Cisco Secure Network Analytics

x2xx 系列硬件设备安装指南 7.4.2

目录

简介

概述

本指南介绍如何安装 Cisco Secure Network Analytics (以前称为 Stealthwatch) x2xx 系列硬件设备。本指南还介绍了 Secure Network Analytics 硬件的安装和安装。

> ⚠ 请在安装 Secure Network Analytics x2xx 设备之前阅读 合规性和安全信息 文档。

x2xx 系列的硬件包括：

设备	部件号
管理器 2210 (以前 Stealthwatch 管理控制台)	ST-SMC2210-K9
Data Store 6200(三个 数据节点)	ST-DS6200-K9(三个 ST-DNODE-G1)
流收集器 4210	ST-FC4210-K9
流收集器 5210 引擎	ST-FC5210-E
流收集器 5210 数据库	ST-FC5210-D
UDP 导向器 2210	ST-UDP2210-K9
流传感器 1210	ST-FS1210-K9
流传感器 3210	ST-FS3210-K9
流传感器 4240	ST-FS4240-K9

受众

本指南适用于负责安装 Secure Network Analytics 硬件的人员。我们假设您已对安装硬件网络设备有了一些大致的了解。

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。

安装设备和配置系统

请注意安装和配置 Secure Network Analytics的整体工作流程。

1. **安装设备：**使用此安装指南安装 Secure Network Analytics x2xx 系列硬件(物理)设备。要安装虚拟版设备，请按照 虚拟版设备安装指南中的说明进行操作。
2. **配置 Secure Network Analytics：**安装硬件和虚拟设备后，您便可配置 Secure Network Analytics 入托管系统。按照 Secure Network Analytics 系统配置指南 v7.4.2 中的说明进行操作。

相关信息

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

- **法规合规安全信息：**请在安装 Secure Network Analytics x2xx 系列设备之前阅读 法规合规安全信息 文档。
- **概述：**https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Data Store 设计指南：**https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **硬件和软件版本支持表：**https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **设备规格：**https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

术语

本指南使用术语 “**设备**” 来表示任何 Secure Network Analytics 产品。

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

常用缩写

本指南中运用了以下缩写：

缩写	说明
DMZ	非军事区(外围网络)
HTTPS	超文本传输协议(安全)
ISE	身份服务引擎
NIC	网络接口卡
NTP	网络时间协议
PCIe	外围组件快速互连
SNMP	简单网络管理协议
SPAN	交换端口分析器
TAP	测试接入端口
UPS	不间断电源
VLAN	虚拟局域网

关于 Secure Network Analytics 设备

Secure Network Analytics 由若干硬件设备构成，这些组件会收集、分析并提供您的网络信息以提高网络性能和安全性。本节介绍每个 Secure Network Analytics x2xx 系列设备。

管理器 2210

管理器管理、协调、配置和组织系统的所有不同组件。Secure Network Analytics软件允许您从任何可以访问网络浏览器的计算机访问控制台的 Web UI。您可以轻松访问关于整个企业关键网段的实时安全和网络信息。管理器具备基于 Java 的平台独立性，支持：

- 集中管理、配置和报告最多 25 个 Secure Network Analytics 流量收集器
- 用于将流量可视化的图形图表
- 用于故障排除的深入分析
- 合并且可定制的报告
- 趋势分析
- 性能监控
- 及时通知安全漏洞

如果要部署 Data Store，则可以将具有 10Gbps SFP+ DAC 接口的 管理器 2210 配置为 eth0，以提高吞吐量。如果不部署 Data Store，只能将 1 Gbps/10 Gbps 接口配置为 eth0。

Data Store 6200

Data Store 提供了一个中央存储库，用于存储由流收集器收集的网络遥测数据。Data Store 由 数据节点集群组成(每个都包含您的数据的一部分)和单独 数据节点 数据的备份组成。由于您的所有数据都在一个集中式数据库中，而不是分布在多个流收集器中，因此与单独查询所有流收集器相比，您的管理器可以更快地从 Data Store 中检索查询结果。Data Store 集群可改善容错能力，提高查询响应速度并加快图形和图表填充。

有关详细信息，请参阅 Secure Network Analytics

流量收集器 4210 和 5210

流量收集器收集 NetFlow、cFlow、J-Flow、Packeteer 2、NetStream 和 IPFIX 数据，以提供基于行为的网络保护。

流收集器从多个网络或网段汇聚高速网络行为数据，可提供端到端保护并提高分散在不同地理位置的网络的性能。

如果要部署 Data Store，则可以将 具有 10Gbps SFP+ DAC接口 的流量收集器 4210 配置为 eth0，以提高吞吐量。如果不部署 Data Store，只能将 100Mbps/1 Gbps/10 Gbps 铜缆接口配置为 eth0。

> 当流量收集器接收数据时，无论是进行数据包加密还是分段处理，它都会识别已知或未知的攻击、内部误用和配置错误的网络设备。Secure Network Analytics 识别行为之后，系统就可以对这种类型的行为执行任何您配置的操作（如果有）。

UDP 导向器 2210

UDP 导向器具有高速、高性能 UDP 数据包复制器。UDP 导向器对于向各个收集器重新分发 NetFlow、sFlow、系统日志或简单网络管理协议 (SNMP) 陷阱很有用。它可以从任何无连接 UDP 应用接收数据，然后将数据重新传送至多个目标，从而在需要时复制数据。

使用 UDP 导向器高可用性 (HA) 配置时，请确保使用交叉电缆连接两个 UDP 导向器设备。有关说明，请参阅 **2. 将设备连接至网络**。

流量传感器 1210、3210和 4240

流量传感器是一种网络设备，其工作原理与传统数据包捕获设备或 IDS 类似，因为它可以连接到交换机端口分析器 (SPAN)、镜像端口或以太网测试接入端口 (TAP) 中。流传感器可以增强对以下网络区域的可视性：

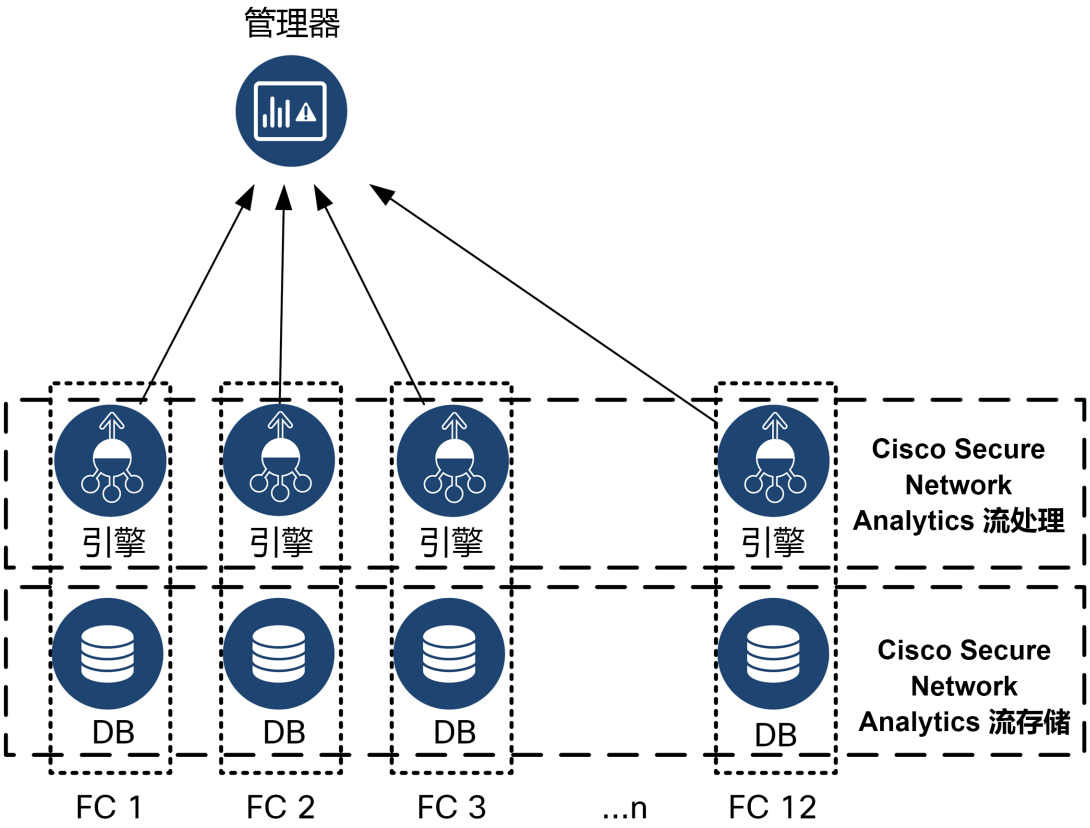
- NetFlow 不可用的情况。
- NetFlow 可用，但您想对性能指标和数据包数据有更深可视性的情况。

