



Splunk 管理者マニュアル

バージョン : 4.0.3

作成日 : 2009 年 8 月 24 日 午後 5 時 1 分

Copyright Splunk, Inc. All Rights Reserved

目次

Splunk インストールマニュアルへようこそ	1
インストールマニュアルの内容	1
システム要件	1
Splunk アーキテクチャとインストール内容	3
Splunk ライセンスについて	4
インストールの前に	7
インストールの段階的手引き	8
プラットフォームの選択	8
Windows へのインストール	8
コマンドラインを使った Windows へのインストール	12
Linux へのインストール	17
Solaris へのインストール	19
Mac OS へのインストール	21
FreeBSD へのインストール	24
AIX へのインストール	26
ライセンスのインストール	28
Splunk デスクトップ・コンフィギュレーションの有効化	30
Splunk の初回起動	32
Splunk の初回起動	32
3.4.x 以前のバージョンからの移行	34
4.0 版に移行す際の留意点	34
UNIX における移行	40
Windows における移行	41
Splunk 4.x に手動で移行する手順	43
4.x Splunk インスタンスはしばらく起動しないでください。	45
4.0 以降からのアップグレード	48
Windows 上の Splunk のアップグレード	48
Linux、Solaris、FreeBSD、AIX、MacOS 上の Splunk のアップグレード	49
その他のタスク	51
Splunk を別のまたは非ルートユーザーから実行	51
Splunk のアンインストール	52
Windows にインストール中に選択したユーザーの訂正	54
スタンドアロン型 3.4.x デプロイメントサーバーの設定	55

Splunk インストールマニュアルへようこそ

インストールマニュアルの内容

インストールマニュアルの内容

本書は、システム要件、ライセンス情報、インストール手順さらに Splunk のマイグレーションについて解説します。

必要な情報を探す

本パネル左側の目次を活用する、または右上の検索ボックスに語句を入力して簡単に検索します。

より具体的なシナリオやベストプラクティスを知りたい場合は、Splunk Community Wiki で他のユーザーが Splunk IT をどのように活用しているかを見ることができます。

システム要件

システム要件

Splunk ソフトのダウンロードまたはインストールを実行する前に、サポートされているシステムに関する要件を説明する下記セクションをお読みください。今後のリリースに追加すべき新機能に関するご意見やご要望がありましたら、Splunk Support までメールしてください。また、弊社の製品ロードマップもご覧ください。

最新バージョンのダウンロードについてはダウンロードページをご覧ください。既知のさらに解決済み問題についての詳しい情報はリリースノートをお読みください。

デプロイメントにあたってのハードウェア・プランニングに関する事例については、Splunk Community Wiki に掲載されている本トピックをご覧ください。

対応OS

- Splunk は、下記のプラットフォーム上でご利用頂けます。
- Solaris 9 & 10 (x86 & SPARC)
- Linux カーネル 2.6.x 版及びそれ以降バージョン (x86)
- FreeBSD 6.1 & 6.2 (x86)
- Windows 2003 (64-bit、32-bit もサポートしているが 64-bit を推奨)
- Windows 2008 (64-bit、32-bit もサポートしているが 64-bit を推奨)
- WindowsXP (32-bit)
- Vista (32-bit & 64-bit)
- MacOSX 10.5 (32-bit)
- AIX 5.2 & 5.3

UTF-8以外のOS上でコンフィギュレーションファイルの作成と編集

Splunk は、コンフィギュレーションファイルは ASCII または UTF-8 で作成されていると推定します。UTF-8 以外の

OS上でコンフィギュレーションファイルを編集または作成する場合は、使用するエディタがASCIIまたはUTF-8で保存するように設定されているか必ず確認してください。

対応ブラウザ

- Firefox 2 および 3.0.x
- Internet Explorer 7 および 8
- Safari 3

推奨ハードウェア

Splunk は、高性能アプリケーションです。生成デプロイメントをするにあたり Splunk の総合評価を実施する際は、通常、生成環境に用いるハードウェアを使用されることをお奨めします。その際ご利用されるハードウェアは、下記に推奨するハードウェア能力仕様に**適合**またはこれを上回ることを条件とします。

注意: どのプラットフォーム上でもバーチャル・マシン(VM)モードで Splunk を実行する場合は、性能が下がります。

推奨・最小ハードウェアキャパシティ

プラットフォーム	推奨ハードウェア能力コンフィギュレーション	最小ハードウェア能力
非 Windows・プラットフォーム	2x クアッドコア Xeon、3GHz、8GB RAM、RAID 0 または 1+0、64 ビット OS 搭載	1x1.4 GHz CPU、1 GB RAM
Windows・プラットフォーム	2x クアッドコア Xeon、3GHz、8GB RAM、RAID 0 または 1+0、64 ビット OS 搭載	Pentium 4 または同等の 2Ghz、2GB RAM

注意: 個人使用に Splunk を利用される場合は、最小ハードウェアガイドラインに従ってください。Splunk をデスクトップ、またはノートブック上で活用される場合は、Splunk デスクトップアプリケーションまたはコンフィギュレーションを活用することを推奨します。

重要: フォワーダを含む全インストールに、インデックス用のスペースの他に、最低 2GB のハードディスクスペースが必要となります。プランニング情報については Splunk Community の KnowledgeBase より必要インデックスサイズ容量の推量に関するトピックをご参照ください。

重要: Splunk に関する最小要件は、Splunk ライトフォワーダインスタンス以外の全コンフィギュレーションに適用されます。

Splunkライトフォワードに関するハードウェア要件

推奨	デュアルコア 1.5Ghz+ プロセッサ、1GB+ RAM
最小	1.0 Ghz プロセッサ、512MB RAM

デプロイメントプランに関する情報は、Splunk Community KnowledgeBase のデプロイメントセクションをご参照ください。

対応ファイルシステム

プラットフォーム	ファイルシステム
Linux	ext2/3、reiser3、XFS
Solaris	UFS、ZFS、VXFS
FreeBSD	FFS、UFS
Mac OS X	HFS
AIX	JFS、JFS2、NFS 3/4
Windows	NTFS、FAT32

注意: 上記以外のファイルシステムのほとんどもサポートしています。上記にないファイルシステムで Splunk を実行すると、locktest というスタートアップユーティリティが実行する場合があります。Locktest は、スタートアップ・プロセスをテストするプログラムです。Locktest が起動されても実行しない場合は、そのファイルシステムが Splunk の実行に不適正であると見なされます。

注意: FreeBSD で、nullfs としてマウントすることはサポートしていません。

対応サーバーのハードウェアアーキテクチャ

32 および 64 ビットアーキテクチャが一部のプラットフォーム向けにサポートされています。詳細はダウンロードページをご参照ください。

Splunk アーキテクチャとインストール内容

Splunk アーキテクチャとインストール内容

プロセス

Splunk サーバーはご使用のホスト上で splunkd および splunkweb と呼ばれる 2 つプロセスを実行します。

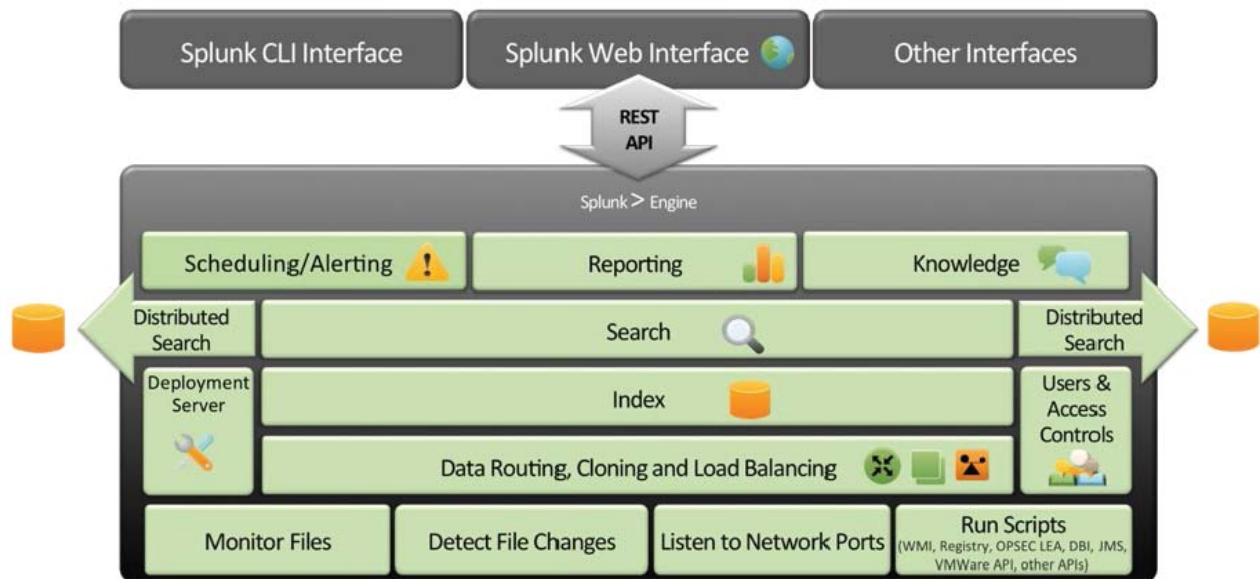
- splunkd は、分散型 C または C++サーバーで、ストリーミング IT データへのアクセス、さらに処理またはインデックスを実行します。それに加え検索要求にも対応します。Splunkd は、一連のパイプラインを使ってデータをストリーミングすることにより処理やインデックスを実行します。各パイプラインは一連のプロセッサから構成されています。
 - ◆ **パイプラインは、splunkd プロセス内のシングルスレッドで、それぞれ XML のシングルスニペットで設定されています。**

- ◆ プロセッサは、個々の再利用可能 C または C++ 機能で、パイプラインを通して IT データのストリームに作用します。パイプラインはキューを経由して互いにデータを渡し合います。Splunkd は検索や表示結果に用いるコマンドラインインタフェース (command-line interface) をサポートします。
- Splunkweb は、cherry.py を基にした Python ベースのアプリケーションサーバーで Splunk Web ユーザーインターフェースを提供します。ユーザーは、Splunk サーバーに記録された IT データを検索したりナビゲートしたり、さらに Web ユーザーインターフェースを通して Splunk のデベロップメント管理が行えます。

splunkweb および splunkd は共に、REST 経由の Web ブラウザと通信できます。

- splunkd はまた、デフォルトで SSL/HTTPS がオンの状態でポート番号 8089 で Web サーバーを実行します。
- splunkweb は、デフォルトで SSL/HTTPS がオフの状態ではポート番号 8000 で Web サーバーを実行します。

構造図



Splunk ライセンスについて

Splunkライセンスについて

Splunk サーバーのインスタンス別にライセンスの取得が必要です。このトピックでは、各種 Splunk ライセンスの違い、ライセンスのインストールと更新の仕方、ライセンス違反が発生した際の対応について解説します。

注意: デプロイメントする Splunk インスタンス別にライセンスの購入が必要です。

ライセンスの種類

Splunk には、無料ライセンスとエンタープライズライセンスの 2 種類があります。エンタープライズ版の機能を試用したい場合は、購入前に評価用のエンタープライズライセンスをご依頼ください。

注意: Splunk Preview リリース版を評価される場合は、その中に必要なライセンスが含まれています。

無料ライセンスとエンタープライズライセンス

注意: Splunk 4.0 から、仮エンタープライズライセンス(60 日間有効)が支給されます。無料ライセンスは今後のリリースでご利用頂ける予定です。

初めて Splunk をダウンロードするとき、登録するよう促されます。登録すると、1 日あたり最大 500MB のデータを取り込み可能な無料ライセンスが支給されます。無料ライセンスは評価用ライセンスではないため、使用有効期限がありません。エンタープライズライセンスでは、さらに多くの容量のデータを取り込むことが可能となる他にも下記の機能がご利用頂けます。

- 複数ユーザーアカウントとアクセスコントロール
- 分散検索とデータルーティング
- デプロイメント管理

エンタープライズライセンスの購入前に上記の機能の試用をご希望の場合は、30 日間有効の評価版エンタープライズライセンスをご用命ください。

各ライセンスの特徴に関する詳細はここをクリックしてください。また、Splunk の無料ライセンス同意書をお読みください。

評価用エンタープライズライセンス

さまざまなサイズおよび使用期間に分かれた評価用エンタープライズライセンスをご請求頂けます。デフォルト評価期限は 30 日です。評価用ライセンスを使用中にライセンスの期限が切れても、Splunk は引き続きデータをインデックスしますが、新しいライセンスがインストールされるまで検索はご利用頂けません。

注意: Splunk 4.0 から、の仮エンタープライズライセンス(60 日間有効)が支給されます。無料ライセンスは今後のリリースでご利用頂ける予定です。その時点からエンタープライズ評価用ライセンスは、ご用命によりご利用可能となります。

プレビューライセンス

Splunk のプレビューリリースには、他の Splunk リリースと互換性を持たない別種のライセンスが必要です。さらに、Splunk のプレビューリリースを評価される間は、無料またはエンタープライズ版のライセンスでは実行頂けません。プレビューライセンスは通常、エンタープライズ版の機能を有効にし、プレビューリリースのみと制限されています。

フォワーディングライセンス

Splunk サーバーの各インスタンスにはそれぞれにライセンス購入が必要です。Splunk には、フォワーダライセンスが含まれています。このライセンスは各 Splunk フォワーダにインストールする必要があります。1 日あたり最大 1MB のデータの転送のみを行うこのライセンスは、既存ライセンスから除外されません。また、複数のフォワーダに適用できます。

1. `./splunk stop` で Splunk を停止します。
2. `$SPLUNK_HOME/etc/splunk-forwarder.license` を `$SPLUNK_HOME/etc/splunk.license` にコピーします。
3. `./splunk start` で Splunk を開始します。

このライセンスは、ご使用のマシンからフォワードできるデータ量に制限はありません。

ライセンスおよび使用量の表示

Splunk Web またはコマンドラインインターフェース(CLI)でご使用のライセンスの詳細をご覧頂けます。詳しいライセンス情報にはライセンスタイプ、インデックスレベル、ライセンスの有効期限などの一般情報が含まれます。

Splunk Webのライセンス情報表示

Splunk Web でご使用のライセンスの詳細を見るには、**管理 > ライセンス**を選択します。“ライセンスおよび利用状況”の下にあります。使用ライセンスに関する一般情報の他に、ライセンスの有効日数、最大インデックス使用量(MB 表示)、ライセンス違反の数などの詳しい情報がご覧になれます。

