



Stealthwatch[®] Management Console VE および Flow Collector[™] VE インストール/コンフィギュレーションガイド (Stealthwatch System v6.9.1 用)

インストール/コンフィギュレーション ガイド : Stealthwatch Management Console VE および Flow Collector VE v6.9.1

© 2017 Cisco Systems, Inc. All rights reserved.

ドキュメントの日付 : 2017年7月6日

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:

www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

目次

目次	iii
はじめに	1
概要	1
対象読者	1
フローコレクタ VE について	1
SMC VE について	2
はじめる前に	3
データストレージ	5
このマニュアルの使い方	6
その他のリソース	8
仮想アプライアンスのインストール	9
概要	9
プロセスの概要	9
通信用ファイアウォールの設定	10
通信ポート	10
VMware vSphere Client へのログイン	13
リソースプールの追加	14
仮想アプライアンスのインストール	16
仮想環境の設定	27
概要	27
IP アドレスの設定	27
デフォルト ユーザパスワードの変更	31
sysadmin パスワードの変更	31
ルート パスワードの変更	34

システムの設定	37
概要	37
プロセスの概要	37
個々のアプライアンスの設定	37
システムの設定	43
SMC VE またはフローコレクタ VE のディスク容量の拡張	54
フローコレクタ VE のメモリの増加	60
アプライアンス管理 インターフェイスによる設定	62
アプライアンス管理 インターフェイスへのログイン	62
システム時刻の設定	64
仮想アプライアンスの再起動	66
通信の確認	69
概要	69
NetFlow データ収集の確認	69
Cisco ISE の追加	71
概要	71
Cisco ISE の追加	71
SLIC 脅威フィード機能の有効化	73

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の、Stealthwatch Management Console(SMC) VE(バーチャルエディション) 、およびフローコレクタ VE のインストールおよび設定ガイドです。

(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](#)
- [フローコレクタ VE について](#)
- [SMC VE について](#)
- [はじめる前に](#)
- [このマニュアルの使い方](#)
- [リソース要件](#)

対象読者

このガイドの主な対象者は、StealthWatch SMC VE とフローコレクタ 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。

フローコレクタ VE について

StealthWatch システムの中心になるのは、高い拡張性を持つ Stealthwatch Flow Collector です。フローコレクタは物理アプライアンスまたは仮想アプライアンスとして提供されます。フローコレクタ VE は、VMware 環境では物理的なものと同じ機能を実行します。

NetFlow の Stealthwatch Flow Collector は、NetFlow、cFlow、J-Flow、Packeteer 2、NetStream、IPFIX データを集めます。従来のプローブベースのアプローチを使用して、ネットワーク全体の可視性を獲得するには、ネットワークの各ルータまたはスイッチにプローブをインストールする必要があります。これには多くの高額なハードウェアのインストールが必要です。逆に、StealthWatch のフローベースのアプローチは、わずかなコストでネットワーク全体の可視性を獲得できます。各フローコレクタは、フローコレクタのモデルとライセンスの制限に応じて、最大 2,000 フローエクスポーターから 1,000,000 ホストのデータを処理できます。

フローベースの異常検出を使用して、フローコレクタは、異常な動作にズームし、SMC に即座にコンテキスト インテリジェンス付でアラームを送信します。このことにより、ユーザは損傷を軽減するために迅速で決定的なアクションを行うことが可能になります。フローコレクタ:

- さまざまなフローの送信元 (ルータ/エクスポータ、スイッチ、ファイアウォール、StealthWatch フローセンサー) からのデータの収集
- 収集したデータの分析
- 通常のネットワークアクティビティのプロファイルの作成
- 通常のプロファイルに含まれないすべての動作に関するアラートの生成

SMC VE について

StealthWatch システムのコントロールセンターとして、SMC はシステムの各コンポーネントをすべて管理、調整、設定し、組織します。SMC クライアント ソフトウェアにより、Web ブラウザへのアクセス権を持つローカルコンピュータから、SMC のユーザフレンドリーなグラフィカルユーザインターフェイスにアクセスすることができます。クライアント インターフェイスを使用して、企業全体の重要なセグメントに関するリアルタイムのセキュリティとネットワーク情報に簡単にアクセスできます。

また、SMC は物理または仮想 アプライアンスとして使用可能で、次のことを行えるようにします。

- 最大 25 のフローコレクタに対する集中型の管理、設定およびレポート
- トラフィックの視覚化のためのグラフィカルチャート
- トラブルシューティングのためのドリルダウンの分析
- 統合型のカスタマイズ可能なレポート
- トレンド分析
- パフォーマンスモニタリング
- セキュリティ違反の即時通知

SMC は、異種 IT グループが、ネットワーク全体のすべてのアクティビティについてのコンテキスト情報を表示し、それに基づいて調査できる、単一の視点を提供します。かつては、最終的に適切な人員を修正措置のために配置できるようになるまでに、さまざまな IT 部門が問題の根本原因を特定しようとして何時間もさらには何日も費やし、頻繁にお互いを非難していました。しかし、SMC を使用することで、それは遠い昔のことになりました。

SMC のユーザフレンドリーなグラフィカル インターフェイスをちょっと見るだけで、オペレータは異常な動作を即座に発見し、ズームできます。SMC のユニークなドリルダウン機能を使用して、管理者は、数分のうちに問題の特定から根本原因の切り分けまでを行うことができ、途中で

影響を受けるアプリケーションおよびユーザを特定し、作業効率を向上させ、コストを削減します。

また、柔軟な SOAP 対応 Web アプリケーション プログラム インターフェイス (API) は、セキュリティ インシデント および イベント マネージャ (SIEM)、ネットワーク マネージャ、トラブル チケット 生成 システム および サードパーティ レポート システム などの、エンタープライズ アプリケーション 内からの StealthWatch データ への、準備の整った プログラム 可能な アクセス を提供 します。

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. フロー センサー VE
4. フロー コレクタ 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 でき ません。

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*』の ドキュメント を 参照 してください。

リソース要件

SMC VE

SMC VE の最小のリソース割り当てを判別するには、SMC にログインすることが予想されるフローコレクタとユーザの数を決定する必要があります。

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。

フローコレクタ	同時ユーザ数*	最小の予約済みメモリ	推奨される予約済みメモリ	予約済み CPU
1	2	16 GB	24 GB	3
3	5	24 GB	32 GB	4
5	10	32 GB	32 GB	4

*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。

予約済みメモリ: システムで限られた数のフローコレクターを使用し、データの収集量が少ない場合は、最小の予約済みメモリの量を使用できます。システムのデータ収集量が多い場合、推奨される予約済みメモリの量を使用します。

SMC VE 2000

次の仕様は、SMC VE 2000 のダウンロードのデフォルト設定、推奨する最小値、同等のハードウェアの見積りです。

	OVF	推奨する最小値	同等ハードウェア*
RAM	64 GB	64 GB	128 GB
CPU	8	8	36
ストレージ	50 GB	200 GB	3.6 TB

*これらの数値は、SMC 2010 アプライアンスと物理(非ハイパー スレッド)コアに基づいています。

フローコレクタ VE

フローコレクタ VE のリソース割り当てを決定するには、ネットワークで予想される秒当たりのフローと、モニタすることが予想されるホストとエクスポート数を決定する必要があります。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。

1 秒あたりのフロー数	エクスポート	Hosts	推奨予約済みメモリ	予約済み CPU	フローコレクタ VE モデル
最大 4,500	最大 250	最大 125,000	16 GB	2	FCVE
最大 15,000	最大 500	最大 250,000	24 GB	3	FCVE

1秒あたりのフロー数	エクスポート	Hosts	推奨予約済みメモリ	予約済みCPU	フローコレクタVEモデル
最大 22,500	最大 1000	最大 500,000	32 GB	4	FCVE
最大 30,000	最大 1000	最大 500,000	32 GB	5	FCVE
最大 60,000	最大 1500	最大 750,000	64 GB	6	2000
最大 120,000	最大 2000	最大 1,000,000	128 GB	7	4000

次に、フローコレクタ VE モデルとその容量*を示します。

FC VE モデル	1秒あたりのフロー数	エクスポート	Hosts	予約済みメモリ	予約済みCPU	最大ディスクストレージ
1000	最大 30,000	最大 1,000	最大 500,000	32 GB	5	1 TB
2000	最大 60,000	最大 1,500	最大 750,000	64 GB	6	2 TB
4000	最大 120,500	最大 2,000	最大 1,000,000	128 GB	7	4 TB

*以下の数値は、VMWare ESXi 5.5.0 892794 のテストに基づいています。

ローカルおよびリモート : Dell R620、384 GB DDR3、2x es02660 2.2 Hz 8C(合計 16C) 、6x 300 GB、10K RAID 6、2x 256 GB Samsung 840Pro VM c\キャッシュ

ローカル: Dell R720、128GB DDR3、2xE5-2670 2.6 GHz8C(合計 16C) 、12x 600 GB 10K RAID 6

VMware から 1G リンク経由でリモート ファイル システムに対し NetApp FAS3220 ストレージ ISCSI/Nfs

データストレージ

フローコレクタ VE または SMC VE で許可されるデータストレージの最大容量は 4 TB です。最大ディスク領域は 5.6 TB です。仮想アプライアンスはデータストレージにディスクの約 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、必要なディスク容量より、常に 40% 多くディスクを拡張します。

重要: 毎日のシステム平均の毎秒 1,000 フロー (FPS) ごとに 1 GB 以上のディスクストレージを割り振り、これに保存する日数を乗じた容量を割り当てることを推奨します。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) 以上のストレージ容量を割り当てます。

(注) 外部イベント処理機能 (syslog) を使用すると、より多くのメモリおよび処理リソースが必要です。

vSphere Client インターフェイスに必要な情報

設定	ESX/vSphere サーバ	フローコレクタ VE	SMC 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 = 192.168.1.4)	(デフォルト = 192.168.1.11)
ネットマスク IP アドレス		(デフォルト = 255.255.255.0)	(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)	(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	フローコレクタ VE	SMC VE
IP アドレス	(デフォルト = 192.168.1.4)	(デフォルト = 192.168.1.11)
ホスト名 (Host Name)		
ネットワークドメイン名		
NTP サーバの IP アドレス		
DNS サーバの IP アドレス		

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
2. 仮想アプライアンスのインストール	通信用のファイアウォールの設定、リソースプールの追加、ソフトウェアのインストールの方法
3. 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
4. システムの設定	トラフィックデータを処理するようにアプライアンスを設定する方法
5. 通信の確認	SMC が NetFlow データを受信していることを確認する方法
6. Cisco ISE の追加	アイデンティティ デバイスを追加する方法
7. SLIC 脅威フィード機能の有効化	SMC クライアント インターフェイスで SLIC 脅威フィード機能を有効にする方法

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 (Maximum Transmission Unit)
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
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、Stealthwatch カスタマーコミュニティ Web サイト (<http://community.lancope.com>) [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)
- Stealthwatch のカスタマーコミュニティ Web サイト (<http://community.lancope.com>) 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。

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. リソースプールの追加
4. 仮想アプライアンスのインストール

先にフローコレクタ VE に対しこれらの手順を実行してから、SMC VE でも同じ手順を繰り返す必要があります。

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、この項に示す図と表表を使用してネットワークを設定します。

次のポートが開いていて、無制限のアクセスを提供できるように、ネットワーク管理者と相談してください。

- 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

ポートがStealthWatchシステムで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
AnyConnect	エンドポイント コンセントレータ	UDP/2055	NetFlow

送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
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	フロー コレクタ	UDP/2055	NetFlow
外部ログソース	SMC	UDP/514	SYSLOG
フロー コレクタ	SMC	TCP/443	HTTPS
SLIC	SMC	TCP/443 または プロキシされた接続	HTTPS
UDP Director	フロー コレクタ - sFlow	UDP/6343	sFlow
UDP Director	フロー コレクタ - NetFlow	UDP/2055*	NetFlow
UDP Director	サードパーティイベント管理システム	UDP/514	SYSLOG
フロー センサー	SMC	TCP/443	HTTPS
フロー センサー	フロー コレクタ - NetFlow	UDP/2055	NetFlow
アイデンティティ	SMC	TCP/2393	SSL
NetFlow エクスポート	フロー コレクタ - NetFlow	UDP/2055*	NetFlow
sFlow エクスポート	フロー コレクタ - sFlow	UDP/6343*	sFlow
SMC	Cisco ISE	TCP/443	HTTPS
SMC	DNS	UDP/53	DNS
SMC	フロー コレクタ	TCP/443	HTTPS
SMC	フロー センサー	TCP/443	HTTPS
SMC	アイデンティティ	TCP/2393	SSL
SMC	フロー エクスポート	UDP/161	SNMP
SMC	エンドポイント コンセントレー	UDP.2055	HTTPS

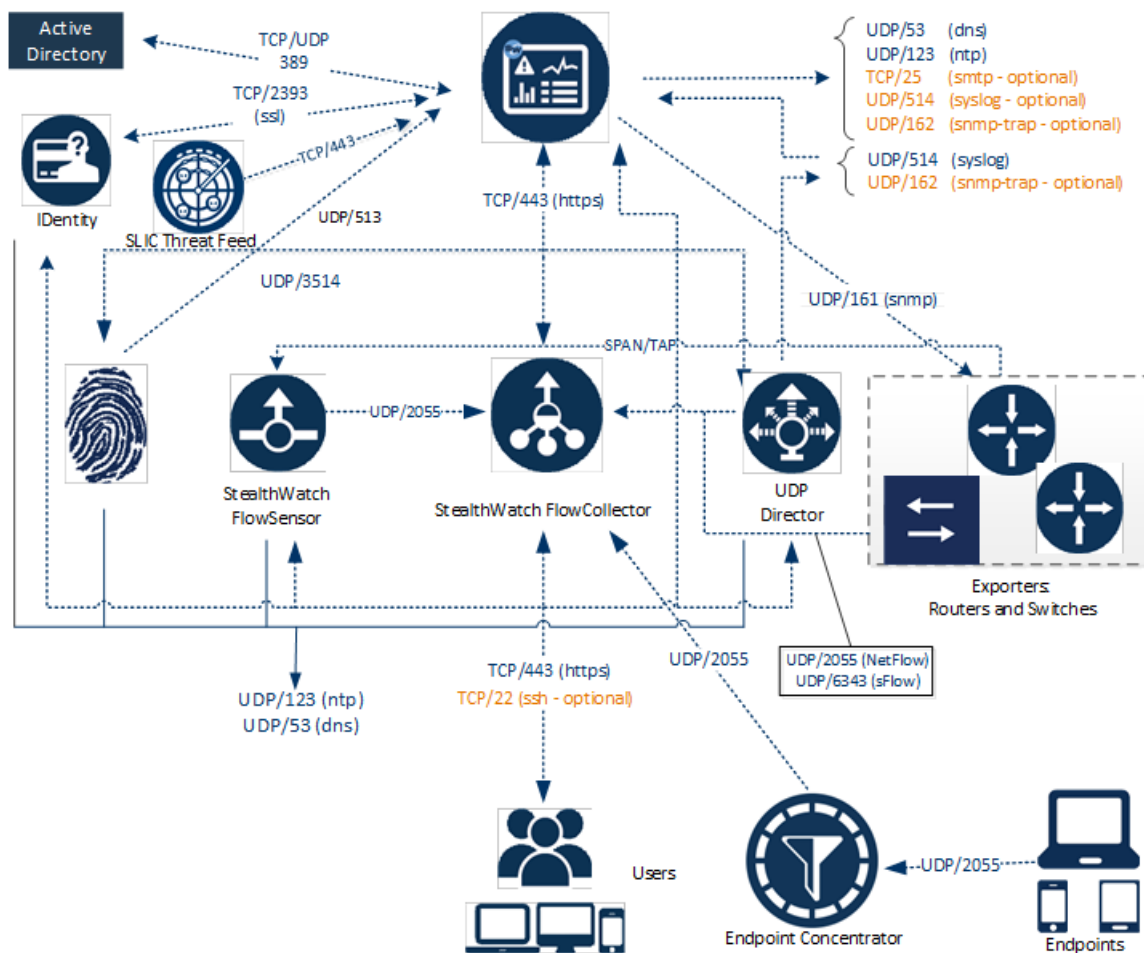
送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
	タ		
ユーザ PC	SMC	TCP/443	HTTPS

