备份/恢复

- 关于备份和恢复， 第 1 页
- 备份和还原要求， 第 2 页
- 备份和恢复的指南和限制， 第 3 页
- 备份和还原的最佳实践， 第 4 页
- 备份托管设备， 第 6 页
- 恢复 CDO 托管设备， 第 7 页

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

您可以对 CDO 中的多台 Cisco Secure Firewall Threat Defense 设备执行按需备份。

注释 威胁防御 高可用性对不支持按需备份。

有关详细信息，请参阅备份托管设备， 第 6 页。

存储备份文件

您只能在本地存储备份。不支持将 威胁防御 设备备份到安全的远程位置。

有关详细信息，请参阅备份托管设备， 第 6 页。

恢复托管设备

您必须使用 威胁防御 CLI 来恢复 威胁防御 设备。

有关详细信息，请参阅恢复 CDO 托管设备， 第 7 页。

备份的内容是什么？

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，只有少数例外。在 CDO 上，恢复事件和威胁智能导向器 (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。
- 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。

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：

- 威胁防御 独立设备，本地实例，容器实例和 HA 对
- Threat Defense Virtual 适用于 VMware 设备，无论是独立或 HA 对

不 支持备份：

- 威胁防御 集群
- Threat Defense Virtual 除 VMware 的实施

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。

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。

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防火墙版本，包括补丁。

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：

- 恢复设备：无。在本地恢复设备。

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

Backup and Restore有以下指南和限制。

⚠

注意 具有 CLI 访问权限的用户可以使用 **expert** 命令访问 Linux 外壳，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在防火墙和 CDO 用户文档明确指示时使用 Linux 外壳。
- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

备份和恢复适用于灾难恢复//退货许可

备份和恢复主要用于退货许可(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，请联系更换硬件。

你也可以使用Backup and Restore来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。

Backup and Restore 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 CDO 所需的所有信息。请勿将 FTD 备份恢复到由其他 管理器管理的设备；恢复的设备将尝试连接到备份中指定的管理器。

恢复为单个和本地恢复

您可以单独和本地恢复 威胁防御设备。这意味着：

- 您无法批量恢复到高可用性（HA）设备。本指南中的还原程序介绍如何在高可用性环境中还原。
- 您无法使用 CDO 恢复设备。 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受管设备之一恢复。管理中心 和 威胁防御 设备维护自己的用户账号。

备份和还原的最佳实践

Backup and Restore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FMC），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。

- 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 FMC，以便新的 FMC 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。

威胁防御 高可用性部署中的Backup and Restore

在 威胁防御 HA 部署中，您必须：

- 从 FMC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 HA 设备生成唯一的备份文件。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。

  威胁防御 HA 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 HA。

  保持 HA 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 HA 同步才能执行此操作。

- 请勿 同时在两个对等体上运行 restore 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 restore 命令，直到第一台设备的恢复过程完成，包括重新启动。

备份前

在备份之前，您必须：

- 检查磁盘空间。

  在开始备份之前，请确保设备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，您必须：

- 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 地址冲突，请先断开旧设备与管理网络的连接，然后再更换备份。

- 请勿 取消注册受管设备。

  无论您是恢复托管设备，都不要从 CDO 注销设备，即使您从网络上物理断开设备。

  如果取消注册，则必须重做一些设备配置，例如安全区域到接口的映射。恢复后，CDO 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，因此您可能必须在重新映像后进行修补。

  如果不重新映像，请记住，CDO 入侵事件和文件列表会合并而不是覆盖。

还原后

在恢复之后，您必须：

- 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。

- 部署。

  恢复设备后，部署到该设备。您 必须 部署。如果设备未标记为过期，请从"设备管理"页面强制部署。

备份托管设备

您可以对支持的设备执行按需或计划备份。

使用 CDO 备份设备不需要使用备份配置文件。

有关详细信息，请参阅从 FMC 备份威胁防御设备 ， 第 6 页。

从 FMC 备份威胁防御设备

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、HA
- Threat Defense Virtual：VMware，独立、HA

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。不要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 2 页
- 备份和恢复的指南和限制 ， 第 3 页
- 备份和还原的最佳实践 ， 第 4 页

⚠

注意 具有 CLI 访问权限的用户可以使用 **expert** 命令访问 Linux 外壳，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在防火墙和 CDO 用户文档明确指示时使用 Linux 外壳。
- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 在“操作”(Actions) 窗格中，点击**监控 (Monitoring)**。

步骤 4 选择 **系统**（⚙），然后点击**托管设备备份 (Managed Device Backup)**。

步骤 5 选择 **Managed Device Backup**。

步骤 6 在**托管设备 (Managed Devices)** 中选择一个或多个威胁防御设备。

步骤 7 设备备份文件的**存储位置**是 `/var/sf/remote-backup/`中的本地存储。

步骤 8 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 FMC。
- 已禁用：将备份保存到 `/var/sf/backup`中的设备。

步骤 9 点击 **开始备份** 开始按需备份。

步骤 10 在**通知 (Notifications)**窗格中的**任务 (Tasks)** 下监控进度。

恢复 CDO 托管设备

对于 威胁防御 设备，您必须使用 威胁防御 CLI 从备份中恢复。您无法使用 管理中心 恢复设备。

以下各节介绍如何恢复托管设备。

- 恢复 威胁防御 设备，第 7 页
- 从备份恢复威胁防御：威胁防御虚拟，第 10 页

恢复 威胁防御 设备

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防火墙设备（独立或 HA 对）。它假定您有权访问要替换的设备的成功备份。

