设备的高可用性

以下主题介绍如何配置主用/备用设备故障转移，以实现 防火墙威胁防御 的高可用性。

Cisco Secure Firewall Threat Defense 高可用性

Cisco Secure Firewall Threat Defense 高可用性是一种故障转移配置，

- 需要两个相同的 Firewall Threat Defense 设备通过专用故障转移链路连接，还可以选择使用状态链路
- 支持主备故障转移，其中一个单元传输流量，而备用单元不主动传输流量，后者会同步配置和状态信息，以及
- 监控活动单元的运行状况（硬件、接口、软件和环境状态），以确定是否满足故障转移条件。

故障转移过程详情

发生故障转移时，主用设备会故障转移到备用设备，后者随即变为主用状态。系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。

注释 在公共云中运行的 Firewall Threat Defense Virtual不支持高可用性。有关配置 Firewall Threat Defense Virtual 设备以实现高可用性的详细信息，请参阅Cisco Secure Firewall Threat Defense Virtual 入门指南。

系统要求

系统要求定义了使 防火墙威胁防御 设备在指定 配置中正常运行所需的硬件、软件和许可证前提条件。

硬件要求

硬件要求是确保 配置中的两台设备可以

- 维护相同的硬件配置，包括型号、接口、模块和 RAM
- 支持适当的同步和故障转移功能，以及
- 确保可靠的高可用性操作。

硬件要求规格

配置中的两台设备必须满足以下要求：

- 型号相同。 此外，对于容器实例，它们必须使用相同的资源配置文件属性。

  对于 Firepower 9300，仅在同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。

  如果在将高可用性对添加到 防火墙管理中心 后更改资源配置文件，则稍后应在**设备** > **设备管理** > **设备** > **系统** > **库存**对话框上更新每个设备的库存。

  如果将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：

  1. 中断高可用性。
  2. 将新配置文件分配给两台设备。
  3. 重新建立高可用性。

- 拥有相同数量和类型的接口。

  对于平台模式下的Firepower 4100/9300 机箱，在启用之前，所有接口都必须在 FXOS 中进行相同的预配置。如果您在启用后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

如果在 配置中使用闪存大小不同的设备，请确保闪存较小的设备具有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

软件要求是 设备为在故障转移配置中正常运行而必须满足的配置规格。

所需软件规格

配置中的两台设备必须满足以下要求：

- 处于相同的防火墙模式（路由或透明）。
- 具有相同的软件版本。
- 位于防火墙管理中心上的同一个域或组中。
- 具有相同的 NTP 配置。请参阅为威胁防御配置 NTP 时间同步。
- 在防火墙管理中心上完全部署且没有未提交的更改。
- 在其任一接口中都未配置 DHCP 或 PPPoE。
- （Firepower 4100/9300）具有相同的流量分流模式，同时启用或禁用。

高可用性对中 Firewall Threat Defense 设备的许可证要求

高可用性对中 Firewall Threat Defense 设备的许可证要求包含以下许可规范

- 需要配置中的两台设备具有相同的许可证
- 为每个许可证类型需要两个许可证授权，以及
- 在高可用性设置期间触发自动许可证同步。

许可证同步过程

高可用性配置中的两台 Firewall Threat Defense 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，防火墙管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基础版 许可证和 IPS 许可证，而备用设备只有 基础版 许可证，防火墙管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 IPS 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

故障转移和状态故障转移链路

故障切换链路和状态同步故障切换链路是专用连接，

- 在采用故障转移配置的两台设备之间建立通信
- 要求在相应设备之间使用相同的接口以实现一致性，并且
- 用于在配对设备之间传输关键的故障转移和状态信息。

配置建议

思科建议在故障转移链路或状态故障转移链路中的两台设备之间使用同一接口。例如，在故障转移链路中，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。

故障切换链路

故障切换链路是一种通信机制，它使故障转移对中的两个单元能够不断通信，以确定每个单元的运行状态。

故障转移链路数据

以下信息通过故障切换链路传输：

- 设备状态（主用或备用）
- Hello 消息 (keep-alives)
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

故障转移链路接口

故障切换链路接口是一个专用的通信通道，

- 仅用于高可用性设备之间的故障转移通信
- 使用未使用的数据接口（物理或 EtherChannel）
- 不能与正常网络接口或用户数据流量共享，并且
- 需要根据设备型号确定特定的接口大小。

要求和限制和要求

您可以使用未使用的数据接口（物理接口 EtherChannel 接口）作为故障转移链路；但不能指定当前已配置名称的接口。您也无法使用子接口，在机箱上定义用于多实例模式的子接口除外。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。

Firewall 威胁防御 用户数据和故障转移链路之间共享接口。 您也不能在同一父接口上使用单独的子接口用于故障转移链路和数据 （仅限多实例机箱子接口）。如果将机箱子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。

注释 使用 EtherChannel 作为故障链路或状态链路时，必须在建立高可用性之前，确认具有相同成员接口的同一 EtherChannel 在两台设备上都存在。

请参阅这些有关故障转移链路的准则：

- Firepower 4100/9300 - 您不能使用管理类型接口作为故障切换链路。
- 请参阅这些有关调整链路大小的准则。

表 *1:* 故障切换链路大小

型号	组合故障转移和状态链路的接口大小
Firewall 200	1 Gbps
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Cisco Secure Firewall 1200	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105—1 Gbps Cisco Secure Firewall 3110—1 Gbps Cisco Secure Firewall 3120—1 Gbps Cisco Secure Firewall 3130—10 Gbps Cisco Secure Firewall 3140—10 Gbps
Firepower 4100	10 Gbps
Cisco Secure Firewall 4200	10 Gbps
Firewall 6100	10 Gbps
Firepower 9300	10 Gbps

交替频率等于设备保持时间。

注释 如果配置较大且设备保持时间较短，则在成员接口之间交替可以防止辅助设备加入/重新加入。这种情况下，请禁用其中一个成员接口，直到辅助设备加入。

对于用作故障转移链路的 EtherChannel，要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障转移链路

故障切换链路可在采用故障转移配置的设备之间启用通信和协调。

您需要在故障转移设备之间建立物理连接，以启用适当的故障转移功能。

过程

使用以下方法之一连接故障切换链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 防火墙威胁防御 设备的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果不在设备之间使用交换机，并且接口发生故障，则两台对等体之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

故障切换链路已物理连接，并为故障转移配置做好准备。

状态故障转移链路

状态同步故障切换链路可以

- 在故障转移设备之间传递连接状态信息，以及
- 必须配置为启用状态故障转移功能。

状态链路配置要求

要使用有状态故障转移，必须配置有状态故障转移链路（也称为有状态链路），以便传送连接状态信息。

共享故障转移链路

共享故障切换链路是一种接口保护方法，可使多个网络功能使用同一故障转移连接，不过大型配置和高流量网络应考虑使用状态和故障转移链路的专用接口。

有状态故障转移链路的专用接口

状态同步故障切换链路的专用接口是一种数据接口配置，该配置使用专门用于故障转移部署中状态链路的物理或 EtherChannel 接口。

性能注意事项

您可以将专用数据接口（如物理或 EtherChannel 接口）用于状态链路。有关专用状态链路的要求，请参阅故障转移链路接口，第 4 页。请参阅有关连接状态链接的的部分了解更多信息 连接故障转移链路，第 6 页。

为了实现最佳的长距离故障转移性能，状态链路延迟应小于 10 毫秒，但不超过 250 毫秒。如果延迟超过 10 毫秒，则由于故障转移消息的重新传输，性能可能会下降。

