通过故障切换实现高可用性

本章介绍如何配置主用/备用或主用/主用故障切换来实现思科 ASA 的高可用性。

关于故障切换

配置故障切换需要通过专用故障切换链路和状态链路（可选）相互连接的两台相同的 ASA。主用单元和接口的运行状况会受到监控，以便确定它们是否满足特定故障切换条件的时刻。如果符合这些条件，将执行故障切换。

故障切换模式

ASA 支持两种故障切换模式，主用/主用故障切换和主用/备用故障切换。每种故障切换模式都有自己确定和执行故障切换的方法。

- 如发生主用/备用故障转移，其中一个设备是主用设备，并传递流量。第二台设备指定为备用设备，不会主动传送流量。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。您可以在单情景模式或多情景模式下为 ASA 使用主用/备用故障切换。
- 在主用/主用故障切换配置中，两台 ASA 均可传递网络流量。主用/主用故障切换仅在多情景模式下适用于 ASA。在主用/主用故障切换中，将 ASA 上的安全情景划分为 2 个故障切换组。故障切换组就是一个或多个安全情景的逻辑组。一个组被指定为主 ASA 上的活动组，另一个组被指定为辅助 ASA 上的活动组。发生故障切换时，会在故障切换组级别进行。

两种故障切换模式都支持状态或无状态故障切换。

故障切换系统要求

本部分介绍在故障切换配置中对于 ASA 的硬件、软件和许可证要求。

硬件要求

故障切换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-36 和 SM-44。可以在 SM-36 模块之间和 SM-44 模块之间创建高可用性对。

- 拥有相同数量和类型的接口。

  对于平台模式下的 Firepower 2100 和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。故障切换如果您在启用故障切换后更改接口，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 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

- 安装有相同的模块（如有）。

- 安装有相同的 RAM。

如果在故障切换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

故障切换 配置中的两台设备必须：

- 处于相同的情景模式（单情景或多情景）。

- 单一模式下：处于相同的防火墙模式（路由或透明）。

  在多情景模式下，防火墙模式在情景级别设置，您可以使用混合模式。

- 具有相同的主要（第一个数字）和次要（第二个数字）软件版本。但是，您可以在升级过程中临时使用不同的软件版本；例如，可以将一台设备从 8.3(1) 版本升级到 8.3(2) 版本，并使故障切换保持主用状态。我们建议将两台设备都升级为相同版本，以便确保长期的兼容性。

- 安装有相同的 AnyConnect 映像。如果在执行无中断升级时，故障切换对具有不匹配的映像，则无客户端 SSL VPN 连接会在升级过程的最终重新启动步骤终止，数据库会显示一个孤立会话，并且 IP 池会显示分配给客户端的 IP 地址“正在使用中”。

- 处于相同的 FIPS 模式下。
- （Firepower 4100/9300）具有相同的流量分流模式，同时启用或禁用。

许可证要求

故障切换配置下的两台设备不需要具有相同的许可证；许可证将整合为故障切换集群许可证。

故障切换和状态故障切换链路

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。

⚠

注意 除非您使用IPsec隧道或故障切换密钥保护通信，否则所有信息会以明文形式通过故障切换和状态链路发送。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果您使用 ASA 来端接 VPN 隧道，我们建议使用 IPsec 隧道或故障切换密钥来保护故障切换通信。

故障切换链路

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、子接口、冗余接口 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。故障切换链路接口不会配置为常规网络接口；该接口仅会因为故障切换而存在。该接口只能用于故障切换链路（还用于状态链路）。大多数型号不能使用管理接口进行故障切换，除非明确作出如下说明。

ASA 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。

请参阅下列有关故障切换链路的指南：

- 5506-X 至 5555-X - 不能使用管理接口作为故障切换链路；您必须使用数据接口。5506H-X 是唯一的例外情况，您可以在其中将管理接口用作故障切换链路。
- 5506H-X - 您可以使用管理 1/1 接口作为故障切换链路。如果配置该接口作为故障切换接口，您必须重新加载设备，更改才能生效。在这种情况下，您也不能使用 ASA Firepower 模块，因为该模块需要使用管理接口实现管理目的。
- 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。 不能使用管理类型接口作为故障切换链路。
- 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。

对于用作故障切换链路的冗余接口，请参见以下因提供更多冗余而带来的优势：

- 当故障切换设备启动时，它会在成员接口之间轮流检测主用设备。
- 如果故障切换设备在其中一个成员接口上停止从对等体接收保持连接消息，它将切换到另一个成员接口。

交替频率等于设备保持时间（**failover polltime unit** 命令）。

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 配置用作故障切换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 ASA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。

ASA在其铜缆以太网端口上支持自动 MDI/MDIX，因此您可以使用交叉电缆或直通电缆。如果使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

状态故障切换链路

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切换链路使用专用接口。

状态故障切换链路的专用接口

您可以将专用接口（物理、冗余或 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。

使用长距离故障切换时，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，重新传输故障切换消息会导致一些性能降级。

避免中断故障切换和数据链路

我们建议，让故障切换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。如果故障切换链路发生故障，ASA 可使用数据接口来确定是否需要进行故障切换。随后，故障切换操作会被暂停，直到故障切换链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障切换网络。

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 ASA 之间的故障切换和数据接口，则交换机或交换机间链路发生故障时，两台 ASA 都都将处于主用状态。因此，不推荐使用下图中显示的 2 种连接方法。

图 *1:* 使用单交换机连接 - 不推荐

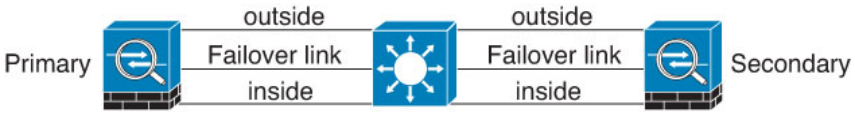
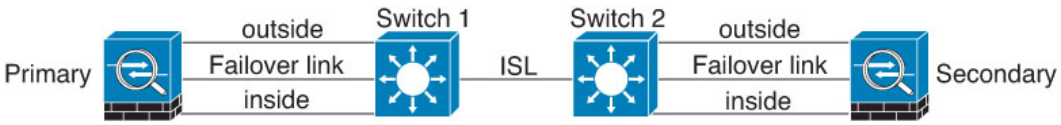


图 *2:* 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们不推荐让故障切换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切换链路，如下图所示。

图 *3:* 使用其他交换机连接

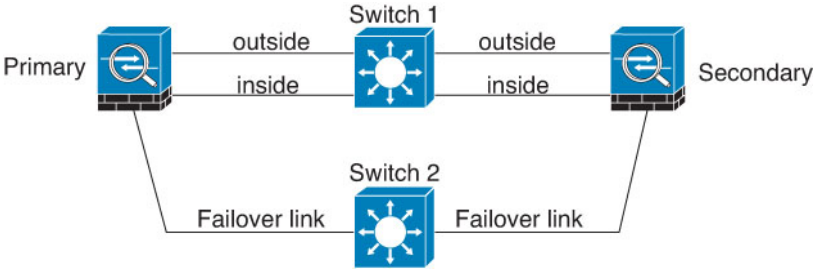
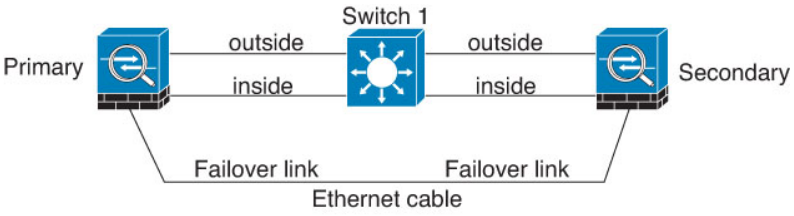


