Cisco Secure Network Analytics

系统配置指南 7.4.2

目录

简介

概述

使用本指南将以下思科 Cisco Secure Network Analytics (前称 Stealthwatch) 硬件和虚拟版 (VE) 设备配置到 v7.4.2 中的一个托管系统：

- Cisco Secure Network Analytics 管理器 (以前称为 StealthWatch 管理控制台)
- Cisco Secure Network Analytics 数据节点
- Cisco Secure Network Analytics 流收集器
- Cisco Secure Network Analytics 流传感器
- Cisco Secure Network Analytics UDP 导向器

有关 Cisco Secure Network Analytics的详细信息，请参见以下在线资源：

- **概述：** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **设备：** https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html
- **发行说明：**有关详细信息，请参见发行说明。

受众

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

如果您希望与专业安装人员合作，请联系您当地的思科合作伙伴或思科支持。

安装要求

在使用本指南将 Cisco Secure Network Analytics 配置到受管系统之前，请使用以下指南安装硬件和虚拟设备：

硬件

- **硬件安装：**在开始此配置之前，使用 Cisco Secure Network Analytics x2xx 系列硬件安装指南 或 Cisco Secure Network Analytics x3xx 系列硬件安装指南 来安装设备硬件（物理设备）。
- **规格：**硬件规格 可在 Cisco.com 上找到。
- **支持的平台：**要查看每个系统版本的支持硬件平台，请参阅 Cisco.com 上的硬件和软件版本支持矩阵。

虚拟版 (VE) 设备

- **虚拟版安装：**在开始此配置之前，请使用 Cisco Secure Network Analytics 虚拟版安装指南 来安装虚拟设备。

快速参考概述

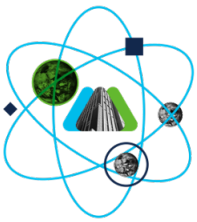
要成功安装，请按顺序执行以下程序。有关详细说明，请点击程序链接。

准备工作和 规划您的系统配置

确保您拥有配置设备和使用 Data Store 或不适用 Data Store 部署 Cisco Secure Network Analytics 所需的所有信息。

1. 使用首次设置配置环境

- **登录：**以 sysadmin 身份（密码：lan1cope）通过控制台登录到每个设备。在命令提示符下键入 `SystemConfig`。
- **带 Data Store 的流量收集器：**以 root 用户身份登录（密码：lan1cope）。
- **所需设备：**所有部署都需要管理器和 流收集器 。对于具有 Data Store 的部署，您还需要配置 数据节点（使用数据节点 内部通信）。



2. 配置受管系统

使用设备设置工具按顺序配置每个设备，以便由您的 管理器进行管理。您还将为设备创建 Data Store 域或非 Data Store 域。

- **设备设置工具：**在浏览器的地址字段中，键入 **https://** 再键入设备的 IP 地址。
- **登录：**管理员
- **密码：**lan411cope
- **系统管理员和 root 密码默认值：**lan1cope

按顺序配置设备。选中“集中管理”库存清单，并且，在开始配置您的集群中的下一个设备之前，请确认设备为 **已连接** (或 **Data Store 未初始化**)。

1. 主 管理器（集中管理）
2. 数据节点
3. 流量收集器 5000 系列数据库
4. 流量收集器 5000 系列引擎
5. 所有其他流量收集器

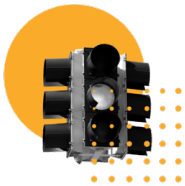
6. UDP 导向器
7. 流量传感器
8. 辅助 管理器

3. 定义 管理器 故障转移关系

- 如果您已配置主管理器和辅助管理器，则需要执行此程序。
- 使用故障转移在两个管理器之间建立故障转移对，以便其中一个控制台用作另一个的备用控制台。
- 按照Cisco Secure Network Analytics故障转移配置指南中的说明进行操作。

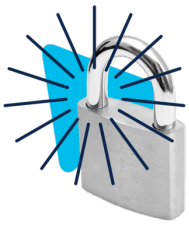
4. 配置站点冗余

- 此程序是可选的，需要您具有 Data Store。
- 使用站点冗余功能在包含单独部署且使用类似设备的两个 Cisco Cisco Secure Network Analytics 站点中跨集群建立近乎冗余。



5. 安装 v7.4.2 补丁

- 可以在 https://software.cisco.com的思科软件中心，从您的思科智能帐户中下载最新的 **v7.4.2 patches** 。
- 请确保按照补丁自述文件中的说明操作安装每个补丁。



6. 正在初始化 Data Store

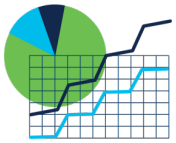
仅部署需要 Data Store 。

1. 以 root 用户身份登录管理器设备控制台 (SystemConfig)。
2. 选择 **Data Store** > **SSH**。
3. 选择 **Data Store** > **初始化**。

7. 安装桌面客户端

仅非 Data Store 部署需要。

- 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。
- 登录管理器。点击 (下载) 图标。



8. 验证通信

- 登录管理器。查看流收集趋势。
- 查看 Data Store 数据库状态以确认其已启动。(配置 > 全局集中管理 > Data Store 选项卡)
- 在报告生成器中运行报告，以确认在 流收集器 和 Data Store 中收到流。(报告 > 报告生成器 > 按流量收集器划分的流收集趋势报告、流数据库注入趋势报告)

9. 完成设备配置

- 流传感器 应用 ID 和负载(所有 流传感器都需要)
- UDP 导向器高可用性
- 其他可选设备配置

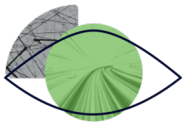
10. 配置遥测

启用其他遥测类型的 Data Store 部署需要。

- **NVM 流：**请确保按照 终端许可证和 Network Visibility Module (NVM) 配置指南中的说明操作
- **防火墙日志：**按照 安全分析和日志记录：防火墙事件集成指南中的说明在您的 管理器上安装应用。

11. 许可 Cisco Secure Network Analytics

- 在评估期结束前90天，在 https://software.cisco.com 上的思科智能账户中注册您的产品实例。
- 请按照 Cisco Secure Network Analytics智能软件许可指南中的说明操作。



12. 管理 Cisco Secure Network Analytics

登录到您的 管理器 并选择:

- **主机组:** 配置 > 检测主机组管理。
- **策略:** 配置 > 检测 策略管理。
- **流搜索:** 调查 > 流搜索。
- **报告:** 控制面板 > 报告生成器。
- **用户管理:** 配置 > 全局用户管理
- **说明:** 从任何页面选择 ?(**帮助**)图标 > **帮助** 。并且,请参阅《管理环境、调查行为和应对威胁》。

查看其他配置、维护和故障排除指南,包括:

- 分析
- 应用
- 身份验证/授权
- 域
- 密码
- SSL/TLS 设备身份和其他 SSL/TLS 客户端身份
- 威胁源
- 集中管理(管理设备)
- Data Store 数据库
- Data Store 维护
- 将 Data Store 添加到非 Data Store 部署和过渡 流量收集器
- 故障排除

准备工作

在开始配置流程之前，请查看本指南以了解此流程以及计划配置所需的准备工作、时间和资源。

术语

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

“**集群**” 是指由 管理器管理的一组 Cisco Secure Network Analytics 设备。

缩写

本指南中可能会出现以下缩写：

缩写	定义
DNS	域名系统(服务或服务器)
dvPort	分布式虚拟端口
ESX	企业服务器 X
GB	千兆字节
IDS	入侵检测系统
IPS	入侵防御系统
ISO	国际标准组织
IT	信息技术
KVM	基于内核的虚拟机
MTU	最大传输单位
NTP	网络时间协议
TB	兆兆字节
UUID	全局唯一标识符
VDS	vNetwork 分布式交换机

缩写	定义
VE	虚拟版
VLAN	虚拟局域网
虚拟机	虚拟机

配置详情

Cisco Secure Network Analytics 系统配置包括如下内容：

- **要求：**您可以使用 Data Store 配置 Cisco Secure Network Analytics，而不使用 Data Store 或混合部署（Data Store Data Store 域）。请参阅 **规划您的系统配置**以查看设备配置和域要求。
- **配置顺序：**确保按照本指南中的说明并按照设备设置工具指定顺序来 配置设备 。
- **证书：**设备安装有一个唯一的自签名设备身份证书。
- **集中管理：**您可以从主 管理器/集中管理器来管理设备。

下载软件

使用思科软件中心下载虚拟设备 (VE) 安装文件、补丁和软件更新文件。访问 https://software.cisco.com 登录您的思科智能账户，或者联系您的管理员。

密码要求

在系统配置期间，您将替换默认密码并为以下内容创建新密码：

用户	默认密码
admin	lan411cope
root	lan1cope
sysadmin	lan1cope
dbadmin	您将在初始化 Data Store时分配密码。
readonlyuser	您将在初始化 Data Store时分配密码。
CIMC 管理员	要远程访问硬件设备，请登录 CIMC。如果您尚未配置 CIMC，请遵循 思科 UCS C 系列集成管理控制器 GUI 配置指南中的说明进行操作。

	默认密码为 **password**。请确保在首次登录时进行更改。

许可

要许可Cisco Secure Network Analytics，您将使用智能账户注册产品实例、管理许可证、运行报告和配置通知。访问 https://software.cisco.com 登录您的思科智能账户，或者联系您的管理员。

在评估模式下使用 Cisco Secure Network Analytics 时，可在 90 天内使用选定功能。要使用 Cisco Secure Network Analytics 和最大范围的默认功能并将许可证和功能添加到您的帐户，请注册您的产品实例以获取智能软件许可。请参阅 **11. 许可 Cisco Secure Network Analytics** 了解详细信息。

> ⚠ 确保在 90 天评估期到期之前注册您的产品实例。当评估期到期时，系统将停止流收集。要再次启动流收集，请注册您的产品实例。

TLS

Cisco Secure Network Analytics 需要 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。

浏览器

Cisco Secure Network Analytics 支持最新版本的 Chrome、Firefox 和 Edge。

主机名

每个设备都需要有唯一主机名。我们无法配置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。

域名

每个设备都需要有完全限定域名。我们无法安装具有空域的设备。

NTP 服务器

- **配置：**每个设备至少需要 1 台 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

所有 Cisco Secure Network Analytics 设备均使用协调世界时 (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时间。

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

规划您的系统配置

在开始配置之前，请查看说明，以便了解在“首次设置”中配置设备并在“设备设置工具”中将其配置到一个受管系统中的规划、时间和要求。

系统配置要求

咨询网络架构师和管理员，确认 v7.4.2 Cisco Secure Network Analytics 部署的详细信息。有关配置要求，请参阅每个部分：

- **Cisco Secure Network Analytics 具有 Data Store**
- **Cisco Secure Network Analytics 不具有 Data Store**
- **Cisco Secure Network Analytics 混合部署**
- **规划您的系统配置**

Cisco Secure Network Analytics 具有 Data Store

在具有 Data Store 的 Cisco Secure Network Analytics 中，流收集器 将其遥测数据发送到 Data Store 数据节点进行存储。

- **数据节点的数量：** Data Store 可以包括 1 个数据节点（单数据节点部署）或 3 个或更多数据节点（多数据节点部署）。不支持只有 2 数据节点的 Data Store 。
- **硬件或虚拟：** 确保您的 数据节点为同样的类型：全部为硬件或全部为虚拟版。
- **大小：** 确保您的 数据节点虚拟版使用的配置文件大小相同，以便具有相同的 RAM、CPU 和磁盘空间。有关详细信息，请参阅 虚拟设备安装指南 。
- **遥测注入：** 除了 NetFlow，您还可以为 NVM 流（网络可视性模块）和防火墙日志配置遥测注入。

要成功配置，请注意以下事项：

1. 在 首次设置中，为 Data Store 配置设备。请确保配置以下设备：
    - **管理器：** 请参阅 **配置 管理器**
    - **流量收集器：** 请参阅 **配置具有 Data Store 的 流收集器**
    - **数据节点：** 请参阅 **配置 数据节点**
2. 在 管理器 设备设置工具中，确保为 Cisco Secure Network Analytics 设备 创建 Data Store 域 。
3. 要为 NVM 流和防火墙日志启用遥测采集，请确保完成 **10. 配置遥测**。

Cisco Secure Network Analytics 不具有 Data Store

在不具有 Data Store 的 Cisco Secure Network Analytics 中，流收集器 将其遥测 Data Store 在本地 流收集器 或 流收集器数据库 上（仅限 5000 系列）。

要成功配置，请注意以下事项：

1. 在 首次设置中，请确保配置以下设备：
   - **管理器：** 请参阅 **配置 管理器**
   - **流量收集器：** 请参阅 **配置不具有 Data Store**
2. 在 管理器 设备设置工具中，确保为 Cisco Secure Network Analytics 设备 创建非 Data Store 域 。

完成受管系统的配置后，您可以在未来将 Data Store 添加到部署中（有关说明，请参阅 **将 Data Store 添加到非 Data Store 部署**）。

您也可以将现有 流收集器转换为使用 Data Store 数据库，而不会丢失转换前的数据或可视性。这样做可以利用仅在 Data Store 中可用的功能。有关详细信息，请参阅 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器**

Cisco Secure Network Analytics 混合部署

在具有混合配置的 Cisco Secure Network Analytics 中，您可以配置特定流量收集器以将遥测发送到 Data Store 数据节点进行存储，还可以配置其他 流收集器在 流收集器 或 流收集器数据库 上本地存储遥测（仅限 5000 系列）。

要成功配置，请按以下顺序配置设备和域：

1. 在 首次设置中，配置不具有 Data Store 的设备。请确保配置以下设备：
   - **管理器：** 请参阅 **配置 管理器**
   - **流量收集器：** 请参阅 **配置不具有 Data Store**
2. 在 管理器 设备设置工具中，确保为 Cisco Secure Network Analytics 设备 创建非 Data Store 域 。
3. 完成 **9. 完成设备配置** 以完成非 Data Store 域的初始系统配置。
4. 按照 **将 Data Store 添加到非 Data Store 部署**中的说明进行操作。您将创建一个 Data Store 域并向其添加 流收集器和 数据节点。

设备配置要求

在首次设置中配置每个设备需要以下信息。您还将使用此信息通过设备设置工具将设备配置为受管系统。

配置要求	详细信息	设备
IP 地址	将可路由 IP 地址分配给 `eth0` 管理端口。	
网络掩码		
网关		
主机名	每个设备都需要有唯一主机名。我们无法配置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。	
域名	每个设备都需要有完全限定域名。我们无法安装具有空域的设备。	
DNS 服务器	用于名称解析的内部 DNS 服务器	
NTP 服务器	用于在服务器之间同步的内部时间服务器。每个设备至少需要 1 台 NTP 服务器。 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。	
邮件中继服务器	用于发送警报和通知的 SMTP 邮件服务器	
流收集器 导出端口	仅流量收集器需要。 Netflow 默认值：2055	
专用 LAN 或 VLAN 中的不可路由 IP 地址（用于数据节点 间通信）	仅数据节点需要。 • 硬件 eth2 或 eth2 和 eth3 的绑定。创建 LACP `eth2/eth3` 绑定端口通道以实现高达 20G 的吞吐量，可加快数据节点相互之间的通信，并加快	

	将 数据节点 添加或替换到 Data Store。请注意，LACP 端口绑定是唯一可用于硬件 数据节点的绑定选项。 • 虚拟 eth1 **IP 地址：**您可以使用提供的 IP 地址，也可以输入满足以下数据节点 通信要求的值。 • 来自 **169.254.42.0/24 CIDR 块**的**不可路由 IP 地址**，介于 169.254.42.2 和 169.254.42.254 之间。 • **前三个八位组：**169.254.42 • **子网：**/24 • **顺序：**为便于维护，请选择顺序 IP 地址（例如 169.254.42.10、169.254.42.11 和 169.254.42.12）。 **网络掩码：** 网络掩码硬编码为 255.255.255.0，无法修改。	
eth0 硬件连接端口	仅适用于具有 Data Store 硬件设备的 Cisco Secure Network Analytics： • 管理器 2210 • 流量收集器 4210 • 数据节点s eth0 硬件连接端口选项： • **SFP+**：SFP+：用于 eth0 的 10G SFP+/DAC 光纤端口。 • **BASE-T**：100Mbs/1GbE/10GbE eth0 的 BASE-T 铜缆端口。BASE-T 是默认设置。	

连接到硬件(物理)设备

使用思科集成管理控制器 (CIMC)、键盘和显示器或串行电缆或串行控制台连接到设备。有关说明，请参阅 x2xx 系列硬件安装指南 或 Cisco Secure Network Analytics x3xx 系列硬件安装指南。

CIMC 访问

要进行远程访问，请登录 CIMC。如果您尚未配置 CIMC，请遵循 思科 UCS C 系列集成管理控制器 GUI 配置指南中的说明进行操作。

默认密码为 **password**。请确保在首次登录时进行更改。

连接到虚拟版设备

1. 连接到虚拟机监控程序主机(虚拟机主机)。
2. 在虚拟机监控程序主机中，找到您的虚拟机。
3. 确认虚拟机未接通电源。

   如果虚拟机未启动，并且您收到有关可用内存不足的错误消息，请执行以下操作之一：

   - **资源：**增加安装设备的系统上的可用资源。有关详细信息，请参阅 虚拟版设备安装指南 中的 **资源要求** 。
   - **VMware 环境：**提高设备及其资源池的内存预留限制。

> 查看资源要求以分配足够多的资源。这一步对于系统性能至关重要。
>
> 如果您选择部署思科 Cisco Secure Network Analytics 设备而没有要求的资源，则必须负责密切监控设备的资源利用率，并根据需要增加资源，以确保部署正常运行。

4. 访问虚拟机控制台。允许虚拟设备完成启动。

> 根据 VM 主机的速度，所有服务可能需要大约 30 分钟才能启动。

1. 使用首次设置配置环境

按照以下说明完成每个设备的基础环境配置。无论是硬件(物理)设备还是虚拟版 (VE) 设备，您都可以在“首次设置”中按任意顺序配置设备。

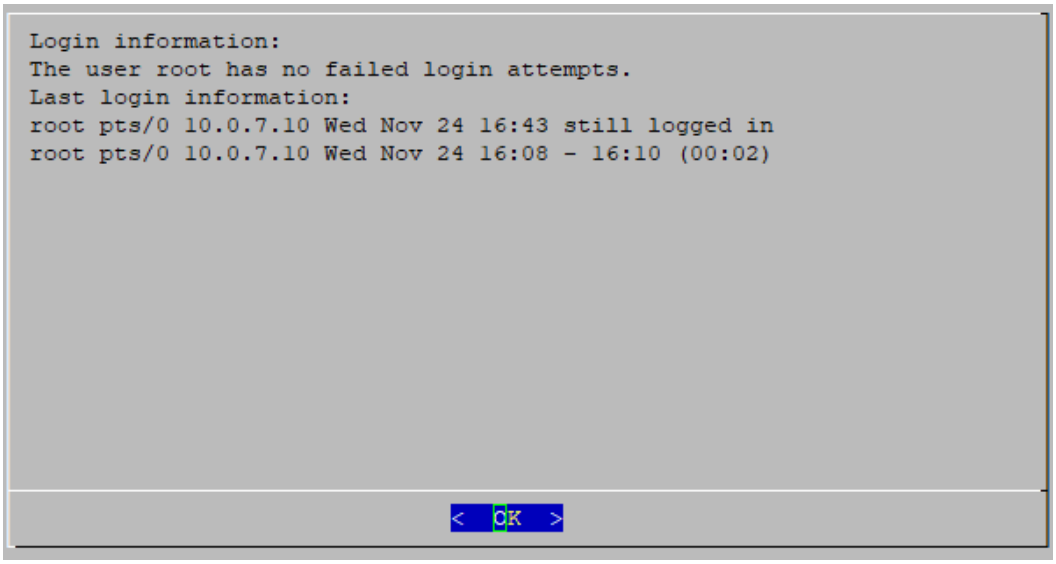
> 在开始这些配置程序之前，请查看 **规划您的系统配置** 。

设备配置概述

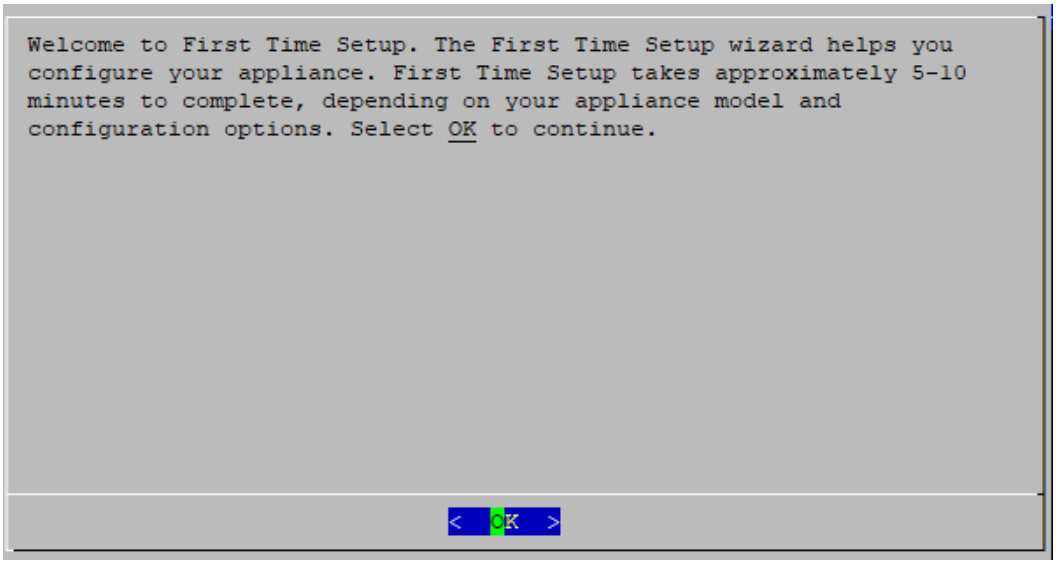
设备说明	Data Store 必须使用	说明
配置 管理器	是	使用 Data Store 和不使用 Data Store 的部署都需要 管理器 。
配置 数据节点	是	您可以部署 1 个数据节点(单数据节点部署)或 3 个或更多数据节点(多数据节点部署)。 不支持仅部署 2 个 数据节点。 确保您的数据节点全部为硬件或全部为虚拟版本。并且，确保您的 数据节点 虚拟版使用的配置文件大小相同，以便具有相同的 RAM、CPU 和磁盘空间。有关详细信息，请参阅 虚拟设备安装指南 。
配置具有 Data Store 的 流收集器	是	流收集器 将其遥测发送到 Data Store 数据节点进行存储。您还将确认要采集的遥测类型。
配置不具有 Data Store		流收集器 将其遥测数据存储在本地 流收集器 或 流收集器数据库 上(仅限 5000 系列)。
配置 流传感器 或 UDP 导向器		流传感器和 UDP 导向器可选。 要安装 思科遥测代理 而不是 UDP 导向器，请按照本指南中的说明完成系统配置。然后，按照 遥测代理虚拟设备部署和配置指南中的指示。

配置 管理器

1. 通过控制台登录管理器。
    - **登录名**:sysadmin
    - **默认密码**:lan1cope
    - 配置系统时,您将更改默认密码。
2. 系统配置 (`SystemConfig`) 将打开。
3. 查看失败的登录尝试信息。选择**确定 (OK)** 继续。

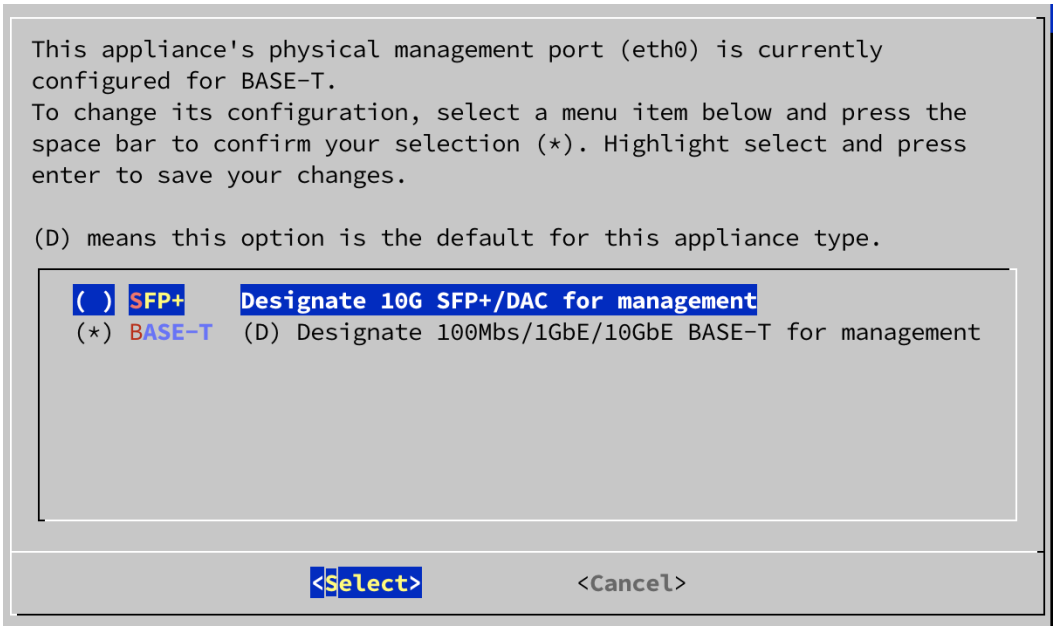


4. 查看首次设置简介。选择**确定 (OK)** 继续。



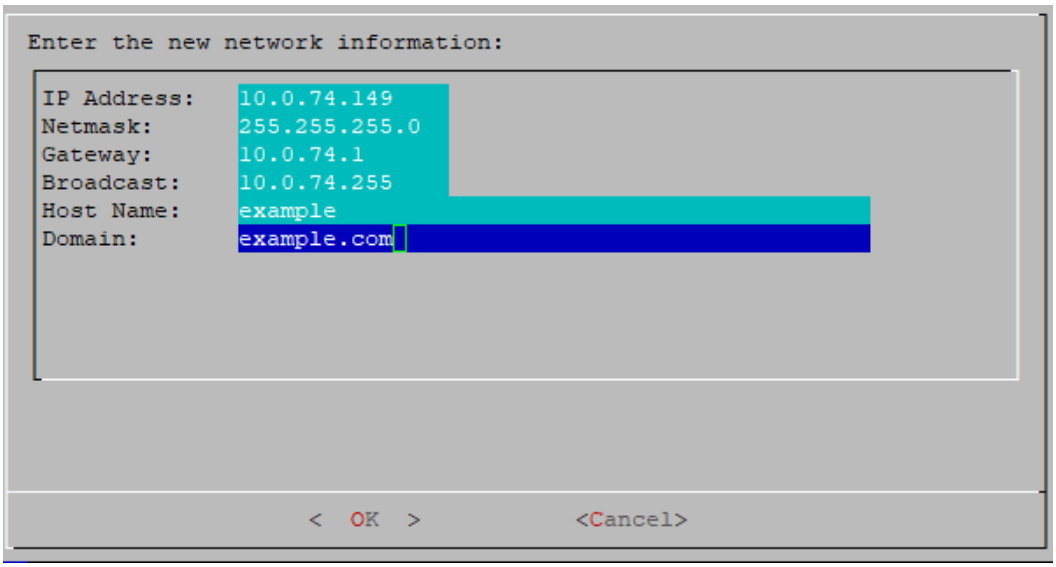
5. **eth0 的端口顺序配置(仅 2210 硬件)**：选择以下选项之一：

   - **SFP+**：配置设备以使用 eth0 的 10G SFP+/DAC 光纤端口。
   - **BASE-T**：将设备配置为使用eth0的 BASE-T 铜缆端口。BASE-T 是默认设置。

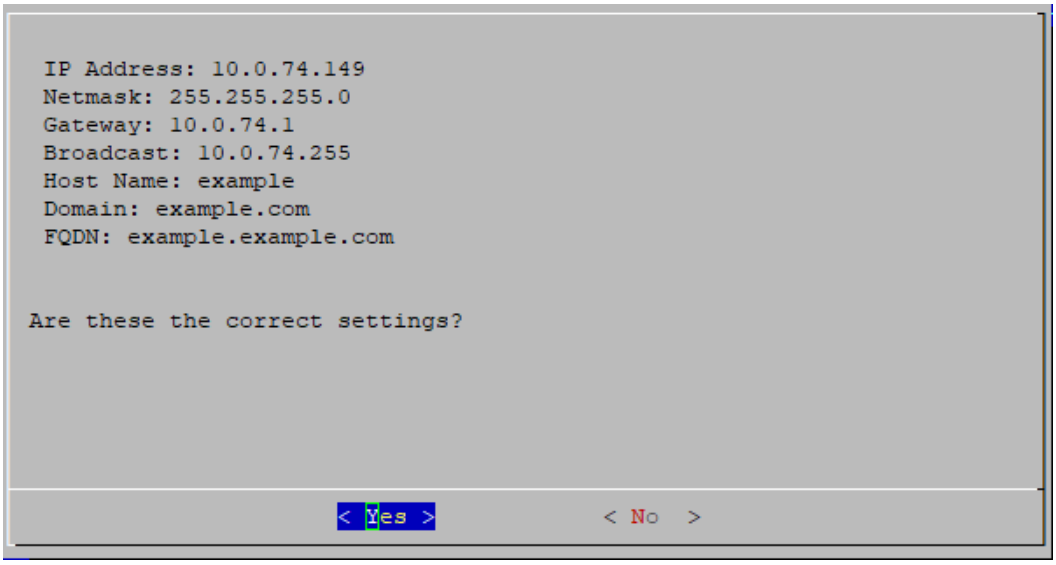


6. 输入管理接口 **IP 地址** (eth0)、**网络掩码**、**网关**、**广播**、**主机名**和 **域**，然后选择 **确定**继续。

> ⚠ 每个设备都需要有唯一主机名。我们无法配置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。



7. 确认设置。选择**是 (Yes)** 继续。



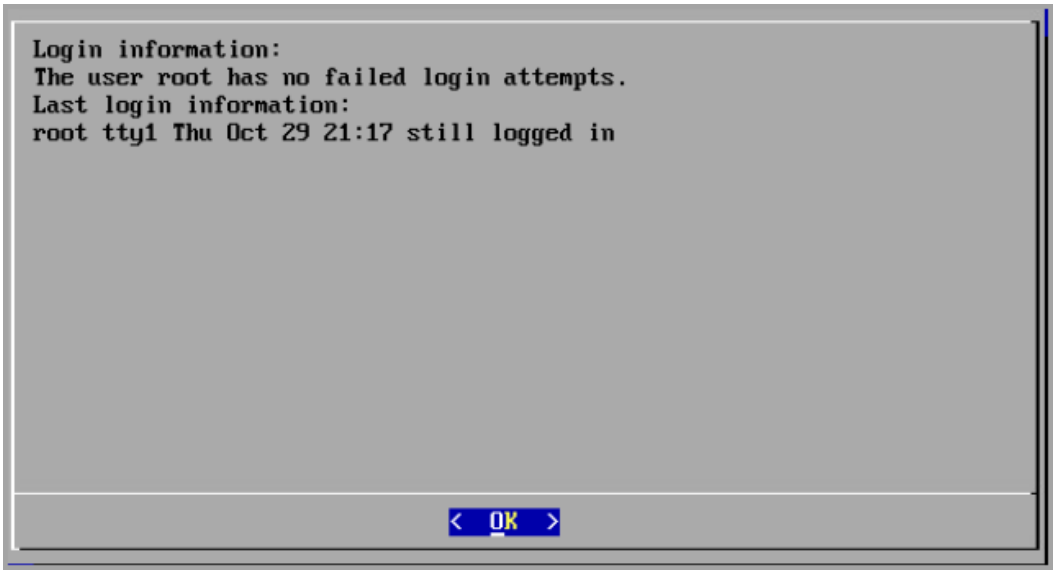
8. 选择**确定 (OK)** 确认您的选择。按照屏幕提示完成虚拟环境并重新启动设备。
9. 按 **Ctrl + Alt** 退出控制台。
10. 对系统中的下一个 管理器 重复 **配置 管理器** 中的所有步骤。

    如果您已在首次设置中配置了所有 管理器，请返回到 **设备配置概述** 并配置您的流收集器和其他设备。

配置 数据节点

您可以部署 1 个数据节点(单数据节点部署)或 3 个或更多数据节点(多数据节点部署)。不支持仅部署 2 个 数据节点。

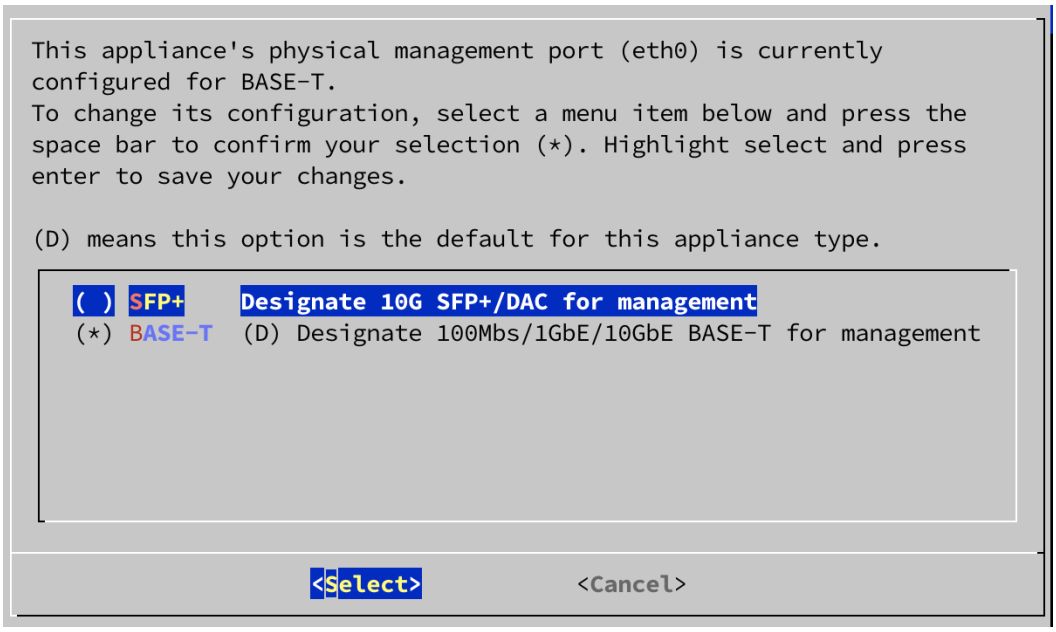
1. 通过控制台登录 数据节点 。
    - **登录:**sysadmin
    - **默认密码:**lan1cope
    - 配置系统时,您将更改默认密码。
2. 系统配置 (`SystemConfig`) 将打开。
3. 查看失败的登录尝试信息。选择**确定 (OK)** 继续。



