Cisco Stealthwatch

7.2 インストールおよびコンフィギュレーション ガイド

目次

はじめに 8
概要 8
バーチャル エディション（VE） 8
ハードウェア 8
対象読者 8
プロセス 8
用語 9
略語 10
はじめる前に 11
ハードウェア 11
仮想アプライアンス 12
インストール方法 12
互換 13
VMware 13
KVM 13
ソフトウェアのダウンロード 14
ライセンス 14
TLS 14
サード パーティ製アプリケーション 14
ブラウザ 14
ホスト名 14
ドメイン名 14
NTP サーバ 15
タイム ゾーン 15
ハードウェア リソース要件 16
バーチャル エディション（VE）のリソース要件 17
Stealthwatch Management Console VE 18
Stealthwatch Management Console VE 2000 18
Stealthwatch Management Console VE のモデルと容量 19
Flow Collector VE 20
Flow Sensor VE 21
Flow Sensor VE ネットワーク環境 22
Flow Sensor VE トラフィック 22

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

UDP Director VE 23
Endpoint Concentrator 23
データ ストレージ 24
クイック リファレンス ワークフロー 26
Stealthwatch ハードウェア 26
Stealthwatch バーチャルエディション（VE） 26
1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定 27
概要 27
アプライアンスの配置 27
Stealthwatch Management Console 27
Stealthwatch Flow Collector 27
Stealthwatch Flow Sensor 27
統合に関する重要な考慮事項 28
TAP 28
Electrical TAP の使用 29
Optical TAP の使用 29
ファイアウォール外部での TAP の使用 30
ファイアウォール内部に Flow Sensor を配置する 30
SPAN ポート 31
Stealthwatch UDP Director 32
通信用ファイアウォールの設定 33
オープンポート 33
Stealthwatch Management Console（SMC）、Flow Collector、Flow Sensor、および UDP Director 33
Endpoint Concentrator 33
通信ポートおよびプロトコル 34
オプションの通信ポート 35
2. VE インストールファイルのダウンロード 37
インストール ファイル 37
1. Cisco Software Central へのログイン 37
2. ファイルをダウンロードする 38
3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF） 39
概要 39
はじめる前に 39
vCenter を使用した仮想アプライアンス（OVF）のインストール 40

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

プロセスの概要 40
1. VMware Web Client へのログイン 40
2. トラフィックを監視するフロー センサーの設定 40
PCI パススルーによる外部トラフィックのモニタリング 41
複数のホストでの vSwitch の監視 41
設定要件 41
単一のホストでの vSwitch の監視 44
設定要件 44
ポートグループを無差別モードに設定 44
3. 仮想アプライアンスのインストール 46
4. 追加モニタリング ポートの定義（Flow Sensor のみ） 50
3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO） 53
概要 53
はじめる前に 53
ESXi スタンドアロン サーバへの仮想アプライアンス（ISO）のインストール 53
プロセスの概要 53
1. VMware Web Client へのログイン 54
2. ISO からの起動 56
3c. KVM ホストへの仮想アプライアンスのインストール（ISO） 58
概要 58
はじめる前に 58
KVM ホストへの仮想アプライアンスのインストール（ISO） 59
プロセスの概要 59
1. KVM ホストへの仮想アプライアンスのインストール 59
トラフィックのモニタリング 59
設定要件 59
KVM ホストへの仮想アプライアンスのインストール 59
2. Open vSwitch への NIC および無差別ポートの監視の追加（Flow Sensor のみ） 66
4. IP アドレスの設定 68
IP アドレスの設定 68
トラブルシューティング 71
証明書エラー 71
アプライアンスへのアクセス 72
5. Stealthwatch システムの設定 73
準備 73

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンス設定ツールの要件 73
管理対象 73
SMC フェールオーバー 73
ベストプラクティス 74
設定の順序 75
1. ログイン 76
2. アプライアンスの設定 76
3. Stealthwatch Management Console の登録 80
4. [集中管理(Central Management)] へのアプライアンスの追加 81
5. アプライアンス ステータスの確認 83
6. アプライアンス設定の完了 85
UDP Director 86
転送ルールの設定 86
ハイアベイラビリティの設定 87
プライマリ ノードおよびセカンダリ ノード 87
要件 88
1. プライマリ UDP Director HA の設定 88
2. セカンダリ UDP Director HA の設定 89
Flow Sensor 90
1. アプリケーション ID およびペイロードの設定 90
2. アプリケーションを識別するための Flow Sensor の設定(オプション) 93
3. アプライアンスの再起動 93
Endpoint Concentrator 94
エンドポイントコンセントレータのトラブルシューティング 95
7. Stealthwatch デスクトップ クライアントのインストール 97
Windows を使用したデスクトップ クライアントのインストール 97
メモリサイズの変更 98
macOS を使用したデスクトップ クライアントのインストール 98
メモリサイズの変更 99
8. 通信の確認 101
NetFlow データ収集の確認 101
9. ライセンス 103
評価モード 103
SMC フェールオーバー関係の定義 104
脅威インテリジェンスフィードの有効化 105

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ライセンス 105
有効 105
アラームとセキュリティイベントの確認 105
SAML SSO の設定 107
1. 設定の準備 107
2. 信頼ストアへの証明書のアップロード 107
3. サービスプロバイダーの設定 108
4. SSO の有効化 109
5. アイデンティティプロバイダーの設定 110
6. SSO ユーザの追加 110
7. SAML ログインのテスト 111
トラブルシューティング 111
Stealthwatch の概要 112
概要 112
環境の管理 112
動作の調査 112
脅威への対応 113
Central Management 114
Central Management とアプライアンス管理インターフェイス 114
Central Management を開く 115
アプライアンス管理を開く 115
Central Management を通じてアプライアンス管理を開く 115
直接ログインを介してアプライアンス管理を開く 115
アプライアンス設定の編集 116
アプライアンス統計情報の表示 117
Central Management からのアプライアンスの削除 117
Central Management へのアプライアンスの追加 118
SSH の有効化/無効化 119
SSH を開く 119
SSH の有効化 119
SSH の無効化 119
パッチのインストールとソフトウェアのアップデート 120
トラブルシューティング 121
構成チャネルのダウン 121
アプライアンス管理インターフェイスを開く 121

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンス アイデンティティの交換 121
設定後のアプライアンスの変更 122
ホスト名の変更 122
ネットワークドメイン名の変更 122
IP アドレスの変更 123
アプライアンス設定ツールを開く 123
システム設定の概要 123
信頼できるホストの変更 124
工場出荷時のデフォルトへのリセット 124
管理者ユーザの有効化/無効化 125
パスワードのリセットの有効化または無効化 125
パスワードをデフォルト設定にリセット 125
SMC の admin パスワードのリセット 126
admin、root、sysadmin パスワードをデフォルトにリセット 126
パスワードの変更 128
sysadmin パスワードの変更 128
ルート パスワードの変更 129
SMC の admin パスワードの変更 129
他のすべてのアプライアンスの admin パスワードの変更 129
サポートへの問い合わせ 130

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

はじめに

概要

次の Cisco Stealthwatch™ Enterprise ハードウェアおよびバーチャルエディション（VE）アプライアンスを設定するには、このガイドを使用します。

- Stealthwatch Management Console（SMC）
- Stealthwatch Flow Collector
- Stealthwatch Flow Sensor
- Stealthwatch UDP Director
- エンドポイント コンセントレータ

Stealthwatch の詳細については、次のオンライン リソースを参照してください。

- **概要**：https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html [英語]
- **アプライアンス**：https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html [英語]

バーチャル エディション（VE）

このガイドは、仮想アプライアンスをインストールおよび設定するために使用できます。

ハードウェア

Stealthwatch ハードウェアを設定する場合は、この設定を開始する前に Stealthwatch x210 シリーズ ハードウェア インストール ガイド [英語] を使用して物理アプライアンスをインストールします。

対象読者

このガイドは、Stealthwatch 製品のインストールおよび設定を担当するネットワーク管理者とその他の担当者を対象としています。

仮想アプライアンスを設定する場合は、VMware または KVM の基本的な知識があることを前提としています。

専門家によるインストールを希望する場合は、最寄りのシスコ パートナーまたは Cisco Stealthwatch サポートに連絡してください。

プロセス

Stealthwatch アプライアンスをインストールおよび設定するためのプロセスがあることに注意してください。この設定には、次のようなものがあります。

- 設定の順序：このガイドの手順に従い、設定の順序を使用してアプライアンスのインストールとアプライアンスの設定を行ってください。
- **証明書**：アプライアンスは、一意の自己署名アプライアンス アイデンティティ証明書とともにインストールされます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **Central Management**：プライマリ SMC/Central Manager からアプライアンスを管理できます。

詳細については、『リリース ノート』を参照してください。

用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての Stealthwatch 製品に対し「アプライアンス」という用語を使用しています。

「クラスタ」は、StealthWatch Management Console（SMC）で管理される Stealthwatch アプライアンスのグループです。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

略語

このガイドでは、次の略語が使用される場合があります。

略語	定義
DNS	ドメイン ネーム システム（サービスまたはサーバ）
dvPort	分散仮想ポート
ESX	Enterprise Server X
GB	ギガバイト
IDS	侵入検知システム
IPS	侵入防御システム
ISO	International Standards Organization; 国際標準化機構
IT	情報技術
KVM	カーネルベース仮想マシン
MTU	最大伝送ユニット
NTP	ネットワーク タイム プロトコル
OVF	オープン仮想化フォーマット
SMC	Stealthwatch Management Console
TB	テラバイト
UUID	汎用一意識別子
VDS	vNetwork 分散型スイッチ
VE	バーチャル エディション
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

はじめる前に

開始する前に、このガイドを参照して、プロセス、およびインストールと設定を計画するために必要な準備、時間、リソースについて確認してください。

ハードウェア

- **インストール**：このガイドを使用して設定する前に、Stealthwatch x210 シリーズ ハードウェア インストール ガイド [英語] を使用してアプライアンス ハードウェア（物理アプライアンス）をインストールしてください。
- **仕様**：ハードウェア仕様 [英語] は Cisco.com で入手できます。
- **サポートされているプラットフォーム**：各システム バージョンでサポートされているハードウェア プラットフォームについては、Cisco.com の ハードウェアおよびバージョンのサポート一覧表 [英語] を参照してください。
- **ワークフロー**：ハードウェアを設定するために必要な手順を確認するには、「**クイック リファレンス ワークフロー**」を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

仮想アプライアンス

仮想アプライアンスのインストールには、VMware 環境または KVM（カーネルベース仮想マシン）を使用できます。

⚠ インストールを開始する前に、「互換性」情報と「リソース要件」を確認します。

インストール方法

次の表を参照して、インストール方法を選択します。また、インストールを開始する前に、「互換性」と「リソース要件」を確認してください。

方法	設置手順（参照用）	インストールファイル	詳細
VMware vCenter	3a. VMware vCenter	OVF	VMware vCenter を使用して仮想アプライアンスをインストールします。
VMware ESXi スタンドアロンサーバ	3b. VMware ESXi スタンドアロンサーバ	ISO	ESXi スタンドアロンホストサーバに仮想アプライアンスをインストールします。
KVM および Virtual Machine Manager	3c. KVM および Virtual Machine Manager	ISO	KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

互換

VMware 環境または KVM（カーネルベースの仮想マシン）に仮想アプライアンスをインストールする場合は、次の互換性情報を確認してください。

VMware

- 互換性：VMware v6.5 または v6.7。
- **OVF の展開**：Update 2 および vSphere フラッシュ Web クライアントを使用して VMware v6.5 を検証済みです。vSphere の他のクライアントを使用すると、問題が発生する場合があります。ESXi 6.5 Update 2 HTML5 クライアントを使用できますが、システム タイムアウトが発生する可能性があります。
- VMware のアップグレード：Stealthwatch v7.2.x では VMware v6.0 はサポートされていません。Stealthwatch アプライアンスが VMware v6.0 にインストールされている場合は、Stealthwatch を v7.2.x にアップグレードする前に、VMware vCenter と ESXi ホストを v6.5 または v6.7 にアップグレードします。手順については、Stealthwatch 更新ガイド（v7.1.x から 7.2.1）[英語] および VMware のマニュアルの「vSphere 6.0 End of General Support」を参照してください。
- ホストからホストへの **ライブ マイグレーション**（vMotion などを使用）はサポートされていません。
- **スナップショット**：仮想マシンのスナップショットはサポートされていません。

> ⚠ すでにインストールされているカスタム バージョンが上書きされるため、Stealthwatch 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

KVM

- **互換性**：任意の互換 Linux ディストリビューションを使用できます。
- **KVM ホスト バージョン**：KVM ホスト上での仮想マシンのインストールに使用される方法は複数あります。次のコンポーネントを使用して KVM をテストし、適切なパフォーマンスが確認されました。
  - libvirt 3.0.0
  - qemu-KVM 2.8.0
  - Open vSwitch 2.6.1
  - Linux Kernel 4.4.38
- **仮想化ホスト**：最小要件と最適なパフォーマンスについては、「**バーチャル エディション（VE）のリソース要件**」の項を確認し、Cisco.com にあるお使いのアプライアンスのハードウェア仕様シートを参照してください。

> ℹ システム パフォーマンスはホスト環境に左右されます。パフォーマンスは異なる場合があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ソフトウェアのダウンロード

Cisco Software Central を使用して、仮想アプライアンス（VE）のインストールファイル、パッチ、およびソフトウェア更新ファイルをダウンロードします。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。詳細については、「**2. VE インストールファイルのダウンロード**」を参照してください。

ライセンス

Stealthwatch のライセンスを取得するには、スマートアカウントを使用して製品インスタンスを登録し、ライセンスを管理し、レポートを実行し、通知を設定します。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

Stealthwatch を評価モードで使用すると、選択された機能を 90 日間使用できます。Stealthwatch のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。詳細については、「**9. ライセンス**」を参照してください。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。

TLS

Stealthwatch には v1.2 が必要です。

サード パーティ製アプリケーション

Stealthwatch は、アプライアンスへのサード パーティ製アプリケーションのインストールをサポートしていません。

ブラウザ

- **互換性のあるブラウザ**：Stealthwatch は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft エッジを使用して VE OVF または ISO ファイルをインストールすることは推奨されません。

ホスト名

アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

ドメイン名

各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

NTP サーバ

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバがサーバのリストに含まれている場合は削除します。このサーバには問題があることが判明しており、シスコのデフォルトの NTP サーバ リストからはすでに除外されています。

タイム ゾーン

すべての Stealthwatch アプライアンスは協定世界時（UTC）を使用します。

- **仮想ホスト サーバ**：仮想ホスト サーバが正しい時刻に設定されていることを確認します。

> ⚠ 仮想アプライアンスをインストールする仮想ホスト サーバに設定された時刻が正しい時刻に設定されていることを確認します。正しくない場合、アプライアンスを起動できないことがあります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ハードウェア リソース要件

次の表を使用して、Stealthwatch アプライアンスを設定するのに必要な設定値を記録します。

設定	Stealthwatch Management Console（SMC）	Flow Collector	Flow Sensor	UDP Director
ホスト名				
IP アドレス	192.168.1.11*	192.168.1.4*	192.168.1.7*	192.168.1.2*
サブネットマスク				
ゲートウェイ				
DNS サーバ				
NTP サーバ				
メール リレー				

＊これらはデフォルト IP アドレスです。フローコレクタ sFlow のデフォルトは 192.168.1.5 です。Flow Collector 5000 シリーズ データベースのデフォルトは 192.168.1.15 です。

さらに、次の設定を使用することもできます。

フロー データをエクスポートするポート（通常は 2055）_____

ルータの SNMP 読み取り専用コミュニティ文字列 _____

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

バーチャル エディション（VE）のリソース要件

このセクションでは、仮想アプライアンスのリソース要件を示します。この項で提供される表を使用して、Stealthwatch VE アプライアンスをインストールおよび設定するために必要な設定を記録します。

- Stealthwatch Management Console（SMC）
- Flow Collector
- Flow Sensor
- UDP Director
- Endpoint Concentrator
- データストレージ

システムに必要なリソースを確保してください。この手順は、システムパフォーマンスにとって重要です。

必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Stealthwatch Management Console VE

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

リソース割り当てを決定するには、次の仕様を参照してください。詳細については、「Stealthwatch Management Console VE のモデルと容量」を参照してください。

フローコレクタ	同時接続数ユーザ*	必須予約済みメモリ	必須予約済み CPU
1	2	24 GB	3
3	5	32 GB	4
5	10	32 GB	4

*同時ユーザには SMC クライアントを同時に使用するスケジュール済みレポートや個人が含まれます。

Stealthwatch Management Console VE 2000

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

	OVF または ISO	必須最小ハードウェア予約済みメモリ	同等ハードウェア*
RAM	64 GB	64 GB	128 GB
CPU	8	8	36

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

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Stealthwatch Management Console VE のモデルと容量

次に、Stealthwatch Management Console VE のモデルとその容量*を示します。

SMC VE モデル	必須 予約済みメモリ	必須予約済み CPU
SMC VE	≤ 63 GB	最大 7 個
SMC VE 2000	≥ 64 GB	8 つ以上

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Flow Collector VE

Flow Collector VE のリソース要件を決定するには、ネットワークで予想される秒当たりのフローと、モニタすることが予想されるホストとエクスポータ数を決める必要があります。リソース要件を決定するには、次の仕様を参照してください。

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

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Flow Sensor VE

Stealthwatch では、Flow Sensor VE の NIC の数に応じて、さまざまなタイプの Flow Sensor VE が用意されています。

- **キャッシュ**:[フローキャッシュサイズ(Flow Cache Size)] 列には、FlowSensor が同時に処理できるアクティブフローの最大数が示されます。キャッシュは予約済みメモリの量で調整され、フローは 60 秒ごとにフラッシュされます。[フローキャッシュサイズ(Flow Cache Size)] を使用して、モニタ対象トラフィックの量に対して必要なメモリの容量を計算します。
- 要件:環境に必要なリソースの量は、さまざまな可変的要因(平均パケットサイズ、バーストレート、その他のネットワークとホストの状況)に応じて異なります。

NIC – モニタリングポート(1 Gb)	必須予約済み CPU	必須最小ハードウェア予約済みメモリ	予測されるスループット	フローキャッシュサイズ(同時フローの最大数)
1	2	4 GB	850 Mbps	32,766
2	4	8 GB	1,850 Mbps PCI パススルーとして設定されているインターフェイス(igb/ixgbe 準拠または e1000e 準拠)	65,537
4	8	16 GB	3,700 Mbps PCI パススルーとして設定されているインターフェイス(igb/ixgbe 準拠または e1000e 準拠)	131,073

オプション:物理 VM ホストで 1 つ以上の 10G NIC を使用できます。

これらの図は、次を搭載した Cisco UCS C220 M4 でのテストに基づいています。

- **プロセッサ**: 2 基の Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40 GHz、2 個のソケット、ソケットあたり 12 コア
- **メモリ**:128 GB
- **ストレージ**:800 GB
- **ESXi**:VMware vSphere 6.7.0
- **モニタリング インターフェイス**:PCI パススルーおよび 1 Gbps/10 Gbps インターフェイス

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Flow Sensor VE ネットワーク環境

Flow Sensor VE をインストールする前に、ご使用のネットワーク環境のタイプを確認してください。このガイドは、Flow Sensor VE でモニタできるすべてのネットワーク環境を扱っています。

互換性:Stealthwatch は VDS 環境をサポートしていますが、VMware Distributed Resource Scheduler(VM-DRS)をサポートしていません。

仮想ネットワーク環境:Flow Sensor VE は、次のタイプの仮想ネットワーク環境を監視します。

- 仮想ローカル エリア ネットワーク(VLAN)トランキングを使用したネットワーク
- (ローカル ポリシーなどの理由で)1 つ以上の VLAN でパケット モニタリング デバイスの接続が禁止されている、分離した VLAN
- プライベート VLAN
- ハイパーバイザ ホスト(VLAN 以外)

統合:統合情報については、「Stealthwatch Flow Sensor」を参照してください。

Flow Sensor VE トラフィック

フロー センサーでは、次の Ethertype でトラフィックを処理します。

Ethertype	プロトコル
0x8000	通常の IPv4
0x86dd	通常の IPv6
0x8909	SXP
0x8100	VLAN
0x88a8 0x9100 0x9200 0x9300	VLAN QnQ
0x8847	MLPS ユニキャスト
0x8848	MLPS マルチキャスト

フロー センサーは、最上位の MPLS ラベルまたは VLAN ID を保存し、エクスポートします。パケットを処理している場合は、他のラベルをバイパスします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

UDP Director VE

UDP Director VE では、仮想マシンが次の要件を満たすことが必要です。

- 8 GB RAM
- **シックまたはシン プロビジョニング**:シン プロビジョニング使用できますが、ディスク容量が制限されている場合はシック プロビジョニングを推奨します。

Endpoint Concentrator

エンドポイント コンセントレータ 1000 の要件は、次のとおりです。

必須予約済み CPU	必須予約済みメモリ	最大 FPS レート
2	8 GB	20,000

> 導入に必要なエンドポイント コンセントレータの数を決定する際に、フロー コレクタの容量を考慮する必要があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

データ ストレージ

アプライアンスのデータ ストレージは、アプライアンスが再起動すると自動的に拡張されます。また、パフォーマンスを向上させるために、アプライアンスのリソース割り当てを拡張することもできます。次の情報を使用して、各アプライアンスのストレージを割り当てます。

> システムに必要なリソースを確保してください。この手順は、システムパフォーマンスにとって重要です。
>
> ⚠ 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

- **拡張の計算**:仮想アプライアンスはデータ ストレージにサーバの約 75% を使用し、25% をオペレーティング システムとキャッシュに残します。したがって、必要な容量より、常に 40 % 多くデータ ストレージを拡張します。
- FPS の計算:毎日のシステム平均の毎秒 1,000 フロー(FPS)ごとに 1 GB 以上のデータ ストレージを割り振り、フローを保存する日数を乗じた容量を割り当てます。たとえば、システムの平均が 2,000 FPS で 30 日間フローを保存するには、60 GB(2 X 30)以上のデータ ストレージ容量を割り当てます。
- **Syslog**:外部イベント処理(syslog)機能を使用する場合は、より多くのメモリおよび処理リソースが必要です。
- データストレージ:次の表を使用して、各アプライアンスに必要なデータストレージを決定します。
- **再起動**:ハイパーバイザ ホストで別の方法を使用して仮想マシンのメモリを増加させる場合は、変更を保存した後にアプライアンスを再起動します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Stealthwatch VE モデル	必須最小データストレージ	最大数アドレス指定可能ストレージ/同等ハードウェア
Stealthwatch Management Console VE	150 GB	5.6 TB
Stealthwatch Management Console VE 2000	200 GB	7.2 TB
Flow Collector NetFlow VE	200 GB	1 TB
Flow Collector NetFlow VE 2000	600 GB	2 TB
Flow Collector NetFlow VE 4000	1.5 TB	7.2 TB
Flow Collector sFlow VE	200 GB	1 TB
Flow Collector sFlow VE 2000	600 GB	2 TB
Flow Collector sFlow VE 4000	1.5 TB	7.2 TB
Flow Sensor	100 GB	
UDP Director	100 GB	

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

クイック リファレンス ワークフロー

このガイドでは、Stealthwatch システムのインストールおよび設定に必要な情報を提供します。必要な情報を素早く見つけ、セットアップに適用されない情報をスキップできるように、リンクを掲載してあります。

Stealthwatch ハードウェア

次のワークフローを使用して、Stealthwatch ハードウェアが管理対象になり、他のアプライアンスと通信できるように設定します。

1. Stealthwatch x210 シリーズ ハードウェア インストレーション ガイド [英語] を使用して、Stealthwatch 物理アプライアンスをインストールします。
2. 「**はじめに**」の項および「**ハードウェア リソース要件**」を参照して設定を計画します。
3. 「**5. Stealthwatch システムの設定**」に進み、このガイドの終わりまで指示に従います。

Stealthwatch バーチャルエディション（VE）

次のワークフローを使用して、仮想アプライアンスをインストールおよび設定します。

1. 「**はじめに**」の項および「**バーチャル エディション（VE）のリソース要件**」を参照して VE のインストールおよび設定を計画します。
2. このガイドの次の手順を使用して、仮想アプライアンスをインストールします。

    - **1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定**
    - **2. VE インストールファイルのダウンロード**
    - **インストール方法の選択：**
        - **3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF）**
        - **3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO）**
        - **3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**
    - **4. IP アドレスの設定**

3. 「**5. Stealthwatch システムの設定**」に進み、このガイドの終わりまで指示に従います。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定

概要

仮想アプライアンスをインストールする前に、次の手順を実行してネットワークを準備します。

1. **アプライアンスの配置**
2. **通信用ファイアウォールの設定**
3. **Stealthwatch Flow Sensor**

アプライアンスの配置

設置する各アプライアンスの配置情報を確認します。

- Stealthwatch Management Console（SMC）
- Flow Collector
- Flow Sensor
- UDP Director

Stealthwatch Management Console

管理デバイスである Stealthwatch Management Console は、データを送信してくるすべてのデバイスにアクセス可能なネットワーク上に設置します。

Stealthwatch Management Console のフェールオーバー ペアがある場合は、プライマリコンソールとセカンダリコンソールを物理的に離れた場所に設置することをお勧めします。この戦略により、ディザスタリカバリ作業（必要な場合）が強化されます。

Stealthwatch Flow Collector

収集およびモニタリング デバイスである Stealthwatch Flow Collector は、Flow Collector にデータを送信する NetFlow または sFlow デバイス、および管理インターフェイスへのアクセスに使用する予定のすべてのデバイスにアクセス可能なネットワーク上の場所に設置する必要があります。

Flow Collector をファイアウォールの外に配置する場合は、[任意のエクスポータからのトラフィックを許可する（Accept traffic from any exporter）] の設定をオフにすることをお勧めします。

Stealthwatch Flow Sensor

IP アクティビティの監視と記録のために、パッシブ モニタリング デバイスとして Stealthwatch Flow Sensor をネットワーク上の複数のポイントに配置できます。これにより、ネットワークの整合性が保護され、セキュリティ違反が検出されます。Flow Sensor には、中央またはリモートのいずれかの管理機能を実装する統合型 Web ベースの管理システムがあります。

次のように、企業ネットワーク上の重要セグメントに Flow Sensor VE アプライアンスを配置すると最も効果的です。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **ファイアウォールの内側**。トラフィックをモニタして、ファイアウォール違反が発生したかどうかを確認できます。
- **ファイアウォールの外側**。トラフィック フローをモニタして、ファイアウォールにとって脅威となるものを分析できます。
- **ネットワーク上の機密セグメント**。不満を持つ従業員やルート アクセス権限を持つハッカーに対する保護を実現できます。
- **リモート オフィス**。リモート オフィスはネットワーク拡張において脆弱なロケーションです。
- **ビジネス ネットワーク**。プロトコルの使用を管理できます（たとえば、ハッカーが Telnet や FTP を実行して顧客の金融データを侵害しているかどうかを確認するには、トランザクション サービス サブネット上に配置します）。

統合に関する重要な考慮事項

Stealthwatch Flow Sensor VE は、さまざまなネットワークトポロジ、テクノロジー、コンポーネントと統合できる十分な多様性を備えています。Flow Sensor VE をインストールする前に、ネットワークとそのモニタ方法についていくつかの事項を決定する必要があります。次を確認することが重要です。

- ネットワークのトポロジーと、特定の監視ニーズを分析します。
- モニタ対象ネットワークとの間でネットワーク伝送を受信し、必要に応じて内部ネットワーク伝送も受信できるように、Flow Sensor を接続します。
- Flow Sensor を使用して物理ネットワークトラフィックを監視する場合に最適なパフォーマンスを得るには、基盤の物理ホストの NIC に直接アクセスして（igb または e1000e 準拠の PCI パススルーを使用するなど）、Flow Sensor VE を設定します。

以降のセクションでは、次のイーサネット ネットワーク デバイスを使用してネットワークに Stealthwatch Flow Sensor VE アプライアンスを統合する方法について説明します。

- TAP
- SPAN ポート

すべてのネットワーク設定をここで説明することはできませんが、モニタリングの要件に最適な設定を決定するうえで、記載されている例を参考にすることができます。これらの例は物理ネットワークのシナリオを説明するものですが、仮想ホストも同じような方法で設定できます。

TAP

テストアクセスポート（TAP）がネットワーク接続に合わせて配置されると、TAP は 1 つ以上の個別のポートで接続を繰り返します。たとえば、イーサネット ケーブルに合わせて配置された Ethernet TAP は、個別のポートでそれぞれの伝送方向を繰り返します。したがって、TAP を使用することは、Flow Sensor を使用するための最も信頼性の高い方法です。使用する TAP のタイプは、ネットワークに応じて異なります。

設定：重要な設定情報については、「Flow Sensor」（「5. Stealthwatch システムの設定」の項）を参照してください。

このセクションでは、次に示す TAP の使用法について説明します。

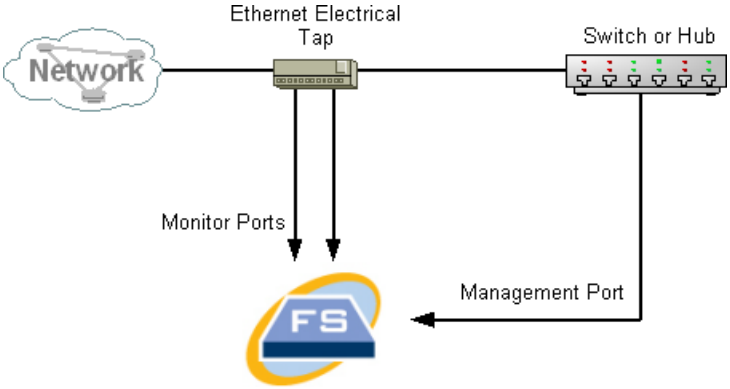
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- Electrical TAP の使用
- Optical TAP の使用
- ファイアウォール外部での TAP の使用
- ファイアウォール内部に Flow Sensor を配置する

TAP を使用するネットワークでは、インバウンドとアウトバウンドの両方のトラフィックをキャプチャする集約 TAP に Flow Sensor VE が接続される場合にのみ、パフォーマンス モニタリング データをキャプチャできます。各ポートで 1 方向のトラフィックだけをキャプチャする単方向 TAP に Flow Sensor VE が接続されている場合、Flow Sensor VE はパフォーマンス モニタリング データをキャプチャしません。

Electrical TAP の使用

次の図は、Ethernet Electrical TAP に接続されている StealthWatch Flow Sensor VE を示しています。この構成を実現するには、図に示すように 2 つの TAP ポートを Flow Sensor VE モニタ ポート 1 と 2 に接続します。

