高可用性

以下主题介绍如何配置思科 Cisco Secure Firewall Management Center的主用/备用高可用性：

关于管理中心高可用性

要确保操作的连续性，可通过高可用性功能指定冗余管理中心以管理设备。管理中心支持主用/备用高可用性，其中一个设备是主用设备并管理设备。备用设备不会主动管理设备。主用设备将配置数据写入数据存储区并复制两个设备的数据，在必要时会通过同步与备用设备共享一些信息。

主用/备用高可用性允许您配置辅助 管理中心，以便在主 管理中心发生故障时接管该设备的功能。当主 管理中心发生故障时，必须升级辅助 管理中心使其成为主用设备。

事件数据从受管设备流到高可用性对中的两个 管理中心。如果一个管理中心发生故障，可以使用另一个管理中心继续不间断地监控网络。

请注意，配置为高可用性对的管理中心既无需在同一可信管理网络上，也不必在同一地理位置中。

注意 由于系统仅对主用管理中心开放某些功能，因此如果该设备发生故障，则必须将备用管理中心升级为主用设备。

注释 在成功部署更改后立即触发 管理中心 切换可能会导致预览配置在新的主用 管理中心上不起作用。这不会影响策略部署功能。建议在完成必要的同步后在 管理中心 上触发切换。

同样，当 管理中心 HA 同步处于降级状态时，触发切换或更改角色可能会使 管理中心 HA 损坏数据库，并且可能会造成灾难性的后果。我们建议您立即联系思科技术支持中心 (TAC) 寻求进一步帮助以解决此问题。

由于各种原因，此 HA 同步最终可能处于降级状态。本章中的 更换高可用性对中的 管理中心，第 19 页 部分介绍了一些故障场景以及修复问题的后续程序。如果降级状态的原因或场景与说明的场景匹配，请按照以下步骤解决问题。对于其他原因，我们建议您联系 TAC。

关于远程接入 VPN 高可用性

如果主设备具有使用 CertEnrollment 对象注册的身份证书的远程接入 VPN 配置，则辅助设备必须具有使用同一 CertEnrollment 对象注册的身份证书。由于特定于设备的重写，CertEnrollment 对象可以具有不同的主设备值和辅助设备值。其局限是必须在高可用性形成之前在两个设备上注册相同的 CertEnrollment 对象。

管理中心高可用性中的 SNMP 行为

在 SNMP 配置的 HA 对中，当您部署警报策略时，主管理中心会发送 SNMP 陷阱。当主 管理中心发生故障时，成为主用设备的辅助 管理中心 会发送 SNMP 陷阱，而无需进行任何其他配置。

Firepower 管理中心高可用性中的角色与状态

主/辅助角色

当在高可用性对中设置 Cisco Secure Firewall Management Center时，您可以将一个 Cisco Secure Firewall Management Center配置为主，将另一个配置为辅助。配置过程中，主设备的策略将同步到辅助设备。在此同步之后，主 Cisco Secure Firewall Management Center成为主用对等体，而辅助 Cisco Secure Firewall Management Center成为备用对等体，并且这两个设备将作为受管设备和策略配置的单个设备。

主用/备用状态

高可用性对中的两个 Cisco Secure Firewall Management Center之间的主要差异与哪个对等体是主用以及哪个对等体是备用相关。主用 Cisco Secure Firewall Management Center保持完整功能，您可以从中管理设备和策略。备用 Cisco Secure Firewall Management Center的功能是隐藏的，您不能进行任何配置更改。

管理中心高可用性对上的事件处理

由于高可用性对中的两个管理中心均可接收来自受管设备的事件，因此不会共享设备的管理 IP 地址。这意味着如果一个管理中心发生故障，您不需要为了确保继续处理事件而进行干预。

AMP 云连接和恶意软件信息

尽管它们共享文件策略和相关配置，但高可用性对中的 管理中心不会共享思科 AMP 云连接和恶意软件处置。为了确保工作连续性以及受检测文件的恶意软件处置情况在两个 管理中心上均相同，主用和备用 管理中心均必须能够访问 AMP 云。

URL 过滤和安全智能

URL 过滤和安全智能配置及信息在高可用性部署中的Cisco Secure Firewall Management Center之间同步。但是，只有主 Cisco Secure Firewall Management Center会下载 URL 类别和信誉数据，以获得安全智能源的更新。

如果主 Cisco Secure Firewall Management Center发生故障，则不仅必须确保辅助 Cisco Secure Firewall Management Center可以访问互联网以更新威胁智能数据，还必须使用辅助 Cisco Secure Firewall Management Center上的 Web 界面将其升级为主用设备。

管理中心 故障切换过程中的用户数据处理

如果主 管理中心 发生故障，则辅助 管理中心 会从 TS 代理身份源传播到受管设备的用户到 IP 映射；并从 ISE/ISE-PIC 身份源传播 SGT 映射。身份源尚未发现的用户被标识为“未知”。

停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”用户。

管理中心 高可用性对上的配置管理

在高可用性部署中，只有主用 管理中心可以管理设备和应用策略。两个管理中心都处于连续同步状态。

如果主用 管理中心失败，则高可用性对进入降级状态，直到您手动将备用设备升级到主用状态。升级完成后，设备将离开维护模式。

管理中心 高可用性灾难恢复

在灾难恢复情况下，必须执行手动切换。当主 管理中心 - FMC1 失败时，访问辅助 管理中心 - FMC2 的 Web 接口并交换对等体。这也适用于辅助 (FMC2) 发生故障的情况。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 17 页。

有关恢复失败的 管理中心，请参阅更换高可用性对中的 管理中心，第 19 页。

单点登录和高可用性对

高可用性配置中的管理中心可以支持单点登录，但必须牢记以下注意事项：

- 高可用性对的成员之间未同步 SSO 配置；您必须在 SSO 对的每个成员上单独配置 SSO。
- 高可用性对中的两个 管理中心必须使用相同的 IdP 进行 SSO。您必须在 IdP 上为每个 管理中心配置的 SSO 配置服务提供商应用。
- 在均配置为支持 SSO 的 管理中心高可用性对中，在用户首次使用 SSO 访问辅助 管理中心 之前，该用户必须首先使用 SSO 至少登录一次主 管理中心。
- 为高可用性对中的 管理中心配置 SSO 时：
  - 如果在主 管理中心上配置 SSO，则不需要在辅助 管理中心上配置 SSO。
  - 如果在辅助 管理中心上配置 SSO，则还需要在主 管理中心 上配置 SSO。（这是因为 SSO 用户必须在登录辅助 管理中心之前至少登录一次主 管理中心 。）