4. 查看首次设置简介。选择**确定 (OK)** 继续。

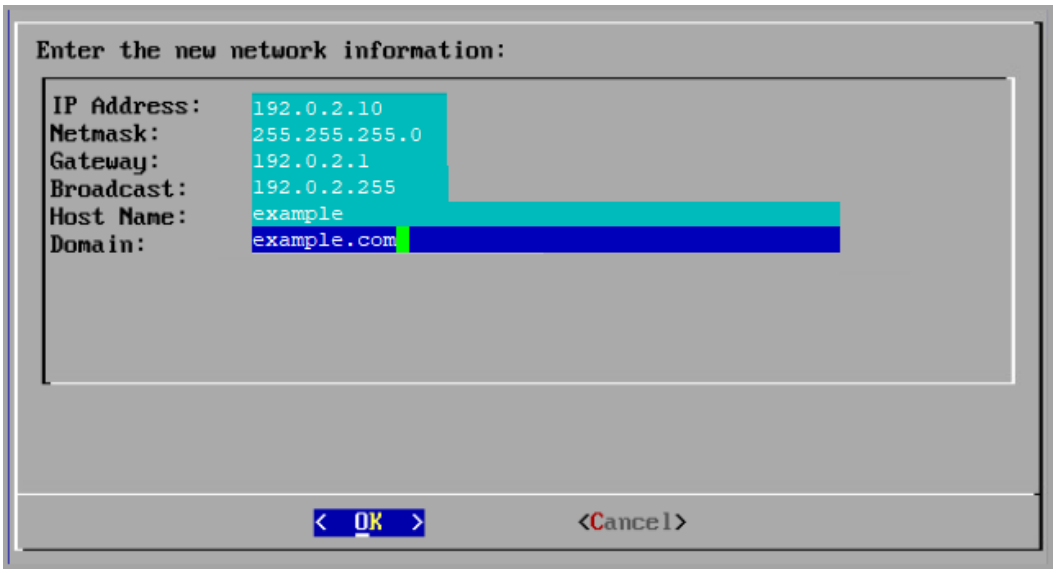
5. **eth0 的端口顺序配置(仅限 Data Store 6200 硬件)：**选择以下选项之一：

   - **SFP+**：配置设备以使用 eth0 的 10G SFP+/DAC 光纤端口。
   - **BASE-T**：将设备配置为使用eth0的 BASE-T 铜缆端口。BASE-T 是默认设置。

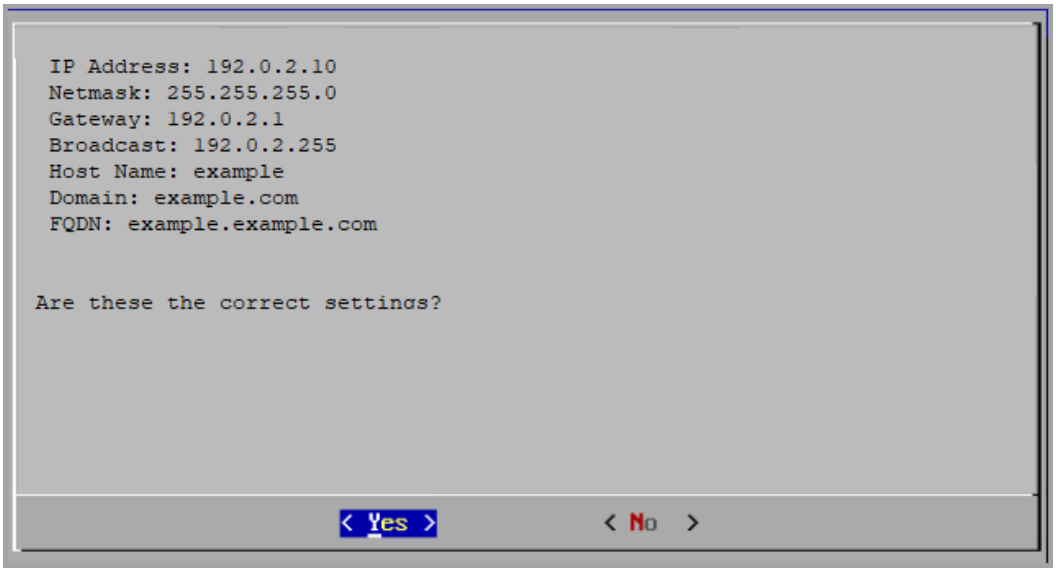


6. 输入管理接口 **IP 地址**、**网络掩码**、**网关**、**广播**、**主机名**和**域**，然后选择**确定 (OK)** 继续。

> ⚠ 每个设备都需要有唯一主机名。我们无法配置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。



7. 确认设置。选择**是 (Yes)** 继续。



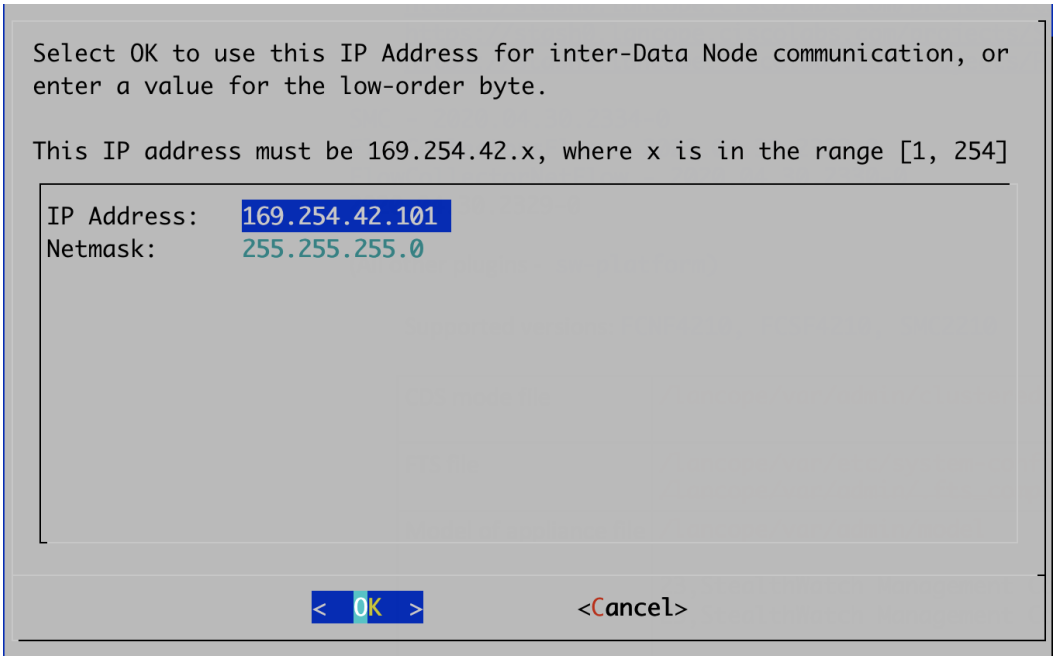
8. 选择**确定 (OK)** 确认您的选择。按照屏幕上的提示进行操作。

9. **为数据节点 内部通信配置物理端口 (eth2) 或端口通道(eth2 和 eth3)。**

> 对于硬件 数据节点，配置 `eth2` 端口以实现10G吞吐量足以实现正常的数据节点 间通信。创建 LACP `eth2/eth3` 绑定端口通道以实现高达 20G 的吞吐量，可加快 数据节点相互之间的通信，并加快将 数据节点 添加或替换到 Data Store，因为每个新 数据节点 会接收来自相邻 数据节点的流量以填充其数据。请注意，LACP 端口绑定是唯一可用于硬件 数据节点的绑定选项。

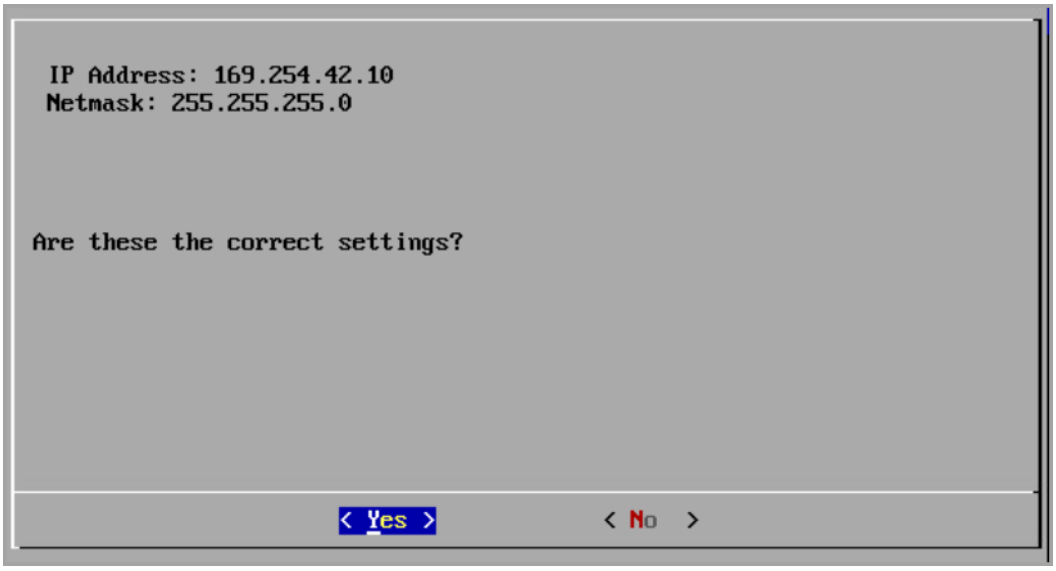
输入以下命令：

字段	要求
IP 地址	使用 **提供的 IP 地址** 或 **输入值**，该值满足以下数据节点内部通信的 eth2 和 eth3 接口要求的值。 • 来自 **169.254.42.0/24 CIDR 块**的**不可路由 IP 地址**，介于 169.254.42.2 和 169.254.42.254 之间。 • **前三个八位组：** 169.254.42 • **子网：** /24 • **顺序：** 为便于维护，请选择顺序 IP 地址(例如 169.254.42.10、169.254.42.11 和 169.254.42.12)。
Netmask	255.255.255.0



10. 选择**确定 (OK)** 继续。

11. 确认设置。选择**是 (Yes)** 继续。



12. 按照屏幕提示完成环境并重新启动设备。
13. 按 **Ctrl + Alt** 退出控制台。
14. 对系统中的下一个 数据节点 重复 **配置 数据节点** 中的所有步骤。

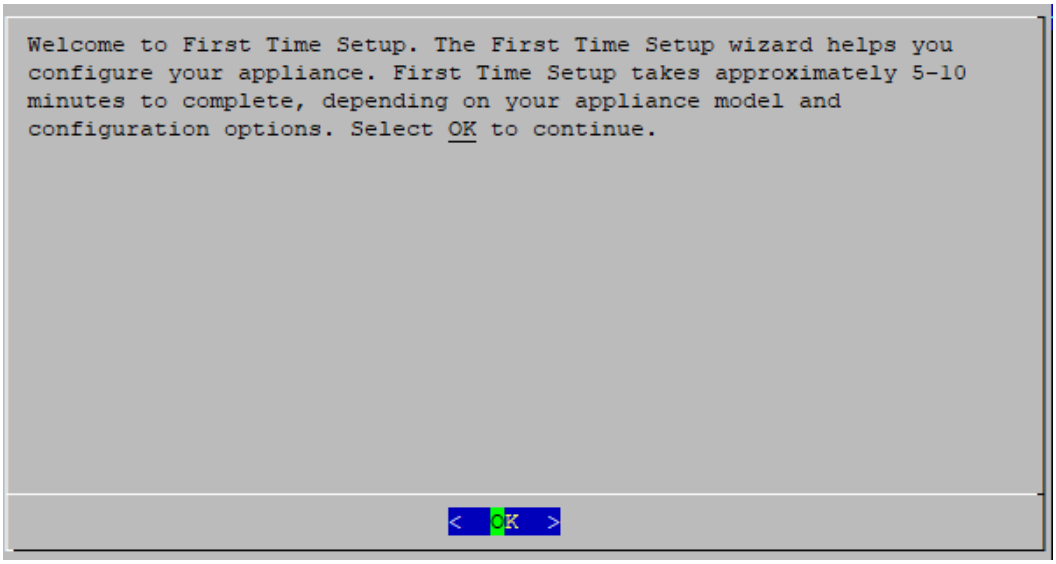
    - 如果您已在首次设置中配置了所有 数据节点，请转至下一部分并使用 Data Store 配置您的 流收集器，或返回到 **设备配置概述** 并配置其他设备。
    - 如果您已在首次设置中配置了所有设备，请转至 **2. 配置受管系统**。

配置具有 Data Store 的 流收集器

如果将 流收集器 配置为与Data Store 配合使用，则 流收集器 会将其遥测发送到 Data Store 数据节点进行存储。您还将确认要采集的遥测类型。

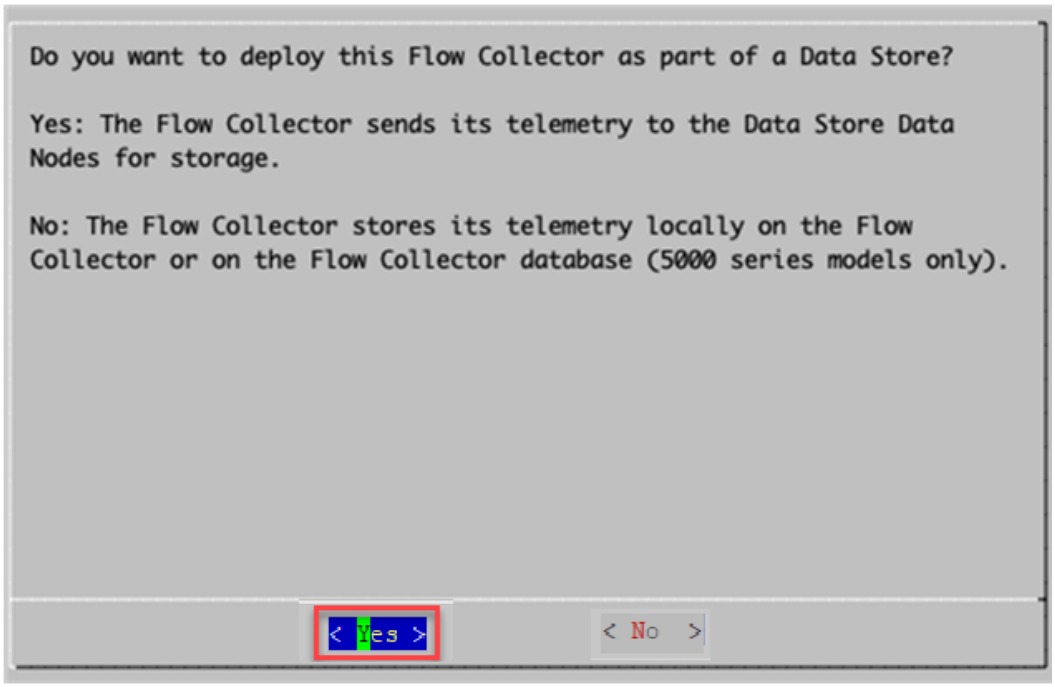
> 从 v7.4.2 开始，您可以将非Data Store 流收集器转换为 Data Store 流收集器。有关详细信息，请参阅 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器** 。

1. 通过控制台登录 流收集器 。
   - **登录名：**root
   - **默认密码：**lan1cope
   - 配置系统时，您将更改默认密码。
2. 在命令提示符下键入 `SystemConfig`。按 Enter 键。
3. 查看失败的登录尝试信息。选择**确定 (OK)** 继续。
4. 查看首次设置简介。选择“确定”以继续。

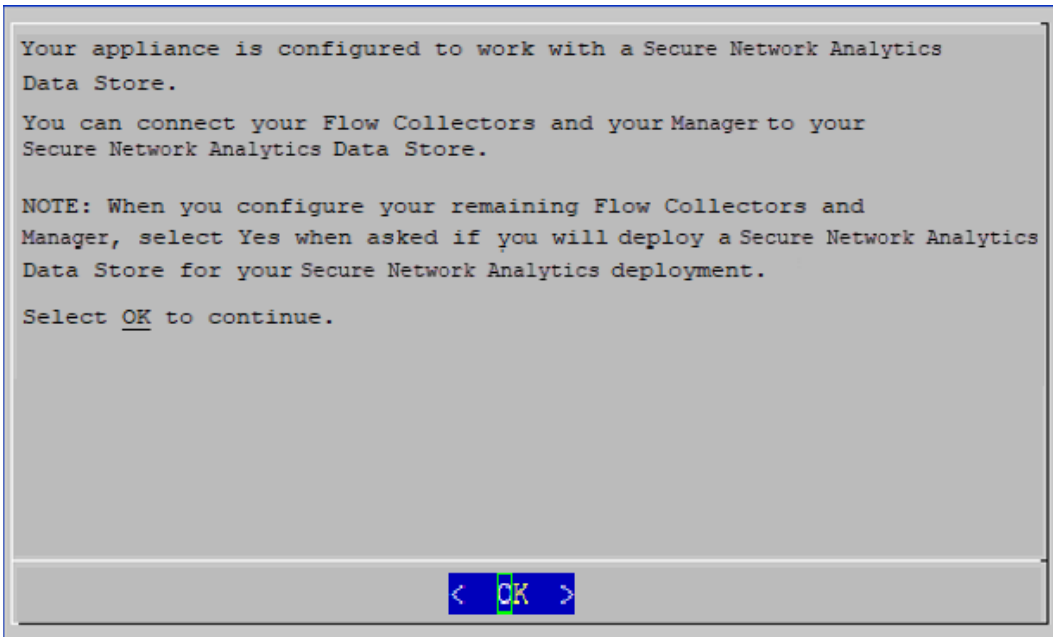


5. 是否要将此流量收集器部署为 Data Store的一部分？选择**是**。

> 在选择配置 流收集器 为与 Data Store一起使用后，您无法更新设备的配置来更改此设置。仅当您计划将 Data Store 部署到网络时才选择“是”。
>
> ⚠ 如果您不需要使用 Data Store部署 Cisco Secure Network Analytics，请不要按照本节中的说明进行操作。按照 配置不具有 Data Store中的说明进行操作。
>
> 如果选择错误，则部署新的虚拟设备或对您的设备进行 RFD。



6. 选择 **确定** 以继续。



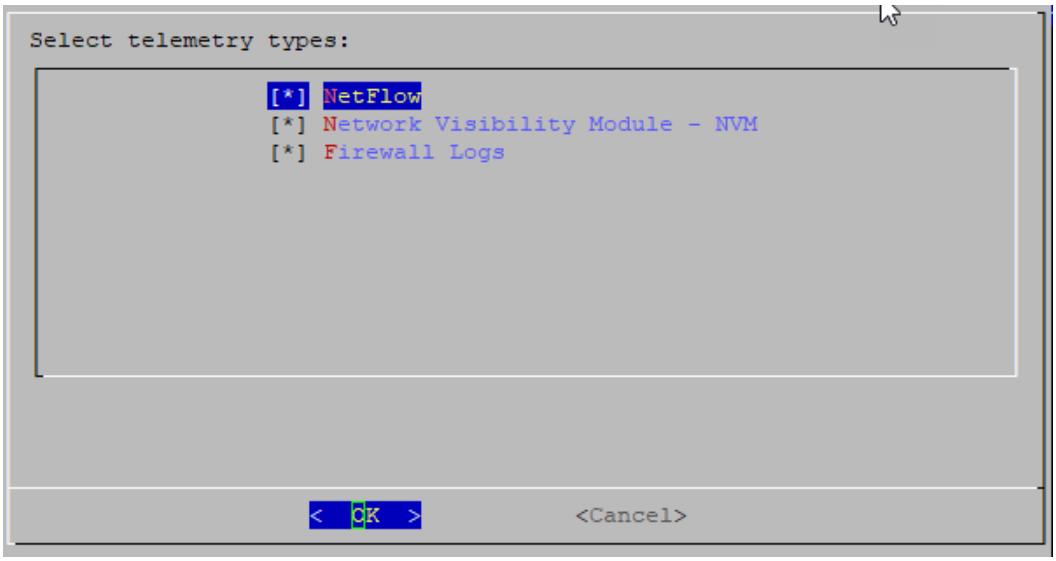
7. 选择要注入的遥测类型。

   - **默认：**默认选择所有遥测类型。星号 (*) 表示所选遥测。
   - **取消选择：**要取消选择遥测，请选择遥测类型并点击它（或按键盘上的空格键）。

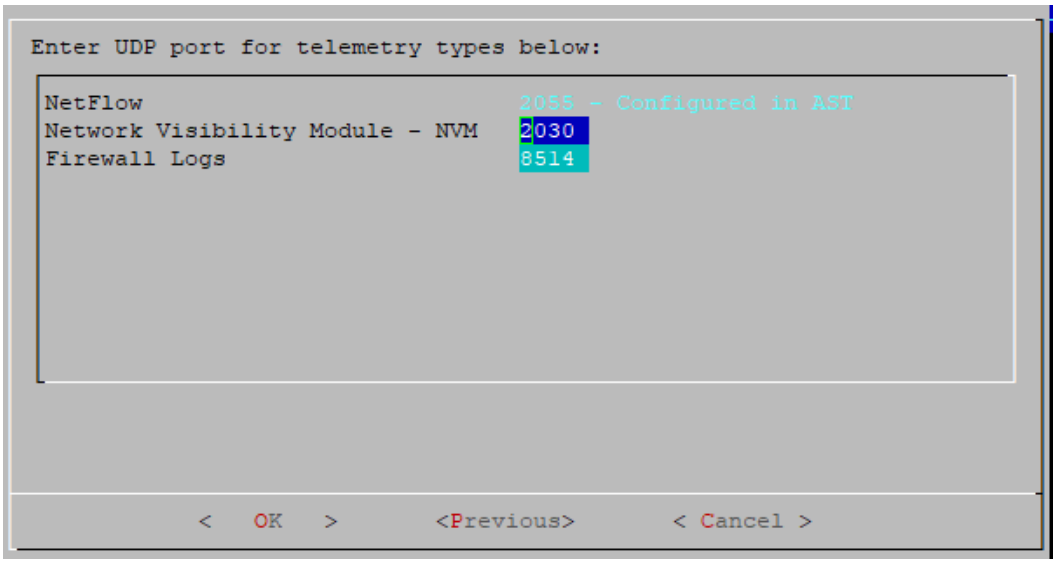
更多信息：

- **网络可视性模块 - NVM：**如果选择网络可视性模块 - NVM，流量收集器将注入并存储 NVM 流。有关详细信息，请参阅 思科安全网络分析终端许可证和网络可视性模块 (NVM) 配置指南 。
- **防火墙日志记录：**如果选择防火墙日志，则流量收集器将为 Cisco Security Analytics and Logging（本地）采集和存储防火墙事件日志。有关详细信息，请参阅 思科安全分析和日志记录：防火墙事件集成指南 。

> 如果将流量收集器配置为禁用 NetFlow，则更新配置选项（例如更改导出器、主机组、安全事件、主机报告等）将不起作用。

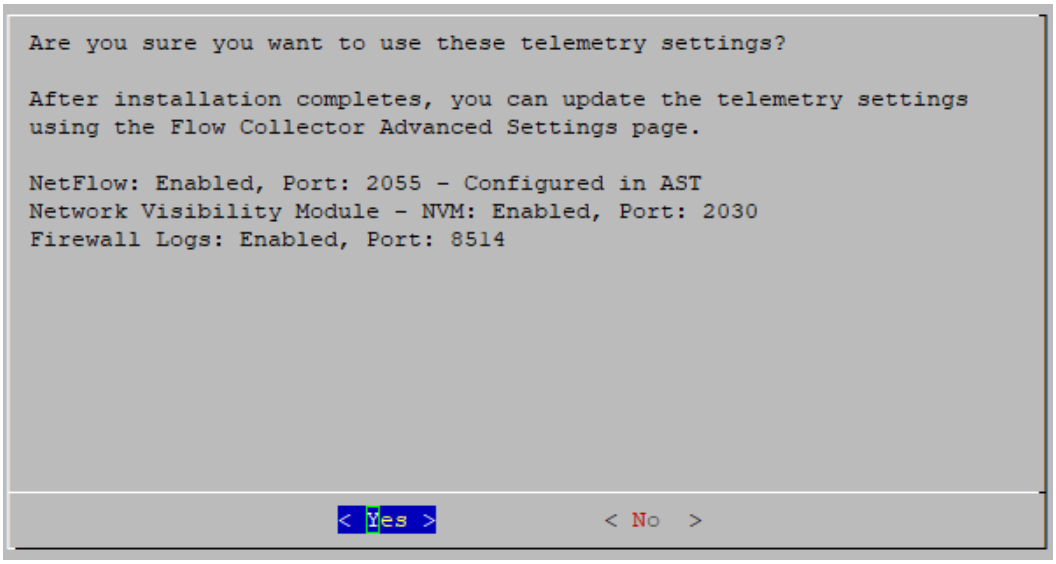


8. 输入所选遥测类型的 UDP 端口。选择**确定**。



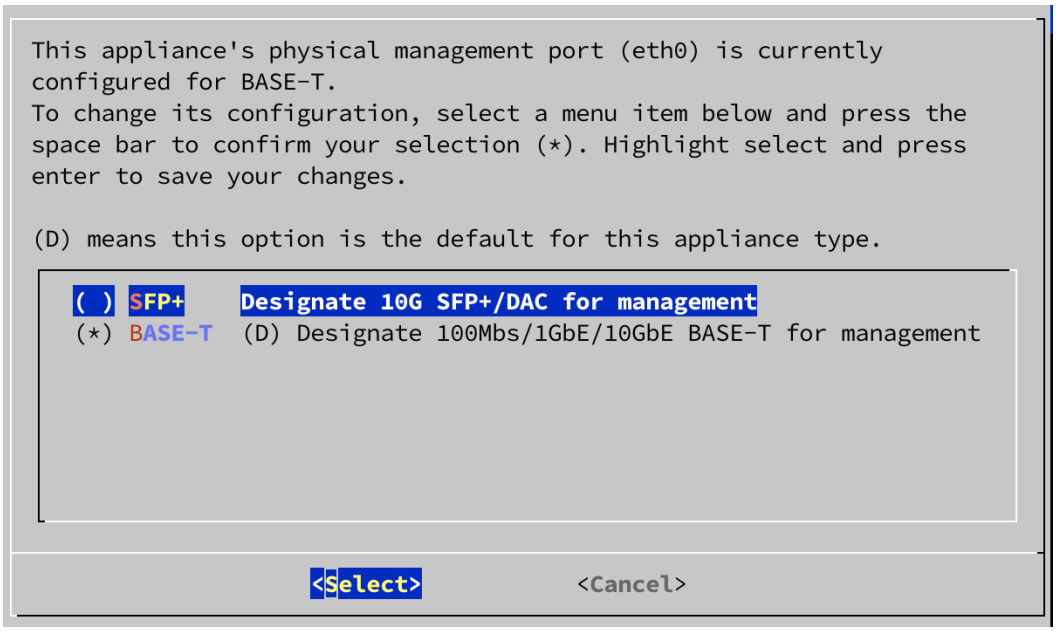
> ⚠ 请确保遥测端口是唯一的。如果配置重复的遥测端口，系统会将端口重置为内部默认设置，以避免丢失流数据。例如，如果将 NetFlow 和 NVM 导出到同一遥测端口，则导出 NVM 数据的每个设备都将在流收集器上创建导出器，并耗尽流收集器引擎中的导出器资源，从而导致流数据丢失。

9. 确认设置。选择**是 (Yes)** 继续。



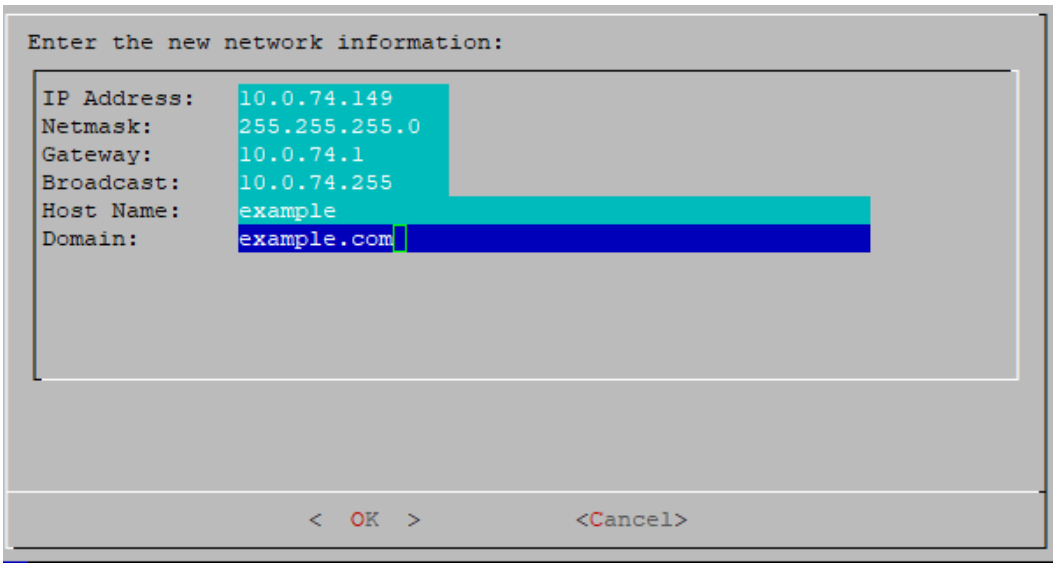
10. **eth0 的端口顺序配置(流收集器 仅 4210 硬件)**：选择以下选项之一：

    - **SFP+**：配置设备以使用 eth0 的 10G SFP+/DAC 光纤端口。
    - **BASE-T**：将设备配置为使用eth0的 BASE-T 铜缆端口。BASE-T 是默认设置。

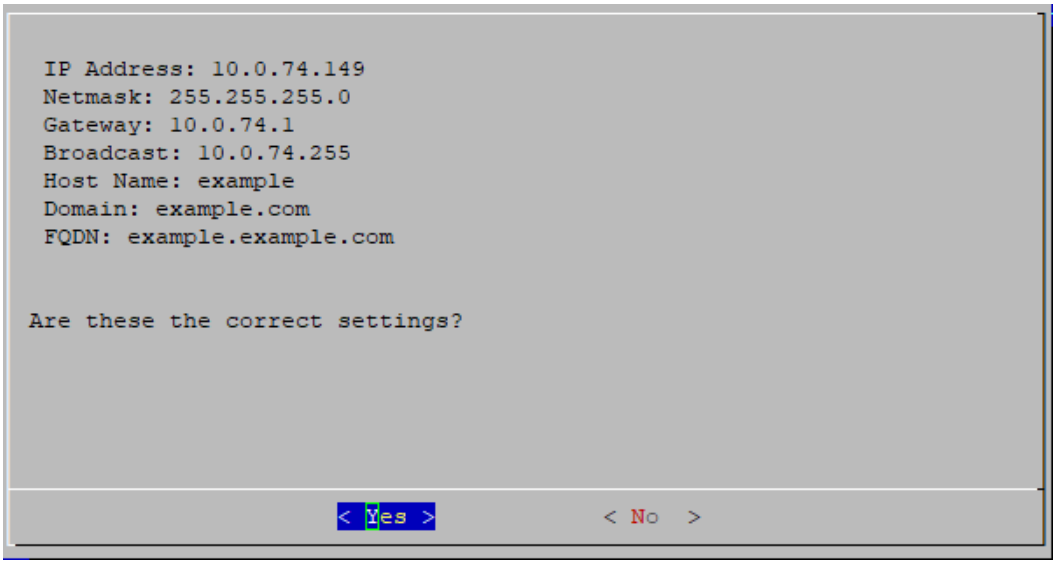


11. 输入管理接口 **IP 地址**、**网络掩码**、**网关**、**广播**、**主机名**和**域**，然后选择**确定 (OK)** 继续。

> ⚠ 每个设备都需要有唯一主机名。我们无法配置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。



12. 确认设置。选择**是 (Yes)** 继续。



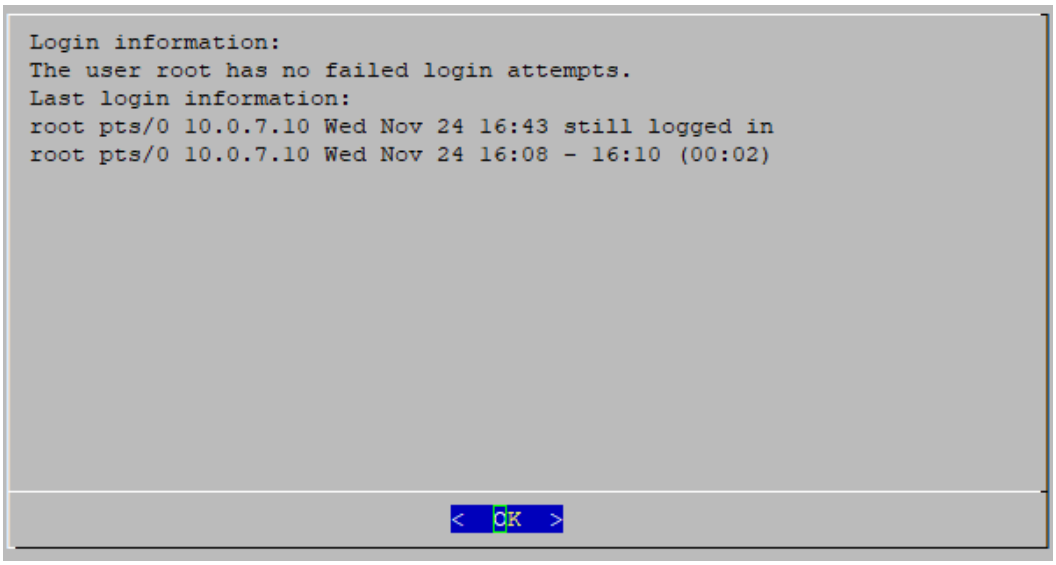
13. 选择**确定 (OK)** 确认您的选择。按照屏幕提示完成虚拟环境并重新启动设备。
14. 按 **Ctrl + Alt** 退出控制台。
15. 对系统中的下一个 流收集器 重复 配置具有 Data Store 的 流收集器 中的所有步骤。

    如果您已在首次设置中为 Data Store 配置了所有 流收集器，请返回到 设备配置概述 并配置您的其他设备。

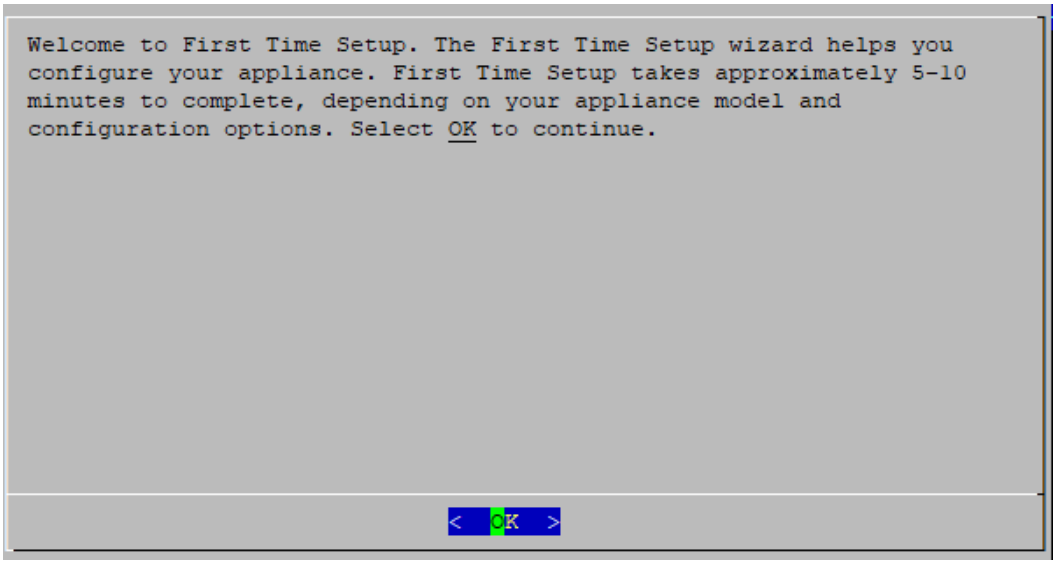
配置不具有 Data Store 的 流收集器

如果您将流量收集器配置为在没有 Data Store 的情况下使用，则 流收集器 会将其遥测 Data Store 在 流收集器 或 流收集器数据库 上(仅限 5000 系列)。

1. 通过控制台登录 流收集器 。
    - **登录**：sysadmin
    - **默认密码**：lan1cope
    - 配置系统时，您将更改默认密码。
2. 系统配置 (`SystemConfig`) 将打开。
3. 查看失败的登录尝试信息。选择**确定 (OK)** 以继续。

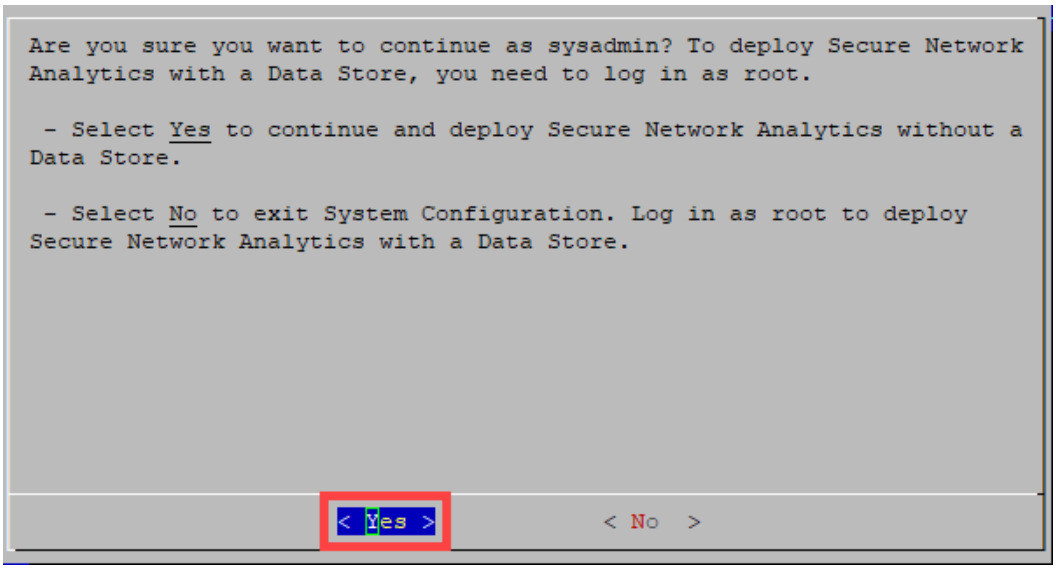


4. 查看首次设置简介。选择**确定 (OK)** 以继续。

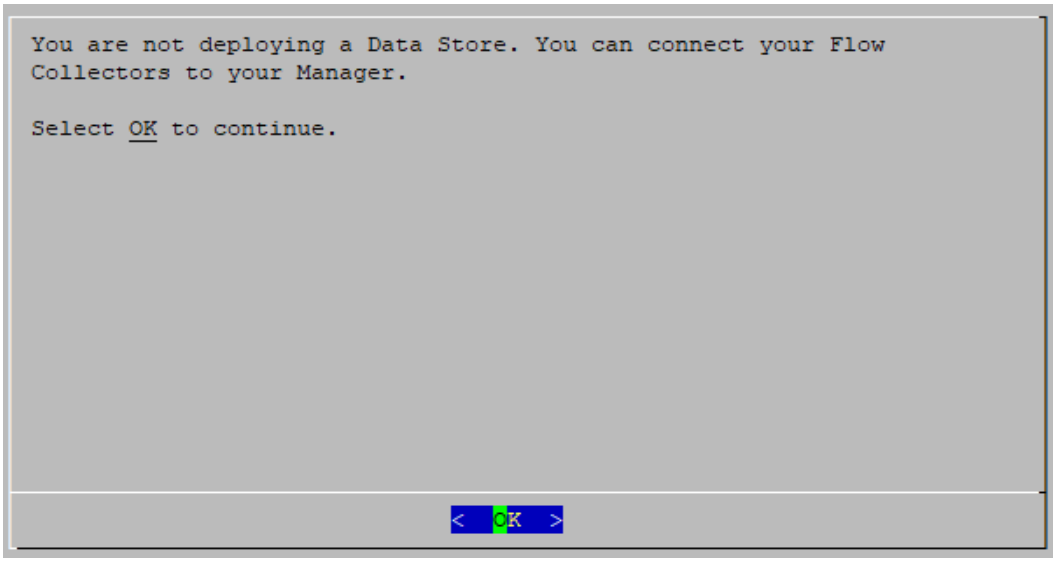


5. 是否确定要以系统管理员身份继续？选择**是 (Yes)** 以继续配置，而无需 Data Store。

> ⚠ 确保选择 **是**。如果您需要使用 Data Store部署 Cisco Secure Network Analytics，请不要按照本节中的说明进行操作。按照 **配置具有 Data Store 的 流收集器**中的说明进行操作。
> If you select the wrong choice, deploy a new virtual appliance or RFD your virtual appliance.