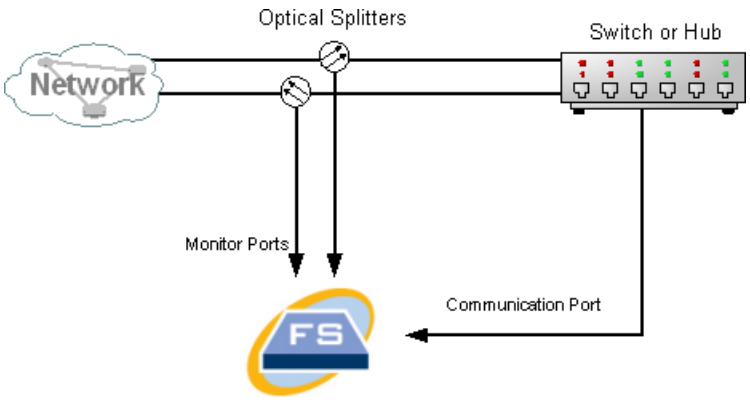


Optical TAP の使用

光ファイバ ベースのシステムには 2 つのスプリッタが 必要です。光ファイバ ケーブル スプリッタを各伝送方向に合わせて配置し、スプリッタを使用して 1 つの伝送方向の光信号を繰り返すことができます。

次の図は、光ファイバ ベースのネットワークに接続されている Flow Sensor を示しています。この構成を実現するには、図に示すように光スプリッタを Flow Sensor VE モニタ ポート 1 と 2 に接続します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



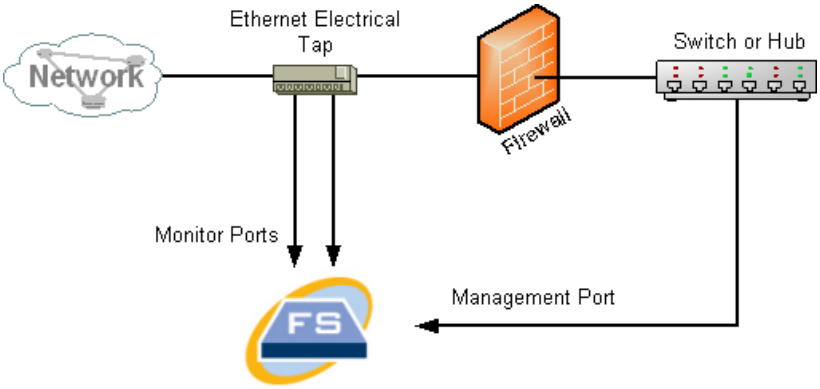
モニタ対象ネットワーク間の接続が光接続である場合、Stealthwatch Flow Sensor VE アプライアンスは 2 つの光スプリッタに接続されます。管理ポートは、モニタ対象ネットワークのスイッチ、または別のスイッチ/ハブに接続されます。

ファイアウォール外部での TAP の使用

Flow Sensor VE によってファイアウォールと他のネットワークの間のトラフィックをモニタするには、Stealthwatch 管理ポートをファイアウォール外部のスイッチまたはポートに接続します。

デバイスの障害が原因でネットワーク全体がダウンしないようにするため、この接続に TAP を使用することを強く推奨します。

次の図に、Ethernet Electrical TAP を使用したこの構成の例を示します。モニタ対象ネットワークのスイッチまたはハブに管理ポートを接続する必要があります。このセットアップは、ネットワークとの間のトラフィックをモニタするセットアップに似ています。

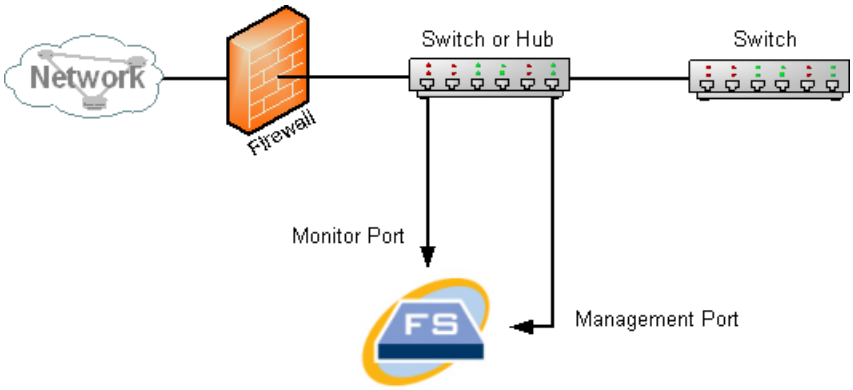


ファイアウォールでネットワーク アドレス変換（NAT）を実行している場合は、ファイアウォール上のアドレスだけを監視できます。

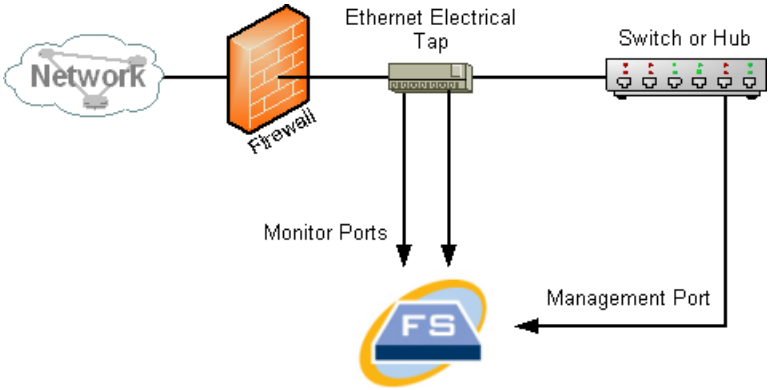
ファイアウォール内部に Flow Sensor を配置する

内部ネットワークとファイアウォールの間のトラフィックをモニタするには、Flow Sensor VE がファイアウォールと内部ネットワークの間のすべてのトラフィックにアクセスできる必要があります。これを実現するには、メイン スイッチでファイアウォールへの接続をミラーリングするミラーポートを設定します。次の図に示すように、Flow Sensor VE モニタ ポート 1 がミラー ポートに接続していることを確認してください。

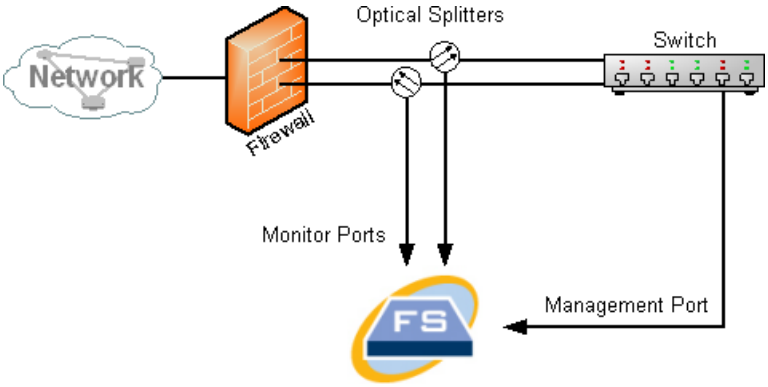
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



TAP を使用してファイアウォール内部のトラフィックをモニタするには、ファイアウォールとメインスイッチまたはハブの間に TAP または光スプリッタを挿入します。TAP の構成を次に示します。



光スプリッタの構成を次に示します。

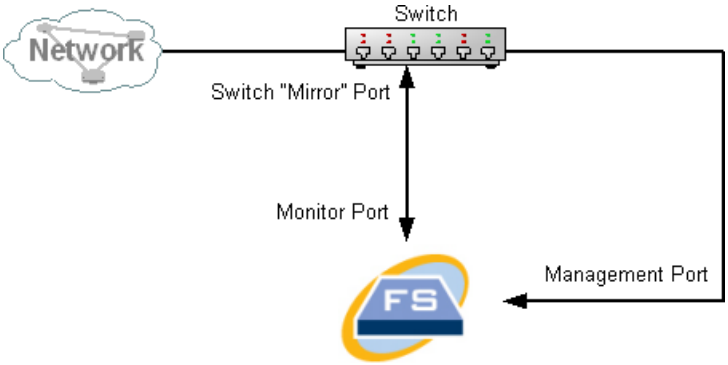


SPAN ポート

また、Flow Sensor VE をスイッチに接続することもできます。ただし、スイッチは各ポートのすべてのトラフィックを繰り返すわけではないので、Flow Sensor VE が正しく機能するには、1 つ以上のスイッチ ポートとの間で伝送されるパケットをスイッチで繰り返すことができる必要があります。このタイプのスイッチ ポートはミラー ポートまたは Switch Port Analyzer（SPAN）と呼ばれることがあります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ネットワークを管理ポート経由で Stealthwatch Flow Sensor VE に接続することでこの構成を実現する方法を次の図に示します。



この構成では、当該ホストとミラー ホストの間のすべてのトラフィックを繰り返すようにスイッチ ポート（ミラー ポート）を設定する必要があります。Flow Sensor VE モニタ ポート 1 をこのミラー ポートに接続する必要があります。これにより、Flow Sensor は当該ネットワークとの間のトラフィック、および他のネットワークへのトラフィックをモニタできるようになります。この場合、すべてのホストまたは一部のホストがスイッチに接続されるネットワーク構成が可能です。

スイッチでネットワークを設定する一般的な方法として、ネットワークをゾーンに区分して、ホスト物理接続ではなく論理接続である仮想ローカル エリア ネットワーク（VLAN）に分けることができます。ミラー ポートが VLAN またはスイッチのすべてのポートをミラーリングするように設定されている場合、Flow Sensor VE は、当該ネットワークとその他のネットワークの内部およびネットワーク間のすべてのトラフィックをモニタできます。

- **設定**：重要な設定情報については、「Flow Sensor」（「5. Stealthwatch システムの設定」の項）を参照してください。
- **ドキュメント**：いずれの場合でも、スイッチの製造元のドキュメントを参照して、スイッチ ミラー ポートの設定方法と、ミラー ポートに繰り返されるトラフィックを確認してください。

Stealthwatch UDP Director

Stealthwatch UDP Director を配置する唯一の要件は、Stealthwatch アプライアンスの他の部分に対して妨げられていない通信パスがあることです。

> シスコの ACI が利用されており、Unicast Reverse Path Forwarding（uRPF）または［サブネットに対する IP 学習を制限（Limit IP learning to subnet）］が有効になっている環境に UDP Director を展開すると、ローカル ネットワークが UDP Director からの転送トラフィックをブロックする可能性があります。ログ データを収集するツールがトラフィックの最初の送信元を知ることができるように、転送ルールの一部として UDP トラフィックをスプーフィングする必要があります。
>
> この場合に UDP Director の正常な動作を保証するには、ネットワークの uRPF または［サブネットに対する IP 学習を制限（Limit IP learning to subnet）］を無効にできる（通常、内部的に）部分に UDP Director を展開します。UDP Director は L3 アウト（IP 学習なし）に配置できます。4.0+ では、VRF ごとにエンドポイント学習を無効にできます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

通信用ファイアウォールの設定

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

オープンポート

Stealthwatch Management Console（SMC）、Flow Collector、Flow Sensor、および UDP Director

ネットワーク管理者に連絡して、次のポートが開いた状態で、無制限のアクセスを提供できることを確認してください。

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Endpoint Concentrator

このセクションのポート情報を使用して、アプライアンスがネットワーク上で通信できるようにネットワークを設定します。

- TCP 22
- TCP 443
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 514
- UDP 2055
- UDP 3514

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

通信ポートおよびプロトコル

Stealthwatch でポートがどのように使用されるかを次の表に示します。

送信元（クライアント）	宛先（サーバ）	ポート	プロトコル
管理者ユーザの PC	すべてのアプライアンス	TCP/443	HTTPS
すべてのアプライアンス	ネットワークの時刻源	UDP/123	NTP
Active Directory	SMC	TCP/389、UDP/389	LDAP
AnyConnect	Endpoint Concentrator	UDP/2055	NetFlow
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	TCP/5222	XMPP
Endpoint Concentrator	Flow Collector	UDP/2055	NetFlow
外部ログ ソース	SMC	UDP/514	SYSLOG
Flow Collector	SMC	TCP/443	HTTPS
UDP Director	Flow Collector：sFlow	UDP/6343	sFlow
UDP Director	Flow Collector：NetFlow	UDP/2055*	NetFlow
UDP Director	サードパーティのイベント管理システム	UDP/514	SYSLOG
Flow Sensor	SMC	TCP/443	HTTPS
Flow Sensor	Flow Collector：NetFlow	UDP/2055	NetFlow
アイデンティティ	SMC	TCP/2393	SSL
NetFlow エクスポータ	Flow Collector：NetFlow	UDP/2055*	NetFlow
sFlow エクスポータ	Flow Collector：sFlow	UDP/6343*	sFlow
SMC	Cisco ISE	TCP/443	HTTPS
SMC	DNS	UDP/53	DNS

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

送信元（クライアント）	宛先（サーバ）	ポート	プロトコル
SMC	Flow Collector	TCP/443	HTTPS
SMC	Flow Sensor	TCP/443	HTTPS
SMC	アイデンティティ	TCP/2393	SSL
SMC	Flow エクスポータ	UDP/161	SNMP
SMC	Endpoint Concentrator	UDP/2055	netflow
SMC	LDAP	TCP/636	TLS
ユーザ PC	SMC	TCP/443	HTTPS

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

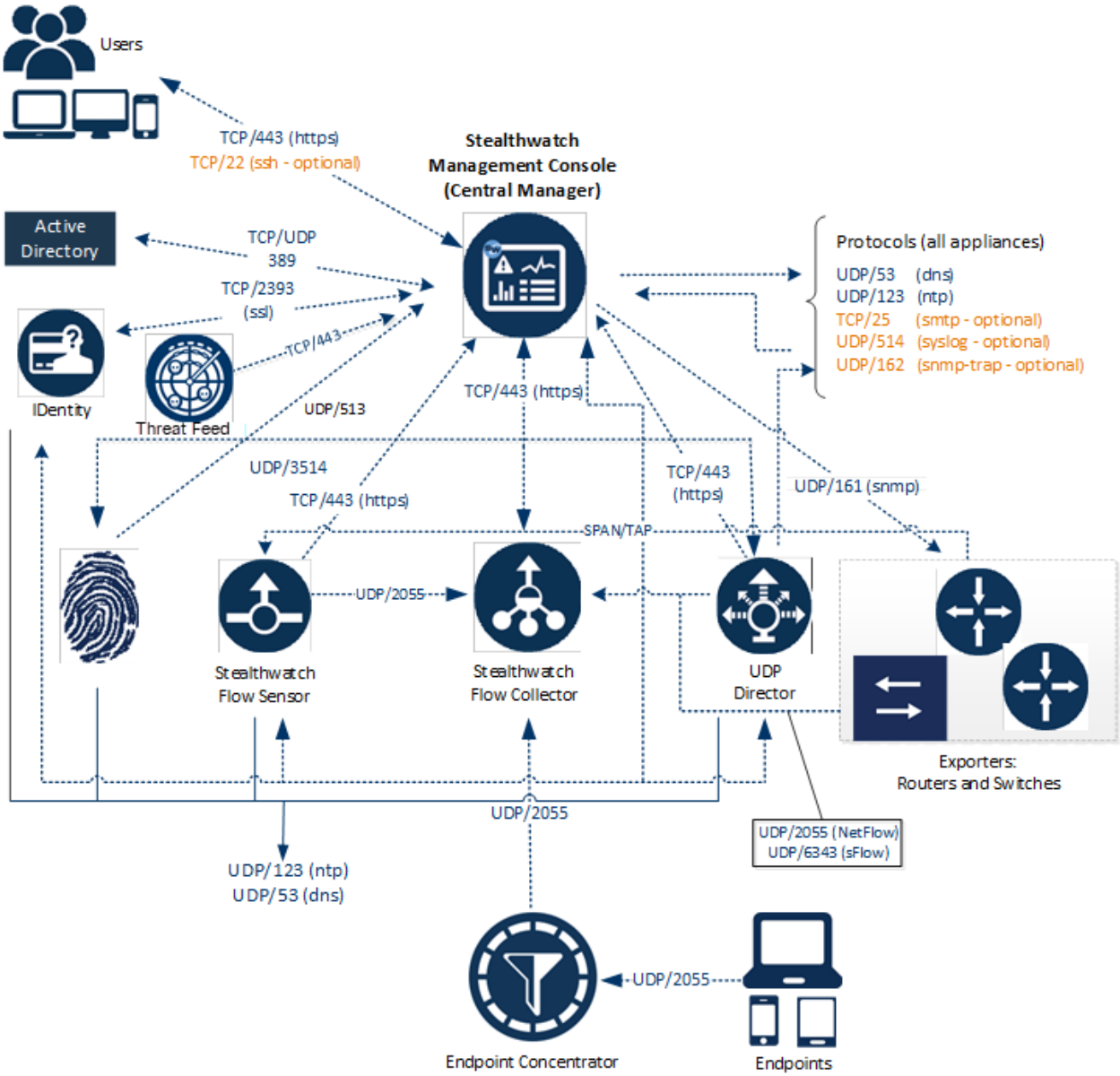
オプションの通信ポート

次の表に、ネットワーク要件によって決まる任意の設定を示します。

送信元（クライアント）	宛先（サーバ）	ポート	プロトコル
すべてのアプライアンス	ユーザ PC	TCP/22	SSH
SMC	サードパーティのイベント管理システム	UDP/162	SNMP－トラップ
SMC	サードパーティのイベント管理システム	UDP/514	SYSLOG
SMC	電子メール ゲートウェイ	TCP/25	SMTP
SMC	脅威インテリジェンスフィード	TCP/443	SSL
ユーザ PC	すべてのアプライアンス	TCP/22	SSH

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

次の図は、Stealthwatch によって使用されるさまざまな接続を示しています。これらのポートの一部はオプションです。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

2. VE インストールファイルのダウンロード

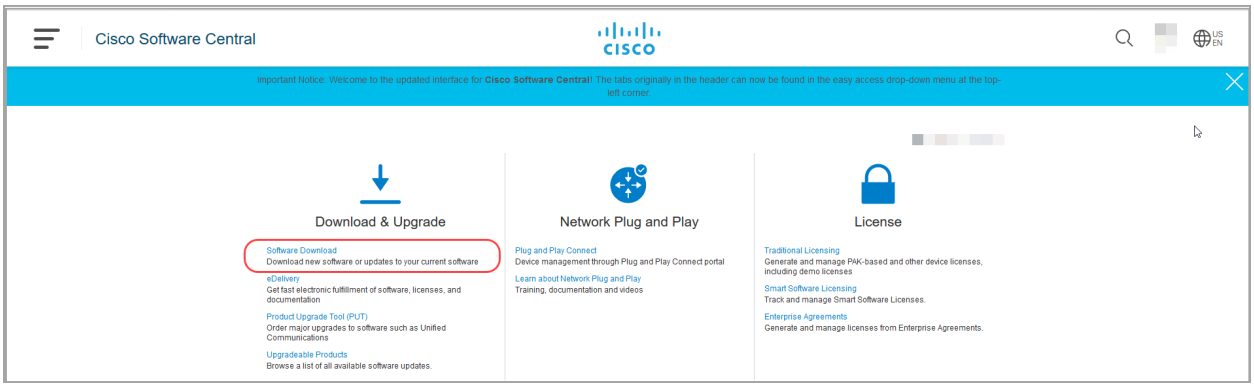
次の手順に従って、仮想アプライアンスのインストール用の OVF または ISO ファイルをダウンロードします。ファイルタイプを判別するには、「**インストール ファイル**」を参照してください。

インストール ファイル

仮想マシン	アプライアンス インストール ファイル	詳細
3a. VMware vCenter	OVF	VMware vCenter を使用した仮想アプライアンスのインストール
3b. VMware ESXi スタンドアロンサーバ	ISO	ESXi スタンドアロンホストサーバがある場合は、この方法を使用してアプライアンスをインストールします。
3c. KVM および Virtual Machine Manager	ISO	KVM および Virtual Machine Manager を使用して仮想アプライアンスをインストールする場合は、この方法を使用します。

1. Cisco Software Central へのログイン

1. https://software.cisco.com で Cisco Software Central にログインします。
2. [ダウンロードとアップグレード(Download and Upgrade)] セクションで、**[ソフトウェアのダウンロード(Software Download)]** を選択します。

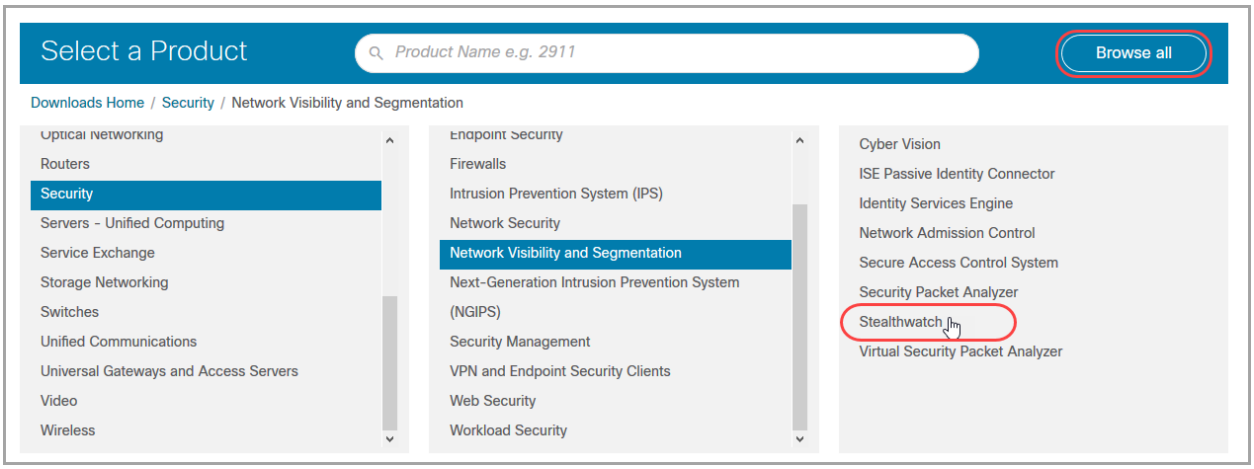


3. [製品の選択(Select a Product)] フィールドが表示されるまで下にスクロールします。
4. Stealthwatch ファイルには、次の 2 つの方法でアクセスできます。

   - **名前で検索**:[製品の選択(Select a Product)] フィールドに **Stealthwatch** と入力します。Enter を押します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **メニューで検索**：[すべてを参照（Browse All）] をクリックします。[セキュリティ（Security）] > [ネットワークの可視性とセグメンテーション（Network Visibility and Segmentation）] > [Stealthwatch] の順に選択します。



2. ファイルをダウンロードする

1. アプライアンスタイプを選択します。

   - Stealthwatch Management Console 仮想アプライアンス
   - Stealthwatch Flow Collector 仮想アプライアンス
   - Stealthwatch Flow Sensor 仮想アプライアンス
   - Stealthwatch UDP Director 仮想アプライアンス
   - エンドポイントコンセントレータ仮想アプライアンス

2. [Stealthwatchシステムソフトウェア（Stealthwatch System Software）] を選択します。
3. [最新リリース（Latest Release）] 列で、[7.2.1]（またはインストールする 7.2.x のバージョン）を選択します。
4. ダウンロード：OVF または ISO インストールファイルを見つけます。[ダウンロード（Download）] アイコンまたは [カートに追加（Add to Cart）] アイコンをクリックします。
5. この手順を繰り返して、アプライアンスタイプごとにファイルをダウンロードします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF）

概要

VMware vCenter を使用して仮想アプライアンスをインストールするには、次の手順に従います。

別の方法を使用する場合は、次を参照してください。

- VMware ESXi スタンドアロンサーバ：「**3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO）**」を使用します。
- KVM：「**3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**」を使用します。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. 互換性：「**互換**」の互換性要件を確認します。
2. リソース要件：「リソース要件」の項を確認し、アプライアンスに必要な割り当てを決定します。 リソースプールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。 詳細については、「**1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定**」を参照してください。
4. ファイル：アプライアンスの OVF ファイルをダウンロードします。 手順については、「**2. VE インストールファイルのダウンロード**」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。正しくない場合、仮想アプライアンスを起動できないことがあります。

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

> ⚠ すでにインストールされているカスタム バージョンが上書きされるため、Stealthwatch 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

vCenter を使用した仮想アプライアンス（OVF）のインストール

VMware vCenter（または同様の環境）がある場合は、次の手順を使用し、OVF を使用して仮想アプライアンスをインストールします。

プロセスの概要

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

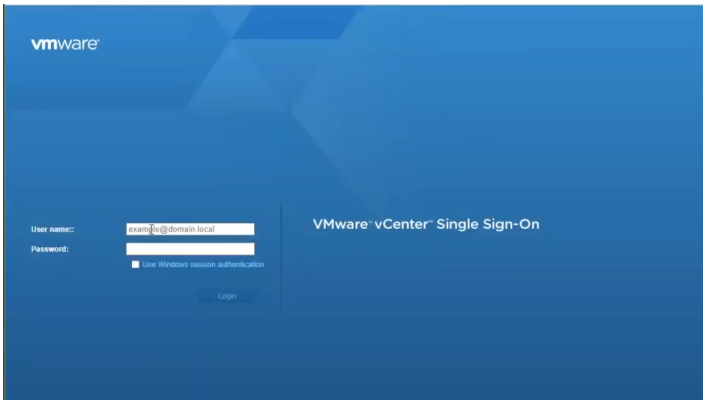
1. VMware Web Client へのログイン
2. トラフィックを監視するフロー センサーの設定
3. 仮想アプライアンスのインストール
4. 追加モニタリング ポートの定義（Flow Sensor のみ）

1. VMware Web Client へのログイン

仮想アプライアンスをインストールするには、VMware Web Client にログインします。

> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. VMware Web クライアントにログインします。



2. フローセンサー：アプライアンスがフローセンサーの場合、「2. トラフィックを監視するフロー センサーの設定」に進みます。

   その他すべてのアプライアンス：アプライアンスがフローセンサーでない場合、「3. 仮想アプライアンスのインストール」に進みます。

2. トラフィックを監視するフロー センサーの設定

Flow Sensor VE には VMware 環境を可視化する機能があり、フロー非対応領域のフロー データを生成できます。各ハイパーバイザ ホスト内部にインストールされる仮想アプライアンスとして、Flow Sensor VE はホスト vSwitch からイーサネット フレームを受動的にキャプチャし、カンバセーション ペア、ビット レート、およびパケット レートに関係する貴重なセッション統計情報を

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

含むフローレコードを作成します。詳細については、「Flow Sensor VE」および「Stealthwatch Flow Sensor」を参照してください。

次の手順を使用して、vSwitch 上のトラフィックを監視するよう、Flow Sensor を次のように設定します。

- **複数のホストでの vSwitch の監視**
- **単一のホストでの vSwitch の監視**

PCI パススルーによる外部トラフィックのモニタリング

また、準拠する PCI パススルーを使用して直接ネットワークモニタリング用に Flow Sensor VE を設定することもできます。

- 要件：igb/ixgbe 準拠 または e1000e 準拠の PCI パススルー。
- リソース情報：「Flow Sensor VE」を参照してください。
- 統合：「**統合に関する重要な考慮事項**」を参照してください。
- 手順：Flow Sensor VE に PCI ネットワーク インターフェイスを追加するには、VMware のマニュアルを参照してください。

複数のホストでの vSwitch の監視

Flow Sensor を使用して、複数の VM またはクラスタの分散 vSwitch 上のトラフィックを監視するには、この項の手順を使用します。

このセクションの内容は、VDS ネットワークにのみ該当します。VDS 以外の環境内にネットワークがある場合は、「**単一のホストでの vSwitch の監視**」に進みます。

設定要件

この設定には、次の要件があります。

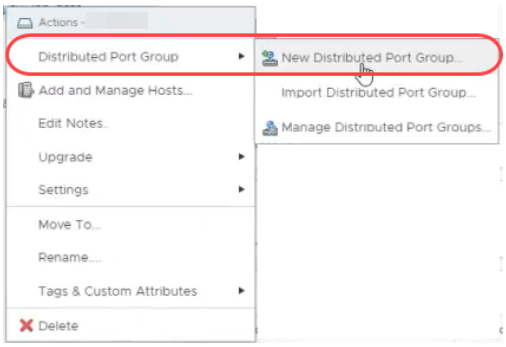
- **分散仮想ポート（dvPort）**：適切な VLAN 設定を行った dvPort グループを Flow Sensor VE で監視する各 VDS に追加します。Flow Sensor VE がネットワーク上の VLAN と VLAN 以外の両方のトラフィックを監視する場合は、それぞれのタイプに 1 つずつ、2 つの dvPort ポートグループを作成する必要があります。
- VLAN ID：環境で VLAN（VLAN トランキングまたはプライベート VLAN 以外）を使用している場合、この手順を実行するには VLAN ID が必要です。
- **無差別モード**：有効
- **無差別ポート**：vSwitch に設定

VDS を使用してネットワークを設定するには次の手順を実行します。

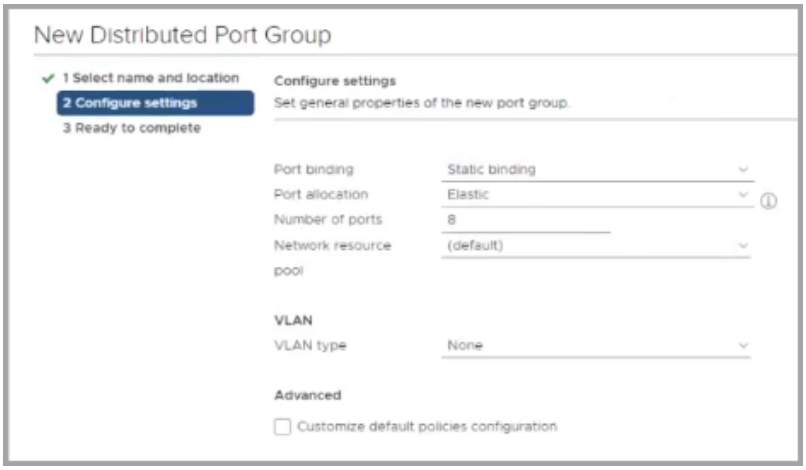
1. ［ネットワーキング（Networking）］アイコンをクリックします。

2. ［ネットワーキング（Networking）］ツリーで、VDS を右クリックします。
3. ［分散ポートグループ（Distributed Port Group）］>［新規分散ポートグループ（New Distributed Port Group）］を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



4. [新規分散ポートグループ（New Distributed Port Group）] ダイアログボックスを使用して、次の手順の仕様を含めてポートグループを設定します。
5. [名前と場所の選択（Select Name and Location）]：[名前（Name）]フィールドに、この dvPort グループを識別する名前を入力します。
6. [設定構成（Configure Settings）]：[ポート数（Number of Ports）] フィールドに、ホストクラスタ内の Flow Sensor VE の数を入力します。