* これはデフォルトの NetFlow ポートです。ただし、どの UDP ポートもエクスポートで設定できます。

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 (Port)]	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	サードパーティイベント管理システム	UDP/514	SYSLOG
SMC	E 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ます。オプションとしてマークされたポートは、ネットワーク要件に応じて使用できます。

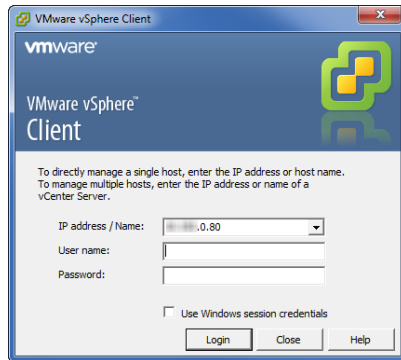


VMware vSphere Client へのログイン

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。

(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。

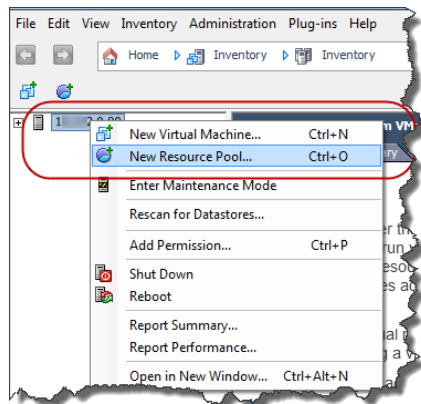
リソースプールの追加

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が適切に割り当てられた新しいリソースプールを追加する方法を説明します。

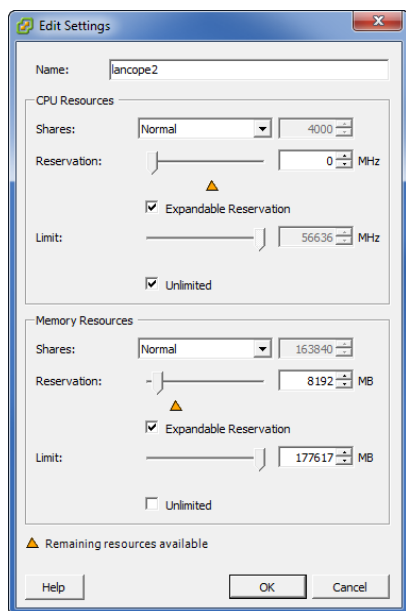
(注) 必要に応じて、仮想アプライアンスに既存のリソースプールを使用できます。ただし、次の手順を確認して、仮想アプライアンスが適切に動作するのに十分なリソースが既存のリソースプールに割り当てられていることを確認する必要があります。VMware Web Client v5.5 インターフェイスを使用する場合、ここに表示されるいくつかの画面は異なります。そのため、必要に応じてオプションの違いを示します。

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)] の順に選択します。



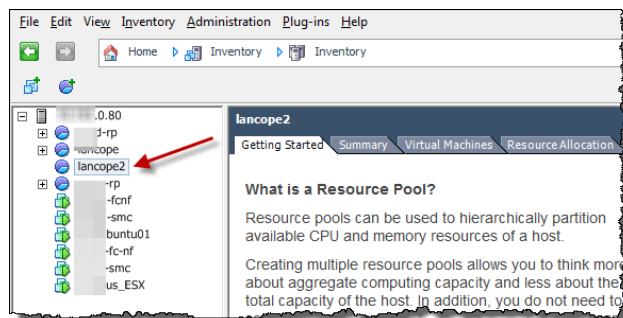
[リソースプールの作成 (Create Resource Pool)] ダイアログが開きます。



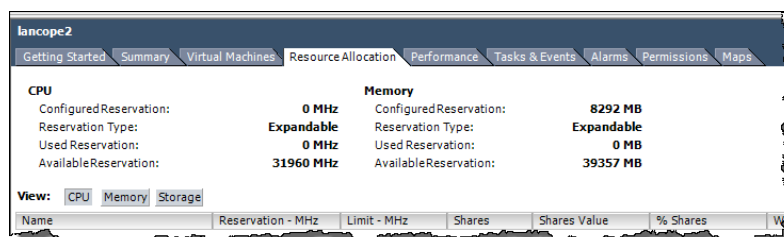
2. [名前 (Name)] フィールドに、このリソースグループの識別に使用する名前を入力します。
3. [CPU リソース (CPU Resources)] セクションの設定は変更しないでください。
4. [メモリリソース (Memory Resources)] セクションで、次の操作を実行します。
 - 「リソース要件」、ページ 3 で該当するアプライアンス用の図で推奨しているように [予約 (Reservation)] フィールドを変更します。
 - [制限 (Limit)] フィールドを少なくとも 4 GB (推奨 8 GB) に変更します。
 - [無制限 (Unlimited)] 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 より少ないメモリはサポートされません。4 GB より少なく割り当てられると、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。

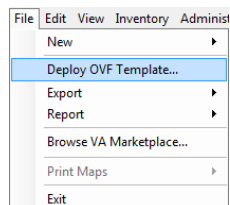


9. 次の項「[仮想アプライアンスのインストール](#)」に進みます。

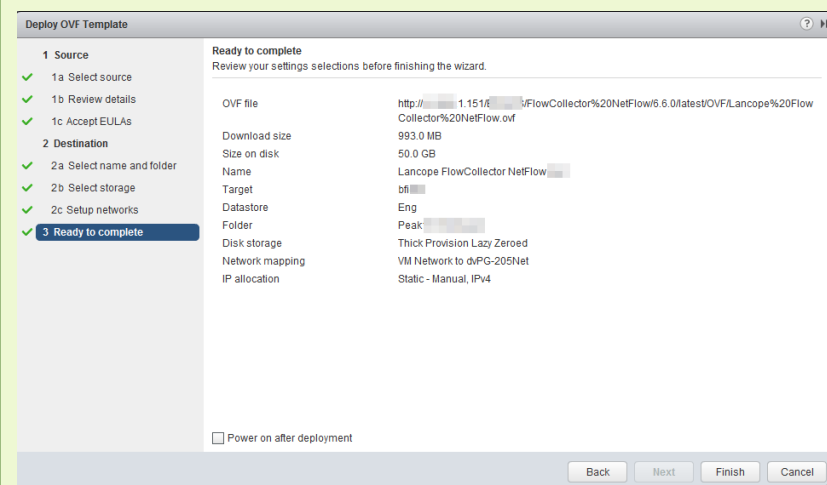
仮想アプライアンスのインストール

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。

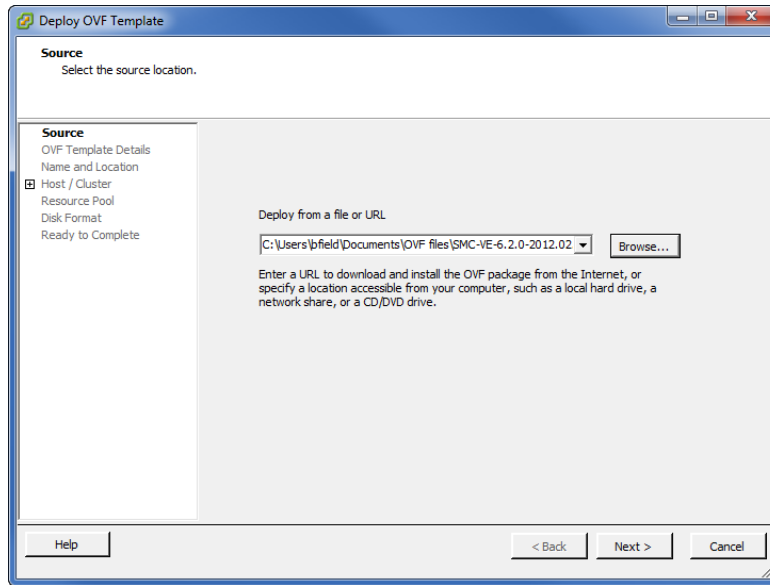
1. ダウンロード済みの仮想アプライアンスソフトウェア (OVF) ファイルを解凍します。
2. vSphere Client メニューで、[ファイル (File)] > [OVF テンプレートの展開 (Deploy OVF Template)] をクリックします。Web クライアントでは、ホストを右クリックして [OVF テンプレートの展開 (Deploy OVF Template)] を選択します。



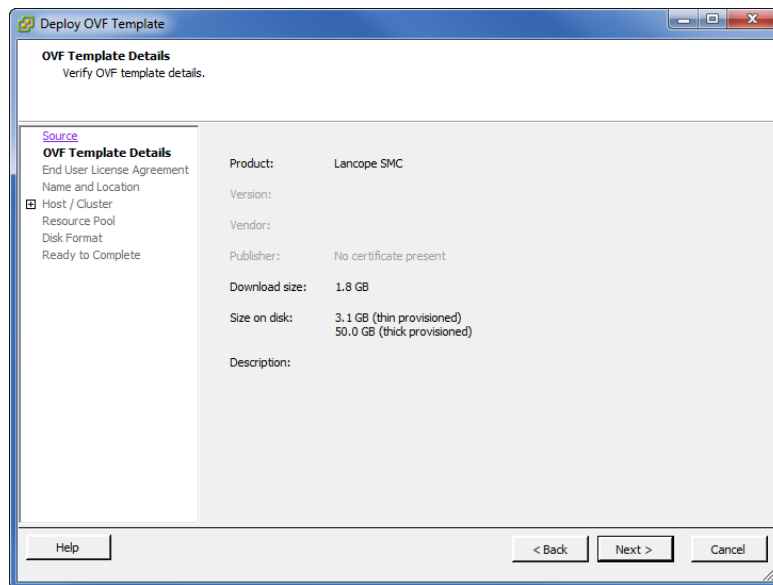
(注) Web クライアントの OVF テンプレート ウィザードでは手順の表現とナンバリングがわずかに異なりますが、手順は同じです。1 つの例として、Web クライアントでは [ソース (Source)] ではなく [ソースの場所 (Source Location)] を使用します。下のイメージでは、展開の準備が整った OVF テンプレートの左側に手順が表示されています。



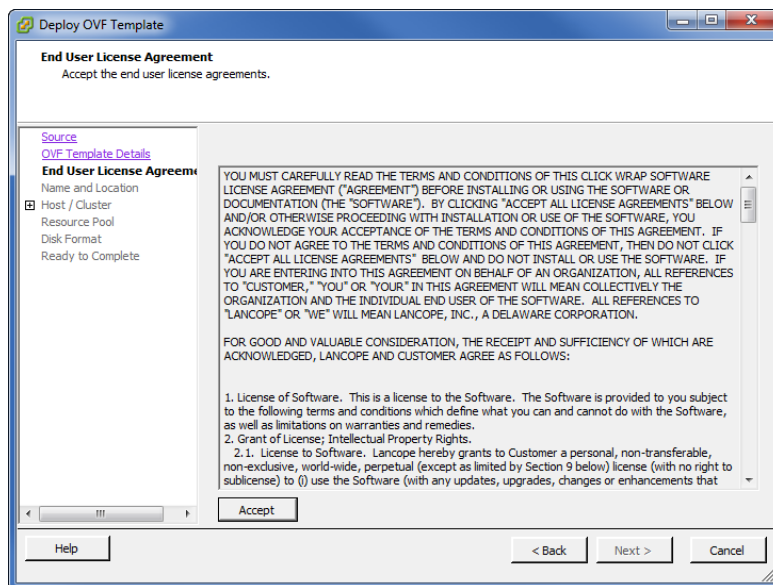
[OVF テンプレートの展開 (Deploy OVF Template)] ウィザードが開きます。



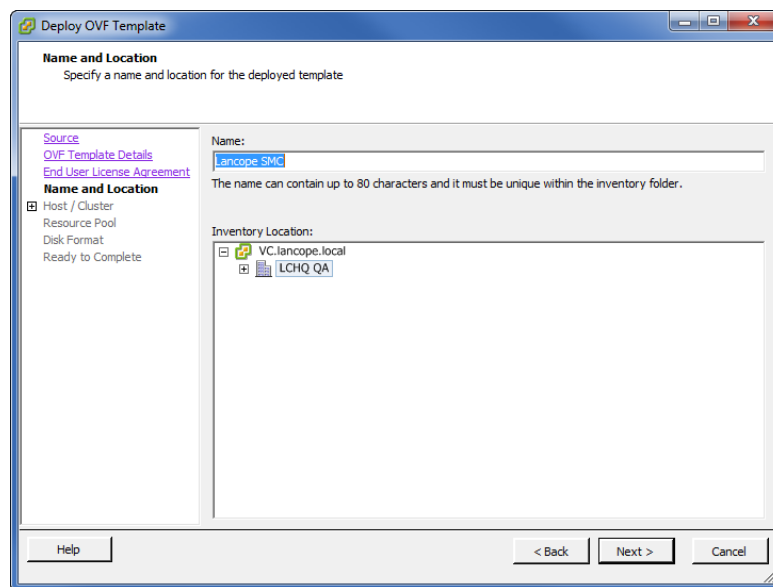
3. [参照 (Browse)] をクリックし、仮想アプライアンス OVF ファイルを探して選択します。
4. [次へ (Next)] をクリックすると、[OVF テンプレートの詳細 (OVF Template Details)] ページ (Web クライアント : 1b. [詳細の確認 (Review details)]) が表示されます。



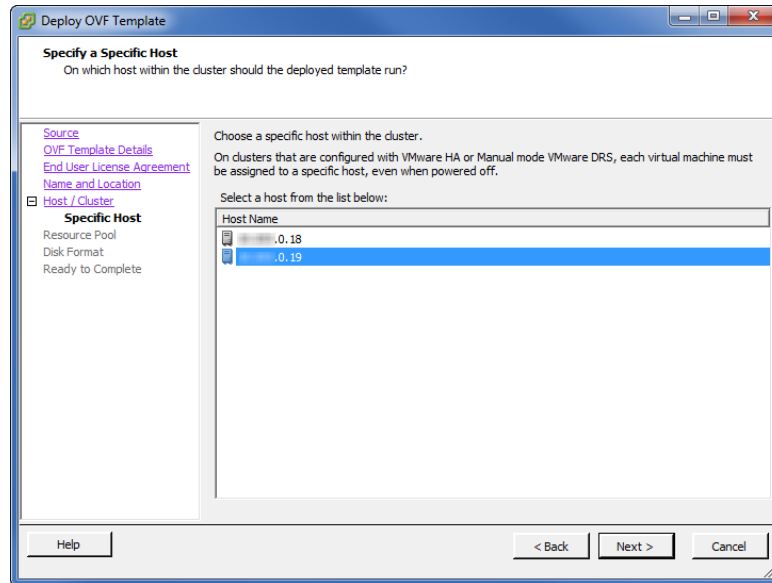
5. [次へ (Next)] をクリックします。[エンド ユーザライセンス契約 (End User License Agreement)] が開きます (1c. [EULA の承認 (Accept EULAs)])。