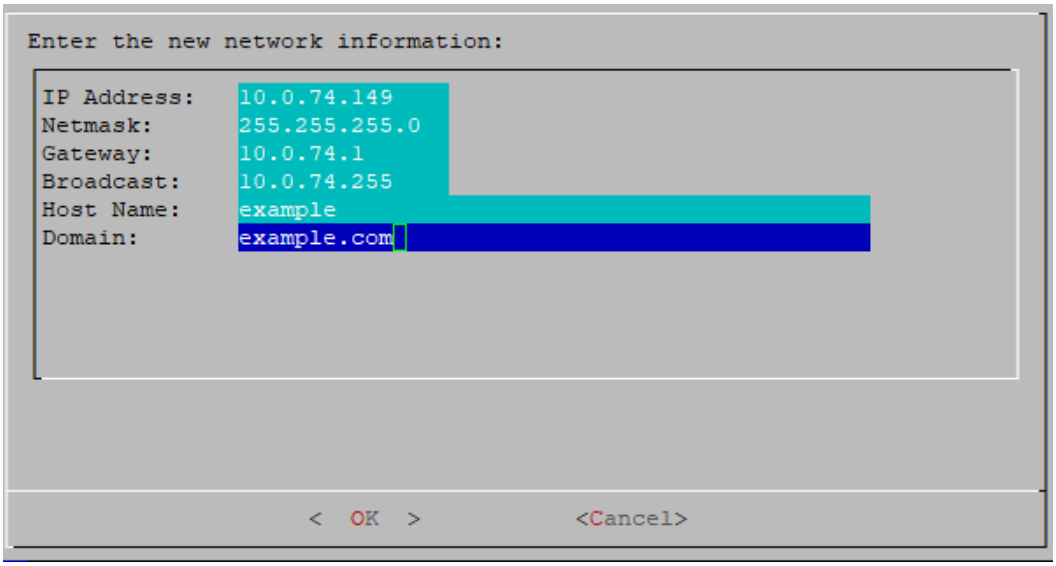


6. 确认您在部署 Cisco Secure Network Analytics 时不使用 Data Store。选择**确定 (OK)** 以继续。

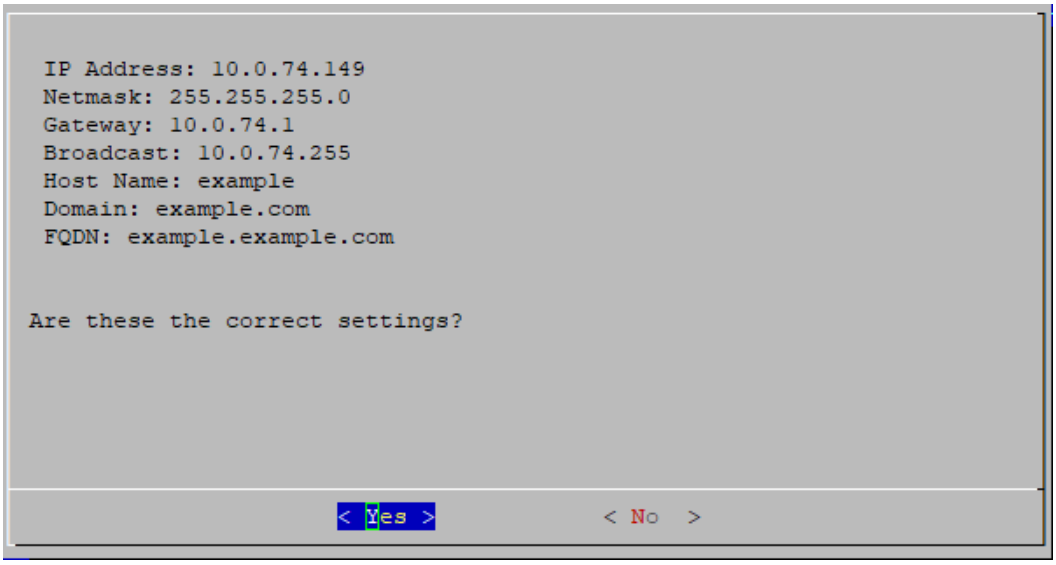


7. 输入管理接口 **IP 地址**、**网络掩码**、**网关**、**广播**、**主机名**和**域**。选择**确定 (OK)** 以继续。

> ⚠ 每个设备都需要有唯一主机名。我们无法配置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。



8. 确认设置。选择**是 (Yes)** 以继续。

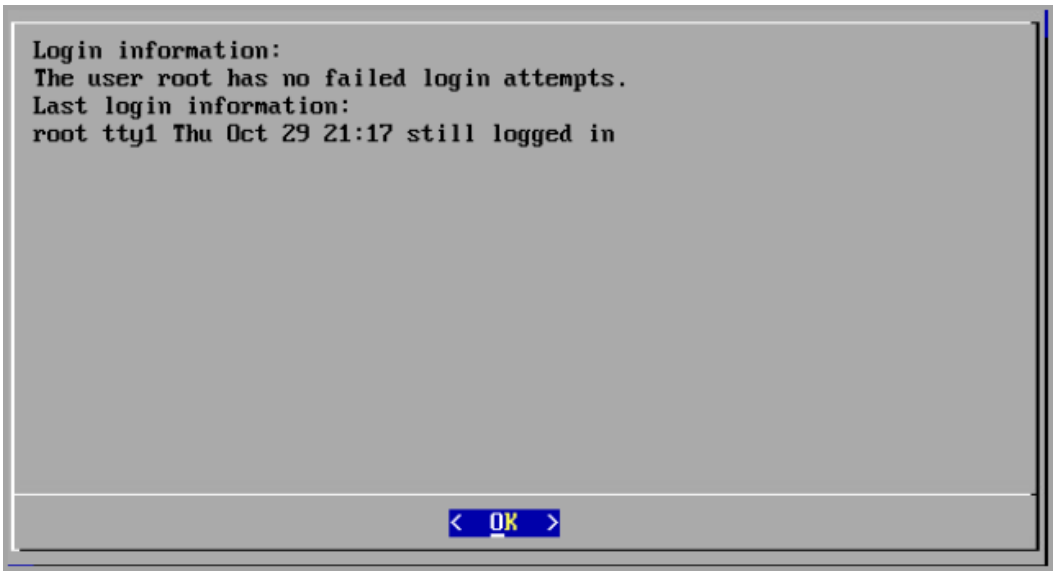


9. 选择**确定 (OK)** 确认您的选择。按照屏幕提示完成虚拟环境并重新启动设备。
10. 按 **Ctrl + Alt** 退出控制台。
11. 为系统中的下一个 流收集器 重复 配置不具有 Data Store 中的所有步骤。

    - 如果您已在“首次设置”中配置了所有 流收集器而未使用 Data Store，请转至下一部分(配置 流传感器 或 UDP 导向器)或返回 设备配置概述 以配置其他设备。
    - 如果您已在首次设置中配置了所有设备，请转至 2. 配置受管系统。

配置 流传感器 或 UDP 导向器

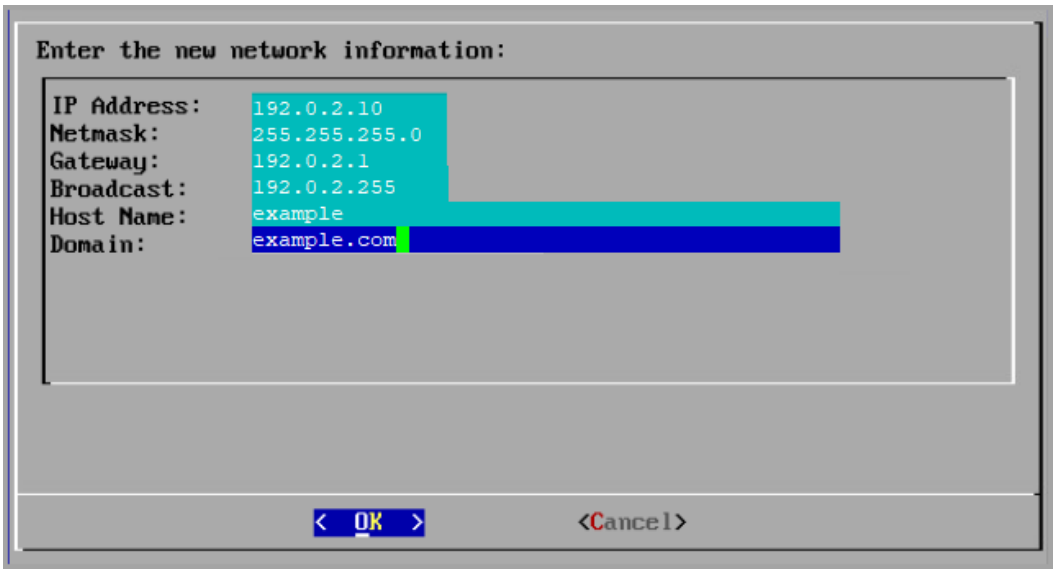
1. 通过控制台登录 流传感器 或 UDP 导向器 。
    - **登录**:sysadmin
    - **默认密码**:lan1cope
    - 配置系统时，您将更改默认密码。
2. 系统配置 (`SystemConfig`) 将打开。
3. 查看失败的登录尝试信息。选择**确定 (OK)** 以继续。



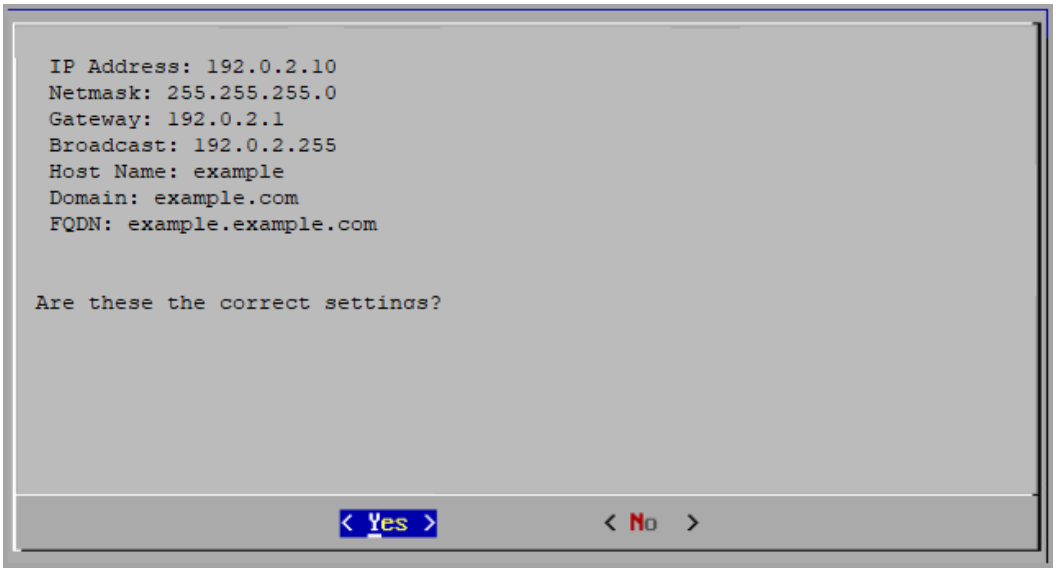
4. 查看首次设置简介。选择**确定 (OK)** 以继续。

5. 输入管理接口 **IP 地址**、**网络掩码**、**网关**、**广播**、**主机名**和**域**，然后选择**确定 (OK)** 继续。

> ⚠ 每个设备都需要有唯一主机名。我们无法配置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。



6. 确认设置。选择**是 (Yes)** 以继续。



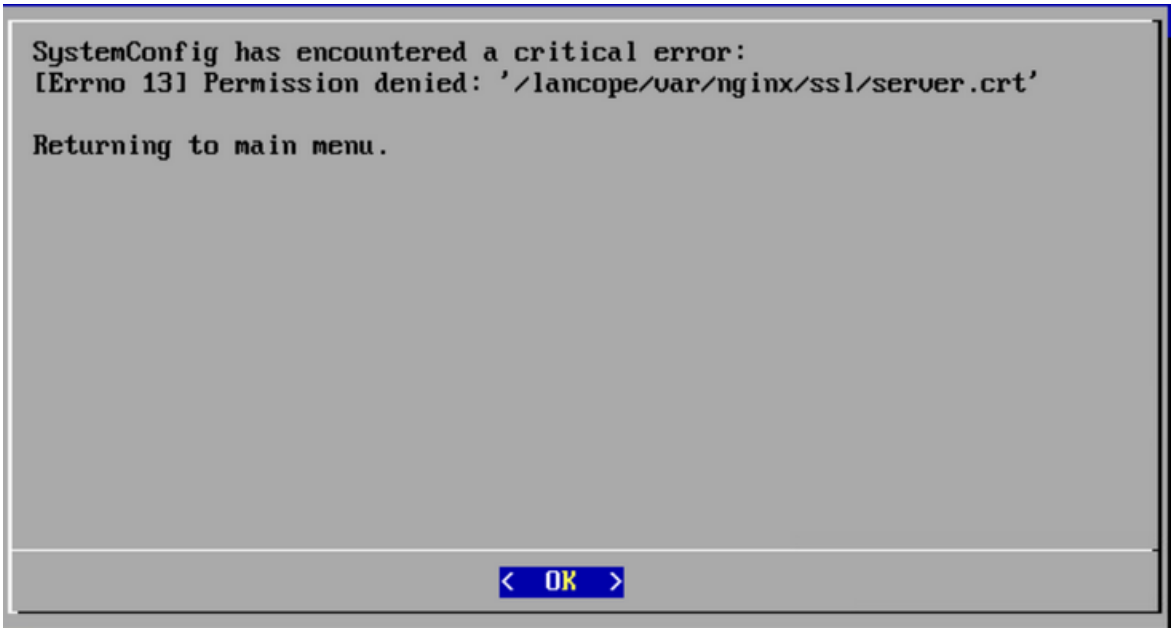
7. 选择**确定 (OK)** 确认您的选择。按照屏幕提示完成虚拟环境并重新启动设备。
8. 按 **Ctrl + Alt** 退出控制台。
9. 重复 **配置 流传感器 或 UDP 导向器** 中的所有步骤，在系统中配置下一个 流传感器 或 UDP 导向器。

如果您已在首次设置中配置了所有设备，请转至 **2. 配置受管系统**。

故障排除

证书错误

如果您的 VM 环境使用率较高，则可能存在时序错误，并且某些事件会发生顺序颠倒。如果您收到以下错误，即由于证书错误 **(.crt)** 而导致权限被拒绝，请执行以下操作：



1. 以**系统管理员**身份登录设备控制台。默认密码是 lan1cope。
2. 选择 **高级 > Root Shell**。
3. 运行以下命令：

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

4. 运行 `SystemConfig`。
5. 退出系统配置。
6. 返回 **设备配置概述** 并完成部分中的所有步骤。如果您无法访问设备，请联系思科支持部门。

访问设备

如果重新启动后无法访问设备，请执行以下操作：

1. 以 root 用户身份登录。
2. 运行以下命令并确认 Docker 容器和服务正常运行：

- `docker ps`
- `systemctl list-units --failed`
- `systemd-analyze critical-chain`

3. 所有 Docker 容器和服务启动并运行后，再次尝试登录。如果您无法访问设备，请联系思科支持部门。

2. 配置受管系统

首次登录设备时，需要使用“设备设置”工具来配置每个设备设置，使其由 管理器来管理。

准备

在开始配置之前，请查看说明，了解设备配置顺序、最佳实践和其他要求。

设备设置工具要求

- 确认您的防火墙和 ACL(访问控制列表)将允许访问。
- 收集设备的主机名和 IP 地址以了解以下信息：
    - 设备
    - 子网掩码
    - 默认和广播网关
    - NTP 和 DNS 服务器
    - 管理器 集中管理的 IP 地址

有关详细信息，请参阅 **设备配置要求**。

受管设备

作为设备设置工具的一部分，您需要将设备配置为由主设备管理 管理器。

当设备由您的 管理器 管理时，您可以使用集中管理编辑设备配置、更新软件、重新启动、关闭等。

管理器 故障转移

如果您有多个管理器，则可以设置管理器故障转移对，以便其中一个充当另一个的备用控制台。

- 使用设备设置工具配置每个设备管理器。
- 计划将管理器作为主和辅助。
- 使用设备设置工具配置 管理器和所有其他设备后，定义 管理器 故障转移关系。有关详细信息，请参阅 **3. 定义 管理器 故障转移关系** 以了解详细信息。

Cisco Secure Network Analytics 域

配置管理器时，将为 Cisco Secure Network Analytics 设备创建 Data Store 域或非 Data Store 域。在设备设置工具中配置其他设备时，会将它们添加到您创建的域中。请参阅 **规划您的系统配置** 。

完成第一个域的系统配置后，您可以将域添加到配置中（请参阅 **域**）。如果使用非Data Store 域配置 Cisco Secure Network Analytics，则可以在完成系统配置后将 Data Store 添加到部署中。按照 **将 Data Store 添加到非 Data Store 部署**中的说明进行操作。

最佳实践

要成功配置系统，请确保按照本指南中的说明进行操作。确保查看以下内容：

- **一次一个：**一次配置一个设备。在开始配置您的集群中的下一个设备之前，请确认设备为 **已连接** (或 **Data Store 未初始化**)。
- **顺序：**按照设备配置顺序。
- **多个中央管理器：**您可以在系统中配置多个中央管理器。但是，每个设备只能由一个主 管理器/中央管理器管理。
- **访问：**您需要拥有管理员权限才能访问“集中管理”。

设备配置顺序

按以下顺序配置设备，并记录每个设备的详细信息：

顺序	设备	详细信息
1.	主要 (Primary) 管理器	您的主 管理器 是中央管理器。 在开始配置系统中的下一个设备之前，请确保 管理器 将显示为 **已连接** 。 配置管理器时，您将创建一个包含 Data Store(Data Store 域) 或不包含 Data Store (非 Data Store 域) 的 Cisco Secure Network Analytics 域。
2.	所有 数据节点	Data Store 部署所必需。 Make sure the 数据节点 appliance status is **Data Store Not Initialized** before you configure the next appliance in your cluster.
3.	流收集器 5000 系列数据库	在启动引擎配置之前，请确保数据库设备状态为 **已连接** 。 **数据库和引擎对：** 如果您有多个数据库和引擎对，请一次配置一个数据库和引擎对。例如，在配置 pair2(数据库 2 和 engine2) 之前配置 pair1(database1 和 engine1) 。在每个对中，确认数据库显示为 **已连接** ，然后再启动引擎配置。 此外，在配置 唯一主机名时，请为每个数据库和引擎对命名，以便在“集中管理”中识别它们。 完成系统配置后，您可以查看每个对的信任存储区中的设备身份证书。有关详细信息，请参阅 **查看信任存储区证书** 。
4.	流收集器 5000 系列引擎	在启动引擎配置之前，请确保 流收集器 5000 系列数据库显示为 **已连接** 。
5.	所有其他 流收集器	**带 Data Store 的流量收集器：** 在集群中

		配置下一个设备之前，请确保设备状态为 **Data Store 未初始化** 。 **未带 Data Store 的流量收集器：** 在集群中配置下一个设备之前，请确保设备状态为 **已连接** 。
6.	UDP 导向器s (也称为 FlowReplicators)	在集群中配置下一个设备之前，请确保 UDP 导向器 设备状态为 **已连接** 。 如果要安装 思科遥测代理 而不是 UDP 导向器，请完成 Cisco Secure Network Analytics 系统配置。然后，按照 遥测代理虚拟设备部署和配置指南中的指示。
7.	流传感器s	在启动 流传感器 配置之前，请确保 流传感器 设备状态为 **已连接** 。
8.	辅助 管理器 (如果使用)	在启动辅助 管理器 配置之前，请确保主管理器 设备显示为 **已连接** 状态。 辅助 管理器 选择自己作为中央管理器。配置所有设备后使用设备设置工具配置故障转移。有关详细信息，请参阅 **3. 定义 管理器 故障转移关系** 以了解详细信息。

您的系统可能没有此处显示的所有设备。

1. 登录设备设置工具

按照以下说明使用设备设置工具配置每个设备。

1. 在浏览器的地址字段中，键入 **https://** 再键入设备的 IP 地址。

   - **主 管理器：**首先配置主 管理器 。
   - **已连接：**在开始配置您的集群中的下一个设备之前，请确认每个设备为“已连接”或 Data Store 未初始化。
   - **顺序：**确保按顺序配置设备，以便它们正确通信。

> 如果无法访问设备，请参阅 1 中的 故障排除 。有关说明，请使用首次设置配置您的环境。

2. 输入以下凭证进行登录：

   - **用户名：**admin
   - **密码：**lan411cope

> 如果这不是首次安装，请转至 故障排除（在本指南最后）以更改设备网络设置，例如主机名、网络域名或 IP 地址。

2. 配置设备

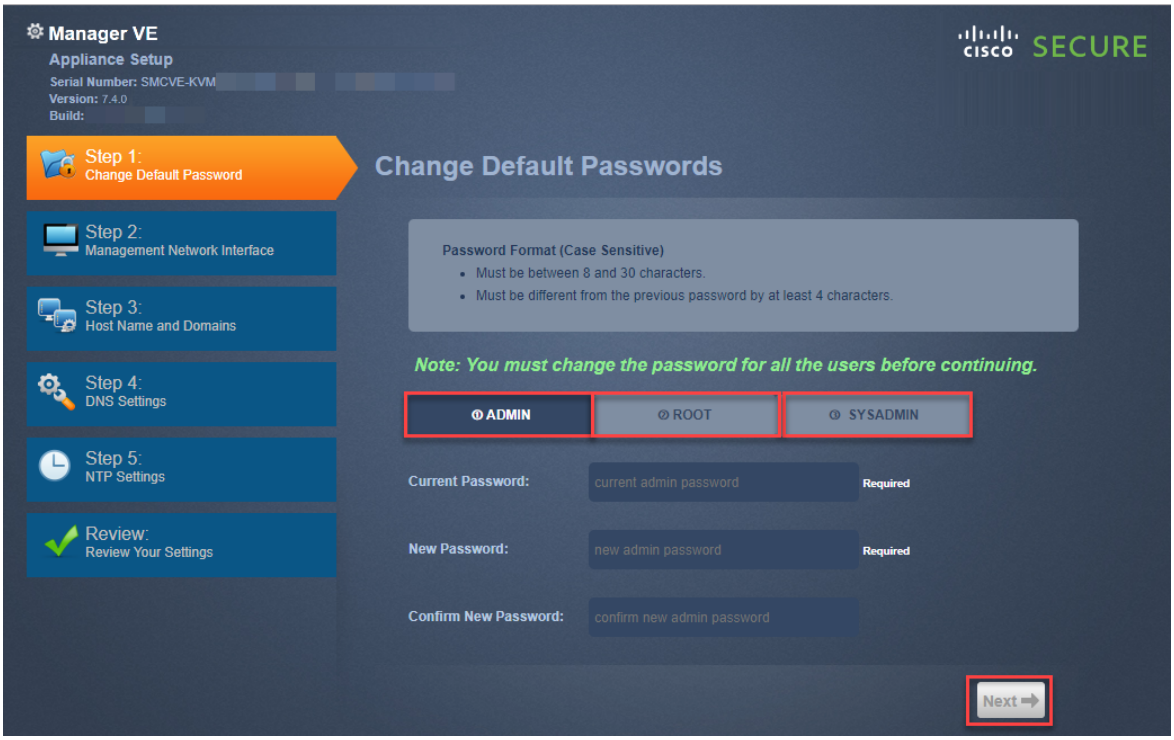
首次登录设备时，设备设置工具会引导您完成每个配置步骤。

1. **更改默认密码：**输入管理员、根和系统管理员的新密码。点击 **下一步 (Next)** 滚动到每个用户。

符合以下条件：

- **长度：**8 到 256 个字符
- **更改：**确保新密码与默认密码相差至少 4 个字符。

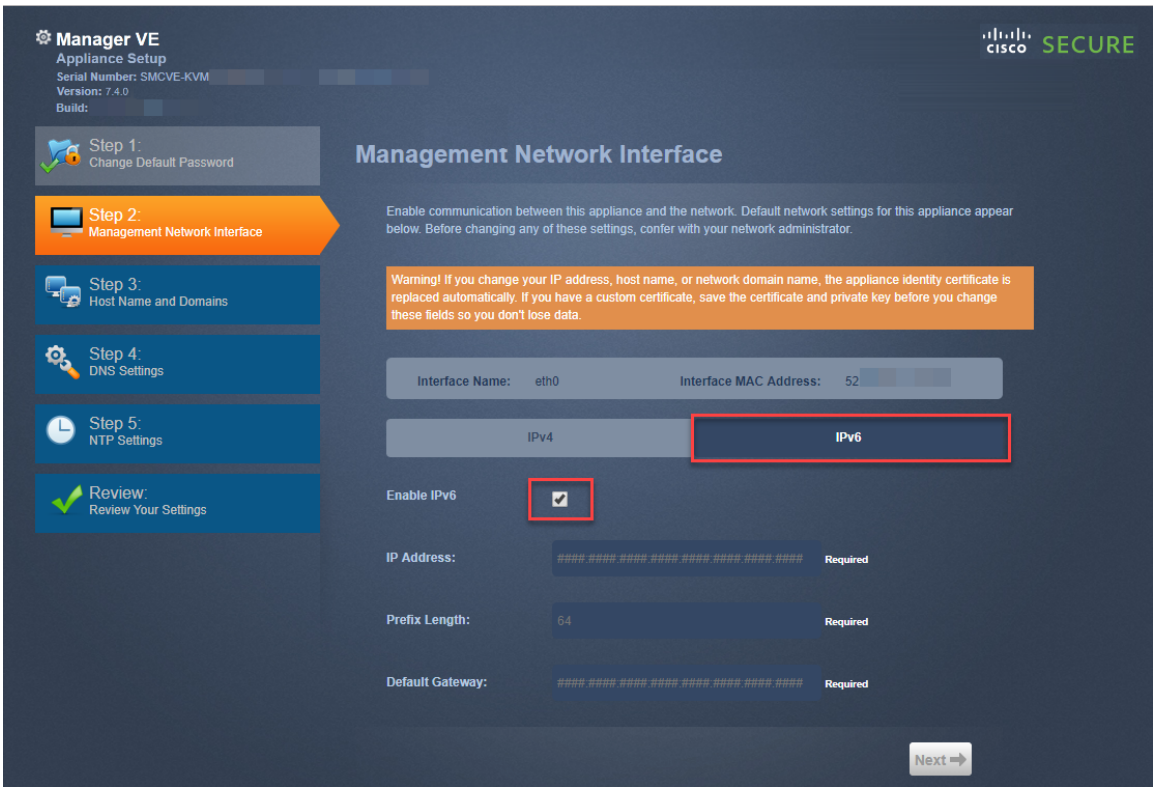
用户	默认密码
admin	lan411cope
root	lan1cope
sysadmin	lan1cope



> 如果您已在硬件安装过程中更改了默认密码，则系统管理员和根菜单不可用。

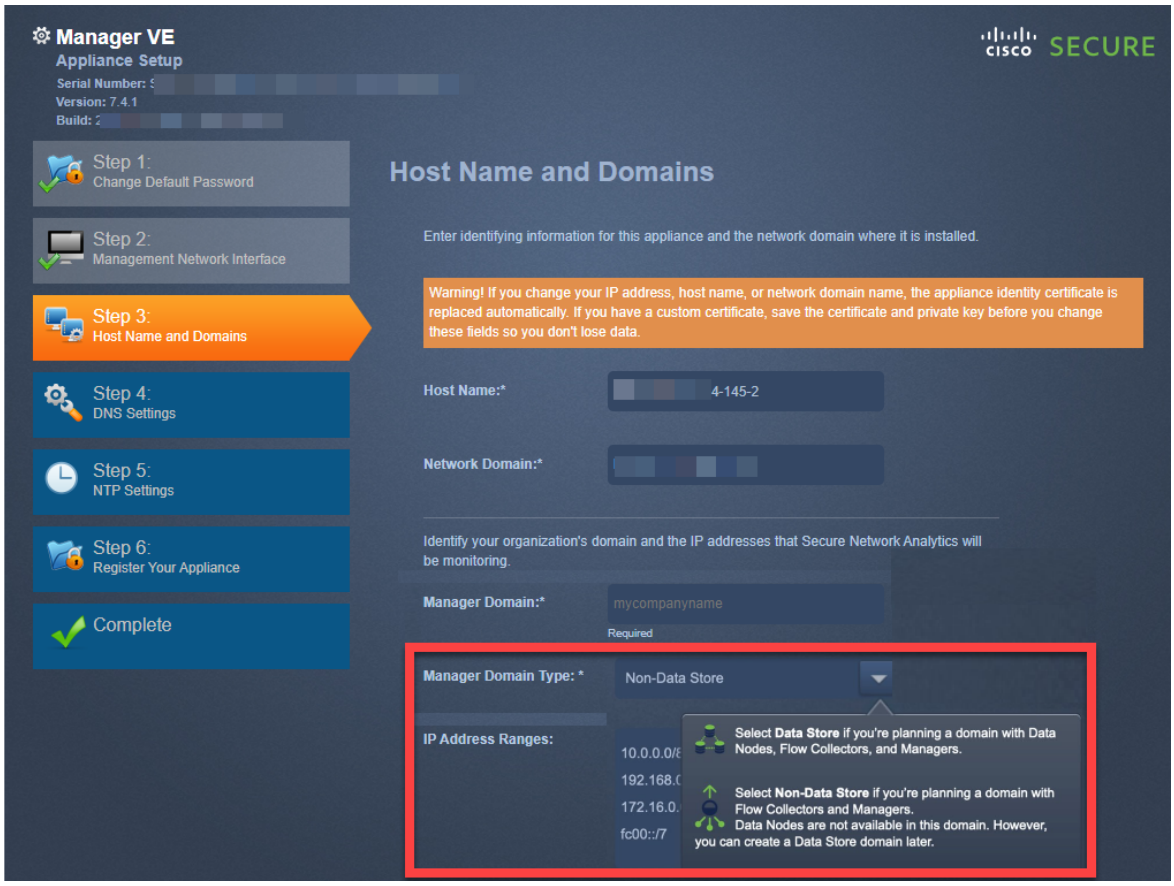
2. **管理网络接口：**查看 IP 地址和网络接口字段。确认默认设置正确。点击**下一步 (Next)**。

