一条指示原因的消息。
- IKEv2 处理已修改为通过划分集群成员来预防 NAT-T 协商失败。在接口上启用 IKEv2 后，将添加新的 ASP 分类域 *cluster_isakmp_redirect* 和规则。使用 **show asp table classify domain cluster_isakmp_redirect** 命令查看规则。

集群中分布式站点间 *VPN* 的高可用性

以下功能针对安全模块或机箱的单一故障提供恢复能力：

- 在集群中任意机箱上的另一个安全模块中备份的 VPN 会话能承受安全模块故障。
- 在另一个机箱上备份的 VPN 会话能承受机箱故障。
- 可以更改集群控制单元而不丢失 VPN 站点间会话。

如果在集群稳定之前发生其他故障，并且主动和备份会话都在故障节点上，那么连接可能会丢失。

当某个节点以正常方式（例如禁用VPN集群模式、重新加载集群节点和其他预期的机箱更改）离开集群时，将做出所有尝试以确保不会丢失任何会话。在这些类型的操作期间，只要为集群提供时间在操作之间重新建立会话备份，会话就不会丢失。如果在最后一个集群节点上触发正常退出，它将正常结束现有会话。

CMPv2

系统将跨所有集群节点同步 CMPv2 ID 证书和密钥对。但只有集群中的控制节点会自动续约 CMPv2 证书并重新生成密钥。控制节点会在续约时将这些新的ID证书和密钥同步至所有集群节点。通过这种方式，集群中的所有节点都能使用CMPv2证书进行身份验证，而且任何节点都能接管成为控制节点。

分布式站点间 VPN 证书

每个集群成员上都需要分布式站点间 VPN 的运营商许可证。

每个 VPN 连接都需要两个其他 *VPN* 许可的会话（其他 *VPN* 许可证是基础许可证的一部分），一个用于主用会话，一个用于备份会话。由于每个会话使用两个许可证，因此集群的最大VPN会话容量不能超过许可容量的一半。

分布式站点间 VPN 的前提条件

型号支持

- Firepower 9300
- 最多 2 个机箱上最多支持 6 个模块。您可以在每个机箱中安装不同数量的安全模块，但我们建议均匀分布。

最高 VPN 会话数

每个安全模块支持多达 6K 个 VPN 会话，跨 6 个节点最多支持约 36K 个会话。

集群节点上支持的实际会话数量取决于平台容量、分配的许可证以及每情景的资源分配。当利用率接近限制时，即使未达到每个集群节点的最大容量，也可能出现创建会话失败的情况。这是因为主用会话分配取决于外部交换，而备份会话分配则取决于内部集群算法。建议客户相应地调整其利用率，并留出非均匀分布的空间。

分布式站点间 VPN 准则

防火墙模式

仅在路由模式下支持分布式站点间 VPN。

情景模式

分布式站点间VPN可在单情景和多情景模式下运行。但在多情景模式下，主用会话重新分发将在系统级别，而不是情景级别进行。这可以防止与情景关联的主用会话移动到包含与其他情景关联的主用会话的集群成员上，从而在不知情的情况下产生无法支持的负载。

不受支持的检查

在分布式站点间 VPN 模式下不支持或已禁用以下检测类型：

- CTIQBE
- DCERPC
- H323、H225 和 RAS
- IPSec 直通
- MGCP
- MMP
- NetBIOS

- PPTP
- RADIUS
- RSH
- RTSP
- SCCP（瘦客户端）
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

其他准则

- 在分布式站点间 VPN 模式下仅支持 IKEv2 IPsec 站点间 VPN。不支持 IKEv1。在集中式 VPN 模式下支持站点间 IKEv1。
- 不支持站点间集群。
- 动态 PAT 在分布式站点间 VPN 模式下不可用。

启用分布式站点间 VPN

启用分布式站点间 VPN，以充分利用 VPN 会话集群的可扩展性优势。

注释 在集中式和分布式之间更改VPN模式需要重新加载集群中的所有节点。更改备份模式是动态的，将不会终止会话。

开始之前

根据 VPN 配置指南配置站点间 VPN。

过程

步骤 1 在集群的控制节点上进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)#
```

步骤 2 启用分布式站点间 VPN。

vpn-mode distributed backup flat

或

vpn-mode distributed backup remote-chassis

在**平面**备份模式下，备用会话建立在任何其他集群节点上。这将保护用户免受模块故障的影响，但不能保证提供机箱故障保护。

在**远程机箱**备份模式下，备用会话建立在集群内另一个机箱的节点上。这将同时保护用户免受模块故障和机箱故障的影响。

如果是在**单机箱**环境中配置远程机箱（特意配置或因故障所致），则在另一个机箱加入之前，将不会创建任何备份。

示例：

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

重新分发分布式站点间 VPN 会话

主用会话重新分发(ASR)将在所有集群成员之间重新分发主用 VPN 会话负载。由于开始会话和结束会话的动态性质，ASR 是跨所有集群成员均衡会话的最佳做法。重复进行重新分发操作将会优化均衡。

重新分发可以在任何时间运行，应该在集群中发生任何拓扑更改后运行，并且建议在新成员加入集群后运行。重新分发的目标是创建稳定的 VPN 集群。稳定的 VPN 集群的节点之间具有几乎相等数量的主用和备份会话。

要移动某个会话，备份会话将变为主用会话，并选择另一个节点托管新的备份会话。移动会话依赖于主用会话的备份位置和该特定备份节点上已有的主用会话数量。如果备份会话节点由于某种原因不能托管主用会话，则原始节点继续作为该会话的所有者。

在多情景模式下，主用会话重新分发将在系统级别，而不是个别情景级别进行。不在情景级别执行重新分发是因为，一个情景中的主用会话可能被移动某个成员，而该成员包含另一个情景中的其他许多主用会话，从而在该集群成员上创建了更多负载。

开始之前

- 如果您想要监控重新分发活动，请启用系统日志。
- 此程序必须在集群的控制单元上执行。

过程

步骤 1 在控制节点上，查看活动会话和备份会话在集群中的分布情况。

show cluster vpn-sessiondb distribution

示例：

系统将显示如下分布信息：

```
ciscoasa# show cluster vpn-sessiondb distribution
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

每行包含成员 ID、成员名称、主用会话数以及备份会话驻留在哪些成员上。对于以上示例，用户可以读出以下信息：

- 成员 0 上具有 209 个主用会话，成员 1 上备份了 111 个会话，成员 2 上备份了 98 个会话
- 成员 1 上具有 204 个主用会话，成员 0 上备份了 108 个会话，成员 2 上备份了 96 个会话
- 成员 2 没有任何主用会话；因此，没有集群成员正在备份此节点的会话。此成员最近才加入集群。

步骤 2 重新分发会话。

cluster redistribute vpn-sessiondb

此命令会立即返回（无任何消息），同时在后台继续执行。

根据需要重新分发的会话数和集群上的负载，这可能需要一些时间。重新分发活动发生时，系统会提供包含以下短语的系统日志（此处未显示其他系统详细信息）：

系统日志短语	说明
已启动 VPN 会话重新分发	仅控制节点
已发送请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅控制节点
未能将会话重新分发消息发送至 *member-name*	仅控制节点
已收到请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅数据节点
已将 *number* 个会话移到 *member-name*	已移至指定集群的活动会话数。
未能收到 *dest-member-name* 的会话移动响应	仅控制节点
已完成 VPN 会话	仅控制节点
检测到集群拓扑更改。已终止 VPN 会话重新分发。	

