系统管理

以下主题介绍如何执行系统管理任务，例如更新系统数据库及备份和恢复系统。

- 安装软件更新， 第 1 页
- 备份和恢复系统， 第 10 页
- 审核与变更管理， 第 15 页
- 导出设备配置， 第 21 页
- 管理 设备管理器 和 威胁防御 用户访问， 第 21 页
- 重启或关闭系统， 第 27 页
- 系统故障排除， 第 28 页
- 不常见的管理任务， 第 39 页

安装软件更新

您可以安装系统数据库和系统软件的更新。以下主题介绍如何安装这些更新。

更新系统数据库和源

系统使用许多个数据库和安全智能源来提供高级服务。思科会对这些数据库和源提供更新，以便您的安全策略采用可用的最新信息。

系统数据库和源更新概述

威胁防御 使用以下数据库 和源 提供高级服务。

入侵规则

随着新的漏洞被发现，思科 Talos 情报小组 (Talos) 会发布入侵规则更新，您可以导入更新的规则。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。

入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。

要使入侵规则更新所做的更改生效，必须重新部署配置。

入侵规则更新可能很大，所以请在网络使用量低的环境下更新重要规则。在慢速网络中，更新尝试可能会失败，您将需要重试。

地理位置数据库 (GeoDB)

Cisco 地理位置数据库 (GeoDB) 是一个与可路由的 IP 地址关联的地理数据数据库（例如国家、城市、坐标）。

GeoDB 更新提供物理位置的更新信息，系统会将这些信息与所检测到的可路由 IP 地址相关联。您可以使用地理位置数据作为访问控制规则的条件。

更新 GeoDB 所需的时间取决于您的设备；安装通常需要 30-40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时的确会占用系统资源。制定更新计划时需要考虑这一点。

漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。防火墙系统可将指纹与漏洞关联，帮助您确定某个特定主机是否会增加网络受攻击的风险。思科 Talos 情报小组 (Talos) 定期发布 VDB 更新。

更新漏洞映射所需的时间取决于网络映射中的主机数量。您可能希望在系统使用量低的期间安排更新，以尽可能地降低对任何系统停机的影响。一般说来，将网络中的主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

在更新 VDB 后必须部署配置，才能使更新的应用检测器和操作系统指纹生效。

思科 Talos 情报小组 (Talos) 安全智能源

Talos 提供对安全智能策略中使用的定期更新智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。这些源包含已知威胁的地址和 URL。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

URL 类别/信誉数据库

系统从思科综合安全智能 (CSI) 获取 URL 类别和信誉数据库。如果您配置过滤类别和信誉的 URL 过滤访问控制规则，请求的 URL 将根据数据库进行匹配。您可以在 **系统设置** > **URL 过滤首选项**上配置数据库更新和某些其他 URL 过滤首选项。您不能通过管理其他系统数据库更新的方式管理 URL 类别/信誉数据库更新。

更新系统数据库

您可以在方便之时，手动检索和执行系统数据库更新。从思科支持站点可检索更新。因此，系统的管理地址必须可连接互联网。

或者，您可以从互联网中自行检索更新软件包，然后从您的工作站上传这些更新软件包。此方法主要用于气隙网络，在其中没有用于从 Cisco 检索更新的互联网路径。从下载系统软件升级的相同文件夹中下载 software.cisco.com 的更新。

注释 在 2022 年 5 月，我们将 GeoDB 拆分为两个包：一个将 IP 地址映射到国家/地区/大洲的国家/地区代码包，以及一个包含与可路由 IP 地址相关的上下文数据的 IP 包。 设备管理器 没有，也从未使用过 IP 数据包中的信息。此拆分可在本地托管 威胁防御 部署中节省大量磁盘空间。如果您自己从 Cisco 获取 GeoDB，请确保获取国家/地区代码软件包，该软件包与旧的一体化软件包具有相同的文件名：Cisco_GEODB_Update-*date-build*。

另外，您还可以设置计划来定期检索和应用数据库更新。由于这些更新可能很大，所以请将它们安排在网络活动少的时间进行更新。

注释 在更新数据库时，您可能会发现用户界面响应操作的速度迟缓。

开始之前

为了避免对进行的更改造成任何潜在影响，请先将配置部署到设备，再手动更新这些数据库。

请注意，VDB 和 URL 类别更新可删除应用或类别。您需要更新使用这些已弃用项目的任何访问控制或 SSL 解密规则，然后才能部署更改。

过程

步骤 1 点击**设备**，然后点击“更新”摘要中的**查看配置**。

此时将打开“更新”(Updates) 页面。该页面上的信息显示每个数据库的当前版本，以及每个数据库的最后更新日期和时间。

步骤 2 要手动更新某数据库，请点击该数据库的相关部分中的以下其中一个选项：

- **从云进行更新**- 使 设备管理器 从 Cisco 检索更新软件包。这是最简单、最可靠的方法，但必须有一个到互联网的路径才能使用它。
- （**向下箭头**）>**选项**- 从您的工作站或连接到工作站的驱动器中选择更新包。该选项将是以下选项之一：
  - **选择文件** - 选择 VDB 或地理位置包。
  - **更新至更高版本** - 选择比当前安装的版本更高的入侵规则包。
  - **降级到更低版本** - 选择比当前安装的版本更低的入侵规则包。

规则和VDB更新需要部署配置，使其处于活动状态。当您从云端更新时，系统会询问是否要立即部署；点击**是**。如果点击**否**，请记住尽早启动部署作业。

如果上传自己的文件，则必须手动部署更改。

注释　手动上传入侵规则包时，请确保为您的 Snort 版本上传正确类型的包：为 Snort 2 上传 SRU；为 Snort 3 上传 LSP。您可以上传非活动 Snort 版本的包，但除非您切换版本，否则系统不会激活此包。有关切换 Snort 版本的信息，请参阅在 Snort 2 和 Snort 3 之间切换。

步骤 3 （可选）要设置定期数据库更新计划，请执行以下操作：

a) 点击所需数据库的**配置**链接部分。如果已有计划，请点击**编辑**。

数据库的更新计划是独立的。您必须单独定义计划。

b) 设置更新开始时间：

- 更新频率（每日、每周或每月）。
- 对于每周或每月更新，希望在星期几或每月几日执行更新。
- 希望开始更新的时间。 您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

c) 对于规则或 VDB 更新，如果希望系统在更新数据库时部署配置，请选中**自动部署更新**复选框。

更新在完成部署之前无效。自动部署还将部署尚未部署的任何其他配置更改。

d) 点击**保存**。

注释　如果要删除定期更新计划，请点击**编辑**链接打开计划对话框，然后点击**删除**按钮。

更新思科安全智能源

思科 Talos 情报小组 (Talos) 提供对定期更新的安全智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

过程

步骤 1 点击**设备 (Device)**，然后点击“更新”(Updates) 摘要中的**查看配置 (Save)**。

此时将打开“更新”页面。页面上的信息显示**安全智能源**的当前版本以及其上次更新日期和时间。

步骤 2 要手动更新源，请点击**安全智能源 (Security Intelligence Feeds)** 组中的**立即更新 (Update Now)**。

如果您在高可用性组中的一台设备上手动更新源，也需要在另一台设备上手动进行此更新，以确保一致性。

步骤 3 （可选。）要配置定期更新频率，请执行以下操作：

a) 点击“思科源”(Cisco Feeds) 部分中的**配置 (Configure)** 链接。如果已有计划，请点击**编辑 (Edit)**。

b) 选择所需的频率。

默认值为**每小时**。您还可以设置**每日**更新（指定具体时间）或**每周**更新（选择星期几和具体时间）。 您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

点击**删除 (Delete)** 阻止自动更新。

c) 点击**确定 (OK)**。

升级 威胁防御

使用此程序可升级 独立 威胁防御 设备。如果您需要更新 FXOS，请先执行此操作。 要升级高可用性威胁防御，请参阅升级 高可用性 威胁防御。

注意 升级时会丢弃流量。即使系统显示为非活动或无响应，也不要在升级过程中手动重新启动或关闭；您可以将系统置于不可用状态并要求重新映像。您可以手动取消失败或正在进行的主要和维护升级，并重试失败的升级。如果问题持续存在，请联系 思科 TAC。

有关升级过程中可能遇到的这些问题和其他问题的详细信息，请参阅威胁防御升级故障排除 ， 第 9 页。

开始之前

完成预升级核对表。确保部署中保持正常运行，并且能够成功通信。

提示 升级前核对表包括规划（首先阅读Cisco Secure Firewall Threat Defense 版本说明）、备份、获取升级包以及执行相关升级（例如 Firepower 4100/9300 的 FXOS）。它还包括必要的配置更改检查、 就绪性检查、磁盘空间检查，以及运行和计划任务的检查。对于详细的升级说明，包括升级前的检查清单，请参阅适用于您的版本的 《适用于设备管理器的 Cisco 安全防火墙威胁防御升级指南》 。

过程

步骤 1 选择**设备 (Device)**，然后点击“更新”(Updates) 面板中的**查看配置 (View Configuration)** 。
“系统升级”(System Upgrade) 面板将显示当前运行的软件版本和您已上传的任何升级包。

步骤 2 上传升级包。

您只能上传一个软件包。如果上传新的软件包，它将替换旧的软件包。请确保您拥有适合您的目标版本和设备型号的软件包。点击**浏览 (Browse)** 或**替换文件 (Replace File)** 以开始上传。

上传完成后，系统将显示确认对话框。在点击**确定 (OK)** 之前，可以选择**立即运行升级 (Run Upgrade Immediately)** 以选择回滚选项并立即升级。如果您现在升级，请务必完成尽可能多的升级前核对表（请参阅下一步）。