相关主题

配置 SAML 单点登录

管理中心备份期间的高可用性行为

对 管理中心高可用性对进行备份时，备份操作会暂停对等体之间的同步。在此操作过程中，您可以继续使用主用 管理中心，但不能使用备用对等体。

备份完成后，同步将继续，这将短暂地禁用主用对等体上的进程。在此暂停期间，“高可用性”页面将短暂显示一个保留页，直到所有进程都恢复为止。

管理中心 高可用性裂脑

如果高可用性对中的活动 管理中心关闭（电源问题、网络/连接问题所致），则可以将备用 管理中心提升为活动状态。当原始活动对等体出现时，两个对等体都可以假定它们处于活动状态。此状态被定义为“裂脑"。出现这种情况时，系统会提示您选择一个活动设备，这会将另一个设备降为备用状态。

如果活动管理中心关闭（或因网络故障而断开连接），您可以断开高可用性或切换角色。备用管理中心进入降级状态。

注释 当您解决裂脑时，不管将哪个设备用作预期的备用设备，都会丢失其所有设备注册和策略配置。例如，您将丢失对存在于预期的备用设备但却不在预期的主设备上的任何策略所做的修改。如果 管理中心处于高可用性裂脑情景中，即两个设备处于活动状态，并且您在解决裂脑之前注册受管设备并部署策略，则在重新建立高可用性之前，必须从预期的备用 管理中心导出所有策略并注销所有受管设备。然后，您可以注册受管设备并将策略导入到预期的活动 管理中心。

管理中心高可用性故障排除

本部分列出了有关某些常见 管理中心高可用性操作错误的故障排除信息。

错误	说明	解决方案
您必须在主用 管理中心 上重置密码，然后方可登录至备用设备。	当您的账户启用强制密码重置时，您尝试登录备用 管理中心 。	由于数据库对于备用 管理中心是只读的，因此请在主用 管理中心的登录页面上重置密码。
500 内部	如果在执行关键的 管理中心高可用性操作（包括切换对等角色或暂停和恢复同步）时尝试访问 Web 界面，可能会出现该错误。	请等到操作完成后再使用 Web 界面。
系统进程正在启动，请稍候 此外，Web 界面不响应。	如果在高可用性或数据同步操作期间管理中心重启（手动或从断电中恢复时），可能出现该错误。	1. 访问 管理中心外壳并使用 `manage_hadc.pl` 命令访问 管理中心高可用性配置实用程序。 **注释** 使用 `sudo` 以根用户身份运行该实用程序。 2. 使用选项 5 暂停镜像操作。 重新加载 管理中心 Web 界面。 3. 使用 Web 界面恢复同步。选择 **集成** > **其他集成**，然后点击 **高可用性** 选项卡，选择 **恢复同步**。
设备注册状态：主机 <*string*> 无法访问	在 威胁防御的初始配置期间，如果指定了 管理中心 IP 地址和 NAT ID，则 **主机** 字段可以留空。但是，在 NAT 后面 管理中心的 HA 环境中，在辅助 管理中心上添加 威胁防御 时会发生此错误。	1. 从主用 管理中心中删除 威胁防御 。请参阅 思科 Cisco Secure Firewall Management Center设备配置指南 中的从 删除设备管理中心。 2. 使用 **configure manager delete** 命令从 威胁防御 删除管理器。请参阅 Cisco Secure Firewall Threat Defense 命令参考。 3. 在 **主机** 字段中，通过 威胁防御 设备的 IP 地址或名称将 威胁防御 添加到 管理中心 。请参阅 思科 Cisco Secure Firewall Management Center 设备配置指南 中的将设备添加到管理中心。

错误	说明	解决方案
设备注册状态：主机 <*string*> 无法访问	在辅助 管理中心 和 威胁防御 设备均位于 NAT 之后，将 威胁防御 设备添加到高可用性部署中的辅助 管理中心 中心时，会发生此错误。	在备用 管理中心 Web 界面上，点击 **集成** > **其他集成** > **高可用性**。在待处理设备注册表下，点击待处理设备的 IP 地址，然后将 IP 地址更改为 威胁防御的公共 IP 地址。 或 1. 访问 威胁防御 shell 并使用 `show manager` 命令获取备用 管理中心 条目标识符值。 2. 在 威胁防御 shell 中，将备用 管理中心 主机名编辑为公共 IP 地址。执行 `configure manager edit` <standby_uuid>主机名<standby_ip> 命令使用条目标识符值和主机 IP 地址。 有关详细信息，请参阅 使用 CLI 解决管理中心 高可用性中的设备注册，第 16 页。
高可用性 管理中心之间的设备配置同步已停止。	在 管理中心 高可用性同步时，设备配置历史记录文件现在与其他配置数据并行同步。如果过去 6 个小时未发生同步， 管理中心 会监控配置历史记录文件同步任务，并在 HA 同步超时时通知您。此运行状况警报显示在主用和备用管理中心中。	主用和备用 管理中心都将进入降级状态。请联系 思科 TAC 以解决问题。

Firepower 管理中心高可用性要求

型号支持

请参阅硬件要求，第 7 页。

虚拟模型支持

请参阅虚拟平台要求，第 7 页。

支持的域

全局

用户角色

管理员

硬件要求

- 所有 管理中心 硬件支持高可用性。对等体必须为同一型号。
- 对等体可能在物理上和地理上在不同的数据中心中相互分离。
- 高可用性配置的带宽要求取决于各种因素，例如网络规模、受管设备数量、事件和日志量，以及配置更新的大小和频率。

  对于典型的 管理中心 高可用性部署，在接近100毫秒的高延迟网络的情况下，建议对等体之间的网络带宽至少为 5 Mbps。

  您可以通过减少 管理中心上保存的配置版本数来提高高可用性同步速度。有关详细信息，请参阅 Cisco Secure Firewall Management Center Snort 3 配置指南中的 设备配置版本的序号 。请注意， Cisco Secure Firewall Management Center 版本 7.3.0 和 7.4.0 不支持此选项。
- 不要将主要对等体的备份恢复到辅助对等体。
- 另请参阅 管理中心高可用性配置的许可证要求，第 8 页。

虚拟平台要求

以下公共云平台支持高可用性：

- Amazon Web Services (AWS)
- Oracle 云基础设施 (OCI)

以及这些内部部署/私有云平台：

- 思科 HyperFlex
- 基于内核的虚拟机 (KVM)
- Microsoft Hyper-V
- VMware vSphere/VMware ESXi

管理中心 必须具有相同的设备管理能力（FMCv2 不支持）和相同的许可。您还需要为每个托管设备提供一个 威胁防御 授权。有关详细信息，请参阅 管理中心高可用性配置的许可证要求，第 8 页。

软件要求

可以访问**设备信息**构件，以验证软件版本、入侵规则更新版本和漏洞数据库更新。默认情况下，该构件将显示在 **详细控制面板** 和 **摘要控制面板**的 **状态** 选项卡上。有关详细信息，请参阅设备信息构件