   - **更改：**要更改此信息，请咨询网络管理员并参阅 故障排除。
   - **IPv6(可选)：**要启用 IPv6，请点击 **IPv6**。选中**启用 IPv6 (Enable IPv6)** 复选框并填写字段。



3. **主机名和域：**输入以下信息。点击**下一步 (Next)**。

字段名称	说明
主机名	每个设备都需要有唯一主机名。如果为您的设备分配相同的主机名，这些设备将无法成功安装。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。 **流收集器 5000 系列数据库和引擎对：**使用唯一主机名命名每个数据库和引擎对，以帮助您在“集中管理”中识别该对。例如，database1 和 engine1、database2 和 engine2。
Network Domain(网域)	每个设备都需要有完全限定域名。
管理器域 (仅限于管理器)	输入 Cisco Secure Network Analytics 部署的域名。
管理器 域类型 (仅限管理器)	**Data Store 域：**如果您通过 Data Store 在首次设置中配置了设备，请选择 Data Store域。 **非Data Store 域：**如果您没有通过 Data Store 在 首次设置中配置设备，请选择非 Data Store 域。 完成本指南中的系统配置后，您可以将域添加到部署中。请参阅 域。
IP 地址范围开始 (仅限管理器)	选择您的 Cisco Secure Network Analytics 网络的 IP 地址范围。



4. **DNS 设置**：确认默认设置是否正确，或输入域服务器 IP 地址。点击**下一步 (Next)**。

   添加或删除 DNS 服务器（可选）：

   - **添加**：点击 + 图标。
   - **删除**：点击复选框以选择 DNS 服务器。点击 - 图标。

5. **NTP 设置**：确认默认设置正确无误，或点击**菜单**图标选择网络时间协议 (NTP) 服务器。点击**下一步 (Next)**。

   - **多个 NTP 服务器**：我们建议设置多个 NTP 服务器以实现冗余和准确性。
   - **公共来源**：pool.ntp.org 是 NTP 的良好公共来源。

添加或删除 NTP 服务器(可选):

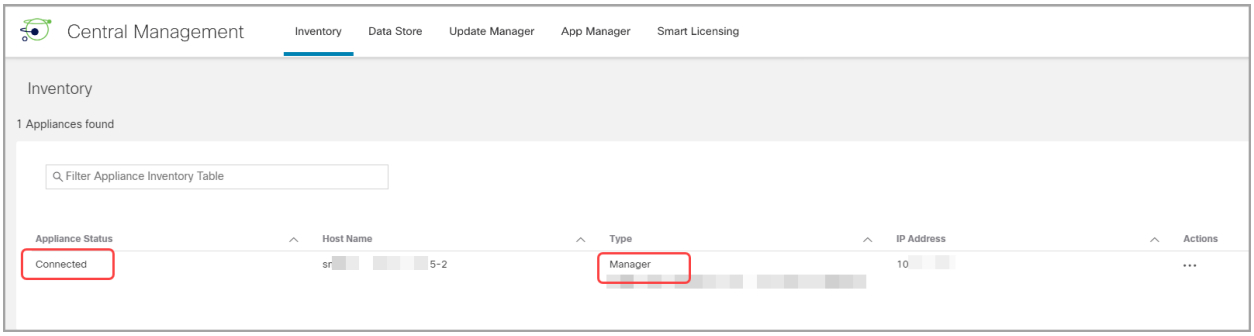
- **添加:** 点击 + 图标。
- **删除:** 点击复选框以选择 NTP 服务器。点击 - 图标。

6. 您的主 管理器 是中央管理器。将设备添加到“集中管理”, 如下所示:

- **管理器s:** 如果设备是 管理器, 请转至 **3. 注册 管理器**。
- **所有其他设备:** 如果设备不是 管理器, 请转至 **4. 将设备添加到“集中管理”**。

3. 注册 管理器

1. **查看您的设置**:确认设备信息准确无误。
2. 点击**应用 (Apply)** 或**重启并继续 (Restart and Proceed)**。
   - 在设备重新启动时,请按照屏幕上的提示进行操作。
   - 等待几分钟,让新系统设置生效。您可能需要刷新页面。
3. 登录管理器。
4. "设备设置工具"再次打开。点击**继续 (Continue)**。
5. 在"注册您的设备"(Register Your Appliance) 选项卡上,查看 IP 地址并点击**保存 (Save)**。
   - 管理器 IP 地址会被自动检测,并且无法更改。
   - 此步骤将在 管理器上安装集中管理。
6. 设备设置完成后,点击**转到控制面板 (Go to Dashboard)**。
7. 选择 **配置 > 全局 > 集中管理**。
8. 查看清单。确认 管理器 设备状态显示为 **已连接**。



> ⚠ 在开始使用 配置顺序和详细信息配置集群中的下一个设备之前,请确保主 管理器 设备状态显示为已连接。

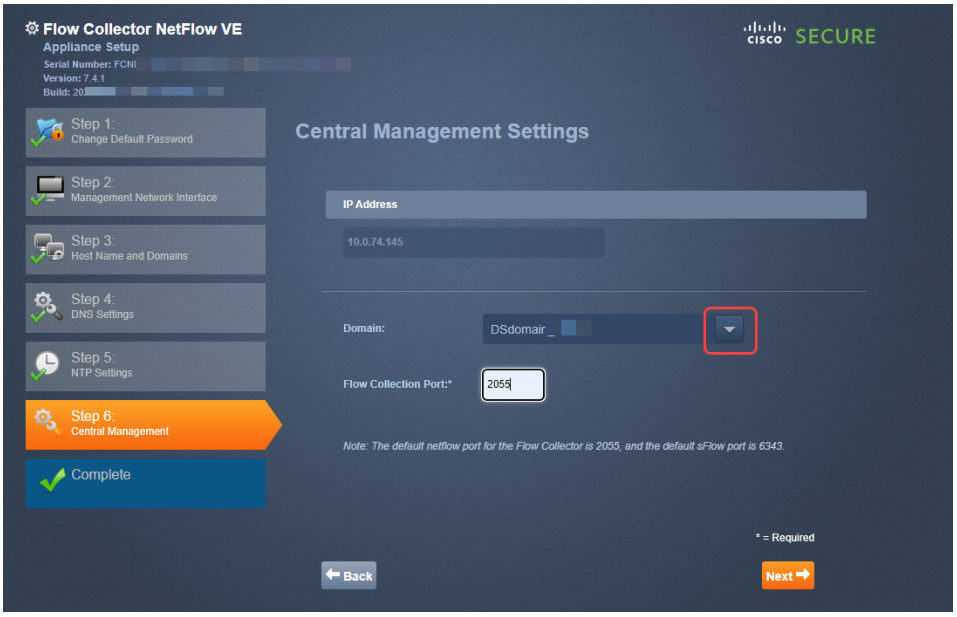
9. 要配置系统中的下一个设备,请返回 **1. 登录设备设置工具** 并配置集群中的下一个设备。

4. 将设备添加到"集中管理"

设备设置工具将继续指导您使用集中管理完成设备配置。某些步骤可能因设备而异。按照屏幕上的提示进行操作。

1. 在集中管理选项卡上，输入主 管理器的 IP 地址。
2. 点击**保存 (Save)**。
3. 按照屏幕上的提示打开桌面客户端并信任主 管理器 设备身份证书。点击 **是** 以信任证书并允许设备与 管理器通信
4. 输入主 管理器的登录凭证。
5. **域：**选择您的 Cisco Secure Network Analytics 域。这是您在注册管理器时配置为 Data Store 域或非 Data Store 域 的域。
   - **流收集器s：**输入流量收集端口号。Netflow 默认值：2055
   - **流传感器s：**选择 流收集器。

选择您的 Cisco Secure Network Analytics 域

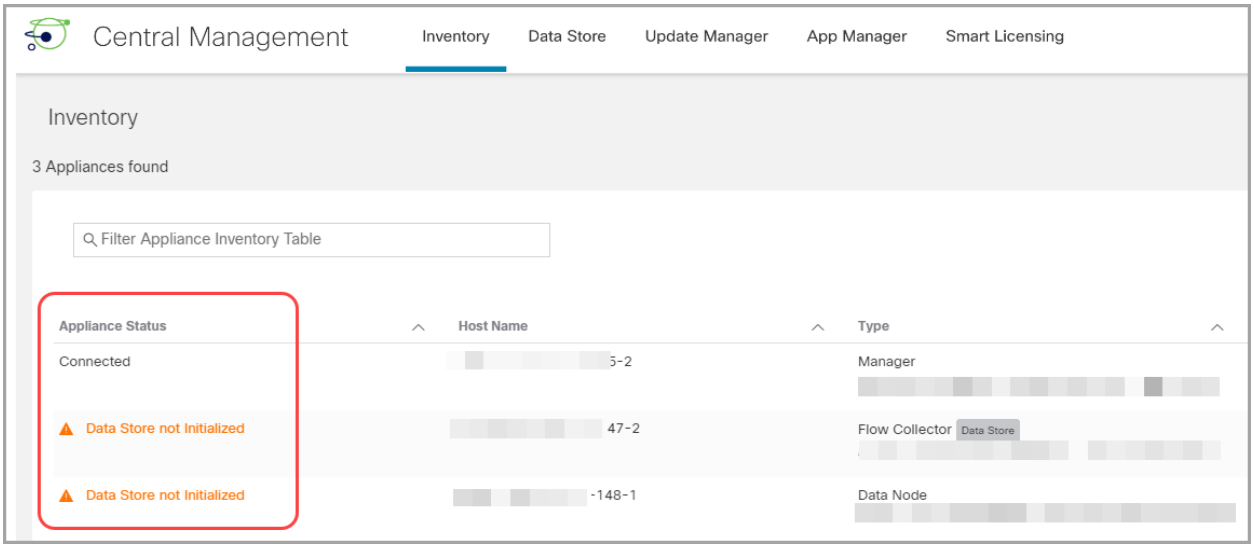


6. 点击**转至集中管理 (Go to Central Management)**。请转至 **5. 确认设备状态** 。

5. 确认设备状态

在设备设置工具中配置设备后，在集中管理中确认设备状态。

1. “设备设置工具”会打开“集中管理”清单，您也可以按以下方式打开它：
   - 登录您的主管理器。
   - 选择**配置 > 全局 > 集中管理**。
2. 查看清单上的设备。
   - 确认设备已显示在清单中。
   - **设备状态：**在开始配置集群中的下一个设备之前，请确保主 管理器 设备状态显示为 **已连接** 。
   - **Data Store 未初始化：**对于 Data Store 域中的流量收集器和数据节点，确认设备状态为 **Data Store 未初始化**。在后续程序中完成初始化后，它们将显示为“已连接”。
   - **类型：**如果流量收集器具有 Data Store 标记，则将其配置为将流发送到 Data Store 数据库。



> ⚠ 在开始使用来配置群集中的下一个设备之前，请确保主管理器和每个设备都显示为已连接（或 Data Store 未初始化）。

3. 要配置系统中的下一个设备，请转至 **1. 登录设备设置工具**，并完成所有步骤 **5. 确认设备状态** 。

3. 定义 管理器 故障转移关系

使用故障转移配置在两个管理器之间建立故障转移对，以便其中一个控制台用作另一个的备用控制台。如果您有 Data Store 部署的 Cisco Secure Network Analytics，则在初始化 Data Store 之前配置故障转移非常重要。

如果没有辅助 管理器，请转至 **5. 安装 v7.4.2 补丁**。

为了成功配置和运行故障转移，请查看要求并按照 Cisco Secure Network Analytics 故障转移配置指南中的说明操作。

> ⚠ 请注意，如果主管理器离线，管理器不会自动切换角色。确保按照 Cisco Secure Network Analytics 故障转移配置指南中显示的顺序更改管理器角色。

Data Store

如果您已通过 Data Store 部署 Cisco Secure Network Analytics，请确保在初始化 Data Store 之前配置故障转移。如果在初始化 Data Store后配置故障转移，请按照 Cisco Secure Network Analytics 故障转移配置指南 中的说明配置辅助 管理器，以便与 Data Store进行安全通信。

配置故障转移

要将管理器配置为故障转移对，请按照 Cisco Secure Network Analytics 故障转移配置指南中的说明操作。

该指南包含对成功配置至关重要的详细信息，包括：

- **证书：**要在设备之间建立信任，以便它们可以通信，请确保将正确的证书保存到所需的设备信任存储区。
- **备份文件：**在开始故障转移配置之前备份设备。
- **配置顺序：**您将在配置主 管理器之前为故障转移配置辅助 管理器 。
- **更改角色：**如果主 管理器 离线，确保按照指南中显示的顺序更改 管理器 角色。顺序非常关键，它们不会自动切换角色。
- **故障排除：**请参阅 Cisco Secure Network Analytics 故障转移配置指南 了解解决方案。

> ⚠ 为了成功配置和运行，请按照 Cisco Secure Network Analytics 故障转移配置指南中的说明操作。

主角色和辅助角色

在配置过程中，您将分配主管理器和辅助管理器。保存配置时，会发生以下情况：

- **主 管理器：**主 管理器 会将其域配置、用户设置和策略推送到辅助 管理器。使用主管理器管理设备、更改设备配置、更改密码、定义警报、应用策略等。

- **辅助 管理器**:辅助 管理器 会删除其配置,以便可以与主 管理器 配置和设置同步。此外,对于所有用户,辅助管理器变为只读属性,这意味着您将无法访问辅助管理器的各个部分,也无法从辅助管理器检索文件。

4. 配置站点冗余

> 如果未配置 Data Store 或不想创建冗余站点，请转至 **6. 正在初始化 Data Store**。

站点冗余功能可以让您在包含单独部署且使用类似设备的两个 Cisco Cisco Secure Network Analytics 站点中跨集群建立近乎冗余。使用站点冗余功能，您就能在主站点中维护域配置和分析配置，然后手动将其与冗余站点同步。此功能还可在数据中心断电时提供高可用性保护。借助站点冗余功能，登录任一冗余集群查看数据，能够看到几乎相同的数据。

> 只有管理员和配置管理者角色可以使用此功能。

站点冗余配置同步包括以下内容：

Data Store 域特定配置以及警报配置（如果已启用）。域配置包括：

- 主机组管理
- 策略管理
- 应用
- 导出器 SNMP 配置文件（不包括密码）
- 警报严重性
- 服务
- 域 AS 编号

分析配置包括以下内容：

- 优先事项
- 国家/地区监视列表
- 风险通告过期

冗余现场要求

在开始配置冗余站点之前，请查看以下要求。

- 使用相同的名称在主站点和冗余站点中创建冗余 Data Store 域。确保两个站点具有相同数量的 Data Store 域，并且两个站点中的 Data Store 域名相同。有关域的更多信息，请参阅 **域**。

> 仅同步 Data Store 域以实现站点冗余。不同步非 Data Store 域。

- 确保两个站点的 Cisco Secure Network Analytics 软件版本相同。
- 将冗余管理器证书添加到主管理器信任存储区。有关更多信息，请参阅将证书添加到信任存储区。
- 将主管理器证书添加到冗余管理器信任存储区。有关更多信息，请参阅将证书添加到信任存储区。

满足这些要求后，您可以继续执行配置冗余站点的程序。

将证书添加到信任存储区

按照以下说明将所需设备身份证书和证书链保存到信任存储区。

信任存储区要求

相应说明将指导您满足以下要求：

- 将冗余管理器证书添加到主管理器信任存储区。
- 将主管理器证书添加到冗余管理器信任存储区。

证书链

如果设备身份证书包括证书链，请确保将证书链（根证书和中间证书）添加到信任存储区。

将证书上传到信任存储区

分别上传每个文件。

1. 下载设备身份证书

按照以下说明下载并保存设备身份证书。具体步骤因您使用的浏览器而异。

如果证书已保存，可跳过此程序。请转至 **2. 将证书添加到管理器信任存储区**。

> 您也可以点击浏览器中的锁/安全图标。按照屏幕上的提示下载证书。具体步骤因您使用的浏览器而异。

1. 在浏览器地址栏中，使用以下路径替换 IP 地址后的路径：**/secrets/v1/server-identity**

   例如：https://<IP 地址>/secrets/v1/server-identity

2. 按照屏幕上的提示保存证书。

   打开：要查看文件，请选择文本文件格式。

   故障排除：如果没有看到下载证书的提示，请检查 Downloads 文件夹中是否已自动下载证书，或尝试使用其他浏览器。

3. 对每个管理器重复步骤 1 和 2。

2. 将证书添加到管理器信任存储区

按照以下说明将冗余管理器设备身份证书和证书链（如有）保存到主管理器信任存储区。

1. 登录管理器。
2. 选择**配置 > 全局 > 集中管理**。

3. 确认“设备状态”显示为“已连接”。
4. 点击管理器的**操作**菜单。
5. 选择**编辑设备配置**。
6. 在**集中管理资产清单 > 常规**选项卡上，找到**信任存储区**部分。
7. 点击**新增**。

> ⚠ 确保分别上传每个设备身份证书和证书链(根证书和中间证书)。

8. 在**友好名称**字段中，输入证书名称。
9. 点击**选择文件**。选择证书。
10. 点击**添加证书**。确认证书显示在“信任存储”列表中。
11. 重复步骤 6 至 9，将任何其他所需证书添加到信任存储区。
    - 如果登录的是冗余管理器，请添加主管理器证书。
    - 如果登录的是主管理器，请添加冗余管理器证书。
12. 点击**应用设置**。按照屏幕上的提示进行操作。
13. **已连接：**在“集中管理资产清单”页面上，确认“设备状态”恢复为“已连接”。
14. 在另一个管理器上重复步骤 1 到 13。

打开“站点冗余配置”

按照以下说明打开“站点冗余配置”。

1. 以管理员或配置管理者身份登录管理器。
2. 从主菜单中，选择**配置 > 全局 > 管理器**。
3. 点击**站点冗余配置**选项卡。

配置冗余站点

按照以下步骤配置冗余站点。

1. 选中**启用配置**复选框。
2. 在**冗余站点管理器的名称**字段中，输入冗余站点管理器的完全限定域名 (FQDN) 或 IP 地址。请注意，管理器名称必须与管理器身份证书中的通用名称或使用者备用名称一致。
3. 点击**保存**按钮保存您所做的更改。
4. 点击**同步**按钮，同步主站点与远程站点。此操作将在两个站点间同步域配置和分析配置。
5. 按照屏幕上的提示确认您要同步更改。点击**同步 (Synchronize)** 以继续。

您将看到“进行中”省略号图标，表示正在进行同步。同步完成后，您将看到说明成功或失败的横幅。

> 在您执行同步时，冗余站点流量收集器引擎配置将在此过程中被覆盖。建议每小时同步不要超过一次。

禁用冗余站点

执行以下步骤以禁用冗余站点。

1. 要禁用冗余站点，请取消选中**启用配置**复选框。
2. 点击**保存**按钮保存您所做的更改。这将禁用冗余站点以及“同步”按钮。
3. (可选)删除已禁用冗余站点的站点证书可以为 Cisco Secure Network Analytics 系统增加一道额外的安全防线。如果要删除在配置冗余站点的过程中添加的站点证书，可以执行以下步骤。
    1. 登录管理器。
    2. 选择**配置 > 全局 > 集中管理**。
    3. 确认“设备状态”显示为“已连接”。
    4. 点击管理器的**操作**菜单。
    5. 选择**编辑设备配置**。
    6. 在**集中管理资产清单 > 常规**选项卡上，找到**信任存储区**部分。
    7. 在**操作**列下，对每个要删除的证书点击**删除**。

故障排除

如果站点冗余配置出现问题，请确保满足以下条件：

- 验证您的证书是否位于正确的信任存储区中。有关更多信息，请参阅将证书添加到信任存储区。
- 两个站点的 Cisco Secure Network Analytics 软件版本需要相同。
- 两个站点上的 Data Store 域数量和名称需要一致。

要查看日志文件以了解错误详情，请导航至 /lancope/var/smc/log/smc-configuration.log

5. 安装 v7.4.2 补丁

在设备上安装最新的 v7.4.2 补丁。

1. 可以在 https://software.cisco.com的思科软件中心，从您的思科智能帐户中下载最新的 **v7.4.2 patches** 。
2. 请确保按照补丁自述文件中的说明操作安装每个补丁。
3. 使用最新补丁更新设备后，请转至本指南中的下一个程序：

    - **Data Store 域名：**按照 **6. 正在初始化 Data Store**。
    - **非 Data Store 域：**按照 **7. 安装桌面客户端** 。

6. 正在初始化 Data Store

使用系统配置初始化您的 Data Store。在此过程中，您将临时启用 SSH。

> 在开始此程序之前，请将所有设备添加到“集中管理”资产。初始化 Data Store 不需要 流收集器，但是在开始初始化过程之前，您的“集中管理”资产中至少需要有一个 数据节点 和一个 管理器 。

1. 以 root 用户身份登录管理器设备控制台 (SystemConfig)。
2. 从主菜单中选择 **Data Store**。
3. 选择 **SSH**。按照屏幕提示启用 SSH。
4. 从 Data Store 菜单中选择 **初始化** 。
5. 按照屏幕上的提示初始化 Data Store。

   退出 Data Store 菜单时，系统会恢复之前的 SSH 设置。

6. 转至下一程序：**8. 验证通信**。

7. 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。

8. 验证通信

。查看流收集趋势

1. 登录您的主管理器。

   故障转移配置：登录主管理器和辅助管理器。

2. 查看流收集趋势。

2. 验证 Data Store 数据库状态

> 如果未使用 Data Store 部署 Cisco Secure Network Analytics，请转至 **3. 运行报告 报告构建器**中运行报告。

1. 在主 管理器 控制面板，选择 **配置 > 全局集中管理**。
2. 点击**Data Store**选项卡。
3. 确认 Data Store 数据库状态显示为“运行”。

   如果数据库状态为“关闭”，请点击数据库的“操作”列中的 ••• (**省略号**)图标 。选择 **启动**。

4. 确认所有数据节点的状态显示为“运行”。

   如果数据节点状态为“关闭”，请点击 数据节点“操作”列中的 ••• (**省略号**)图标 。选择 **启动**。

有关 Data Store 选项卡的详细信息，请参阅 **Data Store 数据库**。

3. 运行报告 报告构建器

1. 返回安全洞察控制面板。
2. 选择 **报告** 菜单。
3. 选择 **报告构建器**。
4. 点击 **创建新报告**。
5. 点击 **流收集趋势(按流量收集器)** 模板
6. 根据需要选择参数。点击**运行**。
7. 查看报告，确认您的流量收集器正在接收流。
8. 如果您有 流收集器数据库（仅限 5000 系列）或 Data Store，请返回“报告生成器”控制面板并重复步骤 4 至 7，以运行 **流数据库采集趋势**报告。确认数据库或 Data Store 正在接收流。

有关报告生成器的详细信息，请参阅“帮助”中的信息。

9. 完成设备配置

确保完成设备的所有必要配置。

设备	必需 配置	可选 配置
数据节点	无	数据压缩 流接口统计信息
流收集器s	无	将 NetFlow 更改为 sFlow
UDP 导向器s	无	高可用性 (仅可用于硬件上)
流传感器s	应用 ID 和负载	识别应用

更改流设置 流收集器

> 以下步骤需要重新启动 流收集器 才能应用这些更改。

按照以下步骤更改流收集器中的流设置。

1. 登录流收集器。
2. 点击 **支持 > 高级设置**。
3. 在 **engine_startup_mode字段**中，输入以下值之一：
   - 模型文件中的默认值 - 0
   - NetFlow -1
   - sFlow - 2

> 如果 engine_startup_mode 字段未出现在“高级设置”列表中，您可以使用“添加新选项”和“选项值”字段在页面底部添加该字段。

4. 点击**应用**，然后点击**确定**。
5. 重新启动流收集器以应用更改。
6. 登录管理器。
7. 选择 **配置 > 系统 流收集器**。
8. 在“监控端口”字段中输入以下数值之一（这些是 NetFlow 和 sFlow 的行业标准默认端口号。如果导出器已配置为使用非标准端口，则必须改用该端口号）。
   - 2055 - NetFlow
   - 6343 - sFlow
9. 点击 **保存** 以保存更改。

   模式切换（从 NetFlow 切换到 sFlow 或从 sFlow 切换到 NetFlow）完成后，基于前一模式的流的以下项目将被清除：
   - 缓存：主机缓存、流缓存、安全事件缓存
   - 已保存的基准文件

您可以检查控制面板上的流趋势图来确认模式切换，以查看流是否正在新模式下进行处理。

为 UDP 导向器配置高可用性（仅限硬件）

按照以下说明将 UDP 导向器配置为高可用性对。

> 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。

- **转发规则:** 如果计划设置“高可用性”, 则至少配置一条转发规则。请参阅 配置转发规则
- **高可用性:** 如果您有多个 UDP 导向器, 则可以设置高可用性对。如果要设置高可用性, 请配置至少一个转发规则(请参阅 配置高可用性)。

配置转发规则

SSL 用于将消息从 UDP 导向器 发送到 管理器。

1. 登录管理器。
2. 选择 **配置 > 全局 UDP 导向器**。
3. 点击设备的**操作 (Actions)** 菜单。选择**配置转发规则 (Configure Forwarding Rules)**。
4. 点击**添加新规则 (Add New Rule)**。
5. **说明:** 输入识别该规则的简短说明。
6. **源 IP 地址:端口:** 键入向 UDP 导向器 发送数据的设备的 IP 地址, 然后输入端口号(通过其发送数据)。
    - **格式:** 使用语法 [IP address]:[Port Number]。
    - **范围:** 您可以使用无类域间路由 (CIDR) 表示法来输入一系列 IP 地址。
    - **全部:** 您可以键入“All”, 在该端口上接受来自任何源 IP 地址的数据。
    - **组合:** 您可以将“源 IP 地址:端口”组合添加到新行中, 从而在规则内添加这些组合。

示例：

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **目标 IP 地址：**输入从 UDP 导向器接收数据的设备的 IP 地址。
8. **目标端口号：**输入接收设备的端口号。
9. 点击**保存 (Save)**。
10. **可选：**要同步更改，请点击“同步”(Sync)。
11. 根据需要重复该过程，以添加转发规则。
12. 要设置高可用性对，请转至 **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。

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版本 7.4.0 或更高版本，请在更新后按照以下说明重新配置高可用性。
> 有关更新 Secure Network Analytics 的详细信息，请参阅 更新指南。

主节点和辅助节点

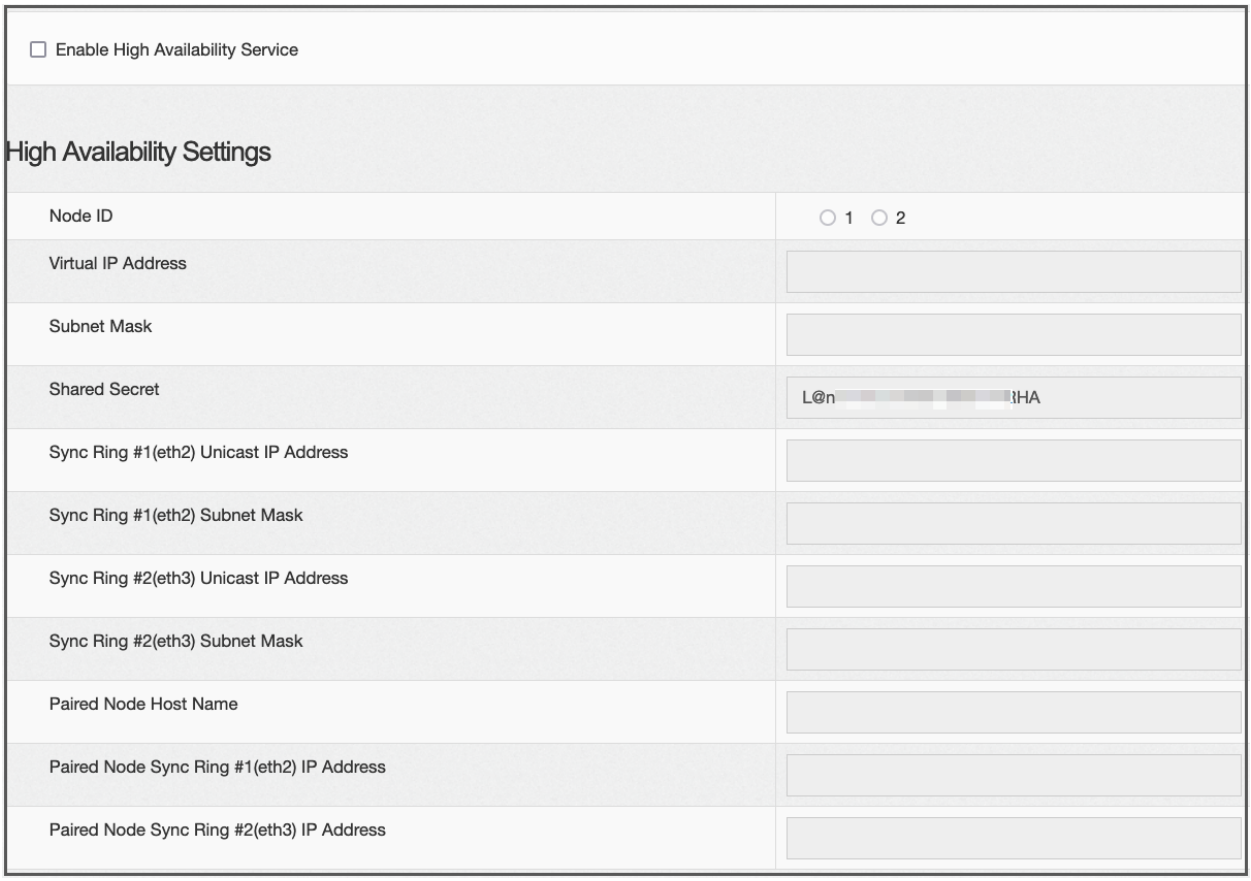
在线节点在对中称为主节点，而离线节点为辅助节点。如果对中的主节点发生故障，辅助节点取而代之成为主节点。

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)**。
3. 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。



4. 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。
5. 在 **虚拟 IP 地址** 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。

> 确保两个节点上的虚拟 IP 地址相同。

6. 在 **共享密钥** 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。)
7. 在 **同步环 1 (eth2) 单播 IP 地址**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。)
8. 在 **同步环 2 (eth3) 单播 IP 地址**字段中，输入 IP 地址和子网掩码。

每个 IP 地址(eth0、eth02、eth03)都必须位于其自己单独的单播子网中。

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集群的第二个 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，请完成以下主 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** 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。

配置 流传感器

1. 配置应用 ID 和负载

流传感器 的配置需要增加一个步骤，即配置应用 ID 和负载。

1. 登录 流传感器 设备管理界面。
2. 点击**配置 (Configuration) > 高级设置 (Advanced Settings)**。

系统将打开“高级设置”(Advanced Settings) 页面。

3. 选择适用于您的网络的设置：

项目	说明
导出数据包负载	允许您指定 流传感器 在其发送至收集器的数据中是否包含二进制负载数据的前 26 个字节。
导出应用标识	允许您指定 流传感器 在向收集器发送数据之前是否尝试识别应用。此外，必须启用此设置，下列设置才会生效： 包括 IPv6 - 允许您指定 流传感器 是否分析 IPv4 和 IPv6 数据包。禁用此设置后，流传感器 仅分析 IPv4 数据包。 导出 HTTPS 报头数据 - 允许您指定 流传感器 在其发送至收集器的数据中是否包含 HTTPS 流量的报头。数据中包含 SSL 公共名称和 SSL 组织名称。此设置需要将“流类型”设置为 IPFIX。最大值为 256 字节。 导出 HTTP 报头数据 - 允许您指定 流传感器 在其发送至收集器的数据中是否包含 HTTP 流量的报头。选择此设置后，辅助字段允许您指定 流传感器 包含为流数据一部分的 HTTP 路径的最大长度(以字节为单位)。此设置需要将“流类型”设置为 IPFIX。
启用 VXLAN 解封	允许您指定 流传感器 是否使用虚拟可扩展局域网 (VXLAN) 解封功能。如果未启用 VXLAN 解封，流传感器 只会将 VXLAN 封装流量作为两个虚拟隧道终端 (VTEP) 之间的流量进行检测。通过解封可以对隧道流量进行分析，进而更深入地了解网络中的流量模式，提供更丰富的内容。 流传感器 仅解封最初发送到标准 VXLAN 端口 (4789) 的 VXLAN 流量。
启用 GENEVE 解封	允许您指定 流传感器 是否对在其监控端口上收到的流量使用通用网络虚拟化封装 (GENEVE) 解封。
启用 ERSPAN 解封	允许您指定 流传感器 是否使用远程封装交换端口分析器 (ERSPAN) 解封功能，以便检测数据包中的 ERSPAN 报头，然后解封该报头并处理内部数据包内容。

项目	说明
	您需要为监控接口分配 IP 地址，以允许终止 流传感器上的 ER SPAN 隧道。 FS 4210 上不支持 ERSPAN 解封。
启用 X-Forwarded-For 处理	允许您指定 流传感器 是否使用 X-Forwarded-For (XFF) 处理来识别通过 HTTP 代理或负载均衡器连接到 Web 服务器的客户端的源 IP 地址。 ETA 和 X-Forwarded-For 处理不能一起配置。
启用 ETA 处理	允许您指定 流传感器 是否使用 ETA 处理来生成 IDP 和 SPLT 字段，并将其发送到 管理器。 启用 ETA 会增加 NetFlow 的带宽使用率，尤其是在使用 v9 时。我们建议使用 IPFIX 作为流导出格式。 ETA 和 X-Forwarded-For 处理不能一起配置。 不能在 Dell 或 PowerEdge 流传感器 型号上启用 ETA。
启用负载均衡	允许您指定 流传感器 4000 系列是否可以向多个 流收集器分配流数据。 如果 流传感器 的流数据超过一个 流收集器的容量，请使用此选项。
监控接口选择	允许您指定以下内容： • 流传感器 4240 - 2 个 40G 或 4 个 10G (SFP) 接口 • 流传感器 4300 - 2 个 40G/100G 或 4 个 10G (SFP) 接口 必须使用多个 流收集器并启用负载均衡，此设置才能正常工作。有关详细信息，请转至 流传感器 和负载均衡器集成指南 。 此选项仅在 流传感器 4240 和流传感器 4300 上可用。 默认设置为 2 x 40G。
缓存模式	允许您选择以下设置之一： 为所有监控端口使用单个共享缓存 -

项目	说明
	• 当存在非对称路由时使用。 • 应用和延迟计算的单状态表。 • 使用较少内存。 • 降低整体 pps 处理速率。 • 导致在多个接口上创建一个 NetFlow 事件。 • 仅当 流传感器 只有两个端口并且通过 TAP 连接时使用 为每个监控端口使用独立缓存 - • 允许在每个 流传感器 接口中对数据包进行重复数据删除。 • 使用较多内存。 • 提高整体 pps 处理速率。 • 每个接口保持自己的延迟和应用数据库。 • 为发现给定数据包的每个接口生成唯一的 NetFlow 记录。

4. 点击**应用 (Apply)** 保存设置。

2. 配置 流传感器 以识别应用(可选)

