Cisco Secure Network Analytics

虚拟版本设备安装指南 7.4.2

目录

简介

概述

使用本指南安装以下思科 Cisco Secure Network Analytics (前称Stealthwatch) 虚拟版设备：

- Cisco Secure Network Analytics 管理器 (前称 Stealthwatch 管理控制台) 虚拟版
- Cisco Secure Network Analytics Data Store 虚拟版
- Cisco Secure Network Analytics 流收集器 虚拟版
- Cisco Secure Network Analytics 流传感器 虚拟版
- Cisco Secure Network Analytics UDP 导向器 虚拟版

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。

如果您配置的是虚拟设备，我们假设您已基本熟悉 VMware 或 KVM。

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 Cisco Secure Network Analytics的整体工作流程。

1. **安装设备：**使用本安装指南安装 Cisco Secure Network Analytics 虚拟版设备。要安装硬件(物理) 设备，请按照 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。
2. **配置 Cisco Secure Network Analytics：**安装硬件和虚拟设备后，您便可配置 Cisco Secure Network Analytics 入托管系统。按照 Cisco 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 Cisco Secure Network Analytics的详细信息，请参见以下资源：

- **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

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。

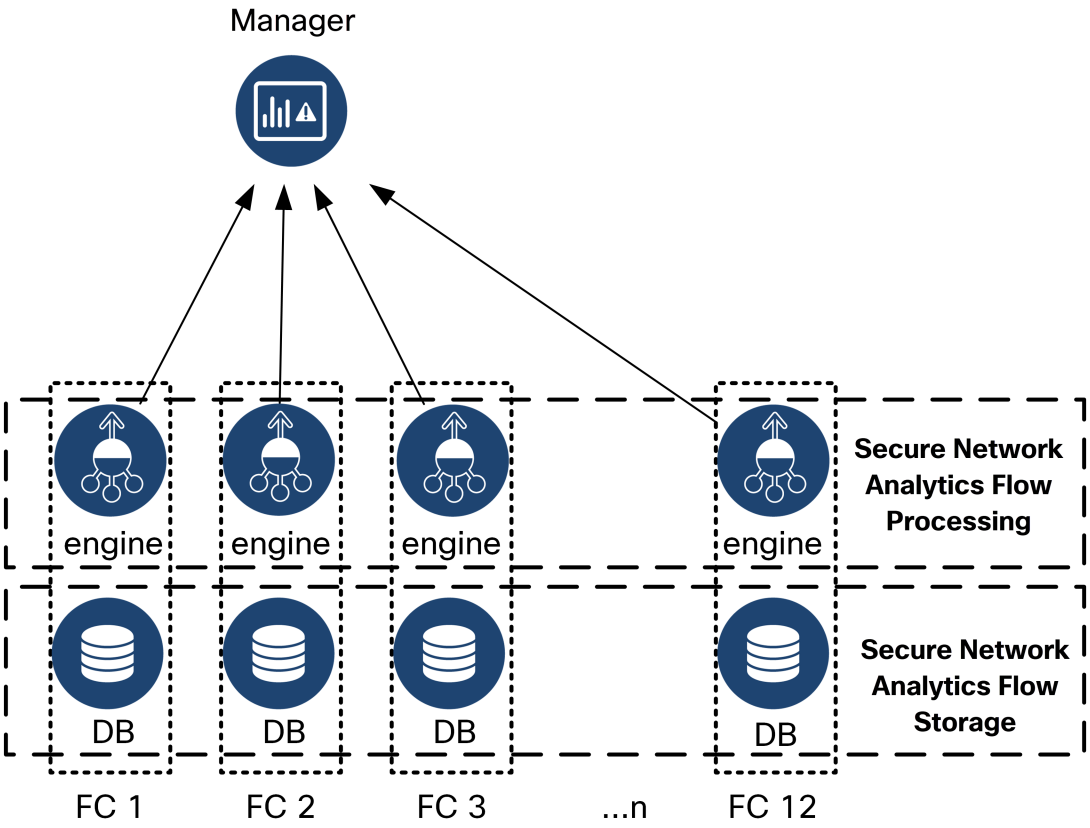
缩写

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
VLAN	虚拟局域网
虚拟机	虚拟机

Cisco Secure Network Analytics 无 Data Store

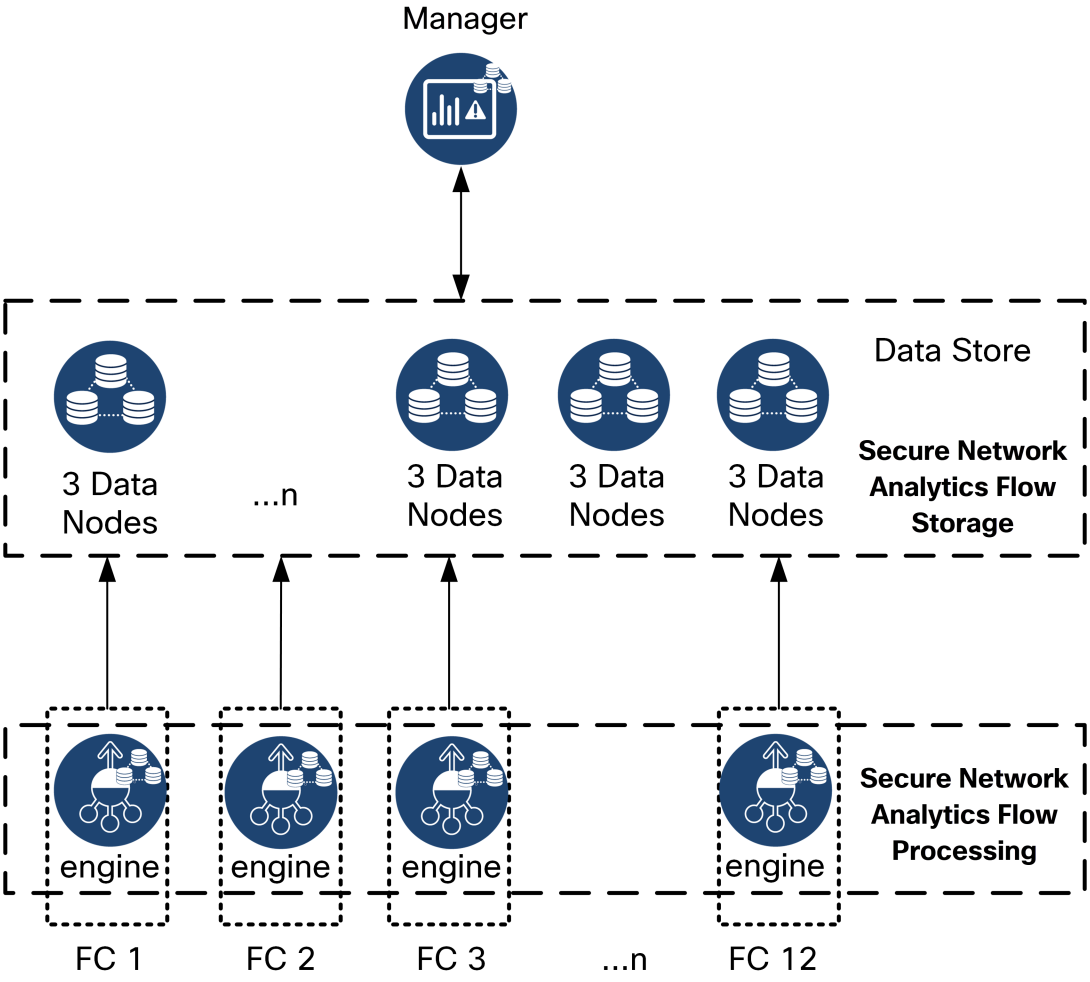
在不具有 Data Store 的 Cisco Secure Network Analytics 部署中，一个或多个流收集器会注入并删除重复数据、执行分析，并将数据和结果直接报告给 管理器。要解析用户提交的查询(包括图形和图表)，管理器会查询所有受管的流收集器。而每个流收集器会将匹配的结果返回给管理器。管理器会整理来自不同结果集的信息，然后生成显示结果的图形或图表。在此部署中，每个流收集器会在本地数据库中存储数据。参见下图中的示例。



带 Data Store 的

Cisco Secure Network Analytics

在具有 Data Store 的 Cisco 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

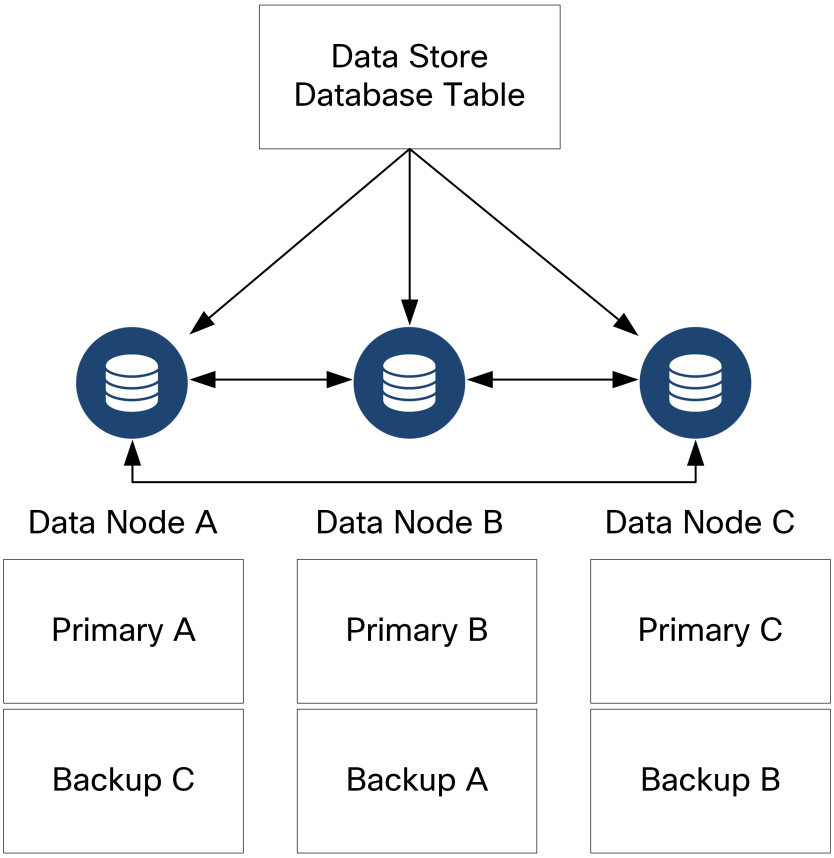
Data Store 会从流收集器收集数据,并将数据平均分配到集群内的 数据节点。每个 数据节点,除了存储整体遥测的一部分外,还会存储另一个 数据节点 遥测的备份。以这种方式来存储数据:

- 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。

安装方法

您可以使用 VMware 环境或 KVM(基于内核的虚拟机)来进行虚拟设备安装。

⚠ 在开始安装之前，请查看以下部分中的 **兼容性** 信息和 **资源要求** 。

方法	安装说明(供参考)	安装文件	详细信息
VMware vCenter	**3a. 使用 VMware vCenter 安装虚拟设备 (ISO)**	ISO	使用 VMware vCenter 安装虚拟设备。
VMware ESXi 独立服务器	**3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO)**	ISO	在 ESXi 独立主机服务器上安装虚拟设备。
KVM 和虚拟机管理器	**3c. 在 KVM 主机上安装虚拟设备 (ISO)**	ISO	使用 KVM 和虚拟机管理器安装虚拟设备。

兼容性

无论您是计划在 VMware 环境中安装虚拟设备还是 KVM(基于内核的虚拟机),请确保查看以下兼容性信息:

所有设备的一般要求

要求	说明
专用资源数量	所有设备都需要分配专用资源,并且无法与其他设备或主机共享。
无实时迁移	由于存在损坏的可能性,设备不支持 vMotion。
网络适配器	所有设备都需要至少一个网络适配器。 流传感器可以配置额外的适配器来支持额外的吞吐量。 作为 Data Store 的一部分,数据节点 需要使用第二个网络适配器与其他数据节点 进行通信。
存储控制器	在 VMware 中配置 ISO 时,请选择 `LSI` 逻辑 `SAS` **SCSI 控制器 (LSI Logic SAS SCSI Controller)** 类型。
存储调配	在部署虚拟设备时分配密集调配的延迟归零存储调配。

VMware

- **兼容性:** VMware 7.0 或 8.0。
- **操作系统:** Debian 11 64 位
- **网络适配器:** 建议使用 VMXNET3 适配器类型以获得最佳性能。
- **ISO 部署:** 安全网络分析 v7.4.2 与 VMware 7.0 和 8.0 兼容。Cisco 安全网络分析 v7.4.x 不支持 VMware 6.0、6.5 或 6.7。有关详细信息,请参阅 vSphere 6.0、6.5 和 6.7 一般支持终止的 VMware 文档。
- **实时迁移:**我们不支持主机间的实时迁移(例如使用 vMotion)。
- **快照:**不支持虚拟机快照。

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

KVM

- **兼容性:**您可以使用任何兼容的 Linux 发行版。
- **KVM 主机版本:**在 KVM 主机上安装虚拟机有多种方法。我们测试了 KVM, 并使用以下组件验证了性能:
  - libvirt 2.10 - 7.1.0
  - qemu-KVM 2.6.1 - 5.2.0
  - Open vSwitch 2.6.x - 2.15.x****
  - Linux 内核 4.4.x 和一些 5.10.x
- **操作系统:** Debian 11 64 位。
- **虚拟化主机**:有关最低要求和最佳性能, 请查看 **资源要求** 部分, 并在 Cisco.com上查看设备的硬件规格表。

> 系统性能取决于主机环境。您的表现可能会有所不同。

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。请参阅 **2. 下载虚拟版安装文件** 以了解有关说明。

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

- **兼容浏览器:** Cisco Secure Network Analytics 支持最新版本的 Chrome、Firefox 和 Edge。
- **Microsoft Edge:** Microsoft Edge 可能存在文件大小限制。我们不建议使用 Microsoft Edge 来安装虚拟版 ISO 文件。

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。

标准设备要求(不具有 Data Store)

如果要安装不具有 Data Store 的 Cisco 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
UDP 导向器	可选
流传感器	可选

要查看具有数据储存的 Cisco 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Cisco Secure Network Analytics，请查看以下部署要求和建议。

设备要求（具有 Data Store）

下表概述了部署具有 Data Store 的 Cisco 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
流传感器	可选

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。

数据节点部署要求

每个Data Store由若干个 数据节点 组成。

- **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)。
- **硬件:** 您还可以安装硬件 数据节点。DN 6300 Data Store 提供 1 数据节点 个硬件机箱。

> 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。

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(同一代)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 数据节点 6300 数据节点混合使用。
- **数据节点配置文件大小:** 如果部署虚拟版本 数据节点，请确保它们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，请参阅资源要求部分中 数据节点虚拟版 。

支持的硬件指标(启用分析)

节点数量	每秒流量	独立内部主机
1	600,000	130 万
3 及以上	600,000	130 万
3 及以上	850,000	700,000

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。如需估算帮助，请联系 思科支持 。

支持的硬件指标(未启用分析)

节点数量	每秒流量	独立内部主机
1	最多 100 万个	最多 3300 万个
3 及以上	最多 300 万个	最多 3300 万个

这些数据是在我们的测试环境中使用客户平均数据和 130 万个独立主机生成的。有一些因素可能会影响您的特定性能(例如，主机数量、流平均大小等)。如需估算帮助，请联系 思科支持 。

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 Cisco Secure Network Analytics 设备的通信。
- **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。

  为提高吞吐量性能，请连接包含 `eth2` 和 `eth3` 的端口通道。确保每个 数据节点 都可以通过虚拟交换机或隔离网络访问 数据节点 。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

