

Cisco Stealthwatch 7.1 フィールド エンジニア トレーニング ラボ v1



Solutions Readiness Engineers と共同執筆

最終更新日時：2020 年 4 月 23 日

重要：このコンテンツはコミュニティによって開発されています。標準の dCloud の検証やサポートの対象にはなりません。詳細については、dCloud サポートにお問い合わせください。

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。

シナリオ 1.	アプライアンス セットアップ ツール	6
シナリオ 2.	アプライアンスのインストール後の設定および検証	50
シナリオ 3.	SMC および Central Management の追加設定	71
シナリオ 4.	ホストグループの設定	80
シナリオ 5.	シスコルータの NetFlow 設定および検証	91
シナリオ 6.	シスコルータの ETA 設定および検証	100
シナリオ 7.	カスタム セキュリティ イベント	113
シナリオ 8.	Stealthwatch デスクトップクライアントへのアクセス	120
シナリオ 9.	フローデータとエクスポートの検証	132

シナリオ 10.	お客様環境の分類	153
シナリオ 11.	未定義のサービスとアプリケーションの分類	190
シナリオ 12.	Cisco ISE (Identity Services Engine) との統合	210
シナリオ 13.	AD LDAP ルックアップ機能の設定	227
シナリオ 14.	カスタムドキュメントの作成	231
シナリオ 15.	応答管理	241
シナリオ 16.	アプライアンスの SNMP エージェントの設定	256
シナリオ 17.	予測される FC データベースストレージ容量の算出	259
シナリオ 18.	設定のバックアップの作成	263
シナリオ 19.	Stealthwatch のパッチ適用 : Central Management	266

要件

次の表に、このデモンストレーションの要件の概要を示します。

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

このハンズオンラボはフィールドエンジニアを対象に、Stealthwatch のインストールと設定に必要なスキルと方法論を提供することを目的としています。記載のラボシナリオを最後まで実行すると、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、現場でのお客様環境への導入に先立って、Stealthwatch のインストールに習熟できます。

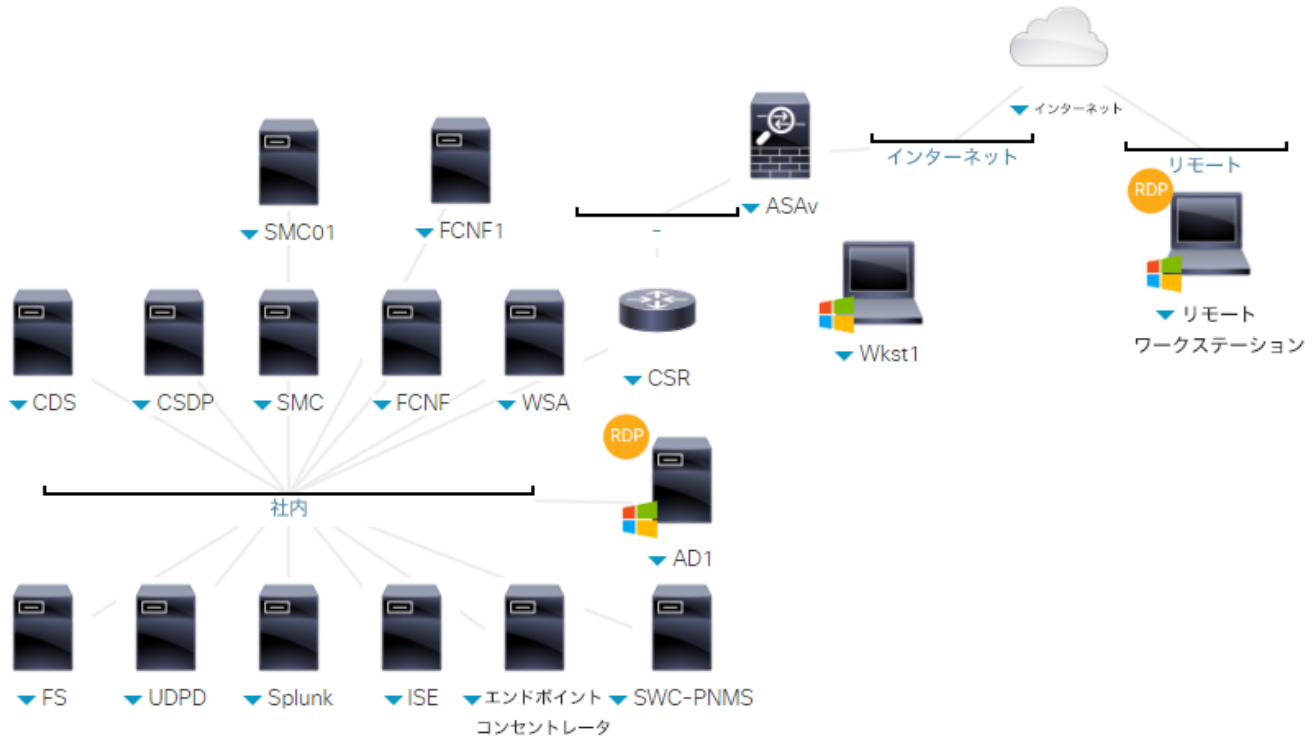
シナリオと dCloud ラボ環境では、Stealthwatch Management Console (SMC)、フローコレクタ (FC)、フローセンサー (FS)、および UDP Director (UDPD) アプライアンスの仮想モデルを使用します。トレーニングラボを完了する時点で、「お客様」はフル機能の Stealthwatch 環境が得られることとなります。アラームの調整はこのトレーニングラボの対象外ですが、応答管理と Stealthwatch システムアラームについては、Stealthwatch の一般的な初期実装の際に必要なため、説明を加えています。

ラボの一連のシナリオは、連続する 2 日間で完了するように設計されています。ラボの全手順を指示どおりに行えば、すべてのアクティビティを 1 日で実行することも可能です。

トポロジ

ラボのすべてのシナリオコンテンツでは、専用の Stealthwatch Management Console (SMC)、フローコレクタ (FC)、UDP Director (UDPD)、およびフローセンサー (FS) アプライアンスを使用します。コース全体では、さまざまなシナリオの必要に応じて追加のシステムを使用します。

dCloud のトポロジ



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、このガイドのシナリオを完了し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。[\[手順を見る\]](#) [英語]

注：セッションがアクティブになるまで、最大で **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、**ad1** ワークステーションへの接続には **Cisco AnyConnect VPN** [\[手順を見る\]](#) [英語] およびラップトップのローカル RDP クライアントを使用します。 [\[手順を見る\]](#) [英語]

- WKST1 : 198.19.30.36、ユーザ名 : dcloud\admin、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 [\[手順を見る\]](#) [英語]。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。ただしこの方法では、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。

シナリオ 1. アプライアンス セットアップ ツール

Stealthwatch アプライアンスは、仮想マシンの導入時に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。ここでは、dCloud セッション内にある Workstation 1 (WKST1) から個々の管理 IP アドレスを使用して、お客様の仮想アプライアンスにアクセスします。dCloud リモートデスクトップセッション (Web ブラウザまたは VPN) を介して WKST1 に接続し、各 Stealthwatch 仮想アプライアンスでアプライアンス セットアップ ツール (AST) を完了するとともに、コース全体で残りのラボをすべて完了します。

注：AST プロセスはそれぞれのアプライアンスで非常に類似していますが、適切に機能させるには、残りの設定手順とラボを進める前に、各アプライアンスですべての手順を完了する必要があります。

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。多くの場合、Stealthwatch の物理および仮想アプライアンスのインストールプロセスに関連する製品マニュアルとガイドランスを提供して、お客様の作業を支援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。System Configuration Utility と、各アプライアンスでの IP アドレスの設定方法の詳細については、このドキュメントの「[リソース](#)」セクションに示す、Stealthwatch のマニュアルと Fire Jumper Tech Talks セッションを必要に応じて参照してください。

アプライアンス セットアップ ツール (AST) 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 デプロイ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. Stealthwatch Management Console (SMC)
2. UDP Director (UDPD)
3. フローコレクタ (FC)
4. フローセンサー (FS)

注：これは、v7.x の新しいインストール順序です。先に進む前に、SMC が設定され、アクセス可能であることを確認してください。これは SMC アプライアンスが、各アプライアンスの Central Management をホストするためです

Stealthwatch Management Console

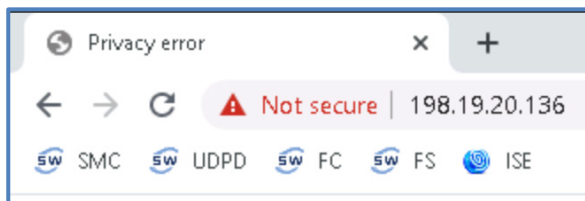
1. dCloud セッション内で **WKST1** システムの **dCloud リモートデスクトップ** セッションを使用していることを確認します。[WKST1] をクリック後、[リモートデスクトップ (Remote Desktop)] をクリックします。リモートデスクトップセッションが現在の Web ブラウザで開きます。
 - **注** : Web ベースのリモートデスクトップの代わりに、Cisco AnyConnect を使用して VPN トンネル経由でネイティブの RDP クライアントを使用することもできます。初期設定はこちらの方が複雑ですが、リモートシステムの画面解像度や画面サイズをより適切に制御できます。




2. WKST1 のデスクトップにあるショートカットを使用して **Chrome** Web ブラウザを開きます。



3. Chrome で **SMC** のブックマークを選択し、SMC の Web インターフェイスにアクセスします。



- Stealthwatch アプライアンスのデフォルトでは、信頼されていない自己署名証明書が使用されるため、ブラウザのセキュリティ警告が表示されます。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)] ボタンをクリックし、[-にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックして、ログインページを開きます。




Your connection is not private

Attackers might be trying to steal your information from **198.19.20.136** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced Back to safety



Your connection is not private

Attackers might be trying to steal your information from **198.19.20.136** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

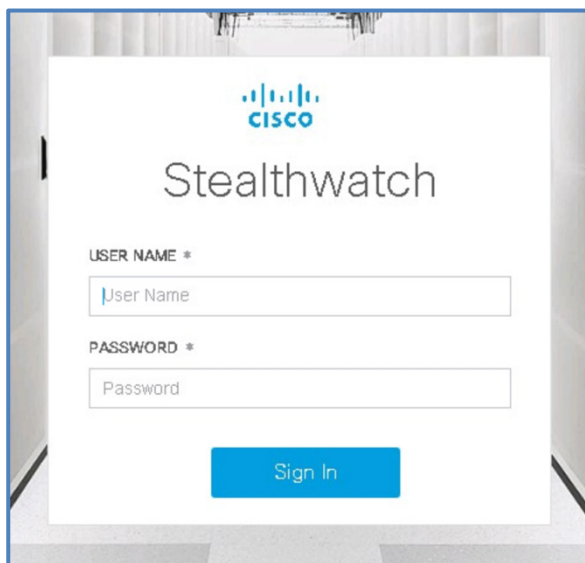
Hide advanced Back to safety

This server could not prove that it is **198.19.20.136**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

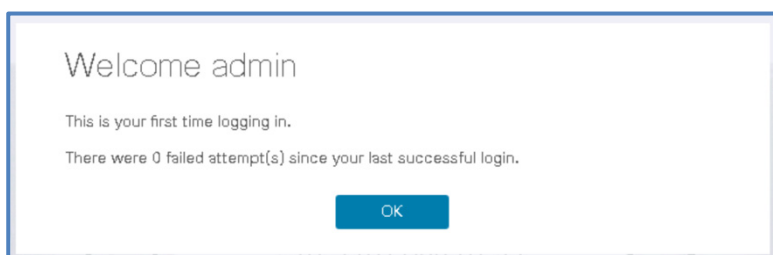
[Proceed to 198.19.20.136 \(unsafe\)](#)

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。[サインイン (Sign In)] をクリックして続行します。

- [ユーザ名 (User Name)] : **admin**
- [パスワード (Password)] : **lan411cope**



5. [ようこそ、admin (Welcome admin)] ページが表示されたら、[OK] をクリックします。



6. AST のウェルカムページが表示されます。[続行 (Continue)] をクリックして先に進みます。



7. [デフォルトパスワードの変更 (Change Default Password)] 画面が表示されます。7.x では、admin、root、および sysadmin のデフォルトパスワードを変更するように求められます。次の手順を完了する際には、各アカウントの現在のパスワードに注意してください。読み込みが完了するまでに数秒かかる場合があります。



The screenshot shows the 'Stealthwatch Management Console VE' Appliance Setup interface. The main heading is 'Change Default Passwords'. On the left, there is a vertical navigation pane with five steps: Step 1 (Change Default Password, highlighted in orange), Step 2 (Management Network Interface), Step 3 (Host Name and Domains), Step 4 (DNS Settings), and Step 5 (NTP Settings). Below these is a 'Review' section for 'Review Your Settings'. The main content area displays the 'Password Format (Case Sensitive)' requirements: must be between 8 and 30 characters, must be different from the previous password by at least 4 characters, and must not be the same as the previous 1 password(s). A note states: 'Note: You must change the password for all the users before continuing.' Below the note are three radio buttons for user selection: ADMIN (selected), ROOT, and SYSADMIN. Underneath are three password input fields: 'Current Password' (with placeholder 'current admin password'), 'New Password' (with placeholder 'new admin password'), and 'Confirm New Password' (with placeholder 'confirm new admin password'). Each field has a 'Required' label. A 'Next' button is located at the bottom right.

- **ADMIN** がすでに選択されています。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan411cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
 - **ROOT** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
 - **SYSADMIN** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
8. [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ため、変更を加える必要はありません。[次へ (Next)] をクリックして続行します。



Stealthwatch Management Console VE
Appliance Setup
Serial Number: SMCVE-VMware-42383d585e9c2d2-df3bb293c96d4dd6
Version: 7.1.2
Build: 2019.10.28.2033-0

Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Review: Review Your Settings

Management Network Interface

Enable communication between this appliance and the network. Default network settings for this appliance appear below. Before changing any of these settings, confer with your network administrator.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

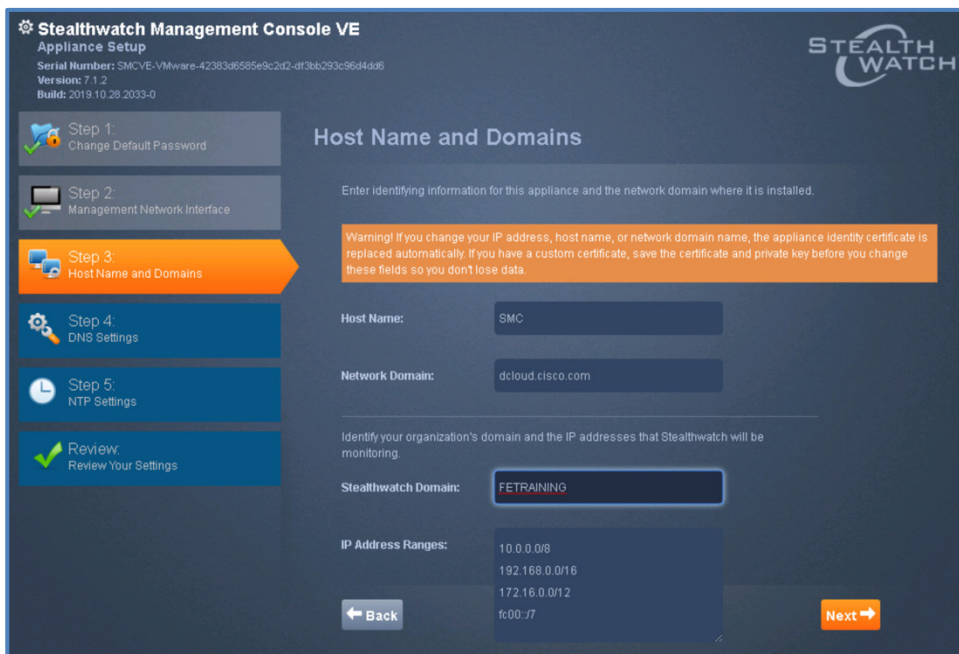
Interface Name: eth0 Interface MAC Address: 00:50:56:b8:6f:5b

	IPv4	IPv6
IP Address:	198.19.20.136	
Subnet Mask:	255.255.255.0	
Default Gateway:	198.19.20.1	
Broadcast Address:	198.19.20.255	

Next →

9. [ホスト名とドメイン (Host Name and Domain)]画面が表示されます。次の値を入力し、[次へ (Next)]をクリックします。

- [ホスト名 (Host Name)] : **SMC**
- [ネットワークドメイン (Network Domain)] : **dcloud.cisco.com**
- [Stealthwatch ドメイン (Stealthwatch Domain)] : **FETRAINING**
- [IP アドレスの範囲 (IP Address Ranges)] : ここではデフォルトのままにします



Stealthwatch Management Console VE
Appliance Setup
Serial Number: SMCVE-VMware-42383d585e9c2d2-df3bb293c96d4dd6
Version: 7.1.2
Build: 2019.10.28.2033-0

Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Review: Review Your Settings

Host Name and Domains

Enter identifying information for this appliance and the network domain where it is installed.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Host Name: SMC

Network Domain: dcloud.cisco.com

Identify your organization's domain and the IP addresses that Stealthwatch will be monitoring.

Stealthwatch Domain: FETRAINING

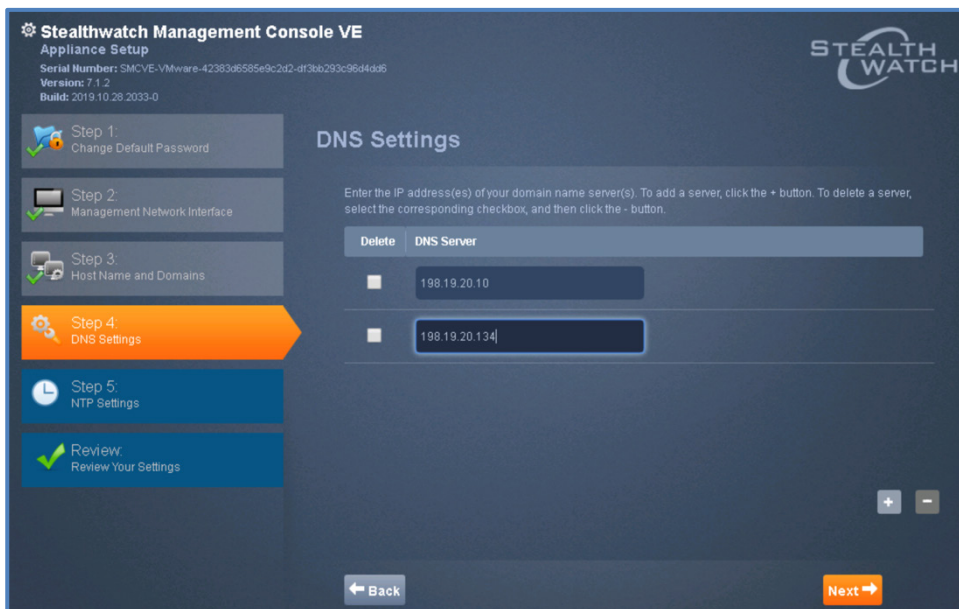
IP Address Ranges:
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
fc00::/7

← Back Next →

10. [DNS 設定 (DNS Settings)] 画面が表示されます。必要な DNS サーバを環境に追加します。

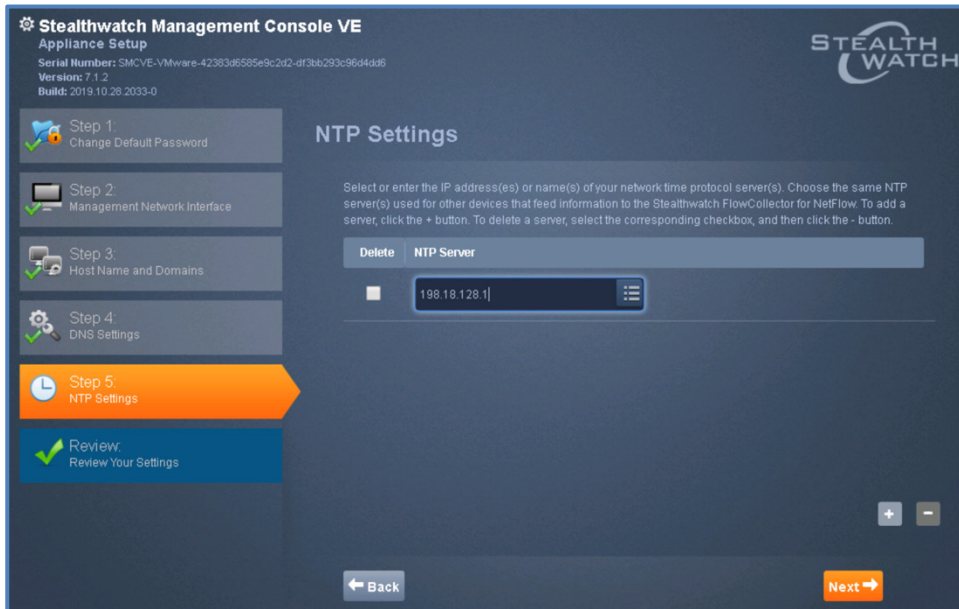
注：dCloud で使用する IP アドレス方式には細心の注意を払ってください。192.x ではなく、198.x です。

- 1 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. 198.19.20.10 を入力します。
- 2 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. 198.19.20.134 を入力します。
- 両方の DNS エントリが表示されたら、[次へ (Next)] 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。環境に適した NTP 設定を入力します。

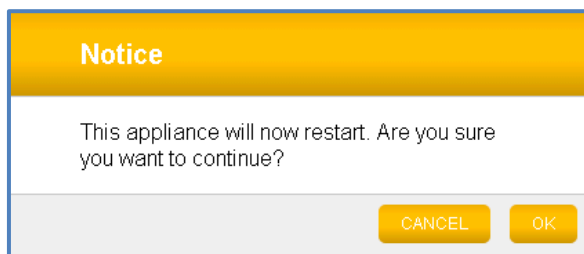
- 全部で3つあるデフォルトの NTP エントリの前にある [削除 (Delete)] チェックボックスをすべてオンにし、[-] ボタンをクリックします。
 - i. すべてのエントリが削除されます。
- [+] ボタンをクリックします。
 - i. 新しい NTP エントリフィールドに **198.18.128.1** と入力します。
 - ii. エントリが 198.18.128.1 のみになります。
- 残っている NTP エントリが 1 つのみであることを確認し、[次へ (Next)] をクリックします。



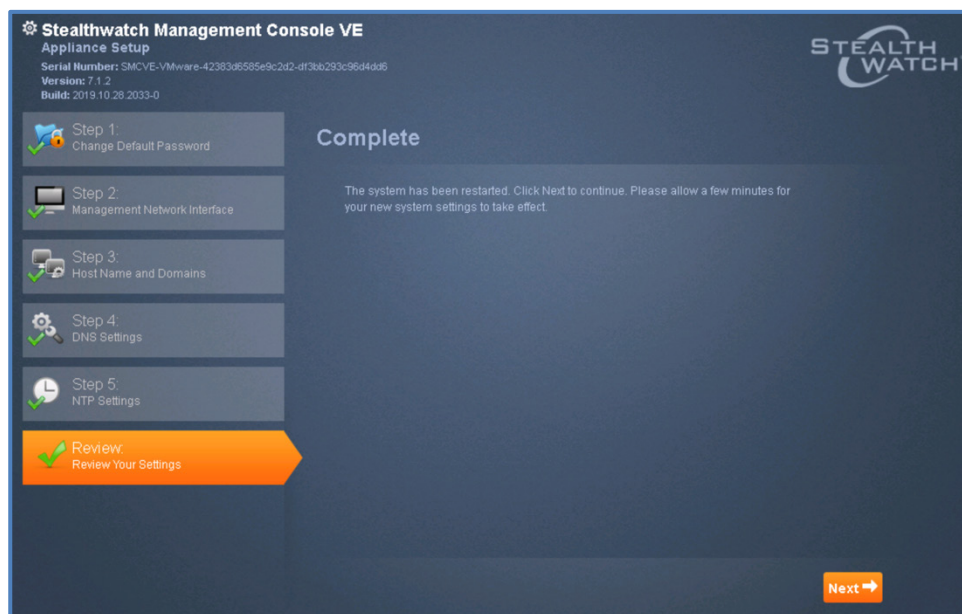
12. [設定の確認 (Review Your Settings)] 画面が表示されます。アプライアンスに設定を適用する前に値を編集する必要がある場合は、ここで行うことができます。ここでは変更は必要ありません。[確定 (Finalize)] が [再起動 (Restart)] に設定されていることを確認し、[適用 (Apply)] をクリックします。



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] をクリックして再起動を確定します。



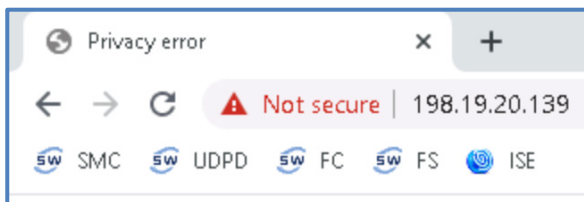
14. 数分以内に、[完了 (Complete)] 画面が表示されます。[次へ (Next)] をクリックします。



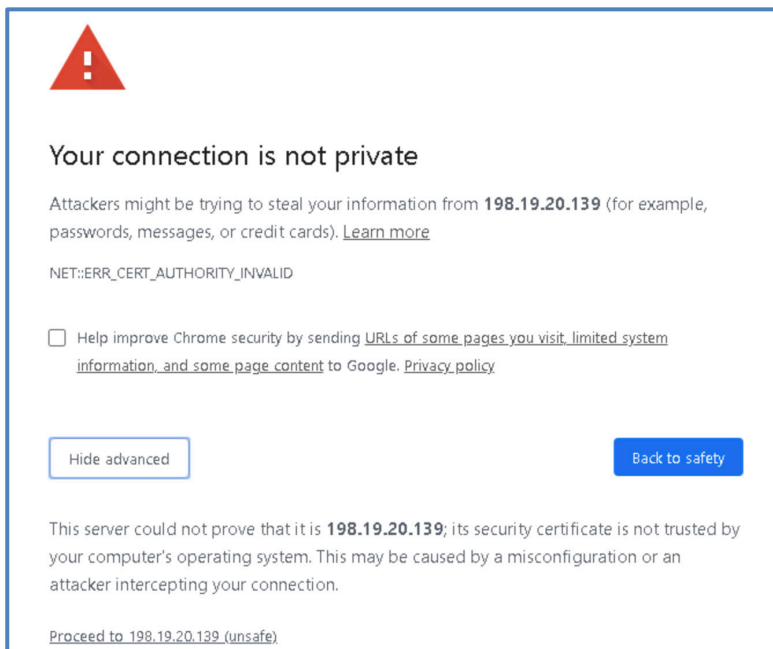
15. SMC が再起動とスタートアップのシーケンスを完了する間に、別のアプライアンスの設定手順を進めることができます。

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. Chrome のブックマークで **UDPD** を選択し、UDP Director 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 アプライアンスのデフォルトでは、信頼されていない自己署名証明書が使用されるため、ブラウザのセキュリティ警告が表示されます。Chrome でブラウザのセキュリティ警告が表示されたら、[詳細設定 (Advanced)] ボタンをクリックし、[- にアクセスする (安全ではありません) (Proceed ... (unsafe))] 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。



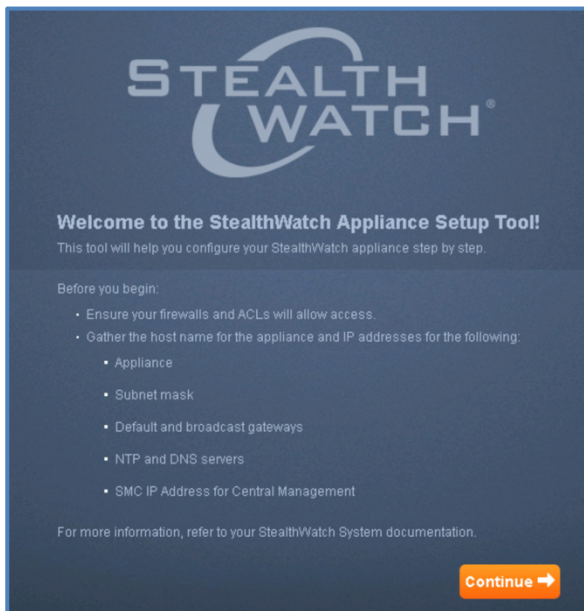
4. Stealthwatch のデフォルトのユーザ名 **admin** と、デフォルトのパスワード **lan411cope** を使用して、アプライアンスにログインします。
 - a. [ユーザ名 (Username)] : **admin**
 - b. [パスワード (Password)] : **lan411cope**



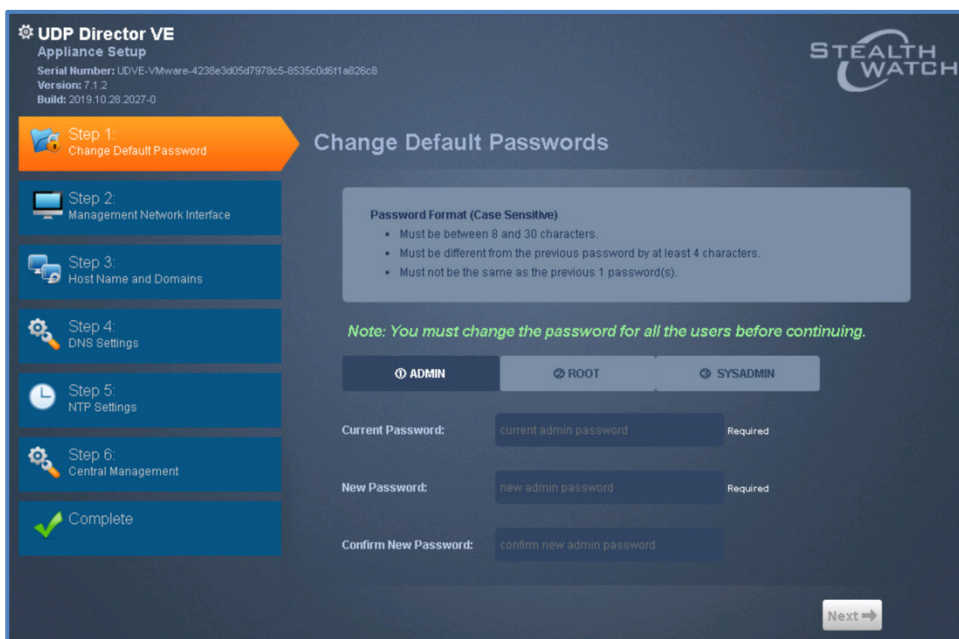
5. [ウェルカム (Welcome)] ポップアップページで [Ok] をクリックします。



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. [デフォルトパスワードの変更 (Change Default Password)]画面が表示されます。7.x では、続行する前に admin、root、および sysadmin のパスワードを設定する必要があります。次の設定手順では、デフォルトのパスワードが異なるため注意してください。

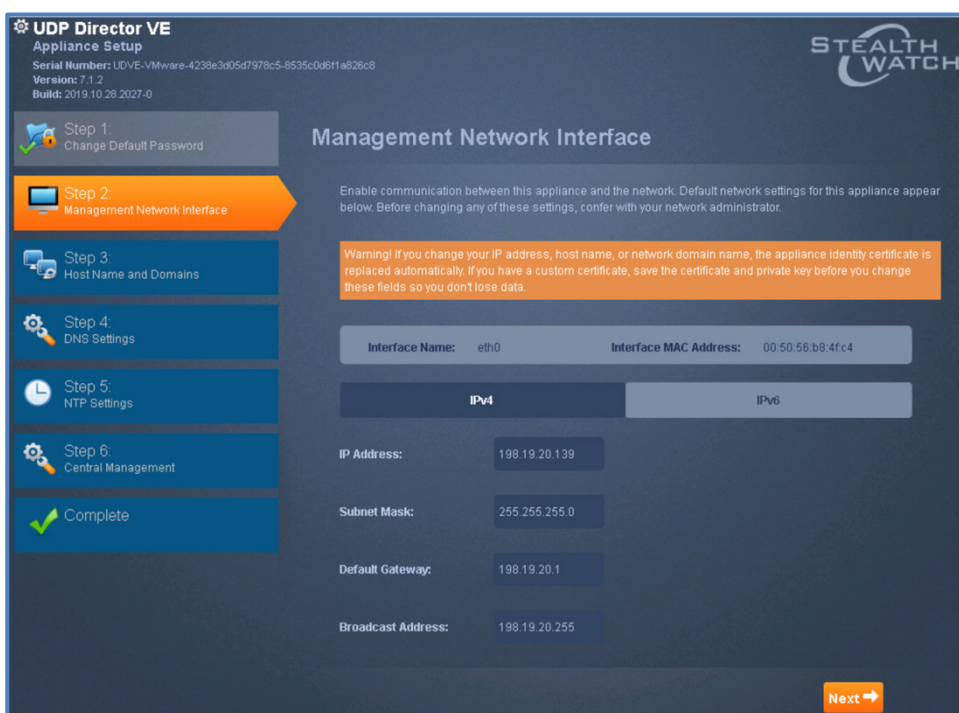


- a. **ADMIN** がすでに選択されています。次の情報を入力し、[次へ (Next)] をクリックします。
- [現在のパスワード (Current Password)] : **lan411cope**
 - [新しいパスワード (New Password)] : **C1sco12345**
 - [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
- b. **ROOT** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。

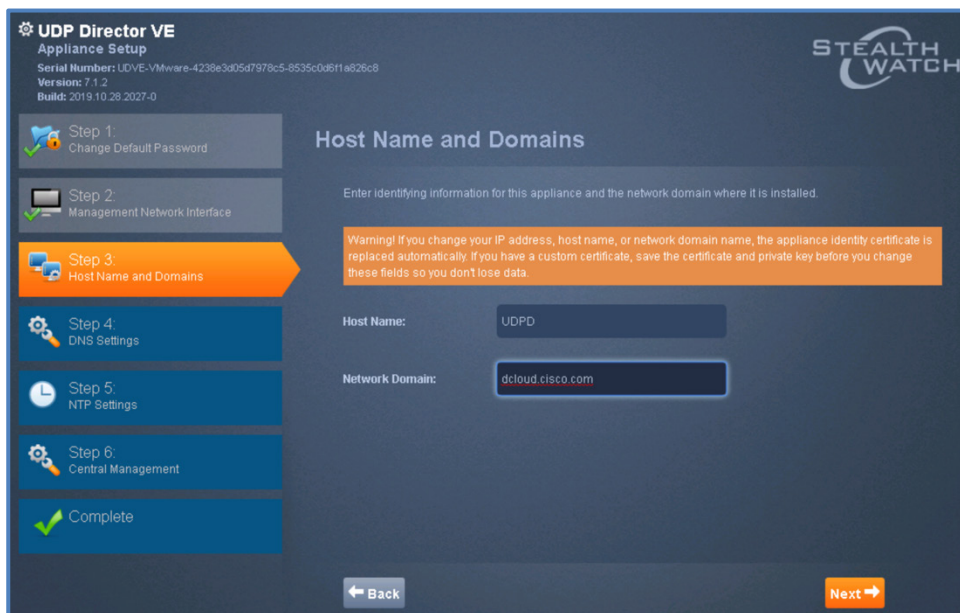
- i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
- c. **SYSADMIN** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。

- i. [現在のパスワード (Current Password)] : **lan1cope**
- ii. [新しいパスワード (New Password)] : **C1sco12345**
- iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**

8. [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ため、変更を加える必要はありません。[次へ (Next)] をクリックして続行します。



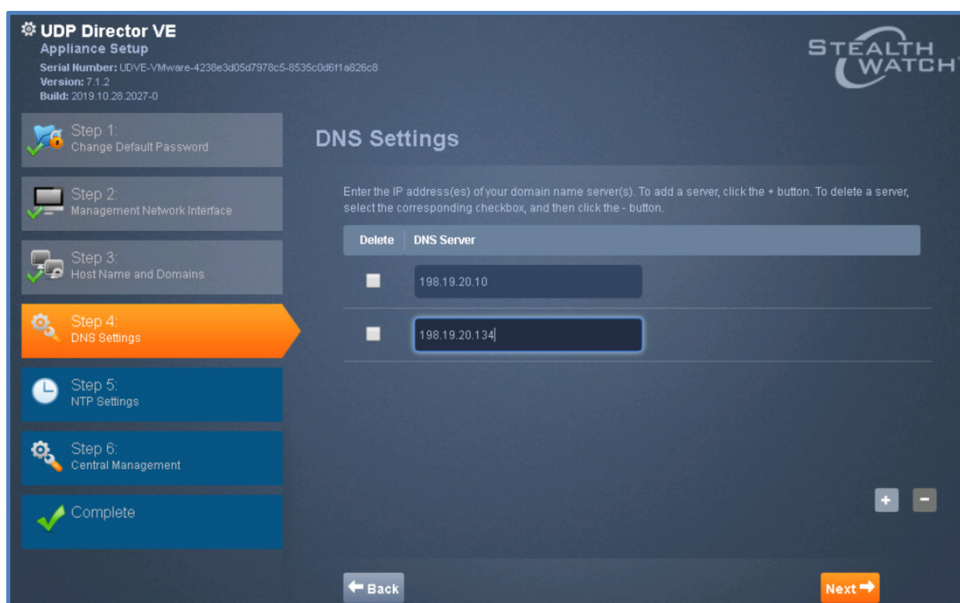
9. [ホスト名とドメイン (Host Name and Domain)] 画面が表示されます。次の値を入力し、[次へ (Next)] をクリックします。
- a. [ホスト名 (Host Name)] : **UDPD**
 - b. [ネットワークドメイン (Network Domain)] : **dcloud.cisco.com**



10. [DNS 設定 (DNS Settings)] 画面が表示されます。必要な DNS サーバを環境に追加します。

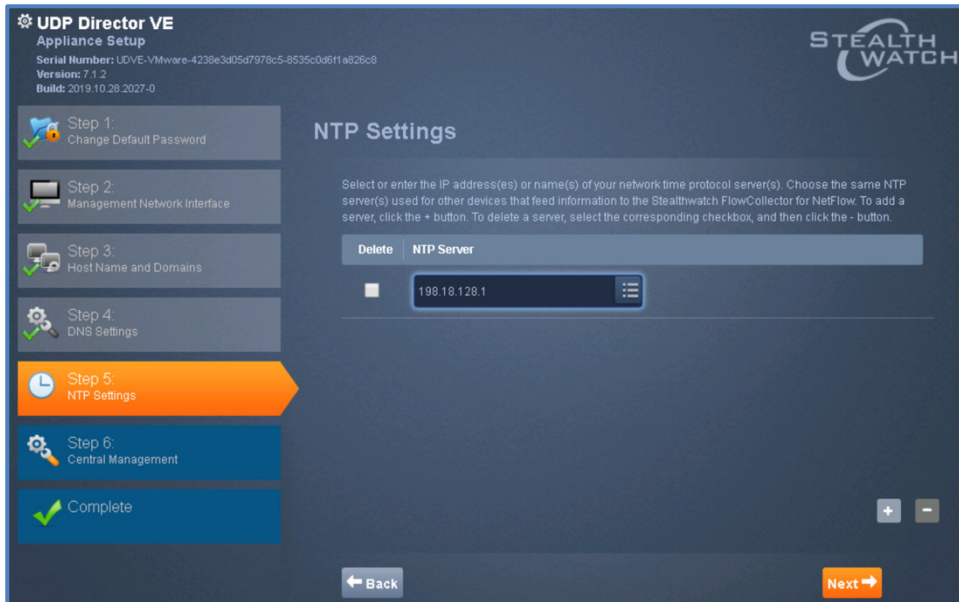
注：dCloud で使用する IP アドレス方式には細心の注意を払ってください。192.x ではなく、198.x です。

- 1 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.10** を入力します。
- 2 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.134** を入力します。
- 両方の DNS エントリが表示されたら、[次へ (Next)] をクリックして続行します。

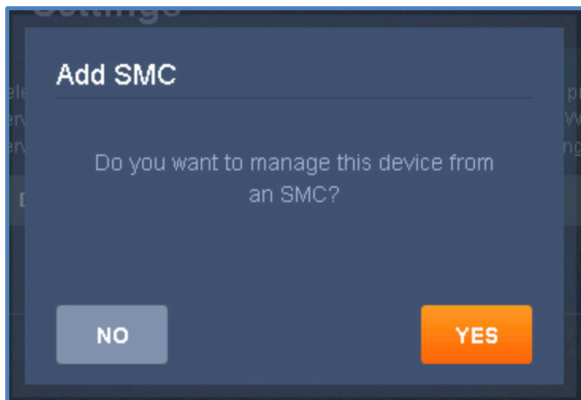


11. [NTP 設定 (NTP Settings)] 画面が表示されます。環境に適した NTP 設定を入力します。

- a. 全部で 3 つあるデフォルトの NTP エントリの前にある [削除 (Delete)] チェックボックスをすべてオンにし、[-] ボタンをクリックします。
 - i. すべてのエントリが削除されます。
- b. [+] ボタンをクリックします。
 - ii. 新しい NTP エントリフィールドに **198.18.128.1** と入力します。
 - iii. エントリが 198.18.128.1 のみになります。
- c. 残っている NTP エントリが 1 つのみであることを確認し、[次へ (Next)] をクリックします。

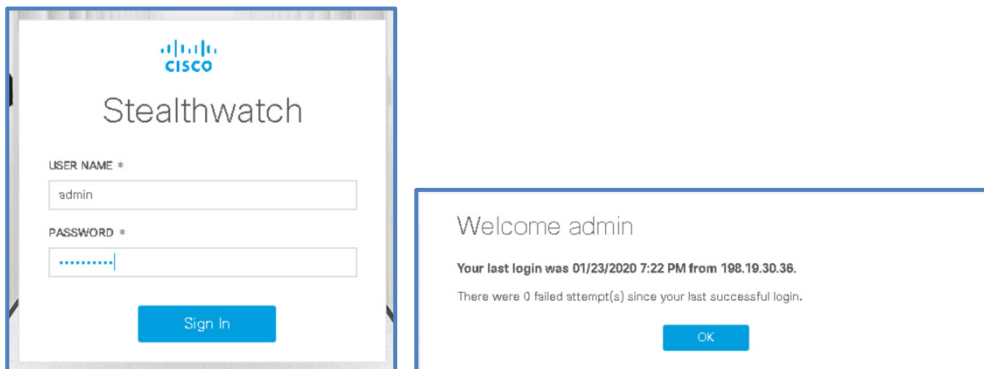


12. [SMC の追加 (Add SMC)] 画面が表示されます。 ボタンをまだクリックしないでください。 その前に SMC の再起動のステータスを確認する必要があります。

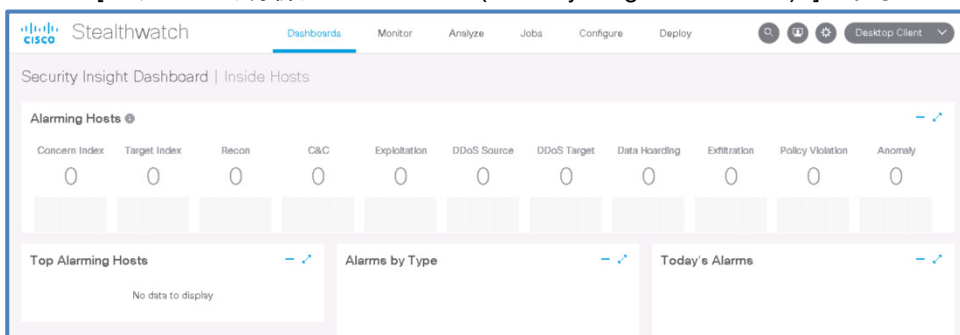


13. Chrome 内の [SMC] タブまたはウィンドウに戻り、ブラウザを**更新**します。
 - a. サイトが表示されない場合、まだ再起動中です。もう 1 分待ってから、再度更新してください。証明書の警告が表示されるまで、必要に応じて更新を繰り返します。
 - b. 証明書に関する警告が表示されたら、[詳細設定 (Advanced)] ボタンをクリックして、[~にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックします。

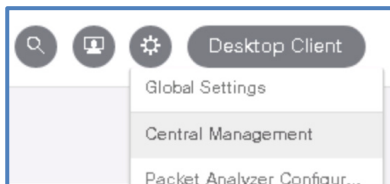
14. サーバの再起動後は、証明書の警告ページが表示され、それをクリックした後でも応答するのに少し時間がかかる場合があります。ログイン画面が表示されたら、新しいクレデンシャル：**admin** および **C1sco12345** を入力して [サインイン (Sign In)]、[OK] の順にクリックします。



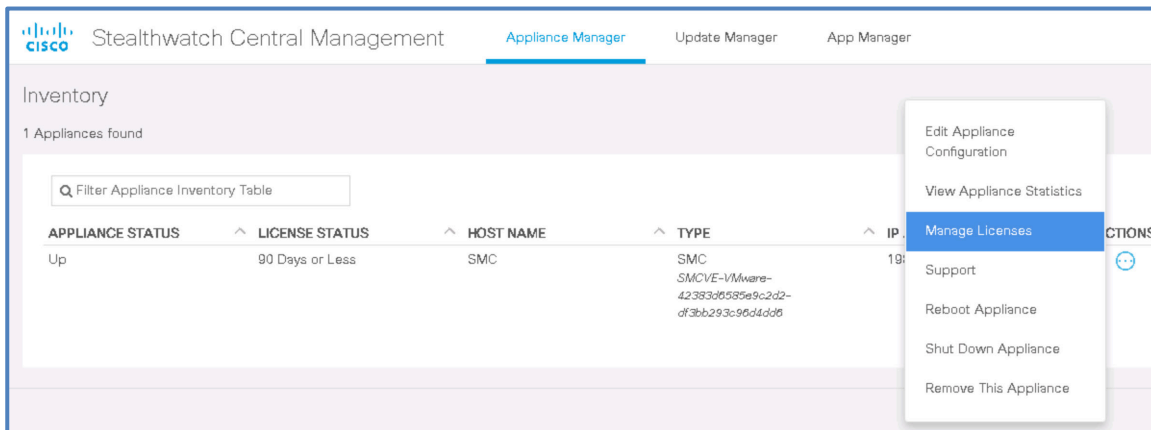
15. SMC の [セキュリティ分析ダッシュボード (Security Insight Dashboard)] が表示されます。



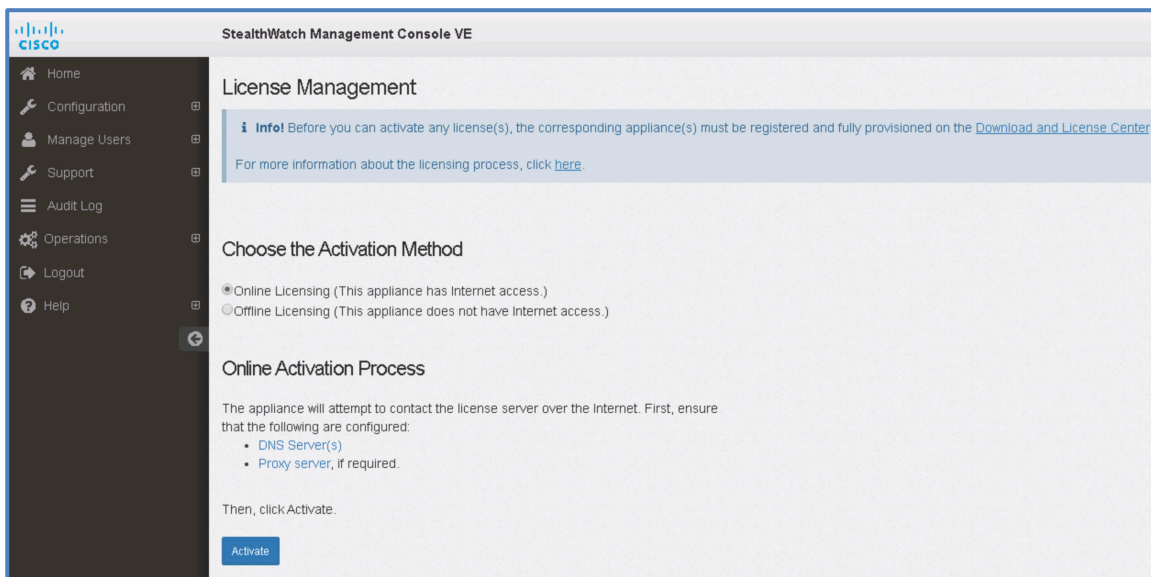
16. 右上隅の歯車アイコンをクリックし、メニューから [Central Management] を選択します。



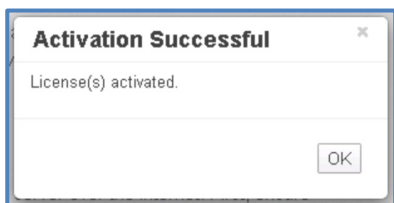
- a. SMC に関連付けられた [アクション (Actions)] アイコン ([インベントリ (Inventory)] の SMC エントリの右側) をクリックし、[ライセンスの管理 (Manage Licenses)] をクリックします。



- b. 有効化の方法として [オンラインライセンス (Online Licensing)] が設定されていることを確認してください。 [有効化 (Activate)] をクリックします。



- c. 有効化が完了したら、[OK] をクリックします。

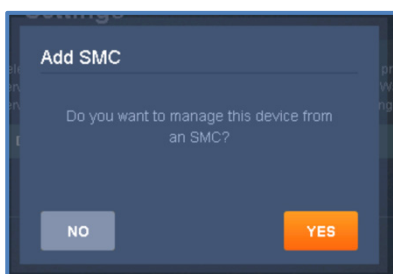


- d. 下にスクロールして、有効化されたライセンスを表示します。

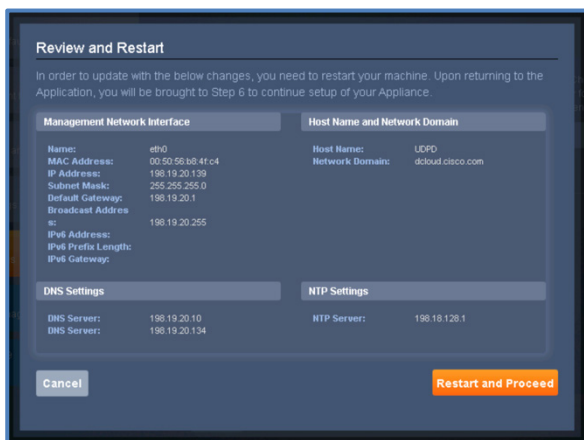
Feature	Count	Start Date	Expiration Date	Status
EndpointLicenseAgents	5000	Mar 04, 2019 UTC	Jul 16, 2022 UTC	Installed
FPS	5000	Mar 04, 2019 UTC	Jul 16, 2022 UTC	Installed
ISE	Uncounted	Mar 04, 2019 UTC	Never	Installed
ProxyWatch	50000	Mar 04, 2019 UTC	Never	Installed
SLIC	Uncounted	Mar 04, 2019 UTC	Jul 16, 2022 UTC	Installed
SMCBASE	Uncounted	Mar 04, 2019 UTC	Never	Installed
SMCRED	Uncounted	Mar 04, 2019 UTC	Never	Installed

e. [UDP] タブを開いたままにして、[SMC 管理 (SMC Administration)] タブと [Central Management] タブの両方を閉じます。

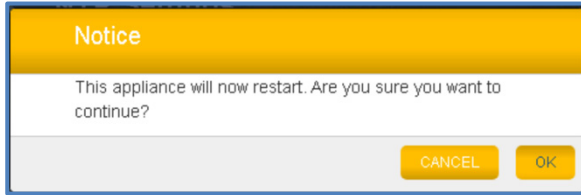
17. これで、Chrome の [UDP] 設定タブまたはウィンドウに戻ることができます。Chrome の [UDP] タブまたはウィンドウに戻り、[SMC の追加 (Add SMC)] 画面で [はい (Yes)] をクリックします。



18. [確認と再起動 (Review and Restart)] ページが表示されます。[再起動と続行 (Restart and Proceed)] をクリックします。

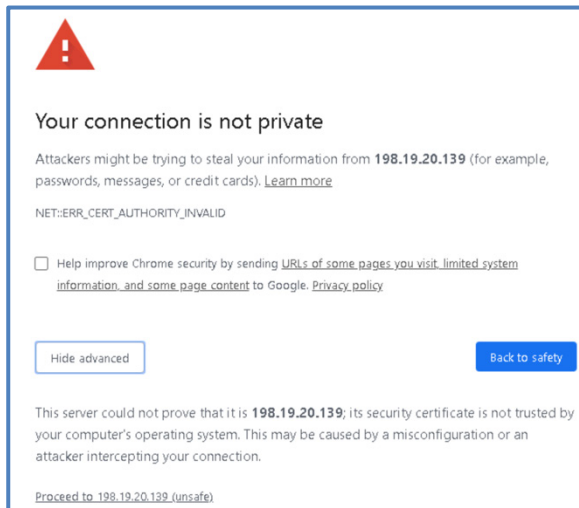


19. [OK] をクリックし、UDP Director の再起動を確定します。

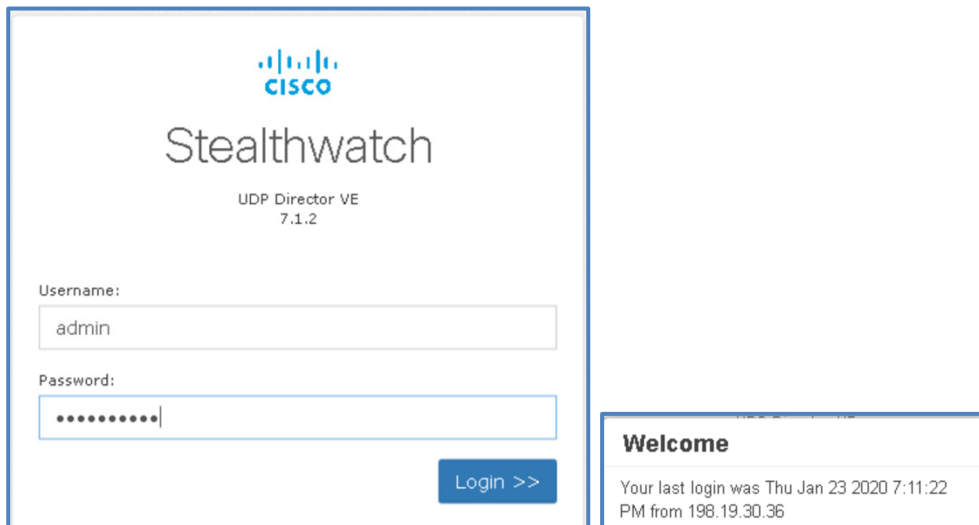


20. UDP Director が再起動する間、しばらくお待ちください。「処理中」というメッセージが表示され、その後「このサイトにアクセスできません」と表示されます。1 ~ 2分待ってから、Web ページのリロードを試みます。

- a. UDP Director 証明書の警告ページが表示されるまで、ページのリロードを続行します。[詳細設定 (Advanced)] ボタンをクリックし、[-にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックします。

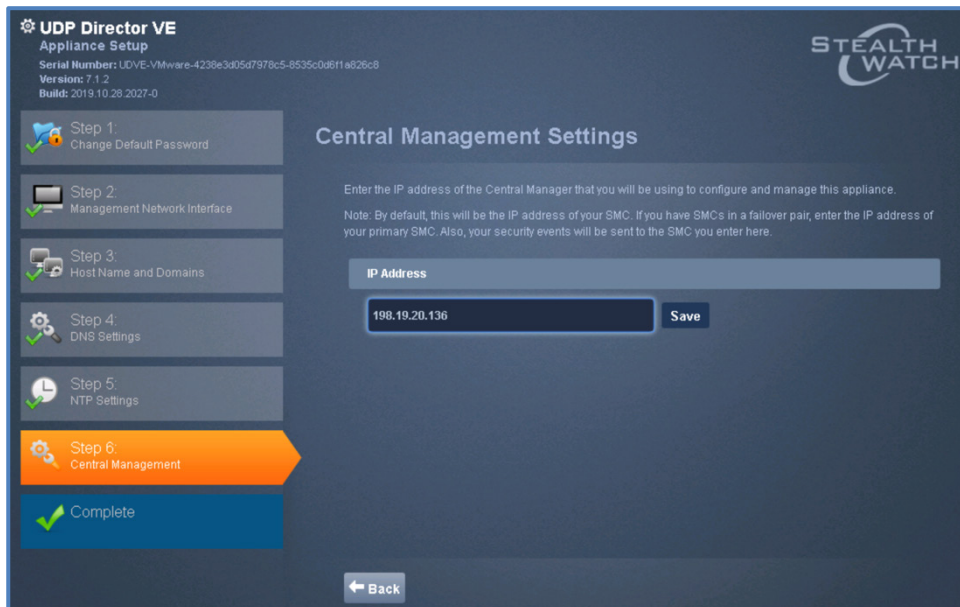


- b. UDP Director に **admin** および **C1sco12345** のクレデンシャルでログインします。次に、[ウェルカム (Welcome)] ページで [Ok] をクリックします。

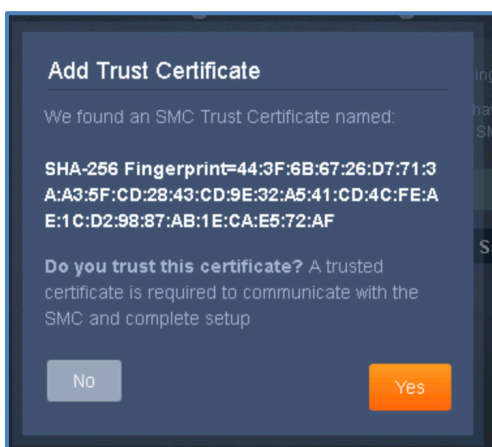


21. 最初に表示される AST のページで [続行 (Continue)] をクリックします。

22. [Central Management 設定 (Central Management Settings)] ページが表示されます。[IP アドレス (IP Address)] フィールドに **198.19.20.136** と入力し、[保存 (Save)] をクリックします。

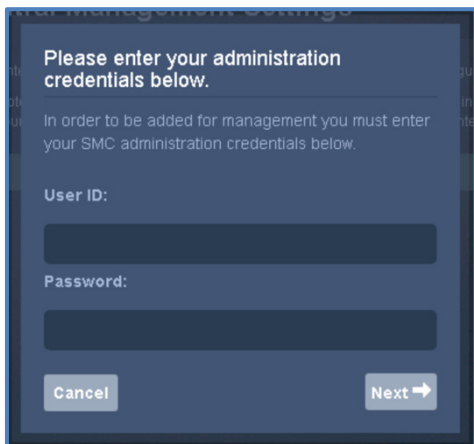


23. [信頼できる証明書の追加 (Add Trust Certificate)] ページが表示されます。[はい (Yes)] をクリックして SMC 証明書を信頼します。



24. SMC 管理者のクレデンシャルを入力するように求められます。入力したら [次へ (Next)] をクリックします。

- a. [ユーザ ID (User ID)] : **admin**
- b. [パスワード (Password)] : **C1sco12345**



Please enter your administration credentials below.

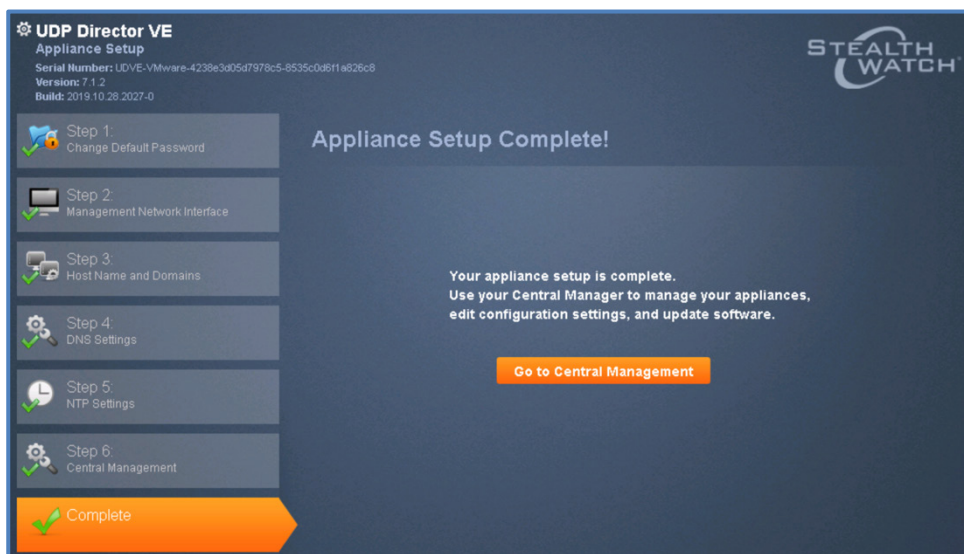
In order to be added for management you must enter your SMC administration credentials below.

User ID:

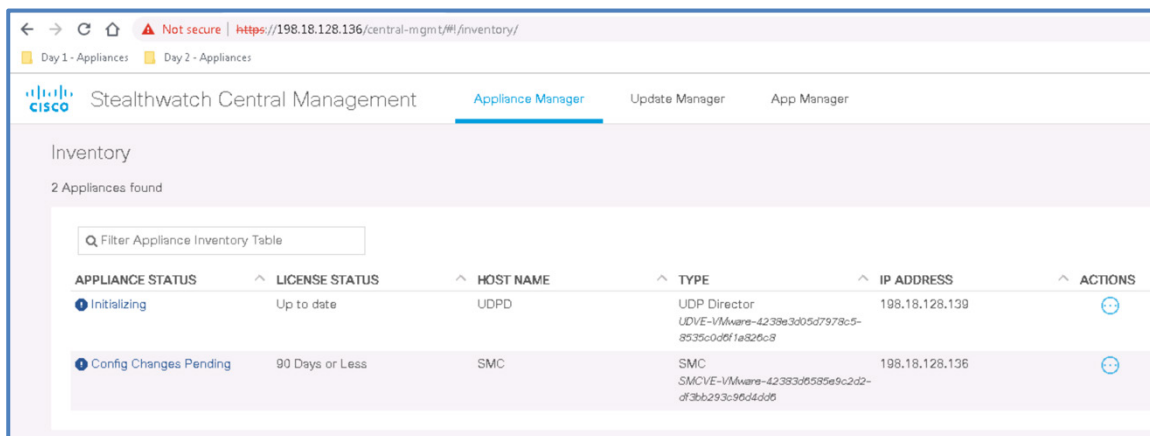
Password:

Cancel Next →

25. 最終的に [アプライアンスのセットアップの完了 (Appliance Setup Complete)] 画面が表示されます。しばらくお待ちください。UDP Director が設定プロセスを完了するまで数分かかる場合があります。設定プロセスが完了したら、[Central Management に移動 (Go to Central Management)] をクリックします。

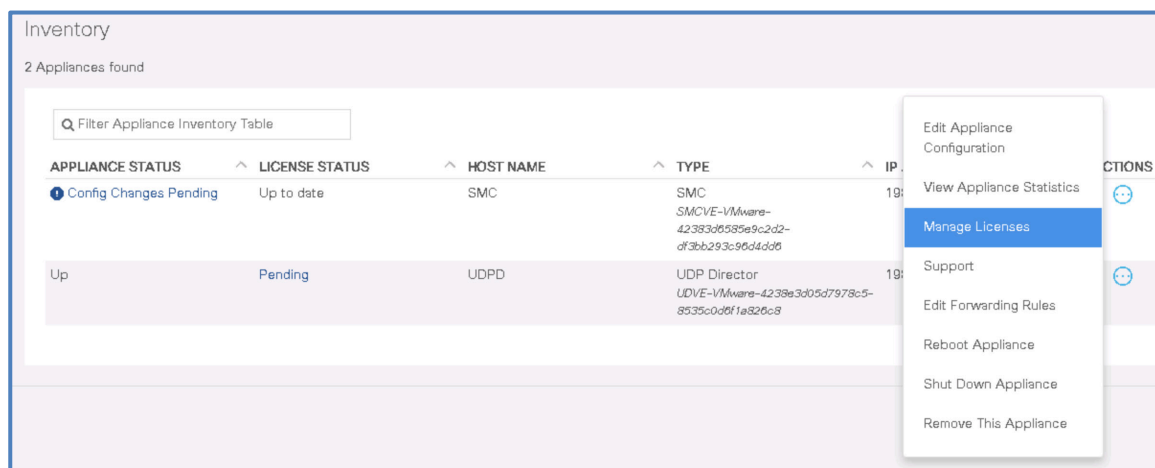


26. SMC の [Stealthwatch Central Management] ページにリダイレクトされます。UDP と SMC の両方のアプライアンスが表示されます。各アプライアンスの [アプライアンスのステータス (Appliance Status)] を確認します。

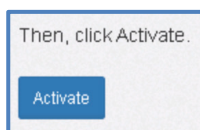


27. UDPD のアプライアンスのステータスが最終的に [Up] に変わったら次に進みます。

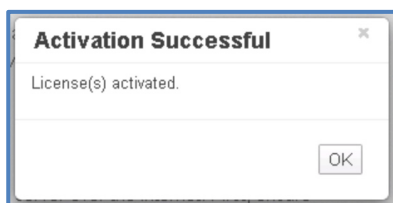
- a. UDPD に関連付けられた [アクション (Actions)] アイコン ([インベントリ (Inventory)] の UDPD エントリの右側) をクリックし、[ライセンスの管理 (Manage Licenses)] をクリックします。



- b. 有効化の方法として [オンラインライセンス (Online Licensing)] が設定されていることを確認してください。[有効化 (Activate)] をクリックします。



- c. 有効化が完了したら、[OK] をクリックします。



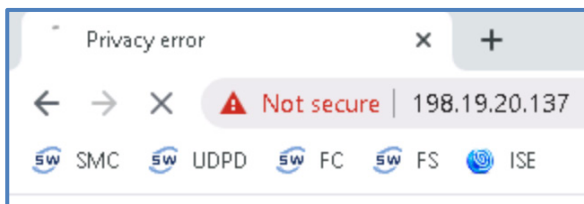
- d. 下にスクロールして、有効化されたライセンスを表示します。

Feature License Status				
Feature ▲	Count ◆	Start Date ◆	Expiration Date ◆	Status ◆
UDVE	Uncounted	Mar 04, 2019 UTC	Never	Installed

28. [UDPD 管理 (UDPD Administration)] タブを閉じ、このページで [Central Management] タブを開いたままにして、ラボの次のセクションに進みます。

フローコレクタ

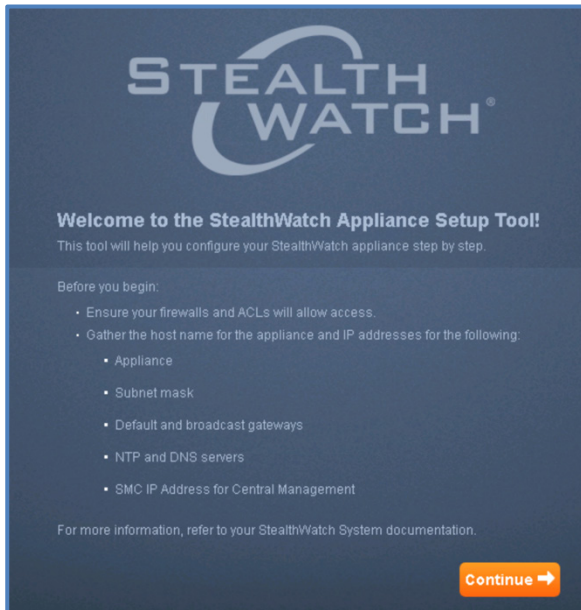
1. **Chrome** Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. Chrome のブックマークで **FC** を選択し、フローコレクタの Web 管理インターフェイスにアクセスします。



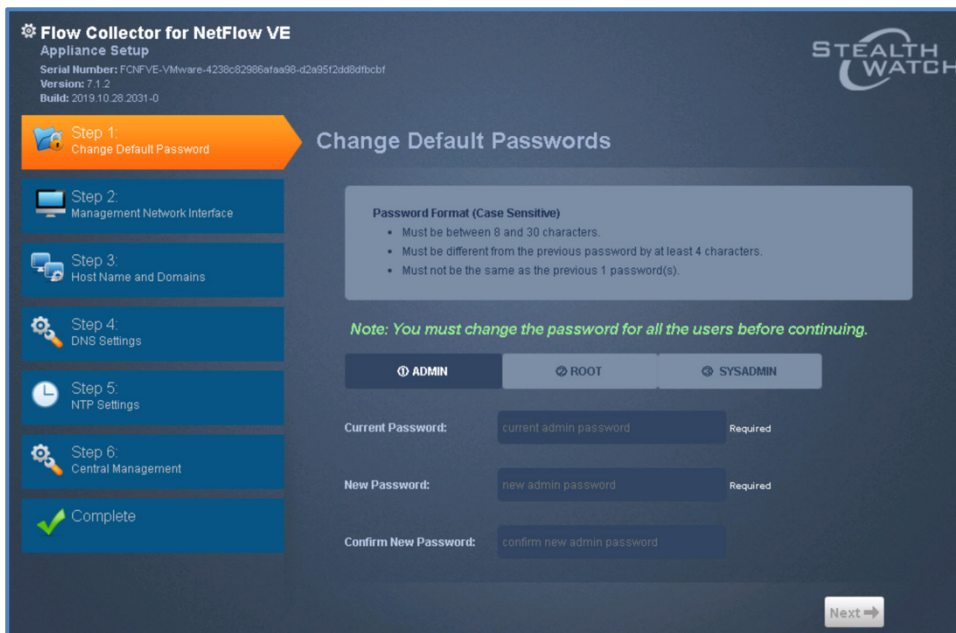
3. Stealthwatch アプライアンスのデフォルトでは、信頼されていない自己署名証明書が使用されるため、ブラウザのセキュリティ警告が表示されます。Chrome でブラウザのセキュリティ警告が表示されたら、[詳細設定 (Advanced)] ボタンをクリックし、[-にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックして、アプライアンス管理ページに進みます。
4. Stealthwatch のデフォルトのユーザ名 **admin** と、デフォルトのパスワード **lan411cope** を使用して、アプライアンスにログインします。
 - a. [ユーザ名 (Username)]: **admin**
 - b. [パスワード (Password)]: **lan411cope**



5. [ウェルカム (Welcome)] ポップアップで [Ok] をクリックします。
6. AST のウェルカムページが表示されます。[継続 (Continue)] をクリックします。



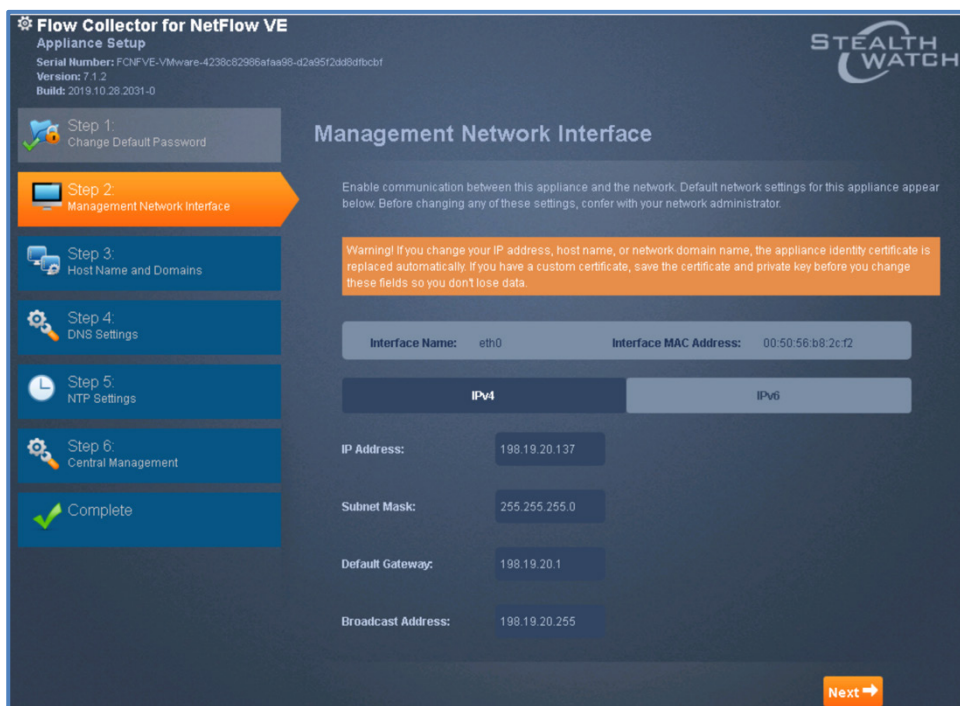
7. [デフォルトパスワードの変更 (Change Default Password)] 画面が表示されます。7.x では、続行する前に admin、root、および sysadmin のパスワードを設定する必要があります。次の設定手順では、デフォルトのパスワードが異なるため注意してください。



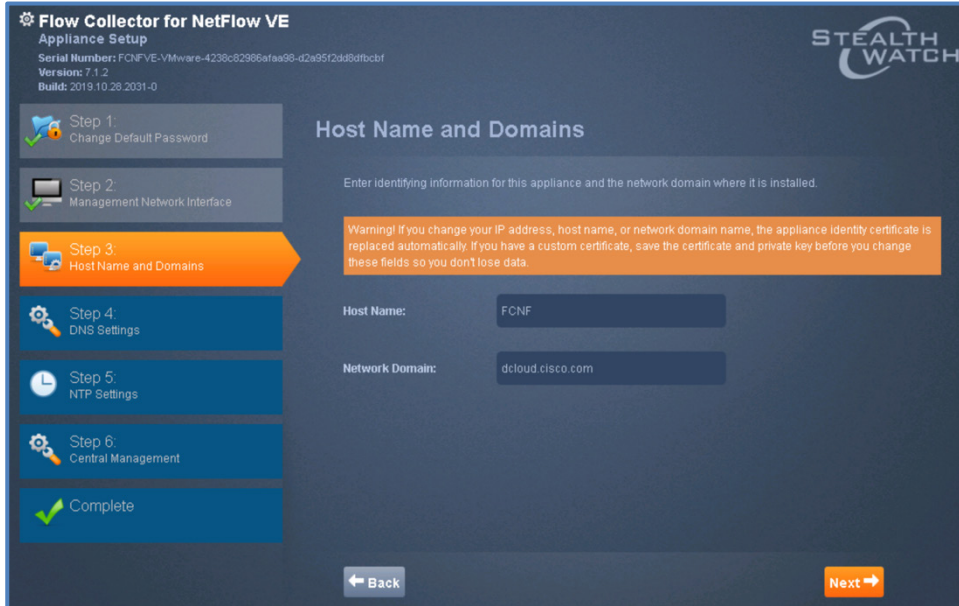
- a. **ADMIN** がすでに選択されています。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan411cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**

- b. **ROOT** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
- c. **SYSADMIN** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。
 - i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**

8. [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ため、変更を加える必要はありません。[次へ (Next)] をクリックして続行します。



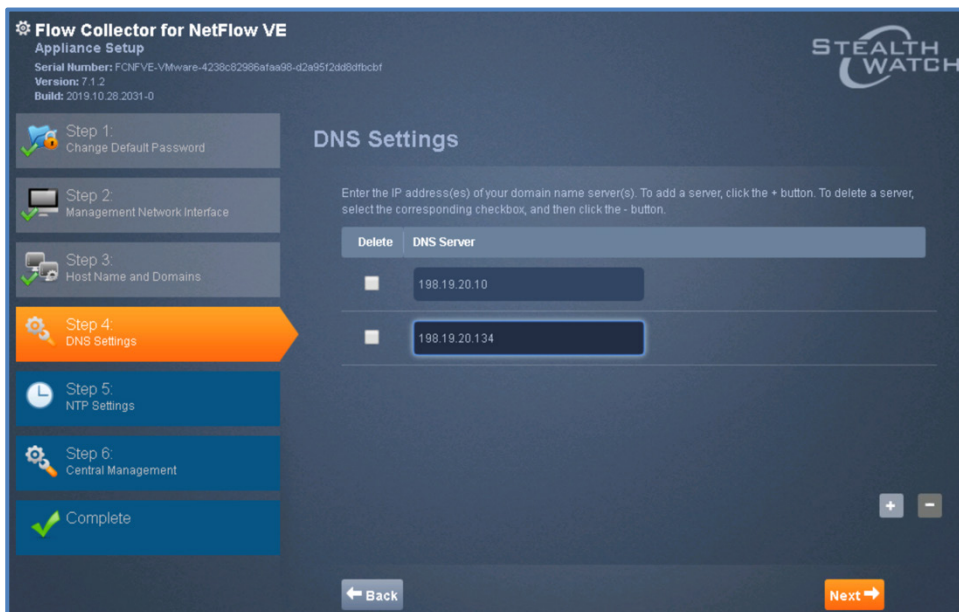
9. [ホスト名とドメイン (Host Name and Domain)] 画面が表示されます。次の情報を入力し、[次へ (Next)] をクリックします。
- a. [ホスト名 (Host Name)] : **FCNF**
 - b. [ネットワークドメイン (Network Domain)] : **dcloud.cisco.com**



10. [DNS 設定 (DNS Settings)] 画面が表示されます。必要な DNS サーバを環境に追加します。

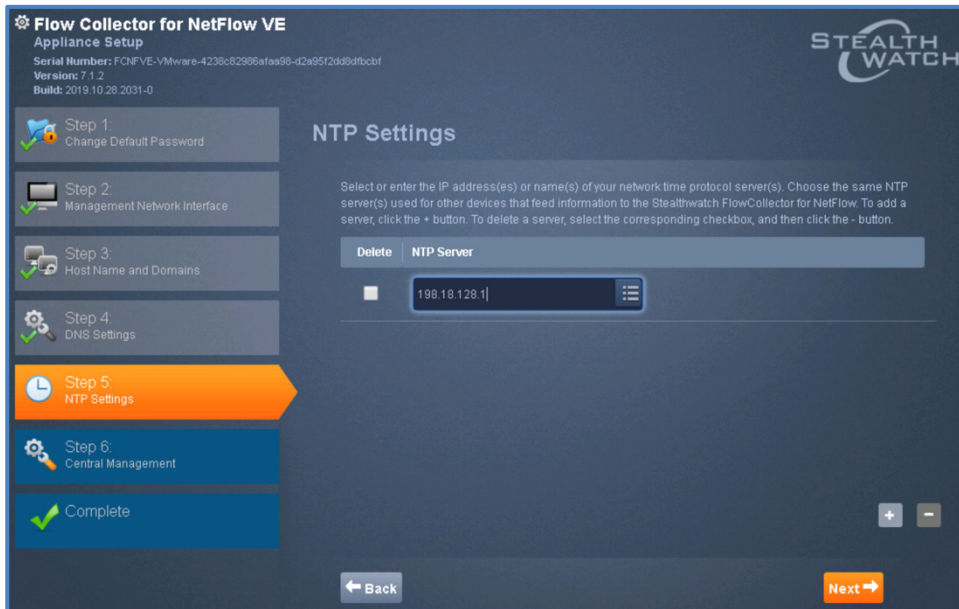
注：dCloud で使用する IP アドレス方式には細心の注意を払ってください。192.x ではなく、198.x です。

- a. 1 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.10** を入力します。
- b. 2 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.134** を入力します。
- c. 両方の DNS エントリが表示されたら、[次へ (Next)] をクリックして続行します。

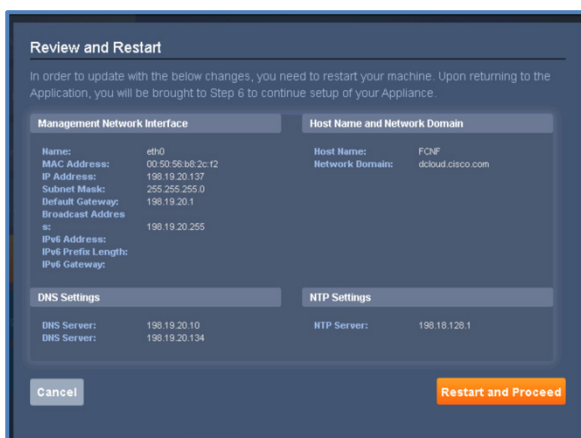


11. [NTP 設定 (NTP Settings)] 画面が表示されます。環境に適した NTP 設定を入力します。

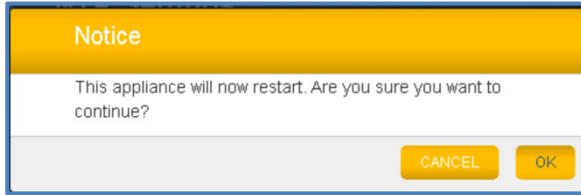
- a. 全部で3つあるデフォルトの NTP エントリの前にある [削除 (Delete)] チェックボックスをすべてオンにし、[-] ボタンをクリックします。
 - i. すべてのエントリが削除されます。
- b. [+] ボタンをクリックします。
 - i. 新しい NTP エントリフィールドに **198.18.128.1** と入力します。
 - ii. エントリが 198.18.128.1 のみになります。
- c. 残っている NTP エントリが 1 つのみであることを確認し、[次へ (Next)] をクリックします。



12. [確認と再起動 (Review and Restart)] ページが表示されます。[再起動と続行 (Restart and Proceed)] をクリックします。

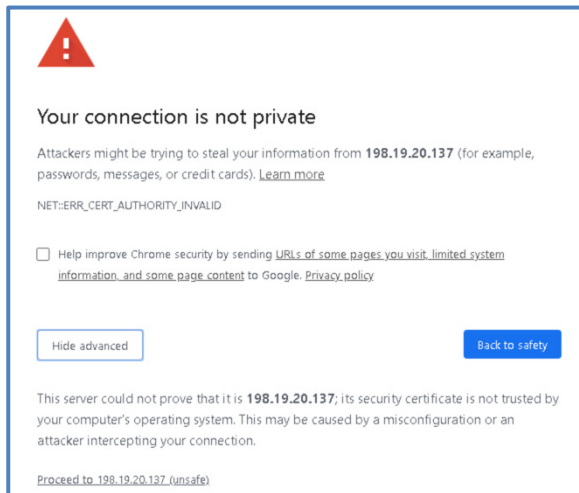


13. [OK] をクリックし、フローコレクタの再起動を確定します。

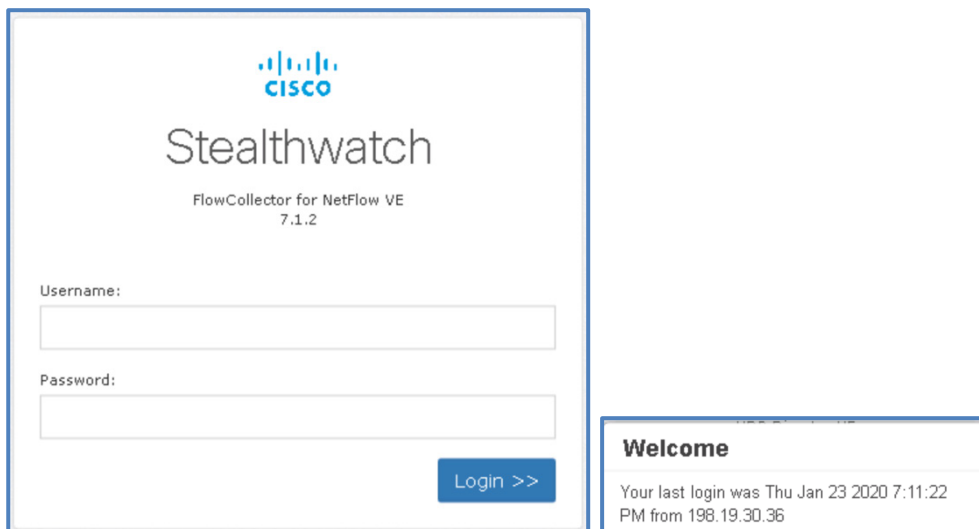


14. フローコレクタが再起動している間、しばらくお待ちください。「処理中」というメッセージが表示され、その後「このサイトにアクセスできません」と表示されます。1 ~ 2分待ってから、Web ページのリロードを試みます。

- a. フローコレクタ証明書の警告ページが表示されるまで、ページのリロードを続行します。[詳細設定 (Advanced)] ボタンをクリックし、[-にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックします。

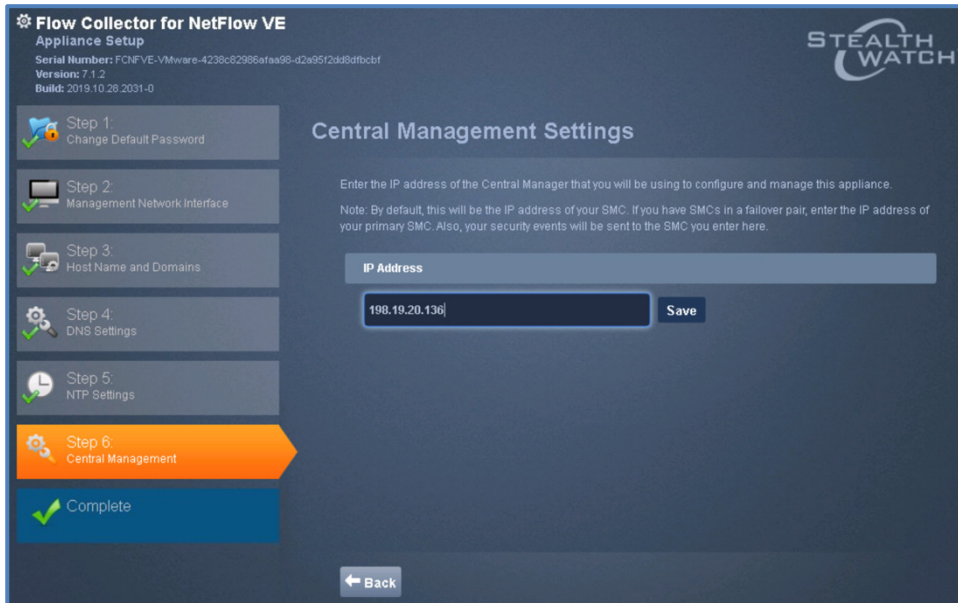


- b. フローコレクタに **admin** および **C1sco12345** のクレデンシャルでログインします。次に、[ウェルカム (Welcome)] ページで [Ok] をクリックします。

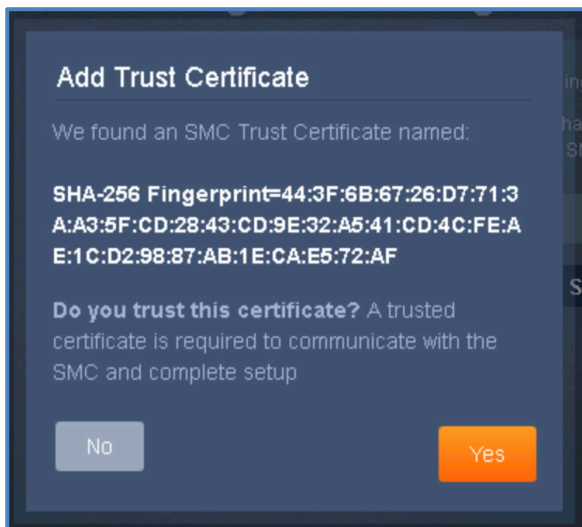


15. 表示される AST ページで [続行 (Continue)] をクリックします。

16. [Central Management 設定 (Central Management Settings)] ページが表示されます。[IP アドレス (IP Address)] フィールドに **198.19.20.136** と入力し、[保存 (Save)] をクリックします。

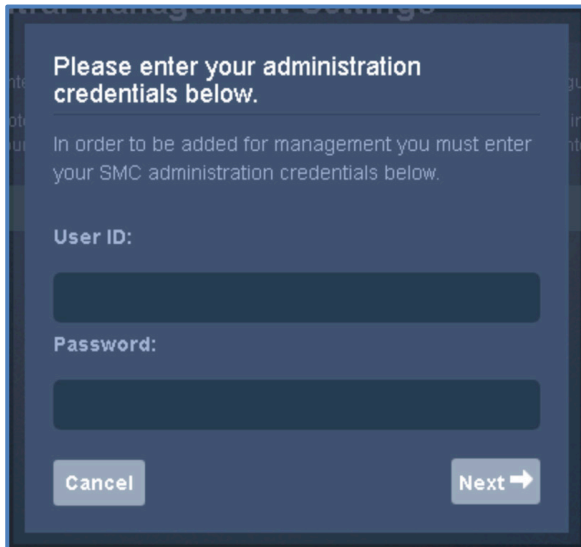


17. [信頼できる証明書の追加 (Add Trust Certificate)] ページが表示されます。[はい (Yes)] をクリックして SMC 証明書を信頼します。



18. SMC 管理者のクレデンシャルを入力するように求められます。入力したら [次へ (Next)] をクリックします。

- a. [ユーザ ID (User ID)] : **admin**
- b. [パスワード (Password)] : **C1sco12345**



Please enter your administration credentials below.