在 威胁防御 HA 部署中，您可以使用此程序替换任一或两个对等体。要同时替换两者，请同时在两台设备上执行所有步骤，但恢复 CLI命令本身除外。请注意，您可以在没有成功备份的情况下替换威胁防御 HA 设备。

注释 请勿 从 CDO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 HA 部署中， 请勿 暂停或中断 HA。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。不要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 2 页
- 备份和恢复的指南和限制， 第 3 页
- 备份和还原的最佳实践， 第 4 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 导航到**系统**（⚙）> **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 3 从**备份管理 (Backup Management)** 下的**设备备份 (Device Backups)** 中找到故障设备的成功备份。

根据备份配置，可以存储设备备份：

- 在故障设备上 - 将备份保存到 `/var/sf/backup` 中的 FMC。
- 在管理中心 - 将备份保存到 `/var/sf/remote-backup/` 中的设备。

在 威胁防御 HA 部署中，您将对作为一个单元进行备份，但备份过程会为对中的每个设备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。

替换设备需要备份，但可以在恢复过程中使用安全复制协议 (SCP) 命令进行检索。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 4 移除（拆开）故障设备并断开所有接口。在威胁防御 HA 部署中，这包括故障切换链路。

请参阅适用于您的型号的硬件安装和入门指南：《思科 Firepower NGFW：安装和升级指南》。

注释 请勿从管理中心取消注册，即使在断开设备与网络的连接时也是如此。在威胁防御 HA 部署中，请勿暂停或中断 HA。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 HA 部署中，请连接故障切换链路。但是， 请勿 连接数据接口。

请参阅适用于您的型号的硬件安装指南：《思科 Firepower NGFW：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《Cisco Secure Firewall ASA 和威胁防御重新映像指南》。

步骤 7 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。您可以使用控制台，也可以通过 SSH 连接到出厂默认管理接口IP地址（192.168.45.45）。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。

请参阅您的型号的入门指南中的初始配置主题： 《Cisco Firepower NGFW：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 8 确保替换设备运行与故障设备相同的 Firewall 软件版本， 包括补丁。

不应从管理中心删除现有设备。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：请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的将设备添加到管理中心。

   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) 为设备打补丁：《Cisco Firewall 管理中心升级指南》。

c) 从管理中心取消注册新安装的设备：请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的从管理中心删除设备。

   如果不取消注册，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 9 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`。

步骤 10 从 FTD 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-hostname username filepath backup tar-file**

- 从本地设备：**restore remote-manager-backup backup tar-file**

步骤 11 登录 CDO 并等待设备进行连接。

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

此时，设备应显示为过时。

步骤 12 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 HA 同步。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 FTD 设备中删除 VPN 证书，包括在执行备份后添加的证书。

步骤 13 部署配置。

您 必须 部署。如果恢复的设备未标记为过期，请从“设备管理”页面强制部署。

步骤 14 连接设备的数据接口。

请参阅适用于您的型号的硬件安装指南：《Cisco Secure Firewall Threat Defense：安装和升级指南》。

从备份恢复威胁防御：威胁防御虚拟

使用此程序可为 VMware 更换故障或发生故障的 threat defense virtual 设备。

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。保持注册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。不要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 2 页
- 备份和恢复的指南和限制，第 3 页
- 备份和还原的最佳实践，第 4 页

过程

步骤 1 导航到**系统**（⚙）> **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 从**备份管理 (Backup Management)** 下的**设备备份 (Device Backups)** 中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：

- 在故障设备上 - 将备份保存到 `/var/sf/backup` 中的 CDO。
- 在 管理中心 - 将备份保存到 `/var/sf/remote-backup/` 中的设备。

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。

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 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 4 部署替换设备。

请参阅《适用于 VMware 的 Cisco Firepower Threat Defense Virtual 入门指南》。

步骤 5 在替换设备上执行初始配置。

使用 VMware 控制台以管理员用户身份访问 threat defense virtual 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。

请参阅入门指南中的 CLI 设置主题：《适用于 VMware 的 Cisco Firepower Threat Defense Virtual 入门指南》。

步骤 6 确保替换设备运行与故障设备相同的 Firewall 软件版本， 包括补丁。

确保不应从 CDO 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 threat defense virtual 补丁应具有相同的版本。 threat defense virtual CLI 没有升级命令。要修补，请执行以下操作：

1. 完成 CDO 中的 threat defense virtual 注册流程。
2. 修补 threat defense virtual 设备。
3. 从 CDO 取消注册最新修补的设备。

步骤 7 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`。

步骤 8 从 威胁防御 CLI 恢复备份。

以 admin 用户身份访问 threat defense virtual 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-hostname username filepath backup tar-file**
- 从本地设备：**restore remote-manager-backup backup tar-file**

步骤 9 登录 CDO 并等待设备进行连接。

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

此时，设备应显示为过时。

步骤 10 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 HA 同步。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 threat defense virtual 设备中删除 VPN 证书，包括在执行备份后添加的证书。

步骤 11 部署配置。

您 必须 部署。如果恢复的设备未标记为过期，请从“设备管理”页面强制部署。

步骤 12 连接设备的数据接口。

请参阅适用于您的型号的硬件安装指南：《Cisco Secure Firewall Threat Defense：安装和升级指南》。

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。