网络和交换注意事项

下表概述了部署具有 Data Store 的 Cisco Secure Network Analytics 时的网络和交换注意事项。

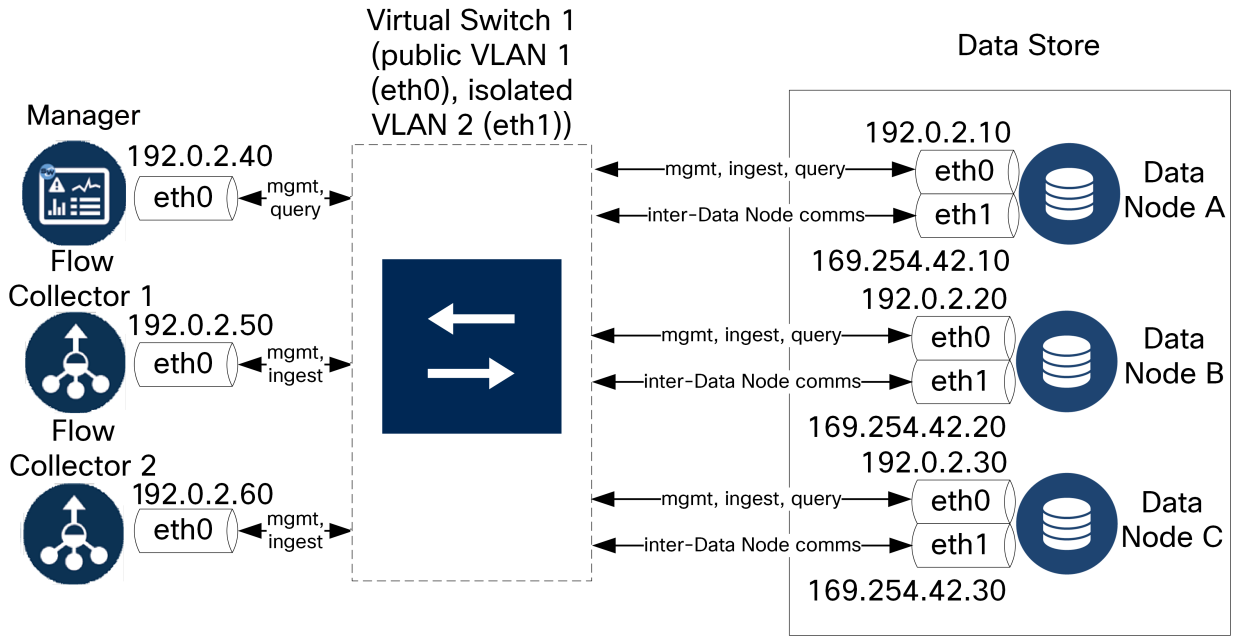
网络注意事项	描述
数据节点 间通信	• 使用虚拟交换机配置隔离的 LAN，以便 数据节点 可以相互进行通信。 • 在数据节点之间建立低于 200 微秒的建议往返时间 (RTT) 延迟 • 在数据节点之间保持 1 秒或更低的时钟偏差。 • 在数据节点之间建立建议的 6.4Gbps 或更高的吞吐量（10 Gbps 全双工交换连接）。
数据节点 交换	• 数据节点需要自己的第 2 层 VLAN 来实现数据节点 间通信。虚拟 数据节点可以连接到隔离网络，具体取决于您部署 数据节点VE 的方式。
Cisco Secure Network Analytics 设备通信	• 管理器和流量收集器必须能够访问所有的 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。

虚拟交换机示例

要在 eth1上启用数据节点 间通信，请为数据节点 间配置具有隔离 LAN 或 VLAN 的虚拟交换机。将虚拟交换机专用于 数据节点 间通信。

另请配置公共 LAN 或 VLAN，以便与 管理器 和流量收集器进行 数据节点 eth0 通信。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。

> 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。
- **物理主机/虚拟机监控程序：**为便于配置，请将所有 数据节点虚拟版部署到同一物理主机/虚拟机监控程序，以简化隔离 LAN 上的数据节点 间配置。
- **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 。

分析部署要求

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 Cisco Secure Network Analytics Data Store 域。

资源要求

本部分介绍虚拟设备的资源要求。

使用本部分提供的表格来记录安装和配置 Cisco Secure Network Analytics 虚拟版设备所需的设置。

- 管理器 虚拟版
- 流收集器 虚拟版
- 数据节点虚拟版
- 流传感器 虚拟版
- UDP 导向器 虚拟版
- 计算每秒流数(可选)

> 确保为系统保留所需的资源。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。

> 下表中的千兆或 GB 引用定义如下：等于 2 的 30 次幂的信息单位，或严格地说是 1,073,741,824 字节。

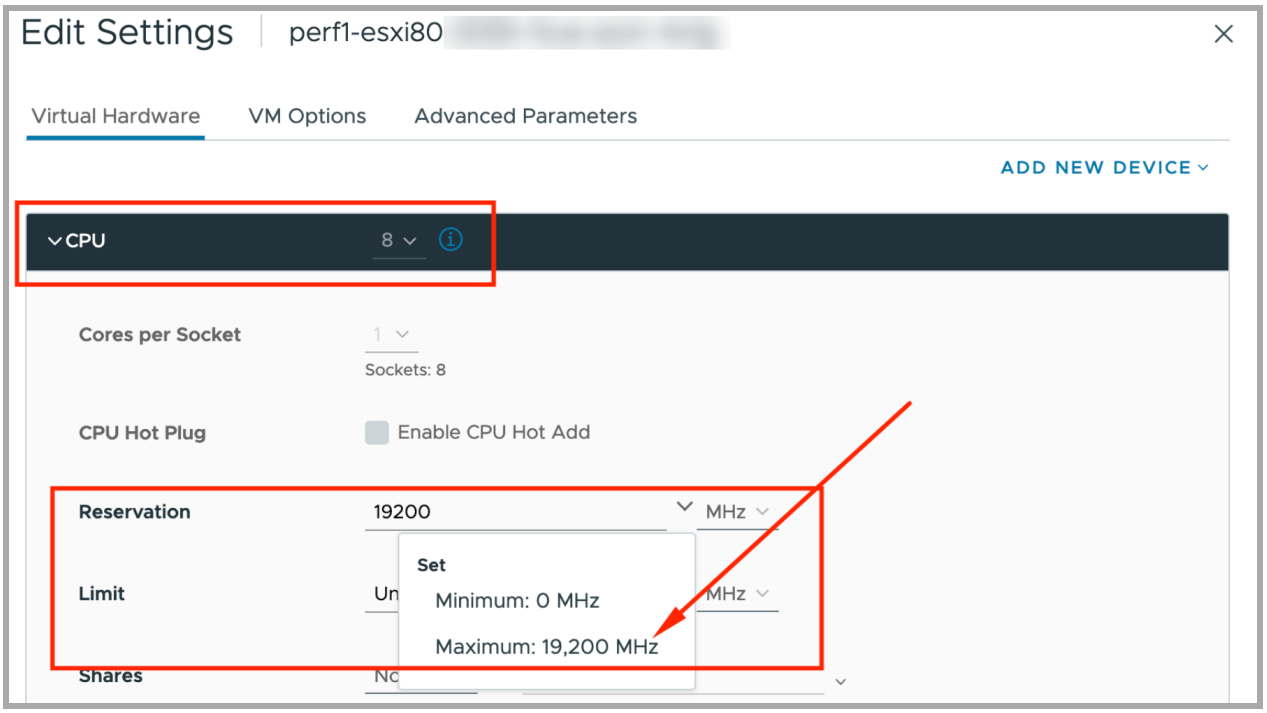
CPU 设置计算

在 EXSi 主机上预留 CPU 时，为了获得最佳性能，请确保在 CPU 设置中，CPU 频率的预留设置使用以下计算：

<推荐的 CPU 数量> * <核心频率> = <频率预留>

您可以在虚拟机监控程序的“主机详细信息”部分下找到 CPU 的核心频率（处理器类型）。

在下面的示例中，您将 8 个 CPU 乘以核心频率，在本例中为 2,400 MHz（或 2.4 GHz）。这将为您提供 19200 MHz 的数量，您将使用它来预留频率。



有关详细信息，请参阅 **3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO)**。

管理器 虚拟版

要确定 管理器 虚拟版的最低资源配置，您应确定预期登录 管理器的并发用户数量。请参阅以下规格以确定您的资源配置。

管理器

并发用户*	所需的保留 CPU	所需的保留内存	所需的最小存储	每秒可处理的流量	内部主机
最多 9	6	40 GB	200 GB	最多 100,000	100,000
超过 10	12	70 GB	480 GB	超过 100,000	250,000

*并发用户包括计划的报告和同时使用 管理器 客户端的人员。

流收集器 虚拟版

要确定 流收集器 虚拟版的资源要求，您应确保网络上预期的每秒流量以及预期监控的导出器和主机数。有关详细信息，请参阅 计算每秒流量 部分。

此外，最小存储空间可能会根据您的 FPS 计算和保留要求而增加。

由于 Data Store 中的 数据节点将存储流而不是 流收集器，因此请确保参考计划部署的规范（不包括 Data Store 或包括 Data Store）。

流收集器 不包括 Data Store

每秒可处理的流量	所需的保留 CPU	所需的保留内存	30 天所需的最小数据存储	接口	导出设备	内部主机
最多 10,000	2	24 GB	600 GB	最多 65535	最多 1024	25,000
最多 30,000	6	32 GB	900 GB	最多 65535	最多 1024	100,000
最多 60,000	8	64 GB	1.8 TB	最多 65535	最多 2048	250,000
最多 120,000	12	128 GB	3.6 TB	最多 65535	最多 4096	超过 250,000

流收集器 包括 Data Store

每秒可处理的流量	所需的保留 CPU	所需的保留内存	所需的最小存储	接口	导出设备	内部主机
最多 10,000	2	24 GB	200 GB	最多 65535	最多 1024	25,000
最多 30,000	6	32 GB	200 GB	最多 65535	最多 1024	50,000
最多 60,000	8	64 GB	200 GB	最多 65535	最多 2048	100,000
最多 120,000	12	128 GB	200 GB	最多 65535	最多 4096	250,000

数据节点虚拟版

查看以下信息以计算 数据节点 虚拟版的资源要求。

- **计算每秒流数:** 确定网络上预期的每秒流数。有关详细信息，请参阅 计算每秒流量 部分。
- **数据节点的数量:** 您可以部署 1 个数据节点或 3 个或更多数据节点(以 3 个为一组)。关于详细信息，请参阅 **设备要求(具有 Data Store)**。

基于 每秒流数 极端，请参阅以下规格来确定您的资源要求:

具有单个虚拟数据节点的 Data Store

每秒可处理的流量	所需的保留 CPU	所需的保留内存	单个 数据节点 30 天保留所需的最小存储空间
最多 30,000	6	32 GB	2.25 TB
最多 60,000	6	32 GB	4.5 TB
最多 120,000	12	32 GB	9 TB
最多 225,000	18	64 GB	18 TB

具有 3 个虚拟数据节点的 Data Store

每秒可处理的流量	所需的保留 CPU	所需的保留内存	每个 数据节点 保留 30 天所需的最小存储空间	3 数据节点 Data Store 30 天保留所需的最小存储空间
最多 30,000	6	32 GB	每个数据节点 1.5 TB	总共 4.5 TB 用于 Data Store
最多 60,000	6	32 GB	每个数据节点 3 TB	总共 9 TB 用于 Data Store
最多 120,000	12	32 GB	每个 6 TB 数据节点	总共 18 TB 用于 Data Store
最多 220,000	18	64 GB	每个 数据节点* 10 TB	总共 30 TB 用于 Data Store*
最多 500,000	18	64 GB	每个 数据节点* 15 TB	总共 45 TB 用于 Data Store*
* 大规模应用 Data Store 优化，以减少遥测的线性增长				

流传感器 虚拟版

本节介绍 流传感器 虚拟版。

- **缓存:** 流量缓存大小列指示 流传感器 可同时处理的最大活动流量。缓存会根据保留的内存量进行调整，并且每 60 秒刷新一次流量。使用“流量缓存大小”(Flow Cache Size) 来计算受监控流量所需的内存量。
- **要求:** 您的环境可能需要更多资源，具体取决于许多变量，例如平均数据包大小、突发速率以及其他网络和主机条件。

NIC 监控端口	所需的保留 CPU	所需的最小保留内存	所需的最小数据存储	估计吞吐量	流量缓存大小 (最大并发流量数)
1 x 1 Gbps	2	4 GB	75 GB	850 Mbps	32,766
2 x 1 Gbps	4	8 GB	75 GB	1,850 Mbps 配置为 PCI 直通的接口(符合 igb/ixgbe 或 e1000e 标准)	65,537
4 x 1 Gbps	8	16 GB	75 GB	3,700 Mbps 配置为 PCI 直通的接口(符合 igb/ixgbe 或 e1000e 标准)	131,073
1 x 10 Gbps*	12	24 GB	75 GB	8 Gbps 配置为 PCI 直通的接口(兼容 Intel ixgbe/i40e)	~512,000

NIC 监控端口	所需的保留 CPU	所需的最小保留内存	所需的最小数据存储	估计吞吐量	流量缓存大小 (最大并发流量数)
2 x 10 Gbps*	22	40 GB	75 GB	16 Gbps 配置为 PCI 直通的接口(兼容 Intel ixgbe/i40e)	~1,000,000

*对于 10 Gbps 吞吐量，请在 1 个插槽中配置所有 CPU。对于每个额外的 10 Gbps NIC，添加 10 个 vCPU 和 16 GB RAM。

可选：可在物理 VM 主机上使用一个或多个 10G NIC。

流传感器 虚拟版网络环境

在安装 流传感器 虚拟版之前，请确保您已知道所拥有的网络环境类型。本指南涵盖 流传感器 虚拟版可以监控的所有类型的网络环境。

兼容性： Cisco Secure Network Analytics 支持 VDS 环境，但不支持 VMware Distributed Resource Scheduler (VM-DRS)。

虚拟网络环境： 流传感器 虚拟版会监控以下类型的虚拟网络环境：

- 具有虚拟局域网 (VLAN) 中继的网络
- 离散 VLAN，其中一个或多个 VLAN 禁止连接数据包监控设备（例如，由于本地策略）
- 专用 VLAN
- 虚拟机监控程序主机而不是 VLAN

流传感器 虚拟版流量

流传感器 将使用以下 Ethertypes 来处理流量：

以太网类型	协议
0x8000	普通 IPv4
0x86dd	普通 IPv6
0x8909	SXP
0x8100	VLAN
0x88a8 0x9100 0x9200 0x9300	VLAN QnQ
0x8847	MLPS 单播
0x8848	MLPS 组播

> 流传感器 会保存顶级 MPLS 标签或 VLAN ID 并将其导出。在处理数据包时，它会绕过其他标签。

UDP 导向器 虚拟版

UDP 导向器 虚拟版要求虚拟机满足以下规格:此外,最小存储空间可能会根据您的 FPS 计算和保留要求而增加。

所需的 保留 CPU	所需的 保留内存	最小数据存储	最大帧率
2	4 GB	75 GB	10,000

计算每秒流数(可选)

如果要根据不同于前面部分中提供的存储量来计算资源需求,可以使用此处显示的每秒流数 (FPS) 计算。

计算 流收集器 存储的每秒流数(没有 Data Store 的部署)

如果部署不具有 Data Store 的 流收集器 (NetFlow),请按如下方式计算存储分配:

[(daily average FPS/1,000) x 1.6 x days]

- 确定您的 每日平均值 (FPS)
- 将此数字除以 1,000 FPS
- 将此数字乘以 1.6 GB 的存储空间,即得出一天的存储量
- 将此数字乘以 流收集器上要为总存储量存储流量的 天数

例如,如果您的系统:

- 每日平均 (FPS) 为 50,000
- 会流量存储 30 天,

按照如下方式计算每个 流收集器:

[(50,000/1,000) x 1.6 x 30] = 7200 GB (7.2 TB)

- 每日平均 FPS = 50,000
- 50,000 每日平均 FPS / 1,000 = 50
- 50 x 1.6 GB = 80 GB,一天的存储量
- 每个 流收集器 80 GB x 30 天 = 每个 流收集器 2400 GB

计算数据节点存储的每秒流数

如果部署带有 3 个 数据节点虚拟版的 Data Store 虚拟版,我们建议为每个 数据节点计算存储分配,如下所示:

[[(每日平均 FPS/1,000) x 1.6 x 天] / 数据节点 的数量

- 确定您的 每日平均值 (FPS)
- 将此数字除以 1,000 FPS
- 将此数字乘以 1.6 GB 的存储空间,即得出一天的存储量
- 将此数字乘以要为总 Data Store 存储量存储流量的天数
- 将此数字除以每个 数据节点 用于存储的 Data Store 中的 数据节点 数量

例如,如果您的系统:

- 每日平均 (FPS) 为 50,000
- 会流量存储 90 天,并且

- 您有 3 个 数据节点

按照如下方式计算每个 数据节点:

[(50,000/1,000) x 1.6 x 90] / 3 = 2400 GB (2.4 TB) / 数据节点

- 每日平均 FPS = 50,000
- 50,000 每日平均 FPS / 1,000 = 50
- 50 x 1.6 GB = 80 GB,一天的存储量
- 每个 Data Store 80 GB x 90 天 = 每个 Data Store 7200 GB
- 7200 GB / 3 数据节点 = 每个 数据节点 2400 GB (2.4 TB)

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 Cisco 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	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

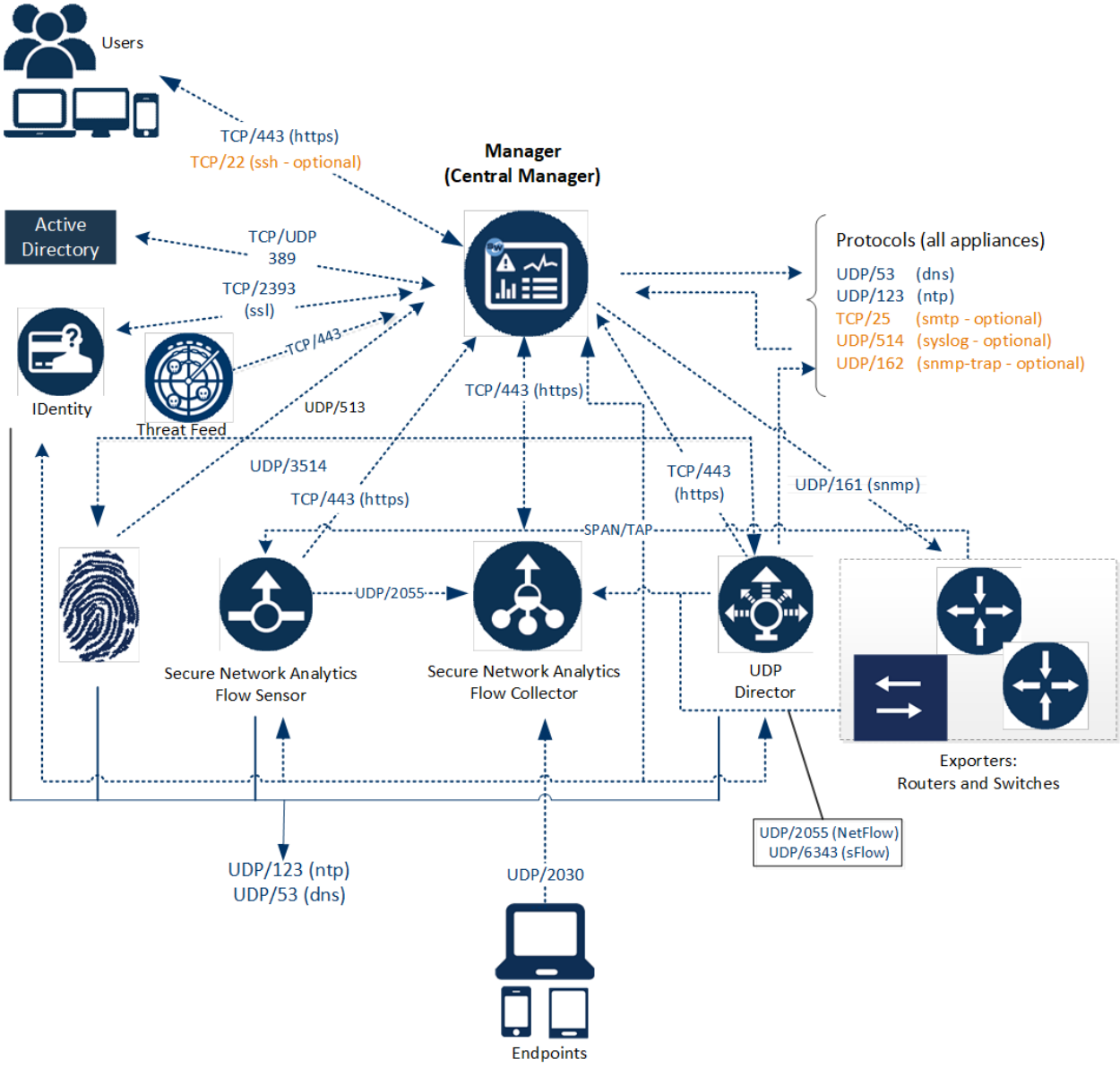
可选通信端口

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

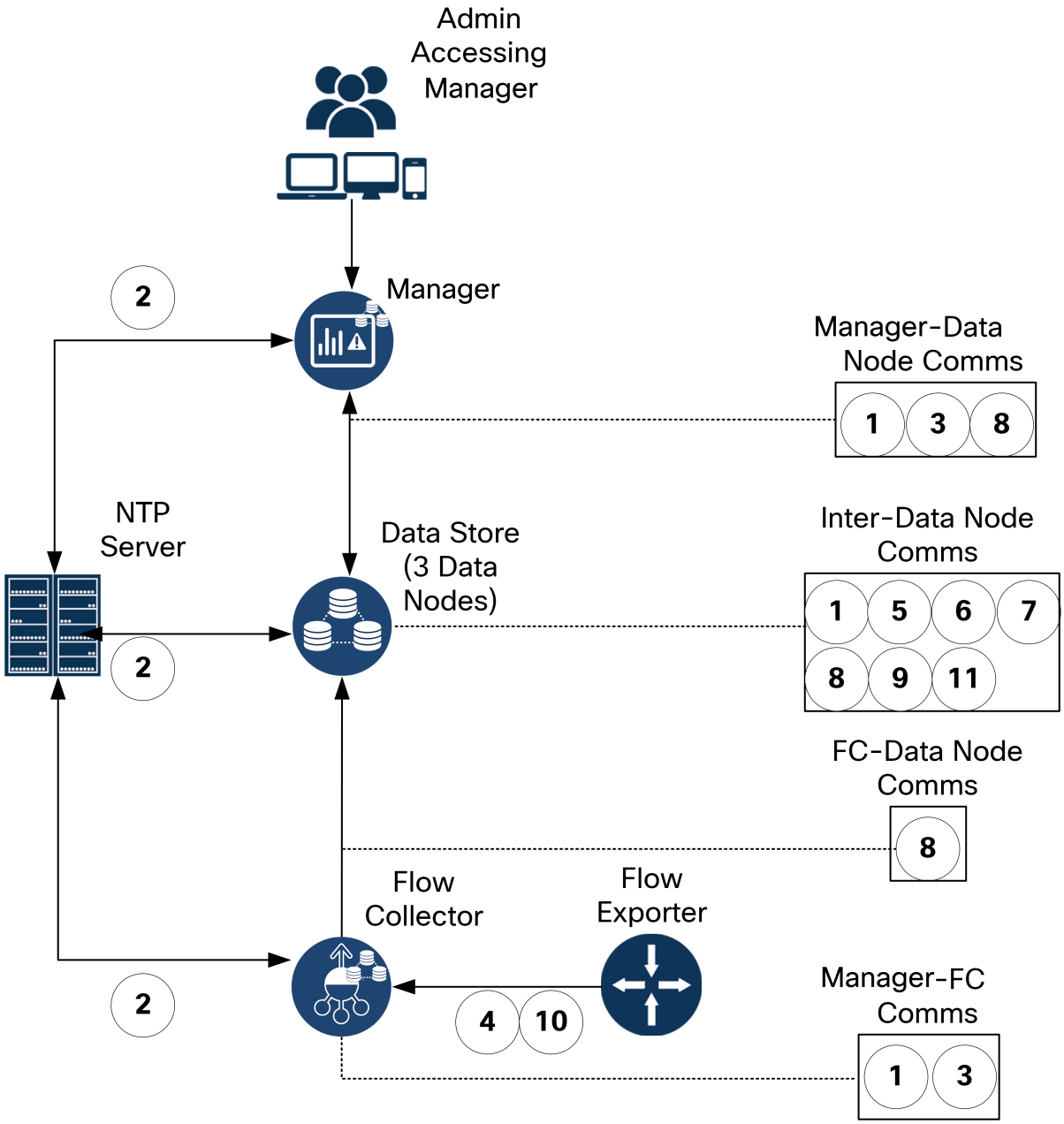
Cisco Secure Network Analytics 部署示例

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



Cisco 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 Cisco 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. 下载虚拟版安装文件

按照以下说明为您的虚拟设备安装下载 ISO 文件。

安装文件

虚拟机	设备安装文件	详细信息
3a. VMware vCenter	ISO	使用 VMware vCenter 安装虚拟设备。
3b. VMware ESXi 独立服务器	ISO	在 ESXi 独立主机服务器上安装虚拟设备。
3c. KVM 和虚拟机管理器	ISO	使用 KVM 和虚拟机管理器安装虚拟设备。

1. 登录思科软件中心

1. 登录思科软件中心 https://software.cisco.com。
2. 在 **下载和管理 > 下载和升级** 部分，选择 **访问下载**。
3. 向下滚动，直到您看到**选择产品 (Select a Product)** 字段。
4. 可通过以下两种方式访问 Cisco Secure Network Analytics 文件：
   - **按名称搜索：**在 **选择产品字段**中键入 **Cisco Secure Network Analytics** 。按下 Enter 键。
   - **按菜单搜索：**点击“浏览全部”(Browse All)。选择 **安全 > 网络可见性和分段 > 安全分析(Stealthwatch)**。

2. 下载文件

1. 选择设备类型。
    - Cisco Secure Network Analytics 虚拟 管理器
    - Cisco Secure Network Analytics 虚拟 流收集器
    - Cisco Secure Network Analytics 虚拟 流传感器
    - Cisco Secure Network Analytics 虚拟 UDP 导向器
    - Cisco Secure Network Analytics 虚拟 Data Store
2. 选择 **Cisco Secure Network Analytics 系统软件**。
3. 在“最新版本”列中，选择 **7.4.2**（或您正在安装的 7.4.x 版本）。
4. **下载：**找到 ISO 安装文件。点击**下载 (Download)** 图标或**添加到购物车 (Add to Cart)** 图标。
5. 重复这些说明，以便下载每种设备类型的文件。

3a. 使用 VMware vCenter 安装虚拟设备 (ISO)

概述

按照以下说明使用 **VMware vCenter** 安装虚拟设备。要使用替代方法，请参阅以下内容：

- **VMware ESXi 独立服务器：**使用 **3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO)**。
- **KVM：**使用 **3c. 在 KVM 主机上安装虚拟设备 (ISO)**。

> Cisco Secure Network Analytics v7.4.2 与 VMware 7.0 或 8.0 兼容。Cisco Secure Network Analytics v7.4.x 不支持 VMware 6.0、6.5 或 6.7。有关详细信息，请参阅 vSphere 6.0、6.5 和 6.7 一般支持终止的 VMware 文档。

准备工作

在开始安装之前，请完成以下准备程序：

1. **兼容性：**查看 **兼容性**中的兼容性要求。
2. **资源要求：**查看 **资源要求**部分，以便确定设备所需的分配。您可以使用资源池或其他方法来分配资源。
3. **防火墙：**为通信配置防火墙。请参阅 **1. 为通信配置 防火墙**。
4. **文件：**下载设备 ISO 文件。请参阅 **2. 下载虚拟版安装文件** 以了解有关说明。
5. **时间：**确认您的 VMware 环境（您将在其中安装虚拟设备）的虚拟机监控程序主机上设置的时间显示了正确的时间。否则，虚拟设备可能无法启动。

> ⚠ 请勿在与 Cisco Secure Network Analytics 设备相同的物理集群/系统上安装不受信任的物理或虚拟机。

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

使用 vCenter 安装虚拟设备 (ISO)

如果您有 VMware vCenter（或类似产品），请按照以下说明使用 ISO 安装虚拟设备。

如果要部署 数据节点或流量传感器，请确保完成所有必要的程序。

数据节点

请完成以下过程：

1. 为 数据节点 间通信配置隔离 LAN。

3. **安装虚拟设备**。安装 数据节点 虚拟设备时，还需要安装 两个网络适配器。

流传感器s

请完成以下过程：

2. **配置 流传感器 以监控流量**
3. **安装虚拟设备**
4. **定义其他监控端口(仅限流传感器)**

所有其他设备

如果设备不是 数据节点 或 流传感器，请完成以下程序：

3. **安装虚拟设备**

> 一些菜单和图形可能与此处所示信息不同。有关此软件的详细信息，请参阅您的 VMware 指南。

1. 为 数据节点 间通信配置隔离 LAN

如果将 数据节点虚拟版 部署到网络中，请使用虚拟交换机配置隔离的 LAN，以便 数据节点可以通过 **eth1** 相互通信，从而实现数据节点 间通信。

有两个选项可用于配置交换机：

- **配置 vSphere 标准交换机**
- **配置 vSphere 分布式交换机**

配置 vSphere 标准交换机

1. 登录到您的 VMware 主机环境。
2. 请按照 VMware 创建 vSphere 标准交换机文档 来配置 vSphere 标准交换机。请注意，在步骤 4 中，您需要为标准交换机选项选择虚拟机端口组。
3. 转至 **3. 安装虚拟设备**。

配置 vSphere 分布式交换机

1. 登录到您的 VMware 主机环境。
2. 按照 VMware 创建 vSphere 分布式交换机 文档配置 vSphere 分布式交换机。请注意，对于步骤 5a 中的上行链路数量，要求至少有 1 个上行链路，但除非您将节点分布在多个主机上，否则无需配置上行链路。如果需要在多个主机之间分布节点，请联系 思科支持 以获取帮助。
3. 转至 **3. 安装虚拟设备**。

2. 配置 流传感器 以监控流量

流传感器 虚拟版能够提供 VMware 环境的可视性，为未启用流的区域生成流数据。作为安装在每个虚拟机监控程序主机内的虚拟设备，流传感器 虚拟版从主机 vSwitch 被动捕获以太网帧，并观察和创建包含与会话对、比特率和数据包速率相关的重要会话统计信息的流记录。

> ℹ 您需要在要监控的环境中的每个主机上安装流量传感器。

使用以下说明配置 流传感器 虚拟版以监控 vSwitch 上的流量：

- **监控有多个主机的 vSwitch**
- **监控有单个主机的 vSwitch**

使用 PCI 直通监控外部流量

您还可以使用兼容的 PCI 直通来配置 流传感器 虚拟版，以便进行直接网络监控。

- **要求：**符合 igb/ixgbe 或 e1000e 标准的 PCI 直通。
- **资源信息：**请参阅 **流传感器 虚拟版**。

- **集成：**请参阅 **1. 为通信配置 防火墙**。
- **说明：**要向 流传感器 虚拟版添加 PCI 网络接口，请参阅您的 VMware 文档。

监控有多个主机的 vSwitch

按照本节中的说明使用 流传感器 虚拟版来监控跨多个 VM 主机或集群的分布式 vSwitch 上的流量。

本部分仅适用于 VDS 网络。如果您的网络处于非 VDS 环境中，请转至 **监控有单个主机的 vSwitch**。

配置要求

> 您需要在要监控的环境中的每个主机上安装流量传感器。

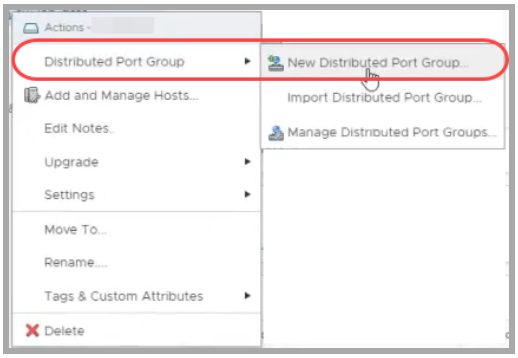
此配置具有以下要求：

- **分布式虚拟端口 (dvPort)：** 为 流传感器 虚拟版将监控的每个 VDS 添加具有正确 VLAN 设置的 dvPort 组。如果 流传感器 虚拟版会监控网络上的 VLAN 和非 VLAN 流量，则需要创建两个 dvPort 组，每种类型各一个。
- **VLAN 标识符：**如果您的环境使用 VLAN(VLAN 中继或专用 VLAN 除外)，则需要 VLAN 标识符来完成此程序。
- **混杂模式：**已启用。
- **混杂端口：**配置为 vSwitch。