步骤 3 执行最终的升级前检查，包括就绪性检查。

重新查看预升级核对表。确保您已完成所有相关任务，尤其是最终检查。 如果不手动运行就绪性检查，它将在您启动升级时运行。如果就绪检查失败，则会取消升级。有关详细信息，请参阅运行 威胁防御的升级就绪性检查 ，第 6 页。

步骤 4 点击 **立即升级** 以开始安装过程。

a) 选择回滚选项。

您可以**升级失败时，系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在主要或维护升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。

b) 点击**继续 (Continue)** 升级并重新启动设备。

您将自动注销并转到状态页面，您可以在其中监控升级，直到设备重新启动。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则可以手动取消或重试升级。

升级时会丢弃流量。 仅对于 ISA 3000，如果您为电源故障配置了硬件旁路，则在升级期间流量会被丢弃，但在设备完成其升级后重新启动时会通过而不进行检查。

步骤 5 尽可能重新登录并验证升级是否成功。

设备摘要页面显示当前运行的软件版本。

步骤 6 完成升级后的任务。

a) 更新系统数据库。如果没有为入侵规则、VDB 和 GeoDB 配置自动更新，请立即进行更新。
b) 完成发行说明中所述的其他任何升级后配置更改。
c) 部署。

运行 威胁防御的升级就绪性检查

在系统安装升级之前，它会运行就绪性检查，以确保升级对系统有效，并会检查有时会阻止成功升级的其他项目。如果就绪性检查失败，您应在再次尝试安装之前修复问题。如果检查失败，下次尝试安装时系统会提示您，并且您可以选择是否强制安装。

您还可以在启动升级之前手动运行就绪性检查，如本程序所述。

开始之前

上传要检查的升级软件包。

过程

步骤 1 选择**设备**，然后点击“更新”摘要中的**查看配置**。

系统升级部分将显示当前运行的软件版本和您已上传的任何更新。

步骤 2 查看**就绪性检查**部分。

- 如果尚未执行升级检查，请点击**运行升级就绪性检查**链接。此区域会显示检查进度。完成此过程大约需要 20 秒。
- 如果已执行升级检查，则此部分会指示检查是成功还是失败。对于失败的检查，请点击**查看详细信息**以查看有关就绪性检查的详细信息。修复问题后，再次运行检查。

步骤 3 如果就绪性检查失败，您应在安装升级之前解决问题。详细信息包括有关如何解决指示问题的帮助。对于失败的脚本，请点击**显示恢复消息**链接以查看信息。

以下是一些典型问题：

- FXOS 版本不兼容 - 在单独安装 FXOS 升级的系统（例如 Firepower 4100/9300）中，升级软件包可能需要与当前运行的 威胁防御 软件版本不同的最低 FXOS 版本。在这种情况下，您必须先升级 FXOS，然后才能升级 威胁防御 软件。
- 不受支持的设备型号 - 无法在此设备上安装升级软件包。您可能上传了错误的软件包，或者设备是旧型号，在新的 威胁防御 软件版本中不再受支持。请检查设备兼容性并上传支持的软件包（如果有）。
- 磁盘空间不足 - 如果可用空间不足，请尝试删除不需要的文件，例如系统备份。仅删除已创建的文件。

监控威胁防御升级

当您开始升级 威胁防御 时，系统会自动将您注销并转到状态页面，您可以在其中监控总体升级进度。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则该页面允许您手动取消或重试升级。

您还可以通过 SSH 连接到设备并使用 CLI： **show upgrade status**。添加 **continuous** 关键字可在创建日志条目时查看日志条目，添加**detail** 可查看详细信息。添加这两个关键字来获取持续的详细信息。

升级完成后，当设备重新启动时，您将失去对状态页面和 CLI 的访问权限。

取消或重试威胁防御升级

使用升级状态页面或 CLI 以手动取消失败或正在进行的主要和维护升级，并重试失败的升级：

- 升级状态页面：点击**取消升级 (Cancel Upgrade)** 可取消正在进行的升级。如果升级失败，您可以点击**取消升级 (Cancel Upgrade)** 以停止作业并返回到升级前的设备状态，也可以点击**继续 (Continue)** 以重试升级。
- CLI：使用 **upgrade cancel** 以取消正在进行的升级。如果升级失败，您可以使用 **upgrade cancel** 以停止作业并返回到升级前的设备状态，也可以使用 **upgrade retry** 以重试升级。

注释 默认情况下，在升级失败时 威胁防御 自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的 升级，请在启动升级时禁用自动取消选项。在高可用性部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。

这些选项不支持打补丁。有关恢复成功升级的信息，请参阅恢复威胁防御 ，第 8 页。

恢复威胁防御

如果主要或维护升级成功但系统未按预期运行，则可以进行恢复。恢复 威胁防御 可将软件恢复到上次主要或维护升级前的状态；无法保留升级后配置更改。修补后恢复必然也会删除修补程序。请注意，您无法恢复单个修补程序或修补程序。

以下程序介绍如何从 设备管理器恢复。如果您无法进入 设备管理器，可以使用 **upgrade revert** 命令从 SSH 会话中的 威胁防御 命令行恢复。您可以使用该 **show upgrade revert-info** 命令查看系统将恢复到哪个版本。

开始之前

如果设备属于高可用性对，则必须恢复这两台设备。理想情况下，同时在两台设备上启动恢复，以便恢复配置，而不会出现故障转移问题。打开与两台设备的会话，并验证每台设备都可以恢复，然后启动恢复过程。请注意，在恢复期间流量将中断，因此请尽可能在非工作时间执行此操作。

对于 Firepower 4100/9300 机箱，主要 威胁防御 版本具有特别限定和推荐的配套 FXOS 版本。这意味着在恢复 威胁防御 软件后，您可能正在运行非推荐版本的 FXOS（太新）。尽管新版本的 FXOS 与旧版 威胁防御 版本向后兼容，但我们会对推荐的组合执行增强测试。您无法降级 FXOS，因此，如果您发现自己需要执行降级，并且想要运行推荐的组合，则需要重新映像设备。

过程

步骤 1 选择**设备**，然后点击**更新**摘要中的**查看配置**。

步骤 2 在**系统升级**部分中，点击**恢复升级**链接。

系统将显示确认对话框，其中显示当前版本以及系统将恢复到的版本。如果没有可恢复的可用版本，则不会显示**恢复升级**链接。

步骤 3 如果您熟悉目标版本（并且有一个目标版本可用），请点击**恢复**。

恢复后，必须向智能软件管理器重新注册设备。

威胁防御升级故障排除

当您升级任何设备时，无论是独立设备还是高可用性对，都可能发生这些问题。要解决特定于高可用性升级的问题，请参阅高可用性 威胁防御升级故障排除。

升级包错误。

要查找升级包正确的型号，请在 思科支持和下载站点上选择或搜索您的型号，然后浏览至相应版本的软件下载页面。列出了可用的升级包以及安装包、修补程序和其他适用的下载。升级包文件名反映平台、软件包类型（升级、补丁、修补程序）、软件版本和内部版本。

从 6.2.1 及更高版本进行升级包经过签名，并在 .sh.REL.tar 中终止。请勿解压已签名的升级包。请勿通过邮件来重命名升级包或传送它们。

升级期间根本无法访问设备。

设备在升级期间或在升级失败时停止传输流量。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。

设备在升级期间显示为非活动状态或无响应。

您可以手动取消正在进行的主要和维护升级；请参阅取消或重试威胁防御升级，第 7 页。如果设备无响应，或者如果您无法取消升级，请联系思科 TAC。

注意 即使系统显示为非活动状态，也不要在升级过程中手动重新启动或关闭。您可以将系统置于不可用状态并要求重新映像。

升级成功，但系统未按预期运行。

首先，确保缓存的信息得到刷新。不要简单地刷新浏览器窗口以重新登录。相反，请从URL中删除任何“额外”路径并重新连接到主页；例如，http://threat-defense.example.com/。

如果问题仍然存在并需要返回到较早的主要或维护版本，则可以恢复；请参阅恢复威胁防御，第 8 页。如果无法恢复，则必须重新映像。

升级失败。

启动主要或维护升级时，请使用**升级失败自动取消... (Automatically cancel on upgrade failure...)**（自动取消）选项，用于选择升级失败时的操作，如下所示：

- 自动取消已启用（默认）：如果升级失败，则升级会取消，并且设备会自动恢复到升级前的状态。请更正所有问题，然后重试。
- 自动取消已禁用：如果升级失败，设备将保持原样。请更正问题并立即重试，或手动取消升级并稍后重试。

有关详细信息，请参阅取消或重试威胁防御升级 ， 第 7 页。如果无法重试或取消，或者问题持续存在，请联系思科 TAC。

重新映像设备

重新映像设备包括擦除设备配置和安装新软件映像。重新映像是为了通过出厂默认配置实现安全安装。

在以下情况下，您可以重新映像设备：

- 要将系统从 ASA 软件转换为 威胁防御软件。无法将运行 ASA 映像的设备升级为运行 威胁防御映像的设备。
- 设备无法正常工作，而修复配置的所有尝试均失败。

有关如何重新映像设备的信息，请参阅针对您的设备型号编写的 重新映像 *Cisco ASA* 或威胁防御设备 或 威胁防御快速入门 指南。如需查阅上述指南，请访问 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html。