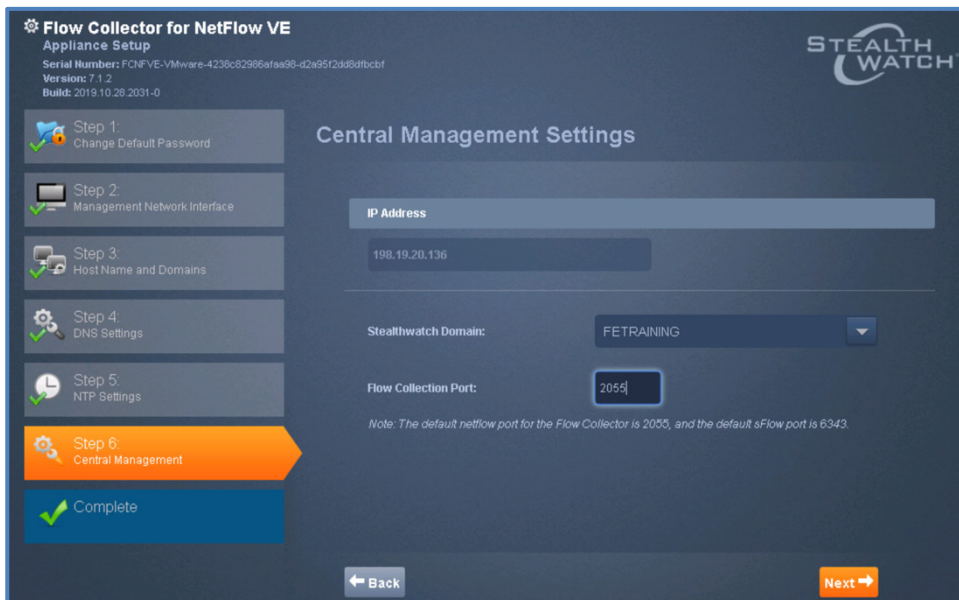
In order to be added for management you must enter your SMC administration credentials below.

User ID:

Password:

Cancel Next →

19. [Central Management 設定 (Central Management Settings)] ページが表示されます。次の設定を行い、[次へ (Next)] を押します。
 - a. [Stealthwatch ドメイン (Stealthwatch Domain)] ドロップダウンから [FETRAINING] を選択します。
 - b. [フローコレクションポート (Flow Collection Port)] に **2055** を入力します。



Flow Collector for NetFlow VE
Appliance Setup
Serial Number: FCMVE-VMware-4238c82986afaa98-d2a95f2d38dfcbf
Version: 7.1.2
Build: 2019.10.29.2031-0

STEALTHWATCH

Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Step 6: Central Management
Complete

Central Management Settings

IP Address: 198.19.20.136

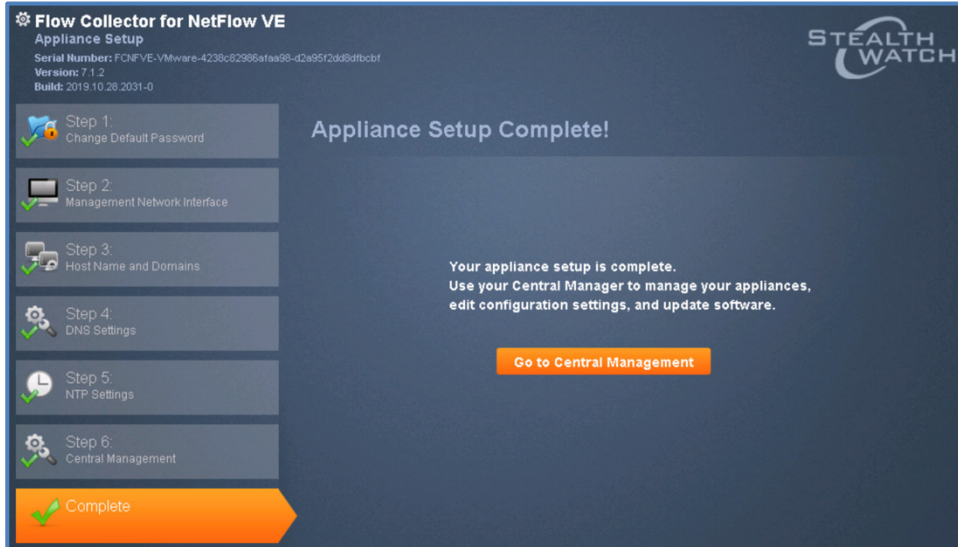
Stealthwatch Domain: FETRAINING

Flow Collection Port: 2055

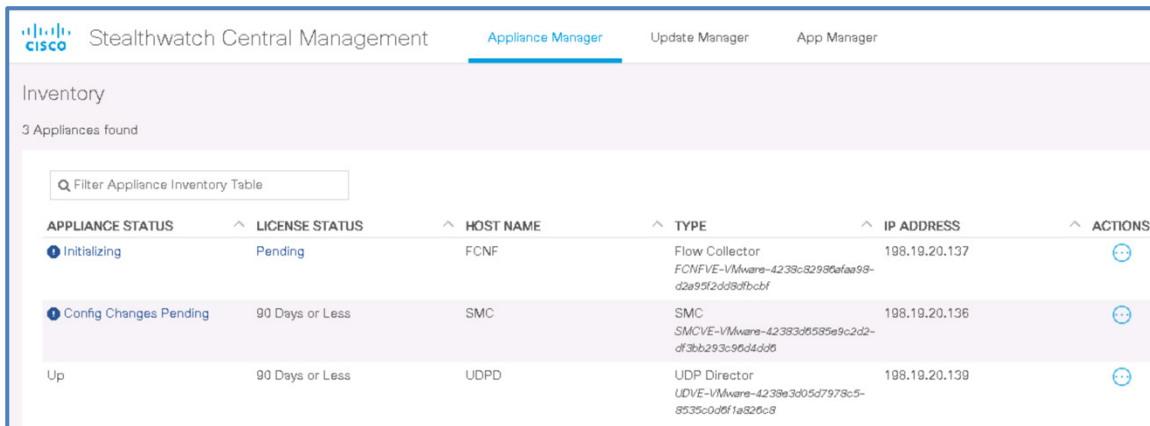
Note: The default netflow port for the Flow Collector is 2055, and the default sFlow port is 6343.

Back Next →

20. 最終的に [アプライアンスのセットアップの完了 (Appliance Setup Complete)] 画面が表示されます。[Central Management に移動 (Go to Central Management)] をクリックします。

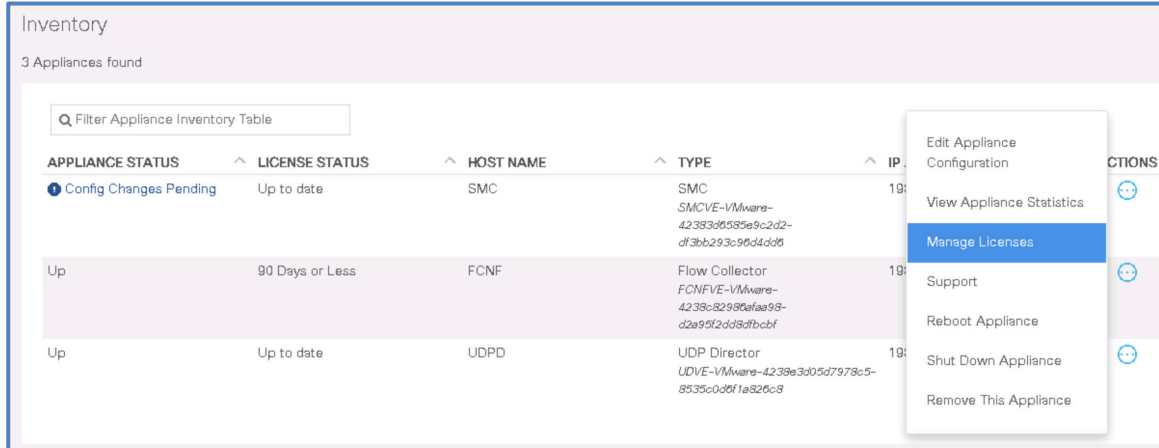


21. SMC の [Stealthwatch Central Management] ページにリダイレクトされます。現在設定されている 3 つの Stealthwatch アプライアンスがすべて表示されます。各アプライアンスの [アプライアンスのステータス (Appliance Status)] を確認します。

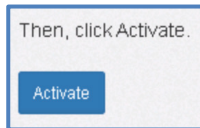


22. FCNF のアプライアンスのステータスが最終的に [Up] に変わったら次に進みます。

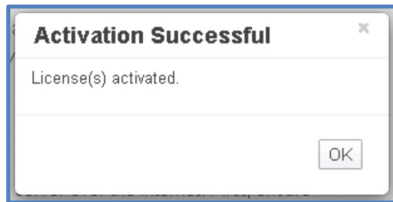
- a. FCNF に関連付けられた [アクション (Actions)] アイコン ([インベントリ (Inventory)] の FCNF エントリの右側) をクリックし、[ライセンスの管理 (Manage Licenses)] をクリックします。



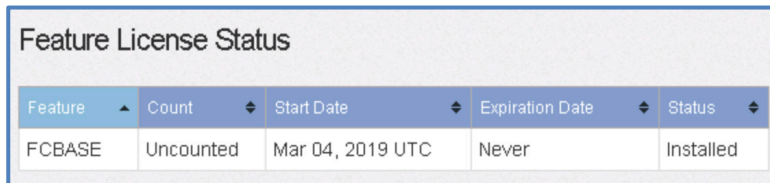
- b. 有効化の方法として [オンラインライセンス (Online Licensing)] が設定されていることを確認してください。[有効化 (Activate)] をクリックします。



- c. 有効化が完了したら、[OK] をクリックします。



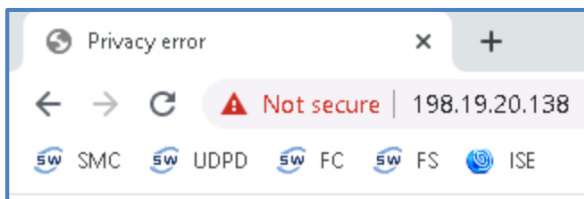
- d. 下にスクロールして、有効化されたライセンスを表示します。



23. [FCNF 管理 (FCNF Administration)] タブを閉じ、このページで [Central Management] タブを開いたままにして、ラボの次のセクションに進みます。

フローセンサー

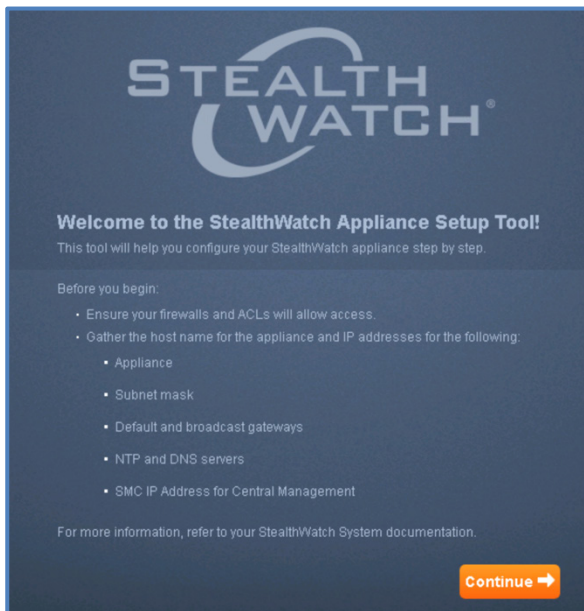
1. **Chrome** Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。
2. Chrome のブックマークで **FS** を選択し、フローセンサーの Web 管理インターフェイスにアクセスします。



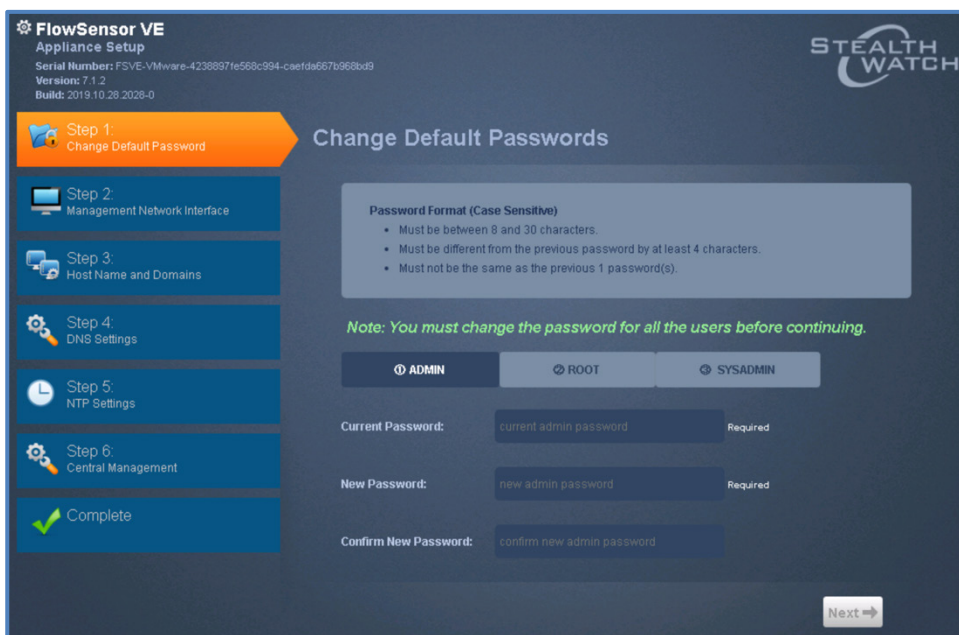
3. Stealthwatch アプライアンスのデフォルトでは、信頼されていない自己署名証明書が使用されるため、ブラウザのセキュリティ警告が表示されます。Chrome でブラウザのセキュリティ警告が表示されたら、[詳細設定 (Advanced)] ボタンをクリックし、[-]にアクセスする (安全ではありません) (Proceed ... (unsafe))]リンクをクリックして、アプライアンス管理ページに進みます。
4. Stealthwatch のデフォルトのユーザ名 **admin** と、デフォルトのパスワード **lan411cope** を使用して、アプライアンスにログインします。
 - a. [ユーザ名 (Username)]: **admin**
 - b. [パスワード (Password)]: **lan411cope**



5. [ウェルカム (Welcome)] ポップアップで [Ok] をクリックします。
6. AST のウェルカムページが表示されます。[続行 (Continue)] をクリックして先に進みます。



7. [デフォルトパスワードの変更 (Change Default Password)]画面が表示されます。7.x では、続行する前に admin、root、および sysadmin のパスワードを設定する必要があります。次の設定手順では、デフォルトのパスワードが異なるため注意してください。

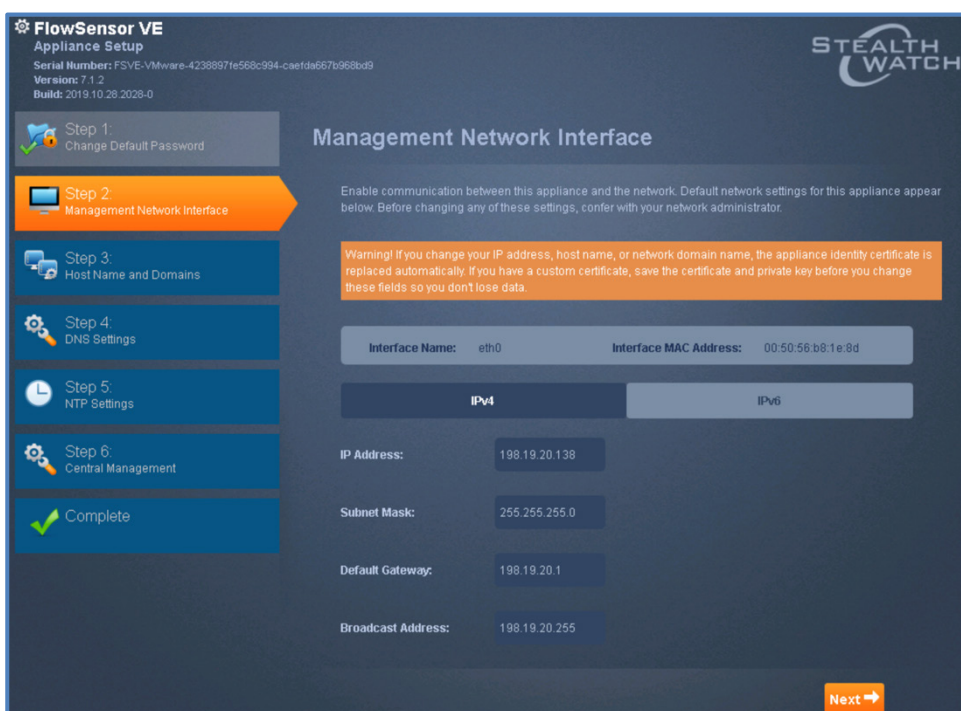


- a. **ADMIN** がすでに選択されています。次の情報を入力し、[次へ (Next)] をクリックします。
- [現在のパスワード (Current Password)] : **lan411cope**
 - [新しいパスワード (New Password)] : **C1sco12345**
 - [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
- b. **ROOT** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。

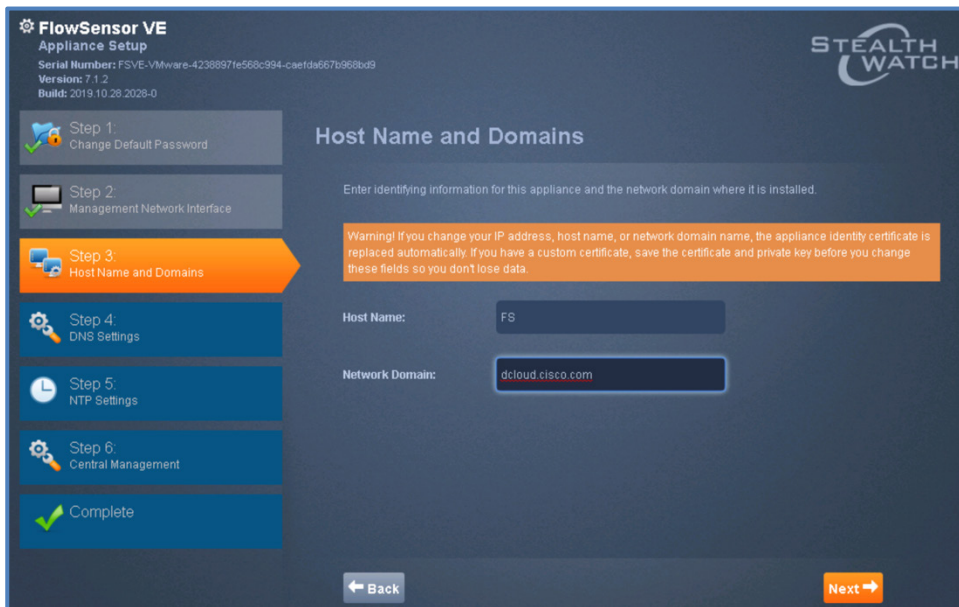
- i. [現在のパスワード (Current Password)] : **lan1cope**
 - ii. [新しいパスワード (New Password)] : **C1sco12345**
 - iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**
- c. **SYSADMIN** が選択されます。次の情報を入力し、[次へ (Next)] をクリックします。

- i. [現在のパスワード (Current Password)] : **lan1cope**
- ii. [新しいパスワード (New Password)] : **C1sco12345**
- iii. [新しいパスワードの確認 (Confirm New Password)] : **C1sco12345**

8. [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ため、変更を加える必要はありません。[次へ (Next)] をクリックして続行します。

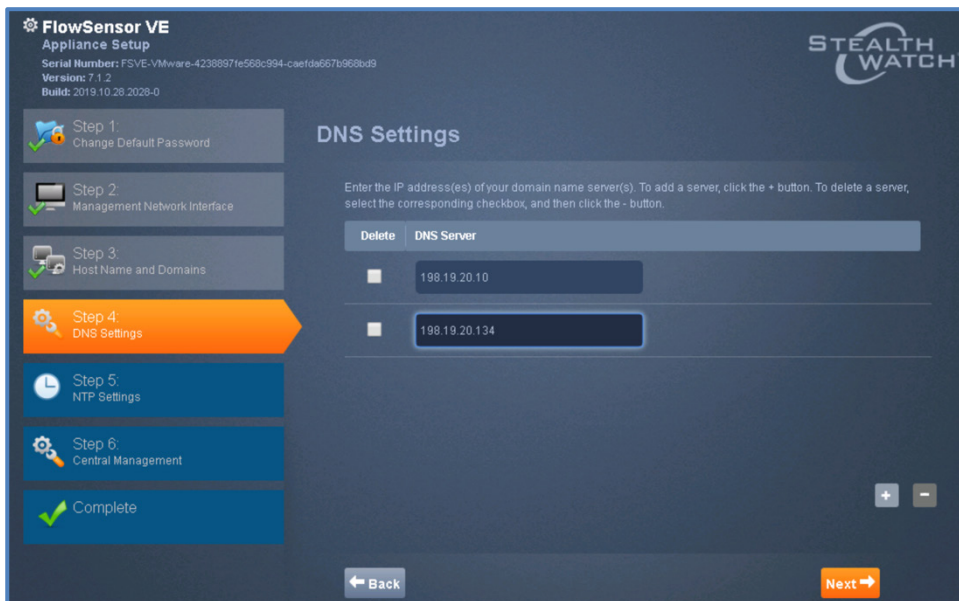


9. [ホスト名とドメイン (Host Name and Domain)] 画面が表示されます。次のパラメータを設定し、[次へ (Next)] をクリックして続行します。
- a. [ホスト名 (Host Name)] : **FS**
 - b. [ネットワークドメイン (Network Domain)] : **dcloud.cisco.com**



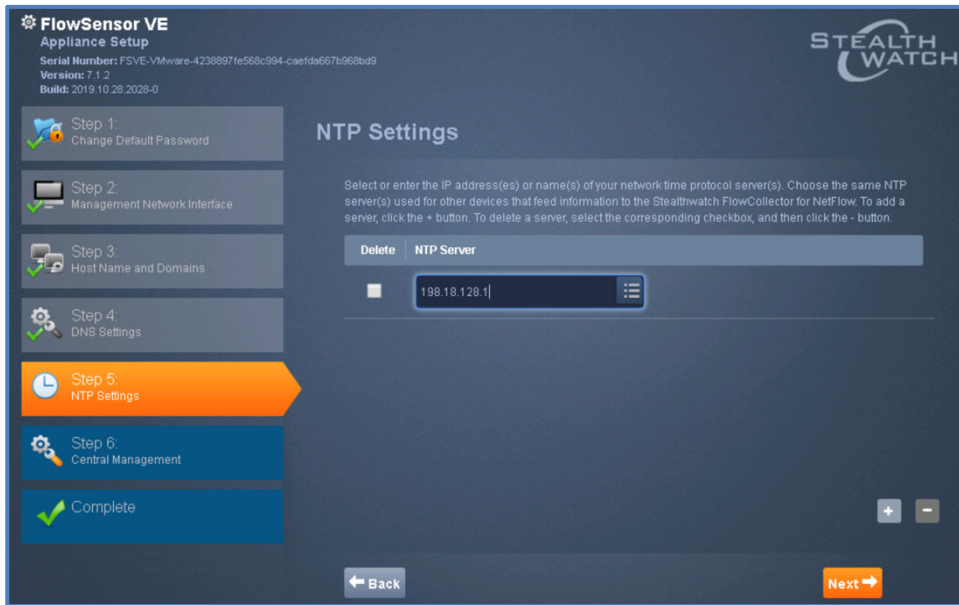
10. [DNS 設定 (DNS Settings)] 画面が表示されます。必要な DNS サーバを環境に追加します。

- a. 1 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.10** を入力します。
- b. 2 つ目の DNS サーバを追加するには、[+] アイコンをクリックします。
 - i. **198.19.20.134** を入力します。
- c. 両方の DNS エントリが表示されたら、[次へ (Next)] をクリックして続行します。

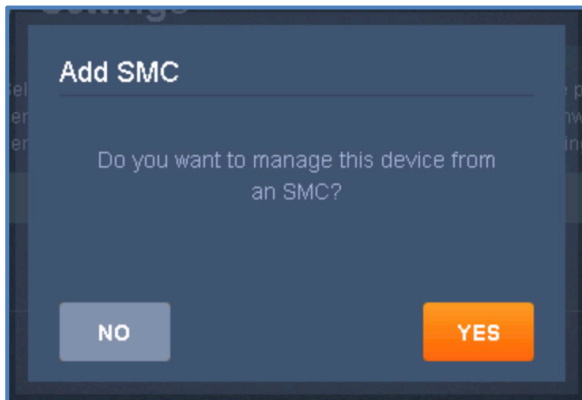


11. [NTP 設定 (NTP Settings)] 画面が表示されます。環境に適した NTP 設定を入力します。

- a. 全部で3つあるデフォルトの NTP エントリの前にある [削除 (Delete)] チェックボックスをすべてオンにし、[-] ボタンをクリックします。
 - i. すべてのエントリが削除されます。
- b. [+] ボタンをクリックします。
 - i. 新しい NTP エントリフィールドに **198.18.128.1** と入力します。
 - ii. エントリが 198.18.128.1 のみになります。
- c. 残っている NTP エントリが 1 つのみであることを確認し、[次へ (Next)] をクリックします。



12. [SMC の追加 (Add SMC)] ポップアップが表示されたら、[はい (YES)] をクリックします。



13. [確認と再起動 (Review and Restart)] ページが表示されます。[再起動と続行 (Restart and Proceed)] をクリックします。

Review and Restart

In order to update with the below changes, you need to restart your machine. Upon returning to the Application, you will be brought to Step 6 to continue setup of your Appliance.

Management Network Interface		Host Name and Network Domain	
Name:	eth0	Host Name:	FS
MAC Address:	00:50:56:b8:1e:8d	Network Domain:	dcloud.cisco.com
IP Address:	198.19.20.138		
Subnet Mask:	255.255.255.0		
Default Gateway:	198.19.20.1		
Broadcast Address:	198.19.20.255		
IPv6 Address:			
IPv6 Prefix Length:			
IPv6 Gateway:			
DNS Settings		NTP Settings	
DNS Server:	198.19.20.10	NTP Server:	198.18.128.1
DNS Server:	198.19.20.134		

14. [OK] をクリックし、フローセンサーの再起動を確定します。

Notice

This appliance will now restart. Are you sure you want to continue?

15. フローセンサーが再起動している間、しばらくお待ちください。「処理中」というメッセージが表示され、その後「このサイトにアクセスできません」と表示されます。**1 ~ 2 分待ってから、Web ページのリロードを試みます。**

- フローセンサー証明書の警告ページが表示されるまで、ページのリロードを続行します。[詳細設定 (Advanced)] ボタンをクリックし、[~ にアクセスする (安全ではありません) (Proceed ... (unsafe))] リンクをクリックします。

Your connection is not private

Attackers might be trying to steal your information from **198.19.20.138** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. [Privacy policy](#)

This server could not prove that it is **198.19.20.138**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 198.19.20.138 \(unsafe\)](#)

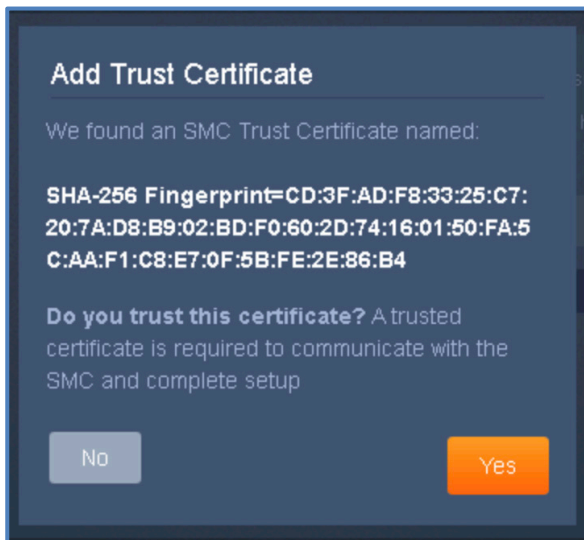
- b. フローセンサーに **admin** および **C1sco12345** のクレデンシャルでログインします。次に、[ウェルカム (Welcome)] ページで [Ok] をクリックします。

The image shows the Stealthwatch login interface. At the top, the Cisco logo and 'Stealthwatch' text are displayed, followed by 'FlowSensor VE 7.1.2'. Below this, there are two input fields: 'Username:' and 'Password:'. A 'Login >>' button is positioned at the bottom right of the login area. To the right of the login area, a 'Welcome' box displays the message: 'Your last login was Thu Jan 23 2020 7:11:22 PM from 198.19.30.36'.

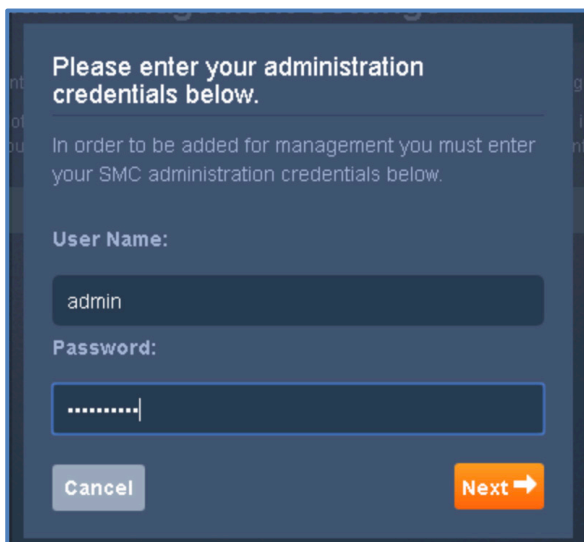
16. 表示される AST ページで [続行 (Continue)] をクリックします。
17. [Central Management 設定 (Central Management Settings)] ページが表示されます。[IP アドレス (IP Address)] フィールドに **198.19.20.136** と入力し、[保存 (Save)] をクリックします。

The image shows the 'Central Management Settings' page in the FlowSensor VE interface. On the left, a vertical list of steps is shown: Step 1 (Change Default Password), Step 2 (Management Network Interface), Step 3 (Host Name and Domains), Step 4 (DNS Settings), Step 5 (NTP Settings), Step 6 (Central Management), and Complete. Step 6 is highlighted in orange. The main content area is titled 'Central Management Settings' and contains the instruction: 'Enter the IP address of the Central Manager that you will be using to configure and manage this appliance. Note: By default, this will be the IP address of your SMC. If you have SMCs in a failover pair, enter the IP address of your primary SMC. Also, your security events will be sent to the SMC you enter here.' Below this, there is an 'IP Address' input field with the value '198.19.20.136' and a 'Save' button. A 'Back' button is located at the bottom left.

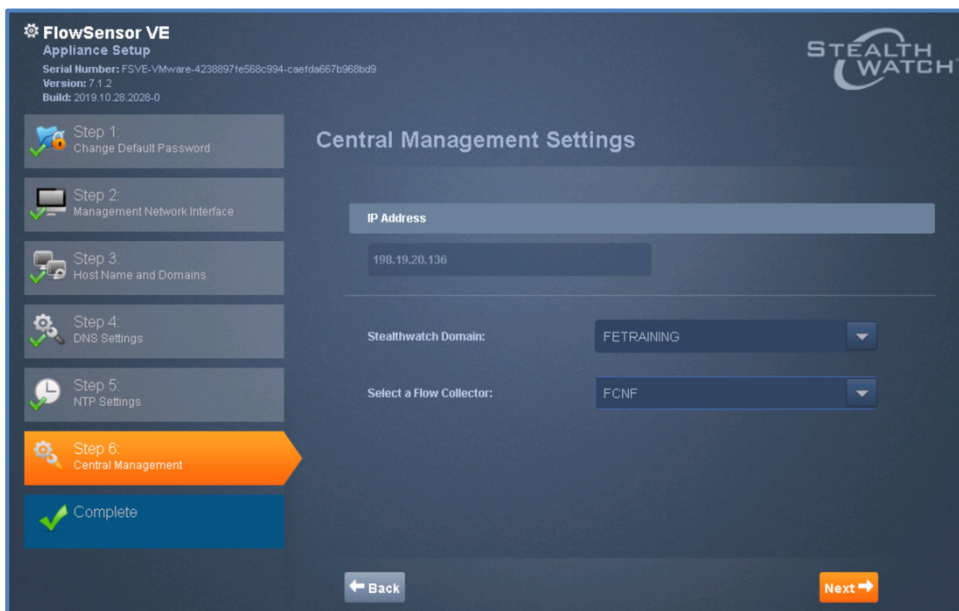
18. [信頼できる証明書の追加 (Add Trust Certificate)] ページが表示されます。[はい (Yes)] をクリックします。



19. SMC 管理者のクレデンシャルを入力するように求められます。 **admin** と **C1sco12345** を入力し、[次へ (Next)] をクリックします。

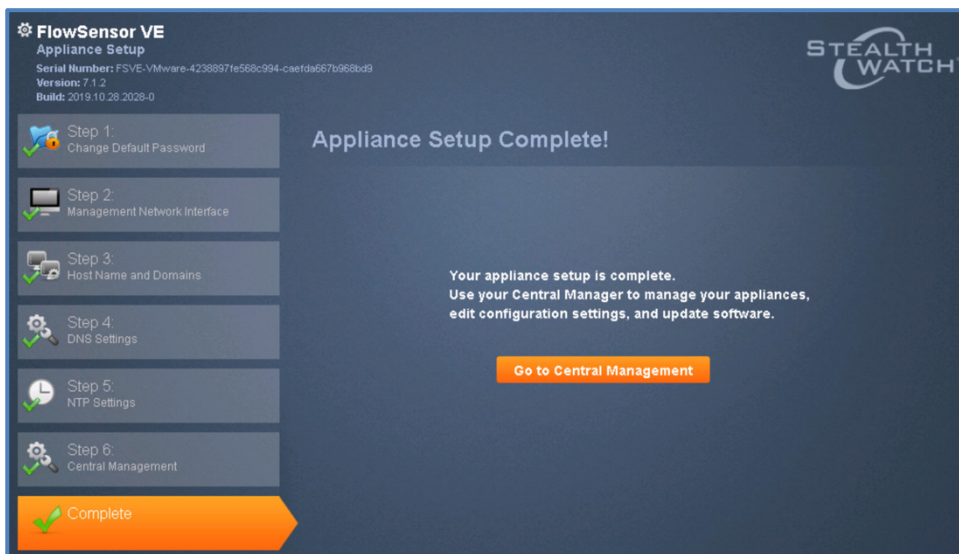


20. [Central Management 設定 (Central Management Settings)] ページが表示されます。 [Stealthwatch ドメイン (Stealthwatch Domain)] ドロップダウンから [FETRAINING] を選択します。
21. 次に、[フローコレクタの選択 (Select a Flow Collector)] ドロップダウンが表示されたら、リストから [FCNF] をクリックします。

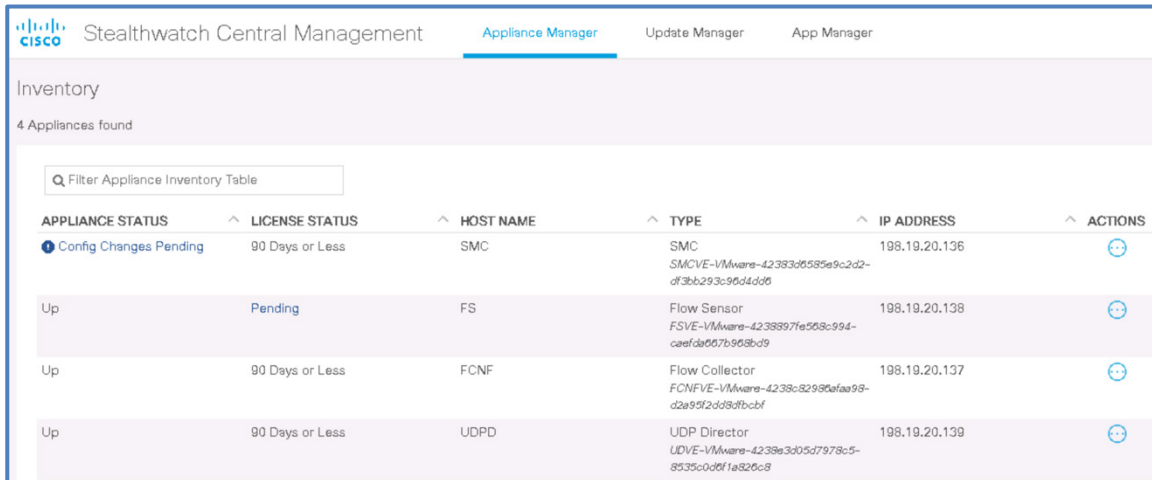


22. [次へ (Next)] をクリックします。

23. セットアップが完了するまでお待ちください。[Central Management に移動 (Go to Central Management)] のボタンが表示されたらクリックします。



24. Central Management のリストに 4 つの appliance がすべて表示されます。



APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	90 Days or Less	SMC	SMC SMCVE-VMware-42383d6585e9c2d2-df3bb293c96d4dd6	198.19.20.136	
Up	Pending	FS	Flow Sensor FSVE-VMware-4238897fe568c994-caefda667b968bd9	198.19.20.138	
Up	90 Days or Less	FCNF	Flow Collector FCNFVE-VMware-4238c82986afaa98-d2a9f2d3d8dfcbf	198.19.20.137	
Up	90 Days or Less	UDPD	UDP Director UDVE-VMware-4238e3d05d7978c5-8535c0d6f1a826c8	198.19.20.139	

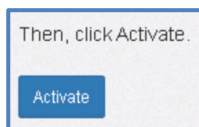
25. FS のアプライアンスのステータスが最終的に [Up] に変わったら次に進みます。

- a. FS に関連付けられた [アクション (Actions)] アイコン ([インベントリ (Inventory)] の FS エントリの右側) をクリックし、[ライセンスの管理 (Manage Licenses)] をクリックします。

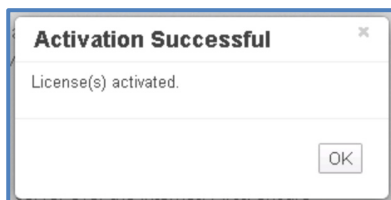


APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	Up to date	SMC	SMC SMCVE-VMware-42383d6585e9c2d2-df3bb293c96d4dd6	198.19.20.136	
Up	Pending	FS	Flow Sensor FSVE-VMware-4238897fe568c994-caefda667b968bd9	198.19.20.138	<ul style="list-style-type: none"> Edit Appliance Configuration View Appliance Statistics Manage Licenses Support Reboot Appliance Shut Down Appliance Remove This Appliance
Up	Up to date	FCNF	Flow Collector FCNFVE-VMware-4238c82986afaa98-d2a9f2d3d8dfcbf	198.19.20.137	
Up	Up to date	UDPD	UDP Director UDVE-VMware-4238e3d05d7978c5-8535c0d6f1a826c8	198.19.20.139	

- b. 有効化の方法として [オンラインライセンス (Online Licensing)] が設定されていることを確認してください。[有効化 (Activate)] をクリックします。



- c. 有効化が完了したら、[OK] をクリックします。



- d. 下にスクロールして、有効化されたライセンスを表示します。

Feature License Status				
Feature ▲	Count ◆	Start Date ◆	Expiration Date ◆	Status ◆
FSBASE	Uncounted	Mar 04, 2019 UTC	Never	Installed

26. [Central Management] タブを開いたままにして、[FS 管理 (FS Administration)] タブを閉じます。

シナリオのまとめ

お客様の導入環境内のすべての Stealthwatch アプライアンスを SMC で管理するために必要な手順を、正常に完了しました。これで、追加のアプライアンス設定タスクを完了する準備が整いました。

シナリオ 2. アプライアンスのインストール後の設定および検証

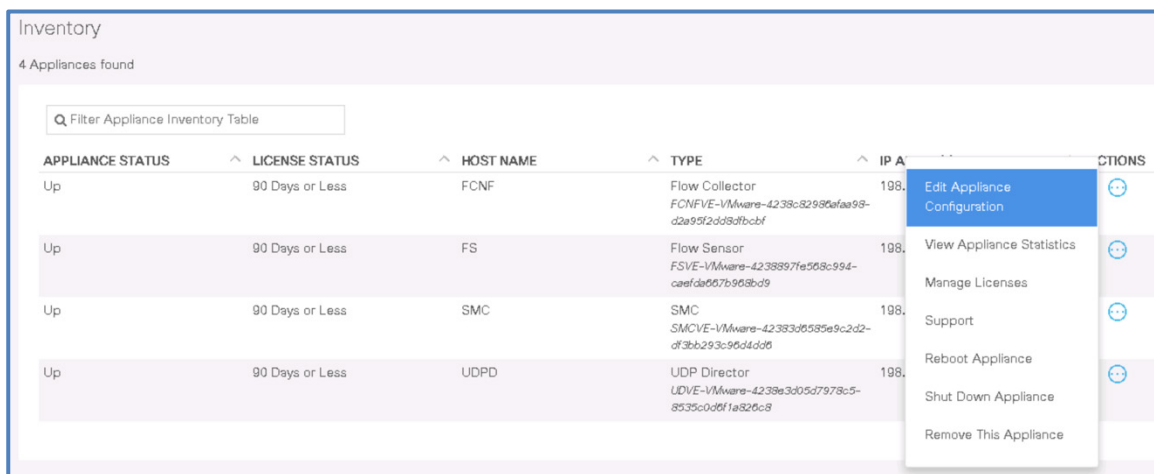
アプライアンス セットアップ ツール (AST) では構成できない設定を、いくつか追加する必要があります。お客様の導入の一環として、アプライアンスで必要な追加設定およびテスト手順を実施します。追加設定には、フローセンサーによる NetFlow 処理、UDP Director による NetFlow 転送、すべてのアプライアンスへの SSH アクセス、および必要な場合のコグニティブ統合有効化の設定が含まれます。また、プロアクティブな DNS および NTP テストを実施して、円滑な導入を実現します。

導入では、トラブルシューティングおよび検証のいくつかの手順で SSH コンソールアクセスを使用します。したがって、各アプライアンスで SSH サービスを有効にします。Cisco Stealthwatch では、Cisco Cognitive Analytics ソリューションと情報を共有して、Stealthwatch で検出されたテレメトリデータに関する追加の検知およびレポート機能を提供できます。この統合を実現するには、SMC とフローコレクタでこの機能を有効にする必要があります。

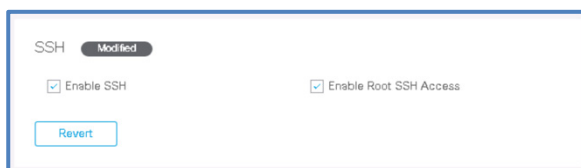
さらに、お客様から提供された DNS および NTP の値が正しく、それらのサービスがアプライアンス上で適切に機能していることを確認します。Stealthwatch ソリューションを完全に機能させ、お客様が利用できるようにするには、これらの手順を完了する必要があります。

アプライアンスでの SSH およびコグニティブの有効化

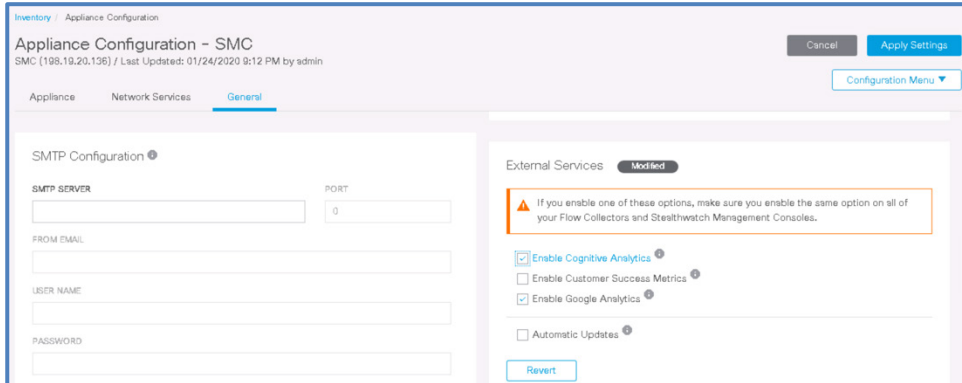
- SMC の [Stealthwatch Central Management] ページ (<https://198.19.20.136/central-mgmt/>) への Chrome の接続を見つけるか、開きます。
- 最初に、Stealthwatch Management Console (SMC) に移動します。
 - インベントリで [SMC] のエントリを見つけ、SMC の [アクション (Actions)] 列の右側にある円形アイコンをクリックします。
 - ポップアップメニューから [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。この場所から多くの一般的な設定オプションにアクセスできます。[アプライアンス設定の編集 (Edit Appliance Configuration)] が表示されない場合は、SMC の [アプリケーションのステータス (Application Status)] の表示が [Up] になるまで待つ必要があります。



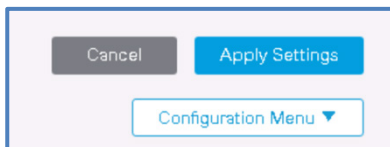
- 下にスクロールして SSH セクションを見つけ、[SSH の有効化 (Enable SSH)] と [ルート SSH アクセスの有効化 (Enable Root SSH Access)] の両方にチェックマークを入れます。



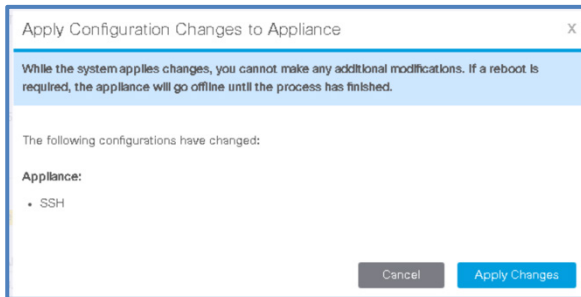
- d. [全般 (General)] タブをクリックし、[外部サービス (External Services)] セクションが表示されるまで下にスクロールし、[Cognitive Analytics の有効化 (Enable Cognitive Analytics)] をクリックします。



- e. [設定の適用 (Apply settings)] をクリックします。



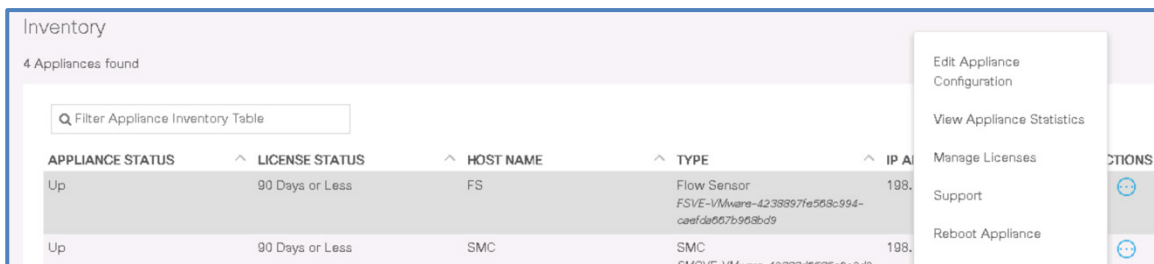
- f. 変更を確認するように求められたら、[変更の適用 (Apply Changes)] を選択します。



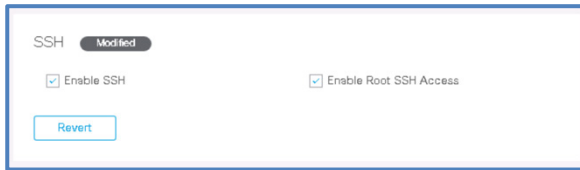
- g. SMC (<https://198.19.20.136/central-mgmt/>) の [Stealthwatch Central Management] ページに戻ります。

3. フローセンサー (FS) の SSH を有効にします。

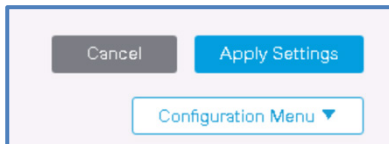
- a. [FS] のエントリを見つけ、FS の [アクション (Actions)] 列の右側にある円形アイコンをクリックします。
- b. ポップアップメニューから [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。この場所から多くの一般的な設定オプションにアクセスできます。



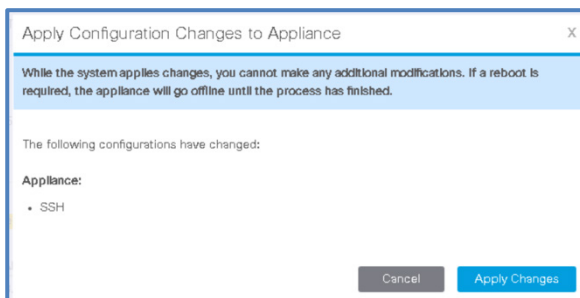
- c. 下にスクロールして SSH セクションを見つけ、[SSH の有効化 (Enable SSH)]と [ルート SSH アクセスの有効化 (Enable Root SSH Access)]の両方にチェックマークを入れます。



- d. [設定の適用 (Apply settings)]をクリックします。



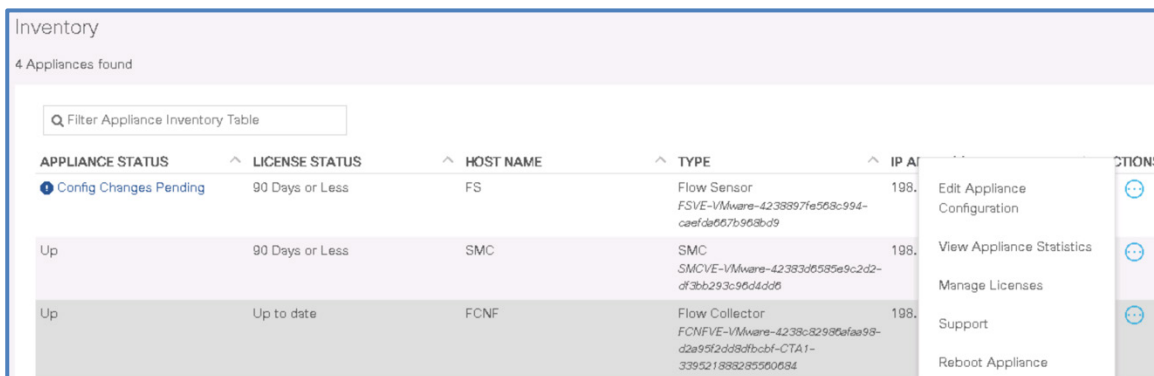
- e. 変更を確認するように求められたら、[変更の適用 (Apply Changes)]を選択します。



- f. SMC (<https://198.19.20.136/central-mgmt/>) の [Stealthwatch Central Management] ページに戻ります。

4. フローコレクタ (FCNF) の SSH を有効にします。

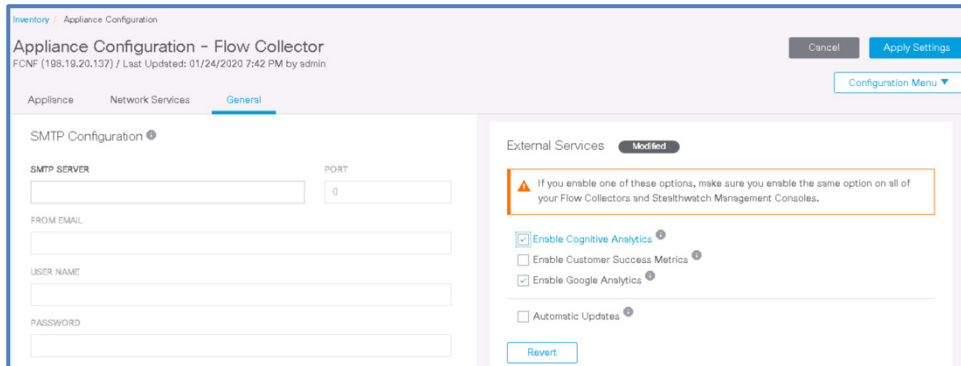
- a. [FCNF] のエントリを見つけ、FCNF の [アクション (Actions)]列の右側にある円形アイコンをクリックします。
- b. ポップアップメニューから [アプライアンス構成の編集 (Edit Appliance Configuration)]を選択します。この場所から多くの一般的な設定オプションにアクセスできます。



APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	90 Days or Less	FS	Flow Sensor FSVE-VMware-4238897e568c994-caefda067b908bd9	198.	Edit Appliance Configuration
Up	90 Days or Less	SMC	SMC VE-VMware-42383d6585e9c2d2-df3bb293c96d4d06	198.	View Appliance Statistics Manage Licenses
Up	Up to date	FCNF	Flow Collector FCNFVE-VMware-4238c82980afaa99-d2a95f2dd8d9cbf-CTA1-33952189828590684	198.	Support Reboot Appliance

- c. SSH セクションを見つけ、[SSH の有効化 (Enable SSH)]と [ルート SSH アクセスの有効化 (Enable Root SSH Access)]の両方が選択されていることを確認します。

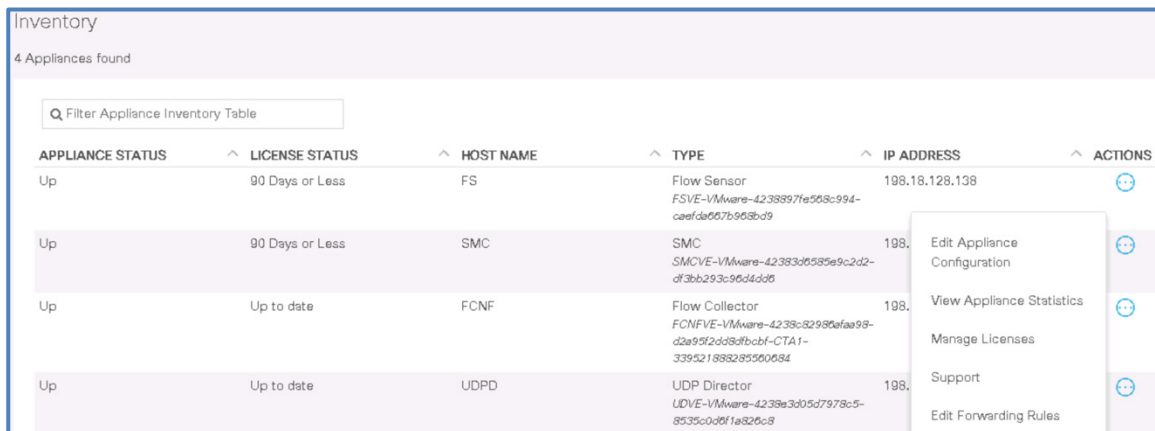
- d. [全般 (General)] タブをクリックし、[外部サービス (External Services)] セクションが表示されるまで下にスクロールし、[Cognitive Analytics の有効化 (Enable Cognitive Analytics)] をクリックします。



- e. 再度 [設定の適用 (Apply Settings)]、[変更の適用 (Apply Changes)] をクリックします。

5. UDP Director (UDPD) の SSH を有効にします。

- a. [UDPD] のエントリを見つけ、UDPD の [アクション (Actions)] 列の右側にある円形アイコンをクリックします。
- b. ポップアップメニューから [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。この場所から多くの一般的な設定オプションにアクセスできます。



APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	FS	Flow Sensor FSVE-VMware-4238897e568c994-caefda667b968bd9	198.18.128.138	[Icon]
Up	90 Days or Less	SMC	SMC SMCVE-VMware-42383c6585e9c2d2-df3bb293c96d4dd6	198.	[Icon] Edit Appliance Configuration
Up	Up to date	FCNF	Flow Collector FCNFVE-VMware-4238c829980afaa98-d2e9f2dd8dfbcbf-CTA1-33952188828550684	198.	[Icon] View Appliance Statistics
Up	Up to date	UDPD	UDP Director UDVE-VMware-4238e3d05d7978c5-8535c0d6f1a826c8	198.	[Icon] Manage Licenses Support Edit Forwarding Rules

- c. SSH セクションを見つけ、[SSH の有効化 (Enable SSH)] と [ルート SSH アクセスの有効化 (Enable Root SSH Access)] の両方が選択されていることを確認します。
- d. 再度 [設定の適用 (Apply Settings)]、[変更の適用 (Apply Changes)] をクリックします。

注：新しいアプライアンスでは、SSH およびルート SSH がデフォルトで無効になっています。このアクセス方法を使用するには有効にする必要があります。このアクセス方法はこのドキュメント内のラボを進めるのに不可欠であるため、各アプライアンスで有効になっていることを確認する必要があります。

6. 再度 [Central Management] ページに戻ります。SMC と FCNF の両方のアプライアンスが [Up] になるまで待ちます。
7. コグニティブが有効になっていることを確認します。Chrome で SMC の Web ページを開くか、そのページに戻ります。
8. [セキュリティ分析ダッシュボード (Security Insight Dashboard)] にいることを確認します ([ダッシュボード (Dashboards)] > [ネットワークセキュリティ (Network Security)])。

9. [Cognitive Threat Analytics] という名前の新しいウィジェットが表示されるまで下にスクロールします。表示されない場合は、Chrome のウィンドウを閉じてから再度 Chrome を開き、SMC アプライアンスに admin と C1sco12345 のクレデンシャルで再接続、認証します。
 - a. この dCloud セッション内で、ライセンス制限によりウィジェットをロードできなくても問題ありません。

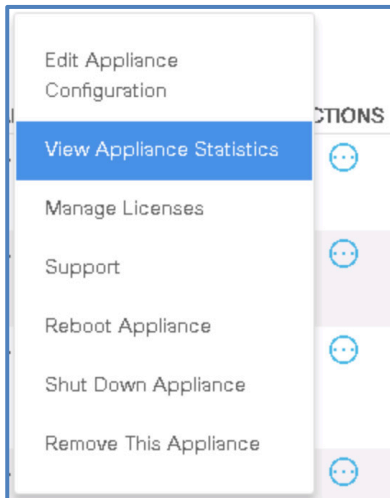


10. ここでは Cognitive Threat Analytics (CTA) のみを有効にします。これで、ラボシナリオの次の部分に進むことができます。

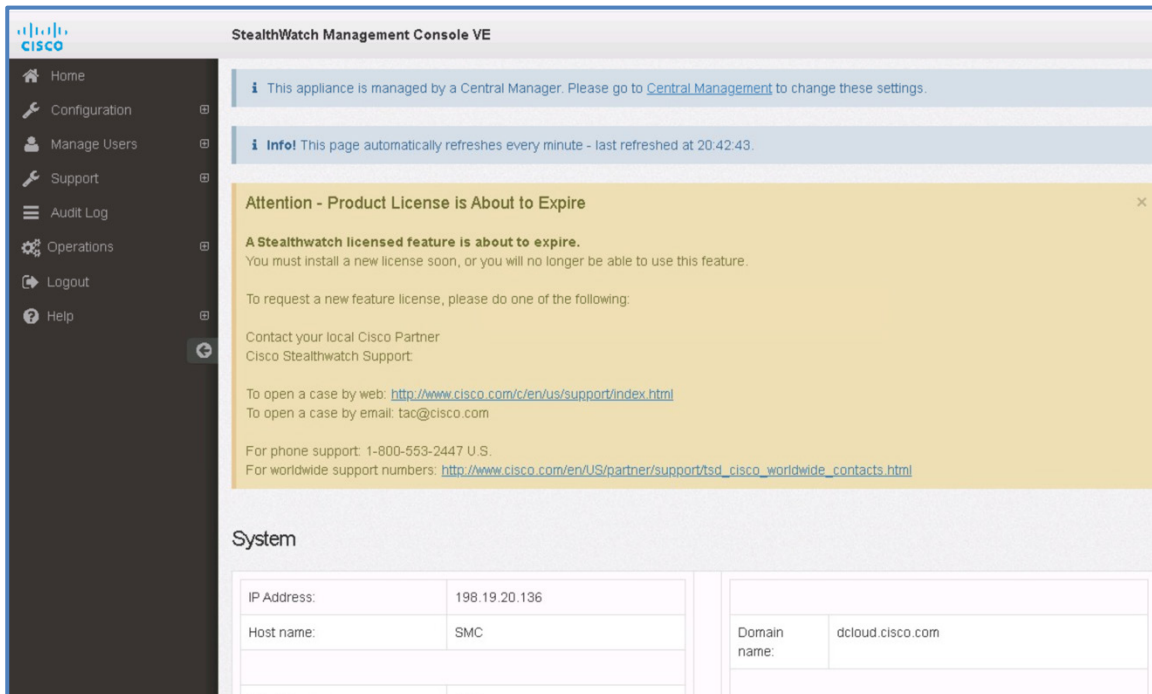
DNS の検証

次に、SMC アプライアンスが、設定した 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を実行し、またライセンスと脅威フィードのアクセスに 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してください。

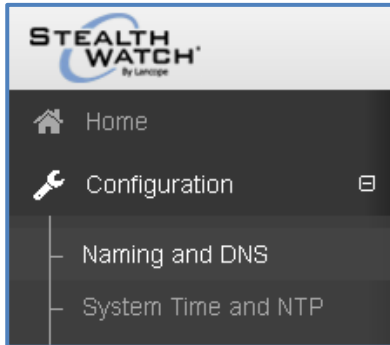
1. SMC の [Stealthwatch Central Management] ページ (<https://198.19.20.136/central-mgmt/>) への Chrome の接続を見つけるか、開きます。
2. **SMC** エントリを見つけ、関連する [アクション (Action)] アイコンをクリックしたら、[アプライアンス統計情報の表示 (View Appliance Statistics)] を選択します。



3. SMC アプライアンス管理のホームページが表示されます (ライセンスの警告は表示されません)。

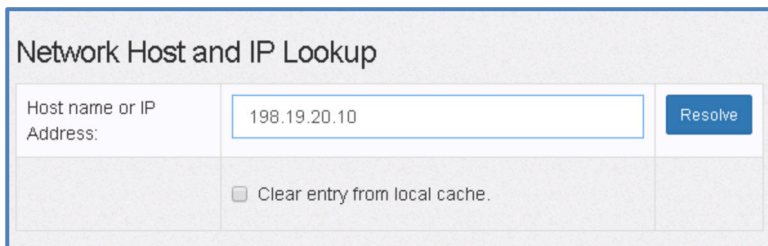


4. [設定 (Configuration)] メニューをクリックし、[ネーミングおよび DNS (Naming and DNS)] メニュー項目を選択します。



5. [ネットワークホストと IP ルックアップ (Network Host and IP Lookup)] セクションを見つけます。

- a. [ホスト名または IP アドレス (Host name or IP Address)] フィールドに IP アドレス **198.19.20.10** を入力し、[解決 (Resolve)] をクリックします。



- b. 新しい Chrome タブが開き、DNS 要求のステータスが表示されます。要求が成功し、IP アドレスの PTR レコードに関連付けられた名前が **ad1.dcloud.local** と表示されます。

```
Current status of cache for 198.19.20.10
Opening socket /var/cache/pdnsd/pdnsd.status
10.20.19.198.in-addr.arpa.
01/23 21:07:18 PTR ad1.dcloud.local.
Succeeded

New Cache Lookup
Opening socket /var/cache/pdnsd/pdnsd.status
Could not find 10.20.19.198.in-addr.arpa in the cache.
Succeeded

Trying "10.20.19.198.in-addr.arpa"
::-->HEADER<<- opcode: QUERY, status: NOERROR, id: 14220
:: flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
:: QUESTION SECTION:
;10.20.19.198.in-addr.arpa. INPTR
:: ANSWER SECTION:
10.20.19.198.in-addr.arpa. 1200 INPTRad1.dcloud.local.
Received 73 bytes from 127.0.0.1#53 in 0 ms

DNS Servers:
198.19.20.134
198.19.20.10

Lookup from Trying "10.20.19.198.in-addr.arpa" Using
domain server: Name: 198.19.20.10 Address:
198.19.20.10#53 Aliases:
::-->HEADER<<- opcode: QUERY, status: NOERROR, id: 5422
:: flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

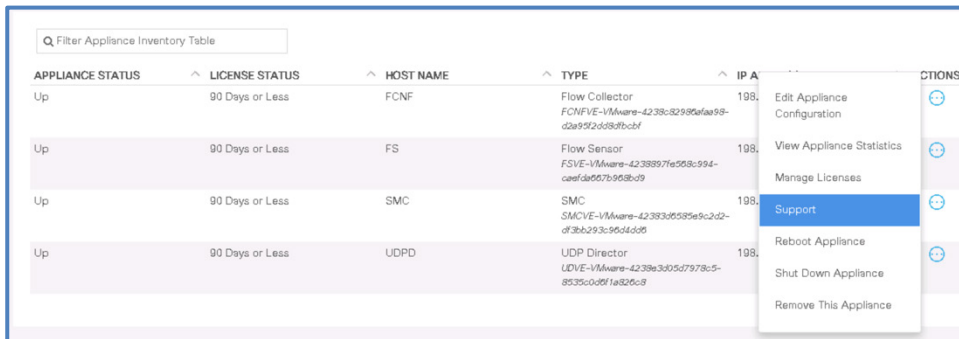
- c. アプライアンスが有効な DNS サーバと正常に通信できることを確認しました。要求が失敗した場合、**ad1.dcloud.local** の PTR レコードは表示されません。

6. この Chrome のタブを閉じ、SMC の Central Management ページに戻るまで、前に開いていた Chrome のタブを閉じます。

NTP の検証

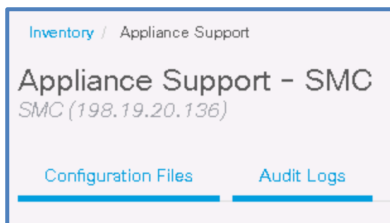
次に、SMC アプライアンスが、設定した NTP サーバと正常に通信できることを確認します。NTP は、すべての Stealthwatch アプライアンスで不可欠なサービスです。時刻の不一致が発見された場合は、製品内でアラームが発生します。お客様環境では、この検証をすべてのアプライアンスで実行してください。お客様から NTP サーバの IP アドレスを提供されても、それが有効な NTP サーバであるとは限らず、その NTP サーバとアプライアンスが通信できるとは限りません。監査ログは、アプライアンスが時刻の更新を正常に受信しているかどうかを判断する、最も簡単な方法です。必要に応じてさらに詳細な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 の機能を確認します。

1. SMC の Stealthwatch Central Management の [インベントリ (Inventory)] ページにいることを確認します。
2. インベントリリストの **SMC** の横にある [アクション (Action)] アイコンをクリックし、[サポート (Support)] をクリックします。



APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	FCNF	Flow Collector FCNFVE-V/Avare-4238c82985fa98-d2a592d3d38fbcbf	198.	Edit Appliance Configuration
Up	90 Days or Less	FS	Flow Sensor FSVE-V/Avare-4238897e568c994-caefda567b958b29	198.	View Appliance Statistics Manage Licenses
Up	90 Days or Less	SMC	SMC SMCVE-V/Avare-42383d585e9c2d2-df3bb293c96d4d3d	198.	Support Reboot Appliance Shut Down Appliance Remove This Appliance
Up	90 Days or Less	UDP	UDP Director UDVE-V/Avare-4238e3405d7978c5-8535c0d6f1a826c8	198.	

3. [監査ログ (Audit Logs)] をクリックします。



4. フィルタが表示されたら、[カテゴリ (Category)] 選択ツールで [管理 (Management)] を選択し、[検索 (Search)] をクリックします。

Appliance Support - SMC
SMC (198.19.20.136)

Configuration Files **Audit Logs**

DATE/TIME: 01/22/2020 09:14:34 pm - 01/23/2020 09:14:34 pm USER NAME: USER LOCATION: CATEGORY: Management Search

Audit Logs

DATE/TIME	CATEGORY	EVENT	EVENT DETAILS	USER NAME	USER LOCATION	PROCESS NAME (...)	SUCCESS
2020-01-23 09:07:19 PM	Management	1100	Entry 198.19.20.10 removed from DNS cache.	admin	198.19.30.36	osxsxd(90158)	Yes
2020-01-23 09:07:08 PM	Management	1100	System time reset from [2020-01-23T21:07:02.129481] to [2020-01-23T21:07:08.582879] for NTP server: 198.18.128.1.	root(0)	198.19.20.136	osxsxd(90048)	Yes

- a. 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 時間経過しているにもかかわらず、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。ここまでのラボの作業を迅速に行っていた場合、まだ監査ログに表示されていない可能性があります。

5. 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。

- a. WKST1 のデスクトップで、**putty** のショートカットを開きます。



- b. 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)] をクリックします。

PuTTY Configuration

Category:

- Session
- Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): Port: 22

Connection type:
 Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

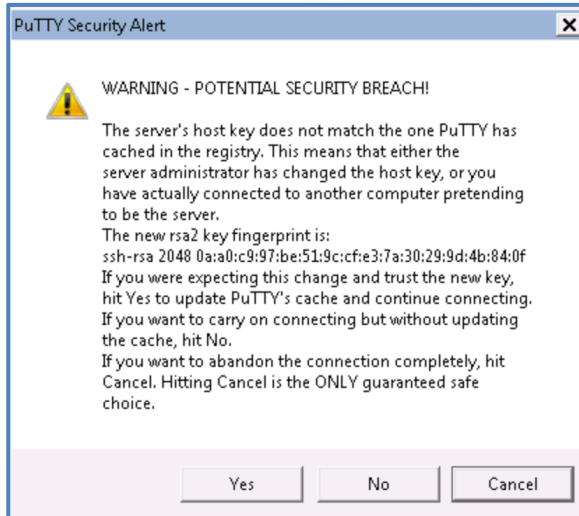
- ASAv
- CSR
- FCNF
- FCNF02
- FS
- SMC**

Load Save Delete

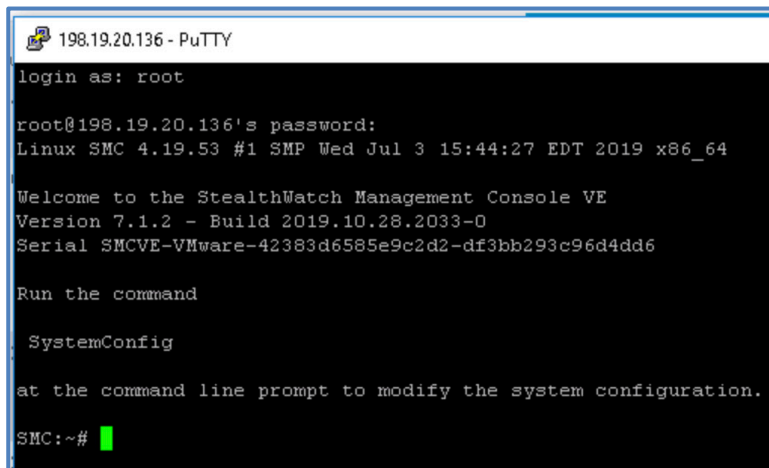
Close window on exit:
 Always Never Only on clean exit

About Open Cancel

- c. 警告が表示されたら、[Yes] をクリックします。



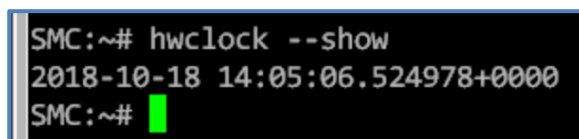
- d. 保存されたセッションへのログインを求められます。
- i. **C1sco12345** のパスワードで **root** としてログインし、**Enter** を押します。
- e. SSH で SMC コンソールにログインした状態になります。



- f. 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
```

- i. アプライアンスのタイムゾーン (UTC) に照らし、有効な日付とタイムスタンプが表示されていることを確認します。



- g. 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`

- i. 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。

```
SMC:~# ntpdate 198.18.128.1
18 Oct 14:06:16 ntpdate[71277]: adjust time server 198.18.128.1 offset 0.022136
sec
SMC:~# █
```

- h. 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`

- i. **注**：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。

```
SMC:~# ntpdate 198.18.128.2
18 Oct 14:07:01 ntpdate[71794]: no server suitable for synchronization found
SMC:~# █
```

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。

6. 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。
7. また、WKST1 で **Central Management ページを 1 つのみ開いたまま残して**、開いているすべての Chrome タブやウィンドウを閉じて構いません。

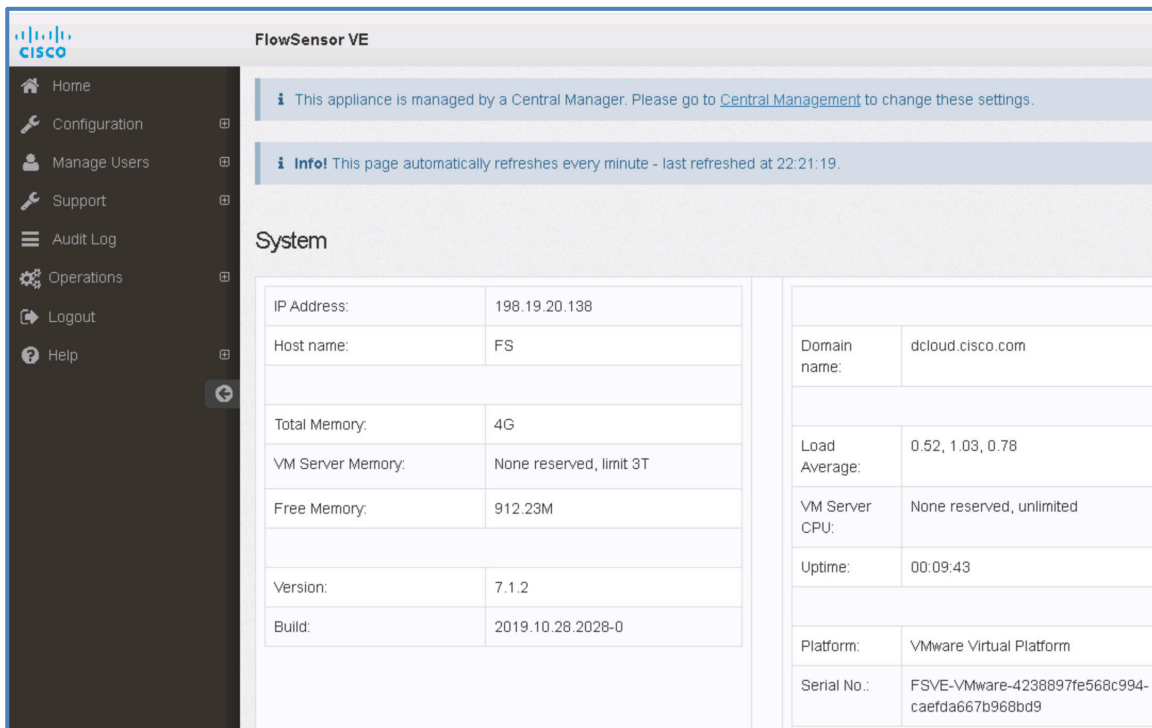
注：お客様環境では、すべてのアプライアンスが、割り当てられている NTP サーバと正常に通信できることを確認することが重要です。Stealthwatch をお客様環境に導入する際は、有効な各 NTP サーバに対して `ntpdate` コマンドを実行し、正常に接続されていることを確認します。

フローセンサーの設定

- SMC の [Stealthwatch Central Management] ページ (<https://198.19.20.136/central-mgmt/>) への Chrome の接続を見つけるか、開きます。[Central Management] ウィンドウの左上にあるシスコのロゴをクリックすると、いつでも [インベントリ (Inventory)] ページに戻ることができます。



- FS** エントリを見つけ、関連する [アクション (Action)] アイコンをクリックしたら、[アプライアンス統計情報の表示 (View Appliance Statistics)] を選択します。
 - 認証を求められたら、次のログイン情報を使用します。
 - [ユーザ名 (Username)] : **admin**
 - [パスワード (Password)] : **C1sco12345**
 - ウェルカムポップアップで [Ok] をクリックします。
- フローセンサーの Web 管理ページが表示されます。

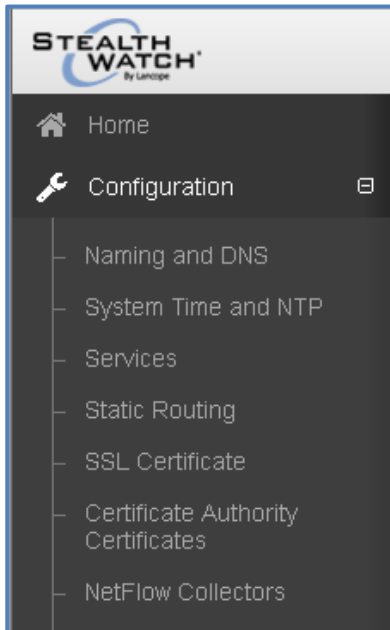


The screenshot displays the 'FlowSensor VE' web management interface. On the left is a navigation menu with options: Home, Configuration, Manage Users, Support, Audit Log, Operations, Logout, and Help. The main content area shows a system status page with two informational messages at the top: 'This appliance is managed by a Central Manager. Please go to Central Management to change these settings.' and 'Info! This page automatically refreshes every minute - last refreshed at 22:21:19.' Below these is a 'System' section with two tables of data.

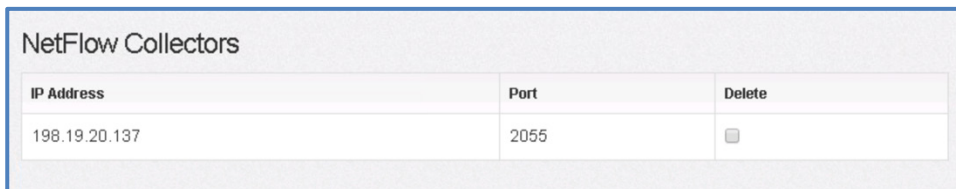
IP Address:	198.19.20.138
Host name:	FS
Total Memory:	4G
VM Server Memory:	None reserved, limit 3T
Free Memory:	912.23M
Version:	7.1.2
Build:	2019.10.28.2028-0

Domain name:	dcloud.cisco.com
Load Average:	0.52, 1.03, 0.78
VM Server CPU:	None reserved, unlimited
Uptime:	00:09:43
Platform:	VMware Virtual Platform
Serial No.:	FSVE-VMware-4238897fe568c994-caefda667b968bd9

- [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。



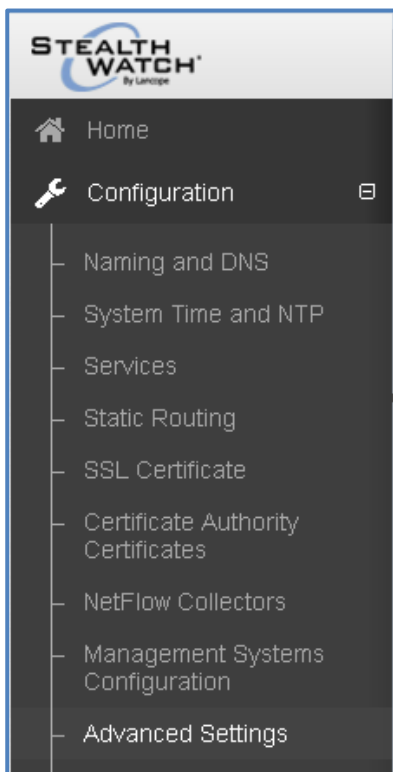
5. **198.19.20.137** のポート **2055** で実行されているフローコレクタのエントリが、[NetFlow コレクタ (NetFlow Collectors)] ページに表示されていることを確認します。



The screenshot shows the NetFlow Collectors table with the following data:

IP Address	Port	Delete
198.19.20.137	2055	<input type="checkbox"/>

6. [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。



7. 次の設定を構成し、完了したら [適用 (Apply)] 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**
 - i. [IPv6 を含める (Include IPv6)] : **オン**
 - ii. [HTTPS ヘッダーデータを含める (Include HTTPS Header Data)] : **オン**
 - iii. [HTTP ヘッダーデータを含める (Include HTTP Header Data)] : **オン**
 1. **256** バイトの HTTP 要求パスをエクスポート
 - c. [VXLAN カプセル化解除の有効化 (Enable VXLAN Decapsulation)] : **オフ**
 - d. [X-Forwarded-For 処理の有効化 (Enable X-Forwarded-For Processing)] : **オフ**
 - e. [ETA 処理の有効化 (Enable ETA Processing)] : **オン**
 - f. [IPFIX] : **選択**
 - g. [キャッシュモード (Cache Mode)] : [シングル...を使用 (Use single...)]
 - h. [適用 (Apply)] をクリックします。

<input checked="" type="checkbox"/> Export Packet Payload
<input checked="" type="checkbox"/> Export Application Identification
<input checked="" type="checkbox"/> Include IPv6
<input checked="" type="checkbox"/> Include HTTPS Header Data <i>(Applies only to IPFIX exports.)</i>
<input checked="" type="checkbox"/> Include HTTP Header Data <i>(Applies only to IPFIX exports.)</i>
Export <input type="text" value="256"/> bytes of the HTTP Request Path.
<input type="checkbox"/> Enable VXLAN Decapsulation
<input type="checkbox"/> Enable X-Forwarded-For Processing
<input checked="" type="checkbox"/> Enable ETA Processing
Flow Export Format:
<input checked="" type="radio"/> IPFIX
<input type="radio"/> NetFlow v9
Cache Mode
<input checked="" type="radio"/> Use single, shared, cache for all monitoring ports
<input type="radio"/> Use independent caches for each monitoring port
<input type="button" value="Apply"/>

i. 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。

8. 必要な追加のフローセンサー設定が正常に完了しました。FS Web 管理ページを閉じ、**Central Management** に戻ります。ラボの次の手順に進みます。

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、それらは実際には Web ブラウズではなく、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。お客様が「IPv6 はない」と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。

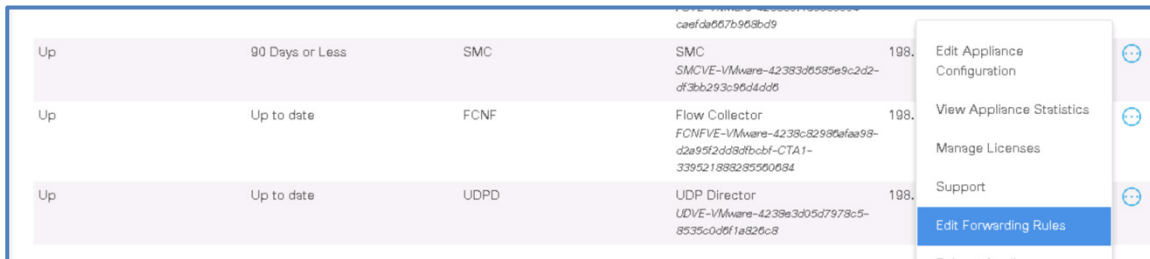
UDP Director の設定

お客様は、UDP Director アプライアンス (UDPD) を使用して、UDP 管理トラフィックの設定および転送を簡素化しています。UDP Director の IP アドレスは、お客様の NetFlow および Syslog トラフィックの単一のターゲットになっています。このデータを UDP トラフィックを必要とするすべてのシステムに転送するように、UDP Director を設定する必要があります。すべてのフローデータがアプライアンスを通過するため、UDPD はお客様環境に不可欠です。この設定に誤りがあると、Stealthwatch は適切に機能するためのデータが得られません。

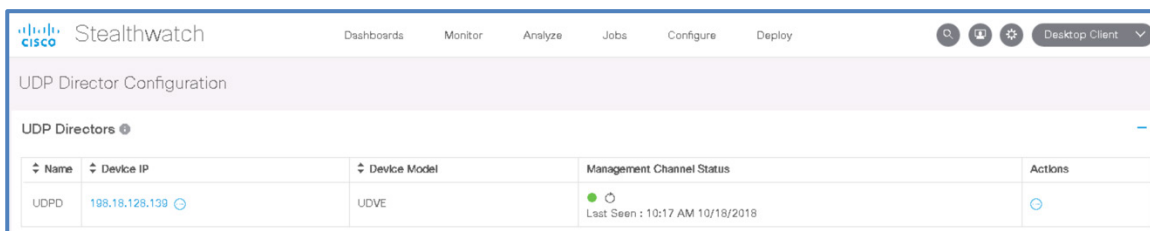
注：UDP Director はオプションの Stealthwatch アプライアンスであり、お客様環境における NetFlow およびその他の UDP 管理トラフィックの単一の宛先として機能します。設定がシンプルになり、Stealthwatch を含むさまざまなソリューションによる、NetFlow、SNMP トラップ、Syslog などのデータ処理の柔軟性が向上します。

UDP Director の IP アドレスは、お客様環境内の NetFlow エクスポートが 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。

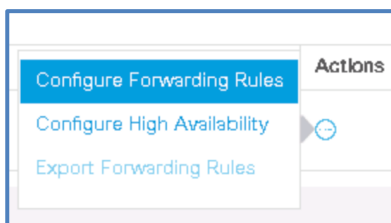
1. SMC の [Stealthwatch Central Management] ページ (<https://198.19.20.136/central-mgmt/>) への Chrome の接続を見つけるか、開きます。
2. **UDPD** エントリを見つけ、関連する [アクション (Action)] アイコンをクリックしたら、[転送ルールの編集 (Edit Forwarding Rules)] を選択します。



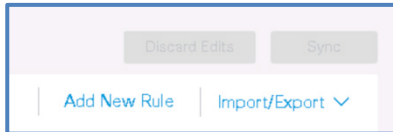
3. SMC の [UDP Director 設定 (UDP Director Configuration)] ページが表示されます。



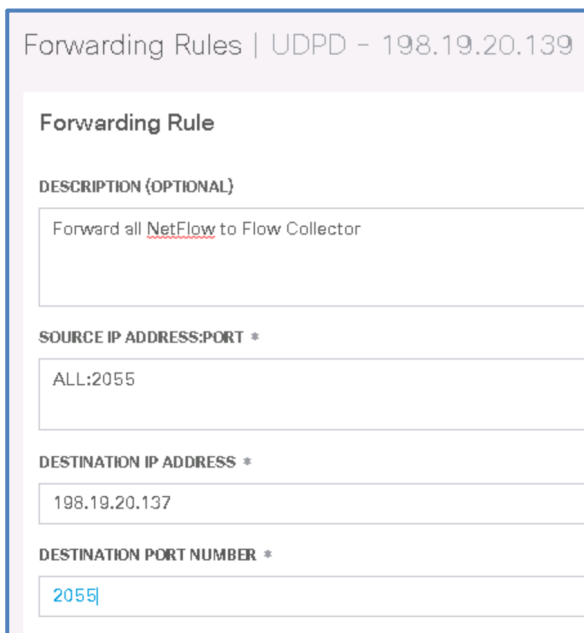
4. UDPD アプライアンスに関連する [アクション (Actions)] アイコンを選択し、[転送ルールの設定 (Configure Forwarding Rules)] をクリックします。



5. [転送ルール (Forwarding Rules)] ページで、[新しいルールの追加 (Add New Rule)] を選択します。



6. UDP Director が UDP/2055 で受信した NetFlow トラフィックを、UDP/2055 の FC アプライアンスに転送するよう設定するの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。
- [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)]
 - [送信元 IP アドレス : ポート (Source IP Address:Port)] : **ALL:2055**
 - [宛先 IP アドレス (Destination IP Address)] : **198.19.20.137**
 - [宛先ポート番号 (Destination Port Number)] : **2055**
 - [保存 (Save)] をクリックします。

A screenshot of the 'Forwarding Rules | UDPD - 198.19.20.139' configuration page. It shows a form with the following fields:

- Forwarding Rule**
- DESCRIPTION (OPTIONAL)**: Forward all NetFlow to Flow Collector
- SOURCE IP ADDRESS:PORT ***: ALL:2055
- DESTINATION IP ADDRESS ***: 198.19.20.137
- 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。非常に単純化した例として、1秒あたりの合計が10万フロー（FPS）に達し、2つのFCに負荷を分散する必要がある場合があります。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）]フィールドで「ALL」値を使用するのではなく、トラフィックを適切なFCに送信するために単一のIPアドレスまたはCIDR範囲を指定する必要があります。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。

UDP設定に関する一般的な問題としては、UDP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が設定されません。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UDP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FCの設定を変更することなく2055のFCに転送するという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。

7. ルールリストに新しいルールが表示されます。

RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER	ACTIONS
1	Forward all NetFlow to Flow Collector	ALL:2055	198.19.20.137	2055	

8. [新しいルールの追加（Add New Rule）] ボタンをクリックして、お客様のプロキシの Syslog トラフィックを転送するための2番目のルールを追加します。

9. 次のパラメータを使用して新しいルールを設定し、完了したら[保存（Save）]をクリックします。

- a. [説明（Description）]：すべての Syslog を SMC に転送（Forward all Syslog to SMC）
- b. [送信元 IP アドレス：ポート（Source IP Address:Port）]：**ALL:514**
- c. [宛先 IP アドレス（Destination IP Address）]：**198.19.20.136**
- d. [宛先ポート番号（Destination Port Number）]：**514**
- e. [保存（Save）]をクリックします。

Forwarding Rule

DESCRIPTION (OPTIONAL)

Forward All Syslog to SMC

SOURCE IP ADDRESS:PORT *

ALL:514

DESTINATION IP ADDRESS *

198.19.20.136

DESTINATION PORT NUMBER *

514

注：UDPが環境がない、または SMC が 1 つしかない環境では、SMC アプライアンス自体の IP アドレスに直接送信されるように Syslog を設定できます。お客様環境にプライマリとセカンダリの両方の SMC アプライアンスがある場合は、それら両方のアプライアンスで syslog が必要となるため、可能であれば UDP を使用して、データを両方の SMC に転送することをお勧めします。

10. [転送ルール (Forwarding Rules)] リストに 2 つのルールが表示されます。これら 2 つのルールを検証します。このページで設定ミスがあると、ラボは期待どおりに動作しません。
 - a. **注：**受講者にありがちな設定ミスとして、IP アドレスに 198.x ではなく 192.x と入力することが挙げられます。

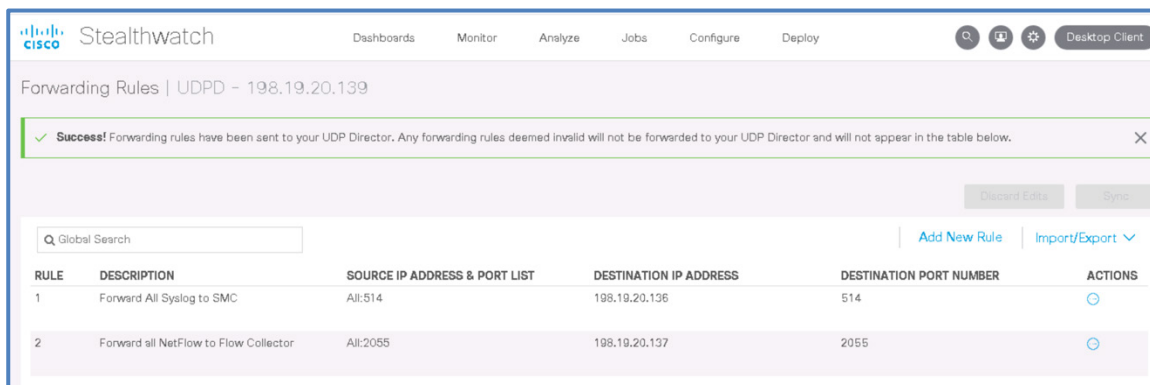
RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER
1	Forward All Syslog to SMC	ALL:514	198.19.20.136	514
2	Forward all NetFlow to Flow Collector	ALL:2055	198.19.20.137	2055

11. ここまでで転送ルールの設定自体は完了していますが、この設定を UDP Director アプライアンスと同期する必要があります。
 - a. [同期 (Sync)] をクリックします。

Discard Edits Sync

Add New Rule Import/Export

12. しばらくすると、ページが更新されて成功メッセージが表示されます。このメッセージが表示され、リストに引き続き 2 つのルールがあることを確認します。問題がある場合は、このラボの手順をたどって問題を修正します。



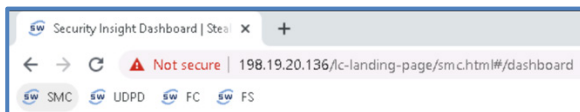
シナリオのまとめ

導入環境における Stealthwatch アプライアンスの残りの設定が完了しました。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。コグニティブが有効化され、設定済みの DNS サーバにアプライアンスがアクセスできることが確認されました。アプライアンスが NTP サーバにアクセスできることも確認されました。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 syslog データを Stealthwatch が処理できるように、UDP とその転送ルールが設定されました。

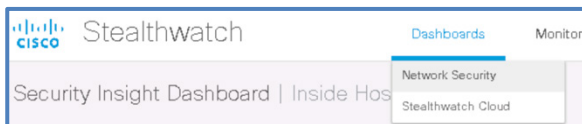
シナリオ 3. SMC および Central Management の追加設定

ここまででアプライアンス（フローセンサー、UDP Director、フローコレクタ）の設定は完了しましたが、ソリューションがお客様にとって適切に機能するように、SMC で追加の設定を行う必要があります。SMC Web UI を使用して、お客様のために Stealthwatch の追加の設定を行います。

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。
 - a. まだ SMC Web UI に接続していない場合は、Chrome で **SMC** のブックマークを選択し、SMC のインターフェイスにアクセスします。
 - b. 認証を求められたら、次のログイン情報を使用します。
 - i. [ユーザ名 (Username)]: **admin**
 - ii. [パスワード (Password)]: **C1sco12345**



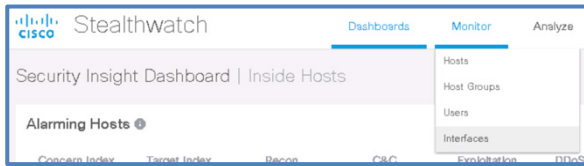
2. SMC にログインしたら、[ダッシュボード (Dashboards)] > [ネットワークセキュリティ (Network Security)] に移動します。



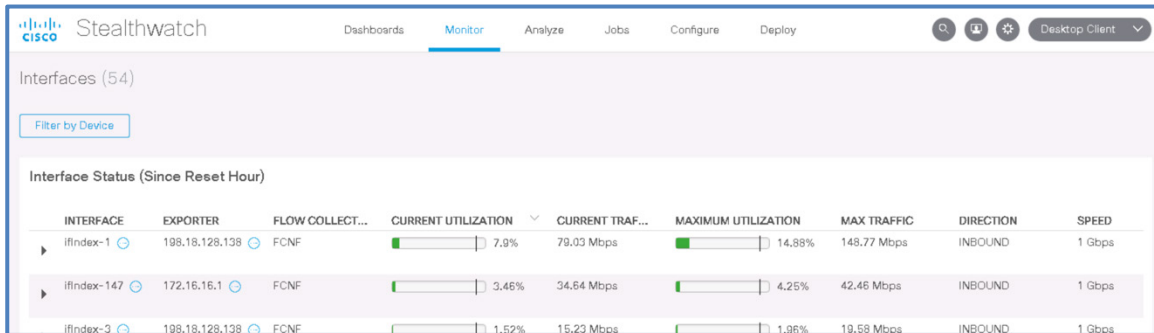
3. [フローコレクショントレンド (Flow Collection Trend)] セクションが表示されるまで、このダッシュボードを下にスクロールします。このウィジェットにフローデータが表示され始めます。トレンドグラフの右側にある **データにマウスポインタを合わせると**、インバウンドフローに関する情報が表示されます。UDP Director の設定が完了して同期された後、フローが Stealthwatch に届き始めてからフロー数が増加するまでに 1 ~ 2 分かかる場合があります。トレンドグラフィックに 1 秒あたり少なくとも数百のフローが表示されるまで、ページを更新しながら待ちます。



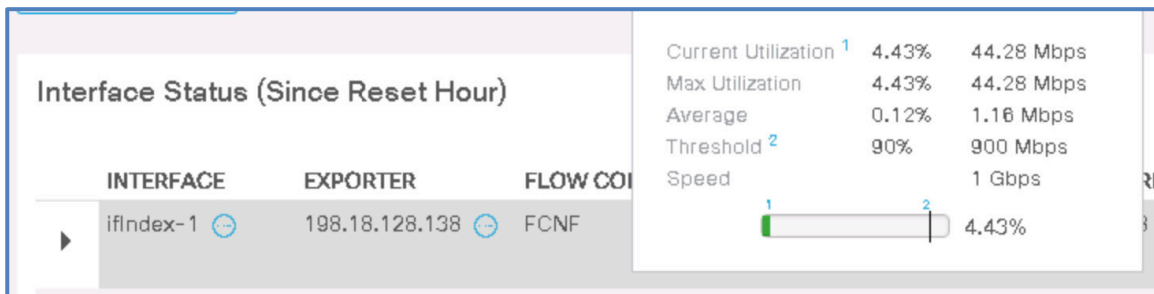
4. ページの上部にあるメニューから、[モニタ (Monitor)] > [インターフェイス (Interfaces)] を選択します。



- a. リストに多数のインターフェイスが表示されます。これらのインターフェイスは、お客様のネットワークからの NetFlow を報告しています。



- b. [現在の使用率 (Current Utilization)] のバー/パーセンテージのいずれかにマウスを合わせると、詳細が表示されます。

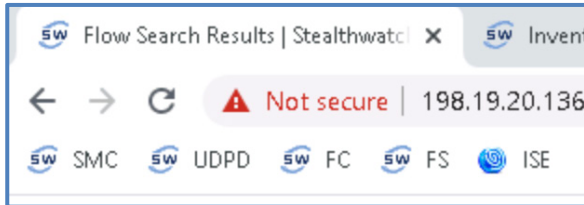


- c. 期待するデータの少なくとも一部が表示されることが確認できたため、残りの SMC 設定タスクを続行できます。

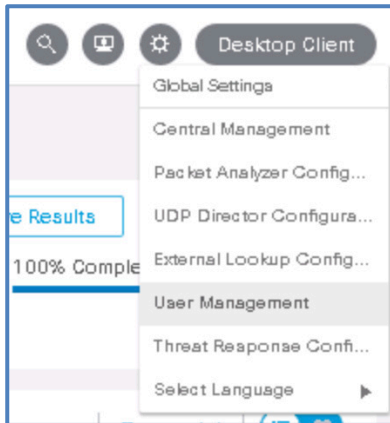
アカウントの作成

ここまでのすべてのアクティビティでは、デフォルトの admin アカウントを使用してきました。最初にこのアカウントに電子メールアドレスを追加します。次に、後のシナリオで使用する汎用 SOC (セキュリティ オペレーション センター) アカウントを作成します。

1. Chrome で **SMC** Web インターフェイスに戻ります (必要に応じて SMC ブックマークを使用)。必要に応じて **admin** および **C1sco12345** を使用してログインします。

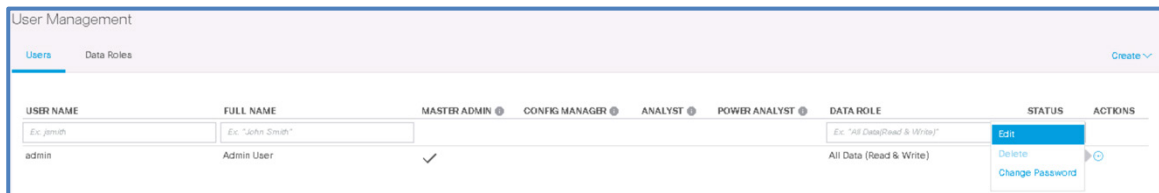


2. 歯車アイコンをクリックし、[ユーザ管理 (User Management)] をクリックします。



3. admin アカウントに電子メールアドレスを追加します。

- a. admin ユーザアカウントの [アクション (Actions)] アイコンをクリックし、[編集 (Edit)] をクリックします。



- b. 電子メールアドレスフィールドに stealthwatchfe@dcloud.local を入力し、[保存 (Save)] をクリックします。

User Management | User

USER NAME *

admin

FULL NAME

Admin User

EMAIL

stealthwatchfe@dcloud.local

4. お客様のセキュリティ オペレーション センター用の汎用アカウントも作成し、後で SOC の大画面でダッシュボードを実行する場合に使用できるようにしましょう。

- a. [作成 (Create)] をクリックし、[ユーザ (Users)] をクリックします。

Create ▾

User

Data Role

STATUS ACTIONS

- b. まず、次のパラメータを設定します。

- i. [ユーザ名 (User Name)] : **SOC**
- ii. [電子メール (Email)] : **soc@dcloud.local**
- iii. [認証サービス (Authentication Service)] : **local**
- iv. [パスワード (Password)] : **C1sco12345**
- v. [パスワードの確認 (Confirm Password)] : **C1sco12345**

USER NAME *	AUTHENTICATION SERVICE
SOC	local
FULL NAME	PASSWORD ● *

EMAIL	CONFIRM PASSWORD *
soc@dcloud.local

- c. 次に、ロール設定までスクロールダウンし、次のように設定します。

- i. [Web] > [Web のロール (Web Roles)] : [パワーアナリスト (Power Analyst)]
- ii. [デスクトップ (Desktop)] > [デスクトップクライアントのロール (Desktop Client Roles)] : [セキュリティアナリスト (Security Analyst)]

i You must select a minimum of one web role and one desktop client role.

