



Splunk ユーザーマニュアル

バージョン : 4.0.3

作成日 : 2009 年 8 月 24 日 午前 5 時 1 分

Copyright Splunk, Inc. All Rights Reserved

目次

はじめに	1
このマニュアルについて	1
Splunk の概要	2
Splunk の概要	2
Splunk のコンポーネント	4
Splunk App(アプリケーション)	5
新しいデータをインデックスする	8
データとインデックスについて	8
インデックスにデータを追加する	9
検索と調査	10
検索について	10
検索開始	11
Splunk Web を使ったインタラクティブな検索	13
1つまたは複数のインデックスを指定した検索	16
1つまたは複数の分散サーバーをまたいだ検索	17
実行中の検索でアクションを実施する	17
時間範囲を変更して検索を絞る	18
時系列を使ってイベントのパターンを調査する	22
検索コマンドの働きについて	23
サブ検索の働きについて	28
知識の習得	29
知識の習得について	29
類似するイベントを分類してグループ化する	29
デフォルトフィールドおよび内部フィールドを使う	31
マルチバリューでフィールドを操作する	36
タグとエイリアスフィールドの値	37
新しいフィールドの抽出と追加	38
検索コマンドを使ったフィールドの抽出	40
Splunk Web を使って対話形式でフィールドを抽出する	41
トランザクションの特定	42
検索を保存して検索結果を共有する	43
検索ジョブの監視	44
Splunk の知識オブジェクトの共有と活用	45

自動モニタリング	48
再発条件のモニタリング	48
保存検索のスケジューリング	48
予約検索に対するアラート条件の設定	50
分析とレポート	53
レポートとチャートについて	53
レポートコマンドの使用	54
レポートの指定とチャートの作成	57
チャートギャラリー	61
レポートを保存し他の人と共有する	65
レポート用ダッシュボードとビューの使用	68
ビジュアルダッシュボードエディタを使った簡単なダッシュボードの作成	69
サマリーインデックスを使ってレポートの効率を上げる	74
サマリーインデックスの例(ファイアウォールトラフィック)	77

はじめに

このマニュアルについて

このマニュアルについて

本書では、Splunk を使って問題を調査し結果報告書を作成する **Splunk エンタープライズユーザー**のための情報および手順について説明しています。

以下の内容について説明しています。

- インデックスにデータを追加する方法
- 用語、論理的な表現、およびフィールドで検索する方法
- 検索結果およびタイムラインを使ってインタラクティブに検索を絞る方法
- イベントタイプ、新しいフィールドの抽出、タグフィールド値を保存する方法
- 検索を保存し、予約検索に対するアラート条件を設定する方法
- 報告書およびチャートを作成して保存したり、他人と共有する方法

Splunk の概要

Splunk の概要

Splunk の概要

Splunk は、データセンターの情報をより簡単に追跡し活用できるようにするパワフルで多目的の IT 検索ソフトウェアです。Splunk があれば、複雑なデータベース、コネクタ、カスタムパーサーまたはコントロールなどを使わなくても、ウェブブラウザとあなたの想像力だけで、あとは Splunk がすべて行ってくれます。

Splunk を使うと以下が行えます。

- IT データをすべてリアルタイムでインデックスに追加
- データに埋め込まれている役立つ情報を自動検索するため、自分で特定する必要がない
- 物理および仮想 IT インフラストラクチャを好きなように検索して、数秒で結果を得る
- 検索結果を保存し、役立つ情報にタグを付けて、システムをスマートに活用する
- 特定のイベント再発を防ぐためシステムを自動モニタリングするアラートを設定
- インタラクティブな図、表、グラフなどの分析レポートを生成し、他人と共有
- 保存した検索結果やレポートを Splunk ユーザーと共有し、チームメンバやプロジェクト関係者にメール配信する
- 積極的に IT システムを見直してサーバーのダウンタイムとセキュリティ問題が発生する前に阻止する
- 会社のニーズに合わせてさまざまな専門的で情報満載のビューおよびダッシュボードをデザインする

新しいデータにインデックスを付ける

Splunk は、すべてのアプリケーション、サーバ、ネットワークデバイスなどからライブログファイル、コンフィグレーション、トラップ、アラート、メッセージ、スクリプト、性能データ、統計などを含む IT インフラストラクチャの情報にリアルタイムでインデックスを付けるための柔軟性の高いさまざまな入力方法を提供しています。ファイルシステムをモニタリングしてスクリプトやコンフィグレーションに変更がないか確認します。ファイルシステムまたは Windows レジストリのモニタリングの切り替えができます。保存ファイルをキャプチャします。アプリケーションサーバのスタックトレースおよびデータベースの監査表を検索して追跡します。ネットワークポートに接続して、syslog、SNMP トラップ、その他のネットワークベースの計測情報を受信します。

データの入手方法やフォーマットに関係なく、Splunk は、同じ方法で、書き込みまたは保持のための特定のパーサーやアダプタを使わずにインデックスを作成します。未加工データとインデックス付けされたデータの両方を効率よく圧縮して、ファイルシステムベースのデータストアに保存します。データの整合性証明が必要な場合は、署名および監査のオプションデータを添え付けます。

Splunk でデータにインデックスを付けるための詳しい情報は、本書の「新しいデータにインデックスを付ける」章を参照してください。

検索と調査

さて、必要なすべてのデータをシステムに保存したら、次は何をしますか？まず最初は、Splunk のパワフルな検索機

能を使って、所定のフィールドのみでなくさまざまな検索を行ってみましょう。時間と用語検索を組み合わせましょう。システム不具合が発生する前に素早く IT インフラストラクチャの各層でエラーやコンフィギュレーションの変更を見つけて見ましょう。Splunk は、検索しながらレコードからフィールドを識別して、早めに鮮明なフィールドマッピングのルールセットを設定する必要があるソリューションによる優れた柔軟性を提供します。システムにテラバイトのデータが保存されている場合でも、Splunk なら精密に検索が可能です。

Splunk の IT 検索機能の詳細については、本書の「検索と調査」を参照してください。

知識の習得

未加工データを自由に検索できるだけではありません。フィールド、イベント、トランザクションなどに関する自分の知識を加えることにより、データの質を高め、検索の絞り込み能力が高まります。項目のビジネス上の役割や、監査要件に従って優先度の高いアセットにタグを付け、イベントに注釈を付けます。一連の関連するサーバエラーを 1 つのタグに収束し、そのタグを使って検索を実行して、そのエラーに関与しているイベントを隔離およびレポートします。頻繁に実行される検索を保存して共有します。Splunk は、最初にデータを標準化するのではなく、検索時間でデータに知識をマッピングして、従来の方法とは違うアプローチで操作をログ(記録)します。このようにして、組織内で使用されるさまざまな Splunk アプリケーションで検索内容、レポート、ダッシュボードを共有することができます。

イベントのタイプやフィールドに関する知識を取り込み、活用するための詳しい情報は、本書の「知識の習得」を参照してください。

自動モニタリング

検索を予約実行することができます。予約実行する検索は、特定の条件が発生したら通知を発行するよう設定できます。この自動警告機能は、アプリケーションからファイアウォールやアクセス制御まで、IT インフラストラクチャ全体で幅広いコンポーネントおよび技術に対応しています。Splunk で電子メールや SNMP 経由で別の操作コンソールに通知を送信します。アラートアクションを準備して、アプリケーション、サーバ、またはネットワークデバイスを再起動したり、トラブルチケットを開くなどの動作を実行するスクリプトを実行します。周知の不具合イベントに対してアラートを設定し、検索による高機能な相互関係を使って、強引な強制アタック、データ漏洩、さらにはアプリケーションレベルの不正行為など、周知のリスクパターンを見つけます。

再発イベントのモニタリングに関する詳しい情報は、本書の「自動モニタリング」を参照してください。

分析とレポート

大量のデータを素早く分析する Splunk の機能を使うと、検索結果をインタラクティブなチャート、グラフ、表などの形式にまとめることができます。統計的なコマンドを使って時間経過に基づく傾向を測定し、最高値を比較し、頻度の多いおよび少ない条件を報告するレポートを生成します。線グラフ、棒グラフ、カラムチャート、円グラフ、散布図、熱分布図など、インタラクティブな方法で視覚的に結果を報告します。

Splunk は、チームメンバーやプロジェクト関係者とレポートを共有するためのさまざまな方法を提供します。予約レポートを定期的に行って、Splunk で各種レポートを電子メールで関係者に送信したり、共通に行うレポートをコミュニティコレクションに保存したり、レポートを専用ダッシュボードに追加して参照したりすることができます。

レポートの定義、図表の生成、その共有などに関する詳しい情報は、本書の「分析とレポート」を参照してください。

積極的なレビュー

Splunk を使いこなせるようになると、IT インフラストラクチャ内のデータフローが理解できるようになり、Splunk を使って不具合が発生する前に見つけることができるようになります。

ログインやその他の動作の傾向をレビューして、疑わしいパターンや異常を発見し、それまでに発見されなかったセキュリティの問題を見つけることができます。Splunk のレポートリンクをサービスデスクや発券ワークフローと統合させて、IT システムの変更による影響を追跡します。サーバネットワークを積極的に監視して、問題が発生する前に、不具合のあるハードウェアを識別します。これだけではありません。

積極的なレビューの方法については、後でご説明します。

Splunk のコンポーネント

Splunk のコンポーネント

Splunk Web

Splunk Web は、Splunk のダイナミックかつインタラクティブなグラフィカル・ユーザー・インタフェース(GUI)です。ウェブブラウザを使ってアクセスする Splunk Web は、検索および調査、結果レポート、複数の Splunk デプロイメントの管理に使われる最初の画面です。対応するオペレーティングシステムおよびブラウザの一覧は、インストールマニュアルの「システム要件」を参照してください。

Splunk Web の Splunk app (アプリケーション)

Splunk Web を初めて起動すると、ある app が表示されます。ほとんどのユーザーは、この検索 app を中心に使用します。ほかにも、プラットフォーム特有の app があり、OS を使用するためのダッシュボードやビューがあります。Splunk を使うときは、これらの app(使用するアプリケーションにより異なるダッシュボードやビュー)を常に使用することになります。Splunk および App については、本章の「Splunk App」項を参照してください。

新しい Splunk 管理ページ

Splunk を起動する際に使用している app に関わらず、画面の右上には、k 管理とジョブの 2 つのリンクが常に表示されます。

k 管理リンクは、Splunk システムおよび app の設定および管理のページを表示します。Splunk 管理については、[coming soon!]を参照してください。

ジョブリンクは、すべての検索ジョブ(完了および実行中の両方)を管理するジョブ管理ウィンドウを表示します。ジョブ管理については、本書の「知識の習得」章の「検索ジョブの監視」を参照してください。

ブラウザから Splunk Web を起動 Splunk のインストールと起動が完了したら、ウェブブラウザを起動して以下へナビゲートします。

`http://mysplunkhost:8000`

ホストおよび HTTP ポートは、インストールで使用したものを採用してください。指定していない場合、HTTP ポートのデフォルトは 8000 です。

エンタープライズライセンスで初めて Splunk にログインする場合は、ユーザー名 admin、およびパスワード changeme を使用します。無料ライセンスの Splunk の場合は、アクセス制御はできません。

Splunk CLI

Splunk ユーザーは、コマンドラインインタフェース(CLI)から直接ほとんどのタスクを実行することができます。実行可能なタスクには、入力およびインデックスの管理、検索、保存、アラートの予約検索、検索結果のエクスポートなどが含まれます。CLI にアクセスできない場合は、Splunk 管理者にご相談ください。詳しくは、管理者マニュアルの「CLI について」を参照してください。

Splunk App(アプリケーション)

Splunk App(アプリケーション)

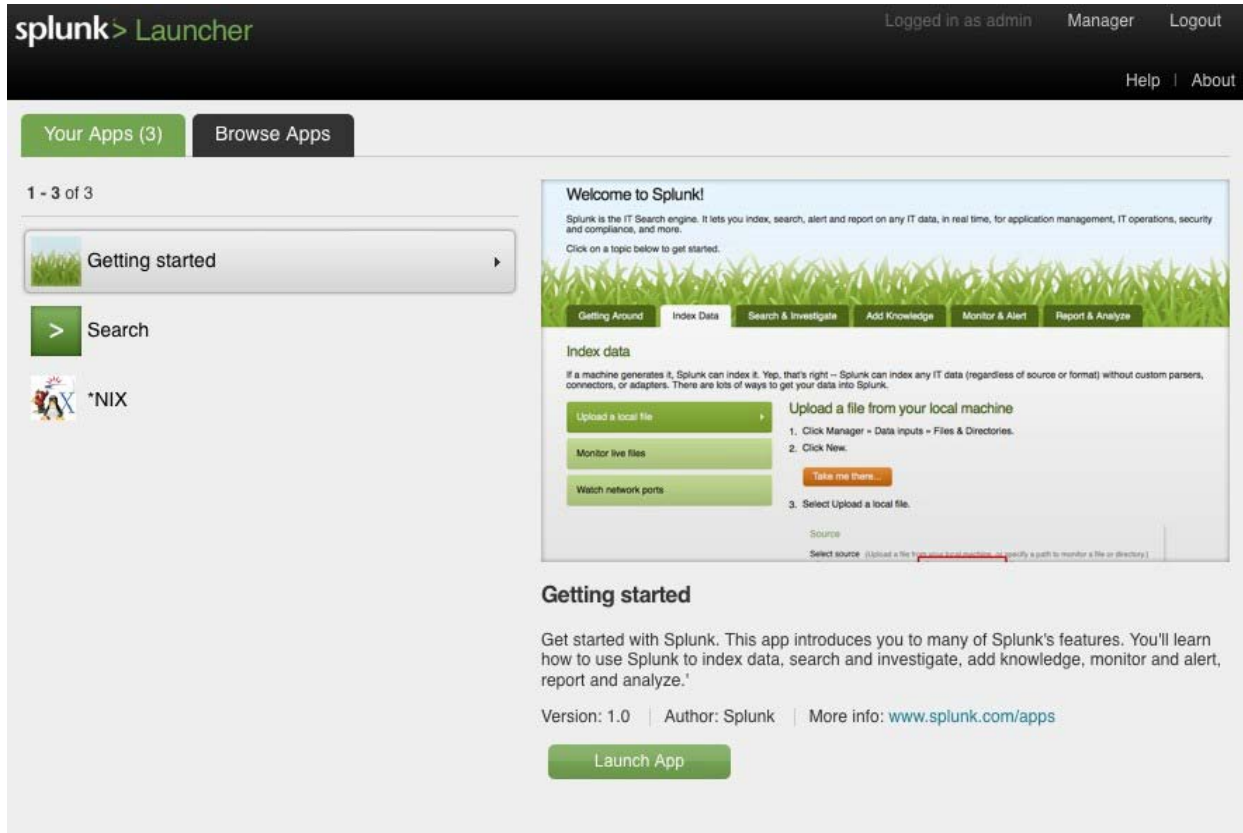
Splunk を使用すると、1 つまたは複数のアプリケーションのコンテンツを使用します。Splunk App はそれぞれが、ダッシュボードとビューで構成されています。また、その中には、特定の OS プラットフォームまたは特定のビジネス目的に特化したアドレスに対するデータを管理するためにデザインされているものがあります。

Splunk を使用するときは常に Splunk の App を使用しています。これを App の「中にある」と言います。

Splunk とその App に関する詳しい情報は、管理者マニュアルの「App とは」を参照してください。

App Launcher と Getting Started App

Splunk 管理者が特別に Splunk デプロイメントを設定していない限り、初めて Splunk をインストールしてログインすると、App Launcher(アプリケーションランチャ)が起動されます。この画面は、予めインストールされている App で使用可能なものを一覧表示します。デフォルトで、その1つに Getting Started(はじめましょう)が含まれています。この App は、Splunk の新規ユーザーにその機能について紹介するものです。Splunk を初めてご使用になる方は、是非ご利用ください。また、お気づきの点などございましたらご連絡ください。

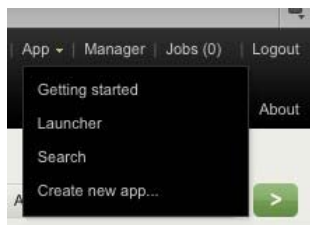


デフォルトで搭載の App

Splunk には、OS に対応した検索 App とその他の App が搭載されています。

- 検索 App は、Splunk の中核機能として一般的な使用を前提にしたインタフェースを提供します。Splunk を使用したことがある場合、この検索 App は、旧バージョンの Splunk Web の主な機能と置き換わっています。検索 App は、検索バーとさまざまなグラフのダッシュボードで構成されています。検索 App で、ウィンドウ左上のビュードロップダウンメニューから新しいものを選択するとダッシュボードやビューを変えることができます。
- OS 専用の App (Splunk for Windows または Splunk for *NIX など) は、特定のプラットフォームで Splunk を使いこなすためのダッシュボードと設定済みの検索画面を提供します。

使用アプリケーションを変更したい場合は、左上の App のドロップダウンメニューで新しい App を選択します。



Launcher に戻り、そこで別の App を選択することもできます。

別のアプリケーションの使用

Launcher または App メニューのアプリケーション一覧に別の App を追加できます。例えば、実行する一連のデータ処理作業にセキュリティ、管理変更、PCI(Payment Card Industry)コンプライアンスなどのタスクが関与する場合、Splunk には、さまざまなタスクに特化したアプリケーションが搭載されています。

ダウンロード可能なアプリケーションについては、Launcher の **App** の参照タブをクリックしてください。

ニーズに合うアプリケーションの構築

Splunk は、企業特有の独特なデータ管理に対応する App の作成に必要なあらゆるツールを提供します。専用のダッシュボードやビューを持つ App をデザインして、お好みでシンプルまたは高度な機能を持たせることができます。

Splunk アプリケーションのデザインと開発については、開発者マニュアルを参照してください。

新しいデータをインデックスする

データとインデックスについて

データとインデックスについて

Splunk を使用するとき、ユーザーは Splunk のインデックスのデータで作業します。通常、本書では、Splunk 管理者によりデータが既に Splunk インデックスに追加されている状態であることを前提に説明しています。その場合、本書の「検索と調査」章は省略することができます。

以下をお読みください。

- Splunk インデックスのデータタイプについて学ぶ
- Splunk インデックスに新しいデータを追加する方法を見る

Splunk インデックスのデータタイプについて

Splunk は、あらゆるソースからリアルタイムで IT データをインデックスすることができます。サーバまたはネットワークデバイスの syslog を Splunk に指定、WMI ポーリングを設定、logfiles をライブで監視、ファイルシステムや Windows レジストリの変化を監視、システムのメトリクスを抽出するスクリプトを定期的に行うなどしてインデックスできます。データの入手方法やフォーマットに関係なく、Splunk は、同じ方法で、書き込みまたは保持のための特定のパーサーやアダプタを使わずにインデックスを作成します。r ローデータとリッチインデックスの両方を効率よく圧縮されたファイルシステムベースのデータストアに保存します。データの整合性証明が必要な場合は、署名および監査のオプションデータを添え付けます。

Splunk でデータを取得する方法

Splunk にデータを追加するとき、柔軟性の高いさまざまな入力方法、Splunk Web、Splunk's CLI、inputs.conf 設定ファイルなど、から選ぶことができます。

Splunk Web を使うと、ほとんどのデータソースを追加できます。s 設定ファイルにアクセスできる場合は、詳しい設定オプションを持つ inputs.conf を使用できます。Splunk Web、または Splunk CLI を使用して行われた変更はすべて inputs.conf に書き込まれます。

「インデックスにデータを追加する」項では、Splunk Web を使って新しいデータを追加する一般的な手順の概要を説明しています。入力の設定に関する詳しい情報は、管理者マニュアルの「データの追加と入力の設定」章を参照してください。

Splunk がデータを保存する場所

本書で使用される「インデックス」には、複数の意味があります。まず、ほとんどの場合は、Splunk が新しいデータにインデックスを付けて、ローデータを検索可能なデータにする処理のことを示しています。次に、Splunk インデックスでは、Splunk がすべてまたは一部のデータを保存するデータの保存場所を指しています。つまり、新しいデータにインデックスするとき、Splunk はインデックスにデータを保存します。さらに、検索は、1 つまたは複数のインデックスのデータから一致するものを探します。

アプリケーションと入力

Splunk に入力値を追加すると、その入力値は、使用しているアプリケーションに関連付けられて追加されます。例えば、Splunk 付属の*nix や Windows App は、入力データを特定のインデックスに書き込みます。(*Nix および Windows の場合は、「os」インデックスに書き込む。) Splunk に保存されているデータが見つからない場合は、検索しているインデックスが正しいか確認してください。

Splunk ユーザーの場合、検索を開始してデータについて詳しく知る前に、これは最低限知っておく必要があります。インデックスでデータを管理する方法について詳しく知りたい場合は、管理マニュアルの「インデックスの管理」章を参照してください。

インデックスにデータを追加する

インデックスにデータを追加する

「データとインデックスについて」の項を読み進めると、Splunk を使って、アプリケーション、サーバ、ネットワークデバイスから、ログ、設定ファイル、トラップとアラート、メッセージ、スクリプトとコード、および性能データにインデックスできることがわかります。 Splunk Web を使うと、ほとんどのデータソースを追加できます。

データ入力設定ページへのアクセス

適切な権限があれば、Splunk 管理のデータ入力設定ページでインデックスのすべてのデータを表示および管理することができます。このページにアクセスするには、以下の操作を行います。

1. 画面右上の**管理**リンクをクリックします。このリンクは、使用している app に関わらず常に表示されています。
2. Splunk サーバの設定ページのリストから、**データ入力**をクリックします。データ入力の設定ページは、データタイプと各タイプに存在する入力件数を一覧表で表示します。

TCP または UDP 経由、またはスクリプトを使ってファイルおよびディレクトリから新しいデータを追加するには、該当する**入力の追加**リンクをクリックします。

Splunk のデータが見つからない場合

Splunk に入力値を追加すると、その入力値は、使用しているアプリケーションに関連付けられて追加されます。例えば、Splunk 付属の*nix や Windows App は、入力データを特定のインデックスに書き込みます。(*Nix および Windows の場合は、「os」インデックスに書き込む。) Splunk に保存されているデータが見つからない場合は、検索しているインデックスが正しいか確認してください。

入力値を追加すると、**Splunk** はその入力値を追加したときに使用したアプリケーションに属する **inputs.conf** のコピーに追加します。つまり、Splunk 管理ヘナビゲートした場合、入力値は、Launcher から直接 `$SPLUNK_HOME/etc/apps/launcher/local/inputs.conf` に追加されます。

検索と調査

検索について

検索について

さて、必要なすべてのデータをシステムに保存したら、次は何をしますか？まず最初は、Splunk のパワフルな検索機能を使って、所定のフィールドだけでなく、さまざまな検索を行ってみましょう。時間と用語検索を組み合わせてみましょう。システム不具合が発生する前に素早く IT インフラストラクチャの各層でエラーや設定の変更を見つけましょう。

Splunk は、検索しながらレコードからフィールドを識別して、先に鮮明なフィールドマッピングのルールセットを設定する必要があるソリューションによる優れた柔軟性を提供します。システムにテラバイトのデータが保存されている場合でも、Splunk なら精密に検索が可能です。

この章では、以下について説明します。

- 簡単な用語、論理的な表現、ワイルドカード、およびフィールドで検索を行う
- Splunk Web でインタラクティブな検索を行う方法
- 1 つまたは複数のインデックスを検索する方法
- 1 つまたは複数の Splunk サーバを検索する方法
- 実行中および完了した検索を操作する方法
- 時間範囲を変更して検索を絞り込む方法
- タイムラインを使ってイベントのパターンを調査する
- 検索コマンドがどのようにデータを処理するかについて知る

イベントデータ、フィールド、検索

Splunk で検索を実行するとき、イベントデータのセグメントに対して検索用語を照合しています。通常、イベントデータという言葉は、Splunk インデックスに追加された後のデータを指しています。イベントとは、1 つのアクションレコードまたは該当するイベントデータのインスタンスです。例えば、ログファイルの 1 つのログエントリをイベントと見ることができます。Splunk は、各イベントを時間情報で分割するため、1 つのイベントは、タイムスタンプにより他のイベントと区別されます。

例えば、

```
172.26.34.223 -- [01/Jul/2005:12:05:27 -0700] "GET /trade/app?action=logout HTTP/1.1" 200 2953
```

イベントは、情報またはフィールドのペアで構成されます。データを追加して、インデックスが付けられると、Splunk は、イベントが発生したホストや、データソースのタイプなど、ユーザーにとって役立つフィールドを自動抽出します。

フィールド名 (属性またはキーとも呼ぶ) やフィールド値を使って特定のイベントデータに対する検索を絞り込むことができます。フィールドについては、ナレッジマネージャマニュアルの「フィールドを使って作業」章「フィールドについて」項などを参照してください。

検索と知識

検索を続けていくと、パターンに気づき始め、検索可能なフィールドに役立つ情報が識別できるようになります。新しいデータをインデックスするとき新しいフィールドを認識するよう Splunk を設定できます。また、検索しながら新しいフィールドを作成することもできます。知れば知るほど、イベントデータのフィールド、イベント、トランザクションに関するこの知識を活用、追加、編集できるようになります。この知識の習得は、より効率の良い検索を実施し、より詳しいレポートを作成する役に立ちます。 イベントデータから知識を習得する、外部ソースから情報を追加するための詳しい情報は、本書の「知識の習得」を参照してください。

