



# Cisco Secure Network Analytics

更新指南 7.4.2



---

# 目录

简介 .....	5
概述 .....	5
受众 .....	5
术语 .....	5
新功能 .....	6
准备工作 .....	7
软件版本 .....	7
思科软件中心 .....	7
许可 .....	8
支持的硬件平台 .....	8
CIMC 固件版本 .....	8
应用版本兼容性 .....	9
Security Analytics and Logging( 本地部署) .....	9
报告构建器 .....	9
分析 .....	9
VMware 版本兼容性 .....	9
1. 查看 VMware 版本 .....	10
2. 查看 VMware 主机 .....	11
兼容的浏览器 .....	11
备用访问 .....	12
证书验证 .....	13
证书检查 .....	13
思科捆绑包 .....	13
服务器身份验证检查( 仅限 7.3.x 至 7.4.2) .....	14
审核日志目的地要求 .....	14
SMTP 配置要求 .....	14
Data Store .....	14
使用新的或现有的流收集器 .....	15
通过转换现有流收集器 .....	15
Data Store 专用 LAN 设置和数据节点扩展 .....	15
身份服务引擎 (ISE) 或 ISE-PIC .....	15

---

跨站点请求伪造 (CSRF) 保护(仅限 v7.3.0 和 v7.3.1)	16
磁盘空间	16
主机名	17
域名	17
NTP 服务器	17
时区	17
备份设备和数据库	17
7.4.0 及更早版本中的 sFlow 设备	18
<b>最佳更新时间</b>	<b>19</b>
软件更新文件	19
所有设备	19
SMC(管理器)和流量收集器。	19
通信	20
<b>更新流程概述</b>	<b>21</b>
<b>1. 查看您的集群</b>	<b>23</b>
<b>2. 下载补丁和更新文件</b>	<b>25</b>
1. 登录思科软件中心	25
2. 下载补丁	26
3. 下载更新文件	27
SWU 文件	28
<b>3. 备份设备配置</b>	<b>30</b>
<b>4. 创建诊断包</b>	<b>31</b>
在 v7.3.x 中创建诊断包	31
在 v7.4.x 中创建诊断包	32
<b>5. 备份 SMC(管理器)和流量收集器的数据库</b>	<b>33</b>
1. 整理流量收集器数据库	33
1. 审核数据库存储统计信息	33
2. 整理界面详细信息	34
3. 整理流详细信息和 CI 事件数据	35
2. 删除数据库快照	35
3. 备份远程文件系统	36
4. 删除数据库快照	38

---

---


<b>6. 备份 Data Store</b> .....	<b>39</b>
1. 估计备份主机存储要求 .....	39
2. 准备备份主机 .....	39
3. 为 dbadmin 启用无密码 SSH 访问 .....	40
4. 初始化备份主机上的备份目录: .....	41
5. 备份 Data Store 数据库 .....	43
Data Store 备份失败 .....	43
<b>7. 检查可用磁盘空间</b> .....	<b>45</b>
<b>8. 安装补丁</b> .....	<b>47</b>
1. 查看已安装版本 .....	47
2. 安装所需的补丁 .....	48
<b>9. 安装 v7.4.2 软件更新</b> .....	<b>51</b>
更新顺序 .....	52
安装软件更新 .....	54
1. 上传 7.4.2 SWU .....	54
2. 安装 7.4.2 SWU .....	55
故障排除 .....	57
<b>10. 配置高可用性</b> .....	<b>61</b>
主节点和辅助节点 .....	61
要求 .....	61
1. 配置主 UDP 导向器 高可用性 .....	62
2. 配置辅助 UDP 导向器 高可用性 .....	63
<b>11. 安装桌面客户端</b> .....	<b>64</b>
使用 Windows 安装 桌面客户端 .....	65
使用 macOS 安装桌面客户端 .....	67
<b>12. 验证管理器(原 SMC)故障转移角色</b> .....	<b>69</b>
联系支持人员 .....	71
更改历史记录 .....	72

# 简介

## 概述

使用本指南将以下 Cisco Secure Network Analytics(原 Stealthwatch) 设备从版本 **7.3.0**、**7.3.1**、**7.3.2**、**7.4.0**、**7.4.1** 更新至 **7.4.2**：

- UDP Director(也称为流量复制器)
- Data Store

 数据节点的更新程序在此更新中是唯一的。如果您部署了 Data Store, 请确保按照说明执行操作。

- 流量收集器
- 流传感器
- SMC(更新到 v7.4.x 后重命名为“管理器”)

在 v7.4.0 中, 我们将思科 Stealthwatch 企业产品更名为 Cisco Secure Network Analytics。有关完整列表, 请参阅[发行说明](#)。在本指南中, 您将看到我们以前的产品名称 Stealthwatch, 必要时使用 Stealthwatch 以及 Stealthwatch 管理控制台和 SMC 等术语。

## 受众

本指南的目标受众包括负责更新 Cisco Secure Network Analytics 产品的网络管理员及其他人员。

## 术语

本指南使用术语“设备”指代任何 Cisco Secure Network Analytics(原 Stealthwatch) 产品, 包括虚拟产品(如 Cisco Secure Network Analytics 流量传感器虚拟版 (VE))。

此外, “群集”是由 SMC 管理的一组设备(更新到 v7.4.x 后将其重命名为“管理器”)。如果设备由 SMC(管理器)管理, 它将显示在您的“集中管理”清单中。

 有关 Cisco Secure Network Analytics v7.4.2 的详细信息, 请参阅[发行说明](#)。

## 新功能

对于已经熟悉更新系统的人员，请确保您了解自上次升级以来的以下更改：

- 如果是从 v7.4.0 更新，则不再需要确保管理器或流量收集器的上次设备重新启动时间超过 1 小时但少于 7 天。但是，如果您从 v7.3.x 更新，则需要确保上次重新启动时间超过 1 小时但少于 7 天。
- 在开始更新过程之前，请确保系统中的所有设备都满足 1 个月 (30 天) 的[基准要求](#)。
- 在开始安装任何 SWU 文件之前，请确保上传所有 SWU 文件。
- 请确保根据您是从 v7.3.x 还是 v.7.4.x 升级，选择正确的 SWU 文件。v7.4.0 (及更高版本) 的 SWU 文件的文件名中将包含“v2”。请参阅 [SWU 文件表](#)，确认此更新所需的 v7.4.2 SWU 文件。
- 请注意，主管理器升级成功后，对于已成功升级的所有设备，设备管理器中的设备状态显示为**已连接**。有关详细信息，请参阅 [通信](#)。
- 在开始更新过程之前，请确保安装 [思科捆绑包](#) 补丁并更新您的 [CIMC 固件版本](#)。
- 在开始更新过程之前，请确保 ISE 证书链是完整的。有关详细信息，请参阅 [身份服务引擎 \(ISE\) 或 ISE-PIC](#)。
- [请勿](#) 卸载报告构建器应用。有关详细信息，请参阅 [报告构建器](#)。
- 从 v7.4.1 升级到 v7.4.2 时，您的分析数据不会结转。有关分析的更多详细信息，请参阅 [分析：检测、警报和观察结果](#)。
- 如果您有多个 UDP 导向器，请参阅 [10. 配置高可用性](#)。
- 作为 SMTP 配置和审核日志目的地更新的一部分，我们将运行 [服务器身份验证检查 \(仅限 7.3.x 至 7.4.2\)](#)。
- 将数据节点更新到 v7.4.1 时，无需在软件更新后在每个数据节点上安装补丁 SWU (像 v7.4.0 要求的那样)。
- 如果您的数据节点上安装了 v7.4.1，请按照说明使用 [更新全部数据节点](#) 按钮同时更新您的数据节点。在**所有**数据节点上成功安装更新 SWU 文件后，请确保在任何数据节点上重新启动 Vertica。

## 准备工作

在开始更新流程之前，请查看本指南以了解此流程，以及成功更新到 v7.4.2 所需的准备工作、时间和资源。

### 软件版本

要将设备软件更新到 v7.4.2，安装的设备版本必须为 **7.3.0**、**7.3.1**、**7.3.2**、**7.4.0** 或 **v7.4.1**。本指南中的说明将介绍如何检查每个设备上的软件版本。还需注意以下事项：

- **更新指南**：如果设备上未安装 **Stealthwatch v7.3.x**、**v7.4.0** 或 **v7.4.1**，请使用 [Cisco.com](https://www.cisco.com) 上的更新指南逐步更新您的系统。例如，如果安装了 **Stealthwatch v7.1.x**，请确保将每个设备从 **v7.1.x** 更新到 **v7.2.1**，然后将 **v7.2.1** 更新到 **v7.3.x**，以此类推。
- **基准**：在开始此更新之前，请确保您的设备已在相同版本的 **v7.3.0**、**v7.3.1**、**v7.3.2**、**v7.4.0** 或 **v7.4.1** 上运行超过 1 个月 (30 天)。如果您在短时间内将系统更新为多个版本，则系统基准可能会受到影响。要获取帮助，请联系 [思科支持](#)。
- **补丁**：作为更新过程的一部分，请确保在设备上安装所需的累积补丁。

 在每台设备上安装每个必需的修补程序最多可能需要 90 分钟。

- **降级**：由于需要在数据结构和配置中进行更新更改，才能支持在更新期间安装的新功能，因此不支持版本降级。
- **TLS**：Cisco Secure Network Analytics 要求安装 TLS v1.2。
- **第三方应用**：Cisco Secure Network Analytics 不支持在设备上安装第三方应用。

### 思科软件中心

要针对 Cisco Secure Network Analytics v7.4.2 管理许可证、下载补丁和下载更新文件，请在 <https://software.cisco.com> 上登录您的思科智能帐户或与管理员联系。



## 许可

开始更新之前，请确保您的设备许可证是最新的。

- **检查:** 登录 SMC( 管理器)，然后选择**全局设置 (Global Settings)** 图标 > **集中管理 (Central Management)** > **智能许可 (Smart Licensing)**。查看**智能许可使用情况 (Smart License Usage)** 部分。
- **说明:** 如果任何许可证显示为“不合规”(Out of Compliance) 或“已过期”(Expired)，请参阅 [智能软件许可指南](#)。

## 支持的硬件平台

要查看每个系统版本的支持硬件平台，请参阅[硬件和版本支持表](#)。

## CIMC 固件版本

对于下表中所示的设备，M4 通用更新过程适用于 UCS C 系列 M4 硬件，M5 通用更新补丁适用于 M5 硬件。

 请勿使用 Cisco.com 上发布的标准 UCS 固件更新信息。


M4 硬件	M5 硬件
SMC 2200( 管理器 2200)	SMC 2210( 管理器 2210)
FC 4200	FC 4210
FC 5020 引擎	—
FC 5020 数据库	—
FC 5200 引擎	FC 5210 引擎
FC 5200 数据库	FC 5210 数据库
FS 1200	FS 1210
FS 2200	—
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210



遵循 [2. 下载补丁](#) 说明;但对于步骤 3, 请选择“所有版本”列中的**固件**, 以访问最新的 CIMC 固件版本通用更新补丁。

请访问 [cisco.com](http://cisco.com) 上的“[版本说明](#)”页面上的[通用补丁自述文件](#), 然后找到适用的自述文件以了解更多详细信息。

## 应用版本兼容性

 如果您以前安装过应用, 请确保它们与您将要安装的 Cisco Secure Network Analytics 版本兼容。

要了解如何确认已安装的应用列表并查看最新的 Cisco Secure Network Analytics 应用兼容性信息, 请参阅 [Cisco Secure Network Analytics 应用版本兼容性表](#)。

## Security Analytics and Logging(本地部署)


报告构建器

成功升级到 Cisco Secure Network Analytics v7.4.2 后, 请确保将 Security Analytics and Logging(本地) 升级到 v3.2.0。有关 Security Analytics and Logging(本地) 部署的详细信息, 请参阅以下文档:

- [安全分析和日志记录\(本地部署\)发行说明](#)
- [思科安全分析和日志记录\(本地部署\)入门](#)
- [安全分析和日志记录\(本地部署\): Firepower 事件集成指南](#)

## 报告构建器

在 v7.4.0 中, 我们将报告构建器从单独的应用移到了核心系统。如果您将 Cisco Secure Network Analytics 从 v7.3.x 更新到 v7.4.2, 您的应用将作为此更新的一部分被自动删除。

 请勿卸载现有的报告构建器应用。如果卸载报告构建器, 与之相关的所有文件(包括保存的报告和临时文件)都会被删除。

## 分析

从 v7.4.1 升级到 v7.4.2 时, 您的分析数据不会结转。有关分析的更多详细信息, 请参阅 [分析:检测、警报和观察结果](#)。

## VMware 版本兼容性

Cisco Secure Network Analytics v7.4.2 与 VMware v7.0 和 v8.0 兼容。Cisco Secure Network Analytics v7.4.x 不支持 VMware v6.0、v6.5 或 v6.7。有关详细信息, 请参阅 vSphere 6.0、6.5 和 6.7 一般支持终止的 VMware 文档。

- **更新前:**如果 Cisco Secure Network Analytics 设备安装在 VMware v6.0、v6.5 或 v6.7 上, 请先将 VMware vCenter 和 ESXi 主机升级到 v7.0 或 v8.0, 然后再将 Cisco Secure Network Analytics 升级到 v7.4.x。

- **检查:** 请参阅 [1. 查看 VMware 版本](#) 和 [2. 查看 VMware 主机](#) 以查看您的 VMware 环境。
- **更新后:** Cisco Secure Network Analytics v7.4.x 更新后, VMware 中可能显示操作系统错误。查看 VMware GUI 并确认您的 VMware vCenter 为 v7.0 或 v8.0, 并且操作系统为 Debian v10。要升级 VMware vCenter 或操作系统, 请参阅您的 VMware 指南。
- **实时迁移:** (例如, 使用 vMotion) 不支持主机间的实时迁移。
- **快照:** 不支持虚拟机快照。

