



インストールおよびセットアップ

- 「はじめに」 (P.1-1)
- 「作業の概要」 (P.1-2)
- 「Splunk ソフトウェア」 (P.1-2)
- 「システム要件」 (P.1-3)
- 「サイズ変更およびスケーリングの推奨事項」 (P.1-3)
- 「Splunk のインストールと設定」 (P.1-4)
- 「Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションのインストール/更新」 (P.1-6)
- 「ログ ファイルのフォルダ構造を作成」 (P.1-7)
- 「履歴データのインポートおよびインデックス作成」 (P.1-7)
- 「継続的なデータ転送の設定」 (P.1-9)
- 「(任意) 部門のメンバーシップ クエリーをセットアップ」 (P.1-11)
- 「(任意) スケジュール済 PDF レポートのセットアップ」 (P.1-13)
- 「追加資料」 (P.1-14)

はじめに

Cisco Web セキュリティ アプライアンス用 Splunk には、カスタマイズされた Splunk アプリケーション、および Cisco Web セキュリティ アプライアンスから収集されたログ データをポーリングする Splunk サーバが含まれます。このアプリケーションは、Cisco Web セキュリティ アプライアンスからの大容量データに対する解析機能を提供するために設計されたレポートとダッシュボードを提供します。

アプリケーションは、Cisco Web セキュリティ アプライアンスからデータを受信し、デフォルト/メイン インデックスに保存します。また、要約を生成し、サマリー インデックスに保存します。ユーザは、事前定義済みレポートを使用して、これらのデータを閲覧することができます。また、flashtimeline ビューおよび Web トラッキング フォームを使用して、アドホック検索を実行できます。



より短いタイムレンジを選択し、できるだけ正確に検索を調整することによってパフォーマンスを向上できます。

作業の概要

-
- ステップ 1 「[Splunk のインストールと設定](#)」 (P.1-4)
 - ステップ 2 「[Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションのインストール/更新](#)」 (P.1-6)
 - ステップ 3 「[ログ ファイルのフォルダ構造を作成](#)」 (P.1-7)
 - ステップ 4 「[履歴データのインポートおよびインデックス作成](#)」 (P.1-7)
 - ステップ 5 「[継続的なデータ転送の設定](#)」 (P.1-9) (Cisco Web セキュリティ アプライアンスのセットアップなど)
-

Splunk ソフトウェア

ダウンロード

Splunk ソフトウェアは、www.splunk.com から無料でダウンロードできます。

Splunk ソフトウェアのインストールおよび使用に関する包括的なドキュメントは、Splunk の Web サイト docs.splunk.com から入手できます。

関連トピック

- 「[Splunk のインストールと設定](#)」 (P.1-4)

サポートされる機能およびサポートされない機能

| コンポーネント | サポートあり | サポートなし |
|-----------------|---|------------------------------------|
| レポート | Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションに含まれるレポート。 | カスタム レポート。 |
| 検索 | Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションに含まれるフォーム ベースの検索 / Web トラッキング ツール。 | ネイティブ Splunk 検索エンジン。 |
| サーバ | 単一サーバ展開 | 複数サーバ展開 |
| トランスポート方式 | FTP (ファイルおよびディレクトリ) | TCP |
| 仮想化 | n/a | Splunk のコア機能の仮想化は、このマニュアル内で参照されます。 |
| PDF サーバアプリケーション | Linux の場合 | Windows の場合 |

マニュアル

このマニュアルでは、Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションの使用について説明します。Splunk 製品自体のマニュアルは、Splunk Web サイトで入手できます (<http://docs.splunk.com>)。

システム要件

Splunk インスタンス

Splunk の最新のシステム要件については、Splunk の Web サイトを参照してください。
<http://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements>