検索開始

検索開始

初めて Splunk を使うとき、ほとんどのユーザーは、ローデータを検索して、アプリケーションエラー、ネットワークの性能問題、セキュリティアラートなどの問題を調査することから始めるでしょう。Splunk を使った検索は、自由、つまり使い慣れたブーリアン操作、ワイルドカード、引用されたストリングなどを使って検索を構築できます。ユーザー名、IP アドレス、特定のメッセージなどをキーワードに入力します。いくつかのイ設定済みフィールドに制限される必要なく、複雑なクエリビルダーやクエリ言語を使う必要なく、検索するフィールドを知る必要もありません。時間、ホスト、ソースごとに検索できます。

注記： 次の例は、以下の情報で構成されるウェブアクセスログを使います。IP アドレス、ブラウザのバージョン、ウェブクエストプロトコル、HTTP ステータスコード、ウェブサイトの URL など。

シンプルな用語による検索

Splunk で検索を開始するため、イベントデータにありそうな用語を入力します。 例えば、HTTP 404 エラーとなるイベントを探したい場合は、キーワードに以下のように入力します。

```
http 404
```

この検索結果には、ローデータに HTTP および 404 の両方を含むすべてのイベントが抽出されます。検索結果は、期待通りとなる場合もあれば、ならない場合もあります。例えば、検索結果には、「http://」で始まるウェブサイトの URL であつたり、「ab/404」などの文字列を含める「404」のインスタンスである場合があります。

以下のキーワードを加えると、さらに検索を絞り込むことができます。

```
http 404 "not found" f
```

キーワードを引用符で囲むことにより、Splunk に文字通りまたは正確に一致するよう検索することを告げます。"not" および "found" を別々のキーワードとして検索すると、Splunk は両方のキーワードを含むイベントを返します。このとき、検索結果は必ずしも、"not found" ではありません。

また、ブーリアン表現を使って検索をさらに絞り込むこともできます。

b ブーリアン表現の追加

Splunk は、ブーリアン演算子 (AND, OR, and NOT) にも対応しています。この演算子は必ず大文字で表記します。

b ブーリアン演算子を括弧でくくってグループ化することもできます。 例えば、

404 または 403 を含まない HTTP クライアントエラーに対するすべてのイベントを検索したい場合は、以下のように入力します。

```
http client error NOT (403 OR 404)
```

Splunk 検索では、**AND 演算子**を使います。上述の例の検索は以下のように書き換わります。

```
http AND client AND error NOT (403 OR 404)
```

この検索は、"HTTP"、"client"、および"error"を含み、"403"および"404"を含まないすべてのイベントを返します。m もう一度繰り返しますが検索結果が期待通りとなる場合もあれば、ならない場合もあります。http 404 の検索結果と同じように、不要なイベントが含まれる場合もあれば、必要なイベントが含まれない場合もあります。

注記： Splunk ではブーリアン演算子を次の順序で評価します。最初に括弧内の表現、次に OR 節、最後に AND または NOT 節の順に処理します。

ワイルドカードを使った検索

Splunk では、アスタリスク (*) ワイルドカードを使った検索に対応しています。* を「すべて一致」という意味で検索して、最大値に達するまですべてのイベントを返します。* を検索単語の一部として検索します。

最も単純な検索は、* を検索してみることです。この検索では、インデックス全体を対象にして、最大数 (イベント 5 万件) までイベントを返します。これは効率的な検索ではありません。インデックスをより具体的な検索方法から始めることをお勧めします。

例えば、クライアントとサーバエラーが一致するイベントのみを検索したい場合は、次のように入力します。

```
http error (40* OR 50*)
```

これは、"HTTP"および"error"を含み、4xx および 5xx の HTTP ステータスコードを含むイベントを検索するよう Splunk に指示しています。この場合も、結果が期待通りである場合もあれば、ない場合もあります。さらに詳しく検索する場合は、情報を抽出して、その情報をフィールドとして保存します。

フィールドを使った検索

データにインデックスを付けると、Splunk はイベントデータにフィールドを自動的に追加します。これらのフィールドを検索に使用したり、フィールドを使いやすく編集したり、追加情報を抽出したり、カスタムフィールドに保存したりできます。フィールドに関する詳細、およびフィールドの使用、編集、追加方法については、本書の「知識の習得」章をお読みください。

Splunk は、抽出したすべてのフィールドを、Splunk Web の検索結果の横にあるフィールドメニューに一覧表示します。この「フィールドの選択」でフィールドを選択してフィールドを検索に追加できます。f フィールドの選択のフィールドで検索をフィルタリングすると、Splunk は選択したフィールドを含めるために検索バーを編集します。

ほかにも、フィールド名や値を直接検索バーに入力することができます。フィールド名と値のペアは、`fieldname="fieldvalue"` または `fieldname=fieldvalue` の 2 つの方法で表現できます。

注記： フィールド名は、大文字小文字を区別します。

ウェブアクセスログのイベントタイプが `eventtype=webaccess` と仮定して、HTTP ステータスコードに対応する

status フィールドをイベントデータに保存したとします。ここで、HTTP エラーを検索する場合は、検索条件を特定の sourcetype に制限することができます。

```
eventtype=webaccess error
```

ワイルドカードを使った複数のフィールド値の検索

ここでは特定のイベントを検索するため、この方法により検索を大幅に絞り込むことができます。ただし、この検索では、データに多く存在する可能性のある「error」文字列を検索しているため、検索結果は期待通りではない可能性があります。そこで、さらに詳しく、HTTP クライアントエラー (4xx) またはサーバエラー (5xx) であるウェブアクセスエラーを検索するよう指定します。

```
eventtype=webaccess status=40* OR status=50*
```

一致するフィールド値を探す比較演算子を使う

比較演算子を使って特定の値またはフィールド値の範囲を検索できます。

演算子	例	結果
=	field=foo	フィールドの値が「foo」と完全に一致する
!=	field!=foo	フィールドの値が「foo」と完全に一致しない
<	field<x	フィールドの数値が x より低い(以下)
>	field>x	フィールドの数値が x より高い(以上)
<=	field<=x	フィールドの数値が x より低い(以下) または等しい
>=	field>=x	フィールドの数値が x より高い(以上) または等しい

注記：数値フィールドには、<、>、<=、>= のみが使用できます。複数の値フィールドには、= および != のみが使用できます。

フィールド値をグループ化するタグの使用

タグを使って類似するフィールド値をグループ化して、そのタグを基にフィールドを検索することができます。タグに関する詳細、タグをフィールド値に追加する方法、およびタグの付いたフィールド値を検索する方法などについては、本書の「タグとエイリアスフィールドの値」をお読みください。

Splunk Web を使ったインタラクティブな検索

Splunk Web を使ったインタラクティブな検索

r ローデータの結果とタイムラインは相互に関係しています。そのため、クリックしてイベントを掘り下げて見たり、異常を確認したり、見つけるのが困難なノイズを排除したりできます。お客様の問題のトラブルシューティングを行う場合も、セキュリティアラートの調査をしている場合も、最終的には、時間や日付単位ではなく、事象が発生した瞬間を調査します。

ここでは、以下について説明します。

検索結果を使って検索を絞り込む

- フィールドの選択を使って検索条件を追加する
- k 検索アシスタントを使って検索条件を作る
- 検索結果を使って検索を絞り込む

検索を実行した後は、いつでも、検索結果からセグメントを選択して強調したり、そのキーワードを素早くかつ対話的に追加、削除、除外することができます。

検索に新しい用語を追加する

検索文字列に含めたフィールドおよび用語は、検索結果の一覧で強調表示されます。検索結果内の特定のセグメント(単語またはフレーズ)は、結果一覧上でマウスを移動させると強調表示されます。これは、それらの用語を検索に追加できることを示しています。別のセグメントを検索に追加するには、それをクリックします。検索条件が更新されて、前の検索結果で一致しない結果はすべて排除されます。

例えば、エラーのあるウェブアクセスイベントを検索するには、以下のように指定します。

```
eventtype=webaccess errors
```

ここでは、特定のホストマシン(alpha)が他のマシンより頻繁に現れることに気付いたとしましょう。その場合、このホストのみを検索することにします。このとき、検索バーにhost=alphaと入力するのではなく、フィールド値からひとつを選択してクリックします。

その検索文字列が自動的に新しいフィルタに加えられ、その検索条件を反映した検索結果に更新されます。

```
eventtype=webaccess errors host=alpha
```

検索から検索用語を削除する

検索条件に新しく用語を追加することが簡単なように、削除も簡単です。削除するには、検索結果の一覧で該当するセグメントを強調表示してクリックします。

例えば、あるマシン(alpha)で発生したウェブアクセスエラーを検索する場合は、以下のように入力します。

```
eventtype=webaccess errors host=alpha
```

検索後、結果を見ているうちに、このマシン(alpha)で起こった別のウェブアクセス操作を見たいと思います。この操作を、検索文字列を編集しないで素早く実行するには、結果から「errors」という用語をひとつ強調表示してクリックします。検索文字列と結果が自動的に以下のように更新されます。

```
eventtype=webaccess host=alpha
```

検索条件を除外する

検索結果の一覧を見ていると、結果の中に調査とは関係のないイベントが含まれていることに気付きました。不要なイベントを手作業で検索バーに入力しないでそのイベントを除外するには、**alt-クリック**を使います。(Windowsの場合は、**ctrl-クリック**を使う) Splunk は、選択した用語を除外するよう検索条件を更新します。

例えば、すべてのウェブアクセスエラーを検索する場合は以下のように指定します。

```
eventtype=webaccess errors
```

その後、alpha のイベントは除外したいと思い、検索結果のホスト値で alt-クリック(または ctrl-クリック) を行います。すると、検索バーが以下のように更新されます。

```
eventtype=webaccess errors NOT host=alpha
```

alpha で発生したすべてのイベントは検索結果の一覧から削除されます。

フィールドで検索条件を追加する

Splunk は、データをインデックに追加すると、そのデータから自動的にフィールドを抽出します。検索を実行した後、デフォルトでイベントデータに 3 つの異なるフィールド (ホスト h、ソースタイプ、ソース) が表示されます。Splunk が特定したその他のフィールド (検索結果にある場合) をすべて表示し、選択してイベントデータで見えるようにすることができます。

検索ビューでは、左側のタイムラインの下にフィールドサイドバーが表示されます。検索を実行すると、このサイドバーに検索結果に表示されるフィールドの一覧が表示されます。

タイムラインの下にある「フィールドの選択」をクリックして、フィールドポップアップウィンドウを開きます。f フィールドウィンドウでは、検索結果で表示されるすべてのフィールドを表示できます。この一覧からフィールドを選択して、検索結果に表示されるようにします。

フィールドを隠す (既に表示されているフィールド) には、「利用できるフィールド」リストまたは「選択フィールド」リストで該当する項目をクリックします。「保存」をクリックすると、イベントデータに適用した変更を反映した検索結果を見ることができます。

検索アシスタントを使って検索条件を作る

検索アシスタントは、検索準備をするユーザーのためのクイックリファレンスです。デフォルトでは、検索アシスタントはアクティブです。検索バーに用語を入力すると、先行打鍵情報を返します。検索コマンドを入力すると、そのコマンドの説明と、使い方の例を紹介します。k 検索アシスタントは、Splunk Web からアクセスできます。検索バーの下にある緑色の下向き矢印をクリックします。

デフォルトビューでは、簡単な説明、使用例、一般的な使い方、一般的に使われる次のコマンドなどを表示します。検索バーが空白 (検索コマンドが入力されていない状態) の場合、検索アシスタントは search コマンドの情報を表示します。

一般的な使い方および一般的に使われる次のコマンドの一覧を表示し、ヘッダーの横にある詳細リンクをクリックするとさらに詳しく一覧を展開することができます。リストの項目をクリックすると、Splunk はその項目を検索に追加します。

詳しい説明を見るには、簡単説明の最後にある **詳細>>**リンクをクリックしてください。この詳細説明には、詳しい説明、コマンド構文、関連するコマンド (ある場合) が表示されます。デフォルトビューに戻るには、**<< 詳細を閉じる** をクリックします。

注記： 検索コマンドの横にあるヘルプリンクをクリックすると、検索アシスタントから素早く検索コマンドの説明書を表示できます。この操作で、検索コマンドの参照ページが別のブラウザタブに表示されます。

1 つまたは複数のインデックスを指定した検索

1 つまたは複数のインデックスを指定した検索

皆さんは、これまでに新しいインデックスを作成して、データを保存する場所を管理する方法について学んできました。ここでは、複数のインデックスに分けられたデータが存在する場合、一度にひとつのインデックスの検索しかできない制限なしに、一度に複数のインデックスをまとめて検索できます。

Splunk の管理者は、ユーザーが検索するデフォルトのインデックスを設定できます。ユーザーの役割と権限を基に、アクセス可能なインデックスの数 (1 つまたは複数) が決まります。例えば、メインインデックスのみ検索できる人もいれば、すべての公開インデックスを検索できる人もいます。また、ユーザーは、検索用に個別インデックス、または複数インデックスのいずれかで、それらのインデックスのサブセットを指定できます。ユーザーと役割の設定については、管理者マニュアルの「ユーザーと役割について」章を参照してください。

インデックスの管理および複数インデックスの設定については、管理者マニュアルの「インデックスの管理について」章を参照してください。

構文

異なるインデックスを指定して、フィールド名と値を指定するのと同じ方法で検索できます。この場合、フィールド名は `index` となり、フィールド値は、以下のような特定のインデックスの名前となります。

```
index=<indexname>
```

ワイルドカード (`*`) を使用してインデックスのグループを指定できます。例えば、"mail"および"main" のインデックスを検索したい場合は、以下のように指定して検索します。

```
index=mai*
```

括弧を使って特定のインデックスに対する異なる検索を区別することができます。詳しくは、例 3 を参照してください。

注記： 検索バーに「index=」と入力すると、先行打鍵はユーザーの役割と権限の設定を基に検索可能なすべてのインデックスを表示します。

例

例 1： 公開インデックス全体の検索 `index=*`

例 2： 公開インデックスと内部インデックス全体の検索 `index=* OR index=_*`

例 3： パーティション(区分)で検索します。この例では、3 つの異なるインデックス `main`、`_internal`、`mail` を検索します。この 3 つのインデックスで「error」と一致するイベントを検索します。さらに、`main` では「warn」、`mail` では「failed」と一致するエラーも検出します。

```
(index=main (error OR warn)) OR (index=_internal error) OR (index=mail (error OR failed))
```

例 4： 異なる Splunk 分散サーバーで複数のインデックスをまたいで検索します。

```
(splunk-server=local index=main 404 ip=10.0.0.0/16) OR  
(splunk-server=remote index=mail user=admin)
```

探したいイベントが見つからない場合

Splunk に入力値を追加すると、その入力値は、使用している App に関連付けられて追加されます。例えば、Splunk 付属の *nix や Windows App は、入力データを特定のインデックスに書き込みます。(*Nix および Windows の場合は、「os」インデックスに書き込む。) Splunk に保存されているデータが見つからない場合は、見ているインデックスが正しいか確認してください。ユーザーが使用する役割に合わせて「os」インデックスをデフォルトインデックスの一覧に追加することもできます。役割については、本書の役割に関するトピックを参照してください。

1 つまたは複数の分散サーバーをまたいだ検索

1 つまたは複数の分散サーバーをまたいだ検索

デフォルトで、また保存や予約検索で、特定の分散検索サーバーへの検索を制限できます。Splunk サーバーの名前は、「splunk_server」フィールドに値として保存されます。

Splunk サーバーが指定されていないと、検索処理は、アクセスの権限があるすべての検索サーバーにアクセスします。ユーザーがアクセス可能なデフォルトサーバーは、管理者が設定したそのユーザーのプロファイルに関連付けられている権限により管理されます。詳しくは、管理者マニュアルの「ユーザーと役割について」を参照してください。

検索を特定のサーバーに制限する機能は、特定の検索サーバーの待ち時間が長い場合や、デフォルトで検索させたくないサーバーがある場合に役立ちます。1 つまたは複数のサーバーを指定したときは、指定したサーバーのみが検索の対象となります。

異なるインデックスを指定して、他のフィールド名と値を指定する場合と同じ方法で検索できます。この場合、フィールド名は「splunk_server」となり、フィールド値には、以下のように特定の分散サーバーの名前となります。

```
splunk_server=<server_name>
```

注記：「local」という値を使って、現在検索している splunk サーバーを参照できます。

```
splunk_server=local
```

フィールド名は大文字小文字を区別しますのでご注意ください。Splunk は、文字が一致しないとフィールド名を認識しません。

例

例 1： 指定サーバーから返された結果

```
splunk_server=NYsplunk OR splunk_server=CAsplunk
```

例 2： 分散 Splunk サーバー「foo」または「bar」での異なるインデックスを検索

```
(splunk_server=foo index=main 404 ip=10.0.0.0/16) OR (splunk_server=bar index=mail user=admin)
```

実行中の検索でアクションを実施する

実行中の検索でアクションを実施する

Splunk は、「実行中」の検索を管理するために使う一連の制御を提供します。この制御は、検索を実行中に検索バーの下に表示されます。表示されるコントロールは以下のとおりです。

- **時停止:** 実行中の検索を一時停止します。時間のかかる検索を実行中に検索を一時停止したい場合に便利です。再開をクリックすると検索を再開し、中断をクリックすると検索を終了します(以下参照)。
- **バックグラウンドに送る:** 別のプロジェクトを最前面で作業するときに検索を「バックグラウンド」に移動します。検索が完了すると、システムから通知が送られます。ジョブページからバックグラウンドに送られた検索にアクセスしてその結果を表示できます。
- **c 中断:** 検索が完了する前に検索を停止して、その時点までに Splunk が読み込んだ結果を表示します。終了した結果を使ってレポートを作成できます。
- **レポート作成:** 時間のかかる検索を実行しているときに検索が完了するのを待たずに、検索結果を基にしたレポートの定義を開始したい場合に、この制御を使ってレポートビルダを起動して準備することができます。レポートビルダを起動した後も検索は継続され、終了レポートには返されたすべてのイベントデータが含まれます。
- **キャンセル:** 実行中の検索を中止して結果をすべて削除します。Splunk は、ジョブページに最近中止した検索を一覧表示します。ただし、結果は既に削除されているため結果を見るためのビューリンクはありません。

ジョブページについては、本書の「検索ジョブの監視」を参照してください。

時間範囲を変更して検索を絞る

時間範囲を変更して検索を絞る

柔軟性のある時間範囲オプションを使うと、履歴データと比較するさらに役立つレポートを作成できます。例えば、前日さらにはその前の日の実績と比較してシステムの1日の性能を見ることができます。また、営業時間中のウェブトラフィックなど、特定の時間帯のデータのみの分析ができます。

検索に正確な時間範囲を指定する

時間範囲メニューには、検索に正確な時間を指定するオプション(**指定日時**、**指定日時以降のすべてのデータ**、**A 指定日時以前のすべてのデータ**、**日時の範囲**)があります。このオプションを選択すると、カレンダーモジュールが開き、日付と時刻を入力する、またはカレンダーから選択することができます。

例えば、第2四半期(4月~6月)に発生したイベントのみを検索したい場合は、日時の範囲を選択します。

Date range

April 2009

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

June 2009

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Start:
Apr 01, 2009

End:
Jun 30, 2009

Apply

Yesterday

Previous week

Previous business week

Previous month

Previous year

Specific date ▶

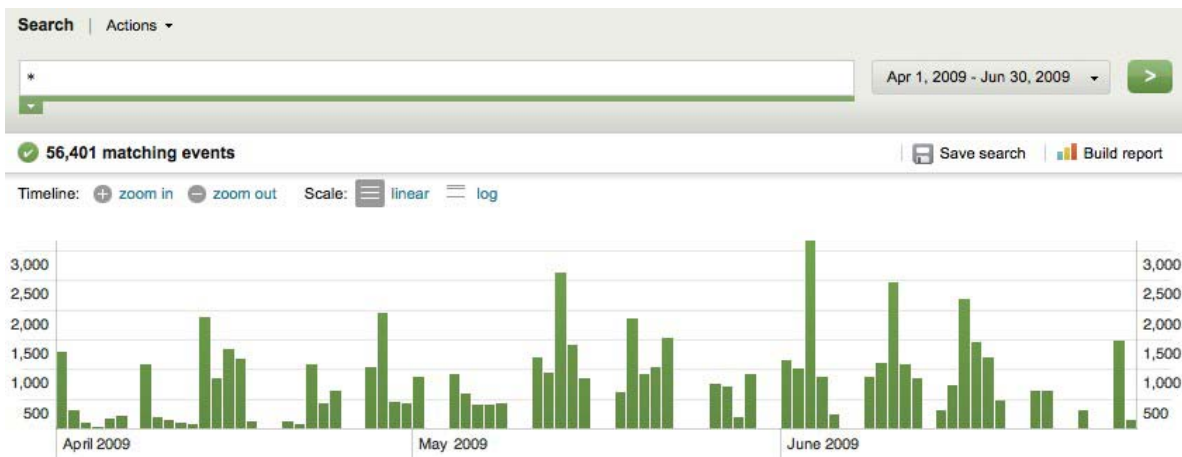
All dates after ▶

All dates before ▶

Date range ▶

All time

時間範囲メニューに選択した日付の範囲が表示されます。また、タイムラインには選択した期間のみが表示されます。



検索に相対時間範囲を指定する

検索を実行または保存するとき、earliest または latest 属性を指定して、検索時間に相対する時間範囲を定義することができます。

```
earliest=<time_identifier>
latest=<time_identifier>
```

「開始(earliest)」属性のみを指定すると、デフォルトで「終了(latest)」属性は現在(今)の時間が設定されます。通常、「終了」は「開始」時間とセットで指定します。

重要： 検索の実行および保存に時間範囲を指定すると、ドロップダウンメニューで選択した時間範囲より優先されます。ただし、検索文字列に直接指定した時間範囲は、サブ検索に適用されません。(ただし、ドロップダウンで選択した期間が適用されます。)

相対時間修飾子の構文

時間量および「スナップショットのような」時間単位(オプション)を示す文字列で、相対時間を検索に定義できます。 s

相対時間修飾子には「スナップショットのような」時間単位のみを指定することもできます。また、「現在」を指定すると、現在の時間(今)を参照します。

1. 文字列の先頭にプラス(+)またはマイナス(-)を指定すると、時間量のオフセットを指定できます。
2. 数字と単位で時間量を定義します。対応する時間単位は以下のとおりです。
 - s, sec, secs, second, seconds
 - m, min, minute, minutes
 - h, hr, hrs, hour, hours
 - d, day, days
 - mon, month, months
 - y, yr, yrs, year, years

指定する時間量が1つの場合は、s なら 1s(1秒)、m なら 1m(1分)のように、1が付加されます。

週の省略形はありません。w は数量として使えません。(7d は有効です。) ただし、w0、w1、w2、w3、w4、w5、w6 は「スナップショットのような」曜日として指定されています。この場合、w0 が日曜日、w1 が月曜日というように対応しています。

3. 「スナップショットのような」時間単位を指定する場合、これは指定した時間量を概算してより近いまたは最新の時間を示します。「スナップショットのような」時間単位を指定しない場合は、Splunk は自動的に秒をスナップショットのようにします。

「@」文字を使うと、「スナップショットのような」時間単位から時間量を区分します。手順 2 に一覧されている時間単位はどれも利用可能です。さらに、先週の日曜日や先週の月曜日など特定の曜日を「スナップショットのように」することもできます。この場合、日曜日には@w0、月曜日には@w1 を指定します。

重要：最近または最新の時間をスナップショットのようにする場合、Splunk は常に最新時間から時間をさかのぼる、または切り捨てます。(指定時間以降にはならない) 例えば、時間が 11:59:00 のときに時間を「スナップショットのように」した場合、11:00 をスナップショットのようにします(12:00 ではない)。

重要：「スナップショットのような」時間単位の前に時間オフセットを指定しないと、Splunk は指定した時間量に「現在の時間にスナップショットしたような」時間とみなします。例えば、現在が金曜日の午後 11:59 の場合、@w6 を使って「土曜日をスナップ写真のように」すると、先週の土曜日の午前 2:01 が結果的な時間となります。

相対時間識別子の例

ここで紹介する例の現時間は、2009年2月5日(水)午後 01:37:05 とします。また、通常1日(1d)は 24 時間ですが、夏時間調整がある場合はそれに該当しない場合があります。

時間修飾子	説明	結果	同等修飾子
now	今、現在の時間	Wednesday, 05 February 2009, 01:37:05 PM	+0, -0
-60m	60 分前	Wednesday, 05 February 2009, 12:37:00 PM	-60m@s
-1h@h	1 時間前、時間単位	Wednesday, 05 February 2009,	

		12:00:00 PM	
-1d@d	昨日	Tuesday, 04 February 2009, 12:00:00 AM	
-24h	24 時間前(昨日)	Tuesday, 04 February 2009, 01:37:05 PM	-24h@s
-7d@d	7 日前、1 週間前の今日	Wednesday, 28 January 2009, 12:00:00 AM	
-7d@m	7 日前、スナップショットのような分単位	Wednesday, 28 January 2009, 01:37:00 PM	
@w0	今週の始まり	Sunday, 02 February 2009, 12:00:00 AM	
+1d@d	明日	Thursday, 06 February 2009, 12:00:00 AM	
+24h	今から 24 時間、明日	Thursday, 06 February 2009, 01:37:05 PM	+24h@s