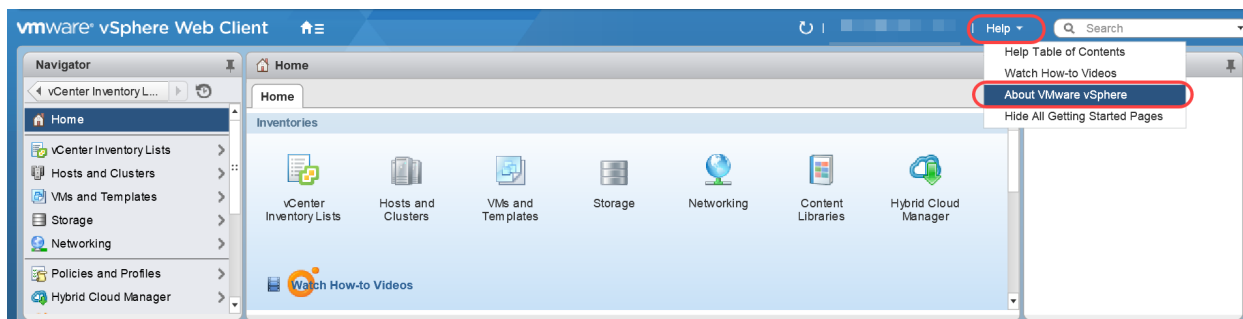
**⚠** 请勿在 Cisco Secure Network Analytics 虚拟设备上安装 VMware 工具, 因为它将覆盖已安装的自定义版本。这样做会使虚拟设备无法操作, 需要重新安装。

## 1. 查看 VMware 版本

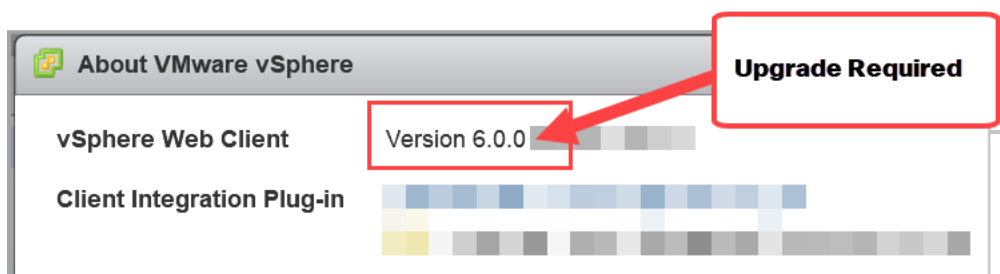
使用以下说明确认 VMware vSphere vCenter 已安装 v7.0 或 v8.0。

**i** VMware UI 中的菜单和图形可能与您在此处看到的不同。有关特定于您的环境的详细信息, 请参阅 VMware 指南。

1. 登录 VMware Web 客户端。
2. 在主页上, 选择 **vCenter 清单列表**。
3. 选择 **帮助 > 关于 VMware vSphere**。



4. 查看 **Web 客户端** 版本。如果是 v6.0、v6.5 或 v6.7, 需要将其升级至 v7.0 或 v8.0。有关说明, 请参阅您的 VMware 指南。



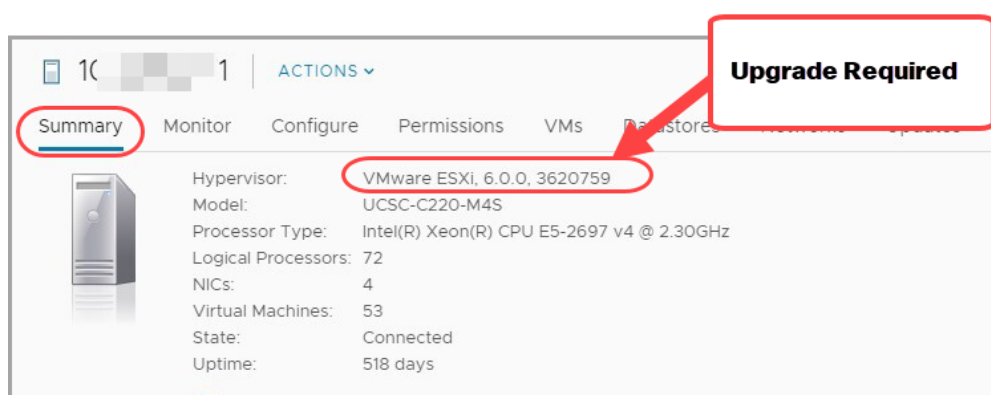
5. 继续下一部分。

## 2. 查看 VMware 主机

使用以下说明查看 ESXi 主机并确认其已安装 v7.0 或 v8.0。如果您的 Cisco Secure Network Analytics 设备安装在多个主机上，请确保选中每个主机。

**i** VMware UI 中的一些菜单和图形与此处所示信息会有所不同。有关此软件的详细信息，请参阅您的 VMware 指南。

1. 在“导航”窗格中，选择 **vCenter 清单列表**。
2. 选择**主机**。
3. 点击主机名。
4. 点击**摘要 (Summary)** 选项卡。




5. 查看**虚拟机监控程序**版本。如果是 v6.0、v6.5 或 v6.7，需要将其升级至 v7.0 或 v8.0。有关说明，请参阅您的 VMware 指南。
6. 在安装有 Cisco Secure Network Analytics 设备的任何其他主机上重复步骤 1 至 5。

## 兼容的浏览器

- **兼容浏览器**：Cisco Secure Network Analytics 支持最新快速版本的 Chrome、Firefox 和 Microsoft Edge。
- **Microsoft Edge**：Microsoft Edge 可能存在文件大小限制。不建议使用 Microsoft Edge 来上传软件更新文件 (SWU)。
- **快捷方式**：如果您使用浏览器快捷方式访问任何 Cisco Secure Network Analytics 设备的“设备管理”(Appliance Admin) 界面，则在更新流程完成后，这些快捷方式可能不起作用。在这种情况下，请删除快捷方式并重建。
- **证书**：某些浏览器更改了设备身份证书的到期日期要求。如果您无法访问设备，请参阅 [《托管设备的 SSL/TLS 证书指南》](#) 以替换证书或联系 [思科支持](#)。

## 备用访问

 启用替代方法来访问您的 **Cisco Secure Network Analytics** 设备以满足未来的任何服务需求，这一点非常重要。

确保您可以使用以下选项之一访问 **Cisco Secure Network Analytics** 设备：

### 虚拟设备 - 控制台(与控制台端口的串行连接)

要通过 **KVM** 访问设备，请参阅虚拟管理器文档；要通过 **VMware** 连接到设备，请参阅 **vSphere** 的 **vCenter** 服务器设备管理接口文档。

### 硬件 - 控制台(与控制台端口的串行连接)

要使用笔记本电脑或带显示器的键盘连接到设备，请参阅 [《安装和升级指南》](#)页面上列出的最新 [《Cisco Secure Network Analytics硬件安装指南》](#)。


### 硬件 - CIMC(UCS 设备)

要通过 **CIMC** 访问设备，请参阅 [《思科集成管理控制器 \(CIMC\) 配置指南》](#)页面上列出的适用于您的平台的最新指南。

### 其他方法

请按照以下说明启用备用方法，以根据任何将来服务需求访问您的 **Cisco Secure Network Analytics** 设备。

如果无法使用虚拟或硬件方法登录设备，可以在设备网络接口上临时启用 **SSH**。

 您需要确保在断电后升级或启动数据库之前，在所有数据节点上启用 **SSH**(方法是选择“启用 **SSH**”(Enable **SSH**) 选项)。启用 **SSH** 后，系统受攻击的风险会增加。务必只在必要时才启用 **SSH**。用完 **SSH** 后，请将其禁用。

按照以下说明打开并启用所选设备的 **SSH**。

1. 打开**集中管理 > 设备管理器**。
2. 点击设备的**操作菜单**。
3. 选择**编辑设备配置**。
4. 选择**设备选项卡**。
5. 找到**SSH** 部分。
6. 选择是仅启用 **SSH** 访问还是同时启用根访问。
  - **启用 SSH**:要在设备上允许 **SSH** 访问，请选中此复选框。
  - **启用根 SSH 访问**:要在设备上允许根访问，请选中此复选框。
7. 点击**应用设置 (Apply Settings)**。
8. 按照屏幕上的提示保存更改。

 请确保在用完后禁用 SSH。

## 证书验证

在开始更新流程之前，请确认设备身份证书有效且为最新。我们无法更新设备身份证书无效或过期的设备。要替换设备身份证书，请按照 [《托管设备的 SSL/TLS 证书指南》](#) (v7.3 或 v7.4) 中的说明进行操作。


设备身份要求	
格式	PEM( .cer、.crt、.pem) 或 PKCS#12( .p12、.pfx、.pks)
RSA 密钥长度	4096 位或 8192 位
公共名称或 Subject Alternative Name	确认公用名和/或使用备用名称与 FQDN 匹配。
身份验证	设备身份证书需要服务器和客户端身份验证。

在将设备更新到 v7.4.2 后，可以将系统证书替换为使用 ECDSA 密钥的自定义证书。有关详细信息，请参阅 [发行说明 v7.4.2](#)。

## 证书检查

如果是从 v7.3.0 更新，那么更新到 v7.3.1、v7.3.2 和 v7.4.x 将进行证书检查，以验证思科捆绑包不会导致您的环境出现问题。

如果使用证书，请确保集中管理信任存储中存在完整的证书链(作为单独的文件)。如果信任存储区中只有最终实体证书，则升级将失败。

 如果您没有将完整的证书链添加到集中管理器信任存储区，则从 Cisco Secure Network Analytics v7.3.0 更新将失败。如果从 v7.3.1 或 v7.3.2 升级，则此检查不适用。

## 思科捆绑包

请确保安装了最新的思科捆绑包通用更新补丁。有关详细信息，请参阅 [思科捆绑包通用更新补丁](#) 的自述文件。补丁：

- 提供选定数量的根证书颁发机构 (CA) 的预验证数字证书捆绑包，并且它
- 包括一个核心证书捆绑包以及一个外部证书捆绑包，分别用于连接到思科服务和非思科服务。

遵循 [2. 下载补丁](#) 说明；但对于步骤 3，请选择“最新版本”列中的 **证书捆绑包** 以访问最新的思科捆绑包通用更新补丁。

## 服务器身份验证检查(仅限 7.3.x 至 7.4.2)

作为从 7.3.x 更新到 7.4.2 的一部分,我们将检查以下配置,以确认它们符合服务器身份验证的要求:

- 审核日志目标(使用 TLS 的系统日志)
- SMTP 配置(响应管理的邮件通知)

在开始更新之前,请检查您的配置。如果配置不符合要求,更新将会失败。

### 审核日志目的地要求

请确保您的审核日志目标配置同时满足以下两个要求:

- 确认设备信任存储区中包含来自支持 Syslog over TLS 的系统日志服务器的根证书颁发机构 (CA) SSL 证书。检查配置了审核日志目的地的每个设备信任存储区。
- 此外,如果您的 syslog 服务器身份证书在“主题”(Subject)或“主题替代名称”(Subject Alternative Name)字段中未包含 syslog 服务器 IP 地址,请将其添加到配置了审计日志目的地的每个设备信任存储区中。

要访问信任存储区,请登录 SMC(管理器)。选择全局设置图标 > 集中管理。点击设备的 ⋮ (省略号) 图标。选择编辑设备配置 (Edit Appliance Configuration)。选择常规 (General) 选项卡,然后滚动到信任存储区 (Trust Store) 部分。有关详细信息,请参阅 [《托管设备的 SSL/TLS 证书指南》\(v7.3 或 v7.4\)](#)。

### SMTP 配置要求

使用以下选项之一进行服务器身份验证:

- 确认您的证书颁发机构 (CA) 中的 SMTP 服务器身份证书具有与您已配置的 IP 地址或主机名匹配的主体或主体备用名称,或
- 将 SMTP 服务器身份证书添加到“信任存储区”。

要访问信任存储区,请登录 SMC(管理器),然后选择全局设置 (Global Settings) 图标 > 集中管理 (Central Management)。点击 SMC(管理器)的 ⋮ (省略号) 图标。选择编辑设备配置 (Edit Appliance Configuration)。选择常规 (General) 选项卡,然后滚动到信任存储区 (Trust Store) 部分。有关详细信息,请参阅 [《托管设备的 SSL/TLS 证书指南》\(v7.3 或 v7.4\)](#)。


## Data Store

如果您的部署中有 Data Store,请确保在所有数据节点上启用 SSH,然后再开始更新。

- 启用 SSH:按照 [备用访问](#) 中的步骤在所有数据节点上启用 SSH,并确保选中启用 SSH (Enable SSH) 复选框,而不是启用根 SSH 访问选项。
- 禁用 SSH:如果要在数据节点上禁用 SSH,则可以在完成升级过程和安装补丁后为每个数据节点禁用 SSH。



- **更新全部数据节点 v7.4.1:** 如果您已安装 v7.4.1, 请按照说明使用 **更新全部数据节点** 按钮同时更新您的数据节点。您将使用用于安装补丁和 SWU 文件的按钮。您可能需要在安装补丁后启动 Data Store 数据库, 但在所有数据节点上成功安装更新 SWU 后, 数据库将自动启动。
- **停机时间:** 如果您担心此更新所需的停机时间, 请联系 [思科支持](#)。

 将数据节点更新到 v.7.4.1 或 v7.4.2 时, 无需在软件更新后在每个数据节点上安装补丁 SWU(像 v7.4.0 要求的那样)。

## 使用新的或现有的流收集器

扩展到 Data Store 环境

更新到 v7.4.1(或更高版本)后, 您可以使用现有的流收集器通过或添加新的流量收集器, 然后添加数据节点来扩展 Cisco Secure Network Analytics 非 Data Store 环境。有关详细信息, 请参阅 [版本说明](#) 和 [系统配置指南](#) 中的说明。要了解安全网络分析数据存储的工作原理, 请查看 [Data Store 解决方案概述](#)。

## 通过转换现有流收集器

扩展到 Data Store 环境

更新到 v7.4.2 后, 您可以通过添加数据节点并将现有流收集器转换为 Data Store 来扩展 Cisco Secure Network Analytics 非 Data Store 环境。有关详细信息, 请参阅 [版本说明](#) 和 [系统配置指南](#) 中的说明。要了解安全网络分析数据存储的工作原理, 请查看 [Data Store 解决方案概述](#)。

## Data Store 专用 LAN 设置和数据节点扩展


从 v7.4.1 开始, Cisco Secure Network Analytics 将对专用 LAN IP 地址实施特定要求。确保使用专用 LAN IP 地址配置的任何数据节点满足以下要求:

- 前三个八位组必须为 **169.254.42**
- 子网必须为 **/24**

 例如: 169.254.42.x/24, 其中 x 表示您的站点分配的数字(2 到 255)。

有关详细信息, 请联系 [思科支持](#)。

## 身份服务引擎 (ISE) 或 ISE-PIC

 在更新到 v7.4.2 之前, 请确保 ISE 中的证书链是完整的。有关详细信息, 请参阅从 [Cisco Secure Network Analytics ISE 和 ISE-PIC 配置指南 7.4](#) 的第 5 页开始的“选项 1 - 使用 ISE 内部证书颁发机构部署证书(推荐)”部分。此外, 请确保通过执行手动同步来更正 ISE 中的任何复制警报问题。有关其他信息: 请参阅 [版本说明](#) 的“已知问题”部分中列出的相关 ISE 集成问题。



- **要求:**如果您的 SMC(管理器)使用 ISE 或 ISE-PIC,请在开始更新之前,确保客户端组包含自适应网络控制(ANC)。
- **检查:**登录 ISE 客户端。选择**管理 > pxGrid 服务**。查看 SMC(管理器) > **客户端组 (Client Group)** 列,并选中列表中的每个 SMC(管理器)。如果未显示思科自适应网络控制(ANC),请选中 SMC(管理器)复选框以将其选中。点击**组 (Group)**将 ANC 添加到组字段,然后点击**保存 (Save)**。

**i** 默认情况下,ANC 将处于禁用状态,只有在启用 pxGrid 后才能启用。要在启用后禁用 ANC,请确保通过管理员门户手动禁用该服务。

- **指南:**有关详细信息,请参阅 [Cisco Secure Network Analytics ISE 和 ISE-PIC 配置指南 7.4](#)和 [思科身份服务引擎管理员指南,版本 2.2](#)。有关 ISE 的其他产品信息,请转至[思科身份服务引擎](#)页面。

## 跨站点请求伪造 (CSRF) 保护 (仅限 v7.3.0 和 v7.3.1)

如果您要将系统从 v7.3.0 或 v7.3.1 更新到 v7.4.2,请确保遵循本节中的步骤。如果您是从 v7.3.2、v7.4.0 或 v7.4.1 至 v7.4.2 更新,则可以跳过此部分。

为了帮助确保针对 CSRF 攻击提供更多保护,系统要求 HTTPS 客户端提交 CSRF 令牌作为其状态更改 HTTPS 请求的一部分。CSRF 标记是会话专用的,将在身份验证过程中通过名为“XSRF-TOKEN”的 Cookie 返回。HTTPS 客户端在发出 HTTPS 请求时,必须将 HTTPS 标头“X-XSRF-TOKEN”设置为该 Cookie 的值。作为此附加保护的一部分,您的身份验证 API 脚本可能会因 HTTP 401 错误而失败。

更新 API 脚本的步骤可能会因环境而异。在将群集从 v7.3.0 或 v7.3.1 升级到 v7.4.2 之前,请确保已对 API 脚本进行了以下更改:

1. 当 HTTPS 客户端进行身份验证时,将返回的 CSRF 标记存储在 XSRF-TOKEN Cookie 中。
2. 在所有 HTTPS 请求中(“GET”除外),脚本都需要通过名为“X-XSRF-TOKEN”的 HTTP 标头返回该存储值。
3. 每当脚本重新进行身份验证时,都需要更新 CSRF 令牌的存储值。

**i** 如果您需要在更新 API 脚本之前更新集群,请联系[思科支持](#)。

## 磁盘空间

在更新准备中,您将确认每个设备上拥有足够的可用磁盘空间来安装补丁和软件更新文件。请参阅 [7. 检查可用磁盘空间](#),了解详细信息。

- **要求:**在每个托管设备上,可用空间应至少是单个软件更新文件(SWU)大小的 4 倍。在 SMC(管理器)上,可用空间应至少是您上传到更新管理器的所有设备 SWU 文件大小的 4 倍。
- **托管设备:**例如,如果流收集器 SWU 文件为 6 GB,则流收集器(/lancope/var)分区上至少需要 24 GB 可用空间(1 SWU 文件 x 6 GB x 4 = 24 GB 可用空间)。

- **SMC(管理器)**:例如,如果要上传 4 个 SWU 文件,而每个文件为 6 GB,则 /lancope/var 分区上至少应有 96 GB 可用空间(4 个 SWU 文件 x 6 GB x 4 = 96 GB 可用空间)。

## 主机名

- **要求**:每个设备都需要有唯一主机名。我们无法更新与其他设备具有相同主机名的设备。此外,请确保每个设备主机名符合对互联网主机的互联网标准要求。
- **检查**:登录 SMC(管理器),然后选择**全局设置 (Global Settings)** 图标 > **集中管理 (Central Management)**。检查每个设备的“主机名”列。


## 域名

- **要求**:每个设备都需要有完全限定域名。我们无法更新具有空域的设备。
- **检查**:登录 SMC(管理器),然后选择**全局设置 (Global Settings)** 图标 > **集中管理 (Central Management)**。在设备的**操作 (Actions)** 列中,点击 **⋮ (省略号)** 图标。选择**编辑设备配置**。在“设备”选项卡上,查看**主机命名**。

## NTP 服务器

- **要求**:每个设备至少需要 1 台 NTP 服务器。
- **检查**:登录 SMC(管理器),然后选择**全局设置 (Global Settings)** 图标 > **集中管理 (Central Management)**。在设备的**操作 (Actions)** 列中,点击 **⋮ (省略号)** 图标。选择**编辑设备配置**。在“网络服务”选项卡上,查看**NTP 服务器**。
- **问题 NTP**:如果服务器列表中具有 130.126.24.53 NTP 服务器,请将其删除。此服务器已知存在问题,在默认 NTP 服务器列表中不再受支持。

## 时区


 确保虚拟主机服务器(已安装虚拟设备)上的时间设置已设为正确时间。否则,设备可能无法启动。

所有设备均使用协调世界时 (UTC)。

- **要求**:开始更新之前,请确保您的设备已设置为 UTC。
- **虚拟主机服务器**:请确保您的虚拟主机服务器设置为正确的 UTC 时间。

## 备份设备和数据库

请确保计划时间来备份系统。如果更新存在问题,您将需要备份文件,并且在通过[思科支持](#)进行故障排除时,诊断包非常重要。

 如果没有备份,则在更新流程中出现问题时,您将无法恢复文件。此外,如果您需要通过联系[思科支持](#)进行故障排除,诊断包会非常重要。

本指南提供有关以下操作的说明:

- 备份每个设备
- 创建诊断包
- 备份 SMC(管理器) 数据库
- 备份流量收集器数据库
- 备份 Data Store

作为备份程序的一部分,您将在备份每个数据库之前和之后删除 SMC(管理器)和流量收集器上的数据库快照。此外,备份流量收集器的程序还包括整理数据库。

请参阅 [5. 备份 SMC\(管理器\)和流量收集器的数据库](#),了解详细信息。



如果您部署了 Data Store,请备份 Data Store 数据库,而不是流收集器数据库。请参阅 [6. 备份 Data Store](#),了解详细信息。

## 7.4.0 及更早版本中的 sFlow 设备

从 7.4.0 版本开始,sFlow 将不再作为单独的 ISO 映像发布。您可以将流收集器 NetFlow 切换到 sFlow。有关详细信息,请参阅联机帮助中的“高级设置”主题。

# 最佳更新时间

在计划时间和资源以更新设备时，请考虑以下几点。

## 软件更新文件

下载补丁和软件更新文件需要一些时间。您可以提前下载。请参阅 [2. 下载补丁和更新文件](#)，了解更多信息。

## 所有设备

- **时间**: 在每台设备上安装此更新的修补程序最多可能需要 **90 分钟**。每个设备的软件更新流程大约需要 **30 分钟** 完成，但根据您的网络可能需要更长时间。这些估计时间不包括创建备份和诊断包所需的时间，这也会根据您的环境而有所不同。
- **流量低**: 如果系统流量相对较低，建议您同时更新整个系统。
- **重新启动**: 设备在重新启动流程中不会收集数据。不过，将保留当前数据。

## SMC(管理器) 和流量收集器。

- **上次重新启动/活动**: 如果要从 **v7.3.x** 升级，请确保在开始更新过程之前，**SMC(管理器)** 和流量收集器已运行 **超过 1 小时以上但不到 7 天**。如果没有，**SWU** 文件将因迁移安全切换而无法安装。此重新启动要求不适用于安装补丁。
- **流量收集器**: 在流量收集器更新并运行后，它将缓存要发送到 **SMC(管理器)** 的数据，直至它被更新。不过，您不会希望此过程运行很长时间。准备所有设备以便同时更新，这是最成功的方法。



请勿从“集中管理”中删除任何流量收集器。这样会导致 **SMC(管理器)** 丢失这些流量收集器的所有历史数据。

## 通信

在更新流程中,当设备更新和重新启动时,SMC(管理器)与设备之间的通信将停止。

在“集中管理”清单中,设备状态将更改为**配置通道关闭**。更新完成后,将重新建立通信,并且设备状态将恢复为**运行(v7.3.x和v7.4.0)**或**已连接(v7.4.1和v7.4.2)**。请参阅 [9. 安装 v7.4.2 软件更新](#),了解详细信息。



在更新集群中的下一个设备之前,请确保设备状态显示为**运行(v7.3.x和v7.4.0)**或**已连接(v7.4.1)**。

# 更新流程概述



确保遵循补丁和 SWU 文件的软件安装顺序。要成功更新, 请务必遵循本指南中的步骤。

要确保成功更新并最大程度减少数据丢失, 请确保按顺序遵循以下说明。

1. 查看您的集群
2. 下载补丁和更新文件
3. 备份设备配置
4. 创建诊断包
5. 备份 SMC(管理器)和流量收集器的数据库
6. 备份 Data Store
7. 检查可用磁盘空间
8. 安装补丁
9. 安装 v7.4.2 软件更新
10. 配置高可用性
11. 安装桌面客户端
12. 验证管理器(原 SMC)故障转移角色






# 1. 查看您的集群

**!** 确保每个设备已安装正确的软件版本。此步骤对于成功更新非常重要。







请务必查看群集，确认每个设备的软件版本。要验证每个设备的当前软件版本是 **7.3.0**、**7.3.1**、**7.3.2**、**7.4.0** 或 **7.4.1**，请完成以下步骤：

1. 以管理员身份登录 SMC(管理器)。

<https://<SMC IP 地址>>

2. 点击  (全局设置) 图标。
3. 选择**集中管理**。
4. 选择**更新管理器**选项卡，然后找到**系统更新**部分。
5. 查看**已安装版本 (Installed Version)**列，确认每个设备在所有设备上安装的 **7.3.x** 版本相同。

**相同版本:** 确保所有设备都使用相同的 **7.3.x** 软件版本。例如，如果您的 SMC 安装了 **7.3.2**，则群集中的其他设备必须安装 **7.3.2**。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc01-10-200-00-9	10.200.00.9	2 hours ago	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
SMC	smc02-10-200-00-10	10.200.00.10	2 hours ago	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
Flow Collector	fcnf-10-200-00-11	10.200.00.11	2 hours ago	7.3.2 patch-fcnf- ROLLUP005-7.3.2-01	-		
Flow Collector	fcnf-10-200-00-12	10.200.00.12	2 hours ago	7.3.2 patch-fcnf- ROLLUP004-7.3.2-01	-		
UDP Director	udp01-10-200-00-13	10.200.00.13	19 hours ago	7.3.2 20210409.0329-58b668961ea	-		
Flow Sensor	fs-10-200-00-14	10.200.00.14	a month ago	7.3.2 20210409.0329-58b668961ea	-		

**!** 开始更新流程后，请勿添加或删除设备、更改集群配置、在设备上更改配置设置或更改设备故障转移角色。



## 2. 下载补丁和更新文件

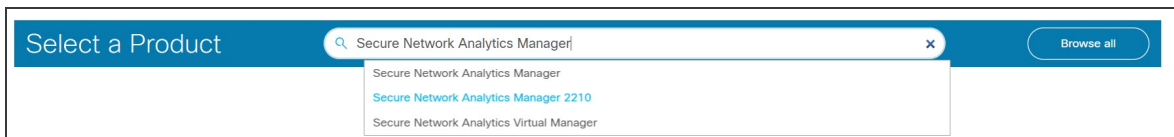
要管理许可证、下载补丁和下载更新文件，请在 <https://software.cisco.com> 登录您的思科智能帐户。

请使用以下说明下载帐户中列出的补丁和 v7.4.2 SWU。

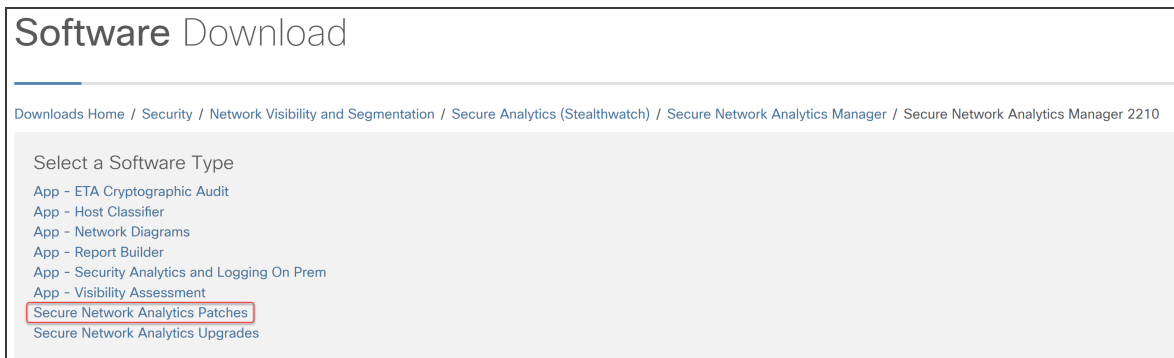
### 1. 登录思科软件中心

1. 登录思科软件中心 <https://software.cisco.com>。
2. 在**下载和管理 (Download and Upgrade)** 部分中，选择**访问下载**。
3. 在**选择产品 (Select a Product)** 字段中键入 **Cisco Secure Network Analytics**，然后选择设备。

您还可以在键入产品名称时包括设备，如下例所示：



4. 当显示“软件下载”(Software Download) 页面时，
  - 选择 **Cisco Secure Network Analytics 补丁 (Secure Network Analytics Patches)**，在开始更新过程之前访问您需要应用的任何补丁文件



- 或选择 **Cisco Secure Network Analytics 升级 (Secure Network Analytics**

## Upgrades) 以访问更新文件

## Software Download

Downloads Home / Security / Network Visibility and Segmentation / Secure Analytics (Stealthwatch) / Secure Network Analytics Manager / Secure Network Analytics Manager 2210

Select a Software Type

- App - ETA Cryptographic Audit
- App - Host Classifier
- App - Network Diagrams
- App - Report Builder
- App - Security Analytics and Logging On Prem
- App - Visibility Assessment
- Secure Network Analytics Patches
- Secure Network Analytics Upgrades

## 2. 下载补丁

i 选择 **Cisco Secure Network Analytics 补丁 (Secure Network Analytics Patches)**，以便在开始更新过程之前访问您需要应用的任何补丁。有关详细信息，请参阅 [补丁自述文件](#)。

选择 **Cisco Secure Network Analytics 补丁 (Secure Network Analytics Patches)** 后，系统将显示设备页面。

1. 选择设备上当前安装的 **Cisco Secure Network Analytics** 版本。例如，如果您的设备已安装 **7.4.1**，请选择 **7.4.1**。

## Software Download

Downloads Home / Security / Network Visibility and Segmentation / Secure Analytics (Stealthwatch) / Secure Network Analytics Manager / Secure Network Analytics Manager 2210 / Secure Network Analytics Patches- 7.4.1

Search...

Expand All Collapse All

Latest Release

- 7.4.1
- Certificate Bundles
- 7.3.2
- 7.1.3

All Release

- Certificate Bundles
- Firmware

### Secure Network Analytics Manager 2210

Release 7.4.1

My Notifications

Related Links and Documentation

- No related links or documentation -

File Information	Release Date	Size	
7.4.1-PATCH SMC Rollup #7 patch-smc-ROLLUP007-7.4.1-v2-01.swu	07-Feb-2023	4665.39 MB	<a href="#">↓</a> <a href="#">🛒</a>

## 2. 下载: 点击下载图标或添加到购物车图标。

下载所选设备的所有补丁。

**i** 确保下载当前版本的所有补丁, 包括每个设备的最新累积补丁, 以及所需的通用更新补丁、CIMC 固件更新补丁和思科捆绑补丁。

## 3. 重复执行[这些说明](#)以对集群中的每个设备下载所有补丁。请参阅 [SWU 文件表](#), 确认您已下载此更新所需的所有文件。

## 3. 下载更新文件

**i** 要访问特定版本的所有文件, 最有效的方法是先选择 **SMC(管理器)**。

选择 **Stealthwatch 升级 (Stealthwatch Upgrades)** 后, 系统将显示设备页面。

### 1. 选择 **7.4.2**。

### 2. 下载: 点击下载图标或添加到购物车图标。

- **所选设备:** 下载针对设备显示的更新文件。
- **相关软件:** 使用“相关软件”(Related Software) 部分下载所有其他设备的更新文件。如果此部分显示了任何补丁, 您需在更新后安装它们。

### 3. 请参阅 [SWU 文件表](#), 确认您已下载此更新所需的所有文件。如果缺少任何更新文件, 请重复执行[这些说明](#)以下载其他设备的更新文件。

## SWU 文件

确认已下载此更新所需的所有文件。如果缺少任何文件，请参阅 [2. 下载补丁和更新文件](#)。

设备	从 v7.3.0、v7.3.1 或 v7.3.2 更新 软件更新 文件名	从 v7.4.0 或 v7.4.1 更新 软件更新 文件名
UDP 导向器 (也称为流量复制器) UDP 导向器 VE (也称为流量复制器 VE)	update-udp- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-udp- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
数据节点	update-dnode- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-dnode- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
流收集器数据库 5000 系列	update-fcdb- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-fcdb- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
流收集器 (NetFlow) (这是流量收集器 5000 系列引擎必 需的) 流收集器 (NetFlow)VE	update-fcnf- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-fcnf- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
流收集器 (sFlow) 流收集器 (sFlow) VE	update-fcsf- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-fcsf- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
流传感器 流传感器 VE	update-fsuf- 7.4.2.20230203.2121- 231b83a5320a-0-01.swu	update-fsuf- 7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu
SMC (管理器)	update-smc-	update-smc-

---

设备	从 v7.3.0、v7.3.1 或 v7.3.2 更新 软件更新 文件名	从 v7.4.0 或 v7.4.1 更新 软件更新 文件名
SMC (管理器) VE	7.4.2.20230203.2121- 231b83a5320a-0-01.swu	7.4.2.20230203.2121- 231b83a5320a-0-v2-01.swu



## 3. 备份设备配置

如果没有备份，则在更新流程中出现问题时，您将无法恢复文件。这些步骤对于帮助将数据丢失降至最低非常重要。

 确保备份每个设备配置。

按照以下说明从“设备管理器”中选择设备，并创建配置设置的备份文件。

1. 打开**集中管理 > 设备管理器**。
2. 点击 **SMC(管理器)** 的**操作 (Actions)** 菜单。
  - **所有托管设备**:要备份由中央管理器管理的所有设备的配置，请选择主 **SMC(管理器)**。
  - **单个受管设备**:要备份“集中管理”中单个设备的配置，请选择设备的“操作”菜单。例如，如果您只需要备份流传感器，请选择流传感器的“操作”菜单。
3. 选择**支持**。
4. 选择**配置文件**选项卡。
5. 点击**备份操作 (Backup Actions)** 下拉列表。
6. 选择**创建备份**。

**SMC(管理器)和集中管理器**:备份主 **SMC(管理器)**和集中管理器时，会有一个 **SMC(管理器)** 备份配置文件和一个集中管理器备份配置文件。

 如果要备份 **SMC(管理器)**和流量收集器，请确保同时备份数据库。同时需要这两项备份才能完全恢复这些设备。有关备份 **SMC(管理器)**和流量收集器数据库的详细信息，请参阅 [5. 备份 SMC\(管理器\)和流量收集器的数据库](#)。

7. 继续 [4. 创建诊断包](#)

## 4. 创建诊断包

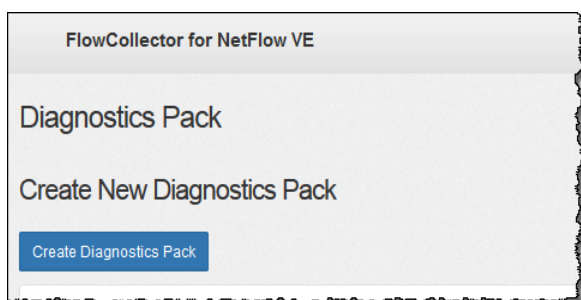
如果您需要通过 [思科支持部门](#) 对问题进行故障排除，则诊断包会非常重要。按照您的 Cisco Secure Network Analytics 版本的说明进行操作：

- **v7.3.x:** 在 [v7.3.x 中创建诊断包](#)
- **v7.4.x:** 在 [v7.4.x 中创建诊断包](#)

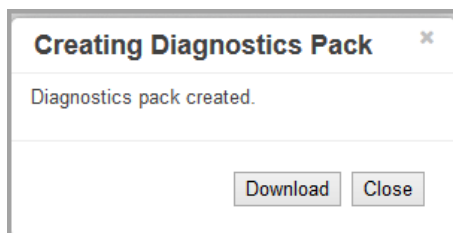
### 在 v7.3.x 中创建诊断包

使用“设备管理”(Appliance Administration) 为每个设备创建诊断包：

1. 登录“设备管理”界面。
2. 点击 **支持 (Support) > 诊断包 (Diagnostics Pack)**。
3. 点击 **创建诊断包 (Create Diagnostics Pack)**。



4. 点击 **下载 (Download)**，并将诊断包 (GPG) 文件保存到您的首选位置。这个过程会需要几分钟的时间。



5. 点击 **关闭 (Close)** 以关闭进度窗口。



**超时:**在大型系统中, 诊断包的生成可能会因超时而失败。要解决此情况, 请打开设备的 **SSH** 控制台, 然后运行以下命令: `doDiagPack`。这将允许生成诊断包, 而不会超时。

诊断包位于 `/lancope/var/admin/diagnostics`。

## 在 v7.4.x 中创建诊断包


使用系统配置为每个设备创建诊断包:

1. 以根身份登录设备控制台。
2. 键入 **SystemConfig**。按下 **Enter** 键。
3. 选择 **恢复模式**。
4. 选择 **诊断包**。
5. 要自定义诊断包, 请选择一个菜单, 然后点击 **编辑 (Edit)**。

菜单	说明
文件名称前缀	为诊断包添加文件名前缀(最多 127 个字符)。
密码	为诊断包创建文件密码。如果您不创建文件密码, 我们将使用默认方法(思科密钥)加密诊断包。
配置备份	选择此选项并按照屏幕上的提示在诊断包中添加配置备份。有关备份的更多信息, 请参阅“帮助”中的备份配置文件。
模块 (Modules)	通过选择要包括的特定模块来编辑诊断包内容。

6. 点击 **完成 (Finish)**。按照屏幕上的提示创建诊断包。

## 5. 备份 SMC(管理器)和流量收集器的数据库

 此程序仅适用于非Data Store 流收集器。如果没有备份,则在更新流程中出现问题时,您将无法恢复文件。请确保按照说明操作并完成数据库备份的所有操作过程。要获取帮助,请联系[思科支持](#)。

在为 SMC(管理器)和流量收集器创建诊断包后,请确保备份数据库。要获取帮助,请联系[思科支持](#)。

此过程涉及完成以下操作过程:

1. 整理流量收集器数据库
2. 删除数据库快照
3. 备份远程文件系统
4. 删除数据库快照

### 1. 整理流量收集器数据库

流量收集器数据库备份可能需要多天才能完成,如果数据库很大,则会降低网络速度。我们建议您在备份数据库之前先整理流量收集器数据库。这样可以释放用于存储流的可用磁盘空间,并减少备份数据库所需的时间。

流量收集器根据磁盘空间和每天收集的数据量存储最大天数。当达到最大值(/lancop/var 分区的 75%)时,数据库会首先删除最早的数据,以允许存入新数据。

#### 1. 审核数据库存储统计信息

按照以下说明检查数据库存储。

1. 登录流量收集器设备管理界面。
2. 选择**支持 > 数据库存储统计信息**。
3. 在“容量”、“流数据摘要”和“CI 事件数据摘要”(或“安全事件数据摘要”)中检查存储的天数。

**Database Storage Statistics**

**Capacity**

	Average	Working
Capacity in Days	50	49
Remaining Days	22	21
Bytes Per Day	549.46M	563

**Flow Data Summary**

Data	Days	Containers	Total	Average Per Day	Largest Day	Total
Flow Details	28	32	148.75M	5.31M	5.49M	3.4
Flow Interface Details	14	20	213.3M	15.24M	15.65M	5.5
Total	28	52	362.05M	20.55M	21.15M	9.4

**CI Event Data Summary**

Data	Days	Containers	Total	Average Per Day	Largest Day	Total
CI Events	28	29	351.17k	12.54k	12.85k	8.53M
CI Event Details	28	29	351.17k	12.54k	12.85k	4.06M
Total	28	58	702.34k	25.08k	25.71k	12.59M

## 2. 整理界面详细信息

流接口数据是与导出器的接口相关的数据。Stealthwatch 可保存流接口数据和流数据。流接口默认设置使系统向外推送流数据，因此它可以保留所有能够保留的接口统计信息。该功能以桌面客户端为主要工具，不适用于 Data Store 系统。可能需要一个节点来指示调整程序仅适用于非 Data Store 系统。

**Quick View for Flow**

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
	Cisco	#Index-2	Outbound			Permitted
	Cisco	#Index-3	Inbound			Permitted

备份这些数据需要时间。如果不需要全部数据，请缩短存储时限(例如:7天)。任何超过时限的数据都将丢失。

按照以下说明清除数据库中超过所设时限的接口统计数据，以便释放用于存储流的可用磁盘空间。

1. 以管理员用户身份登录桌面客户端。
2. 在“企业树”中找到流量收集器。点击加号 (+) 展开容器。

3. 右键点击流量收集器。选择**配置 > 属性**。
4. 在“流量收集器属性”对话框中，点击**高级 (Advanced)**。
5. 选择**存储流接口数据**。
6. 缩短存储时限。例如，如果将限制设置为**最多 7 天**，则超过 7 天的所有数据都会丢失。
7. 点击**确定 (OK)**。
8. 等待 5 分钟，继续执行后续步骤。

### 3. 整理流详细信息和 CI 事件数据

要减少流量收集器数据库中流详细信息和 CI 事件/详细信息的大小，请联系 [Cisco 支持](#)。此步骤是可选步骤，整理过程只需几分钟即可完成，但需要在指导下进行。

整理 **NetFlow** 时，您将指定在流量收集器数据库中保留流详细信息和 CI 事件/详细信息的天数。采用此配置会发生以下两件事：

- 数据库将被整理为您输入的天数。
- 数据库开始根据最早的日期清除较早的数据，但不会尝试尽可能多地保存数据。

## 2. 删除数据库快照

在创建备份文件之前，请确保按照以下说明删除 **SMC(管理器)** 和流量收集器数据库上保存的任何快照。



请确定您要删除 **SMC(管理器)** 和流量收集器数据库快照。此步骤对于成功备份非常重要。

1. 以**管理员**身份登录 **SMC(管理器)** 和流量收集器设备数据库控制台。
2. **查看快照：类型：**

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select * from database_snapshots;"
```

### 3. 删除快照(如果存在):输入以下命令行:

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

### 4. 等待删除快照文件夹:检查:

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

如果结果不为空,请继续等待。您可能需要等待几分钟才能删除文件夹,具体取决于数据库的大小。

### 5. 重复步骤 1 至 4,删除所有已保存的 SMC(管理器)和流量收集器数据库快照。

## 3. 备份远程文件系统

要将数据库备份到远程文件系统,请完成以下步骤:

- **空间:**确保远程文件系统有足够空间来存储数据库备份。
- **时间:**备份一次数据库后,后续备份速度会加快,因为该过程仅备份自上次备份以来发生的更改。此过程每分钟备份约 **0.5 GB** 到 **2 GB** 的数据。

1. 返回设备管理界面(但不要关闭桌面客户端)。
2. 确定远程文件系统上有存储数据库备份所需的**空间**,如下所示:

- 点击**主页 (Home)**。
- 找到**磁盘使用情况**部分。
- 查看 **/lancope/var** 文件系统的**已使用(字节)**列。要存储数据库备份,您至少需要这么大的空间,再加上远程文件系统上 **15%** 的空间。

Disk Usage				
Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G



3. 点击 **配置 (Configuration) > 远程文件系统 (Remote File System)**。

The screenshot shows the 'Remote File System' configuration page. The fields are as follows:

IP Address:	15.32
Port Number:	445
Share Name:	backup
Username:	qa
Password:	.....

Buttons at the bottom: Test, Clear Configuration, Reset, Apply.

4. 使用您要将备份文件存储到的远程文件系统的设置填写这些字段。

文件共享使用 CIFS(通用互联网文件系统) 协议, 也称为 SMB(服务器消息块)。

5. 点击 **应用 (Apply)** 将设置置于配置文件中。

如果在输入密码后, “应用”(Apply) 按钮未启用, 请在“远程文件系统”页面的空白区域中点击一次以启用此按钮。

6. 点击 **测试 (Test)** 以验证设备和远程文件系统是否能够互相通信。

测试完成后, 您应在“远程文件系统”页面底部看到以下消息。

**File sharing appears to be properly configured.**

7. 点击 **支持 (Support) > 备份/恢复数据库 (Backup/Restore Database)**。此时将打开“备份数据库”页面, 如以下示例所示。

The screenshot shows the 'Backup/Restore Database' page. The main content is:

**Backup Database**

Backup database and configuration to [previously configured file share](#).

**Create Backup**


Please see the [help page](#) for information on restoring database backups.

8. 点击 **创建备份 (Create Backup)**。此过程可能需要很长时间。




- 备份过程开始后,可将鼠标从页面移开,进程不会中断。但是,如果在备份过程中点击**取消 (Cancel)**,则可能无法在不重新启动设备的情况下恢复备份。
- 按照屏幕上的提示操作,直到完成备份。
- 要查看备份过程的详细信息,请点击**查看日志 (View Log)**。

9. 点击**关闭 (Close)**以关闭进度窗口。

 如果在备份完成之前取消备份,请确保再次删除数据库快照。请参阅 [4. 删除数据库快照](#)。

## 4. 删除数据库快照

保存好备份文件后,请按照以下说明删除 SMC(管理器)和流量收集器数据库中的快照。

 请确定您要删除 SMC(管理器)和流量收集器数据库快照。此步骤对于成功更新非常重要。

1. 以**管理员**身份登录 SMC(管理器)或流量收集器设备数据库控制台。

2. **查看快照**:输入以下命令行:

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select * from database_snapshots;"
```

3. **删除快照(如果存在)**:输入以下命令行:

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select remove_database_snapshot('StealthWatchSnap1');"
```

4. **等待删除快照文件夹**:检查:

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

如果结果不为空,请继续等待。您可能需要等待几分钟才能删除文件夹,具体取决于数据库的大小。

5. 重复步骤 1 至 4,删除所有已保存的 SMC(管理器)和流量收集器数据库快照。

## 6. 备份 Data Store

**i** 如果您是 Data Store 的新用户，请联系思科专业服务，获取有关规划和实施这些任务的帮助。

有关 Data Store 数据库备份的详细信息，请参阅 [数据存储硬件部署和配置指南](#) 或 [数据存储虚拟版部署和配置指南](#)。

要备份您的 Data Store，请完成以下过程：

1. 估计备份主机存储要求
2. 准备备份主机 在备份主机上安装 Python v3.7 和 rsync v3.0.5

**i** 使用独立于 Cisco Secure Network Analytics 设备的基于 Linux 的主机。

3. 为 dbadmin 启用无密码 SSH 访问 启用无密码 SSH 访问。确保所有数据节点可以使用无密码 SSH 访问访问备份主机。

4. 初始化备份主机上的备份目录：
5. 备份 Data Store 数据库

### 1. 估计备份主机存储要求

1. 以 root 身份登录到数据节点控制台。
2. 复制以下命令并将其粘贴到命令行中，然后按 **Enter** 键使用 vsql 连接到数据库并执行查询。出现提示时，请输入密码。记录下结果。

```
/opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_bytes) FROM storage_containers;"
```

3. 将总和乘以 2 即可估算出备份主机需要多少存储空间。

### 2. 准备备份主机

1. 根据您在 [1. 估计备份主机存储要求](#)，确定网络上运行 Linux 的主机以存储备份，或部署符合必要存储要求的 Linux 主机。

**i** 使用独立于 Cisco Secure Network Analytics 设备的基于 Linux 的主机。

2. 以 root 用户身份登录备份主机控制台。
3. 在命令提示符后，输入 python3 --version 并按 **Enter** 键以查看已安装的 Python 版本。您有以下选择：

- 如果安装了 Python 3.7 或更高版本, 请转至 [步骤 6](#)。
  - 否则, 请从步骤 4 开始安装 Python 3.7。
4. 输入 `sudo apt-get update` 并按 **Enter** 键下载软件包的更新版本, 包括 Python。出现提示时, 请输入密码。
  5. 输入 `sudo apt-get install python3.7`, 然后按 **Enter** 安装 Python 3.7(修改命令以安装不同版本)。
  6. 在命令提示符后, 输入 `rsync -version` 并按 **Enter** 键以查看已安装的 `rsync` 版本。您有以下选择:
    - 如果已安装 `rsync 3.0.5` 或更新版本, 请继续执行 [步骤 9](#)。
    - 否则, 请安装 `rsync 3.0.5`。继续执行步骤 7。
  7. 输入 `sudo apt-get update` 并按 **Enter** 键下载软件包的更新版本, 包括 `rsync`。出现提示时, 请输入密码。
  8. 输入 `sudo apt-get install rsync` 并按 **Enter** 键安装 `rsync`。
  9. 在命令提示符后, 输入 `getent passwd | grep dbadmin` 并按 **Enter** 键确定此主机上是否存在 `dbadmin` 用户帐户。您有以下选择:
    - 如果存在 `dbadmin` 用户帐户, 则备用主机已就绪。继续执行 [3. 为 dbadmin 启用无密码 SSH 访问](#) 启用无密码 SSH 访问:
    - 否则, 请在此主机上创建 `dbadmin` 用户帐户。继续执行步骤 10。
  10. 在命令提示符后, 输入 `useradd dbadmin` 并按 **Enter** 键创建 `dbadmin` 用户帐户。
  11. 输入 `passwd dbadmin` 并按 **Enter** 键为 `dbadmin` 分配一个密码。
  12. 输入 **新密码** 并按 **Enter** 键设置 `dbadmin` 密码。在提示时确认密码。

### 3. 为 dbadmin 启用无密码 SSH 访问

1. 对于 SSH, 在备份主机和每个数据节点之间打开端口 22/TCP; 对于 `rsync`, 打开备份主机和每个数据节点之间的端口 50000/TCP。
2. 有关详细信息, 请参阅 `ssh-copy-id dbadmin@[hostname]` 上的 [OpenSSH](#) 文档。
3. 键入以下命令, 以 `dbadmin` 身份登录数据节点:

```
su dbadmin
```

4. 将以下命令复制粘贴到文本编辑器中:

```
ssh-copy-id dbadmin@[hostname]
```

其中 `[hostname]` 是备份主机的主机名或 IP 地址。
5. 复制更新后的命令, 将其粘贴到命令提示符中, 然后按 **Enter** 键将 `dbadmin` SSH 授权密钥复制到备份主机。
6. 将以下命令复制粘贴到文本编辑器中:

`ssh 'dbadmin@[hostname]'` 其中 `[hostname]` 是备份主机的主机名或 IP 地址。

- 复制更新后的命令，将其粘贴到命令提示符中，然后按 **Enter** 键验证您可以通过 SSH 登录到远程主机的控制台，而无需从此数据节点输入密码。

## 4. 初始化备份主机上的备份目录：

- 以 `root` 身份登录第一个数据节点的控制台。

**i** 记下您用于初始化备份目录的数据节点。您将在以后的过程中使用相同的数据节点备份 Data Store 数据库( [5. 备份 Data Store 数据库](#))。

- 输入 `su-dbadmin`，然后按 **Enter** 以 `dbadmin` 用户身份运行以下命令。
- 输入 `ssh [backup-host]`，其中 `[backup host]` 是备份服务器的主机名或 IP 地址。您应该能够以 `dbadmin` 身份登录到备份主机的界面，而不会提示您输入密码。如果备份主机提示您输入密码，请检查设置。
- 输入 `cd /home/dbadmin` 并按 **Enter** 键更改目录。
- 输入 `mkdir backups` 并按 **Enter** 键创建 `backups` 目录。
- 输入 `exit` 并按 **Enter** 返回到数据节点的命令行提示符。
- 输入 `vi pw.ini` 并按 **Enter** 键创建 `pw.ini` 备份密码文件，然后对其进行编辑。

**i** 如果已使用 `setup-sw-datastore-secure-connectivity` 脚本更新 `dbadmin` 密码，则还必须更新存储在 `pw.ini` 备份密码文件中的密码，否则备份会失败。

- 将以下行复制到文本编辑器中：

```
[Passwords]
dbPassword = [dbadmin-password]
```

- 将 `[dbadmin-password]` 更新为 Data Store `dbadmin` 密码。
- 复制更新后的行并将其粘贴到 `pw.ini` 备份密码文件中。
- 按 **Esc**，然后输入 `:wq`，之后按 **Enter** 退出并保存更改。
- 输入 `chmod 640 pw.ini`，然后按 **Enter** 键以更改 `pw.ini` 文件权限，允许 `dbadmin` 用户读取和编辑文件。如果您使用的是 `v7.4.2` 软件，请跳至 [步骤 15](#)。否则，请继续执行下一步。
- 对于每个节点，编辑/修改 `/etc/default/ssh` 文件中的 `SSHD_OPTS`，如下所示。您必须以 `root` 用户身份登录才能完成此过程。

之前：

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
Banner=/etc/issue.net -o PermitRootLogin=yes -o
AllowTcpForwarding=no"
```

之后：

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
AllowUsers=dbadmin -o Banner=/etc/issue.net -o
PermitRootLogin=yes -o AllowTcpForwarding=yes"
```

- 重新启动 `ssh` 服务, 如下所示:

```
systemctl restart ssh
```

- 复制以下行并将其粘贴到文本编辑器中:

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups
```

```
[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1
```

```
[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

- 输入 `vi config.ini` 并按 **Enter** 键创建 `config.ini` 备份配置文件, 然后对其进行编辑。
- 将您在第 15 步中粘贴的文本复制到纯文本编辑器中, 并将其粘贴到 `config.ini` 文件中。
- 将 `backup-host-ip` 替换为备份主机的 IP 地址。
- 如果 [Mapping] 下的主机名与数据节点不匹配, 请更新这些主机名。要确定数据节点名称, 请执行以下操作:

- 以 `root` 用户身份连接到任何数据节点控制台
  - 输入 `su dbadmin`
  - 输入 `admintools -t node_map`
- 将“NODENAME”列中的节点名称用于 [Mapping] 条目


示例:

```
dbadmin@sdbn-742-10-0-56-133-5:/root$ admintools -t node_map
DATABASE | NODENAME | HOSTNAME
```

```
-----
sw | v_sw_node0001 | 169.254.42.10
sw | v_sw_node0002 | 169.254.42.12
sw | v_sw_node0003 | 169.254.42.15
```

20. 如果您在环境中部署了超过三个数据节点，请确保每一个都有一个条目。如果您只有一个数据节点，请删除额外的 [Mapping] 行，只留下一行数据节点。
21. 按 **Esc**，然后输入 `:wq`，之后按 **Enter** 退出并保存更改。
22. 输入 `vbr -t init -c config.ini`，然后按 **Enter** 初始化备份主机上的 `/home/dbadmin/backups` 目录以接收 **Data Store** 备份。

## 5. 备份 Data Store 数据库

 您只需在其中一个数据节点上发出 **backup** 命令，即可备份整个多节点数据库。

1. 以 `root` 用户身份登录到您在 **4. 初始化备份主机上的备份目录:** 上的备份目录：
2. 输入 `su-dbadmin`，然后按 **Enter** 以 `dbadmin` 用户身份运行以下命令。
3. 输入 `vbr -t backup -c config.ini --debug 3 --dry-run`，然后按 **Enter** 键执行备份测试，而不创建备份。您有这些选择：
  - 如果备份测试成功解析，请备份 **Data Store** 并继续步骤 4。
  - 如果备份测试失败，则可能已创建快照文件，必须将其删除。有关删除说明，请参阅 [数据存储备份失败](#)。如果备份测试未能解析，请查看 `/tmp/vbr` 目录中的调试日志文件，解决根本原因，然后再次测试备份。请联系 [思科支持部门](#) 寻求更多协助。
4. 输入 `vbr -t backup -c config.ini`，然后按 **Enter** 键将 **Data Store** 备份到备份主机上的 `/home/dbadmin/backups` 目录。
5. 继续 **7. 检查可用磁盘空间**。

## Data Store 备份失败

如果 **Data Store** 备份失败，请确保在尝试其他备份之前删除数据库快照。请按照以下步骤删除 **Data Store** 数据库快照。

1. 使用 `vsq1` 连接到 **Data Store** 数据库集群。
2. 执行以下命令以检索快照列表：
 

```
select * from database_snapshots;
```
3. 将“`snapshot_name`”替换为要删除的快照的名称，然后执行以下命令：
 

```
select remove_database_snapshot('snapshot_name');
```

4. 执行以下命令以退出。

```
\q
```



## 7. 检查可用磁盘空间

检查每个设备上的磁盘空间，确认您拥有足够的可用空间以安装补丁和软件更新文件。

**!** 请确保 **SMC(管理器)** 上有足够的可用空间以安装您上传到更新管理器的所有设备 **SWU** 文件。还需确认每个设备上有足够的可用空间。

- **SMC(管理器)** : 当 **SWU** 上传到“集中管理”中的更新管理器时，它将在更新期间使用 **SMC(管理器)** 上的额外空间。此文件将保留在集中管理中的 **SMC(管理器)** 上，直至由同一类型的另一文件替换。

请确保 **SMC(管理器)** 上有足够的可用空间以安装您上传到更新管理器的所有设备 **SWU** 文件。例如，如果通过“集中管理”中的更新管理器更新流量收集器，则此文件将保留在 **SMC(管理器)** 文件系统中，直至您上传新的流量收集器 **SWU** 文件。

- **受管设备** : 如果您通过“集中管理”中的更新管理器更新设备，则在更新完成后，**SWU** 将从设备文件系统中删除。例如，如果您通过“集中管理”中的更新管理器更新流量收集器，则在更新完成后，此文件将从流量收集器文件系统中删除。

按照以下说明确认您拥有足够的可用磁盘空间在 **SMC(管理器)** 和每个托管设备上安装补丁和软件更新文件。

1. 登录“设备管理”界面。
2. 点击 **主页 (Home)**。
3. 找到 **磁盘使用情况** 部分。
4. 查看 **可用(字节)** 列，确认 **/lancope/var/** 分区上具有所需的可用磁盘空间。
  - **要求** : 在每个托管设备上，可用空间应至少是单个软件更新文件 (**SWU**) 大小的四倍。在 **SMC(管理器)** 上，可用空间应至少是您上传到更新管理器的所有设备 **SWU** 文件大小的四倍。
  - **托管设备** : 例如，如果流量收集器 **SWU** 文件为 **6 GB**，则流量收集器 (**/lancope/var**) 分区上至少应有 **24 GB** 可用空间 (**1 个 SWU 文件 x 6 GB x 4 = 24 GB** 可用空间)。
  - **SMC(管理器)** : 例如，如果要将四个 **SWU** 文件上传到 **SMC(管理器)**，而每个文件为 **6 GB**，则 **/lancope/var** 分区上至少应有 **96 GB** 可用空间 (**4 个 SWU 文件 x 6 GB x 4 = 96 GB** 可用空间)。


Name	Used	Size (byte)	Used (byte)	Available (byte)
/	40%	9.55G	3.54G	5.52G
/lancope/var	14%	27.94G	3.81G	23.54G



5. 如果需要扩展设备磁盘空间, 请参阅[安装指南](#)中有关您的设备的“Data Store”部分。
6. 重复步骤 1 至 5, 检查每个设备上的可用空间。

## 8. 安装补丁

在开始软件更新之前，请确保在设备上安装最新的补丁。要下载补丁，请参阅 [2. 下载补丁和更新文件](#) 以了解详细信息。


 在安装修补程序之前，请确认已在群集中的每个托管设备上完成了步骤 3 至 7。

在安装补丁时，建议您遵循以下最佳实践：

- **自述文件：**您可以上传特定设备的更新补丁 **SWU** 文件，或上传适用于集中管理中所有设备的通用更新补丁。有关特定更新补丁的详细信息，请参阅 [cisco.com](https://www.cisco.com) 上的自述文件。
- **顺序：**请确保按照本节中指定的顺序在设备上安装补丁。对于此更新，您需要先在辅助 **SMC(管理器)** 上安装累积补丁。
- **时间：**在每台设备上安装这些修补程序最多可能需要 **90** 分钟。当配置更改挂起或配置通道关闭时，请勿重新启动设备。
- **确认：**确认补丁已安装，并且每个设备状态显示为 **运行(v7.3.x 和 v7.4.0)** 或 **已连接(v7.4.1)**，然后再开始下一个补丁安装。
- **数据节点 (v7.4.1)：**如果您已安装了 **v7.4.1** 的数据节点，请确保使用 **更新所有数据节点 (Update All Data Nodes)** 按钮。

### 1. 查看已安装版本

按照以下说明将补丁上传到“集中管理”中的更新管理器。


1. 登录您的主 **SMC(管理器)**。
2. 点击  (**全局设置**) 图标。
3. 选择 **集中管理**。
4. 查看 **设备状态 (Appliance Status)** 列并确认每个设备均显示为 **运行(v7.3.x 和 v7.4.0)** 或 **已连接(v7.4.1)**。
5. 选择 **更新管理器** 选项卡，然后找到 **系统更新** 部分。
6. 查看 **已安装版本** 列。确认每个设备是一致的，仅安装了版本 **7.3.0、7.3.1、7.3.2、7.4.0 或 7.4.1**。

此示例显示所有设备的安装版本为 **v7.3.2**。

System Updates ●							
APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc01-10.200.99.9	10.200.99.9	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		⋮
SMC	smc02-10.200.99.10	10.200.99.10	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		⋮
Flow Collector	fc01-10.200.99.11	10.200.99.11	2 hours ago ●	7.3.2 patch-fcnf- ROLLUP005-7.3.2-01	-		⋮
Flow Collector	fc02-10.200.99.12	10.200.99.12	2 hours ago ●	7.3.2 patch-fcsf- ROLLUP004-7.3.2-01	-		⋮
UDP Director	udp01-10.200.99.13	10.200.99.13	19 hours ago ●	7.3.2 20210409.0329-58b6668961ea	-		⋮
Flow Sensor	fs-10.200.99.14	10.200.99.14	a month ago ●	7.3.2 20210409.0329-58b6668961ea	-		⋮

## 2. 安装所需的补丁

确保在安装任何所需的 **v7.3.x**(v7.3.0、v7.3.1 或 v7.3.2) 或 **v7.4.x**(v7.4.0 或 v7.4.1) 补丁之前更新到 v7.4.2。

 在**辅助 SMC(管理器)**上安装修补程序, 并确认安装已完成, 然后再在主 SMC(管理器)上安装修补程序。

在**更新管理器 (Update Manager)**页面上:

1. 点击**上传 (Upload)**。
2. 为 SMC(管理器)选择最新的累积补丁 SWU 文件。
3. 在**更新管理器 (Update Manager) > 系统更新 (System Updates)**部分中, 选中 SMC(管理器)的**准备安装 (Ready to Install)**列, 并确认已显示补丁。
4. 点击**辅助 SMC(管理器)**的**操作 (Actions)**菜单, 然后选择**安装更新 (Install Update)**。
  - **主 SMC(管理器)**: 如果您已在**辅助 SMC(管理器)**上完成补丁安装, 请点击主 SMC(管理器)的**操作 (Actions)**菜单。
  - **数据节点 v7.4.1**: 点击**更新所有数据节点 (Update all Data Nodes)**按钮。
  - **所有其他设备和版本**: 在“操作”(Actions)列中, 点击设备的 **⋮ (省略号)**图标。选择**安装更新**。
5. 按照屏幕上的提示确认更新。
  - **更新状态**: “更新状态”列将从“正在等待安装...”更改为“正在安装”。
  - **重新启动**: 设备会自动重新启动。

并非所有修补程序都会重新启动设备。请勿在更改过程中重新启动设备。



在每台设备上安装修补程序最多可能需要 90 分钟。当配置更改挂起或配置通道关闭时，请勿重新启动设备。要确认设备状态为**运行 (v7.3.x 和 v7.4.0)** 或已**连接 (v7.4.1)**，请查看**集中管理 (Central Management) > 设备管理器 (Appliance Manager)** 页面。

## 6. 确认安装：

- 点击 SMC(管理器)的**操作 (Actions)** 菜单。
- 选择**查看更新日志**。
- 确认补丁显示为成功或已安装。如果补丁不成功，请纠正所有错误，然后重试。有关更多信息，请参阅 [故障排除](#)。

7. 在**集中管理 (Central Management) > 设备管理器 (Appliance Manager)** 页面中查看 SMC(管理器)。确认设备状态已显示为**运行 (v7.3.x 和 v7.4.0)** 或已**连接 (v7.4.1)**。
8. 如果您为故障转移配置了两个 SMC(管理器)，请重复步骤 4 至 7，在主 SMC(管理器)上安装修补程序。
9. 按以下顺序对集群中的所有其他设备重复这些步骤：

顺序	设备	注
1.	所有UDP 导向器 (也称为 流量复制器)	如果有高可用性群集，请先在辅助 UDP Director 上安装补丁。
2.	所有数据节点或 流收集器 5000 系列数据库	<div style="border: 1px solid #00a0e3; padding: 5px; margin-bottom: 10px;"> <p> 在 v7.4.1 之前，您的集群不会同时具有数据节点和流量收集器 5000 系列数据库。</p> </div> <p><b>数据节点</b></p> <p>将补丁应用于数据节点中的每个 Data Store。等待“集中管理”将所有数据节点设备状态显示为<b>运行或已连接</b>，然后再继续操作。</p> <p><b>更新所有 数据节点(v7.4.1)</b></p> <p>如果您安装了 v7.4.1，请按照说明使用<b>更新所有数据节点</b>按钮同时在数据节点上安装补丁。在<b>所有</b>数据节点上成功安装更新补丁后，请确保在任何数据节点上重新启动 Vertica。</p>

		<b>流量收集器 5000 系列数据库</b> 在开始引擎更新之前, 确保流量收集器系列数据库完成补丁安装, 设备状态显示为 <b>运行或已连接</b> 。
3.	流量收集器 5000 系列引擎	确保流量收集器系列数据库完成补丁安装, 设备状态显示为 <b>运行或已连接</b> , 然后再开始引擎更新。
4.	所有其他流量收集器 (NetFlow 和 sFlow)	在集群中的下一个设备上安装补丁之前, 请确保流收集器完成补丁安装, 并且设备状态显示为 <b>运行或已连接</b> 。
5.	流量传感器	

#### 10. 确认安装:

- 点击设备的**操作菜单**。
- 选择**查看更新日志**。
- 确认补丁显示为成功或已安装。如果补丁不成功, 请纠正所有错误, 然后重试。有关更多信息, 请参阅 [故障排除](#)。

#### 11. 在更新管理器 (Update Manager) > 系统更新 (System Updates) 部分中, 选中每个设备的**准备安装 (Ready to Install)** 列, 并确认已显示累积补丁。



在每台设备上安装修补程序最多可能需要 90 分钟。当配置更改挂起或配置通道关闭时, 请勿重新启动设备。要确认设备状态为**运行 (v7.3.x 和 v7.4.0)** 或**已连接 (v7.4.1)**, 请查看“集中管理”(Central Management) > “设备管理器”(Appliance Manager) 页面。

#### 12. 数据节点 v7.4.1: 在所有数据节点上成功安装补丁文件后, 在任何数据节点上重新启动 Vertica。

- 转到“集中管理”(Central Management) > Data Store > “数据库控制”(Database Control)。
- 在数据库的“操作”列中, 点击 **⋮ (省略号)** 图标。
- 选择**开始 (Start)**。
- 确认数据库状态显示为**运行**。

## 9. 安装 v7.4.2 软件更新

您将继续使用“更新管理器”页面进行软件更新。



如果要从 v7.3.x 升级，请确保您的 SMC(管理器)和流量收集器已运行超过 1 小时但不到 7 天，然后再开始软件升级。

在安装软件更新时，建议您遵循以下最佳实践：

- **顺序**：开始之前，确保按顺序更新设备，并在 [更新顺序](#) 部分中查看详细信息。
- **等待**：如果要从 v7.3.x 升级，请确保您的 SMC 和流量收集器已运行超过 1 小时但不到 7 天，然后再开始软件升级。
- **确认**：在开始下一次设备更新之前，请确认更新已安装，并且每个设备状态都显示为运行 (v7.3.x 和 v7.4.0) 或已连接 (v7.4.1)。
- **多个设备**：除 SMC(管理器)、流量收集器 5000、高可用性 (HA) 中的 UDP Director 和数据节点外，您可以同时更新多个设备，只要它们是相同的设备类型，并遵循 [设备更新顺序和注意事项](#) 即可。
- **数据存储**：如果部署了 Data Store，请确保在所有数据节点上启用 SSH(通过选择“启用 SSH”(Enable SSH) 选项)，这在断电后升级或启动数据库之前是必需的。

按照 [备用访问](#) 中的步骤在所有数据节点上启用 SSH，并确保选择 **启用 SSH (Enable SSH)** 复选框，而不是“启用根 SSH 访问”(Enable Root SSH Access) 选项。如果要在数据节点上禁用 SSH，则可以在升级过程完成后返回并为每个数据节点禁用 SSH。

## 更新顺序

按以下顺序更新您的设备：

**i** 在开始安装任何 SWU 文件之前，请确保上传任何 SWU 文件。


顺序	设备	注
1.	UDP Director (也称为 流量复制器)	如果您有高可用性集群，请先更新辅助 UDP Director。 确认更新完成，且辅助 UDP Director 设备状态显示为 <b>运行</b> 或 <b>已连接</b> ，然后再更新主 UDP Director。
2.	所有数据节点或 流收集器 5000 系列数据库	<div style="border: 1px solid #00a0e3; padding: 5px; margin-bottom: 10px;"> <p><b>i</b> 在 v7.4.1 之前，您的集群不会同时具有数据节点和流量收集器 5000 系列数据库。</p> </div> <p><b>数据节点</b> 在开始更新之前，请确保已在每个数据节点上启用 SSH。有关详细信息，请参阅简介中的 <a href="#">Data Store</a>。</p> <p><b>更新所有数据节点 (v7.4.1)</b> 如果您安装了 v7.4.1，请按照说明使用<b>更新所有数据节点</b>按钮同时更新您的数据节点。在<b>所有</b>数据节点上成功安装更新 SWU 文件后，请确保在任何数据节点上重新启动 Vertica。</p> <p><b>流量收集器 5000 系列数据库</b> 确保流量收集器系列数据库完成更新，且设备状态显示为<b>运行</b>或<b>已连接</b>，然后再开始引擎更新。</p>
3.	流量收集器 5000 系列引擎	确保引擎更新已完成，且设备状态显示为 <b>运行</b> 或 <b>已连接</b> ，然后再更新集群中的下一设备。
4.	所有其他流量收集器 (NetFlow 和 sFlow)	确保流量收集器已运行超过 1 小时但不到 7 天，然后再开始更新(如果是从 v7.3.x 进行更新)。

		确保流量收集器更新已完成, 且设备状态显示为 <b>运行</b> 或 <b>已连接</b> , 然后再更新集群中的下一设备。
5.	流量传感器	上传流传感器 SWU 文件。如果您是 从 v7.3.x 升级, 则流传感器的设备状态可能显示为 <b>配置更改待处理 (Config Changes Pending)</b> 。