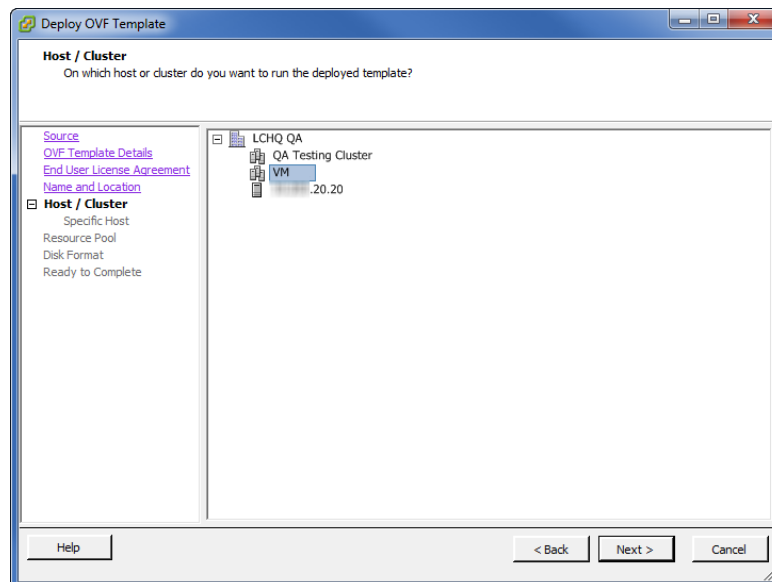
6. 情報を確認した後、[同意する(Accept)] をクリックして [次へ(Next)] をクリックします。[名前と場所 (Name and Location)] ページが開きます (2a. [名前とフォルダの選択 (Select name and folder)])。



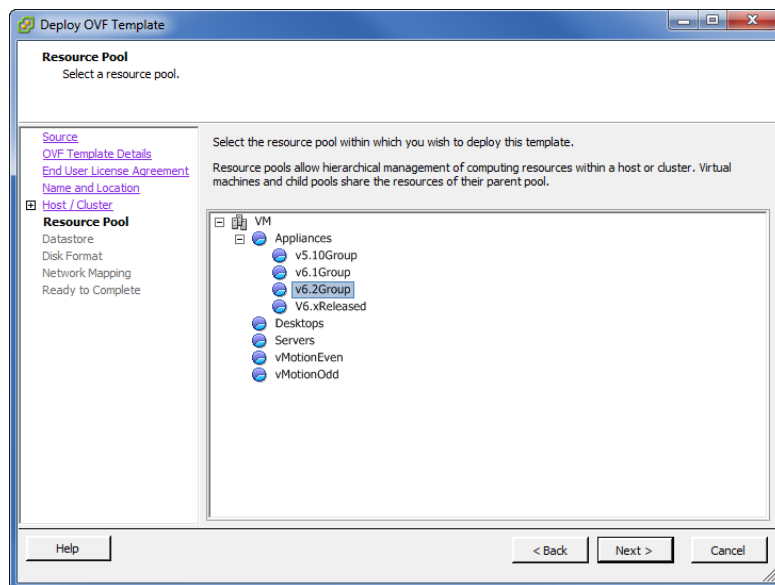
7. 必要に応じて、インベントリツリーに表示される仮想アプライアンスの名前を変更し、[次へ (Next)] をクリックします。
- [特定ホストの指定 (Specify a Specific Host)] ページが開いたら、仮想アプライアンスが存在するホストまたはクラスターを選択します。



- [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。



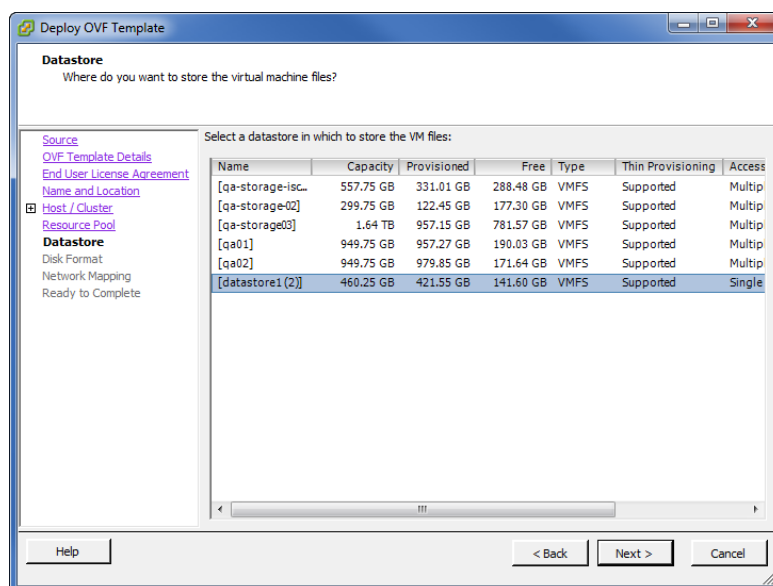
8. [次へ(Next)] をクリックします。[リソースプール(Resource Pool)] ページが開きます。



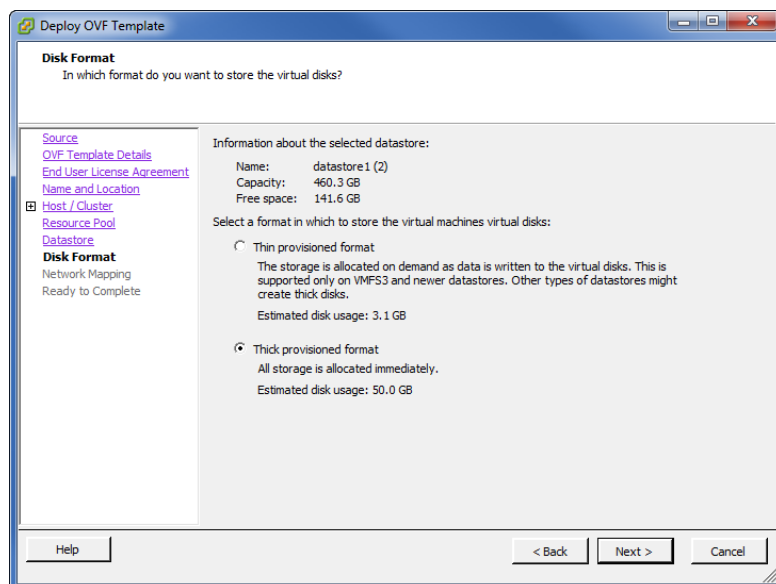
9. 以前に定義したリソースプールを選択して、[次へ (Next)] をクリックします。
 - a. [データストア (Datastore)] ページが開いたら、手順 10 に進みます。
 - b. [ディスク形式 (Disk Format)] ページが開いたら、手順 11 に進みます。

(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。

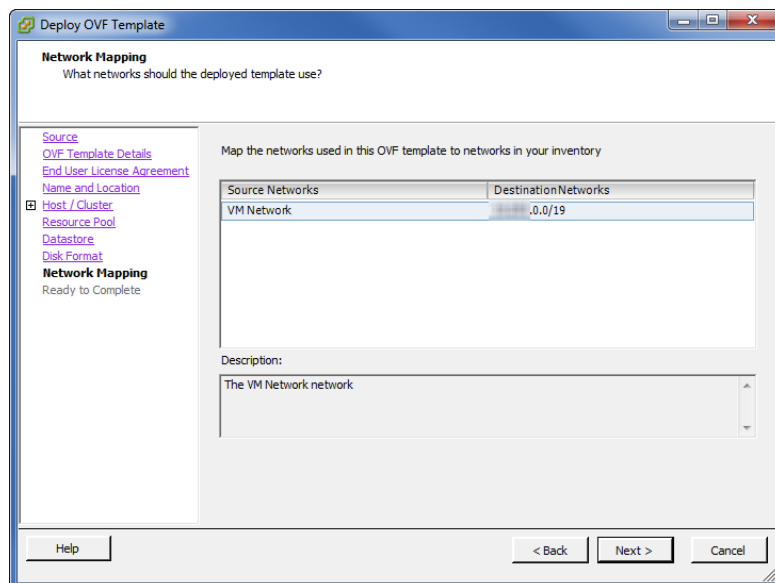


[ディスク形式 (Disk Format)] ページが開きます。

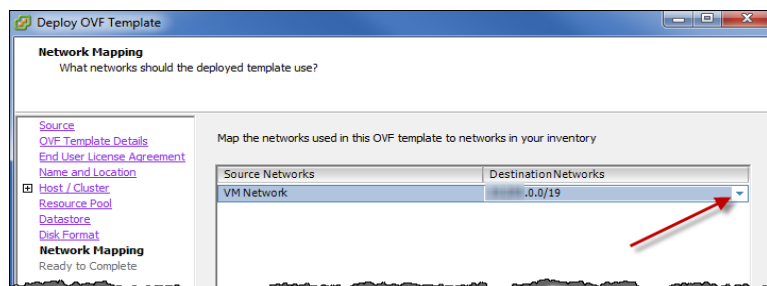


(注) vSphere Client v5 以降では、Lazy Zeroed と Eager Zeroed という2つのシックプロビジョニング形式があります。ご使用のディスクストレージのニーズに最適なものを選択してください。シンプロビジョニング形式は、ディスク容量が制限されている場合にのみ使用します。詳細については、VMware のマニュアルを参照してください。

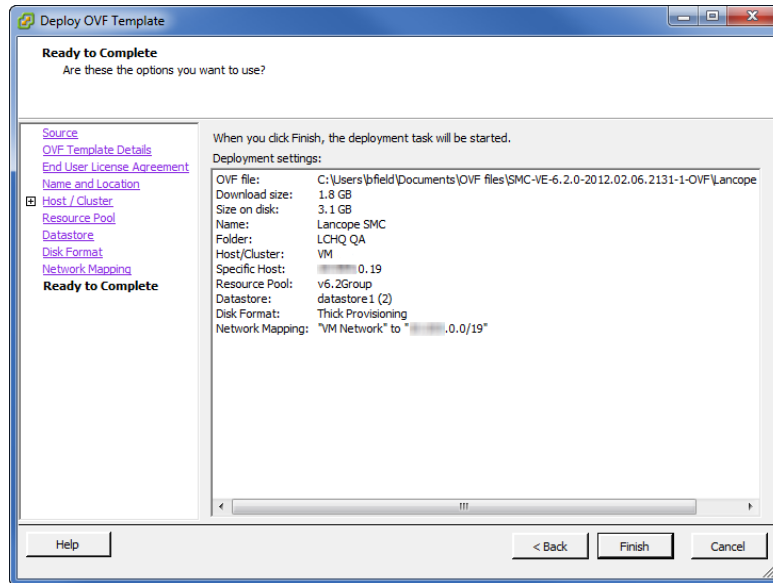
11. [ディスク形式 (Disk Format)] ページで、[シックプロビジョニング形式 (Thick provisioned format)] を選択して、[次へ (Next)] をクリックします。[ネットワークマッピング (Network Mapping)] ページ (Web クライアント : 2c. [ネットワーク設定 (Setup Networks)]) が開きます。



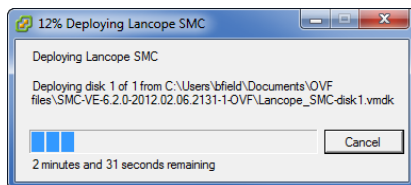
12. [宛先ネットワーク (Destination Networks)] ドロップダウンリストから、仮想アプライアンスの管理ポートを選択します。



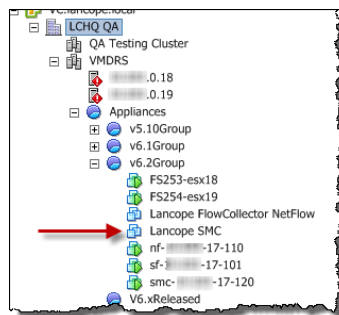
13. [次へ (Next)] をクリックします。設定の概要を示した [完了前の確認 (Ready to Complete)] ページが開きます。



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. すべてのフローコレクタ VE とさらにすべての SMC VE に対し、この章のすべての手順を完了しましたか。

-
- 「はい」の場合、「[仮想環境の設定](#)」に進みます。
 - 「いいえ」の場合、次の仮想アプライアンスに対しこの章のすべての手順を繰り返します。

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すると、これらの仮想環境を設定する準備が整います。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。

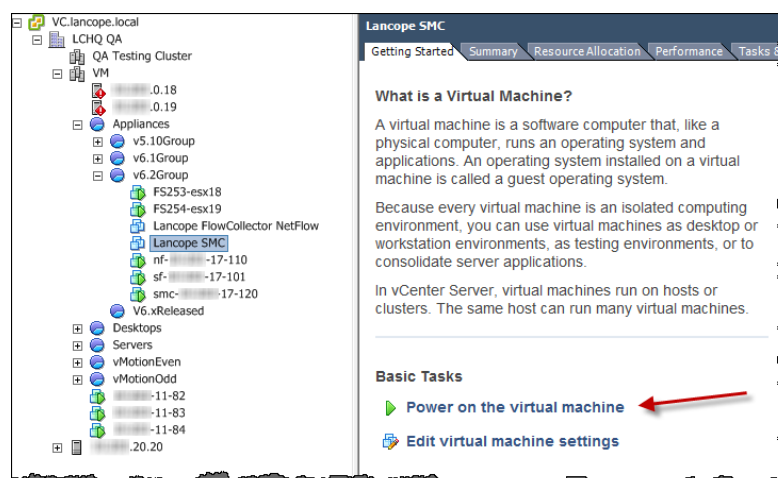
1. IP アドレスの設定
2. デフォルト ユーザパスワードの変更

先にフローコレクタ VE に対しこれらの手順を実行してから、同じ手順を SMC VE にも実行する必要があります。

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。



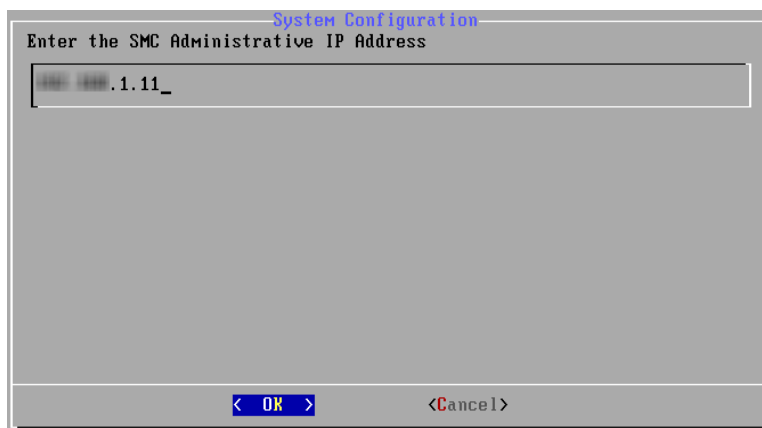
2. インベントリツリーで、設定する StealthWatch 仮想アプライアンスを選択します。
3. [はじめに(Getting Started)] ページで、[仮想マシンの電源投入(Power on the virtual machine)] リンクをクリックします。このリンクを表示するには、下方向へのスクロールが必要になる場合があります。