相対時間修飾子を使った検索の例

例 1： 週の始めから現時点(今)の期間に発生したウェブアクセスエラーの検索

eventtype=webaccess error earliest=@w0

この検索では、今週の日曜日の午前 12:00 から現時点までで該当するイベントを返します。当然ですが、検索を月曜日の正午に実施した場合、36 時間分のデータに対するイベントのみが表示されます。

例 2： 今週の営業日(月～金)に発生したウェブアクセスエラーの検索

eventtype=webaccess error earliest=@w1 latest=+7d@w6

この検索では、今週の月曜日の午前 12:00 から、今週の金曜日の午後 11:59 までの期間で該当するイベントを返します。

この検索を月曜日の正午に実施した場合は、12 時間分のデータに対するイベントのみが表示されます。一方、この検索を金曜日に実行すると、週の始めから金曜日の現時点までに発生したイベントを見ることができます。ただし、時系列は全営業日(月～金)を表示します。

例 3： 先週の営業日中に発生したウェブアクセスエラーの検索

eventtype=webaccess error earliest=-7d@w1 latest=@w6

この検索は、先週の月曜日の午前 12:00 から、先週の金曜日の午後 11:59 までの期間で該当するイベントを返します。

時間範囲を選択してカスタマイズ

Splunk には、さらに多くのビルトイン時間範囲が付属しています。Splunk 管理者は、表示する時間範囲をカスタマイズしたり、検索する際にドロップダウンメニューから選択したりできるようになりました。新しい時間範囲の設定については、管理者マニュアルを参照してください。

時系列を使ってイベントのパターンを調査する

時系列を使ってイベントのパターンを調査する

時系列は、それぞれの時間点で発生したイベント数を視覚的に表示します。時系列を使用して、イベントのパターンを強調したり、イベントのピークや最低値を調べたりできます。

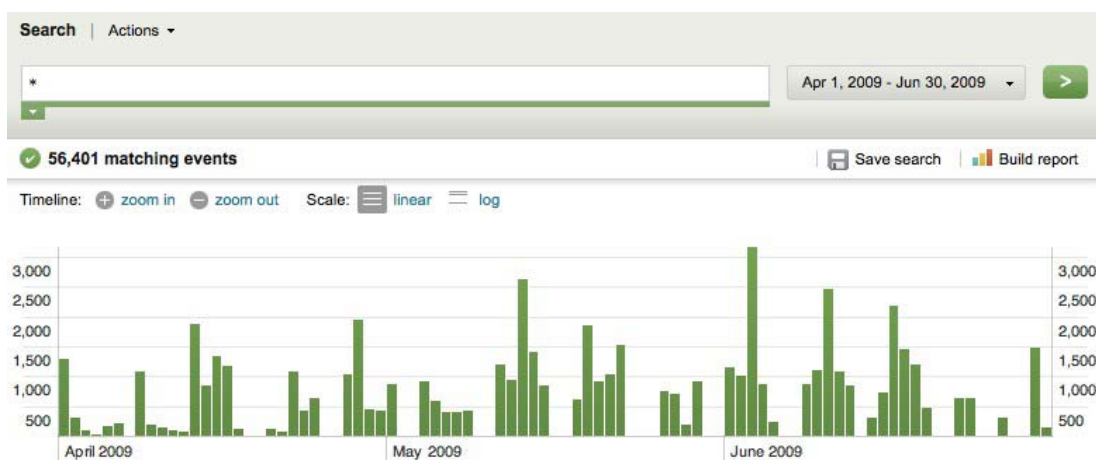
検索結果で時系列を更新すると、それぞれのバーの高さでイベントの数が表示されるため、バーの変化やパターンを見ることができます。時系列のピークや変化で、急な変化やサーバーのダウンタイムを見ることができます。

時系列オプションは時系列の上にあります。ズームインまたはズームアウトしてチャートのスケールを変更できます。

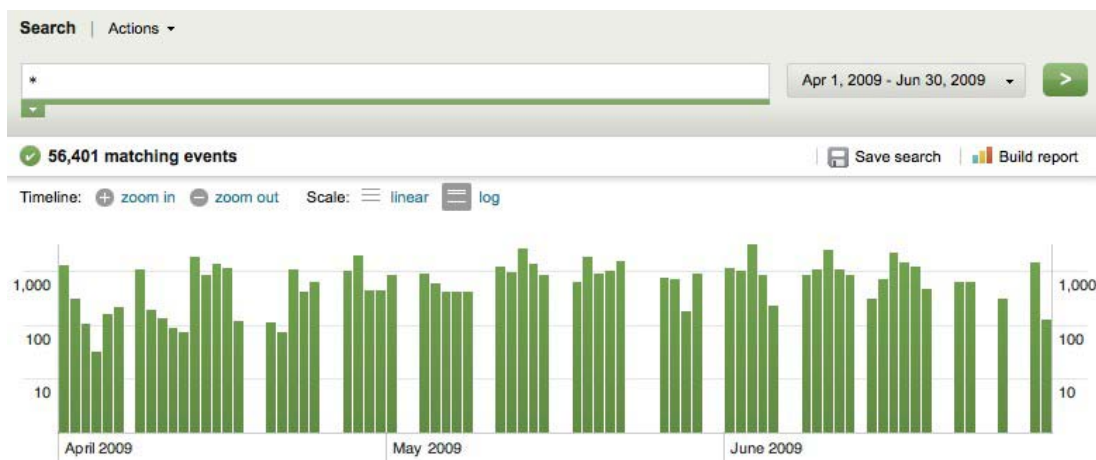
Timeline: zoom in zoom out Scale: linear log

時系列のスケールの変更

時系列は 2 種類のスケール(線グラフまたは対数表(ログ))で表示できます。下図は、第 2 四半期に発生したすべてのイベントを検索した結果を表す線グラフです。



下図は、同様に第 2 四半期に発生したすべてのイベントを検索した結果を表す対数表です。



調査対象イベントをズームイン / ズームアウト表示

時系列のバーでクラスタをクリックしてドラッグします。

検索結果を更新して、選択した時間範囲に発生したイベントのみを表示します。

ズームインをクリックすると、時系列を更新して、選択したイベントの期間のみを表示します。



時系列のバーをクリック

- 検索結果を更新して、選択した時間点に発生したイベントのみを表示します。
- 再度ズームインをクリックすると、時系列を更新して、選択した時間点のイベントのみを表示します。

時系列のすべてのバーを選択する場合は、(前の選択を解除してから)すべてを選択をクリックします。このオプションは、1つ以上のバーを選択した後で、ズームインまたはズームアウトのいずれかを選択する前にのみ利用可能になります。

検索コマンドの働きについて

検索コマンドの働きについて

Splunk による検索は、1つまたは複数のデータ生成コマンドおよびその引数で構成され、それには、文字キーワード、ワイルドカード、ブーリアン演算子、フィールド名および値、そしてサブ検索が含まれます。生成されたデータ(検索結果)は、検索パイプラインの別の検索コマンドへの入力値として使用できます。

大抵、検索コマンドをその動作、例えば、不要な情報をフィルタリングする、情報をさらに抽出する、データを評価する、データを統計結果に変換する、結果を再実行するなどに基づいて、カテゴリに分類します。特定のコマンドが複数のカテゴリに該当するかどうかは、使用する引数によります。検索コマンドの詳細一覧は、検索リファレンスマニュアルを参照してください。

データに対してコマンドがどのような動作を行うかを理解しておく、インデックスされたすべてのデータを表などで見るときに役立ちます。それぞれの検索コマンドで表の形が変化します。ここでは、種類の異なる検索コマンドがデータに対してどのように対応するかを説明しています。

注記: ここでは、データにはインデックスが付けられていることが前提条件です。データとインデックスについては、ユーザーマニュアルを参照してください。

インデックス付きデータの表

検索を行う前に、インデックスされたデータを表としてイメージしてみてください。この表では、各行にインデックスされたイベントが入力されています。イベントでは、インデックスまたは抽出フィールドに名前と値がペアで入力されています。この表では、列にフィールド名が入力され、フィールド値は各行の個別セルに入力されています。

この最初の表には、Splunk が自動的にデータを追加するデフォルトフィールドの列があります。このデフォルト列の後には、その他に抽出されたすべてのフィールド列が続きます。以下は、任意のイベントとフィールドに対応する最初の表の例です。

_raw	_time	host	sourcetype	source	field 1	field 2	...	field y
event 1	time 1	host 1	sourcetype 1	source 1	field 11	field 12	...	field 1y
event 2	time 2	host 2	sourcetype 2	source 2	field 21	field 22	...	field 2y
⋮	⋮	⋮	⋮	⋮	⋮	⋮	...	⋮
event x	time x	hsot x	sourcetype x	source x	field x1	field x2	...	field xy

最初または途中から検索する

検索は、検索コマンドパイプラインのどの時点からでも開始できます。小さい表の検索結果は、列内の同じ番号から検索条件と一致しないイベントの行を引いた数を抽出しています。検索によってセルの値は変わりません。

検索コマンド： crawl, file, savedsearch, search

例： 一致する host の検索する

この表に対して検索を実行する：

time	host	sourcetype	source
2008-11-03T14:08:16-0800	host1	syslog	syslog.log
2008-11-03T14:08:16-0800	http1	access_common	http1access.log
2008-11-03T14:08:15-0800	http2	access_common	http2access.log
2008-11-03T14:07:00-0800	host1	syslog	syslog.log
2008-11-03T14:04:00-0800	http2	access_common	http2access.log

イベントからすべての HTTP サーバーを検索する：

host=http*

_time	host	sourcetype	source
2008-11-03T14:08:16-0800	http1	access_common	http1access.log
2008-11-03T14:08:15-0800	http2	access_common	http2access.log
2008-11-03T14:04:00-0800	http2	access_common	http2access.log

不要な情報のフィルタリング

フィルタリングコマンドは、検索と同じ結果(抽出された表)を生成します。ただし、検索コマンドによっては、抽出された表の行や列の数が異なる場合があります。フィルタリングコマンドによってセルの値は変わりません。

フィルタリングコマンド : dedup, fields, head, localize, regex, search, set, tail, where

次の3つの例では、前述の検索例と同じ表に対して検索を実行しています。

例 : dedup で列内の値が重複するセルを削除する

ホスト名を基に重複するイベントを削除する :

* | dedup host

_time	host	sourcetype	source
2008-11-03T14:08:16-0800	host1	syslog	syslog.log
2008-11-03T14:08:16-0800	http1	access_common	http1access.log
2008-11-03T14:08:15-0800	http2	access_common	http2access.log

例 : fields で列を削除または維持する

host と sourcetype の情報のみを表示する :

* | fields + host, sourcetype

host	sourcetype
host1	syslog
http1	access_common
http2	access_common
host1	syslog
http2	access_common

例 : head で指定した番号以降の行をすべて削除する

検索結果から最初の3行のみを表示する :

* | head 3

_time	host	sourcetype	source
2008-11-03T14:08:16-0800	host1	syslog	syslog.log
2008-11-03T14:08:16-0800	http1	access_common	http1access.log
2008-11-03T14:08:15-0800	http2	access_common	http2access.log

データの評価

評価コマンドは、特定の列の名前やセルの値を変更できます。使用するコマンドにより、評価コマンドで列が追加される場合があります。

評価コマンド : abstract, addtotals, bucket, cluster, collect, convert, correlate, diff, eval, eventstats, format, fillnull, format, kmeans, makemv, mvcombine, mvexpand, nomv, outlier, overlap, replace, strcat, transaction, typelearner, xmlunescape

次の例では、この表に対して検索を行います。その後続く各検索によりデータが付け加えられます。

host	sourcetype	count1	count2
host1	syslog	200	80
http1	access_common	300	80
http2	access_common	300	60
host2	syslog	200	90
http2	access_common	300	60

例： eval 表現の結果となるセルに新しい列を作成する

count1 と count2 の値の合計(sum)を新しいフィールドとして作成します。

* | eval sum=count1+count2

host	sourcetype	count1	count2	sum
host1	syslog	200	80	280
http1	access_common	300	80	380
http2	access_common	300	60	360
host2	syslog	200	90	290
http2	access_common	300	60	360

例： 1つ以上の列の名前を rename で変更する。このコマンドは新しい列を作成しません。

前回の検索結果の表を使って、列名 sum を total に変更します。

* | rename sum as total

host	sourcetype	count1	count2	total
host1	syslog	200	80	280
http1	access_common	300	80	380
http2	access_common	300	60	360
host2	syslog	200	90	290
http2	access_common	300	60	360

例： replace でセルの値を上書きする。このコマンドは新しい列を作成しません。

前回の検索結果である表を使って、host の値、host1 すべてを localhost に変更します。

* | replace host1 with localhost in host

host	sourcetype	count1	count2	total
localhost	syslog	200	80	280
http1	access_common	300	80	380
http2	access_common	300	60	360
host2	syslog	200	90	290
http2	access_common	300	60	360

例： `strcat` で他の列の連結文字列値の列を新しく作成する

前回の検索結果の表を使って、`host` と `sourcetype` の値をハイフンで組み合わせる `hosttype` という名前の文字列の列を追加します。

* | `strcat host "-" sourcetype hosttype`

host	sourcetype	count1	count2	total	hosttype
localhost	syslog	200	80	280	localhost-syslog
http1	access_common	300	80	380	http1-access_common
http2	access_common	300	60	360	http2-access_common
host2	syslog	200	90	290	host2-syslog

結果の並べ替え

並べ替えコマンドは、指定した列名の値に基づいて表全体の行を並べ替えます。このコマンドは、行を追加または削除しません。また、セルの値も変更しません。

並べ替えコマンド： `reverse`, `sort`

例： `sort` で表を並べ替える。

前回の検索結果の表を使って、`total` の昇順で行を並べ替えます。

* | `sort + total`

host	sourcetype	count1	count2	total	hosttype
localhost	syslog	200	80	280	localhost-syslog
host2	syslog	200	90	290	host2-syslog
http2	access_common	300	60	360	http2-access_common
http2	access_common	300	60	360	http2-access_common
http1	access_common	300	80	380	http1-access_common

情報をさらに抽出する

抽出コマンドは、各行の `_raw` 列にある情報を基に新しく行または列を作成します。

抽出コマンド： `addinfo`, `extract/kv`, `iplocation`, `multikv`, `rex`, `top`, `typer`, `xmlkv`

例： `extract/kv` でイベントのキーと値のペアから新しい列を作成する

例： `multikv` で複数ラインまたは表イベントの情報から新しい行を作成する

データを統計結果に変換する

変換コマンドは、全く新しいデータ表を作成します。このコマンドは、各イベントに対して指定したセルの値を、Splunk が統計に使用できる数値に変換します。

変換コマンド： `chart`, `contingency`, `highlight`, `rare`, `stats`, `timechart`, `top`

例： chart

サブ検索の働きについて

サブ検索の働きについて

サブ検索とは、検索パイプラインを引数にして行う検索です。サブ検索は、角括弧 [] を使い、先に評価されます。サブ検索の結果は、一次検索または外部検索の引数として使います。検索条件に直接指定できないが検索から生成できるデータのサブセットを抽出するためにサブ検索を使うことができます。

例えば、1時間前に最も稼働率の高かったホストのイベントをすべて見たい場合、どのホストの稼働率が高いか不明なため特定のホストを指定できません。そこで、先に最も稼働率の高いホストを識別する必要があります。

```
sourcetype=syslog | top limit=1 host | fields +host
```

その後、1時間前に最も稼働率の高かったホストが判明してから、そのホストのすべてのイベントを検索します。この例では、サーバー名を「crashy」とします。

```
sourcetype=syslog host=crashy
```

この情報を取得するために検索を2回実行する代わりに、以下を実行します。

```
sourcetype=syslog [search sourcetype=syslog | top limit=1 host | fields +host]
```

サブ検索を使ってデータを関連付ける

サブ検索を行ってデータを関連付けることができます。これは、分散環境でインデックスや Splunk サーバーが異なる場合にも対応します。

知識の習得

知識の習得について

知識の習得について

「検索と調査」章で説明した自由検索の基本をマスターした後は、検索で得るローデータでは常に必要な回答が得られるとは限らないため、精度のレベルを高めたいと思うことがあります。

構造化データを処理する力を使い、非構造化検索の柔軟性を生かす Splunk の機能を活用します。イベント、フィールド、トランザクション、データのパターンなどに関する知識を高めます。類似するイベントを見つけ、わかりやすい名前(「イベントタイプ」)でグループ化して、フィールドと同じ方法で検索できます。イベントのクラスタに関連するトランザクションを識別して追跡します。関連するフィールドをタグやエイリアスでグループ化します。対話形式でイベントデータまたは外部情報(ルックアップテーブルなど)を基に新しいフィールドを抽出して、検索に追加します。

この章では、以下について説明します。

- 類似または関連するイベントを識別してイベントタイプでグループ化する方法
- Splunk によるインデックス処理で抽出されるデフォルトおよび内部フィールドのリストを表示して、検索で使う方法
- タグやエイリアスを使って値が関連するフィールドをグループ化する方法
- 対話形式で新しいフィールドを抽出および追加する方法
- トランザクションに関連するイベントクラスタを識別して検索で有利に活用する方法
- 対話型のフィールド抽出の例で詳細を見る
- 保存した検索文字列を作成して検索結果を他人と共有する方法
- 処理中および完了した検索ジョブを管理して結果をレビューする方法
- Splunk の知識オブジェクトについて知り、他人と共有する、およびアプリケーションで採用する方法

類似するイベントを分類してグループ化する

類似するイベントを分類してグループ化する

イベントはイベントタイプと同じではありません。イベントはデータのシングルインスタンス、例えば、1つのログエントリです。イベントタイプはイベントにラベルを付け、グループ化するための区分です。例えば、SSH でログインされているすべてのログエントリ、またはすべての sendmail syslog メッセージに対してイベントタイプを作成する場合は、対象のイベントを素早く検索できます。

イベントには対応するイベントタイプの名前が設定されてる、eventtype と呼ばれる複数の値フィールドがあります。これらのイベントのグループ(SSH ログインなど)は、フィールド値を検索する場合と同じ方法で検索できます。

ここでは、イベントタイプを保存して検索で使用する方法について説明しています。イベントに関する詳細、Splunk がイベントを認識する方法、イベントにインデックスを付ける際の動作などについては、ナレッジマネージャマニュアルの「イベントについて」トピックを参照してください。

検索を新しいイベントタイプで保存する

イベントデータを検索するとき、基本的に不要なすべてのイベントを取り除いています。したがって、検索の結果は、共通の特徴を共有するイベントであり、共同の名前を付けることができます。

検索のアクションドロップダウンメニューから「イベントタイプとして保存...」オプションを選択して、検索をイベントタイプで保存します。イベントタイプを保存ウィンドウが表示されます。

イベントタイプを保存ウィンドウで、「イベントタイプ名」テキストエリアに検索名を入力します。必要に応じて検索文字列を変更します。イベントタイプに対するタグを定義することもできます。この詳細は、後述されています。「保存」をクリックしてイベントタイプ名を保存します。

ここで、この `eventtype` と一致するすべてのイベントを素早く検索します。例えば、SSH でログインしたすべてのイベントでイベントタイプ名が `sshlogin` の検索を保存したとします。特定のマシンでホスト名が `alpha` のすべての SSH ログインを検索するには、以下のように記述します。

```
host=alpha eventtype=sshlogin
```

また、より明確な検索を行うように選択して、それぞれの変動を `eventtype` に保存できます。例えば、特定のマシンにおける SSH ログインを頻繁に検索する場合は、検索文字列にホスト名を含め、それぞれの特定のホスト名に対するイベントタイプを保存します。つまり、`alpha` への SSH ログインのみを見たい場合は、イベントタイプの検索を以下のように記述します。

```
eventtype=alpha_sshlogin
```

フィールドの検索については、本書の「検索と調査」章の「検索開始」トピックを参照してください。

`punct`

で類似するイベントを特定する

イベントの句読記号は特定のイベントタイプで固有なため、Splunk はイベントの句読記号文字を `punct` フィールドにインデックスします。このフィールドの値は、解読不能に見えますが、類似するイベントを特徴付ける効果的な方法となる場合があります。

検索結果に `punct` フィールドを適用するには、本書の「検索と調査」章の「Splunk Web を使ったインタラクティブな検索」トピックに説明される「フィールド」ポップアップを使用します。SSH ログインイベントに対する `punct` 値を選択します。こうすると、検索バーにこの `punct` との組み合わせを含めて検索を更新します。句読記号にワイルドカード(`punct=::[*/*]`)を使用して変化の少ない検索を実行してみてください。

`typelearner` を使って新しいイベントタイプを検出する

検索に対して `typelearner` コマンドを実行すると、Splunk の推奨するイベントタイプを見ることができます。デフォルトでは、`typelearner` は検索結果としてのイベントの句読記号を比較し、類似する句読記号や用語を持つイベントをグループ化します。

異なるフィールドを指定して Splunk でイベントをグループ化できます。このとき、`typelearner` はフィールドと同様に機能します。その結果には、このフィールドとフレーズを共通に含むイベント一式(検索結果による)が抽出されます。

詳細および例については、検索コマンドリファレンスの「typelearner」を参照してください。

タグを使って類似するイベントをグループ化および検索する

検索をイベントタイプとして保存するウィンドウで、タグを追加できます。このときのイベントタイプには、イベントに関連する複数のタグが設定できます。イベントタイプのタグの検索は、タグの検索と同じ方法で行います。

ファイアウォールイベントの検索をイベントタイプ `firewall_allowed` で保存し、ログインイベントの検索をイベントタイプ `login_successful` で保存したとします。この2つのイベントタイプを `allow` でタグ付けすると、検索により、いずれかのイベントタイプから該当するすべてのイベントが抽出されます。

```
tag::eventtype="allow"
```

タグの使い方については、本書の「タグとエイリアスフィールドの値」を参照してください。

デフォルトフィールドおよび内部フィールドを使う

デフォルトフィールドおよび内部フィールドを使う

フィールドは、イベントデータにある検索可能な名前と値のペアです。検索では、イベントデータのセグメントに対して検索語が一致するか比較しますが、ここでフィールドを使うとより正確に行うことができます。新しいデータをインデックスすると、Splunk はデータの名前と値のペア、ヘッダー、その他の意味のある情報で自動的にフィールドを認識し、追加します。いくつかのデフォルトフィールドには、データの入手先(ホスト、ソース、ソースタイプなど)に関する情報が記述されています。アンダーバー(_)で始まるフィールドは、内部フィールドです。

フィールドの種類	フィールド	説明
内部フィールド	<code>_raw</code> , <code>_time</code>	Splunk のイベントに関する全般的な情報が格納されているフィールド
デフォルトフィールド	<code>eventtype</code> , <code>host</code> , <code>index</code> , <code>linecount</code> , <code>punct</code> , <code>source</code> , <code>sourcetype</code> , <code>splunk-server</code> , <code>timestamp</code>	イベントの生成場所、インデックスの付加状態、イベントの種類、構成される行数、発生時期などに関する情報が格納されているフィールド。このフィールドはデフォルトでインデックスが付加され、フィールドメニューに追加されます。
デフォルト日付フィールド	<code>date_hour</code> , <code>date_mday</code> , <code>date_minute</code> , <code>date_month</code> , <code>date_second</code> , <code>date_wday</code> , <code>date_year</code> , <code>date_zone</code>	イベントタイムスタンプに検索可能な精度を付加するフィールド。 注記： システムで生成され、内部にタイムスタンプのあるイベントのみに <code>date_*</code> フィールドがあります。 <code>date_*</code> フィールドがあるイベントは、そのイベント自身の日付と時刻の値を示します。タイムゾーンの変換を指定した、またはインデキシング時に日付と時刻を変更したまたは入力した場合(インデックス時または入力時の時間をタイムスタンプに設定する場合など)は、イベント自身の時間を示しません。

フィールドに複数の情報が含まれる場合があります。このようなフィールドおよびその値の取り扱いについては、本章の「複数の値を持つフィールドの構文解析」を参照してください。

Splunk Web を使用、または抽出検索コマンドを使用して、他のフィールドも抽出できます。詳しくは、本章の「新しいフィールドの抽出と追加」を参照してください。

フィールド名の変更または類似するフィールドをグループ化したい場合があります。これは、フィールドおよびフィールドの値にタグまたはエイリアスを付けることで簡単に実現します。詳しくは、本章の「タグとエイリアスフィールドの値」を参照してください。

ここでは、データをインデックスする際に自動的に Splunk が追加する内部フィールドとデフォルトフィールドについて説明します。

内部フィールド

`_raw`

`_raw` フィールドには、イベントのローデータが格納されています。Splunk の `search` コマンドは、検索およびデータ抽出を行うときに `_raw` のデータを使います。

`_raw` は、`search` コマンドの引数として使用できません。`_raw` は、データ処理コマンドでのみ使用します。

例： 「10」で始まる IP アドレスを持つ `sendmail` イベントを返す

```
eventtype=sendmail | regex _raw=*10.\d\d\d\d.\d\d\d\d.\d\d\d\d*
```

`_time`

`_time` フィールドには、イベントのタイムスタンプが Unix タイムで格納されています。Splunk はこのフィールドを使って Splunk Web のイベント時系列を作成します。

`_time` は、データ処理コマンドでのみ使用します。

例： タイプが「mail」で宛先がユーザー「strawsky@bigcompany.com」のすべてのソースを検索してから検索結果をタイムスタンプで並べ替える

```
sourcetype=mail to=strawsky@bigcompany.com | sort _time
```