Cisco Web セキュリティ アプライアンス用 Splunk アプリケーション

オペレーティング システムの要件は以下のとおりです。

- Red Hat Linux
- Windows

プラットフォーム要件：参照ハードウェアは、製品グレードであり、かつ、Cisco のサポート対象となるためには次の最低限の仕様を満たす必要があります。

- Intel x86/64 ビット チップ アーキテクチャ (2 CPU、4 コア、2.5 ~ 3 Ghz)
- 16GB RAM
- 300GB SAS ハードディスク X 4、10,000 rpm、RAID10 (800 IOPS 以上)
- 標準 1Gb イーサネット NIC、管理ネットワーク用セカンド NIC (オプション)



(注) Splunk はディスクの I/O に抑制されることが多いため、ストレージ ハードウェアを選択するときは必ずそれを第一に考慮します。

ファイル システムは、NTFS または EXT2/3 でフォーマットされたローカル ディスク ボリュームでの実行を前提としています。独立した OS ボリュームを、業界のベスト プラクティスにあわせて作成する必要があります。Splunk は、可能な限り論理ボリューム上にインストールする必要があります。

サイズ変更およびスケーリングの推奨事項

- 基本構成は、単一階層アーキテクチャで、1 台のサーバで以下の Splunk の通常のコア機能の 3 つの部分すべてを提供する構成です。
 - 検索ヘッド
 - インデクサ
 - データ ソースのモニタ
- インデックス付きデータ量の推定要件が 100k/ユーザ (推定値: 100GB/日) を超える場合、Splunk のインフラストラクチャには調整が必要です。

- 別の Splunk インスタンスを追加して設定を調整することにより、新しいインフラストラクチャでは、(データのロード バランシング後) インデックス作成および検索パフォーマンスが向上し、ストレージおよび保存容量の向上が提供されます。
- 専用のフォワーダ サーバが Splunk のインフラストラクチャに追加され、WSA のログ ファイルをモニタし、ロード バランシングを使用して複数のインデクサにログ データを転送するように設定されています。
- 10 万ユーザを超える環境の実装および構成を支援するため、シスコは、Cisco Web セキュリティ アプライアンスのお客様のために Splunk プロフェッショナル サービスを実行します。

1 万ユーザの Cisco Web セキュリティ アプライアンス デバイスに対するログ ボリュームの試算によると、収集データ量は非圧縮で 10 GB/日です。インデックスの作成後、データは推定 2.5 GB/日に圧縮されます (インデックス作成済みストレージ使用量)。Splunk インスタンスは、500 GB のボリュームサイズに基づいて、約 200 日間分のインデックス データを保持します。

| Cisco Web セキュリティ アプライアンスユーザ | 推定ログ ボリューム (2,500 トランザクション/ユーザ/日) | 推定インデックス作成済みボリューム | 推定保持 (500GB ボリューム) |
|-----------------------------|-----------------------------------|-------------------|--------------------|
| 10K | 10GB/日 | 2.5GB | 200 日間 |
| 50K | 50GB/日 | 13GB | 40 日間 |
| 100K | 100GB/日 | 25GB | 20 日間 |



(注)

アレイ内の推定ログ ボリュームおよび中規模容量のドライブに基づくガイドライン。

| 日々のボリューム | 77GB/日 | 140GB/日 | 180GB/日 |
|------------------|------------|------------|------------|
| 総トランザクション | 1 億 7200 万 | 3 億 2500 万 | 4 億 1700 万 |
| 事前定義済みレポートのロード時間 | <5 秒 | <10 秒 | <15 秒 |

| | |
|--------------------|--------|
| 総ボリューム | 2.3 TB |
| 保存期間 (営業日) @70GB/日 | 33 |
| 事前定義済みレポートのロード時間 | <20 秒 |