备份和恢复系统

您可以备份系统配置，这样在配置因后续配置错误或物理故障而受损时即可恢复设备。

仅当两台设备的型号相同且运行相同版本的软件（包括内部版本号，而不仅仅是相同的发布版）时，才可将备份恢复到替换设备上。请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一标识设备的信息，所以不能按此方式进行共享。

注释 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。备份也不包括许可或云注册信息，因此系统将保留恢复时存在的所有许可证或云注册状态。

备份仅包括配置，而不是系统软件。如果需要完全重新映像设备，您需要重新安装软件，然后才能上传备份和恢复配置。

在备份期间将锁定配置数据库。在备份期间不能更改配置，但可以查看策略、控制面板等。在恢复期间，系统完全不可用。

“备份和恢复”(Backup and Restore) 页面的表格将列出系统中可用的所有现有备份副本，包括备份的文件名、创建日期和时间及文件大小。备份类型（手动、预定或周期性）以您指示系统创建该备份副本的方式为基础。

提示 备份副本在系统中创建。您必须手动下载备份副本，并将它们存储到安全服务器上，以确保拥有执行灾难恢复所需的备份副本。系统在设备上最多保留 3 个备份副本。新备份将替换最早的备份。

以下主题介绍如何管理备份和恢复操作。

立即备份系统

您可以根据需要随时开始备份。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”(Backup and Restore) 页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 依次点击**手动备份** > **立即备份**。

步骤 3 输入备份名称和说明（后者为可选项）。

如果决定以后再进行备份（而不是立即进行），可以改为点击**计划**。

步骤 4 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 5 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 6 点击**立即备份**。

系统将开始备份过程。备份完成后，备份文件将显示在表格中。然后，您即可将备份副本下载到系统并存储到其他位置（如需）。

初始化备份后，即可离开“备份和恢复”(Backup and Restore) 页面。但是，系统可能会非常缓慢，您应考虑暂停您的工作以让备份完成。

此外，系统将在部分或所有备份期间获取配置数据库上的锁，这可能会阻止您在备份过程的持续时间内进行更改。

在预定时间备份系统

您可以设置预定备份，以便在将来的某个特定日期和时间备份系统。预定备份是一次性事件。如果要创建备份计划以定期创建备份，请配置周期性备份，而不是预定备份。

注释 如果要删除将来备份计划，请编辑该计划并点击**删除**。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**预定备份** > **计划备份**。

如果您已经有计划备份，请点击**预定备份** > **编辑**。

步骤 3 输入备份名称和说明（后者为可选项）。

步骤 4 选择备份的日期和时间。

步骤 5 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 6 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 7 点击**计划**。

当选择的日期和时间到达时，系统将执行备份。完成后，备份将在备份表格中列出。

设置周期性备份计划

您可以设置周期性备份来定期备份系统。例如，您可以在每个周五的午夜执行备份。周期性备份计划有助于确保您始终拥有一组最近的备份。

注释 如果要删除周期性计划，请编辑该计划并点击**删除**。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**周期性备份** > **配置**。

如果您已配置周期性备份，请依次点击**周期性备份** > **编辑**。

步骤 3 输入备份名称和说明（后者为可选项）。

步骤 4 选择**频率**和相关计划：

- **每日** - 选择一天的时间。系统每天在预定时间执行备份。
- **每周** - 选择星期几和当日的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每个星期一、星期三和星期五的 23:00（晚上 11 点）进行。

- **每月** - 选择每月的日期和当日的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每月一 (1) 日、十五 (15) 日和二十八 (28) 日的 23:00（晚上 11 点）进行。

您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

步骤 5 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 6 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 7 点击**保存**。

到所选日期及时间时，系统执行备份。完成后，备份将在备份表格中列出。

周期性计划将持续执行备份，直到您更改或删除该计划为止。

恢复备份

只要设备运行的软件版本（包括内部版本号）与备份时相同，即可根据需要还原备份。只有两台设备的型号相同且运行相同版本的软件（包括内部版本号），才能将备份恢复到替换设备上。

不过，当设备属于高可用性对的一部分时，您无法恢复备份。您必须首先从**设备 (Device)** > **高可用性 (High Availability)** 页面中断高可用性，然后才能恢复备份。如果备份包括高可用性配置，设备将重新加入高可用性组。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。

如果设备中没有要恢复的备份副本，必须先上传该备份，才能进行恢复。

在恢复期间，系统完全不可用。

注释 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。备份也不包括许可或云注册信息，因此系统将保留恢复时存在的所有许可证或云注册状态。

开始之前

如果要在其他系统上恢复备份，例如，在更换设备时，最佳做法是先注册设备并启用备份文件中配置的功能所需的所有可选许可证。备份文件不包含许可证或云服务信息，因此系统将保留在恢复之前所做的所有许可证更改或云注册。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”(Backup and Restore) 页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 如果可用的备份列表中没有要恢复的备份副本，请依次点击**上传** > **浏览**，并上传该备份副本。

步骤 3 点击该文件的恢复图标 ( )。

您需要确认恢复。默认情况下，恢复后系统将删除备份副本，但您可以事先选择**恢复后不删除备份**以保留备份副本，然后再继续进行恢复。

如果备份文件已加密，则必须输入打开文件和解密所需的**密码**。

恢复完成后，系统会重新启动。

注释 系统重新启动后，会自动检查漏洞数据库 (VDB)、地理位置和规则数据库更新，并根据需要进行下载。由于这些更新可能很大，因此初始尝试可能会失败。请检查任务列表，如果下载失败，请手动下载更新，如更新系统数据库，第 2 页中所述。系统还会重新部署策略。在更新成功之前，任何后续部署都将失败。

步骤 4 如有必要，请依次点击**设备** > **智能许可证** > **查看配置**，重新注册该设备，并重新启用所需的可选许可证。

备份不包括许可证或云注册信息。因此，如果将备份恢复到新系统（例如，在更换设备时），并且系统处于评估模式，则需要注册该设备并启用所需的所有许可证。如果在恢复之前注册设备并启用许可证，则无需进行其他更改。

如果您只是将以前的备份恢复到同一系统，则无需对许可证或云注册进行任何更改。但是，请验证是否已启用所需的所有可选许可证，因为备份可能包括需要在创建备份后禁用的许可证的功能。

更换 ISA 3000 设备

您可以移除 ISA 3000 的 SD 卡，将其插入另一台 ISA 3000 设备。如果您在 SD 卡上创建系统备份，可以使用此功能轻松更换设备。只需取出故障设备的 SD 卡，并插入新的设备。然后即可通过备份进行恢复。

要确保您有必要的备份，请配置备份作业以在 SD 卡上创建备份。

管理备份文件

在创建新备份时，备份文件将列在“备份和恢复”(Backup and Restore) 页面。备份副本不会无限期保留：当设备上的磁盘空间使用率达到最大阈值时，系统将删除较早的备份副本以便为较新的备份腾出空间。此外，当您安装除热修复以外的任何升级时，所有备份文件都会被删除。因此，您应定期管理备份文件，确保保存最希望保留的特定备份。

您可以执行以下操作来管理备份副本：

- 将文件下载到安全存储 - 要将备份文件下载到您的工作站，请点击该文件的下载图标 ( )。然后，您就可以将该文件移到安全文件存储了。
- 将备份文件上传到系统 - 如果要恢复设备中不再可用的备份副本，请依次点击**上传 (Upload)** > **浏览文件 (Browse File)**，并从工作站上传文件。然后即可执行恢复。

注释 可以重命名上传的文件，以便与原始文件名匹配。此外，如果系统中的备份副本已超过 3 个，系统将删除最早的备份副本，以便为上传的文件腾出空间。无法上传使用较早的软件版本创建的文件。

- 恢复备份 - 要恢复备份，请点击该文件的恢复图标 ( )。系统在恢复期间不可用，恢复完成后将重新启动。在系统正常运行后，您需要部署配置。
- 删除备份文件 - 如果不再需要某个特定备份，请点击该文件的删除图标 ( )。您需要确认删除。删除后，则无法恢复备份文件。

审核与变更管理

您可以查看有关系统事件以及用户已执行操作的状态信息。此信息可以帮助您审核系统，并确保正确地管理系统。

依次点击**设备 (Device)** > **设备管理 (Device Administration)** > **审核日志 (Audit Log)** 可以查看审核日志。此外，您可以通过点击右上角的**任务列表 (Task List)** 或**部署 (Deployment)** 图标按钮查找系统管理信息。

以下主题介绍系统审核和变更管理的一些主要概念和任务。

审核事件

审核日志可包括以下类型的事件：

自定义源更新事件，自定义源更新失败

这些事件表示已成功完成或失败的自定义安全智能源更新。详细信息包括更新开始者，以及有关正在更新的源的信息。

自定义规则文件导入摘要事件

这些事件表明您导入了包含一个或多个自定义入侵规则的文件。事件中包括已添加、已更新和已删除规则数的摘要，以及显示有关已导入规则的详细信息的差异视图。

部署已完成，部署失败：作业名称或实体名称

这些事件表示部署作业已成功完成或失败。详细信息包括作业发起人以及与作业实体相关的信息。失败的作业包括与失败相关的错误消息。

详细信息还包括一个**差异视图**选项卡，其中显示了作业执行过程中部署到设备的更改。这里汇总了已部署实体的所有实体更改事件。

要过滤这些事件，只需点击**部署历史记录**预定义过滤器。请注意，这些事件的事件类型是部署事件，您无法仅过滤已完成或失败的事件。

事件名称包括用户定义的作业名称（如果进行了配置）或“用户（用户名）触发的部署”。其中还包括，在运行设备设置向导期间发生的“设备设置自动部署”和“设备设置自动部署（最后一步）”作业。