避免故障转移和数据链路中断

避免故障转移和数据链路中断是一种网络设计实践，

- 确保让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。
- 防止故障转移操作在故障切换链路断开时中止，以及
- 通过使用适当的连接场景来保持网络弹性。

连接场景

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路断开，则故障转移操作会被暂停，直到故障转移链路恢复正常。

这些连接情景有助于设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 Firewall Threat Defense设备之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 Firewall Threat Defense设备都将处于主用状态。因此，建议**不要**使用这些图中显示的 2 种连接方法。

图 *1:* 使用单交换机连接 - 不推荐

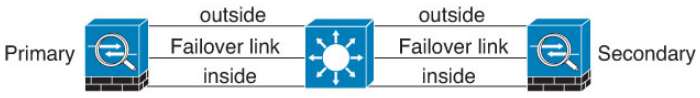
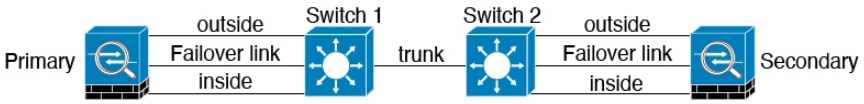


图 *2:* 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要让故障转移链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如下图所示。

图 3: 使用其他交换机连接

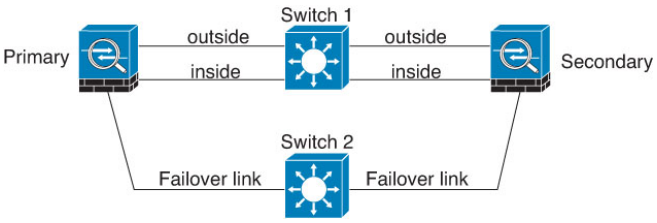
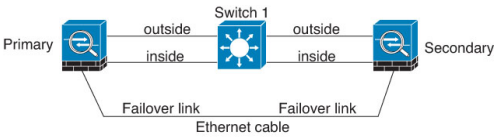


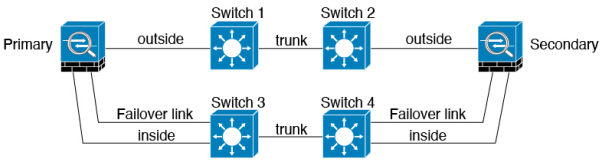
图 4: 通过电缆连接



情景 3 - 推荐

如果 Firewall Threat Defense数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 5: 使用安全交换机连接



中的 MAC 地址和 IP 地址

中的 MAC 地址和 IP 地址是网络寻址机制，

- 在故障转移场景期间为网络接口提供唯一标识
- 在主设备不可用时保持网络连接，以及
- 确保主用和备用配置之间的无缝流量传输。

地址配置类型

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。通常情况下，当发生故障转移时，新的主用设备会接管主用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注释 虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

在发生故障转移时，状态链路的 IP 地址和 MAC 地址不会更改。

主用/备用配置使用特定地址处理方法：

对于主用/备用，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主用设备始终使用主设备的 IP 地址和 MAC 地址。
2. 当主用设备进行故障转移时，备用设备会使用故障设备的 IP 地址和 MAC 地址，并开始传送流量。
3. 当故障设备恢复在线状态时，它现在处于备用状态，并且接管备用 IP 地址和 MAC 地址。

但如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的MAC 地址。当主设备变为可用时，辅助（主用）设备会将MAC 地址更改为主设备的 MAC，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

如果禁用高可用性并将故障转移配置设置为禁用状态，则需要手动恢复高可用性，或者重新启动设备。建议使用命令 **configure high-availability resume** 并恢复高可用性，而不是重新启动设备。如果在禁用故障转移配置的情况下重新加载备用设备，则备用设备将作为主用设备启动，并使用主设备的 IP 地址和 MAC 地址。这会导致 IP 地址重复并导致网络流量中断。使用命令 **configure high-availability resume** 启用故障转移并恢复流量。

注释 如果在独立设备上启用故障转移，数据接口将在故障转移协商状态下关闭，从而中断流量。

使用虚拟MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用MAC 地址是已知的，并在采用新的主设备硬件时保持不变。建议您在主设备和辅助设备上配置虚拟 MAC 地址，以确保辅助设备在作为主用设备时使用正确的MAC地址，即使它在主设备之前上线。如果您没有配置虚拟MAC 地址，则可能需要清除连接的路由器上的ARP表，以便恢复流量。当MAC地址发生变化时，Firewall Threat Defense不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

对于主用/主用故障转移，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主设备为故障转移组 1 和 2 个情景中的所有接口自动生成主用和备用 MAC 地址。如有必要，例如 MAC 地址发生冲突时，您也可以手动配置 MAC 地址。
2. 每台设备将主用 IP 地址和 MAC 地址用于其主用故障转移组，并将备用地址用于其备用故障转移组。例如，主设备是故障转移组 1 的主用设备，因此它使用故障转移组 1 中情景的主用地址。它是故障转移组 2 中情景的备用设备，因此在其中使用备用地址。
3. 当设备进行故障转移时，另一个设备将会承担出现故障的故障转移组的主用 IP 地址和 MAC 地址，并开始传送流量。
4. 当故障设备恢复在线状态，并且您已启用抢占选项时，它将恢复故障转移组。

虚拟 MAC 地址提供专用功能：

Firewall Threat Defense 有多种方法配置虚拟 MAC 地址。我们建议仅使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

对于多实例功能，FXOS 机箱仅为所有接口自动生成主 MAC 地址。如果同时具有主 MAC 地址和辅助 MAC 地址，则可以使用虚拟 MAC 地址覆盖生成的 MAC 地址，但预定义辅助 MAC 地址并非不可或缺；设置辅助 MAC 地址可确保在使用新的辅助设备硬件的情况下发送到设备的管理流量不会中断。

故障转移事件期间会发生 MAC 地址表更新：

在故障转移期间，被指定为新活动设备的设备会为 MAC 表中的每个 MAC 地址条目生成组播数据包，并将其发送到所有桥接组接口。此操作会提示网桥组中的上游交换机使用新活动设备的接口更新路由表，以确保准确的流量转发。

生成组播数据包和更新上游交换机路由表所需的时间取决于 MAC 地址表的条目数量和桥接组接口的数量。使用 **show failover statistics state-switch-delay** 命令可显示与故障转移事件期间遇到的延迟相关的统计信息。

状态故障转移

状态故障转移是一种高可用性机制，

- 不断将每个连接的状态信息从主用设备传递到备用设备
- 发生故障转移后，维护连接信息，以及
- 允许受支持的最终用户应用继续进行通信会话，而无需重新连接。

状态故障转移操作

状态故障转移期间，主用设备会不断将每个连接的状态信息发送至备用设备。发生故障转移之后，相同的连接信息在新主用设备上可用。支持的最终用户应用不需要通过重新连接来保持同一通信会话。

支持的功能

支持的功能指高可用性功能中

- 能使状态信息在状态故障转移期间传递到备用 Firewall Threat Defense 设备
- 能维护连接状态及关键信息以确保流量无缝传输；以及
- 能确保故障转移期间最大限度减少中断。

状态信息类型

对于状态故障转移，这些状态信息将传至备用设备：

- NAT 转换表。

- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表
- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注释 路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障转移期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障转移时评估的连接，有以下注意事项：
  - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障转移之前完成同步，即可实现正确的同步。
  - 入侵检测状态 - 进行故障转移时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
  - 文件恶意软件阻止 - 文件处置必须在故障转移之前变为可用。
  - 文件类型检测和阻止 - 文件类型必须在故障转移之前加以识别。如果在原始主用设备识别文件时发生故障转移，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。

