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 威胁防御 的高可用性。

关于 Cisco Secure Firewall Threat Defense高可用性

配置高可用性需要两台相同的 威胁防御设备，二者之间通过专用故障切换链路和（可选）状态链路彼此互连。威胁防御支持主用/备用故障切换，其中一台设备为传递流量的主用设备。备用设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。发生故障切换时，主用设备会故障切换到备用设备，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切换条件。如果符合这些条件，将执行故障切换。

注释 在公共云中运行的 threat defense virtual不支持高可用性。

远程分支机构部署中 威胁防御 设备上的高可用性支持

在远程分支机构部署中，威胁防御 设备的数据接口会被用于管理 思科防御协调器，而不是设备上的管理接口。由于大多数远程分支机构都只有一个互联网连接，因此外部CDO访问让集中管理成为了可能。

您可以将任何数据接口用于 CDO 访问，例如，如果您有内部 CDO，则使用内部接口。但是，本指南主要介绍外部接口访问，因为它是远程分支机构最可能遇到的场景。

CDO 可在其通过数据接口管理的 威胁防御 设备上提供高可用性支持。运行 7.2 或更高版本软件的设备支持此功能。

有关详细信息，请参阅《思科 Firepower 入门指南》中的使用远程 *FMC* 部署 *Firepower* 威胁防御。

高可用性系统要求

本部分介绍在高可用性配置中对于威胁防御 设备的硬件、软件和许可证要求。

硬件要求

高可用性配置中的两台设备必须：

- 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，高可用性仅在同种类型模块之间受支持；但是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 CDO 后更改资源配置文件，则稍后应在**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **系统 (System)** > **清单 (Inventory)**对话框中更新每个设备的清单。

- 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。高可用性如果您在启用高可用性后更改接口，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。

- 在远程分支机构部署中包含以下设置：
  - 具有处理远程部署中管理流量的相同数据管理接口。

    例如，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。

  - 将数据管理接口用于管理通信。

    不能让一台设备使用数据接口进行管理，而另一台设备却使用管理接口进行管理。

如果在高可用性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

高可用性 配置中的两台设备必须：

- 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 威胁防御 设备的许可证要求

高可用性配置中的两台 威胁防御 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，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 基本 许可证和 威胁 许可证，而备用设备只有 基本 许可证， 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 威胁 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

故障切换链路和可选的有状态故障切换链路是两台设备之间的专用连接。思科建议在故障切换链路或状态故障切换链路中的两台设备之间使用同一接口。例如，在故障切换链路中，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。

故障转移链路

故障切换对中的两台设备会不断地通过故障切换链路进行通信，以便确定每台设备的运行状态。

故障切换链路数据

以下信息将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

故障切换链路接口

您可以使用未使用的数据接口（物理接口 EtherChannel 接口）作为故障切换链路；但不能指定当前已配置名称的接口。 如果接口被配置为与 CDO 通信，则您无法使用数据管理接口。 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）。

威胁防御用户数据和故障切换链路之间共享接口。您也不能在同一父接口上使用单独的子接口用于故障切换链路和数据（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。

请参阅下列有关故障切换链路的指南：

- Firepower 4100/9300- 我们建议您将一个 10 GB 数据接口用于组合的故障切换和状态链路。
- 所有其他型号 - 1 GB 接口对于组合的故障切换和状态链路而言已足够大。

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。

对于用作故障切换链路的 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。

连接故障切换链路

您可以使用以下两种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 威胁防御 设备的故障切换接口。
- 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，当接口出现故障时，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。

状态故障转移链路

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

共享故障切换链路

共享故障切换链路是节约接口的最佳方式。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。

状态故障切换链路的专用接口

您可以将专用接口（物理或 EtherChannel）用于状态链路。有关专用状态链路的要求，请参阅故障切换链路接口，第 3 页，以及有关连接状态链路的信息，请参阅连接故障切换链路，第 4 页。