通过将流传感器定向到任何支持 NetFlow v9 的 流收集器，您可以从 NetFlow 获得有价值的详细流量统计信息。当与 Secure Network Analytics 流量收集器结合使用时，流传感器还可以提供对性能指标和行为指标的深入了解。这些流量绩效指标提供对任何由网络或服务器端应用引起的往返时间延迟的了解。

由于流量传感器具有数据包级的可视性，因此它可以计算往返时间 (RTT)、服务器响应时间 (SRT) 和 TCP 会话数据包损失。它在发送给流量收集器的 NetFlow 记录中包含所有这些附加字段。

Secure Network Analytics 无 Data Store

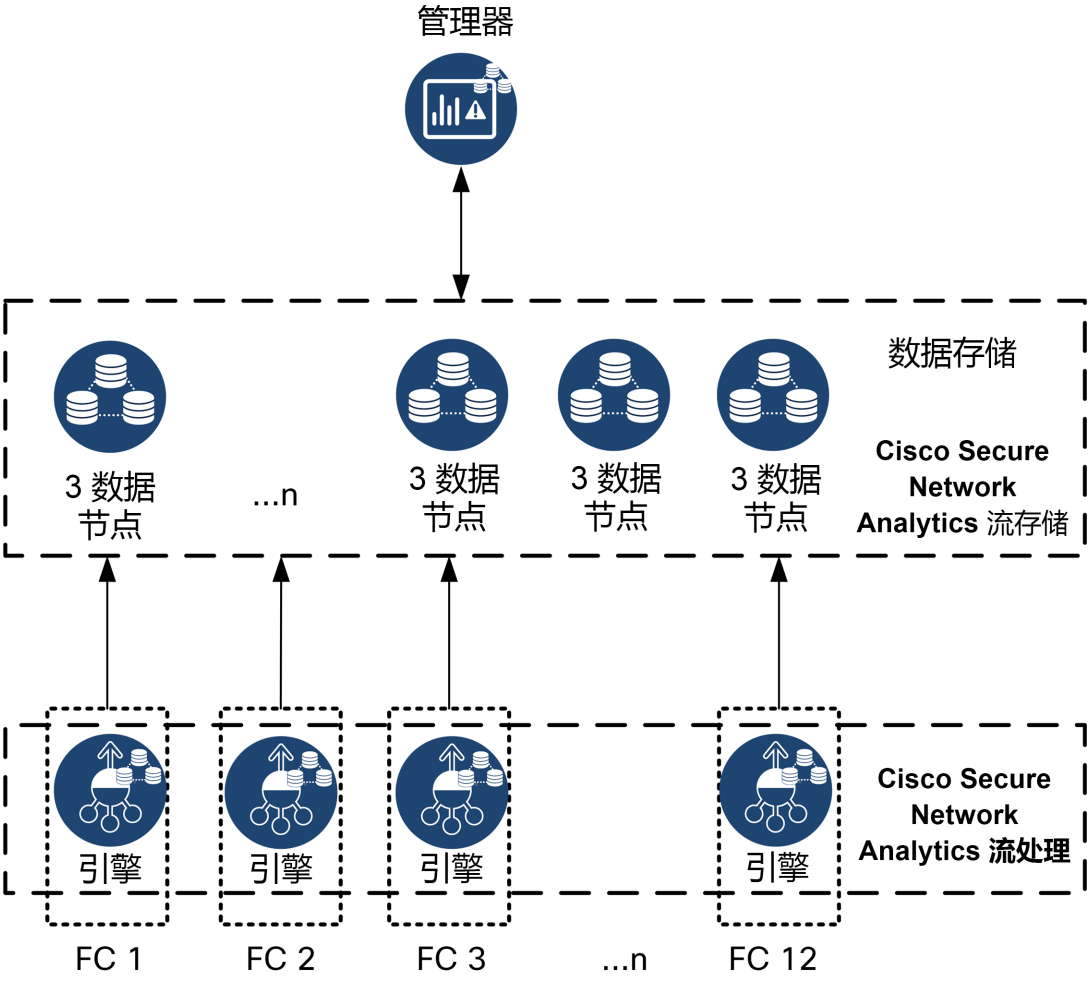
在不具有 Data Store 的 Secure Network Analytics 部署中，一个或多个流收集器会注入并删除重复数据、执行分析，并将数据和结果直接报告给 管理器。要解析用户提交的查询（包括图形和图表），管理器会查询所有受管的流收集器。而每个流收集器会将匹配的结果返回给管理器。管理器会整理来自不同结果集的信息，然后生成显示结果的图形或图表。在此部署中，每个流收集器会在本地数据库中存储数据。参见下图中的示例。



带 Data Store 的

Secure Network Analytics

在具有 Data Store 的 Secure Network Analytics 部署中，Data Store 数据库集群位于管理器和流量收集器之间。一个或多个流量收集器会提取和删除重复流数据，执行分析，并将流数据和结果直接报告给 Data Store，将其大致平均分配给所有的 数据节点。Data Store 会促进流数据存储，将所有流量保持在集中位置，而不是分布在多个流收集器上，并提供比单个流收集器甚至多个流收集器更大的存储容量。参见下图中的示例。



Data Store 提供了一个中央存储库，用于存储由流收集器收集的网络遥测数据。Data Store 由 数据节点集群组成(每个都包含您的数据的一部分)和单独 数据节点 数据的备份组成。由于您的所有数据都在一个集中式数据库中，而不是分布在多个流收集器中，因此与单独查询所有流收集器相比，您的管理器可以更快地从 Data Store 中检索查询结果。Data Store 集群可改善容错能力，提高查询响应速度并加快图形和图表填充。

查询

为解决用户提交的查询(包括图形和图表),管理器 会查询 Data Store。Data Store 在与查询相关的列中找查找匹配结果,然后检索匹配行并将查询结果返回给 管理器。管理器会生成图形或图表,无需从多个流收集器收集多个结果集。与查询多个流收集器相比,这可以降低查询成本,同时提高查询性能。

Data Store 存储和容错能力

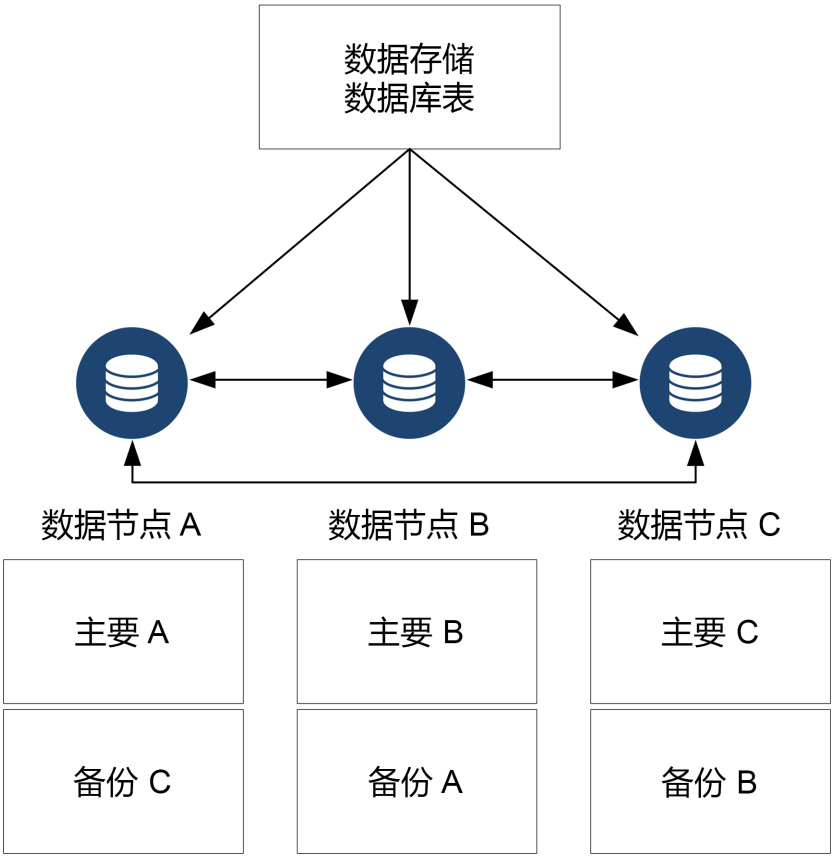
Data Store 会从流收集器收集数据,并将数据平均分配到集群内的 数据节点。每个 数据节点,除了存储整体遥测的一部分外,还会存储另一个 数据节点 遥测的备份。以这种方式来存储数据:

- 帮助实现负载均衡
- 将处理分布到每个节点上
- 确保注入 Data Store 的所有数据都有容错备份
- 允许增加 数据节点 的数量,以提高整体存储和查询性能

如果您的 Data Store 有 3 个或更多数据节点,并且数据节点关闭,但只要数据节点包含其备份的节点仍然可用,并且您的数据节点总数的至少一半仍处于运行状态,则总体 Data Store仍将保持运行状态。这让您有时间修复断开的连接或出现故障的硬件更换出现故障的 数据节点 后,Data Store 会从相邻 数据节点 上存储的现有备份恢复该节点的数据,并在该 数据节点 上创建数据备份。

遥测存储示例

有关 3 数据节点 如何存储遥测的示例，请参阅下图：



一般部署要求

在开始之前，请查看本指南以了解此流程以及计划安装所需的准备工作、时间和资源。

硬件和软件版本发布

有关兼容性的详细信息，请参阅 硬件和软件版本表。该矩阵可从以下网址获取：https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html。

规格

下载您计划安装的每个设备的规格表。该矩阵可从以下网址获取：https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html。

思科集成管理控制器 (CIMC)

安装设备后，请确保配置思科集成管理控制器 (CIMC) 以启用对服务器配置和虚拟服务器控制台的访问。您还可以使用 CIMC 监控硬件运行状况。

- **说明：**请参阅 **使用 CIMC 连接（远程访问需要）**，并按照 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：**作为初始配置的一部分，您将以管理员身份登录 CIMC 并在密码字段中键入 **密码**
- **密码要求：**登录时，请更改默认密码以保护网络安全。

标准设备要求(无 Data Store)

如果不使用 Data Store安装 Secure Network Analytics，请安装以下设备：

设备	要求
管理器	• 至少 1 个 管理器
流收集器	• 至少 1 个 流收集器
流传感器	可选
UDP 导向器	可选

要查看具有数据储存的 Secure Network Analytics 的设备安装要求，请参阅 **Data Store 部署要求**部署要求。

管理器和流量收集器部署要求

对于部署的每个 管理器 和 流收集器，将可路由 IP 地址分配给 `eth0` 管理端口。

Data Store 部署要求

要使用 Data Store 部署Secure Network Analytics，请查看以下部署要求和建议。

设备要求（带 Data Store）

下表概述了使用 Data Store 部署 Secure Network Analytics 所需的设备。

设备	要求
管理器	• 至少 1 个 管理器
Data Store	• 至少 1 个或 3 个数据节点 • 额外的 3 组 数据节点扩展至 Data Store，最多 36 个 数据节点 • 不支持在集群中仅部署 2 个数据节点。
流收集器	• 至少 1 个 流收集器
UDP 导向器	可选
流传感器	可选

⚠ 请勿更新设备 BIOS，否则可能会导致设备功能出现问题。

管理器和流量收集器部署要求

对于部署的每个 管理器 和 流收集器，将可路由 IP 地址分配给 `eth0` 管理端口。

- **eth0 端口配置：**您可以配置使用 **BASE-T** 铜缆 1G/10G 端口或 SFP+ twinax 电缆 10G 端口作为 管理器 和 流收集器`eth0` 管理端口。
- **吞吐量：**我们要求 BASE-T 铜缆端口的吞吐量为 10G 以供 Data Store 使用。如果不部署 Data Store，只能将 100Mbps/1Gbps/10 Gbps 铜缆接口配置为 `eth0`。

数据节点部署要求

每个Data Store由若干个 数据节点 组成。

- **硬件：**每个硬件 数据节点 都有独立的硬件机箱。当您购买硬件 Data Store，会收到多个 数据节点 硬件机箱，对应于该 Data Store 型号指示的节点数量。例如，DS 6200 Data Store 提供 3 个 数据节点 硬件机箱。
- **虚拟版本：**下载虚拟版本Data Store时，可以部署 1 个、3 个或更多虚拟版本数据节点（以 3 个为一组）。

> 确保您的数据节点全部为硬件或全部为虚拟版本。不支持混合使用硬件和虚拟 数据节点，硬件必须来自同一代硬件（全部为 DS 6200 或全部为 DN 6300）。

多数据节点部署

多重数据节点部署可提供最佳性能结果。例如，具有 3 个数据节点的 6200 每秒的Data Store可以处理大约 100 万个流，并将该数据保留大约 90 天。

请注意以下提示：

- **3 个一组：**数据节点可以作为 Data Store 的一部分以 3 的倍数进行集群，从最小 3 到最大 36。不支持在集群中仅部署 2 个数据节点。
- **全部硬件或全部虚拟：**确保您的数据节点全部为硬件或全部为虚拟版本。不支持混合使用硬件和虚拟数据节点，也不支持 Data Store 6200 和 6300 数据节点混合使用。

单 数据节点 部署

如果您选择部署单个 (1) 数据节点：

- **流量收集器：**最多支持 4 个 流收集器。
- **添加数据节点：**如果仅部署一个数据节点，则可以在未来将数据节点添加到部署中。有关详细信息，请参阅 **多数据节点部署**。

> 这些建议仅考虑遥测。您的性能可能因其他因素而异，包括主机计数、流传感器 使用、流量配置文件和其他网络特征。请联系思科支持部门寻求估算协助。

> 目前，如果主 数据节点 发生故障，Data Store 不支持将备用 数据节点 部署为自动替换。请联系思科支持部门寻求指引。

数据节点配置需求

要部署 Data Store，请为每个 数据节点 分配以下内容。您准备的信息将在初始设置中使用系统配置指南进行配置。

- **可路由 IP 地址 (eth0)：**用于管理、注入以及查询与 Secure Network Analytics 设备的通信。
- **eth0 端口配置：**您可以配置使用 **BASE-T** 铜缆 1G/10G 端口或 SFP+ twinax 电缆 10G 端口作为 `eth0` 管理端口。
- **吞吐量：**我们要求 BASE-T 铜缆端口的吞吐量为 10G 以供 Data Store 使用。
- **数据节点间通信：**在专用 LAN 或 VLAN 内配置来自 `169.254.42.0/24` CIDR 块的不可路由 IP 地址，用于数据节点间通信。

  将 数据节点 `eth2` 端口或包含 `eth2` 和 `eth3` 的端口通道连接到交换机以进行数据节点间通信，提高吞吐量性能。作为 Data Store 的一部分，数据节点 会在相互之间通信。
- **网络连接：**两个 10G 网络连接，一个用于管理、接收和查询通信，一个用于数据节点间通信
- **其他连接和交换：**（可选）仅在硬件数据节点上，为了实现数据节点间通信的网络冗余和重要性，安装额外的 10G 连接和额外的交换机用于在数据节点上建立端口通道。

> 配置数据节点，以便使用单独的冗余电源为相邻编号数据节点供电。此配置可改善数据冗余和整体 Data Store 正常运行时间。

网络和交换注意事项

下表概述了使用 Data Store 部署 Secure Network Analytics 时的网络和交换注意事项。

网络注意事项	描述
数据节点间通信	• 在 数据节点之间建立低于 200 微秒 的建议往返时间 (RTT) 延迟 • 在 数据节点之间保持 1 秒或更低的时钟偏差。 • 在 数据节点之间建立建议的 6.4 Gbps 或更高的吞吐量 (10 Gbps 全双工交换连接) 。 • 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。
数据节点硬件电源	• 如果硬件 数据节点 意外断电，数据可能会损坏。在不间断电源的单独电路上使用两个电源。 • 初始化Data Store集群时，请根据数据节点各自使用的电源进行备用数据节点配置。这可以通过减少断电时停机的 数据节点的数量来优化容错能力。
数据节点交换	• 数据节点需要自己的第 2 层 VLAN 来实现数据节点 间通信。硬件 数据节点可以连接到共享或专用 10G 交换机。 • 我们建议硬件 数据节点连接到两台交换机，以帮助确保交换机中断和升级期间的持续连接。数据节点 间通信所需的低延迟，Cisco 建议使用一对冗余的交换机，其中 2 台交换机相互连接，并在两台交换机上承载第二层 VLAN。
Secure Network Analytics 设备通信	• 管理器和流量收集器必须能够访问所有的 数据节点 • 数据节点 必须能够访问管理器、所有流量收集器以及每个 数据节点