步骤 3 重新输入 **show cluster vpn-sessiondb distribution** 命令以查看结果。

FXOS：删除集群设备

以下部分介绍如何临时或永久删除集群中的节点。

临时删除

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

要检查设备当前是否在集群中，在应用内使用 **show cluster info** 命令查看集群状态：

```
ciscoasa# show cluster info
Clustering is not enabled
```

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

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

  要重新启用集群，请在 ASA 上输入 **cluster group** *name*，然后输入 **enable**。

- 禁用应用实例 -在 FXOS CLI 中，请参阅以下示例：

  ```
  Firepower-chassis# scope ssa
  Firepower-chassis /ssa # scope slot 1
  Firepower-chassis /ssa/slot # scope app-instance asa asa1
  Firepower-chassis /ssa/slot/app-instance # disable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

  要重新启用：

  ```
  Firepower-chassis /ssa/slot/app-instance # enable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

- 关闭 安全模块/引擎 - 在 FXOS CLI 中，请参阅以下示例：

  ```
  Firepower-chassis# scope service-profile server 1/1
  Firepower-chassis /org/service-profile # power down soft-shut-down
  Firepower-chassis /org/service-profile* # commit-buffer
  Firepower-chassis /org/service-profile #
  ```

要接通电源：

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- 关闭机箱 -在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

永久删除

您可以使用以下方法永久删除集群节点。

- 删除逻辑设备 -在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- 从服务中删除机箱或安全模块 - 如果从服务中删除设备，则可以将替换硬件添加为集群的新节点。

ASA：管理集群成员

部署集群后，您可以更改配置和管理集群成员。

成为非活动成员

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

开始之前

- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。

- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

从控制单元

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

开始之前

- 您必须使用控制台端口来重新启用集群。其他接口已关闭。
- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。
- 确保故障已解决，再尝试重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

变更控制单元

⚠

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

要更改控制节点，请执行以下步骤：

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在整个集群范围内执行命令

要向集群中的所有成员或某个特定成员发送命令，请执行以下步骤。向所有成员发送 **show** 命令以收集所有输出并将其显示在当前设备的控制台上。（请注意，可能存在您可以在控制设备上输入的显示命令，以查看集群范围内的统计信息。）也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

向所有成员发送命令，或者指定设备名称向某个特定成员发送命令：

cluster exec [unit *unit_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看成员名称，请输入 **cluster exec unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有设备复制到 TFTP 服务器，请在控制设备上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本示例中，asa1 和 asa2 是集群设备名称。

以下是 **cluster exec show memory** 命令的输出示例，显示了集群内每个成员的内存信息：

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA：监控 Firepower 4100/9300 机箱上的 ASA 集群

您可以监控集群状态和连接并排除故障。

注释 在比较 ASA 与 FXOS 中的集群控制链路上的数据包时，FXOS 数据包计数高于 ASA 中显示的计数。在 ASA 中，只有以集群控制链路 IP 地址为目标的数据包才会计入输入数据包。重新注入到数据接口的已转发数据包仅会计入数据接口的 输入 统计信息和集群控制链路的 输出 统计信息。

监控集群状态

请参阅以下用于监控集群状态的命令：

- **show cluster info [health], show cluster chassis info**

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、设备和整个集群的当前运行状况。

  有关 **show cluster info** 命令，请参阅以下输出：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

显示集群设备是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果设备已永久禁用，或设备已在集群中，则此命令将不会显示任何输出。

请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

  - **asp** — 数据平面传输统计信息。
  - **cp** — 控制平面传输统计信息。

    如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

    ```
    ciscoasa# show cluster info transport cp detail
    Member ID to name mapping:
      0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

    Legend:
      U    - unreliable messages
      UE   - unreliable messages error
      SN   - sequence number
      ESN  - expecting sequence number
      R    - reliable messages
      RE   - reliable messages error
      RDC  - reliable message deliveries confirmed
      RA   - reliable ack packets received
      RFR  - reliable fast retransmits
    ```

```
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0
```

```
    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
```

```
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群设备加入失败的原因或设备离开集群的原因的错误消息。

捕获整个集群范围内的数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {cpu | memory | resource} [选项]，**show cluster chassis [cpu | memory | resource usage]**

显示整个集群的聚合数据。可用选项取决于数据类型：

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail | count], cluster exec show conn**

  show conn 命令显示流量是导向器流量、备用流量还是转发器流量。在任意设备上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
```

```
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示所有集群设备之间的流量分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再平衡统计信息。

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1
```

```
Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Memory usage(%) captured over 30 intervals:

Unit ID  0
```

```
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35


CPU usage(%) captured over 30 intervals:

Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [选项]，**show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  显示整个集群的聚合数据。可用选项取决于数据类型：

  有关 **show cluster access-list** 命令，请参阅以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
```

```
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有设备在用连接的 汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):*****************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:************************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**

- **debug route cluster**

  显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*********************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

监控分布式站点间 VPN

使用以下命令监控 VPN 会话的状态和分布：

- 使用 **show cluster vpn-sessiondb distribution** 提供会话的总体分布。如果在多情景环境中运行，则必须在系统执行空间中运行此命令。

  利用此 **show** 命令可以快速查看会话，而无需在每个节点上执行 **show vpn-sessiondb summary**。

- 也可使用 **show cluster vpn-sessiondb summary** 命令提供集群上的 VPN 连接的统一视图。

- 使用 **show vpn-sessiondb** 命令的单独设备监控除了显示常见的 VPN 信息以外，还显示设备上的主用和备份会话数量。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  显示集群的调试消息。

- **debug service-module**

  显示用于刀片级别问题（包括监管程序与应用之间的运行状况检查问题）的调试消息。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

  例如，如果您看到以下消息显示两个具有相同**local-unit**名称的节点充当控制节点，这可能意味着两个节点具有相同的**local-unit**名称（请检查您的配置），或者某个节点正在接收自己的广播消息（请检查您的网络）。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

分布式站点间 VPN 故障排除

分布式 VPN 通知

当运行分布式 VPN 的集群上发生以下错误情况时，您将收到包含确定短语的通知消息：

情况	通知
如果在尝试加入集群时，某个现有或正在加入集群的数据节点未处在分布式 VPN 模式下：	新集群成员 (*member-name*) 由于 vpn 模式不匹配而被拒绝。 和 控制节点 (*control-name*) 拒绝来自设备 (unit-name) 的注册请求，原因是：vpn 模式功能与控制节点配置不兼容
如果分布式 VPN 的集群成员上未正确地配置许可：	错误：控制节点请求集群的 vpn 模式更改为分布式。由于缺少运营商许可证，无法更改模式。
如果接收的 IKEv2 数据包的 SPI 中的时间戳或成员 ID 无效：	收到已到期的 SPI 或 检测到损坏的 SPI
如果集群无法创建备份会话：	未能创建 IKEv2 会话的备份。
IKEv2 初始联系 (IC) 处理错误：	IKEv2 协商因错误而终止：备份上找到过时的备份会话
重新分发问题：	未能将会话重新分发消息发送至 *member-name* 未能收到 *member-name* 的会话移动响应（仅限控制节点）
如果在重新分发会话期间拓扑发生更改：	检测到集群拓扑更改。已终止 VPN 会话重新分发。

您可能遇到以下情况之一：

- 当使用 **port-channel load-balance src-dst l4port**命令为 N7K 交换机配置 L4port 作为负载均衡算法时，站点间 VPN 会话仅被分发到集群中的一个机箱。集群会话分配的示例如下所示：

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

  由于站点间 IKEv2 VPN 使用端口 500 作为源和目标端口，因此 IKE 数据包仅发送至 Nexus 7K 与机箱之间连接的端口通道中的其中一个链路。

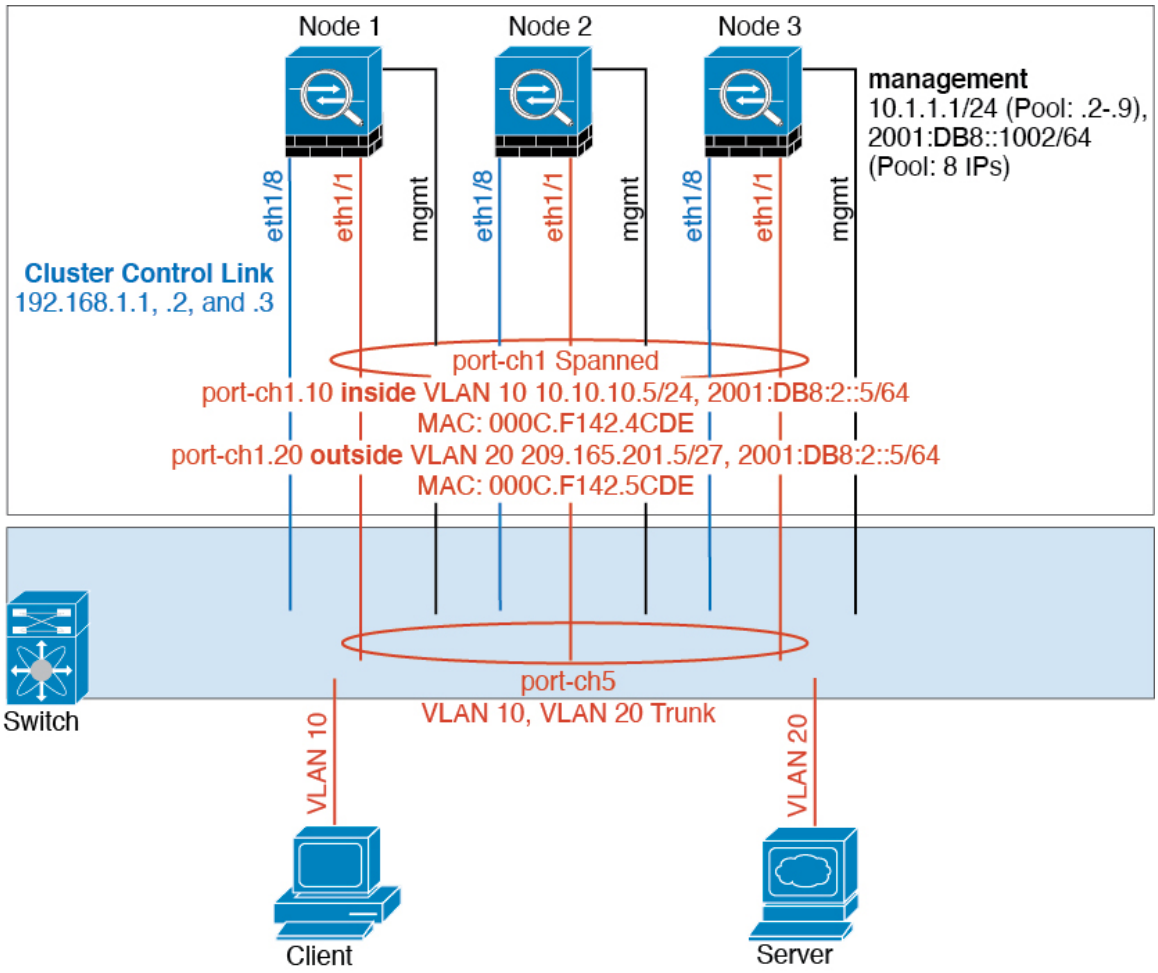
  使用 **port-channel load-balance src-dst ip-l4port** 将 Nexus 7K 负载均衡算法更改为 IP 和 L4 端口。然后，IKE 数据包将被发送至所有链路，进而发送至所有节点。

  要进行更即时的调整，请在集群的控制节点上执行： **cluster redistribute vpn-sessiondb** ，将主用 VPN 会话重新分发至另一机箱的集群节点。

ASA 集群示例

这些示例包含典型部署。

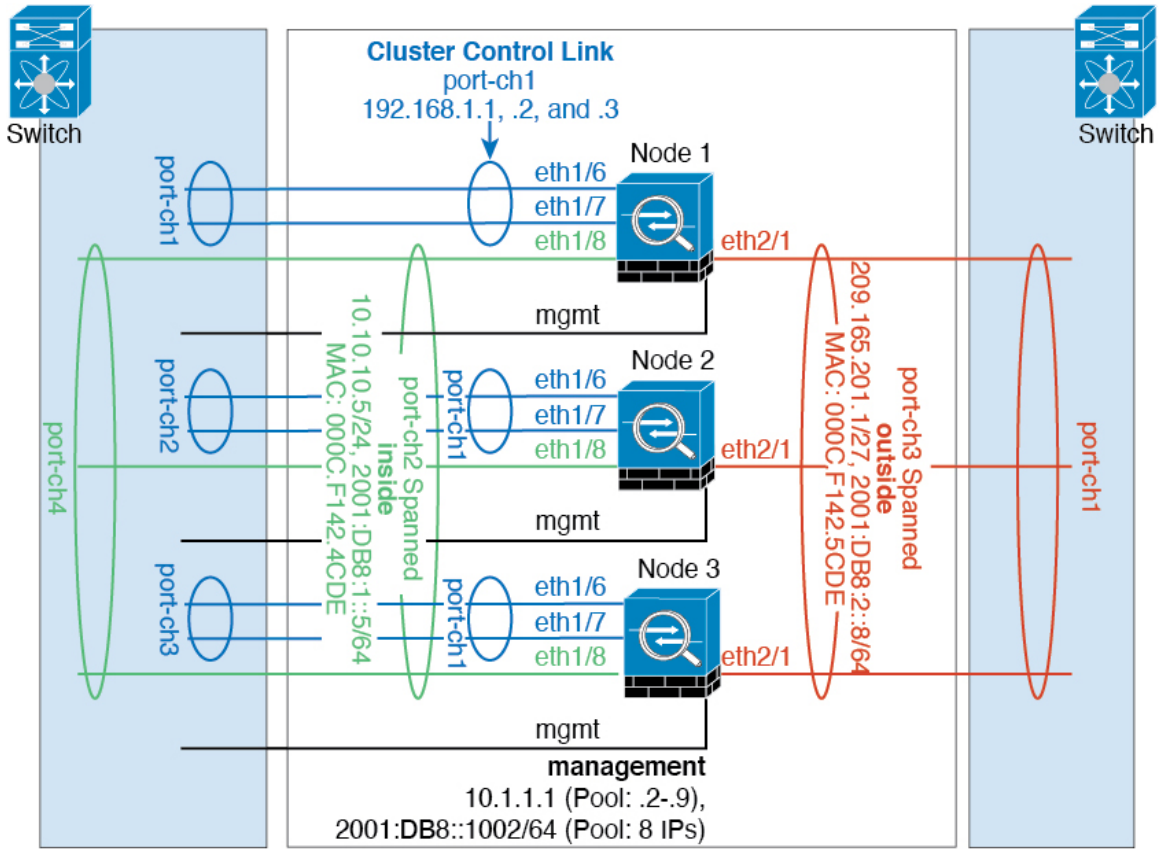
单臂防火墙



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

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

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

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

路由模式站点间集群的 OTV 配置

使用跨区以太网通道的路由模式的站点间集群能否成功，取决于OTV 的配置和监控是否适当。OTV 通过在 DCI 上转发数据包来发挥重要作用。仅当在其转发表中获知 MAC 地址时，OTV 才会通过 DCI 转发单播数据包。如果在 OTV 转发表中未获知 MAC 地址，它将丢弃单播数据包。

OTV 配置示例