实体已创建、实体已更新、实体已删除：实体名称（实体类型）

这些事件表示对识别的实体或对象进行了更改。实体详细信息包括实施更改的人员以及实体名称、类型和ID。您可以过滤这些项目。详细信息还包括一个**差异视图**选项卡，其中显示了应用于对象的更改。

HA 操作事件

这些事件与有关高可用性配置的操作有关，它们可以是您发起的操作，也可以是系统发起的操作。HA 操作事件的类型为事件，但事件名称是以下项之一：

- **HA 已暂停** - 有意暂停系统上的 HA。
- **HA 已恢复** - 有意恢复系统上的 HA。
- **HA 已重置** - 有意重置系统上的 HA。
- **HA故障转移：设备切换模式** - 有意切换模式，或系统由于运行状况指标违规而进行了故障转移。此消息表明，主用对等体变为了备用设备，或备用对等体变为了主用设备。

高可用性同步已完成

主用设备的配置已与备用设备同步。事件包括与同步版本相比之前版本的更改信息。

已扫描接口列表

此事件表示您已扫描接口清单中的更改。

已放弃等待完成的更改

此事件表示已删除所有待完成的更改。此事件与先前的“部署已完成”事件之间由“实体已创建”、“实体已更新”以及“实体已删除”事件指明的所有更改均已删除，并且受影响对象的状态恢复到上一次部署的版本。

规则更新事件

运行 Snort 3 时，来自 LSPUpdateServer 实体的此事件显示在下载和安装新入侵规则包时添加、删除或更改的入侵规则相关详细信息。事件限制为 100 条规则，因此，如果添加、删除或更改的规则超过 100 条，则事件将无法提供完整的信息。对于 Snort 2 更新，系统不会显示此事件。

任务已开始，任务已完成，任务失败

任务事件表示系统或用户发起的作业的开始和结束。这两个事件将会整合到任务列表中的一个任务中，您可以通过点击右上角的**任务列表**按钮进行查看。

任务包括部署作业以及手动或计划的数据库更新等操作。任务列表中的任何项目都将与审核日志中的两个任务事件对应，指示任务开始、成功完成或失败。

用户已登录、用户已注销：用户名

这些事件显示用户登录和注销设备管理器的时间和源IP地址。主动注销和因空闲时间超时而自动注销都会引发“用户已注销”事件。

这些事件无关于与设备建立连接的 RA VPN 用户。它们也不包含登录/注销设备 CLI。

查看和分析审核日志

审核日志包括有关系统发起和用户发起事件的相关信息，例如，部署作业、数据库更新和登录/注销设备管理器。

有关日志中可以显示的事件类型的说明，请参阅审核事件，第 15 页。

过程

步骤 1 点击**设备**，然后点击**设备管理** > **查看配置**链接。

步骤 2 点击目录中的**审核日志**（如果未将其选定）。

事件将按照日期分组，一天内的事件按时间分组，日期/时间最新的事件排在列表顶部。最初，所有事件都处于折叠状态，只能看到时间、事件名称、发起事件的用户以及该用户的源 IP 地址。如果用户和 IP 地址为“系统”，这意味着事件是由设备自身发起的。

可以执行以下操作：

- 点击事件名称旁边的 >，可打开事件并查看详细信息。再次点击该图标可关闭事件。很多事件具有一系列简单的事件属性，例如，事件类型、用户名、源 IP 地址等。但实体和部署事件包含两个选项卡：
  - **摘要**显示基本事件属性。
  - **差异视图**显示现有的“已部署”配置与事件过程中所发生变更的对比信息。如果是部署作业，此视图可能会很长，需要滚动鼠标才能完整查看。它将汇总部署作业过程中实体事件变更的所有差异。
- 从过滤器字段右侧的下拉列表中选择不同的时间范围。默认是查看过去 2 周的事件，但您可以更改范围，查看过去 24 小时、7 天、1 个月或 6 个月的事件。点击**自定义 (Custom)** 可通过输入开始和结束日期与时间指定具体范围。
- 点击日志中的任意链接，为该条目添加搜索过滤器。列表会更新，仅显示包含该条目的事件。您也可以点击**过滤器 (Filter)** 框，直接构建过滤器。此外，还可以点击过滤器框下方的预定义过滤器，加载相关的过滤条件。有关过滤事件的详细信息，请参阅过滤审核日志，第 18 页。

- 重新加载浏览器页面将会刷新日志，以显示最新事件。

过滤审核日志

您可以对审核日志应用过滤器，将视图显示范围缩小到仅显示特定类型的消息。过滤器中的每个元素都是一个准确、完全的匹配。例如，“User = admin”仅显示名为 **admin** 的用户发起的事件。

您可以单独或组合使用以下方法来构建过滤器：每次添加过滤器元素时，列表都会自动更新。

点击预定义过滤器

过滤器字段下方是预定义的过滤器。点击链接即可加载过滤器。系统将要求您进行确认。如果您已应用过滤器，该过滤器会被替换，也不会添加该过滤器。

点击高亮显示的条目

要构建过滤器，最简单的方法是点击日志表或事件详细信息中包含作为过滤标准的值的条目。点击条目后，**过滤器**字段将替换为该值和元素组合的格式设置正确的元素。但是，使用此方法要求现有的事件列表中包含所需的值。

如果可以为条目添加过滤器元素，当您将鼠标指针悬停在该条目上时，该条目会标有下划线，并显示命令**点击添加到过滤器**。

选择原子元素

此外，您还可以通过以下方法创建过滤器：点击**过滤器**字段，从下拉列表中选择所需的原子元素，在等号后面键入匹配值，然后按 Enter 键。您可以过滤以下元素。请注意，对于每种类型的事件而言，并非所有元素都是相关的。

- **事件类型** - 事件类型通常与事件名称（不含实体名称或用户等变量限定符）相同，但并非总是这样。部署事件的事件类型是“部署事件”。有关事件类型的说明，请参阅审核事件，第 15 页。
- **用户** - 发起事件的用户的名称。系统用户采用字母全部大写的形式：SYSTEM。
- **源 IP** - 用户发起事件的源 IP 地址。系统发起事件的源 IP 地址是 SYSTEM。
- **实体 ID** - 实体或对象的 UUID，这是一种比较长且不可读的字符串，例如 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931。通常，要使用此过滤器，您需要点击事件详细信息中的实体 ID，或使用 REST API 通过相关 GET 调用检索所需的 ID。
- **实体名称** - 实体或对象的名称。对于用户创建的实体，实体名称通常是您为对象指定的名称，例如，将网络对象命名为 InsideNetwork。对于系统生成的实体或（在某些情况下）用户定义的实体，实体名称是预定义但可识别的名称，例如，将没有明确命名的部署作业命名为“User (admin) Triggered Deployment”。
- **实体类型** - 实体或对象的类型。这些是预定义但可识别的名称，例如 Network Object。您可以通过查看相关对象模型的“type”值，在 API Explorer 中查找实体类型。API 类型通常采用字母全部小写形式，且不含空格。如果您完全按照模型中所示输入类型，则按 Enter 键

时，字符串会变成可读性更强的格式。这两种输入方式都可以接受。要打开 API Explorer，点击更多选项按钮 (⋮) 并选择 **API Explorer**。

复杂审核日志过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，包括“User = admin”和“User = SYSTEM”将会匹配由任一用户发起的事件。
- 不同类型的元素之间为 AND 关系。例如，包括“Event Type = Entity Updated”和“User = SYSTEM”仅会显示由系统而非活动用户更新实体的事件。
- 您不能使用通配符、正则表达式、部分匹配或简单的文本字符串匹配。

检查部署和实体更改历史记录

部署和实体事件在事件详细信息中包括**差异视图**选项卡。此选项卡以彩色显示旧配置与更改之间的对比情况。

- 对于部署作业，此对比为部署之前设备上运行的配置与实际所部署更改之间的对比。
- 对于实体事件，这些是对之前版本的对象所做的配置更改。之前的版本可能是实际设备使用的版本，也可能是对象尚未部署的变化。

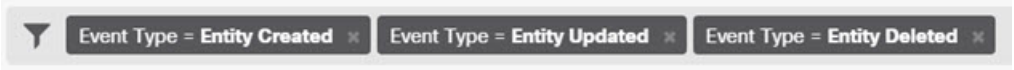
过程

步骤 1 点击**设备**，然后点击**设备管理** > **查看配置**链接。

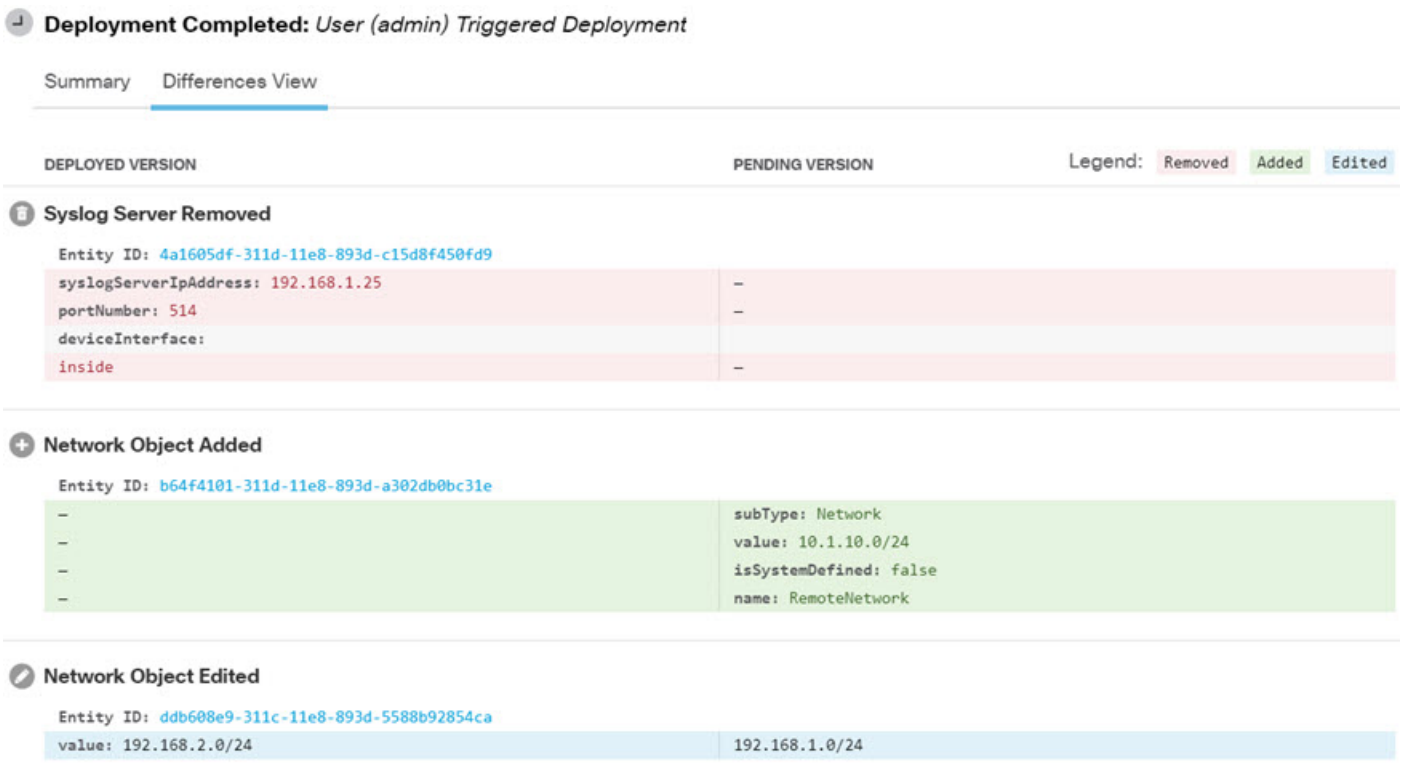
步骤 2 点击目录中的**审核日志**（如果未将其选定）。

步骤 3 （可选。）过滤消息：

- 部署事件 - 点击过滤器框下的**部署历史记录**预定义过滤器。
- 实体更改事件 - 使用事件类型元素为您感兴趣的更改类型手动创建过滤器。要查看所有实体更改，请选择实体已创建、实体已更新和实体已删除这三种规格。过滤器应如下所示：



步骤 4 打开事件，然后点击**差异视图**选项卡。



所做的更改会使用颜色编码，标题指示对象的类型以及对象是被添加（创建）、移除（删除）还是编辑（更新）。编辑的对象仅显示已更改或从该对象删除的属性。在部署作业中，每个更改的实体都有单独的标题。标题表明对象的实体类型。

放弃所有待处理更改

如果您对一套尚未部署的配置更改不满意，您可以放弃所有待处理的更改。此操作使所有功能均恢复到设备上存在的状态。之后，您可以再重新开始部署配置更改。

过程

步骤 1 点击网页右上角的**部署更改 (Deploy Changes)** 图标。

如存在待处理的更改，系统会用圆点高亮显示。

步骤 2 依次点击**更多选项 (More Options)** > **全部放弃 (Discard All)**。

步骤 3 点击确认对话框中的**确定 (OK)**。

系统将放弃更改，操作完成后您会看到一条表示没有待处理更改的消息。系统会在审核日志中添加“已放弃待处理的更改”事件。

导出设备配置

可以 JSON 格式导出一份当前部署的配置。可以使用该文件进行归档或备案。密码和密钥等所有敏感数据均被屏蔽。

无法将文件导入此设备或其他设备。此功能不会取代系统备份。

必须至少完成一个成功的部署作业，才能下载配置。

过程

步骤 1 选择**设备 (Device)**，然后点击**设备管理 (Device Administration)** 组中的**查看配置 (View Configuration)**。

步骤 2 点击目录中的**下载配置 (Download Configuration)**。

步骤 3 点击**获取设备配置 (Get Device Configuration)** 启动创建文件的作业。

如果您之前创建了一个文件，您将看到一个下载按钮和一条含文件创建日期的**文件可供下载**消息。

生成文件可能需要几分钟的时间，具体取决于配置的大小。检查任务列表或审核日志，或者定期返回到此页面，直到导出配置作业完成并生成文件。

步骤 4 生成文件后，返回到此页面并点击**下载配置文件 (Download the Configuration File)** 按钮 () 将文件保存到工作站。

管理 设备管理器 和 威胁防御 用户访问

您可以为登录到威胁防御的用户配置外部身份验证和授权源（HTTPS 访问）。您可以将外部服务器与本地用户数据库和系统定义的 **admin** 用户结合使用，或不使用后两者。请注意，您无法创建用于设备管理器 访问的额外本地用户帐户。

虽然您可以有多个可以更改配置的外部 设备管理器用户帐户，但用户不跟踪这些更改。当一个用户部署更改时，所有用户做出的更改均被部署。没有任何锁定：即，多个用户可能会尝试在同一时间更新同一对象，这将导致只有一个用户能够成功保存更改。您也无法基于用户丢弃更改。

您可以有 5 个并发用户会话。如果第六个用户登录，开始时间最早的用户会话会自动注销。还有空闲超时，非活动用户空闲 20 分钟后注销。

您还可以为对 威胁防御 CLI 的 SSH 访问配置外部身份验证和授权。在使用外部源之前，总是会检查本地数据库，以便您可以创建其他本地用户，实现故障保护访问。请勿在本地源和外部源中重复创建用户。除 **admin** 用户之外，CLI 和 设备管理器 用户之间没有任何交叉：用户帐户是完全独立的。

注释 使用外部服务器时，您可以通过设置单独的 AAA 服务器组，或在仅允许用户访问特定 威胁防御 设备 IP 地址的 AAA 服务器中创建身份验证/授权策略，来控制用户对您部分设备的访问。

以下主题介绍如何配置和管理 设备管理器 用户访问和 CLI 用户访问。

为 设备管理器 (HTTPS) 用户配置外部授权 (AAA)

您可以从外部 AAA 服务器提供对 设备管理器 的 HTTPS 访问权限。通过启用 AAA 身份验证和授权，您可以提供不同级别的访问权限，使并非每个用户都通过本地 **admin** 账户登录。

这些外部用户还有权访问 威胁防御API 和 API Explorer。

您可以通过在 AAA 服务器中设置管理用户的授权来提供基于角色的访问控制 (RBAC)。级别因服务器类型而异。用户登录 设备管理器后，页面右上角将显示用户名和角色：管理员、读写用户或只读用户。在 RADIUS 服务器上正确设置账户后，您可以使用此程序启用账户，以进行管理访问。

RADIUS 用户授权

要提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户以定义 **cisco-av-pair** 属性（注意这是在 ISE 中，而在 Free RADIUS 中该属性拼写为 Cisco-AVPair；请检查系统的拼写是否正确）。必须在用户账户上正确定义此属性，否则系统会拒绝用户访问 设备管理器。以下是受支持的 **cisco-av-pair** 属性值：

- **fdm.userrole.authority.admin** 提供完全管理员访问权限。这些用户可以执行本地 **admin** 用户可以执行的所有操作。
- **fdm.userrole.authority.rw** 提供读写访问权限。这些用户可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止 设备管理器 用户的会话。
- **fdm.userrole.authority.ro** 提供只读访问权限。这些用户可以查看控制面板和配置，但无法进行任何更改。如果用户尝试进行更改，会显示错误消息，指明权限不足。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击 **AAA 配置**选项卡（如果未将其选定）。

步骤 3 配置 **HTTPS 连接**选项：

- **管理/REST API 的服务器组**-选择您想要用作主要身份验证源的 RADIUS 服务器组（用于外部身份验货/授权）或本地用户数据库 (LocalIdentitySource)。

如果尚不存在服务器组，点击链接立即创建服务器组。对于 RADIUS，您还需要为每个服务器创建 RADIUS 服务器对象，将这些对象添加到组（定义服务器组时可以执行此操作）。有关 RADIUS 的详细信息，请参阅 RADIUS 服务器和组。

- **使用本地身份源进行身份验证** （仅限 RADIUS）- 如果您选择外部 RADIUS 服务器组，可以指定如何使用包含本地 **admin** 用户账户的本地身份源。选择以下一个选项：
  - **在外部服务器之前** - 系统首先对照本地源检查用户名和密码。
  - **在外部服务器之后** - 仅当外部源不可用或在外部来源中找不到用户账户时，才检查本地源。
  - **从不** -（不推荐。）从不使用本地源，因此不能以 admin 用户身份登录。

    注意　如果您选择 **从不**，将无法使用 **管理员** 账户登录 设备管理器 。如果 AAA 服务器不可用，或者未在 AAA 服务器中配置账户，您将被锁定在系统外面。

步骤 4 点击**保存 (Save)**。

配置 威胁防御 CLI (SSH) 用户外部授权 (AAA)

您可以从外部 RADIUS 服务器提供对 威胁防御 CLI 的 SSH 访问权限。通过启用 RADIUS 身份验证和授权，您可以从单个身份验证源提供不同级别的访问权限，而无需在每台设备上定义单独的本地用户账户。

