



更改后任务和验证

- [Cisco Unified Communications Manager 节点的更改后任务](#)，第 1 页
- [Cisco Unified Communications Manager 节点的启用安全的群集任务](#)，第 4 页
- [IM and Presence Service 节点的更改后任务](#)，第 5 页

Cisco Unified Communications Manager 节点的更改后任务

执行所有更改后任务，以确保更改在部署中正确实施。



注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

过程

- 步骤 1** 如果在 Cisco Unified Communications Manager 服务器上的任何位置配置了 DNS，请确保已配置正向和反向查找区域，并且 DNS 可访问且在正常工作。
- 步骤 2** 检查活动的服务器关机警告，确保群集中的所有服务器都在运行并可用。使用 Cisco Unified 实时监控工具 (RTMT) 或在第一个节点上使用命令行界面 (CLI) 进行检查。
- 要使用 Unified RTMT 进行检查，请访问警告中心并检查服务器关机警告。
 - 要在第一个节点上使用 CLI 进行检查，请输入以下 CLI 命令并检查应用程序事件日志：

```
file search activelog syslog/CiscoSyslog ServerDown
```

- 步骤 3** 检查群集中所有节点的数据库复制状态，确保所有服务器均已成功复制数据库更改。
- 对于 IM and Presence Service，如果您的部署中有多个节点，请使用 CLI 检查数据库发布方节点上的数据库复制状态。
- 请使用 Unified RTMT 或 CLI。所有节点的状态应显示为 **2**。
- 要使用 RTMT 进行检查，请访问“数据库摘要”并检查复制状态。
 - 要使用 CLI 进行检查，请输入 `utils dbreplication runtimestate`。

对于输出示例，请参阅与数据库复制输出示例相关的主题。有关详细的程序和故障诊断，请参阅与数据库复制验证和数据库复制故障诊断相关的主题。

步骤 4 如以下示例中所示输入 CLI 命令 `utils diagnose`，以检查网络连接和 DNS 服务器配置。

示例:

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
===== test - validate_network : Passed Diagnostics Completed
admin:
```

如果执行的是更改前系统运行状况检查，则任务已完成；否则，继续执行更改后验证步骤。

步骤 5 验证新的主机名或 IP 地址是出现在 Cisco Unified Communications Manager 服务器列表中。在 Cisco Unified Communications Manager 管理中，选择 **系统 > 服务器**。

注释 仅作为更改后任务的一部分执行此步骤。

步骤 6 验证是否在网络中完全实施了对 IP 地址、主机名或两者的更改。在群集中的每个节点上输入 CLI 命令 `show network cluster`。

注释 仅作为更改后任务的一部分执行此步骤。

输出应包含节点的新 IP 地址或主机名。

示例:

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups
DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher callmanager
DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

步骤 7 验证主机名的更改是否已在网络中完全实施。在群集中的每个节点上输入 CLI 命令 `utils network host <new_hostname>`。

注释 仅作为更改后任务的一部分执行此步骤。

输出应确认新的主机名在本地和外部解析为 IP 地址。

示例:

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

tasks.

步骤 8 对于启用安全性的群集（群集安全模式 1 - 混合），更新 CTL 文件，然后重新启动群集中的所有节点，再执行系统运行状况检查和其他更改后任务。

有关详细信息，请参阅 [多服务器群集证书的证书和 ITL 重新生成](#)，第 5 页部分。

步骤 9 如果您使用证书信任列表 (CTL) 文件和 USB 电子令牌启用了群集安全性，必须在更改 8.0 或更高版本节点的 IP 地址或主机名后，重新生成初始信任列表 (ITL) 文件和 ITL 中的证书。如果没有使用证书信任列表 (CTL) 文件和 USB 电子令牌启用群集安全性，则跳过此步骤。

步骤 10 运行手动 DRS 备份并确保成功备份所有节点和活动服务。

有关详细信息，请参阅《*Cisco Unified Communications Manager 管理指南*》。

注释 更改节点的 IP 地址后，必须运行手动 DRS 备份，因为无法使用包含不同 IP 地址或主机名的 DRS 文件恢复节点。更改后 DRS 文件将包含新的 IP 地址或主机名。

步骤 11 更新所有相关的 IP 电话 URL 参数。

步骤 12 使用 Cisco Unified Communications Manager 管理更新所有相关的 IP 电话服务。选择系统 > 企业参数。

步骤 13 更新 Unified RTMT 自定义警告和保存的配置文件。

- 从性能计数器派生的 Unified RTMT 自定义警告包括硬编码的服务器 IP 地址。必须删除并重新配置这些自定义警告。
- 具有性能计数器的 Unified RTMT 已保存配置文件中包括硬编码的服务器 IP 地址。必须删除并重新添加这些计数器，然后保存配置文件以将其更新为新的 IP 地址。

步骤 14 如果使用的是 Cisco Unified Communications Manager 上运行的集成式 DHCP 服务器，请更新该 DHCP 服务器。

步骤 15 检查并对其他关联的 Cisco Unified Communications 组件进行所需的配置更改。

以下是要检查的部分组件的部分列表：

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 干线
- IOS 网守
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 电话的 DHCP 作用域
- 用于 CDR 导出的 Cisco Unified Communications Manager 跟踪集合或作为 DRS 备份目标的 SFTP 服务器
- 向 Cisco Unified Communications Manager 注册的 IOS 硬件资源（会议桥、媒体终结点、代码转换器、RSVP 座席）
- 注册或与 Cisco Unified Communications Manager 集成的 IPVC 视频 MCU
- Cisco Emergency Responder

- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 关联的路由器和网关

注释 请查阅产品文档以确定如何进行必要的配置更改。

Cisco Unified Communications Manager 节点的启用安全的群集任务

初始信任列表和证书重新生成

如果在 Cisco Unified Communications Manager 发行版 8.0 或更高版本的群集中更改服务器的 IP 地址或主机名，则会重新生成初始信任列表 (ITL) 文件和 ITL 中的证书。重新生成的文件与电话上存储的文件不匹配。



注释 如果使用证书信任列表 (CTL) 文件和 USB 电子令牌启用群集安全性，则无需执行以下程序中的步骤，因为信任由电子令牌维护，且电子令牌不会更改。

如果群集安全性未启用，请执行单服务器群集或多服务器群集程序中的步骤以重置电话。

重新生成单服务器群集电话的证书和 ITL

如果是在 Cisco Unified Communications Manager 发行版 8.0 或更高版本的单服务器群集中更改服务器的 IP 地址或主机名，并且使用了 ITL 文件，请执行以下步骤重置电话。

在更改服务器的 IP 地址或主机名之前启用回滚。

过程

- 步骤 1** 确保所有电话都处于在线状态并且已注册，以便它们能够处理更新的 ITL。对于执行此程序时未处于在线状态的电话，必须手动删除 ITL。
- 步骤 2** 将“预备回滚至 8.0 之前的群集”企业参数设置为 True。所有电话会自动重置和下载包含空白信任验证服务 (TVS) 及 TFTP 证书部分的 ITL 文件。
- 步骤 3** 在电话上，选择设置 > 安全 > 信任列表 > ITL 文件，以验证 ITL 文件的 TVS 和 TFTP 证书部分是否为空。

步骤 4 更改服务器的 IP 地址或主机名，并让配置用于回滚的电话注册到群集。

步骤 5 在所有电话成功注册到群集后，将“预备回滚至 8.0 之前的群集”企业参数设置为 **False**。

下一步做什么

如果使用 CTL 文件或令牌，请在更改服务器的 IP 地址或主机名后，或者更改 DNS 域名后，重新运行 CTL 客户端。

多服务器群集电话的证书和 ITL 重新生成

在多服务器群集中，电话应具有主要和辅助 TVS 服务器，以验证重新生成的 ITL 文件和证书。如果电话无法联系主要 TVS 服务器（由于最近的配置更改），它将回滚到辅助服务器。TVS 服务器通过分配给电话的 CM 组标识。

在多服务器群集中，请确保一次仅更改一台服务器上的 IP 地址或主机名。如果使用 CTL 文件或令牌，请在更改服务器的 IP 地址或主机名后，或者更改 DNS 域名后，重新运行 CTL 客户端或 CLI 命令 `set utils ctl`。

IM and Presence Service 节点的更改后任务

执行所有更改后任务，以确保更改在部署中正确实施。



注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

过程

步骤 1 验证对主机名或 IP 地址的更改是否已在 Cisco Unified Communications Manager 服务器上更新。

步骤 2 检查节点上的网络连接和 DNS 服务器配置是否已更改。

注释 如果将 IP 地址更改为不同的子网，请确保您的网络适配器现已连接到正确的 VLAN。此外，如果 IP 地址更改后 IM and Presence Service 节点属于不同的子网，请确保 Cisco XCP 路由器服务参数的“路由通信类型”字段设置为“路由器到路由器”。否则，“路由通信类型”字段应设置为“组播 DNS”。

步骤 3 验证对 IP 地址、主机名或两者的更改是否已在网络中完全实施。

步骤 4 如果更改了主机名，请验证主机名更改是否已在网络中完全实施。

步骤 5 验证是否已成功建立数据库复制。所有节点的状态应显示为 2 并已连接。如果未设置复制，请参阅与数据库复制故障诊断相关的主题。

步骤 6 如果禁用了 SAML 单点登录 (SSO)，现在可以启用它。有关 SAML SSO 的详细信息，请参阅《Cisco Unified Communications Manager 上 IM and Presence Service 的部署指南》。

步骤 7 如果更改了主机名，必须确保 cup、cup-xmpp 和 Tomcat 证书中包含新的主机名。

- a) 从 Cisco Unified 操作系统管理 GUI 中，选择安全 > 证书管理。
- b) 验证信任证书的名称中是否包含新的主机名。
- c) 如果证书中不含新的主机名，请重新生成证书。

有关详细信息，请参阅《Cisco Unified Communications Manager 管理指南》。

步骤 8 如果节点的 IP 地址已更改，则更新 Cisco Unified 实时监控工具 (RTMT) 自定义警告和保存的配置文件：

- 源自性能计数器的 RTMT 自定义警告中包含硬编码的服务器地址。必须删除并重新配置这些自定义警告。
- 具有性能计数器的 RTMT 已保存配置文件中包括硬编码的服务器地址。必须删除并重新添加这些计数器，然后保存配置文件以将其更新为新的地址。

步骤 9 检查并对其他关联的 Cisco Unified Communications 组件（例如 Cisco Unified Communications Manager 上的 SIP 干线）进行任何必要的配置更改。

步骤 10 使用 Cisco Unified 功能配置启用 CUP 服务组下所列的所有网络服务，选择工具 > 控制中心 - 网络服务。

提示 如果您要更改 IP 地址或主机名，或者同时更改二者，则无需完成此步骤。系统会针对这些名称更改自动启动网络服务。但是，如果某些服务在更改后没有自动启动，请完成此步骤以确保所有网络服务均已启动。

必须按以下顺序启动“CUP 服务”网络服务：

1. Cisco IM and Presence 数据监控器
2. Cisco 服务器恢复管理器
3. Cisco 路由数据存储器
4. Cisco 登录数据存储器
5. Cisco SIP 注册数据存储器
6. Cisco Presence 数据存储器
7. Cisco XCP 配置管理器
8. Cisco XCP 路由器
9. Cisco OAM 代理
10. Cisco 客户端配置文件代理
11. Cisco 群集间同步代理
12. Cisco 配置代理

步骤 11 要使用 Cisco Unified 功能配置启动所有功能服务，选择工具 > 控制中心 - 功能服务。启动功能服务的顺序并不重要。

提示 如果您要更改 IP 地址或主机名，或者同时更改二者，则无需完成此步骤。系统会针对这些名称更改自动启动功能服务。但是，如果某些服务在更改后没有自动启动，请完成此步骤以确保所有功能服务均已启动。

步骤 12 确认在重新启用高可用性之前已重新创建 Cisco Jabber 会话。否则，已创建会话的 Jabber 客户端将无法连接。

在所有群集节点上运行 `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 命令。活动会话数应与您禁用高可用性时记录的用户数一致。如果会话启动时间超过30分钟，您可能遇到更大的系统问题。

步骤 13 如果在更改前设置期间禁用了高可用性 (HA)，请在所有在线状态冗余组上启用 HA。

步骤 14 验证更改后 IM and Presence Service 是否正常工作。

a) 从 Cisco Unified 功能配置 GUI 中，选择系统 > **Presence 拓扑**。

- 如果 HA 已启用，验证是否所有 HA 节点都处于“正常”状态。
- 验证所有服务是否均已启动。

b) 从 Cisco Unified CM IM and Presence 管理 GUI 运行系统故障诊断程序，并确保没有测试失败。选择诊断 > 系统故障诊断程序。

步骤 15 更改节点的 IP 地址或主机名后，必须运行手动灾难恢复系统备份，因为无法使用包含不同 IP 地址或主机名的 DRS 文件恢复节点。更改后 DRS 文件将包含新的 IP 地址或主机名。

有关详细信息，请参阅《*Cisco Unified Communications Manager 管理指南*》。