- 身份策略中的用户身份决策，包括通过 ISE 会话目录被动收集的用户到 IP 地址映射以及通过强制网络门户进行的主动身份验证。发生故障转移时进行主动身份验证的用户，可能会被提示再次进行身份验证。
- 网络 AMP - 云查找独立于每台设备，因此故障转移通常不会影响此功能。具体包括：
  - 签名查找 - 如果在文件传输过程中发生故障转移，则不生成文件事件，也不进行检测。
  - 文件存储 - 如果在存储文件时发生故障转移，则文件将存储在原始主用设备上。如果在存储文件时原始主用设备关闭，则不存储文件。
  - 文件预分类（本地分析）- 如果在预分类期间发生故障转移，则检测失败。
  - 文件动态分析（连接至云）- 如果发生故障转移，则系统可能会将文件提交至云。
  - 存档文件支持 - 如果在分析期间发生故障转移，则系统可能会丢失对文件/存档的可视性。
  - 自定义阻止操作 - 如果发生故障转移，系统将不生成事件。
- 安全智能决策。但是，不会完成故障转移过程中发生的基于 DNS 的决策。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在VPN连接上运行的应用，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。
- 在所有连接中，只有已建立的连接会在备用设备上复制。

不支持的功能

不支持的功能指无法满足以下条件的设备功能

- 不会在状态故障转移中同步至备用 Firewall Threat Defense 设备
- 在故障转移事件期间不维护状态信息，以及
- 可能需要在故障转移发生后重新建立。

状态信息限制

对于状态故障转移，以下状态信息不会传送至备用 Firewall Threat Defense：

- 明文隧道（例如 GRE 或 IP-in-IP）中的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 已解密的 TLS/SSL 连接 - 解密状态不同步，如果主用设备发生故障，则系统会重置已解密的连接。需要与新的主用设备建立新连接。未解密的连接（也就是匹配TLS/SSL“不解密”规则操作的连接）不受影响，并且可以正确复制。
- 组播路由。

高可用性的网桥组要求

网桥组对高可用性的要求是需要特别考虑的因素

- 解决了故障转移期间网桥组成员接口上的流量丢失问题
- 防止交换机端口进入阻塞状态 30 到 50 秒，以及
- 提供在拓扑更改期间保持连接的变通方法。

高可用性解决方法

使用网桥组时，高可用性存在特殊的注意事项。

当主用设备故障切换到备用设备时，运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，系统会进入阻塞状态30秒至50秒。当端口处于阻塞状态时，为避免桥接组成员接口上出现流量丢失，您可以配置以下任一变通方案：

- 交换机端口处于接入模式 - 在交换机上启用 STP PortFast 功能：

  ```
  interface interface_id
    spanning-tree portfast
  ```

  链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，它最终会转换为 STP 阻塞模式。

- 如果交换机端口处于中继模式，或无法启用STP PortFast，则您可以使用以下一种会影响故障切换功能或 STP 稳定性的不太理想的变通方案：
  - 对桥接组和成员接口禁用接口监控。
  - 将故障切换条件中的接口保持时间增加到较高的值，以使 STP 在设备进行故障切换之前融合。
  - 减小交换机上的 STP 计时器，以使 STP 比接口保持时间更快地融合。

故障转移运行状态监控

故障转移运行状况监控是一项系统功能，可监控每个设备的整体运行状况和接口运行状况。

健康监控测试

防火墙威胁防御 设备可以执行测试以确定每台设备状态的信息。此部分包括有关 防火墙威胁防御 设备如何执行测试以确定每台设备状态的信息。

设备运行状况监控

设备运行状况监控是一种故障转移机制，

- 通过向故障切换链路发送 Hello 消息来确定对等体单元的运行状况

- 当连续三个 Hello 消息丢失时，在每个数据接口上发送 LANTEST 消息，并且
- 会根据对等设备的响应能力启动适当的故障转移操作。

设备运行状况监控行为

Firewall Threat Defense 设备会通过 Hello 消息监控故障转移链路，进而确定其他设备的运行状况。如果设备在故障转移链路上没有收到三条连续的hello消息，则设备会在每个数据接口（包括故障转移链路）上发送 LANTEST 消息，以验证对等体是否响应。Firewall Threat Defense 设备采取的操作取决于来自其他设备的响应。可能的操作如下：

- 如果 Firewall Threat Defense 设备在故障转移链路上收到响应，则不会进行故障转移。
- 如果 Firewall Threat Defense 设备在故障转移链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障转移。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果 Firewall Threat Defense 设备未在任何接口上收到响应，则备用设备会切换至主用模式，并会将另一台设备分类为故障设备。

注释 在高可用性故障转移事件期间， Firewall Threat Defense 设备 的运行状况监控控制面板中可能会短暂显示为 **离线 (Offline)** 。发生这种情况是因为运行状况警报会在此过程中被清除，并且仅在该过程完成后才会更新。等待故障切换操作完成。

心跳模块冗余

心跳模块冗余是一种高可用性功能，可以

- 使用数据平面传输基础设施发送心跳消息，以补充控制平面心跳数据包
- 在对等体在数据平面中收到心跳数据包时递增计数器
- 在控制平面因流量拥堵时防止虚假故障转移或裂脑场景。

心跳模块冗余行为

HA 中的每个单元定期通过故障转移链路发送广播保活心跳数据包。如果控制平面忙于处理流量，有时心跳数据包无法到达对等体，或者对等体由于 CPU 过载而无法处理心跳数据包。当对等体无法在可配置的超时期限内传达保持连接状态时，会发生错误的故障转移或裂脑场景。

数据平面中的心跳模块有助于避免由于控制平面中的流量拥塞而发生错误的故障转移或裂脑。

- 附加心跳模块的工作原理与控制平面模块类似，但使用数据平面传输基础设施发送和接收心跳消息。
- 当对等体在数据平面中收到心跳数据包时，计数器会递增。

- 如果控制平面中的心跳传输失败，则节点会检查数据平面中的心跳计数器。如果计数器递增，则表示对等体处于活动状态，并且集群在这种情况下不会执行故障转移。

注释

- 每当启用 HA 时，都会默认启用额外的心跳模块。您不必为数据平面中的其他心跳模块设置轮询间隔。此模块使用您为控制平面设置的相同心跳间隔。

接口监控

接口监控是一种故障转移功能，

- 跟踪最多 1025 个接口的运行状况，以检测接口故障
- 当在 15 秒内未收到 hello 消息时执行接口测试，并且
- 当故障接口数达到定义的阈值时，会触发故障转移。

接口监控操作

当设备在 15 个秒，未在受监控的接口上收到 hello 消息时，将运行接口测试。如果对于某个接口，其中一个接口测试失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障，设备停止运行测试。

如果满足您为故障接口数量定义的阈值 （请参阅 **设备** > **设备管理**，然后 **高可用性** > **故障转移触发条件**），并且主用设备的故障接口数量多于备用设备，则会发生故障转移。 如果某个接口在两个单元上都失败，则这两个接口会进入“Unknown”状态，并且不会计入由故障转移接口政策制定的故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的 设备会回到备用模式。

如果接口上配置了 IPv4 和 IPv6 地址， 设备会使用 IPv4 地址执行运行状况监控。如果接口上仅配置了 IPv6 地址，则 设备会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试， 设备会使用所有的 IPv6 节点地址 (FE02::1)。