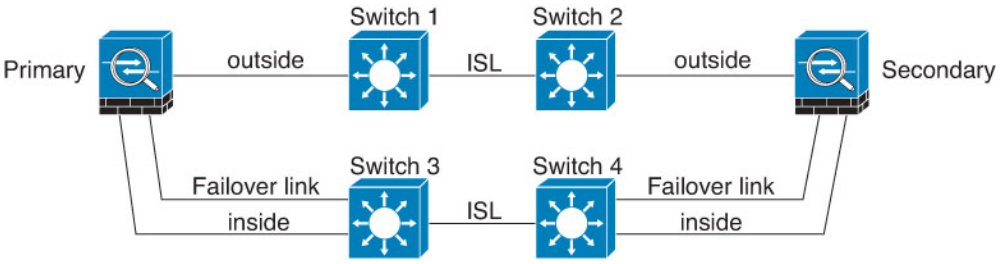
图 *4:* 通过缆线连接



情景 3 - 推荐

如果ASA数据接口连接到多台交换机，则故障切换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

最可靠的故障切换配置使用故障切换链路上的冗余接口，如下图所示。

图 *6:* 使用冗余接口连接

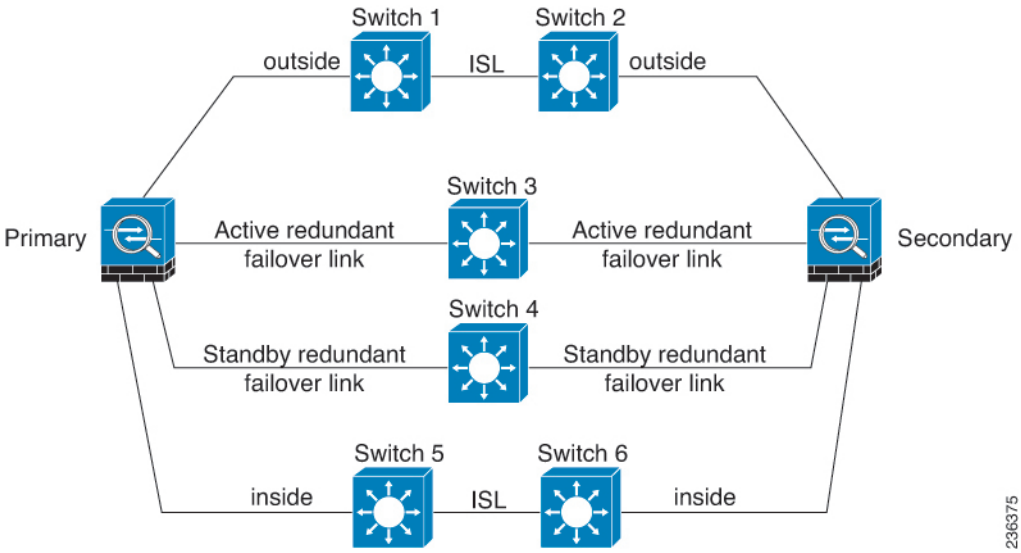
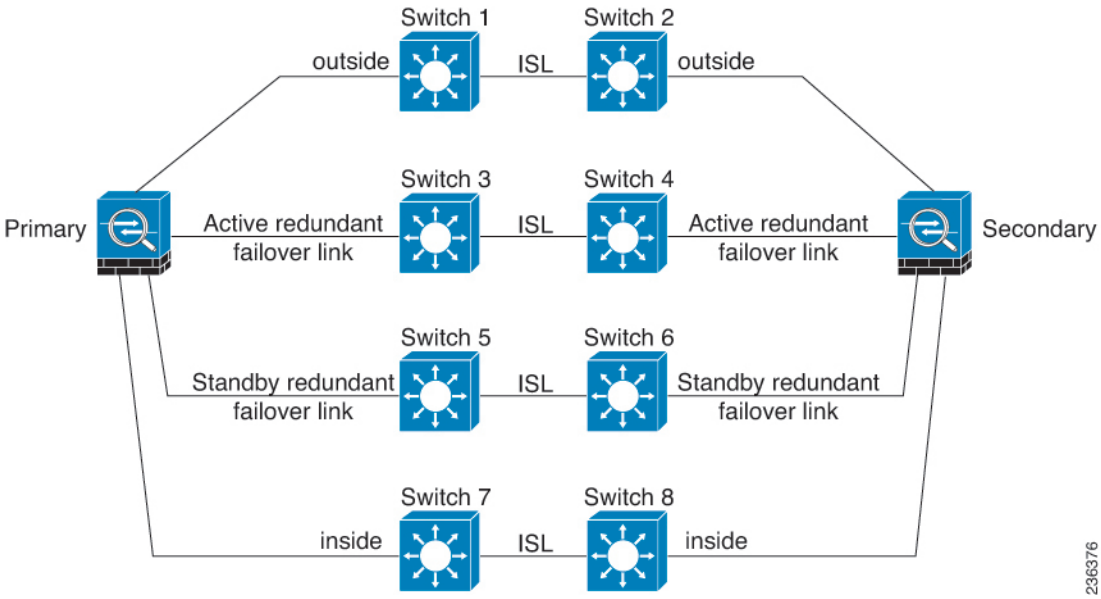


图 *7:* 使用交换机间链路连接



故障切换中的 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，当发生故障切换时，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。

在发生故障切换时，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/备用故障切换，请参阅下文，了解故障切换事件期间 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，ASA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。

主用/主用 IP 地址和 MAC 地址

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

1. 主设备为故障切换组 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切换组，并将备用地址用于其备用故障切换组。例如，主设备是故障切换组 1 的主用设备，因此它使用故障切换组 1 中情景的主用地址。它是故障切换组 2 中情景的备用设备，因此在其中使用备用地址。
3. 当设备进行故障切换时，另一个设备将会承担出现故障的故障切换组的主用 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，它将恢复故障切换组。

虚拟 MAC 地址

ASA 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。手动方法包括接口模式 **mac-address**

命令、**failover mac address** 命令；对于主用/主用故障切换，除了以下所述的自动生成方法之外，还有故障切换组模式 **mac address** 命令。

在多情景模式下，您可以配置 ASA 自动为共享接口生成虚拟主用和备用 MAC 地址，然后将这些分配同步到辅助设备（请参阅 **mac-address auto** 命令）。对于非共享接口，您可以手动设置主用/备用模式的 MAC 地址（主用/主用模式会为所有接口自动生成 MAC 地址）。

对于主用/主用故障切换，始终将虚拟 MAC 地址与默认值或按接口设置的值一同使用。

无状态故障切换和有状态故障切换

对于主用/备用和主用/主用模式，ASA 支持两种故障切换类型：无状态和状态故障切换。

注释 无客户端 SSL VPN 的某些配置元素（如书签和自定义）使用 VPN 故障切换子系统，该子系统是状态故障切换的一部分。您必须使用状态故障切换，在同步故障切换对中的成员之间同步这些元素。不推荐将无状态故障切换用于无客户端 SSL VPN。

无状态故障切换

发生故障切换时，所有活动连接将会被丢弃。在新的主用设备接管时，客户端需要重新建立连接。

注释 无客户端 SSL VPN 的某些配置元素（如书签和自定义）使用 VPN 故障切换子系统，该子系统是状态故障切换的一部分。您必须使用状态故障切换，在同步故障切换对中的成员之间同步这些元素。不推荐将无状态（常规）故障切换用于无客户端 SSL VPN。

状态故障切换

启用状态故障切换时，主用设备会不断将每个连接的状态信息发送至备用设备，在主用/主用故障切换期间，在主用和备用故障切换组之间发送。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

对于状态故障切换，以下状态信息会传送至备用 ASA：

- NAT 转换表。
- TCP 和 UDP 连接和状态。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。
- HTTP 连接表（除非启用 HTTP 复制）。
- HTTP 连接状态（如果已启用 HTTP 复制）- 默认情况下，启用状态故障切换时，ASA 不会复制 HTTP 会话信息。建议启用 HTTP 复制。

- SCTP 连接状态。但是，SCTP 检测状态故障切换是尽力而为。在故障切换期间，如果任何 SACK 数据包丢失，新的主用设备将丢弃队列中其他所有无序的数据包，直到收到缺失的数据包为止。
- 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。
- ICMP 连接状态 - 仅当相应的接口分配给非对称路由组时，才会启用 ICMP 连接复制。
- 静态和动态路由表 - 状态故障切换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。发生故障切换事件时，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。进行故障切换后，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。
- 思科 IP SoftPhone 会话 - 如果在活动思科 IP SoftPhone 会话期间发生故障切换，呼叫将保持活动，因为呼叫会话状态信息已复制到备用设备。呼叫被终止时，IP SoftPhone 客户端将丢失与思科 Call Manager 的连接。发生此连接丢失是因为，没有备用设备上的 CTIQBE 挂机消息的会话信息。如果 IP SoftPhone 客户端在特定时间内未从 Call Manager 收到响应，则会认为 Call Manager 不可访问，并会注销自身。
- RA VPN - 故障切换后，远程接入 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，在故障切换过程中可能会丢失数据包，并且无法从数据包丢失中恢复。

不支持的功能

对于状态故障切换，以下状态信息不会传送至备用 ASA：

- 用户身份验证 (uauth) 表
- TCP 状态绕行连接

- 组播路由。
- 模块的状态信息，如 ASA FirePOWER 模块。
- 选定的无客户端 SSL VPN 功能：
  - 智能隧道
  - 端口转发
  - 插件
  - Java 小程序
  - IPv6 无客户端或 Anyconnect 会话
  - Citrix 身份验证（Citrix 用户在故障切换后必须重新进行身份验证）

故障切换的网桥组要求

使用网桥组时，故障切换存在特殊的注意事项。

设备、ASAv 的网桥组要求

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，您可以根据交换机端口模式，配置以下任一变通方案：

- 访问模式 - 启用交换机上的 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。

- Trunk 模式 - 使用 EtherType 访问规则阻止桥接组成员接口上 ASA 上的 BPDU。

  ```
  access-list id ethertype deny bpdu
  access-group id in interface name1
  access-group id in interface name2
  ```