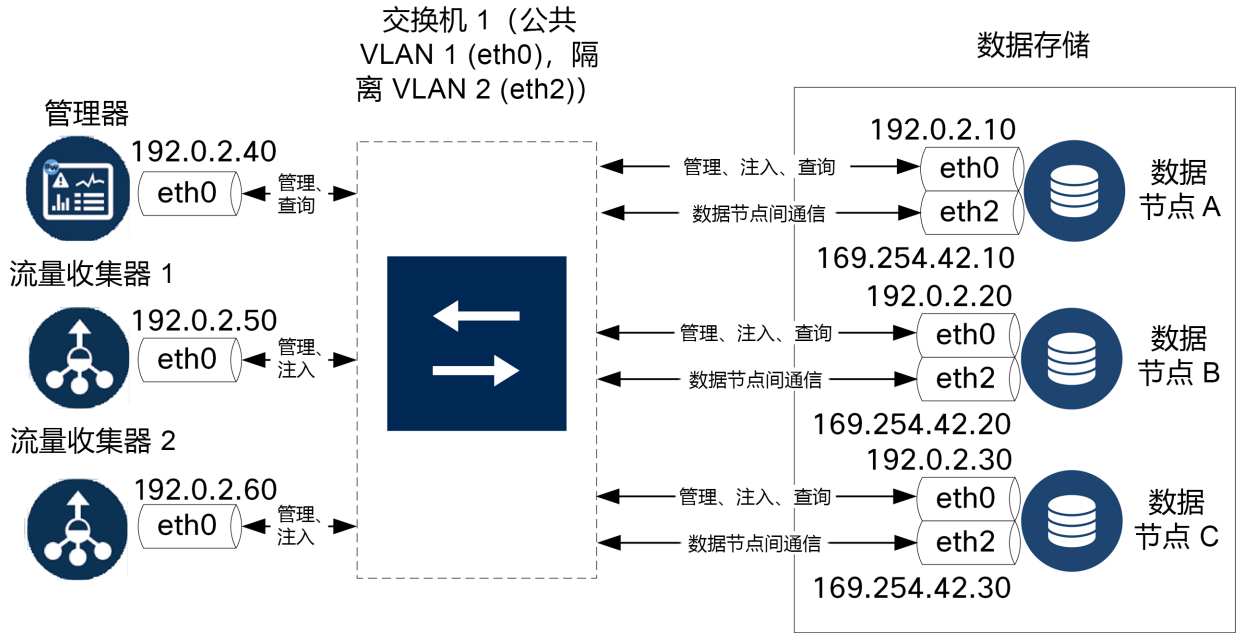
> 目前，如果主 数据节点 发生故障，Data Store 不支持将备用 数据节点 部署为自动替换。请联系思科支持部门获取指导。

硬件交换示例

要启用通过 eth2 或 eth2/eth3 端口通道进行的数据节点 间通信，部署 1 台支持 10G 速度的交换机。

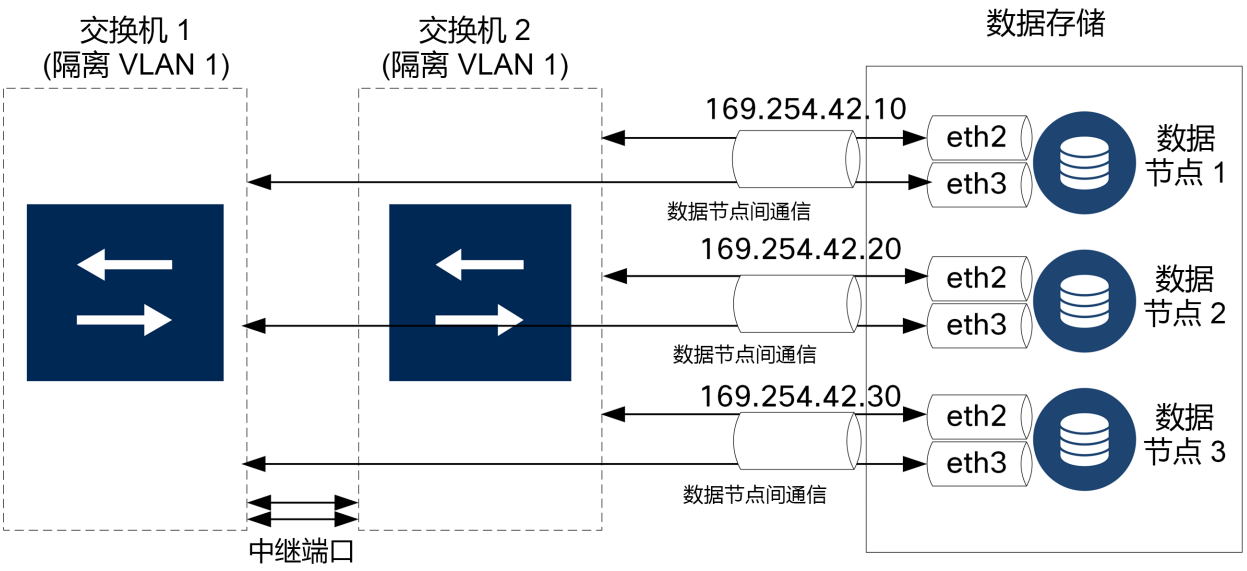
为 数据节点s eth0 与管理器 和流量收集器的通信配置一个公共 LAN 或 VLAN，并为数据节点间通信配置一个隔离 LAN 或 VLAN。

您可以与其他设备共享这些交换机，但要为额外的设备流量创建单独的 LAN 或 VLAN。参见下图中的示例：



Data Store 集群需要隔离 VLAN 内的节点间持续心跳。如果没有心跳，数据节点 可能会离线，而这样会增大 Data Store 停机的风险。

如果您需要额外的网络冗余，为了规划交换机更新和计划中断，确保您使用专用的数据节点 间通信端口通道配置 数据节点。链接每个 数据节点 至 2 台交换机，每个物理端口连接到不同的交换机。参见下图中的示例：



请联系思科专业服务，获取有关规划部署的帮助。

Data Store 放置注意事项

放置每个 数据节点，以便它能够与您的流收集器、管理器以及每个其他 数据节点 进行通信。为获得最佳性能，请协同定位 数据节点和 流收集器以最大限度地减少通信延迟，同时协同定位 数据节点和 管理器 以实现最佳查询性能。

- **防火墙：**我们强烈建议将 数据节点放在您的防火墙内，例如在 NOC 内。
- **电源：**如果 Data Store 由于断电或硬件故障而关闭，则可能会增大数据损坏和数据丢失的风险。安装 数据节点时始终要考虑正常运行时间。

如果 数据节点 意外断电并且您重新启动了设备，那么 数据节点 上的数据库实例可能不会自动重新启动。有关故障排除和手动重启数据库，请参阅 系统配置指南 。

- **策略：**检查是否已将硬件 数据节点 电源恢复策略设置为 **恢复上次状态**，这会在断电后自动重新启动 数据节点 ，并尝试恢复正在运行的进程。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 。

分析部署要求

Secure Network Analytics 使用动态实体建模来跟踪网络状态。在 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。

要启用 Analytics，您的部署必须

- 配置在具有任意数量 Data Store 的虚拟或硬件 流收集器 部署上。
- 仅配置 1 个 Secure Network Analytics Data Store 域。

1. 为通信配置 防火墙

为了使设备正常通信，您应配置网络，以便让防火墙或访问控制列表不会阻止所需的连接。使用此部分提供的信息配置网络，以便设备可以通过网络进行通信。

开放端口(所有设备)