デフォルトフィールド

`eventtype`

`eventtype` フィールドには、ユーザーが定義したイベントタイプが格納されています。`eventtype` フィールドを使って検索をフィルタし、`search` 引数と一致するよう検索結果に対してイベントタイプを指定します。また、`eventtype` を使ってデータ抽出ルールを作成し、レポートを実行します。

データから類似するパターンを見つけてイベントをイベントタイプで分類し、イベントの類似性を基にイベントタイプを保存します。

注記： ワイルドカードを使って1つの表現で複数のイベントタイプを指定できます。(例：`eventtype=access*`)

例 1： 「access」で始まるイベントタイプと一致するイベントを検索する

```
eventtype=access*
```

例 2: splunk3 で最も標準的なイベントタイプ、ソースタイプ「syslog」のイベント上位 10 件を表示する

```
sourcetype="syslog" host=splunk3 | top eventtype
```

host

host フィールドには、発信元ホスト名またはイベントを生成したネットワークデバイスの IP アドレスが格納されています。イベントと一致させる host の値を指定し、host フィールドを使って検索を絞り込みます。ワイルドカードを使って 1 つの表現で複数のホストを指定できます。(例: host=corp*)

host を使ってデータ生成コマンドの結果をフィルタ、またはデータ処理コマンドの引数に使用します。

例 1: ユーザー「strawsky」がアクセスしたすべての「corp」サーバーのイベントを検索する。検索結果から、最新のイベントを 20 件報告する。

```
host=corp* eventtype=access user=strawsky | head 20
```

例 2: 「404」を含むイベントを検索して、検索結果から、ホスト名が「192」で始まるホストを抽出する

```
404 | regex host=*192.¥d¥d¥d¥.¥d¥d¥d¥.¥d¥d¥d¥*
```

index

_index フィールドには、イベントがインデックスされたときのインデックス名が格納されています。index は、index="name_of_index"を使って検索するときに指定します。デフォルトでは、すべてのイベントは main インデックスでインデックスされます。(index="main")

例: インデックスが「myweb」で拡張子が「.php」のイベントを検索する

```
index="myweb" *.php
```

linecount

linecount フィールドには、イベントを構成する行数が格納されています。これは、イベントがインデックスされる前の行数です。linecount を使って、行数が一致するイベントを検索、またはデータ処理コマンドの引数に使用します。一致範囲を指定するには、以上(>)または以下(<)の表現を使います。(例: linecount>10 linecount<20)

例: corp1 を対象に、「40」を含む 40 行のイベントを検索し、400 を含むイベントは除外する

```
40 linecount=40 host=corp1 NOT 400
```

punct

punct フィールドには、イベントから抽出された句読記号のパターンが格納されています。句読記号のパターンは、イベントタイプで固有です。punct を使って検索するイベントをフィルタ、またはデータ処理コマンドのフィールド引数に使用します。

punct フィールドにワイルドカードを使って、検索したい同じ共有文字を共有する複数の句読記号パターンを検索できます。punct フィールドで句読記号パターンを定義するときは、必ず引用符を使用します。

例 1: 始まりと終わりが : であるすべての句読記号パターンを検索する

```
punct=":.*"
```

例 2: `php_error.log` を対象に、句読記号パターンが「`[--_::]__:__:____/-. -'///.____`」である php エラーイベントを検索する

```
source="/var/www/log/php_error.log" punct="[--_::]__:__:____/-. -'///.____"
```

source

`source` フィールドには、イベントがインデックスされたときのファイル名またはパス名が格納されています。

`source` を使って検索するイベントをフィルタ、またはデータ処理コマンドの引数に使用します。ワイルドカードを使って1つの表現で複数のソースを指定できます。(例: `source=*php.log*`)

`source` を使ってデータ生成コマンドの結果をフィルタ、またはデータ処理コマンドの引数に使用します。

例: 「`/var/www/log/php_error.log`」がソースであるイベントを検索する

```
source="/var/www/log/php_error.log"
```

sourcetype

`sourcetype` フィールドには、ソースの分類または種類が格納されています。Splunk 管理者は、予めソースの種類を定義することができます。または、Splunk がインデックスする際に自動的に生成するよう指定することもできます。

`sourcetype` を使って検索するイベントをフィルタ、またはデータ処理コマンドの引数に使用します。ワイルドカードを使って1つの表現で複数のソースを指定できます。(例: `sourcetype=*php.log*`)

例: ソースタイプが「`access log`」のすべてのイベントを検索する

```
sourcetype=access_log
```

```
splunk-server
```

`splunk-server` フィールドには、分散 Splunk 環境の異なるサーバー名が格納されています。

例: サーバー名が `remote` であるリモートサーバーのメインインデックスを検索から除外する

```
splunk-server=remote index=main 404
```

timestamp

`timestamp` フィールドには、イベントのタイムスタンプの値(インデックス付加時に抽出)が格納されています。Splunk は、ユーザー(または Splunk 管理者)によるタイムスタンプ抽出設定を基にタイムスタンプを抽出します。`timestamp` を `search` コマンドの引数として使い、検索をフィルタできます。

例えば、`timestamp=none` を検索に追加して、タイムスタンプとして認識できる値を含まないイベントのみを検索結果に含むよう検索をフィルタできます。

例: データに識別できるタイムスタンプのないイベント数を返す

```
timestamp=none | stats count(_raw) as count
```

デフォルト日付フィールド

`datetime` フィールドを使って検索するイベントをフィルタ、またはデータ処理コマンドのフィールド引数に使用できます。

date_hour

date_hour フィールドには、イベントが発生した時間の値(0~23 の値)が格納されています。この値は、イベントのタイムスタンプ(_time の値)から抽出されます。

例： 今日の午後 10 時から午前 12 時の間に発生した「apache」を含むイベントを検索する

```
apache (date_hour >= 22 AND date_hour <= 24)
```

date_mday

date_mday フィールドには、イベントが発生した月日の値(1~31 の値)が格納されています。この値は、イベントのタイムスタンプ(_time の値)から抽出されます。

例： 今月の 1 日から 15 日の間に発生した「apache」を含むイベントを検索する

```
apache (date_mday >= 1 AND date_mday <= 15)
```

date_minute

date_minute フィールドには、イベントが発生した分の値(0~59 の値)が格納されています。この値は、イベントのタイムスタンプ(_time の値)から抽出されます。

例： 今の時間帯で 15 分から 20 分の間に発生した「apache」を含むイベントを検索する

```
apache (date_minute >= 15 AND date_minute <= 20)
```

date_month

date_month フィールドには、イベントが発生した月の値が格納されています。この値は、イベントのタイムスタンプ(_time の値)から抽出されます。

例： 1 月に発生した「apache」を含むイベントを検索する

```
apache date_month=1
```

date_second

date_second フィールドには、イベントのタイムスタンプの秒部分(1~59 の値)の値が格納されています。この値は、イベントのタイムスタンプ(_time の値)から抽出されます。

例： 現在の分で、1 秒から 15 秒の間に発生した「apache」を含むイベントを検索する

```
apache (date_second >= 1 AND date_second <= 15)
```

date_wday

date_wday フィールドには、イベントが発生した曜日(日曜日~土曜日：1~7)が格納されています。Splunk は、イベントスタンプ(_time の値)からイベントが発生した日付(数値)を抽出し、その日付が何曜日になるか算出します。計算された曜日は、date_wday フィールドの値です。

例： 日曜日(1)に発生した「apache」を含むイベントを検索する

```
apache date_wday=1
```

date_year

date_year フィールドには、イベントが発生した年の値が格納されています。この値は、イベントのタイムスタンプ (_time の値)から抽出されます。

例： 2008 年に発生した「apache」を含むイベントを検索する

```
apache date_year=2008
```

date_zone

date_zone フィールドには、イベントの現地タイムゾーンの時間値が Unix タイムの時間で格納されています。この値は、イベントのタイムスタンプ (_time の値)から抽出されます。date_zone を使って、オフセットを分で指定(-720 ~ 720 の範囲)してイベントのタイムゾーンをオフセットします。

例： 現地(ローカル)のタイムゾーンで発生した「apache」を含むイベントを検索する

```
apache date_zone=local
```

マルチバリューでフィールドを操作する

マルチバリューでフィールドを操作する

Splunk は、検索時にマルチバリューフィールドを構文解析し、検索パイプラインでその値を処理できるようにします。mマルチバリューフィールドを使って作業できる検索コマンドは、makemv、mvcombine、mvexpand、nomv などです。これらの (または他の) コマンドについては、「検索リファレンス」およびこのページの例を参照してください。

fields.conf にマルチバリューフィールドを設定して、1つ以上のフィールド値を1つの抽出されたフィールド値で認識する方法を Splunk に指示します。\$SPLUNK_HOME/etc/system/local/、または\$SPLUNK_HOME/etc/apps/の独自のカスタムアプリケーションディレクトリにある fields.conf を編集します。その方法については、ナレッジマネージャマニュアルの「複数の値フィールドの設定」を参照してください。

例

nomv を使って複数の値フィールドを1つの値に変換する

nomv コマンドを使って、指定したマルチバリューフィールドの値を1つの値に変換できます。nomv コマンドは、fields.conf の複数の値フィールドの構成設定を上書きします。

この例の sendmail イベントでは、senders フィールドの値を1つの値に統合します。

```
eventtype="sendmail" | nomv senders
```

makemv を使ってマルチバリューフィールドに分割する

makemv コマンドを使って、マルチバリューフィールドを複数の独立した値フィールドに分割します。この例の sendmail 検索結果では、「senders」フィールドの値を複数のフィールド値に分割します。

```
eventtype="sendmail" | makemv delim="," senders
```

フィールド値を分割した後は、各値を他のコマンドを通じてパイプできます。例えば、上位の送信者を表示できます。

```
eventtype="sendmail" | makemv delim="," senders | top senders
```

mvexpand を使ってマルチバリューフィールドを基に複数のイベントを作成する

mvexpand コマンドを使って、マルチバリューフィールドの値をそれぞれの値に対応する別のイベントに展開します。この例では、Splunk は、マルチバリューフィールド「foo」のそれぞれの値に対応する新しいイベントを作成します。

```
... | mvexpand foo
```

mvcombine を使って類似するイベントからマルチバリューフィールドを作成する

「foo」の値を区切り文字 ":" で結合します。

```
... | mvcombine delim=":" foo
```

タグとエイリアスフィールドの値

タグとエイリアスフィールドの値

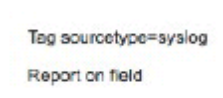
データには、関連したフィールド値を持つイベントのグループがある場合があります。これらのフィールドのグループを効率よく検索する手助けとして、フィールド値にタグを割り当てることができます。さまざまな抽出フィールド(イベントタイプ、ホスト、ソース、ソースタイプなど)に複数のタグを割り当てることができます。

詳しくは、ナリ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。

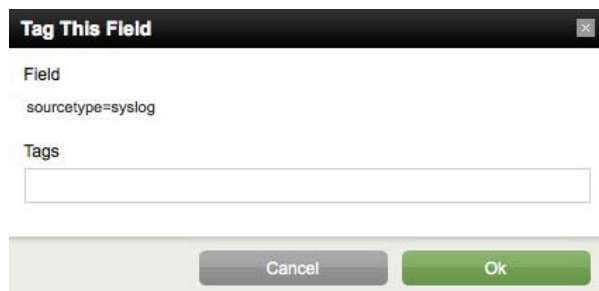
フィールド値にタグおよびエイリアスを付ける方法

フィールド値にタグを付ける

Splunk Web を使って検索結果のフィールド値に直接タグを付けることができます。結果に抽出されたイベントにタグを付けたいフィールド値がある場合は、フィールド値の横にある矢印をクリックします。その値にタグを付けるためのドロップダウンメニューが開きます。例えば、syslog のソースタイプを選択すると、以下が表示されます。



フィールド値に対してタグアクションを選択した後は、「このフィールドにタグを付ける」ポップアップウィンドウにタグ(複数可)を追加します。



フィールド名にエイリアスを付ける

フィールド名に複数のエイリアスを追加できます。また、このフィールドエイリアスを使って異なるフィールド名を正規化できます。この操作は、オリジナルのフィールド名の名前を変更したり、削除したりしません。フィールドにエイリアスを付けた後は、そのエイリアス名を使って検索できます。フィールド名にエイリアスをつけるには、props.conf にアクセスする必要があります。その方法については、ナリッジマネージャマニュアルの「フィールドにエイリアスを作

成」を参照してください。

ソースタイプの名前を変更する

props.conf でソースタイプを設定するとき、ソースタイプの名前を変更できます。複数のソースタイプで同じ名前を共有できます。この方法は、検索のために一連のソースタイプをグループ化する際に便利です。例えば、「-too_small」を含むソースタイプ名を正規化して、分類子を取り除くことができます。その方法については、ナリッジマネージャマニュアルの「ソースタイプの名前を変更する」を参照してください。

タグ付きフィールド値を検索する

タグの検索には 2 つの方法があります。フィールドの値に関連付けられているタグを検索する場合は、次の構文を使います。

```
tag=<tagname>
```

また、特定のフィールドの値に関連付けられているタグを検索する場合は、次の構文を使います。

```
tag::<field>=<tagname>
```

タグの検索にワイルドカードを使う

イベントタイプとタグを含むキーワードとフィールドの値を検索する場合は、アスタリスク(*)のワイルドカードが使えます。

例えば、IP-src や IP-dst など、タイプが異なる IP アドレスに対するイベントタイプのタグが複数ある場合、以下の構文ですべて検索できます。

```
tag::eventtype=IP-*
```

タグに「local」を含むすべてのホストを検索する場合は、以下の構文でタグを検索します。

```
tag::host=*local*
```

また、タグが付けられていないイベントタイプのイベントを検索する場合は、次のブーリアン演算子で検索します。

```
NOT tag::eventtype=*
```

新しいフィールドの抽出と追加

新しいフィールドの抽出と追加

データについての理解を深めるほど、使用したい情報をより多く探すことができます。この情報をイベントから抽出するには、フィールドに保存して検索に利用する、またはレポートを作成するなど、さまざまな方法があります。また、外部ソース(CSV ファイル、スクリプトの出力など)から情報を探してイベントデータに追加することもできます。

ここでは、以下について説明します。

- Splunk Web を使って対話形式でフィールドを抽出して保存する方法
- イベントからフィールドを抽出する検索コマンドについての詳細
- コンフィギュレーションファイルを使ってインデックスタイムにフィールド抽出を定義する方法
- ルックアップテーブルを使ってフィールドを検索し、イベントに新しいフィールドを追加する方法

Splunk Web を使って対話形式でフィールドを抽出する

Splunk Web の対話式フィールド抽出機能(IFX)を使ってカスタムフィールドを同時に作成できます。IFX にアクセスするには、検索を実行して、検索結果のタイムスタンプの下に表示されるドロップダウンから「フィールドを抽出する」を選択します。IFX を使うと、ホスト、ソース、またはソースタイプの値を基に一度に 1 つのフィールドを抽出できるようにします。詳しくは、本書の対話式フィールド抽出の例を参照してください。

検索コマンドを使ったフィールドの抽出

各種検索コマンドを使って、さまざまな方法でフィールドを抽出できます。コマンド一覧をここに示します。各コマンドの使い方の例については、本書の「検索コマンドを使ったフィールドの抽出」を参照してください。

- `rex` は、Perl の正規表記で名前が付けられたグループを使ってフィールド抽出を実行します。
- `extract` (または `kv`, "key/value" の略) は、デフォルトパターンを使ってフィールドおよび値を明確に抽出します。
- `multikv` は、複数ライン、表形式のイベントからフィールドおよび値を抽出します。
- `xmlkv` は、xml 形式のイベントデータからフィールドおよび値を抽出します。
- `kvform` は、規定のフォームテンプレートを基にフィールドおよび値を抽出します。

conf ファイルでフィールド抽出を定義する

IFX を使って追加したフィールド抽出ルールは、設定ファイルに書き込まれます。このファイルへのアクセス権がある場合は、設定ファイルを直接編集することもできます。詳しくは、ナリッジマネージャマニュアルの「設定ファイルを通じて検索時間にフィールドを追加する」を参照してください。

外部データソースのフィールドを探す

ルックアップテーブルなどの外部ソースのフィールドとイベントのフィールドを比較して、一致するものをイベントの追加情報として追加できます。この機能は、「フィールド検索」と呼びます。

- これは、次の用途などに使われます。
- DNS および DNS 逆引き
- URL メタデータの解釈
- アセット検索

ユーザーデータベースの情報検索

ルックアップテーブルは、固定 CSV ファイルまたは Python スクリプトの出力にすることができます。また、検索結果を使って CSV ファイルを作成して、それをルックアップテーブルに設定できます。フィールドルックアップとその定義例については、K ナリッジマネージャマニュアルの「外部データソースからフィールドを追加する」を参照してください。

フィールドルックアップを設定したら、検索 App で `lookup` コマンドを使って呼び出すことができます。

例: ホスト名または IP アドレスを引数にして DNS 検索および DNS 逆引きする Python スクリプトを参照するフィールドルックアップ、`dnslookup` を使い、この検索コマンドで、イベントのホスト名の値とテーブルのホスト名の値が一致するイベントを検索し、そのイベントに対応する IP アドレスの値を追加する

```
... | lookup dnslookup host OUTPUT ip
```

検索コマンドを使ったフィールドの抽出

検索コマンドを使ったフィールドの抽出

「新しいフィールドの抽出と追加」で説明したとおり、各種検索コマンドを使ってさまざまな方法でフィールドを抽出することができます。ここでは、さらに `rex`、`extract`、`multikv`、`xmlkv`、`kvform` コマンドの使用例について説明します。

正規表記によるフィールドの抽出

`rex` 検索コマンドは、検索文字列に含めたグループを指定する Perl の正規表記を使ってフィールドの抽出を行います。この正規表記でローイベントのセグメントを検索し、その値をフィールドに保存します。

この例では、Splunk は「From:」および「To:」文字列の後に発生する単語を照合し、それぞれの値を「from」および「to」フィールドに保存します。

```
... | rex field=_raw "From: (?<from>.*) To: (?<to>.*)"
```

ローイベントに「From: Susan To: Bob」が格納されている場合は、Splunk は「from=Susan」および「to=Bob」をフィールド名と値のペアで抽出します。

検索結果からフィールド値を強制抽出

conf ファイルの定義を強制抽出

抽出(または「key/value」用 `kv`)検索コマンドは、検索結果から強制的にフィールドと値を抽出します。引数を指定しないで `extract` を使うと、Splunk は `props.conf` に追加されたフィールド抽出スタanza(文字列)を使ってフィールドを抽出します。`extract` を使って、手作業で `conf` ファイルに追加したフィールドを抽出するテストができます。

テーブル形式のイベントからフィールドを抽出

`multikv` を使って、複数ライン、表形式のイベントからフィールドおよび値を強制抽出します。このコマンドは、各表の行に対して新しくイベントを作成し、表のタイトルからフィールド名を付けます。

xml 形式のイベントからフィールドを抽出

`xmlkv` コマンドは、ウェブページのトランザクションなど、xml 形式のイベントデータからフィールドおよび値を強制抽出します。

フォームテンプレートを基にイベントからフィールドを抽出

`kvform` コマンドは、予め定義され、`$SPLUNK_HOME/etc/system/local/` または、カスタムアプリケーションのディレクトリ `$SPLUNK_HOME/etc/apps` に保存されているフォームテンプレートを基に、フィールドと値のペアでイベントを抽出します。例えば、`form=sales_order` の場合、Splunk は、`sales_order.form` を検索して、このフォームに対して処理されたすべてのイベントの値を抽出しようとします。

Splunk Web を使って対話形式でフィールドを抽出する

Splunk Web を使って対話形式でフィールドを抽出する

この例では、対話型フィールド抽出(IFX)を使ってデータから IP アドレスを抽出する方法を Splunk に指示します。

概要

IFX にフィールドの抽出方法を指示するには、抽出を適用するホスト、ソース、またはソースタイプなどを指定します。次に、抽出するフィールドの値(例)を指示します。この値は、サンプルイベントに存在する値である必要があります。指示が終わると、IFX は、正規表現を生成します。この正規表現は、編集、テスト、保存が可能です。

注記： 正規表記を手作業で編集しない限り、IFX は一度に 1 つのフィールドを抽出します。

正規表現の生成

1. IFX にアクセスするには、最初に抽出するフィールド値を含むイベントを生成する検索を実行します。

ここでは、IP アドレスを抽出するため、以下のように指定して Apache アクセスログを検索します。

```
sourcetype=access_combined
```

2. 検索結果から、該当するフィールド値(この場合は IP アドレス)を含むイベントを検索します。検索結果のタイプスタンプの下に表示されるドロップダウンリストから「フィールドの抽出」を選択します。

IFX は、新しいウィンドウ「フィールドの抽出」を開きます。

3. **フィールド検索を制限するホスト、ソース、またはソースタイプ**を選択します。

このドロップダウンには、手順 2 で選択したイベントのフィールド値が表示されます。別のホスト、ソース、またはソースタイプの値を選択する場合は、ウィンドウをいったん閉じて、検索結果から別のイベントを選択する、または新たに検索を実行します。

4. Splunk に抽出させたいフィールドの**値(例)**を入力します。値は、**サンプルイベントの一覧**からコピーして貼り付けできます。このとき、結果がわかりやすいように、複数の値を入力してください。

注記： サンプルイベントの一覧は、検索結果から選択したイベントと、指定したフィールドの制限を基にしています。フィールドの制限を変更すると、この一覧の内容が変わりますが、ユーザーが指定したオリジナルのイベントのデータであることには変わりありません。

5. 「**生成**」をクリックします。

Splunk は、フィールドの値と一致するよう生成された正規表記パターンと、生成パターンを基に抽出されたサンプルを一覧表示します。

抽出されたサンプル値が抽出したい値と一致しない場合は、値の横にある灰色のアイコン(X)をクリックして削除します。Splunk は、それを「不正確な抽出結果」に移動して、抽出したくない値として表示します。IFX は、この変更を反映させるよう生成パターンを更新します。削除した後に新しい値を再度追加して、その値の横にあるアイコン(+)をクリックして正規表現をリセットできます。

新しいフィールドを保存する前に、大量のデータに対して正規表現をテストしたり、パターンを手作業で編集すること

もできます。

生成した正規表現をテストする

Splunk で生成した正規表現パターンをテストするには、**テスト**をクリックします。

以下の検索結果を含む新しい検索ウィンドウが開きます。

- ホスト、ソース、またはソースタイプ条件 (最大 1 万件)
- 正規表現を実行する rex コマンド。Splunk が FIELDNAME で生成し、重複する値を削除した後のコマンド

生成した正規表現を編集する

正規表現の記述に慣れてきたら、Splunk で作成した後に手作業でパターンを編集できます。

注記： 正規表現の編集では、正規表現を保存する際に名前を指定するため、抽出した「FIELDNAME」の名前を変更する必要はありません。

抽出したフィールドを保存する

新しいフィールドを保存するには、**保存**をクリックします。

「フィールド抽出を保存」ウィンドウで、新しいフィールド名を指定します。

重要： Splunk で指定できるフィールド名は、以下のアルファベット文字またはアンダーラインのみです。

- フィールド名に指定できる文字：a-z, A-Z, 0-9, _
- フィールド名の最初の文字に 0-9 または _ は指定できません。(アンダースコア(_)から始まる名前は、Splunk の内部変数に使用されています。)

トランザクションの特定

トランザクションの特定

トランザクションは、グループ化したいイベントを集めたメタイベントです。トランザクションは、複数のソースにおよぶことがあります。

トランザクションのタイプは、Splunk のフィールドとして保存されたトランザクションの設定タイプです。

通常、トランザクションの検索は、1つの物理的なイベントを示す1つのメタイベントとして複数のイベントをグループ化するときを使用します。例えば、メモリ不足の問題が発生すると複数のデータベースイベントがログに記録されます。そのログをすべてトランザクションとしてグループ化することができます。トランザクションコマンドを使用して、トランザクションを定義する、または transactiontypes.conf に指定されているトランザクションオプションを上書きします。

例： ある一定の時間内にひとりのユーザー(またはクライアント IP アドレス)が検索したすべてのウェブページをグループ化する検索を実行する

この検索は、アクセスログからイベントを抽出し、(3 時間の間に)双方で 5 分以内に発生した同じ clientip 値を共有するイベントからトランザクションを作成します。

```
sourcetype=access_combined | transaction fields=clientip maxpause=5m  
maxspan=3h
```

使い方および使用例などの詳細は、ナリッジマネージャマニュアルの「イベントをトランザクションヘグループ化」章を参照してください。

検索を保存して検索結果を共有する

検索を保存して検索結果を共有する

期待する検索結果を抽出する検索を実行した後は、検索文字列(後で再利用するため)または、検索結果(後で結果を見るため)を保存できます。

検索結果を csv、xml、html などのファイルにエクスポートしたり、受信者が直接検索ジョブを実行できる URL リンクを知らせて他の人と検索結果を共有できます。

保存済みの検索の作成

検索の保存を選択すると完了した、または終了した検索を保存します。(また、Splunk 管理の保存済み検索ページで新しい検索をクリックすると、新しく保存済み検索を作成できます。)

少なくとも、保存済み検索には、検索文字列と、その検索に関連する時間範囲、検索名(検索を保存した後に**検索とレポート**で表示される名前)を含んでいます。保存済み検索を実行すると、Splunk は、その検索で定義した検索文字列と時間範囲を使って新しい検索ジョブを作成します。

