Cisco Stealthwatch 6.9.x 導入ラボ v1

最終更新日:2017 年 11 月 3 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

制限

dCloud 環境の制限により、導入および設定プロセスの一部がスキップされました。

- このラボでは、Stealthwatch アプライアンスについて、初期 OVF 導入と管理 IP アドレスの割り当て/設定をスキップします。このプロセスは、付録 6 に参照用として記載されています。
- ライセンスに関するプロセスは、ラボおよびライセンス アーキテクチャ上の問題のため、このラボでは対象外とします。

カスタマイズ オプション

このラボの付録では、導入プロセスの一環として実行できる追加のいくつかの機能と手順について説明します。

これには次のものが含まれます。

- ユーザ アカウント管理：アプライアンス管理者パスワードの変更と複数のユーザ ロールの定義
- Cognitive Analytics の有効化：機械学習によるクラウド ベースのネットワーク周辺トラフィック分析を新たに提供するために、Cognitive Analytics との統合を有効化する方法
- UDP Director による FPS のサイジング：導入されたネットワーク環境で FPS ライセンス数をサイジングするために UDP Director を設定して使用する方法

要件

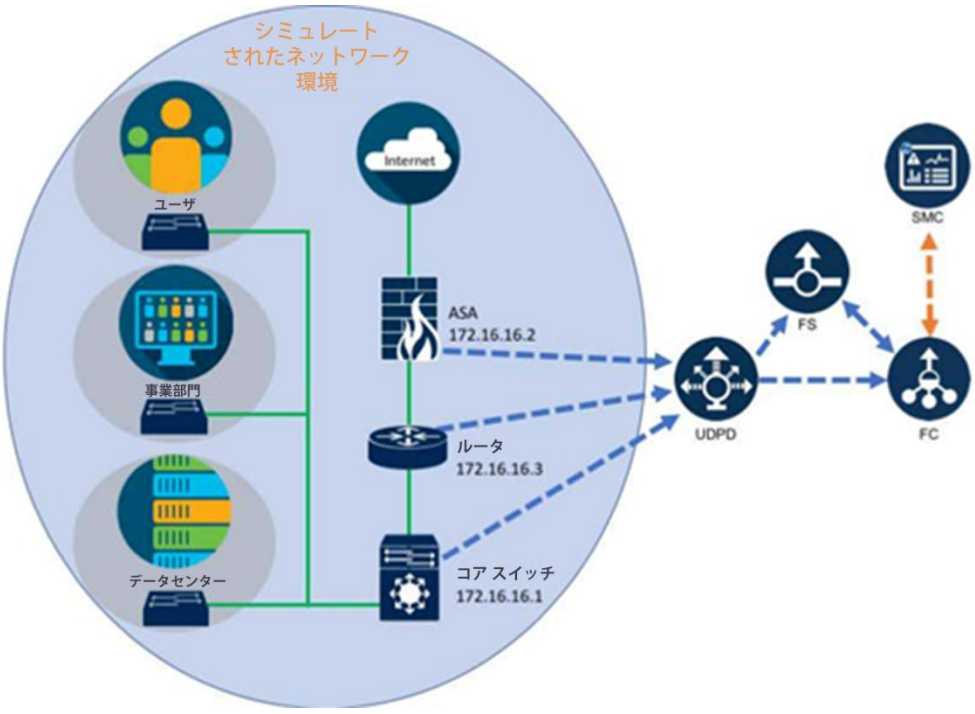
次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
• ラップトップ	• Cisco AnyConnect®

このソリューションについて

この実機によるラボ演習では、基本的な Stealthwatch のインストールを正常に導入するために必要な手法を指導します。記載のラボ シナリオを最後まで実行すれば、シミュレートされたお客様環境に複数の Stealthwatch アプライアンスを導入することになります。



各シナリオでは、ソリューション内のアプライアンスの初期設定を行い、お客様環境に統合するプロセスを体験します。このラボによって、お客様の環境での導入に先立って、Stealthwatch のインストールに習熟することができます。

シナリオとラボ環境では、Stealthwatch Management Console（SMC）、フロー コレクタ（FC）、フロー センサー（FS）、および UDP Director（UDPD）アプライアンスの仮想モデルを使用します。トレーニング ラボを完了したときには、お客様はフル機能の Stealthwatch 環境が得られます。アラームのチューニングは、このトレーニング ラボの対象外です。ただし、応答とユーザ管理については説明します。

Stealthwatch

Cisco Stealthwatch は、ネットワーク データを収集して分析し、最も規模が大きく動的なネットワークに対しても包括的な可視性と保護機能を提供します。Stealthwatch は、シスコと他のベンダーのルータ、スイッチ、ファイアウォールなどのネットワーク デバイスから業界標準の NetFlow データを取得して分析し、内部で拡散するマルウェア、情報漏洩、ボットネット コマンド アンド コントロール トラフィック、ネットワーク調査などの高度で永続的なセキュリティに対する脅威を検出します。Stealthwatch は、ネットワーク トラフィックをキャプチャして分析するセンサーを導入することで、データを作成することもできます。

ネットワークの内部（LAN および境界）のトラフィック パターンを分析して最も複雑なネットワーク脅威を可視化するため、ステルス性の高い巧妙なサイバー攻撃に対抗するための重要なコンポーネントとなります。Cisco Identity Services Engine（ISE）ソリューションでは、ユーザ ID、ユーザ認可レベル、デバイス タイプ、ポスチャなどのコンテキスト（属性）情報によって、Stealthwatch の NetFlow ベースのふるまいを基準にした脅威検出を補強します。Stealthwatch と Cisco ISE を組み合わせることで、ネットワーク セキュリティ アナリストは NetFlow データをコンテキスト情報と合わせて確認できるため、脅威の潜在的な重要度を、低コストの効率的な方法でタイムリーに検出し、識別することができます。

このラボは、Cisco Stealthwatch ソリューションの使用法を理解できるように設計されています。シミュレートされた企業環境で、すでに設定と導入が完了したソリューションを操作できます。

Stealthwatch は、複数のコア コンポーネントとオプション コンポーネントで構成されています。コア コンポーネントは次のとおりです。

- Stealthwatch Management Console
- フロー コレクタ

導入の柔軟性とネットワーク領域に対する可視性を強化するシステムのオプション コンポーネントには、以下のものが含まれます。

- フロー センサー
- UDP Director
- Cognitive Analytics
- プロキシ インジェスション
- エンドポイント ライセンス
- Security Packet Analyzer
- 脅威フィード ライセンス
- Stealthwatch クラウド

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント クレデンシャルは、アクティブ セッションの [トポロジ(Topology)] メニューのコンポーネント アイコンをクリックするか、それらを必要とするシナリオ内の手順を調べることで確認できます。

図 1. dCloud トポロジ

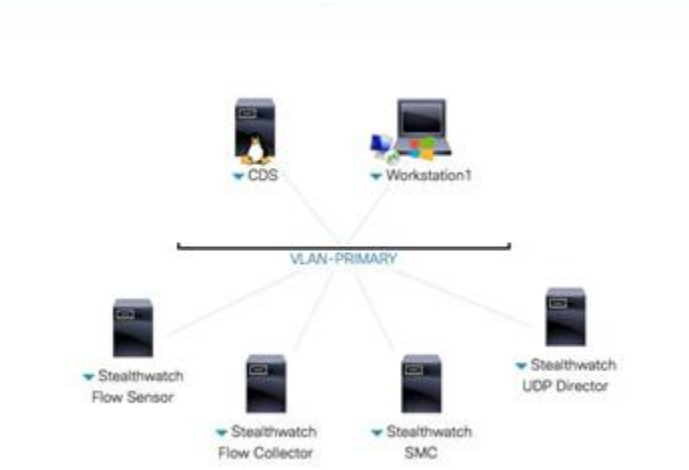


表 2. 機器の詳細

名前	説明	IP アドレス	ユーザ名	パスワード
FS	Stealthwatch Flow Sensor	198.18.128.138	admin	lan411cope
FC	Stealthwatch Flow Collector	198.18.128.137	admin	lan411cope
SMC	Stealthwatch Management Console	198.18.128.136	admin	lan411cope
UDPD	Stealthwatch UDP Director	198.18.128.139	admin	lan411cope
Workstation1	Windows 7	198.18.133.36	administrator	C1sco12345
CDS	ネットワーク トラフィック エミュレータ	198.18.128.134	root	lan1cope

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るために、**Cisco AnyConnect VPN** [手順を見る] および**ラップトップのローカル RDP クライアント** [手順を見る] を使用してワークステーションに接続します。
   - ワークステーション1:**198.18.133.36**、ユーザ名:**administrator**、パスワード:**C1sco12345**

注: Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] 。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。

3. ワークステーションに接続したら、シミュレートされたネットワーク環境を起動して、dCloud Stealthwatch 導入用のネットワーク トラフィック テレメトリが生成されることを確認する必要があります。
4. ワークステーションのデスクトップにある [トラフィックの開始(Start Traffic)] ショートカットを見つけます。ショートカットをダブルクリックして、有効化します。

5. ワークステーションのタスクバーに最小化された PuTTY ウィンドウがある場合、トラフィックの生成は正しく機能しています。**このウィンドウを開いたまま**、演習を開始します。

シナリオ 1.　Stealthwatch アプライアンス セットアップ ツール

重要:ラボを開始する前に、dCloud ワークステーションのデスクトップで [トラフィックの開始(Start Traffic)] リンクを起動していることを確認してください。起動していないと、シミュレートされたネットワーク環境では演習用のテレメトリが適切に生成されない場合があります。詳細は「はじめに」セクションをご覧ください。

ほとんどのお客様は、社内スタッフがアプライアンスの物理的なインストールや、仮想アプライアンスのプロビジョニングを行います。こうしたお客様の取り組みを支援するために、お客様の各種の社内チームに、製品のドキュメントや、物理/仮想ネットワーキング ポートに関するガイダンスを提供する必要があります。また、IP の初期設定プロセスの支援を依頼される場合もあります。

Stealthwatch アプライアンスは、お客様のデータセンター チームによってすでに管理 IP アドレスが割り当てられ、設定されています。

注:OVF 導入手順については、付録 6 を参照してください。

ここで dCloud セッション内のワークステーションから管理 IP アドレスでアプライアンスにアクセスし、アプライアンス セットアップ ツール(AST)ウィザードを完了します。

注:AST プロセスはそれぞれのアプライアンスで非常に似ていますが、適切に機能させるには、すべてのアプライアンスで AST プロセスを完了してから、残りの設定手順を進める必要があります。

Stealthwatch アプライアンスで IP の初期設定を行う場合、通常は、コンソールから物理アプライアンスまたは VM の画面にアクセスします。それにより AST ウィザードがネットワーク インターフェイスを通じて起動します。また、デフォルトの IP アドレスを通じて、各 Stealthwatch アプライアンスの管理イーサネット アダプタに直接物理的に接続し、AST を実行して、コンソール レベルの管理ネットワーキング設定を行うことなく IP アドレスを設定できます。

アプライアンス セットアップ ツールを完了すると、アプライアンスがお客様環境内のその他の Stealthwatch 導入と通信できるように設定されます。アプライアンスでは、次の順序で AST を完了します。

1. フロー センサー(FS)
2. UDP Director(UDPD)
3. フロー コレクタ(FC)
4. Stealthwatch Management Console(SMC)

注:アプライアンスをこの順序で設定することで、NetFlow の生成と処理を実行するアプライアンスが、そのデータに依存するアプライアンスを設定する前に適切に設定され、機能するようになります。フロー センサー アプライアンスは、専用のキャプチャ インターフェイスでキャプチャされたネットワーク トラフィックに基づいて NetFlow レコードを作成し、そのデータを処理するためにフロー コレクタに送信します。UDP Director(UDPD)は NetFlow エクスポータからフロー データを取得し、FC に転送します。処理するフロー データがすべて FC に保存されることで、Stealthwatch Management Console(SMC)が FC を適切に管理し、保存されたフロー データにアクセスできるように設定できます。

アプライアンスの設定に備えて、ネットワーク環境について以下の情報を収集しておく必要があります。

- DNS サーバ IP
- NTP サーバ IP
- お客様環境（DMZ を含む内部ネットワーク）に属する IP アドレス範囲
- Stealthwatch アプライアンスに使用する IP アドレス
- SMTP リレー サーバ（必要に応じて）
- 特定ホストの IP または IP 範囲のリスト（場所、サーバ タイプ、アプリケーション、認可されたネットワーク スキャナなどを含む）
- DNS：
    - 198.18.128.1
    - 198.18.128.134
- NTP：
    - 198.18.128.1
- お客様の IP アドレス範囲：
    - 10.0.0.0/8
    - 192.168.0.0/16
    - 172.16.0.0/12
    - fc00::/7
    - 209.182.184.0/24
- Stealthwatch アプライアンスの IP アドレス：
    - 198.18.128.136（Management Console（SMC））
    - 198.18.128.137（Flow Collector（FC））
    - 198.18.128.138（Flow Sensor（FS））
    - 198.18.128.139（UDP Director（UDPD））
- SMTP リレー サーバ
    - 198.18.128.134

表 3. 具体的な IP アドレス（範囲）

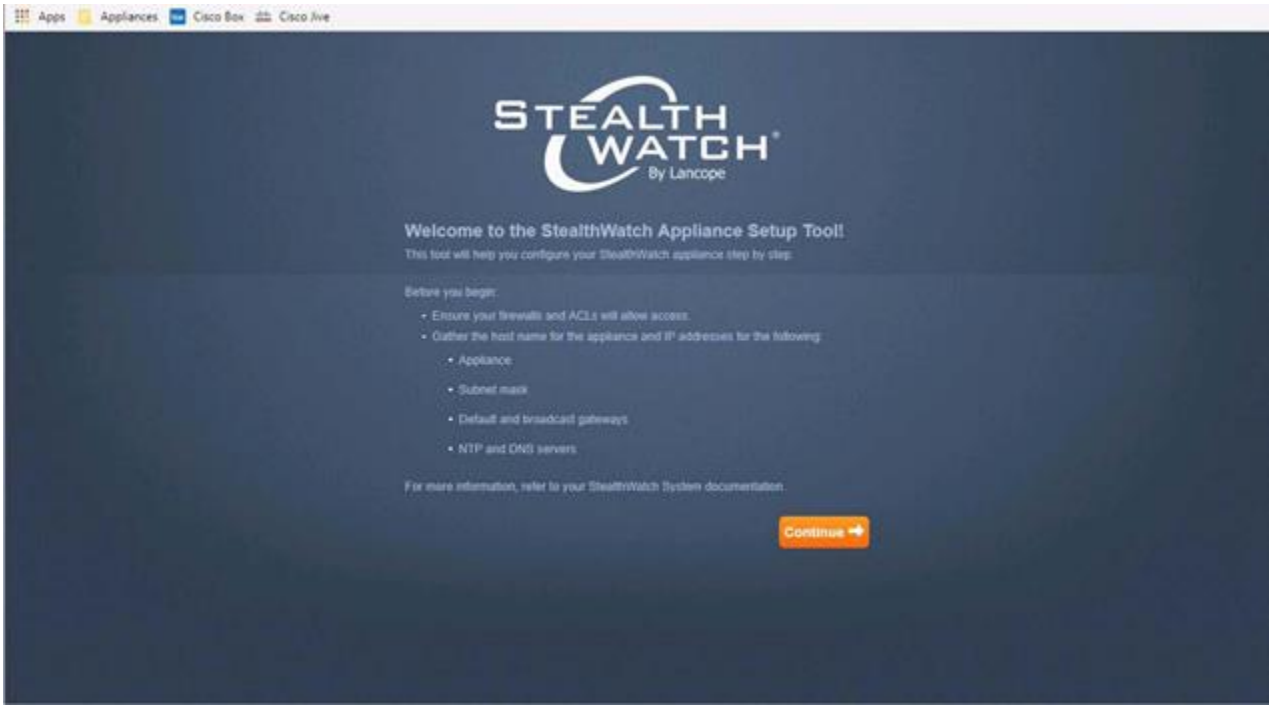
説明	IP アドレス範囲
DNS サーバ	10.10.30.15
DNS サーバ	10.10.30.16
脆弱性スキャナ	10.203.0.207
メール サーバ	10.10.30.23
タイム/NTP サーバ	10.10.30.10
パブリック IP アドレス空間	209.182.184.0/24
Atlanta ホスト	10.201.0.0/16
PCI デバイス	10.201.3.0/24

手順

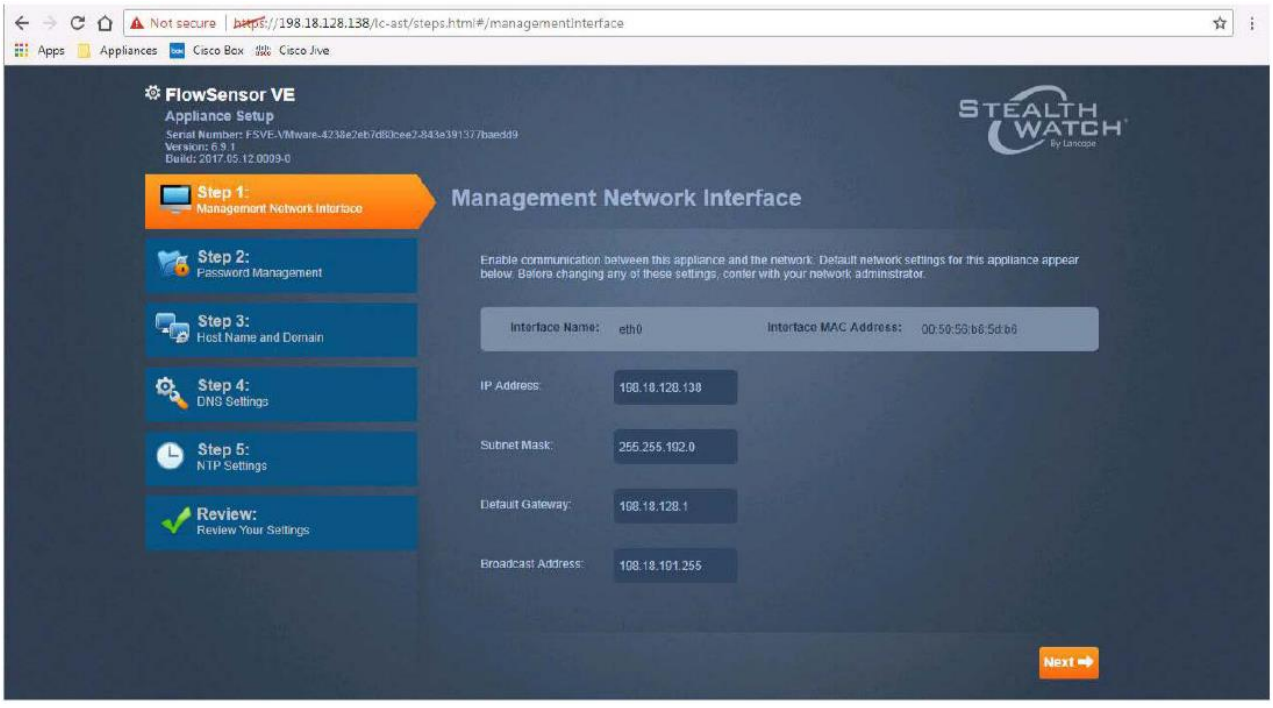
Stealthwatch Flow Sensor

1. 関連付けられている VPN トンネル経由でリモート デスクトップから、または dCloud に含まれるリモート デスクトップの Web ベース機能を使用して、dCloud セッション内のワークステーションに接続します。
2. リモート ワークステーションのデスクトップで、Chrome Web ブラウザのショートカットをダブルクリックして開きます。
3. URL フィールドで「https://198.18.128.138」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [FS] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
4. Stealthwatch アプライアンスでは、信頼されていない自己署名証明書をデフォルトで使用して、ブラウザ セキュリティ警告が生成されます。Chrome でブラウザ セキュリティ警告が表示されたら、[詳細設定（ADVANCED）] オプションをクリックし、[続行（Proceed）] リンクをクリックして、アプライアンス管理ページに進みます。
5. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード lan411cope を使用して、フロー センサー アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：lan411cope

6. AST のウェルカム ページが表示されます。[続行（Continue）] ボタンを押して進みます。



7. [管理ネットワーク インターフェイス（Management Network Interface）] 画面が表示されます。すべての設定が正しいことを確認しているので、変更を加える必要はありません。[次へ（Next）] ボタンをクリックして続行します。



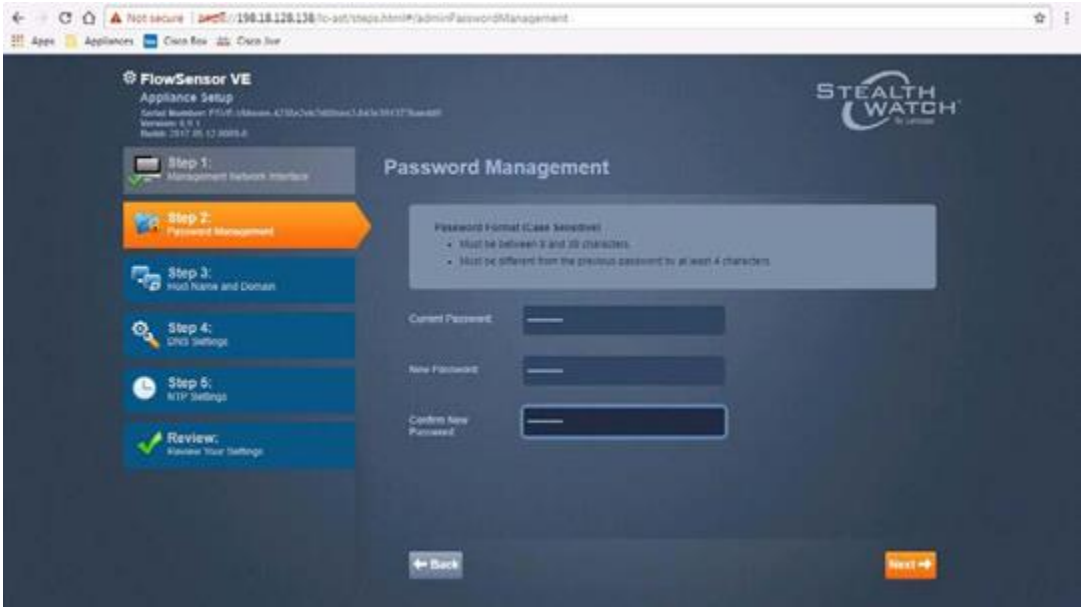
注：このページでは、あなたがオンサイトに到着する前にアプライアンスをラックに設置し、事前設定を行ったお客様が、間違った IP アドレスをアプライアンスに入力していないかどうかを確認できます。たとえば、Stealthwatch アプライアンスで使用する予定の IP アドレスが 4 つある場合は、その 4 つのうち正しい IP アドレスがフロー センサーに割り当てられていることを確認してください。

8. [パスワード管理（Password Management）] 画面が表示されます。デフォルトのパスワード lan411cope を新しいパスワード C1sco12345 に変更します。変更したら、[次へ（Next）] をクリックして続行します。

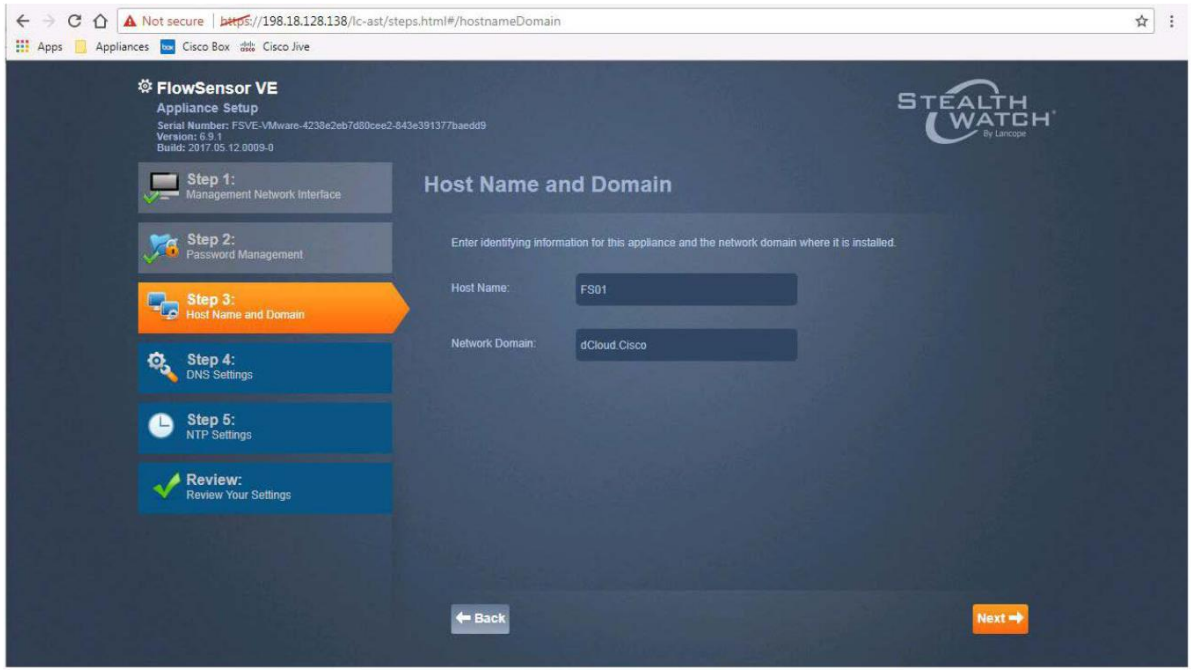
    a. [現在のパスワード（Current Password）]：lan411cope

    b. [新しいパスワード（New Password）]：C1sco12345

    c. [新しいパスワードの確認（Confirm New Password）]：C1sco12345

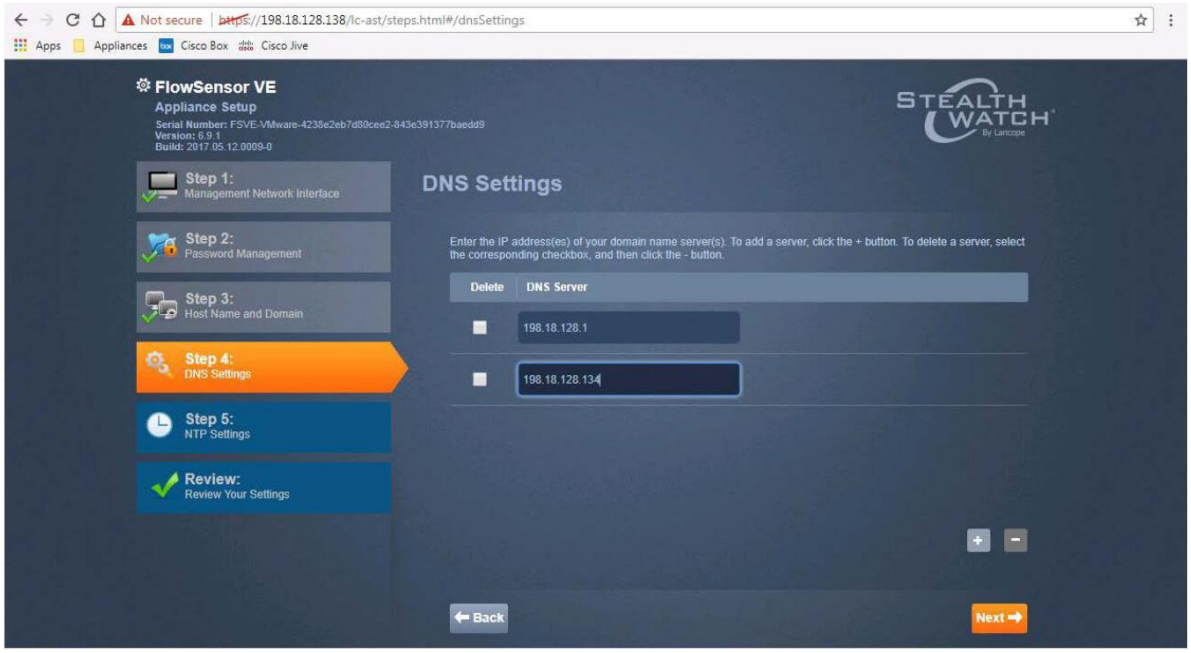


9. [ホスト名とドメイン（Host Name and Domain）] 画面が表示されます。[ホスト名（Host Name）] フィールドと [ネットワークドメイン（Network Domain）] フィールドは自動入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



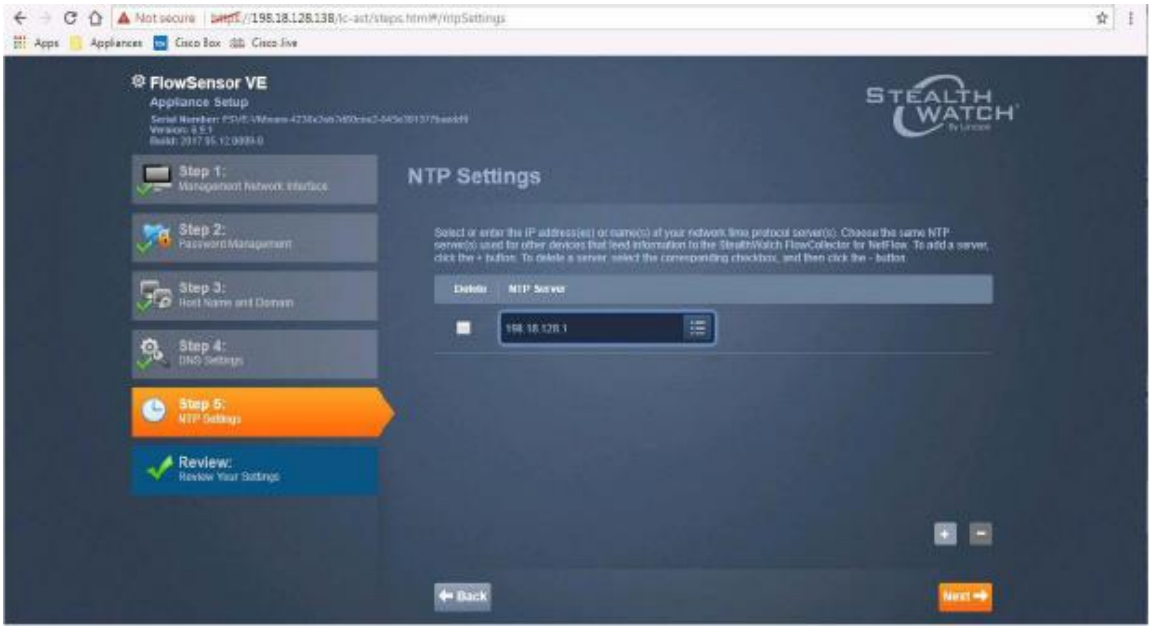
注：お客様の実稼働環境の導入では、その環境に適切なホスト名と DNS ドメイン名を入力します。

10. [DNS 設定（DNS Settings）] 画面が表示されます。この環境の DNS サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



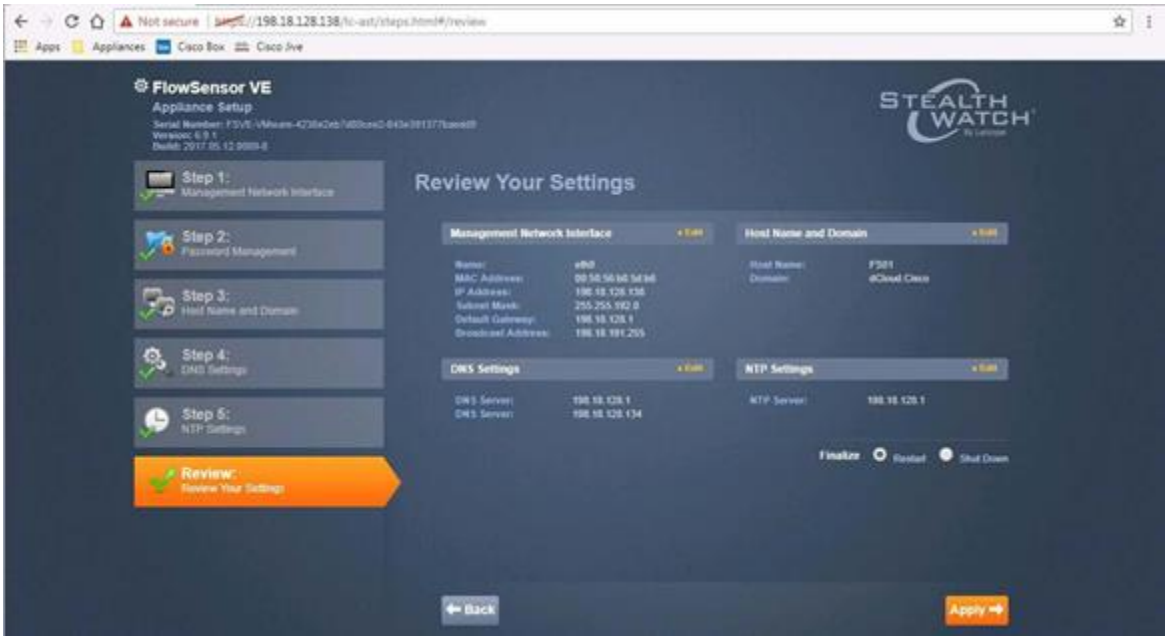
注：お客様の実稼働環境の導入では、その環境に適切な DNS サーバの IP アドレスを入力します。[次へ（Next）] ボタンをクリックして続行します。

11. [NTP 設定（NTP Settings）] 画面が表示されます。この環境の NTP サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



注：お客様の実稼働環境の導入では、その環境に適切な NTP サーバの IP アドレスを入力します。導入環境内のすべての Stealthwatch アプライアンスを、同じ NTP サーバと同期するように設定する必要があります。デバイス間の時刻の不一致が原因で機能にエラーが生じる可能性があります。

12. [設定の確認（Review Your Settings）] 画面が表示されます。アプライアンスに設定を適用する前に値を編集する必要がある場合は、ここで前に戻って変更してください。今回は変更の必要はありません。[確定（Finalize）] が [再起動（Restart）] に設定されていることを確認し、[適用（Apply）] ボタンをクリックします。

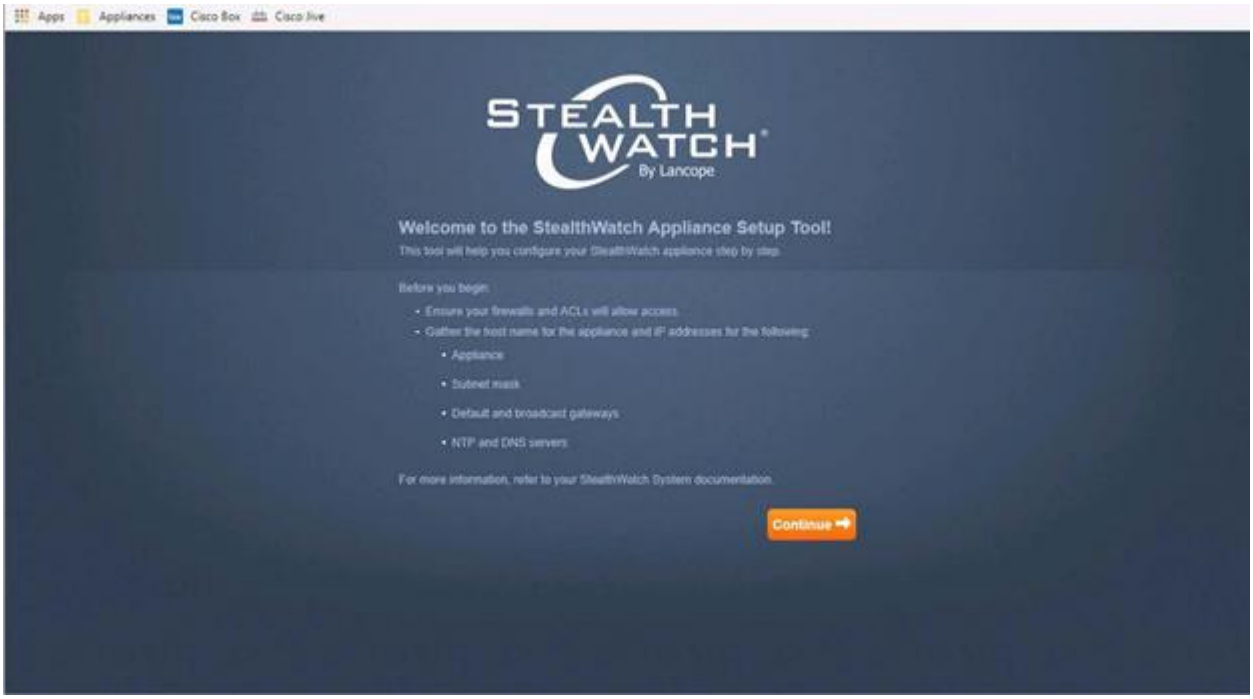


13. アプライアンスの再起動のプロンプトが表示されたら、[OK] ボタンをクリックして再起動を確定します。
14. 次のアプライアンスの AST 設定に進みます。

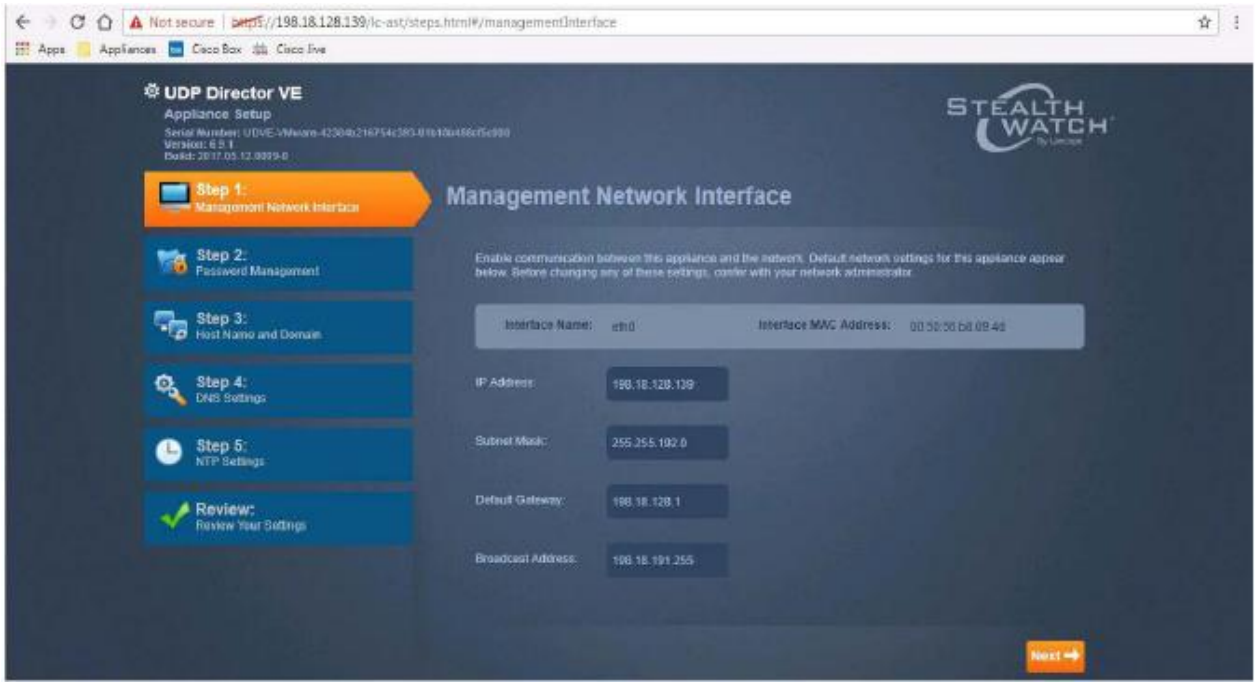
Stealthwatch UDP Director

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.139」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [UDPD] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. Stealthwatch アプライアンスでは、信頼されていない自己署名証明書をデフォルトで使用して、ブラウザ セキュリティ警告が生成されます。Chrome でブラウザ セキュリティ警告が表示されたら、[詳細設定（ADVANCED）] オプションをクリックし、[続行（Proceed）] リンクをクリックして、アプライアンス管理ページに進みます。
4. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード lan411cope を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：lan411cope

5. AST のウェルカム ページが表示されます。[続行（Continue）] ボタンを押して進みます。



6. [管理ネットワーク インターフェイス（Management Network Interface）] 画面が表示されます。すべての設定が正しいことを確認しているので、変更を加える必要はありません。[次へ（Next）] ボタンをクリックして続行します。



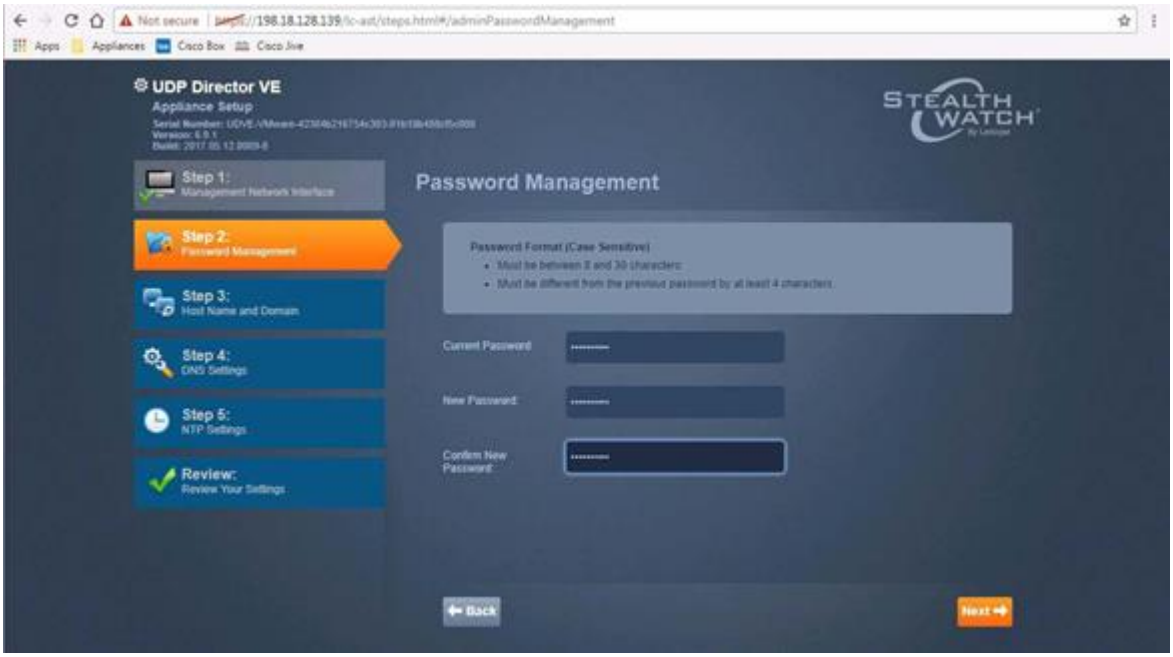
注：このページでは、あなたがオンサイトに到着する前にアプライアンスをラックに設置し、事前設定を行ったお客様が、間違った IP アドレスをアプライアンスに入力していないかどうかを確認できます。たとえば、Stealthwatch アプライアンスで使用する予定の IP アドレスが 4 つある場合は、その 4 つのうち正しい IP アドレスがフロー センサーに割り当てられていることを確認してください。

7. [パスワード管理（Password Management）] 画面が表示されます。デフォルトのパスワード lan411cope を新しいパスワード C1sco12345 に変更します。変更したら、[次へ（Next）] ボタンをクリックして続行します。