请咨询您的网络管理员，确保以下端口已打开并且具有不受限制的访问权限(管理器、流收集器、数据节点、流传感器和 UDP 导向器)：

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

数据节点的其他开放端口

此外，如果将 数据节点 部署到您的网络，请确保以下端口已打开并且具有不受限制的访问权限：

- TCP 5433
- TCP 5444
- TCP 9450

通信端口和协议

下表显示了如何在 Secure Network Analytics中使用端口：

从(客户端)	到(服务器)	端口	协议
管理员用户 PC	所有设备	TCP/443	HTTPS

从(客户端)	到(服务器)	端口	协议
所有设备	网络时间源	UDP/123	NTP
Active Directory	管理器	TCP/389, UDP/389	LDAP
思科 ISE	管理器	TCP/443	HTTPS
思科 ISE	管理器	TCP/8910	XMPP
外部日志来源	管理器	UDP/514	SYSLOG
流收集器	管理器	TCP/443	HTTPS
UDP 导向器	管理器	TCP/443	HTTPS
UDP 导向器	流收集器 (sFlow)	UDP/6343*	sFlow
UDP 导向器	流收集器 (NetFlow)	UDP/2055*	NetFlow
UDP 导向器	第三方活动管理系统	UDP/514	SYSLOG
流传感器	管理器	TCP/443	HTTPS
流传感器	流收集器 (NetFlow)	UDP/2055	NetFlow
NetFlow 导出器	流收集器 (NetFlow)	UDP/2055*	NetFlow
sFlow 导出器	流收集器 (sFlow)	UDP/6343*	sFlow
管理器	UDP 导向器	TCP/443	HTTPS
管理器	思科 ISE	TCP/443	HTTPS
管理器	思科 ISE	TCP/8910	XMPP
管理器	DNS	UDP/53	DNS
管理器	流收集器	TCP/443	HTTPS
管理器	流传感器	TCP/443	HTTPS
管理器	流导出器	UDP/161	SNMP

从(客户端)	到(服务器)	端口	协议
管理器	LDAP	TCP/636	TLS
管理器	CRL 分发点:	TCP/80	HTTP
管理器	OCSP 响应方 URL	TCP/80	OCSP
用户 PC	管理器	TCP/443	HTTPS

*这是默认端口,但可以在导出器上配置任何 UDP 端口。

其他开放端口 Data Store

以下列出了在防火墙上打开以部署 Data Store的通信端口。

#	从(客户端)	到(服务器)	端口	协议或用途
1	管理器	流收集器和 数据节点	22/TCP	SSH, 用于初始化 Data Store 数据库
1	数据节点s	所有其他 数据节点	22/TCP	SSH, 用于初始化 Data Store 数据库和执行数据库管理任务
2	管理器、流收集器和 数据节点	NTP 服务器	123/UDP	NTP, 用于时间同步
2	NTP 服务器	管理器、流收集器和 数据节点	123/UDP	NTP, 用于时间同步
3	管理器	流收集器和 数据节点	443/TCP	HTTPS, 用于设备之间的安全通信
3	流收集器s	管理器	443/TCP	HTTPS, 用于设备之间的安全通信
3	数据节点s	管理器	443/TCP	HTTPS, 用于设备之间的安全通信
4	NetFlow 导出器	流量收集器 - NetFlow	2055/UDP	NetFlow 注入
5	数据节点s	所有其他 数据节点	4803/TCP	数据节点 间的消息服务
6	数据节点	所有其他 数据节点	4803/UDP	数据节点 间的消息服务
7	数据节点s	所有其他 数据节点	4804 / UDP	数据节点 间的消息服务
8	管理器、流收集器和 数据节点	数据节点s	5433/TCP	Vertica 客户端连接

9	数据节点	所有其他 数据节点	5433/UDP	Vertica 消息服务监控
10	sFlow 导出器	流收集器 (sFlow)	6343/UDP	sFlow 注入
11	数据节点s	所有其他 数据节点	6543/UDP	数据节点 间的消息服务

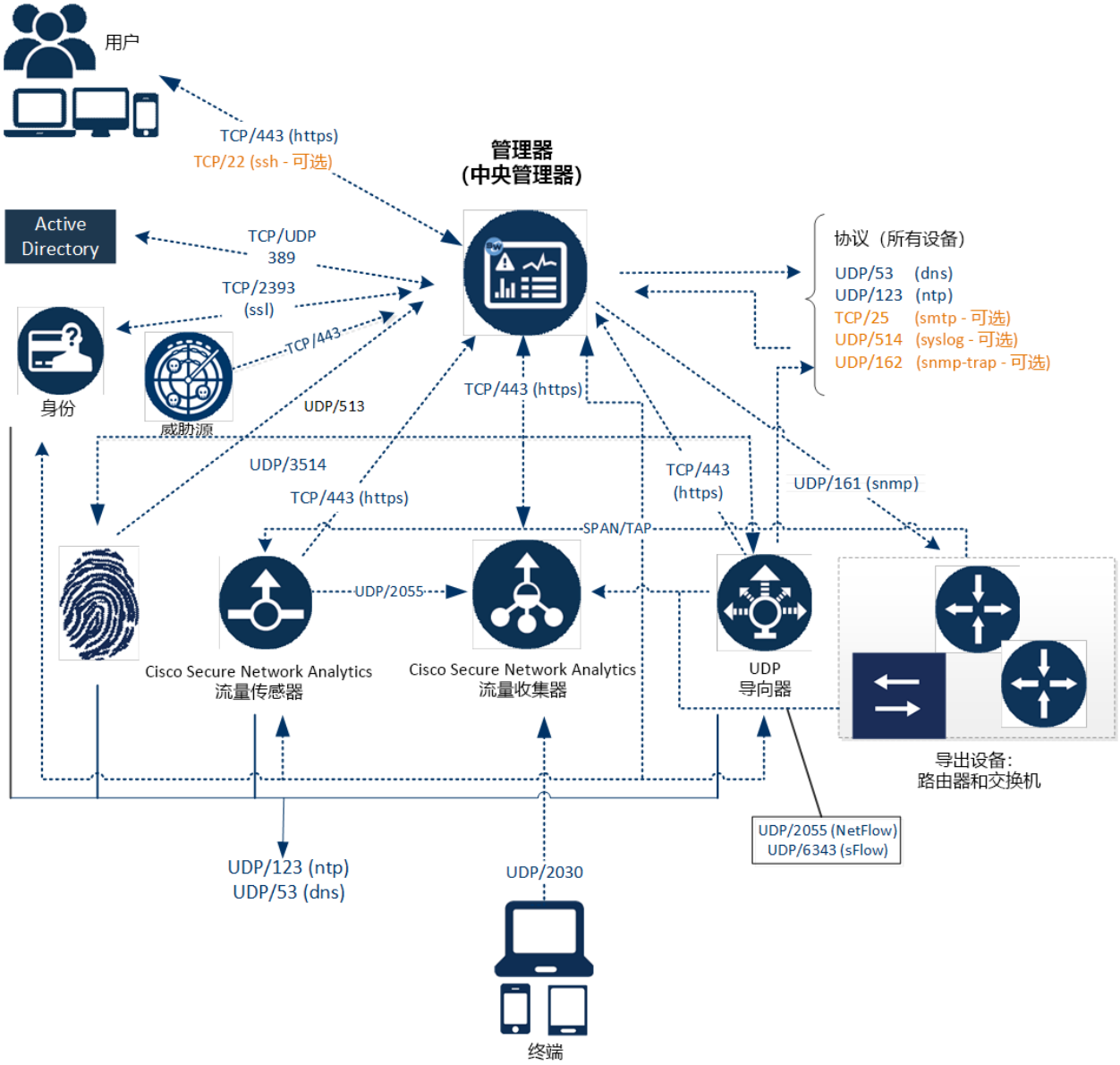
可选通信端口

下表是根据您的网络需求确定的可选配置:

从(客户端)	到(服务器)	端口	协议
所有设备	用户 PC	TCP/22	SSH
管理器	第三方活动管理系统	UDP/162	SNMP-陷阱
管理器	第三方活动管理系统	UDP/514	SYSLOG
管理器	电邮网关	TCP/25	SMTP
管理器	威胁源	TCP/443	SSL
用户 PC	所有设备	TCP/22	SSH

