备份/恢复

关于备份和恢复

灾难恢复能力是任何系统维护计划的重要组成部分。作为灾难恢复计划的一部分，我们建议您定期备份到安全的远程位置。

按需备份

您可以从 管理中心 对 管理中心以及许多 威胁防御 设备执行按需备份。

有关详细信息，请参阅备份 管理中心FMC 或受管设备， 第 9 页。

计划的备份

您可以在 管理中心上使用调度程序来自动执行备份。您还可以从 管理中心 安排远程设备备份。

管理中心 设置过程安排每周仅配置备份，以存储在本地。 这不能替代完整的异地备份-在初始设置完成后，您应查看已安排的任务并进行调整，以满足组织的需求。

有关详细信息，请参阅计划的备份。

存储备份文件

您可以在本地存储备份。但是，我们建议您通过将 NFS、SMB 或 SSHFS 网络卷安装为远程存储，将 管理中心和托管设备备份到安全的远程位置。执行此操作后，所有后续备份都将复制到该卷，但您仍可以使用 管理中心 对其进行管理。

有关详细信息，请参阅远程存储设备 和 管理备份和远程存储 ， 第 27 页。

恢复 管理中心 和受管设备

您可以从备份管理页面恢复 管理中心 。 您必须使用 威胁防御 CLI 来恢复 威胁防御 设备，但 ISA 3000 零接触恢复除外，该恢复使用 SD 卡和重置按钮。

有关详细信息，请参阅恢复 管理中心 和托管设备 ， 第 14 页。

备份的内容是什么？

管理中心 备份可以包括：

- (Recommended Configurations)。

  可以在 管理中心 Web 界面上设置的所有配置都包含在配置备份中，远程存储和审核日志服务器证书设置除外。在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。

- 事件。

  事件备份包括 管理中心 数据库中的所有事件。但是，管理中心 事件备份不包括入侵事件审核状态。已恢复的入侵事件不会显示在“已审核事件”页面上。

- 威胁智能导向器 (TID) 数据。

  关于更多信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 有关备份和恢复威胁智能导向器 数据 。

设备备份始终仅用于配置。

恢复的内容是什么？

恢复配置会覆盖 所有 备份配置，只有极少数例外。在 管理中心 上，恢复事件和 TID 数据会覆盖所有现有事件和 TID 数据，但入侵事件除外。

确保您了解并计划以下事项：

- 您无法恢复未备份的内容。

  管理中心 配置备份不包括远程存储和审核日志服务器证书设置，因此您必须在恢复后重新配置这些设置。此外，由于管理中心 事件备份不包括入侵事件审核状态，因此已恢复的入侵事件不会显示在“已审核事件”页面上。

- 恢复失败 VPN 证书。

  威胁防御 恢复过程会从 威胁防御 设备中删除 VPN 证书和所有 VPN 配置，包括在执行备份后添加的证书。恢复 威胁防御 设备后，必须重新添加/重新注册所有 VPN 证书，并重新部署设备。

- 恢复到已配置的 管理中心（而不是恢复出厂或重新映像）会合并入侵事件和文件列表。

  管理中心 事件恢复过程不会覆盖入侵事件。相反，备份中的入侵事件会添加到数据库中。要避免重复，请在恢复之前删除现有入侵事件。

管理中心 配置恢复过程不会覆盖 恶意软件防护 使用的干净和自定义检测文件列表。相反，它会将现有文件列表与备份中的文件列表合并。要替换文件列表，请在恢复之前删除现有文件列表。

备份和还原要求

Backup and Restore具有以下要求。

型号要求：备份

您可以备份：

- 管理中心
- 威胁防御 独立设备、本地实例、容器实例、高可用性对和集群
- threat defense virtual 用于私有云独立设备、高可用性对和集群

不 支持备份：

- 适用于公共云的 threat defense virtual

如果需要更换不支持备份和恢复的设备，则必须手动重新创建设备特定的配置。但是，备份 管理中心 会备份部署到受管设备的策略和其他配置，以及已从设备传输到 管理中心的事件。

型号要求：恢复

替换受管设备必须与您要替换的设备具有相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。

对于 管理中心，不仅可以在 RMA 场景中使用Backup and Restore，还可以在 管理中心之间迁移配置和事件。关于详细信息，包括支持的目标和目的模型，请参阅《Firepower管理中心型号迁移指南》。

版本要求

作为任何备份的第一步，请注意补丁级别。要恢复备份，旧设备和新设备必须运行相同的软件版本，包括补丁。

此外，要在 Firepower 4100/9300 机箱上恢复软件，机箱必须运行兼容的 FXOS 版本。

对于 管理中心 备份，不需要具有相同的 VDB 或 SRU。但请注意，恢复备份会将现有 VDB 替换为备份文件中的 VDB。

许可证要求

解决最佳实践和程序中所述的许可或孤立权利问题。如果您发现许可冲突，请联系 思科 TAC。

域要求

到：

- 备份或恢复 管理中心：仅限全局。
- 从 管理中心备份设备：仅全局。
- 恢复设备：无。在 CLI 本地恢复设备。

在多域部署中，不能仅备份事件/ TID 数据。您还必须备份配置。

备份和恢复的指南和限制

备份和恢复有以下指南和限制。

备份和恢复适用于灾难恢复/ RMA

备份和恢复主要用于 RMA 场景。在开始故障或发生故障的物理设备的恢复过程之前，请联系 思科 TAC 更换硬件。

您还可以使用Backup and Restore在 管理中心之间迁移配置和事件。这使得更换 管理中心（由于不断增长的组织、从物理实施迁移到虚拟实施、硬件更新等技术或业务等方面的原因）变得更容易。