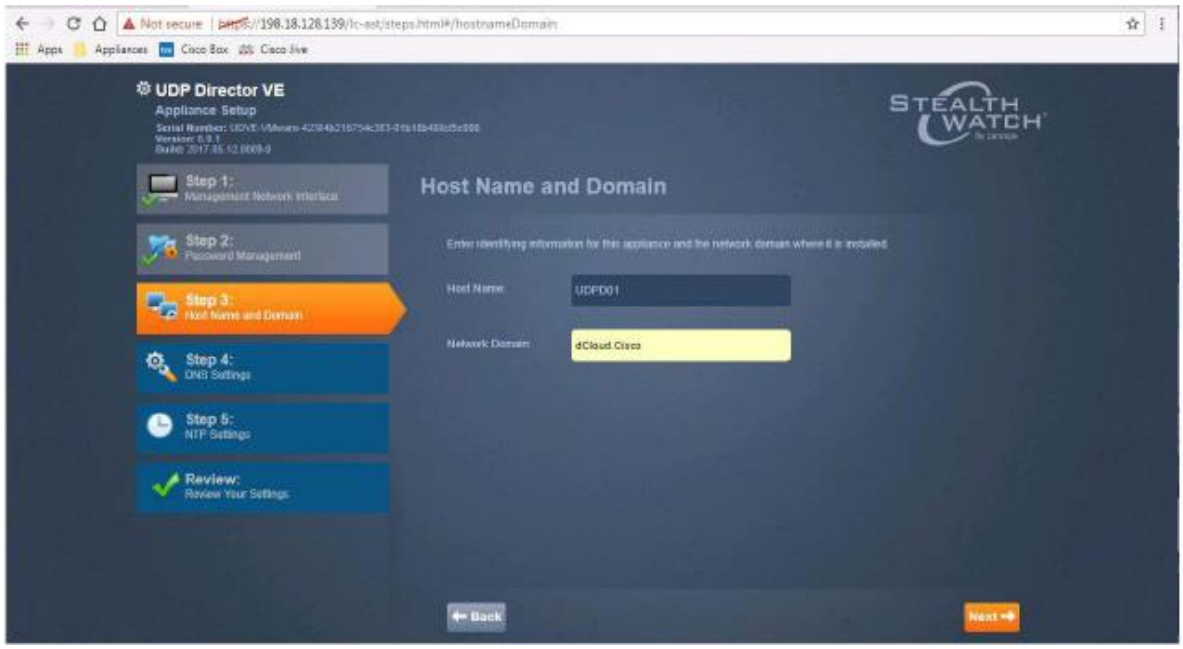
    a. [現在のパスワード（Current Password）]：lan411cope

    b. [新しいパスワード（New Password）]：C1sco12345

    c. [新しいパスワードの確認（Confirm New Password）]：C1sco12345

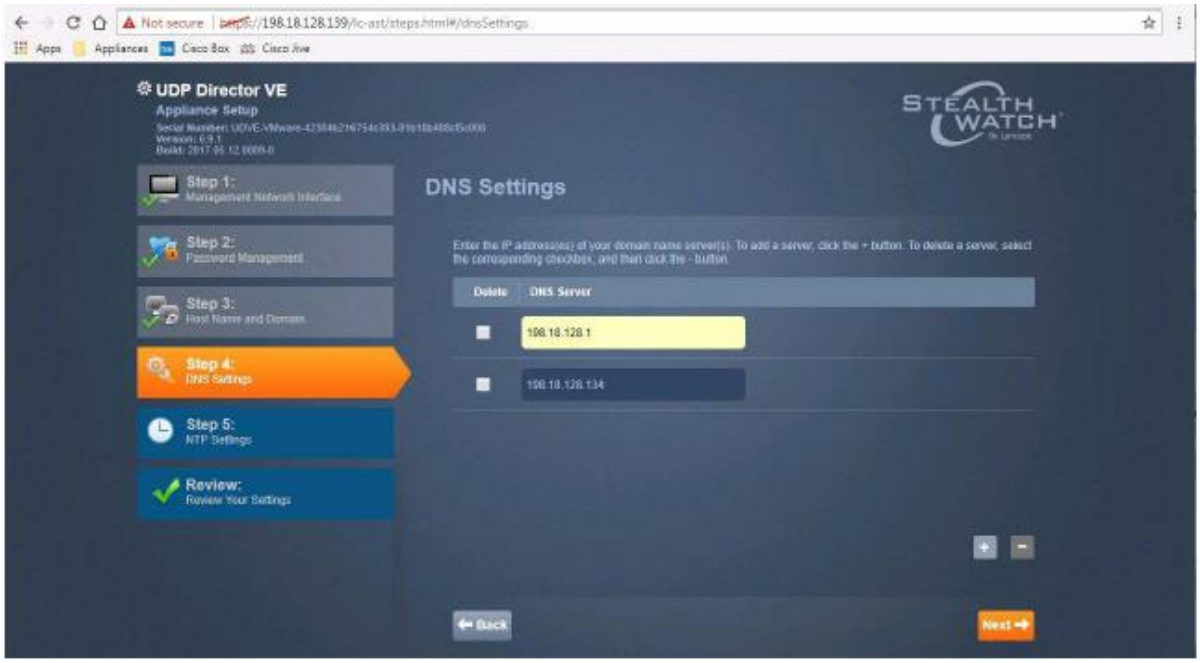


8. [ホスト名とドメイン（Host Name and Domain）] 画面が表示されます。[ホスト名（Host Name）] フィールドと [ネットワークドメイン（Network Domain）] フィールドは自動入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



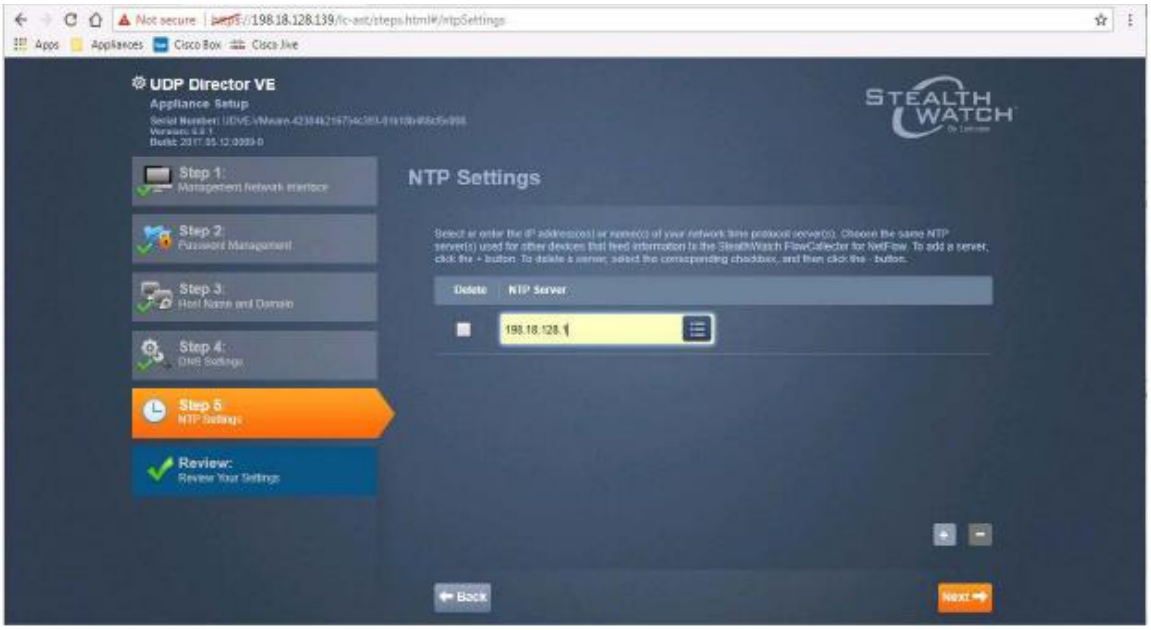
注：お客様の実稼働環境の導入では、その環境に適切なホスト名と DNS ドメイン名を入力します。

9. [DNS 設定（DNS Settings）] 画面が表示されます。この環境の DNS サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



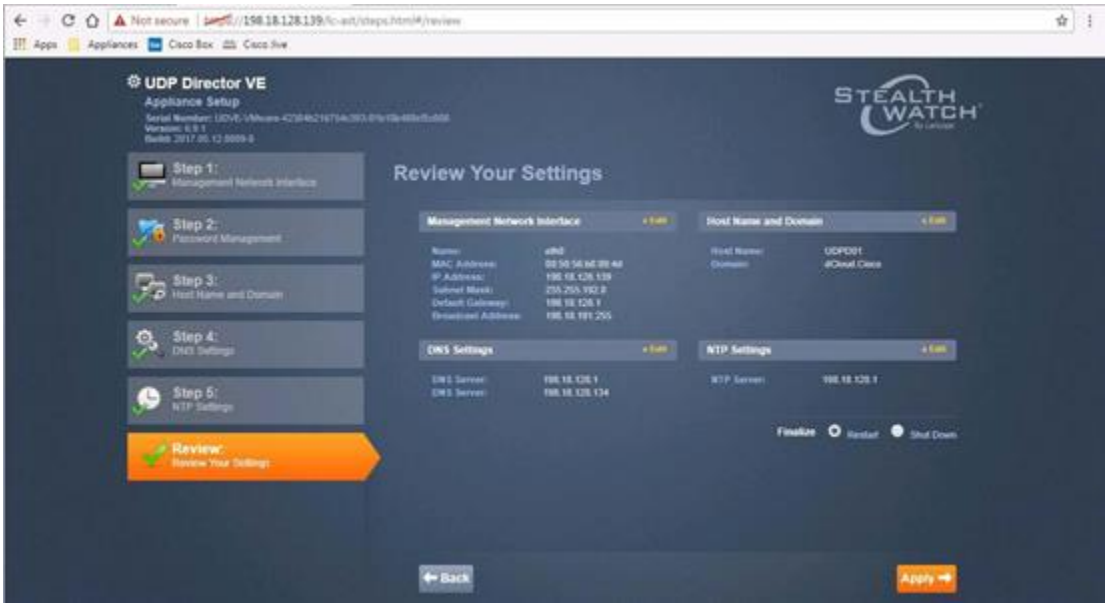
注：お客様の実稼働環境の導入では、その環境に適切な DNS サーバの IP アドレスを入力します。

10. [NTP 設定（NTP Settings）] 画面が表示されます。この環境の NTP サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



注：お客様の実稼働環境の導入では、その環境に適切な NTP サーバの IP アドレスを入力します。導入環境内のすべての Stealthwatch アプライアンスを、同じ NTP サーバと同期するように設定する必要があります。デバイス間の時刻の不一致が原因で機能にエラーが生じる可能性があります。

11. [設定の確認（Review Your Settings）] 画面が表示されます。アプライアンスに設定を適用する前に値を編集する必要がある場合は、ここで行うことができます。今回は変更の必要はありません。[確定（Finalize）] が [再起動（Restart）] に設定されていることを確認し、[適用（Apply）] ボタンをクリックします。

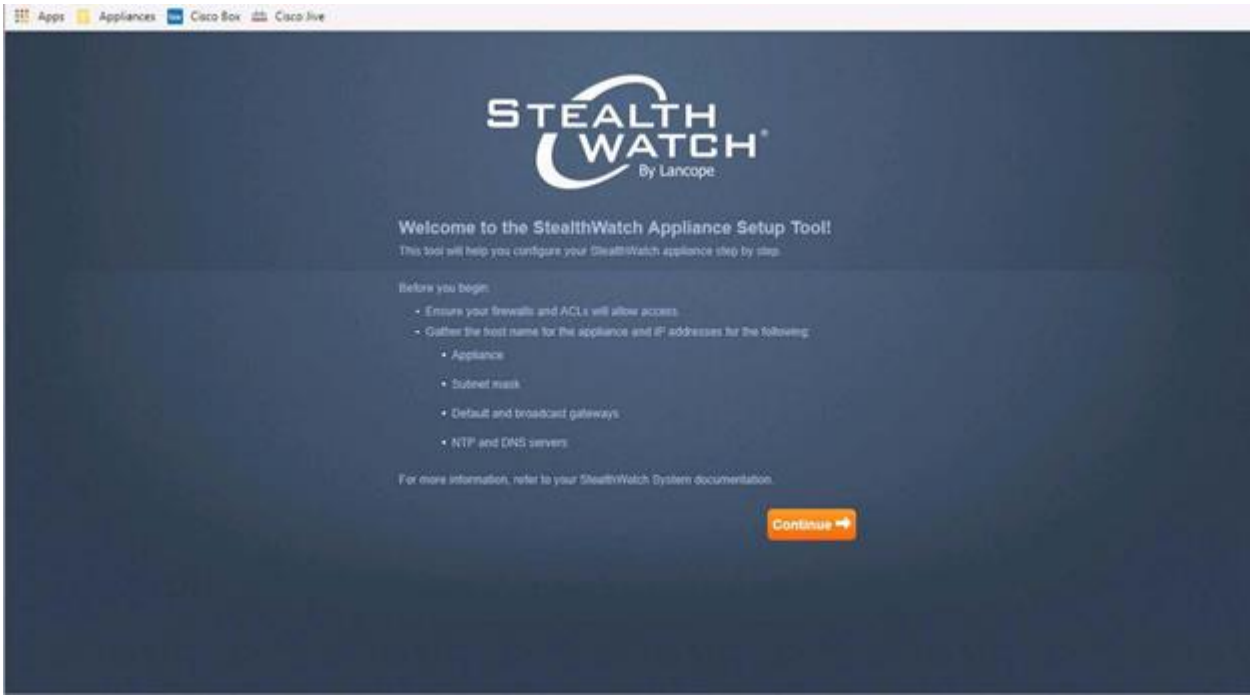


12. アプライアンスの再起動のプロンプトが表示されたら、[OK] ボタンをクリックして再起動を確定します。
13. これで、次のアプライアンスの AST 設定に進むことができます。

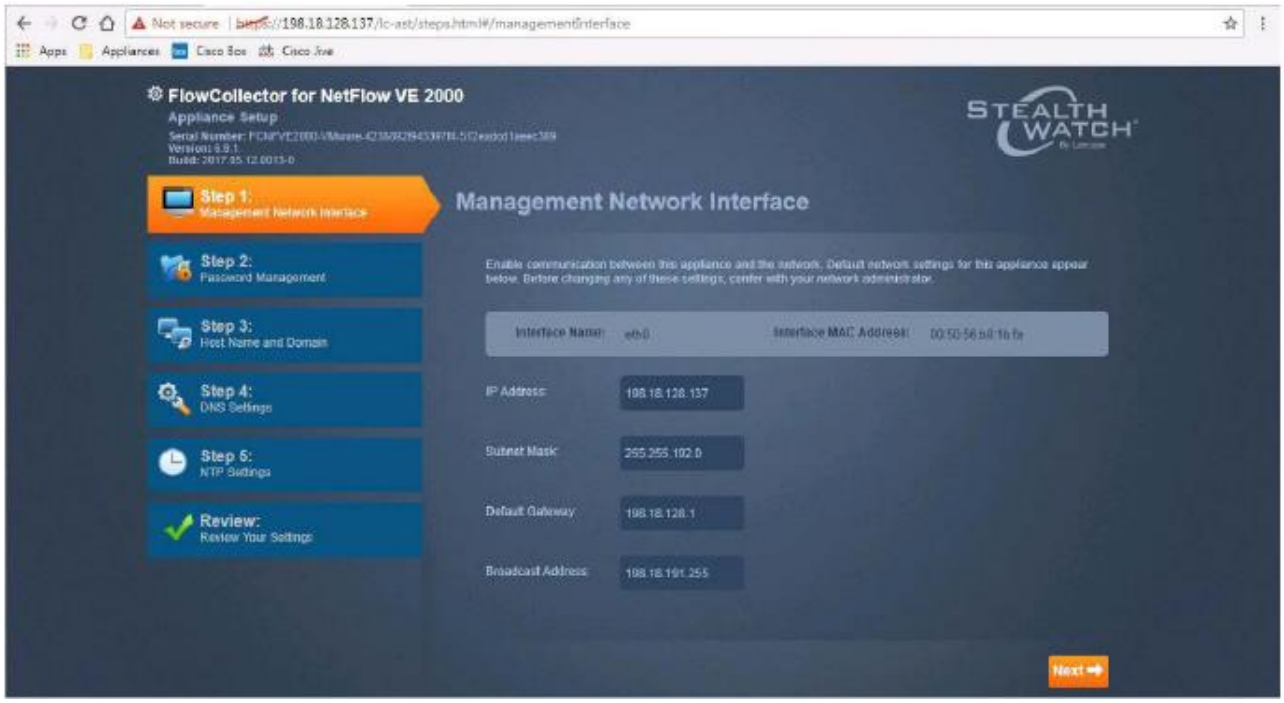
Stealthwatch Flow Collector

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.137」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [FCNF] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. Stealthwatch アプライアンスでは、信頼されていない自己署名証明書をデフォルトで使用して、ブラウザ セキュリティ警告が生成されます。Chrome でブラウザ セキュリティ警告が表示されたら、[詳細設定（ADVANCED）] オプションをクリックし、[続行（Proceed）] リンクをクリックして、アプライアンス管理ページに進みます。
4. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード lan411cope を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：lan411cope

5. AST のウェルカム ページが表示されます。[続行（Continue）] ボタンを押して進みます。



6. [管理ネットワーク インターフェイス（Management Network Interface）] 画面が表示されます。すべての設定が正しいことを確認しているので、変更を加える必要はありません。[次へ（Next）] ボタンをクリックして続行します。



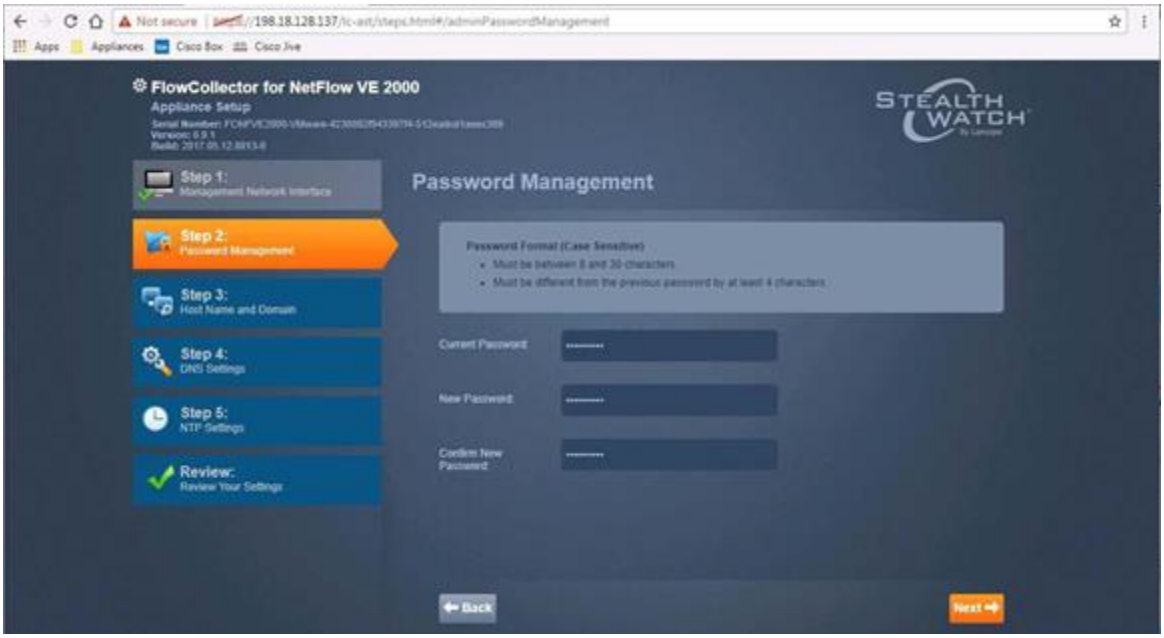
注：このページでは、あなたがオンサイトに到着する前にアプライアンスをラックに設置し、事前設定を行ったお客様が、間違った IP アドレスをアプライアンスに入力していないかどうかを確認できます。たとえば、Stealthwatch アプライアンスで使用する予定の IP アドレスが 4 つある場合は、その 4 つのうち正しい IP アドレスがフロー センサーに割り当てられていることを確認してください。

7. [パスワード管理（Password Management）] 画面が表示されます。デフォルトのパスワード lan411cope を新しいパスワード C1sco12345 に変更します。[次へ（Next）] ボタンをクリックして続行します。

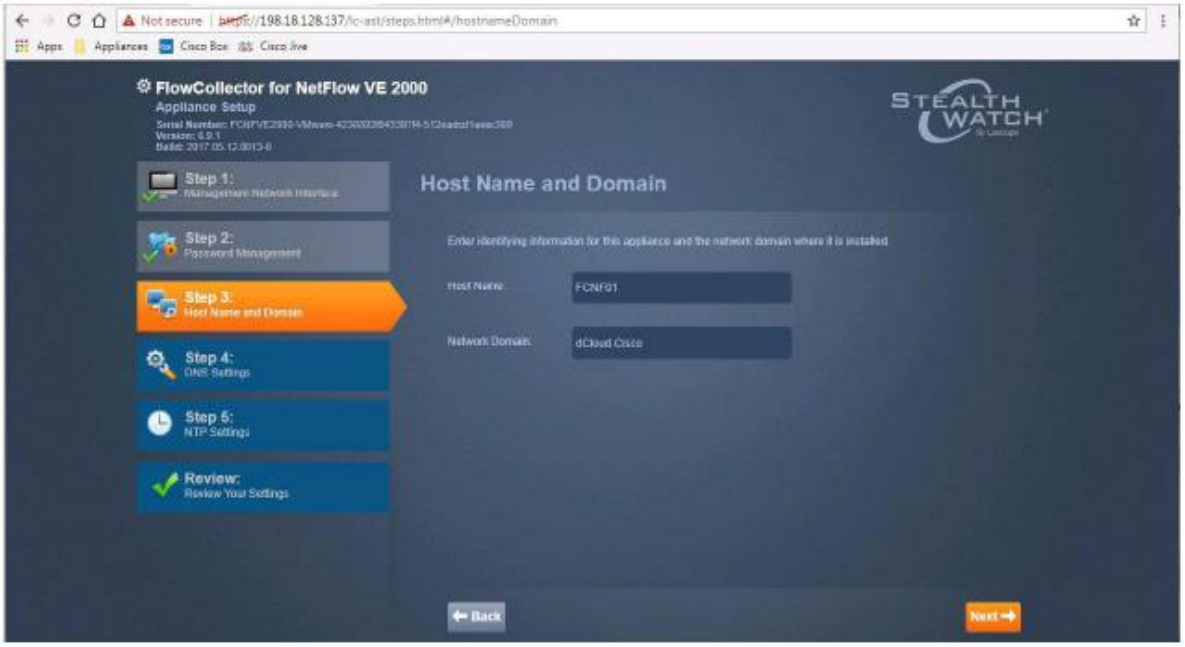
    a. [現在のパスワード（Current Password）]：lan411cope

    b. [新しいパスワード（New Password）]：C1sco12345

    c. [新しいパスワードの確認（Confirm New Password）]：C1sco12345

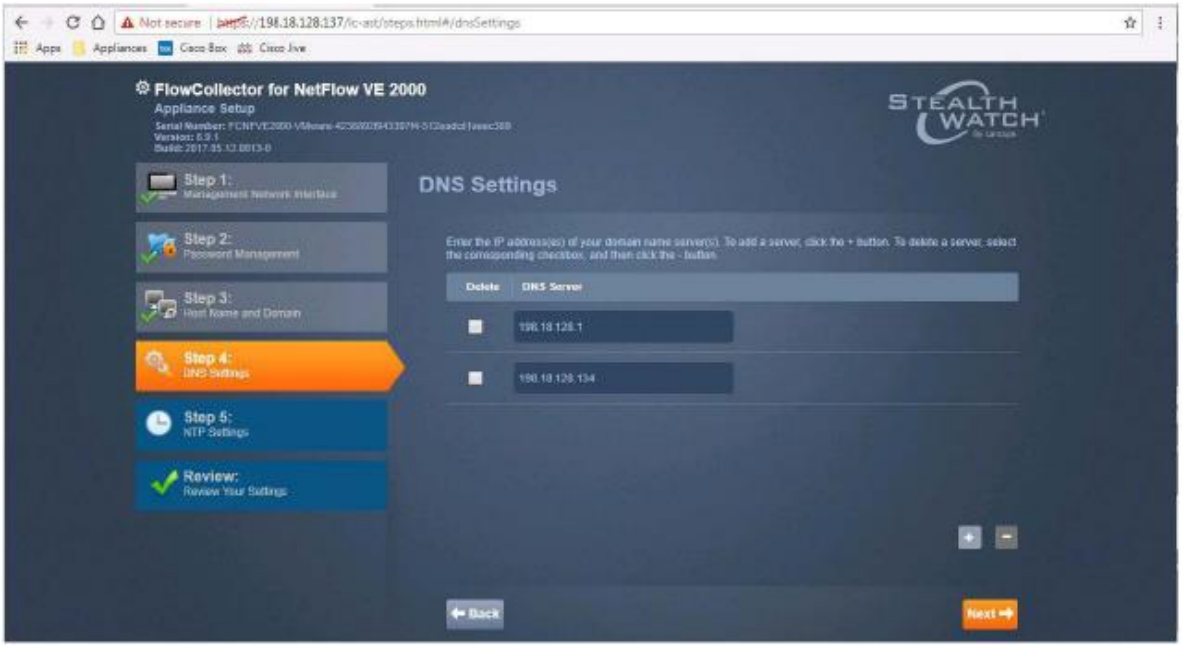


8. [ホスト名とドメイン（Host Name and Domain）] 画面が表示されます。[ホスト名（Host Name）] フィールドと [ネットワークドメイン（Network Domain）] フィールドは自動入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



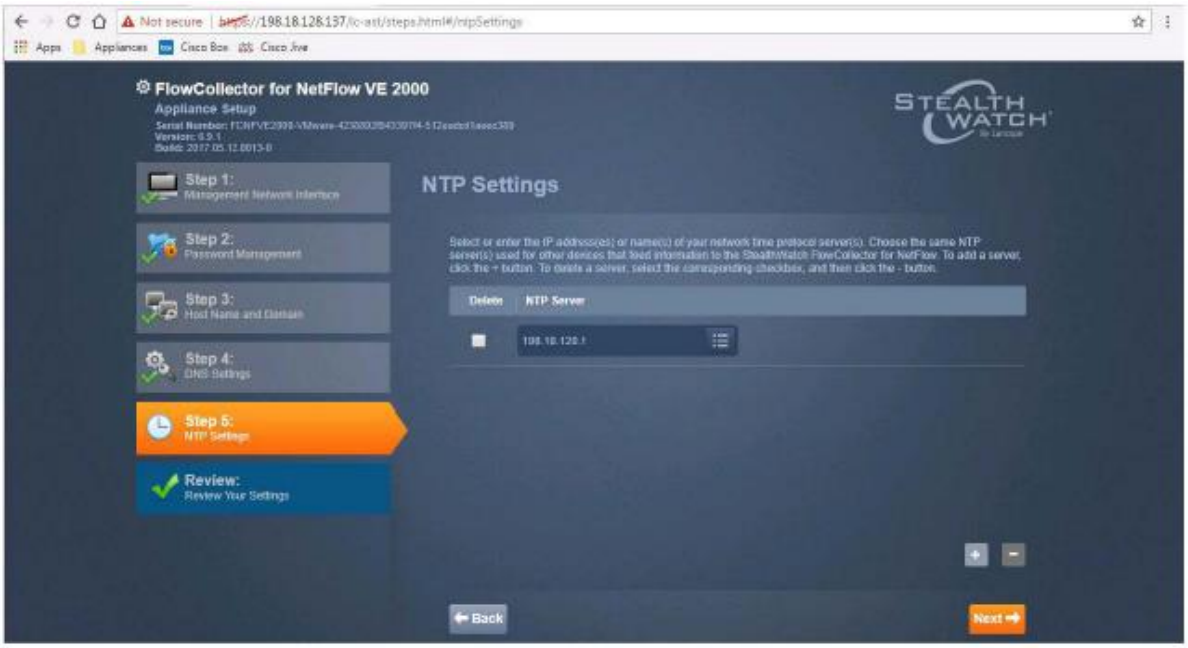
注：お客様の実稼働環境の導入では、その環境に適切なホスト名と DNS ドメイン名を入力します。

9. [DNS 設定（DNS Settings）] 画面が表示されます。この環境の DNS サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



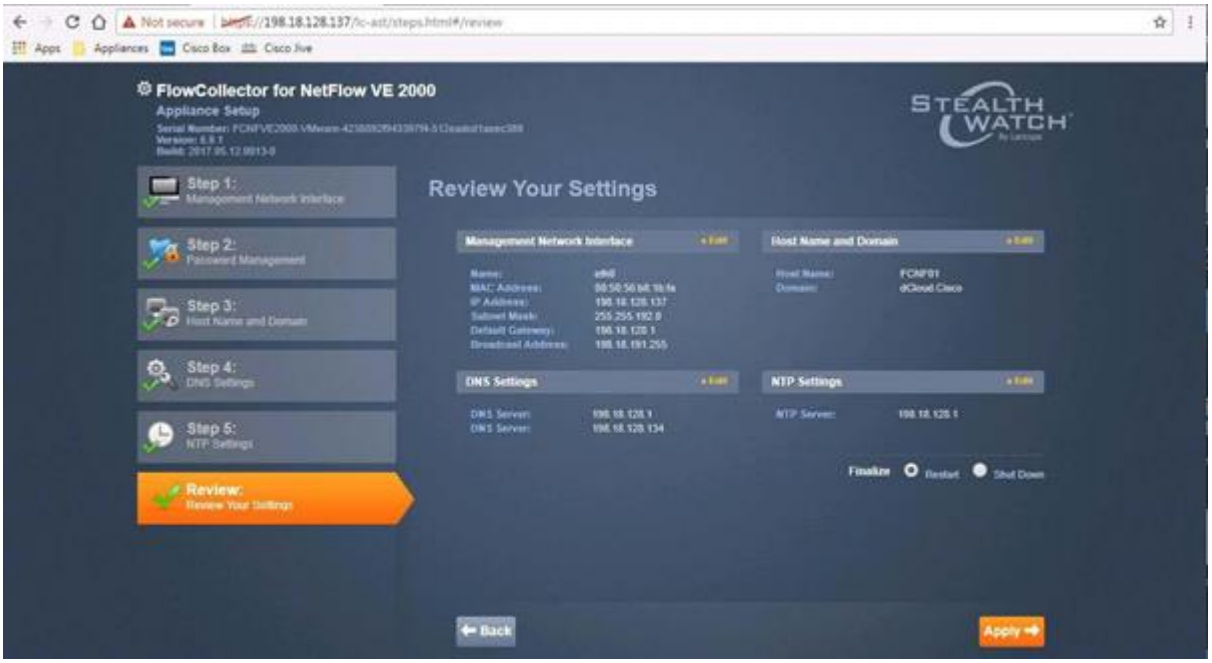
注：お客様の実稼働環境の導入では、その環境に適切な DNS サーバの IP アドレスを入力します。

10. [NTP 設定（NTP Settings）] 画面が表示されます。この環境の NTP サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



注：お客様の実稼働環境の導入では、その環境に適切な NTP サーバの IP アドレスを入力します。導入環境内のすべての Stealthwatch アプライアンスを、同じ NTP サーバと同期するように設定する必要があります。デバイス間の時刻の不一致が原因で機能にエラーが生じる可能性があります。

11. [設定の確認（Review Your Settings）] 画面が表示されます。アプライアンスに設定を適用する前に値を編集する必要がある場合は、ここで行うことができます。今回は変更の必要はありません。[確定（Finalize）] が [再起動（Restart）] に設定されていることを確認し、[適用（Apply）] ボタンをクリックします。



12. アプライアンスの再起動のプロンプトが表示されたら、[OK] ボタンをクリックして再起動を確定します。

Stealthwatch Management Console

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.136/」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

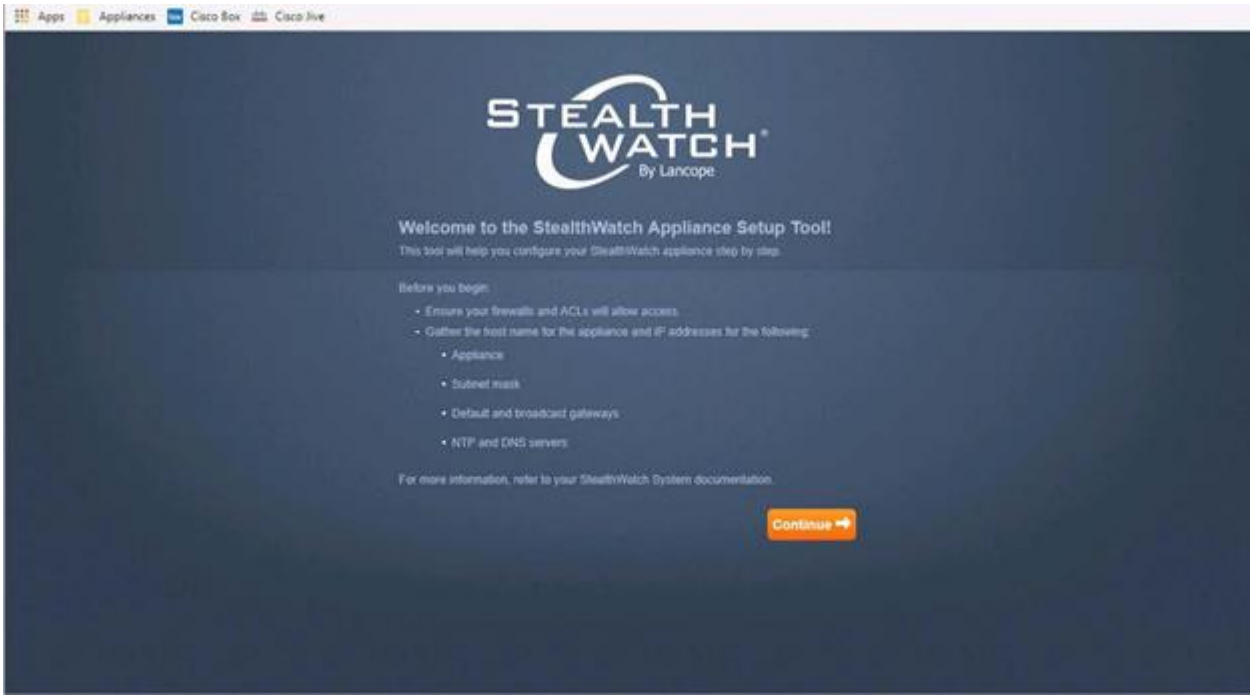
   a. SMC アプライアンスにログインしても AST ウィザードが表示されない場合は、URL https://198.18.128.136/lc-ast をブラウザのアドレスバーに手動で入力して、AST ウィザードを開きます。

3. Stealthwatch アプライアンスでは、信頼されていない自己署名証明書をデフォルトで使用して、ブラウザ セキュリティ警告が生成されます。Chrome でブラウザ セキュリティ警告が表示されたら、[詳細設定（ADVANCED）] オプションをクリックし、[続行（Proceed）] リンクをクリックして、アプライアンス管理ページに進みます。
4. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード lan411cope を使用して、アプライアンスにログインします。

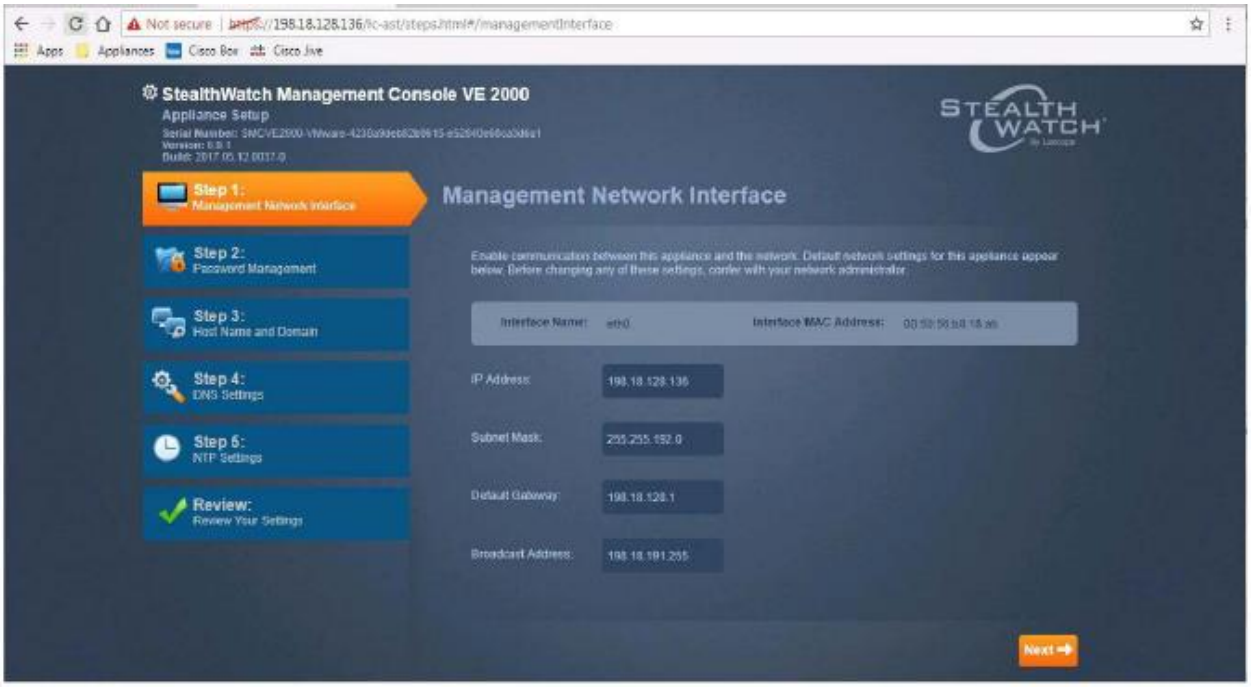
   a. ユーザ名：admin

   b. パスワード：lan411cope

5. AST のウェルカム ページが表示されます。[続行（Continue）] ボタンを押して進みます。



6. [管理ネットワーク インターフェイス（Management Network Interface）] 画面が表示されます。すべての設定が正しいことを確認しているので、変更を加える必要はありません。[次へ（Next）] ボタンをクリックして続行します。



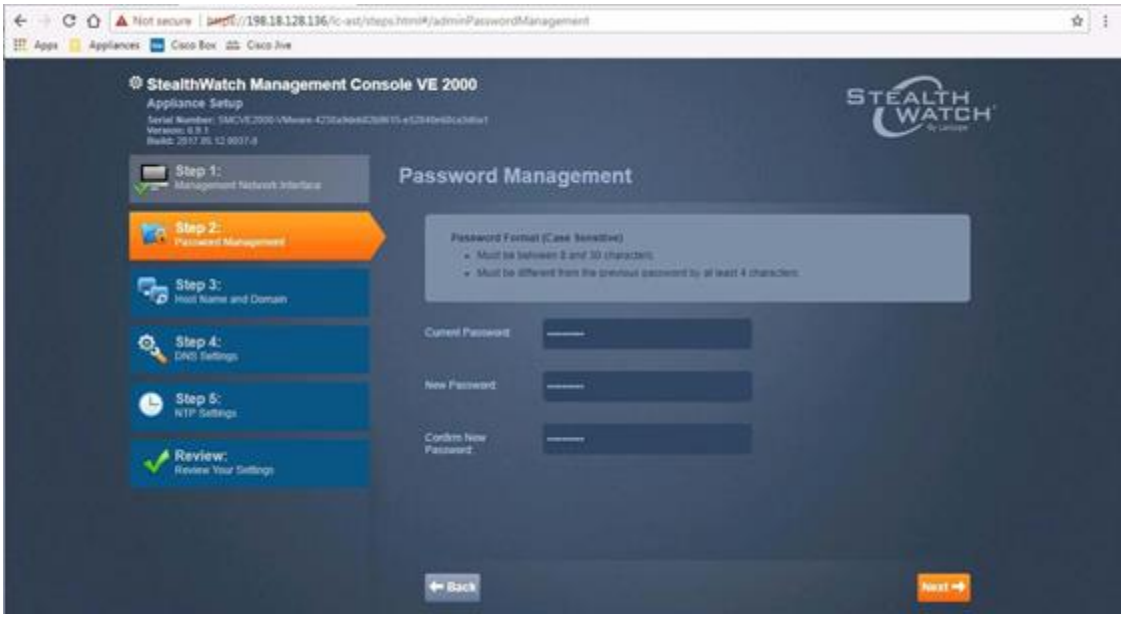
注：このページでは、あなたがオンサイトに到着する前にアプライアンスをラックに設置し、事前設定を行ったお客様が、間違った IP アドレスをアプライアンスに入力していないかどうかを確認できます。たとえば、Stealthwatch アプライアンスで使用する予定の IP アドレスが 4 つある場合は、その 4 つのうち正しい IP アドレスがフロー センサーに割り当てられていることを確認してください。

7. [パスワード管理（Password Management）] 画面が表示されます。デフォルトのパスワード lan411cope を新しいパスワード C1sco12345 に変更します。[次へ（Next）] ボタンをクリックして続行します。

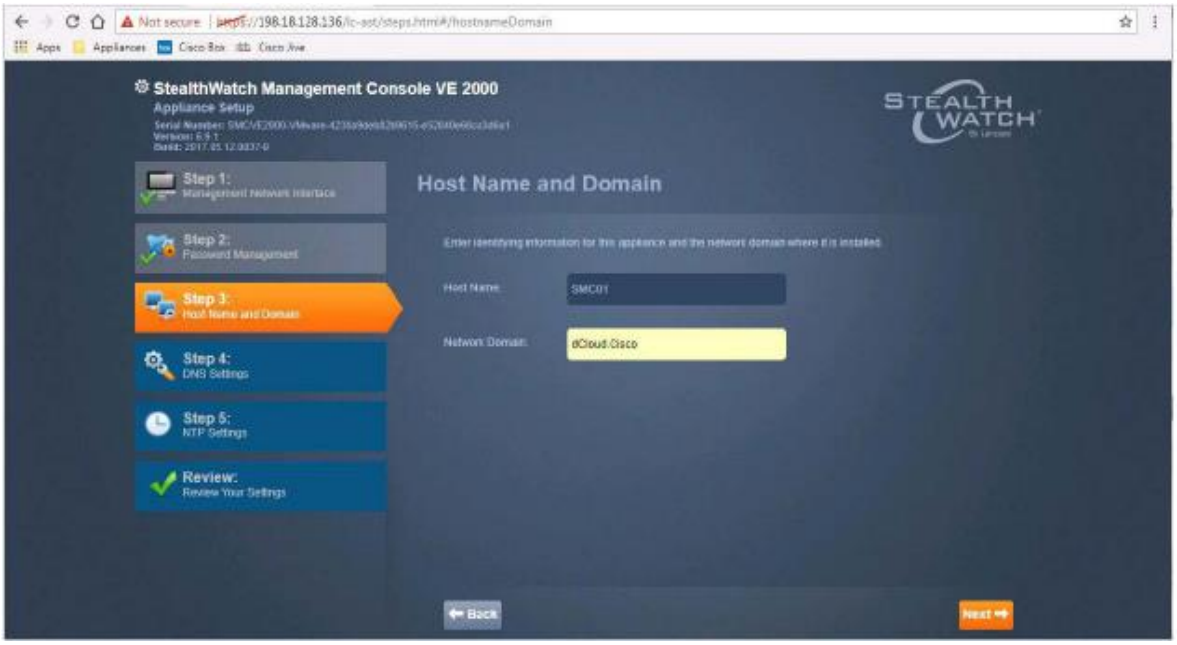
    a. [現在のパスワード（Current Password）]：lan411cope

    b. [新しいパスワード（New Password）]：C1sco12345

    c. [新しいパスワードの確認（Confirm New Password）]：C1sco12345

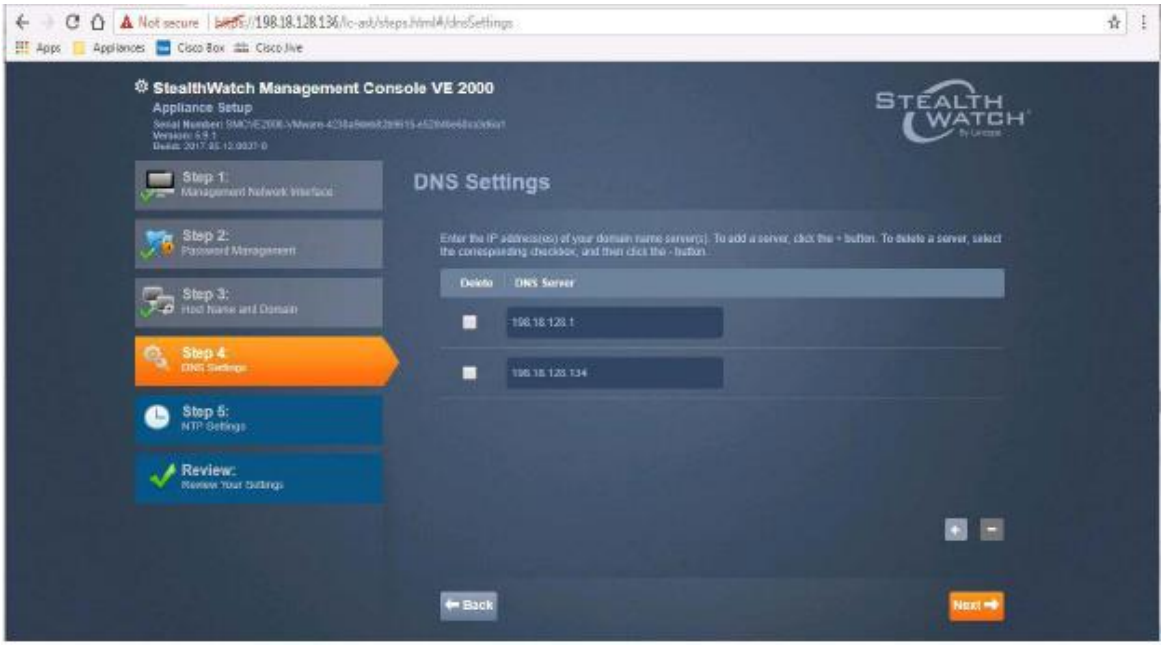


8. [ホスト名とドメイン（Host Name and Domain）] 画面が表示されます。[ホスト名（Host Name）] フィールドと [ネットワークドメイン（Network Domain）] フィールドは自動入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