Web Desktop

WEB ROLES * Compare

Configuration Manager Analyst Power Analyst

Web Desktop

Desktop Client Manager ⓘ

DESKTOP CLIENT ROLES * To manage these roles, access the SMC Desktop Client.

All Configuration Manager Network Engineer Security Analyst StealthWatch Power User

d. [保存 (Save)]をクリックします。

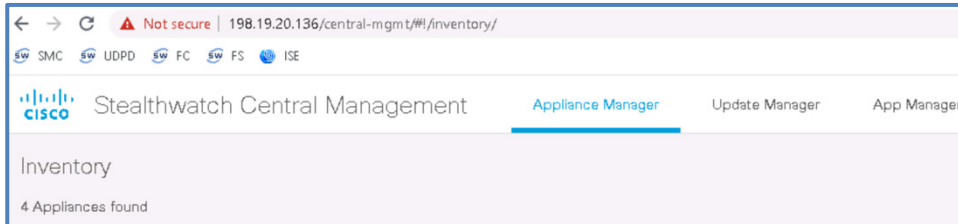
5. 両方のユーザが正常に表示されたら、ラボシナリオで次に進むことができます。

USER NAME	FULL NAME	MASTER ADMIN ⓘ	CONFIG MANAGER ⓘ	ANALYST ⓘ	POWER ANALYST ⓘ
<i>Ex. jsmith</i>	<i>Ex. "John Smith"</i>				
admin	Admin User	✓			
SOC					✓

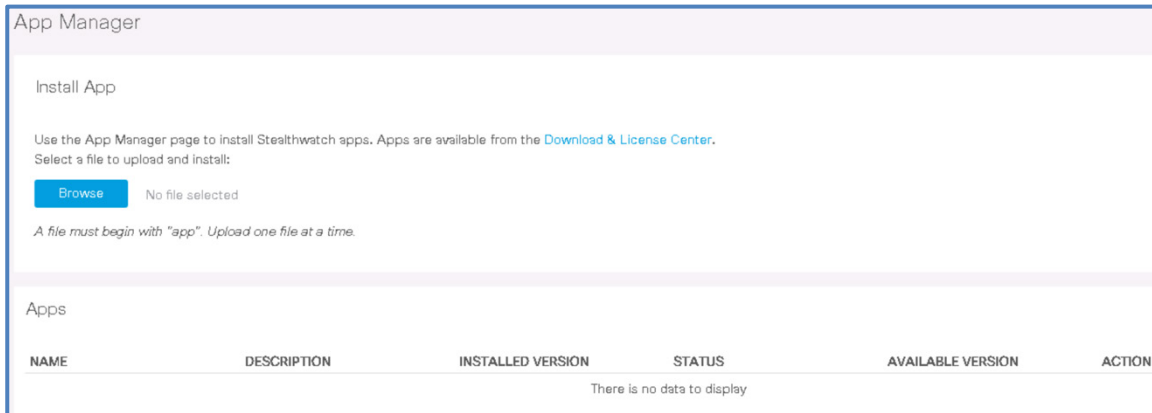
Stealthwatch アプリケーションのインストール

バージョン 7.x では、Stealthwatch アプリケーションを導入環境に追加できます。アプリケーションを使えば、Stealthwatch が受信したデータをさまざまな方法で使用できます。また、フルバージョンのアップグレードなしに、必要に応じて導入環境に追加できます。ここでは、後で使用する 4 つの Stealthwatch アプリケーションをインストールします。

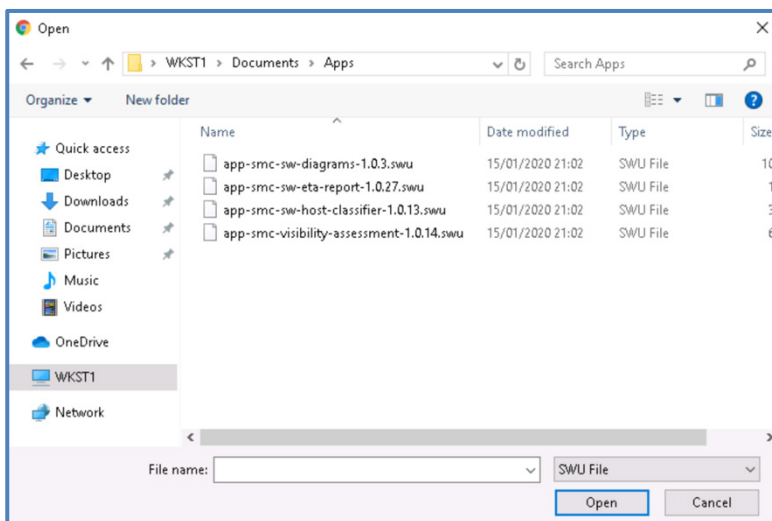
1. [SMC Central Management] の [インベントリ (Inventory)] ページに戻り、[アプリケーションマネージャ (App Manager)] をクリックします。



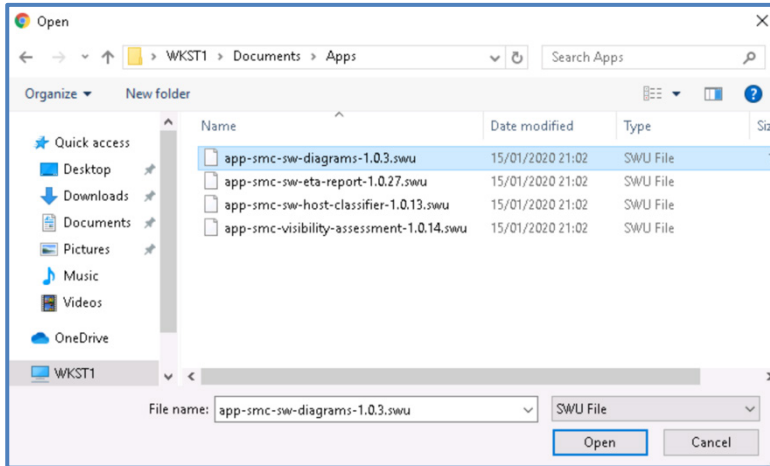
2. 現在インストールされているアプリケーションがないことがわかります。[Browse (参照)] をクリックします。



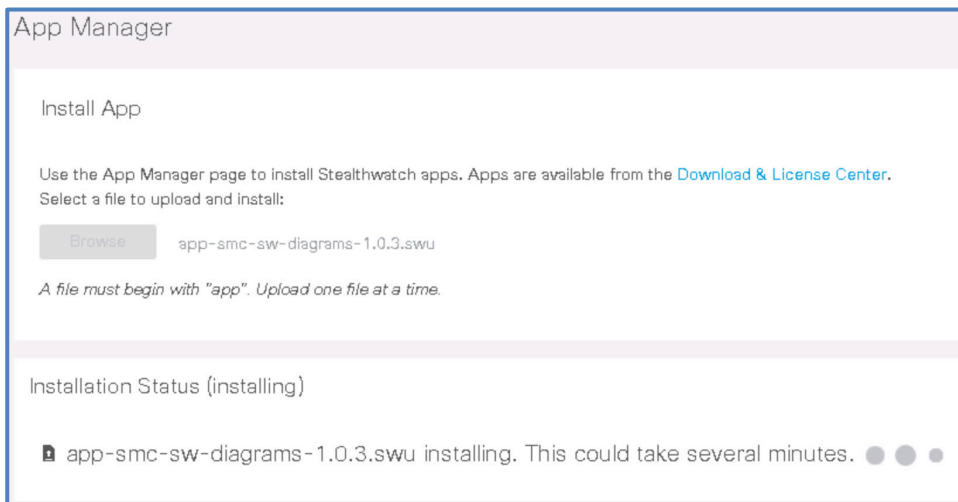
3. [WKST1] > [ドキュメント (Documents)] > [Apps (アプリケーション)] に移動します。



4. **app-smc-sw-diagrams-1.0.3.swu**、[開く (Open)] の順にクリックします。



5. アップロードの進行状況バーと [インストールステータス (Installation Status)] の通知が表示されます。



6. アプリケーションがインストールされると、このページの下部にある [アプリケーション (Apps)] リストに表示されます。

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
Network Diagrams	A visual tool for improving network visibility and detection	1.0.3	UpToDate	-	Uninstall

7. 2 つ目のアプリケーションをインストールします。

- [参照 (Browse)] をクリックします。
- app-smc-sw-eta-report-1.0.27.swu** をクリックします。
- [開く (Open)] をクリックします。
- インストールが完了し、アプリケーションがリストに表示されるまで待ちます。

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
ETA Cryptographic Audit	Use Encrypted Traffic Analytics (ETA) to determine any TLS policy violations and pinpoint weak encryption	1.0.27	UpToDate	-	Uninstall
Network Diagrams	A visual tool for improving network visibility and detection	1.0.3	UpToDate	-	Uninstall

8. 3 つ目のアプリケーションをインストールします。

- [参照 (Browse)] をクリックします。
- app-smc-sw-host-classifier-1.0.13.swu** をクリックします。
- [開く (Open)] をクリックします。
- インストールが完了し、アプリケーションがリストに表示されるまで待ちます。

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
Host Classifier	Dynamic discovery and classification of core assets within the network	1.0.13	UpToDate	-	Uninstall
ETA Cryptographic Audit	Use Encrypted Traffic Analytics (ETA) to determine any TLS policy violations and pinpoint weak encryption	1.0.27	UpToDate	-	Uninstall
Network Diagrams	A visual tool for improving network visibility and detection	1.0.3	UpToDate	-	Uninstall

9. 4 つ目のアプリケーションをインストールします。

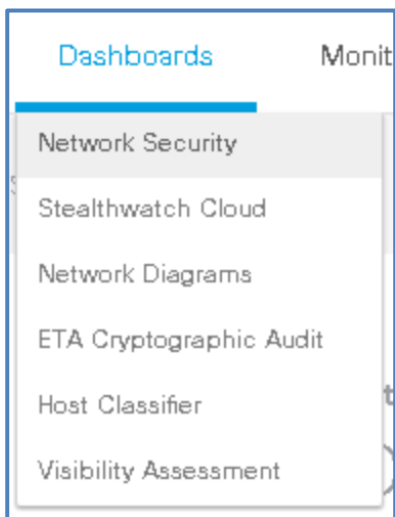
- [参照 (Browse)] をクリックします。
- app-smc-visibility-assessment-1.0.14.swu** をクリックします。
- [開く (Open)] をクリックします。
- インストールが完了し、アプリケーションがリストに表示されるまで待ちます。

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
Visibility Assessment	Quickly gain insights into the areas of security risks within the network.	1.0.14	UpToDate	-	Uninstall
Host Classifier	Dynamic discovery and classification of core assets within the network	1.0.13	UpToDate	-	Uninstall
ETA Cryptographic Audit	Use Encrypted Traffic Analytics (ETA) to determine any TLS policy violations and pinpoint weak encryption	1.0.27	UpToDate	-	Uninstall
Network Diagrams	A visual tool for improving network visibility and detection	1.0.3	UpToDate	-	Uninstall

10. Chrome で **SMC** のブックマークをクリックし、SMC の Web インターフェイスに戻ります。



11. [ダッシュボード (Dashboards)] メニューにマウスポインタを合わせると、利用可能な 4 つの新しいアプリケーション/ダッシュボードが表示されます。



12. これらのダッシュボードについては、まだ確認する必要はありません。お客様のネットワークからさらに NetFlow が受信された後で確認します。

シナリオのまとめ

このシナリオでは、インバウンドの NetFlow の少なくとも一部が処理されていることを確認しました。特定のエクスポートの問題（ある場合）を特定するために、この後さらに詳しく見ていきます。また、ユーザアカウントの作成や、お客様導入環境への 4 つの Stealthwatch アプリの追加など、お客様のために Stealthwatch の追加のカスタマイズも実施しました。

シナリオ 4. ホストグループの設定

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 スペース、承認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。ラボを実施する間、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。お客様から提供された情報が正確でない場合があることを覚えておくことが重要です。

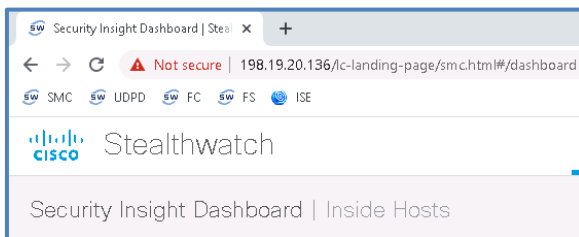
説明	IP アドレス
DNS サーバ	10.10.30.15 10.10.30.16
脆弱性スキャナ	10.203.0.207
メールサーバ	10.10.30.23
タイムサーバ	10.10.30.10
パブリック IP アドレス空間	209.182.184.0/24
アトランタ	10.201.0.0/16
IT	198.19.30.0/24
IT サーバ	198.19.20.0/24
従業員用 VPN	198.19.10.100-103 198.19.10.200-203
PCI デバイス	10.201.3.0/24

パブリック IP 空間の設定

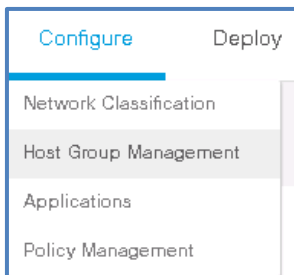
注：ホストグループには、IP アドレスデータだけを含めることができます（MAC アドレスまたは DNS 名は許可されていません）。IP アドレスは、いくつかの異なる形式で入力できます。10.1.2.3 など、1 つの IP アドレスを入力できます。192.168.1.1-57、10.1-167.1.1、172.22.0-255.0-255 などのように、1 つのオクテット内で、ハイフンで連結して範囲を指定できます。完全な IP アドレス - 完全な IP アドレス（192.168.1.1-192.168.1.254）という形式では、範囲を指定しないでください。範囲は 1 つのオクテット内である必要があります（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、パブリック IP 空間内で通信する通常のネットワークトラフィックによって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、分類は正しく行ってください。

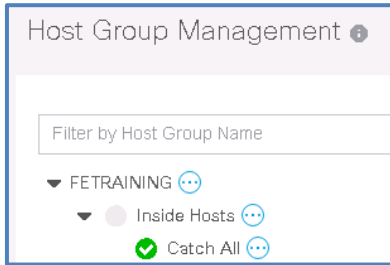
1. SMC Web インターフェイス **WKST1** の [セキュリティ分析ダッシュボード (Security Insight Dashboard)] Web ページに戻るか、Chrome Web ブラウザのブックマークバーにある SMC のエントリをクリックして Web インターフェイスを開きます。



2. [設定 (Configure)] メニューをクリックして、[ホストグループ管理 (Host Group Management)] を選択します。



3. [内部ホスト (Inside Hosts)] オブジェクトを展開し、[すべてを捕捉 (Catch All)] ホストグループを選択します。



4. [すべてを捕捉 (Catch All)] グループを選択した状態で、[編集 (Edit)] ボタンをクリックします。



5. お客様は、従来の RFC1918 IP 空間に加えて、パブリックおよび内部の IP アドレス空間を 209.182.184.0/24、198.19.10.0/24、198.19.20.0/24、198.19.30.0/24 として集約できると述べています。この追加の IP 範囲情報を [すべてを捕捉 (Catch All)] グループに入力します。

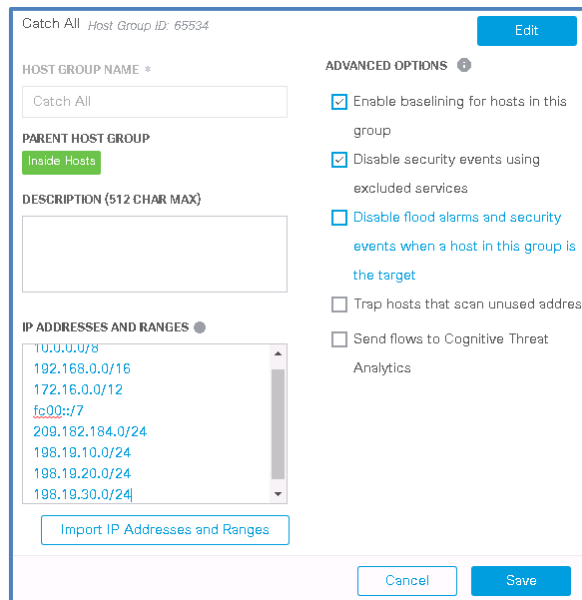
- [ホストグループ管理 (Host Group Management)] ウィンドウの [IP アドレスと範囲 (Addresses and Ranges)] セクションで、**Enter** を使用して、現在のリストの末尾に新しい空白行を作成します。
- [すべてを捕捉 (Catch All)] ホストグループに次の 4 つの IP 範囲を追加します。

209.182.184.0/24

198.19.10.0/24

198.19.20.0/24

198.19.30.0/24



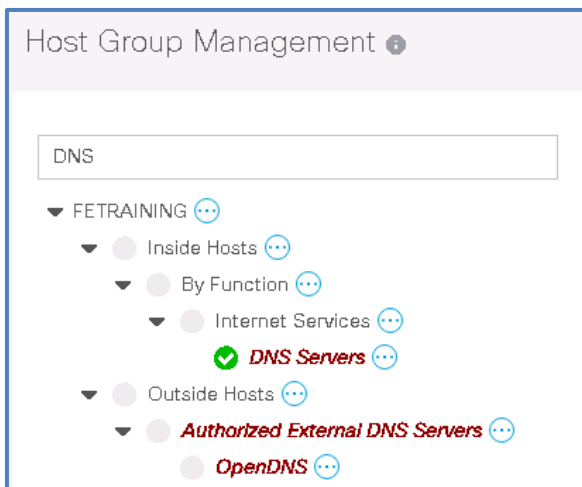
- [保存 (Save)] をクリックします。

6. これで、お客様の内部およびパブリックアドレス空間が、Stealthwatch 内で内部ホストの一部として分類されました。ラボの次の手順に進み、現在のウィンドウは開いたままにしておきます。

Web UI での追加ホストグループの設定

お客様は、ホスト分類のために追加の IP データを提供しています。SMC で追加のホストグループを設定します。

1. [ホストグループ管理 (Host Group Management)] 画面で、[ホストグループ名でフィルタ (Filter by Host Group Name)] スペースをクリックし、**DNS** と入力して結果をフィルタリングします。



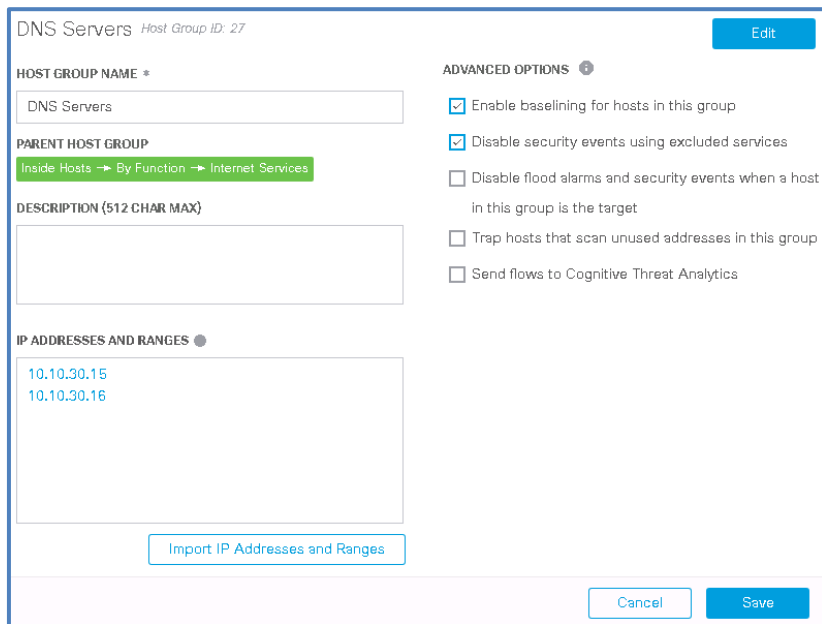
2. [DNS サーバ (DNS Servers)] ホストグループを選択し、[編集 (Edit)] ボタンをクリックします。



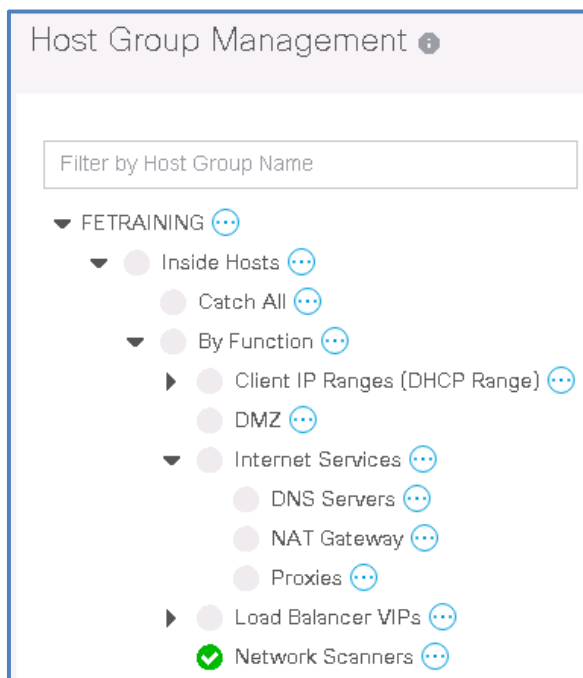
3. [ホストグループ管理 (Host Group Management)] ウィンドウの [IP アドレスと範囲 (IP Addresses and Ranges)] セクションで、ホストグループに次の IP アドレスを追加し、[保存 (Save)] をクリックします。

10.10.30.15

10.10.30.16



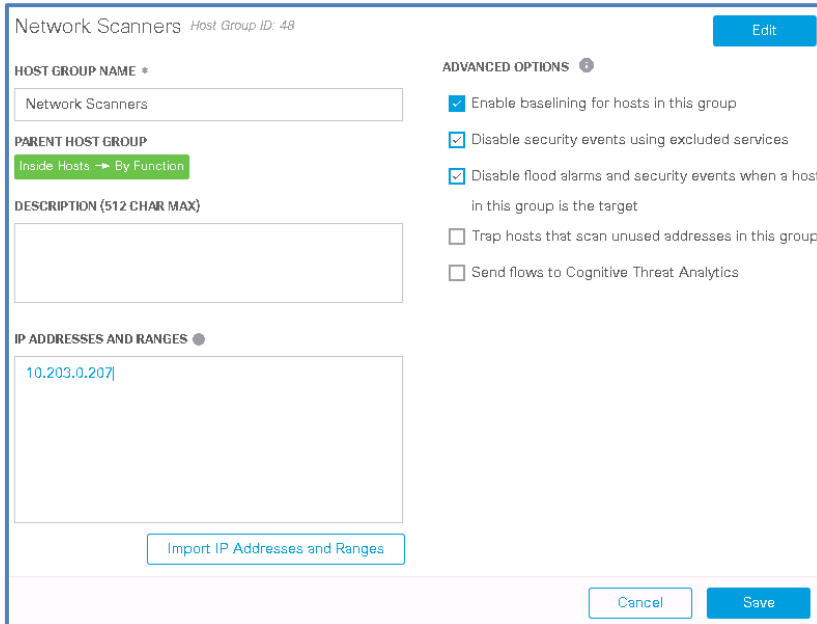
4. ホストグループのツリーで [ネットワークスキャナ (Network Scanners)] ホストグループを見つけます。



5. [ネットワークスキャナ (Network Scanners)] ホストグループを選択し、[編集 (Edit)] ボタンをクリックします。

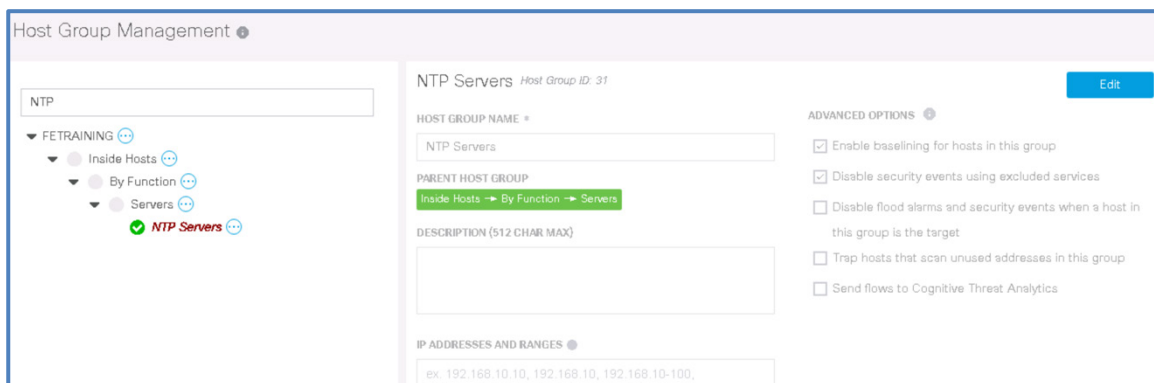


6. [ホストグループの管理 (Host Group Management)] ウィンドウの [IP アドレスと範囲 (IP Addresses and Ranges)] セクションで、ホストグループに IP アドレス **10.203.0.207** を追加し、[保存 (Save)] をクリックします。

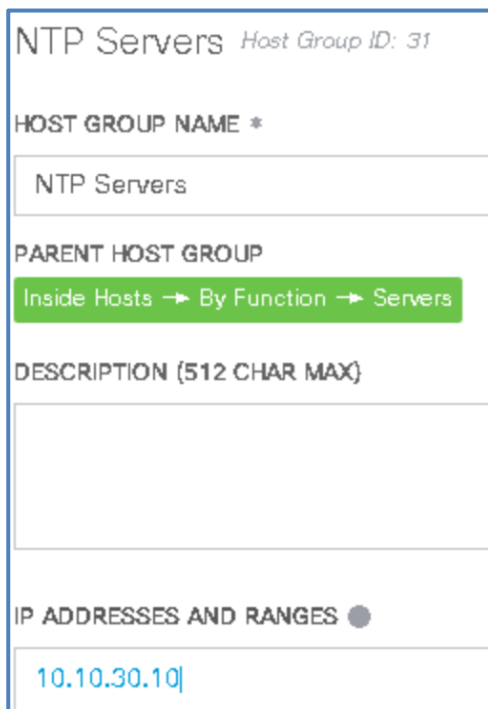


注：[ネットワークスキャナ (Network Scanners)] ホストグループは複数のポリシーから参照されています。通常はネットワーク スキャン アクティビティを実行するホストによってトリガーされるさまざまなタイプのアラームを自動的に停止するために使用されます。お客様の認可済み脆弱性スキャナの IP アドレスを [ネットワークスキャナ (Network Scanners)] ホストグループに設定することで、有効な動作に対するアラームがアクティブになるのを停止することができます。これにより、さらに多くの IP 空間が該当するホストグループに割り当てられるため、お客様のネットワーク上のホストを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

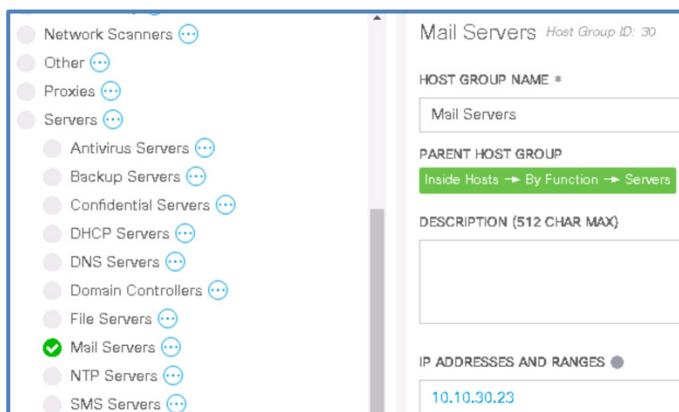
- 再度、[ホストグループ名でフィルタ (Filter by Host Group Name)] フィールドを使用して、[NTP サーバ (NTP Servers)] ホストグループを探します。次に、[NTP サーバ (NTP Servers)] オブジェクトをクリックして、IP アドレスがまだ設定されていないことを確認します。



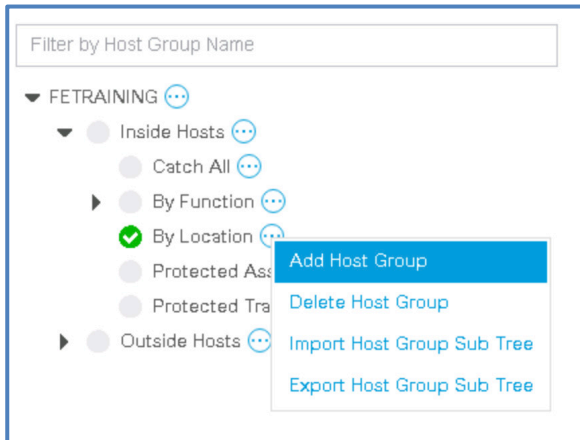
- 右上隅の [編集 (Edit)] ボタンをクリックして、フォームをアクティブにします。[IP アドレスと範囲 (Addresses and Ranges)] テキストボックスに、**10.10.30.10** と入力します。入力したら、[保存 (Save)] をクリックします。



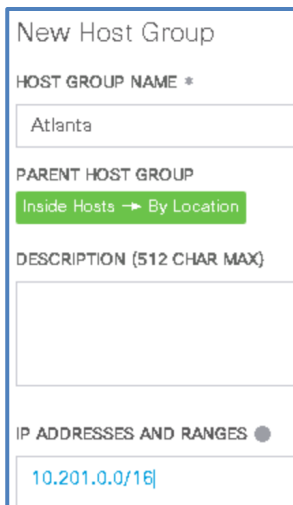
9. [メールサーバ (Mail Servers)] ホストグループを見つけ、[編集 (Edit)] をクリックして、IP アドレス **10.10.30.23** を追加します。完了したら、[Save (保存)] をクリックします。



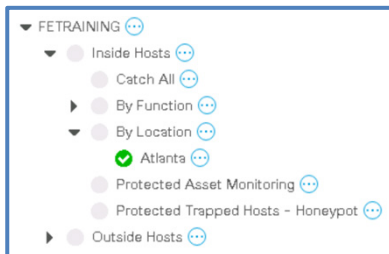
10. 次に、エンタープライズツリーの [内部ホスト (Inside Hosts)] セクション内の [ロケーション別 (By Location)] ホストグループの下にネストされるように、ロケーションベースのホストグループを追加します。
11. ツリーで [ロケーション別 (By Location)] ホストグループを探します (必要に応じて [検索 (Search)] を使用します) 。
12. [ロケーション別 (By Location)] オブジェクトを選択し、右にある円形のアクションアイコンをクリックします。表示されるメニューから [ホストグループの追加 (Add Host Group)] を選択します。



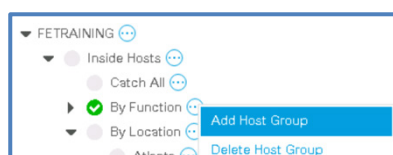
13. 右側のペインに表示される [新しいホストグループ (New Host Group)] フォームで、新しいホストグループの名前として **Atlanta** と入力し、[IP アドレスと範囲 (IP Addresses and Ranges)] フィールドに **10.201.0.0/16** と入力します。入力したら、[保存 (Save)] をクリックします。



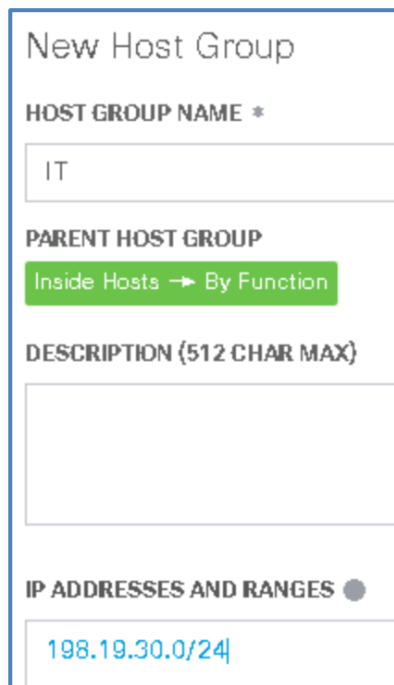
14. 新しいホストグループが、ツリー内の [ロケーション別 (By Location)] の下にネストされて表示されます。



15. 次に、IT 部門の IP 範囲を分類する必要があります。
- a. [機能別 (By Function)] の右側にある **アクションアイコン** をクリックし、[ホストグループの追加 (Add Host Group)] をクリックします。

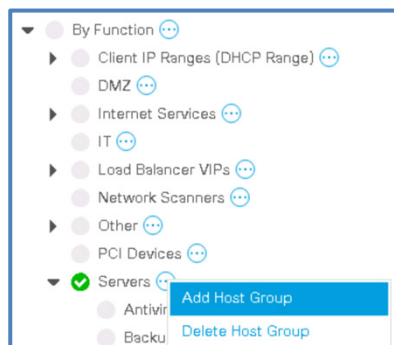


- b. [ホストグループ名 (Host Group Name)]を **IT** に、[IP アドレスと範囲 (IP Addresses and Ranges)]を **198.19.30.0/24** に設定して、[保存 (Save)]をクリックします。

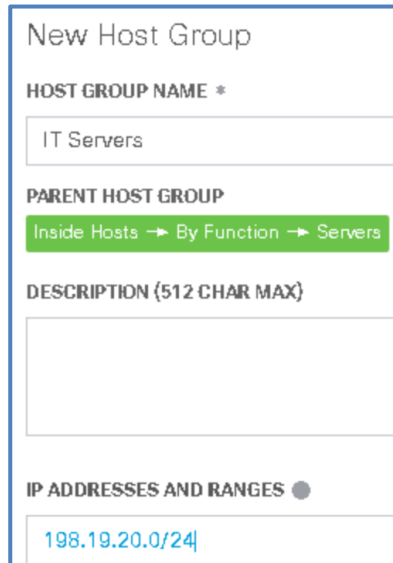


16. また、IT サーバの IP 範囲を分類する必要があります。

- a. [機能別 (By Function)]の下にネストされた[サーバ (Servers)]の右側にあるアクションアイコンをクリックし、[ホストグループの追加 (Add Host Group)]をクリックします。



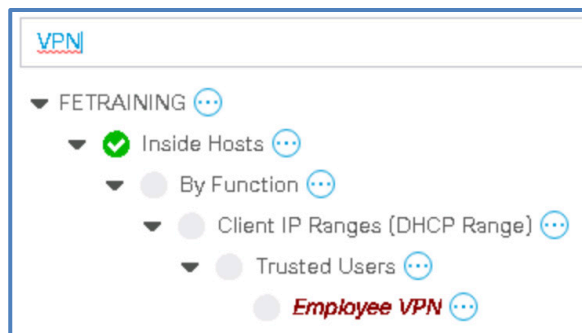
- b. [ホストグループ名 (Host Group Name)]を **IT Servers** に、[IP アドレスと範囲 (IP Addresses and Ranges)]を **198.19.20.0/24** に設定して、[保存 (Save)]をクリックします。



c. [IT サーバ (IT Servers)] ホストグループを変更したら、必ず保存してください。

17. また、従業員 VPN プールの IP 範囲を分類する必要があります。

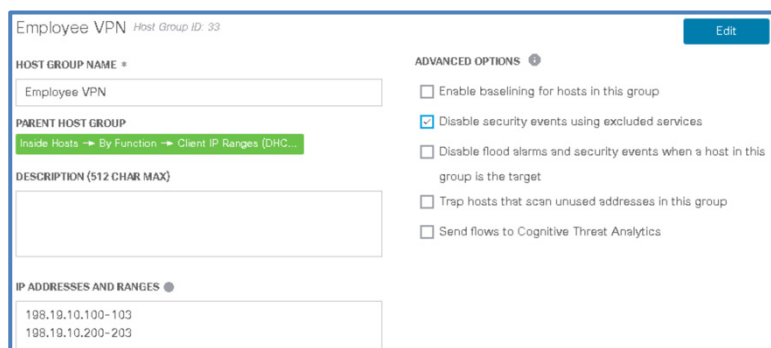
a. 検索フィールドに **VPN** と入力し、**Enter** を押します。



b. [従業員 VPN (Employee VPN)] オブジェクトをクリックしてから [編集 (Edit)] ボタンをクリックして、次の **IP 範囲** を入力します。

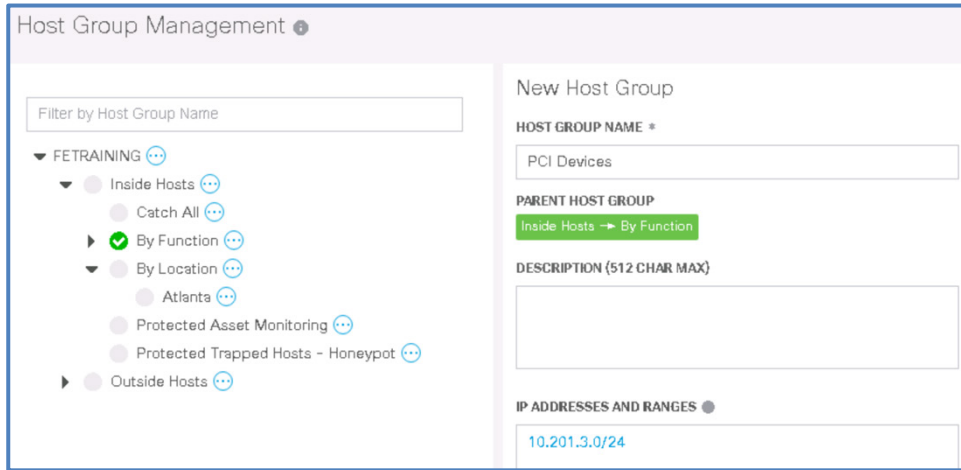
198.19.10.100-103

198.19.10.200-203



c. [保存 (Save)] をクリックします。

18. 前の手順を使用して、**PCI デバイス**という名前の別のホストグループを自分で作成してみましょう。[機能別 (By Function)]ホストグループの下にネストしてください。前の表でお客様が指定した IP 範囲 (**10.201.3.0/24**) を入力します。設定が完了したら、[保存 (Save)]をクリックします。



The screenshot shows the 'Host Group Management' interface. On the left, there is a tree view under 'FETRAINING' with sub-items: 'Inside Hosts', 'Catch All', 'By Function' (selected with a green checkmark), 'By Location', 'Atlanta', 'Protected Asset Monitoring', 'Protected Trapped Hosts - Honeypot', and 'Outside Hosts'. On the right, the 'New Host Group' form is visible. It has the following fields: 'HOST GROUP NAME *' with the value 'PCI Devices'; 'PARENT HOST GROUP' with a dropdown menu showing 'Inside Hosts -> By Function' selected; 'DESCRIPTION (512 CHAR MAX)' which is empty; and 'IP ADDRESSES AND RANGES ●' with the value '10.201.3.0/24'.

19. お客様の指定に従ってホストグループを設定できました。WKST1 システムのすべての **Chrome** ウィンドウを閉じます。

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。Web クライアント インターフェイスの [ホストグループ管理 (Host Group Management)]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 5. シスコルータの NetFlow 設定および検証

お客様は、内部ルータに NetFlow を設定したいと考え、ベストプラクティスに従ってその設定を導入するよう依頼しています。

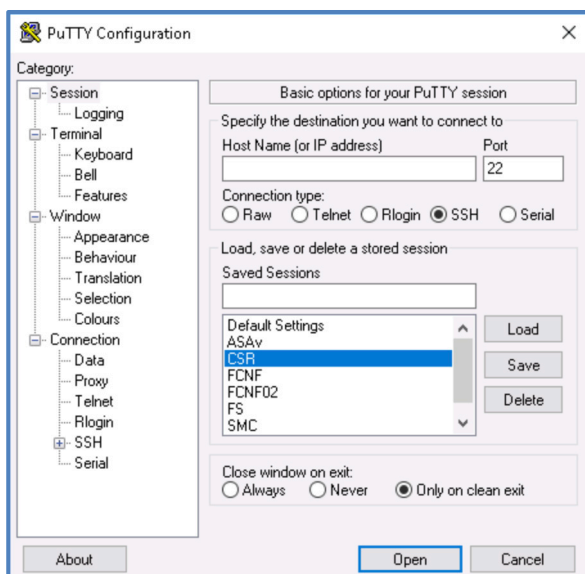
ルータへの NetFlow 設定

Stealthwatch ソリューションと連携するようにシスコのルータを設定します。IOS-XE 16.6.4 コード (dCloud トポロジの CSR) を実行している シスコ クラウド サービス ルータを設定します。ラボ全体で NetFlow と SNMP を設定します。

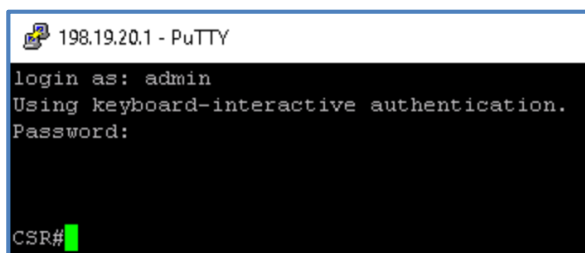
1. **WKST1** システムのデスクトップに戻り、[PuTTY] リンクをクリックします。



2. [CSR] という名前の保存済みセッションをクリックし、[開く (Open)] をクリックします。



3. 「login as:」プロンプトで **admin** と入力し、**Enter** を押します。
4. 「Password:」プロンプトで **C1sco12345** と入力し、**Enter** キーを押します。



5. SSH で正常に認証された場合は、**CSR#** プロンプトが表示されます。

6. まず、次のコマンドを 1 つずつ入力し、各行の最後に Enter を押して、フローレコードを設定します。

```
configure terminal
flow record FLOW_RECORD
description NetFlow record for Stealthwatch
match ipv4 tos
match ipv4 source address
match ipv4 destination address
match transport destination-port
match transport source-port
match interface input
match ipv4 protocol
collect interface output
collect transport tcp flags
collect ipv4 ttl minimum
collect ipv4 ttl maximum
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect ipv4 dscp
exit
```

```
CSR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSR(config)#flow record FLOW_RECORD
CSR(config-flow-record)#description NetFlow record for Stealthwatch
CSR(config-flow-record)#match ipv4 tos
CSR(config-flow-record)#match ipv4 source address
CSR(config-flow-record)#match ipv4 destination address
CSR(config-flow-record)#match transport destination-port
CSR(config-flow-record)#match transport source-port
CSR(config-flow-record)#match interface input
CSR(config-flow-record)#match ipv4 protocol
CSR(config-flow-record)#collect interface output
CSR(config-flow-record)#collect transport tcp flags
CSR(config-flow-record)#collect ipv4 ttl minimum
CSR(config-flow-record)#collect ipv4 ttl maximum
CSR(config-flow-record)#collect counter bytes
CSR(config-flow-record)#collect counter packets
CSR(config-flow-record)#collect timestamp sys-uptime first
CSR(config-flow-record)#collect timestamp sys-uptime last
CSR(config-flow-record)#collect ipv4 dscp
CSR(config-flow-record)#exit
CSR(config)#
```

7. 次のコマンドを1つずつ入力し、各行の最後で Enter を押して、フローエクスポートを設定します。

```
flow exporter FLOW_EXPORTER
description Export NetFlow to Stealthwatch
destination 198.19.20.139
transport udp 2055
template data timeout 30
option interface-table
exit
```

```
CSR(config)#flow exporter FLOW_EXPORTER
CSR(config-flow-exporter)#description Export NetFlow to Stealthwatch
CSR(config-flow-exporter)#destination 198.19.20.139
CSR(config-flow-exporter)#transport udp 2055
CSR(config-flow-exporter)#template data timeout 30
CSR(config-flow-exporter)#option interface-table
CSR(config-flow-exporter)#exit
CSR(config)#
```

8. 次のコマンドを1つずつ入力し、各行の最後で Enter を押して、フローモニタを設定します。

```
flow monitor FLOW_MONITOR
record FLOW_RECORD
exporter FLOW_EXPORTER
cache timeout active 60
cache timeout inactive 15
exit
```



```

CSR(config)#flow monitor FLOW_MONITOR
CSR(config-flow-monitor)#record FLOW_RECORD
CSR(config-flow-monitor)#exporter FLOW_EXPORTER
CSR(config-flow-monitor)#cache timeout active 60
CSR(config-flow-monitor)#cache timeout inactive 15
CSR(config-flow-monitor)#exit
CSR(config)#

```

9. 次のコマンドを入力して、CSR ルーティング プラットフォームのインターフェイスを確認します。

```
do show ip interface brief
```

```

CSR(config)#do show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
GigabitEthernet1  198.19.10.2     YES NVRAM  up      up
GigabitEthernet2  198.19.20.1     YES NVRAM  up      up
GigabitEthernet3  198.19.30.1     YES NVRAM  up      up
CSR(config)#

```

- a. GigabitEthernet2 インターフェイスはアプライアンスと同じ IP 空間にあります。GigabitEthernet1 インターフェイスは ASA と同じ IP 空間にあり、インターネットの方向にあります。GigabitEthernet3 インターフェイスは WKST1 と同じ IP 空間にあります。

10. 次のコマンドを 1 つずつ入力し、各行の最後で Enter を押して、フローモニタをすべてのインターフェイスに割り当てます。

```

interface range gig1-3
ip flow monitor FLOW_MONITOR input
end
write memory

```

```

CSR(config)#interface range gig1-3
CSR(config-if-range)#ip flow monitor FLOW_MONITOR input
CSR(config-if-range)#end
CSR#write memory
Building configuration...
[OK]
CSR#

```

11. **CSR#** プロンプトに戻ります。
12. このデバイスで NetFlow が有効になり、正常に UDP Director に情報が送信されるようになりました。
13. **show flow exporter** と入力し、**Enter** を押します。次の情報が表示されます。送信元 IP アドレスは、エクスポートが Stealthwatch 内で自身を識別する方法であることに注意してください。

```

CSR#show flow exporter
Flow Exporter FLOW_EXPORTER:
  Description:          Export NetFlow to Stealthwatch
  Export protocol:      NetFlow Version 9
  Transport Configuration:
    Destination IP address: 198.19.20.139
    Source IP address:     198.19.20.1
    Transport Protocol:    UDP
    Destination Port:      2055
    Source Port:           53270
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Used
  Export template data timeout: 30
  Options Configuration:
    interface-table (timeout 600 seconds) (active)

CSR#

```

14. また、ローカル CSR キャッシュにすでにフローがあるかどうかを確認することもできます。

- a. `show flow monitor FLOW_MONITOR cache format table` と入力して **Enter** を押します（列の折り返しが発生する場合は、putty ウィンドウのサイズを大きくしてこのコマンドを再度入力することもできます）。

```

CSR#show flow monitor FLOW_MONITOR cache format table
Cache type:          Normal (Platform cache)
Cache size:          200000
Current entries:     72
High Watermark:     111

Flows added:         786
Flows aged:          714
- Active timeout    ( 60 secs) 4
- Inactive timeout  ( 15 secs) 710

IPV4 SRC ADDR      IPV4 DST ADDR      TRNS SRC PORT      TRNS DST PORT      INTF INPUT          IP TOS  IP PROT  tcp flags  intf output
-----
bytes      pkts      time first      time last  ip dscp  ip ttl min  ip ttl max
-----
107.22.210.176    198.19.20.143      443              34532  G11          0x00          6 0x1B      G12
7030
198.19.20.143    3.105.201.232     52614            443  G12          0x00          6 0x1B      G11
1433
52.63.61.11      198.19.20.143      443              60146  G11          0x00          6 0x1B      G12
6267
198.19.20.143    107.22.217.211    39004            443  G12          0x00          6 0x1B      G11
1175
52.63.61.11      198.19.20.143      443              60128  G11          0x00          6 0x1B      G12
6267
3.120.90.227     198.19.20.143      443              48978  G11          0x00          6 0x1B      G12
6264
--More--

```

- b. CSR# プロンプトではなく「--More--」と表示されている場合は、**Q** を押すとプロンプトに戻ります。
- c. CSR# プロンプトが表示されたことを確認します。

15. 最後に、次のコマンドを 1 つずつ入力し、各行の最後で **Enter** を押して、SNMP 読み取り専用アクセスを有効にします。

```
configure terminal
```

```
snmp-server community SupaSecretV2 RO
```

end

write memory

```
CSR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSR(config)#snmp-server community SupaSecretV2 RO
CSR(config)#end
CSR#write memory
Building configuration...
[OK]
CSR#
```

16. [Putty] ウィンドウを閉じます。

17. ラボの次の部分に進んで、NetFlow レコードが受信されていることを検証します。

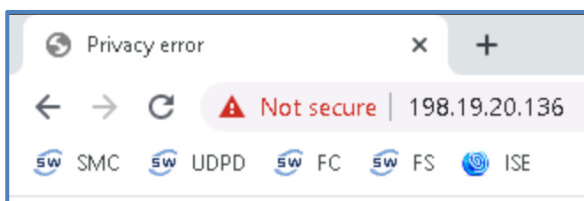
ルータでの NetFlow の検証

お客様環境の CSR ルータで NetFlow が設定されたので、その機能を検証できます。

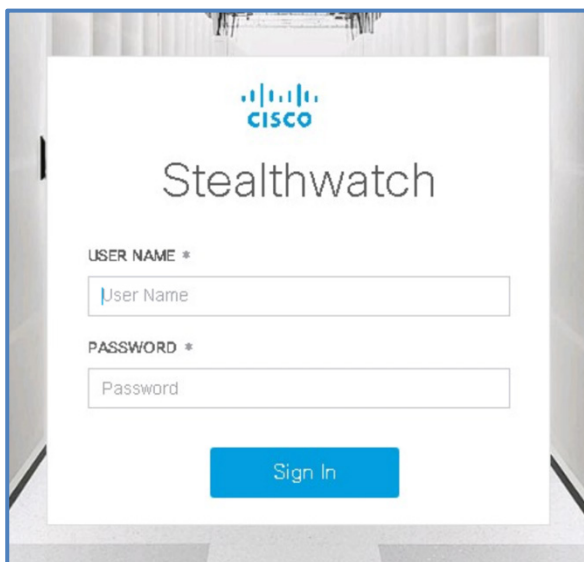
1. まず、残りのラボシステムの CSR の反対側にある WKST1 からの接続をいくつか生成します。これらの接続により、CSR は関連する NetFlow レコードを作成して UDP Director に転送し、UDP Director はそれらをフローコレクタに転送します。
2. WKST1 のデスクトップにあるショートカットを使用して **Chrome** Web ブラウザを開きます。



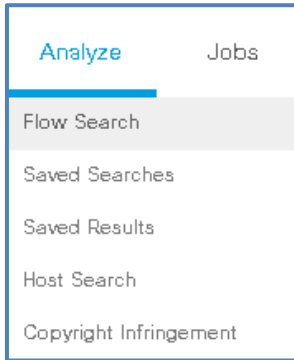
3. Chrome で **SMC** のブックマークを選択し、SMC の Web インターフェイスにアクセスします。



4. 以下のクレデンシャル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 (User Name)] : **admin**
 - b. [パスワード (Password)] : **C1sco12345**



5. [分析 (Analyze)] メニューをクリックし、[フロー検索 (Flow Search)] を選択します。



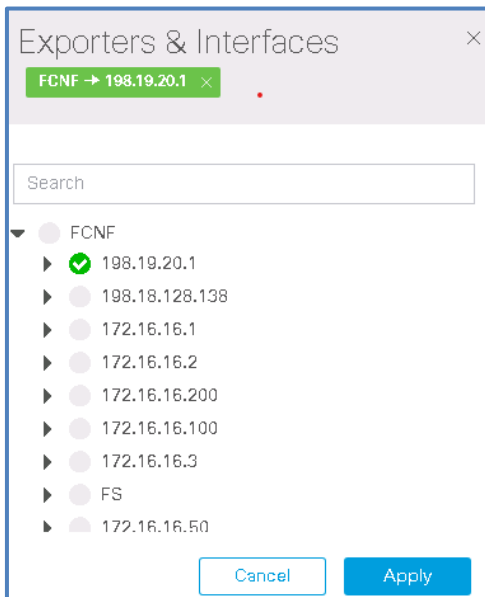
6. [拡張接続オプション (Advanced Connection Options)] をクリックして展開します。



7. [エクスポートとインターフェイス (Exporters & Interfaces)] セクションが表示されるまで下にスクロールし、[選択 (Select)] ボタンをクリックします。



8. [FCNF] オブジェクトを展開し、[198.19.20.1] エクスポートを選択して、[適用 (Apply)] をクリックします。



9. [フロー検索 (Flow Search)] で、CSR デバイスから受信したフローのみを表示するように設定しました。ウィンドウの上部までスクロールし、次のようにフィルタが表示されていることを確認して続行します。

Flow Search ⓘ

Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: Either (Orientation)

Connection: All (Flow Direction) FCNF → 198.19.20.1 ✕

10. ページの右上隅の [検索 (Search)] ボタンをクリックします。



11. 検索結果にフローレコードが返されていることを確認します。次のようにフローレコードが表示されていれば、エクスポートがフローコレクタに有効なフローデータを送信していて、フローコレクタがデータを処理できることがわかります。結果が表示されない場合は、根本原因を特定するための追加のトラブルシューティングが必要になります。検索でフローレコードが返された場合は、残りのラボを続行します。フローレコードが返されない場合は、検索フィルタが正しいことを確認し、1 ~ 2 分待ってからもう一度試してください。UDP ルールが正しいことを確認し、最後に CSR エクスポートの設定を確認してから続行してください。

Flow Search Results (81)

Edit Search Last 5 minutes (Time Range) 2,000 (Max Records) Save Search Save Results Start New Search

Subject: Either (Orientation) 100% Complete Delete Search

Connection: All (Flow Direction) FCNF → 198.19.20.1

Manage Columns Summary Export More

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER
Ex. 06/09/2	Ex. <=50min4t	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. "Corporate"	Ex. <=50M	Ex. 10.255.25	Ex. .2
Mar 4, 2020 12:01:03 AM (16hr 5min 16s ago)	16hr 3min 56s	198.19.20.143	54074/TCP	IT Servers	59.98 K	HTTPS (unclassified)	557 K	107.22.217.211	443/T
Mar 4, 2020 12:01:07 AM (16hr 5min 12s ago)	16hr 3min 52s	198.19.20.143	55466/TCP	IT Servers	60.4 K	HTTPS (unclassified)	554.19 K	107.22.247.3	443/T
Mar 4, 2020 12:01:08 AM (16hr 5min 11s ago)	16hr 3min 51s	198.19.20.143	53306/TCP	IT Servers	59.7 K	HTTPS (unclassified)	553.42 K	107.22.210.176	443/T

シナリオのまとめ

このシナリオでは、Cisco IOS ルータで NetFlow を設定し、検証しました。次のラボに進むことができます。

シナリオ 6. シスコルータの ETA 設定および検証

お客様は、レポートされたデータ内に ETA フローフィールドを含めることで、暗号化コンプライアンスに対応するとともに、ネットワーク内の暗号化された悪意のあるフローを検出する機能についてご存知です。そのため、ネットワークデバイスで ETA を設定し、レポートメカニズムを使用できるように設定を依頼されています。

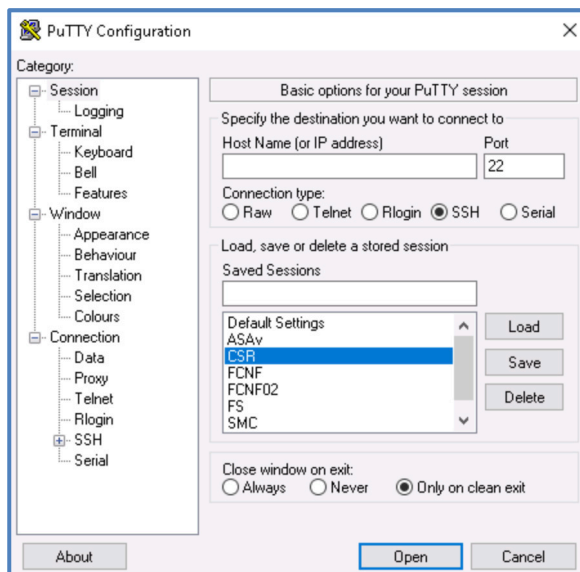
ルータでの ETA 設定

ここでは、ラボのルータで暗号化トラフィック分析 (ETA) を設定します。IOS-XE 16.6.4 コード (dCloud トポロジの CSR) を実行している シスコクラウド サービス ルータを設定します。

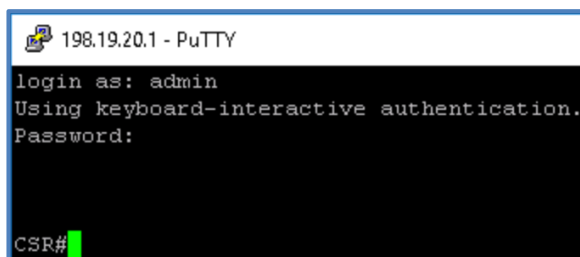
1. リモート コントロール セッションを介して **WKST1** システムのデスクトップに戻り、[Putty] リンクをクリックします。



- a. [CSR] という名前の保存済みセッションをクリックし、[開く (Open)] をクリックします。



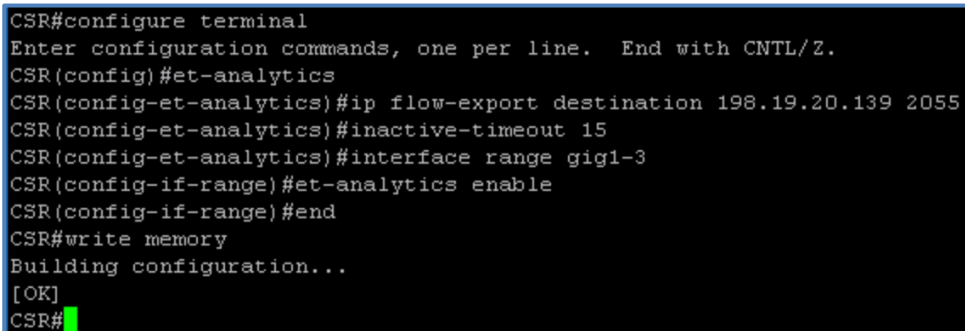
- i. 「login as:」プロンプトで **admin** と入力し、**Enter** を押します。
- ii. 「Password:」プロンプトで **C1sco12345** と入力し、**Enter** を押します。



- b. SSH で正常に認証された場合は、**CSR#** プロンプトが表示されます。

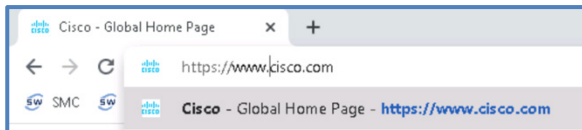
- まず、次のコマンドを 1 つずつ入力し、各行の最後に Enter を押して、フローレコードを設定します。

```
configure terminal
et-analytics
ip flow-export destination 198.19.20.139 2055
inactive-timeout 15
interface range gig1-3
et-analytics enable
end
write memory
```

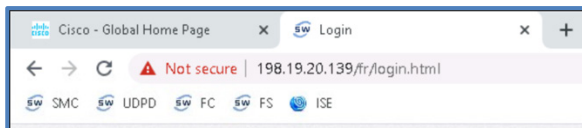


```
CSR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSR(config)#et-analytics
CSR(config-et-analytics)#ip flow-export destination 198.19.20.139 2055
CSR(config-et-analytics)#inactive-timeout 15
CSR(config-et-analytics)#interface range gig1-3
CSR(config-if-range)#et-analytics enable
CSR(config-if-range)#end
CSR#write memory
Building configuration...
[OK]
CSR#
```

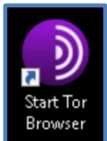
- Chrome** で新しいタブを開き、<https://www.cisco.com> に移動します。ページをロードしている間に、次の手順に進みます。



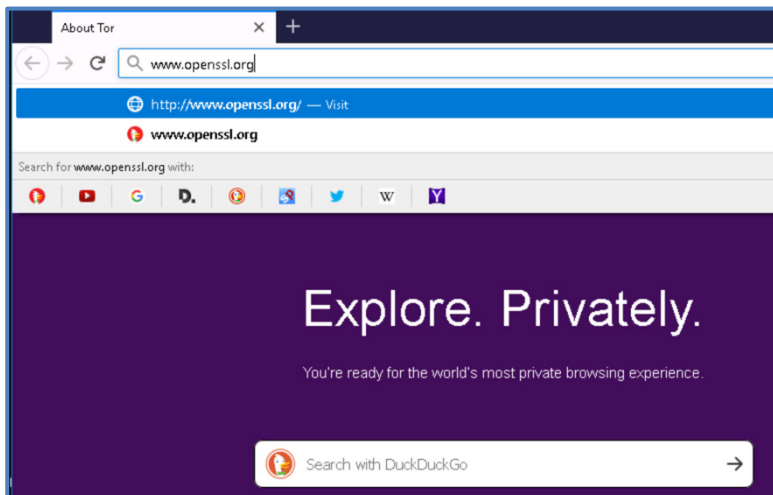
- 新しい **Chrome** タブを開き、ブックマークを使用して **UDPD** に移動します。



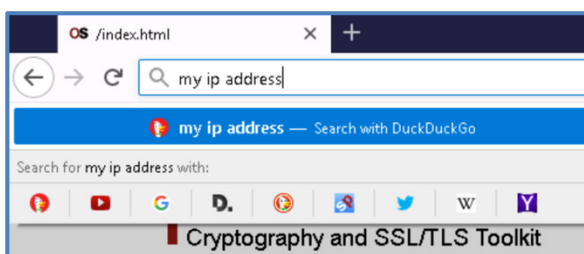
- Chrome** と、開いているすべての **Putty** ウィンドウを閉じます。
- WKST1 のデスクトップで、[Tor ブラウザの起動 (Start Tor Browser)] をダブルクリックします。



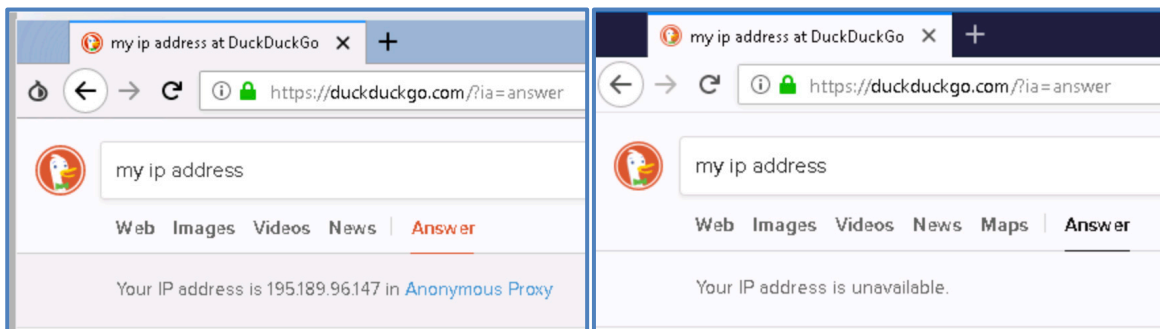
- Tor ブラウザを使用すると、インターネットに安全に接続できます。Tor ブラウザの上部の URL バーから、www.openssl.org に移動します。



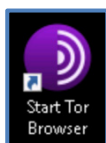
6. ページがロードされたら、ナビゲーションフィールドに **my ip address** と入力し、**Enter** を押します。



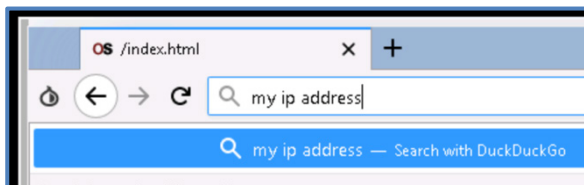
7. 匿名化された Tor の IP アドレスを示す結果が表示され、「匿名プロキシ (Anonymous Proxy)」という説明が付く可能性があります。場合によっては、「IP アドレスを確認できません (Your IP address is unavailable)」と表示され、可能性の高い国や接続元だけがヒントとして表示されます。



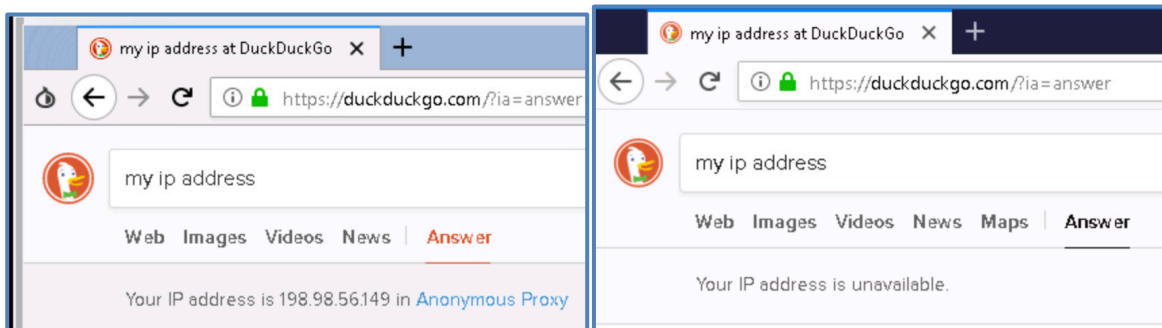
8. Tor ブラウザを閉じます。



9. WKST1 のデスクトップから別の **Tor ブラウザ** を開きます。
10. ナビゲーションフィールドに **my ip address** と入力し、**Enter** を押します。



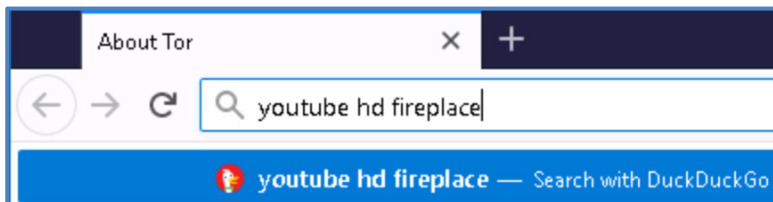
11. 新しい IP アドレス、または IP アドレスが確認できないことを示すメッセージが表示されます。



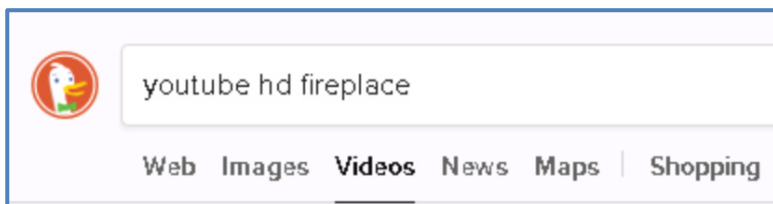
12. Tor ブラウザを閉じます。

13. WKST1 のデスクトップからさらに別の Tor ブラウザを開きます。

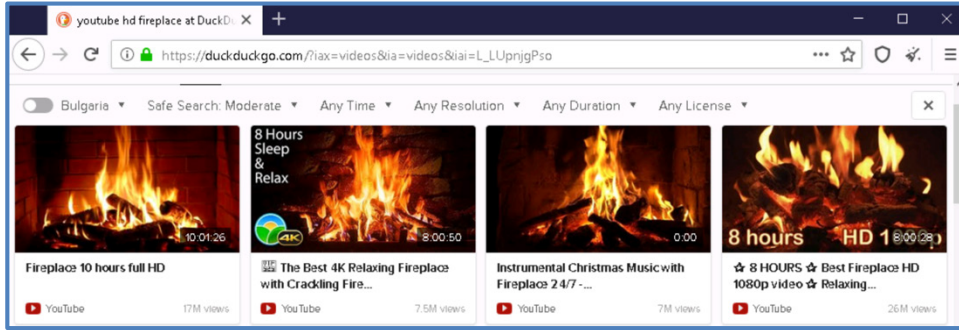
14. Tor Web ブラウザで、最後にもう 1 つページを開きます。検索バーに **youtube hd fireplace** と入力し、**Enter** を押します。



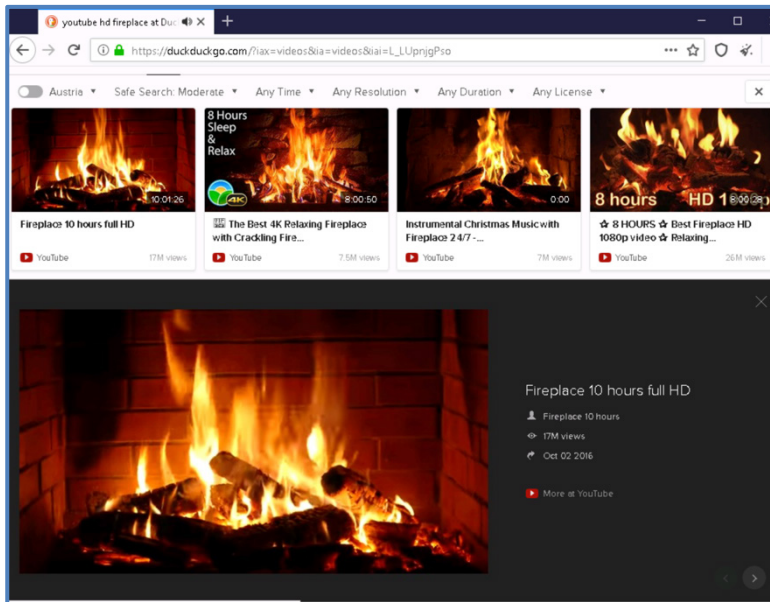
15. [ビデオ (Videos)] をクリックします。



16. ビデオサムネイルが表示されたら、再生時間が数時間ある YouTube の暖炉のビデオのいずれかをクリックします。

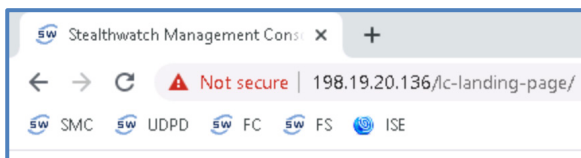


17. ビデオを匿名で視聴することに関する警告が表示された場合は、[ここで視聴 (Watch Here)] オプションをクリックします。Tor ブラウザでビデオの再生が始まります。(再生ボタンのクリックが必要な場合があります)



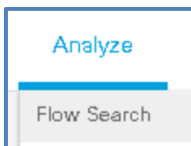
18. ここでは Tor ブラウザを実行したままにします。

19. WKST1 で **Chrome** ブラウザを開き、ブックマークを使用して **SMC** システムに移動します。



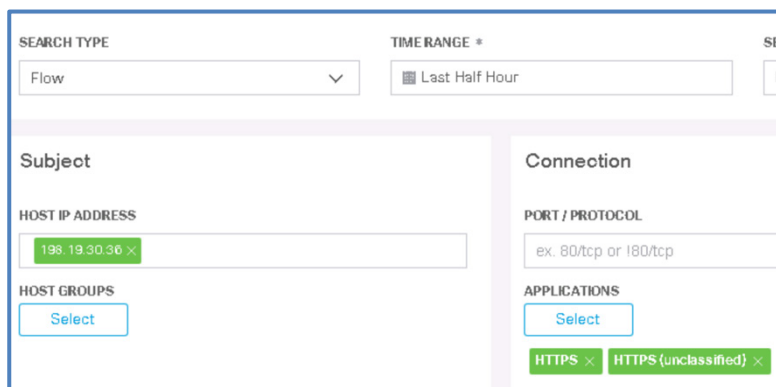
a. 必要に応じて **admin** および **C1sco12345** のクレデンシャルでログインします。

20. [分析 (Analyze)] > [フロー検索 (Flow Search)] を選択します。



21. 次のフロー検索パラメータを設定します。

- a. [時間範囲 (Time Range)] = [直近 30 分 (Last Half Hour)]
- b. [サブジェクト (Subject)] の [ホストの IP アドレス (Host IP Address)] = **198.19.30.36** (このフィールドに入力した後 **Enter** を押す)
- c. [接続 (Connection)] の [アプリケーション (Applications)] ([Select (選択)] ボタンを押す) = **HTTPS** および **HTTPS(unclassified)**
- d. [検索 (Search)] をクリックします。



22. 結果を見やすくするために、レポートに表示される列を変更します。[列の管理 (Manage Columns)] をクリックします。



23. [フローテーブル列 (Flow Table Columns)] フィルタの次の項目を変更します。

- a. [Connection (接続)] タブ
 - i. [期間 (Duration)] をオフにする
 - ii. 「暗号化 (Encryption)」で始まる 5 つのエントリ をすべてオンにする
 - iii. [合計バイト数 (Total Bytes)] をオフにする
- b. [サブジェクト (Subject)] タブ
 - i. [サブジェクトのバイト数 (Uncheck Subject Bytes)] をオフにする
 - ii. [サブジェクトホストグループ (Subject Host Groups)] をオフにする
 - iii. [サブジェクトポート/プロトコル (Subject Port/Protocol)] をオフにする
- c. [ピア (Peer)] タブ
 - i. [ピアのバイト数 (Peer Bytes)] をオフにする
 - ii. [ピアホストグループ (Peer Host Groups)] をオフにする
 - iii. [ピアポート/プロトコル (Peer Port/Protocol)] をオフにする
- d. [設定 (Set)] をクリックします。

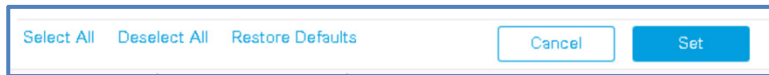
24. 結果をスクロールします。フローレコードの [暗号化 (Encryption)] フィールドに、一部データが表示されていることを確認してください。

START	SUBJECT IP A...	APPLICATION	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADDR...	ACTIONS
Ex: 06/09/2	Ex: 10.10.10.1	Ex: "Corporate"	Ex: 1.0	Ex: ECDH	Ex: ECDSA	Ex: AES_256_...	Ex: SHA384	Ex: 10.255.25		
Nov 8, 2018 3:32:20 PM (2hr 8min 17s ago)	198.19.20.36	HTTPS (unclassified)	--	--	--	--	--	198.18.128.136		
Nov 8, 2018 4:13:21 PM (1hr 27min 16s ago)	198.19.20.36	HTTPS (unclassified)	TLS 1.2	ECDHE	RSA	AES_256_GCM/2 56	SHA384	51.38.112.240		
Nov 8, 2018 4:08:17 PM (1hr 31min 20s ago)	198.19.20.36	HTTPS (unclassified)	TLS 1.3	--	--	AES_256_GCM/2 56	SHA384	72.21.91.70		
Nov 8, 2018 4:09:09 PM (1hr 31min 28s ago)	198.19.20.36	HTTPS (unclassified)	TLS 1.2	ECDHE	RSA	CHACHA20_POLY 1305/256	SHA256	184.50.249.243		
Nov 8, 2018 4:10:46 PM (1hr 29min 51s ago)	198.19.20.36	HTTPS (unclassified)	TLS 1.2	ECDHE	RSA	AES_256_GCM/2 56	SHA384	198.18.128.139		
Nov 8, 2018 4:09:25 PM (1hr 31min 12s ago)	198.19.20.36	HTTPS (unclassified)	TLS 1.3	--	--	AES_128_GCM/1 28	SHA256	31.13.89.228		

25. [列の管理 (Manage Columns)] をクリックして、今後のラボ演習のためにフィルタをリセットします。



a. [デフォルトの復元 (Restore Defaults)] をクリックし、[Set (設定)] をクリックします。



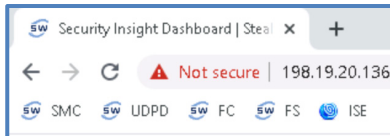
26. これで、Cisco IOS-XE ルータでの NetFlow と ETA の設定と検証が完了しました。WKST1 で 開いているすべてのウィンドウとアプリケーションを閉じます。

a. Stealthwatch のフローセンサー アプライアンスは、ETA のエクスポートもサポートしていることに注意してください。前のラボシナリオでフローセンサーの設定を完了したときに、この機能も設定済みです。

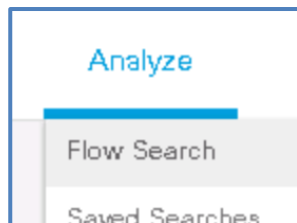
Stealthwatch での ETA の表示およびフィルタリング

お客様は、PCI 要件に関するレポートについて、いくつかカスタマイズしたいと考えています。お客様はいくつか特定のニーズをお持ちで、そのためには Stealthwatch が一致条件に基づいて着信フローデータを常に監視する必要があります。また、カスタムレポートの利用も希望されています。お客様がすぐにソリューションの恩恵を受けることができるようにしましょう。お客様から、PCI データセキュリティ スタンダード (PCI/DSS) に対する最近の変更に準拠していることを確認できるレポートを作成するよう依頼されています。この場合、新しい要件であるため、PCI デバイスの環境内で SSL TLS 1.0 を使用していないことを確認する必要があります。

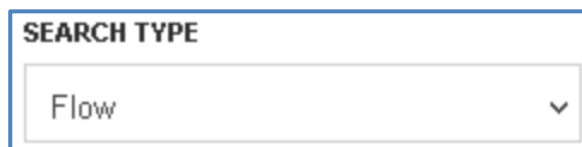
1. **Chrome** で **SMC** にログインしていることを確認し、必要に応じて **admin** および **C1sco12345** を使用してログインします。



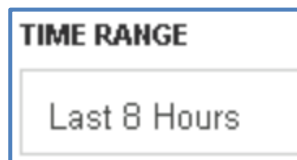
2. 監査チームが調査を希望する最初の問題は、SSL TLS バージョンに関する新しい PCI/DSS 要件に対して、準備が整っていることを確認することです。SSL TLS 1.1 以降を実行している必要があります (TLS 1.2 を推奨)。PCI システムが TLS 1.0 を実行していないことを確認しましょう。
 - a. Web インターフェイスで [分析 (Analyze)]、[フロー検索 (Flow Search)] の順に選択します。



- b. [検索タイプ (Search Type)] を [フロー (Flow)] に設定します。



- c. [時間範囲 (Time Range)] を [過去 8 時間 (Last 8 Hours)] に設定します。

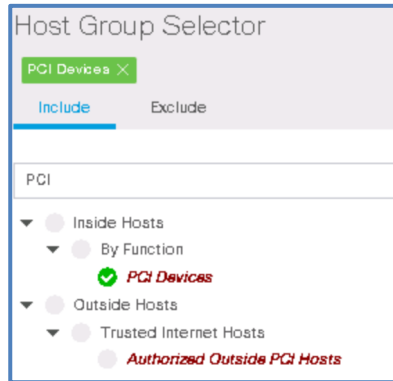


- d. [検索名 (Search Name)] を [PCI TLS 1.0 調査 (PCI TLS 1.0 Investigation)] に設定します。



- e. [返される最大レコード数 (Max Records Returned)] を **10,000** に設定します。

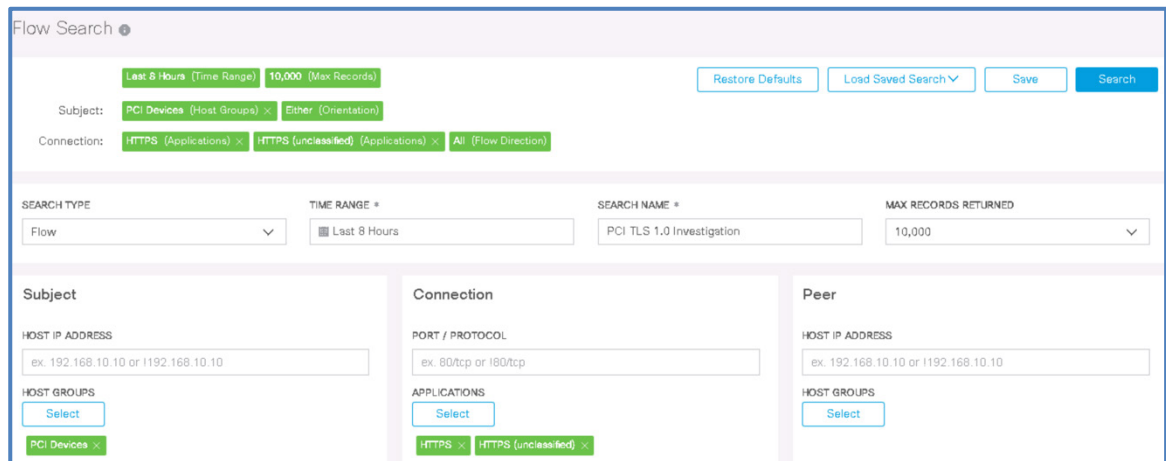
- f. [サブジェクト (Subject)] の [ホストグループ (Host Groups)] の [選択 (Select)] ボタンをクリックします。[サブジェクト (Subject)] の [ホストグループ (Host Groups)] を [PCI デバイス (PCI Devices)] ([内部ホスト (Inside Hosts)] > [機能別 (By Function)] > [PCI デバイス (PCI Devices)]) に設定し、[適用 (Apply)] をクリックします。