备份和恢复不是配置导入/导出

备份文件包含唯一识别设备的信息，并且不能共享。不要使用备份和恢复过程在设备或装置之间复制配置，或作为测试新配置时保存配置的一种方式。相反，请使用导入/导出功能。

例如， 威胁防御 设备备份包括设备的管理IP地址以及设备连接到其管理 管理中心所需的所有信息。请勿将 威胁防御 备份恢复到由其他 管理中心管理的设备；恢复的设备将尝试连接到备份中指定的 管理中心 。

恢复为单个和本地恢复

您可以单独和本地恢复到 管理中心和受管设备。这意味着：

- 您无法批量恢复到高可用性 或集群的 管理中心或设备。
- 您无法使用 管理中心 恢复设备。对于 管理中心，可以使用 Web 接口进行恢复。 对于 威胁防御 设备，必须使用 威胁防御 CLI，但 ISA 3000 零接触恢复除外，该恢复使用 SD 卡和重置按钮。
- 您不能使用 管理中心 用户账号登录并从其托管设备之一恢复。 管理中心和设备维护各自的用户帐号。

Firepower 4100/9300 的配置导入/导出准则

使用配置导出功能将包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于 Firepower 4100/9300 机箱，以返回到已知的正确配置，或从系统故障中恢复。

准则和限制

- 请勿修改配置文件的内容。如果配置文件被修改，使用该文件进行配置导入可能会失败。
- 特定应用的配置设置不包含在配置文件内。您必须使用应用提供的配置备份工具来管理特定应用的设置和配置。
- 将配置导入到 Firepower 4100/9300 机箱 时，Firepower 4100/9300 机箱 上的所有现有配置（包括任何逻辑设备）会被删除并完全替换为导入文件中包含的配置。
- 除了在 RMA 场景中，我们建议您只将配置文件导入当初从中导出该配置的同一个 Firepower 4100/9300 机箱。
- 进行导入的 Firepower 4100/9300 机箱 的平台软件版本应与执行导出时的版本相同。否则，导入操作将无法确保会成功。我们建议您在升级或降级 Firepower 4100/9300 机箱 时导出备份配置。
- 进行导入的 Firepower 4100/9300 机箱 必须在与执行导出时所用的相同插槽中安装相同的网络模块。
- 进行导入的 Firepower 4100/9300 机箱 必须为您正在导入的导出文件中定义的任意逻辑设备安装了正确的软件应用映像。
- 要避免覆盖现有的备份文件，请更改备份操作中的文件名或将现有文件复制到其他位置。

注释 您必须单独备份逻辑应用，因为 FXOS 导入/导出将仅备份 FXOS 配置。FXOS 配置导入将导致逻辑设备重新启动，并使用出厂默认配置重建设备。

备份和还原的最佳实践

备份和恢复具有以下最佳实践。

何时备份

我们建议在维护时段或其他使用率较低的时间进行备份。

当系统收集备份数据时，数据的关联性可能会暂时停顿（仅限管理中心），而且你可能无法改变与备份有关的配置。如果包含事件数据，则 eStreamer 等事件相关功能不可用。

您应在以下情况下进行备份：

- 常规计划的备份

  作为灾难恢复计划的一部分，我们建议您定期执行备份。

  管理中心 设置过程安排每周仅配置备份，以存储在本地。 这不能替代完整的异地备份-在初始设置完成后，您应查看已安排的任务并进行调整，以满足组织的需求。有关详细信息，请参阅计划的备份。

- 在 SLR 更改之后。

对特定许可预留（SLR）进行更改后，备份管理中心。如果您进行更改并恢复较旧的备份，则您的特定许可返回代码会出现问题，并且可能会产生孤立授权。

- 在升级或重新映像之前。

  如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。

- 升级后。

  在升级后进行备份，以便获得新升级的部署的快照。我们建议您在升级其托管设备后备份管理中心，以便新的管理中心备份文件“知道”其设备已升级。

维护备份文件安全

备份存储为未加密的存档（.tar）文件。

PKI 对象中的私钥--代表支持你的部署所需的公钥证书和成对的私钥--在被备份之前被解密在恢复备份时，将使用随机生成的密钥重新加密密钥。

注释 我们建议您将管理中心和设备备份到安全的远程位置并验证传输是否成功。本地删除的备份可以手动删除，也可以通过升级过程删除，从而清除本地存储的备份。

尤其是由于备份文件未加密的情况，因此不允许未经授权的访问。如果修改备份文件，恢复过程将失败。请记住，具有管理员/维护角色的任何人都可以访问“备份管理”页面，他们可以在其中移动和删除远程存储中的文件。

在管理中心的系统配置中，您可以安装NFS、SMB或SSHFS网络卷作为远程存储。执行此操作后，所有后续备份都将复制到该卷，但您仍可以使用管理中心对其进行管理。有关详细信息，请参阅远程存储设备 和 管理备份和远程存储，第 27 页。

请注意，只有管理中心安装网络卷。受管设备备份文件通过管理中心路由。确保你有足够的带宽在管理中心和其设备之间进行大量的数据传输。有关详细信息，请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。

管理中心 高可用性部署中的 Backup and Restore

在管理中心高可用性部署中，备份一个管理中心不会备份另一个。您应定期备份两个对等体。请勿使用来自另一个 HA 的备份文件恢复一个 HA 对等体。备份文件包含唯一识别设备的信息，并且不能共享。

请注意，您可以在没有成功备份的情况下替换 HA 管理中心。有关更换 HA 管理中心（无论是否成功备份）的详细信息，请参阅 更换高可用性对中的管理中心。

威胁防御 高可用性部署中的 Backup and Restore

在威胁防御高可用性部署中，您应该：

- 从管理中心备份设备对，但从威胁防御 CLI 单独和本地恢复。

备份过程会为 威胁防御 高可用性设备生成唯一的备份文件。请勿使用来自另一个高可用性的备份文件恢复一个高可用性对等体。备份文件包含唯一识别设备的信息，并且不能共享。

