Cisco Secure Network Analytics

Virtual Edition アプライアンス設置ガイド 7.4.2

目次

はじめに

概要

次の Cisco Secure Network Analytics（旧 Stealthwatch）Virtual Edition アプライアンスをインストールするには、このガイドを使用します。

- Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）Virtual Edition
- Cisco Secure Network Analytics Data Store Virtual Edition
- Cisco Secure Network Analytics Flow Collector Virtual Edition
- Cisco Secure Network Analytics Flow Sensor Virtual Edition
- Cisco Secure Network Analytics UDP Director Virtual Edition

対象読者

このガイドは、Secure Network Analytics製品のインストールおよび設定を担当するネットワーク管理者とその他の担当者を対象としています。

仮想アプライアンスを設定する場合は、VMware または KVM の基本的な知識があることを前提としています。

専門家によるインストールを希望する場合は、最寄りのシスコパートナーまたはシスコサポートに連絡してください。

アプライアンスのインストールとシステムの設定

Secure Network Analytics のインストールと設定の全体的なワークフローに注意してください。

1. **アプライアンスのインストール**：この設置ガイドに従って、Secure Network Analytics Virtual Edition アプライアンスをインストールします。ハードウェア（物理）アプライアンスをインストールするには、『x2xx Series Hardware Appliance Installation Guide』、または『x3xx Series Hardware Appliance Installation Guide』[英語] の手順に従います。
2. **Secure Network Analytics の設定**：ハードウェアと仮想アプライアンスをインストールしたら、管理対象システムに Secure Network Analytics を構成できます。『Secure Network Analytics System Configuration Guide v7.4.2』の手順に従います。

関連情報

Secure Network Analytics の詳細については、次の技術情報を参照してください。

- **概要**：https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html [英語]
- **Data Store 設計ガイド**：https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf [英語]

用語

このガイドでは、Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 製品に「**アプライアンス**」という用語を使用しています。

「**クラスタ**」は、Manager が管理する Secure Network Analytics アプライアンスのグループです。

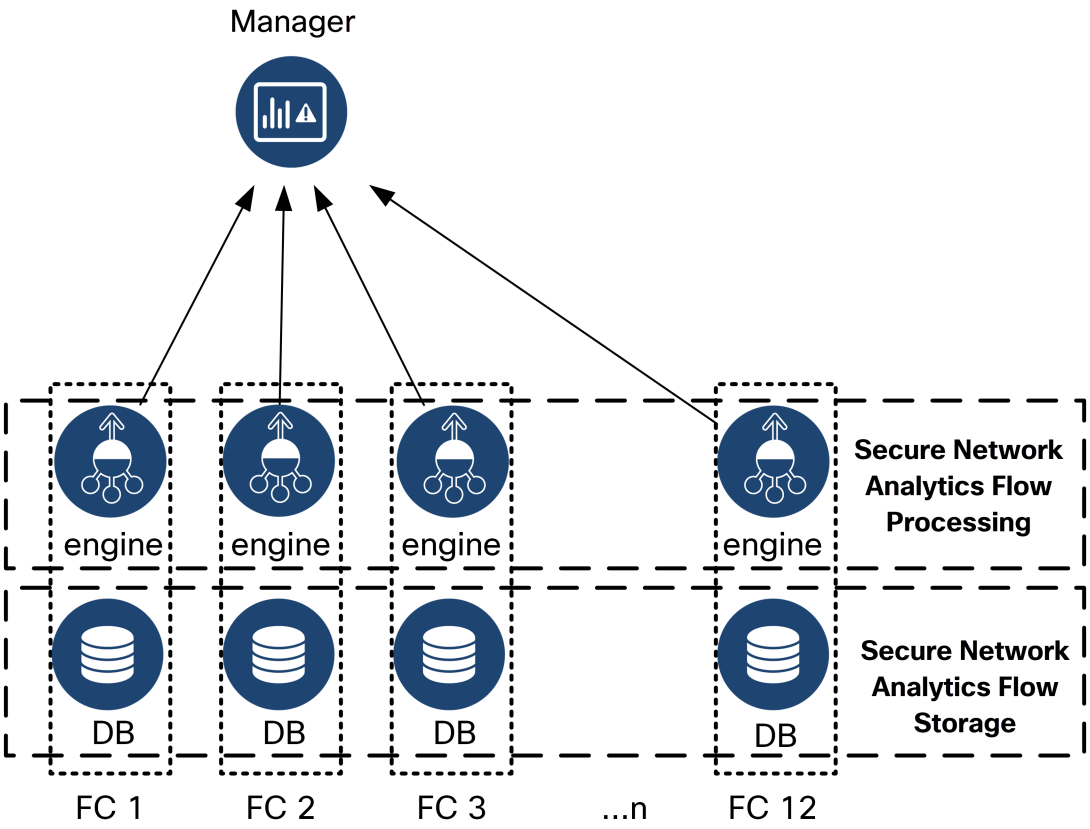
略語

このガイドでは、次の略語が使用される場合があります。

略語	定義
DNS	ドメイン ネーム システム（サービスまたはサーバー）
dvPort	分散仮想ポート
ESX	Enterprise Server X
GB	ギガバイト
IDS	侵入検知システム
IPS	侵入防御システム
ISO	International Standards Organization; 国際標準化機構
IT	情報技術
KVM	カーネルベース仮想マシン
MTU	最大伝送ユニット
NTP	ネットワーク タイム プロトコル
TB	テラバイト
UUID	汎用一意識別子
VDS	vNetwork 分散型スイッチ
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン

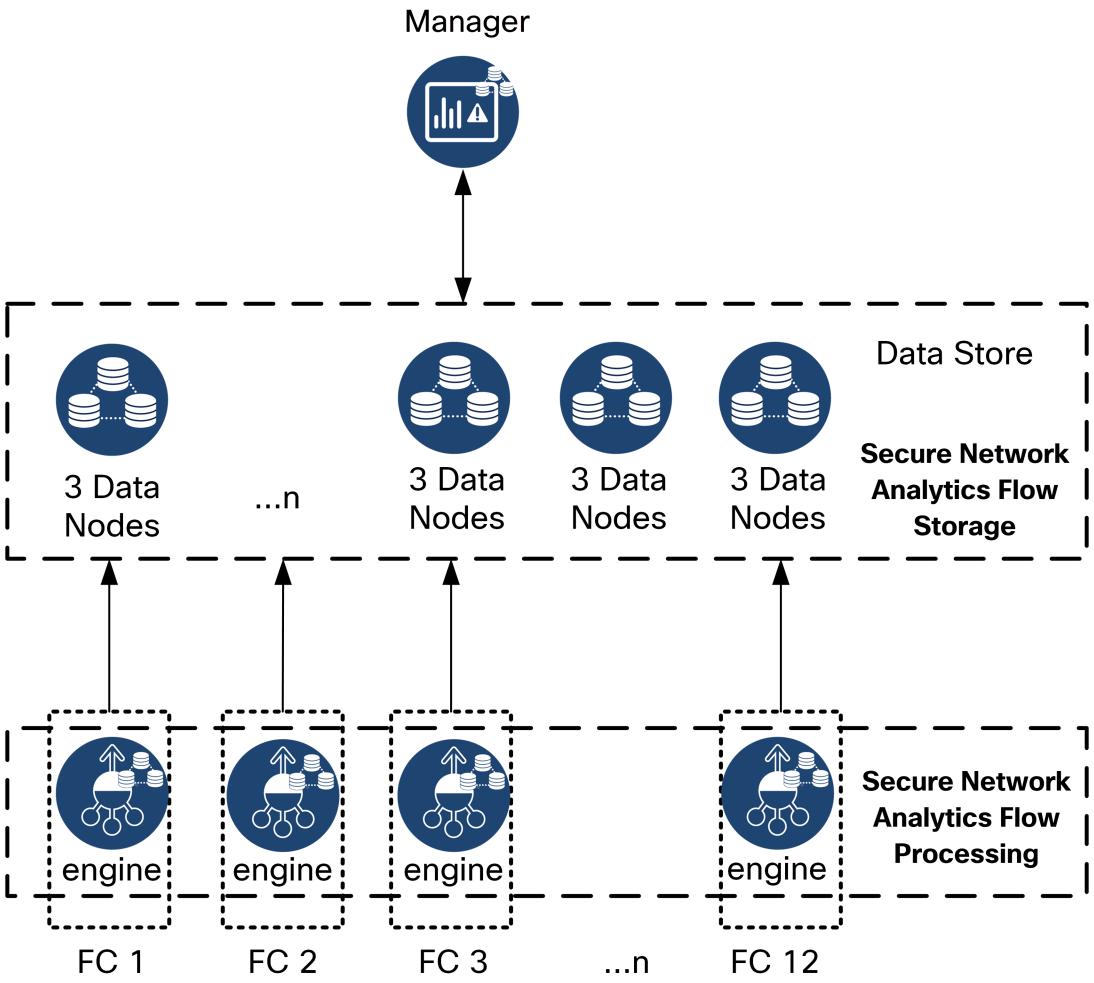
Data Store なしの Cisco Secure Network Analytics

Data Store なしの Secure Network Analytics の展開では、1 つ以上の Flow Collector がデータを取り込んで複製し、分析を実行してデータと結果を Manager に直接レポートします。グラフやチャートを含むユーザーが送信したクエリを解決するために、Manager は管理対象のすべての Flow Collector に照会します。各 Flow Collector は、一致する結果を Manager に返します。Manager はさまざまな結果セットからの情報を照合し、結果を表示するグラフまたはチャートを生成します。この展開では、各 Flow Collector はローカルデータベースにデータを格納します。例として次の図を参照してください。



Data Store ありの Cisco Secure Network Analytics

Data Store を使用した Secure Network Analytics の展開では、Data Store クラスタは Manager と Flow Collector の間に配置されます。1 つ以上の Data Store がフローを取り込み、重複排除し、分析を実行して、データと結果を Data Store に直接報告し、すべての Data Node にほぼ均一に分散させます。Data Store は、データの保管を容易にし、すべてのトラフィックを複数の Flow Collector に分散させずに一元化された場所に保持して複数の Flow Collector よりも大きなストレージ容量を提供します。例として次の図を参照してください。



Data Store は、Flow Collector によって収集されたネットワークのテレメトリを保存する中央リポジトリを提供します。Data Store は、Data Store のクラスタで構成されます。各クラスタには、データの一部と個別 Data Node のデータのバックアップが含まれます。すべてのデータが 1 つの集中型データベースに存在し、複数の Flow Collector に分散されていないため、Manager はすべての Flow Collector に個別にクエリする場合よりも Data Store から迅速にクエリ結果を取得できます。Data Store クラスタは、耐障害性の向上、クエリ応答の改善、グラフとチャート生成の迅速化を実現します。

クエリ

グラフやチャートを含むユーザーが送信したクエリを解決するために、Manager は Data Store に照会します。Data Store は、クエリに関連する列で一致する結果を検索し、一致する行を取得してクエリ結果を Manager に返します。Manager は、複数の Flow Collector からの複数の結果セットの照合を必要とせずに、グラフまたはチャートを生成します。したがって、複数の Flow Collector にクエリする場合と比較して、クエリのコストが軽減され、クエリのパフォーマンスが向上します。

Data Store のストレージと耐障害性

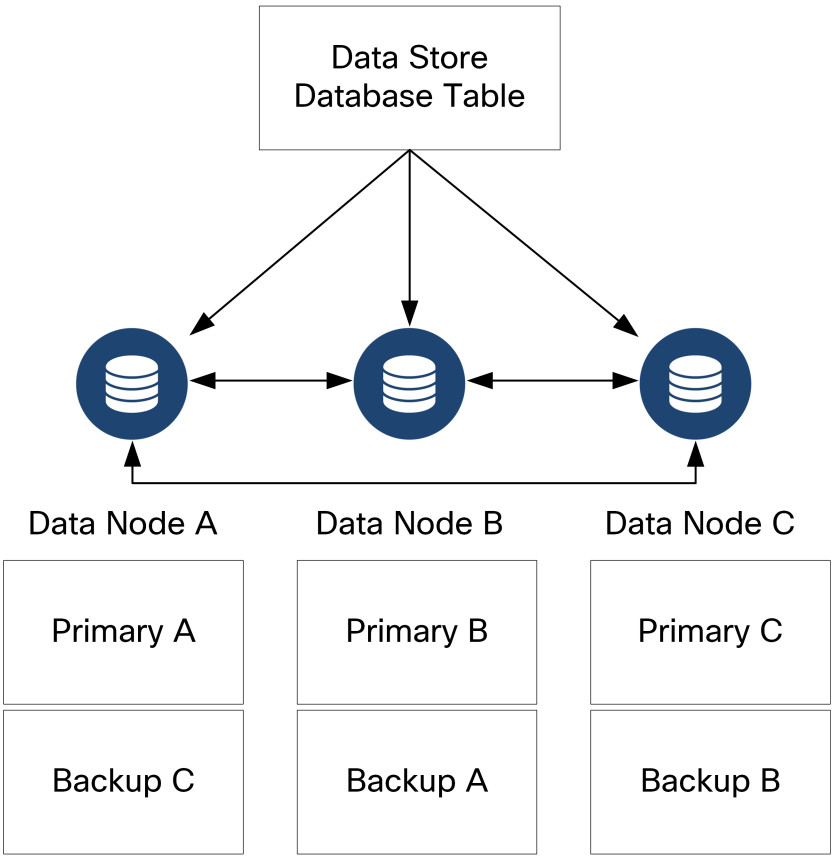
Data Store では、Flow Collector からデータを収集し、クラスタ内の Data Node に均等に分散させます。それぞれの Data Node に、全体のテレメトリの一部が格納され、さらに別の Data Node のテレメトリについてのバックアップも格納されます。この方法でデータを格納することで、次のような利点があります。

- ロードバランシングに役立ちます。
- 各ノードに処理が分散されます。
- Data Store に取り込まれたすべてのデータのバックアップが保持され、耐障害性が確保されます
- Data Node の数を増やすことで、全体的なストレージとクエリのパフォーマンスを向上させることができます

Data Store に 3 つ以上の Data Node がある状況で、いずれかの Data Node が停止した場合、そのバックアップを格納している Data Node がまだ使用可能であり、Data Node の総数の少なくとも半分が稼働していれば、Data Store は全体として稼働状態を維持します。その結果、停止した接続または障害のあるハードウェアを修復する時間的余裕が得られます。問題がある Data Node を交換すると、Data Store により、交換されたノードのデータが隣接する Data Node に格納されている既存のバックアップから復元され、その Data Node にデータのバックアップが作成されます。

テレメトリストレージの例

3 つの Data Node におけるテレメトリの格納方法の例については、次の図を参照してください。



一般的な展開要件

開始する前に、このガイドを参照して、プロセス、およびインストールを計画するために必要な準備、時間、リソースについて確認してください。

インストール方法

仮想アプライアンスのインストールには、VMware 環境または KVM（カーネルベース仮想マシン）を使用できます。

> ⚠ インストールを開始する前に、次のセクションに記載されている「**互換**」の情報と「**リソース要件**」を確認します。

方法	設置手順（参照用）	インストールファイル	詳細
VMware vCenter	**3a. VMware vCenter を使用した仮想アプライアンスのインストール（ISO）**	ISO	VMware vCenter を使用して仮想アプライアンスをインストールします。
VMware ESXi スタンドアロンサーバー	**3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）**	ISO	ESXi スタンドアロンホストサーバーに仮想アプライアンスをインストールします。
KVM および Virtual Machine Manager	**3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**	ISO	KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールします。

互換

VMware 環境または KVM（カーネルベースの仮想マシン）に仮想アプライアンスをインストールする場合は、次の互換性情報を確認してください。

すべてのアプライアンスの一般的な要件

要件	説明
専用リソース	すべてのアプライアンスには専用リソースの割り当てが必要であり、他のアプライアンスまたはホストと共有することはできません。
ライブマイグレーションなし	アプライアンスは、破損の可能性があるため、vMotion をサポートしていません。

要件	説明
ネットワークアダプタ	すべてのアプライアンスには、少なくとも 1 つのネットワークアダプタが必要です。 Flow Sensor に追加のアダプタを設定することにより、追加のスループットをサポートできます。 Data Node には、Data Store の一部として他の Data Node と通信することを目的とした 2 番目のネットワークアダプタが必要です。
ストレージ コントローラ	VMware で ISO を設定する場合は、SCSI コントローラのタイプとして [LSI論理 SAS（LSI Logic SAS）] を選択します。
ストレージのプロビジョニング	仮想アプライアンスを展開する際、シックプロビジョニング（Lazy Zeroed）のストレージプロビジョニングを割り当てます。

VMware

- **互換性**：VMware 7.0 または 8.0
- **オペレーティングシステム**：Debian 11 64 ビット
- **ネットワーク アダプタ**：最高のパフォーマンスを得られるよう、VMXNET3 アダプタタイプの使用をお勧めします。
- **ISO 展開**：Cisco Secure Network Analytics v7.4.2 には VMware 7.0 および 8.0 との互換性があります。VMware 6.0、6.5、または 6.7 と Cisco Secure Network Analytics v7.4.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。
- **ライブマイグレーション**：ホストからホストへのライブマイグレーション（vMotion の使用など）はサポートされていません。
- **スナップショット**：仮想マシンのスナップショットはサポートされていません。

> ⚠ すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

KVM

- **互換性**：任意の互換 Linux ディストリビューションを使用できます。
- **KVM ホスト バージョン**：KVM ホスト上での仮想マシンのインストールに使用される方法は複数あります。次のコンポーネントを使用して KVM をテストし、適切なパフォーマンスが確認されました。
  - libvirt 2.10 ～ 7.1.0
  - qemu-KVM 2.6.1 ～ 5.2.0
  - Open vSwitch 2.6.x ～ 2.15.x****
  - Linux カーネル 4.4.x、および一部の 5.10.x
- **オペレーティングシステム**：Debian 11 64 ビット。

- **仮想化ホスト**：最小要件と最適なパフォーマンスについては、「**リソース要件**」セクションを確認するとともに、Cisco.com にあるアプライアンスのハードウェア仕様シートを参照してください。

> システム パフォーマンスはホスト環境に左右されます。パフォーマンスは変動する場合があります。

ソフトウェアのダウンロード

Cisco Software Central を使用して、仮想アプライアンス（VE）のインストールファイル、パッチ、およびソフトウェア更新ファイルをダウンロードします。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。手順については、「**2. Virtual Edition インストールファイルのダウンロード**」を参照してください。

TLS

Secure Network Analytics v1.2 が必要です。

サード パーティ製アプリケーション

Secure Network Analytics アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して Virtual Edition ISO ファイルをインストールすることは推奨されません。

ホスト名

アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

ドメイン名

各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。

NTP サーバー

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。

タイム ゾーン

すべての Secure Network Analytics アプライアンスは協定世界時（UTC）を使用します。

- **仮想ホスト サーバー**：仮想ホスト サーバーが正しい時刻に設定されていることを確認します。

> ⚠ 仮想アプライアンスをインストールする仮想ホスト サーバーに設定された時刻が正しい時刻に設定されていることを確認します。正しくない場合、アプライアンスを起動できないことがあります。

標準アプライアンスの要件（Data Store なし）

Data Store なしで Secure Network Analytics をインストールする場合は、次のアプライアンスをインストールします。

アプライアンス	要件
マネージャ	• 1 つ以上の Manager
Flow Collector	• 1 つ以上の Flow Collector
UDP Director	オプション
Flow Sensor	オプション