```
//Sample OTV config:
//3151  -  Inside VLAN, 3152  -  Outside VLAN, 202  -  CCL VLAN
//aaaa.1111.1234  -  ASA inside interface global vMAC
//0050.56A8.3D22  -  Server MAC

feature ospf
feature otv
```

```
mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
```

```
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

因站点故障需要修改 OTV 过滤器

如果站点断开，需要删除 OTV 的过滤器，因为无需再阻止全局 MAC 地址。还需要一些其他配置。

您需要在正常工作的站点中的 OTV 交换机上添加 ASA 全局 MAC 地址的静态条目。此条目将允许另一端的 OTV 在重叠接口上添加这些条目。之所以需要此步骤，是因为如果服务器和客户端已有 ASA 的 ARP 条目（对于现有连接即是如此），它们将不再发送该 ARP。因此，OTV 将不会有机会在其转发表中获知 ASA 全局 MAC 地址。由于 OTV 的转发表中没有该全局 MAC 地址，并且根据 OTV 设计，它不会通过重叠接口泛洪发送单播数据包，则它将丢弃从服务器到全局 MAC 地址的单播数据包，现有连接将中断。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

当另一个站点恢复时，您需要重新添加过滤器，并删除 OTV 上的此静态条目。清除两个 OTV 上的动态 MAC 地址表，从而清除全局 MAC 地址的重叠条目，这一点非常重要。

MAC 地址表清除

当站点断开并且全局 MAC 地址的静态条目已添加到 OTV 时，您需要让另一个 OTV 获知重叠接口上的全局MAC地址。在另一个站点恢复后，应清除这些条目。务必清除MAC地址表，以确保OTV的转发表中没有这些条目。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
```

```
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP 缓存监控

OTV 为代理 ARP 维护通过 OTV 接口获知的 IP 地址的 ARP 缓存。

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

站点间集群示例

以下示例显示支持的集群部署。

具有站点特定的 MAC 和 IP 地址的跨区以太网通道路由模式示例

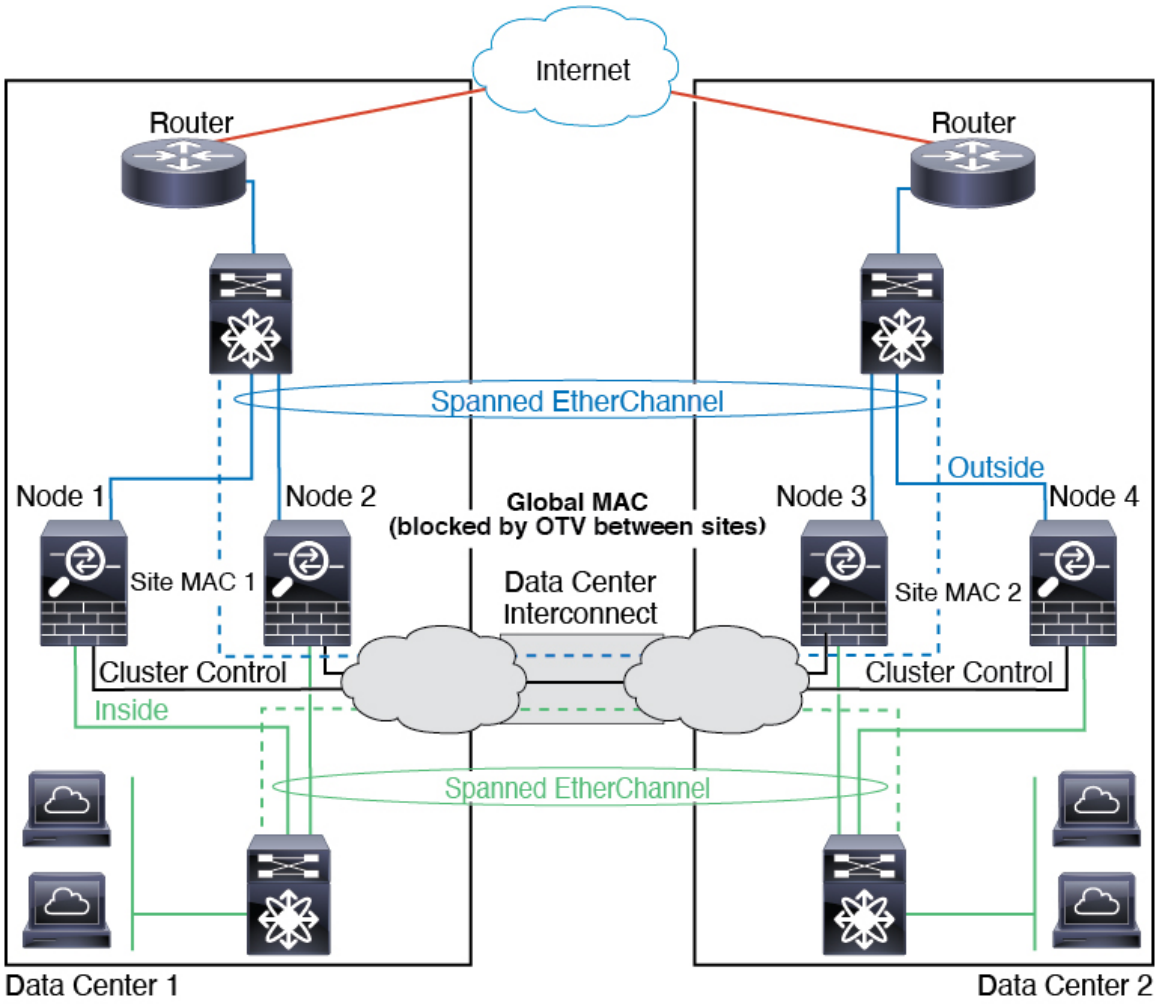
以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和内部网络之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

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。对于某些交换机（例如具有 F3 系列线卡的 Nexus），您还必须使用 ARP 检查屏蔽来自全局 MAC 地址的 ARP 数据包。ARP 检查要求您在 ASA 上设置站点 MAC 地址和站点 IP 地址。如果仅配置站点 MAC 地址，请禁用 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。