威胁防御 高可用性设备的角色记录在其备份文件名中。还原时，请确保选择适当的备份文件：主要与辅助。

- 在恢复之前， 请勿 暂停或中断高可用性。

  保持高可用性配置可确保替换设备在恢复后可以轻松重新连接。请注意，您必须恢复高可用性同步才能执行此操作。

- 请勿 同时在两个对等体上运行 **恢复** CLI 命令。

  假设您已成功备份，您可以替换高可用性对中的一个或两个对等体。您可以同时执行的任何物理更换任务：取消安装，重新安装等。 但是， 请勿 在第二台设备上运行 **恢复** 命令，直到第一台设备的恢复过程完成，包括重新启动。

请注意，您可以在没有成功备份的情况下更换 威胁防御 高可用性设备。

集群部署 威胁防御 中的备份和恢复

在 威胁防御 集群部署中，您应该：

- 从 管理中心备份完整集群，但从 威胁防御 CLI 单独和本地恢复节点。

  备份过程会生成一个捆绑的tar文件，其中包含每个集群节点的唯一备份文件。请勿使用另一个节点的备份文件恢复另一个节点。备份文件包含唯一识别设备的信息，并且不能共享。

  节点的角色记录在其备份文件名中。还原时，请确保选择适当的备份文件：控制或数据。

  您无法备份单个节点。如果数据节点无法备份， 管理中心 仍将备份所有其他节点。如果控制节点备份失败，则取消备份。

- 在恢复之前， 请勿 暂停或中断集群。

  保持集群配置可确保替换设备在恢复后可以轻松重新连接。

- 请勿 同时在多个节点上运行 **恢复** CLI 命令。我们建议您先恢复控制节点，等待其重新加入集群，然后再恢复任何数据节点。

  假设您有成功的备份，则可以替换集群中的多个节点。您可以同时执行的任何物理更换任务：取消安装，重新安装等。但是， 请勿 在其他节点上运行 **恢复** 命令，直到之前节点的恢复过程完成，包括重新启动。

Firepower 4100/9300 机箱的备份和恢复

要在 Firepower 4100/9300 机箱上恢复 威胁防御 软件，机箱必须运行兼容的 FXOS 版本。

当您备份 Firepower 4100/9300 机箱时，我们强烈建议您也备份 FXOS 配置。有关其他最佳实践，请参阅 Firepower 4100/9300 的配置导入/导出准则， 第 4 页。

备份前

在备份之前，您应该：

- 更新 管理中心上的 VDB 和 SRU。

  我们始终建议您使用最新的漏洞数据库（VDB）和入侵规则（SRU）。在备份 管理中心之前，请检查 思科支持和下载站点 是否有较新版本。

- 检查磁盘空间。

  在开始备份之前，请确保设备或远程存储服务器上有足够的磁盘空间。可用空间显示在“备份管理”页面上。

  如果没有足够的空间，备份可能会失败。尤其是在安排备份时，请确保定期删除备份文件或为远程存储位置分配更多磁盘空间。

还原前

在恢复之前，您应：

- 恢复许可更改。

  请恢复自备份以来所做的任何许可更改。

  否则，恢复后您可能会遇到许可证冲突 或孤立的权利问题 。 但是， 请勿 从 Cisco 智能软件管理器（CSSM）注销。如果从 CSSM 注销，则必须在恢复后再次注销，然后重新注册。

  恢复完成后，重新配置许可。如果您发现许可冲突 或孤立的权利，请联系 思科 TAC 。

- 断开故障设备。

  断开管理接口，对于设备，断开数据接口。

  恢复 威胁防御 设备会将替换设备的管理 IP 地址设置为旧设备的管理 IP 地址。为避免 IP 冲突，请先断开旧设备与管理网络的连接，然后再更换备份。

  请注意，恢复 管理中心 不 会更改管理 IP 地址。您必须在更换时手动设置该设置-只需确保先断开旧设备与网络的连接，然后再执行此操作。

- 请勿 取消注册受管设备。

  无论您是恢复 管理中心 或托管设备，都不要从 管理中心注销设备，即使您从网络上物理断开设备。

  如果取消注册，则需要重做一些设备配置，例如安全区域到接口的映射。恢复后，管理中心 和设备应开始正常通信。

- 重新映像。

  在 RMA 场景中，替换设备将配置为出厂默认设置。但是，如果已配置替换设备，我们建议您重新映像。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。您只能重新映像到主要版本，因此您可能需要在重新映像后进行修补。

  如果不重新映像，请记住， 管理中心 入侵事件和文件列表会合并而不是覆盖。

还原后

还原后，您应：

- 重新配置未恢复的任何内容。

  这可能包括重新配置许可，远程存储和审核日志服务器证书设置。 您还必须重新添加/重新注册失败的 威胁防御 VPN 证书。

- 更新 管理中心上的 VDB 和 SRU。

  我们始终建议您使用最新的漏洞数据库（VDB）和入侵规则（SRU）。 这对于VDB 尤其重要，因为备份中的 VDB 将覆盖替换 管理中心上的 VDB。

- 部署。

  恢复管理中心后，部署到所有托管设备。恢复设备后，必须从“设备管理”页面强制部署：请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。无论是恢复 管理中心 还是 必须 部署的设备。

备份 管理中心FMC 或受管设备

您可以对支持的设备执行按需或计划备份。

从 管理中心备份 设备不需要备份配置文件。但是， 管理中心 会备份需要备份配置文件。按需备份过程允许您创建新的备份配置文件。

备份 FMC

使用此程序执行按需 FMC 备份。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

过程

步骤 1 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。它还列出了可用于存储备份的磁盘空间。如果没有足够的空间，备份可能会失败。