7. [VLANタイプ（VLAN type）] ドロップダウンリストをクリックします。

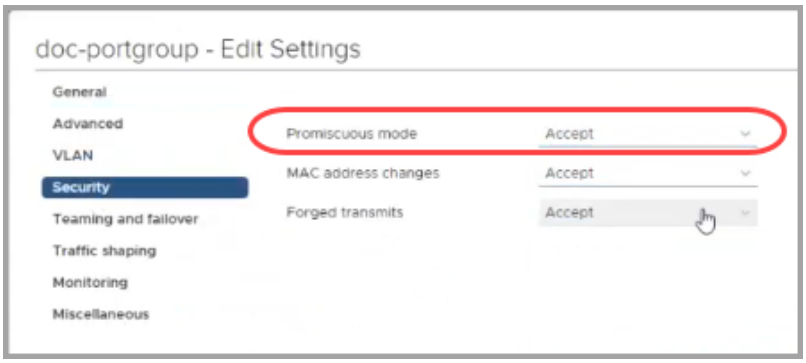
   - 環境内で VLAN を使用しない場合は、[なし（None）] を選択します。
   - 環境内で VLAN を使用する場合は、VLAN タイプを選択します。次のように設定します。

VLAN タイプ	詳細
VLAN	[VLAN ID] フィールドに、ID に一致する番号（1 ～ 4094）を入力します。
VLAN トランキング	すべての VLAN トラフィックを監視するには、[VLANトランク範囲（VLAN trunk range）] フィー

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

VLAN タイプ	詳細
	ルドに **0–4094** と入力します。
プライベート VLAN	ドロップダウンリストから［無差別（Promiscuous）］を選択します。

8. ［終了準備の完了（Ready to Complete）］: 設定を確認します。 ［終了（Finish）］をクリックします。
9. ［ネットワーキング（Networking）］ツリーで、新しい dvPort グループを右クリックします。［設定の編集（Edit Settings）］を選択します。
10. ［セキュリティ（Security）］を選択します。
11. ［無差別モード（Promiscuous Mode）］ドロップダウンリストをクリックします。［許可（Accept）］を選択します。



12. ［OK］をクリックして、ダイアログボックスを閉じます。
13. Flow Sensor VE が VLAN ネットワークトラフィックと非 VLAN ネットワークトラフィックの両方をモニタしますか。
    - 両方を監視する場合は、この「**複数のホストでの vSwitch の監視**」の項の手順を繰り返します。
    - 「いいえ」の場合は、次の手順に進みます。
14. VMware 環境に、Flow Sensor VE による監視対象となる別の VDS がありますか。
    - 別の VDS がある場合は、この「**複数のホストでの vSwitch の監視**」の項の手順を次の VDS で繰り返します。
    - ない場合は、「**3. 仮想アプライアンスのインストール**」に進みます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

単一のホストでの vSwitch の監視

Flow Sensor を使用して、単一ホストの VSwitch 上のトラフィックを監視するには、この項の手順を使用します。

> このセクションの内容は、非 VDS ネットワークにのみ該当します。VDS をネットワークで使用している場合は、「**複数のホストでの vSwitch の監視**」に進みます。

設定要件

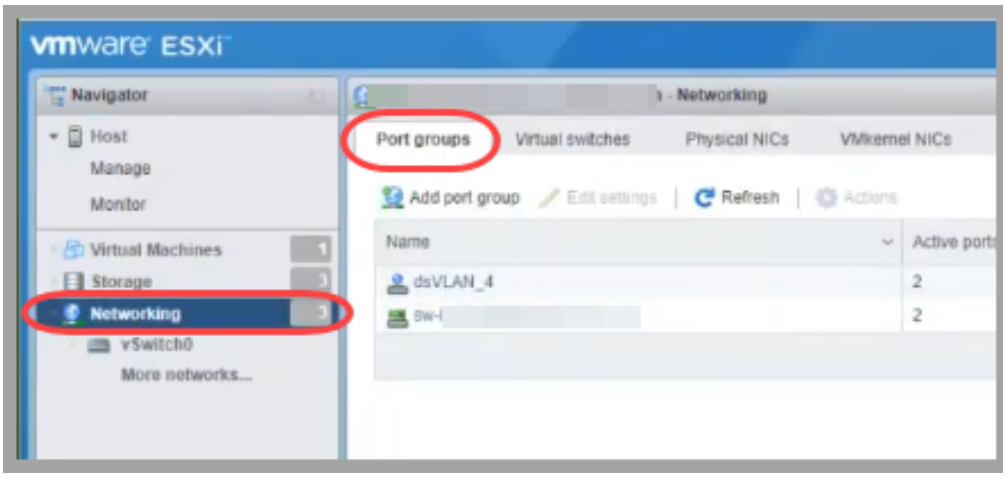
この設定には、次の要件があります。

- **無差別ポートグループ**：Flow Sensor VE で監視する各仮想スイッチに無差別ポートグループを追加します。
- **無差別モード**：有効
- **無差別ポート**：vSwitch に設定

ポートグループを無差別モードに設定

次の手順を使用してポートグループを追加するか、ポートグループを編集して、[無差別（Promiscous）] に設定します。

1. VMware ESXi ホスト環境にログインします。
2. [Networking] をクリックします。



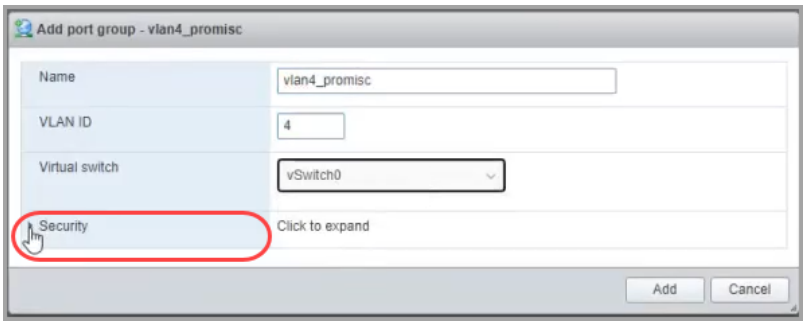
3. [ポートグループ（Port groups）] タブを選択します。
4. 新しいポートグループを作成したり、ポートグループを編集したりできます。
   - [ポートグループの作成（Create Port Group）]：[ポートグループの追加（Add port group）] をクリックします。
   - [ポートグループの編集（Edit Port Group）]：ポートグループを選択します。 [設定の編集（Edit Settings）] をクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

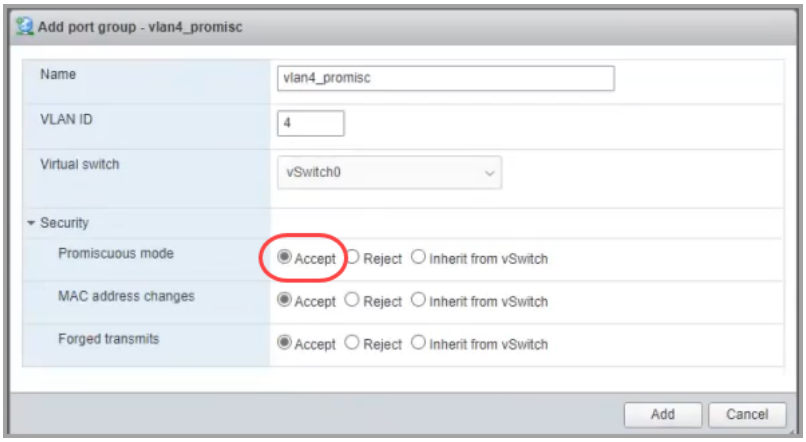
5. ダイアログボックスを使用して、ポートグループを設定します。VLAN ID または VLAN トランキングを設定します。

VLAN タイプ	詳細
VLAN ID（Admin. VLAN ID）	VLAN ID を使用して単一の VLAN を指定します。 [VLAN ID] フィールドに、ID に一致する番号（1 ～ 4094）を入力します。
VLAN トランキング	VLAN トランキングを使用して、すべての VLAN トラフィックをモニタします。デフォルトの範囲は 0 ～ 4095 です。

6. [セキュリティ（Security）] 矢印をクリックします。



7. [無差別モード（Promiscous Mode）]：[同意する（Accept）] を選択します。



8. Flow Sensor VE が、この VMware 環境内の別の仮想スイッチを監視しますか。

   - 「はい」の場合、「**2. トラフィックを監視するフローセンサーの設定**」に戻り、すべての手順を次の仮想スイッチで繰り返します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

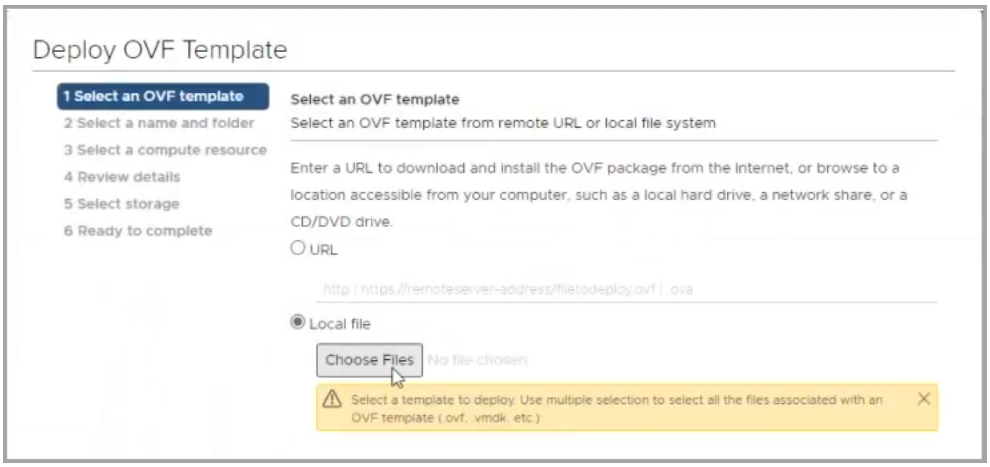
- 「いいえ」の場合は、「**3. 仮想アプライアンスのインストール**」に進みます。

3. 仮想アプライアンスのインストール

仮想アプライアンスをハイパーバイザ ホストにインストールし、仮想アプライアンスの管理およびモニタリング ポートを定義するには、次の手順を実行します。

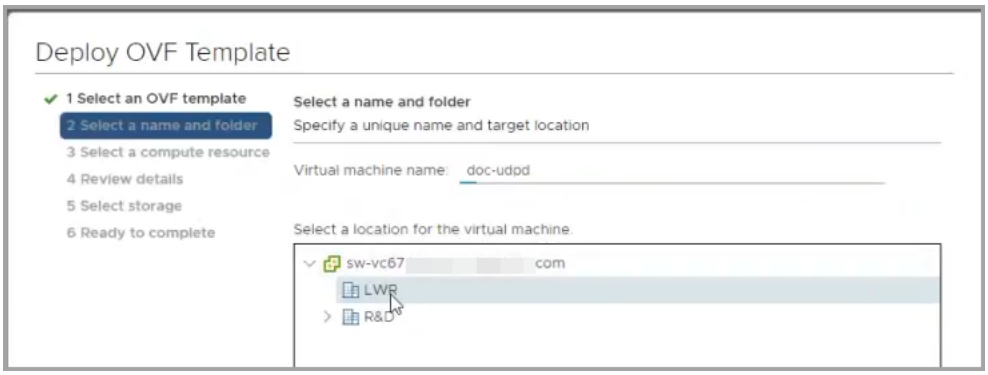
> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. Cisco Software Central からダウンロードした仮想アプライアンス ソフトウェア ファイル（OVF.TGZ）を見つけます。
2. ファイルを解凍するか開いてから、展開します。
   - ファイルを展開するには、フォルダ内のファイルをすべて開き、それらを抽出します。
   - TGZ ファイルの解凍は 2 段階のプロセスで、使用しているソフトウェアによって手順が異なる場合があります。
3. ホストを右クリックします。[OVFテンプレートの展開（Deploy OVF Template）] を選択します。
4. [OVFテンプレートの展開（Deploy OVF template）] ダイアログボックスを使用して、次の手順で指定されているようにアプライアンスを設定します。
5. [OVFテンプレートの選択（Select an OVF template）]：仮想アプライアンス OVF および VMDK ファイルを選択します。

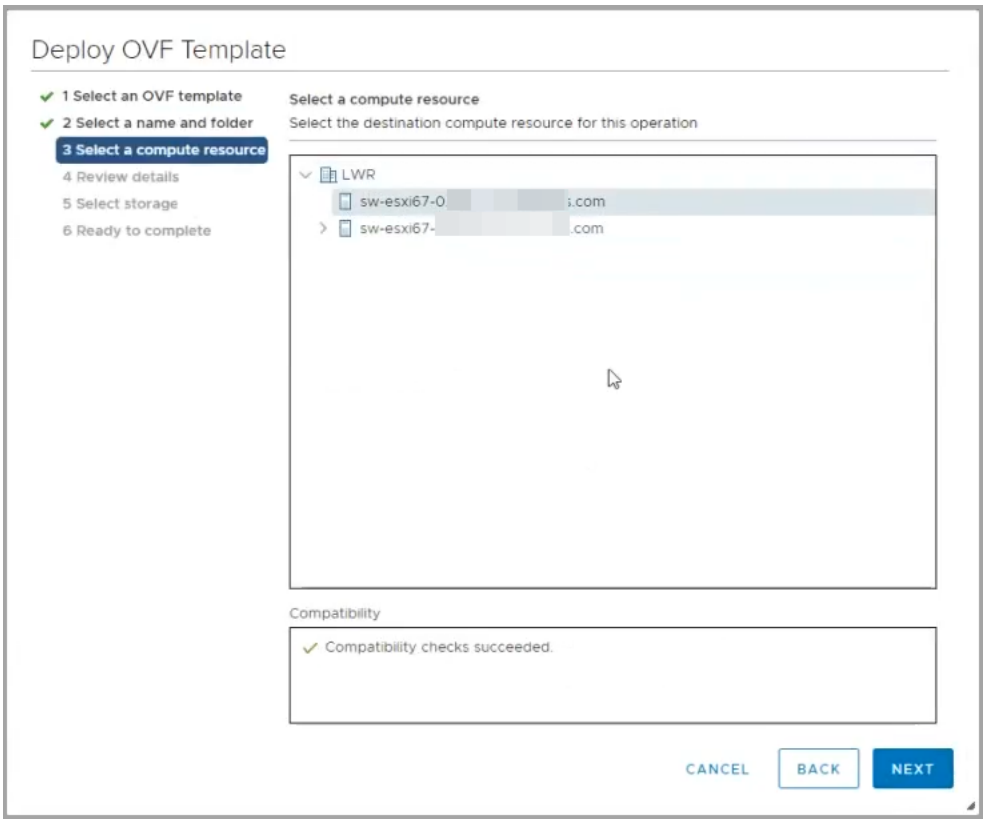


6. [名前とフォルダの選択（Select a name and folder）]：名前が一意になるように名前を変更します。アプライアンスを保存する場所を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



7. [コンピューティングリソースの選択（Select a compute resource）]：宛先のコンピューティングリソースを選択します。



8. [詳細の確認（Review details）]：OVF 導入の詳細を確認します。次の手順でリソースを調整します。

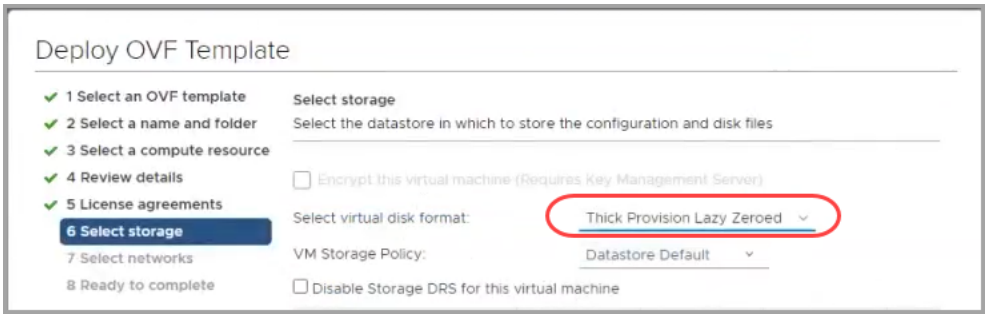
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

9. [ライセンス契約（License agreements）]：エンドユーザライセンス契約を確認して同意します。
10. [ストレージの選択（Select storage）]：データファイルを保存する場所を選択します。

    - [仮想ディスク形式の選択（Select Virtual Disk Format）]：[シックプロビジョニング Lazy Zeroed（Thick Provision Lazy Zeroed）] または [シックプロビジョニング Eager Zeroed（Thick Provision Eager Zeroed）] を選択します。

      シン プロビジョニング形式は、ディスク容量が制限されている場合にのみ使用します。詳細については、VMware のガイドを参照してください。

    - [ストレージ（Storage）]：「リソース要件」を確認して、十分なスペースを割り当てます。



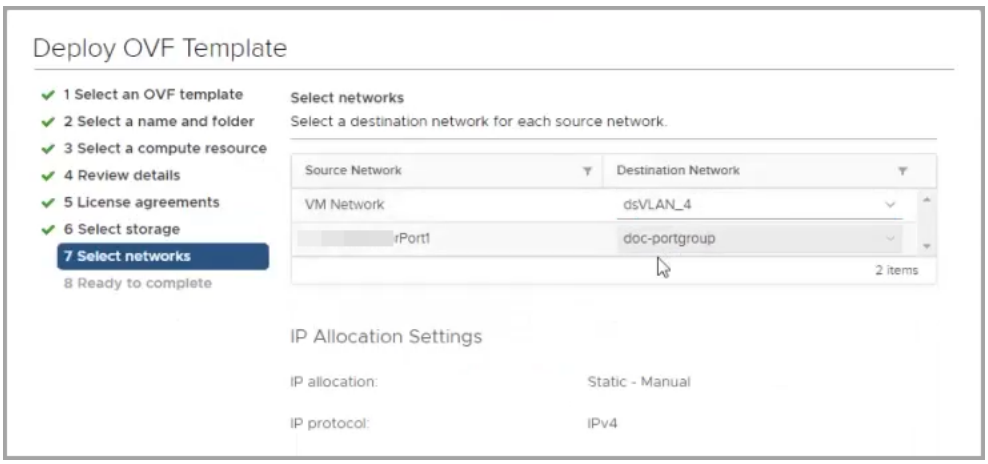
「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。

必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

11. [ネットワークの選択（Select networks）]：仮想アプライアンスのネットワークを選択します。

    [フローセンサー（Flow Sensors）]：アプライアンスがフローセンサーの場合は、作成したポートを選択します。手順については、「**2. トラフィックを監視するフロー センサーの設定**」を参照してください。



12. [終了準備の完了（Ready to Complete）]：設定の概要を確認します。 設定が正しい場合は、[終了（Finish）]をクリックします。
13. 展開はバックグラウンドで開始されます。[最近のタスク（Recent Tasks）] セクションで展開の進行状況をモニタします。次の手順に進む前に、展開が完了し、インベントリツリーに表示されていることを確認します。
14. **フロー センサー**：アプライアンスがフロー センサーであり、VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合は、次の項「**4. 追加モニタリング ポートの定義（Flow Sensor のみ）**」に進みます。
15. システム内の次の仮想アプライアンスに対して、「**3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF）**」のすべての手順を繰り返します。

    システム内ですべての仮想アプライアンスのインストールを完了した場合は、「**4. IP アドレスの設定**」に進みます。

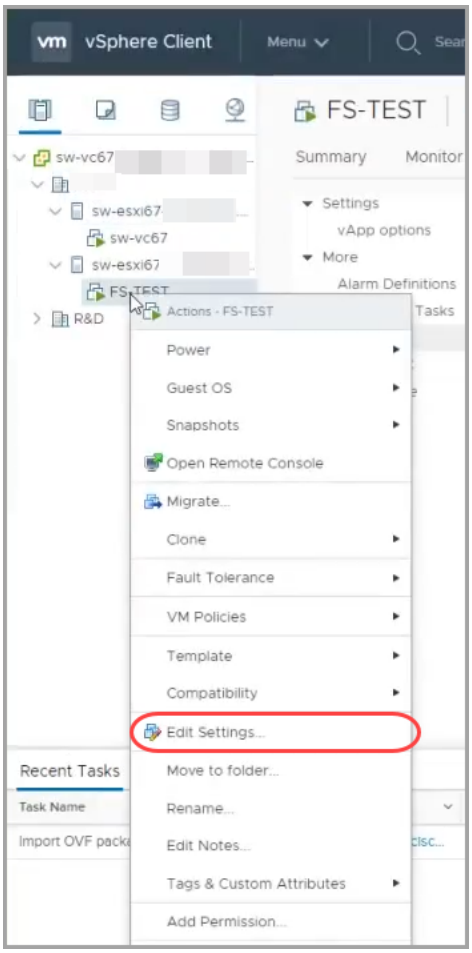
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. 追加モニタリング ポートの定義（Flow Sensor のみ）

この手順が必要となるのは、Flow Sensor VE が VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合です。これがフローセンサーのモニタリング設定ではない場合は、「**4. IP アドレスの設定**」に進みます。

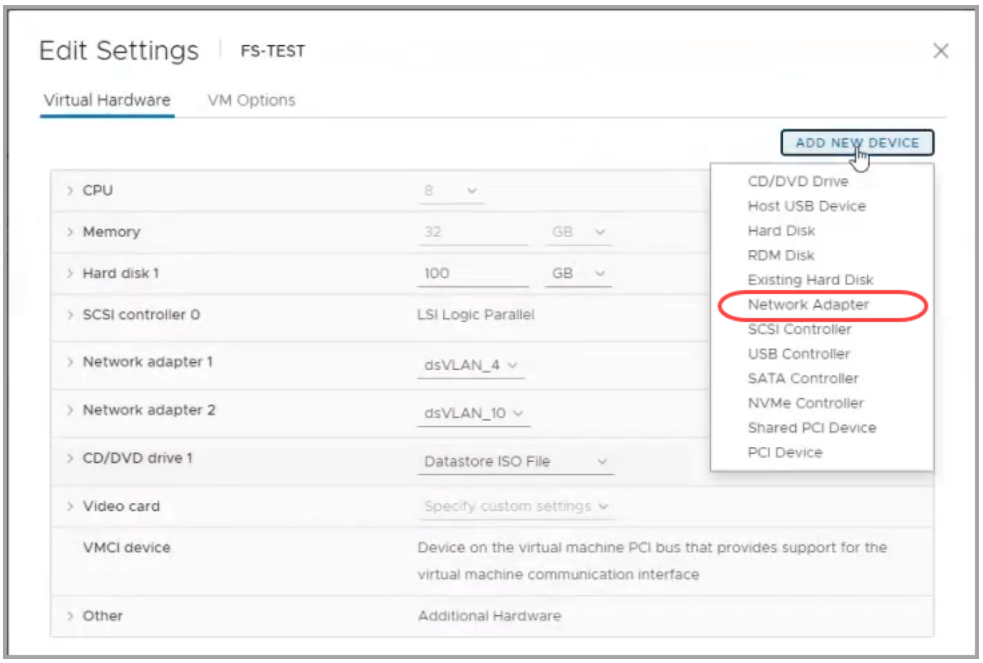
Flow Sensor VE モニタリング ポートを追加するには、次の手順を実行します。

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



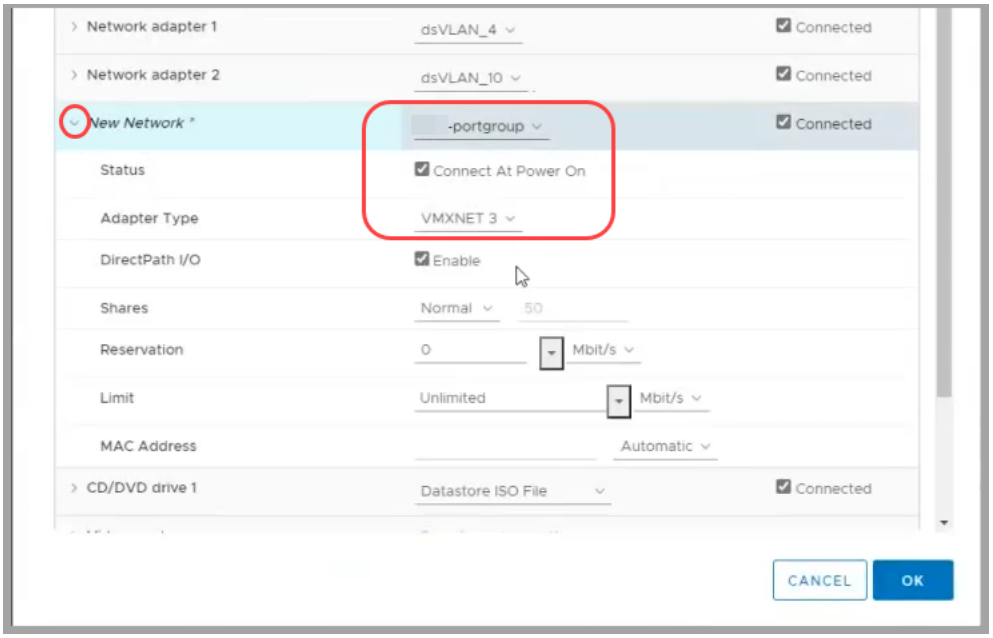
2. [設定の編集（Edit Settings）] ダイアログボックスを使用して、次の指定された設定を構成します。
3. [新規デバイスの追加（Add New Device）] をクリックします。[ネットワークアダプタ（Network Adapter）] を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



4. 新しいネットワークアダプタを見つけます。矢印をクリックしてメニューを展開し、次の内容を設定します。

- [新規ネットワーク接続（New Network）]：未割り当ての無差別ポートグループを選択します。
- [アダプタのタイプ（Adapter Type）]：[VMXNET 3] を選択します。
- [ステータス（Status）]：[パワーオン時に接続（Connect at Power On）] チェックボックスをオンにします。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. 設定を確認後、[OK] をクリックします。
6. 必要に応じて別のイーサネットアダプタを追加する場合は、この手順を繰り返します。

   すべてのイーサネットアダプタを追加した場合は、「**4. IP アドレスの設定**」に進みます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO）

概要

ESXi スタンドアロンサーバを備えた VMware 環境を使用して仮想アプライアンスをインストールするには、次の手順に従います。

別の方法を使用する場合は、次を参照してください。

- VMware vCenter：「**3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF）**」を使用します。
- KVM：「**3c. KVM ホストへの仮想アプライアンスのインストール（ISO）**」を使用します。

はじめる前に

インストールを始める前に、次の準備手順を完了してください。

1. 互換性：「**互換**」の互換性要件を確認します。
2. リソース要件：「リソース要件」の項を確認し、アプライアンスに必要な割り当てを決定します。 リソース プールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。 詳細については、「**1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定**」を参照してください。
4. ファイル：アプライアンスの ISO ファイルをダウンロードします。 手順については、「**2. VE インストールファイルのダウンロード**」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。 正しくない場合、仮想アプライアンスを起動できないことがあります。

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

> ⚠ すでにインストールされているカスタム バージョンが上書きされるため、Stealthwatch 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

ESXi スタンドアロン サーバへの仮想アプライアンス（ISO）のインストール

ESXi スタンドアロンサーバを備えた VMware 環境を使用して仮想アプライアンスをインストールするには、次の手順に従います。

プロセスの概要

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

1. VMware Web Client へのログイン

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

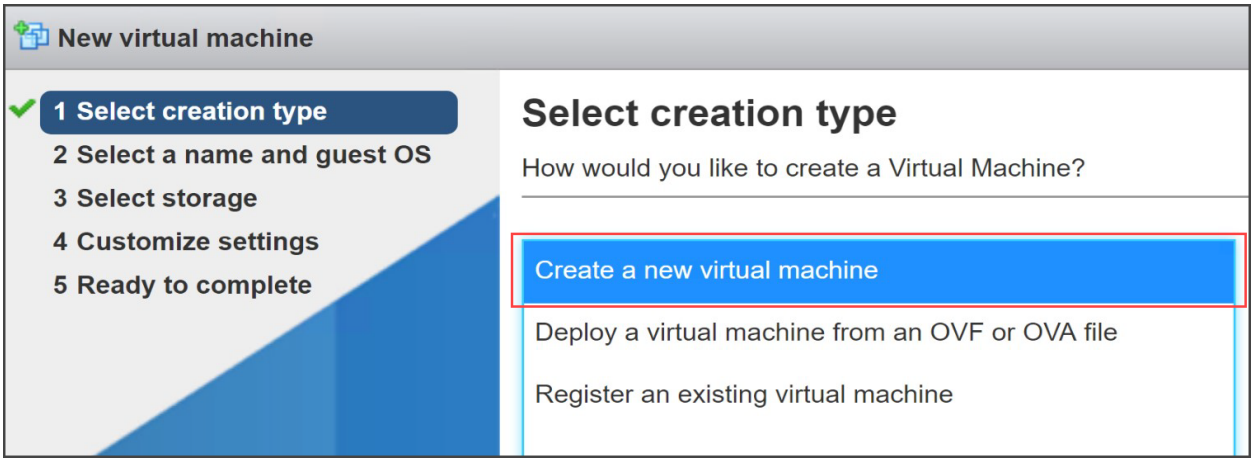
2. ISO からの起動

> フローセンサー：アプライアンスがフローセンサーの場合は、「Stealthwatch Flow Sensor」を参照して、必要な追加の設定手順について理解してください。

1. VMware Web Client へのログイン

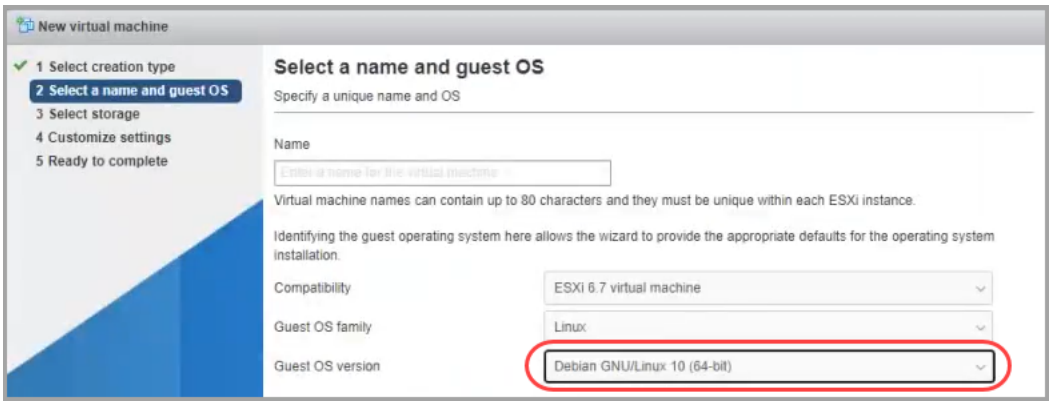
> メニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. VMware Web Client にログインします。
2. [仮想マシンの作成/登録（Create/Register a Virtual Machine）] をクリックします。
3. [新規仮想マシン（New Virtual Machine）] ダイアログボックスを使用して、次の手順で指定されているようにアプライアンスを設定します。
4. **作成タイプの選択（Select Creation Type）**：[新しい仮想マシンの作成（Create a New Virtual Machine）] を選択します。