使用长距离故障转移时，为实现最佳性能，状态链路的延迟应低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障转移消息会导致一些性能降级。

避免中断故障转移和数据链路

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。如果故障转移链路发生故障，威胁防御设备可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被暂停，直到故障转移链路恢复正常。

请参阅以下连接情景，以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 威胁防御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 威胁防御设备都将处于主用状态。因此，建议**不要**使用下图中显示的 2 种连接方法。

图 *1:* 使用单交换机连接❖❖❖不推荐

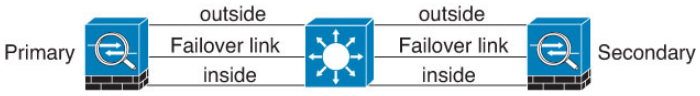
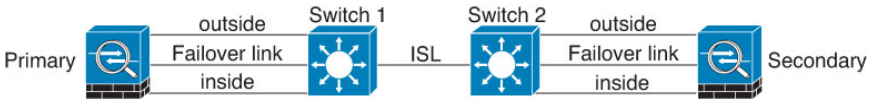


图 *2:* 使用双交换机连接 - 不推荐



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

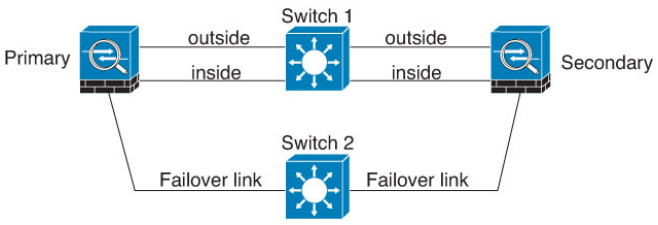
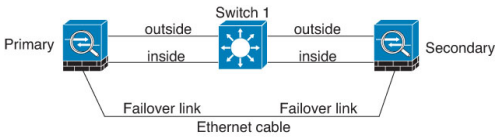


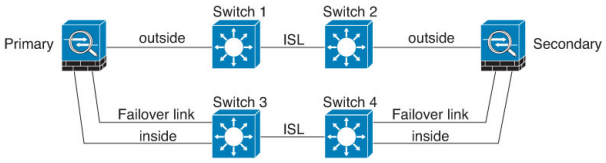
图 *4:* 通过电缆连接



情景 3 - 推荐

如果 威胁防御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



情景 4 - 推荐

最可靠的故障转移配置使用故障转移链路上的冗余接口，如下图所示。

图 *6:* 使用冗余接口连接

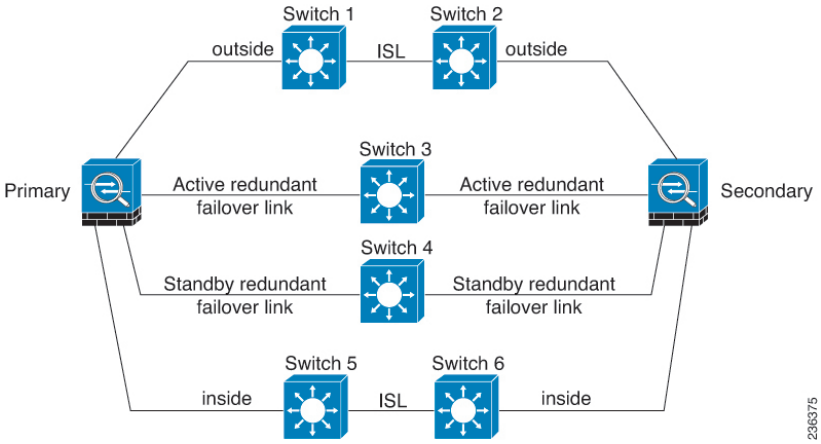
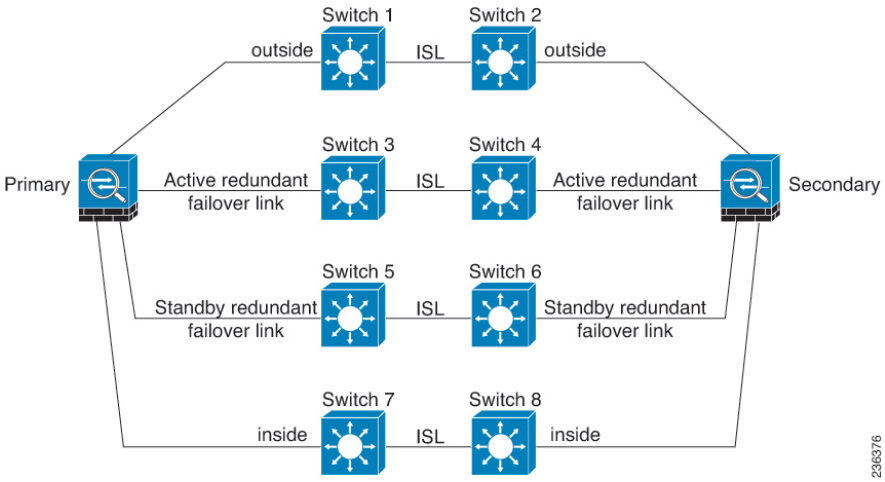