步骤 2 选择是使用现有备份配置文件还是全新启动。

FMC 备份要求您使用或创建备份配置文件。

- 点击 **备份配置文件** 以使用现有备份配置文件。

  在要使用的配置文件旁边，点击编辑图标。然后，您可以点击 **开始备份** 立即开始备份。或者，如果要编辑配置文件，请继续执行下一步。

- 点击 **Firepower 管理备份** 以开始全新的备份并创建新的备份配置文件。

  输入配置文件的 **名称** 。

步骤 3 选择要备份的内容：

- **备份配置**
- **备份事件**
- **备份威胁情报导向器**

在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。有关为每个选项备份的内容的详细信息，请参阅 关于备份和恢复， 第 1 页。

步骤 4 注意 FMC 备份文件的 **存储位置** 。

这将是 `/var/sf/backup/`中的本地存储或远程网络卷。有关详细信息，请参阅管理备份和远程存储， 第 27 页。

步骤 5 （可选） **启用完成时复制** 以将已完成的 FMC 备份复制到远程服务器。

提供主机名或 IP 地址，远程目录的路径以及用户名和密码。要使用 SSH 公共密钥而不是密码，则将 **SSH 公共密钥** 字段中的内容到该机器上指定用户的 `授权的_密钥` 文件中。

注释 如果要在本地存储备份并将其存储到远程位置，此选项非常有用。如果配置了 SSH 远程存储，请 不 要在完成后使用 **复制将备份文件复制到同一目录**。

步骤 6 （可选）启用 **邮件** 并输入在备份完成时收到通知的邮件地址。

要接收邮件通知，必须将 FMC 配置为连接到邮件服务器： 配置邮件中继主机和通知地址。

步骤 7 点击 **开始备份** 开始按需备份。

如果您不使用现有备份配置文件，则系统会自动创建并使用该配置文件。如果决定不立即运行备份，可以点击 **保存** 或 **另存为** 保存配置文件。无论是哪种情况，都可以使用新创建的配置文件来配置计划备份。

步骤 8 在消息中心监控进度。

当系统收集备份数据时，数据的关联性可能会暂时停顿，而且你可能无法改变与备份有关的配置。如果配置了远程存储或启用 **完成时复制**，则 FMC 可能会将临时文件写入远程服务器。这些文件在备份过程结束时进行清理。

下一步做什么

如果配置了远程存储或启用 **完成时复制**，请验证备份文件的传输是否成功。

从 管理中心备份设备

使用此程序对以下任何设备执行按需备份：

- 威胁防御：物理设备、独立、高可用性、集群
- threat defense virtual：私有云、独立、高可用性、集群

备份和恢复不支持任何其他平台或配置。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

如果您要备份 Firepower 4100/9300 机箱，则还必须备份 FXOS 配置： 导出 FXOS 配置文件， 第 12 页

过程

步骤 1 选择 **系统**（⚙）> **工具** > **备份/恢复**，然后点击 **受管设备备份**。

步骤 2 选择一个或多个 **受管设备**。

对于集群，请选择集群。不能在单个节点上执行备份。

步骤 3 请注意设备备份文件的 **存储位置** 。

这将是 `/var/sf/remote-backup/`中的本地存储或远程网络卷。对于 ISA 3000，如果您安装了 SD 卡，也会在 `/mnt/disk3/backup`的 SD 卡上创建备份副本。有关详细信息，请参阅管理备份和远程存储， 第 27 页。

步骤 4 如果未配置远程存储，请选择是否要 **检索到管理中心**。

- 已启用（默认）：将备份保存到 `/var/sf/remote-backup/` 中的 管理中心。

  对于集群，此选项始终处于选中状态。单个节点备份文件将复制到管理中心，然后捆绑为单个压缩 tar 文件，然后再复制到任何远程存储。

- 已禁用：将备份保存到 `/var/sf/backup` 中的设备。

步骤 5 点击 **开始备份** 开始按需备份。

步骤 6 在消息中心监控进度。

下一步做什么

如果配置了远程存储，请验证备份文件的传输是否成功。

导出 FXOS 配置文件

使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。

注释 此程序介绍在备份 威胁防御时如何使用 Cisco Secure Firewall 机箱管理器 来导出 FXOS 配置。有关 CLI 程序，请参阅相应版本的《思科 Firepower 4100/9300 FXOS CLI 配置指南》。

开始之前

查看 Firepower 4100/9300 的配置导入/导出准则。

过程

步骤 1 在 Cisco Secure Firewall 机箱管理器 上依次选择**系统 (System)** > **配置 (Configuration)** > **导出 (Export)**。

步骤 2 要将配置文件导出到本地计算机：

a) 单击**本地 (Local)**。

b) 单击 **Export**。
配置文件已创建，然后根据您的浏览器，该文件可能会自动下载到默认下载位置，或者系统会提示您保存文件。

步骤 3 要将配置文件导出到远程服务器：

a) 单击**远程 (Remote)**。

b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。

c) 输入备份文件应存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

d) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。

e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。

f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。

g) 在**位置 (Location)** 字段中，输入配置文件导出位置的完整路径，包括文件名。

h) 单击的**导出 (Export)** 按钮。
配置文件已创建，并已被导出到指定位置。

创建备份配置文件

备份配置文件是一组已保存的首选项-要备份的内容，备份文件的存储位置等。

FMC 备份 需要备份配置文件。从 FMC 备份设备不需要备份配置文件。

当您执行按需FMC备份时，如果不选择现有备份配置文件，系统会自动创建一个并使用它。然后，您可以使用新创建的配置文件配置计划备份。

以下程序介绍如何在不执行按需备份的情况下创建备份配置文件。

过程

步骤 1 选择 **系统**（⚙）> **工具** > **备份/恢复**，然后点击 **备份配置文件**。

步骤 2 点击 **创建配置文件** 并输入 **名称**。

步骤 3 选择要备份的内容。

- **备份配置**
- **备份事件**
- **备份威胁情报导向器**

在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。有关为每个选项备份的内容的详细信息，请参阅 关于备份和恢复，第 1 页。