- 高可用性配置中的两个 管理中心必须具有相同的主要（第一个数字）、次要（第二个数字）和维护（第三个数字）软件版本。
- 高可用性配置中的两个 管理中心必须安装相同版本的入侵规则更新。
- 高可用性配置中的两个 管理中心必须安装相同版本的漏洞数据库更新。
- 高可用性配置中的两个 管理中心必须安装相同版本的 LSP（轻量安全安装包）。

警告 如果两个 管理中心上的软件版本、入侵规则更新版本和漏洞数据库更新版本不相同，则将无法建立高可用性。

管理中心高可用性配置的许可证要求

每台设备都需要相同的许可证，无论是由单个 管理中心 管理还是由 管理中心高可用性对（硬件或虚拟）中的管理。

示例： 如果要对由 管理中心 对管理的两个设备启用高级恶意软件保护，请购买两个 恶意软件防御许可证和两个 TM 订用，向智能软件管理器注册主要 管理中心，然后将许可证分配给主要 管理中心上的两个设备。

只有主用 管理中心会向智能软件管理器注册。故障切换发生时，系统与智能软件管理器通信，以释放原始主用 管理中心 中的许可证授权，并将其分配到新的主用 管理中心。

在特定许可证预留部署中，只有主 管理中心 需要特定许可证预留。

硬件 管理中心

高可用性对中的 管理中心硬件不需要特殊许可证。

Management Center Virtual

您将需要两个相同许可的 Management Center Virtual。

示例： 对于管理 10 台设备的 Management Center Virtual 高可用性对，您可以使用：

- 两（2） Management Center Virtual 10个授权
- 10 个设备许可证

如果中断高可用性对，则会释放与辅助 Management Center Virtual 关联的 Management Center Virtual 授权。（在本例中，您将有两个独立的 Management Center Virtual 10。）

管理中心 高可用性的前提条件

在建立 管理中心 高可用性对之前：

- 从预期的辅助 管理中心向预期的主 管理中心导出所需的策略。有关详细信息，请参阅导出配置。
- 确保预期的辅助管理中心没有添加任何设备。删除预期的辅助管理中心中的设备，并将这些设备注册到预期的主 管理中心。有关详细信息，请参阅 从 管理中心删除设备 和 向 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理中心 添加设备。
- 将策略导入到预期的主 管理中心。有关详细信息，请参阅导入配置。
- 在预期的主 管理中心上，验证导入的策略，根据需要进行编辑，并将它们部署到相应的设备。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 部署配置更改 。
- 在预期的主 管理中心上，为新添加的设备关联适当的许可证。有关详细信息，请参阅将许可证分配给单个设备。

现在可以继续建立高可用性。有关详细信息，请参阅 建立 管理中心 高可用性 ， 第 9 页。

建立 管理中心 高可用性

建立高可用性可能会花费大量时间，甚至数小时，具体取决于对等体之间的带宽和策略数量。它还取决于已注册到主用 管理中心的设备数量，该数量需要同步到备用 管理中心。可以查看“高可用性”页面，以检查高可用性对等体的状态。

开始之前

- 确认两个 管理中心都符合高可用性系统要求。有关更多信息，请参阅Firepower 管理中心高可用性要求 ， 第 6 页。
- 确认已达到建立高可用性的先决条件。有关详细信息，请参阅 管理中心 高可用性的前提条件 ， 第 8 页。
- 在多域部署中，必须在全局域中才能执行此任务。

过程

步骤 1 登录到希望指定为辅助的 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 在此 管理中心的“角色”下，选择**辅助**。

步骤 5 在**主 Firepower 管理中心主机**文本框中，输入主 管理中心 的主机名或 IP 地址。

如果主 管理中心没有可从对等 管理中心 访问的 IP 地址（可以是公共或私有 IP 地址），则可以将此字段留空。在此情况下，请同时使用**注册密钥**和**唯一 NAT ID** 字段。您需要指定至少一个 管理中心 的 IP 地址才能启用 HA 连接。

步骤 6 在**注册密钥**文本框中输入一个一次性注册密钥。

该注册密钥是任何用户定义的字母数字值，最长 37 个字符。此注册表项将用于注册辅助和主 管理中心。

步骤 7 如果没有指定主 IP 地址，或者如果并未计划指定主 管理中心上的辅助 IP 地址，则请在**唯一 NAT ID** 字段中，输入一个唯一的字母数字 ID。有关详细信息，请参阅NAT 环境。

步骤 8 点击**注册 (Register)**。

步骤 9 使用具有管理员访问权限的帐户登录到要指定为主管理中心的防御中心。

步骤 10 选择**集成** > **其他集成**。

步骤 11 选择**高可用性**。

步骤 12 在此 管理中心的“角色”下，选择**主**。

步骤 13 在**辅助 Firewall Management Center 主机**文本框中输入次要 管理中心 的主机名或 IP 地址。

如果辅助 管理中心 没有可从对等 管理中心 访问的 IP 地址（可以是公共或私有 IP 地址），则可以将此字段留空。在此情况下，请同时使用**注册密钥**和**唯一 NAT ID** 字段。您需要指定至少一个 管理中心 的 IP 地址才能启用 HA 连接。

步骤 14 在第 6 步中使用的**注册密钥**文本框中输入同一个一次性注册密钥。

步骤 15 如果需要，请在**唯一 NAT ID** 文本框中输入在第 7 步中使用的同一个 NAT ID。

步骤 16 点击 **Register**。

下一步做什么

建立 管理中心 高可用性时，注册到主用 管理中心的设备将自动注册到备用 管理中心。

注释 如果已注册的设备拥有 NAT IP 地址，则自动设备注册将失败，并且辅助 管理中心 的“高可用性”页面会将该设备列为本地、待处理状态。随后可在备用 管理中心的“高可用性”页面上为该设备分配另一个 NAT IP 地址。如果自动注册在备用 管理中心上因其他原因失败，但该设备显示为已注册到主用 Cisco Secure Firewall 管理中心，则请参阅 使用 CLI 解决 管理中心 高可用性中的设备注册，第 16 页。