(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。
- メモリの割り当ておよび予約を 4 GB に削減します。

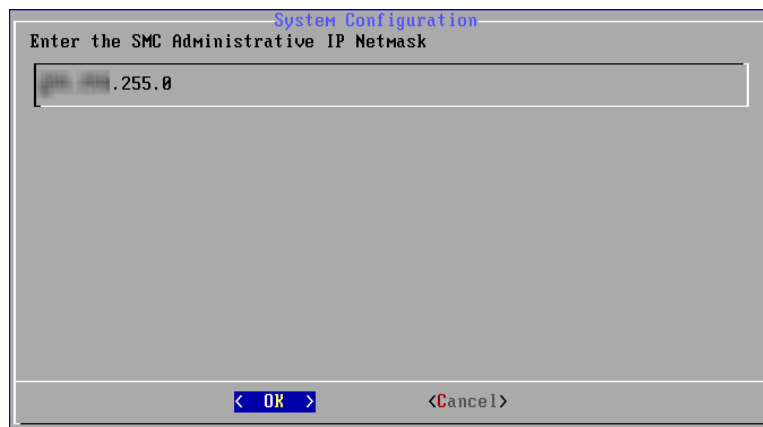
注意! メモリ予約が割り当てよりも少なくなるほどメモリ予約を削減しないでください。4 GB よりも少ない設定にはしないでください。詳細については、「リソース要件」、ページ 3 で該当するアプライアンスの図を参照してください。

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。

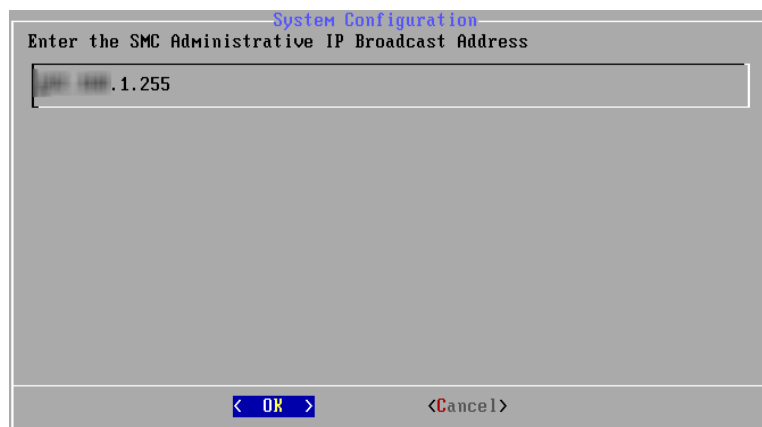
5. ページをクリックしてから、仮想アプライアンスの IP アドレスを入力します。
6. [OK] を選択して、Enter を押します。デフォルトのネットワークマスク IP アドレスが表示された [IP ネットマスク(IP Netmask)] ページが開きます。



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。

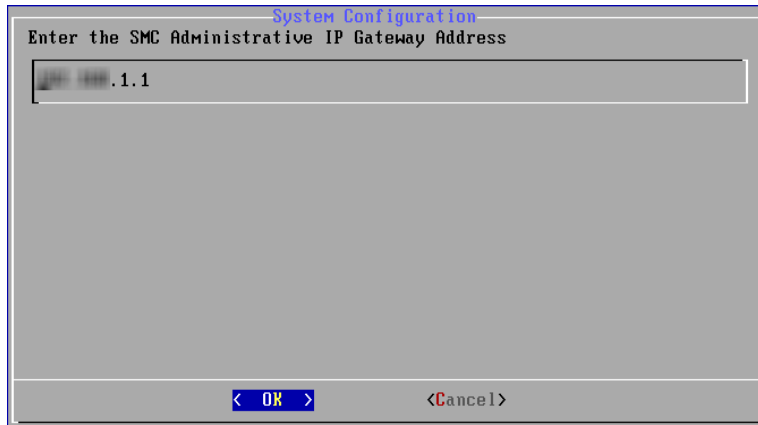
デフォルトのブロードキャスト IP アドレスが表示された [IP ブロードキャスト アドレス (IP Broadcast Address)] ページが開きます。



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。

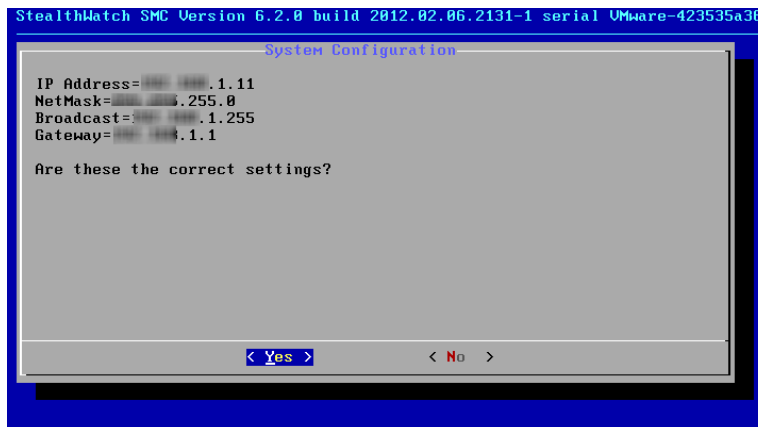
デフォルトのゲートウェイサーバ IP アドレスが表示された [ゲートウェイアドレス (Gateway Address)] ページが開きます。



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。

```
System Configuration
Primary network parameters have been modified. Please note that
modifying the settings for the primary network interface may
disable network access to this system which will require console
access to repair. This system will now be restarted to
implement these changes.
```

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。

```
Setting up networking...
INIT: Entering runlevel: 2

Welcome to StealthWatch SMC Version 6.2.0
smc-01 login: _
```

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。

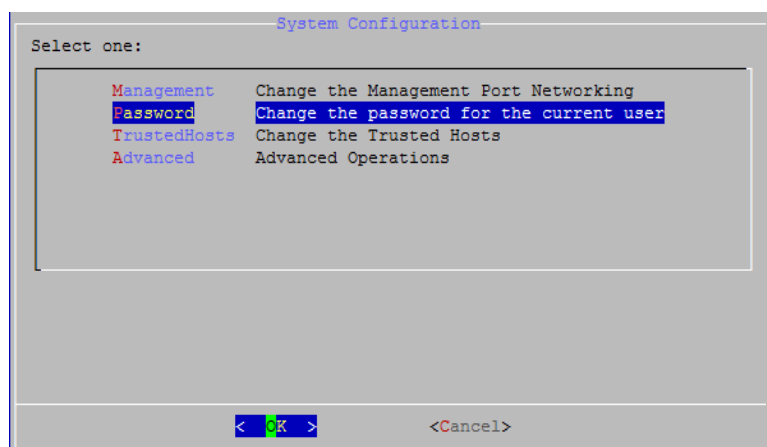
デフォルト ユーザパスワードの変更

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リケーションのルート 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

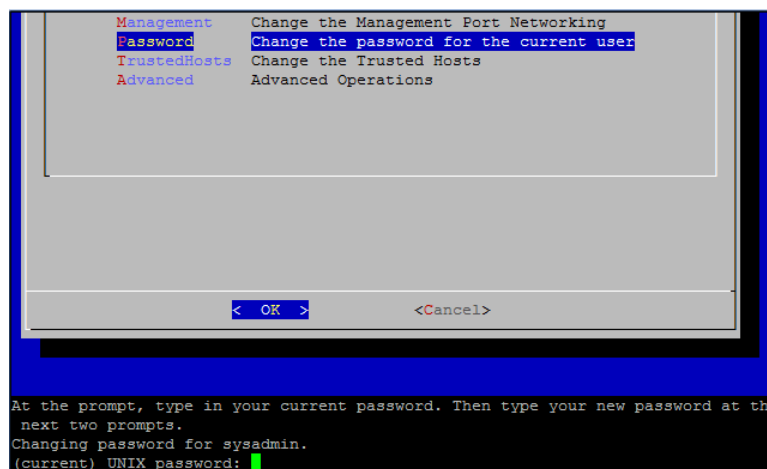
sysadmin パスワードを変更するには、次の手順を実行します。

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。



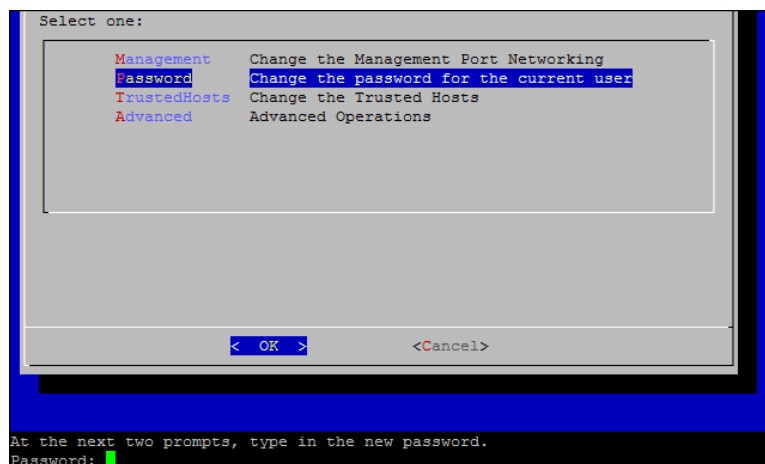
重要: 信頼できるホストのリストをデフォルトから変更する場合、各 Stealthwatch アプライアンスが展開内の他のすべての Stealthwatch アプライアンスの信頼できるホストのリストに含まれていることを確認する必要があります。そうしなければ、アプライアンス間で通信できません。

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。

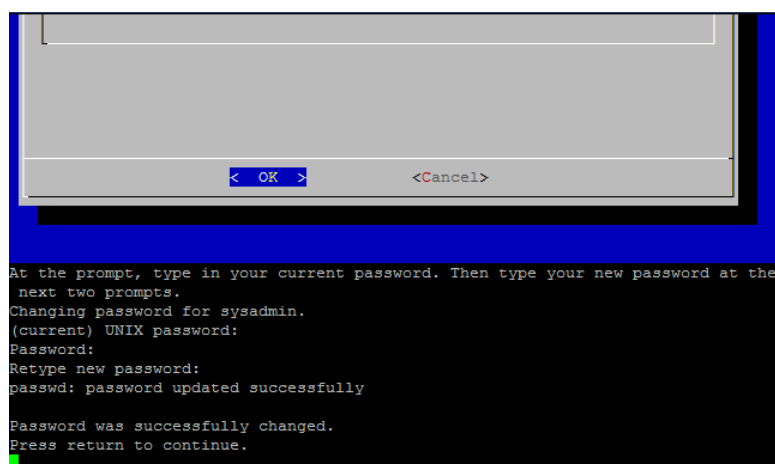


4. 新しいパスワードを入力して、Enter を押します。

(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。



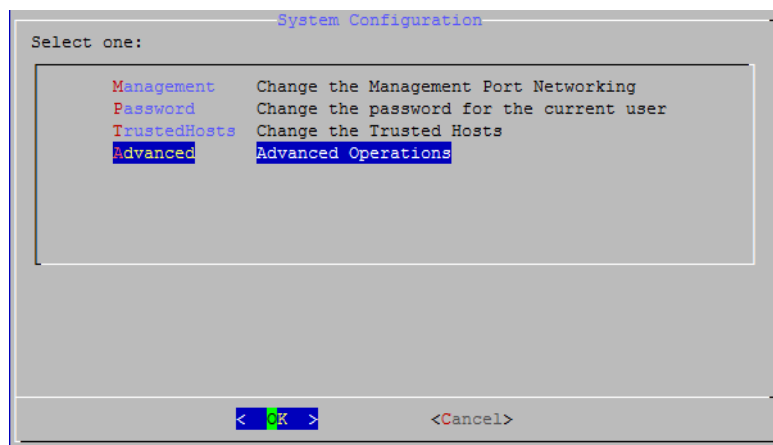
6. Enter を押して、[システム設定 (System Configuration)] コンソールメニューに戻ります。

7. 次の「ルートパスワードの変更」セクションに進みます。

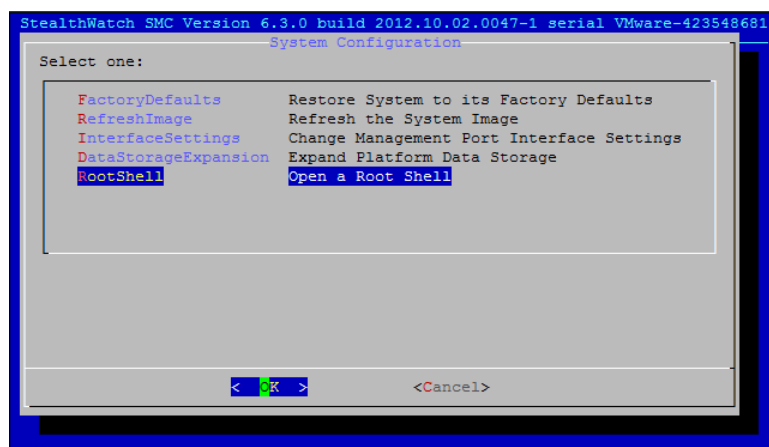
ルート パスワードの変更

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。

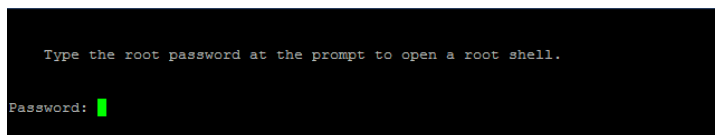
1. [システム設定 (System Configuration)] コンソールメニューで、[詳細 (Advanced)] を選択して Enter を押します。[詳細 (Advanced)] メニューが開きます。



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。

```
Type the root password at the prompt to open a root shell.

Password:
smokenetb-ve-1:~# █
```

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。

```
Select one:

Management      Change the Management Port Networking
Password         Change the password for the current user
TrustedHosts    Change the Trusted Hosts
Advanced         Advanced Operations

< OK >          <Cancel>

At the next two prompts, type in the new password.
Password: █
```

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。

```
< OK >          <Cancel>

At the next two prompts, type in the new password.
Password:
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
Password was successfully changed.
Press return to continue.
█
```

7. 新しいルート パスワードを再入力して、Enter を押します。

```

At the next two prompts, type in the new password.
Password:
Retype new password:
passwd: password updated successfully

Password was successfully changed.
Press return to continue.
exit
  
```

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. すべてのフローコレクタ VE およびすべての SMC VE に対し、この章の手順すべてを完了しましたか。
 - 「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](#)」、[ページ 27](#)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。

システムの設定

概要

この章では、トラフィックデータの処理を開始する仮想アプライアンスを設定する手順を提供します。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」、ページ 3 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 システムの設定には、この章で説明する、次の手順の実行が含まれません。

1. 個々のアプライアンスの設定
2. システムの設定
3. SMC VE またはフローコレクタ VE のディスク容量の拡張
4. フローコレクタ VE のメモリの増加
5. アプライアンス管理 インターフェイスによる設定

