Stealthwatch®

Flow Sensor™ Virtual Edition

インストール/コンフィギュレーション ガイド

(Stealthwatch System v6.9.0 用)

インストール/コンフィギュレーション ガイド : Flow Sensor VE v6.9.0

ドキュメントの日付 : 2017 年 2 月 16 日

シスコの商標

目次

1

はじめに

概要

これは、vSphere Client v4.x 以降を使用するネットワーク内の Flow Sensor VE 向けのインストレーション コンフィギュレーション ガイドです。

(注) VMware ESX v3.x で実行されている Stealthwatch VE アプライアンスは、ESX v4.x と互換性がありません。VMware を ESX v4.x にアップグレードする場合、既存の Stealthwatch VE アプライアンスを削除して再インストールする必要があります。

StealthWatch システムの物理アプライアンスについては、『Stealthwatch System Hardware Installation Guide』と『Stealthwatch System Hardware Configuration Guide』を参照してください。

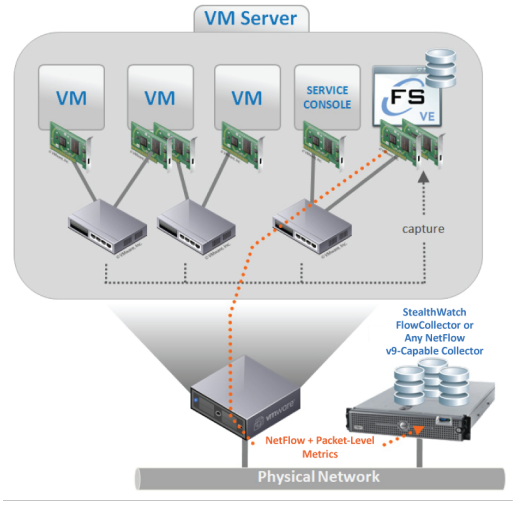
必要に応じて、このガイドの詳細およびサポートへの問い合わせ方法についてはこの章を参照してください。この章の内容は、次のとおりです。

対象読者

このガイドの主な対象者は、StealthWatch Flow Sensor VE アプライアンスをインストールして設定する必要がある管理者です。このガイドは、対象読者が VMware ソフトウェアの基本を理解していることを前提としています。

Flow Sensor VE について

Flow Sensor VE は、StealthWatch Flow Sensor アプライアンスと同じテクノロジーを採用した仮想アプライアンスであり、VMware 環境を可視化し、フローに対応していない領域のフローデータを生成します。



各 vSphere/ESX ホスト内にインストールされている仮想アプライアンスとして、Flow Sensor VE は仮想スイッチに無差別に接続します。インストールが完了すると、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。その後、Flow Sensor VE は任意の NetFlow v9 対応 Flow Collector にこれらのレコードを送信します。

Flow Sensor VE を NetFlow v9 対応の Flow Collector に向けて誘導することで、貴重なトラフィック詳細統計情報を NetFlow から得ることができます。また、Flow Sensor を Stealthwatch Flow Collector for NetFlow と組み合わせると、パフォーマンス指標や動作指標に関する深い洞察を得ることができます。これらのフロー パフォーマンス指標から、ネットワークまたはサーバ側アプリケーションに由来するラウンドトリップ遅延についての洞察が得られます。

Flow Sensor VE はパケット レベルの可視性を備えているので、TCP セッションのラウンドトリップ時間(RTT)、サーバ応答時間(SRT)、およびパケット損失を計算できます。これには、Stealthwatch Flow Collector for NetFlow に送られる NetFlow レコード内のこのような追加的フィールドがすべて含まれます。

はじめる前に

このセクションの情報を使用して、Stealthwatch VE アプライアンスのインストールおよび設定を準備します。設定は、vSphere Client インターフェイスを使用するプロセスとアプライアンス管理インターフェイスを使用するプロセスの 2 つで構成されています。このセクションに示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できます。

次の順序で仮想アプライアンスをインストールおよび設定する必要があります。

1. エンドポイント コンセントレータ
2. UDP Director VE
3. Flow Sensor VE

4. Flow Collector VE
5. SMC VE

Stealthwatch システムの設定時にこの推奨された順序に従わなければ、Stealthwatch システムはアプライアンスから適切にデータを収集できず、それぞれを個別に設定する必要がでてきます。

注意! 仮想アプライアンスをインストールする ESX サーバに設定された時間が正しい時間を示していることを確認します。正しくなければ、アプライアンスを起動できない場合があります。

VE ソフトウェアのダウンロード

このガイドの手順を実行する前に、ダウンロードおよびライセンス センターから OVF(オープン仮想化フォーマット) ファイルを取得する必要があります。各アプライアンスのファイルをダウンロードする方法については、ライセンスのダウンロード センターまたは StealthWatch アプライアンスのヘルプにあるドキュメント ライブラリの『Downloading and Licensing Stealthwatch Products』ドキュメントを参照してください。

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。

Flow Sensor VE

v6.8.0 以降の StealthWatch システムでは、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。すべての VE アプライアンス導入環境では、最初にディスク容量として 50 GB が必要です。

	NIC - モニタリング ポート	予約済み CPU	予約済み メモリ	スループット
Flow Sensor VE	1	1	4 GB	100 Mbps/512 バイト 40 Mbps/64 バイト

Flow Sensor VE

Flow Sensor VE を使用するには、VMware サーバが次の仕様に一致している必要があります。

- 4096 MB RAM
- 4 GB のディスク容量(8 GB を推奨)

(注) vNetwork Distributed Switch(VDS)環境では、各 Flow Sensor VE に 512 MB RAM のリソースプールが 1 つ必要です。

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おく必要があります。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。区別すべき主な点は、ネットワークが VDS を使用するかどうかです。

(注) StealthWatch は VDS 環境をサポートしていますが、VMware Distributed Resource Scheduler(VM-DRS)をサポートしません。

Flow Sensor VE は、次のタイプの VDS ネットワーク環境をモニタします。

- 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
- ESX ホスト(VLAN ではない)

vSphere Client インターフェイスに必要な情報

設定	ESX/vSphere サーバ	Flow Sensor VE
ログイン ユーザ名		
ログイン パスワード		
IP アドレス		(デフォルト = 192.168.1.6)
ネットマスク IP アドレス		(デフォルト = 255.255.255.0)
ゲートウェイIP アドレス		(デフォルト = 192.168.1.1)

アプライアンス管理インターフェイスに必要な情報

設定	Flow Sensor VE
IP アドレス	(デフォルト = 192.168.1.6)
ホスト名	
ネットワークドメイン名	

設定	Flow Sensor VE
NTP サーバの IP アドレス	
DNS サーバの IP アドレス	

Flow Sensor VE には次の追加情報が必要です。

Flow Sensor VE からデータを受信する各 NetFlow コレクタまたは UDP Director™ の IP アドレスとリスニング ポート番号 (デフォルト = 2055)

このマニュアルの使い方

「はじめに」の他に、このガイドは次の章に分かれています。

章	説明
仮想アプライアンスのインストール	vSphere Client v4.x 以降を使用して ESX サーバに VE アプライアンスをインストールする方法
仮想環境の設定	アプライアンスの仮想環境を設定する方法
仮想アプライアンス システムの設定	トラフィック データの処理を開始するようにアプライアンスを設定する方法

略語

このガイドでは、次の略語が使用されます。

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	エンタープライズ サーバ 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
IT	情報技術
MTU	最大伝送ユニット
NTP	ネットワーク タイム プロトコル
OVF	オープン仮想化フォーマット

略語	定義
SMC	Stealthwatch 管理コンソール
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

その他のリソース

このガイド以外に、次のドキュメントおよびオンライン リソースが役に立ちます。

関連資料

Stealthwatch アプライアンスとそのインストールおよび設定に関する詳細については、Stealthwatch マニュアルを参照してください。Stealthwatch 製品の詳細については、オンラインの Cisco Stealthwatch [英語] を参照してください。

詳細情報は、Lancope のコミュニティ Web サイト (https://lancope.force.com/Customer/CustomerCommLogin) [英語] を参照してください。Web サイトへのログイン アクセス権がない場合は、サポートに電子メールを送信してアクセス権を要求してください。

Lancope のブログ

Lancope の「Inside the Threat」ブログ(http://www.lancope.com/blog/) [英語] には、NetFlow、NetFlow 業界、および新しい Stealthwatch 機能に関する豊富な情報と Stealthwatch を使用する際のヒントが掲載されています。

Lancope の高度なサイバーセキュリティ向けリソース & ツール

Stealthwatch の詳細については、Lancope の高度なサイバーセキュリティ向けリソース & ツールのサイト(https://www.lancope.com/resources) [英語] を参照してください。オンライン ビデオ ライブラリ、ホワイト ペーパー、ウェビナーなどのリソースが提供されています。

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
- お電話でのお問い合わせ(+1 800-838-6574)
- Lancope のカスタマー コミュニティ Web サイト (https://lancope.force.com/Customer/CustomerCommLogin) のサポート フォームを使用して問題を送信

ドキュメント フィードバック

このマニュアルについてコメントがございましたら、support@lancope.com にご連絡ください。ご協力をよろしくお願いいたします。

2

仮想アプライアンスのインストール

概要

(注) Stealthwatch の物理アプライアンスをインストールする方法については、『Stealthwatch System v6.x Hardware Installation Guide』を参照してください。

この章では、VMware vSphere Client v4.x 以降を使用した、仮想アプライアンスをインストールする方法を説明します。

(注) 仮想アプライアンスをインストールする ESX サーバに設定された時間が正しい時間を示していることを確認してください。正しくなければ、仮想アプライアンスを起動できない場合があります。

注意! 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。

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します。

1. 通信用ファイアウォールの設定
2. VMware vSphere Client へのログイン
3. 分散型仮想ポート グループの追加
4. リソース プールの追加
5. 無差別ポート グループの追加
6. 仮想アプライアンスのインストール
7. 追加モニタリング ポートの定義

重要： ネットワークに vNetwork Distributed Switch(VDS) が存在する場合は、ステップ 3 で dvPort グループを追加する必要があります。ネットワークに VDS が存在しない場合は、ステップ 5 で無差別ポート グループを追加します。

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。アプライアンスがネットワーク経由で通信できるように、このセクションに示す図と表表を使用してネットワークを設定します。

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

通信ポート

Stealthwatch システム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

送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
Active Directory	SMC	TCP/389、UDP/389	LDAP
AnyConnect	エンドポイント コンセントレータ	UDP/2055	NetFlow
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	TCP/5222	XMPP
エンドポイント コンセントレータ	Flow Collector	UDP/2055	NetFlow
外部ログ ソース	SMC	UDP/514	SYSLOG
Flow Collector	SMC	TCP/443	HTTPS
SLIC	SMC	TCP/443 またはプロキシされた接続	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
アイデンティティ	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	DNS	UDP/53	DNS
SMC	Flow Collector	TCP/443	HTTPS

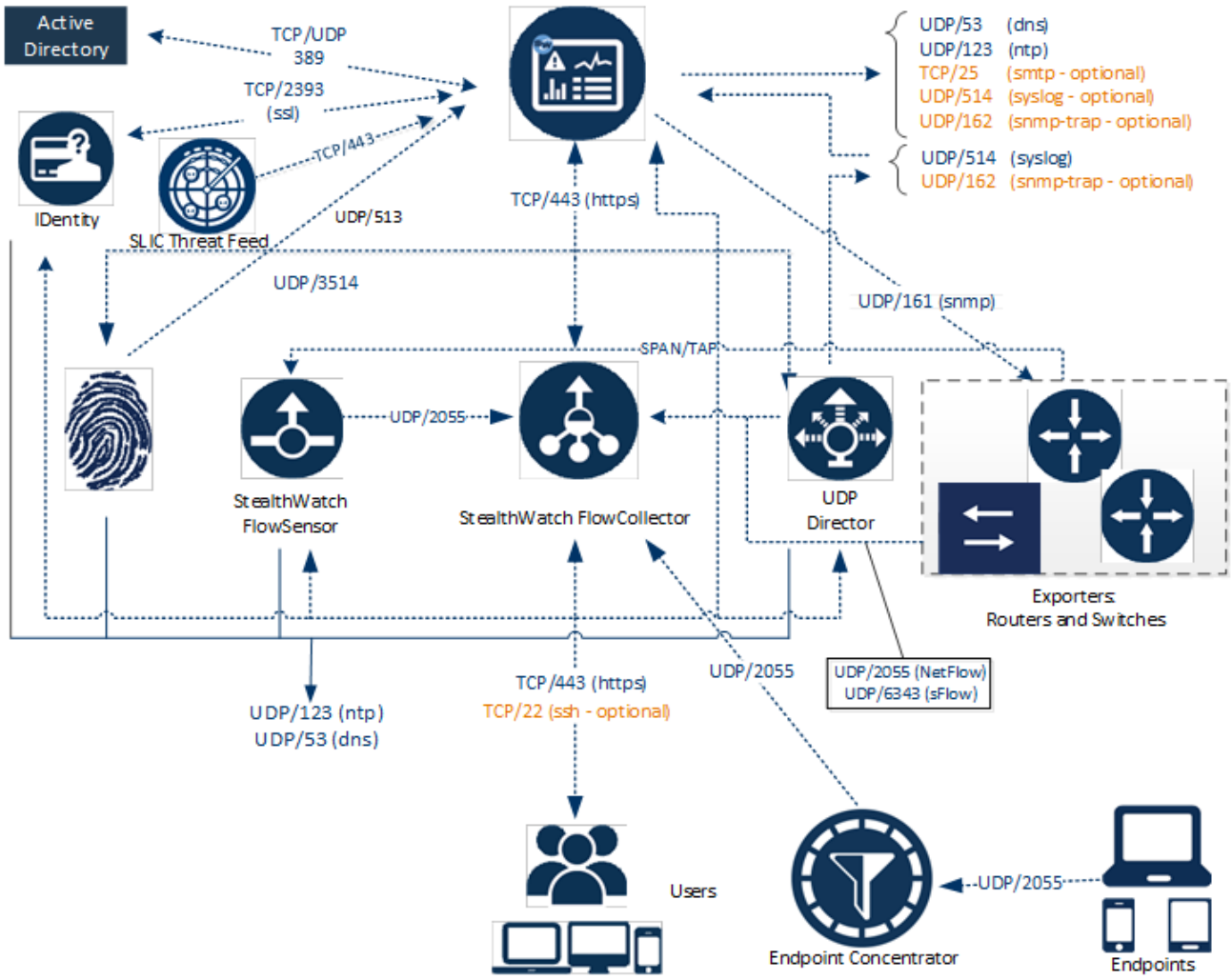
送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
SMC	Flow Sensor	TCP/443	HTTPS
SMC	アイデンティティ	TCP/2393	SSL
SMC	フロー エクスポータ	UDP/161	SNMP
SMC	エンドポイント コンセントレータ	UDP.2055	HTTPS
ユーザ PC	SMC	TCP/443	HTTPS

* これはデフォルト NetFlow 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。

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	SLIC	TCP/443	SSL
ユーザ PC	すべてのアプライアンス	TCP/22	SSH

次の図は、Stealthwatch 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。オプション(optional)というマークが付いたポートを、ネットワーク要件に応じて使用することができます。



VMware vSphere 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、次の手順を実行して、まず VMware vSphere Client にログインする必要があります。

(注) 画面イメージは VMWare v5.0 のものです。ご使用の画面とわずかに異なる場合がありますが、コマンドは同じです。VMware Web クライアント インターフェイスを使用する場合、ここに表示されるいくつかの画面は異なります。そのため、必要に応じて、選択するオプションの違いを示します。

1. VMware vSphere Client ソフトウェアを起動します。ログイン ダイアログが開きます。

2. ESX サーバの IP アドレスとログイン クレデンシャルを入力して、[ログイン(Login)] をクリックします。ホーム ページが開きます。
3. 次の「リソース プールの追加」セクションに進みます。
4. Flow Sensor VE を VDS 環境にインストールしますか。(VDS 環境の詳細については、を参照してください) 。
   - 「はい」の場合、次の「分散型仮想ポート グループの追加」セクションに進みます。
   - 「いいえ」の場合、「リソース プールの追加」(19 ページ) に進みます。

分散型仮想ポート グループの追加

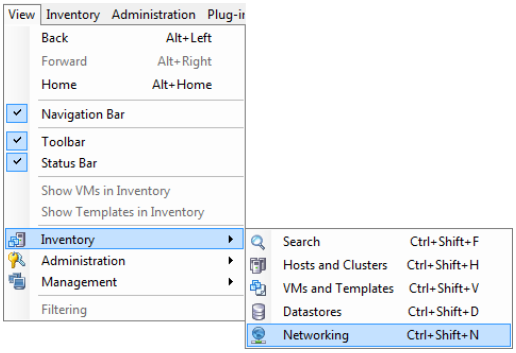
(注) このセクションの内容は、VDS ネットワークにのみ該当します。VDS 以外の環境のネットワークでは、リソース プールの追加に進みます。

VDS を使用するネットワークでは、Flow Sensor VE のモニタ対象となる VDS ごとに、正しい VLAN 設定を使用して分散仮想ポート(dvPort) グループを追加する必要があります。