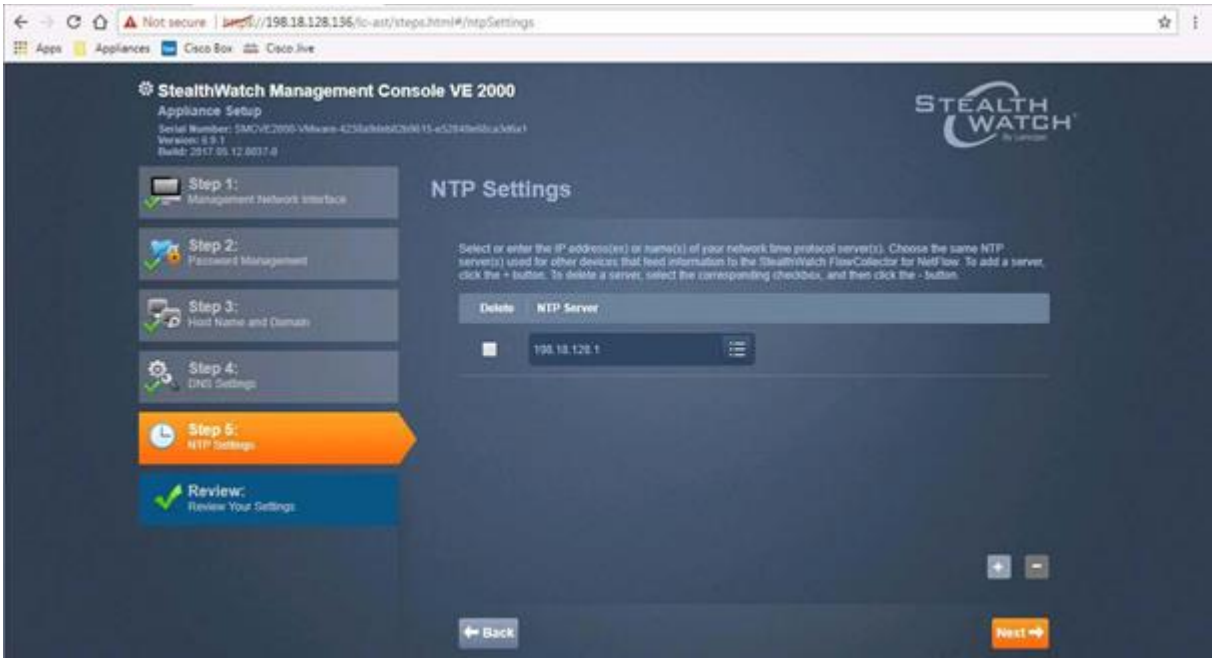
注：お客様の実稼働環境の導入では、その環境に適切なホスト名と DNS ドメイン名を入力します。

9. [DNS 設定（DNS Settings）] 画面が表示されます。この環境の DNS サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



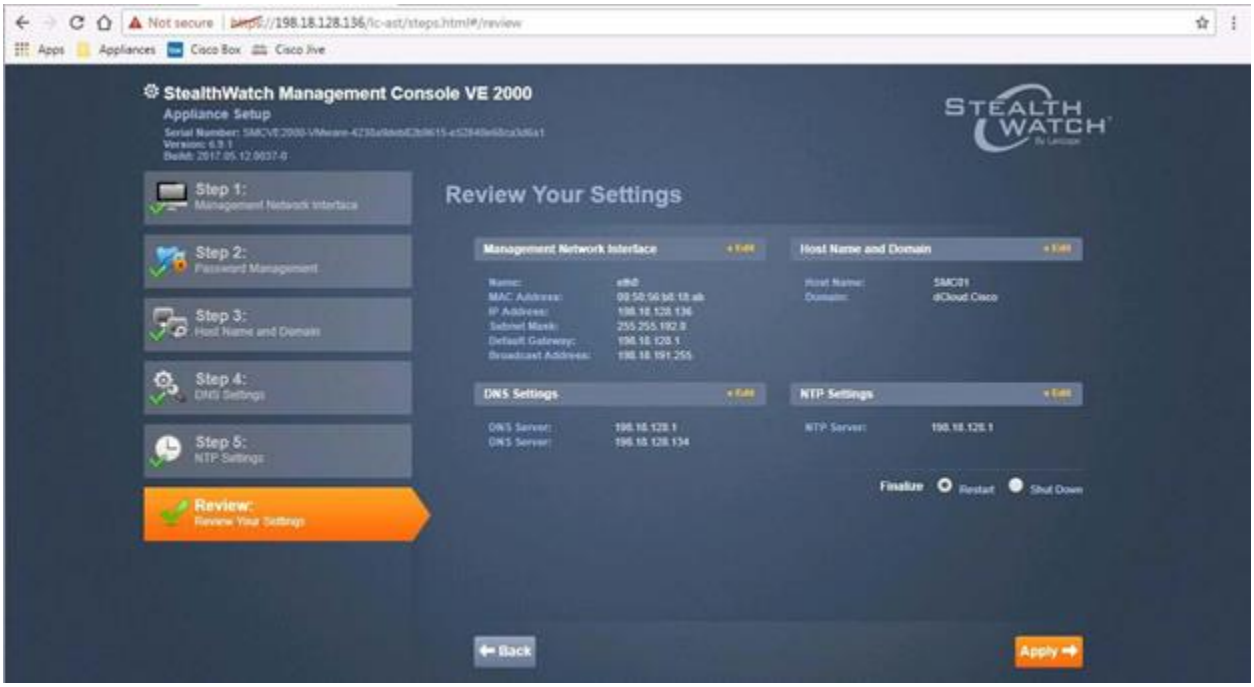
注：お客様の実稼働環境の導入では、その環境に適切な DNS サーバの IP アドレスを入力します。SMC の DNS 設定に複数のエントリがあっても問題はありません。dCloud ラボ環境セッションでは、現時点では DNS 設定を変更しないでください。

10. [NTP 設定（NTP Settings）] 画面が表示されます。この環境の NTP サーバの値はすでに入力されています。変更は必要ありません。[次へ（Next）] ボタンをクリックして続行します。



注：お客様の実稼働環境の導入では、その環境に適切な NTP サーバの IP アドレスを入力します。導入環境内のすべての Stealthwatch アプライアンスを、同じ NTP サーバと同期するように設定する必要があります。デバイス間の時刻の不一致が原因で機能にエラーが生じる可能性があります。

11. [設定の確認（Review Your Settings）] 画面が表示されます。アプライアンスに設定を適用する前に値を編集する必要がある場合は、ここで行うことができます。今回は変更の必要はありません。[確定（Finalize）] が [再起動（Restart）] に設定されていることを確認し、[適用（Apply）] ボタンをクリックします。



12. アプライアンスの再起動のプロンプトが表示されたら、[OK] ボタンをクリックして再起動を確定します。
13. SMC がリブートおよび起動シーケンスを完了してから、以降のラボのシナリオに進んでください。再起動要求後、SMC のログインページが正常にロードされるまで、しばらく時間が（5 ～ 10 分）かかる場合があります。

シナリオのまとめ

お客様のすべてのアプライアンスについて、アプライアンス セットアップ ツール（AST）を完了しました。このプロセスは繰り返し行う場合もありますが、Stealthwatch を正常に導入するには必須の作業になります。次にシステム セットアップ ツール（SST）に移り、Stealthwatch アプライアンスが相互に通信できるように設定します。

シナリオ 2.　Stealthwatch システム セットアップ ツール

AST を通じたアプライアンスの基本的なセットアップが完了したので、Stealthwatch 環境を全体的に処理するための設定を行います。Stealthwatch システム セットアップ ツール（SST）では、導入内のアプライアンス間の通信設定に加えて、Stealthwatch ドメインを設定します。

続行する前に、すべての Stealthwatch アプライアンスをオンラインにし、それぞれについて AST を完了し、ログイン ページへのアクセスを可能にする必要があります。SST の実行中に、SMC はネットワーク経由で他のアプライアンスとの通信を試みるため、アプライアンスがオフラインである場合や利用不可である場合は、SST を正常に完了できません。

注：Stealthwatch の「ドメイン」とは、固有の Stealthwatch アプライアンスと IP アドレスのコレクションです。DNS ドメインや Active Directory ドメインとは関係がありません。ほとんどのお客様環境では、Stealthwatch 内で必要になるドメインは 1 つだけです。複数のドメインが必要になるのは、お客様環境内で IP アドレス空間が重複している場合などです。たとえば、ある企業が別の企業と合併し、両社の社内ネットワークで 172.17.1.0/24 ネットワークが使用されていた場合は、IP 空間の重複と見なされます。Stealthwatch では、IP アドレスを含むフロー レコードを処理する場合には、それが 1 つのエンティティから送信されていると見なします。したがって、たとえば、ネットワーク内の別の場所で、ラップトップとプリンタの両方に同時に 172.17.1.100 が割り当てられていることは想定しません。このシナリオでは、重複する IP 空間を含む 2 番目のドメインを作成して、それぞれの固有のデバイスに対するフローが別に維持され、1 つのデータベースにマージされないようにします。それには、フロー コレクタがドメイン間で共有されず、ホスト グループ、サービス/アプリケーション、ドキュメント、フロー データなどの関連する設定オプションでも共有されないようにする必要があります。追加のドメインを作成するには、フロー コレクタ アプライアンスを追加して、限定的なシナリオで実行するようにします。SST では、この導入のすべてのアプライアンスと設定が含まれた、Stealthwatch の最初のドメインを作成する方法を示します。

手順

アプライアンス間の管理チャネルを確立する

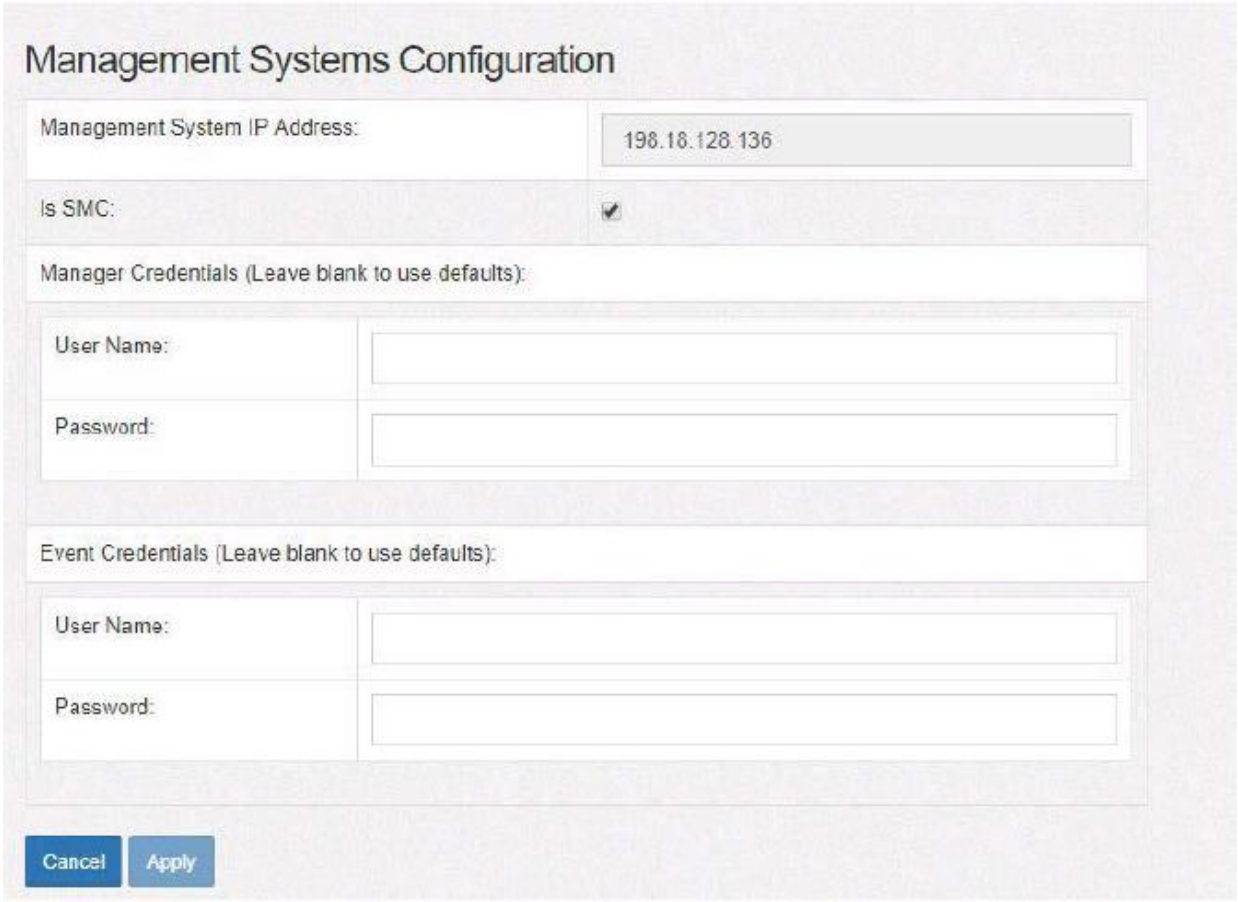
続行するには、フロー コレクタ、フロー センサー、SMC の間に管理チャネルを確立する必要があります。

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. フロー コレクタから始めます。URL フィールドで「https://198.18.128.137/」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [FC] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345

4. FC アプライアンス ページのサイド メニューから [設定（Configuration）] > [管理システムの設定（Management Systems Configuration）] を選択します。

5. [管理システムの設定（Management Systems Configuration）] ページで、[新しい管理システムの追加（Add New Management System）] ボタンをクリックします。

6. [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 アドレスである 198.18.128.136 を入力し、[SMC である（Is SMC）] の横にあるチェックボックスをオンにします。[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドは空白のままにします。[適用（Apply）] をクリックします。



7. 次に、フロー センサーの管理チャネルを有効にします。URL フィールドで「https://198.18.128.138/」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [FS] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
8. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345

9. FC アプライアンス ページのサイド メニューから [設定（Configuration）] > [管理システムの設定（Management Systems Configuration）] を選択します。

10. [管理システムの設定（Management Systems Configuration）] ページで、[新しい管理システムの追加（Add New Management System）] ボタンをクリックします。

11. [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 アドレスである 198.18.128.136 を入力します。[適用（Apply）] をクリックします。

12. これで Stealthwatch SMC、FS、FC の間に管理チャネルを正常に設定できたので、システム設定を続行することができます。

注：管理チャネルは、不正なシステムが Stealthwatch ドメイン内のアプライアンスを管理できないようにするものです。管理チャネルを有効にせずに SMC の設定を続行する場合は、SMC の Java クライアントから FC、FS、UDPD を追加する必要があります。

Stealthwatch システム セットアップ ツール

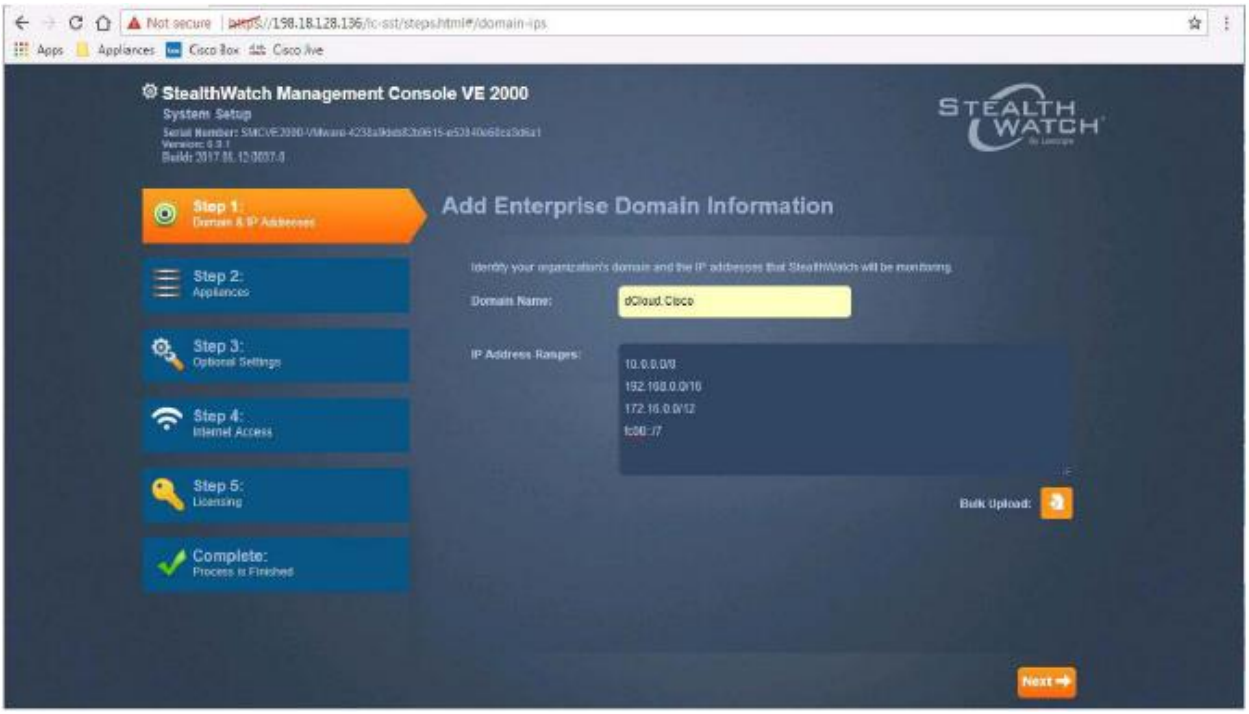
1. それでは、SMC の設定を続行します。URL フィールドで「https://198.18.128.136/」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC（管理）（SMC (Admin)）] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。ページが応答しない場合は、前の AST 完了後のリブートが完了するまで待ちます。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

2. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345
3. SST のウェルカム ページが表示されます。[続行（Continue）] ボタンを押して進みます。

4. [ドメインと IP アドレス（Domain & IP Addresses）] 画面が表示されます。[ドメイン名（Domain Name）] フィールドに「dCloud.Cisco」と入力します。[IP アドレス範囲（IP Address Ranges）] フィールドに、以下を入力します。
    a. 10.0.0.0/8
    b. 192.168.0.0/16
    c. 172.16.0.0/12
    d. fc00::/7

5. [次へ（Next）] ボタンをクリックして続行します。



注：[IP アドレス範囲（IP Address Ranges）] フィールドでは、Stealthwatch によってモニタされる組織が所有し、使用しているすべての IP アドレス範囲を定義します。ネットワークで現在使用されている範囲をすべて把握していない場合は、後で SMC で追加できます。その他の詳細は、後述するホスト グループを使用して定義します。

6. [アプライアンス（Appliances）] > [フロー コレクタ（FlowCollectors）] 画面が表示されます。フロー コレクタ アプライアンスにエントリを追加するプロンプトが表示されます。画面右下にある [+] ボタン（プラス記号ボタン）をクリックして、エントリを追加します。
7. [フロー コレクタの追加（Add FlowCollectors）] ウィンドウが表示されます。FC アプライアンスの IP アドレス 198.18.128.137 を入力し、[次へ（Next）] ボタンをクリックして続行します。
8. SMC と FC の通信が確立されると、[通信が確立されました（Communication Established）] ウィンドウが表示され、モデル、ホスト名、フロー コレクタのモデル番号、FC のバージョンが示されます。[追加（Add）] ボタンを押して続行します。

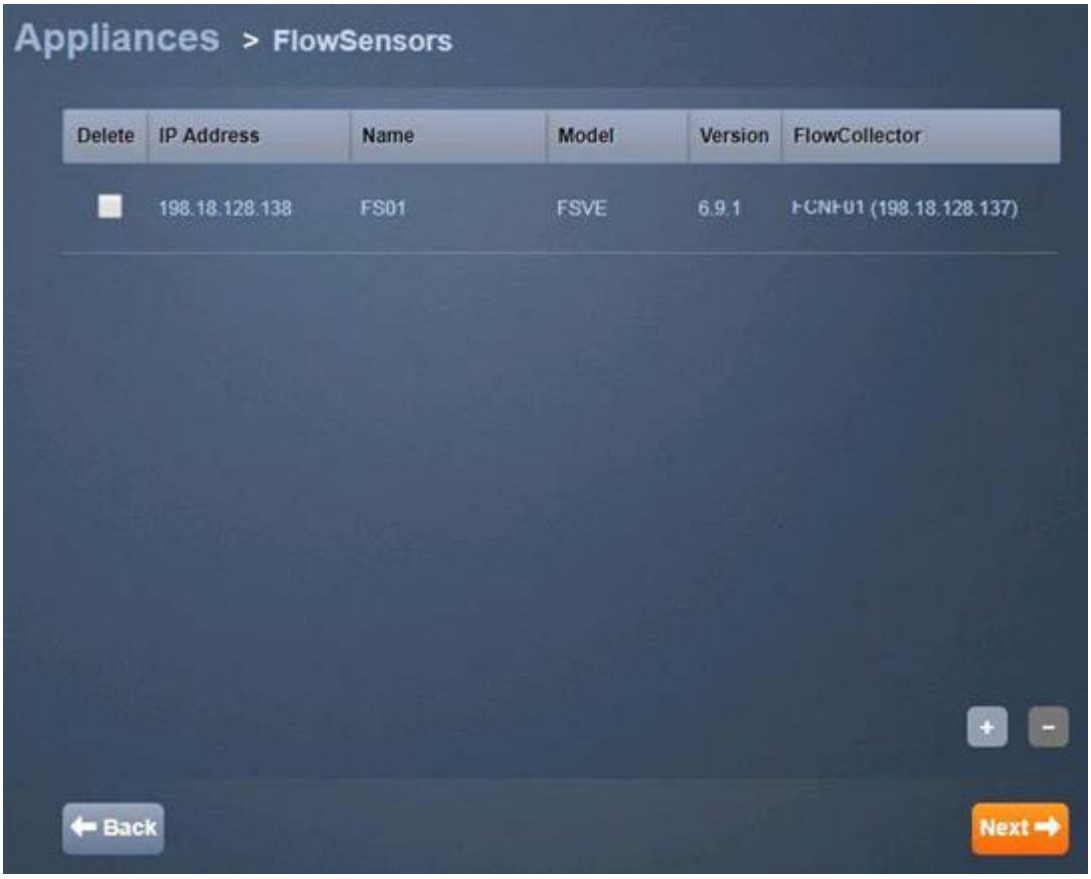
9. FC を SMC に追加する際にエラーが表示された場合は、正しい FC IP アドレスを入力していること、アプライアンスがオンラインになっていること、管理ページにログインできること、管理チャネルが適切に設定されていることを確認してください。
10. FC アプライアンスのエントリは、SST の [アプライアンス（Appliances）] > [フロー コレクタ（FlowCollectors）] ページに表示されます。現在の導入に追加される FC はこれだけです。[次へ（Next）] ボタンをクリックして続行します。

11. [アプライアンス（Appliances）] > [フロー センサー（FlowSensors）] 画面が表示されます。
12. [アプライアンス（Appliances）] > [フロー センサー（FlowSensors）] 画面では、フロー センサー アプライアンスのエントリを追加するプロンプトが表示されます。画面右下にある [+] ボタン（プラス記号ボタン）をクリックして、エントリを追加します。
13. [フロー センサーの追加（Add Flow Sensors）] ウィンドウが表示されます。FS アプライアンスの IP アドレス 198.18.128.138 を入力し、[次へ（Next）] ボタンをクリックして続行します。
14. SMC と FS の通信が確立されると、[通信が確立されました（Communication Established）] ウィンドウが表示され、モデル、ホスト名、FS のバージョンが示されます。
    a. FS を SMC に追加する際にエラーが表示された場合は、正しい FS IP アドレスを入力していること、アプライアンスがオンラインになっていること、管理ページにログインできること、管理チャネルが適切に設定されていることを確認してください。

15. [フロー コレクタ（FlowCollector）] ドロップダウン フィールドには、導入に追加されたすべてのフロー コレクタが表示されます。FS からデータを送信する FC を選択します。この環境で使用される FC は 1 つだけです。フロー コレクタのドロップダウン ボックスをクリックして、エントリ 198.18.128.137 を選択し、[追加（Add）] ボタンをクリックして続行します。

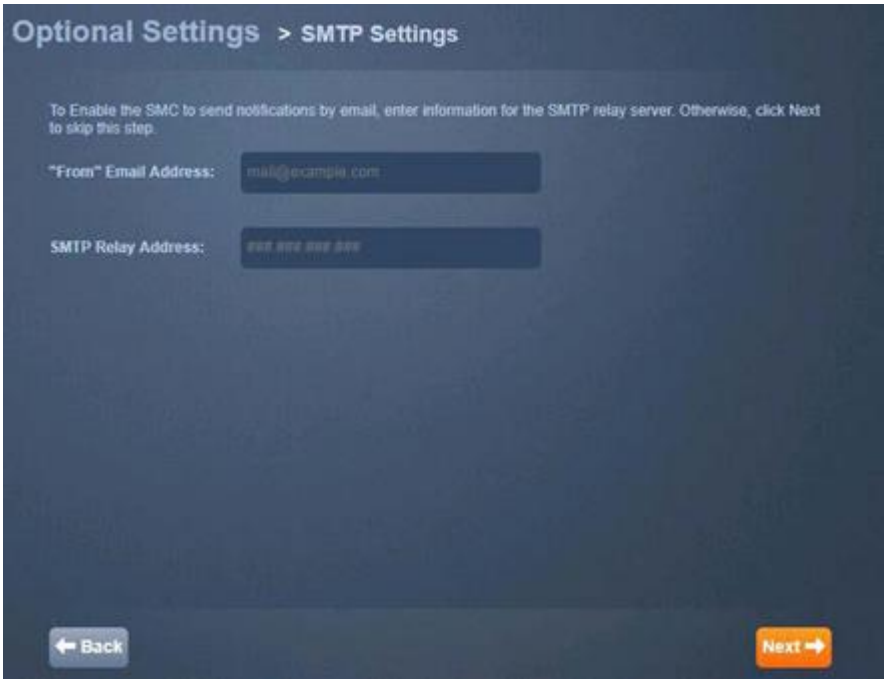
16. フロー センサー VE のログイン クレデンシャル ウィンドウが表示されたら、[スキップ（Skip）] ボタンをクリックして続行します。

17. FS アプライアンスのエントリは、SST の [アプライアンス（Appliances）] > [フロー センサー（FlowSensors）] ページに表示されます。[次へ（Next）] ボタンをクリックして続行します。

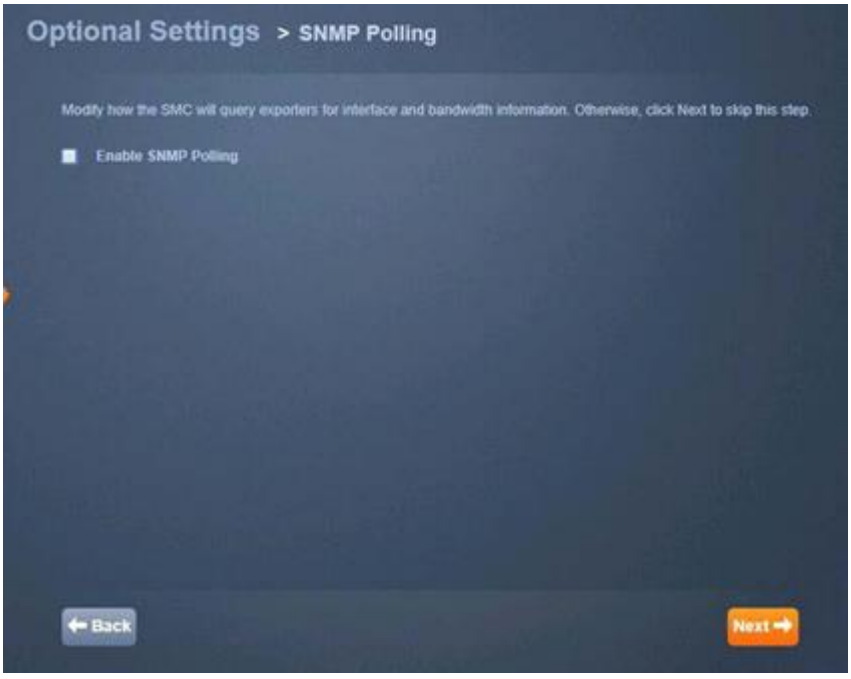


注:このラボ環境内のラボ設定によっては、特に入力していない、他の FS アプライアンスがリストに表示される場合があります。これは、このラボでは許容されます。お客様環境では、SST を通じてまたは手動で、FC を指すように設定された FS アプライアンスだけが、このウィンドウに表示されます。

18. [オプション設定(Optional Settings)] > [SMTP 設定(SMTP Settings)] 画面が表示されます。これらの設定は現時点では不要であるため、後で SMC Java UI を通じて入力します。[次へ(Next)] ボタンをクリックして続行します。



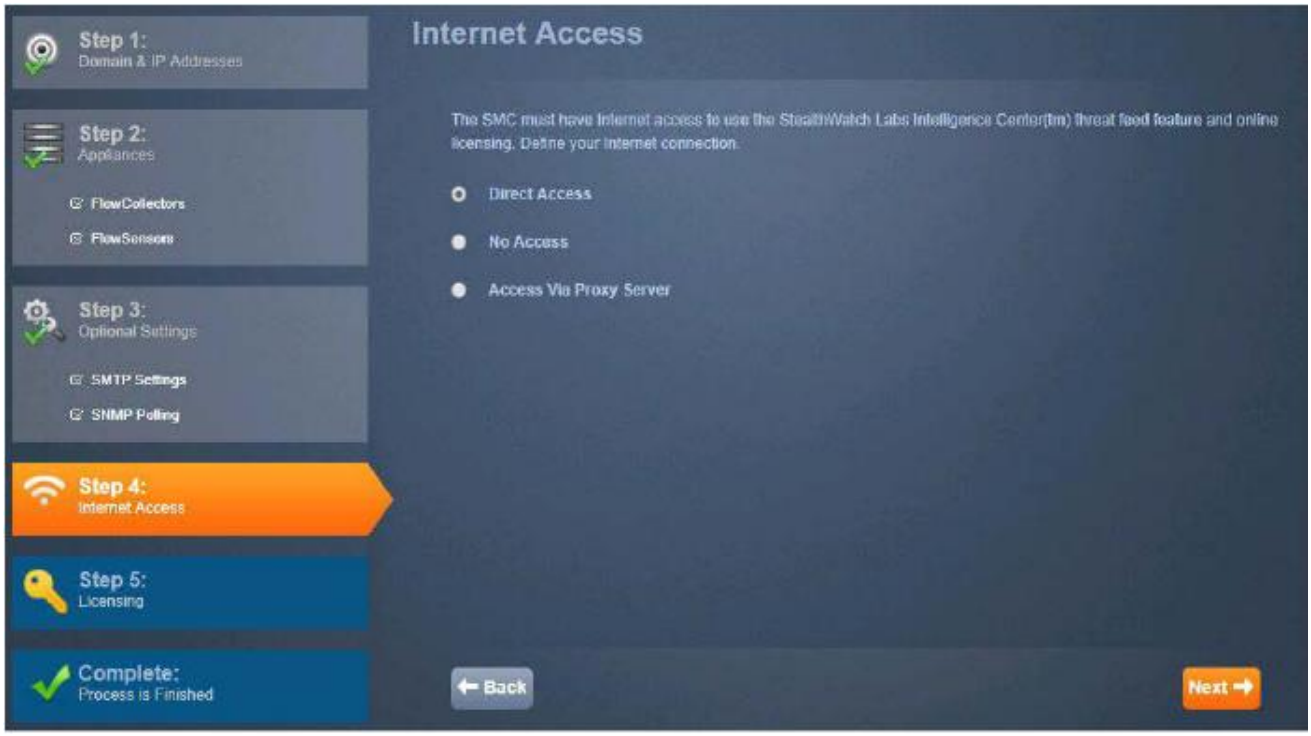
19. [オプション設定(Optional Settings)] > [SNMP ポーリング(SNMP Polling)] 画面が表示されます。エクスポータからデータをポーリングするための SMC の [SNMP ポーリング(SNMP Polling)] 設定は、後で SMC Java UI を通じて設定できます。[SNMP ポーリングの有効化(Enable SNMP Polling)] ボックスをオフにし、[次へ(Next)] ボタンをクリックして続行します。



20. SNMP ポーリングが無効になったことを示す通知が表示されます。[OK] ボタンを押して続行します。

注:お客様から、まだエクスポータに対する SNMP コミュニティ ストリングなどのデータが提供されていません。ここでは設定をスキップして、後で SMC に入力します。

21. [インターネット アクセス(Internet Access)] 画面が表示されます。[ダイレクト アクセス(Direct Access)] オプションをオンにし、[次へ(Next)] ボタンをクリックして続行します。



注:このラボ環境内でのラボ設定により、[インターネット アクセス(Internet Access)] 画面がスキップされる可能性があります。[戻る(Back)] ボタンを押すと、変更を加えて、続行することができます。このラボでは、SMC のインターネット アクセス機能を定義する必要はありませんが、実際の導入ではライセンス アクティベーション プロセスを実行する際に重要となります。

22. [ライセンス(Licensing)] 画面が表示されます。このラボでは [アクセスなし(No Access)] を選択します。

23. [次へ(Next)] ボタンをクリックして続行します。

注:ラボでのアプライアンスのライセンスはすでに有効化されているため、再度有効化する必要はありません。お客様環境では、すべてのアプライアンスとライセンスが登録されていること、SMC がオンラインで License Center にアクセスできるか、適切なライセンス ファイルをオフラインで利用できることを確認する必要があります。

24. 次のように [通知（Notice）] ウィンドウが表示されたら、[OK] ボタンをクリックして続行し、ライセンスに関する通知は無視します。

25. [完了（Complete）] 画面が表示されます。[起動（Launch）] ボタンをクリックして SST を終了します。

シナリオのまとめ

ドメイン内のアプライアンスを安全に管理するために、管理チャネルを確立しました。SMC、FC、FS 間の相互通信の設定、Stealthwatch ドメインの作成、Stealthwatch 環境の一部の基本設定を実施し、システム セットアップ ツール（SST）を完了しました。SST が完了したので、さらに設定タスクを進めることができます。

シナリオ 3.　アプライアンスのインストール後の設定、検証、およびトラブルシューティング

AST および SST ウィザードでは設定できなかったため、ここで追加設定が必要な項目がいくつかあります。初期導入の一環として、ここでアプライアンスに関連するすべての設定手順を行います。これには、Stealthwatch が NetFlow を処理するための設定が含まれます。さらに、導入中に発生する可能性がある問題について、トラブルシューティング方法を提示します。

手順

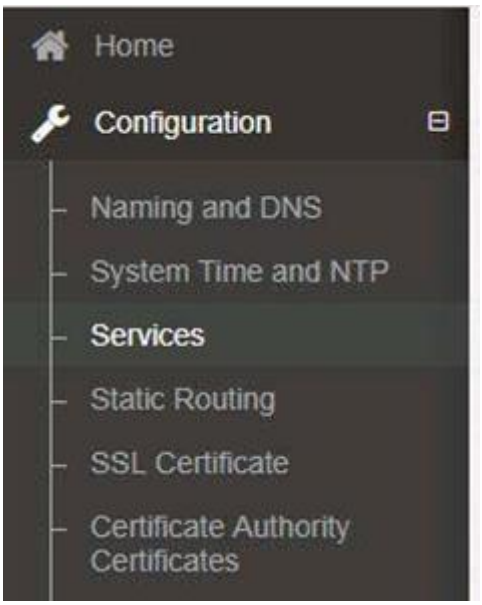
SSH アクセス

この導入では、トラブルシューティングおよび検証に関するいくつかの手順で、SSH コンソール アクセスを使用します。SSH アクセスが有効になっていることを確認します。さらに、DNS や NTP などの特定の設定についてお客様から提供された値が正しく、それらのサービスがアプライアンス上で適切に機能していることを確認します。Stealthwatch ソリューションが完全に機能し、お客様が利用できるようにするために、これらの手順はすべて完了する必要があります。

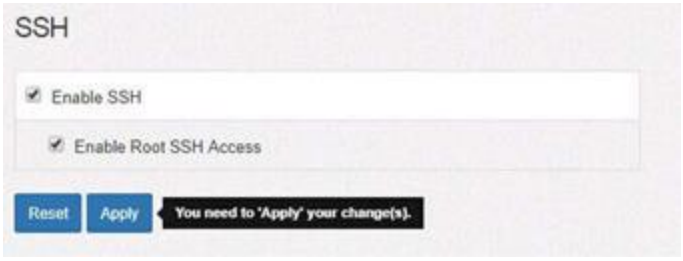
1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.136/smc/index.html」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC（管理）（SMC (Admin)）] を選択して、SMC アプライアンスの Web 管理インターフェイスにアクセスします。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

3. 以下の情報を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345
4. [設定（Configuration）] メニューをクリックし、[サービス（Services）] メニュー項目を選択します。



5. [SSH の有効化（Enable SSH）] および [root による SSH アクセスの有効化（Enable Root SSH Access）] オプションがどちらもオンになっていることを確認します。



6. いずれかのオプションがオフになっている場合は、ボックスにチェックマークを入れ、[適用（Apply）] ボタンをクリックして変更を保存します。
7. 上記の手順を実行して、以下に示すすべてのアプライアンスで SSH が有効になっていることを確認します。
    a. FC：https://198.18.128.137/swa/
    b. FS：https://198.18.128.138/fs/
    c. UDPD：https://198.18.128.139/fr/

注：デフォルトでは、新しいアプライアンスで SSH および root による SSH が無効になっています。このアクセス方法を使用するには、それらを有効にする必要があります。CLI への root による SSH アクセスは、トラブルシューティングするのに非常に便利です。特にハイパーバイザのコンソール アクセスが利用できない場合に有効です。このドメインに関しては、本ドキュメントに記載されているラボの一部で非常に重要となります。

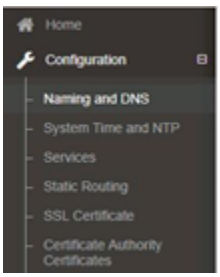
DNS の検証

次に、SMC アプライアンスが DNS サーバと正常に通信できることを確認します。すべてのアプライアンスで DNS を正常に使用できるようにすべきですが、特に SMC アプライアンスでは、製品内のさまざまなドキュメントについて名前解決タスクを実行し、またライセンスと脅威フィード関連のタスクに DNS 解決を使用するため、DNS が不可欠です。お客様環境では、この検証をすべてのアプライアンスで実行する必要があります。

1. SMC の Web 管理ページに接続している場合は、ステップ 4 に進みます。接続していない場合は、Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.136/smc/index.html」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC（管理）（SMC (Admin)）] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

3. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345
4. [設定（Configuration）] メニューをクリックし、[ネーミングおよび DNS（Naming and DNS）] メニュー項目を選択します。



5. ページの最下部にある [ネットワーク ホストと IP ルックアップ（Network Host and IP Lookup）] セクションまでスクロールします。
6. [ホスト名または IP アドレス（Host name or IP Address）] フィールドに google.com と入力し、[解決（Resolve）] ボタンをクリックします。

7. DNS 要求のステータスを示すページが表示されます。要求が正常に処理され、名前解決についての情報が表示されます。
8. アプライアンスが有効な DNS サーバと正常に通信できることを確認しました。要求の処理が失敗した場合、レコードは表示されません。

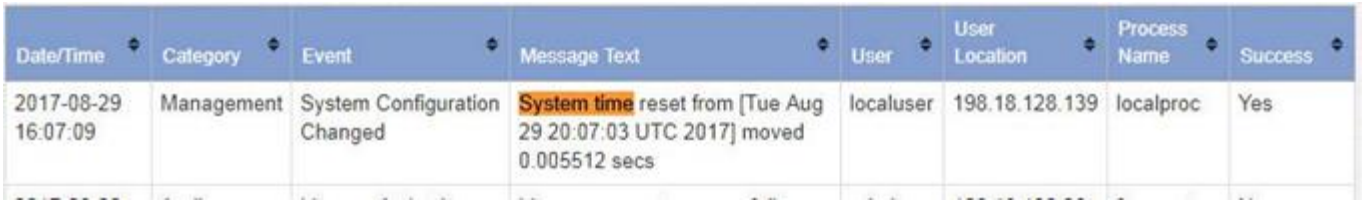
NTP の検証

次に、SMC アプライアンスが NTP サーバと正常に通信できることを確認します。NTP は、すべての Stealthwatch アプライアンスで不可欠なサービスです。時刻の不一致が発見された場合は、製品内でアラームが上がります。お客様環境では、この検証をすべてのアプライアンスで実行する必要があります。お客様から NTP サーバの IP アドレスを提供されても、それが有効な NTP サーバであるとは限らず、また有効であっても、その NTP サーバとアプライアンスが通信できるとは限りません。監査ログは、アプライアンスが時刻の更新を正常に受信しているかどうかを判断する、最も簡単な方法です。必要に応じてさらに詳細なトラブルシューティングができる、コンソール コマンドも用意されています。ここではアプライアンスの Web 管理ページと SSH コンソールを使用して、NTP 機能を確認します。

1. SMC の Web 管理ページに接続している場合は、ステップ 4 に進みます。接続していない場合は、Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.136/smc/index.html」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC（管理）（SMC (Admin)）] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

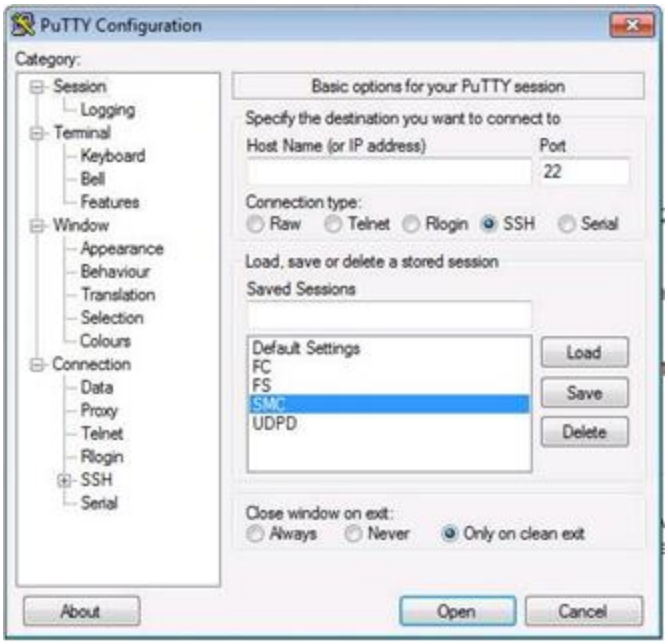
3. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
4. [監査ログ（Audit Log）] メニュー項目を選択します。
5. 監査ログが表示されたら、[メッセージ テキスト（Message Text）] の値が [システム時刻のリセット時（System time reset from）] になっているエントリを探します。エントリは、アプライアンスのブート時刻以後、1 時間に 1 回発生しています。これは、アプライアンスが時刻を受信し、内部クロックを修正していることを示します。アプライアンスがオンラインのまま 1 時間を超え、このエントリがログに表示されていない場合は、NTP サーバのアドレスとネットワーク アクセスを確認してください。



Date/Time	Category	Event	Message Text	User	User Location	Process Name	Success
2017-08-29 16:07:09	Management	System Configuration Changed	System time reset from [Tue Aug 29 20:07:03 UTC 2017] moved 0.005512 secs	localuser	198.18.128.139	localproc	Yes

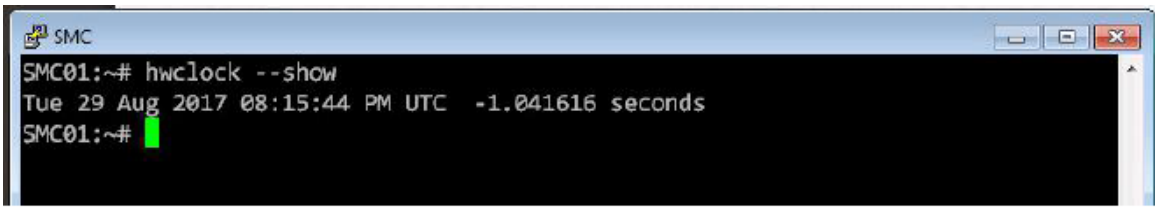
6. NTP について、より高度なトラブルシューティングと検証を行うには、アプライアンスのコンソールにアクセスします。ここで SSH で SMC に接続し、さらに NTP のトラブルシューティングを実行します。

7. dCloud 管理ワークステーションで、デスクトップの [PuTTY] ショートカットを開きます。
8. PuTTY 画面の [保存済みセッション（Saved Sessions）] セクションで、[SMC] エントリを選択して [開く（Open）] ボタンをクリックします。



9. 画面の指示に従って、ユーザ名 root とパスワード lan1cope を使用して、アプライアンスにログインします。
10. 次のコマンドを実行すると、アプライアンスの現在時刻が表示されます。

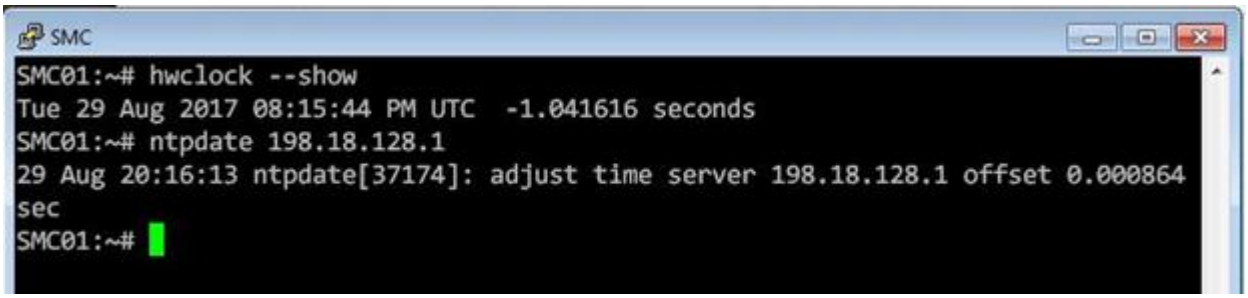
```
hwclock --show
```



11. アプライアンスのタイム ゾーンを考慮して、有効な日付とタイムスタンプが表示されることを確認します。
12. 次のコマンドを実行して、お客様の NTP サーバと同期させます。

```
ntpdate 198.18.128.1
```