(注) ネットワークでフェールオーバー SMC を使用している場合、フェールオーバー アプライアンスを最初に設定します。プライマリ SMC を設定すると、フェールオーバー SMC の IP アドレスを設定できます。

先にフローコレクタ VE に対しこれらの手順を実行してから、SMC VE に同じことを行う必要があります。

個々のアプライアンスの設定

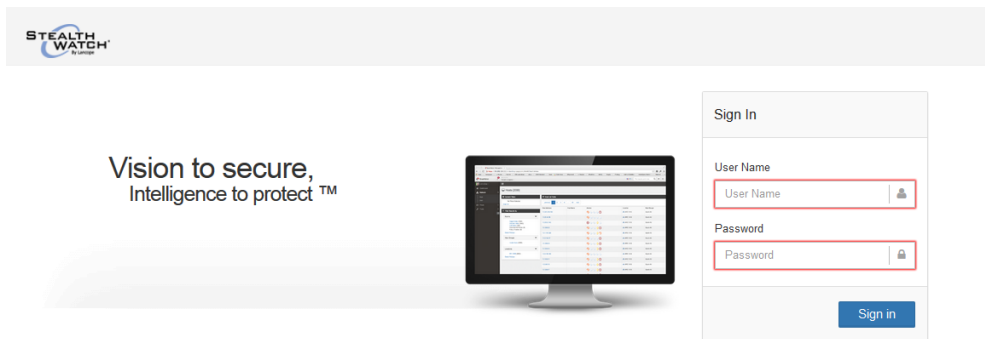
すべてのアプライアンスの初期設定は、アプライアンス設定ツールで実行されます。アプライアンスに初めてアクセスすると、アプライアンス設定ツールが表示されます。システムによっては、UDP Director の前にフローセンサーとフローコレクタを設定してから、最後に、SMC VE を設定する必要があります。SMC VE の初期設定を完了すると、システム設定ツールが開き、StealthWatch システムを設定できます。

開始する前に、「はじめる前に」、ページ 3 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。

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 を設定していますか。
 - 「はい」の場合、手順 4 に進みます。
 - 「いいえ」の場合、手順 3 に進みます。
3. 管理者ログインページが開きます。 **admin** および **Ian411cope** (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。

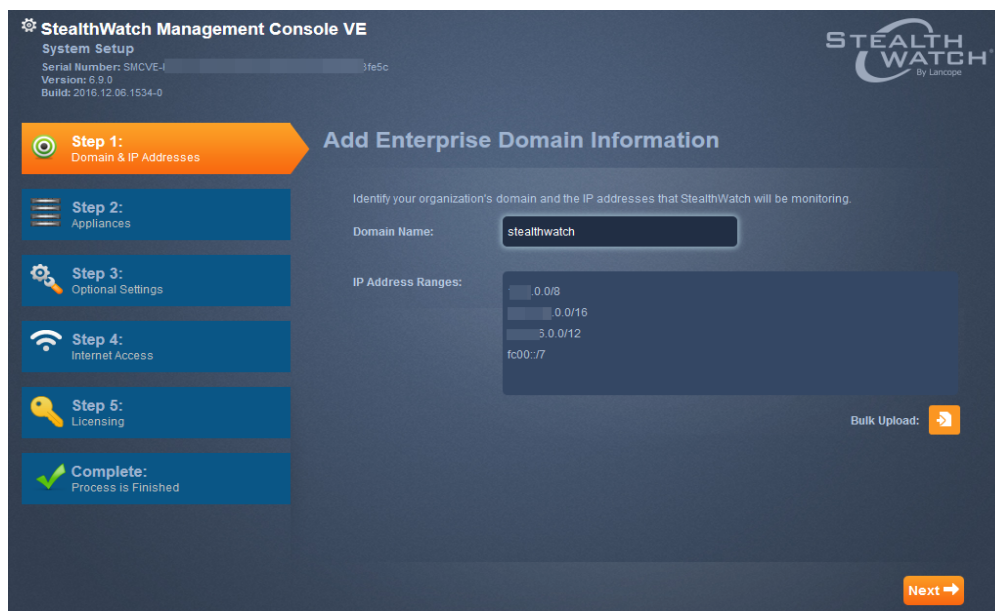


ログインするには、次の手順を実行します。

- a. [ユーザ名 (User Name)] フィールドに **admin** と入力します。
 - b. [パスワード (Password)] フィールドに「**Ian411cope**」と入力します。
 - c. [サインイン (Sign In)] をクリックします。
5. [ようこそ (Welcome)] ページが開きます。[続行 (Continue)] をクリックします。



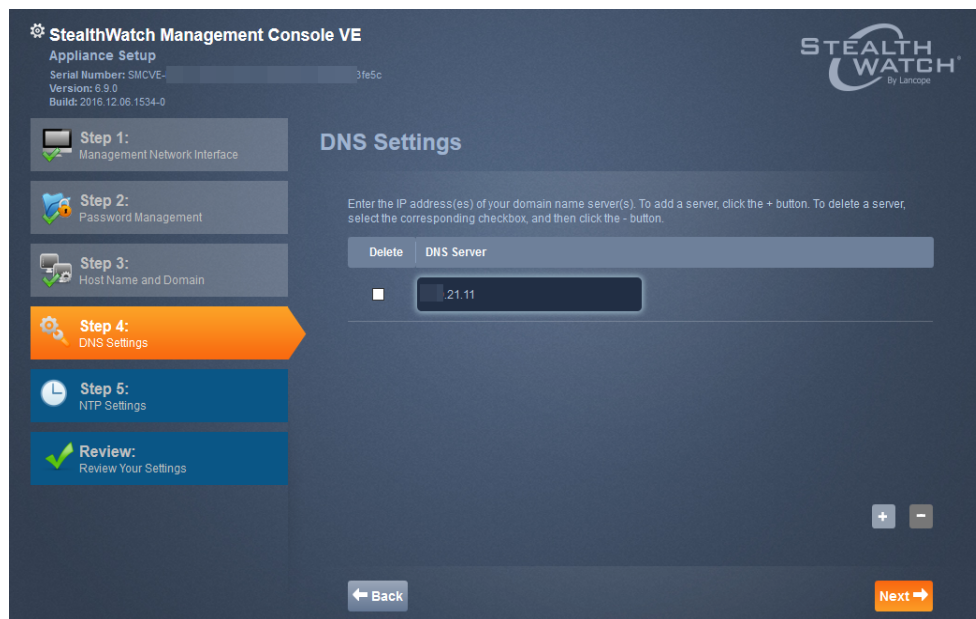
[管理ネットワーク インターフェイス(Management Network Interface)] ページが開きます。



6. 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。

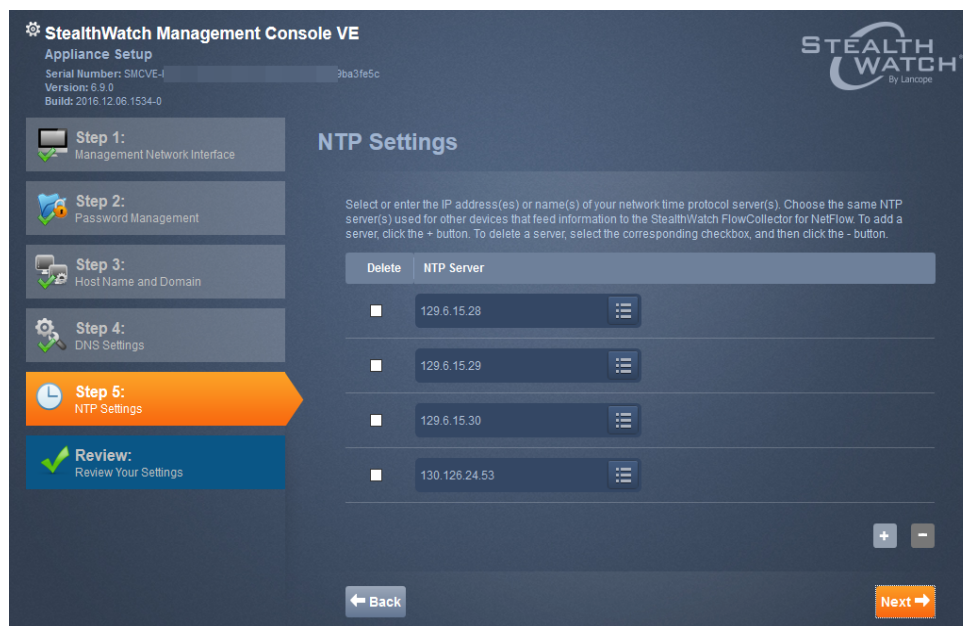
7. 適切なフィールドに新しい管理者パスワードを入力して、[次へ (Next)] をクリックします。[ホスト名とドメイン (Host Name and Domain)] ページが開きます。

8. 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。

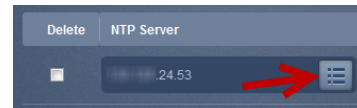


9. [+] ボタンをクリックして、DNS サーバの IP アドレスを入力します。[次へ (Next)] をクリックします。[NTP 設定 (NTP Settings)] ページが開きます。

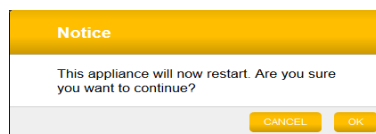
(注) 1 つ目の NTP サーバを pool.ntp.org に設定してください。これによって、Stealthwatch アプライアンスは NTP サーバのランダムな ntp.org プールにアクセスしてアプライアンスの時間を設定できるようになります。



10. 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
11. [次へ (Next)] をクリックします。[レビュー (Review)] ページが開きます。



12. 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。



13. 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。
14. 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。
15. 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 VE を最後に設定することに注意してください。
 - 「いいえ」の場合、次の手順に進みます。

16. 最後または SMC VE のみを設定した後、次の項「[システムの設定](#)」に進みます。

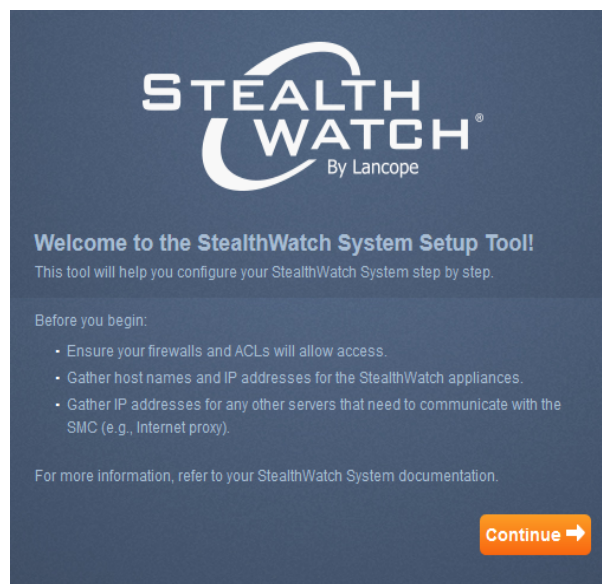
システムの設定

SMC (VE) を含むすべてのアプライアンスの設定を終了したら、システムを設定できます。

注意! SMC の管理対象のすべてのアプライアンスを有効化する必要があります。そうしないと、SMC VE はフローコレクタと通信できず、システムを適切に設定することができません。

重要: フェールオーバー SMC を設定する場合、システムのドメイン名のみを指定し、残りのページで [次へ (Next)] をクリックする必要があります。プライマリ SMC に対し設定するときに、システムを設定できます。

システム設定ツールの [ようこそ (Welcome)] ページが開きます。



1. [続行 (Continue)] をクリックします。[エンタープライズドメイン情報の追加 (Add Enterprise Domain Information)] ページが開きます。



2. システムの IP アドレスの範囲 (CIDR、ダッシュで結んだ範囲、末尾にドットのサブネット、IPv6 を使用できます) を入力するか、IP アドレスの範囲の CSV ファイルをインポートする一括アップロードを実行して、[次へ (Next)] をクリックします。[アプライアンス (Appliance)] ページが開きます。

(注) CSV ファイルの IP アドレスは、カンマ、カンマとスペース、スペース、改行のいずれかで区切る必要があります。



3. [+] ボタンをクリックします。[フローコレクタの追加 (Add Flow Collector)] ダイアログが開きます。



4. フローコレクタの IP アドレスを入力し、[次へ (Next)] をクリックします。[通信 (Communication)] ダイアログが開きます。

Communication Established
X

Review the information below, and click 'Add' to finalize the process.

IP Address	Model
22.32	FCNFVE
Host Name	Version
gs- -fc1	6.9.0

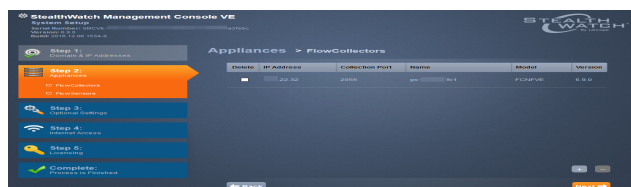
FlowCollection Port
Receives data on this port

2055

BACK
ADD

条件付き手順: この手順でフローコレクタまたはフローセンサーを追加する場合、まずフローコレクタまたはフローセンサーと Stealthwatch Management Console(SMC) 間の管理チャネルを作成しておく必要があります。作成されていない場合、手順のこの時点でエラーメッセージが表示されます。フローコレクターおよびフローセンサーそれぞれに対して管理チャネルを作成するには、次の手順を実行します。

1. ブラウザーとアプライアンスの IP アドレスを使用して、該当するアプライアンス管理インターフェイスにログインします。
 2. 左側のナビゲーションペインで **[設定 (Configuration)] > [管理システム設定 (Management Systems Configuration)]** の順にクリックします。
 3. **[新しい管理システムの追加 (Add New Management System)]** をクリックします。
 4. **[管理システムの IP アドレス(Management System IP Address)]** フィールドに、SMC の IP アドレスを入力します。
 5. **[SMC(Is SMC)]** チェックボックスをオンにします。
 6. **[適用 (Apply)]** をクリックします。
 7. **[システムセットアップツール(System Setup Tool)]** のエラーダイアログで **[キャンセル (Cancel)]** をクリックし、**[適用 (Apply)]** をクリックします。
5. **[追加 (Add)]** をクリックします。フローコレクタ(VE) がシステムに追加されます。



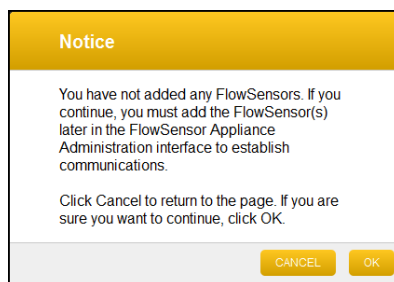
6. **[次へ (Next)]** をクリックします。 **[アプライアンスフローセンサー(Appliance Flow Sensors)]** ページが開きます。



7. 追加するフロー センサーがありますか。

- 「はい」の場合、[+] ボタンをクリックし、手順 9 に進みます。
- 「いいえ」の場合、[次へ (Next)] をクリックし、次の手順に進みます。

8. 警告メッセージが表示されます。[OK] をクリック手順 14 に進みます。



9. [+] ボタンをクリックします。[フロー センサーの追加 (Add Flow Sensor)] ダイアログが表示されます。

10. IP アドレスを入力し、[OK] をクリックします。[確立された通信 (Communication Established)] ダイアログが表示されます。

11. ドロップダウン リストからフロー コレクタを選択し、[追加 (Add)] をクリックします。[フロー センサー VE ログイン クレデンシヤル (Flow Sensor VE Login Credentials)] ダイアログが開きます。