步骤 4 请注意备份文件的 **存储位置** 。

这将是 `/var/sf/backup/`中的本地存储或远程网络卷。对于 ISA 3000，如果您安装了 SD 卡，也会在 `/mnt/disk3/backup`的 SD 卡上创建备份副本。有关详细信息，请参阅管理备份和远程存储，第 27 页。

步骤 5 （可选） **启用完成时复制** 以将已完成的 FMC 备份复制到远程服务器。

提供主机名或 IP 地址，远程目录的路径以及用户名和密码。要使用 SSH 公共密钥而不是密码，则将 **SSH 公共密钥** 字段中的内容到该机器上指定用户的 `授权的_密钥` 文件中。

注释 如果要在本地存储备份并将其存储到远程位置，此选项非常有用。如果配置了 SSHFS 远程存储，请 勿 在完成后使用 **复制将备份文件复制到同一目录**。

步骤 6 （可选）启用 **邮件** 并输入在备份完成时收到通知的邮件地址。

要接收邮件通知，必须将 FMC 配置为连接到邮件服务器： 配置邮件中继主机和通知地址。

步骤 7 单击**保存**。

恢复 管理中心 和托管设备

对于 管理中心，可使用 Web 接口从备份恢复。 对于 威胁防御 设备，必须使用 威胁防御 CLI。您无法使用 管理中心 恢复设备。

以下各节介绍如何恢复 管理中心 和托管设备。

从备份恢复 管理中心

当恢复 管理中心 备份时，可以选择恢复备份文件中包含的任何或所有组件（事件、配置、TID 数据）。

注释 恢复配置会覆盖 所有 配置，只有极少数例外。它还会重新启动 管理中心。恢复事件 和 TID 数据 会覆盖 所有 现有事件 和 TID 数据，但入侵事件除外。确保您已准备就绪。

使用此程序从备份恢复 管理中心 。 有关 管理中心 HA 部署中的备份和恢复的详细信息，请参阅 更换高可用性对中的 管理中心。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

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。您可以点击备份文件以查看其内容。

如果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， 第 27 页。

步骤 3 选择要恢复的备份文件并点击 **恢复**。

步骤 4 从可用组件中选择要恢复的组件，然后再次点击 **恢复** 以开始。

步骤 5 在消息中心监控进度。

如果要恢复配置，可以在 管理中心 重启后重新登录。

下一步做什么

- 如有必要，请重新配置在还原之前恢复的任何许可设置。如果您发现许可冲突 或孤立的权利，请联系 思科 TAC 。
- 如有必要，请重新配置远程存储和审核日志服务器证书设置。这些设置不包括在备份中。
- （可选）更新 SRU 和 VDB。如果 思科支持和下载站点 上提供的 SRU 或 VDB 比当前运行的版本新，请安装新版本。
- 部署配置更改；请参阅《Cisco Secure Firewall Management Center 设备配置指南》 。

从备份恢复 威胁防御： Firepower 1000/2100、Secure Firewall 3100、 ISA 3000 （非零触摸）

威胁防御 备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

如果发生硬件故障，此程序概述了如何更换 Firepower 1000/2100、 Secure Firewall 3100或 ISA 3000 威胁防御 设备、独立或高可用性对 或作为集群。它假定您有权访问要替换的设备的成功备份；请参阅 从 管理中心备份设备， 第 11 页。有关使用 SD 卡在 ISA 3000 上进行零接触恢复的信息，请参阅 从备份的零接触恢复 威胁防御： ISA 3000， 第 18 页。

在 威胁防御 高可用性 和集群 部署中，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 找到故障设备的成功备份。

对于集群，节点备份文件捆绑在集群的单个压缩文件中 (*cluster_name*.*timestamp*.**tar.gz**)。在恢复节点之前，需要提取单个节点备份文件 (*node_name*_**control**_*timestamp*.**tar** or *node_name*_**data**_*timestamp*.**tar**)。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。
- 在 管理中心 中的 `/var/sf/remote-backup`。
- 在远程存储位置。

在威胁防御 高可用性部署中，您将对作为一个单元进行备份，但备份过程会生成唯一的备份文件。设备的角色在备份文件名中注明。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储，第 27 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 3 移除（拆开）故障设备。

断开所有接口。在 威胁防御 高可用性部署中，这包括故障切换链路。 对于集群，这包括集群控制链路。

请参阅您的型号的硬件安装和入门指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 4 安装替换设备并将其连接到管理网络。

将设备连接至电源并将管理接口连接至管理网络。在 威胁防御 高可用性部署中，连接故障切换链路。 对于集群，请连接集群控制链路。但是， 请勿 连接数据接口。

请参阅您的型号的硬件安装指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

步骤 5 （可选）重新映像替换 设备。

在 RMA 场景中，替换设备将配置为出厂默认设置。如果替换设备运行的主版本与故障设备不同，我们建议您重新映像。

请参阅 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

步骤 6 在替换设备上执行初始配置。

以 admin 用户身份访问 威胁防御 CLI。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请勿设置与故障设备相同的管理 IP 地址。如果您需要注册设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅您的型号的入门指南中的初始配置主题： Cisco Secure Firewall Threat Defense：安装和升级指南。

注释 如果需要修补替换设备，请按照入门指南中的说明启动管理中心注册过程。如果不需要修补， 请勿 注册。

步骤 7 确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的 威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的 AC 策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 补丁设备： 《Cisco Firepower 管理中心升级指南》 。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 8 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 /var/sf/backup。 对于集群，请确保从主集群捆绑包中提取单个节点备份文件。

步骤 9 从 威胁防御 CLI 恢复备份。

以 admin 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp*-主机名称 用户名 文件路径 备份 *tar*-文件
- 从本地设备： **restore remote-manager-backup** 备份 *tar*-文件