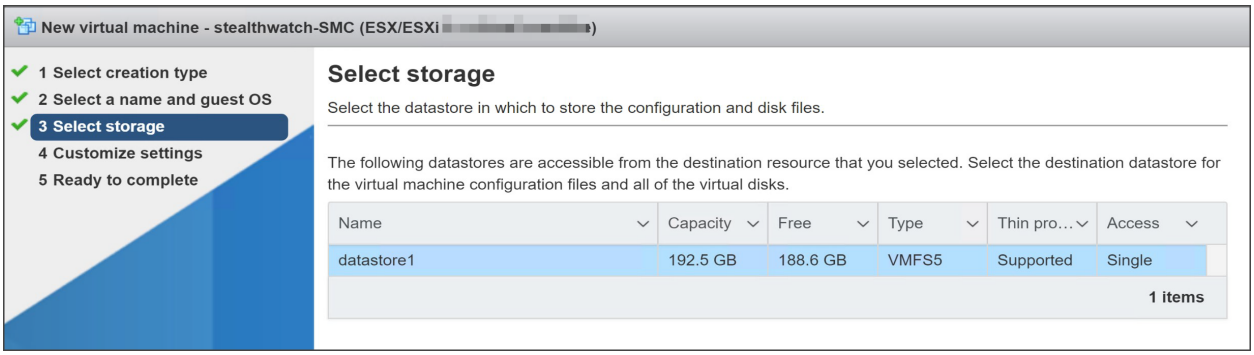


5. **ゲスト OS と名前の選択（Select a Name and Guest OS）**：次の情報を入力または選択します。
   - **名前（Name）**：簡単に識別できるようにアプライアンスの名前を入力します。
   - 互換性（Compatibility）：使用するバージョン（v6.5 または v6.7）を選択します。
   - ゲスト OS ファミリ（Guest OS family）：Linux。
   - ゲスト OS バージョン（Guest OS version）：[Debian GNU/Linux 10（64ビット）（Debian GNU/Linux 10 64-bit）] を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



6. ［ストレージの選択（Select Storage）］：アクセス可能なデータストアを選択します。「リソース要件」を確認して、十分な容量があることを確認します。



> 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

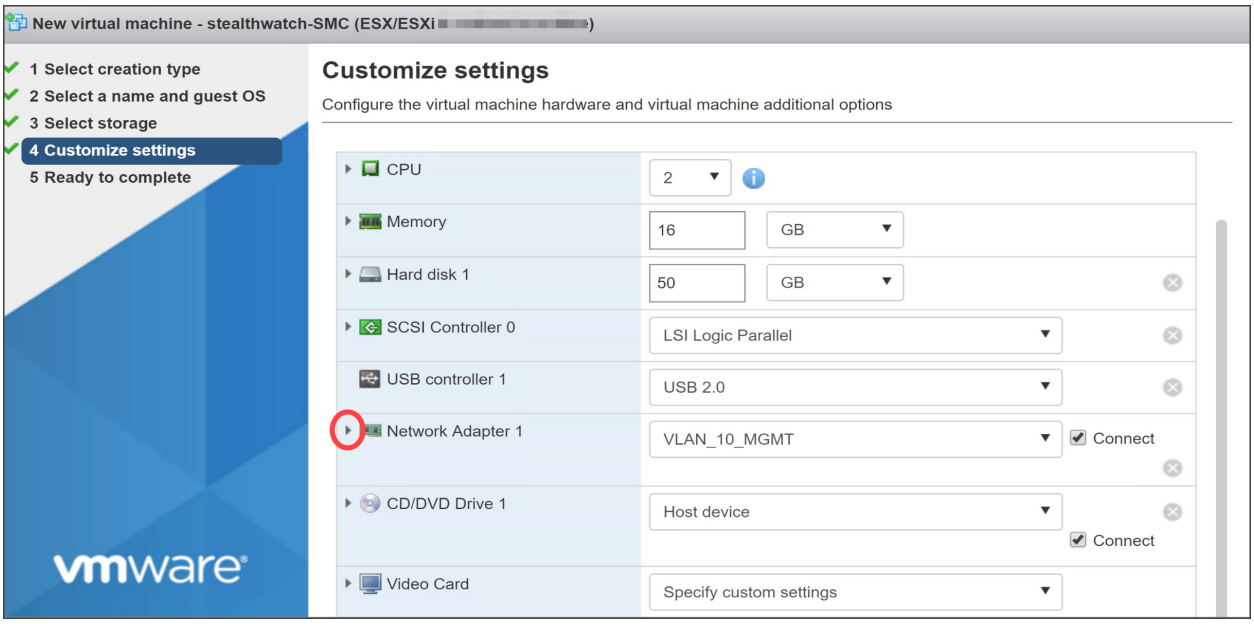
7. **設定のカスタマイズ（Customize Settings）**：アプライアンス要件を入力または選択します（詳細については**リソース要件**を参照してください）。

   次の値を選択したことを確認します。

   - **SCSI コントローラ（SCSI Controller）**：［LSI Logic Parallel］
   - **ネットワーク アダプタ（Network Adapter）**：アプライアンスの管理アドレスを確認します。

     アプライアンスがフロー センサーの場合は、［ネットワーク アダプタの追加（Add Network Adapter）］をクリックして別の管理またはセンシング インターフェイスを追加できます。詳細については、「**Stealthwatch Flow Sensor**」を参照してください。

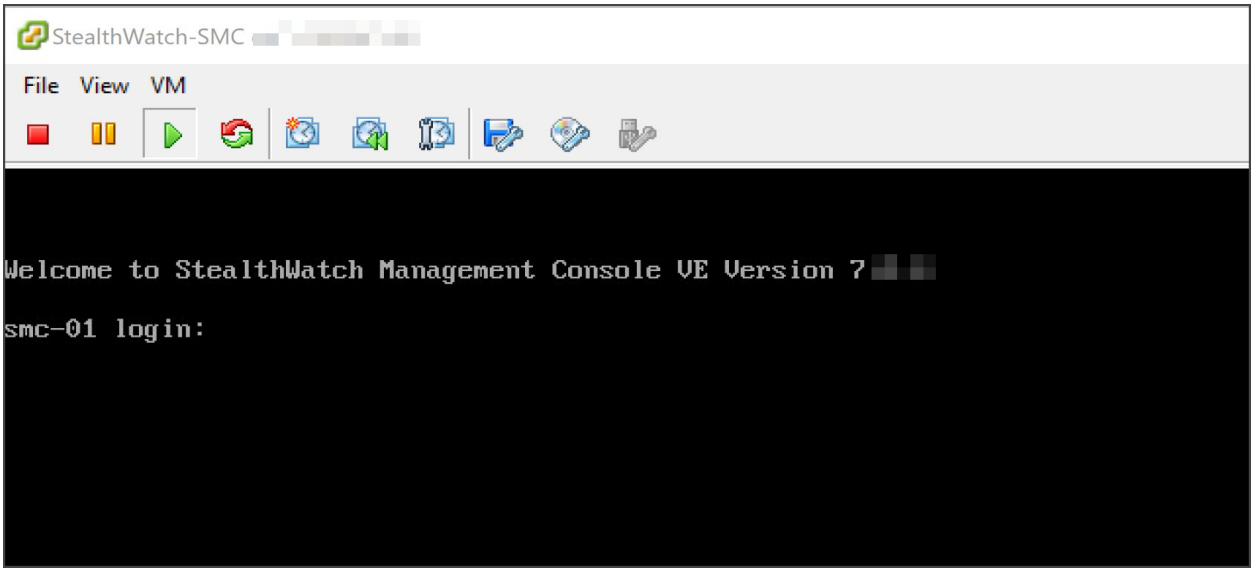
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



8. ネットワーク アダプタの横にある矢印をクリックします。
9. [アダプタのタイプ（Adapter Type）] で、[VMXnet3] を選択します。
10. 設定を確認し、それらが正しいことを確認します。
11. [終了（Finish）] をクリックします。仮想マシン コンテナが作成されます。

2. ISO からの起動

1. VMware コンソールを開きます。
2. 新しい仮想マシンに ISO を接続します。詳細については、VMware のガイドを参照してください。
3. ISO から仮想マシンを起動します。インストーラが実行され、自動的に再起動します。
4. インストールと再起動が完了すると、ログイン プロンプトが表示されます。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. 仮想マシンから ISO を切断します。
6. 次の仮想アプライアンスに対して、「**3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO）**」のすべての手順を繰り返します。
7. フローセンサー：アプライアンスがフローセンサーの場合は、「**Stealthwatch Flow Sensor**」を確認し、このマニュアルの前述の項を参照してセットアップを完了します。
    - **2. トラフィックを監視するフロー センサーの設定**（「単一のホストでの vSwitch の監視」を使用）
    - フロー センサーが VMware 環境内の複数の仮想スイッチ、またはクラスタ内の複数の VDS を監視する場合は、「**4. 追加モニタリング ポートの定義（Flow Sensor のみ）**」に進みます。
8. すべての仮想アプライアンスをインストールした場合は、「**4. IP アドレスの設定**」に進みます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3c. KVM ホストへの仮想アプライアンスのインストール（ISO）

概要

KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールするには、次の手順に従います。

別の方法を使用する場合は、次を参照してください。

- VMware vCenter：「**3a. VMware vCenter を使用した仮想アプライアンスのインストール（OVF）**」を使用します。
- VMware ESXi スタンドアロンサーバ：「**3b. ESXi スタンドアロンサーバへの仮想アプライアンスのインストール（ISO）**」を使用します。

はじめる前に

インストールを始める前に、次の手順を完了してください。

1. 互換性：「**互換**」の互換性要件を確認します。
2. リソース要件：「リソース要件」の項を確認し、アプライアンスに必要な割り当てを決定します。 リソースプールまたは代替方法を使用してリソースを割り当てます。
3. ファイアウォール：通信のファイアウォールを設定します。 詳細については、「**1. 仮想アプライアンスのインストール：ファイアウォールとポートの設定**」を参照してください。
4. ファイル：アプライアンスの ISO ファイルをダウンロードし、KVM ホストのフォルダにコピーします。この項にある例では、var/lib/libvirt/image フォルダを使用します。 手順については、「**2. VE インストールファイルのダウンロード**」を参照してください。
5. 時刻：仮想アプライアンスをインストールする VMware 環境内のハイパーバイザホストに設定された時刻が正しい時刻を示していることを確認します。正しくない場合、仮想アプライアンスを起動できないことがあります。

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

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

KVM ホストへの仮想アプライアンスのインストール（ISO）

KVM ホストがある場合は、次の手順に従い、ISO を使用して仮想アプライアンスをインストールします。

プロセスの概要

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

1. KVM ホストへの仮想アプライアンスのインストール
2. Open vSwitch への NIC および無差別ポートの監視の追加（Flow Sensor のみ）

1. KVM ホストへの仮想アプライアンスのインストール

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

トラフィックのモニタリング

Flow Sensor VE には KVM 環境を可視化する機能があり、フロー非対応領域のフローデータを生成できます。各 KVM ホスト内部にインストールされる仮想アプライアンスとして、Flow Sensor VE は監視対象のトラフィックからイーサネット フレームを受動的にキャプチャし、カンバセーション ペア、ビット レートおよびパケット レートに関係する貴重なセッション統計情報を含むフロー レコードを作成します。詳細については、「Stealthwatch Flow Sensor：ネットワークへの Flow Sensor VE の統合」を参照してください。

設定要件

この設定には次の要件があります。

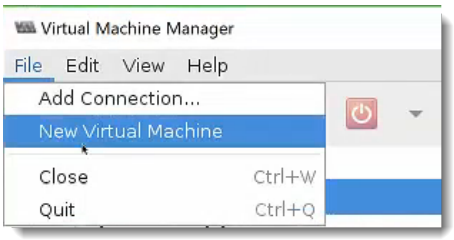
- 無差別モード：有効
- 無差別ポート：Open vSwitch に設定

KVM ホストへの仮想アプライアンスのインストール

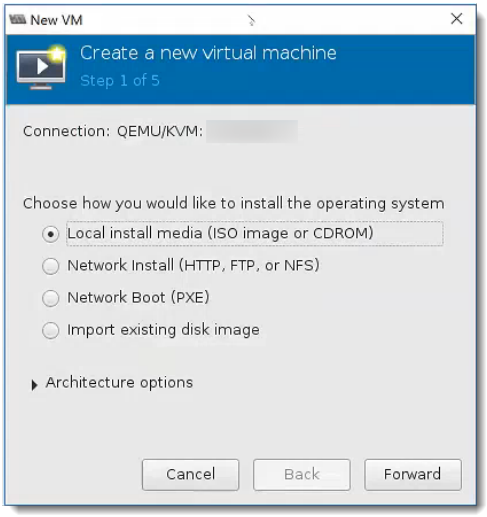
仮想アプライアンスをインストールし、Flow Sensor VE を有効にしてトラフィックを監視するには、次の手順を実行します。

1. Virtual Machine Manager を使用して KVM ホストに接続し、次の手順に従ってアプライアンスを設定します。
2. [ファイル（File）] > [新しい仮想マシン（New Virtual Machine）] をクリックします。

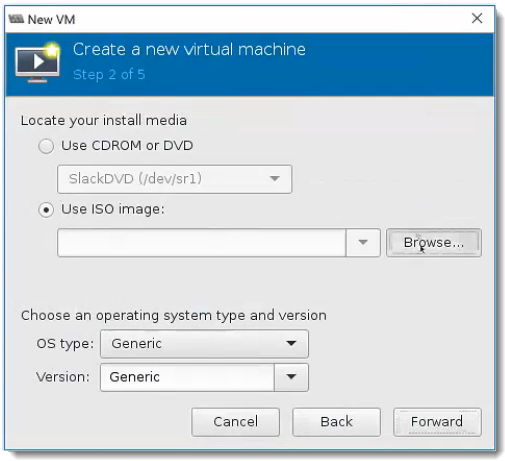
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



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



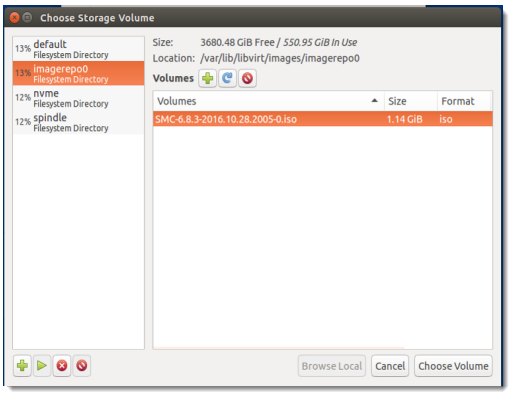
4. [ISOイメージを使用（Use ISO image）] をクリックします。
5. [参照（Browse）] をクリックします。適切なイメージを選択します。



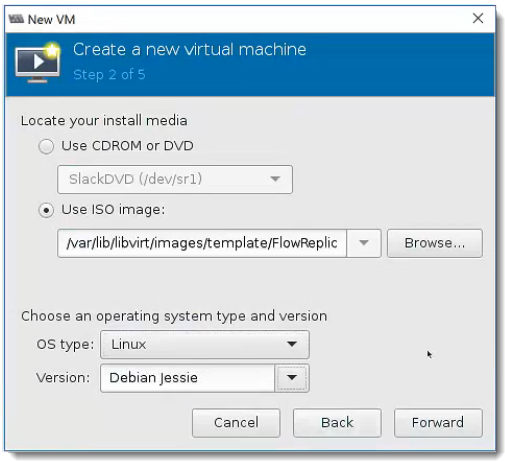
6. ISO ファイルを選択します。[ボリュームの選択（Choose Volume）] をクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

KVM ホストが ISO ファイルにアクセスできることを確認します。



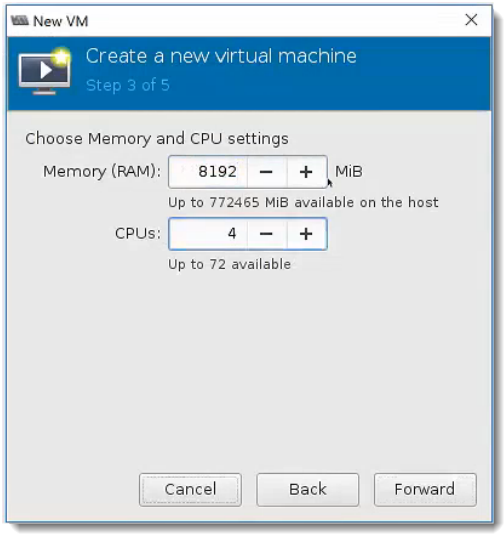
7. [オペレーティング システムのタイプとバージョンの選択（Choose an operating system type and version）] で、[OSタイプ（OStype）] ドロップダウン リストから [Linux] を選択します。
8. [バージョン（Version）] ドロップダウン リストから [Debian Jessie] を選択します。[Forward] をクリックします。



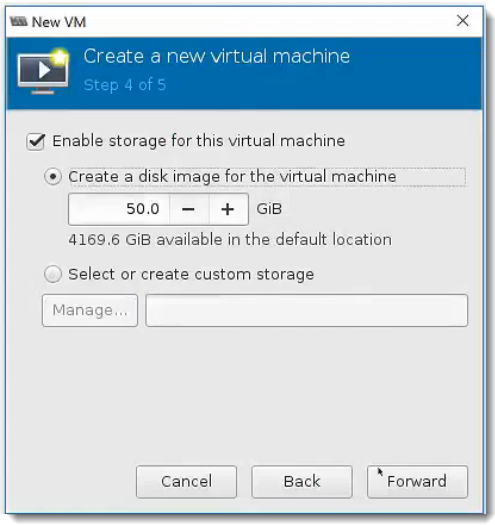
9. メモリ（RAM）と CPU を「**バーチャル エディション（VE）のリソース要件**」の項に示す容量まで増やします。

> 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システム パフォーマンスにとって重要です。
>
> ⚠ 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



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



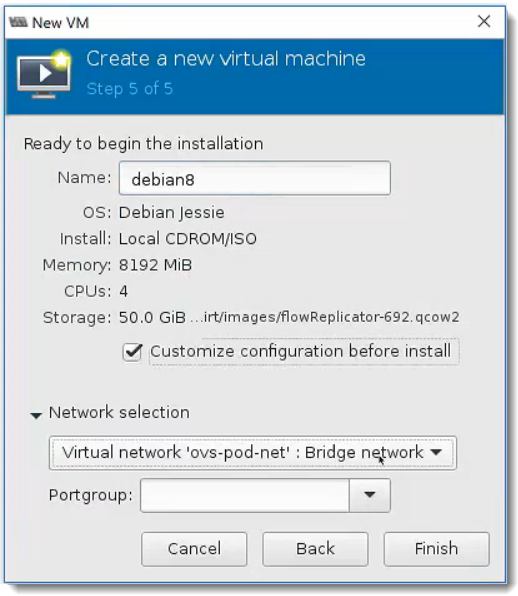
「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。

必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

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

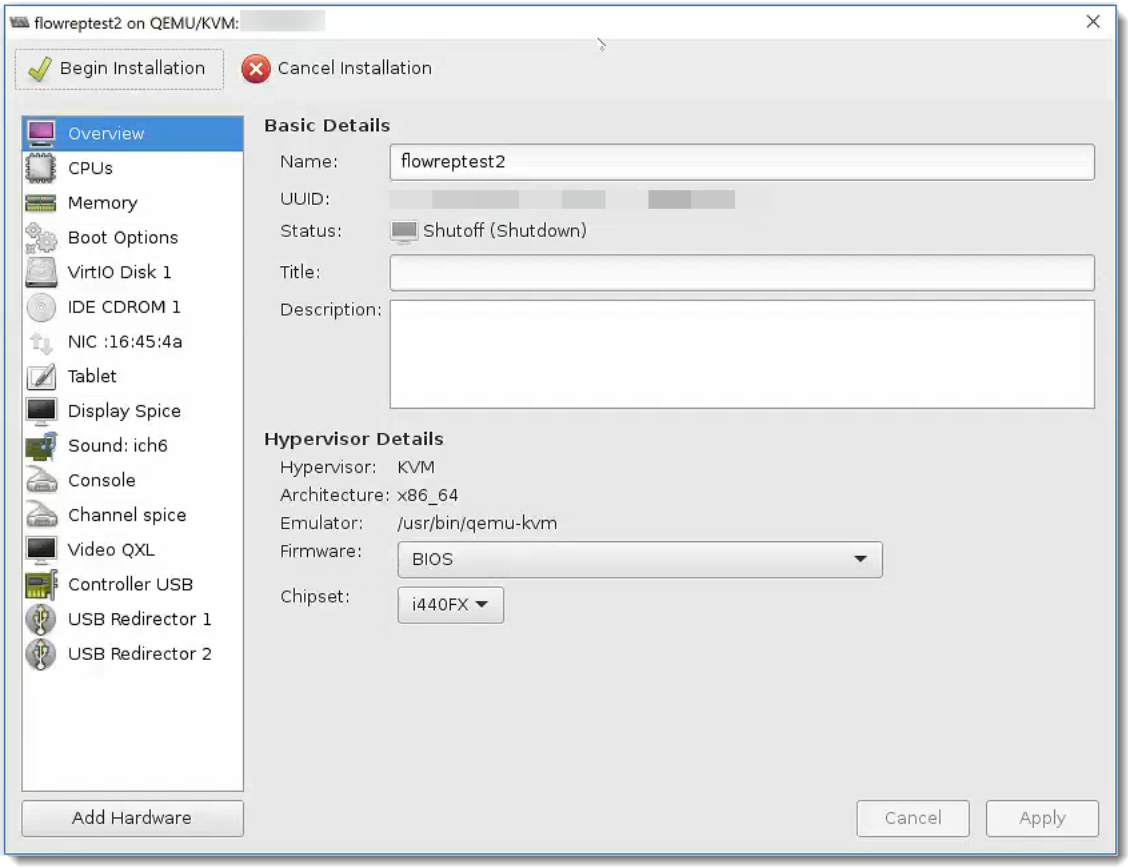
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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



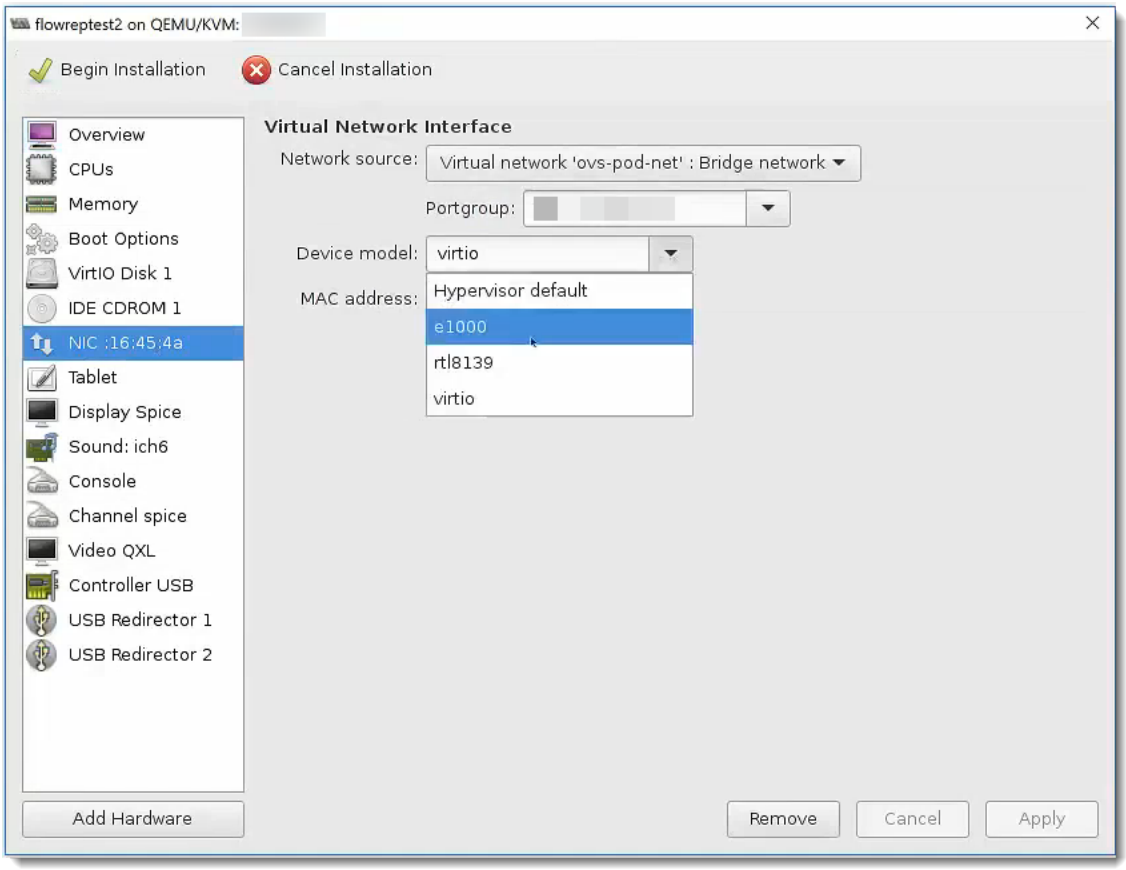
15. ［終了（Finish）］をクリックします。［設定（Configuration）］メニューが開きます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



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

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



18. [VirtIO ディスク 1（VirtIO Disk 1）] をクリックします。
19. [詳細オプション（Advanced Options）] ドロップダウン リストの [ディスク バス（Disk bus）] ドロップダウン ボックスで [SCSI] を選択します。[適用（Apply）] をクリックします。
20. Flow Sensor VE のポートの監視用に NIC を追加する必要がありますか。

    - 「はい」の場合、「**2. Open vSwitch への NIC および無差別ポートの監視の追加（Flow Sensor のみ）**」に進みます。
    - 「いいえ」の場合、次の手順に進みます。

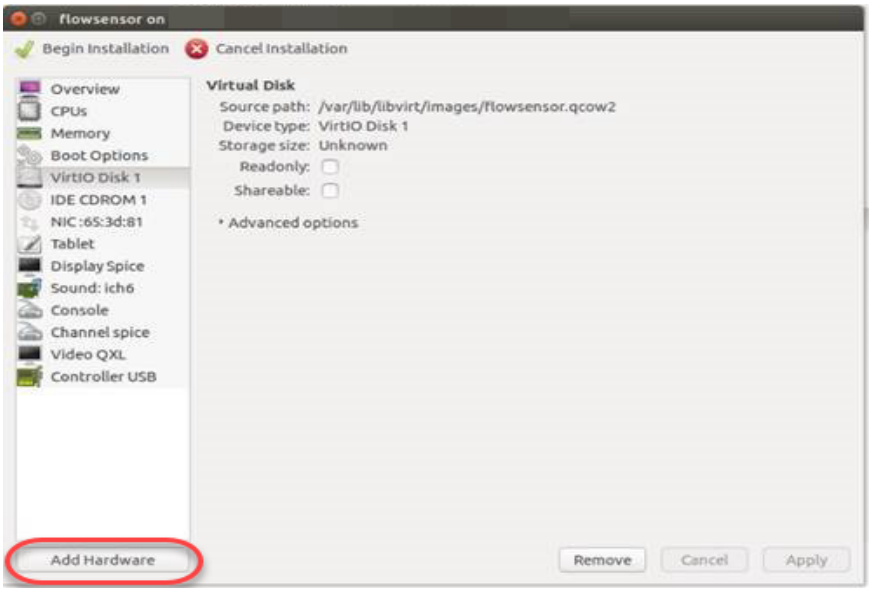
21. [インストールの開始（Begin Installation）] をクリックします。
22. 「**4. IP アドレスの設定**」に進みます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

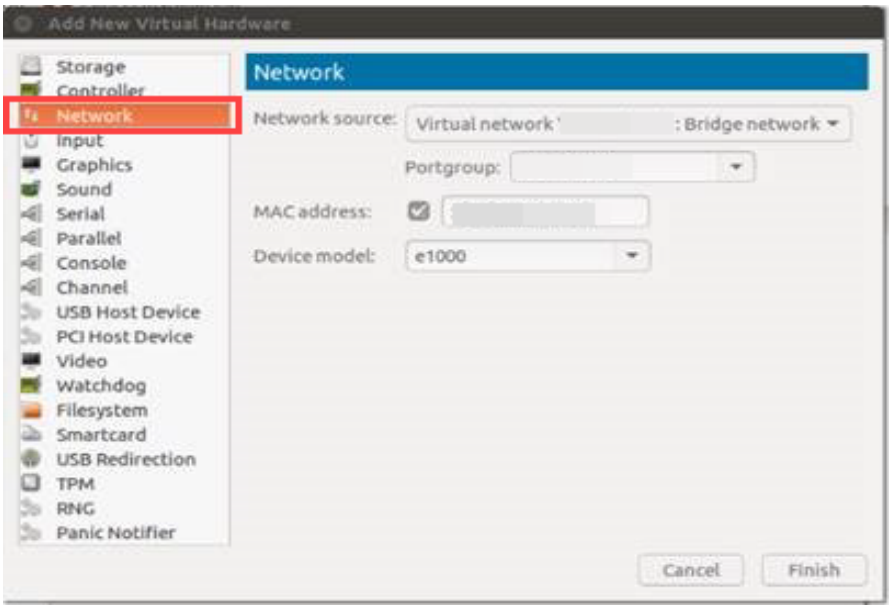
2. Open vSwitch への NIC および無差別ポートの監視の追加（Flow Sensor のみ）

Flow Sensor VE 監視ポート用の NIC を追加し、インストールを完了するには、次の手順を実行します。

1. [設定（Configuration）] メニューで、[ハードウェアの追加（Add Hardware）] をクリックします。[新規仮想ハードウェアの追加（Add New Virtual Hardware ）] ダイアログボックスが表示されます。

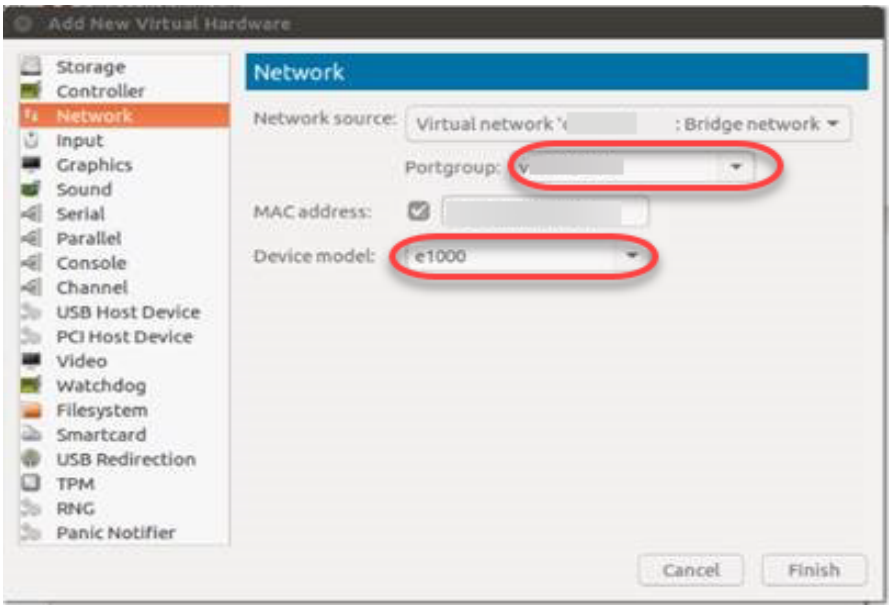


2. 左側のナビゲーション ウィンドウで [ネットワーク（Network）] をクリックします。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. [ポートグループ（Portgroup）]ドロップダウン リストをクリックし、監視する未割り当ての無差別ポート グループを選択します。[デバイス モデル（Device Model）]ドロップダウン リストをクリックし、[e1000] を選択します。