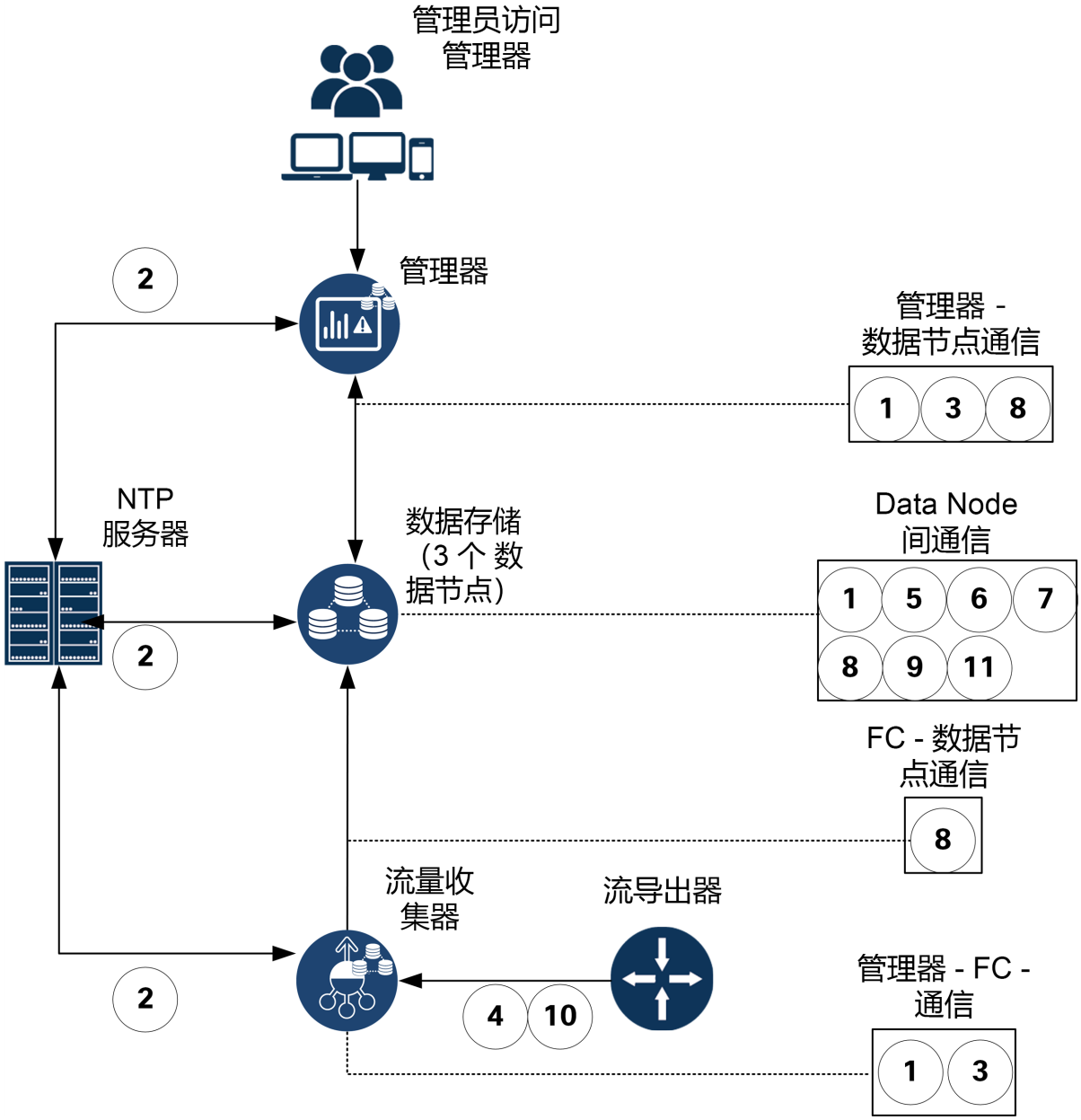
Secure Network Analytics 部署示例

下图显示了 Secure Network Analytics使用的各种连接。其中一些端口是可选的。



Secure Network Analytics 通过 Data Store 部署 示例

如下图所示，您可以战略性地部署 Secure Network Analytics 设备，以在整个网络中提供关键网段的最佳覆盖，无论是在内部网络中、在边界还是在 DMZ 中。



2. 安装警告和指南

安装警告

请在安装 Secure Network Analytics x2xx 设备之前阅读 合规支持和安全信息 文档。

请注意以下警告：

陈述 1071-警告定义

重要安全说明

此警告符号表示危险。您目前所处情形有可能遭受身体伤害。在操作任何设备之前，请务必了解触电危险并熟悉标准工作程序，以免发生事故。请根据每个警告结尾处的声明号来查找此设备随附的安全警告的翻译文本。

请妥善保存这些说明

陈述 1004-安装说明

请在使用、安装或将系统与电源连接前阅读此安装说明。

陈述 1005-断路器

此产品的短路(过载电流)保护由建筑物的供电系统提供。

陈述 1006-关于机架安装和维修的机箱警告

为避免在机架中安装或维修该部件时造成人身伤害，您必须采取特殊的预防措施确保系统固定。为确保您的安全，请遵循以下准则：
- 如果本设备是机架中的唯一设备，则应将其安装在机架底部。
- 如果在部分装满的机架中安装此部件，请按从下往上的顺序安装各个部件，并且最重的部件应安装在机架的底部。
- 如果在部分装满的机架中安装此部件，请按从下往上的顺序安装各个部件，并且最重的部件应安装在机架的底部。

陈述 1015-电池处理

为了降低火灾、爆炸或可燃性液体或气体泄漏的风险：
- 只能使用制造商推荐的相同或同等类型的电池进行更换。
- 请勿拆解、碾压、刺穿或使用锋利的工具卸下电池，也不要造成外部接触点短路或将电池投入火中
- 如果电池变形或胀大，请勿使用。

- 请不要在温度超过 140°F/60°C 的环境中储存或使用电池。
- 请不要在气压低于 69.7 kPa 的环境中储存或使用电池。

陈述 1017-限制区域

本部件应安装在限制进出的区域。仅熟练人员、受指导人员或有资质人员才能进入限制进入的区域。

陈述 191-日本的自愿干扰控制委员会 (VCCI) A 类警告

这是基于 VCCI 委员会标准的 A 类产品。如果在生活环境中使用本设备，可能会造成无线电干扰，在这种情况下，您可能需要采取校正措施。

陈述 164-搬运要求

需要两个人来抬起产品的较重部件。为了避免受伤，请挺直背部，用腿部而非背部力量抬起。

陈述 256-匈牙利的 A 类警告

此设备为 A 类产品，应根据匈牙利 EMC A 类要求 (MSZEN55022) 正确使用和安装。A 类设备专为使用特殊安装条件和保护距离的典型商业机构而设计。

陈述 294-韩国的 A 类警告

这是 A 类设备，符合工业用途的电磁兼容性 (EMC) 要求。卖方或买方应了解这一点。如果此类型被错误地出售或购买，则应将其替换为住宅用途类型。

陈述 340-CISPR22/EN55022/CISPR32/EN55032 的 A 类警告

这是 A 类产品。在生活环境中，此产品可能会造成无线电干扰，您可能需要采取适当措施。

陈述 1021-SELV 电路

为避免触电，请勿将安全的超低电压 (SELV) 电路连接至电话网络电压 (TNV) 电路。LAN 端口包含 SELV 电路，WAN 端口包含 TNV 电路。某些 LAN 和 WAN 端口都使用 RJ-45 连接器。连接电缆时请小心。

陈述 1024-接地导体

接地导体此设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作此设备。如果您不能确定是否已正确接地，请联系合适的电路检测方面的权威人士或电工。

陈述 1028-多个电源

此部件连接的电源可能不止一个。为降低触电风险，在停止为此装置供电时必须断开所有电源。

陈述 1029-空面板和盖板

空面板和盖板具有以下三项重要功能：降低触电和火灾风险；屏蔽电磁干扰 (EMI)，以免影响其他设备；引导冷却气流通过机箱。只有在所有插卡、面板、前盖和后盖都安装到位的情况下才能对系统进行操作。

