Stealthwatch® 管理コンソール (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 v6.10.1 の場合)

目次

目次 ii

仮想アプライアンスのインストール iv

概要 iv

プロセスの概要 iv

通信用ファイアウォールの設定 v

通信ポート v

VMware vSphere Client を使用した仮想アプライアンスのインストールの ix

概要 ix

はじめる前に ix

プロセスの概要 ix

VMware vSphere クライアントへのログイン x

仮想アプライアンスのインストール x

KVM ホストへの仮想アプライアンスのインストール xix

概要 xix

はじめる前に xix

プロセスの概要 xix

KVM ホストへの仮想アプライアンスのインストール xx

仮想環境の設定 xxvi

概要 xxvi

IP アドレスの設定 xxvi

デフォルトユーザ パスワードの変更 xxx

sysadmin パスワードの変更 xxx

ルートパスワードの変更 xxxii

システムの設定 xxxvi

概要 xxxvi

© 2019 Cisco Systems, Inc. All Rights Reserved.

プロセスの概要 xxxvi
個々のアプライアンスの設定 xxxvi
システムの設定 xlii
データストレージおよびリソースの割り当ての拡張 liii
アプライアンス管理インターフェイスを使用した設定 lvi
アプライアンス管理インターフェイスへのログイン lvi
システム時刻の設定 lviii
仮想アプライアンスの再起動 lx
通信の確認 lxii
概要 lxii
NetFlow データ収集の確認 lxii
Cisco ISE の追加 lxiv
概要 lxiv
Cisco ISE の追加 lxiv
SLIC 脅威フィード機能の有効化 lxvi

© 2019 Cisco Systems, Inc. All Rights Reserved.

3

仮想アプライアンスのインストール

概要

この章では、仮想アプライアンスをインストールする方法について説明します。

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。

互換性：バーチャルエディションのインストールには次のいずれかを使用できます。互換性の詳細については、「はじめに」の「互換性」の項を参照してください。

- **VMware vSphere Client v6.x 以降**
- **任意の Linux ディストリビューションを使用した KVM**

Note: 仮想アプライアンスをインストールする仮想ホストサーバに設定された時刻が正しい時刻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。

CAUTION! 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 または KVM を使用した仮想アプライアンスのインストール

先に Flow Collector 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

通信用ファイアウォールの設定

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

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
Active Directory	SMC	TCP/389、UDP/389	LDAP

© 2019 Cisco Systems, Inc. All Rights Reserved.

送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
AnyConnect	Endpoint Con-centrator	UDP/2055	NetFlow
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	TCP/5222	XMPP
Endpoint Con-centrator	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

© 2019 Cisco Systems, Inc. All Rights Reserved.

送信元(クライアント)	宛先(サーバ)	ポート	プロトコル
SMC	Flow Collector	TCP/443	HTTPS
SMC	Flow Sensor	TCP/443	HTTPS
SMC	アイデンティティ	TCP/2393	SSL
SMC	Flow エクスポータ	UDP/161	SNMP
SMC	Endpoint Con-centrator	UDP.2055	HTTPS
ユーザ PC	SMC	TCP/443	HTTPS

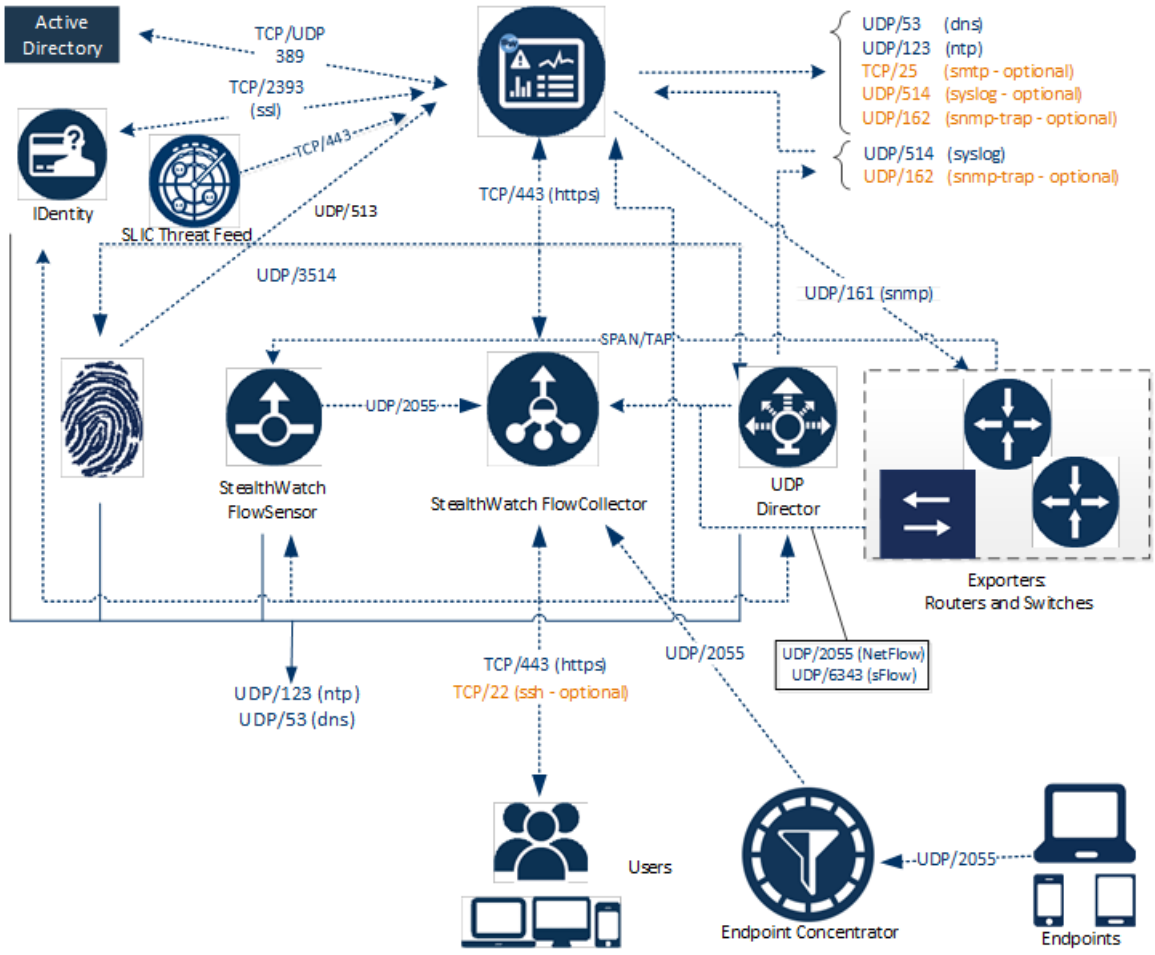
* これはデフォルトの NetFlow ポートですが、任意の UDP ポートをエクスポータで設定できます。

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 System 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



Note: VMware vSphere Client または KVM のうち、使用している仮想アプライアンスのインストール環境に対応するセクションに進みます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

VMWARE VSPHERE CLIENT を使用した仮想アプライアンスのインストールの

概要

この章では、**VMware vSphere Client v6**を使用して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。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. ダウンロードおよびライセンスセンターからOVF ファイルをダウンロードします。手順については、『*Downloading and Licensing Guide*』を参照してください。
2. 「概要」の互換性情報を確認します。
3. 通信のファイアウォールを設定します。
4. 「リソース要件」の項を確認し、アプライアンスの適切な割り当てを決定します。リソースプールまたは代替方法を使用してリソースを割り当てます。
5. 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刻が正しい時刻を示していることを確認します。正しくなければ、仮想アプライアンスを起動できない場合があります。

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

CAUTION! 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する必要があります。

1. VMware vSphere クライアントへのログイン
2. 仮想アプライアンスのインストール

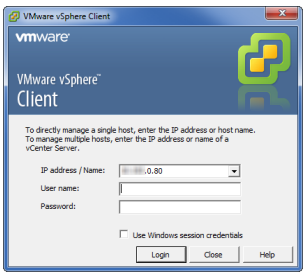
© 2019 Cisco Systems, Inc. All Rights Reserved.

VMware vSphere クライアントへのログイン

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 v6 以降 にログインする必要があります。

Note: VMware vSphere クライアントを使用しているか、または Web クライアントインターフェイスを使用しているかで、グラフィックやコマンドの一部がここに示した情報とは異なる場合があります。ソフトウェア関連の詳細については、使用している VMware vSphere のガイドを参照してください。

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ます。
3. [ログイン(Login)] をクリックします。ホーム ページが開きます。

Note: 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。

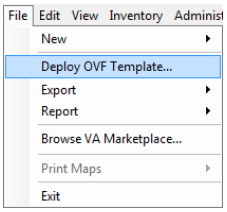
仮想アプライアンスのインストール

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。

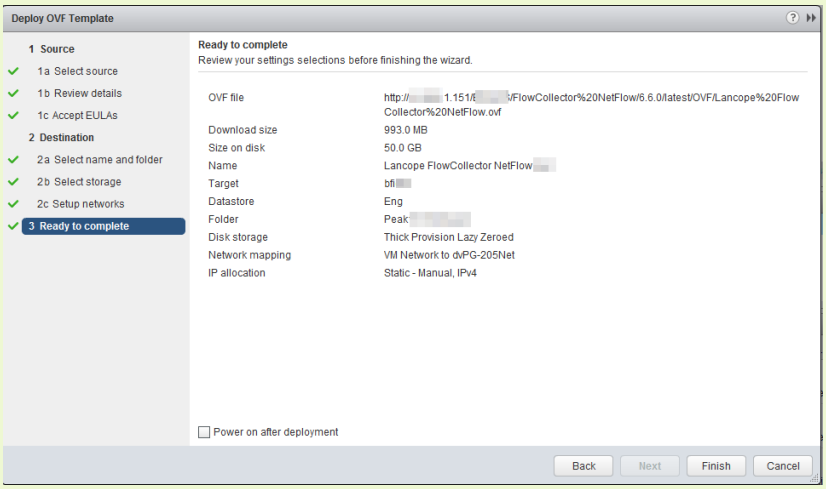
1. ダウンロードおよびライセンス センターからダウンロードした仮想アプライアンス ソフトウェア ファイル(OVF.TGZ) を見つけます。
2. ファイルを解凍するか開いてから、展開します。
   - ファイルを展開するには、フォルダ内のファイルをすべて開き、それらを抽出します。
   - TGZ ファイルの解凍は 2 段階のプロセスで、使用しているソフトウェアによって手順が異なる場合があります。
3. vSphere Client メニューで、[ファイル(File)] > [OVF テンプレートの展開(Deploy OVF Template)] をクリックします。

© 2019 Cisco Systems, Inc. All Rights Reserved.

Web クライアント: ホストを右クリックします。[OVF テンプレートの展開 (Deploy OVF Template)] を選択します。

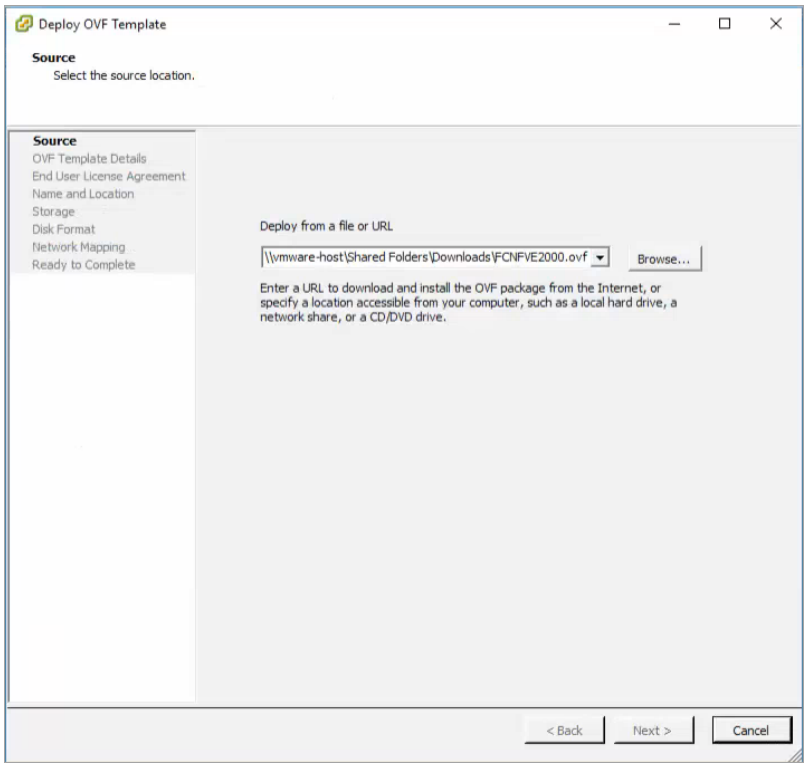


Note: Web クライアント OVF テンプレートウィザードは、ここに示されているイメージや指示と異なる場合がありますが、手順は同様です。1 つの例として、Web クライアントでは [ソース (Source)] ではなく[ソースの場所 (Source Location)] を使用します。下のイメージでは、展開の準備が整った OVF テンプレートの左側に手順が表示されています。



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

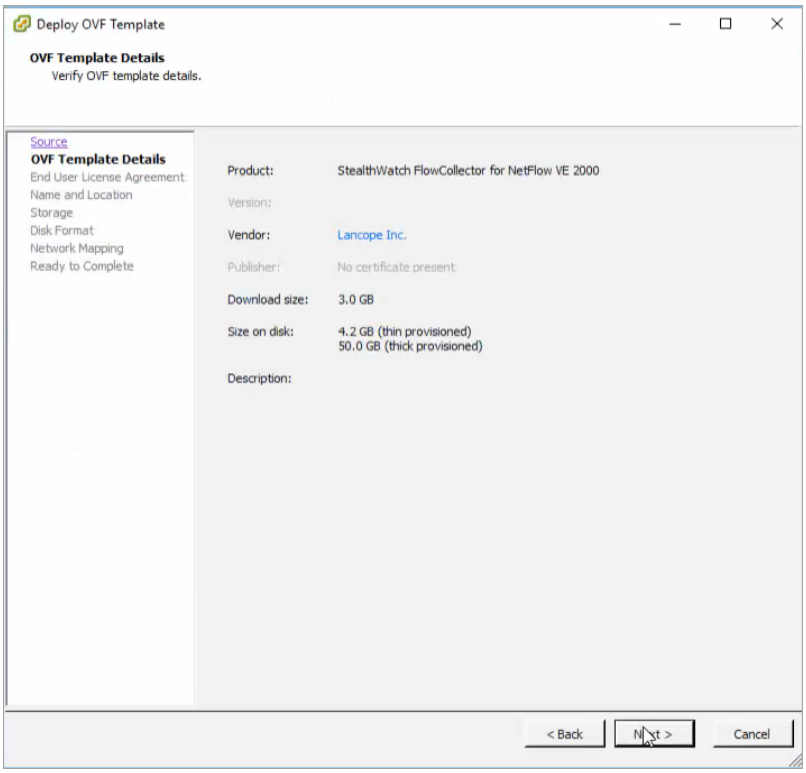
© 2019 Cisco Systems, Inc. All Rights Reserved.