4. [終了（Finish）]をクリックします。
5. 別の監視ポートを追加する必要がある場合は、これまでの手順を繰り返します。
6. すべての監視ポートを追加したら、[インストールの開始（Begin Installation）]をクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. IP アドレスの設定

VMware または KVM を使用して Stealthwatch VE アプライアンスをインストールしたら、それらの仮想環境を設定できます。

IP アドレスの設定

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

   仮想マシンの電源が入っていない場合や、使用可能なメモリの不足に関するエラー メッセージを受信した場合、次のいずれかを実行します。

   - **リソース**:アプライアンスがインストールされているシステムの使用可能リソースを増やします。詳細については、「**バーチャル エディション(VE)のリソース要件**」の項を参照してください。
   - **VMware 環境**:アプライアンスのメモリ予約制限とリソース プールを増やします。

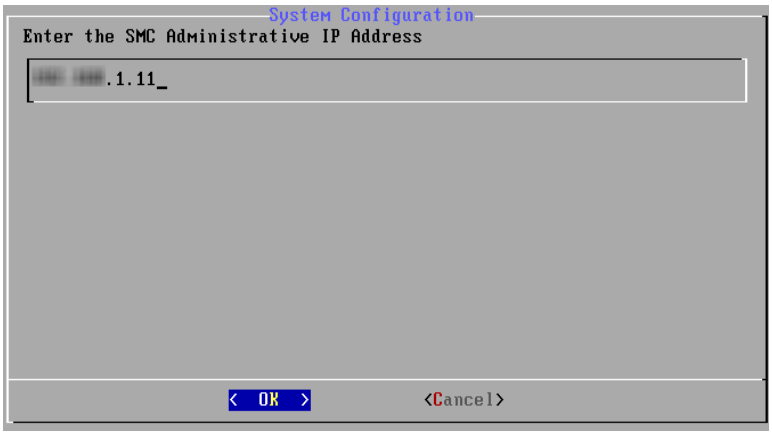
> 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システム パフォーマンスにとって重要です。
>
> ⚠ 必要なリソースがない状態で Cisco Stealthwatch アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

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

   [管理IPアドレス(Administrative IP Address)] ページが自動的に表示されない場合は、コンソール経由でログインします。

   - **ログイン**:sysadmin
   - **デフォルト パスワード**:lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。

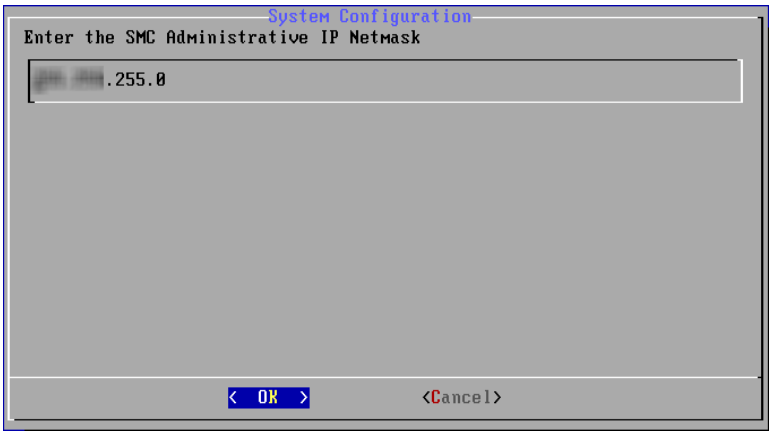
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



> 画面全体を表示するには、全画面モードを有効にする必要があります。

6. ページをクリックします。仮想アプライアンスの IP アドレスを入力します。
7. [OK] を選択します。Enter キーを押します。
8. IP ネットワーク マスクのアドレスを確認します。

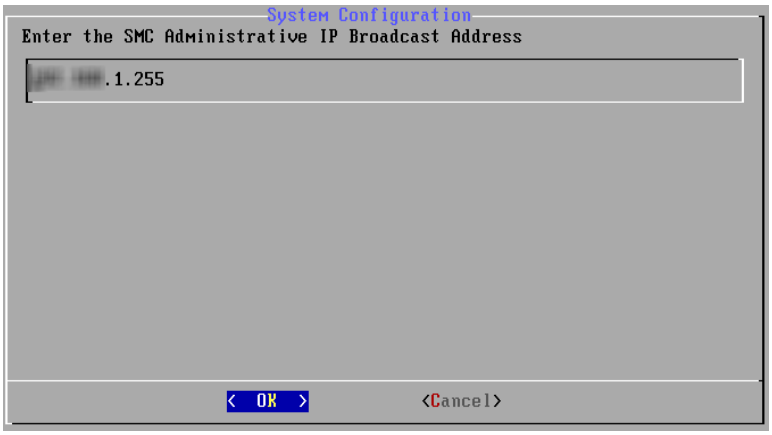
   - デフォルトをそのまま使用するか、新しいアドレスを入力します。
   - [OK] を選択します。**Enter** キーを押して、続行します。



9. ブロードキャスト IP アドレスを確認します。

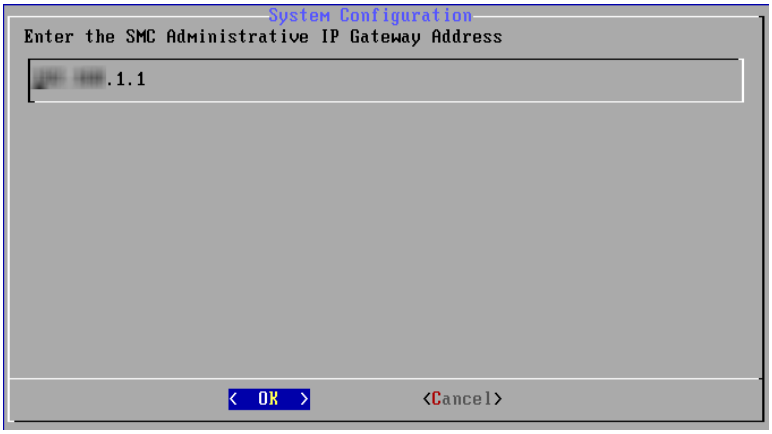
   - デフォルトをそのまま使用するか、新しいアドレスを入力します。
   - [OK] を選択します。**Enter** キーを押して、続行します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



10. ゲートウェイ サーバ IP アドレスを確認します。

    - デフォルトをそのまま使用するか、新しいアドレスを入力します。
    - [OK] を選択します。**Enter** キーを押して、続行します。



11. ホスト名を入力します。

    ホスト名が一意であり、インターネットホストのインターネット標準規格の要件を満たしていることを確認します。

    - [OK] を選択します。
    - **Enter** キーを押して、続行します。

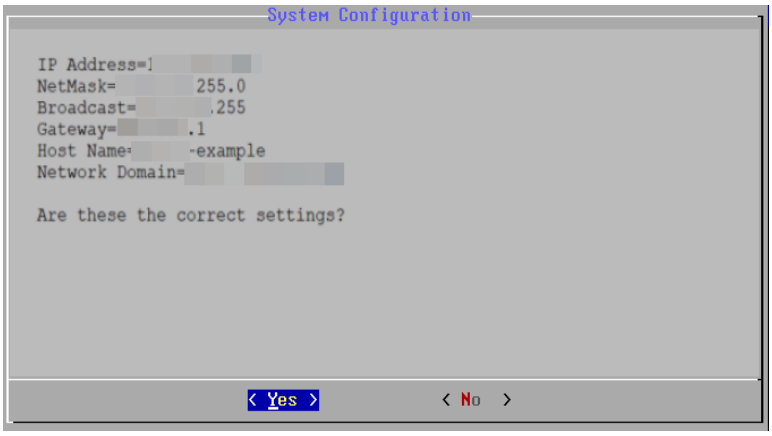
12. ネットワークドメイン名を入力します。

    完全修飾ドメイン名を使用します。

    - [OK] を選択します。
    - **Enter** キーを押して、続行します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

13. 設定を確認します。すべてが正しければ、**Enter** キーを押します。



14. 画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
15. 再起動後、ログイン プロンプトが表示されます。

> アプライアンスにアクセスできない場合は、「トラブルシューティング」の手順を参照してください。

16. [いいえ(No)] を選択します。Enter キーを押します。
17. Ctrl + Alt を押して、コンソールを終了します。
18. システム内の次の仮想アプライアンスに対して、「**4. IP アドレスの設定**」のすべての手順を繰り返します。

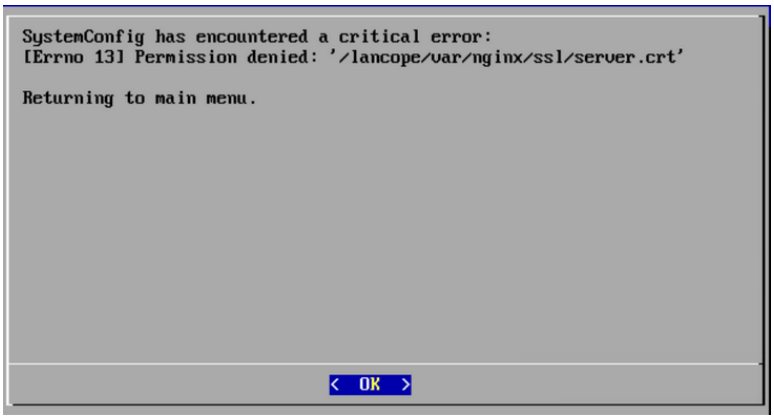
    すべての仮想アプライアンスに対して IP アドレスを設定したら、「**5. Stealthwatch システムの設定**」に進みます。

トラブルシューティング

証明書エラー

VM 環境の使用率が高い場合は、タイミングエラーが発生し、一部のイベントが順不同で発生する可能性があります。証明書エラー(.crt)が原因で権限が拒否されるという次のようなエラーが表示される場合は、次の手順を実行します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



1. アプライアンスコンソールに sysadmin としてログインします。デフォルトのパスワードは、lan1cope です。

   後の手順でデフォルト パスワードを変更します。詳細については、「デフォルトパスワードの変更」を参照してください。

2. 次のコマンドを実行します。

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

3. SystemConfig を実行します。
4. [IPアドレスの設定（Configure the IP Addresses）] に戻り（ステップ 5 以降）、この項のすべてのステップを完了します。**IP アドレスの設定** アプライアンスにアクセスできない場合は、Cisco Stealthwatch サポートにお問い合わせください。

アプライアンスへのアクセス

再起動後にアプライアンスにアクセスできない場合は、次の手順を実行します。

1. root としてログインします。
2. 次のコマンドを実行して、Docker コンテナおよびサービスが稼働していることを確認します。

   - `docker ps`
   - `systemctl list-units --failed`
   - `systemd-analyze critical chain`

3. すべての Docker コンテナおよびサービスが稼働状態になったら、ログインを再試行します。アプライアンスにアクセスできない場合は、Cisco Stealthwatch サポートにお問い合わせください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. Stealthwatch システムの設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールを使用してアプライアンスを設定し、Stealthwatch Management Console（SMC）で管理できるようにします。

準備

設定を開始する前に、手順を確認して、アプライアンスの設定順序、ベストプラクティス、および追加要件を理解してください。

アプライアンス設定ツールの要件

- ファイアウォールと ACL（アクセス制御リスト）でアクセスが許可されていることを確認します。
- アプライアンスのホスト名と次の IP アドレスを収集します。
    - アプライアンス
    - サブネット マスク
    - デフォルト ゲートウェイとブロードキャスト ゲートウェイ
    - NTP サーバと DNS サーバ
    - Central Management の SMC の IP アドレス

管理対象

アプライアンス設定ツールの実行の一環として、プライマリ Stealthwatch Management Console（SMC）によって管理されるようにアプライアンスを設定します。

アプライアンスが Stealthwatch Management Console（SMC）によって管理されている場合、Central Management を使用してアプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどができます。

SMC フェールオーバー

複数の Stealthwatch Management Console（SMC）がある場合、SMC フェールオーバーペアを設定して、SMC の 1 つを他方のバックアップコンソールとして動作させることができます。

- 各 SMC を設定するには、アプライアンス設定ツールを使用します。
- プライマリにする SMC とセカンダリにする SMC を計画します。
- 個々の SMC を設定したら、Central Management 信頼ストアおよび Stealthwatch デスクトップ クライアントを使用して SMC フェールオーバー関係を設定します。詳細については、「**SMC フェールオーバー関係の定義**」を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ベスト プラクティス

システムを正常に設定するには、このガイドの手順に従っていることを確認します。

推奨事項は次のとおりです。

- **1 つずつ**：一度に 1 つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [アップ（Up）] ステータスであることを確認します。
- **順序**：設定の順序に従います。
- **複数の Central Manager**：システムには複数の Central Manager を設定できます。ただし、各アプライアンスは 1 つのプライマリ SMC/Central Manager のみによって管理できます。
- **アクセス**：Central Management にアクセスするための管理者権限が必要です。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

設定の順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

順序	アプライアンス	詳細
1.	プライマリ SMC	プライマリ SMC は、Central Manager です。 システム内で次のアプライアンスの設定を開始する前に、SMC が [アップ(Up)] として表示されていることを確認します。
2.	UDP Director (別名 FlowReplicators)	
3.	Flow Collector 5000 シリーズ データベース	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。
4.	Flow Collector 5000 シリーズ エンジン	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。
5.	その他のすべての Flow Collector (NetFlow および sflow)	
6.	Flow Sensor	フロー センサーの設定を開始する前に、フロー コレクタが [アップ(Up)] として表示されていることを確認します。
7.	エンドポイント コンセントレータ	
8.	セカンダリ SMC (使用する場合)	セカンダリ SMC の設定を開始する前に、プライマリ SMC が [アップ(Up)] として表示されていることを確認します。 セカンダリ SMC は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。詳細については、「**SMC フェールオーバー関係の定義**」を参照してください。

システムによっては、ここに示されているアプライアンスの一部が存在しない場合があります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. ログイン

アプライアンス設定ツールを使用して各アプライアンスを設定するには、次の手順を使用します。

1. ブラウザのアドレス フィールドに、**https://** およびアプライアンスの IP アドレスを入力します。

    - **プライマリ SMC**：最初にプライマリ SMC を設定します。
    - **アップ**：お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが［アップ（Up）］ステータスであることを確認します。
    - **順番**：アプライアンスが正常に通信するように、必ずそれらを順番どおり設定します。

> アプライアンスにアクセスできない場合は、「トラブルシューティング」（「**4. IP アドレスの設定**」セクション）を参照してください。

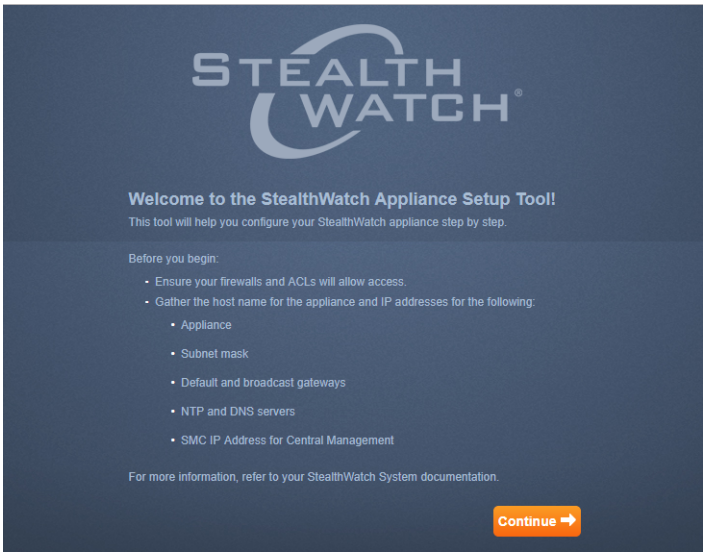
2. 次のクレデンシャルを入力して、ログインします。

    - **ユーザ名**：admin
    - **パスワード**：lan411cope

2. アプライアンスの設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールによって各設定手順が示されます。

> これが初回インストールではない場合、「**トラブルシューティング**」に移動して、ホスト名、ネットワークドメイン名、IP アドレスなどのアプライアンス ネットワーク設定を変更します。



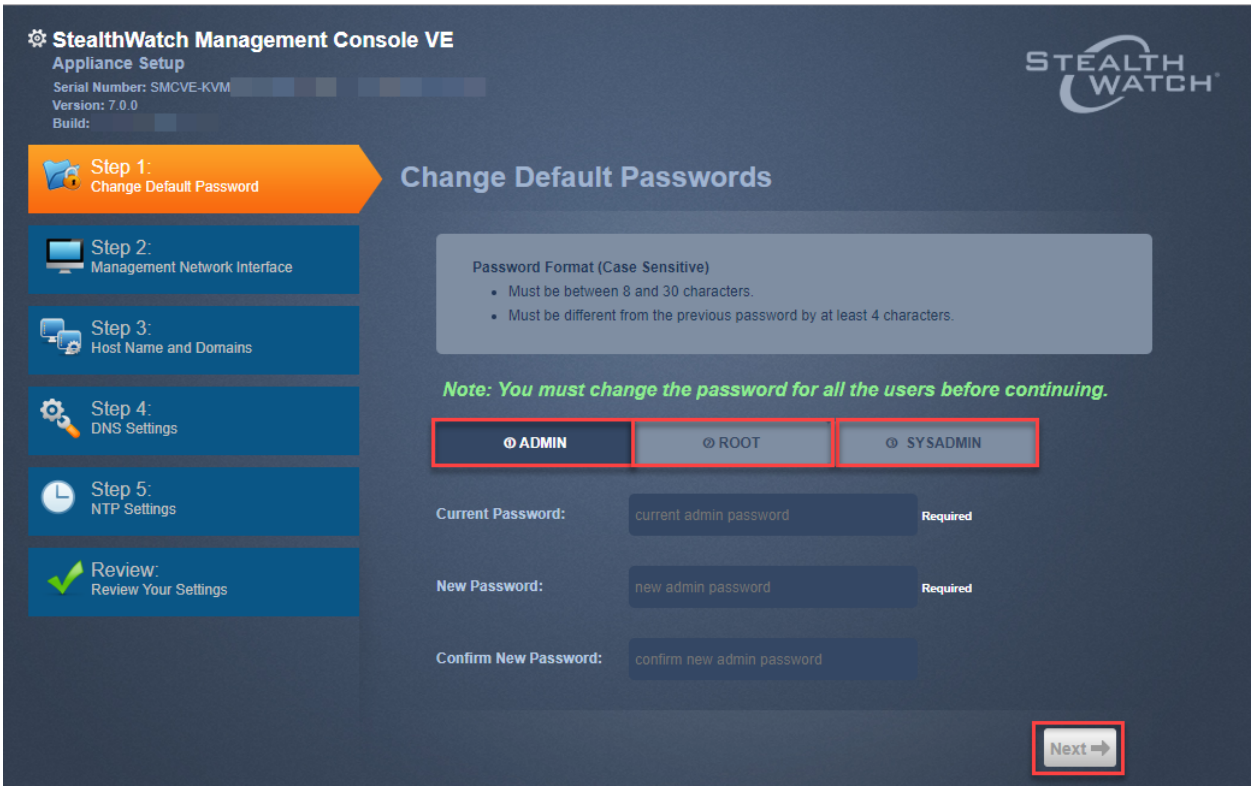
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. **デフォルト パスワードの変更**:admin、root、および sysadmin の新しいパスワードを入力します。[次へ(Next)] をクリックして各ユーザにスクロールします。

   次の基準を使用します。

   - 長さ:8 ～ 256 文字
   - **変更**:新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

ユーザ	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope



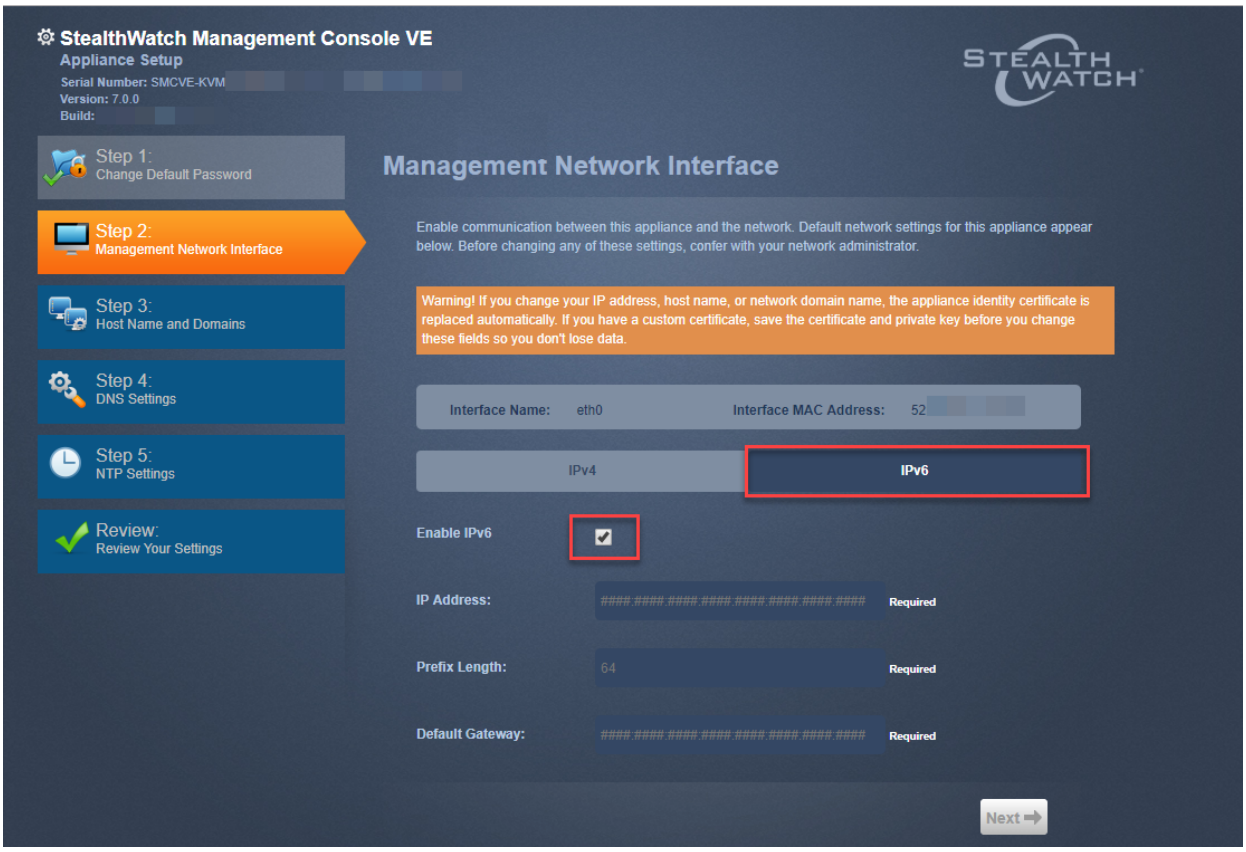
> すでにハードウェア設置時にデフォルト パスワードを変更している場合は、[sysadmin] メニューと [root] メニューは使用できません。詳細については、『Stealthwatch x210 Series Hardware Installation Guide』を参照してください。

2. **管理ネットワーク インターフェイス**:IP アドレスおよびネットワーク インターフェイス フィールドを確認します。デフォルト設定が正しいことを確認します。[次へ(Next)] をクリックし

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ます。

- **変更**:この情報を変更するには、ネットワーク管理者と協議し、トラブルシューティングを参照してください。
- **IPv6(オプション)**:IPv6 を有効にするには、[IPv6] をクリックします。[IPv6 の有効化(Enable IPv6)] チェックボックスをオンにして、フィールドに入力します。



3. **ホスト名とドメイン**:ホスト名とネットワークドメイン名を入力します。[次へ(Next)] をクリックします。

   - **ホスト名**:各アプライアンスには一意のホスト名が必要です。複数のアプライアンスに同じホスト名を割り当てた場合、それらは正常にインストールされません。

     また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

   - **ネットワークドメイン**:各アプライアンスには完全修飾ドメイン名が必要です。
   - **Stealthwatch ドメイン(SMC のみ)**:Stealthwatch アプライアンスの Stealthwatch ドメインを入力します。
   - **IP アドレスの範囲(SMC のみ)**:Stealthwatch ネットワークの IP アドレス範囲を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. **DNS 設定**：デフォルトが正しいことを確認するか、ドメイン サーバ IP アドレスを入力します。[次へ（Next）] をクリックします。

   DNS サーバの追加または削除（オプション）

   - **追加**：[+] アイコンをクリックします。
   - **削除**：チェックボックスをクリックして DNS サーバを選択します。[–] アイコンをクリックします。

5. **NTP の設定**：デフォルトが正しいことを確認するか、[メニュー（Menu）] アイコンをクリックして Network Time Protocol（NTP）サーバを選択します。[次へ（Next）] をクリックします。

   - **複数の NTPサーバ**：冗長性と精度を確保するために複数の NTP サーバを設定することをお勧めします。
   - **パブリック ソース**：NTP の適切なパブリック ソースとして pool.ntp.org が適しています。

   NTP サーバの追加または削除（オプション）

   - **追加**：[+] アイコンをクリックします。
   - **削除**：チェックボックスをクリックして NTP サーバを選択します。[–] アイコンをクリックします。

6. アプライアンスが SMC の場合は、「3. Stealthwatch Management Console の登録」に進みます。

   アプライアンスが SMC でない場合は、「4. [集中管理（Central Management）] へのアプライアンスの追加」に進みます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. Stealthwatch Management Console の登録

1. **設定を確認**:アプライアンスの情報が正確であることを確認します。
2. [適用(Apply)] または [再起動して続行(Restart and Proceed)] をクリックします。

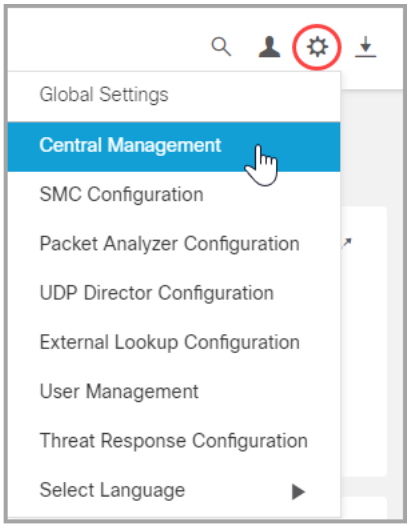
   アプライアンスの再起動中は、画面に表示される指示に従います。

   新しいシステム設定が有効になるまで数分待ちます。ページの更新が必要な場合があります。

3. Stealthwatch Management Console にログインします。
4. アプライアンス設定ツールが再び開きます。**[続行(Continue)]** をクリックします。
5. [アプライアンスの登録(Register Your Appliance)] タブで IP アドレスを確認し、[保存(Save)] をクリックします。

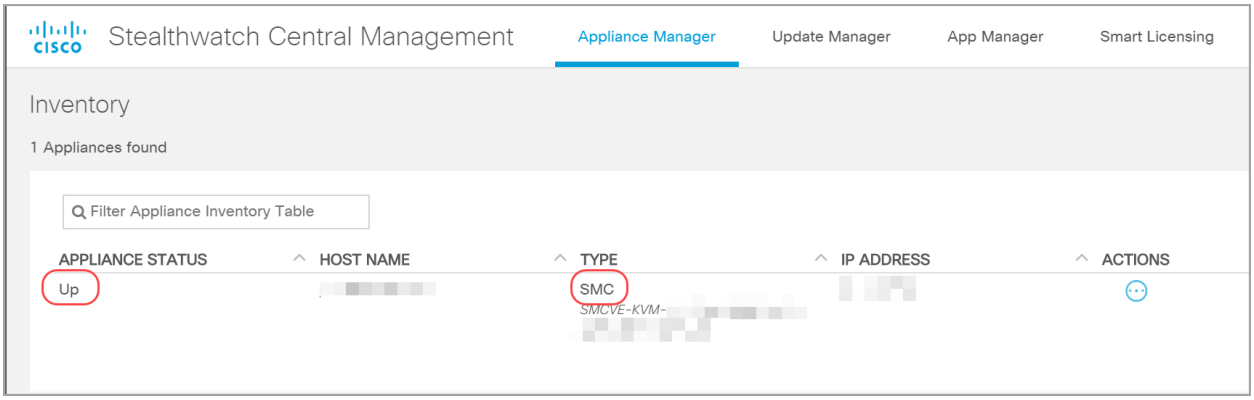
   - Stealthwatch Management Console に Central Management がインストールされます。
   - SMC IP アドレスは自動的に検出されるため、変更できません。

6. アプライアンスの設定が完了したら、[ダッシュボードに移動(Go to Dashboard)] をクリックします。
7. [グローバル設定(Global Settings)] アイコンをクリックします。[集中管理(Central Management)] を選択します。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

8. インベントリを確認します。SMC アプライアンスのステータスが [アップ(Up)] と表示されていることを確認します。



> クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ(Up)] として表示されていることを確認してください(設定の順序と詳細を使用)。

9. システム内の次のアプライアンスを設定するには、「**1. ログイン**」に進み、「**5. アプライアンス ステータスの確認**」までの手順を完了します。

   設定する別のアプライアンスがない場合は、「**6. アプライアンス設定の完了**」に戻ります。

4. [集中管理(Central Management)] へのアプライアンスの追加

アプライアンス設定ツールを使用して、Central Management でのアプライアンスの設定を続けます。一部の手順は、アプライアンスによって異なる場合があります。画面に表示される指示に従って操作します。

1. [Central Management] タブで、プライマリ SMC の IP アドレスを入力します。

   プライマリ SMC は、Central Manager です。

2. **[保存(Save)]**をクリックします。
3. 画面に表示される指示に従って、プライマリ SMC アプライアンスのアイデンティティ証明書を信頼します。[はい(Yes)] をクリックして証明書を信頼し、アプライアンスと SMC との通信を許可します。
4. プライマリ SMC のログイン クレデンシャルを入力します。
5. Stealthwatch ドメインを選択します。