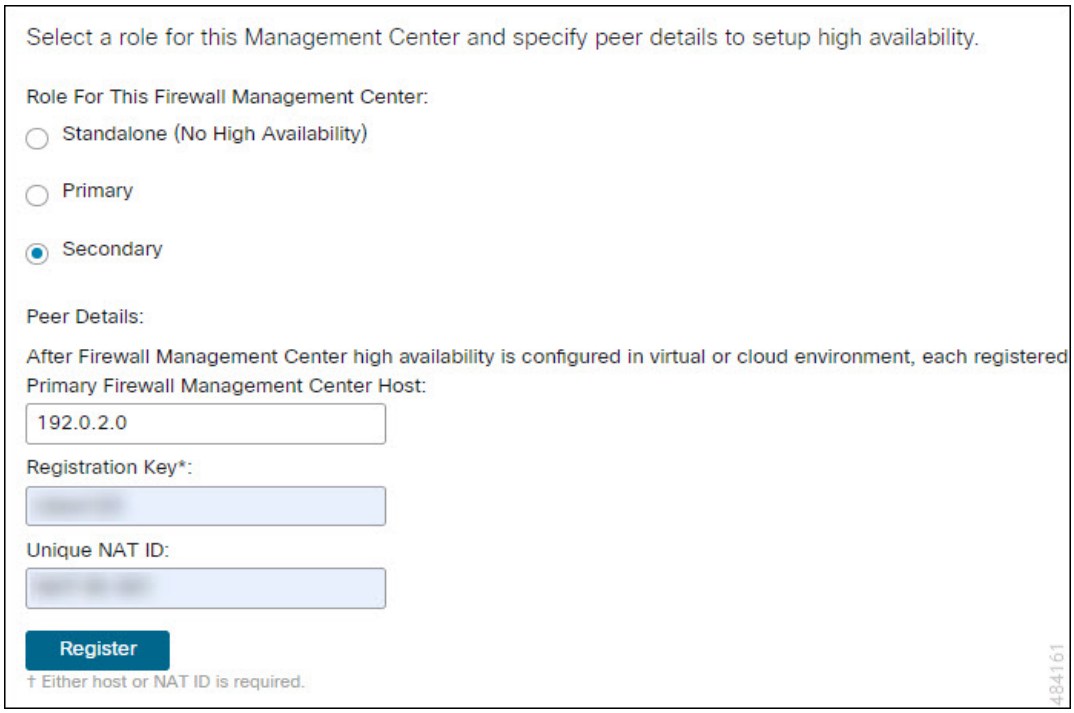
公共云上托管的 管理中心 的高可用性

在公共云上托管的 管理中心 之间建立高可用性时，下面介绍的主要和辅助 管理中心 的 IP 地址或主机名组合可以成功形成高可用性，并让设备在两个对等体上注册。在**高可用性 (High Availability)** 页面（**集成 (Integration)** > **其他集成 (Other Integrations)** > **高可用性 (High Availability)**）中，执行以下配置之一，以在公共云中托管的 管理中心 之间成功形成高可用性。