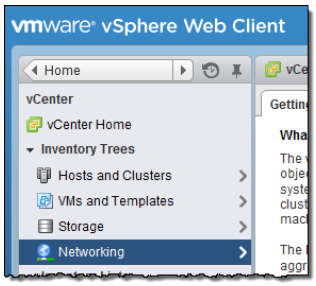
(注) (VLAN トランキングおよびプライベート VLAN 以外の) VLAN を使用している環境では、この手順を行うために VLAN ID が必要です。Flow Sensor VE がネットワーク上の VLAN トラフィックと非 VLAN トラフィックの両方をモニタする場合は、それぞれのトラフィック タイプ用に 1 つずつ、合計 2 つの dvPort グループを作成する必要があります。

dvPort グループを追加するには、次の手順を実行します。

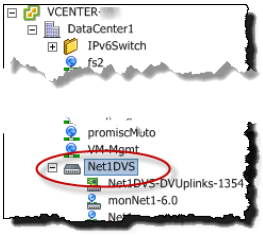
1. [表示(View)] メニューで [インベントリ(Inventory)] > [ネットワーキング(Networking)] を選択します。左側に [ネットワーキング(Networking)] ツリーが表示されます。



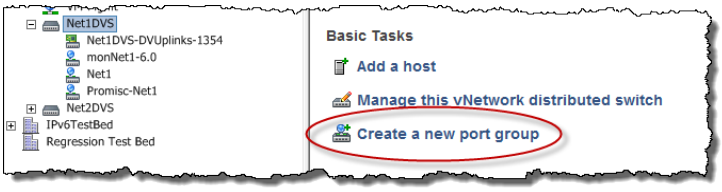
Web クライアントで、[インベントリツリー(Inventory Trees)] リストの [ネットワーキング (Networking)] をクリックします。



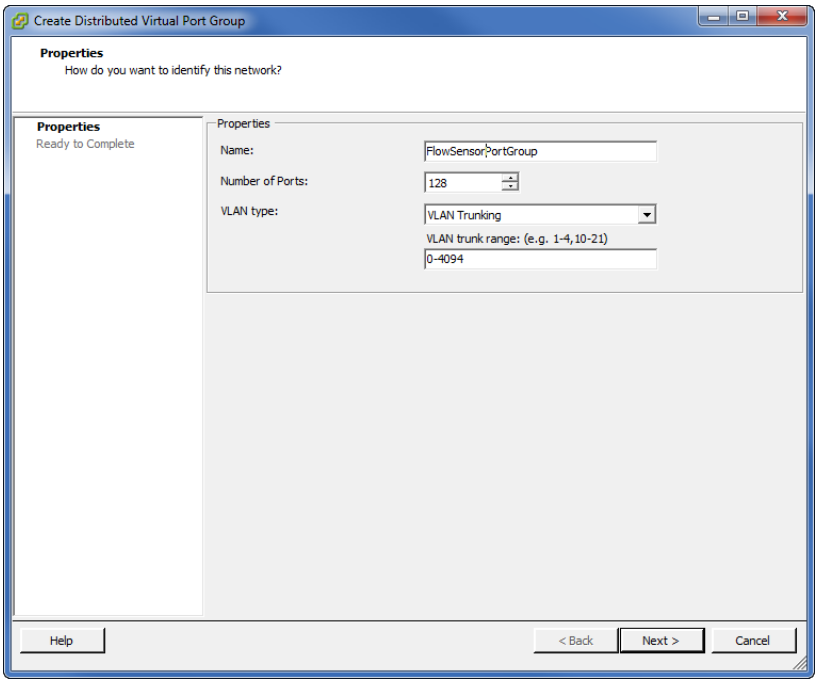
2. [ネットワーキング(Networking)] ツリーで VDS を選択します。



3. 右側のペインで [新しいポート グループの作成(Create a new port group)] をクリックします。



[dvPort グループ作成(Create dvPort Group)] ウィザードが開きます。



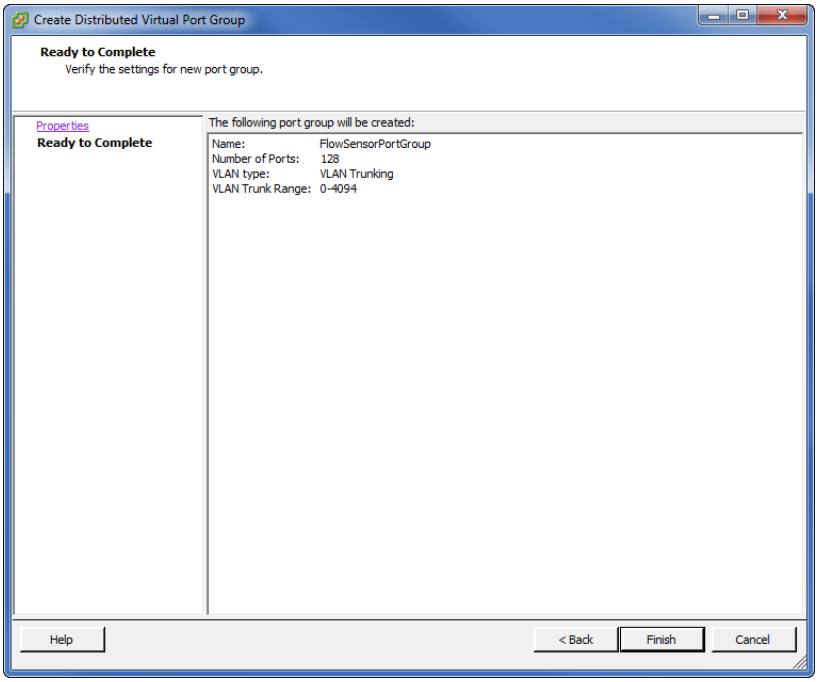
(注) Web クライアントには、[名前と場所の選択(Select name and location)]と[設定構成(Configure settings)]という2つの設定用ダイアログがあります。

4. [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。
5. [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。
6. ご使用の環境でVLANを使用していますか。
   - 「はい」の場合、ドロップダウンリストからVLANタイプを選択します。ステップ7に進みます。
   - 「いいえ」の場合、[VLANタイプ(VLAN type)]ドロップダウンリストから[なし(None)]を選択します。ステップ8に進みます。
7. 選択したVLANタイプに基づいて、次の表に示されているアクションを実行します。

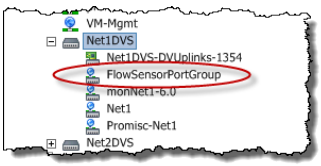
VLANタイプ	詳細
VLAN	[VLAN ID]フィールドに、IDに一致する番号(1～4094)を入力します。
VLANトランキング	すべてのVLANトラフィックをモニタリングするには、[VLANトランク範囲(VLAN trunk range)]フィールドに**0-4094**と入力します。

VLAN タイプ	詳細
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。

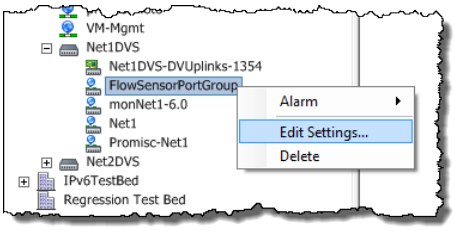
8. [次へ(Next)] をクリックします。サマリーページが開きます。



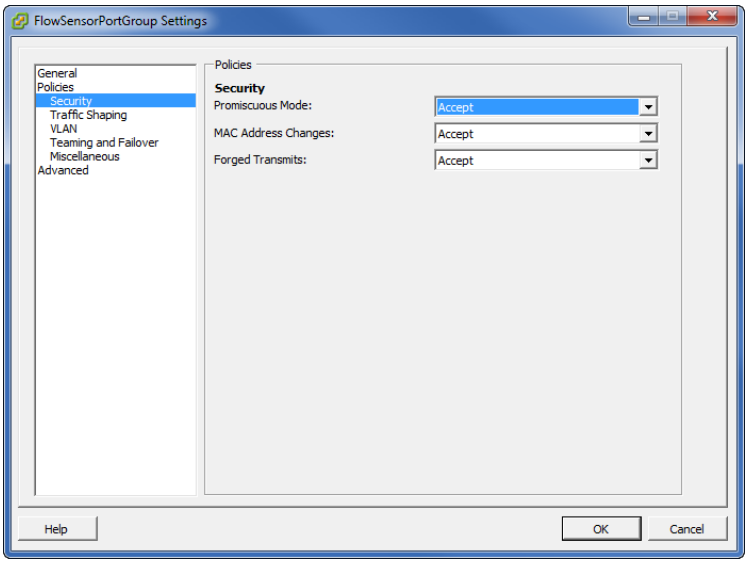
9. 設定を確認した後、[終了(Finish)] をクリックします。[ネットワーキング(Networking)] ツリーに新しい dvPort グループが表示されます。



10. 新しい dvPort グループを右クリックして、[設定の編集(Edit Settings)] を選択します。



[設定(Settings)]ダイアログボックスが開きます。



11. 左側のペインで、[セキュリティ(Security)]を選択します。
12. [無差別モード(Promiscuous Mode)]ドロップダウンリストの右側のペインで、[承認(Accept)]を選択します。
13. [OK]をクリックして、ダイアログを閉じます。
14. 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。
    - 「はい」の場合、該当するステップを繰り返してdvPortグループを追加します。
    - 「いいえ」の場合、次のステップに進みます。
15. ESXサーバに、Flow Sensor VEによるモニタ対象となる別のVDSがありますか。
    - 「はい」の場合、次のVDSに対して該当するステップを繰り返します。
    - 「いいえ」の場合、次のセクションに進みます。

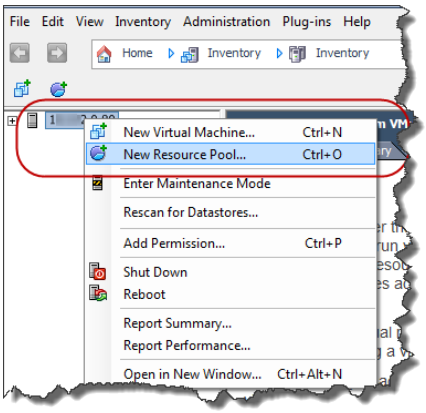
リソースプールの追加

他の仮想マシンに影響せずに稼働できるように、仮想アプライアンスには特定のCPUとメモリリソースが割り当てられたリソースプールが必要です。この手順では、Stealthwatch仮想アプライアンスの適切な割り当てを含む新しいリソースプールを追加する方法について説明します。

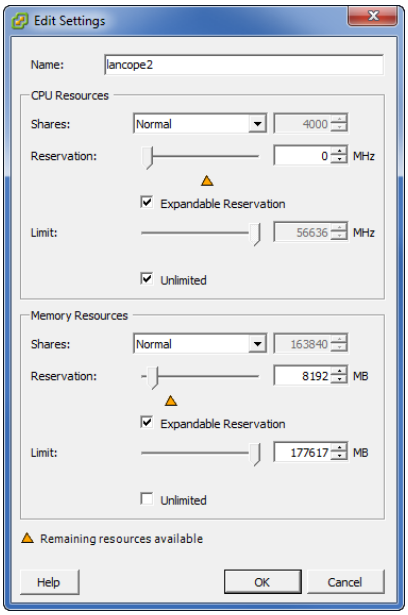
(注) 必要に応じて、仮想アプライアンスに既存のリソースプールを使用できます。ただし、次の手順を確認して、仮想アプライアンスが適切に動作するのに十分なリソースが既存のリソースプールに割り当てられていることを確認する必要があります。VMware Web Client v5.5インターフェイスを使用する場合、ここに表示されるいくつかの画面は異なります。そのため、必要に応じてオプションの違いを示します。

リソースプールが存在するESXサーバに仮想アプライアンス用のリソースプールを追加するには、次の手順を実行します。

1. 左側のインベントリツリーで、ESXサーバのIPアドレスを右クリックし、ポップアップメニューから[新規リソースプール(New Resource Pool)]を選択するか、Webクライアントで[すべてのvCenterアクション(All vCenter Actions)]>[新規リソースプール(New Resources Pool)]を選択します。



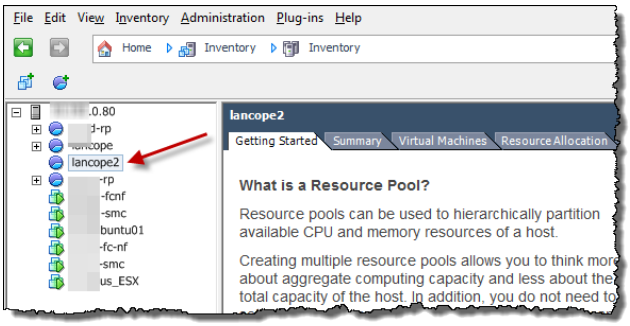
[リソースプールの作成(Create Resource Pool)]ダイアログが開きます。



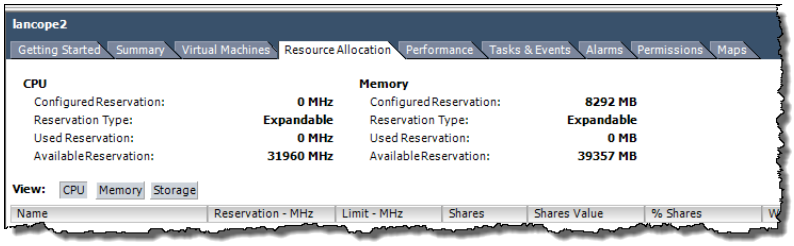
2. [名前(Name)]フィールドに、このリソースグループの識別に使用する名前を入力します。
3. [CPUリソース(CPU Resources)]セクションの設定は変更しないでください。
4. [メモリリソース(Memory Resources)]セクションで、次の操作を実行します。
   - 「リソース要件」(3ページ)のアプライアンスの表で推奨されているように[予約(Reservation)]フィールドを変更します。
   - [無制限(Unlimited)]チェックボックスをクリックしてオフにします。

注意! 4 GB未満のメモリはサポートされません。4 GB未満が割り当てられると、メモリ不足アラームがトリガーされて、フローはデータベースに保存されません。

7. [OK]をクリックします。リソースプールがインベントリツリーのESXサーバの下に表示されます。



8. リソースプールを選択し、[リソースの割り当て(Resource Allocation)] タブをクリックして CPU とメモリリソースの割り当てを確認します。Web クライアントでは、[管理(Manage)] タブをクリックして、[CPU リソースおよびメモリリソース(CPU Resources & Memory Resource)] をクリックします。



9. Flow Sensor VE を非 VDS 環境にインストールしますか。(ネットワーク環境の詳細については、を参照してください) 。
   - 「はい」の場合、次の「無差別ポート グループの追加」セクションに進みます。
   - 「いいえ」の場合、「仮想アプライアンスのインストール」(29 ページ) に進みます。

無差別ポート グループの追加

(注) 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。ネットワークで VDS を使用している場合は、「仮想アプライアンスのインストール」(9 ページ) に進んでください。

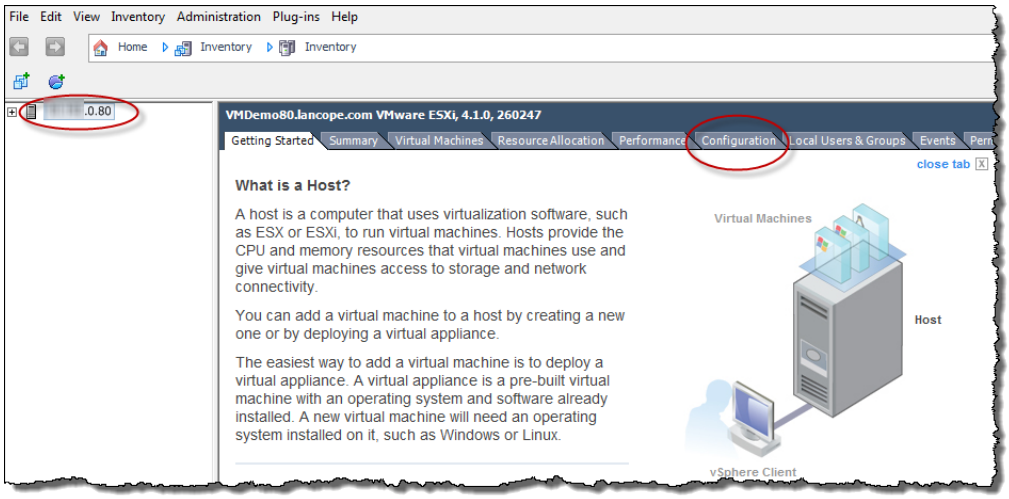
適切なリソース割り当てを使ってリソースプールを定義した後、Flow Sensor VE でのモニタ対象となる仮想スイッチごとに、無差別ポート グループを追加する必要があります。この追加作業では次の 2 つの手順を行います。