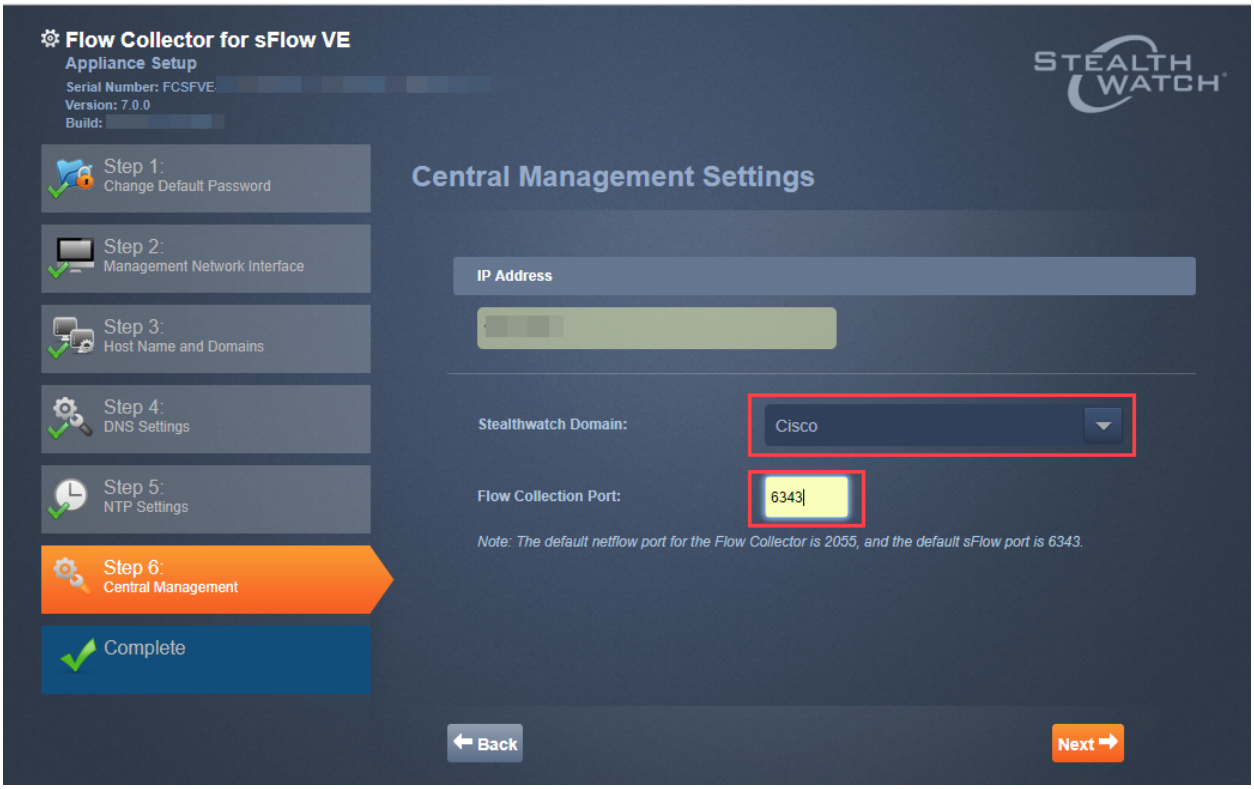
   - [フローコレクタ(Flow Collectors)]:フロー収集のポート番号を入力します。

     NetFlow のデフォルト:2055

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

sFlow のデフォルト：6343

- [フローセンサー（Flow Sensors）]：フローコレクタを選択します。



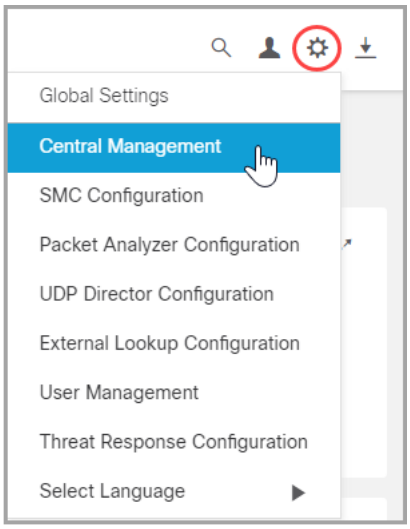
6. [Central Managementに移動（Go to Central Management）]をクリックします。「**5. アプライアンス ステータスの確認**」までの手順を完了します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

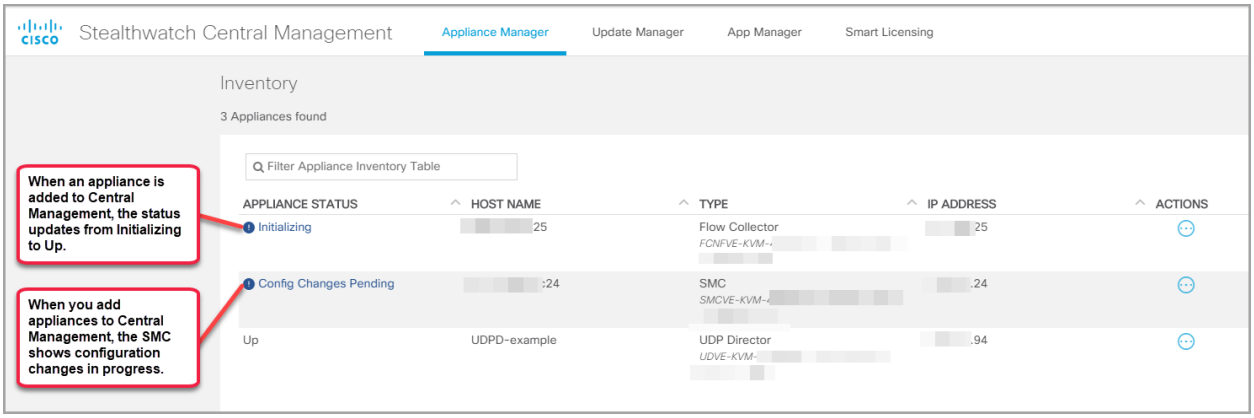
5. アプライアンス ステータスの確認

アプライアンス設定ツールでアプライアンスを設定したら、Central Management でアプライアンスのステータスを確認します。

1. アプライアンス設定ツールが Central Management インベントリで開きます。あるいは、次の手順で開くことができます。
   - プライマリ Stealthwatch Management Console にログインします。
   - [グローバル設定(Global Settings)] アイコンをクリックします。
   - [集中管理(Central Management)] を選択します。



2. Appliance Manager インベントリでアプライアンスを確認します。
   - アプライアンスがインベントリに表示されていることを確認します。
   - アプライアンスのステータスが [アップ(Up)] として表示されていることを確認します。



⚠ クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ(Up)] として表示されていることを確認してください(設定の順序と詳細を使用)。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. システム内の次のアプライアンスを設定するには、「**1. ログイン**」に進み、「**5. アプライアンス ステータスの確認**」までの手順を完了します。

   設定する別のアプライアンスがない場合は、「**6. アプライアンス設定の完了**」に戻ります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

6. アプライアンス設定の完了

各アプライアンスの設定を完了するには、次の手順を使用します。

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

1. 設定しているアプライアンスのリンクをクリックします。

アプライアンス	必須 設定	オプション 設定
Flow Collector	適用対象外	適用対象外
UDP Director		ハイアベイラビリティ （ハードウェアでのみ使用可能）
Flow Sensor	アプリケーション ID およびペイロード	アプリケーションの識別
Endpoint Concentrator	NetFlow コレクタへの接続	

2. 表内の各アプライアンスの設定および再起動が完了したら、「**7. Stealthwatch デスクトップ クライアントのインストール**」に進みます 。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

UDP Director

UDP Director の設定を完了するには、次の手順を使用します。

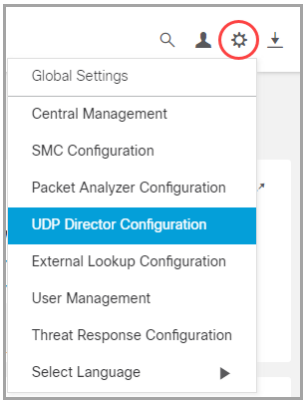
> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

- **転送ルール**：高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します。「**転送ルールの設定**」を参照してください。
- **高可用性**：複数の UDP Director がある場合、高可用性ペアを設定することができます。高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します（「**ハイアベイラビリティの設定**」に進みます）。

転送ルールの設定

UDP Director から Stealthwatch Management Console（SMC）へのメッセージ送信には SSL が使用されます。

1. SMC にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。[UDP Director設定（UDP Director Configuration）] を選択します。



3. アプライアンスの [アクション（Actions）] メニューをクリックします。[転送ルールの設定（Configure Forwarding Rules）] を選択します。
4. [Add New Rule] をクリックします。
5. **説明（Description）**：ルールを識別するための短い説明を入力します。
6. **送信元 IP アドレス：ポート（Source IP Address:Port）**：UDP Director にデータを送信するデバイスの IP アドレスを入力し、データ送信用のポート番号を入力します。
   - **形式**：[IP アドレス]:[ポート番号] の構文を使用します。
   - **範囲**：Classless Inter-Domain Routing（CIDR）表記法を使用して IPアドレスの範囲を入力することができます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **すべて**:「All」と入力すれば、このポートで任意の送信元 IP アドレスからデータを受け入れられます。
- **組み合わせ**:「送信元 IP アドレス:ポート」の組み合わせをルールに追加するには、それらを新しい行に追加します。

例:

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **宛先 IP アドレス(Destination IPAddress)**:UDP Director からデータを受け取るデバイスの IP アドレスを入力します。
8. **宛先ポート番号(Destination Port Number)**:受信するデバイスのポート番号を入力します。
9. **[保存(Save)]**をクリックします。
10. **オプション**:変更を同期するには、[同期(Sync)]をクリックします。
11. 必要に応じて、転送ルールを追加する手順を繰り返します。
12. 高可用性ペアを設定するには、「**ハイアベイラビリティの設定**」に進みます。

> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

高可用性ペアを設定する必要がない場合は、「**6. アプライアンス設定の完了**」に戻ります。

ハイアベイラビリティの設定

複数の UDP Director がある場合は、アプライアンス管理インターフェイスを使用して高可用性を設定します。

> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

UDP Director HA(高可用性)では、冗長 UDP Director を設定できます。両方のノードが完全冗長ですが、任意の時点で 1 つのノードだけがオンラインになります。

プライマリ ノードおよびセカンダリ ノード

ペアの中でオンライン ノードをプライマリ、オフライン ノードをセカンダリといいます。ペアのプライマリ ノードで障害が発生した場合、セカンダリ ノードがそれを引き継いでプライマリになります。

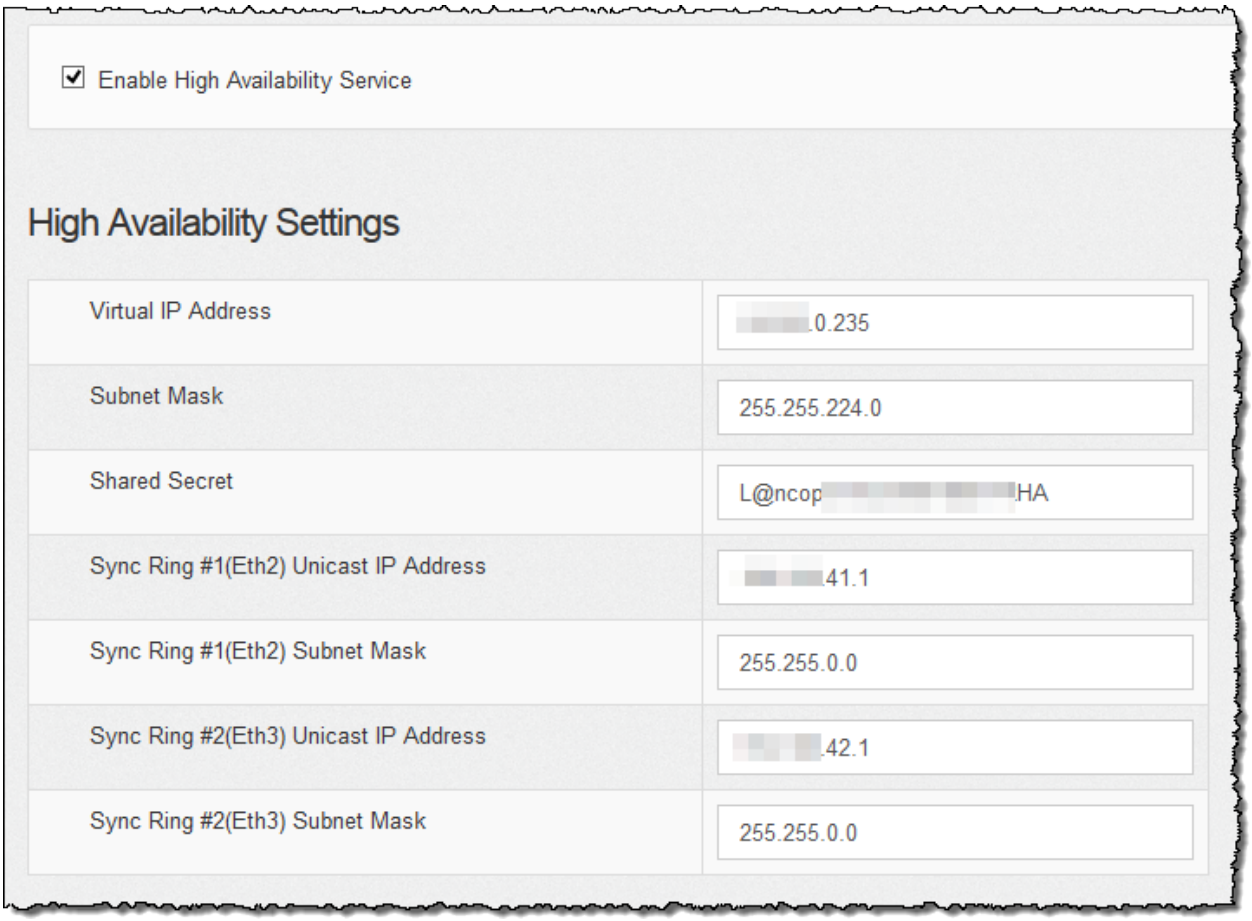
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

要件

- **転送ルール**:HA システムの UDP Director 用の転送ルールを 1 つ以上設定します。
- **ルール設定ファイルを保存**: UDP Director 用のルールがすでに設定されている場合、UDP Director ルールをエクスポート(ルール設定ファイルを保存)します。次に、このファイルを 2 番目の UDP Director にインポートして、それぞれのルールが一致するようにします。
- **順序**:最初にプライマリ UDP Director を設定した後、セカンダリで設定を繰り返します。
- **新規または設定済み**:どちらも新しい UDP Director である場合、それぞれについてこのガイドの手順に従います。ただし、セカンダリがすでに Stealthwatch システム上のアプライアンスとして設定済みであれば、セカンダリ UDP Director にログインし、このセクションの説明に従って HA コンポーネントを設定します。

1. プライマリ UDP Director HA の設定

1. プライマリ UDP Director アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)]>[高可用性(High Availability)]をクリックします。
3. 高可用性設定の[高可用性サービスの有効化(Enable High Availability Service)]チェックボックスをオンにします。



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. [仮想IPアドレス(Virtual IP Address)]フィールドに、eth0 インターフェイスと同じサブネット上にある未使用の IP アドレスを入力します。サブネットマスク値を、eth0 インターフェイスで使用されるサブネットマスクの値に設定します。

> 仮想 IP アドレスが両方のノードで同じであることを確認します。

5. [共有シークレット(Shared Secret)]フィールドで、両方の UDP Director 用の文字列を入力します。(これはセキュアな転送用に暗号化されます。)
6. 同期リング 1(Eth2)ユニキャスト IP アドレス用のフィールドに、IP アドレスとサブネット マスクを入力します。(ユニキャスト IP アドレスは単一のネットワーク宛先を識別します。)
7. 同期リング 2(Eth3)ユニキャスト IP アドレス用のフィールドに、IP アドレスとサブネット マスクを入力します。

   各 IP アドレス(eth0、eth02、eth03)は、それぞれ別個のユニキャスト サブネット上である必要があります。

8. 設定を確認したら、[適用(Apply)]をクリックして、設定を適用します。
9. クラスターの 2 番目の UDP Director を設定するには、次のセクションに進みます。

2. セカンダリ UDP Director HA の設定

セカンダリ UDP Director を設定するには次の手順を実行します。

1. セカンダリ UDP Director アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)]>[高可用性(High Availability)]をクリックします。
3. この画面ですべてのパラメータを設定します(最初のアプライアンスで詳細パラメータを変更した場合にはそれも含みます)。その際、次の項目を除くすべてのフィールドで、最初のアプライアンスとまったく同じ値を設定してください。

   - 同期リング 1(Eth2)ユニキャスト IP アドレス:プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 1 ユニキャスト アドレスと同じサブネットにある必要があります。
   - 同期リング 2(Eth3)ユニキャスト IP アドレス:プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 2 ユニキャスト アドレスと同じサブネットにある必要があります。

4. [適用(Apply)]をクリックして変更内容を保存し、このアプライアンスのクラスタリング サービスを開始します。
5. プライマリ アプライアンスを指定するには、[昇格(Promote)]ボタンをクリックします。
6. **再起動**:[操作(Operations)]>[アプライアンスの再起動(Restart Appliance)]を選択します。
7. 「**6. アプライアンス設定の完了**」に戻ります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

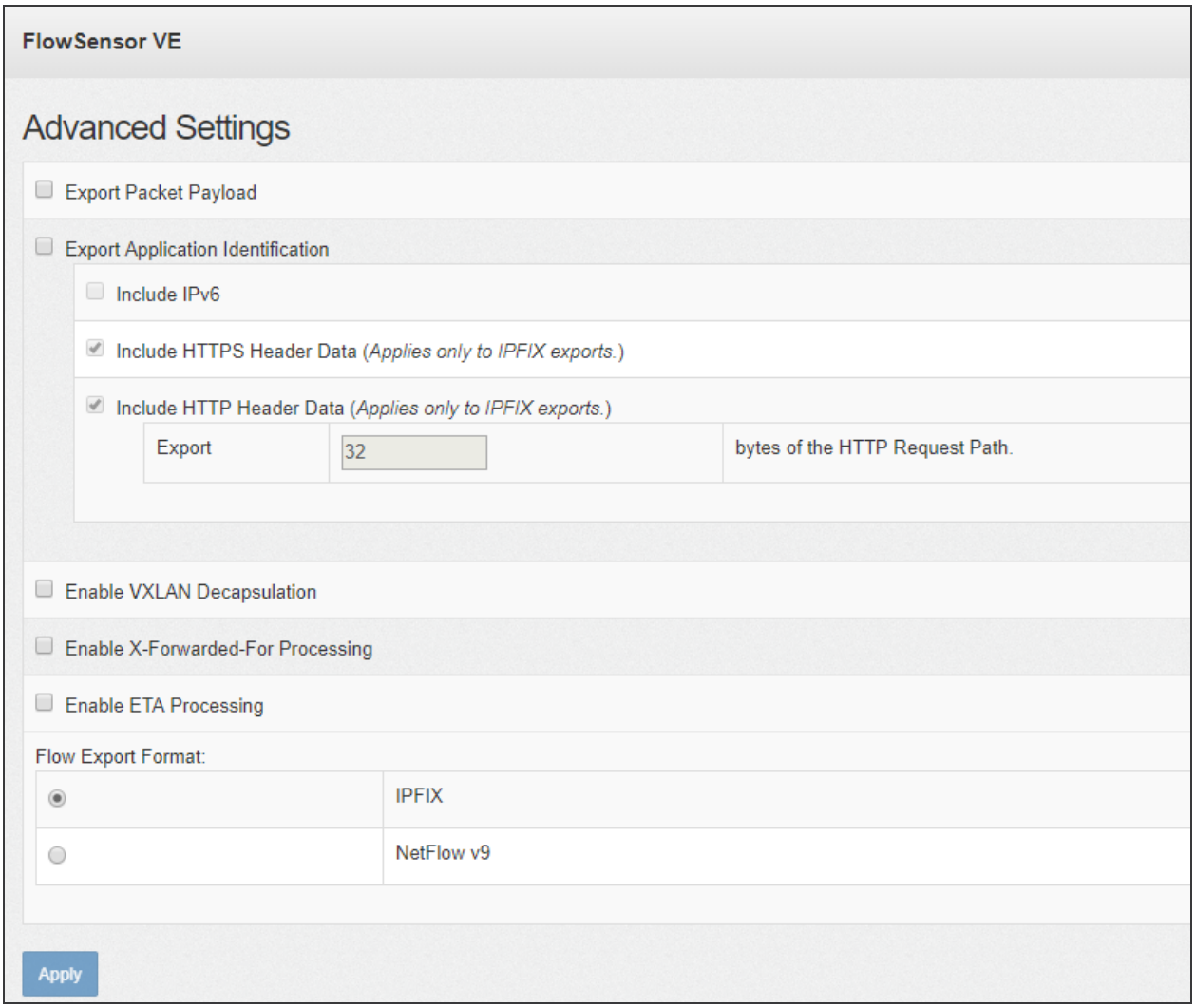
Flow Sensor

1. アプリケーション ID およびペイロードの設定

フロー センサーを設定するには、アプリケーション ID とペイロードを設定する追加の手順が必要です。

1. FlowSensor アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)] > [詳細設定(Advanced Settings)] をクリックします。

エクスポート設定ページが開きます。



3. ネットワークに関する適切な設定を次のように選択します。

項目	説明
パケット ペイロードのエクス	フロー センサーがコレクタに送るデータの中に、最初の 26 バイトのバイナリ ペイロード データを含めるかどうかを指定できます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

項目	説明
ポート（Export Packet Payload）	
アプリケーション識別情報のエクスポート（Export Applications Identification）	コレクタにデータを送る前に、フロー センサーがアプリケーションの識別を試みるかどうかを指定できます。さらに、次の設定が効果を及ぼすには、この設定を有効にする必要があります。 Ipv6 を含める（Include IPv6）：フロー センサーで IPv4 と IPv6 の両方のパケットを分析するかどうかを指定できます。この設定を無効にすると、フロー センサーは IPv4 パケットのみを分析します。 HTTPS ヘッダー データのエクスポート（Export HTTPS Header Data）：フロー センサーからコレクタに送るデータの中に、HTTPS フローのヘッダー データを含めるかどうかを指定できます。データには SSL 共通名と SSL 組織名が含まれます。この設定を使用するには、フロー タイプが IPFIX に設定されている必要があります。最大 256 バイトが可能です。 HTTP ヘッダー データのエクスポート（Export HTTP Header Data）：フロー センサーからコレクタに送るデータの中に、HTTP フローのヘッダー データを含めるかどうかを指定できます。この設定を選択した場合、セカンダリ フィールドを使用して、フロー センサーでフロー データに含める HTTP パスの最大長（バイト単位）を指定できます。この設定を使用するには、フロー タイプが IPFIX に設定されている必要があります。
VXLAN カプセル化解除の有効化（Enable VXLAN Decapsulation）	FlowSensor が Virtual Extensible Local Area Network（VXLAN）カプセル化解除機能を使用するかどうかを指定できます。VXLAN カプセル化解除を使用しない場合、FlowSensor は単純に 2 つの仮想トンネルエンドポイント（VTEP）間のフローとして VXLAN カプセル化トラフィックを検出します。カプセル化解除を使用すると、トンネル化されたトラフィックを分析して、ネットワーク内のトラフィックパターンをより詳細に把握できるため、より豊富なコンテンツを取得できます。 FlowSensor は、標準の VXLAN ポート（4789）に元々送信された VXLAN トラフィックだけをカプセル化解除します。
X-Forwarded-For 処理の有効化（Enable X-Forwarded-For Processing）	FlowSensor が X-Forwarded-For（XFF）処理を使用して、HTTP プロキシまたはロードバランサを介して Web サーバに接続しているクライアントの発信元 IP アドレスを識別するかどうかを指定できます。 ETA と X-Forwarded-For 処理を一緒に設定することはできません。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

項目	説明
ETA 処理の有効化（Enable ETA Processing）	FlowSensor が ETA 処理を使用して、IDP フィールドおよび SPLT フィールドを生成して SMC に送信するかどうかを指定できます。 ETA を有効にすると、特に v9 使用時の NetFlow 帯域幅の使用量が増加します。フローエクスポート形式には IPFIX を使用することをお勧めします。 ETA と X-Forwarded-For 処理を一緒に設定することはできません。 ETA を Dell または PowerEdge FlowSensor モデルで有効にすることはできません。
フロー エクスポート形式（Flow Export Format）	フロー センサーがコレクタにフロー データを送る際に IPFIX または NetFlow v9 のどちらを使用するかを指定できます。
キャッシュ モード（Cache Mode）	次のいずれかの設定を選択できます。 すべての監視ポートに単一の共有キャッシュを使用（Use single, shared, cache for all monitoring ports）： • 非対称ルーティングが存在する場合に使用します。 • アプリケーションと遅延計算に 1 つの状態テーブル。 • より少ないメモリを使用。 • 全体的により低い pps 処理率。 • 結果として複数のインターフェイス全体で 1 つの NetFlow イベントが作成されます。 • フロー センサーにポートが 2 つだけ存在し、TAP で接続されている場合にのみ、これを使用します。 監視ポートごとに独立したキャッシュを使用（Use independent caches for each monitoring port）： • フロー センサー インターフェイスごとにパケットの重複排除が行われます。 • より多くのメモリを使用。 • 全体的により高い pps 処理率。 • 各インターフェイスは独自の遅延とアプリケーション データベースを維

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

項目	説明
	持します。 • 結果として、特定のパケットを認識するインターフェイスごとに固有のNetFlowレコードが生成されます。

4. [適用(Apply)]をクリックして設定を保存します。

2. アプリケーションを識別するための Flow Sensor の設定(オプション)

フロー センサーでアプリケーションを識別する場合、次のように設定します。

1. FlowSensor アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)]>[詳細設定(Advanced Settings)]をクリックします。
3. [アプリケーションIDのエクスポート(Export Application Identification)]チェックボックスをオンにします。デフォルトでは、このオプションは選択されていません。
4. 複数の監視 NIC がある場合、[キャッシュ モード(Cache Mode)]セクションで次のいずれかのオプションを選択します。

   - **すべてのモニタリング ポートに単一の共有キャッシュを使用する(Use single, shared, cache for all monitoring ports)**:通常、TAP 方式でフローをモニタリングするシステムに対して使用します。

   - **モニタリング ポートごとに個別のキャッシュを使用する(Use independent caches for each monitoring port)**:通常、SPAN 方式でフローをモニタリングするシステムの場合、およびパフォーマンスを強化する必要がある場合に使用します。

3. アプライアンスの再起動

1. [操作(Operations)]>[アプライアンスの再起動(Restart Appliance)]を選択します。
2. 「**6. アプライアンス設定の完了**」に戻ります。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Endpoint Concentrator

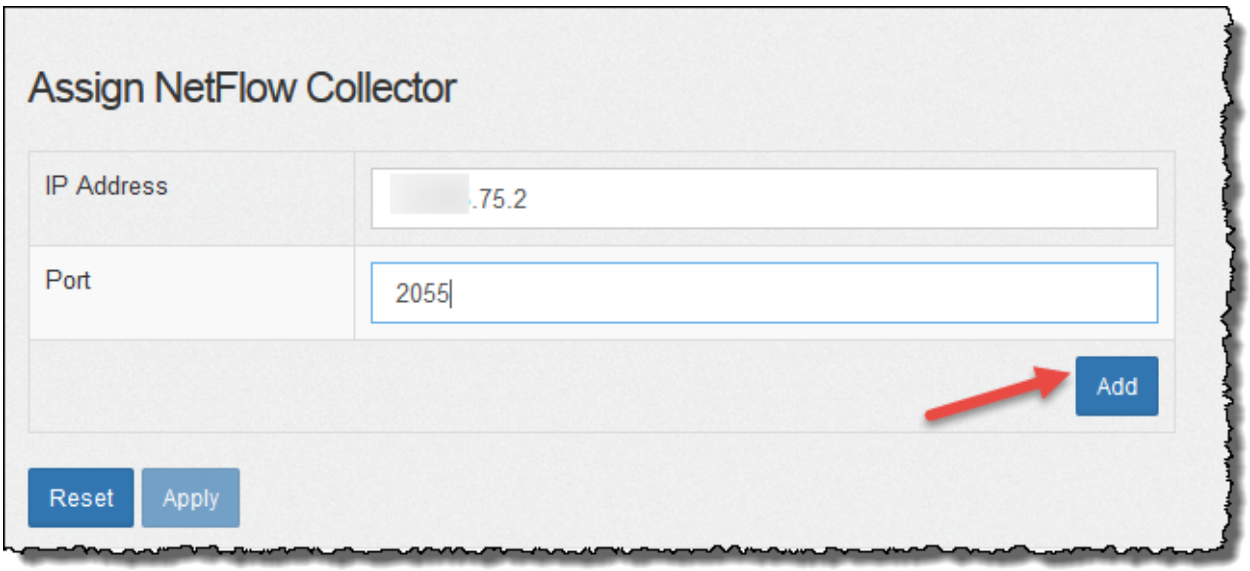
エンドポイントコンセントレータには、次の設定要件があります。

- エンドポイントアプライアンスから NetFlow フローコレクタへの接続を設定します。
- 設定できるフローコレクタは 1 つのみです。

1. エンドポイントコンセントレータにログインします。
2. [設定(Configuration)] > [収集(Collection)] をクリックします。
3. [NetFlow コレクタの割り当て(Assign NetFlow Collector)] フィールドに、エンドポイントコンセントレータがデータを送信するフローコレクタまたは UDP Director の IP アドレスおよびポート番号を入力します。

   ポートのデフォルト: 2055。

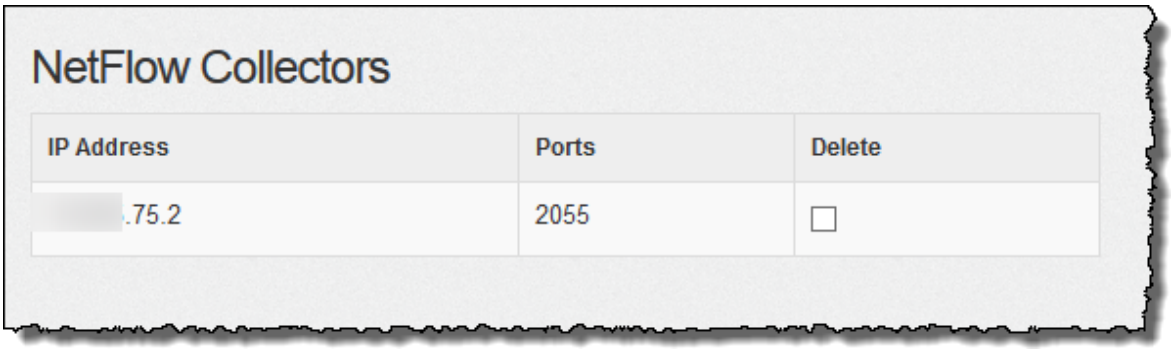
4. [追加(Add)] をクリックします。これにより、IP アドレスとポートが検証され、エントリがテーブルに移されます。