4. [参照(Browse)] をクリックします。移動して仮想アプライアンスの OVF ファイルを選択します。
5. [次へ(Next)] をクリックし、[OVF テンプレートの詳細(OVF Template Details)] ページを表示します。

   Web クライアント: 1.b。[詳細の確認(Review details)] ページが開きます。

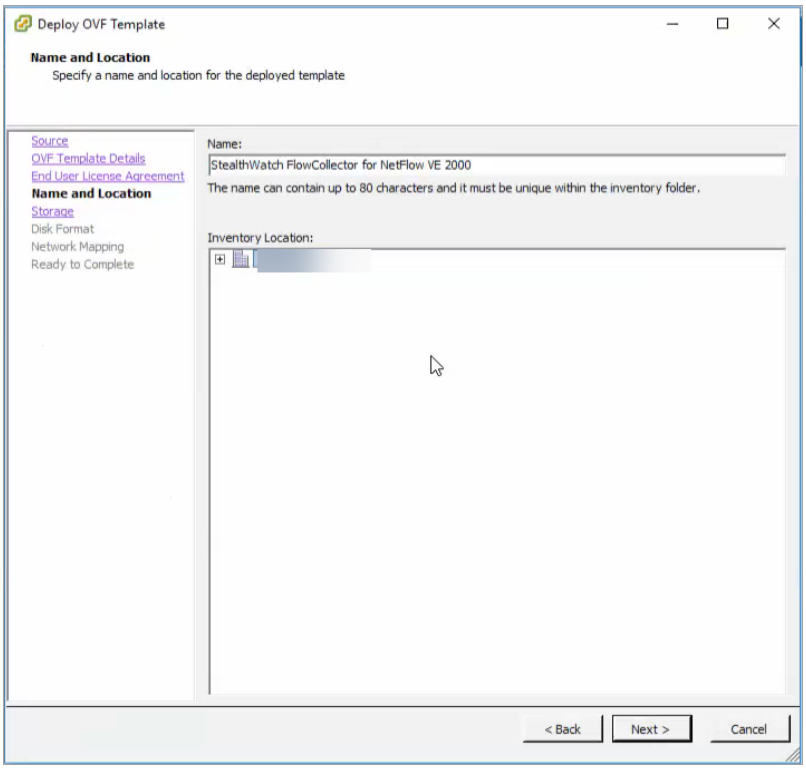
© 2019 Cisco Systems, Inc. All Rights Reserved.



6. [次へ(Next)] をクリックします。エンドユーザ ライセンス契約書を確認します。
   Web クライアント: 1c。EULA を承認します。

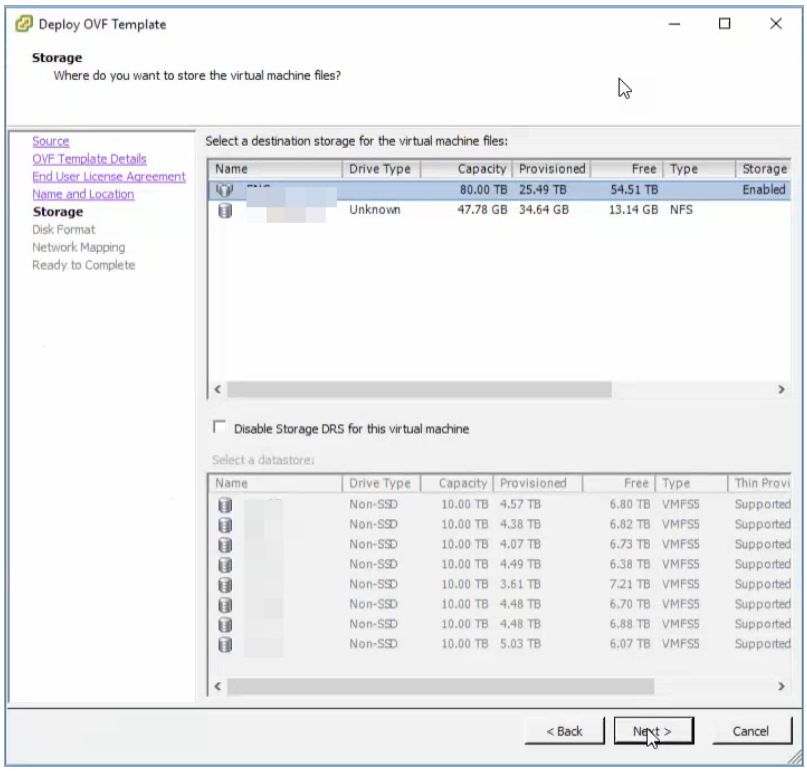
7. 情報を確認した後、[承認(Accept)] をクリックします。[次へ(Next)] をクリックします。[名前と場所(Name and Location)] ページが開きます。
   Web クライアント: 2a。[名前と場所(Name and Location)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



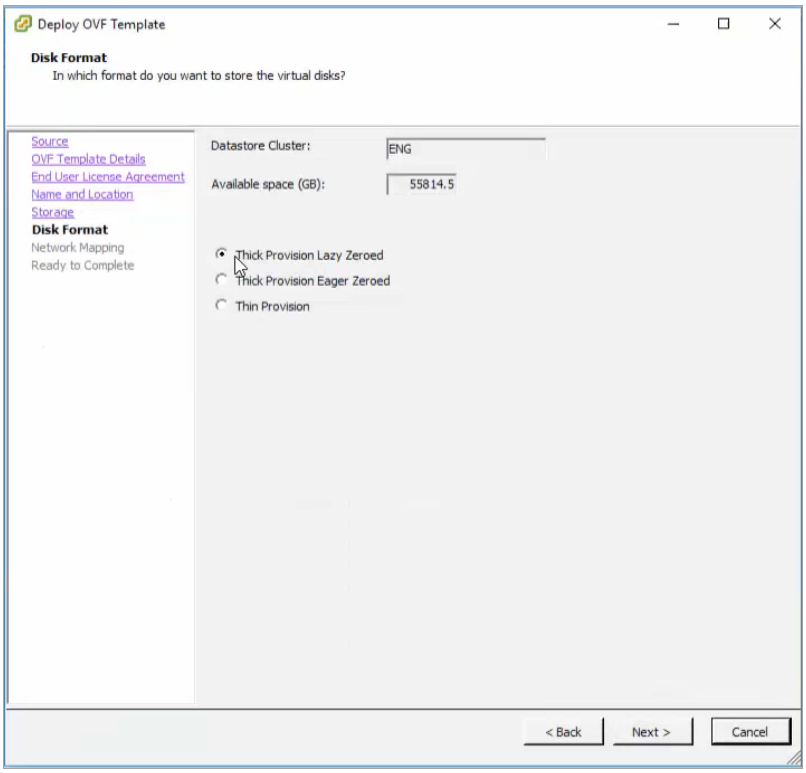
8. **オプション:** 仮想アプライアンスの名前と場所を変更します。これは一意の名前にする必要があります。この名前がインベントリツリーに表示されます。[次へ(Next)] をクリックします。
9. [ストレージ(Storage)] ページで、データファイルの保存先を選択します。[次へ(Next)] をクリックします。

© 2019 Cisco Systems, Inc. All Rights Reserved.



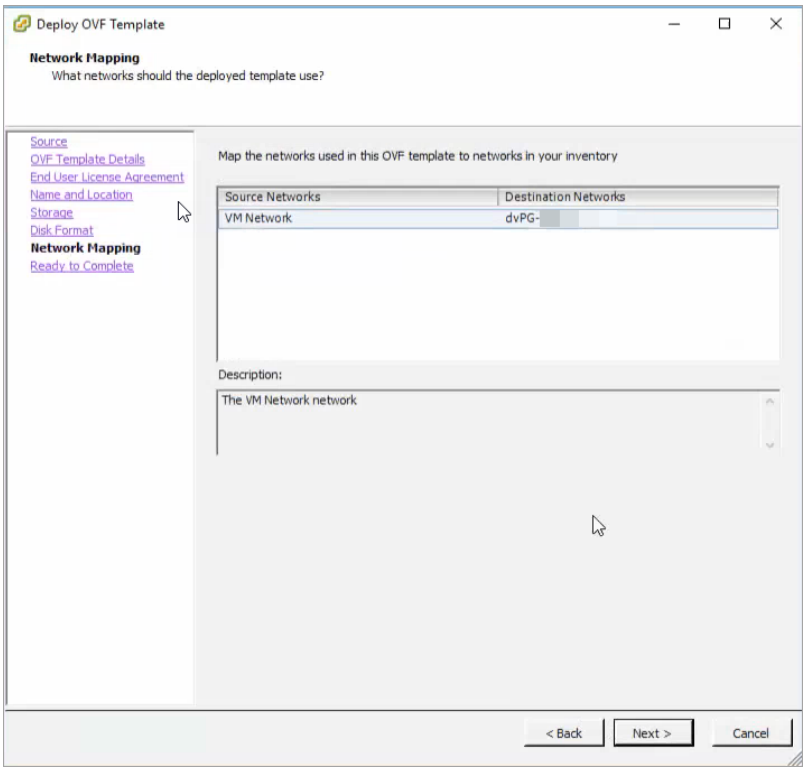
10. [ディスク形式(Disk Format)] ページで、[シックプロビジョニング Lazy Zeroed(Thick Provision Lazy Zeroed)] または [シックプロビジョニング Eager Zeroed(Thick Provision Eager Zeroed)] を選択します。[次へ(Next)] をクリックします。
    - シンプロビジョニング形式は、ディスク容量が制限されている場合にのみ使用します。
    - 詳細については、VMware のマニュアルを参照してください。

© 2019 Cisco Systems, Inc. All Rights Reserved.



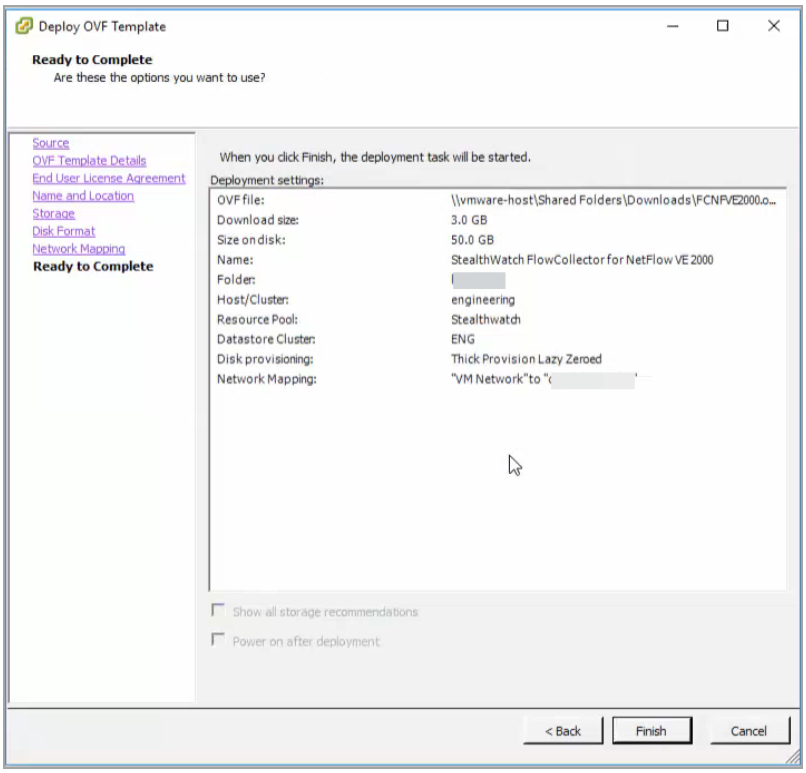
11. [ネットワークのマッピング(Network Mapping)] ページで、仮想アプライアンスのネットワークを選択します。[次へ(Next)] をクリックします。
    Web クライアント: 2c。[ネットワーク設定(Setup Networks)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

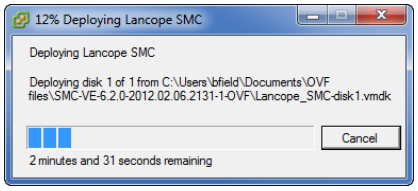


12. [完了する準備ができました(Ready to complete)] ページで、設定の概要を確認します。設定が正しい場合は、[終了 (Finish)] をクリックします。

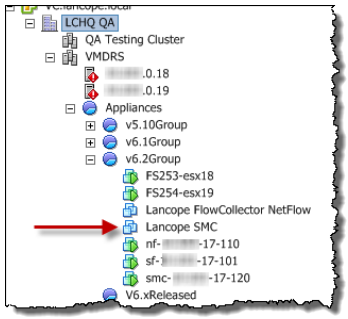
© 2019 Cisco Systems, Inc. All Rights Reserved.



13. [展開(Deployment)] ダイアログボックスが開きます。



14. 展開が完了したら、[閉じる(Close)] をクリックします。インストールした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。



© 2019 Cisco Systems, Inc. All Rights Reserved.

15. すべての Flow Collector 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。

KVM ホストへの仮想アプライアンスのインストール

概要

この章では、**KVM** および **Virtual Machine Manager** を使用して仮想アプライアンスをインストールする方法について説明します。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. ダウンロードおよびライセンスセンターからISO ファイルをダウンロードし、KVM ホストのフォルダにイメージをコピーします。次に示す例では、フォルダは var/lib/libvirt/image です。手順については、『*Downloading and Licensing Guide*』を参照してください。
2. 「概要」の互換性情報を確認します。
3. 通信のファイアウォールを設定します。
4. 「リソース要件」の項を確認し、アプライアンスの適切な割り当てを決定します。
5. 仮想アプライアンスをインストールする仮想ホストサーバに設定された時刻が正しい時刻を示していることを確認します。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。

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

プロセスの概要

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

© 2019 Cisco Systems, Inc. All Rights Reserved.