这些 SSH 外部用户**不**具备访问 威胁防御 API 和 API Explorer 的权限。用于定义 SSH 授权的机制不同于 HTTPS 访问权限所需的机制。但是，您可以配置同时符合 SSH 和 HTTPS 授权条件的 RADIUS 用户，以便指定用户可以通过两种协议访问系统。

要为 SSH 访问权限提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户，以定义 **Service-Type** 属性。必须在用户账户上定义此属性，否则系统会拒绝用户对设备的 SSH 访问。以下是受支持的 **Service-Type** 属性值：

- **管理 (6)** 提供对 CLI 的 **config** 访问授权。这些用户可以在 CLI 中使用所有命令。
- **NAS 提示 (7)** 或除级别 6 以外的任何级别 - 提供 CLI 的**基本**访问授权。这些用户可以使用只读命令（例如 **show** 命令），用于监控和故障排除。

在 RADIUS 服务器上正确设置账户后，您可以使用此程序启用账户，以进行 SSH 管理访问。

注释　请勿在本地源和外部源中重复创建用户。如果创建了重复的用户名，请确保它们具有相同的授权权限。当本地用户账户的授权权限不同时，您无法使用外部版本用户账户的密码登录；您仅可使用本地密码登录。如果权限相同，假定密码不同，则您使用的密码将确定您是登录到外部用户还是本地用户中。即使先检查本地数据库，如果本地数据库中存在用户名但密码不正确，还是会检查外部服务器，如果外部源的密码正确，则登录成功。

开始之前

请告知外部定义的用户以下操作，使他们合理设置预期：

- 外部用户首次登录时，威胁防御 会创建所需的结构，但不能同时创建用户会话。用户只需再次进行身份验证，即可启动会话。用户将看到与以下消息类似的消息：“已识别新的外部用户名。请重新登录以启动会话。”
- 同样地，如果自上次登录以来，Service-Type 中定义的用户授权发生了更改，则用户将需要重新进行身份验证。用户将看到与以下消息类似的消息：“您的授权权限已更改。请重新登录以启动会话。”

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击 **AAA 配置**选项卡（如果未将其选定）。

步骤 3 配置 **SSH 连接**选项：

- **服务器组** - 选择您想要用作主要身份验证源的 RADIUS 服务器组或本地用户数据库 (LocalIdentitySource)。必须选择要使用外部授权的 RADIUS 服务器组。

  如果尚不存在服务器组，点击**创建新 RADIUS 服务器组**链接立即创建服务器组。您还需要为每个服务器创建 RADIUS 服务器对象，将这些对象添加到组（定义服务器组时可以执行此操作）。有关 RADIUS 的详细信息，请参阅 RADIUS 服务器和组。

  请注意，SSH 连接仅使用组中的前 2 个服务器。如果使用的组中包含 3 个或更多的服务器，系统永远不会尝试其余的服务器。此外，系统也不会使用**空载时间**和**最大失败尝试次数**组属性。

- **使用本地身份源进行身份验证** - 如果您选择外部服务器组，则可以指定如何使用本地身份源。对于 SSH 访问，系统始终会在检查外部服务器之前检查本地数据库。

步骤 4 点击**保存 (Save)**。

管理 设备管理器 用户会话

依次选择**监控** > **会话**，查看当前登录到 设备管理器的用户的列表。列表会显示当前会话每个用户登录的持续时间。

如果相同的用户名出现多次，则表示用户从不同的源地址打开会话。系统根据用户名和源地址单独跟踪会话，而且每个会话具有唯一时间戳。

系统允许 5 个并发用户会话。如果第六个用户登录，开始时间最早的当前会话会自动注销。此外，非活动状态长达 20 分钟的空闲用户会被自动注销。

如果 设备管理器 用户输入错误的密码且连续 3 次尝试登录失败，则该用户的账户将锁定 5 分钟。用户必须待锁定时间结束后方可尝试重新登录。无法解锁 设备管理器用户账户，也无法调整重试计数或锁定超时。（请注意，对于 SSH 用户，可以调整这些设置并解锁账户。）

如果有必要，您可以通过点击会话的删除图标 ( ) 终止用户会话。如果您删除您自己的会话，您也会被注销。结束会话没有锁定时段：用户可以立即重新登录。

启用备用 HA 设备上的外部用户 设备管理器 访问权限

如果为 设备管理器用户配置了外部授权，则这些用户可以登录到高可用性对的主用和备用设备。但是，与登录主用设备相比，首次成功登录备用设备还需要执行一些额外操作。

外部用户首次登录到主用设备后，系统会创建一个对象，定义用户和用户的访问权限。随后，管理员或读写用户必须在主用设备上，为要在备用设备上显示的用户对象部署配置。

只有在部署和后续配置同步成功完成之后，外部用户才可登录到备用设备。

管理员和读写用户在登录到主用设备后可以部署更改。但是，只读用户无法部署配置，且必须请求拥有适当权限的用户部署配置。

为 威胁防御CLI 创建本地用户账户

您可以在 威胁防御设备上为 CLI 访问创建用户。这些账户不允许访问管理应用，仅允许访问 CLI。CLI 对于故障排除和监控非常有用。

您不能一次性在多个设备上创建本地用户账户。每个设备都有自己的一组唯一本地用户 CLI 账户。

过程

步骤 1 使用具有配置权限的账户登录设备 CLI。

管理员用户账户具有所需的权限，但具有配置权限的任何账户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些设备型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 威胁防御 CLI。

步骤 2 创建用户账户。

configure user add *username* {**basic** | **config**}

您可以使用以下权限级别定义用户：

- **config** - 提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。
- **basic** - 提供用户基本访问权限。此级别不允许用户输入配置命令。

示例：

以下示例将添加一个名为 joecool 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

注释　　告知用户他们可以使用 **configure password** 命令更改密码。

步骤 3　（可选。）根据安全要求调整该账户的特性。

您可以使用以下命令更改默认账户行为。

- **configure user aging** *username max_days warn_days*

  设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建账户时，密码没有到期日。

- **configure user forcereset** *username*

  强制用户下次登录时更改密码。

- **configure user maxfailedlogins** *username number*

  设置在锁定账户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁账户。新账户的默认值为 5 次连续失败登录。

- **configure user minpasswdlen** *username number*

  设置最小密码长度，此值介于 1 至 127 之间。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4　根据需要管理用户账户。

用户可能被锁定在账户之外了，也可能您需要删除账户或解决其他问题。使用以下命令管理系统中的用户账户。

- **configure user access** *username* {**basic** | **config**}

  更改用户账户的权限。

- **configure user delete** *username*

  删除指定的账户。

- **configure user disable** *username*

  禁用指定的账户，而不将其删除。用户无法登录，直到您启用该账户为止。

- **configure user enable** *username*

启用指定的账户。

- **configure user password** *username*

  更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

- **configure user unlock** *username*

  解锁因超出最大连续失败登录尝试次数而被锁定的用户账户。

重启或关闭系统

如有必要，可以重新启动或关闭系统。

除了以下操作过程，还可以使用 **reboot** 或 **shutdown** 命令通过 SSH 会话或 设备管理器 CLI 控制台执行这些任务。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **重新启动/关闭** > 链路。

如果已经位于“系统设置”页面中，只需点击目录中的**重新启动/关闭 (Reboot/Shutdown)**

步骤 2 点击执行所需功能的按钮。

- **重新启动** - 如果认为系统运行不正确，而其他方法均无法解决问题，则可以重新启动设备。此外，可能有几个操作过程要求重新启动设备以重新加载系统软件。
- **关闭** - 关闭系统，以控制方式关闭电源。例如，如果想要从网络中删除设备（例如，为了更换设备），请使用“关闭”按钮。关闭设备后，可以用硬件开/关按钮重新打开设备。

步骤 3 等待操作完成。

如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

重新启动或关闭系统时，无法在 设备管理器 或 CLI 中执行其他操作。

重新启动期间，设备管理器 页面应在重新启动完成后刷新，并将您带至登录页面。如果在重新启动完成之前尝试刷新页面，则 Web 浏览器可能会基于该时间点的 设备管理器 Web 服务器运行状态返回 503 或 404 错误。

如果关闭设备，系统最终将无法响应，您将收到404错误。这是正常结果，因为您完全关闭了系统。

系统故障排除

以下主题介绍一些系统级故障排除任务和功能。有关对特定功能（如访问控制）进行故障排除的信息，请参阅相应功能的章节。

Ping 地址以测试连接

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否会做出响应。这意味着基本连接正常工作。然而，在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。您可通过打开 CLI 控制台或登录设备 CLI 来使用 **ping** 。

注释 由于系统有多个接口，您可以控制用于 ping 地址的接口。必须确保使用正确的命令，以便测试重要的连接。例如，系统必须能够通过虚拟管理接口访问思科许可证服务器，因此您必须使用**ping system** 命令测试连接。如果使用 **ping**，则测试的是能否通过数据接口访问地址，这可能不会得到相同的结果。

正常 ping 使用 ICMP 数据包测试连接。如果您的网络禁止 ICMP，可以换用 TCP ping（仅用于数据接口 ping）。

您可以对 IP 地址或完全限定主机名 (FQDN) 执行 ping。要对 FQDN 执行 ping，为管理接口或数据接口配置的 DNS 服务器必须成功返回 IP 地址。必须为管理接口和数据接口分别配置 DNS 服务器。如果没有为特定接口配置 DNS 服务器，请使用 **dig** 命令查找给定 FQDN 的 IP 地址。