注意: このページからもライセンスのインストールや更新をご利用頂けます。

CLIのライセンス情報表示

CLIにアクセス可能な場合は、下記の方法でライセンスについての詳細をご覧頂けます。

```
./splunk help show license
```

CLIでも同じ一般詳細を表示します。さらに、猶予期間(違反期限)内に該当ライセンスが容認する最大違反数(最大違反)などのライセンス状況に関する情報も表示します。また、Splunkは"Expiration State"を表示して、使用中のライセンスの期限切れまでの日数を7日または1日で表示します。それ以外は"ok"と表示されません。

ライセンスのインストールと更新

すべてのSplunkサーバーは、無料ライセンス(`splunk-free.license`)またはエンタープライズライセンス(`splunk.license`)に関わらずライセンスを`$SPLUNK_HOME/etc/`に置きます。CLIを利用して、またはSplunk Webの**管理 > ライセンス**ページからライセンスをインストールまたは更新できます。Splunkライセンスのインストールまたは更新に関する説明は**管理マニュアル**を参考してください。

4.0への移行

3.x Splunkインスタンスを直接4.0版に移行する場合は、Splunkを実行する前に

`$SPLUNK_HOME/etc/splunk.license`ファイルを削除してください。すると、そのスタンスは4.0版に含まれている60日間エンタープライズ版トライアルライセンスを取得します。

現在、3.xのエンタープライズライセンスおよびサポート契約がある場合は、更新用ライセンスがご利用可能です。splunk.comにログインして、<http://www.splunk.com/store/myorders>から入手してください。現存の`$SPLUNK_HOME/etc/splunk.license`ファイルを新しいファイルに置き換える、またはSplunkライセンスの更新に関する説明をご覧ください。

分散デプロイメント用ライセンス

分散環境でSplunkを複数のホスト上で実行する場合は、各ホストに固有のライセンスキーが必要です。これ今まですべてのホストに同一のライセンスキーを使用していた場合は、4.0版またはそれ以後のバージョン(4.0.3版以降のエンタープライズ評価用ライセンスを除く)では実行されません。Splunkサポートに問い合わせ、既存のライセンスを複数キーに分割してもらう、またはSplunk販売までメールにて追加キーをご注文ください。

ライセンス違反

使用ライセンスが許可する最大インデックス使用量を超えると違反が発生します。一日の規定量を超えた場合は、違反アラートを受けます。アラートメッセージは14日間持続します。30日間サイクルで5つ以上の違反が発生した場合は、検索機能が無効になります。検索機能は30日間で発生した違反が5つ以下のとき、またはこれまでよりも使用限度の大きいライセンスを新しく適用すると回復します。

注意: ライセンス違反でも**Splunk**はデータインデックスを停止しません。ライセンス限界を超えるとアクセスのみをブロックします。

インストールの前に

インストールの前に

Splunkをインストールする前に、必ずシステム要件を確認し、使用するシステムに適したインストールパッケージをダウンロードしてください。

Splunkを以前のバージョンからアップグレードする場合は、その前に、「4.0版にアップグレードする際の留意事項」の情報をお読みください。

インストールの段階的手引き

プラットフォームの選択

プラットフォームの選択

詳しいインストール手順は下表から選択してください。

- Windows
- Windows コマンドライン説明書
- Linux
- Solaris
- MacOS
- FreeBSD
- AIX

Windows へのインストール

Windowsへのインストール

このトピックは、GUI インストーラーを用いた Windows へのインストール手順について解説します。コマンドライン・インストールを使用すると、より多くのインストールオプション(サイレントインストールなど)がご利用頂けます。

注意: 4.0 から 4.0.2 のバージョンでは、Windows App は、app.conf ファイルでデフォルトで有効に設定されていました。4.0.3 版から、このファイルでデフォルトで無効に設定されています。以下の重要情報をお読みください。

- 4.0 から 4.0.2 のバージョンを 4.0.3 以降のバージョンにアップグレードすると、Windows App は更新前の有効も無効にします。
- 4.0.3 以降のバージョンを新規にインストールすると、Windows App はデフォルトで **MSI 経由**で有効に設定されます。無効でインストールする場合は、SPLUNK_APP msiexec コマンドを使用して「コマンドラインを使った Windows へのインストール」の説明に従って指定します。

重要: Splunk の 32 ビットバージョンを 64 ビットプラットフォームの Windows で実行しないでください。可能な限り 64 ビットの Splunk は 64 ビットハードウェア実行してください。32 ビットバージョンで使用する場合と比べて性能がはるかに改善されます。

Splunkを実行するユーザーの選択

Splunk Windows インストーラーを実行すると、Splunk を実行するユーザーを選ぶオプションが与えられます。

Splunk を Local System ユーザーでインストールすると、ローカルマシンにある重要な情報の全てまたはほぼ全部にアクセスが可能です。反面、Local System ユーザーは、意図的に他の Windows マシンに対して特権を持たないようにデザインされています。Event Logs や WMI を使って他のマシンのパフォーマンスカウンタを読み込む、またはログファイル用のネットワーク共有を読み込む予定がある場合は、ドメインアカウントを取得する必要があります。そのアカウントはローカル管理者または同等であり、Splunk に与えたい外部データへの権利が必要です。Splunk に与える権限が不明確な場合は、アカウント別に御社の Windows ドメイン管理者にご相談ください。

2 つの Splunk サービスに最低限必要な権限

splunkd サービスに必要なユーザー権利:

- Splunk インストールディレクトリへのフルコントロール
- フラットファイルへの読み込みアクセス
- サービスとしてログオンする許可
- バッチジョブとしてログオンする許可
- プロセスレベルトークンの置き換え
- オペレーティングシステムの一部として機能する許可
- トラバースチェックをバイパスする許可

Splunkweb サービスに必要なユーザー権利:

- Splunk インストールディレクトリへのフルコントロール
- サービスとしてログオンする許可

重要:インストール後、Splunk を実行するユーザーを変更する場合は、必ず設定したユーザーが必要な許可を所持していること、さらにユーザーが `$SPLUNK_HOME/var` ディレクトリへのフルコントロールを確保していることを確認してください。

初めてインストールする際に間違ったユーザー名を指定した場合

インストールの際に誤ったユーザーを特定してしまった場合は、それを伝える 2 つのポップアップエラーメッセージが表示されます。インストールを完了した後、関連指示に従って正しいユーザーに訂正してください。必ず Splunk を起動する前に行ってください。

GUI インストーラーを使った Splunk のインストール

Windows インストーラーは MSI ファイルにあります。

1. インストーラーを起動するには、`splunk.msi` ファイルをダブルクリックします。

歓迎パネルが表示されます。

2. インストールを開始するには、次へをクリックします。

注意: 画面上の次へをクリックすると次の画面に進み、戻るをクリックすると前の画面に戻ります。またキャンセルをクリックするとインストーラーがキャンセルされます。

ライセンス画面が表示されます。

3. ライセンス契約書を読み、"ライセンス契約条項に同意する"を選択します。次へをクリックしてインストールを続行します。

顧客情報画面が表示されます。

4. 必要な詳細を入力してから、次へをクリックします。

移動先フォルダ画面が表示されます。

注意: Splunk は、デフォルトにより \Program Files\Splunk にインストールされます。

5. 変更をクリックして、Splunk をインストールする別の場所を指定する、または次へをクリックしてデフォルトを受諾します。

ログオン情報画面が表示されます。

Splunk は、2 つの Windows サービス、splunkd および splunkweb をインストールおよび実行します。このサービスは、この画面で指定したユーザーでインストールおよび実行されます。ローカルシステム証明で Splunk を実行する、または特定のアカウントを指定するかが選択できます。アカウントは、他のマシンからデータを収集する場合は、ローカル管理者の権利さらに適切なドメイン権限の所持が必要です。

Splunk を実行するユーザーには下記を実行できる権限が必要です。

- ◆ サービスとして実行する
- ◆ 監視用の設定ファイルを読み込む
- ◆ 性能または他の WMI データを収集する
- ◆ Splunk のディレクトリに書き込む

注意: ローカルシステムユーザーとしてインストールする場合、一部のネットワークリソースを Splunk アプリケーションよりご利用頂けない場合があります。また、WMI リモート認証は機能しません。このユーザーは null 証明を持つため、通常 Windows サーバーはそのような接続を無効とします。WMI で可能とされたローカルデータの収集のみご利用可能です。指定するユーザーが不明確な場合は、御社のシステム管理者にご相談ください。

6. ユーザータイプを選択して、次へをクリックします。

重要: 移動または更新する場合、この情報は、リリース間で自動的に継承されないため、Splunk を実行するユーザーを再指定する必要があります。

ローカルシステムユーザーを指定した場合は、ステップ 8 に進みます。それ以外の場合は、**ログオン情報: ユーザー名とパスワードを入力画面が表示されます。**

7. ユーザー名とパスワードを指定してインストールし、Splunk を起動してから、次へをクリックします。

注意: 既存のユーザーを使用する場合は、ユーザー名およびドメイン詳細を入力または参照できます。

Splunk は、参照... ボタンを押して有効なユーザーを選択してください。そのユーザーがセキュリティコンテキストに存在しない、またはユーザー名を誤って入力したためにユーザーをブラウズできないと、インストールに失敗します。有効なユーザー名およびパスワードなしで Splunk を起動することはできません。つまり、参照する行為でユーザーが正しいことを確認しています。

インストール前サマリー画面が表示されます。

8. **インストール**をクリックして先に進みます。

インストーラーを実行し、インストール完了画面が表示されます。

警告: インストール手順で間違ったユーザーを指定してしまった場合は、それを説明するポップアップエラーが2つ表示されます。これが発生すると、Splunk はデフォルトでローカルシステムユーザーでインストールします。

この場合 Splunk は、自動的に起動されません。インストールの最終画面まで進み、すべてのボックスをチェックしたままにします。その後、適切な指示に従って、Splunk を起動する前に正しいユーザーに切り替えてください。

9. **その後、Splunk起動とSplunk Web起動**のボックスをチェックします。完了をクリックします。

インストールが完了し、Splunk が起動して、サポートするブラウザから Splunk Web が開始します。

注意: インストール後、初めて Splunk Web にアクセスするときは、デフォルトユーザー名 admin とパスワード changeme でログインします。

WebブラウザからSplunk開始

使用マシンで Splunk を起動した後に Splunk Web にアクセスする場合は、

- スタート>プログラム>Splunk の順に Splunk アイコンをクリックします。

または

- Web ブラウザを開いて、`http://localhost:8000` に移動します。

デフォルトのユーザー名 admin とパスワード changeme でログインします。可能な限り早い段階で、管理者パスワードを変更し、それをメモ書き保存してください。

これで Splunk を使用する準備が整いました。Splunk の使い方については、ユーザーマニュアルを参考にしてください。

Splunk Web または splunkd サービスポートの変更

Splunk Web サービスまたは splunkd サービスを別のポートで使用する場合は、デフォルトを変更します。

- splunk web サービスポートを変更する場合

`$SPLUNK_HOME/bin/ ディレクトリで、splunk set web-port #####` を実行します。

- splunkd サービスポートを変更する場合

`$SPLUNK_HOME/bin/` **ディレクト**で、`splunk set splunkd-port #####` を実行します。

IE 拡張セキュリティのポップアップの防止

IE 拡張セキュリティのポップアップを防止するには、下記の URL を IE 内のイントラネットグループまたは完全に信頼の置けるグループのみに追加します。

- `quickdraw.splunk.com`
- 使用する Splunk インスタンスの URL

ライセンスのインストールまたは更新

Splunk を新しくインストールする、または別のライセンスタイプに切り替える場合は、必ずライセンスをインストールする、または更新しなければなりません。

Splunkのアンインストール

Splunk をアンインストールするには、コントロールパネルのプログラムの追加と削除オプションを使用します。

コマンドラインを使った Windows へのインストール

コマンドラインを使ったWindowsへのインストール

このトピックは、コマンドラインを使用して Splunk を Windows にインストールする手順について解説します。

重要: Splunk 32 ビットバージョンは 64 ビットプラットフォーム上の Windows で実行しないでください。可能な限り、64 ビットハードウェアで 64 ビットの Splunk を実行してください。32 ビットバージョンを使用する場合と比べて性能がはるかに改善されます。

注意: 4.0 から 4.0.2 のバージョンでは、Windows App は、`app.conf` ファイルでデフォルトで有効に設定されていました。4.0.3 版から、このファイルでデフォルトで無効に設定されています。以下の重要情報をお読みください。

- 4.0 から 4.0.2 のバージョンを 4.0.3 以降のバージョンにアップグレードすると、Windows App は更新前のバージョンの有効も無効にします。
- 4.0.3 以降のバージョンを新規にインストールすると、Windows App はデフォルトで MSI 経由で有効に設定されます。無効でインストールする場合は、`SPLUNK_APP msiexec` コマンドを使用してこのトピックで後述される説明に従って指定します。

Splunkを実行するユーザーの選択

Splunk Windows インストーラーを実行すると、Splunk を実行するユーザーを選ぶオプションが与えられません。

Splunk を Local System ユーザーでインストールすると、ローカルマシンにある重要な情報の全てまたはほぼ全部にアクセスが可能です。反面、Local System ユーザーは、意図的に他の Windows マシンに対して特権を持たないようにデザインされています。Event Logs や WMI を使って他のマシンのパフォーマンスカウンタを読み込む、ログファイル用のネットワーク共有を読み込む予定がある場合は、ドメインアカウントを取得する必要があります。そのアカウントはローカル管理者または同等であり、Splunk に与えたい外部データへの権利が必要です。Splunk に与える権限が不明確な場合は、アカウント別に御社の Windows ドメイン管理者にご相談ください。

2 つの Splunk サービスに最低限必要な権限

splunkd サービスに必要なユーザー権利:

- Splunk インストールディレクトリへのフルコントロール
- フラットファイルへの読み込みアクセス
- サービスとしてログオンする許可
- バッチジョブとしてログオンする許可
- プロセスレベルトークンの置き換え
- オペレーティングシステムの一部として機能する許可
- トラバースチェックをバイパスする許可

Splunkweb サービスに必要なユーザー権利:

- Splunk インストールディレクトリへのフルコントロール
- サービスとしてログオンする許可

重要: インストール後、Splunk を実行するユーザーを変更する場合は、必ず設定したユーザーが必要な許可を所持していること、さらにユーザーに`$SPLUNK_HOME/var` ディレクトリへのフルコントロールがあることを確認してください。