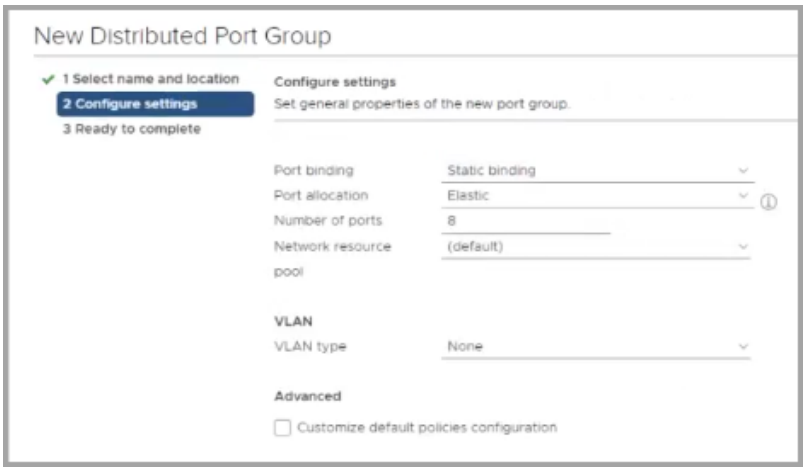
完成以下步骤以使用 VDS 来配置网络：

1. 点击**网络 (Networking)** 图标。

2. 在网络树中，右键点击 VDS。
3. 选择**分布式端口组 (Distributed Port Group)** > **新建分布式端口组 (New Distributed Port Group)**。



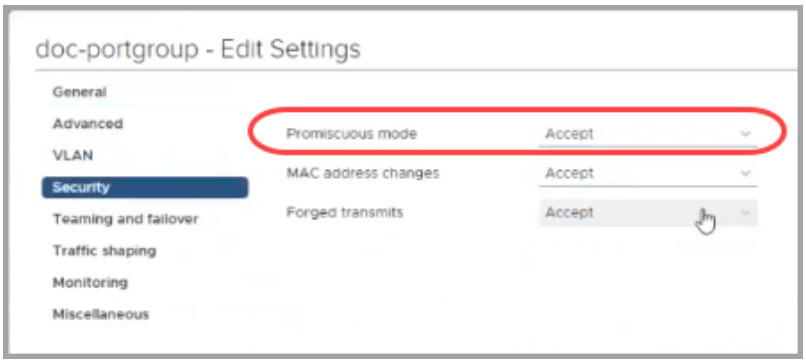
4. 使用**新建分布式端口组 (New Distributed Port Group)** 对话框来配置端口组，包括以下步骤中的规范。
5. **选择名称和位置：**在**名称 (Name)** 字段中，输入名称以标识此 dvPort 组。
6. **配置设置：**在 **端口数量** 字段中，输入主机集群中 流传感器 虚拟版的数量。



7. 点击 **VLAN 类型 (VLAN type)** 下拉列表。
   - 如果您的环境不使用 VLAN，请选择**无 (None)**。
   - 如果您的环境使用 VLAN，请选择 VLAN 类型。按照如下进行配置：

VLAN 类型 (VLAN Type)	详细信息
VLAN	在 **VLAN ID** 字段中，输入与标识符匹配的数字（介于 1 和 4094 之间）。
VLAN 中继	在 **VLAN 干线范围** 字段中，输入 **0-4094** 以监控所有 VLAN 流量。
专用 VLAN	请从下拉列表中选择**混杂 (Promiscuous)**。

8. **准备完成：**查看配置设置。点击**完成 (Finish)**。
9. 在“网络”(Networking) 树中，右键点击新的 dvPort 组。选择**编辑设置 (Edit Settings)**。
10. 选择**安全性 (Security)**。
11. 点击**混杂模式 (Promiscuous Mode)** 下拉列表。选择**接受 (Accept)**。



12. 点击**确定 (OK)** 关闭此对话框。
13. 流传感器 虚拟版是否会同时监控 VLAN 和非 VLAN 网络流量?
    - 如果是，请重复 **监控有多个主机的 vSwitch**部分中的步骤。
    - 如果不需要，则转至下一步。
14. 流传感器 虚拟版是否会监控 VMware 环境中的另一个 VDS?
    - 如果是，请为下一个 VDS 重复 **监控有多个主机的 vSwitch** 部分中的步骤。
15. 转至 **3. 安装虚拟设备**。

监控有单个主机的 vSwitch

按照本节中的说明使用 流传感器 虚拟版来监控有单个主机的 vSwitch 上的流量。

> 本部分仅适用于非 VDS 网络。如果您的网络使用 VDS，请转至 **监控有多个主机的 vSwitch**。

配置要求

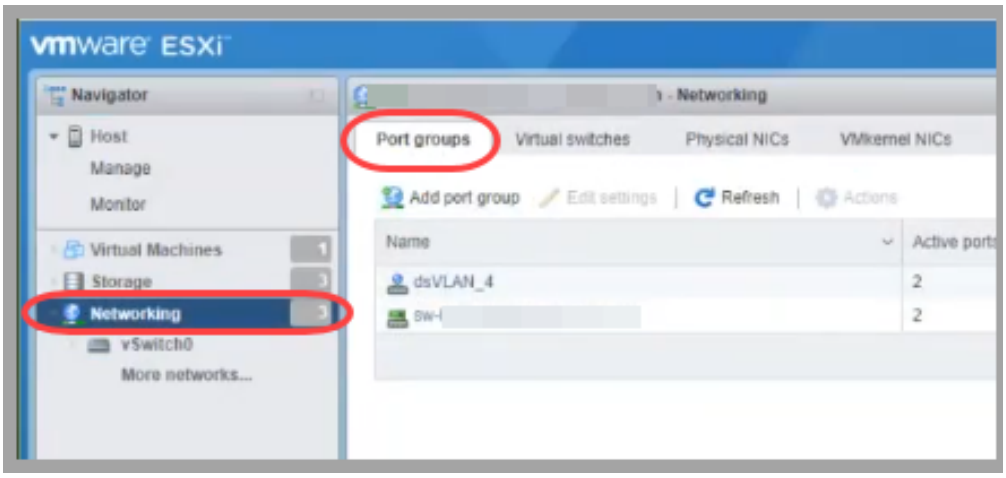
此配置具有以下要求：

- **混杂端口组：**为 流传感器 虚拟版将监控的每个虚拟交换机添加混杂端口组。
- **混杂模式：**已启用。
- **混杂端口：**配置为 vSwitch。

将端口组配置为混杂模式

按照以下说明添加端口组或编辑端口组，并将其设置为“混杂”(Promiscuous)。

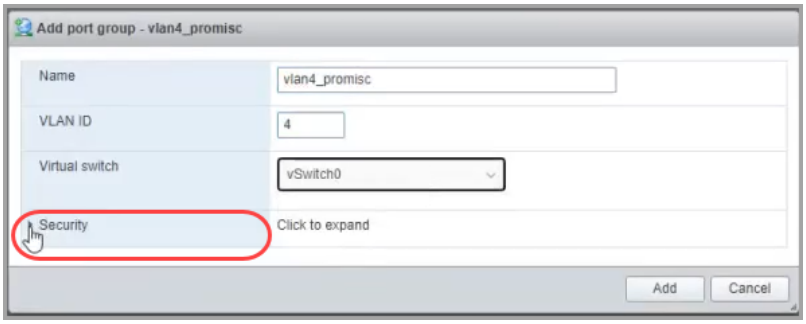
1. 登录到您的 VMware ESXi 主机环境。
2. 点击**网络 (Networking)**。



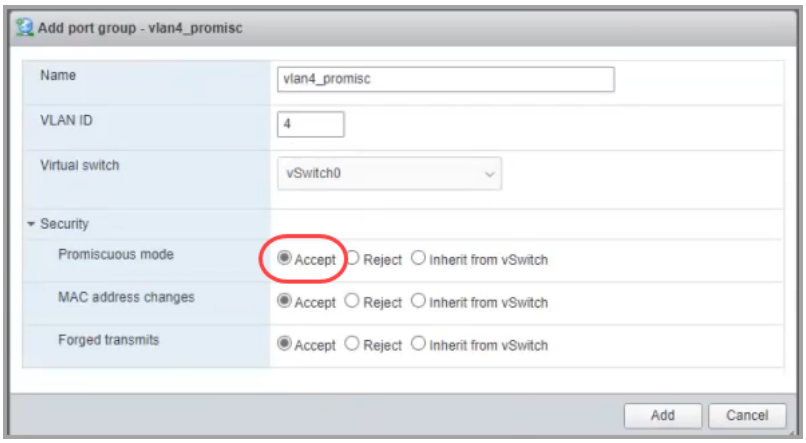
3. 选择**端口组 (Port groups)** 选项卡。
4. 您可以创建新的端口组或编辑端口组。
   - **创建端口组：**点击**添加端口组 (Add port group)**。
   - **编辑端口组：**选择端口组。点击**编辑设置 (Edit Settings)**。
5. 使用对话框来配置端口组。配置 VLAN ID 或 VLAN 中继：

VLAN 类型 (VLAN Type)	详细信息
VLAN ID	使用 VLAN ID 来指定单个 VLAN。 在 **VLAN ID** 字段中，输入与标识符匹配的数字(介于 1 和 4094 之间)。
VLAN 中继	使用 VLAN 中继来监控所有 VLAN 流量。范围默认为 0-4095。

6. 点击**安全性 (Security)** 箭头。



7. **混杂模式**：选择**接受 (Accept)**。



8. 流传感器 虚拟版是否会监控此 VMware 环境中的另一台虚拟交换机？

   如果是，请返回 **2. 配置 流传感器 以监控流量**，并对下一台虚拟交换机重复所有步骤。

9. 转至 **3. 安装虚拟设备**

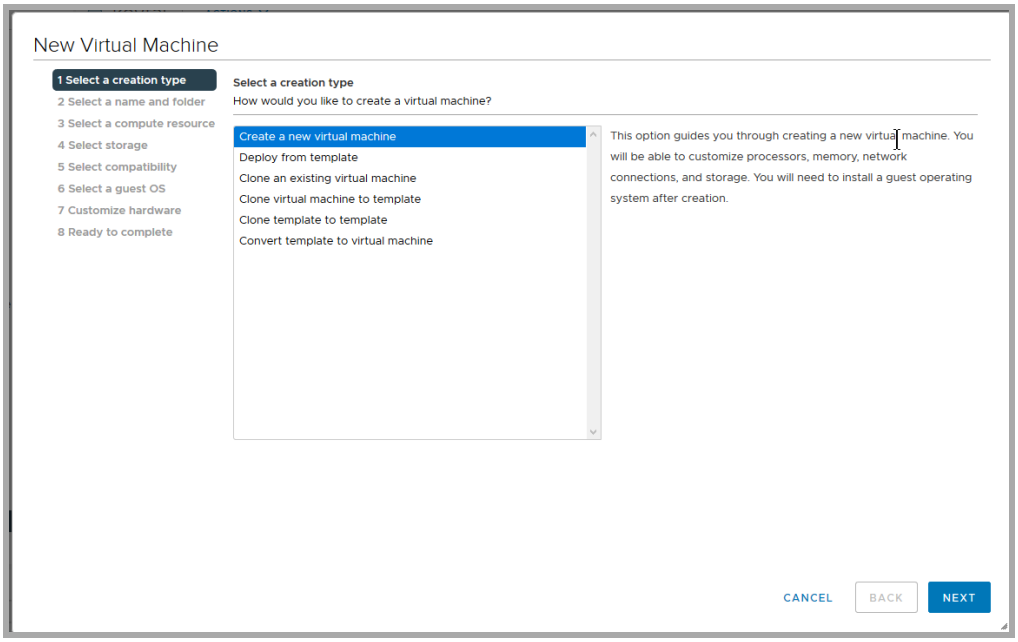
3. 安装虚拟设备

按照以下说明在虚拟机监控程序主机上安装虚拟设备，并定义虚拟设备管理和监控端口。

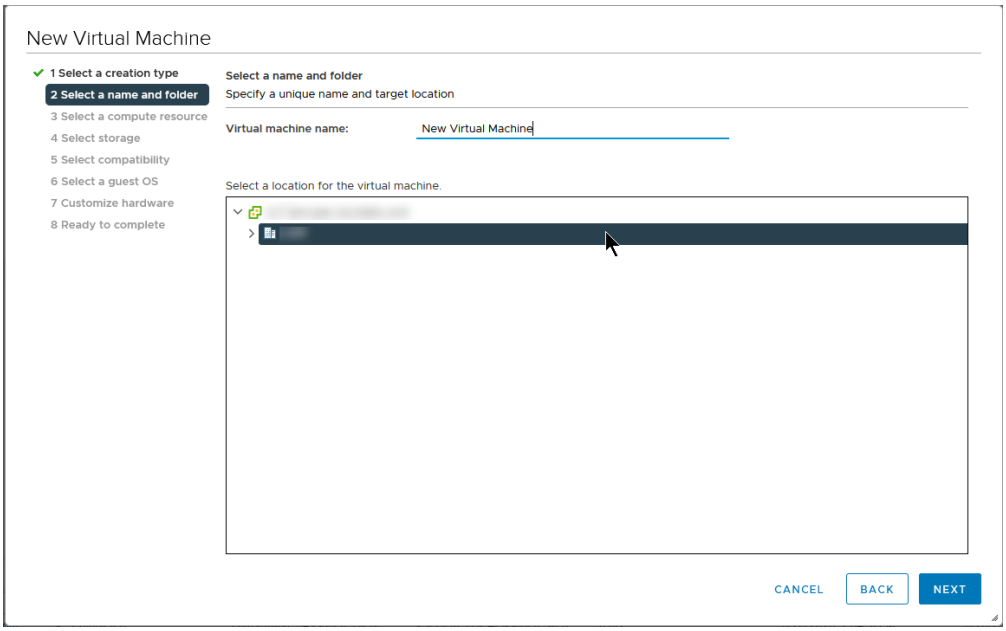
> 一些菜单和图形可能与此处所示信息不同。有关此软件的详细信息，请参阅您的 VMware 指南。

1. 登录 VMware Web 客户端。
2. 找到您从思科软件中心下载的虚拟设备软件文件 (ISO)。
3. 使 ISO 在 vCenter 中可用。您有以下选择：
   - 将 ISO 上传到 vCenter 数据存储。
   - 将 ISO 添加到内容库。
   - 将 ISO 保留在本地工作站上，然后配置部署以引用该文件。

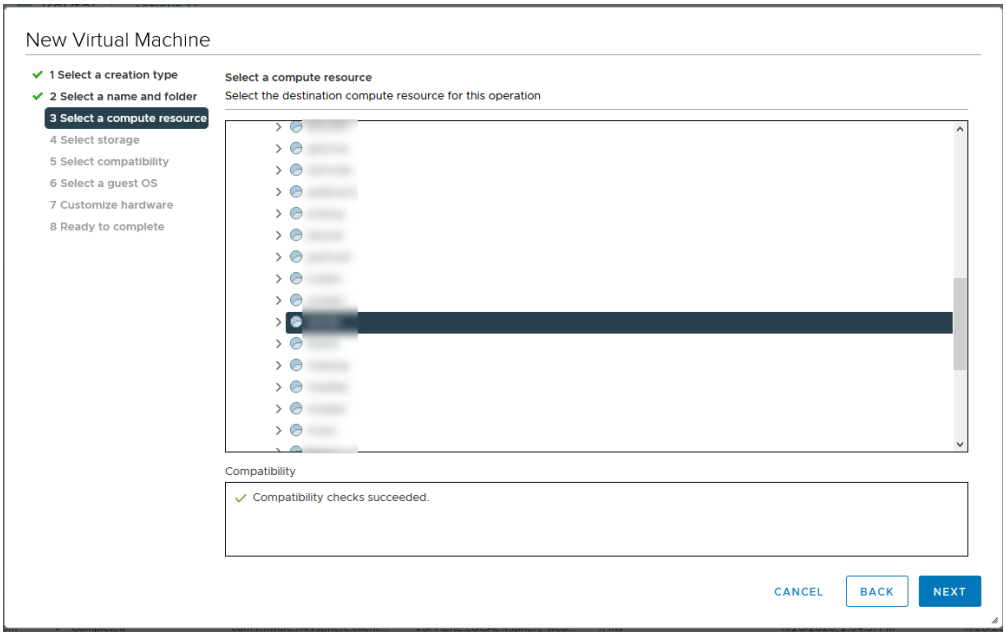
   请参阅 VMware 文档中的详细信息。
4. 在 vCenter UI 中，选择**选择 (Menu) > 主机和集群 (Hosts and Clusters)**。
5. 在导航窗格中，右键点击集群或主机，然后选择**新建虚拟机... (New Virtual Machine...)** 以访问“新建虚拟机”(New Virtual Machine) 向导。
6. 从“选择创建类型”(Select a creation type) 窗口中，选择**创建新虚拟机 (Create a new virtual machine)**，然后点击**下一步 (Next)**。



