Cisco Stealthwatch

Virtual Edition（Data Store 付属）アプライアンス設置ガイド 7.3.2

目次

はじめに **6**
概要 6
対象読者 6
用語 7
略語 7
はじめる前に **8**
インストールと構成の順序 8
初回セットアップ（First Time Setup） 9
データストア 9
Security Analytics and Logging（オンプレミス） 9
インストール方法 10
互換 11
すべてのアプライアンスの一般的な要件 11
VMware 11
KVM 12
ソフトウェアのダウンロード 12
TLS 12
サードパーティ製アプリケーション 12
ブラウザ 12
ホスト名 12
ドメイン名 13
NTP サーバ 13
タイムゾーン 13
リソース要件 **14**
Stealthwatch Management Console VE 15
Stealthwatch Management Console 15
Flow Collector VE 16
Flow Collector とデータストア 16
Data Node VE 17
Flow Sensor VE 19
Flow Sensor VE ネットワーク環境 20
Flow Sensor VE トラフィック 21
UDP Director VE 22

データ ストレージ 23
1. ファイアウォールとポートの設定 25
概要 25
アプライアンスの配置 25
Stealthwatch Management Console 25
Stealthwatch Flow Collector 25
Stealthwatch Flow Sensor 25
統合に関する重要な考慮事項 26
TAP 26
Electrical TAP の使用 27
Optical TAP の使用 27
ファイアウォール外部での TAP の使用 28
ファイアウォール内部に Flow Sensor を配置する 28
SPAN ポート 30
Stealthwatch UDP Director 31
Stealthwatch Data Node 31
通信用ファイアウォールの設定 32
オープンポート 32
Stealthwatch Management Console（SMC）、フローコレクタ、データノード、Flow Sensor、および UDP Director 32
通信ポートおよびプロトコル 33
オプションの通信ポート 34
StealthWatch の展開例 35
データストア を含む Stealthwatch の展開例 36
2. VE インストールファイルのダウンロード 39
インストール ファイル 39
1. Cisco Software Central へのログイン 39
2. ファイルをダウンロードする 40
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） 41
概要 41
はじめる前に 41
vCenter を使用した仮想アプライアンスのインストール（ISO） 42
プロセスの概要 42
1. VMware Web Client へのログイン 42
2a. トラフィックを監視するフロー センサーの設定 43

PCI パススルーによる外部トラフィックのモニタリング 43
複数のホストでの vSwitch の監視 43
設定要件 43
単一のホストでの vSwitch の監視 46
設定要件 46
ポートグループの無差別モードへの設定 46
2b.データノード間通信用の独立 LAN の設定 48
3. 仮想アプライアンスのインストール 49
4. 追加モニタリング ポートの定義（Flow Sensor のみ） 57
3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO） 60
概要 60
はじめる前に 60
ESXi スタンドアロン サーバへの仮想アプライアンス（ISO）のインストール 61
プロセスの概要 61
1. VMware Web Client へのログイン 61
2. ISO からの起動 64
3c. KVM ホストへの仮想アプライアンスのインストール（ISO） 65
概要 65
はじめる前に 65
KVM ホストへの仮想アプライアンスのインストール（ISO） 65
プロセスの概要 66
データノードの独立 LAN の設定 66
1. KVM ホストへの仮想アプライアンスのインストール 66
トラフィックのモニタリング 66
設定要件 66
KVM ホストへの仮想アプライアンスのインストール 67
2. NIC（Data Node、Flow Sensor）および Open vSwitch での無差別ポートの監視（Flow Sensor のみ）の追加 73
4. 初回セットアップを使用した環境の設定 75
Stealthwatch 管理コンソールまたはフローコレクタの設定 75
Data Node の設定 80
Flow Sensor または UDP Director の設定 84
トラブルシューティング 87
証明書エラー 87
アプライアンスへのアクセス 88

5. Stealthwatch システムの設定 89
サポートへの問い合わせ 90

はじめに

概要

次の Cisco Stealthwatch Enterprise Virtual Edition（VE）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。

- Stealthwatch Management Console（SMC）VE
- Stealthwatch フローコレクタ VE
- Stealthwatch データノード VE
    - データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの設置の適切な順序を含む、Data Store の展開に関する詳細な手順について、『Data Store Virtual Edition Deployment and Configuration Guide』で確認してください。このガイドは、仮想アプライアンスのインストールに関する参考資料としてのみ使用してください。
- Stealthwatch Flow Sensor VE
- Stealthwatch UDP Director VE

Stealthwatch の詳細については、次のオンライン リソース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]
- **アプライアンス**：https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html [英語]
- **リリースノート**：詳細については、リリースノートを参照してください。
- **ハードウェア設置ガイド**：Stealthwatch x2xx シリーズ ハードウェアを設置する場合は、https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html からガイドをダウンロードしてください。
- **Data Node および Data Store の設置**：データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの設置の適切な順序を含む、Data Store の展開に関する詳細な手順について、『Data Store Virtual Edition Deployment and Configuration Guide』で確認してください。

対象読者

このガイドは、Stealthwatch 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 Cisco Stealthwatch サポートに連絡してください。

用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべてのStealthwatch 製品に対し「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、StealthWatch Management Console（SMC）で管理される Stealthwatch 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）
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
SMC	Stealthwatch Management Console
TB	テラバイト
UUID	汎用一意識別子
VDS	vNetwork 分散型スイッチ
VE	バーチャル エディション
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン

はじめる前に

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。

インストールと構成の順序

仮想アプライアンスをインストールする前に、Stealthwatch のインストールおよび構成で必要とされる順序を確認してください。

1. **Data Store の概要の確認**:『Data Store Virtual Edition Deployment Overview』を参照して、データストア とともに Stealthwatch を展開するための基本的な前提条件を確認してください。
2. **仮想アプライアンスのインストール**:『Data Store Virtual Edition Deployment and Configuration Guide』を参照して、アプライアンスの展開の適切な順序を含む、Data Store とともに Stealthwatch Virtual Edition(VE)を展開するための詳細な手順について確認してください。この Virtual Edition(Data Store 付属)アプライアンス設置ガイドは、仮想アプライアンスのインストールに関する参考資料として使用してください。
3. **Stealthwatch の設定**:SMC VE、Data Node VE、および Flow Collector VE を展開した後、『Stealthwatch System Configuration Guide v7.3.2』および『Data Store Virtual Edition Deployment and Configuration Guide』を使用して、そのアプライアンスを設定します。

   次の点に注意してください。

   - **構成順序**:適切な順序でアプライアンスを設定してください。
   - **証明書**:アプライアンスは、一意の自己署名アプライアンス アイデンティティ証明書とともにインストールされます。
   - **Central Management**:プライマリ SMC/Central Manager を使用して、アプライアンスを管理し、構成設定を変更してください。

> ⚠ アプライアンスをインストールした後、『Stealthwatch System Configuration Guide v7.3.2』を使用して Stealthwatch を設定してください。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。

4. **Data Store の初期化と保持の設定**:SMC VE、データノード VE、および Flow Collector VE を Stealthwatch に展開して設定した後、『Data Store Virtual Edition Deployment and Configuration Guide』を使用して、Data Store を初期化し、フローインターフェイス統計データの保持を設定します。このガイドには、Data Store のメンテナンス情報も含まれています。

初回セットアップ（First Time Setup）

このガイドの「**4. 初回セットアップを使用した環境の設定**」の一環として、Data Store を展開できるように環境を設定します。SAL オンプレミスを有効にすることもできます。

> ⚠ 初回セットアップでこれらの選択を行った後は、構成を変更できません。選択を誤った場合は、新しい仮想アプライアンスを展開するか、仮想アプライアンスを RFD してください。

データストア

初回セットアップで データストア とともに Stealthwatch を設定する場合は、指示に従い、次の点に注意してください。

- **SMC とフローコレクタ**：SMC およびFlow Collector上に データストア を展開する必要があります。
- **ガイド**：『Data Store Virtual Edition Deployment and Configuration Guide』を参照して、アプライアンスの展開の適切な順序、データストア の初期化、データ保持の設定を含む、Data Store とともに Stealthwatch を展開するための詳細な手順について確認してください。

Security Analytics and Logging（オンプレミス）

セキュリティ分析とロギング（オンプレミス）を有効にし、Stealthwatch の展開を使用して Firepower イベント情報を保存することもできます。これによってフローコレクタで NetFlow 収集が無効になることに注意してください。

- **SMC とフローコレクタ**：SMC でセキュリティ分析とロギングを有効にする場合は、Flow Collectorで SAL を有効にする必要があります。
- **ガイド**：詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。
- **アプリケーション要件**：Security Analytics and Logging（オンプレミス）を設定する場合は、Stealthwatch Management ConsoleでSecurity Analytics and Logging（オンプレミス）アプリをインストールします。

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、「互換性」情報と「リソース要件」を確認します。

次の表を参照して、インストール方法を選択します。また、インストールを開始する前に、「互換性」と「リソース要件」を確認してください。

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	3b. ESXi スタンドアロンサーバ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。
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。 フローセンサーを、追加のアダプタを使用して設定し、追加のスループットをサポートできます。 データノードには、データストア の一部として他の データノードと通信するための 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 v6.5、v6.7、v7.0。
- **オペレーティングシステム**：Debian 10 64 ビット。
- **ISO の展開**：Update 2 および vSphere フラッシュベースの Web クライアントを使用して VMware v6.5 を検証済みです。vSphere の他のクライアントを使用すると、問題が発生する場合があります。ESXi 6.5 Update 2 HTML5 クライアントを使用できますが、システム タイムアウトが発生する可能性があります。
- **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、Stealthwatch 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 3.0.0 ～ 6.5.0
  - qemu-KVM 2.8.0 ～ 5.0.0
  - Open vSwitch 2.6.1 ～ 2.13.0
  - Linux Kernel 4.4.38 ～ 5.4.55
- **オペレーティングシステム**：Debian 10 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**」の項を確認し、Cisco.com にあるお使いの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. VE 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

Stealthwatch には v1.2 が必要です。

サード パーティ製アプリケーション

Stealthwatch は、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**：Stealthwatch 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 VE 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

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバがサーバのリストに含まれている場合は削除します。このサーバ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 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 Stealthwatch 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**：仮想ホスト サーバ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。

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。この項で提供される表を使用して、Stealthwatch VE アプライアンスをインストールおよび設定するために必要な設定を記録します。

- Stealthwatch Management Console（SMC）
- Flow Collector
- データノード
- Flow Sensor
- UDP Director
- データストレージ

> ⚠ 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 Stealthwatch 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。

Stealthwatch Management Console VE

Stealthwatch Management Console VE の最小のリソース割り当て量を決定するには、SMC にログインすることが予想される同時ユーザの数を決める必要があります。

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。

Stealthwatch Management Console

同時接続数ユーザ*	必須予約済みメモリ	必須予約済み CPU	最小ストレージ容量
最大 9	32 GB	4	125 GB
10 以上	64 GB	8	200 GB

*同時ユーザには SMC 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 VE

Flow Collectorではなくデータストア 内の データノード がフローを保存するため、リソース要件は データストア を導入するかどうかによって異なります。

Flow Collector と データストア

1 秒あたりのフロー数	インターフェイス	エクスポータ	必須予約済みメモリ	必須予約済み CPU	必須最小データストレージ
最大 50,000	最大 65,535	最大 2,048	32 GB	6	200 GB
最大 120,000	最大 65,535	最大 4,096	70 GB	8	200 GB

Data Node VE

> データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの展開の適切な順序を含む、Data Store の初期化に関する詳細な手順について、『Data Store Installation and Configuration Guide』で確認してください。

データノード VE 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 秒あたりのフローを決定する必要があります。これは Flow Collector VE のリソース要件にも影響します。リソース要件の詳細については、「**Flow Collector VE**」を参照してください。

ネットワークに導入可能な データノード VE は 3 つまでです。追加の データノード VE を導入することはできません。

3 つの データノード VE に データストア VE を展開する場合は、データノード 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] / データノード 数`

- 日時平均 (FPS) を決定します。
- 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、データストア 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 データストア 内の データノード 数で割って、データノード 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:

- 日時平均 50,000 (FPS)
- 90 日間フローを保存
- 3 つの データノード を装備

データノード 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) データノード`

- 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
- データストア あたり 80 GB X 90 日 = データストア あたり 7,200 GB
- 7,200 GB / 3 データノード = データノード あたり 2,400 GB (2.4 TB)

リソース要件を決定するには、次の仕様を参照してください。

1 秒あたりのフロー数	必須予約済みメモリ	必須予約済み CPU	30 日間に必要な最小データストレージ
最大 50,000	データノード VE あたり 32 GB	データノード VE あたり 6	• Data Node あたり 800 GB データノード • 3 つの データノード で合計 2.4 TB
最大 120,000	データノード VE あたり 32 GB	データノード VE あたり 12	• Data Node あたり 1.92 TB データノード • 3 つの データノード で合計 5.76 TB
最大 220,000	データノード VE あたり 64 GB	データノード VE あたり 16	• Data Node あたり 3.52 TB データノード • 3 つの データノード で合計 10.56 TB

Flow Sensor VE

Stealthwatch では、Flow Sensor VE の NIC の数に応じて、さまざまなタイプの Flow Sensor VE が用意されています。

- **キャッシュ**：[フローキャッシュサイズ（Flow Cache Size）] 列には、FlowSensor 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**	**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	850 Mbps	32,766
2 x 1 Gbps	4	8 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	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	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	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。

これらの図は、次を搭載した Cisco UCS C220 M4 でのテストに基づいています。

- **プロセッサ**：2 基の Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40 GHz、2 個のソケット、ソケットあたり 12 コア
- **メモリ**：128 GB
- **ストレージ**：800 GB
- **ESXi**：VMware vSphere 6.7.0
- **モニタリング インターフェイス**：PCI パススルーおよび 1 Gbps/10 Gbps インターフェイス

Flow Sensor VE ネットワーク環境

Flow Sensor VE 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 VE でモニタ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：Stealthwatch 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 VE 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）

統合：統合情報については、「Stealthwatch Flow Sensor」を参照してください。

Flow Sensor VE トラフィック

フロー センサーでは、次の Ethertype で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

フロー センサーは、最上位の MPLS ラベルまたは VLAN ID を保存し、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 VE

UDP Director VE では、仮想マシンが次の要件を満たすことが必要です。

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	60 GB	10,000

データ ストレージ

アプライアンスのデータ ストレージは、アプライアンスが再起動すると自動的に拡張されます。また、パフォーマンスを向上させるために、アプライアンスのリソース割り当てを拡張することもできます。次の情報を使用して、各アプライアンスのストレージを割り当てます。

> ⚠ 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 Stealthwatch 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。

- **拡張の計算**：仮想アプライアンスはデータ ストレージにサーバの約 75% を使用し、25% をオペレーティング システムとキャッシュに残します。したがって、必要な容量より、常に 40 % 多くデータ ストレージを拡張します。
- FPS の計算：毎日のシステム平均の毎秒 1,000 フロー（FPS）ごとに 1 GB 以上のデータ ストレージを割り振り、フローを保存する日数を乗じた容量を割り当てます。たとえば、システムの平均が 2,000 FPS で 30 日間フローを保存するには、60 GB（2 X 30）以上のデータ ストレージ容量を割り当てます。
- **Syslog**：外部イベント処理（syslog）機能を使用する場合は、より多くのメモリおよび処理リソースが必要です。
- データストレージ：次の表を使用して、各アプライアンスに必要なデータストレージを決定します。
- **再起動**：ハイパーバイザ ホストで別の方法を使用して仮想マシンのメモリを増加させる場合は、変更を保存した後にアプライアンスを再起動します。

Stealthwatch VE モデル	必須最小ハードウェア データストレージ	最大数 アドレス指定可能 ストレージ/ 同等ハードウェア
Stealthwatch Management Console VE	125 GB	5.6 TB
Flow Collector NetFlow または sFlow VE	200 GB	該当なし、Data Store に依存 データストア
データノード VE	詳細については、Data Node VE のリソース要件を参照してください。	詳細については、Data Node VE のリソース要件を参照してください。
Flow Sensor	60 GB	適用対象外
UDP Director	60 GB	n/a

1. ファイアウォールとポートの設定

概要

仮想アプライアンスをインストールする前に、次の手順を実行してネットワークを準備します。

1. **アプライアンスの配置**
2. **通信用ファイアウォールの設定**
3. **Stealthwatch Flow Sensor**

アプライアンスの配置

設置する各アプライアンスの配置情報を確認します。

- Stealthwatch Management Console（SMC）
- Flow Collector
- Flow Sensor
- UDP Director
- データノード

Stealthwatch Management Console

管理デバイスである Stealthwatch Management Console は、データを送信してくるすべてのデバイスにアクセス可能なネットワーク上に設置します。

Stealthwatch Management Console のフェールオーバー ペアがある場合は、プライマリ コンソールとセカンダリ コンソールを物理的に離れた場所に設置することをお勧めします。この戦略により、ディザスタリカバリ作業（必要な場合）が強化されます。

Stealthwatch Flow Collector

収集およびモニタリング デバイスである Stealthwatch Flow Collector は、Flow Collector にデータを送信する NetFlow または sFlow デバイス、および管理インターフェイスへのアクセスに使用する予定のすべてのデバイスにアクセス可能なネットワーク上の場所に設置する必要があります。

Flow Collector をファイアウォールの外に配置する場合は、[任意のエクスポータからのトラフィックを許可する（Accept traffic from any exporter）] の設定をオフにすることをお勧めします。

Stealthwatch Flow Sensor

IP アクティビティの監視と記録のために、パッシブ モニタリング デバイスとして Stealthwatch Flow Sensor をネットワーク上の複数のポイントに配置できます。これにより、ネットワークの整合性が保護され、セキュリティ違反が検出されます。Flow Sensor には、中央またはリモートのいずれかの管理機能を実装する統合型 Web ベースの管理システムがあります。

次のように、企業ネットワーク上の重要セグメントに Flow Sensor VE アプライアンスを配置すると最も効果的です。

- **ファイアウォールの内側**。トラフィックをモニタして、ファイアウォール違反が発生したかどうかを確認できます。

- **ファイアウォールの外側**。トラフィック フローをモニタして、ファイアウォールにとって脅威となるものを分析できます。
- **ネットワーク上の機密セグメント**。不満を持つ従業員やルート アクセス権限を持つハッカーに対する保護を実現できます。
- **リモート オフィス**。リモート オフィスはネットワーク拡張において脆弱なロケーションです。
- **ビジネス ネットワーク**。プロトコルの使用を管理できます(たとえば、ハッカーが Telnet や FTP を実行して顧客の金融データを侵害しているかどうかを確認するには、トランザクション サービス サブネット上に配置します)。

統合に関する重要な考慮事項

Stealthwatch Flow Sensor VE は、さまざまなネットワークトポロジ、テクノロジー、コンポーネントと統合できる十分な多様性を備えています。Flow Sensor VE をインストールする前に、ネットワークとそのモニタ方法についていくつかの事項を決定する必要があります。次を確認することが重要です。

- ネットワークのトポロジーと、特定の監視ニーズを分析します。
- モニタ対象ネットワークとの間でネットワーク伝送を受信し、必要に応じて内部ネットワーク伝送も受信できるように、Flow Sensor を接続します。
- Flow Sensor を使用して物理ネットワークトラフィックを監視する場合に最適なパフォーマンスを得るには、基盤の物理ホストの NIC に直接アクセスして(igb または e1000e 準拠の PCI パススルーを使用するなど)、Flow Sensor VE を設定します。

以降のセクションでは、次のイーサネット ネットワーク デバイスを使用してネットワークに Stealthwatch Flow Sensor VE アプライアンスを統合する方法について説明します。

- **TAP**
- **SPAN ポート**

すべてのネットワーク設定をここで説明することはできませんが、モニタリングの要件に最適な設定を決定するうえで、記載されている例を参考にすることができます。これらの例は物理ネットワークのシナリオを説明するものですが、仮想ホストも同じような方法で設定できます。

TAP

テストアクセスポート(TAP)がネットワーク接続に合わせて配置されると、TAP は 1 つ以上の個別のポートで接続を繰り返します。たとえば、イーサネット ケーブルに合わせて配置された Ethernet TAP は、個別のポートでそれぞれの伝送方向を繰り返します。したがって、TAP を使用することは、Flow Sensor を使用するための最も信頼性の高い方法です。使用する TAP のタイプは、ネットワークに応じて異なります。

> Flow Sensor の構成要件については、『Stealthwatch System Configuration Guide v7.3.2』を参照してください。

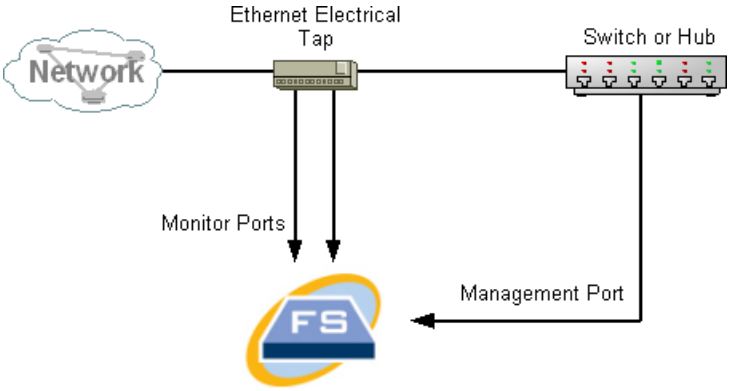
このセクションでは、次に示す TAP の使用法について説明します。

- **Electrical TAP の使用**
- **Optical TAP の使用**
- **ファイアウォール外部での TAP の使用**
- **ファイアウォール内部に Flow Sensor を配置する**

TAP を使用するネットワークでは、インバウンドとアウトバウンドの両方のトラフィックをキャプチャする集約 TAP に Flow Sensor VE が接続される場合にのみ、パフォーマンス モニタリング データをキャプチャできます。各ポートで 1 方向のトラフィックだけをキャプチャする単方向 TAP に Flow Sensor VE が接続されている場合、Flow Sensor VE はパフォーマンス モニタリング データをキャプチャしません。

Electrical TAP の使用

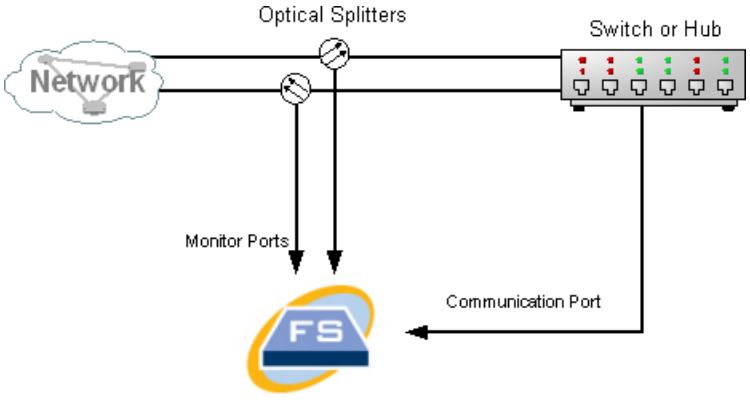
次の図は、Ethernet Electrical TAP に接続されている StealthWatch Flow Sensor VE を示しています。この構成を実現するには、図に示すように 2 つの TAP ポートを Flow Sensor VE モニタ ポート 1 と 2 に接続します。



Optical TAP の使用

光ファイバ ベースのシステムには 2 つのスプリッタが 必要です。光ファイバ ケーブル スプリッタを各伝送方向に合わせて配置し、スプリッタを使用して 1 つの伝送方向の光信号を繰り返すことができます。

次の図は、光ファイバ ベースのネットワークに接続されている Flow Sensor を示しています。この構成を実現するには、図に示すように光スプリッタを Flow Sensor VE モニタ ポート 1 と 2 に接続します。



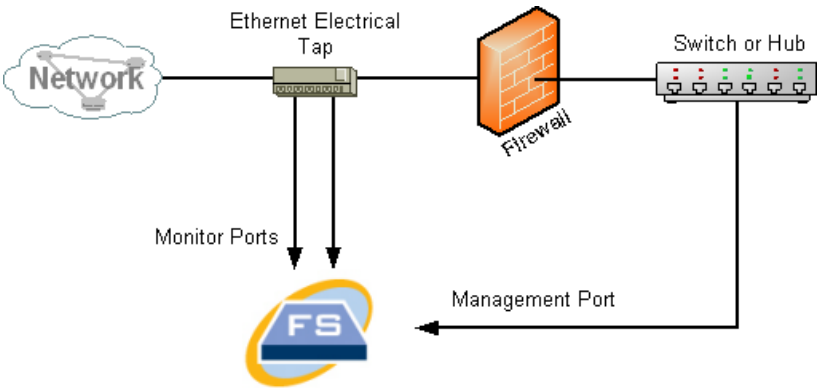
モニタ対象ネットワーク間の接続が光接続である場合、Stealthwatch Flow Sensor VE アプライアンスは 2 つの光スプリッタに接続されます。管理ポートは、モニタ対象ネットワークのスイッチ、または別のスイッチ/ハブに接続されます。

ファイアウォール外部での TAP の使用

Flow Sensor VE によってファイアウォールと他のネットワークの間のトラフィックをモニタするには、Stealthwatch 管理ポートをファイアウォール外部のスイッチまたはポートに接続します。

> ⚠ デバイスの障害が原因でネットワーク全体がダウンしないようにするため、この接続に TAP を使用してください。

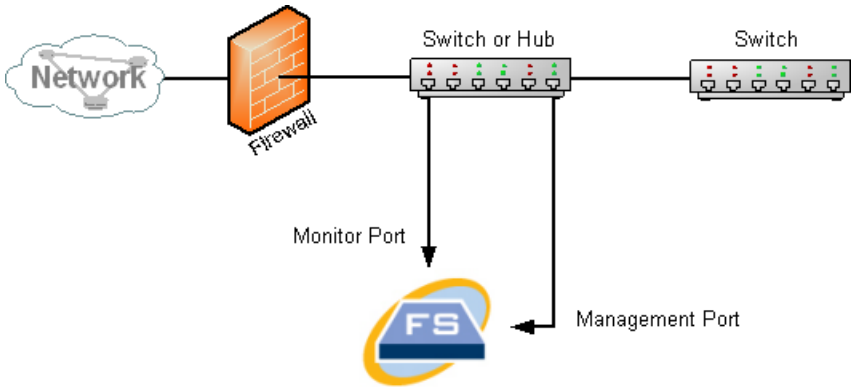
次の図に、Ethernet Electrical TAP を使用したこの構成の例を示します。モニタ対象ネットワークのスイッチまたはハブに管理ポートを接続する必要があります。このセットアップは、ネットワークとの間のトラフィックをモニタするセットアップに似ています。



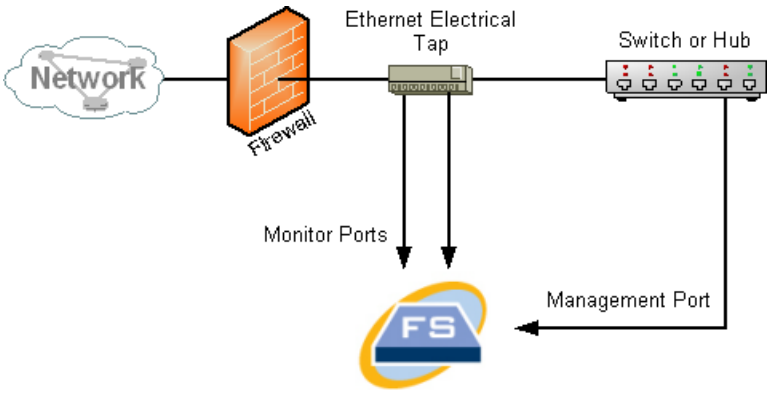
ファイアウォールでネットワーク アドレス変換（NAT）を実行している場合は、ファイアウォール上のアドレスだけを監視できます。

ファイアウォール内部に Flow Sensor を配置する

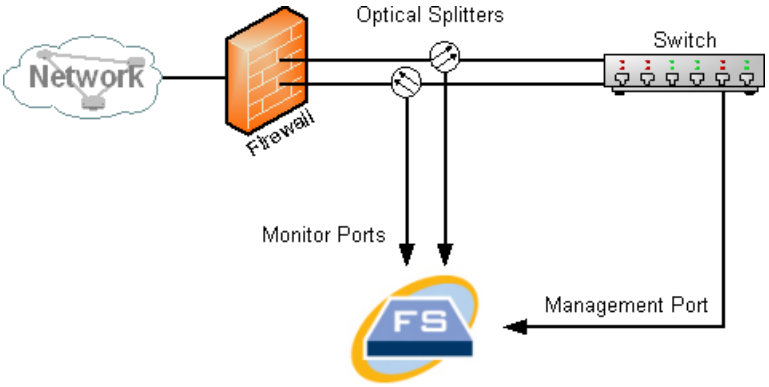
内部ネットワークとファイアウォールの間のトラフィックをモニタするには、Flow Sensor VE がファイアウォールと内部ネットワークの間のすべてのトラフィックにアクセスできる必要があります。これを実現するには、メイン スイッチでファイアウォールへの接続をミラーリングするミラー ポートを設定します。次の図に示すように、Flow Sensor VE モニタ ポート 1 がミラー ポートに接続していることを確認してください。



TAP を使用してファイアウォール内部のトラフィックをモニタするには、ファイアウォールとメインスイッチまたはハブの間に TAP または光スプリッタを挿入します。TAP の構成を次に示します。



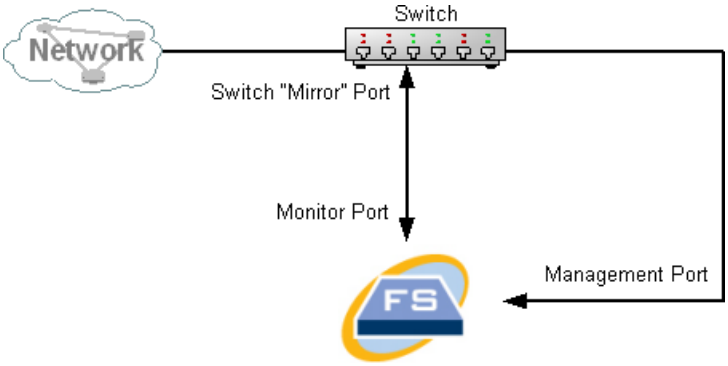
光スプリッタの構成を次に示します。



SPAN ポート

また、Flow Sensor VE をスイッチに接続することもできます。ただし、スイッチは各ポートのすべてのトラフィックを繰り返すわけではないので、Flow Sensor VE が正しく機能するには、1 つ以上のスイッチ ポートとの間で伝送されるパケットをスイッチで繰り返すことができる必要があります。このタイプのスイッチ ポートはミラー ポートまたは Switch Port Analyzer（SPAN）と呼ばれることがあります。

ネットワークを管理ポート経由で Stealthwatch Flow Sensor VE に接続することでこの構成を実現する方法を次の図に示します。



この構成では、当該ホストとミラー ホストの間のすべてのトラフィックを繰り返すようにスイッチ ポート（ミラー ポート）を設定する必要があります。Flow Sensor VE モニタ ポート 1 をこのミラー ポートに接続する必要があります。これにより、Flow Sensor は当該ネットワークとの間のトラフィック、および他のネットワークへのトラフィックをモニタできるようになります。この場合、すべてのホストまたは一部のホストがスイッチに接続されるネットワーク構成が可能です。

スイッチでネットワークを設定する一般的な方法として、ネットワークをゾーンに区分して、ホスト物理接続ではなく論理接続である仮想ローカル エリア ネットワーク（VLAN）に分けることができます。ミラー ポートが VLAN またはスイッチのすべてのポートをミラーリングするように設定されている場合、Flow Sensor VE は、当該ネットワークとその他のネットワークの内部およびネットワーク間のすべてのトラフィックをモニタできます。

- **構成**：Flow Sensor の構成要件については、『Stealthwatch System Configuration Guide v7.3.2』を参照してください。
- **ドキュメント**：いずれの場合でも、スイッチの製造元のドキュメントを参照して、スイッチ ミラー ポートの設定方法と、ミラー ポートに繰り返されるトラフィックを確認してください。

Stealthwatch UDP Director

Stealthwatch UDP Director を配置する唯一の要件は、Stealthwatch アプライアンスの他の部分に対して妨げられていない通信パスがあることです。

> ⚠ シスコの ACI が利用されており、Unicast Reverse Path Forwarding（uRPF）または［サブネットに対する IP 学習を制限（Limit IP learning to subnet）］が有効になっている環境に UDP Director を展開すると、ローカル ネットワークが UDP Director からの転送トラフィックをブロックする可能性があります。ログ データを収集するツールがトラフィックの最初の送信元を知ることができるように、転送ルールの一部として UDP トラフィックをスプーフィングする必要があります。
>
> この場合に UDP Director の正常な動作を保証するには、ネットワークの uRPF または［サブネットに対する IP 学習を制限（Limit IP learning to subnet）］を無効にできる（通常、内部的に）部分に UDP Director を展開します。UDP Director は L3 アウト（IP 学習なし）に配置できます。4.0+ では、VRF ごとにエンドポイント学習を無効にできます。

Stealthwatch Data Node

フローコレクタによって収集されたフローデータのリポジトリとして、また Stealthwatch Management Console がクエリを実行する集中型リポジトリとして、すべてのフローコレクタと Stealthwatch Management Console からアクセス可能なネットワーク上の場所に データノードをインストールします。詳細については、『Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。

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

Stealthwatch Management Console（SMC）、フローコレクタ、データノード、Flow Sensor、および UDP Director

ネットワーク管理者に連絡して、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 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

また、データノード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

Stealthwatch 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	SMC	TCP/389、UDP/389	LDAP
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	TCP/5222	XMPP
外部ログ ソース	SMC	UDP/514	SYSLOG
Flow Collector	SMC	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	SMC	TCP/443	HTTPS
Flow Sensor	Flow Collector : NetFlow	UDP/2055	NetFlow
Identity	SMC	TCP/2393	SSL
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
SMC	Cisco ISE	TCP/443	HTTPS
SMC	Cisco ISE	TCP/5222	XMPP
SMC	DNS	UDP/53	DNS
SMC	Flow Collector	TCP/443	HTTPS

送信元（クライアント）	宛先（サーバ）	ポート	プロトコル
SMC	Flow Sensor	TCP/443	HTTPS
SMC	Identity	TCP/2393	SSL
SMC	Flow エクスポータ	UDP/161	SNMP
SMC	LDAP	TCP/636	TLS
ユーザ PC	SMC	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。

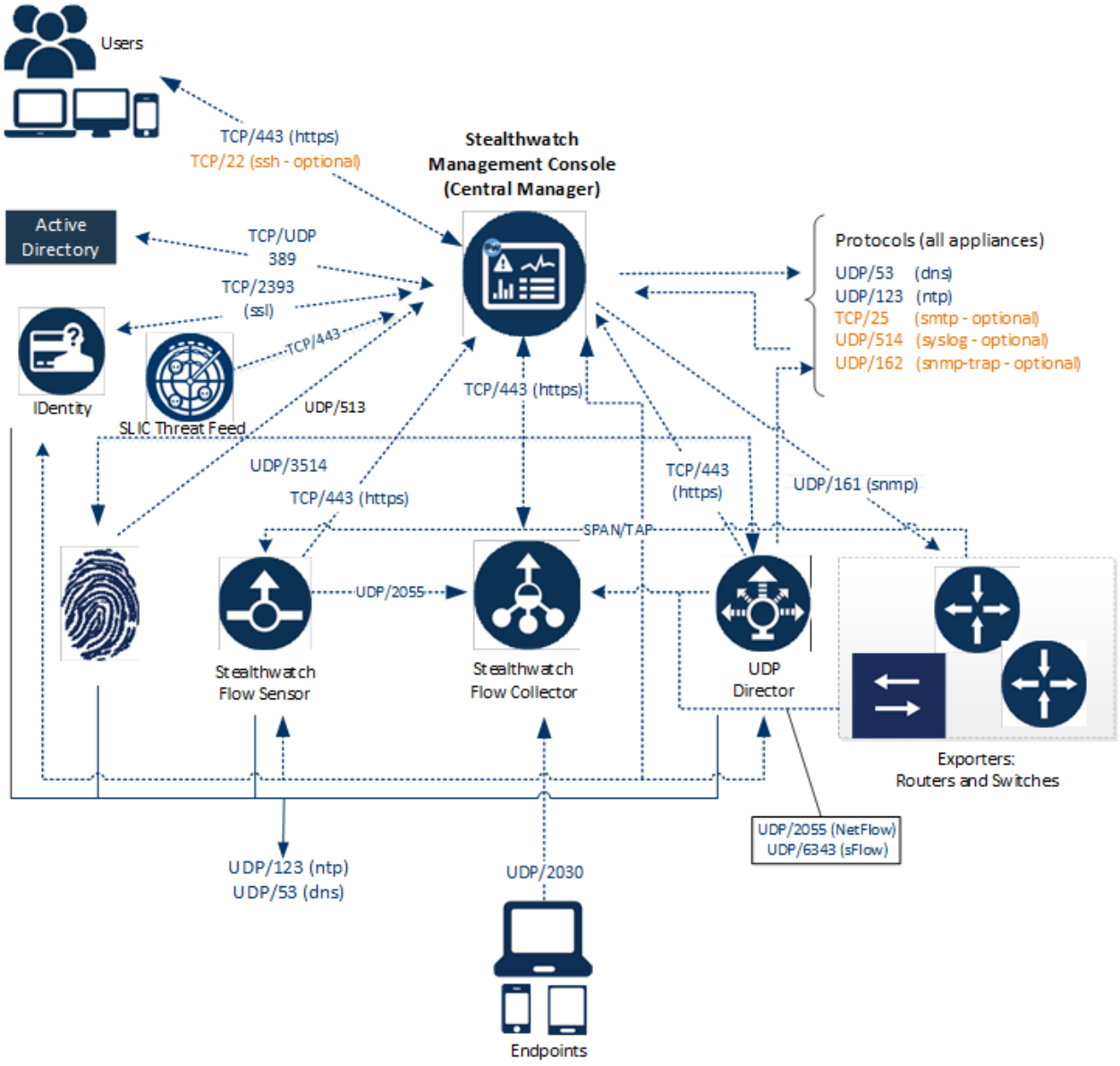
オプションの通信ポート

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 PC	TCP/22	SSH
SMC	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
SMC	サードパーティのイベント管理システム	UDP/514	SYSLOG
SMC	電子メール ゲートウェイ	TCP/25	SMTP
SMC	脅威インテリジェンスフィード	TCP/443	SSL
ユーザ PC	すべてのアプライアンス	TCP/22	SSH

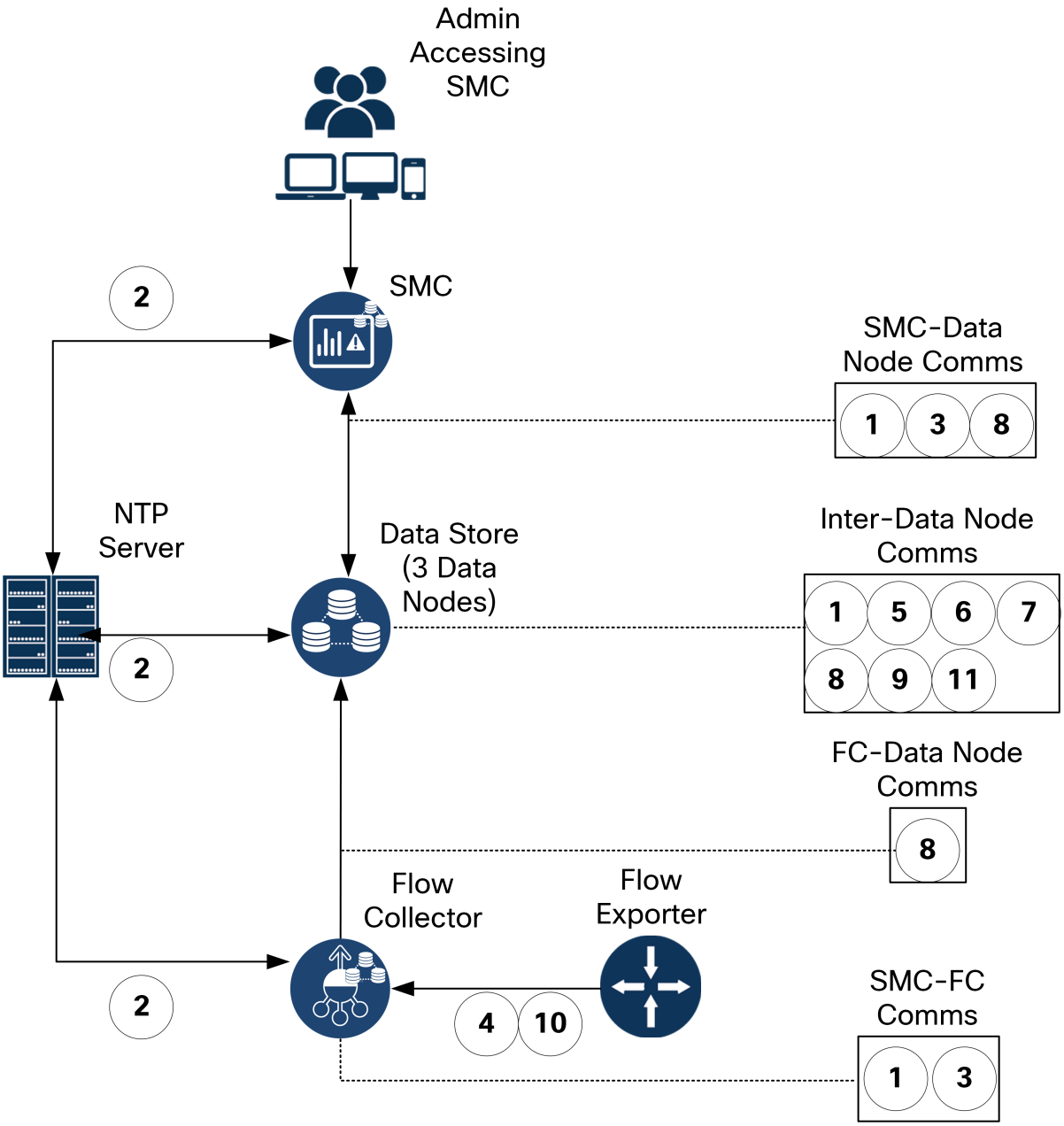
StealthWatch の展開例

次の図は、Stealthwatch 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。



データストア を含む Stealthwatch の展開例

次の図は、データストア が展開された Stealthwatch アーキテクチャの例を示しています。各引き出し線で示されたポートの表を確認してください。



データストア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）	ポート	プロトコルまたは目的
1	SMC	フローコレクタおよび データノード	22/TCP	SSH（データストア 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 データノード	22/TCP	SSH（データストア 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	SMC、フローコレクタ、および データノード	NTP サーバ	123/UDP	NTP（時刻同期に必要）
2	NTP サーバ	SMC、フローコレクタ、および データノード	123/UDP	NTP（時刻同期に必要）
3	SMC	フローコレクタおよび データノード	443/TCP	HTTPS（アプライアンス間のセキュア通信に必要）
3	フロー コレクタ	SMC	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	SMC	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 データノード	4803/TCP	データノード 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 データノード	4803/UDP	データノード 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 データノード	4804/UDP	データノード 間メッセージングサービス
8	SMC、フローコレクタ、および データノード	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 データノード	5433/UDP	Vertica メッセージングサービスのモニタリング

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 データノード	6543/UDP	データノード 間メッセージング サービス

Data Store 通信ポートの詳細については、『Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。

2. VE 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。ファイルタイプを判別するには、「**インストール ファイル**」を参照してください。

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	ISO	ESXi スタンドアロンホストサーバ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. Stealthwatch 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 **Stealthwatch** 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）] > [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。

   - Stealthwatch Management Console 仮想アプライアンス
   - Stealthwatch Flow Collector 仮想アプライアンス
   - Stealthwatch Data Node 仮想アプライアンス
   - Stealthwatch Flow Sensor 仮想アプライアンス
   - Stealthwatch UDP Director 仮想アプライアンス

2. [Stealthwatchシステムソフトウェア(Stealthwatch System Software)]を選択します。
3. [最新リリース(Latest Release)]列で、[7.3.2](またはインストールする 7.3.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。

> データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの展開の適切な順序を含む、Data Store の初期化に関する詳細な手順について、『Data Store Virtual Edition Deployment and Configuration Guide』で確認してください。

別の方法を使用する場合は、次を参照してください。

- VMware ESXi スタンドアロンサーバ：「**3b. ESXi スタンドアロンサーバ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。

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. ファイアウォールとポートの設定**」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. VE 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。

> Stealthwatch システム 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、Stealthwatch 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 を使用した仮想アプライアンスのインストール（ISO）

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。

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。

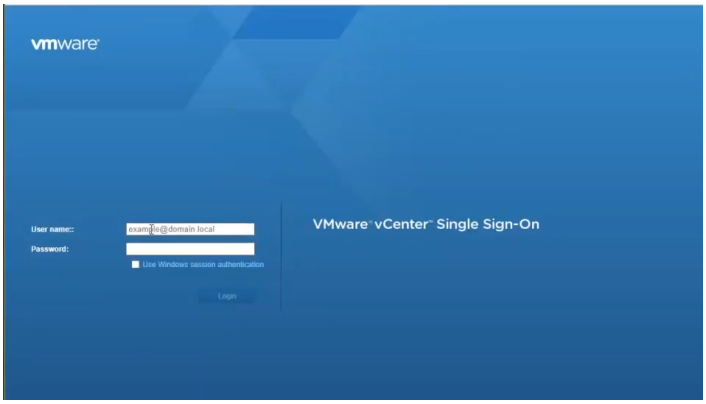
1. VMware Web Client へのログイン
2a. トラフィックを監視するフロー センサーの設定
2b. データノード 間通信用の独立 LAN の設定
3. 仮想アプライアンスのインストール
4. 追加モニタリング ポートの定義（Flow Sensor のみ）

1. VMware Web Client へのログイン

仮想アプライアンスをインストールするには、VMware Web Client にログインします。

> 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. 次の選択肢があります。

   フローセンサー：アプライアンスがフローセンサーの場合、「**2a. トラフィックを監視するフロー センサーの設定**」に進みます。

   データノード：Data Node を展開する場合は、「Data Node 間通信用の独立 LAN の設定」に進みます。

   その他すべてのアプライアンス：アプライアンスがフローセンサーでない場合、「**3. 仮想アプライアンスのインストール**」に進みます。

2a. トラフィックを監視するフロー センサーの設定

Flow Sensor VE 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 VE 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、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情報を含むフロー レコードを作成します。詳細については、「**Flow Sensor VE**」および「**Stealthwatch Flow Sensor**」を参照してください。

次の手順を使用して、vSwitch 上のトラフィックを監視するよう、Flow Sensor 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 VE 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 VE**」を参照してください。
- 統合：「**1. ファイアウォールとポートの設定**」を参照してください。
- 手順：Flow Sensor VE 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 を使用して、複数の VM またはクラスタの分散 vSwitch 上のトラフィックを監視するには、この項の手順を使用します。

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

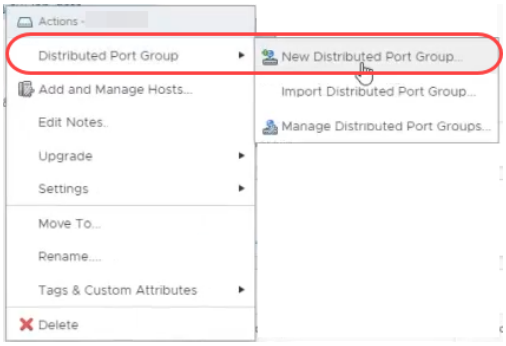
この設定には、次の要件があります。

- 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 VE で監視する各 VDS に追加します。Flow Sensor VE がネットワーク上の VLAN と VLAN 以外の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 ポート 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。

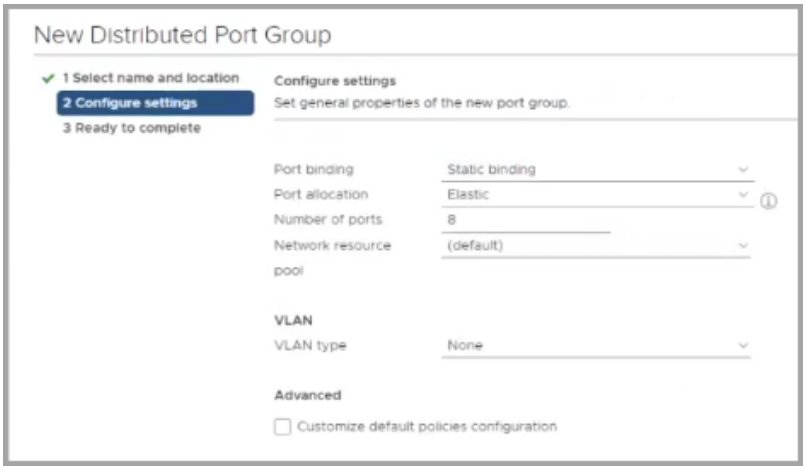
VDS を使用してネットワークを設定するには次の手順を実行します。

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 VE の数を入力します。

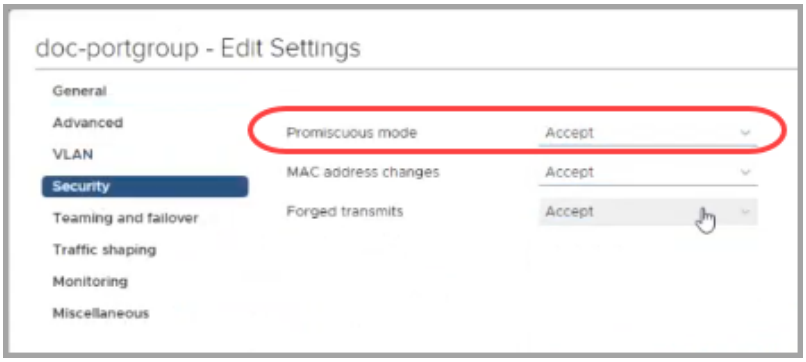


7. [VLANタイプ（VLAN type）]ドロップダウンリストをクリックします。

- 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 VE が VLAN ネットワークトラフィックと非 VLAN ネットワークトラフィックの両方をモニタしますか。

- 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 VE による監視対象となる別の VDS がありますか。

    - 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。
    - ない場合、データノードを展開するときは「Data Node 間通信用の独立 LAN の設定」に進み、展開しないときは「**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 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、この項の手順を使用します。

> 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

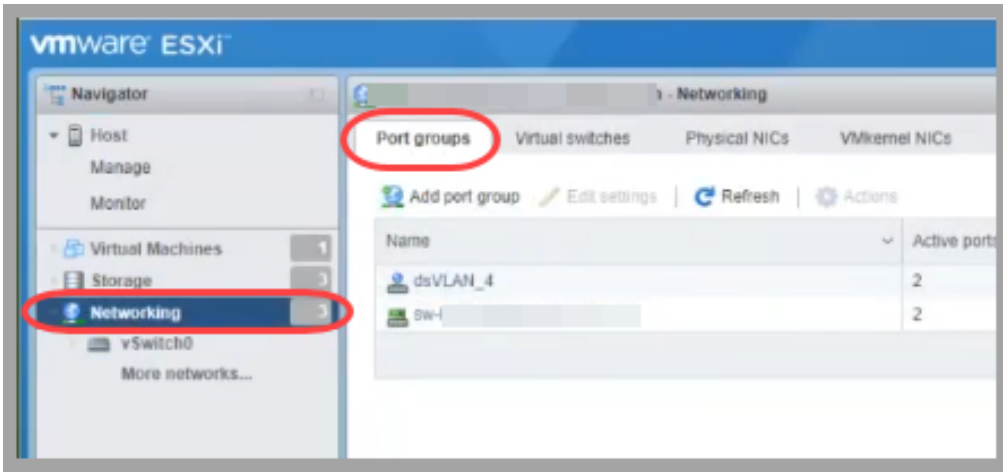
この設定には、次の要件があります。

- **無差別ポートグループ**：Flow Sensor VE 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。



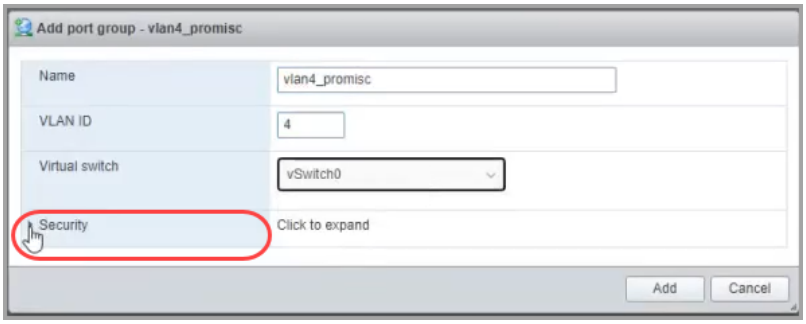
3. [ポートグループ（Port groups）] タブを選択します。
4. 新しいポートグループを作成したり、ポートグループを編集したりできます。

- [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。

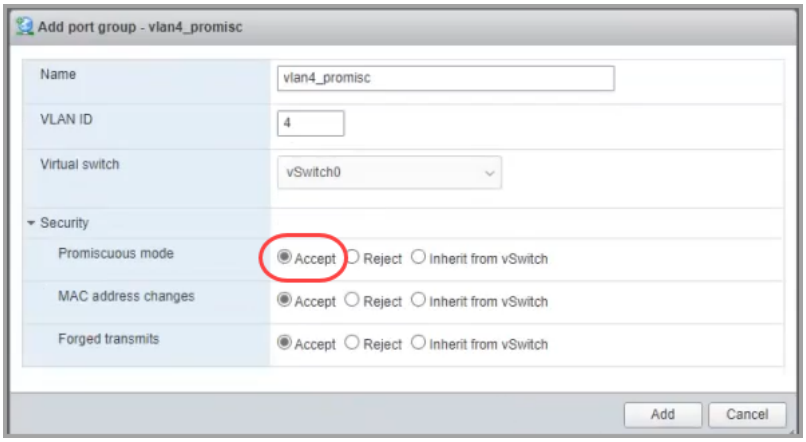
5. ダイアログボックスを使用して、ポートグループを設定します。VLAN ID または VLAN トランキングを設定します。

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 VE が、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、「**2a.トラフィックを監視するフロー センサーの設定**」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。
   - ない場合に、データノードを展開するときは「Data Node 間通信用の独立 LAN の設定」に進み、展開しないときは「**3. 仮想アプライアンスのインストール**」に進みます。

2b.データノード 間通信用の独立 LAN の設定

データノード VE をネットワークに展開する場合は、データノード 間通信用の **eth1** を介して データノード 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。

> すべての データノード VE を同じ ESXi ホストに導入することをお勧めします。別々の ESXi ホストに データノードを導入する場合は、Cisco Professional Services に連絡して、独立した LAN の設定に関する支援を受けてください。

vSphere 標準スイッチを設定するには、次の手順を実行します。

1. VMware ホスト環境にログインします。
2. VMware Host Client インベントリで、[ネットワーキング（Networking）] を右クリックし、[標準vSwitchの追加（Add standard vSwitch）] をクリックします。
3. vSwitch 名を入力します。
4. [仮想スイッチの作成（Create virtual switch）] をクリックします。
5. 物理ネットワークカードをアップリンクとして設定**しない**でください。
6. [Cisco Discovery Protocol] を選択します。
7. [追加（Add）] をクリックします。
8. 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 分散スイッチを設定するには、次の手順を実行します。

1. VMware ホスト環境にログインします。
2. メニューから、[ネットワーキング（Networking）] を選択します。
3. データセンターを右クリックし、[分散スイッチ（Distributed Switch）] > [新規分散スイッチ（New Distributed Switch）] の順に選択します。
4. 名前を入力して [次へ（Next）] をクリックします。
5. ESXi バージョンに基づいて分散スイッチのバージョンを選択し、[次へ（Next）] をクリックします。たとえば、ESXi 7.0 以降を導入している場合は、[7 . 0 . 0] を選択します。
6. [アップリンクの数（Number of uplinks）] で、[0] を選択します。物理ネットワークカードをアップリンクとして設定**しない**でください。
7. [デフォルトポートグループの作成（Create a default port group）] を選択し、ポートグループ名を入力します。
8. [次へ（Next）] をクリックします。

9. [終了（Finish）]をクリックします。
10. 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。

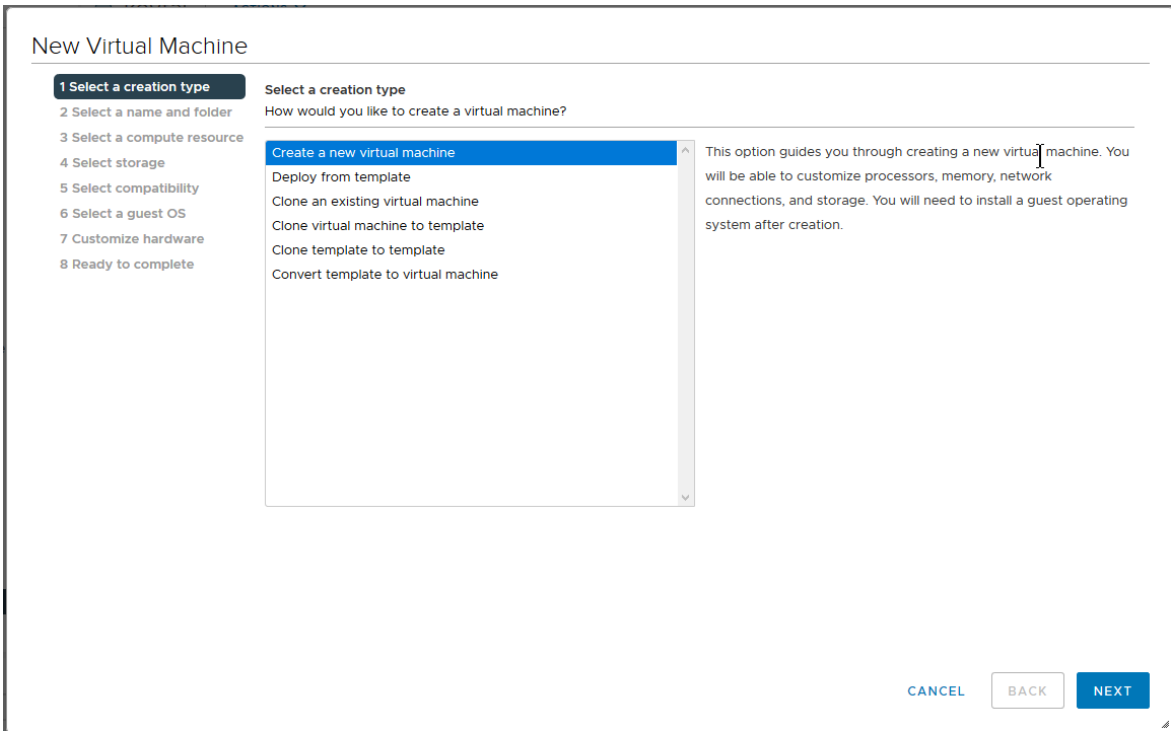
3. 仮想アプライアンスのインストール

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。

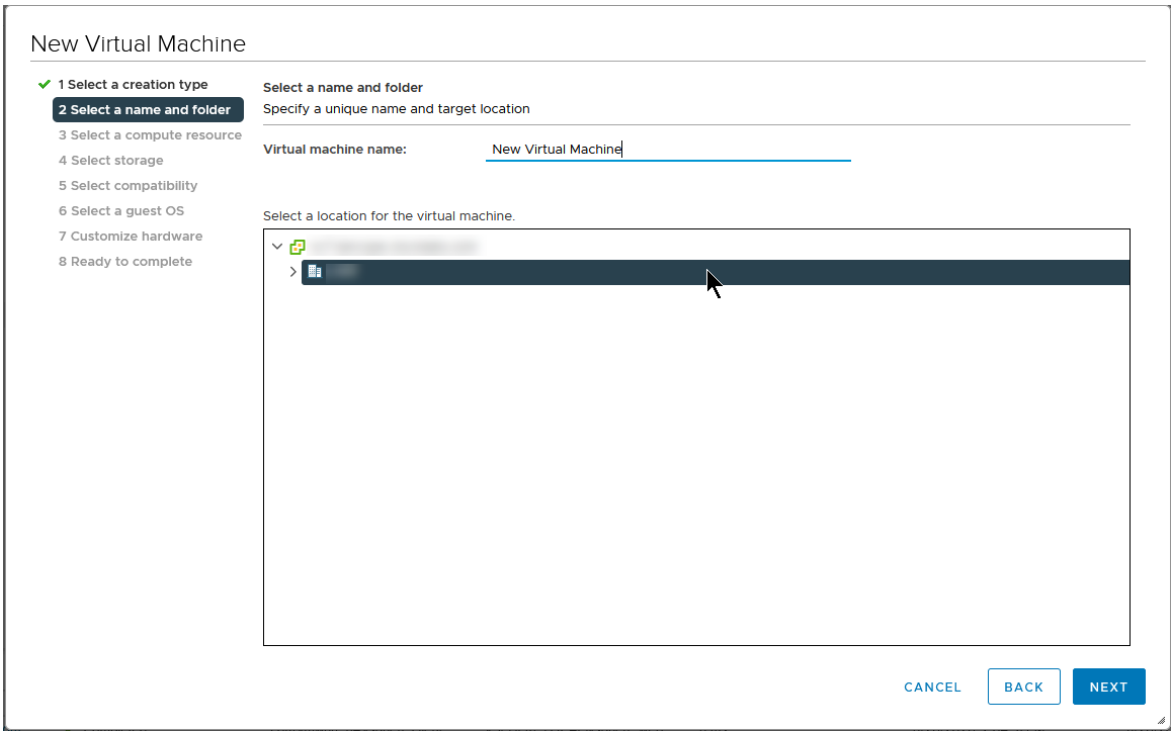
> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. 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。
2. 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。

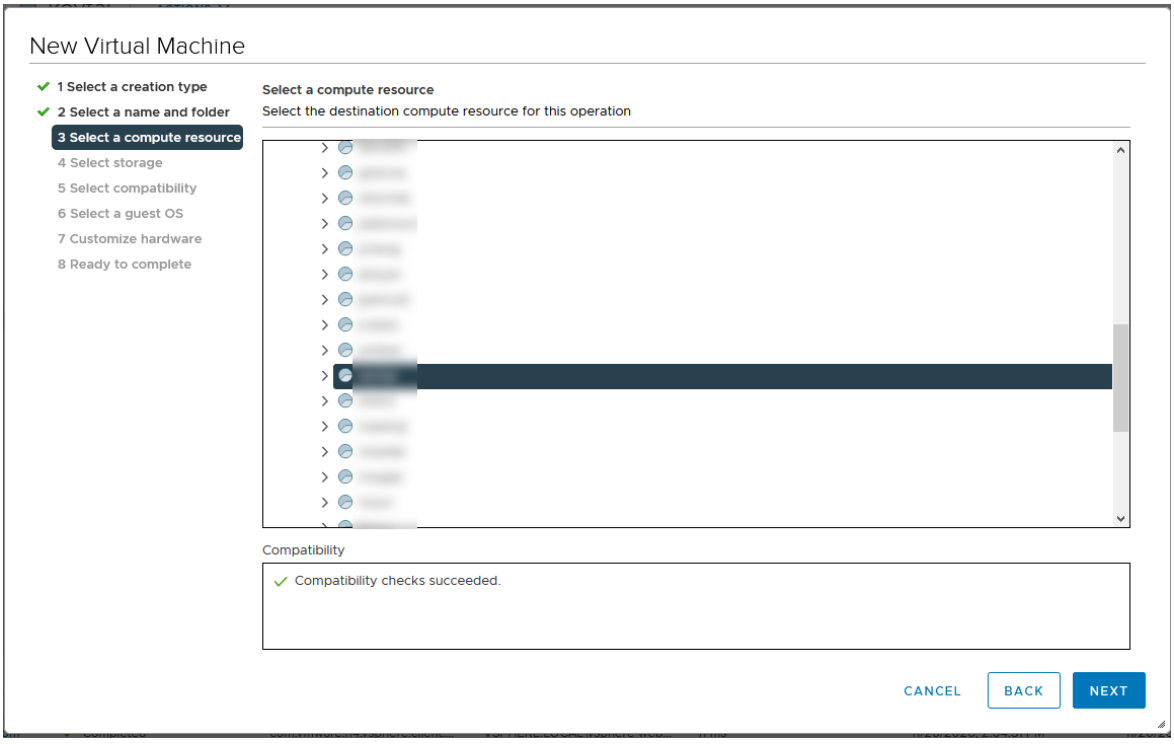
   詳細については、VMware のマニュアルを参照してください。
3. vCenter UI から、[メニュー（Menu）] > [ホストとクラスタ（Hosts and Clusters）] の順に選択します。
4. ナビゲーションウィンドウで、クラスタまたはホストを右クリックし、[新規仮想マシン（New Virtual Machine ...）] を選択して [新規仮想マシン（New Virtual Machine）] ウィザードにアクセスします。
5. [作成タイプの選択（Select a creation type）] ウィンドウで、[新しい仮想マシンの作成（Create a new virtual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



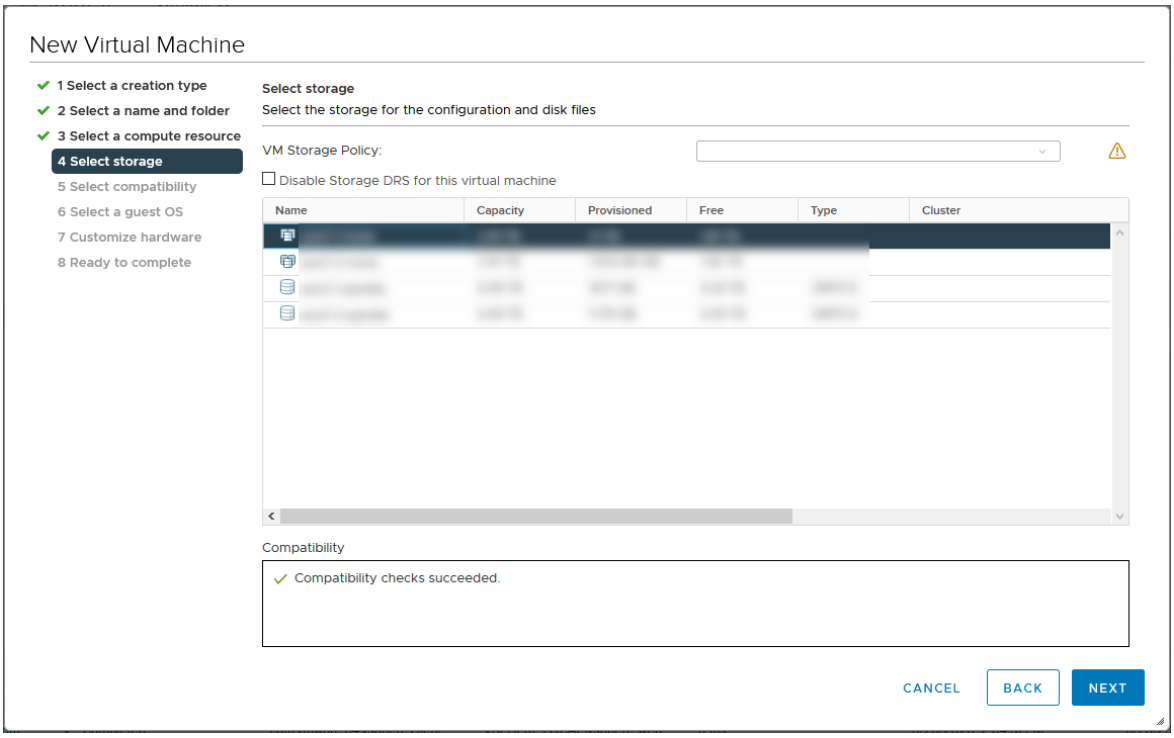
6. [名前とフォルダの選択（Select a name and folder）]ウィンドウで、仮想マシン名を入力し、仮想マシンの場所を選択して、[次へ（NEXT）]をクリックします。



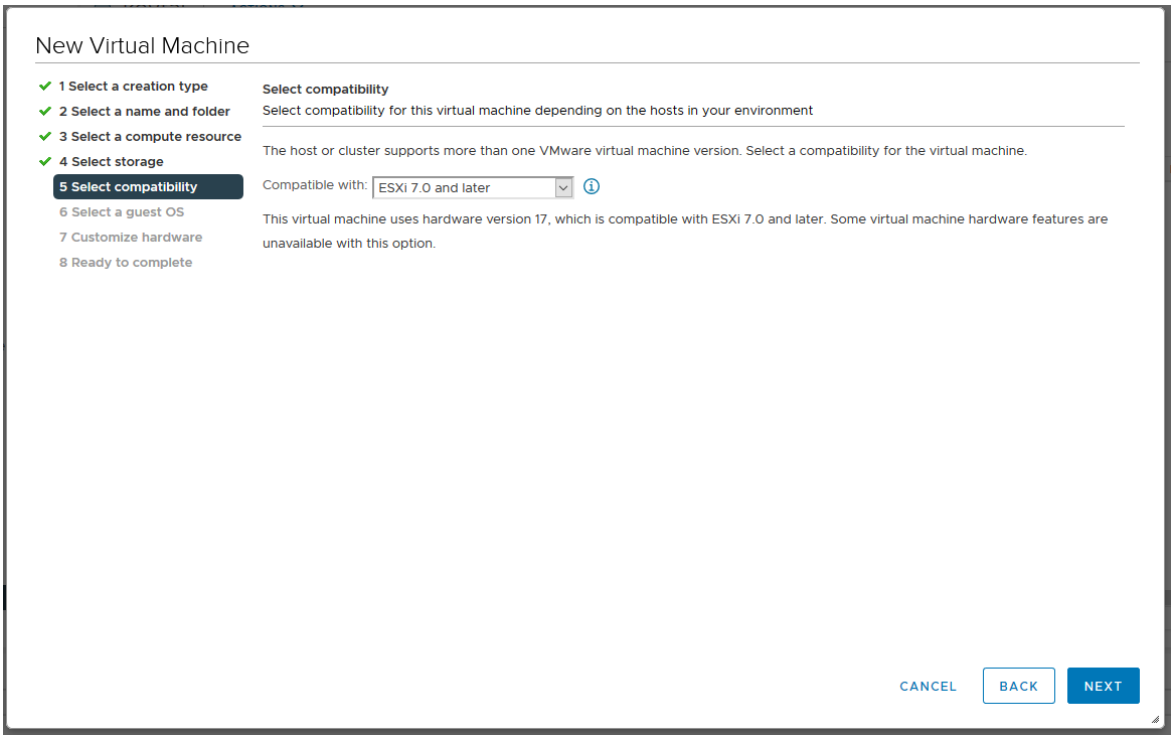
7. [コンピューティングリソースの選択（Select a compute resource）] ウィンドウで、アプライアンスを展開するクラスタ、ホスト、リソースプール、vApp を選択し、[次へ（NEXT）] をクリックします。



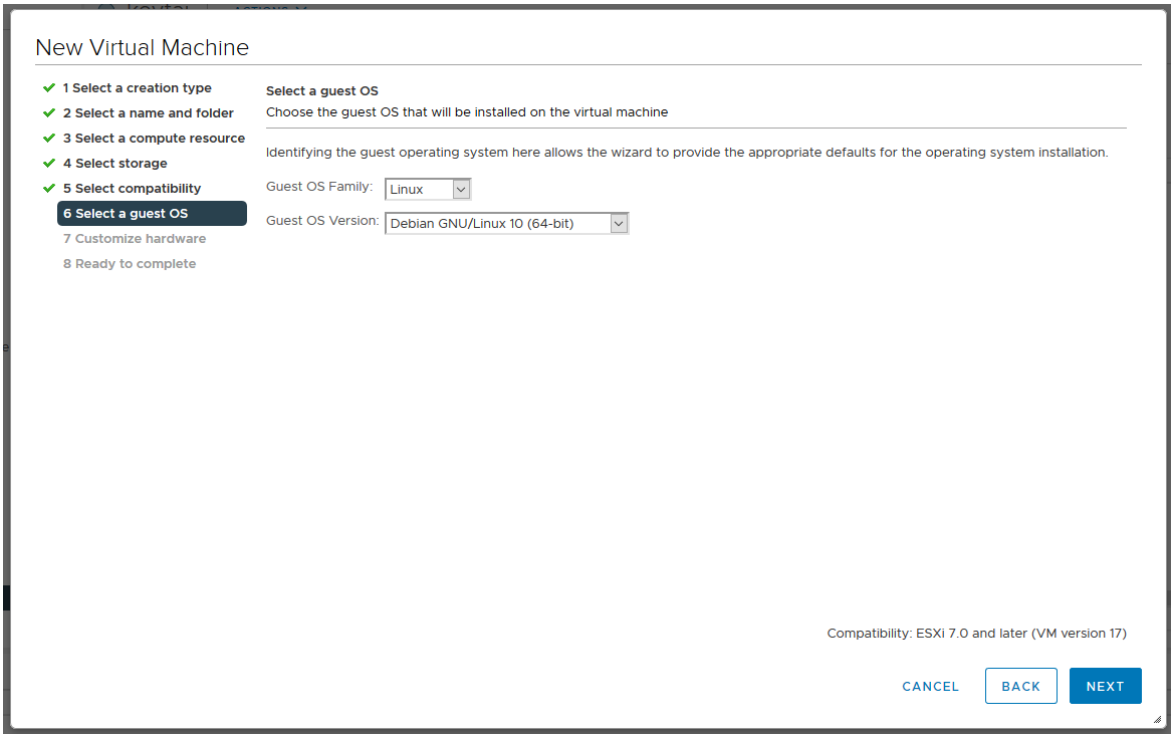
8. [ストレージの選択（Select storage）] ウィンドウで、ドロップダウンから [VMストレージポリシー（VM Storage Policy）] を選択し、保存場所を選択して [次へ（NEXT）] をクリックします。



9. [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。

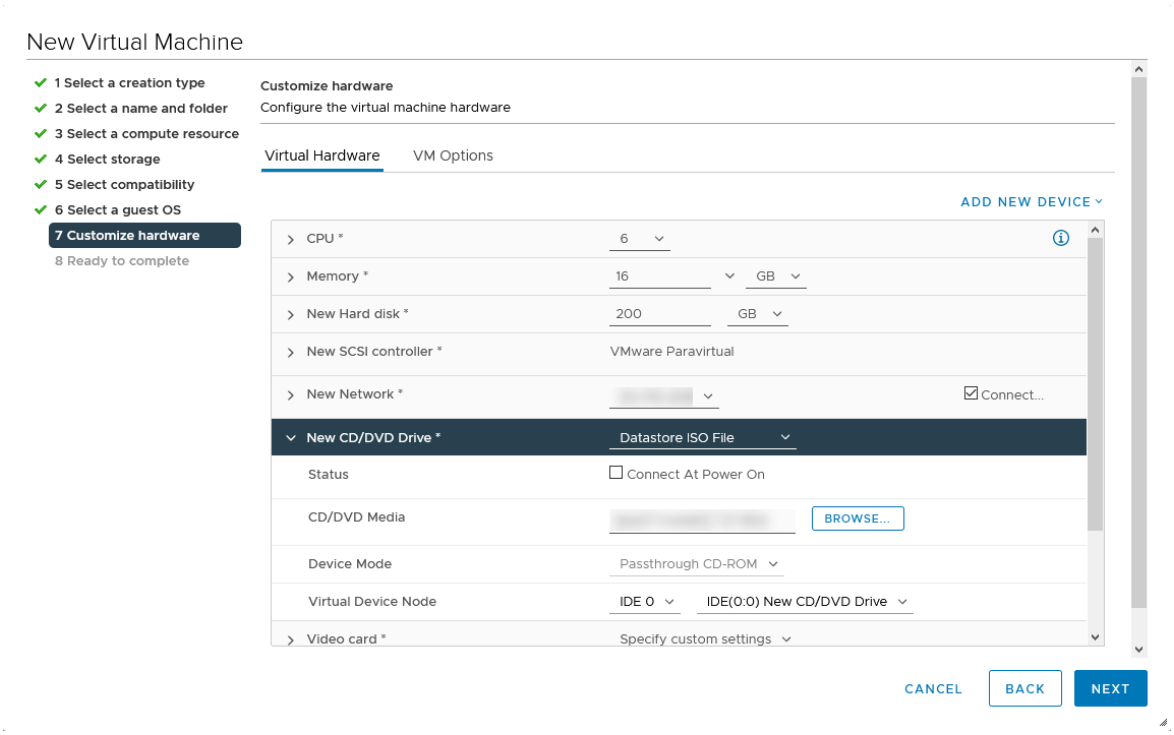


10. [ゲストOSの選択（Select a guest OS）] 画面で、[ゲストOSファミリ（Guest OS Family）] として [Linux] を、[ゲストOSバージョン（Guest OS Version）] として [Debian GNU/Linux 10（64 ビット）（Debian GNU/Linux 10（64-bit））] を選択します。 [次へ（Next）] をクリックします。



11. [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 Stealthwatch 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。

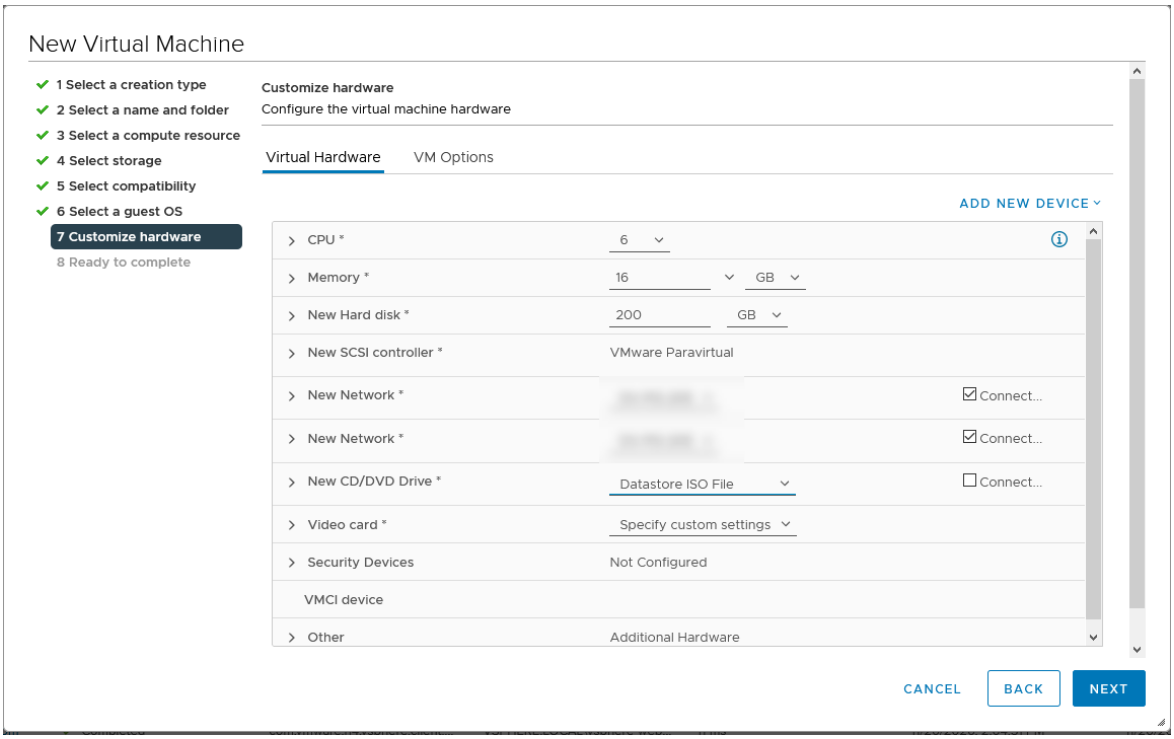


リソース要件に加えて、次の設定を選択します。

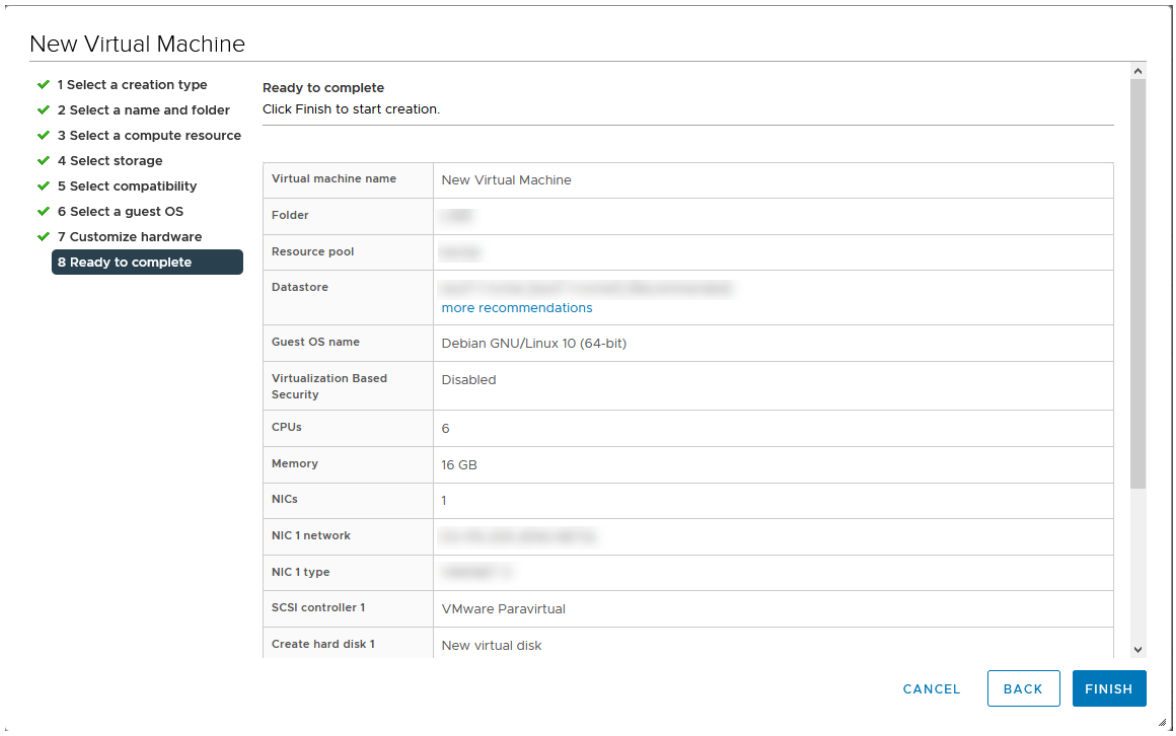
- [新しいハードディスク（New Hard disk）]をクリックして、構成オプションを展開します。[ディスクプロビジョニング（Disk Provisioning）]ドロップダウンから[シックプロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）]を選択します。
- [新しいCD/DVDドライブ（New CD/DVD Drive）]フィールドで、ISO を保存した場所に基づいて ISO の場所を選択します。[新しいCD/DVDドライブ（New CD/DVD Drive）]をクリックして、構成オプションを展開します。[電源投入時に接続（Connect At Power On）]をオンにします。
- [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。
- **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。

12. データノード 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、[ネットワークアダプタ（Network Adaptor）] を選択します。1 番目のネットワークアダプタでは、データノード VE 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、データノード VE が他の データノード と通信できるようにするスイッチとして、「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 データノード について、それぞれの データノード 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。



13. [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。



14. 展開はバックグラウンドで開始されます。[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。
15. **フロー センサー**：アプライアンスがフロー センサーであり、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、次の項「**4. 追加モニタリング ポートの定義（Flow Sensor のみ）**」に進みます。
16. システム内の次の仮想アプライアンスに対して、「**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）**」のすべての手順を繰り返します。

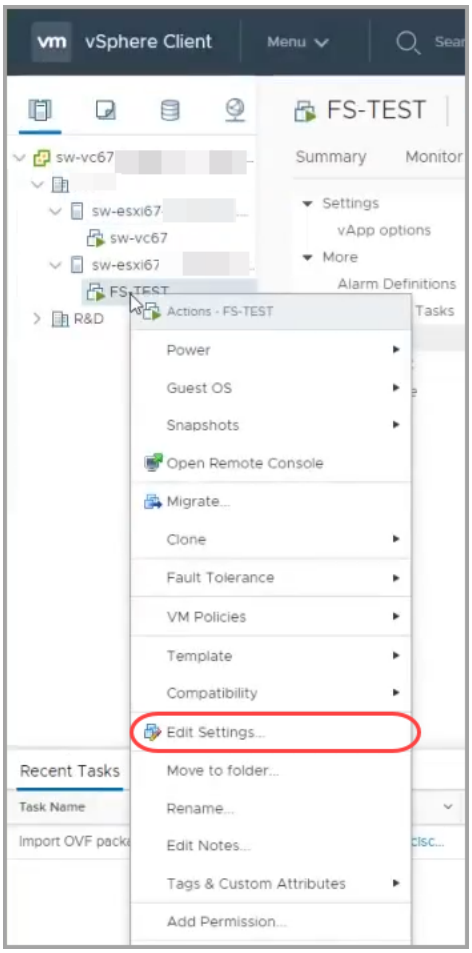
    システム内ですべての仮想アプライアンスのインストールを完了した場合は、「**4. 初回セットアップを使用した環境の設定**」に進みます。

4. 追加モニタリング ポートの定義（Flow Sensor のみ）

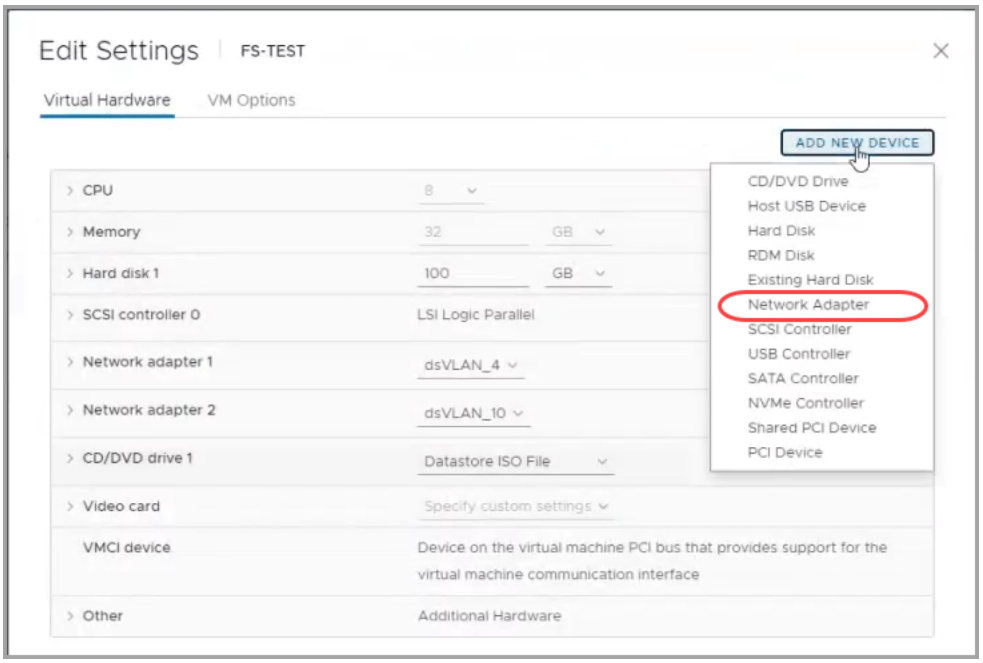
この手順が必要となるのは、Flow Sensor VE が VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合です。Flow Sensor のモニタリング構成ではない場合は、「**4. 初回セットアップを使用した環境の設定**」に進みます。

Flow Sensor VE 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 VE を右クリックします。[設定の編集（Edit Settings）] を選択します。

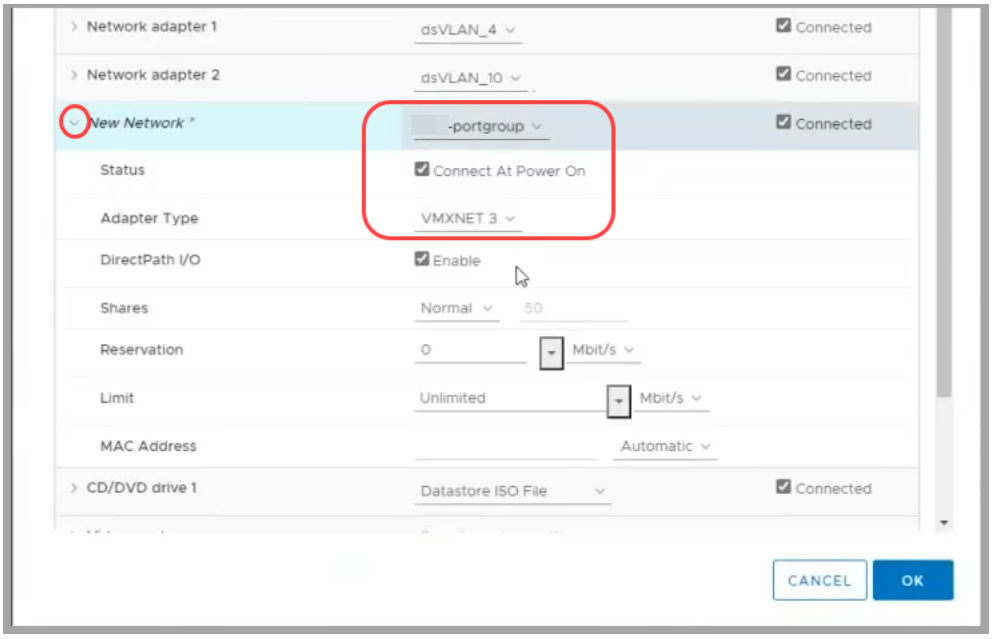


2. [設定の編集（Edit Settings）] ダイアログボックスを使用して、次の指定された設定を構成します。
3. [新規デバイスの追加（Add New Device）] をクリックします。[ネットワークアダプタ（Network Adapter）] を選択します。



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。

   - [新規ネットワーク接続（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。

   すべてのイーサネットアダプタを追加した場合は、「**4. 初回セットアップを使用した環境の設定**」に進みます。

3b. ESXi スタンドアロンサーバ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。

> データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの展開の適切な順序を含む、Data Store の初期化に関する詳細な手順について、『Data Store Installation and Configuration Guide』で確認してください。

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. ファイアウォールとポートの設定**」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. VE 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。

> Stealthwatch システム 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、Stealthwatch 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。

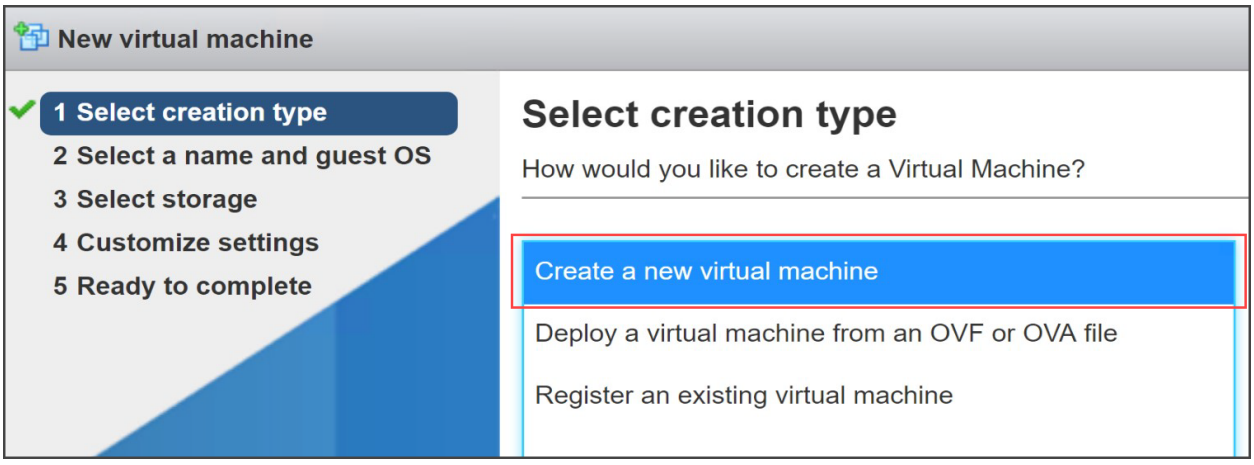
1. VMware Web Client へのログイン
2. ISO からの起動

> フローセンサー：アプライアンスがフローセンサーの場合は、「Stealthwatch Flow Sensor」を参照して、必要な追加の設定手順について理解してください。

1. VMware Web Client へのログイン

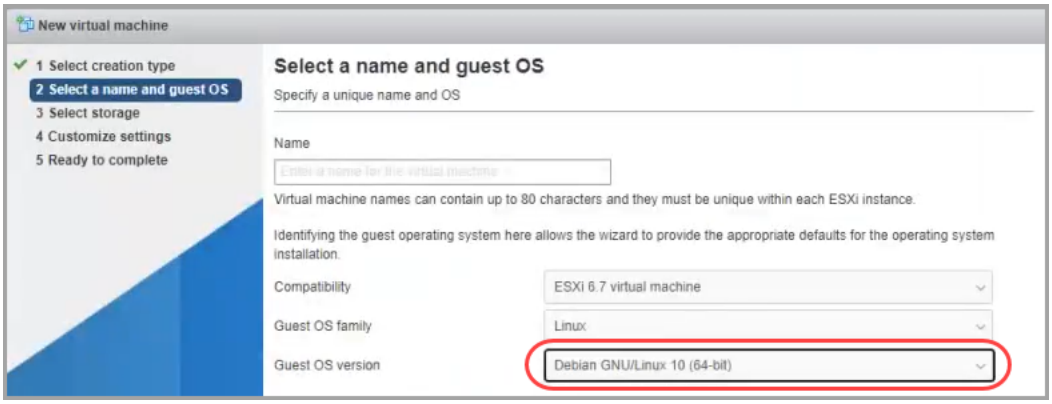
> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

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。

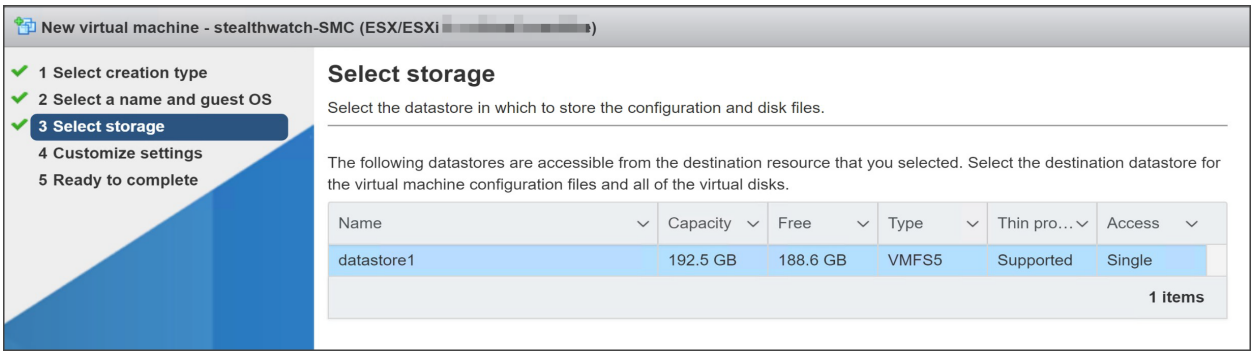


5. ゲスト OS と名前の選択（Select a Name and Guest OS）：次の情報を入力または選択します。

- 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（v6.5 または v6.7）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 10（64ビット）（Debian GNU/Linux 10 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 Stealthwatch 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）。

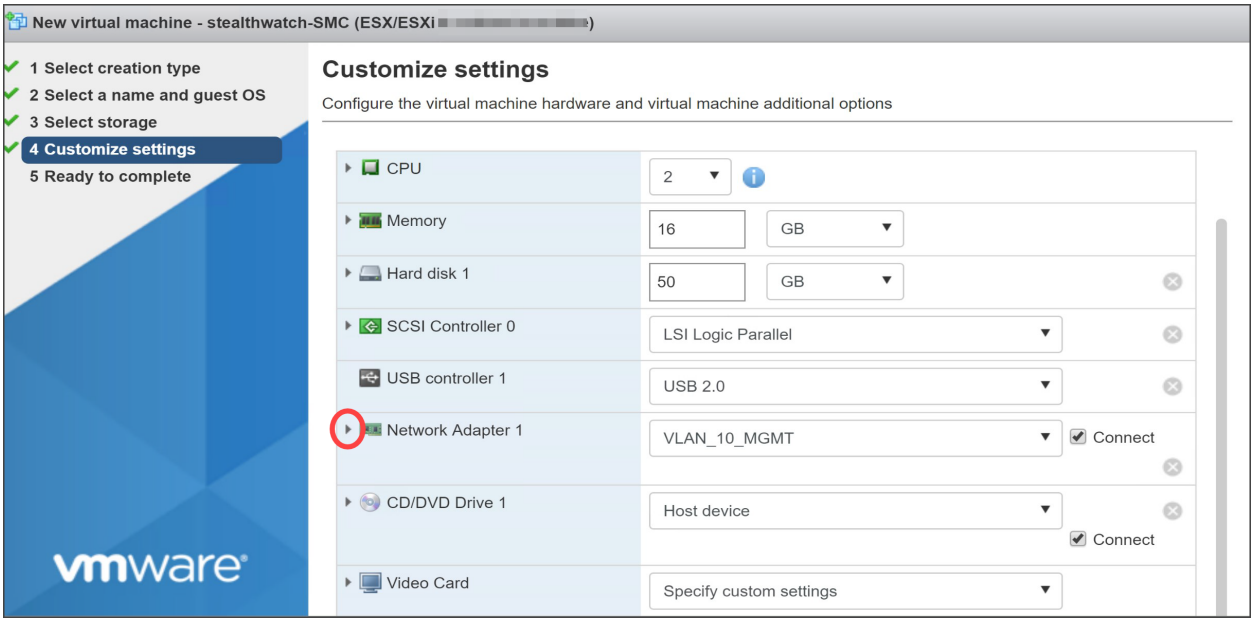
   次の値を選択したことを確認します。

- **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）]

アプライアンスがフロー センサーの場合は、[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。詳細については、「Stealthwatch Flow Sensor」を参照してください。

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。

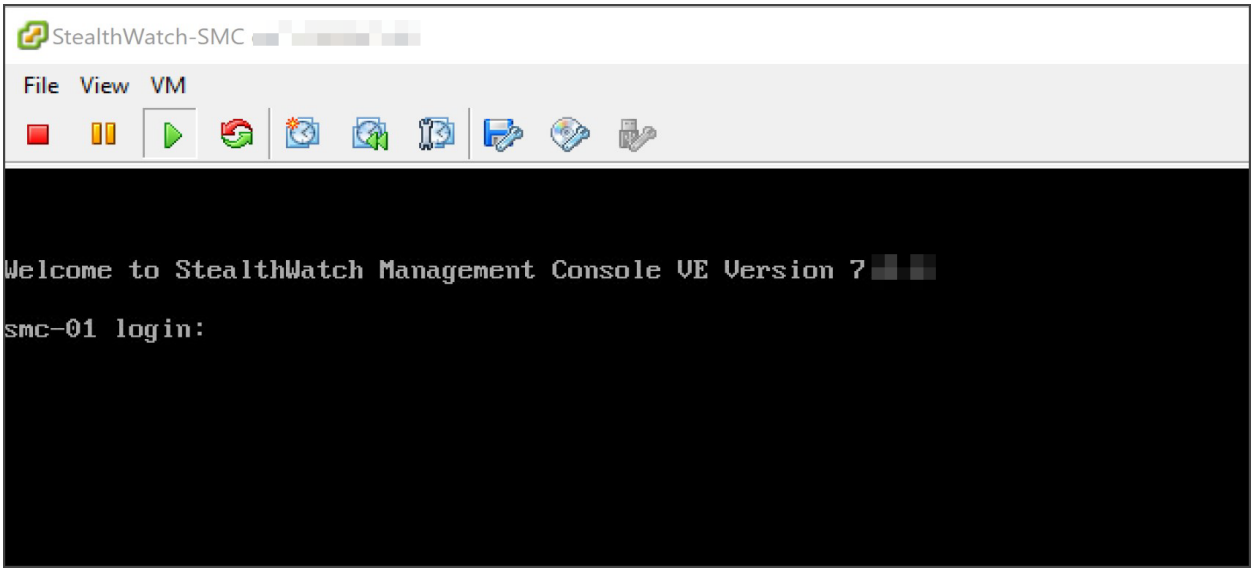
アプライアンスが Data Node の場合、データノード間通信を可能にするために別のネットワーク インターフェイスを追加する必要があります。[ネットワークアダプタの追加（Add Network Adapter）]をクリックします。1 番目のネットワークアダプタでは、データノード VE がパブリックネットワーク上で他のアプライアンスと通信できるようにするスイッチを選択します。2 番目のネットワークアダプタでは、データノード VE が他の データノードと通信できるようにするスイッチとして、「Data Node 間通信用の独立 LAN の設定」で作成したスイッチを選択します。



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。
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. フローセンサー：アプライアンスがフローセンサーの場合は、「Stealthwatch Flow Sensor」を確認し、このマニュアルの前述の項を参照してセットアップを完了します。

    - 2a. トラフィックを監視するフロー センサーの設定（「単一のホストでの vSwitch の監視」を使用）
    - フロー センサーが 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. 初回セットアップを使用した環境の設定」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。

> データノードを Data Store の一部として展開する場合は、開始する前に、アプライアンスの展開の適切な順序を含む、Data Store の初期化に関する詳細な手順について、『Data Store Installation and Configuration Guide』で確認してください。

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。
- VMware ESXi スタンドアロンサーバ：「**3b. ESXi スタンドアロンサーバ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. ファイアウォールとポートの設定**」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、KVM ホストのフォルダにコピーします。この項にある例では、var/lib/libvirt/image フォルダを使用します。手順については、「**2. VE 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。

> Stealthwatch システム 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。

データノード 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. NIC（Data Node、Flow Sensor）および Open vSwitch での無差別ポートの監視（Flow Sensor のみ）の追加

データノード の独立 LAN の設定

データノード VE をネットワークに展開する場合は、データノード 間通信用の **eth1** を介して データノード 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。

> すべての データノード VE を同じ ESXi ホストに導入することをお勧めします。別々の ESXi ホストに データノード を導入する場合は、Cisco Professional Services に連絡して、独立した LAN の設定に関する支援を受けてください。

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 Stealthwatch Management Console（SMC）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リング

Flow Sensor VE 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 VE 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情報を含むフロー レコードを作成します。詳細については、「**Stealthwatch Flow Sensor**：ネットワークへの Flow Sensor VE の統合」を参照してください。

設定要件

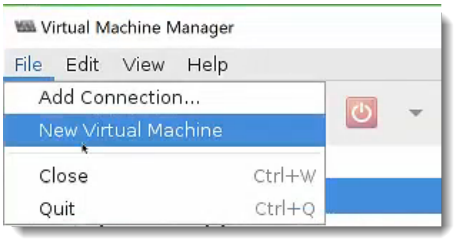
この設定には次の要件があります。

- 無差別モード：有効
- 無差別ポート：Open vSwitch に設定

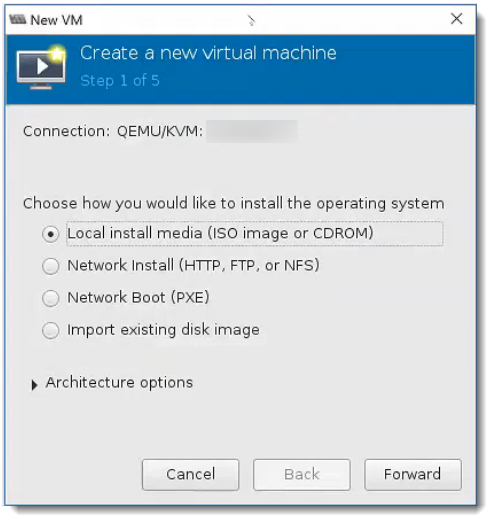
KVM ホストへの仮想アプライアンスのインストール

仮想アプライアンスをインストールし、Flow Sensor VE 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。

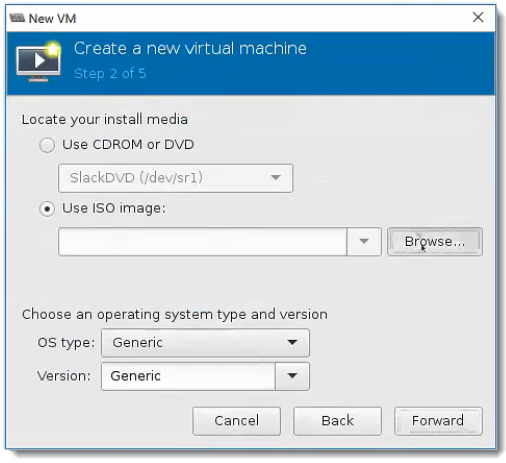
1. Virtual Machine Manager を使用して KVM ホストに接続し、次の手順に従ってアプライアンスを設定します。
2. [ファイル（File）] > [新しい仮想マシン（New Virtual Machine）] をクリックします。



3. [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。[Forward] をクリックします。

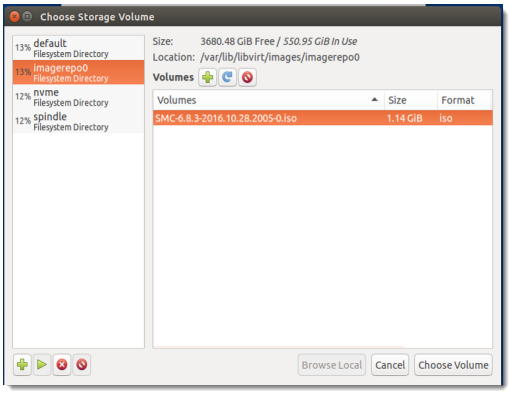


4. [ISOイメージを使用（Use ISO image）] をクリックします。
5. [参照（Browse）] をクリックします。適切なイメージを選択します。

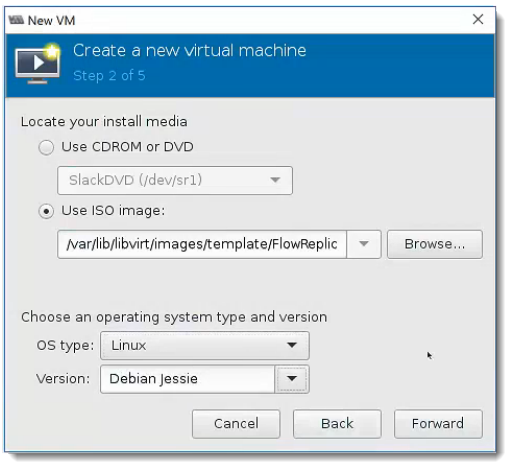


6. ISO ファイルを選択します。[ボリュームの選択（Choose Volume）] をクリックします。

   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。

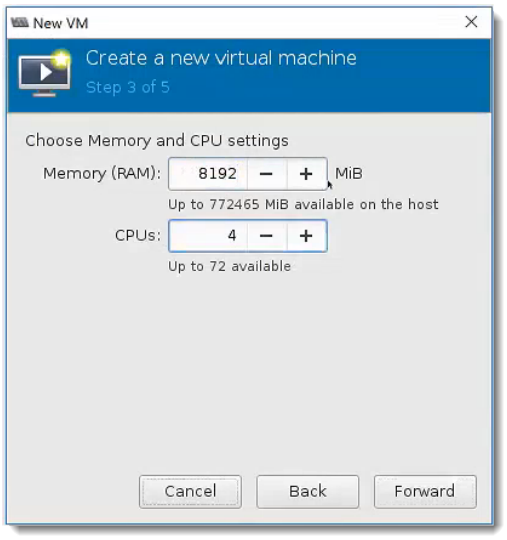


7. [オペレーティング システムのタイプとバージョンの選択（Choose an operating system type and version）] で、[OSタイプ（OStype）] ドロップダウン リストから [Linux] を選択します。
8. [バージョン（Version）] ドロップダウン リストから [Debian Jessie] を選択します。[Forward] をクリックします。

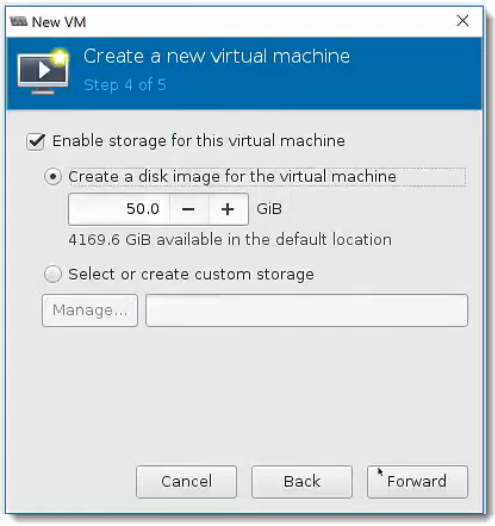


9. メモリ（RAM）とCPUを「**リソース要件**」の項に示す容量まで増やします。

> ⚠ 「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 Stealthwatch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。



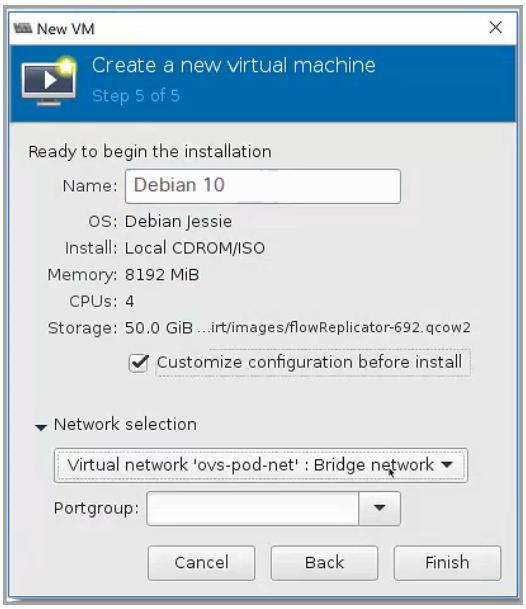
10. [仮想マシンへのディスクイメージの作成（Create a disk image for the virtual machine）]を選択します。
11. 「**リソース要件**」セクションでアプライアンスについて示されているデータストレージ容量を入力します。[Forward]をクリックします。



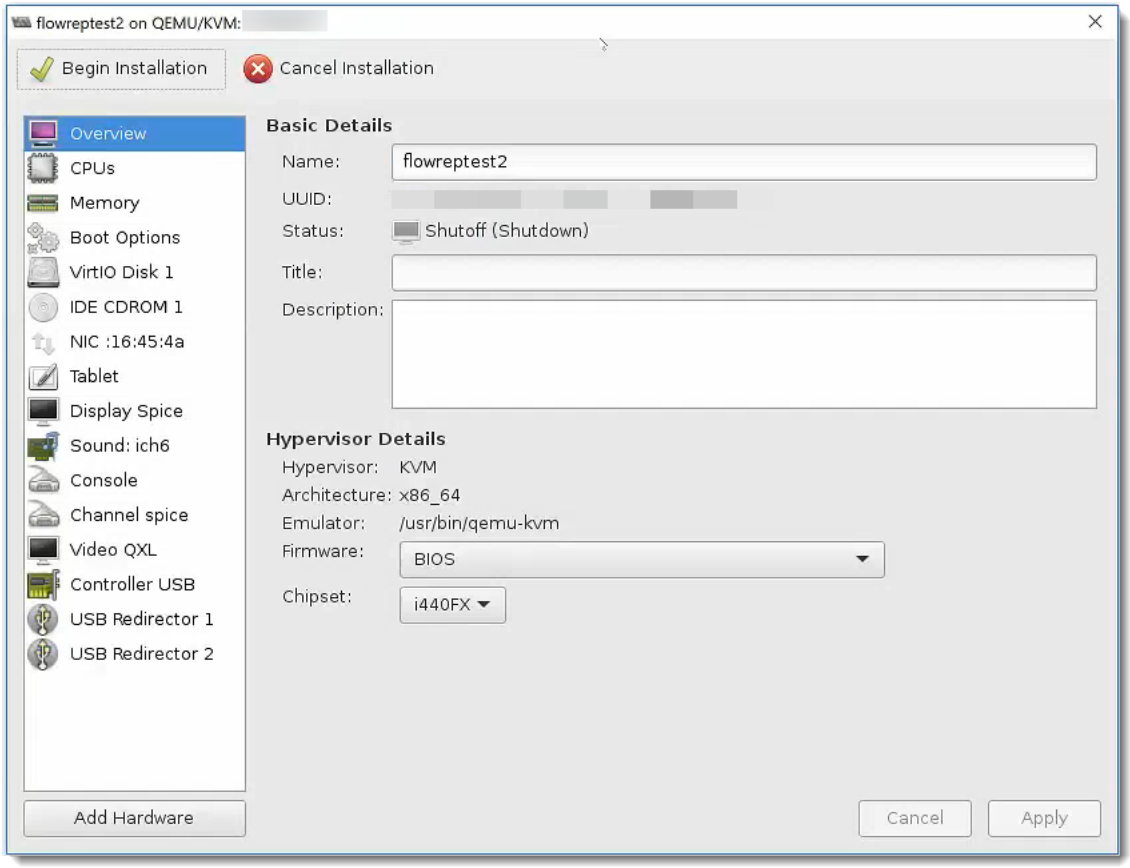
「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。

必要なリソースがない状態で Cisco Stealthwatch 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。

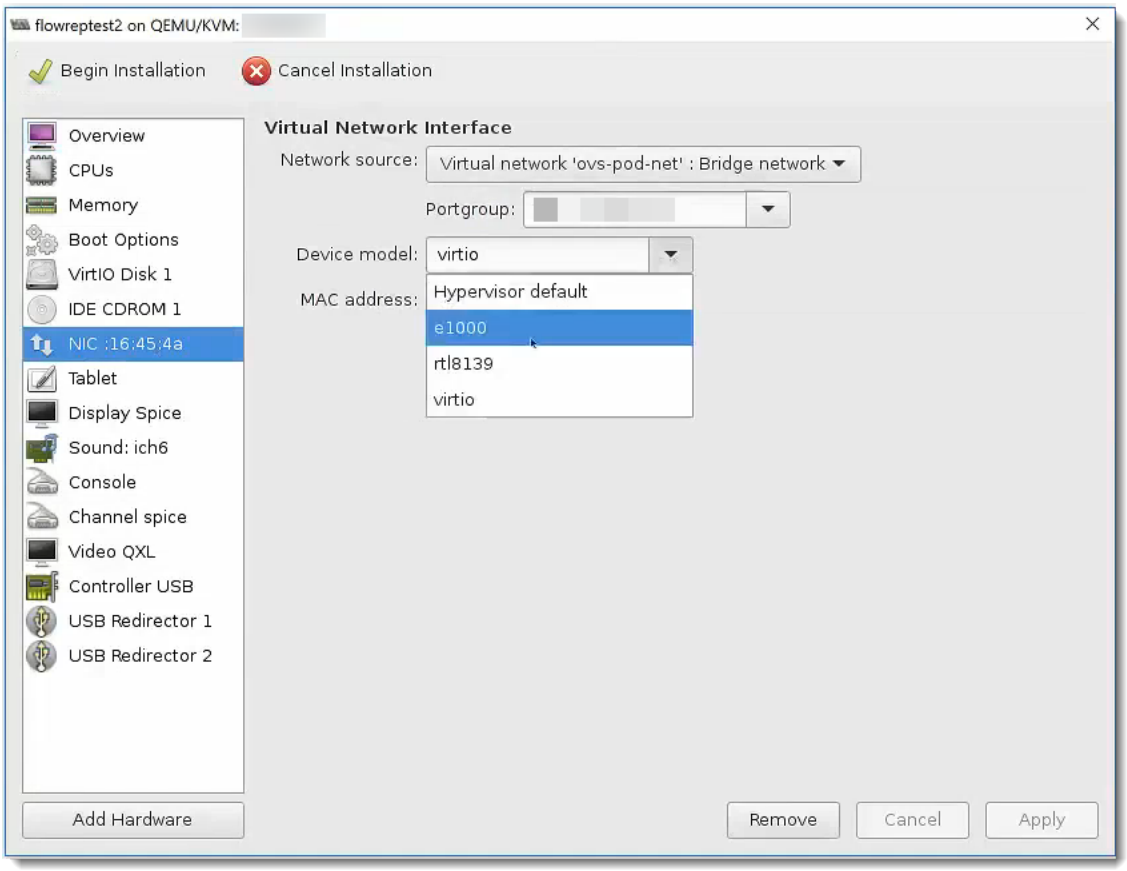
12. 仮想マシンの名前を指定します。これが表示名になるため、後で見つけやすい名前を使用してください。
13. [インストール前に構成をカスタマイズ（Customize configuration before install）] チェックボックスをオンにします。
14. [ネットワークの選択（Network selection）] ドロップダウンボックスで、インストールに適切なネットワークとポートグループを選択します。データノード の場合は、データノード がパブリックネットワーク上で他のアプライアンスと通信できるようにするネットワークおよびポートグループを選択します。



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



16. ナビゲーション ペインで、[NIC] を選択します。
17. [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。



18. [VirtIO ディスク 1（VirtIO Disk 1）] をクリックします。
19. [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。
20. Flow Sensor VE でポートを監視するために、または データノード VE で データノード 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。

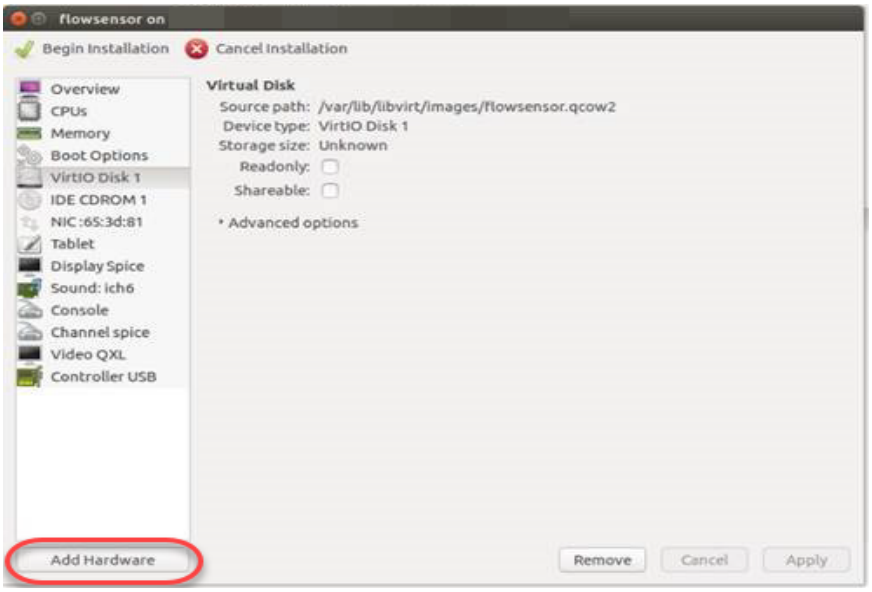
    - 「はい」の場合、「**2. NIC（Data Node、Flow Sensor）および Open vSwitch での無差別ポートの監視（Flow Sensor のみ）の追加**」に進みます。
    - 「いいえ」の場合、次の手順に進みます。

21. [インストールの開始（Begin Installation）] をクリックします。
22. 「**4. 初回セットアップを使用した環境の設定**」に進みます。

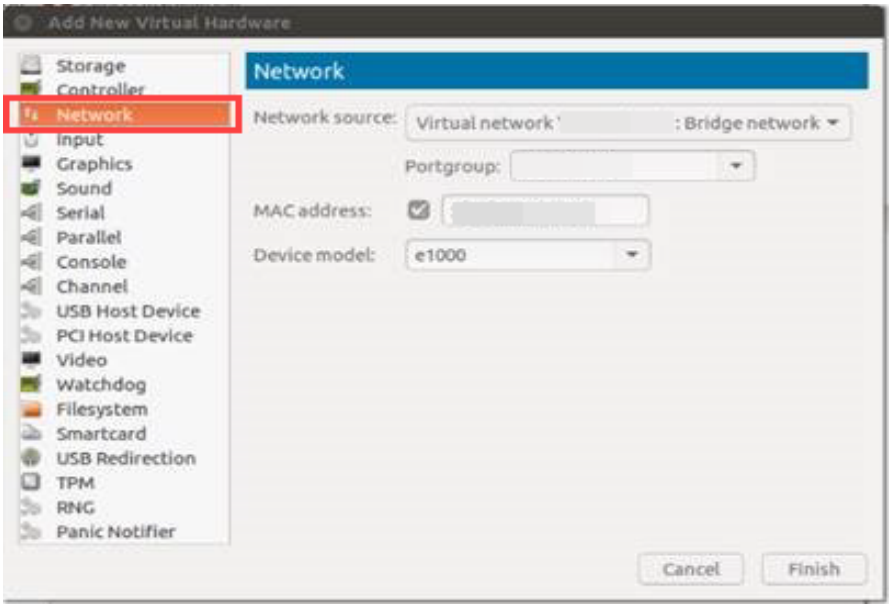
2. NIC（Data Node、Flow Sensor）および Open vSwitch での無差別ポートの監視（Flow Sensor のみ）の追加

Flow Sensor VE 監視ポート用または データノード VE 用の NIC を追加し、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。



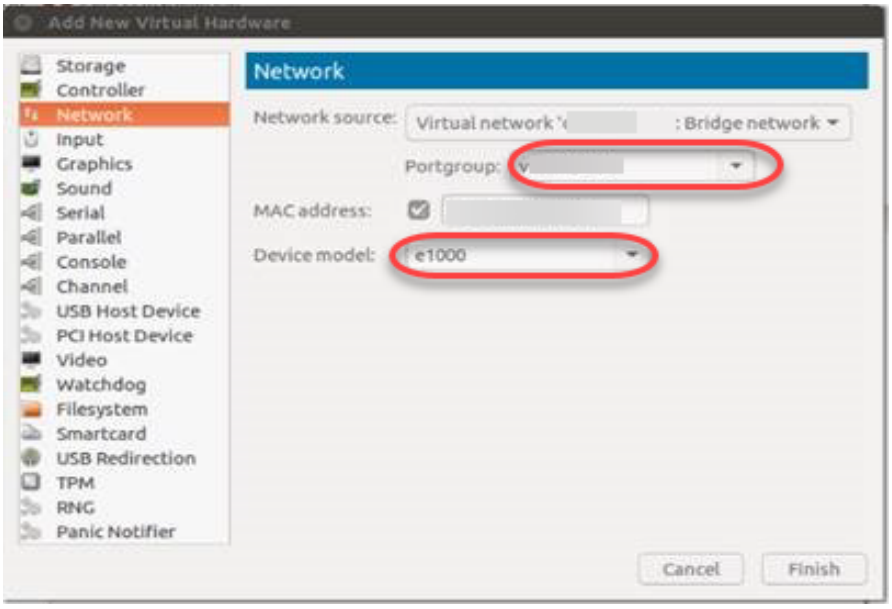
2. 左側のナビゲーション ウィンドウで [ネットワーク（Network）] をクリックします。



3. 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。

   データノード の場合は、「**データノード の独立 LAN の設定**」で作成した構成を使用して、独立 LAN での データノード 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. 初回セットアップを使用した環境の設定

VMware または KVM を使用して Stealthwatch VE アプライアンスをインストールしたら、それらの仮想環境を設定できます。

目的とするアプライアンスの手順を選んでください。

- **Stealthwatch 管理コンソールまたはフローコレクタの設定**
- **Data Node の設定**
- **Flow Sensor または UDP Director の設定**

Stealthwatch 管理コンソールまたはフローコレクタの設定

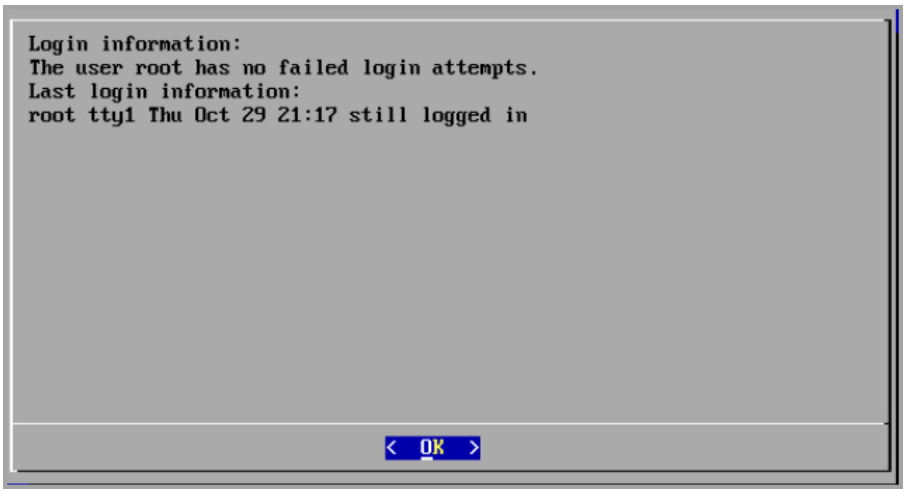
1. ハイパーバイザ ホスト(仮想マシン ホスト)に接続します。
2. ハイパーバイザ ホストで仮想マシンを見つけます。
3. 仮想マシンの電源が入っていることを確認します。

   仮想マシンの電源が入っていない場合や、使用可能なメモリの不足に関するエラー メッセージを受信した場合、次のいずれかを実行します。

   - **リソース**:アプライアンスがインストールされているシステムの使用可能リソースを増やします。詳細については、「**リソース要件**」セクションを参照してください。
   - **VMware 環境**:アプライアンスのメモリ予約制限とリソース プールを増やします。

> ⚠ 「**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 Stealthwatch 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。

4. 仮想マシン コンソールにアクセスします。仮想アプライアンスの起動が完了します。
5. コンソールでログインします。
   - **ログイン**:root
   - **デフォルト パスワード**:lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
6. コマンドプロンプトで、`SystemConfig` と入力します。Enter キーを押します。
7. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。

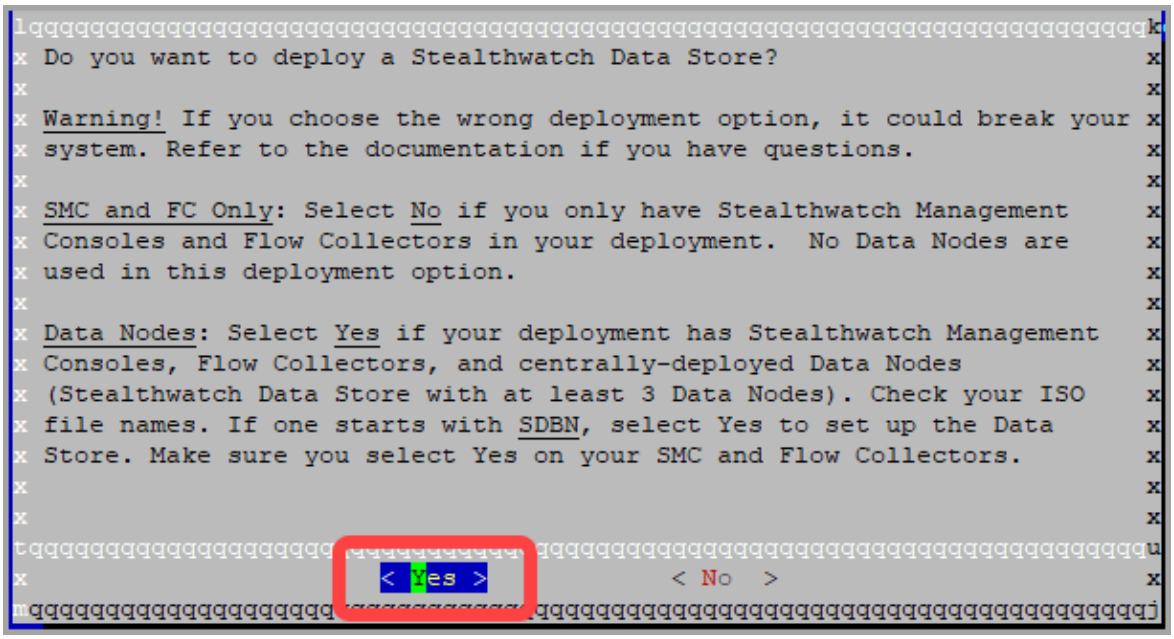


8. 初回セットアップの概要を確認します。[OK]を選択して続行します。

9. [データストアを展開しますか?(Do you want to deploy a Data Store ?)]で、[Yes]を選択します。

   SMC とフローコレクタ:SMC とFlow Collectorについては、[Yes]を選択してください。

> ⚠ データストア とともに使用するために SMC またはフローコレクタを設定することを選択した後は、この構成は変更できません。ネットワークに データストア を展開する場合に**のみ**、[Yes]を選択してください。
>
> 選択を誤った場合は、新しい仮想アプライアンスを展開するか、仮想アプライアンスを RFD してください。

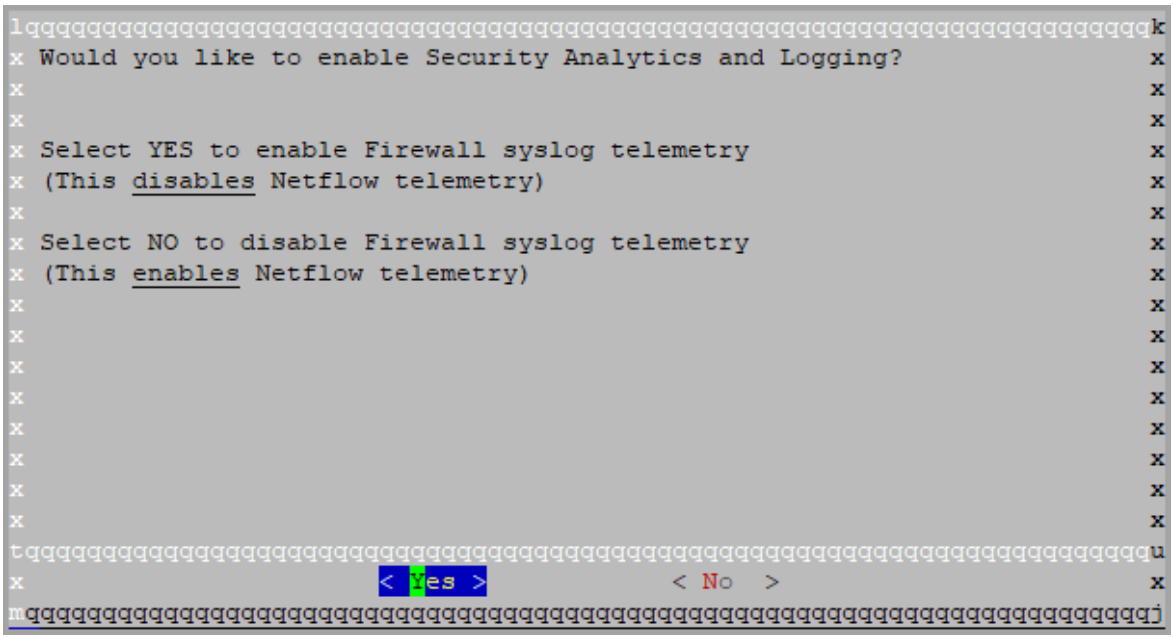


10. **[セキュリティ分析とロギングを有効にしますか?(Do you want to enable Security Analytics and Logging?)]で、**[Yes]または[No]を選択します。

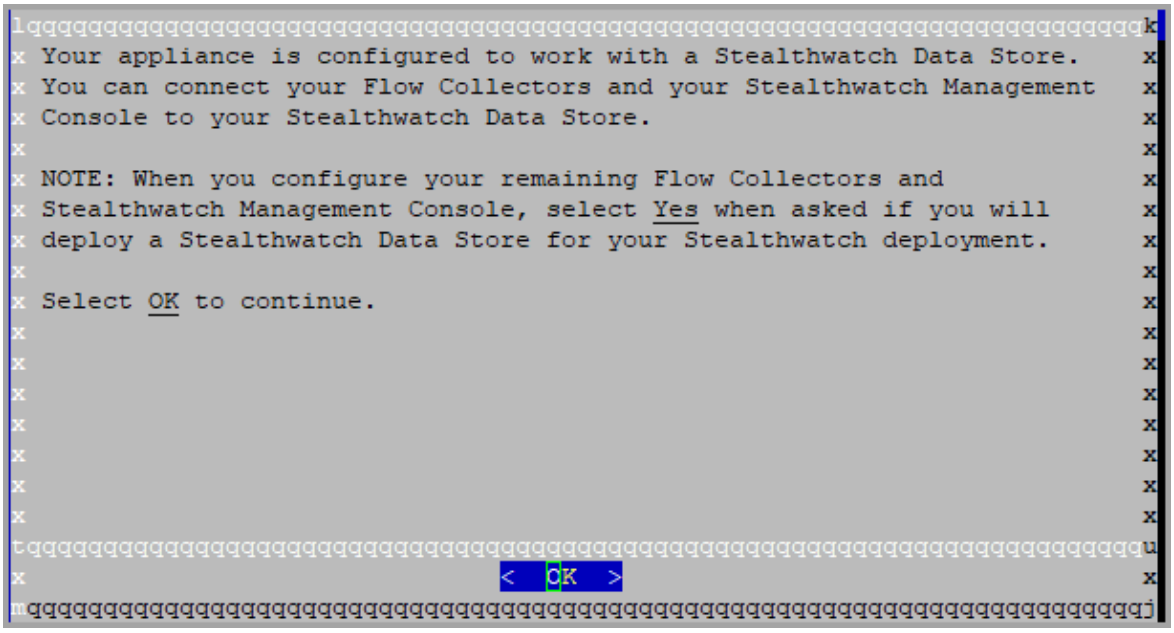
詳細情報:Security Analytics and Logging(オンプレミス)を有効にする場合は、Stealthwatchの展開を使用してFirepowerイベント情報を保存します。これによってフローコレクタでNetFlow収集が無効になることに注意してください。

- **SMCとフローコレクタ**:SMCでセキュリティ分析とロギングを有効にする場合は、Flow CollectorでSALを有効にする必要があります。
- **ガイド**:詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。
- **アプリケーション要件**:Security Analytics and Logging(オンプレミス)を設定する場合は、Stealthwatch Management ConsoleでSecurity Analytics and Logging(オンプレミス)アプリをインストールします。

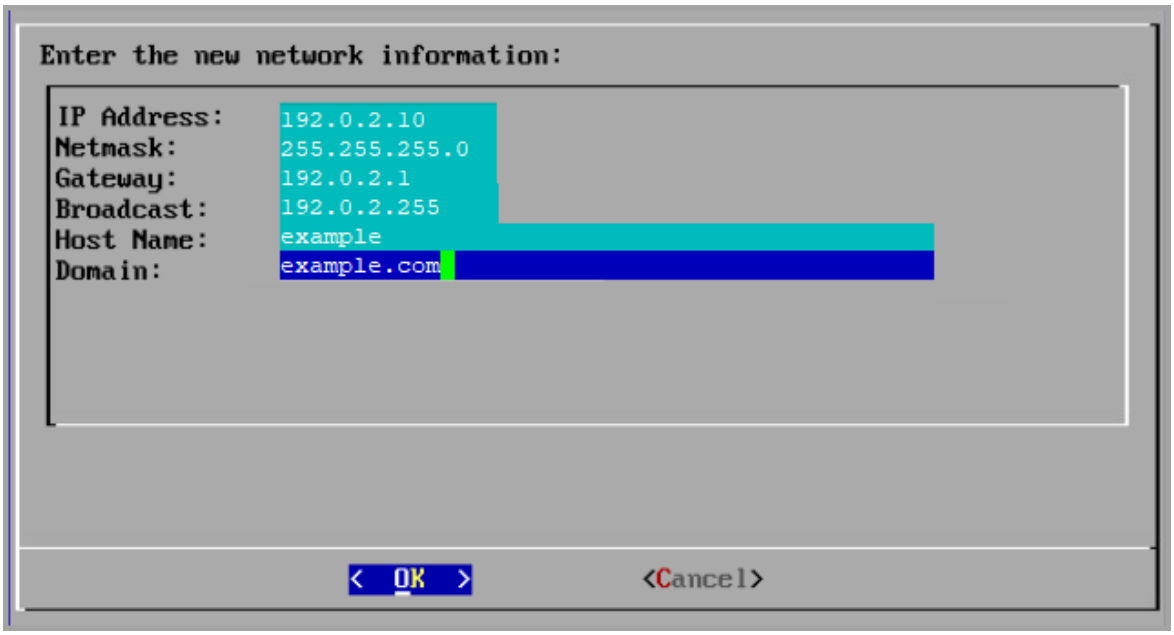
> ⚠ Security Analytics and Logging(オンプレミス)とともに使用するためにSMCまたはフローコレクタを設定することを選択した後は、この構成は変更できません。Security Analytics and Logging(オンプレミス)にStealthwatchを使用してFirepowerイベント情報を保存する場合に**のみ**、[Yes]を選択してください。
>
> 選択を誤った場合は、新しい仮想アプライアンスを展開するか、仮想アプライアンスをRFDしてください。



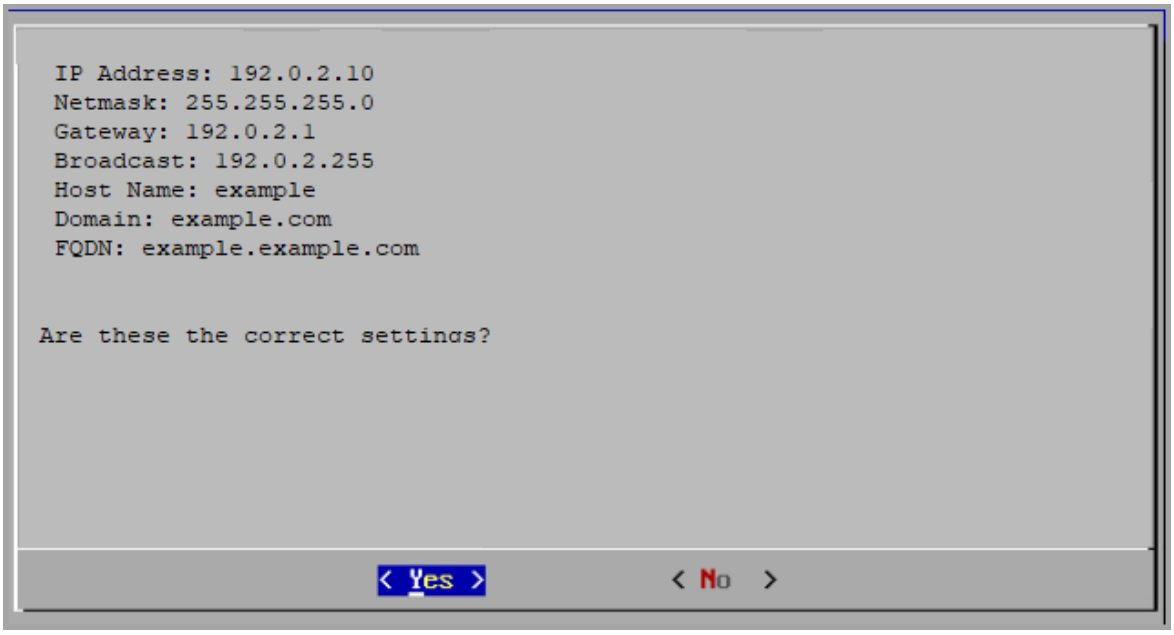
11. [OK]を選択して選択を確定します。



12. 管理インターフェイスの[IPアドレス(IP Address)]、[ネットマスク(Netmask)]、[ゲートウェイ(Gateway)]、[ブロードキャスト(Broadcast)]、[ホスト名(Host Name)]、[ドメイン(Domain)]を入力し、[OK]を選択して続行します。



13. 設定を確認します。[Yes]を選択して続行します。



14. [OK]を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
15. Ctrl + Alt を押して、コンソールを終了します。
16. 「**4. 初回セットアップを使用した環境の設定**」のすべての手順を、システム内の次の SMC またはFlow Collectorについて繰り返します。

    初回セットアップですべての SMC とFlow Collectorを設定した場合は、「**Data Node の設定**」に進みます。

Data Node の設定

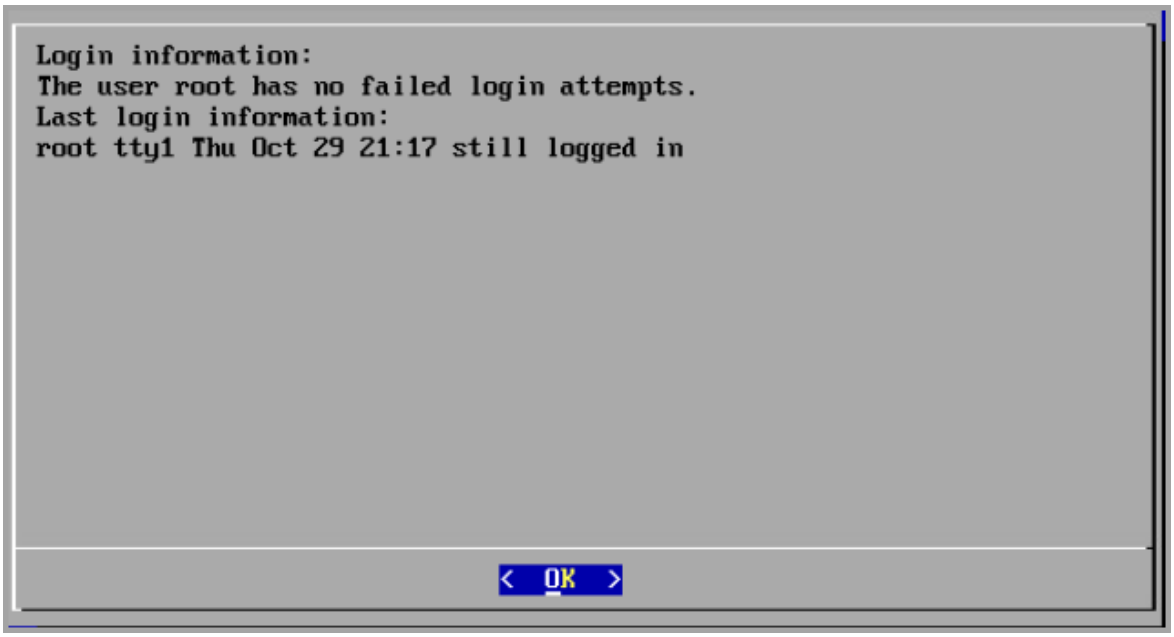
1. ハイパーバイザ ホスト(仮想マシン ホスト)に接続します。
2. ハイパーバイザ ホストで仮想マシンを見つけます。
3. 仮想マシンの電源が入っていることを確認します。

   仮想マシンの電源が入っていない場合や、使用可能なメモリの不足に関するエラー メッセージを受信した場合、次のいずれかを実行します。

   - **リソース**:アプライアンスがインストールされているシステムの使用可能リソースを増やします。詳細については、「**リソース要件**」セクションを参照してください。
   - **VMware 環境**:アプライアンスのメモリ予約制限とリソース プールを増やします。

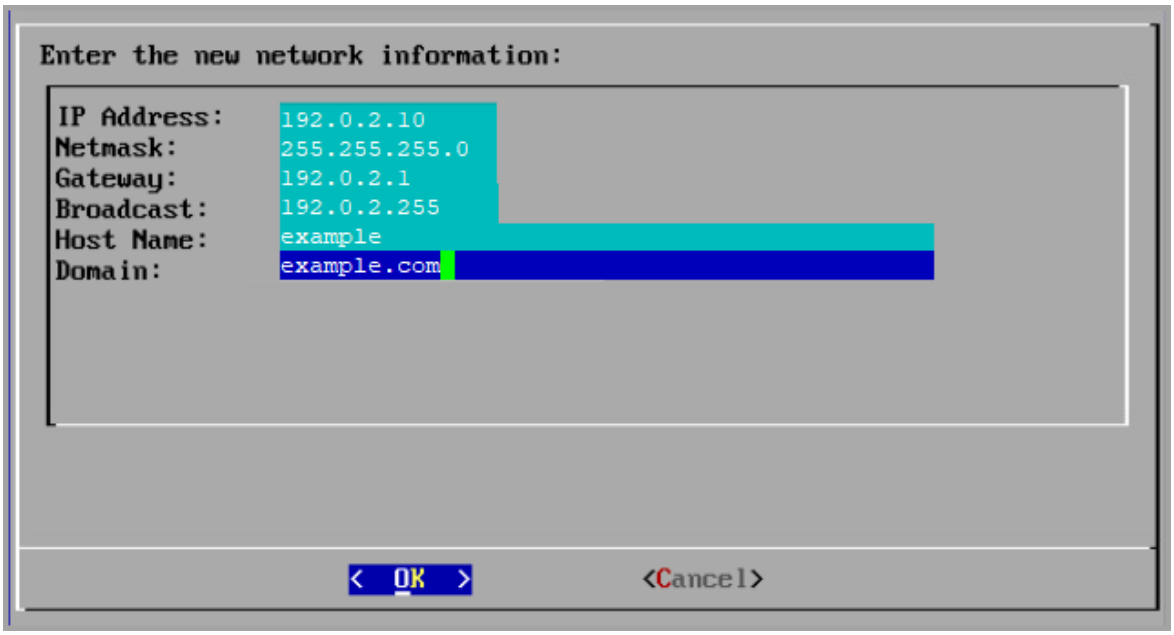
> ⚠ 「**リソース要件**」を確認して、十分なリソースを割り当てます。この手順は、システム パフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

4. 仮想マシン コンソールにアクセスします。仮想アプライアンスの起動が完了します。
5. コンソールでログインします。
   - **ログイン**:root
   - **デフォルト パスワード**:lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
6. コマンドプロンプトで、`SystemConfig` と入力します。Enter キーを押します。
7. 失敗したログイン試行の情報を確認します。[OK]を選択して続行します。

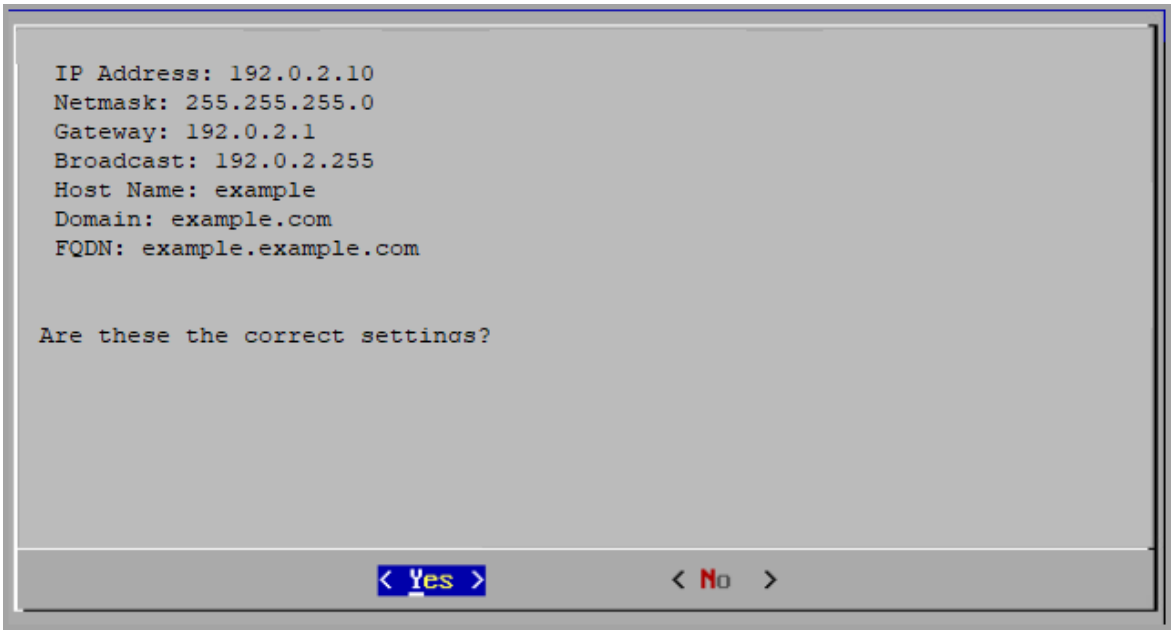


8. 初回セットアップの概要を確認します。[OK]を選択して続行します。

9. 管理インターフェイスの[IPアドレス(IP Address)]、[ネットマスク(Netmask)]、[ゲートウェイ(Gateway)]、[ブロードキャスト(Broadcast)]、[ホスト名(Host Name)]、[ドメイン(Domain)]を入力し、[OK]を選択して続行します。

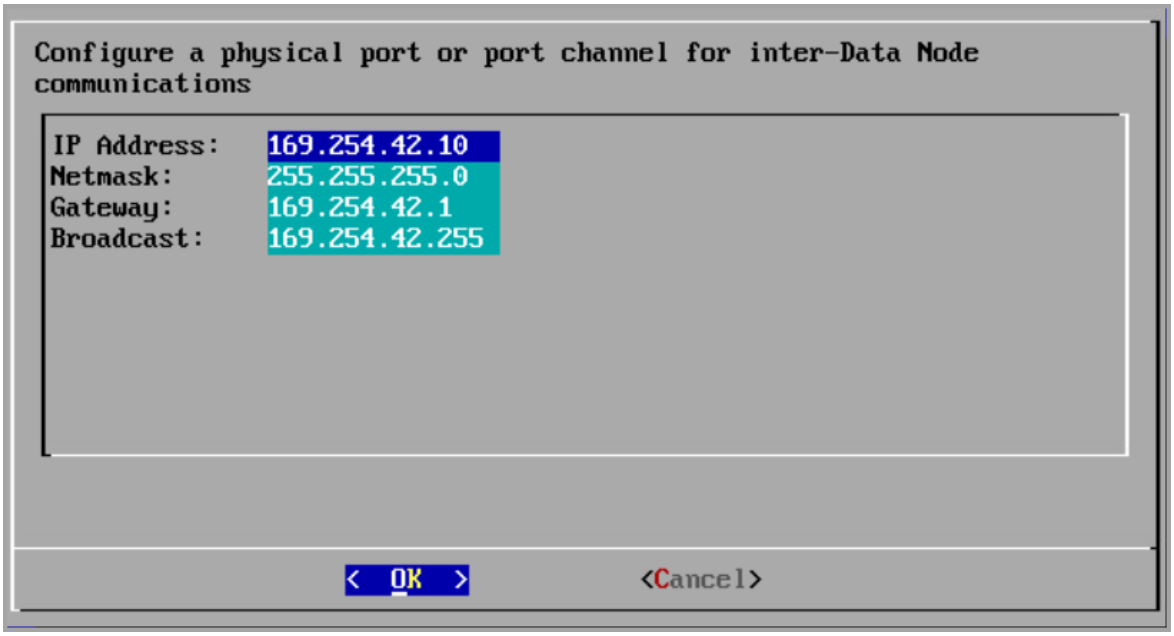


10. 設定を確認します。[Yes]を選択して続行します。

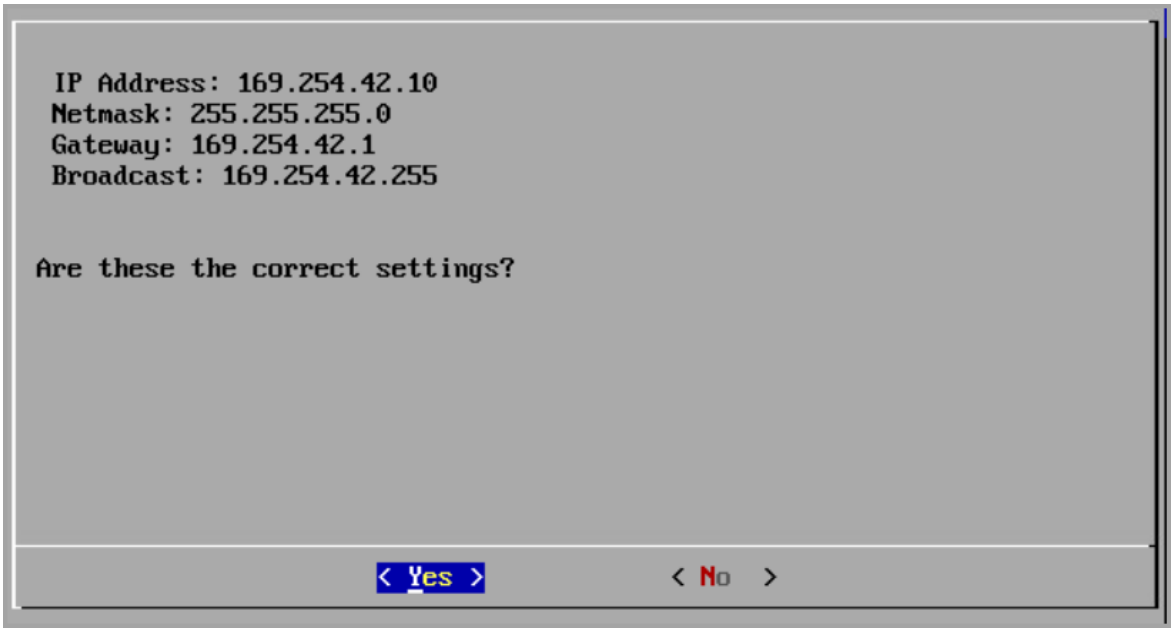


11. [OK]を選択して選択を確定します。画面に表示される指示に従って操作します。
12. データノード間通信用の物理ポートまたはポートチャネルを設定します。次を入力します。
    - [IPアドレス(IP Address)]: 169.254.42.0/24 CIDR ブロック(169.254.42.2 ～ 169.254.42.254)のルーティング不可能な**IP アドレス**を持つ、データノード間通信用の `eth1` インターフェイス。メンテナンスを容易にするために、連続した IP アドレス(169.254.42.10、169.254.42.20、169.254.42.30 など)を選択します。

- [ネットマスク(Netmask)]:255.255.255.0
- [ゲートウェイ(Gateway)]:169.254.42.1
- [ブロードキャスト(Broadcast)]:169.254.42.255



13. [OK]を選択して続行します。
14. 設定を確認します。[Yes]を選択して続行します。



15. 画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
16. Ctrl + Alt を押して、コンソールを終了します。

17. システム内の次の データノード について、「Data Node の設定」のすべての手順を繰り返します。

    - 初回セットアップですべての データノード を設定した場合は、「Flow Sensor または UDP Director の設定」に進みます。
    - 初回セットアップですべての仮想アプライアンスを設定した場合は、「5. Stealthwatch システムの設定」に進みます。

Flow Sensor または UDP Director の設定

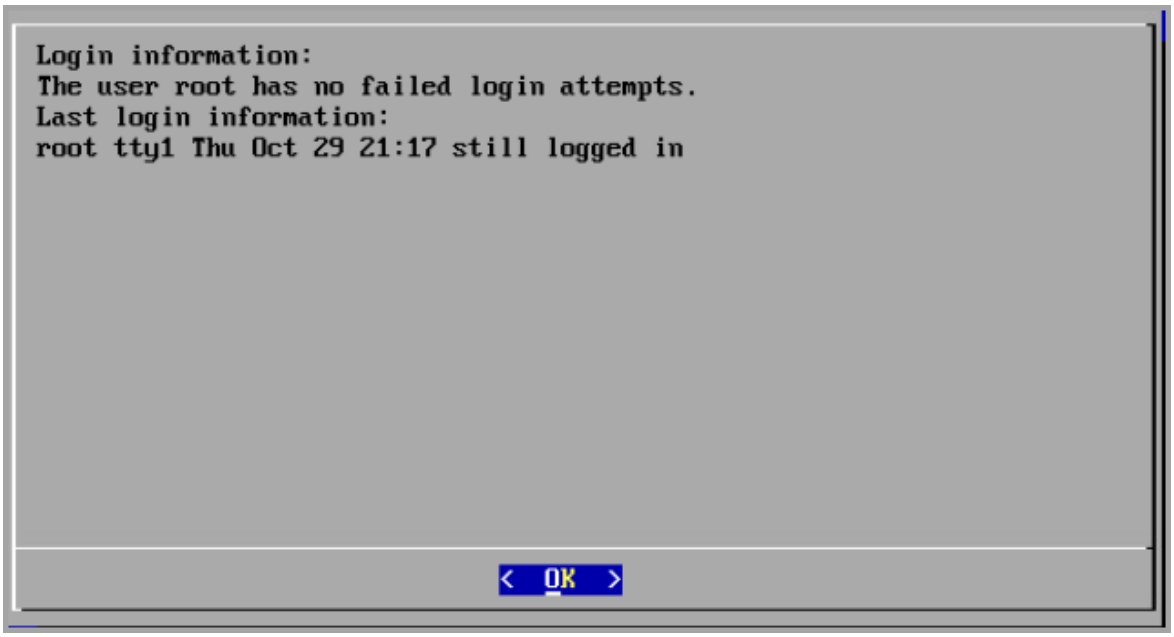
1. ハイパーバイザ ホスト(仮想マシン ホスト)に接続します。
2. ハイパーバイザ ホストで仮想マシンを見つけます。
3. 仮想マシンの電源が入っていることを確認します。

   仮想マシンの電源が入っていない場合や、使用可能なメモリの不足に関するエラー メッセージを受信した場合、次のいずれかを実行します。

   - **リソース**:アプライアンスがインストールされているシステムの使用可能リソースを増やします。詳細については、「リソース要件」セクションを参照してください。
   - **VMware 環境**:アプライアンスのメモリ予約制限とリソース プールを増やします。

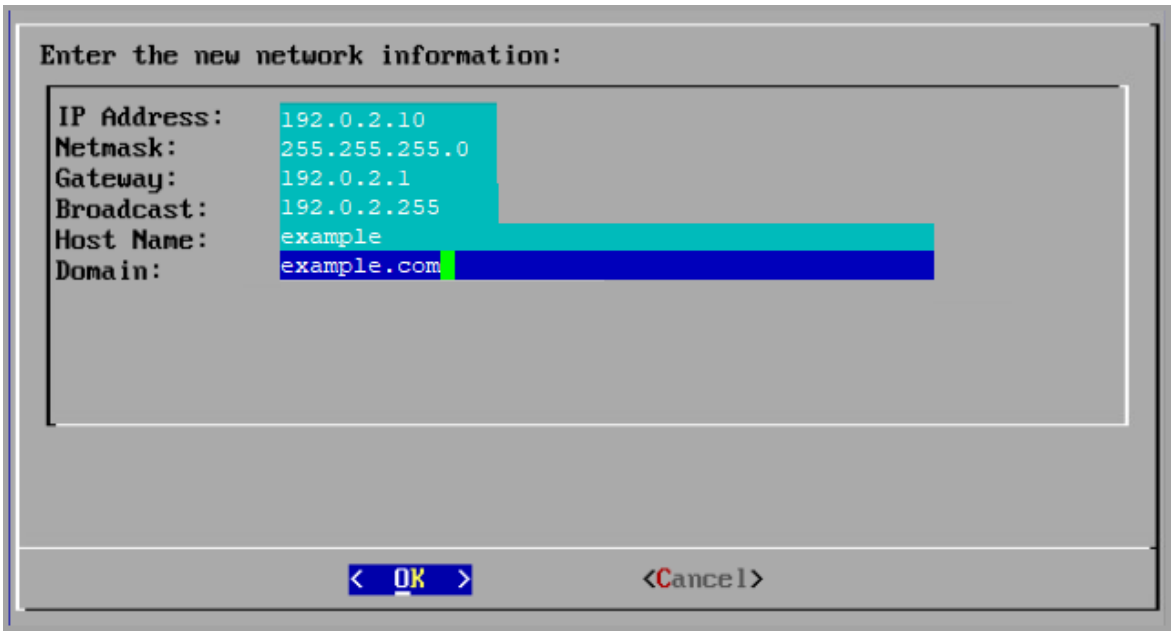
> ⚠ 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システム パフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

4. 仮想マシン コンソールにアクセスします。仮想アプライアンスの起動が完了します。
5. コンソールでログインします。
   - **ログイン**:root
   - **デフォルト パスワード**:lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
6. コマンドプロンプトで、`SystemConfig` と入力します。Enter キーを押します。
7. 失敗したログイン試行の情報を確認します。[OK]を選択して続行します。

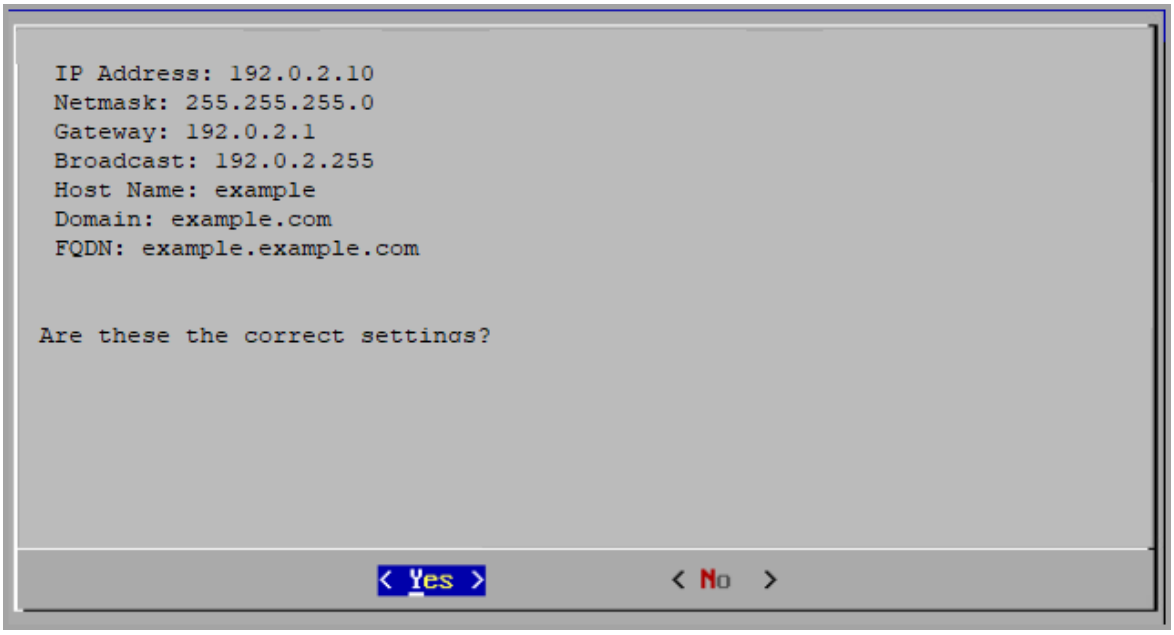


8. 初回セットアップの概要を確認します。[OK]を選択して続行します。

9. 管理インターフェイスの[IPアドレス(IP Address)]、[ネットマスク(Netmask)]、[ゲートウェイ(Gateway)]、[ブロードキャスト(Broadcast)]、[ホスト名(Host Name)]、[ドメイン(Domain)]を入力し、[OK]を選択して続行します。



10. 設定を確認します。[Yes]を選択して続行します。



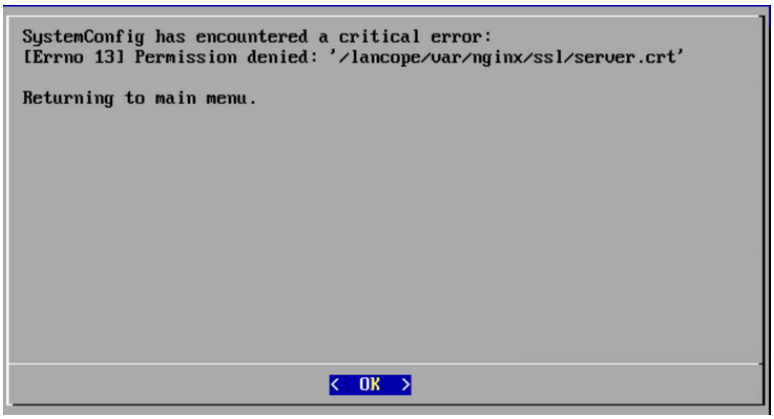
11. [OK]を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
12. Ctrl + Alt を押して、コンソールを終了します。
13. 「**4. 初回セットアップを使用した環境の設定**」のすべての手順を、システム内の次の仮想アプライアンスについて繰り返します。

    初回セットアップですべての仮想アプライアンスを設定した場合は、「**5. Stealthwatch システムの設定**」に進みます。

トラブルシューティング

証明書エラー

VM 環境の使用率が高い場合は、タイミングエラーが発生し、一部のイベントが順不同で発生する可能性があります。証明書エラー(.crt)が原因で権限が拒否されるという次のようなエラーが表示される場合は、次の手順を実行します。



1. アプライアンスコンソールに sysadmin としてログインします。デフォルトのパスワードは、lan1cope です。

   システムを設定するときに、デフォルトのパスワードを変更します。詳細については、『Stealthwatch System Configuration Guide』を参照してください。

2. 次のコマンドを実行します。

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

3. SystemConfig を実行します。
4. 「**4. 初回セットアップを使用した環境の設定**」(ステップ 5 以降)に戻り、セクションのすべてのステップを実行します。アプライアンスにアクセスできない場合は、Cisco Stealthwatch サポートにお問い合わせください。

アプライアンスへのアクセス

再起動後にアプライアンスにアクセスできない場合は、次の手順を実行します。

1. root としてログインします。
2. 次のコマンドを実行して、Docker コンテナおよびサービスが稼働していることを確認します。

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

3. すべての Docker コンテナおよびサービスが稼働状態になったら、ログインを再試行します。アプライアンスにアクセスできない場合は、Cisco Stealthwatch サポートにお問い合わせください。

5. Stealthwatch システムの設定

SMC VE、データノード VE、および Flow Collector VE を展開する際は、『Stealthwatch System Configuration Guide v7.3.2』を使用してそのアプライアンスを設定し、次の点に注意してください。

- **証明書**：アプライアンスは、一意の自己署名アプライアンス アイデンティティ証明書とともにインストールされます。
- **Central Management**：プライマリ SMC/Central Manager を使用して、アプライアンスを管理し、構成設定を変更してください。

次のアプライアンスに進む前に、Central Management で各アプライアンスが稼働していることを確認します。SMC VE、データノード VE、および Flow Collector VE を Stealthwatch に展開して設定した後、『Data Store Virtual Edition Deployment and Configuration Guide』を使用して、Data Store を初期化し、フローインターフェイス統計データの保持を設定します。

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。
- Cisco Stealthwatch サポートのお問い合わせ先：
- 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