  阻止 BPDU 会在交换机上禁用 STP。在您的网络布局中，确保没有任何环路涉及 ASA。

如果以上选项均不可行，则您可以使用以下任一不太理想的变通方案，这些方案可能会影响故障切换功能或 STP 稳定性。

- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障切换之前收敛。

- 降低 STP 计时器的值，以 STP 在接口保持时间之内融合。

故障切换运行状态监控

ASA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 ASA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

ASA 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。 对于 Firepower 9300 和 4100系列，您可以启用双向转发检测 (BFD) 监控，这比 Hello 消息更可靠。ASA 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 ASA 在故障切换链路上收到响应，则不会进行故障切换。
- 如果 ASA 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。故障切换链路会标记为发生故障。您应尽快恢复故障切换链路，因为当故障切换切换发生故障时，设备无法故障切换到备用设备。
- 如果ASA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

您最多可以监控1025个接口（在多情景模式下，会在所有情景之间进行分配）。您应监控重要的接口。例如，在多情景模式下，您可以配置一个用于监控共享接口的情景：因为接口是共享的，所有情景都可以从监控中受益。

当设备在 15 个秒 （默认值），未在受监控的接口上收到 hello 消息时，将运行接口测试。（要更改时间段，请参阅 **failover polltime interface** 命令，如果是主用/主用故障切换，请参阅 **polltime interface** 命令）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，ASA 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。**failover interface-policyinterface-policy** 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 ASA 会回到备用模式。

如果有 ASA FirePOWER 模块，则 ASA 也会通过背板接口监控模块的运行状况。模块故障被视为设备故障，会触发故障切换。此设置可配置。

如果接口上配置了 IPv4 和 IPv6 地址，ASA 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 ASA 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，ASA 会使用所有的 IPv6 节点地址 (FE02::1)。

注释 如果故障设备未恢复，并且您认为其应未发生故障，则可通过输入 **failover reset** 命令重置状态。但是，如果故障切换条件仍然存在，设备将再次失败。

接口测试

ASA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，或故障切换接口保持时间的1/16（请参阅 **failover polltime interface** 命令，对于主用/主用故障切换，请参阅 **interface-policy** 命令）。

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 ASA视为测试失败，然后测试停止。如果状态为打开，则 ASA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 ASA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 ASA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 ASA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。
- 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。
- No Link - 接口的物理链路关闭。
- 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。

注释 如果使用 CLI 或 ASDM 手动进行故障切换，或者重新加载 ASA，则故障切换会立即开始，不受如下所列计时器的约束。

表 2: ASA

故障切换条件	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
主用设备主板接口链路发生故障。	500 毫秒	5 秒	15 秒

故障切换条件	最小	默认	最大
主用设备 4GE 模块接口链路发生故障。	2 秒	5 秒	15 秒
主用设备 Firepower 模块发生故障。	2 秒	2 秒	2 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

配置同步

故障切换包含各种类型的配置同步。

运行配置复制

当故障切换对中的任意一台或两台设备启动时，系统会执行运行配置复制。

在主用/备用故障切换中，配置始终会从主用设备同步到备用设备。

在主用/主用故障切换中，第二个启动的任何设备都会从第一个启动的设备获取正在运行的配置，无论指定的主或从属启动设备如何都是如此。在两个设备正常运行后，在系统执行空间中输入的命令会从其上的故障转移组 1 处于主用状态的设备复制。

备用/第二个设备完成其初始启动后，会清除其运行配置（需要与主用设备通信的**failover**命令除外），而主用设备则会向备用设备发送其完整配置。复制开始时，主用设备上的 ASA 控制台会显示消息“Beginning configuration replication: Sending to mate”；完成时，ASA 显示消息“End Configuration Replication to mate”。根据配置的大小，复制可能需要几秒到几分钟。

在接收配置的设备上，配置仅存在于运行内存中。您应该根据保存配置更改将配置保存到闪存。例如，在主用/主用故障切换中，请在故障切换组 1 处于主用状态的设备的系统执行空间中输入 **write memory all** 命令。该命令会复制到对等设备，该对等设备将继续将其配置写入到闪存。

注释 在复制时，在发送配置的设备上输入的命令可能无法正确地复制到对等设备，并且在接收配置的设备上输入的命令可能已被接受的配置覆盖。在配置复制过程中，应避免在故障切换对中的任一设备上输入命令。

文件复制

配置同步不复制以下文件和配置组件，因此您必须手动复制这些文件，以便它们匹配：

- AnyConnect 映像
- CSD 映像
- AnyConnect 配置文件

ASA 使用存储在 cache:/stc/profiles 中的 AnyConnect 客户端配置文件的缓存文件，而不是存储在闪存文件系统中的文件。要将 AnyConnect 客户端配置文件复制到备用设备，请执行以下其中一项操作：

- 在主用设备上输入 **write standby** 命令。
- 在主用设备上重新应用配置文件。
- 重新加载备用设备。

- 本地证书颁发机构 (CA)
- ASA 映像
- ASDM 映像

命令复制

启动后，您在主用设备上输入的命令会被立即复制到备用设备。 不必将主用配置保存到闪存才能复制命令。

在主用/主用故障切换中，在系统执行空间中输入的命令复制自其上的故障切换组 1 处于主用状态的设备。

未在要进行命令复制的相应设备上输入命令会导致配置不同步。在进行下一次初始配置同步时，这些更改可能会丢失。

以下命令会复制到备用 ASA：

- 除 **mode**、**firewall** 和 **failover lan unit** 之外的所有配置命令
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

以下命令不会复制到备用 ASA：

- 除 **copy** 命令外的所有形式的 **copy running-config startup-config** 命令
- 除 **write** 命令外的所有形式的 **write memory** 命令
- **debug**
- **failover lan unit**
- **firewall**

- **show**
- **terminal pager** 和 **pager**

关于主用/备用故障切换

主用/备用故障切换允许您使用备用ASA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。

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

主/辅助角色和主用/备用状态

在故障切换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切换链路获取主设备 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。

故障切换事件

在主用/备用故障切换中，故障切换会在设备级别进行。即使在多情景模式下运行的系统上，您也无法对个别情景或一组情景进行故障切换。

下表显示了每个故障事件的故障切换操作。对于每种故障事件，该表显示了故障切换策略（故障切换或禁用故障切换）、主用设备执行的操作、备用设备执行的操作，以及有关故障切换条件和操作的所有特别说明。

表 *3:* 故障切换事件

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）	故障切换	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切换链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障切换	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障切换	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。
故障切换链路在运行过程中发生故障	禁用故障切换	将故障切换链路标记为发生故障	将故障切换链路标记为发生故障	您应尽快恢复故障切换链路，因为当故障切换链路发生故障时，设备无法故障切换到备用设备。
故障切换链路在启动时发生故障	禁用故障切换	成为主用设备 将故障切换链路标记为发生故障	成为主用设备 将故障切换链路标记为发生故障	如果故障切换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	禁用故障切换	无需操作	无需操作	如果发生故障切换，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	故障切换	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	禁用故障切换	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。

关于主用/主用故障切换

本部分介绍主用/主用故障切换。

主用/主用故障切换概述

在主用/主用故障切换配置下，两台 ASA 都可以传送网络流量。主用/主用故障切换仅适用于多情景模式下的 ASA。在主用/主用故障切换中，您可将 ASA 上的安全情景最多划分为 2 个故障切换组。

故障切换组就是一个或多个安全情景的逻辑组。您可以将故障切换组指定为在主 ASA 上处于主用状态，并将故障切换组 2 指定为在辅助 ASA 上处于主用状态。发生故障切换时，会在故障切换组级别进行。例如，根据接口故障模式，故障切换组 1 可能会故障切换到辅助 ASA，相应地，故障切换组 2 可能故障切换到主 ASA。在以下情况下可能发生此事件：故障切换组 1 中的接口在主 ASA 上发生故障，但在辅助 ASA 上正常工作，而故障切换组 2 中的接口在辅助 ASA 上发生故障，但在主 ASA 上正常工作。

管理情景始终是故障切换组 1 的成员。默认情况下，所有未分配的安全情景也是故障切换组 1 的成员。如果希望使用主用/主用故障切换，但对多情景不感兴趣，最简单的配置是添加一个额外的情景并将其分配给故障切换组 2。

注释 配置主用/主用故障切换时，请确保两台设备的整合流量在每台设备的处理能力之内。

注释 需要时，可将两个故障切换组分配到一台 ASA，但您将无法利用具有两台主用 ASA 的优势。

故障切换组的主/辅助角色和主用/备用状态

与在主用/备用故障切换中一样，主用/主用故障切换对中的一台设备被指定为主设备，另一台指定为辅助设备。不同于主用/备用故障切换的是，当两台设备同时启动时，此指定不指示哪一台设备会成为主用设备。相反地，主设备/辅助设备指定会进行两个操作：