1. ポート グループの追加
2. ポート グループの無差別モードへの設定

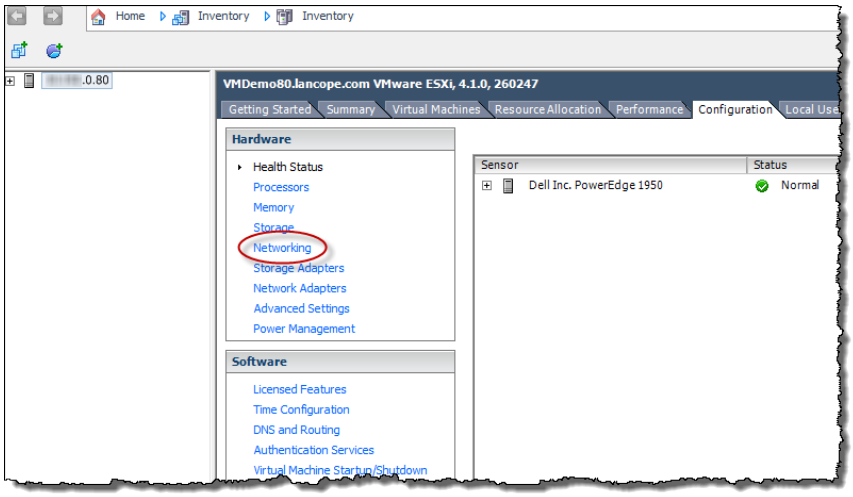
ポート グループの追加

ポート グループを追加するには、次の手順を実行します。

1. インベントリツリーで ESX サーバを選択し、[設定(Configuration)] タブをクリックします。

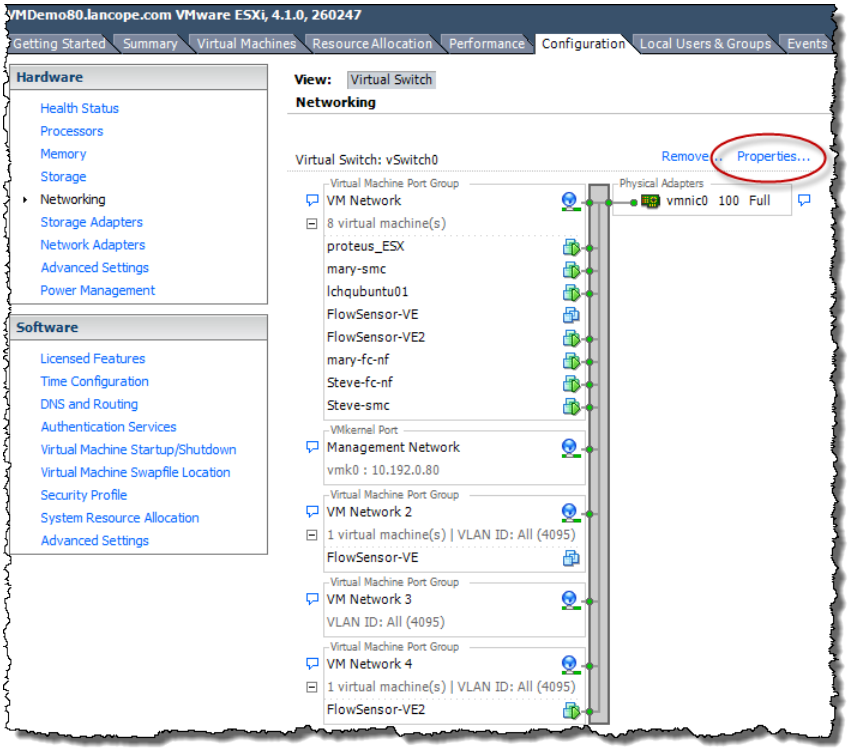


[設定(Configuration)] ページが開きます。



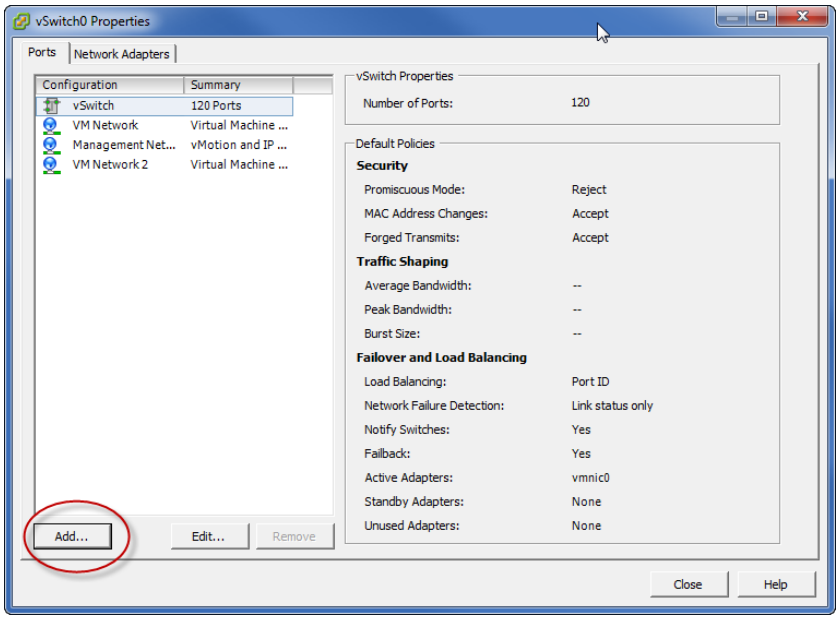
2. [ハードウェア(Hardware)] ペインで [ネットワーキング(Networking)] をクリックします。

   [設定(Configuration)] タブには、インストールされている仮想スイッチのリストが表示されます。

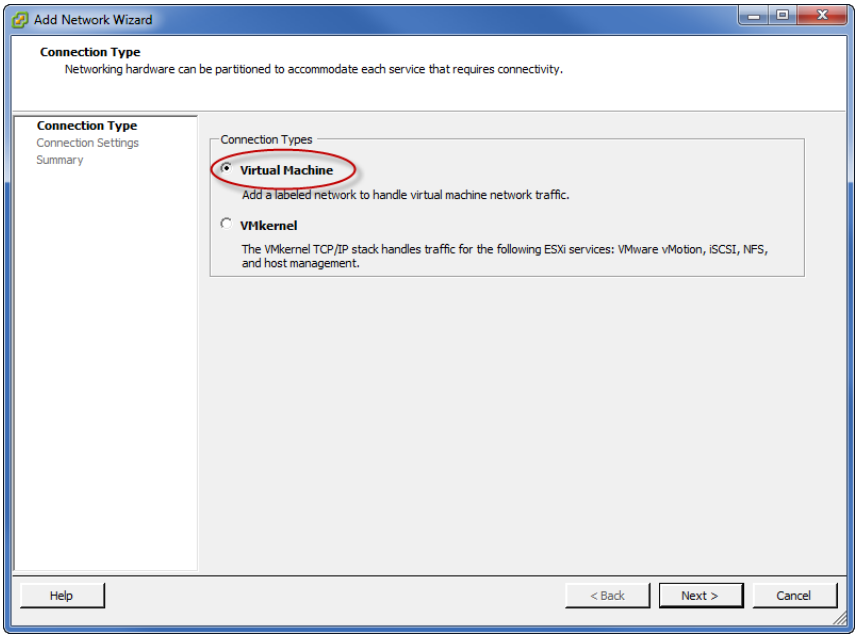


3. リストをスクロールして、Flow Sensor VE によるモニタ対象となる仮想スイッチを見つけ、[プロパティ(Properties)] リンクをクリックします。仮想スイッチの [プロパティ(Properties)] ダイア

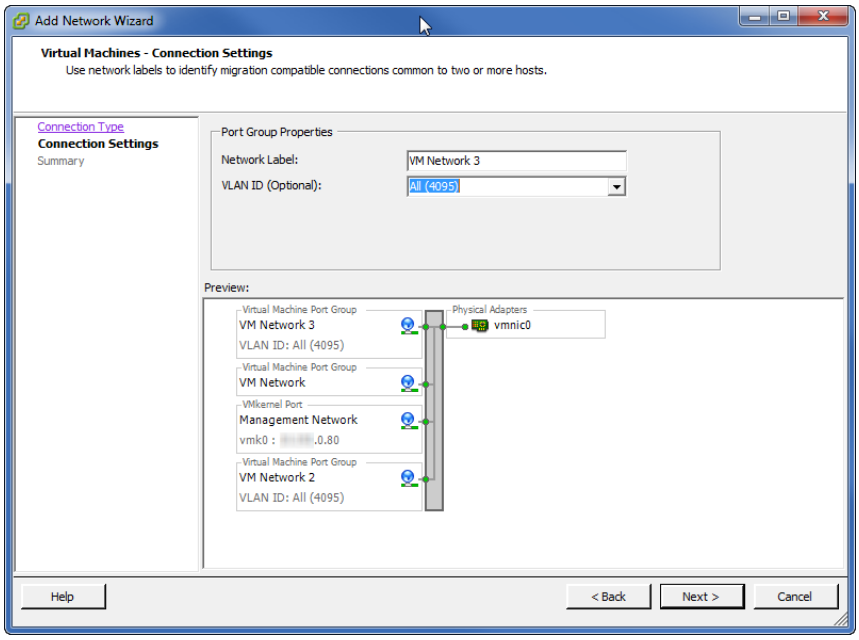
ログボックスが開きます。



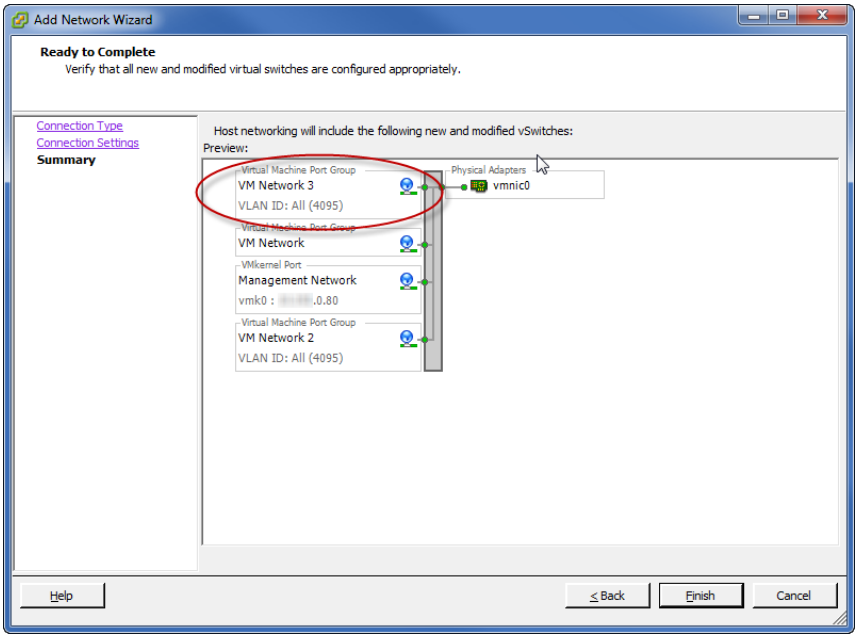
4. [追加(Add)] をクリックします。[ネットワークの追加(Add Network)] ウィザードが開き、[接続タイプ(Connection Type)] ページが表示されます。



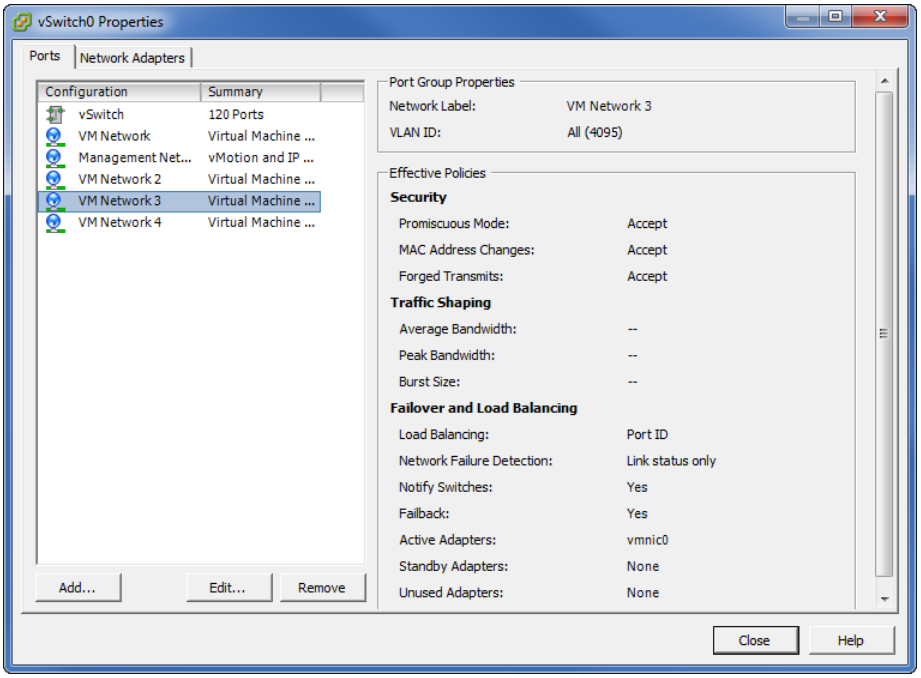
5. [接続タイプ(Connection Types)] の下で [仮想マシン(Virtual Machine)] を選択し、[次へ(Next)] をクリックします。[接続設定(Connection Settings)] ページが開きます。



6. 必要に応じて、ポート グループの [ネットワーク ラベル(Network Label)] を変更します。
7. Flow Sensor VE がこのポート グループ経由ですべての VLAN のトラフィックを監視できるようにするために、[VLAN ID] ドロップダウン リストをクリックして [すべて(4095) (All (4095))] を選択します。
8. [次へ(Next)] をクリックします。サマリー ページが開き、追加したポート グループが表示されます。



9. [終了(Finish)]をクリックすると、仮想スイッチの[プロパティ(Properties)]ダイアログに戻り、新しいポート グループがそこに表示されます。

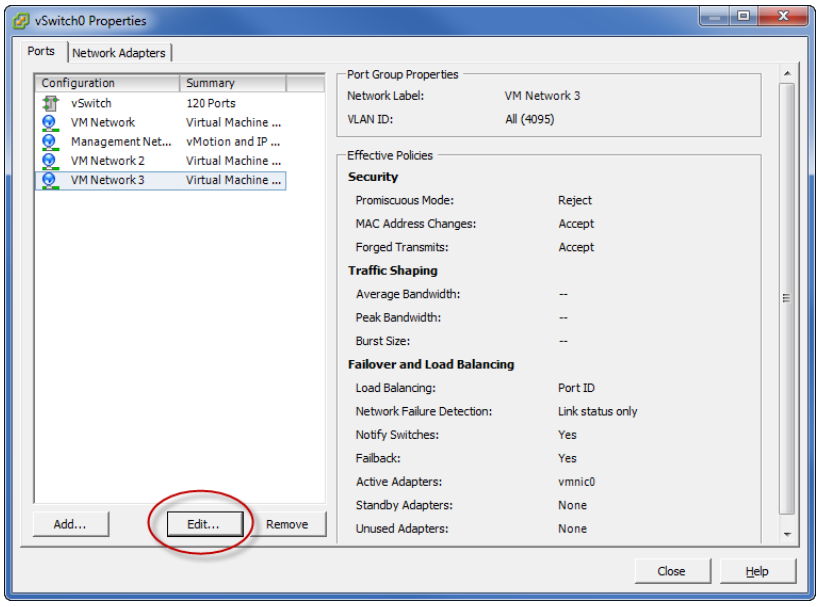


10. 次のセクションに進みます。

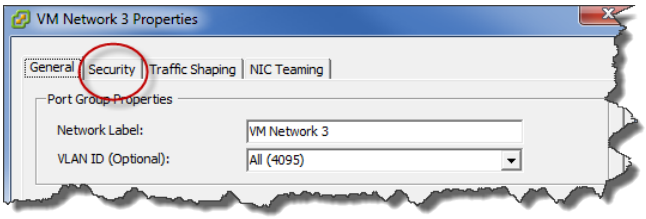
ポート グループの無差別モードへの設定

ポート グループを無差別モードに設定するには、次の手順を実行します。

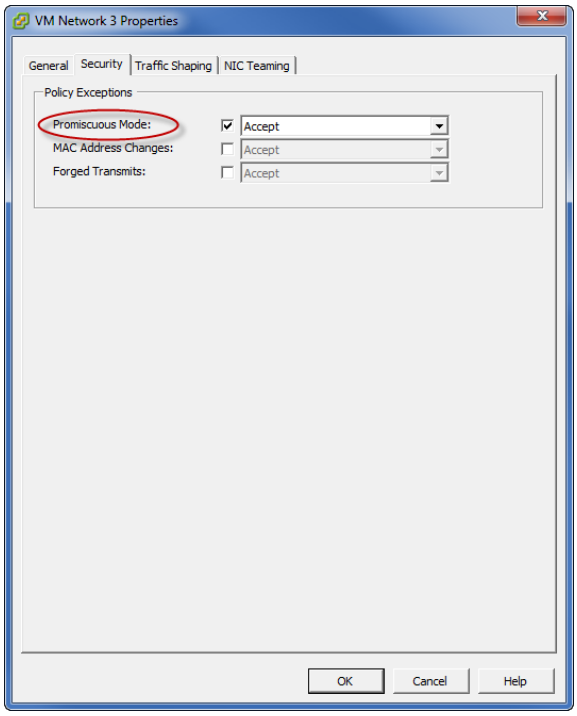
1. 仮想スイッチの[プロパティ(Properties)]ダイアログボックスで、追加したポート グループを選択して[編集(Edit)]をクリックします。