接口测试

接口测试属于以下监控机制：

- 在故障转移场景期间评估接口的运行状态
- 默认情况下按顺序运行，每个测试的持续时间约为1.5秒，并且
- 确定 防火墙威胁防御 设备单元上的接口故障状态。

接口测试顺序

防火墙威胁防御 设备会按顺序使用这些接口测试：

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则 设备视为测试失败，然后测试停止。如果状态为打开，则 设备执行 Network Activity 测试。
2. 网络活动测试 - 接收的网络活动测试。测试开始时，每台设备会清除其接口收到的数据包计数。在测试期间，一旦设备收到符合条件的数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行 ARP 测试。
3. ARP 测试 - 用于测试成功的 ARP 回复。每台设备都向其 ARP 表中最新条目中的 IP 地址发送一个 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果设备未收到 ARP 回复，则 设备会向 ARP 表中的下一个条目中的 IP 地址发送一次 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行广播 Ping 测试。
4. 广播 Ping 测试 - 测试成功的 Ping 回复。每台设备发送一个广播 Ping，然后对收到的所有数据包进行计数。在测试期间，当设备收到任何数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果未收到任何流量，则测试将通过 ARP 测试再次开始。如果两台设备继续没有收到来自 ARP 和广播 Ping 测试的流量，则测试将会一直运行下去。

接口状态

接口状态是一种监控指示器，

- 显示故障转移配置中受监控接口的当前运行状态
- 跟踪对等设备之间的流量接收和 hello 数据包通信，以及
- 确定故障转移进程是否主动监控接口。

接口状态类型

受监控的接口可以具有以下状态类型：

- **未知**：初始状态。此状态也可能意味着状态无法确定。
- **正常**：接口正在接收流量。
- **正常（正在等待）**：接口已打开，但尚未从对等体设备上的对应接口接收欢迎数据包。
- **正常（未受监控）**：接口已打开，但未受故障转移进程监控。
- **正在测试**：接口上有 5 个轮询时间未收听到 Hello 消息。
- **链路断开**：接口或 VLAN 通过管理方式关闭。
- **链路断开（正在等待）**：接口或 VLAN 已通过管理方式关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- **链路断开（未受监控）**：接口或 VLAN 已通过管理方式关闭，但未受故障转移进程监控。

- **无链接**：接口的物理链路关闭。
- **无链接（正在等待）**：接口的物理链路已关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- **无链接（未受监控）**：接口的物理链路已关闭，但未受故障转移进程监控。
- **失败**：在接口上没有收到流量，但在对等体接口上收听到流量。

故障转移触发器和检测计时

故障转移触发器和检测计时是高可用性机制，具有以下功能：

- 当主用设备上发生特定故障条件时，启动自动切换，
- 通过可配置的检测阈值和计时参数监控系统运行状况，以及
- 当故障超过定义的限制时，通过将控制转移到备用设备来确保服务的连续性。

故障转移触发事件和时间参数

这些事件会在 Firepower 高可用性对中触发故障转移：

- 主用设备上超过 50% 的 Snort 实例已关闭。
- 主用设备上使用的磁盘空间已超过 90%。
- 主用设备上运行的是 **no failover active** 命令，而备用设备上运行的是 **failover active** 命令。
- 主用设备的故障接口比备用设备更多。
- 主用设备上的接口故障超过配置的阈值。

  默认情况下，单个接口发生故障会导致故障转换。您可以通过配置接口数量的阈值或为发生故障转移而必须发生故障的受监控接口的百分比来更改默认值。如果主用设备上的阈值被超过，则会发生故障转移。如果备用设备上的阈值被超过，则设备将进入**故障**状态。

  要更改默认故障转移条件，在全局配置模式下输入此命令：

表 *2:* 接口策略命令

命令	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	更改默认故障转移条件。 指定特定接口数时，*num* 参数可以介于 1 和 250 之间。 指定接口百分比时，*num* 参数可以介于 1 和 100 之间。

此表列出了故障转移触发事件及关联的故障检测时间。如果出现故障转移，您可以在消息中心中查看故障转移的原因，以及有关高可用性对的各种操作。您可以将这些阈值配置为指定的最小-最大范围内的值。

表 3: 防火墙威胁防御 故障转移次数

故障转移触发事件	最小	默认	最大
主用设备断电，硬件关闭或软件重新加载或崩溃。当出现这些情况时，受监控接口或故障转移链路不会收到任何 Hello 消息。	800 毫秒	15 秒	45 秒
主用设备接口物理链路发生故障。	500 毫秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

主用/备用故障转移

主用/备用故障转移是一种高可用性配置

- 允许使用备用 Firewall Threat Defense 设备接管故障设备的功能，
- 当主用设备故障，备用设备将变为主用设备，以及
- 若故障为暂时性，故障设备恢复后可重新作为备用设备上线。

若故障非暂时性，必须更换故障设备。更换故障设备前，须先将备用设备设为主设备，以保留辅助设备的配置。

对于多情景模式，ASA 可以在整个设备（包括所有情景）上进行故障转移，但不能在单个情景上单独进行故障转移。

主/辅角色与主/备状态

主/辅角色和主/备状态是故障转移配置概念，

- 定义设备层级结构，在同时启动时主设备优先，
- 确定故障转移操作期间的 IP 地址和 MAC 地址使用模式，以及
- 在主/备故障转移配置中的配对设备之间确立流量传输职责。

主设备与辅设备的差异

当设置主用/备用故障转移时，需要将一台设备配置为主设备，将另一台配置为辅助设备。配置过程中，主设备的策略将同步到辅助设备。此时，两台设备将作为单台设备进行设备和策略配置。但对于事件、控制面板、报告和运行状况监控，它们仍显示为单独的设备。

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

但是，设备之间还存在一些取决于哪一设备为主设备（在配置中指定），哪一设备为辅助设备的差别：

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

启动时主用设备判定是高可用性过程

- 若设备启动时检测到对等体已运行为主用，则该设备置为备用，
- 若设备启动未检测到对等体，则置为主用；
- 若两台设备同时启动，主设备置为主用，辅助设备置为备用。

故障转移事件

故障转移事件是指

- 触发主用/备用故障转移配置中的主用设备将控制权移交给备用设备
- 按设备级别发生，，以及
- 遵循特定故障转移策略以确定是否发生故障转移及各设备应采取的操作。

故障转移事件策略和操作

此表显示各故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *4:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。

故障事件	策略	主用设备操作	备用设备操作	说明
备用设备发生故障（电源或硬件）	禁用故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行过程中发生故障	禁用故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

Config-sync 优化

配置同步优化是一种配置同步增强功能，

- 比较主用设备和加入设备之间的配置散列值，以确定是否需要完全同步
- 通过在散列值匹配时跳过完全配置同步，实现更快的设备重新加入，以及
- 缩短了高可用性操作期间的维护窗口和升级时间。

配置同步优化的准则和局限性

当设备在暂停或恢复高可用性后重启或重新加入时，加入的设备会清除其运行配置。然后，主用设备将其整个配置发送到加入设备，以实现完全的配置同步。如果主用设备配置较大，则此过程可能需要几分钟时间。

配置同步优化功能可通过交换配置散列值来比较加入设备和主用设备的配置。如果主用设备和加入设备上计算的散列值匹配，加入设备就会跳过完全配置同步，重新加入高可用性配置。此功能可确保更快的对等互连，并缩短维护窗口和升级时间。