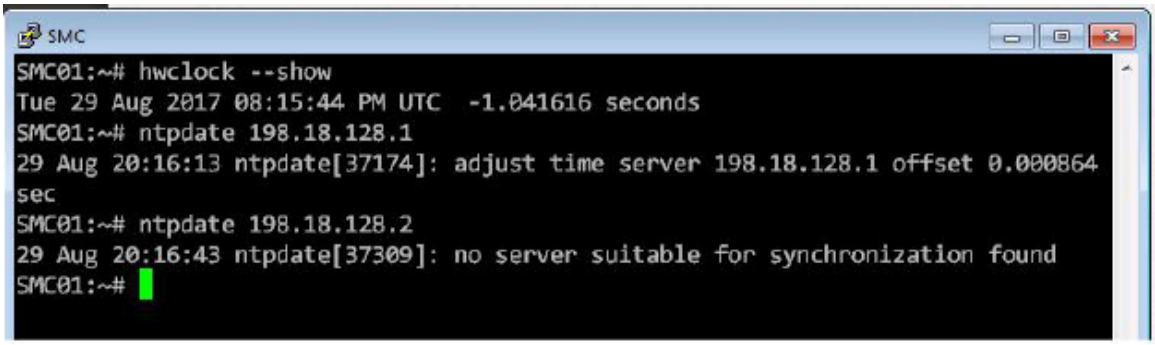
13. お客様の NTP サーバと正常に同期されたことを示す応答が表示されます。



14. 次のコマンドを実行すると、失敗した NTP 同期の結果が表示されます。

```
ntpdate 198.18.128.2
```

15. 無効な NTP サーバ アドレスに対して ntpdate コマンドを実行すると、エラーが発生します。



注:お客様環境で提供された NTP サーバのアドレスと正常に通信できない場合は、お客様のネットワークの ACL またはファイアウォール ルールによって、トラフィックまたは互換性のない NTP サーバがブロックされている可能性があります。

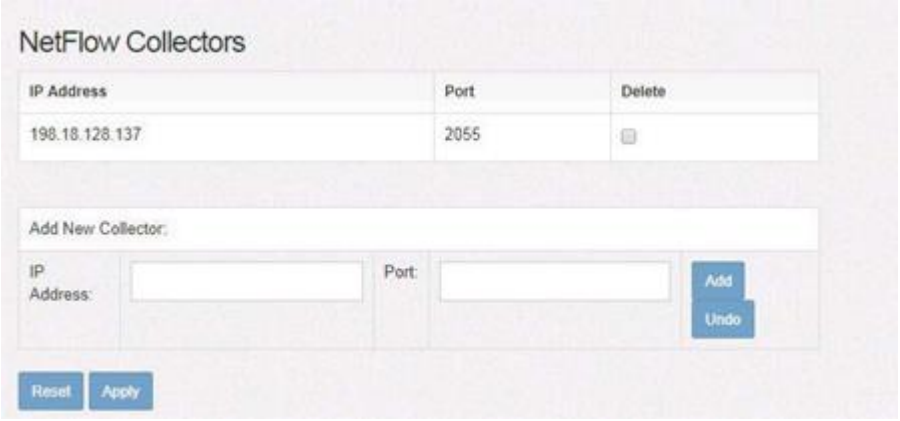
16. アプライアンスがお客様の NTP サーバと通信できることを確認しました。PuTTY SSH セッションを終了します。

注:お客様環境では、すべてのアプライアンスが、割り当てられている NTP サーバと正常に通信できることを確認することが重要です。有効な各 NTP サーバに対して ntpdate コマンドを実行し、Stealthwatch をお客様環境に導入するために正常に接続されていることを確認します。

フロー センサーの設定

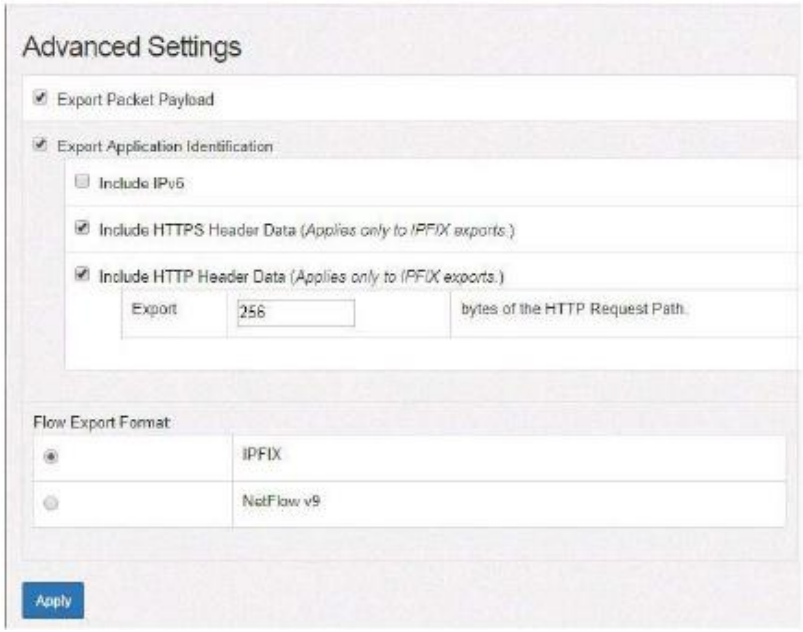
1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.138」と入力するか、またはブックマークから [アプライアンス(Appliances)] > [FS] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード C1sco12345 を使用して、アプライアンスにログインします。
4. [設定(Configuration)] メニューをクリックし、[NetFlow コレクタ(NetFlow Collectors)] メニュー項目を選択します。

5. 198.18.128.137 のポート 2055 で実行されているフロー コレクタのエントリが、[NetFlow コレクタ（NetFlow Collectors）] ページに表示されていることを確認します。



6. 必要に応じて、[IP アドレス（IP Address）] フィールドに 198.18.128.137 と入力し、[ポート（Port）] フィールドに 2055 と入力して、FC のエントリを追加します。
7. [IP アドレス（IP Address）] フィールドと [ポート（Port）] フィールドに入力したら、[追加（Add）] ボタンをクリックしてエントリを追加します。
8. [適用（Apply）] ボタンをクリックして設定を保存します。
9. [設定（Configuration）] メニューをクリックし、[詳細設定（Advanced Settings）] メニュー項目を選択します。

10. 次のように設定されていることを確認したら、[適用（Apply）] ボタンをクリックします。
    a. [パケット ペイロードのエクスポート（Export Packet Payload）]：オン
    b. [アプリケーション ID のエクスポート（Export Application Identification）]：オン
    c. [HTTPS ヘッダー データを含める（Include HTTPS Header Data）]：オン
    d. [HTTP ヘッダー データを含める（Include HTTP Header Data）]：オン



11. 変更を行った場合は、必ず [適用(Apply)] をクリックしてください。

注:[詳細設定(Advanced Settings)] オプションを有効にして正しく設定すると、非常に有益です。それによって、お客様環境に関する貴重な追加情報が得られます。

[パケット ペイロードのエクスポート(Export Packet Payload)]:FS がパケット ペイロードの一部をエクスポートして、SMC で追加データを入力できるようにします。

[アプリケーション ID のエクスポート(Export Application Identification)]:FS は、NetFlow レコードが提供するメタデータだけではなく実際の raw ネットワーク トラフィックを確認しているため、ディープ パケット インスペクション(DPI)を実行できます。FS はこの機能を使用して、送信時に経由するポートとプロトコルだけでなく、パケットのコンテンツに基づいて、特定のタイプのネットワーク トラフィックを自動的に分類します。たとえば、パケットは TCP ポート 80 経由で送信できますが、それらは Web ブラウズではなく、実際にはインスタント メッセージ チャット トラフィックです。

[IPv6 を含める(Include IPv6)]:お客様のネットワーク内に IPv6 があり、FS で IPv6 トラフィック用の NetFlow レコードが生成されるようにする場合は、これをオンにします。IPv6 が存在しないとお客様が述べている場合でも、レポート用にこのオプションをオンにすることをお勧めします。お客様が認識していなくても、実際には IPv6 が使用されている場合が多くあるためです。

[HTTPS ヘッダー データを含める(Include HTTPS Header Data)]:HTTPS トラフィックの署名/暗号化に使用する証明書などの詳細を含めます。

[HTTP ヘッダー データを含める(Include HTTP Header Data)]:HTTP 要求の URL や、ftp、telnet、smtp コマンドのようなクリアテキスト データなどの詳細を含めます。

[x バイトの HTTP 要求パスをエクスポート(Export x bytes of the HTTP Request Path)]:フロー レコードと合わせてエクスポートする HTTP 要求パスのデータ量。デフォルトでは 32 バイトに設定されています。サイズを大きくすると、Stealthwatch で使用できる URL データが増えますが、FS アプライアンスの負荷が増大する場合があります。エクスポートのサイズを大きくする場合は、FS のパフォーマンスを監視してください。

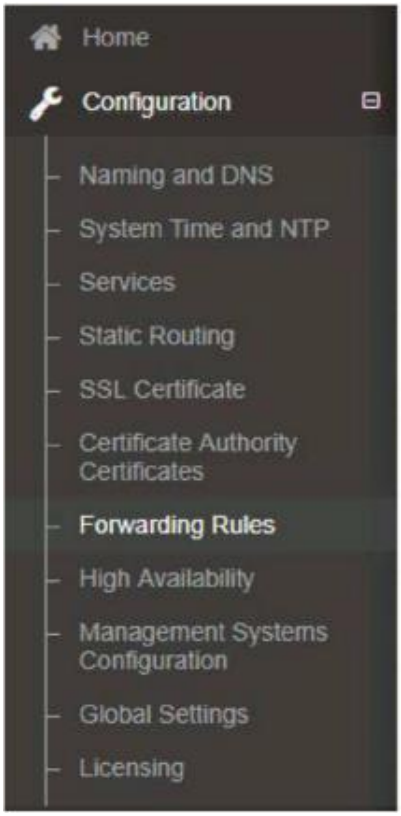
12. フロー センサーが正しく設定されました。ラボの次の手順に進みます。

UDP Director の設定

UDP Director はオプションの Stealthwatch アプライアンスであり、お客様環境における NetFlow およびその他の UDP 管理トラフィックの単一の宛先として機能します。設定がシンプルになり、Stealthwatch を含むさまざまなソリューションによる、NetFlow、SNMP トラップ、Syslog などのデータ処理の柔軟性が向上します。

UDP Director の IP アドレスは、お客様環境内の NetFlow エクスポータが NetFlow レコードを送信する宛先になります。フロー コレクタ アプライアンスにフロー データを転送するように UDPD を設定しないと、Stealthwatch 内でフロー データが処理されません。ここで、NetFlow トラフィックを FC に送信するように、UDPD の転送ルールを設定します。

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.139」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [UDPD] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. Stealthwatch のデフォルトのユーザ名 admin と、デフォルトのパスワード C1sco12345 を使用して、アプライアンスにログインします。
4. [設定（Configuration）] メニューをクリックし、[転送ルール（Forwarding Rules）] メニュー項目を選択します。



注：重要：以後のラボを正しく機能させるためには、この手順を完了する必要があります。

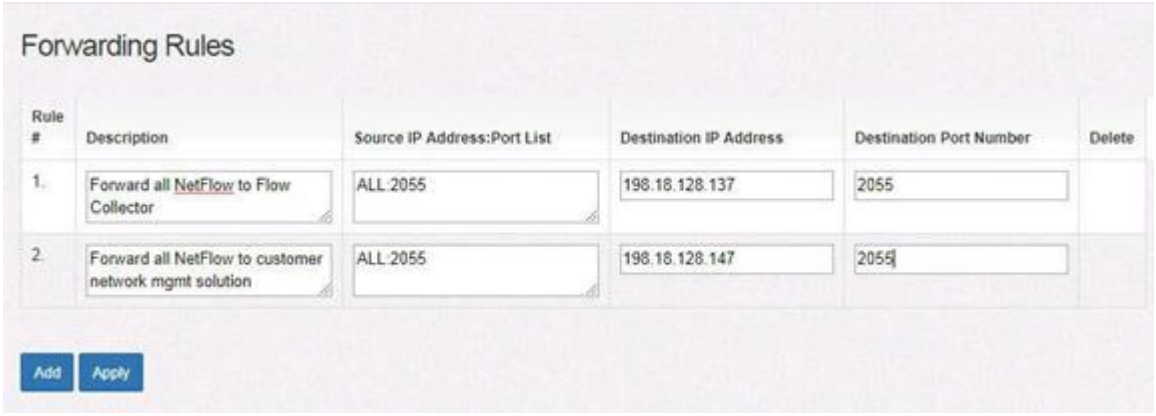
5. 次に、NetFlow トラフィックを FC アプライアンスに転送するように UDPD を設定するために、必要なパラメータを追加します。[転送ルール（Forwarding Rules）] ページに次の値を入力します。
    a. [説明（Description）]：すべての NetFlow をフロー コレクタに転送する（Forward all NetFlow to Flow Collector）
    b. [送信元 IP アドレス:ポート リスト（Source IP Address:Port List）]：ALL:2055
    c. [宛先 IP アドレス（Destination IP Address）]：198.18.128.137
    d. [宛先ポート番号（Destination Port Number）]：2055

注:この環境や、フロー コレクタが 1 つのほとんどの環境では、1 つのルールですべての NetFlow トラフィックを FC IP アドレスに送信することをお勧めします。特定の送信元から特定の宛先だけにトラフィックを転送するように、IP アドレスまたは CIDR 範囲を入力することが可能です。

これは、大量のフロー データがある環境で、複数の FC アプライアンスを使用してロードを処理している環境で有益です。非常に単純な例としては、1 秒あたりの合計フロー数(FPS)が 100,000 で、2 つの FC 間でロードを分割する場合が挙げられます。このシナリオでは、NetFlow の転送ルールで、[送信元 IP アドレス(Source IP Address)] フィールドに ALL を使用せず、1 つの IP アドレスまたは CIDR 範囲を指定して、トラフィックが適切な FC に送信されるようにします。すべての送信元のデバイス/ネットワークで適切な FC にデータが転送されるようにするには、複数のエントリが必要になる場合があります。
UDPD 設定に関する一般的な問題としては、UDPD にデータを送信するデバイスがありながら、そのトラフィックに適合する転送ルールがない場合が挙げられます。

お客様環境によっては、標準の UDP ポートである 2055 を使用するように NetFlow が設定されない場合があります。個々の FC では、フロー トラフィックを 1 つのポートでのみ受信できます(ただしそのポートは任意のポート番号に設定できます)。非標準の NetFlow ポートを使用する UDPD がある環境では、UDP 9055 でトラフィックを受信し、デフォルトのポート番号を変更するように FC の設定を変更せずに 2055 の FC に転送する、転送ルールを記述することが可能です。他にも NetFlow を取り込む必要があるソリューションがお客様環境内にある場合は、元のポート番号、またはソリューションの管理者が任意に指定する値でフローを転送する、別の転送ルールを設定できます。

6. Stealthwatch のルールを設定しましたが、ここで NetFlow トラフィックを取り込むルールがお客様環境内の他のソリューションで設定されているかどうかを確認します。[追加(Add)] ボタンをクリックして追加エントリを作成し、設定フィールドに次の値を入力します。
    a. ルール #2
    b. [説明(Description)]:すべての NetFlow をお客様のネットワーク管理ソリューションに転送する(Forward all NetFlow to customer network mgmt solution)
    c. [送信元 IP アドレス:ポート リスト(Source IP Address:Port List)]:ALL:2055
    d. [宛先 IP アドレス(Destination IP Address)]:198.18.128.147
    e. [宛先ポート番号(Destination Port Number)]:2055



7. [適用(Apply)] ボタンをクリックして変更を保存します。
8. 両方のルールがすべて正しく設定されていることを検証します。
9. このラボ環境に対する UDP Director の設定は終了です。

動作していないアプライアンスのトラブルシューティング

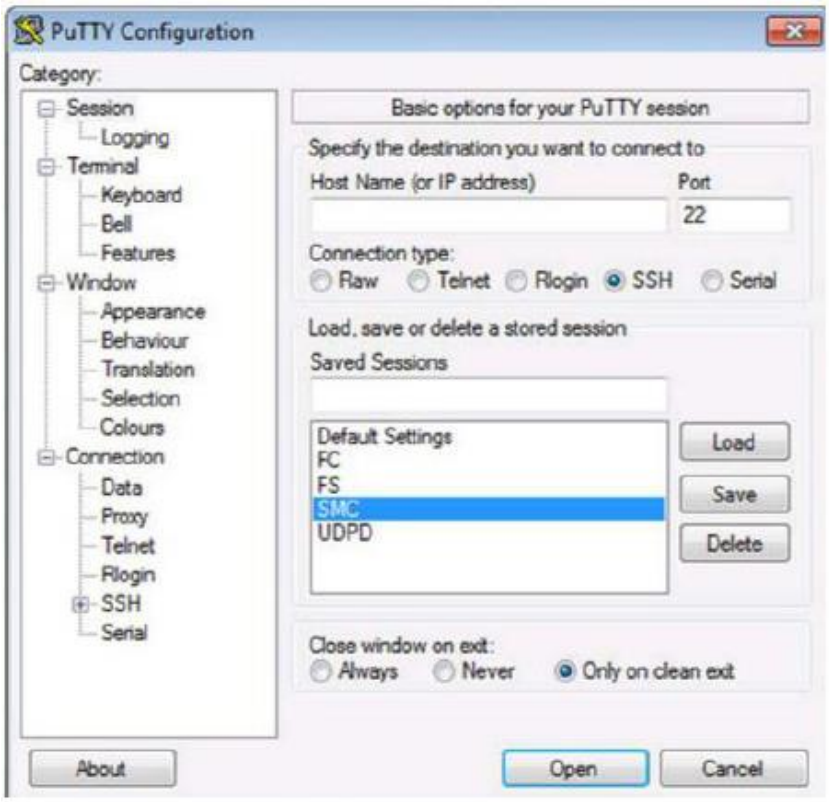
注:このラボ演習は必須ではありませんが、ラボまたは実際の環境でこのような事態に遭遇した場合の参考情報として記載されています。これらの手順を実行するには、root アカウントによる SSH アクセスが有効になっているか、またはコンソールからアプライアンスにアクセスできることが必要です。

ここでは、Stealthwatch アプライアンスが(ssh/コンソール アクセス経由で)起動/再起動し、ログイン プロンプトまで処理を終えているが、Web インターフェイスにアクセスしようとして下記が表示される場合に実施すべき手順について説明します。アプライアンスの再起動には、特に大規模な情報データベースを備えたアプライアンスの場合には、時間がかかる(5 ～ 15 分)ことに注意してください。

これが 15 分または 20 分以上続く場合、一般的には Vertica データベースに問題が発生しているため、手動で再起動するか、場合によりロールバックする必要があります。これはほとんどの場合、仮想環境で発生します。通常は、仮想環境のリソース不足または管理ミスによるものです。詳細については、「付録 D」を参照してください。

ラボで機能を回復するには、以下を行います(このプロセスは、実際の環境とは異なる可能性があります)。

1. dCloud 管理ワークステーションで、デスクトップの [PuTTY] ショートカットを開きます。
2. PuTTY 画面の [保存済みセッション(Saved Sessions)] セクションで、該当のアプライアンス エントリを選択して [開く(Open)] ボタンをクリックします。



3. 次のクレデンシャルを使用して、アプライアンスの CLI にログインします。
    a. ログイン：root
    b. パスワード：lan1cope
4. アプライアンスのコマンド ラインが表示されます。
5. 次のコマンドを実行します。
    a. su - dbadmin
6. dbadmin アカウントとして、下記のコマンドを実行します。
    a. admintools
7. Vertica データベース管理ツール アプリケーションが起動します。
8. オプション 1 の [データベース クラスタの状態を表示（View Database Cluster State）] を選択します。

```
Vertica Analytic Database 7.2.3-0 Administration Tools
 ____________________________________________________________________________


          ┌──────────────────────────────────────────────────┐
          | Main Menu                                        |
          | ┌──────────────────────────────────────────────┐ |
          | |            View Database Cluster            | |
          | |        1  State                              | |
          | |        2  Connect to Database                | |
          | |        3  Start Database                     | |
          | |        4  Stop Database                      | |
          | |        5  Restart Vertica on Host            | |
          | |        6  Configuration Menu                 | |
```

```
| |        7  Advanced Menu                                  |
| |        8  Help Using the Administration Tools            |
| |        E  Exit                                           |
|   └──────────────────────────────────────────────┘   |
├──────────────────────────────────────────────┤
|     <     OK     >     <Cancel>     <     Help     >     |
└──────────────────────────────────────────────┘
```

9. sw DB がダウンとして表示されている場合は、以下の操作を行います。

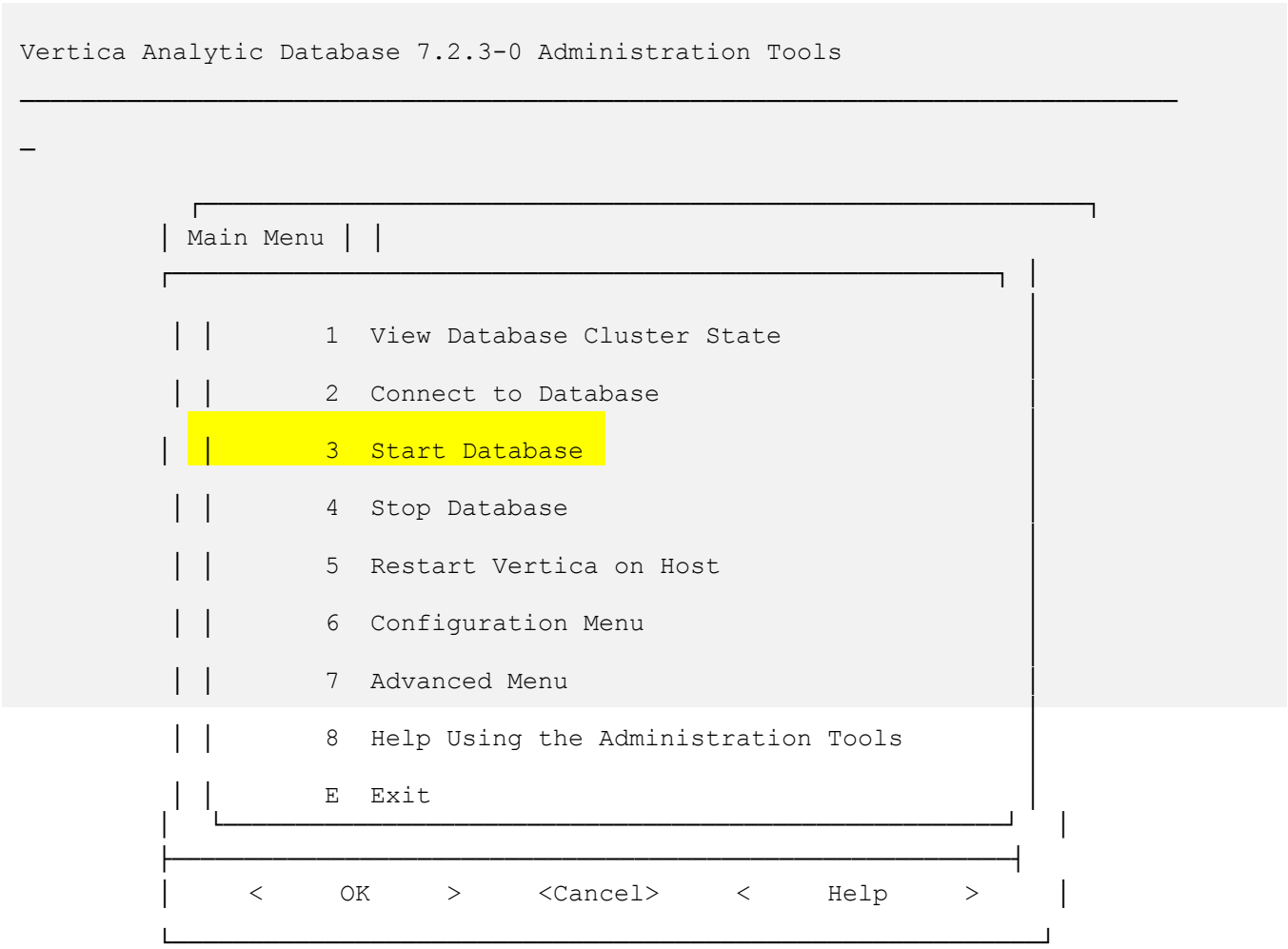
```
Vertica Analytic Database 7.2.3-0 Administration Tools
──────────────────────────────────────────────────────────────────────────────

─

                    ┌──────────────────────────┐
                    |  DB | Host | State      |
                    | ----+------+------       |
                    -                          |
                    |                DOWN_     |
                    |  sw_| ALL__| _           |
                    |                          |
                    |                          |
                    ├──────────────────────────┤
                    |       <  OK  >           |
                    └──────────────────────────┘
```

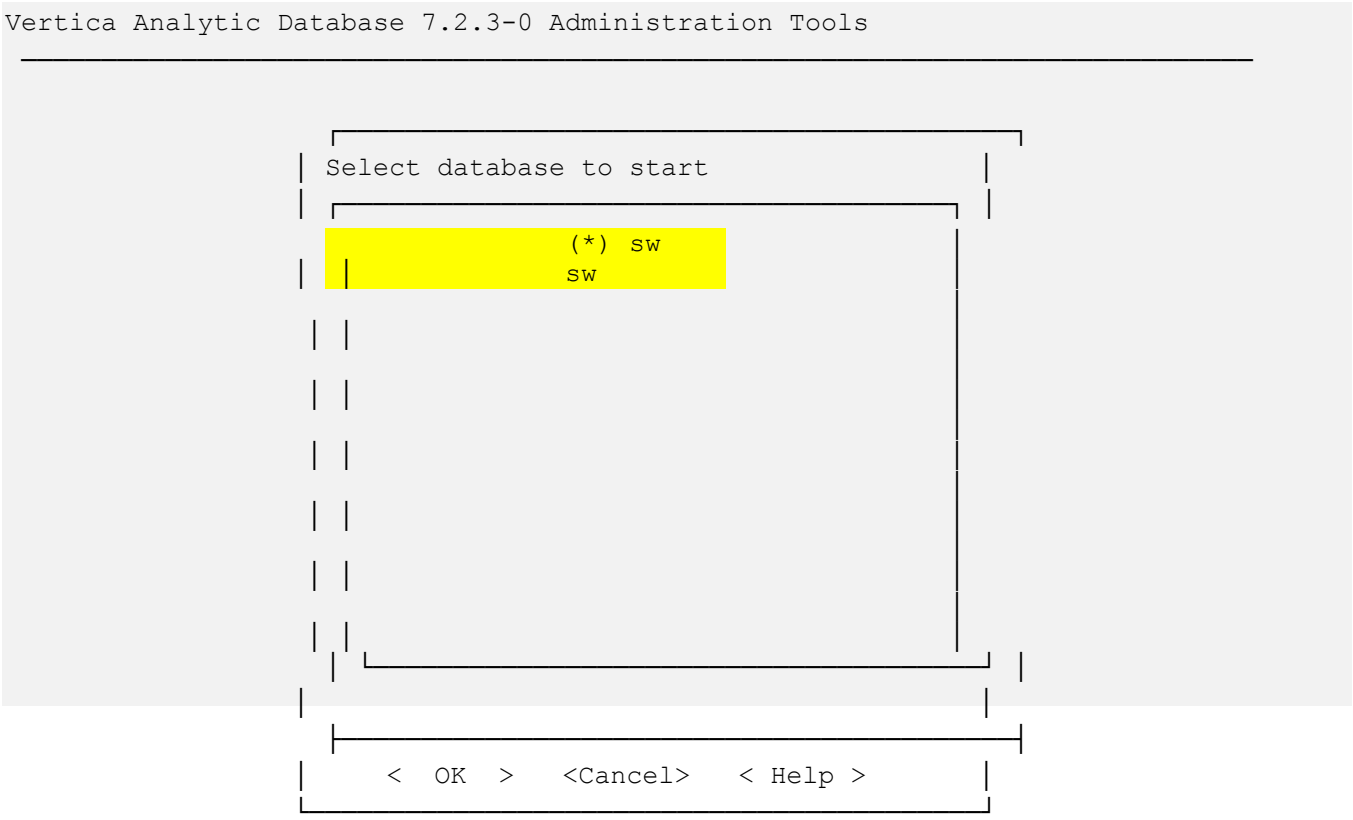
10. オプション 3 [データベースの開始（Start Database）] を選択します。

```
Vertica Analytic Database 7.2.3-0 Administration Tools
```



11. SPACE バーを押して、sw データベースを選択します。

12. [OK] を選択します。



13. sw データベースのパスワード lan1cope を入力します。
14. [OK] を選択します。

```
Vertica Analytic Database 7.2.3-0 Administration Tools
 ──────────────────────────────────────────────────────────────────────────────


          ┌──────────────────────────────────────────────────────┐
          │ Enter the password for database sw: │ │            │
          ┌──────────────────────────────────────────────────┐ │
          │ │********                                        │ │
          │ └──────────────────────────────────────────────────┘ │
          │ │ │ │ │
          ├──────────────────────────────────────────────────────┤
          │ < OK > <Cancel> < Help > │
          └──────────────────────────────────────────────────────┘
```

15. アプライアンスの Vertica データベースが初期化を開始します。

```
*** Starting database: sw ***
Starting nodes:
v_sw_node0001 (127.0.0.1)
Starting Vertica on all nodes.Please wait, databases with large catalog may take a while to initialize.
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Error starting database, no nodes are up
Press RETURN to continue
```

16. 起動が成功した場合は、これで終わりです。メニューを終了し、アプライアンスのコマンド ライン インターフェイスからログアウトします。
17. 起動が（上記のように）失敗した場合、RETURN を押して続行します。

18. 最後の正常なエポックにデータベースをロールバックするプロンプトが表示されます。
19. [はい（Yes）] を選択します。Vertica データベースは、最後の正常なエポックから初期化しようとします。

```
Vertica Analytic Database 7.2.3-0 Administration Tools
 ──────────────────────────────────────────────────────────────────────────────



┌──────────────────────────────────────────────────────────────────────────┐
│ Database startup failed, but enough information is │ │ available to start
the database from a previous epoch.│ │ WARNING: if you say 'yes', changes
made to database after │ │ '2017-03-14 16:09:00.029106+00' (epoch 809) will
be permanently lost.│ │ │ Do you really want to restart the database from
'2017-03-14 │ │ 16:09:00.029106+00' (epoch 809)? │ │ │



├──────────────────────────────────────────────────────────────────────────┤
│ < Yes > < No > │
└──────────────────────────────────────────────────────────────────────────┘
```

20. 最後の正常なエポックにデータベースをロールバックするプロンプトが表示されます。
21. [はい（Yes）] を選択します。Vertica データベースは、最後の正常なエポックから初期化しようとします。

```
*** Restarting database sw at epoch 809 ***
Starting nodes:
v_sw_node0001 (127.0.0.1)
Starting Vertica on all nodes.Please wait, databases with large catalog may take a while to initialize.
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (DOWN)
Node Status: v_sw_node0001: (UP)
```

22. これでデータベースがオンラインになったため、アプライアンスの Web インターフェイスにアクセスできるようになっているはずです。

以前のエポックへのロールバックが失敗した場合は、DB 機能を回復するためにアプライアンスを工場出荷時のデフォルトに戻す必要があります。これにより、現在アプライアンス上にあるすべての設定とデータが消去されます。

現行のネットワーク設定を保存しているときに、アプライアンスを工場出荷時のデフォルトに復元する場合：

23. [システム設定（System Configuration）] メニューを使用するために、root または sysadmin として ssh/コンソール経由でアプライアンスにログインします。
24. 次のコマンドを入力して、System Configuration アプリケーションを起動します。

```
SystemConfig
```

25. [詳細（Advanced）] オプションを選択します。
26. [システムを工場出荷時のデフォルトに復元（Restore System to its Factory Defaults）] を選択します。
27. [OK] を選択して続行します。
28. 続行するには、[はい（Yes）] を選択します。
29. 現在のネットワーク設定を保存/保持してから復元プロセスを開始するには、[いいえ（No）] を選択します。

復元プロセスが完了すると、管理 IP アドレスでアプライアンスの Web インターフェイスにアクセスできるようになります。アプライアンスで行った設定は失われます。

シナリオのまとめ

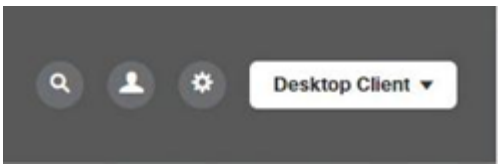
製品の SMC インターフェイスを使用する前に、個々のアプライアンスに関する設定項目を設定しました。すべてのタスクは、フロー データの処理前にアプライアンスを最適に設定し、フロー データが実際に FC に送信されるようにすることを目的としていました。高度なトラブルシューティング タスクを実行できるように、SSH が有効化/確認されました。設定済みの DNS サーバにアクセスするアプライアンスの機能が確認されました。NTP サーバにアクセスするアプライアンスの機能も確認されました。フロー センサー アプライアンスの高度な設定が設定されました。フロー データと ISE syslog データを Stealthwatch が処理できるように、UDPD とその転送ルールが設定されました。最後に、アプライアンスの起動に関する問題が発生した場合に、問題を解決するための予備的な手順が提示されています。次に、SMC Java UI で実行される設定項目に移ります。

シナリオ 4.　SMC インターフェイスの設定

この時点で個々のアプライアンスが完全に設定されましたが、ソリューション全体について、SMC インターフェイスで追加の設定を行う必要があります。SMC インターフェイスを使用して、お客様のために Stealthwatch の設定を完了させます。

手順

1. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. URL フィールドで「https://198.18.128.136」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
3. 認証を求められた場合は、ユーザ名 admin、パスワード C1sco12345 を使用して、ログインします。
4. Stealthwatch の Web インターフェイスにログインします。
5. 画面の右上にある [デスクトップ クライアント（Desktop Client）] ボタンをクリックします。



6. Web ブラウザで、SMC Java インターフェイスのロードに使用する Java JNLP ファイルをダウンロードします。
7. Chrome ブラウザで JNLP のダウンロードに関するプロンプト（Web ブラウザの左下隅）が表示されたら、ファイルを [保持する（Keep）] をクリックします。

8. [保持する（Keep）] ボタンをクリックしたら、Chrome ブラウザの左下にある、ダウンロードされた「launch_512.jnlp」ファイルをクリックします。

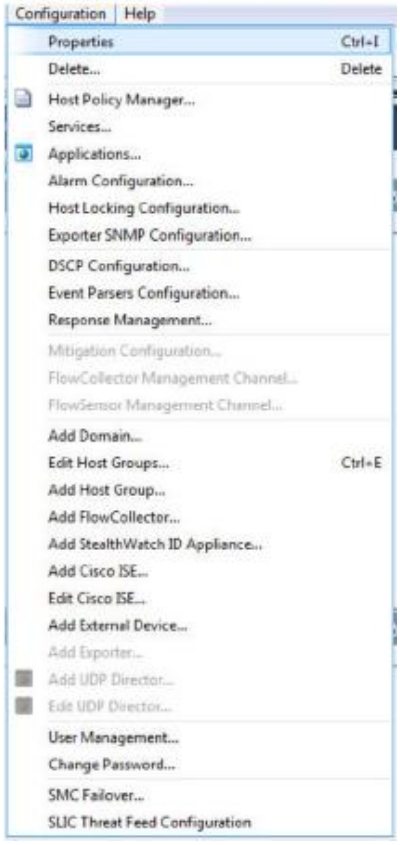
9. Java によって、ファイルのロードに関するセキュリティ プロンプトが表示される場合があります。表示されたら、[続行（Continue）] または [実行（Run）] をクリックします。

10. 認証を求められた場合は、ユーザ名 admin、パスワード C1sco12345 を使用して、ログインします。
11. SMC Java インターフェイス 1 にサインインします。

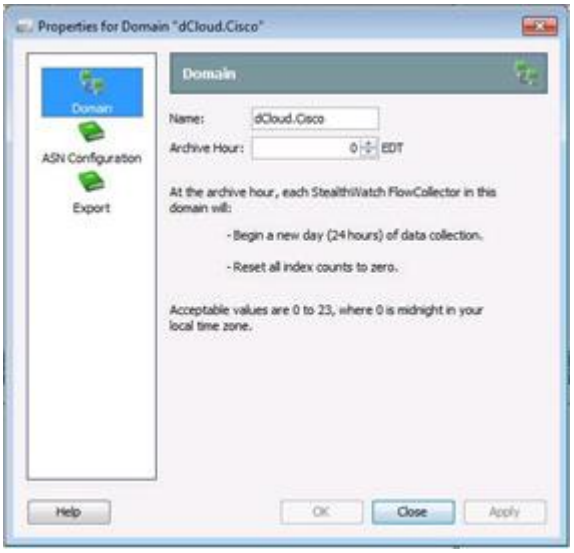
アーカイブ時刻の設定

[アーカイブ時刻（Archive Hour）] の値により、Stealthwatch ドメインでデータを収集する 1 日のサイクルの開始時刻や、High Concern Index や High Target Index などのインデックスの値がリセットされる時刻が定義されます。お客様環境では、アーカイブ時刻を、Stealthwatch のプライマリ ユーザ/管理者が存在するタイム ゾーンの午前 0 時に設定します。現在のお客様は米国東部にいるため、アーカイブ時刻には米国東部時間の午前 0 時が使用されます。

1. SMC の左ペインにある [dCloud.Cisco] ドメインのエントリを選択後、画面上部にある [設定（Configuration）] メニューをクリックして、[プロパティ（Properties）] メニュー項目を選択します。



2. [ドメイン dCloud.Cisco のプロパティ（Properties for Domain dCloud.Cisco）] ウィンドウが表示されたら、左ペインの [ドメイン（Domain）] メニューを選択し、[アーカイブ時刻（Archive Hour）] フィールドの値を 0 に設定します。[OK] ボタンをクリックして変更を保存します。



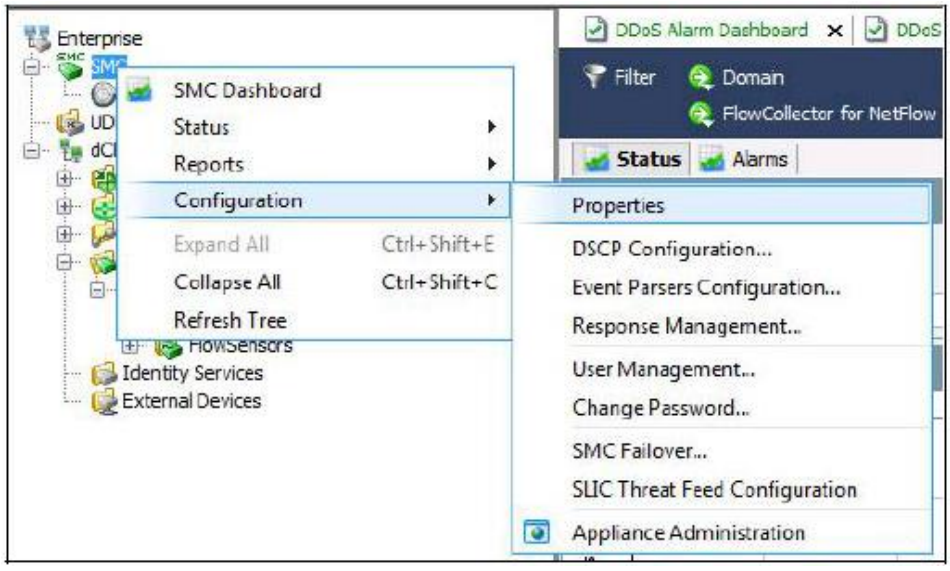
3. 以上で設定は終了し、次の手順に進むことができます。

SMTP リレー設定

Stealthwatch がアラームと定期レポートを電子メールで送信できるようにするには、SMC で SMTP リレー サーバを定義する必要があります。お客様からは、次の SMTP サーバ リレー アドレスと、Stealthwatch から電子メールが送信されるアドレスが提供されています。このラボでは、アプライアンスの設定段階でこれを定義しておく必要があります。定義している場合は、ここで設定を確認します。

- [送信元電子メール アドレス（From Email Address）]：Stealthwatch@dCloud.Cisco.local
- [SMTP リレー アドレス（SMTP Relay Address）]：198.18.128.134

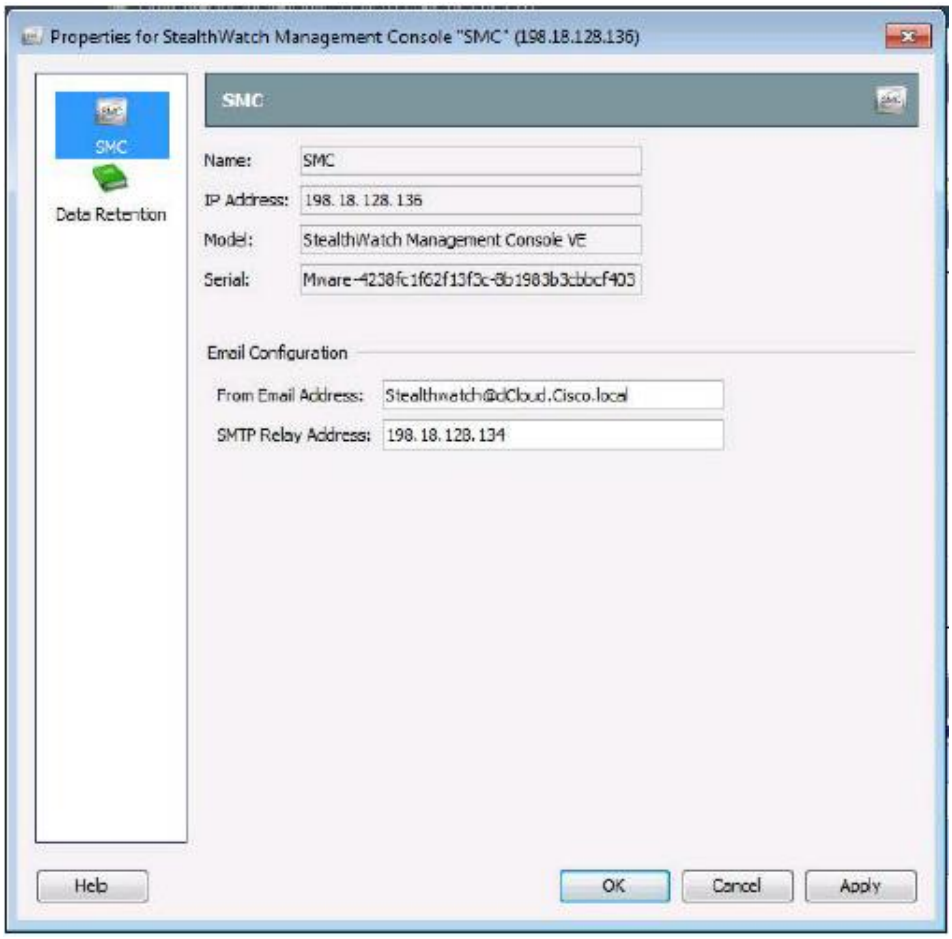
1. 左ペインで SMC オブジェクトを選択して右クリックし、[設定（Configuration）] メニューを選択して、[プロパティ（Properties）] メニュー項目を選択します。



2. SMC プロパティ ウィンドウが表示されたら、左側にある [SMC] メニューを選択し、2 つのフィールドに次の値を入力して、[OK] をクリックします。

    a. [送信元電子メール アドレス（From Email Address）]：Stealthwatch@dCloud.Cisco.local

    b. [SMTP リレー アドレス（SMTP Relay Address）]：198.18.128.134

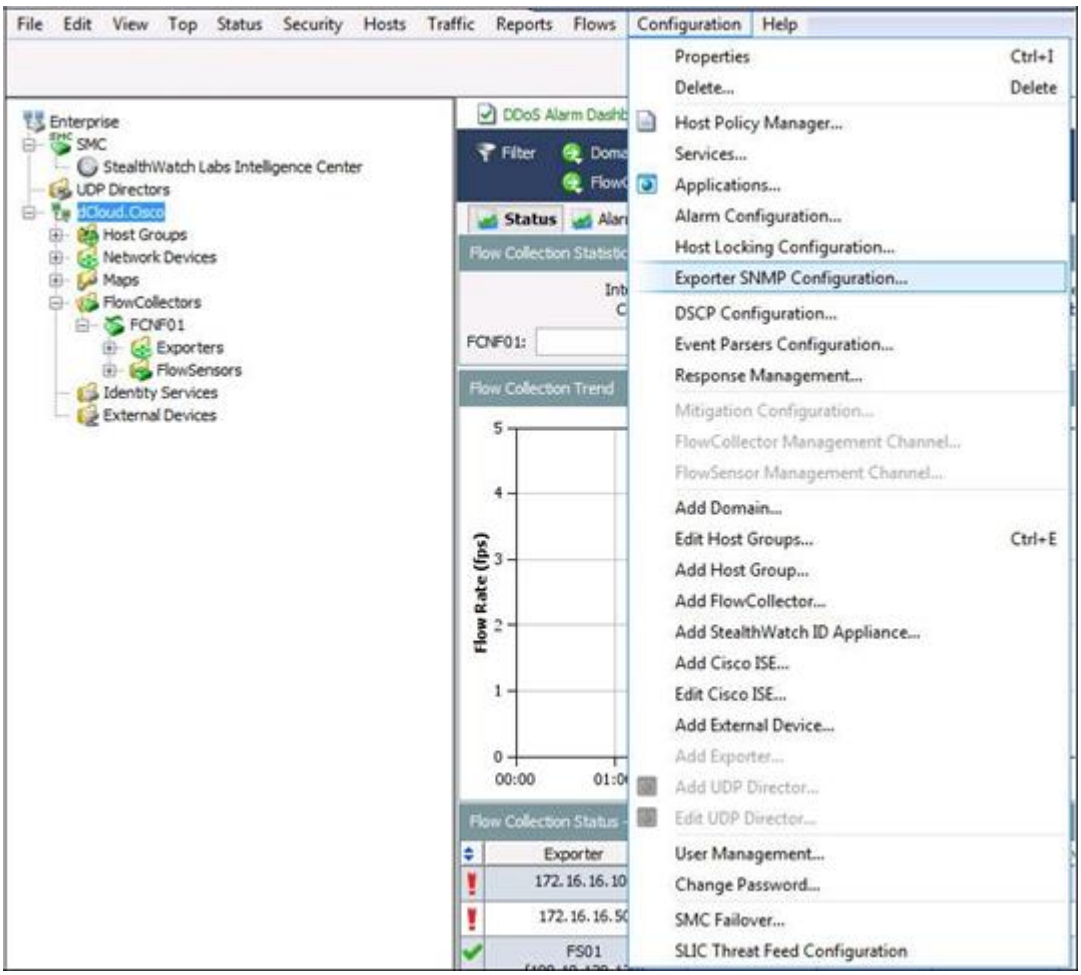


注：[SMTP リレー アドレス（SMTP Relay Address）] の値には、有効な SMTP サーバの IP アドレスまたは DNS を指定できます。指定されたサーバでは、SMC IP アドレスから SMTP サーバを通じてメールをリレーできるようにする必要があります。その場合、SMTP サーバのお客様環境で設定の変更が必要になることがあります。[送信元電子メール アドレス（From Email Address）] の値は、お客様環境内の有効なメールボックスである必要はありませんが、ドメイン名とお客様の電子メール アドレスの DNS ドメイン名が一致していることが推奨されます。SMC が電子メールを送信すると、[送信元電子メール アドレス（From Email Address）] フィールドに入力した値が、SMC から送信される定期レポートとアラームの送信者になります。