- g. [接続 (Connection)] の [アプリケーション (Applications)] の [選択 (Select)] ボタンをクリックします。[HTTPS] と [HTTPS(unclassified)] の両方を選択し、[適用 (Apply)] をクリックします。



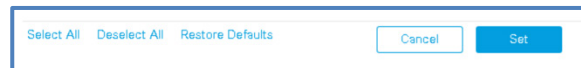
- h. [フロー検索 (Flow Search)] フォームの右上隅にある [検索 (Search)] をクリックします。レポートの実行およびデータの提供には数分かかります。レポートが **100%** 完了するまで待ちます。(100% になるまでは、部分的なデータ調査結果が表示されます)



- i. [列の管理 (Manage Columns)] をクリックします。ポップアップが表示されるまで数秒かかる場合があります。



- i. ポップアップウィンドウの下部にある [すべて選択解除 (Deselect all)] をクリックします。これにより、すべてのタブのすべてのフィールドが削除されます。



ii. 次の列のみを選択します。

1. [Connection (接続)] タブ

a. [開始 (Start)]、[期間 (Duration)]、[アプリケーション (Application)]、および 5 つある [暗号化... (Encryption...)] のオプションをすべて選択します。

2. [サブジェクト (Subject)] タブ

a. [サブジェクトホストグループ (Subject Host Groups)]、[サブジェクト IP アドレス (Subject IP Address)]、[サブジェクトの方向 (Subject Orientation)] を選択します。

3. [ピア (Peer)] タブ

a. [ピアホストグループ (Peer Host Groups)]、[ピア IP アドレス (Peer IP Address)]、および [ピアポート/プロトコル (Peer Port/Protocol)] を選択します。

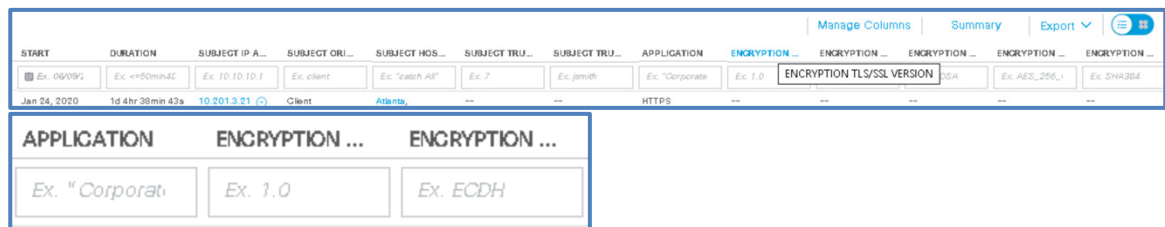
4. 以上の列のみが選択されていることを確認し、[Set (設定)] をクリックします。

5. これで必要な列が表示され、結果をフィルタリングして続行できます。

j. [暗号化 TLS/SSL バージョン (Encryption TLS/SSL Version)] フィールドを探します。

i. 注 1: ディスプレイのサイズによっては、右側のフィールドが表示しきれない場合があります。その場合は、ウィンドウの下部にスクロールし、左右のスライダーで右にスクロールした後、ページの上部にスクロールしてフィルタフィールドを見つける必要があります。

ii. 注 2: ディスプレイサイズによっては、フィールド名が一部しか表示されない場合があります。下に「Ex 1.0」と表示されているフィルタがある [暗号化... (Encryption...)] を探します。



k. このフィルタフィールドに 1.0 と入力します。



l. PCI デバイスで TLS 1.0 が使用されているすべてのフローが表示されます。これらすべてのフローについて、[サブジェクト IP アドレス (Subject IP Address)] が 10.201.3.51 であることに注意してください (この列を表示するには、ページの左側へのスクロールが必要な場合があります)。

- m. ここで使用されている TLS バージョンについて、お客様に報告する必要があります。これらのリモートシステムは、英国にあるお客様のネットワークの外部に配置されているため、お客様にとって重要ではない可能性があります。それでも報告する必要があります。この機能（暗号化データの取得とレポート）は、シスコの ETA 機能に含まれています。

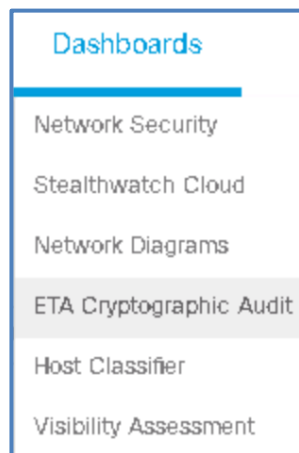
START	DURATION	SUBJECT IP A...	SUBJECT ORI...	SUBJECT HO...	SUBJECT TRU...	SUBJECT TRU...	APPLICATION	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTI...	
Ex. 06/09/2	Ex. <=50min4s	Ex. 10.10.10.1	Ex. client	Ex. "catch All"	Ex. 7	Ex. jsmith	Ex. "Corporat	1.0	x	Ex. ECDH	Ex. ECDS
Oct 22, 2018 11:53:38 AM (54min 19s ago)	4s	10.201.3.51	Client	Atlanta, PCI Devices	4	Employees	HTTPS (unclassified)	TLS 1.0		ECDHE	RSA
Oct 22, 2018 10:53:38 AM (1hr 54min 19s ago)	4s	10.201.3.51	Client	Atlanta, PCI Devices	4	Employees	HTTPS (unclassified)	TLS 1.0		ECDHE	RSA
Oct 22, 2018 9:53:38 AM (2hr 54min 19s ago)	4s	10.201.3.51	Client	Atlanta, PCI Devices	4	Employees	HTTPS (unclassified)	TLS 1.0		ECDHE	RSA

3. 後でこの情報を確認したい場合は、すでに説明したとおり現在のテーブルを csv ファイルにエクスポートできますが、それ以外にも検索を保存したり、結果を保存したりすることもできます。ここでは、いずれのタスクも実行しないでください。

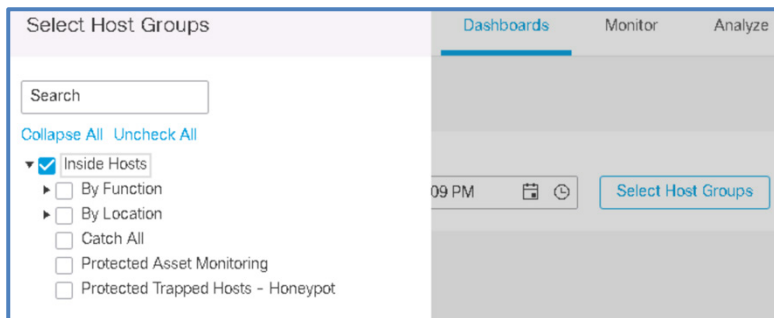
Stealthwatch ETA 暗号化監査アプリケーションの使用

前のシナリオでは、特に ETA ベースの暗号化データを扱う Stealthwatch アプリケーションをインストールしました。ここでは、このアプリケーションから提供された情報を確認します。

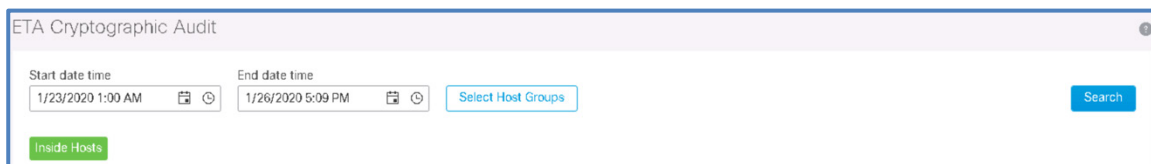
1. [ダッシュボード (Dashboards)] をクリックし、メニューから [ETA 暗号化監査 (ETA Cryptographic Audit)] を選択します。



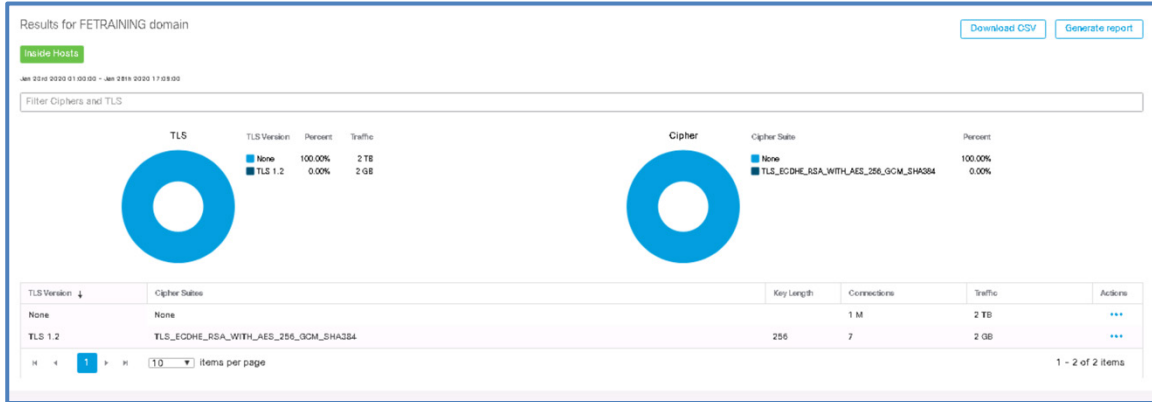
2. 次のフィールドを設定します。
 - a. [開始日時 (Start Date Time)] : ラボの開始日より前の日付を設定します
 - b. [終了日時 (End Date Time)] : 明日の日付を設定します
3. [ホストグループの選択 (Select Host Groups)]、[内部ホスト (Inside Hosts)]、[適用 (Apply)] の順にクリックします。



4. [検索 (Search)] をクリックします。



5. 表示された結果を確認します。



- a. ここから各エントリに関連するフローを表示したり、データを CSV ファイルとしてダウンロードしたり、レポートを生成したりできます。今回はこれらのアクションを実行しないでください。
6. このレポートについて、次のような疑問が出てくるはずですが、直前のクエリで表示された TLS 1.0 が表示されないのはなぜでしょうか。
- a. その答えは非常にシンプルです。このダッシュボード/アプリケーションは、暗号化フローの終点である内部ホスト（サーバとして機能しているホスト）に特化しています。前のクエリでも内部ホストを調べていましたが、環境を出てデータセットの一部となったフローが含まれていました。前のクエリを振り返ってみると、これら TLS 1.0 接続のリモートエンドは、英国のネットワークの外部にあるサーバでした。

シナリオのまとめ

このシナリオでは、CSR ネットワークデバイスで ETA フローを有効にしました。また、サポートされているネットワークデバイスからのフローに組み込まれたシスコの ETA データを使用して、お客様が PCI 基準に準拠していることを確認するための Web ベースの検索を作成しました。さらに、この目的に特化した Stealthwatch アプリケーションで ETA データを表示しました。

シナリオ 7. カスタム セキュリティ イベント

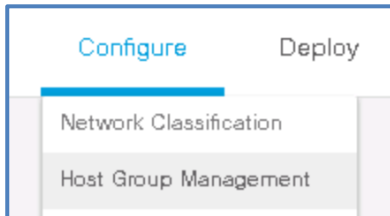
フローデータがお客様環境内で適切に分類されたら、さらなるカスタマイズとレポートに着手できます。製品内には、組み込みのドキュメントやレポートが多数用意されています。ほとんどの場合、これらを使用してお客様の目標を達成できます。ただし、場合によってはソリューションをカスタマイズする必要があります。

お客様は、PCI 環境と一般的なインターネットの使用について、いくつかカスタマイズしたいと考えています。お客様はいくつか特定のニーズをお持ちで、そのためには Stealthwatch が一致条件に基づいて着信フローデータを常に監視する必要があります。また、カスタムレポートの利用も希望されています。お客様がすぐにソリューションの恩恵を受けることができるようにしましょう。

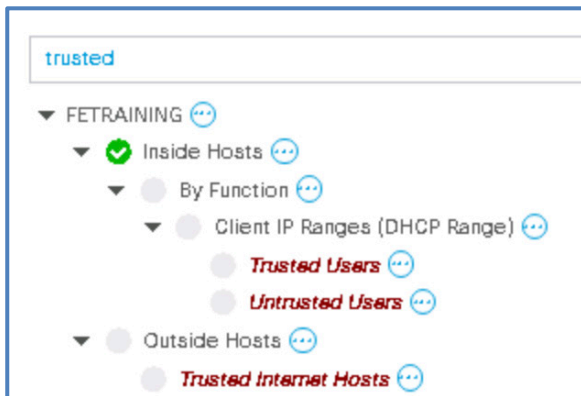
カスタム セキュリティ イベントの作成

お客様の金融取引処理デバイスが、ある PCI 規制の対象になっています。お客様は、これらのデバイスがインターネット上の未認可ホストと通信していないことを確かめ、未認可トラフィックが発生した場合には通知を受け取りたいと希望しています。そこで、認可済みの外部 IP アドレスを含むホストグループを作成し、その後、認可済みホストグループからのトラフィック以外の未認可のネットワークトラフィックをトリガーとするカスタム セキュリティ イベントを作成します。

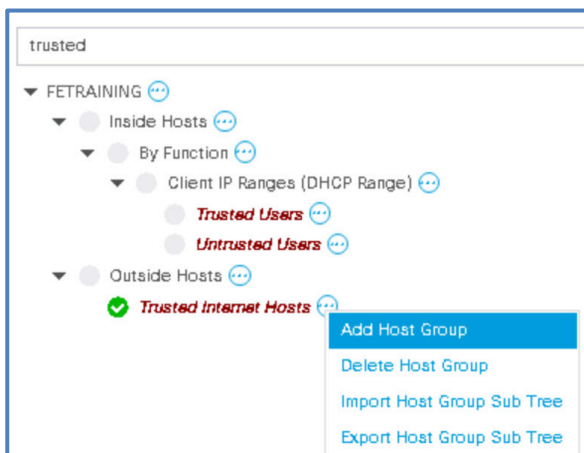
1. WKST1 上の **Chrome** で **SMC** のブックマークを選択し、SMC にアクセスします。
2. SMC Web インターフェイスで、[設定 (Configure)] > [ホストグループ管理 (Host Group Management)] の順にクリックします。



3. [ホストグループ名でフィルタ (Filter by Host Group Name)] フィールドに **Trusted** と入力し、**Enter** を押します。



4. [信頼できるインターネットホスト (Trusted Internet Hosts)] のアクションアイコンを選択し、メニューから [ホストグループの追加 (Add Host Group)] を選択します。



5. 次の値を使用してホストグループを設定します。

- a. [名前 (Name)] : **Authorized Outside PCI Hosts**
- b. [範囲 (Ranges)] : **206.128.157.0/24**

New Host Group

HOST GROUP NAME *

PARENT HOST GROUP

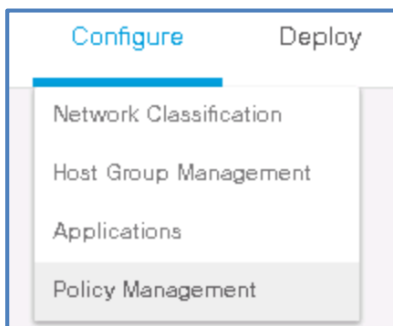
Outside Hosts → Trusted Internet Hosts

DESCRIPTION (512 CHAR MAX)

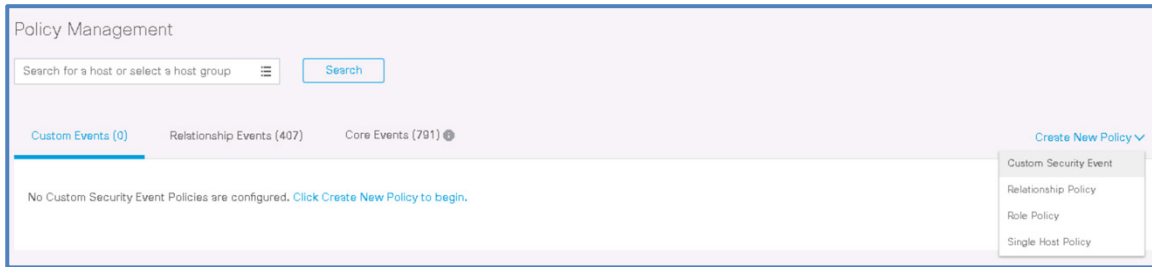
IP ADDRESSES AND RANGES ●

c. [保存 (Save)] をクリックします。

6. [設定 (Configure)] メニューをクリックし、[ポリシー管理 (Policy Management)] メニュー項目を選択します。

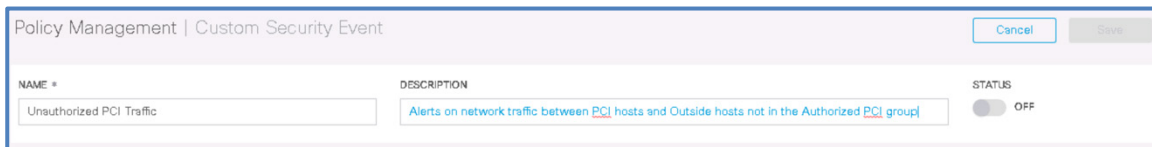


7. [カスタムイベント (Custom Events)] タブがデフォルトでアクティブになっています。[新規ポリシーの作成 (Create New Policy)] > [カスタムセキュリティイベント (Custom Security Event)] の順にクリックします。



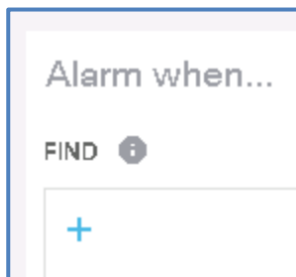
8. 次の値に基づいてカスタム セキュリティ イベントを設定します。

- a. [名前 (Name)] : **Unauthorized PCI Traffic**
- b. [説明 (Description)] : **認可済み PCI グループ以外の外部ホストと PCI ホストとの間のネットワークトラフィックに対するアラート (Alerts on network traffic between PCI hosts and Outside hosts not in the Authorized PCI group)**

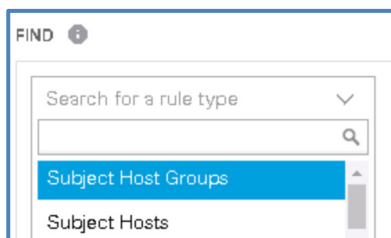


9. ウィンドウの [検索 (Find)] ペインで、次の設定手順を実行します。

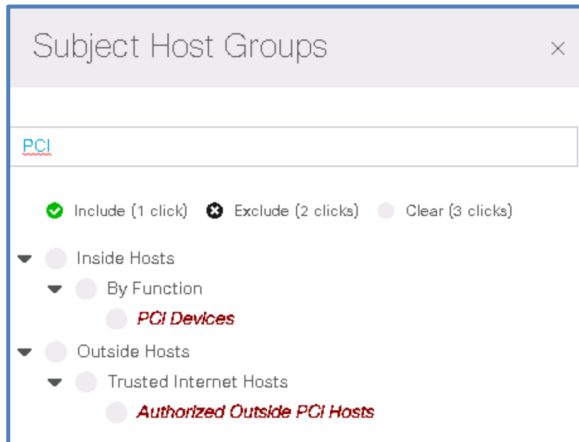
- a. [+] ボタンをクリックして、このカスタム セキュリティ イベントに新しいルールを追加します。



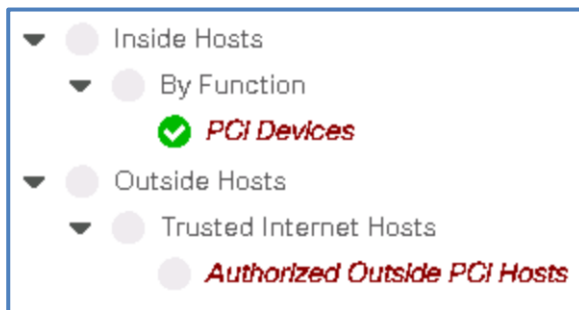
- b. リストから [サブジェクトホストグループ (Subject Host Groups)] を選択します。



- c. 検索フィールドに **PCI** と入力し、**Enter** を押します。



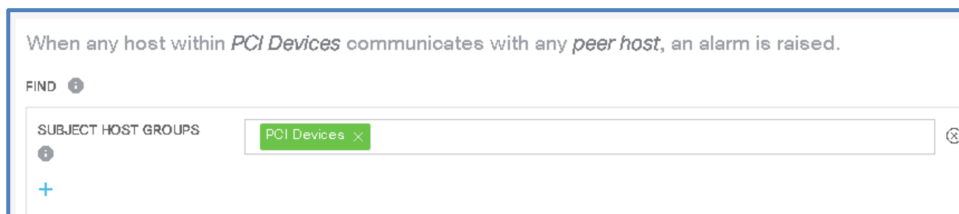
- d. [PCI デバイス (PCI Devices)] ホストグループの前にある円形アイコンをクリックします。チェックマークが表示されます。



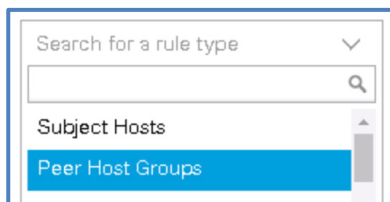
- e. [適用 (Apply)] をクリックします。



- f. 次のような設定が表示されます。再度 [+] ボタンを押して、ルールパラメータの設定を続行します。



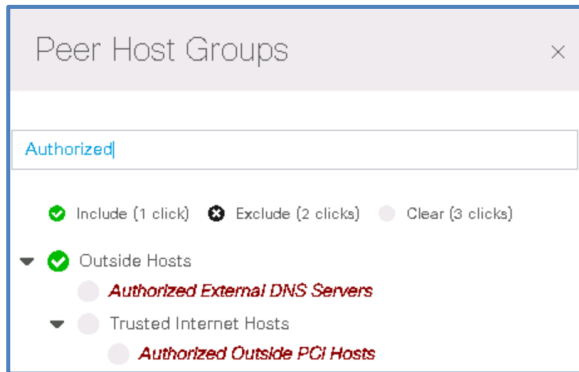
- g. リストから [ピアホストグループ (Peer Host Groups)] を選択します。



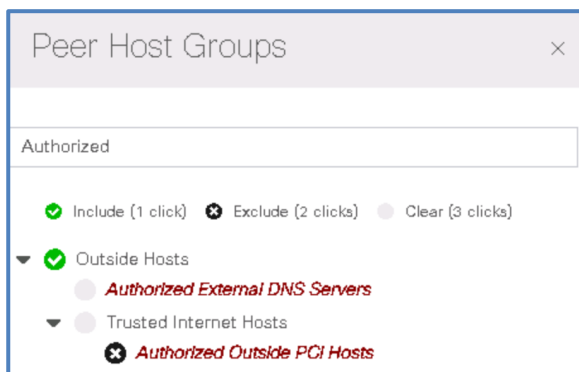
- h. [外部ホスト (Outside Hosts)] ホストグループの前にある円形アイコンをクリックします。チェックマークが表示されます。[適用 (Apply)] はまだクリックしないでください。



- i. 検索フィールドに **Authorized** と入力し、**Enter** を押します。



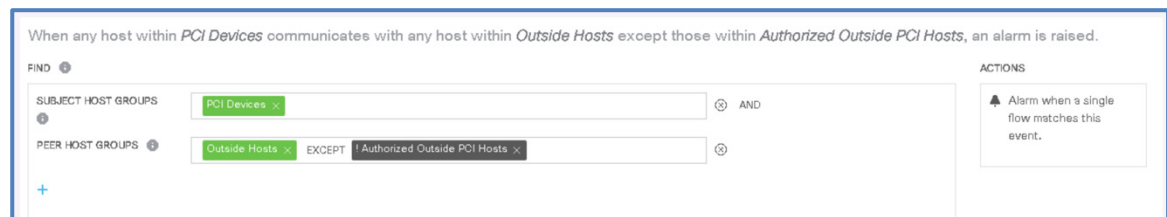
- j. [認可済み外部 PCI ホスト (Authorized Outside PCI Hosts)] の前にある円を **2回**クリックすると、[X] アイコンが表示されます。以上で、ピアマッチングの際に外部ホストを含め、認可済み外部 PCI ホストを除外するよう設定できました。



- k. [適用 (Apply)] をクリックします。



- l. 次のような設定が表示されます。



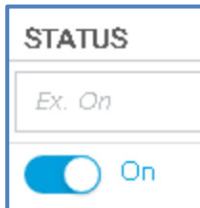
- m. [保存 (Save)] をクリックします。



10. リストに新しいルールが表示されます。

EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
Ex. Data Event	Ex. Data Center	Ex. 01/29/2018 12:00 PM	Ex. Inside Hosts	Ex. Inside Hosts	Ex. On	
Unauthorized PCI Traffic	Alerts on network traffic between PCI hosts and Outside hosts not in the Authorized PCI group	10/22/2018 11:55 AM	PCI Devices	Outside Hosts, Authorized Outside PCI Hosts	Off	

11. このルールを有効にします。ルールを確認したら、[ステータス (Status)]列のトグルボタンをクリックして、[オフ (Off)]から [オン (On)]に切り替えます。



12. 前と同じ手順および方法を使用して、次の場合に起動する追加の**カスタム セキュリティ イベント**を作成します。

- a. 外部ホスト（ただし信頼されているインターネットホストは除く）がクライアントとして動作し、リモートデスクトップ、SSH または Telnet を介して内部ホストと通信した場合。
 - i. ヒント：目的とする結果を得るために、ルールの [サブジェクトホストグループ (Subject Host Groups)]、[ピアホストグループ (Peer Host Groups)]、[ピアアプリケーション (Peer Application)]、[サブジェクトの方向 (Subject Orientation)]の各フィールドを活用します。

Policy Management | Custom Security Event Cancel Save

NAME * DESCRIPTION STATUS OFF

When any host within *Outside Hosts* except those within *Trusted Internet Hosts*, acting as a *client* communicates with any host within *Inside Hosts*; using *remote desktop*, *SSH*, or *Telnet*, an alarm is raised.

FIND

SUBJECT HOST GROUPS EXCEPT AND

SUBJECT ORIENTATION AND

PEER HOST GROUPS AND

PEER APPLICATIONS AND

ACTIONS

13. 以上で、お客様の**カスタム セキュリティ イベント**の作成が正常に完了しました。これでお客様に、作成した IT セキュリティポリシーに違反するネットワーク内の特定の動作について通知されるようになります。次のラボ手順に進みます。

EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
Ex. Data Event	Ex. Data Center	Ex. 01/29/2018 12:00 PM	Ex. Inside Hosts	Ex. Inside Hosts	Ex. On	
Prevent External services Unless Trusted Hosts		10/22/2018 12:08 PM	Outside Hosts, Trusted Internet Hosts	Inside Hosts	On	
Unauthorized PCI Traffic	Alerts on network traffic between PCI hosts and Outside hosts not in the Authorized PCI group	10/22/2018 12:00 PM	PCI Devices	Outside Hosts, Authorized Outside PCI Hosts	On	

シナリオのまとめ

このシナリオでは、PCI トランザクションに関するお客様の IT セキュリティポリシーに違反したネットワークトラフィックを明らかにするための、カスタム セキュリティ イベントを作成しました。また、デスクトップクライアントでダッシュボードとして使用できるカスタムドキュメントの作成方法についても学習しました。

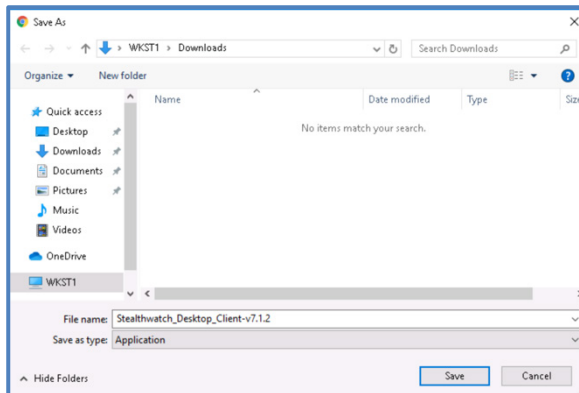
シナリオ 8. Stealthwatch デスクトップクライアントへのアクセス

ここまでは、主に Stealthwatch Web UI の使用方法を学んできました。ここからは、必要に応じて Stealthwatch デスクトップクライアント (Java) を使用します。現在、ソリューションからこのクライアントを除外する方向で開発が行われていることに注意してください。今日、ほとんどのタスクは Web UI 内で実行できますが、Java ベースのクライアントの使用が必要な場合もあります。まずクライアントをインストールしてアクセスした後、クライアントのインターフェイス内から必要な実装タスクを実行します。

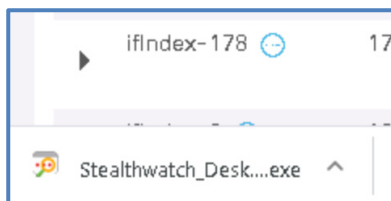
1. SMC デスクトップクライアントをインストールします。SMC Web ページの右上にある [デスクトップクライアント (Desktop Client)] ボタンをクリックします。



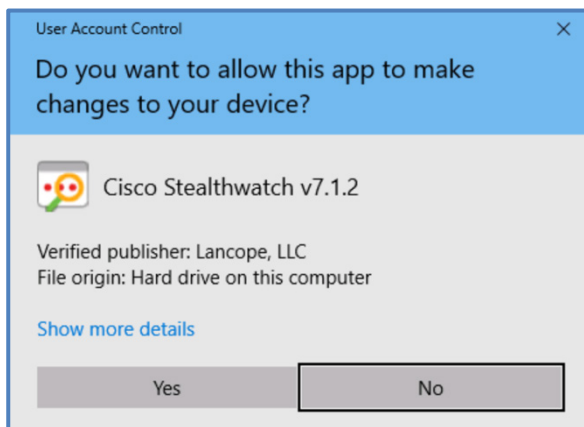
- a. Web ブラウザで、Stealthwatch デスクトップクライアントのインストーラファイルがダウンロードされます。[保存 (Save)] をクリックします。



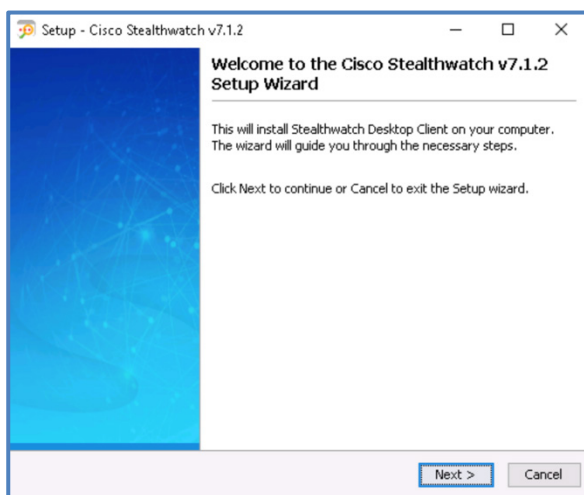
- b. ダウンロードが完了したら、Chrome ウィンドウの左下にある新しい **exe** ファイルをクリックします。クリック後、しばらく待ちます。



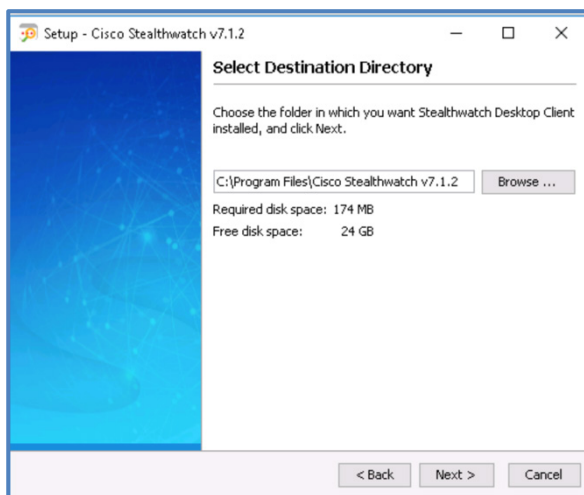
- c. UAC のプロンプトが表示されたら、[はい (Yes)] をクリックします。



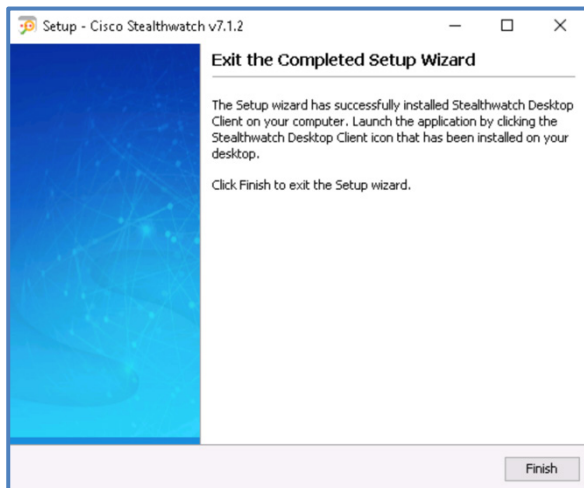
d. インストーラの [次へ (Next)] をクリックします。



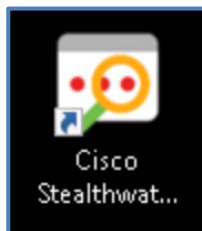
e. [次へ (Next)] をもう一度クリックします。



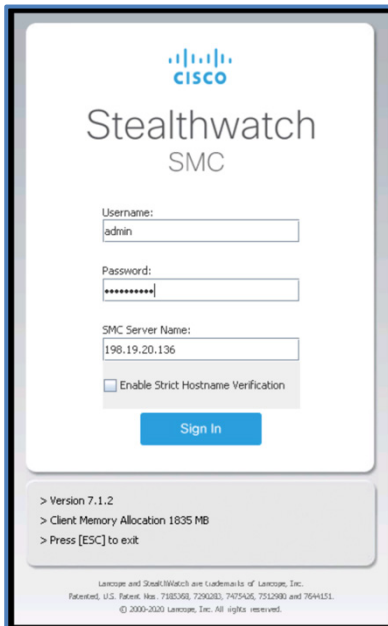
f. [終了 (Finish)] をクリックしてインストールを完了します。



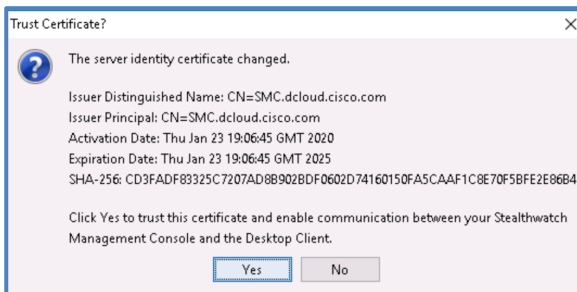
- g. WKST1 デスクトップで開いているすべてのアプリケーションを最小化し、新しい Cisco Stealthwatch アイコンを見つけます。



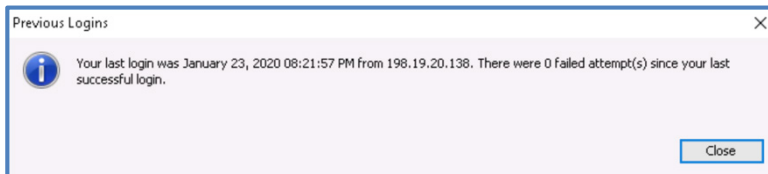
2. 先ほど作成した **Cisco Stealthwatch v7.1.2** アプリケーションのアイコンをダブルクリックします。
3. 次のクレデンシャルを使用してログインします。
 - a. [ユーザ名 (Username)] : **admin**
 - b. [パスワード (Password)] : **C1sco12345**
 - c. [SMC サーバ名 (SMC Server Name)] : **198.19.20.136**
 - d. [サインイン (Sign In)] をクリックします。



e. [はい (Yes)] をクリックして SMC 自己署名証明書を信頼します。

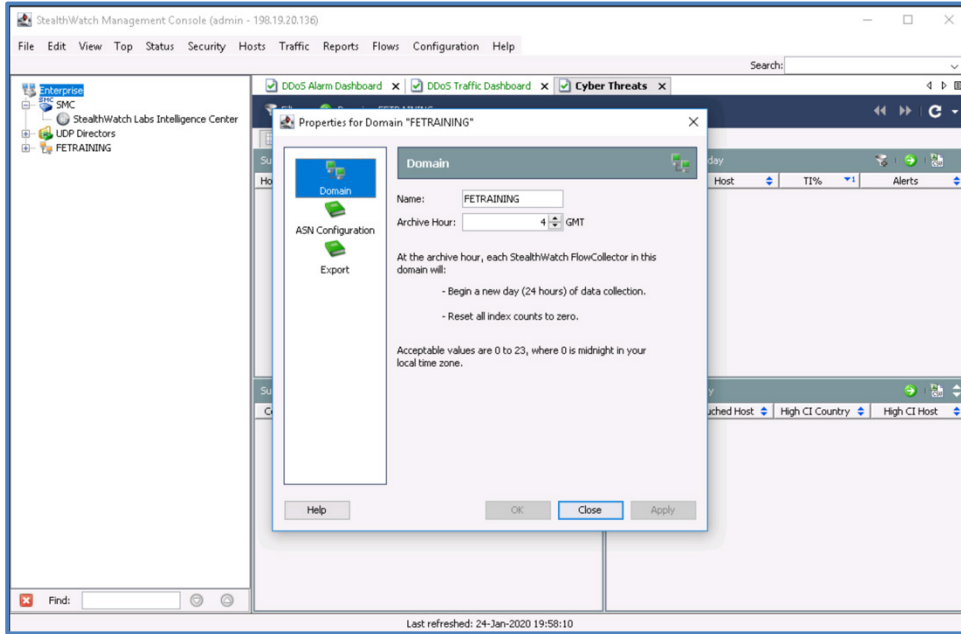


4. [閉じる (Close)] をクリックして、前回のログイン情報を確認します。



5. SMC デスクトップクライアントのインターフェイスが表示されます。[ドメイン「FETRAINING」のプロパティ (Properties for Domain "FETRAINING")] が表示されるまでに、少し時間がかかる場合があります。

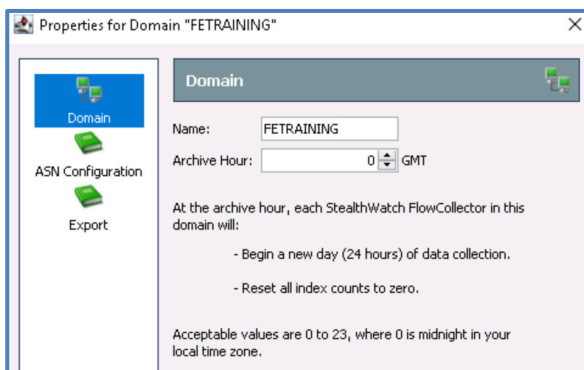
a. ここでは、クライアントとすべてのポップアップウィンドウを開いたままにします。



アーカイブ時間

[アーカイブ時間 (Archive Hour)] の値により、Stealthwatch ドメイン内でデータ収集の新しい 1 日が開始する時刻が指定され、その時刻の High Concern Index や High Target Index などのインデックス数がリセットされます。お客様環境では、アーカイブ時間を、Stealthwatch のプライマリユーザ/管理者が位置するタイムゾーンの午前 0 時に設定します。

1. ここでは、お客様は GMT/UTC タイムゾーンにあるダブリンにいます。[アーカイブ時間 (Archive Hour)] をそのタイムゾーンの深夜にするには、**0 GMT** に変更する必要があります。



2. 値を **0** に設定したら、[OK] をクリックします。

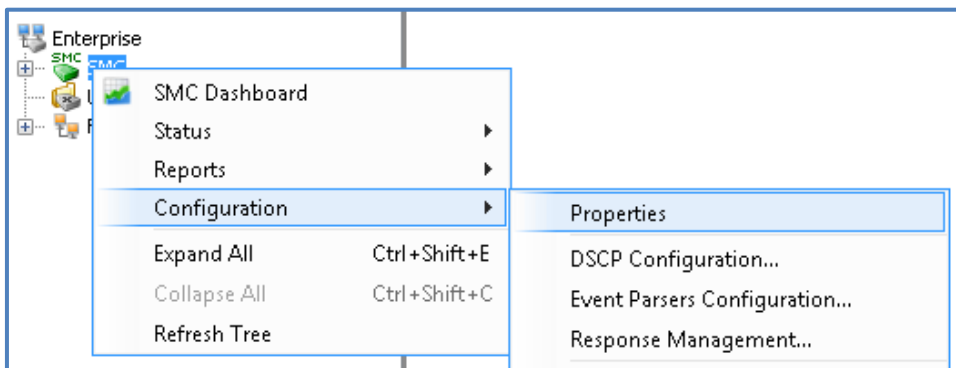
SMTP

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、次の SMTP サーバリレーアドレスと、SMC がメッセージの送信に使用できる電子メールアドレスが提供されています。

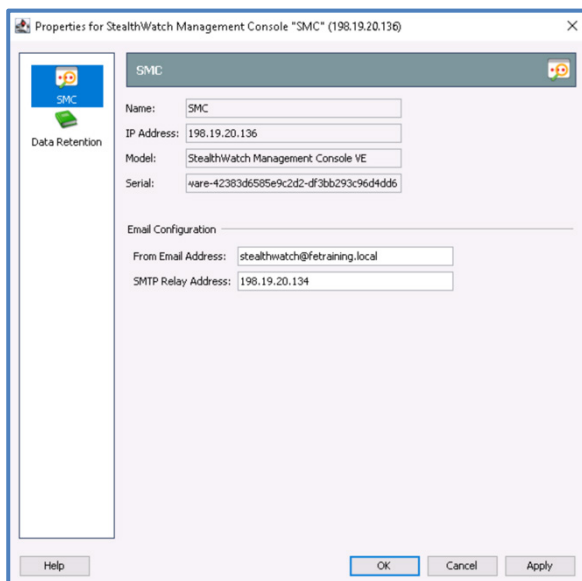
[送信元電子メールアドレス (From Email Address)] : **Stealthwatch@fetraining.local**

[SMTP リレーアドレス (SMTP Relay Address)] :

1. 左ペイン (エンタープライズツリー) 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@fetraining.local**
 - b. [SMTP リレーアドレス (SMTP Relay Address)] : **198.19.20.134**
 - c. [OK] をクリックします。

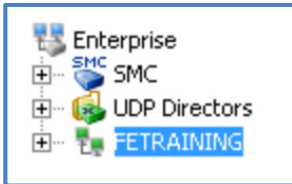


注：[SMTP リレーアドレス (SMTP Relay Address)] の値には、有効な SMTP サーバの IP アドレスまたは DNS 名を指定できます。指定されたサーバでは、SMC IP アドレスから SMTP サーバを通じてメールをリレーできるようにする必要があります。その場合、SMTP サーバについてお客様環境で設定の変更が必要になることがあります。[送信元電子メールアドレス (From Email Address)] の値は、お客様環境内の有効なメールボックスである必要はありませんが、ドメイン名とお客様の電子メールアドレスの DNS ドメイン名が一致していることが推奨されます。SMC 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。

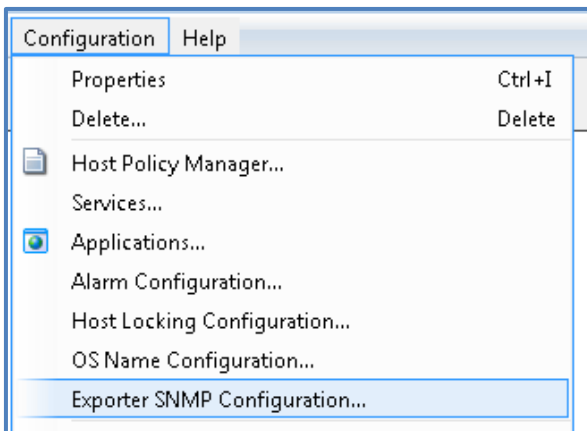
エクスポート SNMP の設定

Stealthwatch では SNMP を使用して、NetFlow をフローコレクタに送信するエクスポート インターフェイスの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ト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。

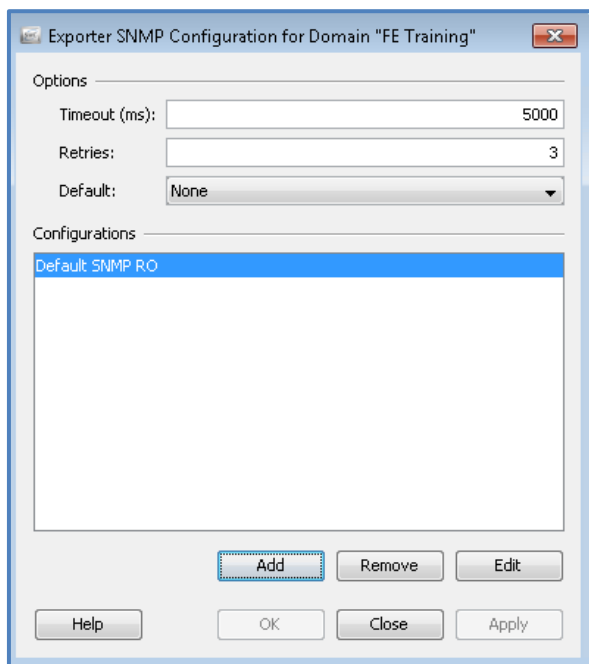
1. SMC デスクトップ クライアント ウィンドウの左ペインで [FETRAINING] ドメインをクリックして、オブジェクトを強調表示します。



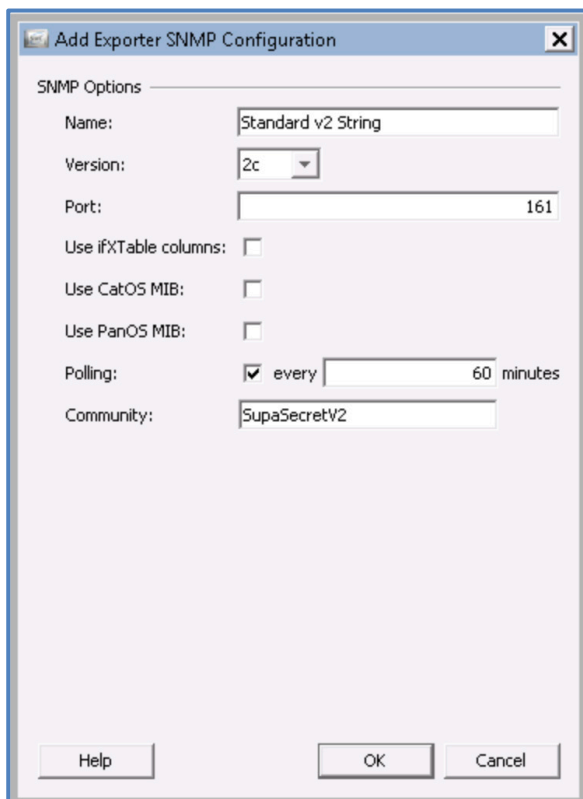
2. 上部のナビゲーションバーから [設定 (Configuration)] メニューをクリックし、[エクスポートの SNMP 設定 (Exporter SNMP Configuration)] メニュー項目を選択します。



3. [追加 (Add)] をクリックします

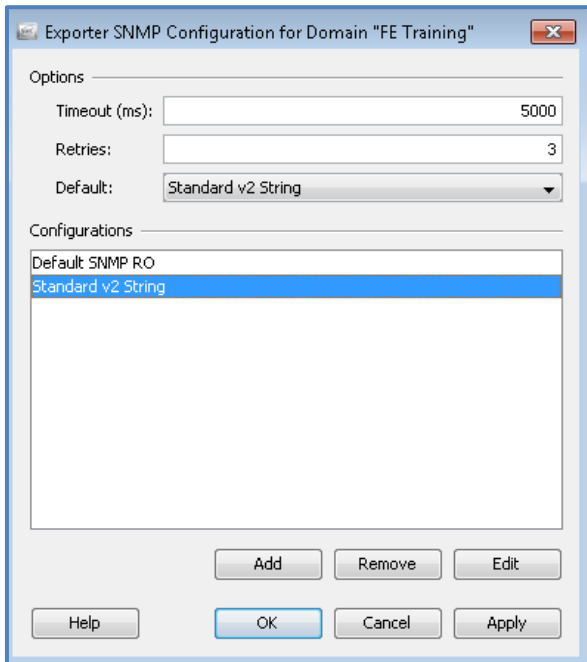


- a. [エクスポートの SNMP 設定の追加 (Add Exporter SNMP Configuration)] ウィンドウが表示されます。次に示す SNMP 設定の値を指定し、[OK] をクリックします。
 - i. [名前 (Name)] : **Standard v2 String**
 - ii. [バージョン (Version)] : **2c**
 - iii. [ポート (Port)] : **161**
 - iv. [ポーリング (Polling)] : **60 分ごと (every 60 minutes)**
 - v. [コミュニティ (Community)] : **SupaSecretV2**
 - vi. [OK] をクリックします。



注：実稼働環境では、SNMP トラフィックを削減して SMC とエクスポートに対する負荷を軽減するために、ポーリング間隔を 720 分（12 時間）以上に設定することを推奨します。dCloud のラボ環境では、ラボ向けに低い値に設定されています。

4. 設定を保存した後、メインの SNMP 設定ページで、[デフォルト (Default)] のドロップダウンメニューの値を [Standard v2 String] に変更し、[OK] をクリックします。



5. お客様から提供された情報に基づいて、SNMP コミュニティストリングを作成できました。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 を使用する場合があります。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。

シナリオのまとめ

必要なインストールタスクとして、Stealthwatch デスクトップクライアントをインストールして使用しました。このインターフェイスは、タスクが必要とする機能に応じて、Web UI とともに引き続き使用します。一部のタスクはどちらのインターフェイスでも完了できますが、長期的には、新しく公開されるバージョンの Stealthwatch で Web UI をサポートするようになるため、Web UI を使用する方が多くなります。

シナリオ 9. フローデータとエクスポートの検証

すべての Stealthwatch アプライアンスを設定し、デスクトップクライアントをインストールしたので、次に Stealthwatch がお客様の既存のネットワーク環境からのフローデータを適切に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トデバイスからの NetFlow データを認識していることを確認します。また、特定のエクスポート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。

エクスポートの正常性

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ト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ト（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。

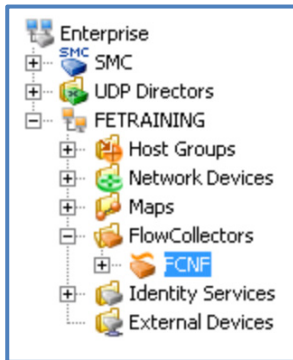
お客様から、Stealthwatch プロジェクトの対象としてフローデータを送信するネットワークデバイスのリストが提供されています。

- 172.16.16.1
- 172.16.16.2
- 172.16.16.3
- 172.16.16.4
- 172.16.16.50
- 172.16.16.100
- 172.16.16.200
- 198.18.128.138 および 198.19.20.138（フローセンサー）

1. WKST1 で **Stealthwatch デスクトップクライアント**に戻るか、または開きます。必要に応じて **admin** および **C1sco12345** のクレデンシャルでログインします。

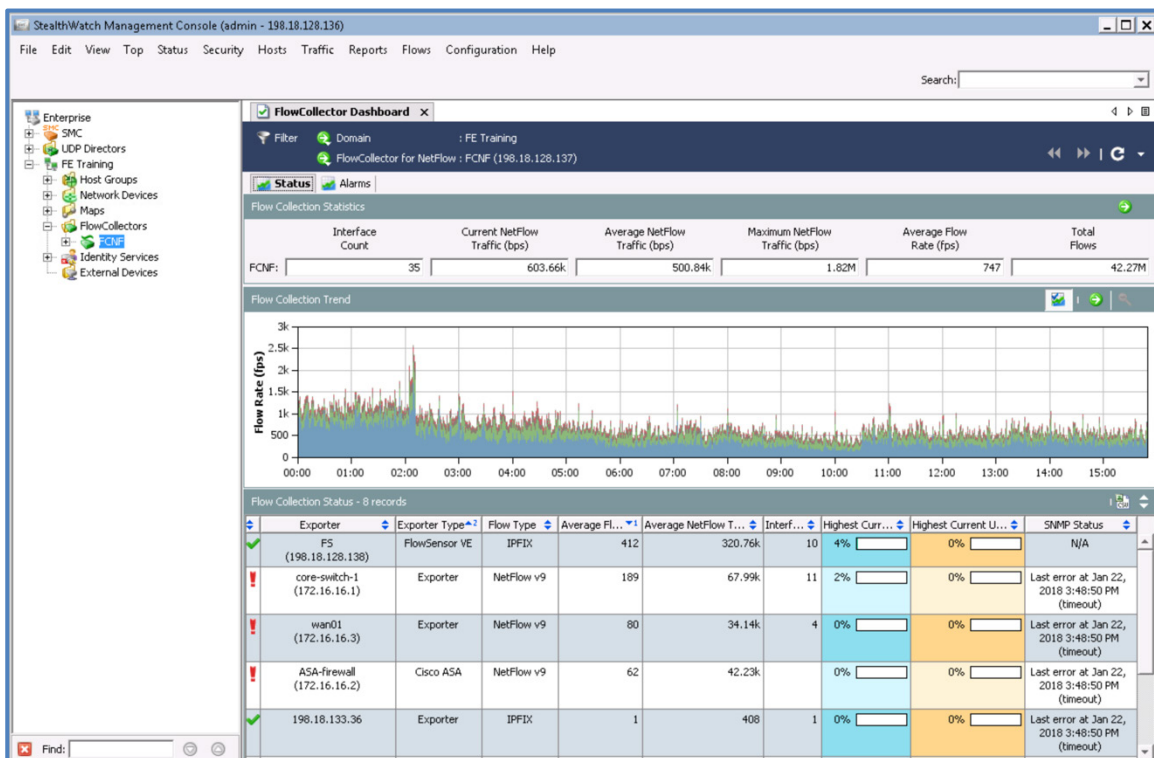


2. ヒントが表示されたら、[閉じる (Close)] をクリックします。
3. 画面左側の [エンタープライズ (Enterprise)] ツリーで、[FETRAINING] ドメインを展開し、[フローコレクタ (FlowCollectors)] コンテナを展開して、[FCNF] フローコレクタを**ダブルクリック**します。



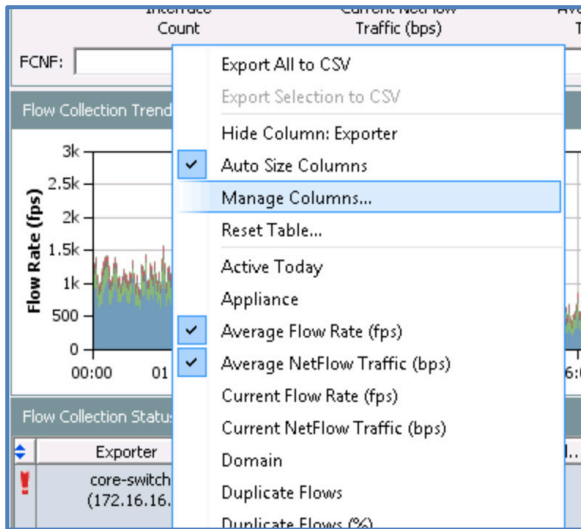
4. [フローコレクタダッシュボード (FlowCollector Dashboard)] ドキュメントが表示されます。

- [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、この 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トレンド (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、エクスポート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、エクスポートと、この FC に送信している各エクスポートで処理される NetFlow データに関する情報が表示されます。

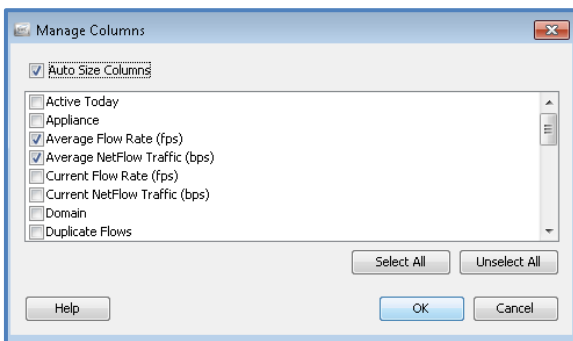


5. [フローコレクショントレンド (Flow Collection Trend)] ペインで、フローコレクタの現在の FPS ロードを確認します。各フローコレクタモデルは、パフォーマンスを低下させずに処理できる FPS の値で評価されます。特に初期のインストールでは、各 FC が過負荷になっていないことを確認してください。

6. [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、このドキュメントのビューに追加します。
7. [フローコレクションステータス (Flow Collection Status)] ペインで、[エクスポート (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。



8. [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して追加できます。



9. 追加で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] をクリックします。
 - a. [現在のフローレート (Current Flow Rate) (fps)]
 - b. [前回のエクスポート (Last Export)]
 - c. [最長期間エクスポート (秒) (Longest Duration Export (seconds))]
10. このビュー内の列をいくつか確認してみましょう。
 - a. [エクスポート (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。

- b. [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、エクスポートから 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デバイスが設定されていない可能性があります。
 - c. [前回のエクスポート (Last Export)]列には、前回エクスポートからフローレコードを受信し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、特定の時間帯のみアクティブになる冗長ネットワークリンクに設置されている場合があります。ただし通常は、このフィールドのタイムスタンプが現在でない場合は、エクスポート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。
 - d. [エクスポートのタイプ (Exporter Type)]列には、フローデータを送信するデバイスを FC が認識する方法が表示されます。ほとんどのルータやスイッチは**エクスポート**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、[不明なエクスポート (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ているフローレコードを正しく認識できていない可能性があります。
 - e. [フロータイプ (Flow Type)]列には、エクスポートから生成される NetFlow のバージョンの詳細が表示されます。
 - f. [最長期間エクスポート (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、エクスポートの 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トについて 60 秒に設定してください。そのため [最長期間エクスポート (Longest Duration Export)]列に表示される値は、約 60 秒になります。数百秒または数千秒の値である場合は、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。
 - g. [SNMP ステータス (SNMP Status)]列には、SMC が SNMP 経由でエクスポート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表示されます。SMC がエクスポート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、エクスポートに対して誤った 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 からエクスポート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。
11. 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ト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. 不明なエクスポートとして表示されているエクスポートはあるか。
 - i. エクスポートでの 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トはあるか。
 - i. エクスポートでの 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トはあるか。
 - i. 以前有効であったエクスポートが、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. [最長期間フロー (Longest Duration Flow)]の値が 60 秒を大幅に超えているエクスポートはあるか (フローセンサーを除く)。

- i. エクスポート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エクスポートはあるか (SNMP 経由で SMC によってクエリされないため、FS では NA と表示されます)。
 - i. SMC がエクスポート (FW、ACL など) に到達できないか、このデバイスの SNMP が SMC で正しく設定されていません。このラボでは、これに対するアクションは必要ありません。

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

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ト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、他のエクスポートと同じ基準を適用する必要はありません。特に [最長期間フロー (Longest Duration Flow)] と [SNMP ステータス (SNMP Status)] は無視して構いません。

エクスポートについては、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。

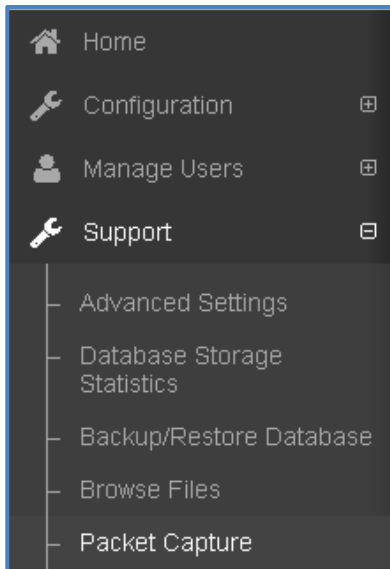
このシミュレートされた環境では、FE が修正のためにエクスポート上で実施するアクション項目はありません。お客様環境では、FE はエクスポートのリストを CSV ファイルとしてエクスポートし、調査が必要なデバイスとその理由を示したリストをお客様用に作成してください。

13. エクスポートが 1 つ欠落しています。エクスポート **172.16.16.4** が FC に表示されていません。このエクスポートデバイスの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

エクスポート 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、エクスポートからの 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。この環境では、フローレコードはエクスポートによって作成され、その後 UDP Director に送信されます。UDP Director はルールに基づいてそれを FC に転送します。FC からエクスポートへと逆方向に確認することで、トラブルシューティング プロセスを開始します。

1. Chrome を開き、**FC** のブックマークを選択して FC 管理インターフェイスにログインします。
 - a. 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。
2. [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。



3. FC に表示されない最初のエクスポートの IP アドレスに対して、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設定を構成します (次のページで続行)。
 - 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**

Capture Setup

Name:	Exporter1
Interface:	eth0
Host IP Address:	172.16.16.4
Port:	Any
Duration (seconds):	300
Packets (100,000 max):	5000

4. 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。
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。

Captures

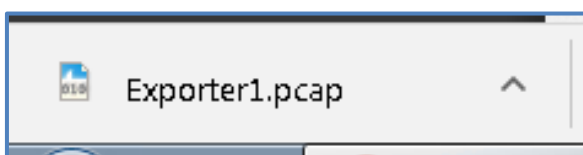
Name	Status	Size(bytes)	Start Time	End Time	Duration(sec)	Action
Exporter1	Running	0	2017-02-01 13:10:44		5	Stop Capture

6. [サイズ (バイト) (Size(bytes))] 列を確認します。0 バイトのままになっているため、キャプチャが現在のフィルタに基づいてデータを収集していないことがわかります。**60 秒後** ([時間 (Duration)] 列)、十分に時間が経過したところで [キャプチャの停止 (Stop Capture)] ボタンをクリックします。
 - a. **注**：実稼働環境では、設定の正しくないエクスポートがトラフィックを送信するのに時間がかかる可能性があるため、より長時間キャプチャすることをお勧めします。
7. キャプチャを停止した後、サイズが 24 バイトに変わっています。これは pcap ファイルの基本フォーマットですが、開いて確認します。
8. キャプチャの [名前 (Name)] 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、[保存 (Save)] をクリックします。

Captures

Name	Status	Size(bytes)	Start Time	End Time	Duration(sec)	Action
Exporter1	Complete	24	2017-02-01 13:10:44	2017-02-01 13:15:45	300	Rerun Delete

9. 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。**Exporter1.pcap** ファイルをクリックして、ローカルにインストールされている Wireshark アプリケーションで開きます。



10. 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 エクスポートからデータを受信していません。Wireshark を閉じます。

注：プロンプトが表示されても Wireshark をアップグレードしないでください。ラボでは必要ありません。

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。

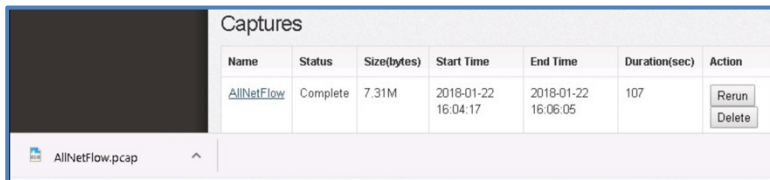
11. 念のため、次の設定で FC でパケットキャプチャを実行し、パケットキャプチャによって**すべての** NetFlow トラフィックをキャプチャできることを確認します。

- 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) (Duration (seconds))] : **300**
- f. [パケット数 (Packets)] : **5000**

Capture Setup	
Name:	AllNetFlow
Interface:	eth0
Host IP Address:	
Port:	netflow (2055)
Duration (seconds):	300
Packets (100,000 max):	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。エクスポートの設定によっては、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。

12. このキャプチャは、キャプチャ設定で別途指定した最大パケット数 (5,000) により、300 秒が経過する前に終了する可能性があります。
13. キャプチャが終了してリンクが使用可能になったら、[AllNetFlow] をクリックしてファイルを [保存 (Save)] します。
14. Chrome で **AllNetFlow.pcap** ファイルのリンクをクリックして、Wireshark で開きます。



15. 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。
16. Wireshark アプリケーションを最大化します。
17. Wireshark ページ上部の [プロトコル (Protocol)] 列にある CFLOW というパケットを選択します。
18. **中央ペイン**で、関連する [>] をクリックして [Cisco NetFlow/IPFIX] を展開し、[FlowSet 1] を展開して、調査する**各フロー (フロー番号)**を展開します。
 - a. 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、またはエクスポートの設定を修正する必要があるかなどを確認できます。
 - b. これは、ルータやその他のデバイスコンソールにアクセスすることなく、エクスポート設定テンプレートの問題を特定するのに最適な方法です。

```

11 0.227994 198.18.128.158 198.19.20.137
12 0.593717 172.16.16.3 108.10.20.127

```

```

SourceId: 0
  FlowSet 1 [id=265] (4 flows)
    FlowSet Id: (Data) (265)
    FlowSet Length: 412
    [Template Frame: 745 (received after this frame)]
  Flow 1
    Flow Id: 59531052
    SrcAddr: 10.201.0.16
    SrcPort: 52938
    InputInt: 3
    DstAddr: 67.228.254.20
    DstPort: 53
    OutputInt: 2
    Protocol: UDP (17)
    IPv4 ICMP Type: 0
    IPv4 ICMP Code: 0
    Post NAT Source IPv4 Address: 209.182.184.2
    Post NAT Destination IPv4 Address: 67.228.254.20

```

注：これは NetFlow のトラブルシューティングに非常に役立ちます。1 つの NetFlow パケットに個別のフローレコードが多数含まれる場合があります。また、エクスポートを通じて送信された特定のフィールドや、NetFlow のバージョンも確認できます。FC がフローデータを正しく処理しているかどうかを確認するには、パケットキャプチャを実行して、送信されたフローデータが正しくフォーマットされているかどうかを確認します。

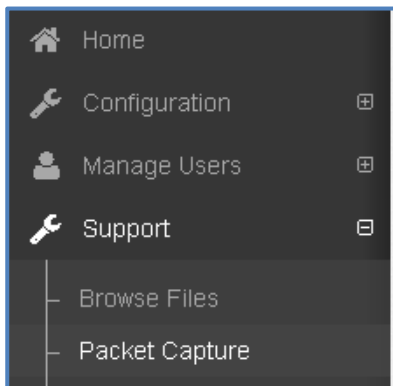
19. この FC がフローデータを認識していることを確認しましたが、さらにキャプチャファイルの調査を続けると (Wireshark の [送信元 (Source)] 列をクリックして、エクスポートを IP アドレスで並べ替えてみてください) 、172.16.16.4 からの UDP/2055 トラフィックが表示されないことがわかります。
 - a. FC がこのエクスポートからのフローデータを認識していないのはなぜでしょうか。
 - b. 引き続き、エクスポートの方向にさかのぼってトラブルシューティングを継続して、この問題を調査しましょう。次に調査するデバイスは UDP Director です。

UDP Director への NetFlow トラフィックの確認

172.16.16.4 のエクスポートの NetFlow トラフィックが FC アプライアン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。次のような問題の可能性が考えられます。

- 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：エクスポートの設定が正しくない。
 - 解決策：問題のエクスポートからの 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：問題のエクスポートからの 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：エクスポートが正しく設定されていないか、UDP 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、UDP がトラフィックを FC に転送していない。
 - 解決策：問題のエクスポート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別のポートで 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 UDP 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ト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：エクスポートの 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、エクスポートデバイスの NetFlow 設定を調査します。

1. Chrome のブックマークで **UDP** を選択し、UDP Director 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。
 - a. 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。
2. [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。



- FC に表示されない最初のエクスポートの IP アドレスに対して、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)]: **UDPD1**
- [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**

Capture Setup	
Name:	UDPD1
Interface:	eth0
Host IP Address:	172.16.16.4
Port:	Any
Duration (seconds):	300
Packets (100,000 max):	5000

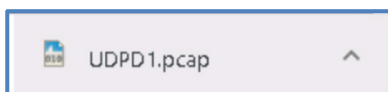
- [スタート (Start)] をクリックします。
- パケットキャプチャが、このページの下部にある [キャプチャ (Captures)] セクションに表示されます。5 分以上経過してキャプチャタイマーが時間切れになってから次に進みます。

Name	Status	Size(bytes)	Start Time	End Time	Duration(sec)	Action
UDPD1	Running	724.99k	2020-01-25 02:55:53		35	Stop Capture

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。[UDPD1] リンクをクリックし、[保存 (Save)]をクリックします。

Name	Status	Size(bytes)	Start Time	End Time	Duration(sec)	Action
UDPD1	Complete	4.64M	2020-01-25 02:55:53	2020-01-25 03:00:53	300	Rerun Delete

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せん。UDPD1.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。

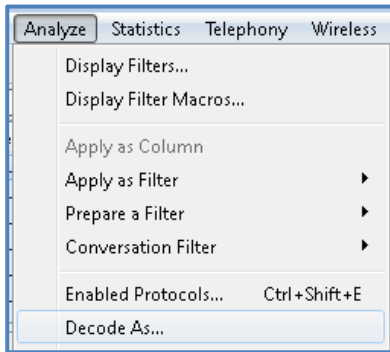


8. Wireshark アプリケーションが pcap ファイルを開きます。見つからないエクスポートから UDPD Director に送信されたパケットが確かにあることがわかります。ただし、パケットの宛先ポート番号に注目してください。デバイスが、本来のポート 2055 ではなく、ポート 2505 に送信するように誤って設定されているように見えます。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.16.4	198.19.20.139	UDP	130	64288 → 2505 Len=88
2	1.468605	172.16.16.4	198.19.20.139	UDP	1490	64293 → 2505 Len=1448
3	1.475464	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
4	1.476528	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
5	1.477933	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
6	1.478932	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
7	1.488285	172.16.16.4	198.19.20.139	UDP	1490	64293 → 2505 Len=1448
8	1.489260	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
9	1.490346	172.16.16.4	198.19.20.139	UDP	1486	64293 → 2505 Len=1444
10	1.491383	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
11	1.492445	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432
12	1.493412	172.16.16.4	198.19.20.139	UDP	1474	64293 → 2505 Len=1432

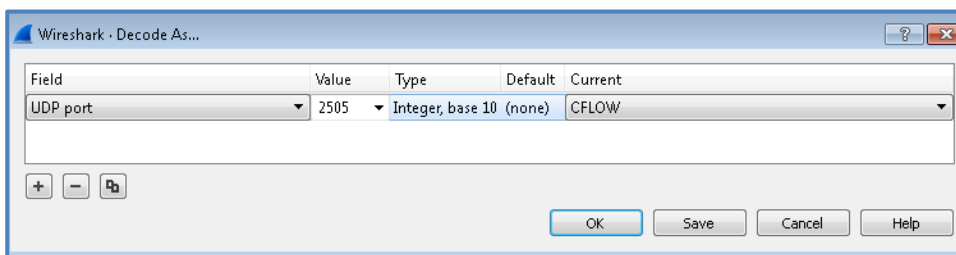
> Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
 > Ethernet II, Src: VMware_b8:01:11 (00:50:56:b8:01:11), Dst: VMware_b8:4f:c4 (00:50:56:b8:4f:c4)
 > Internet Protocol Version 4, Src: 172.16.16.4, Dst: 198.19.20.139
 > User Datagram Protocol, Src Port: 64288, Dst Port: 2505
 > Data (88 bytes)

9. ここで、UDP パケットが確かに NetFlow レコードであることを確認します。
10. [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。

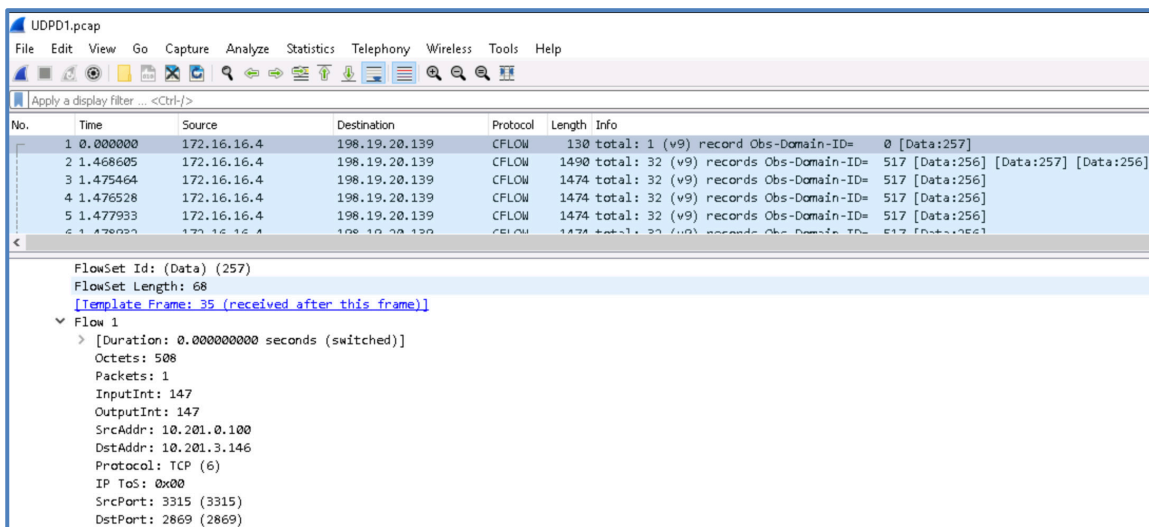


11. [名前を付けてデコード (Decode As)] 画面の**プラス記号**をクリックします。次の値を使用して設定し、[OK] をクリックします。

- a. [フィールド (Field)] : **UDP ポート (UDP Port)**
- b. [値 (Value)] : **2505**
- c. [タイプ (Type)] : **整数、10 進数 (なし) (Integer, base 10 (none))**
- d. [現在 (Current)] : **CFLOW**



12. パケットアナライザは、パケットを NetFlow (CFLOW) として解釈するようになります。パケットが実際の NetFlow レコードであり、想定外のポートに送信されているだけであることがわかります。



13. **Wireshark** アプリケーションを閉じます。

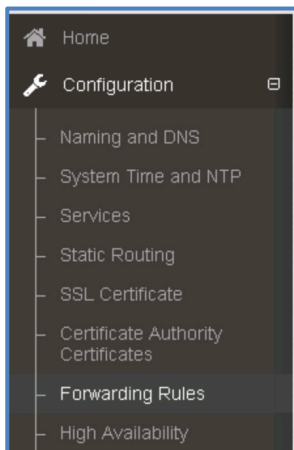
14. 次に UDP Director で転送ルールを作成し、UDP 2505 トラフィックを FC のポート 2055 に転送し、FC がデータを処理できるようにします。

注：導入中にこれと同様の状況が発生した場合は、限られた作業時間を使ってお客様のネットワークチームにデバイスの設定変更をしてもらうより、UDPD ルールを追加して、導入の早い段階で可能な限り多くの NetFlow トラフィックを処理できるようにする方が効率的です。転送ルールを作成してデータを取り込み、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 のポート 2055 向けの標準ルールによってトラフィックが転送されます。

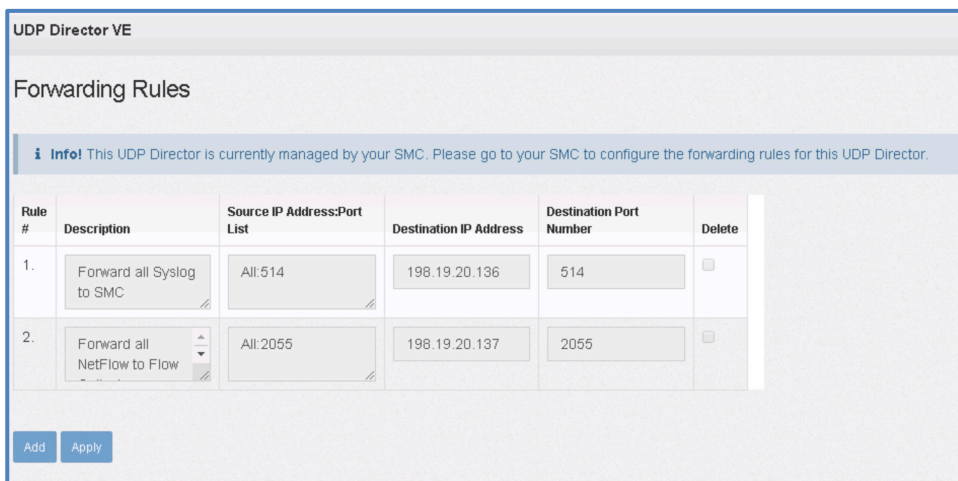
環境によっては、UDP Director をまったく使用せず、すべての NetFlow データを直接 FC に送信する場合があります。FC では、一度に 1 つのポートでのみ NetFlow を処理できます。その場合は、エクスポートデバイスの設定を変更して、期待どおりにポート 2055 に送信する必要があります。

15. Chrome ブラウザの **UDP Web 管理インターフェイス**に戻ります。

16. [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。



17. この UDP Director アプライアンスが SMC によって管理されるようになったため、[転送ルール (Forwarding Rules)] を編集できないことを確認してください。

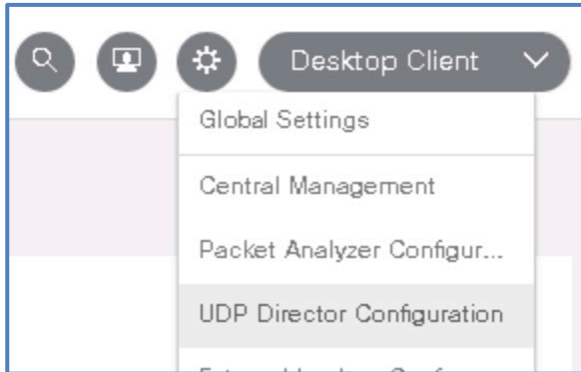


18. Chrome Web ブラウザをもう 1 つ開くか、Chrome 内で別のタブを開きます。


19. Chrome のブックマークで **SMC** を選択し、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。

- a. 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。
- b. Stealthwatch SMC の Web インターフェイスにログインしています。

20. [デスクトップクライアント (Desktop Client)]の近くにある**歯車アイコン**を選択し、[UDP Director 設定 (UDP Director Configuration)]を選択します。




21. UDP Director ルールを編集するには、UDP エントリの横にある [アクション (Actions)]アイコンを選択し、[転送ルールの設定 (Configure Forwarding Rules)]を選択します。

UDP Director Configuration				
UDP Directors				
Name	Device IP	Device Model	Management Channel Status	Actions
UDP	198.19.20.139	UDVE	● Last Seen : 3:08 AM 01/25/2020	

22. 同じ送信先とポートの組み合わせに対して複数のルールを設定することはできません。ポート 2505 に着信したトラフィックをポート 2055 にリダイレクトするには、2055 の既存ルールを変更する必要があります。

23. [すべての NetFlow をフローコレクタに転送 (Forward all NetFlow to Flow Collector)]ルールを変更するには、[宛先 IP アドレス (Destination IP Address)]と[ポート番号 (Port Number)]が 198.19.20.137 2055 の行の [アクション (Actions)]アイコンをクリックし、[編集 (Edit)]をクリックします。

RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER	ACTIONS
1	Forward all Syslog to SMC	All:514	198.19.20.136	514	
2	Forward all NetFlow to Flow Collector	All:2055	198.19.20.137	2055	<div style="border: 1px solid gray; padding: 2px;"> Edit Delete </div>

24. [送信元 IP アドレス : ポート (Source IP Address: Port)]を編集して **All:2505** を追加します。

Forwarding Rule

DESCRIPTION (OPTIONAL)

Forward all NetFlow to Flow Collector

SOURCE IP ADDRESS:PORT *

All:2055
All:2505

DESTINATION IP ADDRESS *

198.19.20.137

DESTINATION PORT NUMBER *

2055

25. [保存 (Save)] をクリックします。

26. UDP Director の変更を確定するには、[同期 (Sync)] をクリックします。

Discard Edits Sync

Add New Rule Import/Export ▾

27. 間もなく、成功の通知と更新されたルールが表示されます。

Forwarding Rules | UDPD - 198.19.20.139

✓ Success! Forwarding rules have been sent to your UDP Director. Any forwarding rules deemed invalid will not be forwarded to your UDP Director and will not appear in the table below.