陈述 1030-设备按照

仅允许经过培训的合格人员安装、更换或维修本设备。

陈述 1032-搬运机箱

为了预防人身伤害或机箱损坏，切勿企图使用模块(如电源、风扇或卡)上的把手提起机箱或使之倾斜。这些类型的把手无法承载单元重量。

陈述 9001-产品处置

该产品的最终处置应遵照所有适用的国家法律和法规进行。

陈述 1051-激光辐射

已断开的光纤或连接器可能会发出不可见的激光辐射。请勿凝视射束或通过光学仪器直接观看。

陈述 1055-1/1M 类激光

存在不可见的激光辐射。勿使用光学仪器直接观看，1类或1M激光产品。

陈述 1008-1 类激光产品

本产品为 1 类激光产品。

陈述 1056-无端接光缆

无端接光纤电缆的末端或连接器可能会发出不可见的激光辐射。请勿通过光学仪器直接观看。使用某些光学仪器(例如,头戴式放大镜、普通放大镜和显微镜)在 100 毫米的距离内观看激光输出可能会对眼睛造成伤害。

光纤类型和纤芯直径 (µm)	波长 (nm)	最大功率 (mW)	波束离散 (rad)
SM 11	1200-1400	39-50	0.1-0.11
MM 62.5	1200-1400	150	0.18 NA
MM 50	1200-1400	135	0.17 NA
SM 11	1400-1600	112-145	0.11-0.13

陈述 1089-受指导人员及熟练人员定义

受指导人员是指接受过熟练人员的指导和培训,并在操作设备时采取了必要预防措施的人员。

熟练人员或有资质人员是指在设备相关技术领域接受过培训或拥有经验,了解操作设备的潜在危害的人员。

陈述 1090-由熟练人员安装

仅熟练人员可以对此设备执行安装、更换或维修操作。有关技术人员的定义,请参阅声明 1089。

陈述 1091-由熟练人员安装

仅熟练人员可以对此设备执行安装、更换或维修操作。有关受指导人员或熟练人员的定义，请参阅声明 1089。

陈述 1074-符合本地和国家电气规范

设备的安装必须符合本地和国家电气规范。

陈述 2017-FCC 的 A 类说明

如未经思科书面许可即修改设备，可能导致设备不再符合 FCC 对 A 类数字设备的要求。在此类情况下，对设备的使用权可能会受到 FCC 规程的限制，且用户需要校正对无线电或电视通信的干扰，费用自行承担。
根据 FCC 规则的第 15 部分，经测试证明该设备符合对 A 级数字装置的限制。这些限制旨在提供合理保护，使设备在商业环境下运行时免于有害干扰。该设备产生、使用且可能辐射射频能量；如未按照说明手册予以安装和使用，则会对无线电通信造成有害干扰。如在住宅区运行该设备，则有可能导致有害干扰，在这种情况下，用户必须校正此类干扰，费用自行承担。

陈述 2021-面向加拿大的 A 类说明

此 A 类数字设备符合加拿大 ICES-003/NMB-003 的要求。

陈述 7001-ESD 规避

此设备可能对 ESD 敏感。在处理设备之前，请务必使用 ESD 脚腕或腕带。将 ESD 腕带的设备端连接到设备机箱的未完成表面或设备上的 ESD 插孔（如果有）。

陈述 7003-建筑物内防雷击浪涌屏蔽电缆要求

设备或子组件的建筑物内端口必须使用两端接地的屏蔽式建筑物内布线/接线。
以下端口被视为此设备上的建筑内端口：

陈述 7005-建筑物内雷击浪涌和交流电源故障

设备或部件的建筑内端口只适用于连接到建筑内布线或明线。禁止使用金属线将设备或部件的建筑内端口连接到 OSP 接口或接线距离超过 6 米（约 20 英尺）的接口。这些接口仅能用作建筑内接口（GR-1089 中所述的 2 类、4 类或 4a 类端口）并要求与 OSP 明线隔离。即使添加了主保护器，也不足以为使用金属

将这些接口线连接到 OSP 布线系统提供充足保护。
以下端口被视为设备上的建筑内端口：

安装准则

请注意以下警告：

陈述 1047-防止过热

为防止系统过热，请勿在温度超过建议的最高环境温度（41°F 至 95°F [5°C 至 35°C]）的地方运行此产品。

陈述 1019-主要的切断装置

组合开关插座必须随时可供操作，因为它是主要的切断装置。

陈述 1075-电源线和交流适配器

在安装此产品时，请使用提供的或指定的连接电缆/电源线/交流适配器/电池。使用任何其他电缆/适配器可能会引起故障或火灾。日本《电器及材料安全法》禁止使用 UL 认证电缆(即电线上带有“UL”或“CSA”字样)，带有“PSE”字样的电线不受该主体法的约束，适用于思科指定产品以外的其他任何电器。

陈述 1073-无用户可维修部件

内部无用户可维修部件。请勿打开。

当您将安装机箱时，请使用以下指导原则：

- 确保机箱周围有充足的空间，以便于维修机箱，并保证充足的气流。此机箱中的气流自前向后流动。

为确保良好的通风，有必要使用导轨套件对您的机箱进行机架安装。在不使用导轨套件的情况下，将一个机箱放在另一个机箱的顶部或堆叠放置，可能会阻碍机箱顶部的通风，从而导致过热、风扇转速提高和功耗增加。我们建议，在您将机箱安装到机架上时，最好将机箱安装到导轨套件上，因为这些导轨可提供机箱间所需的最小间距。使用导轨套件安装机箱时，不需要在机箱间保留额外的间距。

- 确保空调可以保持机箱所在环境的温度为 41°F 至 95°F(5°C 至 35°C)。
- 确保机柜或机架符合机架要求。
- 确保安装场所电源符合规格表中列出的电源要求。如果适用，您可以使用不间断电源 (UPS)，以避免断电。

避免使用铁磁共振技术类型的 UPS。这些 UPS 类型与某些系统配合使用时可能会不稳定，在波动的数据流量模式中，该系统可能会出现巨大的电流消耗波动。

安全建议

以下信息有助于确保您的安全并保护机箱。该信息可能无法解决您工作环境中的所有潜在危险情况，因此请时刻保持警惕，做出合理的判断。

请遵守以下安全准则：

- 在安装前、安装中和安装后，请保持现场干净且没有灰尘。
- 请勿将工具放在人行通道上，以免绊倒自己和他人。
- 不要穿宽松的衣服或佩戴首饰(如耳环、手镯或项链)，以免卡入机箱。
- 如果您在任何可能对眼睛有危险的条件下工作，请佩戴护目镜。
- 切勿执行对人员有潜在危险或使设备不安全的任何操作。
- 切勿尝试一个人搬运过重的物品。

维护用电安全

⚠ 在操作机箱之前，请务必拔下电源线插头。

在通电的设备上工作时，请遵循以下准则：

- 如果工作场所的某个位置存在潜在危险，切勿单独操作。
- 请勿假设电源已断开；应始终通过检查确保电源已断开。
- 仔细检查您的工作区域是否有潜在危险，例如潮湿的地面、未接地的电源延长线、电源线磨损、未安全接地。
- 如果发生用电事故：
  - 保持谨慎，不要让自己成为受害者。
  - 断开系统电源。
  - 如果可能，请其他人去寻求医疗救助。否则，要评估受害者的状况，然后致电求助。
  - 确定受害人是否需要人工呼吸或胸外按压；然后采取适当的措施。
- 在标示的额定电气条件下使用机箱，并注意遵守产品使用说明。

防范 ESD 损害

电子组件处理不当时会发生静电放电 (ESD)，它会损坏设备并损害电路，进而导致设备发生间歇性或完全故障。

卸下和更换组件时，务必遵循 ESD 预防程序。确保机箱电气接地。佩戴防 ESD 腕带，确保腕带与皮肤密切接触。将接地夹连接到机箱架未上漆的表面，以使 ESD 电压安全接地。为正确防范 ESD 损害和电击，腕带和电源线必须保持有效工作。如果没有腕带，请通过触摸机箱的金属部分使自己接地。

为安全起见，请定期检查防静电腕带的电阻值，该值应介于 1-10 兆欧之间。

现场环境

为避免设备故障，降低环境造成停机的可能性，请仔细规划现场布局和设备位置。如果您的现有设备目前遇到停机或异常高的错误率，这些注意事项可帮助您查明故障原因，防止以后出现问题。

电源注意事项

安装机箱时，请考虑以下事项：

- 安装机箱前检查现场电源，确保电源无峰值和噪声。如有必要，安装功率调节器，确保设备输入电压的电压和功率水平合适。
- 为现场安装适当的接地，避免雷电和电源浪涌造成损坏。
- 机箱没有用户可选择的工作范围。参阅机箱上的标签，了解正确的设备输入电源要求。
- 有多种样式的交流输入电源线可供此设备使用；请确保使用适合您的站点的样式。
- 如果您使用双冗余 (1+1) 电源，我们建议您对每个电源使用独立电路。
- 尽可能为您的现场安装不间断电源。

机架配置注意事项

在规划机架配置时，请考虑以下事项：

- 如果在开放式机架中安装机箱，请确保机架框不会阻塞进气口或排气口。
- 请确保封闭机架中通风良好。请确保机架不过度拥塞，因为每个机箱都会产生热量。封闭的机架应配有百叶侧和风扇为其提供冷却空气。
- 在顶部装有散热风扇的封闭机架中，靠近机架底部的设备产生的热量可能被向上牵引而吸入机架中上方设备的进气口。确保为机架底部的设备创造良好的通风条件。
- 导流板可以帮助隔开排气与进气，这样也有助于引导冷却空气流从机箱内流过。导流板的最佳位置取决于机架中的气流模式。尝试不同的排列方式，有效地定位导流板。

3. 安装设备

您可以将 Secure Network Analytics 设备直接安装在标准 19 英寸机架或机柜，任何其他合适的机柜中或平面上。在机架或机柜中安装设备时，请遵循导轨安装套件中的说明。在确定放置设备的位置时，请确保前后面板之间的间隙如下：

- 可以轻松地读取前面板指示器的状态
- 与后面板端口的通路足以实现不受限制的布线
- 后面板电源插座位于可调节的交流电源的范围内。
- 设备周围和通过通风口的气流不受限制。

设备随附的硬件

Secure Network Analytics 设备随附以下硬件：

- 交流电源线
- 快捷键(用于前面板)
- 用于机架安装的导轨套件或小型设备的安装耳
- 对于流量收集器 5210，使用 10 GB SFP 电缆

其他所需硬件

您必须提供以下所需的其他硬件：

- 用于标准 19 英寸机架的安装螺钉
- 正在安装的每个设备的不间断电源(UPS)
- 要在本地配置(可选)，请使用以下方法之一：
    - 带视频电缆和 USB 电缆(用于键盘)的笔记本电脑
    - 带视频电缆的视频显示器和带 USB 电缆的键盘

4. 将您的设备连接至网络

使用相同的程序将每个设备连接到网络。连接的唯一区别是您拥有的设备类型。

1. 检查规格

使用相同的程序将每个设备连接到网络。连接的唯一区别是您拥有的设备类型。

- **规格表:** 有关每个设备的详细规格信息，请参阅 Secure Network Analytics规格表。
- **UCS 平台:** 思科x2xx 硬件均使用相同的 UCS 平台 UCSC-C220-M5SX，但流量收集器 5210 DB 除外，后者使用 UCSC-C240-M5SX。设备的变体包括 NIC 卡，处理器，内存，存储和 RAID。
- **管理器 2210:** 如果要部署 Data Store，则可以将具有 10Gbps SFP+ DAC 接口的 管理器 2210 配置为 eth0，以提高吞吐量。如果不部署 Data Store，只能将 100Mbps/1 Gbps/10 Gbps 铜缆接口配置为 eth0。
- **流量收集器 4210:** 如果要部署 Data Store，则可以将具有 10Gbps SFP+ DAC 接口的流量收集器 4210 配置为 eth0，以提高吞吐量。如果不部署 Data Store，只能将 100Mbps/1 Gbps/10 Gbps 铜缆接口配置为 eth0。
- **流量收集器 5210:** 流量收集器 5210 由两台相连的服务器(数据库和引擎)组成，因此它们充当单个设备。因此，安装与其他设备略有不同。首先，使用 10G SFP+ DA 交叉连接电缆将它们直接连接在一起。然后，连接到您的网络。

  配置系统时，请确保按照 系统配置指南中指定的顺序配置数据库和引擎。

> ⚠ 请勿更新设备 BIOS，否则可能会导致设备功能出现问题。

2. 将设备连接至网络

要将设备连接到网络，请执行以下操作：

1. 将以太网电缆连接到设备背面的管理端口。
2. 为流量传感器和 UDP 导向器连接至少一个监控端口。

    - **UDP 导向器高可用性：**通过交叉线缆连接两个 UDP 导向器。将一个 UDP Director 的 eth2 端口连接到第二个 UDP Director 的 eth2 端口。同样，使用另一根交叉线缆连接每个 UDP Director 的 eth3 端口。电缆可以是光纤或铜缆。
    - **以太网标签：**请务必注意每个端口的以太网标签（eth2、eth3 等）。这些标签对应于系统配置中使用的网络接口（eth2、eth3 等）。

3. 将以太网电缆的另一端连接至您的网络交换机。
4. 将电源线连接到电源。某些设备有两个电源连接：电源 1 和电源 2。

5. 连接至设备

本节介绍如何连接到设备以进行系统配置。

选择连接程序：

- **使用键盘和显示器连接**
- **使用串行电缆或串行控制台连接**
- **使用 CIMC 连接(远程访问需要)** 要连接到设备进行远程访问，请使用此程序。

使用键盘和显示器连接

要在本地配置 IP 地址，请完成以下步骤：

1. 将电源线插入设备。
2. 按下电源按钮打开设备。等待它完全完成启动。请勿中断启动过程。

> 您可能需要拆下前面板才能通电。
>
> 某些型号的电源风扇在系统未通电时打开。检查前面板上的 LED 已启动。
>
> 请务必将设备连接至不间断电源 (UPS)。电源需要电源，否则系统会显示错误。

3. 连接键盘：
   - 如果您有标准键盘，请将其连接到标准键盘接头。
   - 如果您有 USB 键盘，请将其连接到 USB 连接器。
4. 将视频电缆连接到视频接头。出现登录提示。
5. 转至 **4. 配置您的 Secure Network Analytics System**。

使用串行电缆或串行控制台连接

您还可以使用串行电缆或串行控制台连接到设备，例如具有终端仿真器的笔记本电脑。我们在说明中使用笔记本电脑作为示例。

1. 使用以下方法之一，将笔记本电脑连接至设备：
   - 将 RS232 电缆从笔记本电脑上的串行端口连接器 (DB9) 连接到设备上的控制台端口。
   - 将交叉电缆从笔记本电脑上的以太网端口连接到设备上的管理端口。
2. 将电源线插入设备。
3. 按下电源按钮打开设备。等待它完全完成启动。请勿中断启动过程。

   > 您可能需要拆下前面板才能通电。
   >
   > 某些型号的电源风扇在系统未通电时打开。检查前面板上的 LED 已启动。请务必将设备连接至不间断电源 (UPS)。电源需要电源，否则系统会显示错误。

4. 在笔记本电脑上，连接至设备。

   您可以使用任何可用的终端仿真程序与设备通信。

5. 应用以下设置：
   - BPS：115200
   - 数据位：8
   - 停止位：1
   - 奇偶校验：无
   - 流量控制：无

   系统将显示登录屏幕和登录提示。

6. 转至 **4. 配置您的 Secure Network Analytics System**。

使用 CIMC 连接（远程访问需要）

思科集成管理控制器 (CIMC) 支持访问服务器配置和虚拟服务器控制台，以及监控硬件运行状况。您还将在 Secure Network Analytics 系统配置中使用 CIMC。

1. 请参阅 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。
2. 以管理员身份登录 CIMC，然后在密码字段中输入 **密码** 。
3. 更改默认密码以保护网络安全。
4. 转至 **4. 配置您的 Secure Network Analytics System**。

6. 配置您的 Secure Network Analytics 系统

如果您已完成虚拟版设备和/或硬件设备的安装，即可配置 Secure Network Analytics 到托管系统中。

> ⚠ 要配置 Secure Network Analytics，请按照 系统配置指南 v7.4.2中的说明进行操作。这一步对于成功配置和通信系统至关重要。
>
> 请确保按照系统配置指南中指定的顺序配置设备。

系统配置要求

确保您可以通过 CIMC访问设备控制台。

使用下表为每个设备准备所需的信息。

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 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。	

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

版权信息

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 3 月 16 日	更正了“常规部署要求”一章的问题。
1_2	2023 年 3 月 27 日	更新了通信端口和协议表。
1_3	2023 年 3 月 27 日	更正了一个拼写错误。
1_4	2023 年 3 月 29 日	添加了 LACP 端口绑定信息。
1_5	2023 年 6 月 7 日	更新了安装警告和准则部分。