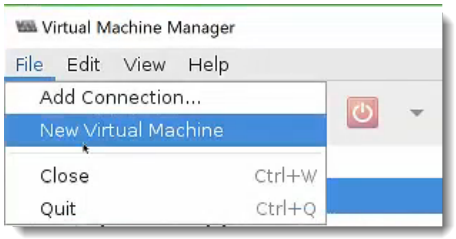
- KVM ホストへの仮想アプライアンスのインストール

KVM ホストへの仮想アプライアンスのインストール

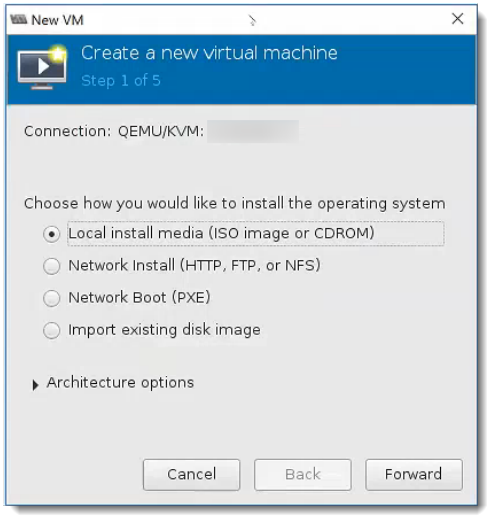
ISO ファイルを使用して KVM ホストに仮想マシンをインストールする方法はいくつかあります。次の手順で、Ubuntu ボックスで実行する Virtual Machine Manager という GUI ツールを使用して仮想 SMC アプライアンスをインストールする一例を示します。互換性のある Linux ディストリビューションを使用できます。互換性の詳細については、「はじめに」の「互換性」の項を参照してください。

仮想アプライアンスをインストールするには、以下の手順を実行します。

1. Virtual Machine Manager を使用して KVM ホストに接続します。
2. [ファイル(File)] > [新しい仮想マシン(New Virtual Machine)] をクリックします。

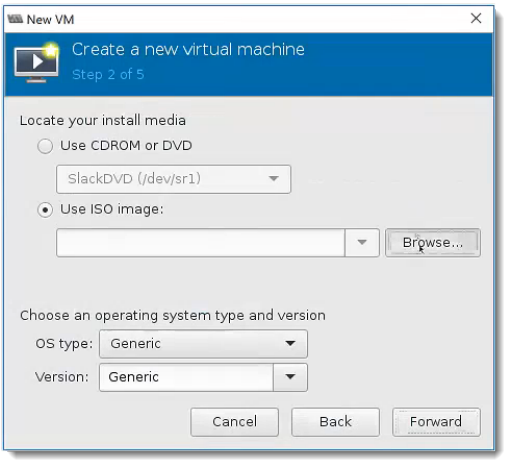


3. [ローカル インストール メディア(ISOイメージまたは CDROM) (Local install media (ISO image or CDROM))] を選択し、[続行(Forward)] をクリックします。



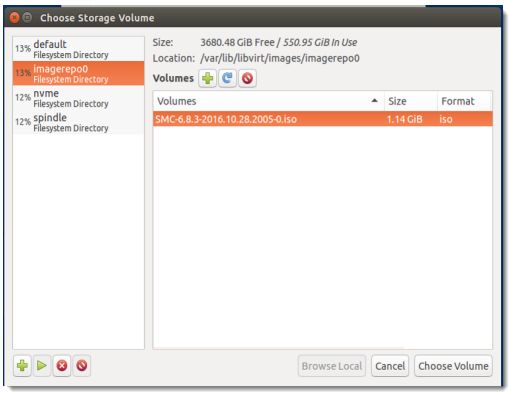
© 2019 Cisco Systems, Inc. All Rights Reserved.

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



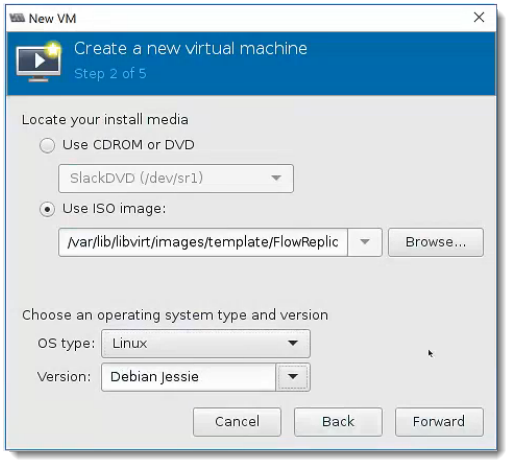
6. ISO ファイルを選択します。[ボリュームの選択(Choose Volume)] をクリックします。

Note: KVM ホストが ISO ファイルにアクセスできることを確認します。

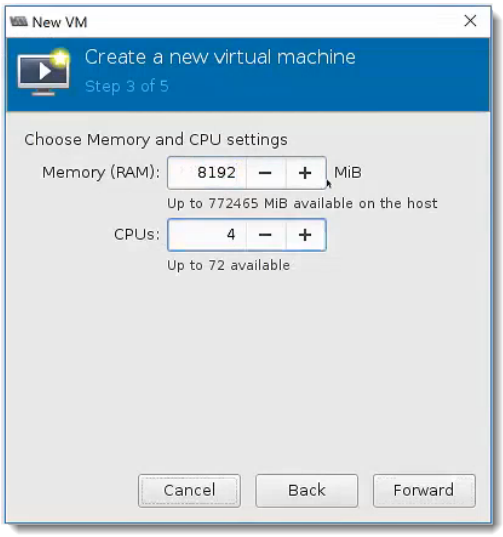


7. [オペレーティング システムのタイプとバージョンの選択(Choose an operating system type and version)] で、[OS タイプ(OStype)] ドロップダウン リストから[Linux] を選択します。
8. [バージョン(Version)] ドロップダウン リストから[Debian Jessie] を選択します。[Forward] をクリックします。

© 2019 Cisco Systems, Inc. All Rights Reserved.

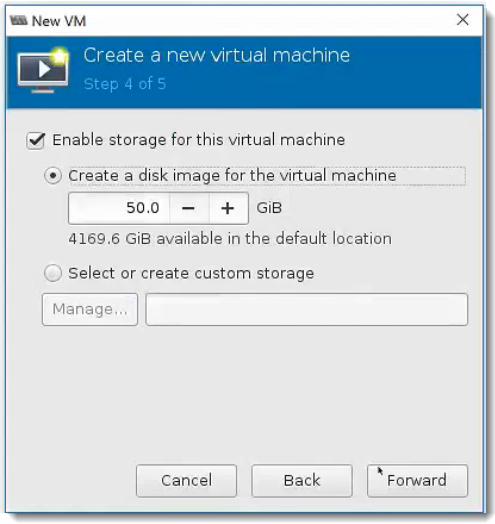


9. メモリ(RAM) とCPU を「リソース要件」の項に示す容量まで増やします。



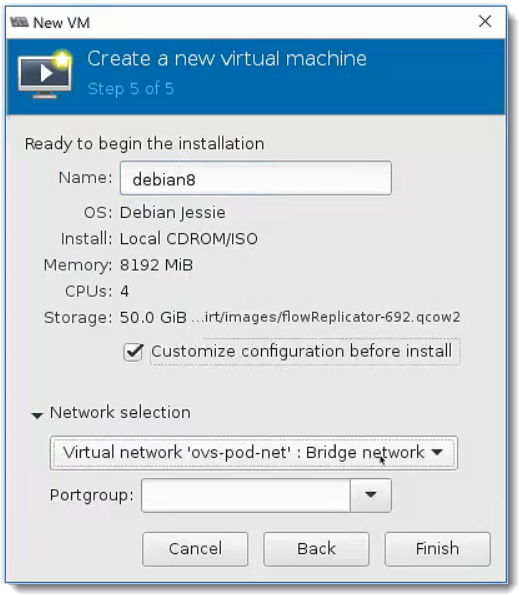
10. [Forward] をクリックします。
11. [仮想マシンへのディスクイメージの作成(Create a disk image for the virtual machine)] を選択します。
12. 「リソース要件」の項のアプライアンスに示されているデータストレージ容量を入力します。[Forward] をクリックします。

© 2019 Cisco Systems, Inc. All Rights Reserved.



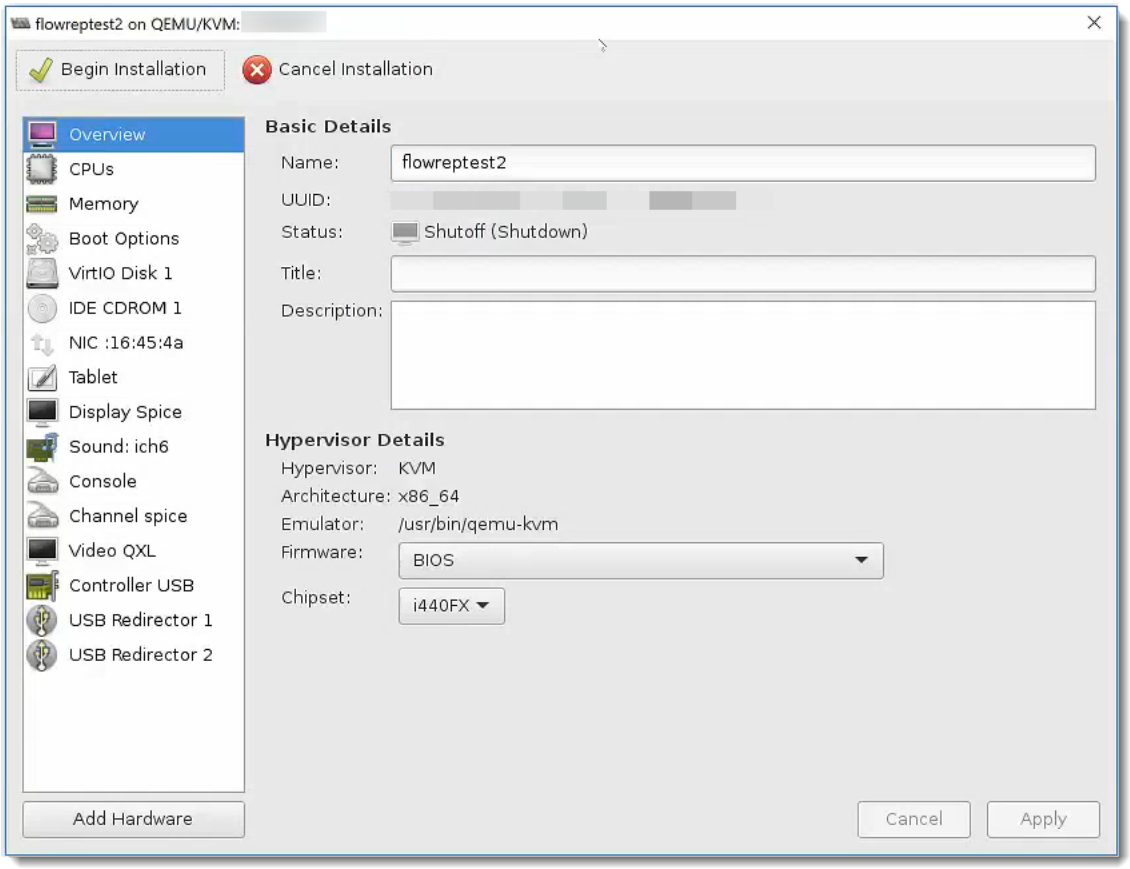
13. 仮想マシンの名前を指定します。これが表示名になるため、後で見つけやすい名前を使用してください。

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



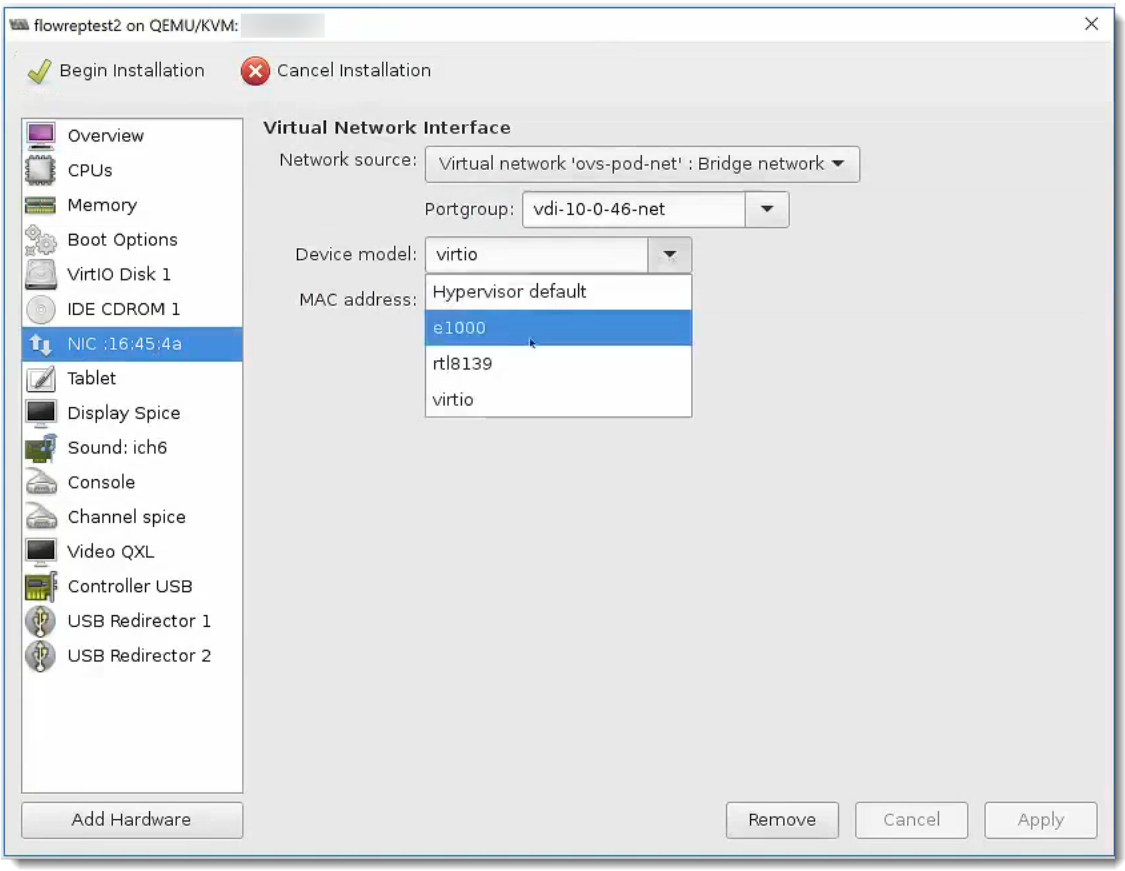
16. [終了(Finish)] をクリックします。[設定(Configuration)] メニューが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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

© 2019 Cisco Systems, Inc. All Rights Reserved.