12. 適切なフィールドに、フロー センサー VE がフロー コレクタと通信するのに必要な次の情報を入力します。

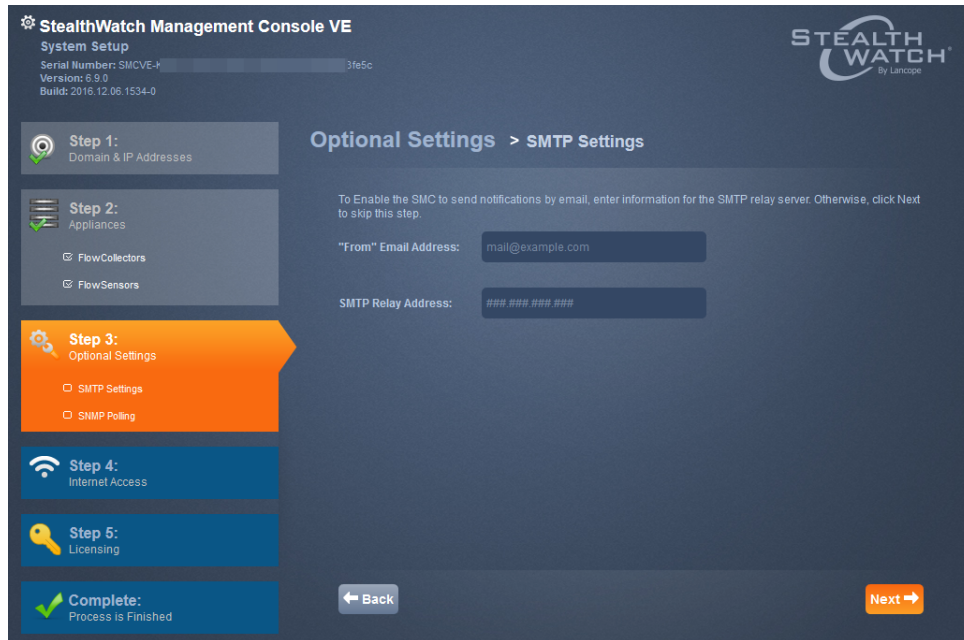
- VM サーバアドレス
- フローセンサーのユーザ名
- パスワード

13. [追加 (Add)] をクリックします。

フローセンサーが追加されます。



14. [次へ (Next)] をクリックします。[SMTP 設定 (SMTP Setting)] ページが開きます。



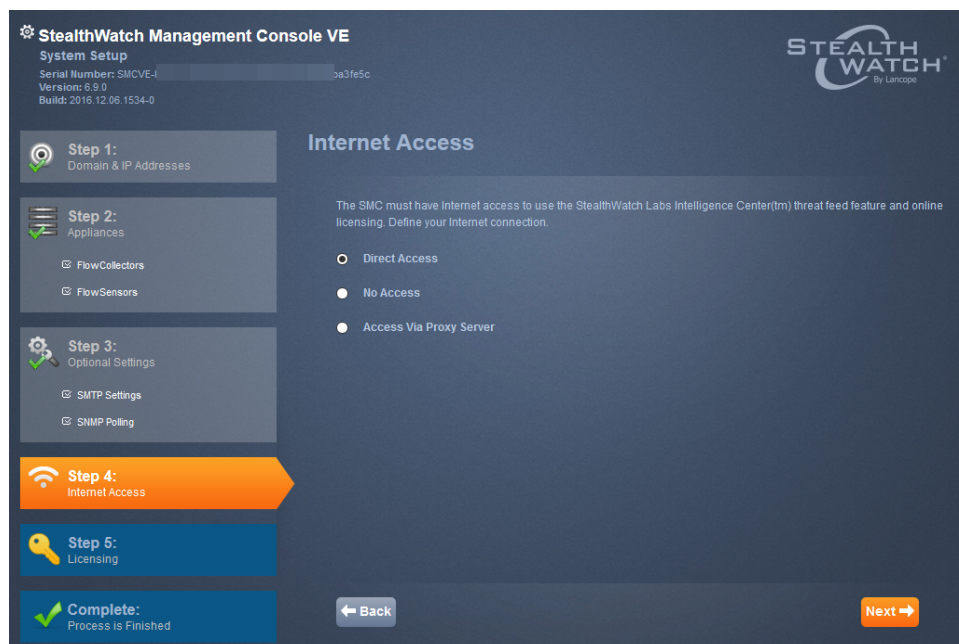
15. SMC が電子メールを送信するときの、[差出人 (from)] フィールドに指定する電子メールアドレスを入力します。
16. SMTP リレー アドレスを入力し、[次へ (Next)] をクリックします。[SNMP 設定 (SNMP Setting)] ページが開きます。



17. 必要に応じて、設定を変更(ここでは1つの文字列のみ設定できます)してから、[次へ (Next)] をクリックします。

(注) [SNMPバージョン3(SNMP Version 3)]を選択した場合、ユーザ名を入力する必要があります。さらにオプションとして認証と暗号化を選択できます。

18. [インターネット アクセス(Internet Access)](SMC 用) ページが開きます。

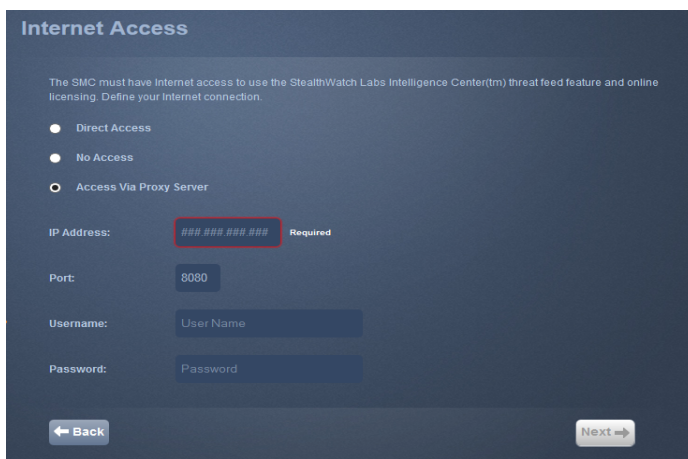


19. インターネット アクセスの適切なタイプを選択します。

- [直接アクセス(Direct access)]: SMC がインターネットに直接接続されます(プロキシサーバを経由しない)。[次へ(Next)] をクリックして、[オンライン(Online)] ページを開きます。
- [アクセスなし(No access)]: SMC はインターネットに接続されません。ダウンロードとライセンスセンターからライセンスを取得するためのアクセス権を取得する必要があります。[オフライン(Offline)] ページの[次へ(Next)] をクリックして、[完了(Complete)] ページを開きます。



- [プロキシ サーバ経由でアクセス(Access via Proxy Server)]: SMC はプロキシ サーバ経由でインターネットに接続されます。プロキシ設定が表示されます。



プロキシ サーバの設定を実行してから、[次へ(Next)] をクリックします。

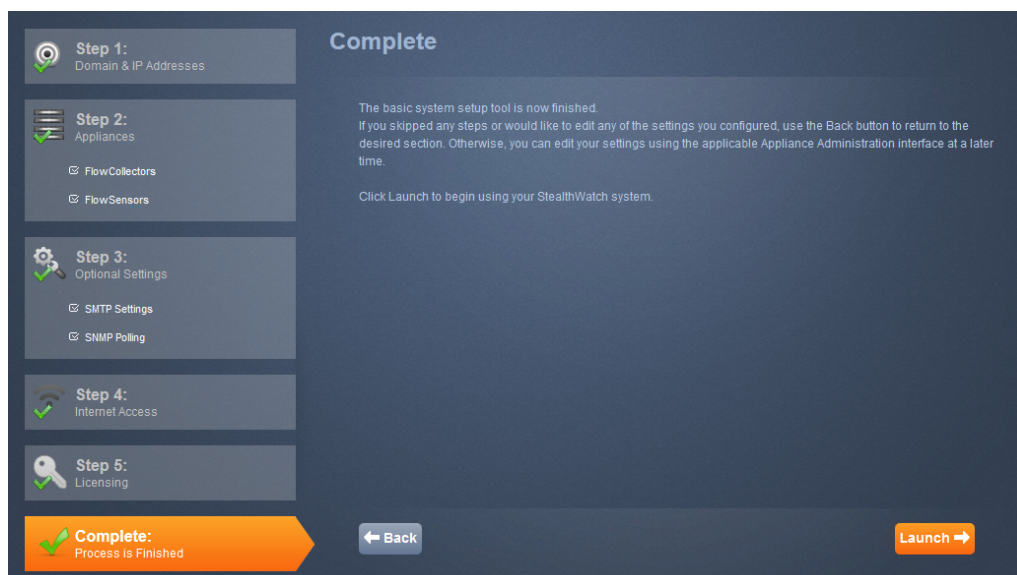
20. [直接アクセス(Direct Access)] を選択するか、またはプロキシ設定を完了したら、[ライセンス(Licensing)] ページが開きます。



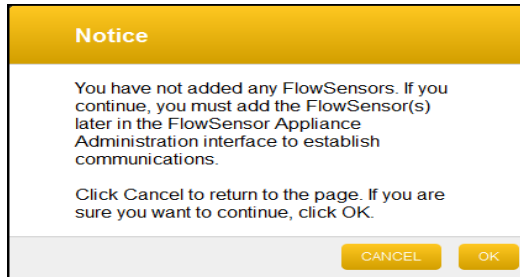
21. [ダウンロード およびライセンス センター(Download and License Center)] リンクをクリックし
ず。『*Downloading and Licensing Stealthwatch Products*』ドキュメントの説明に従って、ラ
イセンスを取得します。
22. ライセンスを取得した後、[有効化 (Activate)] をクリックします。

(注) アプライアンスが登録されていない場合、メッセージが表示されます。

23. [OK] をクリックします。[完了 (Complete)] ページが開きます。



24. SMC クライアントのランディングページにアクセスするには、[起動(Launch)] をクリックします。メッセージが開きます。アプライアンスのライセンスがない場合、どのライセンスがないのかについての情報を含むメッセージが表示されます。メッセージの例を以下に示します。



25. 右上隅の[ようこそ管理ユーザ(Welcome Admin User)] ドロップダウンリストから、[アプライアンスの管理(Administer Appliance)] をクリックして、アプライアンス管理インターフェイスを開き、次のセクションの「アプライアンス管理インターフェイスによる設定」、ページ 62 に進みます。
26. 外部イベントを収集する SMC VE(syslog) またはフローコレクタ VE を設定していますか。
- 「はい」の場合、次の項「SMC VE またはフローコレクタ VE のディスク容量の拡張」に進みます。
 - 「いいえ」の場合、「アプライアンス管理インターフェイスによる設定」、ページ 62 に進みます。

SMC VE またはフローコレクタ VE のディスク容量の拡張

この項では、SMC VE またはフローコレクタ VE のディスク容量を拡張する手順を示します。

(注)

- 外部イベント(syslog) を収集しなければ、SMC VE のディスク容量を拡張する必要はありません。
- ディスクのスナップショットを使用している場合、SMC VE またはフローコレクタ VE のディスク容量を拡張することはできません。スナップショットを最初に削除する必要があります。

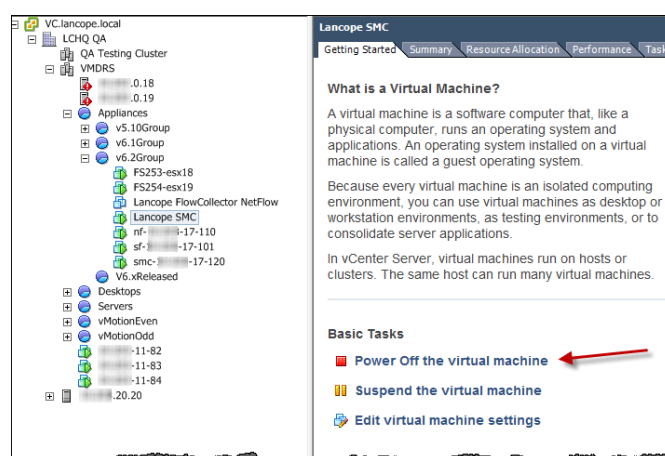
SMC VE はディスクの約 75% を使用し、25% を空けておきます。したがって、必要なディスク容量より、常に 40% 多くディスクを拡張します。

フローコレクタ VE の最大データストレージはモデルによって異なります。最大容量は次のとおりです。

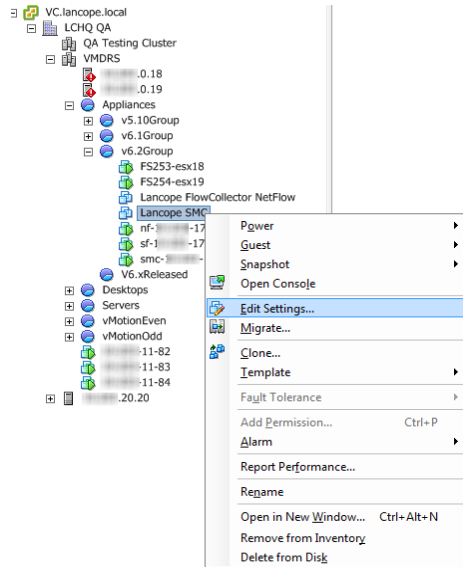
モデル	最大ディスクストレージ
フロー コレクタ VE 1000	1 TB
フロー コレクタ VE 2000	2 TB
フロー コレクタ VE 4000	4 TB

仮想アプライアンスのディスク容量を拡張するには、次の手順を実行します。

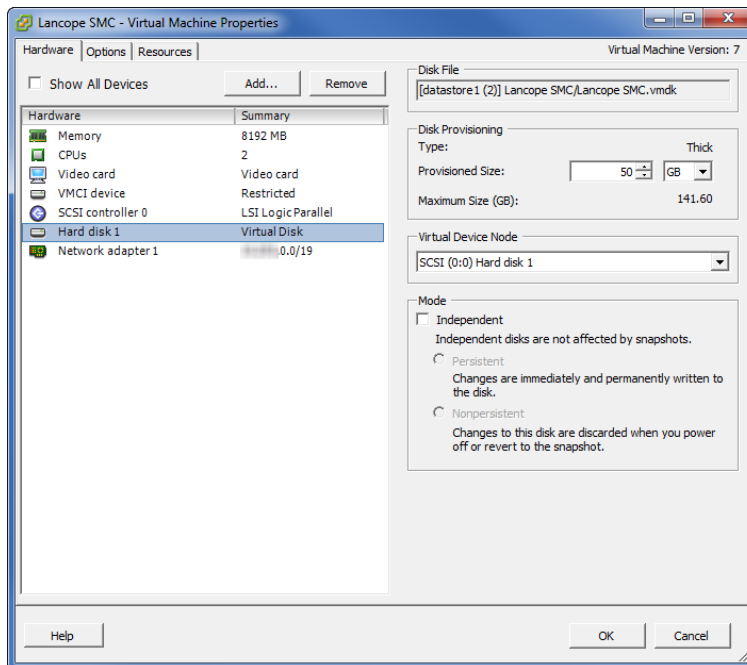
1. インベントリツリーで、仮想アプライアンスを選択し、[仮想マシンをオフにする(Power Off the virtual machine)] をクリックします。