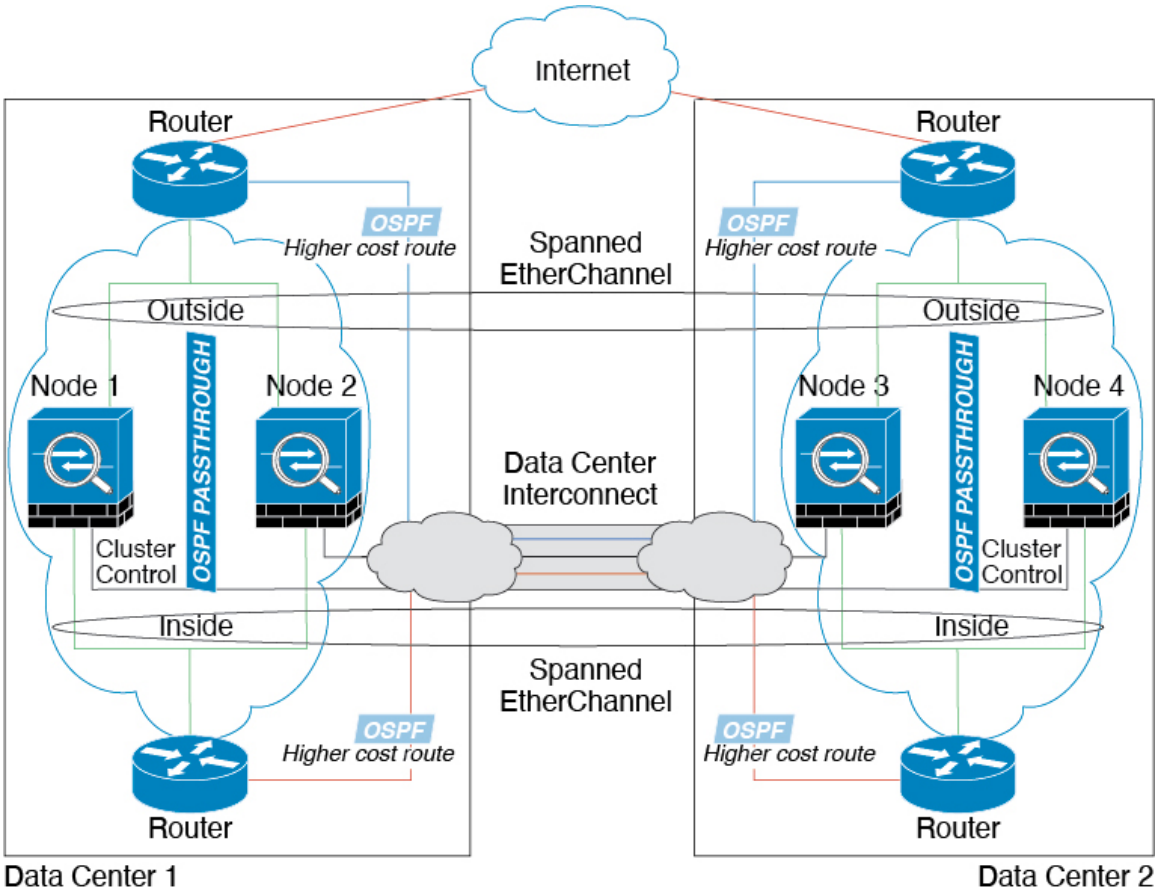
位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- 站点间 VSS、vPC、StackWise 或 StackWise Virtual - 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，而冗余交换机流量通过 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、StackWise 或 StackWise Virtual - 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 对单独的冗余交换机。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”。每个本地冗余交换机系统都会将跨区以太网通道视作站点本地的 EtherChannel。

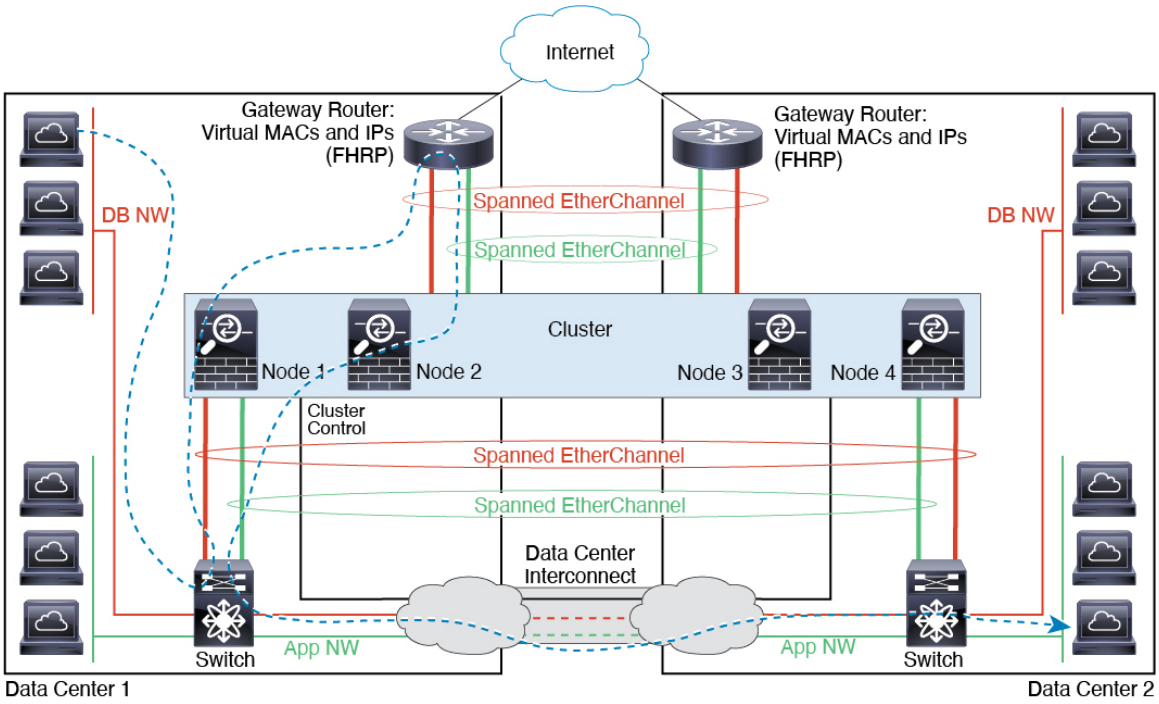


跨区以太网通道 透明模式东西站点间集群示例

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，最好使用使用 **mac-address-table static** *outside_interface mac_address* 命令将网关路由器实际 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。



集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。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。

- 依靠 TLS 代理实现的统一通信功能
- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- IS-IS 路由
- 以下应用检查：
  - CTIQBE

- H323、H225 和 RAS
- IPsec 穿透
- MGCP
- MMP
- RTSP
- SCCP（瘦客户端）
- WAAS
- WCCP

- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡
- 故障转移
- 集成路由和桥接
- 失效连接检测 (DCD)
- FIPS 型号

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

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

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

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS

- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点间 VPN

  在集中式模式下，仅与集群的控制节点建立 VPN 连接。 这是 VPN 集群的默认模式。站点间的 VPN 也可以部署在分布式 VPN 模式，其中 S2S IKEv2 VPN 连接分布在节点之间。
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由

应用到单台设备的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式下的资源管理根据本地使用情况在每个节点上分别执行。
- LISP 流量 - UDP 端口 4342 上的 LISP 流量由每个接收节点进行检查，但是没有为其分配导向器。每个节点都会添加到集群共享的 EID 表，但是 LISP 流量本身并不参与集群状态共享。

用于网络访问的 AAA 和集群

用于网络访问的AAA由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

连接设置

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

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。
- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP 检查

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用 ICMP 检查时，ICMP 流变为双向流，并由导向器/备份流支持。被检查的ICMP流的一个不同之处在于导向器对转发数据包的处理：导向器会将ICMP回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

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

NAT 和集群

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

如果您仍想在集群中使用 NAT，请考虑以下准则：

- PAT 采用端口块分配 - 请参阅该功能的以下准则：

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

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。例如，与通过 TCP/443 的 HTTPS TLS 相比，通过 UDP/443 的 Quic 协议是性能最佳的替代方案，随着它的使用越来越多，应该为 UDP/443 启用每个会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP

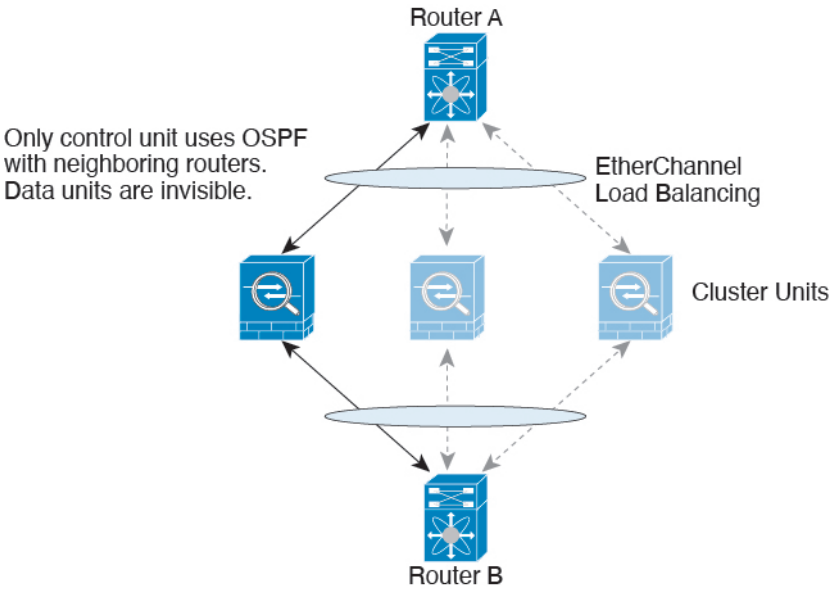
- PPTP
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

动态路由和集群

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

图 *1:* 动态路由



在数据设备向控制设备学习路线后，每个设备将单独做出转发决策。

OSPF LSA 数据库不会从控制设备同步到数据设备。如果切换了控制设备，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

SIP 检测和集群

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

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

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

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持 STUN 检查，因为针孔被复制。但是，节点之间不进行事务 ID 的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志与 NetFlow 和集群

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

思科 TrustSec 和集群

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

Cisco Secure Firewall eXtensible 操作系统 (FXOS) 机箱上的 VPN 和集群

ASA FXOS 集群支持站点间 VPN 两个相互排斥的模式之一，即集中式或分布式：

- 集中式 VPN 模式。默认模式。在集中式模式下，仅与集群的控制设备建立 VPN 连接。

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

将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。与 VPN 相关的密钥和证书将被复制到所有设备。

- 分布式 VPN 模式。在此模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群成员分布，从而提供可扩展性。在集群成员之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

注释 集中式 VPN 集群模式支持站点间 IKEv1 和站点间 IKEv2。

分布式 VPN 集群模式仅支持站点间 IKEv2。

仅在 Firepower 9300 上支持分布式 VPN 集群模式。

集中式和分布式集群模式均不支持远程访问 VPN。

性能换算系数

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

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

控制设备选择

集群成员通过集群控制链路通信，如下选举控制设备：

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

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

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制设备；现有控制设备始终保持为控制设备，除非它停止响应，此时会选择新的控制设备。
5. 在“裂脑”场景中，当临时存在多个控制单元时，具有最高优先级的单元将会保留角色，其他单元则恢复为数据单元角色。

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

集群中的高可用性

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

机箱应用监控

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 ASA应用（每秒）。如果 ASA已启动且无法与 Firepower 4100/9300 机箱管理引擎通信达到 3 秒，则 ASA会生成系统日志消息并离开集群。

如果 Firepower 4100/9300 机箱管理引擎在 45 秒后仍无法与应用通信，则会重新加载 ASA。如果 ASA 无法与管理引擎通信，则会将自身从集群中删除。

设备运行状况监控

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

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。有关详细信息，请参阅控制设备选择，第 81 页。

接口监控

每个节点都会监控使用中的所有硬件接口的链路状态，并向控制节点报告状态更改。对于多机箱集群，跨网络 EtherChannel 使用集群链路聚合控制协议 (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 ASA应用。当启用运行状况监控时，默认情况下监控有物理接口（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（取决于您的最低端口捆绑设置）。 可以选择性地禁用对每个接口的监控。

如果受监控接口在特定节点上发生故障，但在其他节点上处于活动状态，则该节点将从集群中删除。ASA在多长时间后从集群中删除节点取决于该节点是既定成员还是正在加入集群的设备。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA从集群中删除。对于既定成员，节点将在 500 毫秒后删除。

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

修饰符应用监控

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

发生故障后的状态

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

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

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA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，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过在 ASA 端口输入 **cluster group** *name*，然后输入 **enable** 重新启用集群，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在 ASA 控制台端口上通过输入 **cluster group** *name* 和 **enable** 来手动启用集群。此行为是可配置的。
- 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。设备会每 5 秒尝试重新加入集群。
- 机箱应用发生通信故障 - 当 ASA 检测到机箱应用运行状况恢复后，ASA 会立即尝试重新加入集群。或者，您可以将 ASA 配置为使用与处理内部错误相同的重新加入设置（见下文）。
- 修饰器应用发生故障 - 当检测到装饰器应用备份时，ASA 会重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。 设备将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

数据路径连接状态复制

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

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

表 *1:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

集群管理连接的方式

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

连接角色

请参阅为每个连接定义的下列角色：

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

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

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

  如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

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

  如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。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。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

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

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

端口地址转换连接

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

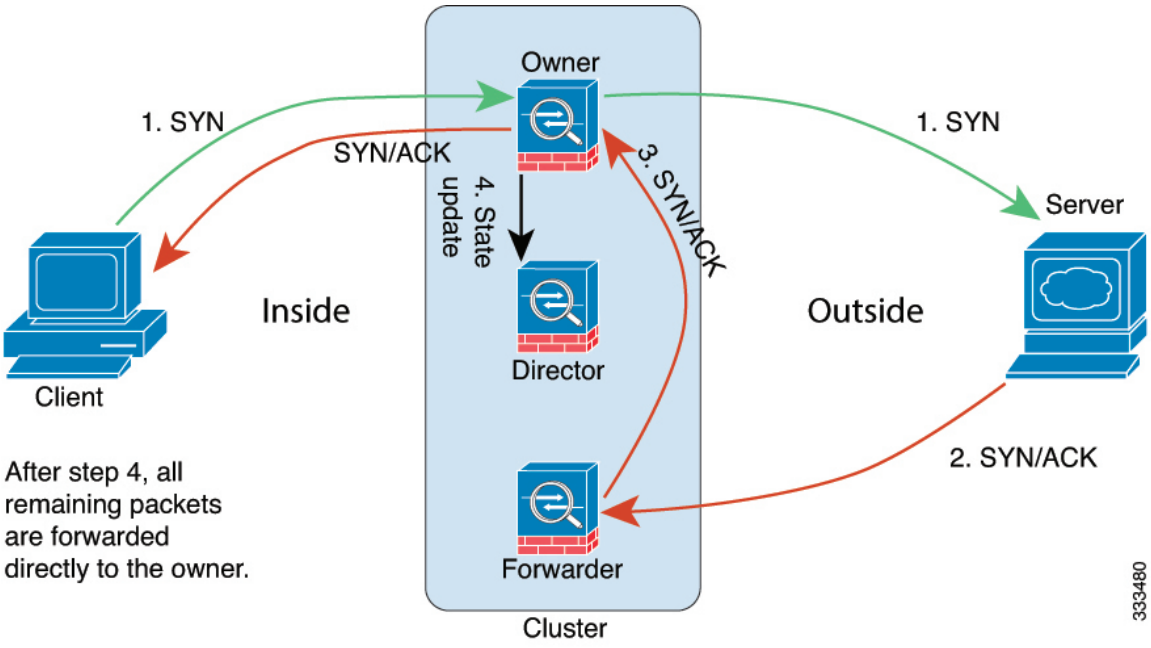
您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