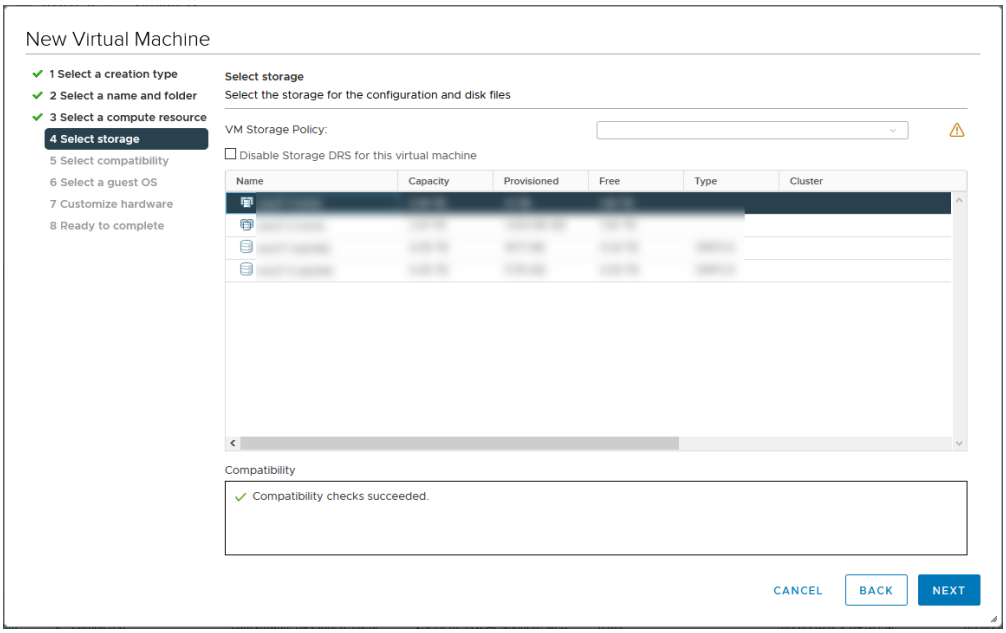
7. 从“选择名称和文件夹”(Select a name and folder) 窗口中，输入**虚拟机名称 (Virtual machine name)**，**选择虚拟机的位置**，然后点击**下一步 (Next)**。



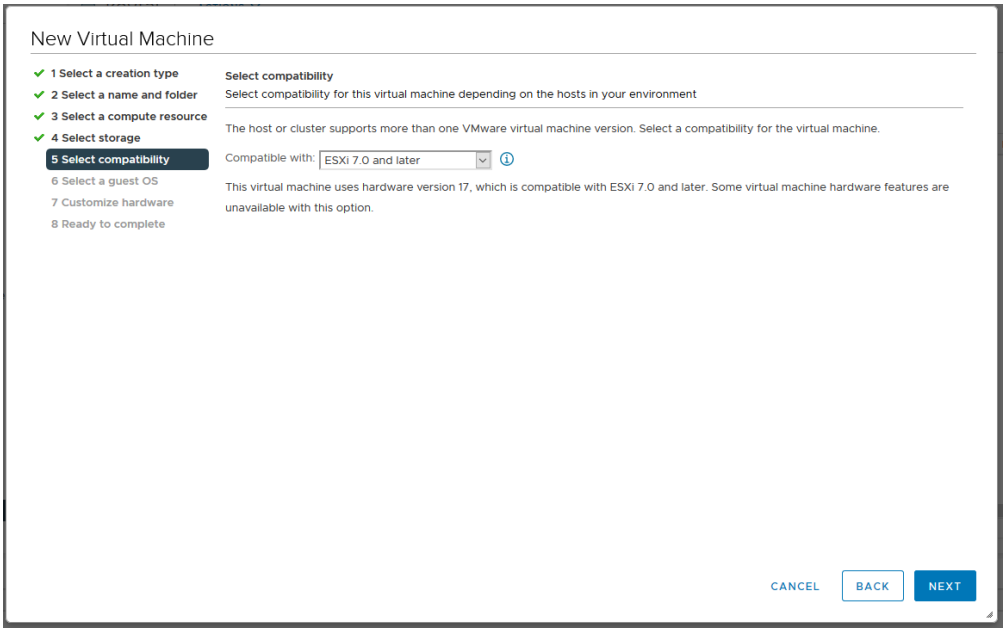
8. 从“选择计算资源”(Select a compute resource) 窗口中，选择要将设备部署到的集群、主机、资源池或 vApp，然后点击**下一步 (Next)**。



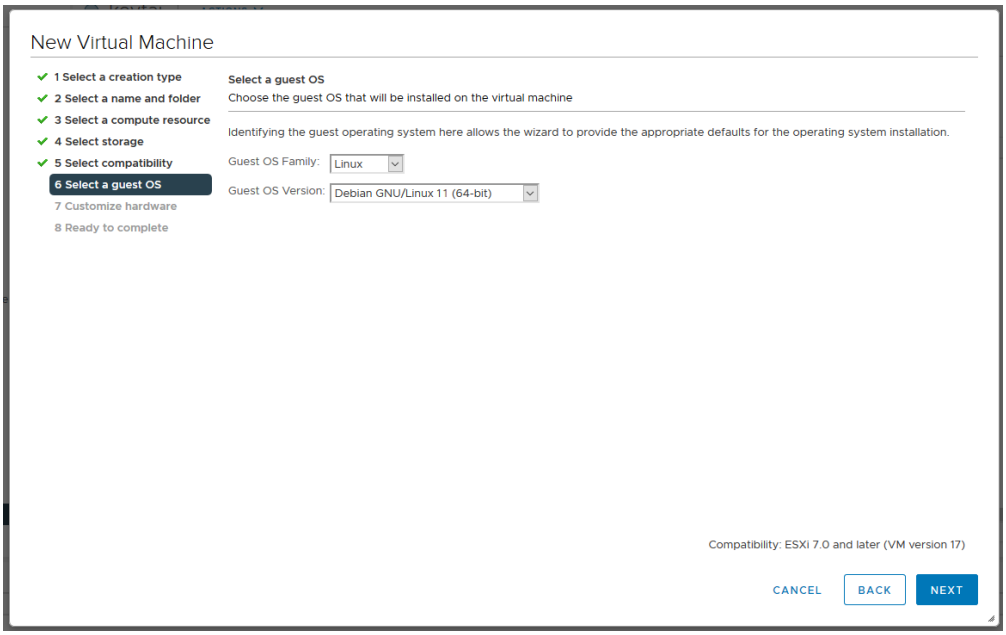
9. 从“选择存储”(Select storage) 窗口中，从下拉列表中选择 **VM 存储策略 (VM Storage Policy)**，接着选择一个存储位置，然后点击**下一步 (Next)**。



10. 在“选择兼容性”(Select compatibility) 窗口中，根据您当前部署的 ESXi 版本，从**兼容 (Compatible with)** 下拉列表中选择虚拟机版本。例如，由于 ESXi 7.0 已部署，以下屏幕截图显示了 **ESXi 7.0 及更高版本**。点击**下一步 (Next)**。

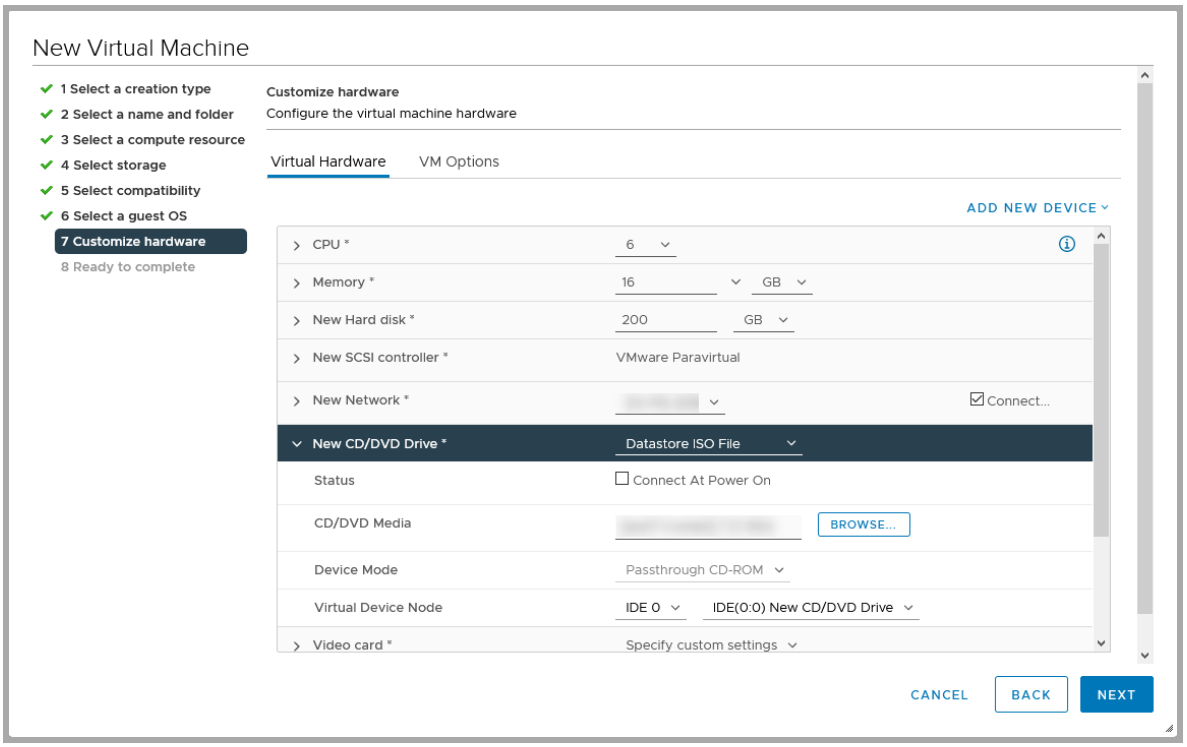


11. 从“选择访客操作系统”屏幕中，选择 **Linux 访客操作系统系列**和 **Debian GNU/Linux 11 (64-bit) 访客操作系统版本**。点击**下一步 (Next)**。



12. 在“自定义硬件”(Customize hardware) 窗口中，配置虚拟硬件。有关设备类型的具体建议，请参见 **资源要求** 。

> ⚠ 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。



除了资源要求之外，请确保选择以下设置：

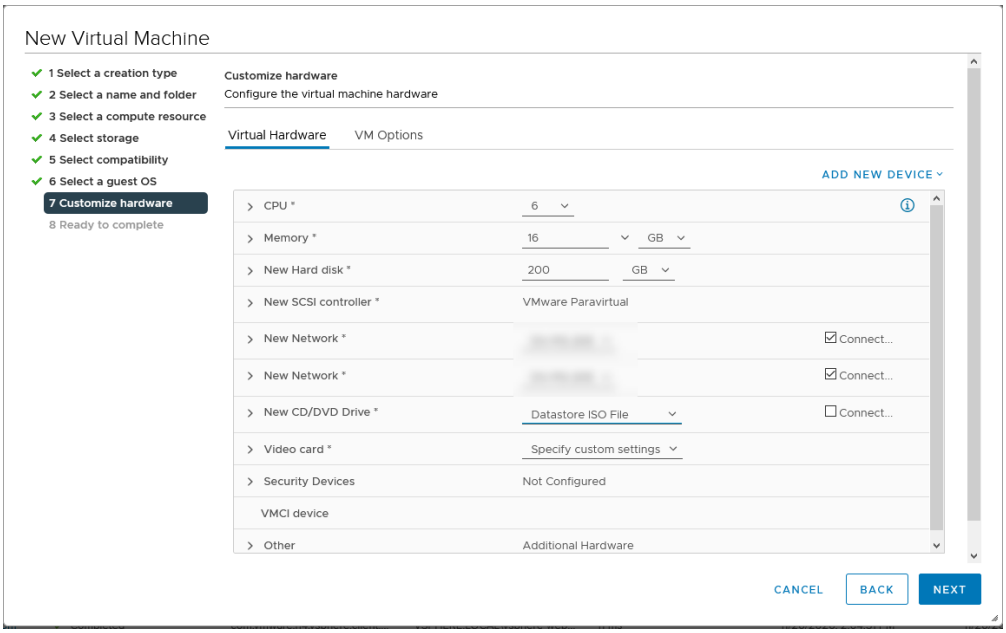
- 点击**新建硬盘 (New Hard disk)** 以展开配置选项。从**磁盘调配 (Disk Provisioning)** 下拉列表中选择**密集调配延迟归零 (Thick Provision Lazy Zeroed)**。
- 点击**新建 SCSI 控制器 (New SCSI controller)** 以展开配置选项。从**更改类型 (Change Type)**下拉列表中选择 **LSI 逻辑 SAS (LSI Logic SAS)**。如果不选择 **LSI 逻辑 SAS (LSI Logic SAS)**，您的虚拟设备可能无法正确部署。
- 在**新建 CD/DVD 驱动器 (New CD/DVD Drive)** 字段中，根据存储 ISO 的位置选择 ISO 位置。点击**新建 CD/DVD 驱动器 (New CD/DVD Drive)** 以展开配置选项。选中**启动时连接 (Connect At Power On)**。
- **如果设备是 流传感器，**并且您正在为网卡配置 10 Gbps 吞吐量，请点击 **CPU** 以展开配置选项。配置所有**每插槽核心数 (Cores per Socket)**，以便让所有 CPU 都位于一个插槽中。

13. **数据节点：**如果要部署 数据节点 虚拟设备，请另外添加一个网络适配器。

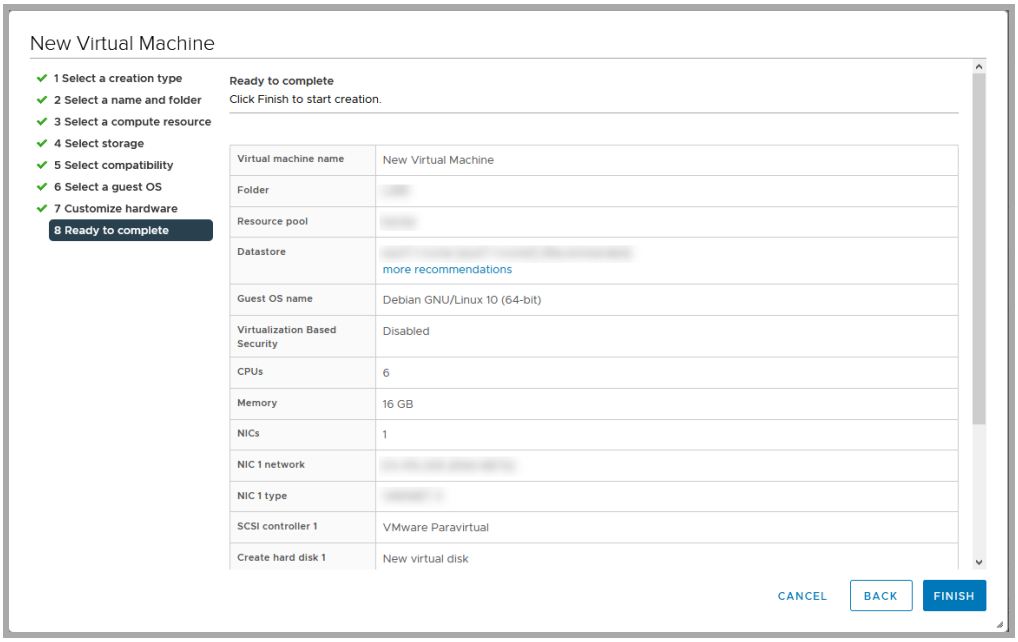
点击 **添加新设备**，然后选择 **网络适配器** 并确保适配器类型为 **VMXNET3**。

- 对于 **第一个网络适配器，**请选择允许 数据节点 虚拟版 在公共网络上与其他设备通信的交换机。
- 对于 **第二个网络适配器，**请选择您在 **1. 为 数据节点 间通信配置隔离 LAN** 这将允许 数据节点 虚拟版 在专用网络上与其他 数据节点通信。