注記： 検索 App のナビゲーションルールを変更して、検索が**検索とレポート**ではなく、ナビゲーションの上位レベルのデフォルト位置に保存されるようにできます。詳しくは、下の「保存済み検索へのナビゲーションの管理する」を参照してください。

検索を保存するとき、その検索を実行する時期を指定したり、アラート条件を設定したりできます。つまり、例えば、特定の条件を満たした場合に、電子メールまたは RSS で検索結果を自分(または別の人)に送信するよう設定できます。

予約検索およびアラートの設定の仕方については、本書の「再発条件のモニタリング」を参照してください。

初めて検索を保存するときは、保存したユーザーのみが表示および使用できます。また、検索を保存したときに実行した app に関連付けられます。他のユーザーと保存済み検索を共有する方法、および他の Splunk app で保存済み検索を使用する方法については、本書の「Splunk の知識オブジェクトの共有と活用」を参照してください。

注記： 保存済み検索には、チャート形成パラメータは**含まれません**。検索にレポートコマンドを含み、独自の形式(デフォルトの棒グラフではなく、円グラフを生成し、タイトル、X 軸、Y 軸に特定の文字を表示するなど)でチャートを生成したい場合は、必ず **レポートビルダからのレポートとして保存してください**。検索として保存すると、レポートビルダのチャート用に設定した書式は失われます。特に、特別な方法でダッシュボードにチャートを表示する場合には重要ですので注意が必要です。

詳しくは、本書の「レポートを保存して共有する」および「ダッシュボードエディタで簡単なダッシュボードを作成する」を参照してください。

検索結果の保存

実行した検索結果を保存して後から見直す場合は、アクションドロップダウンから結果を保存を選択します。この作業では、ジョブマネジャでアクセス可能な検索ジョブを保存します。

ジョブマネジャで検索ジョブを管理する方法については、本書の「検索ジョブの監視」を参照してください。

検索結果の共有

検索結果を他人と共有したい場合は、いくつかのオプションが用意されています。

- **イベントデータをファイルにエクスポートする。**アクションドロップダウンメニューから結果のエクスポート...を選択して、検索結果からイベントデータを、csv、raw、xml ファイルなどにエクスポートします。このファイルは、他社製の図表用アプリケーションで保存および使用できます。
- **結果のリンクを取得(または共有)する。**アクションドロップダウンメニューから結果へのリンクを入手...を選択して、結果レポートの URL リンクを入手します。このリンクを関係者と共有できます。このリンクには、Splunk のインスタンスへのアクセスが必要です。

注記： 結果へのリンクを入手...を選択すると検索ジョブが自動的に保存されます。保存されたジョブは、ジョブページからアクセスできます。結果へのリンクを入手ポップアップウィンドウで保存処理を無効にできます。

保存済み検索へのナビゲーションを管理する

検索を保存すると、ナビゲーションメニューの上位レベルのいずれかのドロップダウンリストに表示されます。例えば、検索 App では、デフォルトで新しい検索は**検索とレポート**リストに表示されます。

App に対して書き込み許可がある場合は、このデフォルトの場所を変更できます。また、名前を特定のキーワードで検索した場合にナビゲーションメニューのカテゴリーを指定して自動保存できるようにも設定できます。例えば、名前に「website」を含む保存済み検索を、ナビゲーションメニューのウェブサイト関連の検索リストに自動的に保存します。また、検索をデフォルトのリストからナビゲーションメニューの上位レベルの異なる場所に移動できます。

詳しくは、ナリッジマネジャマニュアルの「保存済み検索とレポートの定義」およびデベロッパーマニュアルの「ナビゲーションメニューのカスタマイズ」を参照してください。

検索ジョブの監視

検索ジョブの監視

検索を実行またはレポートを生成するとき、Splunk は、検索またはレポートにより返されたイベントデータを含むジョブを作成します。ジョブマネジャを使うと、最近生成したジョブおよび保存したジョブを表示および監視できます。

ただし、ジョブは保存済み検索や保存済みレポートと同じではありません。保存済み検索や保存済みレポートには、その検索やレポートの実行に使われたデータ、つまり、検索実行に使われた検索文字列や時間引数などが含まれます。ジョブは、以前に実行した検索およびレポートの検索結果(アーチファクト)です。ジョブには、検索やレポートを実行した結果が格納されています。ジョブは、予約検索、およびユーザーインターフェースを使って手動で実行された検索やレポートから作られます。

検索の保存については、本書の「検索の保存」を参照してください。レポートの保存については、本書の「レポートの保存」を参照してください。

画面右上の**ジョブリンク**をクリックすると、ジョブマネージャにアクセスします。

注記: バックグラウンドで検索を実行している場合は、**ジョブリンク**に実行中のジョブ数が括弧の中に表示されます。

ジョブマネージャは以下の場合に使用します。

- 最近作成したジョブの一覧を表示する、または保存して後から見直し、ジョブの統計(実効時間、検索したイベント総数など)を見る
- ジョブマネージャに一覧表示されるジョブの結果を見る
 - ◆ 検索関連のジョブの場合は、検索ビューで結果を見ることができる
 - ◆ レポート関連のジョブ場合は、レポートビルダのレポートのフォーマット設定ページで結果を見ることができる
 - ◆ **注記:** ジョブマネージャウィンドウを開いている間にジョブがキャンセルされても、ジョブマネージャの一覧に表示され続けますが、見ることはできません。ジョブマネージャを閉じてから開くと、キャンセルされたジョブは表示されません。
- バックグラウンドで実行されているジョブや予約検索で実行されるジョブの進捗を確認して、必要に応じて一時停止または停止する
- ジョブマネージャに表示された検索またはレポートを保存または削除する(表示および管理する権限が必要)

注記: ジョブマネージャでは、表示および管理する権限のある検索ジョブしか表示できません。

保存されていない検索ジョブは完了した後、設定された時間が経過すると有効期限が切れます。手動で実行した検索ジョブのデフォルトの保存期間は、15分です。(通常、予約検索で実行された検索ジョブの保存期間はさらに短い時間が設定されています。) **期限切れ**欄に、一覧されている各ジョブがシステムから削除されるまでの保存期間が記載されています。期限が過ぎた検索ジョブを表示する、または共有する場合は、保存してください。

ジョブの有効期限が切れていなければジョブマネージャページにアクセスしなくても、ほとんどのビューで、最後に実行した検索またはレポートを保存できます。

- 検索ジョブを保存する場合は、検索ビューの**アクション**ドロップダウンリストから**結果の保存**を選択します。
- レポートジョブを保存する場合は、レポートビルダのレポート生成ページの**保存メニュー**から**検索結果だけを保存**を選択します。

詳しくは、管理者マニュアルの「ジョブとジョブ管理について」を参照してください。

Splunk の知識オブジェクトの共有と活用

Splunk の知識オブジェクトの共有と活用

Splunk では、保存済み検索、保存済みレポート、およびイベントタイプはすべて Splunk の知識オブジェクトです。知識オブジェクトは、Splunk データを充実させる項目で、必要な情報を効率よく探すために役立ちます。

ここでは、Splunk 管理を使って、保存済み検索、保存済みレポート、イベントタイプを共有および活用する方法について説明します。この情報は、navs や views、および Python ベースの検索コマンドなどの知識オブジェクトにも適用されます。これらの知識オブジェクトについては、ナリッジマネージャマニュアルを参照してください。

注記: Splunk の知識オブジェクトには、他にも、フィールド、ソースタイプ、イベントタイプ、タグ、その他の項目

がありますが、これらは現在共有を制御できません。

検索、レポート、イベントタイプなどのオブジェクトを初めて保存するときは、作成したユーザーのみが作成した app でしか利用できません。特定のタイプの知識オブジェクトをさまざまな app から複数のユーザーで活用できるようにするには、以下の操作を行います。(これには操作可能な権限が必要です)

- オブジェクトをあらゆるアプリケーションでグローバルに利用可能にする
- オブジェクトの権限を別の役割またはユーザーに設定する
- オブジェクトを特定の app またはグローバルな app ですべてのユーザーが利用できるようにする

役割またはユーザーをオブジェクトを共有する

保存検索などの Splunk 知識オブジェクトを役割またはユーザーと共有するには、オブジェクトの権限を編集します。オブジェクトを初めて作成したときは、権限は作成ユーザーのみに限定されています。他のユーザーは同じアプリケーションを使用してもアクセスできません。

注記： オブジェクトを操作する許可を役割に対して与えると、その許可をその役割が割り当てられているすべてのユーザーに効率よく転送します。

オブジェクトに対する許可を変更するには、以下の操作を行います。

1. **管理**リンクを選択して Splunk 管理へ移動します。許可を更新したいオブジェクトのタイプに対するページ(保存済み検索やイベントタイプなど)を指定します。
2. 自分が生成したオブジェクトを選択(必要に応じてページ上部のフィルタリングフィールドを使う)してから、**権限**リンクをクリックします。
3. 新しい保存済み検索、保存済みレポート、イベントタイプの許可を編集するときは、ページ左上にあるチェックボックスを選択して、オブジェクトの共有を有効にします。オブジェクトの共有が無効になっていると、許可を更新できません。
4. アクセス制御リストで、オブジェクトに対する権限を設定します。リストで、オブジェクトに対するアクセス権を与えるユーザーおよび役割を選択します。各ユーザーおよび役割に**読み込み**または**書き込み**の許可を選択します。
 - **読み込み**では、該当するユーザーまたは役割がオブジェクトを表示および使用できますが、編集できません。例えば、保存済み検索の場合、**検索**ドロップダウンで見る(検索を作成したアプリケーションを使用している、またはアプリケーションの使用が許可されている場合に限る)または必要に応じて検索を実行することができます。ただし、その保存済み検索の詳細ページを表示したり、編集および同じ名前で作成することはできません。
 - **書き込み**では、該当するユーザーまたは役割がそのオブジェクトを使用し、必要に応じて詳細を更新することができます。
 - ユーザーまたは役割に**読み込み**または**書き込み**のいずれも選択されていない場合は、どのアプリケーションからもそのオブジェクトを表示またはアクセスできません。

App を使うすべてのユーザーでオブジェクトを利用可能にする

すべてのユーザーと役割に対してオブジェクトの権限を与えたい場合は、**世界** 役割 を与えます。例えば、**世界**と**読**

み込み の権限を与えると、誰でもそのオブジェクトを表示して使用することができます。また、管理者を選択して 書き込み(編集)許可を与えることができます。

オブジェクトをあらゆる app でグローバルに利用可能にする

初めてオブジェクトを作成したときには、作成した app と作成したユーザーでしか利用できません。

すべての app のユーザーが利用できるようにするには、そのオブジェクトの権限ページを開き(上述の手順参照)、**検索表示**の設定をこの app だけからすべての App に変更します。

注記： すべてのアプリケーションでオブジェクトを利用できるようにした後は、ユーザーおよび役割レベルを見直して、閲覧者が適切であるかどうかを確認してください。

自動モニタリング

再発条件のモニタリング

再発条件のモニタリング

これまでの章をお読みいただいた方は、Splunkのパワフルな検索機能の使い方やシステムのイベントデータについての理解が深まっていると思います。しかし、これだけではIT業界で誰もが日常的に直面する無数の再発状況を把握することはできません。常にひとりで検索を実行することはできないからです。

そこで、Splunk は、最も柔軟に監視するツールとしてデザインされています。実行される検索はどれも定期的に自動実行するよう設定できます。予約検索を設定して、特定の状況が発生したら、ユーザーや関係者にアラートを送信するよう設定できます。空のショッピングカー、強引なファイアウォール攻撃、サーバーシステムのエラーなど、さまざまなしきい値や傾向を基にしてアラートを設定できます。

この章では、以下について説明します。

- 保存済み検索のスケジューリング
- 予約検索に対するアラート条件の設定

保存検索のスケジューリング

保存検索のスケジューリング

検索ベースのアラートを定義する前に、まず、検索を保存し、それを Splunk で定期的に自動実行するよう設定する必要があります。

保存検索については、本書の「検索を保存して検索結果を共有する」を参照してください。

保存済み検索のスケジューリングでは、30 分ごと、毎日正午、月初めの月曜日深夜など、実行するタイミングを定義します。

このページでは、Splunk Web を使った検索のスケジューリングについて説明します。検索スケジューリングの管理および CLI による警告については、管理者マニュアルの「アラートの働き」を参照してください。

検索スケジュール

検索のスケジュール設定は、検索を保存するとき、または後で行えます。

保存と同時に行う場合は、終了または完了した検索で**検索の保存**を選択した後に表示される検索保存ウィンドウの制御を使います。まず、この**検索をスケジュールする**ボックスをクリックします。

また、以前の保存済み検索をスケジュールする場合は、以下の操作で管理の保存済み検索ページを開きます。

1. 右上の**管理**リンクをクリックします。
2. **保存済み検索**を選択します。

3. スケジュールする検索を探して(または、検索スケジュールを更新して)、名前を選択します。検索のリストが長すぎる場合は、検索の保存ページ上部にあるフィルタを使って検索リストを絞り込みます。App のコンテンツでフィルタリングできます(すべての app でグローバルに共有するよう設定されていない場合は、app が検索に関連付けられている必要があります。)

注記： 自分が作成した保存済み検索または共有および変更可能な保存済み検索のみ編集することができます。ほとんどの検索は、すべてのappでグローバルな利用可能に設定されていない限り、特定のアプリケーションに関連付けられているため、注意が必要です。保存済み検索など、Splunkの知識オブジェクトの共有と変更については、本書の「保存済み検索の共有と活用の管理」を参照してください。

新しいまたは既存の検索の保存済み検索ウィンドウを表示できたら、保存検索のスケジュール設定の手順は同じです。

検索の基本的な詳細(名前、説明、時間範囲など)の入力または見直しが終わったら、検索のスケジュールチェックボックスをクリックします。検索のスケジュールリング制御画面が表示されます。

次に、実行するタイミングを決める方法を選びます。基本またはクローンのいずれかを選択します。

- 基本では、検索を実行するタイミングを予め決められた一覧から選択します。例えば、検索を次の間隔で実行するよう設定します： 毎分、5分、30分、1時間、12時間、毎日深夜零時、毎日午後4時、毎日午後6時、土曜日の深夜零時
- クローンでは、クローン記述を使って予約検索のタイミングを定義します。

以下に クローンの例を示します。

```
* / 5 * * * * : Every 5 minutes * / 30 * * * * : Every 30 minutes 0 * / 12 * * * : Every 12 hours, on the hour * / 20 * * * 1-5 : Every 20 minutes, Monday through Friday 0 9 1-7 * 1 : First Monday of each month, at 9am.
```

検索に特定の時間範囲を追加する

特定の時間範囲内にすべての結果を取得できるようにするには、検索定義(開始時間と終了時間)の時間範囲フィールドを設定して、検索に特定の時間範囲を指定します。これは特に、イベントデータが生成されたときにインデックスマシンに到達しない分散検索の設定に有効です。この場合、検索を数分遅らせるようにスケジュールすると効果的です。

この例では、毎時 30 分に実行する検索を設定し、検索を実行する 1 時間半前のからその時間分のイベントデータを収集しています。(例えば、検索が 3 時半に実行された場合、午後 2 時から 3 時の間に Splunk がインデックス付けしたイベントデータを収集します)

- 開始時間値に「-90m」、終了時間値に「-30m」を設定します。
- クローン記述に「30 * * * *」と設定して、検索を毎時間 30 分おきに実行するように設定します。
- 検索定義で時間範囲を定義するための構文については、本書の「相対時間変更の構文」を参照してください。

完了検索の保管時間の設定

予約検索を頻繁に実行する場合で、特に、特定の状況下でアラートを発行するよう設定している場合や、アラートが発生した検索結果を送信するよう設定している場合は、完了した検索結果をシステム長く保管したくないことがあります。保有時間フィールドを使って、Splunk が予約検索で完了した検索結果を保管する期間を設定できます。

<number> (秒)または<number>p (期間)のいずれかを入力します。期間は、予約検索を実行する時間範囲と同様です。検索を毎時間実行し、保管期間を 10p にすると、完了した検索結果を 10 時間保管します。

予約検索に対するアラート条件の設定

予約検索に対するアラート条件の設定

検索をスケジューリングした後は、その検索を基にアラートを設定できます。

基本条件アラートを設定して、その検索に関与する複数のイベント、ソース、またはホストを監視します。

条件を満たすと、Splunk は電子メールで通知し、カスタムスクリプトまたは RSS を実行します。

また、**詳細条件アラート**を定義すると、予約検索の結果を検索文字列を基に評価します。ここでは、双方の検索の設定方法について説明します。

アラートを定義した後は、Splunk でアラートの発生をユーザーに知らせるための通知方法(電子メール、スクリプト、rss など)を設定します。

基本条件アラートの定義

この手順に従って、イベント、ホスト、ソースに関連するしきい値について通知する基本条件アラートを定義します。

1. **アクションの実行条件**ドロップダウンメニューで、もしイベントの数が、もしソースの数が、もしホストの数がのいずれかを選択します。この 3 つの値から 1 つを選択すると、次の 2 つの基本条件アラート用のフィールドが表示されます。(または、常にを選択すると、毎回検索を実行した際に Splunk がユーザーに通知します。これは、検索を不定期に実行する場合や常に結果を見たい場合に便利です。)

2. **アクションの実行条件**フィールドの下に表示されるドロップダウンから比較演算子(*is greater than*、*is less than*、*is equal to*、*rises by*、*drops by*)を選択します。

3. 比較演算子ドロップダウンに隣接するフィールドに、アラート用のしきい値を整数で入力します。

例えば、検索で返されたイベント数が 10 のしきい値より大きい場合にアラートを通知するよう設定します。

詳細条件アラートの定義

詳細条件アラートを有効にすると、条件検索の結果を基にアラート条件を設定できます。これは、予約検索で返される結果に適用されます。 Splunk は、条件検索が 1 つ以上の結果を返した場合にアラートを発行します。

検索のアラート条件を基にすることにより、アラートを発行する特定の条件を定義し、誤判定によるアラートの発生を減らすことができます。

この手順に従って詳細条件アラートを定義します。

1. **アクションの実行条件**ドロップダウンメニューで**カスタム条件を満たしたときに**を選択します。**カスタム検索**

2. 条件フィールドが表示されます。

カスタム検索条件フィールドに検索条件を入力します。

例えば、次のカスタム検索条件を実行して、条件検索の結果が 100 件以上の場合に通知する詳細条件アラートを設定します。 `stats count | search count > 100`

アラートを通知する方法の設定

Splunk がどのように通知するかを指定します。Splunk が電子メールで通知するよう設定できます。アラートが発行された場合に Splunk でシェルスクリプトを実行するように設定することもできます。

Splunk からユーザーと他の関係者に電子メールを送信するようするには、**メールの送信フィールド**に関連する電子メールアドレスをコンマで区切り、入力します。

アラートメールにアラートを発行した検索結果を添付したい場合は、**メールに結果を含める**を選択します。

注記： Splunk でアラートメールを送信するようするには、`alert_actions.conf` にアラートに対応する電子メールオプションを指定する必要があります。

- Splunk がメール送信に使う SMTP メールサーバーと送信元の電子メールアドレスを指定します。
- 題名と電子メールのフォーマットを指定します。
- アラートの送信先の電子メールアドレスを指定します。

詳しくは、管理者マニュアルの「`alert_actions.conf`」を参照してください。

アラート条件を満たした際に Splunk でシェルスクリプトを実行したい場合は、**シェルスクリプトの実行のトリガ**を選択して、Splunk が実行するスクリプトのファイル名を入力します。例えば、アラートにより SNMP トラップ通知を発行して、ネットワークシステム管理コンソールなど、他のシステムに送信するスクリプトを実行できます。ほかにも、アラート条件を満たした場合に、API を呼び出して、別のシステムに発生イベントを送信するスクリプトを実行することもできます。

注記： セキュリティのため、すべてのアラートスクリプトは、必ず `$SPLUNK_HOME/bin/scripts` ディレクトリに保存されます。このディレクトリは、Splunk がアラートによりトリガされるスクリプトを探す場所です。

`savedsearches.conf` を使ったアラートの設定など、アラートの設定については、管理マニュアルのアラートの節を参照してください。

表示するフィールドの指定

アラートを受信すると、Splunk は、すべてのフィールドを検索に含めます。保存済み検索を編集して、含める(または除外する)フィールドを指定します。

フィールドを除外するには、検索を `fields - $FIELDNAME` にパイプします。

フィールドを追加するには、検索を `fields + $FIELDNAME` にパイプします。

複数のフィールドを指定して、1つの文字列に含める(または除外する)ことができます。例えば、検索フィールドに以下のように指定します。

```
yoursearch | fields - $FIELD1,$FIELD2 + $FIELD3,$FIELD4
```

受信するアラートから、\$FIELD1 および \$FIELD2 を除外して、\$FIELD3 および \$FIELD4 を含めます。

サマリーインデックスを有効にする

サマリーインデックスは、予約検索で実行できるアクションです。サマリーインデックスは、通常、処理に時間がかかり、複数のユーザーが定期的に同様の検索を実行すると性能が低下するため、大量のデータを長い時間をかけて分析/レポートする場合に使用します。

サマリーインデックスを実行するときは、さまざまなタイムスライスのイベントに対して十分な統計(サマリー)を採れる予約検索を指定します。Splunk は、検索を実行する都度、結果を、指定したサマリーインデックスに保存します。その後、サマリーインデックスが基にする大規模のデータセットではなく、この小規模(さらに高速)のサマリーインデックスを使って検索およびレポートを実行します。

この検索でサマリーインデックスを有効にする場合は、**サマリーインデックスを有効にする**を選択します。サマリーインデックスについて、および Splunk Web を使ってサマリーインデックスを設定する方法については、本書の「サマリーインデックスを使ってレポートの効率を上げる」を参照してください。

分析とレポート

レポートとチャートについて

レポートとチャートについて

Splunk のパワフルな IT 検索機能を使って、問題の調査や、企業に関する重要な情報を収集することは、重要な作業の最初の一步です。検索により明らかになった情報を素早く分析する Splunk の機能を利用し、レポートやチャートを見やすく作成します。

この章では、以下について説明します。

- レポートコマンドの主な使い方
- Splunk のレポートビルダを使って総合的なレポートを定義、生成、作成する方法
- 各種レポートやチャートに使える役立つ情報を探す方法
- 企業における日常の業務で重要なデータを示すチャートを含むダッシュボードビューをデザインする方法
- 定期的に大量のデータを処理する場合にレポート作成の効率を上げるサマリーインデックスについて

レポートビルダを起動する

検索を実行すると、時系列の上のジョブステータスバーにレポート作成リンクが表示されます。このリンクをクリックして、レポートの定義、生成、書式の微調整ができるレポートビルダを起動します。

注記： レポートの作成は、検索が完了する前に始めることができます。 Splunk は、検索結果が収集されると、同時に生成したチャートを動的に更新します。

また、レポートビルダには、以下の方法でアクセスできます。

- 検索実施後に、**アクション**ドロップダウンメニューから *レポート作成* をクリックします。
- 検索結果スライダーのフィールドをクリックして、そのフィールドに対応するメニューを表示します。クリックしたフィールドの種類により、時系列の平均、時系列の最大値、時系列の最小値(数値フィールドを選択した場合)、または、時系列の最多値および最多値(文字フィールドを選択した場合)などの対話式メニューによるレポートのリンクが使えます。これらのリンクをクリックすると、Splunkは、該当するリンクによって説明されるチャートを生成するレポートビルダのレポートのフォーマット設定ページを開きます。

注記： 検索文字列にレポートコマンドが含まれる場合は、**レポートを表示** をクリックしてレポートビルダにアクセスします。指定したレポートではすでにレポートを定義しているため、Splunk は、レポート作成プロセスのフォーマット段階にジャンプします。

レポートビルダを使用するために、レポートコマンドについて深く理解している必要はありませんが、理解している事柄が多いほどレポートビルダを効率よく使いこなすことができます。

Splunk では、レポートビルダをポップアップウィンドウで表示するため、レポートパラメータを設定しながら、簡単に検索ページに戻り、検索結果を見直すことができます。

レポートビルダを使って基本的なレポートパラメータを定義する、チャートの形式を指定する、終了したレポートをエクスポートまたは印刷する方法などについては、本書の「レポートの指定とチャートの作成」を参照してください。

注記： レポートジョブは、一定の期間しかシステムに保存されませんのでご注意ください。保存しないと、有効期限がきた時点で、期限切れのレポートジョブでレポートを作成できなくなります。ジョブ管理については、本書の「検索ジョブの監視」を参照してください。

レポートジョブを保存する場合は、レポートビルダのレポート生成ページの**保存メニュー**から**検索結果だけを保存**を選択します。

レポートコマンドの使用

レポートコマンドの使用

検索文字列に直接レポートコマンドを追加して、レポートの作成や検索結果のまとめに役立てることができます。

注記： 検索文字列にレポートコマンドを手作業で追加しなくてもレポートビルダで基本的なレポートを作成できますが、その操作について理解を深める必要があります。フォームベースのインタフェースしか持たないレポートビルダでは、基本的なレポートしか作成できません。Splunk の洗練されたレポート機能をフル活用するためには、検索時系列ビュー、またはレポートビルダの検索バーを使いこなせる程度にレポートコマンドの理解を深めることが必要です。