如果希望 流传感器 识别应用，请配置以下设置：

1. 登录 流传感器 设备管理界面。
2. 点击**配置 (Configuration) > 高级设置 (Advanced Settings)**。
3. 选中**导出应用标识 (Export Application Identification)** 复选框。默认情况下，此选项未选中。
4. 如果您有多个监控 NIC，请在**缓存模式 (Cache Mode)** 部分中选择以下选项之一：
   - **对所有监控端口使用单个共享缓存：**通常用于使用 TAP 方法监控流的系统。
   - **对每个监控端口使用独立缓存：**通常用于体验更好的性能以及使用 SPAN 方法监控流的系统。

3. 重新启动设备

1. 选择**操作 (Operations) > 重新启动设备 (Restart Appliance)**。
2. 在“集中管理”中确认设备状态为“已连接”。

10. 配置遥测

如果您已使用 Data Store 部署 Cisco Secure Network Analytics，则 流收集器可以同时注入多种类型的遥测。您可以在 首次设置 期间配置流量收集器，或者如果它是现有流量收集器，则可以使用 流量收集器高级设置更新遥测采集设置。

> 请确保遥测端口是唯一的。如果配置重复的遥测端口，系统会将端口重置为内部默认设置，以避免丢失流数据。例如，如果将 NetFlow 和 NVM 导出到同一遥测端口，则导出 NVM 数据的每个设备都将在流收集器上创建导出器，并耗尽流收集器引擎中的导出器资源，从而导致流数据丢失。

网络可视性模块

如果选择并配置网络可视性模块 - NVM，则流量收集器将注入并存储 NVM 流。按照 思科安全网络分析终端许可证和网络可视性模块 (NVM) 配置指南 中的说明完成配置要求。

防火墙日志

如果选择并配置防火墙日志，则流量收集器将为 Cisco Security Analytics and Logging(本地) 采集和存储防火墙事件日志。按照 安全分析和日志记录：防火墙事件集成指南 中的说明完成配置要求。

应用要求：如果您选择并配置防火墙日志，请在您的 管理器上安装 Security Analytics and Logging(本地) 应用。

更新遥测设置

如果您有一个现有的流量收集器正在注入 NetFlow 或任何其他遥测，则可以使用“流量收集器高级设置”更新您的遥测设置。以访问高级设置：

1. 登录到流量收集器(以前称为设备管理(管理员) 界面)。
2. 选择 **支持 > 高级设置**。

> 每种遥测类型都有两个设置。有关使用高级设置配置遥测的详细信息，请按照“帮助”中的说明进行操作。选择 **?(帮助) 图标 > 帮助**。

思科遥测代理

您现在可以选择使用 UDP 导向器 从多个输入获取网络遥测，转换遥测格式，以及将该遥测转发到一个或多个目的地，而不是使用 思科遥测代理 将 NetFlow 发送到您的 流收集器。要安装 思科遥测代理，按照 遥测代理虚拟设备部署和配置指南中的指示。

11. 许可 Cisco Secure Network Analytics

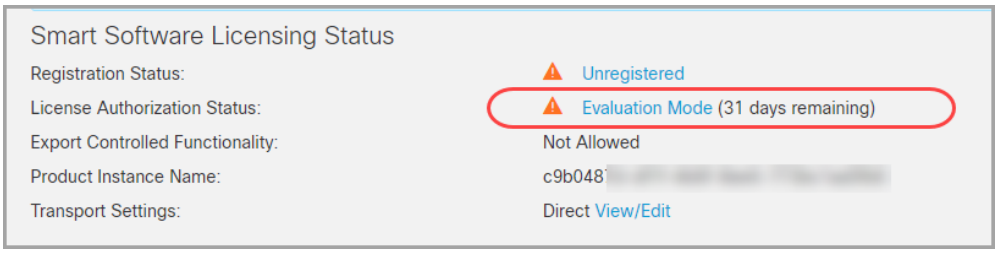
使用思科智能软件许可来许可您的 Cisco Secure Network Analytics 设备和功能。有关详细信息，请参阅 cisco.com 上的智能许可。

- **在线：**要在线使用智能许可和 Cisco Secure Network Analytics，请参阅 Cisco Secure Network Analytics 智能软件许可指南。您需要访问互联网才能进行此配置。
- **离线：**要讨论封闭/气隙网络的许可选项，请联系思科支持部门。
- **思科智能账户：**要设置思科智能账户，请在 https://software.cisco.com 注册或者联系您的管理员。

评估模式

在评估模式下使用 Cisco Secure Network Analytics 时，可在 90 天内使用选定功能。要使用 Cisco Secure Network Analytics 和最大范围的默认功能并将许可证和功能添加到您的帐户，请注册您的产品实例以获取智能软件许可。

> ⚠ 确保在 90 天评估期到期之前注册您的产品实例。当评估期到期时，系统将停止流收集。要再次启动流收集，请注册您的产品实例。



- **管理员用户：**要在 管理器中查看智能许可状态和使用详细信息，请以管理员用户身份登录。
- **剩余天数：**要查看评估模式下的剩余天数，请以管理员用户身份登录 管理器 。转到**集中管理 (Central Management) > 智能许可 (Smart Licensing)**。查看**许可证授权状态 (License Authorization Status)**。
- **产品实例名称：**“产品实例名称”是您的 Cisco Secure Network Analytics 产品实例（包括您的 管理器 和受管设备）使用的标识符。

12. 管理 Cisco Secure Network Analytics

完成设备配置后，帮助提供有关管理环境、调查行为、响应威胁等的说明。

> 要查看说明，请从任何页面选择 ?（**帮助**）图标 > **帮助** 。

配置主机组

1. 登录管理器。
2. 选择 **配置 > 检测 > 主机组管理**。

创建和管理策略

1. 登录管理器。
2. 选择 **配置 > 检测 > 策略管理**。

建立流搜索

1. 登录管理器。
2. 选择 **调查 > 流搜索**。

在报告生成器中运行报告

1. 登录管理器。
2. 选择 **报告 > 报告构建器**。

管理用户权限

1. 登录管理器。
2. 选择 **配置 > 全局用户管理**。

调查行为（警报、安全事件等）

有关调查警报、事件、主机等的信息，请查看“帮助”中的信息。

1. 登录管理器。
2. 点击 ?（**帮助**）图标。
3. 选择 **帮助**。
4. 在页面顶部，选择 **帮助** 菜单。
5. 选择**调查行为 (Investigating Behavior)**。

响应威胁

有关策略信息，请查看“帮助”中的信息。

1. 登录管理器。
2. 点击 ?(**帮助**) 图标。
3. 选择 **帮助**。
4. 在页面顶部，选择 **帮助** 菜单。
5. 选择**响应威胁 (Responding to Threats)**。

分析

Cisco Secure Network Analytics 使用动态实体建模来跟踪网络状态。在 Cisco Secure Network Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。有关详细信息，请参阅分析：检测、警报和观察指南。

要安装设备，请按照虚拟版设备安装指南、x2xx 系列硬件设备安装指南或 x3xx 系列硬件设备安装指南中的说明操作。

应用

Cisco Secure Network Analytics 应用是独立发布的可选功能，可增强和扩展 Cisco Secure Network Analytics的功能。

Cisco Secure Network Analytics 应用的发布计划独立于 Cisco Secure Network Analytics 正常升级过程。因此，我们可以根据需要更新 Cisco Secure Network Analytics 应用，而无需将其与核心 Cisco Secure Network Analytics 版本相连。有时，与 Cisco Secure Network Analytics 新版本对应的应用可能无法立即安装。您可能需要等待几周才能获得最新版本的应用。

有关最新的 Cisco Secure Network Analytics 应用的信息、可用性和兼容性，请参阅以下内容：

- Cisco Secure Network Analytics 应用版本兼容性表
- Cisco Secure Network Analytics 应用版本说明

身份验证/授权

有关每个身份验证或 Cisco Secure Network Analytics授权配置的详细信息，请参阅以下说明。

名称	说明
LDAP	请按照帮助中的相关说明来操作。 1. 登录管理器。 2. 选择 **配置 > 全局 用户管理**。 3. 点击**身份验证和授权**选项卡。 4. 选择 ?(**帮助**) 图标 > **帮助**。
安全断言标记语言单点登录 (SAML SSO)	请参阅本指南中的**配置 SAML SSO** 部分。
TACACS+ 配置指南	请参阅 TACACS+ 配置指南。

配置 SAML SSO

按照以下说明配置安全断言标记语言单点登录 (SAML SSO)。SSO 是允许用户使用一组凭证访问多个应用的身份验证程序。

详细支持信息

请注意，以下配置可能支持也可能不支持。

支持	不支持
用于 SAML/SSO 的 Microsoft Active Directory 联合身份验证服务 (ADFS)	Microsoft ADFS 云服务
Microsoft ADFS 现场解决方案	集成 Windows 身份验证 (IWA)
其他代理	外部服务
	SAML 请求签名

> 在 Data Store 部署中不支持桌面客户端。

1. 准备配置

您需要以下信息来配置 SSO：

要求	Details
身份提供程序 URL	URL 必须使用完全限定域名或 IPv4 地址。
身份提供程序证书	如果 IDP URL 以 HTTPS 开头，请下载 CA 证书。

2. 将证书上传到信任存储区

如果身份服务提供商 (IDP) URL 以 HTTPS 开头，请将 **根 CA 证书** 添加到 管理器 信任存储区。

> 如果 IDP URL 不以 HTTPS 开头，则可以跳过此步骤并转到下一部分，**3. 配置服务提供商**。

按照以下说明将根 CA 证书添加到 管理器 信任存储区。

1. 在 集中管理 清单页面上，点击 管理器的 **操作** 菜单。
2. 选择**编辑设备配置 (Edit Appliance Configuration)**。
3. 在**设备管理器 (Appliance Manager)** > **常规 (General)** 选项卡上，找到“信任存储” (Trust Store) 部分。
4. 点击**新增 (Add New)**。
5. 在**友好名称**字段中，输入证书名称。
6. 点击**选择文件**。选择新证书。
7. 点击**添加证书 (Add Certificate)**。确认新证书显示在“信任存储区”列表中。
8. 点击**应用设置**。按照屏幕上的提示进行操作。
9. **已连接：** 在清单页面上，确保 管理器 完成配置更改，且设备状态恢复为 **已连接**。

> 在配置更改处于待处理状态时，请勿强制重新启动设备。

10. 如果您有辅助 管理器，请重复 此程序 以将根 CA 证书添加到辅助 管理器 信任存储区。
11. 如果已将根 CA 证书添加到 管理器 信任存储区，请转至下一部分。

> 如果您更新 LDP 上的任何元数据，您可能会注意到 SSO 无法连接。需要更新元数据。执行此操作的最简单方法是在系统配置工具中更新新的 SSO 信息后重新启动。

3. 配置服务提供商

1. 以根身份登录到 管理器 控制台。
2. 键入 `SystemConfig`。按下 Enter 键。
3. 选择**高级 (Advanced)**
4. 选择 **SSO**。
5. 确认 **ssoEnable/Disable** 显示为**已禁用 (Disabled)**。

```
                    System Configuration
Select an SSO configuration setting.

        ssoEnable/Disable        Disabled
        CredentialDescription
        IdentityProvider(IDP)
        DownloadIDPXml           Disabled
        ServiceProvider(SP)      Not Available
        ServiceProviderProxy     Not Set
        ssoOnly                  Disabled
        Status                   Not Configured
        SaveChanges              Save Configuration Changes

                <Continue>              < Cancel >
```

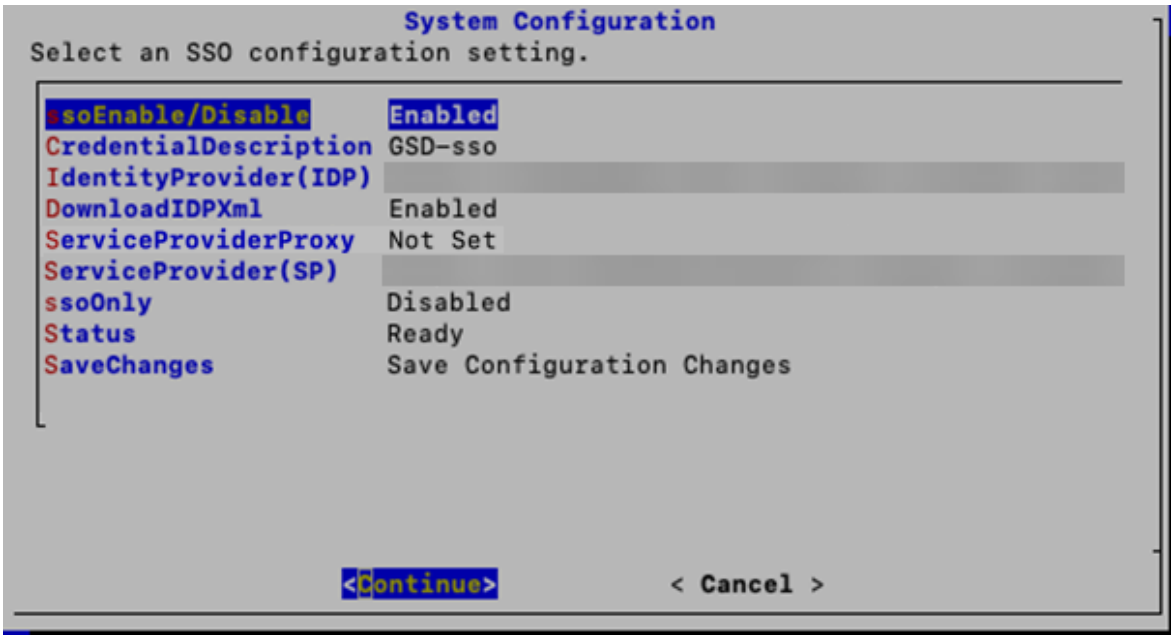
6. 选择 **IdentityProvider (IDP)**。点击**继续 (Continue)**。
7. 输入可下载身份提供程序的配置文件的 URL。

   要求：输入完全限定域名或 IPv4 地址。

8. 选择 **DownloadIDP**。按照屏幕提示启用它。
9. 选择 **SaveChanges**。点击**继续 (Continue)**。

   按照屏幕提示下载 IDP 配置文件。

10. 选择 **SSO**。
11. 查看 **ServiceProvider(SP)**。复制 URL。您将使用它来配置身份提供程序。
12. 查看**状态 (Status)**。确认它显示为**就绪 (Ready)**。



4. 启用 SSO (Enable SSO)

1. 选择 **ssoEnable/Disable**。
2. 按照屏幕提示启用 SSO。
3. 选择 **CredentialDescription**。点击**继续 (Continue)**。
4. 输入用户需要登录的 SSO 服务凭证的说明。
5. 点击**确定 (OK)**。
6. 选择 **DownloadIDP**。禁用 DownloadIDP，直到您需要保存新的 SSO 配置。
   - 点击**继续 (Continue)**。
   - 按照屏幕提示禁用 DownloadIDP。
7. 选择 **SaveChanges**。点击**继续 (Continue)**。
8. 退出系统配置。

5. 配置服务提供商代理(可选)

1. 确认 **ssoEnable/Disable** 显示为 **已启用**。
2. 选择 **ServiceProviderProxy**。
3. 输入要使用的服务提供商代理的完全限定域名 (FQDN)。
4. 点击**确定**。
5. 重新启动 管理器 以完成代理配置过程。

6. 配置标识提供程序

1. 在浏览器的地址字段中，键入服务提供商 URL。
2. 下载服务提供商元数据文件 **sp.xml**。
3. 通过 **sp.xml** 配置标识提供程序。
4. 确保传出声明类型包括用户邮件地址。

   - **例如：**如果属性存储区是 Active Directory，请将传出声明类型设置为 LDAP 属性类型用户 ID 的邮件地址。
   - **Microsoft Active Directory 联合服务 (ADFS)：**如果 IDP 类型为 ADFS，请确认是否显示以下自定义规则：

```
 c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue
(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

7. 添加 SSO 用户

按照以下说明添加 SSO 用户。用户通过身份提供程序进行身份验证。

1. 登录 管理器 (Web 应用)。
2. 选择 **配置 > 全局 用户管理**。
3. 选择**创建 (Create)** > **用户 (User)**。

   有关 说明，请点击 ?(**帮助**) 图标。选择 **帮助**。有关添加用户的详细信息，请参阅“配置用户”。

4. 填写字段以创建新用户。按如下方法来配置用户：
   - **身份验证服务：**选择 SSO。
   - **用户名：**输入 IDP 帐户的邮件地址的第一部分。确保 ID 与登录时用于 SSO 的 ID 相同。例如，对于 name@cisco.com，请在此字段中输入“name”。
5. 点击**保存 (Save)**。
6. 确认 SSO 用户显示在“用户管理”(User Management) 中。

8. 测试 SAML 登录

1. 在 Web UI 登录页面上，选择 **使用 SSO 登录**。
2. 点击凭证按钮。

3. 输入登录凭证。管理器 会打开“安全洞察控制面板”(Security Insight Dashboard)。

故障排除

场景	说明
账户锁定	通过紧急帐户访问从系统配置中禁用“仅限 SSO”(SSO Only)。
无法下载 IDP XML	确保 IDP 证书已被上传到 管理器 信任存储区。
无法保存 IDP 配置	查看 IDP 配置，确保您输入的数据准确无误，并且不包含任何额外空格。此外，请查看 IDP 事件日志。
其他问题	下载适用于您的浏览器的 SAML 跟踪器。重复 SSO 登录以查看 IDP 和 SP 之间的交换。

域

域是您要监控和管理的一组主机和其他设备。流收集器 存在于域中，一个 Cisco Secure Network Analytics 系统中可以有多个域。每个域完全独立于其他域，每个域都包含主机组树。有关主机组树与主机组的关联信息，请参阅帮助中的管理和配置主机组。

本节包括以下主题：

- Data Store 域和非 Data Store 域
- 添加和配置域
- 同步 Data Store 和非Data Store 域
- 删除域

Data Store 域和非 Data Store 域

在 设备设置工具 中配置管理器并设置系统时，您将创建一个包含 Data Store(Data Store域) 的 Cisco Secure Network Analytics 域，或不包含 Data Store (非 Data Store 域) 的域。

- **Data Store 域：** 流收集器 将其遥测数据发送到 Data Store 数据节点进行存储。
- **非 Data Store 域：**流收集器 将其遥测 Data Store 在 流收集器 或 流收集器数据库 上(仅限 5000 系列) 。
- **混合配置：**在具有混合配置的 Cisco Secure Network Analytics 中，您可以配置 Data Store 域和非 Data Store 域。配置流量收集器时，您可以选择它们将使用的域，这决定了它们将数据发送到何处。

> 如果要向非 Data Store 部署添加 Data Store 域，请查看 将 Data Store 添加到非 Data Store 部署。

添加和配置域

按照以下说明添加域并定义域设置。您还可以将非Data Store 配置导入到新 Data Store 域中。

- **角色权限：**您需要管理员或配置经理角色才能配置域。高级分析师只能查看域。
- **Data Store 域：**如果要向非 Data Store 部署添加 Data Store 域，请查看 将 Data Store 添加到非 Data Store 部署 中的说明。

1. 添加域

1. 从菜单栏中选择 **[当前域名] > 添加域**。

2. 配置以下字段：

- **域名**:将要分配给该域的名称。此名称显示在主机组树中。
- **选择方法**:选择下表中所述的一种方法,指定要对添加的域使用的主机组结构。

如果选择此方法...	那么...
默认	Cisco Secure Network Analytics 用默认主机组结构创建域,但不用任何 流收集器。
从文件导入	Cisco Secure Network Analytics 根据导出的特定域内容(主机组和/或域)创建域并使用相应的配置。有关导出包含域配置的 XML 文件的信息,请参阅 导出设置 部分。 • 包含域配置的 XML 文件不会向后兼容。这些文件仅在同一系统版本号内兼容(例如,从 流收集器 v7.0 到 管理器 v7.0)。 • 您还可以使用主机组管理页面来导入整个主机组配置。 • 如果您需要在主机组树的"网络设备"分支中从其他域导入接口组,请使用此选项。您必须先将该分组作为 XML 文件导出到您的本地驱动器中。 • 不会导入 XML 文件中包含的任何流量收集器。

如果将流量收集器添加到现有域,则该域的特定配置(策略、警报严重性、服务、导出器 SNMP 等)将应用到此流量收集器。

3. 选择 **添加域** 以选择域类型。Data Store 域适用于使用 Data Store的 Cisco Secure Network Analytics 系统,而非 Data Store 域适用于未使用 Data Store的 Cisco Secure Network Analytics 系统。有关详细信息,请参阅 **Data Store 域和非 Data Store 域**。

   如果要添加 Data Store 域,请选中 **配置为 Data Store 域** 复选框。

如果您创建了多个 Data Store 域,请勿启用分析,因为这会导致分析性能欠佳。

4. 要保存配置,请点击 **添加**。

通过导入现有非Data Store 域配置来创建 Data Store 域(可选)

如果您当前在非 Data Store 域中,并且想要将 Data Store 域添加到 Cisco Secure Network Analytics 系统,以便将来扩展到 Data Store,则可以通过将非 Data Store 配置导入新的 Data Store 域来实现。

导入现有域时,无需重新配置警报、主机组等项目。从现有域导入类似于使用现有配置创建新域。

如果域是新创建的,则必须重新配置 Cisco Secure Network Analytics 设置。

按照以下步骤添加新的 Data Store 域,并从非 Data Store 域导入其所有配置。

1. 使用**添加域**下拉菜单选择您的非 Data Store 域。
2. 从顶部菜单中，选择**配置 > 系统 > 域属性**。
3. 确保选中**导出所有配置**单选按钮。请参阅下面的 配置域设置 部分，以查看导出数据的列表。
4. 点击 **导出** 按钮以下载 XML 文件。
5. 在任意页面的左上角、主菜单的左侧，选择 **[当前域名] > 添加域**。
6. 在**域名**字段中输入新域的名称。
7. 点击“选择方法”下拉菜单，然后选择**从文件导入**选项。
8. 选择您在步骤 4 中下载的 XML 文件。
9. 点击“**配置为 Data Store** 域”复选框以将其选中。
10. 点击**添加**按钮以添加新域。

2. 配置域设置

1. 对当前添加的域完成以下设置。

设置	说明
域名	当前所在的域的名称。
存档时间	允许您设置域中的每个 流收集器 清除所有计数的时间。您可以输入介于 0 到 23 之间的整数，其中 0 为本地时区的午夜。本地时区在“存档时间”字段的右侧显示。 流收集器 会在定义的时间将所有指数计数重置为 0。此外，流收集器 会保存其在之前 24 小时内已收集的日志文件和 Web 文件，然后开始新一天的数据收集。
内部自治系统 (AS) 编号	在“内部 AS 编号”字段内点击，然后键入您的 AS 编号。使用逗号分隔多个条目，或在每个条目后按 **Enter** 键，将每个条目放在单独的行中。 You can assign internal autonomous system (AS) numbers only to domains that contain Flow Collectors When Cisco Secure Network Analytics encounters traffic containing these numbers in flow data, it categorizes the traffic as "origin" traffic on the Autonomous System Traffic document. 与来自外部系统且经过您的网络的流量(中转流量)相反，源流量表示源自或位于您的网络中的流量。 有关自治系统流量文档的信息，请参阅桌面客户端帮助中的“自治系统流量”主题。

2. 配置导出设置

通过“域属性”对话框上的“导出”页面，您可以导出具体的域内容。您可能希望将内容用作模板，用于将来添加的任何其他域。

有关与可用设置相关的信息，请参阅下表。

如果选中此复选框...	Cisco Secure Network Analytics 导出此数据...
导出所有配置*	以下“导出域配置”中列出的所有数据。此外，还会导出流量收集器以及导出器及其接口的列表。
导出主机组配置*	整个主机组定义结构，包括主机组名称和 IP 地址范围。此输出不包括策略。
导出域配置*	• 来自域属性对话框的存档时间设置。 • 所有服务定义。有关服务的信息，请参阅桌面客户端帮助中的“服务”主题。 • 所有警报配置设置。有关配置警报的信息，请参阅桌面客户端帮助中的“关于警报严重性”主题。 • 整个主机组结构，包括主机组名称和 IP 地址范围。有关更多信息，请参阅 Cisco Secure Network Analytics 帮助中的“管理和配置主机组”主题。 • 所有策略。有关更多信息，请参阅 Cisco Secure Network Analytics 帮助中的“管理核心策略”主题。 缓解警报操作仅当从默认值手动更改为*不继承*时才会导出。
* 您可用这些命令产生的任何 XML 文件来替换主机组配置。有关更多信息，请参阅桌面客户端帮助中的“如何替换主机组配置”主题。	

3. 点击**导出**。

   Cisco Secure Network Analytics 会将下载的 XML 文件中的相应设置保存到您的“Downloads”文件夹中。

> 导出与备份配置不同的域。要备份设备配置，请参阅 **创建设备配置备份**

同步 Data Store 和非Data Store 域

如果您正在将非 Data Store流收集器 转换为 Data Store流收集器，可能需要在非 Data Store 域和 Data Store 域之间保持配置和调整同步。本部分介绍将非Data Store 域与其关联的 Data Store 域同步的过程。

准备工作

确保您已创建要与非 Data Store 域同步的 Data Store 域。如果您已按照 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器**中所述的流程进行操作，则应已创建 Data Store 域。有关添加域的说明，请参阅 **添加和配置域** 。

> 您需要管理员访问权限才能执行此程序。

同步的属性

以下属性将在域之间同步：

- 数据存储域特定配置以及警报配置(如果已启用)。域配置包括：
  - 主机组管理
  - 警报严重性
  - 策略管理
  - 服务和应用
  - 导出器 SNMP 配置文件(不包括密码)
  - 域 AS 编号。

推荐的同步频率

虽然您可以根据需要随时同步域，但我们建议您将同步限制为仅在执行一组更改后进行，或者每天或每周同步一次。这是因为同步过程需要使用从日常处理中删除的资源。

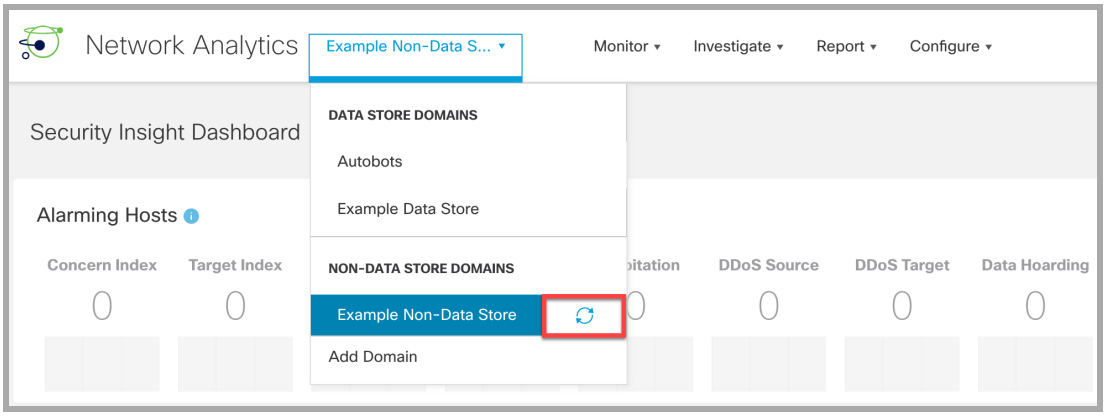
同步域过程

请按照以下步骤将非 Data Store 域(源)与 Data Store 域(目标)同步。

1. 从菜单栏中，选择要与 Data Store 域同步的非 Data Store 域。
2. 从主菜单中，选择**配置 > 系统 > 域属性**。
3. 选择**编辑**按钮。
4. 在**要同步的目标域**下拉菜单中，选择此域要与其同步的 Data Store 域。

> 您只能将目标 Data Store 域与一个源非 Data Store 域同步。如果您尝试将目标 Data Store 域与多个源非 Data Store 域同步，您将收到错误消息。

5. 点击**保存**按钮保存您所做的更改。您选择与您的 Data Store 域同步的非Data Store 域旁边会显示 同步按钮。



删除域同步目标域

请按照以下步骤删除目标域。

1. 从菜单栏中，选择要与 Data Store 域同步的非 Data Store 域。
2. 从主菜单中选择**配置 > 域属性**。
3. 选择**编辑**按钮。
4. 点击**清除目标域**按钮。
5. 点击**保存**按钮保存您所做的更改。

删除域

在删除域之前，请查看这些说明以确保您了解要求。

> ⚠ 删除域后，您将无法访问为该域收集的所有数据。确保仅删除不再需要访问其收集的数据的域。

1. 从“集中管理”删除 流收集器

如果您的域包含流收集器，请在删除域之前将其从“集中管理”中删除。您可以将流收集器添加到另一个域，但该过程包括将其重置为出厂默认设置 (RFD)。有关说明，请参阅以下内容：

1. 从“集中管理”(Central Management) 删除设备
2. 重置出厂默认设置
3. 将设备添加到“集中管理”

> ⚠ 如果从“集中管理”中删除流量收集器并删除域，则会丢失关联的流收集器数据。

2. 删除域

1. 如果首先需要访问域，请从下拉菜单中选择 **[当前域名]**。

2. 从主菜单中，选择**配置 > 系统 > 域属性**。
3. 点击**删除域**。

> ⚠ 删除域后，您将无法访问为该域收集的所有数据。确保仅删除不再需要访问其收集的数据的域。

删除 桌面客户端 域

如果在没有 Data Store 的 Cisco Secure Network Analytics 中使用 桌面客户端，还可以从 桌面客户端中删除域。

> 在决定要删除哪些桌面客户端域时，请谨慎行事，因为您将无法访问为要删除的域收集的所有数据。
>
> **解决方法**：如果您不小心删除了桌面客户端中的所有域并将自己锁定在管理器 Web 应用之外，请在桌面客户端中创建一个新的非 Data Store 域。这样，您就可以重新获得对管理器 Web 应用的访问权限。有关创建域的信息，请参阅桌面客户端帮助中的添加域主题。

集成和其他配置

我们提供以下其他集成和配置

https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html. 可能存在比此处显示的列表更多的集成。

- 为 NSEL 配置思科 ASA 以导出到 Stealthwatch
- 客户成功指标配置指南
- 启用多个 NetFlow 导出器
- 终端许可证和 Network Visibility Module (NVM) 配置指南
- 流传感器和负载均衡器配置指南
- 全局威胁警报配置指南
- ISE 和 ISE-PIC 配置指南
- Cisco Secure Network Analytics 和 SecureX 集成指南
- 受管设备的 SSL/TLS 证书指南
- TACACS+ 配置指南
- Cisco Security Analytics and Logging(本地)

密码

您可以按如下方式更改密码：

- 启用或禁用密码重置
- 将密码重置为默认设置
- 更改密码
- 更改 Data Store 数据库密码
- 更改流量收集器数据库密码（非 Data Store 域）

启用或禁用密码重置

按照以下说明启用或禁用密码重置功能。如果选择“启用”(Enable)，则可以使用 GRUB 命令行界面将密码重置为默认设置。

> ⚠ 如果禁用了密码重置并且又丢失了密码，那么您将无法访问保存到设备的数据。要再次访问设备，请重置出厂默认设置并重新配置。

1. 以根身份登录设备控制台。
2. 键入 **SystemConfig**。按下 Enter 键。
3. 选择**安全性 (Security)**。
4. 选择**重置密码 (Reset Passwords)**。
5. 按照屏幕提示启用或禁用密码重置。

将密码重置为默认设置

有两种方法可将密码重置为默认设置。

- **管理员密码：**使用 在以下位置上重置管理员密码 管理器
- **管理员、根、系统管理员密码：**使用 将管理员、根、系统管理员密码重置为默认值。

> ⚠ 将设备密码重置为默认值后，请确保更改密码。这一步对安全至关重要。有关说明，请参阅 更改密码。

在以下位置上重置管理员密码 管理器

使用以下说明在 管理器上将您的 **管理员** 密码重置为默认设置。然后，更改设备密码以实现最高安全性。

- **要求：**您需要设备根密码才能完成这些说明。
- **其他用户：**这些说明会将管理员用户重置为默认密码。单个用户密码不会被更改。

- **其他设备：**这些说明不会重置其他 Cisco Secure Network Analytics 设备（流收集器、流传感器或 UDP 导向器）上的管理员密码。

1. 以根身份登录设备控制台。
2. 键入 `rm /lancope/var/smc/config/users/admin/user.xml`。按下 Enter 键。
3. 键入 `docker restart smc`。按下 Enter 键。
4. 键入 `docker restart nginx`。按下 Enter 键。

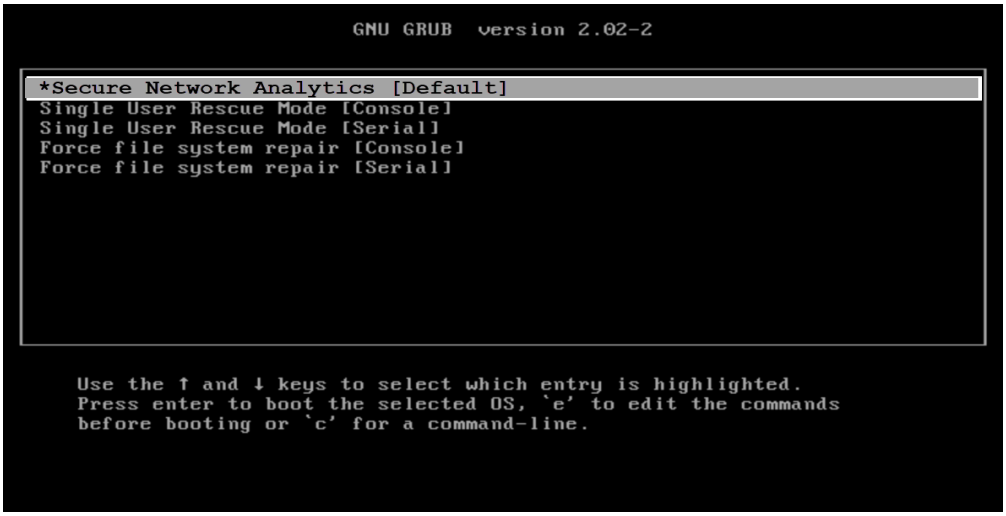
   这样会将管理员密码重置为其默认值

5. 退出设备控制台。
6. 前往 **更改密码** 以更改默认的管理员密码。这一步对安全至关重要。

将管理员、根、系统管理员密码重置为默认值

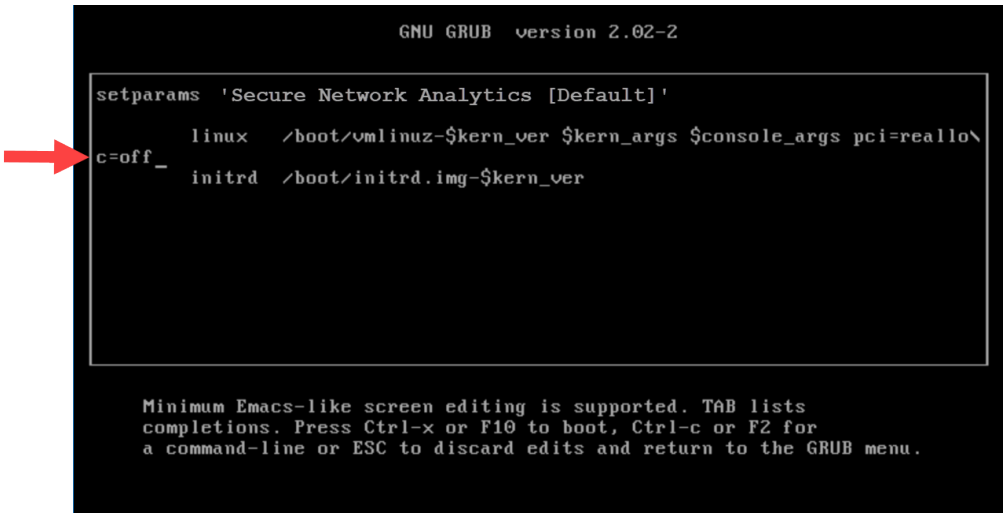
使用控制台访问将设备**管理员**、**根**、**系统管理员**密码重置为默认设置。然后，更改设备密码以确保最高安全性。

1. 登录到设备控制台（CIMC 或虚拟机监控程序）。
2. 重新启动设备。
3. 当控制台屏幕到达 GRUB 菜单时，键入“e”以进入编辑模式。



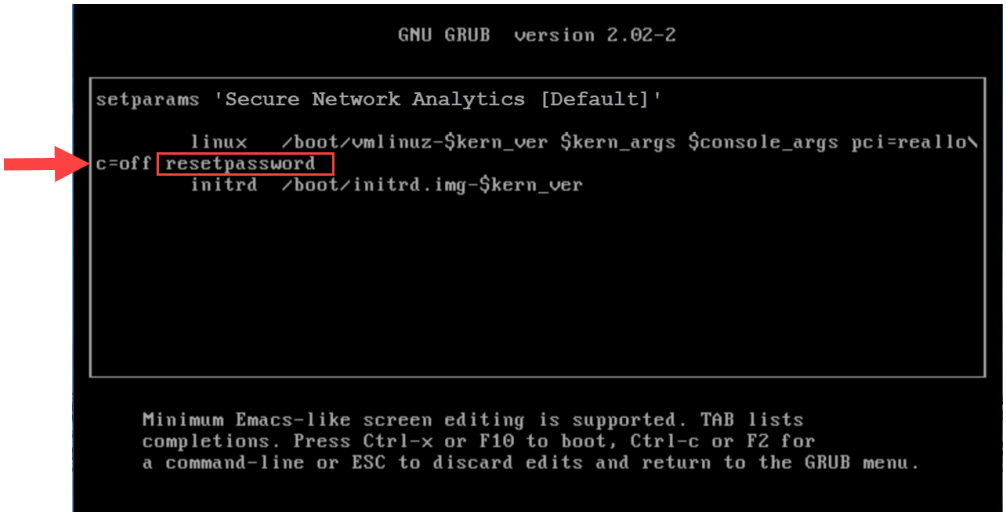
4. 让光标前进到第二行。

   命令行的外观可能略有不同，具体取决于您的设备版本。



5. 在 c=off 后键入 resetpassword，使命令行类似于以下示例：

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
 c=off resetpassword
```