Data Store ありの Secure Network Analytics に関するアプライアンスのインストール要件については、「**Data Store の展開要件**」を参照してください。

Manager と Flow Collector の展開要件

展開する Manager と Flow Collector のそれぞれについて、ルーティング可能な IP アドレスを `eth0` 管理ポートに割り当てます。

Data Store の展開要件

Data Store ありの Secure Network Analytics を展開するには、展開に関する次の要件と推奨事項を確認してください。

アプライアンスの要件（Data Store あり）

次の表に、Data Store を使用した Secure Network Analytics の展開に必要なアプライアンスの概要を示します。

アプライアンス	要件
Manager	• 1 つ以上の Manager
Data Store	• 少なくとも 1 つまたは 3 つの Data Node • Data Store を拡張するための付加的な 3 つの Data Node のセット（Data Node の最大数は 36 個） • 1 つのクラスタに 2 つの Data Node のみを展開することはできません。
Flow Collector	• 1 つ以上の Flow Collector
Flow Sensor	オプション

Manager と Flow Collector の展開要件

展開する Manager と Flow Collector のそれぞれについて、ルーティング可能な IP アドレスを `eth0` 管理ポートに割り当てます。

Data Node の展開要件

各 Data Store は、複数の Data Node で構成されます。

- **Virtual Edition**：仮想 Data Store をダウンロードすると、1 つ、3 つ、またはそれ以上の Data Node Virtual Edition を展開できます（3 つで 1 セット）。
- **ハードウェア**：ハードウェア Data Node をインストールすることもできます。DN 6300 Data Store では 1 つの Data Node ハードウェアシャーシが提供されます。

> Data Node がすべてハードウェアであるか、すべて Virtual Edition であることを確認してください。ハードウェア Data Node と仮想 Data Node の混在はサポートされておらず、ハードウェアは同じハードウェア世代（すべて DS 6200 またはすべて DN 6300）である必要があります。

複数 Data Node 展開

複数 Data Node 展開により、パフォーマンスの面で最大の成果を得られます。

次の点に注意してください。

- **3 つで 1 セット**：Data Node は、Data Store の一部として、最小 3 つから最大 36 まで 3 の倍数でクラスタ化できます。1 つのクラスタに 2 つの Data Node のみを展開することはできません。
- **すべてハードウェアまたはすべて仮想**：Data Node がすべて（同じ世代の）ハードウェアである、またはすべて Virtual Edition であることを確認します。ハードウェア Data Node と仮想 Data Node の混在、または Data Store 6200 と Data Node 6300 の混在はサポートされていません。
- **Data Node のプロファイルサイズ**：Virtual Edition Data Node を展開する場合は、それらがすべて同じプロファイルサイズであり、RAM、CPU、およびディスク容量が同じであることを確認します。詳細については、「リソース要件」セクションの「**Data Node Virtual Edition**」を参照してください。

サポートされるハードウェアメトリック（Analytics が有効な場合）

ノード数	1 秒あたりのフロー	固有内部ホスト
1	600,000	1.3 万
3 以上	600,000	1.3 万
3 以上	850,000	700,000

これらの推奨事項では、テレメトリのみを考慮しています。パフォーマンスは、ホスト数、Flow Sensor の使用、トラフィックプロファイル、その他のネットワーク特性など、追加の要因によって異なる場合があります。サイジングについては、シスコ サポート までお問い合わせください。

サポートされるハードウェアメトリック（Analytics が有効になっていない場合）

ノード数	1 秒あたりのフロー	固有内部ホスト
1	最大 100 万	最大 3,300 万
3 以上	最大 300 万	最大 3,300 万

これらの数値は、130 万の固有ホストにより平均顧客データを使用してシスコのテスト環境で算出したものです。それぞれ環境でのパフォーマンスは、ホスト数や平均フローサイズなど、いくつかの要因によって影響を受ける可能性があります。サイジングについては、シスコ サポート までお問い合わせください。

単一 Data Node 展開

単一（1 つ）の Data Node を展開することを選択した場合：

- **Flow Collector**：最大 4 つの Flow Collector がサポートされます。
- **Data Node の追加**：Data Node を 1 つだけ展開した場合、将来展開に Data Node を追加できます。詳細については、「**複数 Data Node 展開**」を参照してください。

これらの推奨事項では、テレメトリのみを考慮しています。パフォーマンスは、ホスト数、Flow Sensor の使用、トラフィックプロファイル、その他のネットワーク特性など、追加の要因によって異なる場合があります。サイジングについては、シスコサポートにお問い合わせください。

現在、Data Store では、プライマリ Data Node が停止した場合のスペア Data Node との自動交換はサポートされていません。ガイダンスについては、シスコサポートにお問い合わせください。

Data Node の設定要件

Data Store を展開するには、各 Data Node に以下を割り当てます。お客様が準備する情報は、『システム コンフィギュレーション ガイド』を使用して初回セットアップで設定されます。

- **ルーティング可能な IP アドレス（eth0）**：Secure Network Analytics アプライアンスに対する管理、取り込み、クエリ通信に使用します。
- **Data Node 間通信**：Data Node 間通信に使用されるプライベート LAN または VLAN 内の `169.254.42.0/24` CIDR ブロックからルーティング不可能な IP アドレスを設定します。

  スループットパフォーマンスを向上させるには、`eth2` と `eth3` を含むポートチャネルを接続します。各 Data Node から仮想スイッチまたはd独立ネットワークを介してその他すべての Data Node に到達できることを確認します。Data Store の一部として、Data Node は相互に通信します。
- **ネットワーク接続**：管理、取り込み、クエリ通信用と Data Node 間通信用の 2 つのネットワーク接続が必要です。

ネットワーキングとスイッチングに関する考慮事項

次の表に、Data Store ありの Secure Network Analytics を展開する場合のネットワーキングとスイッチングに関する考慮事項の概要を示します。

ネットワークに関する考慮事項	説明
Data Node 間通信	• Data Node が相互に通信できるように、仮想スイッチを使用して独立した LAN を設定します。 • Data Node 間での推奨されるラウンドトリップ時間（RTT）の遅延を 200 マイクロ秒未満に設定します。 • Data Node 間のクロックスキューを 1 秒以下に保ちます。 • Data Node 間での推奨スループットを 6.4 Gbps 以上（10 Gbps 全二重スイッチ接続）に設定します。
Data Node のスイッチング	• Data Node は、Data Node 間通信を可能にするために独自のレイヤ 2 VLAN を必要とします。Data Node VE の展開方法に応じて、仮想 Data Node を独立ネットワークに接続できます。

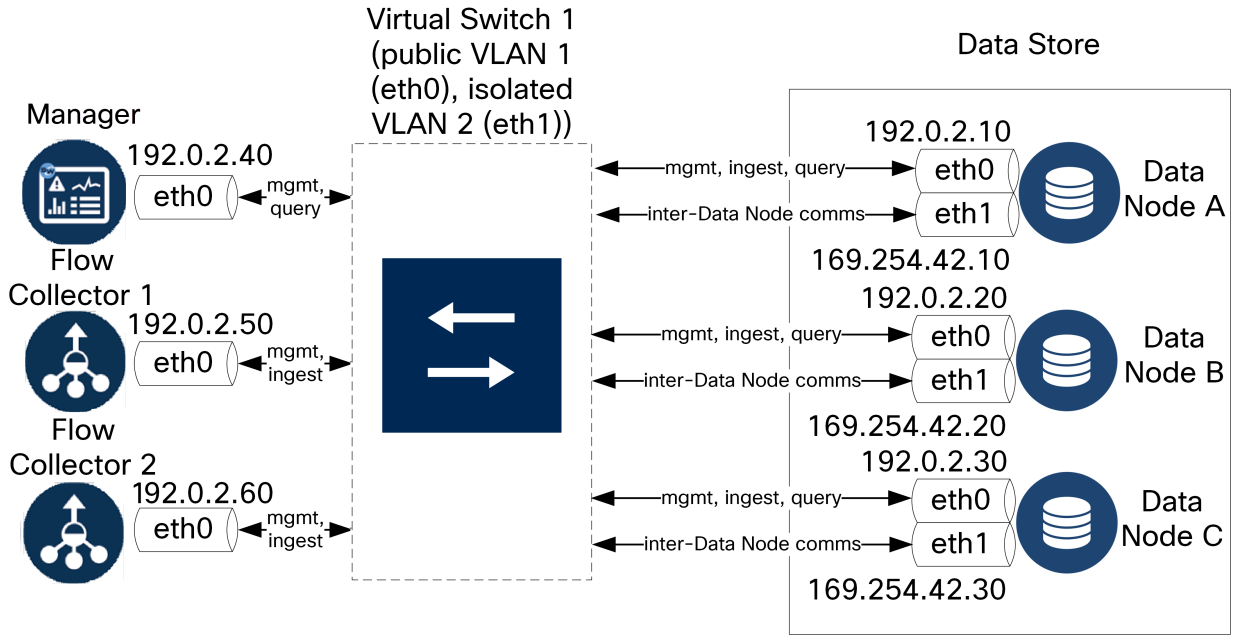
Secure Network Analytics アプライアンス通信	• Manager および Flow Collector は、すべての Data Node に到達できる必要があります • Data Node は、Manager、すべての Flow Collector、および各 Data Node に到達できる必要があります

現在、Data Store では、プライマリ Data Node が停止した場合のスペア Data Node との自動交換はサポートされていません。ガイダンスについては、シスコサポートにお問い合わせください。

仮想スイッチの例

`eth1` を介した Data Node 間の通信を有効にするには、仮想スイッチで Data Node 間の通信用に独立した LAN または VLAN を設定します。この仮想スイッチは Data Node 間の通信専用にします。

また、Data Node の Manager および Flow Collector との `eth0` 通信用にパブリック LAN または VLAN を設定します。例として次の図を参照してください。



Data Store クラスタでは、独立 VLAN 内のノード間で継続的なハートビートが必要です。このハートビートがないと、Data Node がオフラインになる可能性があり、Data Store が停止するリスクが高まります。

導入の計画については、Cisco プロフェッショナルサービスにお問い合わせください。

Data Store の配置に関する考慮事項

Data Node は、それぞれがすべての Flow Collector、Manager、および他の Data Node と通信できるように配置します。最適なパフォーマンスを得るには、Data Node と Flow Collector を同じ場所に配置して通信の遅延を最小限に抑え、Data Node と Manager を同じ場所に配置してクエリのパフォーマンスを最適化します。

- **ファイアウォール**：シスコでは、Data Node をファイアウォール内（NOC 内など）に配置することを強く推奨しています。
- **物理ホスト/ハイパーバイザ**：設定を容易にするために、すべての Data Node Virtual Edition を同じ物理ホストまたはハイパーバイザに展開します。これにより、独立 LAN で Data Node 間の設定を簡単に行えます。
- **電力**：電力の喪失やハードウェアの障害が原因で Data Store が停止すると、データ破損やデータ損失のリスクが高くなります。Data Node の設置においては、常に稼働時間が維持されるように考慮します。

> Data Node の電源が予期せずに失われ、アプライアンスをリブートした場合、その Data Node のデータベースインスタンスが自動的に再起動しないことがあります。データベースのトラブルシューティングと手動での再起動については、『システム コンフィギュレーション ガイド』を参照してください。

Analytics の展開の要件

Secure Network Analytics は、ダイナミック エンティティ モデリングを使用してネットワークの状態を追跡します。Secure Network Analytics のコンテキストにおけるエンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。詳細については、『 Analytics: Detections, Alerts, and Observations Guide』を参照してください。

Analytics を有効にするには、以下の条件で展開を設定する必要があります。

- 任意の数の Flow Collector を備えた仮想またはハードウェア Data Store 展開で設定する。
- Secure Network Analytics Data Store ドメインは 1 つのみ使用する。

リソース要件

このセクションでは、仮想アプライアンスのリソース要件を示します。

このセクションの表を使用して、Secure Network Analytics Virtual Edition アプライアンスのインストールと設定に必要な設定を記録します。

- Manager Virtual Edition
- Flow Collector Virtual Edition
- Data Node Virtual Edition
- Flow Sensor Virtual Edition
- UDP Director Virtual Edition
- 1 秒あたりのフローの計算（オプション）

> ⚠ システムに必要なリソースを確保してください。この手順は、システムパフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

> ℹ 次の表のギガバイトまたは GB の参照は、次のように定義されます。2 の 30 乗、厳密には 1,073,741,824 バイトに等しい情報の単位。

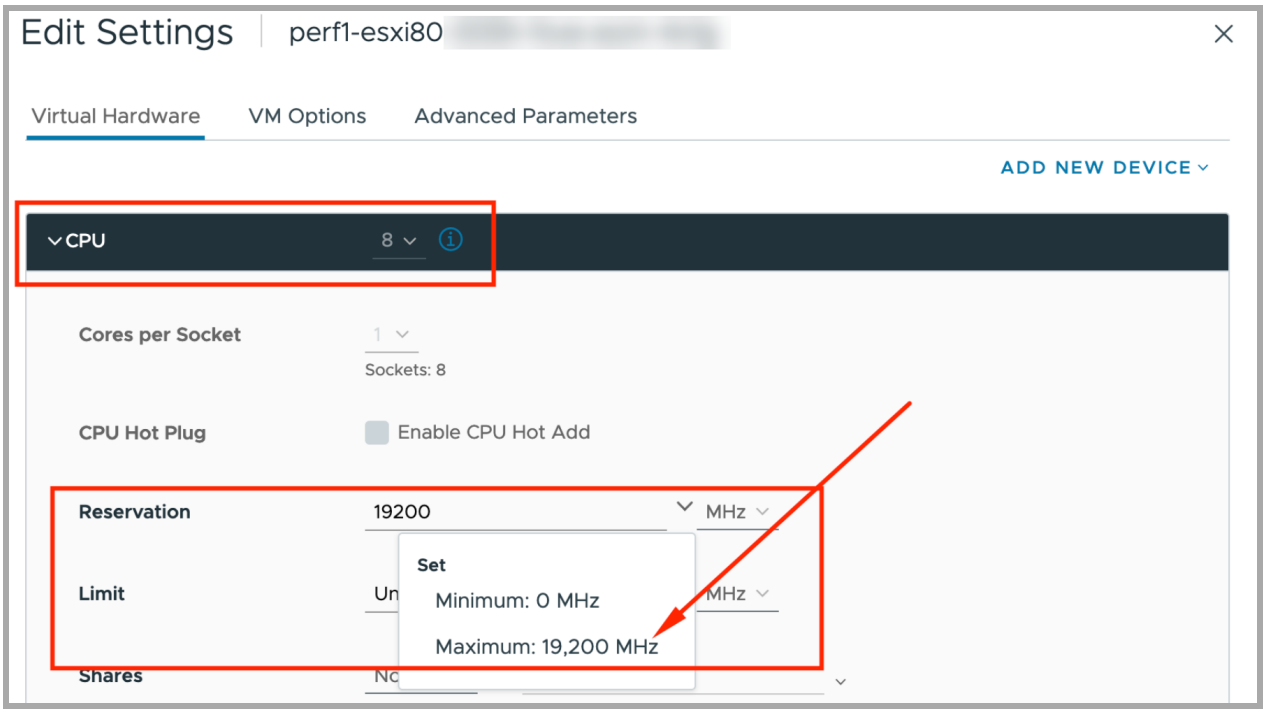
CPU 設定の計算

EXSi ホストで CPU を予約するときに最大のパフォーマンスを得るには、[CPU設定（CPU Settings）] で、CPU 周波数の [予約（Reservation）] 設定に次の計算が使用されていることを確認してください。

<Recommended number of CPUs> * <Core Frequency> = <Frequency Reservation>

CPU のコア周波数（プロセッサタイプ）は、ハイパーバイザの「ホストの詳細」セクションで確認できます。

次の例では、8 個の CPU にコア周波数（この場合は 2,400MHz（または 2.4 GHz））を掛けます。これにより、周波数予約に使用する 19200 MHz の数値が得られます。



詳細については、「3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）」を使用します。

Manager Virtual Edition

Manager Virtual Edition の最小のリソース割り当て量を決定するには、Manager にログインすることが予想される同時ユーザーの数を決めます。リソース割り当てを決定するには、次の仕様を参照してください。

マネージャ

同時接続数ユーザー*	必須予約済み CPU	必須予約済みメモリ	必須最小ストレージ	1 秒あたりのフロー数	内部ホスト
最大 9	6	40 GB	200 GB	最大 100,000	100,000
10 超	12	70 GB	480 GB	100,000 超	250,000

* 同時ユーザーには Manager クライアントを同時に使用するスケジュール済みレポートや個人が含まれます。

Flow Collector Virtual Edition

Flow Collector Virtual Edition のリソース要件を決定するには、ネットワークで予想される 1 秒あたりのフロー数、および監視する予定のエクスポータとホストの数を計算します。詳細については、「1 秒あたりのフローの計算」セクションを参照してください。

また、FPS の計算と保持要件によって最小ストレージ容量が増えることがあります。

Data Store 内の Data Node は、Flow Collector ではなくフローを格納するため、予定している展開（Data Store なし、または Data Store あり）の仕様を必ず参照してください。

Flow Collector（Data Store なし）

1 秒あたりのフロー数	必須予約済み CPU	必須予約済みメモリ	必須最小データストレージ（30 日間）	インターフェイス	エクスポータ	内部ホスト
最大 10,000	2	24 GB	600 GB	最大 65,535	最大 1024	25,000
最大 30,000	6	32 GB	900 GB	最大 65,535	最大 1024	100,000
最大 60,000	8	64 GB	1.8 TB	最大 65,535	最大 2,048	250,000
最大 120,000	12	128 GB	3.6 TB	最大 65,535	最大 4,096	250,000 超

Flow Collector（Data Store あり）

1 秒あたりのフロー数	必須予約済み CPU	必須予約済みメモリ	必須最小ストレージ	インターフェイス	エクスポータ	内線ホスト
最大 10,000	2	24 GB	200 GB	最大 65,535	最大 1024	25,000
最大 30,000	6	32 GB	200 GB	最大 65,535	最大 1024	50,000
最大 60,000	8	64 GB	200 GB	最大 65,535	最大 2,048	100,000
最大 120,000	12	128 GB	200 GB	最大 65,535	最大 4,096	250,000

Data Node Virtual Edition

次の情報を確認して、Data Node Virtual Edition のリソース要件を計算します。

- **1 秒あたりのフローの計算**：ネットワークで予想される 1 秒あたりのフローを決定します。詳細については、「1 秒あたりのフローの計算」セクションを参照してください。
- **Data Node の数**：1 つの Data Node、または 3 つ以上の Data Node を展開できます（3 つで 1 セット）。詳細については、「**アプライアンスの要件（Data Store あり）**」を参照してください。

1 秒あたりのフローの計算に基づいて次の仕様を参照し、リソース要件を決定します。

単一の仮想 Data Node を備えた Data Store

1 秒あたりのフロー数	必須予約済み CPU	必須予約済みメモリ	単一 Data Node の必須最小ストレージ（30 日間保持）
最大 30,000	6	32 GB	2.25 TB
最大 60,000	6	32 GB	4.5 TB
最大 120,000	12	32 GB	9 TB
最大 225,000	18	64 GB	18 TB

