Stealthwatch セキュリティ分析の設定

Stealthwatch セキュリティ分析のインストール

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Software Updates]**。

ステップ 2 左側のペインで [Updates] が選択されていることを確認します。

ステップ 3 [Stealthwatch Security Analytics] の横にある [Install] をクリックします。

インストールが完了すると、[Installed Applications] ウィンドウに Stealthwatch セキュリティ分析サービスが表示されます。

Stealthwatch の登録

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Settings]**の順に選択します。

ステップ 2 左側のペインで、[Search Settings] バーに Stealthwatch と入力します。

ステップ 3 左側のペインで [Stealthwatch] をクリックします。

ステップ 4 Stealthwatch Management Console の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 5 Stealthwatch Management Console へのアクセスに使用するユーザーアカウントのユーザー名とパスワードを入力します。

（注） Stealthwatch Management Console に新しいユーザーを追加したら、そのユーザーが Cisco Stealthwatch と統合する前に Stealthwatch Management Console に少なくとも 1 回ログインしていることを確認します。最初のログイン時に、ユーザーは新しいパスワードを設定し、API アクセスをアクティブにするように求められます。

Stealthwatch ユーザーアカウントに最低限必要な権限は次のとおりです。

- データロール：読み取り専用
- 機能ロール：設定マネージャとネットワークエンジニア

（注） Cisco DNA Center でカスタムユーザーロールを作成して、別のユーザーがデバイスで Stealthwatch セキュリティ分析をプロビジョニングできるように設定することができます。カスタムユーザーロールの作成方法の詳細については、『*Cisco DNA Center Administrator Guide*』を参照してください。

次の表に、ユーザーがデバイスで Stealthwatch セキュリティ分析をプロビジョニングするために最低限必要な権限を示します。

アクセス	説明	Permission
[Network Design] > [Advanced Network Settings]	AAA、PKI 証明書、Stealthwatch についての詳細なネットワーク設定。	書き込み
[Network Design] > [Network Settings]	AAA、NTP、DNS サーバー、IP プールなど、サイト全体で使用する共通のネットワーク設定。ワイヤレスプロファイルを作成するには、[Network Profiles] に対する書き込み権限が必要です。	書き込み
[Network Provision] > [Provision]	サイトの設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。	書き込み
[Network Services] > [Stealthwatch]	サイトの設定とネットワークに対して設定されたポリシーを使用してデバイスを設定します。	読み取り
[System] > [Basic]	個々のユーザー設定にアクセスします。このアクセスはすべてのユーザーに付与されます。	書き込み

ステップ 6 [Save] をクリックします。

Stealthwatch が正常に登録されると、[IP Address] フィールドのすぐ上にステータスが [Active | Registered and Running] と表示されます。

User Datagram Protocol（UDP）Director の設定

User Datagram Protocol（UDP）Director は、NetFlow やその他のトラフィックを受信して複数の宛先に複製します。

始める前に

UDP Director をインストールし、Stealthwatch Management Console で設定します。詳細については、『*UDP Director Virtual Edition Installation and Configuration Guide (for Stealthwatch System v6.9.0)*』を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Network settings]**。

ステップ 2 （任意）左側のペインを使用して、Stealthwatch フローの宛先を設定するサイトまでドリルダウンします。

ステップ 3 下にスクロールして、[Stealthwatch Flow Destination] 領域を展開します。

ステップ 4 Stealthwatch で設定されているフローの宛先を追加するには、対応するオプションボタンをクリックします。または、対応するオプションボタンをクリックして、Stealthwatch Management Console で管理されていない宛先を追加することもできます。

ステップ 5 Stealthwatch で設定されているフローの宛先を選択する場合は、目的のフローの宛先を選択します。「No Stealthwatch flow destination server configured」というエラーが表示される場合は、Stealthwatch の登録 （1 ページ）を参照してください。

外部のフローの宛先を追加する場合は、目的のフローの宛先の IP アドレスおよびポートを指定します。

ステップ 6 [Save] をクリックします。

Stealthwatch セキュリティ分析の有効化

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Stealthwatch Security Analytics]** の順に選択します。

ステップ 2 左側のペインでドロップダウンリストを使用し、Stealthwatch セキュリティ分析をサイトまたはファブリックに対して有効にするかどうかに応じて、[All Sites] または [All Fabrics] を選択します。デフォルトでは、[All Sites] が選択されています。