- 两台设备同时启动时，主设备会提供运行配置。
- 配置中的每个故障切换组都配置了主设备或辅助设备首选项。与抢占一起使用时，此首选项可确保故障切换组启动后在正确的设备上运行。如果不使用抢占，则两个组均在第一台要启动的设备上运行。

启动时的故障切换组主用设备确定

故障切换组在其上变为主用状态的的设备按以下方式确定：

- 一台设备启动时，如果对等设备不可用，则两个故障切换组都会在该设备上变为主用状态。
- 一台设备启动时，如果对等设备处于主用状态（而且两个故障切换组都处于主用状态），则故障切换组将在主用设备上保持主用状态，而无论故障切换组的主设备或辅助设备首选项如何，直到出现以下情形之一：
  - 发生故障切换。
  - 手动强制执行故障切换。

- 为故障切换组配置了抢占，这导致故障切换组在设备变得可用时，自动在首选设备上变为主用状态。

故障切换事件

在主用/主用故障切换配置中，故障切换会在故障切换组级别，而不是系统级别进行。例如，如果您将两个故障切换组指定为主设备上的主用故障切换组，并且故障切换组 1 发生故障，则故障切换组 2 会在主设备上保持主用，而故障切换组 1 则会在辅助设备上变为主用状态。

由于故障切换组可以包含多个情景，并且每个情景可以包含多个接口，因此有可能单个情景中的所有接口都发生故障而不导致相关故障切换组发生故障。

下表显示了每个故障事件的故障切换操作。对于每种故障事件，给出了策略（是否发生故障切换）、主用故障切换组的操作和备用故障切换组的操作。

表 *4:* 故障切换事件

故障事件	策略	主用组操作	备用组操作	备注
设备发生电源或软件故障	故障切换	成为备用设备 标记为发生故障	成为主用设备 将主用设备标记为发生故障	故障切换对中的一台设备发生故障时，该设备上的所有主用故障切换组都会被标记为发生故障，并在对等设备上变为主用状态。
主用故障切换组上的接口故障超过阈值	故障切换	将主用组标记为发生故障	成为主用设备	无。
备用故障切换组上的接口故障超过阈值	禁用故障切换	无需操作	将备用组标记为发生故障	备用故障切换组标记为发生故障后，主用故障切换组不会尝试进行故障切换，即使超过接口故障阈值也是如此。
以前的主用故障切换组恢复	禁用故障切换	无需操作	无需操作	除非配置了故障切换组抢占，否则故障切换组会在其当前设备上保持主用状态。
故障切换链路在启动时发生故障	禁用故障切换	成为主用设备	成为主用设备	如果故障切换链路在启动时发生故障，则两台设备上的故障切换组都会变为主用状态。
状态链路发生故障	禁用故障切换	无需操作	无需操作	如果发生故障切换，状态信息会过时，而且会话会被终止。

故障事件	策略	主用组操作	备用组操作	备注
故障切换链路在运行过程中发生故障	禁用故障切换	n/a	n/a	每台设备都会将故障切换链路标记为发生故障。您应尽快恢复故障切换链路，因为当故障切换链路发生故障时，设备无法故障切换到备用设备。

故障切换许可

对于绝大多数型号，故障切换设备不要求每个设备上具有同一许可证。如果您在两台设备上都有许可证，则这两个许可证会合并为一个运行故障切换群集许可证。此规则存在一些例外情况。有关故障切换的具体许可要求，请参阅下表。

型号	许可证要求
ASA 5506-X 和 ASA 5506W-X	• 主用/备用 - 两个设备上都有增强型安全许可证。 • 主用/主用 - 不支持。 **注释** 每台设备必须拥有相同的加密许可证。
ASAv	请参阅 ASAv 的故障切换许可证。
Firepower 1010	两个设备上都有增强型安全许可证。请参阅Firepower 1010 的故障切换许可证。
Firepower 1100	请参阅Firepower 1100 的故障切换许可证。
Firepower 2100	请参阅Firepower 2100 的故障切换许可证。
Firepower 4100/9300	请参阅 Firepower 4100/9300 机箱上适用于 ASA 的故障切换许可证。
ISA 3000	两个设备上都有增强型安全许可证。 **注释** 每台设备必须拥有相同的加密许可证。

注释 需要有效的永久密钥；在极少数情况下， 可以删除您的 PAK 身份验证密钥。如果密钥全部由 0 组成，则需要重新安装有效的身份验证密钥，然后才能启用故障切换。

故障切换指南

情景模式

- 仅多情景模式支持主用/主用模式。
- 对于多情景模式，请在系统执行空间中执行所有步骤，除非另外说明。

型号支持

- ASA 5506W-X - 您必须为内部 GigabitEthernet 1/9 接口禁用接口监控。这些接口将无法进行通信以执行默认接口监控检查，由于预期的接口通信故障，导致交换机在主用和备用之间来回切换。
- Firepower 1010：
  - 使用故障切换时，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。故障切换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 故障切换网络设置中，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接口可通过故障切换监控，而交换机端口无法通过故障切换监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 故障切换，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切换链路。
- Firepower 9300 - 我们建议您使用机箱间故障切换以实现最佳冗余。
- 由于需要第 2 层的连接，因此不支持常规故障切换在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 ASAv。另请参阅 公共云中的高可用性故障切换。
- ASA FirePOWER 模块不支持直接进行故障切换；当 ASA 进行故障切换时，现有的任何 ASA FirePOWER 数据流都会被传送到新的 ASA。新 ASA 中的 ASA FirePOWER 模块将开始检测来自该点转发的流量；不传送旧检测状态。

  您需负责在高可用性 ASA 对的 ASA FirePOWER 模块上维持一致的策略，以确保故障切换的行为一致。

注释 请在配置 ASA FirePOWER 模块之前先创建故障切换对。如果已在两个设备上配置这些模块，请首先清除备用设备上的接口配置，再创建故障切换对。在备用设备的 CLI 中，输入 **clear configure interface** 命令。

通过 ASAv 故障切换实现高可用性

使用 ASAv 创建故障切换对时，需要按相同顺序将数据接口添加到每个 ASAv。如果完全相同的接口添加到每个 ASAv，但采用不同的顺序，在 ASAv 控制台上会显示错误。故障切换功能可能也会受到影响

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 ASA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。

- 您最多可以在一台设备上监控跨所有情景的 1025 个接口。

- 对于主用/备用 故障切换和 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。

- 对于主用/主用故障切换，不应在相同 ASR 组中配置相同情景中的两个接口。

- 对于主用/主用故障切换，最多可以定义两个故障切换组。

- 对于主用/主用故障切换，删除故障切换组时，必须最后删除故障切换组 1。故障切换组 1 始终包含管理情景。未分配到故障切换组的所有情景将默认分配到故障切换组 1。不能删除已显式分配了情景的故障切换组。

- 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。

- 如果您在评估模式下配置 HA 故障切换加密，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。您必须将 SNMPv3 用户重新添加到主用设备，以强制用户复制到新设备；或者，也可以直接在新设备上添加用户。重新配置每个用户，方法是在控制/主用设备上输入 **snmp-server user** *username group-name* **v3** 命令，或者直接使用未加密形式的 *priv-password* 选项和 *auth-password* 选项直接连接到备用设备。

- ASA 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。

故障切换的默认设置

默认情况下，故障切换策略包含以下内容：

- 在状态故障切换中不进行 HTTP 复制。
- 单个接口故障导致故障切换。
- 接口轮询时间为 5 秒。
- 接口保持时间为 25 秒。
- 设备轮询时间为 1 秒。
- 设备保持时间为 15 秒。
- 在组播情景模式下。
- 监控所有物理接口。

配置主用/备用故障切换

要配置主用/备用故障切换，请在主设备和辅助设备上配置基本故障切换设置。其他所有配置仅在主设备上进行，然后这些设置会同步到辅助设备。

为主用/备用故障切换配置主设备

遵循本节介绍的步骤，配置主用/备用故障切换配置中的主设备。这些步骤提供了在主设备上启用故障切换所需的最小配置。

开始之前

- 我们建议您为除故障切换和状态链路外的所有接口配置备用 IP 地址。 如果您将 31 位子网掩码用于点对点连接，则请不要配置备用 IP 地址。
- 请勿为故障切换和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 将此设备指定为主设备：

failover lan unit primary

步骤 2 指定要用作故障切换链路的接口：

failover lan interface *if_name interface_id*

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途（但用于状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 Firepower 1010 上，该接口是防火墙接口 ID；不能指定交换机端口 ID 或 VLAN ID。 您只能为 ASA 5506H-X 将 Management 1/1 接口指定为故障切换链路。如果您要这样做，必须使用 **write memory** 保存配置，然后 **reload** 会重新加载设备。随后，您将无法将此接口用于故障切换，也将无法使用 ASA Firepower 模块；该模块需要用于管理的接口，并且您只能将其用于一项功能。Firepower 4100/9300 可以使用任何数据类型接口。