インストールの際に誤ったユーザーを指定すると Splunk は、起動しません。これが発生した場合 Splunk は、デフォルトでローカルシステムユーザーとしてインストールします。**必ず Splunk を起動する前に適切な指示に従って正しいユーザーに訂正してください。**

コマンドラインを使ったMSIの使い方

以下を入力するとコマンドラインで MSI を使って Splunk を Windows にインストールできます。

```
msiexec.exe /i Splunk.msi
```

このセクションは、この操作に使用可能なフラグを一覧し、その設定例をいくつか紹介します。

下記を指定できます。

- インデックスする(しない)Windows イベントログ
- 監視する Windows レジストリハイブ
- 取り出す WMI 情報
- Splunk を実行するユーザー(指定するユーザーが適切な権限を持ち、Splunk にインデックスさせるコンテンツにアクセスがあることを確認する)。
- Splunk で有効にするアプリケーションに含まれたコンフィギュレーション(Splunk ライトフォワードなど)
- インストール完了後に Splunk を自動起動するかどうか

注意: インストール後、初めて Splunk Web にアクセスするときは、デフォルトユーザー名 admin とパスワード changeme を用いてログインします。

対応フラグ

コマンドラインを使用して Splunk を Windows にインストールするときに使用可能なフラグの一覧を以下に示します。

このフラグは、インストールするディレクトリを指定します。デフォルトは、`c:\program files\splunk` です。

- `INSTALLDIR=<ディレクトリのパス>`

このフラグは、`splunkd` および `splunkweb` が使用する代替のポートを指定します。

- `SPLUNKD_PORT=<ポート番号>`
- `WEB_PORT=<ポート番号>`

このフラグは、Splunk がある特定の Windows イベントログをインデックスするか否かを指定します。

- `WINEVENTLOGAPPCHECK=1/0`, デフォルトは off
- `WINEVENTLOGSECHECK=1/0`, デフォルトは off
- `WINEVENTLOGSYSCHECK=1/0`, デフォルトは off
- `WINEVENTLOGFWDCHECK=1/0`, デフォルトは off
- `WINEVENTLOGSETCHECK=1/0`, デフォルトは off

このフラグは、Splunk が Windows レジストリ USER ハイブをインデックスするか否かを指定します。デフォルトは 0 (オフ) です。

- `REGISTRYCHECK_U=1/0`
- `REGISTRYCHECK_BASELINE_U=1/0`

このフラグは、Splunk が Windows レジストリ LocalMachine ハイブをインデックスするか否かを指定します。デフォルトは 0 (オフ) です。

- `REGISTRYCHECK_LM=1/0`
- `REGISTRYCHECK_BASELINE_LM=1/0`

このフラグは、インデックスする WMI 性能情報を指定します。デフォルトは 0 (オフ) です。

- WMICHECK_CPUTIME=1/0
- WMICHECK_LOCALDISK=1/0
- WMICHECK_FREEDISK=1/0
- WMICHECK_MEMORY=1/0

このフラグは、Splunk を実行するユーザーを指定します。サポートされる値は、LocalSystem ユーザーが 1、その他のユーザーは 2 です。デフォルト値は 1 です。

- RBG_LOGON_INFO_USER_CONTEXT=1/2

このフラグは、RBG_LOGON_INFO_USER_CONTEXT に指定されているユーザーにドメイン・ユーザー名およびパスワード情報を提供します。"domain\username"フォーマットでは必ず、ユーザー名と共にドメインも指定します。

- IS_NET_API_LOGON_USERNAME="<ドメイン\ユーザー名>"
- IS_NET_API_LOGON_PASSWORD="<パス>"

このフラグは、Splunk アプリケーションに含まれるコンフィギュレーションを Splunk にインストールするかを指定します。現在<SplunkApp>をサポートするオプションは、SplunkLightForwarder、SplunkForwarder、SplunkDesktop です。

フォワーダに関する詳しい情報は Splunk フォワーダおよびライトフォワーダ・コンフィギュレーションについての解説を参照してください。ここで、Splunk フォワーダまたはライトフォワーダのどちらかを指定するのであれば、FORWARD_SERVER="<server:port>"も指定する必要があります。

- SPLUNK_APP=<SplunkApp>

Splunk のデスクトップアプリケーションのコンフィギュレーションは、Windows にインストールする際、デフォルトで無効にされています。インストール完了後、SPLUNK_APP フラグで別のアプリケーションを指定する、または SplunkDesktop アプリケーションを有効にして変更できます。全くアプリケーションなしで Splunk をインストールするには、値に何も指定せずにこのフラグを指定します (SPLUNK_APP="")。

Splunk フォワーダまたはライトフォワーダのいずれかを有効にするために SPLUNK_APP を使用する場合*のみ*、このフラグを使います。このフォワーダがデータを送信する先の Splunk サーバーのサーバーとポートを指定します。

- FORWARD_SERVER="<server:port>"

このフラグは、インストール完了後に Splunk を自動的に起動すべきか否かを指定します。デフォルト値は、1 (オン) です。

- LAUNCHSPLUNK=0/1

重要: Splunk フォワーダを有効にすると、Splunk は自動的に起動します。これを無効にすることはできません。

サイレントインストール

無音でインストールを実行するには、インストールコマンド文字列の最後に `/quiet` を加えます。御社システムが、UAC(時々デフォルトでオンに設定されている)を実行する場合は、必ず管理者でインストールしてください。そのためには、cmd プロンプトを開いた際、右クリックして、"責任者として実行"を選びます。次に cmd 画面から、サイレントインストールコマンドを実行します。

例

以下にフラグを活用した例をいくつか紹介します。

Splunkをローカルシステムユーザーとして実行するためのインストール

```
msiexec.exe /i Splunk.msi RBG_LOGON_INFO_USER_CONTEXT=1
```

ユーザーが属するユーザー名とドメインの指定

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"  
RBG_LOGON_INFO_USER_CONTEXT=2 IS_NET_API_
```

SplunkForwarderを有効にし、Windows Systemイベントログのインデックスを無効にしてサイレントモードでインストーラーを実行

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"  
FORWARD_SERVER="<server:port>" WINEVENTLOGSYSCHECK=
```

"<server:port>"は、このマシンがデータを送付する先である Splunk サーバーのサーバとポートの場所を示します。

WebブラウザからSplunkを起動

使用マシンで Splunk を起動した後に Splunk Web にアクセスする場合は、

- スタート>プログラム>Splunk の順に Splunk アイコンをクリックします。

または

- Web ブラウザを開いて、`http://localhost:8000` に移動します。

デフォルトのユーザー名 `admin` とパスワード `changeme` を用いてログインします。可能な限り早い時期に管理者パスワードを変更し、それをメモ書き保存してください。

これで Splunk を使用する準備が整いました。ユーザーマニュアルを参考にして、Splunk をご活用下さい。

Splunkデスクトップアプリケーションの設定

Splunk を Windows マシンにインストールすると、Splunk デスクトップアプリケーションの設定はデフォルトで無効です。Splunk デスクトップアプリケーションの設定に関する詳細をご確認ください。このトピックで前述したとおり、適切なコマンドラインインストールフラグを用いればデフォルトでこのアプリケー

ションを有効にすることができます。

IE拡張セキュリティのポップアップの防止

IE 拡張セキュリティのポップアップを防止するには、IE 内のイントラネットグループまたは完全に信頼の置けるグループのみに下記の URL を追加します。

- quickdraw.splunk.com
- 使用されている Splunk インスタンスの URL

ライセンスのインストールまたは更新

Splunk を新しくインストールする、または別のライセンスタイプに切り替える際は、必ずライセンスをインストールするまたは更新しなければなりません。

Splunkのアンインストール

- Splunk をアンインストールするには、コントロールパネルのプログラムの追加と削除オプションを使用します。
- また、コマンドラインから `msiexec` も実行できます。

Linux へのインストール

Linuxへのインストール

RPM または DEB パッケージ、さらにターボールを用いて Linux に Splunk をインストールできます。

RedHatでRPMをインストール

デフォルトディレクトリの `/opt/splunk` に Splunk RPM をインストールする場合

```
rpm -i splunk_package_name.rpm
```

別のディレクトリに Splunk をインストールするには、`--prefix` フラグを使用する場合

```
rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
```

RPM を用いてすでにインストールされている Splunk を更新する場合

```
rpm -U splunk_package_name.rpm
```

別のディレクトリにすでにインストールされている Splunk を更新するには、`--prefix` フラグを使用する場合

```
rpm -U --prefix=/opt/new_directory splunk_package_name.rpm
```

kickstart を用いて自動的に RPM インストールを実行する場合は、下記を kickstart ファイルに追加します。

```
./splunk start --accept-license
```

```
./splunk enable boot-start
```

注意: 2 行目は kickstart ファイル用のオプションです。

DebianでDEBをインストール

Splunk DEB パッケージをインストールする場合

```
dpkg -i splunk_package_name.deb
```

注意: Splunk DEB パッケージはデフォルトロケーションの `/opt/splunk` のみにインストール可能です。

ターボールのインストール

Linux システムに Splunk をインストールするには、適切なディレクトリへターボールを拡張します。デフォルトインストールディレクトリは `/opt/splunk` です。

ターボールを用いてインストールする場合

- Splunk は、`splunk` ユーザーを自動作成しません。Splunk を特定のユーザーで実行する場合は、必ず手動でそのユーザーを作成してください。
- インデックスを維持したまま非圧縮ボリュームデータを保持する場合は、ディスクパーティションに十分な容量があるか確認してください。

インストールの内容の確認

Splunk パッケージ状態

```
dpkg --status splunk
```

全パッケージのリスト

```
dpkg --list
```

Splunkの起動

Splunk はローカルシステムでユーザーを指定して実行できます。Splunk を非ルートユーザーで実行する場合は、Splunk に指定した入力の読み込みに適切な権限が与えられているかご確認ください。非ルートユーザーとして Splunk を実行するための詳細は説明書を参考してください。

コマンドラインインタフェースから Splunk を起動する場合は、下記のコマンドを実行します。

```
$(SPLUNK_HOME)/bin/splunk start
```

本書では以下を活用します。

- `$(SPLUNK_HOME)` で、Splunk インストールへのパスを確認します。
- `$(SPLUNK_HOME)/bin/` で、コマンドラインインタフェースの場所を表示します。

起動オプション

新しくインストールした後、Splunk を初めて起動するときは、ライセンス契約条項に同意する必要があります。Splunk の起動とライセンス契約の同意は 1 回で行えます。

```
$(SPLUNK_HOME)/bin/splunk start --accept-license
```

注意: `accept-license` オプションの前にはダッシュが 2 つあります。

Splunk Webの開始とログイン

Splunk を起動してライセンス契約に同意した後に以下を行います。

1. ブラウザ画面より、`http://<hostname>:port` から Splunk Web へアクセスします。
 - Hostname は、ホストマシンです。
 - Port は、インストールで指定したポートです(デフォルトポート番号は、8000)。
2. 無料ライセンス版で Splunk を実行する場合は、ログイン情報を入力しなくても Splunk Web が起動します。エンタープライズ版で Splunk を実行する場合は、ログイン情報(デフォルト、ユーザー名 admin とパスワード changeme)を入力してから Splunk Web が起動されます。

Splunkのアンインストール

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、最初にパッケージからインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスに関するファイルが含まれます。

パッケージ管理コマンドが使用できない場合は、Splunk のコンポーネントの手動アンインストールについての説明書に従ってください。

RedHat Linux

RedHat で Linux をアンインストールする場合

```
rpm -e splunk_product_name
```

Debian Linux

Debian で Linux をアンインストールする場合

```
dpkg -r splunk
```

消去(コンフィギュレーションファイルを含む全てを削除)

```
dpkg -P splunk
```

Solaris へのインストール

Solarisへのインストール

このトピックは Solaris へ Splunk をインストールする手順について解説します。

Splunkのインストール

PKG ファイルまたはターボールとして Solaris を Splunk へインストールできます。

PKGファイルのインストール

PKG インストールパッケージには、Splunk をインストールする前にいくつかの質問に答えるよう促すリクエストファイルが含まれてきます。

```
pkgadd -d ./splunk_product_name.pkg
```

利用可能なパッケージが一覧表示されます。

- 処理するパッケージを選択します(デフォルトは"全て")。

次にインストーラーがベースインストールディレクトリを指定するよう促します。

- デフォルトディレクトリ/opt/splunk にインストールする場合は、ブランクのままにします。

PKGファイルの更新

PKG ファイルを使用してすでにインストールされている Splunk を更新する場合は、新規にインストールするときと同じコマンドラインを活用します。

```
pkgadd -d ./splunk_product_name.pkg
```

変更したファイルを上書きするよう促されますので、全てに"はい"と答えます。

サイレント更新を実行する場合(さらに全ファイル上書きに"はい"と答える必要がない場合)は、下記を入力します。

```
pkgadd -n -d ./splunk_product_name.pkg
```

ターボールのインストール

Solaris システムに Splunk をインストールするには、適切なディレクトリへターボールを拡張します。デフォルトでは、Splunk は/opt/splunk へインストールされます。

ターボールでインストールする場合、

- Splunk は、splunk ユーザーを自動作成しません。Splunk を特定のユーザーで実行する場合は、必ず手動でそのユーザーを作成してください。
- インデックスを維持したまま非圧縮ボリュームデータを保持する場合は、ディスクパーティションに十分な容量があることを確認してください。

インストールの内容

Splunk パッケージ情報

```
pkginfo -l splunk
```

全パッケージのリスト

```
pkginfo
```

Splunkの起動

Splunk はローカルシステムでユーザーを指定して実行します。Splunk を非ルートユーザーで実行する場合は、Splunk に指定した入力を読み込むために適切な権限が与えられているか確認します。非ルートユーザ

一で Splunk を実行するための詳細は説明書を参考してください。

コマンドラインインタフェースから Splunk を起動する際は、下記のコマンドを実行します。

```
$SPLUNK_HOME/bin/splunk start
```

本書では以下を活用します。

- `$SPLUNK_HOME` で、Splunk インストールへのパスを確認します。
- `$SPLUNK_HOME/bin/` で、コマンドラインインタフェースの場所を表示します。

起動オプション

新しくインストールした後、Splunk を初めて起動するときは、ライセンス契約条項に同意する必要があります。Splunk の起動とライセンス契約の同意は 1 回で行えます。

```
$SPLUNK_HOME/bin/splunk start --accept-license
```