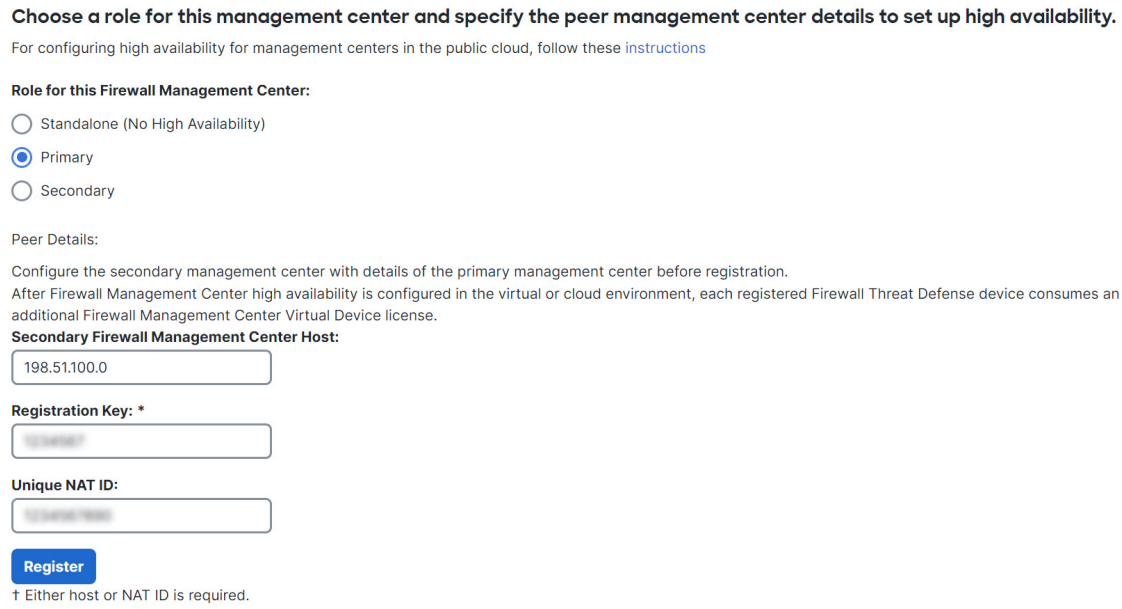
同时对主要和辅助 管理中心 使用公共 IP 地址或主机名

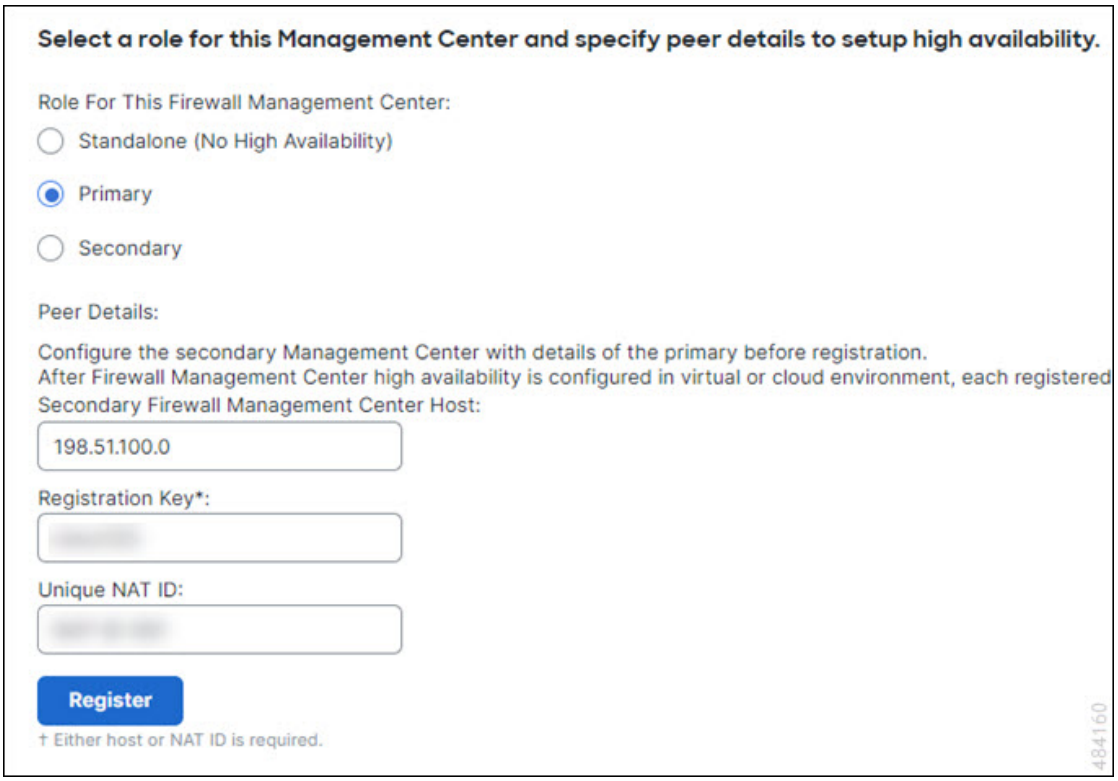
1. 在辅助 管理中心 上，执行以下操作：

1. 选择**辅助 (Secondary)** 作为此 **Firewall Management Center** 的角色。
2. 在**主要防火墙管理中心主机 (Primary Firewall Management Center Host)** 文本框中，输入辅助 管理中心 的公共 IP 地址或主机名。
3. 输入注册密钥。
4. 输入您在主 管理中心 中使用的相同 NAT ID。



2. 在主 管理中心 上，执行以下操作：
   1. 选择**主要 (Primary)** 作为此 **Firewall Management Center** 的角色。
   2. 在**辅助防火墙管理中心主机 (Secondary Firewall Management Center Host)** 文本框中，输入辅助 管理中心 的公共 IP 地址或主机名。
   3. 输入注册密钥。
   4. 输入唯一的 NAT ID。

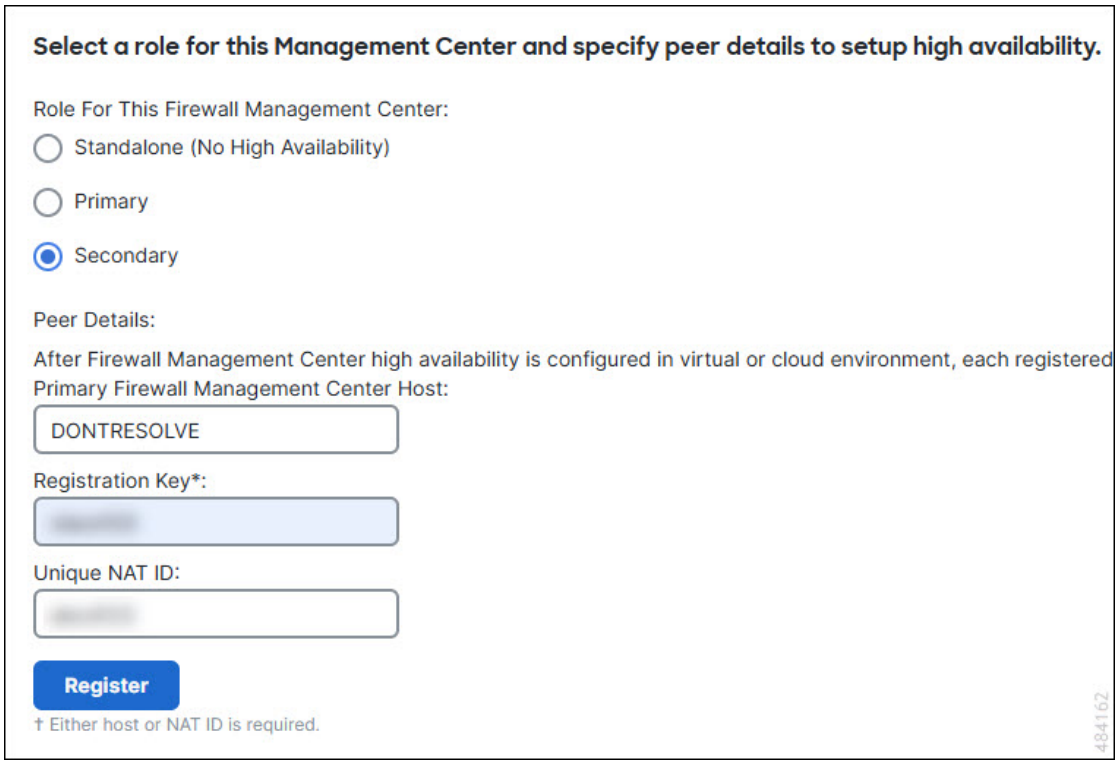




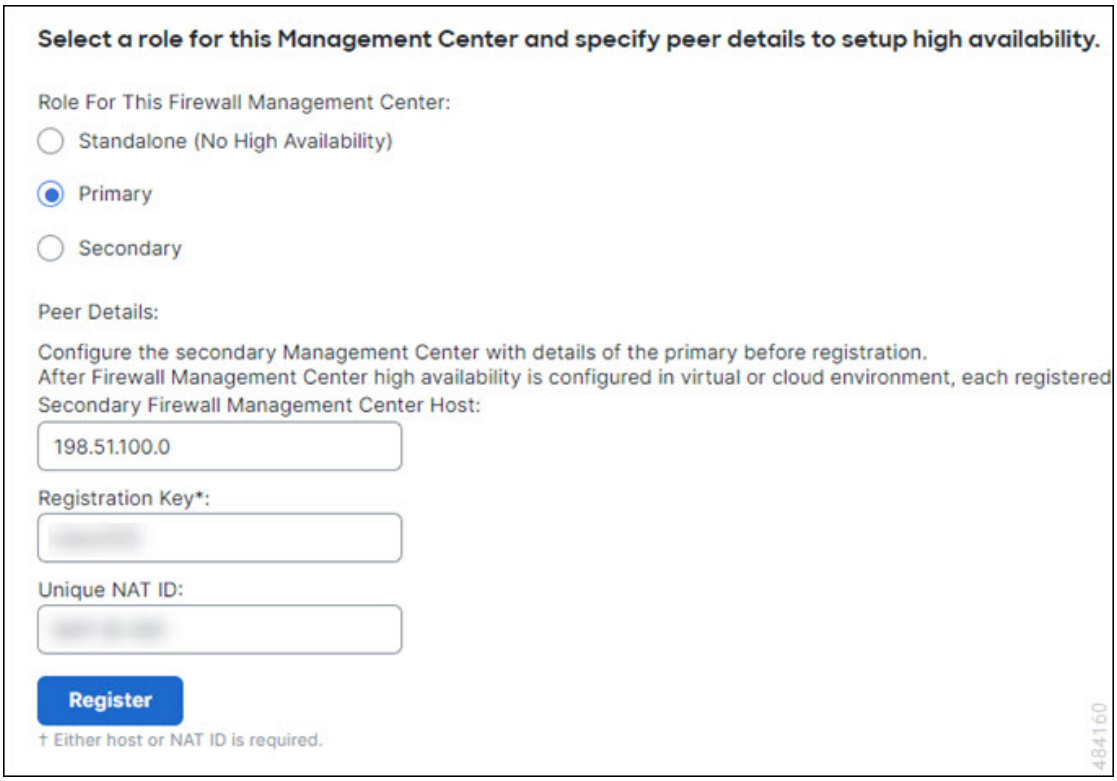
对辅助 管理中心 使用公共 **IP** 地址或主机名

1. 在辅助 管理中心上，执行以下操作：
    1. 选择辅助 **(Secondary)** 作为此 **Firewall Management Center** 的角色。