准则和限制：

- 配置同步优化功能默认已启用。

- Firewall Threat Defense 多情景模式通过在完全配置同步期间共享情景顺序来支持配置同步优化，从而允许在后续节点重新加入期间比较情景顺序。
- 如果配置密码和故障转移 IPsec 密钥，则配置同步优化无效，因为主用设备和备用设备中计算的散列值不同。
- 如果使用动态 ACL 或 SNMPv3 配置设备，则配置同步优化无效。
- 主用设备将 LAN 链路摆动的完整配置作为默认行为进行同步。在主用设备和备用设备之间的故障转移摆动期间，不会触发配置同步优化，设备会执行完整的配置同步。
- 当高可用性配置从主用设备和备用设备之间的网络通信中断或丢失中恢复时，会触发配置同步优化。

监控配置同步优化：

- 系统会生成系统日志消息，显示在主用设备和加入设备上计算的散列值是否匹配，或者操作超时是否已到期。
- 系统日志消息还会显示从发送散列请求到获取并比较散列响应所经过的时间。

注释 **show failover state** 命令中的配置状态会在加入 HA 期间显示配置同步状态。直到启动重新同步之前，此状态不会反映以后的配置部署或更改和设备上的复制。

高可用性的要求和先决条件

本参考介绍了实施高可用性功能所需的要求和前提条件。

型号支持

Cisco Secure Firewall Threat Defense

支持的域

任意

用户角色

管理员

网络管理员

准则

型号支持

- 200/1010/1210/1220:
  - 使用时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。虽然 防火墙管理中心 允许您在高可用性中配置交换机端口/VLAN 接口，但在连接到外部交换机时，可能会因网络环路而导致配置错误。
  - 仅可使用防火墙接口作为故障转移链路。
- Firepower 9300 - 不支持机箱内高可用性。
- 由于需要第 2 层的连接，因此不支持在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 Firewall Threat Defense Virtual。

其他准则

- 当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。
- 发生故障转移事件时，在连接到Firewall威胁防御设备故障转移对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 对于主用/备用 和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往 NMS 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。
- 两个对等设备都进入未知状态，如果在创建高可用性对时在任何对等设备中运行 clish，高可用性配置会失败。
- 故障转移后，系统日志消息的源地址将立即成为故障转移接口地址几秒钟。
- 为了更好地融合（在故障转移期间），您必须关闭 HA 对上未与任何配置或实例关联的接口。

- 在具有共享故障转移和状态接口的高可用性部署中，如果连接转移故障转移接口在备用设备处于“同步配置”状态时发生故障，以及最终在备用设备切换到主用状态时，会导致裂脑。即使有受监控接口，也会出现这种情况。

  连接转移故障转移接口可能在以下情况下发生故障：

  - 备用设备重新启动后，当备用设备处于同步配置状态时，连接切换故障转移接口会发生故障。
  - 启用备用设备上先前禁用的故障转移后，当备用设备处于同步配置状态时，连接故障转移接口会发生故障。

  要避免裂脑，请使用故障转移和状态接口。如果故障转移接口上的连接故障仍然存在，则从网络中隔离新的主用（之前是备用）设备。

- 如果您在评估模式下配置故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。

- 当使用具有故障转移功能的 SNMPv3 时，如果更换故障转移设备，则 SNMPv3 用户不会复制到新设备。 您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。

- 设备不再与其对等体共享 SNMP 客户端引擎数据。

- 如果您有大量访问控制和 NAT 规则，则配置的大小可能会阻止有效的配置复制，导致备用设备需要过长的时间才能达到备用就绪状态。这也会影响您在通过控制台或 SSH 会话进行复制期间连接到备用设备的能力。要提高配置复制性能，请使用 **asp rule-engine transactional-commit access-group** 和 **asp rule-engine transactional-commit nat** 命令为访问规则和 NAT 启用事务提交。

- 转换为备用角色的 对中的设备可将其时钟与主用设备同步。

  示例：

  ```
  firepower#show clock
  01:00:52 UTC Mar 1 2022

  ...
  01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
  Cold Standby               Sync Config               Detected an Active mate

  19:38:21 UTC Apr 9 2022 <======= Updated clock
  Sync Config                Sync File System          Detected an Active mate
  ...
  firepower/sec/stby#show clock
  19:38:40 UTC Apr 9 2022
  ```

- 中的设备不会动态同步时钟。以下是进行同步时的一些事件示例：

  - 将创建一个新的 对。
  - 已中断并已重新创建。
  - 故障转移链路上的通信中断并重新建立。

  - 使用 **no failover/failover** 或 **configure high-availability suspend/resume** （Firewall Threat Defense）命令来在 CLI 手动更改故障转移状态。

- 启用 会强制删除所有路由，并会在 进程变为“活动”状态后重新添加这些路由。在此阶段，您可能会遇到连接丢失的情况。
- 如果更换主设备，则在重新创建高可用性时，应将更换设备设置为辅助设备，以便将配置从以前的辅助设备复制到更换设备。如果将替换设备设置为主设备，则会意外覆盖运行设备上的配置。
- 在形成 之前，请在两台 威胁防御 设备上配置相同的强加密。如果二者不同，则高可用性对等体可能会进入裂脑状态。
- 在配置了数百个接口的高可用性中部署 Firepower 1100 设备可能会导致故障转移时间（秒）增加。
- 在 配置中，短期连接（通常使用端口 53）会快速关闭，并且永远不会从主用设备传输或同步到备用设备，因此两个 设备上的连接数量可能存在差异。这是短期连接的预期行为。您可以尝试比较长期（例如，超过 30-60 秒）的连接。
- 在 配置中，初期连接（尚未完成三次握手过程的连接请求）会快速关闭，并且不会在主用设备和备用设备之间同步。此设计可确保高可用性系统的效率和安全性。因此，两台 设备上的连接数可能存在差异，这是预期行为。
- 如果故障转移LAN链路不是背靠背连接，而是通过一台或多台交换机连接，则中间路径内的故障可能会导致主用设备失去与备用设备的连接，从而导致主用/备用状态不一致。虽然这不会影响 功能，但建议检查并恢复主用设备和备用设备之间的故障转移链路路径。

  当故障转移 LAN 链路发生故障时，不建议部署任何配置，因为它可能不会复制到对等设备。
- 请参阅 Cisco Secure Firewall Threat Defense Virtual 入门指南 并查看 Firewall Threat Defense Virtual 设备配置，以实现高可用性。
- 在 OSPF 中，故障转移后，与对等设备的 OSPF 连接将变为无效。终止无效连接，然后建立新的 OSPF 连接。
- 在透明模式下，如果存在主用设备丢失热备路由器 (HSRP) MAC 地址的问题，请为 MAC 地址创建静态映射。
- 如果威胁防御设备处于高可用性状态，则无法更改UCAPL或CC合规性模式。在形成高可用性对前修改合规模式。

添加高可用性对

建立主/备高可用性对，以确保设备故障时网络防护的连续性。

建立主用/备用高可用性对时，请将其中一台设备指定为主设备，将另一台指定为辅助设备。防火墙管理中心 会将合并的配置应用于配对设备。如果存在冲突，则使用主设备设置。在多域部署中，高可用性对中的设备必须属于同一个域。

注释 故障切换链路和状态故障切换链路位于专用 IP 空间中，仅用于高可用性对中的对等体之间的通信。在高可用性对建立后，无法在不破坏高可用性对并重新配置的情况下修改所选接口链路和加密设置。

注意 创建或中断高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

Before you begin

确认两台设备：

- 型号相同。
- 拥有相同数量和类型的接口。
- 位于同一个域和组中。
- 具有正常运行状态且运行相同的软件。
- 处于路由模式或透明模式下。

注释 数据接口上的管理器访问仅支持路由模式。

- 具有相同的 NTP 配置。请参阅时间同步。
- 完全部署且没有尚未确认的更改。
- 在其任一接口中都未配置 DHCP 或 PPPoE。
- 对于数据接口上的管理器访问：
  - 在两台设备上使用相同的数据接口进行管理器访问。
  - 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。