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 10 登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 11 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 恢复高可用性同步。从 威胁防御 CLI， 输入 `配置高可用性恢复`。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 暂停和恢复高可用性 。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 12 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 13 连接设备的数据接口。

请参阅您的型号的硬件安装指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

从备份的零接触恢复 威胁防御： ISA 3000

威胁防御 备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

万一发生硬件故障，此程序概述了如何更换 ISA 3000 威胁防御 设备（独立或 HA 对）。它假设您在 SD 卡上备份了发生故障的设备；请参阅 从 管理中心备份设备 ， 第 11 页。

在 威胁防御 高可用性 和集群 部署中，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 从故障设备中取出 SD 卡，然后拆开设备。

断开所有接口。在 威胁防御 HA 部署中，这包括故障切换链路。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 3 重新安装替换设备，并将其连接到管理网络。在 威胁防御 HA 部署中，连接故障切换链路。但是，请勿 连接数据接口。

如果需要重新映像设备或应用软件补丁，请连接电源接头。

步骤 4 （可能需要）重新映像更换设备。

在RMA场景中，替换设备将配置为出厂默认设置。如果替换设备未运行与故障设备相同的主版本，则需要重新映像。从 https://www.cisco.com/go/isa3000-software 获取安装程序。

请参阅 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南 以重新映像。

步骤 5 （可能需要）确保替换设备运行与故障设备相同的 Firepower 软件版本， 包括相同的补丁版本。如果需要修补设备，可以连接到 Secure Firewall 设备管理器 （设备管理器）以安装补丁。

以下程序假设您具有出厂默认配置。如果已配置设备，则可以登录 设备管理器 并直接转到 **设备** > **升级** 页面以安装补丁。

无论是哪种情况，都应从 https://www.cisco.com/go/isa3000-software获取补丁包。

a) 将您的计算机直接连接到内部（以太网 1/2）接口，并通过默认 IP 地址访问 设备管理器：**https://192.168.95.1**。
b) 输入 **admin** 用户名和默认密码 **Admin123**，然后点击 **登录**。
c) 完成设置向导。请记住，您不会保留在 设备管理器 中配置的任何内容；您只需跳过任何初始配置，即可应用补丁，因此在设置向导中输入的内容并不重要。
d) 转到 **设备** > **升级** 页面。

   系统升级 部分将显示当前运行的软件版本。

e) 点击 **浏览**上传上传补丁文件。
f) 点击**安装**开始安装过程。

图标旁的信息表示设备是否会在安装期间重新启动。您将从系统中自动注销。安装可能需要 30 分钟或更长时间。

请耐心等候，然后重新登录系统。“设备摘要”（或“系统监控”控制面板）应该显示新版本。

注释 不要只刷新浏览器窗口，而要从 URL 中删除所有路径，然后重新连接到主页。这可确保使用最新代码刷新缓存的信息。

步骤 6 将 SD 卡插入替换设备。

步骤 7 启动或重新启动设备，并在设备启动后不久，按住“重置”按钮不小于 3 秒且不超过 15 秒。

如果您使用 设备管理器 安装过补丁，则可以从 **设备** > **系统设置** > **重启/关机** 页面重启。从 威胁防御 CLI 中，使用 **reboot** 命令。如果尚未连接电源，请立即连接。

使用线规为 0.033 英寸或更小的标准 #1 回形针按下“重置”按钮。恢复过程在启动期间触发。设备将恢复配置，然后重新启动。然后，设备将自动向 管理中心 注册。

如果要恢复高可用性对中的两台设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿恢复第二台设备。

步骤 8 登录 管理中心 并等待替换设备连接。

此时，设备应显示为过时。

步骤 9 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 恢复高可用性同步。从 威胁防御 CLI， 输入 `configure high-availability resume`。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 暂停和恢复高可用性 。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 10 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 11 连接设备的数据接口。

请参阅您的型号的硬件安装指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

从备份恢复 威胁防御： Firepower 4100/9300 机箱

威胁防御 备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

在发生硬件故障的情况下，此程序概述了如何替换 Firepower 4100/9300、独立、高可用性对 或作为集群。它假设您有权访问以下项的成功备份：

- 要替换的逻辑设备；请参阅 从 管理中心备份设备 ， 第 11 页。
- FXOS 配置，请参阅 导出 FXOS 配置文件 ， 第 12 页。

在 威胁防御 高可用性 和集群 部署中，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求 ， 第 3 页
- 备份和恢复的指南和限制 ， 第 4 页
- 备份和还原的最佳实践 ， 第 5 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 找到故障设备的成功备份。

对于集群，节点备份文件捆绑在集群的单个压缩文件中 (*cluster_name*.*timestamp*.**tar.gz**)。在恢复节点之前，需要提取单个节点备份文件 (*node_name*_**control**_*timestamp*.**tar** or *node_name*_**data**_*timestamp*.**tar**)。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。
- 在 管理中心 中的 `/var/sf/remote-backup`。

- 在远程存储位置。

在威胁防御高可用性部署中，您将对作为一个单元进行备份，但备份过程会生成唯一的备份文件。设备的角色在备份文件名中注明。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储，第 27 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 3 找到 FXOS 配置的成功备份。

步骤 4 移除（拆开）故障设备。

断开所有接口。在 威胁防御 高可用性部署中，这包括故障切换链路。 对于集群，这包括集群控制链路。

请参阅您的型号的硬件安装和入门指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 5 安装替换设备并将其连接到管理网络。

将设备连接至电源并将管理接口连接至管理网络。在 威胁防御 高可用性部署中，连接故障切换链路。 对于集群，请连接集群控制链路。但是， 请勿 连接数据接口。

请参阅您的型号的硬件安装指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

步骤 6 （可选）重新映像替换 设备。

在 RMA 场景中，替换设备将配置为出厂默认设置。如果替换设备运行的主版本与故障设备不同，我们建议您重新映像。

请参阅相应的 《Cisco Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南》中有关恢复出厂默认配置的说明。