Splunk のインストールと設定

これらのタスクはこのマニュアルの範囲外ですが、Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションを使用するには実行する必要があります。これらのタスクを実行するには、Splunk の Web サイト上のマニュアルを参照してください。

| タスク | 追加情報 |
|--|--|
| 無料の Splunk ソフトウェアをダウンロードしてインストールします。 | www.splunk.com |
| 管理者アカウントを使用して Splunk にログインし、パスワードを変更します。 | docs.splunk.com |

| タスク | 追加情報 |
|---|--|
| ライセンス : <ol style="list-style-type: none"> 履歴データの初回アップロード時および通常運用時、双方においてインデックスが作成されるデータ量を考慮します。 履歴データのアップロードに十分な Splunk 評価ライセンスを取得およびアップロードします。 インデックスが作成される該当ソース タイプの予想データに対して十分な Splunk エンタープライズライセンスを取得およびアップロードします。 ライセンスのタイプを、トライアルから評価、またはエンタープライズに変更します。 ライセンス プールを編集して、インデックスが正しいプールにレポートされるようにします。 履歴データ入力を処理するために、まず大量のデータに対応した適切な評価ライセンスが必要になる場合があります。次に、 | docs.splunk.com 関連項目 : 「追加資料」 (P.1-14) |
| すべてのユーザ/役割のデフォルトとして、Cisco WSA Splunk アプリケーションを設定します。 | docs.splunk.com |
| (任意) Splunk 内の SSL を有効にします。 | docs.splunk.com |
| (任意) AD/LDAP との関連付けを行うには以下の手順を実行します。 <ol style="list-style-type: none"> 認証に AD/LDAP を使用するよう Splunk を設定します。 Splunk が AD/LDAP サーバに接続できることを確認します。 Splunk の役割に既存の AD/LDAP グループをマッピング 必要に応じて Splunk 内の役割を追加、編集します。 (任意) AD/LDAP サーバで SSL を有効化します。 | 「認証/許可に関する注意事項」 (P.1-5) docs.splunk.com |
| (ベスト プラクティス) Splunk サービスが自動的に再起動し、試行するように設定されていることを確認します。 | docs.splunk.com |

認証/許可に関する注意事項

- Splunk の基本的な認証
- AD/LDAP

Splunk の基本的な認証

Splunk のローカル認証が、設定されている他の認証オプションよりも優先します。

デフォルト設定 :

- 3 つの役割 : ユーザの権限を定義します。

- 1 件のユーザ アカウント : admin は変更不可です。設定、テスト、トラブルシューティングを行うためにこのアカウントを使用します。



ヒント

- ディレクトリ サービスの Splunk 固有グループにユーザを追加します。
- Splunk にそのグループ DN をインポートします。
- 最適なデフォルトの Splunk の役割をそのグループ DN にマッピングするか、またはより適切な役割を作成してマッピングします。

要件がシンプルな場合、たとえば、少数のユーザのみが Splunk データを閲覧できる場合は、ローカル認証を使用するだけでも構いません。

Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションのインストール/更新

Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションのインストール/更新

はじめる前に

- 「[Splunk のインストールと設定](#)」(P.1-4)
- Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションのバージョンをアップグレードする場合、旧バージョンのアプリケーションをアンインストールします。
- Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションの zip または tar ファイルを受け取ります。
- Splunk Web を開きます。

-
- ステップ 1** Splunk Web 内では、[管理者 (Manager)] > [アプリケーション (Apps)] > [ファイルからアプリケーションをインストール (Install Apps from File)] の順に進みます。
- ステップ 2** ブラウズし、Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションの zip または tar ファイルを選択します。
- ステップ 3** アプリケーションが正常にインポートされたとの通知を確認します。
- ステップ 4** Splunk を再起動します : [管理者 (Manager)] > [サーバコントロール (Server Controls)] > [再起動 (Restart)]。
- ステップ 5** Splunk Web にログインします。
- ステップ 6** [管理者 (Manager)] > [アプリケーション (Apps)] の順に進み、Cisco WSA Splunk アプリケーションが表示および有効化されていることを確認します。
-

次の作業

- 「[履歴データのインポートおよびインデックス作成](#)」(P.1-7)

コンフィギュレーションベスト プラクティス

- Cisco Web セキュリティ アプライアンス アプライアンス上で統一したタイムゾーンを設定します。
検索結果に表示される時間は、Splunk インスタンスの「ローカルの」時間を表しています。初期設定では、Cisco Web セキュリティ アプライアンス ログへの Splunk 入力は、すべて TZ = GMT に設定されます。
- ローカル管理者アカウントのパスワードを記録します（選択した認証方法に関係なく）。

ログ ファイルのフォルダ構造を作成

| ログ | デフォルトパス | 変数 |
|------------|---|---|
| トラフィック モニタ | /\$Input_base/wsa_hostname/trafmonlogs/ | \$Input_base = Splunk 展開先 host_name = WSA デバイス |
| アクセス | /\$Input_base/wsa_hostname/accesslogs/ | \$Input_base = 展開先 host_name = WSA デバイス |

履歴データのインポートおよびインデックス作成

サマリー スクリプトのデフォルトは、90 日分の履歴を集約します。デフォルトでは、サマリー スクリプトは 8 つのコアを使用します。

(任意) サマリー スクリプトのカスタマイズ

ステップ 1 編集用にサマリー スクリプトを開きます。

- Linux : \$SPLUNK_HOME/etc/apps/CiscoWSA/bin /summary.sh
- Windows : X:\\$SPLUNK_HOME\etc\apps\CiscoWSA\bin\summary.vbs

ステップ 2 次の文字列を検索します。

```
time $Spath/bin/splunk cmd python $Spath/bin/fill_summary_index.py -app
SplunkforCiscoIronportWSA -namefile
$Spath/etc/apps/SplunkforCiscoIronportWSA/bin/summary.jobs -et -90d -lt now -j 8 -dedup true
```

ステップ 3 開始日、終了日およびサマリー スクリプトで使用されるコア数をカスタマイズします。

| 設定 | デフォルト | 説明 |
|-----|-------|--|
| -et | -90d | 開始日。要約を開始する履歴日の数。デフォルト値の -90d は、現在の日から 90 日さかのぼります。 |
| -lt | now | 終了日。要約を終了する履歴日の数。デフォルト値の now は、現在の日付で終了します。デフォルト値の -1d は、昨日のデータで終了します。 |
| -j | 8 | サマリー スクリプトで使用されるコアの数。 |

(任意) インポート時間の推測

履歴サマリーは、完了までに 9 時間かかります。

-
- ステップ 1** プラットフォーム ハードウェアの推奨要件に基づく、各サマリージョブの 5M イベント（未加工データ 2GB）に対して 4 分かかります。
- 例：25M の履歴イベントを表す 10GB ファイルについては、各サマリー ジョブに対する実行が 20 分かかると想定されます。
- ステップ 2** Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションで使用される 27 個のサマリージョブを可能にします。
-

履歴データのインポートおよびインデックス作成

はじめる前に

- 「Splunk のインストールと設定」(P.1-4) に記載された設定のタスクを完了します。
- フィールドの抽出が正しいことを確認します。第 3 章「フィールドの抽出」を参照してください。
- フォルダ構造を理解します。「ログ ファイルのフォルダ構造を作成」(P.1-7) を参照してください。
- (任意) 「(任意) インポート時間の推測」(P.1-8) を参照してください。

-
- ステップ 1** ログ ファイルのフォルダ構造に、履歴ログ ファイルをコピーします。



(注) デフォルトでは、これらのログは、データがインデックス化されたのち、削除されます。

- ステップ 2** コマンド プロンプトから、サマリー スクリプトを実行します：

Linux : `$SPLUNK_HOME/etc/apps/CiscoWSA/bin /summary.sh`

Windows : `X:\$SPLUNK_HOME\etc\apps\CiscoWSA\bin\summary.vbs`

- ステップ 3** Splunk のフォルダに移動し、画面が表示されたら、Splunk のローカル管理者の資格情報を入力します。



(注) 結果が即座に表示されない場合があります。

- ステップ 4** データがインポートされていることを確認します：

- Splunk Web に、admin としてログインします。
- 検索アプリケーションに移動します。
- [ステータス (Status)] > [インデックス アクティビティ (Index Activity)] > [インデックス アクティビティ 概要レポート (Index Activity Overview report)] に進みます。
- サマリー インデックスの増加分を探します。

- ステップ 5** 履歴データのインポートが Splunk 評価ライセンスで実行された場合、アカウント用にダウンロードしたエンタープライズ デフォルト ライセンスをインストールし、非プロダクション ライセンスをすべて削除してください。

次の作業

- 「Splunk でデータ入力を設定」 (P.1-9)

継続的なデータ転送の設定

Splunk でデータ入力を設定

はじめる前に

- 「履歴データのインポートおよびインデックス作成」 (P.1-7)
- ログ ファイルへのパスを把握します (「ログ ファイルのフォルダ構造を作成」 (P.1-7))。
- Splunk Web を開きます。

- ステップ 1** Splunk Web 内で、[管理者 (Manager)] > [データ入力 (Data Inputs)] > [ファイルとディレクトリ (Files and Directories)] と進みます。
- ステップ 2** CiscoWSA とラベル付けされた入力をすべて無効にします。
- ステップ 3** \$SPLUNK_HOME/etc/apps/CiscoforIronportWSA/default/inputs.conf というファイルを以下のフォルダにコピーします。
\$SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/
- ステップ 4** テキスト エディタを使用して、\$SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/inputs.conf を開きます。
- ステップ 5** 入力方法およびログ ソースに対応するセクションを見つけて、パスを編集します。

| 入力方法 | inputs.conf ファイルのセクション | 追加情報 |
|------|--|---|
| バッチ | sourcetype=wsa_accesslogs interval=60 move_policy = sinkhole | これはデフォルトです。データを読み取り、削除します。 元のデータを削除したい場合のみ、move_policy = sinkhole を追加します。 Splunk を、バッチ入力設定によるログのプライマリ ストレージとして使用しないでください。 |
| モニタ | [monitor://<path>] | Splunk は、ファイルやディレクトリの変更をモニタします。 [batch:///data1/splunklogs/*] (モニタされているフォルダ) |

- ステップ 6** 同じセクション内で、無効に設定する値を編集します : disabled = false。
- ステップ 7** ファイルを保存します。
- ステップ 8** Splunk を再起動します。
- ステップ 9** Splunk Web 内で、[管理者 (Manager)] > [データ入力 (Data Inputs)] > [ファイルとディレクトリ (Files and Directories)] と進みます。

- ステップ 10** Splunk Web で、入力内容が一覧表示および有効化され、正しいパスが設定されていることを確認します。
- ステップ 11** Splunk Web で、各入力項目のソース タイプを `wsa_accesslogs` に手動で設定します。

| ソース タイプ | ファイル/ディレクトリ名 |
|--|-----------------------------|
| [その他の設定 (More settings)] > [ソース タイプの設定 (Set the source type)] > [マニュアル (Manual)] | <code>wsa_accesslogs</code> |

- ステップ 12** Splunk Web では、入力の場合、[その他の設定 (More settings)] > [インデックス (Index)] > [初期設定 (Default)] を選択します。

Cisco Web セキュリティ アプライアンスからのログ転送を確立

はじめる前に

- ログ ファイルへのパスを把握します ([「ログ ファイルのフォルダ構造を作成」\(P.1-7\)](#))。
- 転送の頻度を決定します。60 分単位以下には設定できません。
- Cisco Web セキュリティ アプライアンスの Web インターフェイスを開きます。

- ステップ 1** Cisco Web セキュリティ アプライアンスの Web インターフェイスで、[システム管理 (System Administration)] > [サブスクリプション (Log Subscriptions)] に移動します。
- ステップ 2** [ログ設定を追加... (Add Log Subscription...)] をクリックします。
- ステップ 3** サブスクリプションを設定します。

| 設定 | ログ タイプ | 値 |
|--|------------|---|
| ログ ディレクトリ | アクセス | アクセスログ |
| | トラフィック モニタ | <code>trafmonlogs</code> |
| ファイル サイズによるロールオーバー (WSA バージョン 7.5 またはそれ以上) 最大ファイル サイズ (WSA バージョン 7.1 またはそれ以前) | どちらか | 500 Mb 以下を推奨します。 |
| 時間ごとのロールオーバー (WSA バージョン 7.5 以降) | どちらか | 1 時間 (1h) またはそれ以上頻繁なカスタム ロールオーバー間隔を推奨します。 |
| ログ形式 | アクセス | Squid |
| | トラフィック モニタ | n/a |
| (任意) カスタム フィールド | どちらか | %XK (ウェブ レピュテーション脅威の理由を追加します)。 |
| ファイル名 | どちらか | <ユーザ定義> |
| 取得方法 | どちらか | <hostname_splunk_instance> にある FTP |