注意: `accept-license` オプションの前にはダッシュが 2 つあります。

Splunk Webの起動とログイン

Splunk を起動してライセンス契約に同意した後、以下を行います。

1. ブラウザ画面より、`http://mysplunkhost:port` から Splunk Web へアクセスします。
 - `mysplunkhost` は、ホストマシンです。
 - `port` は、インストール中に特定したポートです(8000)。
2. 無料ライセンス版で Splunk を実行する場合は、ログイン情報を入力しなくても Splunk Web が起動されます。エンタープライズ版で Splunk を実行する場合は、ログイン情報(デフォルト、ユーザー名 `admin` とパスワード `changeme`)を入力すると Splunk Web が起動されます。

Splunkのアンインストール

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、最初にパッケージからインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスに関するファイルが含まれます。

```
pkgrm splunk
```

Mac OS へインストール

Mac OSへインストール

Mac OS の形態は、DMG パッケージとターボールの 2 種類です。下記はその解説です。

- DMG ファイルを使ったグラフィカル(基本)およびコマンドラインからインストール
- ターボールからインストール

グラフィカルインストーラ

1. DMG ファイルをダブルクリックします。

splunk.pkg を含むファインダ画面が開きます。

2. ファインダ画面の splunk.pkg をダブルクリックします。

Splunk インストーラーが開き、バージョンやコピーライト情報をリストした導入が表示されます。

3. 続行をクリックします。

インストール先選択の画面を開きます。

4. 場所を選んで、Splunk をインストールします。

- HDD アイコンをクリックして、デフォルトディレクトリの /Applications/splunk へインストールします。
- フォルダーの選択... をクリックして別の場所を選択します。

5. 続行をクリックします。

インストール前サマリーが表示されます。変更する場合は、

- インストール場所の変更をクリックして、新しいフォルダを選ぶ、または
- 戻るをクリックして前の手順に戻ります。

6. インストールをクリックします。

インストールが始まります。通常数分かかります。

7. インストールが完了したら、完了をクリックします。

コマンドラインからインストール

1. dmg をマウント

```
hdid splunk_package_name.dmg
```

2. インストール

- ルートボリュームの場合

```
installer -pkg splunk.pkg -target /
```

- 別のディスクパーティションの場合

```
installer -pkg splunk.pkg -target /Volumes/Disk
```

-target は、Splunk が /Applications/splunk にインストールされる別のディスクなどのターゲットボリュームを指定します。

任意のボリュームで /Applications/splunk 以外のディレクトリにインストールする場合は、前述のグラフィカルインストーラーを使用します。

ターボールのインストール

Mac OS システムに Splunk をインストールする際、適切なディレクトリへターボールを拡張します。デフォルトインストールディレクトリは `/Applications/splunk` です。

ターボールを用いてインストールする場合、

- Splunk は、splunk ユーザーを自動作成しません。Splunk を特定のユーザーで実行する場合は、必ず手動でそのユーザーを作成してください。
- インデックスを維持したまま非圧縮ポリュームデータを保持する場合は、ディスクパーティションに十分な容量があることを確認します。

Splunkの起動

Splunk はローカルシステムでユーザーを指定して実行します。Splunk を非ルートユーザーで実行する場合は、Splunk に指定した入力を読み込むために適切な権限が与えられているか確認してください。

コマンドラインインタフェースで Splunk を起動する際は、下記のコマンドを実行します。

```
$SPLUNK_HOME/bin/splunk start
```

本書は以下を活用します。

- `$SPLUNK_HOME` で、Splunk インストールへのパスを確認します。
- `$SPLUNK_HOME/bin/` で、コマンドラインインタフェースの場所を表示します。

起動オプション

新しくインストールした後、Splunk を初めて起動するときは、ライセンス契約条項に同意する必要があります。Splunk の起動とライセンス契約の同意は 1 回で行えます。

```
$SPLUNK_HOME/bin/splunk start --accept-license
```

注意: `accept-license` オプションの前にはダッシュが 2 つあります。

Splunk Webの起動とログイン

Splunk を起動してライセンス契約に同意した後、以下を行います。

1. ブラウザ画面より、`http://<hostname>:port` から Splunk Web へアクセスします。
 - `hostname` は、ホストマシンです。
 - `port` は、インストール中に特定したポートです(デフォルトポート番号は、8000 です。)
2. ユーザー名 `admin` とパスワード `changeme` を用いて Splunk にログインします。

ライセンス管理

Splunk を新しくインストールする、または別のライセンスタイプに切り替える際は、必ずライセンスをインストールする、または更新する必要があります。

Splunkのアンインストール

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、最初にパッケージからインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスに関するファイルが含まれます。

または、コマンドラインの\$SPLUNK_HOME/bin に移動して、コマンドラインに./splunk stop を入力して \$SPLUNK_HOME ディレクトリとそれに属する全てを削除します。

FreeBSD へのインストール

FreeBSDへのインストール

FreeBSD の形態は、インストーラー(5.4-intel)とターボール(i386)の 2 種類です。両方ともに TGZ ファイルです。

基本インストール

intel インストーラーを使って FreeBSD へインストールする場合

```
pkg_add splunk_package_name-5.4-intel.tgz
```

この場合、Splunk はデフォルトディレクトリの /opt/splunk/ にインストールされます。

別のディレクトリに Splunk をインストールする場合

```
pkg_add -v -p /usr/splunk splunk_package_name-5.4-intel.tgz
```

ターボールのインストール

FreeBSD システムに Splunk をインストールするには、適切なディレクトリへターボールを拡張します。デフォルトインストールディレクトリは、 /opt/splunk です。

ターボールを用いてインストールする場合、

- Splunk は、splunk ユーザーを自動作成しません。Splunk を特定のユーザーで実行する場合は、必ず手動でそのユーザーを作成してください。
- インデックスを維持したまま非圧縮ボリュームデータを保持する場合は、ディスクパーティションに十分な容量があることを確認してください。

インストール完了後

Splunk が正しく FreeBSD 上で機能することを確認するために、必ず下記を行ってください。

1. 以下を /boot/loader.conf に追加します。

```
kern.maxdsiz="2147483648" # 2GB  
kern.dfldsiz="2147483648" # 2GB  
machdep.hlt_cpus=0
```

2. 以下を/etc/sysctl.conf に追加します。

```
vm.max_proc_mmap=2147483647
```

OS を再起動して変更を反映させます。

インストールの内容

Splunk パッケージリストの表示

```
pkg_info -L splunk
```

全パッケージのリスト

```
pkg_info
```

Splunkの起動

Splunk はローカルシステムでユーザーを指定して実行します。Splunk を非ルートユーザーで実行する場合は、Splunk に特定した入力を読み込むために適切な権限が与えられているか確認してください。

コマンドラインインタフェースから Splunk を起動する際は、下記のコマンドを実行します。

```
$(SPLUNK_HOME)/bin/splunk start
```

本書では以下を活用します。

- \$(SPLUNK_HOME) で、Splunk インストールのパスを確認します。
- \$(SPLUNK_HOME)/bin/で、コマンドラインインタフェースの場所を表示します。

起動オプション

新しくインストールした後、Splunk を初めて起動するときは、ライセンス契約条項に同意する必要があります。Splunk の起動とライセンス契約の同意は 1 回で行えます。

```
$(SPLUNK_HOME)/bin/splunk start --accept-license
```

注意: accept-license オプションの前にはダッシュが 2 つあります。

Splunk Webの起動とログイン

Splunk を起動してライセンス契約に同意した後、以下を行います。

1. ブラウザ画面より、`http://<hostname>:port` から Splunk Web へアクセスします。
 - Hostname は、ホストマシンです。
 - Port は、インストール中に特定したポートです(デフォルトポート番号は、8000 です。)
2. 無料ライセンス版で Splunk を実行する場合は、ログイン情報の入力なくとも Splunk Web が起動されます。エンタープライズ版で Splunk を実行する場合は、ログイン情報(デフォルト、ユーザー名 admin とパスワード changeme)を入力すると Splunk Web が起動されます。

ライセンス管理

Splunk を新しくインストールする、または別のライセンスタイプに切り替える際は、必ずライセンスをインストールする、または更新する必要があります。

Splunkのアンインストール

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、最初にパッケージからインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスに関するファイルが含まれます。

デフォルトロケーションから Splunk をアンインストールする場合

```
pkg_delete splunk
```

別のロケーションから Splunk をアンインストールする場合

```
pkg_delete -p /usr/splunk splunk
```

AIX へのインストール

AIXへのインストール

このトピックは Splunk を AIX プラットフォームにインストールする手順をガイドします。

注意: アップグレードする場合は、本書後述のアップグレード文書をご覧ください。移行する場合は、実施する前に移行に関する注意事項を確認してください。

Splunkのインストール

AIX インストールはターボール形式で行います。

ターボールを用いてインストールする場合、

- Splunk は、`splunk` ユーザーを自動作成しません。Splunk を特定のユーザーで実行する場合は、必ず手動でそのユーザーを作成してください。
- インデックスを維持したまま非圧縮ボリュームデータを保持する場合は、ディスクパーティションに十分な容量があることを確認してください。

AIX システムに Splunk をインストールする際、適切なディレクトリへターボールを拡張します。デフォルトインストールディレクトリは `/opt/splunk` です。

AIX 5.3 の場合、最新版のサービスパックであることを確認してください。Splunk には以下のサービスレベルが必要です。

```
$ oslevel -r  
5300-005
```

Splunkの起動

Splunk はローカルシステムでユーザーを指定して実行します。Splunk を非ルートユーザーで実行する場合は、Splunk に特定した入力を読み込むために適切な権限が与えられていることを確認します。非ルートユーザーとして Splunk を実行するための詳細は説明書を参考してください。

コマンドラインインタフェースから Splunk を起動する際は、以下のコマンドを実行します。

```
$SPLUNK_HOME/bin/splunk start
```

本書では以下を活用します。

- `$SPLUNK_HOME` で、Splunk インストールのパスを確認します。
- `$SPLUNK_HOME/bin/` で、コマンドラインインタフェースの場所を表示します。

起動オプション

新しくインストールをした後、Splunk を初めて起動するときは、ライセンス契約条項に同意する必要があります。Splunk の起動とライセンス契約の同意は 1 回で行えます。

```
$SPLUNK_HOME/bin/splunk start --accept-license
```

注意: `accept-license` オプションの前にはダッシュが 2 つあります。

詳細は、本書の「Splunk 起動オプション」を参考してください。

Splunk Webの起動とログイン

Splunk を起動してライセンス契約に同意した後、以下を行います。

1. ブラウザ画面より、`http://<hostname>:port` から Splunk Web へアクセスします。
 - `hostname` は、ホストマシンです。
 - `port` は、インストール中に特定したポートです(デフォルトポート番号は、8000)。
2. 無料ライセンス版で Splunk を実行する場合は、ログイン情報を入力しなくても Splunk Web が起動されます。エンタープライズ版で Splunk を実行する場合は、ログイン情報(デフォルト、ユーザー名 `admin` とパスワード `changeme`)を入力してから Splunk Web が起動します。

ライセンス管理

Splunk を新しくインストールする、または別のライセンスタイプに切り替える際は、必ずライセンスをインストールするまたは更新しなければなりません。

Splunkのアンインストール

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、最初にパッケージからインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスに関するファイルが含まれます。

ライセンスのインストール

ライセンスのインストール

Splunk サーバーのインスタンス別にライセンスの取得が必要です。このトピックでは、各様 Splunk ライセンスの違い、ライセンスのインストールと更新の仕方、ライセンス違反が発生した際の対応について解説します。

注意: デプロイメントする Splunk インスタンスそれぞれにライセンスの購入が必要です。

ライセンスの種類

Splunk には、無料ライセンスとエンタープライズライセンスの 2 種類があります。エンタープライズ版の機能を試用したい場合は、購入前に評価用のエンタープライズライセンスをご依頼ください。

Splunk プレビューリリース版を評価する場合は、その中に必要なライセンスが含まれています。

注意: Splunk 4.x には現在、500MB エンタープライズ評価用ライセンスが含まれ、デフォルトで有効に設定されています。無料ライセンスは今後のリリースでご利用頂ける予定です。その時点からエンタープライズ評価用ライセンスは、ご用意により利用可能となります。

無料ライセンスとエンタープライズライセンス

初めて Splunk をダウンロードするとき、登録するよう促されます。登録すると、1 日あたり最大 500MB のデータを取り込み可能な無料ライセンスが支給されます。無料ライセンスは評価用ライセンスではないため、使用有効期限がありません。エンタープライズライセンスでは、さらに多くの容量のデータを取り込むことが可能となる他に、下記の機能がご利用頂けます。

- 複数ユーザーアカウントとアクセスコントロール
- 分散サーチとデータルーティング
- デプロイメント管理

重要: 3.4.2 版から、無料ライセンスで Splunk を実行しているユーザーは、フォワーダからデータを受け取るようにインスタンスの設定ができるようになりました。それ以前の Splunk バージョンでは、ユーザーはこの分散設定の変更にエンタープライズ版の取得が必要でした。

エンタープライズライセンスを購入する前に上述の機能を試す場合は、30 日間の評価用エンタープライズライセンスをご請求ください。

ライセンス別の特徴に関する詳しい情報は[ここをクリック](#)してください。また、Splunk の無料ライセンス同意書もお読みください。

評価用ライセンス

さまざまなサイズおよび使用期間に分かれた評価用エンタープライズライセンスをご請求頂けます。デフォルト評価期限は 30 日です。評価用ライセンスを使用中にライセンスの期限が切れても、Splunk は引き続き

データをインデックスしますが、新しいライセンスがインストールされるまで検索はご利用頂けません。

プレビューライセンス

Splunk のプレビューリリースには、他の Splunk リリースと互換性を持たない別種のライセンスが必要です。さらに、Splunk のプレビューリリースを評価される間は、無料またはエンタープライズ版のライセンスでは実行頂けません。プレビューライセンスは通常、エンタープライズ版の機能を有効にし、プレビューリリースのみと制限されています。

フォワーディングライセンス

Splunk サーバーの各インスタンスに対して個別にライセンスの購入が必要です。フォワーダーライセンスは商品付属です。

1. `./splunk stop` から Splunk を停止します。
2. `$SPLUNK_HOME/etc/splunk-forwarder.license` を `$SPLUNK_HOME/etc/splunk.license` にコピーします。
3. `./splunk start` から Splunk を起動します。このライセンスは、