步骤 7 确保 FXOS 运行的是兼容版本。

在重新添加逻辑设备之前，您必须运行兼容的FXOS版本。您可以使用 机箱管理器 导入备份的FXOS配置： 导入配置文件，第 24 页。

步骤 8 使用 机箱管理器 添加逻辑设备并执行初始配置。

请勿设置与故障机箱上的逻辑设备相同的管理 IP 地址。如果您需要注册逻辑设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅 管理中心 适用于您的型号的入门指南中的 FMC 部署章节： Cisco Secure Firewall Threat Defense：安装和升级指南。

注释　如果需要修补逻辑设备，请按照入门指南中的说明注册到管理中心。如果不需要修补，请勿 注册。

步骤 9　确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的 威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 补丁设备： 《Cisco Firepower 管理中心升级指南》 。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 10　确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。 对于集群，请确保从主集群捆绑包中提取单个节点备份文件。

步骤 11　从 威胁防御 CLI 恢复备份。

以 `admin` 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp-主机名称 用户名 文件路径 备份 tar-文件*
- 从本地设备： **restore remote-manager-backup** 备份 *tar-文件*

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 12　登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 13　在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 14 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 15 连接设备的数据接口。

请参阅您的型号的硬件安装指南： Cisco Secure Firewall Threat Defense：安装和升级指南。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

导入配置文件

您可以使用配置导入功能应用之前已从 Firepower 4100/9300 机箱导出的配置设置。此功能允许您返回已知的良好配置或从系统故障中进行恢复。

注释 此程序介绍如何在恢复 Firepower 软件之前使用 机箱管理器 来导入 FXOS 配置。有关 CLI 程序，请参阅相应版本的《思科 Firepower 4100/9300 FXOS CLI 配置指南》。

开始之前

查看 Firepower 4100/9300 的配置导入/导出准则。

过程

步骤 1 在 机箱管理器上选择 **系统 (System)** > **工具 (Tools)** > **导入/导出 (Import/Export)**。

步骤 2 要从本地配置文件导入：

a) 单击**本地 (Local)**。

b) 单击**选择文件 (Choose File)** 以导航到要导入的配置文件并将其选定。

c) 单击 **Import**。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。

d) 单击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 3 要从远程服务器上的配置文件导入：

a) 单击**远程 (Remote)**。

b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。

c) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。

d) 输入备份文件存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。
g) 在**文件路径 (File Path)** 字段中，输入配置文件的完整路径，包括文件名。
h) 单击的**导入 (Import)** 按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
i) 单击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

从备份恢复 威胁防御： Threat Defense Virtual

使用此程序可替换私有云的故障 threat defense virtual 设备、独立设备、高可用性对 或作为集群。

在 威胁防御 高可用性 和集群 部署中，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 高可用性 或集群 部署中， 请勿 暂停或中断高可用性 或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 3 页
- 备份和恢复的指南和限制， 第 4 页
- 备份和还原的最佳实践， 第 5 页

过程

步骤 1 找到故障设备的成功备份。

对于集群，节点备份文件捆绑在集群的单个压缩文件中 (*cluster_name*.*timestamp*.**tar.gz**)。在恢复节点之前，需要提取单个节点备份文件 (*node_name*_**control**_*timestamp*.**tar** or *node_name*_**data**_*timestamp*.**tar**)。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。

- 在 管理中心 中的 /var/sf/remote-backup。
- 在远程存储位置。

在威胁防御 高可用性部署中，您将对作为一个单元进行备份，但备份过程会生成唯一的备份文件。设备的角色在备份文件名中注明。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储，第 27 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 2 删除故障设备。

关机、关闭电源并删除虚拟机。对于程序，请参阅您的虚拟托管环境的相关文档。

步骤 3 部署替换设备。

步骤 4 在替换设备上执行初始配置。

使用控制台以 admin 用户身份访问 威胁防御 CLI。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请勿设置与故障设备相同的管理 IP 地址。如果您需要注册设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

注释 如果需要修补替换设备，请按照入门指南中的说明启动管理中心注册过程。如果不需要修补， 请勿 注册。

步骤 5 确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从 管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 补丁设备： 《Cisco Firepower 管理中心升级指南》。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 6 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 /var/sf/backup。 对于集群，请确保从主集群捆绑包中提取单个节点备份文件。

步骤 7 从 威胁防御 CLI 恢复备份。

以 admin 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp-主机名称 用户名 文件路径 备份 tar-文件*
- 从本地设备： **restore remote-manager-backup** 备份 *tar-文件*

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 8 登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 9 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 10 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 11 添加和配置数据接口。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

管理备份和远程存储

备份存储为未加密的存档（.tar）文件。文件名包括标识信息，包括：

- 与备份关联的备份配置文件或计划任务的名称。
- 备份设备的显示名称或 IP 地址。
- 设备的角色，例如 HA 对的成员。

我们建议备份到安全的远程位置并验证传输是否成功。设备上的备份可以手动或通过升级过程删除；升级会清除本地存储的备份。有关您的选项的详细信息，请参阅 备份存储位置 ， 第 29 页。

注意 尤其是由于备份文件未加密的情况，因此不允许未经授权的访问。如果修改备份文件，恢复过程将失败。请记住，具有管理员/维护角色的任何人都可以访问“备份管理”页面，他们可以在其中移动和删除远程存储中的文件。