エクスポータ SNMP の設定

Stealthwatch では SNMP を使用して、NetFlow をフロー コレクタに送信するインターフェイスに関連するインターフェイス名、タイプ、説明、および速度を取得します。Stealthwatch では、設定の異なる複数の SNMP コミュニティ ストリングを使用できます。次に SMC で、お客様のエクスポータ デバイスのポーリングに使用する SNMP コミュニティ ストリングを設定します。

1. SMC ウィンドウの左ペインにある [dCloud.Cisco] ドメインを強調表示します。[設定（Configuration）] メニューをクリックし、[エクスポータの SNMP 設定（Exporter SNMP Configuration）] メニュー項目を選択します。



2. [追加（Add）] ボタンをクリックします。

3. [エクスポータの SNMP 設定の追加（Add Exporter SNMP Configuration）] ウィンドウが表示されます。次に示す SNMP 設定の値を指定し、[OK] ボタンをクリックします。

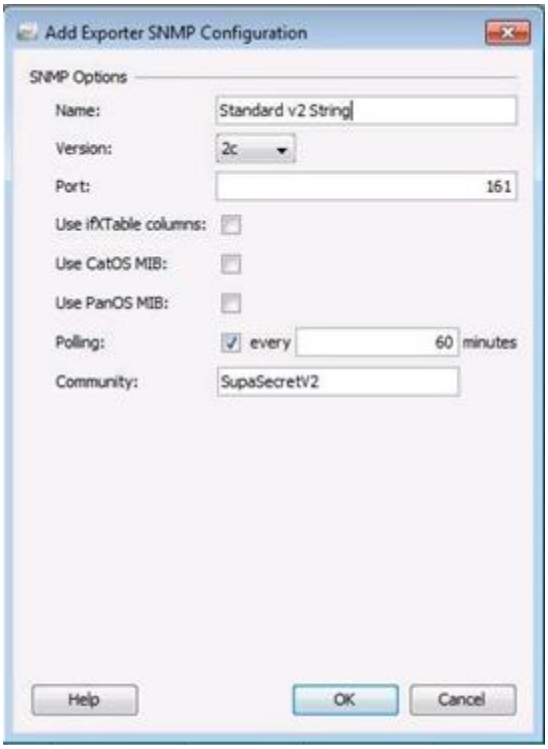
    a. [名前（Name）]：Standard v2 String

    b. [バージョン（Version）]：2c

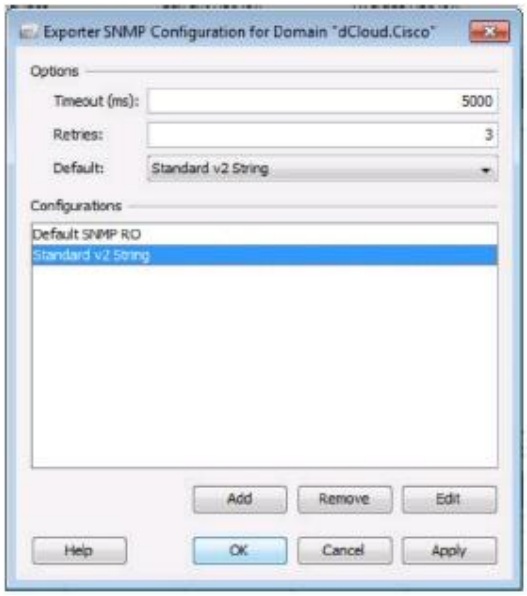
    c. [ポート（Port）]：161

    d. [ポーリング（Polling）]：60 分ごと（every 60 minutes）

    e. [コミュニティ（Community）]：SupaSecretV2



4. ドロップダウン メニューのデフォルトの値を [標準の v2 ストリング（Standard v2 String）] に変更して、[OK] ボタンをクリックします。



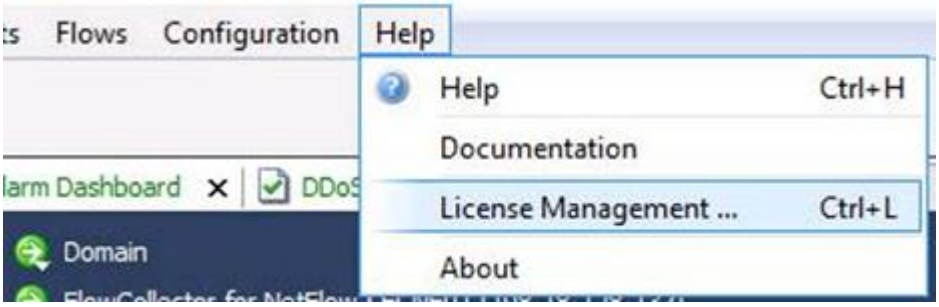
5. お客様から提供される、SNMP コミュニティ ストリングを作成しました。ラボの次の手順に進みます。

注:Stealthwatch では複数の SNMP 設定を作成できます。ごく稀に、お客様がすべてのネットワーク デバイスで SNMP コミュニティ ストリングを 1 つだけ使用している場合があります。一部のデバイスでは SNMP v2 を使用し、別のデバイスでは SNMP v3 を使用する場合もあります。これらすべての設定がサポートされています。最も多く使用されているコミュニティ ストリングをデフォルトのコミュニティ ストリングとして選択します。SMC はデフォルトのコミュニティ ストリングを使用して、すべてのデバイスとの通信を試みます。異なるコミュニティ ストリングを必要とするデバイスでは、個々の SNMP の設定を SMC 内でデバイスごとに手動で行うことができます。

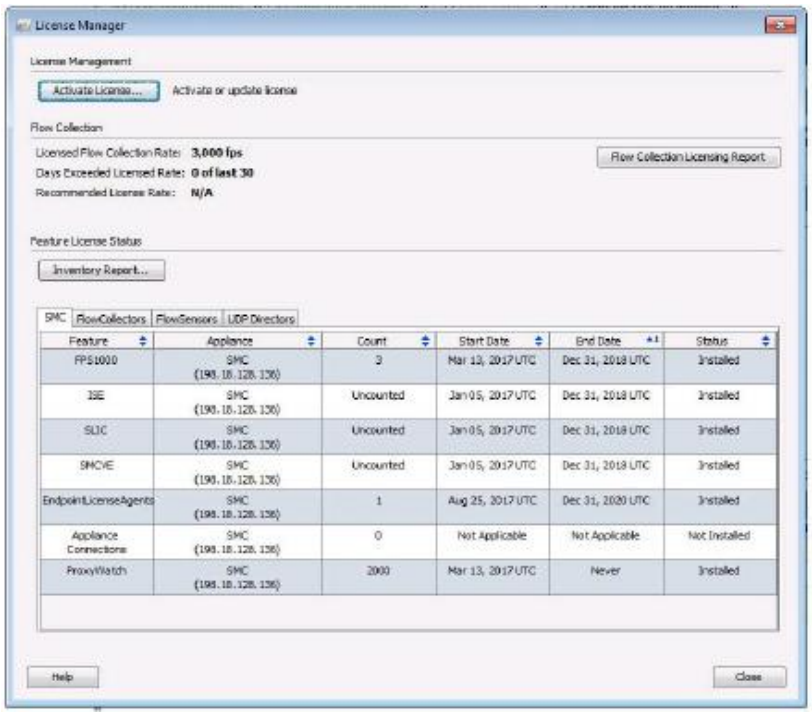
License Manager でのライセンスの確認

次に、適切なライセンスと機能がアプライアンスに適用されていることを確認します。お客様環境でアプライアンスが機能するには、正しいライセンスをインストールする必要があります。

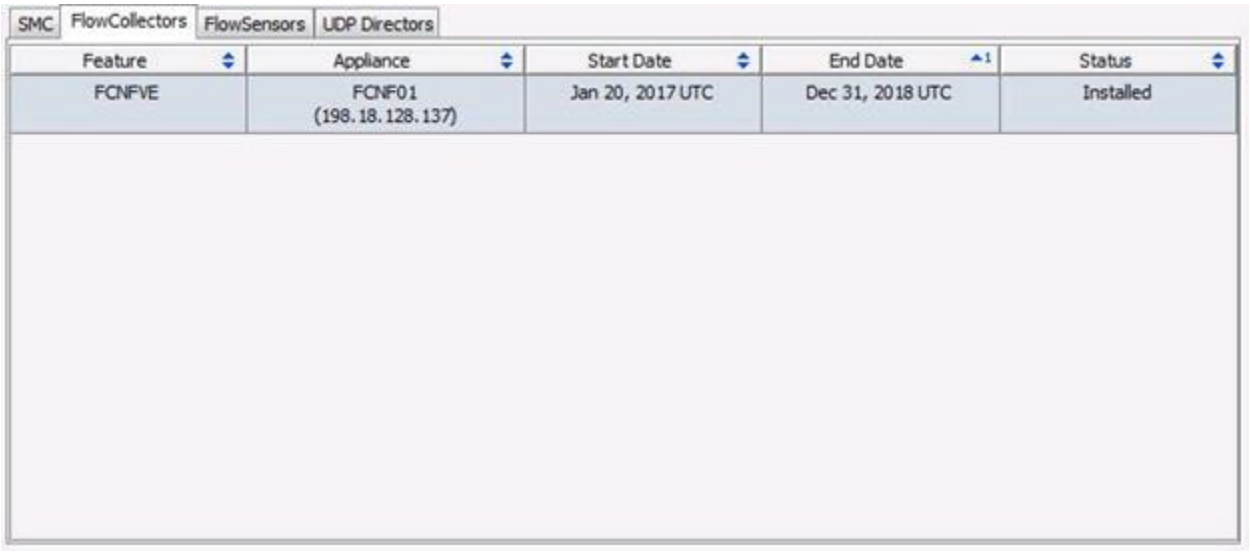
1. SMC Java UI にログインしていることを確認します。
2. [ヘルプ(Help)] メニューをクリックし、[ライセンス管理(License Management)] メニュー項目を選択します。



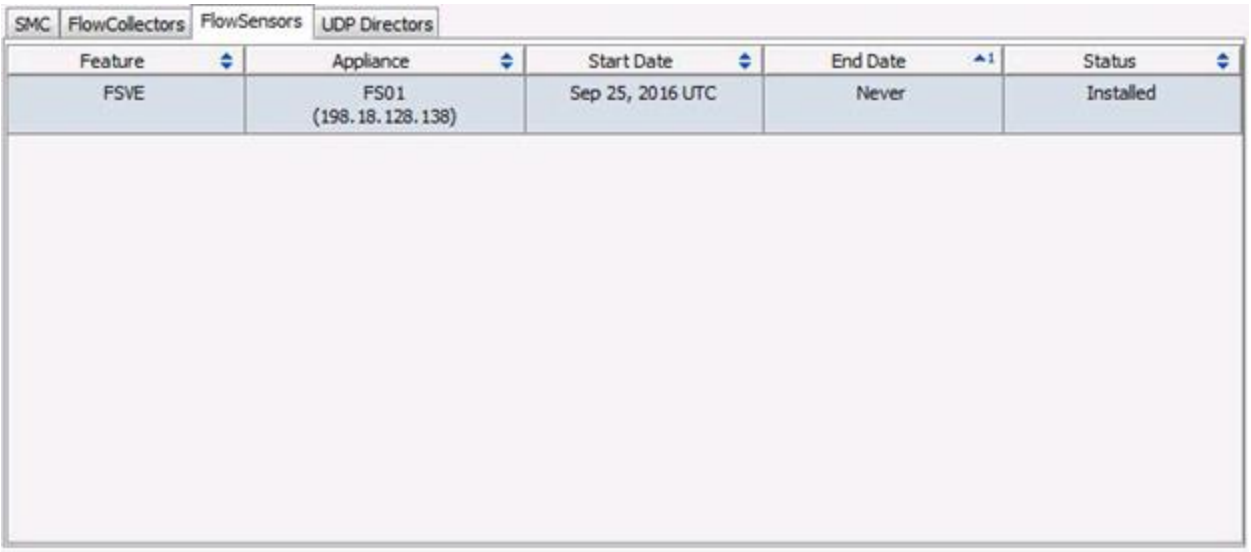
3. [機能ライセンスのステータス(Feature License Status)] セクションに、[SMC]、[フロー コレクタ(Flow Collectors)]、[フロー センサー(Flow Sensors)]、[UDP Director(UDP Directors)] タブが表示されます。これらのタブでは、使用中、または環境内のライセンスについて使用可能な、アプライアンスと SMC の機能が示されます。



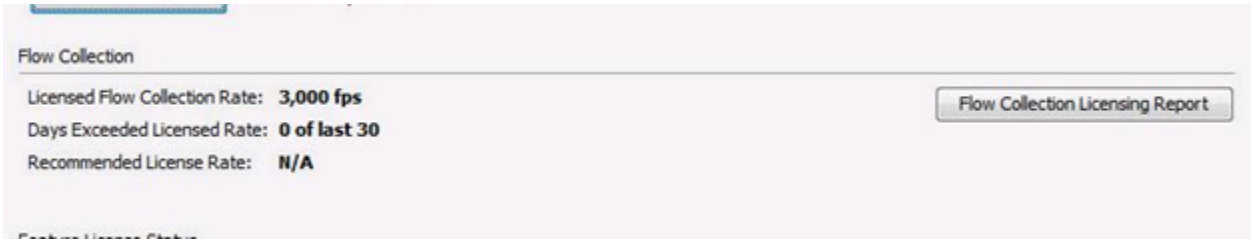
4. SMCVE アプライアンスのエントリを探し、[ステータス（Status）] が [インストール済み（Installed）] であることを確認します。
5. FPS1000 というラベルのエントリを探し、カウント列の値を確認します。これは、そのインストールでライセンスされている 1 秒あたりのフロー数を示します。
6. ISE というラベルのエントリを探します。これは、そのインストールで Cisco ISE との統合のライセンスが付与されているかどうかを示します。
7. SLIC というラベルのエントリを探します。これは、そのインストールで Stealthwatch Threat Feed のライセンスが付与されているかどうかを示します。
8. [フロー コレクタ（Flow Collectors）] タブをクリックして、FCNFVE（Flow Collector for NetFlow Virtual Edition）のエントリのステータスが [インストール済み（Installed）] であることを確認します。



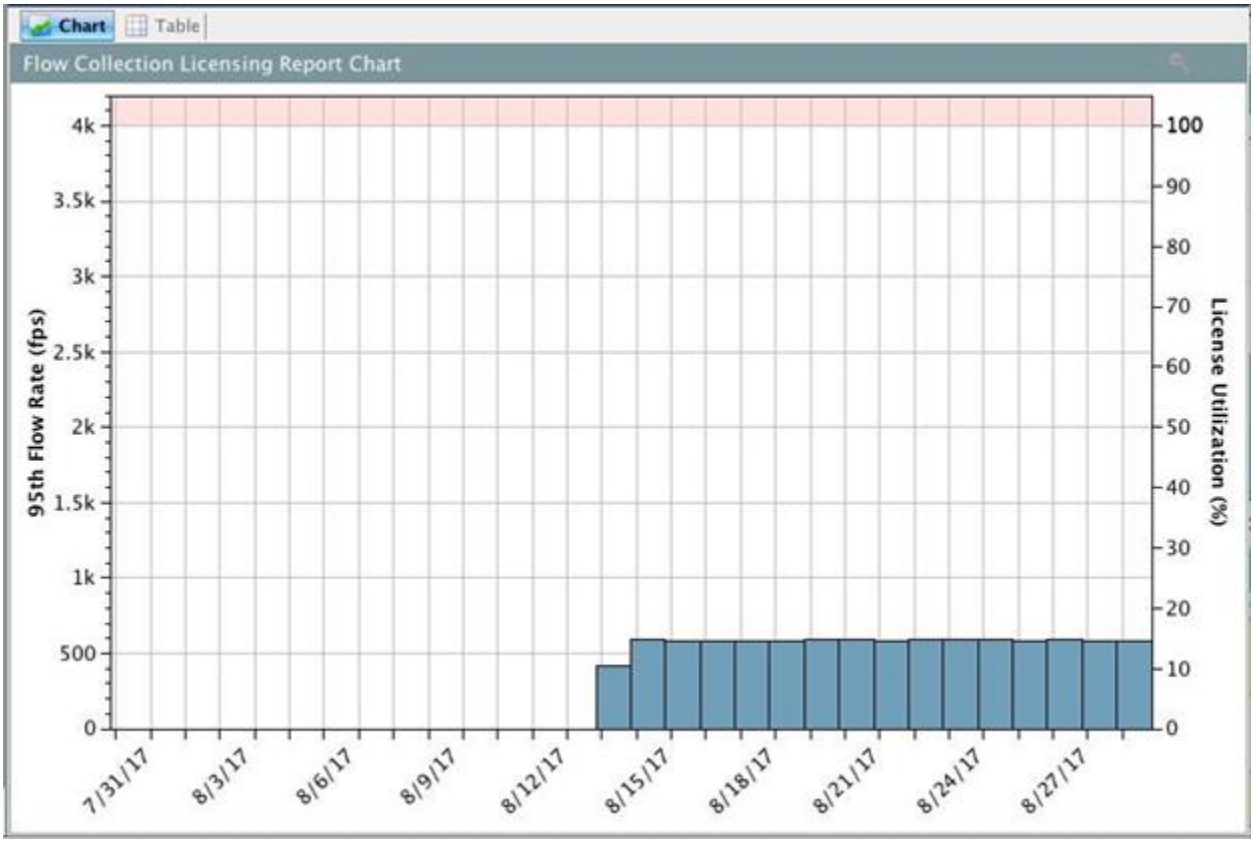
9. [フロー センサー（Flow Sensors）] タブをクリックして、FSVE（Flow Sensor Virtual Edition）のエントリのステータスが [インストール済み（Installed）] であることを確認します。



10. License Manager 画面の [フロー コレクション（Flow Collection）] セクションを確認します。ライセンスされたフロー コレクション率と、直前 30 日間に FPS ライセンスを超過した期間があったかどうかが示されます。[フロー コレクションのライセンス レポート（Flow Collection Licensing Report）] ボタンをクリックします。



11. [フロー コレクションのライセンス レポート チャート（Flow Collection Licensing Report Chart）] には、カスタマー ライセンスに対してカウントされた FPS 数と、ライセンスを超過した日の有無を示す、過去 30 日間のデータが表示されます。このドキュメントは 1 つのドメインに関して合計したものですが、FC ダッシュボードに表示される FPS 数はその FC についてだけのものであり、FS アプライアンスによって生成されたフローは、カスタマー ライセンスに対してカウントされないことがあります。このドキュメントは、FPS ライセンスのコンプライアンスを判定するために使用します。



12. このお客様は、ライセンス制限の範囲内であり、環境の規模が拡大してもかなりの余裕があると考えられます。お客様が初期インストール時にすでに FPS の制限を超えていた場合は、購入されたすべての FPS ライセンスが SMC に割り当てられていることを確認し、必要に応じてアカウント チームに連絡して、設計フェーズで現在の FPS ロードが考慮されているかどうかを調査します。

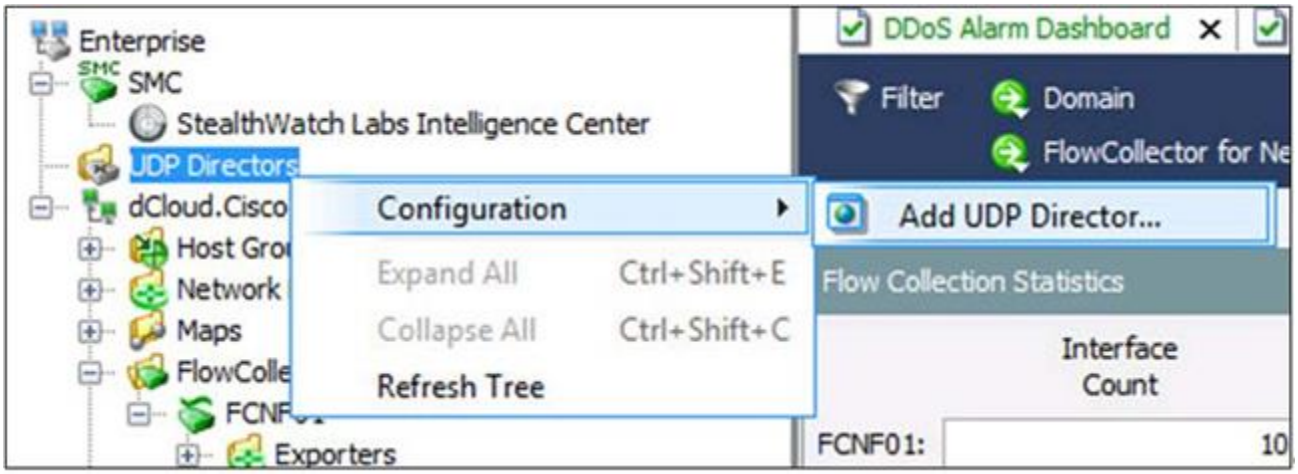
13. お客様のアプライアンスのライセンスと機能がインストールされていることを確認しました。ラボの次の手順に進みます。

注：UDP Director は SMC を通じてライセンスが付与されず、アプライアンス自体でライセンスされます。すべてのアプライアンスのライセンスは、[設定（Configuration）] > [ライセンス（Licensing）] にあるアプライアンスの Web 管理ページを通じて管理できます。

UDP Director アプライアンスを SMC に追加

UDP が処理するトラフィックは SMC で認識できるため、UDP はただちに SMC の管理下に置かれることはなく、SMC の [エンタープライズ（Enterprise）] ツリーには自動的に追加されません。インストール中に SMC に手動で追加する必要があります。次に UDPD を SMC に追加します。

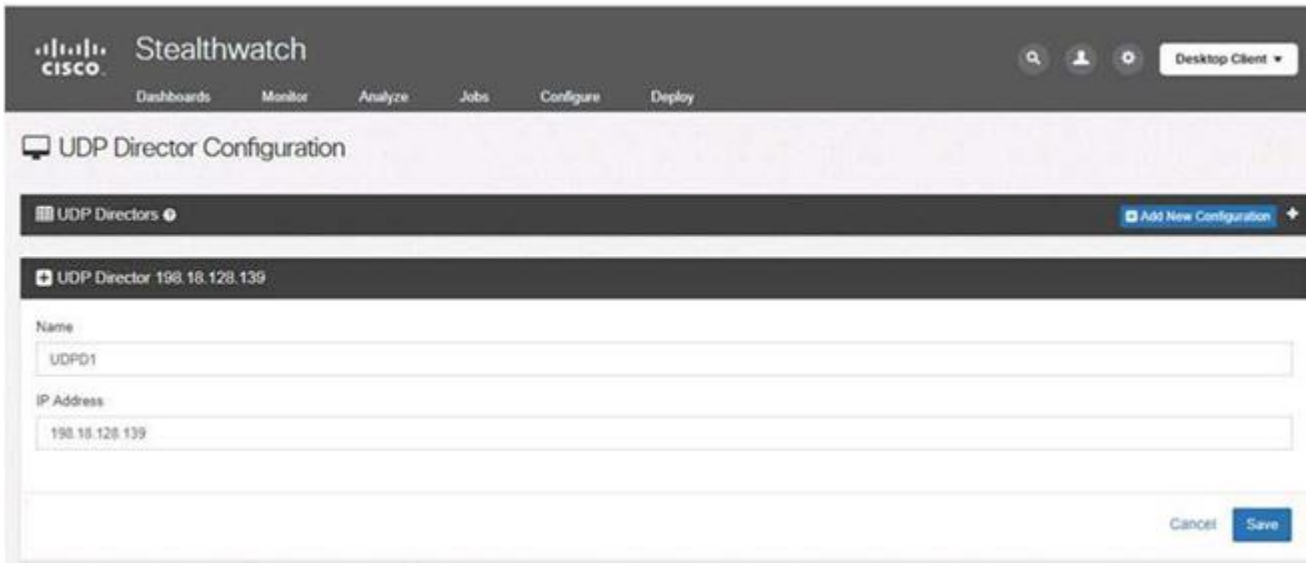
1. SMC Java UI の [エンタープライズ（Enterprise）] ツリーの UDP Directors エントリを右クリック後、[設定（Configuration）] メニューをクリックして、[UDP Director の追加（Add UDP Director）] メニュー項目を選択します。



2. 設定を行う SMC Web インターフェイスが表示されます。設定フィールドに次の値を入力します。終了したら、[続行（Save）] ボタンをクリックします。

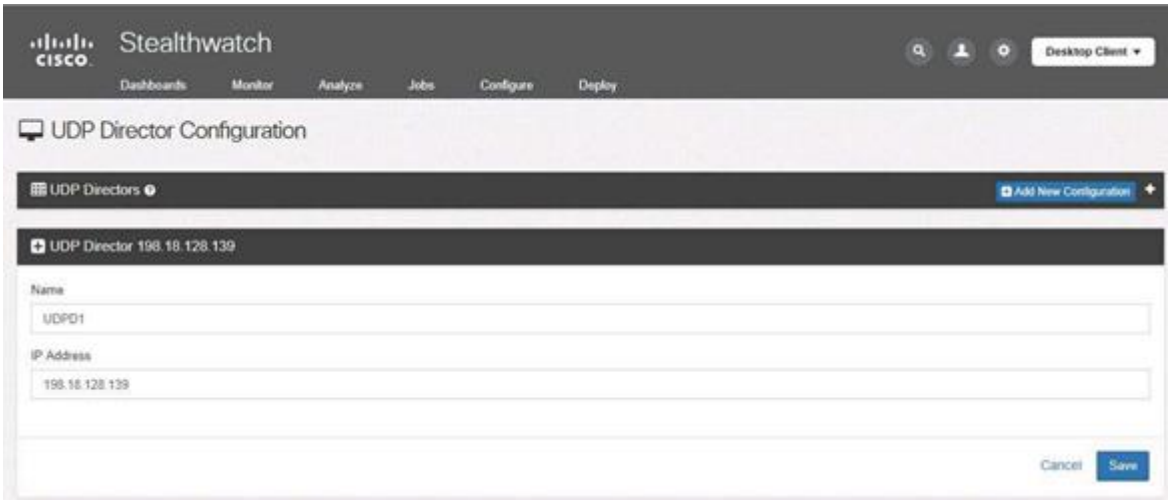
    a. [名前（Name）]：UDPD1

    b. [IP アドレス（IP Address）]：198.18.128.139



3. 次のエラーが表示されます。

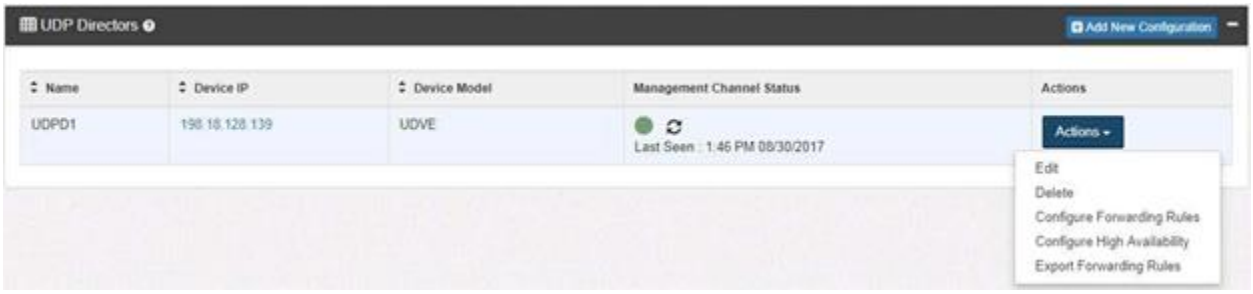
4. SMC から UDP Director を管理するには、管理チャネルを確立する必要があります。ここで、管理チャネルを有効にします。
5. URL フィールドで「https://198.18.128.139/」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [UDPD] を選択して、UDPD アプライアンスの Web 管理インターフェイスにアクセスします。
6. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345
7. UDPD アプライアンス ページのサイド メニューから [設定（Configuration）] > [管理システムの設定（Management Systems Configuration）] を選択します。
8. [管理システムの設定（Management Systems Configuration）] ページで、[新しい管理システムの追加（Add New Management System）] ボタンをクリックします。
9. [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 アドレスである 198.18.128.136 を入力します。[適用（Apply）] をクリックします。
10. SMC Web インターフェイスに戻り、設定を行います。設定フィールドに次の値を入力します。終了したら、[続行（Save）] ボタンをクリックします。
    a. [名前（Name）]：UDPD1
    b. [IP アドレス（IP Address）]：198.18.128.139



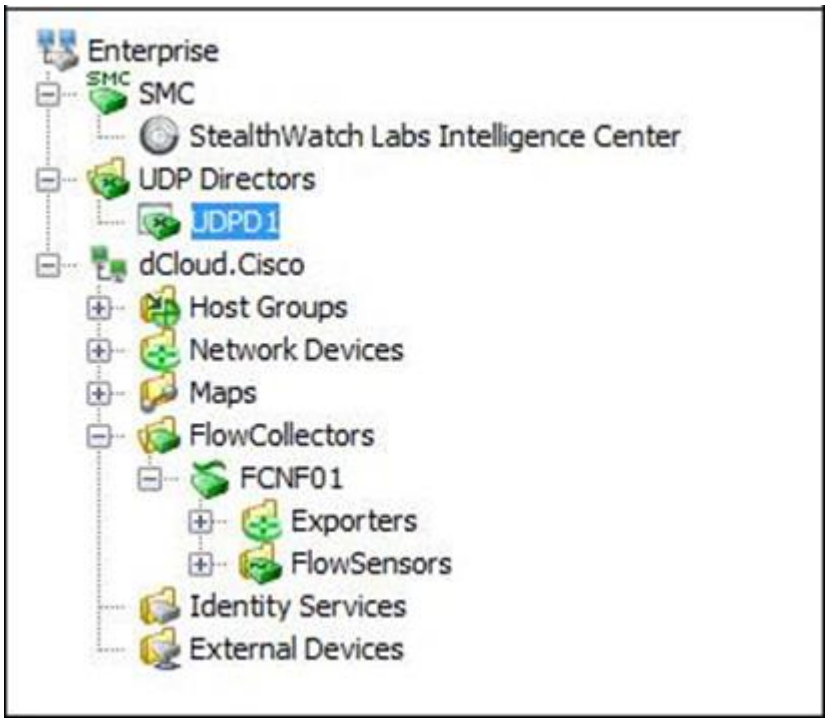
11. これで、UDPD が正常に追加されているはずです。

注：右上隅にある設定用の歯車アイコンをクリックし、[UDP Director 設定（UDP Director Configuration）] を選択して、WebUI から [UDP Director 設定（UDP Director Configuration）] ページに直接アクセスすることもできます。UDPD を管理するように SMC を設定すると、SMC から転送ルールを表示、変更することも可能です。

12. これで、UDP Director エントリが Web インターフェイスで表示されます。



SMC Java インターフェイスにも表示されます（Java インターフェイスでは更新が必要な場合があります。[UDP Director] を右クリックし、[ツリーの更新（Refresh Tree）] を選択します）。



13. SMC インターフェイスに UDPD を追加しました。ラボの次の手順に進みます。

注：UDP Director を SMC に追加しても、製品の動作や UDP Director の設定は技術上変更されません。ただしこれは運用上のベスト プラクティスであり、ステータス情報の取得と UDPD アプライアンスの管理が簡単になります。通常 UDPD は SMC には表示されないため、お客様が UDPD の導入に気づかない場合もあります。SMC に追加することで、NetFlow の設定に関する将来的な問題を回避できます。

シナリオのまとめ

このシナリオでは、さまざまな日次の値を SMC でリセットする時刻を決定するために、アーカイブ時刻の設定を行いました。SMC が電子メール通知を送信できるように、SMTP を設定しました。SNMP コミュニティ ストリングを設定し、SMC が、NetFlow を FC に送信して追加データを収集する対象のネットワーク デバイス（エクスポータ）のポーリングに使用できるようにしました。アプライアンスのライセンスが正しく適用され、現在の FPS のボリュームがライセンス数を超えていないことを確認しました。将来の運用タスクや管理に役立つように、UDP Director を SMC インターフェイスに追加しました。

シナリオ 5.　ネットワーク テレメトリ データの確認

すべての Stealthwatch アプライアンスを設定したので、次に Stealthwatch がお客様環境からのフロー データを処理していることを確認します。SMC のフロー コレクタ ダッシュボードのドキュメントを使用して、FC がお客様のエクスポータ デバイスからの NetFlow データを認識していることを確認します。また、特定のエクスポータからのデータを確認し、Stealthwatch 用に適切にフォーマットされているかどうか判定します。

手順

エクスポータの状態

フロー データを Stealthwatch に送信する、対象となるすべてのネットワーク デバイスが、SMC インターフェイスでエクスポータとして表示されることを確認することが重要です。お客様のインベントリ内のネットワーク デバイスが Stealthwatch に表示されない場合は、お客様のネットワークのその部分を可視化できていない可能性があります。これは、そのデバイスが NetFlow データを送信するように設定されていないか、Stealthwatch に対する NetFlow トラフィックを何かがブロックしていることが原因だと考えられます。

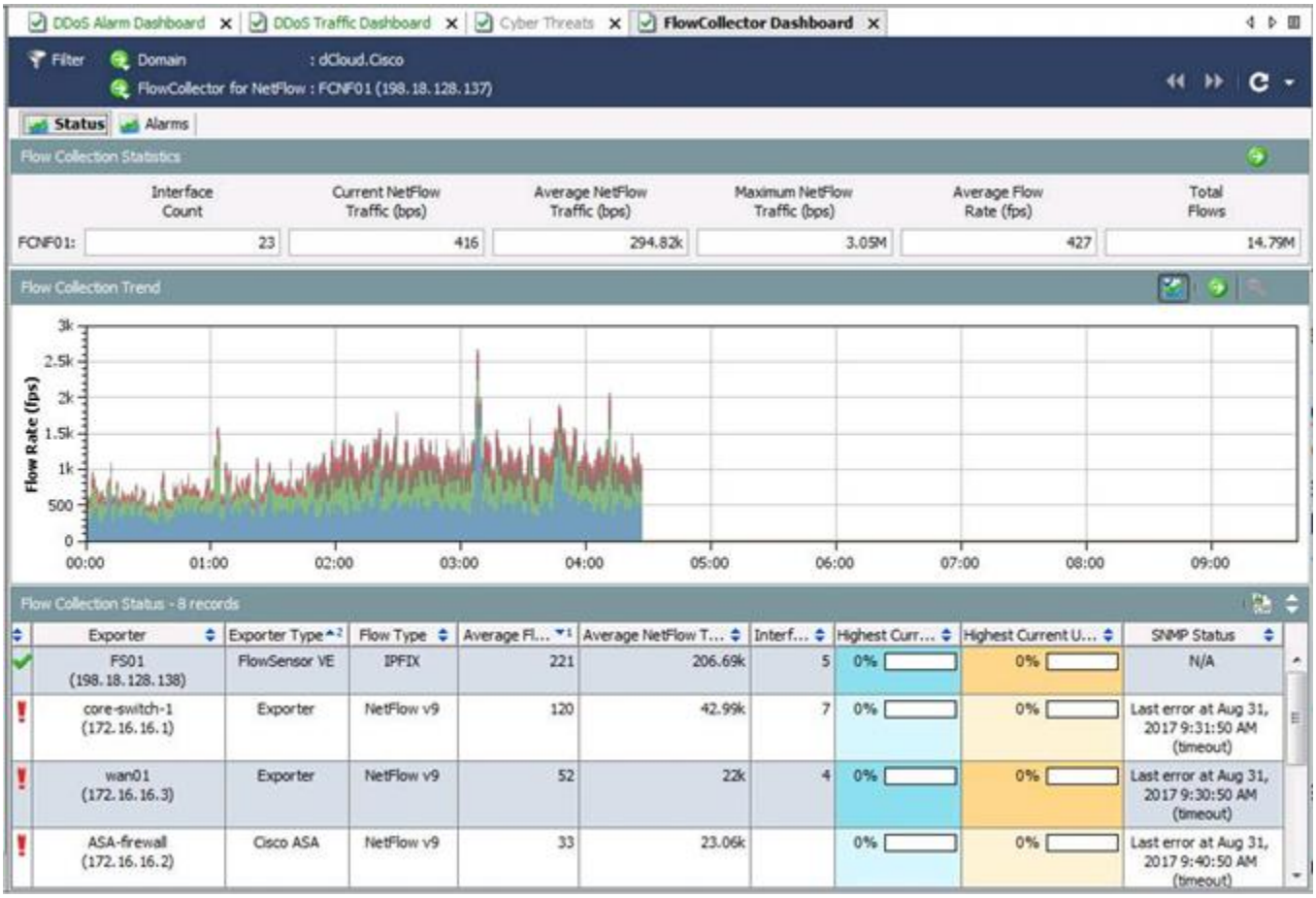
さらに SMC に表示されるデバイスについても、送信されるフロー データが Stealthwatch 用に最適化されて表示されることを確認する必要があります。NetFlow データをフロー コレクタに（この例では UDPD を使用して）送信するエクスポータ（ルータ、スイッチ、ファイアウォールなど）で、最適な NetFlow 設定がなされていることを確認します。

お客様から、Stealthwatch プロジェクトの対象としてフロー データを送信するネットワーク デバイスのリストが提供されています。

- 172.16.16.1
- 172.16.16.2
- 172.16.16.3
- 172.16.16.4
- 172.16.16.50
- 172.16.16.100

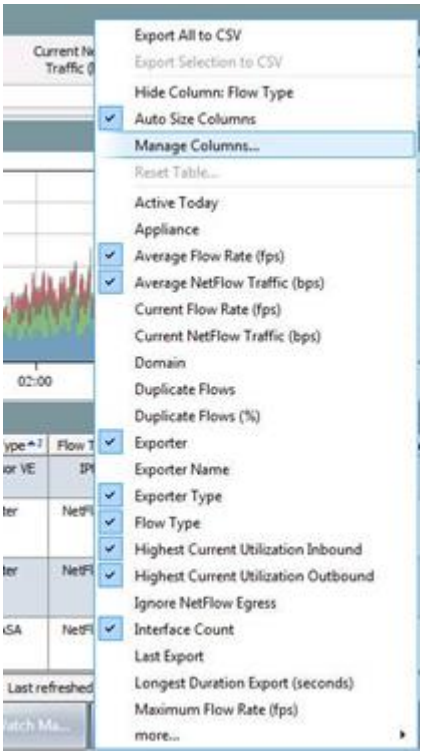
1. [SMC Java] インターフェイスを開きます。
2. 画面左側の [エンタープライズ（Enterprise）] ツリー ペインで、[dCloud.Cisco] ドメインを展開後、[フロー コレクタ（Flow Collectors）] コンテナを展開して、[FCNF01] フロー コレクタをダブルクリックします。

3. [フロー コレクタ ダッシュボード（Flow Collector Dashboard）] ドキュメントが表示されます。
   - [フロー コレクタ ダッシュボード（Flow Collector Dashboard）] では、ドキュメントの上部に統計情報ペインがあり、FC で処理される NetFlow トラフィックの量に関する詳細が表示されます。
   - ドキュメントの中央にある [フロー コレクションの傾向（Flow Collection Trend）] ペインには、FC が処理している 1 秒あたりのフロー数（FPS）が、エクスポータごとに時系列で表示されます。
   - ドキュメントの下部にある [フロー コレクション ステータス（Flow Collection Status）] ペインには、エクスポータと、各エクスポータで処理される NetFlow データに関する情報が表示されます。

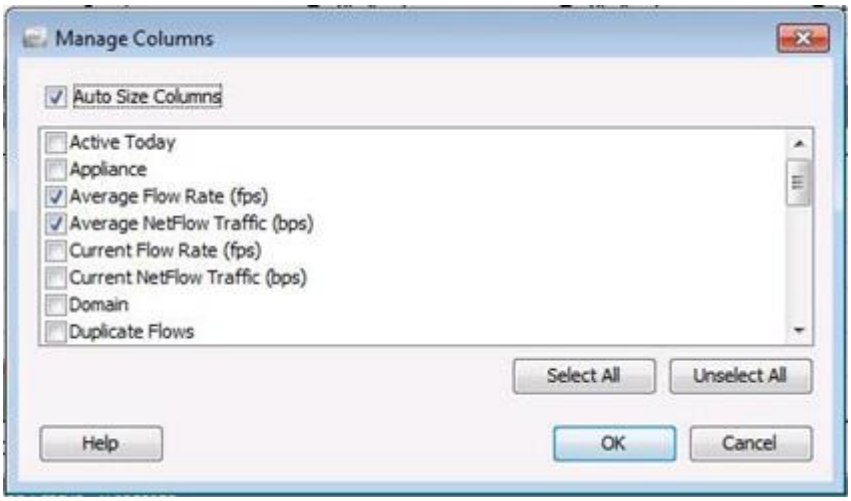


4. [フロー コレクションの傾向（Flow Collection Trend）] ペインで、フロー コレクタの現在の FPS ロードを確認します。各フロー コレクタ モデルは、パフォーマンスを低下させずに処理できる FPS の値で評価されます。特に初期のインストールでは、FC が過負荷になっていないことを確認してください。
5. [フロー コレクション ステータス（Flow Collection Status）] ペインには、使用可能なすべての列がデフォルトで表示されるわけではありません。次に、FC が受信するフロー データの質を判定するためのデータを追加します。

6. [フロー コレクション ステータス（Flow Collection Status）] ペインで、[エクスポータ（Exporter）] などの列ヘッダーを右クリックし、[列の管理（Manage Columns）] メニュー項目を選択します。



7. [列の管理（Manage Columns）] 画面が表示され、ドキュメントで必要な列を選択できます。



8. 次の列エントリの横にあるボックスにチェックマークを入れ、[OK] ボタンをクリックします。
   - [現在のフロー レート（fps）（Current Flow Rate (fps)）]
   - [前回のエクスポート（Last Export）]
   - [エクスポート最長期間（秒）（Longest Duration Export (seconds)）]

9. [エクスポータ(Exporter)] 列には、FC に対する NetFlow データの送信元であるデバイスの IP アドレスが表示されます。SMC が DNS で逆引き参照(PTR)レコードを特定できた場合は、DNS 名も表示されます。対象となるすべてのデバイスがリストに表示されていることを確認してください。対象でありながらここに表示されないデバイスについては、NetFlow データが処理されないため、表示されない原因を調査する必要があります。

10. [現在のフロー レート(Current Flow Rate)] 列には、ドキュメントが前回更新されてから、エクスポータから FC に送信されている現在の FPS の値(1 秒あたりのフロー数)が表示されます(デフォルトでは 5 秒ごと)この値が空白であるか、非常に低い数値である場合は、対象のすべてのインターフェイスからデータがエクスポートされるように、デバイスが設定されない可能性があります。

11. [前回のエクスポート(Last Export)] 列には、エクスポータからフロー レコードが前回送信された日付と時刻が表示されます。アクティブなフローが処理されている限り、フロー データを毎分送信するようにデバイス設定する必要があるため、ほとんどの環境ではこの値が現在時刻に近くなります。デバイスによっては、トラフィック レベルが非常に低いネットワークや、特定の時間枠の中でアクティブになる冗長ネットワーク リンクがあるネットワークにインストールされる場合があります。ただし通常は、このフィールドのタイムスタンプが現在時刻に近くない場合は、エクスポータからのデータ受信に何らかの問題がある可能性があります。