Discard Edits Sync

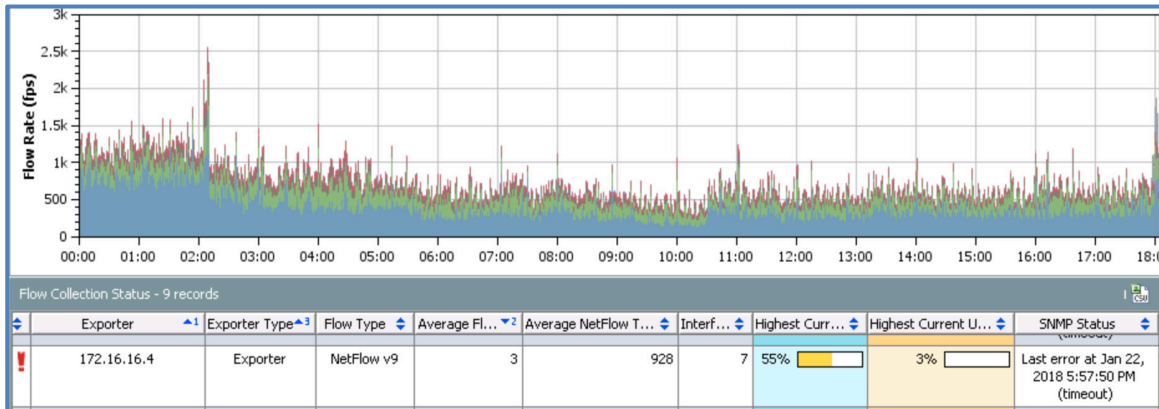
Q Global Search Add New Rule Import/Export ▾

RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER	ACTIONS
1	Forward all Syslog to SMC	All:514	198.19.20.136	514	⊙
2	Forward all NetFlow to Flow Collector	All:2505 All:2055	198.19.20.137	2055	⊙

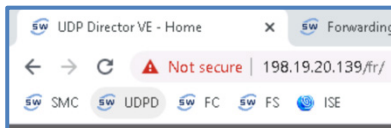
- a. これでお客様は、誤ったポート (2505) に送信されている NetFlow レコードを使用でき、そのネットワークセグメントを可視化できました。

28. フローコレクタが Stealthwatch デスクトップクライアントの FC ダッシュボードドキュメントでこのフローを処理できることを確認します。デスクトップクライアントを開き、[エンタープライズ (Enterprise)] ツリーの [FCNF] フローコレクタに移動して、[FCNF] フローコレクタをダブルクリックします。

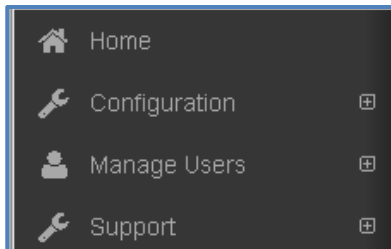
- a. FC ダッシュボードの [フローコレクションステータス (Flow Collection Status)] ペインに、**172.16.16.4** エクスポートが表示されていることを確認します。UDP Director ルールの変更後、フローが到着するまでに 1 分ほどかかる場合があります。



29. UDP Director のラボを終了する前に、UDP Director アプライアンスを使用して、受信しているフローに関するより詳細な情報を提供する方法を紹介します。
30. Chrome ブラウザで **UDP** ブックマークをクリックして **UDP 管理** Web ページを開くか、そのページに戻ります。



31. [ホーム (Home)] メニューオプションをクリックします (Web ページの上部に「UDP Director VE」と表示されていることを確認します)。

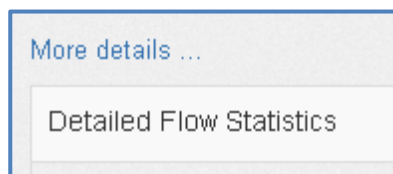


32. UDPD のホームページに [詳細なフロー統計情報 (Detailed Flow Statistics)] オプションがあります。これはアプライアンスの CPU 使用率が増加するため、デフォルトでオフになっています。
 - a. [有効化 (Enable)] ボックスにチェックマークを入れて、このオプションをオンにします。



注：このオプションをオンにすると、Flow Estimator が有効になります。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、各エクスポート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トの 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。お客様の多くは、ネットワークが生成する FPS 数を確認する方法がありません。お客様環境からの FPS のボリュームを判定する目的で、トライアルライセンスで UDPD/UDVE を導入できます。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 UDVE の価値を認識し、Stealthwatch の注文に UDVE のライセンスを含めるきっかけになることです。

33. 統計情報ペインに情報が表示されるまで、1 分ほど時間が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。



34. [ステータスレポート (Status Report)] ページが開き、UDP データの [送信元 (Inbound Sources)] と [宛先 (Outbound Destinations)] 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 UDP Director に送信するデバイスがあり、受信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。

Inbound Sources		
Source	Packet Rate for Last Minute (pps)	Packets Today
198.19.20.138:2055	35.48	8.39k
172.16.16.4:2505	12.20	3.01k
172.16.16.1:2055	5.38	2.05k
172.16.16.2:2055	3.85	1.05k
172.16.16.3:2055	3.13	1.02k
198.18.128.138:2055	3.13	731
198.19.20.1:2055	0.90	189
172.16.16.50:2055	0.32	19

Outbound Destinations		
Destination	Packet Rate for Last Minute (pps)	Packets Today
198.19.20.137:2055	52.20	13.44k
198.19.20.137:2055	12.20	3.01k

35. 転送ルールを確認したら、メニューの [ホーム (Home)] をクリックします。

36. 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。UDP Director が処理した FPS の統計を UDP Director が計算していることがわかります。(注: コンソールに表示されるまでに少し時間がかかる場合があります。次の図を確認して、ラボを先に進めても構いません)。

Detailed Flow Statistics				
				<input checked="" type="checkbox"/> Enable
	95th FPS	Maximum FPS	Average FPS	Errors
Current	920	920	595	0

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。これと同じ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。

System			
IP Address:	198.19.20.139	Domain name:	dcloud.cisco.com
Host name:	UDPD	Load Average:	0.50, 0.29, 0.16
Total Memory:	4G		
VM Server Memory:	None reserved, limit 3T		

37. 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トをお客様のネットワーク オペレーション スタッフに報告しました。
38. **Chrome** ブラウザと **Notepad++** アプリケーションを閉じて、この時点で開いているタブやアプリケーションをクリアアップします。

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ト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。

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 エクスポートの問題は通常、お客様が簡単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。

第 1 日のコンテンツ終了

これで、第 1 日のラボのシナリオのコンテンツは終了します。同じセッションの中で第 2 日のコンテンツに進む場合は、開いているウィンドウをすべて閉じてから続行してください。

シナリオ 10. お客様環境の分類

ネットワーク上のホストや IP アドレスについて、お客様は常に完全に正確なデータを把握できるわけではありません。お客様がデータを利用できない場合や、お客様が提供するデータが不完全または不正確である場合もあります。それによって、お客様のネットワークをホストグループに分類するタスクが複雑になる可能性があります。

Stealthwatch では、特定のタイプのネットワークアクティビティを生成しているホストを検索し、そのホストに特定のアクティビティが許可されているかをお客様に確認し、さらに適切な IP アドレスまたは範囲を使用して、既存のホストグループを編集するか新規にホストグループを作成して Stealthwatch 内で分類することができるため、ホストの分類が効率化されます。

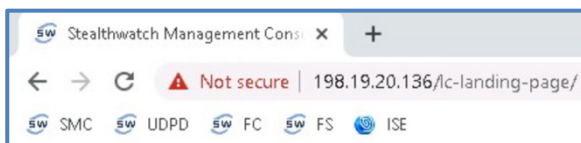
お客様からは、Stealthwatch に入力するための少量の IP 分類データが提供されていました。ここでは、IP アドレスを識別するその他のサーバタイプと動作を特定します。これはお客様の確認後に分類できます。

パブリック IP 空間の分類

お客様が、所有、管理、使用しているすべてのパブリック IP 空間を示すリストを持っていることは稀です。お客様の IP 空間を正しく分類して、内部ホストと外部ホストとして扱えるようにすることが重要です。お客様からは、環境内で使用しているパブリック IP 範囲がすでに提供されています。ここで Stealthwatch を使用して、[すべてを捕捉 (Catch All)] するホストグループに追加する必要があるパブリック IP またはネットワークがないことを確認します。

お客様が所有するパブリック IP 空間を特定する 1 つの方法は、送信元と宛先の両方が外部ホストであるフローを探すことです。両方のホストが実際にお客様のネットワークの外部にある場合は、Stealthwatch にはネットワーク トランザクションが含まれたフローデータのレコードは存在しません。したがって、フロー内の少なくとも 1 つの IP アドレスがお客様によって管理されている可能性があります。「外部ホスト同士のトラフィック」でフィルタリングして [上位カンパセーション (Top Conversations)] ドキュメントを実行すると、お客様所有として分類可能な IP アドレスの特定に役立ちます。

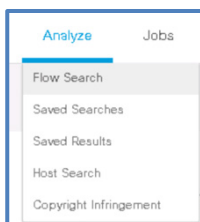
1. WKST1 で **Chrome** Web ブラウザを開き、**SMC** ブックマークを選択して SMC に接続します。



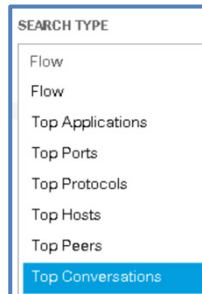
- a. 認証のプロンプトが表示されたら、ユーザ名 : **admin**、パスワード : **C1sco12345** を入力します。

- i. [ユーザ名 (Username)] : **admin**
- ii. [パスワード (Password)] : **C1sco12345**

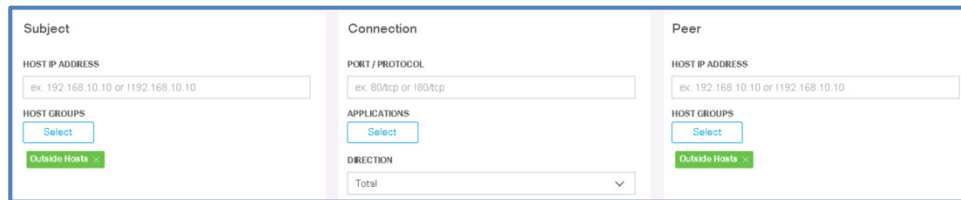
2. [分析 (Analyze)] をクリックしてから、[フロー検索 (Flow Search)] を選択します。



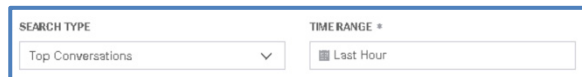
- a. [検索タイプ (Search Type)] フィールドで、[上位カンパセーション (Top Conversations)] をクリックします。



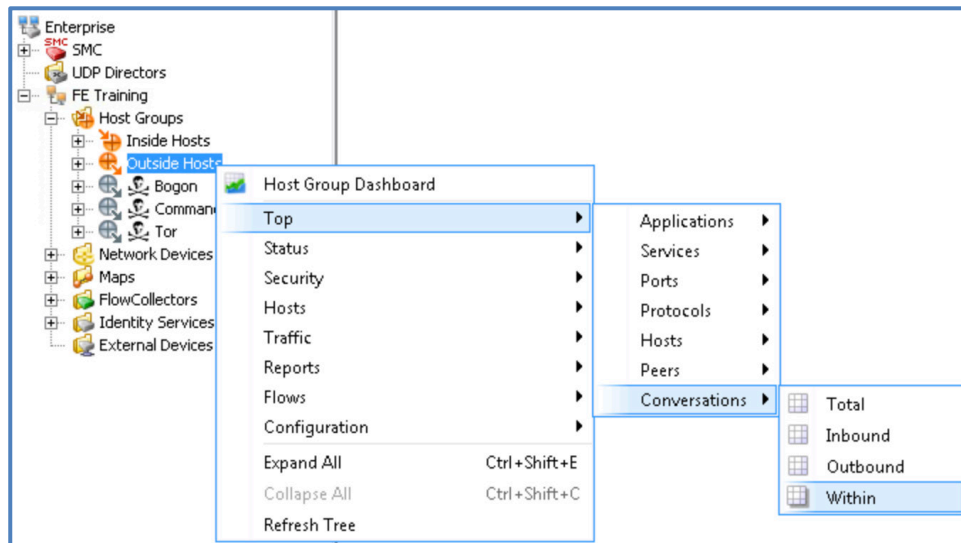
- b. [サブジェクト (Subject)]と[ピア (Peer)]の両方で、[ホストグループ (Host Groups)]を [外部ホスト (Outside Hosts)]に設定します。それぞれ、[選択 (Select)]をクリックしてから [外部ホスト (Outside Hosts)]をクリックする必要があります。



- c. [時間範囲 (Time Range)]で [過去 1 時間 (Last Hour)]を選択します。



- d. [検索 (Search)]をクリックします。



注：このタイプの検索は、デスクトップクライアントで実行することもできます。その場合、[上位カンパセーション (Top Conversations)]ドキュメントのタイプを「Within (内部) 」と指定します。これにより、送信元と宛先の IP アドレスが両方とも同じホストグループ内である (選択されたホストグループ内に留まる) フローを探していることを、システムに伝えることができます。

上記の図は、デスクトップクライアントで同様のフローを探す方法の例です。

3. 次の例の結果では、209.182.185.0/24 範囲の IP アドレスがリスト内で数回表示されているようです（ホストまたはピア列のいずれか）。
 - a. これは、209.182.185.0 ネットワーク内のアドレスが、お客様が所有するネットワークの一部である可能性を示しています。

注：必要に応じて Stealthwatch 以外のツールを使用して、調査中のパブリック IP アドレスに関する追加情報を収集できます。これには、WHOIS、DNS、または IANA 登録データを提供するサイトが含まれます。Stealthwatch では、これらのいくつかのツールを外部参照機能として使用できます。パブリック IP アドレスを右クリックして、[外部参照 (External Lookup)] メニューを選択します。

Top Conversations Search Results (51)

Edit Search Last 5 minutes (Time Range) Save Search Save Results Start New Search

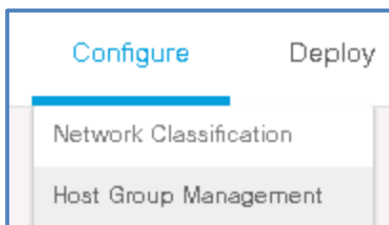
Subject: Outside Hosts (Host Groups) Ether (Orientation) 100% Complete Delete Search

Connection: Total (Direction)

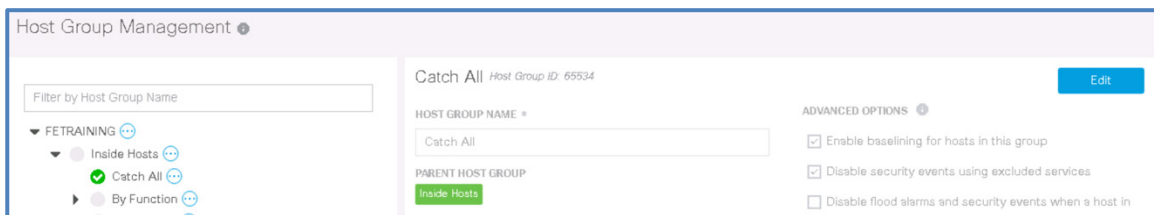
Peer: Outside Hosts (Host Groups)

% OF BYTES	HOST IP ADD...	HOST NAME	HOST ROLE	PEER IP ADDR...	PEER NAME	PORT	BYTES	PACKETS	FLAWS	HOST BY
16.50%	72.8.8.2	static-72-8-8-2.ngn.onecommunications.net	Client	209.182.185.22	--	50519 / TCP	39.98 M	49.14 K	1	0.63%
16.50%	209.182.185.22	--	Server	72.8.8.2	static-72-8-8-2.ngn.onecommunications.net	50519 / TCP	39.98 M	49.14 K	1	99.37%
0.50%	209.182.185.222	--	Client	65.54.51.252	--	443 / TCP (https)	496.72 K	587	1	97.64%
0.50%	65.54.51.252	--	Server	209.182.185.222	--	443 / TCP (https)	496.72 K	587	1	98.38%
0.55%	209.182.185.26	--	Server	68.4.95.92	ip68-4-95-92.oc.oc.cox.net	443 / TCP (https)	485.85 K	1.23 K	1	99.01%
0.55%	68.4.95.92	ip68-4-95-	Client	209.182.185.26	--	443 / TCP	485.85 K	1.23 K	1	99.99%

4. お客様に調査結果を提出したところ、お客様が実際に **209.182.185.0/24** の IP 範囲を所有していることが確認されたため、この IP 範囲は「お客様の管理対象」となり、内部ホストとしてとして分類する必要があります。次に、[すべてを捕捉 (Catch All)] ホストグループを編集して範囲を追加します。
5. [設定 (Configure)] > [ホストグループ管理 (Host Group Management)] に移動します。



6. [内部ホスト (Inside Host)] の下にネストされている、[すべてを捕捉 (Catch All)] ホストグループをクリックします。選択したら、[編集 (Edit)] をクリックします。



- 新しい **209.182.185.0/24** ネットワークを追加します。

Catch All *Host Group ID: 655*

HOST GROUP NAME *

Catch All

PARENT HOST GROUP

Inside Hosts

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES ●

192.168.0.0/16
198.19.10.0/24
198.19.20.0/24
198.19.30.0/24
209.182.184.0/24
209.182.185.0/24
fc00::/7

- [保存 (Save)] をクリックします。
- これで、お客様が使用しているパブリックアドレス空間を検出し、正しく分類しました。ラボの次の手順に進みます。

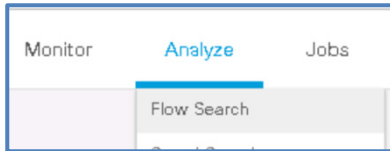
注： ホストグループのメンバーシップの変更は、ホストグループのメンバーシップ編集後に FC によって処理された、新しいフローに対してのみ影響します。このケースでは、209.182.185.0/24 範囲の IP アドレスが、これ以降は内部ホストのメンバーとしてのみ表示されることとなります。ホストグループの編集前の過去の期間に対してドキュメントが実行されると、追加された IP アドレスは、変更前の外部ホストのメンバーとして表示されます。

お客様のパブリック IP スペースを正しく分類することで、内部ホストと外部ホストの通信に関係する、データ損失の疑い、長いフローの疑い、ホストのビーコンなどのアラームを減らせます。

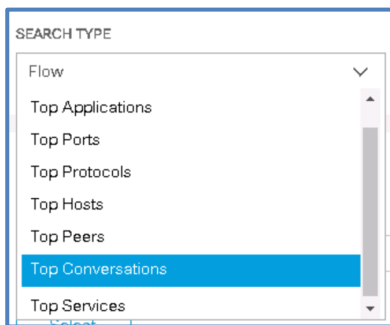
パブリック IP スペースの分類：その他の検索方法

前のクエリでは、お客様が所有している可能性のある外部 IP 範囲を探すために、外部ホストを接続の両側（サブジェクトとピア）に追加しましたが、接続方向オプションを使用して Web クライアント内でクエリを実行することもできます。

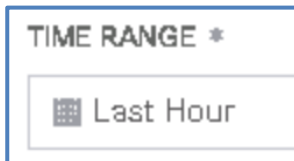
1. [分析 (Analyze)]、[フロー検索 (Flow Search)] の順に選択します。



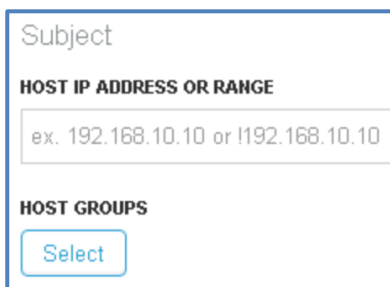
2. [検索タイプ (Search Type)] ドロップダウンで、[上位カンバセーション (Top Conversations)] を選択します。



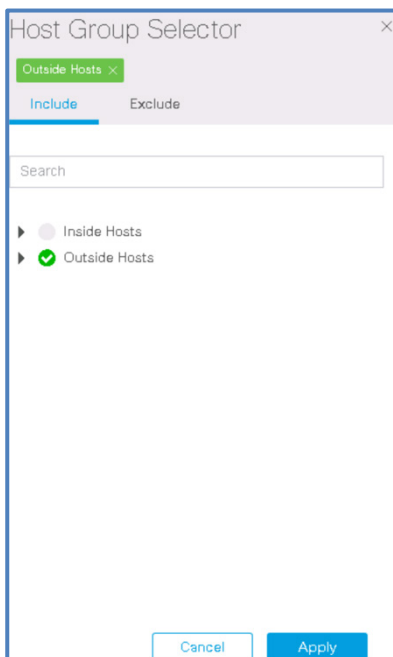
3. [時間範囲 (Time Range)] で [過去 1 時間 (Last Hour)] を選択します。



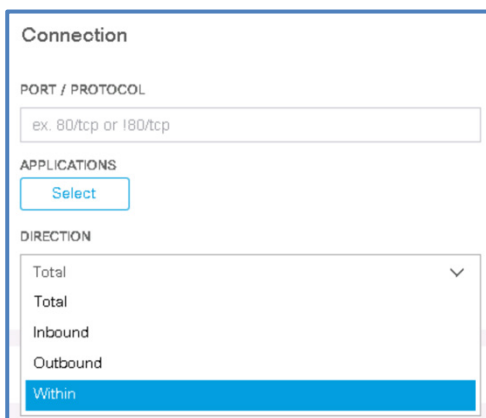
4. [サブジェクト (Subject)] の下にある [選択 (Select)] をクリックします。



5. [ホストグループセクタ (Host Group Selector)] で、[外部ホスト (Outside Host)] をクリックし、[適用 (Apply)] をクリックします。



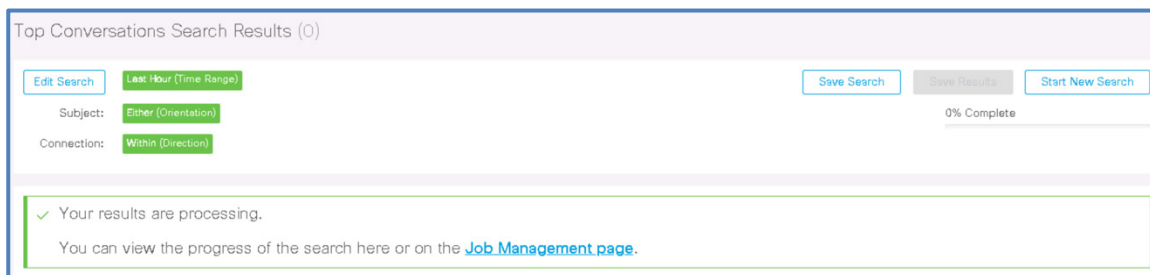
6. [接続 (Connection)] > [方向 (Direction)] をクリックし、[内部 (Within)] を選択します。



7. この検索にはピア情報を設定しないでください。
8. フォームの右上隅で、[検索 (Search)] をクリックします。

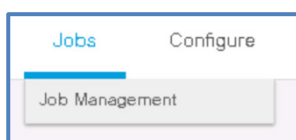


9. クエリの実行には少し時間がかかる場合があります。更新の完了率を確認できます。ラボ環境では、少しの間 0% のままで留まる場合があります。



- a. 返された結果には、209.182.185.0/24 アドレスが依然として表示されています。これはこれらのフローが、[すべてを捕捉 (Catch All)] ホストグループを変更する前に着信したためです。変更後の新しいフローのみが分類されることに注意してください。変更前のフローは再分類されません。

10. [ジョブ (Jobs)] > [ジョブ管理 (Job Management)] の順にクリックします。



- a. ここでは、現在実行しているジョブを確認できます。ジョブを削除したり、ジョブ名をクリックして完了したジョブの結果を表示することもできます。
- b. Web UI のジョブに関して、次のことに注意してください。
 - i. 実行中または保留中のジョブはキャンセルできますが、キャンセルされたジョブは再開できません。
 - ii. 完了およびキャンセルされたジョブは、一定の期間だけこの表に表示されます。レコード数が 10,000 以下のフロー検索の結果は 24 時間利用できます。レコード数が 20,000 以上のフロー検索結果 (CSV のダウンロードによる閲覧のみ) は、7 日間利用できます。
 - iii. Web UI のジョブでは、フィルタで指定した期間内にもっと多くのフローレコードが利用可能な場合でも、フローコレクタごとに約 10,000 のフローレコードをデフォルトとして使用します。要求できる最大フロー数は 400,000 です。
 - iv. レコード数が 10,000 以下のフロー検索およびすべての上位レポートは、レコード数が 20,000 以上のフロー検索とは別のキューで実行されます。
 - v. レコード数がそれぞれ 10,000 以下のジョブを、最大 4 つ同時に実行できます。レコード数が 20,000 以上のレポートは、一度に 1 つしか実行できません。

11. ジョブが完了し、ページの [完了したジョブ (Finished Jobs)] セクションにリストが表示されたら、**ジョブ名をクリック**し、[上位カンバセーション (Top Conversations)] ドキュメントを表示します。

Job Management

Current Jobs

Job Name	Job Owner	Start Date/Time	Progress	Status	Actions
Top Conversations on 10/21/2018 at 11:19 AM	admin	10/21/18 11:20 AM	0%	In progress	

Finished Jobs

Job Name	Job Owner	% Complete	Start Date/Time	End Date/Time	Status	Actions
Top Conversations on 10/21/2018 at 11:17 AM	admin	100%	10/21/18 11:17 AM	10/21/18 11:18 AM	Completed	Delete
Top Conversations on 10/21/2018 at 11:08 AM	admin	100%	10/21/18 11:12 AM	10/21/18 11:20 AM	Completed	Delete

12. 結果が表示されると、前のレポートと同様のカンバセーションが表示されます（タイムフレームは異なります）。お客様に再度、所有している可能性が高い IP アドレスについて確認していただく必要があります。確認後に、[すべてを捕捉 (Catch All)] ホストグループに正しい IP アドレスを入力します。Java クライアントですでにこのタスクを完了しているため、ここでは追加で分類するものではありません。

Top Conversations Search Results (51)

Edit Search Last Hour (Time Range) Save Search Save Results Start New Search

Subject: Outside Hosts (Host Groups) Either (Orientation) 100% Complete Delete Search

Connection: Within (Direction)

% OF BYTES	HOST IP ADD...	HOST NAME	HOST ROLE	PEER IP ADDR...	PEER NAME	PORT	BYTES	PACKETS	FLows	HOST BYTES ...
59%	64.102.254.33	--	Client	209.182.185.22	--	21 / TCP (ftp)	627.14 M	771.66 K	1	0.66%
59%	209.182.185.22	--	Server	64.102.254.33	--	21 / TCP (ftp)	627.14 M	771.66 K	1	89.24%
31%	64.14.29.142	esd.subscribenet.com	Server	209.182.184.8	--	21 / TCP (ftp)	505.37 M	641.07 K	1	89.91%

ネットワークスキャナの分類

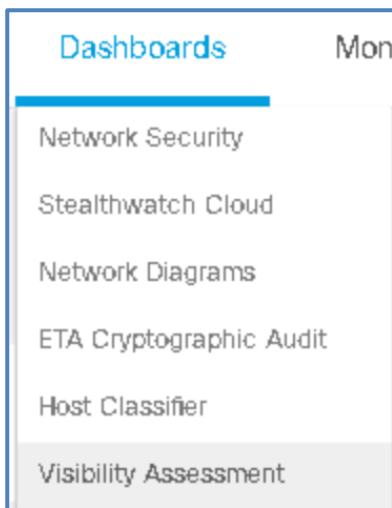
ポートスキャンを実行するネットワーク上のホストによって、Stealthwatch で多量のアラームが発生する場合があります。多くのホストは、脆弱性スキャナ、ネットワークインベントリ/管理システムとしての機能に基づいて通常のアクティビティを実行する無害なホストです。場合によっては開発が不十分なカスタムアプリケーションであることもあります。既知の許可されたネットワークスキャナを分類して、未知のネットワークスキャナとして表示されるホストが、実用的なアラームを生成できるようにすることが重要です。

お客様からネットワーク内の既知のネットワークスキャナの IP データが提供されたため、[ネットワークスキャナ (Network Scanners)] ホストグループに変更を加えて、そのデータを Stealthwatch に追加しました。次に、スキャンアクティビティを実行しているホストを確認して特定し、お客様と連携して、分類が必要な承認済みネットワークスキャナがあるかどうかを判断します。

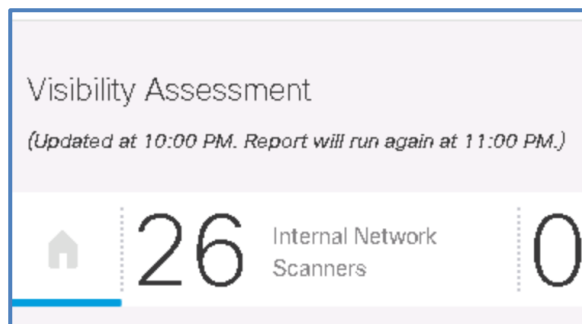
このタスクを実行するには、可視性アセスメントダッシュボード (先にインストール済みの Stealthwatch アプリケーション) を使用します。

注: バージョン 7.1.x 以降では、可視性アセスメントダッシュボードは、お客様環境でネットワークスキャナを表示する際に使用する推奨 Web UI インターフェイスとなっています。

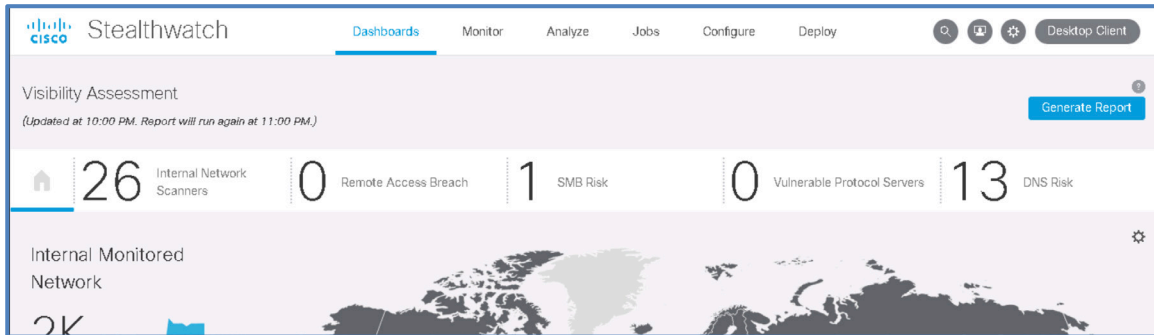
1. **Chrome** を使用して、**admin** ユーザとしてパスワード **C1sco12345** で **SMC** にログインしていることを確認します。
2. [ダッシュボード (Dashboards)]、[可視性アセスメント (Visibility Assessment)] の順にクリックします。



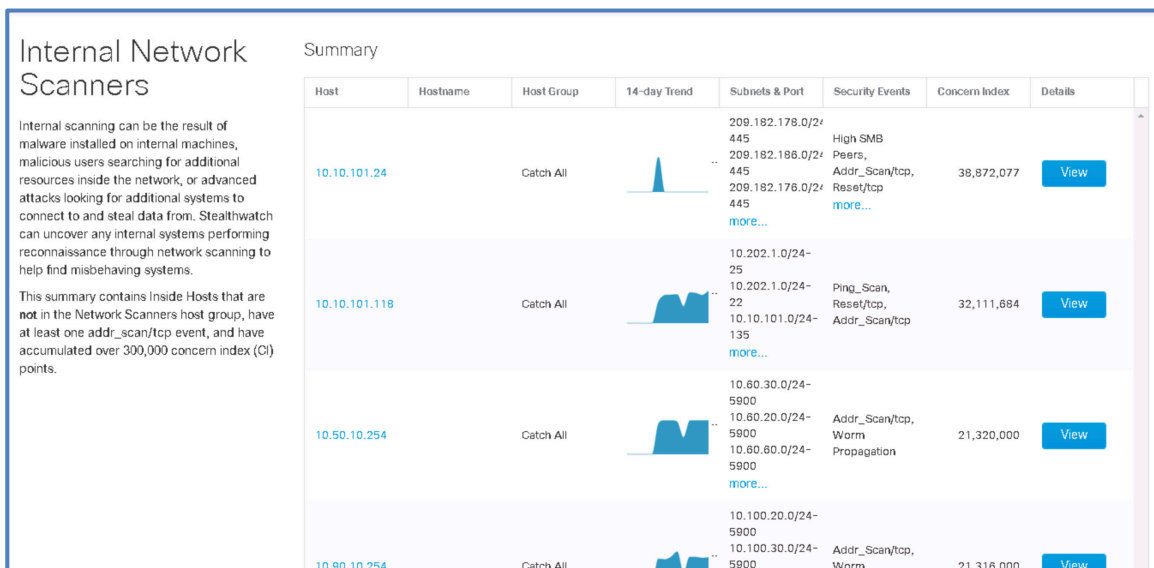
- a. このアプリケーションは 1 時間ごとに実行されます。



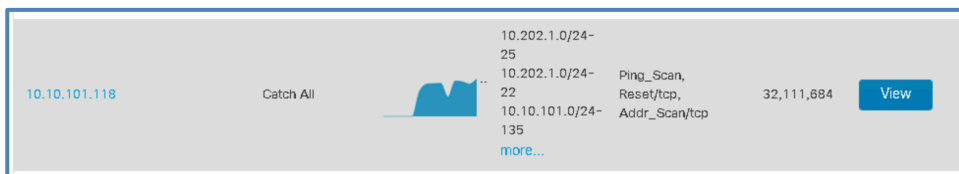
3. ダッシュボードの上部にサマリー行が表示されます。内部ネットワークスキャナの番号をクリックします（以下の図では 26 と表示されています）。



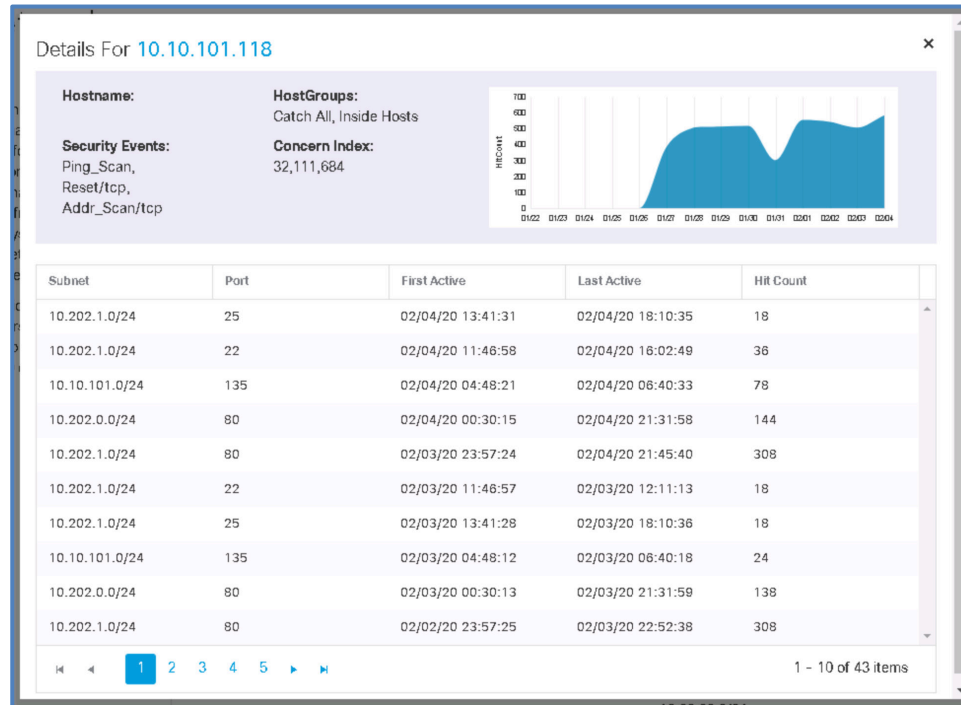
4. ネットワーク内でスキャンアクティビティを実行するシステムについて、複数ページのレポートが表示されます。



5. ドキュメントで IP を選択し、関連する右側の [表示 (View)] ボタンをクリックします。



- a. このホストによって実行されたスキャンアクティビティに関するポップアップレポートが表示されます。

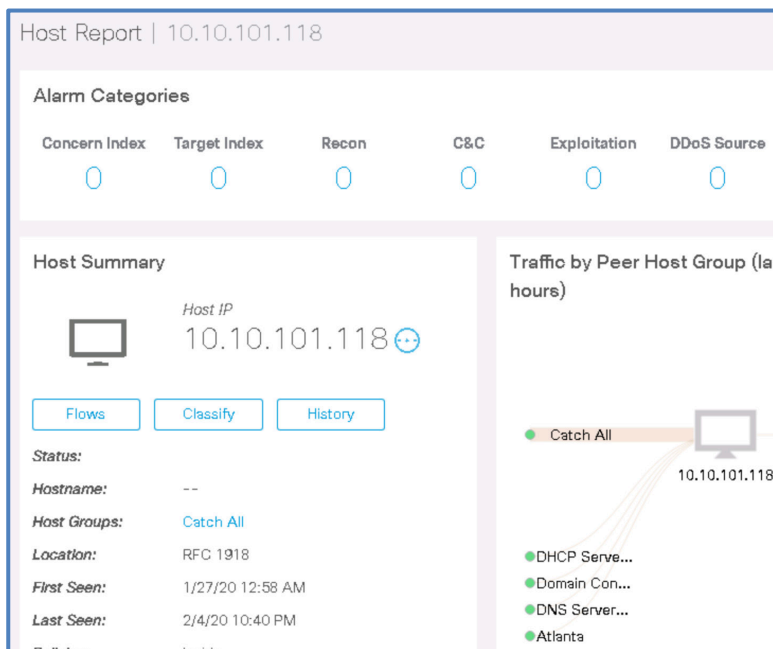


b. データを確認し、右上隅の [X] をクリックして [詳細 (Details)] ページを閉じます。

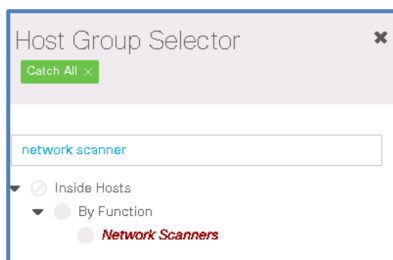
6. このホストをネットワークスキャナとして分類することにします。確認しているホストの IP アドレス をクリックします。



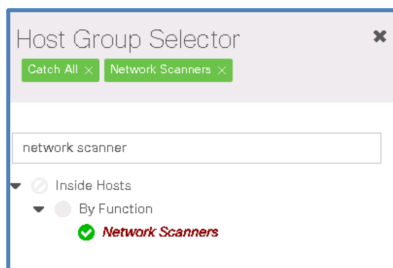
7. この IP アドレスの [ホストレポート (Host Report)] ページが表示されます。必要に応じてここで情報を確認し、[ホストサマリー (Host Summary)] セクションの [分類 (Classify)] をクリックします。



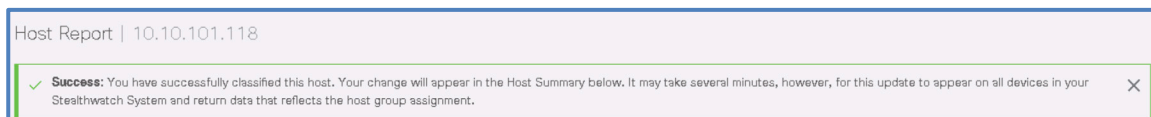
8. [ホストグループセレクタ (Host Group Selector)] が開いたら、検索フィールドに **network scanner** と入力し、**Enter** を押します。



9. [ネットワークスキャナ (Network Scanners)] ホストグループをクリックし、下部の [適用 (Apply)] をクリックします。



10. 成功のメッセージが表示されます。

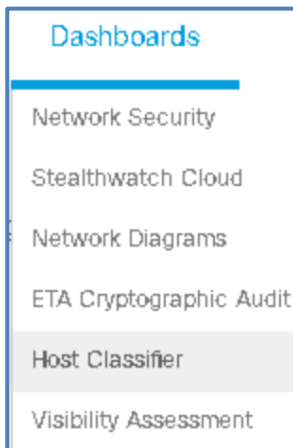


11. 必要に応じて [ダッシュボード (Dashboards)] > [可視性アセスメント (Visibility Assessment)] に戻り、このプロセスを繰り返します。ここでは、追加のネットワークスキャナ分類は実行しないでください。

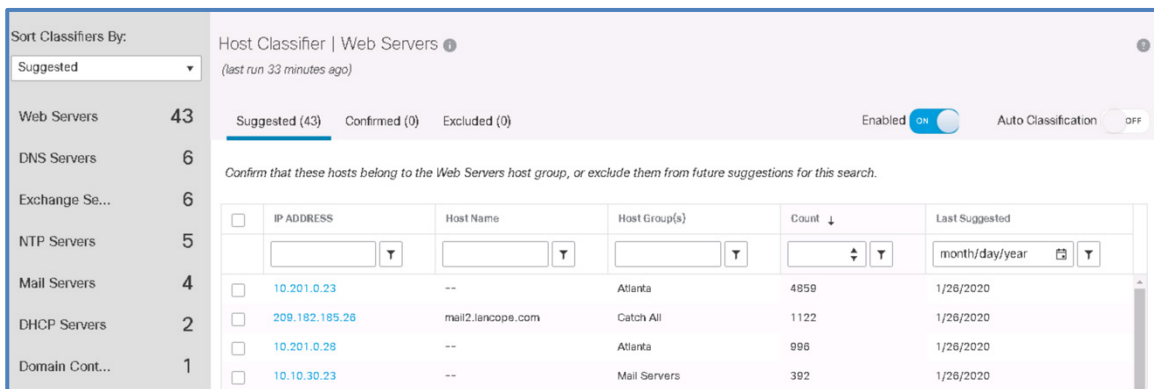
ホスト分類 Stealthwatch アプリケーションの使用

前のシナリオで、ホスト分類 Stealthwatch アプリケーションをインストールしました。ここでは、ホストグループの設定と分類に関連して、このアプリケーションがどのようなデータを提供できるかを確認します。

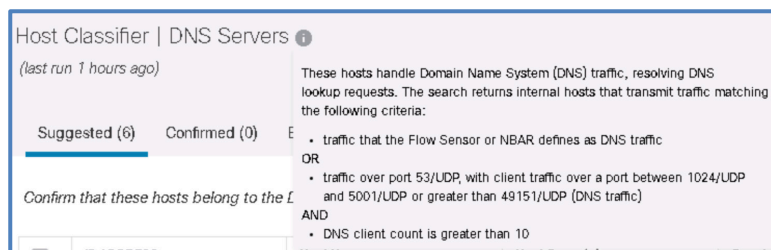
1. Chrome 内で **SMC Web クライアント**に戻ります。
2. [ダッシュボード (Dashboards)]、[ホスト分類子 (Host Classifier)]の順にクリックします。



3. 表示された [ホスト分類子 (Host Classifier)] ダッシュボードを簡単に確認します。



- a. ホスト分類アプリケーションは、お客様のネットワークで分類が必要と思われるホストに関する情報を提供します。
4. ページの左側にある [DNS サーバ (DNS Servers)] をクリックします。
 - a. マウスを [ホスト分類子 | DNS サーバ (Host Classifier | DNS Servers)] の右側の [i] アイコンの上に置きます。



- i. ポップアップには、表内で DNS サーバと考えられるシステムを識別する方法についての説明が表示されます。

Host Classifier | DNS Servers (last run 1 hours ago)

Suggested (6) Confirmed (0) Excluded (0) Enabled ON Auto Classification OFF

Confirm that these hosts belong to the DNS Servers host group, or exclude them from future suggestions for this search.

<input type="checkbox"/>	IP ADDRESS	Host Name	Host Group(s)	Count ↓	Last Suggested
<input type="checkbox"/>	10.201.0.16	--	DNS Servers, NTP Servers, Domain Controllers, Atlanta	196	1/26/2020
<input type="checkbox"/>	10.10.30.15	--	DNS Servers, Domain Controllers	191	1/26/2020
<input type="checkbox"/>	10.201.0.15	--	DNS Servers, NTP Servers, Domain Controllers, Atlanta	170	1/26/2020
<input type="checkbox"/>	10.10.30.16	--	DNS Servers, Domain Controllers	142	1/26/2020
<input type="checkbox"/>	10.201.1.239	--	DNS Servers, Atlanta	69	1/26/2020
<input type="checkbox"/>	209.182.184.2	spyglass.lancope.com	Catch All	26	1/26/2020

- b. DNS サーバの IP アドレスが表示されている上位 5 つのエントリのチェックボックスをオンにし、それ以外はオフにしたまま、[選択内容の確認 (Confirm Selected)] をクリックします。

Host Classifier | DNS Servers (last run 1 hours ago)

Exclude Selected Confirm: Selected

Suggested (6) Confirmed (0) Excluded (0) Enabled ON Auto Classification OFF

Confirm that these hosts belong to the DNS Servers host group, or exclude them from future suggestions for this search.

<input type="checkbox"/>	IP ADDRESS	Host Name	Host Group(s)	Count ↓	Last Suggested
<input checked="" type="checkbox"/>	10.201.0.16	--	DNS Servers, NTP Servers, Domain Controllers, Atlanta	196	1/26/2020
<input checked="" type="checkbox"/>	10.10.30.15	--	DNS Servers, Domain Controllers	191	1/26/2020
<input checked="" type="checkbox"/>	10.201.0.15	--	DNS Servers, NTP Servers, Domain Controllers, Atlanta	170	1/26/2020
<input checked="" type="checkbox"/>	10.10.30.16	--	DNS Servers, Domain Controllers	142	1/26/2020
<input checked="" type="checkbox"/>	10.201.1.239	--	DNS Servers, Atlanta	69	1/26/2020
<input type="checkbox"/>	209.182.184.2	spyglass.lancope.com	Catch All	26	1/26/2020

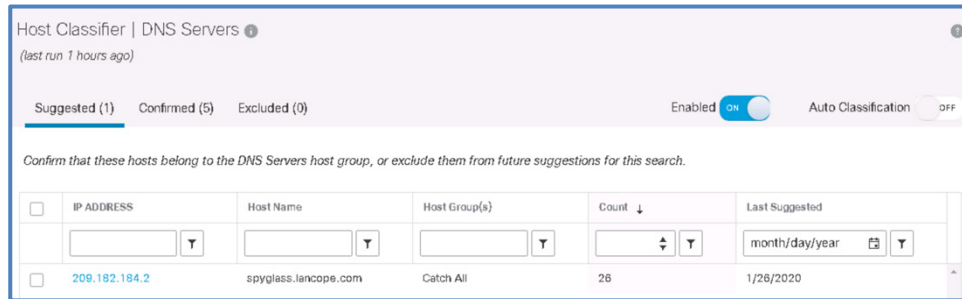
- c. [確認 (Confirm)] をクリックします。

Confirm Selected Hosts

Do you want to confirm the selected hosts?
These hosts will be added to the suggested host group.
It may take several minutes for these changes to be reflected within the host group.

Cancel Confirm

- d. 成功の通知が表示され、更新されたリストが表示されます。[推奨 (Suggested)] (1) および [確認済み (Confirmed)] (5) と表示されていることがわかります。



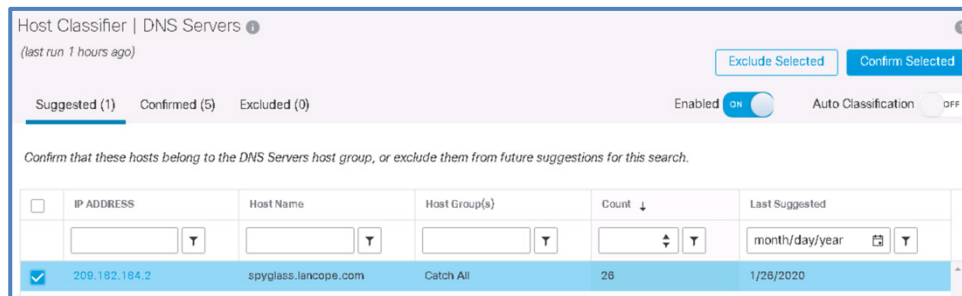
Host Classifier | DNS Servers ⓘ
(last run 1 hours ago)

Suggested (1) Confirmed (5) Excluded (0) Enabled Auto Classification

Confirm that these hosts belong to the DNS Servers host group, or exclude them from future suggestions for this search.

<input type="checkbox"/>	IP ADDRESS	Host Name	Host Group(s)	Count ↓	Last Suggested
<input type="checkbox"/>	209.182.184.2	spyglass.lancope.com	Catch All	26	1/26/2020

- e. お客様より、209.182.184.2 は承認された DNS サーバではないため、除外するよう依頼されています。この IP アドレスの **チェックボックス** をクリックし、[**選択対象を除外 (Exclude Selected)**] をクリックします。[**除外 (Exclude)**] をクリックして確定します。



Host Classifier | DNS Servers ⓘ
(last run 1 hours ago)

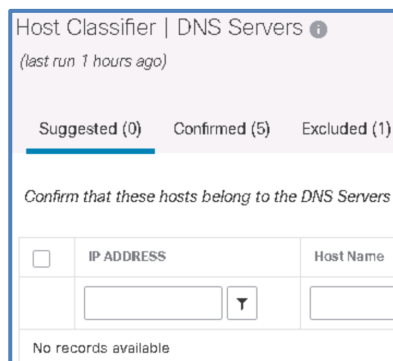
Suggested (1) Confirmed (5) Excluded (0) Enabled Auto Classification

Exclude Selected Confirm Selected

Confirm that these hosts belong to the DNS Servers host group, or exclude them from future suggestions for this search.

<input type="checkbox"/>	IP ADDRESS	Host Name	Host Group(s)	Count ↓	Last Suggested
<input checked="" type="checkbox"/>	209.182.184.2	spyglass.lancope.com	Catch All	26	1/26/2020

- f. [**推奨 (Suggested)**] が (0) となり、推奨 DNS サーバの IP アドレスが表示されなくなりました。



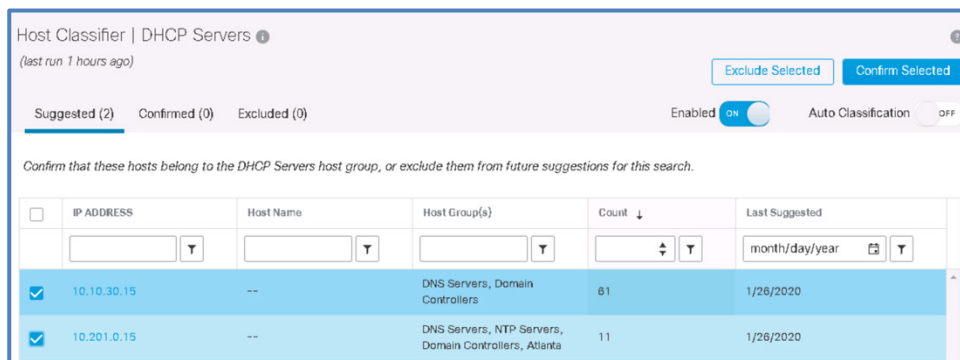
Host Classifier | DNS Servers ⓘ
(last run 1 hours ago)

Suggested (0) Confirmed (5) Excluded (1)

Confirm that these hosts belong to the DNS Servers

<input type="checkbox"/>	IP ADDRESS	Host Name
No records available		

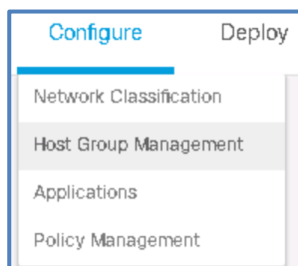
5. このお客様環境では、DHCP サーバの分類はまだ行っていません。ページの左側にある [**DHCP サーバ (DHCP Servers)**] をクリックします。
- a. このリストの上位 2 つの IP アドレスが DHCP サーバであることを確認しました。両方の **チェックボックス** をクリックし、[**選択対象の確認 (Confirm Selected)**] をクリックします。



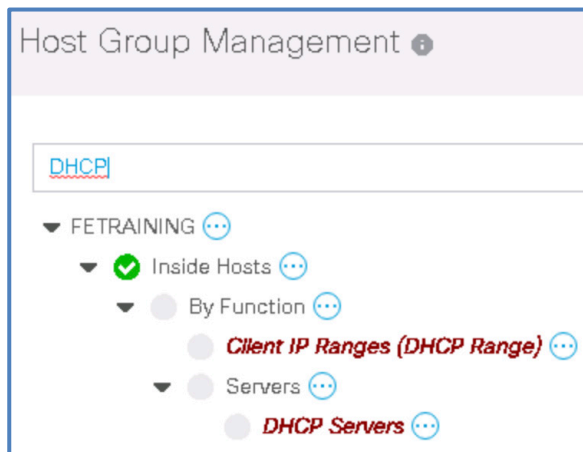
b. [確認 (Confirm)] をクリックします。

6. DHCP サーバの分類が想定どおりに機能しているかを検証しましょう。

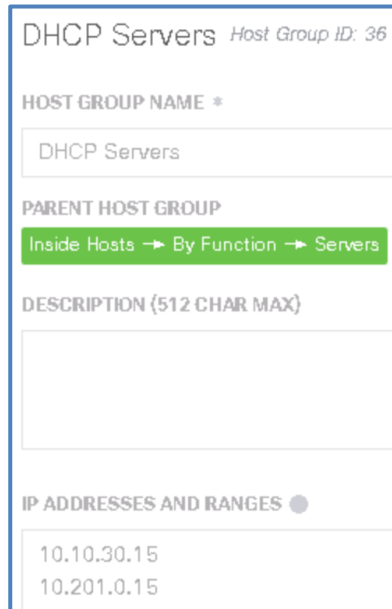
a. [設定 (Configure)] > [ホストグループ管理 (Host Group Management)] の順に選択します。



b. 検索フィールドに **DHCP** と入力し、**Enter** を押します。



c. [DHCP サーバ (DHCP Servers)] をクリックします。

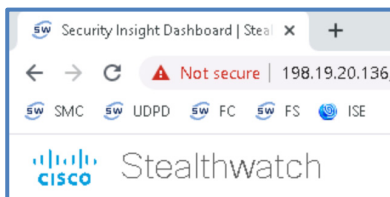


7. 成功しました。2 つの DHCP サーバの IP アドレスが、想定したとおり正しいホストグループに配置されています。

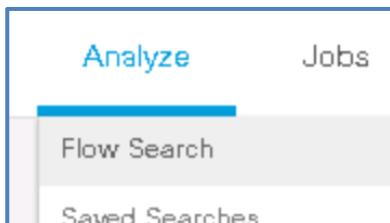
追加のサーバタイプの特定

Web インターフェイス内から、ネットワーク上でさまざまなサーバとして動作しているように見えるシステムを特定することもできます。簡単な検索手順を実行して、別のサービスタイプ (Web サービス (HTTP)) についてこのプロセスを説明します。

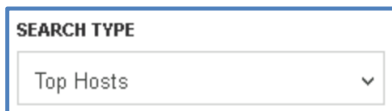
1. **Chrome** を使用して、**SMC Web クライアント** に **admin** ユーザとしてパスワード **C1sco12345** でログインしていることを確認します。



2. Web インターフェイスで [分析 (Analyze)] を選択し、[フロー検索 (Flow Search)] を選択します。



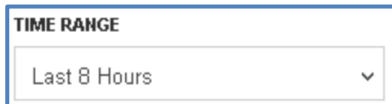
3. 検索タイプを [上位ホスト (Top Hosts)] に設定します。



SEARCH TYPE

Top Hosts

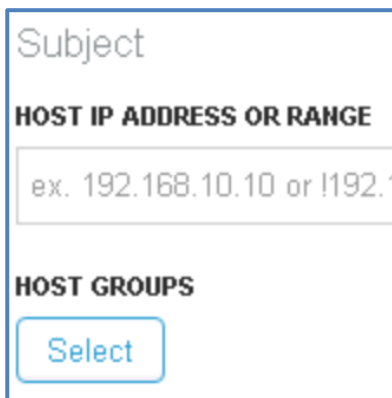
4. [時間範囲 (Time Range)] を [過去 8 時間 (Last 8 Hours)] に設定します。



TIME RANGE

Last 8 Hours

5. [サブジェクト (Subject)] の [ホストグループ (Host Groups)] の [選択 (Select)] ボタンをクリックします。



Subject

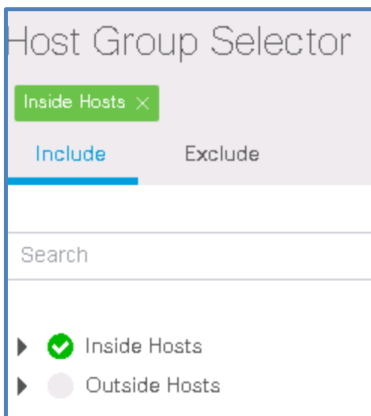
HOST IP ADDRESS OR RANGE

ex. 192.168.10.10 or !192.168.10.10

HOST GROUPS

Select

- a. [含む (Include)] : [内部ホスト (Inside Hosts)] を選択します。



Host Group Selector

Inside Hosts ×

Include Exclude

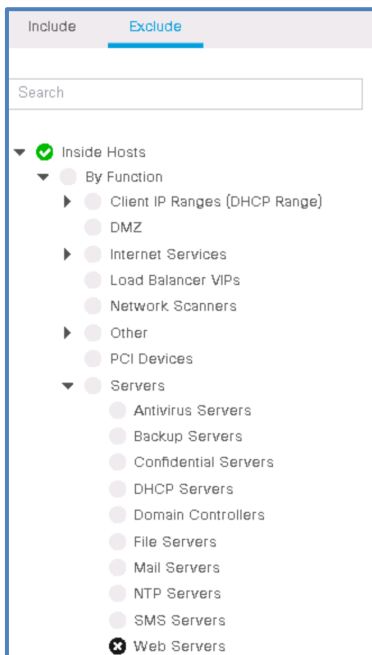
Search

▶ Inside Hosts

▶ Outside Hosts

- b. [除外 (Exclude)] : [Web サーバ (Web Servers)] を選択します。

- i. ヒント : ツリーの上部にある [除外 (Exclude)] をクリックして展開し、その中から選択します。

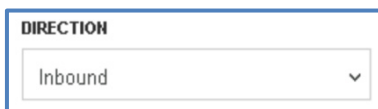


c. [適用 (Apply)] をクリックします。

6. [サブジェクト (Subject)] セクションは次のようになります。

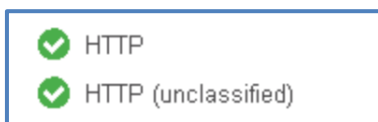


7. [接続 (Connection)] > [方向 (Direction)] で [着信 (Inbound)] を選択します。



8. [接続 (Connection)] > [アプリケーション (Applications)] で [選択 (Select)] ボタンをクリックします。

a. [HTTP] および [HTTP (未分類) (HTTP (unclassified))] を選択します。



b. [適用 (Apply)] をクリックします。

9. [ピア (Peer)] の [ホストグループ (Host Groups)] で [選択 (Select)] ボタンをクリックします。

a. [含む (Include)] : [内部ホスト (Inside Hosts)]

b. [除外 (Exclude)] : 何も選択しない

Host Group Selector

Inside Hosts ×

Include Exclude

Search

▶ Inside Hosts

▶ Outside Hosts

c. [適用 (Apply)] をクリックします。

10. 最終的なフィルタは次のようになります。右上隅の [検索 (Search)] をクリックします。

Top Hosts Search

Last 8 Hours (Time Range) Restore Defaults Load Saved Search Save Search

Subject: Inside Hosts (Host Groups) Web Servers (Host Groups) Other (Orientation)

Connection: HTTP (Applications) HTTP (unclassified) (Applications) Inbound (Direction)

Peer: Inside Hosts (Host Groups)

SEARCH TYPE: Top Hosts TIME RANGE: Last 8 Hours SEARCH NAME: Top Hosts on 10/21/2018 at 11:47 AM

Subject: HOST IP ADDRESS: ex. 192.168.10.10 or 192.168.10.10 HOST GROUPS: Inside Hosts Web Servers

Connection: PORT / PROTOCOL: ex. 80/tcp or 80/tcp APPLICATIONS: HTTP HTTP (unclassified) DIRECTION: Inbound

Peer: HOST IP ADDRESS: ex. 192.168.10.10 or 192.168.10.10 HOST GROUPS: Inside Hosts

11. 処理が終わると（結果が表示されるまで数秒かかる場合があります）、次のようなレポートが表示されます（時刻によって見え方は異なります）。

Top Hosts Search Results (51)

Edit Search Last 8 Hours (Time Range) Save Search Save Results Start New Search 100% Complete Delete Search

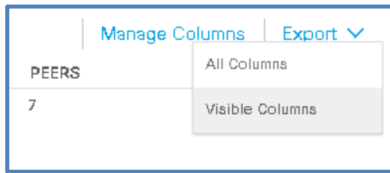
Subject: Inside Hosts (Host Groups) Web Servers (Host Groups) Other (Orientation)

Connection: HTTP (Applications) HTTP (unclassified) (Applications) Inbound (Direction)

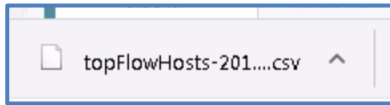
Peer: Inside Hosts (Host Groups)

% OF BYTES	HOST IP ADDRESS	HOST NAME	HOST GROUPS	HOST ROLE	BYTES	PACKETS	FLAWS	PEERS	HOST BYTES RA...
86.41%	10.202.1.151	--	Catch All	Server	12.03 G	26.6 M	41	7	88.03%
8.2%	10.201.3.184	workstation-184	Atlanta, PCI Devices	Client and Server	4.02 G	6.98 M	141	10	1.16%
5.1%	10.201.3.146	workstation-146	Atlanta, PCI Devices	Client and Server	3.03 G	12.12 M	832	11	1.26%

12. 一致する Web サーバのリストをお客様に提供するには、表の右上の [エクスポート (Export)] をクリックしてから [表示可能な列 (Visible Columns)] を選択してデータをエクスポートします。



- CSV 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（またはダウンロードフォルダ）から確認できます。



- これで、お客様のネットワーク内で HTTP 接続を提供するシステムが特定されました。ここでは、これらのホストの分類は行いません。Web インターフェイスでホストを分類する場合は、[設定 (Configure)] > [ホストグループ管理 (Host Group Management)] に進んでください。次の演習に進みましょう。

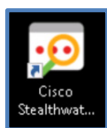
追加のサーバタイプの分類：デスクトップクライアント

デスクトップクライアントのインターフェイスには、Web インターフェイスでまだ利用できないドキュメントがいくつかあります。次の手順では、デスクトップクライアントを使用して分類タスクを実行する方法について説明します。

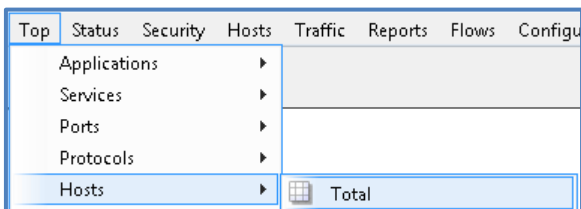
Stealthwatch において機能別に分類されるホストの数が増えるほど、お客様にとってのソリューションの価値は高まります。セキュリティインシデントを調査する際、あるいは潜在的なネットワークパフォーマンスの問題のトラブルシューティングを試みる際、トラフィックの送信元もしくは宛先の IP アドレスが特定のサーバタイプである、またはそれらがお客様のネットワーク内の特定のアプリケーションに関わっているなど、追加のコンテキストがあると非常に便利な場合があります。

お客様からは、サーバの機能的役割について、非常に基本的な IP データが提供されています。しかし、分類されるべきホストがそれ以外にもネットワーク上に存在し、それらをお客様が認識していない可能性もあります。Stealthwatch を利用すると、そのようなホストの有無を判断することができます。では、未分類の DNS、NTP、Active Directory サーバを探してみましょう。

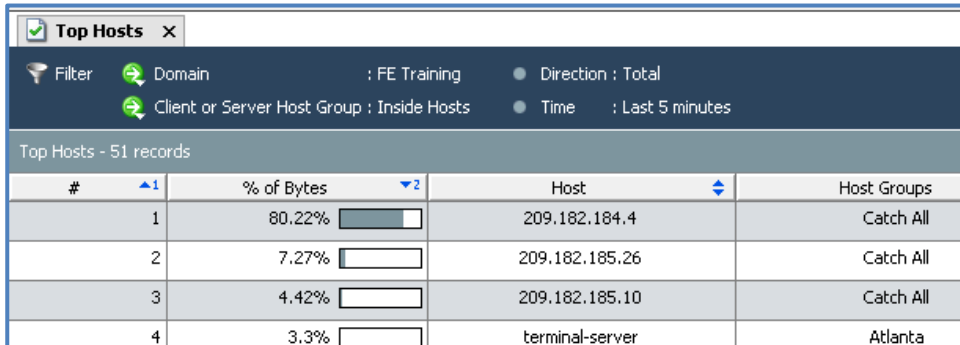
- SMC デスクトップクライアント** に、**admin** ユーザとしてパスワード **C1sco12345** でログインしていることを確認します。



- [エンタープライズ (Enterprise)] ツリー内の [内部ホスト (Inside Hosts)] ホストグループをクリックして**強調表示**させます。
- [上位 (Top)] メニューをクリックし、[ホスト (Hosts)] サブメニューを選択し、[合計 (Total)] メニュー項目を選択します。

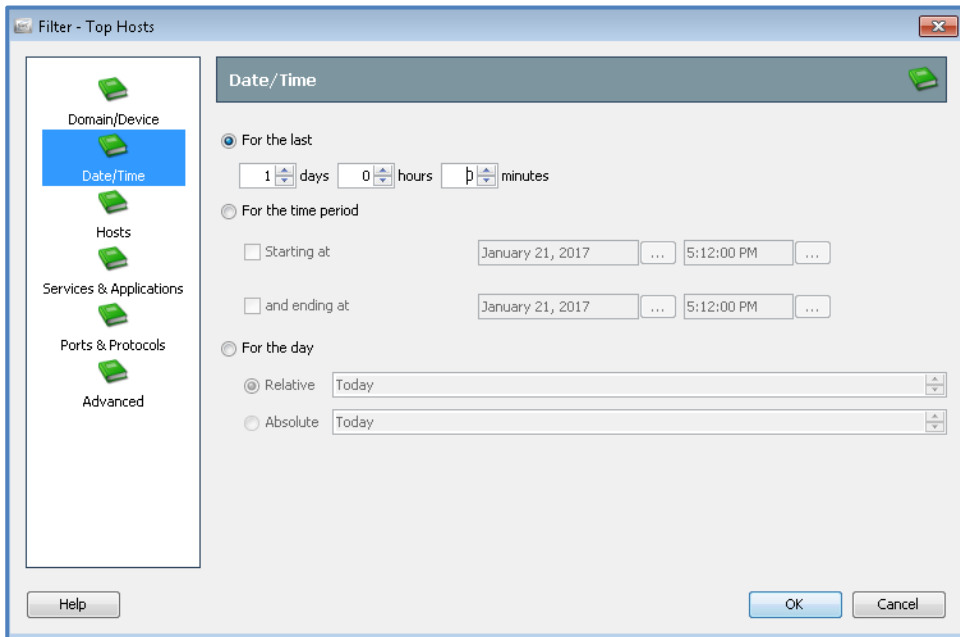


4. お客様のネットワーク内のホストのうち直近 5 分間で最も多くのデータ量を送信したものを示す [上位ホスト (Top Hosts)] ドキュメントが表示されます。ただし、フィルタ変更をいくつか行って、ドキュメントに表示されるデータを調整する必要があります。ドキュメントの左上にある [フィルタ (Filter)] アイコンをクリックします。



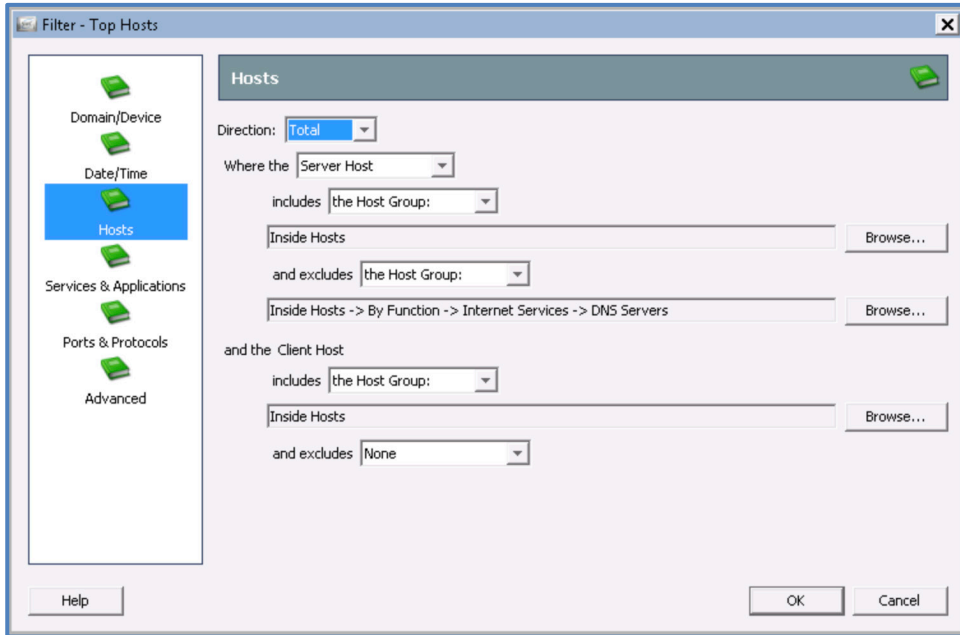
#	% of Bytes	Host	Host Groups
1	80.22%	209.182.184.4	Catch All
2	7.27%	209.182.185.26	Catch All
3	4.42%	209.182.185.10	Catch All
4	3.3%	terminal-server	Atlanta

5. 左ペインの [日時 (Date/Time)] メニューを選択し、タイムフレームの値を [直近 (For the last)] の [1 日 (1 days)] に調整します。



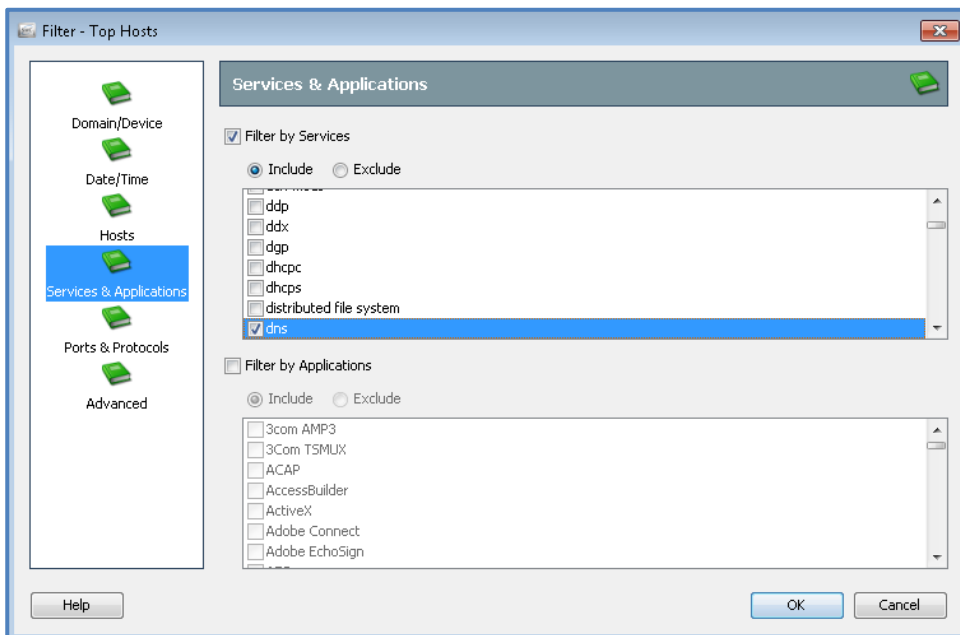
6. 左ペインの [ホスト (Hosts)] メニューを選択し、フィルタを以下のように設定します。
- [方向 (Direction)] : [合計 (Total)]
 - [対象 (Where the)] : [サーバホスト (Server Host)]
 - [含まれるもの (Includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]
 - [除外されるもの (And excludes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)] > [機能別 (By Function)] > [インターネットサービス (Internet Services)] > [DNS サーバ (DNS Servers)]
 - [クライアントホストに含まれるもの (And the Client Host includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]

f. [除外されるもの (And excludes)] : [なし (None)]



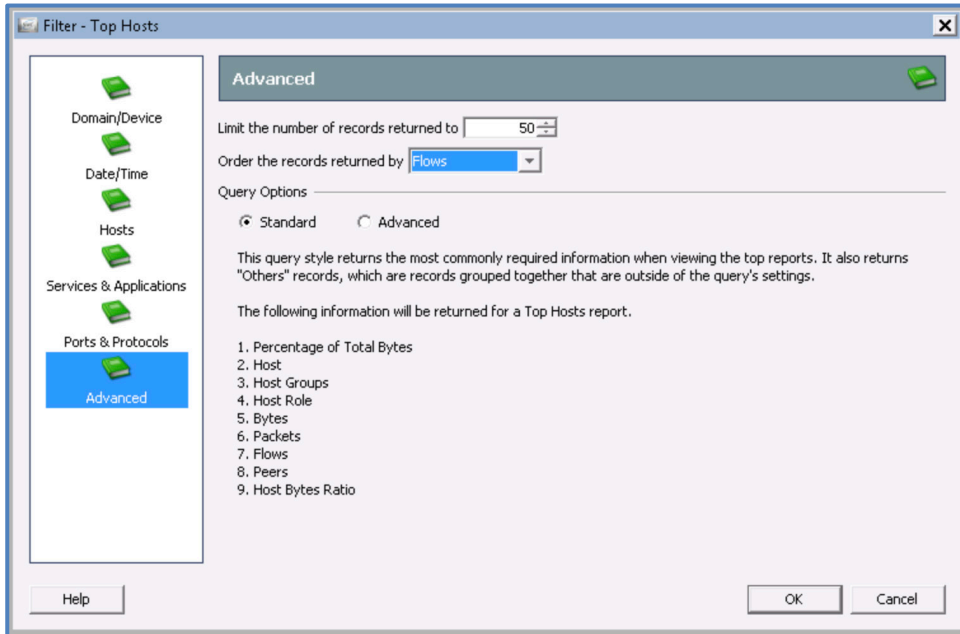
注：このフィルタでは、すでに DNS サーバとして分類済みのホストについての結果は表示されません。ここで特定したい検索対象は、（クライアントではなく）DNS サーバとして機能するホストであって、なおかつ DNS サーバホストグループの既存メニューではないものです。フィルタをこのように設定することで、分類済みの DNS サーバは確実に検索結果から除外されます。[サービスとアプリケーション (Services and Applications)] フィルタ設定で適切なエントリを作成しないと、このフィルタで、DNS サーバに限らずすべてのタイプのサーバが表示されます。さらにフィルタ設定を行う必要があります。

7. 左側の [サービスとアプリケーション (Services & Applications)]メニューを選択し、[サービスでフィルタ (Filter by Service)]チェックマークボックスをオンにし、[dns] サービスエントリのチェックマークをオンにします。サービスオプションが [含まれるもの (Include)]に設定されていることを確認してください。



注：フィルタをこのように設定することで、返される結果が、DNS を含むネットワークトラフィックのみに確実に限定されるようになります。

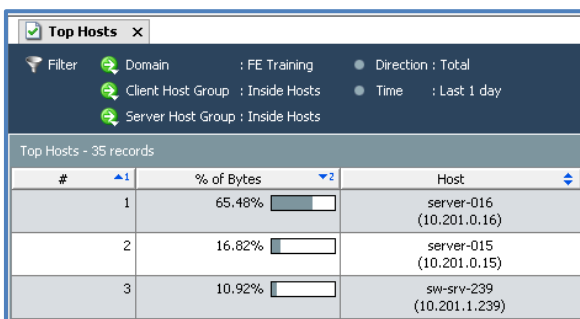
8. 左ペインの [詳細設定 (Advanced)] メニューを選択します。[返されるレコードの並び基準 (Order the records returned by)] 設定を [フロー (Flows)] に変更します。



9. フィルタの変更が終わったら [OK] ボタンをクリックします。

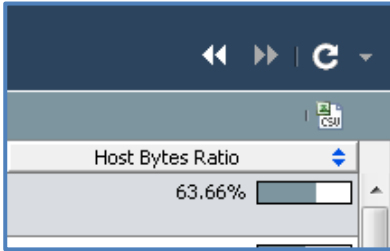
注：一般に、DNS トラフィックでは、生成される転送バイト数は多くありません。環境内で最も利用度の高い DNS サーバであるホストを探すときには、結果をバイトではなくフローに基づいて並べると便利な場合があります。

10. [上位ホスト (Top Hosts)] ドキュメントの実行が完了すると、過去 1 日間に DNS サーバとして機能し、まだエンタープライズツリー内で DNS サーバとして分類されていないすべてのホストが一覧表示されます。

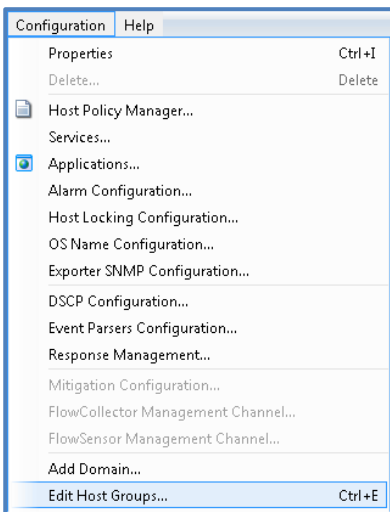


#	% of Bytes	Host
1	65.48%	server-016 (10.201.0.16)
2	16.82%	server-015 (10.201.0.15)
3	10.92%	sw-srv-239 (10.201.1.239)

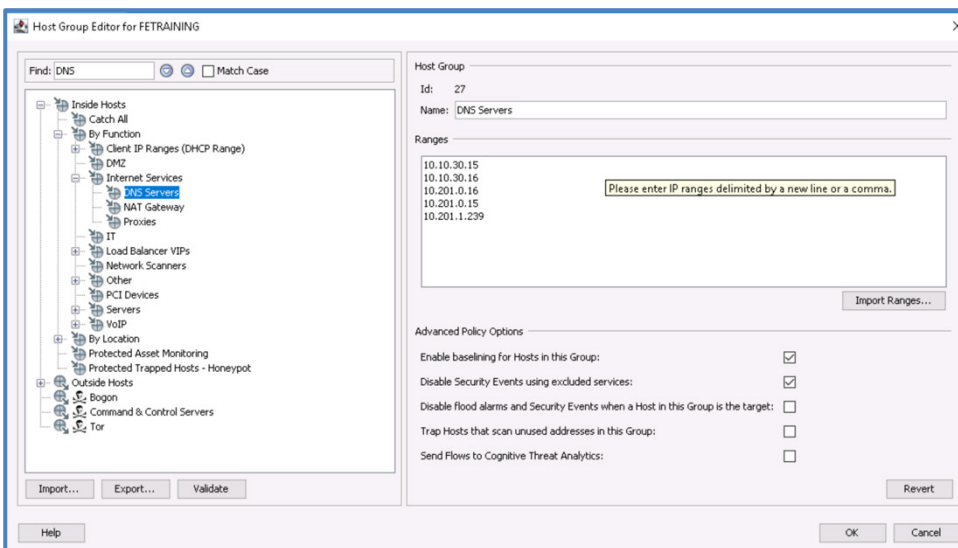
11. 返されたホストの数は、お客様から提供されている DNS サーバの数よりもかなり多くなっています。ここで、Stealthwatch から得られたデータを確認のためお客様に提供して、これらのホストの中に、お客様の環境内で実際に認可されている DNS サーバがあるかどうか判断してもらいます。
12. [上位ホスト (Top Hosts)] ドキュメントを CSV ファイルにエクスポートします。ドキュメントウィンドウの右上にある [CSV] アイコンをクリックし、プロンプトが表示されたら [保存 (Save)] をクリックして CSV ファイルをディスクに保存します。



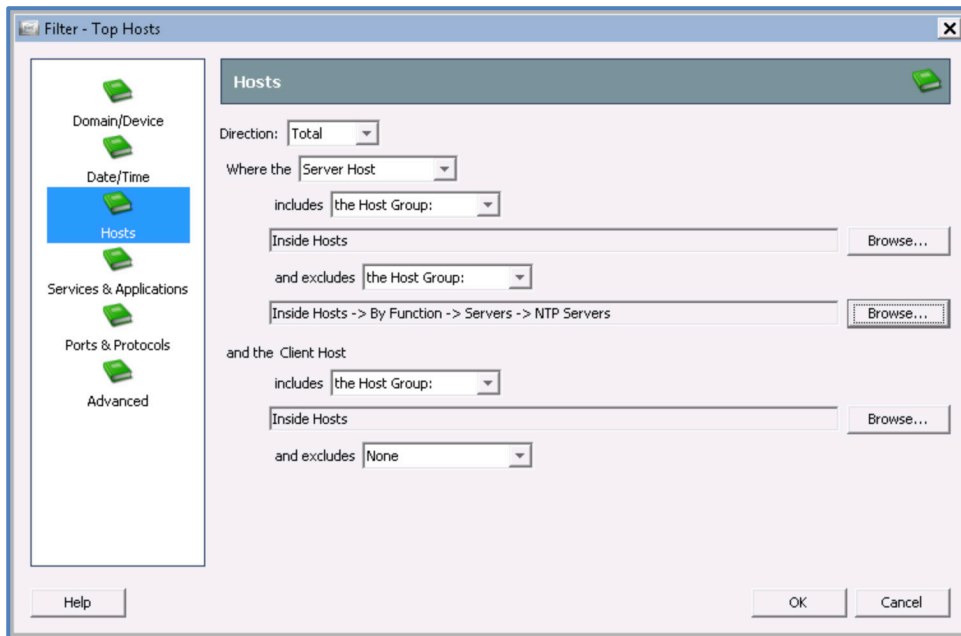
13. お客様が DNS サーバのリストを確認したところ、ドキュメント中の上位 3 つのエントリは、認識から漏れていた認可済み DNS サーバとのことでした。では、これらのホストを DNS サーバホストグループに追加します。
14. [ホストグループエディタ (Host Group Editor)] を開きます。[設定 (Configuration)] メニューをクリックし、[ホストグループの編集 (Edit Host Groups)] メニュー項目を選択します。



15. [DNS サーバ (DNS Servers)] ホストグループに移動して (必要に応じて [検索 (Find)] を使用) 、お客様が承認した [上位ホスト (Top Hosts)] ドキュメントの上位 3 エントリの IP アドレスを追加します。[OK]、[続行 (Continue)] の順にクリックして変更を保存します。

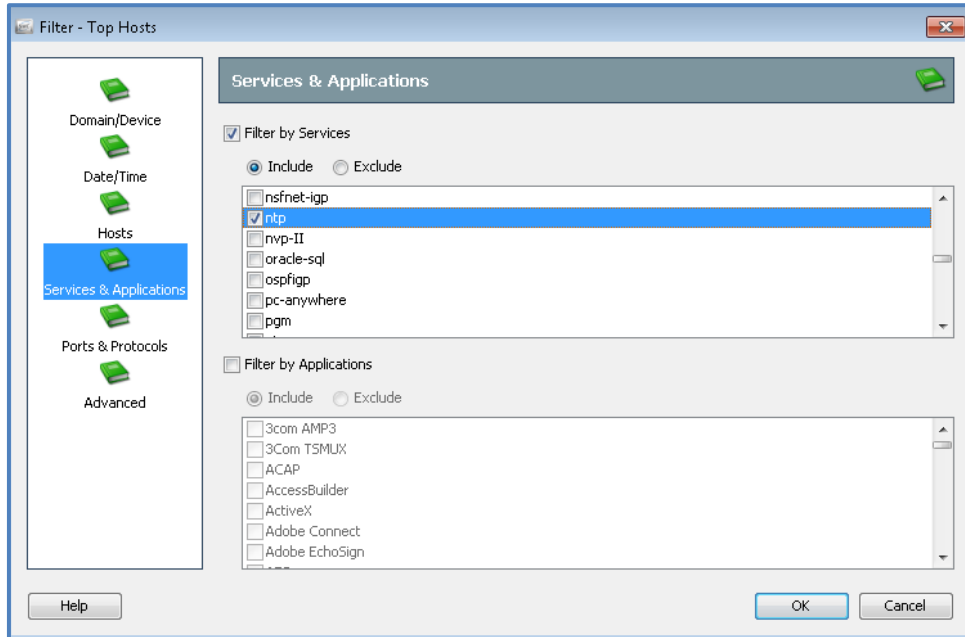


16. 次に、[上位ホスト (Top Hosts)]ドキュメントのフィルタ設定を変更して、未分類の NTP サーバを検索します。左上にある漏斗のアイコンの [フィルタ (Filter)] ボタンをクリックします。
17. [ホスト (Hosts)] メニューを選択します。
 - a. [方向 (Direction)] : [合計 (Total)]
 - b. [対象 (Where the)] : [サーバホスト (Server Host)]
 - c. [含まれるもの (Includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]
 - d. [除外されるもの (And excludes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)] > [機能別 (By Function)] > [サーバ (Servers)] > [NTP サーバ (NTP Servers)]
 - e. [クライアントホストに含まれるもの (And the Client Host includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]
 - f. [除外されるもの (And excludes)] : [なし (None)]



注：フィルタをこのように設定することで、NTP サーバホストグループにすでに定義済みのホストは、除外されます。

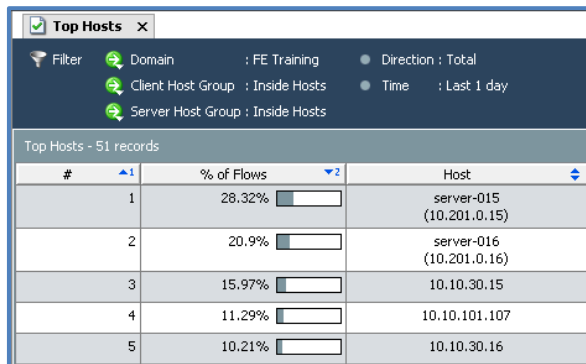
18. [サービスとアプリケーション (Services & Applications)] メニューを選択します。[dns] サービスのチェックボックスをオフにし、[ntp] サービスのチェックマークをオンにします。



19. フィルタの変更が終わったら [OK] ボタンをクリックします。

注： NTP トラフィックでは、生成される転送バイト数は多くありません。環境内で最も利用度の高い NTP サーバであるホストを探すときには、結果をバイトではなくフローに基づいて並べると便利な場合があります。

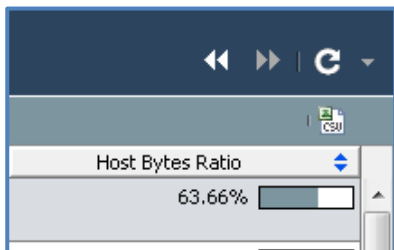
20. [上位ホスト (Top Hosts)] ドキュメントの実行が完了すると、過去 1 日の間に NTP サーバとして機能したすべてのホストの一覧が表示されます。



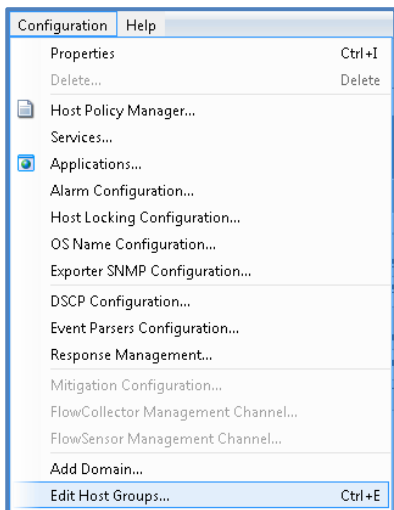
#	% of Flows	Host
1	28.32%	server-015 (10.201.0.15)
2	20.9%	server-016 (10.201.0.16)
3	15.97%	10.10.30.15
4	11.29%	10.10.101.107
5	10.21%	10.10.30.16

21. 返されたホストの数は、お客様から提供されている NTP サーバの数よりもかなり多くなっています。ここで、Stealthwatch から得られたデータを確認のためお客様に提供して、これらのホストの中に、お客様の環境内で実際に承認されている NTP サーバがあるかどうか判断してもらいます。

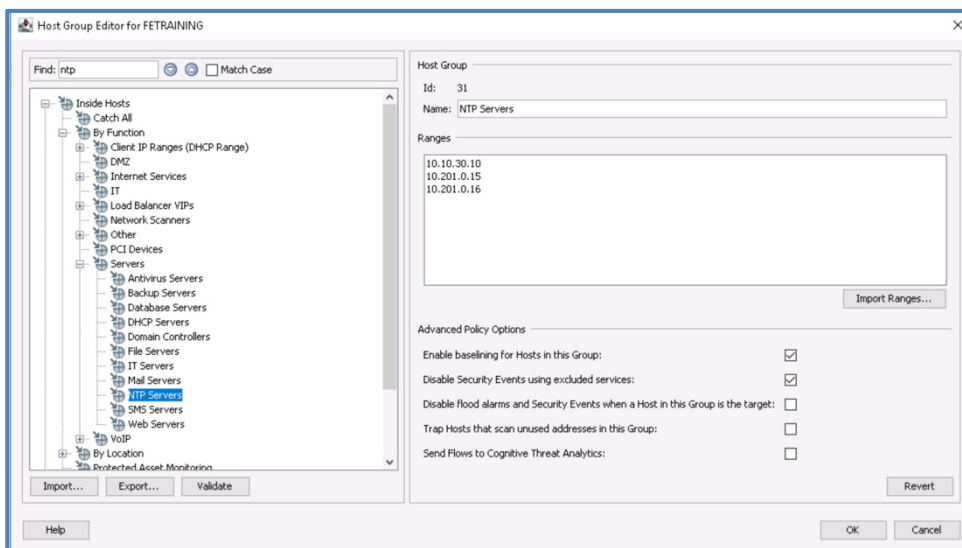
22. [上位ホスト (Top Hosts)] ドキュメントを CSV ファイルにエクスポートします。ドキュメントウィンドウの右上にある [CSV] アイコンをクリックし、プロンプトが表示されたら [保存 (Save)] をクリックして **CSV** ファイルをディスクに保存します。



- 検出された NTP サーバのリストをお客様が確認したところ、ドキュメントの上位 2 つのエントリが、認識から漏れていた承認済み NTP サーバとのことでした。では、これらのホストを NTP サーバホストグループに追加します。
- [ホストグループエディタ (Host Group Editor)]を開きます。[設定 (Configuration)]メニューをクリックし、[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。



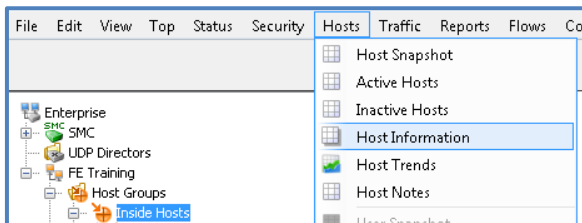
- [NTP サーバ (NTP Servers)]ホストグループに移動して、お客様が承認した [上位ホスト (Top Hosts)]ドキュメントの上位 2 エントリの IP アドレスを追加します。[OK]、[続行 (Continue)]の順にクリックして変更を保存します。



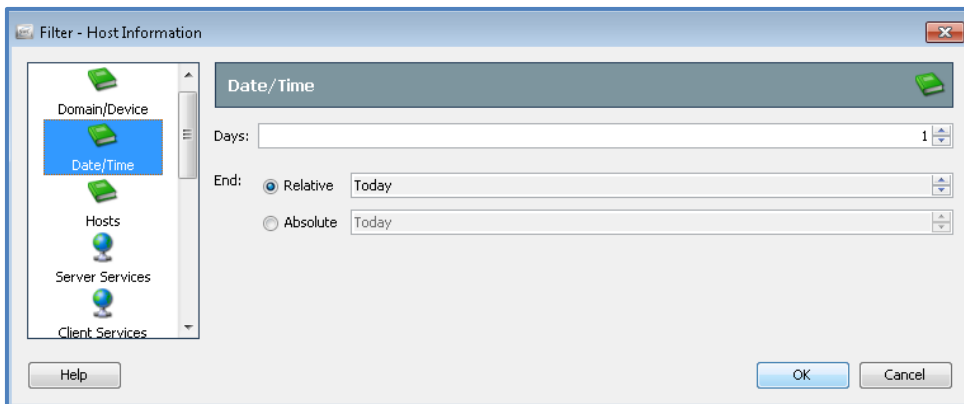
ホスト情報ドキュメント：デスクトップクライアント

特定のタイプのサーバとして機能するホストを割り出す方法としては、これ以外にも、デスクトップクライアント インターフェイス内の [ホスト情報 (Host Information)] ドキュメントを使用する方法があります。今回は、この方法を使用して Active Directory サーバを特定します。

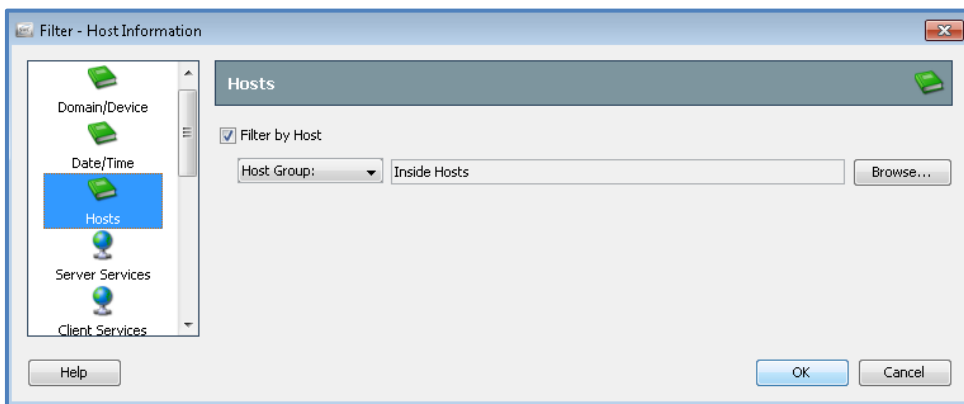
1. デスクトップクライアントに戻ります。
2. [エンタープライズ (Enterprise)] ツリー内の [内部ホスト (Inside Hosts)] ホストグループを選択し、上部のナビゲーションバーから [ホスト (Hosts)] メニューをクリックし、[ホスト情報 (Host Information)] メニュー項目を選択します。



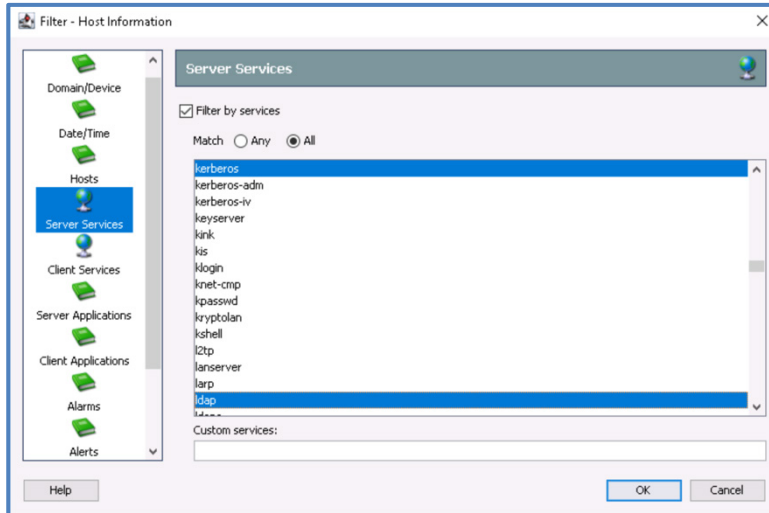
3. [ホスト情報 (Host Information)] ドキュメントのフィルタ設定が表示されます。左ペインの [日時 (Date/Time)] メニューを選択します。[日時 (Date/Time)] 設定が [1 日 (1 days)] になっていることを確認します。



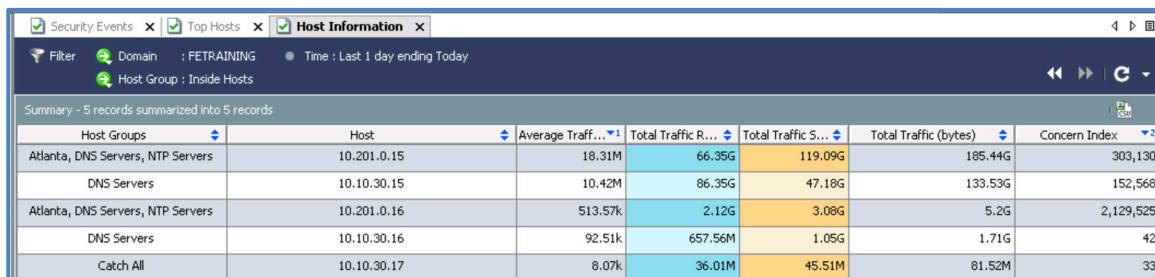
4. 左ペインの [ホスト (Hosts)] メニューを選択します。[ホストでフィルタ (Filter by Host)] が選択されていることと、[ホストグループ (Host Group)] 設定が [内部ホスト (Inside Hosts)] になっていることを確認します。



5. 左ペインの [サーバサービス (Server Services)] メニューを選択します。[サービスでフィルタ (Filter by services)] チェックボックスをオンにします。[一致 (Match)] のオプションとして [すべて (All)] を選択します。リストから [kerberos] と [ldap] の両サービスを選択します (複数のオプションを選択するにはキーボードの Ctrl キーを使用します) 。すべてのフィルタ設定変更が済んだら、[OK] をクリックします。