(注) [ログ設定を追加 (Add Log Subscription)] ページからアクセスできるオンライン ヘルプでは、すべての設定に関する詳細情報をアップデートします。

(任意) 部門のメンバーシップクエリーをセットアップ

部門メンバーの要件を満たすセットアップ手順を次の条件で実行：

- Splunk の役割にバインドした AD/LDAP グループを使用します。
- 組織の役割に基づくデータのレポートを実行します。

関連トピック

- 「職務別の部門レポートへのアクセスを制限」(P.1-12)

部門メンバーシップ レポートをセットアップ

はじめる前に

- Linux ユーザ：次のコマンドを使用して、ldapsearch ツールをインストールします。

```
sudo yum install openldap-clients
```

ステップ 1 メンバーシップ スクリプトの AD/LDAP グループ ベース DN を特定します。

a. テキスト エディタで適切なメンバーシップ スクリプトを開きます。

- Linux : `$SPLUNK_HOME/etc/apps/CiscoWSA/bin/discovery.py`
- Windows : `X:\$SPLUNK_HOME\etc\App\CiscoWSA\bin\discovery.vbs`

b. ヘッダーの一番上の 4 つのフィールドを編集します：

```
strComputer = 'ad_ldap_host'  
strUser = 'cn=service_account,cn=Users,dc=my_directory,dc=net'  
strPassword = 'service_account_password'  
strGroupOUs = 'Group base DN;Group base DN;Group base DN'
```

c. ファイルを保存します。

ステップ 2 `inputs.conf` スクリプトにより、メンバーシップ スクリプトの使用を可能にします。

a. テキスト エディタで、`inputs.conf` スクリプトを開きます。

```
$SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/inputs.conf
```

b. 適切な文字列を検索します。

- # membership script Windows
- # membership script Linux

c. 無効を `false` に設定します：`disabled = false`

ステップ 3 ユーザ データの `departments.csv` にスクリプトが入力されたことを確認します。

```
$SPLUNK_HOME/etc/apps/CiscoWSA/lookups/departments.csv
```

■ (任意) 部門のメンバーシップクエリーをセットアップ

メンバーシップのスクリプトは、毎日実行するように初期設定されます。秒間隔にセットされ、配置要件に合わせて変更できます。

職務別の部門レポートへのアクセスを制限

はじめる前に

- ユーザのデータ閲覧が特定の部門またはグループからのデータに制限されている場合、レイヤ 4 トランスポート モニタ (L4TM) データを利用できるのは管理者のみに限られることを理解します。これは、L4TM データが部門または役割にリンクされていないためです。
- Splunk Web を開きます。

-
- ステップ 1** Splunk Web で、[管理者 (Manager)] > [アクセス コントロール (Access controls)] > [役割 (Roles)] に移動します。
- ステップ 2** [新規 (New)] をクリックするか、既存の役割を編集します。
- ステップ 3** 役割の検索制限を定義します。
- 例：営業部門データの閲覧だけに役割を限定する場合は、制限検索条件のフィールドに「department=sales」と入力します。
- ステップ 4** [保存 (Save)] をクリックします。
-

トラブルシューティング



- ヒント**
- Linux ユーザ：ldapsearch ツールが Splunk ユーザのパスにあることを確認します。
 - departments.csv ファイルがアプリケーションの参照フォルダに存在することを確認します。
 - Windows ユーザ：「option explicit」をコメントアウトし、エラーの発生と原因についてより具体的な情報を示します。
 - LDAP パスの構文が正しいことを確認します。
 - バインド サービスのアカウント名が正しいことを確認します。
 - 正しいバインド パスワードが入力されていることを確認します。
 - ポート 389 経由でリモート マシンにテスト接続します。
 - 正しい属性がメンバー名に設定されていることを確認します。
 - 正しい属性がグループ メンバーシップに使用されたことを確認します。
 - 正しい属性がグループ名に設定されていることを確認します。