使用マシンからフォワードできるデータ量に制限はありません。

ライセンスのインストールまたは更新

すべての Splunk サーバーは、無料ライセンス(`splunk-free.license`)またはエンタープライズライセンス(`splunk.license`)に関わらずライセンスを `$SPLUNK_HOME/etc/` に置きます。CLI を利用して、または Splunk Web からライセンスをインストールまたは更新できます。

Splunk Webを使ったライセンスのインストール

1. 管理者ユーザーで Splunk Web へログインします。
2. **管理>ライセンス**の順にクリックします。
3. **ライセンス変更**をクリックします。
4. ライセンスキーを貼り付けて、**保存**をクリックします。
5. メイン画面の Manager タブに戻り、Splunk **再起動**をクリックします。

初めて実行する前にライセンスをプレシード

4.0.2 版から、デフォルトにより Splunk を初めて実行する際、既存するすべての 3.x ライセンスをバックアップして、仮エンタープライズ評価用ライセンスに切り替えます。これにより、新しいライセンスを取得するまで期限切れになることなく新しいバージョンの Splunk が使用できるようになります。

Splunk 4.0.2 版以降のバージョンに移行し、有効な 4.x ライセンスを取得すると、ライセンスファイルをプレシードすることができ、Splunk 4 を初めて起動する際、新しいライセンスを取り込んでインストールします。これにより、各マシンで Splunk を起動した後、新しいライセンスを手動でコピーする必要がなくなる

ため、特に複数のインスタンスをデプロイするときに非常に便利です。

- 4.0.2 版以降のバージョンに移行した後は、すぐに Splunk を起動しないでください。
- 新しいライセンスを \$SPLUNK_HOME/etc/splunk-user.license へコピーします。
- Splunk を起動します。

デプロイ可能なパッケージを作成している場合、他のシステムへデプロイメントするように複数のファイルを 1 つのファイルにまとめたり、ファイルを zip 形式で圧縮したりする前に更新したライセンスが付いた splunk-user.license ファイルをその中に含めることができます。

ライセンス違反

使用ライセンスが許可する最大インデックス使用量を超えると違反が発生します。一日の規定量を超えた場合は、違反アラートを受けます。アラートメッセージは 14 日間持続します。30 日間サイクルで 5 つ以上の違反が発生した場合は、検索機能が無効になります。検索機能は 30 日間で発生した違反が 5 つ以下のとき、またはこれまでよりも使用限度の大きいライセンスを新しく適用すると回復します。

注意: ライセンス違反でも Splunk はデータインデックスを停止しません。ライセンス限界を超えるとアクセスのみをブロックします。

Splunk デスクトップ・コンフィギュレーションの有効化

Splunk デスクトップ・コンフィギュレーションの有効化

個人使用のために Splunk をインストールするとき、または初めてノートブックパソコンで Splunk を試用するときは、Splunk デスクトップ用コンフィギュレーションを活用してください。Splunk デスクトップは、Windows や Mac のノートブックなど、卓上マシンのために特別にデザインされた簡易設定の Splunk です。Splunk デスクトップは Splunk フォワーダではなく、実生産レベルでない使用向けのハードウェアに対応する Splunk の縮小版です。

Splunk デスクトップの違いとは何か？

この設定は、全体的なインデックスを縮小し、ファイルシステム変更モニタを無効にしました。これにより、Splunk が他の用途(ノートブックなど)に使用するシステムのメモリや処理能力の使用量を減らしています。

Splunk デスクトップの設定を変更する(特定の入力方式を組み入れるなど)場合は、

`$SPLUNK_HOME/etc/apps/SplunkDesktop/default` (`SPLUNK_HOME` は、Splunk がインストールされているディレクトリ) にある SplunkDesktop アプリケーション用の `setup.conf` を編集します。

Splunk デスクトップの概要

Windows に Splunk をインストールした場合、Splunk デスクトップは、デフォルトで無効です。下記に説明する有効にするための手順に従って、Splunk デスクトップを有効にして、使用するデスクトップ/ノート

ブックのフットプリントを減少することができます。

Splunk デスクトップコンフィグレーションは、デプロイメントサーバー機能を無効にしていますが、デプロイメントクライアントとしての実行をサポートします。Splunk デプロイメントサーバーを実行するには、デスクトップコンフィグレーションアプリケーションをオフにする必要があります。

Splunk WebでSplunkデスクトップを有効にする

Splunk Web で Splunk デスクトップを有効にする

1. Splunk Web へログインします。
2. **管理**をクリックして、**App 管理**タブを選択し、この Splunk ホストにインストールされている Apps をクリックします。
3. 該当する SplunkDesktop を探してクリックします。**有効**ドロップダウンリストから True を選択します。
4. 管理のメインページの下部にあるボタンを使って、Splunk サーバーを再起動します。アプリケーションが有効になります。

Splunk WebでSplunkデスクトップを無効にする

Splunk デスクトップを無効にすると Splunk は標準デプロイメントに戻ります。これにより、インデックスやスループットに対するすべての制限が削除されます。また、Splunk は、メモリや処理能力の使用量が元に戻ります。

1. Splunk Web へログインします。
2. **管理**をクリックして、**App 管理**タブを選択し、この本 Splunk ホストにインストールされている Apps をクリックします。
3. 該当する SplunkDesktop を探してクリックします。**有効**ドロップダウンリストから False を選択します。
4. 管理のメインページの下部にあるボタンを使って、Splunk サーバーを再起動します。アプリケーションが無効になります。

CLIでSplunkデスクトップを有効にする

CLI で Splunk デスクトップを有効にする

```
./splunk enable app SplunkDesktop -auth <username>:<password>  
./splunk restart
```

CLIでSplunkデスクトップを無効にする

CLI で Splunk デスクトップを無効にする

```
./splunk disable app SplunkDesktop -auth <username>:<password>  
./splunk restart
```

Splunk の初回起動

Splunk の初回起動

Splunkの初回起動

Splunk の起動

Windows の場合、コマンドラインまたは Windows サービスマネージャーを用いて Windows 上の Splunk を起動します。このセクションで後述するコマンドラインを用いた方法を使うとより多くのオプションが指定できます。cmd 画面で C:\Program Files\Splunk\bin に移動して以下を入力します。

```
splunk start
```

(Windows ユーザーで、Splunk がデフォルトロケーションにインストールされている場合は、後述の例および情報で、\$SPLUNK_HOME を C:\Program Files\ と置き換えます)。

UNIX の場合、Splunk コマンドラインインターフェース(CLI)を使用します。

```
$SPLUNK_HOME/bin/splunk start
```

Splunk は次にライセンス契約書を表示し、起動手順を続ける前に同意するよう促します。

その他の起動オプション

初めて Splunk を起動するときにライセンス同意を自動で行うには、start コマンドに accept-license オプションを追加します。

```
$SPLUNK_HOME/bin/splunk start --accept-license
```

起動時に以下が表示されます。

```
Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
Verifying configuration. This may take a while...
Finished verifying configuration.
Checking index directory...
Verifying databases...
Verified databases: _audit, _blocksignature, _internal, _thefishbucket, history,
main, sampledata, Checking index files
All index checks passed.
All preliminary checks passed.
Starting splunkd...
Starting splunkweb...
Splunk Server started.
The Splunk web interface is at http://<hostname>:8000
If you get stuck, we're here to help. Feel free to email us at
'support@splunk.com'.
```

注意: デフォルトポートが使用中(または使用できない)場合、Splunk は次に利用可能なポートの使用を提示します。このオプションを受諾する、または Splunk が使用するポートを指定できます。

その他に、no-prompt と answer-yes の start オプション 2 種類があります。

- `$SPLUNK_HOME/bin/splunk start --no-prompt` を実行する場合、Splunk は、質問に答えて頂く必要が発生するまで起動を続けます。その後、終了する理由を訊く質問が表示され、終了します。
- `SPLUNK_HOME/bin/splunk start --answer-yes` を実行する場合、Splunk は、起動を続けイエス/ノーで答える質問全てに「イエス」と自動的に回答します。Splunk は引き続き質問と答えを表示します。

すべてのオプションを 1 行で指定して起動する場合は、以下のようになります。

```
$SPLUNK_HOME/bin/splunk start --answer-yes --no-prompt --accept-license
```

Splunk はライセンスへの同意を尋ねません。

Splunk はイエス/ノーで答える質問すべてに「イエス」と回答します。

Splunk はイエス/ノー以外で答える質問に遭遇した場合は、終了します。

個々のプロセスの開始と無効化

start コマンドにオブジェクトとしてプロセスを加えることによって、個々の Splunk プロセスを開始または停止できます。オブジェクトには以下が含まれます。

- splunkd、Splunk サーバーデーモン
- splunkweb、Splunk のウェブインターフェースプロセス
- watchdog、シャットダウン時に splunkd を再起動するキープアライブ・プロセス。splunkd pid が存在しないことに気付くと、splunkd の再起動を 3 回まで試みます。このオプションは Windows では機能しません。代わりに、サービスマネジメントコンソールにリカバリオプションを設定します。

例：splunkd のみを起動する場合

```
$SPLUNK_HOME/bin/splunk start splunkd
```

splunkweb を無効する場合

```
$SPLUNK_HOME/bin/splunk disable webserver
```

または、Splunk watchdog を起動する場合

```
$SPLUNK_HOME/bin/splunk start watchdog
```

watchdog のシャットダウンには、以下のコマンドを使用します。

```
$SPLUNK_HOME/bin/splunk stop watchdog
```

start に関する詳細は、以下の CLI のヘルプページを参照してください。

```
$SPLUNK_HOME/bin/splunk help start
```

3.4.x 以前のバージョンからの移行

4.0 版に移行す際の留意点

4.0版に移行する際の留意点

このトピックは、3.4x 以前のバージョンから 4.0 版に移行する前に検討すべき問題や留意点について解説します。自動的に移行されないデプロイメントの特徴、手動で行わなければならない変更さらにマイグレーションスクリプトが処理する変更などの情報が掲載されています。

注意: 3.4x 以前のバージョンから移行する際は、まず初めに使用中のバージョンを 3.4x 版に移行するための資料に従い、それから移行を行って下さい。4.0 版への移行は 3.4 版からのみサポートしています。

移行する前に、既知問題に関する補足情報もご覧ください。

3.4.x版Splunkユーザーの検討すべき事項とサポート

Splunk 4 は、性能と柔軟性において飛躍的に向上していますが、3.4.x 版から更新する場合に留意しなければならない相互作用変化がいくつかあります。また、更新せずに次のバージョンのリリースを待つこともできます。以下は、Splunk 4 の導入により変更された機能の説明です。

Live テール

- Splunk 4 の著しく改良された検索およびインデック速度に加え、中間検索結果を提供する機能により、ほぼリアルタイムでデータを表示するために個別のライブイベントのコンソールを持つ必要がなくなりました。反面、3.4.x 版の「Live テール」機能に依存するケースがある場合は、Splunk 4 へのアップグレードを待つこともできます。弊社の製品計画では、より大量のデータフローを全域に、さらに分散環境を全域にもたらすライブテール機能の再建築が予定されています。さらに、今後のアーキテクチャ変更の結果に伴い今後改善されるリアルタイムアラートとダッシュボードアップデートにもご注目ください。

カスタムフィールドアクション

- 顧客意見を基に、この機能の再建築を取り決め、柔軟性を改善しさらに複数フィールドを基にしたイベントアクションを可能にします。極めて近い将来にリリースされる 4.x 版に再び盛り込まれる機能としてご期待ください。この機能を使用し、さらにアップグレードを希望する場合は、代わりに外部データベースおよび一覧からデータを Splunk に割り当てる Splunk 4 の新しい「ダイナミックフィールドドックアップ」機能をご検討ください。

スナップショット

- Splunk 4 では、個々の検索に対してタイムラインスナップショットを撮る 3.x 版の性能がさらに改良されています。Splunk 4 の新しいジョブマネージャーは、すでに検索された結果からレポートを含むすべてのキャッシュ検索結果を回収できるようになりました。是非お試しください。

イベントスクローリング

- Splunk 4 では、検索中でも実行可能な新規ページセクターで結果間を自由に移動できる柔軟性が付加されています。引き続きスクロールバーを使用する場合は、今後の 4.x 版リリースにおいてオプション機能として再び盛り込まれる予定です。

タイムラインとタイムスタンプの相互作用

- Splunk 4 では、タイムイランを改良し、ユーザーが検索を再実行する必要なく、検索結果を任意の時間範囲で即座に見れるようにしました。さらに、タイムラインの「ズームイン」をクリックすると、時間範囲を固定して検索を続行する指定が可能です。
- さらに、タイムスタンプのクリック、タイムラインバーのダブルクリックなど、3.4.x 版機能の使いやすさを今後の 4.x 版リリースに向けて改善する予定です。

クローल

- クロールは UI から設定できなくなりましたが、検索コマンドとして引き続きご利用頂けます。顧客からの意見を基に、より簡単かつ効果的にご利用頂くため、この機能の再建築を取り決めました。機能改善と、今後のリリースで紹介される予定の新しいユーザーインターフェースにご期待ください。

FIFO 入力

- この入力タイプは、Splunk 4 よりサポート保証されなくなりました。したがって、データ損失の懸念からベストプラクティスとしての使用はお勧めしません。現在この入力タイプを活用されている場合は、Splunk が監視するフラットファイルへ出力を書き込むことをご検討ください。

移行の準備が整い、アシスタントが必要である場合は当社までお知らせください。

ライセンスの移行

Splunk 4.x 版は旧リリースのライセンスでは機能しません。

- 4.0 または 4.0.1 に移行すると、**インストール後、使用のライセンスは無効ですと伝えるメッセージが表示されます。**
- 現在、エンタープライズをご利用の方は、Splunk.com の注文ページで更新ライセンスをご確認ください。
- 4.0.2 版に移行すると、Splunk 4 を起動する際に 3.x 版のライセンスをバックアップして、エンタープライズ評価用ライセンスに置き換えます。
- x 版の無料ライセンスまたはエンタープライズライセンスで実行すると、Splunk 4.x 版を起動する前に `$SPLUNK_HOME/etc/splunk.license` **ファイルが削除されます。**その後、インスタンスが 60 日間有効のエンタープライズ評価用ライセンスを取得します。

初めて実行する前にライセンスをプレシード

4.0.2 版から、デフォルトにより Splunk を初めて実行する際、既存するすべての 3.x ライセンスをバックア

アップして、仮エンタープライズ評価用ライセンスに置き換えます。これにより、新しいライセンスがコピーされるまで期限切れになることなく新しいバージョンの Splunk が使用できるようになります。

Splunk 4.0.2 版以降のバージョンに移行し、有効な 4.x ライセンスを取得すると、ライセンスファイルをプレシードすることができ、Splunk 4 を初めて起動する際、新しいライセンスを取り込んでインストールされます。これにより、各マシンで Splunk を起動した後、新しいライセンスを手動でコピーする必要がなくなるため、特に複数のインスタンスをデプロイするときに非常に便利です。

- 4.0.2 版以降のバージョンに移行した後は、すぐに Splunk を起動しないでください。
- 新しいライセンスを \$SPLUNK_HOME/etc/splunk-user.license へコピーします。
- Splunk を起動します。

デプロイ可能なパッケージを作成している場合、他のシステムへデプロイメントするように複数のファイルを 1 つのファイルにまとめたり、ファイルを zip 形式で圧縮したりする前に更新したライセンスが付いた splunk-user.license ファイルをその中に含めることができます。

移行に適したバージョンはどれか？

3.x 版デプロイメントを用途に合わせてカスタマイズしていない場合は、Migrate on Windows または Migrate on UNIX と呼ばれる**自動移行プロセス**を活用できる場合があります。

3.x 版デプロイメントをある程度カスタマイズしている場合は、(特に、deployment.conf をカスタマイズしている場合)、手動によるデプロイメントの移行を検討する必要がある場合があります。その場合は、Splunk 4.x への手動移行を行う指示に従ってください。

移行されないアイテム

Splunk 4.x は、以前のバージョンと著しく異なります。そのため、3.x 版デプロイメントの設定ファイルには移行せずに新しい 4.x 版インストールにコピーされるものがあります。ただし、既存のデプロイメントの一部は移行されず、再構築が必要な場合があります。これは、特に 3.x 版のデプロイメントおよび設定が大幅にカスタマイズされている場合に関係します。

Splunk Web 表示のカスタマイズ

Splunk Web についてあらゆるものが再構築され新たに形成されました。その結果、Splunk Web 表示に反映させたカスタマイゼーションのすべてを移行することができなくなりました。つまり、4.x アーキテクチャおよびツールを用いて再構築する必要があります。下記はそのリストです。

- フォームサーチ
- フィールドアクション(field_actions.conf)
- ダッシュボード
- UI プリファレンス(prefs.conf)
- 保存した検索のレポートチャートとテーブルプリファレンス
- UI ストリングへ変更(literals.conf)

アプリケーションに関する留意点

通常、アプリケーションは移行されません。したがって、アプリケーションを再構築して、4.0 版の新しいアーキテクチャに追従する必要があります。4.0 版のアプリケーションに関する詳しい情報は、開発マニュアルを参考してください。アプリケーションの移行に関するより詳しいガイダンスについては、開発マニュアルの 3.x 版 apps の移行に関するトピックを参照してください。

Splunk 3.4.x 版のすべてのアプリケーションが 4.0 版で即座に利用できるとは限りません。新しいアプリケーションは入荷次第すぐに Splunk App Store に追加されます。

Splunk の PCI コンプライアンスと Splunk の変更管理は、今現在 Splunk 4 ではご利用頂けません。このいずれかのアプリケーションを持っている場合は、更新する前にサポートに連絡する、または Splunk のパラレル・インスタンスをインストールして維持することをご検討ください。

デプロイメントサーバーとフォワーダの留意点

Splunk デプロイメントサーバーを使用する際は、必ず 4.x 版の新しいデプロイメント・サーバー・アーキテクチャを使ってデプロイメント・コンフィギュレーションを再構築する必要があります。つまり、移行はできません。3.x 版の `deployment.conf` に変更を加える場合は、新しくインストールした Splunk 4.x 版にコピーしないでください。新しいデプロイメント・サーバー・コンフィギュレーションを構築するためのベースとして使用してください。

その間、3.4.x 版のデプロイメントサーバーとクライアントを持ち、現時点ですべてのクライアントを移行しない場合は、このトピックの指示に従って、必要最低限のものだけ備えた 3.4.x 版デプロイメント・サーバーを設定して、デプロイメント・クライアントを引き続き管理します。

フォワーダをデプロイした場合は、4.x 版に後で移行することが可能です。つまり、**3.3.x 版フォワーダは Splunk の 4.x 版で機能します**。特にこれは大型フォワーダデプロイメントに役立ちます。4.x にフォワーダを移行する前に新しいデプロイメント・サーバー・コンフィギュレーションに慣れるまでのお時間を持つことができます。

3.x版のクライアントを4.0版または4.0.1版Splunkインスタンスと併用するとクライアントがクラッシュする

4.0.2 版でこの問題は解決されました。

4.x 版サーバーが既存の 3.x 版デプロイメント・クライアントに接触しないことを確かにするために、4.x 版インスタンスの管理ポートを変更します。下記を `$SPLUNK_HOME/etc/system/local/web.conf` に加えて、デフォルト番号 8089 ポートから 8090 に変更します。

```
[settings]
mgmtHostPort = 127.0.0.1:8090
```

重要: 4.x 版のフォワーダは、3.x 版のデプロイメント・サーバーには機能しません。

手動で移行するアイテム

Splunk 4.x 版は 3.x 版とは著しく異なり、マイグレーションスクリプトは一部の設定ファイルのコンテンツ

を変換しません。このセクションは、手動で変更するいくつかのアイテムについて記述します。

スケジュール検索とアラートの留意点

スケジュール検索とアラートは、自動的に移行されません。4.0 版のナレッジモデルでは、アプリケーションコンテキスト以外で検索は実行できません。したがって、保存されている検索は検索アプリケーションの一部と見なされます。つまり、それらはすべて apps に受け渡され、グローバルまたは表示はできません。

保存済み検索を移行する場合

1. Splunk の停止 : コマンドを実行します。

```
$SPLUNK_HOME/bin/splunk stop
```

2. \$SPLUNK_HOME/etc/system/local/savedsearches.conf を

\$SPLUNK_HOME/etc/apps/search/local/ に移動します。

3. "savedsearches/" で始まる名前のすべてのスタanzas を

\$SPLUNK_HOME/etc/system/metadata/local.meta から

\$SPLUNK_HOME/etc/apps/search/metadata/local.meta に移動します。

4. Splunk の開始 : コマンドを実行します。

```
$SPLUNK_HOME/bin/splunk start
```

タグとエイリアスの留意点

ソースタイプの名前変更は、「ソースタイプエイリアシング」を置換し、タグで実装されません。詳しい情報は、ナレッジマネージャマニュアルの「タグとエイリアスについて」を参照してください。エイリアスされたソースタイプに依存した保存済み検索は移行しないと機能しません。保存済み検索の移行手順については、スケジュール検索およびアラートに関する移行の留意点をご覧ください。

crawl.confに関する留意点

crawl.conf スタanzas[file_crawler]は、[files]に名前を変更する必要があります。自動変更されません。

CLIに関する移行に問題なし

Splunk 4.x 版のコマンドインターフェイスラインの(CLI)は、完全に書き換えられています。移行に関する既知問題や、過去の互換性問題は報告されていません。CLI への変更をまとめたリストに関するリリースノートを参考にしてください。それには、将来サポートが保証されない CLI コマンドオプションや新機能が含まれます。

自動移行中に発生する変更

移行中、多くの設定ファイルの単純にコピーされるわけではありません。Splunk はこれらのファイルのコンテンツを変換および移行するためのスクリプトを提供し、4.x 版で正確に機能することを確認します。移行プレビューユーティリティを実行して、実際に更新および移行する前に変更される内容を確認すること

ができます。下記は移行の際に発生する変更の一部リストです。

alert_actions.conf

この設定ファイルは、savedsearches.conf により移行されます。

indexes.conf

移行中、いくつかの属性は indexes.conf へ追加されます。一方その他のローカル属性は削除またはグローバル・パラメータへと変更されます。関連パラメータについての詳細は、管理マニュアル内の indexes.conf を参考してください。

下記の属性へのサポートは中止されますので機能しなくなります。

- `_actions`
- `maxTermChars`
- `maxTerms`
- `maxPostings`
- `maxValues`
- `waitForOptimize`

下記のグローバル属性は記述するデフォルトを基に追加されます。

- `indexThreads = auto`
- `maxMemMB = 5`
- `memPoolMB = auto`
- `maxHotSpanSecs = 7776000`
- `maxHotIdleSecs = 0`
- `maxHotBuckets = 1`
- `quarantinePastSecs = 77760000`
- `quarantineFutureSecs = 2592000`

大量インデックス(main など)には、下記のデフォルトを使用します。

- `maxHotBuckets = 10`
- `maxHotIdleSecs = 86400`
- `maxMemMB = 20`

savedsearches.conf

移行中、フォーム検索は無効になり、デフォルトのグローバル・ビューステートがセットされ、オーナー属性が移動されることにより 4.0 版の役割と権限モデルに対応します。

- `search` 属性がマクロ(`$<strings>$`)を含む場合は、`disabled = 1` がスタンザに加えられます。
- 属性が、`"viewstate."`から始まるラインのビューステート`&mdash`を定義する場合は、そのラインは

コメントアウトされます。

- スタンザが 'userid' および/または 'role' 属性を含む場合は、相当する metadata owner/ACL が追加されます。

server.conf

移行中、下記の属性が splunkd.xml から server.conf へと移動されます。

- minFreeMb
- pollingFrequency
- serverName

サーバー許可、キーファイル、パスワードに対して下記の属性が名付けられます。

- keyfile は、sslkeyfile に置き換えられる
- keyfilepassword は、sslkeyfilePassword に置き換えられる

Windows専用のconfファイル

移行中、Windows 専用のファイル(regmon-filters.conf, sysmon.conf, and wmi.conf)およびナレッジオブジェクトはデフォルトから Windows アプリケーションアーキテクチャへと移動されます。

削除されるconfファイル

移行中、下記の conf ファイルが削除されます。

typedefs.conf
searchdata.conf

UNIX における移行

UNIXにおける移行

4.0 版への移行時には、設定ファイルが更新され変更されます。移行プレビューユーティリティを実行して実際に更新および移行する前に変更される内容が確認できます。その際、スクリプトが提案する変更を含むファイルが下記に書き込まれます。

```
$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>
```

移行の前に

移行する前に、移行に関する留意事項を検討し、Splunk の設定、データ、バイナリーを含むすべてのファイルをバックアップすることを強くお勧めします。Splunk では、前のバージョンにダウングレードする方法を提供しません。つまり、旧 Splunk リリースへ戻したい場合は、再インストールしか方法がありません。

移行の仕方

1. `$(SPLUNK_HOME)/bin/splunk stop` コマンドを実行します。
2. 既存の Splunk パッケージを既存の Splunk デプロイメントヘインストールします。

TAR ファイルを使用する場合は、既存の Splunk インスタンスと同じディレクトリへそれを拡張してください。これにより一致するファイルを上書きし置き換えますが、固有のファイルは削除されません。

RPM などのパッケージマネージャーを使用する場合

```
rpm -U splunk_package_name.rpm
```

3. `$(SPLUNK_HOME)/bin/splunk start` コマンドを実行します。

下記の出力が表示されます。

```
This appears to be an upgrade of Splunk.
```

```
-----  
Splunk has detected an older version of Splunk installed on this machine. To  
finish upgrading to the new version, Splunk's installer will automatically  
update and alter your current configuration files. Deprecated configuration  
files will be renamed with a .deprecated extension.
```

```
You can choose to preview the changes that will be made to your configuration  
files before proceeding with the migration and upgrade:
```

```
If you want to migrate and upgrade without previewing the changes that will be  
made to your existing configuration files, choose 'y'.
```

```
If you want to see what changes will be made before you proceed with the  
upgrade, choose 'n'.
```

```
Perform migration and upgrade without previewing configuration changes? [y/n]
```

4. 移行プレビュースクリプトを実行して既存の設定ファイルに変更される内容を確認する、または移行およびアップグレードを実行するの選択ができます。
5. 変更内容の確認を行う場合は、スクリプトで一覧が表示されます。
6. 変更内容を確認し、移行およびアップグレードを実施する準備ができたなら、再び `$(SPLUNK_HOME)/bin/splunk start` を実行します。

注意: ステップ 3 から 5 までを 1 行で記述できます。

アップグレードを実施する前にライセンスの同意と変更内容を確認する(回答'n')場合

```
$(SPLUNK_HOME)/bin/splunk start --accept-license --answer-no
```

変更内容を確認せず(回答'y')にくラインセンスに同意してアップグレードを開始する場合

```
$(SPLUNK_HOME)/bin/splunk start --accept-license --answer-yes
```

Windows における移行

Windowsにおける移行

移行すると、設定ファイルはアップグレードおよび変更が行われ、新しい機能をサポートします。移行プレビューユーティリティを実行して、実際にアップグレードおよび移行する前に変更内容を確認することがで

きます。その際、スクリプトが提案する変更を含むファイルが下記に書き込まれます。

```
$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>
```

移行の前に

- 「4.0 版へアップグレードする際の留意点」の移行に関する注意事項を確認してください。
- **Splunk の設定、データ、バイナリーを含むすべてのファイルをバックアップします。**
- Windows のスタートメニューオプションまたは `$SPLUNK_HOME/bin/splunk stop` コマンドを実行して Splunk を停止します。
- 更新中は Splunk を実行するユーザーを変更することができませんのでご注意ください。Windows のサービスコントロールパネルでもユーザーは変更しないでください。変更すると、Splunk の機能が停止します。ユーザーを変える必要がある場合は、Splunk をアンインストールしてから再インストールする必要があります。
- Windows App は、4.0 から 4.0.2 版においてデフォルトで有効です。4.0.3 版からは、コマンドライン/MSI インストールプロセスを通して明白に有効にしない限りデフォルトでは無効です。

説明書のアップグレード

1. Splunk ダウンロードページで新規 MSI ファイルをダウンロードします。
2. MSI ファイルをダブルクリックします。

歓迎画面が表示されます。画面上の指示に従って Splunk をアップグレードします。

各画面に関する詳細は、インストールマニュアルを参考してください。

インストールの直前に、このアップグレードで変更される内容をプレビューできるオプションが表示されます。

3. 必要に応じてアップグレードおよび移行内容をプレビューしてください。

下記のテキストが表示されます。

```
This appears to be an upgrade of Splunk.
```

```
-----  
Splunk has detected an older version of Splunk installed on this machine. To  
finish upgrading to the new version, Splunk's installer will automatically  
update and alter your current configuration files. Deprecated configuration  
files will be renamed with a .deprecated extension.
```

```
You can choose to preview the changes that will be made to your configuration  
files before proceeding with the migration and upgrade:
```

```
If you want to migrate and upgrade without previewing the changes that will be  
made to your existing configuration files, choose 'y'.
```

```
If you want to see what changes will be made before you proceed with the  
upgrade, choose 'n'.
```

```
Perform migration and upgrade without previewing configuration changes? [y/n]
```

4. 移行プレビュースクリプトを実行して既存の設定ファイルで変更される内容を確認する、または移行およびアップグレードを実行するかの選択ができます。
5. 変更内容の確認(N を選択)を行うと、スクリプトが一覧を表示します。

スクロールアップして変更を確認するまたは

`$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>`で見ることができます。リストの最後にエラーメッセージが表れますが、無視してください。

6. **Enter** を押して、ステップ 3 へ戻る、または **Y** を入力して更新を終了します。

重要: 移行またはアップグレードする際は、Splunk を実行するユーザーを必ず再指定してください。この情報は、リリースが発生する都度、自動的に維持されません。

Splunkの起動

Windows の場合、Splunk はデフォルトで `\Program Files\Splunk` へインストールされます。

Windows サービスマネージャーから次の Splunk プロセスを起動/停止できます。

- Splunk サーバデーモン: `splunkd`
- Web インターフェイス: `splunkweb`

さらに、`\Program Files\Splunk\bin` に下記を入力すると、即座に両プロセスを起動、停止、再起動します。

```
# splunk.exe [start|stop|restart]
```

注意: Splunk サービスの開始を選択しないと、手動スタートアップに設定され、再起動の後スタートしなくなります。必ず Windows Service Manager MMC から開始し、ブート時の際に自動的にスタートを希望する場合は `auto-start` を設定してください。

重要: アップグレードの後、Splunk は、いくつかのファイルをバイナリーとして誤って読み始めることがあります。ソーススタanzaに下記のラインを加えると、`props.conf` 内の動作を上書きできます。

```
NO_BINARY_CHECK = true
```

Splunk 4.x に手動で移行する手順

Splunk 4.xに手動で移行する手順

このトピックは、Splunk 3.x を手動で 4.x バージョンに移行する手順を説明します。始める前に、必ず本書の「4.0 版へアップグレードする際の留意点」をお読みください。

3.x 版デプロイメントをカスタマイズしていない場合は、Migrate on Windows または Migrate on UNIX と呼ばれる自動「インプレース移行プロセス」を利用できる場合があります。特に `deployment.conf` をカスタマイズしていない場合は、自動移行プロセスを使える可能性があります。

カスタム設定のいくつかは全く移行されないため、新しい Splunk のフレームワーク内に再構築されなければなりません。さらに詳しい情報は、このトピックの「移行されないアイテム」および本書の「4.0 版へアップグレードする際の留意点」を参考してください。

手動移行プロセスの概要

手動操作では、既存デプロイメントのバックアップコピーを作成し、3.xとは別のパスで Splunk 4.x をインストールし、その後、3.x デプロイメントからデータや設定ファイルを移行します。この操作は、ダウンタイムを最小限に抑えることを念頭にデザインされています。

この操作には細心の注意が必要です。Splunk 4.x は 3.x バージョンとは著しく異なるため、多くの設定ファイルは単純にコピーできません。Splunk はこれらのファイルのコンテンツを変換および移行するためのスクリプトを提供し、確実に 4.x 版で正しく機能するよう確認しています。

操作する前にこのトピック全文をお読みください。そうすれば、操作による影響を理解し、それに適した計画が行えます。

移行されないアイテム

前述のとおり、Splunk 4.x は、旧バージョンと著しく異なります。既存デプロイメントの一部は移行されないため、再構築する必要があります。

Splunk Web表示のカスタマイズ

Splunk Web についてあらゆるものが再構築され、新たに形成されました。その結果、Splunk Web 表示に反映させたカスタマイゼーションのすべてを移行することができなくなりました。つまり、4.x アーキテクチャおよびツールを用いて再構築する必要があります。下記はそのリストです。

- フォーム検索
- フィールドアクション(field_actions.conf)
- ダッシュボード - 再構築の方法についての説明はここからご覧になれます。
- UI プリファレンス(prefs.conf)
- 保存済み検索のレポートチャートとテーブルプリファレンス
- UI スtringへ変更(literals.conf)
- 3.x Apps - 再作業のガイダンスはディベロッパーマニュアルのトピックをご覧ください。

デプロイメントサーバーとフォワーダに関する留意点

- Splunk デプロイメントサーバーを使用する場合は、移行ができないため、4.x で新しいデプロイメントサーバーのアーキテクチャを再構築する必要があります。3.x で deployment.conf を変更している場合、それを 4.x にコピーしてはいけません。別の場所に保存して、新しいデプロイメントサーバーの設定のベースとしてお使いください。
- フォワーダをデプロイメントした場合は、4.x への移行を遅らせて、3.x のフォワーダを 4.x で機能するようにできます。これは、大量のフォワーダデプロイメントを行う際に便利です。4.x にフォワーダを移行する前に新しいデプロイメント・サーバー・コンフィギュレーションに慣れるまでのお時間を持つことができます。
- バージョン 4.x フォワーダは、バージョン 3.x デプロイメントサーバーでは機能しません。

移行を開始する前に

Splunk データおよび設定ファイルを移行する前に、3.x のバックアップコピーを作成します。もっとも簡単な方法は、Splunk CLI diag ユーティリティを実行し、すべてのインストールを含んだ圧縮(.tar)ファイルを作成します。実行するには、\$SPLUNK_HOME/bin から下記を入力します。

UNIX の場合

```
./splunk diag
```

Windows の場合

```
splunk diag
```

使用環境で diag の実行が困難な場合は、cmd コマンドを用いて直接 python スクリプトを実行します。

```
./splunk cmd python /opt/splunk/lib/python2.5/site-packages/splunk/clilib/info_gather.py
```

これにより、splunk-diag.tar.gz|zip が作成され、3.x のデプロイメントのバックアップとして維持されます。

これが終了したら、本書の手順に従って、3.x がインストールされている場所とは異なるプラットフォームに 4.0 バージョンをインストールします。ただし、すぐには起動しないでください。

4.x Splunk インスタンスはしばらく起動しないでください。

手動による移行を必要としない設定ファイルのインポート

3.x 版デプロイメントの一部の設定ファイルは移行する必要なく、新しい 4.x 版インストールへとコピーされます。

これらのファイルを \$SPLUNK_HOME/etc/system/local から及び同様へ、さらに custom config ディレクトリからコピーすることを忘れないでください。/default にはコピーしないでください。

- deployment.conf を除くすべての設定ファイルをコピーします。
- 新しい 4.x Splunk インスタンスに含める inputs.conf のコピーを編集して、すべての入力を disabled=true に設定します。

ユーザーとパスワード情報のインポート

この時点で、以下からユーザーデータ、パスワード、認証情報を取得できます。

- authentication.conf
- authorize.conf
- splunk.secret
- passwd file

4.x Splunk インスタンスはしばらく起動しないでください。

Splunkインデックスデータの移行

このセクションは、新しくインストールされた 4.x を設定して既存の Splunk インデックスデータを読み込む方法について説明します。旧データは再インデックスされない限り(全員にオプションとされていない)、古いデータを検索しても 4.x 大幅な性能改善を体感できない場合があります。ただし、4.x バージョンへ移行後にインデックスしたデータはすべて、性能改善をサポートしています。

繰り返しますが、ダウンタイムやデータ損失を最低に抑えるために細心の注意を払って指示に従ってください。順序は大事です！また、**迅速に連続して各ステップを実行する準備**をしてください。既存の Splunk デプロイメントで”hot”インデックスデータディレクトリを”warm”へとデプロイメントしたら、素早く次のステップに進み、ダウンタイムを最低限に抑え、新しくインストールした 4.x 版 Splunk でインデックスを始めてください。

Splunk Community Wiki に掲載されている「バックアップのベストプラクティス」を参照し、“hot”および”warm”インデックスディレクトリについて理解を深めてください。

1. 4.x をインストールしたルートディレクトリで、splunk-launch.conf を編集し、SPLUNK_DB 値が 3.x デプロイメントのインデックスデータディレクトリを示すようにします。デフォルトで、この値は /opt/splunk/var/lib/splunk ですが、3.x でデプロイメントの splunk-launch.conf を確認して、正しいパスであるか確認してください。
2. 次に、3.x デプロイメントで、CLI を使って hot インデックスデータディレクトリのすべてのデータローテーションを warm ディレクトリに強制します。これを行うには、以下を入力します。
 - `./splunk search ' | oldsearch !++cmd++::roll' -auth splunk`
 - ◆ 直後に「Hot db が warm へ移行したため、検索実行に失敗しました。」というエラーが表示されますが、無視してください。また、この CLI コマンドを実行するには管理パスワードが必要です。
 - ◆ 現在書き込み中の他のインデックスをローテーションする場合は、以下を使用します。
 - ◆ `./splunk search ' | oldsearch index=<INDEX_NAME> !++cmd++::roll' -auth admin:<ADMIN_PASSWORD>`
3. すべてのインデックスを“hot”から”warm”にローテーションすると、直後に 3.x デプロイメントがシャットダウンされ、4.x のインストールが始ります。4.x を起動すると、コピーした一部の設定ファイルは、自動移行プロセスをたどります。Splunk は、初めて 4.x をスタートするときのこのプロセスに関する情報を表示します。
4. 可能な限り速やかに、新規インストールした 4.x にログインし、確実に 3.x インデックスにあるデータを検索して、すべての移行手順を検証します。新規のデプロイメントが検索を実行し、3.x インデックスのデータを検索できることを確認します。検証に失敗した場合は、トラブルシューティングを行う前に、即座に 3.x デプロイメントを再起動してください。
5. 4.x デプロイメントが 3.x インデックスデータを検索できることが検証できたら、即座に inputs.conf を編集して、入力に disabled=false を設定し、4.x Splunk デプロイメントを再起動して有効にします。そのデータが新規デプロイメントに送られうことを確認します。

これで、新しい 4.x Splunk デプロイメントの使用準備が整いました。

分散検索の使用

分散検索を設定する場合は、必ず新しいキーをすべての検索ピアに配布して、4.xにて分散検索を使用します。このキーは、分散検索が有効の場合に、スタートアップの時点で作成されます。

キーは、`$SPLUNK_HOME/etc/auth/distServerKeys/`に作成されます。

`$SPLUNK_HOME/etc/auth/distServerKeys/trusted.pem` と `private.pem` ファイルをひとつのホストから分散検索ピアの全員に配布します。

4.0 以降からのアップグレード

Windows 上の Splunk のアップグレード

Windows上のSplunkのアップグレード

このトピックは、Windows Splunk インスタンスをバージョン 4.x から最新バージョンにアップグレードする手順を説明します。GUI インストーラーを活用して、または「コマンドライン経由の Windows へのインストール」の説明に従ってコマンドラインで `msiexec` を実行してアップグレードできます。

注意: 4.0 から 4.0.2 のバージョンでは、Windows App は、`app.conf` ファイルでデフォルトで有効に設定されていました。4.0.3 版から、このファイルでデフォルトで無効に設定されています。以下の重要情報をお読みください。

- ◆ 4.0 から 4.0.2 のバージョンを 4.0.3 以降のバージョンにアップグレードすると、Windows App は更新前有効も無効にします。
- ◆ 4.0.3 以降のバージョンを新規にインストールすると、Windows App はデフォルトで **MSI 経由** で有効に設定されます。無効でインストールする場合は、`SPLUNK_APP msiexec` コマンドを使用して「コマンドラインを使った Windows へのインストール」の説明に従って指定します。

更新の前に

重要: アップグレードする際は、必ず初回インストールで指定したユーザーと同じドメインユーザーを指定してください。同じユーザーを指定しないと、Splunk はローカルシステムユーザーをデフォルトにします。インストールの際に誤ったユーザーを指定してしまった場合は、Splunk を起動する前に本書の指示に従って正しいユーザーに訂正してください。

重要: アップグレードする前に、Splunk の設定、データ、バイナリーを含むすべてのファイルをバックアップすることを強くお勧めします。**Splunk は、前のバージョンにダウングレードする方法を提供しません。**つまり、旧 Splunk リリースへ戻したい場合は、再インストールしか方法がありません。

GUIインストーラを使ったアップグレード

1. Windows のスタートメニュー・オプションまたは `$SPLUNK_HOME/bin/splunk stop` コマンドを実行して Splunk を停止します。
2. Splunk ダウンロードページから新しい MSI をダウンロードします。
3. MSI ファイルをダブルクリックします。歓迎画面が表示されます。画面上の指示に従い、Splunk をアップグレードします。各画面に関する詳細は、インストール説明書を参考してください。
4. インストールが完了すると、デフォルトで Splunk が起動されます。

アップグレード中の設定ファイルに対する変更ログは `$TEMP$` に保存されます。

コマンドラインを使ったアップグレード

1. Windows のスタートメニュー・ オプションまたは `$SPLUNK_HOME/bin/splunk stop` コマンドを実行して Splunk を停止します。
2. Splunk ダウンロードページから新しい MSI をダウンロードします。
3. 「コマンドライン経由で Windows にインストール」の手順に従います。Splunk をローカルシステムユーザー以外で実行する場合は、必ずコマンドラインにこのユーザーを指定してください。この時点でポート(SPLUNKD_PORT および WEB_PORT)を変更できます。また、LAUNCHSPLUNK オプションを使って完了時に Splunk を自動的にスタートするかどうかの指定ができます。他の設定は変更できません。
4. マシンの仕様により、インストール完了時に Splunk を自動的に起動する場合があります。

アップグレード中の設定ファイルに対する変更ログは `$TEMP$` に保存されます。

Splunkの起動

Windows の場合、Splunk はデフォルトにより `\Program Files\Splunk` にインストールされて起動されます。

Windows サービスマネージャーで次の Splunk プロセスを起動および停止できます。

- ◆ サーバプロセス: `splunkd`
- ◆ Web インターフェースプロセス: `splunkweb`

さらに、`\Program Files\Splunk\bin` に以下を入力すると、一度に両プロセスを起動、停止、再起動します。

```
# splunk [start|stop|restart]
```

Linux、Solaris、FreeBSD、AIX、MacOS 上の Splunk のアップグレード

Linux、Solaris、FreeBSD、AIX、MacOS上のSplunkのアップグレード

このトピックは、バージョン 4.x からそれ以降のバージョンに Splunk インスタンスをアップグレードするための手順を記述します。

アップグレードのしくみ

アップグレードするとき、設定ファイルは、新しいバージョンのインストールを実行した後で Splunk を起動するまで変更されません。その時点で、移行プレビューユーティリティを実行して、ファイルが更新される前に変更内容を見ることができます。続行する前に変更内容を確認すると、アップグレードスクリプトが勧める変更を含むファイルが `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>` に書き込まれます。

重要: 更新する前に、Splunk の設定、データ、バイナリーを含むすべてのファイルをバックアップすることを強くお勧めします。Splunk は、前のバージョンにダウングレードする方法を提供しません。つまり、旧

Splunk リリースへ戻したい場合は、再インストールしか方法がありません。

アップグレードの手順

1. `$SPLUNK_HOME/bin/splunk stop` コマンドを実行します。
2. バージョン 4.0 以降からアップグレードおよび移行する場合は、Splunk パッケージを既存の Splunk デプロイメントにインストールします。
 - ◆ .tar ファイルを使用する場合は、既存の Splunk インスタンスと同じディレクトリへそれを拡張します。これにより一致するファイルを上書きして置き換えますが、固有のファイルは削除されません。
 - ◆ RPM などのパッケージマネージャーを使用する際は、下記を入力してください。`rpm -U splunk_package_name.rpm`
 - ◆ .dmg file (MacOS 上)を使用する場合は、それをダブルクリックして指示に従います。必ず、既存するインストールと同じインストールディレクトリを指定してください。
3. `$SPLUNK_HOME/bin/splunk start` コマンドを実行します。

下記の出力が表示されます。

```
This appears to be an upgrade of Splunk.
```

```
-----  
Splunk has detected an older version of Splunk installed on this machine. To  
finish upgrading to the new version, Splunk's installer will automatically  
update and alter your current configuration files. Deprecated configuration  
files will be renamed with a .deprecated extension.  
You can choose to preview the changes that will be made to your configuration  
files before proceeding with the migration and upgrade:  
If you want to migrate and upgrade without previewing the changes that will be  
made to your existing configuration files, choose 'y'.  
If you want to see what changes will be made before you proceed with the  
upgrade, choose 'n'.  
Perform migration and upgrade without previewing configuration changes? [y/n]
```

4. 移行プレビュースクリプトを実行して既存の設定ファイルで変更される内容を見る、または移行および更新を即座に実行するかを選択します。
5. 変更内容を見るを選択すると、スクリプトが一覧を表示します。
6. 変更内容を確認して、移行および更新の準備が整ったら、再び `$SPLUNK_HOME/bin/splunk start` を実行します。

注意: ステップ 3 から 5 までを 1 行で記述できます。

アップグレードを実施する前にライセンスに同意(回答'n')して変更予定を表示する場合

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-no
```

変更内容を表示せず(回答'y')にライセンスに同意してアップグレードを開始する場合

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-yes
```

その他のタスク

Splunk を別のまたは非ルートユーザーから実行

Splunkを別のまたは非ルートユーザーから実行

ローカルシステムのユーザーで Splunk を実行します。Splunk を非ルートユーザーで実行する場合は、Splunk に以下の適切な権限があるか確認してください。

- 観察するよう設定したファイルおよび `s` ディレクトリを読み込みます。ログファイルやディレクトリの一部はルートまたはスーパーユーザーアクセスをインデックスする必要があることがあります。
- 自分用のアラートおよびスクリプト入力を Splunk のディレクトリに書き込み、実行します。
- リッスンするネットワークポート(1024 以下のポートは、ルート専用の予備ポート)をバインドします。

注意: 1024 以下のポートはルートアクセスのみに予約されているため、ルートで実行する場合、Splunk はポート 514(syslog のデフォルトリッスンポート)のみをリッスンします。ただし、代わりに別のユーティリティ(syslog-ng など)をインストールして、syslog データをファイルに書き込み、Splunk でそのファイルを監視することが可能です。

手順

非ルートユーザーとして Splunk を実行するには、初めに Splunk を `root` としてインストールする必要があります。その後、初めて Splunk を開始する前に、`splunk` ディレクトリの所有権を希望するユーザーに変更します。下記は Splunk のインストールと非ルートユーザー `splunk` としての実行に関する説明です。

1. `splunk` をユーザーおよびグループで作成する。

Linux、Solaris、FreeBSD の場合

```
useradd splunk
groupadd splunk
```

Mac OS の場合

システム設定 > アカウント 画面を開いて、ユーザーとグループを追加します。

2. `root` として、さらにパッケージ(ターボールを除く)のひとつを用いて、インストールを実行します。

重要: Splunk はまだ起動しないでください。

3. `chown` コマンドを使って、`splunk` ディレクトリとそれに属するすべての所有権を希望のユーザーに変更します。

```
chown -R splunk $SPLUNK_HOME/
```

注意: `$SPLUNK_HOME` は Splunk のインストールディレクトリを参照します。

4. Splunk を起動します。

```
$SPLUNK_HOME/bin/splunk start
```

また、別のユーザーでログインしながら、Splunk を splunk ユーザーで起動する場合は、sudo コマンドを使用します。

```
sudo -H -u splunk $SPLUNK_HOME/bin/splunk start
```

この例のコマンドは下記を前提とします。

- Splunk が別のロケーションにインストールされた場合は、それに従ってコマンド内のパスを更新します。
- 使用システムには sudo がインストールされていません。この場合は、su を使用します。
- ターボールを使ってインストールし、Splunk をある特定のユーザー(splunk など)で実行する場合は、ユーザーを手動で作成する必要があります。
- splunk ユーザーは製品証明を生成するために `tp /dev/urandom` へのアクセスが必要です。

Solaris 10の特権

splunk ユーザーで Solaris 10 へインストールする場合は、必ず追加権限を設定して splunkd を起動し予備ポートを結合しなければなりません。

Solaris 10 上で splunk ユーザーとして splunkd を起動し実行する場合

```
# usermod -K defaultpriv=basic,net_privaddr,proc_exec,proc_fork splunk
```

splunk ユーザーに Solaris 10 上の予備ポートへ結合することを許可し実行(ルートとして)する場合

```
# usermod -K defaultpriv=basic,net_privaddr splunk
```

Splunk のアンインストール

Splunkのアンインストール

アンインストールする前に、Splunk を停止します。\$SPLUNK_HOME/bin に移動し、./splunk stop を入力します(Windows の場合は splunk stop のみ)。

ローカルパッケージ管理コマンドを利用して、Splunk をアンインストールします。ほとんどの場合、パッケージによって最初にインストールされなかったファイルは維持されます。これらのファイルにはインストールディレクトリにあるコンフィギュレーションやインデックスファイルを含みます。

注意: \$SPLUNK_HOME は、Splunk インストールディレクトリです。Windows 上ではデフォルトで、C:\Program Files\Splunk となります。Unix プラットフォームのほとんどの場合、デフォルトインストールディレクトリは /opt/splunk で、Mac OS の場合は、/Applications/splunk です。

RedHat Linux

RedHat で Splunk をアンインストールする場合

```
rpm -e splunk_product_name
```

Debian Linux

Debian で Splunk をアンインストールする場合

```
dpkg -r splunk
```

Debian 上で(コンフィギュレーションファイルを含む全てを削除) を消去する場合

```
dpkg -P splunk
```

FreeBSD

FreeBSD 上のデフォルトロケーションから Splunk をアンインストールする場合

```
pkg_delete splunk
```

FreeBSD 上の別のロケーションから Splunk をアンインストールする場合

```
pkg_delete -p /usr/splunk splunk
```

Solaris

Solaris 上から Splunk をアンインストールする場合

```
pkgrm splunk
```

Windows

Windows 上から Splunk をアンインストールする場合

コントロールパネルの**プログラムの追加と削除**オプションを使用します。

手動による Splunk のアンインストール

パッケージ管理コマンドを利用できない場合は、以下の指示に従って Splunk をアンインストールします。

注意: 以下の指示は、作成されたすべての init スクリプトを削除しません。

1. Splunk を停止します。

```
$(SPLUNK_HOME)/bin/splunk stop
```

2. 名前に"splunk"が含まれるいつまでも消えないプロセスを発見し、kill (削除)します。

Linux および Solaris の場合

```
kill -9 $(ps -ef | grep splunk | grep -v grep | awk '{print $2;}')
```

FreeBSD および Mac OS の場合

```
kill -9 $(ps ax | grep splunk | grep -v grep | awk '{print $1;}')
```

3. Splunk インストールディレクトリの\$(SPLUNK_HOME). For example を削除します。

例：

```
rm -rf /opt/splunk
```

注意: Mac OS の場合、ゴミ箱にフォルダをドラッグしてもインストールディレクトリを削除できます。

3. 存在する場合、最上ディレクトリ以外の Splunk のデータストアまたはインデックスを削除します。

```
rm -rf /opt/splunkdata
```

4. 存在する場合、splunk ユーザーとグループを削除します。

Linux、Solaris、FreeBSD の場合

```
userdel splunk  
groupdel splunk
```

Mac OS の場合:システム設定 > アカウント 画面で、ユーザーとグループを管理できます。

Windows の場合: コマンドプロンプトを開いて、msi パッケージに対してインストールした `msiexec /x` コマンドを実行します。

Windows にインストール中に選択したユーザーの訂正

Windowsにインストール中に選択したユーザーの訂正

Windows GUI インストール中に、“他のユーザー”を選択してしまい、そのユーザーが存在しない、または誤って入力してしまった場合、**Splunk をまだ開始していなければ**、Windows Service Control Manager から正しい情報を指定できます。

Windows GUI インストール段階で無効なユーザーを指定した場合は、それを伝える 2 つのポップアップエラーメッセージが表示されます。

ユーザーを変更する場合

1. コントロールパネル > 管理ツール > サービスの順に選択して、Splunkd および SplunkWeb サービスを探します。

ここで、サービスが開始されていない、および現在ローカルシステムユーザーが所有していることが分かります。

2. 各サービスを右クリックして、**プロパティ**を選択します。サービスに関するプロパティ・ダイアログが表示されます。

3. **ログオンタブ**を選択します。

4. このアカウントのラジオボタンを選択して、正しいドメイン\ユーザー名およびパスワードを入力します。

5. **適用**をクリックします。

6. **OK** をクリックします。

6. 2 つ目のサービスも同様に処理します(必ず Splunkd と Splunk Web の両方を実行して下さい)。

7. これで、Service Manager または Splunk コマンドラインインターフェースから両方のサービスが開始できます。

スタンドアロン型 3.4.x デプロイメントサーバーの設定

スタンドアロン型3.4.xデプロイメントサーバーの設定

Splunk 4.x への移行を予定しているものの、デプロイメントクライアントの移行は後で実施したい場合は、移行を決定するまで必要最低限を備えたスタンドアロン 3.4.x デプロイメントサーバーを設定して、デプロイメントクライアントに使用できます(Splunk 4.x デプロイメントサーバーは、4.x より前のバージョンのクライアントとの互換性はありません)。

この手順は下記を前提にします。

- `fflanda.splunk.com` に既存のデプロイメントサーバーを持ちし、デプロイメントクライアント用ポート番号 8089 でリッスンします。
- デプロイメントクライアントはすべて 3.x であり、このデプロイメントサーバーをポーリングします。
- デプロイメントクラスは、`$SPLUNK_HOME/etc/modules/distributedDeployment/classes` にあります。

この Splunk インスタンスもインデックスサーバーでのアップグレードが必要です。

上述を前提に、以下の手順で実施します。

1. アーキテクチャに適した最新の Splunk 3.4.x をダウンロードします。
2. `tar ?zxvf $SPLUNK_HOME/etc > /tmp/splunk_old_etc.tgz` を用いて、既存の `$SPLUNK_HOME/etc` をバックアップします。
3. Splunk を停止し、`deployment.conf` およびデプロイメントクラスを削除します。
4. `$SPLUNK_HOME = /opt/splunk` のとき、`/opt/splunk_old` に移動します。それ以外は、3.4.x ターボールまたは rpm をデフォルトの場所にインストールします。
5. `splunk_old_etc.tgz` を新規インストールの上に抽出します。
6. `/opt/splunk_depserver/etc/system/local` または `/opt/splunk_depserver/etc/apps/内の inputs.conf/outputs.conf` ファイルを削除/名前変更します。`nputs.conf`、`outputs.conf`、および変更されていない `splunk-launch.conf` 以外はほぼすべて(`uthentication.conf`、`server.conf`、`/opt/splunk/etc/passwd`、`/opt/splunk/etc/auth/*`など)は維持したいはずです。
7. CLI または `web.conf` を利用して新規にインストールしたインスタンスの Splunk Web を無効にします。
8. `mv /opt/splunk /opt/splunk_depserver` を実行します。
9. `/opt/splunk_depserver/etc/splunk-launch.conf` を編集し、`$SPLUNK_HOME` を `/opt/splunk_depserver` に変更します。`$SPLUNK_DB` も設定する場合は、この変数をコメントアウトして、新しいインスタンスが旧データストアに書き込まれないようにします。

10. このデプロイメントサーバーが機能し続けることを確認するため、そのライセンスを 3.x フォワードライセンスに切り替えます。`$SPLUNK_HOME/etc/splunk-forwarder.license` を `$SPLUNK_HOME/etc/splunk.license` にコピーします。
11. `/opt/splunk_depserver/bin/splunk start` を実行します。
12. `mv /opt/splunk_old /opt/splunk` を実行し、その後移行を実行します。
13. 移行した後スタートアップ中に、Splunk は旧管理ポートの結合を検出し、管理者に管理ポートの変更を促します。**この新規ポートの記録は管理して、分散検索または REST コンフィギュレーションの際に更新する必要があります。**
14. `/opt/splunk_depserver/bin/splunk list deploy-clients ?auth admin:changeme` を実行して、デプロイメントクライアントがデプロイメントサーバーと通信していることを確認します。
14. Review `/opt/splunk_depserver/var/log/splunk/splunkd.log` と `/opt/splunk/var/log/splunk/splunkd.log` でエラーの発生を確認します。