6. 键入 CTRL-X 以恢复引导。

   这会将您的管理员、根和系统管理员密码重置为其各自的默认值。

7. 转到 **更改密码** 以更改默认密码。这一步对安全至关重要。

更改密码

按照以下说明更改默认密码或之前的密码。确保符合以下条件：

- **长度:** 8 到 256 个字符
- **更改:** 确保新密码与之前的密码相差至少 4 个字符。

用户	默认密码
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

更改系统管理员密码

1. 以系统管理员身份登录设备控制台。
2. 选择**安全性 (Security)**。
3. 选择**密码 (Password)**。
4. 按照屏幕提示更改系统管理员密码。
5. 退出系统配置。

更改根密码

1. 以根身份登录设备控制台。
2. 键入 **SystemConfig**。按下 Enter 键。
3. 选择**安全性 (Security)**。
4. 选择**密码 (Password)**。
5. 按照屏幕提示更改根密码。
6. 退出系统配置。

更改管理员密码 管理器

1. 以管理员身份登录 管理器 。

    - **URL:** https://<IPAddress>
    - **登录名:** admin
    - **默认密码:** lan411cope

2. 选择 **配置 > 全局 用户管理**。
3. 在列表中找到**管理员 (admin)** 用户。
4. 点击**操作 (Actions)** 菜单。选择**更改密码 (Change Password)**。
5. 按照屏幕提示更改管理员密码。符合以下条件:

- **长度**:8 到 256 个字符
- **更改**: 确保新密码与默认密码相差至少 4 个字符。

在所有其他设备上更改管理员密码

按照以下说明更改单个 数据节点、流收集器、流传感器或 UDP 导向器的管理员密码。

1. 作为管理员登录“设备管理”(Appliance Administration) 界面。

   - **URL:** https://<IPAddress>
   - **登录名**:admin
   - **默认密码**:lan411cope

2. 选择**管理用户 > 更改密码**。
3. 输入当前密码和新密码。
4. 点击**应用**。按照屏幕提示更改密码。
5. 要更改另一个设备的管理密码,请重复步骤 1 到 4。

更改 Data Store 数据库密码

使用“系统配置”更改 Data Store 数据库密码(dbadmin 和 readonlyuser)。在此过程中,您需要临时启用 SSH。

1. 以 root 用户身份登录管理器设备控制台 (SystemConfig)。
2. 从主菜单中选择 **Data Store**。
3. 选择 **SSH**。按照屏幕提示启用 SSH。
4. 从 Data Store 菜单中选择**密码**。
5. 按照屏幕提示更改密码。

   退出 Data Store 菜单时,系统会恢复之前的 SSH 设置。

更改流量收集器数据库密码(非 Data Store 域)

使用“集中管理”页面上的“数据库”选项卡更新非 Data Store 域中所有 流收集器 数据库的流收集器 数据库密码。

> 确保更改默认密码。当有新的流量收集器添加到“集中管理”时,数据库密码会自动更新以匹配当前密码。

1. 打开“集中管理”。
2. 点击“数据库”选项卡。

3. 要生成随机密码，请点击**生成密码**按钮，或在“密码”和“确认密码”字段中输入您的密码。
4. 选中 **显示密码** 复选框可查看您选择的密码。
5. 点击**应用设置**按钮以保存更改。

> 当您更改数据库密码时，只有非 Data Store 流量收集器和转换流量收集器会收到新密码。

SSL/TLS 设备身份和 其他 SSL/TLS 客户端身份

使用 SSL/TLS 设备身份和其他 SSL/TLS 客户端身份管理所选设备的安全套接字层 (SSL) 和传输层安全 (TLS) 证书。请按照受管设备的 SSL/TLS 证书指南中的说明执行所有与证书相关的更改。

> ⚠ 证书对于保障系统安全至关重要。不当修改证书可能会停止 Cisco Secure Network Analytics 设备通信并导致数据丢失。请按照受管设备的 SSL/TLS 证书指南中的说明执行所有与证书相关的更改。

设备身份

每个 Cisco Secure Network Analytics 7.x 版设备都安装有一个唯一的自签名设备身份证书。要替换设备身份证书，请按照受管设备的 SSL/TLS 证书指南中的说明操作。

设备使用 SSL 证书向其他设备证明自己的身份。例如，当 管理器 生成流查询并与 流收集器 通信时，管理器 通过提供其服务器身份证书进行身份验证。流收集器 检查所提供的服务器身份证书是否为可信证书。

客户端身份

客户端身份用于外部服务之间的通信。有关详细信息，请参阅受管设备的 SSL/TLS 证书指南中的说明。

查看证书

按照以下说明查看所选设备的设备身份证书或客户端证书。

1. 打开集中管理 (Central Management)。
2. 点击设备的 ··· (**省略号**) 图标。
3. 选择**编辑设备配置**。
4. 选择**设备**选项卡。
5. **要查看设备身份证书，**请转至“SSL/TLS 设备身份”部分。

   要查看客户端身份证书，请转至“其他 SSL/TLS 客户端身份”部分。

> ⚠ 证书对于保障系统安全至关重要。不当修改证书可能会停止 Cisco Secure Network Analytics 设备通信并导致数据丢失。请按照受管设备的 SSL/TLS 证书指南中的说明执行所有与证书相关的更改。

使用自定义证书将设备添加到“集中管理”

有关详细信息，请参阅 **将设备添加到“集中管理”**。如果设备具有自定义证书，请确保在将设备添加到“集中管理”之前，将身份证书和证书链(根证书和中间证书)保存到 管理器 信任存储区。有关操作说明，请参阅受管设备的 SSL/TLS 证书指南

> ⚠ 如果设备具有自定义证书，请确保在将设备添加到“集中管理”之前，将身份证书和证书链(根证书和中间证书)保存到 管理器 信任存储区。有关操作说明，请参阅受管设备的 SSL/TLS 证书指南

更改主机名、网络域名或 IP 地址

在安装和配置设备后，要更改设备的主机名、网络域名或 IP 地址，请按照受管设备的 SSL/TLS 证书指南中的说明操作。

作为此操作过程的一部分，您将暂时从“集中管理”(Central Management) 中删除设备，并自动替换设备身份证书。

> 作为此操作过程的一部分，系统将自动替换设备身份证书。
>
> ⚠ **如果设备使用自定义证书，**请联系 思科支持部门 来更改这些设置。请勿使用此处显示的说明。确保您拥有自定义证书和私钥的副本。

查看信任存储区证书

将证书添加到设备信任存储区，即表示无论该身份是另一个 Cisco Secure Network Analytics 设备还是外部服务，您都允许与其通信。

- **说明：**请按照 受管设备的 SSL/TLS 证书指南 中的说明执行所有信任存储区更改。
- **上传单个文件：**如果您的文件包含多个证书，请将每个证书逐一上传到信任存储区。

> ⚠ 将证书添加到设备信任存储区后，设备会信任该身份，并允许与其通信。请按照受管设备的 SSL/TLS 证书指南中的说明执行所有信任存储区更改。

按照以下说明查看保存到所选设备信任存储区的证书。

1. 打开集中管理 (Central Management)。
2. 点击设备的**操作** 菜单。
3. 选择**编辑设备配置**。
4. 选择**常规**选项卡。
5. 查看**信任存储区**列表。

威胁源

Cisco Secure Network Analytics 威胁源(以前称为 Stealthwatch 威胁情报源) 提供来自全局 威胁源 的有关对您的网络威胁的数据。威胁情报源会经常更新,内容包括已知用于恶意活动的 IP 地址、端口号、协议、主机名和 URL。威胁情报源中包含以下主机组:命令和控制服务器、Bogon 以及 Tor。

许可

将 威胁源 许可证添加到思科智能账户。有关说明,请参阅 Cisco Secure Network Analytics 智能软件许可指南。

正在启用

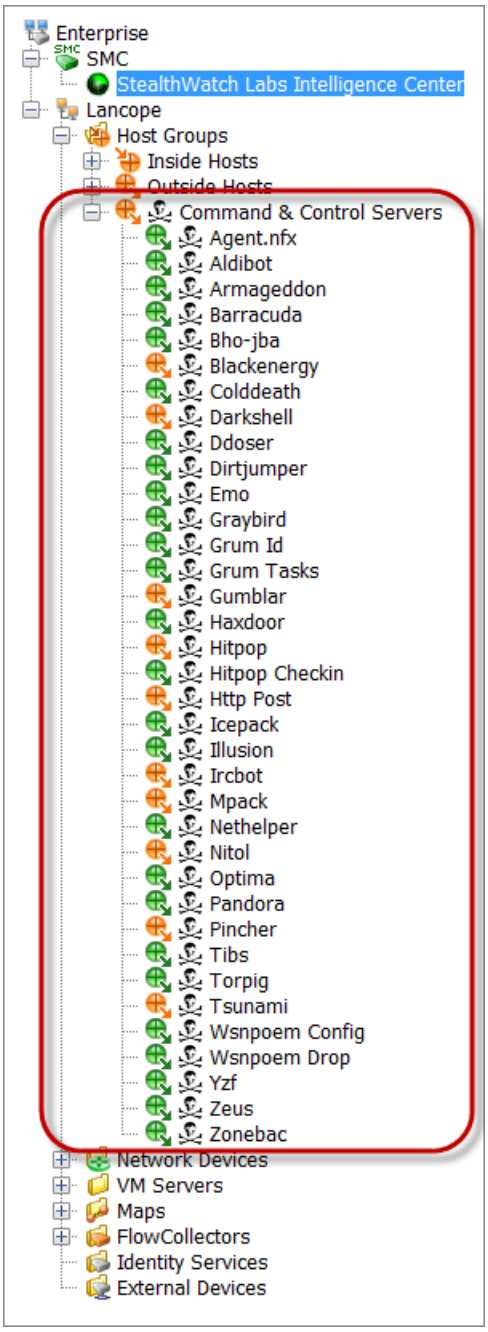
要在"集中管理"中启用源,请按照帮助中的说明操作。请注意,作为说明的一部分,您将配置 DNS 服务器和防火墙。并且,如果有故障转移配置,请确保在主管理器和辅助管理器上启用威胁源。

1. 登录您的主管理器。
2. 选择**配置 > 全局 > 集中管理**。
3. 点击 ?(**帮助**) **图标**。选择 **帮助**。
4. 选择 **设备配置 > 威胁源**。

查看警报和安全事件

启用 威胁源 后, Stealthwatch 实验室智能中心图标将显示在具有警报状态的桌面客户端企业树中,威胁将显示在其各自的主机组分支中。有关更多信息,请参阅 桌面客户端用户指南 或帮助。

> **帮助:** 要访问帮助,右键点击 Stealthwatch **实验室智能中心** 分支,然后选择**配置 (Configuration) > SLIC 威胁源配置 (SLIC Threat Feed Configuration)**。点击**帮助 (Help)**。



集中管理(管理设备)

使用“集中管理”从主 管理器管理设备。我们在此处提供了“集中管理”的概述,有关每个部分的详细信息,请参阅帮助。

- **关于集中管理:**当您的设备由“集中管理”(Central Management)进行管理时,您可以查看其状态并管理以下内容:编辑设备配置、更新软件、重新启动,关闭等。
- **帮助:**要打开“帮助”,请点击 ?(**帮助**)图标。选择 **帮助**。

本节包含以下主题:

- 集中管理和设备管理界面
- 打开“集中管理”
- 打开“设备管理”
- 编辑设备配置
- 查看设备统计信息
- 从“集中管理”删除设备
- 将设备添加到“集中管理”
- 创建设备配置备份
- 启用/禁用 SSH

集中管理和设备管理界面

如果通过“集中管理”(Central Management)来管理设备,您需要在“集中管理”(Central Management)和设备管理界面(设备管理)中访问设备的功能,如下所示:

集中管理	“设备管理”界面
编辑设备配置	查看系统统计信息
查看许可证状态(概览)	
备份配置文件	备份数据库文件
查看审核日志	创建诊断包
重新启动	网络主机和 IP 查找
关闭	数据包捕获
更新软件	清除 DNS 缓存

	设备特定配置

> 如果您对流收集器进行配置以实现 Data Store 兼容性，则“设备管理”界面(“设备管理”)会隐藏某些功能。使用“集中管理”来配置 流收集器 和其他相关任务。

打开“集中管理”

1. 登录您的主管理器。
2. 选择**配置 > 全局 > 集中管理**。

打开“设备管理”

您还可以通过“集中管理”(Central Management) 或直接登录设备来打开“设备管理”(Appliance Admin) 界面。

通过“集中管理”(Central Management) 打开“设备管理”(Appliance Admin)

1. 在 集中管理 清单页面上，点击设备的 **操作** 菜单。
2. 选择**查看设备统计信息**。
3. 登录“设备管理”界面。

通过直接登录打开“设备管理”

1. 在浏览器地址栏中，键入设备 IP 地址，如下所示：

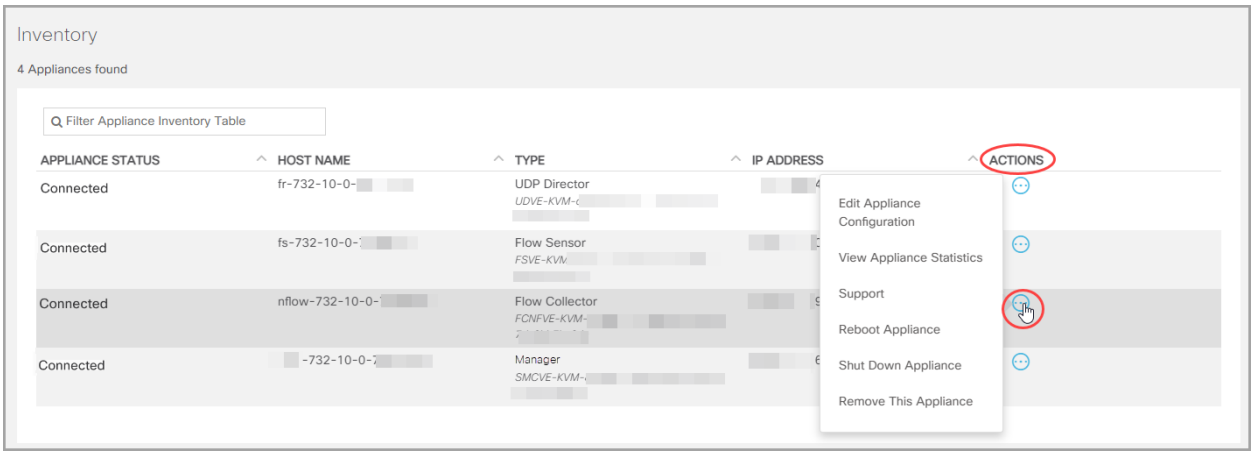
   https://<IPAddress>

   - **管理器：**在 IP 地址后添加 **/管理器index.html** 。
   - **例如：**https://1.1.1.1/管理器/index.html

2. 按下 Enter 键。

编辑设备配置

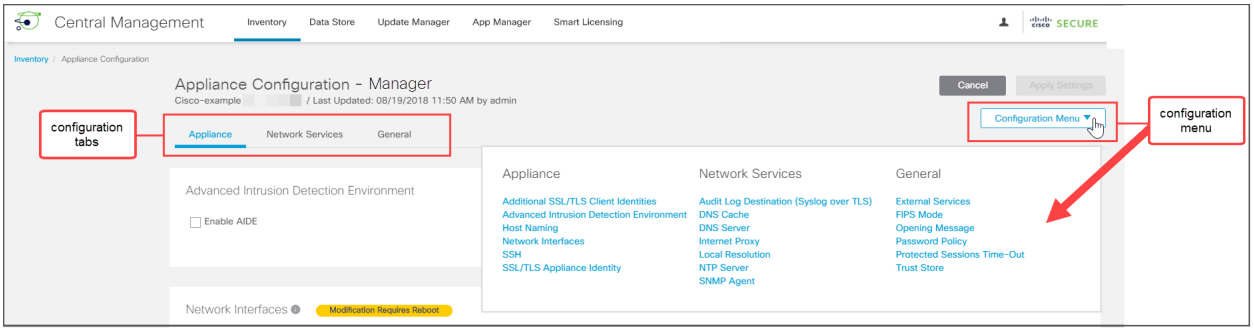
1. 在 集中管理 清单页面上，点击设备的 **操作** 菜单。
2. 选择**编辑设备配置 (Edit Appliance Configuration)**。



3. 点击**配置 (Configuration)** 菜单。从列表中选择一项。

   或

   点击每个选项卡以查看每个配置类别。



4. 根据需要对每个配置部分进行更改。您可以在每个配置选项卡上编辑多个配置类别。

> 有关说明，请点击 **用户 (User)** 图标。

5. 点击**应用设置 (Apply Settings)**。按照屏幕提示保存配置更改。

   某些更改需要重新启动系统。如果您愿意等待，则可以恢复更改，编辑配置设置，并稍后重启。

> 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。要确认设备状态为“已连接”，请查看“集中管理”>“库存”清单。

6. **已连接：**在清单页面上，确保设备完成配置更改，且设备状态恢复为 **已连接**。

查看设备统计信息

悬停：要查看每个设备状态的更多信息，请将指针悬停在状态上。

要查看系统统计信息、服务、磁盘使用情况和 Docker 服务，请登录“设备管理”(Appliance Admin) 界面：

1. 在 集中管理 清单页面上，点击设备的 **操作** 菜单。
2. 选择**查看设备统计信息**。
3. 登录“设备管理”界面。

从“集中管理”删除设备

按照以下说明从中央管理器删除设备。

1. 在 集中管理 清单页面上，点击设备的 **操作** 菜单。
2. 选择**删除此设备**。

   - **Data Store 设备：**请转至 **从中央管理器删除 Data Store 设备**，了解其他要求。
   - **流收集器：**如果您从“集中管理”中删除流量收集器，它也会从域中删除。如果您计划将其添加到其他域，则需要重置出厂默认设置 (RFD)。有关说明，请转至 **将设备添加到“集中管理”** 和 **从“集中管理”删除设备**。
   - **配置通道关闭：**如果由于配置通道关闭而移除设备，请转到故障排除中的配置通道关闭程序，以了解更多说明。
   - **故障排除：**如果您登录到设备管理界面，但设备未从“集中管理”(Central Management) 中删除，请转到故障排除中的配置通道关闭程序以使用“系统配置”(System Configuration) 将其删除。
   - **集中管理：**要将设备添加到其他中央管理器，请使用“设备设置工具”。

> ⚠ 如果设备具有自定义证书，请确保在将设备添加到“集中管理”之前，将身份证书和证书链(根证书和中间证书)保存到 管理器 信任存储区。有关操作说明，请参阅受管设备的 SSL/TLS 证书指南

从中央管理器删除 Data Store 设备

如果从中央管理器(管理器、流收集器、数据节点)中删除 Data Store 设备，则不会将其从 Data Store 中删除。这需要手动清理。

- **管理器和 流收集器：**对于 管理器和 流收集器，可以从 **/lancope/var/services/data-store/config-datastore-inventory-snapshot** 目录中删除它们。
- **数据节点：**联系 思科支持部门 以获取有关删除 数据节点的帮助，因为该过程更加复杂。

将设备添加到“集中管理”

使用设备设置工具将设备添加到“集中管理”(Central Management)。请务必查看以下内容:

- **自定义证书:** 如果设备具有自定义证书,请确保在将设备添加到“集中管理”之前,将身份证书和证书链(根证书和中间证书)保存到其自身的信任存储区以及 管理器 信任存储区。有关操作说明,请参阅受管设备的 SSL/TLS 证书指南
- **管理器 管理凭证:** 您需要使用 管理器用户 ID 和密码才能将设备添加到“集中管理”。
- **RFD:** 如果在设备上重置出厂默认设置,请在将设备 IP 地址、主机名和域添加到集中管理之前进行配置(即使在 RFD 时保留网络设置)。

  以**系统管理员**身份登录设备控制台,并按照屏幕提示配置 IP 地址、主机名和域。有关说明,请参阅 Cisco Secure Network Analytics 硬件或虚拟版安装指南。

- **新安装:** 如果这是新安装,请确保完成安装并配置 IP 地址、主机名和域,然后再将其添加到“集中管理”(Central Management)。有关说明,请参阅 **1. 使用首次设置配置环境**。

> ⚠ 如果设备具有自定义证书,请确保在将设备添加到“集中管理”之前,将身份证书和证书链(根证书和中间证书)保存到 管理器 信任存储区。请参阅受管设备的 SSL/TLS 证书指南。

1. 登录到设备。

   在浏览器地址栏中,键入设备 IP 地址,如下所示: **https://<IPAddress>**

2. 将 URL 的末尾替换为 /lc-ast:

   https://<IPAddress>/lc-ast

3. 按下 Enter 键。
4. 点击**下一步 (Next)** 以滚动到“集中管理”(Central Management) 选项卡。
5. **IP 地址:** 输入 管理器/中央管理器 IP 地址。
6. 点击**保存**。
7. 按照屏幕上的提示输入 管理器 管理凭证,并完成配置。根据设备类型,您可能需要输入其他信息。
8. 有关“设备设置工具”的详细信息,请参阅 **2. 配置受管系统**

创建设备配置备份

使用“集中管理”备份设备配置。

> 在备份设备之前，请确保按照“帮助”中的说明进行操作。要备份 Data Store，请参阅 **创建 Data Store 备份**。要备份 流收集器 数据库，请参阅 **创建数据库备份(非Data Store 域)**。

1. 打开“集中管理”。
2. 点击设备的 ··· (**省略号**)图标。
3. 选择**支持**。
4. 选择 **配置文件** 选项卡。
5. 选择 ?(**帮助**)图标。请按照帮助中的相关说明来操作。

   要恢复设备配置备份，请按照“帮助”中的说明进行操作。

启用/禁用 SSH

使用此部分来控制通过 SSH(安全外壳)访问设备的能力。

默认值:禁用

> ⚠ 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。

打开 SSH

按照以下说明打开所选设备的 SSH。

1. 打开集中管理 (Central Management)。
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。

启用 SSH

1. 找到 SSH 部分。
2. 要在设备上允许 SSH 访问，请选中**启用 SSH** 复选框。
3. 要在设备上允许根访问，请选中**启用根 SSH 访问**复选框。
4. 点击**应用设置**。
5. 按照屏幕上的提示进行操作。

禁用 SSH

1. 要在设备上删除 SSH 访问，请点击**启用 SSH** 复选框以清除它。
2. 要在设备上删除根访问，请点击**启用根 SSH 访问**复选框以清除它。
3. 点击**应用设置**。
4. 按照屏幕上的提示进行操作。

创建数据库备份(非Data Store 域)

按照以下说明备份管理器和流量收集器数据库。要备份 Data Store，请参阅 **创建 Data Store 备份**。

> ⚠ 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。另请注意，此程序仅适用于非 Data Store 流收集器。如需帮助，请联系 思科支持部门。

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

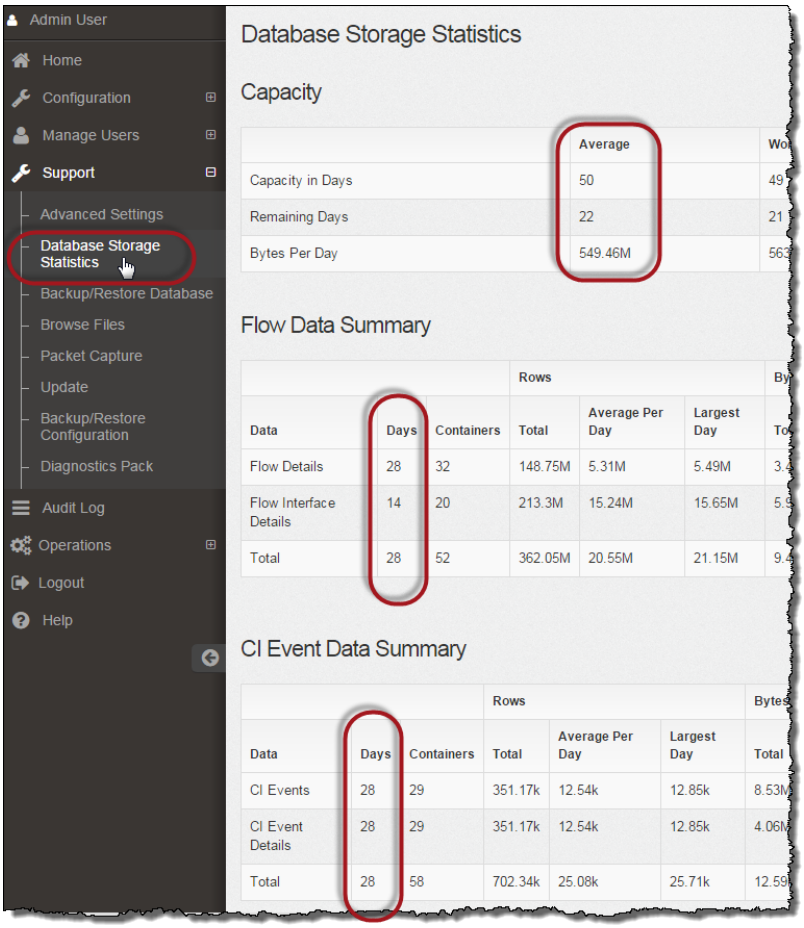
流量收集器数据库备份可能需要多天才能完成，如果数据库很大，则会降低网络速度。我们建议您在备份数据库之前先整理流量收集器数据库。这样可以释放用于存储流的可用磁盘空间，并减少备份数据库所需的时间。

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(/lancope/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。

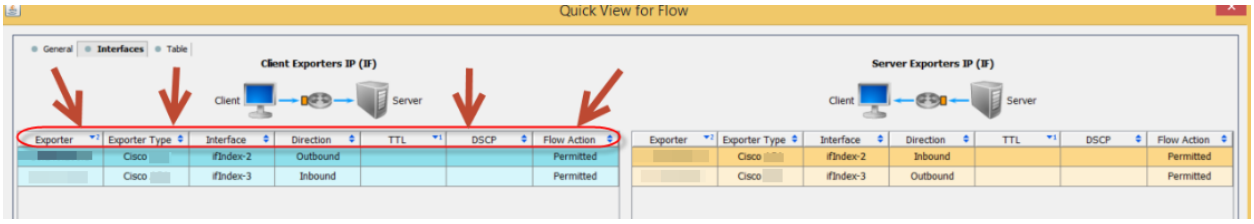
1. 登录流量收集器设备管理界面。
2. 选择**支持 > 数据库存储统计信息**。
3. 在“容量”、“流数据摘要”和“CI 事件数据摘要”(或“安全事件数据摘要”)中检查存储的天数。



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。Cisco Secure Network Analytics 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。



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**。
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**。
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 管理器 和 流收集器 数据库上保存的任何快照。

> ⚠ 请确定您要删除 管理器 和 流收集器 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 管理器 和 流收集器 设备控制台。
2. **查看快照：**类型：

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -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 lan1cope -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 管理器 和 流收集器 数据库快照。

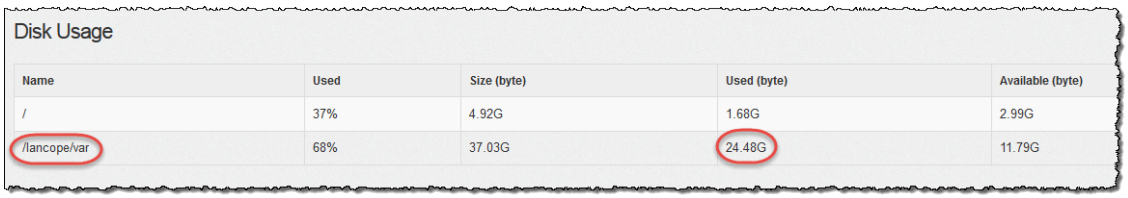
3. 备份远程文件系统

要将数据库备份到远程文件系统,请完成以下步骤:

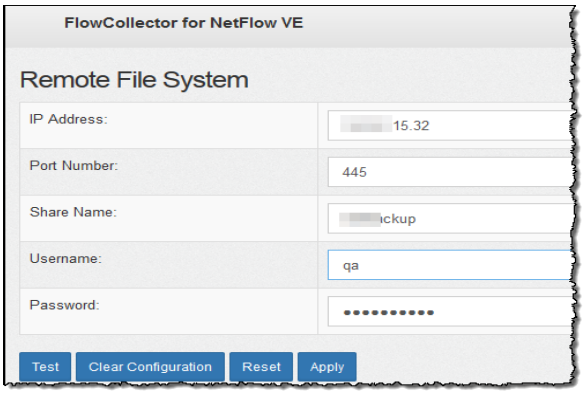
- **空间:**确保远程文件系统有足够空间来存储数据库备份。
- **时间:**备份一次数据库后,后续备份速度会加快,因为该过程仅备份自上次备份以来发生的更改。此过程每分钟备份约 0.5 GB 到 2 GB 的数据。

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**。
   - 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。



3. 单击**配置 > 远程文件系统**。



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. 单击**应用**将设置置于配置文件中。

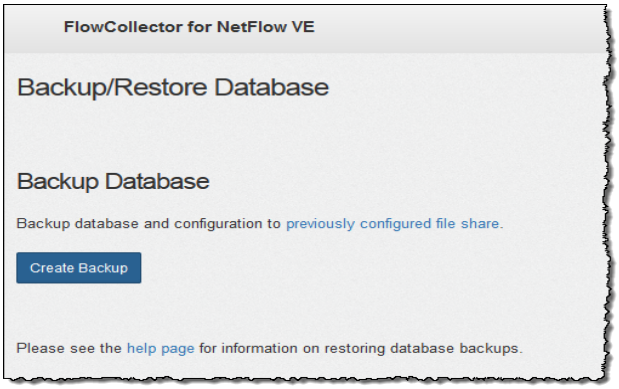
   如果在输入密码后,“应用”按钮未启用,请在“远程文件系统”页面的空白区域中单击一次以启用此按钮。

6. 单击**测试**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. 单击**支持 > 备份/恢复数据库**。此时将打开“备份数据库”页面,如以下示例所示。



8. 点击**创建备份**。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**,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**。

9. 点击**关闭**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 管理器 和 流收集器 数据库中的快照。

> 请确定您要删除 管理器 和 流收集器 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 管理器 或 流收集器 设备控制台。
2. **查看快照:**输入以下命令行:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -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 lan1cope -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 管理器 和 流收集器 数据库快照。

恢复数据库备份(非Data Store 域)

按照以下说明恢复管理器和流量收集器数据库。要恢复 Data Store，请参阅 **恢复 Data Store 备份**。

概述

> ⚠ 我们建议您在恢复数据库之前联系 思科支持部门 。

恢复数据库操作将使用先前备份的内容**覆盖**您当前的数据库和配置。现有网络设置不会被覆盖。

- **相同版本：**不能使用先前版本的 Cisco Secure Network Analytics 设备的备份文件来恢复设备数据库。确保备份文件版本与设备版本匹配。
- **恢复以前的备份：**可以使用命令行界面来恢复以前的数据库备份。备份的数据库是存在于以前配置的远程文件系统(即文件共享)中的数据库。
- **默认：**如果您未指定要恢复的数据库的名称，系统将使用默认名称(您的系统的序列号)。

恢复数据库

> ⚠ 恢复数据库操作将使用先前备份的内容覆盖您当前的数据库和配置。现有网络设置不会被覆盖。
>
> 在恢复进程开始后不要中断。

启动操作后，您可离开页面(“移开鼠标”)，进程将继续，不会中断。您返回后，系统将更新状态。

1. 以系统管理员身份登录设备控制台，访问根 shell。
2. 键入 **sysadmin**，然后按 **Enter**。
3. 显示密码输入提示时，键入 **lan1cope**，然后按 **Enter**。
4. 在“系统配置”菜单中，选择**高级**，然后按 **Enter**。
5. 选择**根 Shell**，然后按 **Enter**。
6. 键入根 shell 密码，然后按 **Enter**。
7. 运行以下命令：

   ```
   cd /var/tmp
   nohup doDbRestore -c -q &
   ```

   如需查看可以使用此工具的交换机，请输入以下命令：`doDbRestore -h`

> ⚠ 如果您未指定要恢复的数据库的名称,系统将使用默认名称(您的系统的序列号)。

8. 要查看正在进行的恢复操作的状态,您可以显示两个文件:

   /lancope/var/logs/VerticaRestore.log

   /lancope/var/logs/DatabaseRestore.log

   完成恢复操作后,系统将重启,然后开始收集数据。

Data Store 数据库

如果已配置具有 Data Store 的 Cisco Secure Network Analytics，则可以访问“集中管理”中的 Data Store 选项卡。

> 要将 Data Store 添加到配置中，请参阅 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器** 和 **将 Data Store 添加到非 Data Store 部署**。