(任意) スケジュール済 PDF レポートのセットアップ



(注)

スケジュール済 PDF レポートには、ネットワークで実行する Splunk の Linux ベース インスタンスが必要です。最小インストール用となります。ただし、Splunk がフォワーダとして構成された Linux 標準イメージ (インデックスまたは Web インタフェースは不要) が、PDF 生成のための複数の Splunk インスタンスの役割を果たします。

Splunk Web ユーザは、ダッシュボード、ビュー、検索またはレポートから、スケジュールされた PDF を生成できます。この機能を有効化するには、PDF レポートのサーバアプリケーションを Splunkbase からダウンロードし、シングル Linux ホストを通じて Splunk インスタンスにインストールする必要があります。さらに、PDF レポートを送信できるようにするために、内部の電子メール サーバを Splunk 内に構成します。

スケジュール済みレポートのセットアップ

- ステップ 1** PDF レポート サーバのアドオンを Splunk からダウンロードし、インストールします。
<http://splunk-base.splunk.com/apps/22348/pdf-report-server-install-on-linux-only>
- ステップ 2** Linux ディストリビューション向けの Xvfb X サーバ、xauth およびフォントがインストールされていることを確認します。これらはほとんどの Linux ディストリビューションに含まれていますが、デフォルトではインストールされません。Red Hat では、次のように入力します。

```
yum install Xvfb xauth bitstream-vera-fonts
```
- ステップ 3** Splunk Web を Linux ホスト上で起動します。
- ステップ 4** [管理者 (Manager)] > [システム設定 (System Settings)] > [電子メール アラート設定 (Email Alert Settings)] に移動します。
- ステップ 5** [PDF レポート サーバを使用 (Use PDF Report Server)] のボックスをチェックします。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** メール サーバの設定で、Splunk が相互作用している SMTP サーバに関連する情報を入力または更新し、警告の電子メールを送信できるようにします。
- ステップ 8** SMTP メール ホスト サーバを識別します。
- ステップ 9** SMTP サーバが必要とする認証ユーザ名/パスワードを提供します。
- ステップ 10** (任意) SMTP サーバと通信する際に、Splunk が SSL または TLS を使用することを指定します。
- ステップ 11** 電子メールの形式で、Splunk が送信する電子メールの形式を設定します。

「送信者」のフィールドに表示される名前を定義し (初期設定では Splunk)、電子メールの件名行の形式を設定できます (初期設定では Splunk アラート: \$name\$ - アラートの基になっている検索の名前が \$name\$ として表示される)。すべてのアラート用電子メールの形式をマネジャーレベルで設定し、また、アラートのメールがインライン結果を提供するか否かを設定できます。

PDF レポート サーバの通信先となる Splunk Web インスタンスのホスト名が DNS で解決できない場合は、IP アドレスまたはそのホスト名を、リンクのホスト名フィールドに入力します。これにより、Splunk Web の PDF レポート サーバへのアクセスと、電子メールで送信された PDF レポート中のリンクの正常な動作が確保されます。フィールドが空白の場合、Splunk はホスト名の自動検出を試行します。

ステップ 12 Splunk コア サービス ポートの変更方法: %SPLUNK_HOME%\bin ディレクトリから: `splunk set splunkd-port #####`

追加資料

- Splunk ライセンスのインストール
: <http://www.splunk.com/base/Documentation/latest/Admin/Installlicense>
- Splunk ライセンス違反
: <http://www.splunk.com/base/Documentation/latest/Admin/Aboutlicenseviolations>
- Splunk データのバックアップ:
<http://www.splunk.com/base/Documentation/latest/admin/Backupindexeddata>
- データのアーカイブ方法:
<http://www.splunk.com/base/Documentation/latest/Admin/Automatearchiving>