注释 如果您使用 零接触调配 注册设备，则当您使用外部接口进行管理器访问时，它会默认使用 DHCP。在启用高可用性之前，需要将 IP 地址更改为静态地址。请参阅更改设备 IP 地址。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

- 在同一子网中有不同的静态 IP 地址。

- 使用相同的管理器配置（**configure manager add** 命令）确保连接相同。
- 不能将数据接口用作故障切换链路或状态链路。

注释 如果主设备上可用的证书在辅助设备上不存在，那么两台 Firewall Threat Defense 设备之间可能会形成高可用性。形成高可用性时，证书将在辅助设备上同步。

过程

步骤 1 根据 向管理中心注册将两台设备添加到 防火墙管理中心。

步骤 2 选择**设备** > **设备管理**。

步骤 3 从 **添加** 下拉菜单中，选择 **高可用性**。

步骤 4 为高可用性对输入显示**名称** 。

步骤 5 为高可用性对选择**主对等 (Primary Peer)** 设备。

步骤 6 为高可用性对选择**辅助对等 (Secondary Peer)** 设备。

步骤 7 点击**继续 (Continue)**。

步骤 8 在 **LAN 故障切换链路 (LAN Failover Link)** 下，选择为故障转移通信保留足够带宽的 **接口** 。

注释
只有没有逻辑名称且不属于安全区域的接口将在 **添加高可用性对** 对话框的 **接口** 下列列表中列出。

步骤 9 键入任何识别**逻辑名称 (Logical Name)**。

步骤 10 为主用设备上的故障切换链路键入**主要 IP (Primary IP)** 地址。

此地址应处于未使用的子网上。

注释
169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

步骤 11 或者，选择**使用 IPv6 地址 (Use IPv6 Address)**。

步骤 12 为备用设备上的故障切换链路键入**辅助 IP (Secondary IP)** 地址。此 IP 地址必须与主要地址在同一子网中。

步骤 13 如果使用 IPv4 地址，请键入适用于主要和辅助 IP 地址的**子网掩码 (Subnet Mask)**。

步骤 14 或者，在**状态性故障切换链路 (Stateful Failover Link)** 下，选择同一**接口**，或选择不同的接口并输入高可用性配置信息。

注释
169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

步骤 15 （可选） 选择**已启用**并为故障转移链路间的 IPsec 加密选择**密钥生成**方法。

步骤 16 点击**确定**。由于此过程会同步系统数据，因此需要花费几分钟时间。

配置成功后，建立高可用性对，其中一台设备为活动状态，另一台为备用状态。。

下一步做什么

备份设备。您可以使用备份在设备发生故障时快速更换设备，并在不断开与防火墙管理中心的连接的情况下恢复高可用性服务。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南。

配置可选高可用性参数

您可以在 防火墙管理中心上查看初始高可用性配置。您无法在不破坏高可用性对，然后重新建立它的情况下编辑这些设置。要编辑这些设置，必须先中断高可用性对，然后重新建立它。您可以修改故障切换触发条件，以改进故障切换结果。接口监控可帮助您确定哪些接口最适合于故障切换。

配置备用 IP 地址和接口监控

为高可用性接口配置备用 IP 地址，以使主用设备能够执行网络测试并检查备用接口运行状况，而不仅仅是跟踪链路状态。

为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

默认情况下，所有命名物理接口均启用监控，而对于200/10101210/1220，所有VLAN接口也会启用监控。您可能希望排除连接到非关键网络的接口，以免影响故障转移策略。交换机端口无法进行接口监控。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** (✎)。

步骤 3 点击**高可用性 (High Availability)** 选项卡。

步骤 4 在**监控的接口**区域中，点击要编辑的接口旁边的 **编辑** (✎)。

步骤 5 选中**监控此接口的故障情况**复选框。

步骤 6 在 **IPv4** 选项卡上，输入**备用 IP 地址**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。

步骤 7 如果手动配置了 IPv6 地址，请在 **IPv6** 选项卡上，点击活动 IP 地址旁边的 **编辑** (✎)，输入**备用 IP 地址**，然后点击**确定**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。对于自动生成的地址和**强制 EUI 64** 地址，系统会自动生成备用地址。

步骤 8 点击**确定**。

编辑高可用性故障切换条件

此任务允许自定义高可用性设备对的故障转移条件，以匹配特定的网络部署要求。

您可以根据网络部署自定义故障切换条件。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**高可用性**。

步骤 4 在**故障切换触发条件 (Failover Trigger Criteria)** 旁边，点击 **编辑** ()。

步骤 5 在**接口故障阈值 (Interface Failure Threshold)** 下，选择在设备进行故障切换之前必须出现故障的接口数目或百分比。

步骤 6 在**呼叫数据包间隔 (Hello packet Intervals)** 下，选择通过故障切换链路发送呼叫数据包的频率。

步骤 7 点击**确定**。

配置虚拟 MAC 地址

配置主用和备用 MAC 地址，最大限度减少故障转移期间的流量损失，并为故障转移提供针对 IP 地址映射的冗余。

可以在 Secure Firewall Management Center上使用以下方法配置主用和备用 MAC 地址以进行故障切换：

- 配置接口期间在 **编辑接口** 页面的 **高级**选项卡；请参阅 配置 MAC 地址。
- 从 **高可用性** 页面访问的 **添加接口 MAC 地址**页面；请参阅此程序。

注释 要在主设备和辅助设备中配置 MAC 地址（以便将 MAC 地址传输到两台高可用性设备的所有子接口），建议使用 **接口** 选项卡在两个设备上复制子接口上的 MAC 地址主用和备用高可用性设备。

如果在两个位置都配置了主用和备用MAC地址，则在配置接口期间定义的地址优先进行故障切换。

通过将主用和备用 MAC 地址指定到物理接口，可以最大限度地减少故障切换期间的流量损失。此功能为故障切换提供了针对 IP 地址映射的冗余。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 点击**高可用性 (High Availability)**。

步骤 4 点击接口 Mac 地址旁边的 **添加** () 图标。

步骤 5 选择**物理接口**。

步骤 6 输入**主用接口 MAC 地址**。

步骤 7 输入**备用接口 MAC 地址**。

步骤 8 点击**确定**。

注释
有关详细信息，请参阅 任务 2， 在 Firepower 设备上配置 FTD 高可用性中的步骤 10 到 14。

管理

本部分介绍您在启用后如何管理，包括如何更改设置以及如何强制从一台设备故障转移到另一台设备。

在 Firewall Threat Defense 高可用性对中切换主用对等体

此任务允许您手动切换高可用性对中的主用和备用设备，从而有效地强制进行故障转移，例如当前主用设备出现持续故障或运行状况事件。

在建立 Firewall Threat Defense 高可用性对以后，可以手动切换主用和备用设备，出于持续性故障或运行状况事件等原因有效执行故障切换。两台设备应该已经完全部署，然后才能完成此程序。

Before you begin

刷新单个 Firewall Threat Defense 高可用性对的节点状态， 第 30 页。这样可以确保 Firewall Threat Defense 高可用性设备对上的状态与 防火墙管理中心 上的状态同步。

请按照以下步骤切换高可用性对中的主用节点：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要更改主用对等体的高可用性对旁边，点击**切换主用对等体 (Switch Active Peer)**。