12. [エクスポータのタイプ(Exporter Type)] 列には、フロー データを送信するデバイスを FC が認識する方法が示されます。ほとんどのルータやスイッチはエクスポータとして表示されますが、特に Cisco ASA やフロー センサーアプライアンスなど、その他の特定のデバイスが認識される場合もあります。フィールドが空白であるか、[不明なエクスポータ(Unknown Exporter)] と表示されている場合、FC はデバイスからエクスポートされるフロー レコードを正しく認識できない可能性があります。

13. [フロー タイプ(Flow Type)] 列には、エクスポータから生成される NetFlow のバージョンの詳細が示されます。

14. [エクスポート最長期間(Longest Duration Export)] 列には、最も長い期間アクティブであったフロー(最初のパケットから最後のパケットまで)の合計時間(秒)が表示されます。実際には、このフィールドは、エクスポータの NetFlow エクスポート設定で「アクティブ タイムアウト」値が正しく設定されているかどうかを示します。アクティブ タイムアウトの値は、すべてのエクスポータについて 60 秒に設定するため、[エクスポート最長期間(Longest Duration Export)] 列に表示される値は、約 60 秒になります。何百秒または何千秒もの値になる場合は、デバイスのアクティブ タイムアウトの値が正しく設定されていることを確認する必要があります。

注:最長フロー時間を検証することは非常に重要です。デバイスで過度の時間が設定されている場合は、できるだけ早く適切に設定する必要があります。

15. [SNMP ステータス(SNMP Status)] 列には、SMC が SNMP 経由でエクスポータを正常にポーリングして、追加のインターフェイス データを収集できるかどうかが示されます。SMC がエクスポータと通信できない場合は、エラーが表示されます。これらのエラーについては、お客様環境で調査を行い、エクスポータに対して誤った SNMP コミュニティ ストリングが使用されていないか、ファイアウォール ルールや ACL によって SMC からエクスポータ デバイスへのネットワーク トラフィックがブロックされていないかなどを判断します。

16. 次に、利用可能なデータに基づいて、お客様環境内のエクスポータのステータスを評価します。次の質問に対する状況を判断します。

    a. 不明なエクスポータとして表示されているエクスポータはあるか。エクスポータでの NetFlow テンプレート設定が誤っている可能性があります。

    b. [フロー タイプ(Flow Type)] フィールドが不明または空白になっているエクスポータはあるか。エクスポータでの NetFlow テンプレート設定が誤っている可能性があります。

    c. [前回のエクスポート(Last Export)] の値が現在のタイムスタンプではないエクスポータはあるか。以前有効であったエクスポータが、ネットワークによってブロックされているかオフラインになっていると考えられます。デバイス上でエクスポート タイマーが誤って設定されている可能性もあります。

    d. [エクスポート最長期間(Longest Duration Export)] の値が 60 秒を大幅に超えているエクスポータはあるか(フロー センサーを除く)。エクスポータのアクティブ タイマーの設定が正しくないと考えられます。1 分(60 秒)に設定してください。

    e. [SNMP ステータス(SNMP Status)] フィールドにエラーが表示されている SNMP エクスポータはあるか(SMC から SNMP でクエリできないため、FS が NA を示す)。SMC が(FW、ACL などにより)エクスポータに到達できないか、このデバイスに対する SNMP が SMC 上で正しく設定されていません。

17. プロジェクトの対象エクスポータのリストにあるエクスポータのうち、FC のエクスポータ リストに表示されていないエクスポータはあるか。

注:フロー センサー アプライアンスは [フロー コレクション ステータス(Flow Collection Status)] セクションにエクスポータとして表示されますが、正常に機能しているかどうかについて、他のエクスポータと同じ基準を適用する必要はありません。特に [エクスポート最長期間(Longest Duration Export)] と [SNMP ステータス(SNMP Status)] は無視して構いません。

注:エクスポータについては、導入の初期段階で潜在的な問題を特定することが重要です。お客様がネットワーク デバイスの設定を変更して問題を修正する場合には、時間がかかる可能性があるためです。

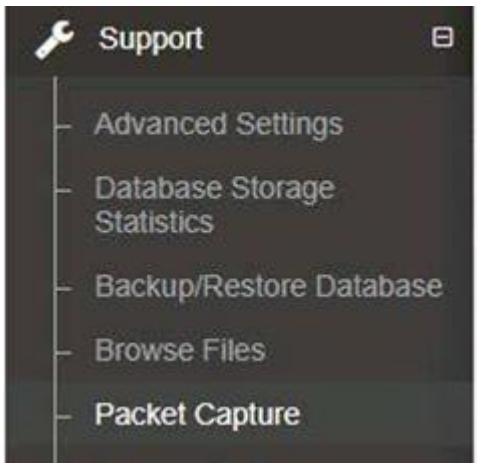
注:このシミュレートされた環境では、FE が修正のためにエクスポータ上で実施するアクション項目はありません。お客様環境では、FE はエクスポータのリストを CSV ファイルとしてエクスポートし、調査が必要なデバイスとその理由を示したリストをお客様用に作成すべきです。

18. 見つからないエクスポータが 2 つあります。エクスポータ 172.16.16.4 が FC に表示されていません。ここで、潜在的な問題についてトラブルシューティングを行います。

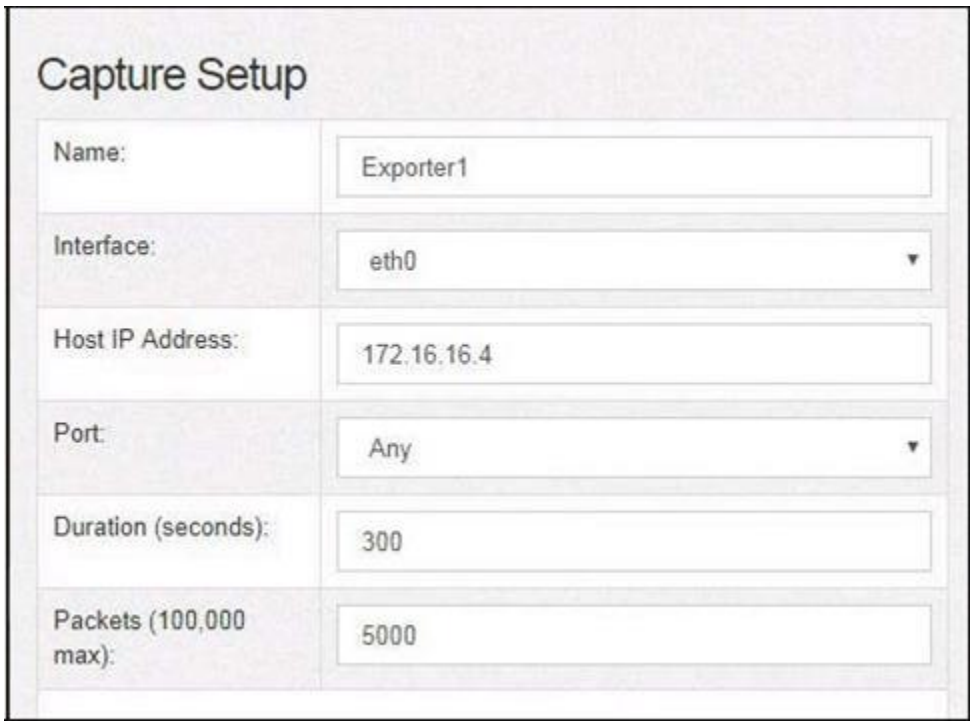
フロー コレクタへの NetFlow トラフィックの検証

エクスポータ 172.16.16.4 が、[フロー コレクタ ダッシュボード(Flow Collector Dashboard)] ドキュメントに、フロー データの送信元として表示されていません。この問題の根本原因を特定する必要があります。FC アプライアンスでパケット キャプチャを実行し、エクスポータからの NetFlow トラフィックが FC に到達しているのに正しく処理されていないのか、それともまったくトラフィックが到達しないのかを判断します。

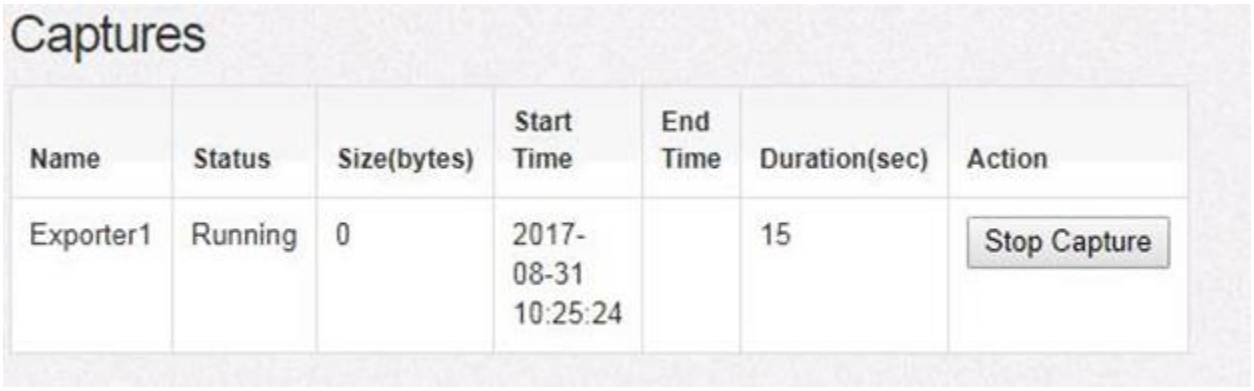
1. Chrome Web ブラウザの URL フィールドで「https://198.18.128.137」と入力するか、またはブックマークから [アプライアンス(Appliances)] > [FCNF] を選択して、FC 管理インターフェイスにアクセスします。
2. 認証のプロンプトが表示されたら、ユーザ名:admin、パスワード:C1sco12345 を入力します。
3. [サポート(Support)] メニューをクリックし、[パケット キャプチャ(Packet Capture)] メニュー オプションを選択します。



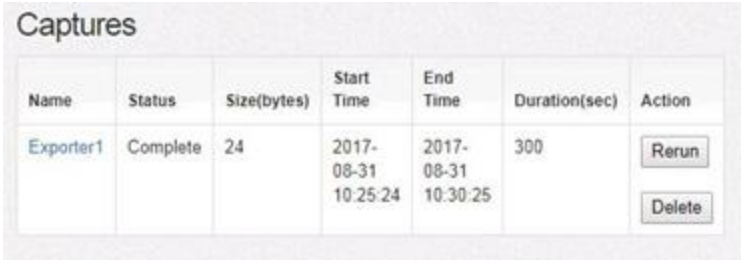
4. FC に表示されない最初のエクスポータの IP アドレスについて、パケット キャプチャを 5 分間実行します。次の値を使用してパケット キャプチャを設定し、パケット キャプチャ ページの [開始（Start）] ボタンをクリックして、パケット キャプチャを開始します。
    a. [名前（Name）]：Exporter1
    b. [インターフェイス（Interface）]：eth0
    c. [ホスト IP アドレス（Host IP Address）]：172.16.16.4
    d. [ポート（Port）]：すべて（Any）
    e. [時間（Duration）]：300
    f. [パケット数（Packets）]：5000



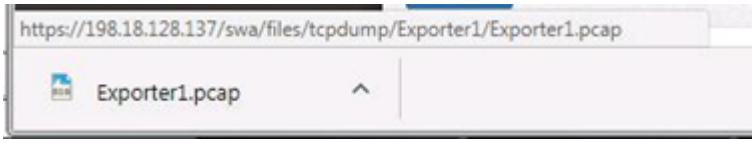
5. パケット キャプチャが、このページの [キャプチャ（Captures）] セクションに表示されます。5 分経過してキャプチャ タイマーが時間切れになってから次に進みます。



6. パケット キャプチャが完了すると名前フィールドがリンクになり、キャプチャ ファイルをダウンロードしてパケット アナライザでレビューを行うことができます。[Exporter1] リンクをクリックします。



7. Chrome ブラウザでファイルがダウンロードされ、ブラウザ ウィンドウの左下隅にダウンロード リンクが表示されます。pcap ファイルをクリックして、Wireshark アプリケーションで開きます。



8. Wireshark が開き、空白の画面が表示されます。指定したキャプチャ設定に基づいてキャプチャされたパケットはなかったようです。FC は 172.16.16.4 エクスポータからデータを受信していません。

注:[キャプチャ(Captures)] セクションにリストされているパケット キャプチャのサイズが 24 バイトであれば、キャプチャされたデータがないと推測できます。

9. どのような潜在的な問題または解決法があるでしょうか。

10. 次の設定で FC でパケット キャプチャを実行し、パケット キャプチャによってすべての NetFlow トラフィックを認識できることを確認します。

    a. [名前(Name)]:AllNetFlow

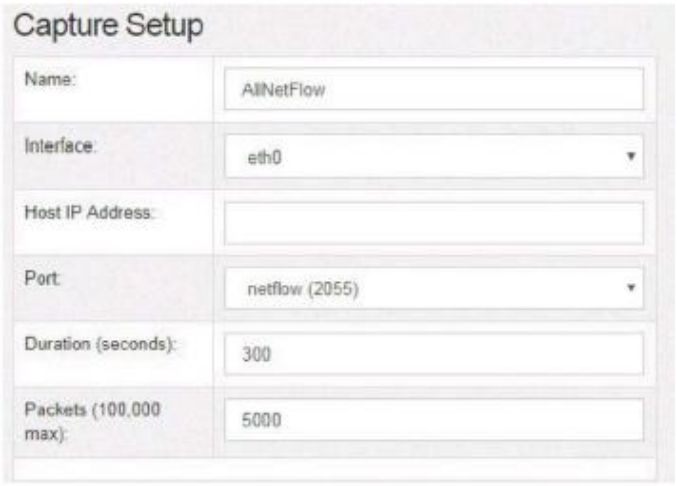
    b. [インターフェイス(Interface)]:eth0

    c. [ホスト IP アドレス(Host IP Address)]:(このフィールドは空白のままにする)

    d. [ポート(Port)]:netflow (2055)

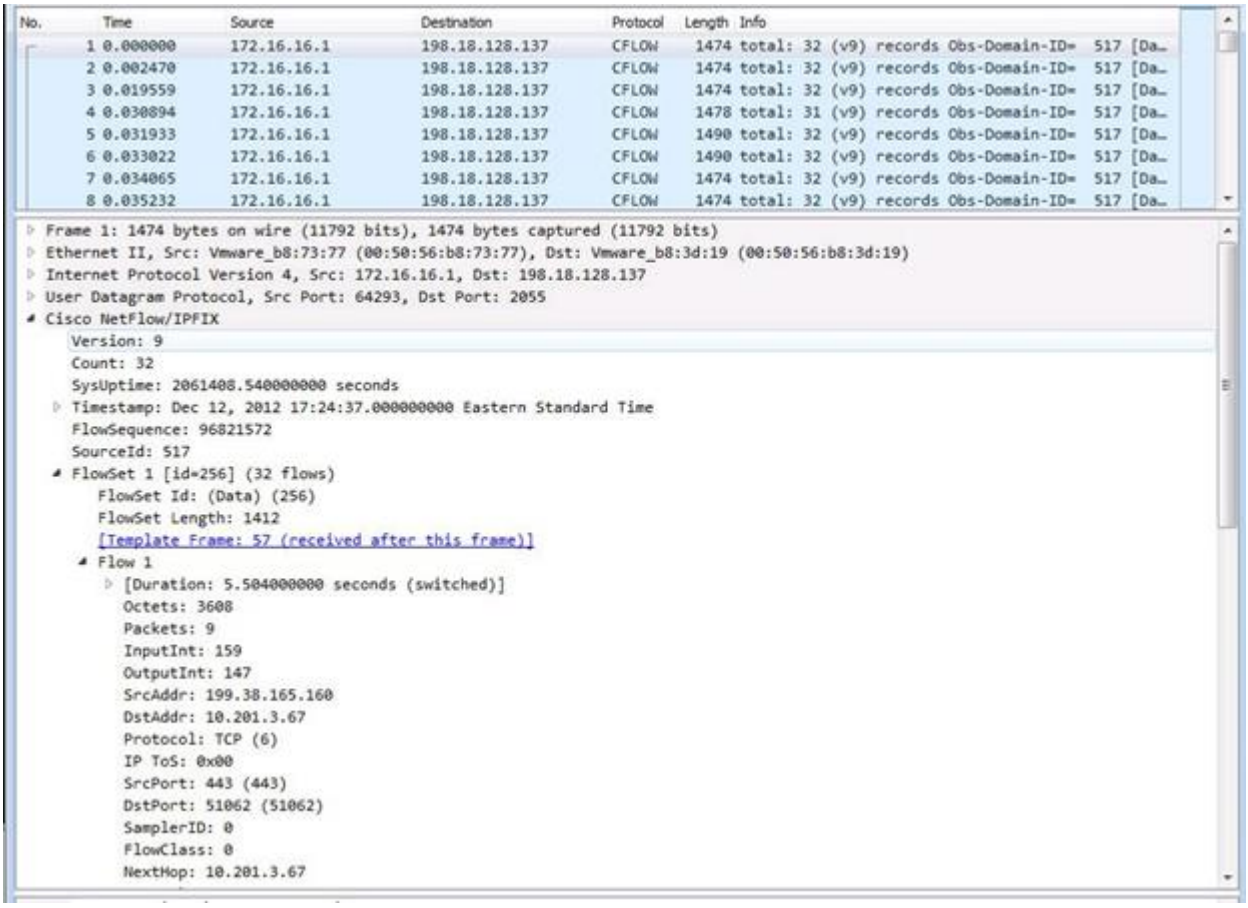
    e. [時間(秒)]:300

    f. [パケット数(Packets)]:5000



注:NetFlow のパケット キャプチャでは、Flexible NetFlow v9/IPFIX のフロー テンプレート パケットをキャプチャするために、パケット キャプチャの時間を長くする場合があります。NetFlow v9 または IPFIX では、NetFlow レコード内のフィールドをカスタマイズできます。Stealthwatch のようなソリューションで、フロー レコード内の各種のフィールドを理解するために、フィールドをマッピングするフロー テンプレートを X パケットごとに送信する必要があります。エクスポータの設定によっては、インデックス パケットの受信まで時間がかかる場合があります(30 分以上)。NetFlow レコードをキャプチャしていて、フロー レコード自体にドリル ダウンできない場合は、キャプチャの実行時間が足りなかった可能性があります。100,000 を超えるパケットをキャプチャする必要がある場合は、コマンド ラインで tcpdump を使用する必要があります。コンソール コマンドを実行する場合は、パケット キャプチャで使用されるハード ディスク容量に注意してください。コマンド ラインで tcpdump を使用する場合は、アプライアンスからレビュー用に転送されたパケット キャプチャ ファイルを必ず削除してください。パケット キャプチャを Web 管理インターフェイスで実行する場合は、パケット制限が課されるため、過剰に大きくなる可能性が低くなります。

11. パケット キャプチャをダウンロードして、Wireshark でキャプチャ ファイルを開きます。
12. パケット アナライザは NetFlow パケットを認識するため、フロー レコード自体にドリル ダウンすることが可能になります。
    a. ページの上部にある CFLOW というパケットを選択します。
    b. ページの下部で Cisco NetFlow/IPFIX を展開後、FlowSet 1 を展開し、調査する各フローを展開します。
    c. このキャプチャを利用して、必要なすべてのフィールドが Stealthwatch システムに送信されたか、またはエクスポータの設定を修正する必要があるかなどを確認できます。



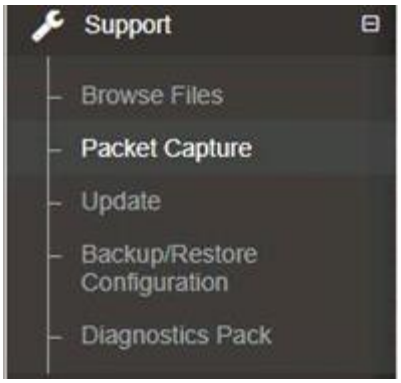
13. 問題のエクスポータはパケット キャプチャで表示されませんが、他のデバイスからは NetFlow データを受信していることを確認しました。次にトラブルシューティング プロセスに進み、見つからないエクスポータにどのような問題があるかを判断します。

UDP Director に対する NetFlow トラフィックの確認

NetFlow トラフィックが FC アプライアンスの IP アドレスに到達していないことを確認しました。トラブルシューティングの次の手順では、トラフィックが UDP Director に到達していることを確認します。次のような潜在的な問題が考えられます。

- 問題：NetFlow トラフィックが UDP Director にまったく到達していない。
  - 考えられる原因：エクスポータの設定が正しくない。
    - 解決策：問題のエクスポータからの NetFlow トラフィックがないことを示すパケット キャプチャを作成し、お客様のネットワーク エンジニア スタッフに NetFlow のエクスポート設定の確認を依頼します。
  - 考えられる原因：ACL またはファイアウォール ルールが NetFlow トラフィックをブロックしている。
    - 解決策：問題のエクスポータからの NetFlow トラフィックがないことを示すパケット キャプチャを作成し、お客様のネットワーク エンジニア スタッフに対し、ネットワーク パスをトレースしてトラフィックがブロックされている場所を判断するように依頼します。
- 問題：NetFlow トラフィックが UDP Director に到達しているが、FC には到達していない。
  - 考えられる原因：エクスポータが正しく設定されていないか、UDPD 設定の転送ルールに適合しないポートに NetFlow を送信しているため、UDPD がトラフィックを FC に転送していない。
    - 解決策：問題のエクスポータからのすべてのトラフィックについて、パケット キャプチャを実行します。定義されているルールに適合しない代替ポートで NetFlow が送信されていないかどうかを判定します（デフォルトの NetFlow ポートは 2055）。これが原因であった場合は、別のポートから FC の 2055 にトラフィックを転送する追加ルールを UDPD 設定に作成するか、お客様のネットワーク チームにエクスポータの設定を行うように依頼します。
- 問題：NetFlow が FC に到達しているが、製品のレポートには表示されない。
  - 考えられる原因：エクスポータの NetFlow 設定に誤りがあるため、ネットワーク トラフィックが FC に到達しても、FC が NetFlow レコードを認識できない。これはお客様が、誤ったテンプレート設定で NetFlow v9 または IPFIX を使用しているためであると考えられます。
    - 解決策：お客様と協力して、エクスポータ デバイスの NetFlow 設定を調査します。

1. URL フィールドで「https://198.18.128.139」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [UDPD] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。
2. 認証のプロンプトが表示されたら、ユーザ名：admin、パスワード：C1sco12345 を入力します。
3. [サポート（Support）] メニューをクリックし、[パケット キャプチャ（Packet Capture）] メニュー オプションを選択します。



4. FC に表示されない最初のエクスポータの IP アドレスについて、パケット キャプチャを 5 分間実行します。次の値を使用してパケット キャプチャを設定し、パケット キャプチャ ページの [開始（Start）] ボタンをクリックして、パケット キャプチャを開始します。
   - [名前（Name）]：Exporter1
   - [インターフェイス（Interface）]：eth0
   - [ホスト IP アドレス（Host IP Address）]：172.16.16.4
   - [ポート（Port）]：すべて（Any）
   - [時間（Duration）]：300
   - [パケット数（Packets）]：5000

5. パケット キャプチャが、このページの [キャプチャ（Captures）] セクションに表示されます。5 分経過してキャプチャ タイマーが時間切れになってから次に進みます。

6. パケット キャプチャが完了すると名前フィールドがリンクになり、キャプチャ ファイルをダウンロードしてパケット アナライザでレビューを行うことができます。

注：[キャプチャ（Captures）] セクションにリストされているパケット キャプチャのサイズが 24 バイトであれば、キャプチャされたデータがないと推測できます。

7. エクスポータから送信された NetFlow データを確認できますか。
8. このエクスポータから UDPD に到達した NetFlow はないと考えられます。確認のためリンクをクリックして pcap ファイルを開くことができます。
9. 172.16.16.4 のエクスポータが、NetFlow テレメトリを Flow Replicator にエクスポートするように正しく設定されていないと考えられます。この時点で、お客様と話して、できるだけ早くエクスポータの設定を変更してもらうように依頼する必要があります。変更が行われると、UDPD に設定したルールにより、トラフィックが転送されます。

注：不明なエクスポータからパケットが送信されているが、非標準ポート（ポート 2055 ではなく 2505 など）が使用されている場合、パケット キャプチャ機能と Wireshark を使用して UDP パケットが実際に NetFlow レコードであることを確認できます。

1. アプライアンスから pcap ファイルをダウンロードします。

2. Wireshark で pcap ファイルを開きます。

3. [分析（Analyze）] メニューをクリックし、[名前を付けてデコード（Decode As）] メニュー項目を選択します。

4. [名前を付けてデコード（Decode As）] 画面のプラス記号をクリックします。次の値を使用して設定し、[OK] ボタンをクリックします。

    [フィールド（Field）]：UDP ポート（UDP Port）

    [値（Value）]：2505

    [タイプ（Type）]：整数、10 進数（なし）（Integer, base 10 (none)）

    [現在（Current）]：CFLOW

5. パケット アナライザは、パケットを NetFlow（CFLOW）として解釈しようとします。パケットが NetFlow として適切に変換されている場合は、エクスポータに設定ミスがあります。すぐに解決する方法としては、お客様と短時間で作業する必要がある場合などは、ネットワーク チームに依頼してデバイスの設定を変更するよりも、導入の早い段階で UDPD ルールを追加して、可能な限り多くの NetFlow トラフィックを処理できるようにするほうが効率的です。転送ルールを作成してデータを取り込み、適切なポートにマッピングする一方で、非標準デバイスの設定を可能な限り早く変更するように、お客様に依頼します。変更されると、UDPD の標準ルールによってトラフィックが転送されます。

注：環境によっては、UDP Director をまったく使用せず、すべての NetFlow データを直接 FC に送信する場合があります。FC では、一度に 1 つのポートでのみ NetFlow を処理できます。その場合、他に一時的な回避策はないため、ポート 2055 で送信するようにデバイスを設定変更する必要があります。

10. これで、対象のすべてのフロー データが UDP Director とフロー コレクタによって処理されたことを確認し、見つからないエクスポータをお客様に報告しました。

シナリオのまとめ

このシナリオでは、Stealthwatch で受信するフロー データが有効であることの確認、NetFlow レコードに関する潜在的な問題の特定、対象のすべてのエクスポータがフロー データを送信していることの確認、お客様に報告を行っていないデバイスの特定を実施しました。これで Stealthwatch がフロー データを処理するようになったので、製品のその他の設定に進みます。

注：フロー データの確認は、可能な限り導入の早い段階で実施することが重要です。NetFlow エクスポータの問題は、一般的にお客様が迅速に解決することができないため、早い段階で問題を特定することが重要になります。

シナリオ 6.　ホスト グループの定義

プロジェクトの開始時に、場所、サーバのタイプ、アプリケーション、パブリック IP 空間、認可済みのネットワーク スキャナなどの情報が含まれた IP データを要求したのに応えて、お客様から IP アドレスと範囲のリストが提供されています。

この IP データを SMC に入力し、適切なホスト グループを設定します。IP データについては、必要に応じて次の表を使用します。ラボの手順を進めます。

表 4.　IP アドレス範囲

説明	IP アドレス範囲
DNS サーバ	10.10.30.15
DNS サーバ	10.10.30.16
脆弱性スキャナ	10.203.0.207
メール サーバ	10.10.30.23
タイム/NTP サーバ	10.10.30.10
パブリック IP アドレス空間	209.182.184.0/24
Atlanta ホスト	10.201.0.0/16
PCI デバイス	10.201.3.0/24

手順

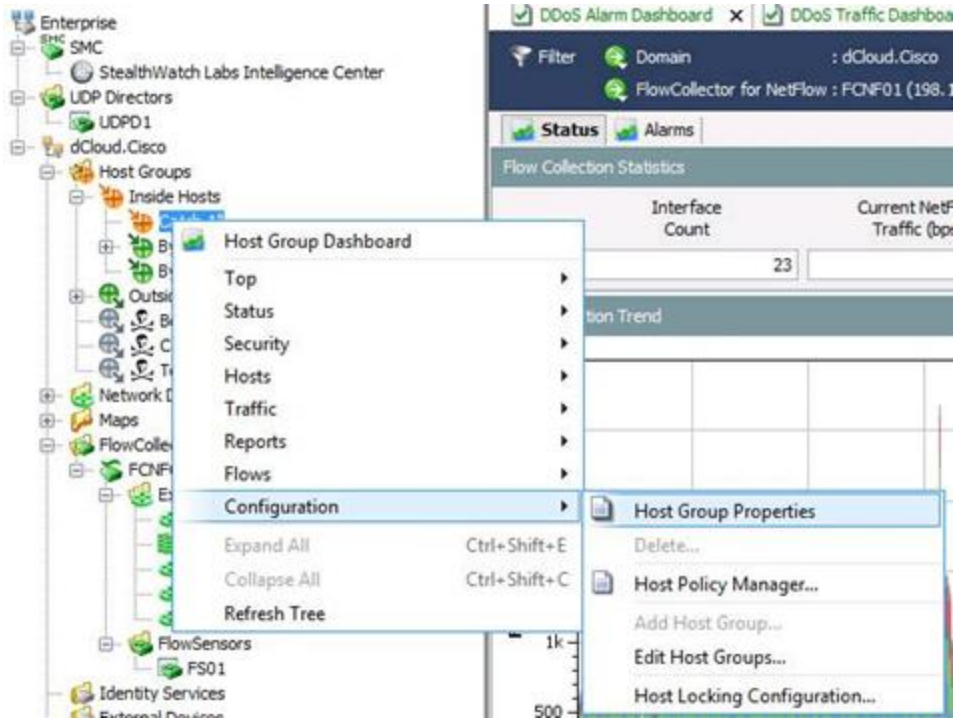
パブリック IP 空間の設定

注:ホスト グループには、IP アドレス データだけを含めることができます(MAC アドレスまたは DNS 名は許可されていません)。IP アドレスは、いくつかの異なる形式で入力できます。10.1.2.3 など、1 つの IP アドレスを入力できます。192.168.1.1-57、10.1-167.1.1、172.22.0-255.0-255 などのように、1 つのオクテット内で、ハイフンで連結して範囲を指定できます。完全な IP アドレス – 完全な IP アドレス(192.168.1.1-192.168.1.254)という形式では、範囲を指定しないでください。範囲は 1 つのオクテット内である必要があります(192.168.1.1-254)。10.245.0.0/16 のような CIDR 表記を使用することもでき、10.100-201.6.0/24 や 172.22-23.0.0/16 などのように範囲と組み合わせることも可能です。

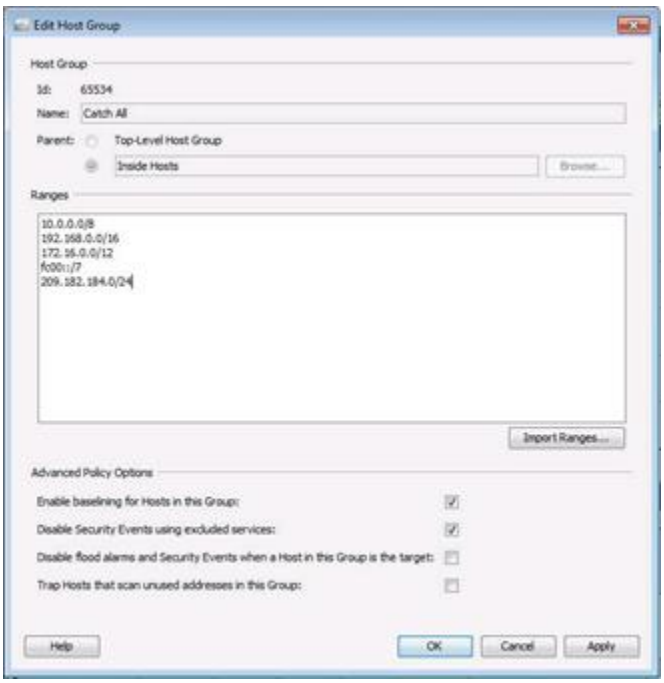
注:Stealthwatch の [すべてを捕捉(Catch All)] グループは、製品内の特殊機能を実行します。[すべてを捕捉(Catch All)] グループの内容によって、企業が使用、所有、または制御する IP アドレスが確立されます。これには、デフォルトですべてのプライベート IPv4 および IPv6 アドレス空間が含まれます。お客様が現在特定のプライベート アドレス範囲を使用していないからといって、それを [すべてを捕捉(Catch All)] から除外する必要はありません。特定の範囲を除外するのは、その範囲が外部エンティティによって使用されていて、お客様のネットワークの一部であるとは見なされない場合に限るべきです。[すべてを捕捉(Catch All)] グループには、お客様のすべてのパブリック IP アドレス空間を追加します。Stealthwatch には、内部ホスト(お客様のネットワーク)から外部ホスト(お客様のネットワーク以外のすべて)に送信されるデータに関する、複数のアラームがあります。お客様のパブリック IP 空間が正しく分類されていないと、通常のネットワーク トラフィックがそのパブリック IP 空間と通信することから、アラームが増加する可能性があります。また将来的な調査やレポートのためにも、分類は正しく行われなければなりません。

1.　[SMC Java] インターフェイスを開きます。

2. 左ペインの [エンタープライズ（Enterprise）] ツリーで [dCloud.Cisco] ドメインを探して展開します。[ホスト グループ（Host Groups）] コンテナを展開後、[内部ホスト（Inside Hosts）] を展開し、最後に [すべてを捕捉（Catch All）] グループを右クリックします。右クリック メニューが表示されたら、[設定（Configuration）] メニューを選択し、[ホスト グループのプロパティ（Host Group Properties）] メニュー項目を選択します。



3. お客様によれば、パブリック IP アドレス空間は 209.182.184.0/24 と定義されています。これを [すべてを捕捉（Catch All）] グループに入力します。[ホスト グループの編集（Edit Host Group）] ウィンドウの [範囲（Ranges）] セクションで、Enter キーを押して新しい空白行を作成します。新しい行に「209.182.184.0/24」と入力し、[OK] ボタンをクリックして変更を確定します。

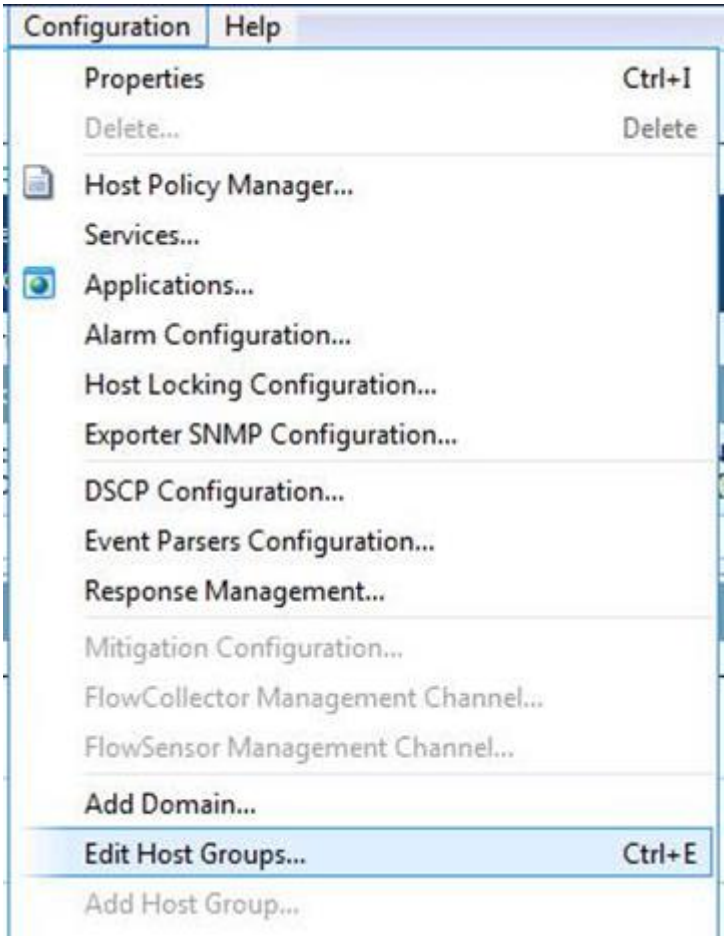


4. お客様のパブリック アドレス空間を分類しました。ラボの次の手順に進みます。

追加ホスト グループの設定

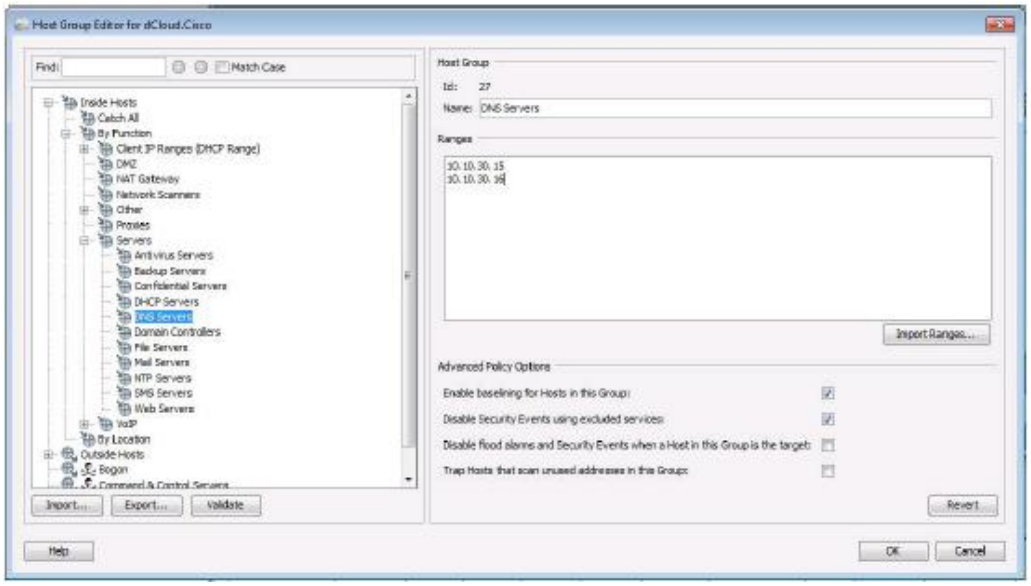
注:ホスト グループの作成、編集、削除には複数の方法があります。ホスト グループを 1 つだけ追加または編集する場合は、[ホスト グループ(Host Group)] ツリー構造を右クリックし、[設定(Configure)] メニューを使用して 1 つのアクションを実行するのが推奨されるオプションです。ただし編集するグループが複数ある場合は、ホスト グループ エディタを使用することで、複数のホスト グループを編集することができ、時間を節約できます。複数の管理者がホスト グループ エディタを同時に開いている場合は、いずれかの管理者が最後に保存した変更が、先に別の管理者が行った変更を上書きすることになります。初期導入では、通常これは問題になりません。ホスト グループを変更できるアクセス権を持つ管理者が多数存在するお客様環境では、注意が必要になります。

1. [設定(Configuration)] メニューをクリックして [ホスト グループ エディタ(Host Group Editor)] を開き、[ホスト グループの編集(Edit Host Groups)] メニュー項目を選択します。



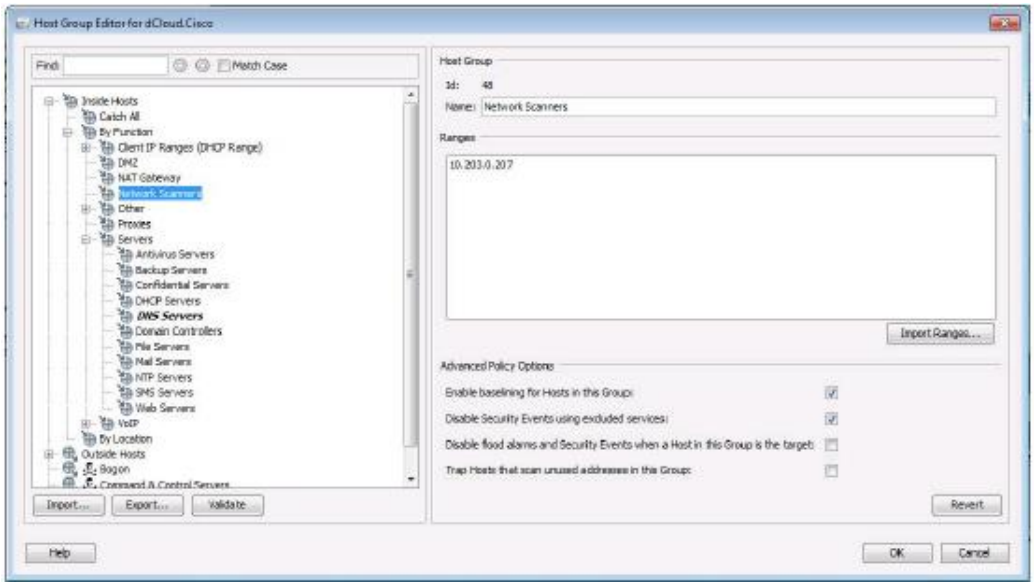
2. ホスト グループ エディタの左上にある [検索(Find)] フィールドに、「DNS」と入力します。ホスト グループ エディタは、最初に検索用語を入力すると自動的に展開されます。[DNS サーバ(DNS Servers)] ホスト グループが選択されていますが、ウィンドウの右側には IP アドレスまたは範囲は入力されていません。

3. お客様から提供された DNS サーバの IP アドレス（10.10.30.15 および 10.10.30.16）を、ウィンドウの [範囲（Ranges）] ペインにそれぞれ別の行で入力し、[OK] をクリックします。



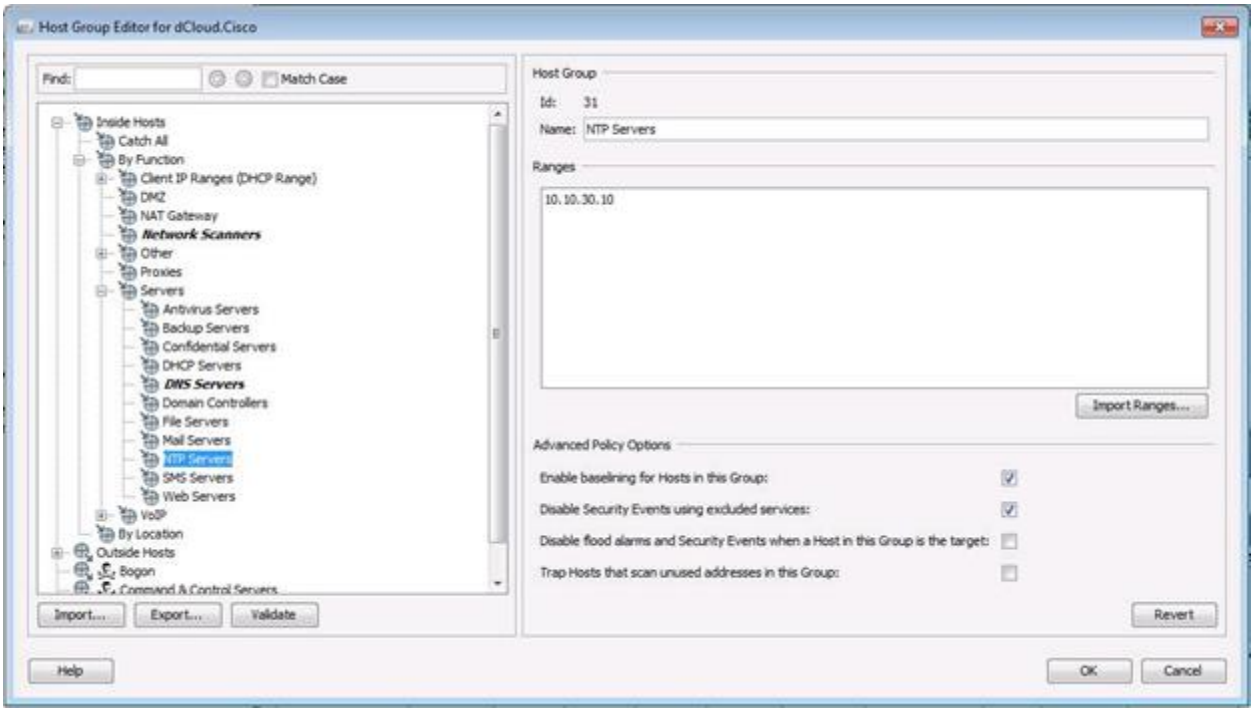
注：ホスト グループ エディタでは、SMC に変更をコミットする前に、ホスト グループ構造に対して複数の変更を行うことができます。複数のホスト グループの編集、作成、削除、移動、名前変更が可能です。1 回のセッション中に行われた変更は、ホスト グループ エディタ ウィンドウで、すべて太字の斜体で表示されます。変更がすべて完了したら、[OK] ボタンをクリックしてすべての変更を保存します。

4. [ホスト グループ エディタ（Host Group Editor）] ウィンドウの [ネットワーク スキャナ（Network Scanners）] ホスト グループを特定し、ウィンドウの右側の [範囲（Ranges）] フィールドに IP アドレス「10.203.0.207」を入力します。