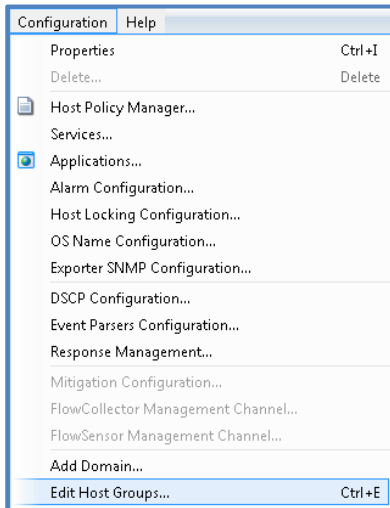


6. [ホスト情報 (Host Information)] ドキュメントが表示されます。すでに分類済みのホストが結果から除外されてはいますが、このドキュメントでは、選択されたすべてのサービスとの一致を要件とすることができます (たとえば、Kerberos または LDAP ポートのいずれかでトラフィックを受け入れるホストの中には Active Directory サーバでないものも多数あり得る一方で、Kerberos と LDAP の両方でサーバとしてトラフィックを受け入れるホストの場合は Active Directory サーバである可能性が高くなります) 。

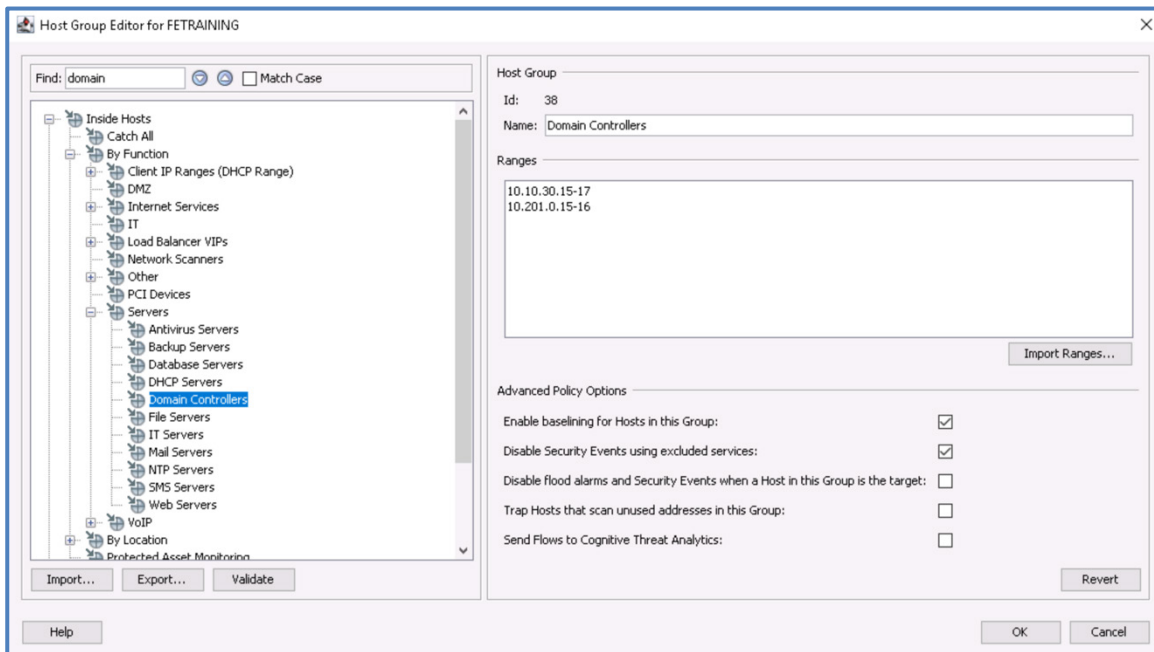


Host Groups	Host	Average Traff...	Total Traffic R...	Total Traffic S...	Total Traffic (bytes)	Concern Index
Atlanta, DNS Servers, NTP Servers	10.201.0.15	18.31M	66.35G	119.09G	185.44G	303,130
DNS Servers	10.10.30.15	10.42M	86.35G	47.18G	133.53G	152,568
Atlanta, DNS Servers, NTP Servers	10.201.0.16	513.57k	2.12G	3.08G	5.2G	2,129,525
DNS Servers	10.10.30.16	92.51k	657.56M	1.05G	1.71G	42
Catch All	10.10.30.17	8.07k	36.01M	45.51M	81.52M	33

7. 検出されたサーバのうち、Active Directory ドメインコントローラの可能性が高いと思われるサーバのリストをお客様が確認したところ、見つかったすべてのエントリを Stealthwatch のドメイン コントローラ ホスト グループに追加することが承認されました。
8. [設定 (Configuration)] メニューをクリックして [ホストグループの編集 (Edit Host Groups)] メニュー項目を選択し、[ホストグループエディタ (Host Group Editor)] を開きます (または CTRL+E を押します) 。



9. [ドメインコントローラ (Domain Controllers)] ホストグループに移動して、お客様が承認した [ホスト情報 (Host Information)] ドキュメントの **IP アドレス** を追加します。
 - a. レポートの 5 つのサーバ IP がすべて含まれるように、次の両方の行を追加します。
 - i. 10.10.30.15-17
 - ii. 10.201.0.15-16
 - b. [OK] をクリックしてから [続行 (Continue)] をクリックして変更を保存します。



10. 特定のタイプのネットワークトラフィックを処理するホストを割り出し、いくつかのサーバタイプを分類する作業が無事に完了しました。また、検出されたデータを反映するためにホストグループの編集 (分類) も実施しました。ラボの次の手順に進みます。

注：Stealthwatch のデフォルトのホストグループを使用して特定のタイプのホスト（ネットワークスキャナ、メールサーバ、ファイルサーバ、バックアップサーバなど）を分類しておく、アラームを減らすのに役立ちます。その他のサーバ機能の役割を分類することでフィールドエンジニアやお客様が得られるメリットとしては、お客様のネットワーク上の未承認アクティビティを識別でき、それらのホストが生成したトラフィックについてのレポートが得られるということがあります。

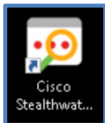
たとえば、認可済みの NTP サーバすべてが NTP サーバホストグループに定義されている場合、Stealthwatch でドキュメントを実行して、NTP サーバホストグループを利用していない NTP トラフィックを探ることができます。これにより、サーバとして適切でないタイプのサービスを実行しているホストと、誤った設定により本来と異なる NTP サーバを使用しているクライアントの双方を割り出すことができます。これは、設定の標準化や WAN 帯域幅の潜在的削減に役立つとともに、不適切な時刻源の参照によりタイムクロックが誤っている可能性のあるホストを識別するうえでも役に立ちます。NTP はあくまでも 1 つの例にすぎません。これと同じ方法は、お客様が標準設定の実装を選択し、その設定からの逸脱は最適ではないと考えられる環境であれば、どのサービスまたはアプリケーションにも応用できます。

ネットワークスキャナの分類：デスクトップクライアント

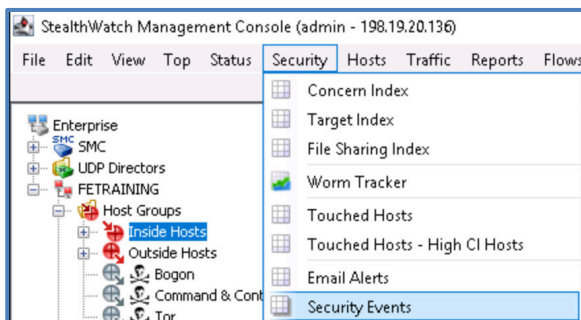
注：Stealthwatch のセキュリティイベントでは、さまざまなタイプの疑わしいまたは悪意のあるネットワーク動作が追跡されます。特定のセキュリティイベントに一致するトラフィックが FC で処理されると、ネットワークトラフィックを生成するホストの Concern Index に Concern Index ポイントが追加されます。Concern Index はデメリットシステムに類似するものです。疑わしい動作が検出されると、その数に応じて CI の値も増えます。

デスクトップクライアントは、ホストが生成したセキュリティイベントに基づいてホストのリストを表示できます。これを使用して、ネットワーク スキャン アクティビティなどの特定のタイプのアクティビティを検索できます。

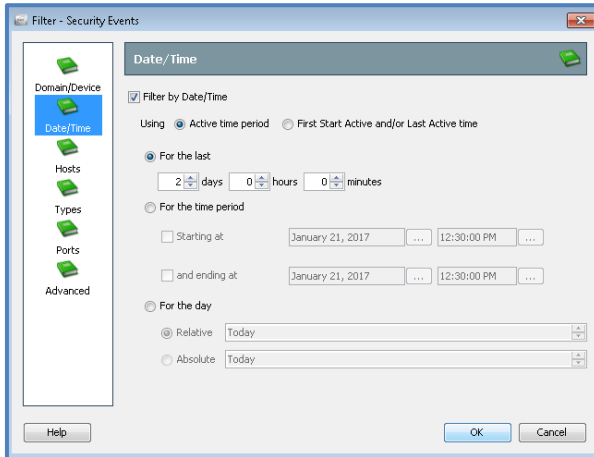
1. **Stealthwatch デスクトップクライアント** を使用して、SMC に **admin** ユーザとしてパスワード **C1sco12345** でログインしていることを確認します。



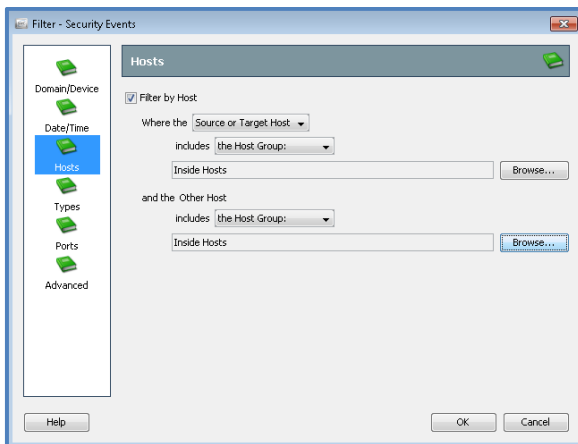
2. [エンタープライズ (Enterprise)] ツリー内の [内部ホスト (Inside Hosts)] ホストグループに移動し、グループを**強調表示**させ、上部のナビゲーションバーから [セキュリティ (Security)] メニューをクリックし、[セキュリティイベント (Security Events)] メニュー項目を選択します。



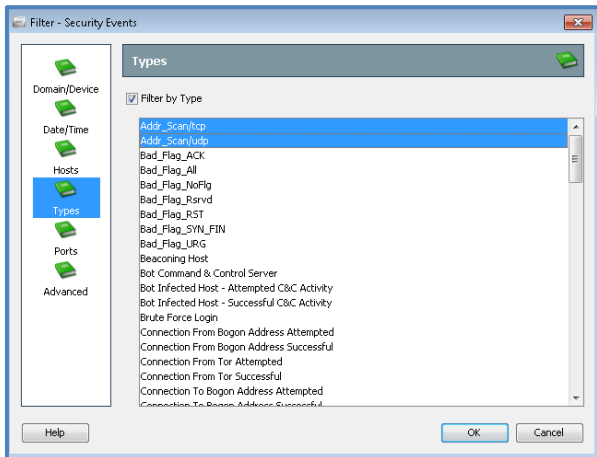
3. [フィルタ - セキュリティイベント (Filter - Security Events)] ウィンドウが表示され、セキュリティ イベント ドキュメントにフィルタ設定を適用するプロンプトが表示されます。左ペインで [日付/時刻 (Date/Time)] メニューを選択し、設定をフィルタ [直近 (For the last)] で [2 日 (2 Days)] に変更します。



4. 左ペインから [ホスト (Hosts)] メニューを選択し、フィルタオプションを次のように設定します。
 - a. [送信元または宛先ホスト (Where the Source or Target Host)]
 - b. [含まれるもの (Includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]
 - c. [およびその他のホスト (And the Other Host)]
 - d. [含まれるもの (Includes)] : [ホストグループ (The Host Group)] > [内部ホスト (Inside Hosts)]

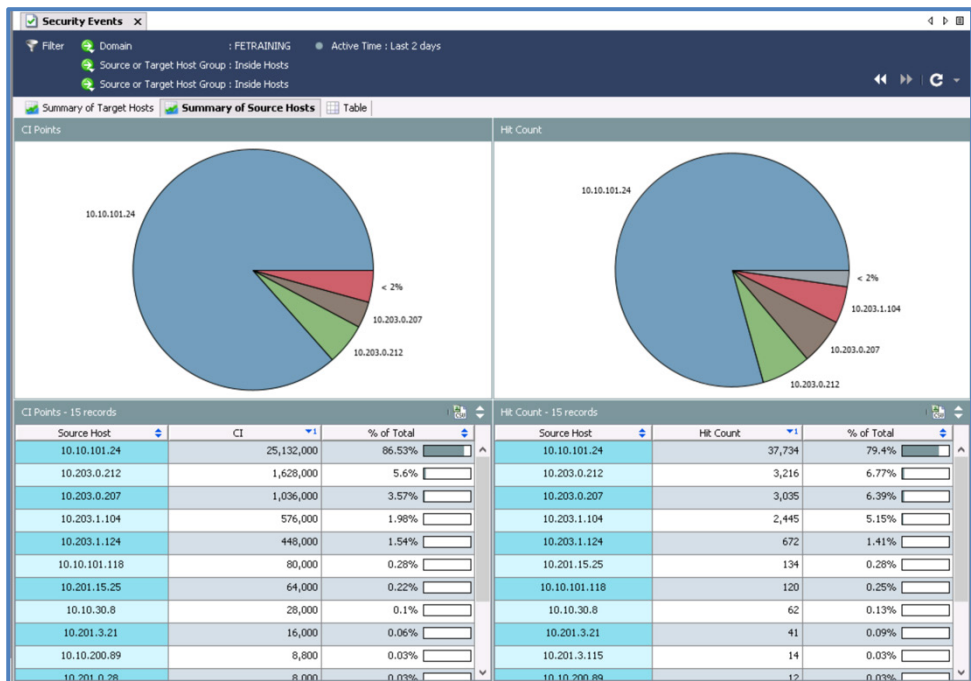


5. 左ペインから [タイプ (Types)] メニューを選択し、[タイプでフィルタ (Filter by Type)] チェックボックスをオンにし、リストから [Addr_Scan/tcp] および [Addr_Scan/udp] セキュリティイベントを両方選択します (**Ctrl** キーを押しながら両方を同時に選択)。[OK] をクリックしてドキュメントをロードします。



注：Addr_Scan/tcp および Addr_Scan/udp セキュリティイベントは、特にネットワーク上の多数のホストに対するネットワーク スキャン アクティビティを実行するホストを対象にしています（各セキュリティイベントの詳細については Stealthwatch のオンラインヘルプを参照）。これが探していたタイプのアクティビティであるため、セキュリティ イベント ドキュメントの結果を制限して、リストされている多様なセキュリティイベントのいずれかを実行したすべてのホストではなく、スキャンアクティビティだけが表示されるようにします。

6. セキュリティ イベント ドキュメントのロードが終了したら、[送信元ホストのサマリー (Summary of Source Hosts)] タブをクリックします。比較的高い割合でスキャンアクティビティを処理しているホストがあることがわかります。



7. ドキュメントの [テーブル (Table)] ページを開き、セキュリティイベントの詳細を確認します。



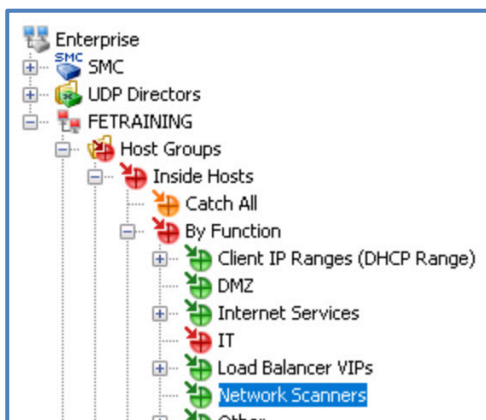
Start Active Time	Source Host Groups	Source Host	Target Host Groups	Target Host	Concern In...	Security Events
25-Jan-2020 00:10:00 (21 hours 50 minutes 17s ago)	Catch All	10.10.101.24	Catch All	209.182.184.0/24	4,400,000	Addr_Scan/tcp-445(6,606)
24-Jan-2020 19:55:59 (1 day 2 hours 4 minutes ago)	Catch All	10.10.101.24	United States	209.182.191.0/24	1,388,000	Addr_Scan/tcp-445(2,082)
24-Jan-2020 19:55:13 (1 day 2 hours 5 minutes ago)	Catch All	10.10.101.24	United States	209.182.187.0/24	1,372,000	Addr_Scan/tcp-445(2,062)
24-Jan-2020 19:55:19 (1 day 2 hours 4 minutes ago)	Catch All	10.10.101.24	United States	209.182.188.0/24	1,372,000	Addr_Scan/tcp-445(2,062)
24-Jan-2020 19:54:27 (1 day 2 hours 5 minutes ago)	Catch All	10.10.101.24	United States	209.182.183.0/24	1,356,000	Addr_Scan/tcp-445(2,036)
24-Jan-2020 19:53:44 (1 day 2 hours 6 minutes ago)	Catch All	10.10.101.24	United States	209.182.179.0/24	1,348,000	Addr_Scan/tcp-445(2,022)
24-Jan-2020 19:53:41 (1 day 2 hours 6 minutes ago)	Catch All	10.10.101.24	United States	209.182.177.0/24	1,344,000	Addr_Scan/tcp-445(2,020)
24-Jan-2020 19:55:47 (1 day 2 hours 4 minutes ago)	Catch All	10.10.101.24	United States	209.182.190.0/24	1,340,000	Addr_Scan/tcp-445(2,016)
24-Jan-2020 19:55:45 (1 day 2 hours 4 minutes ago)	Catch All	10.10.101.24	United States	209.182.189.0/24	1,336,000	Addr_Scan/tcp-445(2,004)
24-Jan-2020 19:55:08 (1 day 2 hours 5 minutes ago)	Catch All	10.10.101.24	Catch All	209.182.185.0/24	1,304,000	Addr_Scan/tcp-445(1,958)
24-Jan-2020 19:54:12 (1 day 2 hours 6 minutes ago)	Catch All	10.10.101.24	United States	209.182.182.0/24	1,288,000	Addr_Scan/tcp-445(1,934)
24-Jan-2020 19:53:44 (1 day 2 hours 6 minutes ago)	Catch All	10.10.101.24	United States	209.182.178.0/24	1,284,000	Addr_Scan/tcp-445(1,926)

注：お客様に「この IP アドレスはどこのもので、なぜネットワークをスキャンしているのか」と尋ねるだけでなく、ホストと動作を特定して、詳細なコンテキストを提供することは有益です。質問するだけではお客様を支援できません。お客様がホストを特定し、アクティビティが無害かどうかを判別するために役立つものとしては、他にトラフィックのターゲットホストやプロトコル/ポート番号などがあります。

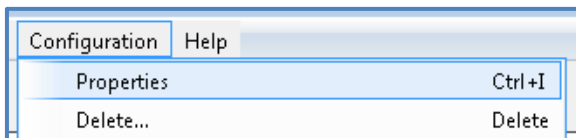
- セキュリティ イベント ドキュメントを通じて取得されたデータに基づいて、多量のスキャンアクティビティを発生させていることが特定されたホストに関する情報をお客様に提供することで、お客様はそのホストがスキャンアクティビティを実行している理由を判定しやすくなります。
- お客様より、このホスト (IP 10.10.101.24) が既知の内部ホストであり、お客様のサーバモニタリングシステムの一部として、Windows サーバマシンのディスク領域をチェックするという有効なアクティビティを実行していることを確認したとの回答がありました。お客様は、このホストのスキャンアクティビティについて、アラームを発生させる必要はありません。デフォルトのネットワーク スキャナ ホスト グループに IP アドレスを追加し、製品に組み込まれたデフォルトの権限ポリシーによってアラームが停止するようにします。

注：このタスクを実行する別の方法としては、特定のサーバタイプについて新しいホストグループを作成し、そのグループ内のホストのアドレススキャンを無効にする権限ポリシーを適用します。

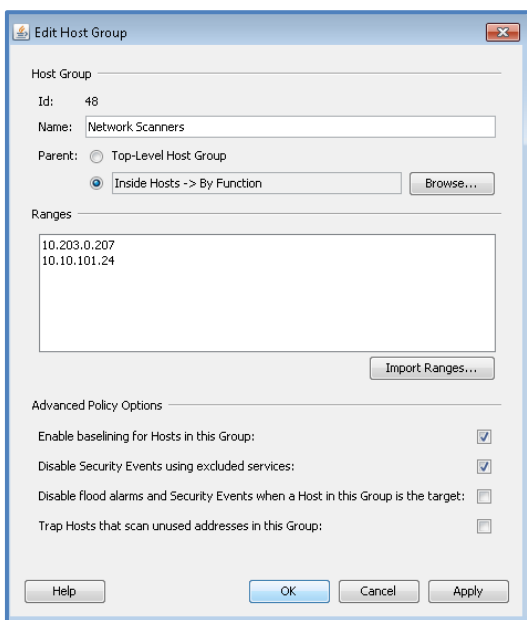
- [エンタープライズ (Enterprise)] ツリーで [ネットワークスキャナ (Network Scanners)] ホストグループに移動し、ホストグループを強調表示します。



11. 上部のナビゲーションバーから [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。



12. [セキュリティイベント (Security Events)] ドキュメントを使用して検出された IP アドレス **10.10.101.24** を、ホストグループのプロパティで [範囲 (Ranges)] フィールドの新しい空白行に入力し、[OK] をクリックして保存し、閉じます (すでにこのホストを前の手順で分類している場合は、ホストグループのプロパティウィンドウを閉じてラボを進めます) 。



13. 既知のネットワークスキャナを分類する作業が無事に完了しました。これにより、不要なアラームの生成が防止され、お客様のネットワークの分類に役立ちます。

注：製品に組み込まれた権限ポリシーにより、ネットワーク スキャナ グループのメンバーである IP アドレスには、そのスキャン動作に起因する Concern Index ポイント が付与されません。

シナリオのまとめ

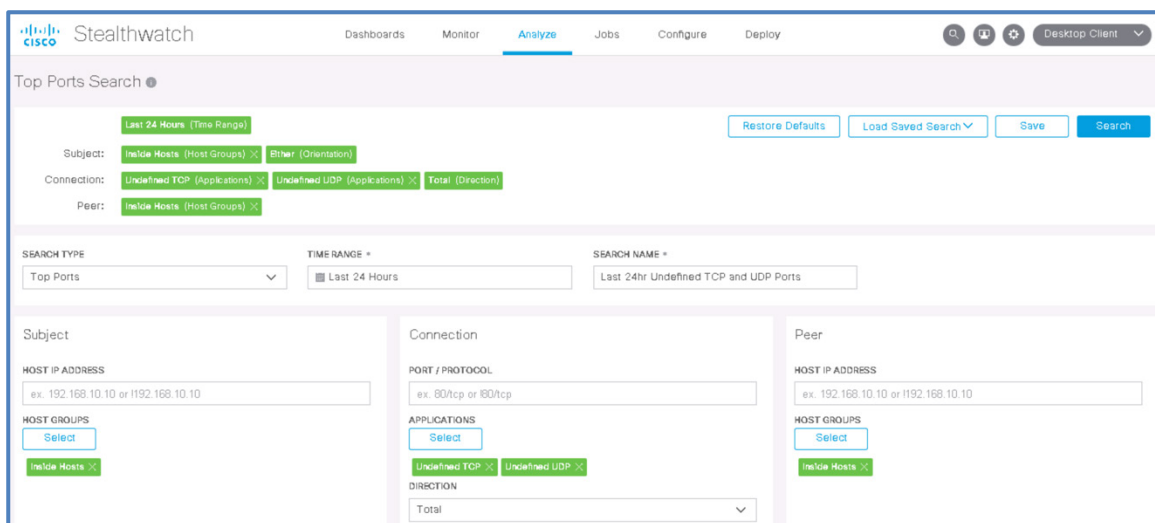
このシナリオでは Stealthwatch を使用して、お客様から事前に提供された IP データセット内のギャップを割り出しました。さまざまなタイプの機能を持つホストを、それが生成または終了するネットワークトラフィックに基づいて識別しました。お客様環境をホストグループに分類することは、Stealthwatch の導入時に必ず完了しておくべき非常に重要なプロセスです。

シナリオ 11. 未定義のサービスとアプリケーションの分類

Stealthwatch では、サービス（レイヤ 4）およびアプリケーション（レイヤ 7）を使用して、異なるタイプのネットワークトラフィックを分類します。サービスおよびアプリケーションがデフォルトで付属している製品は数多くありますが、Stealthwatch には、お客様のネットワーク上のすべてのネットワークトラフィック向けに定義されているサービス/アプリケーションはありません。それでも Stealthwatch でトラフィックを処理してレポートすることは可能です。しかし、未定義のトラフィックはできるだけ少なくする方が、お客様にとってははるかに有意義かつ有用です。これから、お客様の環境における未定義トラフィックの量を確認し、適切なサービスおよびアプリケーションを作成します。Web インターフェイスでアプリケーションを分類する方法と、デスクトップ インターフェイスでサービスを分類する方法を確認します。

注： サービスおよびアプリケーションを分類すると、Stealthwatch がネットワーク カンパセーションにおけるクライアントとサーバの役割を判定するうえでも役に立ちます。

1. SMC Web インターフェイスにログインしていることを確認します。
2. SMC Web インターフェイス内から [分析 (Analyze)] を選択し、[フロー検索 (Flow Search)] を選択します。
3. 次の検索条件を入力します。
 - a. [検索タイプ (Search Type)] : [上位ポート (Top Ports)]
 - b. [検索名 (Search Name)] : [過去 24 時間の未定義の TCP および UDP ポート (Last 24hr Undefined TCP and UDP Ports)]
 - c. [時間範囲 (Time Range)] : [過去 24 時間 (Last 24 Hours)]
 - d. [サブジェクト (Subject)] の [ホストグループ (Host Group)] : [内部ホストを含める (Include Inside Hosts)] を選択
 - e. [ピア (Peer)] の [ホストグループ (Host Group)] : [内部ホストを含める (Include Inside Hosts)] を選択
 - f. [接続 (Connection)] の [アプリケーション (Applications)] : [未定義の TCP (Undefined TCP)] と [未定義の UDP (Undefined UDP)] の両方を選択
 - g. [接続 (Connection)] の [方向 (Direction)] : [合計 (Total)]
 - h. [詳細オプション (Advanced Options)] : [並び基準 (Order By)] = [フロー (Flows)]
4. [検索 (Search)] をクリックします。



5. 24 時間分のラボデータを処理するため、完了までに数分かかる場合があります。しばらくお待ちください。システムでは、過去 24 時間のすべての未定義の TCP および UDP ポートに関連するレポートを作成し、このドキュメントをポートでソートして、バイト数が最大のものから最小のものまで順番に表示します。
 - a. この元のページから、またはジョブ管理を使用して、レポートの進行状況をモニタできます。
6. 最上位の結果はポート 5900/TCP です。SMC のこのトラフィックには、「(vnc)」というテキストによって明らかのように、ポートとプロトコルに一致するサービス定義がありますが、アプリケーション分類はありません。お客様が VNC プロトコルを使用するリモート制御製品を利用していることを確認できたため、そのアプリケーション分類を作成します。

Top Ports Search Results (51)

Edit Search Last 24 Hours (Time Range) Save Search Save Results Start New Search

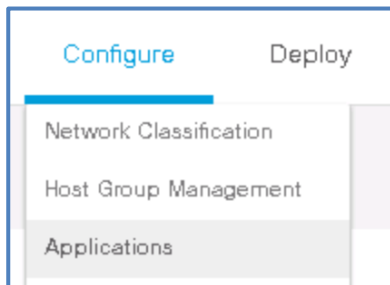
Subject: Inside Hosts (Host Groups) Either (Orientation) 100% Complete Delete Search

Connection: Undefined TCP (Applications) Undefined UDP (Applications) Total (Direction)

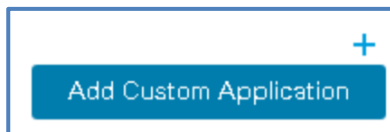
Peer: Inside Hosts (Host Groups)

% OF BYTES	PORT	HOST ROLE	BYTES	PACKETS	FLows	HOSTS	PEERS	HOST BYTES R...
65.18%	5900 / TCP (vnc)	Client and Server	176.7 M	1.21 M	151,341	29,958	29,958	50.00%
1.79%	5355 / UDP (lmmr)	Client and Server	6.69 M	161.28 K	4,162	190	190	50.00%
1.66%	548 / TCP (appleshare)	Client and Server	423 K	66.48 K	3,844	178	178	50.00%
1.54%	49155 / TCP	Client and Server	117.39 M	409.63 K	3,572	247	247	50.00%

7. [設定 (Configure)] > [アプリケーション (Applications)] メニュー項目の順にクリックします。



8. [カスタムアプリケーションの追加 (Add Custom Application)] をクリックします。



9. 次の値を使用して、VNC アプリケーションを設定します。
 - a. [名前 (Name)] : **VNC**
 - b. [説明 (Description)] : [リモート制御トラフィック (Remote control traffic)]
 - c. [ポート/プロトコル (Port/Protocol)] : **5900/TCP**

Custom Application: VNC

NAME: *

VNC

DESCRIPTION (OPTIONAL):

Remote control traffic

ADD RULE

1 Enter at least one criteria to define the custom application below. Criteria within each block is 'AND-ed' together. Subsequent blocks are 'OR-ed' together.

Port/Protocol: ⚙

5900/TCP

Server: ⚙

IP Address

ex. 192.168.10.10

DPI Classification: ⚙

Select an Option...



+ Add to Rules

10. [ルールに追加 (Add to Rules)]をクリックします。

11. アプリケーションルールのエントリが [アプリケーションルール (App Rules)] のリストに追加されます。
[保存 (Save)]をクリックします。


App Rules

Port/Protocol: 5900/TCP

12. [適用 (Apply)]をクリックして、変更内容を適用します。

Applications

 **Unsaved Changes** You have 1 unsaved changes. [Apply](#) [Revert](#)

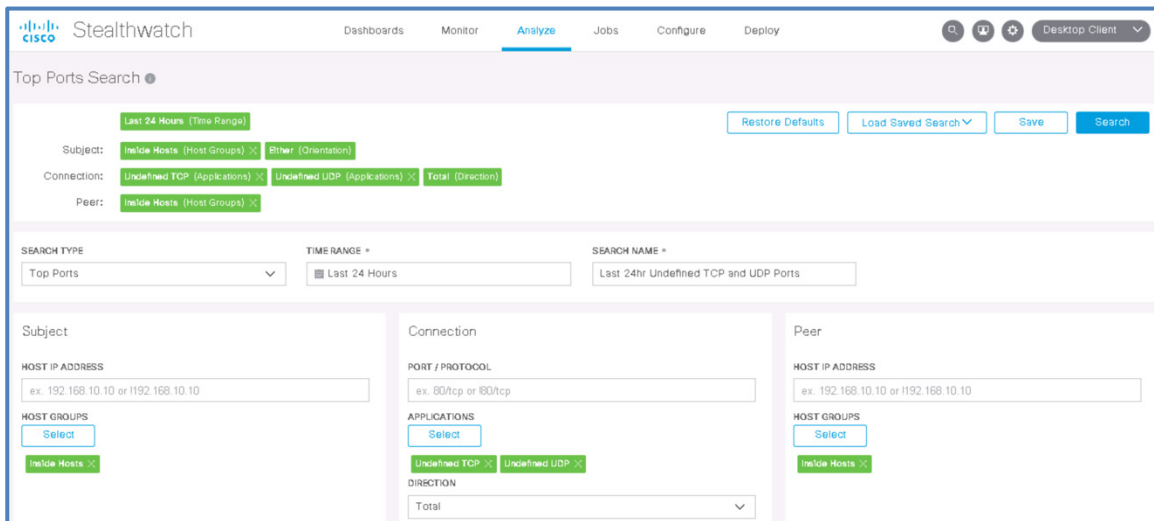
13. アプリケーション分類がリストに表示されます。

Applications

Custom Applications ⓘ

Priority	Application Name	Description
1	VNC	Remote control traffic

14. 次に、アプリケーションとして分類可能なその他のネットワークトラフィックを探します。
15. SMC Web インターフェイス内から [分析 (Analyze)] を選択し、[フロー検索 (Flow Search)] を選択します。
16. 次の検索条件を入力します。
 - a. [検索タイプ (Search Type)] : [上位ポート (Top Ports)]
 - b. [検索名 (Search Name)] : [過去 24 時間の未定義の TCP および UDP ポート (Last 24hr Undefined TCP and UDP Ports)]
 - c. [時間範囲 (Time Range)] : [過去 24 時間 (Last 24 Hours)]
 - d. [サブジェクト (Subject)] の [ホストグループ (Host Group)] : [内部ホストを含める (Include Inside Hosts)] を選択
 - e. [ピア (Peer)] の [ホストグループ (Host Group)] : [内部ホストを含める (Include Inside Hosts)] を選択
 - f. [接続 (Connection)] の [アプリケーション (Applications)] : [未定義の TCP (Undefined TCP)] と [未定義の UDP (Undefined UDP)] の両方を選択
 - g. [接続 (Connection)] の [方向 (Direction)] : [合計 (Total)]
 - h. [詳細オプション (Advanced Options)] : [並び基準 (Order By)] = [バイト (Bytes)]
17. [検索 (Search)] をクリックします。



The screenshot shows the Cisco Stealthwatch web interface. The top navigation bar includes 'Dashboards', 'Monitor', 'Analyze', 'Jobs', 'Configure', and 'Deploy'. The 'Analyze' tab is active. The main content area is titled 'Top Ports Search'. It features a search configuration section with the following settings:

- Time Range:** Last 24 Hours (Time Range)
- Subject:** Inside Hosts (Host Groups) and Ether (Orientation)
- Connection:** Undefined TCP (Applications) and Undefined UDP (Applications) and Total (Direction)
- Peer:** Inside Hosts (Host Groups)

Below the search configuration, there are three columns for detailed settings:

- SEARCH TYPE:** Top Ports
- TIME RANGE *:** Last 24 Hours
- SEARCH NAME *:** Last 24hr Undefined TCP and UDP Ports

The detailed settings are organized into three panels:

- Subject:** HOST IP ADDRESS (ex. 192.168.10.10 or !192.168.10.10), HOST GROUPS (Select, Inside Hosts)
- Connection:** PORT / PROTOCOL (ex. 80/tcp or !80/tcp), APPLICATIONS (Select, Undefined TCP, Undefined UDP), DIRECTION (Total)
- Peer:** HOST IP ADDRESS (ex. 192.168.10.10 or !192.168.10.10), HOST GROUPS (Select, Inside Hosts)

18. 24 時間分のラボデータを処理するため、完了までに数分かかる場合があります。しばらくお待ちください。システムでは、過去 24 時間のすべての未定義の TCP および UDP ポートに関連するレポートを作成し、このドキュメントをポートでソートして、バイト数が最大のものから最小のものまで順番に表示します。
 - a. この元のページから、またはジョブ管理を使用して、レポートの進行状況をモニタできます。
19. 返されたドキュメントの結果を見ると、未分類のトラフィックのうち **TCP ポート 22609** の割合が大きいことがわかります。これを適切に分類できるように、ネットワークトラフィックの識別に役立つ追加のコンテキストを収集してみましょう。

Top Ports Search Results (51)

Edit Search | Last: 24 Hours (Time Range) | Save Search | Save Results | Start New Search

Subject: Inside Hosts (Host Groups) | Ether (Orientation) | 100% Complete | Delete Search

Connection: Undefined TCP (Applications) | Undefined UDP (Applications) | Total (Direction)

Peer: Inside Hosts (Host Groups)

% OF BYTES	PORT	HOST ROLE	BYTES	PACKETS	FLAWS	HOSTS	PEERS	HOST BYTES RA...
54.08%	22609 / TCP	Client and Server	367.55 G	311 M	1	2	2	50.00%
27.22%	2055 / UDP (netflow)	Client and Server	166.64 G	144.34 M	164	28	28	50.00%

Manage Columns | Export

20. この最初のエントリの [フロー (Flows)] の数字をクリックします ([フロー (Flows)] 列の数字はリンクになっています)。表示されるドキュメントは、Java クライアントで表示される上位カンパセーションドキュメントに似ています。

Flow Search Results (1)

Edit Search | 10/20/2018 12:17 PM - 10/21/2018 12:17 PM (Time R...) | 1,000 (Max Records) | Save Search | Save Results | Start New Search

Subject: Inside Hosts (Host Groups) | Ether (Orientation) | 1% Complete | Cancel Search

Connection: 22609/TCP (Port / Protocol) | Undefined TCP (Applications) | Undefined UDP (Applications) | All (Flow Direction) | PCNF (Flow Collector Name)

Peer: Inside Hosts (Host Groups)

START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST C
Oct 20, 2018 9:15:53 PM [15hr 6min 41s ago]	15hr 2min 6s	10.201.3.20	50928/TCP	Atlanta, PCI Devices	2.71 M	Undefined TCP	2.2 G	10.201.1.51	22609/TCP	Atlanta

Manage Columns | Summary | Export

50 items per page | 1 - 1 of 1 items

21. この画面に列を追加して、接続の方向 (クライアント/サーバ) を表示できるようにします。[列の管理 (Manage Columns)] をクリックします。



22. ポップアップウィンドウの上部メニューから [サブジェクト (Subject)] を選択し、[サブジェクトの方向 (Subject Orientation)] 列を選択します。

Flow Table Columns

Connection Subject Peer General

Subject ASN
 Subject ASN Assignment
 Subject Byte Rate
 Subject Byte Ratio
 Subject Bytes
 Subject File Hash
 Subject FIN Packets
 Subject Hostname
 Subject Host Groups
 Subject Interfaces
 Subject IP Address
 Subject Location
 Subject MAC Address
 Subject MAC Vendor
 Subject NAT

Subject NAT Hostname
 Subject NAT Port
 Subject Orientation
 Subject Packet Rate
 Subject Packets
 Subject Parent File Hash
 Subject Parent Process Name
 Subject Payload
 Subject Port/Protocol
 Subject Process Account
 Subject Process Name
 Subject RST Packets
 Subject SYN Packets
 Subject SYN/ACK Packets
 Subject TrustSec ID

Subject TrustSec Name
 Subject User

Select All Deselect All Restore Defaults

Cancel Set

23. [ピア (Peer)] > [ピアの方向 (Peer Orientation)] の列も追加します。

Flow Table Columns

Connection Subject Peer General

Peer ASN
 Peer ASN Assignment
 Peer Byte Rate

Peer NAT Hostname
 Peer NAT Port
 Peer Orientation

Peer TrustSec Name
 Peer User

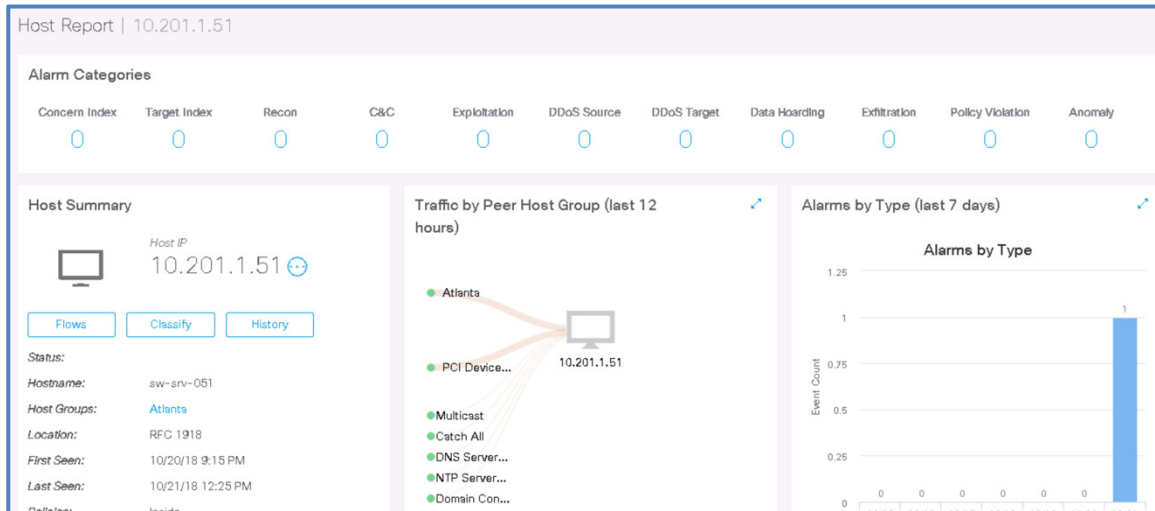
24. [設定 (Set)] をクリックします。

25. このドキュメントに変更が適用され、ホスト 10.201.1.51 が 22609/TCP のサーバとして機能し、10.201.3.20 がクライアント/ピアとなっていることがわかります (一部の列は右にスクロールしないと表示されない場合があります)。

START	DURATION	SUBJECT IP AD...	SUBJECT ORE...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...	PEER ORIENTAT...	PEER PORT PR...
Ex. 06/05	Ex. <=50min	Ex. 10.10.10	Ex. client	Ex. 57100/UA	Ex. *catch AI	Ex. <=50M	Ex. *Corpora	Ex. <=50M	Ex. 10.255.2	Ex. Server	Ex. 2055/UD
Jul 24, 2018 2:38:...	5d 22hr 58min 26s	10.201.3.20	Client	50928/TCP	Atlanta, PCI Dev...	1.46 G	Undefined TCP	288.62 G	10.201.1.51	Server	22609/TCP

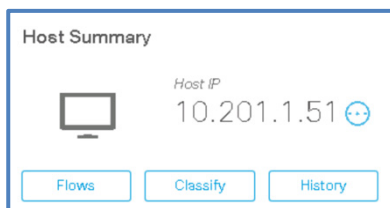
- ネットワークトラフィックに関連するホストについての情報をお客様に提供したところ、これは IP ビデオ監視システムからのものと判断されました。では、サーバとネットワークトラフィックの双方を適切に分類しましょう。

26. ドキュメント内の **10.201.1.51** IP アドレスをクリックすると、この IP アドレスの [ホストレポート (Host Report)] が表示されます (表示される結果は下の図と異なる場合があります)。



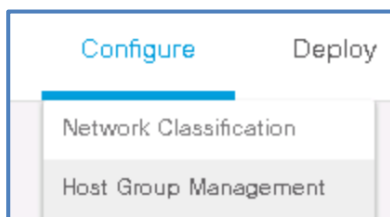
a. この画面を上下にスクロールして、問題のホストに関する豊富なデータが表示されることを確認します。

27. [分類 (Classify)] をクリックします。



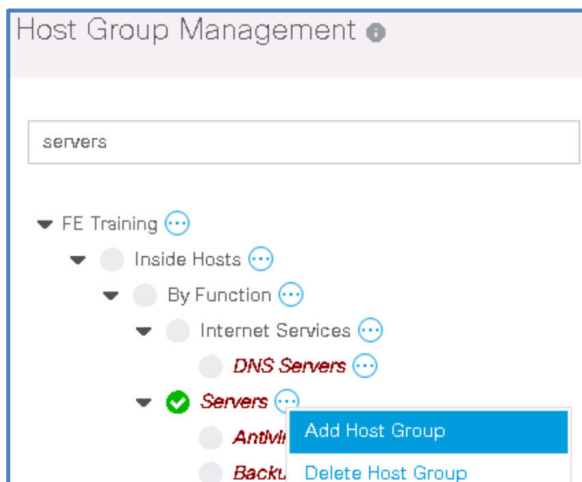
28. [ホストグループセレクタ (Host Group Selector)] が開きます。ホストはすでにアトランタのシステムとして分類されていることがわかります。カメラサーバ用の新しいホストグループを作成する必要がありますが、ここからは作成できません。[ホストの分類 (Classify Hosts)] エディタで [キャンセル (Cancel)] をクリックします。

29. 新しいホストグループを作成するには、[設定 (Configure)] > [ホストグループ管理 (Host Group Management)] を選択する必要があります。

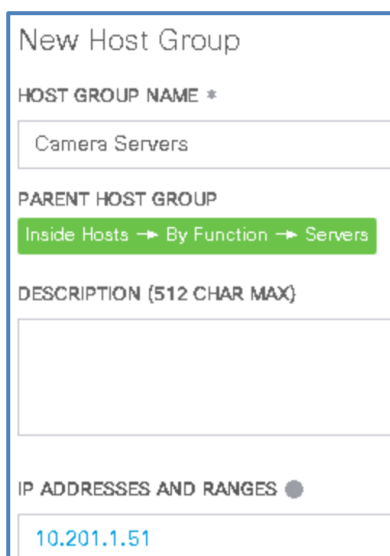


30. [ホストグループ名でフィルタ (Filter by Host Group Name)] フィールドに **servers** と入力し、**Enter** を押します。

31. リストがフィルタリングされたら、[サーバ (Servers)] の **アクションアイコン** をクリックし、[ホストグループの追加 (Add Host Group)] をクリックします。

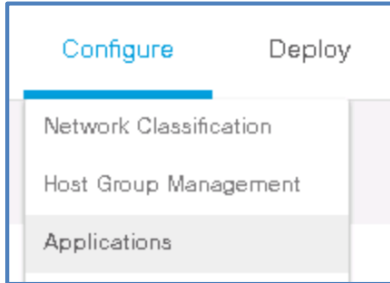


32. [新規ホストグループ (New Host Group)] ウィンドウが表示されたら、次の値を入力して**カメラサーバ**のための新しいホストグループを設定し、[保存 (Save)] をクリックして続行します。
- [ホストグループ名 (Host Group Name)] : **Camera Servers**
 - [IP アドレスと範囲 (IP Address and Ranges)] : **10.201.1.51**
 - [保存 (Save)] をクリックします。

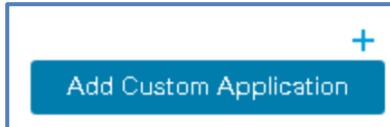


注 : カメラサーバをホストグループに分類したので、アプリケーション分類を、そのホストグループ宛てのトラフィックのみに限定できるようになります。もう 1 つのメリットとしては、このホストが Stealthwatch ドキュメントに表示されると、それがカメラサーバであることがホスト グループ メンバーシップによって示され、お客様に追加のコンテキストが提供されるとともに、ホストグループに対するレポートの実行が可能になるということもあります。では、これからセキュリティ カメラ トラフィックのためのアプリケーションを作成しましょう。

33. [設定 (Configure)] > [アプリケーション (Applications)] メニュー項目の順にクリックします。



34. [カスタムアプリケーションの追加 (Add Custom Application)] をクリックします。



35. 次の値を使用して、セキュリティカメラビデオのアプリケーションを設定します。

- a. [名前 (Name)]: **Security Camera Video**
- b. [説明 (Description)]: [ストリーミングセキュリティカメラのビデオフィード (Streaming security camera video feeds)]
- c. [ポート/プロトコル (Port/Protocol)]: **22609/TCP**
- d. [サーバ (Server)] フィールドを [ホストグループ (Host Group)] に変更して、[選択 (Select)] ボタンをクリックします。[ホストグループセクタ (Host Group Selector)] ウィンドウが表示されます。[エンタープライズ (Enterprise)] ツリーをたどって、作成したばかりの [カメラサーバ (Camera Servers)] ホストグループを見つけ ([内部ホスト (Inside Hosts)] > [機能別 (By Function)] > [サーバ (Servers)] > [カメラサーバ (Camera Servers)])、[カメラサーバ (Camera Servers)] ホストグループを選択します。選択したら、[適用 (Apply)] ボタンをクリックします。

Custom Application: Security Camera Video

NAME: *

DESCRIPTION (OPTIONAL):

ADD RULE

1 Enter at least one criteria to define the custom application below. Criteria within each block is 'AND-ed' together. Subsequent blocks are 'OR-ed' together.

Port/Protocol: ⓘ

Server: ⓘ

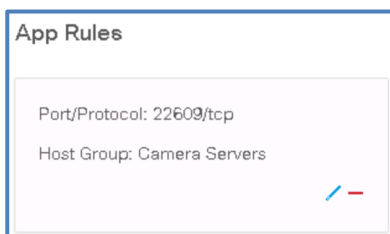
Host Groups

Select

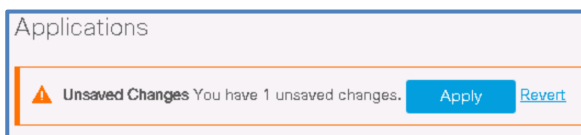
DPI Classification: ⓘ

36. [ルールに追加 (Add to Rules)] をクリックします。

37. アプリケーションルールのエントリが [アプリケーションルール (App Rules)] のリストに追加されます。[保存 (Save)] をクリックします。



38. [適用 (Apply)] をクリックして、変更内容を適用します。



39. 不明なトラフィックをポート別に特定し、それまで未分類だったネットワークトラフィックの定義を作成し、ホストグループを作成し、既知のホストを IP アドレスによりこのグループに割り当てました。これにより、レポートの面でお客様の役に立つだけでなく、Stealthwatch のクライアント/サーバ判定にも役立ちます。ラボの次の手順に進みます。

注：セキュリティ カメラ ビデオ アプリケーションとして分類されるのは、TCP/22609 を使用するカメラサーバホストグループ宛ての新しいフローだけです。以前のフローレコードの新しいアプリケーション定義による再分類は行われません。対象となるのはこの時点以降のフローのみです。

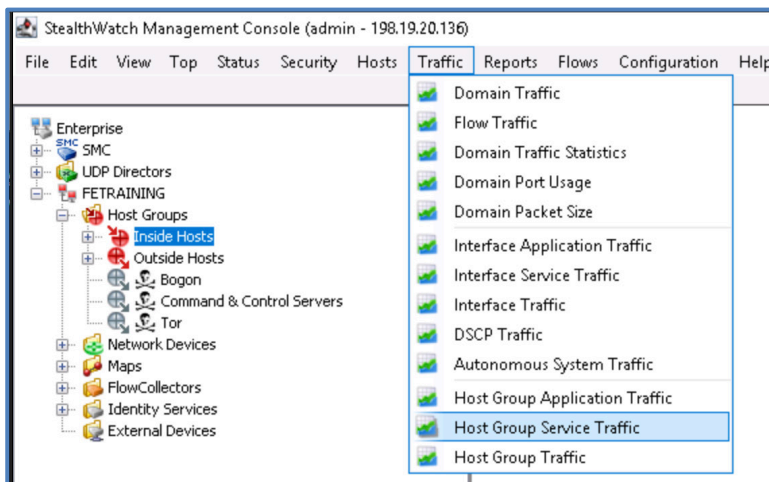
未定義のサービスの分類：デスクトップクライアント

Stealthwatch では、レイヤ 4 のネットワークトラフィック分類方式でサービスを分類します。Web クライアントでまだ確認していない、セキュリティイベントとアラームポリシーの関連サービスに固有の設定があります。サービスだけでなくアプリケーションも分類するのがベストプラクティスです。ここでは、デスクトップクライアントのサービス分類プロセスについて説明します。

40. admin ユーザとしてデスクトップクライアントにログインしていることを確認します。



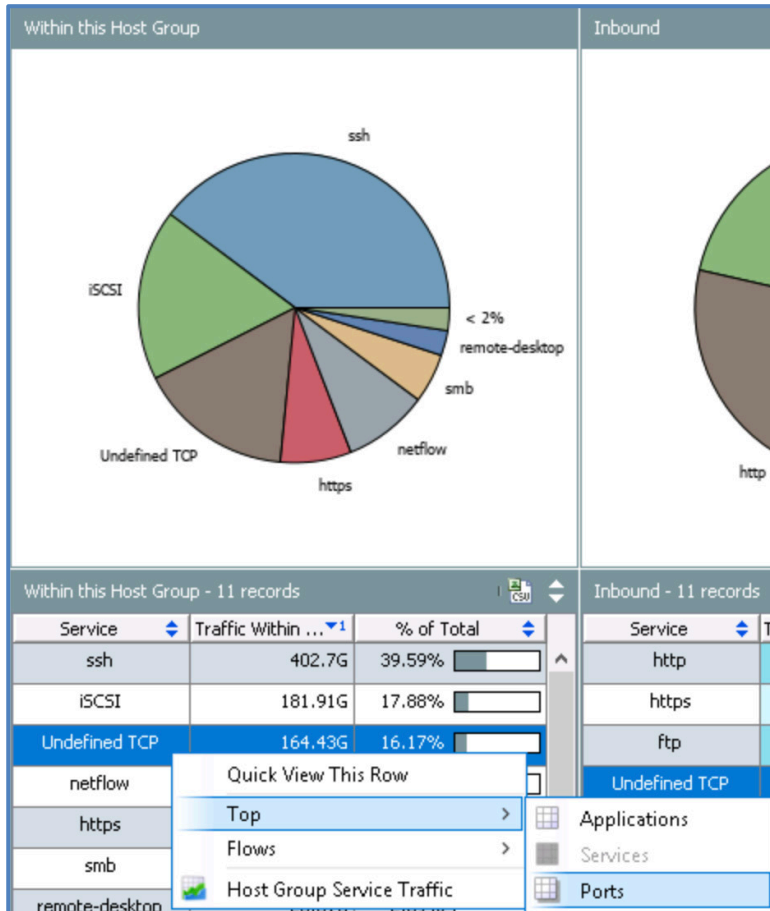
41. [エンタープライズ (Enterprise)] ツリー内の [内部ホスト (Inside Hosts)] ホストグループに移動し、[内部ホスト (Inside Hosts)] ホストグループを選択します。
42. [トラフィック (Traffic)] メニューをクリックし、[ホストグループサービストラフィック (Host Group Service Traffic)] メニューオプションを選択します。



43. [ホストグループサービストラフィック (Host Group Service Traffic)] ドキュメントが表示されます。[サマリー (Summary)] ページをクリックし、[未定義 TCP (Undefined TCP)] のエントリに注目します。そのリストに表示された数字は、そのドキュメントのタイムフレームでのサービス未定義のトラフィックの量を表しています。

Within this Host Group - 11 records			Inbound - 11 records			Outbound - 11 records		
Service	Traffic	% of Total	Service	Traffic In...	% of Total	Service	Traffic Ou...	% of Total
ssh	424.08G	41...	http	41.09G	...	http	4.86G	...
iSCSI	188.82G	18...	https	38.36G	...	https	2.37G	...
Undefined TCP	169.67G	16...	ftp	12.43G	...	Undefined TCP	736.99M	...
https	83.19G	8...	Undefined TCP	11.46G	...	Others	372.67M	...
smb	55.53G	5...	netflow	6.59G	...	ftp	244.68M	...
netflow	36.52G	3...	Others	870.09M	...	ssh	33.93M	...
remote-desktop	28.43G	2...	ssh	340.2M	...	smb	4.12M	...

44. データの [このホストグループ内 (Within this Host Group)] 列で、[未定義 TCP (Undefined TCP)] のエントリを右クリックし、[上位 (Top)] メニューを選択し、[ポート (Ports)] メニュー項目を選択します。



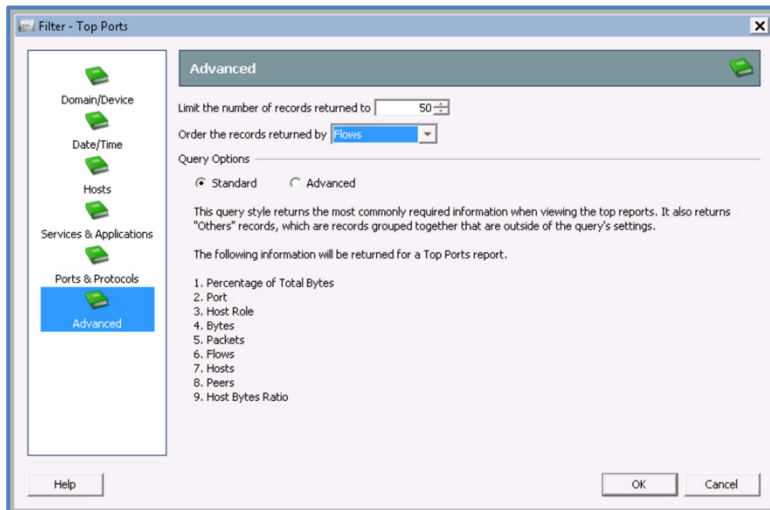
45. クエリが完了すると、上位ポートのドキュメントが表示されます。結果の中に、TCP ポート 3268 のエントリがあります。これは、Microsoft Active Directory グローバルカタログポートです。このラボで後ほど、これに関するエントリを [サービスおよびアプリケーション (Services and Applications)] で作成します。

#	% of Bytes	Port	Host Role
1	65.23%	57081/tcp (Undefined TCP)	Client and Server
2	10.15%	2393/tcp (Undefined TCP)	Client and Server
3	9.45%	44022/tcp (Undefined TCP)	Client and Server
4	5.94%	3268/tcp (Undefined TCP)	Client and Server

注：お客様の環境では、通常、トラフィックまたはフローを最も多く生成するポートの分類を重点的に行うことになります。お客様の環境の固有の知識または業界知識からすぐに識別可能なトラフィックタイプがあるという場合は、先に進み、検証をほとんどあるいはまったく行わずにトラフィックのサービスまたはアプリケーションの定義を作成しても構いません。そうでない場合は、未定義ネットワークトラフィックの具体的な内容を判断する指標とするための、お客様の組織に関する知識が必要になります。

問題のトラフィックタイプを生成しているマシンを示す [上位ホスト (Top Hosts)] または [上位カンバセーション (Top Conversations)] などの追加ドキュメントを提供することで、お客様をサポートできます。この追加コンテキストは、お客様にとって、トラフィックの実態を判定するために非常に有益である可能性があります。たとえば、お客様は具体的なポート番号を把握していないかもしれませんが、ネットワークトラフィックに関連するすべてのホストがバックアップサーバであることを知れば、そのトラフィックがエンタープライズ バックアップ アプリケーションによって生成されていると判断でき、その後、それに応じた分類を行うことが可能になります。

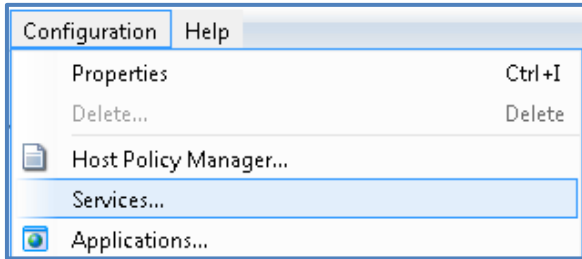
46. 返される値の並びを、[バイト (Bytes)] から [フロー (Flows)] に変更します。ドキュメントの左上にある漏斗のような形の [フィルタ (Filter)] ボタンをクリックします。
47. 左ペインの [詳細設定 (Advanced)] メニューを選択し、[返されるレコードの並び基準 (Order the records returned by)] オプションを [フロー (Flows)] に変更し、[OK] をクリックします。



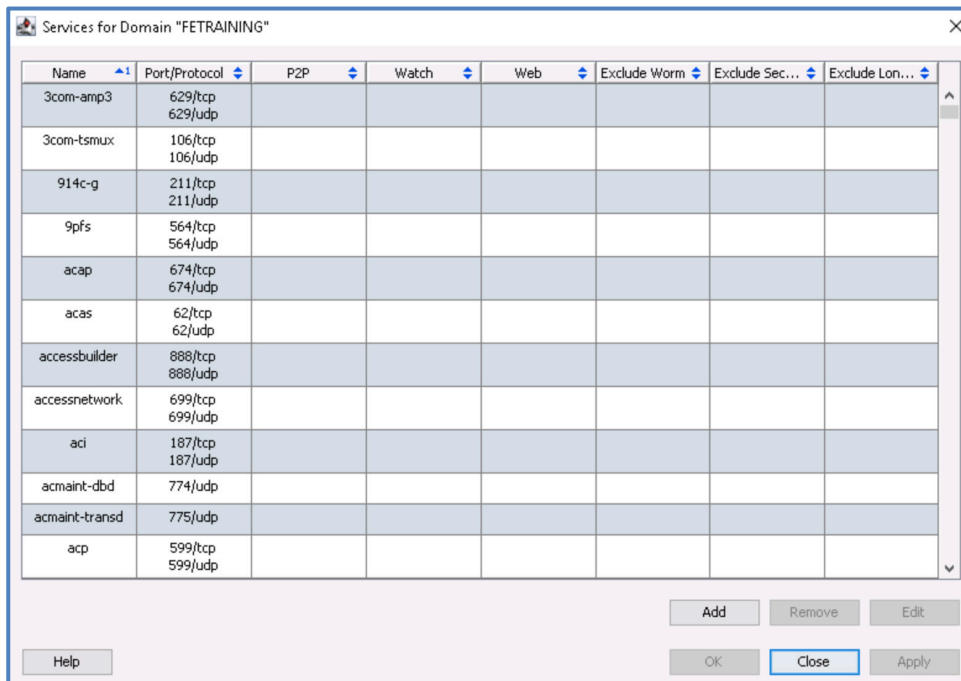
48. トラフィックの並びがバイト数順ではなくフロー順になり、結果が変更されます。ドキュメントの TCP ポート 52311 では多くのフローが記録されています。お客様の環境に関する知識をもとにして、このトラフィックは IBM BigFix (ソフトウェアの配布、インベントリ、およびパッチ適用の目的でお客様が使用しているシステム管理ソフトウェア) と判断されました。

	% of Flows	Port	Host Role	Bytes	Packets	Flows	Hosts	Peers	Host Bytes Ratio
1	19.66%	52311/tcp (Undefined TCP)	Client and Server	743.91M	912,688	8,116	126	126	50%
2	7.59%	8014/tcp (Undefined TCP)	Client and Server	2.68G	2,861,678	3,134	102	102	50%
3	5.44%	49155/tcp (Undefined TCP)	Client and Server	56.5M	204,390	2,247	175	175	50%
4	3.51%	60274/tcp (Undefined TCP)	Client and Server	4.55M	31,868	1,448	123	123	50%

49. これから、識別された 2 つのネットワーク トラフィック タイプのためのサービスを作成します。[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。



50. [サービス (Services)] ウィンドウが表示され、定義済みのすべてのサービスが表示されます。



51. [追加 (Add)] をクリックし、次の値を入力してサービスを定義し、[OK] をクリックします。

a. [名前 (Name)] : AD Global Catalog

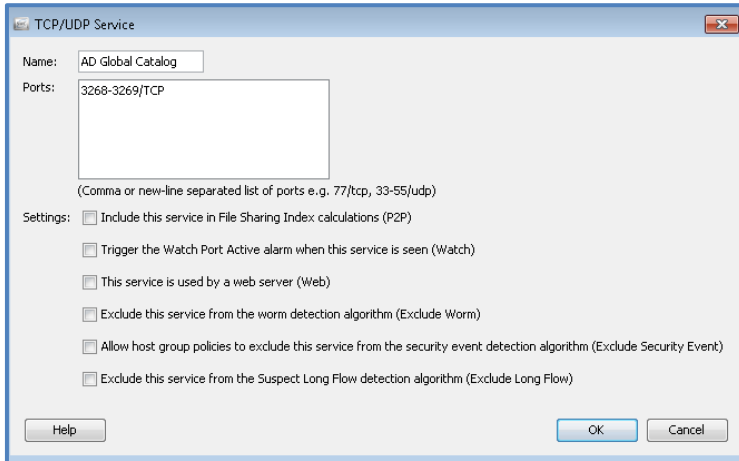
- i. [名前 (Name)] フィールドは、[サービス (Service)] フィールド表示のあるドキュメントにおけるネットワークトラフィックの表示名を指定するものです。

b. [ポート (Ports)] : **3268-3269/tcp**

- i. ポートフィールドでは、分類対象のネットワークトラフィックに一致するポートとプロトコルの組み合わせとして複数のエントリを指定できます。
- ii. ポートの定義には個々のポートまたはポートの範囲を使用できます。さらに、同じサービス定義に UDP ポートと TCP ポートを入れることも可能です。
- iii. 3268 は保護のないグローバル カタログ トラフィックであり 3269 は保護されたグローバル カタログ トラフィックであるため、この例ではポート 3268-3269/tcp を使用しています。これはこのお客様の環境に特有のものではなく、むしろ業界標準です。

- iv. 特定の 1 つのポートを定義できるサービスエントリは 1 つだけです。3268/tcp を AD グローバルカタログとして定義すると、別のサービスの定義には使用できなくなります。

c. ここではエントリにこれ以外の設定を指定する必要はありません。



TCP/UDP Service

Name: AD Global Catalog

Ports: 3268-3269/TCP

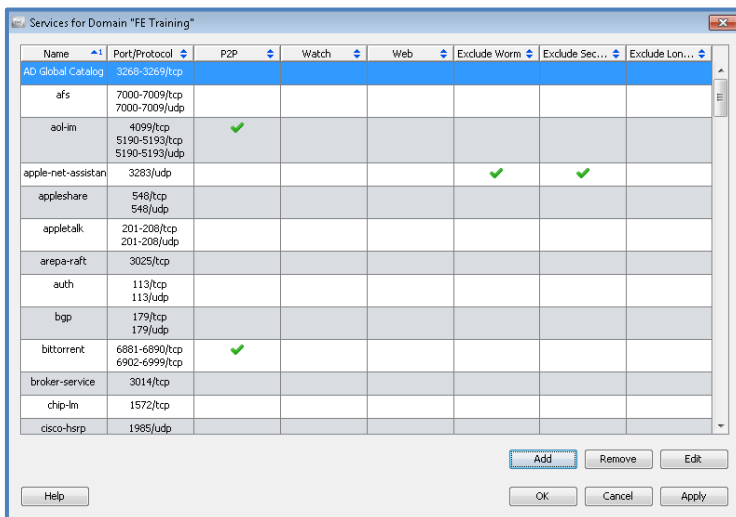
(Comma or new-line separated list of ports e.g. 77/tcp, 33-55/udp)

Settings:

- Include this service in File Sharing Index calculations (P2P)
- Trigger the Watch Port Active alarm when this service is seen (Watch)
- This service is used by a web server (Web)
- Exclude this service from the worm detection algorithm (Exclude Worm)
- Allow host group policies to exclude this service from the security event detection algorithm (Exclude Security Event)
- Exclude this service from the Suspect Long Flow detection algorithm (Exclude Long Flow)

Buttons: Help, OK, Cancel

52. AD グローバルカタログサービスが作成され、[サービス (Services)] ウィンドウに表示されます。



Name	Port/Protocol	P2P	Watch	Web	Exclude Worm	Exclude Sec...	Exclude Lon...
AD Global Catalog	3268-3269/tcp						
afs	7000-7009/tcp 7000-7009/udp						
ad-in	4099/tcp 5190-5193/tcp 5190-5193/udp	✓					
apple-net-assistan	3283/udp				✓	✓	
appleshare	548/tcp 548/udp						
appletalk	201-208/tcp 201-208/udp						
arepa-raft	3025/tcp						
auth	113/tcp 113/udp						
bgp	179/tcp 179/udp						
bittorrent	6881-6890/tcp 6902-6999/tcp	✓					
broker-service	3014/tcp						
chip-in	1572/tcp						
cisco-hsrp	1985/udp						

Buttons: Add, Remove, Edit, Help, OK, Cancel, Apply

53. 追加のサービスを追加するには、[追加 (Add)] をクリックし、次の値を入力してサービスを定義し、[OK] をクリックします。

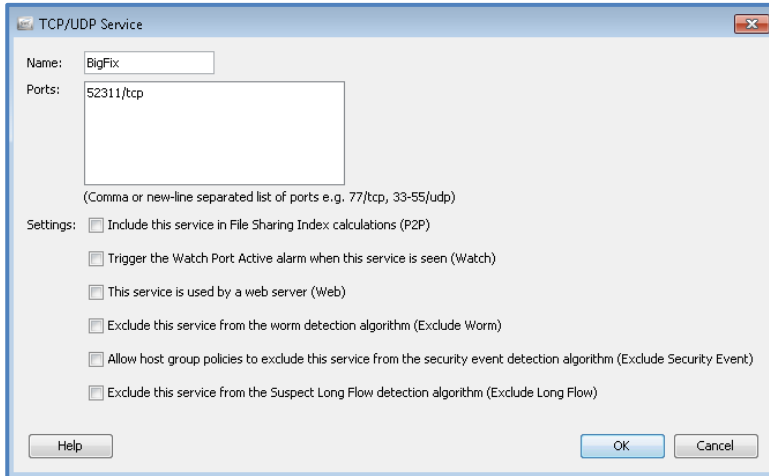
d. [名前 (Name)]: **BigFix**

- i. [名前 (Name)] フィールドは、[サービス (Service)] フィールド表示のあるドキュメントにおけるネットワークトラフィックの表示名を指定するものです。

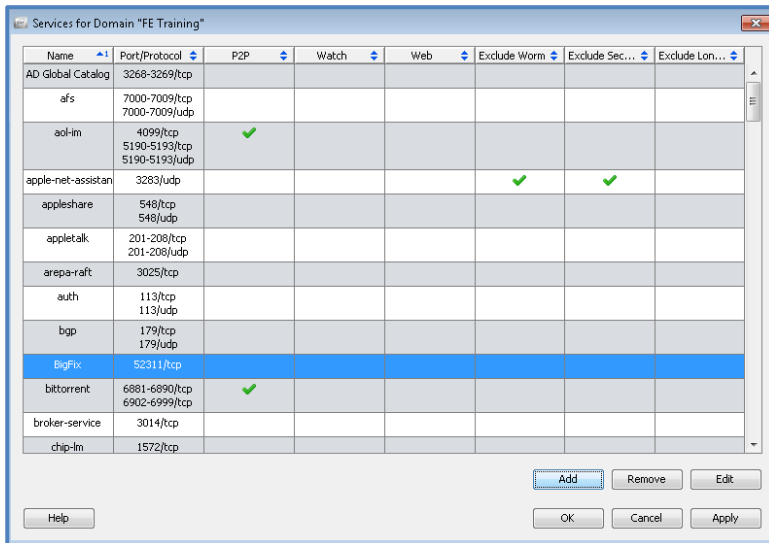
e. [ポート (Ports)]: **52311/tcp**

- i. ポートフィールドでは、分類対象のネットワークトラフィックに一致するポートとプロトコルの組み合わせとして複数のエントリを指定できます。
- ii. ポートの定義には個々のポートまたはポートの範囲を使用できます。さらに、同じサービス定義に UDP ポートと TCP ポートを入れることも可能です。

- iii. 52311/tcp ポートは IBM BigFix トราフィックのデフォルトのポートです。
- iv. 特定の 1 つのポートを定義できるサービスエントリは 1 つだけです。52311/tcp を BigFix として定義すると、別のサービスの定義には使用できなくなります。
- f. ここではエントリにこれ以外の設定を指定する必要はありません。



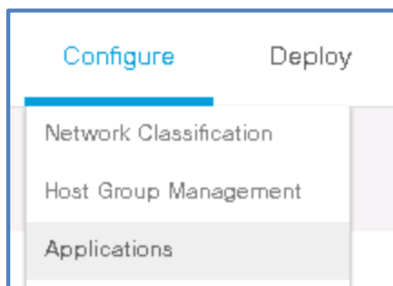
54. [OK] をクリックし、サービスに対する変更を確定します。



Name	Port/Protocol	P2P	Watch	Web	Exclude Worm	Exclude Sec...	Exclude Lon...
AD Global Catalog	3268-3269/tcp						
afs	7000-7009/tcp 7000-7009/udp						
aol-Im	4099/tcp 5190-5193/tcp 5190-5193/udp	✓					
apple-net-assistan	3283/udp				✓	✓	
appleshare	548/tcp 548/udp						
appletalk	201-208/tcp 201-208/udp						
arspar-raft	3025/tcp						
auth	113/tcp 113/udp						
bgp	179/tcp 179/udp						
BigFix	52311/tcp						
bittorrent	6881-6890/tcp 6902-6999/tcp	✓					
broker-service	3014/tcp						
chip-Im	1572/tcp						

55. また、サービスの作成時にアプリケーションも作成することをお勧めします。デスクトップクライアントで作成した 2 つのサービス用のアプリケーションを作成します。

56. SMC Web クライアントに戻り、[設定 (Configure)]メニューをクリックして、[アプリケーション (Applications)]を選択します。



注：アプリケーションには、設定を定義する「ルール」を複数持たせることが可能です。これらのルールは「OR」演算に似ています。つまり、いずれかのルールに一致すれば、ルールに一致したネットワークトラフィックはそのアプリケーションとして分類されます。

57. [カスタムアプリケーションの追加 (Add Custom Application)] をクリックし、[ルールの追加 (Add Rule)] セクションで、次の値を使用してアプリケーションを設定し、終わったら [ルールに追加 (Add to Rule)] をクリックします。

g. [名前 (Name)] : **AD Global Catalog**

i. SMC のドキュメントおよびレポートにおけるネットワークトラフィックの名称。

h. [説明 (Description)] : [Active Directory グローバルカタログポート (Active Directory Global Catalog Ports)]

i. 説明を記述するフィールド (省略可能)

i. [ポート/プロトコル (Port/Protocol)] : **3268-3269/TCP**

i. 単一のポートまたは連続するポート範囲およびプロトコル (TCP または UDP)

ii. 複数のポート範囲または複数の単一インスタンスポートを持つアプリケーションを定義する場合は、アプリケーションに追加ルールを追加する必要があります。

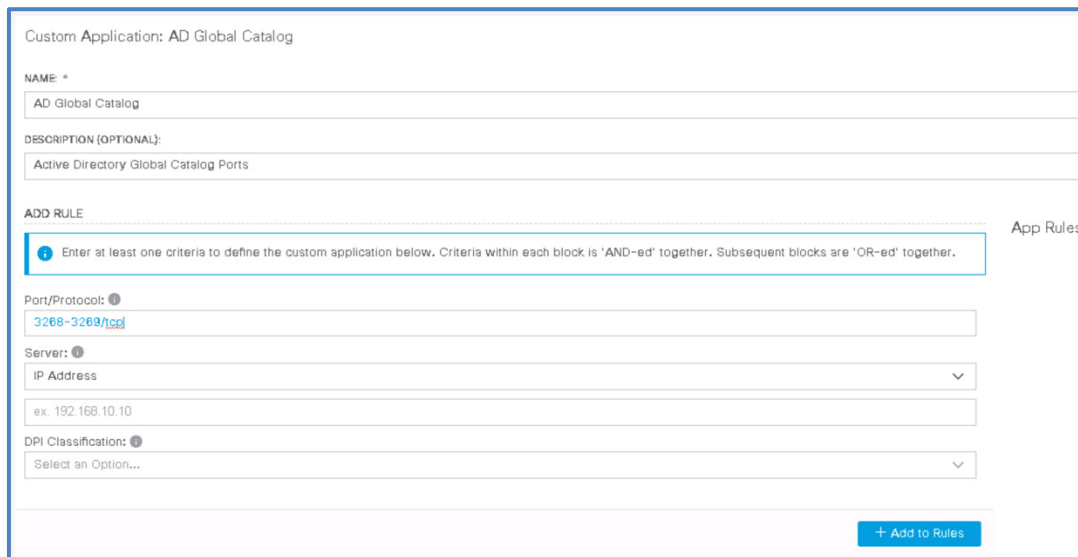
j. [サーバ (Server)] : **(省略可能 - このフィールドは空白のままにする)**

i. アプリケーション設定の選択肢としては、特定の IP 範囲またはホストグループを対象とするネットワークトラフィックのみを分類するオプション、またはポート/プロトコルの組み合わせに一致するあらゆるネットワークトラフィックを分類するオプションがあります。

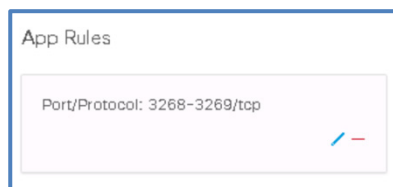
k. [DPI 分類 (DPI Classification)] : **(このフィールドは空白のままにする)**

i. これは、ディープ パケット インスペクションの定義に特化されているフィールドです。フローセンサーまたはその他の DPI ソースがないお客様の場合、このルールはどのネットワークトラフィックにも当てはまりません。

ii. これを使用する非常に特殊なユースケースがある場合を除いては、DPI フィールドには何も入力しないでください。

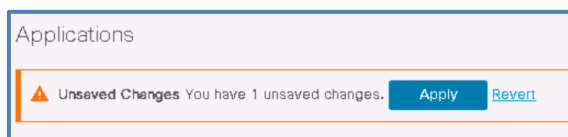


58. フォームの入力が終わったら、必ず [+ルールに追加 (+ Add to Rules)] をクリックしてください。
59. 今指定したばかりの条件が、アプリケーションの [アプリケーションルール (App Rules)] セクションに表示されます。

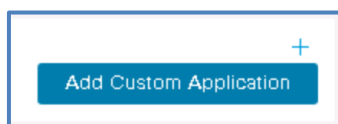


注： 追加ポートまたは追加すべき条件がある場合には、該当する値をすべて入力し [ルールに追加 (Add to Rules)] ボタンを再度クリックして、追加ルールをアプリケーションに追加します。

60. これでアプリケーションの設定が完了しました。必要に応じて下にスクロールし、[保存 (Save)] ボタンをクリックして終了します。
61. ここで、SMC アプリケーション設定への変更の適用または取り消しを確認するプロンプトが表示されます。[適用 (Apply)] クリックして、設定を保存します。



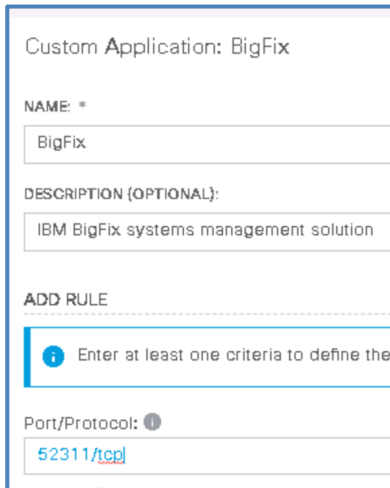
62. 次に、BigFix ネットワークトラフィックのためのアプリケーション分類を作成します。[カスタムアプリケーションの追加 (Add Custom Application)] ボタンをクリックします。



63. 次の値を使用してアプリケーションを設定し、[ルールに追加 (Add to Rule)] をクリックします。

- a. [名前 (Name)] : **BigFix**

- b. [説明 (Description)] : [IBM BigFix システム管理ソリューション (IBM BigFix systems management solution)]
- c. [ポート/プロトコル (Port/Protocol)] : **52311/TCP**



Custom Application: BigFix

NAME: *

BigFix

DESCRIPTION (OPTIONAL):

IBM BigFix systems management solution

ADD RULE

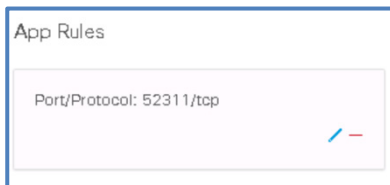
Enter at least one criteria to define the

Port/Protocol: ①

52311/tcp

64. 必ず [+ルールに追加 (+ Add to Rules)] をクリックしてください。

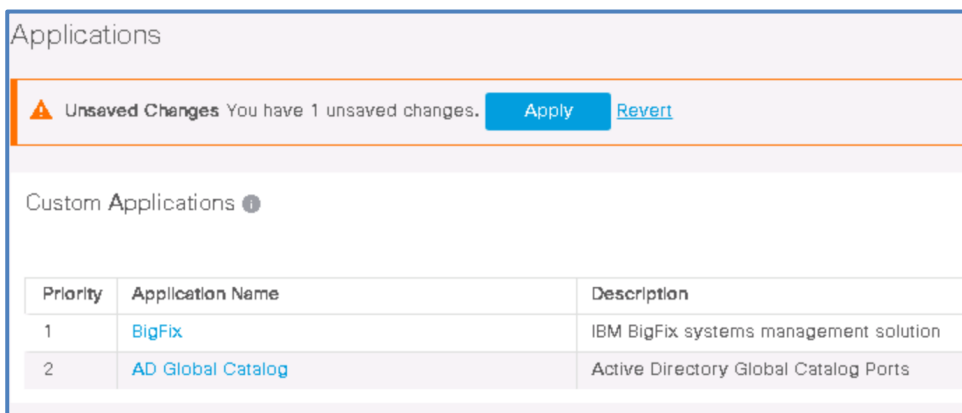
65. [アプリケーションルール (App Rules)] セクションにエントリが表示されます。[保存 (Save)] をクリックします。



App Rules

Port/Protocol: 52311/tcp

66. [適用 (Apply)] をクリックして変更内容を保存します。



Applications

⚠ Unsaved Changes You have 1 unsaved changes. [Apply](#) [Revert](#)

Custom Applications ①

Priority	Application Name	Description
1	BigFix	IBM BigFix systems management solution
2	AD Global Catalog	Active Directory Global Catalog Ports

任意：追加のサーバタイプの分類

このセクションの受講完了は必須ではありません。後で時間のあるときに、さらに練習が必要な場合のみ行ってください。以前に定義した手順を使用して、特定のタイプのネットワークトラフィックのサーバとして機能するホストの識別、Stealthwatch (Web クライアントまたは Java クライアント) を使用した以下のようなタイプのサーバの識別、既存のホストグループへの適切なホストの追加、新しいホストグループの作成などを実施してみましょう。レポートに記載された、サーバとして機能する上位 2 ~ 3 のホストが、お客様の環境にとって正当なものであり、それらを分類する必要があるとします。下記のサーバタイプの分類が終わったら、ラボの次の手順に進むことができます。ここに記載されている 5 つのホストグループの割り当てを完全に設定する必要はありませんが、プロセスに慣れるために必要な数だけ試行することが理想的です。

以前の方法を使用して、下記のサーバタイプのサーバとして機能するホストを識別し、必要に応じてホストグループを作成/定義します。

- **MS SQL サーバ (TCP ポート 1433、UDP ポート 1434)**
- **Oracle SQL サーバ (TCP ポート 1521)**
- **FTP (TCP ポート 21)**
- **リモートデスクトップ (TCP ポート 3389)**
- **DHCP (UDP ポート 67)**

任意：追加のサービスおよびアプリケーションの分類

このセクションの受講完了は必須ではありません。後で時間のあるときに、さらに練習が必要な場合のみ行ってください。以前に定義した手順を使用して、サービスとアプリケーションの定義の作成、SMC にまだエントリのない、次のタイプの一般的なネットワークトラフィックエントリの作成、さらに、SMC で定義済みのすべてのポートの作成などを実施してみましょう。各エントリにサービス定義とアプリケーション定義の両方を作成します。以下のネットワークポートのサービスおよびアプリケーションの作成が完了したら、ラボの次のセクションに進むことができます。ここに記載されている 3 つのアプリケーション/サービスの割り当てを完全に設定する必要はありませんが、プロセスに慣れるために必要な数だけ試行することが理想的です。

以前の方法を使用して、新しいサービスおよびアプリケーションの双方として定義すべきネットワークトラフィックを識別し、必要な設定を完了します。

- **SIP (UDP ポート 5060 ~ 5061)**
- **Symantec Endpoint Protection (TCP ポート 8014)**
- **Commvault (TCP ポート 8400 ~ 8402)**

シナリオのまとめ

このシナリオでは、Stealthwatch を使用してお客様のアプリケーションおよびサービスのデータセット内のギャップを割り出しました。サービスまたはアプリケーションの定義がなかったネットワークトラフィックを、必要に応じて分類/作成しました。お客様の環境を分類することは、導入時に必ず完了しておくべき非常に重要なプロセスです。

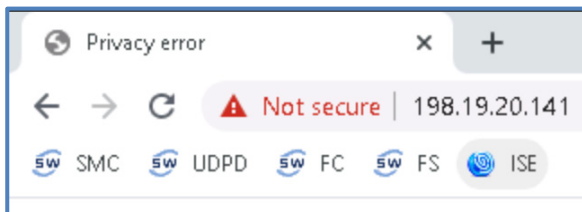
シナリオ 12. Cisco ISE (Identity Services Engine) との統合

Cisco ISE を Stealthwatch と統合することで、ユーザ アイデンティティ データを取得でき、またユーザの隔離に pxGrid を活用することもできます。このアイデンティティデータは、ネットワークトラフィックとユーザアイデンティティを相互に関連付け、エンドポイントデバイスの詳細なデータを表示するのに使用されます。統合プロセスには次のような側面があります。

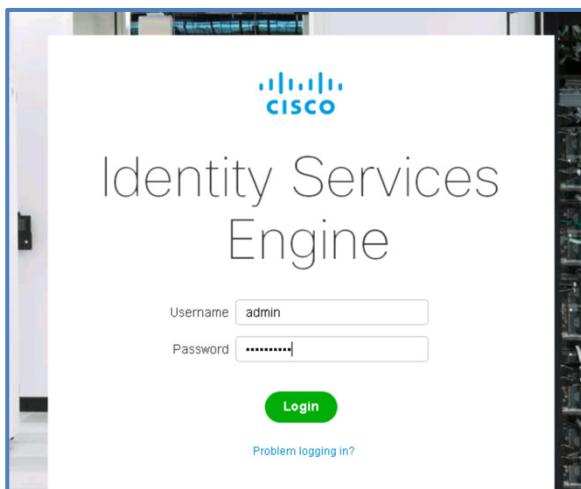
- ISE ノード (およびノード自体) で使用される証明書に署名する root CA を SMC が信頼していることを確認する
- ISE が pxGrid 経由で SMC と通信するように設定する
- ISE CA によって発行された信頼できる証明書を使用して SMC から ISE に対する認証を行う
- SMC コンソール内のすべての ISE 管理およびポリシーノードにエントリを追加する

ISE 管理者は、PxGrid 操作に必要な ISE アプライアンスをすでに設定済みですが、ISE アプライアンスと SMC が相互に信頼し、ユーザ アイデンティティ データが正しく処理されていることを確認する必要があります。

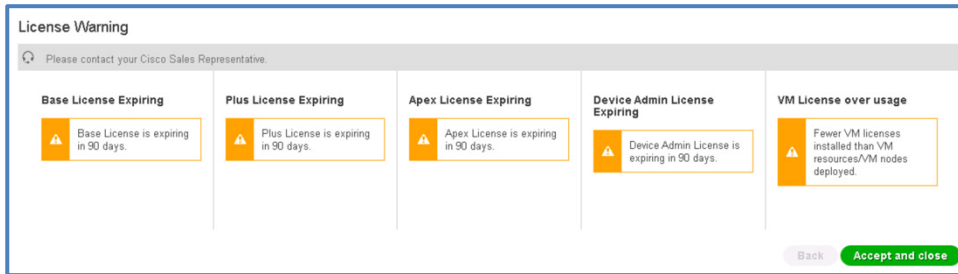
1. **Chrome** で新しいタブを開き、**ISE** のショートカットをクリックします。



2. 証明書の警告が表示されたら、[詳細設定 (Advanced)] ボタンをクリックして、[続行 (Proceed)] リンクをクリックします。
3. 次のログイン情報を使用して Identity Services Engine (ISE) にログインします。
 - a. [ユーザ名 (Username)]: **admin**
 - b. [パスワード (Password)]: **Cisco12345**
 - c. [ログイン (Login)] をクリックします。



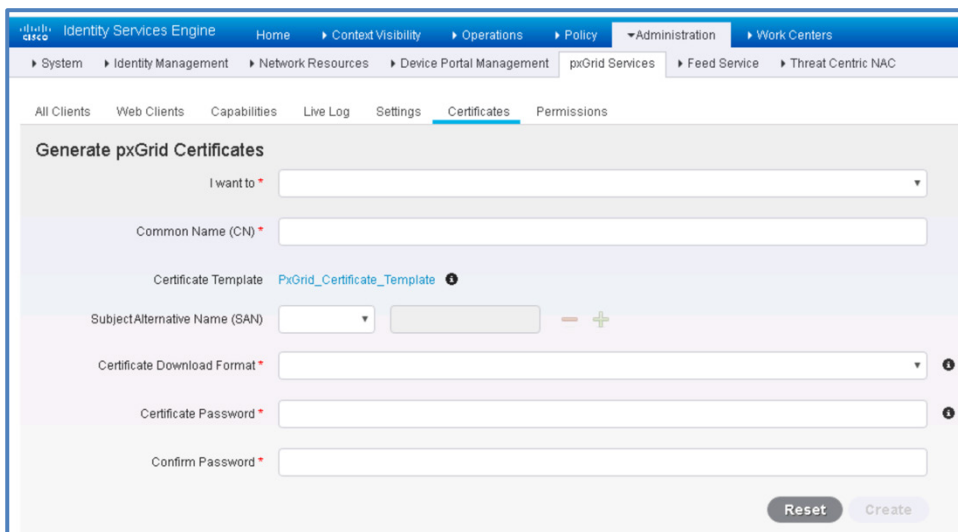
4. [同意して閉じる (Accept and close)] をクリックして、ラボの [ライセンス警告 (License Warning)] の警告を閉じます。



5. [管理 (Administration)] をクリックし、ポップアップメニューから [pxGrid サービス (pxGrid Services)] をクリックします。

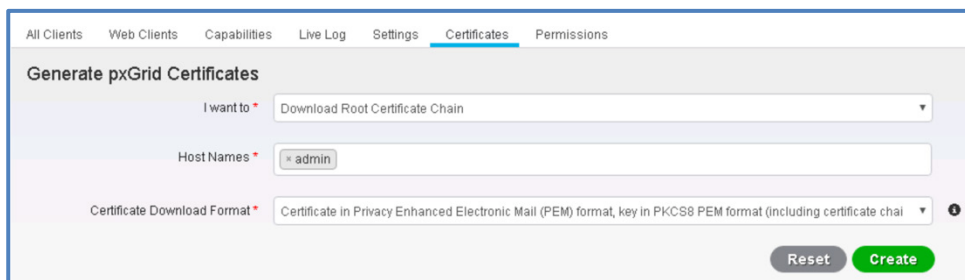


6. [証明書 (Certificates)] メニューオプションをクリックすると、[PxGrid 証明書の生成 (Generate pxGrid Certificates)] ページが表示されます。