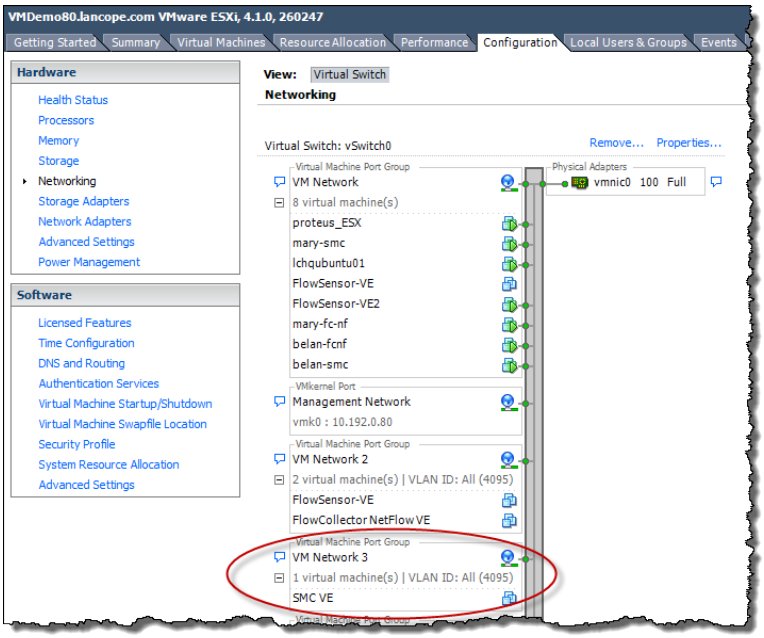
ポート グループの [プロパティ(Properties)] ダイアログボックスが開きます。



2. [セキュリティ(Security)] タブをクリックして、[ポリシーの例外 (Policy Exceptions)] のオプションを表示します。



3. [無差別モード(Promiscuous Mode)] チェックボックスをオンにし、ドロップダウンリストから [承認(Accept)] を選択します。
4. [OK] をクリックして、仮想スイッチの [プロパティ(Properties)] ダイアログに戻ります。
5. [閉じる(Close)] をクリックして、仮想スイッチの [プロパティ(Properties)] ダイアログを終了します。新しいポートグループが、[設定(Configuration)] タブの [ネットワーキング(Networking)] ページに表示されます。

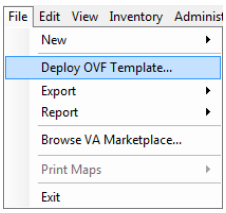


6. Flow Sensor VE が、この ESX サーバ上の別の仮想スイッチをモニタしますか。
   - 「はい」の場合、「ポート グループの追加」(22 ページ) に戻り、次の仮想スイッチに対してすべてのステップを繰り返します。
   - 「いいえ」の場合、次の「仮想アプライアンスのインストールセクションに進みます。

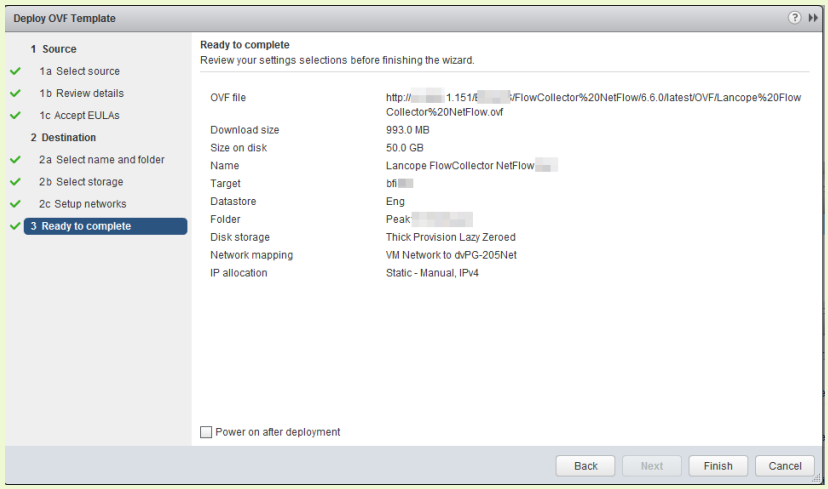
仮想アプライアンスのインストール

仮想アプライアンスを ESX サーバにインストールし、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。

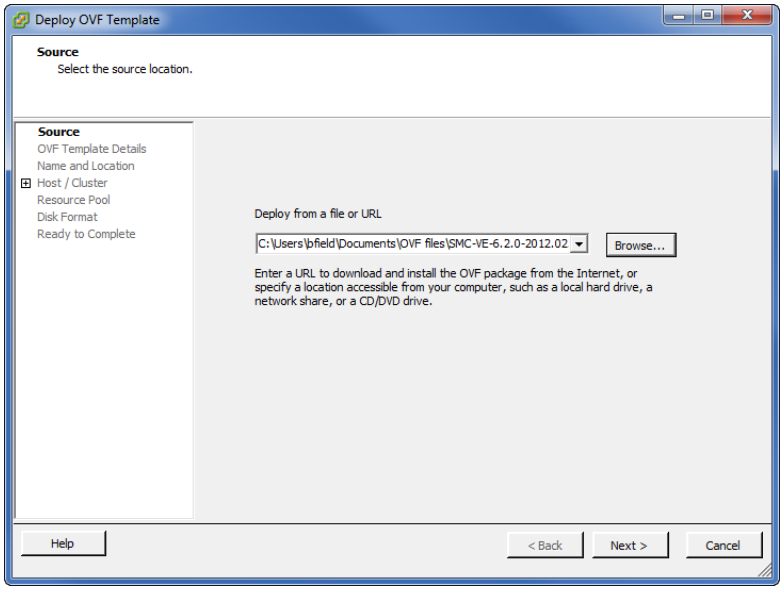
1. ダウンロード済みの仮想アプライアンス ソフトウェア(OVF) ファイルを解凍します。
2. vSphere Client メニューで、[ファイル(File)] > [OVF テンプレートの展開(Deploy OVF Template)] をクリックします。Web クライアントでは、ホストを右クリックして [OVF テンプレートの展開(Deploy OVF Template)] を選択します。



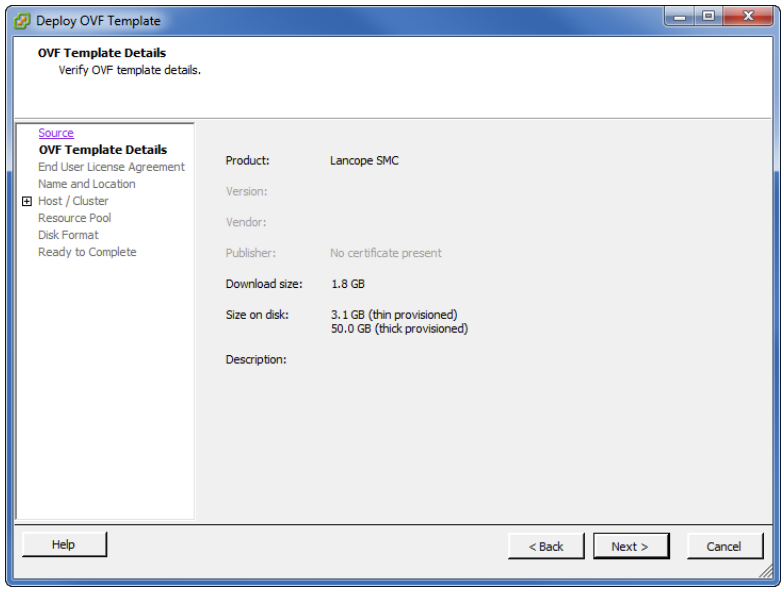
(注) Web クライアントの OVF テンプレート ウィザードでは手順の表現とナンバリングがわずかに異なりますが、手順は同じです。1 つの例として、Web クライアントでは [ソース(Source)] ではなく[ソースの場所 (Source Location)] を使用します。下のイメージでは、展開の準備が整った OVF テンプレートの左側に手順が表示されています。



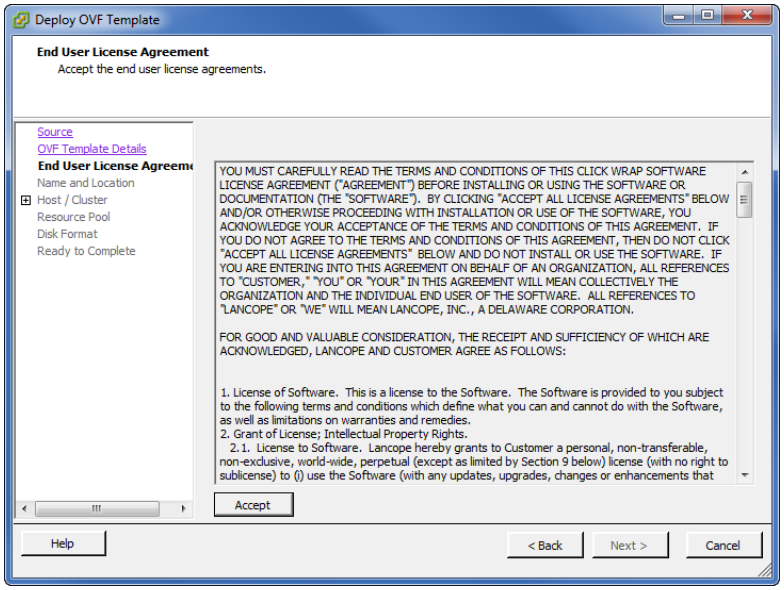
[OVF テンプレートの展開 (Deploy OVF Template)] ウィザードが開きます。



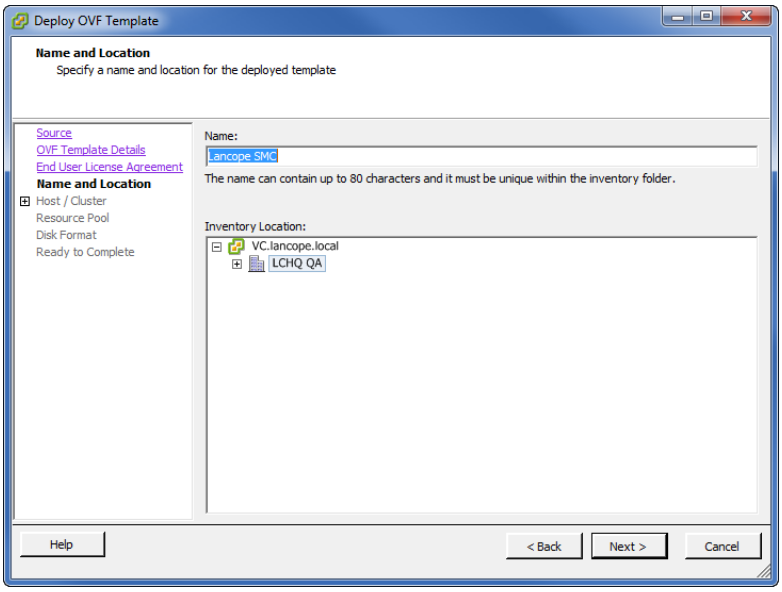
3. [参照 (Browse)] をクリックし、仮想アプライアンス OVF ファイルを探して選択します。
4. [次へ(Next)] をクリックすると、[OVF テンプレートの詳細 (OVF Template Details)] ページ (Web クライアント : 1b. [詳細の確認 (Review details)]) が表示されます。



5. [次へ(Next)] をクリックします。[エンド ユーザ ライセンス契約(End User License Agreement)] が開きます(1c. [EULA の承認(Accept EULAs)]) 。

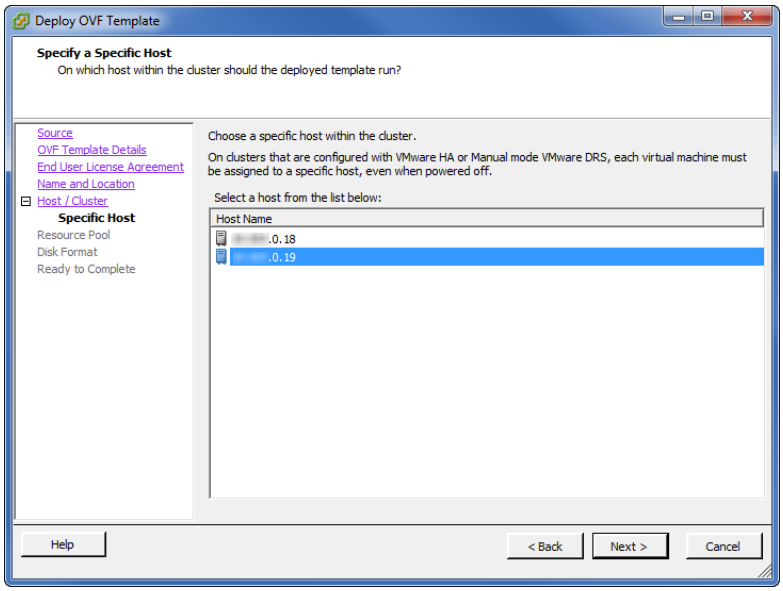


6. 情報を確認した後、[同意する(Accept)] をクリックして [次へ(Next)] をクリックします。[名前と場所(Name and Location)] ページが開きます(2a. [名前とフォルダの選択(Select name and folder)]) 。

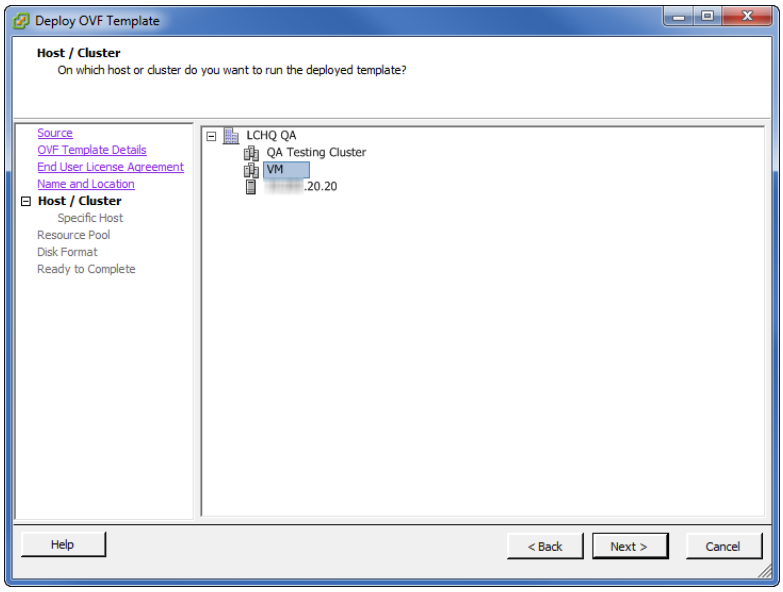


7. 必要に応じて、インベントリツリーに表示される仮想アプライアンスの名前を変更し、[次へ(Next)]をクリックします。

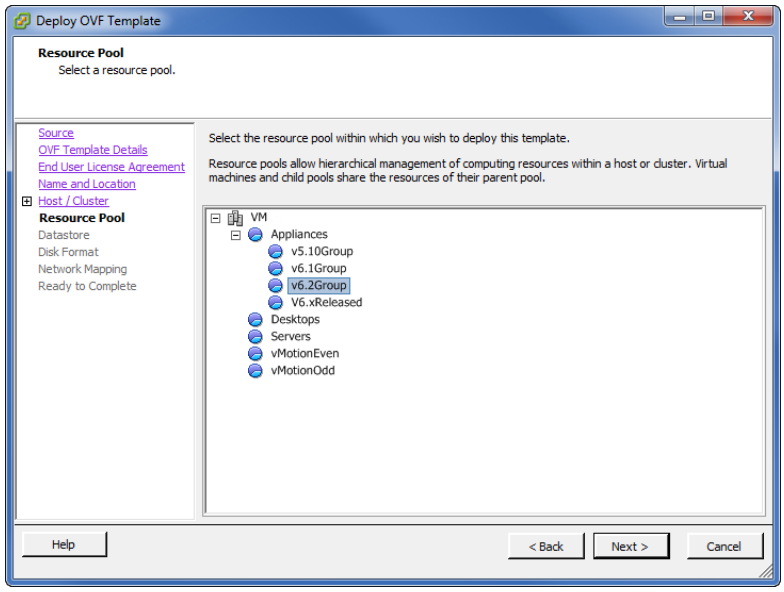
   - [特定ホストの指定(Specify a Specific Host)]ページが開いたら、仮想アプライアンスが存在するホストまたはクラスタを選択します。