步骤 3 选择一个选项：

- 点击**是**将使备用设备立即变成高可用性对中的主用设备。
- 点击 **No** 将取消并返回到 Device Management 页面。

刷新单个 Firewall Threat Defense 高可用性对的节点状态

当通信问题导致数据不同步时，刷新高可用性节点状态以获取有关高可用性对中主用设备和备用设备的准确信息。

每当重新引导 Firewall Threat Defense 高可用性对中的主用或备用设备时， 防火墙管理中心 可能不会显示这两种设备的准确高可用性状态。这是因为，当设备重新引导时，高可用性状态会在设备上立即更新，其相应的事件将会发送到 防火墙管理中心。但是，状态可能不会在 防火墙管理中心 上更新，因为设备和 防火墙管理中心 之间的通信尚未建立。

防火墙管理中心 与设备之间出现通信故障或通信隧道信号弱，可能会导致数据不同步。切换高可用性对中的主用设备和备用设备时，即使持续很长时间，这种更改可能也不会反映在 防火墙管理中心 中。

在此类情况下，可以刷新高可用性节点状态以获取有关高可用性对中主用设备和备用设备的准确信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在希望刷新节点状态的高可用性对旁边，点击 **刷新 HA 节点状态**。

步骤 3 点击 **是** 来刷新节点状态。

暂停和恢复高可用性

当有用时，可以暂停高可用性对中的设备：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障转移。

当您暂停高可用性时，当前主用设备保持活动状态，并继续处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障转移到现在的伪备用设备。

使用数据接口进行管理器访问时，管理连接将断开，直到您恢复。

暂停高可用性和中断高可用性之间的主要区别是，在暂停的高可用性设备上将保留高可用性配置。如果中断高可用性，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

要暂停高可用性，请使用 **configure high-availability suspend** 命令。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。备用设备接口配置也会被清除。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障转移至暂停的设备。

要恢复故障转移，请使用 **configure high-availability resume** 命令。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。

注释 暂停高可用性是一种临时状态。如果您重新加载一台设备，它会自动恢复高可用性配置，并与对等体协商主用/备用状态。

更换 Firewall Threat Defense 高可用性对中的设备

本参考介绍在 Firewall Threat Defense 高可用性对中更换故障设备的流程，包括备份恢复和手动更换程序。

要使用备份文件替换 Firewall Threat Defense 高可用性对中的故障设备，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 恢复 防火墙管理中心和托管设备 。

如果没有故障设备的备份，则必须中断高可用性。然后，将替换设备注册到 Secure Firewall Management Center 并重新建立高可用性。该过程会因设备是主设备还是辅助设备而有所不同：

- 将主 Firewall Threat Defense 高可用性设备替换为无备份 ， 第 31 页
- 将辅助 Firewall Threat Defense HA 单元更换为无备份 ， 第 32 页

将主 Firewall Threat Defense 高可用性设备替换为无备份

此任务将替换 Firewall Threat Defense 高可用性对中出现故障的主设备，以恢复冗余并维持网络保护。

按照这些步骤更换 Firewall Threat Defense 高可用性对中出现故障的主设备。如果无法执行这些步骤，系统可能会覆盖现有的高可用性配置。

注意 创建或中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

注意 切勿在未重新映像磁盘的情况下将磁盘从传感器或防火墙管理中心移动到其他设备。这是不受支持的配置，可能会导致功能中断。

过程

步骤 1 选择**强制中断**以分隔高可用性对；请参阅中断高可用性对 ， 第 33 页。

注释
中断操作会从 Firewall Threat Defense 和 防火墙管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 防火墙管理中心取消注册主 Firewall Threat Defense 设备；请参阅 从 防火墙管理中心 取消注册设备。

步骤 3 将替换 Firewall Threat Defense 注册到 防火墙管理中心；请参阅 向管理中心注册。

步骤 4 配置高可用性，在注册期间使用现有的辅助/主用设备作为主设备，并将更换设备用作辅助/备用设备；请参阅添加高可用性对 ， 第 24 页。

将辅助 Firewall Threat Defense HA 单元更换为无备份

此任务允许您通过更换 Firewall Threat Defense 高可用性对中出现故障的辅助设备来恢复高可用性功能。

当高可用性配置中的辅助设备发生故障时，您需要更换该设备并重新创建 HA 对，以维持网络冗余和保护。

注意 创建或中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

过程

步骤 1 选择**强制中断**以分隔高可用性对。

请参阅中断高可用性对，第 33 页。

注释
中断操作会从 Firewall Threat Defense 和 防火墙管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 防火墙管理中心 取消注册辅助 Firewall Threat Defense 设备。

请参阅从 防火墙管理中心 取消注册设备。

步骤 3 将替换 Firewall Threat Defense 注册到 防火墙管理中心。

请参阅向管理中心注册。

步骤 4 在注册期间使用现有主/主用设备作为主设备并将替换设备作为辅助/备用设备配置高可用性。

请参阅添加高可用性对，第 24 页。

中断高可用性对

中断高可用性对，以从两台设备中删除高可用性配置，同时保持主用设备上的流量。

中断高可用性对时，将从两台设备中删除高可用性配置。

使用管理接口进行管理器访问时： 主用设备保持运行并传递流量。备用设备接口配置被清除。

使用数据接口进行管理器访问时： 请参阅以下详细信息。

- 主用设备保持运行并传递流量。
- 备用设备的数据接口将关闭，但管理器访问接口除外，该接口使用备用 IP 地址保持运行，因此可以维护管理连接。
- 在远程分支机构部署设置中，所有分配了逻辑名称的备用机数据接口都会关闭，但管理器访问接口除外，因为管理器访问接口仍处于运行状态，以保持管理连接。
- 如果主设备处于备用状态：
  - 管理器访问的 IP 地址在 防火墙管理中心 配置中永久交换：主设备使用备用 IP 地址，辅助设备使用主用 IP 地址。
  - 如果 防火墙管理中心 发起了管理连接，并且您为设备指定了主机名，则需要更新 DNS 服务器，以便将交换的 IP 地址与正确的主机名关联。

- 中断高可用性会导致部署到备用设备。如果由于IP地址交换而尚未重新建立管理连接，则部署可能会失败。在这种情况下，您需要稍后（在建立管理连接后）手动触发部署。在将更改部署到主用设备之前，请务必完成备用部署。

在断开操作之前尚未部署到主用设备的策略，在断开操作完成后仍会保持未部署状态。请在断开操作完成后，在独立设备上部署这些策略。

注释

- 在 Firewall Threat Defense 设备上的高可用性接口上启用 IPsec 时，设备无法确定进入高优先级接收队列的加密数据包的优先级。因此，在高数据流量场景下，尝试中断高可用性可能会失败，因为设备无法有效管理大量加密连接并确定其优先级。要查看设备的资源使用情况和最大吞吐量，请使用 显示资源使用 命令。
- 如果无法使用 防火墙管理中心访问高可用性对，请连接到每台设备上的 CLI 并输入 **configure high-availability disable** 以手动中断高可用性。另请参阅取消注册高可用性对和注册新 防火墙管理中心，第 35 页。

注意 中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

Before you begin

- 刷新单个 Firewall Threat Defense 高可用性对的节点状态，第 30 页。这样可以确保高可用性设备对上的状态与 防火墙管理中心上的状态同步。

按照以下步骤中断高可用性对：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要中断的高可用性对旁边，点击 **更多** (⋮) 并选择**中断 (Break)**。