2. 在**主要防火墙管理中心主机 (Primary Firewall Management Center Host)** 字段中输入 **DONTRESOLVE**。
3. 输入注册密钥。
4. 输入您在主 管理中心 中使用的相同 NAT ID。



2. 在主 管理中心 上，执行以下操作：
   1. 选择**主要 (Primary)** 作为此 **Firewall Management Center** 的角色。
   2. 在**辅助防火墙管理中心主机 (Secondary Firewall Management Center Host)** 文本框中，输入辅助 管理中心 的公共 IP 地址或主机名。
   3. 输入注册密钥。
   4. 输入唯一的 NAT ID。



查看 管理中心 高可用性状态

在识别主用和备用 管理中心后，可以查看关于本地 管理中心及其对等体的信息。

注释 在此上下文中，“本地对等体”是指您要查看其系统状态的设备。“远程对等体”是指其他设备，无论是处于主用还是备用状态。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

可以查看：

摘要信息

- 高可用性对的运行状态。当备用设备从主用设备接收配置更改时，正常运行的系统的状态将在“运行状况正常”和“正在进行同步任务”之间摆动。

- 高可用性对的当前同步状态
- 主用对等体的 IP 地址及其上次同步时间
- 备用对等体的 IP 地址及其上次同步时间

系统状态

- 两个对等体的 IP 地址
- 两个对等体的操作系统
- 两个对等体的软件版本
- 两个对等体的设备型号

注释
您只能在主用 管理中心上查看出口控制和合规性状态。

在 管理中心 高可用性对上同步的配置

在两个 管理中心之间建立高可用性时，两个设备之间将同步以下配置数据：

- 许可证授权
- 访问控制策略
- 入侵规则
- 恶意软件和文件策略
- DNS 策略
- 身份策略
- SSL 策略
- 预过滤策略
- 网络发现规则
- 应用检测器
- 关联策略规则
- 风险通告
- 扫描程序
- 响应组
- 用于调查事件的外部资源的上下文交叉启动

- 补救设置，但您必须在两个 管理中心上安装自定义模块。有关补救设置的详细信息，请参阅管理补救模块。

在高可用性对中配置对 管理中心 数据库的外部访问

在高可用性设置中，我们建议您仅使用活动对等体来配置对数据库的外部访问。为外部数据库访问配置备用对等体时，会导致频繁断开连接。要恢复连接，必须 暂停成对管理中心之间的通信 并 重新启动成对 管理中心之间的通信 备用对等体的同步。有关如何启用对 管理中心的外部数据库访问的信息，请参阅 启用对数据库的外部访问。

使用 CLI 解决 管理中心 高可用性中的设备注册

如果备用 管理中心上的自动设备注册失败，但似乎已注册到主用 管理中心，请完成以下步骤：

警告 如果执行辅助 管理中心 RMA或添加辅助 管理中心RMA，则受管设备会注销，因此会删除其配置。

过程

步骤 1 从主用 管理中心中删除设备。在 Cisco Secure Firewall Management Center 设备配置指南从 管理中心删除（注销）设备 。

步骤 2 要在备用设备 管理中心上触发设备的自动注册，请完成以下步骤：

1. 登录到受影响设备的 CLI。
2. 运行 CLI 命令： **configure manager delete**。

   此命令将会禁用并删除当前的 管理中心。
3. 运行 CLI 命令： **configure manager add**。

   此命令会将设备配置为发起与 管理中心的连接。

   提示
   仅面向活动 管理中心在设备上配置远程管理。建立高可用性时，设备将自动注册到备用 管理中心。
4. 登录主用 管理中心 并注册设备。

步骤 3 如果备用 管理中心 位于 NAT 之后，请完成以下步骤以编辑备用 管理中心的主机名：

1. 访问 威胁防御 shell 并使用 `show manager` 命令获取备用 管理中心 条目标识符值。

2. 在 威胁防御 shell 中，将备用 管理中心 主机名编辑为公共 IP 地址。执行 `configure manager edit` <standby_uuid>主机名<standby_ip>命令使用条目标识符值和主机 IP 地址。

在管理中心高可用性对中切换对等体

由于系统将某些功能限制为适用于主用管理中心，因此如果该设备发生故障，则必须将备用管理中心升级为主用设备：

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**切换角色**以将本地角色从主用更改为备用，或者从备用更改为主用。在 Primary 或 Secondary 指定保持不变的情况下，角色在两个对等体之间切换。

暂停成对管理中心之间的通信

如果要临时禁用高可用性，您可以在管理中心之间禁用通信信道。您可以从主用或备用对等体上暂停同步。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**暂停同步**。

重新启动成对 管理中心之间的通信

如果暂时禁用了高可用性，可以通过启用管理中心之间的通信通道重新启动高可用性。您可以从主用或备用对等体恢复同步。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**恢复同步**。

在高可用性对中更改 管理中心 的 IP 地址

如果更改其中一个高可用性对等体的IP地址，则此更改不会在另一个对等体上自动更新，即使在执行高可用性同步之后也是如此。要确保远程对等体 管理中心 也已更新，您必须手动更改 IP 地址。

过程

步骤 1 登录到要在其中手动修改另一个对等管理器的 IP 地址的对等体 管理中心 。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**对等体管理器**。

步骤 5 选择**编辑** (✎)。

步骤 6 输入设备的显示名称，该名称仅在系统环境内使用。

输入另一个显示名称不会更改设备的主机名。

步骤 7 输入完全限定域名、通过本地 DNS 解析为有效 IP 地址的名称（即，主机名）或主机 IP 地址。

步骤 8 点击**保存 (Save)**。

禁用 管理中心 高可用性

过程

步骤 1 登录高可用性对中的其中一个管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**破坏高可用性**。