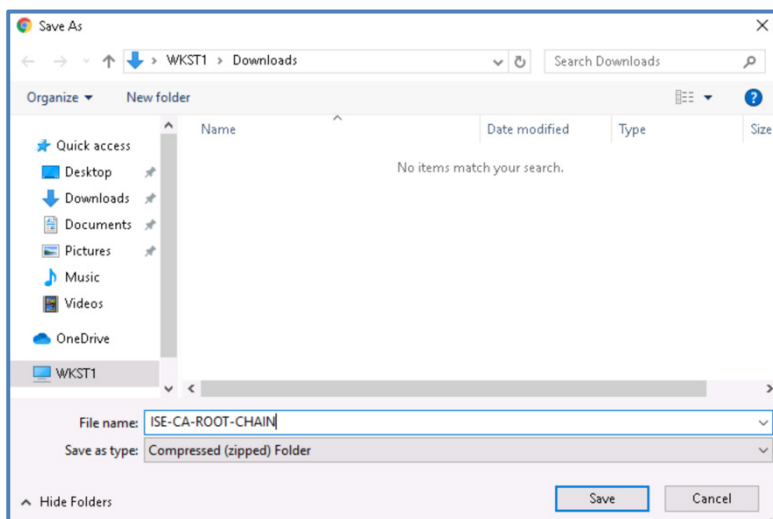


7. 次のようにフォームに入力します。
- [処理の選択 (I want to)] フィールドをクリックし、[ルート証明書チェーンのダウンロード (Download Root Certificate Chain)] を選択します。
 - [ホスト名 (Host Names)] フィールドをクリックし、[admin] を選択します
 - [証明書のダウンロード形式 (Certificate Download Format)] フィールドをクリックし、[PEM] オプションを選択します。

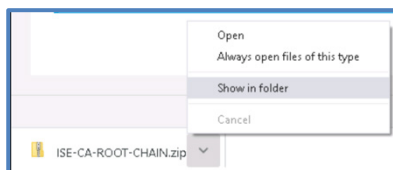
d. [作成 (Create)] をクリックします。



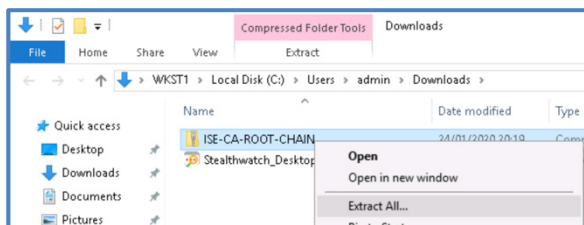
e. [名前を付けて保存 (Save As)] ページが開いたら、ファイル名を **ISE-CA-ROOT-CHAIN** に変更し、[保存 (Save)] をクリックします。



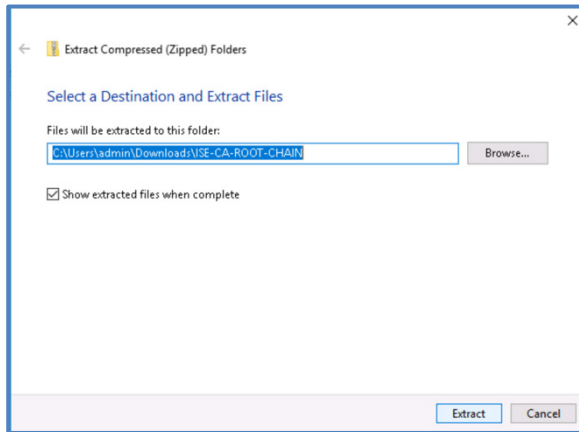
f. Chrome の下部にある **ISE-CA-ROOT-CHAIN.zip** ファイルの右側の記号をクリックし、[フォルダを開く (Show in folder)] をクリックします。



g. ISE-CA-ROOT-CHAIN.zip ファイルを右クリックし、[すべて展開 (Extract All...)] をクリックします。

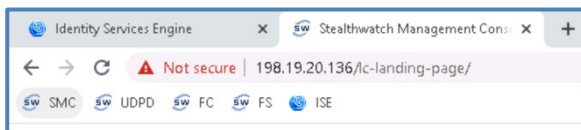


h. [展開 (Extract)] をクリックします。

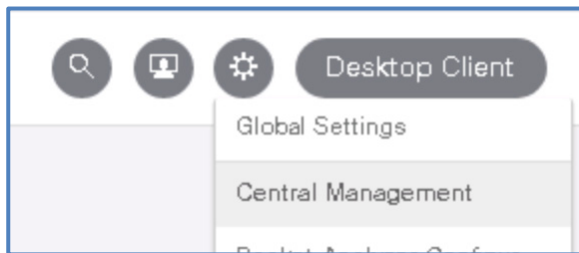


i. 両方のファイルブラウザのウィンドウを閉じ、Chrome Web ブラウザは開いたままにします。

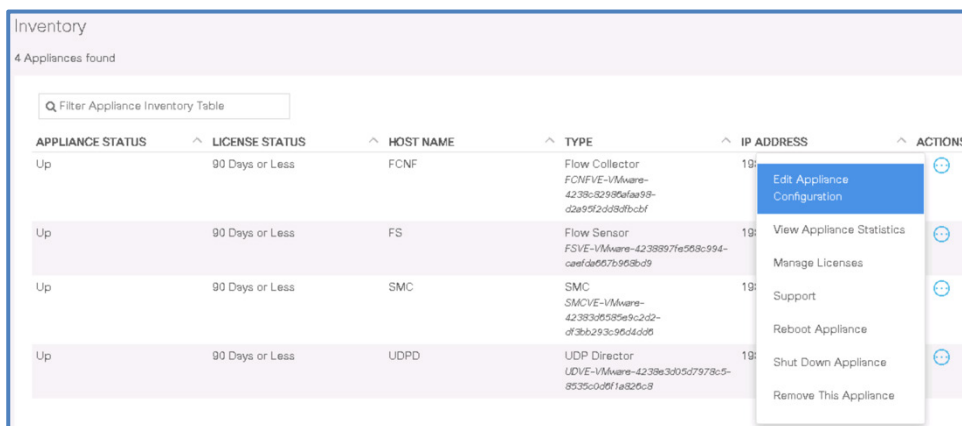
8. 新しい **Chrome** タブを開き、SMC のブックマークをクリックします。必要に応じて **admin** および **C1sco12345** を使用してログインします。



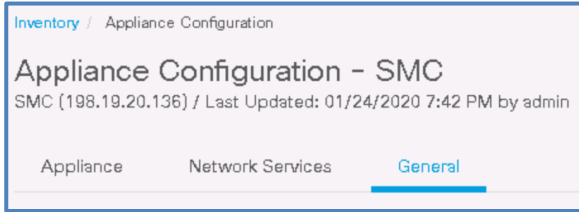
a. SMC ページの右上にある **歯車アイコン** をクリックし、[Central Management] をクリックします。



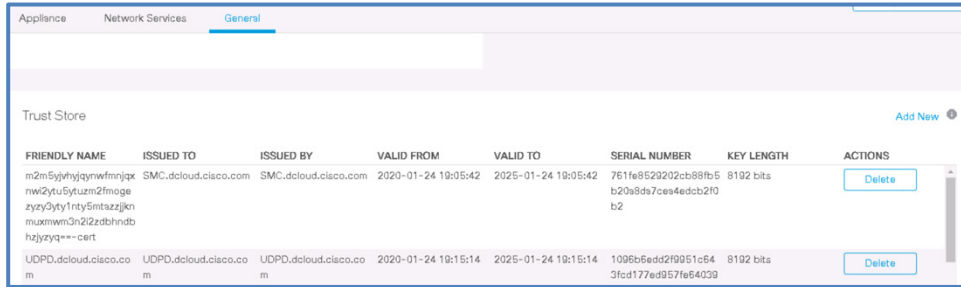
b. [Central Management] ページで、[SMC] アプライアンスを見つけて、関連付けられた [アクション (Actions)] アイコンをクリックし、[アプライアンス設定の編集 (Edit Appliance Configuration)] を選択します。



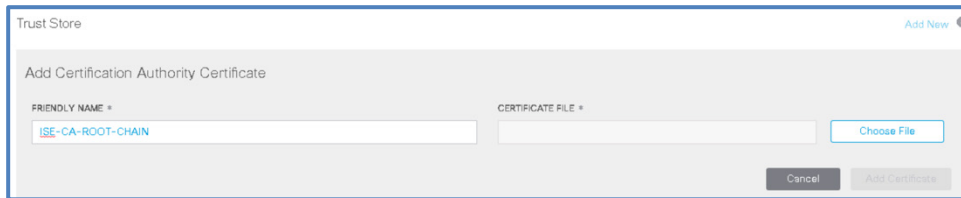
c. [一般設定 (General)] をクリックします。



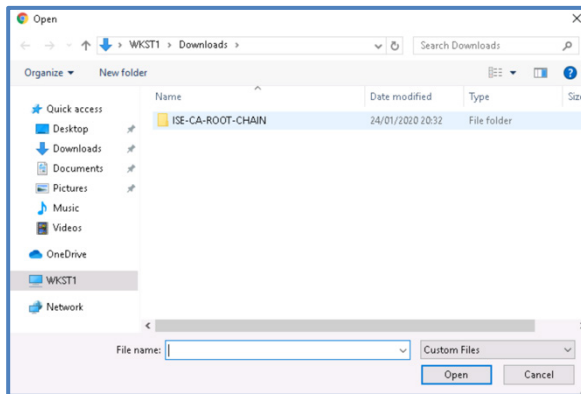
- i. [信頼ストア (Trust Store)]が表示されるまで下にスクロールし、[新規追加 (Add New)]をクリックします。



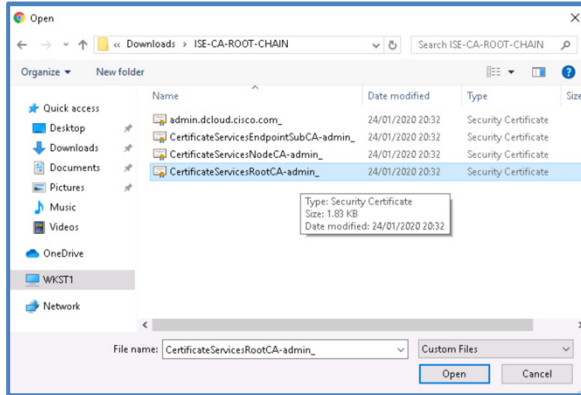
- ii. [フレンドリ名 (Friendly Name)]フィールドに **ISE-CA-ROOT-CHAIN** と入力し、[ファイルの選択 (Choose File)]をクリックします。



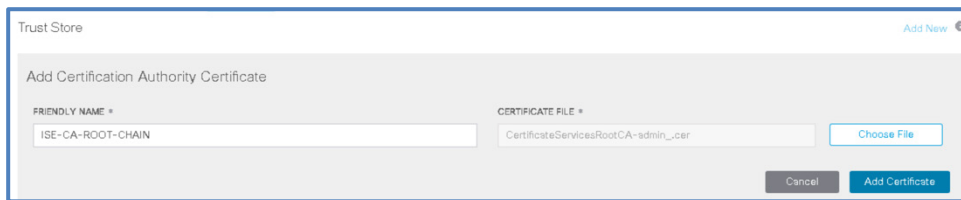
- iii. [WKST1] > [ダウンロード (Downloads)]の順に移動して、**ISE-CA-ROOT-CHAIN** フォルダをダブルクリックします。



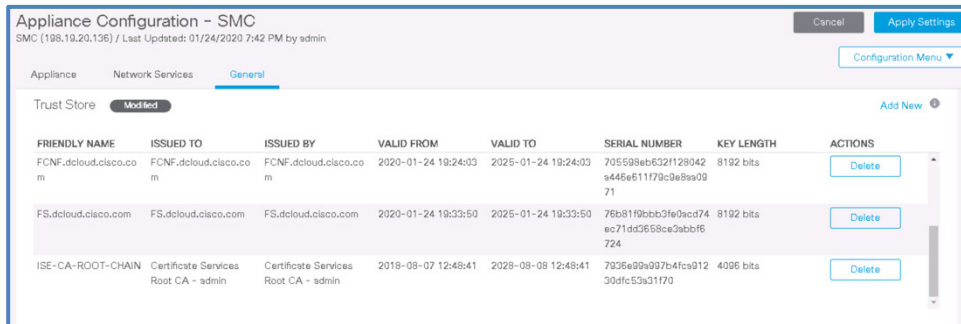
- iv. **CertificateServicesRootCA admin_** ファイルをクリックし、[開く (Open)]をクリックします。



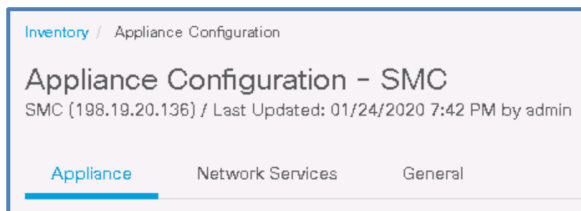
v. [証明書の追加 (Add Certificate)] をクリックします。



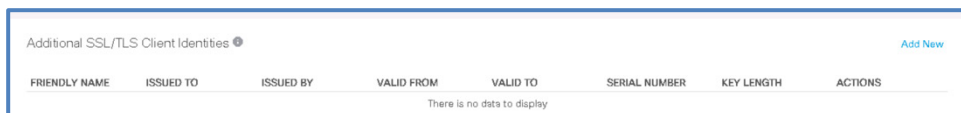
vi. SMC 信頼ストアに新しく追加した証明書が表示されます (信頼ストアで下にスクロールする必要があります)。これで、SMC が ISE CA によって発行された証明書を信頼するようになります。



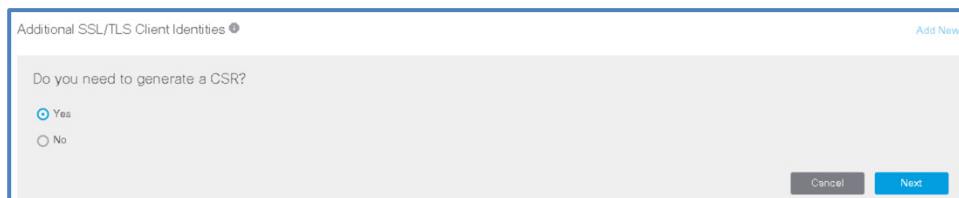
d. [アプライアンス (Appliance)] タブをクリックします。



i. [追加の SSL/TLS クライアントアイデンティティ (Additional SSL/TLS Client Identities)] セクションが表示されるまで下にスクロールし、[新規追加 (Add New)] をクリックします。



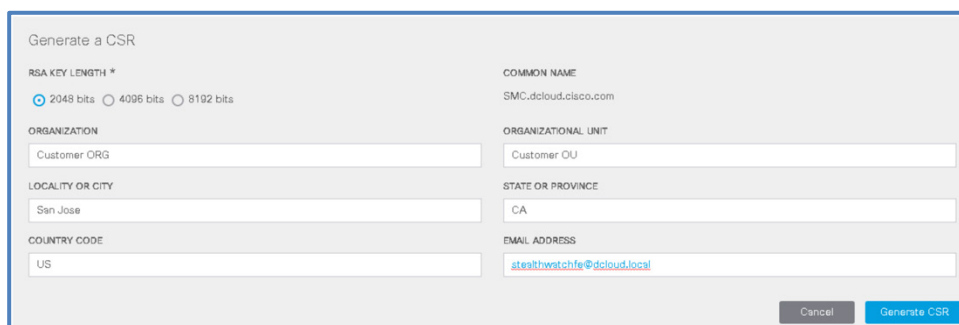
- ii. CSR を生成する必要があるかどうか尋ねられたら、[はい (Yes)] が選択された状態で [次へ (Next)] をクリックします。



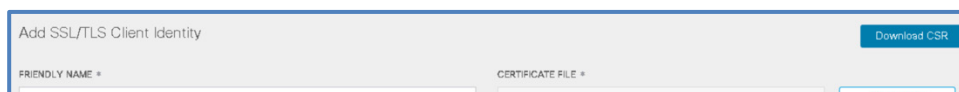
- iii. CSR に次のように入力します。

1. [RSA キー長 (RSA Key Length)] : [2048 ビット (2048 bits)]
2. [組織 (Organization)] : **Customer ORG**
3. [組織単位 (Organizational Unit)] : **Customer OU**
4. [市区町村 (Locality or City)] : **San Jose**
5. [州または都道府県 (State or Province)] : **CA**
6. [国コード (Country Code)] : **US**
7. [電子メールアドレス (Email Address)] : stealthwatchfe@dcloud.local

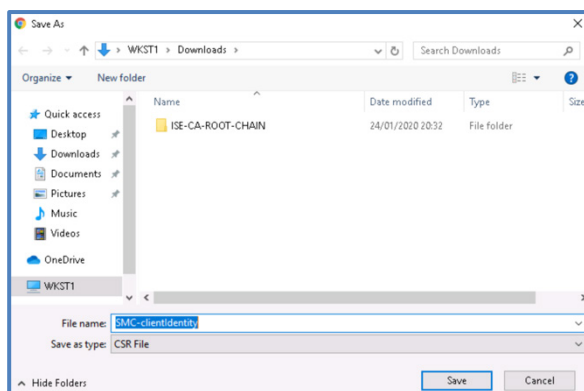
- iv. [CSR の生成 (Generate CSR)] をクリックします。



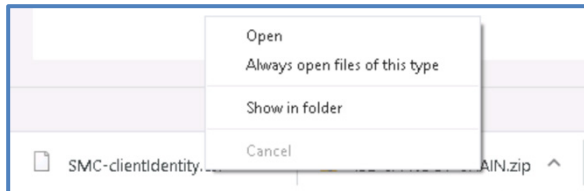
- v. [CSR のダウンロード (Download CSR)] をクリックします。



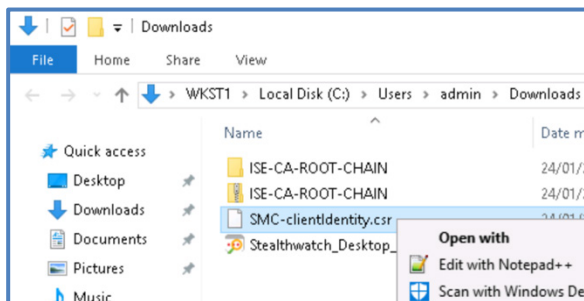
- vi. [名前を付けて保存 (Save As)] ポップアップで [保存 (Save)] をクリックします。



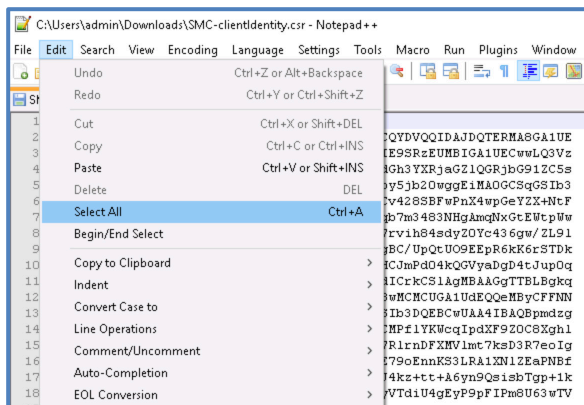
- vii. Chrome の下部にある SMC-clientidentity.csr ファイルを右クリックし、[フォルダを開く (Show in folder)] オプションをクリックします。



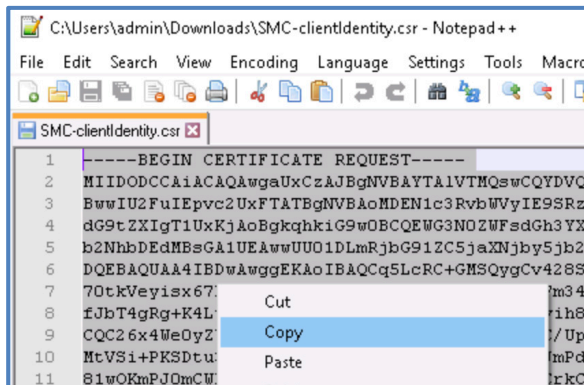
- viii. **SMC-clientidentity.csr** ファイルを右クリックし、[Notepad++で編集 (Edit with Notepad++)] を選択します。



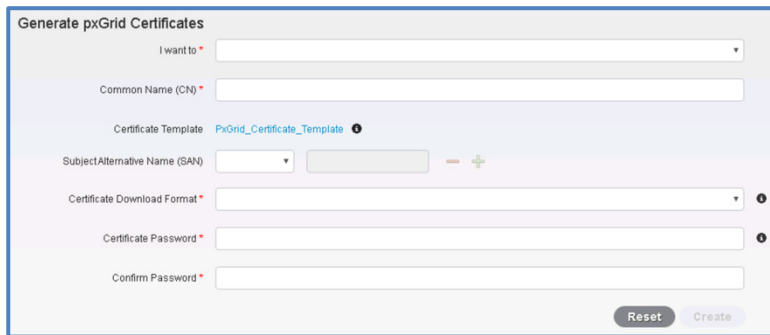
- ix. Notepad++ で [編集 (Edit)] をクリックし、[すべて選択 (Select All)] をクリックします。



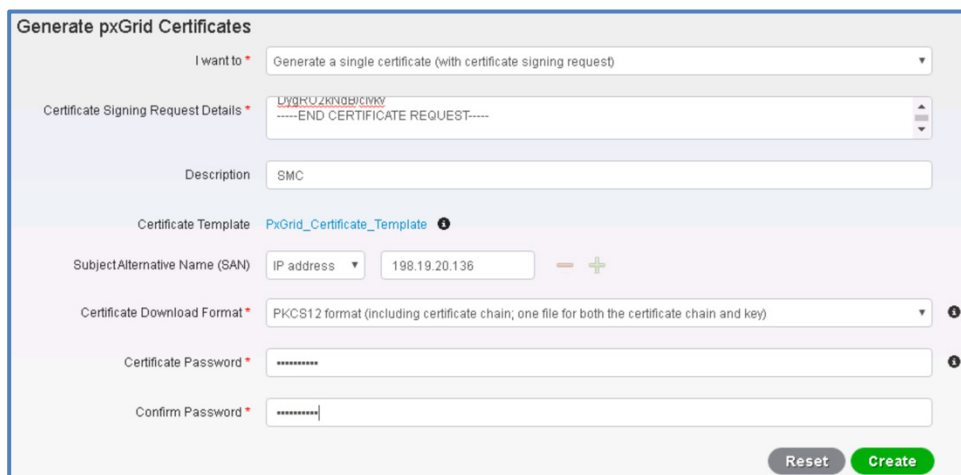
- x. 強調表示されたテキストを右クリックし、[コピー (Copy)] を選択します。



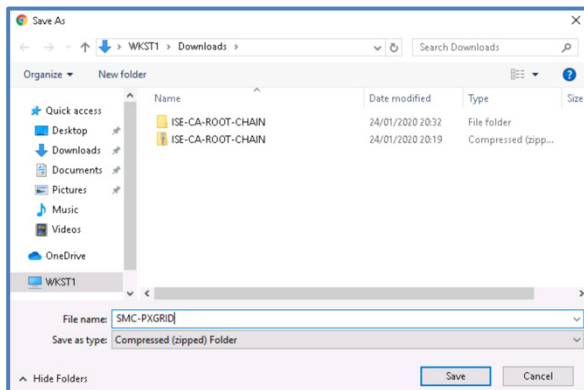
- xi. Identity Services Engine の Chrome ブラウザタブに戻ります。
- e. [リセット (Reset)]をクリックしてフォームをクリアします。



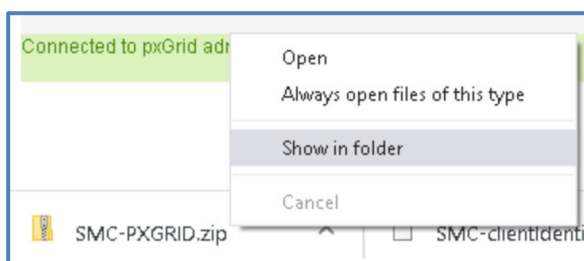
- i. [pxGrid 証明書の生成 (Generate pxGrid Certificates)] フォームに次のように入力します。
 1. [処理の選択 (I want to)] フィールドで、[単一の証明書の生成 (証明書署名要求あり) (Generate a single certificate (with certificate signing request))] を選択します。
 2. [証明書署名要求の詳細 (Certificate Signing Request Details)] フィールドで右クリックし、[貼り付け (Paste)] をクリックします。これにより、Notepad++ で取得した証明書情報が貼り付けられます。
 3. [説明 (Description)] フィールドに **SMC** と入力します。
 4. [SAN] フィールドで [IP アドレス (IP Address)] を選択し、関連する IP アドレスとして **198.19.20.136** を入力します。
 5. [証明書のダウンロード形式 (Certificate Download Format)] オプションとして [PKCS12 形式 (PKCS12 format)] を選択します。
 6. 両方のパスワードフィールドに **C1sco12345** を入力します。
 7. [作成 (Create)] をクリックします。



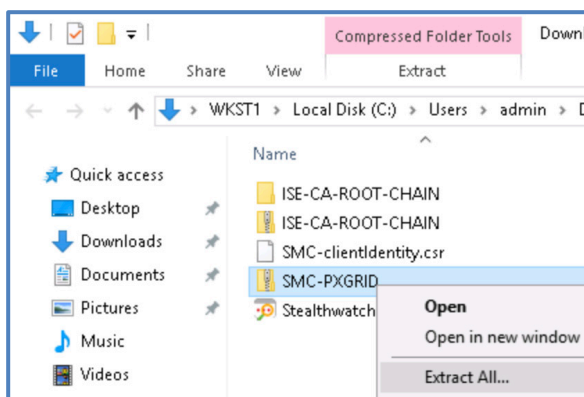
- ii. ファイル名を **SMC-PXGRID** に設定し、[保存 (Save)] をクリックします。



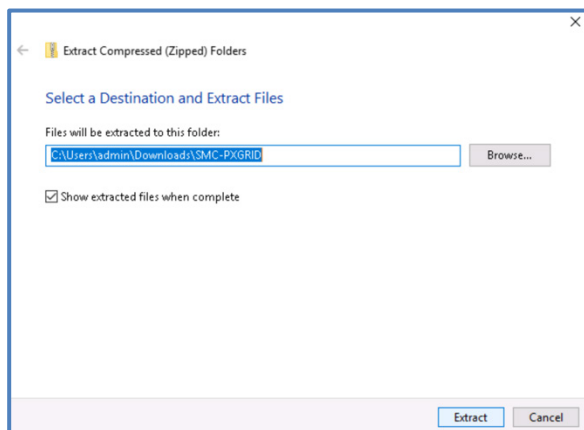
iii. Chrome の下部にある **SMC-PXGRID.zip** ファイルを右クリックし、[フォルダを開く (Show in folder)] をクリックします。



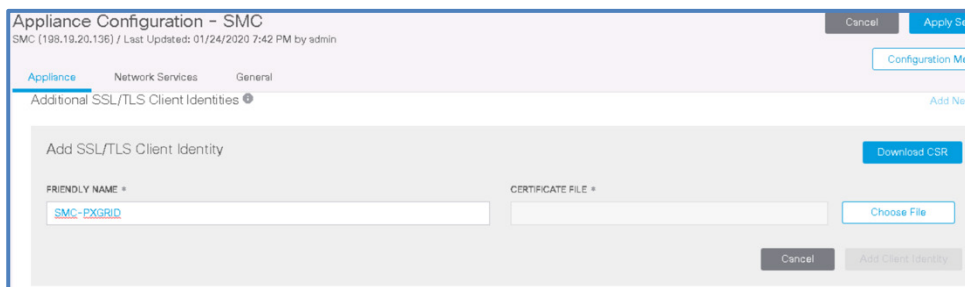
iv. **SMC-PXGRID.zip** ファイルを右クリックし、[すべて展開 (Extract All...)] を選択します。



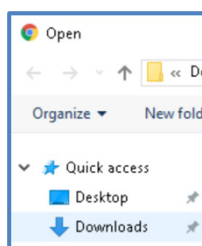
v. [展開 (Extract)] をクリックします。



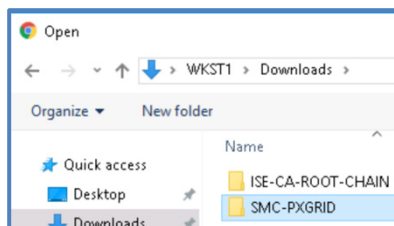
- vi. 開いているすべてのファイルブラウザのウィンドウを閉じ、Chrome は開いたままにします。
- f. Chrome の [SMC アプライアンス設定 (SMC Appliance Configuration)] タブに戻り、[SSL/TLS クライアントアイデンティティの追加 (Add SSL/TLS Client Identity)] フォームの [フレンドリ名 (Friendly Name)] に **SMC-PXGRID** を入力し、[ファイルの選択 (Choose File)] をクリックします。



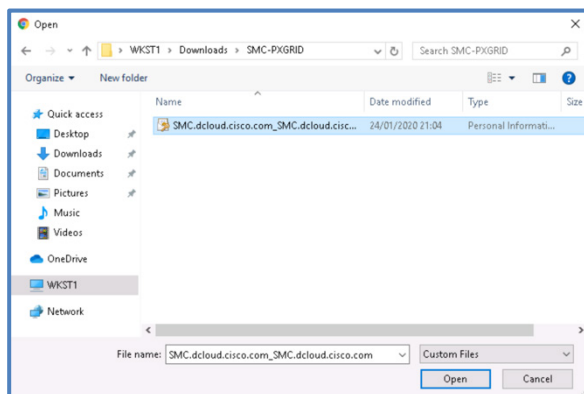
- i. 表示された [開く (Open)] ページの左側にある [ダウンロード (Downloads)] をクリックします。



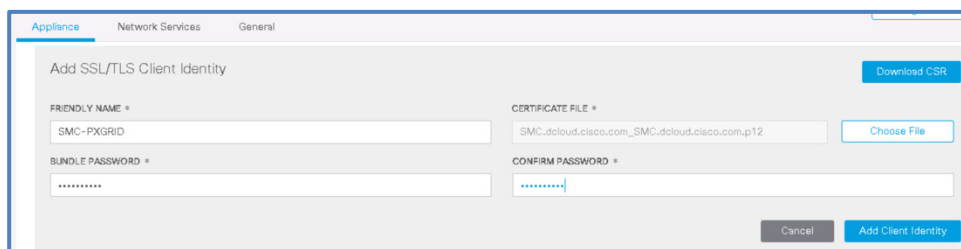
- ii. **SMC-PXGRID** フォルダをダブルクリックします。



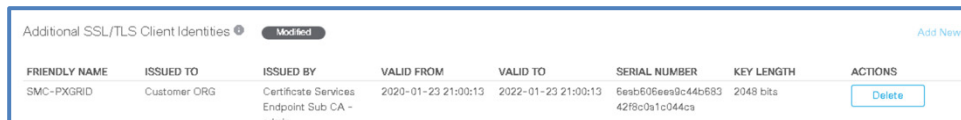
- iii. **SMC.dcloud.cisco.com...** ファイルをクリックし、[開く (Open)] をクリックします。



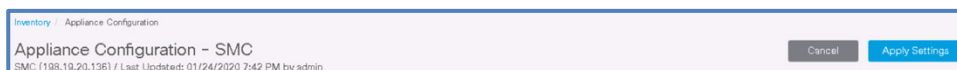
- iv. [バンドルパスワード (Bundle Password)] と [パスワードの確認 (Confirm Password)] フィールドの両方に **C1sco12345** を入力します。
- v. [クライアントアイデンティティの追加 (Add Client Identity)] をクリックします。



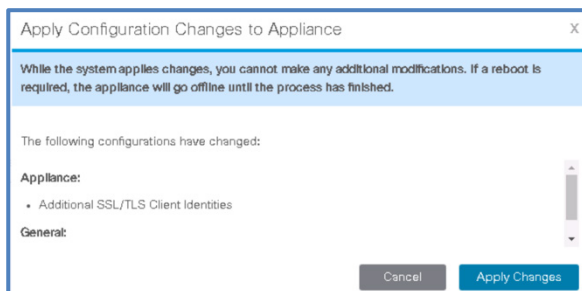
- vi. **SMC-PXGRID** のクライアント証明書が表示されます。



- g. [設定の適用 (Apply Settings)] をクリックします。



- h. [変更の適用 (Apply Changes)] をクリックします。

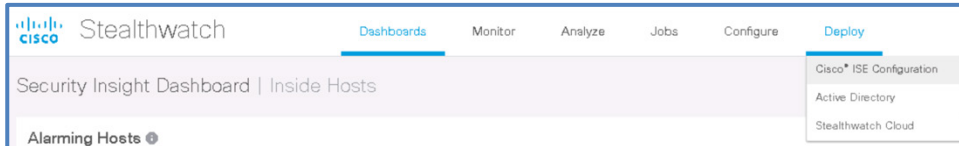


- 9. SMC の [アプライアンスステータス (Appliance Status)] が [設定変更の保留 (Config Changes Pending)] から [Up] になるまで、[インベントリ (Inventory)] ページで待機します。必要に応じてページを更新し、ステータスを確認します。

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	90 Days or Less	SMC	SMC SMC/E-VMware- 42383d58599a3d2- df3b6293c95d4d00	198.19.20.136	

10. Chrome ブラウザで **SMC Web UI** に戻ります (必要に応じて新しいタブを開き、SMC のブックマークをクリックします)。

11. [導入 (Deploy)] をクリックし、[Cisco ISE 設定 (Cisco ISE Configuration)] を選択します。

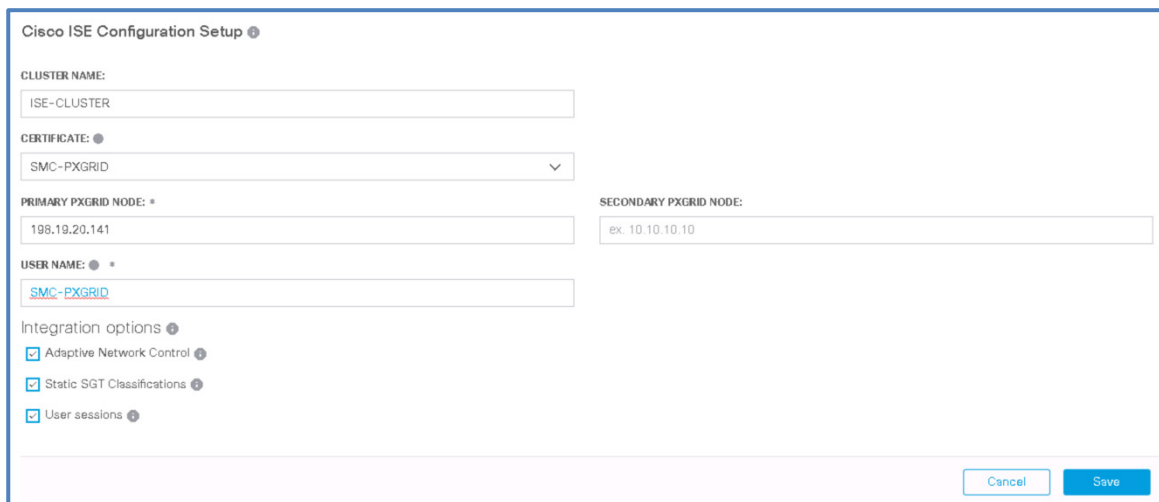


a. [Cisco ISE 設定 (Cisco ISE Configuration)] ページで [新しい設定の追加 (Add new configuration)] をクリックします。

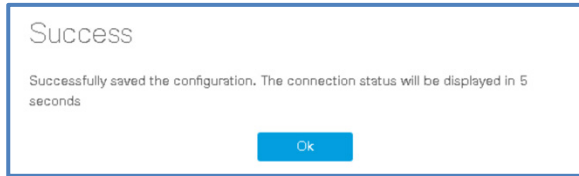


b. ISE 設定フォームで次のように設定します。

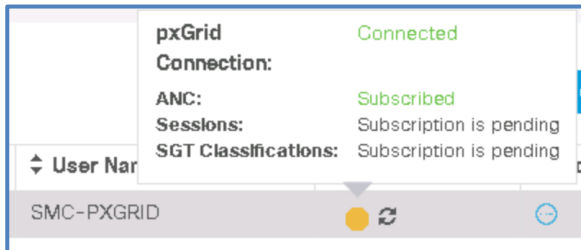
- i. [クラスタ名 (Cluster Name)] : **ISE-CLUSTER**
- ii. [証明書 (Certificate)] : **SMC-PXGRID**
- iii. [プライマリ PxGrid ノード (Primary PxGrid Node)] : **198.19.20.141**
- iv. [ユーザ名 (User Name)] : **SMC-PXGRID**
- v. 3つの [統合オプション (Integration options)] のチェックボックスをすべてオンにします。
- vi. [保存 (Save)] をクリックします。



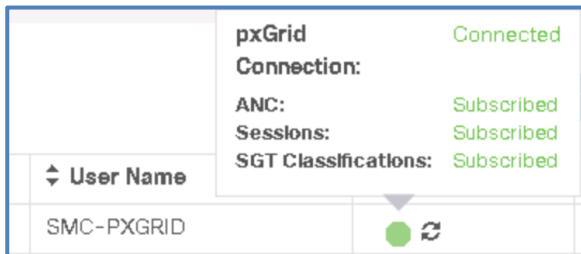
- c. 成功のメッセージが表示されます。[OK] をクリックします。



12. ISE-CLUSTER の円形のステータスアイコンをクリックして、接続を検証します。まだ接続されていない場合や、一部接続されていない場合があります。円形のステータスアイコンの隣にある更新アイコンをクリックして、ステータスを更新します。



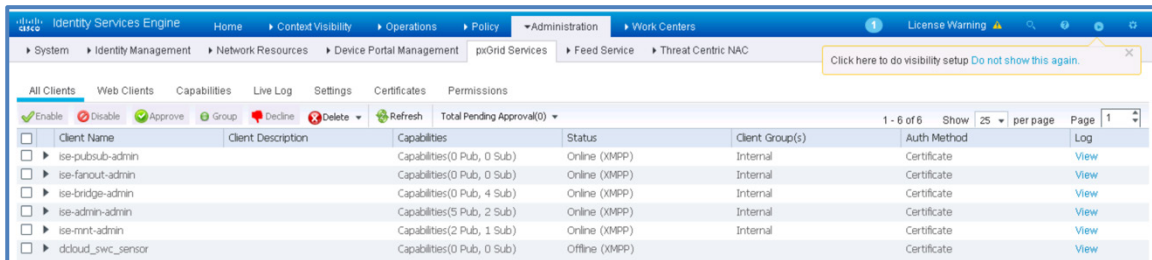
13. すべてのエントリについて [接続済み (Connected)] および [登録済み (Subscribed)] と表示されるまで、ステータスの確認を続行します。円形のステータスアイコンの隣にある更新アイコンをクリックして、ステータスを更新します。



注： dCloud ラボ環境では、ISE アクティビティのシミュレーションとともに、単一のライブ ISE ノードも実行します。シミュレーションされたシステムは、ユーザ情報（ログイン/ログアウトイベント）を 1 日を通して特定のポイントにプッシュします。

14. Chrome の ISE タブに戻ります。

15. [すべてのクライアント (All Clients)] をクリックします。



16. [更新 (Refresh)] ボタンをクリックします。



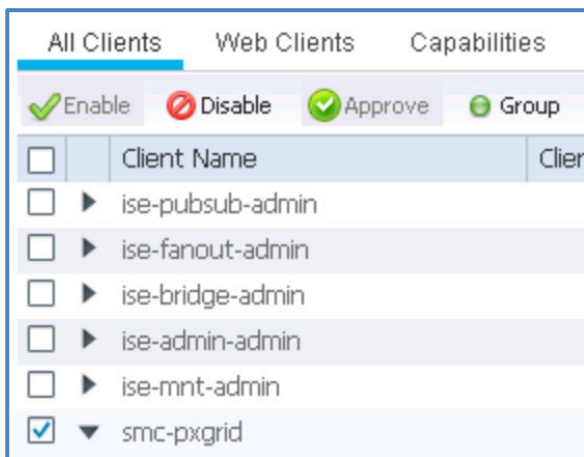
17. [smc-pxgrid] エントリを展開して、機能を確認します。



Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
ise-pubsub-admin		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-admin		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-admin		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-admin		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
ise-mnt-admin		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
smc-pxgrid		Capabilities(0 Pub, 4 Sub)	Online (XMPP)		Certificate

Capability Name	Capability Version	Messaging Role	Message Filter
AdaptiveNetworkControl	1.0	Sub	
Core	1.0	Sub	
SessionDirectory	1.0	Sub	
TrustSecMetaData	1.0	Sub	

18. [smc-pxgrid] の前のチェックボックスをクリックし、[グループ (Group)] ボタンをクリックします。



Client Name	Client Description	Client
ise-pubsub-admin		
ise-fanout-admin		
ise-bridge-admin		
ise-admin-admin		
ise-mnt-admin		
<input checked="" type="checkbox"/> smc-pxgrid		

19. [グループ (Group)] フィールドをクリックして [セッション (Session)] を選択した後、フィールドを再度クリックして [ANC] を選択し、[保存 (Save)] をクリックします。



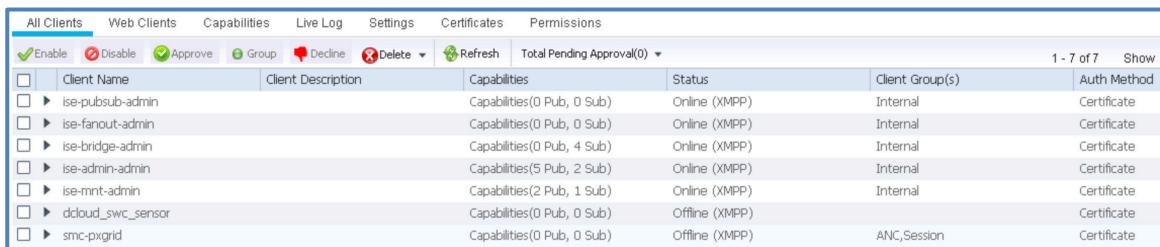
Client Group

Name: smc-pxgrid

Groups: Session ANC

Save Cancel

20. smc-pxgrid 回線に紐付けられた ANC および Session のクライアントグループが表示されます。



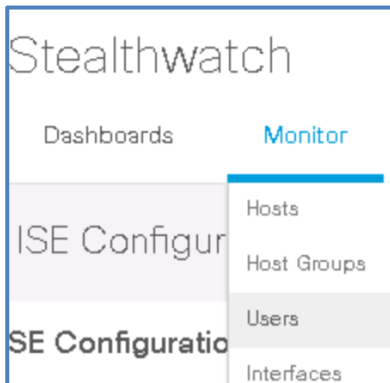
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
ise-pubsub-admin		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-admin		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-admin		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-admin		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
ise-mnt-admin		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
dcloud_sw_c_sensor		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
smc-pxgrid		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	ANC,Session	Certificate

21. Chrome の ISE タブを閉じます。

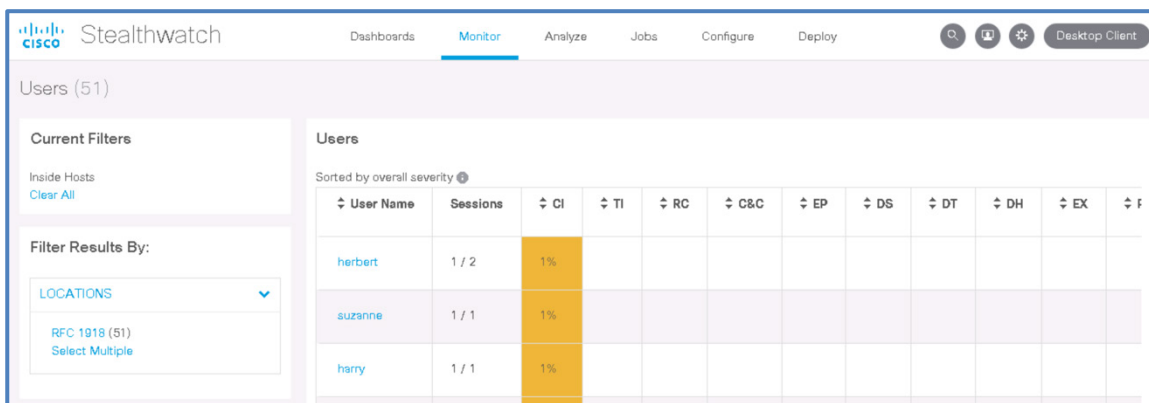
22. Chrome の下部にあるダウンロードバーを、右端にある [X] をクリックして閉じます。

23. Chrome の **SMC Web UI** に戻ります。

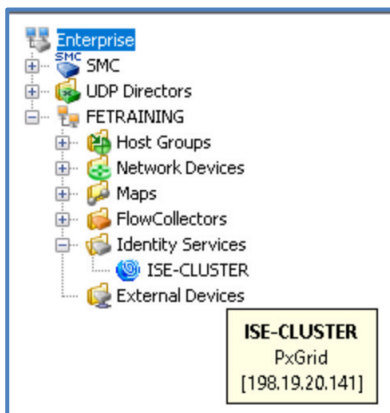
24. [モニタ (Monitor)] > [ユーザ (Users)] の順にクリックします。



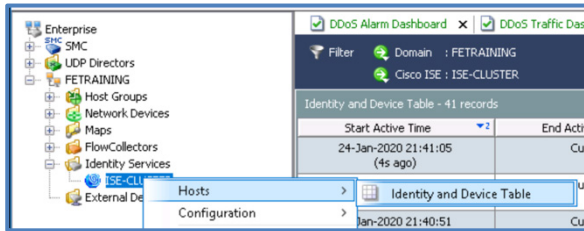
25. インターフェイス内にユーザデータが表示されます。左上隅のユーザ数を確認します。また、関連するカテゴリインデックス情報とともにユーザが表示される表にも注目してください。ユーザデータがまだ表示されていない場合は、必要な接続がまだ発生していない可能性があります。しばらく待つか、先に残りのラボを進めたい場合は後で確認してください。



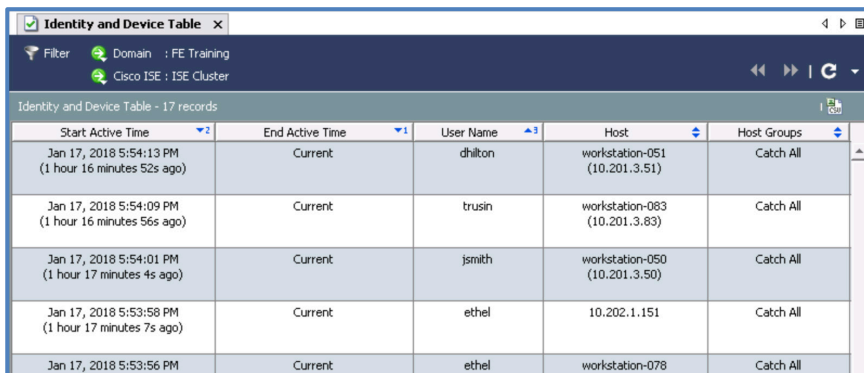
26. Stealthwatch デスクトップクライアントでユーザデータを確認することもできます。デスクトップクライアント インターフェイスに戻り、[FETRAINING] ドメインの下にある [アイデンティティサービス (Identity Services)] フォルダを展開します。Web UI で追加した [ISE-CLUSTER] が表示されます。ISE クラスタの上にマウスを置くと、接続が PxGrid 経由であることが示されます。



27. アクティブユーザを表示するには、[ISE-CLUSTER] オブジェクトを**ダブルクリック**するか、[ISE-CLUSTER] オブジェクトを**右クリック**して [ホスト (Hosts)] メニューをクリックし、[アイデンティティおよびデバイステーブル (Identity and Device Table)] オプションを選択します。



28. SMC インターフェイスの右ペインに、[アイデンティティおよびデバイステーブル (Identity and Device Table)] ドキュメントが、複数のユーザ アイデンティティ レコードとともに表示されます。



Start Active Time	End Active Time	User Name	Host	Host Groups
Jan 17, 2018 5:54:13 PM (1 hour 16 minutes 52s ago)	Current	dhilton	workstation-051 (10.201.3.51)	Catch All
Jan 17, 2018 5:54:09 PM (1 hour 16 minutes 56s ago)	Current	trusin	workstation-083 (10.201.3.83)	Catch All
Jan 17, 2018 5:54:01 PM (1 hour 17 minutes 4s ago)	Current	jsmith	workstation-050 (10.201.3.50)	Catch All
Jan 17, 2018 5:53:58 PM (1 hour 17 minutes 7s ago)	Current	ethel	10.202.1.151	Catch All
Jan 17, 2018 5:53:56 PM	Current	ethel	workstation-078	Catch All

29. pxGrid 経由で Cisco ISE の統合を設定し、アイデンティティデータが ISE から SMC に正しく送信されることを確認しました。

シナリオのまとめ

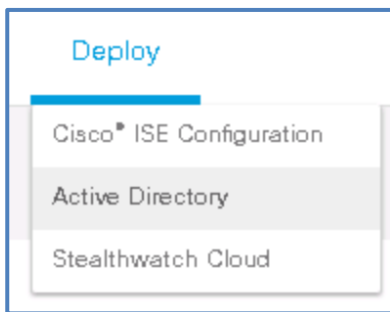
このシナリオでは、Stealthwatch と Cisco ISE の統合を設定し、その機能を検証しました。

シナリオ 13. AD LDAP ルックアップ機能の設定

ここまでで、お客様の Cisco ISE 導入を Stealthwatch に統合し、ユーザ アイデンティティ データを取得して、フローデータと関連付けることができるようになりました。お客様は Active Directory を使用していて、Stealthwatch でアイデンティティデータにアクセスしたときに追加のユーザ情報を得るために、ディレクトリに対してクエリができることを求めています。ここでは、AD ルックアップ機能の設定を行います。

注： Cisco ISE は、ユーザ アイデンティティ データを取得する方法の 1 つです。お客様の設定によっては、Cisco ASA ファイアウォール（および特定のベンダー製ファイアウォール）で、Cisco ISE とは別個に Stealthwatch にユーザ アイデンティティ データを提供できます。お客様に ISE がなくても、別の送信元からユーザ アイデンティティ データを取得している場合があります。AD ルックアップ機能が役立ちます。ただし AD ルックアップ機能では、Cisco ISE や ASA など他の送信元からすでに Stealthwatch が取得しているユーザ アイデンティティ データのユーザ詳細だけが得られます。AD ルックアップ機能自体がデータを提供することはなく、すでに Stealthwatch にあるユーザ アイデンティティ データを利用しなければなりません。

1. Chrome ブラウザの SMC Web UI に戻るか、Chrome Web ブラウザウィンドウの **SMC** ブックマークを選択します。**admin** ユーザとして、パスワード **C1sco12345** でログインしていることを確認します。
2. [導入 (Deploy)] メニューをクリックし、[Active Directory] メニュー項目を選択します。



3. [新しい設定の追加 (Add new configuration)] をクリックします。



4. 以下に示す値を使用して設定を完了し、[保存 (Save)] ボタンをクリックします。
 - a. [名前 (Name)] : **Customer AD Environment**
 - i. 接続する AD インスタンスについて定義された名前。これは実際の AD DNS または NT ドメイン名には関連しません。
 - b. [説明 (Description)] : **Customer AD Instance 01**
 - i. 環境に関する任意の説明。お客様は複数の AD 環境を使用している場合があります。ここでそれらを差別化できます。
 - c. [ホスト (Host)] : **198.19.20.10**
 - i. 接続先の AD サーバの FQDN または IP アドレス
 - d. [ポート (Port)] : **389**

- i. 接続するポート番号。セキュアでない LDAP ではポート 389 を使用します。それにより、ネットワーク上でセキュアでない状態でデータを引き出していたユーザ名とパスワードが送信されます。お客様の AD サーバに証明書がインストールされていない場合は、ポート 389 のセキュアでない LDAP が唯一のオプションになります。ただし、AD サーバでセキュアな LDAP (LDAPS) がサポートされている場合は、ポート番号 636 を使用するのがベストプラクティスになります。
- e. [SSL]: **オフ**
- i. ポート 389 がセキュアでない LDAP で使用されている場合は、このオプションをオフにします。証明書がインストールされているドメインコントローラとの接続にポート 636 が使用されている場合は、ボックスにチェックマークを入れます。
- f. [ベース DN (Base DN)]: **CN=Users,DC=dcloud,DC=local**
- i. お客様のディレクトリ内でユーザデータの検索を開始するレベルでの、DN (識別名) の LDAP パス。この設定にどのような値を指定しても、この DN 以下にあるユーザデータが取得されます。
 - ii. 例: ユーザアカウントの DN が「CN=BobRoss,OU=CorpLearning,DC=dcloud,DC=local」で、ベース DN 設定の値が「OU=Sales,DC=dcloud,DC=local」の場合、BobRoss ユーザはクエリ対象のパスには入らず、結果は返されません。
 - iii. ただし、ベース DN の値が「DC=dcloud,DC=local」の場合は、BobRoss ユーザのパスがベース DN パスの子オブジェクトになるため、BobRoss ユーザが返されます。
 - iv. LDAP パスでは大文字と小文字は区別されます。実稼働環境に機能を導入する前に、有効な設定をお客様から取得してください。
- g. [バインド DN (Bind DN)]: **CN=sw-ldap,CN=Users,DC=dcloud,DC=local**
- i. バインド DN の値は、Stealthwatch がお客様の AD インスタンスで認証し、ユーザデータを取得するために使用する、ユーザアカウントの DN です。これは、管理アクセス権を持つユーザである必要はありません。通常の「ドメインユーザ」グループの権限で、デフォルトの権限を持つ AD 構造にアクセスできます。お客様が OU 構造の権限をカスタマイズしている場合、ユーザアカウントにはユーザ属性の読み取り権限だけが必要になります。
- h. [パスワード (Password)]: **C1sco12345**
- i. [バインド DN (Bind DN)] 設定で指定されているユーザアカウントのパスワード
- i. [保存 (Save)] をクリックします。

Active Directory: Customer AD Environment

NAME *

Customer AD Environment

DESCRIPTION (OPTIONAL) (200 CHAR MAX)

Customer AD Instance 01

HOST *

198.19.20.10

PORT *

389

SSL (Optional)

BASE DN *

CN=Users,DC=dcloud,DC=local

BIND DN *

CN=sw-ldap,CN=Users,DC=dcloud,DC=local

PASSWORD *

Cancel Save

5. 接続を確立できた場合は確認メッセージが表示されます。[OK] をクリックします。

Confirmed

Your AD connection has been established and confirmed.

OK

6. 保存された AD ルックアップ設定インスタンスが画面に表示されます。

注：複数の設定エントリを指定することが可能です。これは、お客様環境に複数の LDAP ディレクトリまたは複数の AD ドメインがある場合、あるいは同じディレクトリ内で複数のベース DN パスを指定する場合に必要になります。

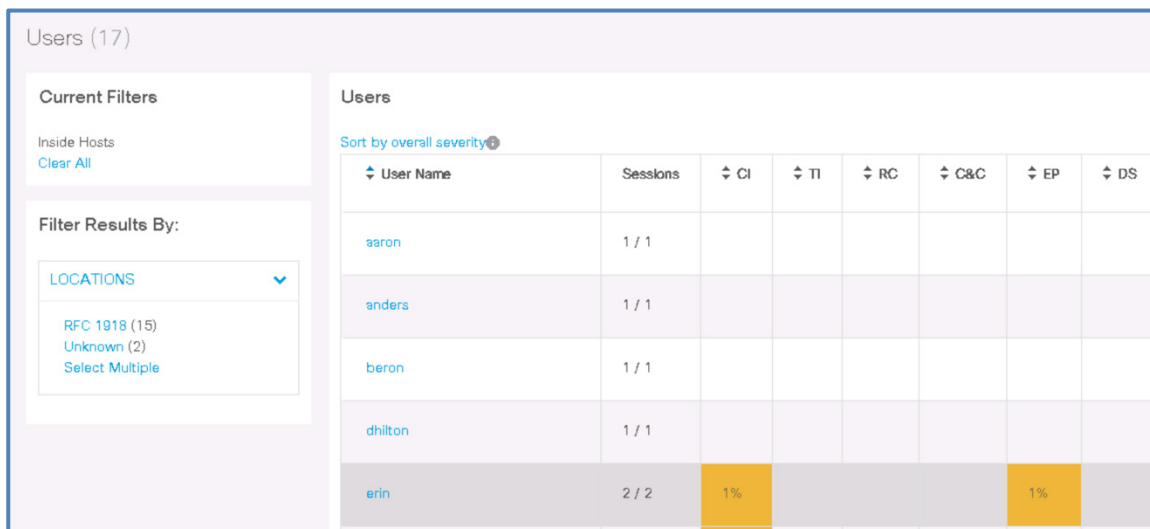
Active Directory

Active Directory Lookup Configuration

Add new configuration

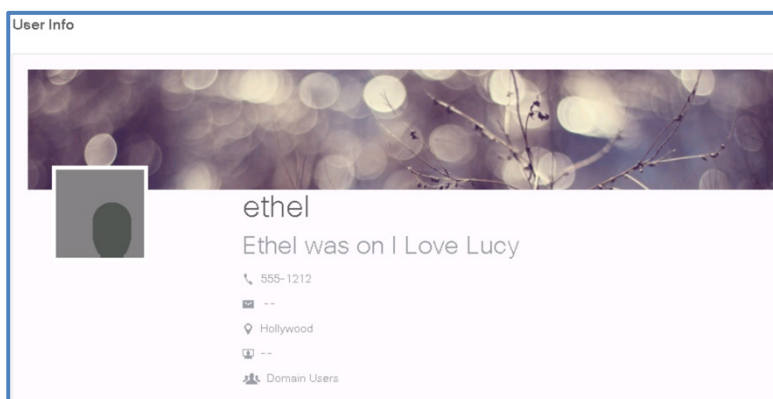
Lookup	Name	Description	Order	Actions
1	Customer AD Environment	Customer AD Instance 01		

7. 次に、Stealthwatch がお客様の AD 環境からデータを正しく引き出していることを確認します。Stealthwatch の Web インターフェイスで、[モニタ (Monitor)]メニューをクリックし、[ユーザ (Users)]メニュー項目を選択します。



↓ User Name	Sessions	↕ CI	↕ TI	↕ RC	↕ C&C	↕ EP	↕ DS
aaron	1 / 1						
anders	1 / 1						
beron	1 / 1						
dhilton	1 / 1						
erin	2 / 2	1%				1%	

8. [ユーザ名 (User Name)] 列のヘッダーにある上下の三角形をクリックして、[ユーザ (Users)] ページを [ユーザ名 (User Name)] 列でソートします。
9. [ユーザ (Users)] ページを下にスクロールして、ユーザ ethel のエントリを探して、ethel ユーザのリンクをクリックします。または、URL <https://198.19.20.136/lc-landing-page/smc.html#/userentity/ethel> を入力することもできます。
10. [ユーザ情報 (User Info)] ページに、Ethel の Active Directory の詳細、Stealthwatch からの Ethel のアラームデータ、Ethel が認証を受けたデバイスのリストが表示されます。



11. これで AD ルックアップ機能を設定し、お客様が Stealthwatch に表示されるユーザデータについてディレクトリにクエリを実行できるようになりました。

シナリオのまとめ

このシナリオでは、お客様が、Stealthwatch にユーザ名情報を提供する Cisco ISE、または他の統合を通じてインポートされたアイデンティティデータに含まれるユーザアカウントに関する詳細を収集できるように、AD ルックアップ機能を設定しました。

シナリオ 14. カスタムドキュメントの作成

フローデータがお客様環境内で適切に分類されたら、さらなるカスタマイズとレポートに着手できます。製品内には、組み込みのドキュメントやレポートが多数用意されています。ほとんどの場合、これらを使用してお客様の目標を達成できます。ただし、場合によってはソリューションをカスタマイズする必要があります。お客様は、NOC 用のダッシュボードのカスタマイズを開始するにあたって支援を求めています。

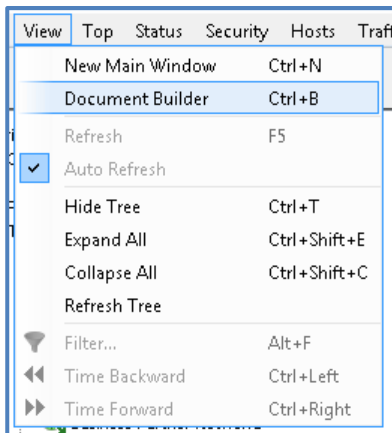
カスタムドキュメントの作成

お客様から、インターネットトラフィック使用状況のデータを表示するデスクトップクライアントのダッシュボードを作成するよう依頼を受けました。具体的には、複数のドキュメントを開かなくても SMC で 1 つのドキュメントを開くだけで必要なデータを取得できるようなものを求められています。お客様の依頼に応えるため、カスタムドキュメントビルダーを使用して、複数のコンポーネントが含まれる単一のドキュメントを作成します。

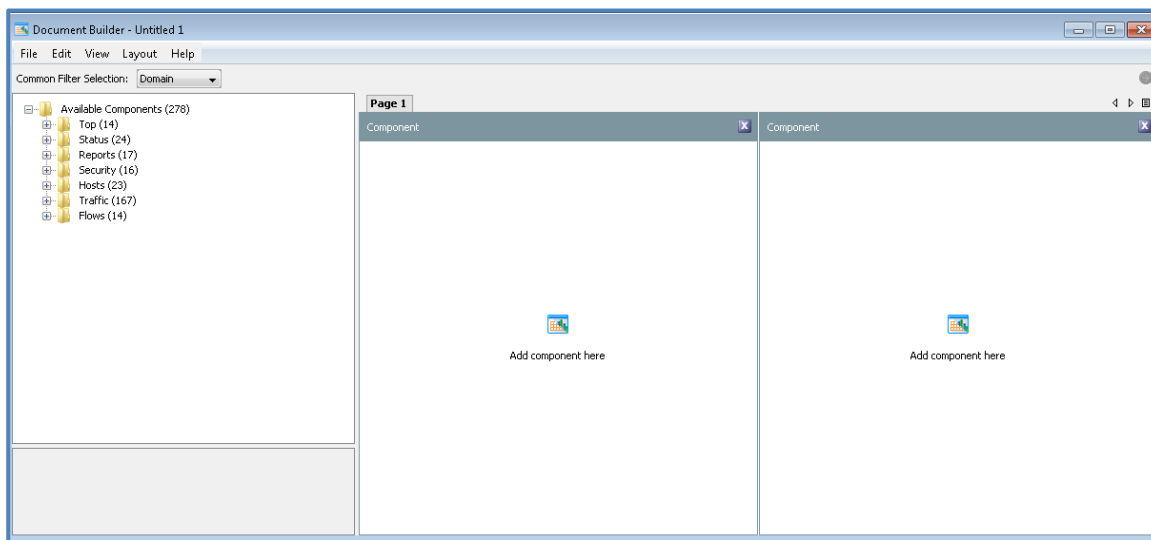
1. **Stealthwatch** デスクトップクライアントを開きます。



2. [表示 (View)] メニューをクリックし、[ドキュメントビルダー (Document Builder)] メニュー項目を選択します。

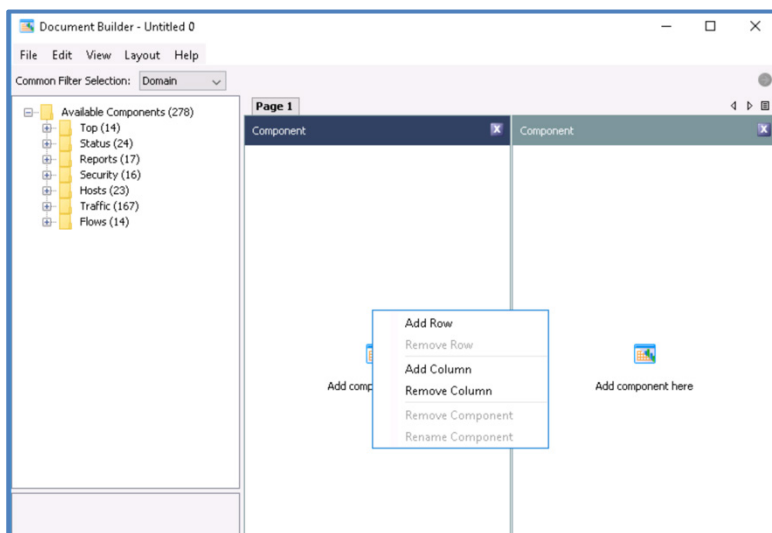


3. ドキュメントビルダーのウィンドウが開き、ドキュメントに追加できる利用可能なコンポーネントがすべて表示されます。

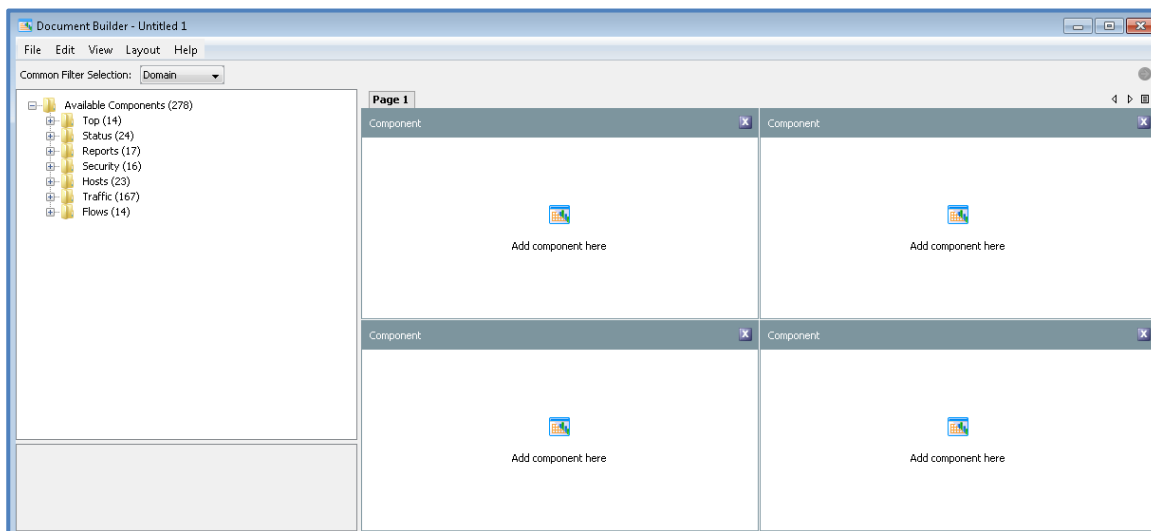


注：利用可能なコンポーネントはすべて、SMC にすでに存在する各種の事前作成済みドキュメントからのオプションです。ドキュメントビルダーでできるのは、単に既存のタイプの複数のコンポーネント/ドキュメントを1つのドキュメントに結合することです。

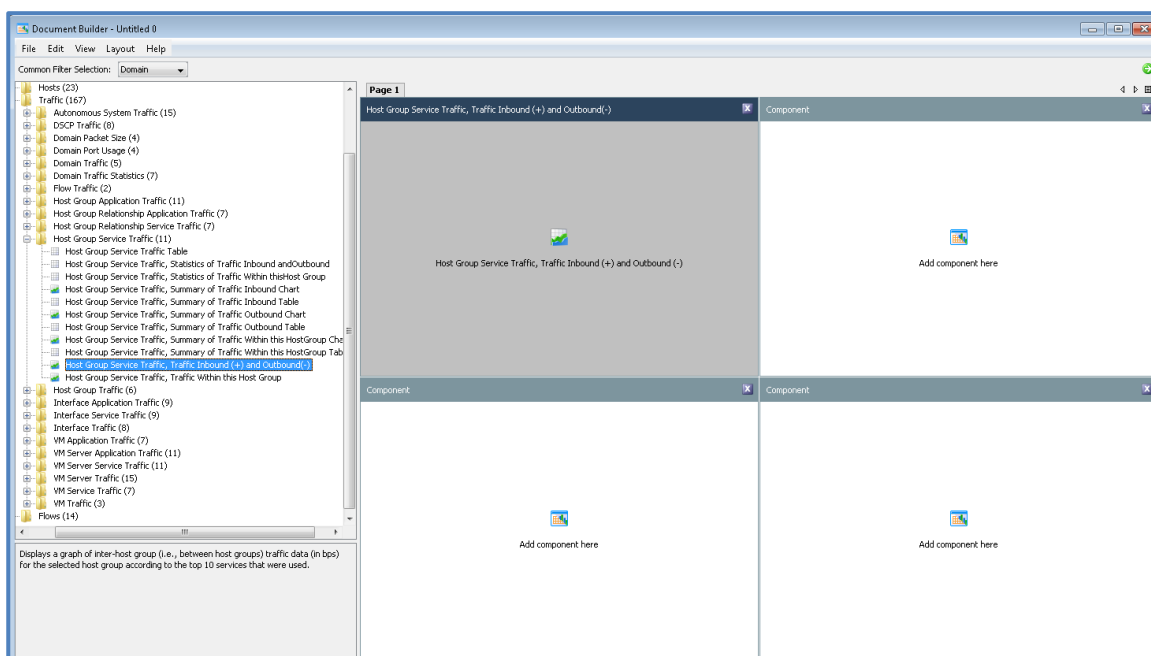
4. 左のコンポーネントウィンドウ（ドキュメントビルダーの中央）を右クリックして、[行の追加（Add Row）] オプションを選択します。



5. 右のコンポーネントウィンドウを右クリックして、[行の追加（Add Row）] オプションを選択します。最終的に下の画像のように表示されます。

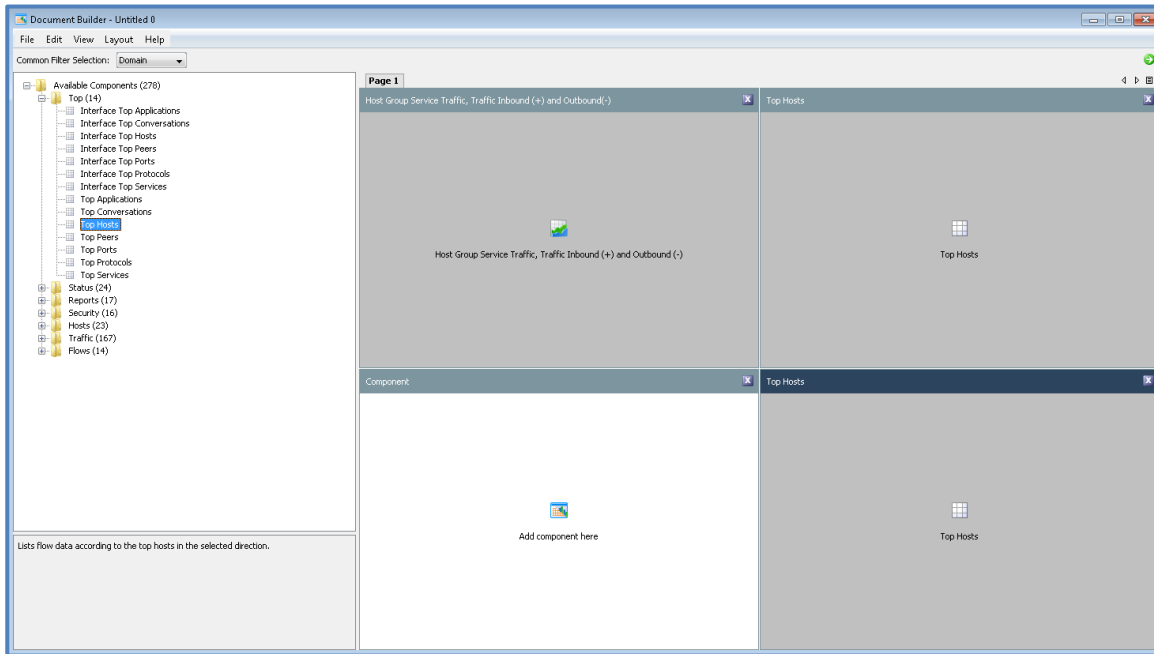


6. ウィンドウの左側にある [利用可能なコンポーネント (Available Component)] ツリーを展開し、[トラフィック (Traffic)] フォルダから [ホストグループサービストラフィック (Host Group Service Traffic)] フォルダを展開し、[ホストグループサービストラフィック、着信トラフィック (+) と発信トラフィック (-) (Host Group Service Traffic, Traffic Inbound (+) and Outbound (-))] コンポーネントを選択して、そのコンポーネントを左上のコンポーネントウィンドウにドラッグします。

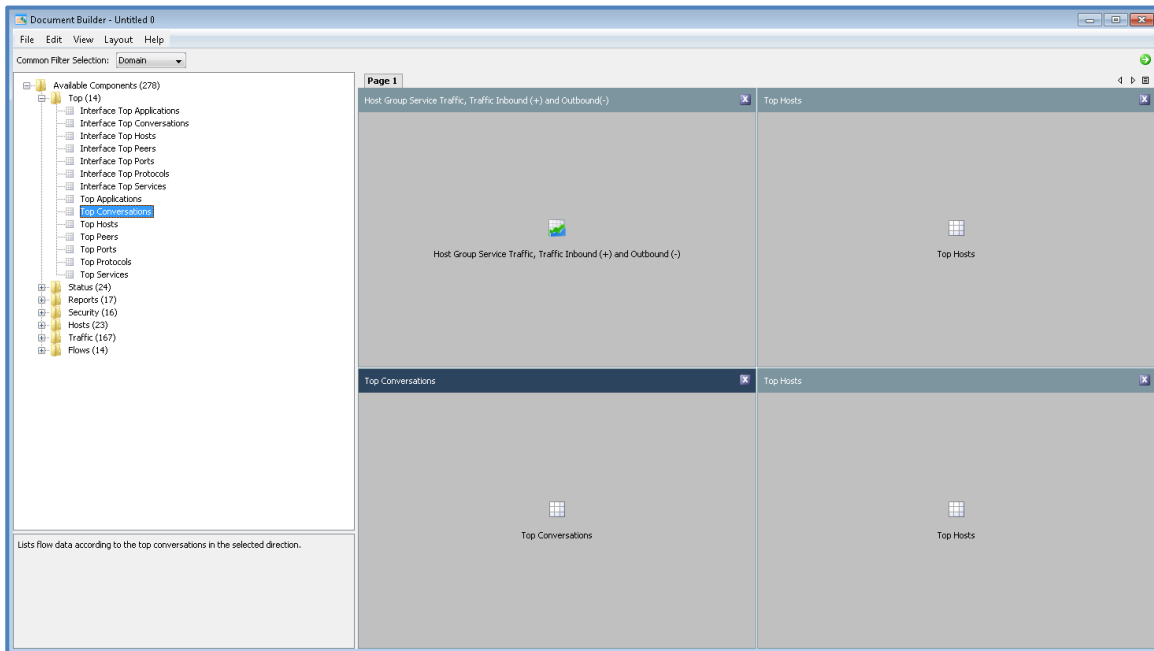


7. ウィンドウの左側にある [利用可能なコンポーネント (Available Component)] ツリーを展開し、[上位 (Top)] フォルダを展開し、[上位ホスト (Top Hosts)] コンポーネントを選択して、そのコンポーネントを右上のコンポーネントウィンドウにドラッグします。

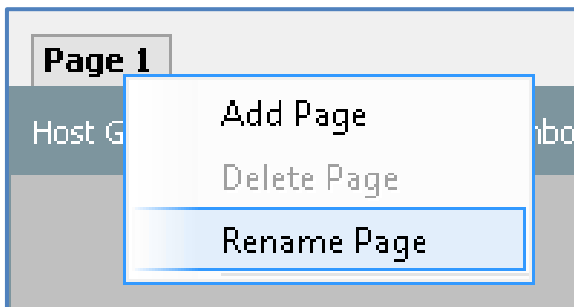
8. ウィンドウの左側にある [利用可能なコンポーネント (Available Component)] ツリーを展開し、[上位 (Top)] フォルダを展開し、[上位ホスト (Top Hosts)] コンポーネントを選択して、そのコンポーネントを右下のコンポーネントウィンドウにドラッグします。



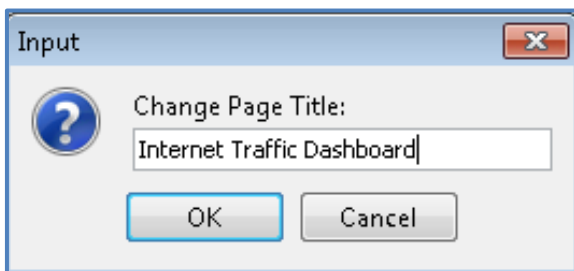
9. ウィンドウの左側にある [利用可能なコンポーネント (Available Component)] ツリーを展開し、[上位 (Top)] フォルダを展開し、[上位カンバセーション (Top Conversations)] コンポーネントを選択して、そのコンポーネントを左下のコンポーネントウィンドウにドラッグします。



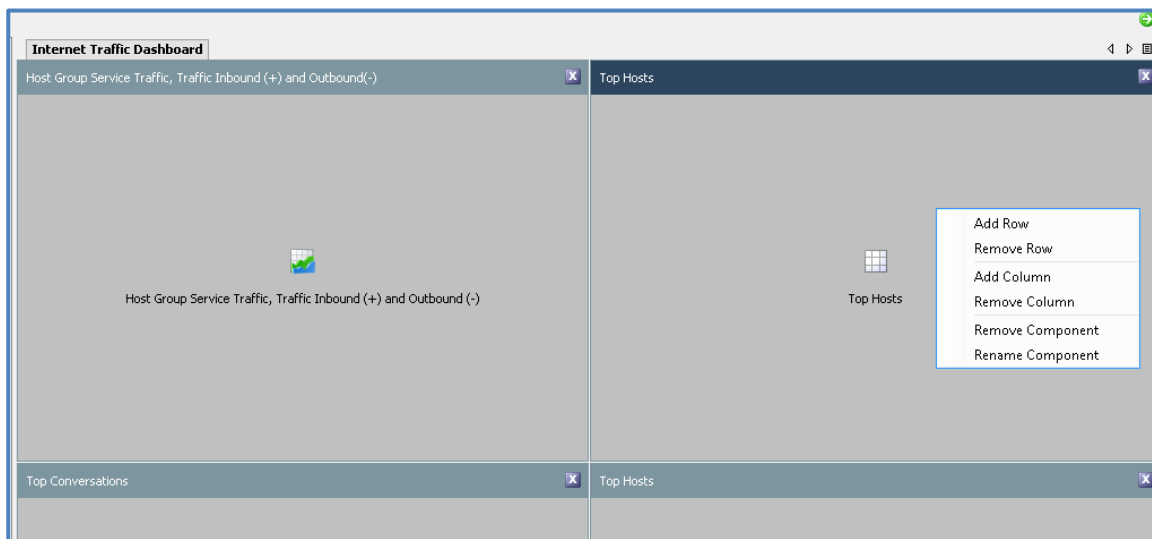
10. 画面上部の [ページ 1 (Page 1)] ヘッダータブを右クリックし、[ページ名の変更 (Rename Page)] メニュー項目を選択します。



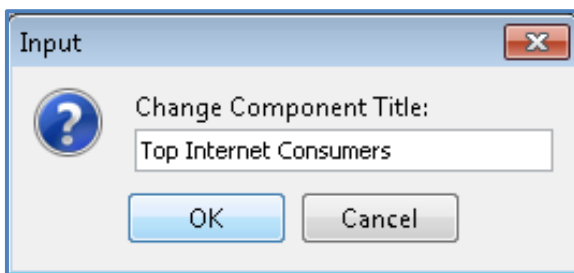
11. ページ名を **Internet Traffic Dashboard** に変更して [OK] をクリックします。



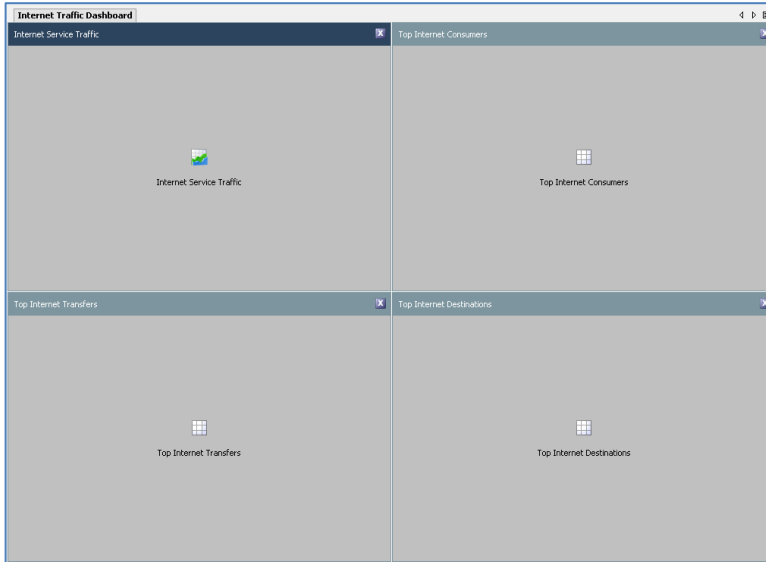
12. 右上の [上位ホスト (Top Hosts)] コンポーネントを右クリックし、[コンポーネント名の変更 (Rename Component)] オプションを選択します。



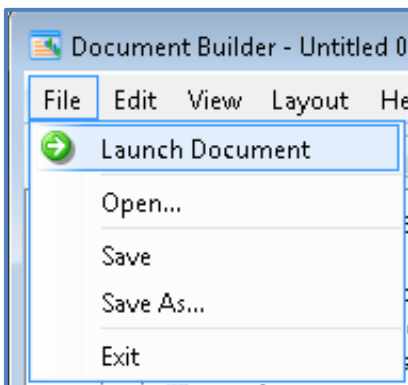
13. コンポーネントのタイトルを **Top Internet Consumers** に変更して [OK] をクリックします。



14. 右下の [上位ホスト (Top Hosts)] コンポーネントの名前を **Top Internet Destinations** に変更します。
15. 左下の [上位カンバセーション (Top Conversations)] コンポーネントの名前を **Top Internet Transfers** に変更します。
16. 左上の [ホストグループサービストラフィック (Host Group Service Traffic)] コンポーネントの名前を **Internet Service Traffic** に変更します。



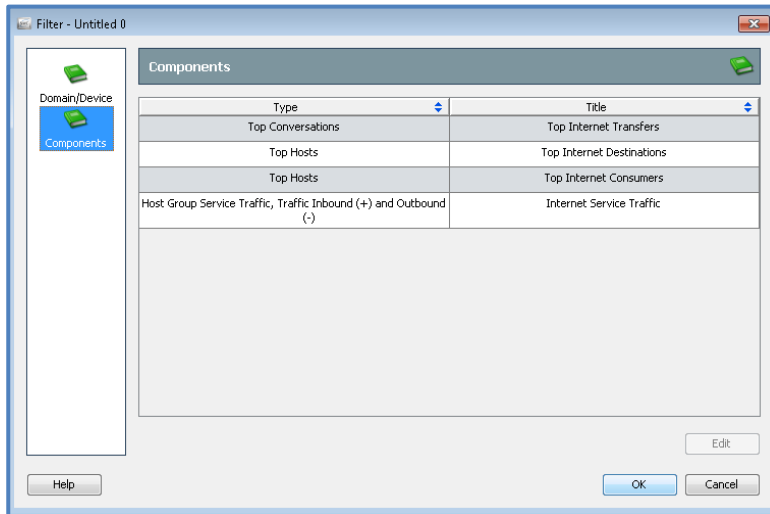
17. ドキュメントのフォーマットが完成しました。次に、SMC デスクトップクライアントでテンプレートを起動して、各コンポーネントの関連フィルタを設定します。[ファイル (File)] メニューをクリックし、[ドキュメントの起動 (Launch Document)] メニュー項目を選択します。



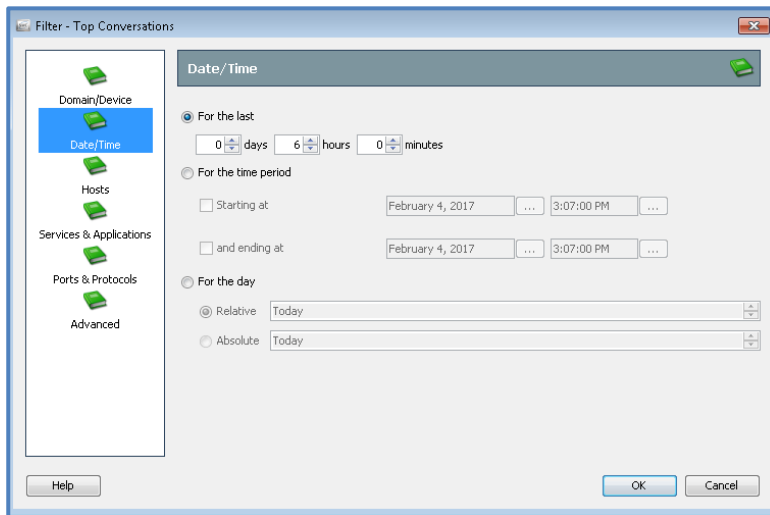
注：カスタムドキュメントビルダーは、ドキュメント自体を作成するのではなく、ドキュメントの作成に使用するテンプレートを作成するものです。ドキュメントビルダーでは、1つのドキュメントのページ数ならびに掲載コンポーネントの数および種類を指定することはできますが、個々のコンポーネント自体の内容は設定できません。ドキュメント全体として希望どおりのデータを表示できるようにするには、SMCでドキュメントを起動して各コンポーネントのフィルタオプションを設定する必要があります。

1つのカスタムドキュメントに追加するコンポーネントの数が増えるほど、すべてのデータが同時に返されることによるSMCへの負荷が大きくなるため、注意してください。多数のコンポーネントを追加した場合、各コンポーネントに選択したフィルタオプションによっては、データが返されるのに数分かかることがあります。

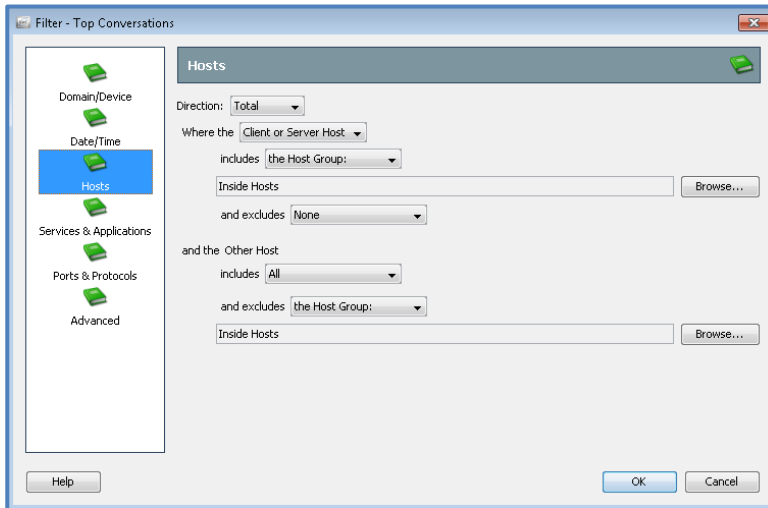
18. ここで SMC デスクトップクライアントに戻り、[フィルタ (Filter)] ウィンドウが表示されて、カスタムドキュメントに追加した各コンポーネントのフィルタオプションを変更するよう求められます。左側の [コンポーネント (Components)] をクリックします。



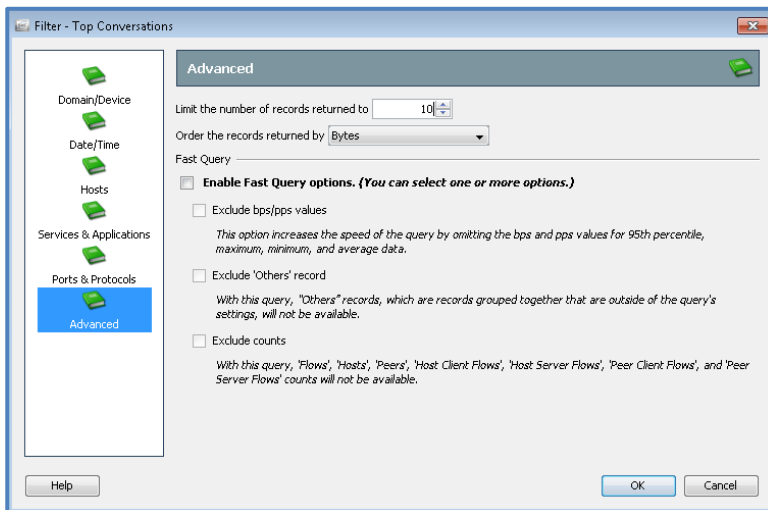
19. [上位インターネット転送 (Top Internet Transfers)] コンポーネントを選択し、[編集 (Edit)] をクリックします。
- a. [日時 (Date/Time)] メニューを選択し、[直近 (For the last)] の [6 時間 (6 hours)] に絞り込むオプションを選択します。



- b. [ホスト (Hosts)] メニューを選択し、オプションが次のように設定されていることを確認します。
 - i. [方向 (Direction)] : [合計 (Total)]
 - ii. [対象 (Where the)] : [クライアントまたはサーバホスト (Client or Server Host)]
 - iii. [含まれるもの (includes)] : [ホストグループ (the Host Group)] : [内部ホスト (Inside Hosts)]
 - iv. [除外されるもの (And excludes)] : [なし (None)]
 - v. [もう一方のホスト (and the Other Host)] : [含まれるもの (includes)] : [すべて (All)]
 - vi. [除外されるもの (and excludes)] : [ホストグループ (the Host Group)] : [内部ホスト (Inside Hosts)]