步骤 3 为故障切换链路分配主用和备用 IP 地址：

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

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)，仅包含两个 IP 地址。169.254.0.0/16 和 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。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4 启用故障切换链路：

interface *failover_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
```

```
ciscoasa(config-if)# no shutdown
```

步骤 5 （可选）指定要用作状态链路的接口：

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link folink gigabitethernet0/3
```

可与状态链路共享故障切换链路。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 Firepower 1010 上，该接口是防火墙接口 ID；不能指定交换机端口 ID 或 VLAN ID。

步骤 6 如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

此地址应处于不同于故障切换链路的未使用子网上。 此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 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。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享状态链路，请跳过此步骤。

步骤 7 如果您指定了单独的状态链路，请启用状态链路。

interface *state_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享状态链路，请跳过此步骤。

步骤 8 （可选）请执行以下任一操作，以加密故障切换和状态链路上的通信：

- （首选）在设备之间的故障切换和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障切换通信：

failover ipsec pre-shared-key [**0** | **8**] 密钥

示例：

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

该*key*的最大长度为128个字符。确定两台设备上的相同密钥。此密钥由IKEv2用于建立隧道。

如果使用主密码（请参阅配置主密码），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。默认情况下使用 **0**，表明未加密的密码。

failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

如果您未配置故障切换和状态链路加密，故障切换通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。不过，如果使用主密码，则在配置 IPsec 加密之前必须首先使用 **no failover key** 命令删除故障切换密钥。

故障切换 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障切换和状态链路上的故障切换通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  使用 1 到 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

  如果使用主密码（请参阅配置主密码），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9 启用故障切换：

failover

步骤 10 将系统配置保存到闪存：

write memory

示例

以下示例配置主设备的故障切换参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

为主用/备用故障切换配置辅设备

在辅助设备上只需要配置故障切换链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令可确定每台设备是主设备，还是辅助设备。

开始之前

- 请勿为故障切换和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令除外。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。请参阅为主用/备用故障切换配置主设备，第 24 页。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config-ifc)# failover link folink gigabitethernet0/3
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

步骤 2 故障切换配置同步之后，会将配置保存到闪存：

```
ciscoasa(config)# write memory
```

配置主用/主用故障切换

本节介绍如何配置主用/主用故障切换。

为主用/主用故障切换配置主设备

遵循本节介绍的步骤，配置主用/主用故障切换配置中的主设备。这些步骤提供了在主设备上启用故障切换所需的最小配置。

开始之前

- 根据启用或禁用多情景模式启用多情景模式。
- 除故障切换和状态链路之外，我们建议您根据路由模式接口和透明模式接口为所有接口配置备用 IP 地址。 如果对于点对点连接使用 31 位子网掩码，请勿配置备用 IP 地址。
- 请勿为故障切换和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 将此设备指定为主设备：

failover lan unit primary

步骤 2 指定要用作故障切换链路的接口：

failover lan interface *if_name interface_id*

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途（但用于状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口、冗余接口或 EtherChannel 接口 ID。Firepower 4100/9300 可以使用任何数据类型接口。

步骤 3 为故障切换链路分配主用和备用 IP 地址：

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

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)，仅包含两个 IP 地址。169.254.0.0/16 和 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。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4 启用故障切换链路：

interface *failover_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

步骤 5 （可选）指定要用作状态链路的接口：

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

我们建议，指定与故障切换链路或数据接口不同的独立接口。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口、冗余接口或 EtherChannel 接口 ID。

步骤 6 如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

此地址应处于不同于故障切换链路的未使用子网上。 此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 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。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享状态链路，请跳过此步骤。

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
```

```
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

步骤 7 如果您指定了单独的状态链路，请启用状态链路：

interface *state_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享状态链路，请跳过此步骤。

步骤 8 （可选）请执行以下任一操作，以加密故障切换和状态链路上的通信：

- （首选）在设备之间的故障切换和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障切换通信：

  failover ipsec pre-shared-key [**0** | **8**] 密钥

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  该 *key* 的最大长度为 128 个字符。确定两台设备上的相同密钥。此密钥由 IKEv2 用于建立隧道。

  如果使用主密码（请参阅配置主密码），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。默认情况下使用 **0**，表明未加密的密码。

  failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

  不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。不过，如果使用主密码，则在配置 IPsec 加密之前必须首先使用 **no failover key** 命令删除故障切换密钥。

  故障切换 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障切换和状态链路上的故障切换通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

使用 *shared_secret*（1 到 63 个字符）或 32 个字符的 **十六进制** 密钥。

对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

如果使用主密码（请参阅配置主密码），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

如果您未配置故障切换和状态链路加密，故障切换通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9 创建故障切换组 1：

failover group 1

primary

preempt [*delay*]

示例：

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

通常，您可以将组 1 分配给主设备，将组 2 分配给辅助设备。两个故障切换组在首次启动的设备上都会变成主用状态（即使它们看似同时启动，但一台设备会首先变成主用状态），不考虑该组的主要或辅助设置。当指定设备变得可用时，**preempt** 命令会使故障切换组自动在该设备上变为主用状态。

您可以输入可选的 *delay* 值，该值指定故障切换组在指定设备上自动变为主用状态之前，在当前设备上保持主用状态的秒数。有效值范围为 1 至 1200。

如果启用状态故障切换，则抢占会延迟，直到连接从当前处于主用状态的故障切换组所在的设备中复制为止。

如果手动执行故障切换，则会忽略 **preempt** 命令。

步骤 10 创建故障切换组 2，并将其分配至辅助设备：

failover group 2

secondary

preempt [*delay*]

示例：

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

步骤 11 进入给定情景的情景配置模式，然后将该情景分配给故障切换组：

context 名称

join-failover-group {**1** | **2**}

示例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

对每个情景重复此命令。

所有未分配的情景会自动分配到故障切换组 1。管理情景始终是故障切换组 1 的成员；您不能将其分配给组 2。

步骤 12 启用故障切换：

failover

步骤 13 将系统配置保存到闪存：

write memory

示例

以下示例配置主设备的故障切换参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

为主用/主用故障切换配置辅助设备

在辅助设备上只需要配置故障切换链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令可确定每台设备是主设备，还是辅助设备。

开始之前

- 根据启用或禁用多情景模式启用多情景模式。
- 请勿为故障切换和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令除外。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。您也不需要输入 **failover group** 和 **join-failover-group** 命令，因为这些命令会从主设备复制。请参阅为主用/主用故障切换配置主设备，第 29 页。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

步骤 2 故障切换配置通过主设备同步后，将配置保存到闪存：

ciscoasa(config)# **write memory**

步骤 3 如果需要，可强行要求故障切换组 2 在辅助设备上处于主用状态：

failover active group 2

配置可选故障切换参数

您可以视需要自定义故障切换设置。

配置故障切换条件和其他设置

有关您可在本节中更改的许多参数的默认设置，请参阅故障切换的默认设置，第 24 页。对于主用/主用模式，您可以设置每个故障切换组的大多数条件。。

开始之前

- 在多情景模式下，可在系统执行空间中配置这些设置。
- 如需为设备运行状况监控配置双向转发检测 (BFD)，请参阅以下限制：
  - 仅限 Firepower 9300 和 4100。
  - 仅限主用/备用。
  - 仅限路由模式

过程

步骤 1 更改设备的轮询和保持时间：

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

示例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

polltime 范围介于 1 和 15 秒之间，或者 200 和 999 毫秒之间。**holdtime** 范围介于 1 到 45 秒之间或 800 到 999 毫秒之间。输入的保持时间值不能小于设备轮询时间的 3 倍。设置的轮询时间越快，ASA 便可越快检测到故障并触发故障切换。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

如果设备在一个轮询周期内未收到故障切换通信的呼叫数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障切换组设置此速率。

步骤 2 为设备运行状况监控配置 BFD。

定期监控设备可能会在 CPU 使用率高时导致错误报警。BFD 方法是分布式的，所以高 CPU 不会影响其运行。

a) 定义要用于故障切换运行状况检测的 BFD 模板：

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

示例：

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

min-tx 指定 BFD 控制数据包被发送到故障切换对等体的速率。范围介于 50 到 999 毫秒之间。**min-rx** 指定预计收到来自故障切换对等体的 BFD 控制数据包的速率。范围介于 50 到 999 毫秒之间。**multiplier** 指定在 BFD 声明对等体不可用之前必须错过来自该故障切换对等体的连续 BFD 控制数据包数。范围为 3 到 50。

此外，还可以为此模板配置回应和身份验证；请参阅创建 BFD 模板。

b) 为运行状况监控启用 BFD：

failover health-check bfd *template_name*

示例：

```
ciscoasa(config)# failover health-check bfd failover-temp
```

步骤 3 更改接口链路状态轮询时间：

failover polltime link-state msec *poll_time*

示例：

```
ciscoasa(config)# failover polltime link-state msec 300
```

范围为 300 至 799 毫秒。默认情况下，故障切换对中的每个 ASA 每隔 500 毫秒检查一次其接口的链路状态。您可以自定义轮询时间；例如，如果将轮询时间设置为 300 毫秒，则 ASA 可以更快地检测接口故障并触发故障切换。

在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障切换组设置此速率。

步骤 4 设置每秒连接中的会话复制速率：

failover replication rate *conns*

示例：

```
ciscoasa(config)# failover replication rate 20000
```

最小和最大速率取决于您的型号。默认值为最大速率。在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障切换组设置此速率。

步骤 5 禁用在备用设备或情景中直接进行任何配置更改的功能：

failover standby config-lock

默认情况下，允许备用设备/情景上进行配置，但系统会显示一条警告消息。

步骤 6 （仅主用/主用模式）指定要自定义的故障切换组：

{| } **failover group1 2**

示例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

步骤 7 启用 HTTP 状态复制：

- 对于主用/备用模式：

  failover replication http

- 对于主用/主用模式：

  replication http

要允许在状态信息复制中包含 HTTP 连接，您需要启用 HTTP 复制。我们建议启用HTTP状态复制。

注释 由于使用故障切换时从备用设备中删除 HTTP 数据流会产生延迟，所以 **show conn count** 输出在主用设备与备用设备上可能显示不同的数量；如果等待几秒钟再重新发出该命令，则会在两台设备上看到相同的数量。

步骤 8 设置接口发生故障时的故障切换阈值：

- 对于主用/备用模式：

  failover interface-policy *num* [%]

  示例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- 对于主用/主用模式：

  interface-policy *num* [%]

  示例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

默认情况下，一个接口故障会导致故障切换。

在指定接口的特定数量时，*num* 参数可介于 1 到 1025 之间。

在指定接口的百分比时，*num* 参数可介于 1 到 100 之间。

步骤 9 更改接口轮询和保持时间：

- 对于主用/备用模式：

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  示例：

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

- 对于主用/主用模式：

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  示例：

```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

- polltime-设置向对等体发送呼叫数据包之间的等待时间。轮询时间的有效值介于1到15秒之间；如果使用可选的 **msec** 关键字，则有效值介于 500 到 999 毫秒之间。默认值为 5 秒。
- **holdtime***time*-设置从对等体设备最后收到的*Hello*消息与开始接口测试以确定接口运行状况之间的时间（作为计算）。它还将每个接口测试的持续时间设置为holdtime / 16。有效值范围为 5 至 75 秒。默认值为轮询时间的5倍。输入的保持时间值不得短于设备轮询时间的 5 倍。

  要计算开始接口测试之前的时间（y），请执行以下操作：

  1. x =（*holdtime*/*polltime*）/ 2，四舍五入为最接近的整数。（.4 和向下四舍五入； 0.5 和向上四舍五入。）
  2. y = x**polltime*

  例如，如果使用默认保持时间25和轮询时间5，则y = 15秒。

步骤 10 配置接口的虚拟 MAC 地址：

- 对于主用/备用模式：

  failover mac address *phy_if active_mac standby_mac*

  示例：

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- 对于主用/主用模式：

  mac address *phy_if active_mac standby_mac*

  示例：

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

phy_if 参数是接口的物理名称，例如，gigabitethernet0/1。

active_mac 和 *standby_mac* 参数是 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 将需要输入 000C.F142.4CDE。

active_mac 地址与接口的活动 IP 地址相关联，而 *standby_mac* 与接口的备用 IP 地址相关联。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。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。

使用 **show interface** 命令可显示接口使用的 MAC 地址。

步骤 11 （仅限主用/主用模式）对于其他故障切换组重复此操作步骤。

配置接口监控

默认情况下，在所有物理接口上启用监控，或者对于 Firepower 1010，则为所有 VLAN 接口以及在 ASA 上安装的任何硬件或软件模块（例如 ASA Firepower 模块）启用监控。Firepower 1010 交换机端口无法进行接口监控。

您可能希望排除连接到非关键网络的接口，以免影响故障切换策略。

您最多可以在一台设备上监控 1025 个接口（跨多情景模式下的所有情景）。

开始之前

在多情景模式下，请在每个情景中配置接口。

过程

启用或禁用接口运行状况监控：

[**no**] **monitor-interface** {*if_name* | **service-module**}

示例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

如果您不希望硬件或软件模块故障（如 ASA FirePOWER 模块）触发故障切换，则可以使用 **no monitor-interface service-module** 命令禁用模块监控。

配置非对称路由数据包支持（主用/主用模式）

在主用/主用故障切换下运行时，设备可能会收到其对等设备发起的连接的一个返回数据包。由于收到该数据包的 ASA 没有该数据包的任何连接信息，该数据包会被丢弃。主用/主用故障切换对中的两台 ASA 连接到不同的运营商，并且出站连接不使用 NAT 地址时，最常发生此丢弃。

您可以通过允许非对称路由数据包来防止返回数据包。为此，您需要将每台ASA上的相似接口分配到同一个ASR组。例如，两台ASA的内部接口连接到内部网络，但外部接口连接到不同的ISP。在主设备上，将主用情景外部接口分配给 ASR 组 1；在辅助设备上，将主用情景外部接口分配给相同 ASR 组 1。当主设备外部接口收到没有其会话信息的数据包时，它会检查相同组中处于备用情景中

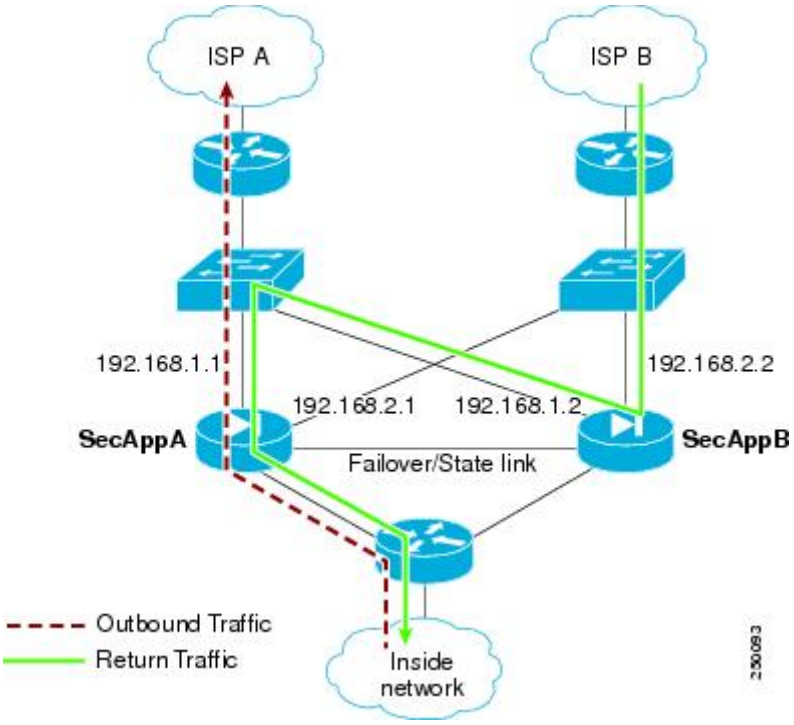
的另一接口的会话信息；在此示例中，即 ASR 组 1。如果没有找到匹配项，数据包会被丢弃。如果找到匹配项，则会进行以下的操作：

- 如果传入流量来自对等设备，第 2 层报头的部分或全部内容会被重写，数据包会被重定向到另一设备。只要会话处于活动状态，此重定向即可继续。
- 如果传入流量来自相同设备上的不同接口，第 2 层报头的部分或全部内容会被重写，数据包会被重新注入数据流。

注释 此功能不提供非对称路由；它会将非对称路由数据包恢复到正确接口。

下图显示非对称路由数据包的示例。

图 *8: ASR* 示例



1. 出站会话使用主用 SecAppA 情景通过 ASA。该会话退出接口 outsideISP-A (192.168.1.1)。
2. 由于上游某处配置了非对称路由，返回流量会使用主用 SecAppA 情景通过 ASA 上的接口 outsideISP-B (192.168.2.2) 传回。
3. 由于没有接口 192.168.2.2 上的流量的会话信息，返回流量通常会被丢弃。但是，此接口被配置为 ASR 组 1 的一部分。设备会在配置为相同的 ASR 组 ID 的所有其他接口上查找该会话。
4. 会话信息会在接口 outsideISP-A (192.168.1.2) 上找到，该接口在使用 SecAppB 情景的设备上处于备用状态。状态故障切换会将会话信息从 SecAppA 复制到 SecAppB。

5. 第 2 层报头会使用接口 192.168.1.1 的信息重写，流量会被重定向，通过接口 192.168.1.2，在该接口上，流量随后会通过设备上的来源接口（SecAppA 上的 192.168.1.1）返回，而不是将流量丢弃。此转发会视需要继续，直到会话结束。

开始之前

- 状态故障切换 - 将主用故障切换组中的接口上的会话的状态信息，传送给备用故障切换组。
- 复制 HTTP - HTTP 会话状态信息不会传送给备用故障切换组，因此不存在于备用接口上。为了使 ASA 能够重新路由非对称路由的 HTTP 数据包，您需要复制 HTTP 状态信息。
- 请在主设备和辅助设备上的每个主用情景中，执行本程序。
- 您无法在一个情景中同时配置 ASR 组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。

过程

步骤 1 在主设备上，指定要允许非对称路由数据包的接口：

interface *phy_if*

示例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

步骤 2 设置接口的 ASR 组编号：

asr-group *num*

示例：

```
primary/admin(config-ifc)# asr-group 1
```

num 的有效值范围为 1 到 32。

步骤 3 在辅助设备上，指定要允许非对称路由数据包的类似接口：

interface *phy_if*

示例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

步骤 4 设置接口的 ASR 组编号，以匹配主设备接口：

asr-group *num*

示例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

示例

两台设备具有以下配置（配置仅显示相关命令）。图中标记为 SecAppA 的设备是故障切换对中的主设备。

主设备系统配置

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA 情景配置

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

SecAppB 情景配置

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

管理故障切换

本部分介绍您在启用故障切换后如何管理故障切换，包括如何更改故障切换设置以及如何强制从一台设备故障切换到另一台设备。

强制故障切换

要强制要求备用设备成为主用设备，请执行以下程序。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 在备用设备上输入时，可以强制故障切换。备用设备将成为主用设备。

如果指定 **group** *group_id*，则在指定主用/主用故障切换组的备用设备上输入此命令时，将强制进行故障切换。备用设备将成为故障切换组的主用设备。

- 对于备用设备上的主用/备用模式：

  failover active

- 对于备用设备上的主用/主用模式：

  failover active [**group** *group_id*]

  示例：

  ```
  standby# failover active group 1
  ```

步骤 2 在主用设备上输入时，可以强制故障切换。主用设备将成为备用设备。

如果指定 **group** *group_id*，在指定故障切换组的主用设备上输入时，此命令将强制进行故障切换。主用设备将成为故障切换组的备用设备。

- 对于主用设备上的主用/备用模式：

no failover active

- 对于主用设备上的主用/主用模式：

  no failover active [**group** *group_id*]

  示例：

```
active# no failover active group 1
```

禁用故障切换

在一台或两台设备上禁用故障切换，将会导致每台设备保持其主用和备用状态，直到您重新加载。对于主用/主用故障切换对，故障切换组在其处于主用状态的设备上保持主用状态，而无论它们被配置为首选哪一设备。

禁用故障切换时，请参阅以下特征：

- 备用设备/情景保持备用模式，以便两台设备都不开始传输流量（这称为假备用状态）。
- 备用设备/情景继续使用其备用 IP 地址，即使它不再连接到主用设备/情景也是如此。
- 备用设备/情景继续侦听故障切换链路上的连接。如果在主用设备/情景上重新启用故障切换，则备用设备/情景会在重新同步其他配置后恢复普通备用状态。
- 不要在备用设备上手动启用故障切换将其激活；请参阅强制故障切换，第 43 页。如果您在备用设备上启用故障切换，将看到可能会妨碍 IPv6 流量的 MAC 地址冲突。
- 要真正禁用故障切换，请将禁用故障切换配置保存到启动配置，然后重新加载。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 禁用故障切换：

no failover

步骤 2 要完全禁用故障切换，请保存配置并重新加载：

write memory

reload

恢复故障设备

要将故障设备恢复到无故障状态，请执行以下程序。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 将故障设备恢复为无故障状态：

- 对于主用/备用模式：

  failover reset

- 对于主用/主用模式：

  failover reset [**group** *group_id*]

  示例：

```
ciscoasa(config)# failover reset group 1
```

将故障设备恢复到无故障状态，不会自动使其成为主用设备；恢复后的设备将保持在备用状态，直到故障切换（强制或自然）使其变为主用状态。例外情况是，配置了故障切换抢占的故障切换组（仅主用/主用模式）。如果故障切换组之前处于主用状态且配置了抢占，并且它是在首选设备上发生故障的，则该故障切换组将变为主用状态。

如果指定 **group** *group_id*，此命令会将发生故障的主用/主用故障切换组恢复到无故障状态。

步骤 2 （仅主用/主用模式）要在故障切换组级别重置故障切换，请执行以下步骤：

a) 在 System 中，依次选择 **Monitoring > Failover > Failover Group #**，其中 # 是要控制的故障切换组的编号。

b) 点击 **Reset Failover**。

重新同步配置

如果在主用设备上输入 write standby 命令，备用设备将清除其运行配置（用于与主用设备进行通信的故障切换命令除外），并且，主用设备会将其完整配置发送到备用设备。

对于多情景模式，当您在系统执行空间中输入 **write standby** 命令时，系统将复制所有情景。如果在情景中输入 **write standby** 命令，该命令只会复制情景配置。

复制命令会存储在运行配置中。

测试故障切换功能

要测试故障切换功能，请执行以下程序。

过程

步骤 1 测试您的主用设备是否在通过使用 FTP（例如）来在不同接口上的主机之间发送文件，从而如预期传送流量。

步骤 2 在主用设备上输入以下命令，从而强制进行故障切换：

主用/备用模式：

ciscoasa(config)# **no failover active**

主用/主用模式：

ciscoasa(config)# **no failover active group** *group_id*

步骤 3 使用 FTP 在相同的两台主机之间发送另一个文件。

步骤 4 如果测试不成功，请输入 **show failover** 命令检查故障切换状态。

步骤 5 完成后，您可以在新的主用设备上输入以下命令，从而将设备恢复到主用状态：

主用/备用模式：

ciscoasa(config)# **no failover active**

主用/主用模式：

ciscoasa(config)# **failover active group** *group_id*

注释 ASA 接口关闭时，为了进行故障切换，该接口仍被视为是设备问题。如果 ASA 检测到接口关闭，会立即进行故障切换，而不等待接口保持时间。仅当 ASA 将接口状态视为 OK 时，接口保持时间才有用，但ASA并未从对等体接收呼叫数据包。要模拟接口保持时间，请关闭交换机上的 VLAN，以阻止对等体收到彼此的呼叫数据包。

远程命令执行

远程命令执行允许您将在命令行输入的命令发送到特定的故障切换对等体。

发送命令

由于配置命令会从主用设备或情景复制到备用设备或情景，所以无论您登录哪台设备，都可以使用 **failover exec** 命令在正确设备输入配置命令。例如，如果您登录到备用设备，可以使用 **failover exec active** 命令向主用设备发送配置更改。这些更改随后会复制到备用设备。不要使用 **failover exec** 命令向备用设备或情景发送配命令；这些配置更改不会被复制到主用设备，而且两种配置不会再进行同步。

configuration、exec 和 **show** 命令的输出显示在当前终端会话中，所以您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

过程

步骤 1 如果您处于多情景模式下，请使用 **changeto context***name* 命令更改要配置的情景。无法使用 **failover exec** 命令在故障切换对等体上更改情景。

步骤 2 使用以下命令，将命令发送到指定的故障切换设备：

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

使用 **active** 或 **standby** 关键字可导致命令在指定设备上执行，即便该设备为当前设备。使用 **mate** 关键字可导致命令在故障切换对等体上执行。

导致命令模式更改的命令不会更改当前会话的提示。必须使用 **show failover exec** 命令来显示执行该命令的命令模式。有关详细信息，请参阅更改命令模式。

更改命令模式

failover exec 命令会保持独立于您的终端会话命令模式的命令模式状态。默认情况下，**failover exec** 命令在指定设备的全局配置模式下启动。您可以使用 **failover exec** 命令发送适当的命令（如 **interface** 命令）来更改该命令模式。当使用 **failover exec** 更改模式时，会话提示不会更改。

例如，如果您登录到故障切换对的主用设备的全局配置模式，然后使用 **failover exec active** 命令切换到接口配置模式，终端提示将保持处于全局配置模式，但使用 **failover exec** 输入的命令在接口配置模式下输入。

以下示例显示了终端会话模式和 **failover exec** 命令模式之间的差异。在此示例中，管理员将主用设备上的 **failover exec** 模式更改为 GigabitEthernet0/1 接口的接口配置模式。之后，使用 **failover exec active** 将输入的所有命令都会发送到接口 GigabitEthernet0/1的接口配置模式。然后，管理员使用 failover exec active 为该接口分配 IP 地址。虽然提示表明处于全局配置模式，**failover exec active** 模式实际上处于接口配置模式。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

更改设备当前会话的命令模式不会影响 **failover exec** 命令使用的命令模式。例如，如果您在主用设备上处于接口配置模式，并且您未更改 **failover exec** 命令模式，以下命令将在全局配置模式下执行。结果是您与设备的会话将保持处于接口配置模式，而使用 **failover exec active** 输入的命令将发送到指定的路由进程的路由器配置模式。