3 つの仮想 Data Node を備えた Data Store

1 秒あたりのフロー数	必須予約済み CPU	必須予約済みメモリ	各 Data Node の必須最小ストレージ（30 日間保持）	3 つの Data Node Data Store の必須最小ストレージ（30 日間保持）
最大 30,000	6	32 GB	Data Node あたり 1.5 TB	Data Store 用に合計 4.5 TB
最大 60,000	6	32 GB	Data Node あたり 3 TB	Data Store 用に合計 9 TB
最大 120,000	12	32 GB	Data Node あたり 6 TB	Data Store 用に合計 18 TB
最大 220,000	18	64 GB	Data Node あたり 10 TB*	Data Store 用に合計 30 TB*
最大 500,000	18	64 GB	Data Node あたり 15 TB*	Data Store 用に合計 45 TB*
* 大規模環境では、テレメトリの線形増加を抑えるために Data Store 最適化が適用されます。				

Flow Sensor Virtual Edition

このセクションでは、Flow Sensor Virtual Edition について説明します。

- **キャッシュ**：[フローキャッシュサイズ（Flow Cache Size）] 列には、Flow Sensor が同時に処理できるアクティブフローの最大数が示されます。キャッシュは予約済みメモリの量で調整され、フローは 60 秒ごとにフラッシュされます。[フローキャッシュサイズ（Flow Cache Size）] を使用して、モニター対象トラフィックの量に対して必要なメモリの容量を計算します。
- **要件**：環境に必要なリソースの量は、さまざまな可変的要因（平均パケットサイズ、バーストレート、その他のネットワークとホストの状況）に応じて異なります。

NIC – モニターリング ポート	必須予約済み CPU	必須最小ハードウェア予約済みメモリ	必須最小データストレージ	予測されるスループット	フロー キャッシュ サイズ（同時フローの最大数）
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 PCI パススルーとして設定されているインターフェイス（igb/ixgbe 準拠または e1000e 準拠）	65,537
4 X 1 Gbps	8	16 GB	75 GB	3,700 Mbps PCI パススルーとして設定されているインターフェイス（igb/ixgbe 準拠または e1000e 準拠）	131,073
1 X 10 Gbps *	12	24 GB	75 GB	8 Gbps PCI パススルーとして設定されているインターフェイス（インテル ixgbe/i40e 準拠）	~512,000
2 x 10 Gbps *	22	40 GB	75 GB	16 Gbps PCI パススルーとして設定されているインターフェイス（インテル ixgbe/i40e 準拠）	~1,000,000

* 10 Gbps スループットの場合、すべての CPU を 1 つのソケットに設定します。追加の 10 Gbps NIC ごとに、10 個の vCPU と 16 GB の RAM を追加します。

オプション：物理 VM ホストで 1 つ以上の 10G NIC を使用できます。

Flow Sensor Virtual Edition ネットワーク環境

Flow Sensor Virtual Edition をインストールする前に、ご使用のネットワーク環境のタイプを確認してください。このガイドは、Flow Sensor Virtual Edition で監視できるすべてのネットワーク環境を扱っています。

互換性：Secure Network Analyticsは VDS 環境をサポートしていますが、VMware Distributed Resource Scheduler（VM-DRS）をサポートしていません。

仮想ネットワーク環境：Flow Sensor Virtual Edition は、次のタイプの仮想ネットワーク環境を監視します。

- 仮想ローカル エリア ネットワーク（VLAN）トランキングを使用したネットワーク
- （ローカル ポリシーなどの理由で）1 つ以上の VLAN でパケット モニターリング デバイスの接続が禁止されている、分離した VLAN
- プライベート VLAN
- ハイパーバイザ ホスト（VLAN 以外）

Flow Sensor Virtual Edition のトラフィック

Flow Sensor は、次の Ethertype のトラフィックを処理します。

Ethertype	プロトコル
0x8000	通常の IPv4
0x86dd	通常の IPv6
0x8909	SXP
0x8100	VLAN
0x88a8 0x9100 0x9200 0x9300	VLAN QnQ
0x8847	MLPS ユニキャスト
0x8848	MLPS マルチキャスト

Flow Sensor は、最上位の MPLS ラベルまたは VLAN ID を保存およびエクスポートします。パケットを処理している場合は、他のラベルをバイパスします。

UDP Director Virtual Edition

UDP Director Virtual Edition では、仮想マシンが次の要件を満たす必要があります。また、FPS の計算と保持要件によって最小ストレージ容量が増えることがあります。

必須予約済み CPU	必須予約済みメモリ	最小データ ストレージ	最大 FPS レート
2	4 GB	75 GB	10,000

1 秒あたりのフローの計算（オプション）

前述のセクションで示したものとは異なるストレージ容量に基づいてリソース要件を計算する場合は、ここに示す 1 秒あたりのフロー（FPS）の計算を使用できます。

Flow Collector ストレージの 1 秒あたりのフローの計算（Data Store なしでの展開）

Data Store なしで Flow Collector（NetFlow）を展開する場合は、次のようにストレージの割り当てを計算します。

[（日平均 FPS/1,000）X 1.6 X 日数]

- daily average FPS を算出します。
- この数値を 1,000 FPS で割ります。
- この数値にストレージの 1.6 GB を掛けると、1 日分のストレージに相当する値が得られます。
- この数値に Flow Collector の全ストレージのフローを保存する日数を掛けます。

たとえば、次のシステムの場合：

- 50,000 daily average FPS を処理
- 30 日間フローを保存

Flow Collector ごとに次のように計算します。

[(50,000/1,000)X 1.6 X 30] = 7,200 GB(7.2 TB)

- 日時平均 FPS = 50,000
- 日時平均 50,000 FPS / 1,000= 50
- 50 X 1.6 GB = 1 日あたりのストレージ相当量 80 GB
- Flow Collector あたり 80 GB X 30 日 = Flow Collector あたり 2400 GB

Data Node ストレージの 1 秒あたりのフローの計算

3 つの Data Node Virtual Edition に Data Store Virtual Edition を展開する場合は、Data Node ごとに、ストレージ割り当てを次の方法で計算することを推奨します。

[（日時平均 FPS/1,000） X 1.6 X 日数] / Data Node 数

- daily average FPS を算出します。
- この数値を 1,000 FPS で割ります。

- この数値にストレージの 1.6 GB を掛けると、1 日分のストレージに相当する値が得られます。
- この数値に、Data Store の全ストレージのフローを保存する日数を掛けます。
- この数値を Data Store 内の Data Node 数で割って、Data Node あたりのストレージを算出します。

たとえば、次のシステムの場合:

- 50,000 daily average FPS を処理
- 90 日間フローを保存
- 3 つの Data Node を装備

Data Node あたりの数値を次のように算出できます。

[(50,000/1,000) X 1.6 X 90] / 3 = Data Node あたり 2,400 GB (2.4 TB)

- 日時平均 FPS = 50,000
- 日平均 50,000 FPS / 1,000 = 50
- 50 X 1.6 GB = 1 日あたりのストレージ相当量 80 GB
- Data Store あたり 80 GB X 90 日 = Data Store あたり 7,200 GB
- 7,200 GB / 3 Data Node = Data Node あたり 2,400 GB(2.4 TB)

1. 通信用ファイアウォールの設定

アプライアンスが適切に通信できるようにするには、ファイアウォールまたはアクセス コントロール リストによって必要な接続がブロックされないようにネットワークを設定する必要があります。この項に示される情報を使用して、アプライアンスがネットワークを介して通信できるようにネットワークを設定します。

オープンポート（すべてのアプライアンス）

次のポートが開いた状態になってアプライアンス（Manager、Flow Collector、Data Node、Flow Sensor、UDP Director）で無制限のアクセスが可能になるように、ネットワーク管理者と話し合ってください。

- 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

Data Node 用のその他のオープンポート

また、Data Node をネットワークに展開する場合は、次のポートが開いた状態で、無制限のアクセスを提供できることを確認してください。

- TCP 5433
- TCP 5444
- TCP 9450

通信ポートおよびプロトコル

Secure Network Analytics でポートがどのように使用されるかを次の表に示します。

送信元 （クライアント）	宛先 （サーバ）	ポート	プロトコル
管理者ユーザーの PC	すべてのアプライアンス	TCP/443	HTTPS
すべてのアプライアンス	ネットワークの時刻源	UDP/123	NTP
Active Directory	Manager	TCP/389、 UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
外部ログ ソース	Manager	UDP/514	SYSLOG
Flow Collector	Manager	TCP/443	HTTPS
UDP Director	Manager	TCP/443	HTTPS
UDP Director	Flow Collector（sFlow）	UDP/6343*	sFlow
UDP Director	Flow Collector（NetFlow）	UDP/2055*	NetFlow
UDP Director	サードパーティのイベント管理システム	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector（NetFlow）	UDP/2055	NetFlow
NetFlow エクスポータ	Flow Collector（NetFlow）	UDP/2055*	NetFlow
sFlow エクスポータ	Flow Collector（sFlow）	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS
Manager	Cisco ISE	TCP/443	HTTPS
Manager	Cisco ISE	TCP/8910	XMPP
Manager	DNS	UDP/53	DNS

送信元 （クライアント）	宛先 （サーバ）	ポート	プロトコル
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Flow エクスポータ	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	CRL 分散ポイント	TCP/80	HTTP
Manager	OCSP レスポンダ	TCP/80	OCSP
ユーザー PC	Manager	TCP/443	HTTPS

＊これはデフォルト ポートですが、任意の UDP ポートをエクスポータで設定できます。

Data Store 用のその他のオープンポート

Data Store を展開するためにファイアウォールで開く通信ポートを次に示します。

#	送信元 （クライアント）	宛先（サーバー）	ポート	プロトコルまたは目的
1	Manager	Flow Collector と Data Node	22/TCP	SSH（Data Store データベースの初期化に必要）
1	データノード	他のすべての Data Node	22/TCP	SSH（Data Store データベースの初期化およびデータベース管理タスクに必要）
2	Manager、Flow Collector、および Data Node	NTP サーバー	123/UDP	NTP（時刻同期に必要）
2	NTP サーバー	Manager、Flow Collector、および Data Node	123/UDP	NTP（時刻同期に必要）
3	Manager	Flow Collector と Data Node	443/TCP	HTTPS（アプライアンス間のセキュア通信に必要）
3	Flow Collector	Manager	443/TCP	HTTPS（アプライアンス間のセキュア通信に必要）

3	データノード	Manager	443/TCP	HTTPS（アプライアンス間のセキュア通信に必要）
4	NetFlow エクスポータ	Flow Collector：NetFlow	2055/UDP	NetFlow の取り込み
5	データノード	他のすべての Data Node	4803/TCP	Data Node 間メッセージングサービス
6	データノード	他のすべての Data Node	4803/UDP	Data Node 間メッセージングサービス
7	データノード	他のすべての Data Node	4804/UDP	Data Node 間メッセージングサービス
8	Manager、Flow Collector、および Data Node	データノード	5433/TCP	Vertica クライアント接続
9	データノード	他のすべての Data Node	5433/UDP	Vertica メッセージングサービスのモニターリング
10	sFlow エクスポータ	Flow Collector（sFlow）	6343/UDP	sFlow の取り込み
11	データノード	他のすべての Data Node	6543/UDP	Data Node 間メッセージングサービス

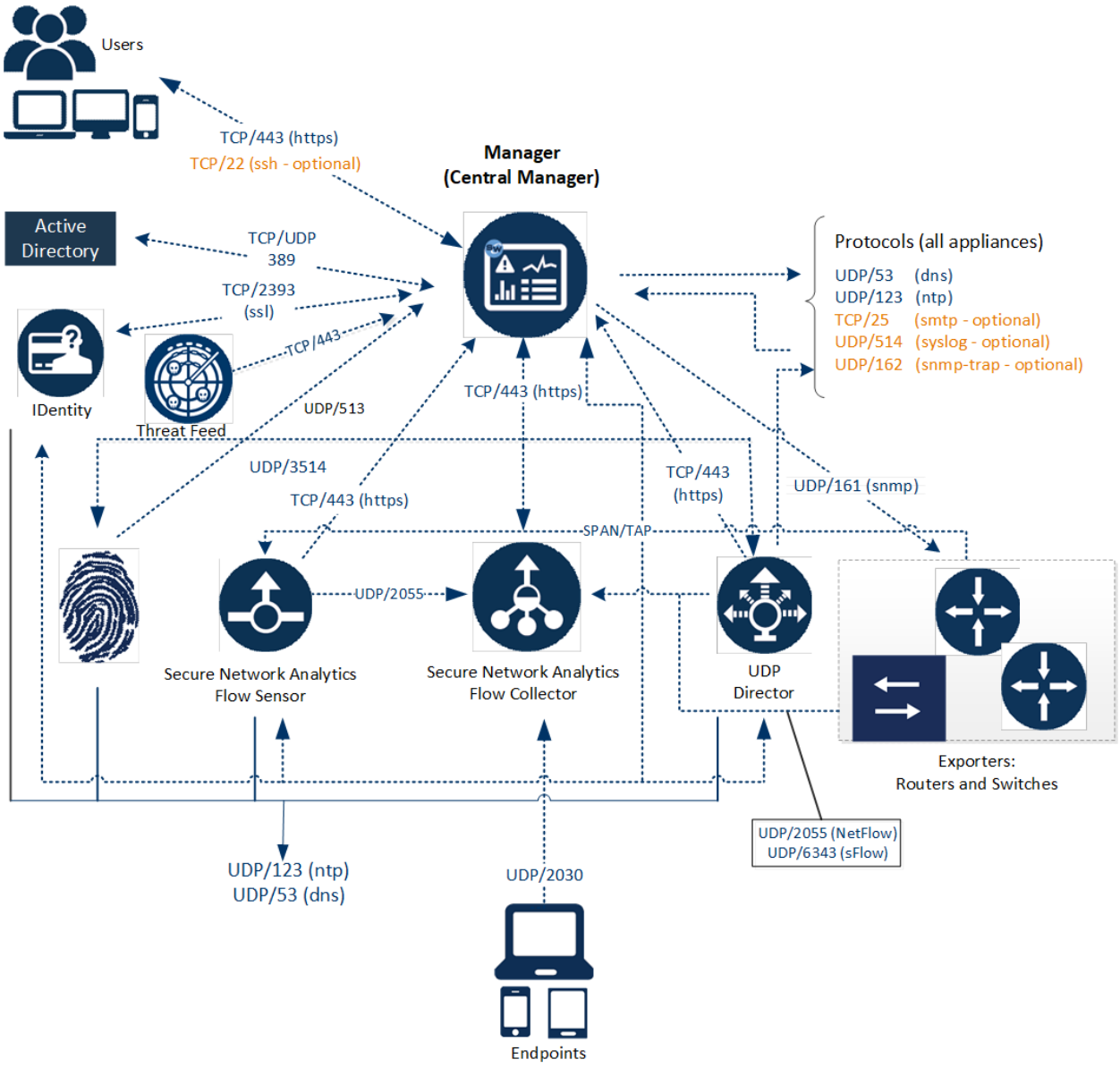
オプションの通信ポート

次の表に、ネットワーク要件によって決まる任意の設定を示します。

送信元（クライアント）	宛先（サーバ）	ポート	プロトコル
すべてのアプライアンス	ユーザー PC	TCP/22	SSH
Manager	サードパーティのイベント管理システム	UDP/162	SNMP – トラップ
Manager	サードパーティのイベント管理システム	UDP/514	SYSLOG
Manager	電子メール ゲートウェイ	TCP/25	SMTP
Manager	脅威フィード	TCP/443	SSL
ユーザー PC	すべてのアプライアンス	TCP/22	SSH

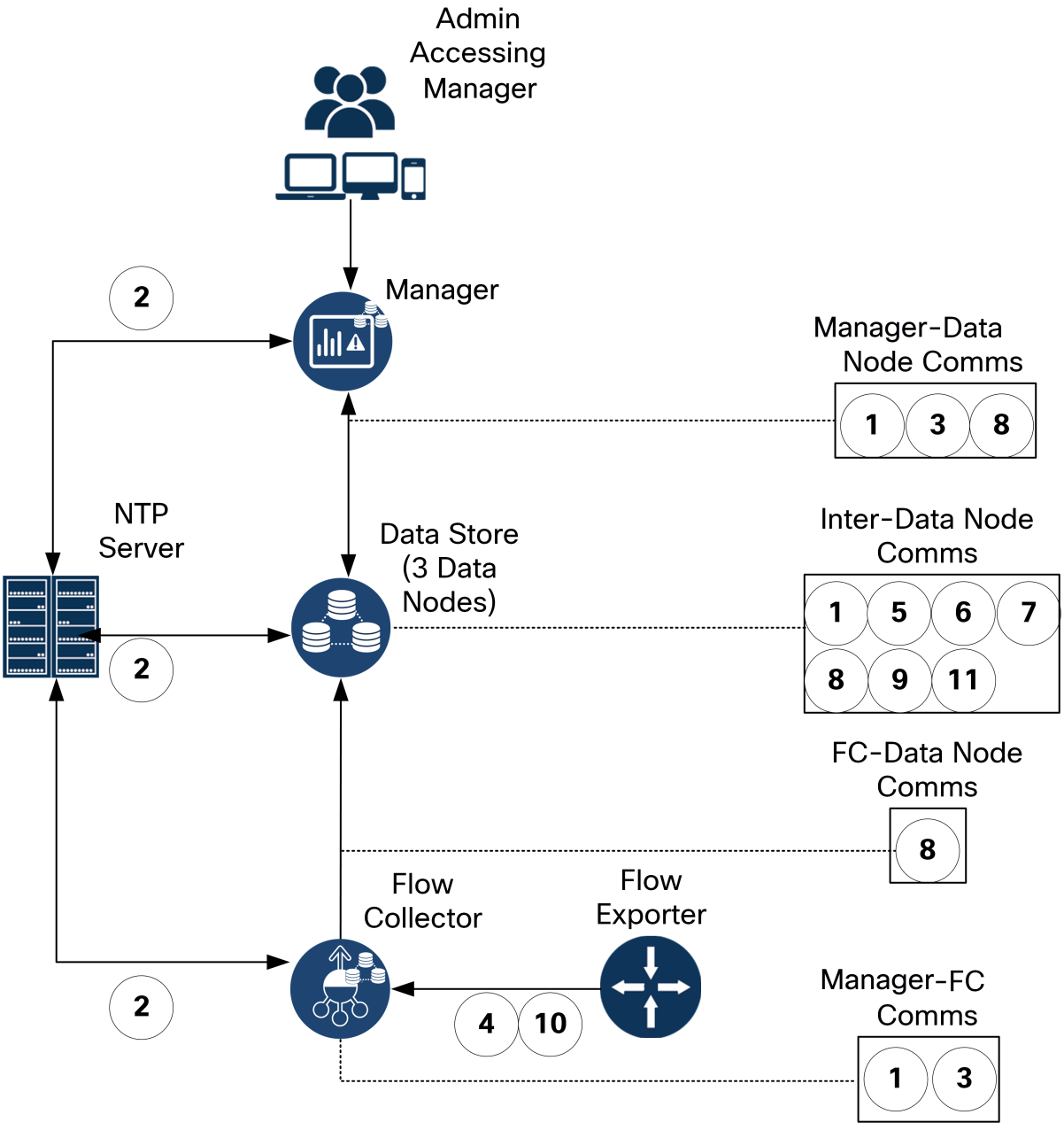
Cisco Secure Network Analytics の展開の例

次の図は、Secure Network Analytics システムによって使用されるさまざまな接続を示しています。これらのポートの一部はオプションです。



Data Store ありの Cisco Secure Network Analytics の展開の例

以下の図に示すように、Secure Network Analytics アプライアンスは、内部ネットワーク、ネットワーク周辺、または DMZ 内のいずれであっても、ネットワーク全体で重要なネットワークセグメントの最適なカバレッジが提供されるように戦略的に展開することができます。