新连接所有权

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

TCP 的数据流示例

以下图例显示了新连接的建立。



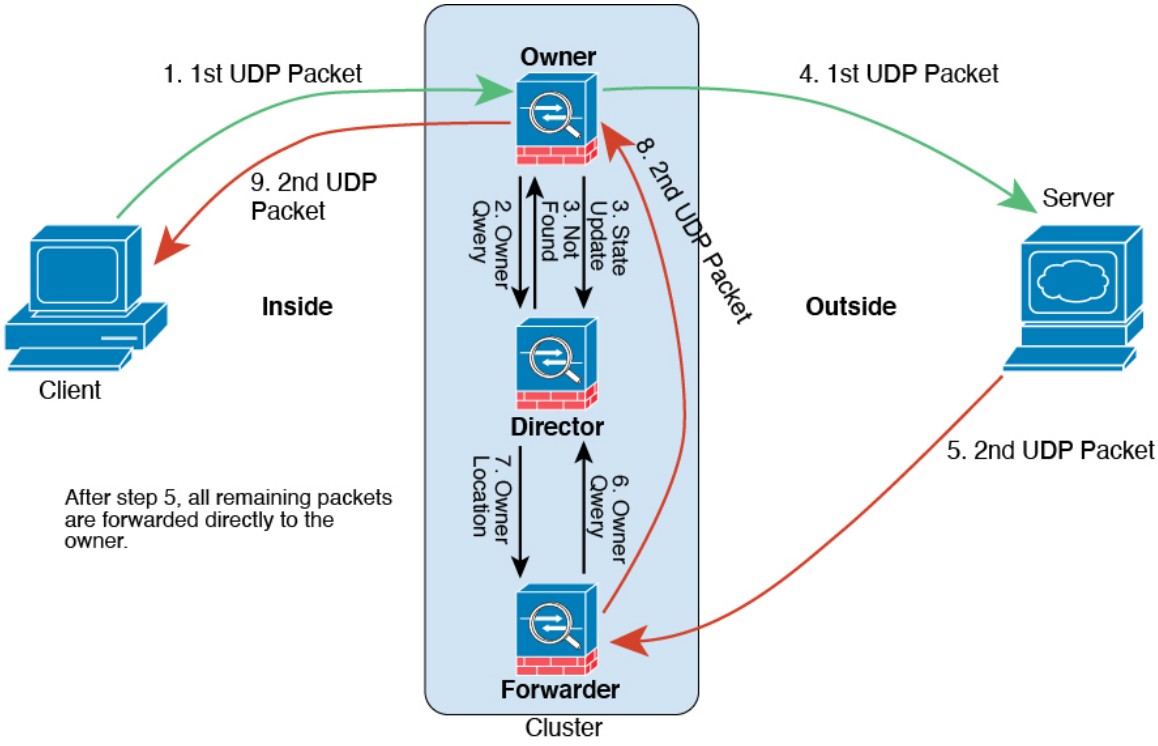
1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。

2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *2: ICMP* 和 *UDP* 数据流



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

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。

3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

跨集群实现新 TCP 连接再均衡

如果上游或下游路由器的负载平衡功能导致流量分布不平衡，则可以配置新的连接再平衡，这样每秒新连接数较高的节点就会将新 TCP 流量重定向到其他节点。现有流量将不会移至其他节点。

由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

Firepower 4100/9300上 ASA 集群的历史

功能名称	版本	功能信息
机箱心跳故障后重新加入集群的可配置延迟 (Firepower 4100/9300)	9.20(2)	默认情况下，如果机箱心跳失败然后恢复，则节点会立即重新加入集群。但是，如果配置 **health-check chassis-heartbeat-delay-rejoin** 命令，则它将根据 **health-check system auto-rejoin** 命令的设置重新加入。 新增/修改的命令：**health-check chassis-heartbeat-delay-rejoin**
流状态的可配置集群保持连接间隔	9.20(1)	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
删除偏差语言	9.19(1)	包含术语“主”和“从”的命令、命令输出和系统日志消息已被更改为“控制”和“数据”。 新增/修改的命令：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**

功能名称	版本	功能信息
改进了 Firepower 4100/9300 上集群的 PAT 端口块分配	9.16（1）	改进的PAT端口块分配可确保控制设备保留端口以供加入节点，并主动回收未使用的端口。为了最好地优化分配，您可以使用 **cluster-member-limit** 命令来设置您计划在集群中拥有的最大节点数。然后，控制单元可以分配端口块到计划的节点数量，并且不必为您不打算使用的额外节点预留端口。默认值为16节点。您还可以监控系统日志747046，以确保有足够的端口可用于新节点。 新增/修改的命令：**cluster-member-limit**、**show nat pool cluster** [**summary**]、**show nat pool ip detail**
show cluster history 命令改进	9.16（1）	我们为 **show cluster history** 命令添加了其他输出。 新增/修改的命令：**show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
并行配置同步到数据设备	9.14(1)	控制设备现在默认将配置更改并行同步到数据设备。以前，同步是按顺序发生的。 新增/修改的命令：**config-replicate-parallel**
集群加入失败或逐出的消息已添加到 **show cluster history**	9.14(1)	关于集群设备无法加入集群或离开集群的新消息添加到了 **show cluster history** 命令。 新增/修改的命令：**show cluster history**
集群中的“死连接检测”(DCD)支持的发起方和响应方信息。	9.13(1)	如果启用死连接检测(DCD)，则可以使用该**show conn detail** 命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 **show conn** 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出）
监控集群的流量负载	9.13(1)	现在，您可以监控集群成员的流量负载，包括总连接计数、CPU和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的设备可以处理负载，您可以选择在设备上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。 新增/修改的命令：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor**
加快加入集群的速度	9.13(1)	当数据设备与控制设备具有相同的配置时，它将跳过同步配置步骤并更快加入。默认情况下启用此功能。此功能在每个设备上分别配置，不会从控制设备复制到数据设备。 **注释** 某些配置命令与加速集群加入不兼容;如果设备上存在这些命令，即使已启用加速集群加入，也将始终出现配置同步。您必须删除不兼容的配置，以加速集群加入工作。使用 **show cluster info unit-join-acceleration incompatible-config** 查看不兼容的配置。 新增/修改的命令： **unit join-acceleration**、**show cluster info unit-join-acceleration incompatible-config**

功能名称	版本	功能信息
适用于集群的每站点免费 ARP	9.12(1)	现在，ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。当使用来自集群的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，集群接收的数据包使用全局MAC 地址和IP地址。如果流量不是定期从全局MAC 地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。当您为每台设备设置站点ID和为每个跨区以太网通道设置站点MAC地址时，默认情况下会启用 GARP。 新增/修改的命令：**site-periodic-garp interval**
设备按机箱并行加入集群	9.10(1)	对于 Firepower 9300，此功能可确保机箱中的安全模块同时加入集群，以便在模块之间均匀分配流量。如果某个模块先于其他模块很早加入，它可能会收到超过所需的流量，因为其他模块还无法分担负载。 新增/修改的命令：**unit parallel-join**
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	9.10(1)	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 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 中的集群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 FXOS 命令：**set cluster-control-link network**
集群接口防反跳时间现在应用于从故障状态更改为正常运行状况的接口	9.10(1)	在发生接口状态更新时，ASA 会等待 **health-check monitor-interface debounce-time** 命令或 ASDM **配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群**菜单项中指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。此功能现在应用于从故障状态更改为正常运行状态的接口。例如，对于从故障状态转换为正常运行状态的EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群上的接口仅仅因为另一个集群设备在绑定端口时的速度更快便显示为故障状态。 未修改任何命令。
内部故障后自动重新加入集群	9.9(2)	过去，许多错误条件导致集群设备从集群中移除，并且在解决问题后需要手动重新加入集群。现在，设备默认将尝试以下列时间间隔自动重新加入集群：5 分钟、10 分钟以及 20 分钟。这些值是可配置的。内部故障包括：应用程序同步超时、不一致的应用程序状态等。 新增或修改的命令：**health-check system auto-rejoin**、**show cluster info auto-join**
显示集群可靠传输协议消息的传输相关统计信息	9.9(2)	现在，您可以查看每台设备的集群可靠传输缓冲区使用情况，因此您可以确定在控制平面的缓冲区已满时发生的丢包问题。 新增或修改的命令：**show cluster info transport cp detail**