步骤 3 如果备用对等体没有响应，请选中 **强制中断**。

步骤 4 点击 **Yes**。

断开操作将从主用和备用设备中删除高可用性配置。

在主用设备上部署的 FlexConfig 策略可能会在中断高可用性操作后显示部署失败。您必须在主用设备上修改并重新部署 FlexConfig 策略。

下一步做什么

如果在主用设备上使用 FlexConfig 策略，请修改并重新部署 FlexConfig 策略以消除部署错误。

注释 中断高可用性后，作为主用设备运行的 Firewall Threat Defense 设备仍将在其配置中列出备用设备的 IP 地址。要解决此问题，请在以前主用 Firewall Threat Defense 设备上执行其他部署，以从其配置中删除备用设备的 IP 地址。

取消注册高可用性对和注册新 防火墙管理中心

此任务允许您从防火墙管理中心中取消注册高可用性配对，从而保持高可用性配对的完整性。如果要将其注册到新的防火墙管理中心或无法再访问该对，则防火墙管理中心可能需要取消注册该对。

取消注册高可用性对：

- 会切断 防火墙管理中心 和该对之间的所有通信。
- 从 **设备管理** 页面删除对。
- 如果对的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将对返回本地时间管理。
- 保持配置不变，以便设备对继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

再次向相同或不同的 防火墙管理中心 注册该对会导致配置被删除，因此该对将在该点停止处理流量；高可用性配置保持不变，因此您可以将其作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

Before you begin

- 此过程需要 CLI 对主节点 拥有访问权限。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要注销的高可用性对旁边，点击 **更多** (⋮) 并选择**取消注册 (Unregister)**。

步骤 3 点击**是 (Yes)**。设备高可用性对随即会被注销。

步骤 4 您可以通过将主设备添加为新设备来将该对注册到新的（或相同的） 防火墙管理中心 。

a) 通过连接到一台设备上的 CLI 并输入 **show failover** 命令来确定主设备。

输出的第一行显示此设备是主设备还是辅助设备。

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) 在主设备的 CLI 中，使用 **configure manager add** 命令识别新 防火墙管理中心 。请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口。

c) 选择 **设备** > **设备管理**，然后点击**添加** > **设备**。

您只需将主设备添加为设备， 防火墙管理中心 即可发现辅助设备。

监控

监控 是一种系统功能，可让您查看 状态。

查看故障切换历史记录

在单个视图中查看高可用性设备的故障转移历史记录，了解故障转移事件的时间顺序及其原因。

您可以在单个视图中查看两个高可用性设备的故障切换历史记录。历史记录按时间顺序显示，并包括任何故障切换的原因。

Before you begin

按照以下步骤查看故障转移历史记录：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**摘要**。

步骤 4 在“常规”(General) 下，点击 **视图** ()。

查看状态故障切换统计信息

通过此任务，可以通过监控状态故障切换链路统计信息来评估高可用性配置的性能和运行状况。

您可以在高可用性对中查看主设备和辅助设备的状态故障切换链路统计信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**高可用性**。

步骤 4 在“状态故障切换链路”(Stateful Failover Link) 下，点击 **视图** ()。

步骤 5 选择一个设备来查看统计信息。

配置同步失败故障排除

形成故障转移对时，加入设备会清除其运行配置并从主用设备复制整个配置。完成完整配置同步后，加入设备将承担备用就绪角色并建立故障切转移。设备加入故障转移对后，主用设备上的任何配置更改也会复制到备用设备上，以保持两台设备同步。

如果备用设备无法复制任何配置更改命令，它会报告配置同步失败并通过禁用故障转移退出高可用性。本节介绍备用设备报告的配置同步失败错误的识别和故障转移步骤。

要查看配置同步错误或统计信息，您可以通过 SSH 会话或威胁防御 CLI 使用这些 CLI 命令：

- **show failover config-sync errors all** 显示与故障转移相关的所有配置同步错误。
- **show failover config-sync stats all** 查看有关故障转移配置同步的统计信息。

要重新启用高可用性，请执行以下操作：

- 通过在主用设备上执行 **failover reset** 命令来重新启用故障转移。
- 如果重新启用故障转移不成功，请删除或更新备用设备无法复制的配置更改，然后重新启用故障转移。

注释 如果达到最大接口限制，主用设备和备用设备上的VPN隧道数可能不一致。这种情况下，在主用设备上运行**write standby**命令以同步配置。

高可用性历史记录

本参考提供了按时间顺序排列的在各种软件版本中实施的高可用性功能、增强功能和改进的历史记录。这些信息有助于您跟踪高可用性功能的发展，并了解各项功能的引入时间。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
改进了故障转移期间的角色切换时间	7.7	7.7	发生故障转移时，新的活动设备会为每个 MAC 地址条目生成组播数据包，并将其发送到所有网桥组接口，从而促使上游交换机更新路由表。生成组播数据包并将其发送到网桥接口的任务现在可以在数据平面中异步运行，从而使控制平面中的关键故障转移任务能够无延迟地进行。此增强功能可缩短故障转移期间的角色切换时间，并减少停机时间。
管理器访问数据接口的高可用性支持	7.4	7.4	您现在可以使用数据接口进行 Firewall Threat Defense 高可用性管理器访问。
取消注册高可用性对现在可以在不中断高可用性对的情况下重新注册	7.3	任意	删除（取消注册）高可用性对时，无需再在 CLI 中手动断开配对并重新注册独立设备。您现在可以将主设备添加到新防火墙管理中心，系统将自动发现备用设备。重新注册该对仍将清除配置，并且您的策略将需要重新应用。
策略支持回滚以实现高可用性	7.2	任意	**configure policy rollback** 命令支持高可用性。
配置同步优化功能可实现更快的高可用性对	7.2	任意	配置同步优化功能通过交换配置散列值来比较加入设备和主用设备的配置。如果在主用设备和加入设备上计算的散列值匹配，则加入设备将跳过完全配置同步并重新加入 HA。此功能可实现更快的 HA 对等，并缩短维护窗口和升级时间。
改进了集群和高可用性设备的升级工作流程。	7.1	任意	我们改进了集群与高可用性设备的升级流程： • 升级向导现在可以将集群和高可用性设备正确显示为组，而不是单个设备。系统可以识别、报告和预先要求修复您可能遇到的组相关问题。例如，如果您在 Firepower 机箱管理器上进行了未同步的更改，则无法升级 Firepower 4100/9300 上的集群。 • 我们提高了将升级包复制到集群和高可用性对的速度和效率。以前，FMC 会按顺序将数据包复制到每个组成员。现在组成员可在正常同步过程中互相获取软件包。 • 您现在可以指定集群中数据设备的升级顺序。控制设备始终最后升级。
清除高可用性组或集群中的路由。	7.1	任意	在以前的版本中， **清除路由** 命令仅清除设备上的路由表。现在，在高可用性组或集群中运行时， 命令仅在主用或控制设备上可用，并清除组或集群中所有设备上的路由表。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
FTD 高可用性加固	6.2.3	任意	版本 6.2.3 为高可用性中的 FTD 设备引入了以下功能： • 每当重启高可用性对中的主用或备用 FTD 设备时， 可能不会显示这两种托管设备的准确高可用性状态。但是，状态可能不会在FMC上更新，因为设备和 FMC 之间的通信尚未建立。通过 **设备** > **设备管理** 页面上的 **刷新节点状态** 选项，可以刷新高可用性设备状态以获取有关高可用性对中主用设备和备用设备的准确信息。 • FMC UI 的 **设备** > **设备管理** 页面上有一个新的 **交换机活动对等体** 图标。 • 版本 6.2.3 包括一个新的 REST API 对象、**设备高可用性对服务**，其中包含四个功能： • 删除 **ftddevicehapairs** • **PUT ftddevicehapairs** • **POST ftddevicehapairs** • **GET ftddevicehapairs**

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。

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。

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。