6.	辅助 SMC(管理器) *如果使用	<p>确保 SMC(管理器) 已运行超过 1 小时但不到 7 天, 然后再开始更新(如果是从 v7.3.x 进行更新)。</p> <p>如果您的系统使用辅助 SMC(管理器), 请确认辅助 SMC(管理器) 更新已完成, 并确认辅助 SMC(管理器) 设备状态显示为<b>运行</b>或<b>已连接</b>, 然后再开始主 SMC(管理器) 更新。</p> <p>更新完成后, 这两个 SMC(管理器) 可能都会以辅助角色重新启动。如果发生这种情况, 请参阅 <a href="#">12. 验证管理器 (原 SMC) 故障转移角色</a> 以了解详细信息。在更新两个 SMC(管理器) 之前, 请勿更改故障转移角色。</p>
7.	主 SMC(管理器)	<p>确保 SMC(管理器) 已运行超过 1 小时但不到 7 天, 然后再开始更新(如果是从 v7.3.x 进行更新)。</p> <p>如果您的系统使用辅助 SMC(管理器), 请确认辅助 SMC(管理器) 更新已完成, 并确认辅助 SMC(管理器) 设备状态显示为<b>运行</b>或<b>已连接</b>, 然后再开始主 SMC(管理器) 更新。</p> <p>更新完成后, 这两个 SMC(管理器) 可能都会以辅助角色重新启动。如果发生这种情况, 请参阅 <a href="#">12. 验证管理器 (原 SMC) 故障转移角色</a> 以了解详细信息。在更新两个 SMC(管理器) 之前, 请勿更改故障转移角色。</p>





## 安装软件更新

按照以下说明在“集中管理”中的设备上安装软件更新。

 单独安装设备软件更新文件。由于文件大小和 Web 应用限制，我们不建议压缩或捆绑软件更新文件。







### 1. 上传 7.4.2 SWU

1. 登录 SMC(管理器)。
2. 在浏览器地址栏中键入 `https://<SMC IP address>`。
3. 点击  (全局设置) 图标。
4. 选择**集中管理**。
5. 选择**更新管理器**选项卡，然后找到**系统更新**部分。

 开始之前，请确保按顺序更新设备并查看详细信息。在开始下一次设备更新之前，请确认更新已安装，并且每个设备都显示为**运行 (v7.3.x 和 v7.4.0)** 或**已连接 (v7.4.1)**。

6. 查看**已安装版本**列。确认每个设备都安装了相同的 **7.3.0**、**7.3.1**、**7.3.2**、**7.4.0** 或 **7.4.1** 版本。

此示例显示所有设备都安装了相同的版本 **7.3.2**。请注意，所有设备都安装了相同的版本。

System Updates ●							
APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc01-10-200-99-9	10.200.99.9	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
SMC	smc02-10-200-99-10	10.200.99.10	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
Flow Collector	fc01-10-200-99-11	10.200.99.11	2 hours ago ●	7.3.2 patch-fcnf- ROLLUP005-7.3.2-01	-		
Flow Collector	fc02-10-200-99-12	10.200.99.12	2 hours ago ●	7.3.2 patch-fcsf- ROLLUP004-7.3.2-01	-		
UDP Director	udp01-10-200-99-13	10.200.99.13	19 hours ago ●	7.3.2 20210409.0329-58b6668961ea-	-		
Flow Sensor	fs-10-200-99-14	10.200.99.14	a month ago ●	7.3.2 20210409.0329-58b6668961ea-	-		

7. 点击**上传 (Upload)**。
8. 按照屏幕上的提示选择 **SWU** 文件。一次上传一个文件。

 在开始安装任何 **SWU** 文件之前，请确保上传所有 **SWU** 文件。


- **更新:**为“集中管理”中的每个设备类型上传 SWU 文件。
- **磁盘空间:**如果需要确认您是否有足够的磁盘空间,请参阅 [7. 检查可用磁盘空间](#)。

## 2. 安装 7.4.2 SWU

按照以下说明,使用“集中管理”更新软件。

 请确保按顺序更新设备并查看说明信息。请参阅 [更新顺序](#)。


1. 确认所有设备的设备状态显示为**运行**(v7.3.x 和 v7.4.0) 或**已连接**(v7.4.1)。
2. 选择**更新管理器**选项卡。
3. 查看**系统更新 (System Updates)** 部分。检查设备的以下列,确认其已准备好更新:
  - **准备安装:**确认 **7.4.2** SWU 文件已发布。
  - **SMC(管理器)和流量收集器的上次重新启动:**确保上次重新启动的时间超过 1 小时但不到 7 天(如果是从 v7.3.x 更新)。
    - 如果不到 1 小时,请等待以继续。
    - 如果超过 7 天,请点击**操作菜单 > 重新启动设备 (Reboot Appliance)** 以重新启动设备。等待至少 1 小时,确认所有进程和安全检查均已就绪。

 当配置更改挂起或配置通道关闭时,请勿重新启动设备。要确认设备状态为**运行**(v7.3.x 和 v7.4.0) 或**已连接**(v7.4.1),请查看**集中管理 (Central Management) > 设备管理器 (Appliance Manager)** 页面。

4. **数据节点 v7.4.1:**点击**更新所有数据节点 (Update all Data Nodes)** 按钮。

**所有其他设备和版本:**在“操作”(Actions) 列中,点击设备的 **⋮ (省略号)** 图标。选择**安装更新**。

5. 按照屏幕上的提示确认更新。
  - **更新状态:**“更新状态”列将从“正在等待安装...”更改为“正在安装”。屏幕每分钟刷新一次。
  - **重新启动:**设备将自动重新启动以进行软件更新。

 设备会自动重新启动。在配置更改处于待处理状态时,请勿强制重新启动设备。


6. 检查**已安装版本 (Installed Version)** 列以确认它显示 **7.4.2** 软件更新。

- **安装成功:**如果 **7.4.2** 显示为设备的安装版本, 请继续下一步以确认设备状态。
  - **安装失败:**如果“更新状态”列显示“安装失败”, 请点击**操作菜单 > 查看更新日志 (View Update Log)** 以了解详细信息。如果能够解决问题, 请重新尝试更新。有关更多信息, 请参阅 **故障排除**。
7. 在“安全洞察控制面板”(Security Insight Dashboard) 上, 选择**配置 (Configure) > 全局 (GLOBAL) 集中管理**, 然后在清单中找到设备。
- **运行或已连接:**确认设备状态显示为**运行 (v7.3.x 和 v7.4.0)** 或**已连接 (v7.4.1)**。安装主管理器后, **v7.4.2** 中所有成功安装的设备的状态均显示为**已连接**。
  - **主管理器:**确认主管理器的设备状态显示为**已连接**。在主管理器更新之前, 辅助管理器状态将保持为**运行**。然后, 所有设备的状态将显示为**已连接**。
8. **数据节点 v7.4.1 至 v7.4.2:**确认所有数据节点的以下状态:
- 前往 **Data Store > 数据库更新状态 (Database Update Status)** 选项卡。确认所有数据节点的数据节点更新状态显示为**成功**, 并且上次状态已更改为最新状态。您可能需要刷新页面才能看到最新状态。
  - 点击**数据库控制 (Database Control)** 选项卡。确认数据库状态显示为**运行**。确认所有数据节点的状态显示为**运行**。
9. 对下一个设备重复 **2. 安装 7.4.2 SWU** 部分中所有步骤。请确保按顺序更新设备。
- 如果您已在“集中管理”中将每个设备更新为 **v7.4.2**, 请转至 **10. 配置高可用性** (仅限 UDP Director)。
  - 如果您的部署中没有 **UDP Director**, 请转至 **7. 安装桌面客户端**

## 故障排除

错误说明或类别	详细信息
“安装更新”按钮不可用	<p>如果<b>安装更新 (Install Update)</b>按钮灰显,无法点击,请确认设备 SWU 文件显示在<a href="#">准备安装 (Ready to Install)</a>列中。如果设备是流量传感器,请在更新 SMC(管理器)后<a href="#">上传</a> SWU 文件。</p> <p>还需检查上次<b>重新启动</b>列以确认上次启动 SMC (管理器)和流量收集器已超过 1 小时且不到 7 天(如果是从 v7.3.x 更新)。</p> <ul style="list-style-type: none"> <li>• 如果不到 1 小时,请等待以继续。</li> <li>• 如果超过 7 天,请转至“设备清单”。点击<b>操作 (Actions)</b>菜单 &gt; <b>重新启动设备 (Reboot Appliance)</b>以重新启动设备。等待至少 1 小时,确认所有进程和安全检查均已就绪。</li> </ul>
SMC(管理器)与受管设备之间的网络连接中断	<p>恢复网络连接,并确认设备清单上的每个设备显示为<b>运行或已连接</b>。如果设备状态为<b>配置通道关闭</b>,请参阅<a href="#">《安装和配置指南》</a>中的“故障排除”部分,以了解相关说明。</p> <p>在确认网络连接恢复后,请重试补丁或软件更新文件安装。</p>
失败:无法将此文件与数字签名匹配。请尝试重新上传文件。如果问题仍然存在,请联系思科支持部门。	<p>确认您拥有正确的 SWU。如果您无法确定是否拥有正确的 SWU,请联系<a href="#">思科支持</a>。</p>
设备上没有剩余空间(磁盘空间)	<p>检查每个设备上的磁盘空间,确认您拥有足够的可用空间以安装补丁和软件更新文件。</p> <p>在每个受管设备上,可用空间应至少是单个软件更新文件(SWU)大小的 4 倍。在 SMC(管理器)上,可用空间应至少是您上传到更新管理器的所有设备 SWU 文件大小的 4 倍。</p> <ul style="list-style-type: none"> <li>• <b>托管设备:</b>例如,如果流量收集器 SWU 文件为 6 GB,则流量收集器 (/lancope/var) 分区上至少应有 24 GB 可用空间(1 个 SWU 文件 x 6 GB x 4 = 24 GB 可用空间)。</li> </ul>

错误说明或类别	详细信息
	<ul style="list-style-type: none"> <li>• <b>SMC(管理器)</b>:例如,如果要将四个 SWU 文件上传到 SMC(管理器),而每个文件为 6 GB,则 /lancope/var 分区上至少应有 96 GB 可用空间(4 个 SWU 文件 x 6 GB x 4 = 96 GB 可用空间)。</li> <li>• <b>其他信息</b>:请参阅 <a href="#">7. 检查可用磁盘空间</a>,了解详细信息。</li> </ul>
意外退出状态!	<p>如果遇到此错误,可能是以下原因之一:</p> <ul style="list-style-type: none"> <li>• 在安装准备期间,服务无法顺利停止</li> <li>• 更新已启动,但未满足重新启动要求。</li> </ul> <p>确认每个设备在设备清单上显示为<b>运行或已连接</b>。如果设备状态为<b>配置通道关闭</b>,请参阅 <a href="#">《安装和配置指南》</a>中的“故障排除”部分,以了解相关说明。</p> <p>还需检查<b>上次重新启动</b>列以确认上次启动 SMC (管理器)和流量收集器已超过 1 小时且不到 7 天(如果是从 v7.3.x 更新)。</p> <ul style="list-style-type: none"> <li>• 如果不到 1 小时,请等待以继续。</li> <li>• 如果超过 7 天,请转至“设备清单”。点击<b>操作 (Actions)</b>菜单 &gt; <b>重新启动设备 (Reboot Appliance)</b>以重新启动设备。等待至少 1 小时,确认所有进程和安全检查均已就绪。</li> </ul>
SIVR-CHECK 警告! 我们发现了证书验证问题,这些问题会破坏以下集成。	<p>您的审核日志目标或 SMTP 配置配置不符合服务器身份验证的要求。有关详细信息,请参阅 <a href="#">服务器身份验证检查(仅限 7.3.x 至 7.4.2)</a>。请更正配置,然后重新尝试更新。</p>
上传失败	<p>在开始上传另一 SWU 文件之前,确认每个上传已完成并显示在<b>准备安装</b>列中。您还可以查看日志文件:/lancope/var/logs/containers/svc-central-management.log 以查看上传失败的原因。</p> <p>请参阅 <a href="#">9. 安装 v7.4.2 软件更新</a>,了解详细信息。如果您继续看到此错误消息,请联系<a href="#">思科支持</a>。</p>

 如果您无法解决此错误, 请联系 [客户支持部门](#)。




## 10. 配置高可用性

如果您有多个 UDP 导向器, 请使用“设备管理”界面来配置高可用性。

-  高可用性仅在 UDP 导向器硬件设备上可用, 而在虚拟设备上不可用。

UDP 导向器 高可用性 (HA) 允许用户配置冗余 UDP 导向器 的设置。两个节点完全冗余; 但是, 一次只有一个节点在线。

-  如果您在 UDP 导向器上配置了高可用性并将安全网络分析更新到 v7.4.0 或更高版本, 请确保在更新后使用 [1. 配置主 UDP 导向器 高可用性](#) 来重新配置高可用性。

### 主节点和辅助节点

在线节点在对中称为主节点, 而离线节点为辅助节点。如果对中的主节点发生故障, 辅助节点取而代之成为主节点。

### 要求

- 转发规则:** 为高可用性系统中的 UDP 导向器 配置至少一个 [转发规则](#)。
- 保存规则配置文件:** 如果已使用规则配置 UDP 导向器, 请导出(保存规则配置文件) UDP 导向器 规则。然后, 将文件导入到第二个 UDP 导向器, 以确保每个规则都匹配。
- 顺序:** 配置主 UDP 导向器, 然后对辅助导向器重复此配置过程。
- 新的或已有:** 如果两个 UDP 导向器都是新的, 请确保让每一个都遵循本指南中的程序。但如果辅助导向器已配置为 Cisco Secure Network Analytics 系统上的设备, 则要登录到辅助 UDP 导向器 并按照此处所述配置其高可用性组件。



## 1. 配置主 UDP 导向器 高可用性

1. 登录到主 UDP 导向器。
2. 点击 **配置 (Configuration) > 高可用性 (High Availability)**。

选中“高可用性设置”(High Availability Settings) 的启用高可用性服务 (**Enable High Availability Service**) 复选框。

<input type="checkbox"/> Enable High Availability Service	
<b>High Availability Settings</b>	
Node ID	<input type="radio"/> 1 <input type="radio"/> 2
Virtual IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Shared Secret	L@n [ ] iHA
Sync Ring #1(eth2) Unicast IP Address	<input type="text"/>