5. 情報が正しい場合は、[適用(Apply)] をクリックします。これにより、新しい情報でサービスが再起動します。

   このフィールドに入力できる値は 1 つのみです。受信者を追加する必要がある場合は、Cisco UDP Director の使用を検討してください。

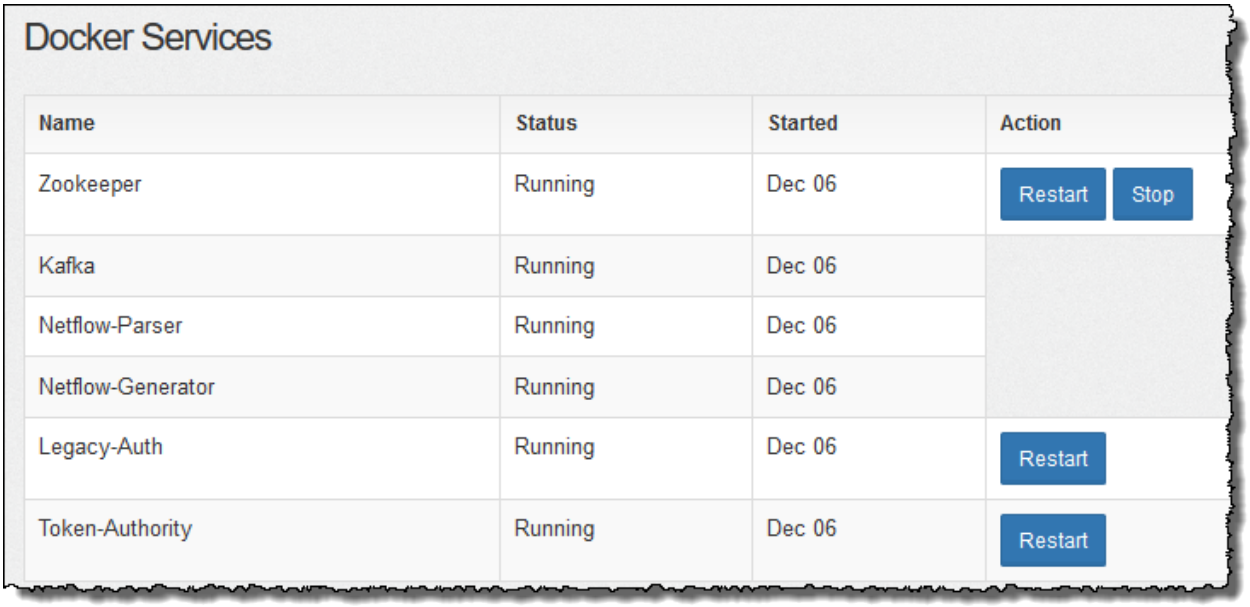
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



ページ上部のテーブルに、NetFlow コレクタの設定が表示されます。

コレクタの設定を変更する必要がある場合は、[削除(Delete)] チェック ボックスをオンにして現在のコレクタを削除してから [適用(Apply)] をクリックします。その後、新しいコレクタを設定できます。

6. メイン メニューで、[ホーム(Home)] をクリックします。Docker サービス テーブルを確認します。



7. すべての Docker サービスが [実行中(Running)] として表示されている場合は、アプライアンスを再起動します。[操作(Operations)] > [アプライアンスの再起動(Restart Appliance)] を選択します。その後、「**6. アプライアンス設定の完了**」に戻ります。

   Docker サービスが [実行中(Running)] として表示されていない場合は、「**エンドポイント コンセントレータのトラブルシューティング**」に進みます。

エンドポイント コンセントレータのトラブルシューティング

AnyConnect エージェントとエンドポイント コンセントレータの設定後、システムが動作しているかどうかを判断するために確認できるいくつかの項目があります。システムが期待どおりに

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

データを処理していないことがわかった場合は、次の手順を使用できます。

1. エンドポイントコンセントレータが AnyConnect エージェントからコレクタへのフローを受信していることを確認します。

    - Web 管理ページ経由のエンドポイントコンセントレータへの SSH アクセスを有効にします。

    - [設定(Configuration)] > [サービス(Services)]:[SSHを有効化(Enable SSH)]

2. エンドポイントコンセントレータコンソールにログインします。「docker ps」を実行します。

    - kafka、netflow-parser、zookeeper、および netflow-generator を含む 4 つのエントリがあることを確認します。コンテナ ID とイメージ バージョンは違うことに注意してください。
    - 実行されていない場合は、アプライアンスからサービスを再起動します。

3. ディレクトリを「/lancope/var/logs/containers」に変更し、「tail -f svc-endpoint-engine:vx.x.x.log」を実行します。ここで、x.x.x.x はファイル名に示されているバージョンです。ステータスのプリントアウトで数値がゼロではないことを確認します。ステータスがゼロと表示される場合、エンドポイントコンセントレータは Netflow を生成していません。
4. AnyConnect エージェントがエンドポイントコンセントレータにデータを送信できることを確認します。

    - AnyConnect エージェントを実行しているいずれかのマシンで、端末プロンプトまたはコマンドプロンプトを開き、「ping <IPofEndpointConcentrator>」を実行します。
    - 応答バイトがある場合、エージェントはエンドポイントコンセントレータにエクスポートできると考えられます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

7. Stealthwatch デスクトップ クライアントのインストール

以下の手順で、Windows または macOS を使用して Stealthwatch デスクトップ クライアントをインストールします。次の点に注意してください。

- Stealthwatch デスクトップ クライアントのさまざまなバージョンをローカルにインストールすることができます。
- Stealthwatch デスクトップ クライアントの複数のバージョンにアクセスするには、各 SMC において異なる実行ファイルが必要になります。
- プライマリ SMC とセカンダリ SMC の両方を使用している場合は、一方の SMC をログオフして、その後もう一方の SMC にログインする必要があります。
- Stealthwatch デスクトップ クライアントの複数のバージョンを同時に開くことができます。
- Stealthwatch の最新のバージョンに更新する場合は、Stealthwatch デスクトップ クライアントの新しいバージョンをインストールする必要があります。
- すでに Stealthwatch デスクトップクライアントがあり、v7.1 に更新する場合、Stealthwatch デスクトップクライアントで Oracle Java を使用できなくなります。

Windows を使用したデスクトップ クライアントのインストール

- Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
- Stealthwatch デスクトップ クライアントには、64 ビットのオペレーティング システムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

1. Stealthwatch Web アプリケーションの任意のページの右上隅にある [ダウンロード (Download)] アイコンをクリックします。

2. .exe ファイルをクリックして、インストール プロセスを開始します。
3. ウィザードの手順を実行して Stealthwatch デスクトップ クライアントをインストールします。
4. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
5. SMC ユーザ名およびパスワードを入力します。
6. SMC サーバ名または IP アドレス(IPv4 または IPv6)を入力します。
7. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

メモリサイズの変更

Stealthwatch デスクトップ クライアント インターフェイスを実行するために、クライアント コンピュータで割り当てるランダム アクセス メモリ(RAM)の量を変更できます。開いている多数のドキュメントや大量のデータ セット(100,000 個を超えるレコードが含まれたフロー クエリなど)を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. Windows Explorer で、ホームディレクトリに移動します。
2. これらのフォルダを次の順に開きます。AppData > ローミング > Stealthwatch。

   フォルダが非表示の場合は、「Stealthwatch」を検索する必要がある場合があります。

3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して **application.vmoptions** ファイルを開き、編集を開始します(このファイルは、Stealthwatch デスクトップ クライアントを最初に開いた後に作成されます)。

   最小メモリサイズ(Xms):512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

   最大メモリサイズ(Xmx):最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

   すべての番号を使用します。たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

> - Stealthwatch デスクトップ クライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
> - Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

macOS を使用したデスクトップ クライアントのインストール

> - Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
> - Stealthwatch デスクトップ クライアントには、64 ビットのオペレーティング システムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. Stealthwatch Web アプリケーションの任意のページの右上隅にある [ダウンロード (Download)] アイコンをクリックします。

2. .dmg ファイルをクリックして、インストール プロセスを開始します。

   アイコンとフォルダは、以下に示すようにモニタに表示されます。

3. Stealthwatch デスクトップ クライアントのアイコンを ( ) アプリケーションのフォルダにドラッグします。

   アイコンは、スタート パッドに追加されます。

4. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
5. SMC ユーザ名およびパスワードを入力します。
6. SMC サーバ名または IP アドレス (IPv4 または IPv6) を入力します。
7. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

メモリサイズの変更

Stealthwatch デスクトップ クライアント インターフェイスを実行するために、クライアント コンピュータで割り当てるランダム アクセス メモリ (RAM) の量を変更できます。開いている多数のドキュメントや大量のデータ セット (100,000 個を超えるレコードが含まれたフロー クエリなど) を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. 検索で、ホーム ディレクトリに移動します。
2. Stealthwatch フォルダを開きます。
3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して application.vmoptions ファイルを開き、編集を開始します (このファイルは、Stealthwatch デスクトップ クライアントを最初に開いた後に作成されます)。

   最小メモリサイズ (Xms) : 512 MB 以上を割り当てることをお勧めします。この番号は、

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ファイルの 3 番目の行に表示されます。

コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

最大メモリサイズ(Xmx) : 最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

すべての番号を使用します。たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

- Stealthwatch デスクトップ クライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
- Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

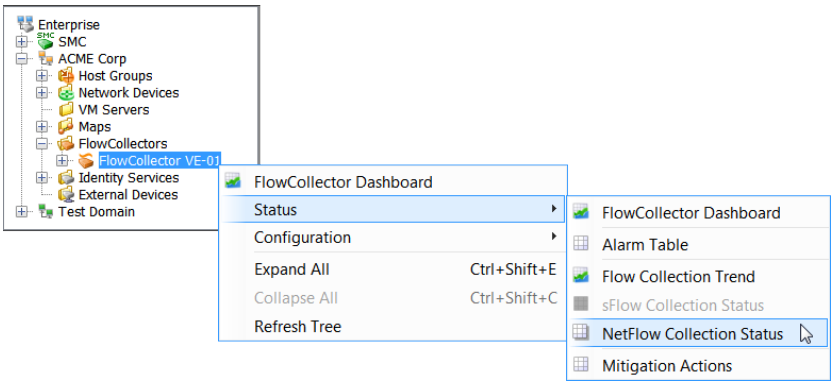
© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

8. 通信の確認

次の手順を使用して、Stealthwatch Management Console が NetFlow データを受信していることを確認します。

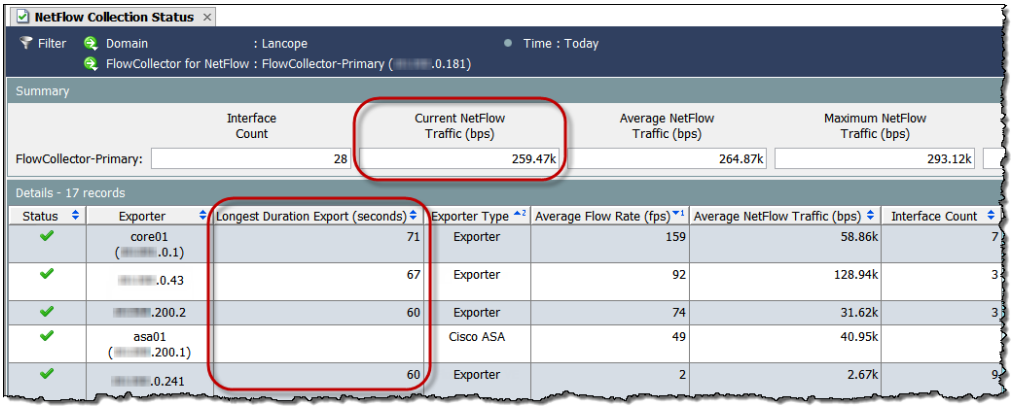
NetFlow データ収集の確認

1. Stealthwatch デスクトップ クライアントのエンタープライズ ツリーで、フローコレクタを右クリックします。[ステータス(Status)] > [NetFlowコレクションステータス(NetFlow Collection Status)] の順に選択します。



2. [NetFlowコレクションステータス(NetFlow Collection Status)] ページで、ドキュメントの上部にある [現在のNetFlowトラフィック(Current NetFlow Traffic)] フィールドを参照します。この統計情報は検出された NetFlow トラフィックの量を示します。

   - トラフィックが表示されている場合は、次の手順に進みます。
   - トラフィックが表示されていない場合は、エクスポータおよびルータの設定を確認します。詳細については、SMC クライアントのオンライン ヘルプを参照してください。次の手順に進みます。



3. [最も長い継続時間のエクスポート(Longest Duration Export)] 列を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

列の追加:この列をダッシュボードに追加するには、列ヘッダーを右クリックし、メニューから[最も長い継続時間のエクスポート(Longest Duration Export)]を選択します。

4. 各エクスポータの値は 100 よりも下ですか。

   - 「はい」の場合、キャッシュのエクスポートタイマーは正常です。
   - 「いいえ」の場合、高い値はキャッシュのエクスポートタイマーが正しくないことを示し、誤ったアラームが発生する可能性があります。エクスポータおよびルータの設定を確認します。詳細については、SMC クライアントのオンライン ヘルプを参照してください。

5. Congratulations! Stealthwatch のシステム設定が完了しました。
6. 次のステップ:「**9. ライセンス**」を確認し、評価期間が終了する前に Cisco スマートアカウントに製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。

7. Stealthwatch に別のサービスと機能を追加するには、次のリソースを参照してください。

   - **SMC フェールオーバー関係の定義**
   - **脅威インテリジェンスフィードの有効化**
   - **SAML SSO の設定**

> ℹ Cisco.com を参照して Stealthwatch のガイドを確認し、Cisco Threat Response、Cisco Identity Services(ISE)、TACACS+ などの追加機能を設定します。

Stealthwatch の使用を開始するには、このガイドの次の項を参照してください。

- **概要**:**Stealthwatch の概要**の項には、環境の管理、動作の調査、脅威への対応などに関する詳細が記載されています。
- **Central Management**:アプライアンス管理と設定変更の詳細については、このガイドの「Central Management」の項を参照してください。
- **トラブルシューティング**:このガイドの「トラブルシューティング」の項を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

9. ライセンス

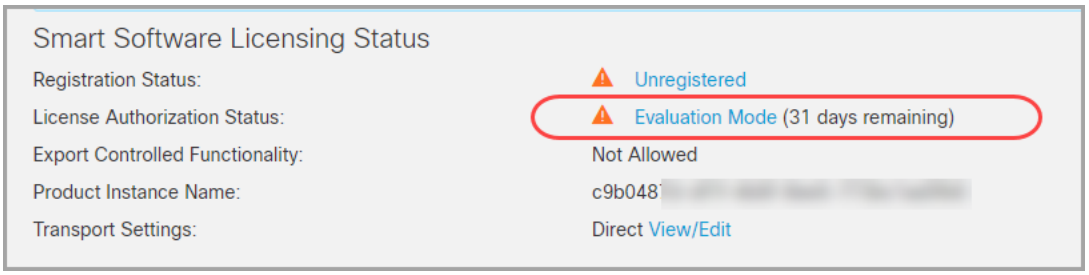
シスコ スマート ソフトウェア ライセンシングを使用して、Stealthwatch のアプライアンスおよび機能をライセンシングします。詳細については、cisco.com のスマートライセンシングを参照してください。

- **オンライン**：スマートライセンシング および Stealthwatch をオンラインで使用するには、『Stealthwatch Smart Software Licensing Guide』を参照してください。この設定にはインターネットアクセスが必要です。
- **オフライン**：クローズド/エアギャップネットワークのライセンスオプションの説明については、Cisco Stealthwatch サポートに連絡してください。
- **Cisco スマートアカウント**：Cisco スマートアカウントを設定するには、https://software.cisco.com で登録するか、管理者にお問い合わせください。

評価モード

Stealthwatch を評価モードで使用すると、選択された機能を 90 日間使用できます。Stealthwatch のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。



- **管理者ユーザ**：Stealthwatch Management Console でスマートライセンシングのステータスと使用状況の詳細を確認するには、管理者ユーザとしてログインします。
- **残り日数**：評価モードの残り日数を確認するには、管理者ユーザとして Stealthwatch Management Console にログインします。[集中管理（Central Management）] > [スマートライセンシング（Smart Licensing）] の順に移動します。[ライセンス承認ステータス（License Authorization Status）] を確認します。
- **製品インスタンス**：製品インスタンスはお客様の Stealthwatch の製品インスタンスに使用する識別子であり、Stealthwatch Management Console と管理アプライアンスが含まれます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SMC フェールオーバー関係の定義

2 つの Stealthwatch Management Console（SMC）間のフェールオーバー関係を確立することにより、それらの一方がもう一方のバックアップ コンソールとして機能するようにすることができます。フェールオーバー関係を定義する場合は、1 つの SMC をプライマリ、1 つの SMC をセカンダリとして指定します。プライマリがオフラインの場合は、セカンダリ SMC を手動でプライマリ SMC に設定してシステムのモニタリングを継続することができます。

SMC フェールオーバー関係を定義するには、Stealthwatch オンライン ヘルプの手順に従います。

- **最初にセカンダリ SMC を設定して、**プライマリ SMC がそれを認識して通信できるようにします。
- ライセンス：詳細については、Stealthwatch スマート ソフトウェア ライセンシング ガイド [英語] を参照してください。
- **信頼ストア証明書**：この手順の一環として、必要な信頼ストアにアプライアンス アイデンティティ証明書を追加します。手順に従ってください。
- **アプライアンスの追加または削除**：Central Management でのアプライアンスの追加や削除は、フェールオーバーの設定を完了し、Central Management でセカンダリ SMC アプライアンスのステータスが [アップ（Up）] と表示されるまで行わないでください。

1. プライマリにする SMC とセカンダリにする SMC を計画します。
2. ログインします。
3. システム内でのフェールオーバー ロールを設定する前に、Stealthwatch オンライン ヘルプの手順を確認し、その手順に従ってください。

    - エンタープライズ ツリーで、SMC を右クリックします。
    - [設定（Configuration）] > [SMCフェールオーバー（SMC Failover）] を選択します。
    - [ヘルプ（Help）] をクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

脅威インテリジェンスフィードの有効化

脅威インテリジェンスフィードは、ネットワークに対する脅威に関するグローバル脅威インテリジェンスフィードからのデータを提供します。フィードは頻繁に更新され、悪意のあるアクティビティに使用されたことがわかっている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれています。フィードには、コマンドアンド コントロール サーバ、bogon、および Tor の各ホストグループが含まれています。

ライセンス

脅威インテリジェンスフィードのライセンスを Cisco スマートアカウントに追加します。手順については、Stealthwatch スマート ソフトウェア ライセンシング ガイド [英語] を参照してください。

有効

Central Management でフィードを有効にするには、オンラインヘルプの手順に従います。手順の一部として DNS サーバとファイアウォールを設定することに注意してください。

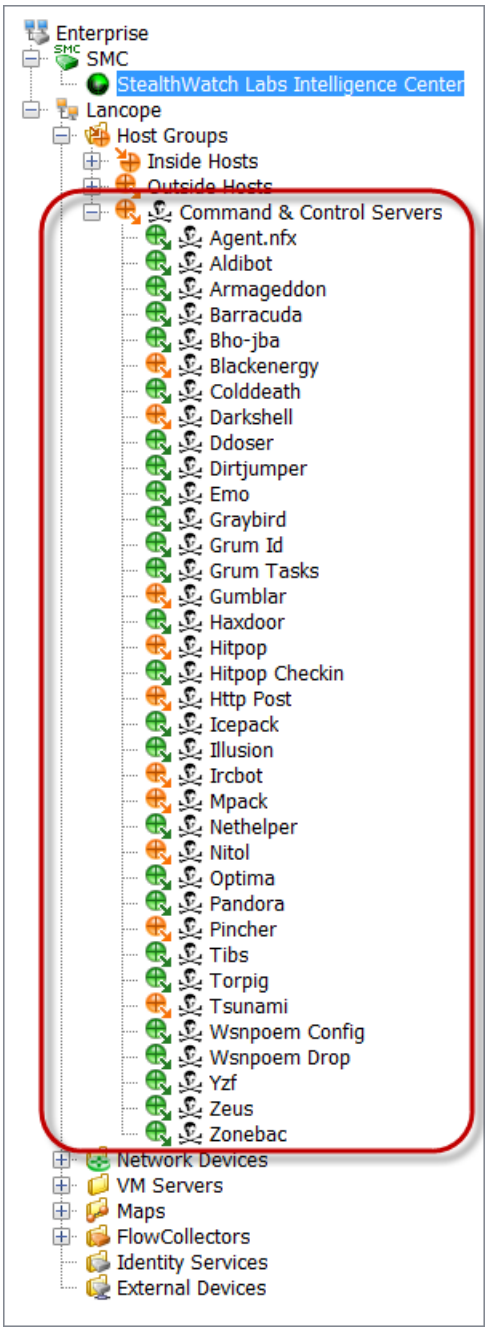
1. プライマリ Stealthwatch Management Console にログインします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [集中管理 (Central Management)] を選択します。
4. [ユーザ (User)] アイコンをクリックします。[Stealthwatch オンライン ヘルプ (Stealthwatch Online Help)] を選択します。
5. [アプライアンス設定 (Appliance Configuration)] > [脅威インテリジェンスフィード (Threat Intelligence Feed)] を選択します。

アラームとセキュリティイベントの確認

脅威インテリジェンスフィードが有効になっている場合、Stealthwatch Labs Intelligence Center のアイコンが Stealthwatch デスクトップクライアントの企業ツリーにアラームステータスとともに表示され、脅威は各ホストグループのブランチに表示されます。詳細については、Stealthwatch デスクトップ クライアント ユーザ ガイド [英語] またはオンラインヘルプを参照してください。

> **オンラインヘルプ**:オンラインヘルプにアクセスするには、[Stealthwatchラボインテリジェンスセンター (Stealthwatch Labs Intelligence Center)] ブランチを右クリックし、[設定 (Configuration)] > [SLIC脅威フィード設定 (SLIC Threat Feed Configuration)] の順に選択します。[ヘルプ (Help)] をクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SAML SSO の設定

以下の手順に従って、セキュリティアサーション マークアップ言語シングル サインオン(SAML SSO)を設定します。SSO は、ユーザが 1 組のクレデンシャルで複数のアプリケーションにアクセスすることを可能にする認証プロセスです。

未サポート:SSO は Stealthwatch デスクトップ クライアントではサポートされていません。SSO は統合 Windows 認証(IWA)ではサポートされていません。

1. 設定の準備

SSO を設定するには次の情報が必要です。

要件	詳細
アイデンティティ プロバイダーの URL	この URL には完全修飾ドメイン名または IPv4 アドレスを使用する必要があります。
アイデンティティ プロバイダーの証明書	IDP の URL が「HTTPS」で始まる場合は、CA 証明書をダウンロードしてください。

2. 信頼ストアへの証明書のアップロード

アイデンティティ サービス プロバイダー(IDP)の URL が「HTTPS」で始まる場合は、**ルート CA 証明書**を SMC 信頼ストアに追加します。

> IDP の URL が「HTTPS」で始まらない場合は、この手順をスキップして次のセクション「**3. サービス プロバイダーの設定**」に進むことができます。

以下の手順に従って、ルート CA 証明書を SMC 信頼ストアに追加します。

1. [Central Management] の [Appliance Manager] ページで、SMC の [アクション(Actions)] メニューをクリックします。
2. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
3. [Appliance Manager] > [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
4. [新規追加(Add New)] をクリックします。
5. [フレンドリ名(Friendly Name)] フィールドに、証明書の名前を入力します。
6. [ファイルの選択(Choose File)] をクリックします。新しい証明書を選択します。
7. [証明書の追加(Add Certificate)] をクリックします。[信頼ストア(Trust Store)] リストに新しい証明書が表示されることを確認します。
8. [設定の適用(Apply settings)] をクリックします。画面に表示される指示に従って操作します。
9. **Up**:[Appliance Manager] ページで、SMC が設定変更を完了し、アプライアンスのステータスが **Up** に戻ることを確認します。

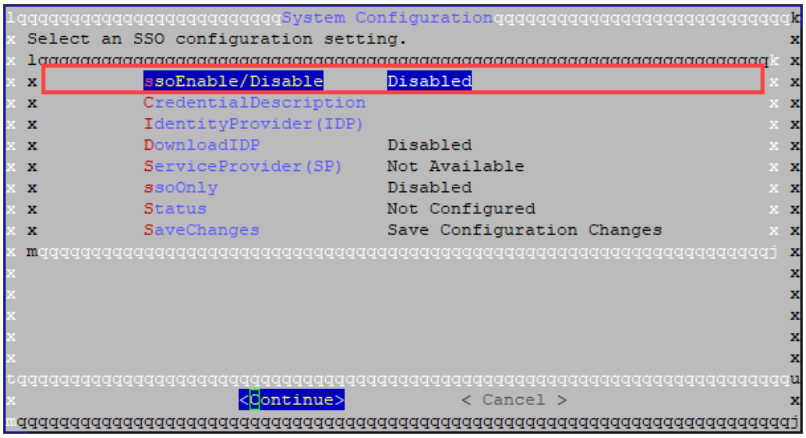
> ⚠ 設定の変更が保留中の間は、アプライアンスを再起動させないでください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

10. セカンダリ SMC がある場合は、この手順を繰り返して、ルート CA 証明書をセカンダリ SMC 信頼ストアに追加します。
11. ルート CA 証明書を SMC 信頼ストアに追加した場合は、次のセクションに進みます。

3. サービス プロバイダーの設定

1. SMC コンソールに root としてログインします。
2. `SystemConfig` と入力します。Enter を押します。
3. [詳細設定(Advanced)] を選択します。
4. [SSO] を選択します。
5. [SSO 有効/無効(ssoEnable/Disable)] が [無効(Disabled)] と表示されていることを確認します。



6. [アイデンティティプロバイダー(IDP)(IdentityProvider(IDP))] を選択します。[続行(Continue)] をクリックします。
7. アイデンティティプロバイダーの設定ファイルをダウンロードできる URL を入力します。

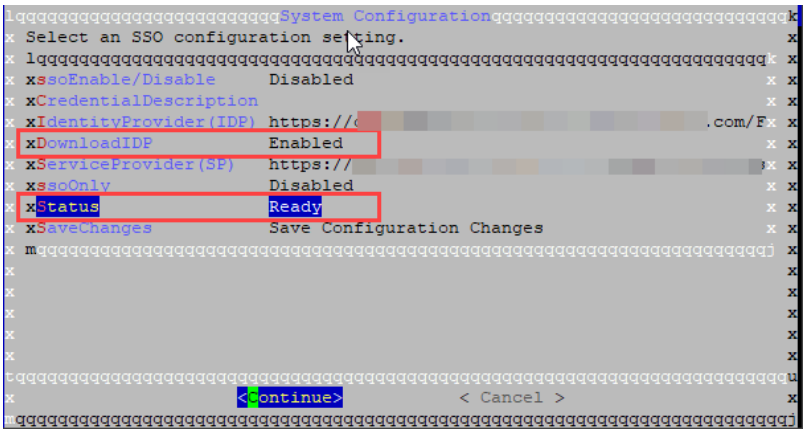
   Requirements(要件):完全修飾ドメイン名または IPv4 アドレスを入力します。

8. [IDP のダウンロード(DownloadIDP)] を選択します。画面に表示される指示に従って、有効にします。
9. [変更の保存(SaveChanges)] を選択します。[続行(Continue)] をクリックします。

   画面の指示に従って、IDP 設定ファイルをダウンロードします。

10. [SSO] を選択します。
11. [サービスプロバイダー(SP)(ServiceProvider(SP))] を確認します。URL をコピーしてください。これは、アイデンティティプロバイダーの設定に使用します。
12. [ステータス(Status)] を確認します。これが [準備(Ready)] と表示されていることを確認してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



4. SSO の有効化

1. [SSO 有効/無効(ssoEnable/Disable)]を選択します。
2. 画面に表示される指示に従って、SSO を有効にします。
3. [クレデンシャルの説明(CredentialDescription)]を選択します。[続行(Continue)]をクリックします。
4. ユーザがログインするために必要な SSO サービス クレデンシャルの説明を入力します。
5. [OK]をクリックします。
6. [IDP のダウンロード(DownloadIDP)]を選択します。新しい SSO 設定を保存する必要があるまで[IDP のダウンロード(DownloadIDP)]を無効にします。

   - [続行(Continue)]をクリックします。
   - 画面に表示される指示に従って、[IDP のダウンロード(DownloadIDP)]を無効にします。

7. [変更の保存(SaveChanges)]を選択します。[続行(Continue)]をクリックします。
8. システム設定を終了します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. アイデンティティ プロバイダーの設定

1. ブラウザのアドレス フィールドにサービス プロバイダーの URL を入力します。
2. サービス プロバイダーのメタ データファイル sp.xml をダウンロードします。
3. sp.xml を使用してアイデンティティ プロバイダーを設定します。
4. 発信クレーム タイプにユーザの電子メール アドレスが含まれていることを確認します。

   - **例**：属性ストアが Active Directory の場合、発信クレーム タイプを LDAP 属性タイプのユーザ ID の電子メール アドレスに設定します。
   - **Microsoft Active Directory ファイル サーバ（ADFS）**：IDP タイプが ADFS の場合は、次のカスタム ルールが表示されていることを確認します。

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

6. SSO ユーザの追加

SSO ユーザを追加するには、次の手順を使用します。ユーザはアイデンティティ プロバイダーを介して（アイデンティティ プロバイダーによって）認証されます。

1. SMC（Stealthwatch Web アプリケーション）にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [ユーザ管理（User Management）] を選択します。
4. [作成（Create）] > [ユーザ（User）] の順に選択します。

   手順については、[ユーザ（User）] アイコンをクリックします。 [Stealthwatch オンライン ヘルプ（Stealthwatch Online Help）] を選択します。ユーザの追加の詳細については、「ユーザの設定」を参照してください。

5. フィールドに入力して、新しいユーザを作成します。次のようにユーザを設定してください。

   - **認証サービス（Authentication Service）**：[SSO] を選択します。
   - **ユーザ名（User Name）**：IDP アカウントの電子メール アドレスの最初の部分を入力します。ID がログイン時に SSO に使用されるものと同じであることを確認してください。たとえば、name @ cisco.com の場合、このフィールドに「 name 」と入力します。

6. [保存（Save）] をクリックします。
7. [ユーザ管理（User Management）] に [SSO ユーザ（SSO User）] が表示されていることを確認します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

7. SAML ログインのテスト

1. SMC（Stealthwatch Web アプリケーション）にログインします。
2. ログイン ページで、ドロップダウンをクリックします。
3. [SAML] を選択します。
4. クレデンシャル ボタンをクリックします。
5. ログイン クレデンシャルを入力します。[セキュリティ分析ダッシュボード（Security Insight Dashboard）] が開きます。