图 7: 使用交换机间链路连接



高可用性中的 MAC 地址和 IP 地址

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 IP 地址和 MAC 地址

对于主用/备用高可用性，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切换时，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。

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。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，威胁防御设备不会发送静态 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。

虚拟 MAC 地址

威胁防御设备 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。

状态故障切换

状态故障切换期间，主用设备会不断将每个连接的状态信息发送至备用设备。发生故障切换之后，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

对于状态故障转移，以下状态信息会传送至备用 威胁防御设备：

- 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复制到备用 ASA 上。

不支持的功能

对于状态故障转移，以下状态信息不会传送至备用 威胁防御设备：

- 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。
- TCP 状态绕行连接
- 组播路由。

高可用性的桥接组要求

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，则端口最终会转换为 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。

故障切换运行状态监控

威胁防御 设备会监控每台设备的整体运行状态和接口运行状态。此部分包括有关 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

威胁防御 设备会通过 Hello 消息监控故障切换链路，进而确定其他设备的运行状况。当设备在故障切换链路上没有收到三条连续的 Hello 消息时，设备将在每个数据接口（包括故障切换链路）上发送接口 LANTEST 消息，来验证对等体是否响应。威胁防御 设备采取的操作取决于来自其他设备的响应。请参阅以下可以执行的操作：

- 如果 威胁防御 设备在故障切换链路上收到响应，则不会进行故障切换。
- 如果 威胁防御 设备在故障切换链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障切换。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 威胁防御 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。

接口监控

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。

如果满足为故障接口数量定义的阈值（请参阅命令，或者对于主用/主用故障切换，请使用命令）（请参阅配置设备管理高可用性和可扩展性故障切换标准接口策略）（请参阅设备设备管理高可用性故障切换）触发条件（Trigger Criteria）），并且主用设备的故障接口比备用设备多，则发生故障切换。> > > 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切换接口政策制定的故障切换限制。

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

威胁防御 设备使用以下接口测试。默认情况下，每个测试的持续时间约为1.5秒。

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

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Normal (Waiting) - 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。
- Normal (Not-Monitored) - 接口已打开，但未受故障切换进程监控。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- Link Down (Waiting) - 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。
- Link Down (Not-Monitored) - 接口或 VLAN 已通过管理方式关闭，但未受故障切换进程监控。
- No Link - 接口的物理链路关闭。
- No Link (Waiting) - 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。
- No Link (Not-Monitored) - 接口的物理链路已关闭，但未受故障切换进程监控。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

故障切换触发器和检测时间

以下事件会在 Firepower 高可用性对中触发故障切换：

- 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切换而必须发生故障的受监控接口的百分比来更改默认值。如果在主用设备上达到阈值，则会发生故障切换。如果备用设备上的阈值超出阈值，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以下命令：