- c. [詳細設定 (Advanced)]メニューを選択し、[返されるレコード数の制限 (Limit the number of records returned to)]の値を [10] に変更します。



- d. コンポーネントのフィルタの設定が完了したら、[OK] をクリックします。

20. 上に示した手順を使用して、[上位インターネット接続先 (Top Internet Destinations)]コンポーネントの設定を次のように指定します。

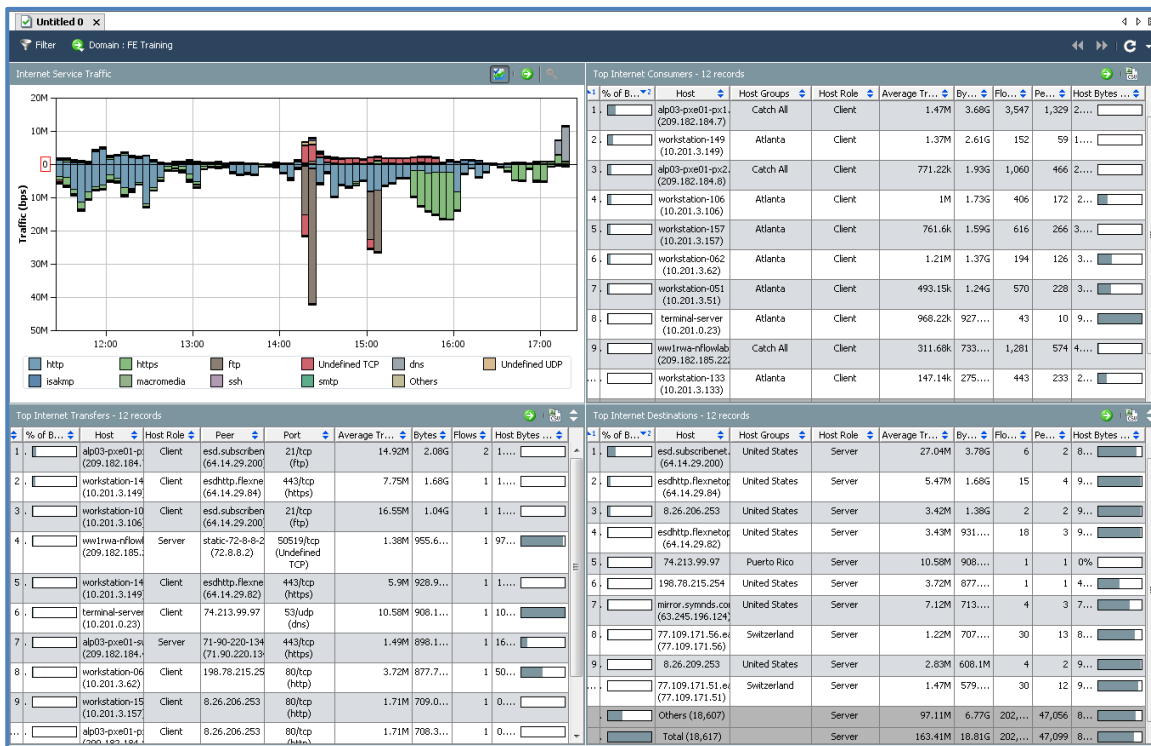
- [日時 (Date/Time)] : [直近 (last)] の [6 時間 (6 hours)]
- [ホスト (Host)] : [対象 (Where the)] に [サーバホスト (Server Host)], [含まれるもの (includes)] に [ホストグループ (the Host Group)] の [外部ホスト (Outside Hosts)], [除外されるもの (and excludes)] は [なし (None)], [もう一方のホスト (and the Other Host)] の [含まれるもの (includes)] に [ホストグループ (the Host Group)] の [内部ホスト (Inside Hosts)], [除外されるもの (and excludes)] は [なし (None)]
- [詳細設定 (Advanced)] : [返されるレコード数の制限 (Limit the number of records returned to)] は [10]

21. 上に示した手順を使用して、[上位インターネットコンシューマ (Top Internet Consumers)]コンポーネントの設定を次のように指定します。

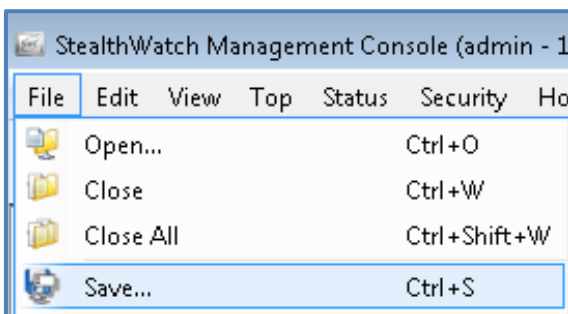
- [日時 (Date/Time)] : [直近 (last)] の [6 時間 (6 hours)]

- b. [ホスト (Host)] : [対象 (Where the)]に [クライアントホスト (Client Host)], [含まれるもの (includes)]に [ホストグループ (the Host Group)]の [内部ホスト (Inside Hosts)], [除外されるもの (and excludes)]は [なし (None)], [もう一方のホスト (and the Other Host)]の [含まれるもの (includes)]に [ホストグループ (the Host Group)]の [外部ホスト (Outside Hosts)], [除外されるもの (and excludes)]は [なし (None)]
 - c. [詳細設定 (Advanced)] : [返されるレコード数の制限 (Limit the number of records returned to)]は [10]
22. 上に示した手順を使用して、[インターネットサービストラフィック (Internet Service Traffic)]コンポーネントの設定を次のように指定します。

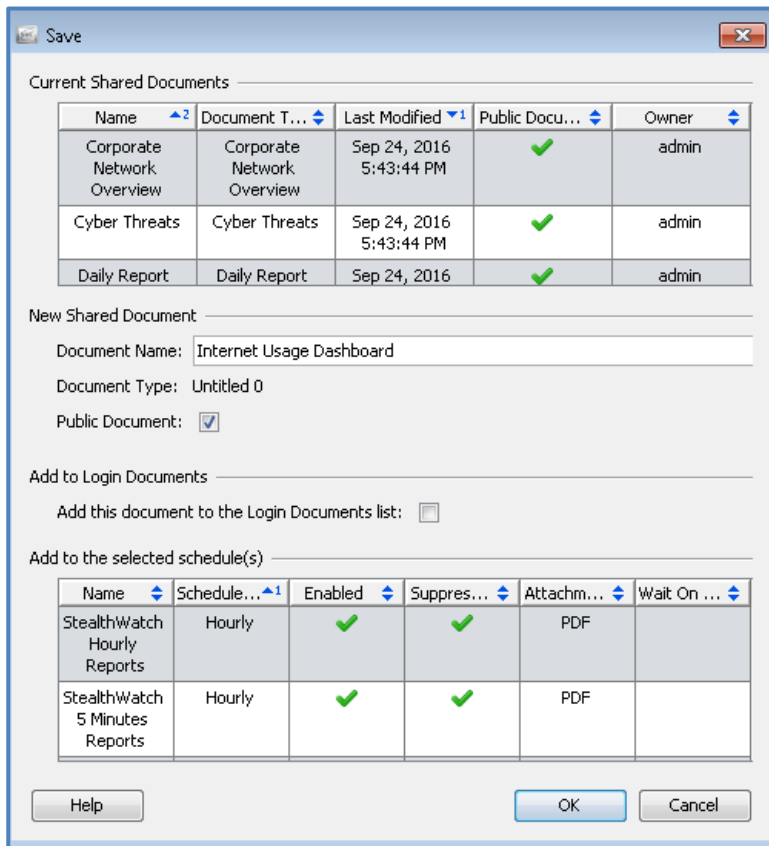
- a. [日時 (Date/Time)] : [直近 (last)]の [6時間 (6 hours)]
 - b. [ホスト (Hosts)] : [外部ホスト (Outside Hosts)]
23. すべてのフィルタの設定が終わったら、[OK]をクリックします。
24. カスタムドキュメントが表示されます。データが返されるまでに数分かかる場合があります。ドキュメントのタイトルが [無題 0 (Untitled 0)]になっていることに注意してください。このドキュメントはまだ SMC 自体には保存されていません。この時点でドキュメントを閉じると、適用したすべてのフィルタ設定が失われてしまいます。



25. SMC にドキュメントを保存するために、[ファイル (File)]メニューをクリックし、[保存 (Save)]メニュー項目を選択します。



26. [保存 (Save)] ウィンドウが表示され、ドキュメントに名前を付けるよう求められます。**Internet Usage Dashboard** という名前を使用して、[パブリックドキュメント (Public Document)] チェックマークボックスをオンにします。完了したら [OK] をクリックします。



27. SMC にアクセスできる人なら誰でも、[ファイル (File)] メニューをクリックして [開く (Open)] メニュー項目を選択し、保存されたドキュメントのタイトルを選択することで、ドキュメントを取得できるようになりました。
28. お客様のカスタムドキュメントを作成して SMC に保存する作業が、無事に完了しました。ラボの次の手順に進みます。

注：このドキュメントの作成は、Stealthwatch を実装するための必須要件ではありません。ただし、製品のドキュメントに関し、同一のドキュメントに複数のコンポーネントが含まれることを希望するお客様は非常に多いと思われます。そのニーズに応えられる設定済み製品ドキュメントがない場合には、ドキュメントビルダーが、要求を満たす唯一の方法となります。

シナリオのまとめ

このシナリオでは、PCI トランザクションに関するお客様の IT セキュリティポリシーに違反したネットワークトラフィックを明らかにするための、カスタムセキュリティ イベントを作成しました。また、デスクトップクライアントでダッシュボードとして使用できるカスタムドキュメントの作成方法についても学習しました。

シナリオ 15. 応答管理

SMC では、製品のアラームが起動した際にさまざまなタイプの通知を送信できます。ここでは、重要なアラームがトリガーされたときに、お客様の SIEM および Stealthwatch の管理者に通知が行くように Stealthwatch を設定します。この作業には、syslog 通信の設定と、通知送信のタイミングを制御するルールの定義が含まれます。

注： Stealthwatch のどのような導入環境においても、Stealthwatch アプライアンスの正常性に関するシステムアラームがお客様に通知されるよう設定してください。製品のチューニングがあまり進んでいない導入の早期段階では、ネットワーク上のホストのふるまいに関する「ホスト」アラームの有効化が必ずしも保証されない場合があります。それでも、システムアラームは常に有効にして、問題発生時にお客様が通知を受け取れるよう設定しておく必要があります。システムアラームに対応することで、製品に関わる問題の拡大防止に役立つ可能性があります。

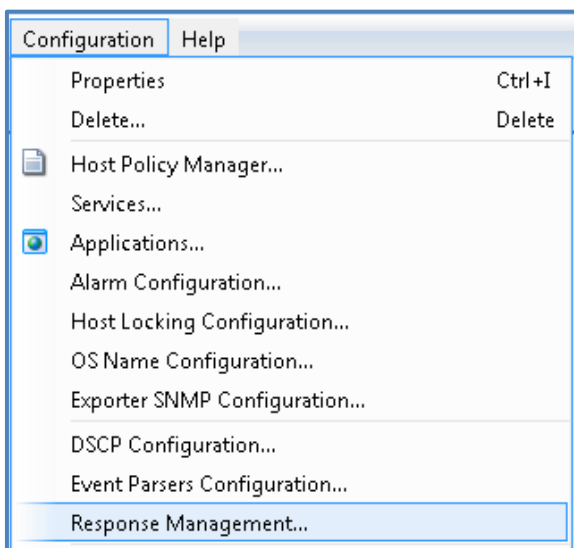
RAID ドライブの障害メッセージが数週間または数カ月間無視されたり、システムアラームが有効化されなかったためまったく送信されなかったりすると、必然的に、長期にわたるサービスの中断やアプライアンスの RMA が発生する可能性があります。アラームがタイミング良く通知されることで、修正措置を行ってサービスの中断を防ぐことができます。Stealthwatch は自身の正常性について一定程度、状況を監視することができます。これらのアラームを監視することは重要です。

Stealthwatch システムアラームの作成

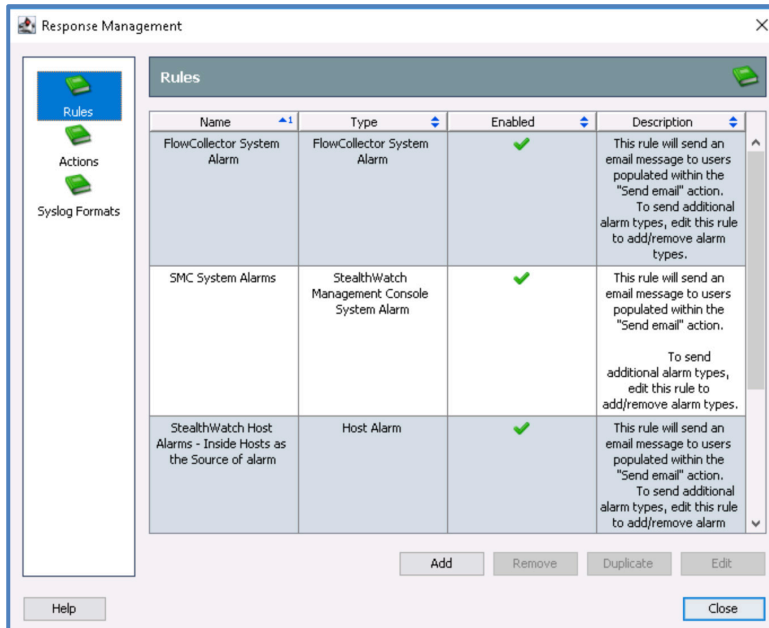
1. **Stealthwatch** デスクトップクライアントを使用していることを確認します。必要に応じて、**admin** として、パスワード **C1sco12345** を使用してログインします。



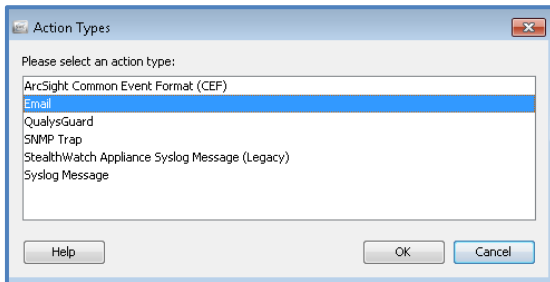
2. [設定 (Configuration)] メニューをクリックし、[応答管理 (Response Management)] メニュー項目を選択します。



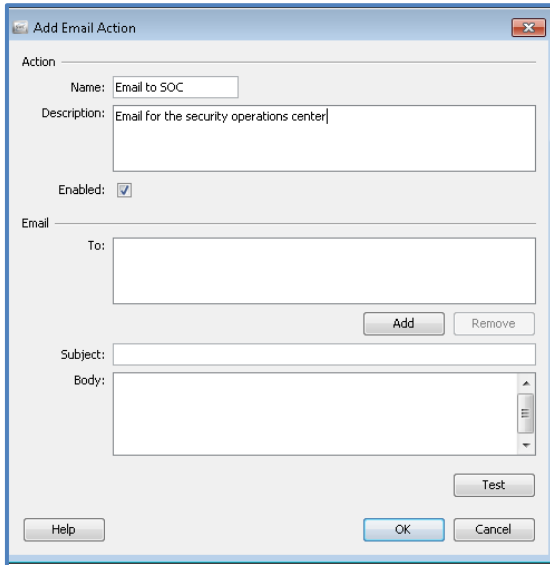
3. [応答管理 (Response Management)] ウィンドウが表示されたら、[アクション (Actions)] メニューを選択し、[追加 (Add)] をクリックします。



4. [アクションタイプ (Action type)] で [電子メール (Email)] を選択し、[OK] をクリックします。



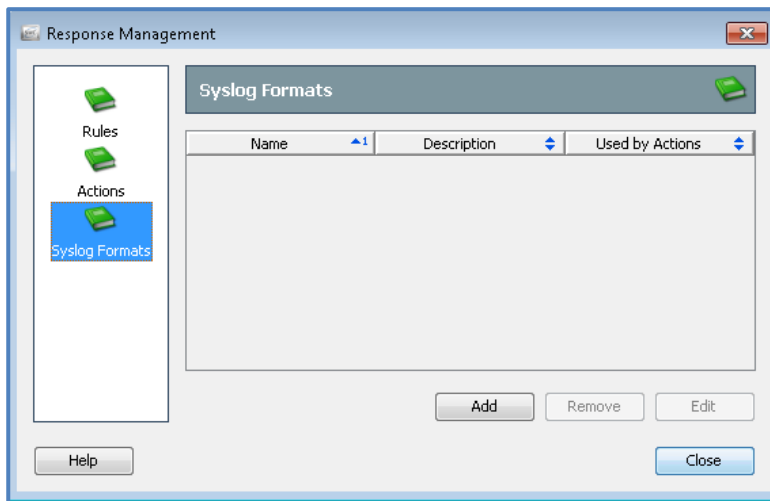
5. [電子メールアクションの追加 (Add Email Action)] ウィンドウの [名前 (Name)] フィールドに **Email to SOC** と入力します。
6. [説明 (Description)] に セキュリティ オペレーション センターへの電子メール (Email for the security operations center) と入力します。
7. [追加 (Add)] をクリックして、電子メールアクションの宛先とする電子メールアドレスを持つユーザアカウントを追加します。



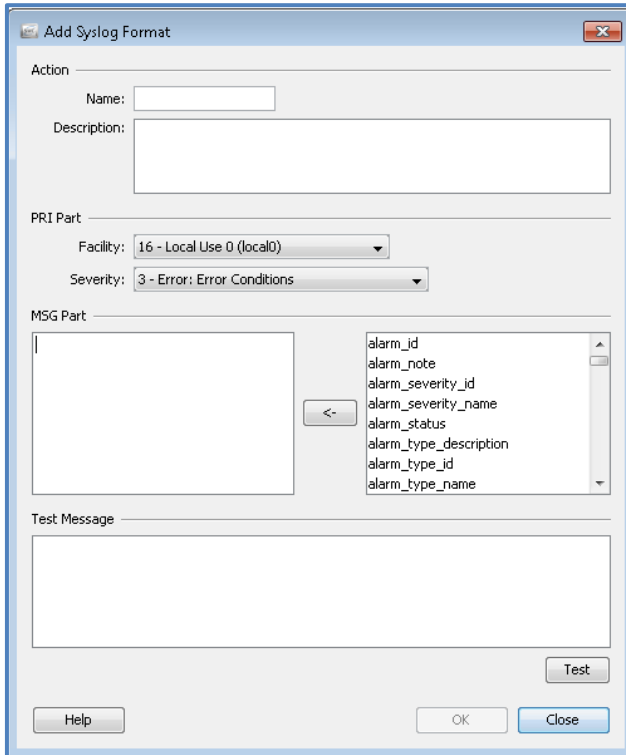
8. [SOC] ユーザアカウントを選択し、[OK] をクリックします。

注：電子メールアクションの宛先として使用するメールアドレスの入力はできません。定義されている SMC ユーザアカウントを選択する必要があります。同報グループに電子メールを送るようお客様が求めている場合、またはユーザに SMC ユーザアカウントが定義されていない場合は、アカウントを作成する必要があります。そのような場合でも、実際にログインあるいはユーザアカウントを使用しなければならないわけではありません。単に、[応答管理 (Response Management)] の設定で選択する目的のために、正しい電子メールアドレスを持つアカウントの存在が必要になります。

9. Stealthwatch は、アラーム生成時に [件名 (Subject)] と [本文 (Body)] のフィールドを自動入力します。お客様が特定のテキストを必要とする場合を除き、値を指定する必要はありません。[OK] をクリックして電子メールアクションを保存します。
10. [Syslog フォーマット (Syslog Formats)] メニューをクリックし、[追加 (Add)] をクリックします。



11. 次に、お客様の SIEM にデータを送信するときに使用する Syslog フォーマットを定義します。[名前 (Name)] フィールドを **Customer SIEM Instance 01** と設定し、[説明 (Description)] フィールドは空白のままにします。



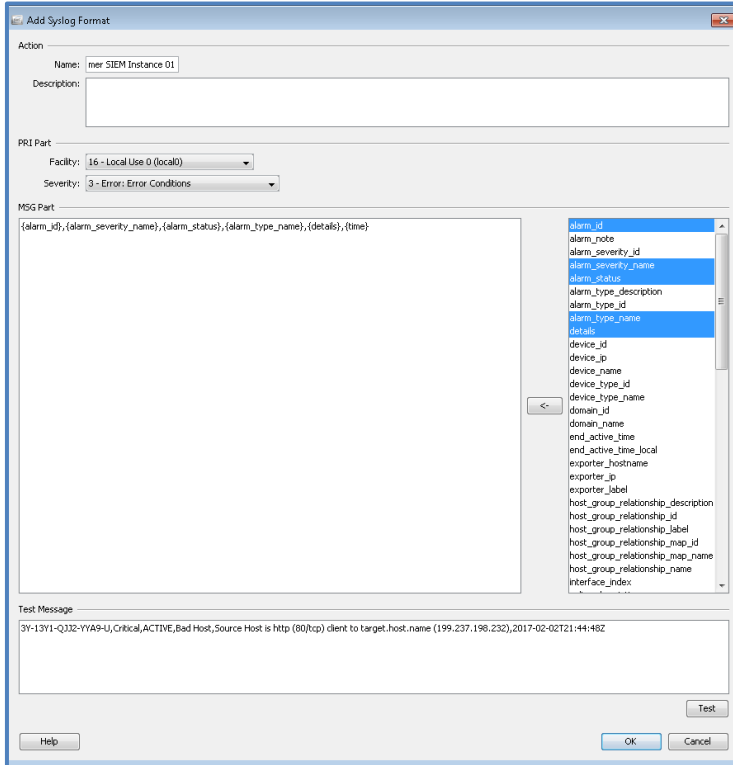
注：SIEM または Syslog サーバソリューションが異なれば、データ解析の方法も異なります。Stealthwatch は、お客様がどのような形式を選んでも、設定によって対応することができます。[MSG パーツ (MSG Part)] では、メッセージに挿入する変数を指定できます。これにより、Stealthwatch で生成されるアラーム内でデータを参照できるようになります。どの MSG パーツを使えば syslog の宛先でメッセージが確実に正しく解析され、役立つものとなるかについてお客様と検討します。以下に、syslog フォーマットのサンプルを示します。syslog フォーマットは複数作成できます。アラームのタイプごとにフィールドを変えると便利でしょう。

```
Cisco Stealthwatch 通知 : {alarm_type_id},{alarm_type_name},{alarm_severity_id}, msg={alarm_type_description}:{details}
dst={target_ip} src={source_ip} start={start_active_time} end={end_active_time} cat={alarm_category_name}
externalId={alarm_id} cs3={source_host_group_names} cs3Label=SourceHostGroups cs4={target_host_group_names}
cs4Label=TargetHostGroups cs5={source_url} cs5Label=Source_URL cs6={target_url} cs6Label=Target_URL dpt={port}
proto={protocol} dvchost={device_name} dvc={device_ip} dvcpid={domain_id} deviceExternalId={device_name}
```

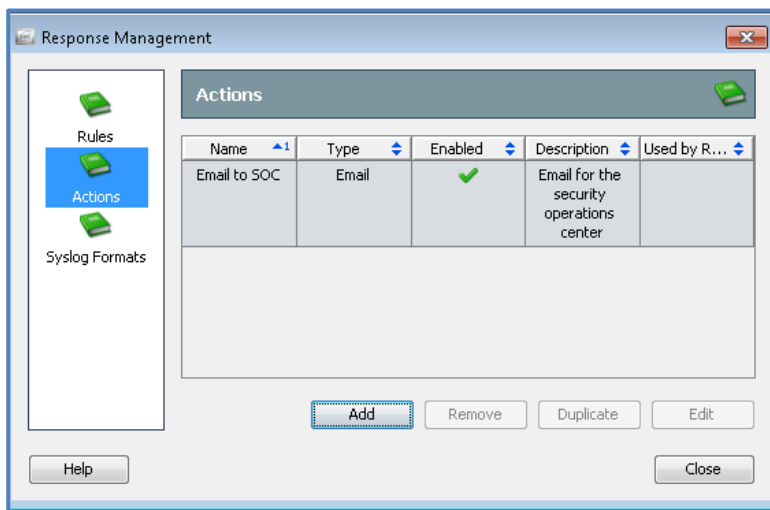
12. 右側の選択ウィンドウから次の MSG パーツを選択し、オプションごとに一度ずつ矢印ボタンをクリックして、左側の [MSG パーツ (MSG Part)] 設定に追加します。メッセージパーツ同士を区切るには、各メッセージパーツの間にカンマ (または他の区切り文字) を入れます。

- a. **Alarm_id**
- b. **Alarm_severity_name**
- c. **Alarm_status**
- d. **Alarm_type_name**
- e. **Details**

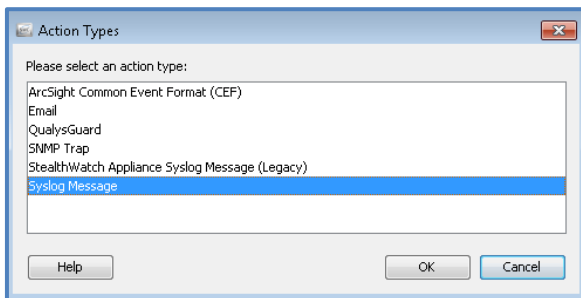
f. Time



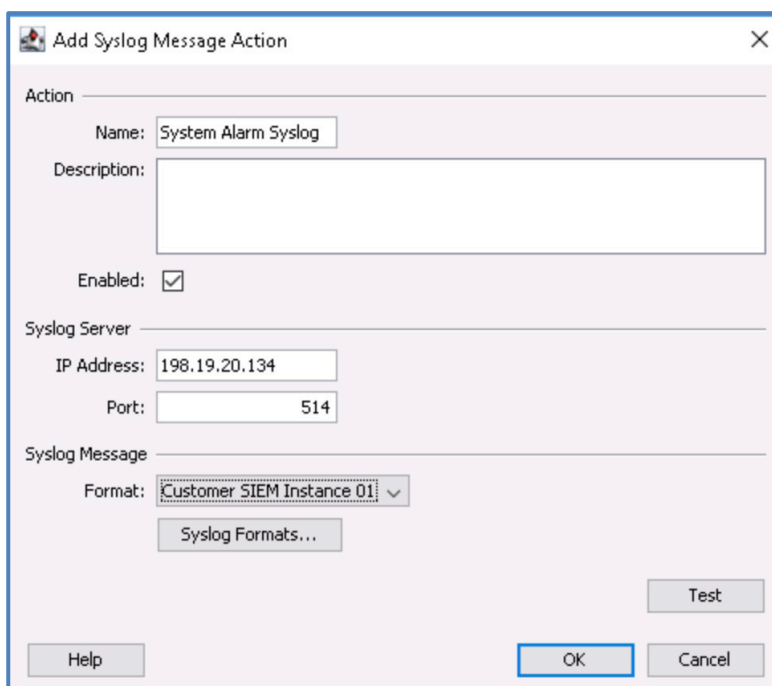
13. [テスト (Test)]をクリックすると、syslog フォーマットのサンプル出力が表示されます。
14. MSG パーツを追加または削除して syslog フォーマットを自由に変更できます。
15. 終わったら、[OK] をクリックして syslog フォーマットを保存します。
16. [アクション (Actions)]メニューをクリックし、[追加 (Add)]をクリックして、Syslog メッセージを送信する新しいアクションを追加します。



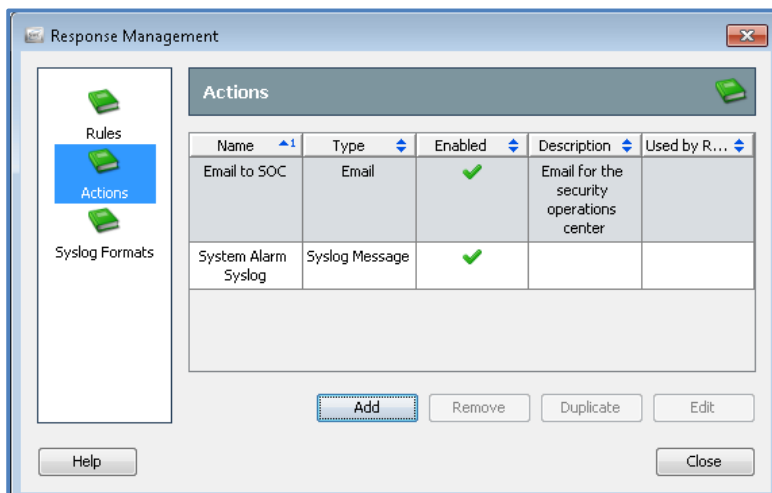
17. [Syslog メッセージ (Syslog Message)] オプションを選択して、[OK] をクリックします。



18. 次の値を使用して [Syslog メッセージアクションの追加 (Add Syslog Message Action)] 画面の設定を行い、[OK] をクリックして変更を保存します。
- a. [名前 (Name)] : **System Alarm Syslog**
 - b. [説明 (Description)] : **(syslog メッセージの使用目的の説明を入力する)**
 - c. [有効化 (Enabled)] : **オン**
 - d. [IP アドレス (IP Address)] : **198.19.20.134**
 - e. [ポート (Port)] : **514**
 - f. [フォーマット (Format)] : **[Customer SIEM Instance 01]**

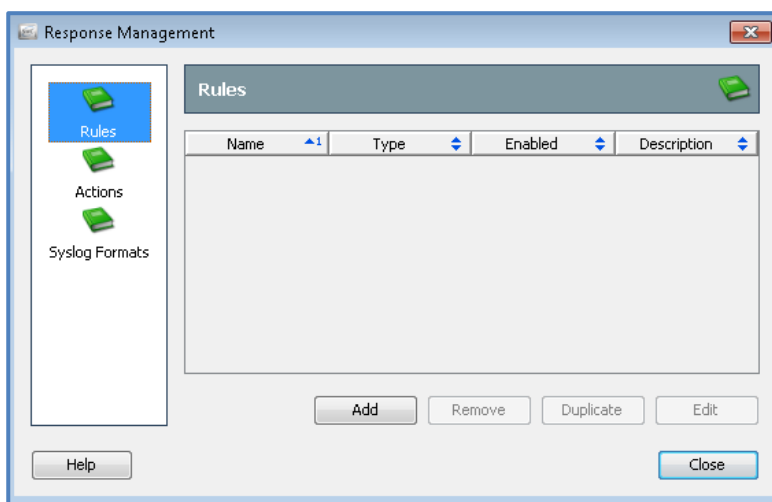


19. 利用可能なアクションが [アクション (Actions)] 画面に表示されます。



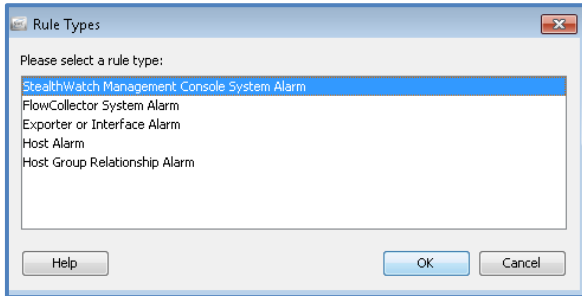
注：複数のインスタンスに同一のアクションタイプを指定できます。たとえば、複数の syslog フォーマットが必要な場合や、データを必要とする syslog サーバまたは SIEM が複数存在する場合があります。また、オプションがそれぞれ異なる複数の電子メールアクションを定義することもできます。

20. [ルール (Rules)]メニューをクリックし、[追加 (Add)]ボタンを選択します。



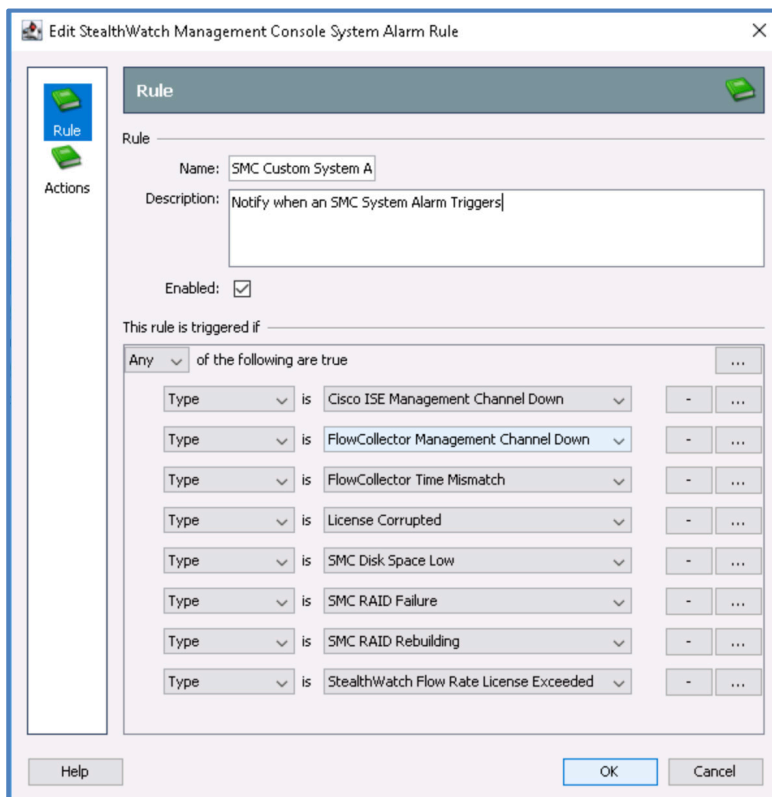
21. 作成したいルールのタイプを尋ねるプロンプトが表示されます。[Stealthwatch 管理コンソールシステムアラーム (Stealthwatch Management Console System Alarm)]を選択して [OK] をクリックします。

注：システムアラームは、Stealthwatch アプライアンスまたは製品の健全性に関連する問題を取り扱うものです。[エクスポートまたはインターフェイスアラーム (Exporter or Interface Alarm)]は、いくつかの [フローセンサーシステムアラーム (Flow Sensor System Alarm)]同様、エクスポートの帯域幅使用率を取り扱います。[ホストアラーム (Host Alarm)]は、Stealthwatch 監視対象ホストのセキュリティ関連の項目を取り扱います。[ホストグループリレーションシップアラーム (Host Group Relationship Alarm)]は、マップと、マップを使用して作成されたオブジェクトを取り扱います。



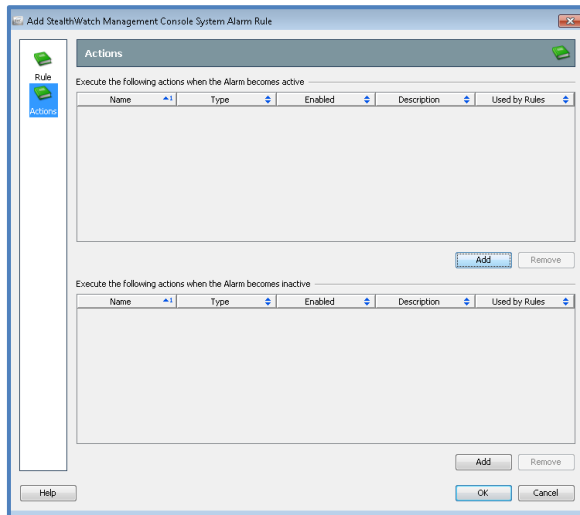
22. 左ウィンドウペインの [ルール (Rule)] メニューを選択します。ここでは、システムアラームルール実行のタイミングを決定するルール条件を設定します。

- a. このポップアップが画面に対して大きすぎる場合（下部の [OK]/[キャンセル (Cancel)] ボタンが見えない場合）、他の Windows アプリケーションと同様に、ポップアップウィンドウの上部を下にドラッグしてサイズを変更します。
- b. ルールの [名前 (Name)] を **SMC Custom System Alarms** と設定します。
- c. ルールの [説明 (Description)] に SMC システムアラームがトリガーされた時に通知 (Notify when an SMC System Alarm triggers) と入力します。
- d. ルールの [有効化 (Enabled)] が選択されていることを確認します。
- e. [このルールのトリガー条件 (This rule is triggered if)] セクションでは、次の設定を使用します。
 - i. [が真の場合 (of the following are true)] に [いずれか (Any)] を設定します。
 1. これは、設定に関する一般論的な問題です。デフォルトではこのオプションが [すべて (All)] に設定されています。このままだと、すべての条件に該当しないとルールアクションが起こらないことになります。SMC で、事実上利用可能なすべてのアラームが同時にトリガーされることはあり得ないので、値が [すべて (All)] に設定されていると、通知は送られません。
- f. 右側の **省略記号ボタンをクリックし**、ドロップダウンからさまざまなタイプの SMC システムアラームを選択することにより、複数の条件を追加します。 **以下に指定されたタイプを追加します**（追加後に [OK] をクリックしないでください）。
 - i. [Cisco ISE 管理チャンネルダウン (Cisco ISE Management Channel Down)]
 - ii. [フローコレクタ管理チャンネルダウン (Flow Collector Management Channel Down)]
 - iii. [フローコレクタ時間不一致 (Flow Collector Time Mismatch)]
 - iv. [ライセンス破損 (License Corrupted)]
 - v. [SMC ディスク容量低下 (SMC Disk Space Low)]
 - vi. [SMC RAID 障害 (SMC RAID Failure)]
 - vii. [SMC RAID 再構築 (SMC RAID Rebuilding)]
 - viii. [Stealthwatch フローライセンス超過 (Stealthwatch Flow License Exceeded)]

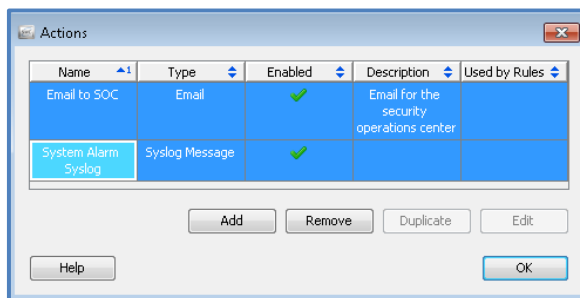


注：適しているシステムアラームは、お客様によって異なる場合があります。仮想アプライアンスには RAID アラームは必要ありません。ISE 統合を利用していない環境または UDP Director がない環境では、それぞれに対応するアラームは必要ありません。システムアラームを実装する際は、すべてのアラームを確認して、お客様の環境に関連性のあるものを判断してください

23. **[OK] はまだクリックしないでください。** SMC システムアラームルールのトリガー条件の設定が終わったので、今度は、ルールがトリガーされたときに実施されるアクションを設定する必要があります。左ウィンドウペインの [アクション (Actions)] メニューを選択します。
 - a. [アクション (Actions)] 画面では、アラームがアクティブになったときと非アクティブになったときに実施されるアクションを設定できます。

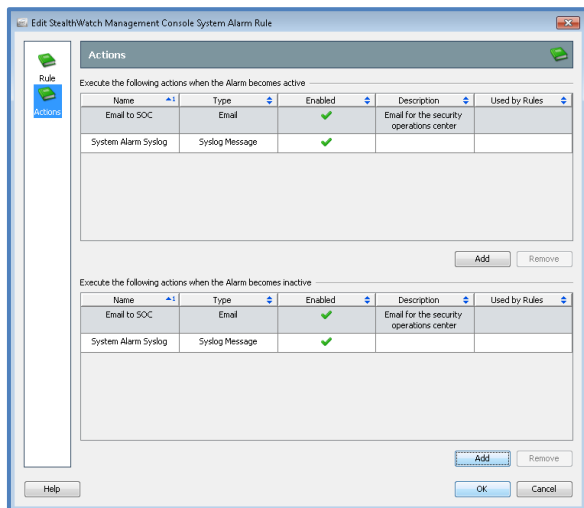


- b. [アラームがアクティブになったときに実施するアクション (Execute the following actions when the Alarm becomes active)]セクションの [追加 (Add)]をクリックします。
 - i. [SOC にメール (Email to SOC)]アクションと [システムアラーム Syslog (System Alarm Syslog)]アクションの両方を選択 (Ctrl + クリック) して、[OK] をクリックします。



- c. [アラームが非アクティブになったときに実施するアクション (Execute the following actions when the Alarm becomes inactive)]セクションの [追加 (Add)]をクリックします。
 - i. [SOC にメール (Email to SOC)]アクションと [システムアラーム Syslog (System Alarm Syslog)]アクションの両方を選択 (Ctrl + クリック) して、[OK] をクリックします。

24. [OK] をクリックして、SMC システムアラームルールの変更を確定します。



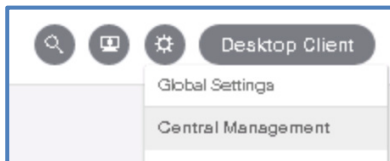
25. ここで少し時間をとって、Stealthwatch の初期インストールに含まれていたデフォルトのルールを確認します。必要に応じてこれらのルールを変更すると、カスタム環境でフローコレクタと SMC システムアラームに関する応答管理を迅速に設定できます。
26. すべての変更を保存して、[応答管理 (Response Management)] ウィンドウを閉じます。これで、Stealthwatch の正常性に関連する問題の発生時にアラームを発信するための SMC 設定作業が、無事に完了しました。ラボの次の手順に進みます。
27. [閉じる (Close)] をクリックします。

注： 実稼働環境では、お客様をフォローアップして、SMC によって生成されるアラームに対応するワークフローが実行されているか検証してください。SMC が通知を送信してもお客様が問題を調査しなければ、通知を行う意義がありません。

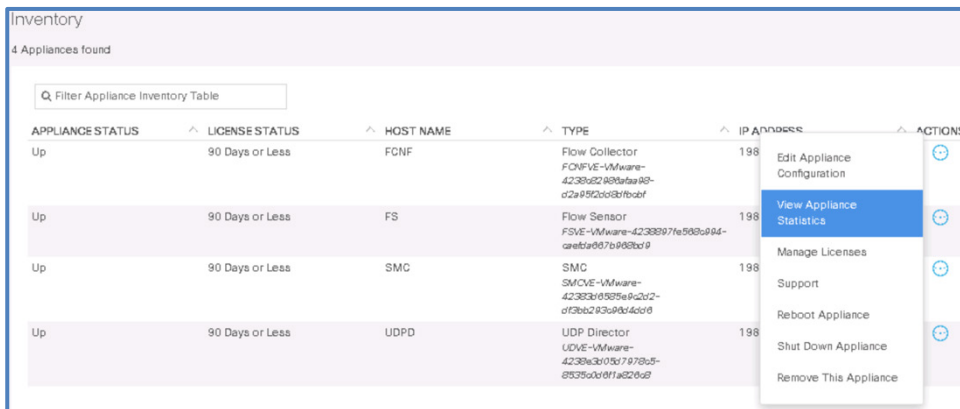
Stealthwatch システムアラームの検証

応答管理ルールで以前設定したとおりの電子メールと syslog 通知を、お客様が受信できていません。お客様の SMTP および syslog 管理者は、Stealthwatch に問題があるはずだと主張しています。そこで、SMC が SMTP および syslog 通知を送信していることを検証する必要があります。アプライアンスのパケットキャプチャ機能を使用して、SMC により生成されるトラフィックをキャプチャします。

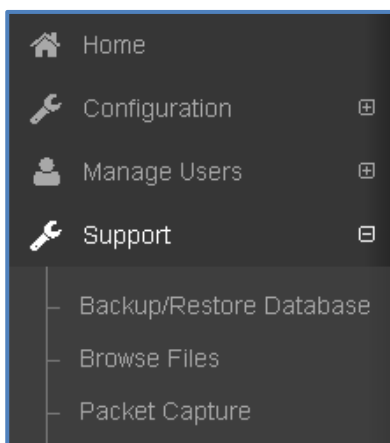
1. ブックマークを使用して、**Chrome** で **SMC Web** インターフェイスに接続します。
2. Web インターフェイスで**歯車アイコン**をクリックし、[Central Management] をクリックします。



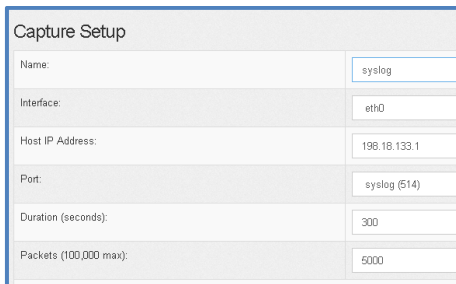
3. SMC の [アクション (Actions)] アイコンをクリックし、[アプライアンス統計情報の表示 (View Appliance Statistics)] を選択します。



4. [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)] メニュー項目を選択します。

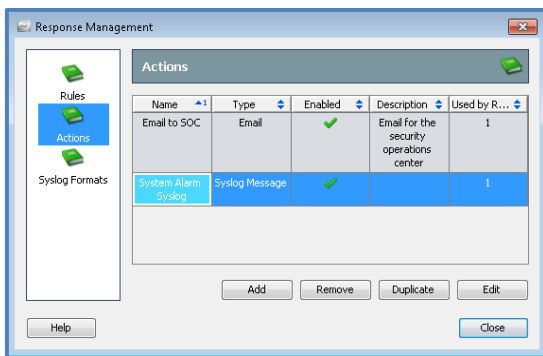


5. [キャプチャ設定 (Capture Setup)] ウィンドウで、以下の設定を使用してパケットキャプチャを構成し、ページ上の [開始 (Start)] をクリックしてキャプチャを開始します。
 - a. [名前 (Name)] : **syslog**
 - b. [インターフェイス (Interface)] : **eth0**
 - c. [ホスト IP アドレス (IP Address)] : **198.19.20.134**
 - d. [ポート (Port)] : **syslog (514)**
 - e. [時間 (Duration)] : **300**
 - f. [パケット数 (Packets)] : **5000**

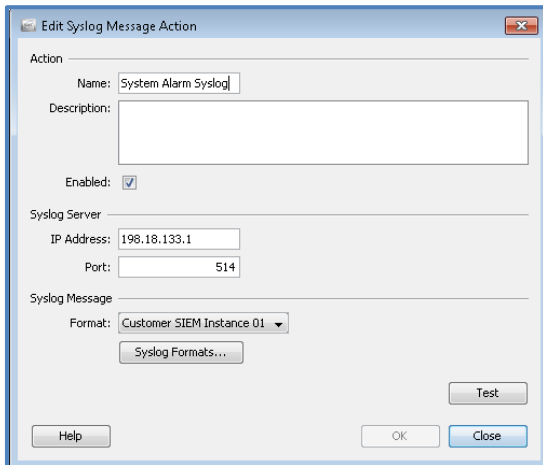


Field	Value
Name	syslog
Interface	eth0
Host IP Address	198.18.133.1
Port	syslog (514)
Duration (seconds)	300
Packets (100,000 max)	5000

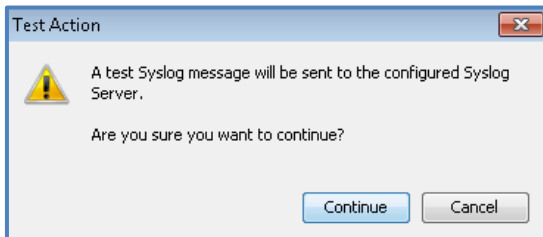
6. パケットキャプチャが開始されます (開始されない場合は、[開始 (Start)] をクリックします)。これから 5 分以内にいくつかの syslog メッセージを生成してテストする必要があります。
7. デスクトップクライアントに戻り、[設定 (Configuration)] メニューの [応答管理 (Response Management)] をクリックします。
8. 左ペインの [アクション (Actions)] メニューを選択し、[システムアラーム Syslog (System Alarm Syslog)] アクションを選択し、[編集 (Edit)] をクリックします。



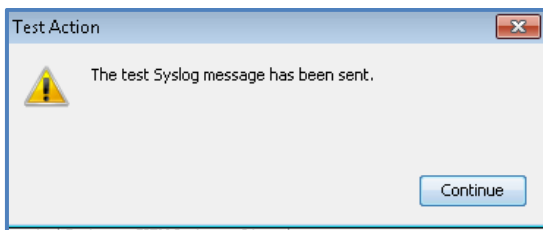
9. syslog アクションの設定が表示されます。[テスト (Test)] をクリックして宛先 syslog サーバに syslog テストメッセージを生成します。



10. 確認画面が表示されたら、[続行 (Continue)] をクリックします。



11. Syslog メッセージが送信されたら、[続行 (Continue)] をクリックします。

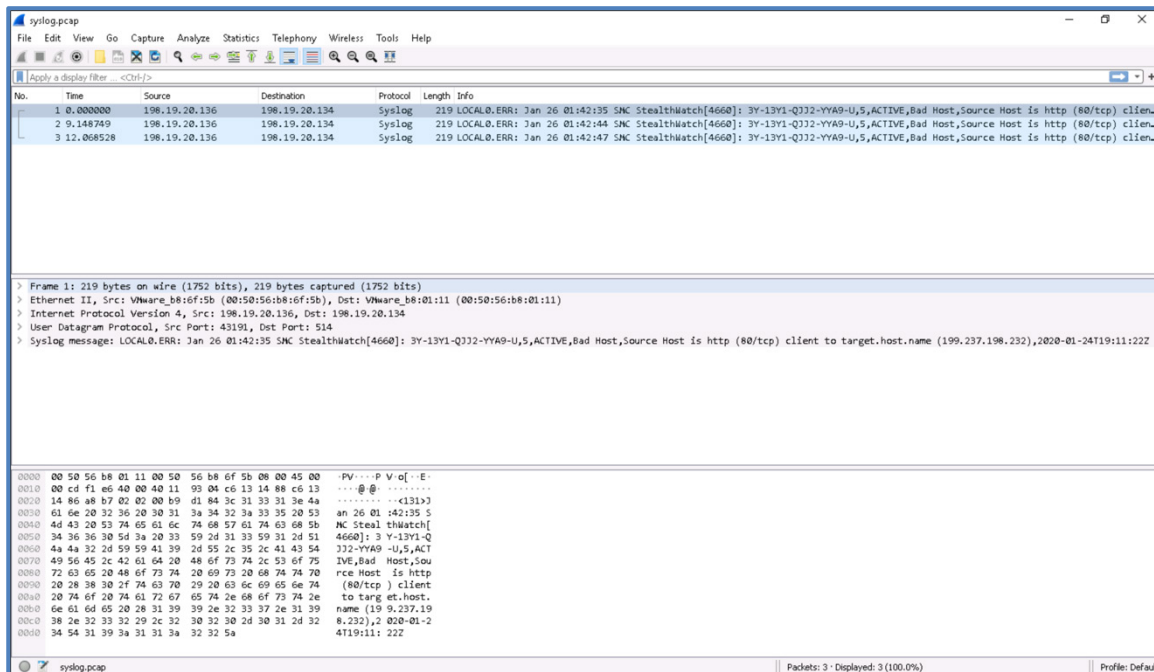


12. テストメッセージのプロセスをさらに数回繰り返してから、SMC のパケットキャプチャ インターフェイスに戻ります。
13. [閉じる (Close)] をクリックし、[応答管理 (Response Management)] の [閉じる (Close)] をクリックして終了します。
14. **Chrome** で **SMC** アプライアンスのキャプチャページに戻ります。
15. まだキャプチャ実行中の場合は、この時点でキャプチャを停止しても構いません。
16. パケットキャプチャの [syslog] リンクをクリックしてファイルをダウンロードします。確認画面が表示されたら、[保存 (Save)] をクリックします。

Captures						
Name	Status	Size(bytes)	Start Time	End Time	Duration(sec)	Action
syslog	Complete	996	2017-02-03 17:45:15	2017-02-03 17:50:15	300	<input type="button" value="Rerun"/> <input type="button" value="Delete"/>

17. Chrome ブラウザの左下に pcap ファイルが現れます。ダウンロードされたファイルをクリックすると、Wireshark で pcap が開きます。

18. 198.19.20.134 のポート UDP 514 に syslog パケットが送信されていることを確認できます。syslog メッセージを表示して、フォーマットが正しいか確認することもできます。



19. この事例では、ここでパケットキャプチャをお客様に転送して、SMC が実際に正しい IP アドレスに syslog を送信していることを説明できます。お客様の SIEM により syslog が処理されない原因としては、ACL またはファイアウォールがトラフィックをブロックしているか、SIEM が syslog メッセージを受け入れるよう正しく設定されていない可能性が考えられます。宛先ホストでのパケットキャプチャはトラブルシューティングに役立つ可能性があります。
20. **Wireshark** を閉じます。

シナリオのまとめ

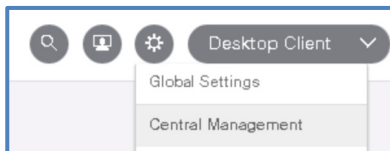
このシナリオでは、Stealthwatch 自体の正常性の監視を支援するシステムアラームを作成しました。お客様の SIEM に送信する syslog メッセージフォーマットを設定し、syslog および電子メール通知を送信するアクションを作成し、Stealthwatch のためのシステムアラームを作成しました。

シナリオ 16. アプライアンスの SNMP エージェントの設定

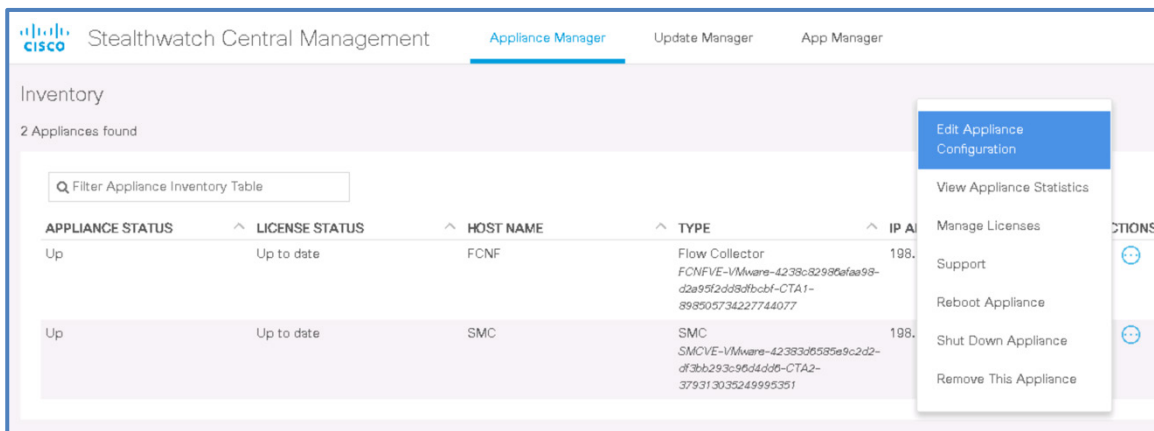
お客様は、ネットワーク運用パフォーマンス監視システムと SNMP プロトコルを介して Stealthwatch アプライアンスを監視することを希望しています。お客様からは、監視システムが SNMP 経由でアプライアンスにアクセスできるようにアプライアンスを設定してほしいと依頼されました。

注：アプライアンスに関しては、常に、SNMP および ICMP などの外部メカニズムを介してお客様に監視してもらうことがベストプラクティスです。これらのメカニズムは、アプライアンスで TCP/443 が開いていることをポーリングして検証します。アプライアンスおよびクリティカルプロセスをリモートで監視するには、多くの方法があります。重要なポイントは、監視チームと連携して実際に監視を実行するようにお客様に要請することです。アプライアンスには、設定したシステムアラームがトリガーされないほどの非常に重大な問題が発生する可能性があります。SMC がダウンしてあらゆるシステムアラームをまったくトリガーできない可能性もあります。外部監視は重要です。これによって、早い段階でお客様に問題を警告することができます。

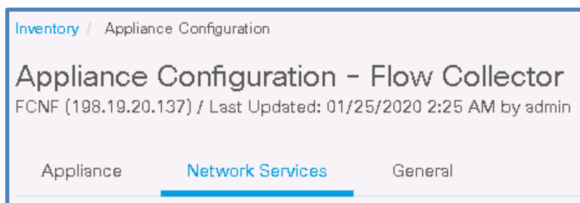
1. **SMC Web インターフェイス**に戻り、**歯車アイコン**をクリックして、**[Central Management]** を選択します。



2. **[FCNF] フロー コレクタ アプライアンスの [アクション (Actions)] アイコン**をクリックし、**[アプライアンス設定の編集 (Edit Appliance Configuration)]** を選択します。



3. **[ネットワークサービス (Network Services)] タブ**をクリックします。



4. **[SNMP エージェント (SNMP Agent)] セクション**で、次の値を入力して SNMP エージェントを設定します。
 - a. **[有効 (Enable)]** : **オン**
 - b. **[読み取り専用コミュニティ (Read Only Community)]** : **CustomerROv2String**

- c. [SNMP ポート (SNMP Port)] : **161**
- i. SNMP を標準以外のポートで実行することをお客様が求めている場合は、この設定でポート番号を変更できます。お客様が特に指定しない限り、この値は 161 のままにします。
- d. [sysLocation] : **Customer Datacenter02**
- i. リモート監視システムが SNMP 経由でアプライアンスを照会すると、アプライアンスの [ロケーション (Location)] フィールドにこの値が表示されます。この値はお客様から入手します。お客様の監視システムに表示するアプライアンスのロケーションとして、お客様が指定したとおりの内容を入力してください。
- e. [sysContact] : **所有者名**
- i. リモート監視システムが SNMP 経由でアプライアンスを照会すると、アプライアンスの [連絡先 (Contact)] フィールドにこの値が表示されます。この値はお客様から入手します。お客様の監視システムに表示するアプライアンス連絡先表示として、お客様が指定したとおりの内容を入力してください。
- f. [sysName] : **FCNF**
- i. 通常この値には、お客様によって割り当てられたホスト名を入力します。この値が、リモート監視システムに表示される名前となります。お客様が複数の Stealthwatch アプライアンスを所有している場合にデフォルト値を使用すると、すべてのアプライアンスが同じ名前が表示されます。お客様がこの目的のために割り当てたホスト名を使用します。
- g. [sysServices] : **(デフォルト値のままにする)**
- h. [sysDescription] : **Stealthwatch FlowCollector**
- i. この値には、アプライアンスの目的を説明するテキストを自由に入力できます。お客様の標準値がある場合は、ここにその命名規則を適用します。それ以外は、アプライアンス名と型番を記述します。
- i. [sysObjectID] : **(デフォルト値のままにする)**
- j. [SNMP バージョン (SNMP Version)] : **V2**

SNMP Agent Modified

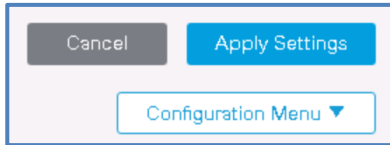
Enable

<p>READ ONLY COMMUNITY *</p> <input type="text" value="CustomerROv2String"/>	<p>SNMP PORT (DEFAULT 161) *</p> <input type="text" value="161"/>
<p>SYSLOCATION *</p> <input type="text" value="Customer Datacenter02"/>	<p>SYSCONTACT *</p> <input type="text" value="Owner Name"/>
<p>SYSNAME *</p> <input type="text" value="FCNF"/>	<p>SYSSERVICES *</p> <input type="text" value="72"/>
<p>SYSDESCRIPTION *</p> <input type="text" value="Stealthwatch FlowCollector"/>	<p>SYSOBJECTID *</p> <input type="text" value="1.3.6.1.4.1.8712.1.1"/>





SNMP VERSION

V2 V3

5. SNMP 値を設定したら、[設定の適用 (Apply Settings)]、[変更の適用 (Apply Changes)]の順にクリックします。



6. 設定がそのアプライアンスに適用されている間、アプライアンスのステータスが変更されていることを確認します。

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
● Config Changes Pending	90 Days or Less	FCNF	Flow Collector FCNFVE-VMware-4238c82980faa98-d2a952d3d8fbcbf	198.19.20.137	
Up	90 Days or Less	FS	Flow Sensor FSVE-VMware-4238997e568c994-caefda667b968bd9	198.19.20.138	
Up	90 Days or Less	SMC	SMC SMCVE-VMware-42383d58e9c2d2-df3bb293c96d4d06	198.19.20.136	
Up	90 Days or Less	UDP	UDP Director UDVE-VMware-4238e3d05d7978c5-8535c0d0f1a826c8	198.19.20.139	

注：アプライアンスの SNMP エージェントの設定は、外部システムが SNMP を介してアプライアンスをポーリングできるように設定するものです。この設定により、Stealthwatch アプライアンスが自身の主要機能を実行する能力が影響を受けることは一切ありません。SNMP エージェントの設定は、SNMP を介してエクスポートをポーリングする SMC との相互作用はなく、SMC が応答管理を介して SNMP トラップを送信する能力にも関係していません。SNMP エージェントの唯一の機能は、アプライアンスのリモート監視です。その目的のためにこれを有効にすることを強くお勧めしますが、実用上は省略可能です。

シナリオのまとめ

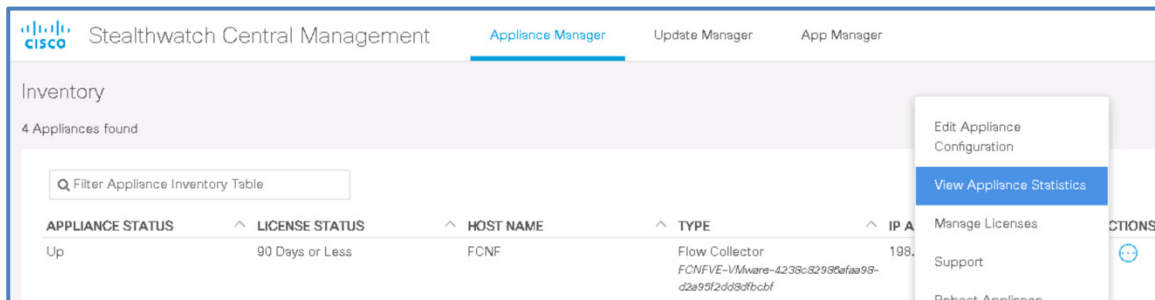
このシナリオでは、FC の SNMP エージェントを設定して、サードパーティの SNMP 監視システムから監視できるようにしました。ラボでは、この手順をすべてのアプライアンスに実行する必要はありません。ただしお客様の環境では、可能な場合、すべての Stealthwatch アプライアンスをお客様のシステムで監視してください。

シナリオ 17. 予測される FC データベースストレージ容量の算出

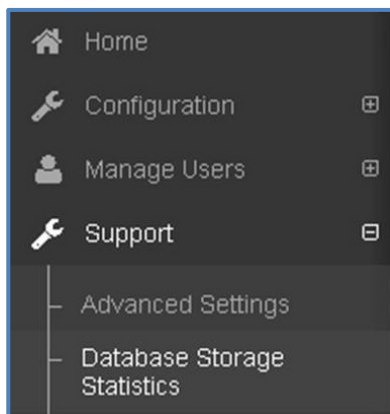
どのフロー コレクタ アプライアンスでも、フローデータの保存に利用できるストレージスペース容量は限られています。購入したアプライアンスモデル、仮想アプライアンスに割り当てられているストレージ量、およびお客様の環境で生成されるフローデータの量によって、お客様がアクセスできるデータは、1 年分の場合もあれば、辛うじて丸 1 ヶ月分程度という場合もあります。

アプライアンスがインストールされ、FC がスコープ内のすべてのエクスポートからフローデータを取り込むようになったため、お客様は、システムが保持できるフローデータの量を尋ねてきました。データを保持できる日数についての概算をお客様に提示するために、FC のデータベースストレージ統計機能を活用します。

1. Chrome Web ブラウザで [Central Management] を開きます。
2. [FCNF] アプライアンスの [アクション (Actions)] アイコンをクリックし、[アプライアンス統計情報の表示 (View Appliance Statistics)] を選択します。



3. **admin** および **C1sco12345** を使用してログインします。
4. [サポート (Support)] メニューをクリックし、[データベースストレージ統計情報 (Database Storage Statistics)] メニュー項目をクリックします。



5. [データベースストレージ統計情報 (Database Storage Statistics)] 画面が現れ、FC 容量の詳細が表示されます。

Database Storage Statistics		
Capacity		
	Average	Worst Case
Capacity in Days	369	145
Remaining Days	296	72
Bytes Per Day	320.5M	567.74M

注：ここに表示される値は、フローコレクタで保存される 1 日あたりフローデータ量の平均に基づいた推定値です。[最悪の場合 (Worst Case)] の値は、1 日間のストレージ量の最大値を使用して計算されます。FC がオンラインでフローデータを取り込んできた期間が長くなるほど、この情報の精度が上がります。[保持可能日数 (Capacity in Days)] は総容量を表し、[残り日数 (Remaining Days)] の値は、古いデータを削除しない場合にあと何日分の新しいデータを保存できるかを示しています。物理アプライアンスのストレージ容量は、アプライアンスの型番とそのモデルの内部ストレージ容量によって決まります。仮想アプライアンスでプロビジョニングされるストレージ容量も、お客様のライセンスの VE アプライアンスの型番に関係があります。

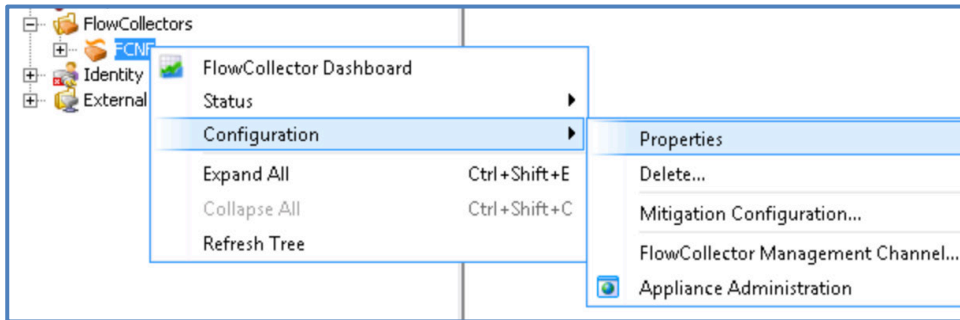
- [フローデータの概要 (Flow Data Summary)] セクションに、[フローの詳細 (Flow Details)] と [フローインターフェイスの詳細 (Flow Interface Details)] によるストレージ量の詳細が表示されます。[フローインターフェイスの詳細 (Flow Interface Details)] には、お客様のネットワークを通過したフローの処理を行ったエクスポート インターフェイスに関する情報が含まれます。このデータは、FC データベース内の容量を大量に消費する可能性があります。そこで、保持される [フローインターフェイスの詳細 (Flow Interface Details)] が一定の量に制限されるようにお客様の FC を設定します。

Flow Data Summary								
Data	Days	Containers	Rows			Bytes		
			Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	73	83	221.12M	3.03M	6.52M	5.23G	71.64M	177.44M
Flow Interface Details	5	21	49.95M	9.99M	15.44M	1.24G	247.98M	386.73M
Total	73	104	271.08M	13.02M	21.96M	6.47G	319.62M	564.17M

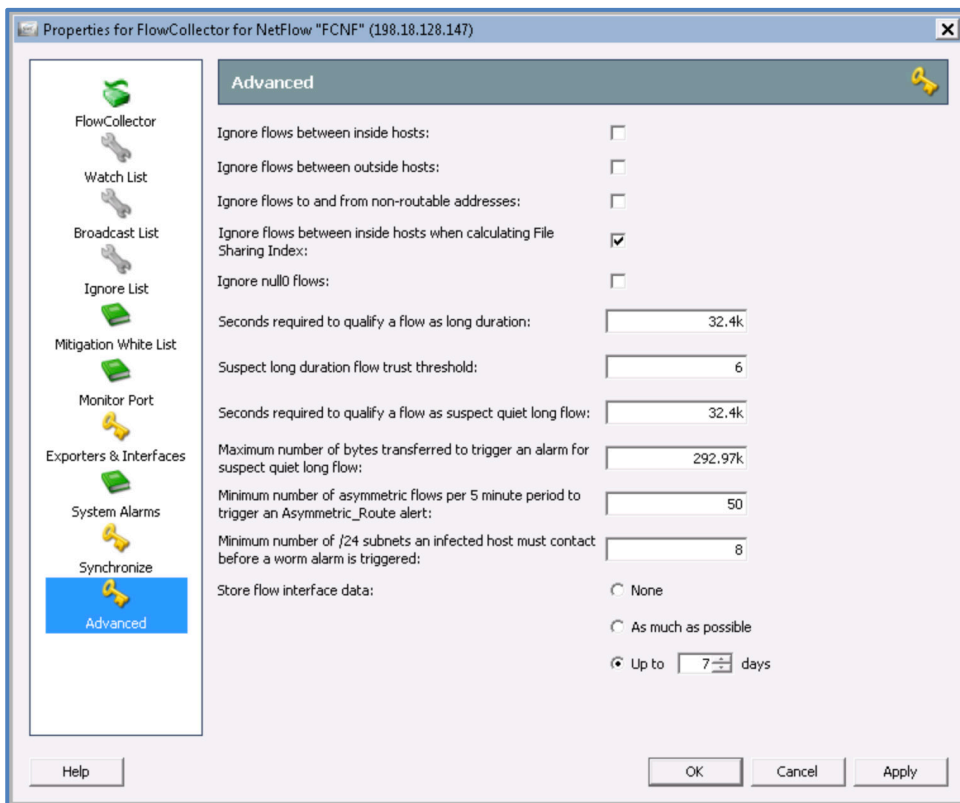
- Stealthwatch デスクトップクライアント を開き、admin ユーザとしてパスワード C1sco12345 でログインしていることを確認します。



- [エンタープライズ (Enterprise)] ツリーをたどり、[FCNF] フローコレクタエントリをクリックして強調表示させます。[FCNF] を右クリックし、[設定 (Configuration)]、[プロパティ (Properties)] メニュー項目の順に選択します。



9. 左ペインの [詳細設定 (Advanced)] メニューを選択します。
 - a. 次の画像に示されているオプション全体が表示されない場合には、他のウィンドウと同様、ウィンドウの端または角をクリックしたまま拡大してウィンドウを大きくする必要があります。
10. [フローインターフェイスデータの保存 (Store flow interface data)] の設定が [最大 7 日間 (Up to 7 days)] の値になっていることを確認して、[閉じる (Close)] をクリックします。



注：FC のデフォルト値は、フロー インターフェイス データを最大 7 日間保存するように設定されています。FC 上のハードディスクの最大容量に達すると、新しいデータを保存するスペースを確保するために、最も古いデータの削除が始まります。しかし、フロー インターフェイス データを保存すると、FC で実際のフローデータを保存できる期間が短くなる場合があります。この設定により、一定期間を超えたフローデータを削除するのではなく、フローが通過したインターフェイスのデータを保持しないことでフローデータの保持を優先できるようになります。

この値を一定の数（たとえば 7 日など）に設定すると、7 日を超えた古いフロー インターフェイス データがデータベースに含まれなくなるため、より多くのフローデータを FC に保存できるようになります。お客様の環境によっては、フロー インターフェイス データの制限に変更を加える前に、数週間または数カ月間 FC を実行させて、保存できるフローデータとフロー インターフェイス データの量を判断するとよいでしょう。これは、お客様が必要に応じてフローデータのデータ保持期間を延長したい場合に役立つツールです。この設定は FC 1 台ごとに行い、FC が複数ある環境ではそれぞれのアプライアンスに設定を適用する必要があることに注意してください。

シナリオのまとめ

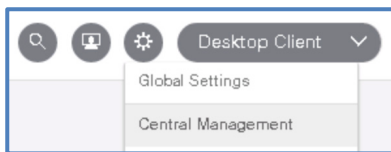
このシナリオでは、現在フローコレクタに送信されているフローデータの量に基づいて、FC に保存できるデータの推定量を算出しました。また、今後 FC データベースに保存されるフローデータの量を増やすため、インターフェイス詳細の保持については、データが 7 日間だけ保存されるように設定しました。

シナリオ 18. 設定のバックアップの作成

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、正常な状態をキャプチャしておくといよいでしょう。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環境内の管理ワークステーションに保存します。そうすることで、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ミスをした場合、またはその他の設定不良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、正常な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り、工場出荷時の初期状態にリセットされたりした場合は、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。

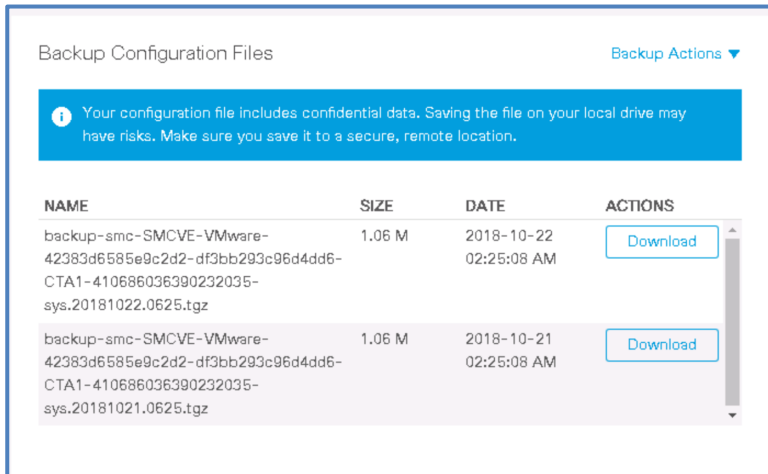
1. **Chrome** で **SMC** のブックマークを使用して、SMC Web インターフェイスに戻ります。
 - a. ユーザ名 **admin** とパスワード **C1sco12345** を使用して、アプライアンスにログインします。
2. **歯車アイコン**をクリックし、メニューから [Central Management] を選択します。



3. [SMC] の [アクション (Actions)] アイコンを選択し、[サポート (Support)] メニューオプションを選択します。

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP A	ACTIONS
Up	90 Days or Less	FCNF	Flow Collector FCNFVE-VMware-4238c82980faa98-d2e95f2d380bcbf	198.	Edit Appliance Configuration
Up	90 Days or Less	FS	Flow Sensor FSVE-VMware-4238897e908c994-caefda667b968bd9	198.	View Appliance Statistics Manage Licenses
Up	90 Days or Less	SMC	SMC SMCVE-VMware-42383b585e9c2d2-of3bb293c96d4d06	198.	Support
Up	90 Days or Less	UDPD	UDP Director UDVE-VMware-4238e3d05d7978c5-8535c0d0f1a826c8	198.	Reboot Appliance Shut Down Appliance Remove This Appliance

4. 毎日の設定バックアップにより、アプライアンス自体に保存されたバックアップの一覧が表示されます。



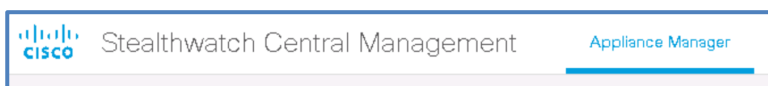
5. [バックアップアクション (Backup Actions)]、[バックアップの作成 (Create Backup)] を順にクリックして、オンデマンドのバックアップを作成します。



6. バックアップが作成されると、上部のリストに表示されます。該当するバックアップの [ダウンロード (Download)] ボタン、[保存 (Save)] の順にクリックします。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。



7. [アプライアンスマネージャ (Appliance Manager)] をクリックし、[Central Management] の [インベントリ (Inventory)] ページに戻ります。



8. 残りのすべての Stealthwatch アプライアンスについてこのシナリオの手順を繰り返し、最新の設定バックアップを作成してダウンロードします。
 - a. フローコレクタ
 - b. フローセンサー
 - c. UDP Director

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。

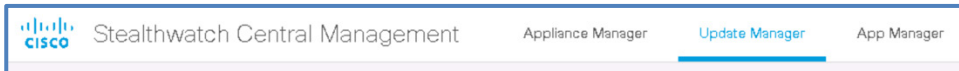
シナリオのまとめ

このシナリオでは、すべてのアプライアンスについて設定のバックアップを実行して、バックアップファイルを管理ワークステーションに保存しました。これによって、アプライアンスに障害が発生した場合やお客様が設定ミスをした場合に、インストールプロセス全体を再実行することなく、環境を以前の設定に確実に戻すことができます。

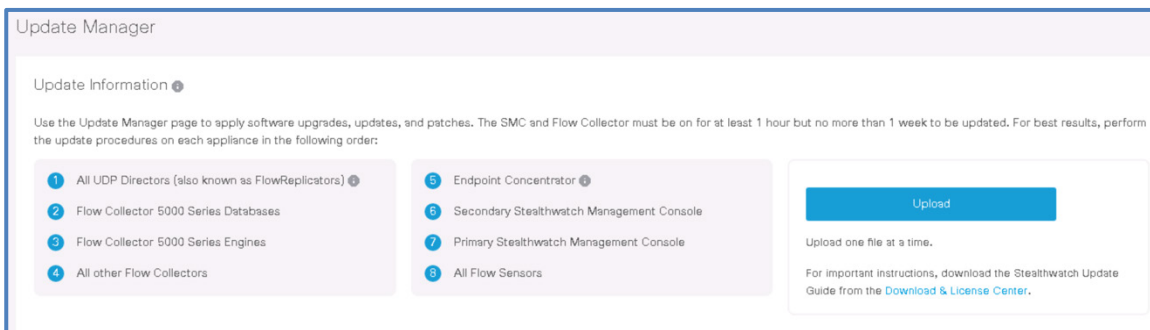
シナリオ 19. Stealthwatch のパッチ適用 : Central Management

導入環境はいずれ、パッチの適用やアップグレードが必要となります。このプロセスの経験を積めるように、このラボでは SMC のパッチインストールについて説明します。最新の設定バックアップはすでに作成してダウンロードしているため、更新を開始する準備は整っています。

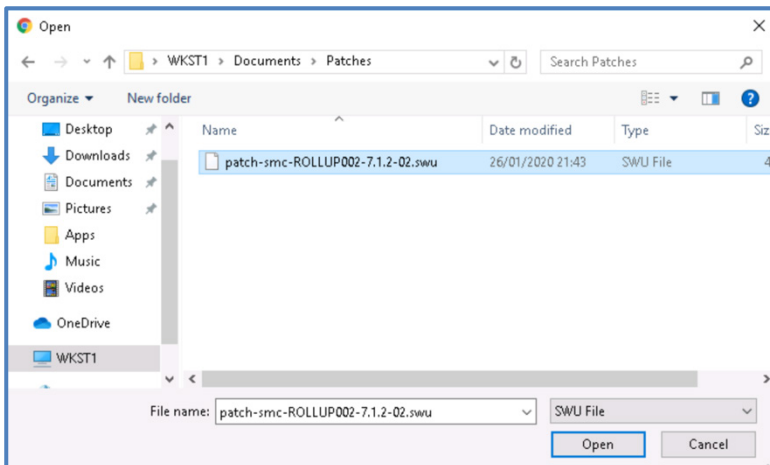
1. SMC の [Central Management] ページで、[更新マネージャ (Update Manager)] タブをクリックします。



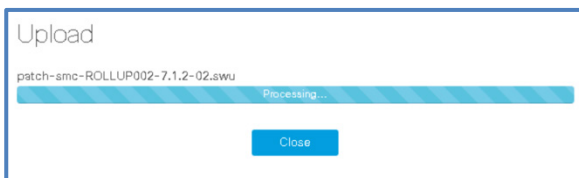
2. [アップロード (Upload)] をクリックして、パッチを Central Management にアップロードします。



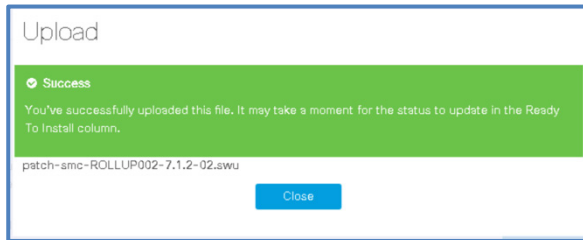
3. [WKST1] > [ドキュメント (Documents)] > [パッチ (Patches)] の順に移動して **patch-smc-ROLLUP002-7.1.2-02.swu** をクリックし、[開く (Open)] をクリックします。







4. ファイルが SMC にアップロードされます。[閉じる (Close)] はまだクリックしないでください。



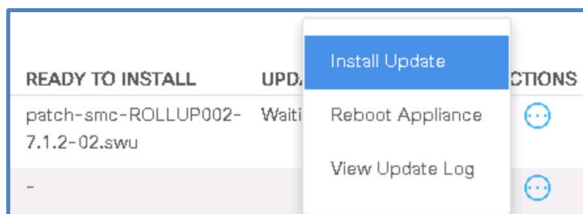
5. 成功メッセージが表示されたら、[閉じる (Close)] をクリックします。



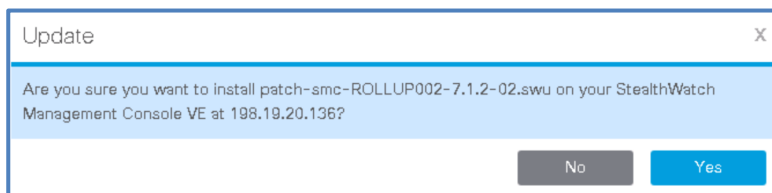
6. SMC のパッチが [インストール待機中 (Waiting to Install)] としてリストに表示されます。これが表示されない場合は、ブラウザウィンドウを更新します。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	SMC	198.19.20.136	2 days ago	7.1.2 2019.10.28.2033-0	patch-smc-ROLLUP002- 7.1.2-02.swu	Waiting to Install	
Flow Collector	FCNF	198.19.20.137	2 days ago	7.1.2 2019.10.28.2031-0	-	-	
Flow Sensor	FS	198.19.20.138	2 days ago	7.1.2 2019.10.28.2028-0	-	-	
UDP Director	UDPD	198.19.20.139	2 days ago	7.1.2 2019.10.28.2027-0	-	-	

7. SMC の [アクション (Actions)] アイコンをクリックして、[更新のインストール (Install Update)] を選択します。



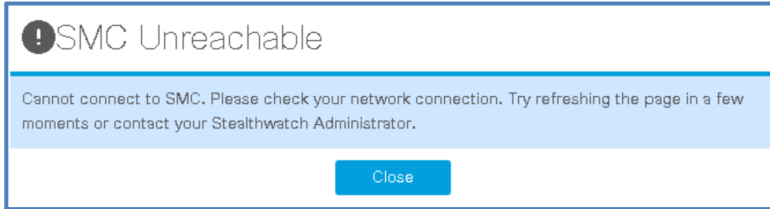
8. [はい (Yes)] をクリックして更新を確定します。



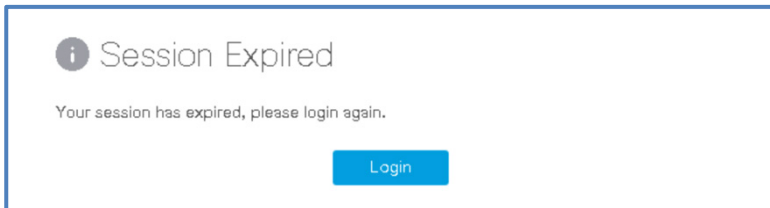
9. [更新ステータス (Update Status)] が [インストール中 (Installing)] に変わります。(少し時間がかかる場合があります。しばらくお待ちください)。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS
SMC	SMC	198.19.20.136	2 days ago	7.1.2 2019.10.28.2033-0	patch-smc-ROLLUP002- 7.1.2-02.swu	Installing

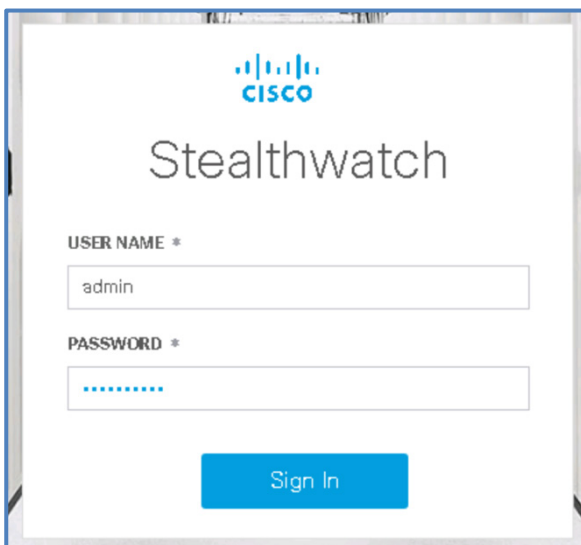
10. SMC への接続が失われたら、[閉じる (Close)] をクリックします。



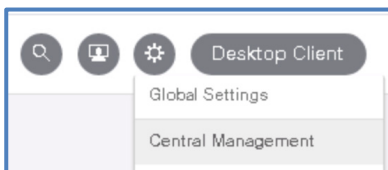
11. 必要に応じて、[Central Management] の Web ブラウザページを更新します。SMC によりサービスがリブート/再起動されると、次のような [セッションの期限切れ (Session Expired)] のポップアップメッセージまたは別の Web ページが表示されます。これにはかなり時間がかかる場合があります。



12. **admin** および **C1sco12345** を使用してログインします。



13. [Central Management] に戻ります。



14. [更新マネージャ (Update Manager)] をクリックします。



15. SMC の [インストール準備完了 (Ready to Install)] と [更新ステータス (Update Status)] の両方の表示が消えていることを確認します。SMC の [アクション (Actions)] アイコンをクリックして、[更新ログの表示 (View Update Log)] を選択します。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPD.	ACTIONS
SMC	SMC	198.19.20.136	2 days ago	7.1.2 2019.10.28.2033-0	-		Install Update Reboot Appliance View Update Log
Flow Collector	FCNF	198.19.20.137	2 days ago	7.1.2 2019.10.28.2031-0	-		

16. このログは、新しい Chrome タブで開きます。ROLLUP002 ファイルが記載されています。ログファイルの最下部までスクロールし、プロセスが正常に完了したことを確認します。

```

2020-01-26 22:43:52,618 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/90-FILE-PLACER]
2020-01-26 22:43:52,861 - patch-smc-ROLLUP002-7.1.2-02 - INFO - Command produced the following output on stdout:
2020-01-26 22:43:52,861 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Executing 90-FILE-PLACER with arg: /lancope/var/admin/upgrade/extract/patch-smc-ROLLUP002-7.1.2-02/swu.ini
2020-01-26 22:43:52,861 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >
2020-01-26 22:43:52,861 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:43:52,861 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/91-REDEPLOYWARFILES]
2020-01-26 22:44:55,431 - patch-smc-ROLLUP002-7.1.2-02 - INFO - Command produced the following output on stdout:
2020-01-26 22:44:55,431 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >WAR file redeploy true
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Stopping tomcat...
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Removing old deployment areas...
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >['/bin/rm', '-rf', '/lancope/tomcat/webapps/smc', '/lancope/tomcat/webapps/smc-client', '/lancope/tomcat/webapps/lc-landing-page', '/lancope/tomcat/webapps/smc-core', '/lancope/tomcat/webapps/flow-receiver', '/lancope/tomcat/webapps/cloud-dashboard', '/lancope/tomcat/webapps/smc-configuration', '/lancope/tomcat/webapps/smc-users']
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Starting tomcat...
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:44:55,432 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/92-NAPATECH-FIRMWARE-UPDATE]
2020-01-26 22:44:55,518 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:44:55,519 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/95-IMAGE-PLACER]
2020-01-26 22:44:55,591 - patch-smc-ROLLUP002-7.1.2-02 - INFO - Command produced the following output on stdout:
2020-01-26 22:44:55,591 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Executing 95-IMAGE-PLACER with arg: /lancope/var/admin/upgrade/extract/patch-smc-ROLLUP002-7.1.2-02/swu.ini
2020-01-26 22:44:55,591 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >
2020-01-26 22:44:55,591 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:44:55,592 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/96-FIXORUBCFG]
2020-01-26 22:44:56,345 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:44:56,345 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/97-RESTARTSERVICES]
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - Command produced the following output on stdout:
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Verica reboot false
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >tomcat restart true
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >engine restart false
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >uwsgi restart false
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >
2020-01-26 22:45:38,540 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:45:38,541 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Running [./EXEC/99-REINITAIDE]
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - Command produced the following output on stdout:
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >Executing 99-REINITAIDE with arg: /lancope/var/admin/upgrade/extract/patch-smc-ROLLUP002-7.1.2-02/swu.ini
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >AIDE initialization succeeded
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - >
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - *** Normal exit status.
2020-01-26 22:45:38,713 - patch-smc-ROLLUP002-7.1.2-02 - INFO - No errors detected in update commands.
Installation program ran to completion.Sun Jan 26 22:45:38 2020
Cleaning up the /lancope/var/admin/upgrade/extract.Sun Jan 26 22:45:38 2020

```

17. SMC のパッチ更新プロセスが完了しました。

シナリオのまとめ

このシナリオでは、お客様環境の Stealthwatch SMC アプライアンスに対するパッチ適用プロセスを実行しました。これにより、既知のバグと問題が、製品を使用するお客様に悪影響を及ぼすのを防げるようになります。

SW フィールドエンジニアラボの完了

Stealthwatch 101 FE トレーニングラボのすべてのシナリオが完了しました。



次に必要な作業

詳細は以下を参照してください。

- Cisco Stealthwatch Tech Talk セッション : <https://communities.cisco.com/docs/DOC-30977>
 - このラボの前提となる学習要件
- Cisco dCloud ヘルプページを参照する : <https://dcloud-cms.cisco.com/help>
- 利用できるすべての Cisco dCloud コンテンツを確認する : <https://dcloud.cisco.com>
- dCloud のお問い合わせ先 : <https://dcloud-cms.cisco.com/help/contact-us-security>

©2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2020年4月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



お問い合わせ先

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>