主なレポートコマンド

ここでは、レポートコマンドの主な分類と検索におけるその使用例について説明します。

主な検索コマンドは以下のとおりです。

- `chart`: 描画したい一連のデータを表示するチャートを作成するときに使用します。チャートのX軸に指定するフィールドを決めます。
- `timechart`: 常にX軸に `_time` を使う「時系列傾向」レポートを作成するときに使います。
- `top`: フィールドの最も標準的な値を表示するチャートを生成します。
- `rare`: フィールドの最も希少な値を表示するチャートを作成します。
- `stats`と`eventstats`: 要約統計データ表示するレポートを作成します。
- `associate`, `correlate`と`diff`: データのフィールド間の関連性、相関、相違を見ることができるレポートを作成します。

注記： 次の例で説明されていますが、レポートコマンドは、必ず「パイプ」記号 (`|`) でリンクさせて検索コマンドの

後に記述します。

chart、timechart、stats、eventstats はすべて、統計演算子とともに使用します。以下に、利用可能な統計演算子を示します。

- count, distinct count
- mean, median, mode
- min, max, range, percentiles
- standard deviation, variance
- sum
- first occurrence, last occurrence

時間ベースのチャートを作成する

timechart レポートコマンドを使って、チャートの X 軸に時間を描画して時系列統計傾向を表示する役立つチャートを作成します。オプションで、データを別のフィールドに分割、つまり、「以下で分ける」フィールドの値でチャートを分割します。通常、これらのレポートは、折れ線グラフまたは面グラフを形成しますが、カラムチャートも形成できます。

例えば、このレポートは、Splunk の内部ログデータを使って、Splunk の時間経過に伴う平均インデックススループット(kbps のインデックス)をプロセッサ別に視覚的に表示します。

```
index=_internal "group=thruput" | timechart avg(instantaneous_eps) by processor
```

時間ベースでないチャートを作成する

チャートレポートコマンドを使用して、一連のデータを表示するチャートを作成します。timechart コマンドと違い、chart コマンドで作成されたチャートは、X 軸に不定のフィールドを使用します。over キーワードを使って X 軸となるフィールドを決めます。

例えば、次のレポートでは、ウェブアクセスデータを使って、平日に訪れた訪問者の平均人数を表示します。

```
index=sampled data sourcetype=access* | chart avg(clientip) over date.wday
```

オプションで、データを別のフィールドに分割、つまり、「以下で分ける」フィールドの値でチャートを分割します。検索に「以下で分ける」節を含める場合は、「以下で分ける」節の前に over 節を記述します。

次のレポートでは、host 別に指定された時間範囲内に各 clientip が処理した総数 (キロバイト) を表示するチャートを作成します。完了したチャートでは、kb の値を Y 軸、clientip を X 軸で表示します。遅延値はホストで区分されています。レポートビルダを使って、このレポートで積み重ね棒グラフを作成することもできます。

```
index=sampled data sourcetype=access* | chart sum(kb) over clientip by host
```

高低を見やすくする

最多および最小レポートコマンドを使って、最大および最小標準値とフィールドの最小値を表示するチャートを作成します。

このコマンドの組み合わせで、ファイアウォール情報を並べ替えて、システムが使用したあて先ポートの上位 100 件を

一覧表示するレポートを作成します。

```
index=sampleddata | top limit=100 dst_port
```

逆に、この文字列は、同じ一連のファイアウォールデータを使って、最も拒否が少ないソースレポートを表示するレポートを作成します。限界を指定しない場合は、最多または最小で表示される値のデフォルト値は、10 です。

```
index=sampleddata action=Deny | rare src_port
```

要約統計データ表示するレポートの作成

stats および eventstats レポートコマンドを使って、フィールドに関連した要約統計データを表示するレポートを作成します。

stats コマンドを使いこなすには、「以下で分ける」節を含める必要があります。例えば、次のレポートでは、十分な情報を含めることができません。

```
sourcetype=access_combined | stats avg(kbps)
```

このレポートでは、ソースタイプが access_combined であるすべてのイベントに対する kbps の平均値を1つの値で示しています。結果のカラムチャートには、1つのカラムしかありません。

しかし、これを以下で分けるフィールドで分割すると、Splunk はそのフィールド別に統計データを表示するレポートを作成します。次のレポートでは、access_combined ログを使って並べ替えて、ホスト別に平均スループット(kbps)を表示するカラムチャートを作成します。

```
sourcetype=access_combined | stats avg(kbps) by host
```

これは、さらに洗練された stats コマンドの例です。このレポートでは、Splunk の CPU 使用量を降順に並べ替えて表示します。

```
index=_internal "group=pipeline" | stats sum(cpu_seconds) by processor | sort sum(cpu_seconds) desc
```

eventstats コマンドは、stats コマンドと全く同じように機能します。ただし、コマンドの集約結果(各イベントに関連する集約のみ)が各イベントのインラインに追加される点が異なります。

as 引数を追加することにより、eventstats 結果に対するフィールド名を指定します。上述の最初の例では、eventstats avg(kbps)演算子の結果を含む新しいフィールドの名前を「avgkbps」とすることができます。

```
sourcetype=access_combined | eventstats avg(kbps)as avgkbps by host
```

このコマンドセットを実行すると、Splunk は、kbps フィールドを含む sourcetype=access_combined イベントに新しい avgkbps フィールドを追加します。 avgkbps の値は、そのイベントに対する平均速度(kbps)です。

さらに、Splunk はこのコマンドセットを使って、ホスト別にソースタイプ access_combined を持つすべてのイベントに対して平均速度(kbps)を表示するチャートを作成します。

検索結果の関連性、相関点、相違点を探す

associate、correlate、diff コマンドを使って、検索結果のフィールド値の間の関連性、相関点、相違点を探します。

関連レポートコマンドは、フィールドとフィールド値について互いに関連性のあるイベントを特定します。例えば、あるイベントの referer_domain が「http://www.google.com/」にあり、別のイベントの referer_domain に同じ

URL がある場合は、それらに関連性があると判断します。

`associate` コマンドで得られた結果を、`supcnt`、`supfreq`、`improv` 引数で「調整」することができます。これらの引数については、検索リファレンスの関連ページを参照してください。

例えば、このレポートは、アクセスソースタイプを検索して、フィールド/フィールド値の関連性を少なくとも 3 つ共有するイベントを特定します。

```
sourcetype=access* | associate supcnt=3
```

関連レポートコマンドは、フィールド間の統計的な相互関係を計算します。 `cocur` 演算子を使って、2 つのフィールドが同じ結果の一連に存在する時間的な割合(%)を算出します。

次のレポートは、`eventtype=goodaccess` となるすべてのイベントを検索し、すべてのフィールド間の共起的相互関係を算出します。

```
eventtype=goodaccess | correlate type=cocur
```

`diff` レポートコマンドを使って、2 つの検索結果の違いを比較します。 デフォルトでは、`attribute` 引数を使って特定のフィールド属性に指定されていない限り、選択した検索結果のローテキストを比較します。

例えば、このレポートは、検索で返された 44 番目と 45 番目のイベントを見て、その ip アドレスの値を比較します。

```
eventtype=goodaccess | diff pos1=44 pos2=45 attribute=ip
```

レポートの指定とチャートの作成

レポートの指定とチャートの作成

Splunk のレポートビルダを使うと、完成した、または終了した検索の結果を使って高度なレポートを簡単に作成できます。 レポートパラメータとチャートタイプの両方に豊富なレポートオプションが用意されています。

レポートビルダを使うと、確実に情報の多いレポートを作成するために、`stats`、`top`、`chart`、`timechart` などのレポートコマンドを理解しておく必要はありません。ただし、コマンドを使用する方が便利だと思う場合は、検索にコマンドをお使いいただいて構いません。

レポートコマンドの使用例については、本書の「レポートコマンドの使用」を参照してください。

レポートビルダは、2 つ(レポート内容の定義とレポートのフォーマット設定)に分割されています。レポート内容の定義ページでは、レポートの種類やレポートするフィールドなど、最初のレポートパラメータを設定します。

これらの初期設定を行った後は、Splunk がチャートや対応する表などを作成するレポートのフォーマット設定ページに移動します。このページでは、チャート書式の微調整、関連する表の表示、保存、印刷、結果の出力などを行います。

レポートビルダを起動する方法については、本書の「レポートビルダを起動する」を参照してください。

レポート内容の定義

レポート内容の定義ページで、お好きな方法で自由にレポートパラメータを指定できます。レポートコマンドを使いこなせる方で、高度な検索言語を使ってレポート内容を定義したい場合はそのように行ってください。

ただし、以下の場合は、デフォルトのフォームを使ってレポート内容を定義してください。

- レポートコマンドの使用に自信がない場合
- レポートするフィールドについて知る必要がなく、ドロップダウンリストを使って効率よく素早くレポートを設定したい場合

いずれの場合も、レポート内容の定義ページには、検索がプレロードされた検索バーと、レポートの時間範囲を変更できる時間範囲選択リストを表示されます。

注記： 時間範囲選択を使ってレポートの時間範囲を変更する場合は、レポートするフィールドを含む時間範囲を選択するよう注意が必要です。

フォームベースのモードを使ってレポート内容を設定する

レポート内容の定義ページのフォームベースモードでは、一連のリストフィールドを使ってレポートパラメータを素早く設定することができます。このモードでは、検索バーの言語を手作業で更新することはできませんが、フォームを使ってレポートパラメータを設定すると、同等の検索コマンドで検索バーを自動的に更新します。

レポートには、次の3種類があります。

- **時系列値**レポートは、選択した時間範囲でフィールド値の動向を表示します。このレポートは、`timechart` レポートコマンドを使います。棒グラフ、カラムチャート、折れ線グラフ、面グラフを表示できます。
- **最多値**レポートは、最も標準的な値を表示して検索を調整します。このレポートでは、`top` コマンドを使い、棒グラフ、カラムチャート、円グラフを表示できます。
- **最小値**レポートは、最も希少な値を表示して検索を調整します。このレポートでは、`rare` コマンドを使い、棒グラフ、カラムチャート、円グラフを表示できます。

注記： 灰色で表示される **値の分布**および**元の値**レポートタイプは、Splunkで今後追加される機能です。この値は、`chart` などのレポートコマンドを使って直接レポートを指定し場合に、現在レポートビルダで作成できるレポートで処理されます。

時系列値を選択すると、複数のフィールドまたは以下で分けるフィールドを使ってレポートを指定します。この種のレポートは、各ビンで時間範囲を指定できます。

レポートタイプを指定した後、レポートするフィールドを選択できます。

時系列値のレポートタイプを選択した場合は、統計演算子 (`count`、`direct count`、`average`、`mode`、`median` など) を主要フィールドに関連付けます。

レポートの初期パラメータの設定が終わったら、**次のステップ：レポートのフォーマット設定**をクリックします。Splunk は、デフォルトの書式パラメータを使ってレポートを生成するレポートビルダのレポートのフォーマット設定ページを表示します。

注記： フォームインタフェースを使用中はいつでも、検索言語モードを切り替えて、表示されているレポートコマンドを変更できます。例えば、**最多値のレポートタイプ**をホストのフィールドの値に設定します。これらの値を選択すると、検索ボックスに以下の検索構文が表示されます。

```
... | top host limit=1000
```

Splunk のレポートビルダで作成できるレポートのデフォルト上限は、1000 です。つまり、Splunk はテーブルおよびレ

ポートを作成する検索から上位 1000 項目を抽出します。大量の結果を抽出する検索を処理する場合は、検索言語入力モード(下参照)に切り替えて、手作業で上限値を必要な値(limit=20 など)に変更して、このデフォルトを変更できます。

検索言語を使ってレポート内容を設定する

レポートビルダのレポート内容の定義ページを表示している場合で、レポート言語を手作業で指定したい場合は、そのページで検索言語入力モードを使います。検索コマンドを使用したレポートの定義をクリックしてモードを切り替えます。

検索言語入力モードに切り替えたら、レポートコマンドを検索バーに直接入力します。このとき、必要に応じて自由に簡単または複雑な言語を入力できます。

レポートコマンドの使用例については、本書の「レポートコマンドの使用」を参照してください。

注記： 初期検索にレポートコマンドを含める場合は、表示されているレポートの表示ボタンをクリックすると、レポートビルダのレポートのフォーマット設定ページを開きます。(レポート内容の定義ページは表示しません。)

フォームベースモードで、初期レポートパラメータを設定したら、次のステップ: レポートのフォーマット設定をクリックします。Splunk は、デフォルトの書式パラメータを使ってレポートを生成するレポートビルダのレポートのフォーマット設定ページを表示します。

レポートのフォーマット設定

レポートのフォーマット設定ページでは、レポートのデフォルト形式を微調整できます。このレポートは、大きく 2 つのセクションに分かれています。

- チャートセクションは、レポート結果をチャートで表示します。
- テーブルセクションは、レポート結果を表で表示します。

Splunk でレポートのフォーマット設定ページを開くと、レポートタイプに関連付けられているデフォルトのレポートパラメータと検索に関する統計演算子を使ってチャートを生成します。例えば、レポート内容の定義ページでレポートタイプに時系列の傾向を選択すると、Splunk はカウントまたは重複を除いたカウント統計演算子を使ってデフォルトのカラムチャートを描画します。(別の統計演算子(平均など)を使うと、折れ線グラフを描画します。)

注記： レポートコマンドを含む検索を実施するときに、カスタムフォーマットでレポートを生成する検索を実施してチャートを作成したい場合(デフォルトの棒グラフの代わりに円グラフを作成する)は、グラフのフォーマットが完了したら、レポートビルダでレポートとして保存してください。保存検索には、チャートの書式パラメータは含まれないため、保存済みレポートが必要です。保存済みレポートにダッシュボードパネルを設定して、そのパネルでカスタム書式パラメータを表示する予定がある場合は特に重要です。

チャートセクションの上部に、チャートの書式オプションを設定するためのフォーマットのオプションサブセクションが表示されます。

このセクションでは、チャートの種類を変更(カラムチャートから棒グラフなどに変更)して、その他のさまざまな書式オプションを選択できます。フォーマットでは、書式を制御する一般、Y 軸、X 軸を切り替えます。変更した後は、適用ボタンをクリックして、Splunk で書式変更を適用したチャートを作成します。

注記： レポートジョブの期限が切れた後にレポートの書式を微調整しようとする、Splunk は空白のチャートを作成します。この問題は、保存したレポートジョブを基にレポートを作成すれば発生しません。検索ジョブとレポートジョブを保存する方法については、本書の「ジョブの管理」を参照してください。

チャートタイプの選択

チャートタイプドロップダウンリストを使って、Splunk でレポートデータを描画する方法を変更します。このリストには以下のチャートタイプが含まれます。

- 縦棒
- 横棒
- 折れ線
- 面
- 円
- 散布図
- バブル(現バージョンでは使用不可)

利用可能なチャートタイプオプションは、作成したレポートの種類により異なります。例えば、レポート内容の定義ページでレポートタイプを時系列の値に設定すると、利用できるチャートタイプは、縦棒チャート、折れ線グラフ、面グラフです。

Splunk のレポートビルダで作成可能なチャートの種類については、本書の「チャートギャラリー」を参照してください。各種チャートの図例と各チャートの使用に適した状態に関する情報などが紹介されています。また、各チャートを作成するためのコマンドとレポートビルダの設定についても説明しています。

一般チャートの書式オプションの更新

一般チャート書式オプションは、選択したチャートの種類により異なります。縦棒チャート、棒グラフ、折れ線グラフ、面グラフを作成する場合は、スタックモードで更新できます。折れ線グラフまたは面グラフを作成する場合は、チャートで Null 値を表示するよう微調整できます。

作成しているチャートの種類に関わらず、チャートのタイトルと説明の配置を更新できます。

X 軸、Y 軸の書式オプションの更新

X 軸と Y 軸の書式オプションでは以下が行えます。

- X および Y 軸のタイトルの変更
- 縦棒チャート、折れ線グラフ、面グラフの X 軸および Y 軸の最大および最小値の変更
- 棒グラフの X 軸の最大値および最小値の変更
- 折れ線グラフと面グラフの表示マーカーのオンとオフの切り替え
- 縦棒チャート、折れ線グラフ、面グラフ、散布図、バブルチャートの Y 軸のスケールを線形と対数表示の間で切り替え(棒グラフの X 軸のスケールに対しても同様)

Y 軸(棒グラフの場合は X 軸)の最大値および最小値を調整して、ほとんど違いのない結果グループの違いを強調できます。

例えば、Y 軸のすべての値が 114 から 145 の間にある縦棒チャートを表示しているとします。ここで、Y 軸の最小値を 110 に設定し、Y 軸の最大値を 150 に設定します。こうすると、必要でない類似点より、各縦棒の相違点を強調したグラフが作成できます。

同様に、チャートを対数表で表示すると、値に大きなばらつきがある場合に便利です。例えば、ほとんどの値が 10 から 50 の間にあり、最大値が 1000 まで広がっている縦棒チャートがあるとします。このチャートを対数表で表示すると、低い値との違いが見やすくなります。

チャートギャラリー

チャートギャラリー

Splunk のレポートビルダと Splunk のパワフルなレポートコマンド言語を組み合わせ、さまざまな方法でデータを視覚的にレポートするチャートを作成できます。

ここでは、Splunk でユーザーが作成できるさまざまなチャートについて、各種チャートの使用に適したいくつかの状況について説明します。

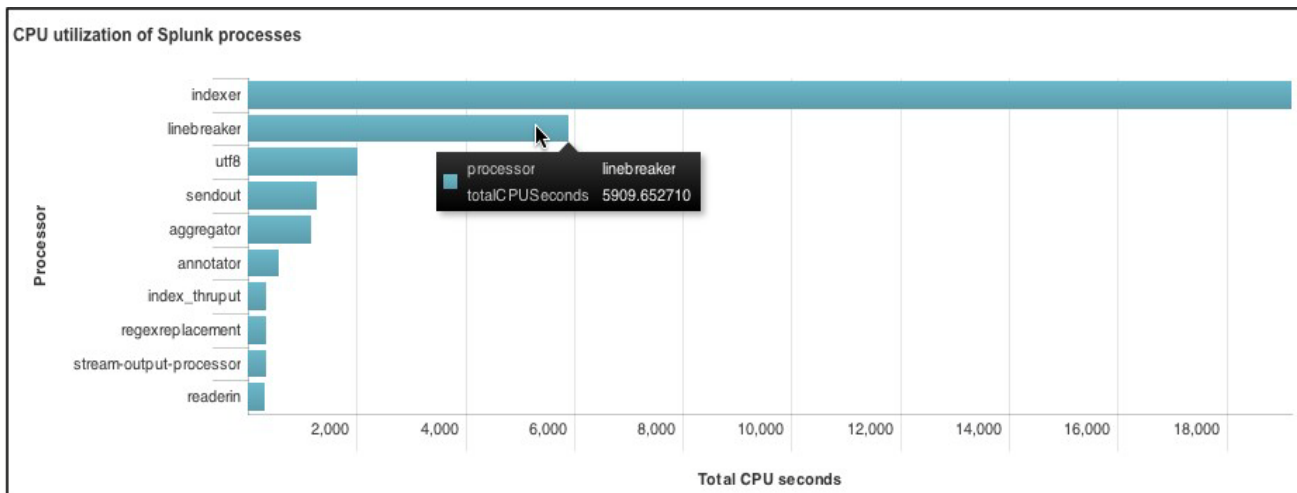
レポートビルダについては、本書の「レポートの指定とチャートの作成」を参照してください。

縦棒チャートと棒グラフ

縦棒チャートまたは棒グラフで、データのフィールド値の頻度を比較できます。縦棒チャートでは、通常、X 軸の値はフィールドの値(または時間)、Y 軸には、他のフィールドの値、値の数、またはフィールド値の統計的算出値を指定します。棒グラフも全く同じですが、X 軸および Y 軸の値は、決まっています。

次の縦棒チャートは、Splunk の内部メトリクスを使った検索の結果を表示しています。プロセッサ別に CPU_seconds の合計を探し、上位 10 個のプロセッサを降順に並べ替えて表示します。

```
index=_internal "group=pipeline" | stats sum(cpu_seconds) as totalCPUSeconds by processor
| sort 10 totalCPUSeconds desc
```

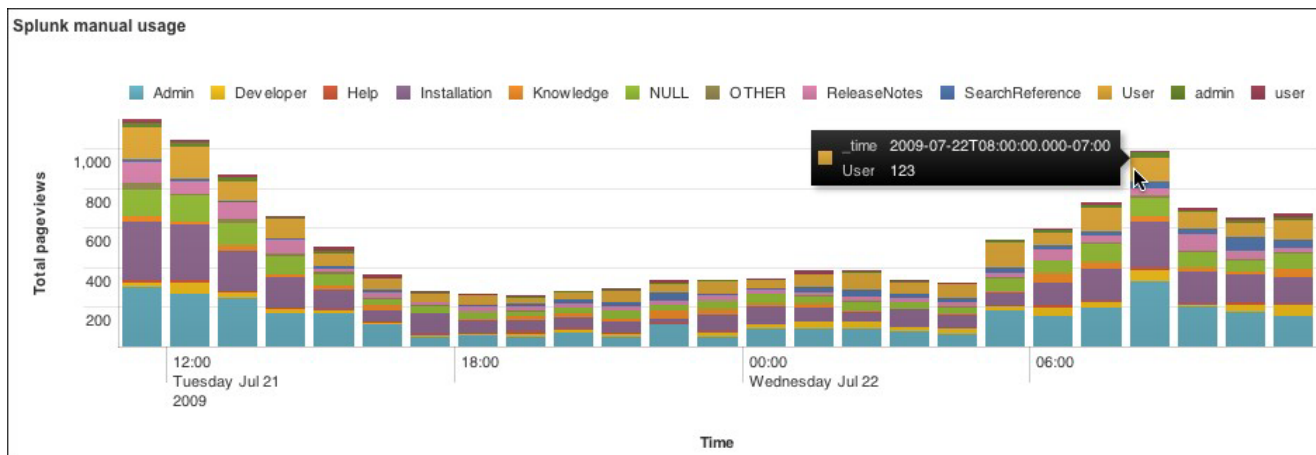


積み上げ縦棒チャートと棒グラフ

積み上げ縦棒チャートと積み上げ棒グラフを使って、データのフィールド値の頻度を比較できます。積み上げ縦棒チャートは、すべての縦棒が1つの縦棒のセグメントであることを除いて普通の縦棒チャートと同じです。合計縦棒の値は、セグメントの合計です。

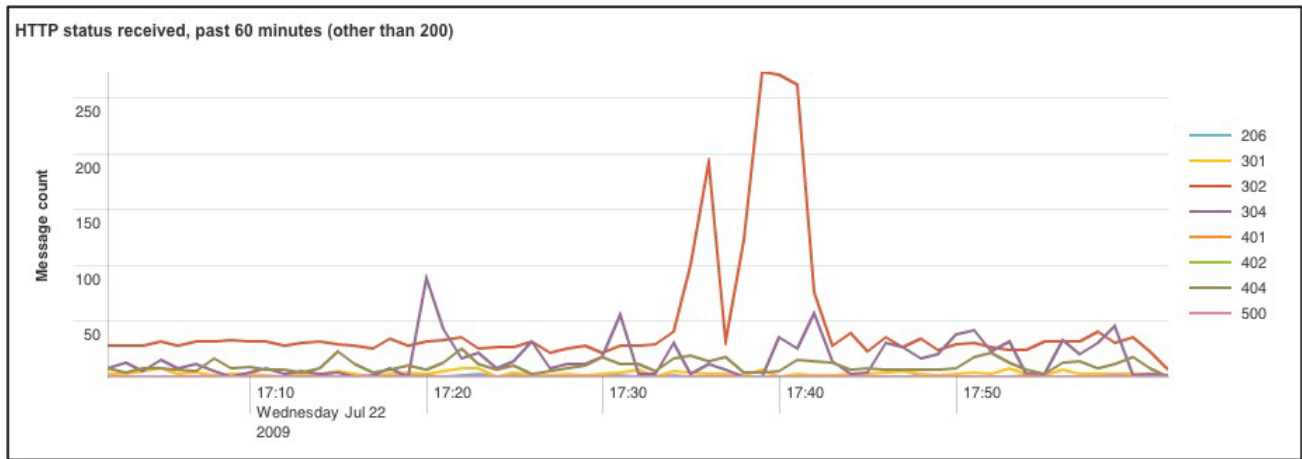
注記: 積み上げ縦棒チャートと棒グラフを使って、一連のデータセット内のデータの相対的長さ(重要性)を強調します。

次のチャートは、Splunk 4 を発売後の Splunk 説明書の使用頻度を図示しています。各縦棒のセグメントは、特定の説明書で表示されたページ数を10分ごとに示しています。