2. Virtual Edition インストールファイルのダウンロード

次の手順に従って、仮想アプライアンスのインストール用の ISO ファイルをダウンロードします。

インストールファイル

仮想マシン	アプライアンス インストール ファイル	詳細
3a. VMware vCenter	ISO	VMware vCenter を使用して仮想アプライアンスをインストールします。
3b. VMware ESXi スタンドアロンサーバー	ISO	ESXi スタンドアロンホストサーバーに仮想アプライアンスをインストールします。
3c. KVM および Virtual Machine Manager	ISO	KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールします。

1. Cisco Software Central へのログイン

1. https://software.cisco.com で Cisco Software Central にログインします。
2. [ダウンロードと管理(Download and manage)] > [ダウンロードとアップグレード(Download and Upgrade)] セクションで、[ダウンロードにアクセス(Access downloads)] を選択します。
3. [製品の選択(Select a Product)] フィールドが表示されるまで下にスクロールします。
4. Secure Network Analyticsファイルには、次の 2 つの方法でアクセスできます。

    - **名前で検索**:[製品の選択(Select a Product)] フィールドに Secure Network Analytics と入力します。Enter を押します。
    - **メニューで検索**:[すべてを参照(Browse All)] をクリックします。[セキュリティ(Security)] > [ネットワークの可視性とセグメンテーション(Network Visibility and Segmentation)] > **[Secure Analytics]**(**[Stealthwatch]**)の順に選択します。

2. ファイルをダウンロードする

1. アプライアンスタイプを選択します。

    - Secure Network Analytics Virtual Manager
    - Secure Network Analytics 仮想 Flow Collector
    - Secure Network Analytics 仮想 Flow Sensor
    - Secure Network Analytics 仮想 UDP Director
    - Secure Network Analytics 仮想 Data Store

2. [Secure Network Analyticsシステムソフトウェア（System Software）] を選択します。
3. [最新リリース（Latest Release）] 列で、[7.4.2]（またはインストールする 7.4.x のバージョン）を選択します。
4. **ダウンロード**：ISO インストールファイルを見つけます。[ダウンロード（Download）] アイコンまたは [カートに追加（Add to Cart）] アイコンをクリックします。
5. この手順を繰り返して、アプライアンスタイプごとにファイルをダウンロードします。

3a. VMware vCenter を使用した仮想アプライアンスのインストール（ISO）

概要

VMware vCenter を使用して仮想アプライアンスをインストールするには、次の手順に従います。別の方法を使用する場合は、次を参照してください。

- VMware ESXi スタンドアロンサーバー：「**3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）**」を使用します。
- KVM：「**3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**」を使用します。

> Secure Network Analytics v7.4.2 は、VMware 7.0 または 8.0 と互換性があります。VMware 6.0、6.5、または 6.7 と Secure Network Analytics v7.4.x はサポートしていません。詳細については、『vSphere 6.0, 6.5 ,and 6.7 End of General Support』の VMware のマニュアルを参照してください。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. 互換性：「**互換**」の互換性要件を確認します。
2. リソース要件：「**リソース要件**」の項を確認し、アプライアンスに必要な割り当てを決定します。リソース プールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。詳細については、「**1. 通信用ファイアウォールの設定**」を参照してください。
4. ファイル：アプライアンスの ISO ファイルをダウンロードします。手順については、「**2. Virtual Edition インストールファイルのダウンロード**」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。正しくない場合、仮想アプライアンスを起動できないことがあります。

> Secure Network Analytics アプライアンスと同じ物理クラスタ/システムに信頼できない物理マシンまたは仮想マシンをインストールしないでください。

> すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

vCenter（ISO）を使用した仮想アプライアンスのインストール

VMware vCenter（または同様の環境）がある場合は、次の手順を使用し、ISO を使用して仮想アプライアンスをインストールします。

Data Node または Flow Sensor を展開する場合は、必要な手順のすべてを完了していることを確認してください。

データノード

次の手順を実行します。

1. Data Node 間通信用の独立 LAN の設定。

3. 仮想アプライアンスのインストール」に進みます。Data Node 仮想アプライアンスをインストールするときは、2 つのネットワークアダプタもインストールする必要があります。

Flow Sensor

次の手順を実行します。

2. トラフィックを監視する Flow Sensor の設定

3. 仮想アプライアンスのインストール

4. 追加モニターリング ポートの定義（Flow Sensor のみ）

その他すべてのアプライアンス

アプライアンスが Data Node または Flow Sensor でない場合は、次の手順を実行します。

3. 仮想アプライアンスのインストール

> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. Data Node 間通信用の独立 LAN の設定

Data Node Virtual Edition をネットワークに展開する場合は、Data Node 間通信用の **eth1** を介して Data Node が相互に通信できるように、仮想スイッチを使用して独立 LAN を設定します。

スイッチの設定には 2 つのオプションがあります。

- **vSphere 標準スイッチの設定**
- **vSphere 分散スイッチの設定**

vSphere 標準スイッチの設定

1. VMware ホスト環境にログインします。
2. vSphere 標準スイッチの設定については、VMware の vSphere 標準スイッチの作成に関するドキュメント [英語] に従ってください。手順 4 では、[標準スイッチ（Standard Switch）] オプションの [仮想マシンポートグループ（Virtual Machine Port Group）] を選択することに注意してください。
3. 次の項に進みます。「**3. 仮想アプライアンスのインストール**」に進みます。

vSphere 分散スイッチの設定

1. VMware ホスト環境にログインします。
2. vSphere 分散スイッチの設定については、VMware の vSphere 分散スイッチの作成に関するドキュメント [英語] に従ってください。手順 5a のアップリンクの数には、少なくとも 1 つのアッ

プリンクが必要ですが、複数のホストにノードを分散させる場合でない限り、アップリンクを設定する必要はありません。複数のホストにノードを分散する必要がある場合は、シスコ サポート にお問い合わせください。

3. 次の項に進みます。「**3. 仮想アプライアンスのインストール**」に進みます。

2. トラフィックを監視する Flow Sensor の設定

Flow Sensor Virtual Edition には VMware 環境を可視化する機能があり、フロー非対応領域のフローデータを生成できます。各ハイパーバイザホスト内部にインストールされる仮想アプライアンスとして、Flow Sensor Virtual Edition はホスト vSwitch からイーサネットフレームを受動的にキャプチャし、カンバセーションペア、ビットレート、パケットレートに関係する貴重なセッション統計を含むフローレコードを確認および作成します。

> 監視する環境内の各ホストにフローセンサーをインストールする必要があります。

次の手順に従って、vSwitch 上のトラフィックを監視するよう、Flow Sensor Virtual Edition を次のように設定します。

- **複数のホストでの vSwitch の監視**
- **単一のホストでの vSwitch の監視**

PCI パススルーによる外部トラフィックのモニターリング

また、準拠する PCI パススルーを使用して直接ネットワークモニタリング用に Flow Sensor Virtual Edition を設定することもできます。

- **要件**：igb/ixgbe 準拠 または e1000e 準拠の PCI パススルー。
- **リソース情報**：「**Flow Sensor Virtual Edition**」を参照してください。
- **統合**：「**1. 通信用ファイアウォールの設定**」を参照してください。
- **手順**：Flow Sensor Virtual Edition に PCI ネットワーク インターフェイスを追加するには、VMware のマニュアルを参照してください。

複数のホストでの vSwitch の監視

Flow Sensor Virtual Edition を使用して、複数の VM ホストまたはクラスタにわたる分散 vSwitch 上のトラフィックを監視するには、このセクションの手順に従います。

このセクションの内容は、VDS ネットワークにのみ該当します。VDS 以外の環境内にネットワークがある場合は、「**単一のホストでの vSwitch の監視**」に進みます。

設定要件

> 監視する環境内の各ホストにフローセンサーをインストールする必要があります。

この設定には、次の要件があります。

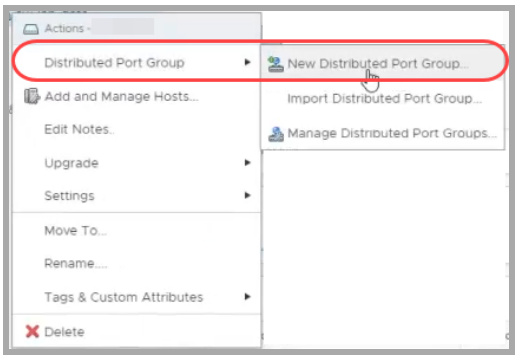
- 分散仮想ポート（dvPort）：適切な VLAN 設定を行った dvPort グループを Flow Sensor Virtual Edition で監視する各 VDS に追加します。Flow Sensor Virtual Edition がネットワーク上の VLAN と VLAN 以外両方のトラフィックを監視する場合は、それぞれのタイプに 1 つずつ、2 つの dvPort グループを作成する必要があります。
- VLAN ID：環境で VLAN（VLAN トランキングまたはプライベート VLAN 以外）を使用している場合、この手順を実行するには VLAN ID が必要です。

- 無差別モード：有効。
- 無差別ポート：vSwitch に設定。

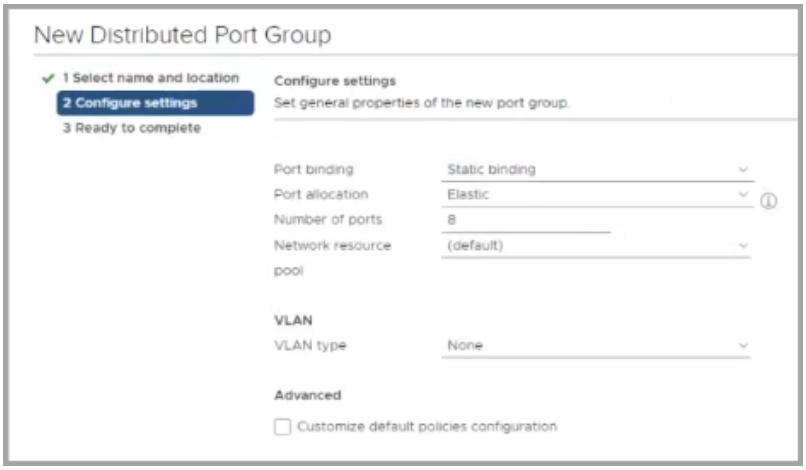
VDS を使用してネットワークを設定するには次の手順を実行します。

1. [ネットワーキング（Networking）] アイコンをクリックします。

2. [ネットワーキング（Networking）] ツリーで、VDS を右クリックします。
3. [分散ポートグループ（Distributed Port Group）] > [新規分散ポートグループ（New Distributed Port Group）] を選択します。



4. [新規分散ポートグループ（New Distributed Port Group）] ダイアログボックスを使用して、次の手順の仕様を含めてポートグループを設定します。
5. [名前と場所の選択（Select Name and Location）]：[名前（Name）]フィールドに、この dvPort グループを識別する名前を入力します。
6. [設定構成（Configure Settings）]：[ポート数（Number of Ports）] フィールドに、ホストクラスタ内の Flow Sensor Virtual Edition の数を入力します。

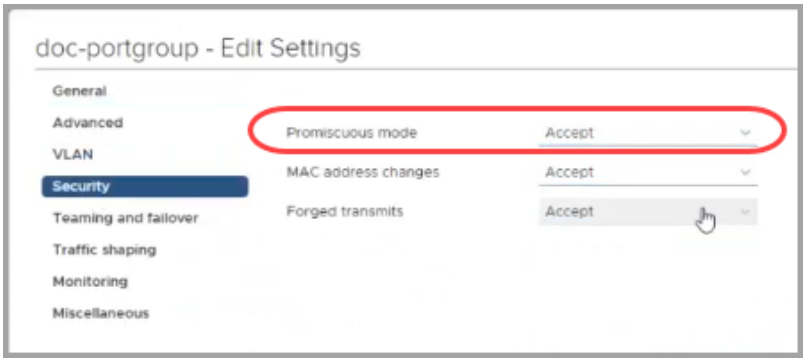


7. [VLANタイプ（VLAN type）]ドロップダウンリストをクリックします。

   - 環境内で VLAN を使用しない場合は、[なし（None）]を選択します。
   - 環境内で VLAN を使用する場合は、VLAN タイプを選択します。次のように設定します。

VLAN タイプ	詳細
VLAN	[VLAN ID] フィールドに、ID に一致する番号（1 ～ 4094）を入力します。
VLAN トランキング	すべての VLAN トラフィックを監視するには、[VLANトランク範囲（VLAN trunk range）]フィールドに **0–4094** と入力します。
プライベート VLAN	ドロップダウンリストから [無差別（Promiscuous）]を選択します。

8. [終了準備の完了（Ready to Complete）]：設定を確認します。[終了（Finish）]をクリックします。
9. [ネットワーキング（Networking）]ツリーで、新しい dvPort グループを右クリックします。[設定の編集（Edit Settings）]を選択します。
10. [セキュリティ（Security）]を選択します。
11. [無差別モード（Promiscuous Mode）]ドロップダウンリストをクリックします。[許可（Accept）]を選択します。



12. [OK] をクリックして、ダイアログボックスを閉じます。
13. Flow Sensor Virtual Edition で VLAN と VLAN 以外両方のネットワークトラフィックを監視しますか。

    - 両方を監視する場合は、この「**複数のホストでの vSwitch の監視**」セクションの手順を繰り返します。
    - 「いいえ」の場合は、次の手順に進みます。

14. VMware 環境に Flow Sensor Virtual Edition で監視する別の VDS はありますか。

    - 別の VDS がある場合は、この「**複数のホストでの vSwitch の監視**」の項の手順を次の VDS で繰り返します。

15. 次の項に進みます。「**3. 仮想アプライアンスのインストール**」に進みます。

単一のホストでの vSwitch の監視

Flow Sensor Virtual Edition を使用して、単一ホストの vSwitch 上のトラフィックを監視するには、このセクションの手順に従います。

> このセクションの内容は、非 VDS ネットワークにのみ該当します。VDS をネットワークで使用している場合は、「**複数のホストでの vSwitch の監視**」に進みます。

設定要件

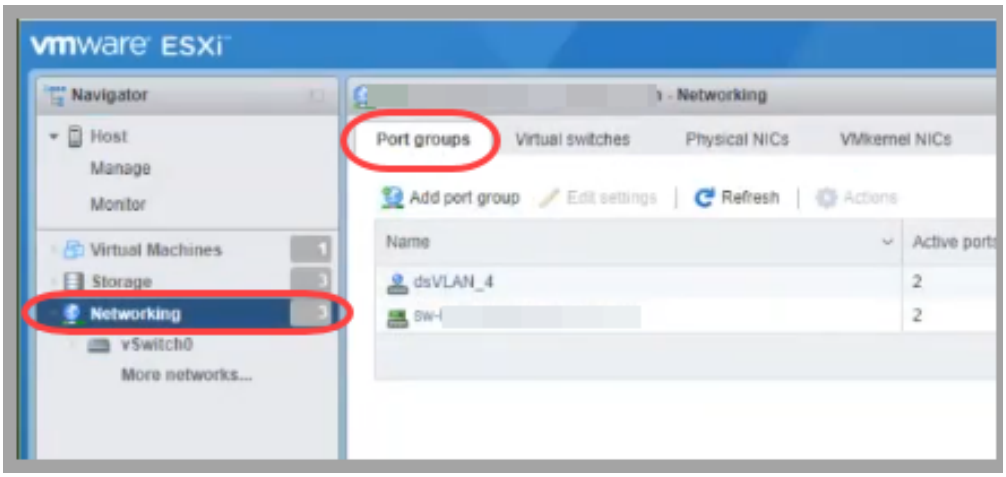
この設定には、次の要件があります。

- **無差別ポートグループ**：Flow Sensor Virtual Edition で監視する各仮想スイッチに無差別ポートグループを追加します。
- **無差別モード**：有効。
- **無差別ポート**：vSwitch に設定。

ポートグループの無差別モードへの設定

次の手順を使用してポートグループを追加するか、ポートグループを編集して、[無差別（Promiscuous）] に設定します。

1. VMware ESXi ホスト環境にログインします。
2. [ネットワーキング（Networking）] をクリックします。



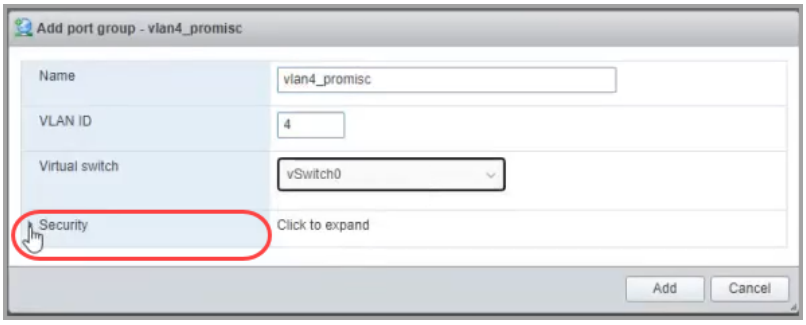
3. [ポートグループ（Port groups）] タブを選択します。
4. 新しいポートグループを作成したり、ポートグループを編集したりできます。

- [ポートグループの作成（Create Port Group）]：[ポートグループの追加（Add port group）] をクリックします。
- [ポートグループの編集（Edit Port Group）]：ポートグループを選択します。[設定の編集（Edit Settings）] をクリックします。

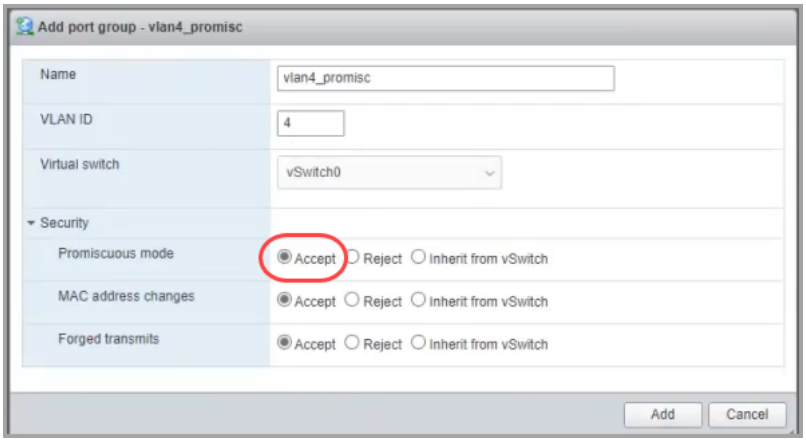
5. ダイアログボックスを使用して、ポートグループを設定します。VLAN ID または VLAN トランキングを設定します。

VLAN タイプ	詳細
VLAN ID（Admin. VLAN ID）	VLAN ID を使用して単一の VLAN を指定します。 [VLAN ID] フィールドに、ID に一致する番号（1 ～ 4094）を入力します。
VLAN トランキング	VLAN トランキングを使用して、すべての VLAN トラフィックをモニターします。デフォルトの範囲は 0 ～ 4095 です。