步骤 5 选择以下选项之一来处理受管设备：

- 要使用此 管理中心控制所有受管设备，请选择**从此控制台管理注册设备**。所有设备都将从对等体取消注册。
- 要使用其他 管理中心控制所有受管设备，请选择**从对等体控制台管理注册设备**。所有设备都将从此管理中心取消注册。
- 要一起停止管理设备，请选择**从两个控制台停止管理注册设备**。所有设备都将从这两个管理中心取消注册。

注释
如果选择要从辅助管理中心管理注册的设备，则设备将从主要管理中心取消注册。设备现在已注册为由辅助 管理中心管理。但是，应用到这些设备的许可证会由于高可用性中断操作而取消注册。您现在必须从辅助 管理中心中的设备继续重新注册（启用）许可证。有关详细信息，请参阅将许可证分配到设备。

步骤 6 点击**确定 (OK)**。

更换高可用性对中的 管理中心

如果需要更换管理中心高可用性对中的故障设备，则必须按照下面列出的程序之一进行操作。该表列出了四种可能的故障场景，及其相对应的更换程序。

故障状态	数据备份状态	更换程序
主 管理中心发生故障	数据备份成功	更换出现故障的主 管理中心（成功备份），第 19 页
	数据备份未成功	更换发生故障的主 管理中心（成功备份），第 20 页
辅助 管理中心发生故障	数据备份成功	更换出现故障的辅助 管理中心（成功备份），第 21 页
	数据备份未成功	替换失败的辅助 管理中心（不成功的备份），第 22 页

更换出现故障的主 管理中心（成功备份）

两个 管理中心、*FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务描述在主设备数据备份成功时更换发生故障的主 管理中心、*FMC1* 的步骤。

开始之前

验证发生故障的主 管理中心的数据备份是否成功。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC1*。

步骤 2 当主 管理中心 - *FMC1* 失败时，访问辅助 管理中心 - *FMC2* 的 Web 接口并交换对等体。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 17 页。

这会将辅助 管理中心 - *FMC2* 升级到主用状态。

可以将 *FMC2* 用作主 管理中心，直到主 管理中心 - *FMC1* 被替换。

注意
不要破坏 *FMC2*中的 管理中心 高可用性，因为从 *FMC1* 同步到 *FMC2* 的许可证（故障之前）将从 *FMC2* 中删除，您将无法从 *FMC2*执行任何部署操作。

步骤 3 使用与 *FMC1*相同的软件版本重新映像更换的 管理中心 。

步骤 4 将从 *FMC1* 检索到的数据备份还原到新的 管理中心。

步骤 5 安装所需的 管理中心补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC2*。

新的 管理中心和 *FMC2* 现在都是主用对等体，导致高可用性被破坏。

步骤 6 当 管理中心 Web 界面提示您选择主用设备时，请选择 *FMC2* 作为主用设备。

这会将最新的配置从 *FMC2* 同步到新的 管理中心 - *FMC1*。

步骤 7 配置成功同步后，访问辅助 管理中心 - *FMC2* 的 Web 界面并交换角色，以使主 管理中心 - *FMC1* 变成主用状态。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 17 页。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

更换发生故障的主 管理中心（成功备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务介绍在从主管理中心进行数据备份不成功时，替换失败的主 管理中心 -*FMC1* 的步骤。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC1*。

步骤 2 当主 管理中心 - *FMC1* 失败时，访问辅助 管理中心 - *FMC2* 的 Web 接口并交换对等体。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 17 页。

这会将辅助 管理中心 - *FMC2* 升级到主用状态。

可以将 *FMC2* 用作主 管理中心，直到主 管理中心 - *FMC1* 被替换。

注意
不要破坏 *FMC2*中的 管理中心 高可用性，因为从 *FMC1* 同步到 *FMC2* 的许可证（故障之前）将从 *FMC2* 中删除，您将无法从 *FMC2*执行任何部署操作。

步骤 3 使用与 *FMC1*相同的软件版本重新映像更换的 管理中心 。

步骤 4 安装所需的 管理中心补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC2*。

步骤 5 从思科智能软件管理器取消注册 管理中心 - *FMC2*。有关详细信息，请参阅取消注册 管理中心。

从思科智能软件管理器取消注册管理中心可将管理中心从您的虚拟帐户中删除。与 管理中心关联的所有许可证授权将释放回虚拟账户。注销后，管理中心会进入“执行”模式，在此模式下，不允许对许可功能进行更新或更改。

步骤 6 访问辅助 管理中心 - *FMC2* 的 Web 截面，并中断 管理中心 高可用性。有关详细信息，请参阅禁用 管理中心 高可用性，第 18 页。在提示选择用于处理受管设备的选项时，请选择**通过此控制台管理已注册的设备**。

因此， 同步到辅助 管理中心的证书 - *FMC2*的典型和智能许可证将被删除，您无法从 *FMC2*执行部署活动。

步骤 7 通过将 管理中心 - *FMC2* 设置为主并将 管理中心 - *FMC1* 设置为辅助，重新建立 管理中心 高可用性。有关详细信息，请参阅建立 管理中心 高可用性，第 9 页。

步骤 8 向主 管理中心 - *FMC2*注册智能许可证。有关详细信息，请参阅将管理中心注册到智能软件管理器。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

更换出现故障的辅助 管理中心（成功备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务描述当来自出现故障的辅助 管理中心 -*FMC2* 的数据备份成功时更换该设备的步骤。

开始之前

验证来自出现故障的辅助 管理中心的数据备份是否成功。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC2*。

步骤 2 继续使用主 管理中心 - *FMC1* 作为主用 管理中心。

步骤 3 使用与 *FMC2*相同的软件版本重新映像更换的 管理中心 。

步骤 4 将从 *FMC2* 的数据备份还原到新的 管理中心。

步骤 5 安装所需的 管理中心 补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC1*。

步骤 6 从新的 管理中心 - *FMC2*的 Web 界面恢复数据同步（如果已暂停），以同步来自主 管理中心 - *FMC1* 的最新配置。有关详细信息，请参阅重新启动成对 管理中心之间的通信， 第 17 页。

“经典”和“智能”许可证将无缝工作。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

替换失败的辅助 管理中心（不成功的备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务介绍了在从辅助设备备份数据失败后，更换发生故障的辅助 管理中心 (*FMC2*) 的步骤。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC2*。

步骤 2 继续使用主 管理中心 - *FMC1* 作为主用 管理中心。

步骤 3 使用与 *FMC2*相同的软件版本重新映像更换的 管理中心 。

步骤 4 安装所需的 管理中心 补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC1*。

步骤 5 访问主 管理中心 - *FMC1* 的 Web 截面，并中断 管理中心 高可用性。有关详细信息，请参阅禁用 管理中心 高可用性， 第 18 页。在提示选择用于处理受管设备的选项时，请选择**通过此控制台管理已注册的设备**。