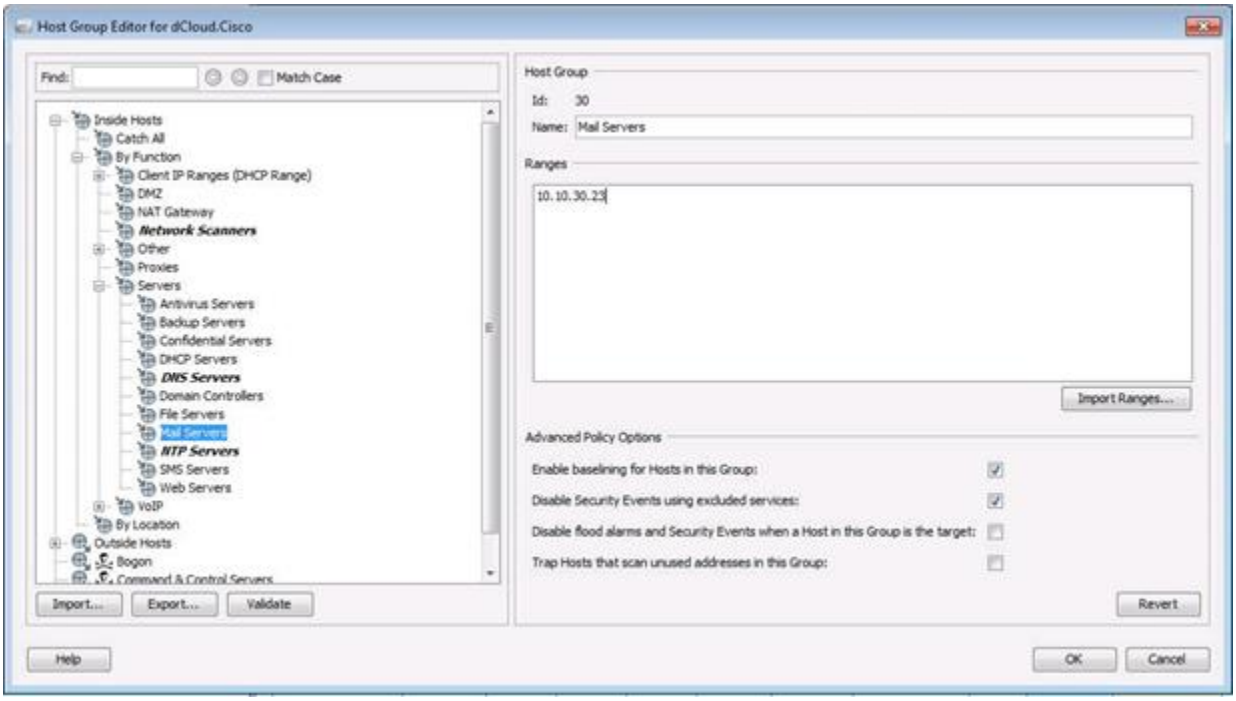


注：[ネットワーク スキャナ（Network Scanners）] ホスト グループは複数のポリシーから参照されています。通常はネットワーク スキャン アクティビティを実行するホストによってトリガーされるさまざまなタイプのアラームを自動的に停止するために使用されます。お客様の認可済み脆弱性スキャナの IP アドレスを [ネットワーク スキャナ（Network Scanners）] ホスト グループに設定することで、通常はアクティブになるはずの、有効な動作に対するアラームを停止することができます。それによって該当するホスト グループにより多くの IP 空間が割り当てられるため、お客様のネットワーク上のホストを分類するために役立ちます。

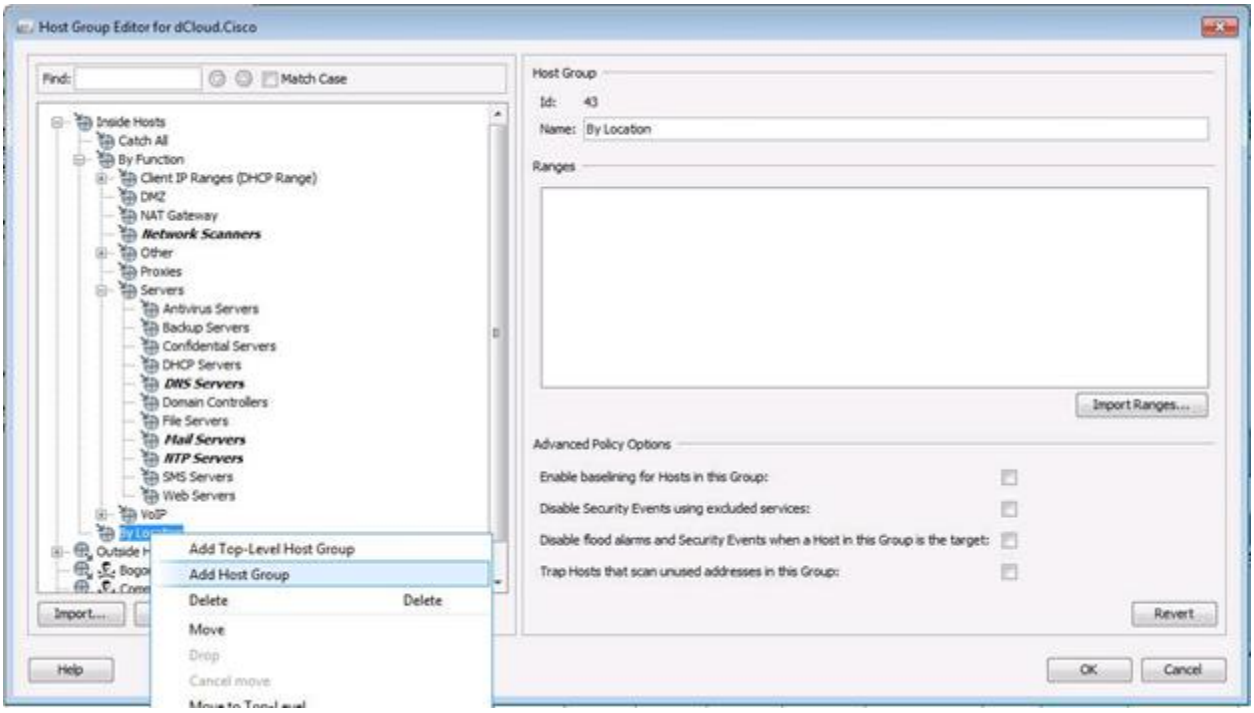
5. [ホスト グループ エディタ(Host Group Editor)] ウィンドウの [NTP サーバ(NTP Servers)] ホスト グループを特定し、[範囲(Ranges)] フィールドに IP アドレス「10.10.30.10」を入力します。



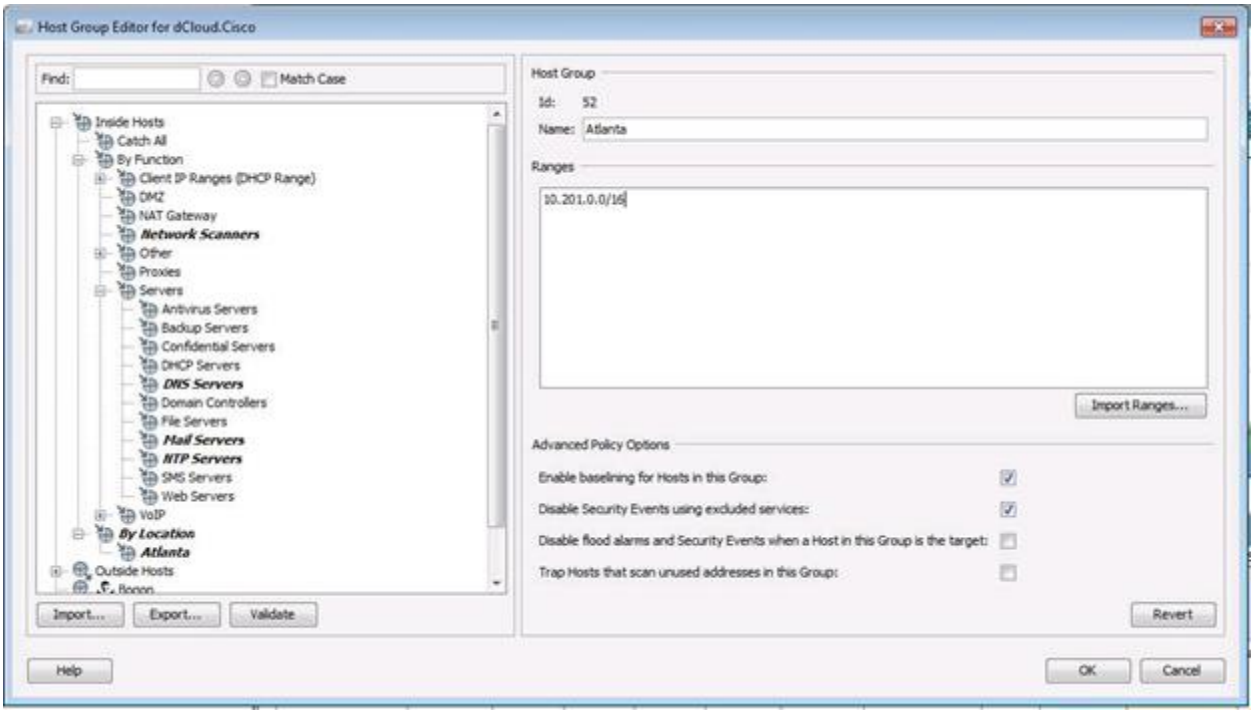
6. [ホスト グループ エディタ(Host Group Editor)] ウィンドウの [メール サーバ(Mail Servers)] ホスト グループを特定し、[範囲(Ranges)] フィールドに IP アドレス「10.10.30.23」を入力します。



7. 次に、[内部ホスト（Inside Hosts）] ツリー内の [ロケーション別（By Location）] ホスト グループの下に、ロケーション ベースのホスト グループを追加します。[ロケーション別（By Location）] ホスト グループを特定して右クリックし、[ホスト グループの追加（Add Host Group）] メニュー オプションを選択します。



8. 新しいホスト グループの名前として「Atlanta」と入力し、[範囲（Ranges）] フィールドに「10.201.0.0/16」と入力します。



9. [OK] ボタンをクリックして SMC に変更をコミットし、[変更内容を適用（Apply Changes）] プロンプトが表示されたら [続行（Continue）] ボタンをクリックします。

10. 示された手順に従って、[機能別（By Function）] ホスト グループの下に PCI デバイスのホスト グループを作成します。お客様が指定した IP 範囲を入力します。
11. お客様の指定に従ってホスト グループを設定しました。ラボの次の手順に進みます。

シナリオのまとめ

このシナリオでは、お客様から提供された IP アドレス データに基づいてホスト グループを作成しました。[ホスト グループ エディタ（Host Group Editor）] インターフェイスを使用して、お客様のパブリック IP 空間を [すべてを捕捉（Catch All）] グループに追加し、お客様の管理対象であるとマークしました。また、適切なホスト グループを作成しました。

シナリオ 7.　設定のバックアップ

これまでに、お客様の Stealthwatch ソリューションの初期導入と設定が無事に完了しています。今回のお客様との業務を終了する前に、各アプライアンスの設定をバックアップして、正常だとわかっている状態をキャプチャしておくとよいでしょう。ここでは、アプライアンスの設定のバックアップを実行し、そのファイルを、作業のために提供されたお客様の環境内の管理ワークステーションに保存します。そうしておけば、お客様がそのファイルを自身のファイル サーバにコピーして保管することができます。

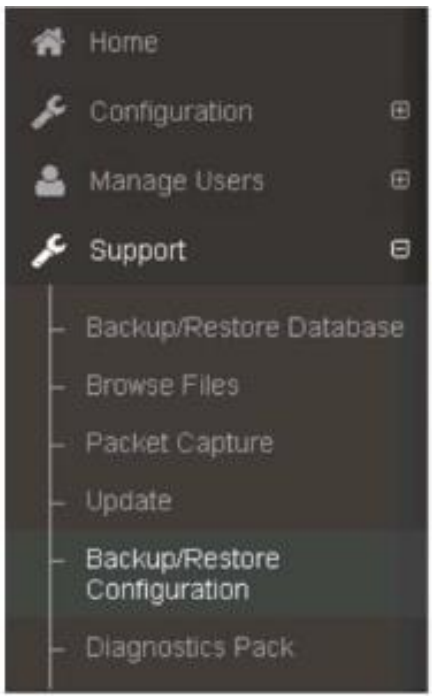
注:各アプライアンスは、自身の設定のバックアップ コピーを毎日自動的にローカル ディスクに保存し、30 日間保持します。管理者がホストグループ ツリーを削除するなどの設定エラーをした場合、またはその他の**誤設定**が発生した場合には、これが役に立つ可能性があります。こうした問題が発生後 30 日以内に見つかった場合であれば、アプライアンスに保存されているバックアップを使用して、動作するための設定にマシンを戻すことができます。ただし、アプライアンスが故障した場合または工場出荷時の初期状態にリセットされた場合は、ローカルで保存された設定のバックアップは失われます。設定のバックアップは外部のマシンに保存しておくことが重要です。

注:[設定のバックアップ/復元(Backup/Restore Configuration)] 画面では、構造化された可視性評価を実施する場合、PoV 設定テンプレートを適用します。

1. デスクトップにあるショートカットをダブルクリックして Chrome Web ブラウザを開きます。
2. URL フィールドで「https://198.18.128.136/smc/index.html」と入力するか、またはブックマークから [アプライアンス(Appliances)] > [SMC(管理)(SMC (Admin))] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。

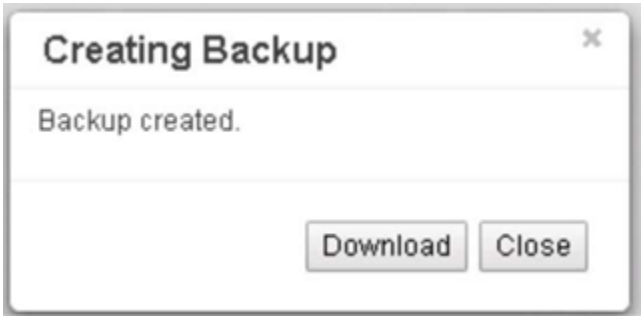
注:URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

3. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名:admin
    b. パスワード:C1sco12345
4. [サポート(Support)] メニューをクリックして、[設定のバックアップ/復元(Backup/Restore Configuration)] メニュー項目を選択します([データベース(Database)] オプションではありません)。



5. 毎日の設定バックアップによりこれまでに保存されアプライアンス自体に存在しているバックアップの一覧が表示されます。[バックアップの作成（Create Backup）] ボタンをクリックして、随時のバックアップを作成します。

6. バックアップが作成されたら、[ダウンロード（Download）] ボタンをクリックします。



7. 設定のバックアップが Web ブラウザによってダウンロードされ、Downloads フォルダに保存されます。
8. すべてのアプライアンスについて上記の手順を繰り返します。
    a. Flow Collector
    b. Flow Sensor
    c. UDP Director
9. お客様のアプライアンスに関する設定のバックアップが無事に完了しました。

注：設定のバックアップの実行は、アプライアンスのアップグレード前に行うべきプロセスの一部でもあります。

付録 A.　ユーザ アカウントの管理

手順

アプライアンス管理者アカウントのパスワード変更

お客様によれば、どの Stealthwatch アプライアンスでも、内部の IT セキュリティ ポリシーに準拠する上で、デフォルトのパスワードを使用するユーザ アカウントは必要ではありません。ここでアプライアンスの設定を変更して、sysadmin、root、および管理者ユーザ アカウントのデフォルトのパスワードを変更します。

一般に、アプライアンスのパスワードを変更することはセキュリティ上のベストプラクティスです。メインとなるラボで明示的に示されてはいませんが、Stealthwatch 導入の一環として実施する方法を知っておく必要があります。

注：すべての Stealthwatch アプライアンスには、3 つのユーザ アカウントが組み込まれています。

管理者ユーザ アカウントは、アプライアンスの Web 管理ページにアクセスするために使用します。SMC の場合は、製品の Web インターフェイスおよび Java インターフェイスにアクセスする場合にも使用します。管理者アカウントのデフォルトのパスワードは lan411cope です。AST ウィザード（アプライアンス セットアップ ツール）では、デフォルトのパスワードから新しいパスワードへの変更が強制されます。アプライアンスの Web 管理ページでは、管理者アカウントのパスワードを手動で変更する方法が示されます。

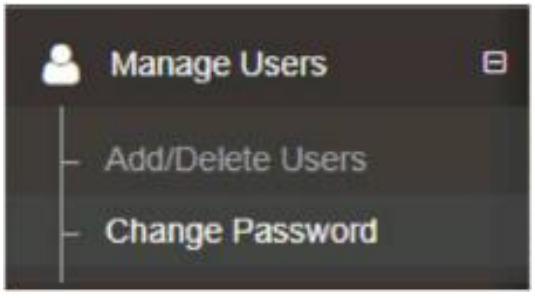
sysadmin アカウントは、[システム設定（System Configuration）] メニューにアクセスするために使用する、コンソール/SSH 専用のアカウントです。[システム設定（System Configuration）] メニューでは、アプライアンスの IP 設定や、その他の詳細設定を変更します。sysadmin ユーザはシェルに対するフル アクセス権を持っていません。sysadmin ユーザのデフォルトのパスワードは lan1cope です。

root ユーザ アカウントは、アプライアンスのオペレーティング システムに対するフル アクセス権を持つ、コンソール/SSH 専用のユーザ アカウントです。ユーザが不適切なコマンドを実行すると、アプライアンスが機能しなくなる可能性があるため、このアカウントは注意して使用する必要があります。

1. デスクトップにあるショートカットをダブルクリックして Chrome Web ブラウザを開きます。
2. URL フィールドで「https://198.18.128.136/smc/index.html」と入力するか、またはブックマークから [アプライアンス（Appliances）] > [SMC（管理）（SMC (Admin)）] を選択して、アプライアンスの Web 管理インターフェイスにアクセスします。

注：URL への接続に問題がある場合は、「動作していないアプライアンスのトラブルシューティング」を参照してください。

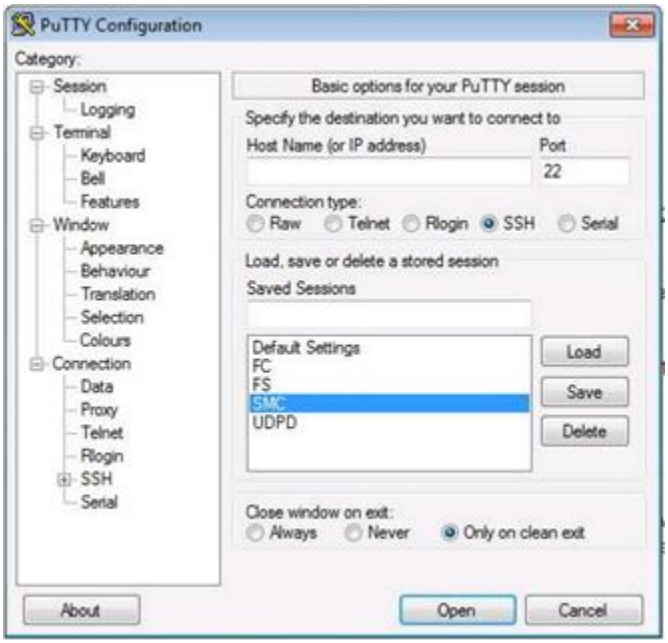
3. ユーザ名 admin と、パスワード C1sco12345 を使用して、アプライアンスにログインします。
    a. ユーザ名：admin
    b. パスワード：C1sco12345
4. [ユーザの管理（Manage Users）] メニューをクリックし、[パスワードの変更（Change Password）] メニュー項目を選択します。



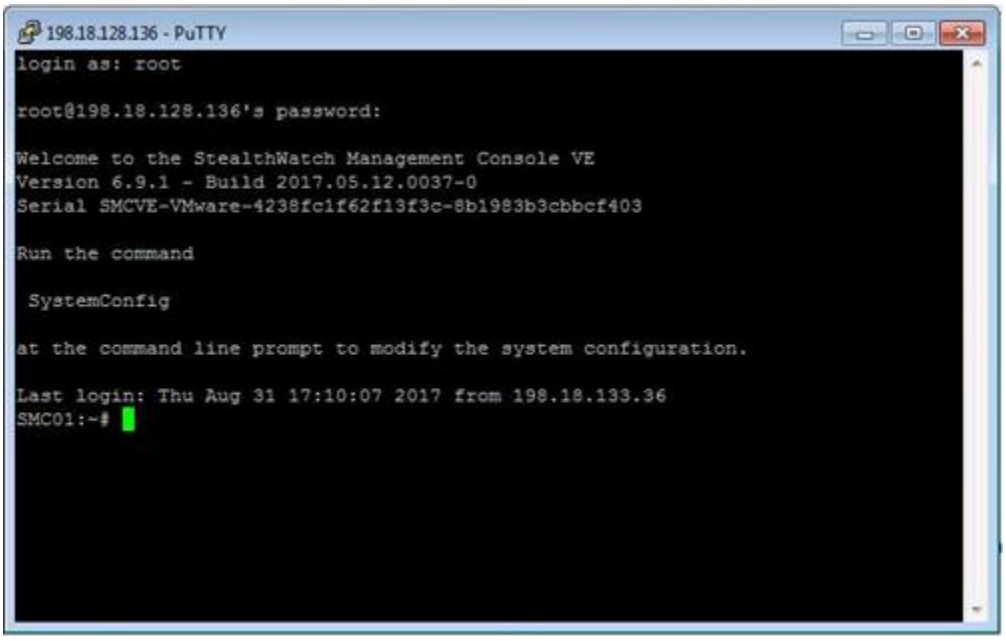
5. [パスワードの変更（Change Password）] 画面が表示されます。アプライアンス セットアップ ツールによって管理者アカウント パスワードが C1sco12345 に変更されていない場合は、この画面で変更することができます。現時点ではパスワードを変更しないでください。

注：導入時には、インストール プロセスを進めるために、管理者ユーザ用の一時的なパスワードを選択する必要があります。すべてのアプライアンスが稼動したら、管理、root、および sysadmin ユーザ アカウントに適用するパスワードをお客様から取得して、アプライアンスで変更するのがベスト プラクティスになります。

6. 次に SMC アプライアンスのコンソール/SSH インターフェイスに接続して、root および sysadmin ユーザのパスワードを変更します。
7. dCloud 管理ワークステーションで、デスクトップの [PuTTY] ショートカットを開きます。
8. PuTTY 画面の [保存済みセッション（Saved Sessions）] セクションで、[SMC] エントリを選択して [開く（Open）] ボタンをクリックします。



9. ログインするよう求められたら、以下に示す root ユーザ アカウント情報をアプライアンスに入力します。
    a. ユーザ名：root
    b. パスワード：lan1cope



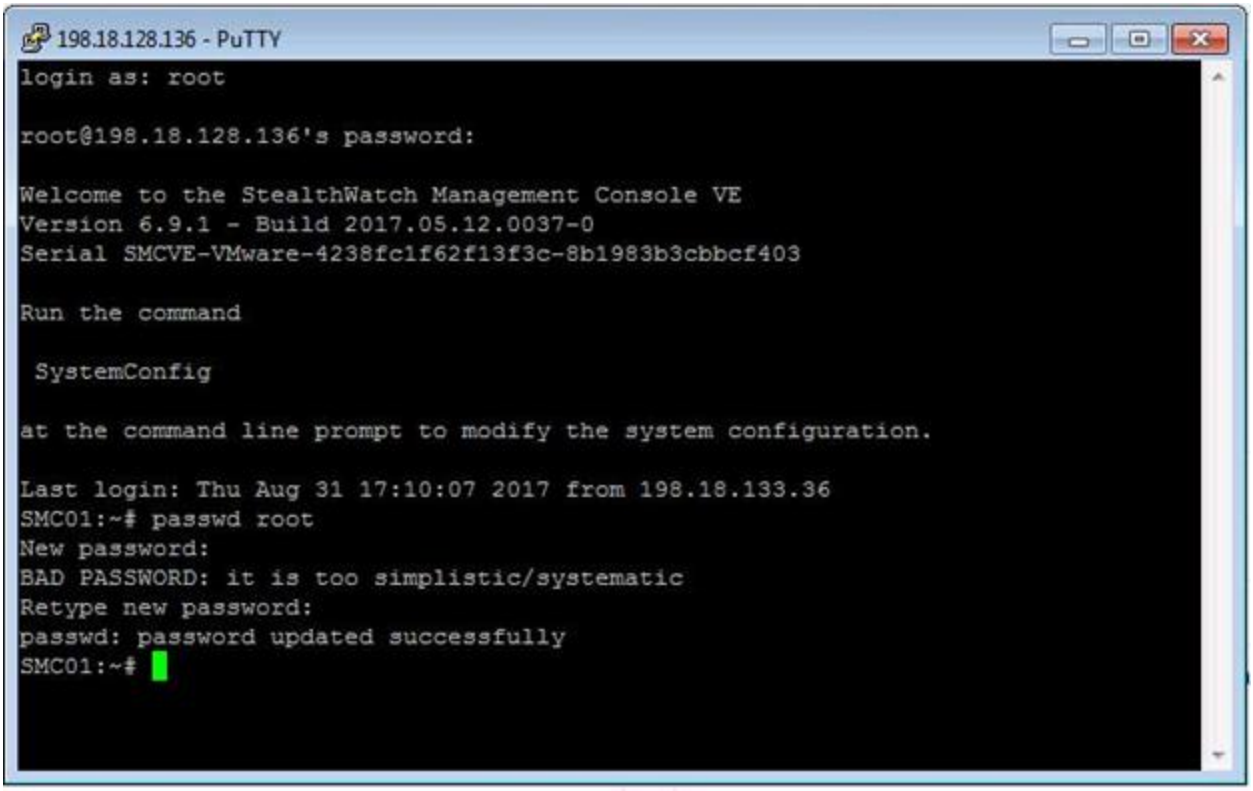
10. sysadmin アカウント パスワードを変更するには、次のコマンドを入力して Enter を押します。
    a. passwd sysadmin
11. 新しいパスワードを入力するプロンプトが表示されたら、次を入力します。
    a. C1sco12345
    b. 「パスワードが正しくありません：単純すぎるか規則正しすぎます（BAD PASSWORD: it is too simplistic/systematic）」という警告が表示されます。これは、新しいパスワードの複雑さが不足していることを示します。このラボでは、C1sco12345 パスワードをそのまま使用できます。コマンドは正常に処理されます。
    c. 完了すると、「passwd：パスワードが正常に更新されました）（passwd: password updated successfully）」というメッセージが表示されます。
12. root アカウント パスワードを変更するには、次のコマンドを入力して Enter を押します。
    a. passwd root

13. 新しいパスワードを入力するプロンプトが表示されたら、次を入力します。

    a. C1sco12345

    b. 「パスワードが正しくありません：単純すぎるか規則正しすぎます（BAD PASSWORD: it is too simplistic/systematic）」という警告が表示されます。これは、新しいパスワードの複雑さが不足していることを示します。このラボでは、C1sco12345 パスワードをそのまま使用できます。コマンドは正常に処理されます。

    c. 完了すると、「passwd：パスワードが正常に更新されました）（passwd: password updated successfully）」というメッセージが表示されます。



14. 「exit」と入力して SSH セッションを終了します。

15. SMC で上記の手順を繰り返して、FC、FS、UDPD アプライアンスの sysadmin および root ユーザ アカウントのパスワードを変更します。

    a. PuTTY アプリケーションによって、FC、FS、UDPD の正しい IP アドレスで各アプライアンスのエントリが保存されました。

16. これで、お客様のセキュリティ ポリシーに準拠して、組み込みのすべてのアカウントにデフォルト以外のパスワードが設定されました。

Stealthwatch のユーザ管理およびロール管理の概要

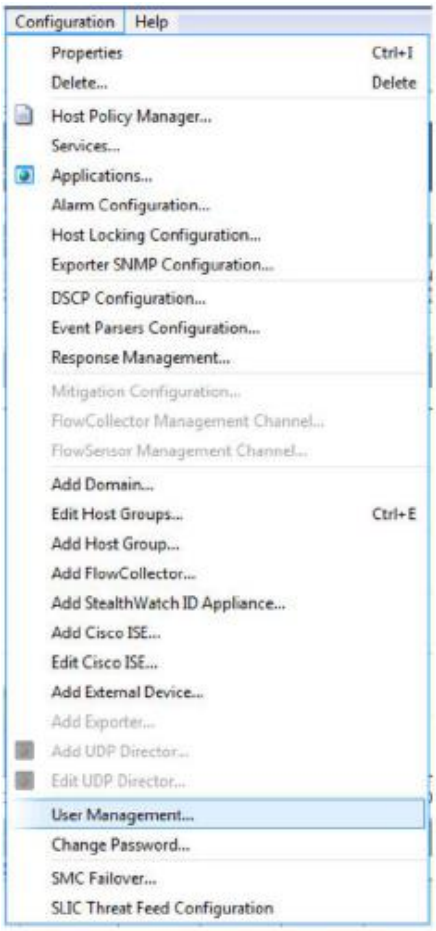
この演習では、お客様の環境には、Stealthwatch に対するさまざまなレベルのアクセス権を必要とする、数名の異なる従業員がいます。特に、必ずしも全員が、設定の変更が可能な完全な管理アクセス権を必要とするわけではありません。Stealthwatch に含まれているデータに対する完全なアクセス権を必要としながら、管理機能を必要としないユーザもいれば、特定の機能とネットワーク トラフィックに対するアクセスだけを必要とするユーザもいます。

Stealthwatch は、製品内のデータ ロールと機能ロールによる、ロール ベース アクセス コントロールをサポートしています。データ ロールは、ユーザがデータを読み取るオブジェクト（ホスト グループ、アプライアンス、エクスポータなど）を制御します。機能ロールは、ユーザが利用できるドキュメントやメニュー項目（グラフ、表、チャートなど）を判断します。

お客様からは次のように、Stealthwatch へのアクセスを必要とするユーザの表が提供されています。ここでユーザを作成し、この情報に基づいて適切なアクセス許可を割り当てます。

ユーザ名	データへのアクセス	機能へのアクセス
soc	すべてのデータへの読み取りアクセス	設定に関係しないすべての機能へのアクセス
helpdesk	Atlanta の IP アドレスのみへの読み取りアクセス	トラフィック グラフ、上位カンバセーション、ホストのスナップショット、フロー テーブルへのアクセス
swadmin	フル アクセス	管理者としての製品設定へのフル アクセス

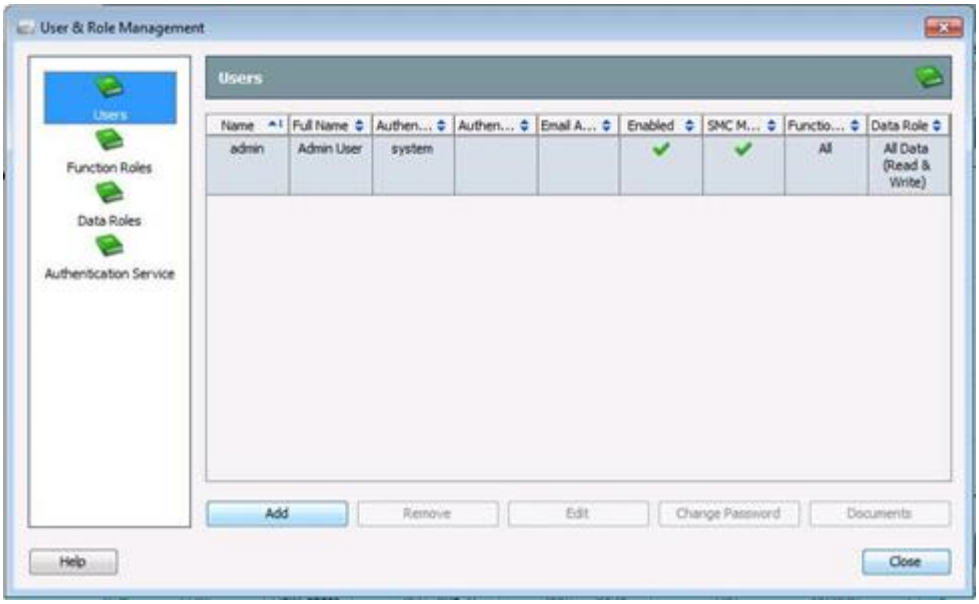
1. SMC Java インターフェイスを開きます。
2. [設定(Configuration)] メニューをクリックし、[ユーザ管理(User Management)] メニュー項目を選択して、[ユーザ管理(User Management)] を開きます。



注:soc ユーザは、Stealthwatch のすべてのデータおよび設定に関係しないすべての機能へのアクセスを必要としています。この目的で使用できる、デフォルトのデータ ロールと機能ロールが用意されています。次にユーザを作成し、関連するデータ/機能ロールを割り当てます。

3. 左ペインで、[ユーザ(Users)] メニューを選択します。SMC で定義されたユーザとユーザ アカウントの属性を示すリストが表示されます。

4. [追加(Add)] ボタンをクリックします。



5. [ユーザの追加(Add User)] ウィンドウで、次のデータを使用してユーザ設定を完了し、[OK] ボタンをクリックします。

   a. [ユーザ名(User Name)]:soc

   b. [フルネーム(Full Name)]:Security Operations Center

   c. [認証(Authentication)]:ローカル(local)

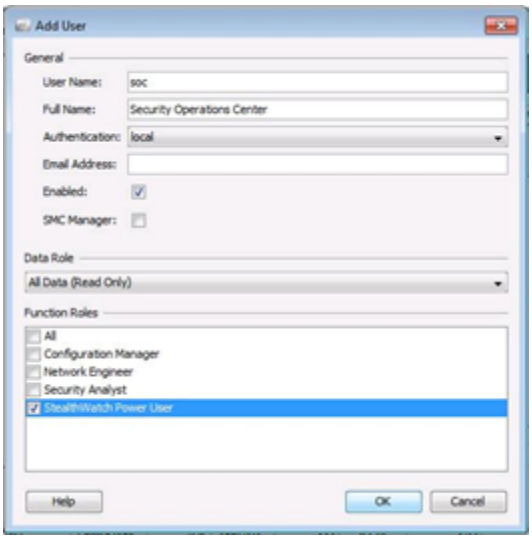
   d. [電子メール アドレス(Email Address)]:socadmin@customer.local

   e. [有効化(Enabled)]:オン

   f. [SMC Manager]:オフ

   g. [データ ロール(Data Role)]:すべてのデータ(読み取り専用)

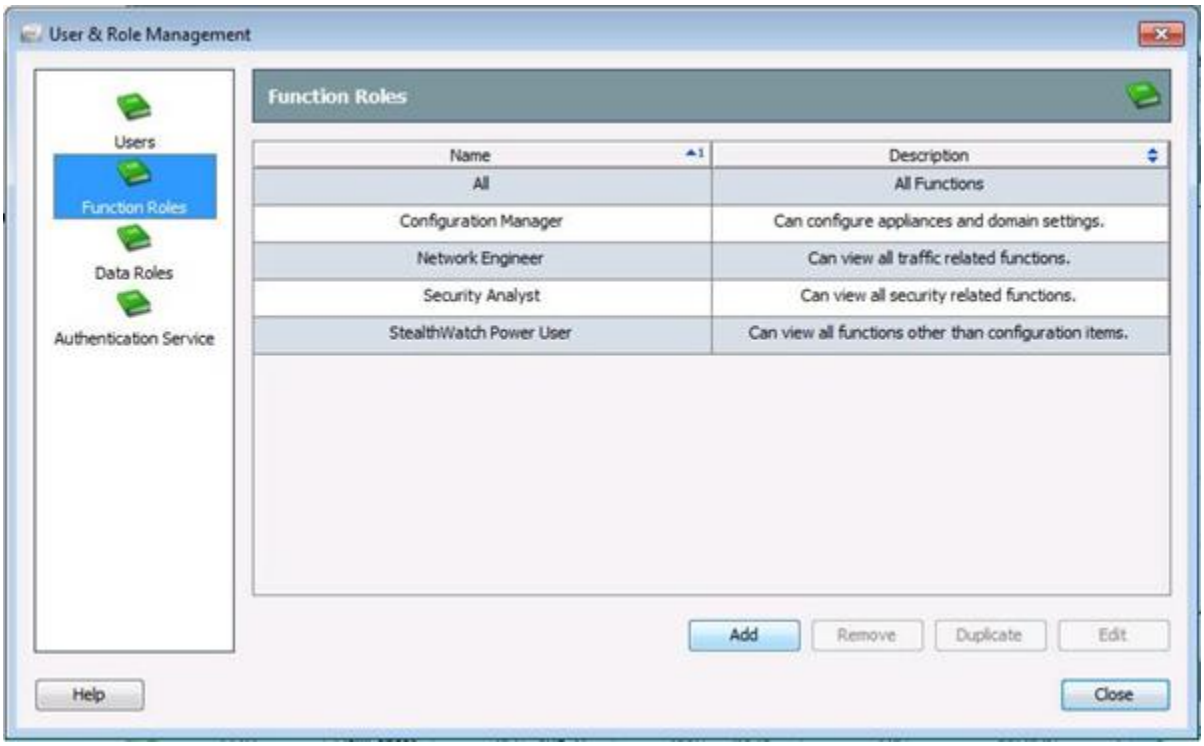
   h. [機能ロール(Function Role)]:Stealthwatch パワー ユーザ(Stealthwatch Power User)



6. パスワード データを入力するプロンプトが表示されます。最初のフィールドには、新しいユーザ アカウントの作成に使用するユーザ アカウントのパスワードを入力します。この場合は管理者ユーザです。[新規（New）] パスワード フィールドでは、作成した新しいユーザに割り当てるパスワードを 2 回入力するように求められます。3 つすべてのフィールドに「C1sco12345」と入力し、[OK] ボタンをクリックします。

7. ヘルプデスクのユーザ アカウントでは、カスタム データ ロールと機能ロールを作成する必要があります。左ペインで [機能ロール（Function Roles）] メニューを選択して続行します。

8. [追加（Add）] ボタンをクリックします。



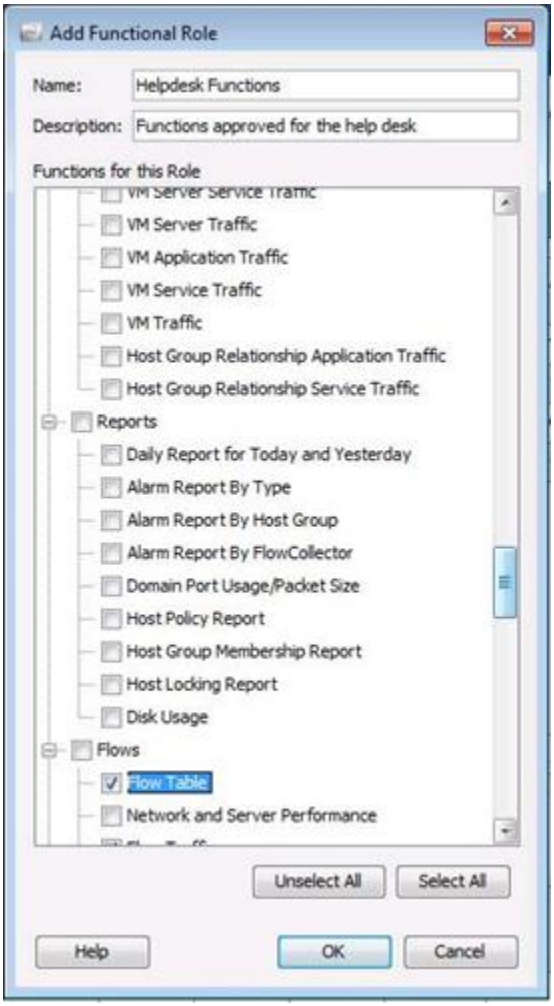
9. [機能ロールの追加（Add Functional Role）] ウィンドウで、この機能ロールが割り当てられたユーザに許可されるメニュー項目とドキュメントを指定します。このエントリは Stealthwatch のメニュー項目に類似しています。次の値を使用して機能ロールを設定し、[OK] をクリックします。

    a. [名前（Name）]：Helpdesk Functions

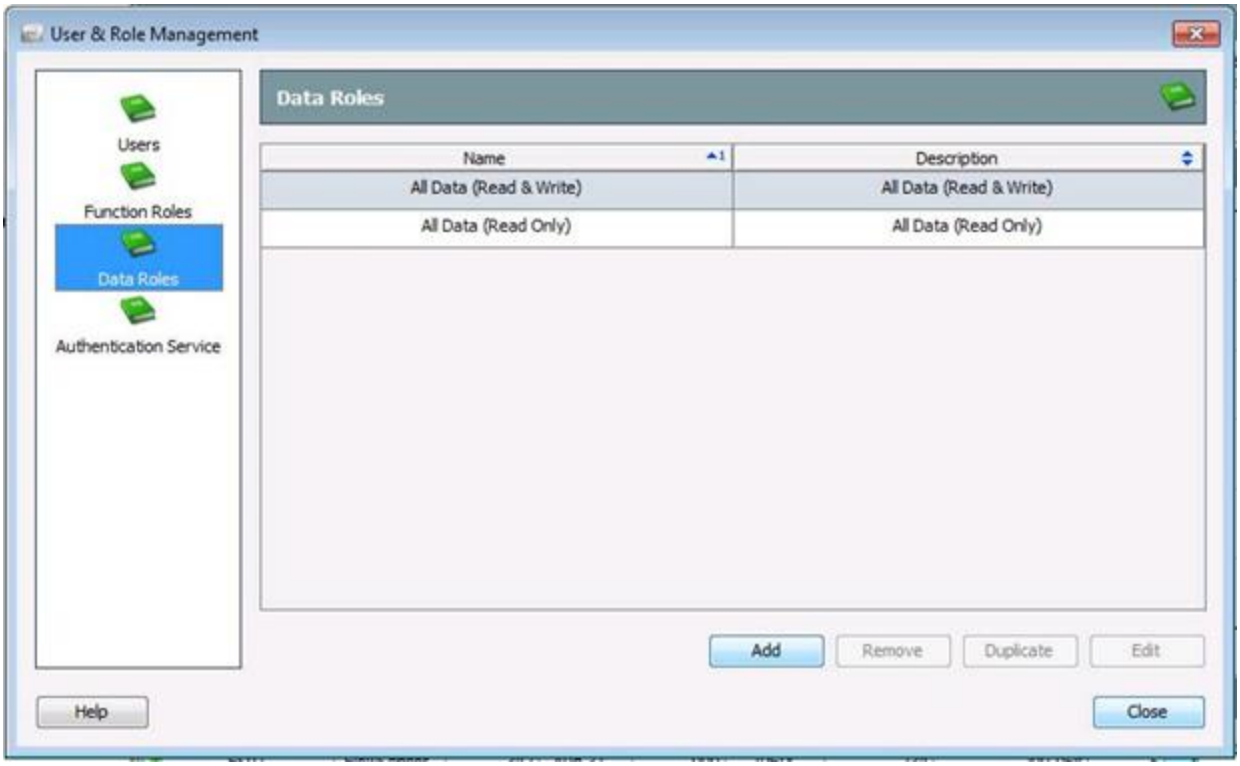
    b. [説明（Descriptions）]：ヘルプデスクに対して承認される機能（Functions approved for the help desk）

    c. [このロールに対する機能（Functions for this Role）]：（次のオプションをオンにする）

        - [上位フロー カンバセーション（Top Flow Conversations）]
        - [ホストのスナップショット（Host Snapshot）]
        - [フロー トラフィック（Flow Traffic）]
        - [フロー テーブル（Flow Table）]



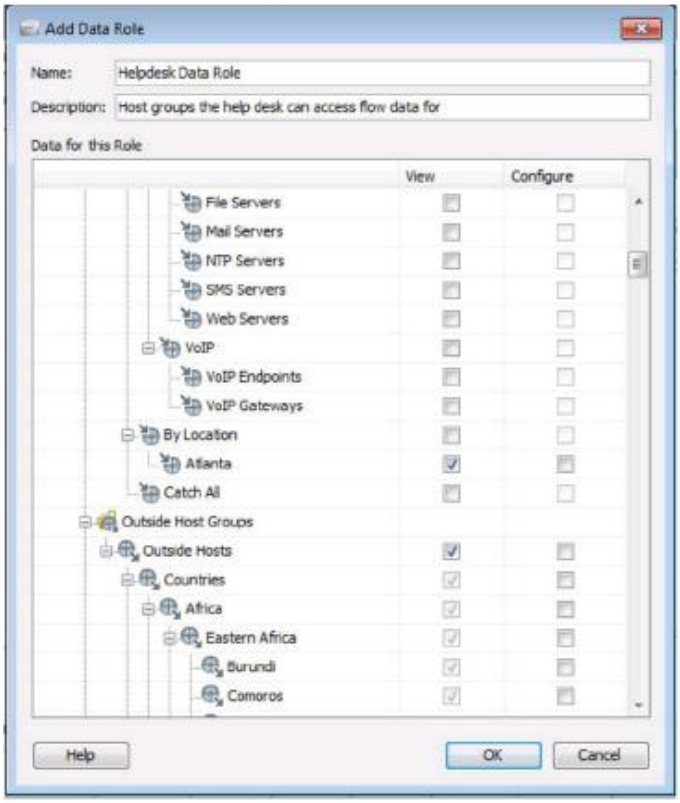
10. 製品のどの部分にユーザがアクセスできるかを制御する、機能ロールが作成されます。Stealthwatch に保存されているフロー データへのアクセスを制御する、データ ロールが作成されます。
11. 左ペインで、[データ ロール（Data Roles）] メニューを選択します。
12. [追加（Add）] ボタンをクリックします。