```
ciscoasa(config-if)# failover exec active router ospf 100
```

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

使用 **show failover exec** 命令可显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。**show failover exec** 命令接受与 **failover exec** 命令相同的关键字：**active**、**mate** 或 **standby**。系统将单独跟踪每台设备的 **failover exec** 模式。

例如，以下内容是在备用设备上输入的 **show failover exec** 命令的示例输出：

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

安全注意事项

failover exec 命令使用故障切换链路向对等设备发送命令并接收对等设备的命令执行输出。您应在故障切换链路上启用加密，以防止窃听或中间人攻击。

远程命令执行的限制

当您使用远程命令时，会面临以下限制：

- 如果使用零停机升级程序升级一台设备，而不升级另一台设备，则两台设备正在运行的软件必须都支持 **failover exec** 命令。
- 命令完成和情景帮助对于 *cmd_string* 参数中的命令不可用。
- 在多情景模式下，只能向对等设备上的对等情景发送命令。要将命令发送到不同情景，必须在所登录的设备上切换到该情景。
- 不能将以下命令与 **failover exec** 命令配合使用：
  - **changeto**
  - **debug** (**undebug**)
- 备用设备处于故障状态时，如果这种故障是因服务卡故障引起，则该设备仍可以从 **failover exec** 命令接收命令；否则远程命令执行失败。
- 不能使用 **failover exec** 命令在故障切换对等体上从授权的 EXEC 模式切换到全局配置模式。例如，如果当前设备处于授权的 EXEC 模式下，并且您输入 **failover exec mate configure terminalfailover exec mate configure terminal**，则 **show failover exec mate** 输出将显示故障切换执行会话处于全局配置模式。但使用 **failover exec** 为对等体设备输入配置命令将会失败，直到您在当前设备上刚进入全局配置模式为止。
- 不能输入 recursive failover exec 命令，例如 **failover exec mate failover exec mate** 命令。

- 需要用户输入或确认的命令必须使用 **noconfirm** 选项。例如，要重新加载该伙伴，请输入：

  failover exec mate reload noconfirm

监控 故障切换

此部分用于监控故障切换状态。

故障切换消息

发生故障切换时，两台 ASA 都会发送系统消息。

故障切换系统日志消息

ASA 在优先级别 2 发出大量与故障切换有关的系统日志消息，级别 2 表示一种关键情况。要查看这些消息，请参阅系统日志消息指南。与故障切换关联的消息 ID 的范围是：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx 和 727xxx。例如，105032 和 105043 表示故障切换链路存在问题。

注释 故障切换期间，ASA 按照逻辑先关闭接口，再启动接口，从而生成日志消息 411001 和 411002。这是正常活动。

故障切换调试消息

要查看调试消息，请输入 **debug fover** 命令。有关更多信息，请参阅命令参考。

注释 由于调试输出在 CPU 进程中分配的高优先级，它可能会极大地影响系统性能。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug fover** 命令。

SNMP 故障切换陷阱

要接收故障切换的 SNMP 系统日志陷阱，请将 SNMP 代理配置为发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。

监控故障切换状态

要监控故障切换状态，请输入以下其中一个命令：

- **show failover**

  显示有关设备的故障切换状态的信息。

- **show failover group**

  显示有关故障切换组的故障切换状态的信息。显示的信息类似于**show failover**命令显示的信息，只不过前者限定于指定的组。

- **show monitor-interface**

  显示有关受监控接口的信息。

- **show running-config failover**

  显示运行配置中的故障切换命令。

故障切换历史记录

功能名称	版本	功能信息
主用/备用故障切换	7.0(1)	引入了此功能。
主用/主用故障切换	7.0(1)	引入了此功能。
故障切换密钥支持使用十六进制值	7.0(4)	现在可以指定十六进制值用于故障切换链路加密。 修改了以下命令：**failover key hex**。
支持故障切换密钥的主密码	8.3(1)	故障切换密钥现在支持主密码，该密码用于加密运行配置和启动配置中的共享密钥。如果您在不同 ASA 之间复制共享密钥（例如通过 **more system:running-config** 命令），您可以成功复制和粘贴加密的共享密钥。 注释 **failover key** 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。 修改了以下命令：**failover key** [**0** | **8**]。
添加了故障切换的 IPv6 支持。	8.2(2)	修改了以下命令：**failover interface ip**、**show failover**、**ipv6 address** 和 **show monitor-interface**。
在“同时”启动过程中，更改为故障切换组设备首选项。	9.0(1)	较早的软件版本中允许“同时”启动，以便故障切换组无需 **preempt** 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障切换组在要启动的第一台设备上都变为主用状态。

功能名称	版本	功能信息
支持 IPsec LAN 到 LAN 隧道加密故障切换和状态链路通信。	9.1(2)	现在可以将 IPSec LAN 到 LAN 隧道用于故障切换和状态链路加密，而不是对故障切换密钥使用专有加密（**failover key** 命令）。 注释 故障切换 LAN 到 LAN 隧道不计入 IPSec（其他 VPN）许可证。 引入或修改了以下命令：**failover ipsec pre-shared-key**、**show vpn-sessiondb**。
禁用硬件模块的运行状况监控	9.3(1)	默认情况下，ASA 会监控 ASA FirePOWER 模块等已安装硬件模块的运行状况。如果您不希望硬件模块故障触发故障切换，则可以禁用模块监控。 修改了以下命令：**monitor-interface service-module**
锁定故障切换对中的备用设备或备用情景上的配置更改	9.3(2)	现在可以锁定备用设备（主用/备用故障切换）或备用情景（主用/主用故障切换）上的配置更改，因此，除了正常的配置同步之外，将无法在备用设备上做出更改。 引入了以下命令：**failover standby config-lock**
在 ASA 5506H 上启用管理 1/1 接口作为故障切换链路	9.5(1)	现在您只能在 ASA 5506H 上将管理 1/1 接口配置为故障切换链路。此功能允许您使用设备上的所有其他接口作为数据接口。说明：如果您使用了此功能，便不能使用 ASA Firepower 模块，因为它要求管理 1/1 接口仍作为常规管理接口。 修改了以下命令：**failover lan interface**、**failover link**
现在支持在故障切换和 ASA 群集中增强运营商级 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）。现在支持在故障切换和 ASA 集群部署中使用此功能。 修改了以下命令：**show local-host**

功能名称	版本	功能信息
缩短了使用主用/备用故障切换时从 AnyConnect 进行动态 ACL 同步的时间	9.6(2)	当您在故障切换对上使用 AnyConnect 时，将关联的动态 ACL (dACL) 同步到备用设备的时间现在已缩短。以前，对于大量 dACL，同步时间可能需要几小时，在此期间，备用设备会一直忙于同步而不是提供高度可用的备份。 未修改任何命令。
多情景模式下 AnyConnect 连接的有状态故障切换	9.6(2)	现在，多情景模式下 AnyConnect 连接支持有状态故障切换 未修改任何命令。
现在，可为故障切换配置接口链路状态监控轮询以加快检测速度	9.7(1)	默认情况下，故障切换对中的每个ASA都会每隔 500 毫秒检查一次其接口的链接状态。现在，您可以在 300 毫秒和 799 毫秒之间配置轮询间隔；例如，如果将轮询时间设置为300毫秒，ASA则可以更快地检测接口故障并触发故障切换。 引入了以下命令：**failover polltime link-state**
Firepower 9300 和 4100 上支持使用双向转发检测 (BFD) 进行主用/备用故障切换运行状况监控	9.7(1)	您可以针对 Firepower 9300 和 4100 上主用/备用对两台设备之间的故障切换运行状况检查启用双向转发检测 (BFD)。将BFD用于运行状况检查比默认健康检查方法更可靠，并且 CPU 占用更少。 引入了以下命令：**failover health-check bfd**
禁用故障切换延迟	9.15（1）	当您使用网桥组或 IPv6 DAD 时，当发生故障切换时，新的主用设备会等待 3000 毫秒，等待备用设备完成网络任务并转换到备用状态。然后，主用设备便可以开始传输流量。要避免此类延迟，您可以禁用等待时间，主用设备将在备用设备转换之前开始传输流量。 新增/修改的命令：**failover wait-disable**