   - [ホスト/クラスタ(Host/Cluster)]ページが開いたら、アプライアンスが存在するホストまたはクラスタを選択します。



8. [次へ(Next)] をクリックします。[リソースプール(Resource Pool)] ページが開きます。



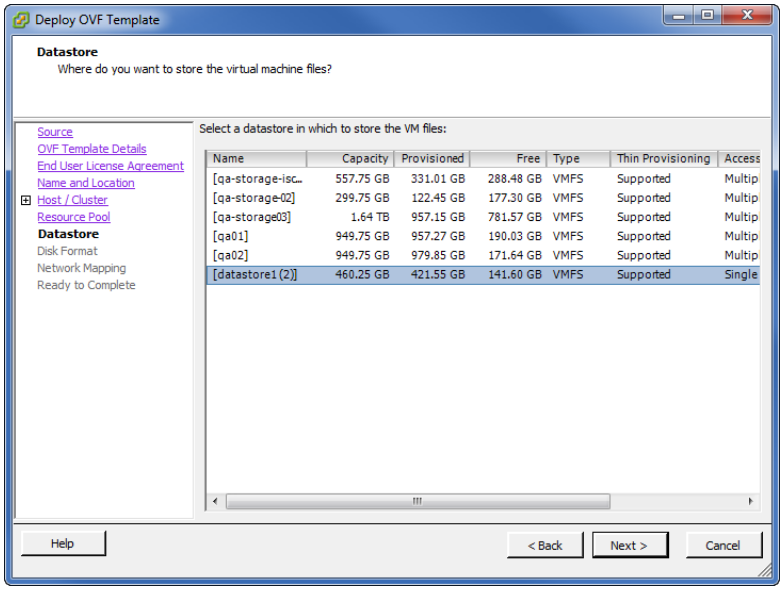
9. 以前に定義したリソースプールを選択して、[次へ(Next)] をクリックします。

   a. [データストア(Datastore)] ページが開いたら、手順 10 に進みます。

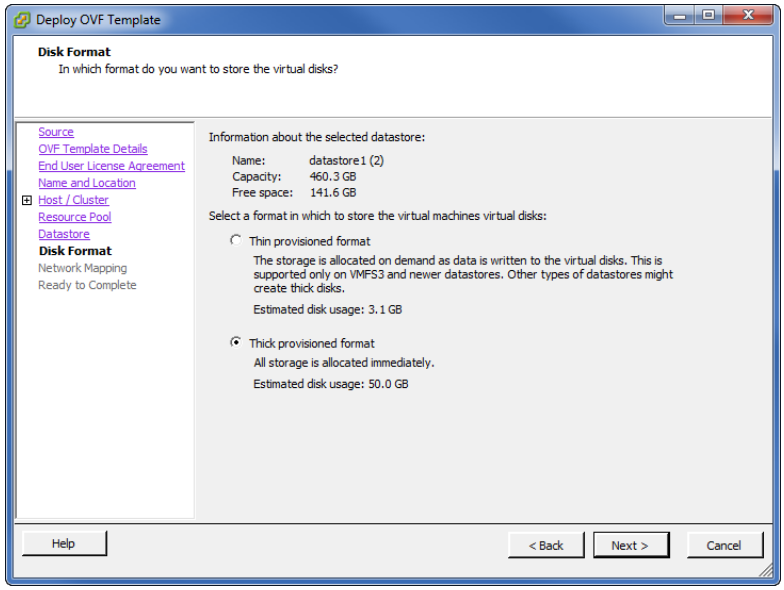
   b. [ディスク形式(Disk Format)] ページが開いたら、手順 11 に進みます。

(注) Web クライアントでは、[ストレージの選択(Select storage)] ページが開き、データストアとディスク形式の両方が表示されます。

10. [データストア(Datastore)] ページで、仮想アプライアンスを保存する場所を選択して、[次へ(Next)] をクリックします。

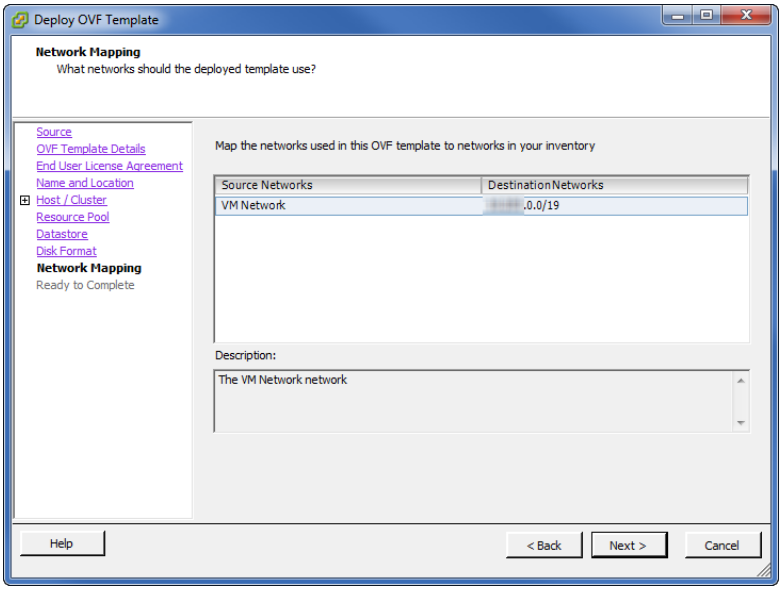


[ディスク形式(Disk Format)] ページが開きます。

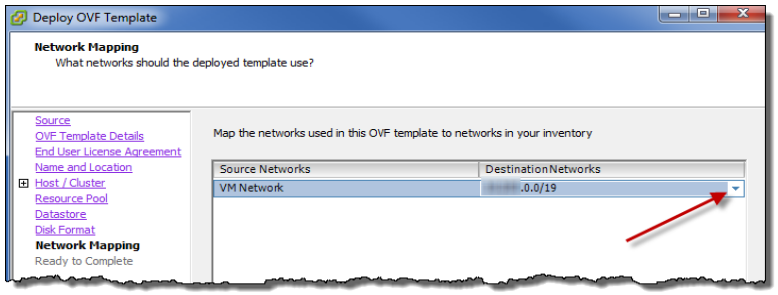


(注) vSphere Client v5 以降では、Lazy Zeroed と Eager Zeroed という 2 つのシックプロビジョニング形式があります。ご使用のディスクストレージのニーズに最適なものを選択してください。シンプロビジョニング形式は、ディスク容量が制限されている場合にのみ使用します。詳細については、VMware のマニュアルを参照してください。

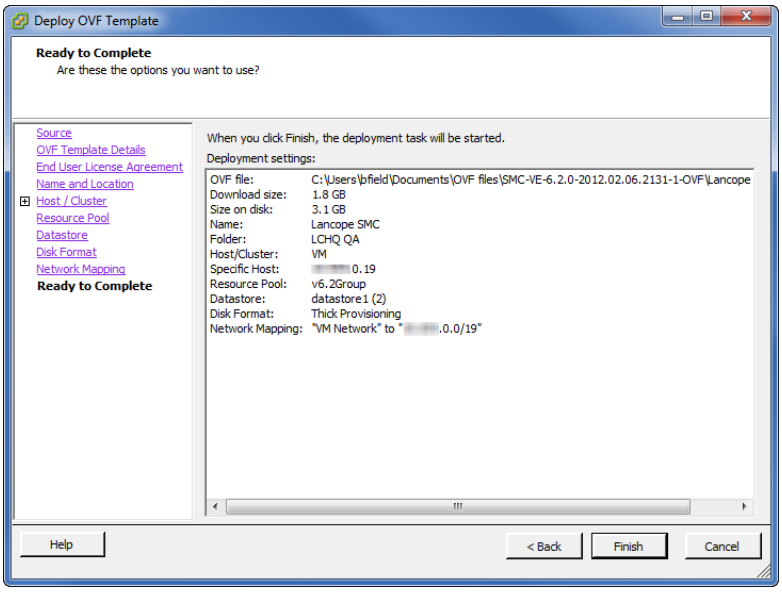
11. [ディスク形式(Disk Format)]ページで、[シックプロビジョニング形式(Thick provisioned format)]を選択して、[次へ(Next)]をクリックします。[ネットワークマッピング(Network Mapping)]ページ(Webクライアント:2c. [ネットワーク設定(Setup Networks)])が開きます。



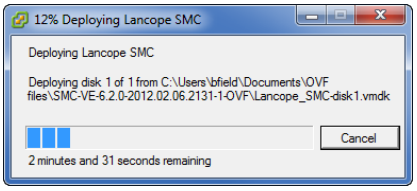
12. [宛先ネットワーク(Destination Networks)]ドロップダウンリストから、仮想アプライアンスの管理ポートを選択します。



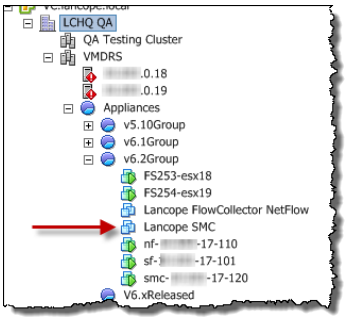
13. [次へ(Next)]をクリックします。設定の概要を示した[完了前の確認(Ready to Complete)]ページが開きます。



14. 設定を確認した後、[終了(Finish)]をクリックします。進捗状況ダイアログが開きます。



15. 展開が完了したら、[閉じる(Close)]クリックして進捗状況ダイアログを閉じます。仮想アプライアンスがインベントリツリーに表示されます。



16. ESX サーバ上の複数の仮想スイッチまたはクラスタ内の複数の VDS をモニタする Flow Sensor VE をインストールする予定ですか?

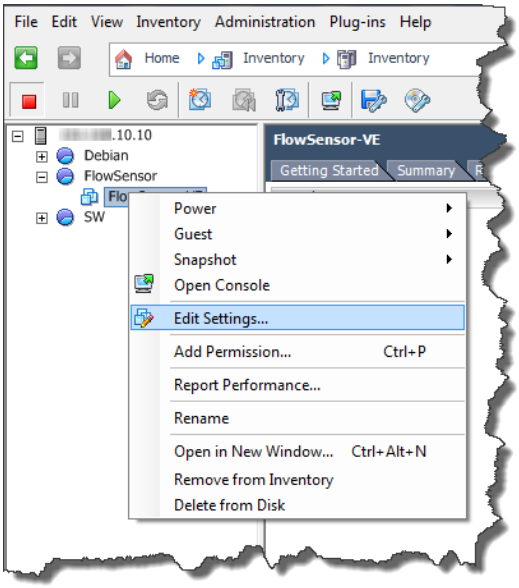
- 「はい」の場合、次の「追加モニタリングポートの定義」セクションに進みます。
- 「いいえ」の場合、51 ページ「仮想アプライアンスシステムの設定」に進みます。

追加モニタリング ポートの定義

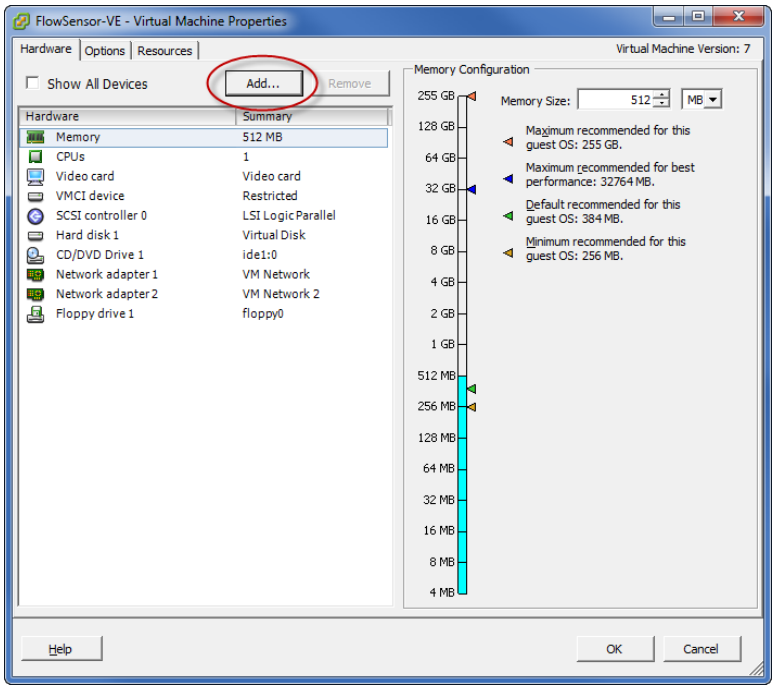
（注） この手順が必要となるのは、Flow Sensor VE が ESX サーバの複数の仮想スイッチ、またはクラスタ内の複数の VDS をモニタする場合だけです。

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。

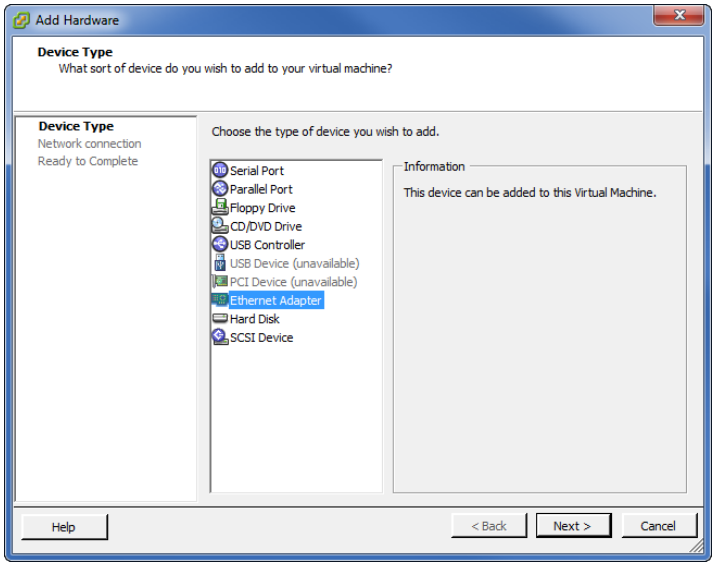
1. インベントリツリーで Flow Sensor VE を右クリックし、[設定の編集（Edit Settings）] を選択します。



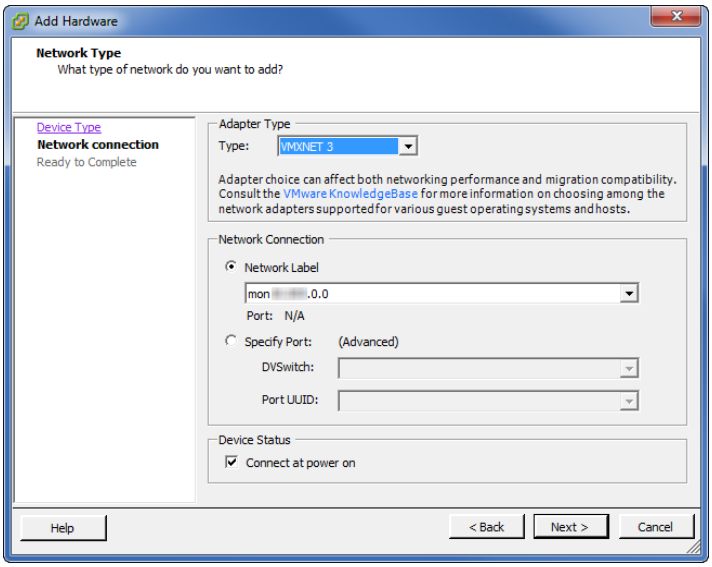
[Flow Sensor VE 仮想マシンのプロパティ（Flow Sensor VE Virtual Machine Properties）] ダイアログが開きます。



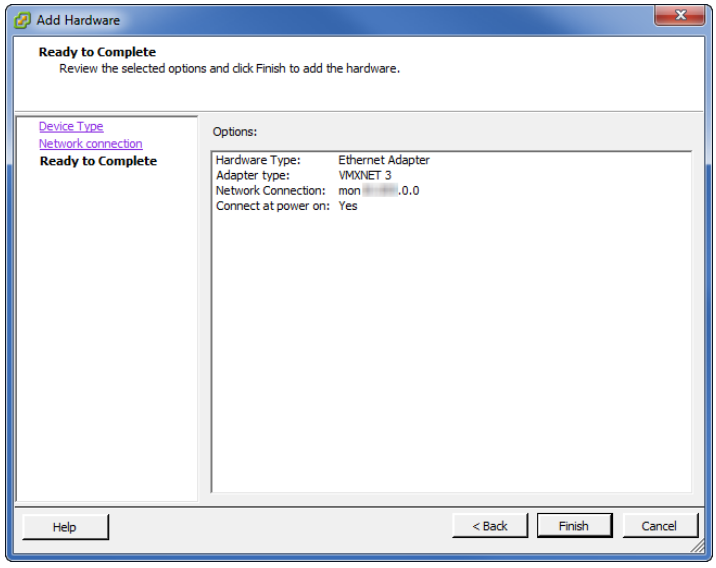
2. [追加(Add)] をクリックします。[ハードウェアの追加(Add Hardare)] ウィザードが開き、[デバイスのタイプ(Device Type)] ページが表示されます。



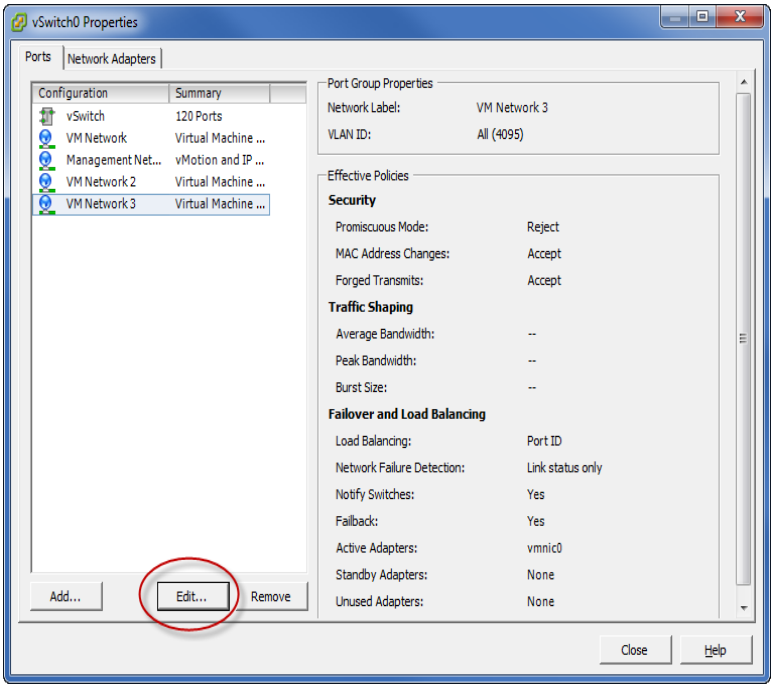
3. デバイスタイプのリストから [イーサネット アダプタ(Ethernet Adapter)] を選択し、[次へ(Next)] をクリックします。[ネットワークのタイプ(Network Type)] ページが開きます。



4. 次の手順を実行します。
   - [アダプタのタイプ(Adapter Type)] セクションで [VMXNET 3] を選択します。
   - [ネットワーク接続(Network Connection)] セクションで、未割り当ての無差別ポート グループを選択します。
   - [デバイスのステータス(Device Status)] セクションで、[電源投入時に接続(Connect at power on)] チェックボックスがオンになっていることを確認します。
5. [次へ(Next)]をクリックして、サマリーを表示します。



6. 設定を確認した後、[終了(Finish)]をクリックします。
7. [Flow Sensor VE 仮想マシンのプロパティ(Flow Sensor VE Virtual Machine Properties)]ダイアログが開き、新たに定義したモニタポートが表示されます。



8. Flow Sensor VE で、ESX サーバ/クラスタ上の別の仮想スイッチ/VDS をモニタする予定ですか?
   - 「はい」の場合、次の仮想スイッチに対してこの手順を繰り返します。
   - 「いいえ」の場合、[OK] をクリックして vSphere クライアント ホームページに戻ります。
9. 次の「仮想環境の設定」の章に進みます。

3

仮想環境の設定

概要

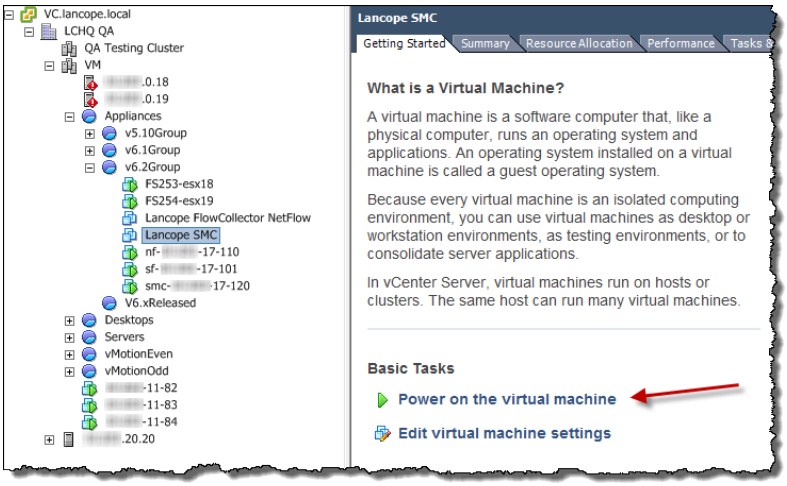
StealthWatch VE アプライアンスをインストールした後、これらのアプライアンス用の仮想環境を設定できます。このプロセスでは、この章で説明する次の手順を実行します。

1. IP アドレスの設定
2. デフォルト ユーザ パスワードの変更

IP アドレスの設定

仮想アプライアンスの IP アドレスを設定するには、次の手順を実行します。

1. 必要に応じて、vSphere Client ソフトウェアを起動してログインします。
   [はじめに(Getting Started)] ページが開きます。



2. インベントリツリーで、設定する StealthWatch 仮想アプライアンスを選択します。

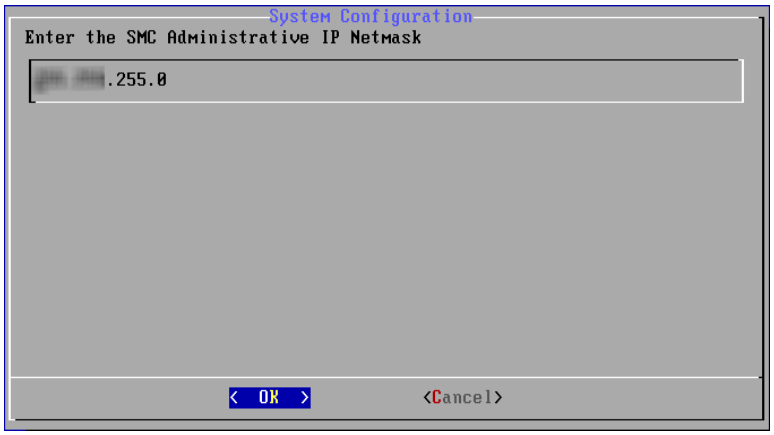
3. [はじめに(Getting Started)] ページで、[仮想マシンの電源投入(Power on the virtual machine)] リンクをクリックします。このリンクを表示するには、下方向へのスクロールが必要になる場合があります。

> **(注)** 仮想マシンの電源が入っていない場合や使用可能メモリの不足について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。
>
> - 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加します。
> - アプライアンスをインストールするシステムの使用可能リソースを増加します。

4. [コンソール(Console)] タブをクリックします。(Web クライアントで、[概要(Summary)] タブをクリックして [コンソールの起動(Launch Console)] リンクをクリックします。) 仮想アプライアンスの起動が完了します。仮想アプライアンスの [管理 IP アドレス(Administrative IP Address)] ページが開きます。

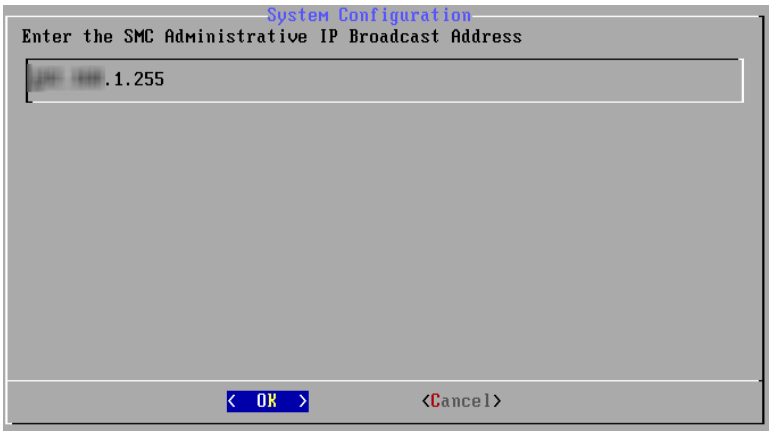
> **(注)** 画面全体を表示するには、全画面モード(Ctrl + Alt + Enter) を有効にする必要があります。

5. ページをクリックしてから、仮想アプライアンスの IP アドレスを入力します。
6. [OK] を選択して、Enter を押します。デフォルトのネットワークマスク IP アドレスが表示された [IP ネットマスク(IP Netmask)] ページが開きます。



7. 次の手順を実行します。
   - デフォルト値を受け入れるか、環境に基づいて新しい値を入力します。
   - [OK] を選択し、Enter を押して続行します。

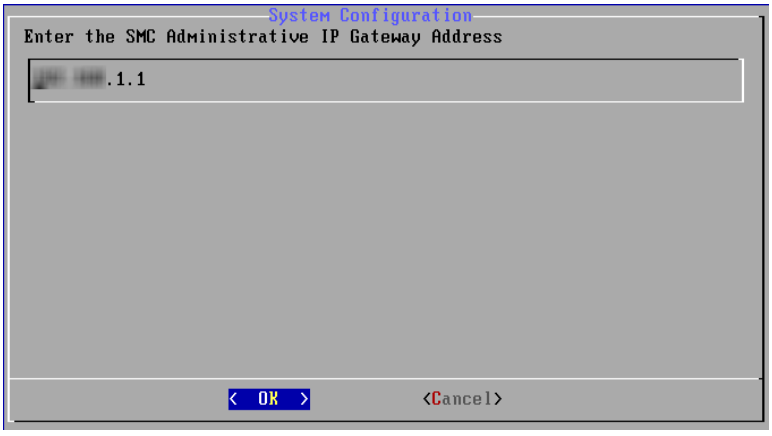
   デフォルトのブロードキャスト IP アドレスが表示された [IP ブロードキャストアドレス(IP Broadcast Address)] ページが開きます。



8. 次の手順を実行します。

   - デフォルト値を受け入れるか、環境に基づいて新しい値を入力します。
   - [OK] を選択し、Enter を押して続行します。

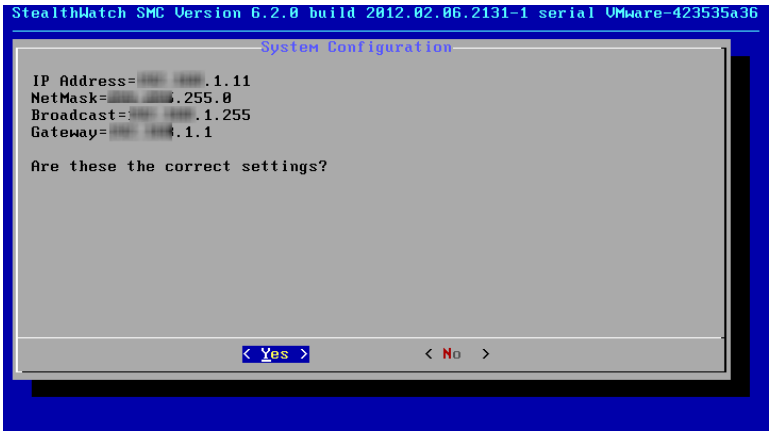
   デフォルトのゲートウェイ サーバ IP アドレスが表示された [ゲートウェイ アドレス(Gateway Address)] ページが開きます。



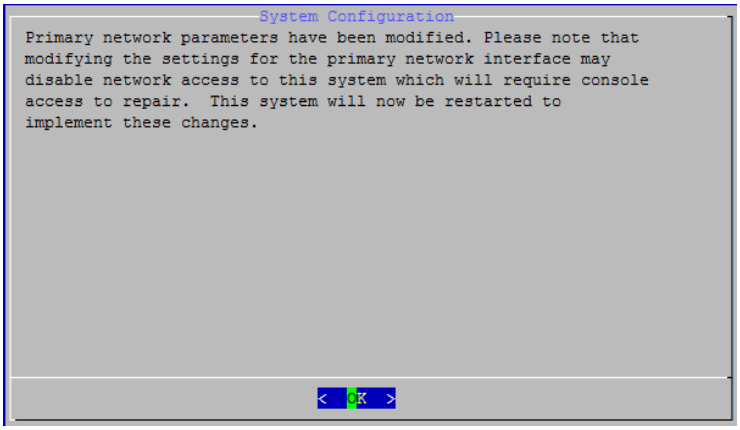
9. 次の手順を実行します。

   - デフォルト値を受け入れるか、環境に基づいて新しい値を入力します。
   - [OK] を選択し、Enter を押して続行します。

   入力内容の概要を示すページが開きます。



10. 画面の情報を確認します。設定は正しいですか。
    - 正しい場合、次の手順に進みます。
    - 正しくない場合、手順 13 に進みます。
11. Enter キーを押します。 システムの再起動ページが開きます。



12. Enter キーを押します。システムが再起動し、変更が実装されます。完了すると、ログインプロンプトが表示されます。
13. [いいえ(No)] を選択して、Enter を押します。[管理 IP アドレス(Administrative IP Address)] ページが開きます。手順 5 ～ 10 を繰り返して、必要な変更を行います。システムの再起動ページが開きます。
14. Enter キーを押します。システムが再起動し、変更が実装されます。完了すると、ログインプロンプトが表示されます。

15. Ctrl + Alt を押して、コンソールを終了します。
16. この章の次の「デフォルト ユーザ パスワードの変更」に進みます。

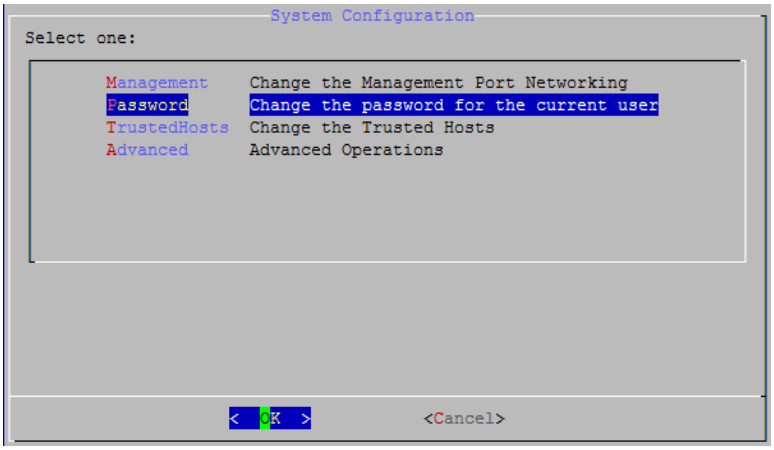
デフォルト ユーザ パスワードの変更

ネットワークの安全性を確実なものにするには、sysadmin のデフォルト パスワードと仮想アプライアンスのルート パスワードの両方を変更する必要があります。

sysadmin パスワードの変更

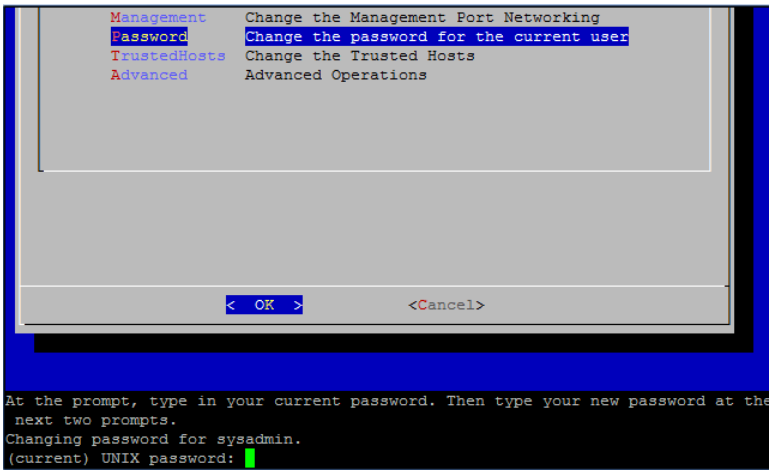
sysadmin パスワードを変更するには、次の手順を実行します。

1. ログイン ページで、次の操作を実行します。
   a. パスワード プロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
   b. **sysadmin**(大文字と小文字を区別します) と入力して、Enter を押します。
2. [システム設定 (System Configuration)] メニューで、[パスワード (Password)] を選択して Enter を押します。



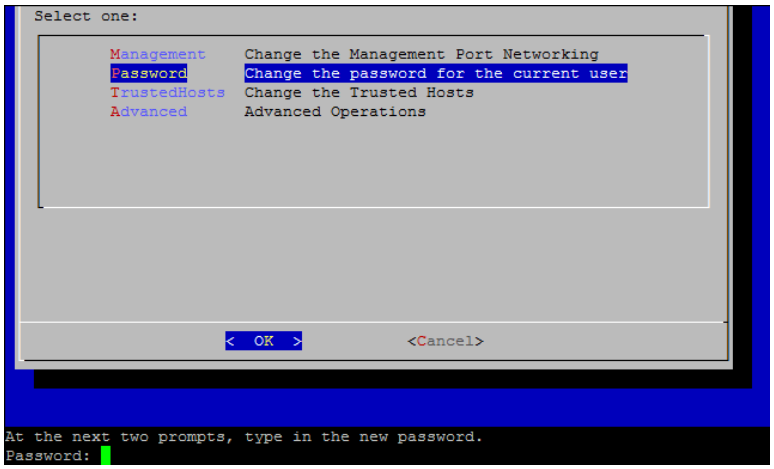
重要： 信頼できるホストのリストをデフォルトから変更する場合、各 Stealthwatch アプライアンスが展開内の他のすべての Stealthwatch アプライアンスの信頼できるホストのリストに含まれていることを確認する必要があります。そうしなければ、アプライアンス間で通信できません。

現在のパスワードのプロンプトがメニューの下に表示されます。



3. 現在のパスワードを入力して、Enter を押します。

新しいパスワードのプロンプトが表示されます。



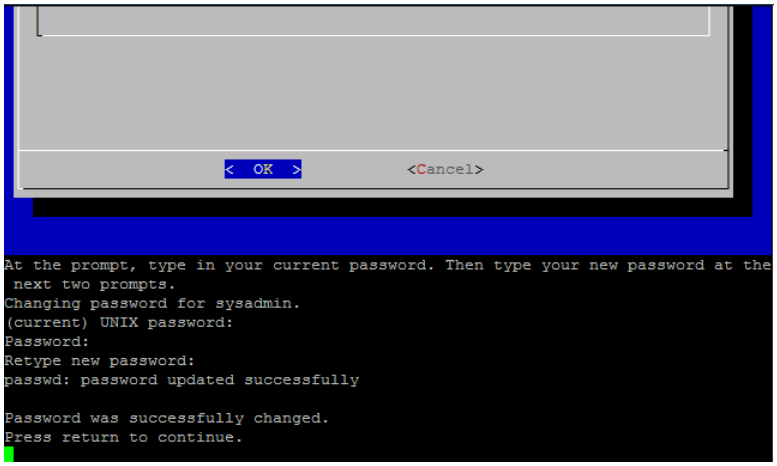
4. 新しいパスワードを入力して、Enter を押します。

(注)

- パスワードは、スペースを含めずに 5 ～ 30 文字の英数字にする必要があります。$.~!@#%_=?:,{}() の特殊文字も使用できます。

- 変更するパスワードは、以前のパスワードと4文字以上異なる必要があります。

5. 新しいパスワードを再度入力して、Enterを押します。パスワードが正常に更新されたことを示すメッセージが表示されます。

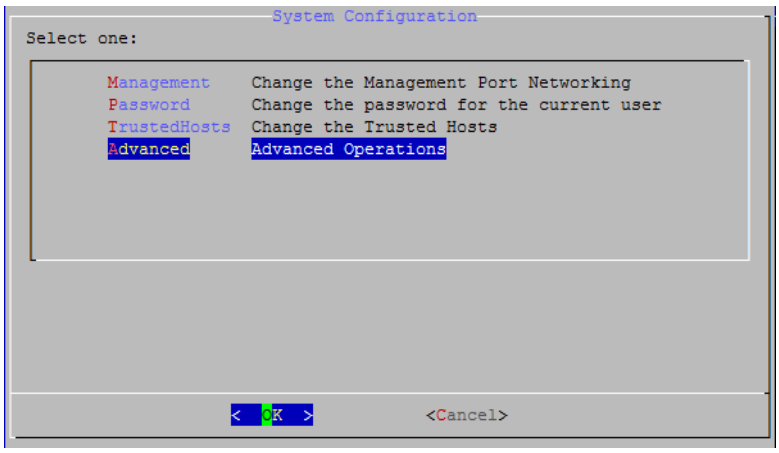


6. Enterを押して、[システム設定(System Configuration)]コンソールメニューに戻ります。
7. 次の「ルート パスワードの変更」セクションに進みます。

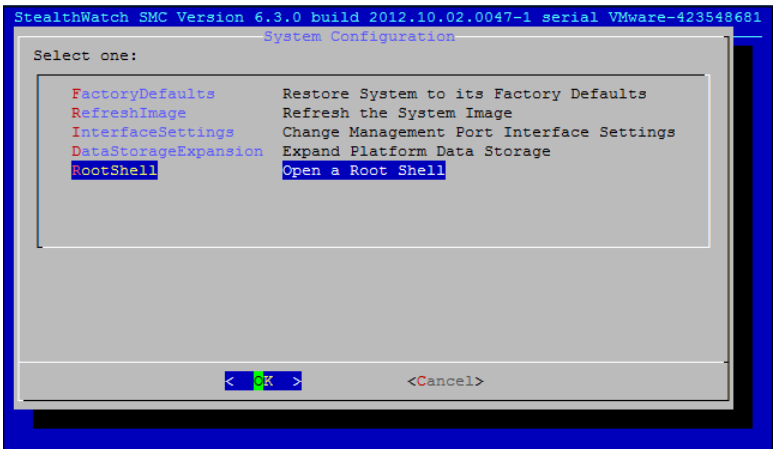
ルート パスワードの変更

ルート パスワードを変更するには、次の手順を実行します。

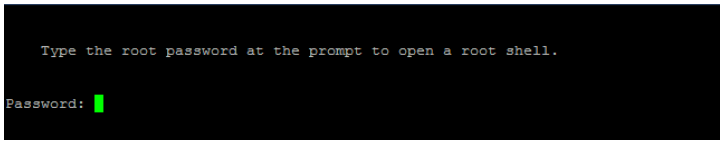
1. [システム設定(System Configuration)]コンソールメニューで、[詳細(Advanced)]を選択してEnterを押します。[詳細(Advanced)]メニューが開きます。



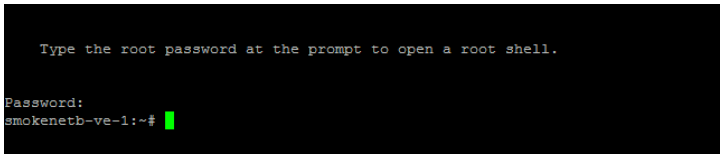
2. [詳細(Advanced)]メニューで、[RootShell]を選択してEnterを押します。



ルート パスワードのプロンプトが表示されます。



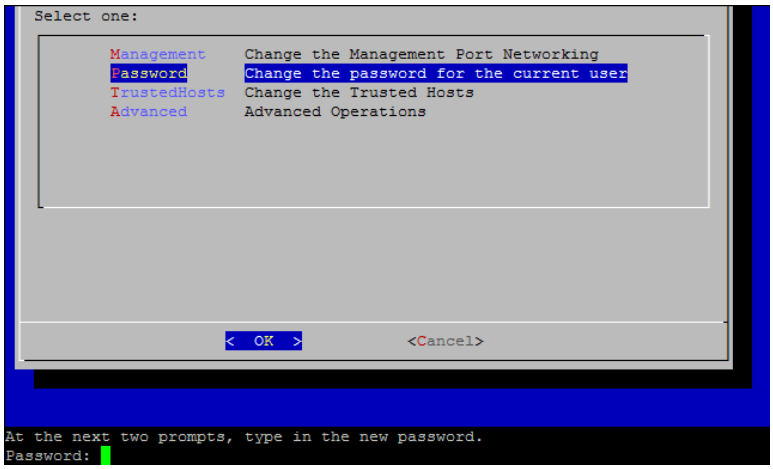
3. 現在のルート パスワード **lan1cope** を入力して、Enter を押します。ルート シェルのプロンプトが表示されます。



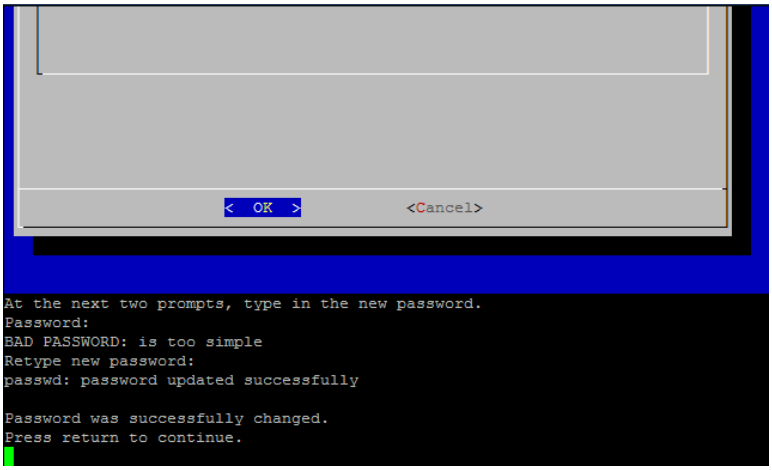
4. **SystemConfig**(大文字と小文字を区別します) と入力して、Enter を押します。

   これによって、[システム設定(System Configuration)] メニューに戻り、ルート パスワードを変更できます。

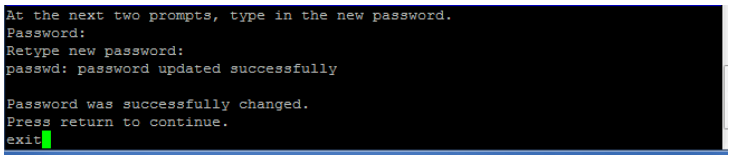
5. [パスワード(Password)] を選択して、Enter を押します。パスワードのプロンプトが表示されます。



6. 新しいルート パスワードを入力して、Enter を押します。メニューの下に 2 つ目のプロンプトが表示されます。



7. 新しいルート パスワードを再入力して、Enter を押します。



パスワードが正常に更新されたことを示すメッセージが表示されます。

8. パスワードの変更が成功したら、**exit** と入力して Enter を押します。これで、デフォルトの sysadmin パスワードとルート パスワードの両方が変更されました。
9. Ctrl + Alt を押して、コンソール環境を終了します。

10. すべての仮想アプライアンスに対して、この章に記載されているすべての手順を実行しましたか。

    - 「はい」の場合、「仮想アプライアンスシステムの設定」に進みます。
    - 「いいえ」の場合、「IP アドレスの設定」(41 ページ) に戻って、次の仮想アプライアンスのためにこの章のすべての手順を繰り返します。その後、「仮想アプライアンスシステムの設定」に進みます。

4

仮想アプライアンスの設定

概要

この章では、仮想アプライアンスを設定し、トラフィックデータの処理を開始する手順について説明します。この章の手順を完了すると、インストールおよび設定プロセスが完了します。

先に進む前に必要な情報については、「はじめる前に」(2ページ)のチェックリストを参照してください。

プロセスの概要

仮想 Stealthwatch アプライアンスを設定するには、この章で説明する次の手順を完了します。

1. 個々のアプライアンスの設定
2. Flow Sensor VE のメモリを増やす
3. アプライアンス管理インターフェイスによる設定

個々のアプライアンスの設定

すべてのアプライアンスの初期設定は、アプライアンス設定ツールで実行されます。アプライアンスに初めてアクセスすると、アプライアンス設定ツールが表示されます。システムによっては、UDP Director の前に Flow Sensor および Flow Collector を設定して、最後に SMC を設定する必要があります。SMC の初期設定を完了すると、システム設定ツールが開き、Stealthwatch システムを設定できます。

開始する前に、「はじめる前に」(2ページ)で詳細情報を収集します。

(注) 環境によって、ここに表示されている画面とわずかに異なる画面が表示されることがあります。

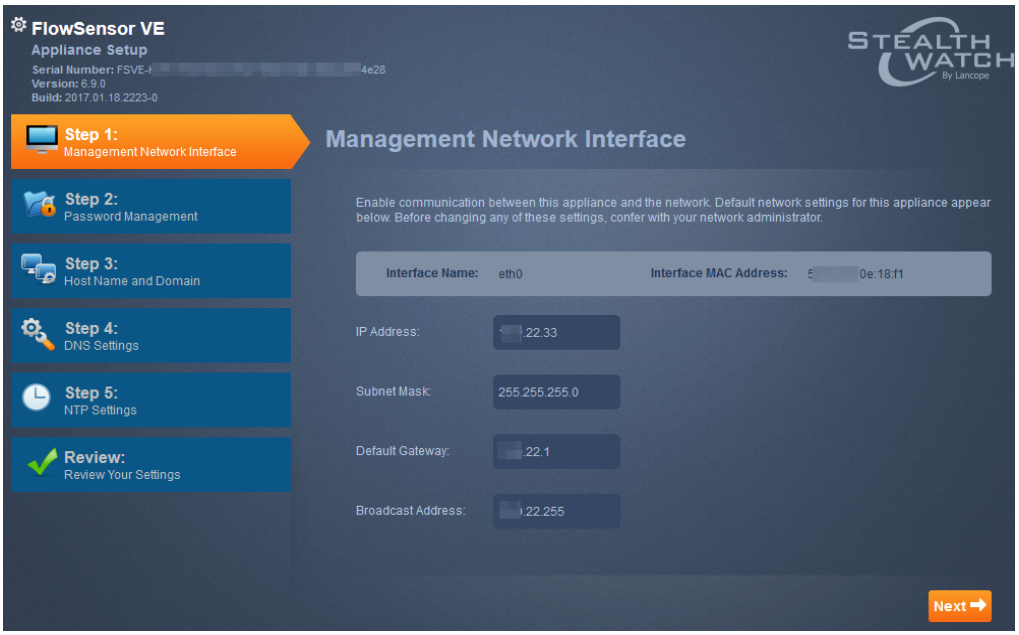
アプライアンスを設定するには、次の手順を実行します。

1. ブラウザのアドレスフィールドに **https://** と入力し、その後に仮想アプライアンスの IP アドレスを入力して、Enter を押します。

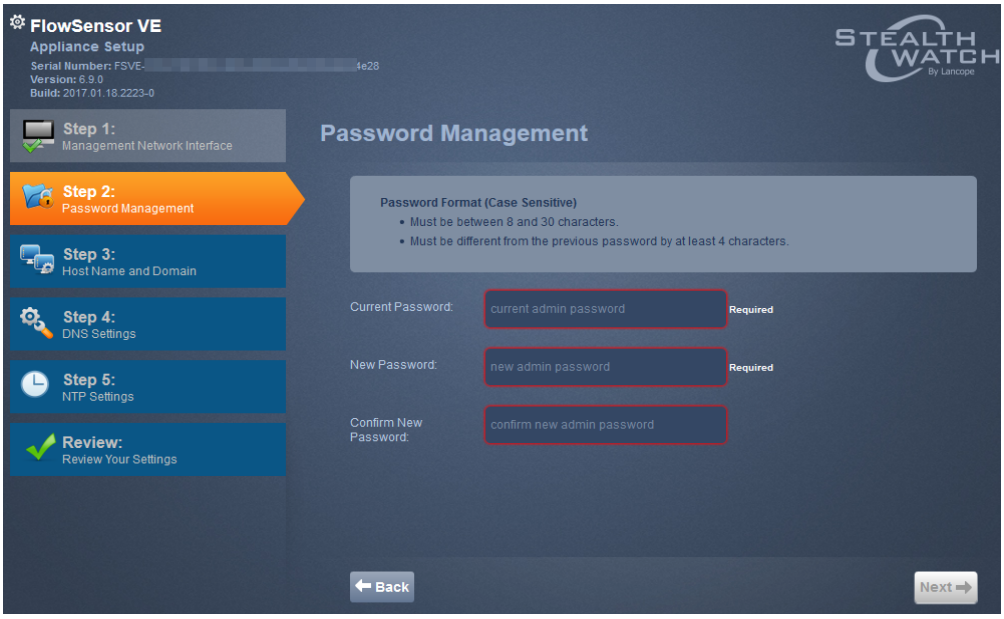
2. 管理者ログイン ページが開きます。**admin** および **lan411cope**(両方とも大文字と小文字を区別します) と入力して、[ログイン(Login)] をクリックします。手順 5 に進みます。

3. [ようこそ(Welcome)] ページが開きます。[続行 (Continue)] をクリックします。

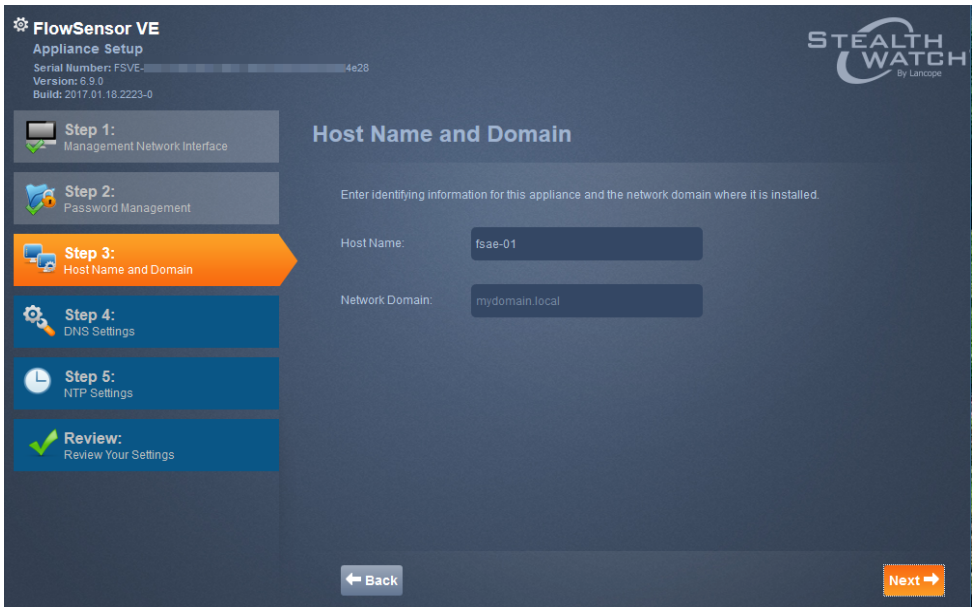
[管理ネットワーク インターフェイス(Management Network Interface)] ページが開きます。



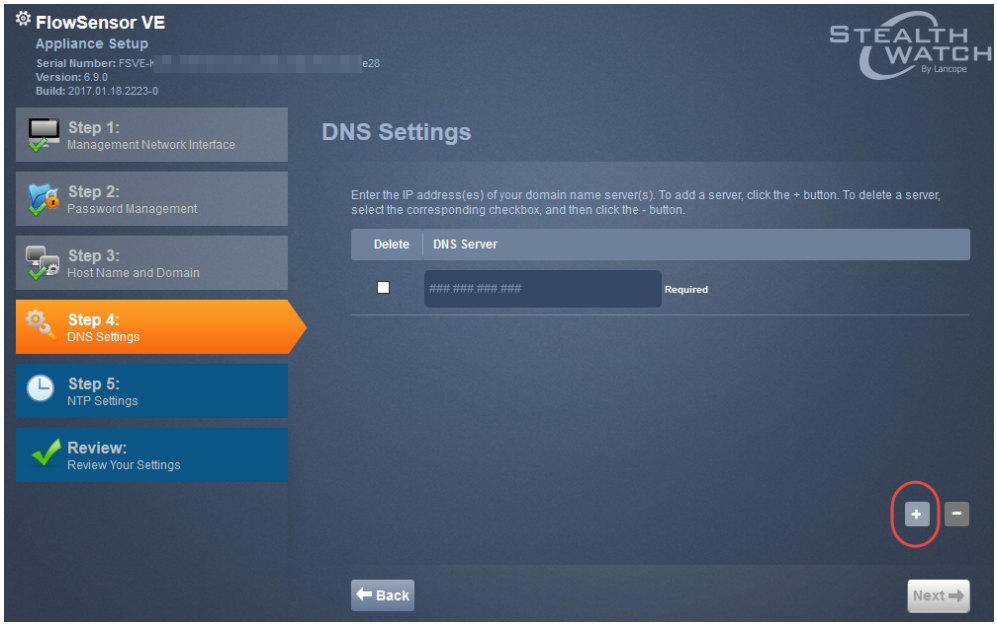
4. 前に入力した設定を確認して、[次へ(Next)] をクリックします。[パスワード管理(Password Management)] ページが開きます。



5. 適切なフィールドに新しい管理者パスワードを入力して、[次へ(Next)] をクリックします。[ホスト名とドメイン(Host Name and Domain)] ページが開きます。



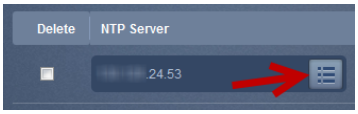
6. 適切なフィールドにホスト名とネットワークドメイン名を入力して、[次へ(Next)] をクリックします。[DNS 設定(DNS Settings)] ページが開きます。



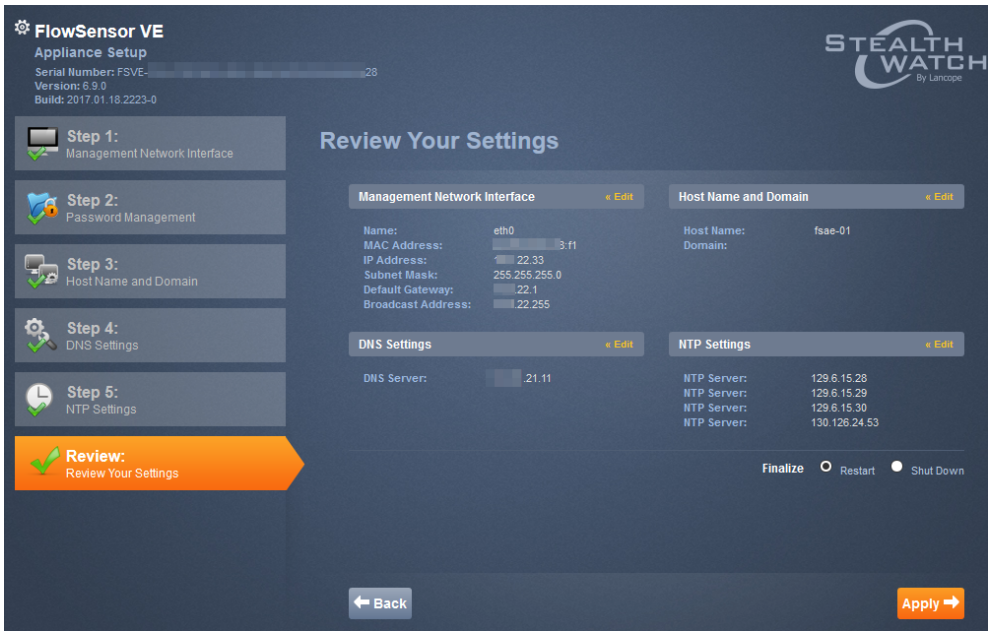
7. [+] ボタンをクリックして、DNS サーバの IP アドレスを入力します。[次へ(Next)] をクリックします。[NTP 設定(NTP Settings)] ページが開きます。

（注） 1 つ目の NTP サーバを pool.ntp.org に設定してください。これによって、Stealthwatch アプライアンスは NTP サーバのランダムな ntp.org プールにアクセスしてアプライアンスの時間を設定できるようになります。

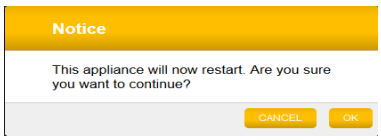
8. デフォルト設定を受け入れるか、NTP サーバの IP アドレスを入力するか、またはリスト アイコンをクリックしてドロップダウン リストから名前を選択して別のサーバを入力することができます。「アプライアンス管理インターフェイスによる設定」を参照してください。



9. [次へ(Next)] をクリックします。[レビュー(Review)] ページが開きます。



10. 設定を確認して、[適用(Apply)]をクリックします。確認ダイアログが開きます。



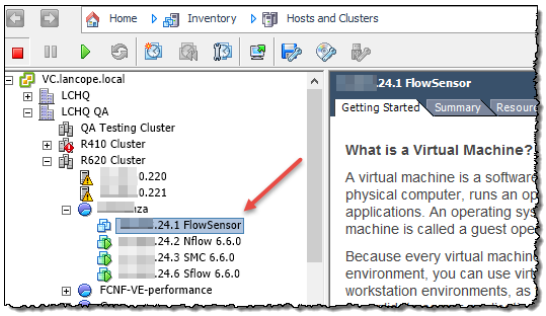
11. 新しいシステム設定が有効になるまで数分かかります。その後、[次へ(Next)]をクリックします。完了すると、アプライアンスのログインページが開きます。
12. ログインクレデンシャルを入力して、[ログイン(Login)]をクリックします。
13. 設定する他のアプライアンスがありますか。
    - 「はい」の場合、手順1に戻り、次のアプライアンスに対しこの手順を繰り返します。プライマリSMCを必ず最後に設定してください。
    - 「いいえ」の場合、次のステップに進みます。

次の「Flow Sensor VE のメモリを増やす」のセクションに進みます。

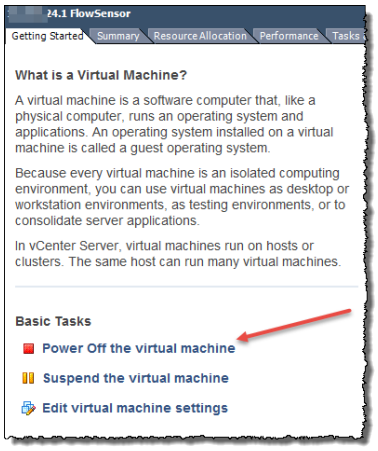
Flow Sensor VE のメモリを増やす

メモリのサイズを増やすには、次の手順を実行します。

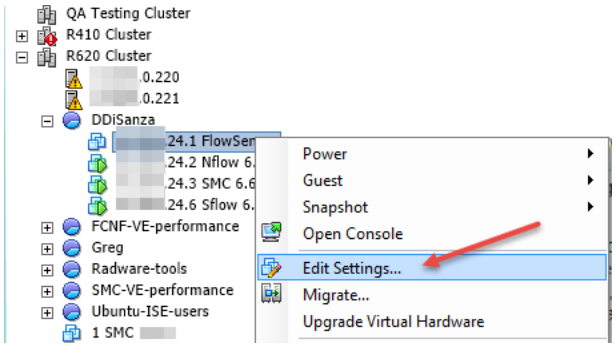
1. アプライアンスを選択します。



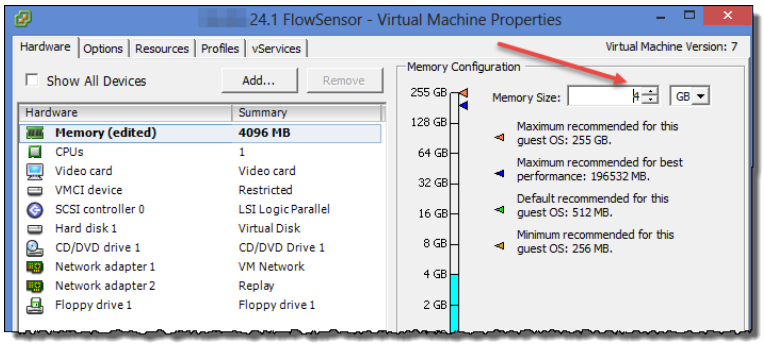
2. 必要に応じて、アプライアンスをオフにします。



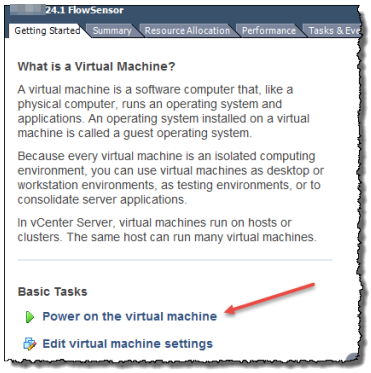
3. 右クリックして [設定の編集 (Edit Settings)] を選択します。



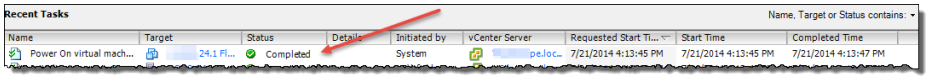
4. [ハードウェア(Hardware)] タブで [メモリ(Memory)] を選択し、メモリサイズを 4 GB に増やします。



5. [OK] をクリックして変更を適用します。インターフェイスは [はじめに(Getting Started)] ページに戻ります。

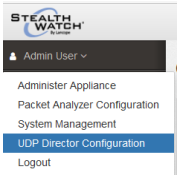


6. [アプライアンスの電源をオンにする(Power on the appliance)] をクリックしてアプライアンスを再起動します。ページの下部に確認メッセージが表示されます。



7. 次の「アプライアンス管理インターフェイスによる設定」セクションに進みます。

アプライアンス管理インターフェイスによる設定



このセクションでは、アプライアンス管理インターフェイスを使用して仮想アプライアンスの設定を完了する次の手順について説明します。

1. アプライアンス管理インターフェイスへのログイン
2. システム時刻の設定
3. 仮想アプライアンスの再起動

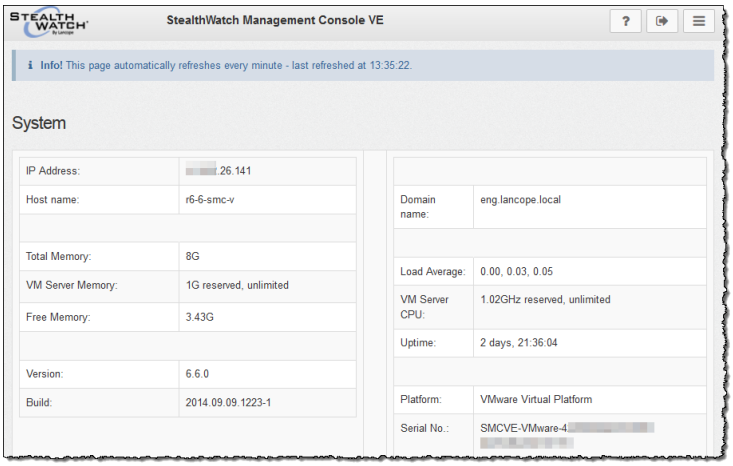
アプライアンス管理インターフェイスへのログイン

アプライアンス管理インターフェイスにログインするには、次の手順を実行します。

(注)

- Stealthwatch についてサポートされているブラウザは、Internet Explorer バージョン 9 以降と Firefox バージョン 3 以降です。
- ページのロードに問題が発生した場合は、ブラウザのキャッシュをクリアし、ブラウザを閉じて再度開き、もう一度ログインします。

1. ブラウザのアドレスフィールドに **https://** と入力して、その後に仮想アプライアンスの IP アドレスを入力し、Enter を押します。
2. SMC VE アプライアンス管理インターフェイスを開いていますか。
3. [ユーザ名 (User Name)] フィールドに **admin** と入力します。
4. [パスワード (Password)] フィールドに、アプライアンス設定で作成した管理者パスワードを入力します。
5. [ログイン(Login)] をクリックします。アプライアンス管理インターフェイスのホームページが開きます。

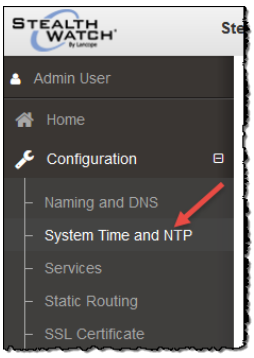


システム時刻の設定

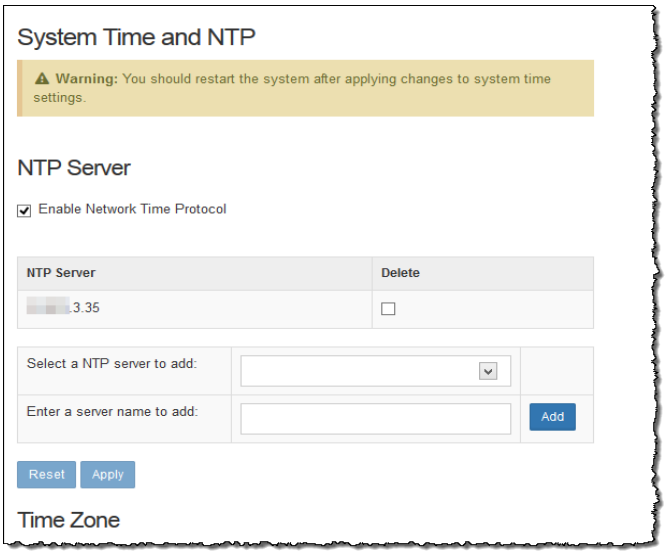
Network Time Protocol(NTP) およびシステム時刻 (タイムゾーン) 設定を仮想アプライアンスで設定するには、次の手順を実行します。

注意！ SMC に情報を送るフローコレクタやその他のデバイスに使用されているのと同じ NTP サーバを使用します。

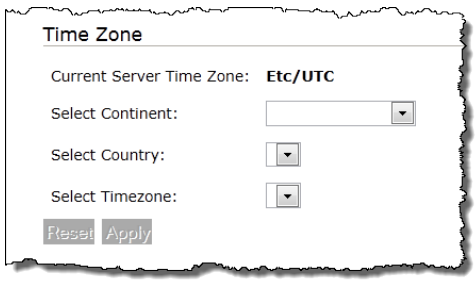
1. アプライアンス管理インターフェイスのナビゲーション ページで、[構成(Configuration)] の横のプラス記号(+) をクリックして、[システム時刻とNTP(System Time and NTP)] をクリックします。



アプライアンス設定ツールを使用して初期設定で設定したNTP サーバが表示された [NTP サーバ(NTP Server)] ページが開きます。

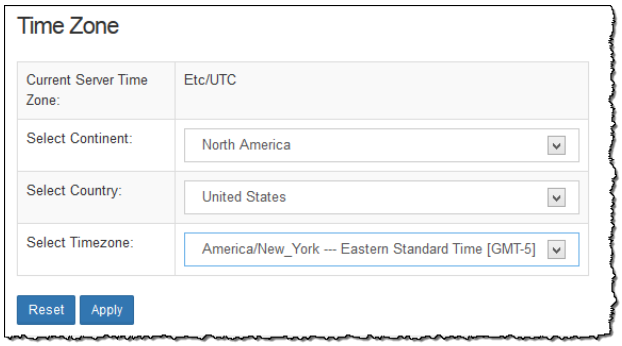


2. ページの [タイムゾーン(Time Zone)] セクションまで下にスクロールして、仮想アプライアンスシステム時刻を設定します。

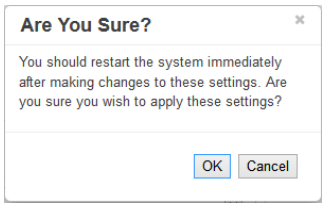


3. 次の手順を実行します。
   - ドロップダウンリストから、大陸を選択します。
   - ドロップダウンリストから、国を選択します。
   - ドロップダウンリストから、タイムゾーンを選択します。

   [適用(Apply)]が表示されます。



4. [適用(Apply)]をクリックして、変更内容を確定します。確認ウィンドウが開きます。

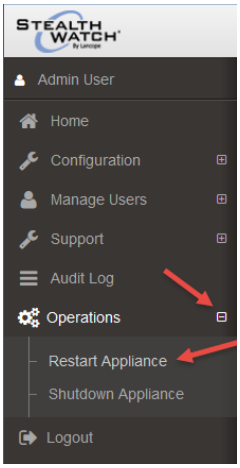


5. [OK]をクリックします。
6. 次の項「仮想アプライアンスの再起動」に進みます。

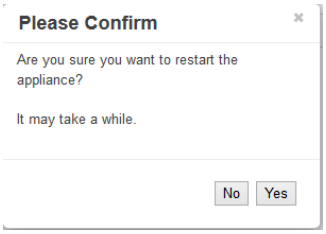
仮想アプライアンスの再起動

仮想アプライアンスを再起動するには、次の手順を実行します。

1. アプライアンス管理インターフェイス メニューで、[操作(Operations)] > [アプライアンスの再起動(Restart Appliance)] を選択します。



確認ダイアログが開きます。



2. [はい(Yes)] をクリックします。
3. 再起動後、Flow Sensor VE は VM 環境からデータを収集してそれを NetFlow コレクタに送信するようになります。

Flow Sensor VE のインストールと設定が完了しました。[SMC クライアント エンタープライズ(SCM Client Enterprise)] ツリーの [Flow Sensor(Flow Sensors)] ブランチと [VM センサー(VM Servers)] ブランチの下に、この Flow Sensor が表示されます。Flow Sensor がトラフィックを検出して Flow Collector にデータを送信し、さらにそこから SMC に転送されるようになるまで、Flow Sensor は SMC エンタープライズ ツリーには表示されません。

詳細については、SMC クライアントのオンライン ヘルプを参照してください。