6. [セキュリティ（Security）] 矢印をクリックします。



7. [無差別モード（Promiscuous mode）]：[承諾（Accept）] を選択します。



8. Flow Sensor Virtual Edition でこの VMware 環境内の別の仮想スイッチを監視しますか。

「はい」の場合は、「**2. トラフィックを監視する Flow Sensor の設定**」に戻り、すべての手順を次の仮想スイッチで繰り返します。

9. 次の項に進みます。「**3. 仮想アプライアンスのインストール**」

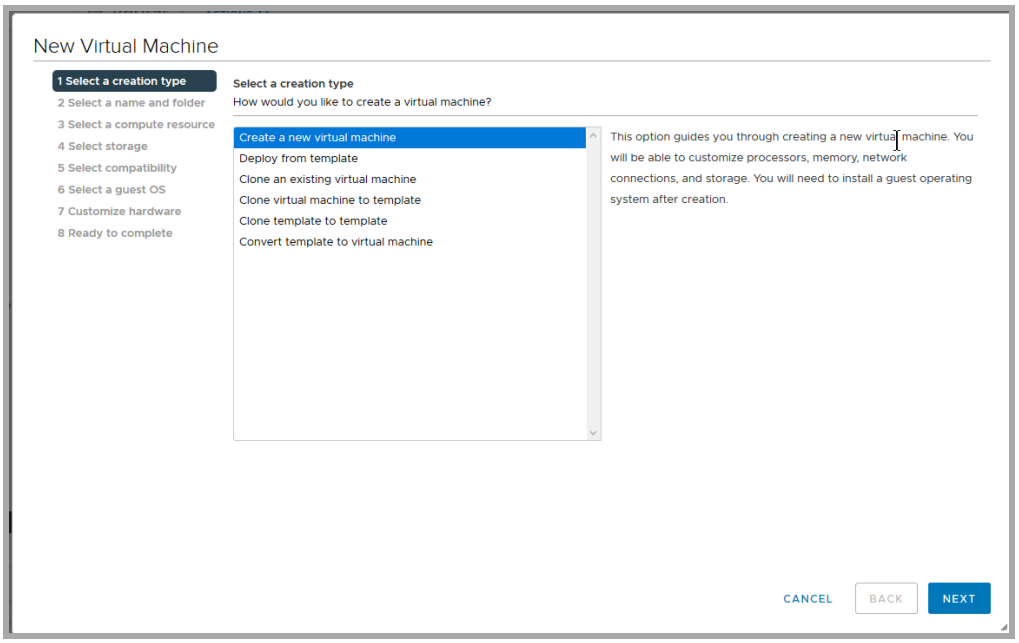
3. 仮想アプライアンスのインストール

仮想アプライアンスをハイパーバイザ ホストにインストールし、仮想アプライアンスの管理およびモニターリング ポートを定義するには、次の手順を実行します。

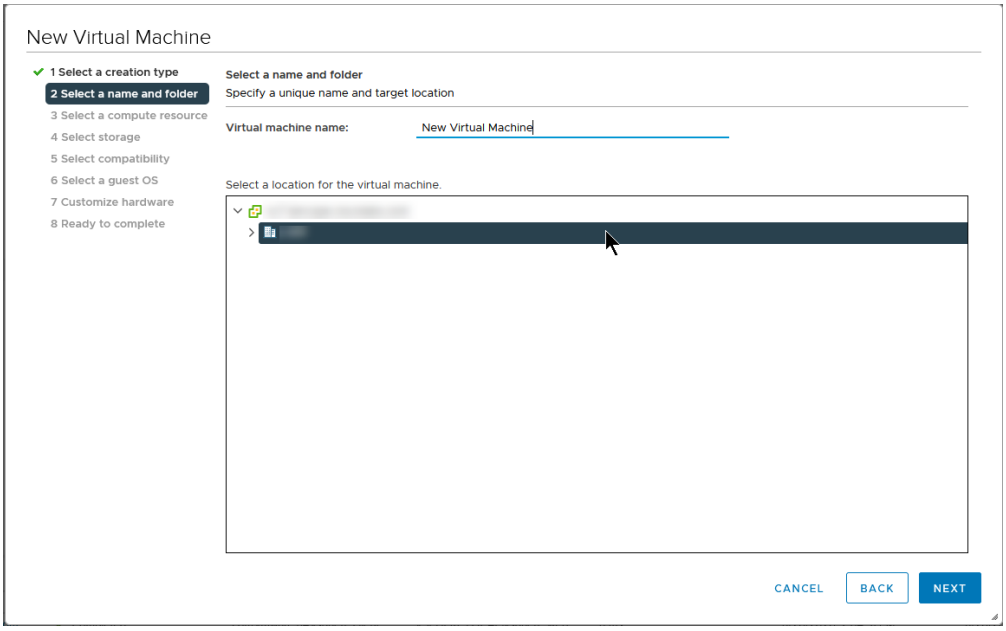
> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. VMware Web クライアントにログインします。
2. Cisco Software Central からダウンロードした仮想アプライアンス ソフトウェア ファイル（ISO）を見つけます。
3. vCenter で ISO を使用できるようにします。次の選択肢があります。
   - vCenter データストアに ISO をアップロードします。
   - コンテンツライブラリに ISO を追加します。
   - ローカルワークステーションに ISO を保持し、そのファイルを参照するように展開を設定します。

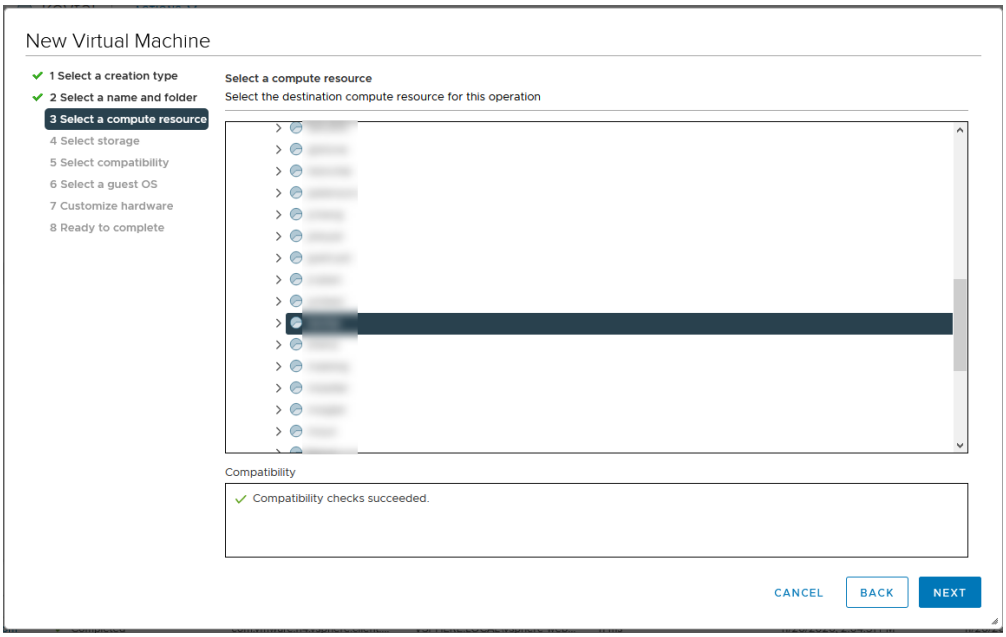
   詳細については、VMware のマニュアルを参照してください。
4. vCenter UI から、[メニュー（Menu）] > [ホストとクラスタ（Hosts and Clusters）] の順に選択します。
5. ナビゲーションウィンドウで、クラスタまたはホストを右クリックし、[新規仮想マシン（New Virtual Machine ...）] を選択して [新規仮想マシン（New Virtual Machine）] ウィザードにアクセスします。
6. [作成タイプの選択（Select a creation type）] ウィンドウで、[新しい仮想マシンの作成（Create a new virtual machine）] を選択し、[次へ（Next）] をクリックします。



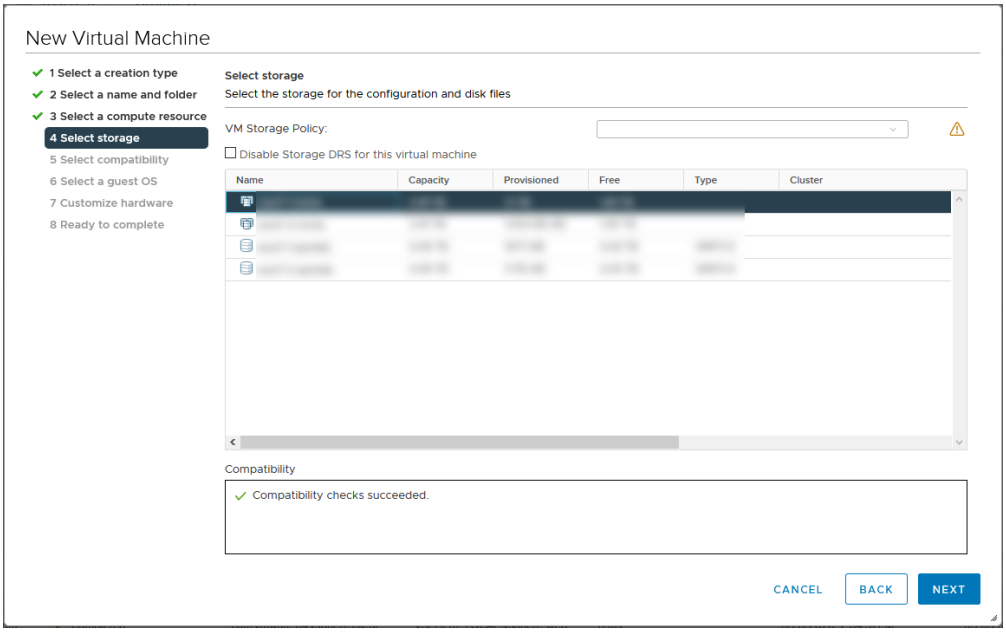
7. [名前とフォルダの選択（Select a name and folder）] ウィンドウで、[仮想マシン名（Virtual machine name）] を入力し、仮想マシンの場所を選択して、[次へ（Next）] をクリックします。



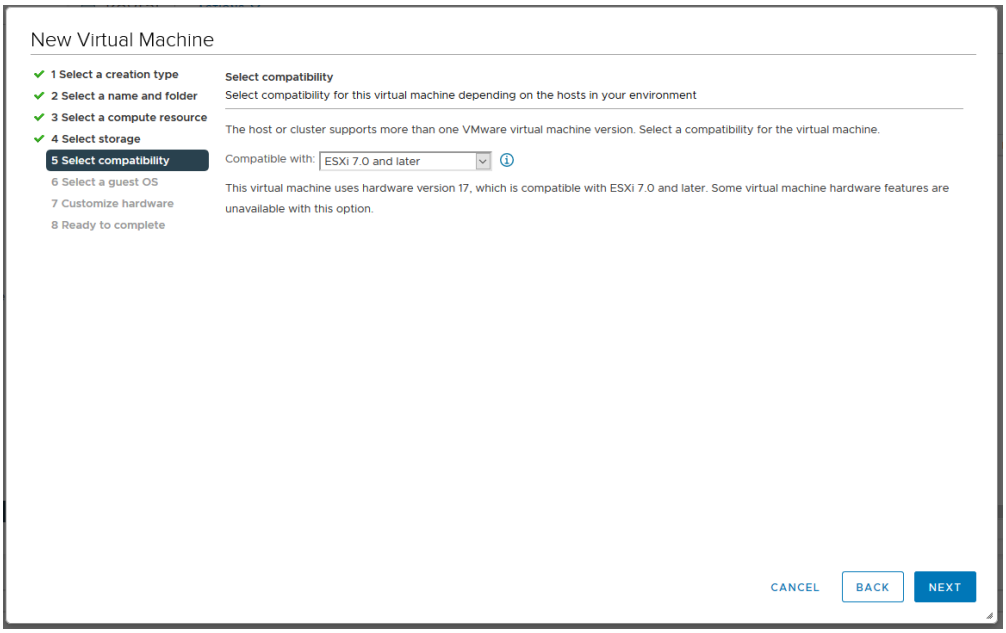
8. [コンピューティングリソースの選択（Select a compute resource）] ウィンドウで、アプライアンスを展開するクラスタ、ホスト、リソースプール、vApp を選択し、[次へ（Next）] をクリックします。



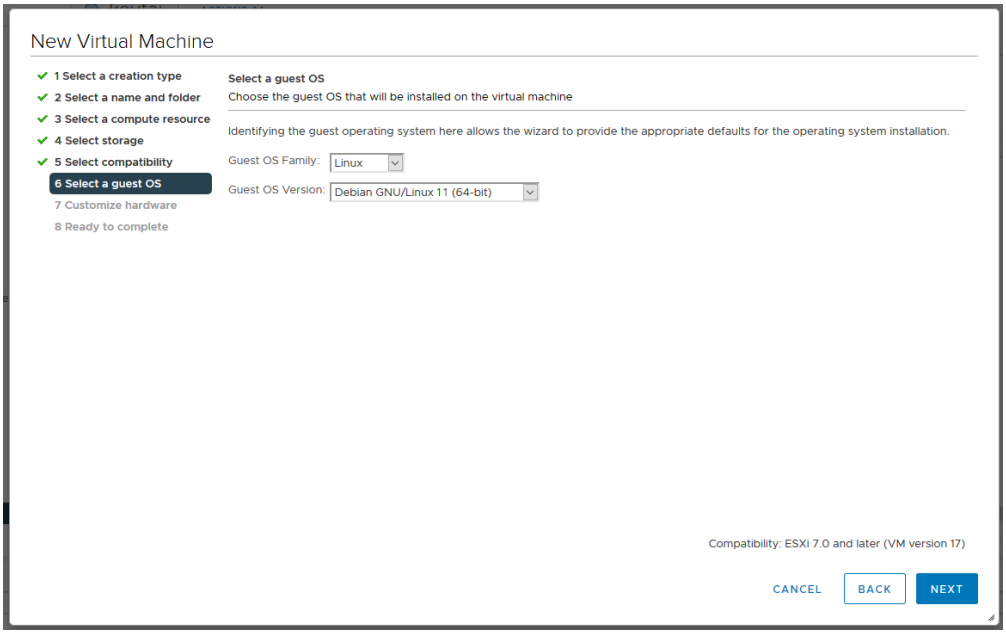
9. [ストレージの選択（Select storage）] ウィンドウで、ドロップダウンから [VMストレージポリシー（VM Storage Policy）] を選択し、保存場所を選択して [次へ（Next）] をクリックします。



10. [互換性の選択（Select compatibility）] ウィンドウで、現在展開されている ESXi バージョンに基づいて、[次と互換：（Compatible with）] ドロップダウンから仮想マシンのバージョンを選択します。たとえば、次のスクリーンショットでは、ESXi 7.0 が展開されているため [ESXi 7.0以降（ESXi 7.0 and later）] を選択しています。[次へ（Next）] をクリックします。



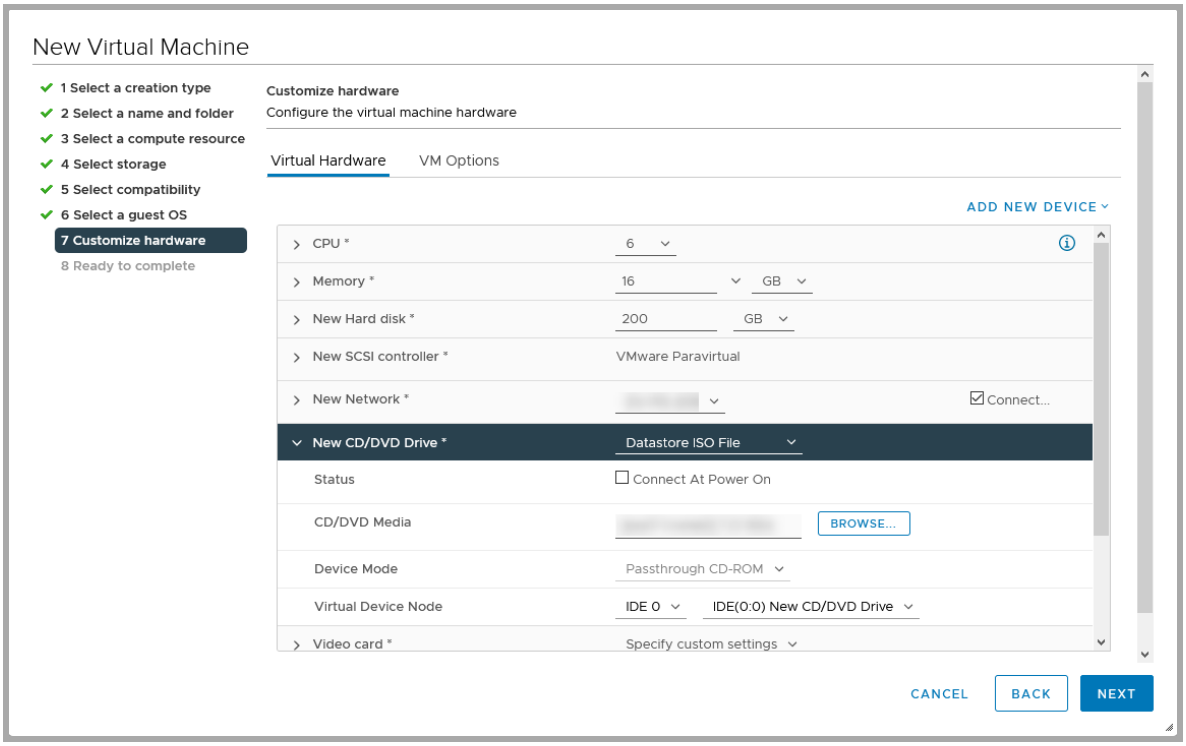
11. [ゲストOSの選択（Select a guest OS）] 画面で、[Linux ゲストOSファミリ（Linux Guest OS Family）] として [ゲストOSバージョン（Guest OS Version）] として [Debian GNU/Linux 11（64 ビット）（Debian GNU/Linux 11 (64-bit)] を選択します。 [次へ（Next）] をクリックします。



12. [ハードウェアのカスタマイズ（Customize hardware）] ウィンドウで、仮想ハードウェアを設定します。アプライアンスタイプに固有の推奨事項については、「**リソース要件**」を参照してください。

> ⚠ この手順は、システムパフォーマンスにとって重要です。必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライア

ンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。



リソース要件に加えて、次の設定が選択されていることを確認します。

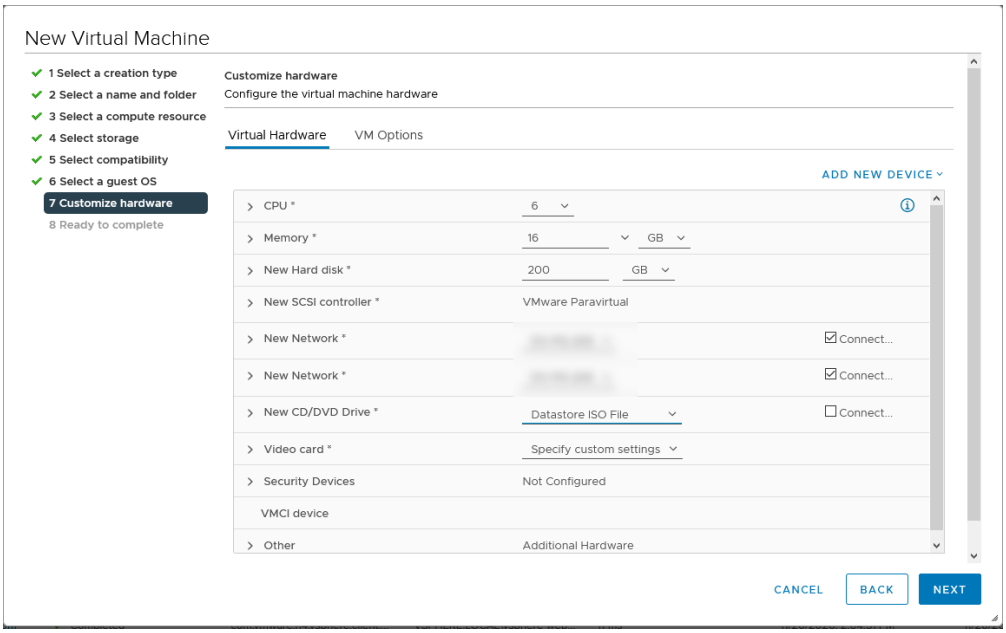
- [新しいハードディスク（New Hard disk）] をクリックして、構成オプションを展開します。[ディスクプロビジョニング（Disk Provisioning）] ドロップダウンから [シックプロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] を選択します。
- [新しいSCSIコントローラ（New SCSI controller）] をクリックして、構成オプションを展開します。[タイプの変更（Change Type）] ドロップダウンから [LSI論理SAS（LSI Logic SAS）] を選択します。[LSI論理SAS（LSI Logic SAS）] を選択しないと、仮想アプライアンスが正しく展開されない可能性があります。
- [新しいCD/DVDドライブ（New CD/DVD Drive）] フィールドで、ISO を保存した場所に基づいて ISO の場所を選択します。[新しいCD/DVDドライブ（New CD/DVD Drive）] をクリックして、構成オプションを展開します。[電源投入時に接続（Connect At Power On）] をオンにします。
- **アプライアンスが Flow Sensor で、**NIC に 10 Gbps スループットを設定している場合は、[CPU] をクリックして構成オプションを展開します。すべての CPU が 1 つのソケットに収まるように、[ソケットあたりのコア数（Cores per Socket）] を設定します。

13. **Data Node**：Data Node 仮想アプライアンスを展開する場合は、2 番目のネットワークアダプタも追加します。

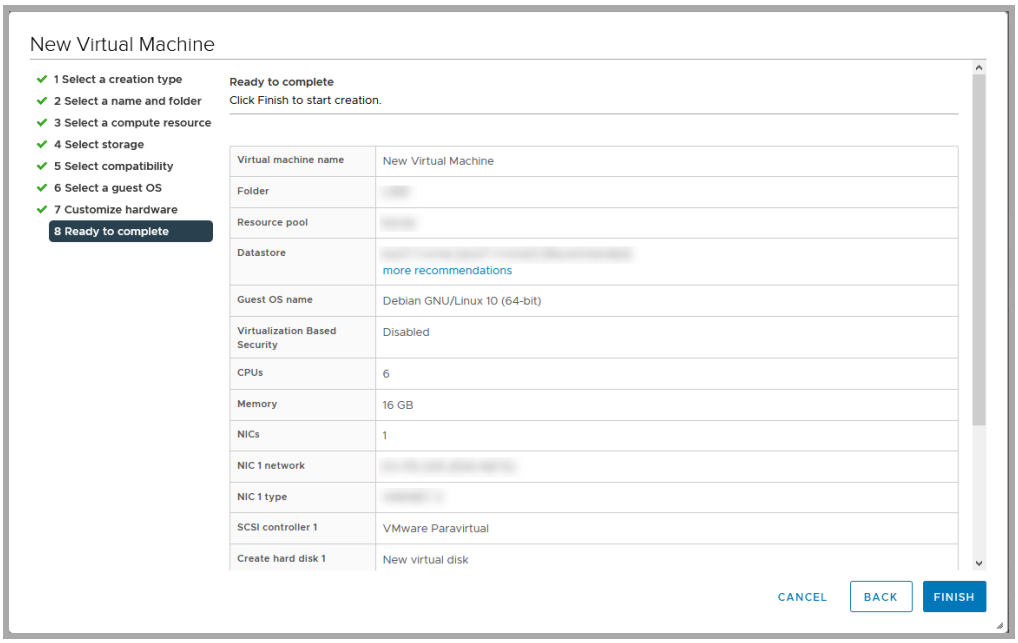
    [新しいデバイスの追加（Add New Device）] をクリックしてから [ネットワークアダプタ（Network Adapter）] を選択し、[アダプタタイプ（Adapter Type）] が [VMXNET3] であることを確認します。

- **1 番目のネットワークアダプタ**では、Data Node Virtual Edition がパブリックネットワーク上で他のアプライアンスと通信できるようにするスイッチを選択します。
- **2 番目のネットワークアダプタ**では、Data Node Virtual Edition がプライベートネットワーク上で他の Data Node と通信できるようにするスイッチとして、「**1. Data Node 間通信用の独立 LAN の設定**」で作成したスイッチを選択します。

展開内のすべての Data Node について、それぞれの Data Node を展開する際に、ネットワークアダプタと仮想スイッチを適切に割り当てるようにしてください。



14. [完了の準備（Ready to complete）] ウィンドウで、設定を確認し、[完了（FINISH）] をクリックします。



15. [電源オン（Power On）] アイコンをクリックすると、展開が開始されます。[最近のタスク（Recent Tasks）] セクションで展開の進行状況をモニターします。次の手順に進む前に、展開が完了し、インベントリツリーに表示されていることを確認します。
16. 次の手順：

- **Flow Sensor**：アプライアンスが Flow Sensor であり、VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合は、次のセクション「**4. 追加モニターリング ポートの定義（Flow Sensor のみ）**」に進みます。
- **その他すべてのアプライアンス**：このセクション（「**3. 仮想アプライアンスのインストール**」）のすべての手順を繰り返して他の仮想アプライアンスを展開します。

17. システム内ですべての仮想アプライアンスのインストールを完了した場合は、「**4. Secure Network Analytics システムの設定**」に進みます。

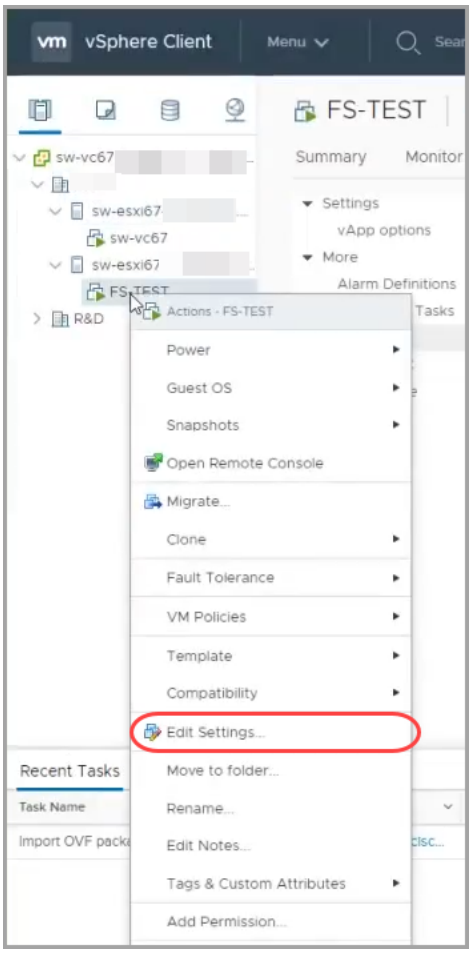
4. 追加モニターリング ポートの定義（Flow Sensor のみ）

この手順が必要となるのは、Flow Sensor Virtual Edition が VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合です。

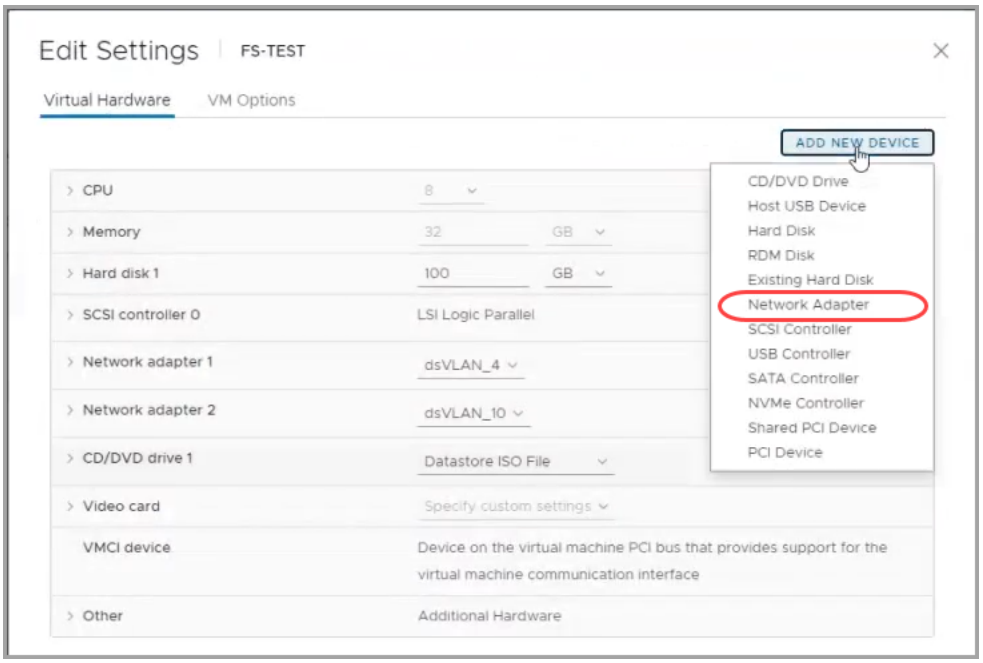
> Flow Sensor でこのようなモニタリング設定を行っていない場合、この手順を完了する必要はありません。

Flow Sensor Virtual Edition モニタリングポートを追加するには、次の手順を実行します。

1. インベントリツリーで Flow Sensor Virtual Edition を右クリックします。[設定の編集（Edit Settings）] を選択します。

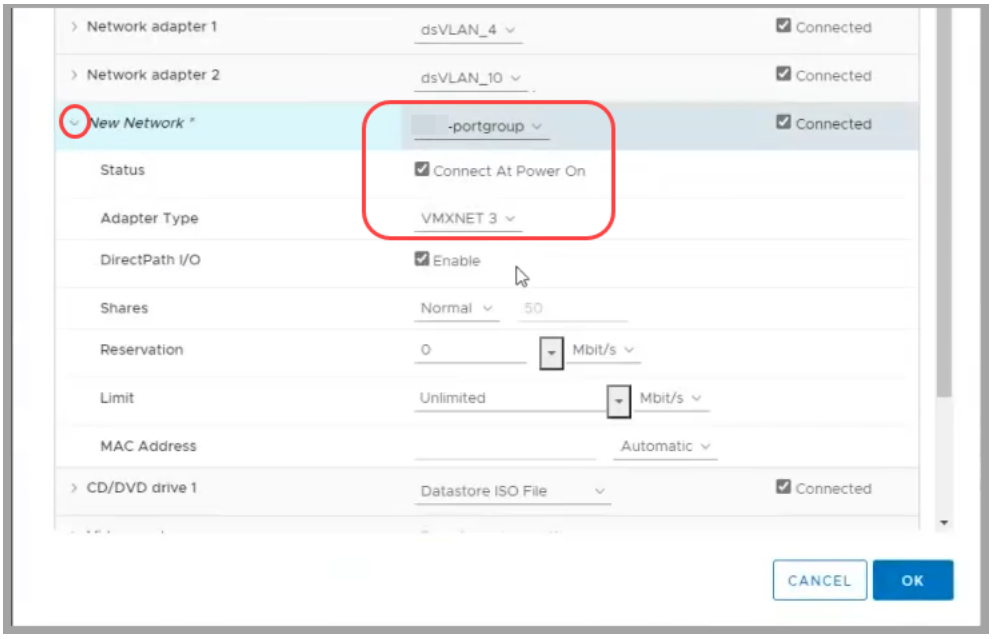


2. [設定の編集（Edit Settings）] ダイアログボックスを使用して、次の指定された設定を構成します。
3. [新規デバイスの追加（Add New Device）] をクリックします。[ネットワークアダプタ（Network Adapter）] を選択します。



4. 新しいネットワークアダプタを見つけます。矢印をクリックしてメニューを展開し、次の内容を設定します。

   - **[新規ネットワーク（New Network）]**：未割り当ての無差別ポートグループを選択します。
   - **[アダプタのタイプ（Adapter Type）]**：[VMXNET 3] を選択します。
   - **[ステータス（Status）]**：[パワーオン時に接続（Connect at Power On）] チェックボックスをオンにします。



5. 設定を確認後、[OK] をクリックします。
6. 必要に応じて別のイーサネットアダプタを追加する場合は、この手順を繰り返します。
7. 次の手順：

- [フローセンサー（Flow Sensor）]：別の Flow Sensor を設定するには、「**2. トラフィックを監視する Flow Sensor の設定**」に進みます。
- その他すべてのアプライアンス：このセクション（「**3. 仮想アプライアンスのインストール**」）のすべての手順を繰り返して他の仮想アプライアンスを展開します。
- システム内ですべての仮想アプライアンスのインストールを完了した場合は、「**4. Secure Network Analytics システムの設定**」に進みます。

3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）

概要

ESXi スタンドアロンサーバーを備えた VMware 環境を使用して仮想アプライアンスをインストールするには、次の手順に従います。

> Secure Network Analytics v7.4.2 は、VMware v7.0 または 8.0 と互換性があります。VMware v6.0、v6.5、または v6.7 と Secure Network Analytics v7.4.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。

別の方法を使用する場合は、次を参照してください。

- VMware vCenter：「**3a. VMware vCenter を使用した仮想アプライアンスのインストール（ISO）**」を使用します。
- KVM：「**3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**」を使用します。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. 互換性：「**互換**」の互換性要件を確認します。
2. リソース要件：「**リソース要件**」の項を確認し、アプライアンスに必要な割り当てを決定します。リソース プールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。詳細については、「**1. 通信用ファイアウォールの設定**」を参照してください。
4. ファイル：アプライアンスの ISO ファイルをダウンロードします。手順については、「**2. Virtual Edition インストールファイルのダウンロード**」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。正しくない場合、仮想アプライアンスを起動できないことがあります。

> Secure Network Analytics アプライアンスと同じ物理クラスタ/システムに信頼できない物理マシンまたは仮想マシンをインストールしないでください。

> すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

ESXi スタンドアロンサーバーへの仮想アプライアンス（ISO）のインストール

ESXi スタンドアロンサーバーを備えた VMware 環境を使用して仮想アプライアンスをインストールするには、次の手順に従います。

プロセスの概要

仮想アプライアンスのインストールでは、この章で説明する次の手順を実行する必要があります。

1. VMware Web Client へのログイン
2. ISO からの起動

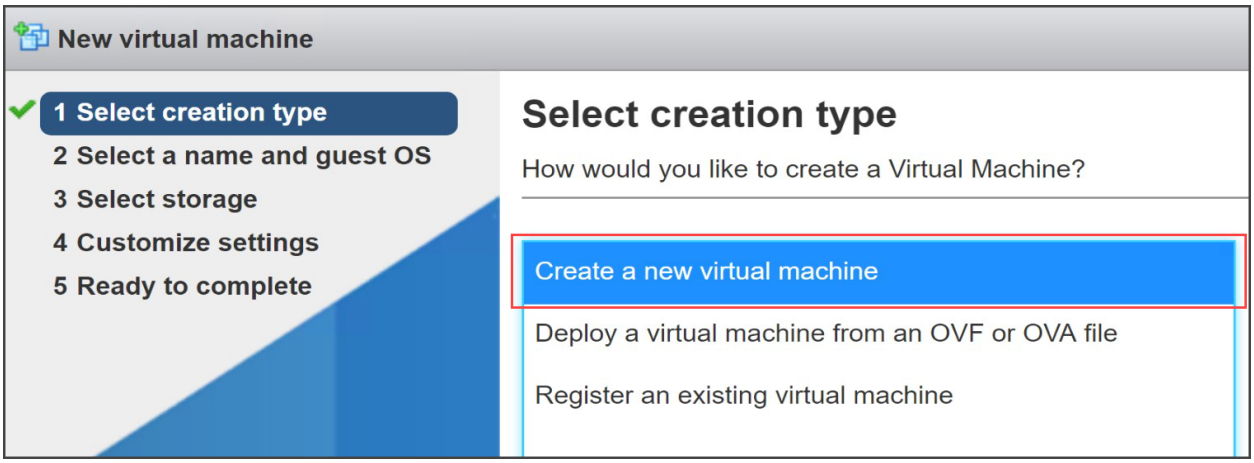
データノード

Data Node を展開する場合は、前述のセクション「1. Data Node 間通信用の独立 LAN の設定」の手順を実行してからこのセクションの手順を完了します。

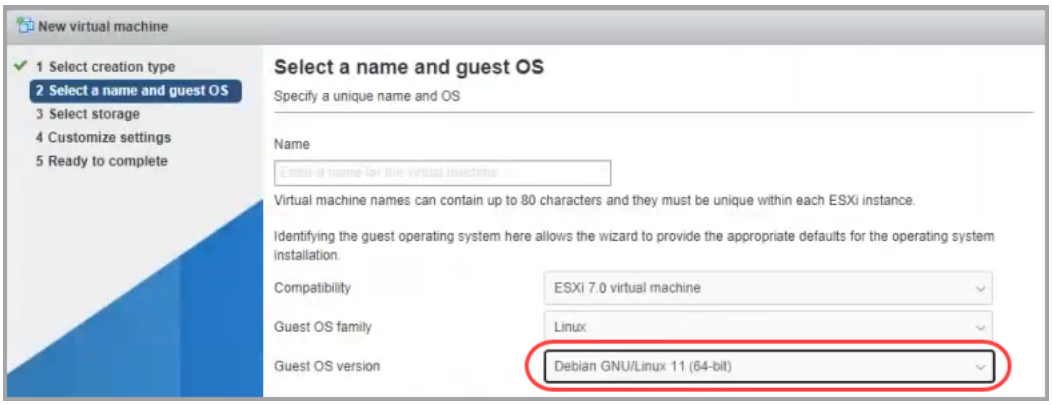
1. VMware Web Client へのログイン

> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

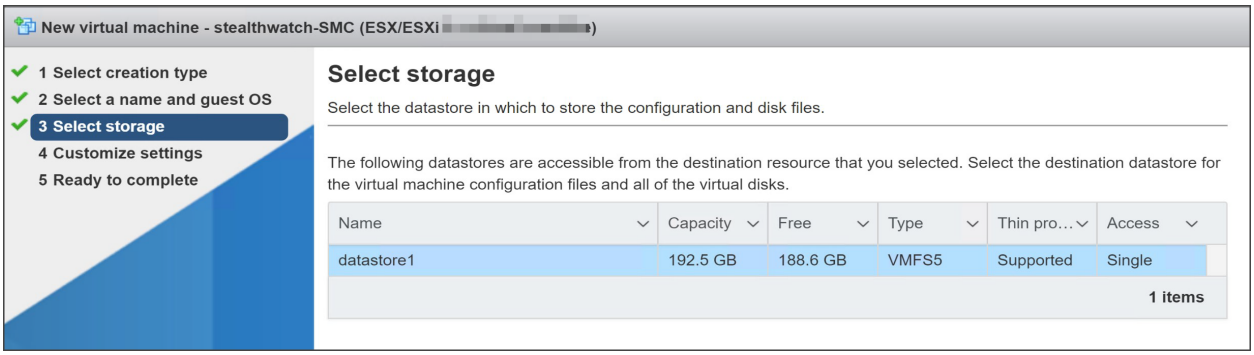
1. VMware Web Client にログインします。
2. [仮想マシンの作成/登録（Create/Register a Virtual Machine）] をクリックします。
3. [新規仮想マシン（New Virtual Machine）] ダイアログボックスを使用して、次の手順で指定されているようにアプライアンスを設定します。
4. 作成タイプの選択（Select Creation Type）：[新しい仮想マシンの作成（Create a New Virtual Machine）] を選択します。