19. [VirtIO ディスク1(VirtIO Disk 1)] をクリックします。
20. [詳細オプション(Advanced Options)] ドロップダウン リストの [ディスク バス(Disk bus)] ドロップダウン ボックスで [SCSI] を選択します。[適用 (Apply)] をクリックします。

21. [インストールの開始 (Begin Installation)] をクリックします。
22. 「仮想環境の設定」に進みます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

4

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 Flow Collector 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

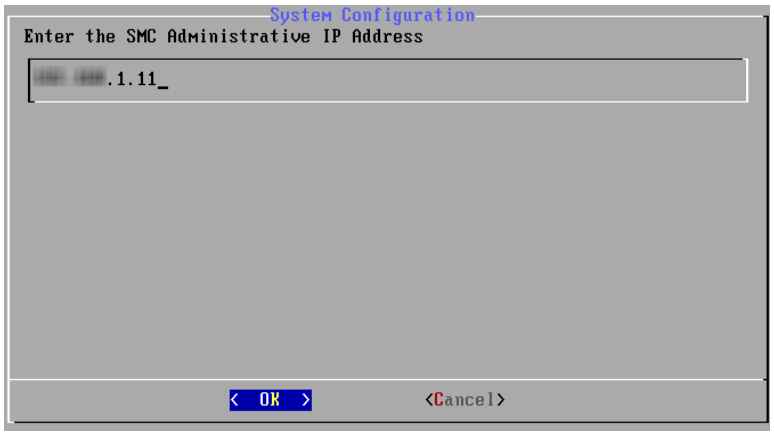
仮想アプライアンスの IP アドレスを設定するには、次の手順を実行します。

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

> **Note:** 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。詳細については、「リソース要件」の項を参照してください。
> - **ESX サーバ:** アプライアンスのメモリ予約制限とリソース プールを増加させます。

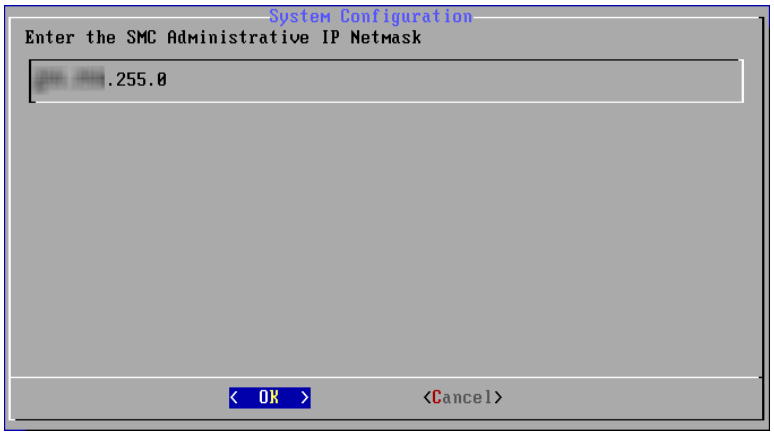
4. 仮想マシン コンソールにアクセスします。
5. 仮想アプライアンスの起動が完了します。仮想アプライアンスの [管理 IPアドレス(Administrative IP Address)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



Note: 画面全体を表示するには、全画面モードを有効にする必要があります。

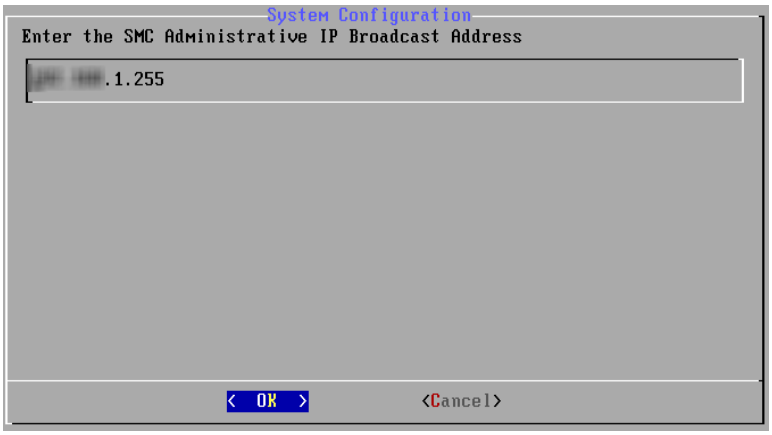
6. ページをクリックします。仮想アプライアンスの IP アドレスを入力します。
7. [OK] を選択して、Enter を押します。デフォルトのネットワークマスクの IP アドレスが表示された [IP ネットマスク(IP Netmask)] ページが開きます。



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。

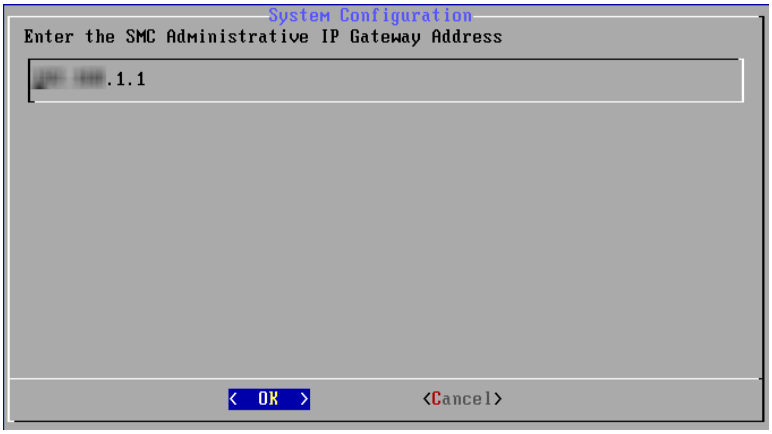
© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

   デフォルトのゲートウェイ サーバ IP アドレスを示す [ゲートウェイアドレス(Gateway Address)] ページが開きます。

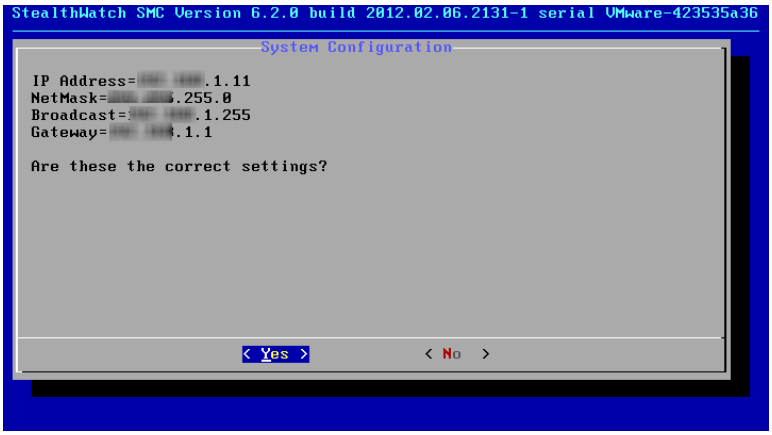


10. 次の手順を実行します。

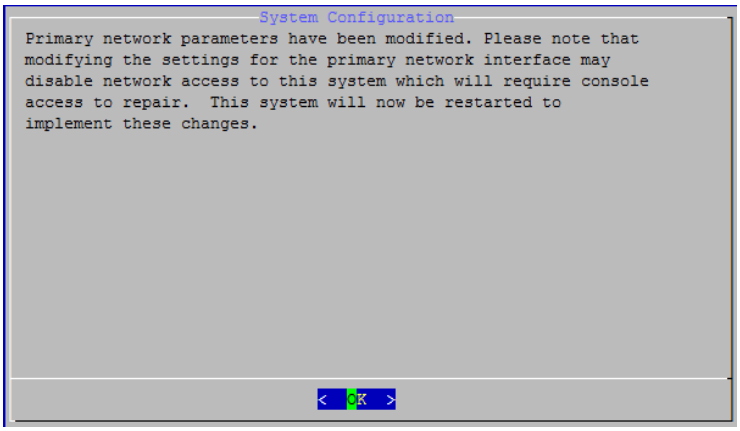
    - デフォルト値を受け入れるか、環境に基づいて新しい値を入力します。
    - [OK] を選択し、Enter を押して続行します。

    入力内容の概要を示すページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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



13. 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。
14. [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。
15. 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

16. Ctrl + Alt を押して、コンソールを終了します。
17. 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

Important: ネットワークの安全性を確保するには、sysadmin とルートユーザのデフォルトパスワードを変更する必要があります。

sysadmin パスワードの変更

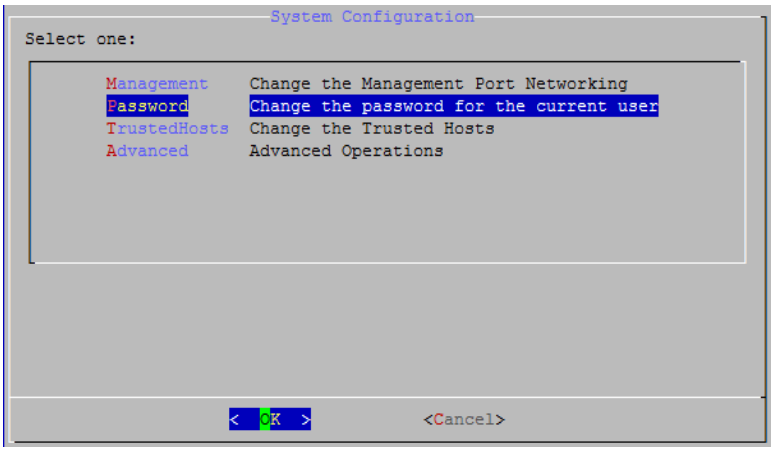
sysadmin パスワードを変更するには、次の手順を実行します。

1. ログインページで、次の操作を実行します。

   a. **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。

   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。

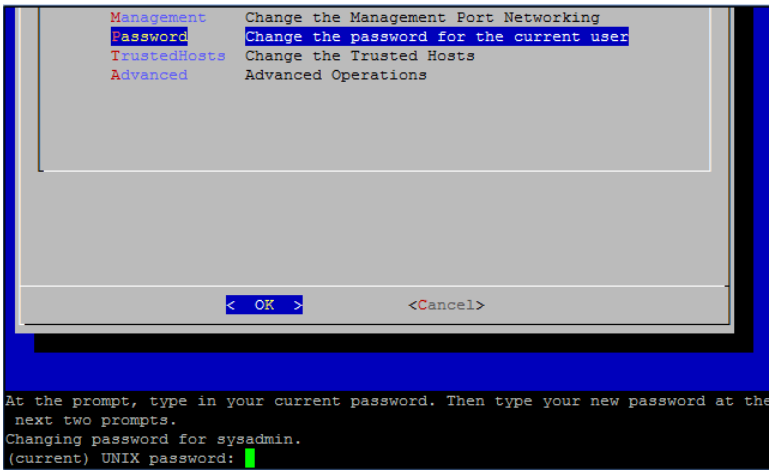
2. [システム設定 (System Configuration)] メニューで、[パスワード(Password)] を選択して Enter を押します。



© 2019 Cisco Systems, Inc. All Rights Reserved.

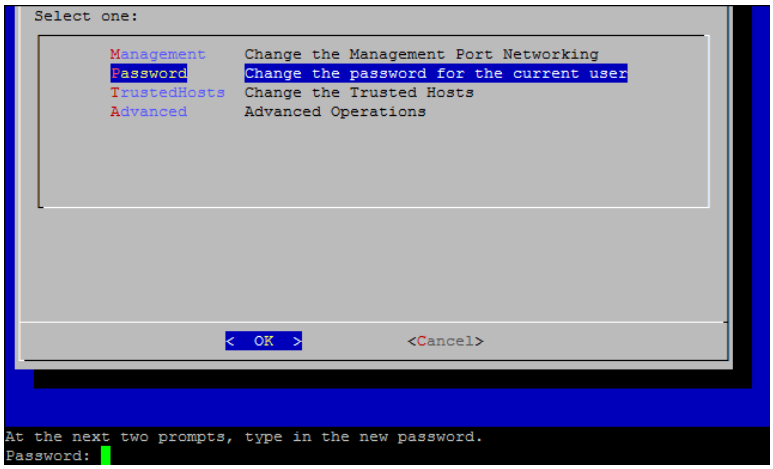
Important: 信頼できるホストのリストをデフォルトから変更する場合、各 Stealthwatch アプライアンスが展開内の他のすべての Stealthwatch アプライアンスの信頼できるホストのリストに含まれていることを確認する必要があります。そうしない場合、アプライアンス間で通信できません。

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。

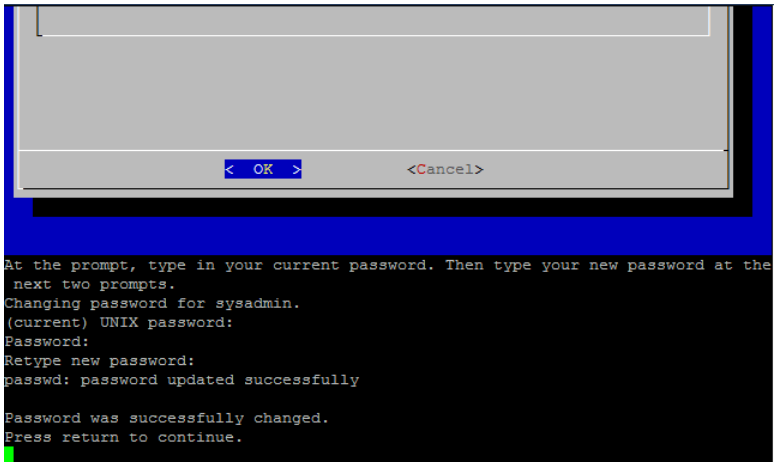
注：

- パスワードは、スペースを含めずに 8 ～ 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

- 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。

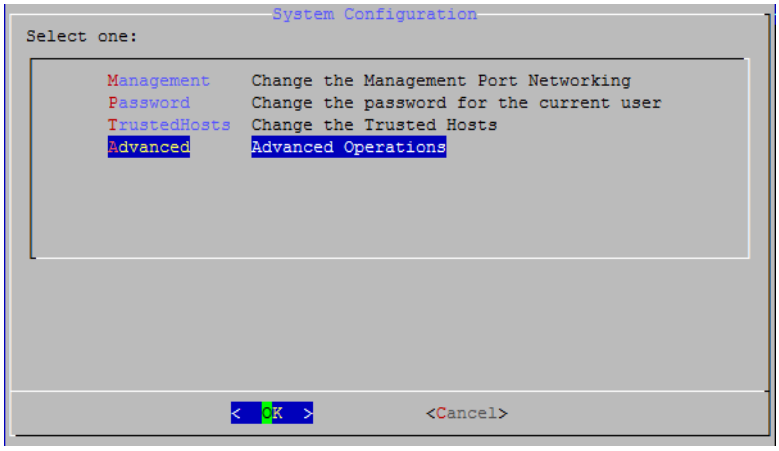


6. Enter を押して、[システム設定(System Configuration)] コンソール メニューに戻ります。
7. 次の項「ルートパスワードの変更」に進みます。

ルートパスワードの変更

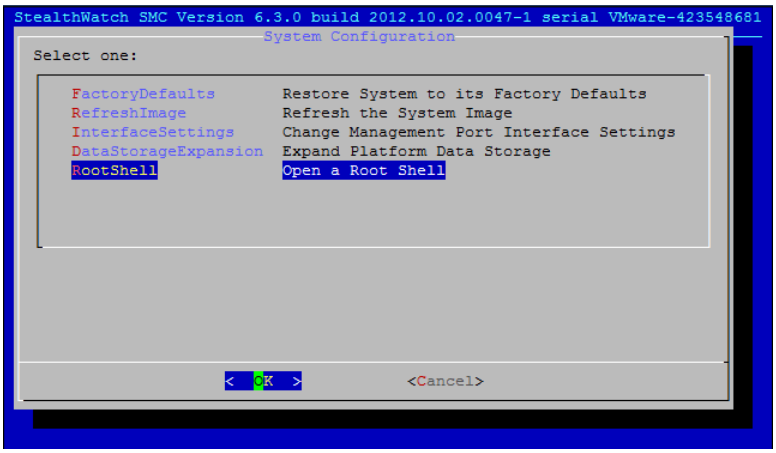
ルートパスワードを変更するには、次の手順を実行します。

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。

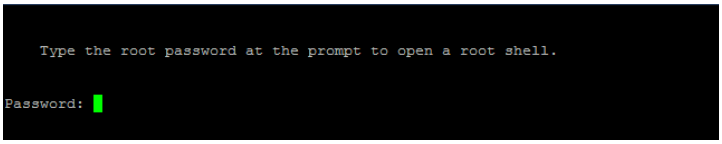


2. [詳細(Advanced)] メニューで、[RootShell] を選択して Enter を押します。

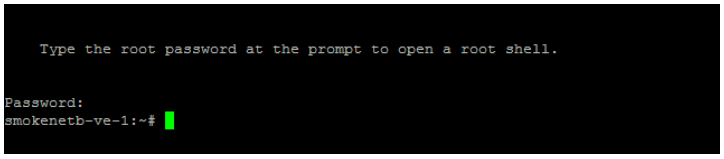
© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

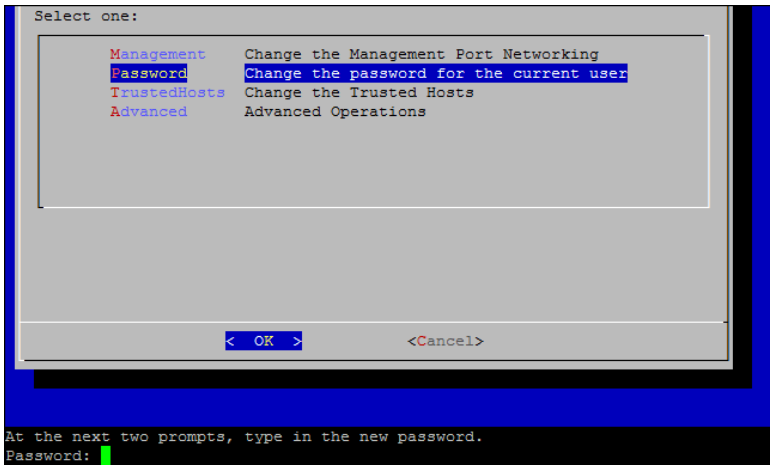


4. **SystemConfig** (大文字と小文字を区別します) と入力して、Enter を押します。

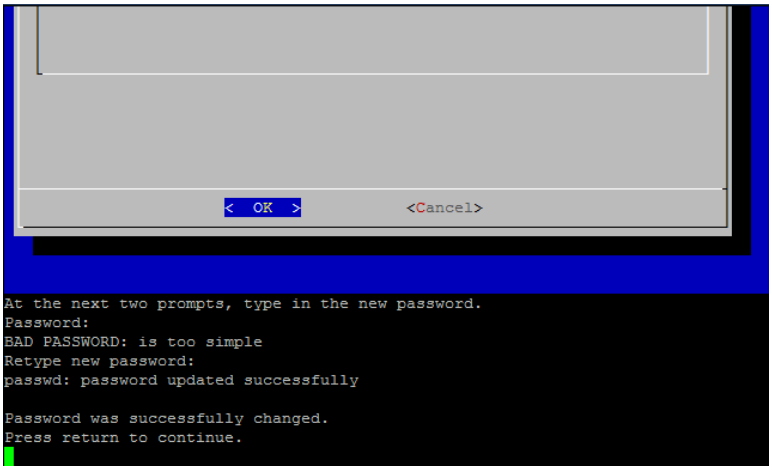
   これによって、[システム設定 (System Configuration)] メニューに戻り、ルートパスワードを変更できます。

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。

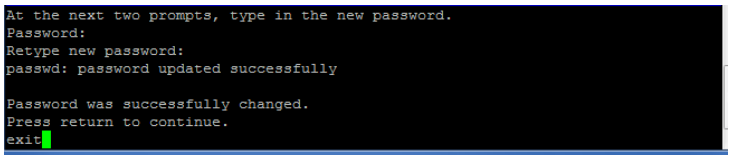
© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

10. すべての Flow Collector 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。

    - 実行している場合は、「仮想アプライアンスシステムの設定」に進みます。
    - 実行していない場合は、「IP アドレスの設定」に戻って、次の仮想アプライアンスに対してこの章のすべての手順を繰り返します。その後、「システムの設定」に進みます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

5

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のプロセスが完了します。

Note: 先に進む前に必要な情報については、「はじめる前に」(1 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 System 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す。

1. 個々のアプライアンスの設定
2. システムの設定
3. データストレージおよびリソースの割り当ての拡張
4. アプライアンス管理インターフェイスを使用した設定

Note: 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 Flow Collector 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。

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ことが重要です。

1. UDP Director VE
2. Flow Collector Database 5000 コンソール(使用している場合)

© 2019 Cisco Systems, Inc. All Rights Reserved.

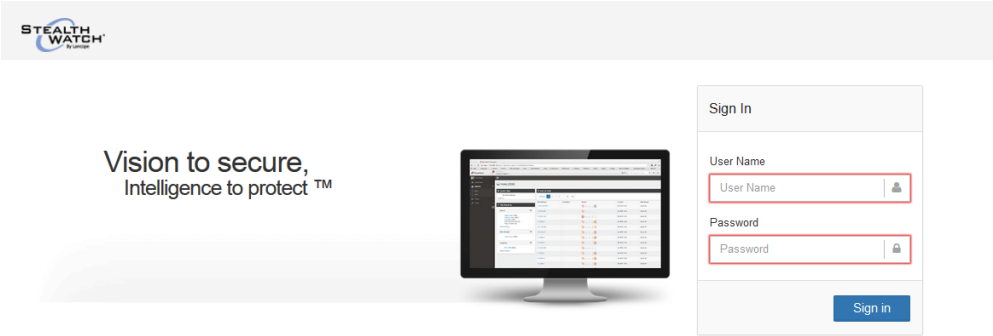
3. その他のすべての Flow Collector
4. すべての Flow Sensor
5. クラウド ライセンス コンセントレータ
6. エンドポイント コンセントレータ
7. セカンダリStealthwatch 管理 コンソール
8. プライマリStealthwatch 管理 コンソール

開始する前に、「はじめる前に」(1 ページ) で詳細情報を収集します。

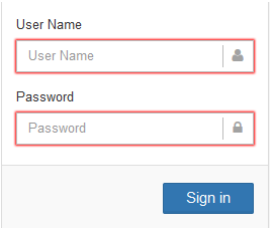
Note: 環境によっては、画面はここに表示されるものと若干異なる場合があります。

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、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. 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 **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。



ログインするには、次の手順を実行します。



© 2019 Cisco Systems, Inc. All Rights Reserved.

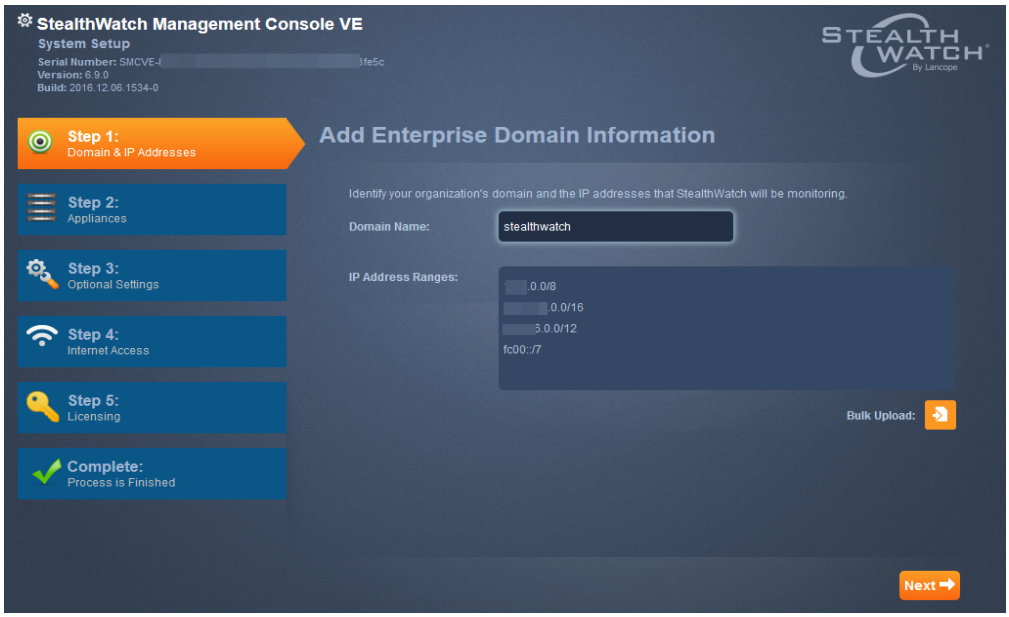
a. [ユーザ名 (User Name)] フィールドに **admin** と入力します。

b. [パスワード(Password)] フィールドに **lan411cope** と入力します。

c. [サインイン(Sign In)] をクリックします。

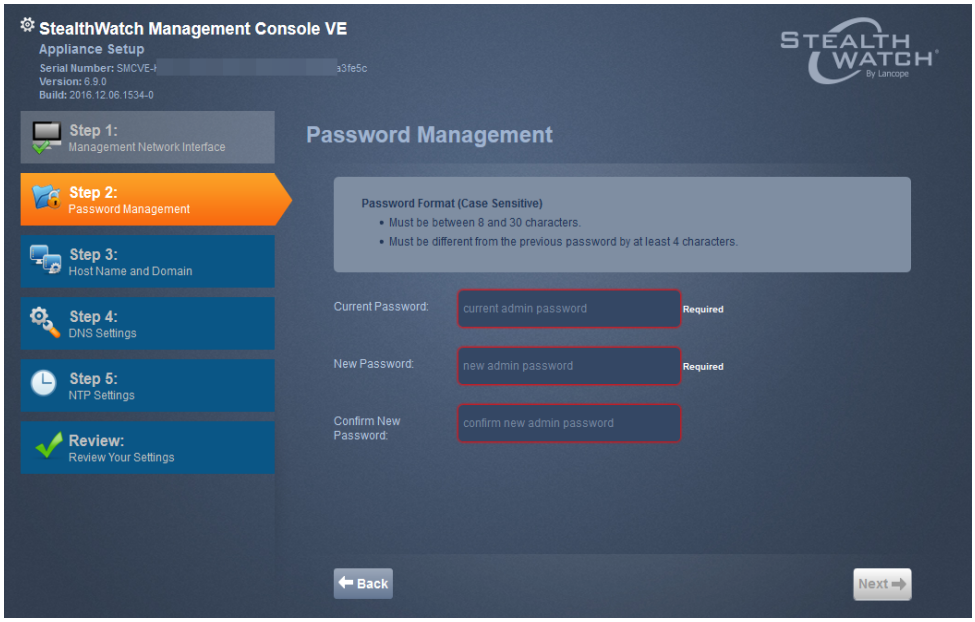
5. [ようこそ(Welcome)] ページが開きます。**[続行 (Continue)]** をクリックします。

[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。

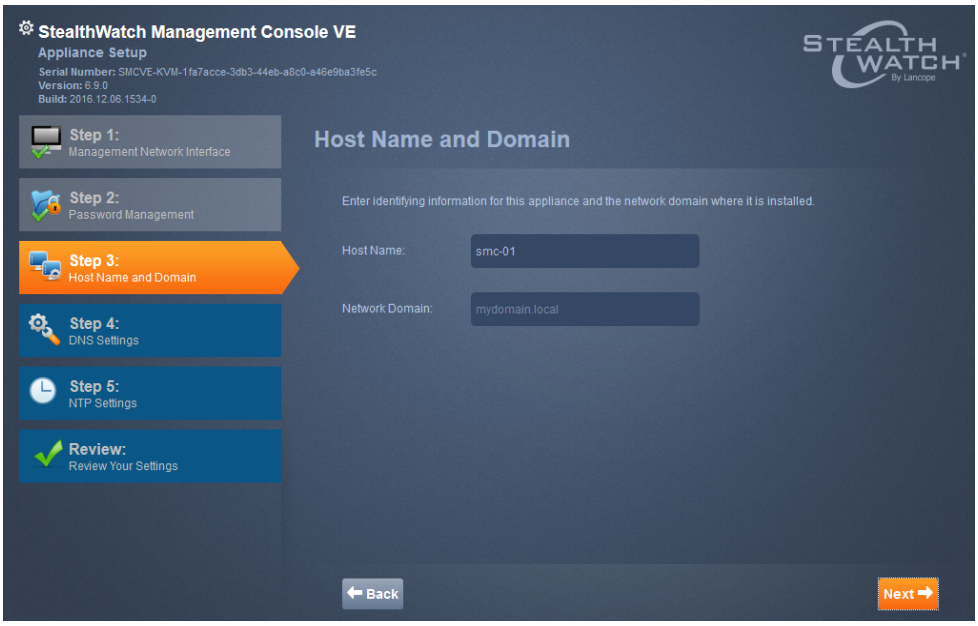


© 2019 Cisco Systems, Inc. All Rights Reserved.

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。

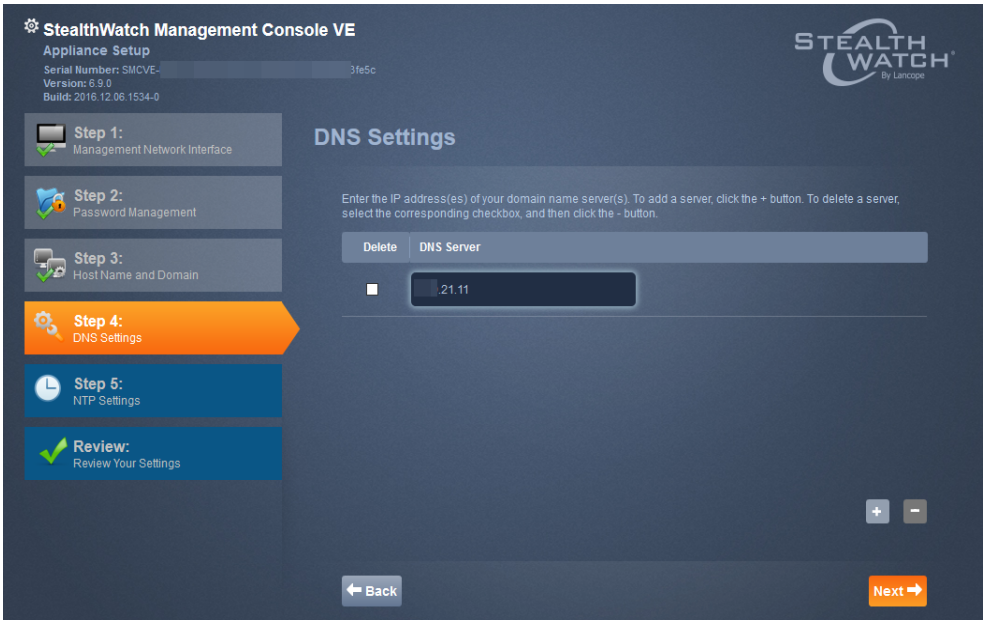


7. 適切なフィールドに新しい管理者パスワードを入力して、[次へ(Next)] をクリックします。[ホスト名とドメイン(Host Name and Domain)] ページが開きます。



© 2019 Cisco Systems, Inc. All Rights Reserved.

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。

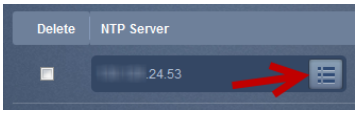


9. [+] ボタンをクリックして、DNS サーバの IP アドレスを入力します。[次へ(Next)] をクリックします。[NTP設定(NTP Settings)] ページが開きます。

Note: 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

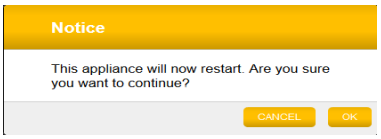
10. デフォルト設定を受け入れるか、NTP サーバの IP アドレスを入力するか、またはリストアイコンをクリックしてドロップダウンリストから名前を選択して別のサーバを入力することができます。「アプライアンス管理インターフェイスを使用した設定



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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

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. 最後の、または唯一のSMC VE 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

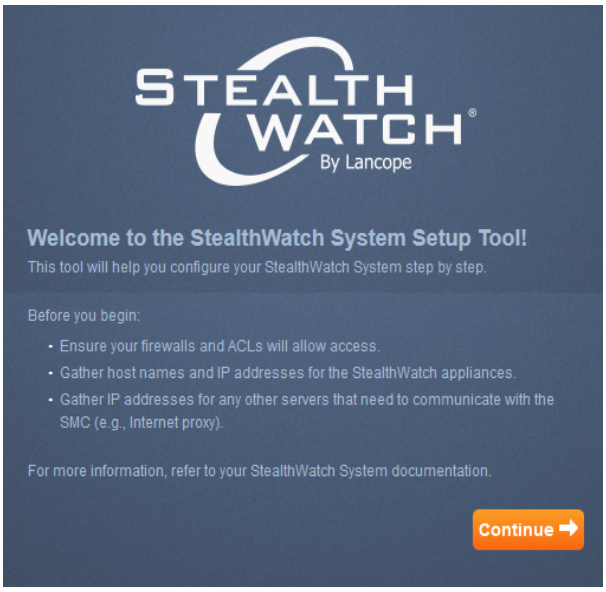
SMC(VE) を含むすべてのアプライアンスの設定を終了すると、システムを設定できます。

CAUTION! 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。そうしない場合、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。

Important: 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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

© 2019 Cisco Systems, Inc. All Rights Reserved.

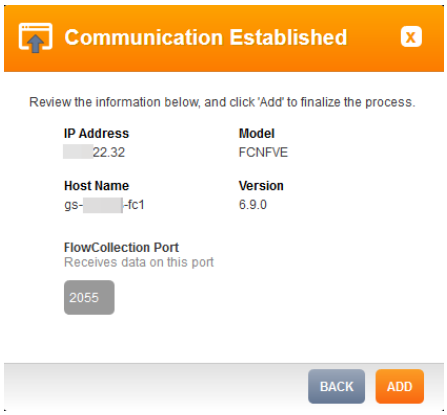
括アップロードを実行して、[次へ(Next)] をクリックします。[アプライアンス(Appliance)] ページが開きます。

Note: 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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

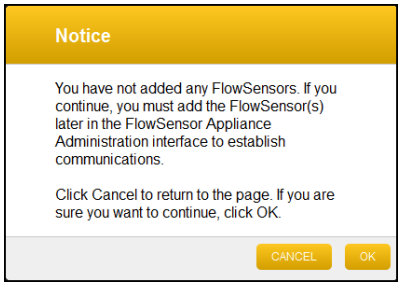
1. ブラウザーとアプライアンスの IP アドレスを使用して、該当するアプライアンス管理インターフェイスにログインします。
2. 左側のナビゲーションウィンドウで、[設定(Configuration)] > [管理システムの設定(Management Systems Configuration)] の順にクリックします。
3. [新しい管理システムの追加(Add New Management System)] をクリックします。
4. [管理システムのIPアドレス(Management System IP Address)] フィールドに、SMC の IP アドレスを入力します。
5. [SMC(Is 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の [エラー(Error)] ダイアログで [キャンセル(Cancel)] をクリックして、[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。

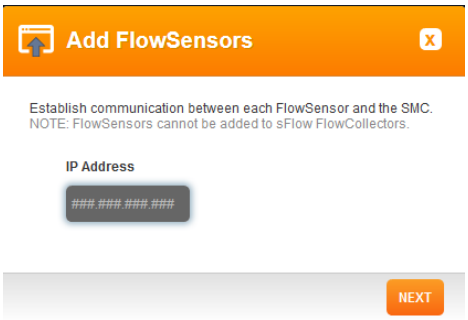
© 2019 Cisco Systems, Inc. All Rights Reserved.

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] をクリックします。手順 14 に進みます。

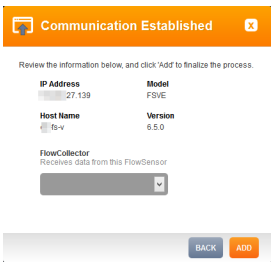


9. [+] ボタンをクリックします。[フローセンサーの追加(Add Flow Sensor)] ダイアログが表示されます。

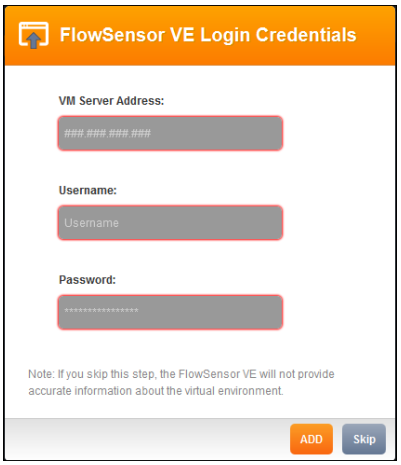
© 2019 Cisco Systems, Inc. All Rights Reserved.



10. IP アドレスを入力し、[OK] をクリックします。[通信が確立されました(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ャル(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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

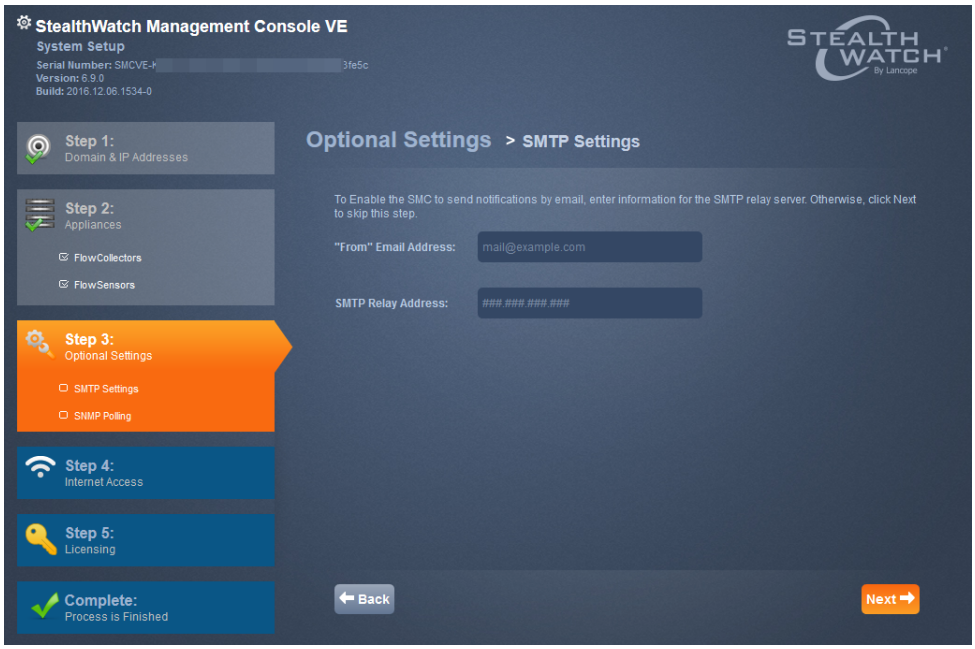
- VM サーバ アドレス
- フロー センサーのユーザ名
- パスワード

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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



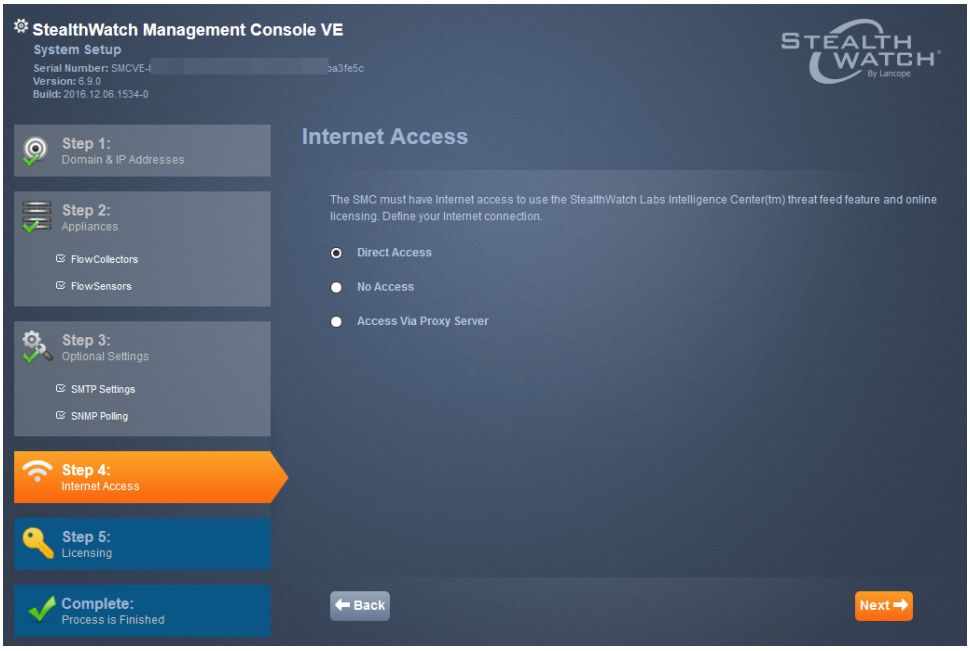
15. SMC が電子 メールを送信するときの、[差出人 (from)] フィールドに指定する電子 メール アドレスを入力します。
16. SMTP リレー アドレスを入力し、[次へ(Next)] をクリックします。SNMP ページが開きます。

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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

Note: [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、さらにオプションとして認証と暗号化を選択できます。

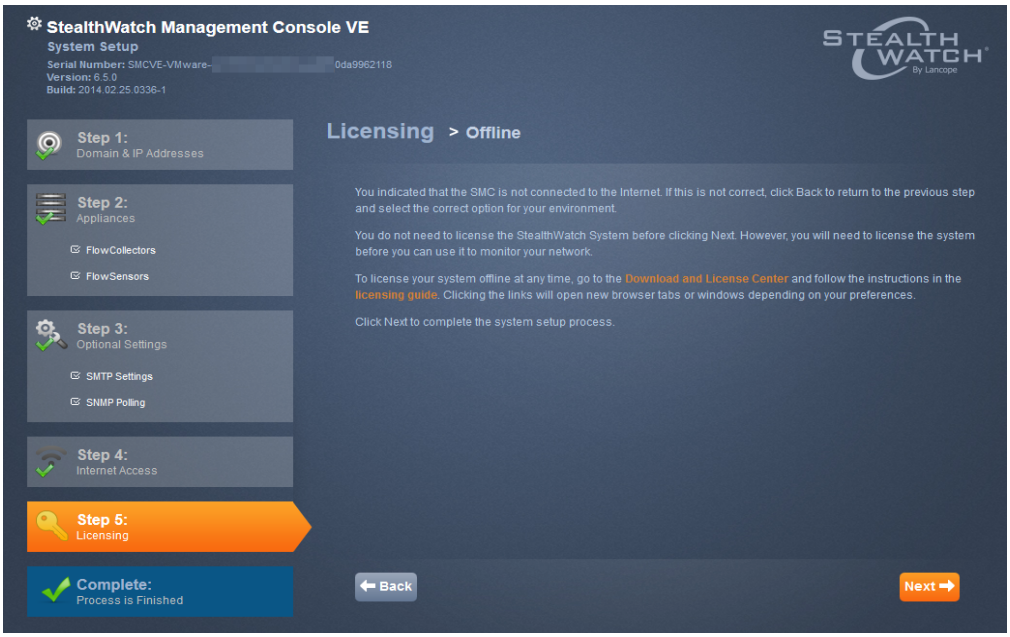
18. [インターネットアクセス(Internet Access)](SMC 用) ページが開きます。



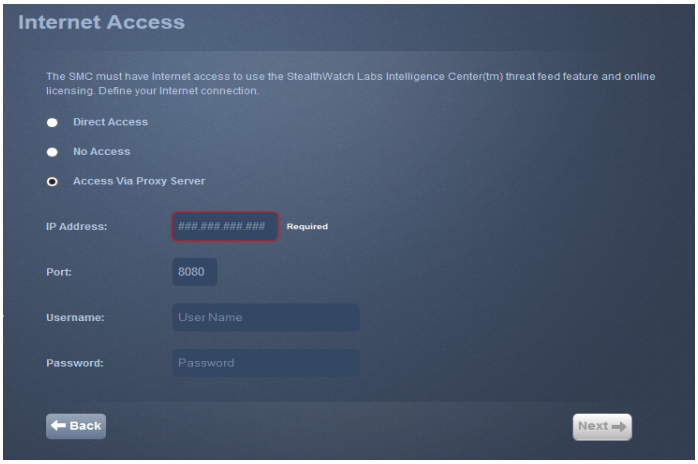
19. インターネットアクセスの適切なタイプを選択します。

- [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)] をクリックすると、[完了 (Complete)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



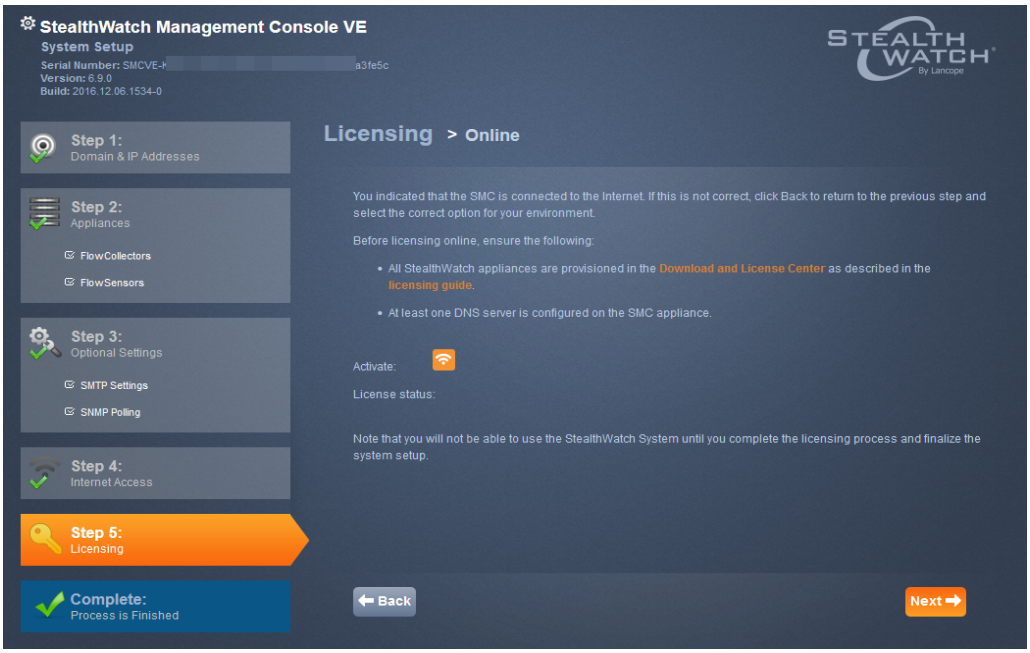
- [プロキシサーバ経由でアクセス(Access via Proxy Server)]: SMC はプロキシサーバ経由でインターネットに接続されます。プロキシ設定が表示されます。



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. [ダイレクトアクセス(Direct Access)] を選択した場合、またはプロキシ設定が完了した場合には、[ライセンス(Licensing)] ページが開きます。

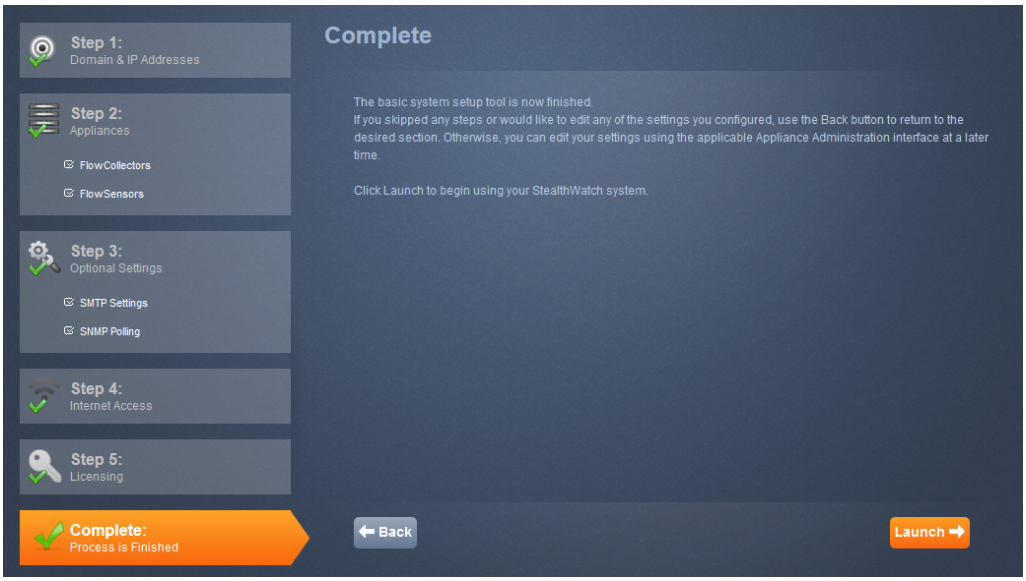
© 2019 Cisco Systems, Inc. All Rights Reserved.



21. [ダウンロードおよびライセンスセンター(Download and License Center)] のリンクをクリックします。『*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。

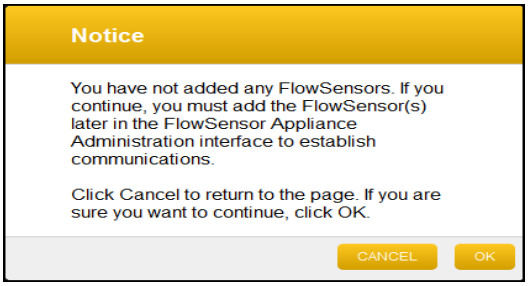
Note: アプライアンスが登録されていない場合、メッセージが表示されます。

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



© 2019 Cisco Systems, Inc. All Rights Reserved.

24. [起動(Launch)] をクリックすると、SMC クライアントのランディング ページが開きます。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を使用した設定" on page lviに進みます。
26. 外部イベントを収集するSMC VE(syslog) または Flow Collector VE を設定していますか。
    - 「はい」の場合、次の項「データストレージおよびリソースの割り当ての拡張」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を使用した設定" on page lviに進みます。

データストレージおよびリソースの割り当ての拡張

仮想アプライアンスをインストールするには、使用可能なデータストレージを拡張しなければならない場合があります。また、パフォーマンスを向上させるために、アプライアンスのリソース割り当てを拡張することもできます。この手順は、Flow Collector VE で必要となります。

- データストレージの範囲およびリソース割り当てについては、「リソース要件：データストレージ」の項を参照してください。
- **Flow Collector 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。
- ハイパーバイザ ホストで別の方法を使用して仮想マシンのメモリを増加させる場合は、変更を保存した後にアプライアンスを再起動します。

仮想アプライアンスのデータストレージを拡張するには、次の手順を実行します。

© 2019 Cisco Systems, Inc. All Rights Reserved.

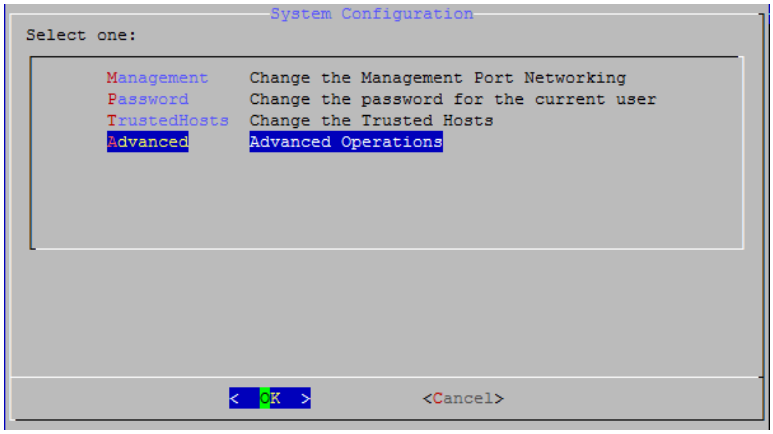
Note: 仮想マシンに関連付けられたスナップショットがある場合は、SMC VE または Flow Collector VE のデータストレージを拡張することができません。データストレージの拡張を開始する前に、スナップショットを削除してください。

1. ハイパーバイザホスト(仮想マシンホスト)に接続します。
2. ハイパーバイザホストで仮想マシンを見つけます。
3. 仮想マシンの電源をオフにします。
4. 仮想マシンコンソールにアクセスします。
5. ページをクリックし、次のように実行します。

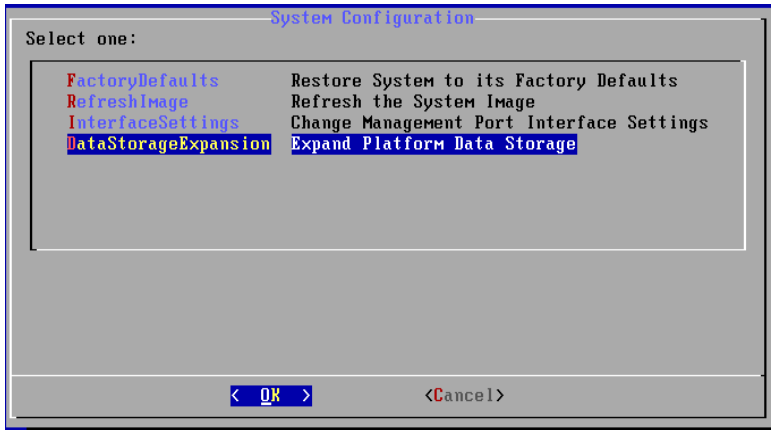
   a. **sysadmin** と入力して、Enter を押します。

   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。

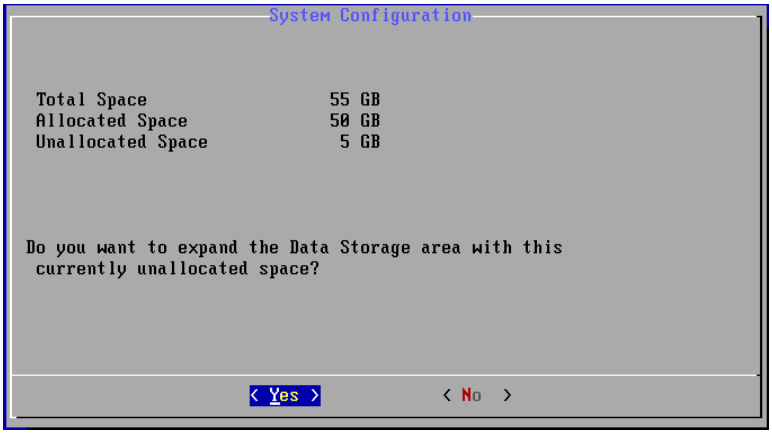


6. [詳細(Advanced)] オプションを選択し、Enter を押します。[詳細(Advanced)] メニューページが開きます。

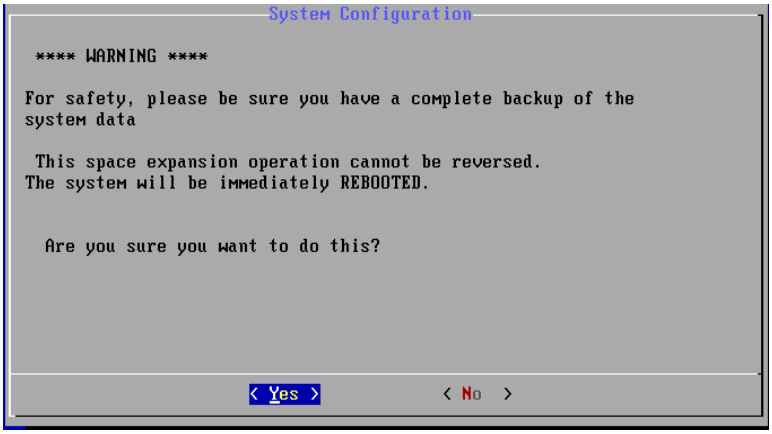


© 2019 Cisco Systems, Inc. All Rights Reserved.

7. [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。



8. 情報を確認し、必要に応じて変更します。変更を保存するには、[はい(Yes)] をクリックし、Enter キーを押します。[警告(Warning)] ページが開きます。



9. [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。
10. Ctrl+Alt を押してコンソール環境を終了します。
11. データストレージに加えた変更を確認します。

© 2019 Cisco Systems, Inc. All Rights Reserved.

アプライアンス管理インターフェイスを使用した設定

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(Admin)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)

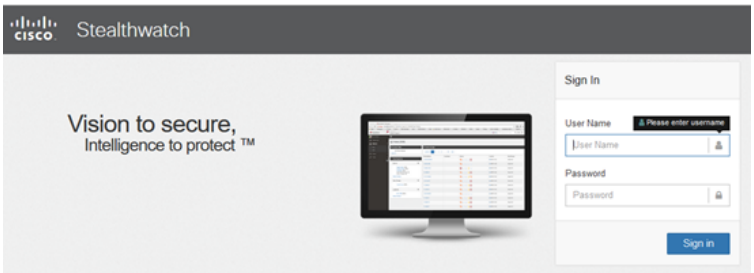
- Stealthwatch をサポートしているブラウザは、Internet Explorer バージョン 11 以降と最新バージョンの Firefox、Google Chrome、および Safari です。
- ページのロードに問題が発生した場合は、別のブラウザを試すか、ブラウザのキャッシュをクリアし、ブラウザを閉じて再度開き、もう一度ログインします。

1. ブラウザのアドレスフィールドに **https://** と入力し、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。

   Note: お使いの VM ホストの速度によっては、すべてのサービスが起動するまでに 30 分程度かかることがあります。

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。

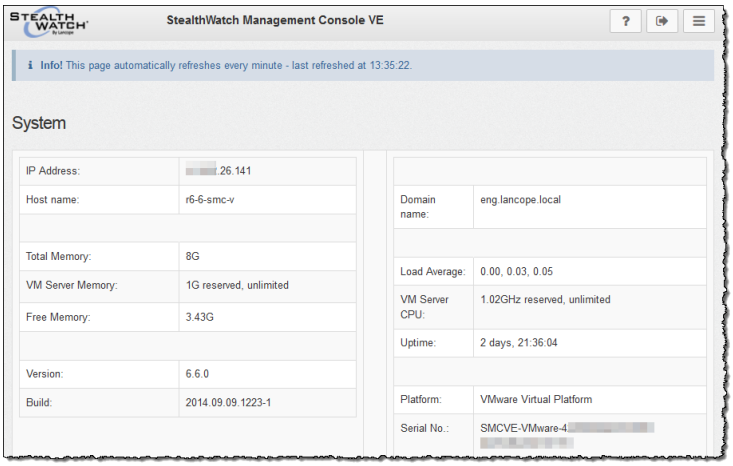
   - 「はい」の場合、[ランディング(Landing)] ページが開きます。右上隅の [設定(Settings)] アイコンをクリックして、[アプライアンスの管理(Administer Appliance)] をクリックします。



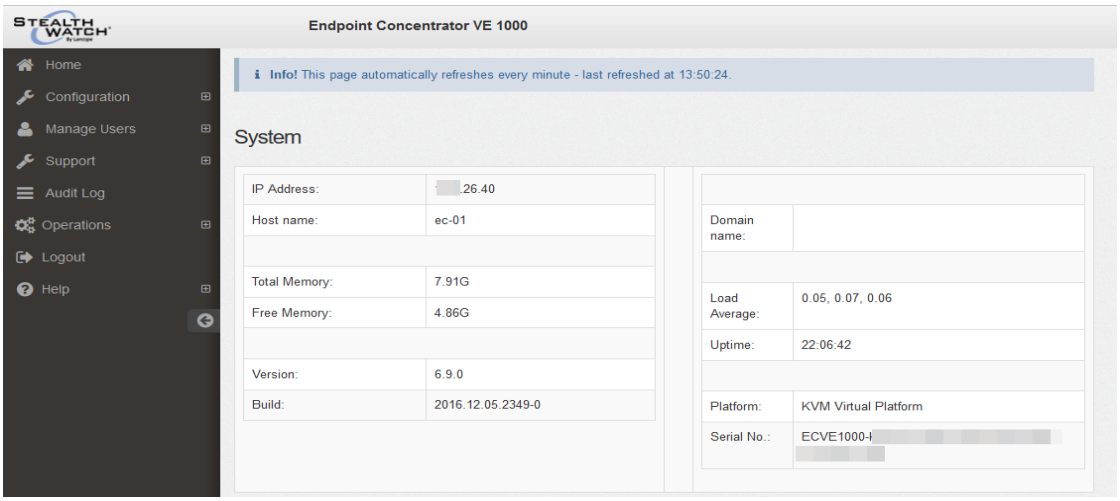
   - 「いいえ」の場合、仮想アプライアンスの [ログイン(Login)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

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。



© 2019 Cisco Systems, Inc. All Rights Reserved.