> 确保在部署每个 数据节点 时为部署中的每个 数据节点 正确分配网络适配器和虚拟交换机。



14. 在准备完成窗口中查看您的设置，然后点击**完成 (Finish)**。



15. 当您点击 **电源** 图标时，部署开始。在**最近的任务 (Recent Tasks)** 部分中监控部署进度。在继续后续步骤之前，请确保部署已完成并显示在库存树中。
16. 后续步骤：

- **流量传感器：**如果设备是 流传感器，并且将监控 VMware 环境中的多个虚拟交换机或集群中的多个 VDS，请继续下一节的第 **4. 定义其他监控端口(仅限流传感器)**。

- **所有其他设备：**重复本节中的所有程序 **3. 安装虚拟设备** 以部署另一个虚拟设备。

17. 如果您已完成系统中所有虚拟设备的安装，请转至 **4. 配置您的 Cisco Secure Network Analytics 系统** 。

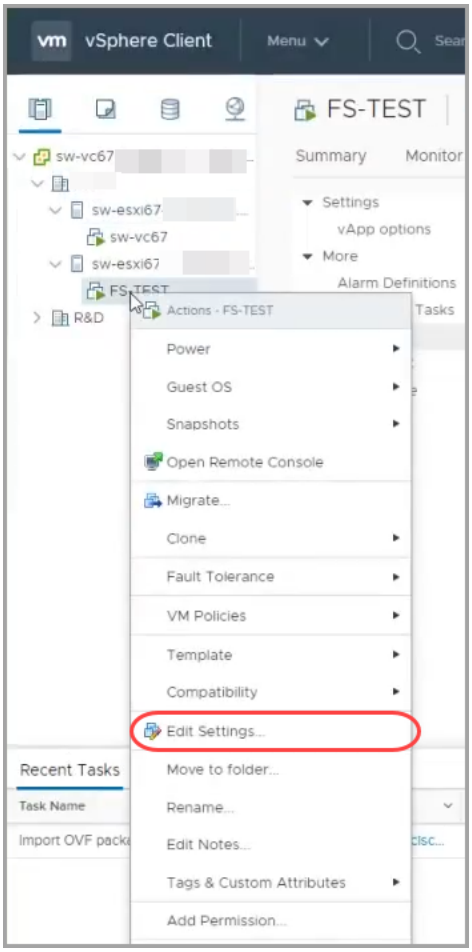
4. 定义其他监控端口(仅限流传感器)

如果 流传感器 虚拟版将监控 VMware 环境中的多个虚拟交换机或集群中的多个 VDS，则需要执行此程序。

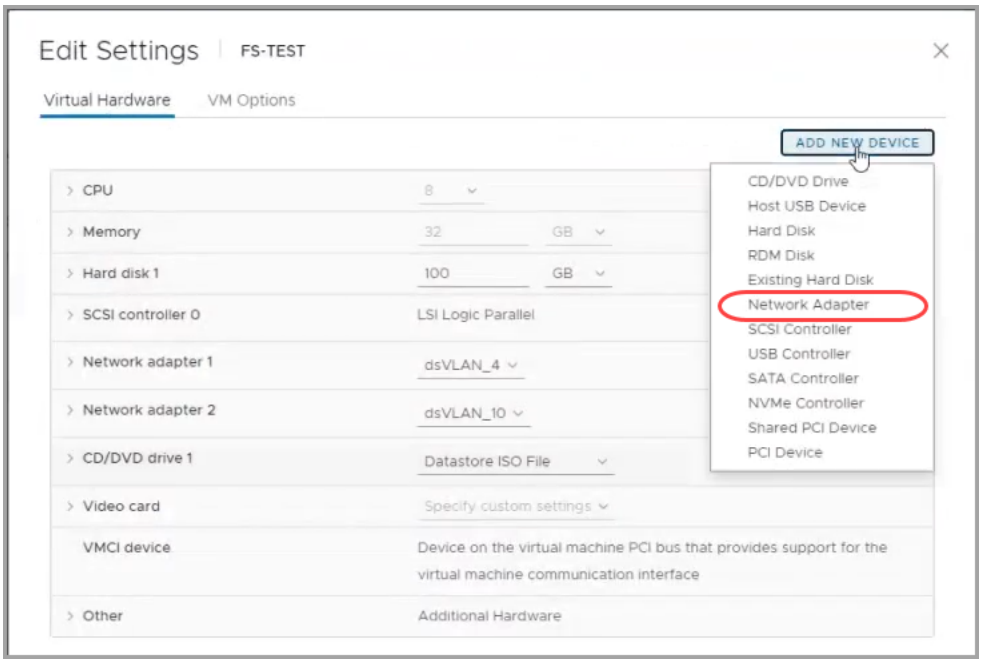
> 如果这不是 流传感器的监控配置，则无需完成此程序。

要添加 流传感器 虚拟版监控端口，请完成以下步骤：

1. 在库存树中，右键点击 流传感器 虚拟版。选择**编辑设置 (Edit Settings)**。

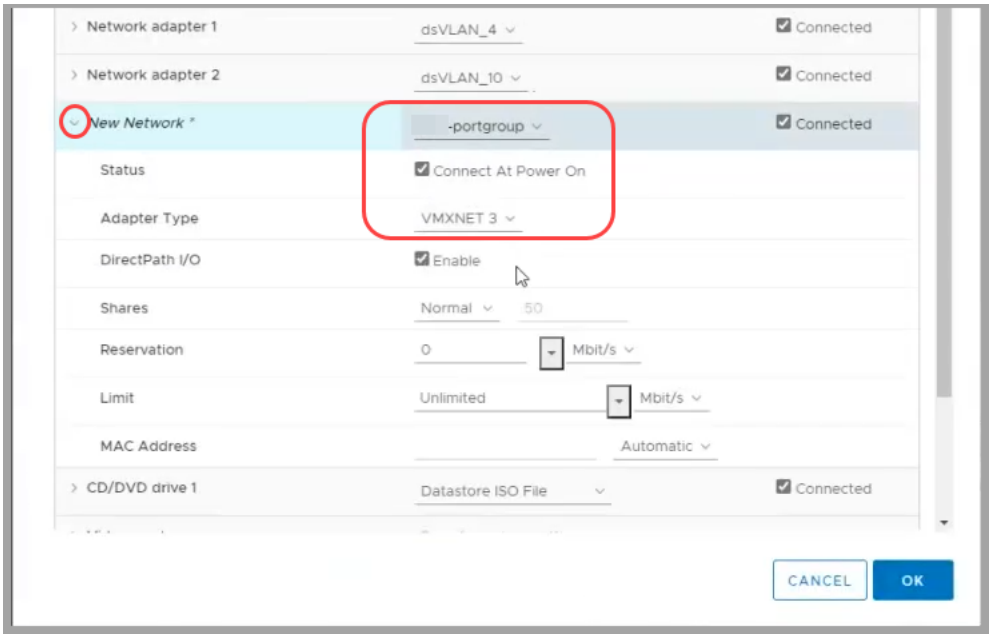


2. 使用**编辑设置 (Edit Settings)** 对话框来配置以下指定设置。
3. 点击**添加新设备 (Add New Device)**。选择**网络适配器 (Network Adapter)**。



4. 找到新的网络适配器。点击箭头以展开菜单，然后配置以下内容：

- **新建网络：**选择未分配的混杂端口组。
- **适配器类型：**选择 **VMXNET 3**。
- **状态：**选中 **启动时连接** 复选框。



5. 查看设置后，点击**确定 (OK)**。
6. 重复此程序，以便根据需要添加另一个以太网适配器。
7. 后续步骤：

- **流量传感器：**要配置其他 流传感器，请转至 **2. 配置 流传感器 以监控流量**。
- **所有其他设备：**重复本节中的所有程序 **3. 安装虚拟设备** 以部署另一个虚拟设备。
- 如果您已完成系统中所有虚拟设备的安装，请转至 **4. 配置您的 Cisco Secure Network Analytics 系统** 。

3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO)

概述

按照以下说明使用 **VMware 环境和 ESXi 独立服务器**来安装虚拟设备。

> Cisco Secure Network Analytics v7.4.2 与 VMware v7.0 或 8.0 兼容。Cisco Secure Network Analytics v7.4.x 不支持 VMware v6.0、v6.5 或 v6.7。有关详细信息，请参阅 vSphere 6.0、6.5 和 6.7 一般支持终止的 VMware 文档。

要使用替代方法，请参阅以下内容：

- **VMware vCenter：**使用 **3a. 使用 VMware vCenter 安装虚拟设备 (ISO)**。
- **KVM：**使用 **3c. 在 KVM 主机上安装虚拟设备 (ISO)**。

准备工作

在开始安装之前，请完成以下准备程序：

1. **兼容性：**查看 **兼容性**中的兼容性要求。
2. **资源要求：**查看 **资源要求**部分，以便确定设备所需的分配。您可以使用资源池或其他方法来分配资源。
3. **防火墙：**为通信配置防火墙。请参阅 **1. 为通信配置 防火墙**。
4. **文件：**下载设备 ISO 文件。请参阅 **2. 下载虚拟版安装文件** 以了解有关说明。
5. **时间：**确认您的 VMware 环境（您将在其中安装虚拟设备）的虚拟机监控程序主机上设置的时间显示了正确的时间。否则，虚拟设备可能无法启动。

> ⚠ 请勿在与 Cisco Secure Network Analytics 设备相同的物理集群/系统上安装不受信任的物理或虚拟机。

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

在 ESXi 独立服务器上安装虚拟设备 (ISO)

按照以下说明使用 **VMware 环境和 ESXi 独立服务器**来安装虚拟设备。

流程概述

安装虚拟设备需要完成本章介绍的以下程序：

1. 登录到 VMware Web 客户端

2. 从 ISO 启动

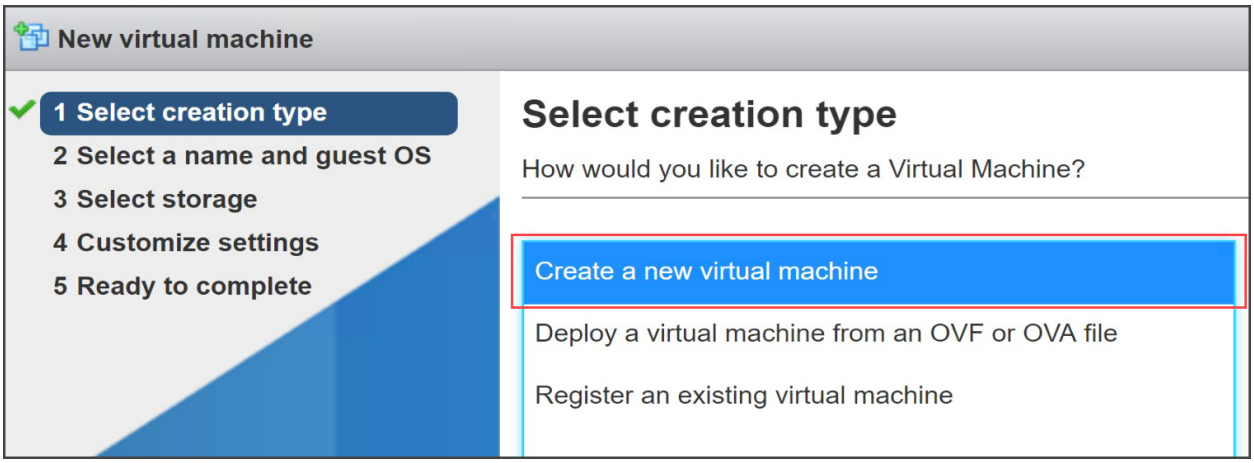
数据节点

如果要部署数据节点，请按照上一部分中的说明进行操作 **1. 为 数据节点 间通信配置隔离 LAN**。

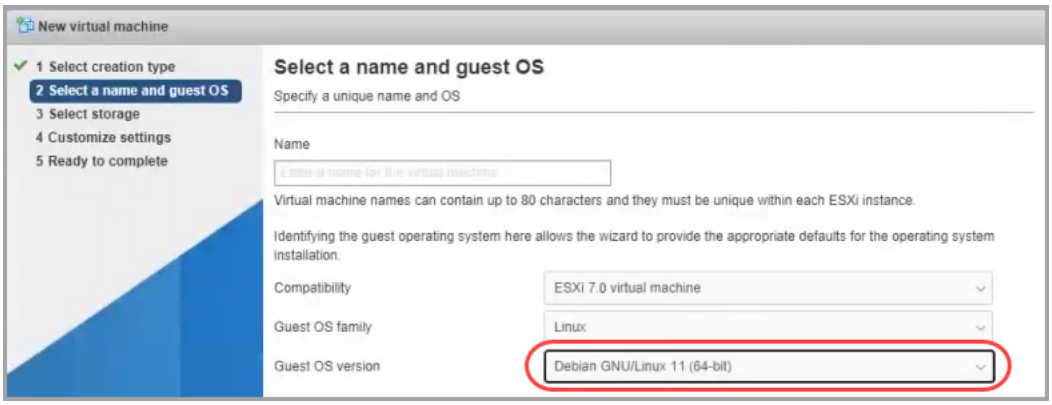
1. 登录到 VMware Web 客户端

> 一些菜单和图形可能与此处所示信息不同。有关此软件的详细信息，请参阅您的 VMware 指南。

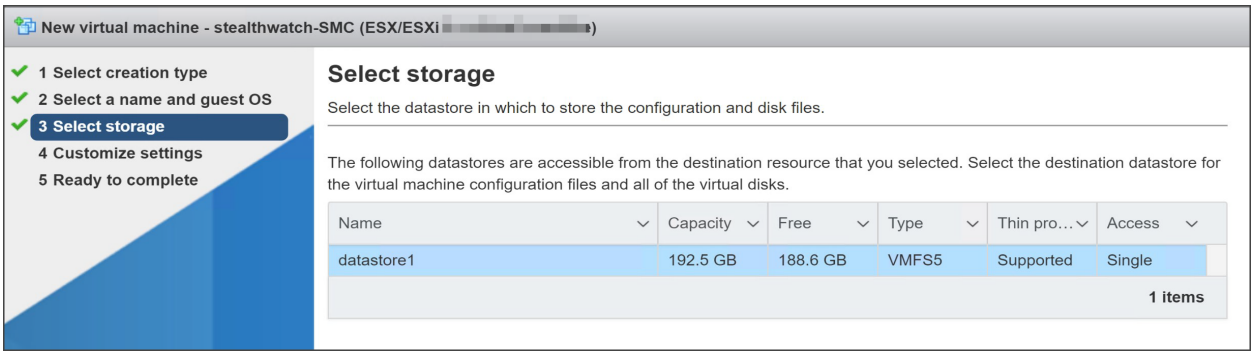
1. 登录到 VMware Web 客户端。
2. 点击**创建/注册虚拟机 (Create/Register a Virtual Machine)**。
3. 使用**新建虚拟机 (New Virtual Machine)** 对话框按照以下步骤中指定的方法来配置设备。
4. **选择创建类型：**选择**创建新虚拟机 (Create a New Virtual Machine)**。



5. **选择名称和访客操作系统：**输入或选择以下选项：
   - **名称：**为设备输入一个名称，以便您能够轻松识别。
   - **兼容性：**选择您使用 (v7.0 或 8.0) 的版本。
   - **访客操作系统系列：**Linux。
   - **访客操作系统版本：**选择 **Debian GNU/Linux 11 64-bit**。



6. **选择存储:**选择可访问的数据存储。查看资源要求以确认您有足够的空间。



> 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。

7. **自定义设置:**输入或选择设备要求(有关详细信息，请参阅资源要求)。

   确保选择以下选项:

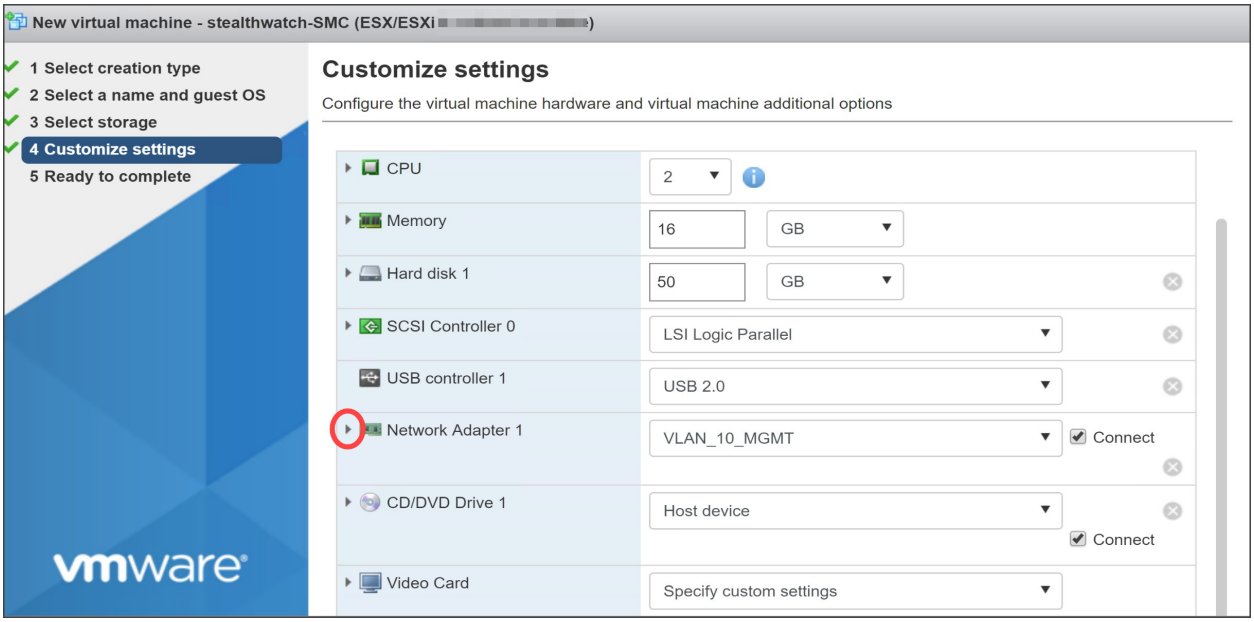
   - **SCSI 控制器:**LSI 逻辑 SAS
   - **网络适配器:**确认设备的管理地址。
   - **硬盘:**密集调配延迟归零

   如果设备是 流传感器，则可以点击 **添加网络适配器** 以添加其他管理或感应接口。

   如果设备是 流传感器，并且您正在为网卡配置 10 Gbps 吞吐量，请点击 **CPU** 以展开配置选项。在一个插槽中配置所有 CPU。

   如果设备是数据节点，则必须添加另一个网络接口以允许数据节点 间通信。点击**添加网络适配器 (Add Network Adapter)**。

- 对于 **第一个网络适配器**，请选择允许 数据节点 虚拟版 在公共网络上与其他设备通信的交换机。
- 对于 **第二个网络适配器**，请选择您在 **1. 为 数据节点 间通信配置隔离 LAN** 这将允许 数据节点 虚拟版 在专用网络上与其他 数据节点通信。



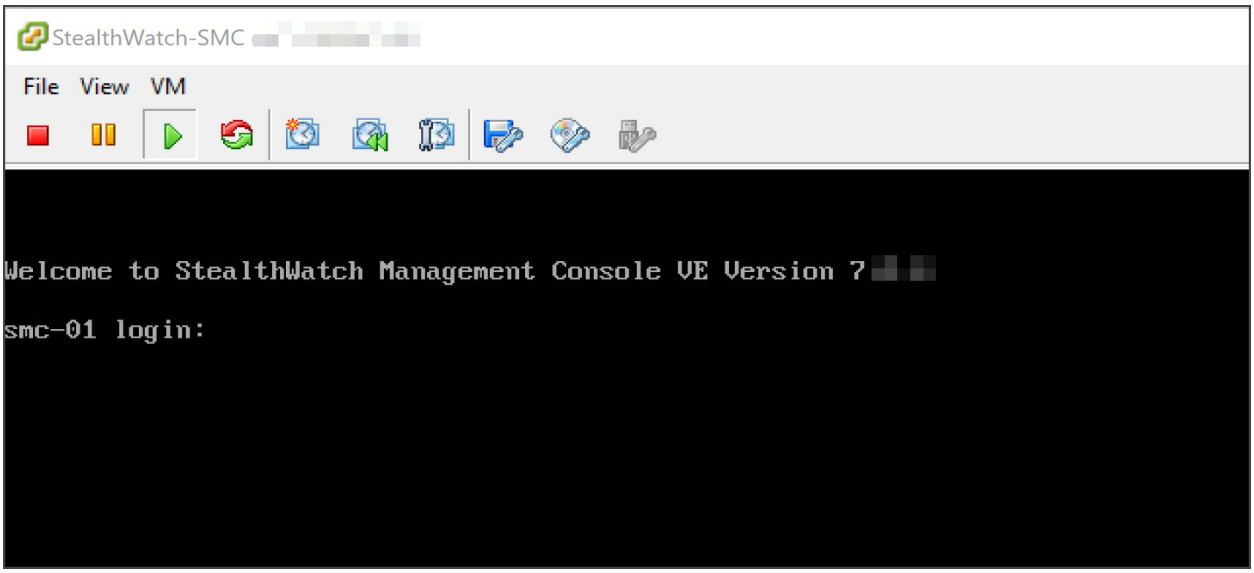
8. 点击“网络适配器”(Network Adapter) 旁边的箭头。
9. 对于适配器类型，选择 **VMXnet3**。

> 虽然思科支持使用 E1000 (1G dvSwitch)、1G PCI 直通和 VMXNET 3 接口，但思科强烈建议您使用 VMXNET3 接口，因为它已被证明可为思科虚拟设备提供最佳网络性能。

10. 查看您的配置设置并确认它们正确无误。
11. 点击**完成 (Finish)**。系统会创建一个虚拟机容器。

2. 从 ISO 启动

1. 打开 VMware 控制台。
2. 将 ISO 连接到新的虚拟机。有关详情，请参阅 VMware 指南。
3. 从 ISO 启动虚拟机。它会运行安装程序并自动重启。
4. 安装和重新启动完成后，您将看到登录提示。



5. 断开 ISO 与虚拟机的连接。
6. 对下一台虚拟设备重复 **3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO)** 中的所有程序。
7. **流传感器:** 如果设备是 流传感器, 使用本手册前面的部分完成设置:
   - **2. 配置 流传感器 以监控流量**(使用通过单主机监控 vSwitch)
   - 如果 流传感器 将监控 VMware 环境中的多个虚拟交换机或集群中的多个 VDS, 请转至 **4. 定义其他监控端口(仅限流传感器)**。
8. 如果您已完成系统中所有虚拟设备的安装, 请转至 **4. 配置您的 Cisco Secure Network Analytics 系统** 。

3c. 在 KVM 主机上安装虚拟设备 (ISO)

概述

按照以下说明**使用 KVM 和虚拟机管理器**来安装虚拟设备。

要使用替代方法，请参阅以下内容：

- **VMware vCenter：**使用 3a. 使用 VMware vCenter 安装虚拟设备 (ISO)。
- **VMware ESXi 独立服务器：**使用 3b. 在 ESXi 独立服务器上安装虚拟设备 (ISO) 。

> Linux KVM 已在许多 KVM 主机版本上进行测试和验证。有关我们已针对 7.3.1 及更高版本 Cisco Secure Network Analytics 测试和验证的 KVM 组件的详细列表，请参阅 KVM 。

准备工作

在开始安装之前，确保完成以下程序：

1. **兼容性：**查看 兼容性中的兼容性要求。
2. **资源要求：**查看 资源要求部分，以便确定设备所需的分配。您可以使用资源池或其他方法来分配资源。
3. **防火墙：**为通信配置防火墙。请参阅 1. 为通信配置 防火墙。
4. **文件：**从下载 ISO 文件并将映像复制到 KVM 主机上的文件夹。在本节提供的示例中，我们使用以下文件夹：var/lib/libvirt/image。请参阅 2. 下载虚拟版安装文件 以了解有关说明。
5. **时间：**确认您的 VMware 环境（您将在其中安装虚拟设备）的虚拟机监控程序主机上设置的时间显示了正确的时间。否则，虚拟设备可能无法启动。

> ⚠ 请勿在与 Cisco Secure Network Analytics 设备相同的物理集群/系统上安装不受信任的物理或虚拟机。

在 KVM 主机上安装虚拟设备 (ISO)

如果您有 KVM 主机，请按照以下说明使用 ISO 来安装虚拟设备。

流程概述

安装虚拟设备需要完成本章介绍的以下程序：

为 数据节点配置隔离 LAN

1. 在 KVM 主机上安装虚拟设备

2. 在开放式 vSwitch 上添加 NIC (数据节点、流传感器) 和混杂端口监控（仅限流传感器）

为 数据节点配置隔离 LAN

如果将 数据节点虚拟版 部署到网络中，请使用虚拟交换机配置隔离的 LAN，以便 数据节点可以通过 **eth1** 相互通信，从而实现数据节点 间通信。有关创建隔离 LAN 的详细信息，请参阅虚拟交换机的文档。

1. 在 KVM 主机上安装虚拟设备

使用 ISO 文件在 KVM 主机上安装虚拟机有多种方法。以下步骤提供了一个示例，说明如何通过在 Ubuntu 机器上运行的名为虚拟机管理器的 GUI 工具来安装虚拟 管理器 。您可以使用任何兼容的 Linux 发行版。有关兼容性的详细信息，请参阅 兼容性。

监控流量

流传感器 虚拟版能够提供 KVM 环境的可视性，为未启用流的区域生成流数据。作为安装在每个 KVM 主机内的虚拟设备，流传感器 虚拟版从其观察到的流量中被动捕获以太网帧，并创建包含与会话对、比特率和数据包速率相关的重要会话统计信息的流记录。

配置要求

此配置具有以下要求：

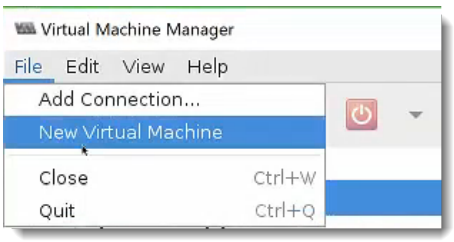
- **混杂模式：**已启用。
- **混杂端口：**配置为开放式 vSwitch。

> 我们建议您使用 virt-manager 2.2.1 在 KVM 主机上安装虚拟设备。

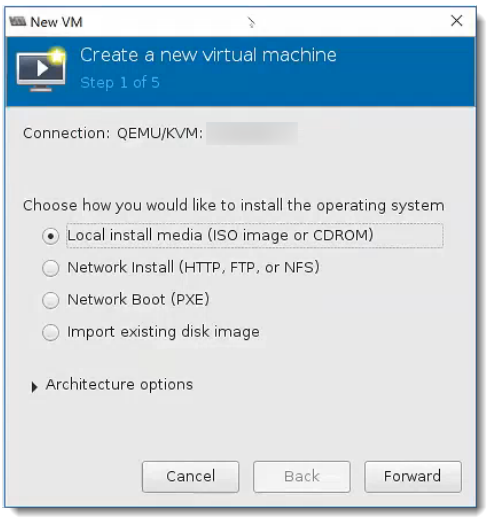
在 KVM 主机上安装虚拟设备

要安装虚拟设备并启用 流传感器 虚拟版以监控流量，请完成以下步骤：

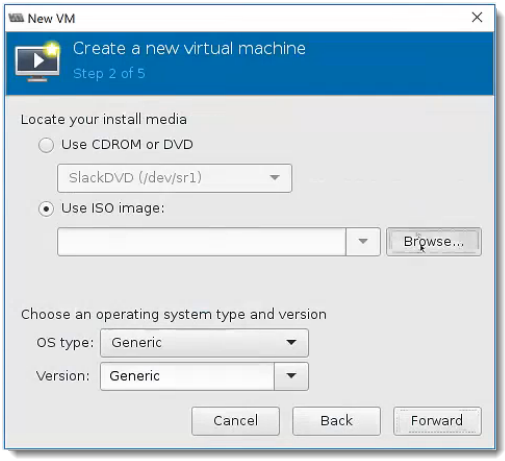
1. 使用虚拟机管理器连接到 KVM 主机，并按照以下步骤中指定的方法来配置设备。
2. 点击**文件 (File) > 新建虚拟机 (New Virtual Machine)**。



3. 选择 **QEMU/KVM** 进行连接，然后选择 **本地安装介质 (ISO 映像或 CDROM)** 。点击**继续 (Forward)**。

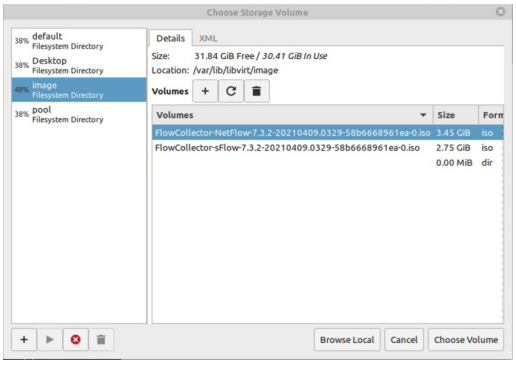


4. 点击 **浏览** 以选择设备映像文件。

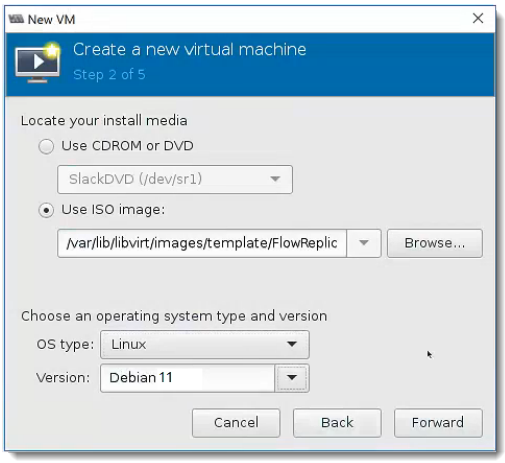


5. 选择 ISO 文件。点击**选择卷 (Choose Volume)**。

   确认 KVM 主机可访问 ISO 文件。

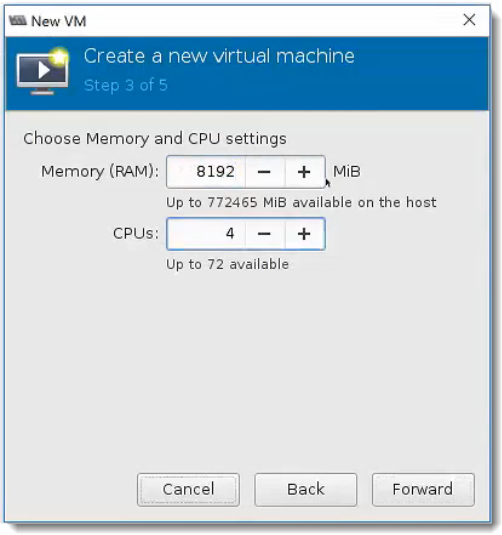


6. 取消选中“从安装介质/源自动检测”复选框。在选择操作系统类型和版本下，开始键入“Debian”，然后选择显示的 **Debian 11 (debian 11)** 选项。点击**继续 (Forward)**。

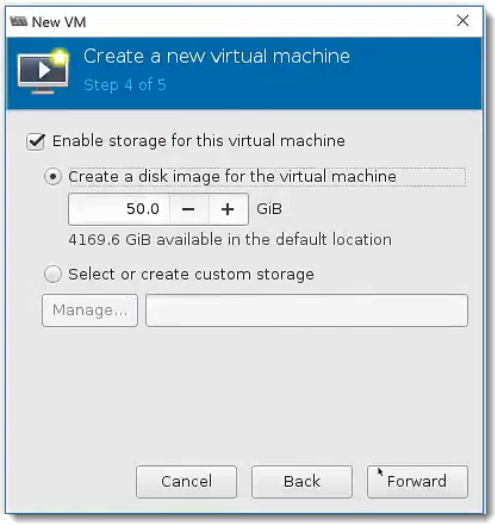


7. 将内存 (RAM) 和 CPU 数量增加到 **资源要求** 部分中所示的数量。

> 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。



8. 选择**创建用于虚拟机的磁盘映像 (Create a disk image for the virtual machine)**。
9. 输入在 **资源要求** 部分中所示的设备数据存储量。点击**继续 (Forward)**。