5. ゲスト OS と名前の選択（Select a Name and Guest OS）：次の情報を入力または選択します。
   - 名前（Name）：簡単に識別できるようにアプライアンスの名前を入力します。
   - 互換性（Compatibility）：使用するバージョン（v7.0 または 8.0）を選択します。
   - ゲスト OS ファミリ（Guest OS family）：Linux。
   - ゲスト OS バージョン（Guest OS version）：[Debian GNU/Linux 11（64ビット）（Debian GNU/Linux 11 64-bit）] を選択します。



6. [ストレージの選択（Select Storage）]：アクセス可能なデータストアを選択します。「リソース要件」を確認して、十分な容量があることを確認します。



> ⚠ 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

7. **設定のカスタマイズ（Customize Settings）**：アプライアンス要件を入力または選択します（詳細については「リソース要件」を参照してください）。

   次の値を選択したことを確認します。

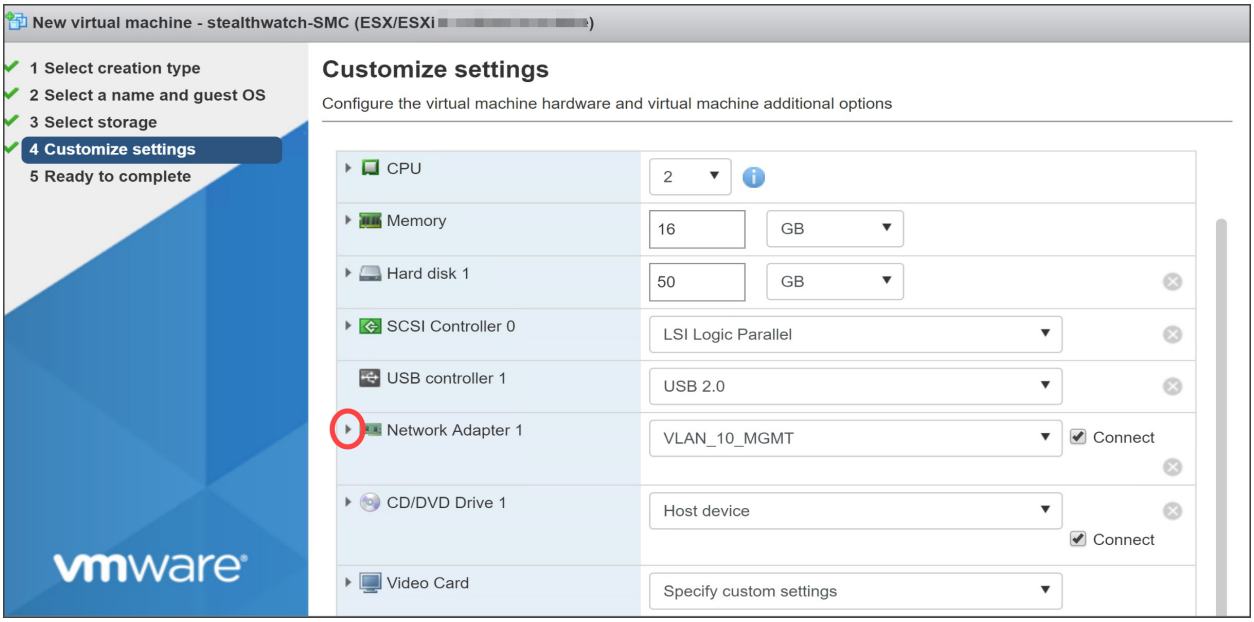
   - **SCSI コントローラ**：[LSI論理SAS（LSI Logic SAS）]
   - **ネットワーク アダプタ（Network Adapter）**：アプライアンスの管理アドレスを確認します。
   - **ハードディスク**：[シックプロビジョニング（Lazy Zeroed）（Thick Provisioning Lazy Zeroed）]

     アプライアンスが Flow Sensor の場合は、[ネットワークアダプタの追加（Add Network Adapter）]をクリックして別の管理またはセンシングインターフェイスを追加できます。

アプライアンスが Flow Sensor で、NIC に 10 Gbps スループットを設定している場合は、[CPU] をクリックして構成オプションを展開します。すべての CPU を 1 つのソケットに設定します。

アプライアンスが Data Node の場合、Data Node 間通信を可能にするために別のネットワーク インターフェイスを追加します。[ネットワークアダプタの追加（Add Network Adapter）] をクリックします。

- **1 番目のネットワークアダプタ**では、Data Node Virtual Edition がパブリックネットワーク上で他のアプライアンスと通信できるようにするスイッチを選択します。
- **2 番目のネットワークアダプタ**では、Data Node Virtual Edition がプライベートネットワーク上で他の Data Node と通信できるようにするスイッチとして、「1. Data Node 間通信用の独立 LAN の設定」で作成したスイッチを選択します。



8. ネットワーク アダプタの横にある矢印をクリックします。
9. [アダプタのタイプ（Adapter Type）] で、[VMXnet3] を選択します。

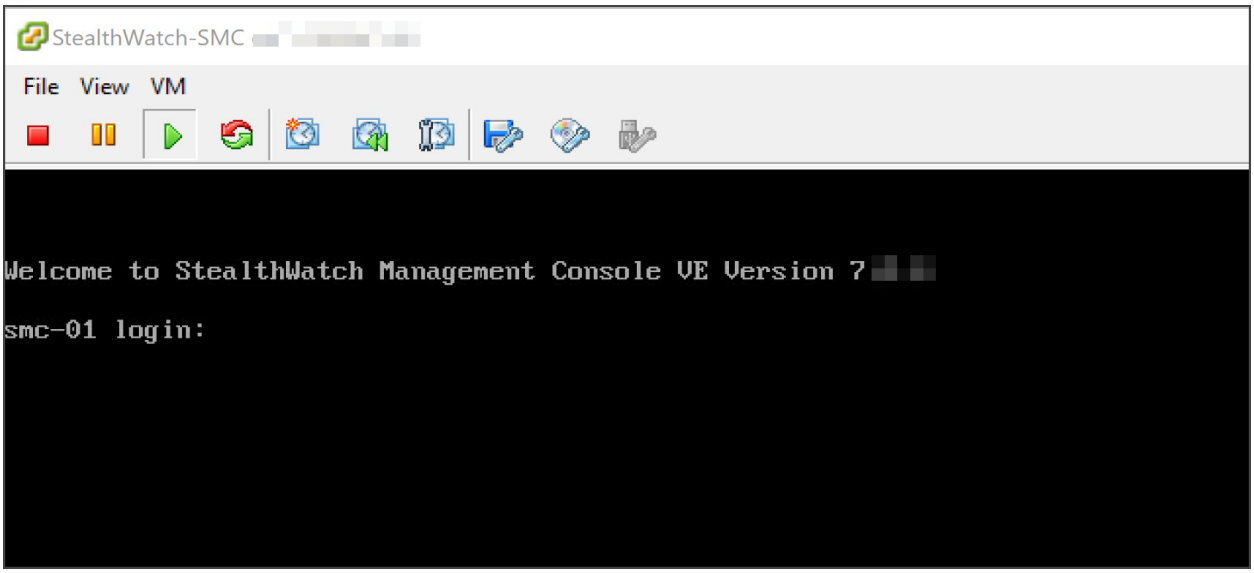
> シスコは、E1000（1G dvSwitch）、1G PCI パススルー、および VMXNET 3 インターフェイスの使用をサポートしていますが、シスコの仮想アプライアンスに最高のネットワークパフォーマンスをもたらすことが証明されている、VMXNET3 インターフェイスを使用することを強くお勧めします。

10. 設定を確認し、それらが正しいことを確認します。
11. [終了（Finish）] をクリックします。仮想マシン コンテナが作成されます。

2. ISO からの起動

1. VMware コンソールを開きます。
2. 新しい仮想マシンに ISO を接続します。詳細については、VMware のガイドを参照してください。

3. ISO から仮想マシンを起動します。インストーラが実行され、自動的に再起動します。
4. インストールと再起動が完了すると、ログイン プロンプトが表示されます。



5. 仮想マシンから ISO を切断します。
6. 次の仮想アプライアンスに対して、「3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）」のすべての手順を繰り返します。
7. **Flow Sensor**: アプライアンスが Flow Sensor の場合は、このマニュアルの前述のセクションを参照してセットアップを完了します。

    - 2. トラフィックを監視する Flow Sensor の設定（「単一のホストでの vSwitch の監視」を参照）
    - Flow Sensor が VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合は、「4. 追加モニターリング ポートの定義（Flow Sensor のみ）」に進みます。

8. システム内ですべての仮想アプライアンスのインストールを完了した場合は、「4. Secure Network Analytics システムの設定」に進みます。

3c. KVM ホストへの仮想アプライアンスのインストール（ISO）

概要

KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールするには、次の手順に従います。

別の方法を使用する場合は、次を参照してください。

- VMware vCenter：「3a. VMware vCenter を使用した仮想アプライアンスのインストール（ISO）」を使用します。
- VMware ESXi スタンドアロンサーバー：「3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）」を使用します。

> Linux KVM は、さまざまな KVM ホストバージョンでテストおよび検証されています。Secure Network Analytics バージョン 7.3.1 以降でテストおよび検証された KVM コンポーネントの詳細なリストについては、「KVM」を参照してください。

はじめる前に

インストールを始める前に、次の手順を完了してください。

1. 互換性：「互換」の互換性要件を確認します。
2. リソース要件：「リソース要件」の項を確認し、アプライアンスに必要な割り当てを決定します。リソース プールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。詳細については、「1. 通信用ファイアウォールの設定」を参照してください。
4. ファイル：アプライアンス ISO ファイルをダウンロードし、それを KVM ホストのフォルダにコピーします。このセクションで提供される例では、次のフォルダを使用します：var/lib/libvirt/image。手順については、「2. Virtual Edition インストールファイルのダウンロード」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。正しくない場合、仮想アプライアンスを起動できないことがあります。

> Secure Network Analytics アプライアンスと同じ物理クラスタ/システムに信頼できない物理マシンまたは仮想マシンをインストールしないでください。

KVM ホストへの仮想アプライアンスのインストール（ISO）

KVM ホストがある場合は、次の手順に従い、ISO を使用して仮想アプライアンスをインストールします。

プロセスの概要

仮想アプライアンスのインストールでは、この章で説明する次の手順を実行する必要があります。

Data Node の独立 LAN の設定

1. KVM ホストへの仮想アプライアンスのインストール

2. Open vSwitch への NIC（Data Node、Flow Sensor）および無差別ポートモニタリングの追加（Flow Sensor のみ）

Data Node の独立 LAN の設定

Data Node Virtual Edition をネットワークに展開する場合は、Data Node 間通信用の **eth1** を介して Data Node が相互に通信できるように、仮想スイッチを使用して独立 LAN を設定します。独立 LAN の作成の詳細については、仮想スイッチのマニュアルを参照してください。

1. KVM ホストへの仮想アプライアンスのインストール

ISO ファイルを使用して KVM ホストに仮想マシンをインストールする方法はいくつかあります。次の手順で、Ubuntu ボックスで実行する Virtual Machine Manager という GUI ツールを使用して仮想 Manager をインストールする一例を示します。互換性のある Linux ディストリビューションを使用できます。互換性の詳細については、「**互換**」を参照してください。

トラフィックのモニターリング

Flow Sensor Virtual Edition には KVM 環境を可視化する機能があり、フロー非対応領域のフローデータを生成できます。各 KVM ホスト内部にインストールされる仮想アプライアンスとして、Flow Sensor Virtual Edition は監視対象のトラフィックからイーサネットフレームを受動的にキャプチャし、カンバセーションペア、ビットレート、およびパケットレートに関係する貴重なセッション統計を含むフローレコードを作成します。

設定要件

この設定には次の要件があります。

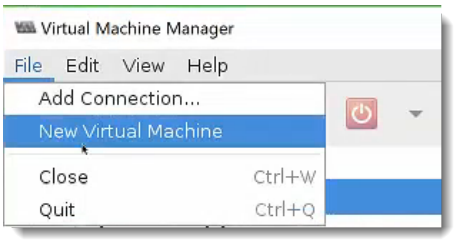
- 無差別モード：有効
- 無差別ポート：Open vSwitch に設定

> KVM ホストに仮想アプライアンスをインストールするには、virt-manager 2.2.1 を使用することをお勧めします。

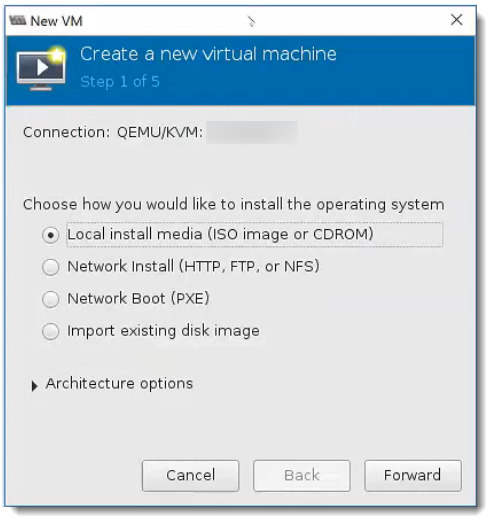
KVM ホストへの仮想アプライアンスのインストール

仮想アプライアンスをインストールし、Flow Sensor Virtual Edition を有効にしてトラフィックを監視するには、次の手順を実行します。

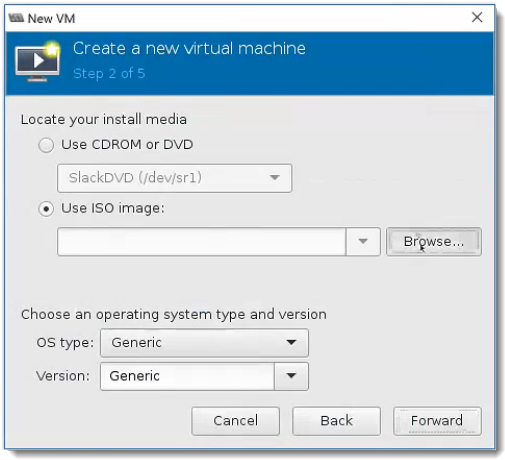
1. Virtual Machine Manager を使用して KVM ホストに接続し、次の手順に従ってアプライアンスを設定します。
2. [ファイル（File）] > [新しい仮想マシン（New Virtual Machine）] をクリックします。



3. 接続に [QEMU/KVM] を選択し、[ローカルインストールメディア（ISOイメージまたはCDROM）（Local install media (ISO image or CDROM)）] を選択します。[続行（Forward）] をクリックします。

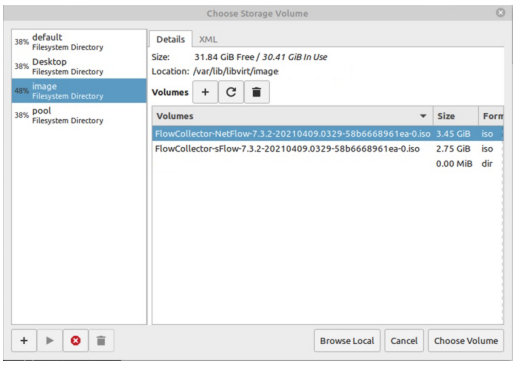


4. [参照（Browse）] をクリックして、アプライアンスイメージを選択します。

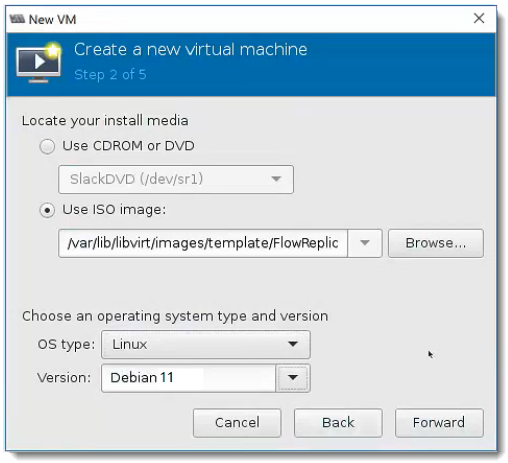


5. ISO ファイルを選択します。[ボリュームの選択（Choose Volume）] をクリックします。

   KVM ホストが ISO ファイルにアクセスできることを確認します。



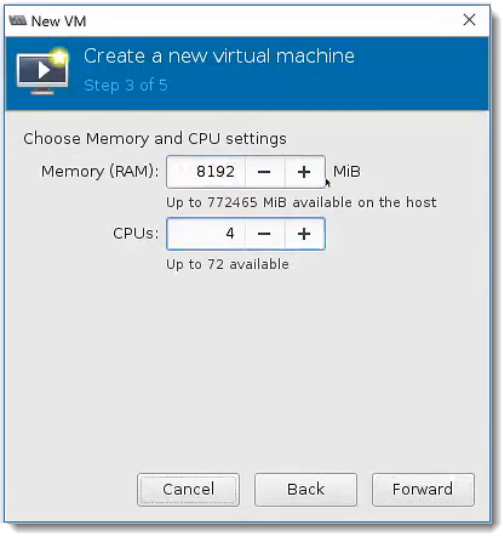
6. [インストールメディア/ソースから自動的に検出する（Automatically detect from the installation media/source）] チェックボックスをオフにします。[オペレーティングシステムタイプおよびバージョンの選択（Choose an operating system type and version）] で、「Debian」と入力し始めると表示される [Debian 11（debian 11）] オプションを選択します。[Forward] をクリックします。



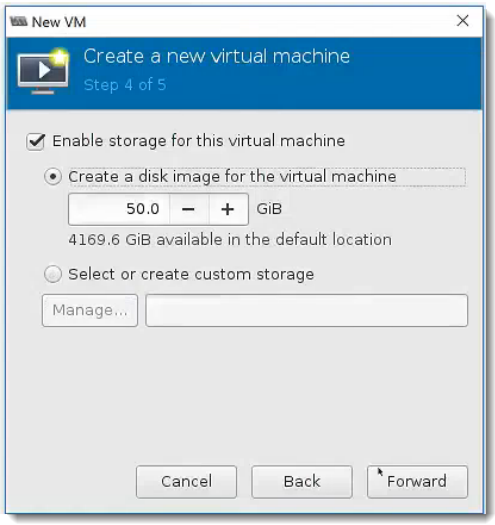
7. メモリ（RAM）と CPU を「**リソース要件**」の項に示す容量まで増やします。

「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。

⚠ 必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。



8. [仮想マシンへのディスク イメージの作成（Create a disk image for the virtual machine）] を選択します。
9. 「**リソース要件**」の項のアプライアンスに示されているデータ ストレージ容量を入力します。[Forward] をクリックします。