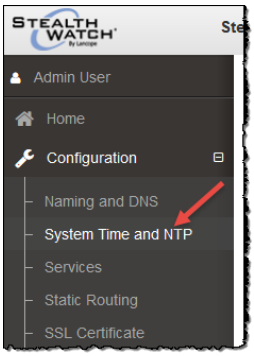
6. 次の項「システム時刻の設定」に進みます。

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。

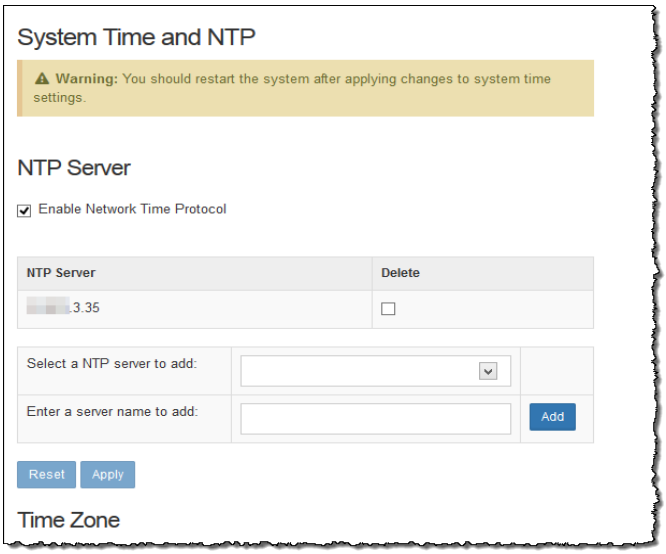
CAUTION! SMC に情報を送るフローコレクタやその他のデバイスに使用されているものと同じ NTP サーバを使用します。

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。

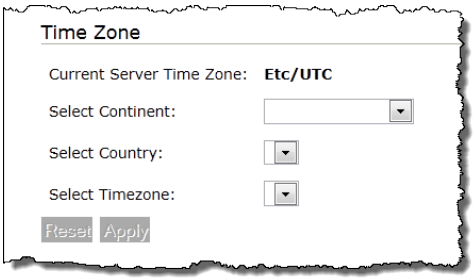


アプライアンス設定ツールを使用して初期設定で設定した NTP サーバが表示された [NTPサーバ(NTP Server)] ページが開きます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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

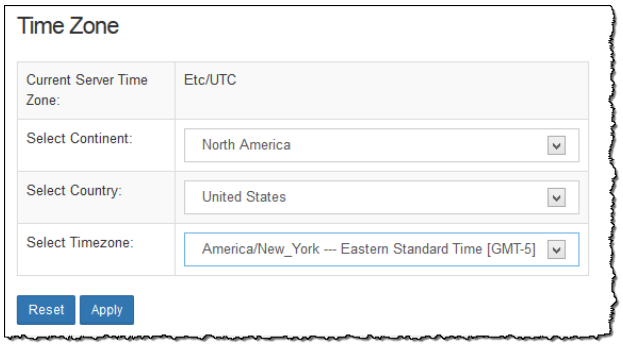


3. 次の手順を実行します。

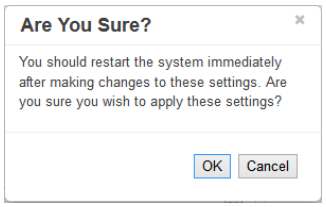
- ドロップダウン リストから、大陸を選択します。
- ドロップダウン リストから、国を選択します。
- ドロップダウン リストから、タイムゾーンを選択します。

[適用(Apply)] が表示されます。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

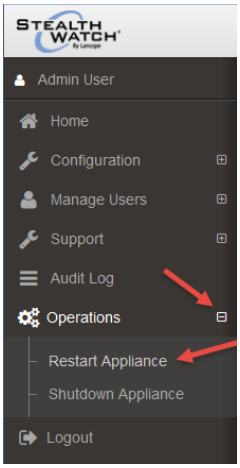


5. [OK] をクリックします。
6. 次の項「仮想アプライアンスの再起動」に進みます。

仮想アプライアンスの再起動

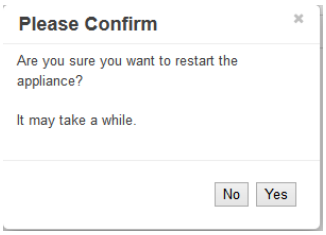
仮想アプライアンスを再起動するには、次の手順を実行します。

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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



2. [はい(Yes)] をクリックします。

9. SMC VE または Flow Collector VE を設定しましたか。

   - SMC VE を設定している場合、再起動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。
   - Flow Collector VE を設定している場合、次の章「通信の確認」に進みます。

© 2019 Cisco Systems, Inc. All Rights Reserved.

6

通信の確認

概要

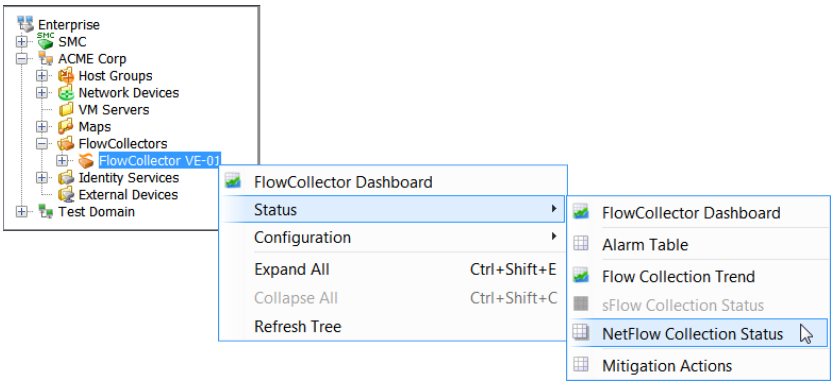
Stealthwatch アプライアンスのライセンス供与後、NetFlow データを受信していることを確認する必要があります。確認するには、この章で説明している次の手順を実行します。

CAUTION! 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

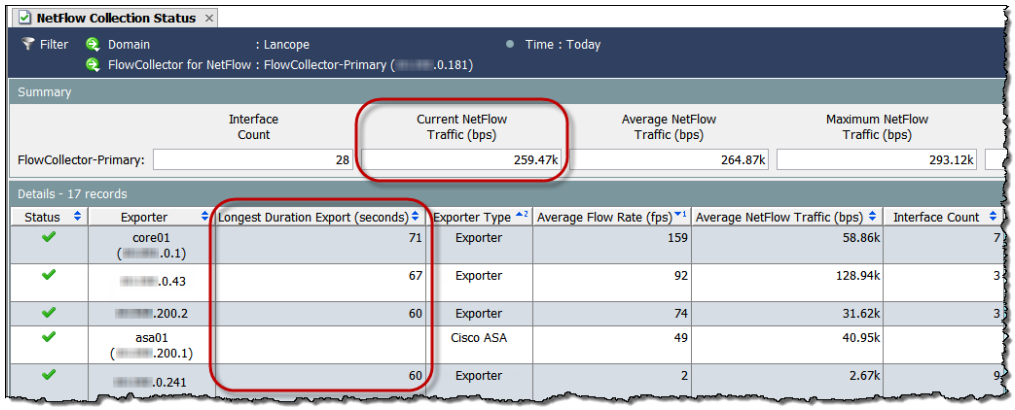
SMC へフローコレクタを追加すると、フローコレクタは SMC にフロー情報を伝え、さまざまな文書を介してユーザフレンドリーな方法でこの情報を表示します。NetFlow データを本当に収集していることを確認するには、次の手順を実行します。

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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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。

   - 「はい」の場合、次の手順に進みます。
   - 「いいえ」の場合、エクスポータおよびルータの設定を確認します。(詳細は、『*SMC Client Online Help*』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。各エクスポータの値は 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。エクスポータおよびルータの設定を確認します。(詳細は、『*SMC Client Online Help*』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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

7

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)

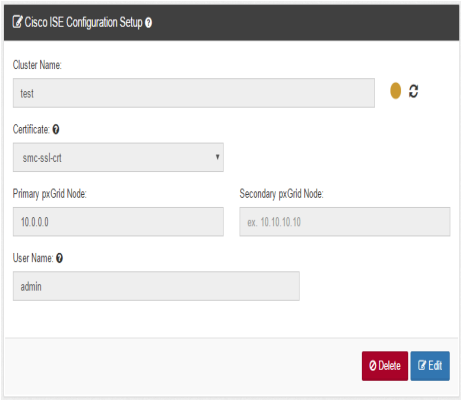
- 複数の独立したCisco ISE クラスタをドメインに追加できます。
- StealthWatch システムにCisco ISE-PIC を追加する手順は、ここで説明しているものと同じです。Cisco ISE-PIC の設定の詳細については、Cisco ISE のマニュアルを参照してください。

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。

© 2019 Cisco Systems, Inc. All Rights Reserved.



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] をクリックします。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。

© 2019 Cisco Systems, Inc. All Rights Reserved.

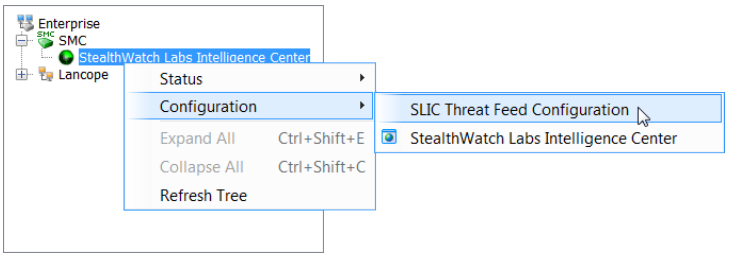
7

SLIC 脅威フィード機能の有効化

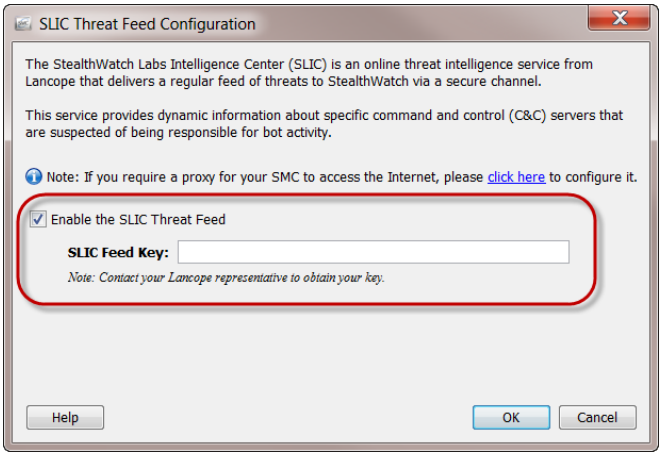
StealthWatch パッケージのインストールと設定の最後の手順は、SMC のクライアントインターフェイスを使用して SLIC 脅威フィードを有効にすることです。

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。



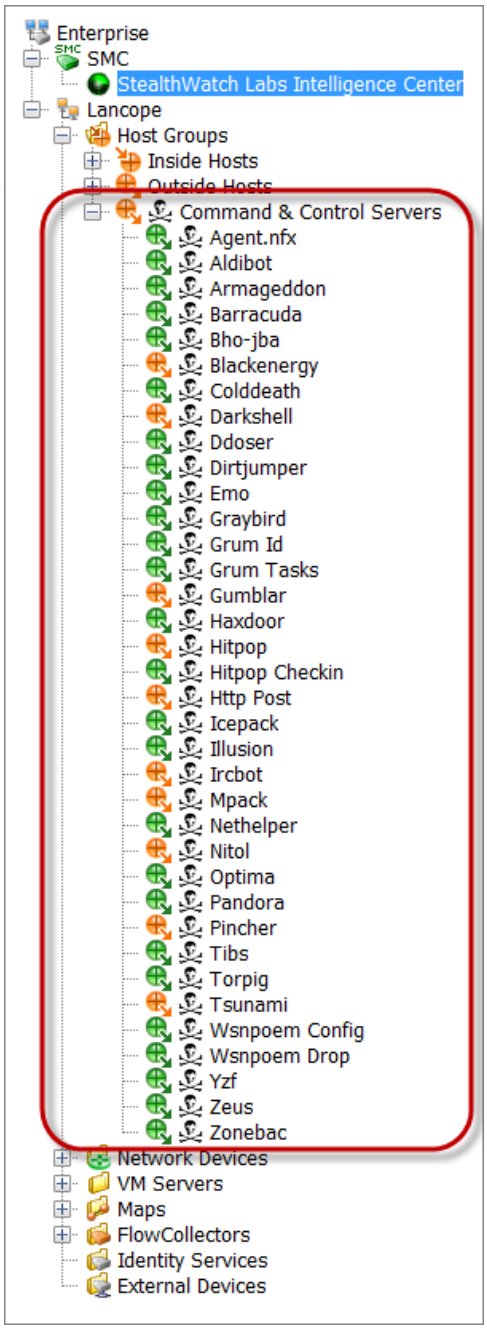
[SLIC脅威 フィード設定 (SLIC Threat Feed Configuration)] ダイアログが表示 されます。



© 2019 Cisco Systems, Inc. All Rights Reserved.

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。



© 2019 Cisco Systems, Inc. All Rights Reserved.

© 2019 Cisco Systems, Inc. All rights reserved.