ステップ 3 左側のペインで、Stealthwatch セキュリティ分析を有効にするサイトまたはファブリックまでドリルダウンします。または、検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 4 サイトカードをクリックして、Stealthwatch セキュリティ分析を有効にするサイトまたはファブリックを選択します。必要に応じて、サイトおよびファブリックの階層を特定のフロアまで移動できます。

サイトカードには、[Enabled]、[Ready]、および [Not Ready] のデバイスの数が表示されます。

（注） Stealthwatch セキュリティ分析を有効にするには、少なくとも 1 つのデバイスを待受中の状態にする必要があります。

ステップ 5 事前チェックを確認し、[Get Started] をクリックします。

ステップ 6 選択したサイトまたはファブリックに対して設定されているフローの宛先を確認します。フローの宛先を変更する場合は、[Change Settings] をクリックします。新しいフローの宛先を設定し、ワークフローを再開します。

「Select a flow destination for the site to proceed」というエラーが表示された場合は、[Update Settings] をクリックしてフローの宛先を設定します。ワークフローを再開します。

ステップ 7 [Next] をクリックします。

ステップ 8 デバイステーブルで [Ready] タブが選択されていることを確認します。

ステップ 9 有効にするデバイスのリストを確認します。

ここから、トグルスイッチを使用して、すべてのデバイスまたは特定のデバイスを有効化の対象から除外します。

ステップ 10 [ETA Telemetry] 列のトグルスイッチを使用して、暗号化トラフィック分析 テレメトリデータの収集を有効または無効にします。デフォルトでは、このオプションは暗号化トラフィック分析 対応デバイスに対して有効になっています。暗号化トラフィック分析 と互換性のあるデバイスのリストについては、Stealthwatch セキュリティ分析の有効化 （3 ページ）を参照してください。

ステップ 11 対応するオプションボタンを選択して、アプリケーションをすぐに（[Now]）、または後で（[Later]）展開します。

（注） 後で展開するようにスケジュールする場合は、画面の右上にある通知リストから [Edit] をクリックしてスケジュール時刻を編集できます。

展開時刻が近づくと一連の事前チェックが実行され、その時点のデバイスのCPUなどがチェックされます。失敗した事前チェックは、タスクマネージャに表示されます。

ステップ 12 [Enable] をクリックします。

ステップ 13 展開ステータスを表示するには、[View Deployment Status] をクリックします。または、Cisco DNA Center のメインメニューから **[Activity]** > **[Tasks]** の順に選択して、展開ステータスを表示します。

タスクが完了すると、展開ステータスが [In Progress] から [Success] に変わります。ステータスの表示を更新するには、通知リストの右上にある [Refresh] ボタンをクリックします。

（注） プロビジョニングアクションをすぐに実行する場合も後で実行する場合も、実行前に一連の事前チェックが追加で実行されます。次の場合はタスクが失敗します。

- その時点でデバイスの CPU が 70% を超えている。
- アクセススイッチで NBAR が有効になっている。
- スイッチに Stealthwatch セキュリティ分析の適用可能なインターフェイスがない。
- ルータのルート情報がない。

Stealthwatch セキュリティ分析の事前チェック

Stealthwatch セキュリティ分析サービスでは、サイトとファブリックのデバイスについて、それらが展開の条件を満たしていることを確認するために自動の事前チェックを実施します。

次のチェックが実施されます。

- [Required Software]：デバイスで実行されているソフトウェアが最小要件を満たしている必要があります。
- [Required Device Role]：デバイスロールでサービスの展開がサポートされている必要があります。ASR および ISR シリーズのルータを使用している場合は、[Device Role] が [Border Router] に設定されていることを確認します。9300 および 9400 シリーズのスイッチを使用している場合は、[Device Role] が [Access] に設定されていることを確認します。
- [Required Hardware]：デバイスハードウェアでサービスの展開がサポートされている必要があります。
- [Required Licenses]：サイトのデバイスのアクティブなライセンスが最小要件を満たしている必要があります。
- [No Conflicts with Other Services]：他のサービスとの間に互換性の問題がないようにする必要があります。このチェックは次の場合に失敗します。
  - デバイスが vManage で管理されている。
  - デバイスで NBAR が有効になっている。

（注） NBAR 競合は、Flexible NetFlow が有効になっているデバイスと、17.3.1 より前のバージョンを実行している Catalyst 9300 および Catalyst 9400 スイッチに適用されます。