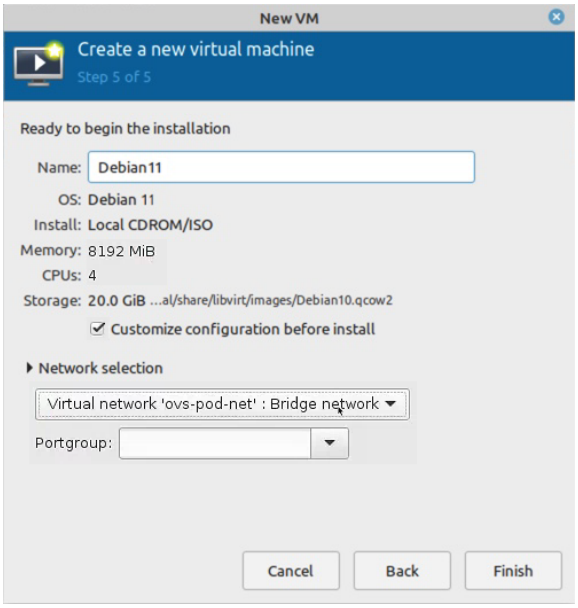
「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。

必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

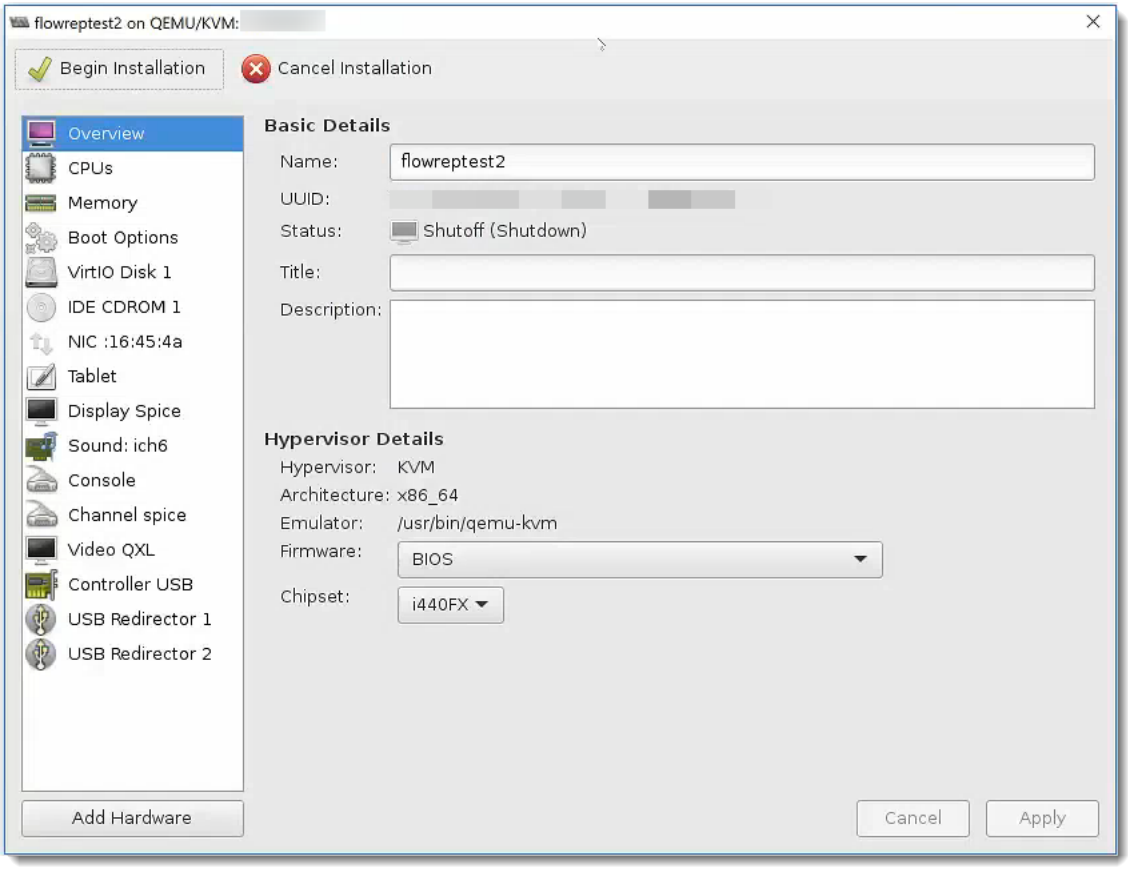
10. 仮想マシンの名前を指定します。これが表示名になるため、後で見つけやすい名前を使用してください。

11. [インストール前に構成をカスタマイズ（Customize configuration before install）] チェックボックスをオンにします。
12. [ネットワークの選択（Network selection）] ドロップダウンボックスで、インストールに適切なネットワークとポートグループを選択します。

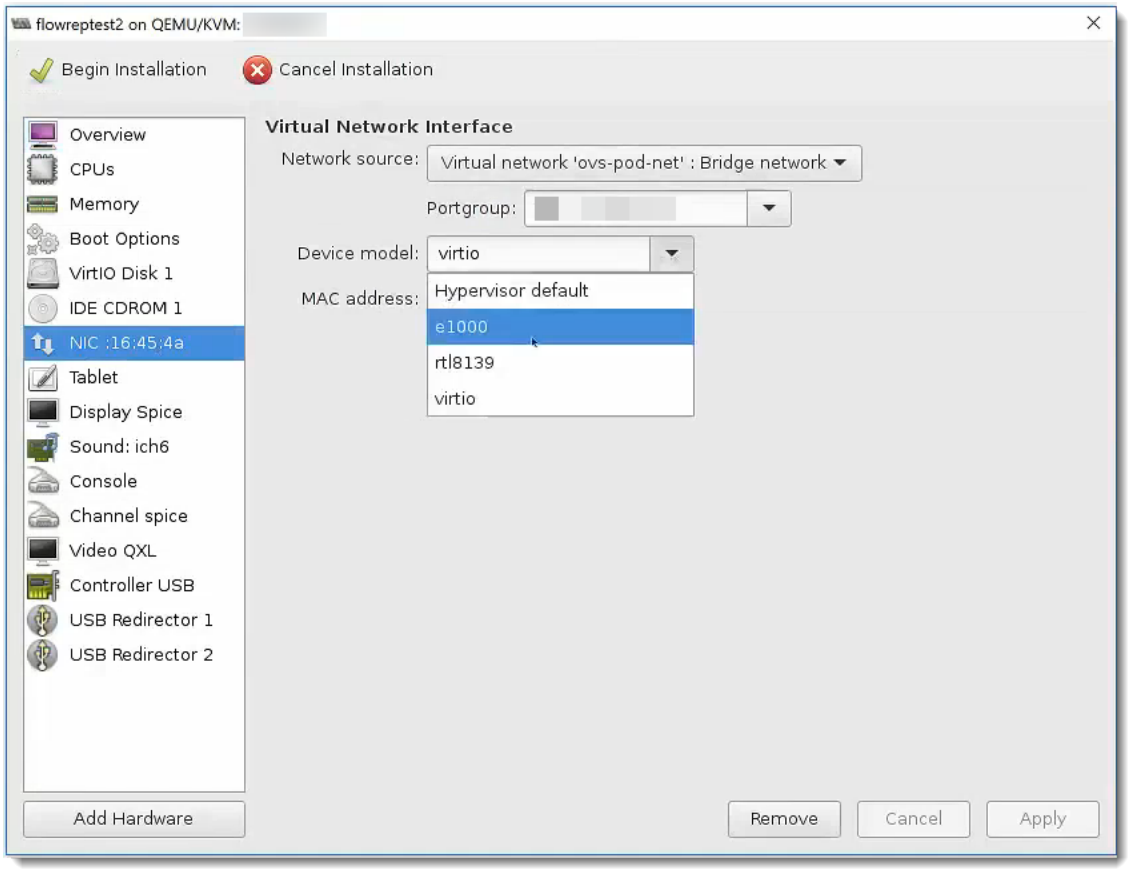
    Data Node：Data Node の場合は、Data Node がパブリックネットワーク上で他のアプライアンスと通信できるようにするネットワークおよびポートグループを選択します。



13. [終了（Finish）] をクリックします。[設定（Configuration）] メニューが開きます。



14. ナビゲーション ペインで、[NIC] を選択します。
15. [仮想ネットワーク インターフェイス（Virtual Network Interface）] の [デバイス モデル（Device model）] ドロップダウン ボックスで [e1000] を選択します。[適用（Apply）] をクリックします。



16. [VirtIO ディスク 1（VirtIO Disk 1）] をクリックします。
17. [詳細オプション（Advanced Options）] ドロップダウン リストの [ディスク バス（Disk bus）] ドロップダウン ボックスで [SCSI] を選択します。[適用（Apply）] をクリックします。
18. Flow Sensor Virtual Edition でポートを監視するために、または Data Node VE で Data Node 間通信を可能にするために、NIC を追加する必要がありますか。

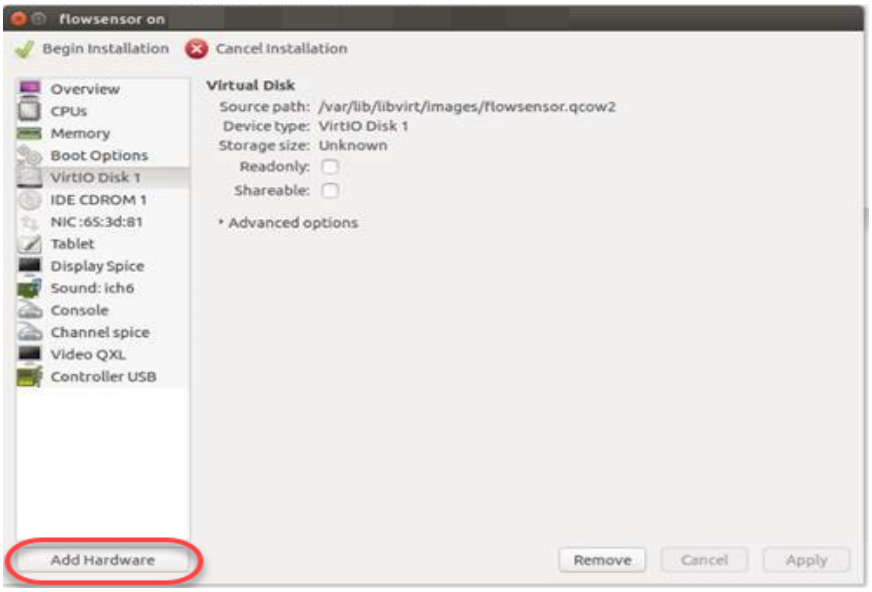
    - 「はい」の場合は、「2. Open vSwitch への NIC（Data Node、Flow Sensor）および無差別ポートモニタリングの追加（Flow Sensor のみ）」。
    - 「いいえ」の場合、次の手順に進みます。

19. [インストールの開始（Begin Installation）] をクリックします。
20. 「4. Secure Network Analytics システムの設定」に進みます。

2. Open vSwitch への NIC（Data Node、Flow Sensor）および無差別ポートモニタリングの追加（Flow Sensor のみ）

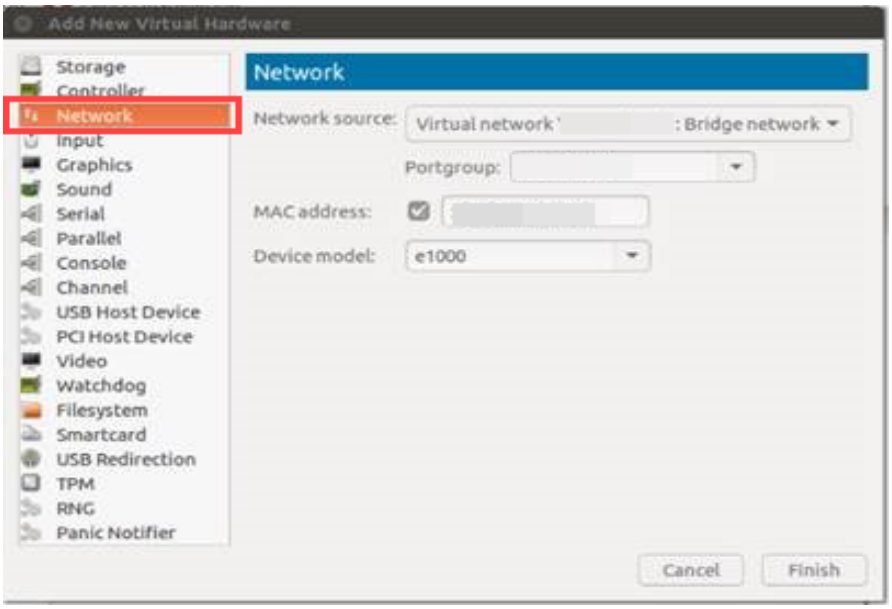
Flow Sensor Virtual Edition モニタリングポート用または Data Node Virtual Edition 用の NIC を追加してインストールを完了するには、次の手順を実行します。

1. [設定（Configuration）] メニューで、[ハードウェアの追加（Add Hardware）] をクリックします。[新規仮想ハードウェアの追加（Add New Virtual Hardware ）] ダイアログボックスが表示されます。



2. 左側のナビゲーション ウィンドウで [ネットワーク（Network）] をクリックします。

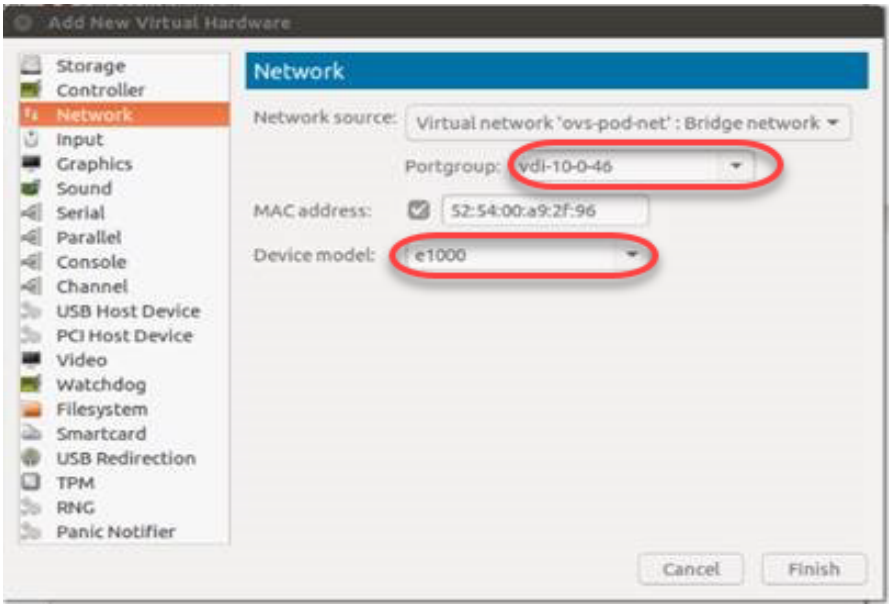
   Data Node の場合は、Data Node がパブリックネットワーク上で他のアプライアンスと通信できるようにするネットワークおよびポートグループを選択します。



3. **Flow Sensor**：フローセンサーの場合は、[ポートグループ（Portgroup）] ドロップダウンリストをクリックし、監視する未割り当ての無差別ポートグループを選択します。

   [デバイス モデル（Device Model）] ドロップダウン リストをクリックし、[e1000] を選択します。

   Data Node：Data Node の場合は、「**Data Node の独立 LAN の設定**」で作成した設定を使用して、独立 LAN での Data Node 間通信を可能にするネットワークソースを選択します。



4. [終了（Finish）] をクリックします。
5. 別の監視ポートを追加する必要がある場合は、これまでの手順を繰り返します。
6. すべての監視ポートを追加したら、[インストールの開始（Begin Installation）] をクリックします。

4. Secure Network Analytics システムの設定

Virtual Edition アプライアンスやハードウェアアプライアンスのインストールが完了したら、管理対象システムに Secure Network Analytics を構成できます。

> ⚠ Secure Network Analytics を設定するには、『Secure Network Analytics System Configuration Guide v7.4.2』の手順に従ってください。この手順は、システムの設定と通信を正常に完了させるために重要です。
>
> 必ず、システム構成ガイドで指定されている順序でアプライアンスを設定してください。

システム設定要件

ハイパーバイザホスト（仮想マシンホスト）を介してアプライアンスコンソールにアクセスできることを確認します。

次の表を使用して、各アプライアンスに必要な情報を準備します。

設定要件	詳細	アプライアンス
IPアドレス	`eth0` 管理ポートにルーティング可能な IP アドレスを割り当てます。	
ネットマスク		
ゲートウェイ		
ホスト名	アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。	
ドメイン名	各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。	
DNS サーバ	名前解決のための内部 DNS サーバー	
NTP サーバ	サーバー間同期のための内部タイムサーバー。各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。 130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。	
メールリレーサーバー	アラートと通知を送信する SMTP メールサーバー	

Flow Collector エクスポートポート	Flow Collector のみに必要です。 NetFlow のデフォルト：2055	
プライベート LAN または VLAN 内のルーティング不可能な IP アドレス（Data Node 間通信用）	Data Node のみに必要です。 • ハードウェア eth2、または eth2 と eth3 のボンディング。最大 20G のスループットを実現するボンディングされた LACP `eth2/eth3` ポートチャネルを作成すると、Data Node 間の高速な通信が可能になり、Data Store への Data Node の追加や交換が迅速になります。LACP ポートボンディングは、ハードウェア Data Node で使用できる唯一のボンディングオプションであることに注意してください。 • 仮想 eth1 **IP アドレス**：提供された IP アドレスを使用するか、Data Node 間通信の次の要件を満たす値を入力できます。 • **169.254.42.0/24 CIDR ブロック**（169.254.42.2 ～ 169.254.42.254）の**ルーティング不可能な IP アドレス** • **最初の 3 オクテット**：169.254.42 • **サブネット**：/24 • **シーケンシャル**：メンテナンスを容易にするために、連続した IP アドレス（169.254.42.10、169.254.42.11、169.254.42.12 など）を選択します。 **ネットマスク**： ネットマスクは 255.255.255.0 にハードコードされており、変更できません。	
eth0 ハードウェア接続ポート	データ ストア ハードウェア アプライアンスを使用する Secure Network Analytics でのみ必要です。 • マネージャ • Flow Collector • Data Node eth0 ハードウェア接続ポートオプション： • **SFP+**：	

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 2 月 27 日	最初のバージョン
1_1	2023 年 3 月 27 日	通信ポートとプロトコルの表を更新しました。
1_2	2023 年 3 月 27 日	タイプミスを修正しました。
1_3	2023 年 4 月 20 日	VMware サポートの説明が改善されました。これは仮想ガイドであるため、「サポートされているハードウェアメトリック」の表を削除しました。KVM ホストバージョンのサポートに関する説明が改善されました。
1_4	2023 年 8 月 15 日	メモリリソースのメモを GB から GiB に変更しました。
1_5	2023 年 4 月 27 日	VMware 8.0 のサポートが追加されました。展開の推奨事項が改訂されました。
1_6	2023 年 11 月 16 日	「CPU 設定の計算」セクションを更新しました。AVX/AVX2 要件を追加しました。
1_7	2023 年 11 月 17 日	「サポートへの連絡」ページの問題を修正しました。