步骤 6 通过将 管理中心 - *FMC1* 设置为主并将 管理中心 - *FMC2* 设置为辅助，重新建立 管理中心 高可用性。有关更多信息，请参阅建立 管理中心 高可用性， 第 9 页。

- 在成功建立高可用性后，将来自主 管理中心 - *FMC1* 的最新配置同步到辅助 管理中心 - *FMC2*。
- “经典”和“智能”许可证将无缝工作。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

管理中心 高可用性灾难恢复

在灾难恢复情况下，必须执行手动切换。当主 管理中心 - FMC1 失败时，访问辅助 管理中心 - FMC2 的 Web 接口并交换对等体。这也适用于辅助 (FMC2) 发生故障的情况。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 17 页。

有关恢复失败的 管理中心，请参阅更换高可用性对中的 管理中心，第 19 页。

恢复高可用性对中的管理中心（无硬件故障）

要在没有硬件故障的情况下恢复 管理中心 高可用性对，请执行以下程序：

- 在主要管理中心恢复备份 ，第 23 页
- 在辅助管理中心恢复备份，第 23 页

在主要管理中心恢复备份

开始之前

- 没有硬件故障和更换管理中心。
- 您熟悉备份和恢复过程。请参阅备份/恢复。

过程

步骤 1 验证主要 管理中心 的备份是否可用 - /var/sf/backup/ 中的本地存储或远程网络卷。

步骤 2 在主要 管理中心上暂停同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以暂停同步。

步骤 3 恢复所更换的主要 管理中心的备份。恢复完成后， 管理中心 会重新启动。

步骤 4 一旦主要管理中心处于活动状态且其用户接口可访问，则在辅助 管理中心上恢复同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以恢复同步。

在辅助管理中心恢复备份

开始之前

- 没有硬件故障和更换管理中心。
- 您熟悉备份和恢复过程。请参阅备份/恢复。

过程

步骤 1 验证辅助 管理中心 的备份是否可用 - /var/sf/backup/ 中的本地存储或远程网络卷。

步骤 2 在主要 管理中心上暂停同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以暂停同步。

步骤 3 在辅助 管理中心上恢复备份。恢复完成后， 管理中心 会重新启动。

步骤 4 一旦辅助 管理中心 处于活动状态且其用户接口可访问，则在主要 管理中心上恢复同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以恢复同步。

高可用性管理中心的统一备份

您可以在主用 管理中心上执行统一备份，其中为主用和备用 管理中心创建单个备份文件。统一备份仅适用于仅配置备份。如果需要事件或 TID 备份，则必须对主用和备用 管理中心进行单独的备份。当您选择仅配置备份时，默认情况下会应用统一备份。在统一备份中，如果主用设备 管理中心无法从备用设备 管理中心获取备份 tar 文件，则会为主用设备生成可用于恢复的正常备份文件。与普通备份相比，统一备份有几个优势：

- 统一备份不要求您在主用和备用 管理中心上进行单独的备份。
- 备份中的冗余数据和存储限制在统一备份中删除。
- 在正常备份中，当主设备发生故障且辅助设备备份不可用时，您必须中断辅助 RMA 的高可用性配对。这种情况在统一备份中被根除。
- 通常，无法安排备用设备的备份。在计划的统一备份中，会同时使用主用设备和备用设备的备份。
- 执行统一备份时，不必暂停 HA 同步即可在备用设备上执行备份。

如果发生意外事件，您可以使用统一备份来恢复新的 RMA 设备。您可以通过名称识别统一备份文件。在统一备份文件名中添加前缀“Unified”。您可以选择 管理中心 进行恢复，也可以选择其状态（主用/备用）。

确保选择已恢复 管理中心 的适当状态，以防止裂脑冲突。

从统一备份恢复管理中心

使用此程序可从 统一备份恢复 管理中心 （仅配置）。

过程

步骤 1 登录到要恢复的 管理中心 。

步骤 2 选择**系统** (⚙) > **工具** > **备份/恢复**。

“备份管理”页面列出所有本地和远程存储的备份文件，包括统一的备份文件（仅配置）。

如果统一备份文件不在列表中，并且您已将其保存在本地计算机上，请点击**上传备份**；请参阅管理备份和远程存储。

步骤 3 选择要恢复的统一备份文件并点击 **恢复**。

步骤 4 在 **恢复备份** 页面中，选择要恢复的设备。由于统一备份存储主设备和辅助设备 管理中心的备份配置，因此您需要选择要恢复的设备。

步骤 5 要选择已恢复的 管理中心的状态，请点击 **主** 用或 **备用** 单选按钮。请务必验证正在使用的管理中心的角色和状态，以免两个对等体的角色和状态配置相同。在恢复时，如果为管理中心选择的角色和状态不正确，可能会带来高可用性失败。

步骤 6 点击 **恢复**，然后点击 **确认恢复** 开始恢复。

管理中心 高可用性历史

功能	管理中心最低版本	威胁防御最低版本	详情
用于高可用性管理中心的单个备份文件。	7.4.1 7.2.6	任意	对高可用性对中的主用管理中心执行仅配置备份时，系统现在会创建一个备份文件，您可以使用该文件恢复任一设备。 其他版本限制：不支持管理中心版本 7.3.x 或 7.4.0。
管理中心高可用性同步增强功能。	7.4.1	任意	管理中心高可用性 (HA) 包括以下同步增强功能： • 大型配置历史记录文件可能会导致高延迟网络中的同步失败。为了防止这种情况发生，设备配置历史记录文件现在与其他配置数据并行同步。此增强功能还缩短了同步时间。 • 管理中心现在监控配置历史记录文件同步过程，并在同步超时时显示运行状况警报。 新增/修改的屏幕：您可以在以下屏幕上查看这些警报： • **通知** > **邮件中心** > **运行状况** • **集成** > **其他集成** > **高可用性** > **状态** （在 **摘要** 下）
Hyper-V 上的高可用性支持。	7.4.0	任意	我们现在支持适用于 Hyper-V 的 Management Center Virtual 高可用性。
支持 KVM 上的高可用性。	7.3.0	任意	我们现在支持适用于 KVM 的 Management Center Virtual 高可用性。
支持 AWS 和 OCI上的高可用性。	7.1.0	任意	我们现在支持适用于 AWS 和 OCI 的 Management Center Virtual 高可用性。

功能	管理中心最低版本	威胁防御最低版本	详情
HyperFlex 上的高可用性支持。	7.0.0	任意	我们现在支持适用于 HyperFlex 的 Management Center Virtual 高可用性。
VMware 上的高可用性支持。	6.7.0	任意	我们现在支持适用于 VMware 的 Management Center Virtual 高可用性。
单点登录。	6.7.0	任意	为单点登录配置高可用性对的一个或两个成员时，必须考虑特殊注意事项。

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。