Data Store 选项卡

使用“集中管理”中的 Data Store 选项卡执行以下操作：

- **状态：**查看数据库或任何 数据节点的状态。有关详细信息，请参阅查看 **查看 Data Store 数据库状态** 。
- **启动或停止：**启动或停止数据库或任何 数据节点。有关详细信息，请参阅查看 **查看 Data Store 数据库状态** 。
- **存储使用情况：**查看数据库的当前存储使用情况统计信息。您可以为流接口数据修改保留状态 。有关更多信息，请参阅 **查看数据库保留**。
- **更新状态：**在更新期间查看所有 数据节点的状态。有关详细信息，请参阅 **监控 数据节点 更新状态**。

> 确保在所有 数据节点上启用 SSH。如果未在所有 数据节点上启用 SSH，则无法成功完成某些数据库操作。

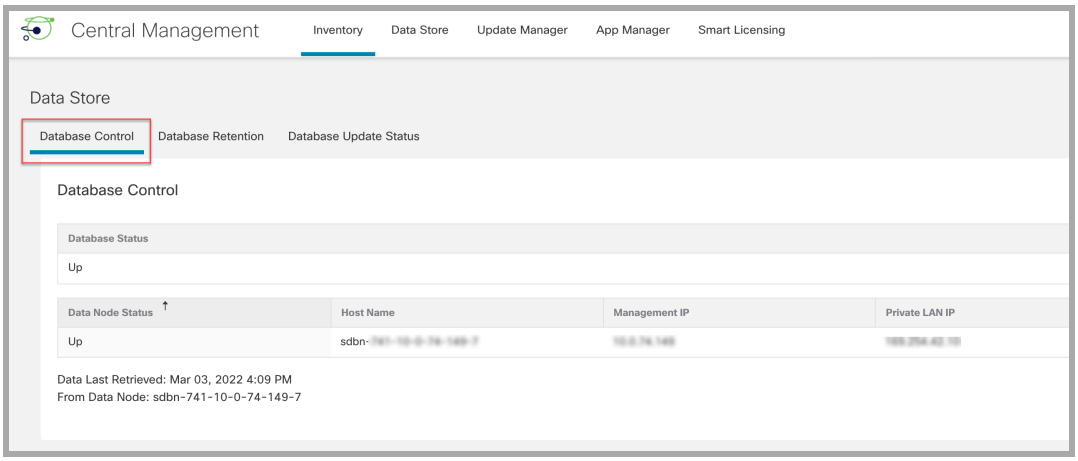
打开 Data Store 选项卡

1. 登录管理器。
2. 选择 **配置 > 全局 集中管理**。
3. 点击**Data Store**选项卡。

查看 Data Store 数据库状态

点击“集中管理”上的 Data Store 选项卡时，系统会打开“数据库控制”选项卡页面。此选项卡显示数据库和每个数据节点的状态。

- **排序：**默认情况下，此选项卡上的 数据节点按其专用 LAN IP 排序。您可以点击要作为排序依据的列标题，对 数据节点 节点重新排序。
- **状态：**在正常情况下，您的数据库和所有 数据节点都将显示 **运行**状态。您的数据库可能为“运行”，但其中一个 数据节点的状态可能为“关闭”。恢复故障 数据节点后，您可能会看到数据库显示为“运行”，但新恢复的 数据节点 处于“正在恢复”状态。
- **操作菜单：**确保使用“操作”菜单启动或停止数据库（或 Data Node）。



确保使用“操作”菜单启动或停止数据库(或 Data Node)。

启动数据库

1. 确保选中“数据库控制”选项卡。
2. 在数据库的“操作”列中，点击 ••• (**省略号**)图标 。
3. 选择 **启动**。
4. 确认数据库状态显示为“运行”。

停止数据库

1. 确保选中“数据库控制”选项卡。
2. 在数据库的“操作”列中，点击 ••• (**省略号**)图标 。
3. 选择 **停止**。
4. 确认数据库状态显示为“关闭”。

启动 数据节点

请按照以下步骤启动数据节点。

1. 确保选中“数据库控制”选项卡。
2. 找到要启动的 数据节点 。点击“操作”列中的 ••• (**省略号**)图标。
3. 选择**启动**以启动数据节点。
4. 确认 数据节点 状态显示为“运行”。

停止 数据节点

请按照以下步骤停止数据节点。

1. 确保选中“数据库控制”选项卡。
2. 查找要停止的 数据节点 。点击“操作”列中的 ··· (**省略号**) 图标。
3. 选择**停止**以停止数据节点。
4. 确认 数据节点 状态显示为“关闭”。

查看上次操作结果

无论用户数量如何，任何时候都只能进行一项操作。当某项操作正在进行时，无法执行其他操作。操作完成后，将在屏幕顶部的横幅中对所有用户显示完成状态。请按照以下步骤查看上次操作结果。

1. 确保选中“数据库控制”选项卡。
2. 点击屏幕底部的**上次操作结果**链接。“操作结果”横幅将保留在屏幕上，直到您将其关闭。

查看数据库保留

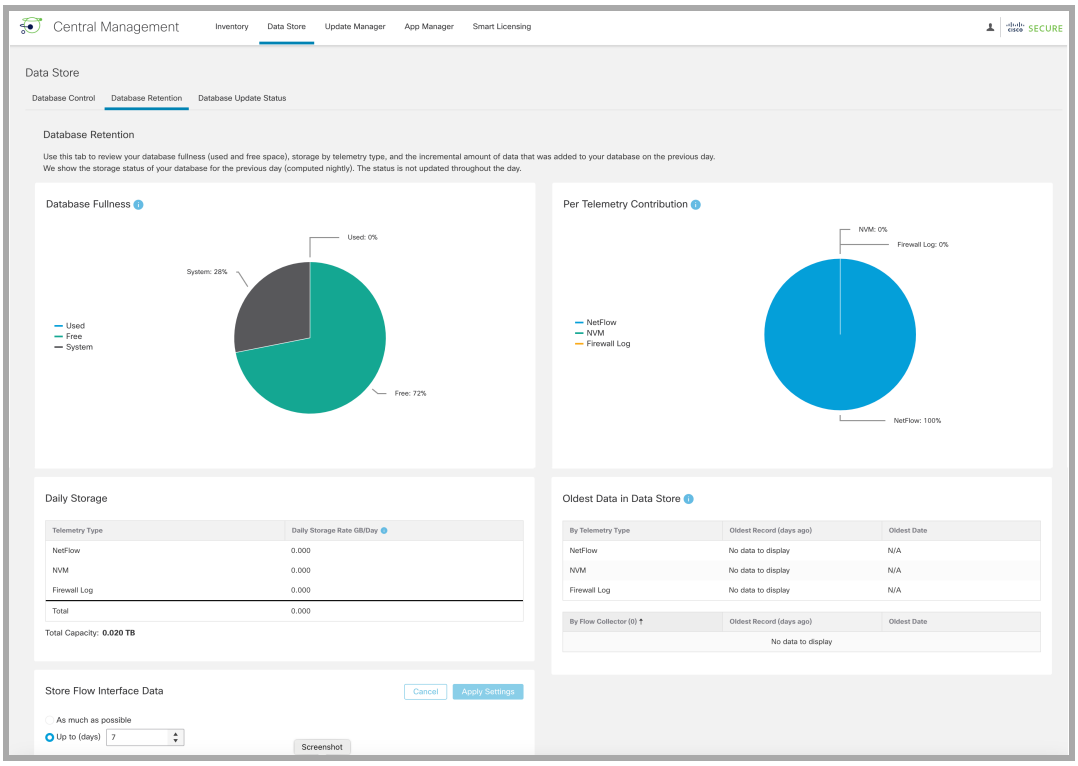
“数据库保留”选项卡可回答以下问题：

- 我的数据库有多满？
- 每种遥测类型（NetFlow、NVM、防火墙日志）在此占用度的占比为多大？
- 昨天我的数据库中新存储了多少数据？
- 我的数据库的总容量是多少？

> 此页面上的所有图表以及“数据存储统计信息”部分每天更新一次。

打开“Data Store” -“数据库保留”选项卡

1. 选择**配置 > 全局 > 集中管理**。
2. 点击**Data Store**选项卡。
3. 点击**数据库保留**选项卡。



数据库占用度图表

“数据库占用度”图表显示 Data Store 数据库中的已用空间和可用空间。

每项遥测的占用度图表

“每项遥测的占用度”图表显示 Data Store 数据库中现有数据的细分。

每日存储

“每日存储”部分显示前一天添加到数据库的数据增量。通过监控每日存储速率，您可以评估数据库的填充速度以及每种遥测类型对每日存储累积的占用度。

Data Store 中最早的数据

此表显示自最早记录写入 Data Store 以来的日期和天数。此数据每天更新一次。

此表中不包含本地存储在流量收集器(或流量收集器数据库)中的数据。如果正在从非 Data Store 流量收集器转换为 Data Store 流量收集器并已制定数据保留策略，可以使用此表来了解您的 Data Store 中有多少新数据，并了解何时是完成转换的理想时间。

更改流接口数据存储

流量接口统计信息提供流统计信息的更详细视图。它们可通过在网络中为给定流量提供多个有利位置来排除故障和调查最近的流数据。例如，如果在多个导出器或同一导出器的多个接口上观察到流量，则详细信息会存储在流量接口统计信息中。

Data Store 会尽可能长时间地保留数据，而保留时间的长短取决于系统的注入速率。一旦 Data Store 达到最大容量，它就会开始自动删除最早的数据。

流量接口统计信息以更高的速率消耗存储，可能会减少您可以保留其他重要数据（例如流统计信息）的时间。

> 更改流接口数据存储期仅影响占用系统空间的数据的 NetFlow 部分。默认值为 7 天。您可以根据需要增加或减少保留天数。

1. 在存储流接口数据部分中，选择 **尽可能多** 或 **最多天数**（点击向上或向下箭头可更改天数）。
2. 点击**应用设置**。

   - 将保留期更改为更长时段时，等到所相差的时间结束，然后存储的数据才会准确对应于保留期设置。在此时间之前，使用最低（最粗糙）的可用时间间隔来显示数据。例如，如果将保留时间从 3 天改为 10天，现在您就需要等待 7 天，然后存储的数据才会准确对应于保留期设置。
   - 数据可能会比您选择的保留期更早被删除，这是由于根据磁盘使用情况对数据进行了关键性的修剪。如果您选择存储数据的时间尽可能长，当 Data Store 达到最大容量时，系统就会开始删除最早的数据。

监控 数据节点 更新状态

从 数据节点集中管理更新管理器启动 数据节点更新后，可使用"数据库更新状态"选项卡监控每个上的数据库服务更新进度。

打开 Data Store -"数据库更新状态"选项卡

1. 选择 **配置 > 全局 集中管理**。
2. 点击**Data Store**选项卡。
3. 点击**数据库更新状态**选项卡。

监控数据库更新状态

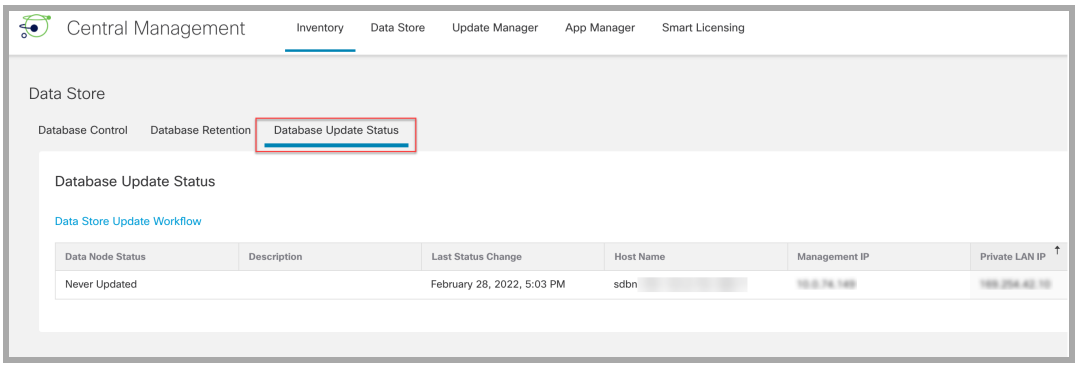
在更新期间，每个数据节点都会经历一系列状态。点击"Data Store 更新工作流程"链接，可直观地再现更新过程（如下所示）。

> 为实现成功更新，请按照 Cisco Secure Network Analytics 系统更新指南中的更新顺序和说明操作。

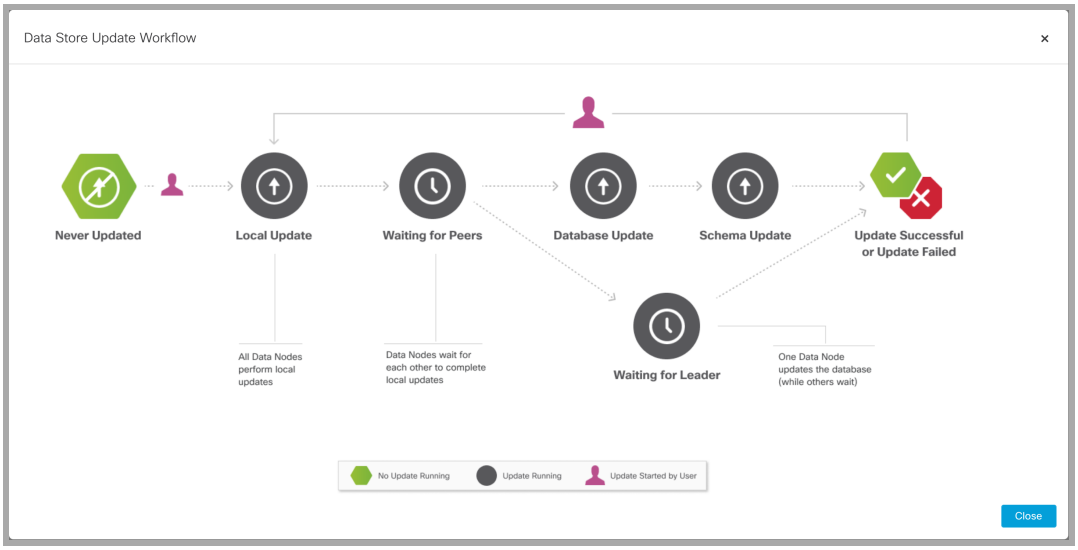
> 下图所示的一些状态转换在更新过程中转瞬即逝，因此在屏幕刷新时您可能看不到这些转换。

"数据库更新状态"选项卡显示当前 数据节点的更新状态。在更新管理器中启动软件更新（升级或修补）后，使用此"数据库更新"选项卡监控各数据节点的状态，以确认其完成更新。要查看更新工作流程的可视化表示，请点击 **查看图表**。

更新完成后，请转到 **Data Store 数据库** 选项卡，以确认数据库状态为"运行"。有关详细信息，请参阅 更新指南。



下图显示了 Data Store 更新工作流程。



创建 Data Store 备份

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。

在开始备份程序之前，请务必阅读并按照说明在 数据节点 上安装 *update-dnode-ROLLUP20231018-7.4.2- v2-01.swu* Data Store Update Patch。

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

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。

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 python 3.7`，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。

7. 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：

1. 以 `root`身份登录第一个 数据节点 的控制台。

> 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）。

2. 输入 `su-dbadmin`，然后按 Enter 以 `dbadmin` 用户身份运行以下命令。
3. 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。
4. 输入 `cd /home/dbadmin` 并按 Enter 键更改目录。
5. 输入 `mkdir backups` 并按 Enter 键创建 `backups` 目录。
6. 输入 `exit` 并按 Enter 返回到 数据节点 的命令行提示符。
7. 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。

> 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。

8. 将以下行复制到文本编辑器中：

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

9. 将 `[dbadmin-password]` 更新为 Data Store `dbadmin` 密码。
10. 复制更新后的行并将其粘贴到 `pw.ini` 备份密码文件中。
11. 按 Esc，然后输入 `:wq`，之后按 Enter 退出并保存更改。
12. 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。
13. 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
```

14. 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。
15. 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。
16. 将 *`backup-host-ip`* 替换为备份主机的 IP 地址。
17. 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 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
    ```

18. 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。
19. 按 Esc，然后输入 `:wq`，之后按 Enter 退出并保存更改。
20. 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。

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 **vsql**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
   ```

恢复 Data Store 备份

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。

要备份您的 Data Store，请完成以下过程：

1. 查看备份名称和软件版本
2. 停止 Data Store 数据库
3. 从备份
4. 启动 Data Store
5. 删除目录快照
6. 查看恢复的数据库

您只能将 Data Store 备份恢复到您从 Data Store 中获取备份的位置。您不能从一个 Data Store 备份恢复到另一个 Data Store。创建 Data Store 备份时，请使用任何 数据节点 发出备份命令。恢复 Data Store 备份时，请使用任何 数据节点 发出恢复命令(不需要与用于创建备份的 数据节点 相同)。

1. 查看备份名称和软件版本

1. 确认 Data Store 数据库备份和 Data Store 具有相同的 数据节点 名称和相同数量的数据节点。
2. 确认 Data Store 数据库备份和 Data Store 安装了相同版本的 Cisco Secure Network Analytics 。

不支持将数据库恢复到与备份不同的版本。

2. 停止 Data Store 数据库

1. 登录管理器。
2. 选择 **配置 > 全局 集中管理**。
3. 点击**Data Store**选项卡。
4. 找到数据库。
5. 点击“操作”列中的 ··· (**省略号**)图标。
6. 选择 **停止**。
7. 保持 Data Store 数据库控制选项卡打开。您将在后续程序中使用它。

3. 从备份

恢复 Data Store

> 确保在恢复数据库之前和之后都要运行以下命令，以进行比较：
> `/opt/vertica/bin/vsql -U dbadmin -w <'password'> -c "select* from partitions;" >/lancope/var/tcpdump/partitions-full-DBbackup`

1. 如果使用 `setup-sw-datastore-secure-connectivity` 脚本更新了 `dbadmin` 密码，则还必须更新存储在 `pw.ini` 备份密码文件中的密码，否则恢复会失败。
2. 标识在其中存储 `config.ini` 备份配置文件的 数据节点，然后以 `root` 身份登录其控制台。请参阅 **4. 初始化备份主机上的备份目录：**上的备份目录：
3. 输入 `su-dbadmin`，然后按 Enter 以 `dbadmin` 用户身份运行以下命令。
4. 在命令提示符后，输入 `vbr --task restore --config-file config.ini`，然后按 Enter 键从备份主机恢复 Data Store。

> 您只需在其中一个 数据节点 上发出恢复命令，即可恢复整个多节点数据库。

4. 启动 Data Store

1. 返回“集中管理”中的 Data Store 数据库控制选项卡。
2. 找到数据库。
3. 点击“操作”列中的 ··· (**省略号**) 图标。
4. 选择 **启动**。