  - デバイスの 1 つ以上のインターフェイスで既存の NetFlow モニターが有効になっている。

これらのすべての条件を満たすデバイスが [Ready] と見なされ、その総数が表示されます。

（注） ハードウェア、ソフトウェア、およびライセンスの要件については、Stealthwatch セキュリティ分析の事前チェック （5 ページ）を参照してください。

準備ができていないデバイスの確認

1 つ以上のソフトウェア、互換性、およびライセンスのチェックに失敗したデバイスは、Stealthwatch セキュリティ分析を有効にする準備ができていないと見なされます。[Not Ready] のデバイスのリストを表示するには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Stealthwatch Security Analytics]** の順に選択します。

ステップ 2 左側のペインで、Stealthwatch セキュリティ分析を有効にする準備ができていないデバイスを表示するサイトまたはファブリックまでドリルダウンします。または、検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 3 該当するサイトカードをクリックして、準備ができていないデバイスを表示するサイトまたはファブリックを選択します。

ステップ 4 [Get Started] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 デバイステーブルで、[Not Ready] をクリックします。

Stealthwatch セキュリティ分析を有効にする準備ができていないデバイスのリストが表示され、それぞれのデバイスに対する各チェックのステータスが示されます。

ステップ 7 赤色のアイコンにカーソルを合わせて、失敗したチェックに関する詳細情報を確認します。

Stealthwatch Cloud への Flexible NetFlow エクスポートの有効化

Stealthwatch Cloud への Flexible NetFlow エクスポートを有効にするように Stealthwatch セキュリティ分析を設定できます。

Stealthwatch Cloud は、Cisco IOS XE リリース 17.3.1 以降を実行している Cisco Catalyst 9300 および 9200 デバイスをサポートします。

始める前に

- Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認します。

- Stealthwatch セキュリティ分析のユーザーロールに設定マネージャとネットワークエンジニアの権限があることを確認します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出し、サイトに追加します。

ステップ 1 Stealthwatch Cloud ポータルで、**[Settings]** > **[Sensors]** > **[Service key]** の順に選択します。

ステップ 2 [Service key] フィールドで、サービスキーをコピーし、後で使用するために保存します。

Stealthwatch Cloud では、次の地域に Flexible NetFlow データを送信できます。

- US
- EU
- APJC

サービスキーは地域によって異なります。サイトに応じて、最大 3 つの異なるサービスキーを使用できます。

ステップ 3 Stealthwatch フローの宛先を Stealthwatch Cloud に設定します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。
b) 左側のペインを使用して、Stealthwatch フローの宛先を設定するサイトまでドリルダウンします。
c) 下にスクロールして、[Stealthwatch Flow Destination] 領域を展開します。
d) [Stealthwatch Cloud] オプションボタンをクリックします。
e) [Service key] フィールドに、前にコピーしたサービスキーを貼り付けます。
f) [Save] をクリックします。

ステップ 4 **[Provision]** > **[Services]** > **[Stealthwatch Security Analytics]** の順に選択します。

ステップ 5 左側のペインで、目的のサイトにドリルダウンします。

ステップ 6 サイトカードをクリックし、[Get Started] をクリックします。

ステップ 7 フローの宛先が [Stealthwatch Cloud] に設定されていることを確認し、[Next] をクリックします。

ステップ 8 [Ready] タブで、Stealthwatch Cloud に展開するデバイスを選択し、[Enable] をクリックします。

ステップ 9 展開のステータスをモニターするには、[View Deployment Status] をクリックします。

ステップ 10 [閉じる（Close）] をクリックします。

ステップ 11 [Enabled] タブには、SWC ステータスが [Enabled] になっている新しいデバイスが表示されます。対応するオプションボタンを選択して、更新をすぐに（[Now]）、または後で（[Later]）適用します。[Apply] をクリックします。

ステップ 12 Stealthwatch Cloud ポータルに戻り、**[Settings]** > **[Sensors]** の順に選択します。新しいセンサーを探します（センサー名はデバイスのホスト名です）。Stealthwatch Cloud ポータルへのデータのアップロードが開始されると、センサーが緑色に変わります。データが送信されない場合、センサーは赤色になります。Stealthwatch Cloud ポータルで、センサーが緑色に変わると、トラフィックの詳細がダッシュボードに表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。