表 *1:*

命令	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	更改默认故障切换条件。 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。

下表列出了故障切换触发事件及关联的故障检测时间。如果出现故障切换，您可以在消息中心中查看故障切换的原因，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 *2:* 威胁防御故障切换时间

故障切换触发事件	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，受监控接口或故障切换链路不会收到任何 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

关于主用/备用故障转移

主用/备用故障转移允许您使用备用 威胁防御设备来接管故障设备的功能。当主用设备发生故障时，备用设备将变为主用设备。

主/辅助角色和主用/备用状态

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

主用设备按以下方式确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备会成为备用设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备用设备。

故障转移事件

在主用/备用故障转移中，故障转移会在设备级别进行。

下表显示了每个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 *3:* 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。
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切换，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。

故障事件	策略	主用设备操作	备用设备操作	说明
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切换，即使超过接口故障阈值也是如此。

高可用性的要求和前提条件

型号支持

Cisco Secure Firewall Threat Defense

支持的域

任意

用户角色

管理员

高可用性指南

型号支持

- Firepower 1010：
  - 使用高可用性时，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。高可用性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 高可用性网络设置中，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。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
  - 仅可使用防火墙接口作为故障转移链路。

注释 在 6.5 或更高版本由 管理中心 6.5 或更高版本新安装和管理的 Firepower 1010 设备上，默认接口将为交换机端口类型。由于故障切换不支持交换机端口功能，请关闭这些接口上的交换机端口，执行部署，然后创建故障切换。对于从 6.5 之前的版本升级的 Firepower 1010 系统，默认接口将与之前版本中的相同。

- Firepower 9300 - 不支持机箱内高可用性。
- 由于需要第 2 层的连接，因此不支持高可用性在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 threat defense virtual。

其他规定

- 当主用设备故障切换到备用设备时，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。

- 发生故障切换事件时，在连接到 威胁防御设备故障切换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 高可用性和 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。
- 故障切换后，系统日志消息的源地址将立即成为故障切换接口地址几秒钟。
- 为了更好地融合（在故障切换期间），您必须关闭 HA 对上未与任何配置或实例关联的接口。
- 如果您在评估模式下配置 HA 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。
- 当使用具有故障切换功能的 SNMPv3 时，如果更换故障切换设备，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。
- 威胁防御 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。
- 转换为备用角色的高可用性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
```

- 高可用性（故障切换）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 HA 对。
  - HA 已中断并已重新创建。
  - 故障切换链路上的通信中断并重新建立。
  - 已使用 **no failover/failover** 或 **configure high-availability suspend/resume** (威胁防御 CLISH) 命令来手动更改故障切换状态。
- 在平台上运行的 ASA/威胁防御 HA 对中，同步仅适用于 ASA/威胁防御 等应用，而不适用于机箱。
- 启用 HA 会强制删除所有路由，并会在 HA 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。
- 在使用管理中心或设备管理器创建威胁防御高可用性期间，所选辅助威胁防御设备上的所有现有配置都将替换为从所选主要威胁防御设备复制的配置，因此在高可用性期间请谨慎选择主设备（ HA) 创建。例如，如果在现有主设备出现故障并使用退货授权 (RMA) 进行更换时，HA 被破坏并重新创建，则在创建 HA 期间，应选择更换设备作为辅助设备，以便从所选的主设备将被复制到替换设备。

添加 威胁防御 高可用性对

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。系统会将合并的配置应用于配对设备。如果存在冲突，则系统会应用已指定为主设备的设备中的配置。

注释 系统使用故障切换链路同步配置，而使用状态故障切换链路同步对等体之间的应用内容。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 威胁防御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，取决于目标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。

开始之前

确认两台设备：

- 型号相同。
- 拥有相同数量和类型的接口。
- 具有处理远程部署中管理流量的相同数据接口。例如，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。
- 将静态 IP 地址分配给处理远程部署管理流量的数据接口。
- 在远程部署中具有兼容的 IPv6 地址。数据托管接口上的辅助 IPv6 地址列表大小应与主 IPv6 地址列表大小匹配。
- 在远程部署中具有相同的 IPV6 地址前缀。主设备中的每个 IPv6 地址前缀都应与辅助 IPv6 地址列表中的一个完全匹配。
- 请勿在远程部署中为 IPv6 地址启用 EUI 64 选项。如果为任何设备启用此选项，则高可用性创建失败。
- 在远程部署中具有同一子网中的 IP 地址。
- 为它们分配不同的 IP 地址。
- 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 远程部署仅支持路由模式。

- 具有相同的 NTP 配置。请参阅为威胁防御配置 NTP 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。

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 威胁防御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 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡并选择要建立为主设备的设备。

步骤 4 在 **管理** 窗格中，点击 **高可用性**。

步骤 5 为高可用性对输入显示**名称 (Name)**。

步骤 6 在**设备类型 (Device Type)** 下，选择 **Firepower 威胁防御 (Firepower Threat Defense)**。

步骤 7 为高可用性对选择**主对等 (Primary Peer)** 设备。

步骤 8 为高可用性对选择**辅助对等 (Secondary Peer)** 设备。

注释 在远程部署中， **辅助对等体** 列表中显示的设备取决于在 **主对等体** 列表中选择的主用设备：

- 如果选定的主要对等体使用数据接口进行管理，则辅助对等体列表中仅列出数据接口受管设备。
- 如果主对等体上的数据管理接口配置了 IPv4 地址，则辅助对等体仅列出配置了 IPv4 地址的数据接口受管设备。相同的规则也适用于 IPv6 管理的设备。
- 主设备和辅助设备的数据管理接口名称应相同。具有不同接口名称的设备不会列在辅助对等体列表中。

步骤 9 点击**继续 (Continue)**。

步骤 10 在 LAN 故障切换链路下，选择为故障切换通信保留足够带宽的**接口 (Interface)**。

注释 只有没有逻辑名称，不属于安全区域且不用于处理管理流量的接口将在 **添加高可用性对** 对话框的 **接口** 下列列表中列出。

步骤 11 键入任何识别**逻辑名称 (Logical Name)**。

步骤 12 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。 此子网可以是 31 位 (255.255.255.254 或 /31) 的，仅包含两个 IP 地址。

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

步骤 13 或者，选择**使用 IPv6 地址 (Use IPv6 Address)**。

步骤 14 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 15 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 16 或者，在状态性故障切换链路下，选择同一**接口 (Interface)**，或选择不同的接口并输入高可用性配置信息。

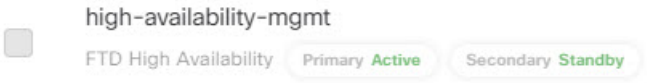
此子网可以是 31 位 (255.255.255.254 或 /31) 的，仅包含两个 IP 地址。

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

步骤 17 或者，选择**已启用 (Enabled)** 并为故障切换链路之间的 IPsec 加密选择**密钥生成 (Key Generation)** 方法。

步骤 18 点击 **OK**。由于此过程会同步系统数据，因此需要花费几分钟时间。

成功配置后，您可以在 CDO **清单 (Inventory)** 页面上的 威胁防御 节点上看到 **FTD 高可用性 (FTD High Availability)** 标签。选择节点以查看您为实现高可用性而配置的主用和备用设备



。

下一步做什么

确保来备份设备。您可以使用备份在设备发生故障时快速更换设备，并在不断开与管理中心的连接的情况下恢复高可用性服务。

配置可选高可用性参数

您可以在 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。

您可以编辑故障切换触发条件，以改进故障切换结果。通过接口监控，您可以确定哪些接口更适合于故障切换。

配置备用 IP 地址和接口监控

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，在所有物理接口上启用监控，而对于 Firepower 1010 的所有 VLAN 接口，还会配置逻辑名称。您可能希望排除连接到非关键网络的接口，以免影响故障切换策略。Firepower 1010 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**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

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 (OK)**。

编辑高可用性故障切换条件

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**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

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。

注释 如果在 Firepower 2100 上使用远程访问 VPN，请使用默认 Hello 数据包间隔。否则，您可能会看到高 CPU 使用率，从而导致发生故障切换。

步骤 7 点击**确定 (OK)**。

配置虚拟 MAC 地址

可以在 Cisco Secure Firewall Management Center上的两个位置配置主用和备用 MAC 地址以进行故障切换：

- 配置接口期间“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

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**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 选择**高可用性**。

步骤 4 选择接口 Mac 地址旁边的 **添加**（）。

步骤 5 选择**物理接口**。

步骤 6 在**主用接口 Mac 地址**中键入相应的值。

步骤 7 在**备用接口 Mac 地址**中键入相应的值。

步骤 8 点击**确定 (OK)**。

管理高可用性

本部分介绍您在启用高可用性后如何管理高可用性，包括如何更改高可用性设置以及如何强制从一台设备故障切换到另一台设备。

在 威胁防御 高可用性对中切换主用对等体

在建立威胁防御高可用性对以后，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。

开始之前

刷新单个 威胁防御 高可用性对的节点状态 ，第 23 页。这样可以确保 威胁防御 高可用性设备对上的状态与 管理中心 上的状态同步。

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 您可以执行以下操作：

- 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 威胁防御 高可用性对的节点状态

每当重新引导 威胁防御 高可用性对中的主用或备用设备时， 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 管理中心。但是，状态可能不会在 管理中心 上更新，因为设备和 管理中心 之间的通信尚未建立。

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 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

可以暂停高可用性对中的设备。此功能适用于以下情形：

- 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切换。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障切换到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，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。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切换至暂停的设备。

要恢复故障切换，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 威胁防御 高可用性对中的设备

要使用备份文件替换 威胁防御 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 Cisco 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 威胁防御 高可用性设备替换为无备份 ， 第 24 页
- 将辅助 威胁防御 HA 单元更换为无备份 ， 第 25 页

将主 威胁防御 高可用性设备替换为无备份