5. 删除目录快照

重新启动 Data Store 后，删除名为 `catalog` 的快照。在恢复解析后将不再需要此快照，并可防止 Vertica 运行保留管理。

1. 以 `root` 身份登录到 数据节点 控制台。
2. 输入 `su-dbadmin`，然后按 Enter 以 `dbadmin` 用户身份运行以下命令。
3. 键入以下命令，将 `[password]` 替换为您的 `dbadmin` 密码，然后按 Enter 键。这将删除 目录 快照。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select remove_database_snapshot('catalog');"
   ```

6. 查看恢复的数据库

> 确保在恢复数据库之前和之后都要运行以下命令，以进行比较：
> `/opt/vertica/bin/vsql -U dbadmin -w <password> -c "select* from partitions;" >/lancope/var/tcpdump/partitions-full-DBbackup`

Data Store 维护

本节包括以下 Data Store 主题：

- 在 Data Store 中启用数据压缩
- 添加 Data Store 域
- 在 Data Store 初始化后添加辅助 管理器 或 流收集器
- 将 数据节点添加到 Data Store
- 更换 数据节点 (仅限硬件)

> 请确保在开始之前查看该程序。其中一些程序包括联系思科支持部门寻求帮助。

在 Data Store 中启用数据压缩

默认情况下，在配置了 Data Store的 流收集器的新安装中启用数据压缩。您可以使用它减少流量收集器和 Data Store 之间的带宽使用量。它在从流量收集器到 Data Store 的网络带宽有限的情况下尤其有用。

启用压缩可将此带宽最多减少 90%。数据压缩处于禁用状态，并且可以针对每个流量收集器启用。在“流量收集器”界面中进行以下配置更改，以启用对发送到 Data Store的数据的压缩。

1. 登录 流收集器 设备管理界面。
2. 点击**支持 > 高级设置**。
3. 在 ingest_enable_compression 字段中，输入以下任一值
   - 1 - 启用数据压缩
   - 0 - 禁用数据压缩
4. 点击 **应用** ，然后在信息窗口中点击 **确定** 。

虽然此页面上的许多设置当设置不正确时可能会对性能产生负面影响，但对于流量收集器 与 Data Store 之间的数据传输，启用数据压缩只会提高系统性能。

添加 Data Store 域

您可以向现有 Data Store 域中添加 管理器、流收集器和 数据节点，如本节所示。如果您的部署中没有 Data Store 域，请按照 将 Data Store 添加到非 Data Store 部署中的说明进行操作。

在 Data Store 初始化后添加辅助 管理器 或 流收集器

如果您已初始化 Data Store，请按照以下说明添加辅助管理器或 流收集器 。

有关辅助 Manager 和故障转移配置的详细信息，请参阅 3. 定义 管理器 故障转移关系。

如果您配置了不使用 Data Store的现有 流收集器，则可以按照 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器**的说明将其转换到 Data Store 流收集器，而不会丢失转换前的数据或可见性。

将 数据节点添加到 Data Store

> 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。

要求

在您将 数据节点添加到 Data Store之前，查看以下要求：

- Data Store 支持 1 个或 3 个或更多数据节点。您可以添加 3 个数据节点。
- 如果您有单数据节点 (1) 部署，则可以添加 2 个数据节点，将部署扩展到 3 个数据节点（以及 3 个额外节点）。
- 不支持只有 2 数据节点的 Data Store。

准备工作

在扩展 Data Store时，您可能需要考虑使用维护窗口。

在扩展 Data Store之前，所有数据均匀分布在您的 数据节点上。例如，在三个节点 Data Store中，每个 数据节点上都有三分之一的数据。扩展 Data Store后，所有数据都将在新添加的节点之间平均重新分发。例如，如果将 3 个节点的 Data Store 扩展到总共 6 个节点，则重新分发会在每个 数据节点上生成六分之一的数据。将单个节点 Data Store 扩展到三个节点时，数据会重新分发到每个节点的三分之一。

在重新分发数据的操作期间，您的 Data Store 的查询性能可能会暂时降低。影响的大小和持续时间与需要移动的数据量和 数据节点间的专用 LAN 带宽有关。例如，具有端口绑定的硬件 Data Store 可以使用 20GB 的专用 LAN 带宽来移动数据。数据库将在重新分发数据期间保持运行，但如果您想最大限度地减少对用户的影响，我们建议使用维护窗口。

操作过程

要将 数据节点添加到部署中，请完成以下程序：

1. 创建 Data Store 备份

在添加 数据节点之前，请备份 Data Store。有关详细信息，请参阅 **创建 Data Store 备份**。

2. 配置数据节点并将其添加到“集中管理”

1. 将 数据节点部署到网络。有关指导，请参阅 x2xx 系列硬件设备安装指南、Cisco Secure Network Analytics x3xx 系列硬件安装指南或 虚拟版设备安装指南。

> 确保在安装过程中为 数据节点 虚拟版 分配两个网络适配器。When you start First Time Setup, it will fail to resolve if it cannot detect a second network adapter,

> which will prevent you from assigning a non-routable IP address for inter-数据节点 communications.

2. 在 首次设置中配置数据节点。您将在此程序中分配可路由 (eth0) 管理 IP 地址并配置数据节点 内部通信。
3. 使用 设备设置工具将数据节点添加到“集中管理”。

3. 将 数据节点添加到 Data Store

1. 以 root 身份登录 管理器 设备控制台。
2. 键入 `SystemConfig` 并按 Enter 键。
3. 选择**Data Store**。
4. 选择 **SSH**。等待您的设备启用 SSH。
5. 从 **Data Store** 菜单中选择 **新的 数据节点**。按照屏幕上的提示进行操作。

    - 完成此过程后，请检查“集中管理”以确保设备状态为“已连接”。
    - 退出 Data Store 菜单时，系统会恢复之前的 SSH 设置。

4. 重新平衡数据 Data Store

> 将其他数据节点添加到 Data Store 后，需要重新平衡。如需有关此程序的帮助，请联系思科支持 。

更换 数据节点 (仅限硬件)

按照以下说明为以下场景准备新的(备件) 数据节点：

- 将 数据节点 替换为具有不同 IP 地址的备件 数据节点
- 更换无响应的 数据节点
- 在现有 数据节点 发生故障后添加备件 数据节点

在所有情况下，您都需要准备新的(备件) 数据节点 并与 思科支持团队 合作完成更换。

> 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。

1. 准备新的(备件) 数据节点

1. 在与现有 数据节点 设备相同的机架设置中安装新(备件) 数据节点 设备。有关安装说明，请参阅 x2xx 系列硬件设备安装指南 或 Cisco Secure Network Analytics x3xx 系列硬件安装指南。

    选中以下复选框：

- 确保新的数据节点连接到相同的交换机/端口。
- 确保新数据节点与现有 数据节点上的专用和公共接口位于同一 VLAN 中。

2. 将数据节点连接到电源并打开电源。
3. 升级新 数据节点 上的映像，以匹配现有 数据节点上已运行的映像。请联系思科支持部门寻求帮助。
4. 在 首次设置中配置 数据节点 。为其分配适当的 eth0 管理 IP 和专用 IP 地址，并确认它与现有 数据节点 eth0 和专用 IP 位于同一 VLAN 中。
5. 通过执行以下步骤验证完全连接：

    - 从 管理器 和所有 流收集器对新的 数据节点的 eth0 IP 地址执行 ping 操作。
    - 从所有现有的 数据节点对新 数据节点的专用 IP 执行 ping 操作。
    - 从新的 数据节点 到 管理器 和所有 流收集器的 eth0 管理 IP 执行 ping 操作。
    - 从新的 数据节点 到所有现有 数据节点的专用 IP 执行 ping 操作。

2. 创建 Data Store 备份

有关详细信息，请参阅 **创建 Data Store 备份** 。

3. 联系思科支持

请联系思科支持部门完成更换。

将 Data Store 添加到非 Data Store 部署和过渡
流量收集器

通过以下指示，将非Data Store 流收集器转换为 Data Store 流收集器。通过此过程，您可以将现有 流收集器转换为使用 Data Store 数据库，而不会丢失转换前的数据或可视性。完成以下步骤后，您可以保留先前存在的数据，直到不再需要这些数据。将非Data Store 流收集器转换为 Data Store 流收集器，也可以利用只有 Data Store 可提供的功能，例如：

- **提高注入容量：** Data Store 部署可扩展到每秒收集高达 300 万个流，并可在一定程度上缓解您当前的注入容量限制。在 Data Store 模式下，流收集器的性能最多可提高 200%。
- **多遥测支持：** Data Store 部署能够处理 NetFlow、远程员工/终端 (NVM) 以及防火墙连接和安全事件遥测。
- **长期数据保留：** Data Store 部署提供可扩展存储，无需添加 流收集器即可实现长期数据保留（最长可达 2 年）。
- **企业级数据恢复能力：** 以冗余方式跨多个 数据节点存储遥测数据。这可确保在单个节点发生故障期间不会中断服务。
- **显著提高查询和报告响应速度：** 与非Data Store 部署模式相比，Data Store 可显著提高查询性能和报告响应速度，在某些情况下可提高 10 倍或 10 倍以上。
- **分析：** 分析可提供更多检测和建模功能以及新界面功能，利用这些功能，您可以查看任何安全问题、确定其优先级并加以解决。分析提供：
  - 自动角色检测
  - 其他报警功能
  - 实验性警报控制面板
  - 支持设备报告
- **SAL 遥测：** 安全分析和日志记录 (SAL) 通过汇聚来自防火墙（FTD 和 ASA）的日志并提供网络活动的直观视图来简化决策制定。您可以自行决定扩展 SAL，以便进行更长时间的保留和分析，甚至可以对防火墙中发现的潜在威胁发出警报。

准备

在开始转换之前，请查看说明，以便了解转换 流收集器所需的准备工作和步骤。

请注意以下提示：

- **一次一个：** 一次只能启动一个 流收集器 转换。但是，可以有许多 流收集器同时处于转换状态。
- **查询选项：** 一旦 流收集器 进入转换状态后，您可以查询在启动转换之前通过非

Data Store Data Store域收集的历史非数据，以及通过非 Data Store 域在转换后在 Data Store 中收集的新数据 Data Store 域。

备份配置文件

> ⚠ 请确保在更改 流收集器 状态(非 Data Store、转换或 Data Store)后备份“集中管理”配置文件。只有当 流收集器处于与进行备份时相同的状态时，才能恢复到系统。

流收集器 转换要求

在转换流量收集器之前，请确认您已部署至少一个 数据节点，并且 Data Store 已完成初始化过程，如 **6. 正在初始化 Data Store**。如果您尚未部署至少一个 数据节点，请参阅 x2xx 系列硬件设备安装指南、x3xx 系列硬件安装指南或 虚拟版设备安装指南 。部署数据节点后，您可以按照 **启动流量收集器转换到 Data Store** 程序进行操作。

启动流量收集器转换到 Data Store

请按照以下步骤将非-Data Store 流收集器 转换到 Data Store 流收集器。

> ⚠ 开始此过程后，您将无法将流量收集器恢复到以前的状态。您需要按照以下步骤完成过渡。

1. 查看您的 Data Store 域

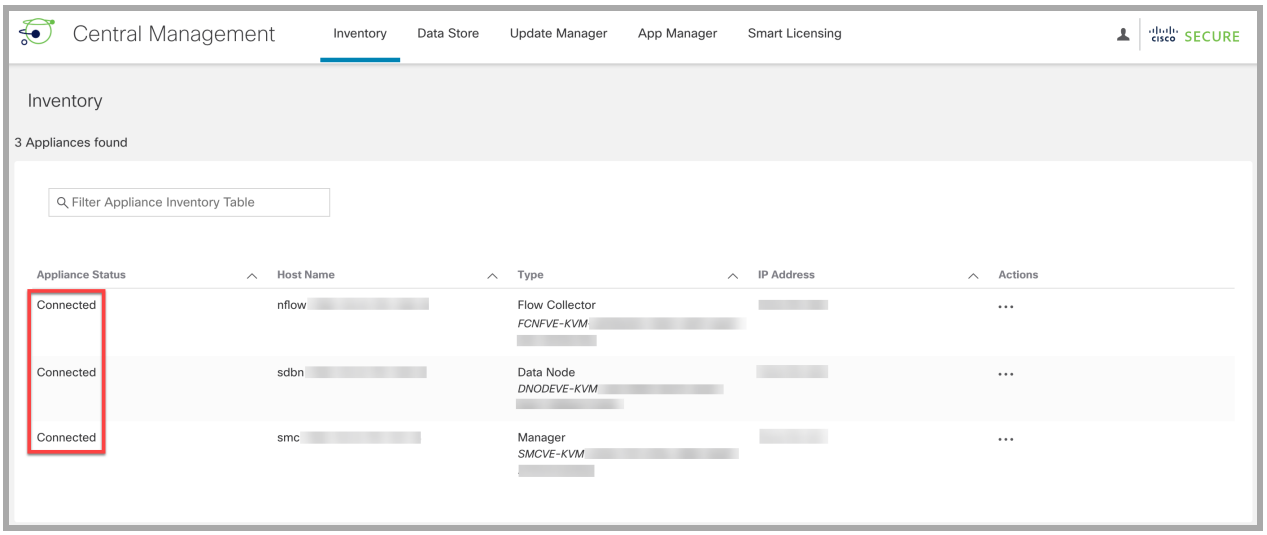
确定与您将要转换的 流收集器 对应的 Data Store 域。您的 流收集器 将转换到此域。

- **添加 Data Store 域：**如果需要添加 Data Store 域，可以按照本指南 **添加和配置域** 部分中的说明创建一个域。
- **导入现有域：**如果要从现有非Data Store 域导入设置，请确保按照 **通过导入现有非Data Store 域配置来创建 Data Store 域(可选)** 中的说明进行操作。
- **同步域：**在转换 流收集器 期间，您可以在转换前的非Data Store 域和 Data Store 域之间保持配置和调整同步。有关详细信息，请参阅 **同步 Data Store 和非Data Store 域** 。

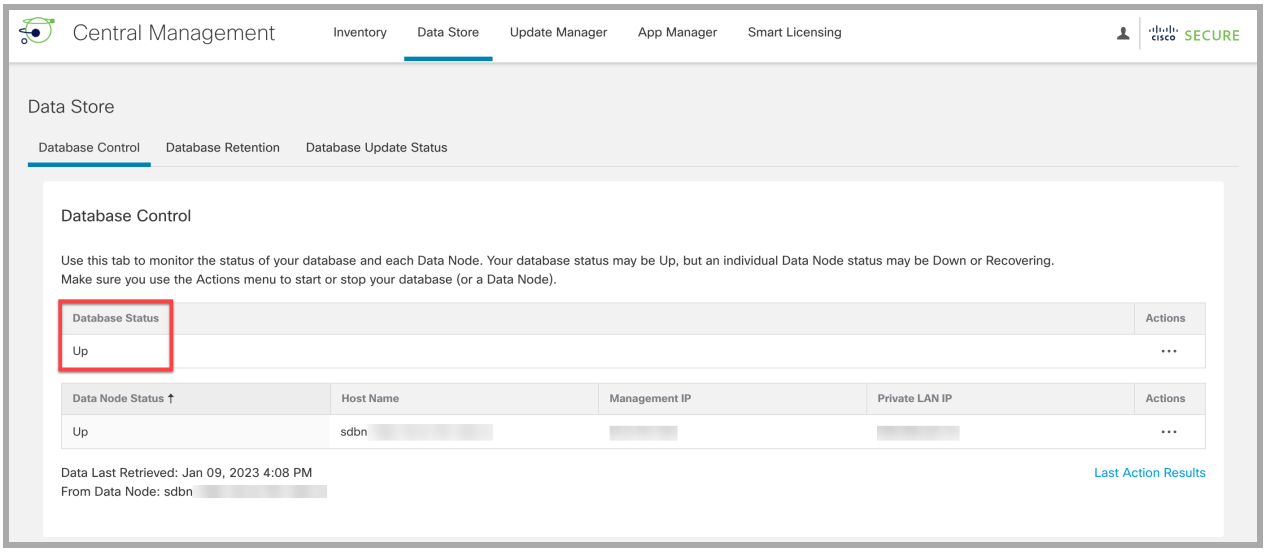
2. 检查设备状态

查看“集中管理”清单

1. 选择 **配置 > 全局 集中管理**。
2. 确认所有设备都显示为 **已连接**。如果设备不处于这些状态，请尝试使其进入这些状态，然后再继续下一步。如果您的设备无法进入这些状态，请联系思科支持。



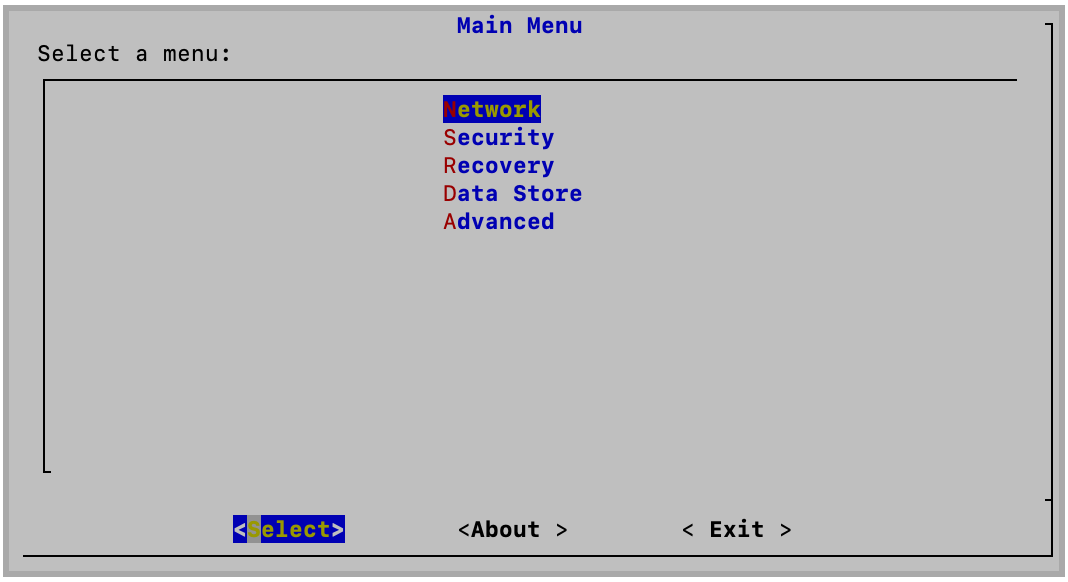
3. 选择 **Data Store 数据库控制** 选项卡。确认您的数据库状态显示为 **运行**。



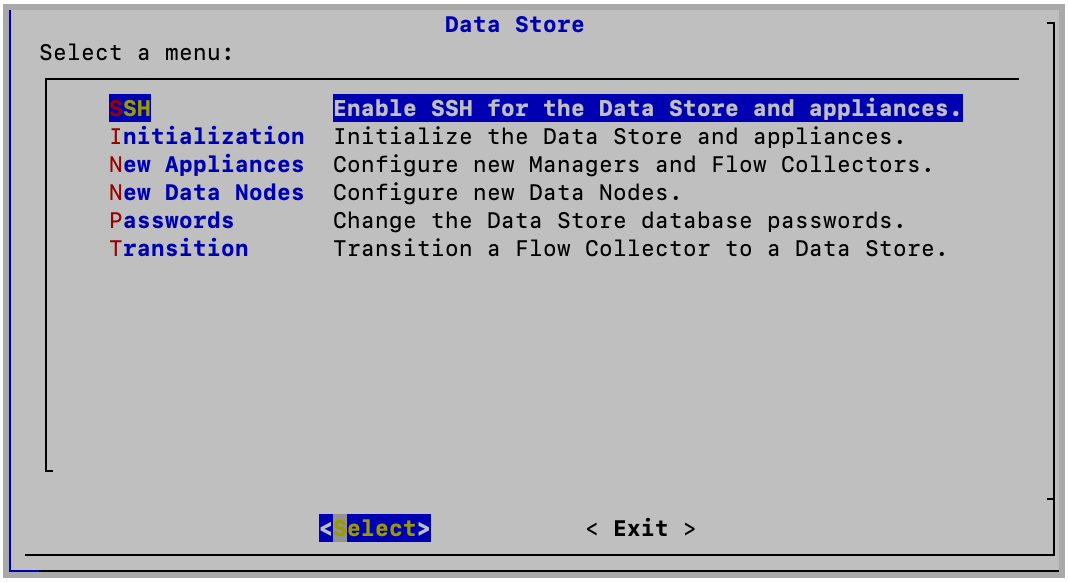
3. 转换流量收集器

> 流收集器 将在转换操作期间重新启动。重新启动完成后，流收集器 将开始将新 Data Store 在 Data Store 数据库中，而不是在 流收集器上的本地 Vertica 数据库中。

1. 以 root 用户身份登录管理器设备控制台 (SystemConfig)。



2. 选择 **Data Store > SSH**。此操作将启用 SSH。



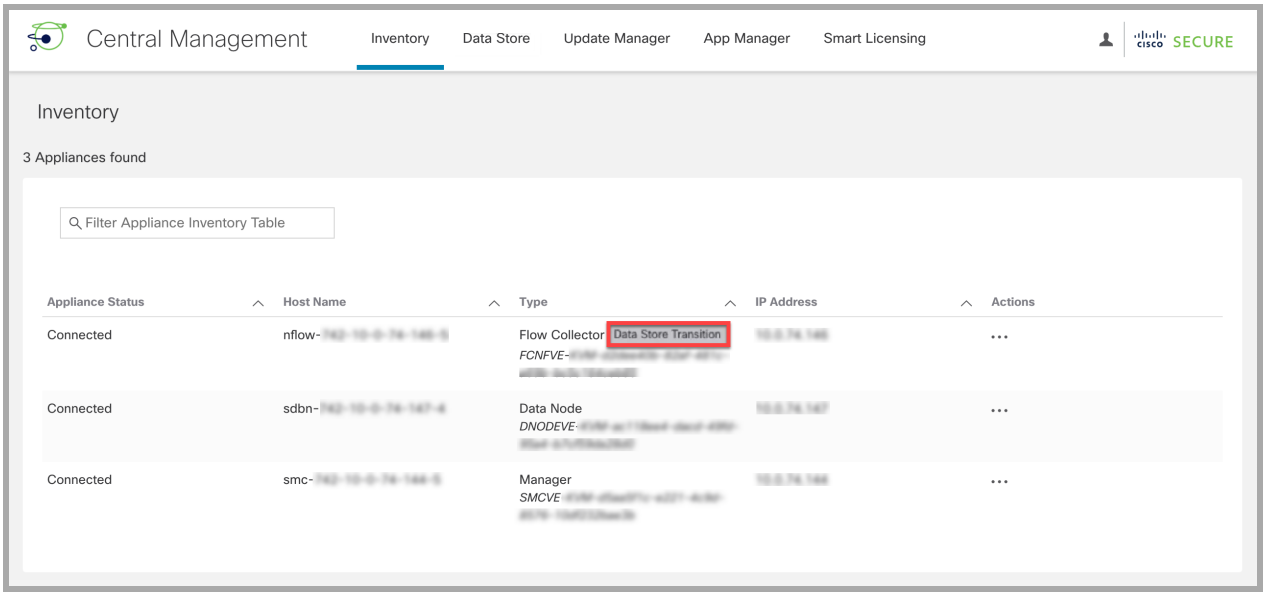
> 如果您没有看到 Data Store 菜单，请确保您有一个 Data Store 域。有关详细信息，请参阅 **1. 查看您的 Data Store 域**。

3. 从 Data Store 菜单中，选择 **转换 > 启动转换**。
4. 选择要转换的流量收集器。
5. 在 Data Store 域屏幕上，选择您在 1 中识别(或创建)的 Data Store 域。查看您的 Data Store 域。转换后的 Data Store 流收集器 数据将被路由到 Data Store 数据库，并可通过此新域而不是先前的非Data Store 域进行访问。
6. 按照屏幕上的提示确认转换。

> ⚠ 完成启动转换程序后，在确认不再需要 流收集器本地存储的历史数据之前，请勿完成 流收集器 转换，因为这些数据将在此过程中被删除。有关详细信息，请参阅 **完成 Data Store 流量收集器转换**。

7. 查看“集中管理”资产（**配置 > 全局集中管理**）。

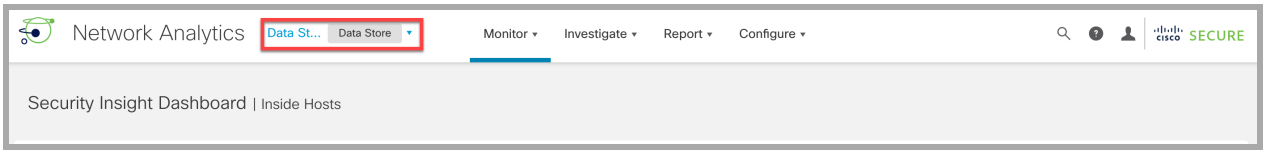
   确认您转换的流量收集器显示 **Data Store 转换** 标记。



4. 验证通信

确认您的 Data Store 正在接收流。

1. 返回安全洞察控制面板。
2. 确保从屏幕顶部的“域”菜单中选择 Data Store 域。



3. 选择 **报告** 菜单。
4. 选择 **报告构建器**。
5. 点击 **创建新报告**。
6. 点击 **流数据库注入趋势报告** 模板。
7. 根据需要选择参数。点击**运行**。
8. 查看报告以确认数据库或 Data Store 正在接收流。

除了运行流数据库注入趋势报告外，您还可以通过执行以下操作来确认您的 Data Store 正在接收流：

- **流收集器 趋势表：**导航至安全见解控制面板以查看 流收集器 趋势表。如果您的 Data Store 正在接收流，您将在此处看到它们。
- **数据库保留：**打开“集中管理”(配置 > 全局集中管理)，然后查看 Data Store > 数据库保留选项卡上的信息。此页面上的 Data Store 表中的最早数据将帮您跟踪自最早记录写入 Data Store以来的日期和天数。请注意，此表中的数据每天仅更新一次，因此您在过渡当天不会在此表中看到任何数据。有关更多信息，请参阅本指南的 **查看数据库保留** 部分。

运行流搜索

选择调查 > 流搜索，按域运行流查询。使用自定义日期范围自定义结果。

- **转换前查询：**要查询非域Data Store 中的转换前历史数据，请务必选择早于 流收集器 转换日期的结束日期。
- **转换后查询：**要查询所有过渡后 Data Store 数据，请务必选择开始日期，该日期开始于 流收集器转换日期或之后。

从集中管理器清单中删除正在转换的流量收集器

> ⚠ 请勿从集中管理器清单中删除正在转换的 流收集器 。如果这样做，您需要在思科支持部门的协助下完成转换流程。

转换流量收集器行为

转换 流收集器将表现出以下行为。

- **新数据：**完成 **启动流量收集器转换到 Data Store** 过程后，正在转换的 流收集器 会将所有新遥测数据发送到 数据节点上的 Data Store 数据库。您的新数据将可在您在 **1. 查看您的 Data Store 域**，您的本地转换前数据将继续存在于非Data Store 域中。
- **转换前数据：**流收集器只要您希望保持对这些数据的访问，就会继续在本地存储转换前数据。有关如何删除不再需要的转换前数据的说明，请参阅 **完成 Data Store 流量收集器转换** 。
- **系统性能：**在 流收集器 转换期间的系统性能将类似于转换前的性能。转换完成后，您将看到与 Data Store 流收集器一致的性能改进。

同步 Data Store 和非Data Store 域

在转换 流收集器 期间，您可以在转换前的非Data Store 域和 Data Store 域之间保持配置和调整同步。本部分介绍将非Data Store 域与其关联的 Data Store 域同步的过程。

> ℹ 您需要管理员访问权限才能执行此程序。

同步的属性

以下属性将在域之间同步：

- 数据存储域特定配置以及警报配置(如果已启用)。域配置包括:
  - 主机组管理
  - 警报严重性
  - 策略管理
  - 服务和应用
  - 导出器 SNMP 配置文件(不包括密码)
  - 域 AS 编号。

推荐的同步频率

虽然您可以根据需要随时同步域,但我们建议您将同步限制为仅在执行一组更改后进行,或者每天或每周同步一次。这是因为同步过程需要使用从日常处理中删除的资源。

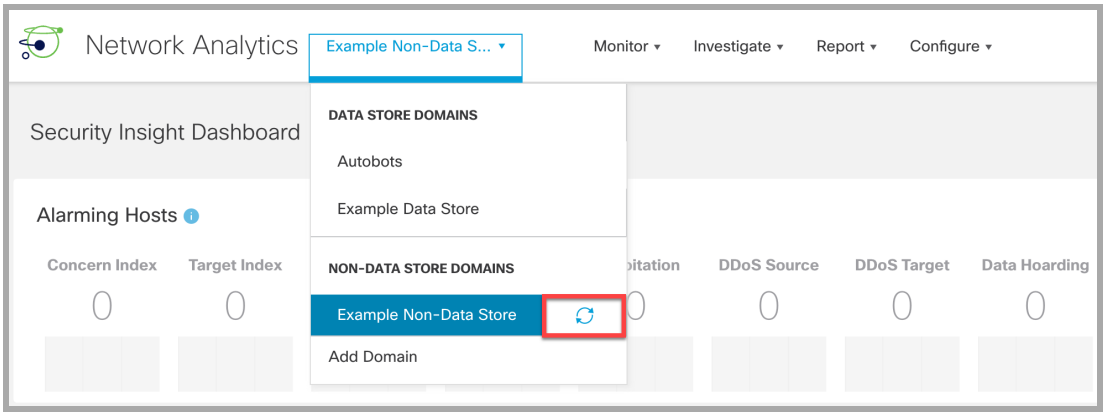
同步域过程

请按照以下步骤将非 Data Store 域(源)与 Data Store 域(目标)同步。

1. 从菜单栏中,选择要与 Data Store 域同步的非 Data Store 域。
2. 从主菜单中,选择**配置 > 系统 > 域属性**。
3. 选择**编辑**按钮。
4. 在**要同步的目标域**下拉菜单中,选择此域要与其同步的 Data Store 域。

> 您只能将目标 Data Store 域与一个源非 Data Store 域同步。如果您尝试将目标 Data Store 域与多个源非 Data Store 域同步,您将收到错误消息。

5. 点击**保存**按钮保存您所做的更改。您选择与您的 Data Store 域同步的非Data Store 域旁边会显示 同步按钮。



正在完成 流收集器 转换

不再需要转换前的数据后，您可以按照 **完成 Data Store 流量收集器转换**中的步骤完成流收集器 转换。

> ⚠ 在确认不再需要 流收集器本地存储的历史数据之前，请勿完成 流收集器 转换，因为这些数据将在此过程中被删除。

完成 Data Store 流量收集器转换

如果您已遵循将非Data Store 流收集器 数据转换为 Data Store 流收集器 的 流程，并且不再需要保留本地存储的非Data Store 数据，则可以完成 Data Store 流收集器 转换。

将您的非Data Store 流收集器转换为 Data Store 流收集器涉及两个主要程序。

1. 按照 **启动流量收集器转换到 Data Store** 过程中的步骤启动转换过程。这会将您的流收集器转换为 Data Store 转换状态，如 **转换流量收集器行为**中所述。
2. 完成转换过程。这会导致您的 流收集器 变为 Data Store 流收集器。系统将删除此流量收集器正在存储的所有现有非Data Store 数据，并恢复资源，从而提高 流收集器的性能。

要求

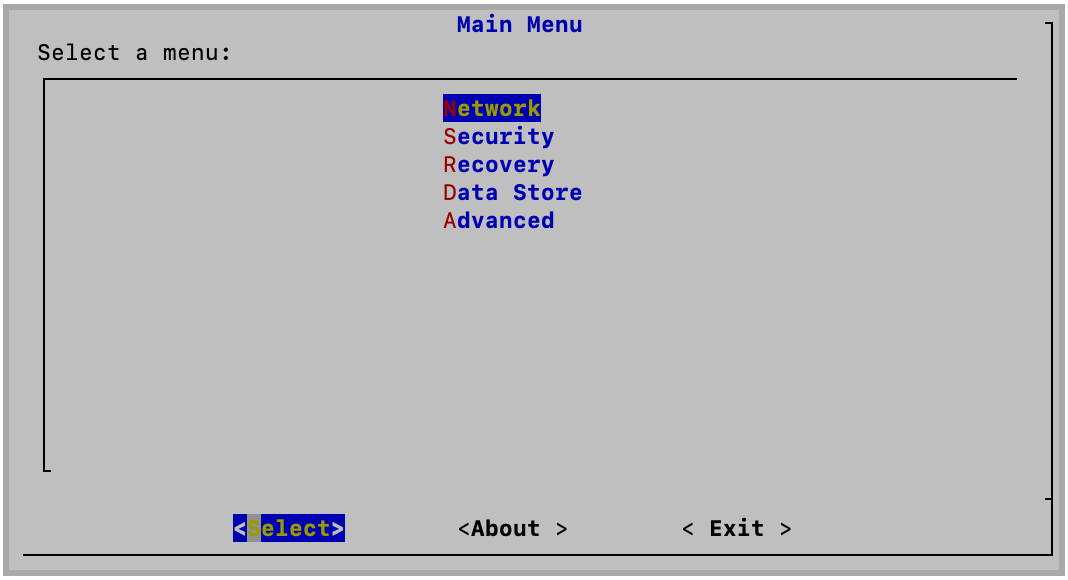
在完成 Data Store 流量收集器转换之前，请查看以下内容：

- **启动转换：**确认您已完成 **启动流量收集器转换到 Data Store** 的过程。
- **历史数据：**确认您不再需要在 流收集器上本地存储历史数据，因为这些数据将在此过程中被删除。如果您有非Data Store 数据的数据保留策略，并希望在完成 Data Store 转换之前了解 Data Store 有多少新数据，请查看 Data Store 中的最旧数据表。有关更多信息，请参阅 **查看数据库保留**。

完成流量收集器转换到 Data Store

按照以下步骤操作，以完成 Data Store 流收集器 转换。

1. 以 root 用户身份登录管理器设备控制台 (SystemConfig)。



2. 选择 **Data Store > 转换 > 完成转换**。
3. 选择 流收集器 以完成转换到 Data Store
4. 按照屏幕上的提示完成转换。
5. 查看“集中管理”资产(**配置 > 全局集中管理**)。

   确认您转换的流量收集器显示 **Data Store** 标记。

完成后注释

在完成 **完成流量收集器转换到 Data Store**程序后:

- 在非Data Store 域中，您将不会再在 流收集器 流查询中看到任何 NetFlow 记录。
- 如果旧的非 流收集器域中没有Data Store，则可以删除该域。有关详细信息，请参阅 **删除域** 。
- 系统已删除此流量收集器正在存储的所有现有非Data Store 数据，并已恢复资源，从而提高 流收集器的性能。
- 您将看到 流收集器 转换后的磁盘空间使用量显着减少。要查看系统统计信息、服务、磁盘使用情况和 Docker 服务，请登录“设备管理”(Appliance Admin) 界面:

  1. 在 集中管理 资产清单页面中，点击设备的 ••• (**省略号**)图标 。
  2. 选择**查看设备统计信息**。
  3. 选择**主页**以查看统计信息。

将 Data Store 添加到非 Data Store 部署

在使用这些说明之前，请确保您已在具有非Data Store 域的 Cisco Secure Network Analytics 系统中工作。有关说明，请参阅 **规划您的系统配置**。

使用相应的说明将 Data Store 添加到非Data Store 部署中。

- **使用现有的 流收集器**
- **添加 Data Store 和新 流收集器**

> 有关 Data Store 兼容性信息，请参阅安全网络分析硬件和软件版本支持表。

使用现有的 流收集器

添加 Data Store

要将现有的 流收集器添加到 Data Store，请参阅 **将 Data Store 添加到非 Data Store 部署和过渡 流量收集器**。通过此过程，您可以将现有 流收集器 转换为使用 Data Store 数据库，而不会丢失转换前的数据或可视性。

添加 Data Store 和新 流收集器

请按照以下步骤将新的 流收集器 添加到您的 Data Store。

1. 确保您的 流收集器 和设备都在同一软件版本上运行。按照 安全网络分析更新指南中的说明进行操作。
2. 确认您已在 Cisco Secure Network Analytics 中创建要与 流收集器 关联的 Data Store 域。有关详细信息，请参阅本指南中的创建 Data Store 域部分。
3. 部署并安装硬件或虚拟 流收集器。有关详细信息，请参阅 x2xx 系列硬件设备安装指南、Cisco Secure Network Analyticsx3xx 系列硬件安装指南或虚拟版设备安装指南。
4. 在 流收集器上运行 首次设置，确保将 流收集器 部署为 Data Store的一部分。
5. 将 流收集器 添加到集中管理器。如果您有 52xx 流收集器，请务必添加 流收集器 数据库和 流收集器 引擎（按此顺序）。选择您希望 流收集器 加入的 Data Store 域。
6. 对要添加到 Data Store的所有 流收集器重复上述步骤。
7. 登录 管理器 设备控制台 (SystemConfig) 并选择 **Data Store > 新建设备 (New Appliances)**，将您的 流收集器（多个）添加到 Data Store 。

故障排除

Analytics 作业滞后

在以下两种情况下，都会触发“Analytics 性能已下降”系统警报。

辅助管理器已升级为主管理器

如果您将主管理器的角色更改为辅助管理器角色，并且超过 5 个小时以后才恢复原始主管理器并重新为其分配主管理器角色，则会触发“Analytics 性能已下降”系统警报。Analytics 将恢复并运行过去 6 小时内（原始主管理器关闭期间）发生的作业。作业性能将继续滞后，直到系统处理完过去 6 小时内的所有作业并开始实时处理作业。

设备因性能下降而关闭

如果系统性能下降（通常是由于 CPU 或内存等资源不足），作业将开始滞后。如果此滞后超过 5 个小时，则会触发“Analytics 性能已下降”系统警报。此时，结果将不完整和不可靠。

此故障的原因可能是您增加了每秒流数，使其超出了设置支持的范围。要解决此问题，要么减少每秒流数，要么增加管理器或 Data Store 上的资源，或者两者都增加。如果您无法解决此问题，请联系思科支持部门。

设备状态：配置通道关闭

如果库存清单页面显示的设备状态为 **配置通道关闭**，请检查以下内容：

- **通信设置：**确认您的网络通信设置。
- **信任存储区：**确保将设备身份证书保存到正确的信任存储区。有关操作说明，请参阅受管设备的 SSL/TLS 证书指南
- **证书：**如果您已更改设备身份证书，请检查程序并确认证书已被保存到正确的信任存储区。有关操作说明，请参阅受管设备的 SSL/TLS 证书指南
- **删除设备：**如果在配置通道关闭时从“集中管理”(Central Management) 中删除设备，请确保同时从“系统配置”(System Configuration) 中删除设备：
  - 以系统管理员身份登录设备控制台。
  - 键入 **SystemConfig**。按下 Enter 键。
  - 选择**恢复 (Recovery) > 删除设备 (RemoveAppliance)**。

设备状态：Data Store 未初始化

您需要完成 Cisco Secure Network Analytics 系统配置。

将所有管理器、流量收集器和数据节点添加到集中管理资产后，您需要初始化 Data Store。有关说明，请参阅 **6. 正在初始化 Data Store**。

设备状态：Data Store 未配置

如果您已将新的 管理器、流收集器或 数据节点 添加至 Data Store，您需要完成系统配置。有关说明，请参阅 **Data Store 维护**。

打开设备管理界面

您还可以通过“集中管理”(Central Management) 或直接登录设备来打开“设备管理”(Appliance Admin) 界面。

如果您已从中央管理器中删除 管理器 以进行故障排除，则可能需要登录到设备管理。

1. 在浏览器地址栏中，键入设备 IP 地址，如下所示：

   https://<IPAddress>

   - **管理器：**在 IP 地址后面添加 **/manager/index.html** 。
   - **示例：**https://xx.xxx.xx.xxx/Manager/index.html

更换设备身份

每个 Cisco Secure Network Analytics 7.x 版设备都安装有一个唯一的自签名设备身份证书。要用证书颁发机构的证书替换设备身份证书，请参见受管设备的 SSL/TLS 证书指南中的说明。

> ⚠ 证书对于保障系统安全至关重要。不当修改证书可能会停止 Cisco Secure Network Analytics 设备通信并导致数据丢失。

从中央管理器删除 Data Store 设备

如果从中央管理器(管理器、流收集器、数据节点)中删除 Data Store 设备，则不会将其从 Data Store 中删除。这需要手动清理。

- **管理器和 流收集器：**对于 管理器和 流收集器，可以从 **/lancope/var/services/data-store/config-datastore-inventory-snapshot** 目录中删除它们。
- **数据节点：**联系 思科支持部门 以获取有关删除 数据节点的帮助，因为该过程更加复杂。

更改主机名、网络域名或 IP 地址

在安装和配置设备后，要更改设备的主机名、网络域名或 IP 地址，请按照受管设备的 SSL/TLS 证书指南中的说明操作。

作为此操作过程的一部分，您将暂时从“集中管理”(Central Management) 中删除设备，并自动替换设备身份证书。

> 作为此操作过程的一部分，系统将自动替换设备身份证书。
>
> **如果设备使用自定义证书，**请联系 思科支持部门 来更改这些设置。请勿使用此处显示的说明。确保您拥有自定义证书和私钥的副本。

打开域属性

从主菜单中，选择**配置 > 系统 > 域属性**。

有关详细信息，请参阅 **域**。

删除 桌面客户端 域

> 在决定要删除哪些桌面客户端域时，请谨慎行事，因为您将无法访问为要删除的域收集的所有数据。
>
> **解决方法**：如果您不小心删除了桌面客户端中的所有域并将自己锁定在管理器 Web 应用之外，请在桌面客户端中创建一个新的非 Data Store 域。这样，您就可以重新获得对管理器 Web 应用的访问权限。有关创建域的信息，请参阅桌面客户端帮助中的添加域主题。

打开设备设置工具

在配置设备后，按照以下说明打开“设备配置工具”(Appliance Setup Tool)。

> 如果您使用“设备配置工具”(Appliance Setup Tool) 更改主机名、网络域名或 IP 地址，则将自动替换设备身份证书。
>
> **如果设备使用自定义证书，**请联系思科支持部门来更改这些设置。请勿使用此处显示的说明。确保您拥有自定义证书和私钥的副本。

1. 在设备浏览器地址栏中，在 IP 地址之后，用 /lc-ast 替换 URL 的末尾：

   https://<IPAddress>/lc-ast

2. 按下 Enter 键。
3. 有关详细信息，请参阅 **1. 使用首次设置配置环境**

系统配置概述

我们使用新的菜单结构更新了系统配置。系统配置通常涉及故障排除。要获取帮助，请联系思科支持。

- **用户:**可用菜单由您是以根、系统管理员还是管理员身份登录来确定。
- **SSH:**您可能需要启用 SSH 才能访问菜单。

1. 登录设备控制台。
2. 键入 **SystemConfig**。按下 Enter 键。
3. 从主菜单中，选择一个菜单：

- **网络:** 要更改设备管理端口网络、可信主机和网络接口 (eth0 configuration , MTU 等)，请选择“网络”。
- **安全:** 要更改或重置密码(请参阅 **密码**)并管理系统日志合规性，请选择“安全”。
- **恢复:** 要从集中管理中删除设备，重置出厂默认设置，创建诊断包或刷新映像，请选择“恢复”。
- **高级:** 要打开根 Shell、管理管理员用户帐户或配置单点登录，重启或关机，请选择“高级”。
- **Data Store:** 此菜单在配置为与 Data Store配合使用的 管理器中可用。使用此菜单启用 SSH、初始化、向 Data Store添加新的管理器和 流收集器、将 Data Node 添加到 Data Store、更改 Data Store 数据库密码和 将流量收集器转换为 Data Store。

更改可信主机

您可以使用“系统配置”(System Configuration) 从设备默认值更改可信主机列表。但是，在更改可信主机之前，请联系思科支持部门。

> ⚠ 在更改可信主机之前，请联系思科支持部门。

如果从默认值更改受信任主机列表，请确保部署中每台其他 Cisco Secure Network Analytics 设备的每台 Cisco Secure Network Analytics 设备都包含在受信任主机列表中。否则，设备将无法相互通信。

1. 以系统管理员身份登录设备控制台。
2. 选择**网络 (Network) > 可信主机 (Trusted Hosts)**。
3. 按照屏幕提示更改可信主机。

配置最大传输单位 (MTU)

按照以下说明配置设备 eth0 网络接口的最大传输单位 (MTU)。数值设置每个事务允许的 eth0 接口传输的最大数据包大小。

> ⚠ MTU 会影响您的网络处理。如果更改此编号，请确保其在网络中的配置一致。

1. 以系统管理员身份登录设备控制台。
2. 选择 **网络 > 接口**。
3. 选择 **eth0**。
4. 输入 **1500** (默认)、**9000**或符合网络配置要求的数字。

> 防火墙日志支持的最大 MTU 设置为 8,192 字节，NetFlow、sFlow 和 NVM 流支持的最大 MTU 设置为 9,216 字节。如果您使用 Security Analytics and Logging (本地) 和其他遥测类型获取防火墙日志，请不要将 MTU 设置配置为大于 8,192 字节。

5. 选择 **确认**。
6. 按照屏幕上的提示确认更改。

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。按照以下说明为单个设备创建诊断包。

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

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。

5. 点击**完成 (Finish)**。按照屏幕上的提示创建诊断包。

重置出厂默认设置

按照以下说明将设备重置为其出厂默认值 (RFD)。要完全清除数据，请确保重置两次出厂默认设置。

- **RFD 两次:**要完全清除数据,请确保重置两次出厂默认设置。
- **备份配置:**如果您计划恢复设备配置,请确保保存备份配置和数据库备份文件。有关详细信息,请参阅帮助中的 **备份配置文件** (在"集中管理"中)和 **备份/恢复数据库** (设备管理界面)主题。要在 RFD 后恢复备份,请联系思科支持。

> ⚠ 如果在设备上重置出厂默认设置 (RFD),则所有现有数据和配置信息都将被删除,并且只有在之前进行了备份才能恢复。

> ⚠ 如果将设备重置为其出厂默认设置,则无法使用"集中管理"恢复配置。要获取帮助,请联系思科支持。

1. 以系统管理员身份登录设备控制台。
2. 选择**恢复 > 出厂默认值**。
3. 按照屏幕提示重置出厂默认设置并重新启动设备。

> ⚠ 确保对每个设备进行两次 RFD 以彻底擦除数据。

4. 以**系统管理员**身份登录设备控制台,并按照屏幕提示配置设备 IP 地址、主机名和域。有关说明,请参阅本指南的 使用初始设置配置环境 部分。即使在 RFD 时保留网络设置,也需要执行此步骤。
5. 登录设备设置工具并将设备添加到"集中管理"。有关详细信息,请参阅 **集中管理 (管理设备)**。

启用/禁用管理员用户

使用下面的说明来启用或禁用默认的管理员帐户。

1. 以系统管理员身份登录设备控制台。
2. 选择**高级 (Advanced)**。
3. 选择**管理员用户 (Admin User)**。
4. 按照屏幕提示启用或禁用管理员用户帐户。
5. 重复这些说明,在您的 Cisco Secure Network Analytics 集群中的所有设备上启用或停用"管理员用户"帐户。

Data Store 部署故障排除

硬件部署故障排除

有关部署或配置设备的问题，请参阅 x2xx 系列硬件设备安装指南或 Cisco Secure Network Analytics x3xx 系列硬件安装指南。

虚拟设备部署故障排除

有关部署或配置虚拟版设备的问题，请参阅虚拟版设备安装指南，以了解详细信息。

首次设置和数据节点虚拟版

如果在安装过程中没有为 数据节点虚拟版 分配两个网络适配器，则首次安装将无法解析，因为它无法检测到第二个网络适配器。这将阻止您为数据节点 内部通信分配不可路由的 IP 地址。有关更多信息，请参阅虚拟版设备安装指南。

Data Store故障排除

请注意，Data Store 最多保留 40% 的可用存储空间来维护 Data Store。最多有 60% 的总空间可用于遥测存储。

Vertica 分析平台在 数据节点 断电并重新启动后不会自动重新启动

如果 数据节点 意外断电并且您重新启动了设备，那么由于数据可能已损坏，数据节点上的 Vertica 分析平台 (Vertica) 实例可能不会自动重启。如果仍有足够多正在运行的 数据节点 以允许 Data Store 继续运行，则 Data Store 会继续从流收集器接收数据。但是，您需要尽快重新启动 数据节点，以允许其重新加入 Data Store，从相邻 数据节点 的检索丢失的数据，并赶上其余的 数据节点。

要重新启动数据节点，请尝试以下每种方法：

- 在“集中管理”> “Data Store”选项卡上启动数据节点。有关详细信息，请参阅启动 **启动 数据节点**。
- 如果数据节点不从 Data Store 选项卡开始，请登录 数据节点 并强制手动重启 Vertica，这样会删除损坏的数据并让 Vertica 正确重启。

对于 数据节点 硬件设备，您可能需要在重新启动之前更新 数据节点的电源恢复策略。如果电源恢复策略设置为“关闭电源”，则必须在断电后手动重新启动 数据节点 。有关在 CIMC 中配置电源恢复策略的详细信息，请参阅 UCS C 系列 GUI 配置指南。

1. 以根身份登录 数据节点 设备控制台。
2. 将以下命令复制粘贴到文本编辑器中：

```
tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
catalog/ErrorReport.txt
```

3. 将 *[node_name]* 替换为 数据节点 的名称(例如, node0001)。
4. 复制更新后的命令并将其粘贴到命令行接口中,然后按 Enter 键以查看 ErrorReport.txt 错误文件中的最新条目。如果错误消息指出可能存在数据一致性或数据损坏问题,请继续执行下一步以强制 Vertica 重新启动。
5. 将以下命令复制粘贴到文本编辑器中:

   ```
   admintools -t restart_node --hosts=[data-node-ip-address] --
   database='sw-datastore' --password="[dbadmin-password]" --force
   ```

6. 将 *[data-node-ip-address]* 替换为受影响 数据节点 的 IP 地址。确保使用 **Data Store 选项卡**中显示的专用 IP 地址。请勿使用 eth0 管理 IP 地址。
7. 将 *[dbadmin-password]*Data Store 替换为您的 dbadmin 密码。
8. 复制更新后的命令并将其粘贴到 CLI 中,然后按 Enter 键在受影响的 数据节点 上强制重新启动 Vertica。Vertica 会删除任何损坏的数据,并从相邻的 数据节点 中恢复相关数据。
9. 如果系统提示您 Do you want to continue waiting? (yes/no) [yes](是否要继续等待? [是/否]) [是]),输入 yes,然后按 Enter 键继续等待。

   由于 Vertica 会从相邻 数据节点 还原受影响 数据节点 的信息,因此,如果在受影响的 数据节点 停机期间 数据节点 注入了大量的流量,则受影响的 数据节点 可能需要一段时间才能恢复。

10. 查看思科关于为您的 数据节点供电的建议。有关详细信息,请参阅 x2xx 系列硬件设备安装指南、Cisco Secure Network Analyticsx3xx 系列硬件安装指南或虚拟版设备安装指南。

Data Store 电源故障后不启动

在“集中管理”的“Data Store”选项卡上查看数据库状态。您可以从此处启动数据库或数据节点。有关详细信息,请参阅 **查看 Data Store 数据库状态** 。

安装补丁和更新软件

为软件版本安装最新补丁，确保让 Cisco Secure Network Analytics 始终处于最新状态。有关详细信息和说明，请访问思科软件中心。

软件更新也会发布到思科软件中心的思科智能账户。为实现成功更新，请确保按照 Cisco Secure Network Analytics 更新指南中的说明进行操作。

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
- 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 2 月 27 日	初始版本。
1_1	2023 年 4 月 5 日	次要更新
1_2	2023 年 4 月 6 日	次要更新
1_3	2023 年 8 月 10 日	次要更新
1_4	2023 年 2 月 27 日	更新 Data Store 备份初始化程序 修复断开的链接

版权信息