以下程序介绍如何管理备份文件。

过程

步骤 1 选择**系统**（⚙）> **工具** > **备份/恢复**。

“备份管理”页面列出了可用的备份。它还列出了可用于存储备份的磁盘空间。如果没有足够的空间，备份可能会失败。

步骤 2 执行以下操作之一：

表 *1:* 远程存储和备份文件管理

收件人	相应操作
为备份启用或禁用远程存储，而无需编辑 FMC 系统配置。	点击 **启用备份的远程存储**。 此选项仅在配置远程存储后显示。在此处切换也会在系统配置（**系统 > 配置 > 远程存储设备**）中切换它。 **提示** 要快速访问远程存储配置，请点击 **备份管理** 页面右上角的远程存储。 **注释** 要将备份存储在远程存储位置，还必须启用**检索到管理中心 (Retrieve to Management Center)** 选项（请参阅从 管理中心备份设备，第 11 页）。
在 FMC 和远程存储位置之间移动文件。	点击 **移动**。 您可以根据需要来回移动文件多次。这将从当前位置删除（而不是复制）文件。 将备份文件从远程存储移动到 FMC 时，其存储在 FMC 上的位置取决于备份的类型： • FMC 备份： `/var/sf/backup` • 设备备份： `/var/sf/remote-backup`
查看备份的内容。	点击备份文件。
删除备份文件。	选择文件，并点击 **删除**。 您可以删除本地和远程存储的备份文件。

收件人	相应操作
从您的计算机上传备份文件。	点击 **上传备份**，选择一个备份文件，然后再次点击 **上传备份** 。
将备份下载到您的计算机。	选择备份文件，然后点击 **下载**。 与移动备份文件不同，此操作不会从 FMC 中删除备份。

备份存储位置

下表介绍 管理中心 和受管设备的备份存储选项。

表 *2:* 备份存储位置

位置	详细信息
远程，通过安装网络卷（NFS、SMB、SSHFS）。	**注释** 仅当您已配置远程存储并启用检索到管理中心选项时，备份才会存储在远程存储位置（请参阅）。从管理中心备份设备，第 11 页 在 管理中心的系统配置中，您可以将 NFS、SMB 或 SSHFS 网络卷安装为 管理中心 和设备备份的远程存储；请参阅 远程存储设备。） 执行此操作后，所有后续 管理中心 备份 和 管理中心发起的设备备份都将复制到该卷，但您仍可以使用 管理中心 来管理它们（恢复、下载、上传、删除、移动）。 请注意，只有 管理中心 安装网络卷。 受管设备备份文件通过 管理中心路由。确保你有足够的带宽在管理中心 和其设备之间进行大量的数据传输。有关详细信息，请参阅将数据从Firepower管理中心下载到受管设备的准则（故障排除技术说明）。
远程，通过复制（SCP）。	**注释** 仅当您已配置远程存储并启用**检索到管理中心 (Retrieve to Management Center)** 选项时，备份才会存储在远程存储位置（请参阅 从 管理中心备份设备，第 11 页）。 对于 管理中心，可以使用**完成时复制 (Copy when complete)** 选项将已完成（SCP）的备份安全复制到远程服务器。 与通过安装网络卷的远程存储相比，**完成时复制** 无法复制到 NFS 或 SMB 卷。您无法提供 CLI 选项或设置磁盘空间阈值，并且它不会影响报告的远程存储。您也无法在备份文件复制后对其进行管理。 如果要在本地存储备份 并 将其 SCP 放置到远程位置，此选项非常有用。 **注释** 如果在 管理中心 系统配种中配置 SSHFS 远程存储，请勿在完成后使用**复制将备份文件复制到同一目录**。

位置	详细信息
本地，在 管理中心上。	如果未通过安装网络卷配置远程存储，则可以在 管理中心上保存备份文件： • 管理中心 备份保存到 /var/sf/backup。 • 如果在执行备份时启用**检索到管理中心 (Retrieve to Management Center)** 选项，设备备份将保存到 管理中心 上的 /var/sf/remote-backup 。
本地，位于设备内部闪存上。	如果您执行以下操作，设备备份文件将保存到设备上的 /var/sf/backup： • 请勿通过安装网络卷配置远程存储。 • 请勿启用 **向管理中心检索**。
本地，位于设备 SD 卡上。	对于 ISA 3000，当您将设备备份到本地 /var/sf/backup 内部闪存位置时，如果您安装了 SD 卡，备份将自动复制到 SD 卡，位于 /mnt/disk3/backup/ 用于零接触恢复。

备份和恢复历史记录

功能	版本	详细信息
支持集群备份和恢复	7.3	现在，您可以使用管理中心执行集群备份。要恢复集群节点，必须使用设备 CLI。 新增/修改的屏幕：**系统** > **工具** > **备份/恢复** > **受管设备备份** 新增/修改的命令：**restore remote-manager-backup** **注释** 对于虚拟防火墙，仅在 VMware 上支持集群的备份和恢复。
使用 SD 卡在 ISA 3000 上进行零接触恢复	7.0	执行本地备份时，备份文件将复制到 SD 卡（如果有）。要恢复替换设备上的配置，只需在新设备中安装 SD 卡，并在设备启动期间按住重置按钮 3 到 15 秒。
支持 威胁防御 容器实例的备份和恢复	6.7	您现在可以使用 管理中心 在 Firepower 4100/9300 上对 威胁防御 容器实例执行按需远程备份。
恢复的 VDB 要求	6.6	从备份恢复 管理中心 会将现有 VDB 替换为备份文件中的 VDB。在恢复之前，您不再需要匹配 VDB 版本。
自动安排的备份	6.5	对于新的或重映的 管理中心，设置流程会创建每周计划的任务，以备份 管理中心 配置并将其存储在本地。

功能	版本	详细信息
受管设备的按需远程备份	6.3	您现在可以使用管理中心来预定某些受管设备的按需远程备份。 有关支持的平台，请参阅 备份和还原要求，第 3 页。 新增/修改的屏幕： **系统 > 工具 > 备份/恢复 > 受管设备备份** 新增/修改的 威胁防御 CLI 命令：**restore**

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。