按照以下步骤更换 威胁防御 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 威胁防御 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，取决于目标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 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；请参阅高可用性对中的独立设备，第 26 页。

注释 中断操作会从 威胁防御 和 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 管理中心注销出现故障的主 威胁防御 设备。

步骤 3 将替换 威胁防御 注册到 管理中心将设备载入 云交付的防火墙管理中心的前提条件。

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 威胁防御 高可用性对，第 17 页。

将辅助 威胁防御 HA 单元更换为无备份

按照以下步骤替换 威胁防御 高可用性对中出现故障的辅助设备。

注意 创建或中断 威胁防御 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，取决于目标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；请参阅高可用性对中的独立设备，第 26 页。

注释 中断操作会从 威胁防御 和 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 管理中心。

步骤 3 将替换 威胁防御 注册到 管理中心将设备载入 云交付的防火墙管理中心的前提条件。

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 威胁防御 高可用性对 ， 第 17 页。

高可用性对中的独立设备

断开高可用性对后，主用设备将保留所有已部署功能。备用设备将丢失故障切换和接口配置，并成为独立设备。

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。

提示 FlexConfig 策略例外。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。

注释 您无法使用 管理中心访问高可用性对，请使用 CLI 命令 **configure high-availability disable** 删除两个设备上的故障切换配置。

开始之前

- 刷新单个 威胁防御 高可用性对的节点状态 ， 第 23 页。这样可以确保 威胁防御 高可用性设备对上的状态与 管理中心 上的状态同步。

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 **中断高可用性**图标。

步骤 3 （可选）选中该复选框可以在备用对等体不响应时强制断开。

步骤 4 点击 **Yes**。系统分隔设备高可用性对。

断开操作将从主用和备用设备中删除故障切换配置。

下一步做什么

（可选）如果在主用设备上使用 flex-config 策略，请修改并重新部署 flex-config 策略以消除部署错误。

取消注册高可用性对

您可以从 管理中心中删除该对，并使用 CLI 禁用每个设备的高可用性。

开始之前

此过程需要 CLI 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 **删除**（ ）。

步骤 3 点击 **Yes**。设备高可用性对随即会被删除。

步骤 4 在每个设备上，访问 威胁防御 CLI，然后输入以下命令：

configure high-availability disable

如果不输入此命令，则无法重新注册这些设备并形成一个新的 HA 对。

注释 在更改防火墙模式之前输入此命令；如果更改该模式，则该设备以后将不会允许您输入 **configure high-availability disable** 命令，并且 管理中心无法在没有此命令的情况下重新形成高可用性对。

监控 高可用性

此部分用于监控高可用性状态。

查看故障切换历史记录

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。

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**（ ）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

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

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**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

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。

对远程分支机构部署中的高可用性中断进行故障排除

本部分介绍如何解决在远程部署中中断高可用性对时可能遇到的一些常见问题。

- 两台设备均处于主用-主用状态。
- 主设备或辅助设备已断开与 CDO 的连接，并且故障切换链路已无法运行。
- 辅助设备处于故障或禁用状态，并且已断开与 CDO 的连接。

如何中断处于主用-主用状态的高可用性对

远程部署中的两台设备均处于主用-主用状态，因为故障转移接口无法运行，并且它们停止了在其数据接口上接收响应。在这种情况下，两台设备都会使用其数据管理接口上的活动 IP 地址，而这样会导致设备和 CDO 之间的网络不稳定。

您可以通过登录设备 CLI 并在两台设备上使用“show failover state”命令来确定它们是否都处于主用模式。两台设备的设备状态均显示为“活动”，并且为两台设备分配了相同的活动 IP 地址。

注释 您可以尝试纠正故障转移接口以恢复两个对等体之间的通信，然后执行**强制中断**操作。

如果无法修复故障转移接口的连接问题，请执行以下步骤：

过程

步骤 1 在两台设备中确定要从网络中删除的设备。

步骤 2 通过控制台端口或使用 SSH 连接至已确定设备的 CLI。

步骤 3 使用“管理员”(Admin) 用户名和密码登录。

步骤 4 输入 **pmtool disablebyid sftunnel** 命令。

注释 只能在思科技术支持中心的指导下使用 **pmtool** 命令。

步骤 5 断开所有接口与要从网络中删除的设备的连接。

步骤 6 输入 **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip_address* **interface***interface_id* 命令。

在 *ip_address* 中指定备用设备的 IP 地址。

示例：

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully..!!
```