功能名称	版本	功能信息
cluster remove unit命令行为与 **no enable** 行为匹配	9.9(1)	现在，**cluster remove unit** 命令将从集群中删除一个设备，直到您手动重新启用集群或重新加载，类似于 **no enable** 命令。以前，如果从 FXOS 重新部署了引导程序配置，则集群会重新启用。现在，即使重新部署了引导程序配置，仍然保持禁用状态。但是，重新加载 ASA 将重新启用集群。 新增或修改的命令：**cluster remove unit**
改进了机箱运行状况检查故障检测	9.9(1)	现在，您可以为机箱运行状况检查配置较低的保持时间：100 毫秒。以前的最小值为 300 毫秒。请注意，最小组合时间（间隔x重试计数）不能小于 600 毫秒。 新增或修改的命令：**app-agent heartbeat interval**
站点间集群冗余	9.9(1)	站点间冗余可确保流量的备份所有者将始终位于不同于该所有者的另一站点。此功能可防范站点发生故障。 新增或修改的命令：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag**
通过 Firepower 9300 上的集群支持分布式站点间 VPN	9.9(1)	Firepower 9300 上的 ASA 集群在分布式模式下支持站点间 VPN。使用分布式模式能够在 ASA 集群的成员之间分布多个站点间 IPsec IKEv2 VPN 连接，而不仅分布在控制设备上（如集中模式一样）。这将在集中式 VPN 功能的基础上大幅扩展 VPN 支持，并提供高可用性。分布式站点间 VPN 在最多由两个机箱组成的集群上运行，每个机箱最多包含三个模块（集群成员总共包含六个），每个模块最多支持 6K 个活动会话（总共 12K 个），最多支持大约 36K 个活动会话（总共 72K 个）。 新增或修改的命令：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2**
改进的集群设备运行状况检查故障检测	9.8(1)	现在可为设备运行状态检查配置更短的保持时间：最小值为 0.3 秒。过去的最小值为 0.8 秒。此功能可将设备运行状态检查消息传递方案从控制平面中的 *keepalives* 更改为数据平面中的 *heartbeats*。使用心跳设置可改进集群的可靠性和响应能力，使其不易受控制平面 CPU 占用和调度延迟所影响。请注意，配置较低的保持时间值会增加集群控制链路消息活动。我们建议您在配置低保持时间值之前先分析网络状况；例如，确保在保持时间/3 范围内通过集群控制链路返回从一台设备到另一台设备的 ping，因为在一个保持时间间隔内有三次心跳消息。如果在将保持时间设置为 0.3 - 0.7 后对 ASA 软件降级，则此设置将恢复为默认的 3 秒，因为新设置不受支持。 修改了以下命令：**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details**
Firepower 4100/9300 机箱可配置防反跳时间，以将接口标记为发生故障	9.8(1)	您现在可以配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。此功能可以加快接口故障检测的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。默认的防反跳时间是 500 毫秒，该时间的范围是 300 毫秒至 9 秒。 新增或修改的命令：**health-check monitor-interface debounce-time**

功能名称	版本	功能信息
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	9.7(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。 修改了以下命令：**site-id**
导向器本地化：数据中心的站点间集群改进	9.7(1)	为了提高性能和将流量保存在数据中心站点间集群的某个站点内，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA 会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。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。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。 引入或修改了以下命令：**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail**
支持 16 个机箱 Firepower 4100 系列	9.6(2)	现在，您可以向 Firepower 4100 系列的集群中添加最多 16 个机箱。 未修改任何命令。
支持 Firepower 4100 系列	9.6(1)	使用 FXOS 1.1.4，ASA 在 Firepower 4100 系列上支持机箱间集群。 未修改任何命令。
在路由、跨区以太网通道模式下支持站点特定的 IP 地址	9.6(1)	对于使用跨区以太网通道的路由模式下的站点间集群，除了站点特定的MAC地址以外，现在还可配置站点特定的IP地址。添加站点IP地址后，允许您对重叠传输虚拟化 (OTV) 设备使用 ARP 检测来防止通过数据中心互联 (DCI) 传输的全局 MAC 地址的 ARP 响应（可能导致路由问题）。对于无法使用 VACL 来过滤 MAC 地址的某些交换机，需要使用 ARP 检测。 修改了以下命令：**mac-address**、**show interface**
16 个模块的机箱间集群，以及 Firepower 9300 ASA 应用的站点间集群	9.5(2.1)	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。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。 未修改任何命令。
在路由防火墙模式下，跨区以太网通道支持站点间集群的站点特定的 MAC 地址	9.5(2)	现在您可以在路由防火墙模式下对跨区以太网通道使用站点间集群。要避免 MAC 地址摆动，请为每个集群成员配置一个站点ID，这样就可在站点的设备间共享每个接口的站点特定 MAC 地址。 我们引入或修改了以下命令：**site-id**、**mac-address site-id**、**show cluster info**、**show interface**
自定义接口或集群控制链路发生故障时的ASA集群自动重新加入行为	9.5(2)	现在您可以自定义接口或集群控制链路发生故障时的自动重新加入行为。 我们引入了以下命令：**health-check auto-rejoin**

功能名称	版本	功能信息
ASA 集群支持 GTPv1 和 GTPv2	9.5(2)	ASA 集群现在支持 GTPv1 和 GTPv2 检测。 未修改任何命令。
TCP 连接的集群复制延迟	9.5(2)	该功能可以延迟导向器/备份流的创建，从而避免与短期流量相关的“不必要的工作”。 引入了以下命令：**cluster replication delay**
针对站点间流移动性的 LISP 检测	9.5(2)	思科定位编号分离协议 (LISP) 架构将设备身份与设备位置分离开，并分隔到两个不同的编号空间，使服务器迁移对客户端透明化。ASA 可以通过检测 LISP 流量确定位置更改，并使用此信息进行无缝集群操作；ASA 集群成员检查第一跳路由器与出口隧道路由器 (ETR) 或入口隧道路由器 (ITR) 之间的 LISP 流量，然后将流所有者位置更改为新站点。 引入或修改了以下命令：**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key**
现在支持在故障转移和 ASA 集群中增强运营商级 NAT	9.5(2)	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。现在支持在故障转移和 ASA 集群部署中使用此功能。 修改了以下命令：**show local-host**
可配置级别集群跟踪条目	9.5(2)	默认情况下，所有级别的集群事件都储存在跟踪缓冲区中，包括大量低级事件。要将跟踪事件级别限制为更高级别，您可以设置集群跟踪事件的最低级别。 引入了以下命令：**trace-level**
Firepower 9300 的机箱内 ASA 集群	9.4(1.150)	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 引入了以下命令：**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

当地语言翻译版本说明

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