トラブルシューティング

シナリオ	注記
アカウントのロックアウト	緊急アカウント アクセスを使用してシステム設定で [SSO のみ（SSO Only）] を無効にします。
IDP XML をダウンロードできない	IDP 証明書が SMC 信頼ストアにアップロードされていることを確認します。
IDP 設定を保存できない	IDP 設定を調べて、入力したデータが正確で、余分なスペースが含まれていないことを確認します。また、IDP イベント ログを調べます。
その他の問題	使用しているブラウザ用の SAML トレーサーをダウンロードします。SSO ログインを繰り返して、IDP と SP の間の交換を確認します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Stealthwatch の概要

アプライアンスの設定が完了したら、Stealthwatch オンラインヘルプで、環境の管理、動作の調査、脅威への対応などに関する指示を得られます。

概要

Stealthwatch の概要については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [Stealthwatchコンポーネント(Stealthwatch Components)] > [Stealthwatch Management Console(SMC)の概要(Stealthwatch Management Console(SMC) Overview)] > [Stealthwatch Webアプリケーションのバージョン(About Stealthwatch Web App)] の順に選択します。

環境の管理

ネットワークセキュリティ管理の一環として、いくつかの準備作業を行う必要があります。各ページにアクセスするためのメニューが、次の各トピックとともに表示されます。手順については、任意のページから [ユーザ(User)] アイコン > [Stealthwatchオンラインヘルプ(Stealthwatch Online Help)] を選択して確認してください。

- ホストグループの設定([設定(Configure)] > [ホストグループ管理(Host Group Management)]))
- ポリシーの作成と管理([設定(Configure)] > [ポリシー管理(Policy Management)])
- フロー検索の作成([分析(Analyze)] > [フロー検索(Flow Search)])
- Stealthwatch を使用するためのユーザ権限の管理([グローバル設定(Global Settings)] アイコン > [ユーザ管理(User Management)])

動作の調査

アラーム、イベント、ホストなどの調査については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [動作の調査(Investigating Behavior)] を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

脅威への対応

ポリシー情報については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [脅威への対応(Responding to Threats)] を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Central Management

Central Management を使用して、プライマリ SMC からアプライアンスを管理します。ここでは、Central Management の概要について説明します。各セクションの詳細については、Stealthwatch オンライン ヘルプを参照してください。

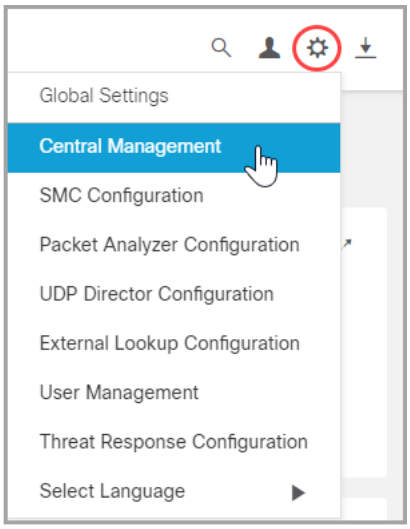
- **Central Management について**：アプライアンスが Central Management によって管理されている場合、それらのステータスを確認できるのに加えて、アプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどを管理できます。
- Stealthwatch オンラインヘルプ：Stealthwatch オンラインヘルプを開くには、[ユーザ（User）] アイコンをクリックします。 [Stealthwatch オンライン ヘルプ（Stealthwatch Online Help）] を選択します。

Central Management と アプライアンス管理インターフェイス

アプライアンスが Central Management で管理されている場合、アプライアンスの機能には、Central Management およびアプライアンス管理インターフェイス（アプライアンス管理）からアクセスします（次の表を参照）。

Central Management	アプライアンス管理インターフェイス
アプライアンス構成の編集	システム統計情報の表示
ライセンス ステータスの確認（概要）	
構成ファイルのバックアップ	データベースファイルのバックアップ
監査ログの表示	診断パックの作成
再起動	ネットワークホストと IP の検索
シャットダウン	パケット キャプチャ
ソフトウェアの更新	DNS キャッシュのクリア
	アプライアンス固有の設定

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



Central Management を開く

1. プライマリ SMC にログインします。
2. [グローバル設定(Global Settings)] アイコンをクリックします。
3. [集中管理(Central Management)] を選択します。

アプライアンス管理を開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

Central Management を通じてアプライアンス管理を開く

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
3. アプライアンス管理インターフェイスにログインします。

直接ログインを介してアプライアンス管理を開く

1. ブラウザのアドレス フィールドに、次のようにアプライアンスの IP アドレスを入力します。

   https://<IPAddress>

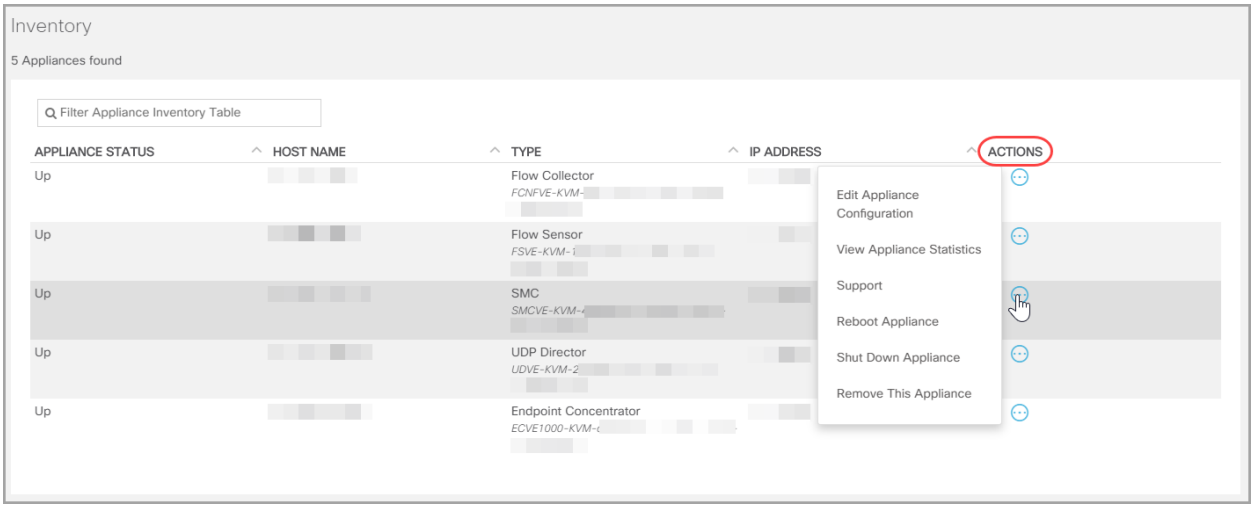
   - **SMC**:IP アドレスの後ろに **/smc/index.html** を追加します。
   - 例:https://1.1.1.1/smc/index.html

2. Enter を押します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンス設定の編集

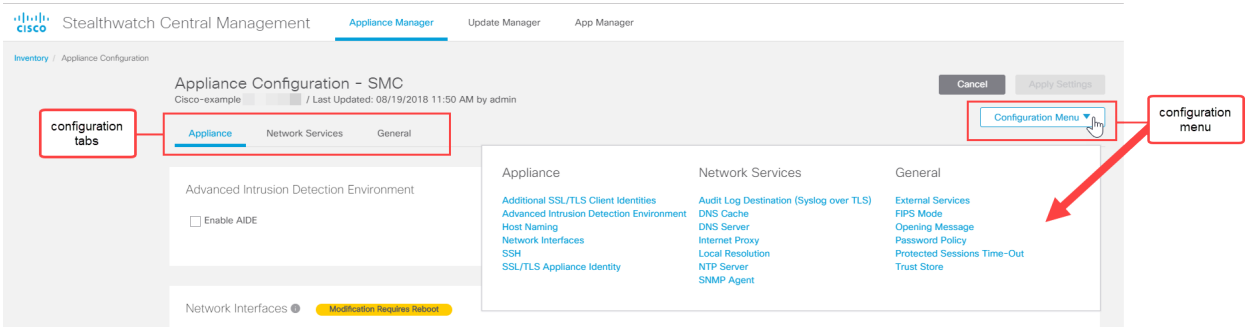
1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション (Actions)] メニューをクリックします。
2. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。



3. [設定 (Configuration)] メニューをクリックします。リストから項目を選択します。

   または

   各タブをクリックして、各設定カテゴリを確認します。



4. 必要に応じて、各設定セクションに変更を加えます。各設定タブでは、複数の設定カテゴリを編集することができます。

> 手順については、[ユーザ (User)] アイコンをクリックします。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. [設定の適用(Apply settings)]をクリックします。画面に表示される指示に従って、設定変更を保存します。

   一部の変更には、システムの再起動が必要です。待機する場合は、変更を元に戻して、後で設定を編集して再起動します。

> ⚠ アプライアンスが自動的に再起動します。設定の変更が保留中の間は、アプライアンスを再起動させないでください。アプライアンスのステータスが[アップ(Up)]であることを確認するには、[Central Management] > [Appliance Manager] インベントリを参照します。

6. **Up**:[Appliance Manager]ページで、アプライアンスが設定変更を完了し、アプライアンスのステータスが **Up** に戻ることを確認します。

アプライアンス統計情報の表示

ホバー:各アプライアンス ステータスの詳細を確認する場合は、ステータスの上にマウス ポインタを置きます。

システムの統計情報、サービス、ディスク使用率、および Docker サービスを確認するには、アプライアンス管理インターフェイスにログインします。

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [アプライアンス統計情報の表示(View Appliance Statistics)]を選択します。
3. アプライアンス管理インターフェイスにログインします。

Central Management からのアプライアンスの削除

次の手順に従って、Central Manager からアプライアンスを削除します。

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [このアプライアンスを削除(Remove This Appliance)]を選択します。

   構成チャネルのダウン:構成チャネルがダウンしているためアプライアンスを削除する場合、「トラブルシューティング」の「構成チャネルのダウン」に移動して追加の手順を参照してください。

   トラブルシューティング:アプライアンス管理インターフェイスにログインしても、アプライアンスが Central Management から削除されない場合は、「トラブルシューティング」の「構成チャネルのダウン」の手順に進み、システム設定を使用して削除します。

   Central Management:異なる Central Manager にアプライアンスを追加するには、アプライアンス設定ツールを使用します。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)を SMC 信頼ストアに保存してください。Stealthwatch のオンライン ヘルプの信頼ストアの手順を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Central Management へのアプライアンスの追加

Central Management にアプライアンスを追加するには、アプライアンス設定ツールを使用します。次を確認することが重要です。

- **カスタム証明書**:アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)をその独自の信頼ストアおよび SMC 信頼ストアに保存してください。Stealthwatch のオンライン ヘルプの信頼ストアの手順を参照してください。
- **SMC 管理のクレデンシャル**:Central Management にアプライアンスを追加するには、SMC、ユーザ ID、およびパスワードが必要です。
- **RFD**:アプライアンスで工場出荷時のデフォルトにリセットした場合、アプライアンス設定ツールの一部としてホスト名、ドメイン名、およびその他の構成情報を入力します。
- **新規インストール**:これが新規インストールであり、アプライアンスが設定されていない場合は、「**クイック リファレンス ワークフロー**」に移動します。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)を SMC 信頼ストアに保存してください。Stealthwatch のオンライン ヘルプの信頼ストアの手順を参照してください。

1. アプライアンス管理インターフェイスにログインします。
2. アプライアンスのブラウザ アドレス バーで、IP アドレスの後ろの URL の終わりを /lc-ast に置き換えます。

   https://<IPAddress>/lc-ast

3. Enter を押します。
4. [次へ(Next)] をクリックして [Central Management] タブにスクロールします。
5. **IP アドレス**:SMC/Central Manager の IP アドレスを入力します。
6. [保存(Save)] をクリックします。
7. 画面の指示に従って SMC 管理者の資格情報を入力し、設定を終了します。アプライアンスの種類によっては、追加情報を入力する必要があります。
8. アプリケーション設定ツールの詳細については、「**5. Stealthwatch システムの設定**」を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SSH の有効化/無効化

このセクションは、SSH(セキュア シェル)を使用してアプライアンスにアクセスできるかどうかを制御する場合に使用します。

デフォルト:無効

> ⚠ SSH を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

SSH を開く

次の手順に従って、選択したアプライアンスの SSH を開きます。

1. Central Management を開きます。
2. アプライアンスの [**アクション**(Actions)] メニューをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [**アプライアンス**(Appliance)] タブを選択します。

SSH の有効化

1. [SSH] セクションを見つけます。
2. アプライアンスへの SSH アクセスを許可するには、[SSH の有効化(Enable SSH)] チェックボックスをオンにします。
3. アプライアンスへのルート アクセスの有効化を許可するには、[ルート SSH アクセスの有効化(Enable Root SSH Access)]チェックボックスをオンにします。
4. [設定の適用(Apply settings)] をクリックします。
5. 画面に表示される指示に従って操作します。

SSH の無効化

1. アプライアンスへの SSH アクセスを削除するには、[SSH の有効化(Enable SSH)] チェックボックスをオフにします。
2. アプライアンスへのルート アクセスを削除するには、[ルート SSH アクセスの有効化(Enable Root SSH Access)] チェックボックスをオフにします。
3. [設定の適用(Apply settings)] をクリックします。
4. 画面に表示される指示に従って操作します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

パッチのインストールとソフトウェアのアップデート

お使いのソフトウェアバージョンに対する最新のパッチをインストールすることで、Stealthwatch を最新の状態に保つようにしてください。詳細および手順については、Cisco Software Central にアクセスして確認してください。

ソフトウェアアップデートは、Cisco Software Central の Cisco スマートアカウントにも送信されます。正常に更新するには、Stealthwatch 更新ガイド [英語] の手順に従ってください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

トラブルシューティング

構成チャネルのダウン

Appliance Manager で、アプライアンス ステータスとして [構成チャネルのダウン (Config Channel Down)] が表示されている場合は、次を確認します。

- **通信の設定**:ネットワーク通信の設定を確認します。
- **信頼ストア**:アプライアンス アイデンティティ証明書が正しい信頼ストアに保存されていることを確認します。Stealthwatch オンライン ヘルプの手順を参照してください。
- **証明書**:アプライアンス アイデンティティ証明書を変更した場合は、その手順を確認し、証明書が正しい信頼ストアに保存されていることを確認します。詳細については、「**アプライアンス アイデンティティの交換**」を参照してください。
- ライセンスの有効期限:詳細については、Stealthwatch スマート ソフトウェア ライセンシング ガイド [英語] を参照してください。
- **アプライアンスの削除**:構成チャネルのダウン中にアプライアンスを削除する場合は、システム設定からもアプライアンスを削除してください。
  - アプライアンスコンソールに sysadmin としてログインします。
  - **SystemConfig** と入力します。Enter を押します。
  - [リカバリ (Recovery)] > [アプライアンスの削除 (RemoveAppliance)] を選択します。

アプライアンス管理インターフェイスを開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

トラブルシューティングのために Central Manager から SMC を削除した場合は、アプライアンス管理にログインする必要があります。

1. ブラウザのアドレス フィールドに、次のようにアプライアンスの IP アドレスを入力します。

   https://<IPAddress>

   - **SMC**:IP アドレスの後ろに **/smc/index.html** を追加します。
   - **例**:https://1.1.1.1/smc/index.html

2. Enter を押します。

アプライアンス アイデンティティの交換

Stealthwatch バージョン 7.x アプライアンスはそれぞれ、固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。アプライアンス アイデンティティ証明書は、Stealthwatch オンライン ヘルプの「アプライアンス アイデンティティの更新」に記載された手順を使用して更新できます。

1. [**Central Management**] > [Appliance Manager] を開きます。
2. アプライアンスの [**アクション** (Actions)] メニューをクリックします。
3. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. [**アプライアンス**(Appliance)] タブを選択します。
5. [SSL/TLSアプライアンスアイデンティティ(SSL/TLS Appliance Identity)] セクションに移動します。
6. [アイデンティティの更新(Update Identity)] をクリックします。
7. 警告で、Stealthwatch オンライン ヘルプのリンクをクリックします。
8. 手順に従って証明書を変更し、信頼ストアを更新します。

> ⚠ 証明書はシステムのセキュリティにとって重要です。不適切に証明書を変更すると、Stealthwatch アプライアンスの通信が停止し、データ損失が発生します。

設定後のアプライアンスの変更

アプライアンス ホスト名、ネットワークドメイン名、または IP アドレスを変更するには、Stealthwatch オンライン ヘルプの手順に従います。

手順の一環として、アプライアンスを Central Management から一時的に削除します。アプライアンス アイデンティティ証明書が自動的に置き換えられます。また、場合によってはアプライアンスの信頼ストアを確認する必要があります。

> ⚠ アプライアンス アイデンティティ証明書は、この手順の一環として自動的に置き換えられます。
>
> **アプライアンスがカスタム証明書を使用している場合は、**これらの設定の変更について Cisco Stealthwatch サポートにお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

ホスト名の変更

ホスト名が一意であり、インターネットホストのインターネット標準規格の要件を満たしていることを確認します。

1. [**Central Management**] > [Appliance Manager] を開きます。
2. アプライアンスの [**アクション**(Actions)] メニューをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [**アプライアンス**(Appliance)] タブを選択します。
5. [ホスト名(Host Naming)] セクションで、[情報(Info)] アイコンをクリックします。
6. Stealthwatch オンライン ヘルプのリンクをクリックします。
7. 手順に従ってホスト名を変更します。

ネットワークドメイン名の変更

必ず完全修飾ドメイン名を使用してください。

1. [**Central Management**] > [Appliance Manager] を開きます。
2. アプライアンスの [**アクション**(Actions)] メニューをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [**アプライアンス**(Appliance)] タブを選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. [ホスト名(Host Naming)] セクションで、[情報(Info)] アイコンをクリックします。
6. Stealthwatch オンライン ヘルプのリンクをクリックします。
7. 手順に従ってネットワークドメイン名を変更します。

IP アドレスの変更

1. [Central Management] > [Appliance Manager] を開きます。
2. アプライアンスの [**アクション**(Actions)] メニューをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [**アプライアンス**(Appliance)] タブを選択します。
5. [ネットワークインターフェイス(Network Interfaces)]セクションで、[情報(Info)] アイコンをクリックします。
6. Stealthwatch オンライン ヘルプのリンクをクリックします。
7. 手順に従ってネットワークドメイン名を変更します。

アプライアンス設定ツールを開く

アプライアンスの設定後にアプライアンス設定ツールを開くには、次の手順を使用します。

> アプライアンス設定ツールを使用してホスト名、ネットワークドメイン名、または IP アドレスを変更する場合、アプライアンス アイデンティティ証明書が自動的に置き換えられます。
>
> **アプライアンスがカスタム証明書を使用している場合は、**これらの設定の変更について Cisco Stealthwatch サポートにお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

1. アプライアンスのブラウザ アドレス バーで、IP アドレスの後ろの URL の終わりを /lc-ast に置き換えます。

   https://<IPAddress>/lc-ast

2. Enter を押します。
3. 詳細については、「**5. Stealthwatch システムの設定**」を参照してください。

システム設定の概要

新しいメニュー構造でシステム設定が更新されました。多くの場合、システム設定にはトラブルシューティングを伴います。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

- [ユーザ(Users)]: 使用可能なメニューは、ログイン ID(root、sysadmin、または admin)によって決まります。
- SSH: メニューにアクセスするには、SSH を有効にする必要があります。

1. アプライアンスコンソールにログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから次のメニューを選択します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **ネットワーク**:アプライアンス管理ポートネットワーク、信頼できるホスト、およびネットワーク インターフェイスを変更するには、[ネットワーク(Network)]を選択します。
- セキュリティ:パスワードの変更またはリセット、Syslogコンプライアンスの管理を実行するには、[セキュリティ(Security)]を選択します。
- **リカバリ**:集中管理からのアプライアンスの削除、工場出荷時の初期状態へのリセットを実行するには、[リカバリ(Recovery)]を選択します。
- **詳細**:アプライアンスモデルの更新、ルートシェルのオープン、管理ユーザアカウントの管理、またはシングルサインオンの設定を実行するには、[詳細(Advanced)]を選択します。

信頼できるホストの変更

システム設定を使用すると、信頼できるホストのリストをアプライアンスのデフォルトから変更できます。ただし、信頼できるホストを変更する前に、Cisco Stealthwatch サポートにお問い合わせください。

> ⚠ 信頼できるホストを変更する前に、Cisco Stealthwatch サポートにお問い合わせください。

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

1. アプライアンスコンソールに sysadmin としてログインします。
2. [ネットワーク(Network)]>[信頼できるホスト(Trusted Hosts)]を選択します。
3. 画面に表示される指示に従って、[信頼できるホスト(Trusted Hosts)]を変更します。

工場出荷時のデフォルトへのリセット

アプライアンスを工場出荷時のデフォルト(RFD)にリセットするには、次の手順を使用します。データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。

- RFD を 2 回:データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。
- 設定のバックアップ:アプライアンスの設定を復元する場合は、バックアップ設定とデータベースのバックアップファイルを保存してください。詳細については、Stealthwatch オンラインヘルプの「Backup Configuration Files (in Central Management)」および「Backup/Restore Database (Appliance Admin interface)」の各トピックを参照してください。RFD 後にバックアップを復元するには、Cisco Stealthwatch サポートにお問い合わせください。

> ⚠ アプライアンスを工場出荷時のデフォルト設定にリセット(RFD)すると、すべての既存データと設定情報が削除され、バックアップを作成した場合にのみ復元できます。

> ⚠ アプライアンスを工場出荷時のデフォルトにリセットすると、Central Management を使用して設定を復元できません。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ(Recovery)] > [工場出荷時のデフォルト(Factory Defaults)] を選択します。
3. 画面に表示される指示に従って工場出荷時のデフォルトにリセットし、アプライアンスを再起動します。

> ⚠ データを完全に消去するには、各アプライアンスで RFD を2 回 実行してください。

管理者ユーザの有効化/無効化

デフォルトの管理者アカウントを有効または無効にするには、次の手順を使用します。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [詳細設定(Advanced)] を選択します。
3. [Adminユーザ(Admin User)] を選択します。
4. 画面に表示される指示に従い、管理者ユーザ アカウントを有効または無効にします。
5. 上記の手順を繰り返して、Stealthwatch クラスタ内のすべてのアプライアンスで管理ユーザ アカウントを有効または無効にします。

パスワードのリセットの有効化または無効化

パスワードのリセット機能を有効化または無効化するには、次の手順を使用します。[有効化(Enable)] を選択すると、GRUB コマンドライン インターフェイスを使用してパスワードをデフォルト設定にリセットできます。

> ⚠ パスワードのリセットを無効化し、パスワードを失った場合は、アプライアンスに保存されているデータへのアクセスが失われます。再度アプライアンスにアクセスするには、工場出荷時のデフォルトにリセットして再設定してください。

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ(Security)] を選択します。
4. [パスワードのリセット(Password Reset)] を選択します。
5. 画面に表示される指示に従い、パスワードのリセットを有効または無効にします。

パスワードをデフォルト設定にリセット

パスワードをデフォルト設定にリセットする方法はいくつかあります。

- admin パスワード:「**SMC の admin パスワードのリセット**」を使用します。
- admin、root、sysadmin パスワード:「**admin、root、sysadmin パスワードをデフォルトにリセット**」を使用します。

> ⚠ アプライアンスのパスワードをデフォルトにリセットしたら、必ずパスワードを変更してください。この手順は、セキュリティにとって重要です。手順については、「**パスワードの変更**」を参照してください。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SMC の admin パスワードのリセット

次の手順を使用して、admin パスワードを SMC のデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

- **要件**：次の手順を完了するには、アプライアンスのルート パスワードが必要です。
- **その他のユーザ**：次の手順により、admin ユーザがデフォルト パスワードにリセットされます。個人ユーザのパスワードは変更されません。
- その他のアプライアンス：これらの手順では、他のアプライアンス（Flow Collector、Flow Sensor、UDP Director、またはエンドポイント コンセントレータ）の admin パスワードはリセットされません。Stealthwatch

1. アプライアンスコンソールに root としてログインします。
2. `rm /lancope/var/smc/config/users/admin/user.xml` と入力します。Enter を押します。
3. `docker restart smc` と入力します。Enter を押します。
4. `docker restart nginx` と入力します。Enter を押します。

   これにより、admin パスワードがデフォルト値にリセットされます。

5. アプライアンスコンソールを終了します。
6. admin パスワードをデフォルトから変更するには、「**パスワードの変更**」に進みます。この手順は、セキュリティにとって重要です。

admin、root、sysadmin パスワードをデフォルトにリセット

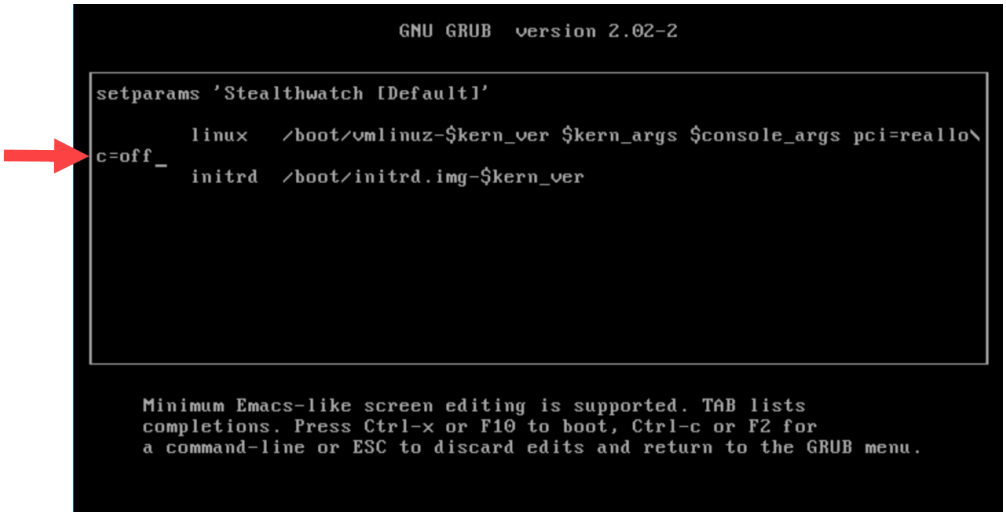
コンソールアクセスを使用して、アプライアンスの admin、root、および sysadmin パスワードをデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

1. アプライアンスコンソール（CIMC またはハイパーバイザ）にログインします。
2. アプライアンスを再起動します。
3. コンソール画面に GRUB メニューが表示されたら、「e」と入力して編集モードに切り替えます。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. 2 番目の行にカーソルを移動します。

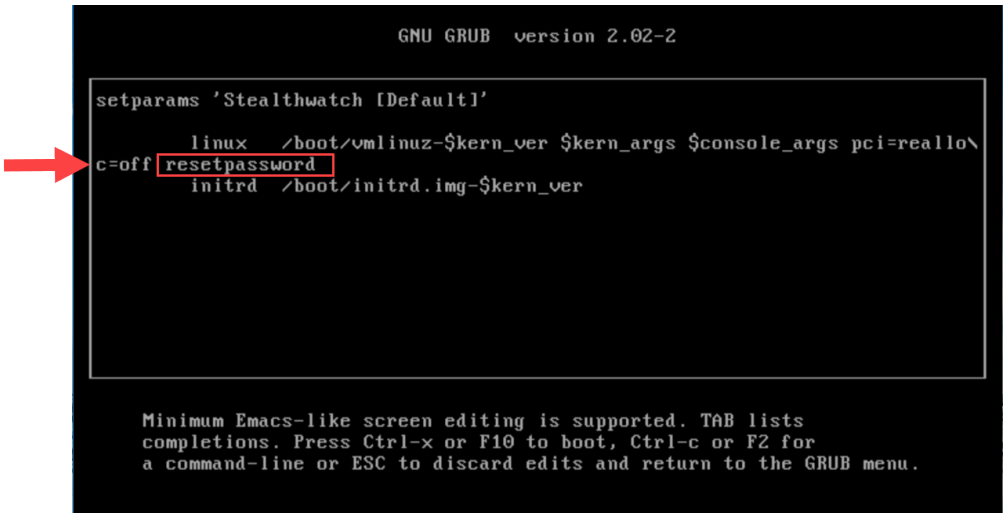
   コマンド ラインは、アプライアンスのバージョンによってわずかに異なる場合があります。



5. `c=off` の後に `resetpassword` と入力して、コマンド ラインを次の例のようにします。

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
c=off resetpassword
```

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



6. Ctrl+X を押して起動を再開します。

   admin、root、および sysadmin パスワードがデフォルト値にリセットされます。

7. パスワードをデフォルトから変更するには、「**パスワードの変更**」に進みます。この手順は、セキュリティにとって重要です。

パスワードの変更

デフォルトのパスワードまたは以前のパスワードからパスワードを変更するには、次の手順を使用します。次の基準を使用していることを確認します。

- 長さ:8 ～ 256 文字
- 変更:新しいパスワードが以前のパスワードと最低 4 文字異なっていることを確認します。

ユーザ	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

sysadmin パスワードの変更

1. アプライアンスコンソールに sysadmin としてログインします。
2. [セキュリティ(Security)]を選択します。
3. [パスワード(Password)]を選択します。
4. 画面に表示される指示に従って、sysadmin パスワードを変更します。
5. システム設定を終了します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ルート パスワードの変更

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ(Security)] を選択します。
4. [パスワード(Password)] を選択します。
5. 画面に表示される指示に従って、ルート パスワードを変更します。
6. システム設定を終了します。

SMC の admin パスワードの変更

1. SMC に admin としてログインします。

   - URL : https://<IPAddress>
   - ログイン : admin
   - デフォルトパスワード : lan411cope

2. [グローバル設定(Global Settings)] アイコンをクリックします。[ユーザ管理(User Management)] を選択します。
3. リスト内で admin ユーザを見つけます。
4. [アクション(Actions)] メニューをクリックします。[パスワードの変更] を選択します。
5. 画面に表示される指示に従って、admin パスワードを変更します。次の基準を使用します。

   - 長さ : 8 ～ 256 文字
   - **変更** : 新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

他のすべてのアプライアンスの admin パスワードの変更

Flow Collector、Flow Sensor、UDP Director、またはエンドポイント コンセントレータの admin ユーザパスワードを変更するには、次の手順を使用します。

1. admin としてアプライアンス管理インターフェイスにログインします。

   - URL : https://<IPAddress>
   - ログイン : admin
   - デフォルトパスワード : lan411cope

2. [ユーザの管理(Manage Users)] > [パスワードの変更(Change Password)] を選択します。
3. 現在のパスワードと新しいパスワードを入力します。
4. [適用(Apply)] をクリックします。画面に表示される指示に従って、パスワードを変更します。
5. 別のアプライアンスの admin パスワードを変更するには、ステップ 1 ～ 4 を繰り返します。

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先：
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、
URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコ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。（1721R）

© 2020 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.