2. インベントリツリーで、インベントリツリーの仮想アプライアンスを右クリックし、[設定の編集 (Edit Settings)] を選択します。

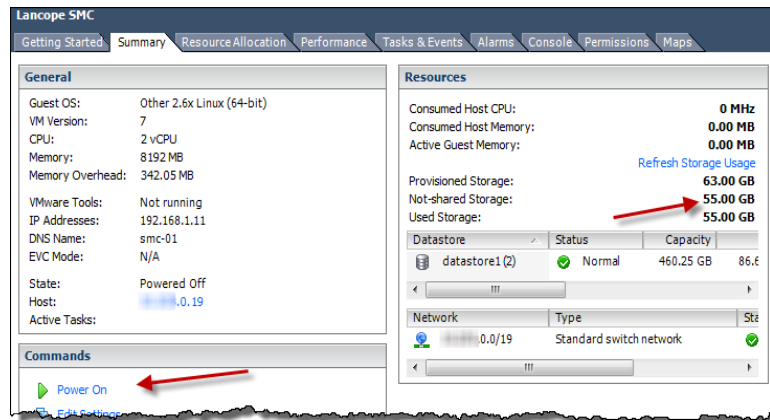


[仮想マシンのプロパティ (Virtual Machine Properties)] ダイアログが開きます。



3. [ハードウェア (Hardware)] リストで [ハード ディスク (Hard disk)] を選択します。Web クライアントで、ハード ディスク 1 のリストを展開します。ディスク情報が右側に表示されます。
4. [ディスクプロビジョニング (Disk Provisioning)] セクションの、[プロビジョニングサイズ (Provisioned Size)] フィールドに適切なディスク容量を入力し、[OK] をクリックします。ダイアログが閉じます。

5. ストレージ容量が変更されたことを確認するには、[サマリー(Summary)] タブをクリックします。



6. [電源オン(Power On)] をクリックします。
7. [コンソール(Console)] タブをクリックします(Web クライアントでは、[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。ログインページが開きます。

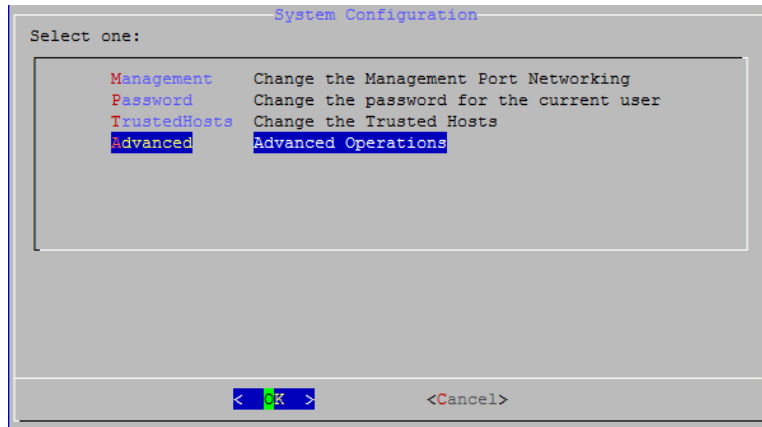
```

Loading, please wait...
[ 1.550619] sd 0:0:0:0: [sdal] Assuming drive cache: write through
[ 1.550937] sd 0:0:0:0: [sdal] Assuming drive cache: write through
[ 1.564200] sd 0:0:0:0: [sdal] Assuming drive cache: write through
INIT: version 2.80 booting
[ 2.091343] ACPI: I/O resource piix4_smbus [0x1040-0x1047] conflicts with ACP
I region SMB_ [0x1040-0x104b]
INIT: Entering runlevel: 2

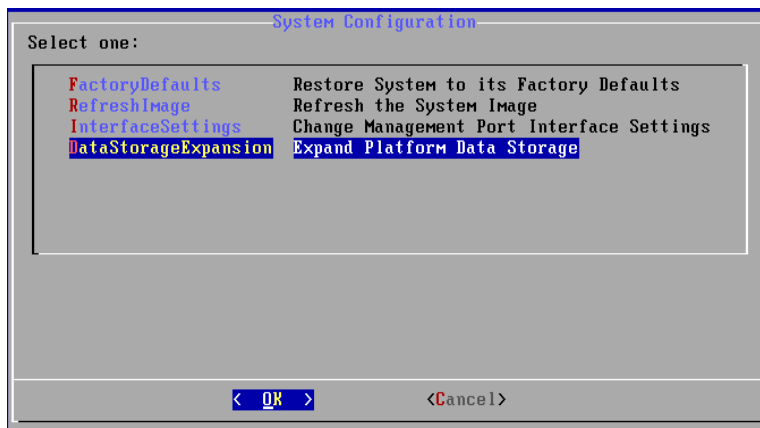
Welcome to StealthWatch SMC Version 6.5.0
smc-01 login:

Welcome to StealthWatch SMC Version 6.5.0
smc-01 login: sysadmin_
    
```

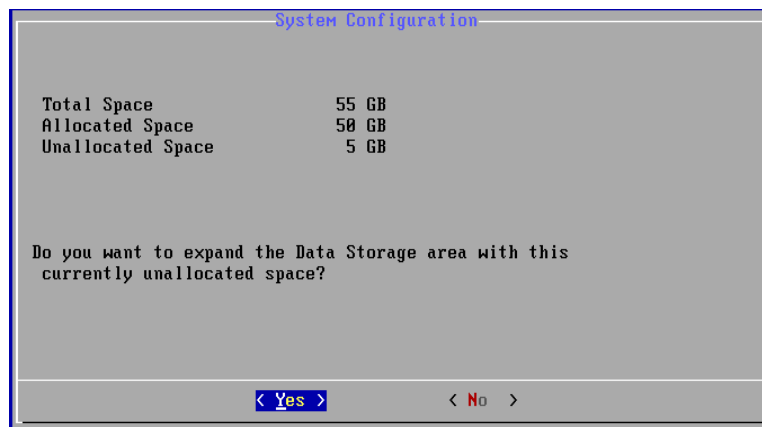
8. ページをクリックし、次のようにしてください。
 - a. 「sysadmin」と入力して、Enter を押します。
 - b. パスワード プロンプトが表示されたら、lan1cope と入力して Enter を押します。
 [システム設定 (System Configuration)] メニューが開きます。



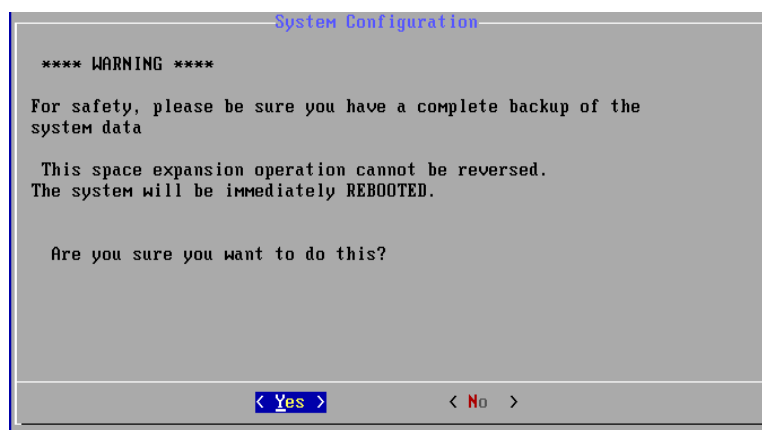
9. [詳細 (Advanced)] オプションを選択し、Enter を押します。[詳細 (Advanced)] メニューページが開きます。



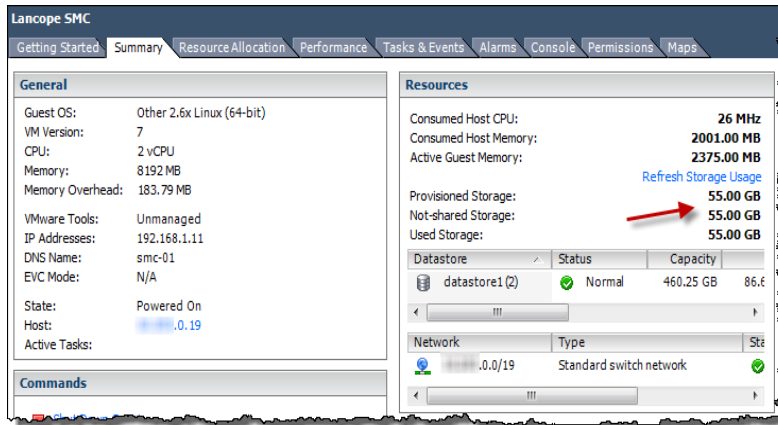
10. [データストレージの拡張 (DataStorageExpansion)] オプションを選択します。[データストレージの拡張 (Data Storage Expansion)] ページが開きます。



11. 情報を確認して [はい(Yes)] を選択し、Enter を押します。[警告(Warning)] ページが開きます。



12. [はい(Yes)] を選択して、Enter を押します。仮想アプライアンスを再起動して変更を実装します。
13. Ctrl + Alt を押して、コンソール環境を終了します。
14. [概要(Summary)] タブをクリックして、データストレージへの変更を確認します。



15. 次の項「フローコレクタ VE のメモリの増加」に進みます。

フローコレクタ VE のメモリの増加

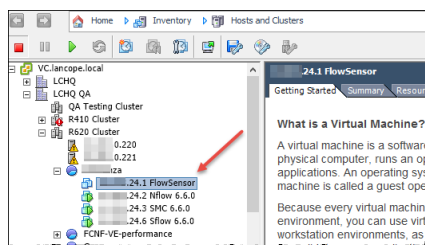
フローコレクタ VE では、パフォーマンスが適切なレベルにあるように、メモリを増加する必要があります。

フローコレクタ VE の最大メモリはモデルによって異なります。最大容量は次のとおりです。

モデル	最大メモリ
フローコレクタ VE 1000	32 GB
フローコレクタ VE 2000	64 GB
フローコレクタ VE 4000	128 GB

メモリのレベルを上げるには、次の手順を実行します。

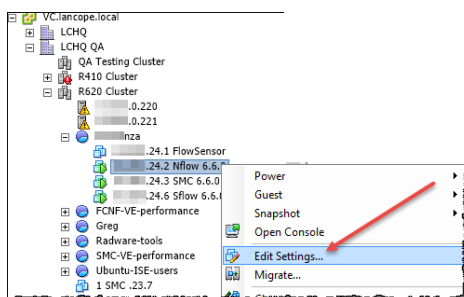
1. アプライアンスを選択します。



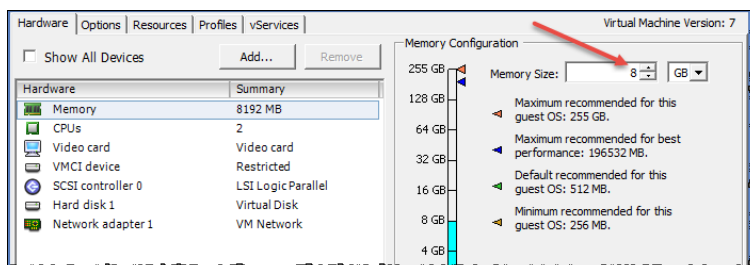
2. 必要に応じて、アプライアンスをオフにします。



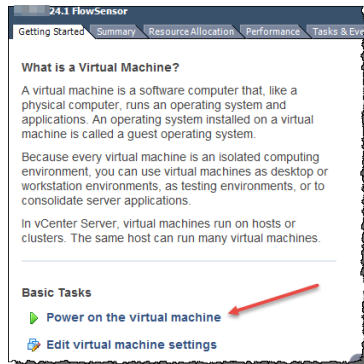
3. 右クリックして [設定の編集 (Edit Settings)] を選択します。



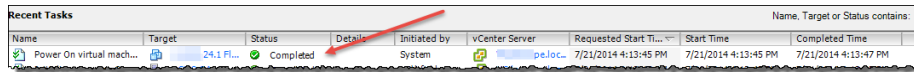
4. [ハードウェア (Hardware)] タブで、[メモリ (Memory)] を選択し (クリックすると [メモリ (Memory)] が開きます)、8 GB にメモリサイズを増加します。



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. 「アプライアンス管理インターフェイスによる設定」の項に進みます。

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。

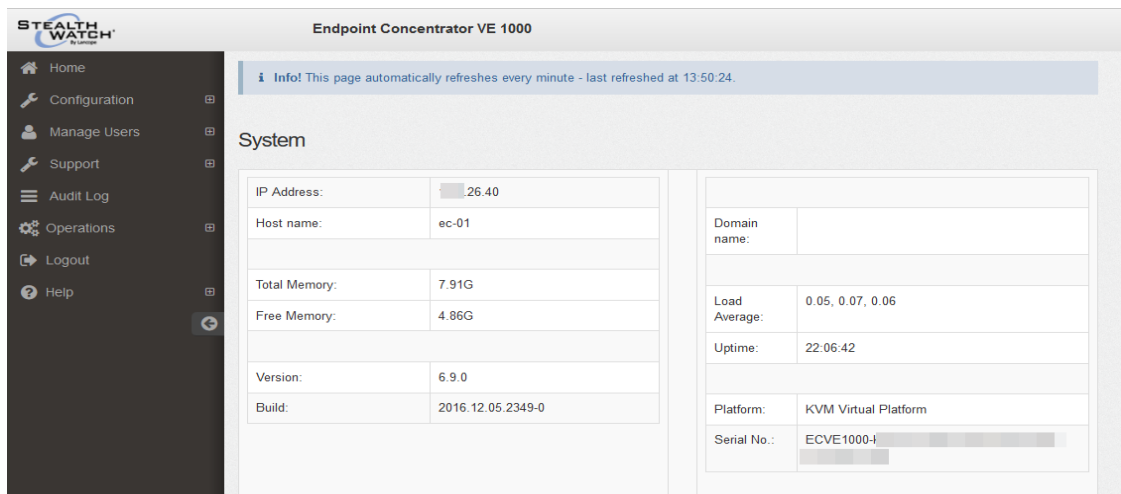
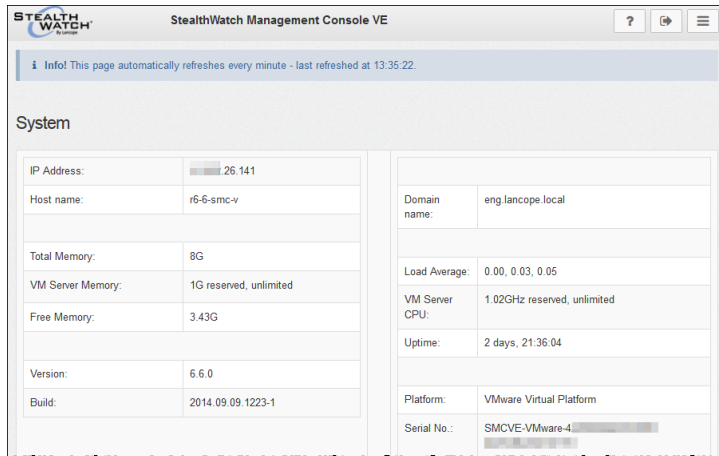
- 「はい」の場合、[ランディング(Landing)] ページが開きます。右上隅の[設定 (Settings)] アイコンをクリックして、[アプライアンスの管理 (Administer Appliance)] をクリックします。