以下是 ping 网络地址的主要选项。

通过虚拟管理接口 ping 地址

使用 **ping system** 命令。

ping system *host*

主机可以是 IP 地址或完全限定域名 (FQDN)，例如 www.example.com。不同于通过数据接口进行 ping 操作，系统 ping 没有默认计数。ping 操作会持续执行，直到您使用 Ctrl+c 将其停止。例如：

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

使用路由表，通过数据接口 ping 地址

使用 **ping** 命令。测试的是系统一般能否找出通往主机的路由。因为这是系统正常路由流量的方式，所以您通常需要对此进行测试。

ping *host*

例如：

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

注释 您可以指定超时、重复计数、数据包大小甚至发送时所用的数据模式。在 CLI 中使用帮助指示符？查看可用的选项。

通过特定数据接口 ping 地址

如果要通过特定数据接口测试连接性，可使用 **ping interface** *if_name* 命令。 您还可以使用此命令指定诊断接口，但不能指定虚拟管理接口。

ping interface *if_name host*

例如：

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

使用 TCP ping，通过数据接口 ping 地址

使用 **ping tcp** 命令。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。

ping tcp [**interface** *if_name*] *host port*

您必须指定主机和 TCP 端口。

您可以选择指定接口，即 ping 的源接口，而不是用于发送 ping 的接口。此类 ping 通常使用路由表。

TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。例如：

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

注释 您还可以指定 TCP ping 的超时、重复计数和源地址。在 CLI 中使用帮助指示符 ? 查看可用的选项。

跟踪主机路由

如果您向某个IP地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。traceroute 的工作方式是从无效端口向目标发送 UDP 数据包或者向目标发送 ICMPv6 回应。通往目标沿途的路由器以 ICMP Time Exceeded 消息响应，并向 traceroute 报告该错误。每个节点会收到三个数据包，因此对于每个节点，您有三次机会获得信息性结果。您可通过打开 CLI 控制台或登录设备 CLI 来使用 **traceroute** 。

注释 通过数据接口 (**traceroute**) 或通过虚拟管理接口 (**traceroute system**) 跟踪路由有单独的命令。请务必使用正确的命令。

下表说明了输出中显示的每个数据包的可能结果。

输出符号	说明
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

通过虚拟管理接口跟踪路由

使用 **traceroute system** 命令。

traceroute system *destination*

主机可以是 IPv4/IPv6 地址或完全限定域名 (FQDN)，例如 www.example.com。例如：

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
```

```
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

通过数据接口跟踪路由

使用 **traceroute** 命令。

traceroute *destination*

如果为数据接口配置 DNS 服务器，主机可以是 IPv4/IPv6 地址或完全限定域名 (FQDN)，例如 www.example.com。如果没有为特定接口配置 DNS 服务器，请使用 **dig** 命令查找给定 FQDN 的 IP 地址。例如：

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

注释 您可以指定超时、生存时间、每个节点的数据包数量，乃至要用作 traceroute 源的 IP 地址或接口。在 CLI 中使用帮助指示符 ? 查看可用的选项。

使设备显示在跟踪路由上

默认情况下，威胁防御不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，您必须创建配置所需的服务策略规则和其他选项的 FlexConfig 对象。

有关服务策略和流量类别的详细讨论，请参阅《思科 *ASA* 系列防火墙配置指南》，网址为 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 创建减小 TTL 的对象。

a) 点击 **+** 按钮以创建新的对象。

b) 为对象输入名称。例如，**Decrement_TTL**。

c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从FlexConfig策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) 点击**确定**保存对象。

步骤 4 将对象添加到 FlexConfig 策略中。

仅部署在 FlexConfig 策略中选择的对象。

a) 点击目录中的 **FlexConfig 策略**。

b) 在组列表中点击 **+**。

c) 选择 Decrement_TTL 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

NTP 故障排除

系统靠时间准确一致来正常运行，并确保事件和其他数据点得到准确处理。您必须配置至少一个（最好是三个）网络时间协议 (NTP) 服务器来确保系统始终能获得可靠的时间信息。

设备摘要连接图（在主菜单中点击**设备 (Device)**）显示至 NTP 服务器的连接状态。如果状态为黄色或橙色，说明与配置的服务器存在连接问题。如果连接问题仍然存在（不仅仅是一个临时问题），请尝试以下操作。

- 首先，确保在**设备** > **系统设置** > **NTP** 上配置至少三个 NTP 服务器。尽管不要求配置至少三个 NTP 服务器，但这样做可以大大提高可靠性。
- 确保管理接口 IP 地址（在**设备** > **系统设置** > **管理接口**中定义）与 NTP 服务器之间存在网络路径。
  - 当管理接口网关是数据接口时，如果默认路由不充足，则可以在**设备** > **路由**上配置到 NTP 服务器的静态路由。
  - 如果设置了显式管理接口网关，请登录设备 CLI，并使用 **ping system** 命令测试与每个 NTP 服务器之间是否存在网络路径。
- 登录设备 CLI，并使用以下命令检查 NTP 服务器的状态。
  - **show ntp**- 此命令显示 NTP 服务器的基本信息及其可用性。但是， 设备管理器 中的连接状态使用其他信息指示其状态，所以此命令的显示以及连接状态图的显示可能存在不一致的地方。还可从 CLI 控制台发出此命令。
  - **system support ntp** - 此命令包括 **show ntp** 的输出以及标准 NTP 命令 **ntpq**（该命令记录在 NTP 协议中）的输出。如果需要确认 NTP 同步，请使用此命令。

    查找“Results of ‘ntpq -pn’ ”部分。例如，您可能会看到类似如下的内容：

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

    在本例中，NTP 服务器地址前的 + 表示作为潜在候选者。此处的星号 * 表示当前的时间源对等体。

    NTP 后台守护程序 (NTPD) 使用每个对等体中的八个示例的滑动窗口，并选出一个示例，然后根据时钟选择确定正确的报时器和错误的断续器。然后，NTPD 会确定往返距离（候补者的偏移不得超过往返延迟的一半）。如果连接延迟、丢包或服务器问题导致一个或全部候补者被拒绝，则同步中会出现较长的延迟。而且，该调整很长一段时间后才会完成：时钟偏移和振荡器错误必须通过时钟训练算法解决，这可能会需要数小时的时间。

注释 如果 refid 是 .LOCL.，则表明对等体是一个未经训练的本地时钟，也即它只使用其本地时钟来设置时间。如果所选的对等体是 .LOCL.，则 设备管理器 始终将 NTP 连接标为黄色（未同步）。如果还有更好的证书，NTP 通常不会选择 .LOCL. 证书，这就是应配置至少三个服务器的原因所在。

为管理接口排除 DNS 故障

必须配置至少一个DNS服务器供管理接口使用。需要使用该服务器来云连接到智能许可、数据库更新（如 GeoDB、规则和 VDB）等服务，和处理其他需要域名解析的任何活动。

配置 DNS 服务器非常简单。只需在初始配置设备时输入所用 DNS 服务器的 IP 地址。随后可在**设备 (Device)** > **系统设置 (System Settings)** > **DNS 服务器 (DNS Server)** 页面进行更改。

但是，由于网络连接问题或 DNS 服务器本身的问题，系统可能会无法解析完全限定域名 (FQDN)。如果您发现系统无法使用您的DNS服务器，请考虑以下操作来识别和解决问题。另请参阅常规DNS问题故障排除。

过程

步骤 1 确定是否存在问题。

a) 使用 SSH 登录设备 CLI。

b) 输入 **ping system www.cisco.com**。如果您获得类似于下文的“未知主机”消息，系统将无法解析域名。如果 ping 操作成功，问题得到解决：DNS 正常工作。（按 Ctrl+C 可停止 ping 命令。）

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

注释 务必在 **ping** 命令中添加 **system** 关键字。**system** 关键字通过管理 IP 地址执行 ping 操作，该接口也是使用管理 DNS 服务器的唯一接口。访问 www.cisco.com 也是一个不错的选择，因为您需要到该服务器的路由以获得智能许可和更新。

步骤 2 验证管理接口的配置。

a) 依次点击**设备 (Device)** > **系统设置 (System Settings)** > **管理接口 (Management Interface)**，并验证以下内容。如果您进行更改，点击**保存**后会立即应用所做的更改。如果您更改管理地址，需要重新连接并重新登录。

- 管理网络的网关IP地址是正确的。如果您使用数据接口作为网关，后续步骤将验证该配置。
- 如果您不使用数据接口作为网关，请验证管理 IP 地址/子网掩码和网关 IP 地址位于同一子网。

b) 依次点击**设备 (Device)** > **系统设置 (System Settings)** > **DNS 服务器 (DNS Server)**，并验证是否正确配置 DNS 服务器。

如果您在网络边缘部署设备，运营商可能会对您可以使用的 DNS 服务器提出特定要求。

c) 如果您使用数据接口作为网关，确认您具有所需的路由。

您需要为 0.0.0.0 提供默认路由。如果 DNS 服务器不能使用默认路由的网关，您可能需要额外的路由。这种情况基本分为两类：

- 如果您使用 DHCP 获取外部接口的地址且选择 **使用 DHCP 获取默认路由 (Obtain Default Route using DHCP)** 选项，默认路由在 设备管理器中不可见。从 SSH 输入 **show route** 验证是否存在适用于0.0.0.0的路由。由于这是外部接口的默认配置，您可能会遇到这样的情况。（请转至 **设备** > **接口** 查看外部接口的配置。）
- 如果您在外部接口上使用静态 IP 地址或不从 DHCP 获取默认路由，则打开**设备** > **路由**。验证已为默认路由使用正确的网关。

如果无法通过默认路由访问 DNS 服务器，则必须在**路由页**为其定义静态路由。请注意，不应为直连网络（即直接连接到系统任何数据接口的网络）添加路由，因为系统可以自动路由到这些网络。

此外，验证没有静态路由将发往服务器的流量错误引导至不正确的接口。

d) 如果部署按钮指示存在未部署的更改，请现在部署这些更改并等待部署完成。

e) 重新测试 **ping system www.cisco.com**。如果问题仍然存在，继续执行下一步。

步骤 3 在 SSH 会话中，输入 **dig www.cisco.com**。

- 如果 **dig** 指示可获取 DNS 服务器的响应，但服务器找不到名称，这意味着，DNS 已正确配置，但所用的 DNS 服务器没有适用于 FQDN 的地址。此错误由 NXDOMAIN 状态指示。响应应类似于以下内容：

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
```

```
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

解决方案：在这种情况下，您需要配置不同的DNS服务器，或获取已更新的服务器，使其能够解析需要解析的 FQDN。联系您的网络管理员或 ISP，获取可用于您网络的 DNS 服务器的 IP 地址。

- 如果命令超时，系统将无法访问 DNS 服务器，或所有 DNS 服务器目前均有故障，无法响应（不太可能出现这种情况）。继续进行下一步。

步骤 4 使用 **traceroute system** *DNS_server_ip_address* 命令追踪到 DNS 服务器的路由。

例如，如果 DNS 服务器为 10.100.10.1，请输入：

```
> traceroute system 10.100.10.1
```

下文是可能出现的结果：

- 跟踪路由完成并到达 DNS 服务器。在这种情况下，实际上存在通向 DNS 服务器的路由，且系统可以访问该服务器。因此，没有任何路由问题。但是，由于某种原因，到此服务器的DNS请求没有获得响应。

  解决方案：可能是因为沿该路径的路由器或防火墙丢弃 UDP/53 流量，这是用于 DNS 的端口。您可以沿其他网络路径尝试连接DNS服务器。这种问题比较棘手，因为您需要确定哪个节点阻止流量，并联系系统管理员才能更改访问规则。

- 跟踪路由连一个节点都无法访问，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
(and so forth)
```

  解决方案：在这种情况下，系统存在路由问题。尝试为网关IP地址执行 **ping system**。按照之前步骤中的介绍重新验证管理接口的配置，确保您已配置所需的网关和路由。

- 跟踪路由可以通过几个节点，之后便不再能够解析路由，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
 2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
 3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
 4  * * *
 5  * * *
 6  * * *
```

解决方案：这种情况下，路由在最后一个节点出现问题。您可能需要联系系统管理员，以在该节点安装正确的路由。但是，如果有意地在该节点不设置通往DNS服务器的路由，您需要更改网关，或创建自己的静态路由， 使其指向可以将流量路由到 DNS 服务器的路由器。

分析 CPU 和内存使用情况

要查看有关CPU和内存使用情况的系统级信息，请依次选择**监控**>**系统**，然后查找CPU和“内存”条形图。这些图表显示通过 CLI 使用 **show cpu system** 和 **show memory system** 命令收集的信息。

如果打开 CLI 控制台或登录 CLI，还可以使用这些命令的其他版本查看其他信息。通常，只有当使用情况存在长时间持续的问题时，或者奉思科技术支持中心 (TAC) 之命，才会查看此信息。其中许多详细信息比较复杂，需要 TAC 加以解释。

以下是您可以检查的一些要点。您可以在思科 Firepower 威胁防御命令参考（网址为 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）中找到有关这些命令的更多详细信息。

- **show cpu** 显示数据平面 CPU 使用情况。
- **show cpu core** 分别显示每个 CPU 核心的使用情况。
- **show cpu detailed** 显示其他每个核心及总数据平面的 CPU 使用情况。
- **show memory** 显示数据平面内存使用情况。

注释 某些关键字（上文未提及）需要先使用 **cpu** 或 **memory** 命令设置分析或其他功能。这些功能只能奉 TAC 之命使用。

查看日志

系统会记录各种操作的信息。您可以使用 **system support view-files** 命令打开系统日志。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

该命令将显示一个菜单供您选择日志。请使用以下命令在向导中导航：

- 要更改为子目录，请键入该目录的名称并按 Enter 键。
- 要选择欲查看的文件，请在提示符后输入**s**。然后系统将提示您输入文件名。请键入完整名称，并注意区分大小写。文件列表会显示日志的大小，您最好考虑一下再打开非常大的日志。
- 看到--More--时，按空格键可查看下一页日志条目；按Enter键仅查看下一个日志条目。到达日志末尾后，即会转到主菜单。--More-- 行会显示日志的大小和已查看部分的大小。**如果不想翻阅完整个日志，请使用 Ctrl+C 关闭日志并退出命令**。

- 键入 **b** 返回菜单结构的上一级。

如果要保持日志打开以便及时看到添加的新消息，请使用 **tail-logs** 命令而非 **system support view-files**。

以下示例显示如何查看 cisco/audit.log 文件，该文件用于跟踪系统登录尝试。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files-----------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files-----------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,
```

```
<remaining log truncated>
```

创建故障排除文件

在提交问题报告时，思科技术支持中心 (TAC) 人员可能要求您提交系统日志消息。这些信息可帮助他们诊断问题。您无需提交诊断文件，除非要求您这样做。

以下步骤程序介绍了如何创建和下载诊断文件。

过程

步骤 1 点击**设备**。

步骤 2 在**故障排除**下，点击**请求创建文件**或**重新请求创建文件**（如果您之前已创建一份文件）。

系统将开始生成诊断文件。您可以转至其他页面，再返回此处检查状态。当该文件准备就绪后，会显示文件创建日期和时间及下载按钮。

步骤 3 当该文件准备就绪后，请点击下载按钮。

系统将使用浏览器的标准下载方法，将该文件下载到您的工作站。

不常见的管理任务

以下主题介绍您即便执行，也不会经常执行的操作。所有这些操作都可能清除您的设备配置。在进行这些更改之前，请确保设备当前没有向生产网络提供重要服务。

更改防火墙模式

威胁防御 防火墙可在路由模式或透明模式下运行。路由模式防火墙是指路由的跳跃，可作为连接到任一屏蔽子网的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，其作用相当于“网络嵌入式”或“隐形防火墙”，不会被视为路由器跳跃至相连设备。

本地 设备管理器仅支持路由模式。不过，如果需要在透明模式下运行该设备，则可以更改防火墙模式，开始使用 管理中心管理设备。相反，您可以将透明模式设备转换为路由模式，然后选择使用本地管理器对其进行配置（也可以使用 管理中心管理路由模式设备）。

无论执行本地还是远程管理，都必须使用设备 CLI 更改模式。

以下步骤程序介绍了使用本地管理器或计划使用本地管理器时如何更改模式。

⚠

注意 更改防火墙模式会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

开始之前

如果要转换为透明模式，请先安装 管理中心 ，再更改防火墙模式。

如果启用了任何功能许可证，您必须首先在设备管理器中禁用它们，然后才能删除本地管理器和切换为远程管理。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅启用或禁用可选许可证。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或**configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与**管理 IP 地址**的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

连接到管理 IP 地址时，请务必执行此过程。使用 设备管理器时，您可以选择通过数据接口上的 IP 地址管理设备。但是，必须使用“管理”物理端口和管理 IP 地址来远程管理设备。

如果无法连接到管理 IP 地址，请解决以下问题：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。在 设备管理器中，在**设备** > **系统设置** > **管理接口**上配置地址和网关。（在 CLI 中，使用 **configure network ipv4/ipv6 manual** 命令。）

  注释 确保使用外部网关作为管理 IP 地址。使用远程管理器时，不能将数据接口用作网关。

步骤 2 要从路由模式更改为透明模式，并且使用远程管理：

a) 禁用本地管理，并进入无管理器模式。

若有活动管理器，则无法更改防火墙模式。使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 将防火墙模式更改为透明。

configure firewall transparent

示例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 配置远程管理器

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

其中：

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} 指定管理此设备的 管理中心 的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 管理中心注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在 管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此项为必填项。

例如，要在 192.168.0.123 处使用该管理器，注册密钥为 **secret**，请输入以下信息：

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

d) 登录 管理中心并添加设备。

有关详细信息，请参阅 管理中心在线帮助。

步骤 3 要从透明模式更改为路由模式并转换为本地管理，请执行以下操作：

a) 从 管理中心 注销设备。

b) 访问 威胁防御 设备 CLI，首选使用控制台端口。

由于更改模式会清除配置，管理 IP 地址将恢复为默认值，所以更改模式后，您可能会丢失与管理 IP 地址的 SSH 连接。

c) 将防火墙模式更改为路由。

configure firewall routed

示例：

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) 启用本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。

重置配置

如果要重新开始，您可以将系统配置重置为出厂默认设置。虽然无法直接重置配置，但删除和添加管理器可清除配置。

如果您计划擦除配置，然后恢复备份，请确保您已下载要恢复的备份副本。重置系统后，您需要上传备份副本，然后才能执行恢复。

开始之前

如果启用了任何功能许可证，必须首先在 设备管理器 中禁用它们，然后才能删除本地管理器。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅启用或禁用可选许可证。

如果设备已配置为高可用性，您必须首先使用 设备管理器（如果可能）或**configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

步骤 2 使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 3 配置本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。清除配置后，系统会提示您完成设备安装向导。

Cisco Secure Firewall 3100上的热插拔 SSD

如果您有两个SSD，它们会在您启动时形成RAID。防火墙启动时，您可以在CLI上执行以下任务：威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
```

```
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

configure raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

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。