棒線グラフ

棒線グラフを使って、時系データまたは別のフィールドの動向を示します。折れ線グラフでは複数の列が表示できます。

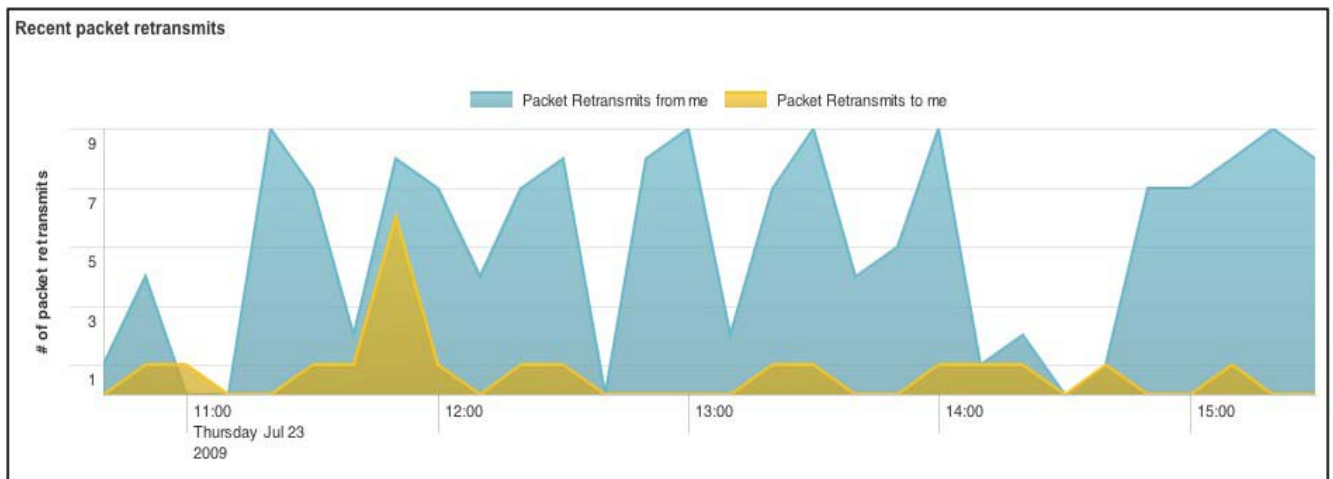


面グラフ

面チャートを使って、データの動向を、時間の経過または別のフィールド値との比較のいずれかで表示します。データの下に影が付いた部分は、質量を強調します。

次の面チャートは、以下の構文で作成されています。

```
sourcetype="tcptrace" | search host1_rexmt_data_pkts>0 OR host2_rexmt_data_pkts>0 |
timechart max(host1_rexmt_data_pkts),max(host2_rexmt_data_pkts) | fillnull value=0 | rename
max(host1_rexmt_data_pkts) as "Packet Retransmits from"
```

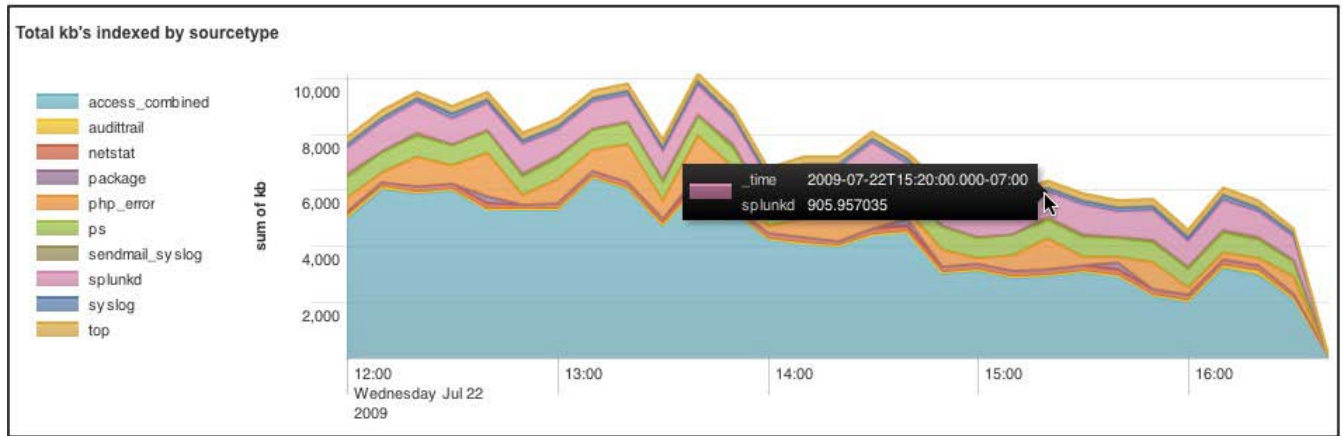


積み上げ面グラフ

積み上げ面グラフを使って、データの動向を面グラフで表現できる方法で複数の列を表示します。積み上げ面グラフは、各データ列がすべてのデータとどのように関係しているかを示します。

次のチャートは、Splunk の内部メトリクス情報を表現する別の例を示しています。次の構文でチャートを作成します。

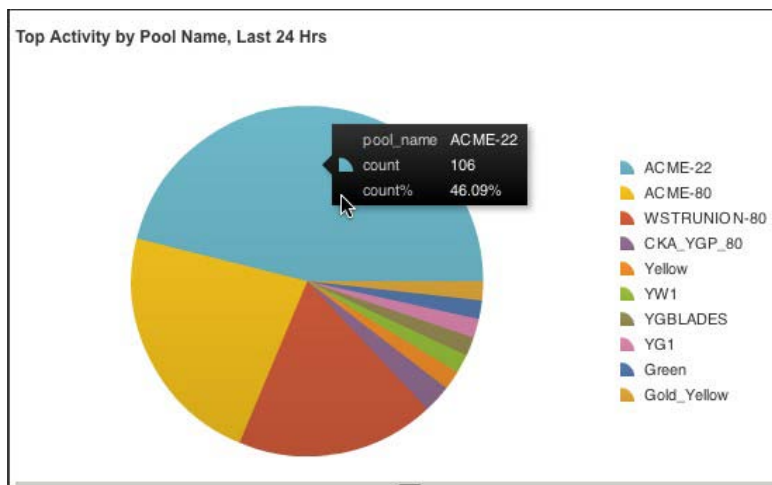
```
index=_internal per_sourcetype_thruput | timechart sum(kb) by series useother=f
```



円グラフ

円グラフでは、データの各部分とデータ全体との関係を示します。円グラフのスライスのサイズは、すべての値の合計に対するデータ値の大きさの割合で決めています。

次の円グラフは、ネットワークトラフィックプールを、過去 24 時間で頻度の高いアクティビティで示しています。円グラフの各項目の指標は、マウスを項目の上に置くと表示されます。



散布図

散布図(または「scatter plot」)では、データの離散値間の関係の動向を示します。通常、散布図では、定期的には発生しない、またはシリーズに属する離散値を表示します。これは、通常、標準的な点の列を描画する折れ線グラフと異なる点です。

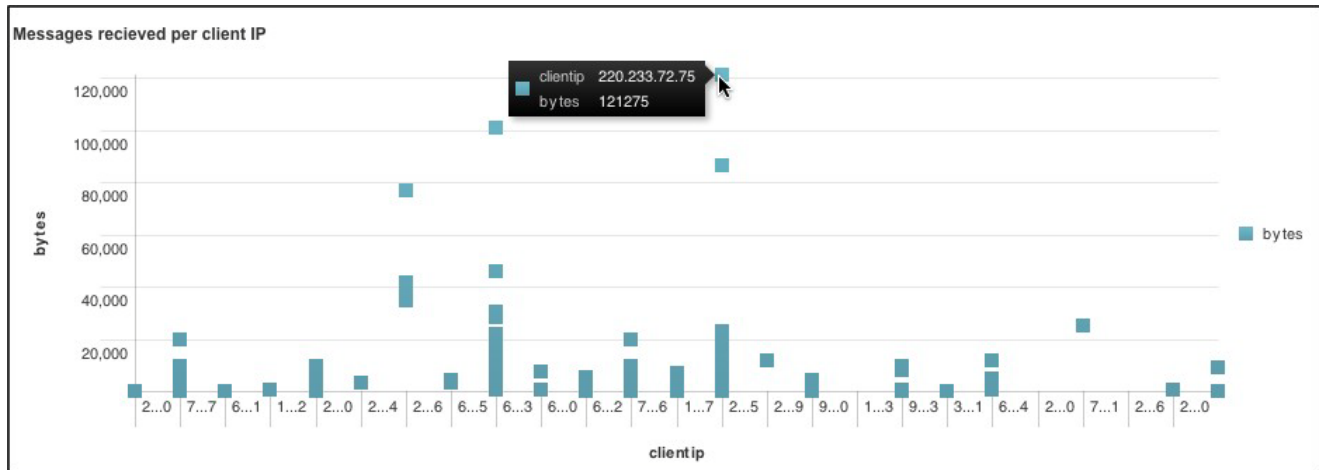
他にも、複数の列で作表していない場合でも、X軸の値に対してY軸の値が複数ある場合、分散図でその状況を図示する方法があります。このような状況は、次のようにグラフィイベントを直接検索すると発生します。

```
* | fields - *_ | fields clientip bytes
```

この検索は、複数のクライアント IP から受信したすべてのパケットを検索し、各パケットのバイト数で並べ替えます。

- この検索では、アンダーラインで始まるフィールド(_time フィールドなど)をすべて排除します。
- 2つ目の fields コマンドは、チャートの X および Y 軸に使用する 2つのフィールドを隔離します。適切な

結果を得るためには、Y軸の値を数値にします。(この例の場合、X軸は clientip、Y軸は bytes です。)



注記：このような分散図を作成するには、**検索コマンドを使用したレポートデータの定義**をクリックして、レポートコマンドを直接レポートビルダに入力する必要があります。このレポートは、検索バーでも実行できますが、レポートビルダを開くと、レポートを形成する前に削除しなくてはならないタイムチャートコマンドを追加します。

さらに複雑な分散図は、XMLベースのダッシュボード構成構文を使って、ダッシュボードで設定することもできます。**ダッシュボードで分散図をデザインする手順は、今後紹介いたします。**

バブルチャート

バブルチャートでは、データの動向と離散値の相対的重要度を示します。

バブルの大きさは、値の相対的重要度を示します。チャート上のバブルの位置を描画する X 軸と Y 軸の値に加えて 3 つの寸法で表現します。この寸法は、チャートの他の要素と関連させてバブルのサイズを決めます。

注記：バブルチャートは、Splunk の現バージョンではご利用できません。

レポートを保存し他の人と共有する

レポートを保存し他の人と共有する

新しく作成したレポートに満足したら、保存する、または他の人と共有するなどのオプションが選べます。

レポートの保存または結果レポート

レポートビルダのレポートのフォーマット設定ページで**保存**ドロップダウンリストを選択すると、2つの保存方法が選択できます。レポート検索文字列、時間範囲、関連する書式パラメータを保存して、その設定を基に新しいレポートを実行できます。

または、レポート結果をレポートジョブとして保存して、特別に実行したレポートの結果を後から見直すことができます。

保存済みレポートの作成

レポートビルダの結果のフォーマット設定ページで、**保存**をクリックしてから**レポートの保存...**を選択すると、レポー

ト検索文字列、関連するコンテンツ、書式パラメータを固有の名前で保存できます。レポートは、指定した名前で、トップレベルのナビゲーションバーの**検索とレポート**ドロップダウンに表示されます。

保存済みレポートを実行すると、関係付けられている検索文字列、時間範囲、チャート書式パラメータを使って新しいレポートを作成します。これは、保存済みレポートを他人またはベースダッシュボードパネルで共有する予定がある場合には、特に注意が必要です。(保存検索にはチャート書式パラメータは**含まれません**。書式を取り込むには、検索ベースのレポートを作成して保存してください。)

注記： **検索とレポート**ドロップダウンリストからレポートを簡単に探すには、タイトルに「レポート」または「チャート」を含めて検索との差別化を図ります。大量のレポートを保存する場合は、それぞれの保存レポートを見つけやすくするために、命名の仕方を考慮してください。

レポートを保存するとき、予約実行するよう指定したり、アラートを発行するよう指定したりできます。つまり、例えば、特定の条件を満たしたときにレポートで電子メールを送信するよう指定できます。予約レポートおよびアラートの設定の仕方については、本書の「再発条件のモニタリング」を参照してください。

注記： 保存済みレポートは、保存済み検索、イベントタイプ、タグ、および Splunk のデータを充実させるその他の項目と同様に一種の Splunk の知識であり、Splunk の操作を簡単にします。初めて Splunk の知識項目を保存する場合は、作成したユーザーと作成に使用した app でのみ利用可能です。**検索とレポート**ドロップダウンで、他のユーザーおよび複数の app 利用可能にするには、変更を行う権限がある場合に、共有対象ユーザーと他の app で表示する方法を指定する必要があります。

保存済みレポートを利用できるユーザーを増やし、複数の app でも利用可能にする方法については、本書の「実行中および完了した検索を操作する方法」を参照してください。

保存済みレポートの編集

レポートを保存した後に、レポートを更新する必要がある場合があります。例えば、レポート生成の基準となる検索言語を微調整したい場合、または、レポートのチャート表示が気に入らない場合に、そのレポートのチャートの書式パラメータを調整できます。

保存済みレポートを編集するには、まず保存済みレポートに戻ります (これは App のナビゲーションのトップレベルから選択します)。保存済みレポートを再実行すると、Splunk はレポートを保存したときに設定したチャートパラメータを使ってチャートを自動生成します。検索言語および/または書式パラメータを更新して、変更を保存するには、ページのほぼ上部に表示される**レポートの編集**ボタンを選択します。レポートビルダが表示されて、検索言語とレポートの書式の更新が行えます。更新が完了したら、**保存**をクリックしてから**レポートの保存**(元の保存済みレポートを変更内容で上書き)または**レポートとして保存...**(新しい保存済みレポートに変更を取り込んで違う名前で保存)を選択します。**検索結果だけを保存**を選択すると、このレポートの実行結果を保存します(下参照)。

レポートの検索結果だけを保存する

レポートビルダの結果のフォーマット設定ページで、特定のレポートを実行した**結果**を保存して、後から見直したい場合は、**保存**をクリックして**検索結果だけを保存**を選択します。この作業では、ジョブページからアクセス可能なレポート「ジョブ」を保存します。

大量のジョブを保存する場合は、ジョブページのリンクを入手... ボタンを選択して後からジョブを探す作業が簡単になります。このリンクを使うと、レポートを保存して、そのジョブに直接リンクできるようにします。このリンクをブックマークしておけば、後で見る場合や、他の人と共有する場合に便利です。

ジョブページで検索ジョブおよびレポートジョブを管理する方法については、本書の「検索ジョブの監視」を参照してください。

保存済みレポートへのナビゲーションを管理する

レポートを保存すると、ナビゲーションメニューの上位レベルのいずれかのドロップダウンリストに表示されます。例えば、検索アプリケーションでは、デフォルトで保存済みレポートは**検索とレポート**リストに表示されます。

アプリケーションの書き込み権限がある場合は、このデフォルトを変更して、名前に特定のキーワードを持つレポートをナビゲーションメニューの特定の категория に自動保存するよう設定することもできます。例えば、Splunk で名前に「website」を含むレポートを、ナビゲーションメニューのウェブサイト関連の検索およびレポートカテゴリーに自動保存します。また、すでに保存されているレポートをデフォルトのリストからナビゲーションメニューの上位レベルの異なる場所に移動できます。

詳しくは、ナレッジマネージャマニュアルの「保存済み検索とレポートのナビゲーションの定義」およびデベロッパーマニュアルの「ナビゲーションメニューをカスタマイズ」を参照してください。

レポートの共有

完成したレポートに他の人に有益な情報が含まれている場合は、自分だけで保管しておく必要はありません。Splunk には、共有するためのさまざまな方法が用意されています。

イベントデータをファイルにエクスポートする。 レポートのイベントデータを csv、txt、json、xml ファイルにエクスポートできます。このロー表データを保存したり、他社製のアプリケーション (MS Excel など) に入力したりできます。

レポートを印刷する。 Splunk は、作成したレポートのイメージと対応する表を直接プリンタに送信したり、レポートを .pdf ファイルに保存 (利用可能なプリンタドライバにより異なる) したりできます。

結果のリンクを取得(または共有)する。 **リンクの入手...** を選択してレポートの結果にリンクする URL を入手します。このリンクを関係者と共有できます。このリンクには、Splunk のインスタンスへのアクセスが必要です。

注記: **リンクを入手...** を選択するとレポートジョブが自動的に保存されます。保存されたジョブは、ジョブページからアクセスできます。結果へのリンクを入手ポップアップウィンドウには、この保存処理を行うリンクも表示されます。

ビューとダッシュボードにレポートを追加する

指定したレポートを表示する専用のビューやダッシュボードをデザインすることもできます。ダッシュボードでは、パネル毎にチャート、リスト、その他の表示されない予め定義された検索で生成されたデータなどを表示する複数のパネルで構成することもできます。

Splunk には、簡単なダッシュボードを素早く作成するビジュアルダッシュボードエディタが装備されています。詳しくは、本書の「ダッシュボードエディタで簡単なダッシュボードを作成する」を参照してください。ビューや高度なダ

ツッシュボードを作成する方法については、デベロッパーマニュアルを参照してください。

レポート用ダッシュボードとビューの使用

レポート用ダッシュボードとビューの使用

Splunk の検索 app には、当社の検索およびレポートモジュールの異なる構成を実現する役目も果たす便利なダッシュボードとビューが一式装備されています。これらの機能は、ダッシュボードやビューを独自にデザインする方法を探し出す役に立ちます。

Splunk app の各ページはビューです。ビューは、検索バー、タイムライン表示、リンクリスト、結果テーブルなどのモジュールの集合体です。例えば、プレロードされた検索を使って、企業のウェブサイトにかさねくカスタマイズした結果項目に値を入力するビューを構成できます。独自の app に合わせてビューを作成する方法については、デベロッパーマニュアルの「検索ビュー」を参照してください。

ダッシュボードはビューの一種です。各ダッシュボードは、ボックス、フィールド、チャート、表、リストなどのモジュールで構成されるパネルで作られています。多くのパネルは、ダッシュボードをロードしたときに起動されるプリセットされた保存検索に接続され、最新のメトリクスと分析を提供します。

注記: Splunk のビジュアルダッシュボードエディタを使って基本ダッシュボードを起動する方法を習得してください。詳しくは、本書の「ダッシュボードエディタで簡単なダッシュボードを作成する」を参照してください。

高度なダッシュボードを作成する方法は、デベロッパーマニュアルの「ダッシュボードの構築」を参照してください。

サマリーダッシュボード

サマリーダッシュボードは、検索アプリケーションを起動すると最初に表示される画面です。これには、最初の検索条件を入力して、検索を実行するための検索バーが表示されます。その下には、この Splunk のインスタンスに対応するインデックスメトリクスがあり、これらはすべて、ダッシュボードにリンクされているインライン検索および保存済み検索で生成されます。また、インデックス付けされたイベントの総数のほかにも、Splunk インスタンスでインデックスされたさまざまなソース、ソースタイプ、ホストを表示するリストなどが、各フィールドに対してインデックスされたイベントの総数の順に表示されます。リスト項目を選択すると、特定のフィールドの発生の検索を開始します。

注記: インデックスの権限は、役割レベルで設定されるため注意が必要です。つまり、サマリーダッシュボードのビューには、ユーザーの役割に従って、表示権限のあるインデックスに対するインデックス情報しか表示されない場合があります。ユーザー、役割、役割ベースのインデックス許可については、管理者マニュアルの「ユーザーの追加と管理」を参照してください。

探したいイベントが見つからない場合

Splunk に入力値を追加すると、その入力値は、使用しているアプリケーションに関連付けられて追加されます。例えば、Splunk 付属の *nix や Windows App は、入力データを特定のインデックスに書き込みます。(*Nix および Windows の場合は、「os」インデックスに書き込む。) Splunk に保存されているデータが見つからない場合は、見ているインデックスが正しいか確認してください。ユーザーの使用用途に合わせて「os」インデックスをデフォルトインデックスの一覧に追加することもできます。役割については、管理者マニュアルの役割に関するトピックを参照してください。

ダッシュボードのステータス

検索 app には、Splunk のさまざまな状態情報を表示する 4 つのダッシュボードが装備されています。

トップレベルのナビゲーションバーのステータスの下に表示されます。

注記： このダッシュボードは、管理者権限のあるユーザーにしか表示されません。ユーザーと役割については、管理者マニュアルの「ユーザーの追加と管理」を参照してください。ダッシュボードに対する権限の設定については、ナレッジマネージャマニュアルを参照してください。

- **管理者状況** - このダッシュボードは、基本的な Splunk アプリケーションの性能に関連するさまざまなメトリクスを表示します。Splunkd および Splunk Web についてレポートされたエラーの数、発生した最新エラーの一覧、タイムスタンプの問題、処理されていない例外、この時間に発生した平均アクセス遅延(秒)などを表示します。
- **検索状況** - このダッシュボードは、Splunk インスタンスに対する最近の検索動作について一目でわかる情報を表示します。ユーザーが検索を実行する方法、頻繁に検索を実行するユーザー、頻繁に使われる検索、検索実行時間に関連するメトリクスの選択の表示(長い検索を実行するユーザー、時間のかかる検索項目、過去 24 時間の検索負荷など)を表示します。
- **インデックス状況** - このダッシュボードは、Splunk インスタンスで現在実施されているインデックス処理に関する統計を表示します。インデックスされたイベントの総数(インデックス別)、インデックスされたソースタイプの上位 5 位、過去 24 時間にソースタイプでインデックスされた割合、インデックスエラーの一覧、その他便利な項目を表示します。
- **入力状況** - このダッシュボードは、Splunk の入力に関する情報を表示します。処理した最新ファイルや無視したファイルなどが表示されます。

応用的な部ラフ作成の表示

ナビゲーションバーのトップレベルにあるビューには、**応用的なグラフ作成ビュー**があります。この例では、別のレポートビルダウィンドウを開かなくてもチャートが作成できるビューの構造を紹介しています。検索バーにレポート言語を使う検索条件を入力すると、結果エリアに結果のチャートが表示されます。

ビューの管理

ビューリストの**ビューの管理**リンクを使うと、管理、権限の変更、新しいビューの追加を行う権限のあるビューを表示して更新できる管理の管理ビューを開きます。ここでビューを作成または更新するには、XML について、また、Splunk でビューを展開する方法について知り、理解しておく必要があります。詳しくは、デベロッパーマニュアルを参照してください。

ビジュアルダッシュボードエディタを使った簡単なダッシュボードの作成

ビジュアルダッシュボードエディタを使った簡単なダッシュボードの作成

Splunk のビジュアルダッシュボードエディタを使うと、コードを使わずに簡単なダッシュボードを素早く作成できます。Splunk は、保存済み検索と保存済みレポートを使って、ダッシュボードパネルに便利なメトリクスとチャートを作成します。

注記: ビジュアルダッシュボードエディタは、すぐ使える簡単で機能性の高いダッシュボードを数分で作成します。さらに、ビジュアルダッシュボードエディタで複雑なダッシュボードを作成し、ビジュアルエディタではできないことを実行したい場合にも対応します。詳しくは、デベロッパーマニュアルの「ダッシュボードの構築」、特に簡単なダッシュボードの作成に関する項を参照してください。

作成開始

- アクションドロップダウンリストを開き、**ダッシュボードの新規作成...**をクリックします。
- 新しいダッシュボードに名前を付けます。固有の ID を指定して、ナビゲーションメニューのトップレベルに表示される名前を付けます。
- **作成**をクリックして、新しいダッシュボードを作成します。
- 新しいダッシュボードは、空白で表示されます。パネルの定義を始めるには、**ダッシュボードの編集**をクリックして、ビジュアルダッシュボードエディタを開きます。

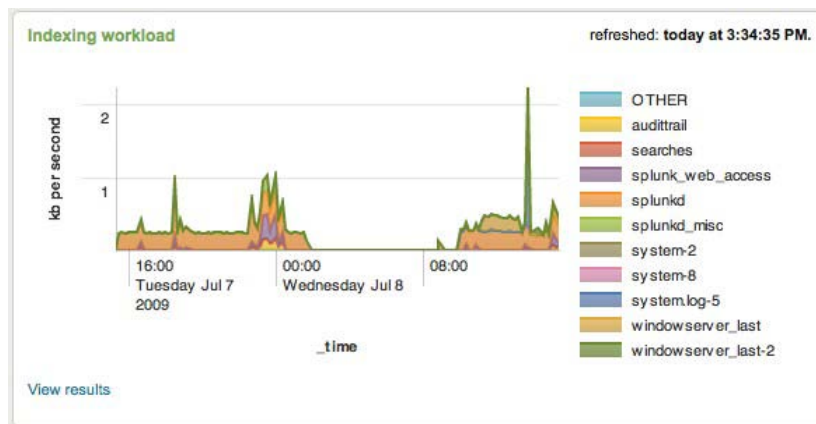
最初のパネルの作成

ビジュアルダッシュボードエディタで、**パネルタイプ**を選択して作業を開始します。ダッシュボードパネルは 4 種類あります。

- **データテーブルパネル**は、レポートの結果を表形式で表示します。

	series	sum(kb)
1	splunkd	14690.891861
2	splunk_web_access	1914.944329
3	windowserver_last	1633.437498
4	splunkd_misc	1399.706060
5	audittrail	1301.993130