- 「いいえ」の場合、仮想アプライアンスの[ログイン(Login)] ページが開きます。



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。



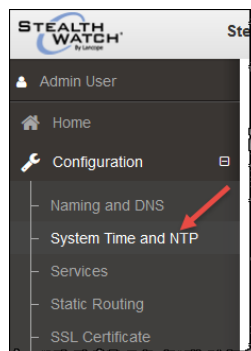
6. 次の項「システム時刻の設定」に進みます。

システム時刻の設定

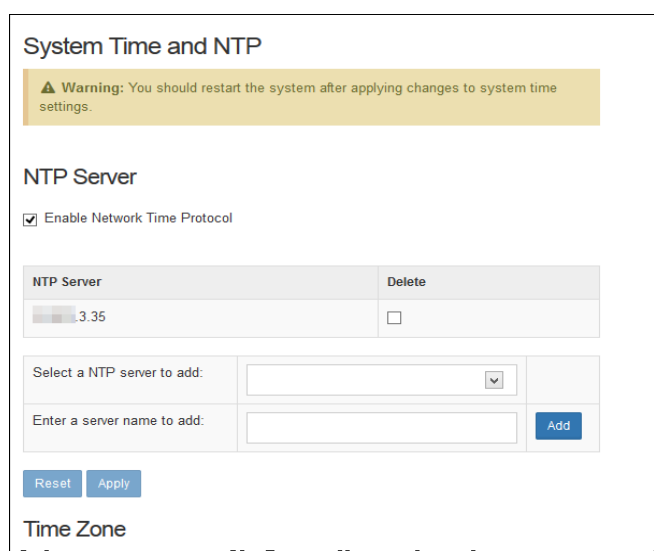
Network Time Protocol(NTP) およびシステム時刻(タイムゾーン)設定を仮想アプライアンスで設定するには、次の手順を実行します。

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。

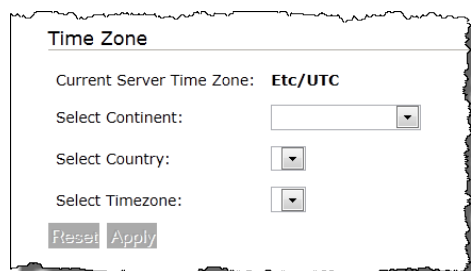
1. アプライアンス管理インターフェイスのナビゲーションページで、[構成(Configuration)]の横のプラス記号(+)をクリックして、[システム時刻とNTP(System Time and NTP)]をクリックします。



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。



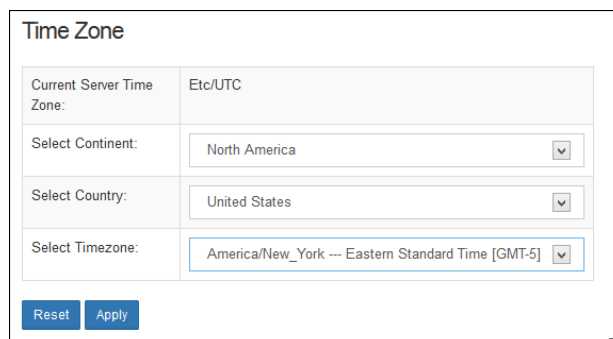
2. ページの [タイムゾーン(Time Zone)] セクションまで下にスクロールして、仮想アプライアンスシステム時刻を設定します。



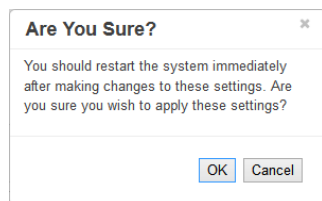
3. 次の手順を実行します。

- 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。

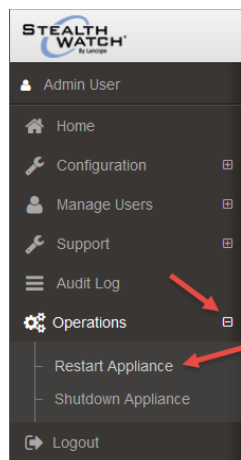


5. [OK] をクリックします。
6. 次の項「[仮想アプライアンスの再起動](#)」に進みます。

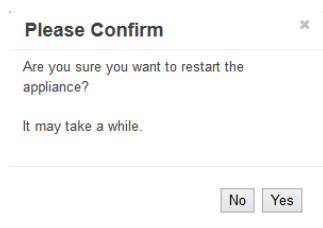
仮想アプライアンスの再起動

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。

9. SMC VE またはフローコレクタ VE を設定しましたか。

- SMC VE を設定している場合、再起動の後に、フローコレクタと通信を開始します。仮想アプライアンスのインストールと設定が完了しました。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。
- フローコレクタ VE を設定している場合、次の章「[通信の確認](#)」に進みます。

通信の確認

概要

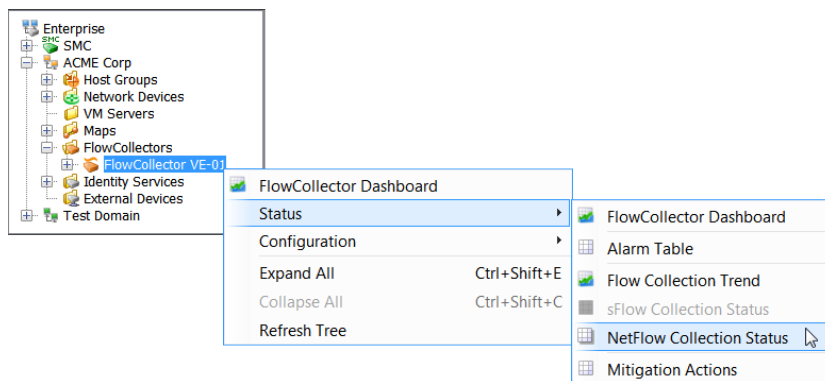
StealthWatch アプライアンスのライセンス供与後、NetFlow データを受信していることを確認する必要があります。確認するには、この章で説明している次の手順を実行します。

注意! この項の手順を開始する前に、各アプライアンスに対し前の項のライセンス手順をすべて完了した後、30分待ちます。

NetFlow データ収集の確認

SMC へフローコレクタを追加すると、フローコレクタは SMC にフロー情報を伝え、さまざまな文書を介してユーザフレンドリーな方法でこの情報を表示します。NetFlow データを本当に収集していることを確認するには、次の手順を実行します。

1. エンタープライズツリーで、フローコレクタを右クリックし、
[ステータス(Status)] > [NetFlow コレクション ステータス(NetFlow Collection Status)] の順
に選択します。



NetFlow コレクションのステータスに関するドキュメントが開きます。

The screenshot shows the 'NetFlow Collection Status' window. The 'Summary' section includes a table with the following data:

Interface Count	Current NetFlow Traffic (bps)	Average NetFlow Traffic (bps)	Maximum NetFlow Traffic (bps)
FlowCollector-Primary: 28	259.47k	264.87k	293.12k

The 'Details - 17 records' section includes a table with the following data:

Status	Exporter	Longest Duration Export (seconds)	Exporter Type	Average Flow Rate (fps)	Average NetFlow Traffic (bps)	Interface Count
✓	core01 (.0.1)	71	Exporter	159	58.86k	7
✓	.0.43	67	Exporter	92	128.94k	3
✓	.200.2	60	Exporter	74	31.62k	3
✓	asa01 (.200.1)	60	Cisco ASA	49	40.95k	3
✓	.0.241	60	Exporter	2	2.67k	9

2. ドキュメントの上部にある [現在の NetFlow トラフィック(Current NetFlow Traffic)] フィールドを参照してください。この統計情報は検出された NetFlow トラフィックの量を示します。フローのトラフィックが表示されていますか。
 - 正しい場合、次の手順に進みます。
 - 「いいえ」の場合、エクスポートおよびルータの設定を確認します。(詳細は、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。) 次の手順に進みます。
3. [最も長い継続時間のエクスポート(Longest Duration Export)] 列を参照してください。列ヘッダーを右クリックし、ポップアップメニューから、[最も長い継続時間のエクスポート(Longest Duration Export)] を選択して、この列を追加する必要がある場合があります。各エクスポートの値は 100 よりも下ですか。
 - 「はい」の場合、キャッシュのエクスポート タイマーは正常です。
 - 「いいえ」の場合、高い値はキャッシュのエクスポート タイマーが正しくないことを示し、誤ったアラームが発生する可能性があります。エクスポートおよびルータの設定を確認します。(詳細は、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。)
4. アイデンティティ デバイスがありますか。
 - 「はい」の場合、次の章「Cisco ISE の追加」に進みます。
 - 「いいえ」の場合、次の手順に進みます。
5. SLIC 機能はありますか。
 - 「はい」の場合、「SLIC 脅威フィード機能の有効化」の章に進みます。
 - 「いいえ」の場合、アプライアンスの設定は完了です。

Cisco ISE の追加

概要

アイデンティティデバイスがあれば、それらを SMC に追加できます。この章には、Cisco ISE (Identity Services Engine) を追加する手順が含まれます。

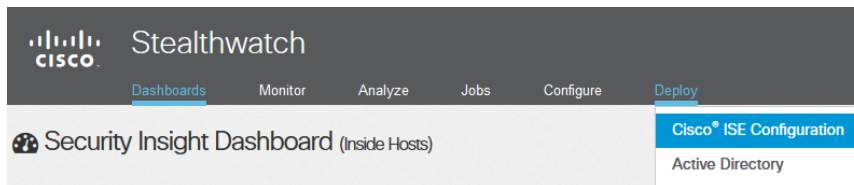
Cisco ISE の追加

(注)

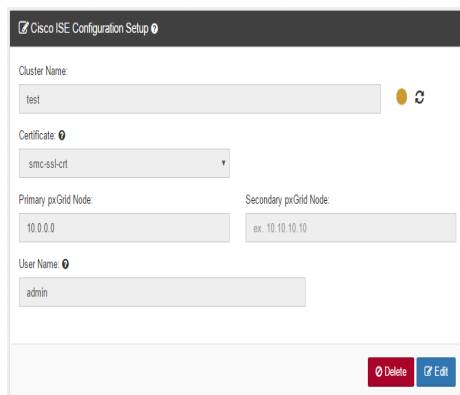
- 複数の独立した Cisco ISE クラスタをドメインに追加できます。
- StealthWatch システムに Cisco ISE-PIC を追加する手順は、ここで説明しているものと同じです。Cisco ISE-PIC の設定の詳細については、Cisco ISE のマニュアルを参照してください。

Cisco ISE を追加するには、次の手順を実行します。

1. SMC Web App インターフェイスのメニューで [展開 (Deploy)] > [Cisco ISE の設定 (Cisco ISE Configuration)] の順に選択します。



[Cisco ISE の追加 (Add Cisco ISE)] ダイアログが開きます。



2. Cisco ISE クラスタの名前を入力します。使用される StealthWatch システムの各ドメインの Cisco ISE クラスタを設定する必要があります。
3. 該当する証明書を選択します。これはアプライアンスがクライアントとして ID を認証できる (つまり SMC が ISE に提供するクライアント証明書)、アプライアンス管理 (Admin) インターフェイスの [SSL 証明書 (SSL Certificate)] ページの [フレンドリ名 (Friendly Name)] フィールド ([アイデンティティのアップロード (Upload an Identity)] セクション内) に入力したのと同じ名前です。
4. アプライアンスを統合する ISE クラスタのプライマリ pxGrid ノードの IP アドレスを入力します。
5. (オプション) アプライアンスを統合する ISE クラスタのセカンダリ pxGrid ノードの IP アドレスを入力します。このノードは、フェールオーバーのために使用されます。プライマリノードへの接続が失敗すると、セカンダリノードが使用されます。
6. Cisco ISE デバイスのユーザアカウント用に設定したユーザ名を入力します。この名前は ISE アプライアンスの ISE クラスタの pxGrid クライアント リストに表示されます。
7. [追加 (Add)] > [OK] の順にクリックします。Cisco ISE が Identity Services フォルダのドメインに追加されます。
8. SLIC 機能はありますか。
 - 「はい」の場合、次の章「[SLIC 脅威フィード機能の有効化](#)」に進みます。
 - 「いいえ」の場合、アプライアンスの設定は完了です。

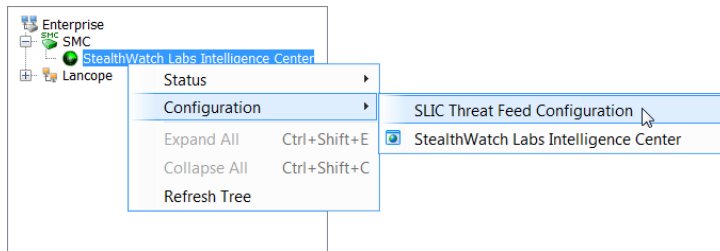
6

SLIC 脅威フィード機能の有効化

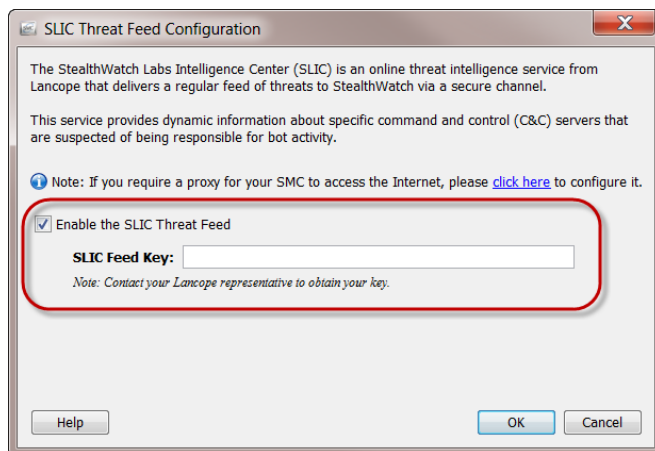
StealthWatch パッケージのインストールと設定の最後の手順は、SMC のクライアント インターフェイスを使用して SLIC 脅威フィードを有効にすることです。

次の手順を実行します。

1. エンタープライズ ツリーで、[Stealthwatch ラボ インテリジェンス センター(Stealthwatch Labs Intelligence Center)] ブランチを右クリックし、[設定 (Configuration)] > [SLIC 脅威フィード 設定 (SLIC Threat Feed Configuration)] の順に選択します。



[SLIC 脅威フィード 設定 (SLIC Threat Feed Configuration)] ダイアログが表示されます。



2. [SLIC 脅威フィードを有効にする(Enable the SLIC Threat Feed)] チェックボックスを選択します。
3. [SLIC フィード キー(SLIC Feed Key)] フィールドにキーを入力します。
4. [OK] をクリックします。10 分以内に、エンタープライズ ツリーは、コマンド & コントロールサーバ(C&C) ホスト グループのブランチを更新して、識別済みのアクティブな C&C サーバのリストを表示します。

おめでとうございます。これで、StealthWatch システムの多くのセキュリティとネットワークのモニタリングの利点を活用できるようになります。詳細については、『*Stealthwatch Management Console User's Guide*』または SMC クライアント インターフェイス オンライン ヘルプを参照してください。[ヘルプ(Help)] をクリックします。