Sync Ring #1(eth2) Subnet Mask	<input type="text"/>
Sync Ring #2(eth3) Unicast IP Address	<input type="text"/>
Sync Ring #2(eth3) Subnet Mask	<input type="text"/>
Paired Node Host Name	<input type="text"/>
Paired Node Sync Ring #1(eth2) IP Address	<input type="text"/>
Paired Node Sync Ring #2(eth3) IP Address	<input type="text"/>

3. 选择您的 **节点 ID**。如果是主 UDP 导向器，请选择 1。如果这是辅助 UDP 导向器，请选择 2。
4. 在 **虚拟 IP 地址 (Virtual IP Address)** 字段中，输入与 eth0 接口位于同一子网中的未占用的 IP 地址。将 **子网掩码** 值设置为 eth0 接口上使用的子网掩码值。

**i** 确保两个节点上的虚拟 IP 地址相同。

5. 在 **共享密钥 (Shared Secret)** 字段中，键入两个 UDP 导向器的字符串。(这将被加密以进行安全传输。)
6. 在 **同步环 1 (eth2) 单播 IP 地址 (Sync Ring #1 (eth2) Unicast IP Address)** 字段中，输入 IP 地址和子网掩码。(单址广播 IP 地址标识单个网络目标。)

7. 在 **同步环 2 (eth3) 单播 IP 地址 (Sync Ring #2 (eth3) Unicast IP Address)** 字段中, 输入 IP 地址和子网掩码。
8. 每个 IP 地址 (eth0、eth02、eth03) 都必须位于其自己单独的单播子网中。在 **配对节点同步环 1(eth2) IP 地址** 字段中, 输入辅助 UDP 导向器的 Eth2 IP 地址。
9. 在 **配对节点主机名** 字段中, 输入辅助 UDP 导向器的主机名。
10. 在 **配对节点同步环 1(eth2) IP 地址** 字段中, 输入辅助 UDP 导向器的 Eth2 IP 地址。
11. 在 **配对节点同步环 1(eth3) IP 地址** 字段中, 输入辅助 UDP 导向器的 Eth3 IP 地址。
12. 在查看该设置后, 点击 **应用 (Apply)** 以设置配置。
13. 继续下一部分以配置群集的第二个 UDP 导向器。

## 2. 配置辅助 UDP 导向器 高可用性

 如果您在上面的 [步骤 4](#) 中选择了节点 ID 2, 请完成这些主 UDP 导向器的步骤。

要配置辅助 UDP 导向器, 请执行以下步骤:

1. 登录辅助 UDP 导向器。
2. 点击 **配置 (Configuration) > 高可用性 (High Availability)**。
3. 在 **配对节点主机名** 字段中输入辅助 UDP 导向器的主机名。
4. 使用配置第一个设备时每个字段完全相同的值配置此屏幕上的所有参数(包括在第一个设备上可能已更改的所有高级参数), 但以下参数除外:
  - **同步环 1 (eth2) 单播 IP 地址:** 输入与您在主要设备上的此字段中配置的 IP 地址不同的 IP 地址, 但是该地址必须与主要设备上提供的“同步环 1 单播”地址位于同一个子网中。
  - **同步环 2 (eth3) 单播 IP 地址:** 输入与您在主要设备上的此字段中配置的 IP 地址不同的 IP 地址, 但是该地址必须与主要设备上提供的“同步环 2 单播”地址位于同一个子网中。
  - **配对节点主机名:** 在此字段中输入主 UDP 导向器的主机名。
  - **配对节点同步环 1(eth2) IP 地址:** 在此字段中输入主 UDP 导向器的 Eth2 IP 地址。
  - **配对节点同步环 1(eth3) IP 地址:** 在此字段中输入主 UDP 导向器的 Eth3 IP 地址。
5. 点击 **应用 (Apply)** 以保存更改, 并在此设备上启动集群服务。
6. 点击 **升级 (Promote)** 指定主设备。
7. **重新启动:** 选择 **操作 (Operations) > 重新启动设备 (Restart Appliance)**。

# 11. 安装桌面客户端

 从 v7.4.0 开始, SMC 已重命名为 管理器。SMC 在本节中称为 管理器。

 如果您的 Cisco Secure Network Analytics 系统仅部署了 Data Store 流收集器, 则不会使用 桌面客户端。对于混合 Data Store/非 Data Store 系统, 桌面客户端 将仅适用于非 Data Store 域。

以下信息适用于安装和使用桌面客户端:

- 可以在本地安装不同版本的桌面客户端。
- 桌面客户端包括 **Stealthwatch** 术语, 例如 **Stealthwatch** 管理控制台 和 **SMC**( 管理器)。
- 如果要访问多个版本的桌面客户端, 则每个 管理器 都需要不同的可执行文件。
- 如果您同时使用主和辅助 管理器, 则需要先注销一个 管理器, 然后才能登录另一个 管理器。
- 可以同时打开不同版本的桌面客户端。
- 更新到更高版本的 **Cisco Secure Network Analytics** 时, 需要安装新版本的桌面客户端。
- 如果要部署 **Data Store**, 请使用 **Web** 应用监控和配置 **Cisco Secure Network Analytics** 安装。桌面客户端与 **Data Store** 不兼容。

安装桌面客户端的说明因您使用的是 **Windows** 还是 **macOS** 而异:

- [使用 \*\*Windows\*\* 安装 桌面客户端](#)
- [使用 \*\*macOS\*\* 安装桌面客户端](#)



您还将以不同方式更改内存大小, 具体取决于您使用的是 **Windows** 还是 **macOS**:

- [从 \*\*Windows\*\* 资源管理器更改内存大小](#)
- [从查找器更改内存大小](#)


## 使用 Windows 安装 桌面客户端

- 您必须具有足够的权限才能安装桌面客户端。
- 桌面客户端需要 64 位的操作系统，它不能在 32 位的操作系统或 Linux 上运行。

按照以下说明使用 Windows 安装桌面客户端：

1. 登录管理器。
2. 点击  (下载) 图标。
3. 点击 .exe 文件以开始安装过程。
4. 按照向导中的步骤安装桌面客户端。
5. 在桌面上，点击“桌面客户端”图标 。
6. 在 **SMC 服务器名称** 字段，输入 管理器 服务器名称或 IP 地址 (IPv4 或 IPv6)。
7. 输入 管理器 用户名和密码。
8. 按照屏幕上的提示打开桌面客户端并信任设备身份证书。

### 从 Windows 资源管理器更改内存大小

 您可以更改在客户端计算机上分配的随机访问内存 (RAM) 量以运行桌面客户端界面。

如果您处理多个打开的文档或大数据集(例如，对超过 10 万条记录进行流查询)，请考虑分配更大的内存。

1. 在 Windows 资源管理器中，转至主目录。
2. 打开以下文件夹: AppData > 漫游 > Stealthwatch。  
如果此文件夹处于隐藏状态，您可能需要搜索“Stealthwatch”。
3. 在 Stealthwatch 目录中，打开包含所需 Stealthwatch 版本的文件夹。
4. 使用适当的编辑应用打开 **application.vmoptions** 文件以开始编辑。(首次打开桌面客户端后，系统会创建此文件。)

**最小内存大小 (Xms):** 建议分配的内存不低于 512 MB。此数字列在文件的第三行。对于以一个连续行显示内容的编辑器，请参阅下图中突出显示的数字，以查看哪个数字代表最小内存大小。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

**最大内存 (Xmx):** 对于最大内存大小，最多可以分配计算机 RAM 大小的一半。此数字列在文件的第四行。

对于以一个连续行显示内容的编辑器, 请参阅下图中突出显示的数字, 以查看哪个数字代表最大内存大小。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```


请使用整数。例如, 输入 `Xmx512m`, 而不是 `Xmx0.5m`。

- 如果您发现桌面客户端似乎经常“挂起”, 请尝试增加内存大小。
- 如果您收到涉及 **Java** 的错误消息, 请尝试选择较低的内存分配。

## 使用 macOS 安装桌面客户端



- 您必须具有足够的权限才能安装桌面客户端。
- 桌面客户端需要 64 位的操作系统, 它不能在 32 位的操作系统或 Linux 上运行。

按照以下说明使用 macOS 安装桌面客户端:


1. 登录管理器。
2. 点击  (下载) 图标。
3. 点击 .dmg 文件以开始安装过程。

显示器上会显示一个图标和文件夹, 如下所示。



4. 将桌面客户端图标 () 拖入“应用”文件夹中。  
该图标随即添加到启动板中。
5. 在桌面上, 点击“桌面客户端”图标 .
6. 在 **SMC 服务器名称** 字段, 输入 管理器 服务器名称或 IP 地址 (IPv4 或 IPv6)。
7. 输入 管理器 用户名和密码。
8. 按照屏幕上的提示打开桌面客户端并信任设备身份证书。

### 从查找器更改内存大小

-  您可以更改在客户端计算机上分配的随机访问内存 (RAM) 量以运行桌面客户端界面。

如果您处理多个打开的文档或大数据集(例如, 对超过 10 万条记录进行流查询), 请考虑分配更大的内存。

1. 在查找器中, 转至主目录。
2. 打开 **Stealthwatch** 文件夹。
3. 在 **Stealthwatch** 目录中, 打开包含所需 **Stealthwatch** 版本的文件夹。
4. 使用适当的编辑应用打开 **application.vmoptions** 文件以开始编辑。(首次打开桌面客户端后, 系统会创建此文件。)

**最小内存大小 (Xms):** 建议分配的内存不低于 **512 MB**。此数字列在文件的第三行。对于以一个连续行显示内容的编辑器, 请参阅下图中突出显示的数字, 以查看哪个数字代表最小内存大小。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

**最大内存大小 (Xmx):** 对于最大内存大小, 最多可以分配计算机 RAM 大小的一半。此数字列在文件的第四行。

对于以一个连续行显示内容的编辑器, 请参阅下图中突出显示的数字, 以查看哪个数字代表最大内存大小。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

**请使用整数。**例如, 输入 **Xmx512m**, 而不是 **Xmx0.5m**。

- 如果您发现桌面客户端似乎经常“挂起”, 请尝试增加内存大小。
- 如果您收到涉及 **Java** 的错误消息, 请尝试选择较低的内存分配。

## 12. 验证管理器(原 SMC)故障转移角色

**提醒:**从 v7.4.0 开始, SMC 已重命名为 管理器。SMC 在本节中称为 管理器。

**警告:**在更新两个 管理器 之前, 请勿更改故障转移角色。

**警告:**在完成故障转移配置并确认辅助 管理器 设备状态在“集中管理”中显示为**已连接**之前, 请勿在“集中管理”中添加或删除设备。

使用以下说明确认主 管理器 和辅助 管理器 在更新后保留了其角色。

1. 作为管理员用户登录**辅助** 管理器。
2. 选择**配置 (Configure) > 全局管理器 (GLOBAL Manager)**。
3. 点击**故障转移配置 (Failover Configuration)**选项卡。
4. 确认**故障转移角色 (Failover Role)**显示为**辅助 (Secondary)**。

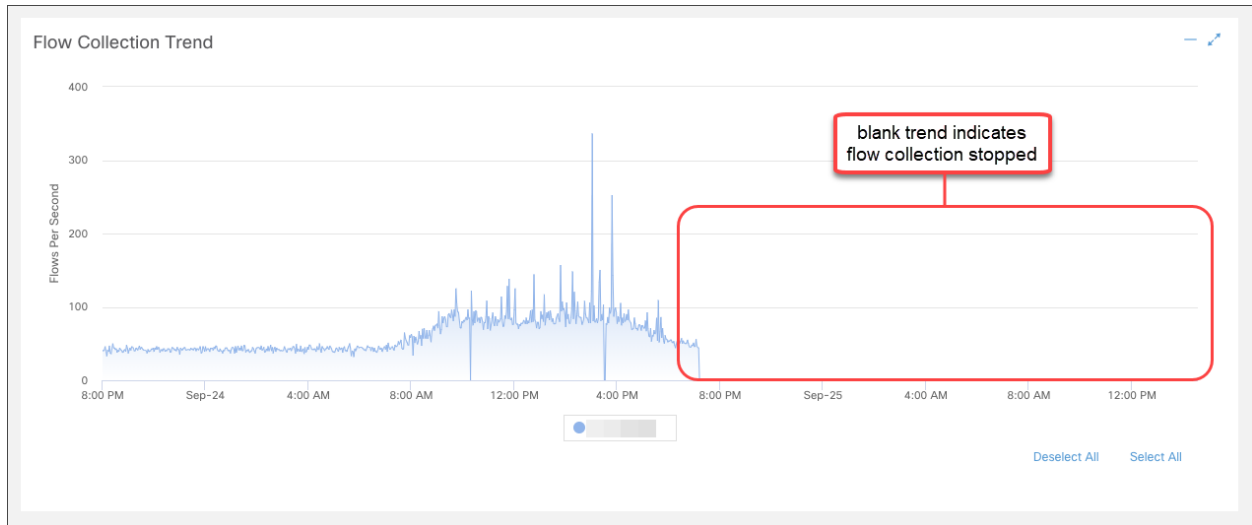
The screenshot shows the 'Manager Configuration' interface. At the top, there are fields for Name, IP Address (121), Model, and Serial. Below this, there are tabs for Data Retention, DSCP Configuration, and Failover Configuration. The Failover Configuration tab is active, showing a 'Failover Configuration' section with a 'Cancel' and 'Save' button. A blue informational message states: 'Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).' Below this, the 'Failover Role\*' dropdown menu is set to 'Secondary' and is highlighted with a red box. At the bottom, there is an 'Other Manager' section with fields for IP Address (141) and Failover Role (Primary).

5. 登录**主** 管理器。按照步骤 2 至 4 确认**故障转移角色 (Failover Role)**显示为**主 (Primary)**。
6. 如果两个 管理器 均显示为辅助 SMC, 请更改故障转移角色, 以便拥有一个主 管理器 和一个辅助 管理器。请确保遵循 [《故障转移配置指南》](#)中的配置顺序和说明。

**提醒:**有关说明, 请参阅 [《故障转移配置指南》](#)。

7. 登录**辅助**管理器。
8. 查看流收集趋势。





9. 如果流收集正在进行，则无需进一步操作。转至下一步。

如果流收集停止，将使用“集中管理”来重新启动流量收集器和辅助管理器。

- 登录到主管理器。
- 选择配置 (Configure) > 全局集中管理 (GLOBAL Central Management)。
- 在清单中找到流量收集器。
- 点击 ⋮ (省略号) 图标。
- 选择重新启动设备。按照屏幕上的提示进行操作。
- 流量收集器：重复这些步骤以在“集中管理”中重新启动每个流量收集器。
- 辅助管理器：重复这些步骤以重新启动辅助管理器。

10. 登录到主管理器。

11. 查看集中管理清单。确认辅助管理器设备状态显示为已连接。

## 联系支持人员

如果需要技术支持人员, 请执行以下操作之一:

- 联系您当地的思科合作伙伴
- 联系思科支持
- 通过以下网址反映问题: <http://www.cisco.com/c/en/us/support/index.html>
- 通过以下邮箱反映问题: [tac@cisco.com](mailto:tac@cisco.com)
- 美国支持电话: 1-800-553-2447
- 全球支持电话: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

## 更改历史记录

文档版本	发布日期 (Published Date)	说明
1_0	2023年3月1日	初始版本
1_1	2023年3月27日	更新了已知问题部分。
2_0	2023年5月26日	更新了分析和终端许可证和网络可视性模块增强功能部分。
3_0	2023年10月12日	添加了更换未过期的 <i>Cisco</i> 自签名设备身份证 书(证书更新)部分。 更新了已知问题部分。
3_1	2023年10月20日	添加了 VMware 8.0 支持。

---

## 版权信息

思科和思科徽标是思科和/或其附属机构在美国和其他国家/地区的商标或注册商标。要查看思科商标列表,请访问以下 URL: <https://www.cisco.com/go/trademarks>。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1721R)