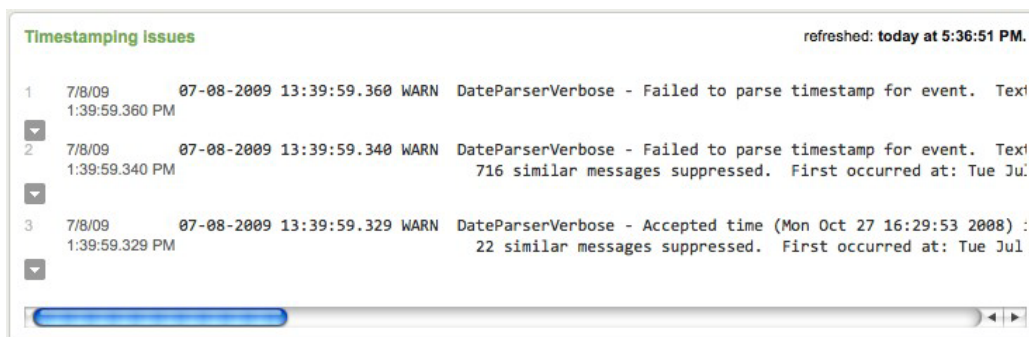
- **チャートパネル**は、レポートの結果をチャートで表示します。チャートパネルは、保存済みレポートに保存されているチャート書式パラメータを使います。チャートパネルが縦棒チャートを表示している場合に、積み上げ面グラフを表示したい場合は、パネルと関連付けた保存済みレポートの書式パラメータを変更します。
 - ◆ **注記:** カスタマイズした書式(デフォルトの棒グラフから円グラフに変更して、グラフのラベル、X 軸、Y 軸などを指定する)のダッシュボードにチャートを表示したい場合は、2 つのオプションから選びます。
 - 必要なチャート書式パラメータを含む保存済みレポートに関連付けたパネルであることを確認します。(保存検索には、チャート書式パラメータは含まれません)
 - パネルに対応するシンプル構造ダッシュボードXMLを変更すると、デフォルトのチャートの書式を上書きします。詳しくは、下の「ビジュアルダッシュボードエディタで作成したダッシュボードの編集」を参照してください。



- 1つの値パネルは、結果に1つの数値を表示します。例えば、このパネルを、過去1時間にサーバーで発生した404エラーの総数を返す検索に接続する、または、ウェブサーバーの平均アクセス遅延を表示する検索に接続します。このパネルは、最初の結果から最初のフィールドの値を読み出します。



- イベントリストパネルは、検索で返されたイベントのリストを表示します。このパネルタイプは、重要だがめったに発生しないエラーを含む発生頻度の低いイベントの検索に適しています。



パネルの名前を入力してから、関連付けられている保存済み検索またはレポートを選択します。パネルを追加をクリックして新しいパネルをパネルレイアウトセクションに追加します。

注記： 当社では、必要に応じて、特に大勢のユーザーで使用する予定のある場合は、予約検索を使うダッシュボードパネルを設定するよう推奨しています。予約検索でダッシュボードパネルを作成する場合、Splunk はダッシュボードを更新(リフレッシュ)したときに最後に実行した予約検索に関連付けられ、データを読み出します。こうすることで、ダッシュボードを更新した際に最初からすべての処理を実施するよりシステムの稼働が少なくなり、複数のユーザーが同時にたくさんのレポートを実施するような状況を避けることができます。

予約検索の指定については、本書の「保存検索のスケジューリング」を参照してください。

ダッシュボードパネルのレイアウト設定

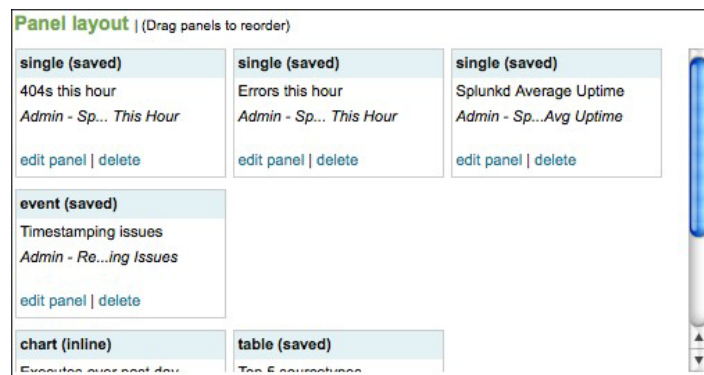
最初に作成したパネルと同じ方法で追加パネルを作成します。追加パネルがセクションパネルレイアウトに表示されたら、そのタイトルをクリックして、ダッシュボードの適切な場所にドラッグして調整します。

ビジュアルダッシュボードエディタを使って、3つのパネルの1つにダッシュボードを設定します。デフォルトでは、Splunkはそれぞれのパネルの幅が同じになるように設定します。ただし、高さはパネルのタイプと表示する情報により異なります。

ここからは、パネルグループを使ってダッシュボードのレイアウトを作成するときに従う必要のあるガイドラインについて説明します。

- 1つの値を表示するパネルは小さいため、3行で表示するよう指定します。1行または2行で表示すると、空白部分が多くなるため適切ではありません。
- イベントリストパネルは、横のスクロールバーを使って表示されるイベントデータのラインを表示するため、1行のパネル行で表示します。
- データ表パネルとチャートパネルは、1行または2行のパネルで表示します。表およびチャートパネルを同じ行に混ぜ合わさることができですが、データ表パネルは、表示するデータの長さにより高さが異なります。(トップまたは上位5位を返す検索を実行した場合で想定)

ここでは、上述のガイドラインに従ったダッシュボードのレイアウト例を示します。一番上の行には、1つの値のパネルを3つ配置し、中央の行には、1つのイベント一覧パネル、下の行には、チャートパネルとデータ表パネルをそれぞれ配置しています。



注記: ほとんどの表示問題は、ダッシュボードの背後にあるXMLコードを少し調整すれば解決します。長いデータの表パネルにページコントロールを追加し、同じヘッダでパネルをグループ化させ、チャート書式パラメータを変更します。ビジュアルダッシュボードエディタウィンドウの下部にある**編集 名前/XML**をクリックすると、XMLにアクセスできます。ビジュアルダッシュボードエディタで作成したダッシュボードのXMLを編集する方法については、デベロッパーマニュアルの「シンプルなダッシュボード」を参照してください。

インライン検索文字列をダッシュボードパネルに追加する

ビジュアルダッシュボードエディタを使うと、保存済み検索を行う代わりにインライン検索文字列を実行するようにダッシュボードパネルを編集できます。エディタに追加したパネルで**パネルの編集**をクリックします。パネルの編集ウィンドウで、パネルの現在の設定を編集する、または、**保存済み検索**から**インライン検索文字列**に切り替えます。

インライン検索文字列を選択した場合は、表示されるフィールドにインライン検索文字列を挿入して、**開始時間**および**終了時間**フィールドに相対的な時間識別子を指定して、検索時間範囲を入力します。

注記： ビジュアルダッシュボードエディタでは、チャートパネルの書式パラメータの設定はできません。インライン検索でチャートパネルをデザインした後にチャートの書式を調整する場合は、ダッシュボードの背後にあるシンプル構造ダッシュボード XML を編集しなければなりません。

ビジュアルダッシュボードエディタで作成したダッシュボードを編集する

ビジュアルダッシュボードエディタ (または、簡単なダッシュボード構文を使って) で作成したダッシュボードは、ダッシュボードを表示して、**アクションメニューのダッシュボードの編集...** をクリックして編集できます。ビジュアルダッシュボードエディタが表示されます。

編集 名前/XML を選択して、ダッシュボードの名前および、ダッシュボードの背後にあるシンプル構造ダッシュボード XML を編集します。ビジュアルダッシュボードエディタで作成したダッシュボードの XML を編集する方法については、デベロッパーマニュアルの「シンプルなダッシュボード」を参照してください。

権限を編集 を選択して、ダッシュボードに対応する役割ベースの読み込みおよび書き込み権限を変更します。ダッシュボードの権限を設定するときに、アプリケーションの利用可能度も指定できます。ダッシュボードには、以下の設定が適用できます。

- 自分でしか見れないプライベートビュー
- 1 つの app にのみ対応(app がそのようにデザインされている場合)
- システムのすべての Splunk アプリケーションで「グローバル」な利用が可能

ダッシュボードナビゲーションの管理

ダッシュボードは一種のビューであるため、デフォルトでは、ユーザーが作成した新しいダッシュボードは、ナビゲーションメニューのトップレベルのビューリストに表示されます。ナビゲーションメニューの背後にあるコードを編集して以下を行います。

- 分類されていないダッシュボードの保存場所を変更する。ダッシュボードはナビゲーションメニューの既存のリスト (または「ビューコレクション」) に移動したり、新しいリストを作成できます。
- 同類のダッシュボードを分類するネストしたコレクション(ナビゲーションバーリストにあるビューコレクション)を作成する。例えば、ダッシュボードドロップダウンでは、ウェブサーバーのファイアウォール情報に関連する情報を表示する一連のダッシュボードをまとめてグループ化する「ウェブサーバー」コレクションを持つことができます。

注記： ナビゲーションは、app を基に app で管理します。ダッシュボードがシステム内のすべての app にグローバルに対応するよう変更されている場合、最初は、その app のトップレベルのナビゲーションバーの「分類されていない」ビューに対応するデフォルトのドロップダウンリストに表示されます。アプリケーションに書き込み権限のあるユーザーは、アプリケーション用ナビゲーションメニューの適切な箇所にダッシュボードを移動できます。

アプリケーションに書き込み権限がある場合は、管理を開き、**ナビゲーションメニュー**をクリックして、該当する app のナビゲーションメニューの名前をクリックして、ナビゲーションメニューコードにアクセスできます。ナビゲーションメニューのコードを操作する方法については、デベロッパーマニュアルの「ナビゲーションメニューをカスタマイズ」を参照してください。

サマリーインデックスを使ってレポートの効率を上げる

サマリーインデックスを使ってレポートの効率を上げる

長い時間をかけて大量のデータセットでレポートを実行することは手間のかかる作業です。このような作業は、頻繁に行われなためあまり問題にはなりません。しかし、このようなレポートを定期的に行うとなると実用的ではないばかりか、社内で Splunk を使って同様のレポートを実行するユーザーが急激に増える現象を引き起こす可能性があります。

サマリーインデックスを使うと、大量のデータでも効率よくレポートが作成できます。サマリーインデックスを使うと、レポートに含めたい貴重な情報を抽出する保存済み検索を指定できます。この検索をユーザーのニーズに合わせて定期的(毎週、毎時間など)に実行するようスケジュールリングします。Splunk で検索を実行する都度、最後に検索を実行してからの結果をユーザーが指定したサマリーインデックスに保存します。検索を実行して、大量のデータセットで作業する代わりに、この小規模で「速い」サマリーインデックスにレポートします。

サマリーインデックスは以下のような場合に使用できます。

- 数少ないオリジナルのイベントを小規模なサマリーインデックスに取り込んでレポートの効率化を図る
- 定期レポートを作成する(統計の集約を実行するなど)

注記： サマリーインデックスにインデックスするイベントは、全体的なライセンスボリュームに含まれます。本当に必要のない限り、サマリーインデックスに、大量のイベントをインデックスしないようにしてください。ライセンスボリュームへの影響については、Splunk サポートにご相談ください。

サマリーインデックスの例

例 1： 毎日、会社で Splunk を使って大量のイベントをインデックスしている状況を思い浮かべてください。表示したページ数を表示するレポート、過去 30 日以内にウェブサイトを訪れたビジター数をサイト別に表示するレポートなどを含めた、社員用のダッシュボードを設定したいと思っています。

このレポートは、主なデータボリュームを対象に実行することができますが、期待するデータを抽出するには、Splunk でウェブトラフィックに全く関係のない大量のイベントを並べ替える必要があるため、処理に時間がかかる可能性があります。それだけでなく、実際、このレポートは頻繁に使用するダッシュボードに含まれているため、実行頻度が高く、平均実行時間を大幅に拡張して、他のユーザーに迷惑となる可能性があります。

しかし、サマリーインデックスを使うと、ウェブサイトの表示ページとビジター情報を収集して、指定したサマリーインデックスに毎週、毎日、または毎時間実行する保存済み検索を設定することができます。その後、月の最後にこの小規模なサマリーインデックスでレポートを実行すれば、小規模に必要なデータセットを対象に検索を実行するため、レポートの作成時間も短縮されるはずです。

例 2： 長期にわたって実行統計数を表示するレポート、例えば、自分が管理するウェブサイトからファイルのダウンロードを実行した回数を表示するレポートを実行したいと思っています。最初に、特定の期間でダウンロードした総数を返す保存検索をスケジュールリングします。次に、サマリーインデックスを使って、Splunk で検索結果をサマリーインデックスに保存します。その後は、サマリーインデックスのデータが必要なときにレポートを実行して、最新のダウ

ンロードの総数を取得します。

別のビューの場合は、サマリーインデックスの理論と使い方を紹介するこの Splunk デベロッパービデオをご覧ください。

サマリーインデックス用レポートコマンドの使用

サマリーインデックスにデータを入力する検索を指定するときにサマリーインデックス用レポートコマンド (`sichart`, `sitimechart`, `sistats`, `sitop`, `sirare`) を使います。これらのコマンドを使う場合は、最終的にサマリーインデックスを実行する検索で使用する同じ検索文字列を使うことができます。ただし、後者の検索で使う通常のレポートコマンドは除きます。例えば、サマリーインデックスで次の検索を実行します。

```
eventtype=firewall | stats count by src_ip | sort count desc | head=20
```

サマリーインデックスの作成に使う検索文字列は以下の通りです。

```
eventtype=firewall | sistats count by src_ip | sort count desc | head=20
```

注記： Splunk の旧版では、サマリーインデックスの入力に使う検索の設計、特に、集約統計に関与する終了したサマリーインデックスを実行する検索では、不正な結果を抽出しないよう慎重に「インデックス入力」検索を設定する必要があったため注意が必要でした。例えば、故障サーバーからの平均応答時間を返す終了したサマリーインデックスの検索を実行したい場合は、インデックス入力検索を以下のように設定します。

- サマリーインデックスに対して実行するよりも頻繁に実行するようにスケジューリングする。
- サマリーインデックスに対して実行する検索よりも大量のデータをサンプリングする
- インデックス入力検索で加重平均を確実に生成する追加の検索コマンドを追加する

新しいサマリーインデックス用レポートコマンドでは、これらをすべて処理し、必要な調整を自動で決定するため、統計的に不正確な結果を生成しないデータをサマリーインデックスに入力します。

特別なサマリーインデックス用レポートコマンドを使わずサマリーインデックスに入力する検索を手動で指定する方法については、ナリッジマネージャマニュアルの「サマリーインデックスの設定」を参照してください。

Splunk Web でサマリーインデックスを設定する

Splunk Web インタフェースを使えば、簡単にサマリーインデックスが設定できます。サマリーインデックスは、保存済み検索および予約検索のアラートオプションです。サマリーインデックスの入力に使用する検索が決まったら、以下の手順に従います。

1. 検索またはレポートビルダインタフェースから**検索を保存**を選択する、または、Splunk 管理の保存済み検索ページで検索名を選択するのいずれかの方法で検索の検索詳細ページを開きます。
2. **この検索をスケジュール**を選択してから、適切なインターバルでスケジューリングします。アラート条件を毎回確認しないで検索を実行する場合は、アラート条件に「常に」を選択します。
3. アラートオプションに**サマリーインデックスを有効にする**を選択します。

4. 表示されるインデックストロップダウンを使って、検索を実行するサマリーインデックスを選択します。
Summary インデックスがデフォルトのサマリーインデックスです。さまざまなサマリーインデックス検索を実行する予定がある場合は、追加のサマリーインデックスを作成する必要があります。

5. Splunk 管理を使う場合は、オプションで、1 から 4 つのフィールド/値のペアをサマリーインデックス定義に追加できます。キー/値のペアは、各イベントで注釈が付けられます。これには、後で検索しやすいようにサマリーインデックスが付けられます。例えば、サマリーインデックスに入力(`report=firewall_daily_summary_dst_ip`)する保存検索の名前、または検索に入力(`index=summary`)するインデックスの名前を追加して、後から検索できるようにします。

注記: `savedsearches.conf` のサマリーインデックスの設定に追加のフィールド/値のペアを追加できます。詳しくは、ナリッジマネージャマニュアルの「サマリーインデックスの設定」を参照してください。

検索の保存、スケジューリング、アラートの設定については、本書の「検索を保存して検索結果を共有する」、「保存検索のスケジューリング」、および「予約検索に対するアラート条件の設定」を参照してください。

投入検索をスケジューリングしてデータの格差および重複を防ぐ

データ格差および重複を最小限にするには、確実に適切なインターバルを設定して、サマリーインデックスに投入する検索のスケジュールを遅らせるようにします。

サマリーインデックスのデータの格差は、サマリーインデックスでイベントをインデックスしていない場合の時間です。この格差は、以下の場合に発生する可能性があります。

- `splunkd` で失敗した
- 予約保存検索(1 つはサマリーインデックス付き)の実行に時間がかかり、次の予約実行時間を過ぎても実行している 例えば、通常実行に 7 分かかる検索の場合に、5 分ごとにサマリーにデータを投入する検索をスケジューリングしたら、前の検索が終わらないと次の検索を実行できないため、問題が発生します。

重複は、同じタイムスタンプを共有するサマリーインデックス(同じ検索)のイベントです。重複イベントは、サマリーインデックスで作成したレポートおよび統計を混乱させます。重複は、保存済み検索で設定した時間範囲が検索のスケジュールの頻度より長くなる、または収集コマンドを使って手動でサマリーインデックスを実行すると発生する場合があります。

サマリーインデックスの原理

Splunk Web で、サマリーインデックスは、予約保存済み検索のアラートオプションです。サマリーインデックスをオンにしたまま保存済み検索を実行すると、検索結果は一時的に

(`$SPLUNK_HOME/var/spool/splunk/<savedsearch_name>_<random-number>.stash`) ファイルに保存されます。Splunk は、そのファイルから、(`addinfo` コマンドを使用して)現在の検索および設定で指定したフィールドに関する全般的な情報をそれぞれの結果に追加して、指定したサマリーインデックスの結果イベントデータをインデックスします(デフォルト、`index=summary`)。

注記: `addinfo` コマンドを使って、現在の検索に関する全般的な情報を持つフィールドを、サマリーインデックスに投入する検索結果に追加します。検索について追加された全般情報は、サマリーインデックスに格納する結果レポートの実行に役立ちます。

Splunk がサマリーインデックスの結果をインデックスした後は、検索でサマリーインデックスの名前を指定して検索およびレポートを実行します。

例：

この検索は、「サマリー」インデックスに注目して、そのインデックスで最も標準的な参照値からイベントを返します。

```
* index=summary | top referrer
```

データの格差と重複を特定する

データの格差と重複を特定するには、サマリーインデックスに対する検索に重複コマンドを使います。このコマンドは、格差または重複を含むインデックスの時間範囲を特定します。開始時間および終了時間または期間と保存検索の名前のいずれかを指定して格差と重複を検索する時間範囲を指定して、検索文字列の `| overlap` コマンドに従います。

2 のコマンドを使って、特定のカレンダーの時間範囲を指定します。

- **開始時刻:** 不足データの検索を開始する時間、`starttime= mm/dd/yyyy:hh:mm:ss` (例： 05/20/2008:00:00:00).
- **終了時刻:** 不足データの検索を終了する時間、`endtime= mm/dd/yyyy:hh:mm:ss` (例： 05/22/2008:00:00:00).

または、次の 2 つのコマンドを使って、時間範囲を指定して、保存検索で不足イベントを検索します。

- **ピリオド:** 検索を実行する時間の長さを指定する、`period=<integer>[smhd]` (例： 5m)
- **SavedSearchName:** 不足イベントを検索する保存検索の名前を指定する、`savedsearchname=string` (ワイルドカード不可)

格差を特定する場合は、格差が発生した期間で予約保存済み検索を実行して、収集コマンドで結果にサマリーインデックスを付けます。重複イベントを特定する場合は、検索言語を使ってサマリーインデックスから手作業で重複を削除します。

サマリーインデックスの例(ファイアウォールトラフィック)

サマリーインデックスの例(ファイアウォールトラフィック)

サマリーインデックスを使うと、データ量を小さいサブセットに減らし、最終的に個別に収集されたすべての結果を最終結果として処理することで、大量のデータを効率よく処理できるようになります。

シナリオ

サマリーインデックスは、大量のファイアウォールまたはウェブアクセスログデータで共通に使用されています。ファイアウォールのトラフィック(頻繁に使われるソース、あて先、サービスなど)を毎月レポートしなければならないことを想像してみてください。あなたの職場では、毎日約 1000 万個のイベントが生成されていると仮定すると、月末のレポートでは、約 280M から 310M のイベントを処理することになり、月次レポートの実行にはかなりの時間がかかります。

サマリーインデックスの設定

これを処理するには、メインインデックスからイベントのサブセットを構成するサマリーインデックスを作成する必要があります。このサマリーインデックスには、検索に必要なデータ範囲のみが含まれています。これはかなり小さなイ

ンデックスとなるため、長い期間を対象に検索する場合でも、完了までにさほど時間がかからないはずで

このサマリーインデックスを作成するには、ファイアウォールから特定のサブセットを検索する予約検索を指定して、その後、サマリー検索を有効にします。こうすると、Splunk が新しい「サマリー」インデックスを作成します。(同じインデックスに保存できますが、通常、サマリーデータの保管期間が異なります。)

タイトルが **Do Not Click - Summary Index - Firewall Daily Summary Source IP** の保存済み検索で、前日に発生したファイアウォールイベントの上位 200 件の検索を毎日午前 2 時に実行するようにスケジューリングします。

```
starthoursago=26 endhoursago=2 eventtype=firewall | stats count by src_ip | sort count desc | head 200
```

実際にシステムで実行する検索は以下のとおりです。

```
search eventtype=firewall | stats count by src_ip | sort count desc | head 200 | addinfo | collect addtime index="summary" ¥ marker="info_search_name=¥"Do Not Click - Summary Index - Firewall Daily Summary Source IP¥",report=¥"firewall_daily_summary_src_ip¥"
```

システムによりいくつかのコマンドが自動的に追加され、保存済み検索ページに追加指定も発生しています。追加フィールド(report)に値(firewall_daily_summary_src_ip)が追加されています。このフィールドは、後でレポートを作成するときに、サマリーインデックスの複数の設定を差別化するのに役立ちます。

サマリーインデックスの検索

この検索は、サマリーインデックスを作成します。1 日に処理するデータ量を 1 千万から 200 イベントに減らし、200 件の src_ip アドレスが格納されています。これで、毎月の月末に、システムが上位 20 件を算出するために処理するイベントは、5600 から 6200 個に減りました。サマリーインデックスに対して月末に実行する検索は、以下のとおりです。

```
earliest=-1mon index=summary report=firewall_daily_summary_src_ip | stats sum(count) by src_ip | sort sum(count) desc | head 20
```

このサマリーインデックスの検索は、並べ替えるには、全体的に極めて小規模なイベントセットなため、短時間で完了します。

利点がわかりやすい： 先月のデータのレポートが素早く作れるだけでなく、このレポートを過去 30 日の間に定期的に行うこともできます。週次、四半期、年次レポート(最も一般的なシナリオ)が必要な場合だと、よりいっそう明白になります。必要に応じて、サマリーデータを使って別のサマリーの収集が作成できます。(日次データによる月次サマリーの作成など)

別のサマリーインデックス検索を追加する

同様のサマリーインデックスを上位あて先 (dst_ip) および上位サービス(dst_port)に対して実行します。この場合、以下のような検索を設定します。

毎日午前 3 時に保存検索(**Do Not Click - Summary Index - Firewall Daily Summary Destination IP** – 追加フィールド report=firewall_daily_summary_dst_ip)を実行します。

```
starthoursago=27 endhoursago=3 eventtype=firewall | stats count by dst_ip | sort count desc | head 200
```

毎日午前 4 時に保存検索(**Do Not Click - Summary Index - Firewall Daily Summary Destination Port** – 追加フィールド

`report=firewall_daily_summary_dst_port`)を実行します。

```
starthoursago=28 endhoursago=4 eventtype=firewall | stats count by dst_port | sort count desc | head 200
```

複数のサマリーインデックス検索を組み合わせる

ときには、3つの検索を1つの検索に組み合わせることが可能です。こうすると、パフォーマンスは向上しますが、最終結果の精度に悪影響を及ぼす場合があるため、収集する結果件数を増やすようお勧めします。例：

毎日午前2時に保存検索(**Do Not Click - Summary Index - Firewall Daily Summary** – 追加フィールド

`report=firewall_daily_summary`)を実行します。

```
starthoursago=26 endhoursago=2 eventtype=firewall | stats count by src_ip, dst_ip, dst_port | sort count desc | head 2000
```

重要： 上述のサマリーインデックス検索は、わざと **Do Not Click - *** という名前にしてあります。

注意事項

上述で使用した値は、図示をわかりやすくするためのものです。毎日1000万件ものイベントを取り扱う場合は、より頻繁にサマリー収集検索を実施して、処理するイベントの数を減らした方が良いでしょう。

効率のよい実施

- 個別サブセットに対して、常に最終結果として予測するより広い範囲で計算してください。(毎日上位10件を算出する場合は、毎時上位100件を算出する)
- サブセットを算出するときは、時間幅を約5から10分ずらして、データの遅延に対応します。(サマリーインデックス検索を1時間10分後に実行して、70から10分前のイベントを収集する)。`startminutesago=70` `endminutesago=10` を使用。

合計を算出する場合は、`sum()` を使用する。(`count()` ではない)

警告と問題

- サマリーインデックスに関する主な問題の1つは、システムは収集を開始した時点からしかサマリーデータを持つことができないことであり、古いデータのサマリーインデックスを参照しなければなりません。(日次処理の初日のデータは、収集を開始した前日のデータとなる) このように特別な状況に対応するためのスクリプトが用意されています。詳細は、「サマリーインデックスをアーカイブデータで埋め合わせ」を参照してください。
- サマリーインデックスの付いた特定のカウンタを使うと、**サマリーインデックス用レポートコマンドを使わない**と、不明確な結果が生成されることがあります。これは、サマリーの範囲を超えると発生します。(時間が境界の場合でも、1:59 と 2:00 で値が表示される)