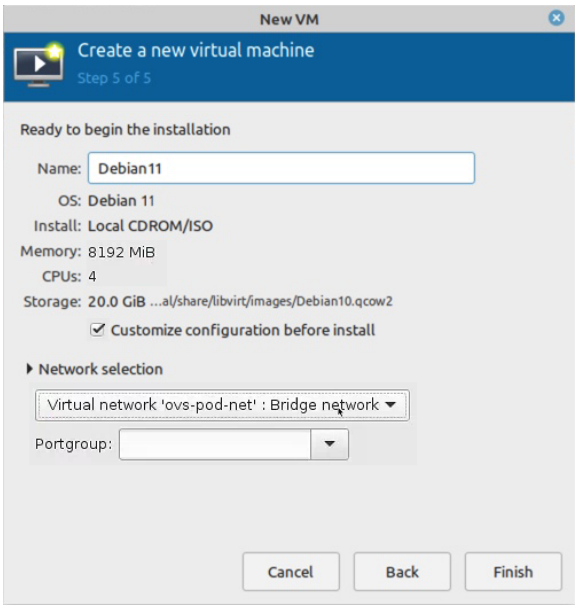


查看资源要求以分配足够多的资源。这一步对于系统性能至关重要。

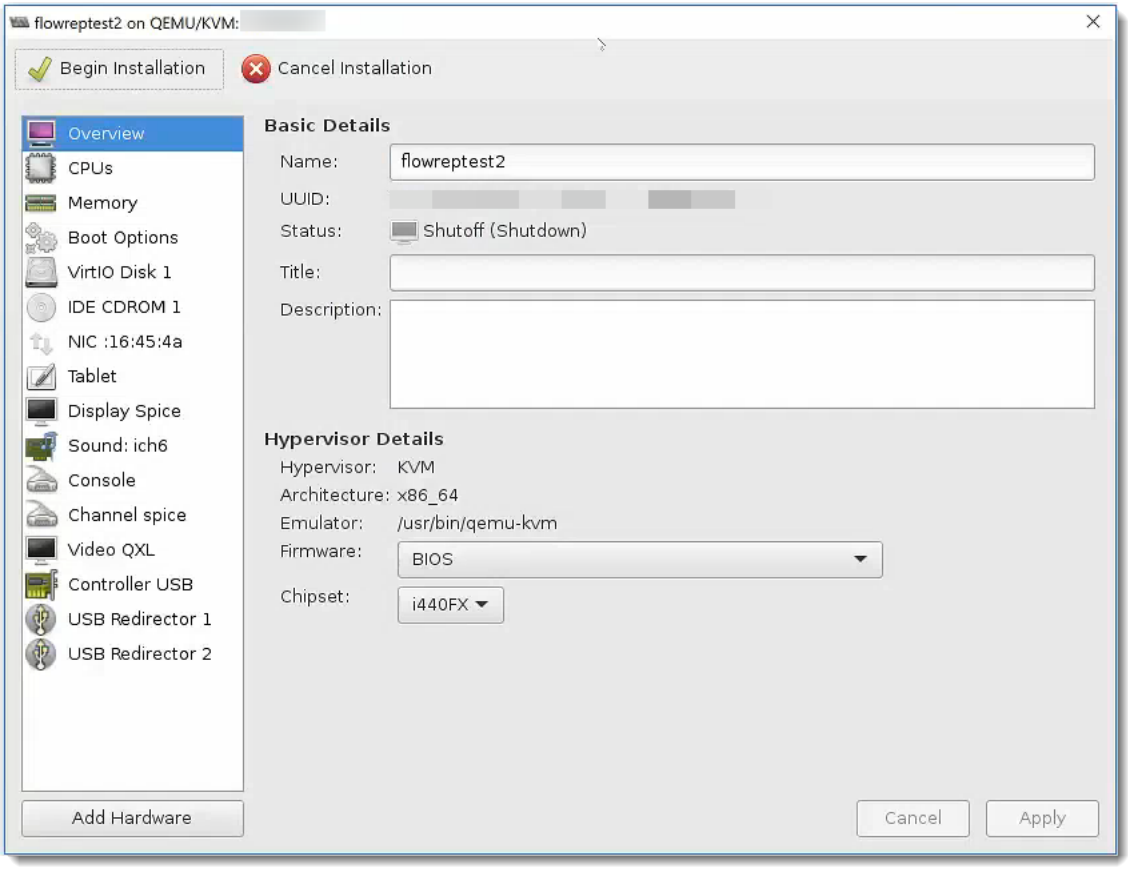
⚠ 如果您选择部署思科 Cisco Secure Network Analytics 设备而没有要求的资源，则必须负责密切监控设备的资源利用率，并根据需要增加资源，以确保部署正常运行。

10. 为虚拟机分配一个名称。这将作为显示名称，因此请使用有助于您稍后查找的名称。
11. 选中**安装前自定义配置 (Customize configuration before install)** 复选框。
12. 在**网络选择 (Network selection)** 下拉框中，选择适用的网络和端口组进行安装。

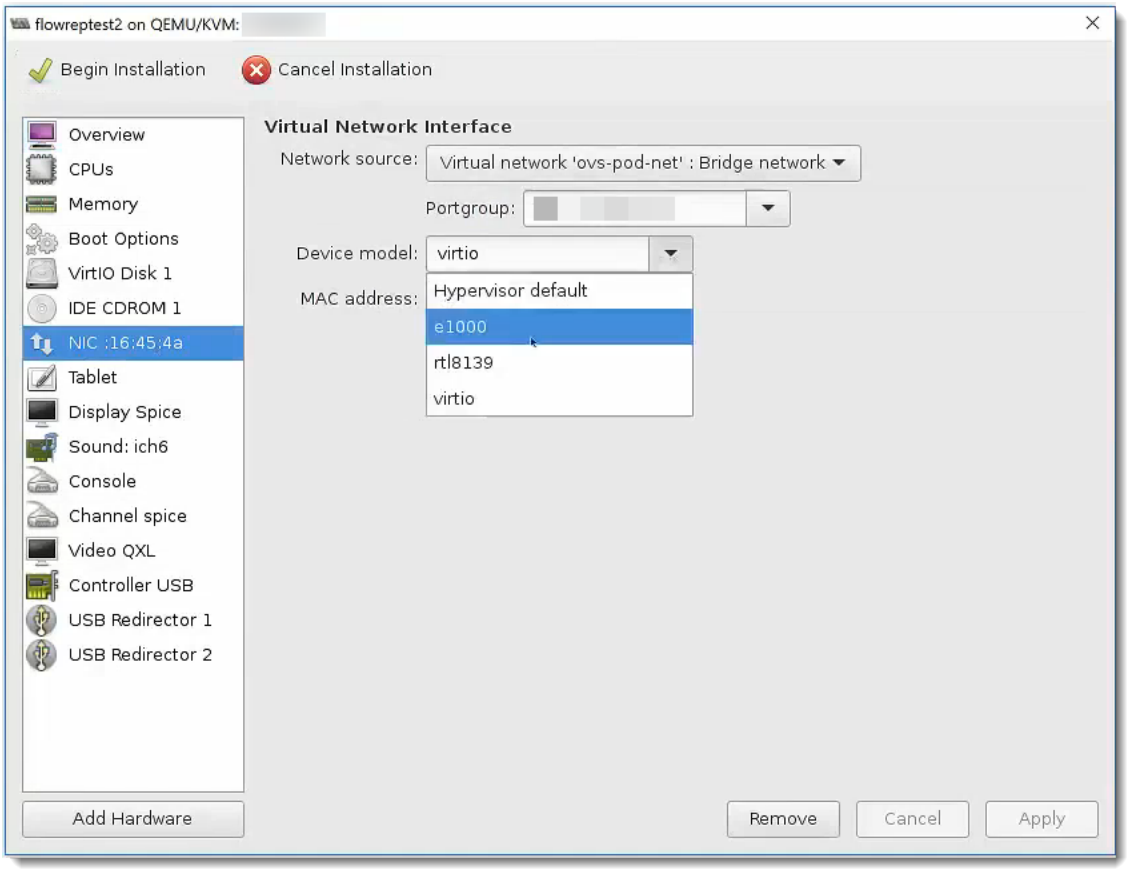
    数据节点：如果是 数据节点，请选择允许 数据节点 在公共网络上与其他设备通信的网络和端口组。



13. 点击**完成 (Finish)**。此时将打开配置菜单。



14. 在导航窗格中，选择 **NIC**。
15. 在虚拟网络接口下，在设备型号下拉框中选择 **e1000**。点击**应用 (Apply)**。



16. 点击 **VirtIO Disk 1**。
17. 在“高级选项”(Advanced Options) 下拉列表中，在磁盘总线下拉框中选择 **SCSI**。点击**应用 (Apply)**。
18. 是否需要添加其他 NICS 来监控 流传感器 虚拟版上的端口，或在 数据节点 VE 上启用数据节点 间通信？

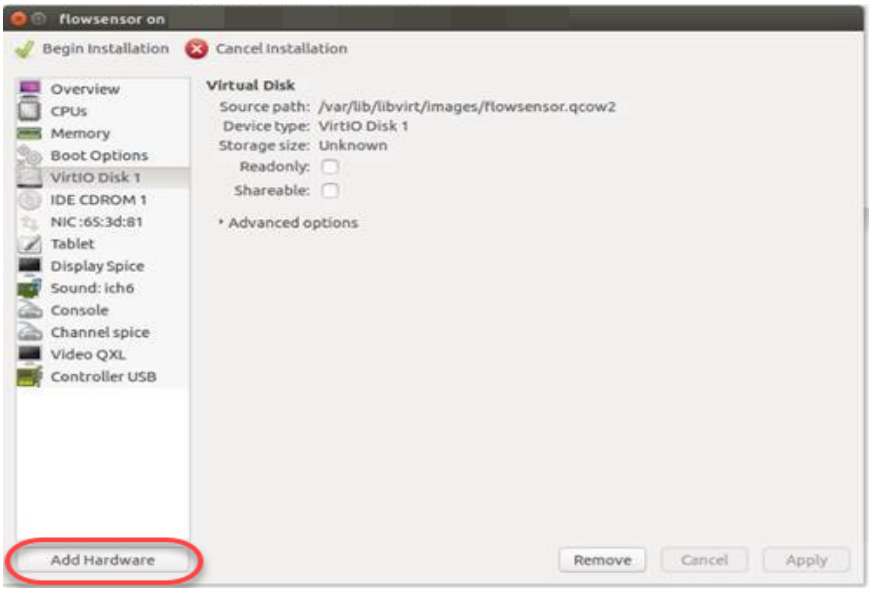
    - 如果是，请转至 **2. 在开放式 vSwitch 上添加 NIC (数据节点、流传感器) 和混杂端口监控(仅限流传感器)**
    - 如果否，则转至下一步。

19. 点击**开始安装(Begin installation)**。
20. 转至 **4. 配置您的 Cisco Secure Network Analytics 系统** 。

2. 在开放式 vSwitch 上添加 NIC (数据节点、流传感器) 和混杂端口监控(仅限流传感器)

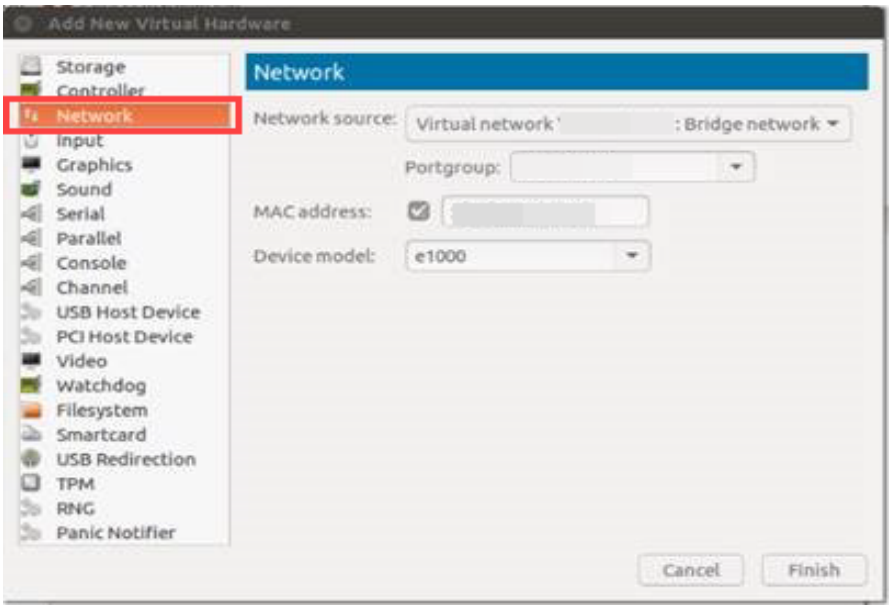
要为 流传感器 虚拟版监控端口或 数据节点 虚拟版添加其他 NIC 并完成安装，请完成以下步骤：

1. 在“配置”(Configuration) 菜单中，点击**添加硬件 (Add Hardware)**。系统随机会显示“添加新的虚拟硬件”(Add New Virtual Hardware) 对话框。



2. 在左侧导航窗格中，点击**网络 (Network)**。

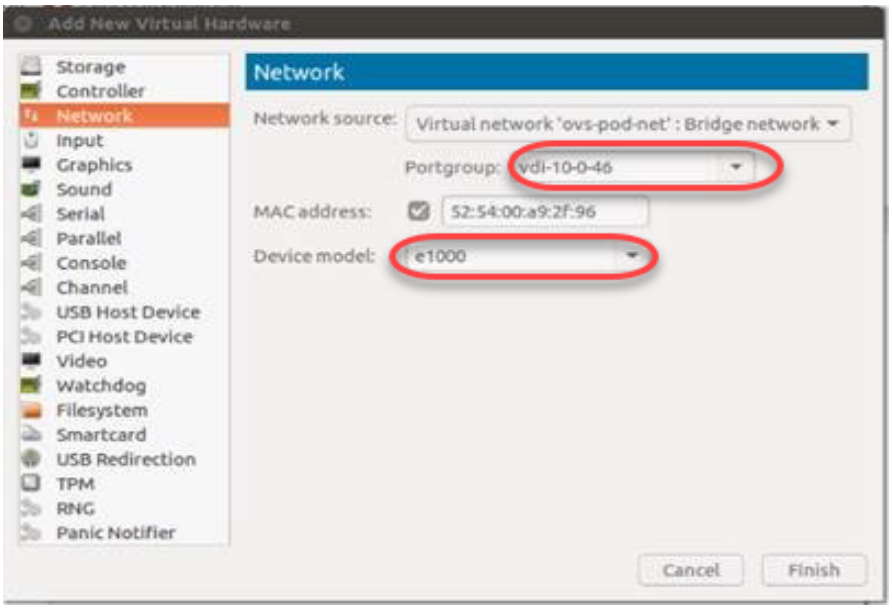
   如果是 数据节点，请选择允许 数据节点 在公共网络上与其他设备通信的网络和端口组。



3. **流量传感器：**如果是 流传感器，请点击端口组下拉列表，选择要监控的未分配混杂端口组。

   点击“设备型号”(Device Model) 下拉列表，选择 **e1000**。

   数据节点：如果是 数据节点，请使用在参阅 **为 数据节点配置隔离 LAN** 。



4. 点击**完成 (Finish)**。
5. 如果需要添加其他监控端口，请重复这些操作。
6. 添加所有监控端口后，点击**开始安装 (Begin Installation)**。

4. 配置您的 Cisco 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 Cisco Secure Network Analytics 到托管系统中。

> ⚠ 要配置 Cisco Secure Network Analytics，请按照 Cisco Secure Network Analytics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

确保您可以通过虚拟机监控程序主机(虚拟机主机)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	仅具有 Data Store 的 Cisco Secure Network Analytics 硬件设备需要： • 管理器 • 流收集器 • 数据节点s	

	eth0 硬件连接端口选项： • **SFP+**:	

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 27 日	更新了通信端口和协议表。
1_2	2023 年 3 月 27 日	更正了一个拼写错误。
1_3	2023 年 4 月 20 日	改进了 VMware 支持的说明。删除了“支持的硬件指标”表，因为这是一个虚拟指南。改进了 KVM 主机版本支持的说明。
1_4	2023 年 8 月 15 日	已将内存资源注释从 GB 更改为 GiB。
1_5	2023 年 4 月 27 日	添加了对 VMware 8.0 的支持。修改了部署建议。
1_6	2023 年 11 月 16 日	更新了“CPU 设置计算”部分。添加了 AVX/AVX2 要求。
1_7	2023 年 11 月 17 日	更正了“联系支持人员”页面中的问题。