步骤 7 输入 **configure high-availability suspend** 以暂停 HA。

```
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.
```

步骤 8 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 9 点击 **设备** 选项卡，找到您的设备。

步骤 10 点击 **FTD** 选项卡并选择主设备。

步骤 11 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 12 选择**设备 (Device)** > **设备管理 (Device Management)**。

步骤 13 在要分隔高可用性对的高可用性对旁边，点击**强制中断 (Force Break)**。

系统将显示一条消息，表明已成功分离高可用性对。

步骤 14 将所有接口连接到设备。

步骤 15 在 FTD CLI 中，输入 **pmtool enablebyId sftunnel**。

威胁防御设备会在某个时间与 CDO 建立连接。

注释 设备可能需要 5 分钟才能与 CDO 建立通信。

步骤 16 输入 **sftunnel-status-brief** 命令以查看管理连接状态。

```
sftunnel-status-brief
```

```
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Wed Feb 9 09:21:57 2020 UTC
Last disconnect time : Wed Feb 9 09:19:09 2020 UTC
```

步骤 17 选择**部署 (Deploy)** > **部署 (Deployment)** 以部署更改。

在 CDO 部署更改之前，它将检测配置差异并停止部署。CDO 会检测在防御协调器之外对设备进行的 IP 地址更改。

步骤 18 与 CDO 同步接口更改。请参阅与 管理中心同步接口更改。

步骤 19 现在，您可以将待处理的更改部署到设备。请参阅部署配置更改。。

设备现在成为了具有备用设备的新 IP 地址的独立设备。

下一步做什么

（可选）将所有待处理更改部署到具有主用设备 IP 地址的其他设备。

如何在主用或备用设备失去连接时中断高可用性对

问题：其中一个对等体断开与 管理中心 的连接，并且故障转移链路已无法运行。

表 *4:* 场景：

主设备状态	辅助设备状态	与 CDO 的主设备连接？	与 CDO 的辅助设备连接？	故障转移链路是否正常运行？（主设备和辅助设备之间的连接）
主用	待机	是	否	不支持
备用	主用	不支持	是	否

解决方案：

首先，您可以尝试纠正故障转移接口以恢复两个对等体之间的通信，然后执行中断或强制中断操作来分隔设备。

如果无法修复故障转移接口的连接问题，则必须在执行高可用性中断操作后使用设备 CLI 来完成其他步骤。

过程

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡并选择主设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 5 依次选择**设备** > **设备管理**。

步骤 6 在要中断的高可用性对旁边，点击**中断 HA (Break HA)**。

步骤 7 （可选）您也可以选中此复选框以便在其中一个对等体无响应时强制中断。

步骤 8 点击 **Yes**。

步骤 9 从 CDO 中删除备用设备。

a) 依次选择**设备** > **设备管理**。

b) 在要删除的设备旁，点击**删除 (Delete)**。

步骤 10 通过控制台端口或使用 SSH 连接至备用设备的 CLI。

步骤 11 使用“管理员”(Admin) 用户名和密码登录。

步骤 12 输入 **configure manager delete** 以删除管理器。

此命令将会禁用当前的管理器 CDO。

步骤 13 输入 **configure high-availability disable** 以删除故障转移配置并禁用设备上的数据管理接口。

步骤 14 输入 **configure network management-data-interface**。

示例：

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

新的网络设置会被分配给数据设备。

下一步做什么

如果需要，您可以将设备作为独立设备载入 CDO。

如何在辅助设备处于故障或禁用状态时中断高可用性对

问题：辅助设备处于故障或禁用状态，并且已断开与 CDO 的连接。此外，故障转移链路可能会运行，但也可能不会运行。

表 *5:* 场景：

主设备状态	辅助设备状态	与 CDO 的主设备连接？	与 CDO 的辅助设备连接？	故障转移链路是否正常运行？ （主设备和辅助设备之间的连接）
主用	失败	是	否	是/否
活动	已禁用	是	否	是/否

解决方案：

执行高可用性强制中断以便分隔设备，然后使用设备 CLI 从备用设备中删除配置，并让设备成为独立设备。

过程

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡并选择主设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 5 依次选择**设备** > **设备管理**。

步骤 6 在要中断的高可用性对旁边，点击**中断 HA (Break HA)**。

步骤 7 选中此复选框可在其中一个对等体无响应时强制中断。

步骤 8 点击 **Yes**。

步骤 9 从 CDO 中删除备用设备。

a) 依次选择**设备** > **设备管理**。

b) 在要删除的设备旁，点击**删除 (Delete)**。

步骤 10 通过控制台端口或使用 SSH 连接至备用设备的 CLI。

步骤 11 使用“管理员”(Admin) 用户名和密码登录。

步骤 12 输入 **configure high-availability disable** 以删除故障转移配置并禁用设备上的数据管理接口。

步骤 13 输入 **configure network management-data-interface**。

示例：

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

新的网络设置会被分配给数据设备。

下一步做什么

如果需要，您可以将设备作为独立设备载入 CDO。

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。