13. [データ ロールの追加（Add Data Role）] ウィンドウで、データ ロールによってアクセスが許可されるオブジェクトを指定します。

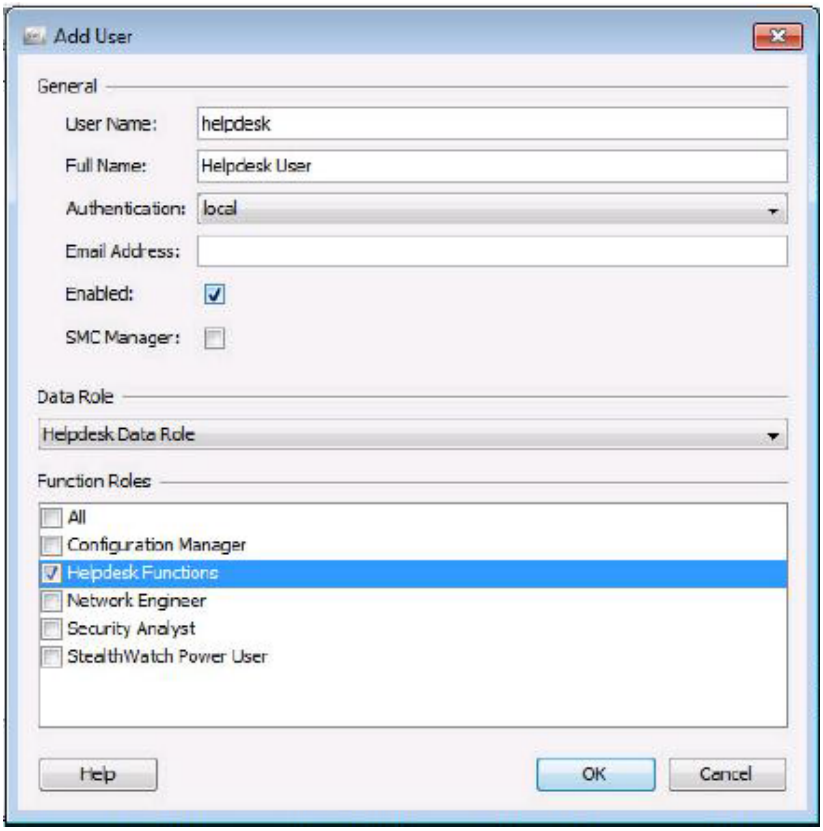
    a. [Atlanta] ホスト グループを特定し、[Atlanta] ホスト グループの [表示（View）] チェックマーク ボックスをオンにします。
    b. [外部（Outside）] ホスト グループを特定し、[外部（Outside）] ホスト グループの [表示（View）] チェックマーク ボックスをオンにします。
    c. [名前（Name）] および [説明（Description）] フィールドに次の値を入力します。
    d. [名前（Name）]：Helpdesk Data Role
    e. [説明（Description）]：ヘルプデスクがフロー データにアクセスできるホスト グループ（Host groups the help desk can access flow data）

14. [OK] ボタンをクリックします。



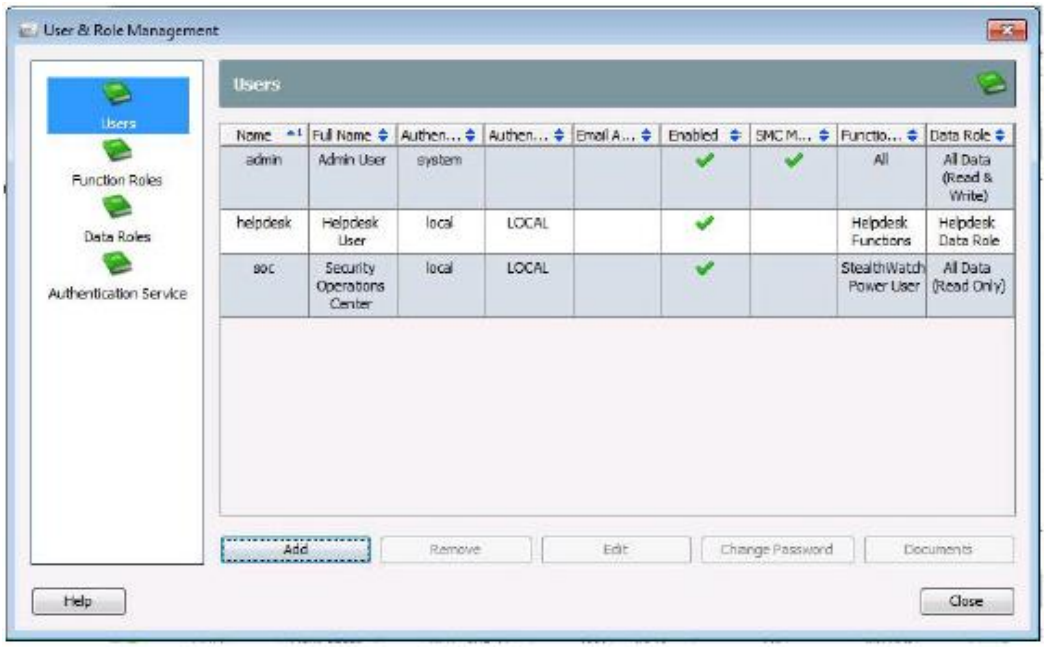
注:表示アクセス許可では、このデータ ロールを割り当てられたユーザが、選択したホスト グループの IP アドレスから送信されたデータを表示できます。[設定(Configure)] チェックマーク ボックスをオンにすると、ユーザに、ホスト グループに対する変更(IP アドレスの追加/削除)が許可されます。

15. 機能ロールとデータ ロールを作成したので、次にヘルプデスクのユーザ アカウントを作成します。左ペインの [ユーザ(Users)] メニューを選択し、[追加(Add)] ボタンをクリックします。
16. [ユーザの追加(Add User)] ウィンドウで、次のデータを使用してユーザ設定を完了し、[OK] ボタンをクリックします。
    a. [ユーザ名(User Name)]:helpdesk
    b. [フルネーム(Full Name)]:Helpdesk User
    c. [認証(Authentication)]:ローカル(local)
    d. [有効化(Enabled)]:オン
    e. [SMC Manager]:オフ
    f. [データ ロール(Data Role)]:ヘルプデスク データ ロール(Helpdesk Data Role)
    g. [機能ロール(Function Role)]:ヘルプデスク機能(Helpdesk Functions)



17. パスワード データを入力するプロンプトが表示されます。最初のフィールドには、新しいユーザ アカウントの作成に使用するユーザ アカウントのパスワードを入力します。この場合は管理者ユーザです。[新規（New）] パスワード フィールドでは、作成した新しいユーザに割り当てるパスワードを 2 回入力するように求められます。3 つすべてのフィールドに「C1sco12345」と入力し、[OK] ボタンをクリックします。

18. 次に、swadmin ユーザのユーザ アカウントを作成します。このユーザは、Stealthwatch に対する完全な管理者アクセスを必要としています。このアクセスはデフォルトのオプションによって許可できるため、カスタム データ ロールまたはカスタム機能ロールは不要です。[追加（Add）] ボタンをクリックします。



19. [ユーザの追加（Add User）] ウィンドウで、次のデータを使用してユーザ設定を完了し、[OK] ボタンをクリックします。

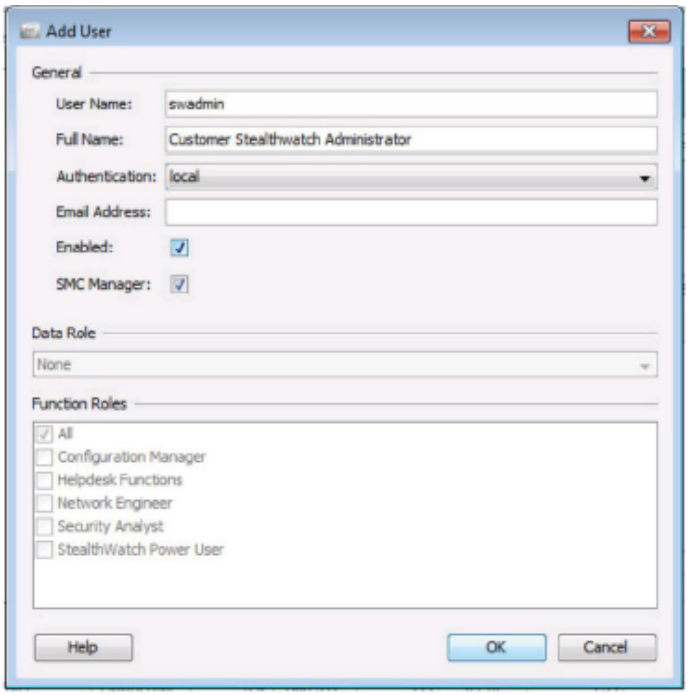
    a. [ユーザ名（User Name）]：swadmin

    b. [フルネーム（Full Name）]：Customer Stealthwatch Administrator

    c. [認証（Authentication）]：ローカル（local）

    d. [有効化（Enabled）]：オン

    e. [SMC Manager]：オフ



注：[SMC Manager] ボックスをオンにすると、その他すべてのオプションがグレーアウトされます。データ ロールと機能ロールは、SMC Manager アクセス許可を持つユーザに割り当てることはできません。SMC Manager は、SMC 内のすべてのオブジェクトに対する完全な制御が可能です。

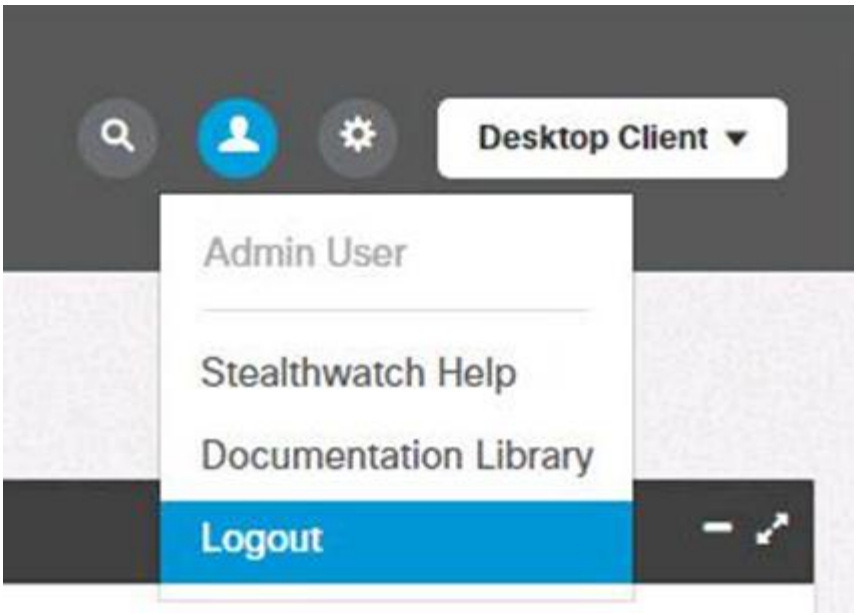
20. パスワード データを入力するプロンプトが表示されます。最初のフィールドには、新しいユーザ アカウントの作成に使用するユーザ アカウントのパスワードを入力します。この場合は管理者ユーザです。[新規（New）] パスワード フィールドでは、作成した新しいユーザに割り当てるパスワードを 2 回入力するように求められます。3 つすべてのフィールドに「C1sco12345」と入力し、[OK] ボタンをクリックします。

21. [ユーザおよびロール管理（User & Role Management）] ウィンドウが表示されたら、[閉じる（Close）] ボタンをクリックしてウィンドウを閉じ、SMC のメインのインターフェイスに戻ります。

注：SMC Manager アクセス許可と完全な機能/データ ロール アクセス許可によって定義されたユーザ アカウントを作成した場合でも、デフォルトの管理者ユーザ アカウントには、管理者ユーザだけが実行できる特別な機能があります。特定の管理者ユーザ専用の機能は、通常は Stealthwatch サポート ケースに関連する場合のみ使用されます。また、管理者ユーザ アカウントを削除することはできません。

22. ここで管理者ユーザとして SMC からログアウトし、作成したそれぞれのユーザ アカウントでログインして、アクセス許可をテストし、必要なアクセス権が設定されていることを確認します。[SMC Java] インターフェイスを閉じます。

23. Chrome Web ブラウザから SMC Web インターフェイスに戻ります。ウィンドウの右上側で [ユーザ（User）] アイコンをクリックし、[ログアウト（Logout）] メニュー オプションを選択します。



24. 管理者ユーザがログアウトされます。メインのログイン ページに戻ります。

25. SMC にログインし、それぞれのアカウントで Java インターフェイスを起動してステップ 26 を実行します。

    a. アカウント:

    b. soc

    c. helpdesk

    d. swadmin

26. 各アカウントを使用して、SMC で次のタスクを実行します。ユーザ アカウントの設定によっては、実行できないタスクがある場合があります。各ユーザとしてログインし、各手順を実行して、データ/機能ロールに対して先に行った設定を確認します。

    a. SMC にログインし、Java インターフェイスを起動します。
    b. 内部ホストのフロー トラフィック グラフ
        i. [内部ホスト（Inside Hosts）] ホスト グループに移動し、ホスト グループを選択します。
        ii. [トラフィック（Traffic）] メニューをクリックし、[フロー トラフィック（Flow Traffic）] メニュー項目を選択します。
    c. 内部ホストの上位カンバセーション
        i. [内部ホスト（Inside Hosts）] ホスト グループに移動し、ホスト グループを選択します。
        ii. [上位（Top）] メニューをクリックし、[上位カンバセーション（Top Conversations）] サブメニューを選択して、[全体（Total）] メニュー項目を選択します。
    d. 内部ホスト用のホスト グループ ダッシュボード
        i. [内部ホスト（Inside Hosts）] ホスト グループをダブルクリックします。
    e. Atlanta のフロー トラフィック グラフ
        i. [Atlanta] ホスト グループに移動し、ホスト グループを選択します。
        ii. [トラフィック（Traffic）] メニューをクリックし、[フロー トラフィック（Flow Traffic）] メニュー項目を選択します。
    f. Atlanta の上位カンバセーション
        i. [Atlanta] ホスト グループに移動し、ホスト グループを選択します。
        ii. [上位（Top）] メニューをクリックし、[上位カンバセーション（Top Conversations）] サブメニューを選択して、[全体（Total）] メニュー項目を選択します。
    g. Atlanta のホスト グループ ダッシュボード
        i. [Atlanta] ホスト グループをダブルクリックします。
    h. フロー コレクタ – システム アラーム [フロー コレクタのデータが削除されました（Flow Collector Data Deleted）] のチェックマーク ボックスのオン/オフを切り替え
        i. [エンタープライズ（Enterprise）] ツリーで FCNF01 フロー コレクタに移動します。
        ii. [設定（Configuration）] メニューをクリックし、[プロパティ（Properties）] メニュー項目を選択します。
        iii. 左側の [システム アラーム（System Alarms）] メニューを選択します。
        iv. [データ削除（Data Deleted）] オプションのオン/オフを切り替えて、変更を保存します。

i. [ロケーション別（By Location）] の下に、Brisbane という新しいホスト グループを作成します。
    i. [ロケーション別（By Location）] ホスト グループに移動します。
    ii. [ロケーション別（By Location）] ホスト グループを右クリックします。
    iii. [設定（Configuration）] メニューをクリックし、[ホスト グループの追加（Add Host Group）] メニュー項目を選択します。

シナリオのまとめ

これで、ユーザ プロビジョニングは終了です。各種のデータ ロールと機能ロールを扱い、製品内のさまざまなアクセス許可の効果を確認しました。セキュリティのベストプラクティスに従うために、sysadmin および root ユーザ アカウントのパスワードをデフォルト以外の値に変更しました。

付録 B.　NetFlow エクスポータの設定

手順

シスコ デバイスにおける NetFlow 設定は、次の 4 つの手順から構成されます。

1. フロー レコードを定義する
2. フロー エクスポータを設定する
3. フロー モニタを設定する
4. フロー モニタをインターフェイスに適用する

フロー レコードを定義する

フロー レコードは、フロー内のパケット数、フローごとに収集されるカウンタのタイプなど、NetFlow が収集する情報を定義します。あらかじめ定義された netflow-original 以外のカスタム フロー レコードを作成する場合は、一連の match コマンドと collect コマンドを指定して、送信 NetFlow PDU に含めるフィールドをデバイスに指示します。

match フィールドは、キー フィールドです。これらは、フローを一意にするために使用されます。collect フィールドは単なる追加情報であり、コレクタにレポートと分析のための詳細を提供するものです。

match フィールドについては、それほど変更する必要はありません。以下に記載されている 7 つの match エントリは、常に設定に含まれている必要があります。

一方、collect フィールドは、コレクタに送信する情報の量に応じてかなり異なる場合があります。

Stealthwatch のインストールには、以下の設定をお勧めします。

下記で「required」と記載されているフィールドは、Stealthwatch がフロー レコードを受け入れて作成するために必要なフィールドです。

```
Flow record STEALTHWATCH1
match  ipv4 protocol                          (required; key field)
match  ipv4 source address                    (required; key field)
match  ipv4 destination address               (required; key field)
match  transport source-port                  (required; key field)
match  transport destination-port             (required; key field)
match  interface input                        (required; key field)
match ipv4 tos                                (required; key field)
collect interface output                      (required; key field)
collect counter bytes                         (required; key field)
collect counter packets                       (required; key field)
collect timestamp sys-uptime first            (required; for calculating duration)
collect timestamp sys-uptime last             (required; for calculating duration)
collect routing next-hop address ipv4         (optional; used for closest interface determination)
collect ipv4 dscp                             (optional; used for closest interface determination)
collect ipv4 ttl minimum                      (optional; used for closest interface determination)
collect ipv4 ttl maximum                      (optional; used for closest interface determination)
collect transport tcp flags                   (optional; used for closest interface determination)
collect routing destination as                (optional; used for closest interface determination)
```

フロー エクスポータを定義する

フロー レコードが作成されたら、それをフロー エクスポータに結び付けます。

フロー エクスポータ設定では、NetFlow データの送信先となるフロー コレクタの物理または仮想 IP アドレスを定義します。また、フロー エクスポータ デバイスが NetFlow データを送信する際の送信元インターフェイスを定義します。これは、物理アドレスでも論理アドレスでも構いません。NetFlow データの送信元としてループバック インターフェイスを使用することも検討する価値があります。ループバックは通常、他のインターフェイスに障害が発生しても稼動を続け、トランスポートの継続が可能になるためです（ルーティングが許可されている場合）。また、ここでは、トランスポート プロトコル（TCP または UDP）と宛先ポートも定義されます。宛先ポートは NetFlow コレクタ固有のもので、この場合は Stealthwatch Flow Collector によって使用されるポートを参照します。

フロー エクスポータを定義するには、次の手順を実行します。

```
flow exporter Stealthwatch_Exporter
description Stealthwatch Export to Flow
Collector destination [Collector_IP_Address]
source [Physical_Interface | Logical_Interface]

transport udp 2055
```

フロー モニタを定義する

フロー モニタは、すべてのコンストラクトを結合して、フロー エクスポータとフロー レコードを参照します。フロー モニタを定義するには、次の手順を実行します。

```
flow monitor Stealthwatch_Monitor
description Stealthwatch Flow Monitor
exporter Stealthwatch_Exporter
cache timeout active 60
record STEALTHWATCH1
```

上記のキャッシュ タイムアウト行に注意してください。これは Stealthwatch の推奨設定です。シスコ デバイスのデフォルト設定は 30 分で、異常のレポートが目的の場合には長すぎます。

フロー モニタの設定には、以前に設定されたフロー エクスポータとフロー レコードが結び付いています。命名規則については何でも指定できます。ただし、正しい名前を参照している場合に限ります。IOS でコンテキスト センシティブ ヘルプを使用すると、以前に設定された全パラメータをいつでも表示できるため、便利です。

コンテキスト センシティブ ヘルプを使用して、設定されたフロー レコードとフロー エクスポータ、および利用可能なシステム デフォルト レコードを知る方法については、以下の例を参照してください。

```
BR_ASW1(config)#flow monitor STEALTHWATCH_MONITOR
BR_ASW1(config-flow-monitor)#record ?
STEALTHWATCH_RECORD User defined
wireless Templates for Wireless Traffic
BR_ASW1(config-flow-monitor)#exporter ?
STEALTHWATCH_EXPORTER Stealthwatch Export to Flow Collector
```

最後に、上記のすべての NetFlow 設定を、フロー分析が必要な各インターフェイスに適用する必要があります。下記を参照してください。

フロー モニタをインターフェイスに適用する

```
interface [Interface_ID]
ip flow monitor Stealthwatch_Monitor input
```

NetFlow 設定の例は以下のとおりです。

Cisco NetFlow の設定

NetFlow レコードを設定するコマンド、フィールドは、プラットフォームによって異なる場合があります。

```
flow record Stealthwatch_FlowRecord
description Flow Record for Export to Stealthwatch (optional)

match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match ipv4 tos
match transport source-port
match transport destination-port
match interface input
match flow direction
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 ttl minimum
collect ipv4 ttl maximum
collect transport tcp flags
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

TrustSec 固有の match フィールド

```
match flow cts source group-tag
match flow cts destination group-tag
```

NBAR2 固有のコレクション（プロトコル パックはルータ上でアクティブ）

```
collect application name
collect application http url
collect application http host
```

AVC 固有のフィールド

```
collect connection initiator
collect connection new-connections
collect connection sum-duration
collect connection delay response to-server sum
collect connection delay response to-server min
collect connection delay response to-server max
collect connection server counter responses
collect connection delay response to-server histogram late
```

```
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application min
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter packets long
collect connection client counter packets long
collect connection client counter bytes retransmitted
collect connection server counter bytes network long
collect connection client counter bytes network long
collect connection delay network client-to-server num-samples
collect connection delay network to-server num-samples
collect connection delay network to-client num-samples
```

付録 C.　Cognitive Analytics の有効化

Cisco Cognitive Analytics は、不審な Web トラフィックや NetFlow に対する分析レイヤを追加し、お客様環境内にプレゼンスを確立しようとする悪意のある試みが発生した場合にアラートを表示するだけでなく、すでに進行中の攻撃を特定します。Stealthwatch システムでこの機能が有効化されると、Stealthwatch は NetFlow データとプロキシ Web ログ データ（利用可能な場合）を分析のために Cognitive クラウドに送信します。

お客様環境でこの機能が有効化されると、3 つのカテゴリに分類されるデータ（境界 NetFlow、限定された内部 DNS トラフィック、プロキシ Web ログ）が、ロンドンの CTA データセンターに SCP および HTTPS 経由で送信されます。Web ログ データは、Stealthwatch プロキシ インジェスチョンが設定されている場合にのみ送信されます。

これは、お客様から明確に許可を得られた場合にのみ、有効にしてください。この機能はデフォルトで無効に設定されています。

この機能を有効にするには、Stealthwatch ドメインに存在する SMC および FC 上で機能を有効にする必要があります。また、これらのアプライアンスは、テレメトリ データを送信し、分析結果およびアラートを受信するためにインターネット上のホストにアクセスできる必要があります。

SMC の要件：

- 以下へのアクセス
    - cognitive.cisco.com（108.171.128.81）、443 ポート経由

FC の要件：

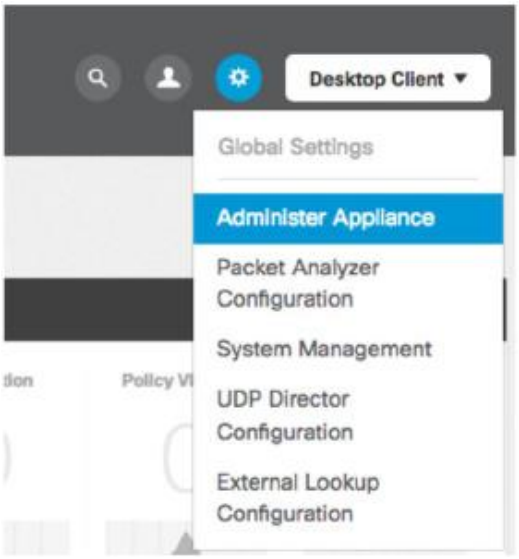
- 以下へのアクセス
    - etr.cloudsec.sco.cisco.com（108.171.128.86）、443 ポート経由
    - cognitive.cisco.com（108.171.128.81）、443 ポート経由

注：パブリック DNS が許可されていない場合は、Stealthwatch Management Console および Flow Collector 上でローカルに名前解決を設定する必要があります。

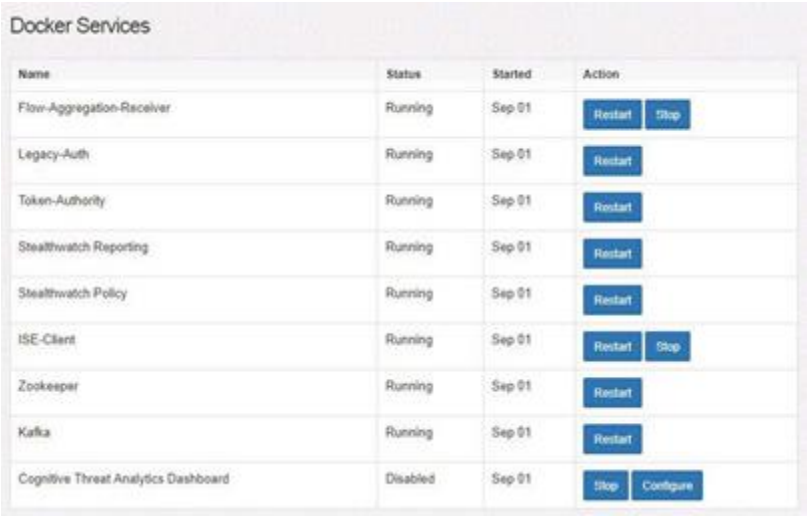
手順

管理コンソールで Cognitive Analytics を有効にします。

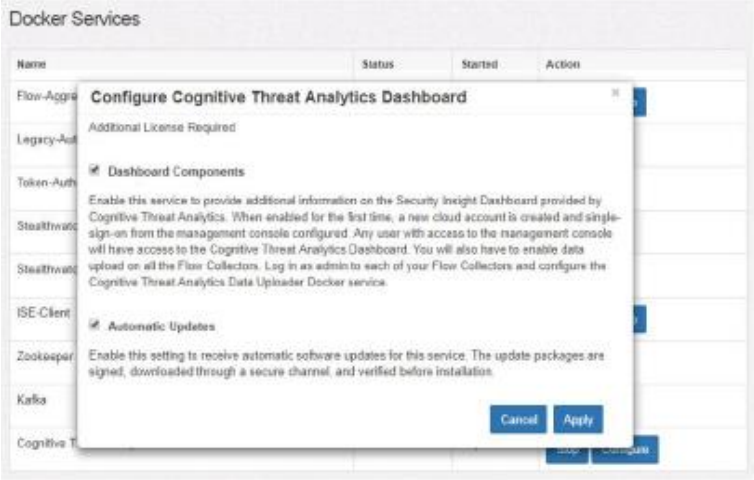
1. SMC に管理者権限でログインします。
2. [デスクトップ クライアント（Desktop Client）] ドロップダウンの横にある歯車アイコンをクリックし、[アプライアンスの管理（Administer Appliance）] を選択して、[アプライアンス管理（Appliance Administration）] 画面に移動します。



3. [ホーム（Home）] ページで、[Docker サービス（Docker Services）] までスクロール ダウンします。
4. [Cognitive Threat Analytics データ ダッシュ ボード（Cognitive Threat Analytics Data Dashboard）] で [設定（Configure）] をクリックします。



5. [ダッシュボード コンポーネント（Dashboard Components）] と [自動更新（Automatic Updates）] の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。

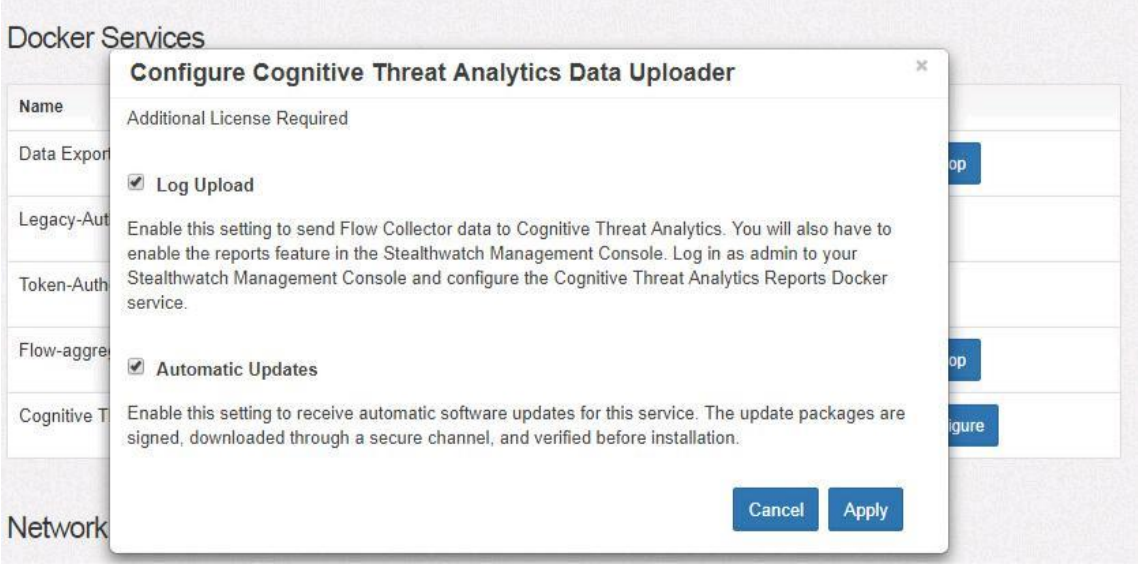
注:無効にする場合に、[停止(Stop)] をクリックしないでください。Cognitive Analytics を無効にするには、[設定(Configure)] メニューのオプションのチェックを外します。

7. [設定(Configuration)] ページを閉じ、SMC からログアウトしてログインし直します。これで、SMC のダッシュ ボードに [Cognitive Threat Analytics] パネルが表示されます。

フロー コレクタで Cognitive Analytics を有効にする

1. フロー コレクタに管理者権限でログインします。
2. [ホーム(Home)] ページで、[Docker サービス(Docker Services)] までスクロール ダウンします。

3. [Cognitive Threat Analytics データのアップローダ（Cognitive Threat Analytics Data Uploader）] で [設定（Configure）] をクリックします。



4. [ログのアップロード（Log Upload）] と [自動更新（Automatic Updates）] のチェックボックスをオンにします。
5. [適用（Apply）] をクリックします。

注：無効にする場合に、[停止（Stop）] をクリックしないでください。Cognitive Analytics を無効にするには、[設定（Configure）] メニューのオプションのチェックを外します。

付録 D.　VM の要件

注:VMware ESXi 環境において、すべての Stealthwatch アプライアンスに対して vMotion を無効にする必要があります。データ書き込み中に vMotion のアクティビティが発生するとデータベース破損の原因となります。破損した場合は、データベースをロールバックするか、アプライアンスを工場出荷時の初期状態にリセットする必要があります。

Stealthwatch Management Console 仮想エディション

SMC VE に割り当てる最小限のリソースを判断するためには、フロー コレクタ数および SMC への予測ログイン数を見極める必要があります。最小仕様よりも少ないリソースで Stealthwatch アプライアンスを実行すると、パフォーマンスと安定性に悪影響を与えます。

表 5.　リソース割り当て

モデル	サポートされるフロー コレクタ	同時ユーザ数	予約済み CPU	最小の予約済みメモリ	推奨の予約済みメモリ	ディスク領域	セッション データを ISE/その他から収集する場合
SMC VE	1	2	3	16 GB	24 GB	100 GB	SMC VE < 10,000 ユーザ
SMC VE	3	5	4	24 GB	32 GB	100 GB	SMC VE < 10,000 ユーザ
SMC VE	5	10	4	32 GB	32 GB	100 GB	SMC VE < 10,000 ユーザ
SMC VE 2000	25	15	8	64 GB	64 GB	200 GB	SMC VE 2000 > 10,000 ユーザ

*同時ユーザ数には、スケジュールされたレポートの数および SMC クライアントを同時に使用しているユーザの数が含まれます。

予約済みメモリ:システムのフロー コレクタ数が限られ、データ収集量が少ない場合は、最小の予約済みメモリ量でも構いません。データの収集量が多い場合は、推奨の予約済みメモリ量を使用してください。

Stealthwatch Flow Collector 仮想エディション

Flow Collector VE に割り当てるリソースを判断するには、ネットワーク上で想定される 1 秒あたりのフロー数、エクスポータ数およびモニタ対象のホスト数を見極める必要があります。

表 6.　リソース割り当て

モデル	1 秒あたりのフロー数	エクスポータ	ホスト数	予約済み CPU	予約済みメモリ	ディスク領域
FCVE	最大 4,500	最大 250	最大 125,000	2	16 GB	1 TB
FCVE	最大 15,000	最大 500	最大 250,000	3	24 GB	1 TB
FCVE	最大 22,500	最大 1000	最大 500,000	4	32 GB	1 TB
FCVE	最大 30,000	最大 1000	最大 500,000	5	32 GB	1 TB
FCVE 2000	最大 60,000	最大 1500	最大 750,000	6	64 GB	2 TB
FCVE 4000	最大 120,000	最大 2000	最大 1,000,000	7	128 GB	4 TB

Stealthwatch Flow Sensor 仮想エディション

v6.9.1 以降の Stealthwatch システムは、Flow Sensor VE の NIC 数に応じて、さまざまなタイプの Flow Sensor VE を提供しています。VE アプライアンスを導入する場合はすべて、ディスク容量を 50 GB 以上にする必要があります。

フロー キャッシュ サイズは、予約済みのメモリ量に応じて調整します。フロー キャッシュ サイズを使用して、モニタ対象のトラフィック量に必要なメモリの量を計算します。

注:表に記載されている割り当ては、推奨事項に過ぎません。必要なスループットを達成するには、特定の環境に応じたリソースが必要です。平均パケット サイズ、バースト レート、および他のネットワーク状況やホスト状況などの多数の変数によって異なる可能性があります。

表 7. 推奨の割り当て

モデル	NIC モニタリング ポート数(1 GB)	予約済み CPU	予約済み メモリ	ディスク 領域	相当するハードウェア スループット	フロー キャッシュ サイズ
Flow Sensor Base、Flow Sensor VE	1	1	4 GB	50 GB	該当なし	32,766
Flow Sensor Base	4	8	16 GB	50 GB	最大 FS1200 * PCI パススルーとしてインターフェイスが設定されていること	131,073
Flow Sensor Base	5	32	32 GB	50 GB	最大 FS2200 * PCI パススルーとしてインターフェイスが設定されていること	262,145

Stealthwatch UDP Director 仮想エディション

UDP Director VE では、VMware サーバが以下の仕様を満たしていることが必要です。

- 4 GB の RAM
- ディスク空き容量:50 GB

付録 E.　UDP Director による FPS のサイジング

UDP Director でこの機能を有効にすると、Flow Estimator が有効化されます。通常 UDPD では、着信および送信パケット数に関する情報が表示されますが、[詳細なフロー統計情報（Detailed Flow Statistics）] オプションをオンにしない限り、各エクスポータを通じて送信される FPS（1 秒あたりのフロー数）は認識されません。これをオンにすると、UDPD では NetFlow パケットを分析して、UDPD にフロー レコードを送信する各エクスポータの FPS レートが判定されます。これは、Stealthwatch を購入する前に FPS ロードを判断する必要があるお客様環境で有効です。

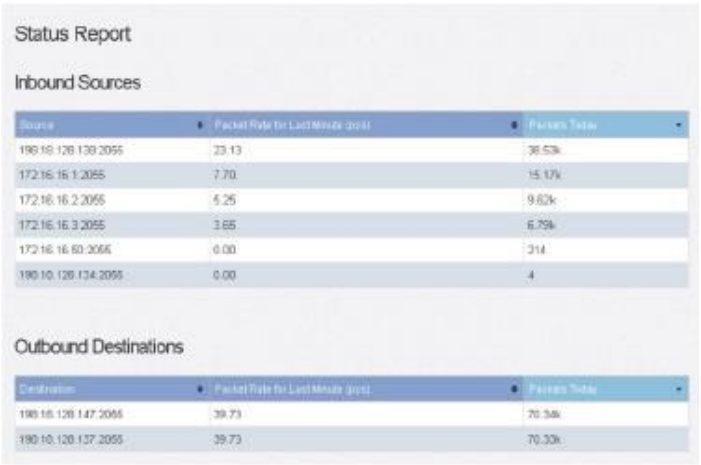
手順

1. UDP Director に管理者のクレデンシャルを使用してログインします。
2. [ホーム（Home）] メニューをクリックします。
3. UDPD のホーム ページに [詳細なフロー統計情報（Detailed Flow Statistics）] オプションがあります。これはアプライアンスの CPU 使用率が増加するため、デフォルトでオフになっています。[有効化（Enable）] ボックスにチェックマークを入れて、このオプションをオンにします。

注：お客様環境では、初期導入中に [詳細なフロー統計情報（Detailed Flow Statistics）] 機能を有効にすると役立ちます。UDP Director で CPU 負荷（負荷平均）に注意し、すでにビジーである UDPD が、フロー統計情報を有効にすることで過負荷にならないようにします。

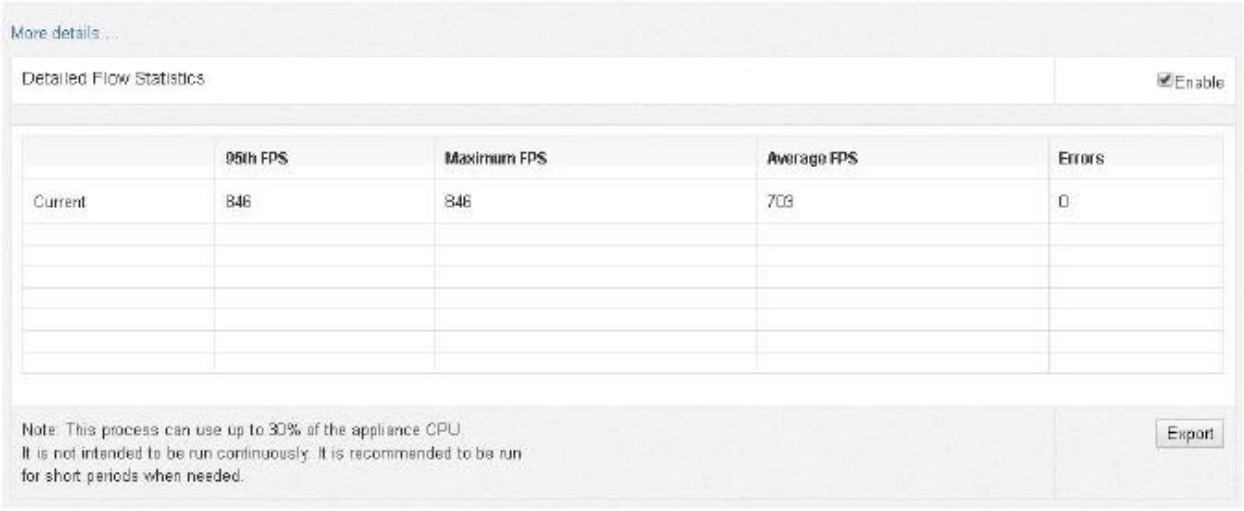
負荷平均は、アプライアンスのホーム ページで確認できます。負荷平均は CPU 使用率のパーセンテージではありません。負荷平均は、使用されている CPU 数、またはアプリケーションがリソースを待機している CPU 数に関係します。基本的な例として、2 つの CPU アプライアンスの負荷平均が 0 の場合、CPU 使用率は 0 % になります。別の例として、同一システムで負荷平均が 1 の場合、アプライアンスの CPU 使用率は約 50 % になります。これは概算ですが、この値が CPU のパーセンテージではないことを理解してください。

4. 統計情報ペインに情報が表示されるまで、数分かかる場合があります。統計情報を生成している間に、その他のデータを確認することができます。[詳細なフロー統計情報（Detailed Flow Statistics）] のすぐ上にある [詳細の表示（More details）] リンクをクリックします。
5. [ステータス レポート（Status Report）] ページが開き、送信元の UDP データと宛先が表示されます。転送ルールに適合する送信元/宛先のみが表示されます。UDP データを UDPD に送信するデバイスがあり、インバウンド トラフィックに適合するルールが転送ルールの設定に含まれていない場合、トラフィックは表示されず、転送もされません。



注：この情報は、NetFlow 設定に関する問題のトラブルシューティングにも役立ちます。

6. UDPD のホームページに戻ります。
7. ホームページの [詳細なフロー統計情報（Detailed Flow Statistics）] セクションを確認します。UDPD が処理した FPS の統計を UDPD が計算していることがわかります。



注：お客様の多くは、ネットワークが生成する FPS を確認する方法がありません。お客様環境の FPS ボリュームを判定するという明確な目的で、価値の実証プロセスで UDPD を導入することができます。もう 1 つの利点は、お客様が UDP 管理トラフィックを転送できるという UDPD の価値を認識し、Stealthwatch の注文に UDPD のライセンスを含めるきっかけになることです。

付録 F.　Stealthwatch OVF の導入

このラボでは、Stealthwatch アプライアンスについて、初期 OVF 導入と管理 IP アドレスの割り当て/設定をスキップします。これらの手順について、以下に参照用として要点を説明します。

手順

リソース プールの追加

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

1. VMware vSphere クライアント ソフトウェアを起動します。[ログイン（Login）] 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、[ログイン（Login）] をクリックします。
3. [はじめに（Getting Started）] ページが開きます。
4. 左側の [インベントリ（Inventory）] 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）] を選択します。
5. [リソース プールの作成（Create Resource Pool）] ダイアログが開きます。
6. [名前（Name）] フィールドで、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。
7. [CPU リソース（CPU Resources）] セクション内の設定は変更しないでください。
8. [メモリ リソース（Memory Resources）] セクションで、以下を実行します。
9. [制限（Limit）] フィールドを最低 32 GB（SMC と FC の 2 つを組み合わせる場合 40 GB を推奨、これより大規模な環境をインストールする場合はさらに増やす）に変更します。アプライアンス向けに予約するリソースのサイジングについては、付録の「VM の要件」を参照してください。
10. [制限なし（Unlimited）] チェックボックスをクリックしてオフにします。
11. [OK] をクリックします
12. リソース プールがインベントリ ツリー上の ESX サーバの下に表示されます。
13. リソース プールを選択し、[リソース割り当て（Resource Allocation）] タブをクリックして、CPU とメモリのリソース割り当てを確認します。

OVF の導入

ESX サーバに仮想アプライアンスをインストールし、仮想アプライアンスの管理ポート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. 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 クライアント メニューで [ファイル（File）] > [OVF テンプレートのデプロイ（Deploy OVF Template）] をクリックします。
    a. [OVF テンプレートのデプロイ（Deploy OVF Template）] ウィザードが開きます。
3. [参照（Browse）] をクリックし、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。
4. [OVF テンプレートの詳細（OVF Template Details）] ページで [次へ（Next）] をクリックします。
5. [次へ（Next）] をクリックします。[エンド ユーザー使用許諾契約書（End User License Agreement）] が開きます。

6. 情報を確認した後 [承諾（Accept）] をクリックし、[次へ（Next）] をクリックします。
    a [名前と場所（Name and Location）] ページが開きます。
7. 必要に応じて、[インベントリ（Inventory）] 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。
8. [ディスク形式（Disk Format）] ページが開きます。
9. [ディスク形式（Disk Format）] ページで [シック プロビジョニング（Thick provisioned）] 形式を選択して、[次へ（Next）] をクリックします。
10. [次へ（Next）] をクリックします。
    a. [終了準備の完了（Ready to Complete）] ページが開き、設定の概要が表示されます。
11. 設定を確認したら、[終了（Finish）] をクリックします。
    a. 進行状況を示すダイアログが開きます。
12. デプロイが終了したら、[閉じる（Close）] をクリックして、このダイアログを閉じます。
    a. 仮想アプライアンスは、インベントリ ツリーに表示されます。

アプライアンスの IP アドレスの設定

仮想アプライアンスに IP アドレスを設定する手順は、次のとおりです。

1. vSphere クライアント ソフトウェアを起動し、ログインします。
    a. [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、[仮想マシンのパワーオン（Power on the virtual machine）] というリンクをクリックします。
4. [コンソール（Console）] タブをクリックします。仮想アプライアンスの起動完了を許可します。
    a. 仮想アプライアンスの [管理用 IP アドレス（Administrative IP Address）] ページが開きます。
5. ページをクリックし、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 Enter を押します。
    a. [IP ネットマスク（IP Netmask）] ページが開き、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ます。
7. 次の手順を実行します。
    a. デフォルト値を受け入れるか、ご使用の環境に応じて新しい値を入力します。
    b. [OK] を選択し、Enter を押して続行します。
    c. [IP ブロードキャスト アドレス（IP Broadcast Address）] ページが開き、デフォルトのブロードキャスト IP アドレスが表示されます。
8. 次の手順を実行します。
    a. デフォルト値を受け入れるか、ご使用の環境に応じて新しい値を入力します。
    b. [OK] を選択し、Enter を押して続行します。
    c. [ゲートウェイ アドレス（Gateway Address）] ページが開き、デフォルト ゲートウェイ サーバの IP アドレスが表示されます。

9. 次の手順を実行します。
    a. デフォルト値を受け入れるか、ご使用の環境に応じて新しい値を入力します。
    b. [OK] を選択し、Enter を押して続行します。
    c. ページが開き、エントリのサマリーが表示されます。
10. Enter を押します。システム再起動ページが開きます。
11. Enter を押します。
    a. システムが再起動し、変更が適用されます。
    b. 完了すると、ログイン プロンプトが表示されます。

インストール指示について詳しくは、付録「Stealthwatch のオンライン リソース」を参照してください。

付録 G.　Stealthwatch のオンライン リソース

Cisco.com の Stealthwatch ドキュメント [英語]:

http://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html

インストールとアップグレード ガイド:

http://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-guides-list.html

テクニカル リファレンス:

https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-technical-reference-list.html

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp