Hewlett Packard Enterprise

HPE Security ArcSight Logger

ソフトウェアバージョン: 6.4

管理者ガイド

2017年4月14日

ご注意

保証

Hewlett Packard Enterprise製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、Hewlett Packard Enterpriseはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

本書の例で使用しているネットワーク情報 (IPアドレスやホスト名を含む) は、説明のみを目的としています。

HPE Security ArcSight製品は高い柔軟性を持ち、お客様の設定に応じて機能します。データのアクセス性、完全性、機密性については、ユーザーが責任を負います。包括的なセキュリティ戦略を実施し、優れたセキュリティ慣習に従ってください。

本書は機密情報です。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、Hewlett Packard Enterpriseからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

著作権と承認の完全な表明については、以下のリンク先をご覧ください。
https://www.protect724.hpe.com/docs/DOC-13026

サポート

連絡窓口

電話	電話番号のリストは、HPE SecurityArcSightテクニカルサポートページに記載されています: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
サポートWebサイト	https://softwaresupport.hpe.com
Protect 724コミュニティ	https://www.protect724.hpe.com

コンテンツ

第1章: 概要

このガイドでは、ArcSight Logger 6.4の管理、設定、使用について説明します。また、ストレージ、受信者、転送者の設定、イベントの使用、ユーザー管理に関する説明、およびセットアップとメンテナンスに関する留意事項が記載されています。

Loggerの概要

Loggerは、ログ管理ソリューションの1つで、きわめて高いイベントスループット、効率的な長期保存、高速なデータ分析を実現するために最適化されています。Loggerは、イベントの受信と保存、検索、取得、レポート作成をサポートしています。また、選択したイベントを転送することもできます。rawデータは圧縮されますが、フォレンジクス調査における信頼性の高い訴訟データを得るために、要求に応じていつでも圧縮前のデータを取得できます。

Loggerはスタンドアロンで1つだけ使用することも、必要に応じて複数のLoggerを使用することもできます。Loggerは、ArcSight Data Platform (ADP) の基本コンポーネントの1つであり、ArcSight Management Center (ArcMC) によって管理されます。複数のLoggerを連携させてスケールアップし、すべてのLoggerに分散された検索クエリを使用して、きわめて大量のイベントをサポートします。

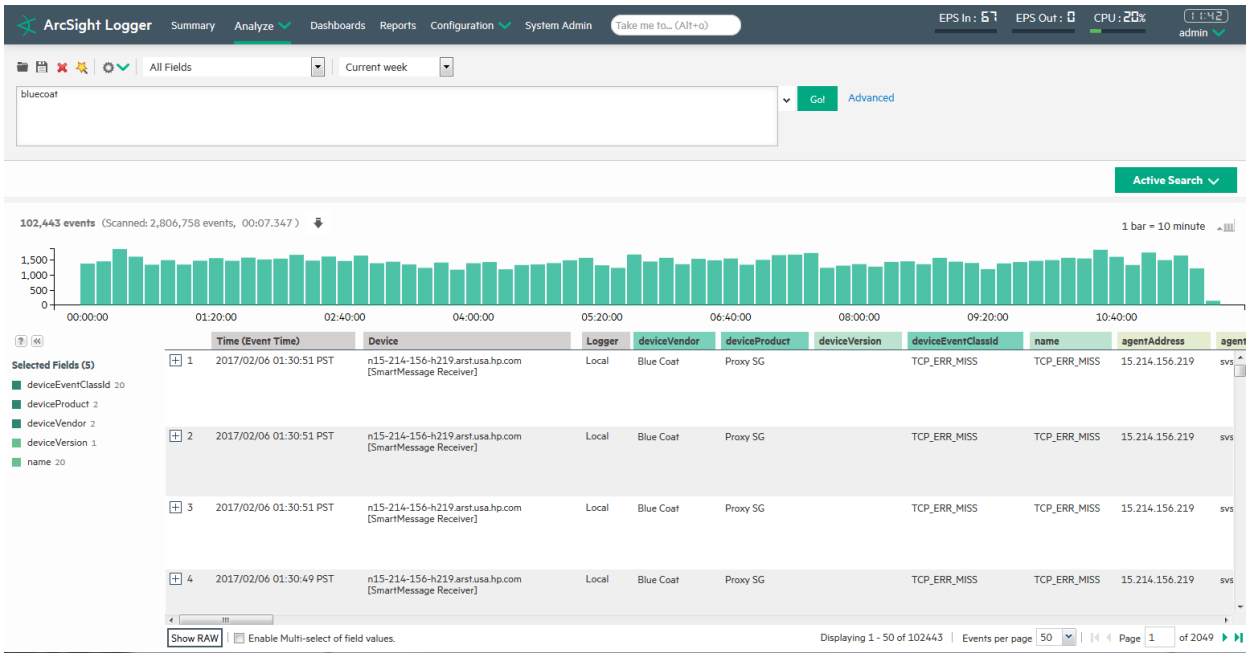
Loggerは、アプライアンスおよびソフトウェアフォームファクターで利用できます。アプライアンスベースのソリューションは、強化された専用のエンタープライズクラスのシステムであり、きわめて高いイベントスループット、効率的な長期保存、高速なデータ分析のために最適化されています。ソフトウェアベースのソリューションは、特徴と機能の点ではアプライアンスベースのソリューションと似ていますが、サポートされている任意のプラットフォームにArcSight Loggerをインストールできます。ソフトウェアバージョンは、VMware仮想マシンに加えて、Amazon Web Service (AWS) やMicrosoft Azureといったクラウドコンピューティングプラットフォームでも利用できます。

注: Loggerのタイプに明確な違いがない場合、本書ではすべてのタイプのLoggerをLoggerと称します。違いがある場合は、Loggerのタイプを明示します。

Loggerイベント

イベントは、受信時刻、イベント時刻、ソース(ホスト名またはIPアドレス)、およびメッセージ部分からなります。Loggerでは、イベントについて記述したフィールドとともに、表形式でイベントが表示されます。

[分析] > [検索] ページ (検索結果を表示)



ArcSightマネージャーと同じように、Loggerは正規化された共通イベントフォーマット (CEF) の形式で構造化されたデータと、syslogイベントのような構造化されていないデータを受信します。Logger上で設定されているファイルタイプの受信者は、イベントのイベント時刻のみを解析します。Loggerはメッセージに依存しませんが、イベントやログを生成するデバイスの相互運用性向けの業界標準形式である、CEFに準拠したメッセージであれば、高度な処理を実行できます。

CEFの詳細については、『ArcSight CEF』ドキュメントを参照してください。このガイドをダウンロードするには、Protect 724のArcSight製品マニュアルのコミュニティで「ArcSight Common Event Format (CEF) Guide」を検索しアクセスしてください。

Loggerの機能

以下の各セクションで、Loggerの主な機能の概要について説明します。このガイドの該当するセクションへはリンクされています。

ストレージ設定

Loggerイベントは、任意のLogger上にローカルに保存することも、ストレージネットワーク(SAN)をサポートするLoggerアプライアンスモデルではリモートに保存することもできます。SANを使用すると、両方のタイプのLogger上にイベントを保存できますが、イベントの保存には1つのLUNのみ使用できます。ネットワークファイルシステム(NFS)をイベントのプライマリストレージとして使用することは推奨されません。

Loggerアプライアンスには、イベント用のオンボードストレージが含まれています。一部のLoggerモデルには、RAID 1またはRAID 5ストレージシステムが含まれています(http://www8.hp.com/us/en/software-solutions/enterprise-security.htmlでLoggerの仕様を参照してください)。

イベントは、圧縮された状態で保存されます。圧縮レベルを設定することはできません。

NFSまたはCIFSシステムは、イベントアーカイブ、保存された検索、エクスポートされたフィルターとアラート、および設定のバックアップ情報といったLoggerデータのアーカイブに使用できます。また、Loggerを設定してCIFSホストからイベントデータやログファイルを読み出すこともできます。

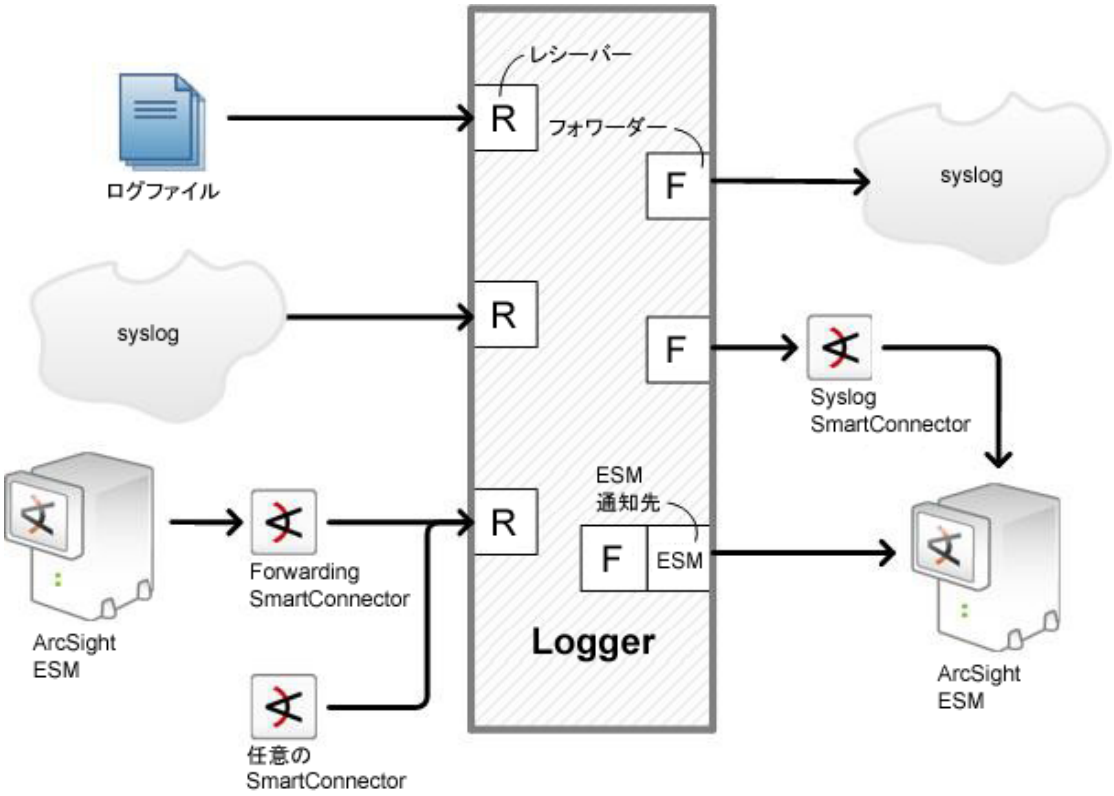
ストレージボリュームは、外部ストレージかローカルストレージかを問わず、それぞれ個別の保有ポリシーを持つ複数のストレージグループに分割できます。最初にLoggerを設定したとき、2つのストレージグループが作成されます。新規のストレージグループを後で追加することができます。ストレージグループのサイズを増減したり、定義した保有ポリシーを変更したりすることもできます。

ストレージ戦略の詳細については、『Loggerインストールガイド』を参照してください。イベントのストレージの詳細については、「ストレージ」(428ページ)を参照してください。

受信者の設定

Loggerは、イベントをsyslogメッセージ、暗号化されたSmartMessage、共通イベントフォーマット(CEF)メッセージとして受信したり、ログファイルを読み取ることで取得します。伝統的に、syslogメッセージはUser Datagram Protocol (UDP)を使用して送信されますが、Loggerでは、syslogおよびCEFメッセージを、より信頼性の高いTransmission Control Protocol (TCP)を使用して受信することもできます。

また、Loggerは、リモートホスト上のテキストログファイルからイベントを読み取ることもできます。ログファイルには、通常、1行に1つのイベントが格納されるか、複数の行にまたがる複数のイベントメッセージが、改行 (\n) や復帰 (\r) などの文字を使用して区切って格納されます。各イベントにはタイムスタンプが含まれている必要があります。Loggerは、リモートフォルダーをポーリングして、ファイル名パターンに一致する新しいファイルを確認するように設定できます。Loggerは、新しいファイル中のイベントを読み取った後、ファイルを削除または名称変更したり、単に読み取ったことを記録することができます。Loggerは、SCP、SFTP、FTPプロトコル、作成済みのNFSまたはCIFSマウント、SAN (一部のLoggerアプライアンスモデル) を使用してネットワークドライブ上のリモートファイルを読み取ることができます。



また、Loggerは、ArcSightマネージャーからCEF形式のsyslogメッセージとしてイベントを受信することもできます。これらのイベントは、ArcSight Forwarding SmartConnectorと呼ばれる専用のソフトウェアコンポーネントを通じてLoggerに転送され、そこでCEF形式のsyslogメッセージに変換されてからLoggerに送信されます。

- 受信者の設定の詳細については、「受信者」(368ページ) を参照してください。
- SmartConnectorの設定の詳細については、『Loggerインストールガイド』を参照してください。
- ArcSight ESMからのイベントの収集の詳細については、『Loggerインストールガイド』を参照してください。

イベントの分析

イベントを検索し、特定のクエリに一致するイベントの表を生成できます。クエリは、手動で入力するか、イベント表内の用語をクリックすることで自動的に作成できます。クエリでは、英語のキーワード (全文検索)、事前に定義されたフィールド、正規表現を使用できます。Loggerでは、フローベースの検索言語がサポートされており、複数の検索コマンドをパイプライン形式で指定できます。

デフォルトで、ピアのLoggerが設定されている場合でも、Loggerはプライマリデータストアのみに対してクエリを実行します。ただし、選択したピアのLoggerに対しては、クエリを分散するように設定できます。

クエリは、フィルターまたは保存された検索として保存できます。保存したフィルターは、転送するイベントを選択したり、後で同じものに対してフィルター処理を行ったりするために使用できます。保存された検索を使用して、選択したイベントをエクスポートしたり、結果をファイルに保存したりできますが、これは一般にスケジュールされたタスクとして実行されます。

イベントの分析に関する詳細については、以下の各トピックを参照してください。

- 「イベントの検索」(106ページ)
- 「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ)
- 「フィルター」(329ページ)
- 「保存された検索」(333ページ)
- 「パーサー」(392ページ)

イベントのグループ化

ソースIPアドレスとLogger受信者を組み合わせたものをデバイスと呼びます。イベントを受信すると、IPと受信者のペアごとにデバイスが自動的に作成されます。デバイスは手動で作成することもできます。

デバイスは、1つ以上のデバイスグループのメンバーにすることで分類できます。受信イベントは必ず1つのデバイスのみに属しますが、複数のデバイスグループに関連付けることができます。

ストレージルールによって、デバイスグループがストレージグループに関連付けられます。ストレージルールは重要度の順に並べられ、最初に一致したルールによって、受信イベントがどのストレージグループに送信されるかが決まります。

デバイスグループ、デバイス、ストレージグループ、ピアLoggerのそれぞれを使用し、検索条件を使用してイベントをフィルター処理することができます。検索条件は、[分析] ページで対話的に指定するか、フィルターまたは保存された検索を作成するときに指定できます。

イベントのグループ分けに関する詳細情報については、以下のトピックを参照してください。

- 「イベントアーカイブ」(432ページ)
- 「ストレージルール」(430ページ)
- 「ピアの検索 (分散検索)」(115ページ)

イベントのエクスポート

Loggerアプライアンスは、各種ソースにイベントをエクスポートできます。現在のクエリに一致するイベントを、NFSマウントやCIFSマウントにファイルとしてローカルにエクスポートできます。また、アプライアンスがSANをサポートしている場合は、SANにエクスポートすることもできます。

ソフトウェアLoggerからのイベントは、Loggerにローカルにエクスポートするか (<インストールディレクトリ>/data/loggerディレクトリ)、Loggerに接続するために使用しているブラウザーにエクスポートできます。<インストールディレクトリ>/data/loggerディレクトリは、NFSまたはCIFSにマウントできます。

イベントは、外部のアプリケーションで容易に処理できるようにCSV (カンマ区切り値) 形式でエクスポートするか、PDFファイルとしてエクスポートして、簡単なレポートとして使用できます。PDFレポートには、検索結果の表と、結果に対して生成されたすべてのグラフが含まれています。rawイベント (構造化されていないデータ) とCEFイベント (構造化されているデータ) の両方を、PDF形式でエクスポートするレポートに含めることができます。

CEFのイベントには、追加の列が定義され、データがより便利になっていますが、必要に応じてCEFでないイベントもエクスポートできます。エクスポート対象のフィールドは、ユーザーが制御できます。

保存された検索ジョブを作成することで、エクスポートを定期的に実行するようにスケジュールできます。まず、保存された検索を作成します。手作業で作成するか、[分析] ページでクエリを保存します。既存のフィルターに基づいて保存された検索を作成することもできます。保存された検索ジョブは、1つ以上の保存された検索とスケジュールを、エクスポートオプションとともに組み合わせたものです。

イベントのエクスポートに関する詳細については、以下の各トピックを参照してください。

- 「検索結果のエクスポート」(139ページ)
- 「時刻/NTP」(497ページ)
- 「スケジュールされた検索/アラート」(335ページ)

転送者の設定

Loggerは、イベント (受信したイベントまたは過去のイベント) を、UDPまたはTCPを使用して他のホストに送信したり、Logger Streaming SmartConnectorやArcSightマネージャーに送信できます。特定のホストに送信されるイベントはクエリによってフィルター処理できます。その場合、一致するイベントのみが送信されます。送信されるsyslogメッセージは、元のソースIP

とタイムスタンプを渡すように設定するか、Loggerの「送信時刻」とIPアドレスを使用するように設定できます。

syslogメッセージは、syslog SmartConnectorを使用してArcSightマネージャーに送信できますが、組み込みのSmartConnectorを使用してCEFイベントをArcSightマネージャーに直接送信することもできます。Loggerは、大量のイベントを受信し、フィルター処理後のより少ないイベントをArcSightマネージャーに送信するための「ファネル(絞り込み)」としての役割を果たすことができます(「Loggerは、選択したイベントをArcSightマネージャーに転送するための「ファネル(絞り込み)」としての役割を果たします。」(28ページ)を参照)。

イベントの転送に関する詳細については、以下の各トピックを参照してください。

- 「転送者」(398ページ)
- 「ESM通知先」(419ページ)

ユーザー管理

Logger管理者は、システムの各ユーザーを区別するために、ユーザーアカウントを作成できます。ユーザーアカウントは、それが属するユーザーグループから権限を継承します。ユーザーグループにイベントフィルターを適用して、特定ユーザーが参照できるイベントを制限できます。

ユーザー管理に関する詳細については、以下の各トピックを参照してください。

- 「ユーザ/グループ」(530ページ)
- 「自分のパスワードの変更」(547ページ)
- 「検索グループフィルター」(332ページ)

その他のセットアップとメンテナンス

受信者、フィルター、保存された検索ジョブなど、イベントを除くすべてのLoggerの設定は、設定のバックアップファイルとしてディスクにバックアップし、後で復元できます。

デバッグなどの目的で、Loggerの動作を詳細に記述したログを、必要に応じてブラウザーを通じてダウンロードできます。他のシステム情報を参照したり、さまざまなシステム設定を変更できます。一部の設定については、変更内容を反映するために、システムの再起動が必要です。

Loggerアプライアンスを再起動するには、ユーザーインターフェイス内のコントロールを使用します。ソフトウェアLoggerの場合は、Loggerサービスと関連するプロセスを再起動できます。ソフトウェアLoggerを開始、停止、再起動するには、「ソフトウェアLoggerのコマンドラインオプション」(557ページ)の手順に従ってください。

セットアップとメンテナンスに関する詳細については、以下の各トピックを参照してください。

- 「設定のバックアップとリストア」(468ページ)
- 「ログの取得」(446ページ)

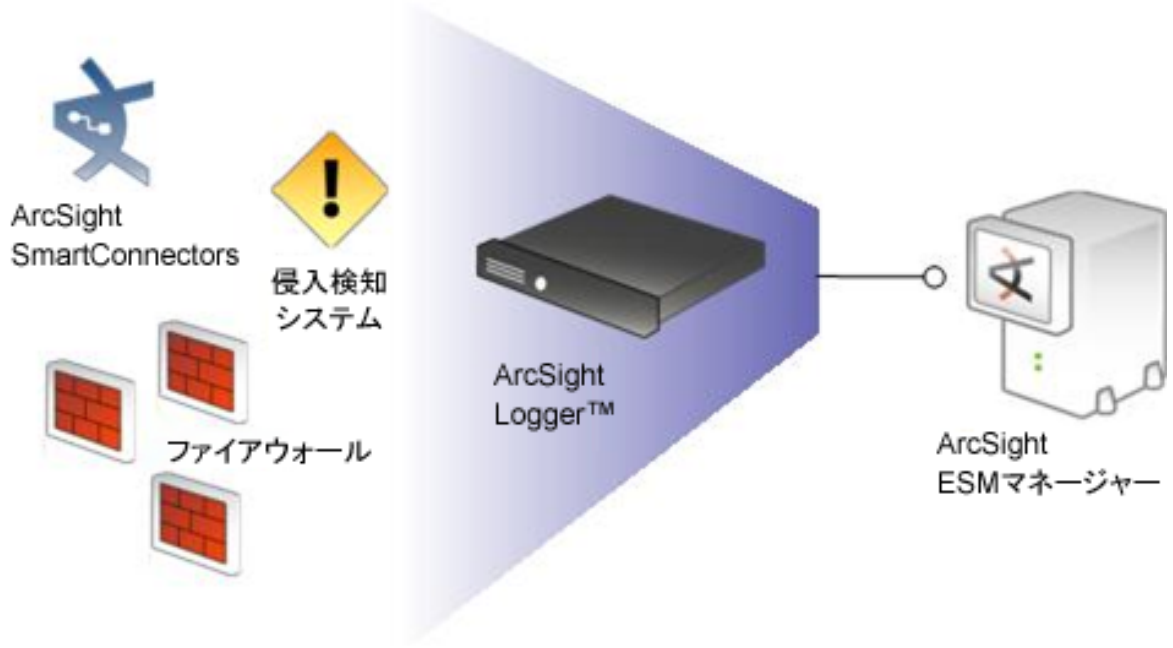
- 「ストレージ」(509ページ)
- 「システム」(491ページ)
- 「ライセンスと更新」(501ページ)
- 「ネットワーク」(493ページ)

展開シナリオ

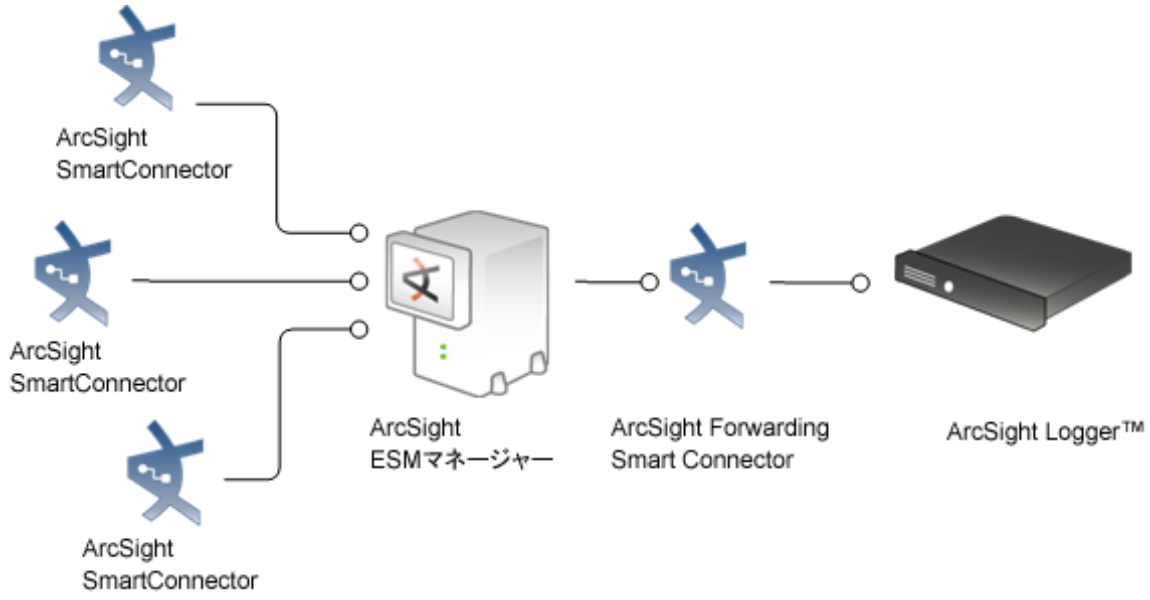
一般に、Loggerは、社内のファイアウォールの内側で物理的なセキュリティ強度が高い場所に展開し、収集したイベント情報に対する改変を防ぎます。Loggerには、他のArcSight製品は不要です。Loggerは、さまざまなハードウェアおよびソフトウェアネットワーク製品によって作成されたsyslogおよびログファイルイベントを受信して転送します。

また、Loggerは、次の図に示すように、ArcSightマネージャーと相互運用できます。Loggerの一般的な用途は、ファイアウォールなどのデータを収集し、データのサブセットをArcSightマネージャーに送信して、リアルタイムな監視と関連付けを行うことです (下図参照)。Loggerは、コンプライアンスまたはサービスレベル合意目的で、未処理のファイアウォールデータを保存できます。

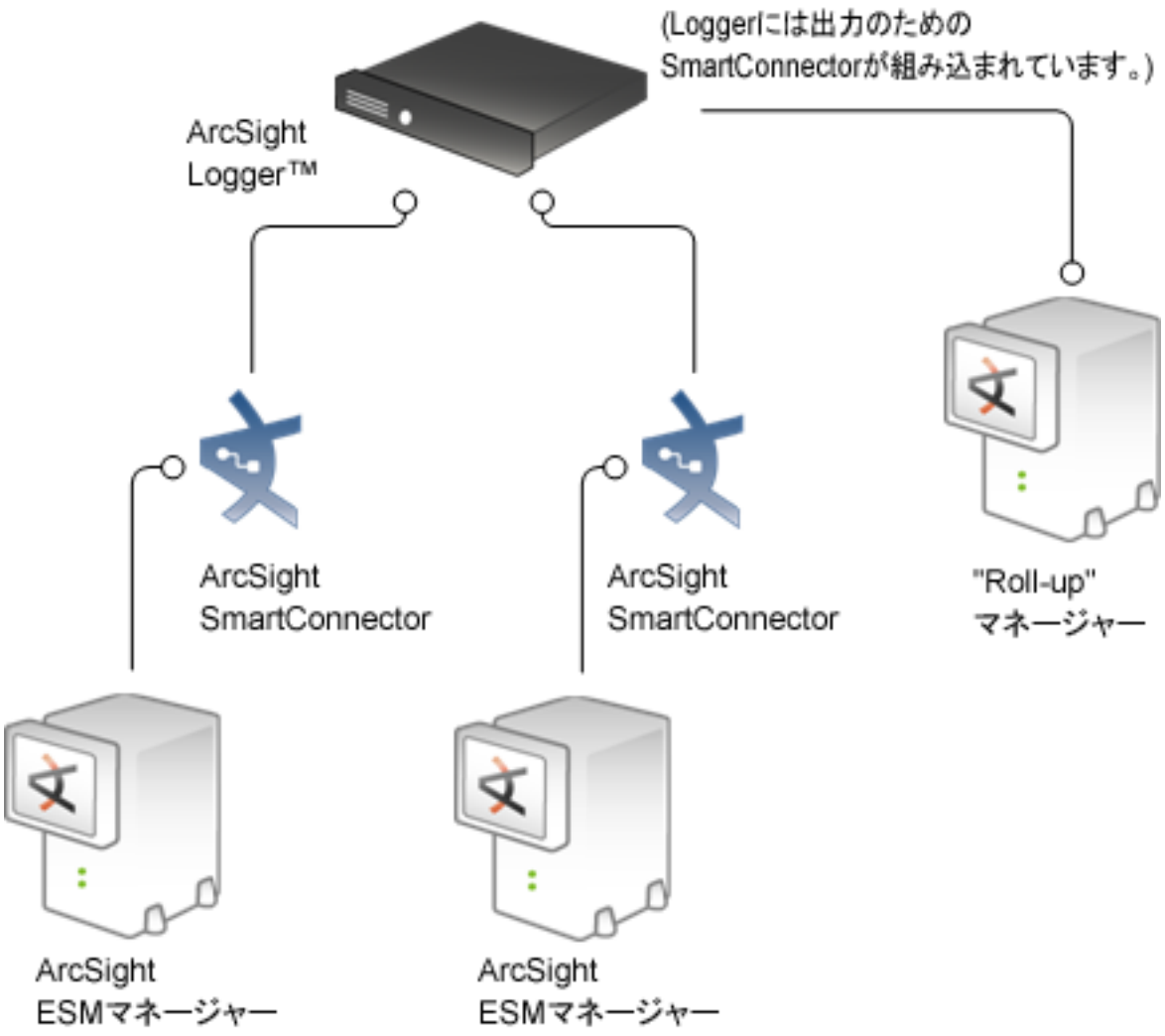
Loggerは、選択したイベントをArcSightマネージャーに転送するための「ファネル (絞り込み)」としての役割を果たします。



Loggerは、ArcSightマネージャーによって送信されたイベントを保存できます。



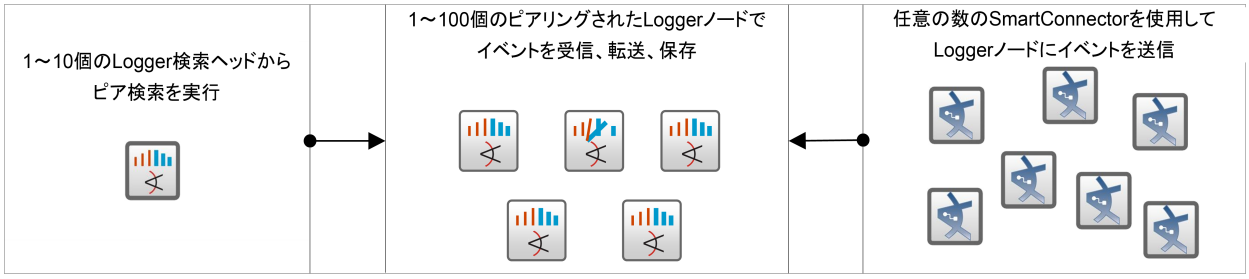
Loggerは、フィルター処理したイベントを、階層型に配置されたArcSightマネージャーに保存および送信できます。



検索ヘッドのセットアップによるピアの検索の高速化

ピアリングされた複数のLoggerと多数のユーザーが存在し、同時に検索を行う必要がある場合は、一部のLoggerをイベントの受信、保存、および転送用に使用し、その他のLoggerをピアの検索のみに使用するように、Loggerをセットアップできます。

ノードは、イベントの受信、保存、および転送に使用されるピアリングされたLoggerです。検索ヘッドは、検索のみに使用されるピアリングされたLoggerです。検索ヘッドは、イベントの転送、受信、または保存を行いません。検索ヘッドを利用するには、検索ヘッドとして使用するLoggerにデータが送信されないようにアーキテクチャーをセットアップする必要があります。



ヒント: 最適な検索速度を実現するには、ノードおよび検索ヘッドの両方に、16 GB以上のRAM (32 GBを推奨) が必要です。

この構成を使用すると、10人のユーザーが検索ヘッドにログインして、指定された10個のノードで同時に検索を実行できます。これをスケールアウトし、10個の検索ヘッドをセットアップすることにより、100人のユーザーが同時に検索を行うことが可能になります。

IPv6データのLoggerへの送信

IPv6データをLoggerに送信するには、バージョン7.5.0以上のSmartConnectorを使用します。詳細については、「SmartConnectorを設定してLoggerにイベントを送信する」(600ページ)、および『SmartConnectorユーザーガイド』の説明と手順を参照してください。

LoggerにIPv6データがある場合は、IPv4アドレスと同様に、IPv6アドレスでフィルター処理を行うことができます。「IPv6アドレスの検索」(121ページ)を参照してください。

一元管理

HPE ADP ArcSight Management Center (ArcMC) では、Loggerおよびコネクターを一元管理し、管理対象のすべてのArcSight ADP製品を1つのパネルで表示できます。

ArcMCを使用すると、管理対象製品の設定を作成またはインポートして、その設定をネットワーク内の同じタイプの製品にすばやくプッシュできるため、1回の操作で管理対象製品を同じように設定することができます。Loggerおよびコネクターに対し、個別にまたは複数まとめて、さまざまなリモート管理タスクを実行できます。ArcMCを使用して実行できるLoggerのタスクには、初期設定、ピア設定、およびユーザー管理などがあります。

詳細については、営業担当者に問い合わせるか、『ArcSight Management Center管理者ガイド』を参照してください。

暗号化されたアプライアンスでのLoggerの実行

Loggerは暗号化されたハードウェア上で実行できるため、保存されている機密データをセキュリティで保護し、コンプライアンス規制やプライバシーの課題に対応することができます。

Webページ (Server Management Software > HP Secure Encryption) から入手可能なHPE Secure Encryptionを使用して、L7600Loggerアプライアンスを暗号化できます。手順については、そのページのTechnical Support> Manualsリンクからアクセスできる PDFおよびCHM形式の『HPE Secure Encryption Installation and User Guide』を参照してください。

L7600Loggerアプライアンスは暗号化可能です。HP Secure Encryptionを使用した暗号化に必要なものがあらかじめインストールされています。暗号化に必要な時間は、暗号化されるサーバー上のデータ量によって異なります。弊社のテストでは、7.5TBのデータが格納されたGen 9アプライアンスの暗号化に約72時間かかりました。暗号化の実行中も、引き続きLoggerを使用できます。既存のLoggerアプライアンスを暗号化した後で、パフォーマンスが低下することがあります。

注意: Loggerを暗号化した後では、暗号化前の状態に復元することはできません。

第2章: ユーザーインターフェイスとダッシュボード

次の各トピックでは、Loggerへの接続方法の概要を示し、Loggerのダッシュボードについて詳しく説明します。Loggerの標準ダッシュボードには、受信者、転送者、ストレージ、CPU、ディスク使用率統計情報のリアルタイムステータスと履歴ステータスが表示されます。ダッシュボードを独自に作成して、関心のあるLogger情報をすべて1か所に表示することもできます。

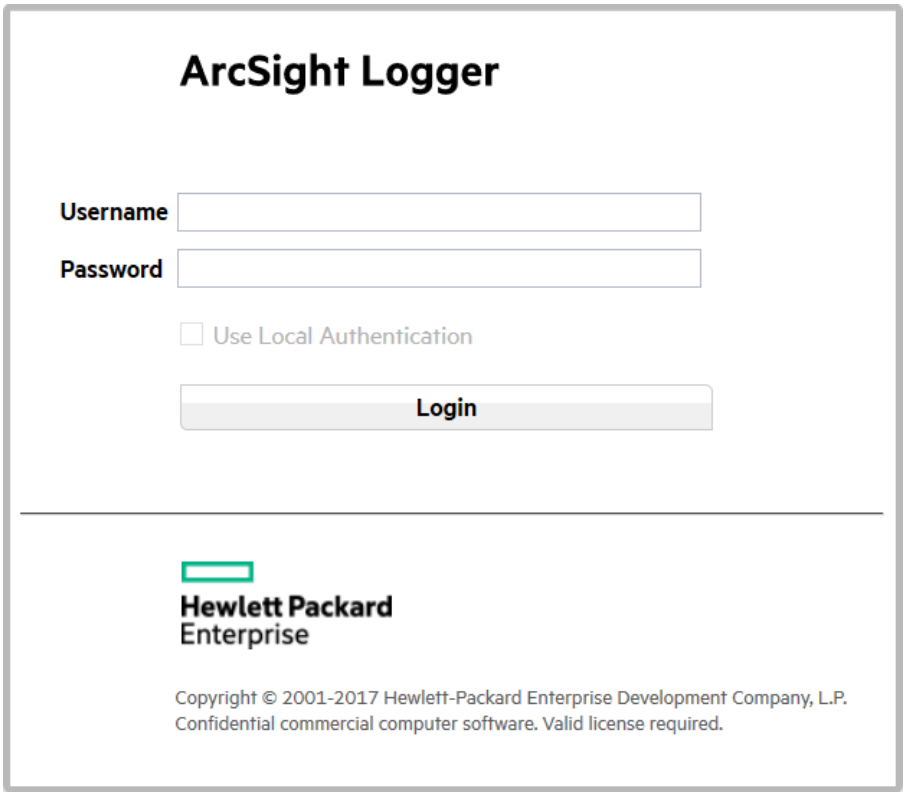
Loggerへの接続

Loggerへの接続とログインは、Chrome、Firefox、Internet Explorerなどの大半のブラウザーで行うことができます。このリリースでサポートされているブラウザーのリストについては、『Release Notes』を参照してください。

Loggerに接続してログインするには

1. Loggerのインストール時に設定したURLを使用し、サポートされているブラウザーを通じてLoggerに接続します。
   - Loggerのアプライアンスについては、`https://<ホスト名またはIPアドレス>`を使用してください
     エンドユーザーライセンス契約 (EULA) が表示されます。EULAを読んで承諾します。
   - ソフトウェアLoggerについては、`https://<ホスト名またはIPアドレス>:<設定済みポート>`を使用してください。このホスト名またはIPアドレスはLoggerソフトウェアがインストールされているシステムを指し、<設定済みポート>は、Loggerのインストール時に設定したポートを指します (該当する場合)。

   ログイン画面が開きます。



2. ユーザー名とパスワードを入力し、[**ログイン (Login)**] をクリックします。初めて接続する場合や、デフォルトの認証情報をまだ変更していない場合は、以下の認証情報を使用します。

   ユーザー名: **admin**
   パスワード: **password**

   - ログインに成功すると、[サマリー] ページ (Loggerのデフォルトホームページ) が表示されます。[サマリー] ページについては、「サマリー」(39ページ) を参照してください。
   - ログインに失敗すると、ログイン画面の上部に「認証失敗」というメッセージが表示されます。正しいユーザー名とパスワードの組み合わせを入力し、再試行してください。

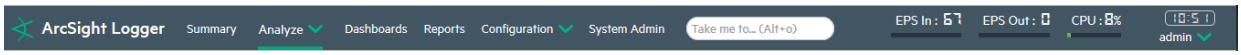
   > **注:** 初めてログインするときにデフォルトのユーザー名とパスワードを使用する場合、後でパスワードの変更が必要になります。

システム管理設定によっては、以下のオプションも使用できる場合があります。

- **パスワードを忘れた場合**: Loggerで [パスワードを忘れた場合] リンクの表示が設定されている場合、このリンクが表示されます。パスワードを変更するには、このリンクをクリックしてください。[パスワードを忘れた場合] リンクの詳細については、「パスワードを忘れた場合」(534ページ) を参照してください。
- **ローカル認証の使用**: [ローカル認証の使用] チェックボックスは常に表示されますが、ログインに失敗した場合にのみアクティブになります。デフォルトでは、このオプションはデフォルト管理者のみが使用できます。[ローカル認証の使用] オプションの詳細については、「ローカルパスワード」(531ページ) を参照してください。

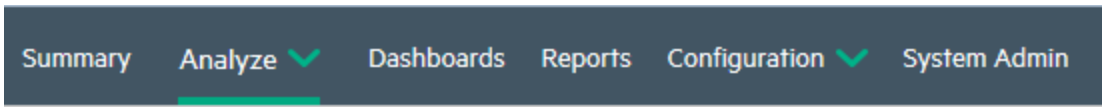
ユーザーインターフェイスの操作

ユーザーインターフェイスのすべてのページの上部には、操作情報バー (ナビバー) があります。



メニュー、移動、ゲージ

[サマリー (Summary)]、[分析 (Analyze)]、[ダッシュボード (Dashboards)]、[レポート (Reports)] メニュータブでは、Loggerの各種の機能と保存されているデータにアクセスできます。

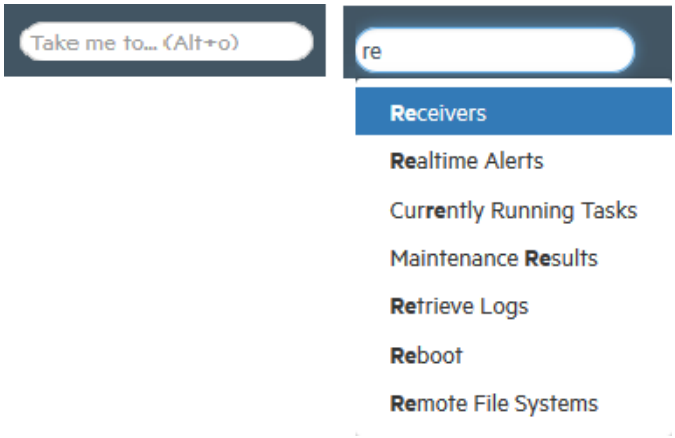


システム設定と管理機能の設定は、[設定 (Configuration)] メニューと [システム管理 (System Admin)] メニューで行うことができます。それぞれのメニューの詳細については、以下のセクションを参照してください。

- [サマリー] メニューのオプションについては、「サマリー」(39ページ) を参照してください。
- [ダッシュボード] メニューのオプションについては、「ダッシュボード」(43ページ) を参照してください。
- [分析] メニューのオプションについては、「イベントの検索と分析」(67ページ) を参照してください。
- [レポート] メニューのオプションについては、「レポート」(162ページ) を参照してください。
- [設定] メニューのオプションについては、「設定」(328ページ) を参照してください。
- [システム管理] メニューのオプションについては、「システム管理」(490ページ) を参照してください。

[移動] ナビゲーションボックス

メニュータブの右にある [**移動**] ナビゲーションボックスでは、UIの任意の場所に素早く簡単に移動できます。[**移動**] 機能を使用すると、機能名の先頭文字を入力するだけで、Loggerの任意の機能に移動できます。

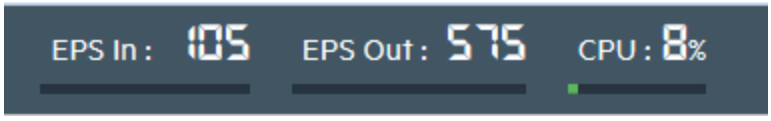


[移動 (Take me to…)] ナビゲーションボックスにアクセスするには、このボックスをクリックするか、ホットキーAlt+o、Alt+p、またはCtrl+Shift+oを使用します。入力すると、一致する機能の一覧がドロップダウンに表示されます。リスト中の項目をクリックするか、Enterを押して指定した機能に移動します。

現在のページのヘルプを開くには、[**移動**] 検索ボックスに「help」と入力します。

ゲージ

画面右上にあるゲージには、スループットとCPU使用率が表示されます。詳細は [モニター] ダッシュボードに表示されます (「ダッシュボード」(43ページ) を参照)。

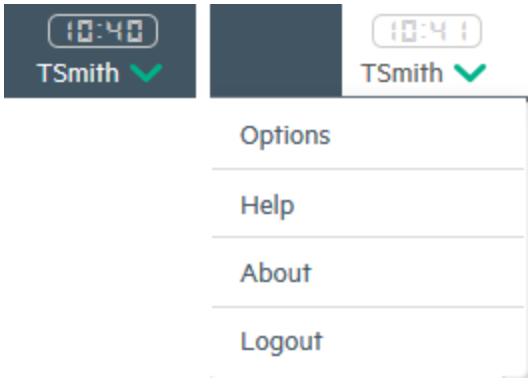


ゲージの範囲は [オプション] ページで変更できます (「Loggerのオプション」(37ページ) を参照)。

サーバークロック、現在のユーザー、[オプション] ドロップダウン

サーバークロック、現在ログインしているユーザーの名前、および [オプション] ドロップダウンの矢印がゲージの右に表示されます。

サーバークロックには、Loggerサーバーのシステム時刻が表示されます。これは、ユーザーのローカル時刻と違っている可能性があります。



クロックの下には、現在のユーザーのログイン名が表示されます。ユーザーのログイン名の右側にはドロップダウンの矢印があり、ここから、「Loggerのオプション」(37ページ)と「ヘルプ、バージョン情報、およびログアウト」(42ページ)のオプションを開くことができます。

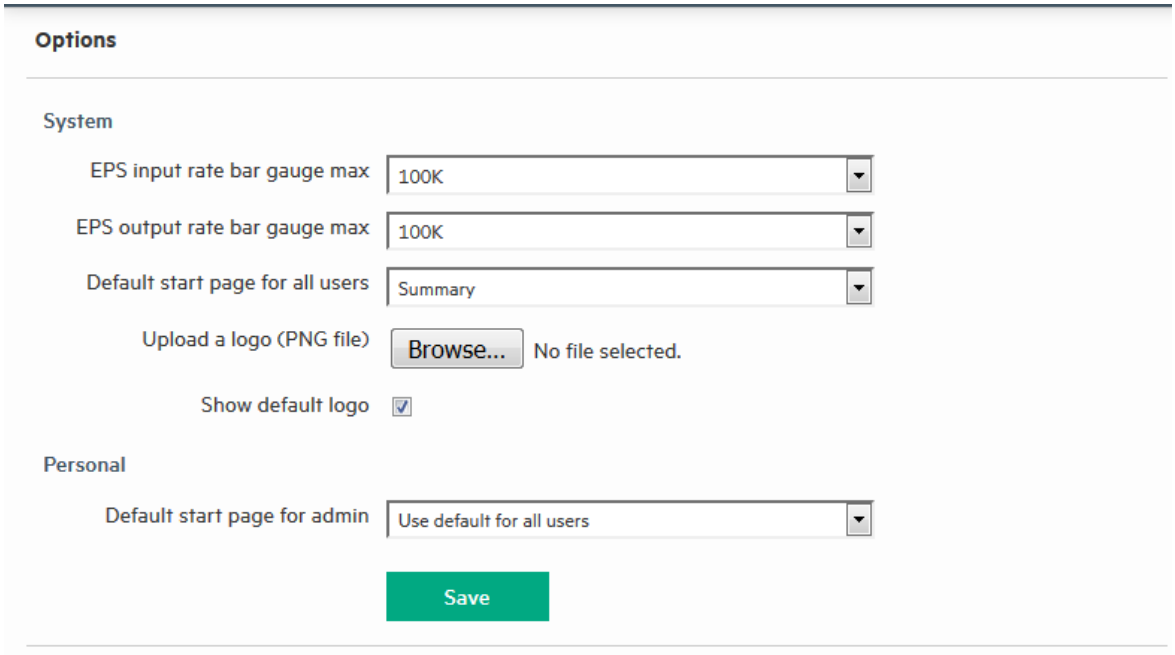
Loggerのオプション

[オプション]ドロップダウンの矢印をクリックすると、[オプション]ページのほか、「ヘルプ、バージョン情報、およびログアウト」(42ページ)のオプションにアクセスすることができます。

[**オプション**]ページでは、すべてのユーザーのデフォルト開始ページ(ホームページ)と、個々のユーザー専用の開始ページを設定でき、デフォルトロゴの代わりにカスタムのロゴをアップロードし、表示させることができます。

いずれかのユーザーインターフェイスページから [オプション] ページにアクセスするには

ユーザー名の横の下矢印 (▼) をクリックし、[**オプション**]を選択します。



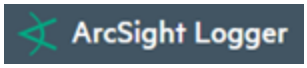
最大EPSのカスタマイズ

[EPSイン] ゲージと[EPSアウト] ゲージの最大レートを設定するには、[オプション] メニューで **[EPS入力レート棒グラフのゲージの最大値]** と **[EPS出力レート棒グラフのゲージの最大値]** のそれぞれのドロップダウンを使用します。イベントレートが指定した最大を超えると、範囲が自動的に広がります。

ロゴのカスタマイズ

オプションメニューの [**ロゴ (PNG ファイル) のアップロード**] オプションからHPE ArcSight Loggerのロゴをカスタムロゴで置き換えることができます。ロゴは.png形式である必要があります。ロゴの推奨サイズは150 × 30ピクセル、最大ファイルサイズは1MBです。

150 × 30ピクセルのロゴ:



カスタムのロゴを表示するには

1. [オプション] メニューの [**ブラウズ**] をクリックして、使用するロゴを選択し、[**開く**] をクリックします。ロゴの名前が [ブラウズ] ボタンの横に表示されます。
2. [**デフォルトロゴの表示**] のチェックを外します。ログインページとメニューバーにカスタムロゴが表示されます。

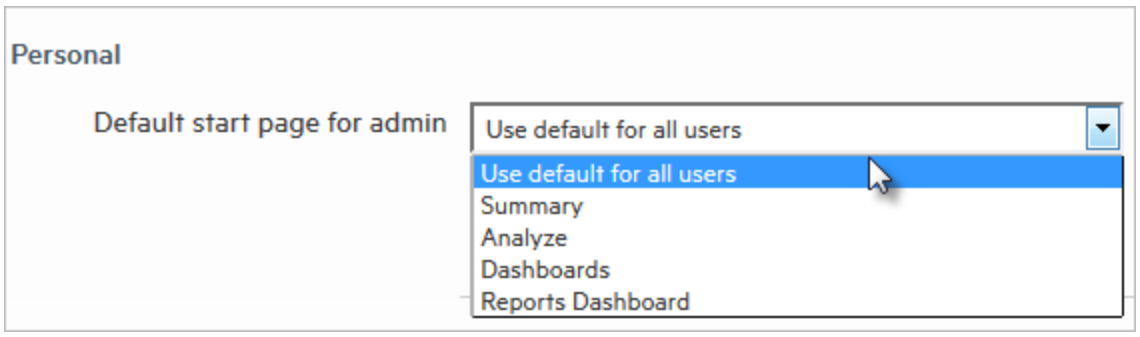
デフォルトのHPE ArcSightのロゴを表示するには

[**デフォルトロゴの表示**] チェックボックスをオンにします。

開始ページのカスタマイズ

個人用の開始ページを設定するには

[オプション] メニューの [個人用 (Personal)] セクションから、いずれか1つの開始ページオプションを選択します。



[すべてのユーザーのデフォルトの開始ページ (Default start page for all users)] オプションは、ユーザーのログイン後に表示するユーザーインターフェイスページを示します。すべてのユーザーのデフォルト開始ページ (ホームページ) と、個々のユーザー専用の開始ページを設定できます。専用の開始ページの設定方法については、次の表を参照してください。

設定内容	設定方法
すべてのユーザーに対し同じ開始ページを設定	[すべてのユーザーのデフォルトの開始ページ] オプションを目的のページに設定します。 これは、Loggerのグローバルな設定です。この設定をオーバーライドするには、[<ユーザー名>のデフォルトの開始ページ] オプションを使用して、ユーザーごとに開始ページを設定します。 [すべてのユーザーのデフォルトの開始ページ] オプションを [ダッシュボード (Dashboards)] に設定すると、デフォルトのダッシュボードである [モニター] ダッシュボードがすべてユーザーに対して表示されます。ただし、他のダッシュボードをデフォルトとして設定したユーザーについては例外です。詳細については、「デフォルトのダッシュボードの設定」(66ページ)を参照してください。
特定のユーザーに対し異なる開始ページを設定	[<ユーザー名> のデフォルトの開始ページ] オプションを目的のページに設定します。 この設定は、グローバル設定の [すべてのユーザーのデフォルトの開始ページ] よりも優先されます。 このオプションが「すべてのユーザーにデフォルトを使用」に設定されている場合、グローバルデフォルトページ ([すべてのユーザーのデフォルトの開始ページ]) の値がすべてのユーザーで使用されます。
特定のユーザーに特定のダッシュボードを設定 または すべてのユーザーに特定のダッシュボードを設定	[<ユーザー名> のデフォルトの開始ページ] オプションをダッシュボードに設定します。 [モニター] ダッシュボードが、すべてのユーザーに表示されるデフォルトダッシュボードになります。ただし、1人以上のユーザーに別のダッシュボードを表示する場合は、そのユーザーでログインしたときに、目的のダッシュボードをデフォルトとして設定します。詳細については、「デフォルトのダッシュボードの設定」(66ページ)を参照してください。

サマリー

Loggerのデフォルトホームページは [サマリー] ページです。(別のページをホームページとして使用する方法については、「Loggerのオプション」(37ページ)を参照してください)。[サマリー] ページは、Loggerに関する要約されたイベント情報を1画面に表示するダッシュボードです。このページでは、受信イベントアクティビティやインデックス作成の状況を確認できます。Loggerのプライマリストレージにあるイベント (保有またはアーカイブデータに起因してエージアウトされていないもの) を使用してサマリー情報が生成されます。

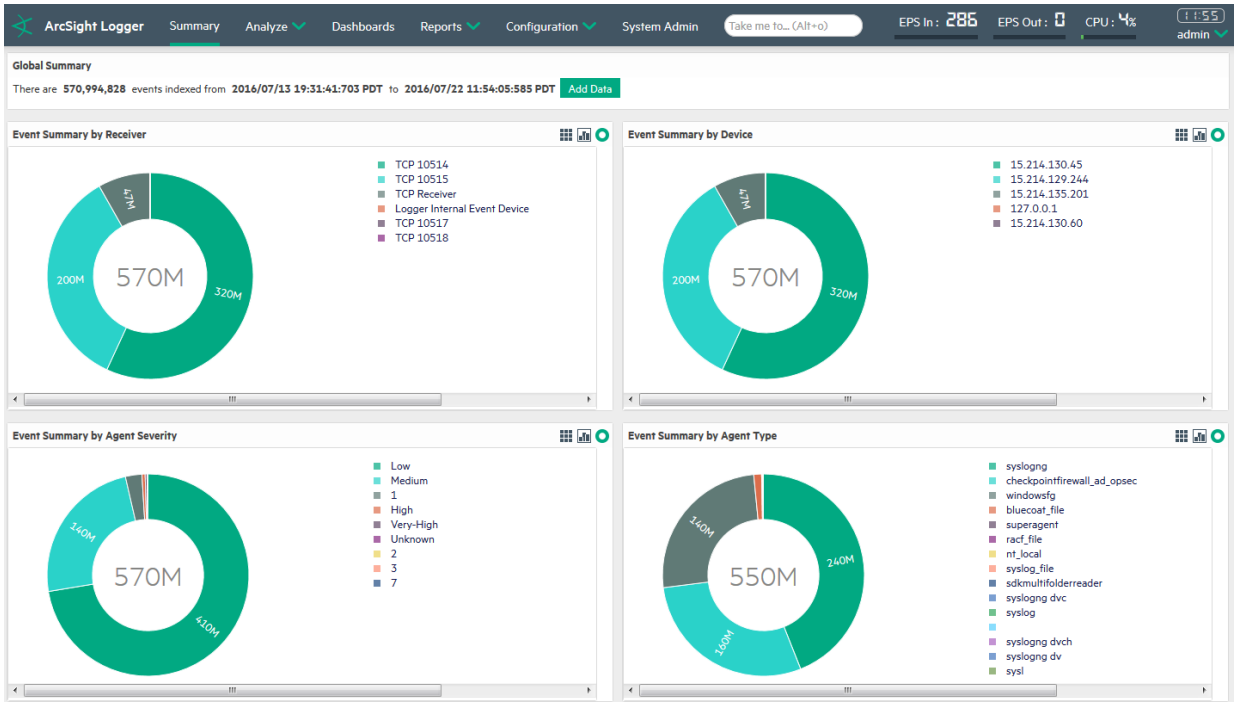
Loggerのホームページである [サマリー] ページでは、データが4つのパネルに表示されます。各パネルはデフォルトでドーナツグラフで表示されます。該当するアイコンをクリックして、各パネルの表示設定を変更することができます。

- リストは、を選択します。
- 縦棒グラフは、を選択します。
- ドーナツグラフは、を選択します。

注: ドーナツグラフのドーナツの中央には、イベント合計が表示されます。これは、グラフに表示されるイベントの総数です。イベント数が1000を上回ると、イベント合計の表示には、標準のメートル法接頭辞 (k、M、G、T) から該当するものが使用されます。

[サマリー] ページの各パネルには、最大で30個の項目が表示されます。30を上回る場合は、イベント数の上位30項目が表示されます。

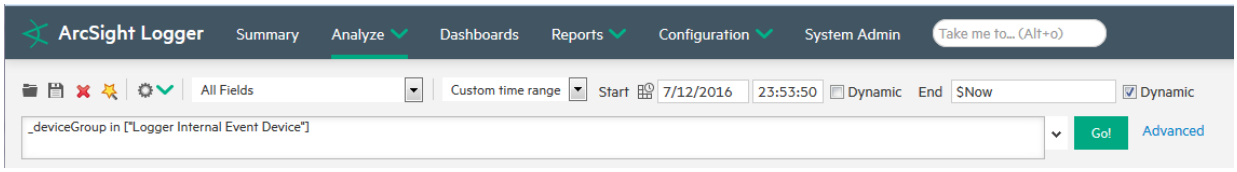
Loggerのホームページ[サマリー] ページ



カラム、ドーナツグラフのスライス、または凡例の項目の上にポインターを移動すると、それぞれに関する情報が表示されます。さらに、特定のリソース (受信者、デバイス、エージェントの緊急度、エージェントの種類) に絞って掘り下げ、イベントの詳細情報を表示できます。詳細情報を表示するには、カラム、ドーナツグラフのスライス、リストリソースをクリックしてイベントを検索します。[検索] ページが開き、検索ボックスが表示されます。検索ボックスの中には、[サマリー] ページでクリックした情報を生成した検索内容が自動的に表示されます。[開始 (Start)] フィールドには、システムに格納されている最も古いイベント (保有データに起因してエージアウトされていないイベント) の時刻が表示され、[終了 (End)] フィールドには現在の時刻が表示されます。

たとえば、[受信者別イベントサマリ (Event Summary by Receiver)] の [Logger 内部イベントデバイス (Logger Internal Event Device)] をクリックした場合、**[分析 (Analyze)] > [検索]** ページを開くと、ページには次のクエリが表示され、検索を実行できます。必要に応じて検索

クエリをさらに調整し、ニーズに合わせて検索結果をフィルター処理することができます。検索を再度実行するには、**[実行! (Go!)]** をクリックします。



[サマリー] ページを変更したり、他のパネルを追加したりすることはできません。他の情報を表示する必要がある場合は、カスタムダッシュボードを作成できます (「ダッシュボード」(43ページ) を参照)。

[サマリー] ページに表示される情報はローカルLoggerのみの情報であり、ピアLoggerが設定されている場合でも、ピアの情報は含まれません。

[サマリー] ダッシュボードパネル

- **[グローバルサマリー]:** 画面上に表示されている期間中に、Logger上でインデックス作成されたイベント数を表示します。この期間は、Loggerで設定されている保有ポリシーによって変わります。開始時刻は、Loggerが再起動されてからLoggerに格納されていて、保有ポリシーでエージアウトされていない最も古いイベントの時間です。上部の **[データの追加]** (Add Data) ボタンをクリックすると [受信者] ページが開き、Loggerにログデータを渡す受信者を追加および管理できます。受信者の管理の詳細については、「受信者」(368ページ) を参照してください。
- **[受信者別イベントサマリ]:** Loggerに設定されている受信者のリスト、各受信者上で受信したイベントの数 (Loggerのプライマリストレージにあり、保有またはアーカイブデータに起因してエージアウトされていないイベント)、および各受信者で最後に受信したイベントのタイムスタンプを表示します。受信者が削除されても、そのサマリー情報は、その受信者で受信したイベントがLoggerのプライマリストレージからエージアウトされるまで表示され続けます。ただし、受信者名は、削除された受信者の受信者ID (数字列) に変わります。
- **[デバイス別イベントサマリ]:** デバイスは、名前が付けられたイベントソースであり、IPアドレス (またはホスト名) と受信者名からなります。[デバイス別イベントサマリ] パネルには、Loggerに設定されているデバイスのリスト、各デバイス上で受信したイベントの数 (Loggerのプライマリストレージにあり、保有またはアーカイブデータに起因してエージアウトされていないイベント)、および各デバイスで最後に受信したイベントのタイムスタンプが表示されます。デバイスが削除されても、そのサマリー情報は、そのデバイスで受信したイベントがLoggerのプライマリストレージからエージアウトされるまで表示され続けます。ただし、デバイス名をクリックして、削除されたデバイスに関連付けられているイベントを表示することはできません。
- **[エージェントの緊急度別イベントサマリ]:** ArcSight SmartConnectorからLoggerへの受信イベントの緊急度レベルのリスト、各緊急度レベルの受信イベントの数、および各緊急度レベルの最後に受信したイベントのタイムスタンプ。Loggerのプライマリストレージにあるイベント (保有またはアーカイブデータに起因してエージアウトされていないイベント) のみが、この情報のサマリーを作成する際に考慮されます。

- **[エージェントタイプ別 イベント サマリ]:** LoggerにイベントをSend しているArcSight SmartConnectorのリスト、各SmartConnectorからReceive したイベントの数 (Loggerのプライマリストレージにあり、Retain またはアーカイブデータに起因してエージアウトされていないイベント)、および各SmartConnectorから最後にReceive したイベントのタイムスタンプをDisplay します。SmartConnectorがDelete されても、そのサマリー情報は、そのSmartConnectorからReceive したイベントがLoggerのプライマリストレージからエージアウトされるまでDisplay され続けます。

[サマリー] ページでの検索グループフィルターの効果

ストレージグループにAssign する権限をApply する検索グループフィルターは、[サマリー] ページにDisplay される内容にApply されます。ただし、デバイスグループに権限をApply する検索グループフィルターはApply されません。そのため、[サマリー] ページには、ユーザーが権限を持っていないデバイスグループ内のイベントの数がContain まれています。しかし、ユーザーがドリルダウンしてイベントをDisplay しようとすると、アクセス権に基づいて結果が返されます。これは、検索クエリが [分析] ページ上でExecute され、すべての種類の検索グループフィルターがApply されるためです。同様に、検索グループフィルターが、ストレージグループとデバイスグループの両方に権限をApply する場合、ストレージグループの権限のみが [サマリー] ページにApply されます。

ヘルプ、バージョン情報、およびログアウト

[オプション] ドロップダウン矢印をクリックすると、次のオプションと「Loggerのオプション」(37ページ) ページにアクセスすることができます。

オンラインヘルプにアクセスするにはいずれかのユーザーインターフェイスページから、ユーザー名の横の下矢印 () をクリックし、[**ヘルプ**] をSelect します。

ヒント: Loggerの最新ドキュメントは、Protect 724のArcSight製品マニュアルのコミュニティからAdobe Acrobat PDF形式でProvide されています。

バージョン情報にアクセスするにはLoggerいずれかのユーザーインターフェイスページから、ユーザー名の横の下矢印をクリックし、[**バージョン情報**] をSelect します。

Loggerからログアウトするにはいずれかのユーザーインターフェイスページから、ユーザー名の横の下矢印をクリックし、[**ログアウト**] をSelect します。[ログイン] 画面に戻ります。

ヒント: ログアウトは、誰も操作していないLoggerセッションをPermit されていないユーザーが使用する機会をなくすための、優れたセキュリティ慣習です。Loggerは、ユーザーが設定した時間 (デフォルトでは15分) 後に自動的にログアウトします。この時間をChange するには、「ユーザ/グループ」(530ページ) をSee してください。

注意: ブラウザーウィンドウを閉じるだけでは自動的にログアウトしません。悪意のあるユーザーがブラウザーをRestart し、Loggerセッションを再開する可能性をなくすために、[**ログア**

ウト] リンクをクリックしてください。

ダッシュボード

ダッシュボードは、関心のあるLogger情報を1か所で表示できるようにしたものです。デフォルトダッシュボードのいずれかを選択して表示するか、独自のカスタムダッシュボードを作成することができます。

各Loggerダッシュボードには、以下の種類の1つ以上のパネルが含まれています。

- **検索結果:** [検索結果] パネルには、パネルに関連付けられているクエリに一致するイベントが表示されます。
- **モニター:** [モニター] パネルには、受信者、転送者、ストレージ、CPU、ディスクなどの各種Loggerコンポーネントのリアルタイムなステータスと履歴ステータスが表示されます。
- **サマリー:** [サマリー] パネルには、特定のリソースタイプまたはフィールドタイプの受信イベント数、そのリソースタイプまたはフィールドタイプの最後に受信したイベントのタイムスタンプなど、Loggerに関する要約されたイベント情報が表示されます。

デフォルトダッシュボード

Loggerには、以下で説明するデフォルトダッシュボードがいくつか用意されています。別のダッシュボードをデフォルトとして設定していなければ、[モニター] ダッシュボードがデフォルトで表示されます。

- [イベント数] ダッシュボード (「[イベント数] ダッシュボード」(57ページ) を参照) には、各受信者または転送者が処理したイベントの数が表示されます。
- [Intrusion and Configuration Events] ダッシュボード (「[Intrusion and Configuration Events] ダッシュボード」(54ページ) を参照) には、システムの設定変更および侵入に関する情報が表示されます。
- [Login and Connection Activity] ダッシュボード (「[Login and Connection Activity] ダッシュボード」(55ページ) を参照) には、システム上のログインおよび接続アクティビティに関する情報が表示されます。
- [モニター] ダッシュボードには [サマリー] パネルが表示され、CPU使用率、イベントフロー、受信者、転送者、ストレージグループのステータスがサマリービューに表示されます。このダッシュボードで利用できる他のパネルとしては、[プラットフォーム]、[ネットワーク]、[Logger]、[受信者]、[転送者]、[ストレージ] があります。これらのビューについては、「[モニター] ダッシュボード」(45ページ) で詳しく説明します。

[システム概要] ダッシュボードを除き、デフォルトダッシュボードで使用できるパネルを変更または調整することはできません(「システム概要ダッシュボード」(52ページ)を参照)。ただし、カスタムダッシュボードに特定の[検索結果]パネルを追加することは可能です(「カスタムダッシュボードの作成と管理」(60ページ)を参照)。

[モニター] パネルと[サマリー] パネルを追加することもできます。これらのパネルは、デフォルトの[モニター] ダッシュボードや[サマリー] ダッシュボードと同じ情報を提供しますが、モジュール形式になっており、特定のビューを選択できます。(デフォルトの[サマリー] ダッシュボードの詳細については、「サマリー」(39ページ)を参照してください。)

たとえば、すべての受信者の過去4時間のEPSを表示する場合は、パネルタイプ[モニター(グラフ)]を追加し、[グラフ]として[(Logger) すべてのEPSアウト - すべてのEPSイン - 4時間]を選択できます。また、転送者のEPSを表形式で表示する場合は、[モニター(転送者)]パネルタイプを選択します。同様に、Logger上の受信者のサマリー情報のみを表示するには、タイプ[サマリー(受信者)]のパネルを追加します。4つのサマリーパネル([エージェントの緊急度]、[エージェントタイプ]、[受信者]、および[デバイス])の他に、ユーザー定義のサマリーパネルを作成して、インデックスが付いた、時間以外のフィールドを選択し、これによりイベントサマリーを分類できます。たとえば、「destinationAddress」で分類されたイベントサマリーを表示するサマリーパネルを追加する場合は、このフィールドがLogger上でインデックス作成されていれば、タイプが[サマリー(ユーザー定義)]のパネルを追加できます。

また、追加する[モニター]および[サマリー]パネルに表示されるリソースのいずれかにドリルダウンして、[分析(検索)]ページで特定のリソースまたはフィールド値別にイベントを表示することもできます。たとえば、[モニター]パネルのストレージグループをクリックして、その過去24時間以内のイベントを表示することができます。また、イベント名 [Network Usage - Inbound]をクリックして、過去1時間のその名前のすべてのイベントを表示することができます。さらに、[モニター]パネルに表示されるいずれかのリソースの[設定]ページにアクセスして、リソースを設定することもできます。たとえば、受信者を設定する場合、[モニター(受信者)]パネルの上部にある[設定]リンクをクリックします。

デバイスグループに対する権限を制限する検索グループフィルターは、サマリーパネルでは適用されません。そのため、サマリーパネルには、ユーザーが権限を所有していないデバイスグループ内のイベントの数が含まれています。しかし、ユーザーがドリルダウンしてイベントを表示しようとすると、アクセス権に基づいて結果が返されます。これは、検索クエリが[分析]ページ上で実行され、すべての種類の検索グループフィルターが適用されるためです。同様に、検索グループフィルターが、ストレージグループとデバイスグループの両方に権限を適用する場合、ストレージグループの権限のみがサマリーパネルに適用されます。

ユーザーは、共有ダッシュボードとプライベートダッシュボードを作成できます。

- 共有ダッシュボードは、適切な権限を所有するすべてのユーザーが参照できます。
- プライベートダッシュボードは、作成者または「admin」権限を所有するユーザーのみが参照できます。
- いずれのダッシュボードも、編集または削除できるのは、作成者または「admin」権限を所有するユーザーのみです。

共有ダッシュボードにアクセスするユーザーは、ダッシュボードに表示される情報を参照するための権限を所有している必要があります。権限を所有していない情報は表示されず、情報が表示されない理由を示すメッセージが、関連付けられているパネルに表示されます。

[モニター] ダッシュボード

デフォルトで表示される [モニター] ダッシュボードには、受信者、転送者、ストレージ、CPU、およびディスク使用率統計情報のリアルタイムなステータスと履歴ステータスが表示されます。ソフトウェアLoggerでは、CPUおよびディスク使用率統計情報は、Loggerプロセスによるリソースの使用量だけでなく、システム全体で使用されるリソースの量を示します。

ドロップダウンメニューを通じて使用できるモニターパネルは、[サマリー]、[プラットフォーム]、[ネットワーク]、[Logger]、[受信者者]、[転送者]、[ストレージ] があります。これらのデフォルトパネルを変更または調整することはできませんが、最も関心のある項目を監視するための独自のダッシュボードを作成できます。詳細については、「カスタムダッシュボードの作成と管理」(60ページ) を参照してください。

[サマリー] パネルを除くすべてのモニターパネルには、期間を制御するためのドロップダウンメニューが含まれています。[サマリー] パネルには、代わりにボタンが表示されます。どちらの場合も、履歴データの期間として、4時間、24時間、7日間、30日間、90日間、365日間の中から1つを選択できます。データ上にポインターを移動すると、詳細が表示されます。2つのフィールドを表示するダッシュボードの場合、両フィールドの詳細が表示され、凡例には、各フィールドを表す色が表示されます。

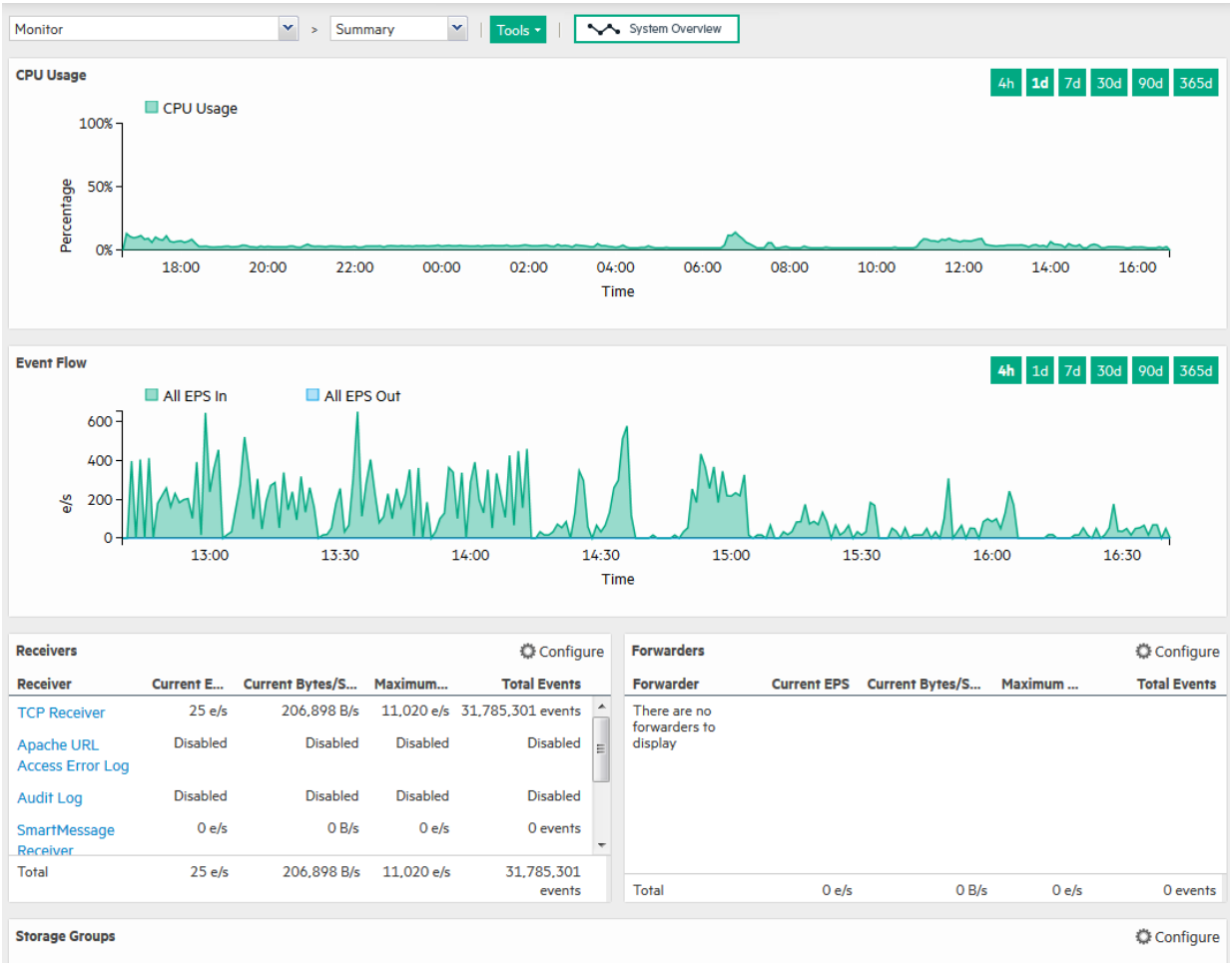
これらのダッシュボードでは、秒あたりのイベント数 (e/s) が表示されます。数が1000を上回る場合、標準のメートル法接頭辞 (k、M、G、T) が使用されます。1000未満の数は整数値で表示されます。

[システム概要] ダッシュボードには、これらのパネルが別の形式で表示されます。このような表示の詳細については、「システム概要ダッシュボード」(52ページ) を参照してください。

[モニター] ダッシュボードの [サマリー] パネル

デフォルトで表示される [サマリー] パネルには、CPU使用率、イベントフロー、受信者、転送者、ストレージグループのステータスがサマリービューに表示されます。

[モニター (Monitor)] ダッシュボード - [サマリー (Summary)] パネル



[サマリー] パネルで受信者、転送者、またはストレージグループ名をクリックすると、[検索] ページにジャンプし、選択したリソースがクエリに追加されます。

また、**[設定 (Configure)]** (Configure) をクリックして、受信者、転送者、ストレージグループの [設定] ページを開くこともできます。

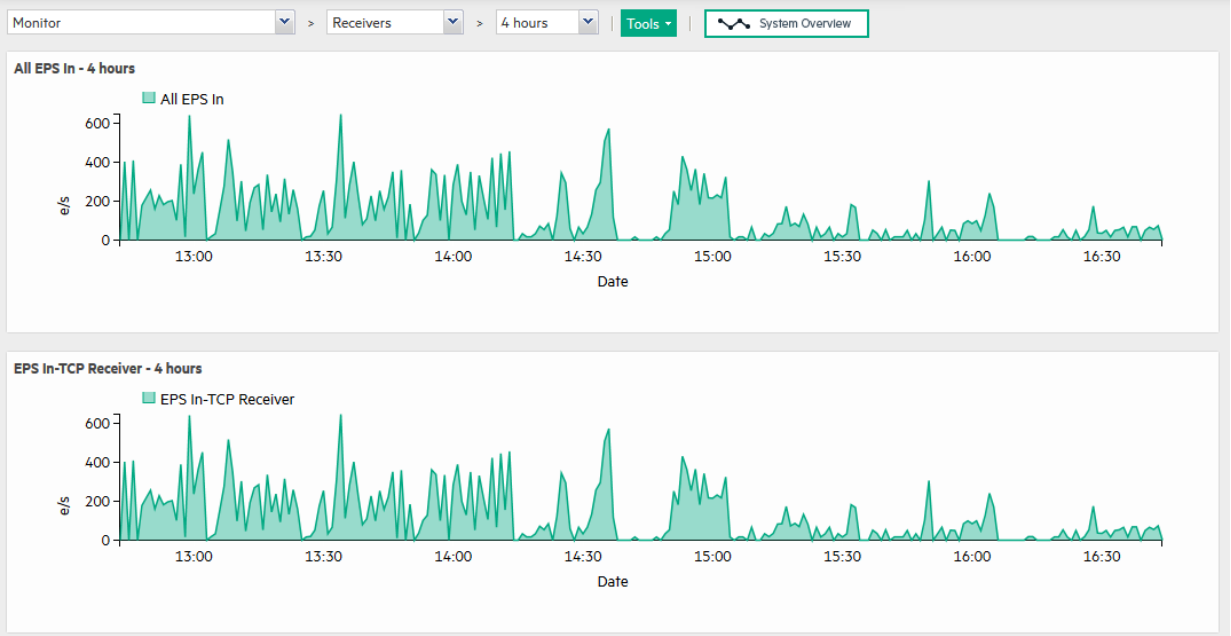
注: ストレージグループに割り当てられる合計スペースには、グループがほぼ一杯のときでも新しいイベントを受信できるように予約された一定の量が含まれています。その結果、ストレージグループの使用スペースのパーセンテージが100%に達することはありません ([モニター] > [サマリー] パネルに表示)。最小設定を使用してインストールされたソフトウェア

Loggerの場合は、各ストレージグループの最大の[% が使用済み] ([モニター] > [サマリー] パネル) は、66.33%です。(それぞれ3 GBの2つのストレージグループ。各グループで、新しいイベント用に1 GBが予約されます。2 GBのスペースが使用され、新しいイベントが最後の1 GBに書き込まれている最中に、Loggerは保有処理を自動的に起動し、使用済みスペースの1 GBを再利用します。そのため、各ストレージグループの[% が使用済み] フィールドは、最大で66.33%にしかなりません)。

[モニター] ダッシュボードの[受信者] パネル

[モニター] ダッシュボードの[受信者] パネルには、受信したすべての秒あたりのイベント数 (EPS) と、設定されている受信者ごとの値が表示されます。受信者のリストには、無効になっている受信者を含め、システムが認識しているすべての受信者が含まれます。(新しい受信者を作成したり、受信者を有効または無効にしたりするには、「受信者の使用」(374ページ) を参照してください。)

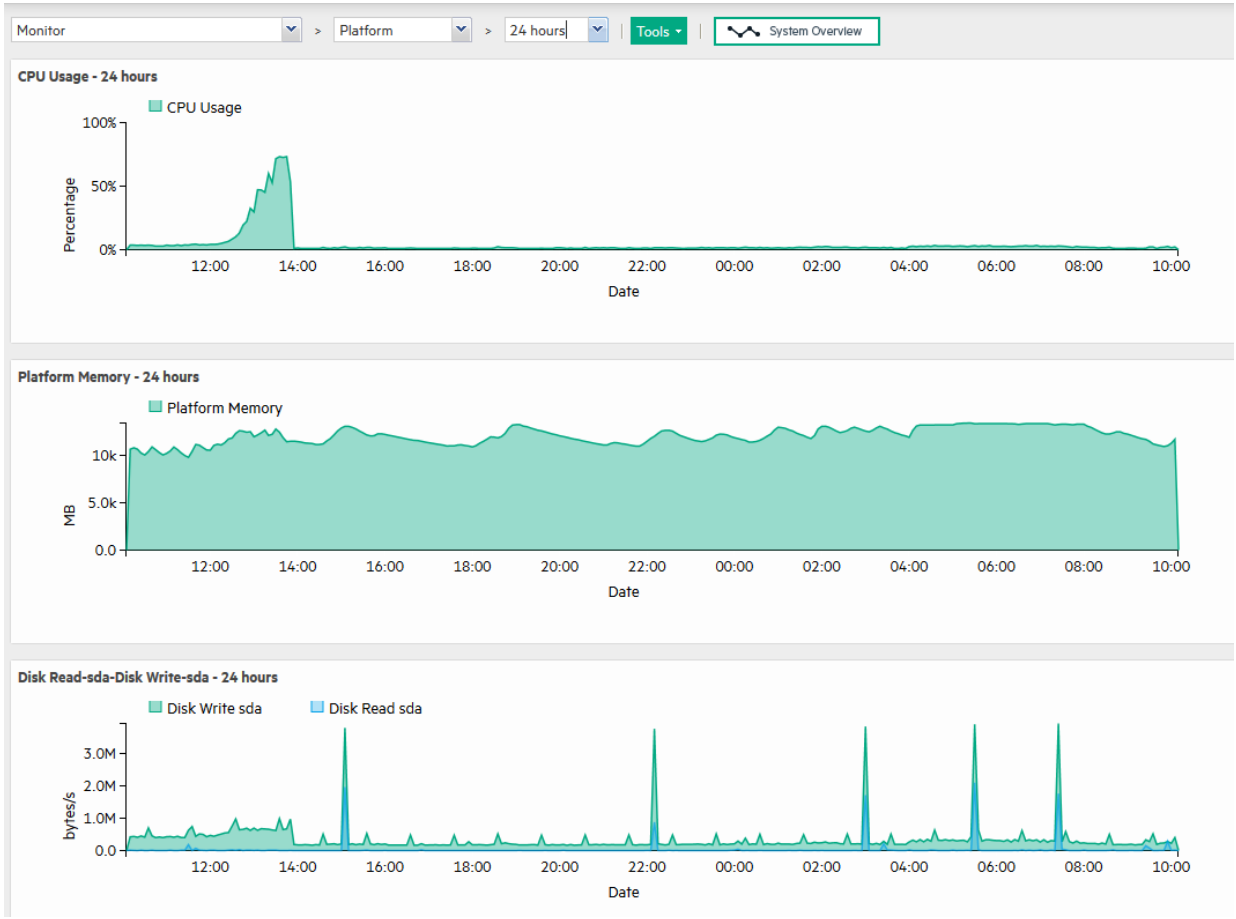
[モニター (Monitor)] ダッシュボード - [受信者 (Receivers)] パネル



[モニター] ダッシュボードの [プラットフォーム] パネル

[プラットフォーム] モニターパネルには、CPU使用率、メモリ使用率、ネットワーク上の送受信バイト数、rawディスク読み書き回数が表示されます。

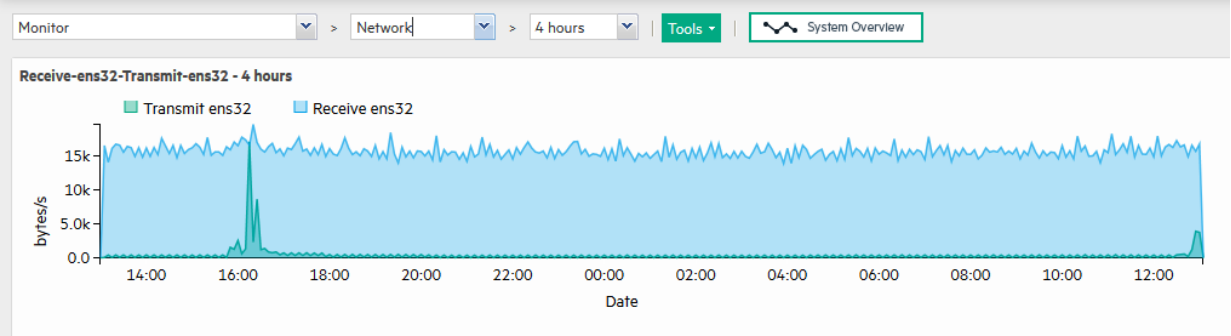
[モニター (Monitor)] ダッシュボード - [プラットフォーム (Platform)] パネル



[モニター] ダッシュボードの [ネットワーク] パネル

[ネットワーク] モニターパネルには、各ネットワークインターフェイスカードのグラフが表示されます (ネットワークインターフェイスカードの数は、ハードウェアモデルによって異なります)。グラフには、受信バイト数の上に送信バイト数がオーバーレイ表示されます。

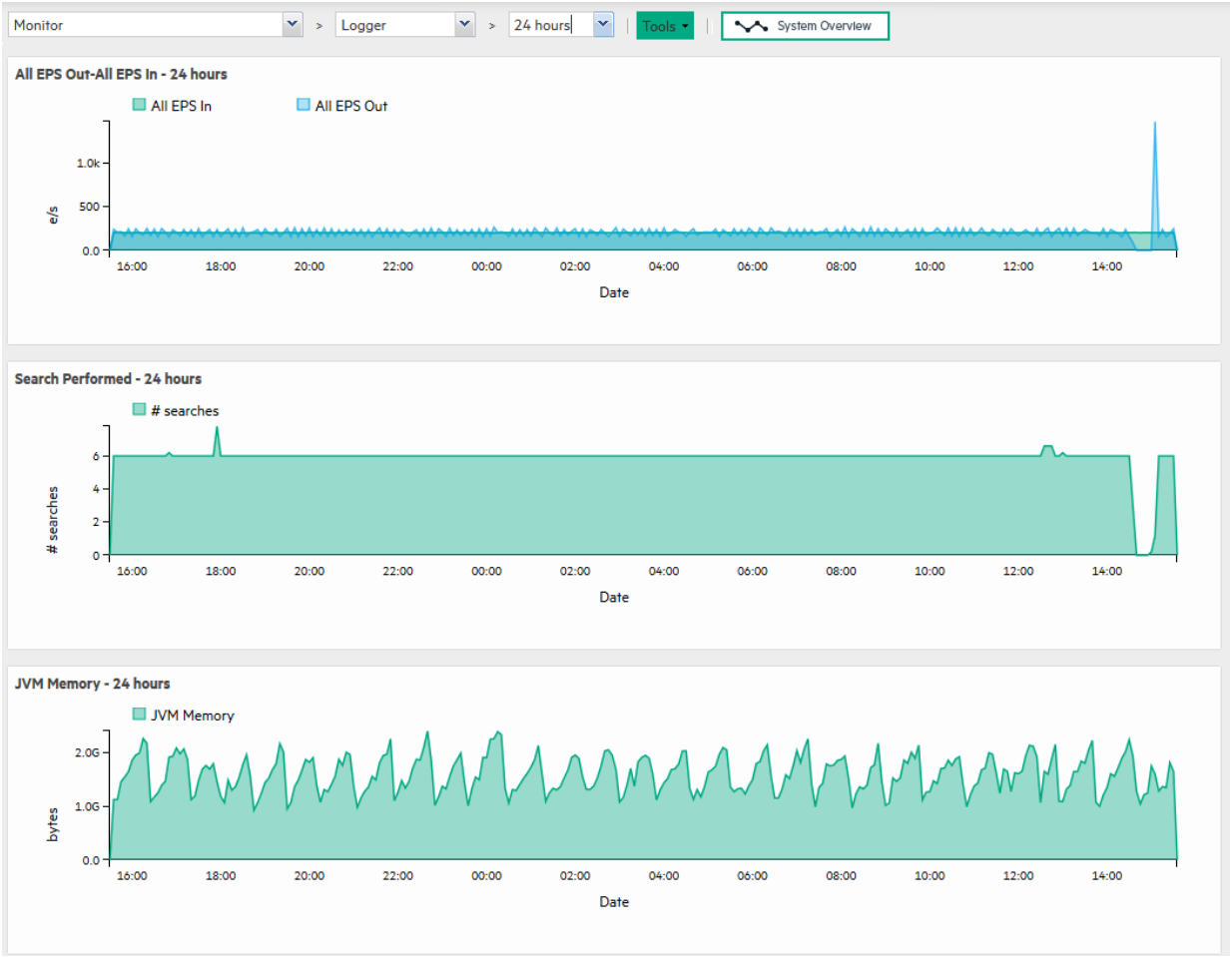
[モニター (Monitor)] ダッシュボード - [ネットワーク (Network)] パネル



[モニター] ダッシュボードの [Logger] パネル

[モニター] ダッシュボードの [Logger] パネルには、イベント、検索、メモリに関する情報が表示されます。[JVM Memory Usage] グラフには、Loggerのバックエンドサーバープロセスによって使用されているメモリが表示されます。たとえば、UIから検索クエリを受信した後に検索を実行するために使用されるメモリが表示されます。

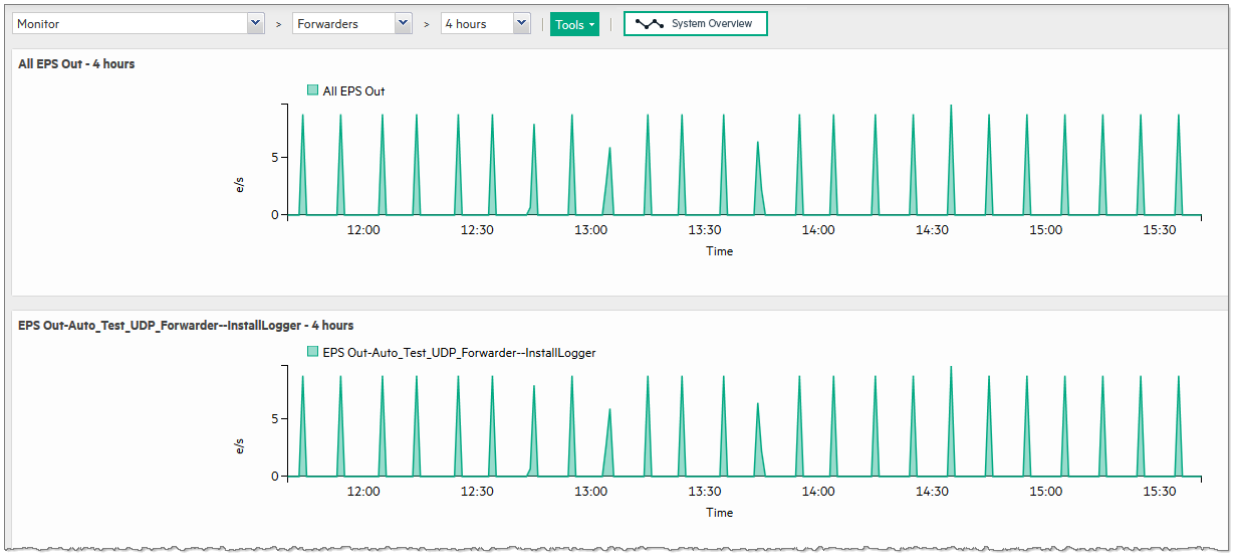
[モニター (Monitor)] ダッシュボード - Logger パネル



[モニター] ダッシュボードの [転送者] パネル

[モニター] ダッシュボードの [転送者] パネルには、送信された秒あたりのイベント数 (EPS) の合計と、設定されている転送者ごとの値が表示されます。転送者のリストには、無効になっている転送者を含め、システムが認識しているすべての転送者が含まれます。新しい転送者を作成したり、転送者を有効または無効にしたりするには、「転送者」(398ページ) を参照してください。

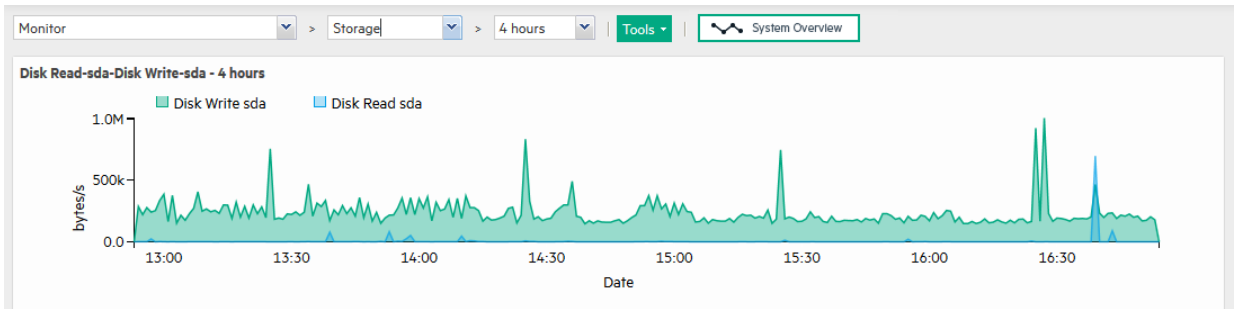
[モニター (Monitor)] ダッシュボード - [転送者 (Forwarder)] パネル



[モニター] ダッシュボードの [ストレージ] パネル

[ストレージ] モニターパネルには、ディスク読み取りとディスク書き込み情報が表示されます。ストレージグループの一覧には、各グループの割り当て済みスペースと使用済みスペースの比較が表示されます。スペースは1 GBファイル単位で使用されるため、5 GBのストレージグループは、セットアップ後すぐに20%使用済みと表示されます。ストレージグループの詳細については、「ストレージグループ」(428ページ) を参照してください。

[モニター (Monitor)] ダッシュボード - [ストレージ (Strage)] パネル



システム概要ダッシュボード

システム概要ダッシュボードは、複数の[モニター]ダッシュボードパネルに代わる表示形式です。このダッシュボードには、Loggerの監視に使用する[CPU使用率]、[プラットフォームメモリ]、[ディスク読み取り-sda]、[ディスク書き込み-sda]、[検索実行回数]、[送信-eth0]、[受信-eth0]、[JVMメモリ]、[すべてのEPSイン]、[すべてのEPSアウト]の各パネルが表示されます。これらのパネルの一部を他のLoggerモニターパネルと入れ替えて、ニーズに合わせて表示を調整することができます。

システム概要ダッシュボードを表示するには、[ダッシュボード]メニューを開き、[モニター]ダッシュボードの上部にある**[システム概要 (System Overview)]**をクリックします。

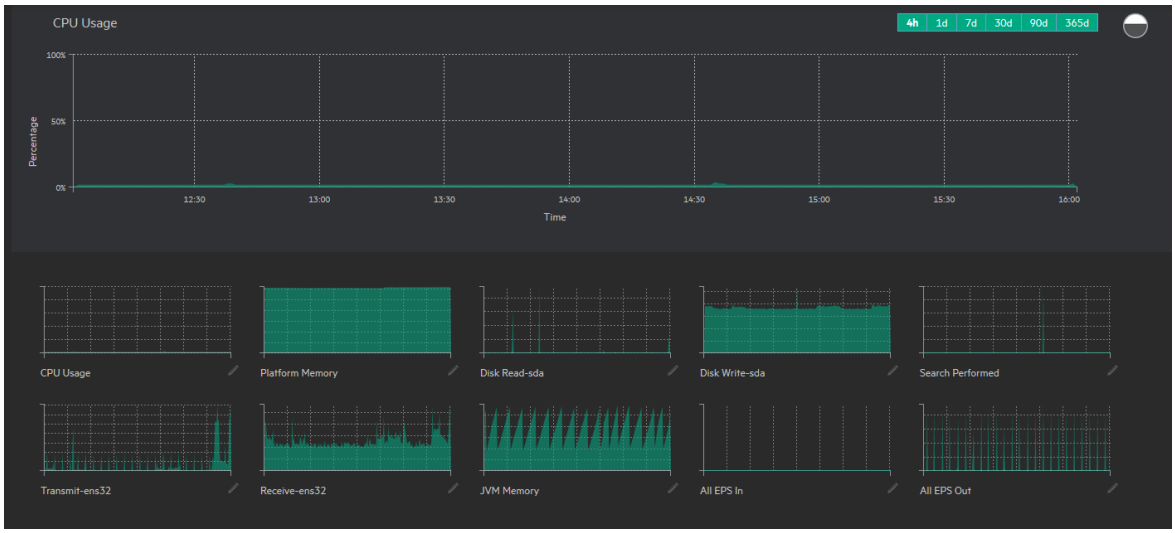
システム概要ダッシュボードが表示されます。

システム概要ダッシュボード、明るい背景

システム概要ダッシュボードでは、暗い背景と明るい背景を切り替えることができます。

背景色を変更するには、右上の[背景切り替え]アイコン ( ) をクリックします。

新しいモニターダッシュボード、暗い背景



1つのモニターパネルが画面上部に大きく表示され、その他のパネルは下部に横並びに小さく表示されます。

- 表示する時間範囲を調整するには、大きいパネルの上にある [4時間 (4h)]、[1日 (1d)]、[7日 (7d)]、[30日 (30d)]、[90日 (90d)]、または [365日 (365d)] をクリックします。
- 大きいパネルのセクションの上にポインターを移動すると、その部分の詳細が表示されます。
- 画面下部の小さいパネルをクリックすると、パネルは上部に移動し、大きく表示されます。
- 他のモニターパネルをデフォルトのパネルの代わりに表示することができます。

> **注:** 表示できるのは既存のモニターパネルだけです。[検索結果] パネルや [サマリー] パネルを表示することはできません。
>
> 表示可能な [転送者]、[受信者]、[ストレージ] パネルは、Loggerの設定によって異なります。

カスタムパネルをデフォルトのパネルの代わりに表示するには

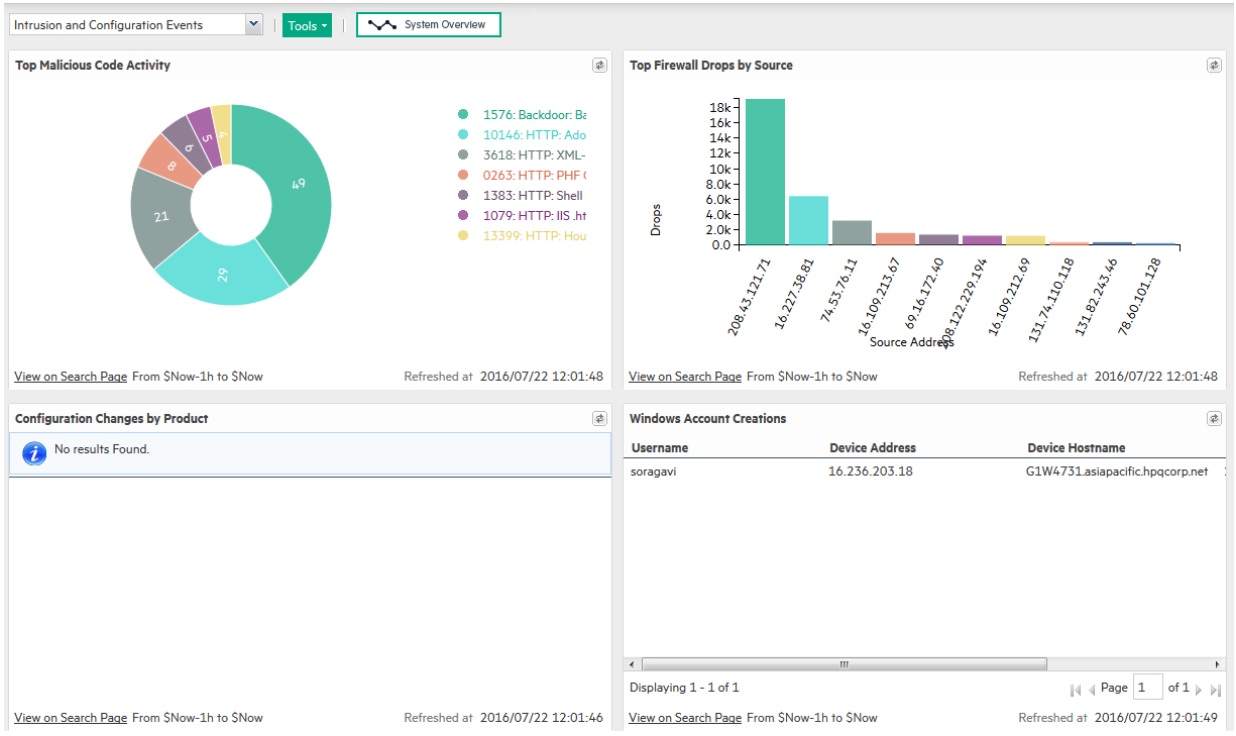
1. パネル名の横の編集アイコン (✎) をクリックします。
2. テキストボックスに文字を入力して、利用可能なパネルのリストを表示します。例えば、受信者を表示するには、まず「re」と入力してください。
3. リスト内のパネルをクリックして選択します。別のパネルを選択しないでダイアログを閉じる場合は、キャンセルアイコン ✖ をクリックします。

[Intrusion and Configuration Events] ダッシュボード

[Intrusion and Configuration Events] ダッシュボードには、システムの設定変更や侵入に関する次のような情報が表示されます。

- Top Malicious Code Activity: 最も活発な悪意のあるコードを表示します。
- Top Firewall Drops by Source: ファイアウォールによってトラフィックがドロップされたイベントを表示します。
- Configuration Changes by Product: 設定が変更された製品を表示します。
- Windows Account Creations: Microsoft Windowsオペレーティングシステム上で作成されたユーザーアカウントを示します。

[Intrusion and Configuration Events] ダッシュボード



各ダッシュボードには、標準システムコンテンツで見つかった保存された検索の検索結果が、クエリを最後に実行した日付および時刻とともに表示されます。

デフォルトのダッシュボードで使用されるシステムコンテンツは更新できませんが、ニーズに合わせて検索を編集し、変更内容を保存し、新規に保存された検索を独自のダッシュボードで使用して、関心のある情報を探すことができます。ダッシュボードの新規作成は、「カスタムダッシュボードの作成と管理」(60ページ)の手順に従ってください。

注: グラフを表示するダッシュボードは、アグリゲートされたクエリです。したがって、検索全体が完了しなければ、グラフは表示されません。イベント数が多い場合には、処理に時

間がかかることがあります。

- ダッシュボードは自動的には更新されません。更新  をクリックすると検索結果が更新されます。
- **[検索ページの表示]** をクリックすると **[分析] > [検索]** ページが開き、保存された検索が自動的に実行されます。
- グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、特定のフィールド値を持つイベントにドリルダウンできます。(ドリルダウンは、表が表示されるダッシュボードでは使用できません)。

グラフのドリルダウン

グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、グラフでクリックしたフィールド名と値が含まれるWHERE句が追加されたクエリが、[分析 (検索)] ページで再度実行されます。

ドリルダウン情報には、検索結果のヒストグラムと表が含まれています。ヒストグラムにドリルダウンして、詳細情報を表示できますヒストグラム上のドリルダウンの詳細については、「ヒストグラムのドリルダウン」(126ページ) を参照してください。

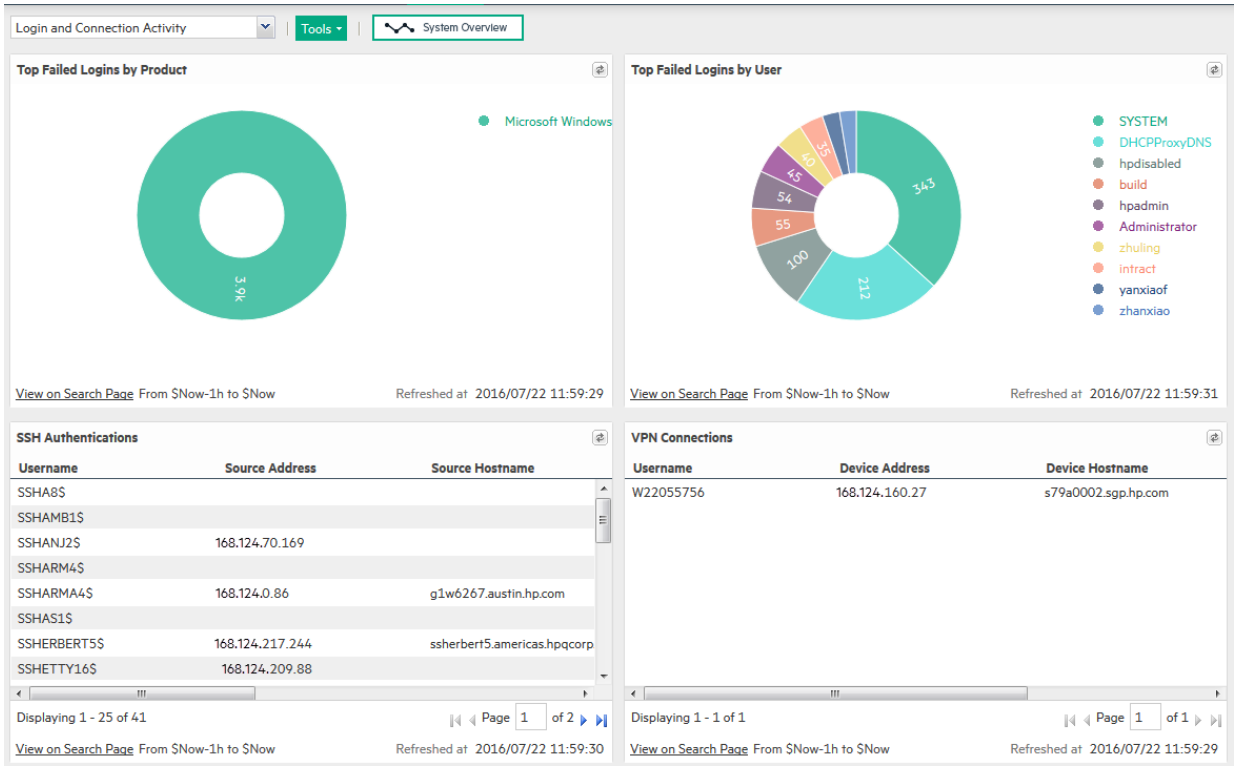
注: ダッシュボードの [検索結果] パネルに関連付けられている保存された検索クエリは変更されません。ドリルダウン画面からダッシュボードに戻る必要がある場合は、ブラウザーの「戻る」機能を使用します。

[Login and Connection Activity] ダッシュボード

[Login and Connection Activity] ダッシュボードには、システム上の次の種類のログインおよび接続アクティビティに関する情報が表示されます。

- **Top Failed Logins by Product**: 失敗したログイン数の上位部分がデバイス製品でソートされて表示されます。
- **Top Failed Logins by User**: 失敗したログイン数の上位部分がユーザー名でソートされて表示されます。
- **SSH Authentications**: SSHを使用したログイン頻度またはログイン試行頻度の高いユーザーを表示します。
- **VPN Connections**: VPN接続を使用したログイン頻度またはログイン試行頻度の高いユーザーを表示します。

[Login and Connection Activity] ダッシュボード



各ダッシュボードには、標準システムコンテンツで見つかった保存された検索の検索結果が、クエリを最後に実行した日付および時刻とともに表示されます。

デフォルトのダッシュボードで使用されるシステムコンテンツは更新できませんが、ニーズに合わせて検索を編集し、変更内容を保存し、新規に保存された検索を独自のダッシュボードで使用して、関心のある情報を探すことができます。ダッシュボードの新規作成は、「カスタムダッシュボードの作成と管理」(60ページ)の手順に従ってください。

注: グラフを表示するダッシュボードは、アグリゲートされたクエリです。したがって、検索全体が完了しなければ、グラフは表示されません。イベント数が多い場合には、処理に時間がかかることがあります。

- ダッシュボードは自動的には更新されません。更新をクリックすると検索結果が更新されます。
- **[検索ページの表示]**をクリックすると**[分析] > [検索]**ページが開き、保存された検索が自動的に実行されます。
- グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、特定のフィールド値を持つイベントにドリルダウンできます。(ドリルダウンは、表が表示されるダッシュボードでは使用できません)。

グラフのドリルダウン

グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、グラフでクリックしたフィールド名と値が含まれるWHERE句が追加されたクエリが、[分析 (検索)] ページで再度実行されます。

ドリルダウン情報には、検索結果のヒストグラムと表が含まれています。ヒストグラムにドリルダウンして、詳細情報を表示できますヒストグラム上のドリルダウンの詳細については、「ヒストグラムのドリルダウン」(126ページ) を参照してください。

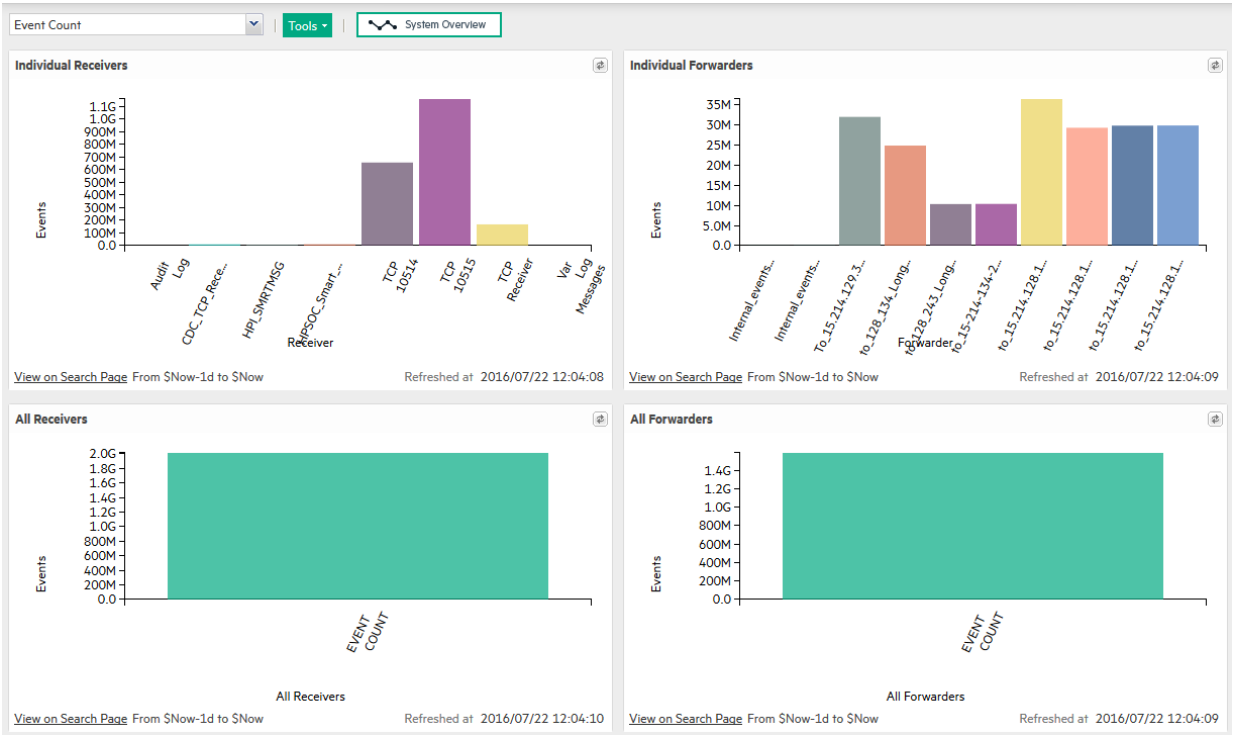
注: ダッシュボードの [検索結果] パネルに関連付けられている保存された検索クエリは変更されません。ドリルダウン画面からダッシュボードに戻る必要がある場合は、ブラウザーの「戻る」機能を使用します。

[イベント数] ダッシュボード

[イベント数] ダッシュボードには、システム上の次の種類のイベント入力/出力アクティビティに関する情報が表示されます。

- **個別の受信者:** 受信したイベントの数を受信者ごとに表示します。
- **個別の転送者:** 転送したイベントの数を転送者ごとに表示します。
- **すべての受信者:** すべての受信者が受信した総イベント数を表示します。
- **すべての転送者:** すべての転送者が転送した総イベント数を表示します。

[イベント数 (Event Count)] ダッシュボード



各ダッシュボードには、標準システムコンテンツで見つかった保存された検索の検索結果が、クエリを最後に実行した日付および時刻とともに表示されます。

デフォルトのダッシュボードで使用されるシステムコンテンツは更新できませんが、ニーズに合わせて検索を編集し、変更内容を保存し、新規に保存された検索を独自のダッシュボードで使用して、関心のある情報を探すことができます。ダッシュボードの新規作成は、「カスタムダッシュボードの作成と管理」(60ページ)の手順に従ってください。

注：グラフを表示するダッシュボードは、アグリゲートされたクエリです。したがって、検索全体が完了しなければ、グラフは表示されません。イベント数が多い場合には、処理に時間がかかることがあります。

- ダッシュボードは自動的には更新されません。更新をクリックすると検索結果が更新されます。
- **[検索ページの表示]**をクリックすると**[分析] > [検索]**ページが開き、保存された検索が自動的に実行されます。
- グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、特定のフィールド値を持つイベントにドリルダウンできます。(ドリルダウンは、表が表示されるダッシュボードでは使用できません)。

グラフのドリルダウン

グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、グラフでクリックしたフィールド名と値が含まれるWHERE句が追加されたクエリが、[分析 (検索)] ページで再度実行されます。

ドリルダウン情報には、検索結果のヒストグラムと表が含まれています。ヒストグラムにドリルダウンして、詳細情報を表示できますヒストグラム上のドリルダウンの詳細については、「ヒストグラムのドリルダウン」(126ページ) を参照してください。

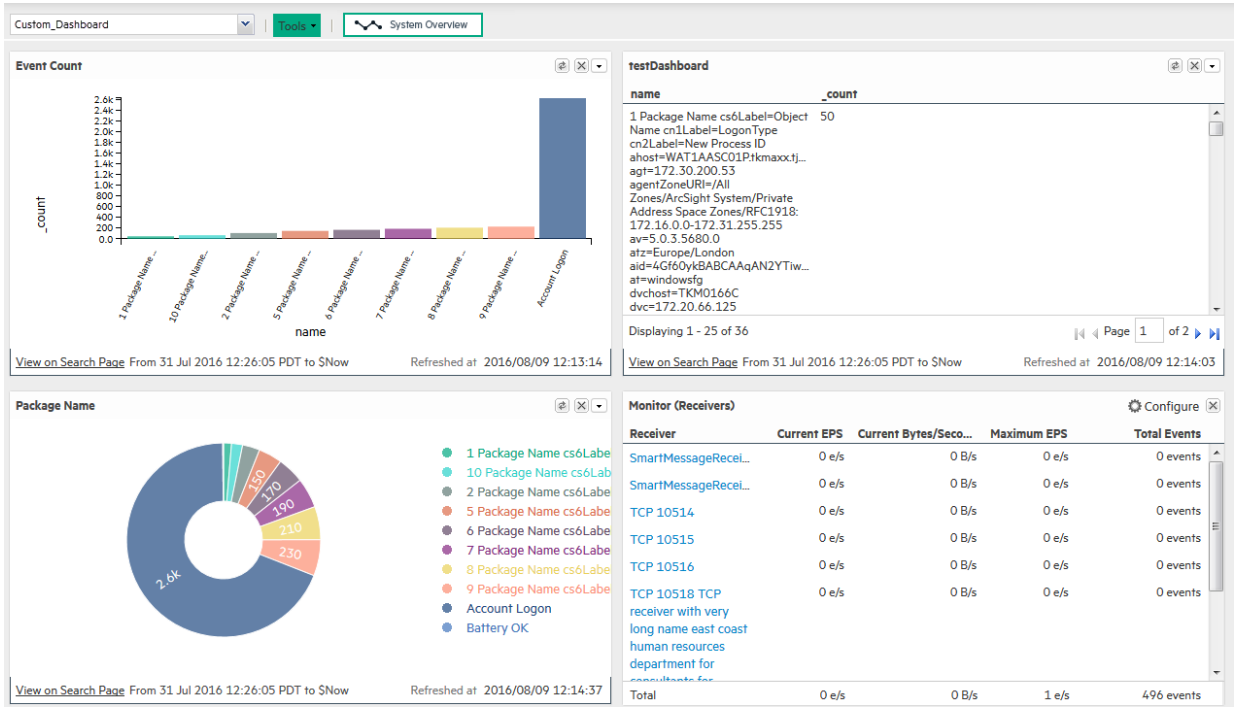
注: ダッシュボードの [検索結果] パネルに関連付けられている保存された検索クエリは変更されません。ドリルダウン画面からダッシュボードに戻る必要がある場合は、ブラウザーの「戻る」機能を使用します。

カスタムダッシュボード

ダッシュボードには、[検索結果]、[モニター]、[サマリー] パネルを混在させることができます。関心のあるイベントを照合するさまざまな検索クエリや、受信者、転送者、ストレージ、CPU、ディスクなどのLoggerリソースのステータス、またはその両方を組み合わせて、1つのダッシュボードに表示します。

1つのダッシュボードに追加できる [モニター] パネルと [サマリー] パネルの数に制限はありませんが、追加する [検索結果] パネルは4つまでにしてください。

サンプルのカスタムダッシュボード



各 [検索結果] パネルには、保存された検索クエリが関連付けられています。この種類のパネルには、chartまたはtopなど、アグリゲーション演算子を含む保存された検索クエリのみを関連付けることができます。

[検索結果] パネルの**[検索] ページのビュー**をクリックして、**[分析] > [検索]** ページを開き、イベントの詳細を表示します。パネルクエリは自動的に実行され、検索結果が表示されます。

また、任意のグラフからドリルダウンして、特定のフィールド値を持つイベントを素早くフィルター処理できます。そのためには、[検索結果グラフ] パネル上のグラフの値を探し、クリックしてその値に一致するイベントにドリルダウンします。

グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、グラフでクリックしたフィールド名と値が含まれるWHERE句が追加されたクエリが、[分析 (検索)] ページで再度実行されます。

注: グラフを表示するダッシュボードは、アグリゲートされたクエリです。したがって、検索全体が完了しなければ、グラフは表示されません。イベント数が多い場合には、処理に時間がかかることがあります。

- ダッシュボードは自動的には更新されません。更新 をクリックすると検索結果が更新されます。
- **[検索ページの表示]** をクリックすると **[分析] > [検索]** ページが開き、保存された検索が自動的に実行されます。
- グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、特定のフィールド値を持つイベントにドリルダウンできます。(ドリルダウンは、表が表示されるダッシュボードでは使用できません)。

グラフのドリルダウン

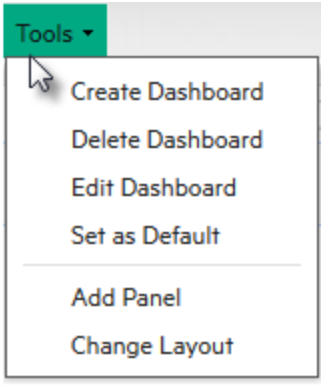
グラフの値 (縦棒、横棒、ドーナツグラフの一部) をクリックすると、グラフでクリックしたフィールド名と値が含まれるWHERE句が追加されたクエリが、[分析 (検索)] ページで再度実行されます。

ドリルダウン情報には、検索結果のヒストグラムと表が含まれています。ヒストグラムにドリルダウンして、詳細情報を表示できますヒストグラム上のドリルダウンの詳細については、「ヒストグラムのドリルダウン」(126ページ) を参照してください。

注: ダッシュボードの [検索結果] パネルに関連付けられている保存された検索クエリは変更されません。ドリルダウン画面からダッシュボードに戻る必要がある場合は、ブラウザーの「戻る」機能を使用します。

カスタムダッシュボードの作成と管理

[ダッシュボード] > [ツール] メニューに表示されるオプションは許可によって異なります。



ダッシュボード操作を実行するには以下の権限が必要です (Logger Rightsグループ)。

- ダッシュボードの使用と表示
- ダッシュボードの編集、保存、削除

これらの権限がある場合、ダッシュボードの作成 (「カスタムダッシュボードの追加」(61ページ)を参照) と、作成したダッシュボードへのパネルの追加が可能です (「ダッシュボードへのパネルの追加と管理」(62ページ)を参照)。

ヒント: [検索結果] パネルを追加する場合は、保存された検索が存在している必要があります。保存された検索が存在しない場合は、[検索結果] パネルオプションが表示されません。

カスタムダッシュボードの追加

ダッシュボードを追加するには

1. [**ダッシュボード**] メニューを開きます。
2. [**ツール**] ドロップダウンメニューをクリックし、[**ダッシュボードの作成**] を選択します。
3. [**名前**] フィールドに、ダッシュボードの意味のある名前を入力します。
4. ダッシュボードの [**タイプ**] として、[プライベート] または [共有] を選択します。
   プライベートダッシュボードは作成したユーザーのみが表示でき、共有ダッシュボードはすべてのLoggerユーザーが表示できます。ただし、権限を持たない情報を表示することはできません。
5. [**作成**] をクリックします。
   ダッシュボードを作成したら、「ダッシュボードへのパネルの追加と管理」(62ページ)の説明に従って、パネルを追加する必要があります。

カスタムダッシュボードの編集

[ダッシュボードの編集] ページでは、カスタムダッシュボードの名前とプライバシー設定を変更することができます。ダッシュボードパネルを追加または編集するには、「ダッシュボードへのパネ

ルの追加と管理」(62ページ) を参照してください。

以下のプライバシーオプションがあります。

- プライベート — 作成者のみがダッシュボードを表示できます。
- 共有 — 自分が作成したダッシュボードをすべてのLoggerユーザーが表示できます。ただし、権限を持たない情報を表示することはできません。

  たとえば、あるユーザーが特定のストレージグループに対する権限を持たず、共有ダッシュボード内のパネルにそのストレージグループのイベントにアクセスするクエリが含まれている場合、ユーザーが共有ダッシュボードにアクセスすると、そのパネルは空白になります。

ダッシュボードを編集するには

1. [**ダッシュボード**] メニューを開きます。
2. [**ツール**] ドロップダウンメニューをクリックし、[**ダッシュボードの編集**] を選択します。
3. ダッシュボードの名前を変更する場合は、[**名前**] フィールドに新しい名前を入力します。
4. ダッシュボードのプライバシー設定を変更する場合は、[**タイプ**] ドロップダウンメニューから適切な設定を選択し、[**保存**] をクリックします。
5. ダッシュボードパネルを追加または編集するには、「ダッシュボードへのパネルの追加と管理」(62ページ) を参照してください。

カスタムダッシュボードの削除

ダッシュボードを削除するには

1. **[ダッシュボード]** メニューを開きます。
2. 削除するダッシュボードを選択します。
3. **[ツール]** ドロップダウンメニューをクリックし、**[ダッシュボードの削除]** を選択します。
4. 確認メッセージで **[Yes]** をクリックしてアクションを確定するか、**[No]** をクリックして変更せずに終了します。

ダッシュボードへのパネルの追加と管理

ダッシュボードを作成した後、必要な情報を表示するにはパネルを追加する必要があります。ダッシュボードには、[検索結果]、[モニター]、[サマリー] パネルを混在させることができます。1つのダッシュボードに追加できる [モニター] パネルと [サマリー] パネルの数に制限はありませんが、最適なパフォーマンスを得るには、追加する [検索結果] パネルは4つまでにしてください。

ダッシュボードにパネルを追加する前に、まずダッシュボードを作成する必要があります。詳細については、「カスタムダッシュボードの作成と管理」(60ページ) を参照してください。

以下の種類のパネルを追加できます。

- 検索結果: グラフと表
- [モニター]: デフォルトの [モニター] ダッシュボードで使用できる4つの種類すべて
- [サマリー]: デフォルトの [サマリー] ダッシュボードで使用できる4つの種類すべてとユーザー定義サマリーパネル

パネルのダッシュボードへの追加

パネルをダッシュボードに追加するには

1. **[ダッシュボード]** メニューを開きます。
2. パネルを追加するダッシュボードを選択します。
3. **[ツール]** プルダウンメニューをクリックし、**[パネルの追加]** を選択します。
4. パラメーターを設定し、**[追加]** をクリックします。

パラメーター	説明
タイプ	パネルの種類を以下の中から選択します。 • [検索結果 (グラフ)]: 検索結果をグラフ形式で表示します。 • [検索結果 (テーブル)]: 検索結果を表形式で表示します。 • [モニター (グラフ)]: 選択したリソースのグラフを表示します。 • [モニター (転送者)]: 転送者情報を表形式で表示します。 • [モニター (受信者)]: 受信者情報を表形式で表示します。 • [モニター (ストレージグループ)]: ストレージグループ情報を表形式で表示します。 • [サマリー (エージェントの緊急度)]: イベントサマリーを、Logger上で設定されているエージェントの緊急度で分類して表示します。 • [サマリー (エージェントタイプ)]: イベントサマリーを、Logger上で設定されている受信者で分類して表示します。 • [サマリー (受信者)]: イベントサマリーを、Logger上で設定されている受信者で分類して表示します。 • [サマリー (デバイス)]: イベントサマリーを、Logger上で設定されているデバイスで分類して表示します。 • [サマリー (ユーザー定義)]: イベントサマリーを、パネルの追加時に選択したフィールドで分類して表示します。 **注:** 保存された検索クエリがLogger上に存在しない場合、[保存された検索] パネルタイプはプルダウンメニューの選択肢として表示されません。
タイトル	パネルの意味のある名前を入力します。 このフィールドにはデフォルトの名前が表示されますが、変更してかまいません。

パラメーター	説明
グラフ	[モニター (グラフ)] パネルのみに適用されます。 パネルに表示するグラフの種類を選択します。選択可能なオプションとしては、[CPU Usage - 4時間]、[Platform Memory Usage - 24時間]、[Disk Read-Write - 7日] などがあります。
保存された検索	[検索] パネルのみに適用されます。 パネルに表示するイベントを検索するために使用する保存された検索クエリを選択します。
グラフタイプ	[検索結果 (グラフ)] パネルのみに適用されます。 一致イベントを表示するグラフの種類。選択できるのは、 カラム、棒、円グラフ、エリア、ライン、積み上げカラム、積み上げ棒グラフです。 デフォルト値: [カラム]
グラフ制限	[検索結果 (グラフ)] パネルのみに適用されます。 プロットする一意の値の数。デフォルト値: 10
フィールド名	[サマリー (ユーザ定義)] パネルのみに適用されます。 [サマリー] パネル上のイベントサマリーを分類するイベントフィールド名。デフォルト値: agentSeverity

ダッシュボードパネルの編集

ダッシュボードに追加したパネルを編集できるかどうかは、パネルの種類によって変わります。[検索結果] パネルと [サマリー (ユーザー定義)] パネルは編集できますが、[モニター] パネルと一部の [サマリー] パネルは編集できません。

次の表に、編集できるパネルと、その中で編集できる項目の一覧を示します。

アクション	説明
すべてのパネル	
削除	パネルをダッシュボードから削除します。
検索結果パネル	
パネルの編集	タイトル、関連付けられている保存された検索、グラフの種類、グラフの制限を変更します。
保存された検索を編集	関連付けられている保存された検索クエリを編集するための [保存された検索を編集] ページにアクセスします。
[検索] ページのビュー	パネルのクエリを [検索結果] ページ ([分析] > [検索]) 上で実行し、一致するイベントをそのページに表示します。

アクション	説明
更新	パネルの現在の内容を更新します。 **注:** 他のすべての種類のパネルは、自動的に更新されるため、明示的な更新は不要です。
サマリーパネル - ユーザー定義	
パネルの編集	タイトルまたはイベントを分類するフィールド名を変更します。

パネルを編集するには

1. **[ダッシュボード]** メニューを開きます。
2. 編集するパネルが含まれているダッシュボードを選択します。
3. ユーザー定義サマリーパネルを編集する場合
   a. [編集] ( ) アイコンをクリックします。
   b. タイトルとフィールド名のいずれかまたは両方を編集します。
4. 検索結果パネルを編集する場合
   a. アイコンをクリックします。
   b. **[パネルの編集]** を選択し、パネルのタイトルを編集するか、異なる保存された検索を選択する、または該当する場合はグラフの種類またはグラフの制限を変更します。
   c. 保存された検索クエリを編集するために [保存された検索を編集] ページ (**[設定 | 検索] > [保存された検索]**) にアクセスするには **[保存された検索を編集]** を選択します。
5. **[保存]** をクリックします。

ダッシュボードパネルの削除

パネルをダッシュボードから削除するには

デフォルトの [モニター] ダッシュボードまたはデフォルトの [サマリー] ダッシュボードからパネルを削除することはできません。ただし、[ダッシュボード] メニューオプション下に作成したダッシュボードに追加した [モニター] パネルと [サマリー] パネルは削除できます。

1. **[ダッシュボード]** メニューを開きます。
2. 削除するパネルが含まれているダッシュボードを選択します。
3. アイコンをクリックします。
4. 確認メッセージで **[はい]** をクリックしてアクションを確定するか、**[いいえ]** をクリックして変更せずに終了します。

ダッシュボードのレイアウト変更

ダッシュボードのレイアウトを変更するには

自分が作成したダッシュボードのレイアウトのみを変更できます。[モニター] ダッシュボードのレイアウトは変更できません。

1. **[ダッシュボード]** メニューを開きます。
2. 配置を変更するパネルが含まれているダッシュボードを選択します。
3. **[ツール]** ドロップダウンメニューをクリックし、**[レイアウトの変更]** を選択します。
4. パネルのタイトルが表示されている青い帯にカーソルを合わせ、パネルを別の位置にドラッグします。
5. パネルの配置を変更したら **[保存]** をクリックします。

デフォルトのダッシュボードの設定

特定のダッシュボードをデフォルトとして設定すると、そのダッシュボード画面が [ダッシュボード] メニューに移動したときに表示されるデフォルトになります。この設定はユーザー固有であるため、自分のダッシュボードと他のユーザーのダッシュボードが異なる可能性があります。

[サマリー] ページ (最上位のメニューバー内の [サマリー] ナビゲーションオプションからアクセス可能) は、すべてのLoggerユーザーのデフォルトホームページです。つまり、他のページを自分のホームページとして選択していない限り、最初のログインでは [サマリー] ページが表示されます。

自分で作成したダッシュボードを含む特定のダッシュボードがホームページとして表示されるように、Loggerを設定することができます。

特定のダッシュボードをホームページとして選択するには

1. 「Loggerのオプション」(37ページ) の説明に従って個人の [**<ユーザー名> のデフォルトの開始ページ**] を設定する場合は、[**ダッシュボード**] オプションを選択してください。
2. [**ダッシュボード**] メニューを開きます。
3. デフォルトに設定したいダッシュボードを選択します。
4. [**ツール**] ドロップダウンメニューをクリックし、[**デフォルトとして設定**] を選択します。
5. 確認メッセージで [**はい**] をクリックしてアクションを確定するか、[**いいえ**] をクリックして変更せずに終了します。

第3章: イベントの検索と分析

特定の条件に一致するイベントを分析するときや、イベントをレポートに含めるとき、またはArcSight ESMなどの別のシステムに転送するときに、イベントを検索する必要があります。イベントを検索するには、クエリを作成します。作成するクエリの複雑さは、ニーズに応じて変化します。クエリは、単純な項目であったり、複数のIPアドレスやポートを含むイベントや、特定のストレージグループで特定の時間範囲内に発生したイベントを照合するなど、かなり複雑になる場合があります。

以下のトピックでは、Loggerで特定のイベントを検索する方法について説明します。これらのトピックでは、検索で使用できる方法、イベントに対するクエリの実行、定義したクエリとクエリで見つかったイベントを将来使用するために保存する方法について説明します。また、Loggerが特定の条件に一致するイベントを受信したときに、特定のユーザーに通知するためにアラートを設定する方法について説明します。

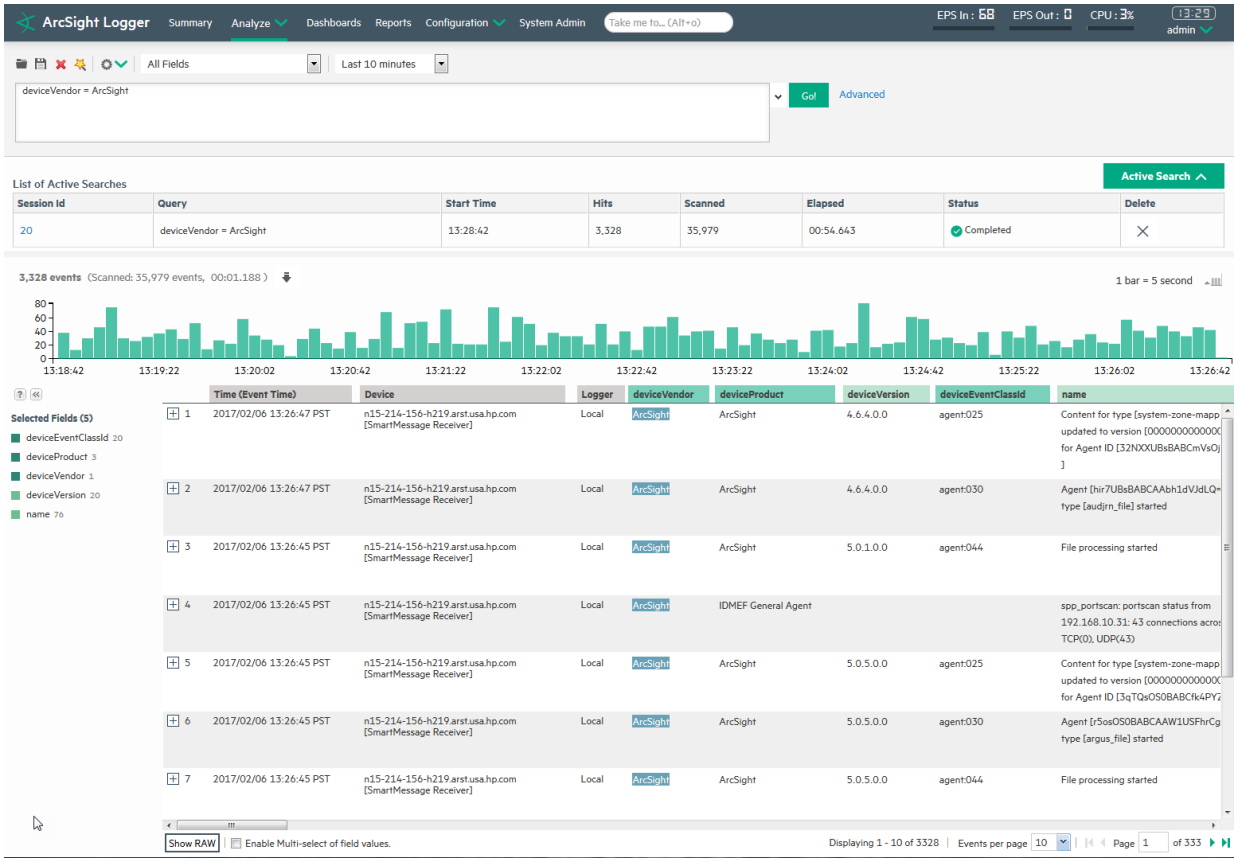
イベントの検索の処理

検索処理は、最適化された検索言語を使用し、複数の検索コマンドをパイプライン形式で指定できます。また、検索結果の表示のカスタマイズ、検索結果のグラフ表示などを行うことができます。

検索を実行するための最も単純な方法は、探している (クエリ) キーワードまたは情報を検索テキストボックスに入力し、時間範囲を選択し、**[実行!]** をクリックすることです。「`hostA.companyxyz.com`」のような単純なキーワードを入力することも、論理式、キーワード、

フィールド、正規表現を含む複雑なクエリを入力することもできます。指定した条件に一致するデータが検索され、インデックスステータスを示す色分けされた列に結果が表示されます。詳細については、「検索フィールドの色について」(70ページ)を参照してください。

[Logger検索 (Logger Search)] ページ



クエリがすべてのデータのスキャンを終了していなくても、検索結果は返されるとすぐに表とヒストグラムに表示されます。この例については、「単純なクエリの例」(69ページ)を参照してください。アクティブな検索リストには、進行中の検索に加えて、まだ有効期限が切れていない完了した検索も表示されます。

検索にグラフを追加し、最も重要な情報をより意味のある方法で表示することもできます。グラフは、すべてのデータが返されるまで表示されません。この例については、「グラフを使用したクエリの例」(69ページ)を参照してください。

検索クエリは、いくつかの便利な方法で入力できます。検索テキストボックスにクエリを入力したり、検索ビルダーツールを使用してクエリを作成したり、または以前保存したクエリを使用することができます (フィルターまたは保存された検索と呼びます)。

クエリを入力するとき、検索ヘルパーによって、クエリ式の作成を支援するために、提案される入力と一致の候補が表示されます(詳細については、「検索ヘルパー」(102ページ)を参照してください)。

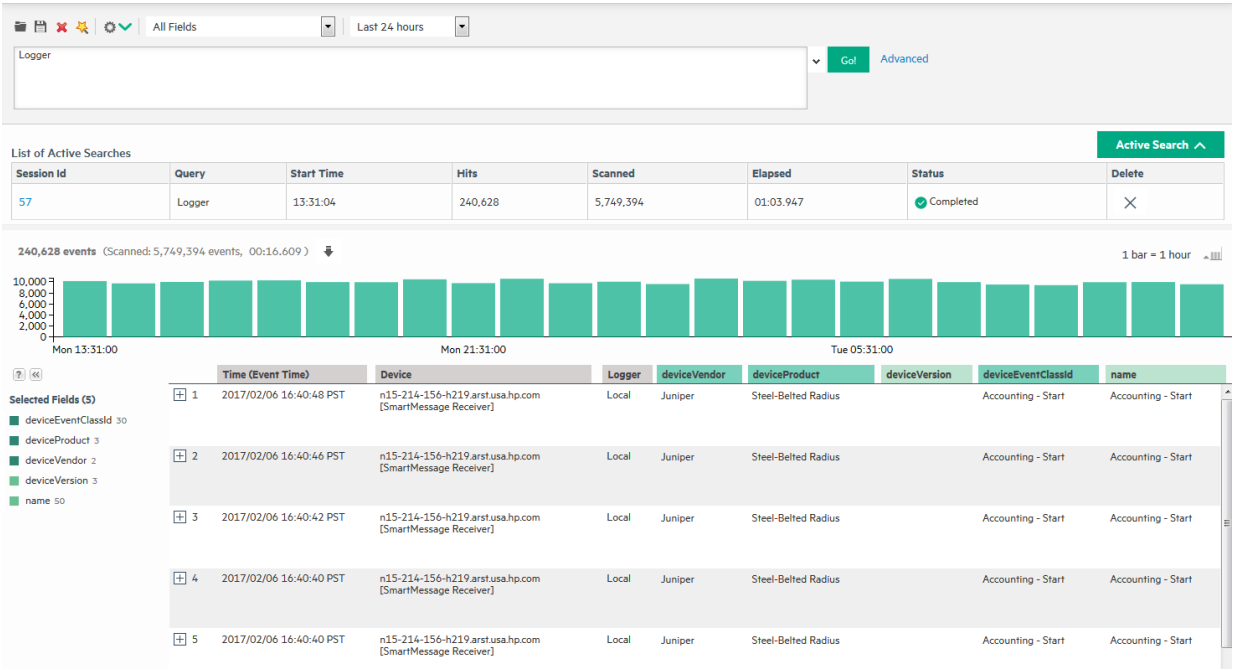
[検索] テキストボックスにクエリを入力するのに加えて、以下のことが可能です。

- Advanced Searchツールを使用してクエリを作成する。詳細については、「検索の詳細設定ビルダーの使用」(94ページ)を参照してください。
- クエリを保存して後で使用する。詳細については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ)を参照してください。
- システムに付属している定義済みのクエリから新しいクエリを作成する。詳細については、「システムフィルター/事前定義フィルター」(145ページ)を参照してください。

最も単純な検索クエリはキーワードですが、「検索クエリの要素」(71ページ)で説明するクエリのすべての要素に習熟すれば、検索処理が持つ潜在的な力を完全に活用できます。

単純なクエリの例

このクエリ例では、「Logger」という単語を含むイベントを探します。検索ボックスにLoggerと入力し、**[実行!]**をクリックします。

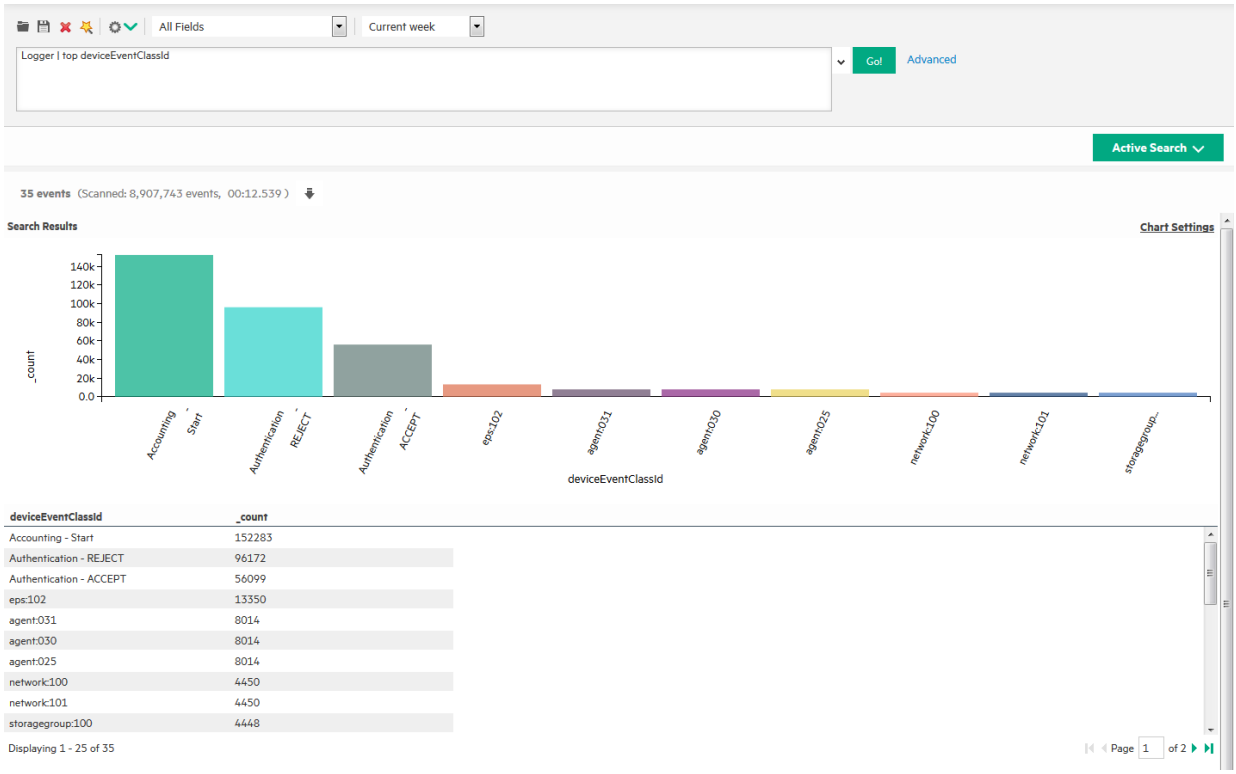


グラフを使用したクエリの例

chart、top、rareなどのアグリゲーション検索演算子は、検索結果のグラフを生成します。このクエリ例では、「Logger」という単語を含むイベントを探し、名前フィールドの内容で上位10個のイベントをグラフ化します。検索ボックスに次のクエリを入力し、**[実行!]**をクリックします。

```
Logger | top deviceEventClassId
```

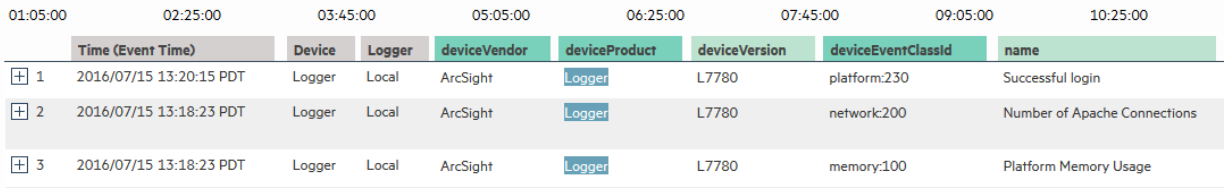
この例に似たグラフが表示されます。



検索演算子の詳細については、「検索演算子」(564ページ)を参照してください。グラフの作成と使用の詳細については、「グラフのドリルダウン」(131ページ)および「フィールドサマリーからの検索の精緻化とグラフ化」(137ページ)を参照してください。

検索フィールドの色について

検索結果の表の各カラムは、カラムに含まれるフィールドのタイプと、フィールドがインデックス付きかどうかが分かるように色分けされます。色分けされたカラムラベルは、検索を適切に絞り込んで迅速に結果を得るのに役立ちます。



フィールドタイプのアイコンは、フィールドセットエディター、[デフォルト フィールド] ページ、および検索の自動補完など、検索フィールドが使用されるページにも表示されます。

アイコン	カラムの色	フィールドタイプ	フィールドがインデックス付きになるか
	深緑色	スーパーインデックス付き	デフォルトでインデックス付き
	緑色	インデックス付き	デフォルトでインデックス付き
	薄い緑色	Logger共通のイベントフォーマット (CEF)、カスタムフィールドも含む	はい (インデックス付け可能)
	薄い灰色	メタデータ	なし
	色なし	LoggerでないCEF	なし

検索クエリの要素

単純な検索クエリは、クエリ式、時間範囲、およびフィールドセットで構成されます。Loggerの高度な検索クエリには、特定のストレージグループやピアLoggerに検索を制限する制約を含めることもできます。

クエリ式

クエリ式は、検索の実行時にイベントを選択するために使用される条件セットです。式には、「login」やIPアドレスなど、照合のための非常に単純な項を指定できます。また、複数のIPアドレスやポートを含むイベントや、特定のストレージグループで特定の時間範囲の間に発生したイベントを照合するために、より複雑な式も可能です。

検索テキストボックスに以下の構文を使用してクエリを指定します。

<インデックス検索> | <検索演算子>

クエリ式は、パイプライン方式で左から右に評価されます。まず、クエリの指定したインデックス検索部分に一致するイベントが検索されます。次に、一致したイベントに対し、最初のパイプ(「|」)文字の後にある検索演算子が適用され、後続の検索演算子が順に適用されて検索結果が絞り込まれます。

クエリに一致するイベントが見つかると、検索結果の表とヒストグラムに表示されます。追加のイベントが一致すると、検索結果の表とヒストグラムが更新されます。HEADやTAILなどのアグ

リゲーション演算子では、クエリの実行が終了してから検索結果が表示されます。詳細については、「検索演算子」(564ページ)を参照してください。

- クエリのインデックス検索部分については、「クエリのインデックス検索部分」(72ページ)を参照してください。
- クエリの検索演算子部分については、「クエリの検索演算子部分」(79ページ)を参照してください。
- その他のクエリを記述する際に考慮すべき点は、「検索クエリの作成について」(110ページ)に記載されています。

クエリのインデックス検索部分

クエリのインデックス検索部分は、フィールドを使用して該当するデータを迅速かつ効率的に検索します。検索式を使用して、イベントテキスト内の検索対象キーワードを指定したり、論理形式のフィールドベースの式を使用したりして検索できます。

キーワード検索 (フルテキスト検索)

キーワードは、`failed`、`login`のように、単なる検索対象の単語です。1つのクエリ式で、論理演算子 (`AND`、`OR`、`NOT`) を使用して複数のキーワードを指定できます。論理式は、`(John OR Jane) AND Doe*`のようにネストしてかまいません。`AND`、`OR`、または`NOT`という文字自体 (大文字、小文字、大文字と小文字の混在) を検索する必要がある場合は、二重引用符 (`""`) で囲み、検索エンジンによって演算子として解釈されないようにします。

注: 論理演算子`AND`、`OR`、および`NOT`は、演算子として使用するときに大文字、小文字、大文字と小文字を混在して指定できますが、クエリを読みやすくするために、大文字を使用することをHPEからお勧めします。

キーワード検索式の指定に関するガイドライン

キーワード検索式を指定するときには、以下のガイドラインに従ってください。

- 「クエリ式の構文リファレンス」(89ページ)に記載されている要件に従ってください。
- その他のクエリを記述する際に考慮すべき点は、「検索クエリの作成について」(110ページ)に記載されています。
- キーワード検索では、大文字と小文字は区別されません。
- 複数のキーワードをつなげる場合は、論理演算子 (`AND`、`OR`、`NOT`) を使用してください。2つのキーワードの間で論理演算子を指定しなかった場合、デフォルトではAND演算子が適用されます。また、キーワードを指定したフィールドとつなげる場合は論理演算子を使用してください。
- 完全一致用の単一の単語を囲むには、二重引用符 (`" "`) を使用します。そうしない場合、その単語は`<search string>*`として扱われます。たとえば、`log`を検索するには、"log"

と入力します。log (二重引用符なし) と入力すると、検索では、logで始まるすべての単語 (log、logger、loggingなど) に一致します。

- ブール演算子 (AND、OR、またはNOT) をキーワードとして指定する際、演算子を二重引用符 (“ ”) で囲んでください。例えば、“AND” のようにします。
- バックスラッシュ (\) は、\、“、および*のエスケープ文字として使用します。ただし、キーワードが二重引用符で囲まれている場合、バックスラッシュはこれらの文字をエスケープしません。

次の表は、特殊文字がキーワード検索でどのように扱われるかをまとめたものです。

キーワード検索での特殊文字の使用

文字	使用方法			
スペース タブ 改行 , ; ( ) [ ] { } “ | *	左の欄の文字を含むキーワードは指定**できません**。そのため、failed loginのような句を検索するには、"failed" AND "login"と入力します。 **注:** *は、ワイルドカード文字検索で有効な文字です。			
= : / \ @ - ? # $ & _ % > < !	左の欄のいずれかの文字を含むキーワードを指定するには、キーワードを**二重引用符** (" ") で囲みます。完全一致のために、キーワードの最後にアスタリスク (*) を指定することもできます。 例 • "C:\directory" • "result=failed"			
* アスタリスク	ワイルドカード文字であるアスタリスク (*) を使用してキーワードを検索できますが、ワイルドカードは、キーワードの先頭文字には使用できません。従って、次の使用法が有効です。			
	log*	log*	log*	
	log*app	log*app*	"log*"	
	しかし、次の使用法は有効ではありません。			
	*log	*log*app*		

フィールドベースの検索

Loggerのスキーマには、定義済みのフィールドが複数含まれています。Logger上で収集するイベントに該当するフィールドをスキーマに追加できます。フィールドベースの検索では、Loggerのスキーマに含まれているフィールドのみを含めることができます「スキーマへのフィールドの追加」(461ページ)。

Loggerのインデックス作成機能では、スキーマのフィールドに対してインデックスを作成できます。Loggerの検索操作とレポートでは、インデックスが作成されたフィールドを利用して、検索とレポート作成のパフォーマンスを大幅に向上させています。インデックス作成されたフィールドとインデックス作成されていないフィールドの両方を検索クエリに含めることができますが、検索とレポート作成のパフォーマンスは、クエリのすべてのフィールドにインデックスが作成されてい

る場合にはるかに高速になります。詳細と、インデックス作成できるフィールドの一覧については、「インデックス作成」(152ページ)を参照してください。フィールドベースのクエリパフォーマンスの説明については、「クエリにおけるインデックス作成されたフィールドに対するパフォーマンスの最適化」(99ページ)を参照してください。

- 各フィールド条件の間で、ここに示す演算子を使用することで、複数のフィールド条件を1つのクエリ式で指定できます。条件は、次の例のように入れ子にすることができます。

  ```
  (name="John Doe" OR name="Jane Doe")AND message!="success"
  ```

  注: クエリに論理演算子ORとメタデータ識別子 (「制約」(87ページ)を参照) が含まれている場合、ORで評価する式は、次の例に示すように括弧で囲まれている必要があります。

  ```
  (success OR fail) _storageGroup IN ["Default Storage Group"]
  ```

  式が括弧で囲まれていない場合、エラーメッセージが表示されます。

- 表中のどのリテラル演算子も、大文字か小文字、または大文字と小文字を混在させて指定できます。これらの単語をイベント内のリテラルとして検索するには、二重引用符 ("") で囲みます。例:

  ```
  message CONTAINS "Between"
  ```

- クエリ演算子でIPv6アドレス全体または一部を検索する場合、アドレスは正規の形式でなければなりません。IPv4射影IPv6アドレスは使用しないでください。詳細については、「フィールドベースの検索演算子の制限」(79ページ)を参照してください。
- フィールドのデータ型を決定するには、「デフォルトのフィールド」(354ページ)を参照してください。
- カスタムフィールドのサイズを決定するには、「カスタムフィールド」(356ページ)を参照してください。

フィールドベースの検索演算子

クエリ式で使用できるフィールド演算子を以下の表に示します。フィールド演算子に加えて、「クエリの検索演算子部分」(79ページ)で説明する検索演算子も使用できます。

フィールドベースの検索演算子

演算子	例	説明
AND	name="Data List" AND message="Hello" AND 1.2.3.4	すべてのデータ型で有効です。
OR	(name="TestEvent" OR message="Hello") AND type=2 AND 1.2.4.3	すべてのデータ型で有効です。
NOT	NOT name="test 123"	すべてのデータ型で有効です。
!=	destinationPort != 100	すべてのデータ型で有効です。

フィールドベースの検索演算子 (続き)

演算子	例	説明

	`message!="failed login"`
	
	`message!=failed*login`
	`(* means wildcard) “test”`
	
	`message!=failed\*login`
	`(* is literal in this case)`	

=	`bytesIn = 32`
	
	`message="failed login"`
	
	`message=“failed*login”`
	`(* means wildcard)`
		すべてのデータ型で有効です。
		
		スキーマ内の各フィールドのサイズはあらかじめ決められています。検索対象の文字列がフィールド長よりも長い場合は、=検索ではなくSTARTSWITHを使用し、フィールドサイズを超えない文字数を含めることをお勧めします。デフォルトのフィールドのサイズを決定するには、「デフォルトのフィールド」(354ページ)を参照してください。カスタムフィールドのサイズを決定するには、「カスタムフィールド」(356ページ)を参照してください。

フィールドベースの検索演算子 (続き)

演算子	例	説明
>*	bytesIn > 100	すべてのデータ型で有効です。 * これらの演算子は、条件を辞書的に評価します。たとえば、deviceHostName BETWEEN AM AND EUは、名前の先頭がAM、AMA、AMB、AN、AO、AP...EUのすべてのデバイスを検索します。そのため、名前がAK、ALなどで始まるデバイスはすべて無視されます。同様に、名前がEUA、EUB、FA、GBなどのデバイスも無視されます。
<*	startTime <“$Now - 1d”	
>=*	endTime >=“01/13/2015 07:07:21” endTime >=“2015/13/01 00:00:00 PDT” endTime >=“Sep 10 2015 00:00:00 PDT”	
<=*	startTime <=“$Now - 1d”	
IN*	priority IN [2,5,4,3] destinationAddress IN [“192.0.2.4”, “192.0.2.14”] _deviceGroup IN [“DM1”] _storageGroup NOT IN [“Internal Event Storage Group”, “SG1”] _peerLogger IN [“192.0.2.10”, “192.0.2.11”]	
BETWEEN*	priority BETWEEN 1 AND 5	
STARTSWITH	message STARTSWITH “failed”	文字列 (テキスト) データ型でのみ有効です。
ENDSWITH	message ENDSWITH “login”	文字列 (テキスト) データ型でのみ有効です。
CONTAINS	message CONTAINS “foobar”	文字列 (テキスト) データ型でのみ有効です。 **注:** この演算子には、正規の完全なIPv6アドレスを使用する必要があります。断片的なIPv6アドレスは使用しないでください。
IS	sessionId IS NULL sessionId IS NOT NULL	すべてのデータ型で有効です。

フィールドベースの検索演算子 (続き)

演算子	例	説明
INSUBNET	sourceAddress insubnet "192.0.2.*" agentAddress insubnet "2001:db8::-2001:db8::ffff:ffff:ffff" agentAddress insubnet "192.0.*.*" AND NOT deviceAddress insubnet "192.0.2.*" agentAddress insubnet "192.0.1.0-192.0.2.0" AND NOT destinationAddress insubnet "198.51.100.0/24" agentAddress insubnet "192.0.*.*"AND NOT deviceAddress insubnet "192.0.2.*" agentAddress insubnet "192.0.2.0/24" AND deviceAddress insubnet "198.51.100.0/24" deviceAddress insubnet "192.0.2.0/24" OR destinationAddress insubnet "2001:db8::/32" agentAddress insubnet "2001:db8::/32" OR sourceAddress insubnet "192.0.2.0/16"	sourceAddress、deviceAddress、agentAddress、destinationAddressといったアドレスフィールドのサブネットに基づいて、IPv4、IPv6のアドレスをフィルターします。 次のいずれかの方法で、サブネットを指定できます。 • CIDR表記:「アドレス/プレフィックス長」。例: 192.0.2.23/24 • アドレス範囲: address1-address2。例: 192.0.2.0-192.0.2.255 • 1つ以上のアスタリスクでアドレスの右側の情報を置き換えるワイルドカード式。例: 192.0.2.* INSUBNETを使用したIPv6アドレスの検索例については、「INSUBNET演算子を使用したIPv6アドレスの検索」(122ページ)を参照してください。

フィールドベースの検索式のガイドライン

フィールドベースの式を指定するときには、以下のガイドラインに従ってください。

- 「クエリ式の構文リファレンス」(89ページ)に記載されている要件に従ってください。
- その他のクエリを記述する際に考慮すべき点は、「検索クエリの作成について」(110ページ)に記載されています。
- 高速な検索のために、「出現頻度の少ないフィールド値の検索」(117ページ)および「検索パフォーマンスの調整」(116ページ)の推奨事項に従ってください。
- デフォルトでは、フィールドベースの検索で大文字と小文字が区別されます。大文字と小文字の区別は、[設定 | 検索] > [検索オプション] ページの [フィールド検索オプション] セク

ションで変更できます。詳細については、「グローバル検索オプション」(349ページ)を参照してください。

- あらかじめ定義されたLoggerスキーマフィールドを指定できます。例えば、`cat = /Monitor/CPU/Usage`のように指定します。完全な一覧については、「インデックス作成」(152ページ)を参照してください。
- スキーマに追加したカスタムフィールドを指定できます。例えば、`SSN=333-333-3333`のように指定します。カスタムスキーマフィールドの詳細については、「スキーマへのフィールドの追加」(461ページ)を参照してください。
- あらかじめ定義されたパーサーまたはユーザー定義のパーサーを通じて作成したユーザー定義フィールドは、クエリのインデックス検索部分に指定できません(クエリのインデックス検索部分は、最初のパイプライン文字の前の式です)。

  クエリ式 (インデックス検索 | 検索演算子) は、パイプライン方式で左から右に評価されます。設計により、パーサー (あらかじめ定義されたパーサーまたはユーザー定義のパーサー) は、検索クエリで検索演算子が処理されるときにイベントに適用されます。そのため、イベントにパーサーが適用されるときのフィールド作成は、インデックス検索ステージの後に発生します。その結果、これらのフィールドをフィールドベースの検索クエリで指定することはできません。

  たとえば、Apache Access Logパーサーは、フィールド`SourceHost`を作成します。次のクエリ式を指定することはできません。

  ```
  SourceHost="192.0.2.0"
  ```

  しかし、次の例に示すように、最初のパイプラインの後でこのフィールドを使用できます。

  ```
  | where SourceHost="192.0.2.0"
  ```

  または、Apache Access Log`SourceHost="192.0.2.0"`のみを検索する場合は、次の式を指定できます。

  ```
  | where parser="Apache Access Log" and clientIP="192.0.2.0"
  ```

  また、全文 (キーワード) 検索を`"192.0.2.0"`に対して次のように実行できます。

  ```
  "123.456.789" | where SourceHost="192.0.2.0"
  ```

- イベントフィールドに、予期しない型のデータが含まれている場合 (たとえば、整数を期待しているときに文字列が含まれている場合)、データは無視されます。そのため、そのデータ値の検索では結果が生成されません。たとえば、ポートフィールドに8080 (英数字) ではなく値8080A (英数字) が含まれている場合、英数字の値は無視されます。スキーマフィールドのデータタイプは、[設定 | 検索] > [デフォルトのフィールド] ページで参照できます。この情報を参照する方法の詳細については、「デフォルトのフィールド」(354ページ)を参照してください。
- 最適な検索パフォーマンスのためには、クエリで指定した時間範囲について、すべてのピアのイベントフィールドにインデックスが作成されていることを確認してください。指定した時間範囲について、あるシステムではイベントフィールドのインデックスが作成されていても、そのピ

アでインデックスが作成されていない場合、分散検索の実行がそのピアで低速になります。ただし、ローカルシステムでは最適な速度で実行されます。そのため、そのような設定での検索パフォーマンスは低下します。

- レポート生成を高速化するためには、レポートのすべてのフィールド (レポートに表示されるフィールドを含む) にインデックスが作成されている必要があります。つまり、クエリのWHERE句のフィールドに加えて、SELECT句のフィールドにもインデックスを作成する必要があります。

フィールドベースの検索演算子の制限

クエリ演算子 (STARTSWITH、ENDSWITH、およびINSUBNETなど) を使用して、IPv6アドレスの全体または一部を検索する場合、アドレスは正規形式 (RFC 5952で指定) である必要があります。IPv4射影IPv6アドレスは使用しないでください。

CONTAINS演算子を使用するクエリでは、完全なIPv6アドレスのみを使用します。断片的なIPv6アドレスは使用しないでください。

正規形式の詳細については、https://tools.ietf.org/html/rfc5952, section 4: A Recommendation for IPv6 Text Representationを参照してください。

クエリの検索演算子部分

クエリの検索演算子部分では、インデックス検索フィルターに一致したデータをさらに絞り込むことができます。検索演算子の一覧と使用例については、「検索演算子」(564ページ)を参照してください。

rex検索演算子は、Syslogイベント (rawデータまたは構造化されていないデータ) に役立ちます。または、あるイベントの15文字目など、1つのイベントの特定の場所から情報を抽出する場合にも便利です。head、tail、top、rare、chart、sort、fields、evalなどの他の演算子は、指定したフィールドか、rex演算子を使用して抽出した情報に適用されます。

時間範囲

イベントのタイムスタンプには、Loggerで受信したときの受信時刻が設定されます。**検索クエリは、この受信時刻を使用して一致するイベントを探します**。

ほとんどの状況では、Loggerの受信時刻はイベント時刻と同じです。しかし、イベント時刻と、Loggerによるイベントの受信時刻は違う可能性があります。なぜなら、一般に、イベントがデバイスから送信されてからLoggerで受信されるまでには、若干の遅れがあるためです。デバイスのクロックがLoggerのクロックよりも進んでいるか遅れていると、遅れや進みが大きくなります。

検索演算子では、イベントを検索する時間範囲を指定する必要があります。定義済みの多数の時間範囲から選択するか、ニーズに合ったカスタム時間範囲を定義できます。

クエリで時間範囲を定義する際には、「サマータイムの変更がLoggerの処理に与える影響」(499ページ)に記載されている内容を考慮する必要があります。

定義済みの時間範囲: 「過去2時間」や「本日」といった定義済みの時間範囲を選択する場合、時間範囲は現在時刻からの相対になります。たとえば、「過去2時間」を、7月13日の午後2時00分00秒に選択すると、7月13日の午前12時00分00秒から午後2時00分00秒までのイベントが検索されます。同じ日の午後5時00分00秒に検索結果を更新すると、時間ウィンドウが再計算されます。そのため、指定した条件に一致し、7月13日の午後3時00分00秒から5時00分00秒の間に発生したイベントが表示されます。

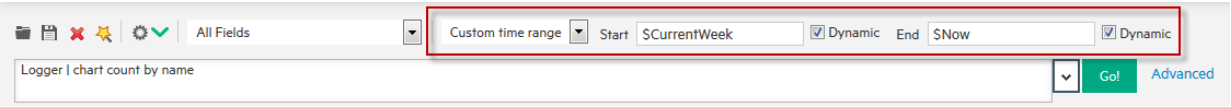
カスタム時間範囲: ニーズに合わせて、24時間形式で時間範囲を指定できます。たとえば、カスタム時間範囲を次のように指定できます。

開始: 2015年8月13日の午後1時36分30秒
終了: 2015年8月13日の午後10時36分30秒

デフォルトでは、カスタム時間範囲の終了時刻はLogger上の現在時刻であり、開始時刻は現在時刻の2時間前になります。

変数を使用してカスタム時間範囲を指定することもできます。たとえば、$Now - 2h (2時間前) に開始され、$Now (現在時刻) に終了する動的な日付範囲を指定できます。この動的検索は、クエリの実行時点を基準としたものです。スケジュールされた検索処理では、このメカニズムを使用して、実行のたびにより新しいイベントデータを検索します。

ユーザーインターフェイスの「動的」フィールドを使用すると、次の図に示すように動的な時刻を指定できます。



次に、結果を過去2時間の活動に制限する、動的検索の典型的な例を示します。

開始: $Now - 2h
終了: $Now

動的検索の構文は次のとおりです。

```
<current_period> [ +/- <units>]
```

ここで、<current_period>には、$Nowのように単独で指定するか、プラス(「+」) またはマイナス(「-」) と2h (2時間)などの単位数値を続けて指定します。<current_period>は、「現在の期間」(80ページ) に示すように、常に「$」で始まる単語からなり、大文字と小文字が区別され、スペースを含みません。<units>部分を指定する場合は、「単位」(81ページ) に示すように、整数と、大文字と小文字が区別される単一の文字からなります。

現在の期間

期間	説明
$Now	現在の分
$Today	現在の日の午前零時 (最初の分の始まり)

現在の期間 (続き)

期間	説明
$CurrentWeek	前の月曜日の午前零時 (今日が月曜日の場合は$Todayと同じ)
$CurrentMonth	現在の月の最初の日の午前零時
$CurrentYear	現在の年の最初の日の午前零時

単位

単位	説明
m (小文字)	分 (月を表す「M」と間違えないこと)
h	時間
d	日
w	週
M (大文字)	月 (分を表す「m」と間違えないこと)

Loggerのタイムスタンプ

イベントは、受信時刻、イベント時刻、ソース (ホスト名またはIPアドレス)、未解析のメッセージ部分からなります。

イベント時刻は、Logger受信者がイベントを受信した時刻です。Loggerは、検索およびレポート作成時に、このフィールドを使用して一致するイベントを見つけます

受信時刻は、イベントがストレージグループ (ディスク) に書き込まれた時刻です。すべてのイベントのタイムスタンプには、Loggerで受信したときの受信時刻が設定されます。

注: ほとんどの状況では、Loggerの受信時刻はイベント時刻と同じです。しかし、イベント時刻と、Loggerによるイベントの受信時刻は違う可能性があります。なぜなら、一般に、イベントがデバイスから送信されてからLoggerで受信されるまでには、若干の遅れがあるためです。その他の要因で遅れが生じることもあります。たとえば、ファイル受信者でイベント時刻の解析が有効になっている場合、受信時刻がイベント時刻よりも遅くなる場合があります。

- Loggerでは、転送やストレージ保管およびアーカイブを行う際に、受信時刻フィールドを使用して一致するイベントを見つけます。
- 転送者フィルターにイベントの転送を評価する期間が指定されている場合、Loggerによるイベントの受信時刻を使用して、イベントを通知先に転送するかどうかが判定されます。
- Loggerは、イベントの受信時刻を使用してそのアーカイブ日を決定します。
- 検索結果は、Loggerのイベント時刻順にソートされます。
- ヒストグラムは、Loggerのイベント時刻に基づいています。

- デフォルトのフィールドは自動的にインデックス作成されます。残りのフィールドについて、Loggerはイベントの受信時刻と、フィールドがインデックスに追加された時刻を使用して、そのイベントのインデックスを作成するかどうかを判定します。イベントの受信時刻が、フィールドがインデックスに追加された時刻と同じかそれよりも後の場合は、イベントのインデックスが作成されます。そうでない場合は作成されません。

イベント時刻と受信時刻の他にも、Loggerのイベントでは、次のようなタイムスタンプを参照できます。

エージェントの受信時刻は、コネクターがイベントを受信した時刻です。Loggerではこのフィールドは使用されませんが、検索することができます。

終了時刻は、デバイス上でのイベントの元の時刻です。Loggerではこのフィールドは使用されませんが、検索することができます。

マネージャー受信時刻は、ESMがイベントを受信した時刻です。Loggerではこのフィールドは使用されませんが、検索することができます。

フィールドセット

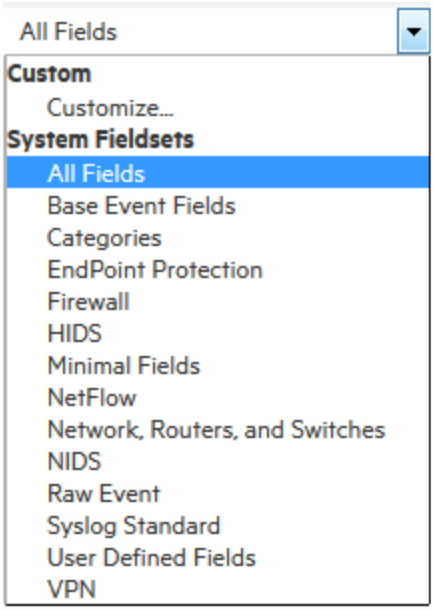
フィールドセットは、検索クエリに一致する各イベントについて、検索結果に表示されるフィールドを決定します。フィールドセットを選択することで、検索結果に表示されるフィールドを選択することになります。詳細については、「フィールドセットを使用した検索結果表示の変更」(129ページ)を参照してください。あらかじめ定義されたフィールドセットを使用するか、独自のフィールドセットを作成できます。

事前定義フィールドセット

システムには、事前定義の多数のフィールドセットが用意されています。

利用可能なフィールドの一覧を表示するには

1. [フィールド] ダイアログボックスの下矢印をクリックします。[システムフィールドセット (System Fieldsets)] リストが表示されます。



特定のフィールドセットを使用して検索結果を表示するには

1. ドロップダウンリストからフィールドセットをクリックします。

注: 一致したイベントで使用できるフィールドのみが検索結果表示 (またはエクスポートされたファイル) に表示されます。したがって、[**すべてのフィールド (All Fields)**] フィールドセットを選択しても、検索結果にはすべてのフィールドは表示されず、検索で見つかったイベントに含まれるフィールドのみが表示されます。

フィールドセットの詳細については、「フィールドセットの管理」(354ページ) を参照してください。

[ユーザ定義フィールド] フィールドセット

`rex`、`rename`、`eval`などの、新しいフィールドを定義する検索演算子を使用すると、各フィールドの新しい列が現在選択されている表示に追加されます。これらの新たに定義されたフィールドは、デフォルトで表示されます。[**ユーザ定義フィールド (User Defined Fields)**] フィールドセットを使用すると、新たに定義したフィールドのみが表示されます。

[rawイベント] フィールドセット

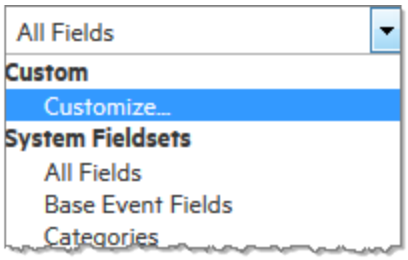
[**rawイベント (Raw Event)**] フィールドセットは、rawEventという名前の列にraw syslogイベント全体を表示し、イベントは列に収まるように書式設定されます。

rawイベントフィールドは、syslogイベントに最も適していますが、CEFイベントに関連するrawイベントをrawEvent列に表示することもできます。そのためには、イベントをLoggerに送信しているコネクターが、rawEventフィールドにrawイベントを設定するようにします。

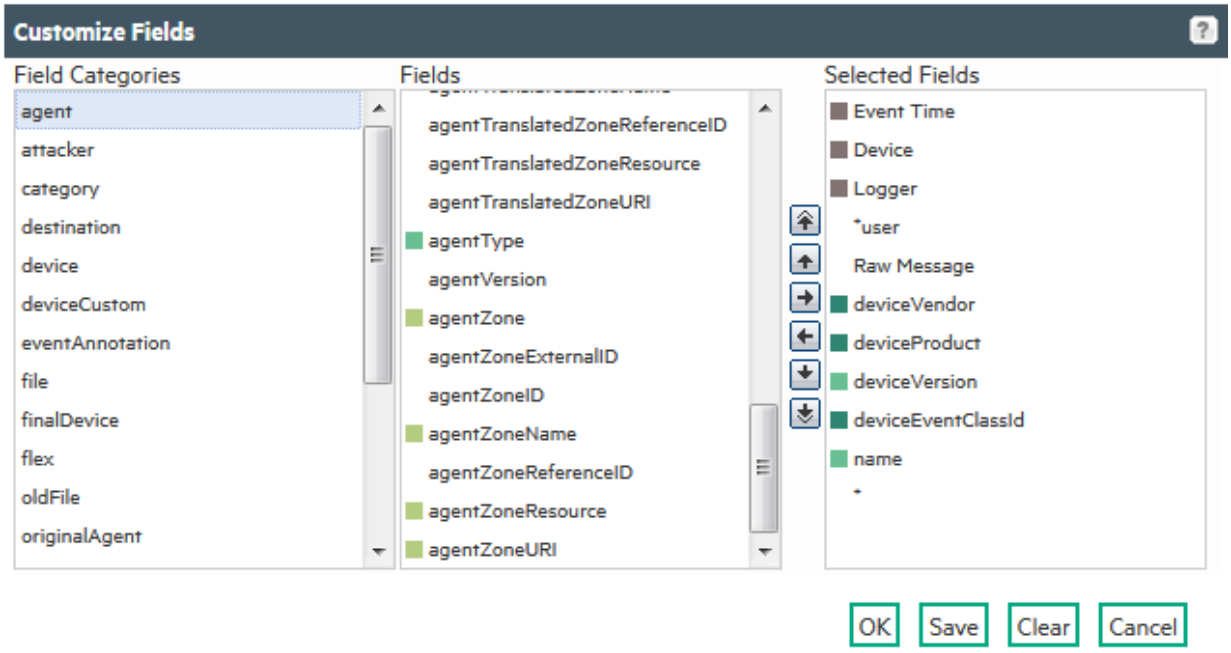
注: rawEvent列でrawイベントを表示するには、検索オプション [syslog イベントの rawEvent フィールドを生成] を有効にします。詳細については、「グローバル検索オプション」(349ページ) を参照してください。

カスタムフィールドセット

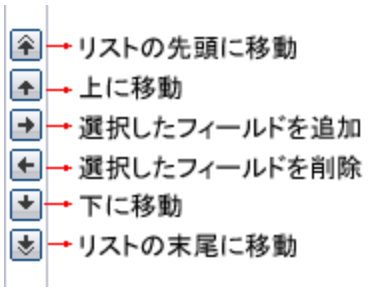
[フィールド] ドロップダウンメニューから [カスタマイズしています... (Customize…)] を選択することで、独自のフィールドセットを作成できます。



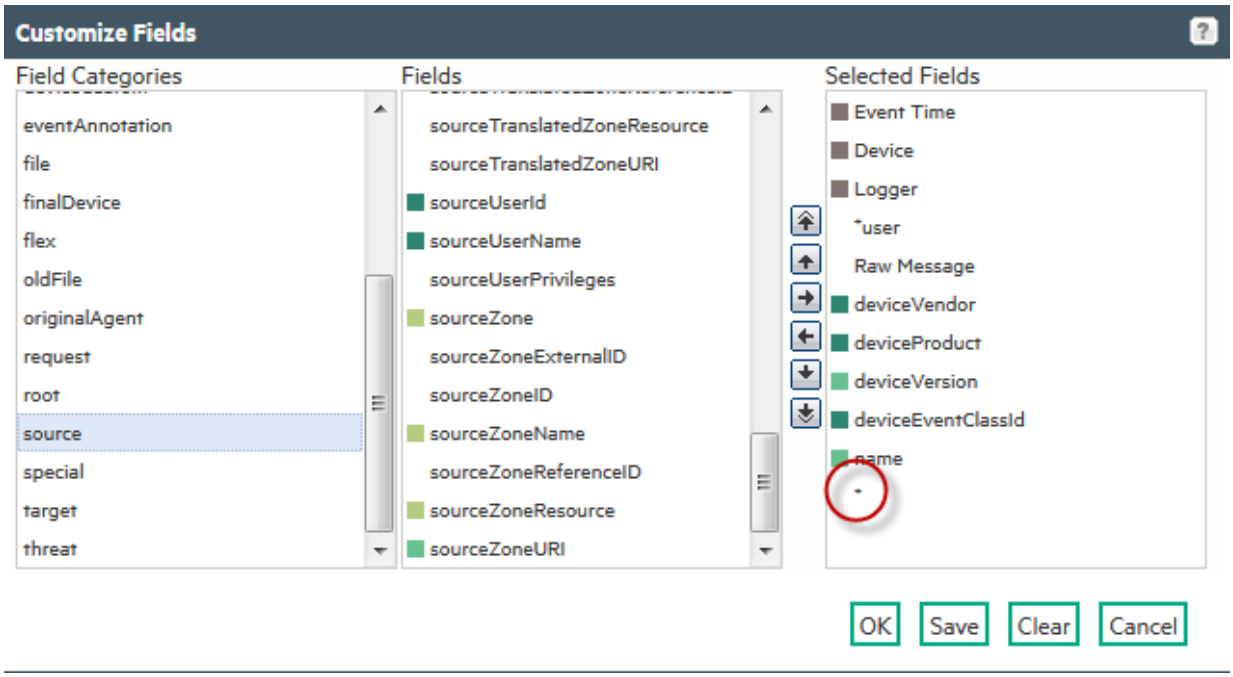
このユーザーインターフェイスを使用すると、フィールドセットに含めるイベントフィールドを選択および移動できます。



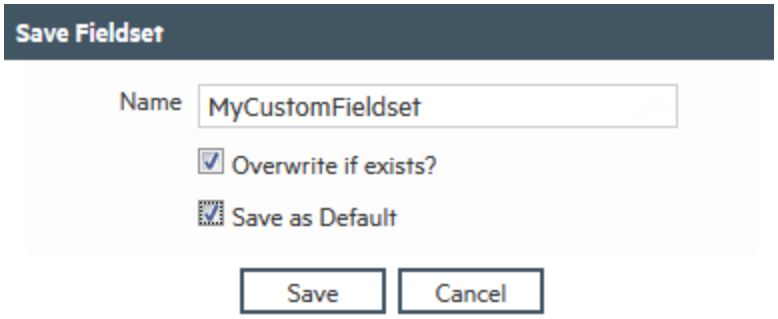
次のボタンを使用してカスタムフィールドセットを作成および編集します。



ワイルドカードフィールド (「*」) は、カスタムフィールドセットを作成すると[フィールド]リストで使用可能になります。このフィールドには、カスタムフィールドセット定義に個別に表示されない、イベントで使用できるすべてのフィールドが含まれています。たとえば、次のカスタムフィールドセット定義で、検索結果には、アスタリスク (「*」) の前にあるフィールドが最初に表示され、イベント内の他のフィールドがそれに続きます。最後に、**deviceEventClassId**フィールドと**Name**フィールドが表示されます。



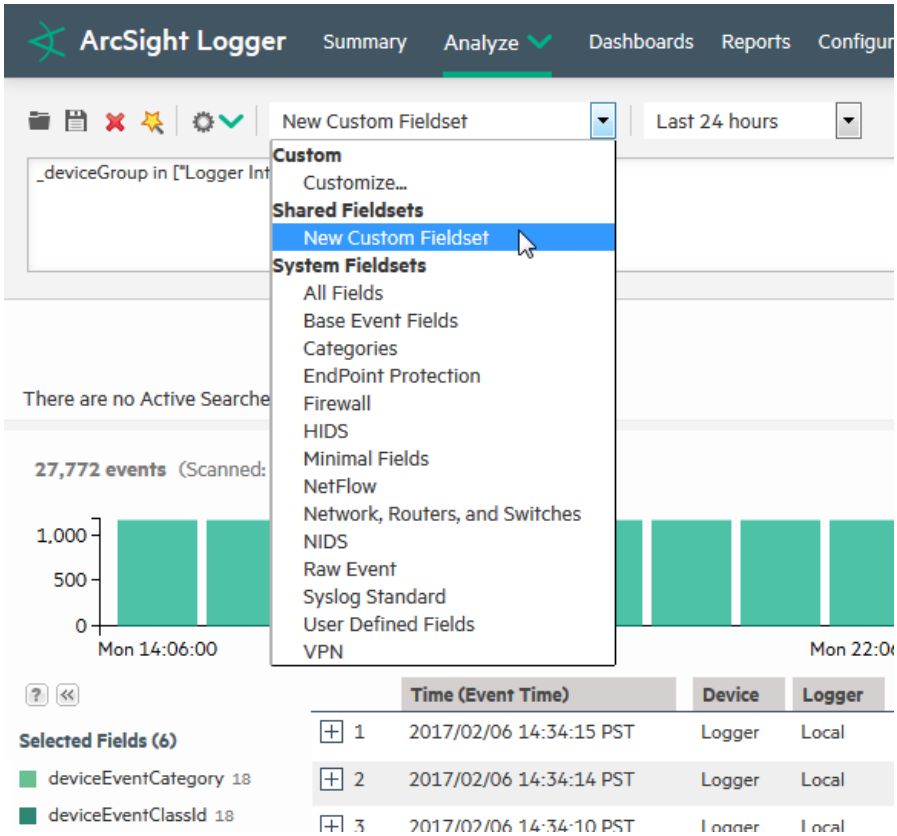
カスタムフィールドセットは、保存することも、現在のセッションのみで使用することもできます。



[**OK**] をクリックすると、フィールドセットがCustomカテゴリに表示されます。「カスタム (保存しない)」というラベルが付けられ、他のユーザーからは見えません。このセッションで引き続き使用できます。現在のセッションをログアウトすると、一時的なフィールドセットは削除されます。一度に設定できる一時的なカスタムフィールドセットは1つだけです。

[保存] をクリックすると、次の図に示すように、フィールドセットが [共有フィールドセット] カテゴリの下に表示され、他のユーザーが参照および使用できるようになります。保存したフィールドセットは、編集および削除できます。

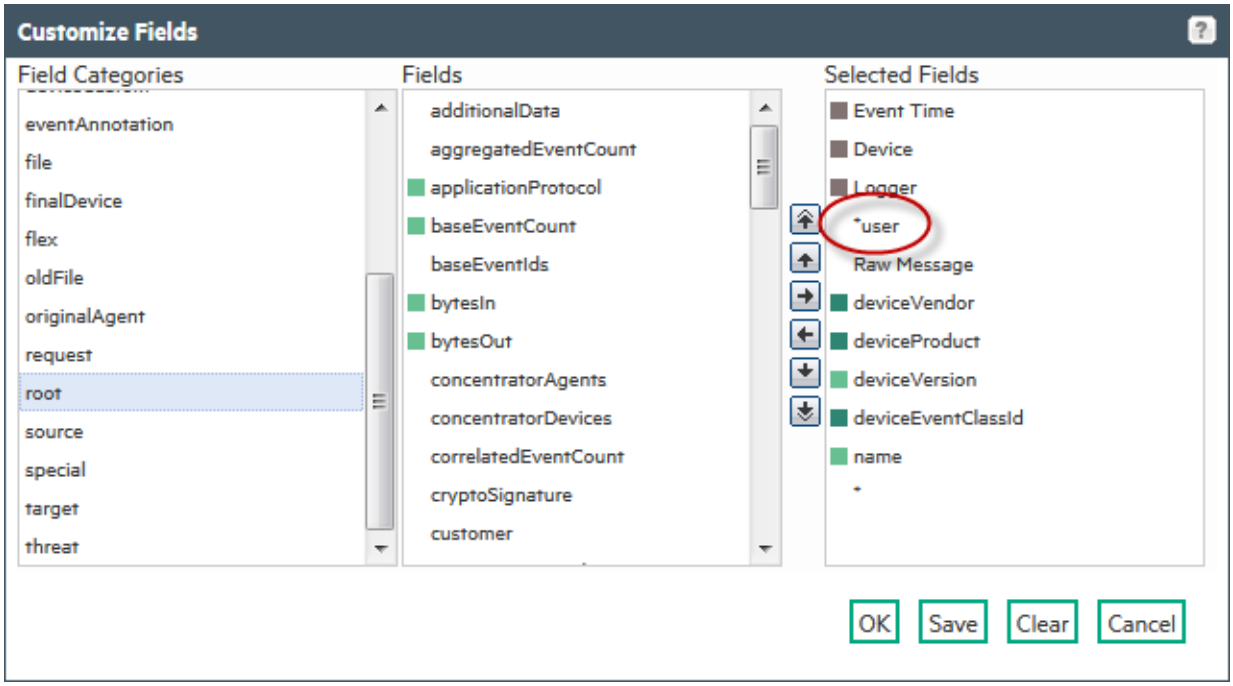
カスタムフィールドセットを保存するとき、このシステムのデフォルトとして指定できます。そうすると、そのシステムですべてのユーザーのデフォルトフィールドセットになります。デフォルトとして指定しない場合、フィールドセットは自分の検索結果のみに使用され、同じシステムに接続する他のユーザーには影響を与えません。



カスタムフィールドセットの削除の詳細については、「フィールドセットの管理」(354ページ)を参照してください。

注: フィールドセットは、保存されたフィルター定義に含まれません。

以下に示す*userフィールドは、検索演算子 (rex、rename、extract、またはeval) で定義されるフィールドと、パーサーがイベントに適用されるときに作成されるフィールドの表示を制御します。*userがカスタムフィールドセットの [選択したフィールド (Selected Fields)] リストに含まれている場合、作成または定義したフィールドが表示されます。



制約

クエリで制約を使用すると、検索処理を高速化できます。これは、制約によって、検索で必要なデータの範囲が制限されるためです。制約を使用すると、以下の1つ以上から受信したイベントにクエリを制限できます。

- 特定のデバイスグループ
- 特定のストレージグループ
- 特定のピア

たとえば、ローカルシステム上のストレージグループSG1およびSG2のみのイベントや、特定のピア上のイベントを検索できます。

ストレージグループとピアの詳細については、「ストレージ」(428ページ)、「デバイスグループ」(367ページ)、「ピアノード」(483ページ)を参照してください。

制約を指定する際には、以下のガイドラインに従ってください。

- 検索クエリ式で制約を指定するには、以下の演算子を使用します。

メタデータ識別子	例
_deviceGroup	_deviceGroup IN [“DM1”, “HostA”] ここで、DM1はデバイスグループ、HostAはデバイスです。 **注:** このフィールドを使用して、個々のデバイスを指定できます。
_storageGroup	_storageGroup IN [“Internal Event Storage Group”, “SG1”]
_peerLogger	_peerLogger IN [“192.0.2.10”, “192.0.2.11”]

- クエリに論理演算子ORとメタデータ識別子が含まれている場合、ORで評価する式は、次の例に示すように括弧で囲まれている必要があります。

  ```
  (success OR fail) _storageGroup IN [“Default Storage Group”]
  ```

  ORを使用して評価する式が括弧で囲まれていない場合、ユーザーインターフェイス画面にエラーメッセージが表示されます。
- 複数のグループを制約で指定する場合は、_storageGroup IN [“SGA”, “SGB”]のように、グループ名を角括弧で囲みます。
- 検索クエリに制約を適用するには、以下のいずれかの方法を使用します。
  a. [検索]テキストボックスに制約を入力する。

     「_s」(ストレージグループの場合)、「_d」(デバイスグループの場合)または「_p」(ピアの場合)を[検索]テキストボックスに入力すると、検索ヘルパーにより、該当する項と演算子のドロップダウンリストが自動的に表示され、そこから選択できるようになります。

     注意: 検索クエリに制約と正規表現が含まれている場合は、制約が正規表現の前に指定されていることを確認してください。例: _peerLogger IN [“192.0.2.10”] name contains abc | REGEX=“:\d31”

  b. 検索の詳細設定ツールからストレージグループまたはピアを選択する検索の詳細設定ツールにアクセスするには、クエリを入力するテキストボックスのすぐ下の[**検索の詳細設定**]をクリックします。「検索の詳細設定ビルダーの使用」(94ページ)を参照してください。

クエリ式の構文リファレンス

有効で正確なクエリ式を作成するには、以下の要件に従ってください。

クエリ構文の要件

動作	全文検索	フィールド検索	正規表現
大文字小文字の区別	区別しない (変更不可)	区別する (調整オプションを使用して変更できます。「グローバル検索オプション」(349ページ)を参照してください。)	区別しない (調整オプションを使用して変更できます。「グローバル検索オプション」(349ページ)を参照してください。)

エスケープ文字	\
	\をエスケープするために使用します。他の文字はエスケープできません。
		\
		\、"、*をエスケープするために使用します。
		例:
		`name=log\\ger (matches log\ger)`
		`name=logger\* (matches logger*)`
			\
			任意の特殊文字をエスケープするために使用します。
			例:
			文字"["を含む項を検索するには
			`|REGEX= “logger\[”`

ワイルドカード文字のエスケープ	*を検索不可 例: `log\*`は無効	文字をエスケープすることで*を検索できます。 例: `name=log\*`は有効	文字をエスケープすることで*を検索できます。 例: `name=log\*`は有効

クエリ構文の要件 (続き)

動作	全文検索	フィールド検索	正規表現
完全一致/検索文字列に含まれる演算子または特殊文字	キーワードを二重引用符で囲みます。二重引用符で囲まない場合は、キーワードの末尾にワイルドカードが付いているものとして処理されます。 例: `log` (log、logging、loggerなどに一致) `"log"` (logのみに一致) **ヒント:** この表の後のほうにある、二重引用符で囲んでも検索できない特殊文字の一覧を参照してください。	値を二重引用符で囲みます。 例: `message="failed login"`	特別な要件はありません。
入れ子 (「(a OR b) AND c」などのカッコで囲む句を含む)	許可 • キーワードを接続およびネストするには、論理演算子を使用します。 • メタデータ識別子 (_storageGroup、_deviceGroup、および_peerLogger)。ただし、クエリ式の最上位のみに使用できます。クエリに正規表現が含まれている場合、メタデータ識別子は正規表現の前にあることが必要です。	許可 • 「フィールドベースの検索」(73ページ) に記載されている任意の演算子を使用して、フィールド検索式を接続およびネストします。 • メタデータ識別子 (_storageGroup、_deviceGroup、および_peerLogger)。ただし、クエリ式の最上位のみに使用できます。	複数の正規表現を、次の構文を使用して1つのクエリで指定できます。 `|REGEX= "<REGEX1>" |REGEX="<REGEX2>"|...`

クエリ構文の要件 (続き)

動作	全文検索	フィールド検索	正規表現

演算子	大文字、小文字、または大文字と小文字が混在したブーリアン演算子 (AND、OR、NOT)。演算子が指定されていない場合は、ANDが使用されます。
	
	イベント中の演算子AND、OR、NOTそのものを検索するには、二重引用符で囲みます。
	
	例: “AND”、“OR”、“Not”
	
	注: クエリに論理演算子ORとメタデータ識別子 (_storageGroup、_deviceGroup、および_peerLogger) が含まれている場合、ORで評価する式は、括弧で囲まれている必要があります。
	
	例:
	
	`(success OR fail) _storageGroup IN [“Default Storage Group”]`
		「フィールドベースの検索」(73ページ) セクションに一覧表示されている演算子を使用してください。
		
		• 値が二重引用符で囲まれていない限り、値の間のスペースはANDと解釈されます。
		例えば、`name=John Doe`は`John AND Doe`と解釈されます。
		• 演算子が複数のフィールド式の間に指定されていない場合は、ANDが使用されます。
		• 演算子そのものを検索するには、演算子を二重引用符で囲みます。
		例:
		`message STARTSWITH=“NOT”`
		`message=“LOGIN DID NOT SUCCEED”`
		• クエリに論理演算子ORとメタデータ識別子 (_storageGroup、_deviceGroup、および_peerLogger) が含まれている場合、ORで評価する式は、括弧で囲まれている必要があります。
		例:
		`(success OR fail) _storageGroup IN [“Default Storage Group”]`
			| および「時間範囲」(79ページ) に記載されている演算子。
			
			この演算子を使用して、1つのクエリ式で複数の正規表現をAND演算します。

クエリ構文の要件 (続き)

動作	全文検索	フィールド検索	正規表現
一次区切り文字: スペース , ; ( ) [ ] } “ | * > < !	キーワードを二重引用符で囲むことで、一次区切り文字を含むキーワードを検索できます。 例: “John Doe”“Name=John Doe”“www.hp.com”	これらの文字を検索できます。値にこれらの文字のいずれかが含まれている場合は、値を二重引用符で囲みます。 例: name=“John*”	指定する正規表現で、指定したパターンのみを含むイベントを検索するのでない限り、検索対象文字として「^」を先頭に指定したり、「$」を末尾に指定したりすることはできません。 \や?などの特殊な正規表現文字はエスケープする必要があります。 例: \|REGEX= “^test$” は、"test" (引用符なし) という単語のみを含むイベントを検索します。
二次区切り文字: = .: / \ - ? # $ & _ %	「グローバル検索オプション」(349ページ) で説明するフルテキスト検索オプションを設定した後は、セカンダリ区切り文字を含むキーワードを検索することもできます。 例: hpe.comをURL http://www.hpe.com/apps中で検索するには、検索文字列としてhpe.comを指定します。	これらの文字を検索できます。値にこれらの文字のいずれかが含まれている場合は、値を二重引用符で囲みます。 例: name=“John”	• 指定する正規表現が、指定しているパターンのみを含むイベントを探しているのでなければ、一致文字として、先頭に^、終わりに$を含めることはできません。たとえば、\|REGEX= "^test$" は、"test" (引用符なし) という単語のみを含むイベントを検索します。 • \や?などの特殊な正規表現文字はエスケープする必要があります。
構文	keyword1 boolean_operator keyword2 boolean_operator keyword3	field_name operator field_value (「イベントフィールド名のマッピング」(645ページ) のフィールドの一覧) (「フィールドベースの検索」(73ページ) の演算子の一覧)	|REGEX=“<REGEX1>” | REGEX=“<REGEX2>”|...

クエリ構文の要件 (続き)

動作	全文検索	フィールド検索	正規表現
タブ 改行 { “ *	**これらの文字は検索できません。** 例: "John{Doe"は無効です。	制限はありません。 特殊文字は二重引用符で囲みます。ワイルドカード文字と二重引用符をエスケープします。 例: `name=“John\* \“Doe”` (`John* “Doe"`に一致)	制限はありません。 (、)、[、]、{、}、"、|、* などの特殊な正規表現文字はエスケープする必要があります。

特定の時刻に発生したイベントを検索する場合の時刻形式	特定の形式はありません。クエリは正確なタイムスタンプ文字列を含んでいる必要があります。たとえば"10:34:35"と指定します。
	注: 文字列にスペースを含めることはできません。たとえば、`"Oct 19"`は無効です。
		次の形式を使用して、クエリでタイムスタンプを使用します (**二重引用符を含む**)。
		`"mm/dd/yyyy hh:mm:ss"`
		または
		`"yyyy/mm/dd hh:mm:ss timezone"`
		または
		`"MMM dd yyyy hh:mm:ss timezone"`
		ここで、
		`mm`: 月
		`dd`: 日
		`yyyy`: 年
		`hh`: 時
		`mm`: 分
		`ss`: 秒
		`timezone`: EDT, CDT, MDT, PDT
		`MMM`=月名の最初の3文字 (たとえば、Jan、Mar、Sep)
		時間範囲を狭めるには、演算子<=および>=を使用します。=や!=は使用しないでください。
			制限はありません。

クエリ構文の要件 (続き)

動作	全文検索	フィールド検索	正規表現

ワイルドカード	「*」を先頭に指定することはできません。指定できるのはサフィックスまたはキーワード間のみです。
	例:
	• *logは無効
	• log*は有効
	• lo*g*は有効
		*は、値のどこにでも現れることができます。
		例:
		`name=*log` (ablog、blogなどを検索)
		`name="\*log"`
		`name=\*log`
		(どちらも`*log`を検索)
			*はどこにでも現れることができます。

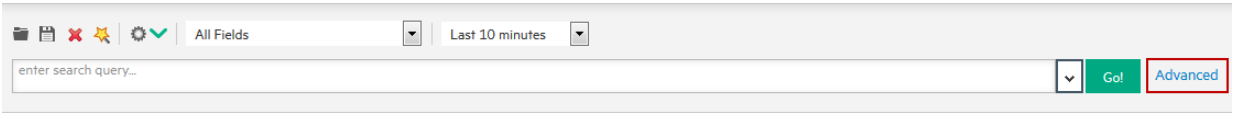
検索の詳細設定ビルダーの使用

検索の詳細設定ツールは、検索クエリを素早く正確に作成するための論理条件エディターです。このツールでは、クエリに含める条件が視覚的に表現されます。このツールを使用して、キーワード、フィールドベースの条件、正規表現を指定できます。また、ピア、デバイスグループ、ストレージグループなどの検索制約も指定できます (「制約」(87ページ)を参照)。ここでは、このツールの使用方法について説明します。

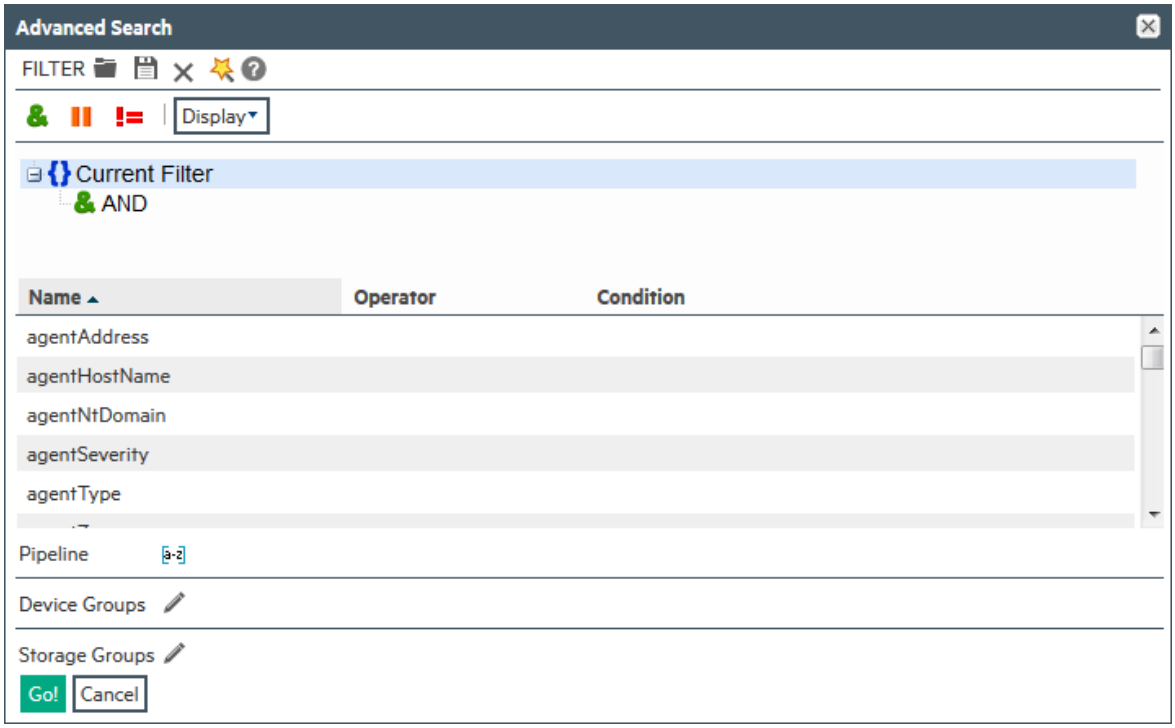
検索の詳細設定ビルダーへのアクセス

検索の詳細設定ビルダーを表示するには

[分析] > [検索] をクリックして検索ページを開き、次の図に示すように、Go!ボタンの右にある、検索テキストボックスの **[検索の詳細設定]** をクリックします。



検索の詳細設定ビルダーを表示するには



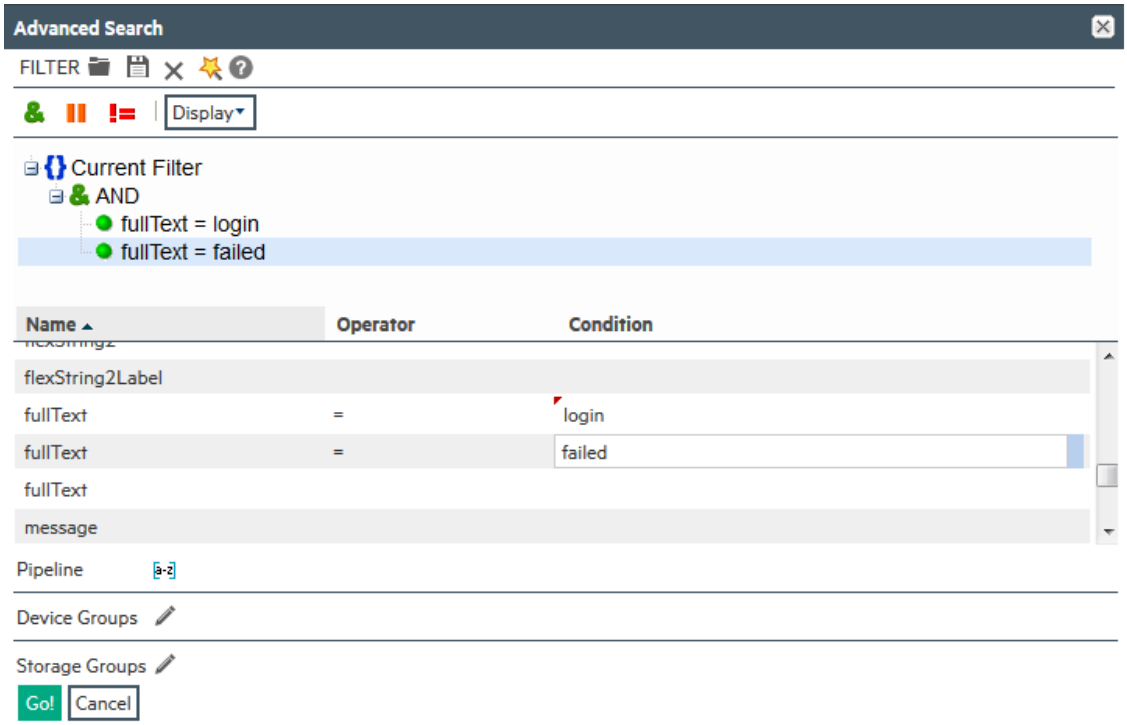
検索の詳細設定ビルダーで新しい検索クエリを作成するには

1. **[分析] >** [検索] をクリックして検索ページを開き、**[検索の詳細設定]** をクリックします。
2. 追加する条件に適用する論理演算子を、検索ビルダーの上部から選択します。次の演算子を選択できます。

演算子	意味
&	AND
||	OR
!=	NOT

3. システムフィルターまたは保存されているフィルター、または保存された検索を読み込むには、アイコンをクリックします。表示されるリストからフィルターまたは保存されている検索を選択し、**[読み込み＋クローズ]** をクリックします。

   詳細については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) および「システムフィルター/事前定義フィルター」(145ページ) を参照してください。
4. キーワード (全文検索) またはフィールド条件を追加するには、以下の手順を実行します。
   a. [名前 (Name)] 列で、追加するフィールドを探します。
      キーワードを指定するには (全文検索)、次の図に示すように、[名前] 列で**fullText** フィールドを使用します。



b. フィールドに関連付けられている [演算子 (Operator)] 列をクリックし、表示されるリストから演算子を選択し、**Enter**キーを押します。

c. フィールドに適用される演算子のみがリストに表示されます。

d. フィールドに関連付けられている [条件 (Condition)] 列で、値を入力し**Enter**キーを押します。

   条件を編集するには、条件を右クリックしてプルダウンメニューを表示し、条件を編集、切り取り、コピー、削除します。

   注: IPアドレスの範囲を指定することはできません。そのため、ある範囲内の複数のIPアドレスを検索するには、CONTAINS演算子とワイルドカード文字を [条件 (Condition)] 列で使用します。たとえば、192.0.2.*と入力します。

5. 上記の手順を繰り返し、すべての条件を追加します。
6. 検索クエリに正規表現を含める場合は、[Regex] フィールドに入力します。
7. 検索クエリを特定のデバイスグループ、ストレージグループ、Loggerに制約する場合は、制約カテゴリの横の✎アイコンをクリックします。該当するグループとLoggerを選択します (複数のグループを選択するには、Ctrlキーを押したまま選択します)。

   Device Groups制約では、デバイスまたはデバイスグループを指定できます。

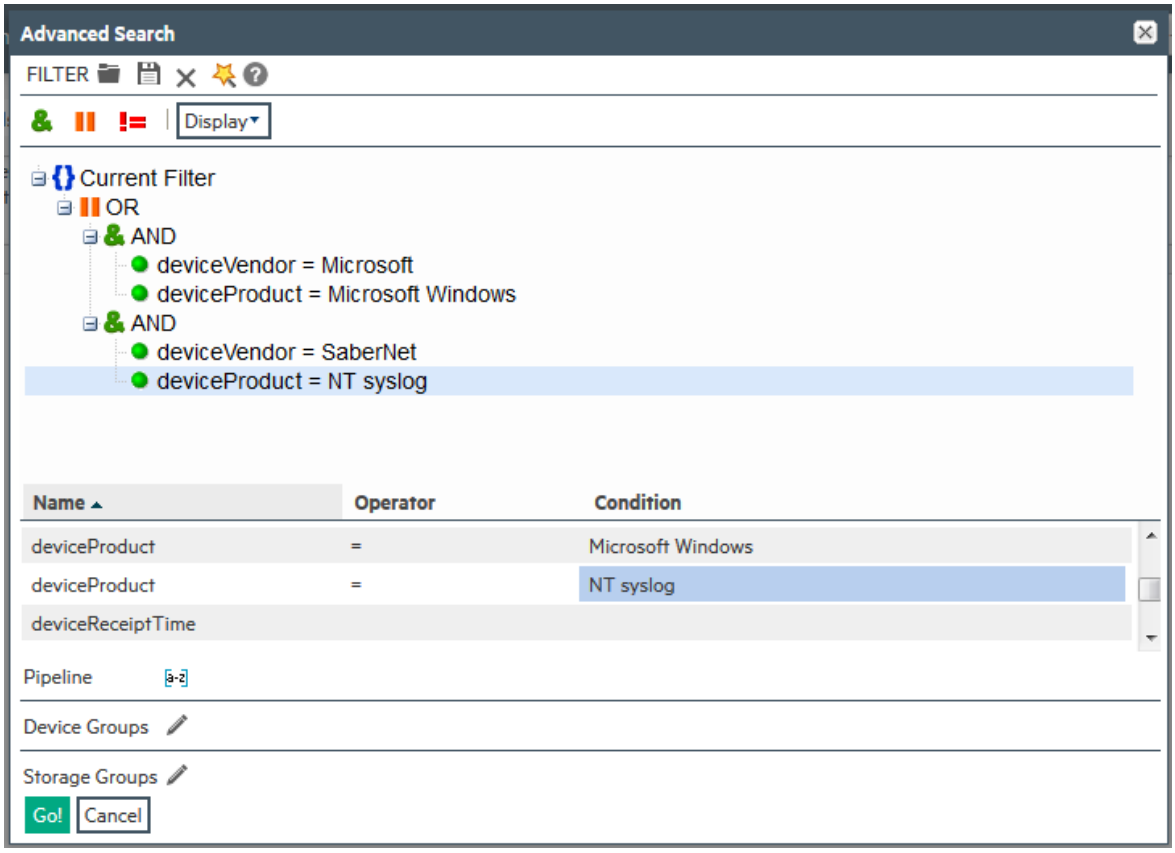
   Loggerの制約カテゴリは、LoggerでLoggerが設定されている場合のみ表示されます。

   1つの制約に複数の値を選択した場合、それらの値はOR演算されます。たとえば、デバイスグループA、B、Cを指定した場合、クエリは、デバイスグループA、B、またはCのイベントを検索します。

8. **[実行! (Go!)]** をクリックします。
   クエリが [検索] テキストボックスに自動的に表示され、実行準備ができた状態になります。
   または
   アイコンをクリックし、後で使用するためにクエリを保存します (保存されたフィルターまたは保存された検索と呼びます)。クエリ保存の詳細については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) を参照してください。

ネストした条件

検索ビルダーで、ネストした条件を含む検索クエリを作成できます。そのためには、次の条件をネストさせる演算子をクリックし、「検索の詳細設定ビルダーへのアクセス」(94ページ) の説明に従って条件を追加します。



ネストした条件を追加するには、

1. クエリの上のアイコンから、追加する演算子を選択します。
2. クエリの下のメニューから、条件を選択します。

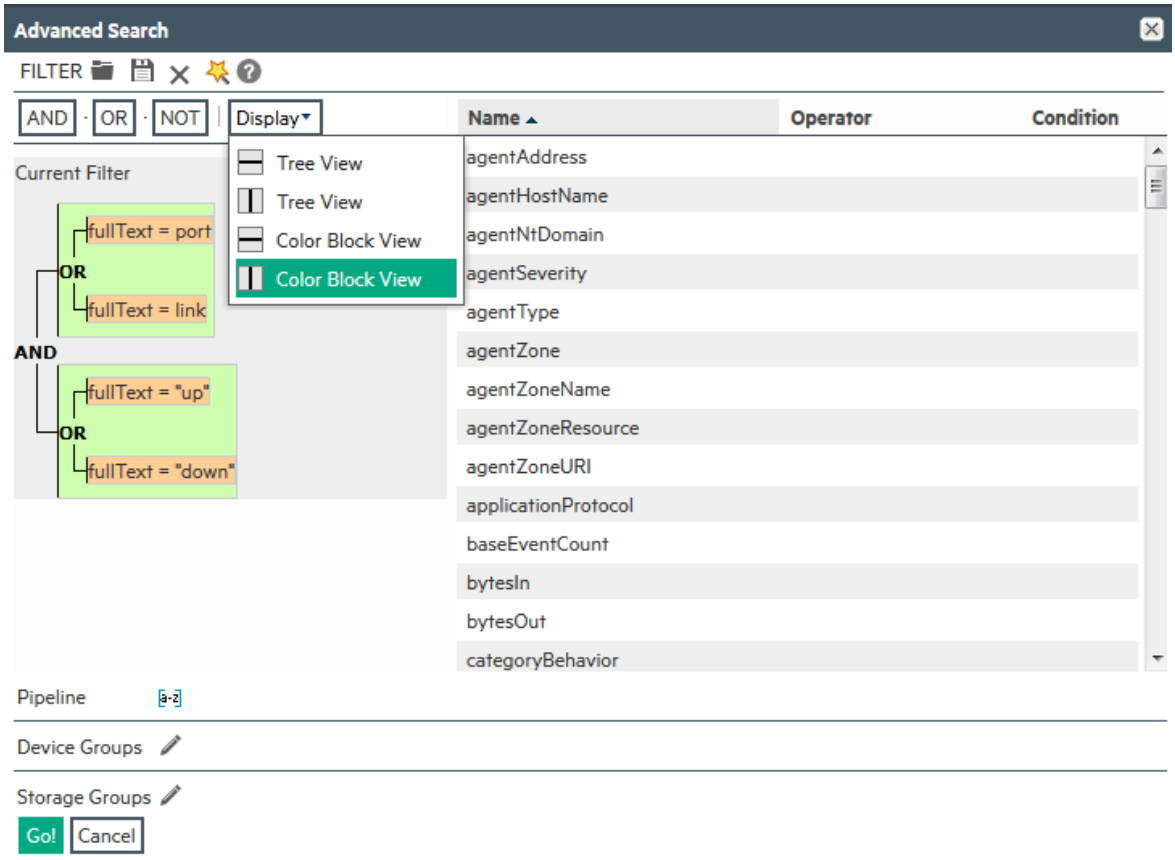
3. 演算子とサポートされるクエリの条件 (たとえば、`deviceProduct = Microsoft`) を追加します。
4. **[実行! (Go!)]** をクリックします。

検索ビルダーでクエリを作成するための他のビュー

デフォルトでは、このセクションのこれまでの図に示すように、条件のツリービュー表現が表示されます。ビューをカラーブロック方式に変更したり、選択したフィールドが表示される場所を変更したりできます。これらは、画面の下部か、条件が表示される場所の右に表示できます。

ビューを変更するには

検索ビルダーツールで **[表示 (Display)]** をクリックし、表示するビューを選択します。

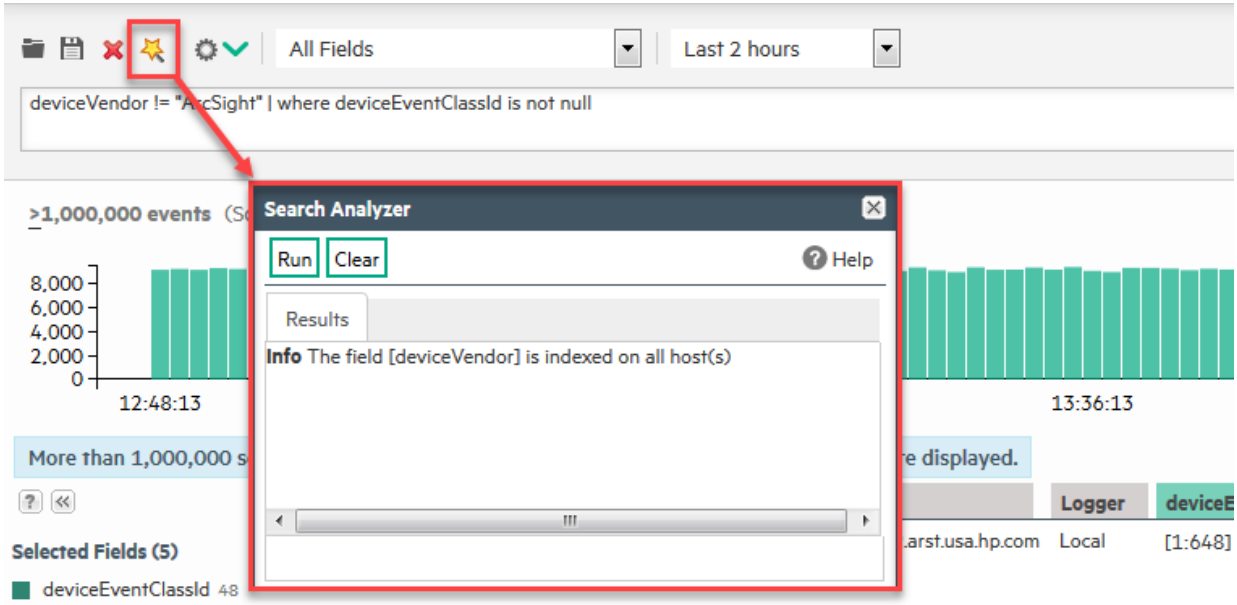


検索アナライザー

クエリのパフォーマンスは、システムの負荷、検索対象データのサイズ、クエリに含まれるインデックス作成されたフィールドまたはインデックス作成されていないフィールド、クエリの複雑さ (多数の条件、ワイルドカード文字、ネスト) などによって変わります。

検索アナライザーツールでは、クエリを分析して、クエリに含まれるいずれかのフィールドが、指定された時間範囲に対してインデックス作成されておらず、クエリのパフォーマンスに影響を与えるかどうかが判定されます。

このツールは、クエリの実行に予想よりも時間がかかる場合など、必要に応じて実行できます。検索アナライザーは、クエリを実行した後や、検索ビルダーを使用してクエリを作成している間に使用できます。検索アナライザーツールにアクセスするには、  をクリックします。



クエリにおけるインデックス作成されたフィールドに対するパフォーマンスの最適化

検索クエリにインデックス作成されたフィールドが含まれていても、次の状況ではパフォーマンス向上が実感されない可能性があります。

- インデックスが作成されたフィールドとインデックスが作成されていないフィールドを1つのクエリに含めた場合。この場合は、クエリで最も頻繁に使用されるフィールドを明確にし、それらすべてのフィールドについてインデックスを作成することをお勧めします。「検索フィールドの色について」(70ページ)を参照すると、クエリ内でインデックス作成されたフィールドとインデックス作成されていないフィールドを識別するのに役立ちます。
- 大量のデータから出現頻度の少ない値を探す検索で、スーパーインデックスが作成されていないフィールドか、=以外のフィールド演算子を含めた場合、スーパーインデックスが作成されたフィールドの期待されるパフォーマンス向上が得られない可能性があります。出現頻度の少ない値を検索する際に最も高速に結果を得るには、「出現頻度の少ないフィールド値の検索」(117ページ)の推奨事項に従ってください。
- 現在インデックスが作成されているフィールド (クエリに含まれる) の、インデックスが作成され

ていなかった時間範囲のデータに対して検索を実行した場合。

たとえば、8月13日の午後2時00分に"port"フィールドのインデックスを作成し、8月14日の午後1時00分に検索を実行して、ポート80を含み、8月11日から8月12日の間に発生したイベントを検索したとします。"port"フィールドは、8月11日から12日の間にインデックスが作成されていないため、クエリの動作が低速になります。

- Loggerでインデックス作成中のフィールドを検索クエリに含めた場合。この場合は、フィールドをインデックスに追加してから、検索クエリでフィールドを使用するまでに、少し待ちます。
- インデックス作成されたフィールドを含むクエリを、アーカイブされたイベントに対して実行した場合、データがアーカイブされていないときと比べてクエリの実行が低速になります。これは、Loggerのインデックスデータはイベントとともにアーカイブされないためです。アーカイブされたイベントの検索速度を向上させるには、インデックスを作成します。詳細については、「アーカイブされたイベントのインデックス付け」(441ページ)を参照してください。

正規表現ヘルパーツール

正規表現ヘルパーツールを使用すると、rexパイプライン演算子とともに使用して、関心のあるフィールドをイベントから抽出することができる正規表現を作成できます(正規表現の詳細については、「クエリの検索演算子部分」(79ページ)または「rex演算子の使用」(604ページ)を参照してください。)このツールは、rex演算子用の正規表現を作成する作業を単純化するだけでなく、正規表現を効率的で誤りのないものにすることもできます。

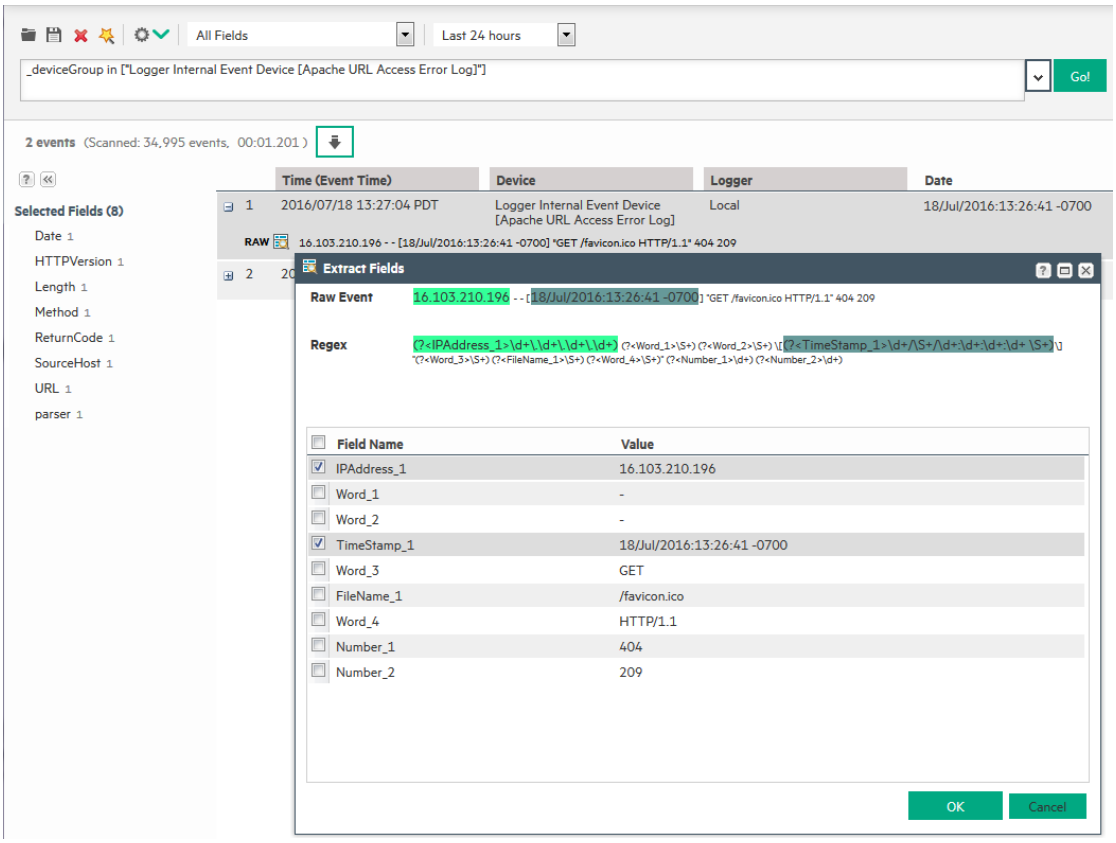
このツールは、非CEFイベント (構造化されていないデータ) に対してのみ使用でき、raw syslogイベントを解釈してフィールドに分割し、リストとして表示します。クエリのrex式に含めるフィールドを選択します。選択されたフィールドは、rex式として検索クエリに自動的に挿入されます。

このツールを使用するには、以下の手順を実行する必要があります。

注: これらの手順は、手順の後にある図にも示してあります。

1. 関心のあるイベントを探す検索クエリを入力します検索実行の詳細については、「イベントの検索」(106ページ)を参照してください。
2. さらに分析するsyslogイベントを特定します。たとえば、図の中のイベント#7がさらに分析するイベントです。
3. 特定したイベントのアイコン (一番左の列) をクリックして展開し、そのrawイベントを表示します。
4. アイコン (**RAW**という単語の横) をクリックし、正規表現ヘルパーツールを起動します。
5. 抽出するフィールドを選択します。

6. **[OK]** をクリックします。



選択したフィールドに関係するrex式が検索クエリボックスに自動的に入力されます。この例では、イベントからIPアドレスを抽出します。そのため、IPAddress_1フィールドが正規表現ヘルパーツールで選択されています(正規表現ヘルパーツールは、あるデータ型がイベント中に複数回現れる場合、インクリメンタルなラベルを割り当てます)。たとえば、IPアドレスには、IPAddress_1、IPAddress_2、IPAddress_3などのラベルが割り当てられます)。

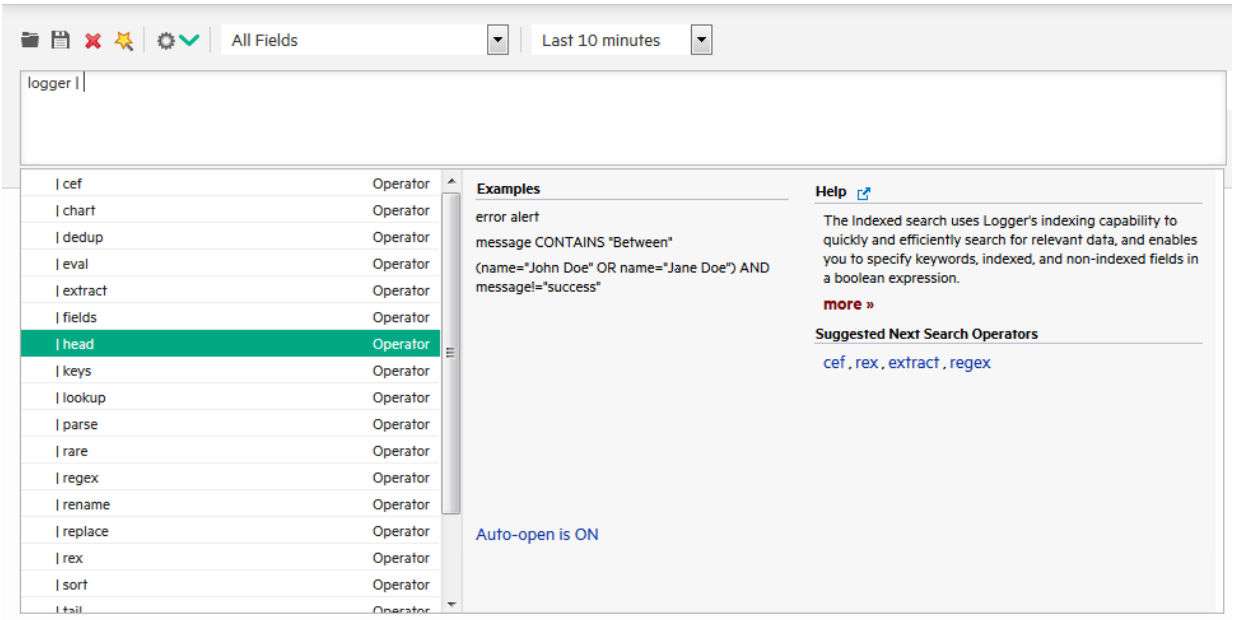
Ipアドレスを選択して **[OK]** をクリックすると、次の例に示すように、それらのIPアドレスの正規表現を含むrex式が [検索] テキストボックスに表示されます。

```
_deviceGroup in ["Logger Internal Event Device [Apache URL Access Error
Log]"] | rex "(?<IPAddress_1>\d+\.\d+\.\d+\.\d+) \S+ \S+ \[(?<TimeStamp_
1>\d+/\S+/\d+:\d+:\d+:\d+ \S+)\.*"
```

この時点で、パイプライン演算子をこのクエリに追加してグラフを作成したり、上位5個のIPアドレスを特定したりすることができます。次の例では、上のクエリを変更して、上位のIPアドレスを特定します。

```
_deviceGroup in ["Logger Internal Event Device [Apache URL Access Error
Log]"] | rex "(?<IPAddress_1>\d+\.\d+\.\d+\.\d+) \S+ \S+ \[(?<TimeStamp_
1>\d+/\S+/\d+:\d+:\d+:\d+ \S+)\.*"| top IPAddress_1
```

検索ヘルパー



検索ヘルパーは、検索専用のユーティリティであり、現在検索テキストボックスに入力されているクエリに基づいて、該当する情報を自動的に表示します。

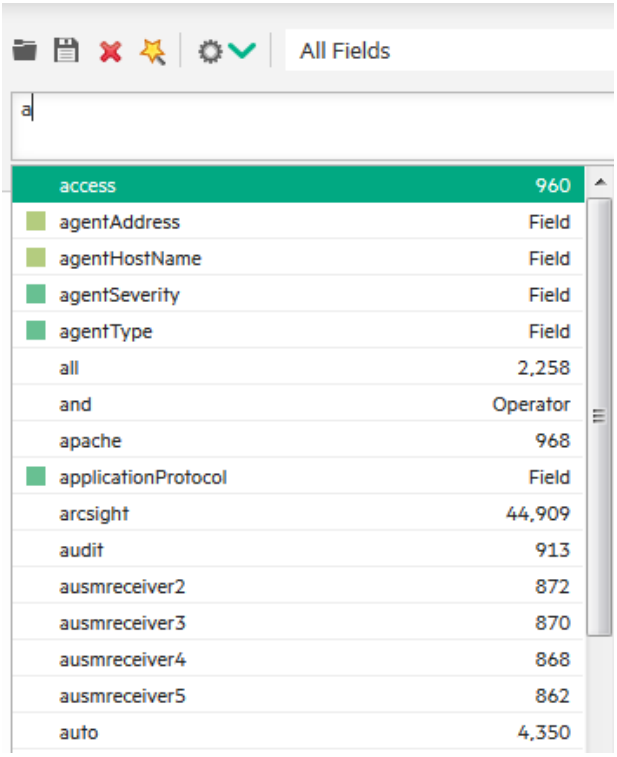
検索ヘルパーはデフォルトで有効です。検索ヘルパーに自動的に表示しないようにするには、[**自動オープンON (Auto-open is ON)**] リンク (検索ヘルパーのウィンドウ内) をクリックします。リンクが [**自動オープンOFF**] に変わります。オフにした後に検索ヘルパーにアクセスするには、[検索] テキストボックスの右の下矢印ボタンをクリックします。

検索ヘルパーには、自動補完検索機能、検索履歴、検索演算子履歴、ヘルプシステムへのリンク、および次の検索演算子候補が表示されます。

自動補完検索

自動補完機能は、検索ボックスに現在入力されているテキストに基づいて、全文キーワードとフィールド提案を提供します。入力候補により、キーワード、フィールド、フィールド値、検索演算子、メタデータの項を入力しないで、リストから選択できるため、クエリ式をより素早く作成できます。

入力を開始すると、次の図に示すように、入力候補のリストに多くの種類のエントリが表示されます。



入力したテキストが全文キーワードとスキーマフィールドの両方に含まれている場合、そのすべてが提案リストに表示されます。

「|」(パイプライン文字)を入力すると、Loggerで使用可能な演算子のリストが表示されます。

全文キーワードの提案は、Loggerですでにインデックス作成されている全文キーワードから取得されます。

Loggerスキーマフィールドがインデックス作成済み、スーパーインデックス作成済み、またはインデックス作成可能な場合、フィールド名の左側にインデックス状態に合わせたアイコンが表示されます。詳細については、「検索フィールドの色について」(70ページ)を参照してください。

注: システム定義フィールドは、自動補完でフィールドとして使用できません。システム定義フィールドおよびLogger検索の詳細については、「検索クエリの作成について」(110ページ)および「検索結果のその他のフィールド」(127ページ)を参照してください。

全文キーワードとフィールド値は、各提案の横にカウントが表示されます。これは、Loggerに保存されているキーワードまたはフィールド値のインスタンス数を示します。

カウントは、フィールドに保存された値の数を表します。カウントは、多数の要因に依存し、正確でない可能性があります。クエリに一致するイベントの数を示しているわけではありませ

ん。イベント一致の数は、クエリの時間範囲、検索制約、検索演算子など、多数の要因で決まります。

注: 自動補完の提案とカウントは、ローカルシステムのみに保存されているデータを基に計算されます。Loggerが再開すると、カウントがリセットされます。ピアデータは含まれていません。

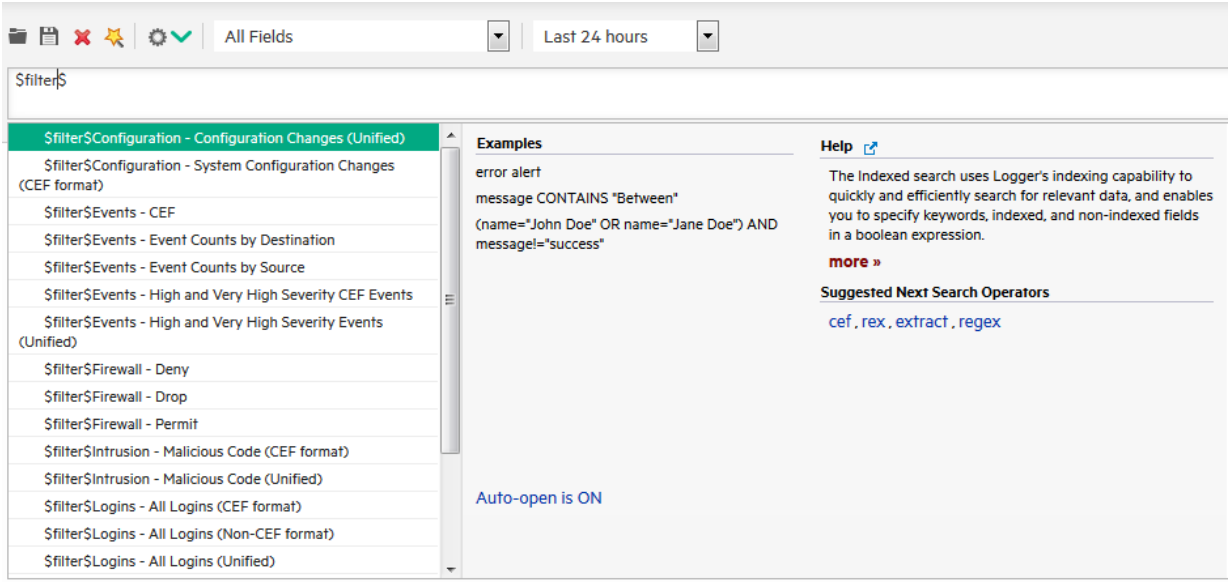
検索グループフィルター (ストレージグループとデバイスグループに対する権限を制限します) は、自動補完リストには適用されません。そのため、リストには、ユーザーが権限を持っていないストレージグループやデバイスグループのイベントのキーワード、フィールド、フィールド値、カウントが含まれています。

アーカイブをLoggerにロードしても、自動補完リストには、イベントがアーカイブされる前に使用できた全文キーワードやフィールド値は表示されません。このようになるのは、サマリーデータがイベントデータとともにアーカイブされないため、イベントデータをアーカイブからロードしたときに、アーカイブデータがサマリーに含まれていないためです。

自動補完を通じてフィルターと保存された検索を開く

Logger 6.0では、自動補完定数`$filter$`と`$ss$`が追加されており、検索ボックスから直接フィルターと保存された検索を開くことができます。

検索ボックスに`$filter$`と入力すると、使用可能なフィルターが自動補完に表示されます (フィルターにはクエリのみが含まれます)。提案をクリックして選択するか、フィルター名の入力を続けて選択肢を絞り込みます。自動補完からフィルターを選択すると、Loggerにより検索ボックスの内容がフィルター定義で置き換えられます。



検索ボックスに`$ss$`と入力すると、使用可能な保存された検索が自動補完に表示されます(保存された検索には、クエリ、開始日時、終了日時、ローカルのみなどが含まれます)。

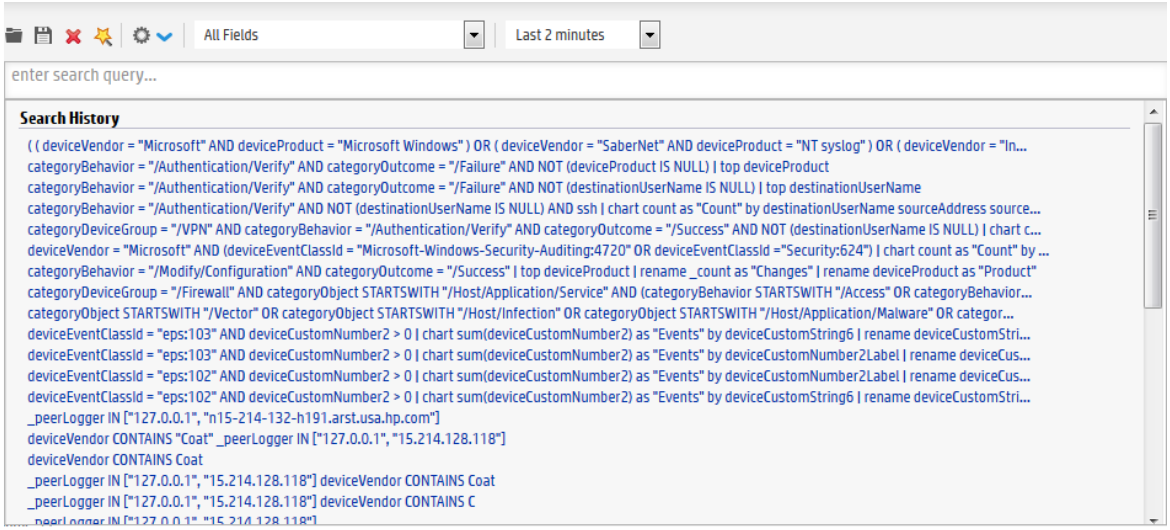
提案をクリックして選択するか、保存された検索の名前の入力を続けて選択肢を絞り込みます。自動補完から保存された検索を選択すると、Loggerにより検索ボックスの内容が保存された検索の定義で置き換えられます。

自動補完提案を使用するには

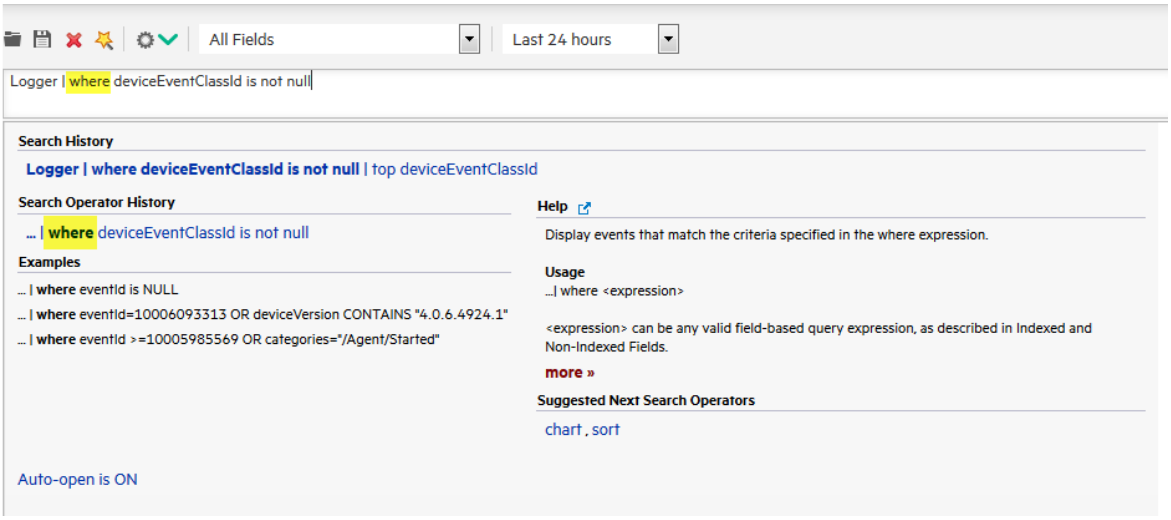
1. 検索の自動補完リストから、提案をクリックして、検索ボックスに移動します。
2. **[実行!]** をクリックしてその検索を実行するか、入力を続けて検索をさらに絞り込みます。

検索履歴および検索演算子の履歴

[検索履歴 (Search History)] には、現在入力されている検索に一致する、最近実行したクエリが表示されます。最近のクエリを再度実行するには、クエリをクリックします。検索履歴を表示するには、検索の入力を開始するか、**[実行!]** ボタンの横にある下矢印をクリックします。



[検索演算子履歴 (Search Operator History)] には、現在 [検索] テキストボックスに入力されている検索演算子とともに以前使用したフィールドが表示されます。検索演算子履歴は、このシステム上で検索を実行するために、現在入力されている演算子を以前使用したことがある場合にのみ表示されます。演算子をクリックして検索に追加します。



例、使用法、次の検索演算子候補、およびヘルプ

[例 (Examples)] セクションには、[検索] テキストボックスに最後に入力したクエリ演算子に関係する例がリスト表示されます。

[使用法 (Usage)] セクションには、検索演算子の構文が表示されます。

[次の検索演算子候補 (Suggested Next Search Operators)] セクションには、現在入力されているクエリに続くことが多い演算子のリストが表示されます。たとえば、`logger |`と入力すると、それに続くことが多い演算子は`rex`、`extract`、または`regex`です。表示されるいずれかの演算子を選択して、現在検索テキストボックスに入力されているクエリに自動的に追加できます。このリストにより、次に考えられる演算子を推測したり、手動で入力したりする必要がなくなります。

[ヘルプ (Help)] セクションには、現在 [検索] テキストボックスに入力されているクエリに最後に入力した演算子のコンテキスト依存のヘルプが表示されます。また、アイコンをクリックすると、Loggerのオンラインヘルプが表示されます。

イベントの検索

このセクションのトピックでは、Loggerでのイベントの検索方法について説明します。

権限と必須条件

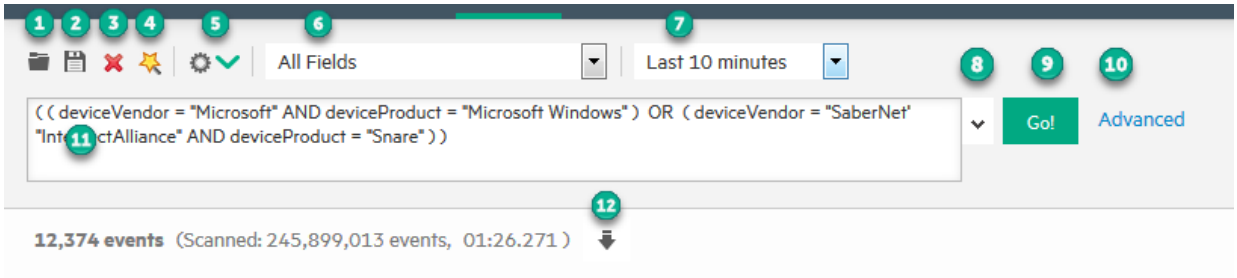
Loggerの検索ユーザーに対して、以下のユーザーグループ権限を有効にします。

- デフォルトロガー検索グループ > 検索 > イベント検索 (ローカル検索のみ)
- デフォルトロガー検索グループ > 検索 > リモートピアのイベント検索 (分散検索用)
- デフォルトLogger権限 > ピア > 登録されたピアを表示 (ピアを参照する場合)

場合により、その他の権限も適用されます。詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

検索の実行

検索ページに表示されるオプションを使用すると、検索クエリの作成と実行に役立ちます。



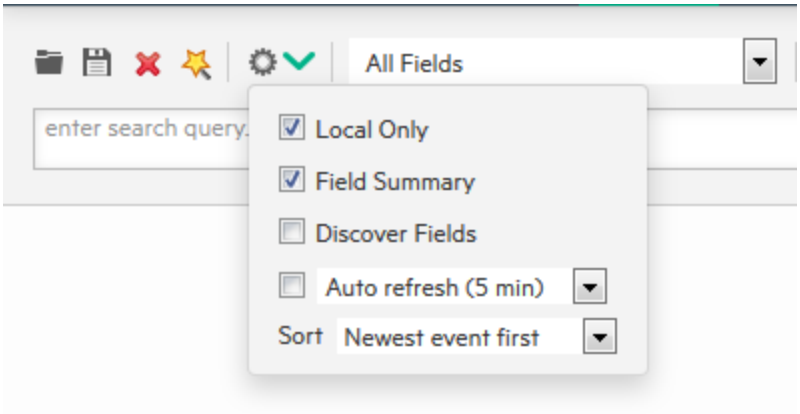
検索バーの凡例

オプション	説明	オプション	説明
1	保存された検索またはフィルターのロード	7	時間範囲の設定
2	クエリの保存	8	検索履歴を開く
3	クエリのクリア	9	検索の開始またはキャンセル
4	検索アナライザーを開く	10	検索の詳細設定ビルダーを開く
5	検索オプションの更新	11	クエリの入力
6	フィールドセットの選択	12	検索結果のエクスポート

検索ページに表示されるオプションに加え、[設定] > [検索オプション] ページを使用すると、それぞれの環境に合わせて検索操作を調整できます。「グローバル検索オプション」(349ページ)を参照してください。同時検索およびアクティブな検索については、「同時検索」(111ページ)を参照してください。

Loggerでイベントを検索するには

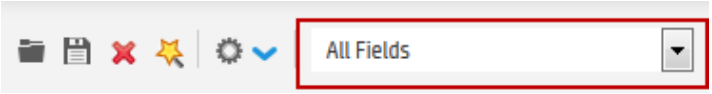
1. [**分析**] メニューを開き、[**検索**] をクリックします。
2. 下矢印をクリックして検索オプションを表示および調整します。デフォルト値を使用するか、要件に合わせて変更します。



- **ローカルのみ (Local Only):** このオプションは、システムにピアが設定されている場合にのみ表示されます。[ローカルのみ] はデフォルトでオンになっています。検索にピアを含める場合は、[ローカルのみ] チェックボックスをオフにします。このチェックボックスが表示されない場合は、Loggerにピアが設定されていません。詳細については、「ピアの検索 (分散検索)」(115ページ) を参照してください。
- **フィールドサマリー (Field Summary):** 表示されているイベントの選択されたCEFフィールドが一覧表示されます。[選択したフィールド] リストにデフォルトで含まれるフィールドは、deviceEventClassId、deviceProduct、deviceVendor、deviceVersion、およびnameです。このリストは、要件に合わせて変更できます (を参照)。このオプションを選択すると、[フィールドを検出] オプションが有効化されます。[フィールドサマリー] オプションと [フィールドを検出] オプションの詳細については、「フィールドサマリーパネル」(132ページ) を参照してください。
- **フィールドを検出 (Discover Fields):** rawイベント中に見つかった非CEFフィールドが一覧表示されます。このオプションは、[フィールドサマリー] がオンになっている場合にのみ考慮されます。
- **自動リフレッシュ (Auto Refresh):** デフォルトで、検索結果は自動的に更新されず、10分後 (デフォルト値)、または設定された有効期限に到達したときに、期限切れになります (「同時検索」(111ページ) を参照)。選択した検索で検索結果が自動更新されるようにするには、このオプションをオンにします。更新間隔としては、30秒、60秒、2分、5分、15分から選択できます。
- **ソート (Sort):** 検索結果の表示方法に応じて、[古いイベント順] または [新しいイベント順] を選択します。

3. **フィールドセット:** デフォルトでは、すべてのフィールド (All Fields) が検索結果に表示されます。しかし、別の定義済みフィールドセットを選択したり、カスタムフィールドセットを指定

したりすることができます。詳細については、「フィールドセット」(82ページ)を参照してください。



4. **時間範囲:** デフォルトでは、[10分前から現在まで(Last 10 minutes)]に受信したデータに対してクエリが実行されます。ドロップダウンリストをクリックして別の定義済み時間範囲を選択するか、カスタム時間範囲を指定します。詳細については、「時間範囲」(79ページ)を参照してください。

5. 次の方法を1つまたは複数使用して、[検索]テキストボックスでクエリ式を指定します。

   注: クエリ式を作成する前に、「キーワード検索 (フルテキスト検索)」(72ページ)、「フィールドベースの検索」(73ページ)、「出現頻度の少ないフィールド値の検索」(117ページ)で手順、例外、無効な文字の一覧を参照してください。

   a. [検索]テキストボックスにクエリ式を入力します。適用可能な演算子の一覧など、クエリ式の作成については、「検索クエリの要素」(71ページ)を参照してください。
   b. クエリを入力するときには、Loggerの検索ヘルパーにより、提案、考えられる一致、適用される演算子が自動的に提供されることで、素早くクエリ式を構築できます。詳細については、「検索ヘルパー」(102ページ)を参照してください。
   c. 検索クエリに各種の要素を含めるには、以下のガイドラインに従ってください。
      - Loggerスキーマのフィールドの完全な一覧については、「フィールドベースのインデックス付け」(153ページ)を参照してください。
      - メタデータ項 (`_storageGroup`、`_deviceGroup`、`_peerLogger`)

        制約項と演算子のドロップダウンリストを取得するには、「_s」(ストレージグループの場合)、「_d」(デバイスグループの場合)または「_p」(Loggerの場合)を[検索]テキストボックスに入力します。
      - 正規表現項 (`|REGEX=`)

        注: クエリ式に、検索を制約する複数のデバイスグループとストレージグループが含まれている場合は、`_storageGroup IN ["SGA", "SGB"]`のように、グループ名を必ず角括弧で囲みます。

      - 検索ビルダーツールを使用するには[**詳細**]をクリックします(詳細については、「検索の詳細設定ビルダーの使用」(94ページ)を参照してください)。また、このオプションを使用して、検索を制限するデバイスグループ、ストレージグループ、Loggerを指定します。
   d. 保存されたフィルター、システムフィルター、保存された検索をロードするには、アイコンをクリックします。表示されるリストからフィルターまたは保存されている検索を選択

し、**[読み込み + クローズ]** をクリックします。

詳細については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) および「システムフィルター/事前定義フィルター」(145ページ) を参照してください。

6. オプションで、新しいブラウザータブで同時検索を開始できます。「同時検索」(111ページ) を参照してください。

検索クエリの作成について

検索クエリを作成する際には、以下の点を考慮してください。

- `Time`、`Device`、`Logger`、`parser`、`source`、`sourceType`などのシステム定義フィールド内の値は、キーワード検索でもフィールドベースの検索でも検索できません。これらはシステム定義フィールドで、rawイベントテキスト内には存在しません。そのため、これらのフィールドのデータを検索しても結果は返されません。

  parserフィールドはパーサーの名前だけを含み、検索できません。しかし、パーサーは関連付けられたソースタイプに基づいてフィールドを定義し、これらのフィールドは検索可能です。詳細については、「検索結果のその他のフィールド」(127ページ) を参照してください。

  注: 検索可能でないフィールドは、検索結果内でマウスを重ねても、強調表示されず、自動補完検索でフィールドとしてマークされません。詳細は、「検索結果での検索の絞り込み」(128ページ) および「自動補完検索」(102ページ) を参照してください。

- Null値は検索結果に含まれません。たとえば、イベントデータに対して`NOT deviceCustomString1=bar`のような検索を行う場合、「deviceCustomString1が "bar" ではない」という条件に一致する検索結果が返されますが、deviceCustomString1の値がNullのイベントは返されません。Null値は、`<field> IS NOT NULL`または`<field> IS NULL`を使用して明示的に指定する必要があります。

  注: NOT検索条件にNull値を含めるようにLoggerを設定するには、検索オプション **[NOT演算子の結果にNULLフィールド値を含める]** を [はい] に設定します。詳細については、「グローバル検索オプション」(349ページ) を参照してください。

- トークン化されている文字列内に含まれるデータは、検索できません。検索可能なキーワードは、rawテキスト文字列をトークンと呼ばれる検索可能な単位に解析するために使用される一連の区切り文字によって特定されます。これらの区切り文字は、**[設定] > [検索オプション]** ページで制御します。
  - Loggerには、全文 (キーワード) 検索で使用するプライマリ区切り文字として、スペース、タブ、改行、コンマ、セミコロン、(、)、[、]、{、}、"、|、*が含まれています。**[設定] > [検索オプション]** 画面で、これらのプライマリ区切り文字のみが [はい] に設定されていて、rawイベントに`dmz:10.9.9.9/20`という文字列が含まれている場合、この文字列全体が1つの検索可能なキーワードになります。

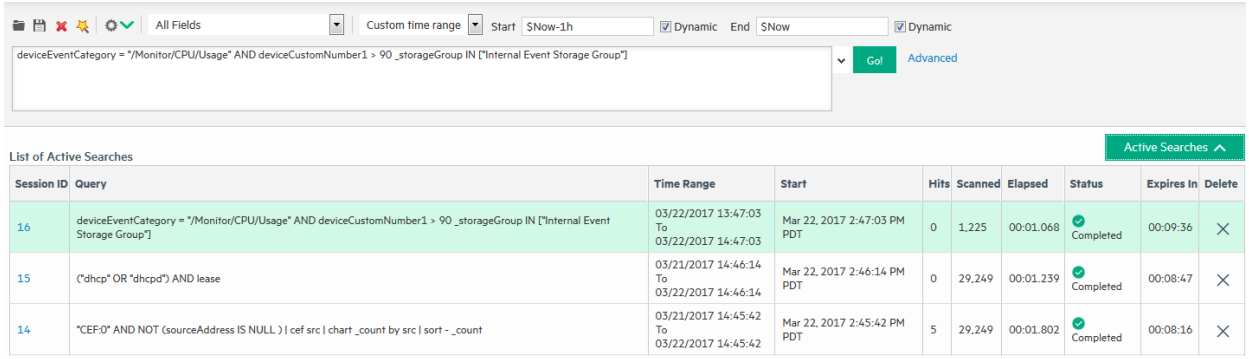
- **[設定] > [検索オプション]** 画面では、検索時にセカンダリ区切り文字の使用を有効にすることもできます。セカンダリ区切り文字も [はい] に設定されている場合、=、.、:、/、\、@、-、?、#、&、_、>、<という区切り文字によって文字列がさらにトークン化されます。そのため、rawイベントに`dmz:10.9.9.9/20`の文字列が含まれている場合、このイベントの検索可能なキーワードは、`dmz`、`10`、`9`、および`20`になります。

  プライマリおよびセカンダリ区切り文字の設定の詳細については、「グローバル検索オプション」(349ページ) を参照してください。

同時検索

Loggerでは、複数のブラウザータブで同時に複数の検索を実行できるようになりました。

各ユーザーは、検索の期限が切れる前であればいつでも、[検索] ホームページの**アクティブな検索リスト (List of Active Searches)**を使用して、検索の表示、再開、削除を行うことができます。セッションIDをクリックすると、新しいブラウザーウィンドウが開いて、新しい検索のインスタンスが開始されます。「アクティブな検索リストの使用」(112ページ) を参照してください。



最大同時検索数

実際に実行できる同時検索数は、システム負荷、検索のサイズ、その他の要因に依存します。

- Loggerでは、実行中の検索または終了した検索数のデフォルト値 ([設定] > [検索オプション] ページで設定) は**0** (無制限) に設定されていますが、Loggerの管理者は**1** (同時検索なし) から**1000**の間でこの値を調整できます。
- この値により、ユーザーではなく、Loggerによるメモリ内の検索の合計数 (実行中の検索または終了した検索) が制限されます。

  例: Loggerの最大同時検索数が10に設定されている場合、ユーザー**A**が6つの検索を実行していて、いずれかの検索が有効期限切れになる前にユーザー**B**が5つ以上の同時検索を実行しようとすると、エラーが返されます。

有効期限

Loggerが検索結果を削除する前にメモリ内に保持する時間も、検索能力に影響する可能性があります。検索を実行するたびに、Loggerのストレージ容量とCPU帯域幅が消費されます。

- このため、検索のデフォルトの有効期限は**10分**になっています。Loggerの管理者は、この時間を**1～60**分の範囲で調整できます。
- セッションIDをクリックすると、新しいタブに検索結果が表示され、有効期限がリセットされます。検索のためにページ番号リンクを使用する(表示ページ間を移動する)場合にも、有効期限がリセットされます。
- 有効期限は、同時検索の結果と単独の検索結果の両方に影響します。

その他の考慮事項

同時検索を実行する際には、以下に注意してください。

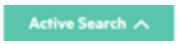
- 最大検索数と有効期限は、[設定] > [検索] > [**検索オプション**] ページで設定します。このページを使用するには、管理者権限が必要です。「同時検索オプション」(353ページ)を参照してください。
- 管理者は、[設定] > [検索] > [**実行中の検索**] ページで、継続中の検索の表示と削除を行うことができます。「実行中の検索」(356ページ)を参照してください。
- ダッシュボードの検索(実行中の場合)は、検索の最大数に含まれますが、アクティブな検索リストには表示されません。(ダッシュボードの検索は、完了後65秒で有効期限切れになります。)ダッシュボードの検索が問題になる場合、管理者はダッシュボードページからダッシュボードの更新をキャンセルできます。
- 検索の最大数の制限は、保存された検索やスケジュールされた検索には適用されません。
- 検索の最大数の制限は、レポートツールから実行された検索およびクエリには適用されません。ただし、検索クエリの実行と同時にレポートを実行すると、パフォーマンスに影響する可能性が高くなります。

アクティブな検索リストの使用

アクティブな検索リストには、実行中および完了した検索に関する情報が表示されます。設定された有効期限を過ぎた検索や、再度開かれた検索は表示されません。

注: 自動リフレッシュが有効になっている場合は、指定した間隔で検索結果が再生成されます。他のレポートには影響しません。「検索結果の自動更新」(130ページ)を参照してください。

アクティブな検索リストを開く

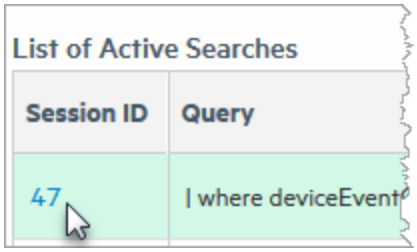
1. 検索ホームページで、検索を開始します。「検索の実行」(107ページ) を参照してください。
2. 

[アクティブな検索 (Active Search)] をクリックします。実行中の検索と完了した検索のリストが表示されます。

ヒント: 実行中のアクティブな検索が存在しない場合、アクティブな検索リストは使用できません。

アクティブな検索を再度開く

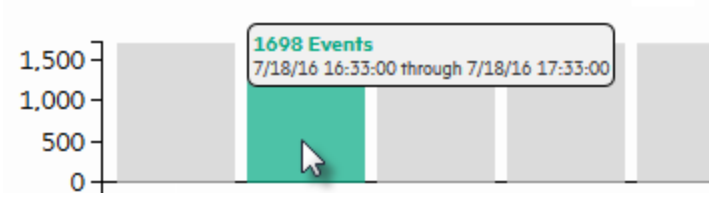
1. 検索がアクティブな (まだ期限切れになっていない) 状態で、**[アクティブな検索 (Active Search)]** をクリックします。
2. 再度開く検索の**セッションID**をクリックします。



検索結果が新しいブラウザータブに表示されます。

アクティブな検索の有効期限をリセットする

1. 検索がアクティブな (まだ期限切れになっていない) 状態で、次のいずれかの方法で検索を操作します。
   - 検索のヒストグラムのバーをクリックします。「ヒストグラム」(125ページ) を参照してください。

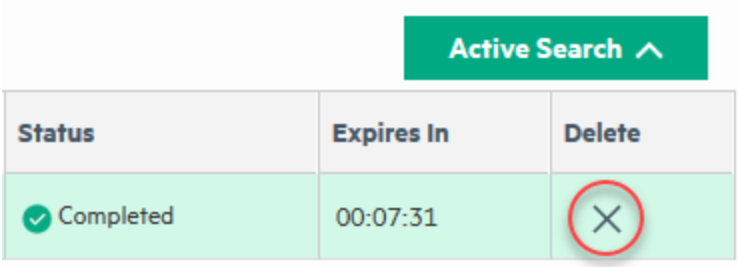


   - 検索の右下にある検索ページツールを使用して、レポートのページを移動します。「検索結果の表示の調整」(123ページ) を参照してください。

検索の有効期限がリセットされます。

アクティブな検索を削除する

1. 検索がアクティブな (まだ期限切れになっていない) 状態で、[**アクティブな検索**] をクリックします。
2. アクティブな検索リストで、削除するレポートの右端にある [**X**] をクリックします。クリックした検索が削除されます。



未保存の検索がある場合、ブラウザーを閉じるか、ログアウトすると、これらの検索も削除されます。

同時検索の実行

Loggerのメモリ内に実行中の検索や期限切れになっていない検索が存在する場合は、アクティブな検索リストを表示できます。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

1. 同時検索を有効化および設定するには
   - デフォルトシステム管理グループ
2. 同時検索を実行するには
   - デフォルトLogger検索グループ

「Loggerのユーザー権限の設定」(546ページ) を参照してください。

ヒント: お使いのLoggerの検索制限および有効期限については、管理者にお問い合わせください。

2つ以上の同時検索を実行するには

1. [分析] > [**検索**] のメインページで、検索を開始します。「検索の実行」(107ページ) を参照してください。
2. 最初の検索が実行されている間に、新しいブラウザータブを開き、同じLoggerにログインします。

3. 次の検索文字列を入力し、2つ目の検索を開始します。
4. さらに多くの同時検索を実行するには (お使いのLoggerで指定された最大同時検索数まで)、ステップ2～3を繰り返します。

ピアの検索 (分散検索)

検索クエリを実行するとき、デフォルトでは、ローカルなLoggerのみで一致するイベントが検索されます。ただし、クエリを指定する際に、ピアのLoggerで検索を実行するオプションを選択できます。

前提条件

ピアの検索を実行して検索結果を表示するには、以下のグループと権限が必要です。

ユーザーがピアの検索を実行して検索結果を表示するには、ユーザーが、ここに示す許可を持つ以下のユーザーグループに属している必要があります。

- 「リモートピアのイベント検索」が有効になっているLogger検索グループ。
- 「登録されたピアを表示」が有効になっているLogger権限グループ。

ピアにまたがって検索する場合は、以下のガイドラインに従ってください。

- 検索するピアのLoggerを指定します (「制約」(87ページ) を参照)。
- Loggerは、同じ検索で最大100のピアの検索をサポートします。
- 最適な検索パフォーマンスと機能を実現するには、すべてのピアで最新バージョンのLoggerが使用されている必要があります。複数のピアを大将とする検索は、最も古いバージョンのピアの機能によって制限されます。
  - 演算子が対応していないピアのバージョンがある場合、そのピアではクエリは実行されません。
  - 古いバージョンのピアは、そのバージョンのパフォーマンスで動作するため、これらのピアの検索結果が返されるまでに時間がかかります。
- 非パイプライン検索で最適なパフォーマンスを実現するには、`regex`、`rex`、`parse`、`keys`、`transaction`、`extract`、または`lookup`検索演算子をクエリに含めないようにします。
- ピアのLoggerのストレージグループ名またはデバイスグループ名が同じでない場合、検索クエリ処理は、それらのピア上でそれらのグループのイベントの検索を省略します。
- カスタムスキーマフィールドがLoggerスキーマに存在する場合、それらのフィールドはすべてのピアに存在している必要があります。それらのフィールドを含む検索クエリは実行されず (複数のピアにまたがって実行した場合)、エラーが返されます。「スキーマへのフィールドの追加」(461ページ) を参照してください。
- 検索処理の途中でLoggerが使用不能になると、エラーメッセージが表示されます。表示されるメッセージは、検出されたエラーによって変わります。考えられる原因として最も可能

性が高いのは、ネットワークの問題やピアのダウンです。ピアリング関係に問題があることが原因の場合もあります。問題が修正された後でも、進行中だった検索に対するエラーメッセージが表示される可能性があります。しかし、新しい分散検索を実行したときにメッセージが表示されなくなる場合は、そのようなメッセージを無視してかまいません。ピアの詳細については、「ピアノード」(483ページ)を参照してください。

- 検索ヘッドを使用すると、検索演算子 (特に、chart、sort、topなどのアグリゲーション演算子) を使用する検索でピアの検索を高速化できます。検索ヘッドで実行するクエリを作成する際に最適な検索パフォーマンスを実現するには、クエリで検索対象のすべてのピアを指定し、ローカルのLoggerを除外します。「検索ヘッドのセットアップによるピアの検索の高速化」(30ページ)を参照してください。

  注: 検索ヘッドを使用することによるピアの検索の高速化は、ユーザーインターフェイス経由で実行された検索にのみ適用されます。検索ヘッドを使用しても、スケジュールされた検索やLogger Webサービス経由で実行された検索は高速化されません。

複数のピアを対象に検索する場合のクエリの例:

5つのフィールドをソートする検索:

```
_peerLogger IN [“peer1”, “peer2”, …] | sort deviceEventCategory eventId
deviceCustomNumber1 deviceCustomNumber2 deviceCustomNumber3
```

フィールド抽出を使用する検索:

```
_peerLogger IN [“peer1”, “peer2”, …] | rex "(?<src_ip>\d{1,3}\.\d{1,3}\.\d
{1,3}\.\d{1,3})"
```

変数を評価する検索:

```
_peerLogger IN [“peer1”, “peer2”, …] | eval (int)urllength=len(requestUrl)
|sort urllength
```

結果をグループ化しトップ50リストとしてカウントする検索:

```
_peerLogger IN [“peer1”, “peer2”, …] | and priority > 0 | top 50 name
```

長いURLを含むイベントの検索:

```
_peerLogger IN [“peer1”, “peer2”, …] | eval n=len(requestUrl) | where n =
"1023"
```

検索パフォーマンスの調整

検索パフォーマンスは多数の要因に依存し、クエリごとに異なります。検索パフォーマンスに影響を与える可能性がある要因の一部を以下に示します。検索パフォーマンスを最適化するには、以下の推奨事項に従ってください。

- 一般的でないフィールド値を検索する場合には、スーパーインデックスを使用して検索が必要なデータの範囲を狭めます (「出現頻度の少ないフィールド値の検索」(117ページ)を参照)。
- イベント中で発生するすべてのフィールドについて、フィールドベースのインデックス作成を有効にします。イベントのインデックスを作成すると、Loggerは素早く効率的に該当するデータを検索できます。デフォルトでは、推奨されるフィールドセットはLogger上でインデックス作成されます。「フィールドベースのインデックスにフィールドを追加するには」(347ページ)に従って、他のフィールドの追加が必要になる可能性があります。
- クエリで数百万個のイベントのスキャンが必要になるような時間範囲を指定することは避けます。
- 特定のストレージグループとピアに検索を制限します。
- クエリを実行する必要があるときは、スケジュールジョブ、多数の受信イベント、複数のレポート実行など、システム上の他の負荷を減らします。
- クエリを実行する前に、クエリを実行するすべてのLoggerがクエリの機能をサポートしていることを確認します。

検索パフォーマンス改善の詳細については、『Logger Best Practices』ガイドを参照してください。

出現頻度の少ないフィールド値の検索

一般的なIPアドレス、ホスト名、ユーザー名のフィールドについて、出現頻度の少ないフィールド値を素早く検索できるようにするため、Loggerでは、受信した新しいデータについてスーパーインデックスを作成します。スーパーインデックスフィールドを活用するように作成された検索は、ヒットがないかどうかを非常に高速に通知し、ヒット数が少ない場合には通常の検索よりも高速に結果を返します。このため、スーパーインデックスは、大量のデータから出現頻度の少ない値を素早く検索する場合に最適です。詳細については、「スーパーインデックス作成」(155ページ)を参照してください。

注: スーパーインデックスは、受信した新しいデータに対して作成されるため、Logger 5.5以降で収集されたデータのみに適用されます。以前のバージョンのLoggerからのアップグレードにより引き継がれたデータについては、スーパーインデックスが作成されないため、検索速度の向上は見られません。

スーパーインデックスフィールドを使用した検索速度の向上

スーパーインデックスを活用し、検索速度を最大限に速めるには、`sourceAddress=192.0.2.0`のように等号 (=) 検索を実行し、クエリのインデックス検索部分を、次の表に示すスーパーインデックスが作成されたフィールド内の一般的でない値を探すように作成します。

スーパーインデックスフィールド

deviceEventClassId	deviceProduct	deviceVendor	destinationHostName
destinationPort	destinationAddress	destinationUserId	destinationUserName
deviceAddress	deviceHostName	sourceHostName	sourcePort
sourceAddress	sourceUserId	sourceUserName	

注: 「フィールドベースのインデックス付け」(153ページ) で説明する、インデックス作成されたフィールドと異なり、スーパーインデックスが作成されたフィールドのリストを追加することはできません。

検索パフォーマンスを高めるには、スーパーインデックスが作成されたフィールドを必ず=演算子を使用して検索し、スーパーインデックスが作成されていないフィールドとのANDのみでつなげます。スーパーインデックスは、クエリ式のインデックス検索部分で等号 (=) 演算子を使用した検索を高速化します。クエリのインデックス検索部分で、大なり不等号 (>)、小なり不等号 (<)、不等号 (!=)、その他の演算子を使用した検索については、パフォーマンスの影響はありません。Loggerは、全文検索をサポートしていますが、スーパーインデックスが作成されていないフィールドに対する検索と、>、<、!=などを使用する検索では、検索速度が高速でない可能性があります。

ANDとORを=演算子とともに使用すると、スーパーインデックスが作成されたフィールドを検索するときに非常に強力になる可能性があります。しかし、検索速度を最大限に高めるには、慎重に使用する必要があります。次の表に、スーパーインデックスを活用したクエリを作成する方法を理解するのに役立つ例を示します。

注: 検索を最大限に高速化するには、クエリで使用するすべてのフィールドにインデックスが作成されている必要があります。

大量のデータから出現頻度の少ない値を探す検索におけるスーパーインデックス作成のためのクエリ例

クエリ	検索速度が向上するか
arcsight (全文)	違いはありません。 これは全文クエリであり、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることができません。
192.0.2.0 (スーパーインデックスが作成されたフィールドのように見える全文検索)	違いはありません。 これは、IPアドレスの可能性がありますが、全文検索であり、スーパーインデックスが作成されたフィールドの1つに対する=検索ではありません。そのため、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることができません。
sourceAddress = 192.0.2.0 (スーパーインデックスが作成された	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。

大量のデータから出現頻度の少ない値を探す検索におけるスーパーインデックス作成のためのクエリ例 (続き)

クエリ	検索速度が向上するか
フィールドに対する=)	Loggerで、sourceAddressとして192.0.2.0が見つからないと、メッセージ「結果が見つかりません」が素早く返されます。そのsourceAddressが見つかると、検索対象のイベントの範囲が狭められます。
sourceAddress = 192.0.2.0 OR sourceAddress = 192.0.2.2 (スーパーインデックスが作成されたフィールドに対するORを使用した=)	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。 Loggerで、sourceAddressとして192.0.2.0または192.0.2.2が見つからないと、メッセージ「結果が見つかりません」が素早く返されます。そのいずれかが見つかると、検索対象のイベントの範囲が狭められます。
sourceAddress = 192.0.2.0 AND destinationAddress = 192.0.2.2 (スーパーインデックスが作成されたフィールドに対するANDを使用した=)	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。 Loggerで、sourceAddressとして192.0.2.0が見つからないと、メッセージ「結果が見つかりません」が素早く返されます。 同様に、destinationAddressとして192.0.2.2がLoggerで見つからないと、sourceAddressとして192.0.2.0が見つかった場合でも、メッセージ「結果が見つかりません」が素早く返されます。 Loggerの両方が見つかると、検索対象のイベントの範囲が狭められます。
sourceAddress != 192.0.2.0 (スーパーインデックスが作成されたフィールドに対する!=)	違いはありません。 スーパーインデックス作成は、否定には役立たないため、このクエリでは、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることはできません。
sourceAddress != 192.0.2.0 OR destinationAddress= 192.0.2.2 (スーパーインデックスが作成されたフィールドに対するORを使用した!=)	違いはありません。 sourceAddressに否定があり、これはOR条件であるため、このクエリは、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることはできません。
sourceAddress != 192.0.2.0 AND destinationAddress = 192.0.2.2 (スーパーインデックスが作成されたフィールドに対するANDを使用した!=)	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。 これはAND条件であるため、両方の条件がtrueになる必要があります。 sourceAddressに否定があるにもかかわらず、Loggerの192.0.2.2のdestinationAddressアドレスが見つからないと、このAND条件は満たされません。その場合、メッセージ「結果が見つかりません」が素早く返されます。 LoggerのdestinationAddressが見つかると、検索対象のイベントの範囲が狭められます。
sourceAddress = 192.0.2.0 AND arcsight	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。

大量のデータから出現頻度の少ない値を探す検索におけるスーパーインデックス作成のためのクエリ例 (続き)

クエリ	検索速度が向上するか
(スーパーインデックスが作成されたフィールドに対する=と全文検索のAND)	Loggerの192.0.2.0のsourceAddressが見つからないと、このAND条件は満たされません。その場合、全文検索があっても、メッセージ「結果が見つかりません」が素早く返されます。 LoggerのsourceAddressが見つかると、検索対象のイベントの範囲が狭められます。
sourceAddress = 192.0.2.0 OR arcsight (スーパーインデックスが作成されたフィールドに対する=と全文検索のOR)	違いはありません。 Loggerの192.0.2.0のsourceAddressが見つかったかどうかにかかわらず、OR条件では、"arcsight"に対する全文検索が必要なため、このクエリでは、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることはできません。
name = "CPU Usage" AND sourceAddress = 192.0.2.0 (インデックスフィールドおよびスーパーインデックスフィールド)	検索速度が向上し、ヒットがないときに結果が非常に素早く返されます。 名前はスーパーインデックスが作成されたフィールドの1つではありませんが、クエリでAND条件が使用されているため、192.0.2.0のsourceAddressが見つからない場合、Loggerによってメッセージ「結果が見つかりません」が素早く返されます。 LoggerのsourceAddressが見つかると、検索対象のイベントの範囲が狭められます。
name = "CPU Usage" OR sourceAddress = 192.0.2.0 (インデックスフィールドまたはスーパーインデックスフィールド)	違いはありません。 sourceAddressは、スーパーインデックスが作成されているフィールドの1つですが、スーパーインデックスが作成されていない名前とのOR条件であるため、このクエリでは、スーパーインデックスが作成されたフィールドの検索速度向上の恩恵を受けることはできません。
sourceAddress = 192.0.2.0 AND (sourceHostName = myhost.com OR sourcePort = 80) AND (destinationAddress = 192.0.2.2 OR arcsight) (スーパーインデックスが作成されたフィールド AND (ネストしたOR条件) AND (ネストしたOR条件))	ヒットしない場合、結果は非常に高速に返されます。 Loggerの192.0.2.0のsourceAddressが見つからないと、上位のANDはtrueになりません。その場合、メッセージ「結果が見つかりません」が素早く返されます。 myhost.comのLoggerのsourceHostNameが見つからず、かつsourcePortに80が見つからない場合、OR条件はtrueになりません。そのため、上位のAND条件がtrueになりません。その場合、メッセージ「結果が見つかりません」が素早く返されます。 Loggerが、上記の条件がfalseであることを示すことができない場合、検索速度に違いはありません。 destinationAddressは、スーパーインデックスが作成されたフィールドの1つですが、"arcsight"の全文検索とのOR条件であるため、検索対象のイベントの範囲を狭めることができません。

IPv6アドレスの検索

LoggerでIPv6アドレスのフィールドが設定されている場合は、IPv4アドレスの場合と同様に、Loggerのアドレスフィールド内のIPv6アドレスをフィルター処理することができます。

IPv6アドレスの正規形式

クエリ検索演算子を使用して、IPv6アドレスの全体または一部を検索する場合、IPv6アドレスは正規の(正規化された)形式である必要があります。IPv4射影IPv6アドレスは使用しないでください。「フィールドベースの検索演算子の制限」(79ページ)を参照してください。正規形式の詳細については、https://tools.ietf.org/html/rfc5952, section 4: A Recommendation for IPv6 Text Representationを参照してください。

- デフォルトでインデックス付けされるアドレスフィールドでは、正規形式のIPv6アドレスが必要です。これには以下が含まれます。
  - `destinationAddress`
  - `deviceAddress`
  - `sourceAddress`
- インデックス付けされないアドレスフィールドは、正規形式のIPv6アドレスに制限されません。これには以下が含まれます。
  - `agentAddress`

ただし、`agentAddress`フィールドに対するクエリの処理は遅くなります。これは、その場でその都度フィールドのインデックス付けが行われるためです。`agentAddress`フィールドに対して多数のクエリを実行する場合は、Loggerでこのフィールドをインデックス付けすることを検討してください。追加のフィールドを正規化する必要がある場合は、カスタマーサポートまでご連絡ください。インデックス付けするフィールドを追加する必要がある場合は、「検索インデックス」(346ページ)を参照してください。

IPv6アドレスの一部の検索

アドレスの一部をあらかじめ正しい形式で入力した場合は、IPアドレスの一部を検索できます。クエリで入力するすべてのIPv6アドレスは、データベース内に格納されているIPv6アドレスと一致するように、正規形式に変換されます。クエリに含まれるアドレスの一部が正しい形式でない場合、データベース内に格納されているIPv6アドレスと一致しないため、結果は返されません。

フィールドベースの検索とキーワード検索

これらのアドレスフィールドのいずれかに対してキーワード検索またはフィールドベースの検索を実行すると、元のIPv6アドレスの形式に関係なく、等価なIPv6値に一致するすべてのイベントが検索されます。

IPv4射影IPv6アドレスはIPv4アドレスと照合され、逆もまた同様に処理されます。例えば、`src=::ffff:10.10.11.12`は`src=10.10.11.12`のイベントに一致します。

注: この機能は、INSUBNET演算子やルックアップ関数では使用できません。「INSUBNET演算子を使用したIPv6アドレスの検索」(122ページ)を参照してください。

IPv6でのアグリゲーション演算子

アグリゲーション演算子は、フィールドベースの検索とキーワード検索で同じように動作します。等価なIPv6アドレスに関する結果は1つの行にまとめられ、正規形式のIPv6アドレスが表示されます。有効な形式であればどの形式でアドレスを入力しても、IPv6アドレスを検索できます。これが関係あるのは、結果の表示のみです。Loggerによって、実際のイベントや値が変更されることはありません。

例: IPv6アドレスの検索

- `sourceAddress IS NULL`
- `destinationAddress = 2001:db8:85a3:0042:1000:8a2e:0370:7334`
- `deviceAddress IS NOT NULL`

INSUBNET演算子を使用したIPv6アドレスの検索

INSUBNET演算子を使用すると、通常のLoggerアドレスフィールドおよびLoggerスキーマに追加されたカスタムフィールド内のIPv4およびIPv6アドレスをフィルター処理できます。IPv4アドレスのフィルター処理の例は、「フィールドベースの検索」(73ページ)に記載されています。この演算子に関する制限事項については、「フィールドベースの検索演算子の制限」(79ページ)を参照してください。

例: INSUBNETを使用したIPv6アドレスのフィルター処理

- `sourceAddress insubnet "2001:db8::/32"`
- `agentAddress insubnet "2001:db8::-2001:db8::ffff:ffff:ffff"`
- `destinationAddress insubnet "2001:db8::*:*:*"`

例: INSUBNETを使用したIPv4アドレスとIPv6アドレスの組み合わせのフィルター処理

- `deviceAddress INSUBNET "192.0.2.0/24" OR destinationAddress INSUBNET "2001:db8::/32"`
- `agentAddress INSUBNET "2001:db8::/32" OR sourceAddress INSUBNET "192.0.2.0/16"`

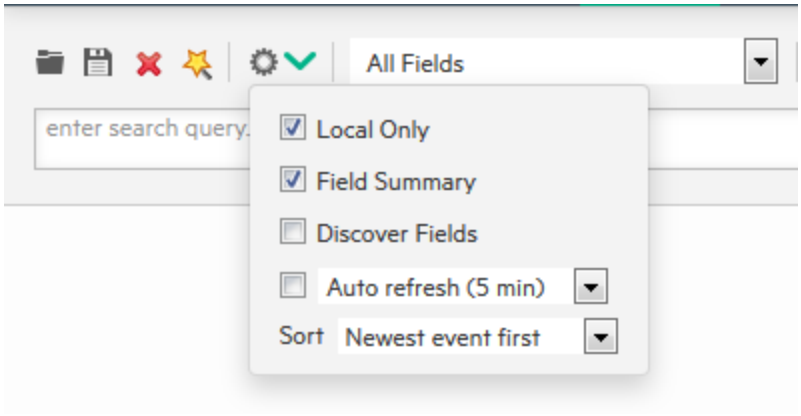
検索結果の表示

検索を開始した後、検索を実行したのと同じ画面の下部に検索結果が表示されます。数百万個のイベントを検索する必要がある場合、検索処理には時間がかかる可能性があります。指定した条件に一致するイベントの最初の画面が使用可能になると、Loggerは自動的に検索を一時停止し、一致したイベントを表示します。

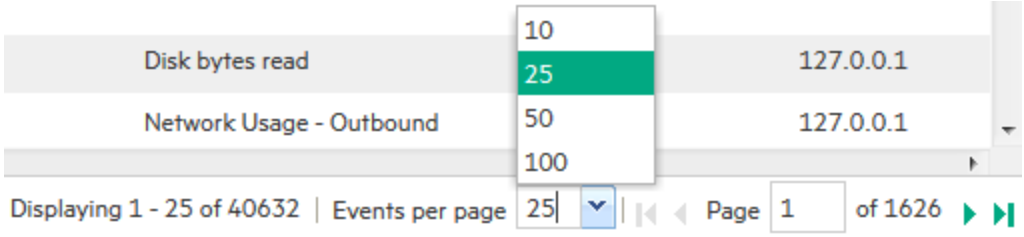
イベントデータはフィールド名別に分類され、各フィールドは色分けされた個別の列として表示されます。たとえば、Loggerでイベントを受信した時刻 (イベント時刻) は、[**時刻 (イベント時刻)**] というラベルの付いたグレーの列 (■はメタデータを示す) に表示されます。

検索結果の表示の調整

検索結果はLoggerの受信時刻でソートされます。イベントは、検索実行時の選択内容に応じて、古い順または新しい順に表示されます。ソート順序を変更するには、再度検索を実行する必要があります。ソート順序を変更するには、検索オプションのドロップダウンを開き、[ソート (Sort)] フィールドで [古いイベント順 (Oldest event first)] または [新しいイベント順 (Newest event first)] を選択します。



デフォルトでは、1画面に25個のイベントが表示されます。1画面に表示されるイベントの数を変更するには、検索結果の下部にある [ページごとのイベント数 (Events per Page)] ポップアップメニューを開き、表示するイベントの数を選択します。



検索によっては、多数のページの結果を返す可能性があります。検索結果でページ間を移動するには、該当する矢印をクリックするか、移動先のページ番号を入力してEnterキーを押します。

各イベントは、raw形式または解析済みデータで利用できます。このページのrawイベントデータは、表示/非表示を切り替えることができます。詳細については、「rawイベントの表示」(129ページ)を参照してください。

データの表示方法を変更するだけでなく、検索結果の表示から検索を絞り込むこともできます。詳細については、「検索結果での検索の絞り込み」(128ページ)を参照してください。

進行中の検索のキャンセル

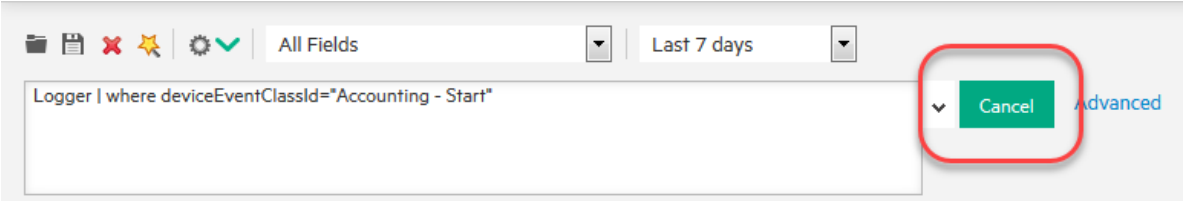
クエリが実行されている場合、一致するイベントが見つかると検索結果が表示されます。そのため、[**キャンセル (Cancel)**] をクリックすると、これまでに見つかった一致イベントが検索結果として表示されます。この機能は、クエリが大量のデータセットをスキャンする必要があるものの、これまでに表示された検索結果の中に探していたイベントが表示されている場合に便利です。部分的に表示された結果は、さらに処理できます。たとえば、結果のエクスポート、ヒストグラムを使用した結果のドリルダウン、検索結果の任意のテキストをクリックしてクエリに追加し、さらに検索結果をドリルダウンするといったことが可能です。

注: クエリにHEAD、TAIL、またはSORT演算子が含まれている場合、部分的な結果は表示されません。また、クエリに、CHART、RARE、またはTOPなどの演算子が含まれていて、クエリが中断された場合、部分的な結果のグラフは表示されません。

検索ウィンドウ内で実行されている検索をキャンセルするには

1. 検索が進行している間は、[**実行!**] ボタンが [キャンセル (Cancel)] に変わります。[**キャンセル (Cancel)**] をクリックすると検索が停止します。

   注: キャンセルしても、検索は削除されません。



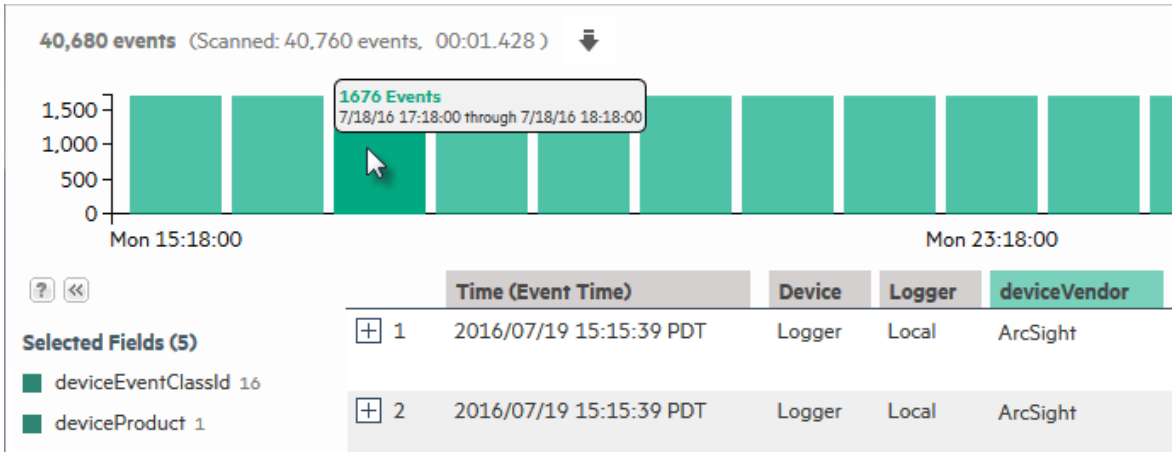
ヒストグラム

[検索結果] ページには、検索クエリに一致するイベントをグラフィカルに表現するヒストグラムが表示されます。ヒストグラムは、Loggerによるイベントの受信時刻に基づきます (Loggerの受信時刻を使用してイベントを検索する検索クエリと同様です)。

次の図に示すように、X軸はイベント時刻を表し、Y軸は一致イベント数を表します。X軸の時間分布は、クエリで指定された時間範囲に基づき、自動的に決定されます。

注: X軸の時間範囲は検索クエリで指定した時間範囲と一致しない可能性があります。これは、X軸の開始時刻と終了時刻が、検索クエリの最初と最後の一致イベントのイベント時刻で決定されるためです。

マウスオーバー時に詳細を表示するヒストグラム



ヒストグラムは、イベントが検索クエリに一致するのに従って、漸次的に作成されて表示されます。検索クエリが大量のデータまたは長い時間範囲をスキャンする必要がある場合、最初に表示されたヒストグラムは、クエリの実行中に何度も更新される可能性があります。検索クエリの完全な(最終的な)ヒストグラムを表示するには、クエリの動作が完了するまで(つまり、画面に丸い「待機」アイコンが表示されなくなるまで)待ちます。

最初の100万個の一致イベントがヒストグラムにプロットされます。検索クエリが100万個を超えるイベントに一致する場合、情報メッセージが画面に表示されます。100万個を超えるイベントに一致する検索クエリで、イベント分析にヒストグラム表示を使用する必要がある場合は、検索クエリで指定された時間範囲を調整して、一致が100万個未満となるようにすることをお勧めします。これにより、完全で意味のあるヒストグラムが得られます。また、top、head、chartなどのパイプライン演算子を使用して、検索結果をさらに絞り込み、ヒットの総数が100万イベント未満となるようにすることもできます。

ヒストグラムの表示

ヒストグラムを無効にすることはできませんが、ヒストグラムの右上隅にあるヒストグラムアイコンをクリックして非表示にすることはできます。非表示のヒストグラムを表示するには、アイコンを再度クリックします。

マウスオーバー

ヒストグラムのいずれかのバーにマウスを合わせると、バーが強調表示され、一致イベント数と、バーが表す期間が表示されます。たとえば、前の図で、強調表示されたバーは、7月18日の午後5時～6時の間の1,676個のイベントを表しています。ヒストグラムの下に表示される一致イベントは変化せず、ヒストグラムには引き続きすべての一致イベントが表示されます。

ヒストグラムのドリルダウン

特定の期間のイベントにドリルダウンするには、その期間を表すヒストグラム上のバーをクリックします。ドリルダウンするバーが強調表示され、その期間に一致するイベントがヒストグラムの下に一覧表示されます。次の図に示すように、ヒストグラムにはマッチしたすべてのイベントが継続して表示されます。

期間の選択を解除するには、再度バーをクリックします。ヒストグラム上の複数の連続するバーを選択して、選択したすべての期間の一致イベントを表示することもできます。

検索結果の表

検索結果の表には、スキャンされたイベントの数、検出されたイベントの数、各イベントタイプのインデックスステータス、および検索に要した時間が表示されます。

ヒストグラムの下には、イベントが表形式で表示され、1つのイベントにつき1つの行が表示されます。クエリに一致する項は強調表示され、イベントがクエリに一致した理由が簡単にわかるようになっています。イベント表の他の項にマウスをロールオーバーすると、緑で強調表示されます。

表示された検索結果にドリルダウンするには、緑色に強調表示された項をクリックして、現在のクエリに追加します。たとえば、"login"を検索し、検索結果の単語"fail"にロールオーバーすると、"fail"が緑色で強調表示されます。単語"fail"をクリックすると、クエリが"login AND fail"に変わります。

ヒント: また、表示される任意の列を強調表示してテキストをコピーすることもできます。この機能は、IPアドレスまたはURLをコピーする必要があるときに便利です (クリックしてカーソルをドラッグしてテキストを選択します。次に右クリックして [**コピー**] オプションを表示します)。

デフォルトでは、フィールドサマリーパネルが一致イベントの左側に表示されます。ここには、一致イベント内に発生するフィールドと、それらのイベント内の各フィールドの一意の値の数が表示されます。フィールドサマリーの詳細については、「フィールドサマリーパネル」(132ページ)を参照してください。

検索結果のその他のフィールド

Loggerのスキーマフィールドに加えて、他のタイプのフィールドが検索結果に表示される場合があります。

ユーザ定義フィールド

ユーザ定義フィールドは、検索クエリに`rex`、`extract`、`rename`などの演算子が含まれる場合に作成されます。このような演算子の詳細については、「検索演算子」(564ページ)を参照してください。これらのフィールドは、[システムフィールドセット] の [すべてのフィールド] ビューの追加の列として表示されます。これらの列のみを表示するには、[システムフィールドセット] リストから [**ユーザ定義フィールド**] を選択します。

システム定義フィールド

検索クエリが、定義されたソースタイプから受信し、あらかじめ定義されたパーサーまたはユー

ザー定義パーサーを使用して解析されたイベントに一致する場合、検索結果にはパーサーフィールドが含まれ、[検索オプション] ページの設定に応じて、ソースタイプとソースのフィールドが含まれる可能性があります。詳細については、「グローバル検索オプション」(349ページ)を参照してください。

システム定義フィールドにはイベントデータが含まれていないため、検索できません。詳細については、「検索クエリの作成について」(110ページ)を参照してください。

フィールド	説明
パーサー	イベントが解析されたかどうかと、解析された場合はどのパーサーが使用されたかを示します。 **注:** パーサーフィールドは検索可能ではありませんが、パーサーは関連付けられたソースタイプに基づいて検索可能なフィールドを定義します。これらのフィールドは、ソースタイプによって変わります。詳細については、「パーサー」(392ページ)を参照してください。 イベントが解析された場合、このフィールドにはパーサーの名前が表示されます。イベントが正常に解析されなかった場合、このフィールドには「Not parsed」と表示されます。ソースタイプにパーサーが定義されていない場合や、ソースタイプがない場合、このフィールドは空になります。
ソースタイプ	イベントの受信元のファイルの種類。[**ソースタイプ**] ページ ([設定 | データ] > [ソースタイプ]) で定義します。詳細については、「ソースタイプ」(388ページ)を参照してください。 イベントを受信したときにソースタイプが適用されなかった場合、このフィールドは空になります。このフィールドを表示するかどうかを、[検索オプション] ページで制御できます。
ソース	イベントの受信元のログファイルの名前。たとえば`/opt/mnt/testsoft/web_server.out.log`と表示されます。 イベントを受信したときにソースが適用されなかった場合、このフィールドは空になります。このフィールドを表示するかどうかを、[検索オプション] ページで制御できます。

検索結果での検索の絞り込み

次のショートカットを使用し、表示された検索結果の列やrawイベントから項を選択して、検索クエリを調整します。

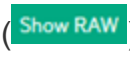
- 検索結果の項をクリックして検索クエリに追加し、検索をすぐに再度実行します。
- [**フィールド値の複数選択を有効にします (Enable Multi-select of field values)**] チェックボックス (☐ Enable Multi-select of field values.) をオンにし、検索クエリに追加する複数の項をクリックします。複数の項が追加されると、条件がAND演算子で結合されます。[**実行!**] をクリックして検索を実行します。

- Ctrlキーを押しながらクリックして検索クエリ全体を、<フィールド名> + "CONTAINS" + <選択した項>に置き換え、検索をすぐに再度実行します。
- 項のNOTを追加してクエリを実行するには、検索結果でAltまたはShiftを押しながら項をクリックします。こうすることで、選択した項に一致するイベントが除去されます。
- Altキーを押しながら検索結果の項を選択して、複数のNOT条件を追加します。複数の条件が追加されると、条件がAND演算子で結合されます。[**フィールド値の複数選択を有効にする (Enable Multi-select of field values)**] がオンになっている場合は、[**Go!**] をクリックして検索を実行します。オンになっていない場合は、項をクリックしたときに検索が実行されます。
- `Ctrl+Alt`キー (または`Ctrl+Shift`キー) を使用して、検索クエリを `NOT + <field name> + "CONTAINS" + <selected term>`に置き換えます。

> **注:** 検索可能でないフィールドは、検索結果でマウスを重ねても、強調表示されないため、クリックして検索に追加することはできません。検索対象の詳細については、「検索クエリの作成について」(110ページ) および「検索結果のその他のフィールド」(127ページ) を参照してください。

rawイベントの表示

各イベントは、raw形式または解析済みデータで利用できます。デフォルトでは、解析済みデータが表示されます。

- 個別のイベントのrawデータを表示するには、イベントの左側にある⊞アイコンをクリックします。
- 表示されたすべてのイベントのrawデータを表示するには、画面の下部にある [**RAWを表示**] (

) をクリックします。

[検索オプション] ページで [syslogイベントのrawEventフィールドを生成] オプションを有効にした場合は、syslog rawイベントを`rawEvent`という名前の書式設定された列に表示することもできます。「グローバル検索オプション」(349ページ) を参照してください。rawイベントの表示の詳細については、「事前定義フィールドセット」(82ページ) を参照してください。

フィールドセットを使用した検索結果表示の変更

デフォルトでは、検索結果は [すべてのフィールド] フィールドセットを使用して表示され、イベントに含まれるすべてのフィールドが表示されます。別のフィールドセットを選択すると、次に変更するまでそれがデフォルトの表示になります。フィールドセットの詳細については、「フィールドセット」(82ページ) を参照してください。

Raw Eventフィールドセットを使用して検索結果を表示する場合は、以下のガイドラインに従ってください。

- rawEvent列にrawイベントが表示される場合でも、この列はLoggerデータベースに追加されず、インデックスが作成されません。そのため、イベントに対して、キーワード検索 (全文検索) または正規表現検索のみを実行できます。
- 正規表現ヘルパーツールを使用して、クエリに追加するrawEvent列内のraw syslogイベントから文字列を識別することができます(rawEvent列に表示されるCEFイベントに対しては正規表現ヘルパーを使用できません)。正規表現ヘルパーツールの詳細については、「正規表現ヘルパーツール」(100ページ)を参照してください。

複数行のデータ表示

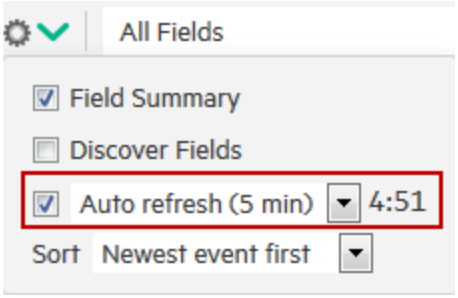
イベントフィールドは、改行 (\n) または復帰 (\r) などの文字で区切られた複数の行にまたがる可能性があります。例:

```
0x0000: 0000 0100 0000 0000 0000 0000 0000 0000 ................
0x0010: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0x0020: 0000 0000 0000 0000 0000 0000 0000 ..............
```

Loggerユーザーインターフェイスはこれらを複数行にわたって表示し、行区切りは削除せず、メッセージを1行にまとめます。

検索結果の自動更新

自動更新機能は、指定した間隔で検索を実行し、新しいイベントがクエリに一致する場合に検索結果を更新します。このオプションは、[検索オプション] メニューで設定します。



要件に応じて、検索結果を以下の間隔で自動更新できます。

- 30秒
- 60秒
- 2分
- 5分 (デフォルト)
- 15分

このオプションは、検索処理を実行する前または後に有効にできます。検索でこのオプションを有効にすると、明示的に無効にしない限り、そのタブのすべての検索操作に対してこの設定が保持されます。他のタブで同時に行う検索には影響しません。それぞれのタブごとに個別に設定する必要があります。

検索結果を自動更新するには

1. ナビゲーションバーで、[分析] > [検索] を選択します。
2. [検索オプション] メニューで、[**自動リフレッシュ (Auto refresh)**] ボックスをオンにし、必要なリフレッシュ間隔を選択します。

グラフのドリルダウン

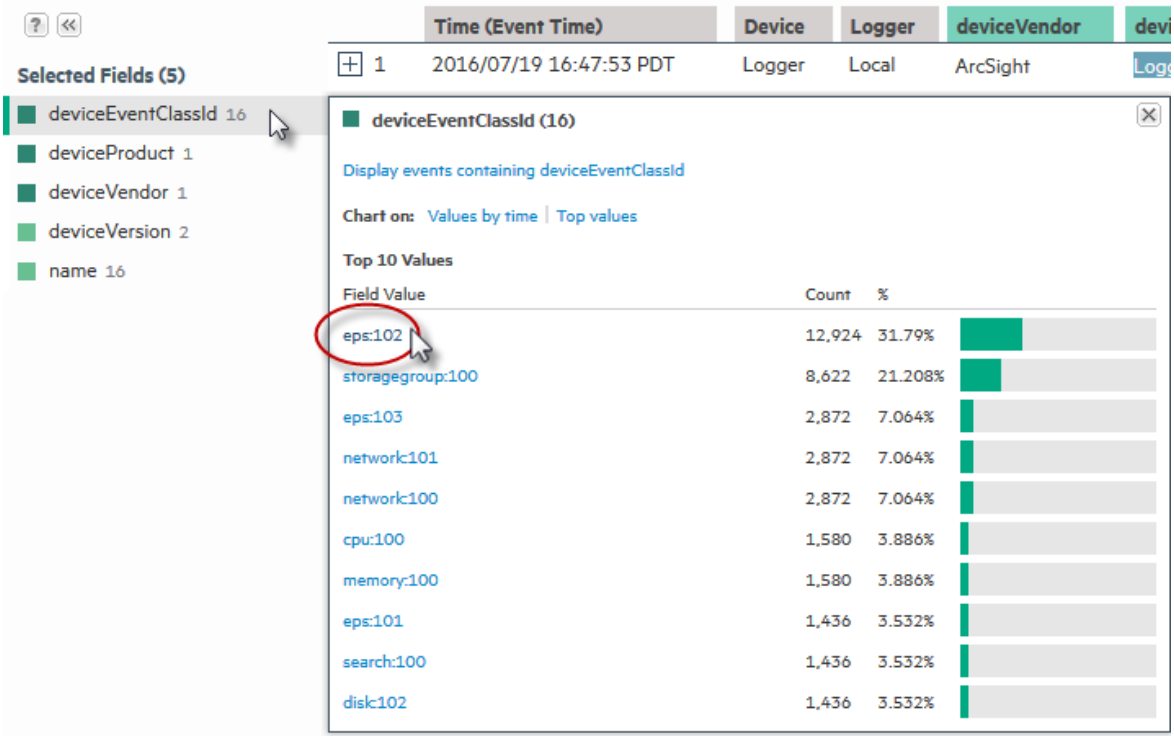
CHART、TOP、RAREなどのアグリゲーション検索演算子は、検索結果のグラフを生成します。グラフのドリルダウン機能を使用すると、特定のフィールド値を持つイベントを素早く絞り込むことができます。

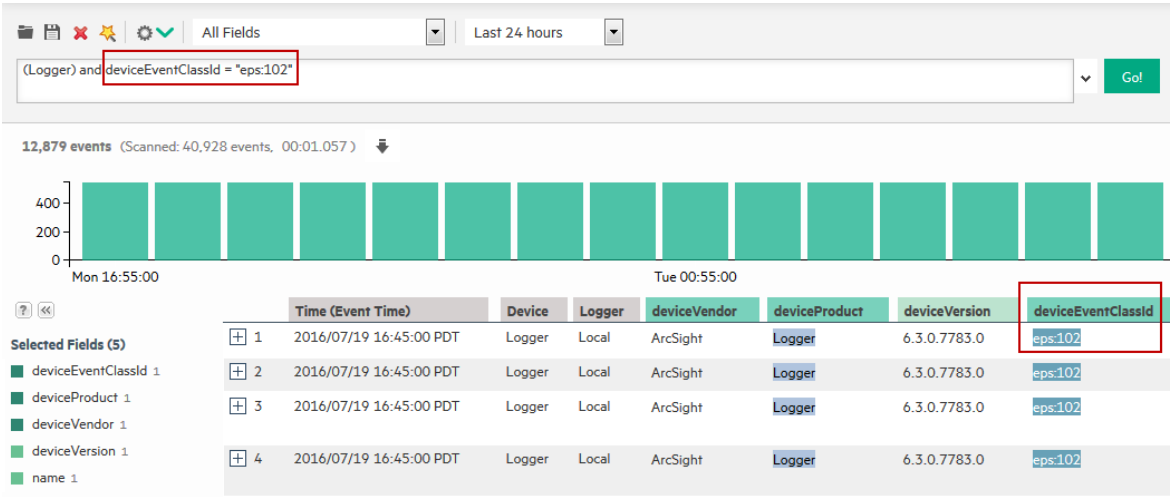
検索結果のグラフで値を特定し、クリックしてその値に一致するイベントにドリルダウンします。たとえば、次のグラフで、デバイスイベントクラスIDがeps 102のイベントを表示するには、**eps:102**というラベルの付いた列をクリックして、2番目の図に示すイベントを表示します。

グラフの値 (縦棒、横棒、またはドーナツグラフの一部) をクリックすると、既存の検索クエリが変更されてそのフィールド名と値を含むWHERE演算子が追加され、自動的に再実行されます。

ドリルダウン画面から元のクエリに戻るには

1. ブラウザーの「戻る」機能を使用してください。



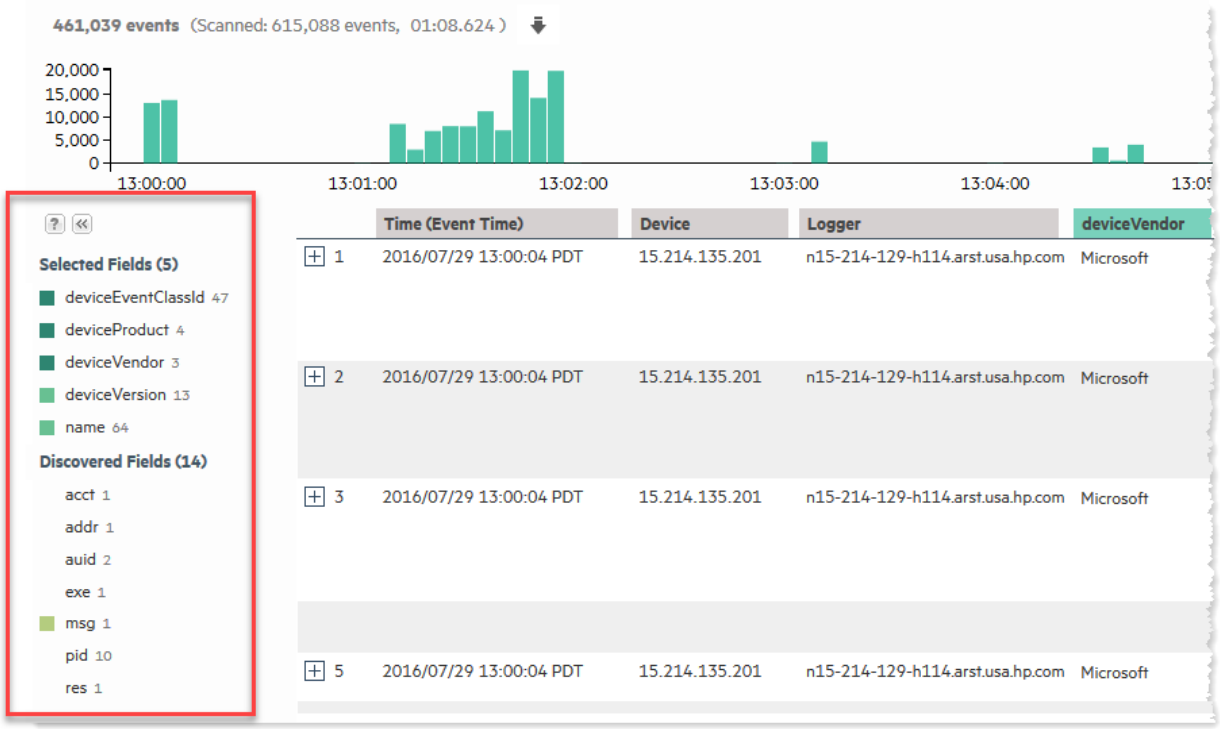


フィールドサマリーパネル

クエリを実行すると、フィールドサマリーパネルに、一致イベント内のCEFおよび非CEFフィールドと、それらイベント内の各フィールドの一意の値の数が表示されます。このパネルは、グラフを生成しないクエリのみで表示されます。ピア検索を実行すると、要約されたフィールド値にピアLoggerからのカウントが含まれます。

フィールドサマリーパネルには、**[選択されたフィールド]** と **[検出されたフィールド]** の2つのセクションがあります。[選択されたフィールド (Selected Fields)] セクションにはCEFフィールドが表

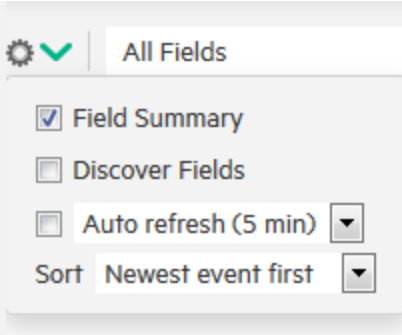
示されるのに対し、[検出されたフィールド (Discovered Fields)] セクションには、rawイベント内で見つかった非CEFフィールドが表示されます。



フィールドサマリーパネルの表示

[フィールドサマリー (Field Summary)] 機能は、デフォルトで有効になっており、[フィールドを検出 (Discover Fields)] オプションは無効になっています。これらのオプションは「グローバル検索オプション」(349ページ)でグローバルに制御され、検索結果の表示オプションのチェックボックスでローカルに制御されます。[分析] > [検索] ページでこれらのオプションを選択すると、[検索オプション] ページでのこれらのオプションの設定が上書きされます。[フィールドの検出] オプションの詳細については、「rawイベントデータでのフィールドの検出」(136ページ)を参照してください。

[フィールドサマリー] パネルは、検索結果の表示オプションの [フィールドサマリー (Field Summary)] チェックボックスを使用して表示/非表示を切り替えることができます。



選択済みフィールドのリスト

デフォルトでは、[選択済みフィールド] には、

- `deviceEventClassId`
- `deviceProduct`
- `deviceVendor`
- `deviceVersion`
- `name`

このリストは必要に応じて編集できます。このリストには、デフォルトで各フィールドの上位10個の値が表示されます。

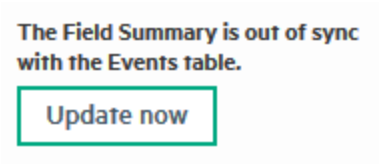
フィールドセットを変更すると、フィールドサマリーパネルの [選択したフィールド] リストに表示されるフィールドを変更できます。定義済みのフィールドセットのいずれかを使用するか、独自のフィールドセットを作成して必要なフィールドのみを含めることができます。

[選択したフィールド] リストを変更するには

1. [選択したフィールド] リストに含めるフィールドを追加するには、既存のカスタムフィールドセットを定義または更新します。カスタムフィールドセットの作成については、「フィールド

セット」(82ページ) を参照してください。

2. 定義したカスタムフィールドセットを選択して、検索結果を表示します。
3. 検索クエリを実行した後、異なるフィールドセットを選択した場合、フィールドサマリーパネルに以下のメッセージが表示されます。



このメッセージは、フィールドサマリーパネルに表示されているフィールドが、新たに選択されたフィールドセットに一致しないことを示しています。新しいフィールドセットで指定したフィールドを表示するには、**[今すぐ更新 (Update now)]** をクリックします。

フィールドサマリーのドリルダウン

[フィールドサマリー] パネルでは、表示される任意のフィールドや、表示されるフィールドの特定の値でドリルダウンできます。

たとえば、deviceEventClassId (特定のフィールド) を含むすべてのイベントを表示したり、deviceEventClassIdが「storagegroup:100」(フィールドの特定の値) のイベントを表示したりできます。

値がSTRING型のフィールドでは、すべてのイベントの表示、上位10個の表示、一致イベントのグラフの作成を行うことができます。値がNUMERIC型のフィールドでは、平均、最小、最大などの算術演算を実行できます。

クエリを実行するか、特定のフィールドまたは値にドリルダウンするたびに、新たに選択した条件を使用した新たなクエリが実行され、[フィールド サマリー] リストが更新されます。

フィールドサマリーでドリルダウンを表示するには

1. [分析] > [検索] をクリックして検索ページを開きます。
2. 検索オプションの下矢印 (⌄) をクリックして、検索表示オプションを設定し、**[フィールド サマリー (Field Summary)]** をオンにします。
3. 検索を実行します。
4. [フィールド サマリー] リストで、詳細を確認するフィールド名をクリックします。
5. [<フィールド名><値の数>] ダイアログボックスに、上位10個のフィールド値が表示されます。
6. オプションで、**[<フィールド名>を含むイベントの表示]** をクリックして、該当するイベントのみを表示する検索を実行します。
7. オプションで、フィールド値をクリックして、該当するイベントのみを表示する検索を実行します。

8. オプションで、「フィールドサマリーからの検索の精緻化とグラフ化」(137ページ)の説明に従って、結果のグラフを作成します。

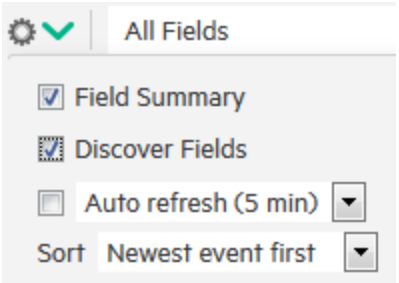
rawイベントデータでのフィールドの検出

フィールドサマリー機能では、[フィールドを検出 (Discover Fields)] が有効になっている場合に、CEF以外のフィールドをrawイベントから自動的に検出できます。デフォルトで、[フィールドを検出 (Discover Fields)] オプションは無効になっています。

Logger上のすべての検索で [フィールドを検出 (Discover Fields)] オプションを有効にする必要がある場合は、次の図に示すように、[検索オプション] ページ ([設定 | 検索] > [検索オプション]) でこれらのオプションのデフォルト値「いいえ (No)」を「はい (Yes)」に変更します。

しかし、[フィールドを検出 (Discover Fields)] オプションを時々使用する必要がある (すべての検索で使用するわけではない) 場合は、検索クエリを実行するユーザーインターフェイスページ ([分析] > [検索]) で一度だけ使用するためにこのオプションを有効にできます。そのためには、検索表示オプションで **[フィールドを検出 (Discover Fields)]** チェックボックスをオンにしてからクエリを実行します。

注: [検索] ページでこれらのオプションを選択すると、[検索オプション] ページでのこれらのオプションの設定が上書きされます。



ヒント: フィールドを自動検出するには、rawイベントに「key=value」形式でデータが含まれている必要があり、「value」の先頭文字が、カンマ、スペース、タブ、セミコロンのいずれかであってはなりません。

rawイベントに見つかるそれぞれの「key=value」ペアについて、「key」という名前の新しいフィールドが作成されます。フィールドサマリーには、[検出されたフィールド] セクションに、すべての新しいフィールドの値の要約が含まれています。検出されたフィールドには、デフォルトで「String」型が割り当てられます。自動検出機能は、最初の10,000個の一致イベントの

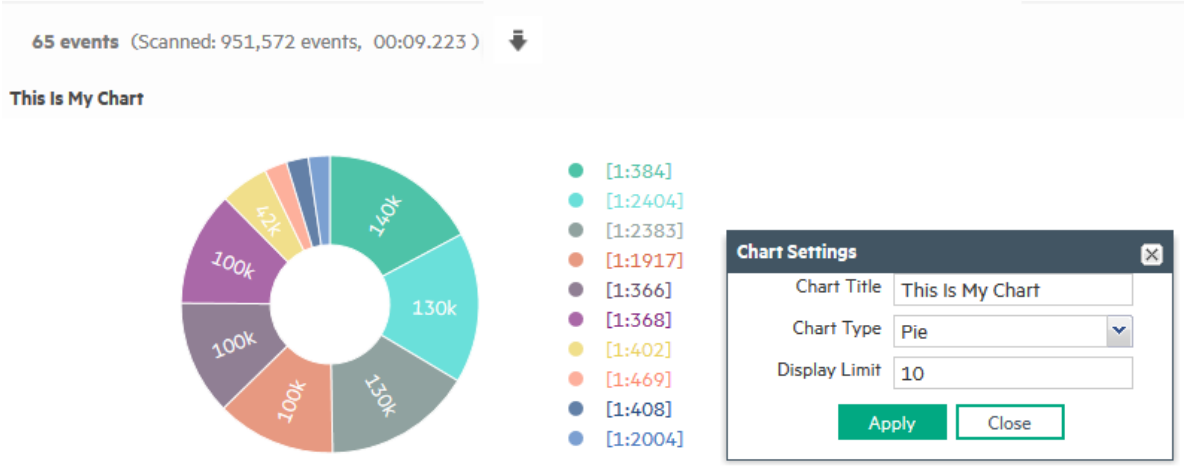
2,500個以上に「key=value」ペアが含まれている場合にのみ機能します。このしきい値が満たされていない場合、自動検出は自動的に無効になります。ただし、一致イベント数が10,000個未満の場合はこのしきい値が適用されず、フィールドは必ず検出されます。

フィールドサマリーからの検索の精緻化とグラフ化

フィールドサマリーでフィールドをクリックすると、<フィールド名><値の数>というラベルが付いたダイアログボックスにフィールドに関する情報が表示されます。ここからドリルダウンして詳細を表示したり、検索結果のグラフを作成したりできます。

フィールドサマリーからフィールドの詳細を表示するには

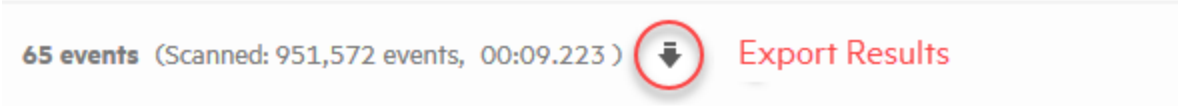
1. 検索を実行し、必要なデータにドリルダウンします (「フィールドサマリーのドリルダウン」(135ページ)を参照)。
2. 検索結果のグラフを作成するには、[**時間別の値**]、[**トップの値**] など、値に対するいずれかのグラフをクリックします。
3. 結果が結果グラフと結果テーブルに表示されます。
4. 結果グラフで、[**グラフ設定**] をクリックしてグラフを調整します。
5. [**グラフタイトル**] に有用なグラフのタイトルを入力します。
   - データに最適な [**グラフタイプ**] を選択します。
   - [**表示制限**] で表示制限を設定します。有効な最大値は100です。



6. 結果テーブルで、ナビゲーションボタンを使用して、結果のリスト中を前後に移動したり、検索を更新したりできます。

   検索結果を含むPDFまたはCSVファイルを作成するには、[**結果のエクスポート**] をクリック

します。詳細については、「検索結果のエクスポート」(139ページ)を参照してください。



検索結果の保存

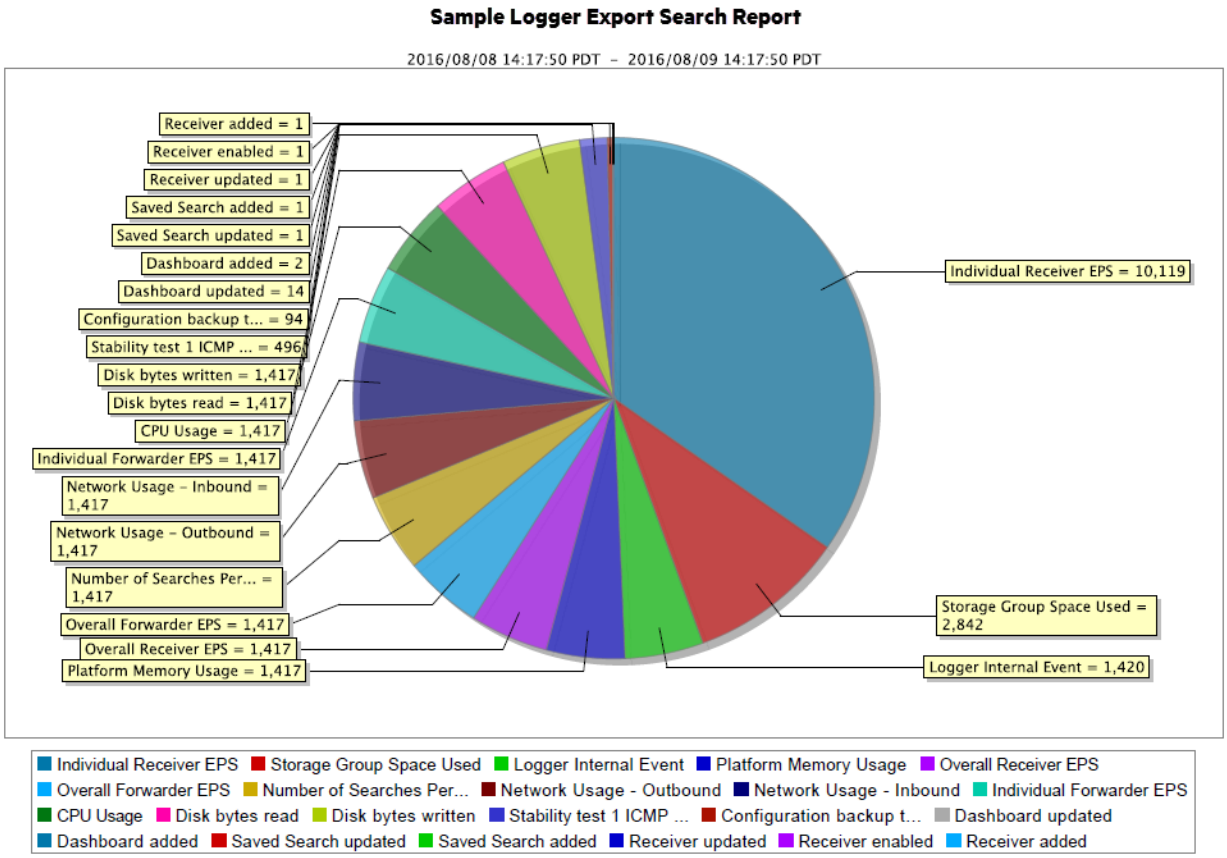
検索結果を保存するには、次のように、PDFまたはCSV形式でエクスポートします。

- **PDF**: 検索結果の簡易レポートを生成するのに便利です。レポートには、検索結果の表と、結果用に生成されたすべてのグラフが含まれています。rawイベント (構造化されていないデータ) とCEFイベント (構造化されているデータ) の両方を、エクスポートするレポートに含めることができます。
- コンマ区切り値 (**CSV**) ファイル: 他のソフトウェアアプリケーションでさらに分析するのに便利です。レポートには、検索結果の表が含まれています。この形式にはグラフを含めることができません。

時間フィールドである、`deviceReceiptTime`、`startTime`、`endTime`、`agentReceiptTime`のデータが、人間が見やすい形式でエクスポートされます。たとえば、`2015/03/21 20:22:09 PDT`といった具合です。

PDF形式でのクイックレポートの例 (検索結果のエクスポート)

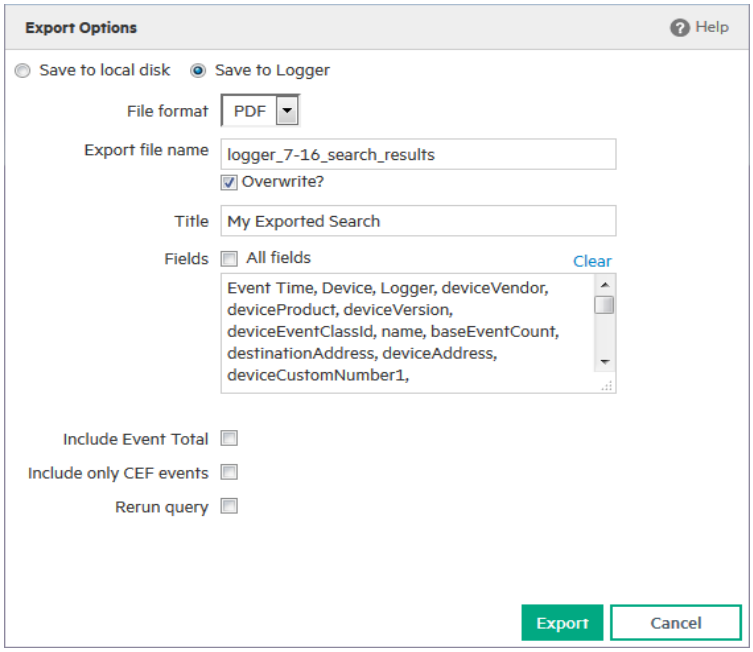
以下に、PDF形式で生成された簡易レポートの例を示します。まずグラフが表示され、次に一致イベントの表が表示されます (この例には示されていません)。生成されるすべてのグラフ (積み上げグラフを含む) をエクスポートできます。



検索結果のエクスポート

検索結果をエクスポートするには

1. **[分析] > [検索]** ページまたは **[分析] > [アラート]** ページで検索クエリを実行します。
2. ヒストグラムの上にある結果のエクスポートの矢印をクリックします。



3. 指定可能なオプションを選択し、[**エクスポート (Export)**] をクリックします。表示されるオプションは、選択内容に基づいて変わります。

オプション	説明
ローカルディスクに保存	ファイルは、Loggerへのアクセス元のローカルシステムに保存するか、ブラウザーに送信して表示または保存されます。
リモートロケーションへエクスポート	ファイルをエクスポートするときに選択 Loggerアプライアンスでは、ファイルは、NFSマウント、CIFSマウント、またはSANシステムに書き込まれます。 Loggerソフトウェアでは、データが<インストールディレクトリ>/data/loggerディレクトリに常に保存されます。このディレクトリは、Loggerソフトウェアを実行しているシステムのローカル、またはNFSやCIFSなどのリモートストレージシステム上に作成できます。 **注:** Loggerアプライアンスは、ユーザーインターフェイスを通じたマウントをサポートしています。ソフトウェアLoggerは、そのファイルシステムを使用します。これには、オペレーティングシステムによってマウントされたリモートフォルダーを含めることができます。
Loggerに保存	Loggerのローカルシステムにファイルを書き込むときに選択します。
ファイル形式	[**CSV**] を選択すると、CSV (コンマ区切り値) ファイルが生成されます。 [**PDF**] を選択すると、検索結果を表とグラフで記載したレポート形式のPDFが生成されます。グラフは、検索クエリにchartやtopなどのグラフを作成する演算子が含まれている場合にのみ含まれます。

オプション	説明
ファイル名のエクスポート	([リモートロケーションへエクスポート] オプションがオンの場合のみ使用可能) イベントのエクスポート先のファイル名を指定します。 指定した名前のファイルが存在しない場合、ファイルが作成されます。指定した名前のファイルが存在し、[上書き] チェックボックスがオフになっている場合、エラーが生成されます。[上書き] チェックボックスがオンになっている場合、既存のファイルが上書きされます。
タイトル	(オプション。ファイル形式が「PDF」の場合のみ使用可能) PDFファイルの先頭に表示される、意味のある名前を入力します。タイトルを指定しないと、「Untitled」となります。
フィールド	エクスポートされたファイルに含まれるイベントフィールドのリストを表示します。デフォルトでは、すべてのフィールドが含まれます。 [すべてのフィールド] を選択解除して、フィールドを入力したり、表示されるフィールドを編集したりできます。 演算子`rex`、`extract`、`rename`、または`eval`の結果として作成されるフィールドや、パーサーがイベントに適用されるときに作成されるフィールドをエクスポートするには、[フィールド] リストで`*user`が選択されていることを確認します。
グラフタイプ (PDFのみ)	(検索結果でグラフが使用可能な場合のみ使用可能) PDFファイルに含めるグラフの種類を選択します。選択できるのは、カラム、棒、円グラフ、エリア、ライン、積み上げカラム、積み上げ棒グラフです。 **注:** [グラフタイプ] が、[検索結果] 画面に表示されるグラフと異なる場合、このオプションで選択した値で画面に表示される値が上書きされます。そのため、エクスポートされるPDFには、画面に表示されるグラフではなく、このオプションで指定したグラフが含まれます。
グラフ結果リミット (PDFのみ)	(検索結果でグラフが使用可能な場合のみ使用可能) プロットする一意の値の数を指定します。デフォルト値: 10 設定された [グラフ結果リミット] の値が、クエリの一意の値数未満の場合、上位から [グラフ結果リミット] の値に等しい数の値がプロットされます。つまり、グラフ結果リミットが5で、一意の値が7個見つかった場合、上位5個の値がプロットされます。
イベント合計を含む	選択すると、エクスポートされる検索結果にイベントの合計数が含まれます。
CEF イベントのみを含む	選択すると、エクスポートされる検索結果にCEFイベントのみを含めます。
ベースイベントを含む (アラートのみで使用可能)	選択すると、エクスポートされる検索結果にベースイベントを含めます。 **ヒント:** ベースイベントオプションは、**[分析] > [アラート]** ページから検索結果をエクスポートする場合のみ使用できます。
クエリの再実行	選択すると、検索結果をエクスポートする前にクエリが再実行されます。

エクスポート処理のスケジュール

検索結果のエクスポートに要する時間は、エクスポートするイベントの数に比例します。そのため、イベント数が多い場合は、エクスポート処理を後で実行するようにスケジュールするため、クエリと時刻のパラメーターを保存された検索として保存してから、保存された検索ジョブをスケジュールすることをお勧めします。スケジュールされた検索の作成方法など、保存された検索ジョブの詳細については、「スケジュールされた検索/アラート」(335ページ)を参照してください。

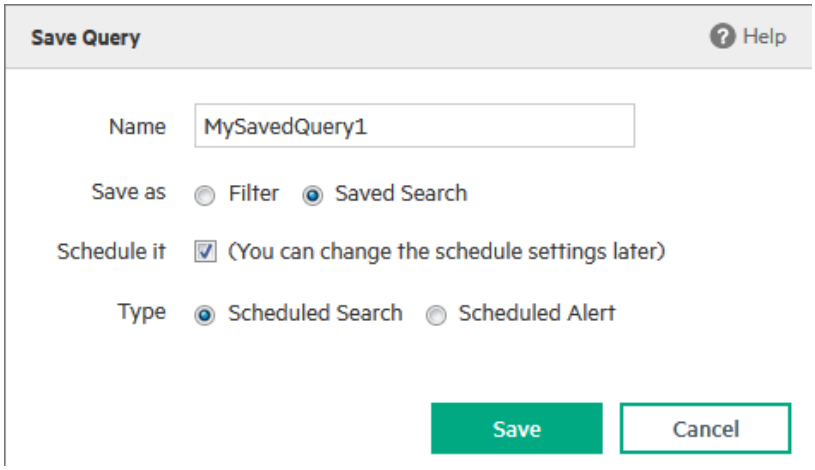
クエリの保存 (保存された検索、保存されたフィルターの作成)

同じ検索クエリを定期的に実行する必要がある場合は、フィルターまたは保存された検索として保存できます。

- フィルターとして保存するとクエリ式が保存されますが、時間範囲やフィールドセット情報は保存されません。
- 保存された検索として保存すると、指定したクエリ式と時間範囲が保存されます。

クエリを保存するには

1. 「イベントの検索」(106ページ)または「検索の詳細設定ビルダーの使用」(94ページ)に説明されているとおりにクエリを定義します。
2. [保存] アイコン () をクリックし、クエリの名前を [名前] フィールドに入力します (下図を参照)。

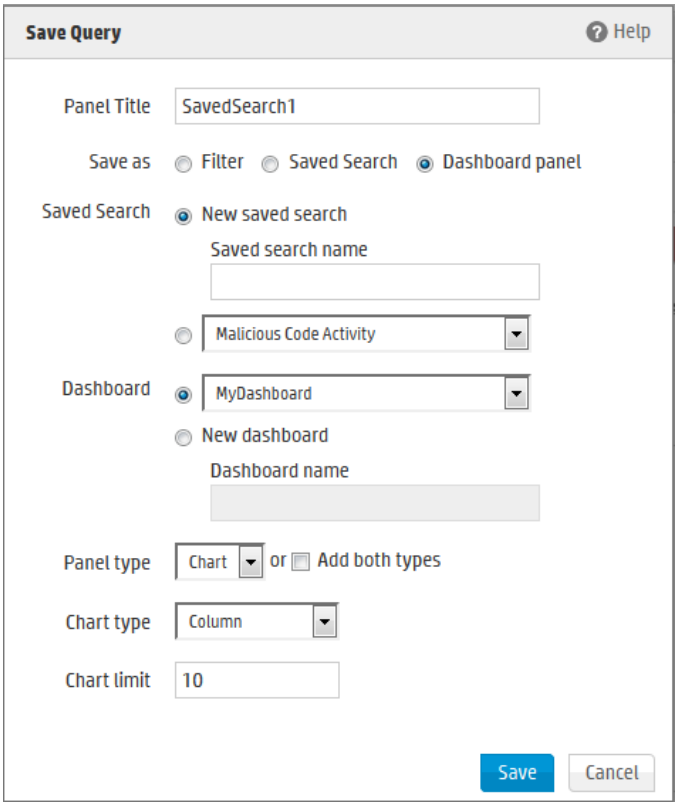


3. [名前を付けて保存] フィールドで、このクエリをフィルターとして保存するのか、保存された検索として保存するのか、ダッシュボードパネルとして保存するのかを選択します。

   保存された検索として保存する場合は、保存されたクエリを [保存された検索 (Saved Search)] として保持するか、または **[スケジュールに入れる (Schedule it)]** チェックボックスをオンにして、[スケジュールされた検索 (Scheduled Search)] や [スケジュールされたアラート (Scheduled Alert)] に変更することができます。(アグリゲーション演算子を含むクエリを、保存された検索アラートで使用することはできません。)保存された検索アラートの詳細については、「保存された検索アラート」(343ページ) を参照してください。

   検索クエリに、chartやtopなどのアグリゲーション演算子が含まれている場合、クエリをダッシュボードパネルに保存するための選択肢も表示されます。

   [ダッシュボード パネル (Dashboard panel)] オプションを選択すると、ダッシュボードオプションが表示されます。



以下のパラメーターを入力します。

パラメーター	説明
タイトル	ダッシュボードに追加されるパネルの意味のある名前を入力します。
保存された検索	ドロップダウンボックスから、このクエリで上書きされる既存の保存された検索を選択します。 または [保存された新しい検索] を選択して、新しい保存された検索クエリを作成します。テキストボックスに新しい名前を入力します。
ダッシュボード	ドロップダウンボックスから、[検索結果] パネルを追加する既存のダッシュボードを選択します。 または [新規のダッシュボード] を選択して、[検索結果] パネルを新しいダッシュボードに追加します。新しいダッシュボードの名前を、[ダッシュボード名] フィールドに入力します。

パラメーター	説明
パネルタイプ	パネルの種類を以下の中から選択します。 • グラフ: 検索結果をグラフ形式で表示します。 • テーブル: 検索結果を表形式で表示します。 • グラフとテーブル: 2つのパネルを追加します。1つは検索結果をグラフ形式で表示するためのものであり、もう1つは検索結果を表形式で表示するためのものです。
グラフタイプ	一致するイベントを表示するグラフの種類を選択します。選択できるのは、 カラム、棒、円グラフ、エリア、ライン、積み上げカラム、積み上げ棒グラフです。 デフォルト値: カラム
グラフ制限	[検索結果 (グラフ)] パネルのみに適用されます。 プロットする一意の値の数を指定します。デフォルト値: 10

4. [**保存**] をクリックします。
5. [スケジュールに入れる] を選択すると、スケジュール設定を編集するかどうかを確認する画面が表示されます。[**OK**] をクリックします。[**キャンセル**] をクリックすると、保存された検索またはアラートは作成されません。
6. スケジュールオプションを適切に設定します。これらのオプションの詳細については、「日付と時刻のスケジュールのオプション」(150ページ) を参照してください。
7. スケジュールされた保存された検索に関して、必要なオプションを選択します。パラメーターの詳細については、「検索ジョブのオプション」(340ページ) を参照してください。
8. スケジュールされたアラートに関して、必要なオプションを選択します。パラメーターの詳細については、「アラートジョブのオプション」(342ページ) を参照してください。
9. [**保存**] をクリックします。

システムフィルター/事前定義フィルター

Loggerには、いくつかの定義済みファイルター (システムフィルターとも呼びます) が付属しています。これらのフィルターでは、よく検索されるイベントが定義されています。たとえば、成功しなかったログイン試行やソースごとのイベントなどです。フィルタークエリは、統合クエリおよび正規表現クエリとして使用できます。統合クエリは検索とレポート生成で使用できますが、正規表現クエリはアラートと転送者を定義するためのものです。

注: ファイアウォールまたはUNIXサーバーユースケースフィルター (次の表に示します) を効果的に使用するには、関心のあるファイアウォールデバイスまたはUNIXサーバーを含むデバイスグループを定義し、それらのデバイスグループに検索を制約します。デバイスの種類に固有のデバイスグループを作成しないと、検索結果は、ファイアウォールデバイスのみではなく、すべてのデバイスからのすべてのDeny、Drop、またはPermitイベントに一致しま

す。同様に、「Unix - IO エラーおよび警告」フィルターには、UNIXサーバーのみではなく、すべてのデバイスからのIOエラーと警告が含まれます。

以下に、すべてのシステムフィルターのリストを示します。各フィルターの説明については、「システムフィルター」(687ページ)を参照してください。

定義済みのシステムフィルターを使用するには、「保存済みクエリでの検索」(149ページ)の手順に従ってください。

注: [システムアラート] カテゴリのフィルター (次の表の最後のセクションに記載されています) がソフトウェアLoggerのユーザーインターフェイスに表示されている場合でも、これらのフィルターは適用されません。

システムフィルター

カテゴリ	統合クエリフィルター	正規表現クエリフィルター
Login Status use case	All Logins	All Logins (Non-CEF) All Logins (CEF format)
	Unsuccessful Logins	Unsuccessful Logins (Non-CEF) Unsuccessful Logins (CEF format)
	Successful Logins	Successful Logins (Non-CEF) Successful Logins (CEF format)
	Failed Logins	
Configuration	Configuration Changes	System configuration changes (CEF format)
Events use case	High and Very High Severity Events	High and Very High Severity CEF events
	Event Counts by Source	
	Event Counts by Destination	
		All CEF events
Intrusion use case	Malicious Code	Malicious Code (CEF format)
Firewall use case	Deny (Firewall Deny)	
	Drop (Firewall Drop)	
	Permit (Firewall Permit)	
Network use case	DHCP Lease Events	
	Port Links Up and Down	

システムフィルター (続き)

カテゴリ	統合クエリフィルター	正規表現クエリフィルター
	Protocol Links Up and Down	
Connector System Status use case	CPU Utilization by Connector Host	
	Disk Utilization by Connector Host	
	Memory Utilization by Connector Host	
UNIX Server use case	CRON related events	
	IO Errors and Warnings	
	PAM and Sudo Messages	
	Password Changes	
	SAMBA Events	
	SSH Authentications	
	User and Group Additions	
	User and Group Deletions	
Windows Events use case	Account Added to Global Group Account Added to Global Group (CEF)	
	Audit Policy Change Audit Policy Change (CEF)	
	Change Password Attempt Change Password Attempt (CEF)	
	Global Group Created Global Group Created (CEF)	
	Logon Bad User Name or Password Logon Bad User Name or Password (CEF)	
	Logon Local User Logon Local User (CEF)	

システムフィルター (続き)

カテゴリ	統合クエリフィルター	正規表現クエリフィルター
	Logon Remote User Logon Remote User (CEF)	
	Logon Unexpected Failure Logon Unexpected Failure (CEF)	
	New Process Creation New Process Creation (CEF)	
	Pre-Authentication Failure Pre-Authentication Failure (CEF)	
	Special Privileges Assigned to New Logon Special Privileges Assigned to New Logon (CEF)	
	User Account Changed User Account Changed (CEF)	
	User Account Password Set User Account Password Set (CEF)	
	Windows Events (CEF)	
System Alerts	以下のフィルターは、特別な内部ストレージグループにCEF形式で書き込まれている、特定の内部アラートイベントを検索します。**これらのフィルターは、両方の検索方法で使用できます。**以下のフィルターに加えて、「システムヘルスイベント」(551ページ) に示すシステムヘルスイベントに基づき、独自のアラートを定義できます。 **注:** これらのフィルターはソフトウェアLoggerに表示されますが、適用はされません。	
	CPU Utilization Above 90 Percent	CPU Utilization Above 90 Percent
	CPU Utilization Above 95 Percent	CPU Utilization Above 95 Percent
	Disk Failure	Disk Failure
	Root Partition Below 10 Percent	Root Partition Below 10 Percent
	Root Partition Below 5 Percent	Root Partition Below 5 Percent
	Device Configuration Changes	Device Configuration Changes

システムフィルター (続き)

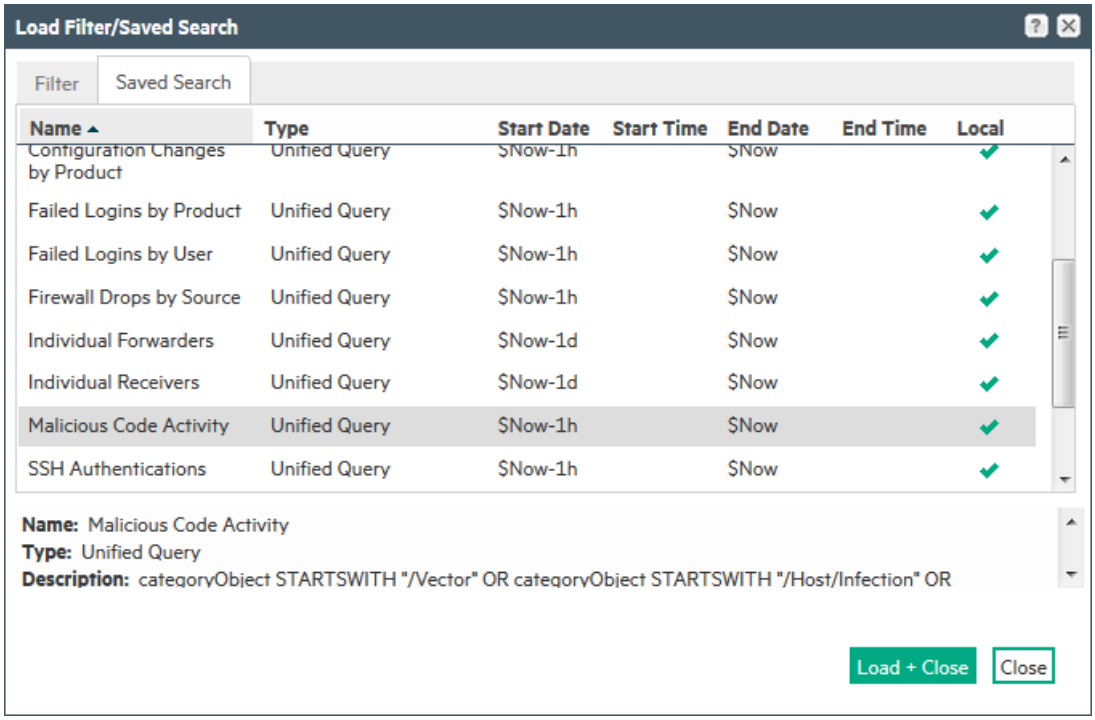
カテゴリ	統合クエリフィルター	正規表現クエリフィルター
	Filter Configuration Changes	Filter Configuration Changes
	High CPU Temperature	High CPU Temperature
		Bad Fan
	Power Supply Failure	Power Supply Failure
	RAID Controller Issue	RAID Controller Issue
	RAID Status Battery Failure	RAID Status Battery Failure
	RAID Status Disk Failure	RAID Status Disk Failure
	Storage Configuration Changes	Storage Configuration Changes
	Storage Group Usage Above 90%	Storage Group Usage Above 90%
	Storage Group Usage Above 95%	Storage Group Usage Above 95%
	Zero Events Incoming	Zero Events Incoming
	Zero Events Outgoing	Zero Events Outgoing

保存済みクエリでの検索

ユーザーが作成したフィルターと保存された検索および定義済みのシステムフィルターを使用して検索することができます (「システムフィルター/事前定義フィルター」(145ページ) を参照)。

既存のクエリを使用するには

1. [**分析**] メニューを開き、[**検索**] をクリックします。
2. 以下のいずれかの方法を使用して、目的のフィルター、システムフィルター、または保存された検索を選択します。
   - 検索テキストボックスに`$filter$`または`$ss$`と入力し、ドロップダウンリストからフィルターまたは保存された検索を選択します。詳細については、「自動補完を通じてフィルターと保存された検索を開く」(104ページ) を参照してください。
   - [保存されているフィルターの読み込み] アイコン () をクリックし、すべての保存されたフィルターまたは保存された検索の一覧を表示し、下図に示す [フィルター/保存された検索をロード] インターフェイスを表示します。



[フィルター/保存された検索をロード] インターフェイスを使用すると、保存されたフィルタークエリと保存された検索クエリを素早く見つけることができます。情報をソートするには、いずれかの列名をクリックします。フィルターまたは保存された検索の詳細を表示するには、その行をクリックします。下のテキストボックスに詳細が表示されます。

フィルターをロードするには、使用するフィルターまたは保存された検索を選択し、[**読み込み+クローズ**] をクリックします。フィルター行に検索クエリが表示されます。

保存されたクエリをロードするには、[**保存された検索**] ページを開き、検索を選択し、[**読み込み+クローズ**] をクリックします。

日付と時刻のスケジュールのオプション

ヒント: スケジュールを設定する前に、「時刻/NTP」(497ページ) に記載されている内容を十分に確認してください。

上のプルダウンメニューから、[毎日]、[曜日]、[日付] のいずれかを選びます。

注: 複数の日を指定する場合は、コンマで区切ります。時刻を指定する場合は、24時間形式を使用します。

1. [**毎日**] の場合は、下のプルダウンメニューから以下のオプションのいずれかを選択し、必要な値を入力します。
   - **時刻**: (0～23) [時] フィールドにタスクを実行する時刻 (24時間形式) を入力します。夜の12時はゼロ (0) で表します。

- **毎**: 右端のプルダウンメニューから [時] または [分] を選択し、タスクを実行する間隔を指定します。
- **時**: (1～23) タスクを実行する間隔 (時間) を入力します。結果は、毎日n時間間隔で実行されるスケジュールになります。
  分: (15～59) タスクを実行する間隔 (分) を入力します。結果は、毎日n分間隔で実行されるスケジュールになります。

2. [**曜日**] の場合は、下のプルダウンメニューから以下のオプションのいずれかを選択し、必要な値を入力します。
   - **日**: (1～7) タスクを実行する曜日を選択します (日曜日=1、月曜日=2など)。
   - **時刻**: (0～23) 右側のテキストフィールドに、タスクを実行する時刻を入力します。0は夜の12時を表します。
   - **毎**: 右端のプルダウンメニューから [時] または [分] を選択し、タスクを実行する間隔を指定します。
     時: (1～23) タスクを実行する間隔 (時間) を入力します。結果は、選択した日にn時間間隔で実行されるスケジュールになります。
     分: (15～59) タスクを実行する間隔 (分) を入力します。結果は、選択した日にn分間隔で実行されるスケジュールになります。
3. [**日付**] の場合は、下のプルダウンメニューから以下のオプションのいずれかを選択し、必要な値を入力します。
   - **日**: (1～31) タスクを実行する1つまたは複数の日付を入力します。

     注: 1か月の日数は月によって異なります。スケジュールされたタスクは、その月に指定された日付が存在する場合にのみ実行されます。31日にスケジュールされたタスクは、2月、4月、6月、9月、11月には実行されません。29日にスケジュールされたタスクは、うるう年の2月にのみ実行されます。
   - **時刻**: (0～23) タスクを実行する時刻を入力します。(このオプションで、[毎] を選択することはできません。)

例

- スケジュールされたジョブを毎日45分おきに実行するには、上の [スケジュール] プルダウンメニューで [**毎日**] を選択します。下のプルダウンメニューから [**毎**] を選択し、テキストボックスに「**45**」と入力して、[**分**] を選択します。
- スケジュールされたジョブを火曜日と木曜日に4時間おきに実行するには、上の [スケジュール] プルダウンメニューから [**曜日**] を選択し、[**日**] として「**3,5**」を入力します。次に、下のプルダウンメニューから [**毎**] を選択し、テキストボックスに「**4**」を入力します。
- スケジュールされたジョブを毎月14日の午前3時に実行するには、上の [スケジュール] プルダウンメニューから [**日付**] を選択し、[**日**] として「**14**」を入力します。次に、下のプルダウンメ

ニューから**[時刻]**を選択し、テキストボックスに**「3」**を入力します。(スケジュールされたジョブを午前3時と午後3時に実行する場合は、「3,15」と入力します。)

静的相関関係を通じたLoggerデータの強化

lookup検索演算子では、外部ファイルからのデータを使用してLoggerのデータを強化できます。これにより、静的相関関係を通じたジオタグ付け、資産タグ付け、ユーザー識別などが可能となります。

lookup演算子を使用して、Loggerに保存されている元のデータに含まれていない情報を検索結果に追加できます。そのためには、データが格納された外部ファイルを作成し、そのルックアップファイルをLoggerにアップロードし、lookup演算子を使用してLoggerイベントとアップロードしたルックアップファイルを結合します。

たとえば、Loggerの検索結果にソースIPアドレスがある国を含める場合、IPアドレスと国の一覧を記載したファイルを作成し、そのファイルをLoggerにルックアップファイルとしてアップロードできます。その後、lookup演算子を使用してLoggerイベントのsourceAddressフィールドとルックアップファイルのIPアドレス列を結合し、検索結果に国を表示できます。

- Lookupファイルの作成とLoggerへのアップロードについては、「ルックアップファイル」(357ページ)を参照してください。
- 検索時にlookup演算子を使用する方法については、「lookup」(580ページ)を参照してください。

インデックス作成

Loggerを初期化すると、自動的なイベントのスキャンとそのイベントのインデックス作成が開始されます。

Loggerのストレージテクノロジーでは、次の3つの方法でイベントの自動インデックス作成が可能です。

- 全文インデックス作成: 各イベントがトークン化されてインデックス作成されます。「全文インデックス作成 (キーワードインデックス作成)」(153ページ)を参照してください。
- フィールドベースのインデックス作成: イベントフィールドは、あらかじめ決められたスキーマに基づいてインデックス作成されます。「フィールドベースのインデックス付け」(153ページ)を参照してください。
- スーパーインデックス作成: 出現頻度の少ないフィールド値を素早く検索できるように、特定のイベントフィールドにスーパーインデックスが作成されます。「スーパーインデックス作成」(155ページ)を参照してください。

初期化後に受信されたすべてのイベントは、全文検索用にインデックスが作成され、デフォルトのフィールドセットはフィールドベースの検索用にインデックスが作成されます。また、デフォ

ルトのフィールドセットは、大量のデータから出現頻度の少ない値を素早く検索するためにスーパーインデックスが作成されます。

すべてのイベントのタイムスタンプには、Loggerで受信したときの受信時刻が設定されます。デフォルトのフィールドは自動的にインデックス作成されます。残りのフィールドについて、Loggerはイベントの受信時刻と、フィールドがインデックスに追加された時刻を使用して、そのイベントのインデックスを作成するかどうかを判定します。イベントの受信時刻が、フィールドがインデックスに追加された時刻と同じかそれよりも後の場合は、イベントのインデックスが作成されます。そうでない場合は作成されません。

注: アーカイブを作成する際に、インデックス作成情報はアーカイブされません。アーカイブの作成後に、アーカイブにインデックス作成情報を追加することができます。詳細については、「アーカイブされたイベントのインデックス付け」(441ページ) を参照してください。

全文インデックス作成 (キーワードインデックス作成)

全文インデックス作成では、Loggerで受信された各イベント (CEFまたは非CEF) がスキャンされ、キーワードに分割されてLoggerに保存されます。イベントがトークン化される方法は、全文検索オプションで制御されます (「グローバル検索オプション」(349ページ) を参照)。

フィールドベースのインデックス付け

フィールドベースのインデックス作成機能では、イベントのフィールドにインデックスを作成できます。フィールドは、あらかじめ決められたスキーマに基づいています。Loggerのレポートとフィールド検索処理では、これらのインデックスが作成されたフィールドを利用して、検索とレポート作成のパフォーマンスを大幅に向上させています。

推奨されるフィールドセットに対するフィールドベースのインデックス作成は、Loggerの初期化時に自動的に有効になります。フィールドはいつでもインデックスに追加できます (手順については、「フィールドベースのインデックスにフィールドを追加するには」(347ページ) を参照してください)。一度追加したフィールドは削除できません。

デフォルトのインデックスフィールドの一覧と、それぞれのフィールドの説明は、Loggerの [設定] メニューから利用できます。デフォルトのLoggerスキーマフィールドを表示する方法については、「デフォルトのフィールド」(354ページ) を参照してください。

注: HPEでは、検索クエリとレポートクエリで使用するフィールドのインデックスを作成することを強くお勧めします。

定義済みまたはユーザー定義のrexパーサーが非CEFイベントを解釈するときに作成されるフィールドは、フィールドベースのインデックス作成機能を使用してインデックス作成できません。rexパーサーの詳細については、「パーサー」(392ページ) を参照してください。

Loggerでは、フィールドベースのインデックス作成リストに含まれているフィールドにインデックスを作成するほかに、すべてのイベントのイベントメタデータフィールド (イベント時刻、Loggerの受信時刻、デバイスアドレス) にもインデックスを作成します。イベントメタデータフィールドは、「内部」フィールドとも呼ばれます。

インデックス作成では以下のフィールドを使用できます。Loggerの初期化後に、Loggerによって自動的にインデックス作成が開始されるフィールドは、太字フォントで示してあります。

注: Logger 6.4 (ADP 2.6) 以降のリリースは、`requestUrl`フィールドのインデックス付けをサポートします。このフィールドは、World Wide WebからWebサイトアドレスを返します。`requestUrl`をインデックス付けすると、結果を返すまでにかかる時間を短縮できますが、検索結果のサイズが大幅に増加するので、検索ストレージ容量に影響を及ぼす可能性があります。

インデックスフィールド		
agentAddress	deviceCustomDate2	flexDate1Label
agentHostName	deviceCustomDate2Label	**filePath**
agentNtDomain	**deviceCustomNumber1**	flexNumber1
agentSeverity	deviceCustomNumber1Label	flexNumber1Label
agentType	**deviceCustomNumber2**	flexNumber2
agentZone	deviceCustomNumber2Label	flexNumber2Label
agentZoneName	**deviceCustomNumber3**	flexString1
agentZoneResource	deviceCustomNumber3Label	flexString1Label
agentZoneURI	**deviceCustomString1**	flexString2
applicationProtocol	deviceCustomString1Label	flexString2Label
baseEventCount	**deviceCustomString2**	message
bytesIn	deviceCustomString2Label	**name**
bytesOut	**deviceCustomString3**	**priority**
categoryBehavior	deviceCustomString3Label	requestClientApplication
categoryDeviceGroup	**deviceCustomString4**	requestContext
categoryObject	deviceCustomString4Label	requestMethod
categoryOutcome	**deviceCustomString5**	requestUrl
categorySignificance	deviceCustomString5Label	requestUrlFileName
categoryTechnique	**deviceCustomString6**	requestUrlQuery
customerName	deviceCustomString6Label	sessionId
destinationAddress	**deviceEventCategory**	**sourceAddress**

インデックスフィールド		
destinationDnsDomain	**deviceEventClassId**	**sourceHostName**
destinationHostName	deviceExternalId	sourceMacAddress
destinationMacAddress	**deviceHostName**	**sourceNtDomain**
destinationNtDomain	deviceInboundInterface	**sourcePort**
destinationPort	deviceOutboundInterface	**sourceProcessName**
destinationProcessName	**deviceProduct**	sourceServiceName
destinationServiceName	deviceReceiptTime	sourceTranslatedAddress
destinationTranslatedAddress	deviceSeverity	**sourceUserId**
destinationUserPrivileges	**deviceVendor**	**sourceUserName**
destinationUserId	**deviceVersion**	sourceUserPrivileges
destinationUserName	deviceZone	sourceZone
destinationZone	deviceZoneName	sourceZoneName
destinationZoneName	deviceZoneResource	sourcezoneResource
destinationZoneResource	**deviceZoneURI**	**sourceZoneURI**
destinationZoneURI	**endTime**	startTime
deviceAction	**eventId**	**transportProtocol**
deviceAddress	externalId	type
deviceCustomDate1	**fileName**	vulnerabilityExternalID
deviceCustomDate1Label	flexDate1	vulnerabilityURI

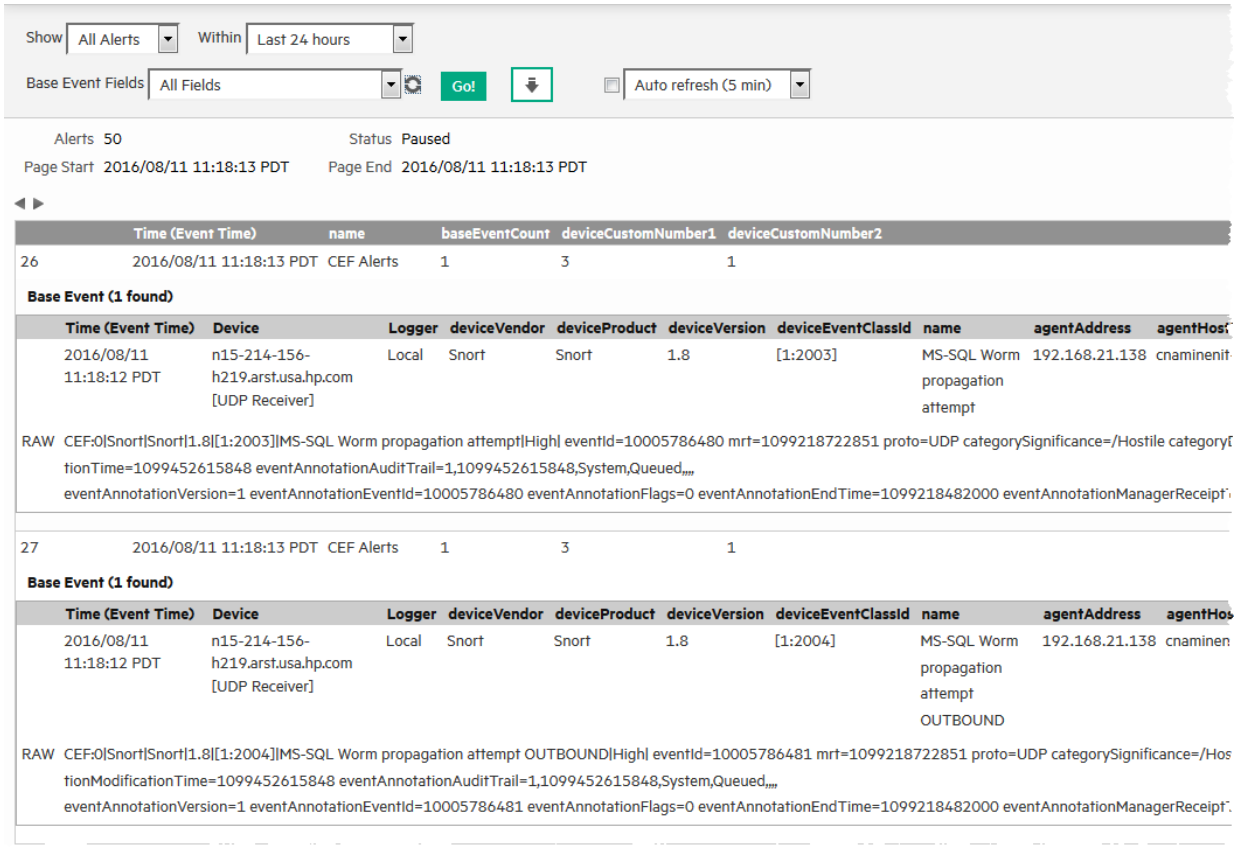
スーパーインデックス作成

全文インデックス作成とフィールドベースインデックス作成に加えて、Logger以降では、一般的なIPアドレス、ホスト名、ユーザー名フィールドに対してスーパーインデックスが作成されます。スーパーインデックスを使用すると、Loggerは、特定のフィールド値がこのLoggerに格納されているかどうかを素早く決定できます。格納されていれば、そのフィールド値が存在するデータセクションに検索を絞り込むことができます。そのため、ヒットしない場合、スーパーインデックスを利用する検索は非常に高速に結果が返され、ヒット数が非常に少ない場合は通常の検索よりも高速に結果を返します。

- スーパーインデックスの使用方法については、「出現頻度の少ないフィールド値の検索」(117ページ)を参照してください。
- スーパーインデックスが作成されるフィールドの完全な一覧は、「スーパーインデックスフィールドを使用した検索速度の向上」(117ページ)にあります。

アラートの表示

特定のクエリに一致する新しいイベントを受信した場合や、指定された数の一致が所定の時間しきい値内に発生した場合に、電子メール、SNMPトラップ、またはSyslogメッセージでアラートを起動するようにLoggerを設定できます。詳細については、「Loggerアラートの種類」(412ページ)を参照してください。電子メール、SNMPトラップ、またはSyslogメッセージでアラートを受信するのに加えて、**[分析] > [アラート]** ページでアラートとそれを起動したベースイベントを表示することもできます。



アラートを表示するには、「過去の2時間」や「本日」などの定義済みの時間範囲を選択するか、「カスタム時間範囲」を選択して、手動で時間範囲を指定するための追加フィールドを表示します。この点は [検索] と同様です。詳細は「時間範囲」(79ページ)を参照してください。

アラートを作成したら、名前を入力します。特定のアラートに関連付けられているイベントのみを表示するには、**[表示 (Show)]** オプションを使用します。デフォルトは [すべての警告 (All Alerts)] です。

「Action Engine」というラベルが付いたイベントはアラートイベントです。アラートを起動したイベントはベースイベントです。また、**[ベース イベント フィールド (Base Event Fields)]** オプションを

使用して、ベースイベントを表示するかどうか、およびどのフィールドを表示するかを指定することもできます。

[検索] ページと同様に、[**実行**] ボタンで検索を実行し、[**結果のエクスポート**] ボタンで検索結果を含むPDFまたはCSVファイルを作成し、[**自動リフレッシュ**] オプションで検索結果の表示の更新の有無と頻度を設定できます。

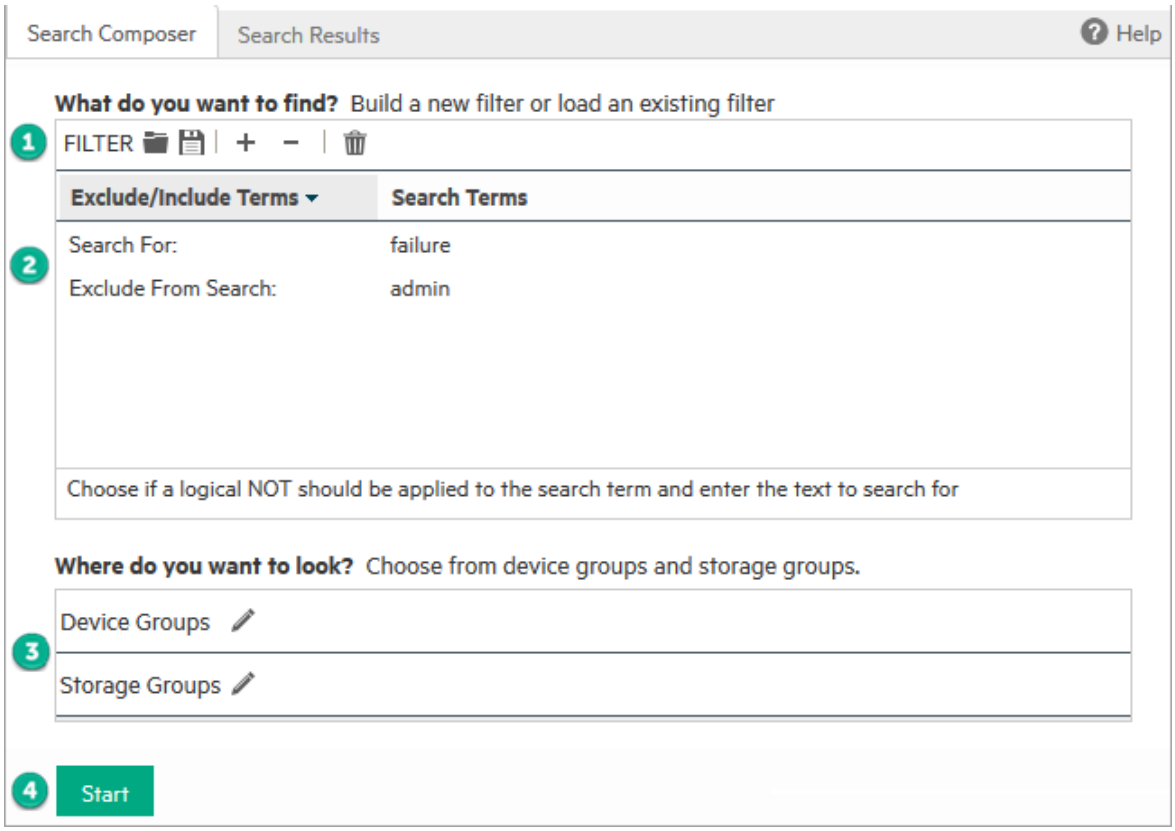
ライブイベントビューアー

ライブイベントビューアーは、指定した条件に一致する受信イベントをリアルタイムに表示します。この機能は、イベントを素早く表示することが重要な環境で便利です。たとえば、金融機関では、特定のトランザクションタイプが発生したらすぐに表示することに関心がある可能性があります。イベントがLoggerに到着してから表示されるまでの遅延が非常に少ないため、表示前にLoggerでインデックス作成されていない可能性があります。

ライブイベントビューアーは、[検索設定] と [検索結果] の2つのタブからなります。[検索設定] は検索条件を定義するためのものであり、[検索結果] タブには、一致イベントがリアルタイムに表示されます。

下図は [検索設定] を示しています。複数の検索項を指定すると、最終的なクエリではAND演算子を使用して項が結合されます。たとえば、最初の検索項で「failure」を検索し、2番目の項で「admin」を**除外する**場合、最終的なクエリは「failure AND NOT admin」となります。

検索設定

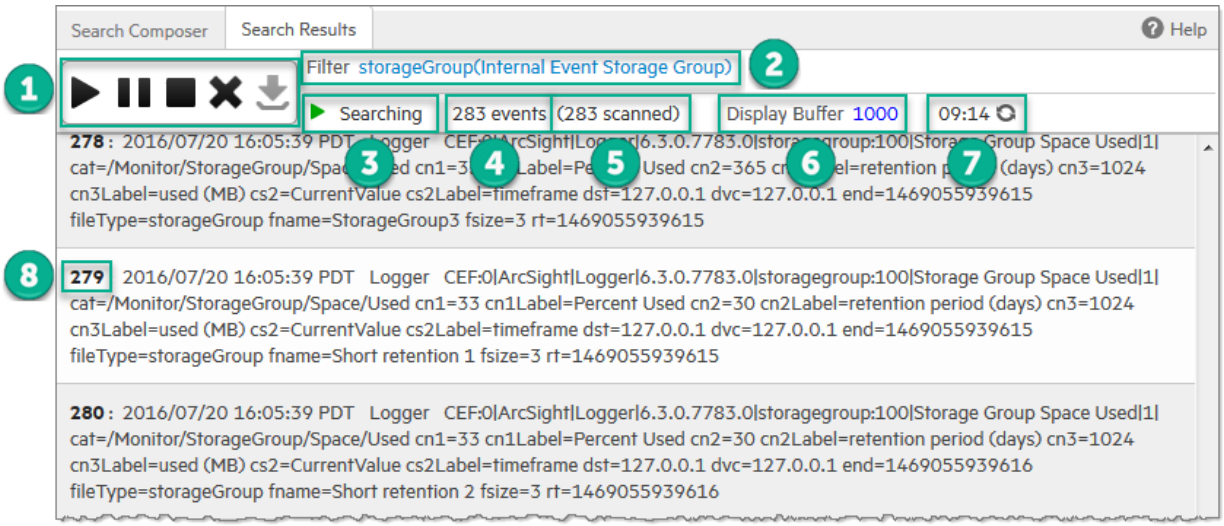


検索設定の凡例

機能	説明	機能	説明
1	保存されているフィルターの読み込み 現在のフィルターの保存 フィルター行の追加 フィルター行の削除 全フィルターの削除	3	デバイスグループの指定 ストレージグループの指定
2	検索条件の入力	4	ライブイベントビューアーの開始または停止

[検索結果] タブには、[再生]、[一時停止]、[停止]、[クリア]、[エクスポート] の各ボタンがあり、電子機器と同様の方法で表示を制御できます (下図を参照してください)。

[検索結果] タブ



検索結果の凡例

機能	説明	機能	説明
1	再生/一時停止/停止/削除/エクスポート	5	これまでにスキャンされたイベント
2	検索設定で指定されたフィルター	6	イベント表示の最大値
3	現在の状態	7	検索タイマー
4	これまでに見つかったイベント	8	一致したイベント数

次のリストでは、[検索結果] 表示の機能のうち主なものについて説明します。

- イベントはrawイベント形式で表示され、検索クエリを実行した場合の [検索結果] ページ (**[分析] > [検索]**) のような列、表形式では表示されません。
- ユーザーが起動できるライブイベントビューアーは最大で1つです。Loggerで一度に実行できるライブイベントビューアーの最大数は5です。
- 一致イベントを識別するために、正規表現検索方法が使用されます。そのため、[検索設定] で、検索項として正規表現を指定できます。
- バッファーサイズは、ビューアーに表示するイベントの最大数を定義します。バッファーサイズのデフォルト値は1000ですが、20～5000の間の任意の数に設定できます。
- デフォルトでは、検索は15分間実行され、システムリソースを節約するために停止します。検索を15分以上実行する必要がある場合は、カウントダウンタイマーの横にあるアイコンをクリックし、タイマーを15分にリセットします。
- [一時停止] をクリックすると、[検索結果] の表示が止まります。ただし、検索処理はバックグラウンドで継続され、新しい一致イベントはバッファーに格納されます。バッファーへの格

納が停止する条件は、最大で1000個のイベントがバッファーに格納されるか、[検索結果]の表示を止めてもカウントダウンし続ける検索タイマーが00:00になることです。

- タイマーが00:00になっていない場合は、[再生]をクリックして一時停止した検索処理を再開できます。[再生]をクリックすると、バッファーに格納されたイベントが表示されます。[検索結果]表示画面では、新たに見つかったイベントが以前見つかったイベントに追加されます。
- [停止]をクリックすると、一致イベントの検索と検索タイマーのカウントダウンが停止します。[再生]をクリックすると、検索が最初から開始されます。現在表示されているイベントは[検索結果]画面からクリアされ、検索タイマーは15分にリセットされ、検索が再度開始されます。
- 一致イベントをエクスポートするには、検索処理を停止する必要があります。

ライブイベントビューアーを起動するには

注: ライブイベントビューアーは、リソースを大量に消費するアプリケーションであり、長時間実行すると、Loggerの全体的なパフォーマンスに影響を与えかねません。そのため、この機能は、実行する時間を選び、短い時間だけ使用してください。

1. [**分析**]メニューを開き、[**ライブイベントビューアー**]をクリックします。
2. [検索設定]タブで、検索項を入力するか、(📁) アイコンをクリックして保存されたフィルターを選択します。

   イベントに含まれている必要がある検索 ([検索対象:]) 項を入力するか、イベントに含まれていてはならない項 ([検索対象から除外:]) を入力できます。[検索対象:]フィールドをクリックしてドロップダウンリストを表示し、そこから[検索対象から除外:]を選択できます。

   複数の検索項を指定すると、LoggerはAND演算子を使用してそれらを結合し、最終的な検索クエリを作成します。

   - 検索項を追加するには、(+) アイコンをクリックします。
   - 検索項を削除するには、(−) アイコンをクリックします。
   - すべての検索項を削除するには、(🗑) アイコンをクリックします。
3. 検索を特定のデバイスグループ、デバイス、ストレージグループに制限する制約を、[どこで探しますか?] セクションに入力します。✎アイコンをクリックして表示されるリストから制約を選択できます。
4. **[開始]**をクリックします。
5. 検索結果は[検索結果]表示画面に自動的に表示されます。

ライブイベントビューアークエリを更新するには

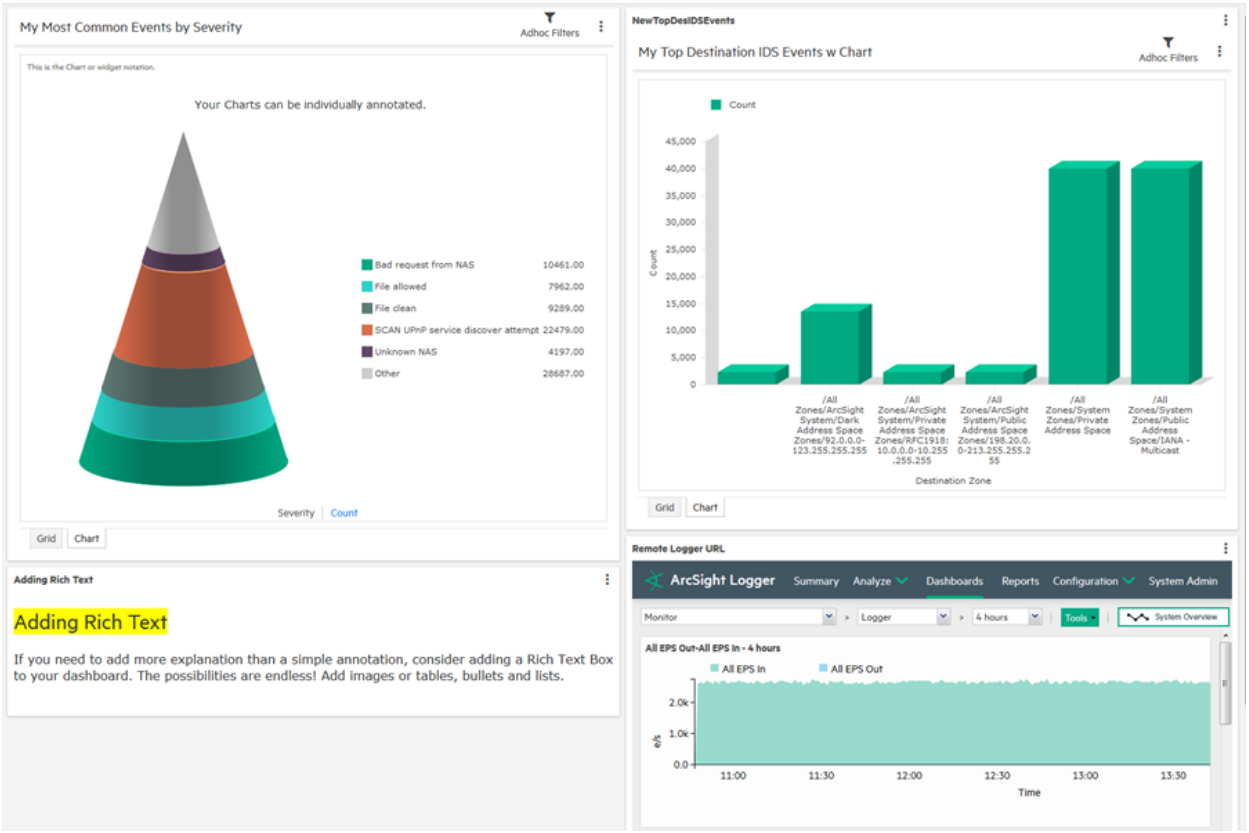
1. ライブイベントビューアーの [検索設定] タブで、検索項を更新します。
2. まず [**停止**] をクリックし、次に [**開始**] をクリックして新しい検索項を使用した検索を開始します。

[検索結果] 表示をエクスポートするには

1. 必ずライブイベントビューアーを停止します。そのために、[検索結果] 表示ウィンドウの■アイコンをクリックします。
2. アイコンをクリックして [エクスポートオプション] ウィンドウを表示します。
3. 表示されている検索結果をエクスポートするには、「検索結果をエクスポートするには」(139ページ) の説明に従って、エクスポートオプションを選択し、[**エクスポート**] をクリックします。

第4章：レポート

レポートは、ネットワークセキュリティの状態を内外の関係者に伝えるうえで不可欠なツールです。レポートは、イベントをキャプチャーしたビューまたはサマリーです。レポートは、Logger内で表示することも、エクスポートして各種ファイル形式で共有することもできます。



管理の必須条件

ユーザーがレポートの作成と表示を行う前に、Logger管理者は以下のタスクを行う必要があります。

- ユーザーとユーザーグループにアクセス権を割り当てます。「アクセス権限の割り当て」(163ページ) を参照してください。
- レポート管理設定の一つであるデータベース接続タイムアウト値の調整が必要になる場合があります。「実行に長い時間がかかるレポートのタイムアウト値の調整」(164ページ) を参照してください。

  注: ご使用のLoggerで、有効なスタンドアロンライセンスまたはADP Loggerライセンスを実行する必要があります。これらのライセンスがない場合、レポートは使用できません。

管理レポートツールとオプションのリストについては、「レポート管理」(304ページ) を参照してください。

アクセス権限の割り当て

管理者は、さまざまなレポートカテゴリ、レポート、レポートオプション (表示、発行、編集) に対し、ユーザーロールとLoggerレポートグループの所属に基づいてアクセス権を設定できます。たとえば、一部のレポートを表示できてもレポートを表示する権限はない、レポートを表示できてもスケジュール設定や公開はできない、レポートの表示とスケジュール設定はできても編集はできないというように、権限を付与することができます。

レポートオプションとユーザーグループのアクセス権限は、[システム管理] メニューの **[ユーザ管理]** リンクで設定し、管理します。システム管理ユーザーとグループの管理の詳細については、「Loggerのユーザー権限の設定」(546ページ) を参照してください。

必要なアクセス権限

アクセス権限はフォルダーレベルで付与します。特定のレポートにアクセスするには、レポートのパスに含まれるすべての上位レベルフォルダーへのアクセス権限が必要です。

たとえば、あるユーザーがUser Trackingレポート (**[Foundation] > [侵入モニタリング] > [User Tracking]**) へのアクセスを必要とする場合、User Trackingだけでなく、[Foundation] ノードと [侵入モニタリング] ノードへのアクセス権限もそのユーザーに付与する必要があります。

一部のユーザーのアクセスをレポートの一部に限定しなければならない場合があります。

- 特定のレポートカテゴリへのアクセスを必要とするユーザーがいる場合、そのカテゴリのみのアクセス権限を持つユーザーグループを作成し、そのユーザーグループにユーザーを割り当てます。「レポートユーザーグループの作成」(304ページ) を参照してください。
- 特定のレポートへのアクセスを必要とするユーザーがいる場合、必要なレポートのみを格納した新しいカテゴリフォルダーを作成し、そのフォルダーへのアクセス権限を該当ユーザーに付与します。「レポートカテゴリ」(308ページ) を参照してください。

実行に長い時間がかかるレポートのタイムアウト値の調整

実行に長い時間がかかるレポートに影響を与えるタイムアウト値は2つあります。

- **クライアントタイムアウト**は1時間です。アドホックレポートの実行に1時間以上かかる場合、実行はタイムアウトします。代わりにスケジュールレポートを使用してください。
- スケジュールレポートのデフォルトの**データベース接続タイムアウト**は4時間です。スケジュールレポートの実行に4時間以上かかる場合は、データベース接続タイムアウトを [レポートの設定] ページで長くすることができます。「レポートの設定」(305ページ) を参照してください。

大きいレポートをバックグラウンドでの実行に限定するオプションもあります。「長いレポートをバックグラウンドでの実行に限定する方法」(194ページ) を参照してください。

レポートのユーザーインターフェイス

今回のリリースでは、Loggerレポートの更新、改善、拡張が行われました。複数のタブ、新しいツール、表示オプションなどの新しい要素により、レポートの操作性が向上します。

タブによるマルチタスク

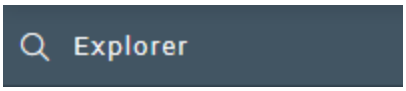
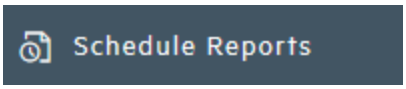
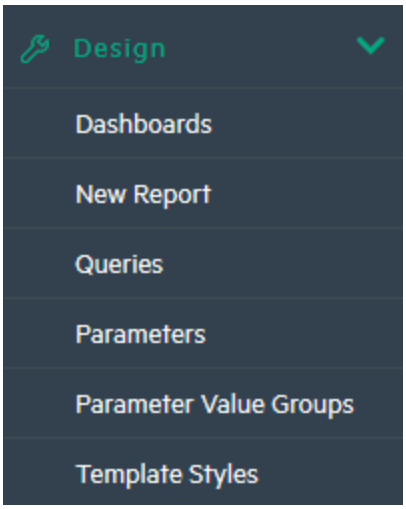
レポートアクティビティがタブ内に表示されるようになりました。Loggerではレポートのタブを最大10個開くことができるため、レポートの作成、管理、生成の際に、ある画面から別の画面に簡単に移動することができます。

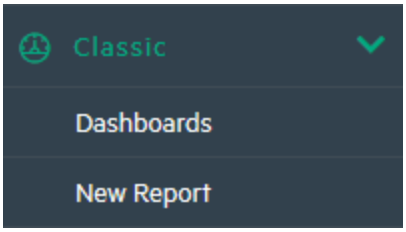
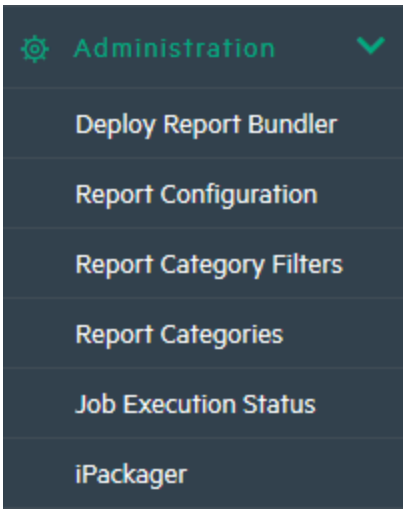
- 最初のタブは **[最近のレポート]** で、これがレポートのホームページです。このタブは閉じません。「[レポート] ホームページ」(167ページ) を参照してください。
- レポート、ダッシュボード、クエリ、他のレポート機能を別々のタブで同時に実行することができます (ただし、Loggerのパフォーマンスに影響する場合があります)。「レポート実行のベストプラクティス」(192ページ) を参照してください。

レポートのメニュー

レポートのメニューを使用すると、レポート内のどのタブやページからでもすべてのレポートツールに簡単にアクセスすることができます。

注: これらのツールへのアクセス権限を管理者から付与されている必要があります。「管理の必須条件」(163ページ)を参照してください。

メニューセクション	説明
	**[エクスプローラー (Explorer)]** は、目的のレポート、クエリ、パラメーター、ダッシュボード、ダッシュボードウィジェット、お気に入り項目に移動するために使用します。Loggerの以前のリリースには、カテゴリまたはオブジェクト別に1つずつ、計5種類のエクスプローラーがありました。今回のリリースから、このメニューを使用してすべてのレポートまたはオブジェクトにアクセスできます。「レポートエクスプローラー」(171ページ)を参照してください。
	**[スケジュール報告 (Schedule Reports)]** では、システムの負荷が低いときに、または一定の間隔でレポートを実行することができます。また、通常の実行では1時間でタイムアウトしてしまうレポートを実行できます。レポートジョブのスケジューリングの一部として、配布オプションを、たとえば結果レポートのメール送信、保存、公開のいずれかに設定できます。「スケジュールレポート」(185ページ)を参照してください。
	**[デザイン (Design)]** ツールは、レポートを構成する各種「オブジェクト」の作成とカスタマイズに使用します。 以下の新しいツールが追加されました。 • **ダッシュボード (Dashboards)**: アドホックダッシュボードだけでなく、スマートダッシュボードも簡単に作成できます。スマートダッシュボードでは、別々のクエリを使用する複数のグラフを表示できます。「ダッシュボードの作成」(252ページ)を参照してください。 • **新しいレポート (New Report)**: デフォルトレポートや公開済みレポートを使用して新しいレポートを作成したり、一から新しいレポートを作成したりします。[スマートビュー] ページを使用すると、目的の作業を実行する場所に移動できます。 以下は、Loggerの従来のツールです。 • **クエリ (Queries)**: レポートを強化するクエリを作成し、編集します。「クエリ」(262ページ)を参照してください。 • **パラメータ (Parameters)**: レポートクエリのデータ値を定義するパラメーターを作成し、編集します。「パラメーター」(292ページ)を参照してください。 • **パラメータ値グループ (Parameter Value Groups)**: パラメーター値のグループを作成し、編集します。レポートの実行時に簡単に値を適用できるようになります。「パラメーター値グループ」(300ページ)を参照してください。

メニューセクション	説明
	• **テンプレートのスタイル (Template Styles)**: レポートテンプレートのスタイルを作成してカスタマイズし、独自の外観を与えます。「テンプレートスタイル」(302ページ)を参照してください。
	**[クラシック (Classic)]** ツールは、Loggerを従来から使用しているユーザー向けのツールです。使い慣れたアドホックデザイナーやアドホックダッシュボードのツールを使用して、ダッシュボードとレポートを作成し、カスタマイズすることができます。 • **新しいレポート (New Report)**: 使い慣れた従来のインターフェイスであるアドホックレポートデザイナーを使用して、スマートレポートやアドホックレポートを作成し、カスタマイズします。既存のレポートを土台にして新しいレポートを作成することも、自分で新しいレポートを作成することもできます。「クラシック: アドホックレポートデザイナー」(233ページ)を参照してください。 • **ダッシュボード (Dashboards)**: アドホックダッシュボードの作成、表示、管理、保守を行います。「クラシックダッシュボード」(254ページ)を参照してください。 **注:** クラシックダッシュボードは、スマートレポートとアドホックレポート両方のウィジェットをサポートしますが、1つのダッシュボードには1つのクエリオブジェクトしか含めることができません。スマートダッシュボードを作成する手順については、「ダッシュボードの作成」(252ページ)を参照してください。
	**[管理 (Administration)]** ツールは、Loggerレポート環境のカスタマイズと設定、レポートジョブのトラブルシューティング、レポート内容のバックアップと復元に使用します。Loggerレポートのサポートと保守に携わるユーザー向けのツールです。 • **Deploy Report Bundler**: 新しいレポートまたは更新済みレポートのパッケージをロードし、Loggerシステムに導入します。「レポートバンドルの展開」(325ページ)を参照してください。 • **レポートの設定 (Report Configuration)**: レポートサーバーの設定値を表示または変更します。「レポートの設定」(305ページ)を参照してください。 • **レポート カテゴリ フィルタ (Report Category Filters)**: 検索グループフィルターの割り当てまたは削除を行います。「レポートカテゴリフィルター」(315ページ)を参照してください。 • **レポート カテゴリ (Report Categories)**: エクスプローラーのカテゴリの追加、変更、削除を行います。「レポートカテゴリ」(308ページ)を参照してください。 • **ジョブ実行ステータス (Job Execution Status)**: すべてのレポートジョブのステータスを表示できます。「ジョブ実行ステータス」(315ページ)を参照してください。 • **iPackager**: レポートとレポートオブジェクトのパッケージを作成し、このパッケージを他のLoggerにインポートしたり、アップグレード後に再導入したりすることができます。レポート設定を複数のLoggerに展

メニューセクション	説明
	開することもできます。「iPackagerユーティリティ」(317ページ) を参照してください。

[レポート] ホームページ

[マイ・レポート] ホームページは **[最近のレポート]** タブに常に表示されるため、実行した最新のレポートに簡単にアクセスできます。同時に、他のタブを9個まで表示することができます。

[レポート] ホームページは以下の3つの動的リストで構成されています。

- **最近のレポート**: 最近実行された10個のレポートが実行時順にリスト表示されます。「最近のレポート」(178ページ) を参照してください。
- **公開済みレポート**: 後で使用できるように出力結果が保存されているレポートがリスト表示されます。「レポートの発行」(213ページ) を参照してください。
- **他のレポート**: バックグラウンドレポートの表示または削除、スケジュールされたレポートやオンデマンドレポートの表示を行うことができます。

各リストで使用できる機能は、レポートのタイプ、表示形式、ユーザーの権限などによって異なります。

[レポート] ホームページへのアクセス

[レポート] ホームページにアクセスするには

1. Loggerのナビゲーションバーの **[レポート]** をクリックします。

レポートツールから [レポート] ホームページに戻るには

1. **最近のレポート** タブ (左上のタブ) をクリックします。

ジョブに適したツールの使用

目的のタスクに適したレポートツールを見つけるには、次の表を参考にしてください。

目的	該当するレポートツール
• 複数のタスクのレポートオブジェクトを検索、整理、選択する • レポートを実行する	「レポートエクスプローラー」(171ページ)
• 最近使用したレポートを実行または再実行する • 最近実行したレポートを変更するためにデザイナーで該当レポートを開く	「最近のレポート」(178ページ)

目的	該当するレポートツール
• 公開済みレポートをビューアーで開き、その公開済みレポートに対して、コメントの追加、アップロード、またはエクスポートを行う	「公開済みレポート」(180ページ)
• バックグラウンドレポートまたは他のレポートをビューアーで開く • バックグラウンドレポートを削除する	「他のレポート」(183ページ)
• レポートを特定の時刻および頻度で実行するようにスケジュールする • スケジュールされたレポートを編集、有効化/無効化、または削除する • 完了までに1時間以上かかるレポートを実行する	「スケジュールレポート」(185ページ)
• 以前のレポートから新しいレポートを作成する • 新しいレポートを最初から作成する	「カスタムレポートのデザイン」(223ページ)
• 機能強化されたスマートダッシュボードを作成または変更する • クラシックダッシュボードを作成または変更する	「ダッシュボードの作成」(252ページ)
• レポートで使用する新しいクエリを作成する	「クエリ」(262ページ)

一般的な質問

Loggerレポートツールは、従来のアドホックツールからスマート対応レポートツールに移行しつつあります。選択肢が増えた反面、多少の混乱も予想されます。Loggerのレポートとツールの最適な使用方法を判断するために、以下の一般的な質問を確認してください。

スマートレポートとアドホックおよびスタジオレポートとの違いは?

スマートレポートはアドホックおよびスタジオレポートとほぼ同じですが、一部、重要な違いがあります。

- **スマート形式とiHTML形式** — 表示やエクスポートなどでスマート形式とiHTML形式が使用できるのはスマートレポートのみです。スマート対応レポートは、短い(iHTML)レポートと長い(スマート)レポートをWebに素早く表示するために、単純でページ分割のないテンプレートを使用します。スマートレポートは、最小限の処理でデータを確認したいときのために、迅速に表示されるように設計されています。「レポートの表示形式とエクスポート形式」(206ページ)を参照してください。

  ヒント: スマートレポートを作成するには、[エクスプローラー]からアドホックレポートを選択し、コンテキストメニューから[スマート形式で実行]を選択します。「新しいスマートレポートの作成」(228ページ)を参照してください。

- **スマートダッシュボード** — 複数のクエリに対応したスマートダッシュボードを作成するには、公開済みのスマートレポートウィジェットからスマートツール([デザイン] > [ダッシュボード])を使用する必要があります。どちらのダッシュボードデザイナーもアドホックダッシュボードを作成できますが、ダッシュボード1つにつき、クエリは1つに制限されています。

- **スタジオレポート** — 従来のレポートタイプであり、クラシックレポートツールを使用して変更と管理を行う必要があります。

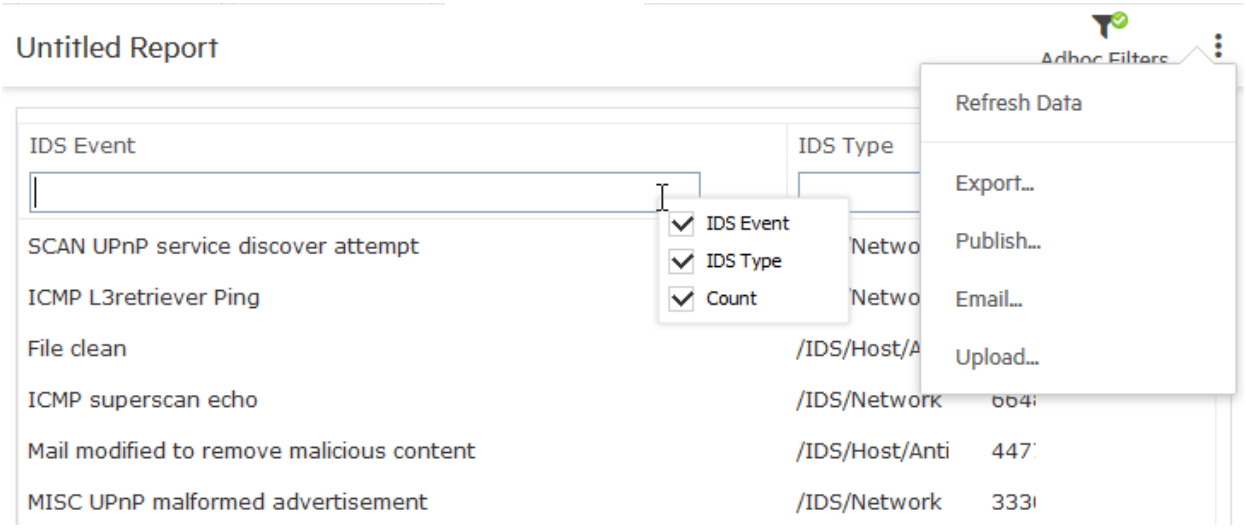
どのレポートがどこで表示されますか?

- [エクスプローラー] からアドホックレポートをスマートレポートとして実行すると、レポートはスマートビューアーに表示されます。ここでは、更新、エクスポート、公開、電子メール、アップロードを行うことができます。データ行の中では、ディスプレイコラムのオンとオフを切り替えることができます。「スマートレポートビューアー」(203ページ) を参照してください。
- アドホックまたはスタジオレポートをHTML形式 (デフォルト) で実行すると、レポートはアドホックパワービューワに表示されます (以前の形式であるスタジオレポートは、アドホック形式でしか実行できません)。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
- 他の形式を使用するレポートを実行するとき、ファイルを保存するか、適切なアプリケーションで開くかを選択する場合があります。
- レポートインスタンスを表示するために開くと、適切なビューアーに表示されます。「スマートビューアーとアドホックビューアーの違いは?」(169ページ) を参照してください。

スマートビューアーとアドホックビューアーの違いは?

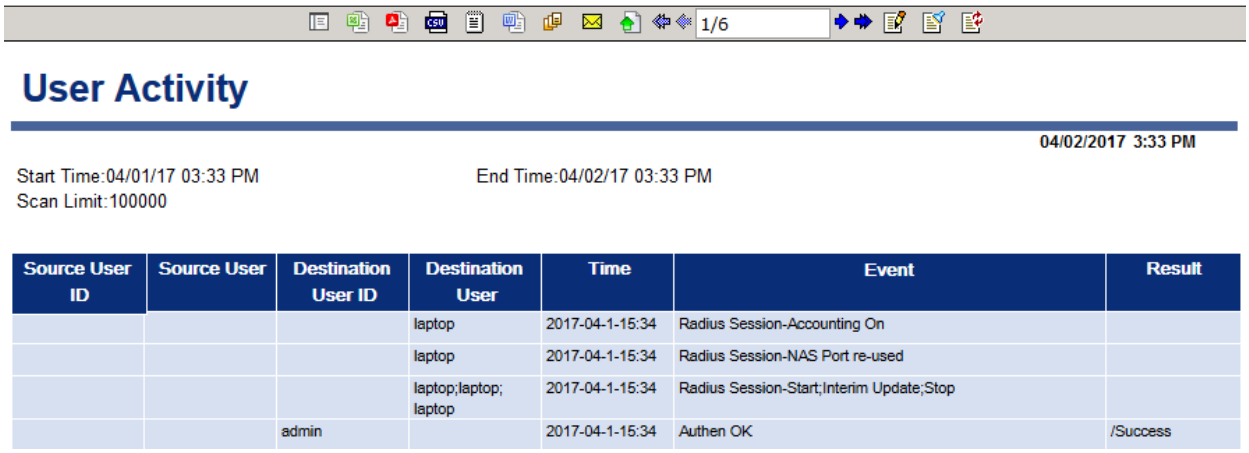
外観とレイアウトが異なりますが、機能は同じです。メニューオプションには、更新、エクスポート、公開、コメント、アップロードがあります。「レポートの表示」(201ページ) を参照してください。

スマートビューアーとメニュー



ヒント: スマートビューアーのユーザーインターフェイス (UI) はスマートツールへの移行の一環であり、アドホックツールは最終的に廃止されます。

アドホックビューアーとメニュー



スマートデザインツールとアドホックデザインツールの違いは?

外観とレイアウトが異なりますが、機能は同じです。どちらもほぼ同じレポート要素とオプションを使用します。ビューアーオプションに加え、データソース、フォーミュラフィールド、テンプレートの変更、グラフ、表、マップの作成などを行うことができます。

レポートの作成またはカスタマイズには、以下の3つのオプションがあります。

- **スマートデザイナー** — [エクスプローラー] から作業を開始する場合も、レポートの [デザイン] メニューの **[新しいレポート]** をクリックする場合も、スマートデザイナーであれば、グラフ、マップ、カスタマイズ、レポートの調整などをすべて行うことができます。「スマートレポートデザイナー」(227ページ) を参照してください。
- **アドホックパワービューワ** — このツールとアドホックレポートの関係は、スマートレポートとスマートデザイナーの関係に相当します。レポート内を右クリックすると、グラフやマップを作成、カスタマイズしたり、新しいレポートとして保存したりすることができます。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
- **アドホックレポートデザイナー** — レポートの [クラシック] メニューの **[新しいレポート]** をクリックすると、このデザイナーが開き、レポートオブジェクトを作成、変更、再利用し、これらを新しいレポートとして保存することができます。「クラシック: アドホックレポートデザイナー」(233ページ) を参照してください。

レポートの検索と管理

Loggerには、レポートの検索、整理、管理に使用できる数多くのツールがあります。

- **動的なレポートリスト** — [最近のレポート]、[公開済みレポート]、[他のレポート] には、使用頻度の高いレポートが動的に表示されます。
- **レポートストレージ** — [エクスプローラー] には、アクセス権限のあるレポートや、クエリ、パラメーター、ダッシュボード、ダッシュボードウィジェット、お気に入りの各レポートオブジェクトが

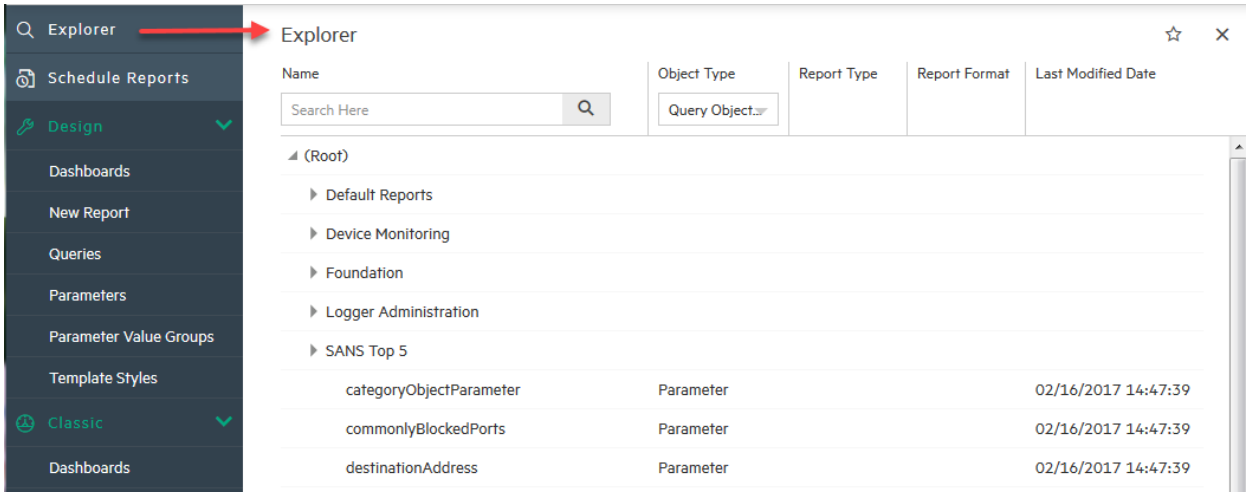
すべて格納され、これらを管理することができます。「レポートエクスプローラー」(171ページ)を参照してください。

- **レポート管理** — レポート管理者は、管理ツールを使用して、レポートジョブとレポートジョブが格納されるカテゴリフォルダーを管理することができます。「レポート管理」(304ページ)を参照してください。

ヒント: アクセス権限が限られているレポートユーザーには、権限を持つレポートのみが表示されます。「アクセス権限の割り当て」(163ページ)を参照してください。

レポートエクスプローラー

エクスプローラーは、アクセス権限のある既存のレポートや、クエリ、パラメーター、ダッシュボード、ダッシュボードウィジェット、お気に入りの各レポートオブジェクトを整理して素早くアクセスできるようにするツールです。Loggerの以前のバージョンには、各レポートオブジェクトタイプに1つずつ、計6種類のエクスプローラーがありました。今回のリリースから、これらのエクスプローラーは統合され、すべてのレポートオブジェクトを1つのツールで簡単に処理できるようになりました。



レポートと、クエリやパラメーターなどのレポートオブジェクトは、その機能に基づいて整理され、フォルダー(カテゴリという)にまとめられます。たとえば、データベースに関連するレポートは、データベースカテゴリの下に格納できます。

エクスプローラーには、カテゴリ分けしたすべてのレポートとレポートオブジェクトが一覧表示されます。あらかじめ定義された、よく使用されるカテゴリがいくつか提供されています。必要なアクセス権限があれば、必要に応じてカスタムカテゴリを追加することもできます。

注: デフォルトでは、レポートへの完全なアクセス権を持つユーザーは管理者のみです。「アクセス権限の割り当て」(163ページ) を参照してください。

エクスプローラーを開くには

1. レポートメニューの上部にある  **[エクスプローラー (Explorer)]** をクリックします。

   このアクションを行うと、エクスプローラーの表示/非表示が切り替わります。新しいタブは開きません。このように、エクスプローラーはどのタブからでも表示でき、不要なときには閉じておくことができます。

レポートオブジェクトとは

レポートオブジェクトは、モジュールとしてデザインされ、ダッシュボードや複雑なレポートに使用できます。レポートオブジェクトには以下のようなものがあります。

- 標準レポートとカスタムレポート
- 公開済みレポートとスケジュールされたレポート
- ダッシュボード
- ダッシュボードウィジェット
- クエリオブジェクト
- パラメーターオブジェクト
- カテゴリ (フォルダー)

エクスプローラーの操作

エクスプローラーでは、ツリー構造で分類されたレポートオブジェクトに対して、アクセス、格納、検索、管理を行うことができます。このプロセスの一環として、以下の操作を行うことができます。

- レポートオブジェクトのブラウズ
- 名前、オブジェクトタイプ、最終更新日などによる検索
- レポートタイプとレポート形式によるフィルタリング
- カテゴリの追加、管理、削除 (該当する権限を持つ場合)
- 素早い検索のための、お気に入りへのレポートオブジェクトの追加。「お気に入りエクスプローラー」(174ページ) を参照してください。

レポートを手動で実行するには

1. カテゴリフォルダーの横にあるをクリックして、カテゴリオブジェクトとサブカテゴリを表示します。
2. 目的のレポートに移動し、レポートを右クリックします。
3. コンテキストメニューから、**[Quick Run with Default Options]**、**[バックグラウンドで実行]**、**[レポートの実行]**、**[スマート形式で実行]** のいずれかを選択します。
4. 実行時フィルターまたはパラメーター条件があれば入力します。「実行時フィルター、条件、パラメーター」(196ページ) を参照してください。
5. **[実行]**、**[今すぐ実行]**、**[プレビュー]**、または **[バックグラウンドで実行]** をクリックします。「レポートの実行」(190ページ) を参照してください。

レポートオブジェクトをブラウズするには

1. カテゴリフォルダーの横にあるをクリックして、カテゴリオブジェクトとサブカテゴリを表示します。
2. 目的のレポートオブジェクトに移動します。
3. カテゴリ内のオブジェクトを右クリックし、それに対して操作を実行します。オプションの説明については、「エクスプローラーのオプションとコンテキストメニュー」(175ページ) を参照してください。

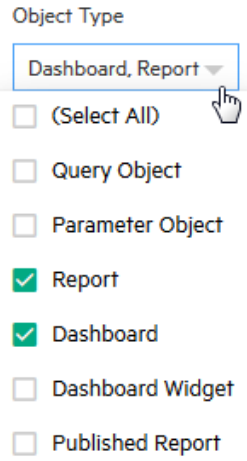
レポートオブジェクトを名前で検索するには

1. [名前 (Name)] カラムの上にある検索ツールに検索文字列を入力します。この例では、`device`です。

2. をクリックして結果をフィルタリングします。"device" という語を含むレポートオブジェクトがすべて表示されます。
3. 検索フィルターをキャンセルするには、**X**をクリックしてエクスプローラーの表示をリセットします。

オブジェクトタイプでフィルタリングするには

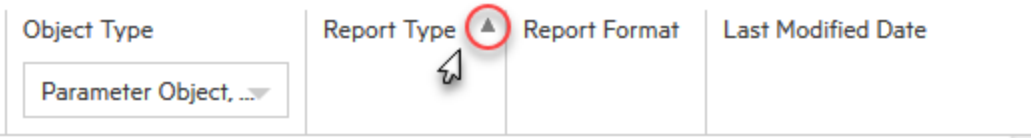
1. [オブジェクトタイプ (Object Type)] カラム見出しのドロップダウンメニューをクリックして、オブジェクトフィルターのリストを表示します。
2. オブジェクトをオンまたはオフにして、表示するオブジェクトを選択します。



3. フィルターリストの外側をクリックしてエクスプローラーを更新すると、選択したオブジェクトが表示されます。

カラムリストのソート順を変更するには

1. 変更するカラムヘッダーの中をクリックします。小さいグレーの三角形が表示されます。



2. ▲をクリックすると、結果がそのカラムでフィルタリングされます。▼をクリックすると、ソート順序がA-Z順、Z-A順、または日付順に切り替わります。

エクスプローラーのカテゴリを管理するには

1. 目的のカテゴリフォルダーに移動します。
2. カテゴリフォルダーを右クリックします。カテゴリのコンテキストメニューが表示されます。
3. メニューからアクションを選択します。「エクスプローラーのオプションとコンテキストメニュー」(175ページ) を参照してください。

ヒント: レポート管理者は、レポート管理ツールを使用して、カテゴリとカテゴリフィルターを直接操作することもできます。「レポートカテゴリ」(308ページ) および「レポートカテゴリフィルター」(315ページ) を参照してください。

お気に入りエクスプローラー

頻繁に使用する項目に素早くアクセスするために、レポート、クエリ、パラメーター、ダッシュボード、ダッシュボードウィジェットをお気に入りとしてマークできます。

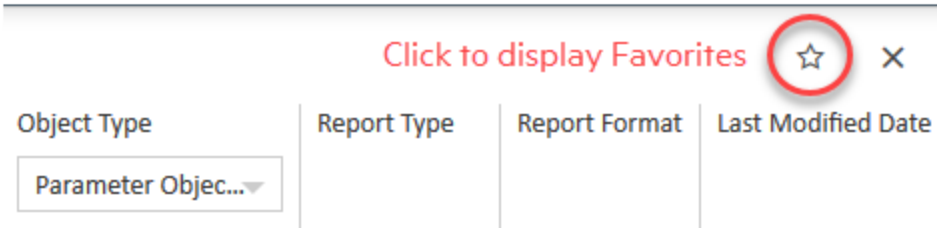
注: お気に入りオブジェクトをカテゴリに分類することはできません。

レポートオブジェクトをお気に入りとして追加するには

1. 簡単にアクセスできるようにするレポートオブジェクトをエクスプローラーから選択します。
2. そのオブジェクトを右クリックします。アクションメニューが表示されます。
3. **[お気に入りに追加]** をクリックします。確認メッセージが表示されます。

お気に入りリストからオブジェクトにアクセスするには

1. エクスプローラーのX (閉じる) アイコンの左にあるお気に入りの星印をクリックします。



   お気に入りとして指定したレポートオブジェクトが表示されます。
2. レポートオブジェクトを選択し、右クリックすると、アクションメニューが開きます。
3. アクションを選択します。

お気に入りリストからオブジェクトを削除するには

1. エクスプローラーの☆をクリックして、お気に入りのリストを開きます。
2. そのレポートオブジェクトを右クリックします。
3. **[お気に入りから削除]** を選択します。

エクスプローラーのオプションとコンテキストメニュー

エクスプローラーでは、既存のレポートやレポートオブジェクトに一元的にアクセスし、それらを保守することができます。カテゴリフォルダーまたは他のレポートオブジェクトを右クリックすると、そのフォルダーまたはオプションのコンテキストメニューが表示されます。メニューオプションは、オブジェクトタイプとパラメーターの要件によって異なります。

どのエクスプローラーオブジェクトにも、以下のメニューオプションがあります。

全エクスプローラーオブジェクト共通

アイコン	メニューオプション	説明
☆	お気に入りに追加 お気に入りから削除	エクスプローラーのお気に入りリストにこのオブジェクトを追加するか、リストから削除します。「お気に入りエクスプローラー」(174ページ)を参照してください。
	{オブジェクト}をコピー 貼り付け	このオプションは、エクスプローラーオブジェクトを別のカテゴリフォルダーにコピーするために使用します。コピーを保存するには、カテゴリフォルダーを右クリックし、**[貼り付け]**を選択します。
	{オブジェクト}を切り取り 貼り付け	このオプションは、エクスプローラーオブジェクトを別のカテゴリフォルダーに移動するために使用します。オブジェクトを移動するには、カテゴリフォルダーを右クリックし、**[貼り付け]**を選択します。
	{オブジェクト}の削除	エクスプローラーオブジェクトを削除します。 **注意:** 削除するのはデフォルトオブジェクトのコピーのみにし、デフォルトオブジェクトそのものは削除しないように注意してください。

レポートには一般に以下のエクスプローラーメニューオプションがあります。各種実行オプションの説明については、「レポート実行オプションについて」(191ページ)を参照してください。

エクスプローラーのレポート関連オプション

メニューオプション	説明
Quick Run with Default Options	デフォルトの環境設定または最後に保存した環境設定を使用してレポートを実行します。レポートにユーザーパラメーターがある場合、[レポート・パラメータ]タブに入力し、**[今すぐ実行]**または**[バックグラウンドで実行]**を選択して実行します。
バックグラウンドで実行	デフォルトの環境設定または最後に保存した環境設定を使用してレポートをバックグラウンドプロセスとして実行します。レポートにユーザーパラメーターがある場合、[レポート・パラメータ]タブに入力し、**[今すぐ実行]**または**[バックグラウンドで実行]**を選択して実行します。
レポートの実行	レポート形式など、新しい環境設定を設定してからレポートを実行します。
スマート形式で実行	レポートをマルチページのInteractive HTML形式で生成します。これらのスマートレポートは、ページ分割されたWeb形式で表示され、グリッドやインタラクティブグラフをカスタマイズできます。
公開済みのリスト出力	選択したレポートの公開済みレポートのリストを新しいタブに表示します。
ダッシュボードウィジェットの作成	[ウィジェット・デザイナ]ページが開き、あらかじめ生成されたレポートウィジェットを作成することができます。
このレポートをカスタマイズ	スマートデザイナー(スマートレポートの場合)またはアドホックレポートデザイナーが開き、レポートに変更を加えたり、レポートを新しいレポートとして保存したりすることができます。

エクスプローラーのレポート関連オプション (続き)

メニューオプション	説明
をコピーする	レポートファイルをクリップボードにコピーします。
リンクレポートとしてコピー	レポートオブジェクトへのリンクを別のディレクトリに追加します。ショートカットと同様の機能です。
プロパティ	レポートの [プロパティ] ウィンドウを表示します。
レポートをダウンロード	レポートのオフラインコピーをIBM WebSphere ILOG JRulesルールー言語 (IRL) 形式で保存します。 **注:** この種のファイルを開くには、IRLをサポートする適切なアプリケーションがオフラインシステムに必要です。
説明を表示	レポートの説明を情報ウィンドウに表示します。

カテゴリには、以下のエクスプローラーメニューオプションがあります。

エクスプローラーのカテゴリ関連オプション

メニューオプション	説明
新しいカテゴリを追加	エクスプローラーに新しいカテゴリフォルダーを追加します。
更新	カテゴリの内容を更新します。
プロパティ	カテゴリの [プロパティ] ウィンドウを表示します。

クエリには、以下のエクスプローラーメニューオプションがあります。

エクスプローラーのクエリ関連オプション

メニューオプション	説明
クエリ詳細を編集	選択したクエリをクエリオブジェクトエディターで開いて編集します。
Create Query Object	クエリを作成するためにクエリオブジェクトエディターを開きます。

パラメーターには、以下のエクスプローラーメニューオプションがあります。

エクスプローラーのパラメーター関連オプション

メニューオプション	説明
パラメータの詳細を編集	選択したパラメーターをパラメーターオブジェクトエディターで開いて編集します。
パラメータオブジェクトの作成	クエリを作成するためにパラメーターオブジェクトエディターを開きます。
パラメータ値グループの作成	新しいパラメーター値グループを作成するために、[パラメータ値グループ] ページを開きます。

最近のレポート

[最近のレポート] ウィジェットには、現在実行中のレポートと最近実行またはアクセスしたレポートのうち、最新の10個のレポートが一覧表示されます。デフォルトでは、スケジュールされたレポート以外のすべてのレポートが対象になります。

注意: このリストからレポートを実行すると、レポートは通常の**ビューアー**ではなく、それぞれの**デザイナー**に表示されます。そのため、エクスポートやコメントの追加だけでなく、レポートの変更を行うことができます。元のレポートを変更する前に、必ず **[名前を付けて保存]** を使用してレポートを別名で保存してください。

最近のレポートの実行

最近のレポートを実行するには

1. [最近のレポート] タブの **[最近のレポート]** アイコンをクリックして、最近のレポートのリストを開きます。
2. ラジオボタンをクリックしてレポートを選択します。レポートを選択した後、 **[実行]** ボタンと **[再実行する]** ボタンが左上隅に表示されます。
3. **[実行]** をクリックします。保存されている最新のパラメーターを使用してレポートが生成されます。

   レポートが新しいタブで開きます。ここでは、ビューアーツールを使用して、公開、表示、コメントなどのタスクを実行できます。

   - スマート形式で実行されたレポートは、スマートビューアーに表示されます。「スマートレポートビューアー」(203ページ) を参照してください。
   - アドホックレポートは、アドホックビューアーに表示されます。「アドホックレポートビューアー」(201ページ) を参照してください。
   - レポートをバックグラウンドで実行すると、[他のレポート] ページが開き、そこでレポートを選択して開くことができます。「バックグラウンドレポートの実行」(193ページ) を参照してください。

最近のレポートの再実行

最近のレポートを再実行するには

1. **[最近のレポート]** アイコンをクリックして、最近のレポートのリストを開きます。
2. ラジオボタンをクリックしてレポートを選択します。レポートを選択した後、**[実行]** ボタンと **[再実行する]** ボタンが左上隅に表示されます。
3. **[再実行する]** をクリックします。[レポート設定] メニューが **[データソース]** タブに表示されます。
4. 必要に応じてテンプレートを選択します。デフォルトは、**[プレーン]** です。「Loggerレポートテンプレートの操作」(303ページ) を参照してください。
5. レポートの形式を選択します。デフォルトは、**[HTML]** です。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
6. **[オプションを表示]** をクリックして、ページ数、zipファイル、ページ設定など、形式に適したオプションを設定します。「表示オプション」(208ページ) を参照してください。
7. 変更後、以下のいずれかのアクションをクリックしてレポートを生成します。

アクション	説明
実行	レポートを実行し、適切なビューアでレポートを表示します。
プレビュー	タイトルやカラム見出しを含む、レポートの短いサンプルを表示します。
バックグラウンドで実行	バックグラウンドプロセスとしてレポートを実行するようにスケジュールし、新しいタブでアクションを確認します。

レポートが新しいタブで開きます。ここでは、ビューアーツールを使用して、公開、表示、コメントなどのタスクを実行できます。

- スマート形式で実行されたレポートは、スマートビューアーに表示されます。「スマートレポートビューアー」(203ページ) を参照してください。
- アドホックレポートは、アドホックビューアーに表示されます。「アドホックレポートビューアー」(201ページ) を参照してください。
- レポートをバックグラウンドで実行すると、[他のレポート] ページが開き、そこでレポートを選択して開くことができます。「バックグラウンドレポートの実行」(193ページ) を参照してください。

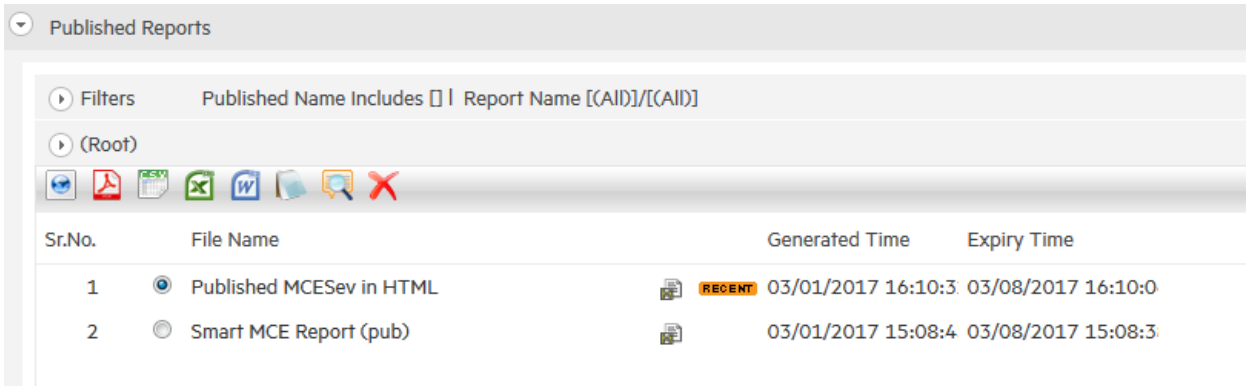
公開済みレポート

実行後、公開されたレポートは、[最近のレポート] タブの **[公開済みレポート]** ウィジェットから、表示、エクスポート、または削除することができます。

[公開済みレポート] ウィジェットから公開済みレポートを開くには

1. [最近のレポート] タブの をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 必要に応じて、**[フィルター (Filters)]** メニューを使用して結果をフィルタリングします。「公開済みレポートの操作」(215ページ) を参照してください。
3. 公開済みレポートを選択します。
4. 必要に応じて、をクリックしてそのレポートの [コメントを表示] ウィンドウを開きます。
5. レポートの表示アイコンを選択します (「表示オプション」(208ページ) を参照)。選択した表示形式でレポートが表示されます。
   - スマート形式で実行されたレポートは、スマートビューアーに表示されます。「スマートレポートビューアー」(203ページ) を参照してください。
   - アドホックレポートは、アドホックビューアーに表示されます。「アドホックレポートビューアー」(201ページ) を参照してください。

レポートを公開するには、「レポートの発行」(213ページ) を参照してください。



公開済みレポートの操作

[公開済みレポート] ウィジェットでは、レポートの表示、保存、削除のほか、レポートに付加されたコメントも表示することができます。ウィジェット内でのレポートの表示方法や生成方法は、選択したファイル形式によって異なります。

- ブラウザーに表示可能なレポート形式は、新しいタブに表示されます。
- 別のアプリケーションで表示する必要のあるレポート形式は、新しいウィンドウに表示され、そこでレポートの保存、エクスポート、アップロードを行うことができます。

[公開済みレポート] のリストが長い場合は、公開名、日付、ソースレポート、その他のオプションを使用してリストをフィルタリングできます。

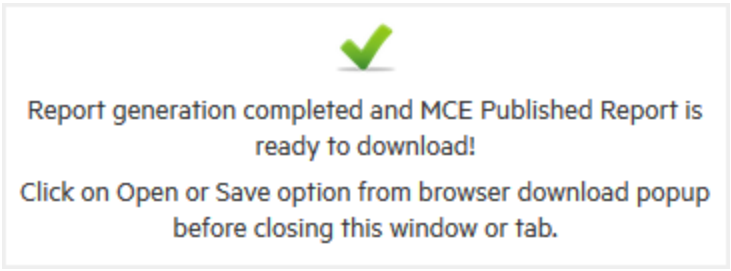
公開済みレポートを表示するには

1. [最近のレポート] タブの をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 公開済みレポートを選択します。
3. アイコンメニューから表示形式を選択してクリックします。「表示オプション」(208ページ) を参照してください。レポートは適切なビューワで表示されます。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
4. **[適用]** をクリックします。
5. 右上の をクリックして [公開済みレポート] のリストに戻ります。

公開済みレポートをダウンロードするには

1. [最近のレポート] タブの をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 公開済みレポートを選択します。
3. アイコンメニューから、PDF、CSV、Excel、Word、テキストなどのファイル形式を選択してクリックします。「表示オプション」(208ページ) を参照してください。

   新しいタブが開き、以下のようなメッセージが表示されます。



4. ブラウザーのポップアップウィンドウからダウンロードオプションを選択し、**[OK]** をクリックします。
5. 必要な情報を入力し、**[OK]** をクリックします。

公開済みレポートのコメントを表示するには

1. [最近のレポート] タブの をクリックして **[公開済みレポート (Published Reports)]** を開きます。

2. 公開済みレポートを選択します。
3. アイコンメニューの  をクリックします。**[コメントを表示]** ウィンドウが開き、該当レポートに追加されたコメントが表示されます。
4. 確認を終えたら、**[完了]** をクリックします。「レポートへのコメントの追加」(204ページ) を参照してください。

公開済みレポートを削除するには

1. [最近のレポート] タブの  をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 公開済みレポートを選択します。
3.  をクリックし、アクションを確認します。[公開済みレポート] のリストからレポートのインスタンスが削除されます。

[公開済みレポート] のリストをフィルタリングするには

1. [最近のレポート] タブの  をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. **[フィルター]** をクリックしてフィルターメニューを開きます。
3. フィルター条件を入力します。

注: これらのフィルター条件へのアクセスは、使用中のLoggerレポートのアクセス権限ポリシー、役割、自分自身のアクセス権限に基づきます。他の権限が必要になることもあります。「アクセス権限の割り当て」(163ページ) を参照してください。

フィルター条件	説明
次を含む公開済みの名前	公開済みレポートの名前の一部または全部を示すテキスト文字列を入力します。
更新の間に	レポートを更新時刻で絞り込むために、日付の範囲を入力します。日付を`MM/dd/yyyy`形式で手入力するか、  をクリックして日付選択カレンダーを開きます。
レポートの選択	 をクリックして [オブジェクト選択] ウィンドウを開きます。レポートまたはフォルダーを選択します。
 孤立行	レイアウト (親レポート) が存在しない (見つからない、または削除された) 公開済みレポートを検索する場合にのみ、**[孤立行]** をオンにします。
オーナーの選択	ユーザーがアクセス権限を持つレポートオーナーから選択します。
Private Owned By	ユーザーがアクセス権限を持つプライベートレポートから選択します。

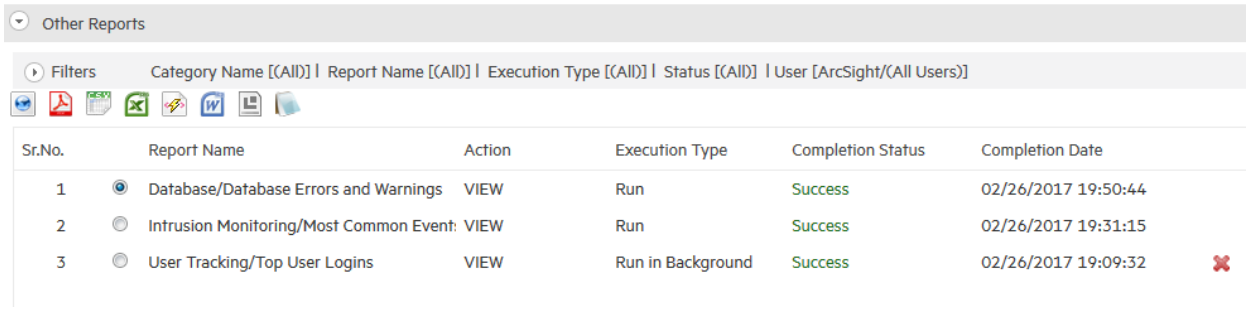
フィルター条件	説明
Public Owned By	ユーザーがアクセス権限を持つオーナーリストからパブリックレポートオーナーを選択します。

4. 必要に応じて **[(ルート)]** をクリックしてカテゴリフィルターを開き、目的の公開済みレポートまで移動します。
5. **[更新]** をクリックします。フィルタリングされたリストが表示されます。

他のレポート

デフォルトでは、**[他のレポート (Other Reports)]** の動的リストには、公開済みレポートを除くすべてのレポートに関する情報が表示されます。

このリストをフィルタリングして、表示対象を広げたり、絞り込んだりすることができます。「[他のレポート] のリストのフィルタリング」(184ページ) を参照してください。



注: 手動で実行するレポート (実行の種類 (Execution Type): **[実行 (Run)]**) は、このリストに表示されてから1時間後に期限切れになります。バックグラウンドレポートとスケジュールされたレポートは、自動的に期限切れにはなりません。

[他のレポート (Other Reports)] のリストのレポートを表示またはダウンロードするには

1. レポートを選択すると、レポートの表示に必要なオプションや、レポートをダウンロードして別の場所で表示するためのオプションが表示されます。「表示オプション」(208ページ) を参照してください。

ヒント: iHTMLおよびスマートレポートオプションを持つのはスマートレポートのみです。

バックグラウンドレポートを削除するには

1. [実行の種類 (Execution Type)] が **[バックグラウンドで実行 (Run in Background)]** のレポートを選択します。
2. そのレポートの右側にある をクリックします。削除を確定します。

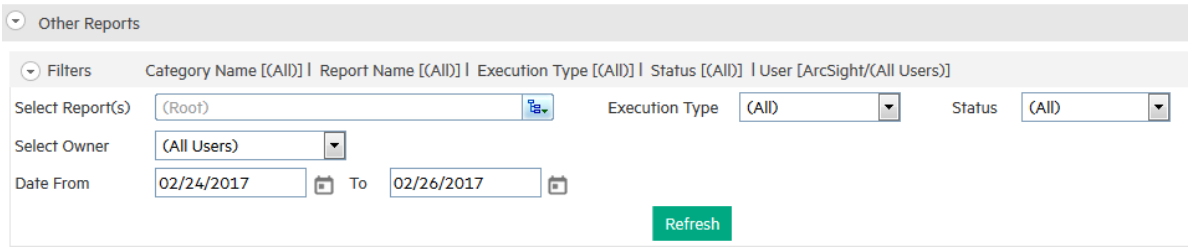
ヒント: このリストから削除できるのはバックグラウンドレポートのみです。

[他のレポート] のリストのフィルタリング

特定のレポートオブジェクトや、バックグラウンドで実行されたそのオブジェクトの特定のインスタンスを探す場合、[フィルター (Filters)] メニューを使用します。

[他のレポート] をフィルタリングするには

1. [最近のレポート] タブの をクリックして **[他のレポート (Other Reports)]** を開きます。
2. [他のレポート (Other Reports)] ウィジェットの をクリックして **[フィルター (Filters)]** メニューを開きます。



3. 以下のフィルター条件を必要に応じて入力します。

フィルター条件	説明
レポートの選択 (Select Report(s))	 をクリックして[オブジェクト選択]ウィンドウを開きます。レポートまたはフォルダーを選択します。
実行の種類 (Execution Type)	以下の実行の種類に基づいてフィルタリングします。 • すべて (All): 実行の種類をすべて表示します • 実行: レポートリストから直接実行されるレポートを表示します。 • スケジュール: スケジュールされたレポートを表示します。 • バックグラウンドで実行: バックグラウンドで実行されるレポートを表示します。
ステータス (Status)	以下の実行のステータスに基づいてフィルタリングします。 • 実行中: まだ実行中のレポートを表示します。 • 完了: 生成が完了したレポートを表示します。
オーナーの選択 (Select Owner)	個別のユーザーを選択するか、デフォルトの[(全ユーザー) ((All Users))]のままにします。
[日付指定: 最初の日付 (Date From)]と[最後の日付 (To)]	日付の範囲を入力すると、その期間に実行されたレポートがすべて表示されます。日付を`MM/dd/yyyy`形式で手入力するか、  をクリックして日付選択カレンダーを開きます。

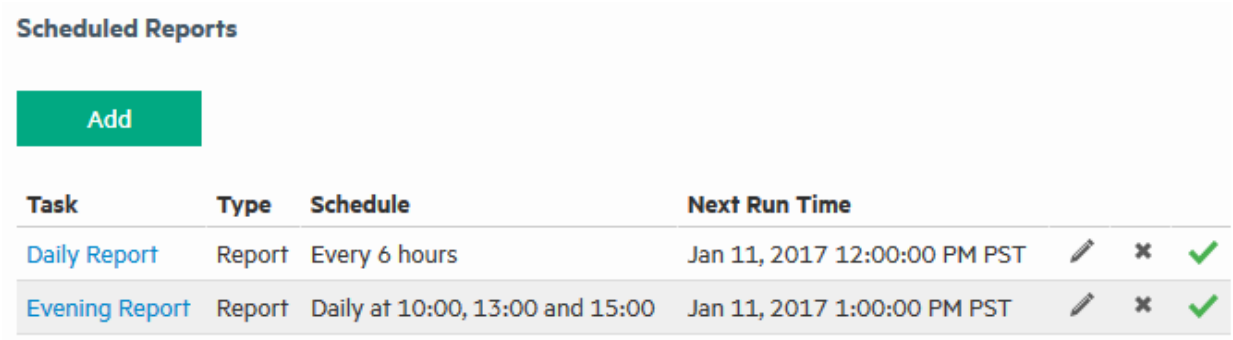
4. **[更新]**をクリックします。フィルタリングされたリストが表示されます。

スケジュールレポート

スケジュールジョブとして実行するレポートを、一度だけ、または、定期的に実行するようにスケジュールできます。レポートジョブのスケジューリングの一環として、配布オプションを、結果レポートの公開、メール送信、またはその両方に設定できます。

レポートのスケジューリングはできる限り行ってください。スケジューリングを行えば、生成までに1時間以上かかるレポートはタイムアウトにならず、負荷の小さい時間帯に実行されます。

注: スケジュールレポートの完了に時間がかかる場合、デフォルトでは4時間でタイムアウトします。



前提条件

スケジュールレポートを表示するには、ユーザーがLoggerレポートグループ、Logger検索グループ、Logger権限グループに属している必要があります。「ユーザ/グループ」(530ページ) を参照してください。

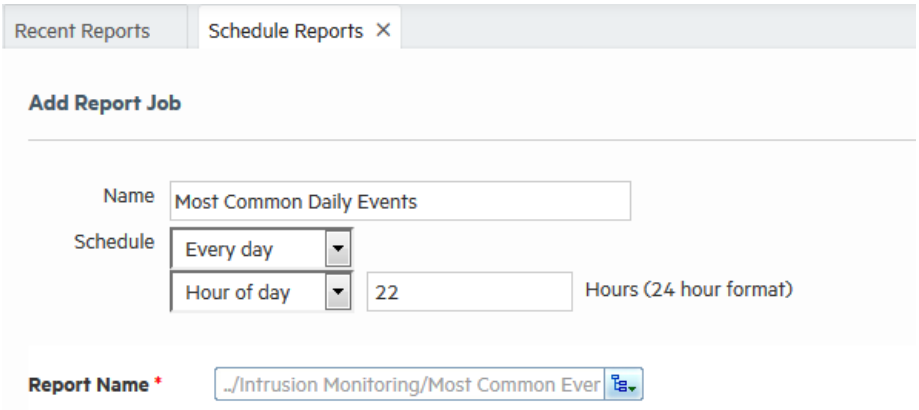
レポートのスケジュール

レポートの実行時刻を、毎日の特定時刻、または毎日数時間おき、あるいは特定曜日の特定時刻、毎月の特定の日の特定時刻にスケジュールすることができます。

ヒント: スケジュールされたレポートは、夏時間の開始または終了に伴う時刻変更により、影響を受ける可能性があります。詳細については、「サマータイムの変更がLoggerの処理に与える影響」(499ページ) を参照してください。

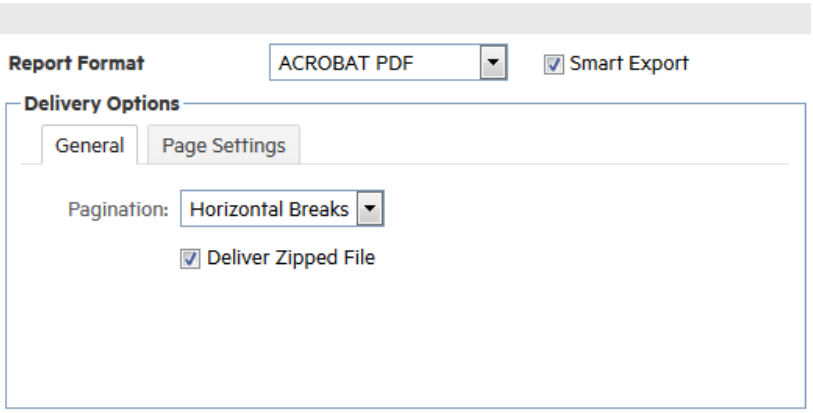
スケジュールされたレポートを設定するには

1. [レポート] メニューから **[スケジュールされたレポート]** をクリックします。[スケジュール報告 (Schedule Reports)] ページがタブに表示されます。
   a. 表示権限のあるスケジュール済みレポートがある場合、リストが表示されます。レポートには、編集または削除するためのオプションがあります。
   b. スケジュールされたレポートがない場合、「表示するジョブのレポートはありません」と表示されます。
2. **[追加 (Add)]** をクリックして [ジョブのレポートを追加 (Add Report Job)] ページを表示します。



3. **[名前 (Name)]** フィールドにレポートの表示名を入力します。
4. **[スケジュール (Schedule)]** オプションで、レポートの実行頻度を指定します。
   - **毎日 (Every day)** - 指定された時刻または指定された時間ごとに、日次レポートを実行します。
   - **曜日** - 指定された曜日にレポートを実行します。例: `Su, M, T, W, Th, F, Sa`。
   - **日付** - 指定された日付にレポートを実行します。例: `1,5,20,21`。
   - **時刻 (Hour of day)** - 指定された時刻にレポートを実行します。例: `0300`。
   - **時間ごと** - 指定された時間数または分数ごとにレポートを実行します。例: `90分`。
5. **[レポート名 (Report Name)]** プルダウンメニューからレポートを選択し、✔をクリックしてレポートをロードします。
6. **[レポートの配布]** セクションで、以下のオプションのいずれかまたは両方を設定します。
   - **公開する**: (デフォルトで選択済み) スケジュールされた時刻にレポートを公開します。発行オプションの設定の詳細については、「レポート公開オプション」(214ページ)を参照してください。
   - **電子メール**: スケジュールされた時刻にレポートをリンクまたは添付ファイルとして電子メールで送信します。メール配信オプションの詳細については、「電子メールの配布設定」(222ページ)を参照してください。

   ヒント: 別のタブに移動する前にレポートを保存する必要はありません。ただし、ページを閉じる前には必ずレポートを保存してください。
7. **[レポートの形式 (Report Format)]** セクションで、レポートの形式と配布オプションを選択します。



- レポートの形式を選択します。「レポートの表示形式とエクスポート形式」(206ページ)を参照してください。
- 配信オプションを選択します。「エクスポートオプション」(211ページ)を参照してください。
- Excel、Word、またはPDFファイルをネイティブ形式で使用できるようにする場合は、**[スマートエクスポート (Smart Export)]** をオンにします。「スマートエクスポートとは」(188ページ)を参照してください。

8. **[レポートのパラメータ]** セクションでは、デフォルトパラメーターをそのまま使用するか、変更することができます。レポートパラメーターの指定については、「パラメーター」(292ページ)を参照してください。
9. **[保存]** をクリックします。

追加したレポートがスケジュールされ、**[スケジュールされたレポート]** リストに表示されます。

スマートエクスポートとは

MS Excel、Acrobat PDF、MS Wordの各形式を使用するスケジュール済みレポートでは、[スマートエクスポート] オプションを使用できます。レポートはそのネイティブ形式でエクスポートされるため、ユーザーは各ツールの機能を利用することができます。「レポートの表示形式とエクスポート形式」(206ページ)を参照してください。

- グリッド情報は、Excel、Word、PDFでは同じような表としてエクスポートされます。
- 行列は、Excelではピボットテーブルとしてエクスポートされ、WordとPDFでは表としてエクスポートされます。
- レポートのグラフは、ExcelとWordではグラフとしてエクスポートされ、PDFではイメージとしてエクスポートされます。

これら3つの形式のスケジュール済みレポートでは、[スマートエクスポート] はデフォルトで有効です。

レポートの [スマートエクスポート] を有効にするには

1. [スケジュールされたレポート] ページで、スケジュールされた既存のレポートを編集するか、**[追加]** をクリックして、スケジュールされたレポートの新規作成を開始します。「レポートのスケジュール」(186ページ) を参照してください。
2. [レポートの形式] セクションで、[マイクロソフトエクセル]、[Acrobat PDF]、[マイクロソフトワード] のいずれかを選択します。**[スマートエクスポート]** チェックボックスが使用可能になります。
   - **オン** (デフォルト): レポートは、サポート対象プログラムのネイティブファイルとしてエクスポートされます。
   - **オフ**: レポートは通常の方法でエクスポートされます。たとえば、グラフはイメージとしてエクスポートされます。
3. 他の情報と変更がすべてこのレポートに反映されていることを確認します。
4. **[保存]** をクリックします。

スケジュールされたレポートの操作

スケジュール済みのレポートは、[スケジュールされたレポート] ページに表示されます。スケジュールされたレポートの有効化/無効化、編集、削除は、このページで行うことができます。

注: デフォルトでは、スケジュールされたレポートは、作成時点で有効化されます。

スケジュールレポートを編集するには

1. [レポート] メニューから **[スケジュール報告]** をクリックします。
2. 編集するスケジュールされたレポートジョブの横にある ✎ をクリックするか、レポートをクリックします。
3. **[ジョブのレポートを編集]** ページで必要な設定を変更します。
   詳細については、「レポートのスケジュール」(186ページ) を参照してください。

   注: ジョブ名は編集できません。
4. **[保存]** をクリックします。[スケジュールされたレポート] ページが表示されます。

スケジュールされたレポートを有効または無効にするには

1. [レポート] メニューから **[スケジュールされたレポート]** をクリックします。
2. **無効化**: スケジュールされたレポートジョブの右側にある ✔ をクリックします。アイコンは ⊘ に変わり、レポートの [次の実行時刻] に **[無効]** と表示されます。
3. **有効化**: スケジュールされたレポートジョブの右側にある ⊘ をクリックします。アイコンは ✔ に変わり、[次の実行時刻] に時刻が表示されます。

スケジュールされたレポートを削除するには

1. [レポート] メニューから **[スケジュールされたレポート]** をクリックします。
2. 削除するスケジュールされたレポートジョブの右にある  をクリックします。
3. 削除を確定します。

ヒント: [スケジュールされたレポート] リストからレポートを削除すると、レポート自体や過去に発行されたレポートの出力ではなく、スケジュールされたジョブが削除されます。

レポートの実行

Loggerレポートは多くの場所から実行できます。また、そのレポートに最適な実行オプションを選択できます。

ヒント: デザインプロセスの一環としてレポートを実行することも可能です。このセクションでは、実行準備の整ったレポートを対象とします。

レポート実行オプションについて

以下の表で、使用可能なレポート実行オプションについて説明します。レポートが表示されるビューアーやリストは、選択したレポート形式と実行アクションによって異なります。

Loggerのレポート実行オプション

アクション	使用できる場所	説明
Quick Run with Default Options	エクスプローラー	指定されたデータフィルターを使用してレポートを実行します。[デバイス グループ]、[ストレージ グループ]、[デバイス]、[ピア] など、タイムフレームと制約に関する実行時パラメーターを追加または変更することができます。「実行時フィルター、条件、パラメーター」(196ページ) を参照してください。
バックグラウンドで実行	エクスプローラー レポートのパラメータ	レポートをバックグラウンドプロセスとして実行します。バックグラウンドレポートの表示、エクスポート、削除は、[レポート] ホームページの [他のレポート] リストで行うことができます。「バックグラウンドレポートの実行」(193ページ) および「他のレポート」(183ページ) を参照してください。
レポートの実行	エクスプローラー	保存されている最新のパラメーターを使用してレポートを実行します。必要に応じて実行時パラメーターを追加または変更することができます。「フィルター条件の選択」(199ページ) を参照してください。
スマート形式で実行	エクスプローラー	このオプションは、親であるアドホックレポートからスマートレポートを作成します。レポートは、スマート形式で実行されるとスマートレポートになり、デフォルトではスマートビューアーとスマートデザイナーツールで表示されます。公開済みのスマートレポートは、スマートダッシュボードウィジェットとして使用することもできます。「スマートエクスポートとは」(188ページ) を参照してください。
実行	最近のレポート	保存されている最新のパラメーターを使用してレポートを実行します。必要に応じて実行時パラメーターを追加または変更することができます。「最近のレポート」(178ページ) を参照してください。
再実行する	最近のレポート	レポートの実行前に、新しいレポートパラメーター、表示オプション、フィルター条件を保存することができます。[再実行する] では、[レポートのパラメータ] タブが開き、前回の実行で指定した値が表示されます。これらを引続き使用することも、別の値に置き換えることもできます。[再実行する] には、レポートをプレビューするオプションや、レポートをバックグラウンドプロセスとして実行するオプションもあります。「最近のレポート」(178ページ) を参照してください。
プレビュー	レポートパラメーター	タイトルやカラム見出しを含む、レポートの短いサンプルを表示します。必要に応じて実行時パラメーターを追加または変更することができます。「実行時フィルター、条件、パラメーター」(196ページ) を参照してください。
今すぐ実行	レポートパラメーター	レポートをすぐに実行し、適切なビューアーに表示します。「実行時フィルター、条件、パラメーター」(196ページ) を参照してください。
リフレッシュデータ	スマートビューアー	既存のフィルターとオプションでレポートを実行します。

レポート実行のベストプラクティス

Loggerは、レポートの実行中もイベントを処理するように設計されていますが、イベントの処理が優先されます。イベント処理システムに負荷がかかっている状態で複雑なレポートを実行すると、イベントがドロップするのではなくレポートがタイムアウトします。

システムリソースの需要を効果的に管理するには、スケジュールされたレポートを使用して、負荷が軽いときにレポートが実行されるようにすることをお勧めします。アドホックレポートを実行する必要がある場合は、システムの負荷がないときに実行してください。「レポートのスケジュール」(186ページ) を参照してください。

大きいレポートをバックグラウンドでの実行に限定するオプションもあります。「長いレポートをバックグラウンドでの実行に限定する方法」(194ページ) を参照してください。

分散レポートを実行している場合は、「グループ、デバイス、ピアの選択」(200ページ) で説明するベストプラクティスも参照してください。

レポートの実行

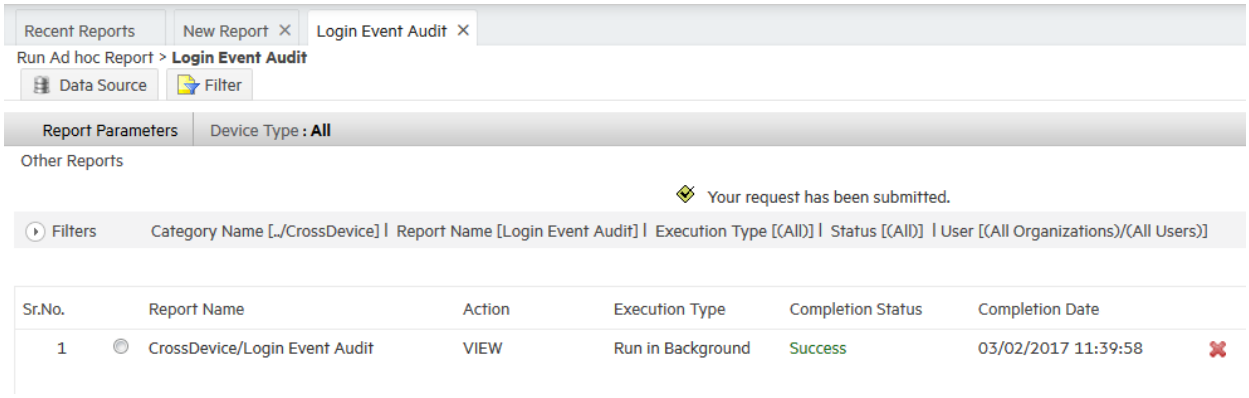
レポートを実行する方法や場所は数多くありますが、利用できるオプションが最も多いのはエクスプローラーです。詳細については、「レポートエクスプローラー」(171ページ) を参照してください。

エクスプローラーからレポートを実行するには

1. [レポート] メニューから **[エクスプローラー]** をクリックします。
2. レポートを選択します。「レポートエクスプローラー」(171ページ) を参照してください。
3. そのレポートを右クリックします。そのレポートのアクションメニューが表示されます。「エクスプローラーのオプションとコンテキストメニュー」(175ページ) を参照してください。
4. そのレポートの実行オプションを選択します。「レポート実行オプションについて」(191ページ) を参照してください。
5. 実行時フィルターまたはパラメーター条件があれば入力します。「実行時フィルター、条件、パラメーター」(196ページ) を参照してください。
6. **[実行]**、**[バックグラウンドで実行]**、または **[プレビュー]** をクリックします。Loggerはレポートを実行し、適切なデザイナーでレポートを開きます。デザイナーでは、レポートをカスタマイズし、データを表示するグラフの作成や編集を実行できます。「カスタムレポートのデザイン」(223ページ) を参照してください。

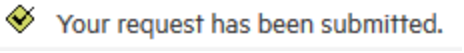
バックグラウンドレポートの実行

バックグラウンドレポートを実行すると、そのレポートは専用のタブの [他のレポート (Other Reports)] リストに確認メッセージと共に表示されます。



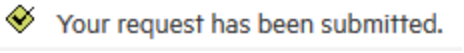
エクスプローラーからバックグラウンドレポートを実行するには

1. エクスプローラーで、実行するレポートに移動します。
2. レポート名を右クリックし、**[バックグラウンドで実行]** を選択します。
3. 追加のフィルターやレポートパラメーターがあれば設定します。
4. **[バックグラウンドで実行]** をクリックします。確認メッセージが表示されます。



フィルターまたはパラメーターページからバックグラウンドレポートを実行するには

1. [最近のレポート] で、実行するレポートに移動します。
2. をクリックしてレポートを再実行します。
3. 追加のフィルターやレポートパラメーターがあれば設定します。
4. **[バックグラウンドで実行]** をクリックします。確認メッセージが表示されます。

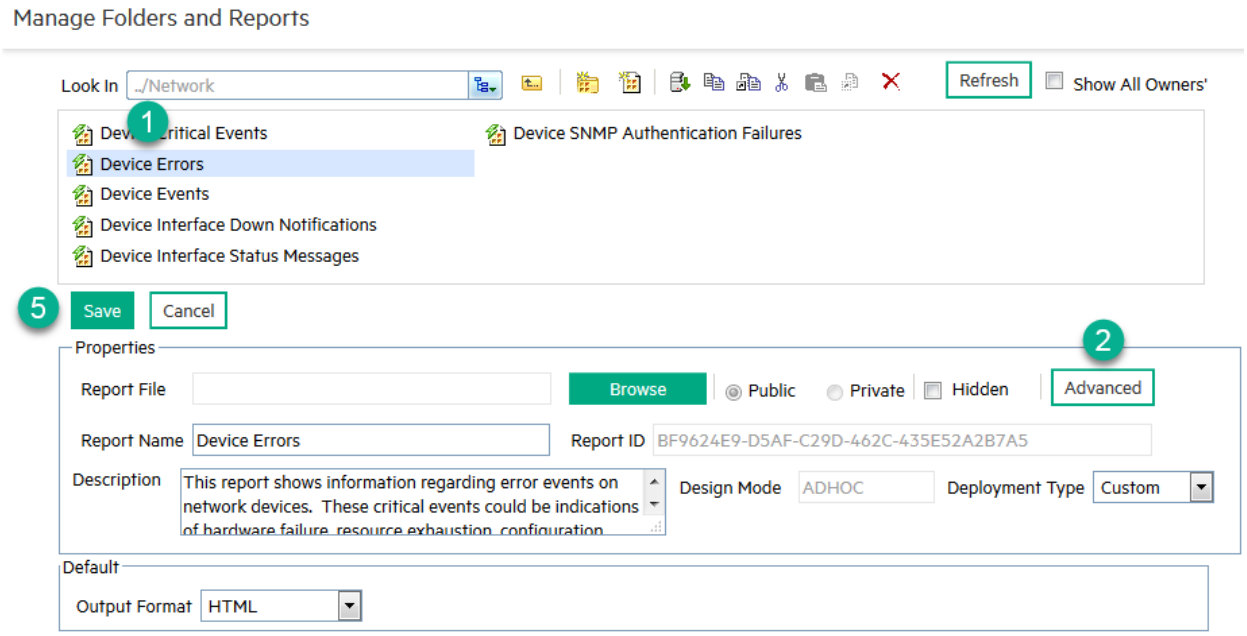


バックグラウンドレポートを削除するには

1. [最近のレポート] タブの **[他のレポート]** をクリックします。[他のレポート] リストが表示されます。
2. 削除するバックグラウンドレポートの右にある をクリックします。
3. 削除を確定します。

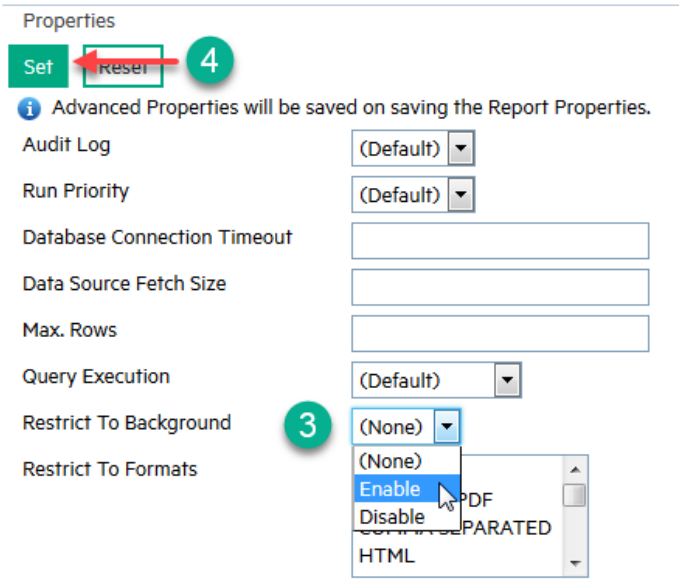
長いレポートをバックグラウンドでの実行に限定する方法

管理者は、実行に長い時間がかかるレポートをバックグラウンドでの実行に限定することができます。そのためには、[レポート カテゴリ] の [プロパティ (Properties)] メニューを使用します。



レポートをバックグラウンドでの実行に限定するには

1. [レポート] メニューの [管理] セクションから **[レポート カテゴリ]** をクリックします。
2. 限定対象のレポートを選択します 1 。
3. [プロパティ (Properties)] セクションの **[詳細 (Advanced)]** 2 をクリックします。レポートの [詳細プロパティ (Advanced Properties)] メニューが表示されます。



4. [バックグラウンドに限定 (Restrict To Background)] メニュー3の **[有効にする (Enable)]** をクリックします。
5. **[セット (Set)]** 4 をクリックします。メニューが閉じます。
6. [フォルダとレポートを管理 (Manage Folders and Reports)] ページの **[保存 (Save)]** 5 をクリックします。

分散レポートの実行

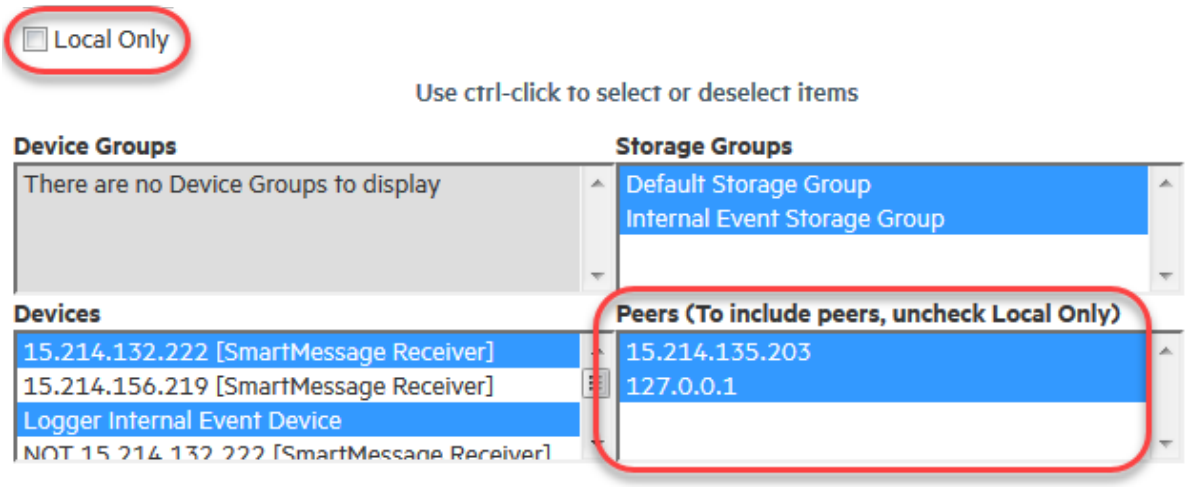
分散レポートには、指定されたLoggerのピアからの一致イベントが含まれます。レポートを実行するピアは、[ピア] リストで選択します。ピアが設定されていない場合、[ピア (Peers)] リストにはローカルホストのIPアドレス (127.0.0.1) しか表示されません。ピアが設定されている場合は、そのIPアドレスが一覧表示されます。

前提条件

分散レポートを実行するには、ピアデバイスを1つ以上設定しておく必要があります。

分散レポートを実行するには

1. [追加フィルタ] メニューの **[ローカルのみ (Local Only)]** をオフにします。
2. 検索対象にするピアを [ピア (Peers)] リストから選択します。



3. レポートを実行します。

実行時フィルター、条件、パラメーター

大部分のレポートには、適切な実行時フィルターを設定したり、デバイスやその他の検索条件、パラメーターを選択したりするオプションが備わっています。このセクションでは、これらのカスタマイズツールを使用してデータを好みに応じて表示する方法について説明します。

フィルターを定義したり、レポートに組み込まれているフィルターを変更したりすることができます。フィルター式は、レポートを実行するときに適用され、レポートの範囲を指定した条件に絞り込みます。

たとえば、[Top Password Changes] に対するレポートについて、指定したユーザー名や指定したIPアドレスに関係するパスワード変更についてのみレポートするように、フィルター条件を設定できます。これらのフィルターの作成方法の詳細については ([フィールド]、[条件]、および [値] フィールドを使用)、「フィルター」(238ページ) を参照してください。

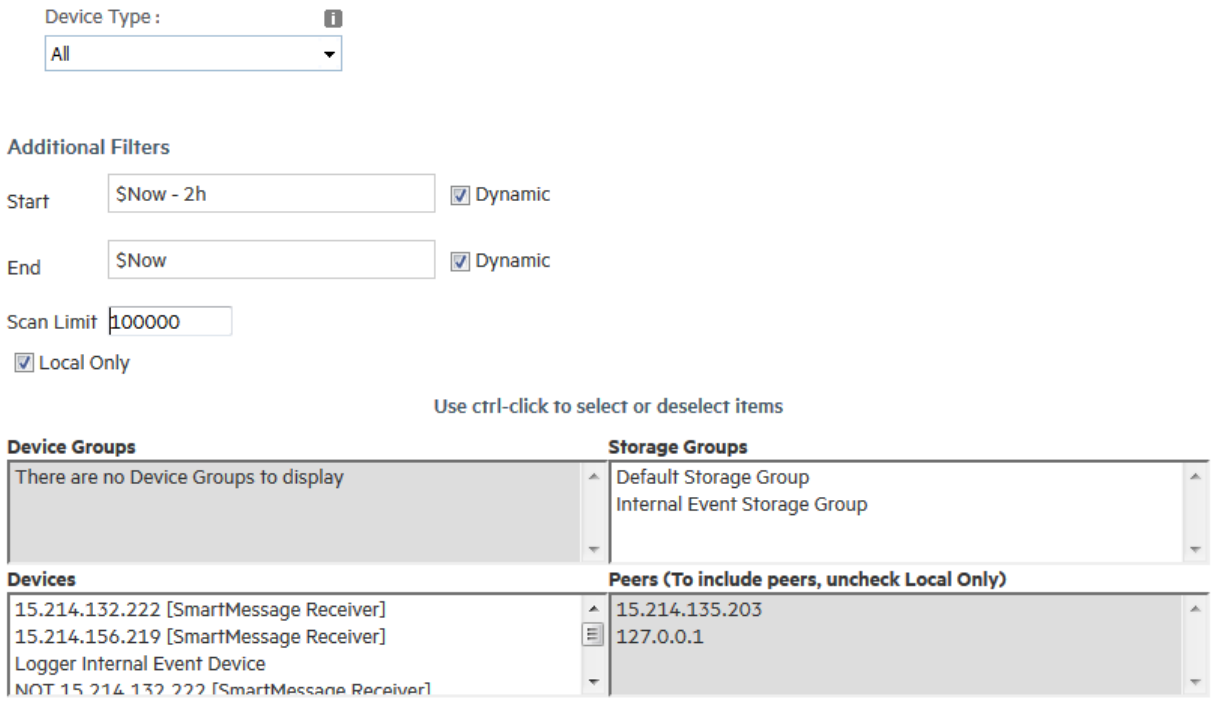
デフォルトを上書きする実行時パラメーターを指定しないでレポートを実行すると、レポートは、このレポートの設計時に指定されたデフォルトを使用して生成されます。[レポートの実行] パラメーターを指定した後で、レポートをバックグラウンドで実行できます。

注: レポート実行時に定義されるフィルター条件は、このレポート実行のみに適用されます。この方法で設定されたフィルターは保存されず、他のユーザーは使用できません。組み込みのデフォルトフィルター条件を、レポート設計の一部として設定することもできます。

追加フィルター

レポートを実行するときには、[デバイスグループ (Device Groups)]、[ストレージグループ (Storage Groups)]、[デバイス (Devices)]、[ピア (Peers)] など、タイムフレームと制約に関する

追加の実行時フィルターを選択するオプションがあります。何も選択しない場合、すべてのグループとデバイスが対象になります。



注: デフォルトでは、ピアは含まれません。ピアを対象とする場合は、明示的に選択する必要があります。「分散レポートの実行」(195ページ) を参照してください。

レポートの追加フィルターのパラメーター

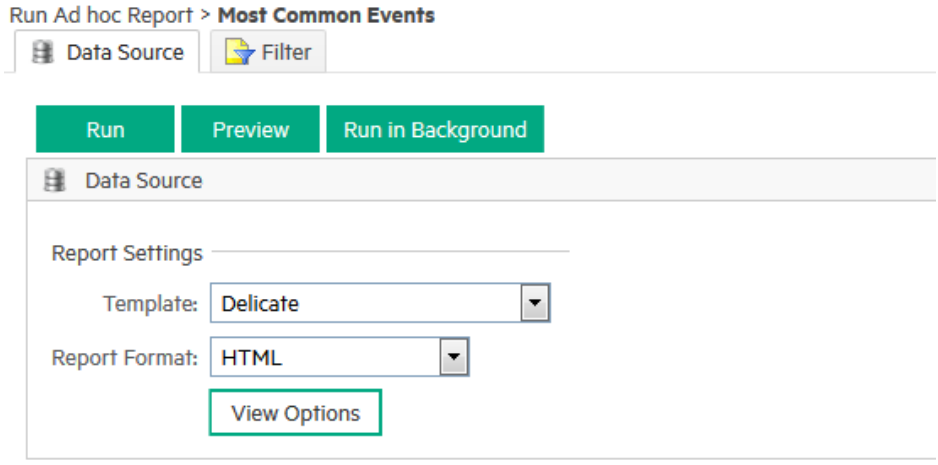
オプション	説明
デバイスタイプ (Device Type)	一部のレポートでは、レポートに含めるデバイスタイプを選択することができます。
開始 (Start)	イベントデータベースからのデータ収集の開始時刻を指定します。 デフォルトでは、開始時刻は**動的データ式** (`$Now - 2h`) を使用して指定されます。 動的な式を変更して、異なる動的開始時刻を指定するか、**[動的 (Dynamic)]** を無効にして、カレンダーオプションを使用して固定の開始時刻を指定します。
終了 (End)	データ収集の終了時刻を指定します。これは、開始時刻より後の時刻になります。 期間を長くすると、データが大量になり、システムのパフォーマンスに影響を与える可能性があることに注意してください。 デフォルトでは、終了時刻は**動的データ式** (`$Now`) を使用して指定されます。 動的な式を変更して、異なる動的終了時刻を指定するか、**[動的]** を無効にして、カレンダーオプションを使用して固定の終了時刻を指定します。
検索数の制限値	スキャンするイベント数を指定します。

レポートの追加フィルターのパラメーター (続き)

オプション	説明
(Scan Limit)	スキャン制限を指定すると、手動のレポート実行でスキャンされるイベントの数が、指定した上限に制限されます。この制限により、レポート生成が高速化されます。スキャン制限の指定は、Loggerに保存されているすべてのイベントを処理するのではなく、指定した時間範囲のN個のイベントのみを処理する場合に便利です。 デフォルトのスキャン制限は100,000です。スキャン制限を0 (ゼロ) に設定すると、すべてのイベントがスキャンされます。 **注:** この設定はスケジュールされたレポートに適用されません。
デバイスグループ (Device Groups)	レポートクエリを実行する特定のデバイスグループがある場合は選択します。「グループ、デバイス、ピアの選択」(200ページ) を参照してください。
ストレージグループ (Storage Groups)	レポートクエリを実行する特定のストレージグループを選択します。「グループ、デバイス、ピアの選択」(200ページ) を参照してください。
デバイス (Devices)	レポートクエリを実行する特定のデバイスを選択します。「グループ、デバイス、ピアの選択」(200ページ) を参照してください。
ピア (Peers)	レポートクエリを実行するピアLogger (ピアが設定されている場合) を選択します。「グループ、デバイス、ピアの選択」(200ページ) を参照してください。

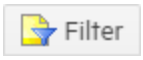
データソースのレポート設定

レポートの **[レポートの実行]** オプションを選択すると、このレポート実行について、ファイル形式の選択、ページ数の指定、データフィルター条件の変更を行うことができます。デフォルトを上書きする実行時パラメーターを指定しないでレポートを実行すると、レポートは、このレポートの設計時に指定されたデフォルトを使用して生成されます。



次の表で、**[レポート設定 (Report Settings)]** オプションについて説明します。

データソースのレポート設定

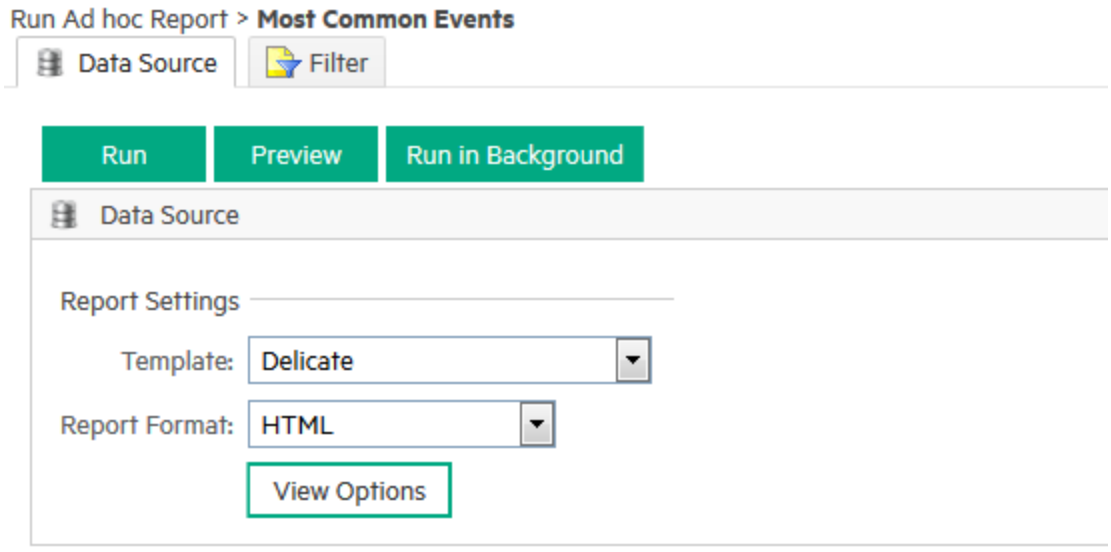
オプション	説明
テンプレート (Template)	このレポートに適用するテンプレートを選択します。[テンプレート (Template)] プルプダウンメニューに、提供されているテンプレートと、追加したすべてのカスタムテンプレートが表示されます。レポートを実行するために使用する開始時刻、終了時刻、スキャン制限、デバイスグループ、ストレージグループ、デバイス情報をレポートに含めるには、**BlankWithHeader**テンプレートを選択します。「テンプレートスタイル」(302ページ) を参照してください。
レポートの形式 (Report Format)	出力のファイルタイプまたは「形式」を指定します。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
オプションを表示 (View Options)	そのレポートで使用できるオプションから選択します。「表示オプション」(208ページ) を参照してください。
 [フィルター (Filter)] タブ	オプション。フィルターを定義するか、既存のデフォルトフィルターを変更します。「フィルター条件の選択」(199ページ) を参照してください。 フィルター式は、レポートを実行するときに適用され、レポートの範囲を指定した条件に絞り込みます。 たとえば、"Top Password Changes" レポートの場合、特定のユーザー名またはIPアドレスに関連するパスワード変更のみが表示されるように、フィルター条件を設定することができます。 これらのフィルターの作成方法の詳細については ([フィールド]、[条件]、および [値] フィールドを使用)、「フィルター」(238ページ) を参照してください。 **注:** レポート実行時に定義されるフィルター条件は、このレポート実行のみに適用されます。この方法で設定されたフィルターは保存されず、他のユーザーは使用できません。組み込みのデフォルトフィルター条件を、レポート設計の一部として設定することもできます。

フィルター条件の選択

レポートの **[レポートの実行]** リンクを選択すると、フィルターオプションが表示され、このレポート実行に限定して、データフィルター条件を変更できます。フィルターを定義したり、レポートに組み込まれているフィルターを変更したりすることができます。フィルター式は、レポートを実行するときに適用され、レポートの範囲を指定した条件に絞り込みます。

たとえば、[Top Password Changes] に対するレポートについて、指定したユーザー名や指定したIPアドレスに関係するパスワード変更についてのみレポートするように、フィルター条件を設定できます。これらのフィルターの作成方法の詳細については ([フィールド]、[条件]、および [値] フィールドを使用)、「フィルター」(238ページ) を参照してください。

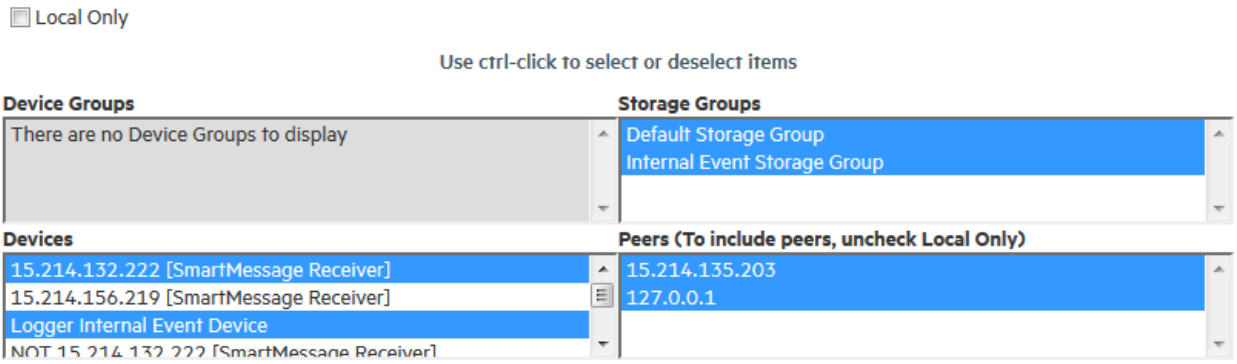
デフォルトを上書きする実行時パラメーターを指定しないでレポートを実行すると、レポートは、このレポートの設計時に指定されたデフォルトを使用して生成されます。[レポートの実行] パラメーターを指定した後で、レポートをバックグラウンドで実行できます。



注: レポート実行時に定義されるフィルター条件は、このレポート実行のみに適用されます。この方法で設定されたフィルターは保存されず、他のユーザーは使用できません。組み込みのデフォルトフィルター条件を、レポート設計の一部として設定することもできます。

グループ、デバイス、ピアの選択

[追加フィルタ] 設定の一環として、[デバイス グループ (Device Groups)]、[ストレージ グループ (Storage Groups)]、[デバイス (Devices)]、[ピア (Peers)] のどのデータソースをレポートに含めるかを選択することができます。



デフォルトでは、何も選択されていないため、すべてのグループとデバイスのイベントが対象となります。レポート実行時にデータ収集の対象を特定のグループまたはデバイスに限定するには、それらのソースのみを選択します。

注: ピアに対してレポートクエリを実行するには、ピアが明示的に選択されている必要があります。ピアが選択されていない場合、クエリはローカルLoggerに対してのみ実行されます。

[デバイス グループ (Device Groups)]、[デバイス (Devices)] のリスト、[ピア (Peers)] で選択した項目は、レポートクエリにOR演算子で追加されます。[ストレージ グループ (Storage Groups)] などの他の選択項目には、AND演算子で追加されます。

特定のデータソースを選択するには

1. 項目をクリックして選択します。
2. 複数の項目を選択または選択解除するには、Ctrlキーを押しながらクリックします。

使用可能なすべてのデータソースを選択するには

1. 選択したデータソースをすべて選択解除します。

レポートの表示

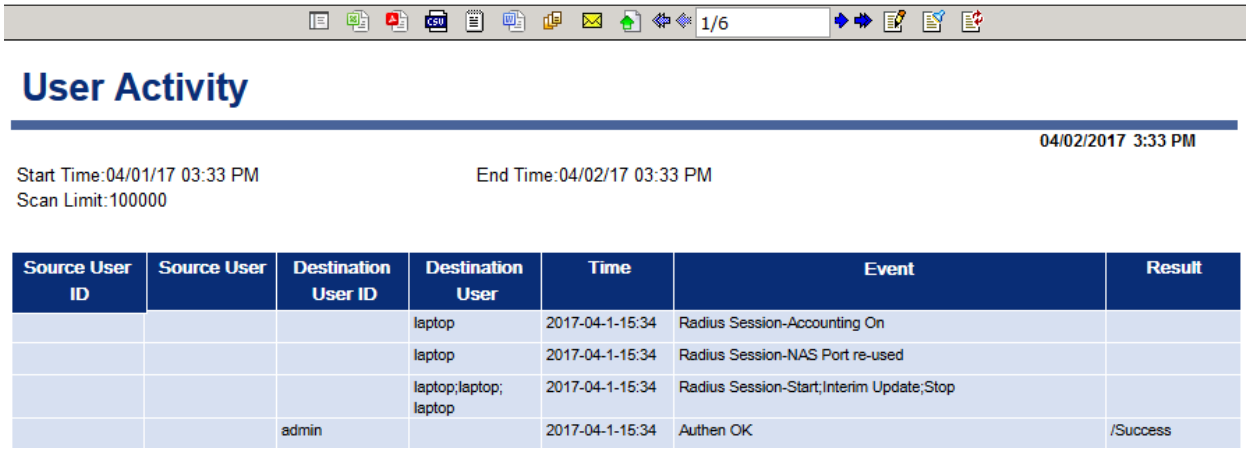
レポートを実行した後、スマートビューアーまたはアドホックビューアーで、今後の使用のためにそのレポートを公開したり、コメントの追加や電子メールでの送信、アップロード、または別の出力形式へのエクスポートを行ったりすることができます。

レポートビューアーでのオプションは、コメントの追加や他の場所への送信に限定されています。レポートを変更してカスタマイズするには、「カスタムレポートのデザイン」(223ページ) を参照してください。

ロゴやグラフの追加、表示オプションの変更など、レポート結果の変更については、「スマートレポート デザイナー」(227ページ) および「アドホック パワービューワデザイナー」(232ページ) を参照してください。

アドホックレポートビューアー

アドホックレポートを ([エクスプローラー]、[公開済みレポート] リスト、[他のレポート] リストなどから) 表示すると、アドホックレポートビューアーに表示されます。このビューアーでは、レポート属性のカスタマイズ、コメントの追加、別の出力形式へのエクスポートを行うことができます。



User Activity

04/02/2017 3:33 PM

Start Time:04/01/17 03:33 PM End Time:04/02/17 03:33 PM
Scan Limit:100000

Source User ID	Source User	Destination User ID	Destination User	Time	Event	Result
			laptop	2017-04-1-15:34	Radius Session-Accounting On	
			laptop	2017-04-1-15:34	Radius Session-NAS Port re-used	
			laptop;laptop; laptop	2017-04-1-15:34	Radius Session-Start;Interim Update;Stop	
		admin		2017-04-1-15:34	Authen OK	/Success

アドホックビューアーのメニューオプション

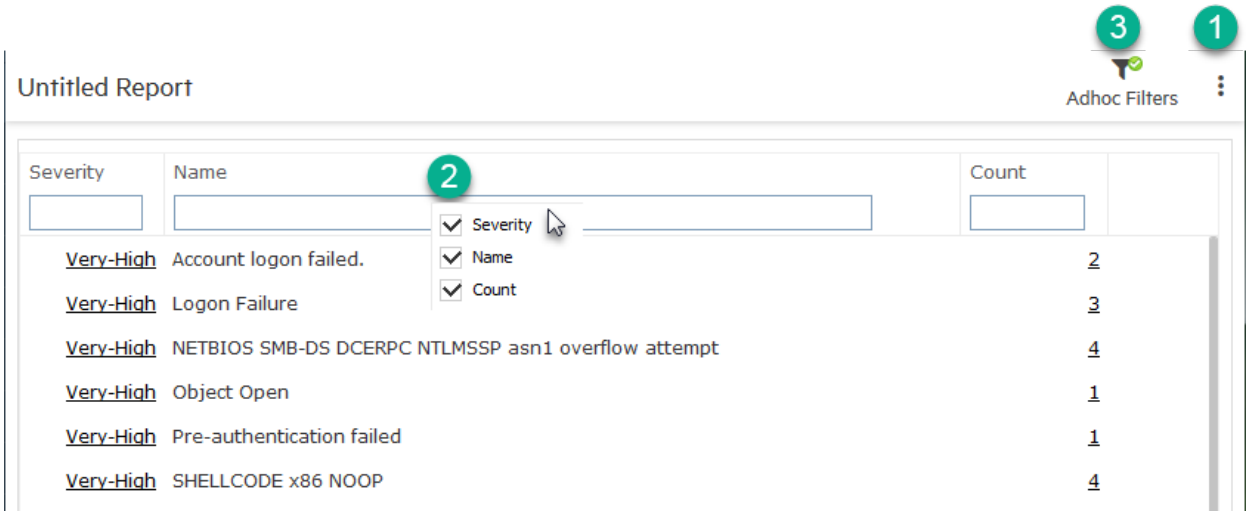
アドホックレポートを実行すると、アドホックビューアーメニューバーの次のオプションを使用できます。

アイコン	説明
	目次を追加します。
	Excelスプレッドシートで表示します。「表示オプション」(208ページ)を参照してください。
	PDFで表示します。「表示オプション」(208ページ)を参照してください。
	CSVファイルで表示します。「表示オプション」(208ページ)を参照してください。
	テキストファイルで表示します。「表示オプション」(208ページ)を参照してください。
	Microsoft Wordドキュメントで表示します。「表示オプション」(208ページ)を参照してください。
	レポートをエクスポートします。「レポートのエクスポートと保存」(218ページ)を参照してください。
	レポートをメールで送信します。「レポートのメール送信」(221ページ)を参照してください。
	レポートをサーバー、またはFTPサイトにアップロードします。「サーバーまたはFTPサイトへのレポートのアップロード」(219ページ)を参照してください。
1/1	レポートナビゲーションツール。クリックしてレポートの前または次のページ、先頭または最終ページに移動したり、ページ番号を入力して移動したりすることができます。

アイコン	説明
	コメントを追加します。「レポートへのコメントの追加」(204ページ)を参照してください。
	コメントを表示します。「レポートへのコメントの追加」(204ページ)を参照してください。
	コメントを更新します。コメントの表示ウィンドウを更新します。

スマートレポートビューアー

実行したスマートレポートは、スマートレポートビューアーに表示されます。このビューアーでは、レポート属性のカスタマイズ、コメントの追加、別の出力形式へのエクスポートを行うことができます。



スマートビューアーには、3つのメニューまたは作業領域があります。

ID	エリア	オプション
1	ビューアーメニュー	クリックするとメニューが表示されます。レポートの更新、エクスポート、公開、電子メール送信、アップロードのオプションから選択できます。「スマートビューアーのメニューオプション」(204ページ)を参照してください。
2	カラムメニューの表示/非表示	カラムヘッダーを右クリックすると、使用可能なカラムのリストが表示されます。表示する、または非表示にするカラムを選択します。
3	アドホックフィルター (Adhoc Filters)	クリックすると、[アドホックフィルター (Adhoc Filters)] メニューが開きます。「フィルター条件の選択」(199ページ)を参照してください。

スマートビューアーのメニューオプション

スマートレポートビューアーには、以下のオプションとアクションがあります。

メニューオプション	説明
リフレッシュデータ	既存のフィルターとオプションでレポートを実行します。「レポート実行オプションについて」(191ページ)を参照してください。
エクスポート...	[エクスポート オプション] ポップアップが表示されます。「レポートのエクスポートと保存」(218ページ)を参照してください。
公開する...	[レポートを公開] メニューが表示されます。「レポートの発行」(213ページ)を参照してください。
電子メール...	[電子メールレポート] メニューが表示されます。「レポートのメール送信」(221ページ)を参照してください。
アップロード...	[アップロード・オプション] メニューが表示されます。「サーバーまたはFTPサイトへのレポートのアップロード」(219ページ)を参照してください。

レポートのコラボレーション

Loggerユーザーは、公開済みレポートをHTMLフォーマットで表示し、コメントを加えるなどのコラボレーションを行うことができます。管理者は、必要に応じて、コメントを表示できるユーザーを指定することができます。

ヒント: コメントを追加するには、レポートに対する実行アクセス権限と公開アクセス権限が必要です。

レポートへのコメントの追加

[公開済みレポート] から表示可能なレポートプレビューを含め、生成済みのどのレポートページからでも、公開済みレポートのコメントの表示とコメントの追加を行うことができます。コメントを表示できるユーザーを選択することもできます。

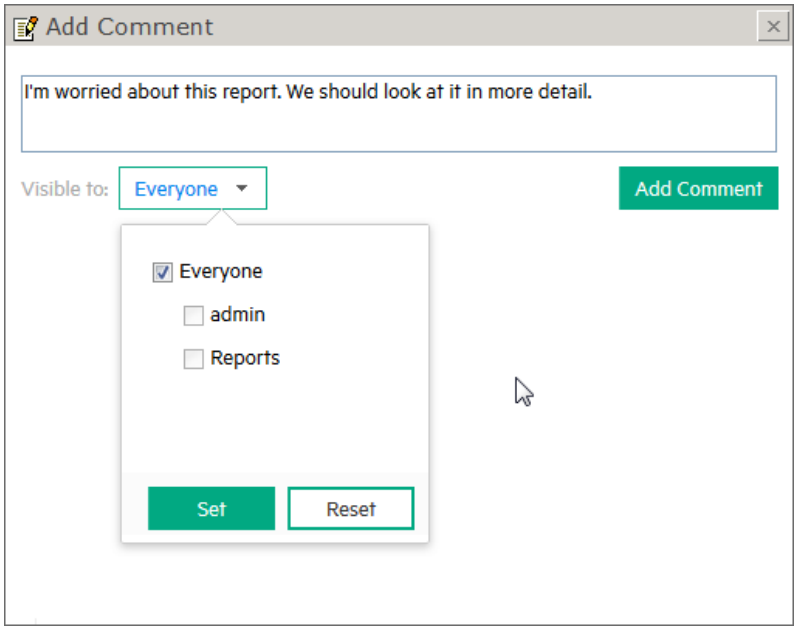
注: セキュリティ上の理由から、一度レポートに追加されたコメントを削除することはできません。

コメントをレポートに追加するには

1. レポート表示から以下のいずれかを実行します。
   - アドホックパワービューワのツールバーの をクリックします。
   - スマートレポートビューアーの [オプション] メニューにある [公開する...] を選択します。

[公開する] メニューダイアログが開きます。

2. **[コメントを追加 (Add Comment)]** をクリックします。[コメントを追加 (Add Comment)] ウィンドウが開きます。
3. テキストフィールドにコメントを入力します。



4. 必要に応じて **[表示対象: (Visible to:)]** ドロップダウンメニューをクリックして、このコメントの表示を特定のユーザーに許可するか、デフォルトのアクセス許可 (**[全員 (Everyone)]**) のままにします。「アクセス権限の割り当て」(163ページ) を参照してください。 **[セット (Set)]** をクリックします。
5. **[コメントを追加 (Add Comment)]** をクリックします。コメントはそのレポートと共に保存されます。
6. コメントを他のレポートビューアーから表示できるようにするには、**[公開する]** をクリックします。

レポートでのIPv6アドレスの検索

アドホックフィルターを使用すると、IPv6アドレスを含むフィールドを検索することができます。アドホックフィルターにこれらのフィールドが表示されるようにするには、フィールドを含むクエリオブジェクトを作成する必要があります。フィールドを含むクエリオブジェクトを作成すると、このクエリをレポートに追加できます。このクエリを作成するには、「レポートに使用するIPv6検索クエリの作成」(265ページ) を参照してください。

次のフィールドにはIPv6アドレスを含めることができます。

- deviceAddress
- agentAddress

- sourceAddress
- destinationAddress

IPv6アドレスの形式

クエリオブジェクトでIPv6アドレスを使用するには、Loggerが結果を返すことができるように、アドレスを正規の形式で指定する**必要があります**。たとえば、以下のように指定します。

```
SELECT from arc_deviceAddress, arc_agentAddress, arc_sourceAddress, arc_
destinationAddress

FROM events

WHERE arc_destinationAddress = "3ffe:b00::1:0:0:a"
```

(有効な英数字は`0-9`と`a-f`です。A-Fなどの大文字は**無効**です)

`3FFE:B00:0000:0000:0001:0:0:000A`のように非正規の形式を使用すると、上記のクエリは結果を返しません。

詳細については、「レポートに使用するIPv6検索クエリの作成」(265ページ)を参照してください。正規の形式については、https://tools.ietf.org/html/rfc5952のセクション4「A Recommendation for IPv6 Text Representation」を参照してください。

レポートの表示形式とエクスポート形式

どのレポートにもデフォルトの表示形式があります。ただし、大部分のレポートは、一般的な多くの形式で表示またはエクスポートできます。レポートを表示するときには、テンプレートやその他のフォーマット設定を使用できます。レポートのエクスポートでは、すべてのオプションにこれらの設定があるわけではありません。

各レポートで使用できる表示オプションの説明については、「表示オプション」(208ページ)を参照してください。各レポートで使用できるエクスポートオプションの説明については、「エクスポートオプション」(211ページ)を参照してください。

サポートされているレポート形式は、以下の表のとおりです。すべてのレポートがすべてのオプションをサポートするとは限りません。

レポートの表示形式

アイコン	形式	説明
	HTML	ハイパーテキストマークアップ言語。Web表示のデフォルト形式です。これらのレポートは、ナビゲーションオプションを持つHTMLレポートビューアーで表示されます。
	PDF	Adobeのページ記述形式。さまざまな環境に対応した印刷形式ですが、そのままでは編集できません。これらのレポートは、PDFビューアーで表示されます。

レポートの表示形式 (続き)

アイコン	形式	説明
	マイクロソフトエクセル	Microsoft ExcelのXLS形式。これらのスプレッドシート形式のレポートは、MS Excelで表示と編集ができ、ExcelのXLSテンプレート、グリッド、グラフなど、カスタマイズ可能なオプションを備えています。
	コンマ区切り	フォーマットされたカンマ区切り値 (CSV)。これらのスプレッドシート形式のレポートは、ExcelのXLSテンプレート、グリッド、グラフなど、カスタマイズ可能なオプションを備えています。
	FAST CSV	フォーマットされていないCSV。テンプレート、グリッド、グラフオプションなしでCSVファイルをダウンロードします。データを重視せず、フォーマットを必要としない場合、非常に大きいレポートを処理するには最速のオプションです。
	テキスト	ASCIIテキスト形式。
	マイクロソフトワード	Microsoft WordのDOC形式。これらのレポートは、MS Wordで表示と編集ができます。
	iHTML	単一ページのInteractive HTML。単純でページ分割のないテンプレートで高速実行されたスマートレポートであり、短いレポートをWebに素早く表示することができます。スマートレポートは、最小限の処理でデータを確認したいときのために、迅速に表示されるように設計されています。
	スマート	マルチページのInteractive HTML。単純でページ分割のないテンプレートで高速実行されたスマートレポートであり、長いレポートをWebに素早く表示することができます。スマートレポートは、最小限の処理でデータを確認したいときのために、迅速に表示されるように設計されています。

ヒント: 各ユーザーが使用できるレポート形式は、そのユーザーのユーザーアカウントに関連付けられているアクセス権によって異なります。「アクセス権限の割り当て」(163ページ)を参照してください。

レポートのページ分割について

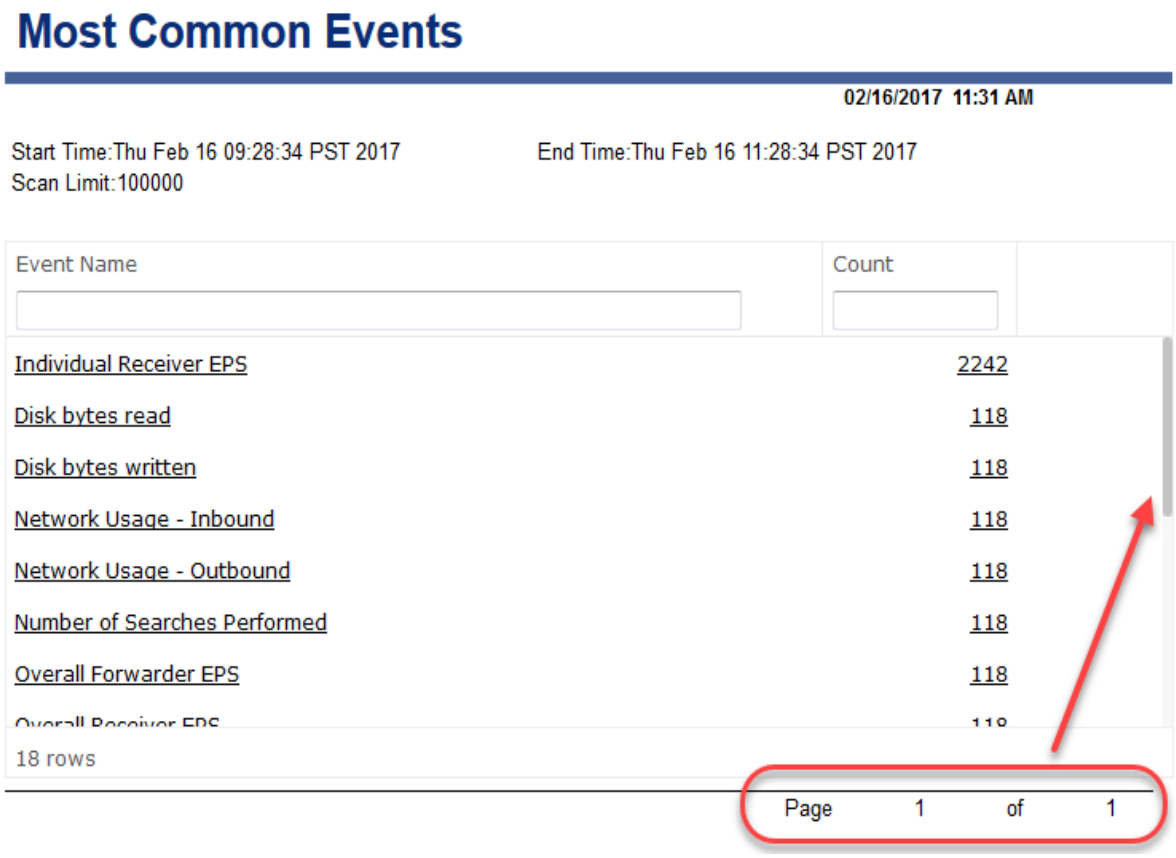
レポートに多くの列が含まれ、レポートクエリで指定したデフォルトの幅ではすべての列を表示できない場合、レポートは横方向でページ分割されて、残りの列が以降のページに表示されます。

たとえば、レポートに45個の列が含まれており、一度に5個しか表示できない場合、レポートは、1ページに列1から5、2ページに列6から10というようにページ分割されます。その結果、縦方向に表示可能な行数よりも多くの行がレポートに含まれる場合、2番目の行グループは10ページから開始されます。

現在Loggerでは、横方向のページ分割のページ数が10に制限されています。その結果、レポートにすべての列を表示するために必要なページが10を超える場合、完全なレポート結果

が表示されない可能性があります。そのようなレポートのすべての列を表示するには、クエリオブジェクトエディターで列の幅を手動で調整し、すべての列が10ページ以下に収まるようにします。「クエリの操作」(264ページ) を参照してください。

以下の例に示すように、単一ページレポートは、スクロールウィンドウに表示されます。

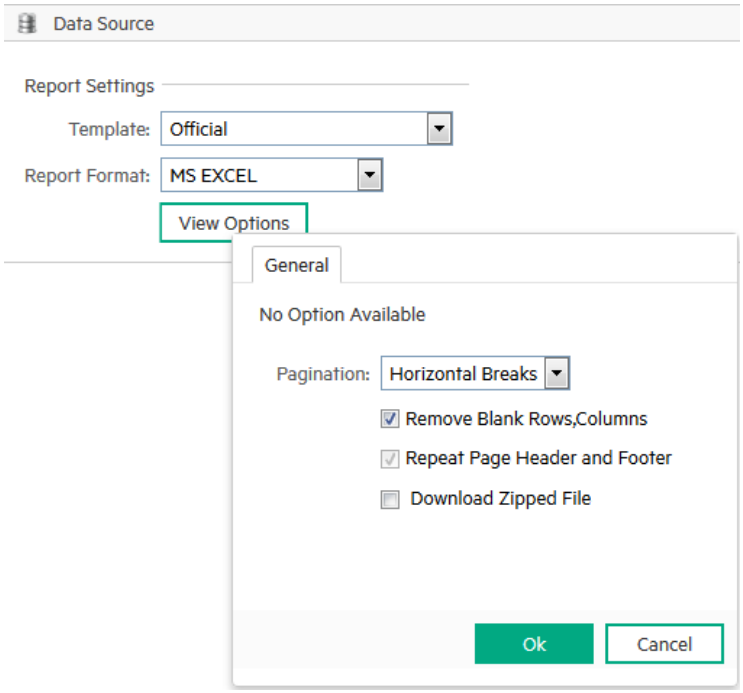


ヒント: このオプションは短いレポートに使用してください。長いレポートに使用すると、結果の一部が表示されなかったり、欠落したりする可能性があります。こうしたレポートには、複数ページオプションを使用してください。

表示オプション

レポート形式を選択するとき、その形式に関連する設定を表示し、指定するには、**[オプションを表示 (View Options)]** をクリックします。一部の形式では、必要に応じて、レポートに表示テンプレートを適用することができます。「テンプレートスタイル」(302ページ) を参照してください。

ヒント: エクスポートオプションは表示オプションと似ていますが、同じではありません。「エクスポートオプション」(211ページ) を参照してください。



以下の表に、すべてのレポートで使用できる表示オプションを示します。**太字**はデフォルトです。各形式オプションの説明については、「レポートの表示形式とエクスポート形式」(206ページ)を参照してください。

表示オプション - 全レポート

レポートの形式	オプション	設定
HTML	テンプレート (Template)	オプション
	ページ数 (Pagination)	1つのページ | 複数のページ | **水平区切り (Horizontal Breaks)**
PDF	テンプレート	オプション
	ページ数	1つのページ | 複数のページ | **水平区切り**
	圧縮済ファイルをダウンロード (Download Zipped File)	有効/**無効**
マイクロソフトエクセル	ページ数	1つのページ | 複数のページ | **水平区切り**
	ページ・ヘッダーとフッターを繰り返し (Repeat Page Header and Footer)	**有効**
	圧縮済ファイルをダウンロード	有効/**無効**

表示オプション - 全レポート (続き)

レポートの形式	オプション	設定
コンマ区切り	セパレータ	事前定義 [**コンマ** | タブ] | カスタム [文字を入力]
	エンクロージャ	事前定義 [**引用符** (" ")] | カスタム [文字を入力]
	テンプレートXLS	オプションのExcelテンプレート。
	Include	グリッド **はい**/いいえ | グラフ はい/**いいえ** | 行列 はい/**いいえ**
テキスト	ページ数	1つのページ | 複数のページ | **水平区切り**
	圧縮済ファイルをダウンロード	有効/**無効**
マイクロソフトワード	テンプレート	オプション
	ページ数	複数のページ
	圧縮済ファイルをダウンロード	有効/**無効**
Fast CSV	セパレータ	事前定義 [**コンマ** | タブ] | カスタム [文字を入力]
	エンクロージャ	事前定義 [**引用符** (" ")] | カスタム [文字を入力]
	ページ数	1つのページ
	圧縮済ファイルをダウンロード	有効/**無効**

以下の表に、スマートレポート専用の表示オプションを示します。**太字**はデフォルトです。

表示オプション - スマートレポート

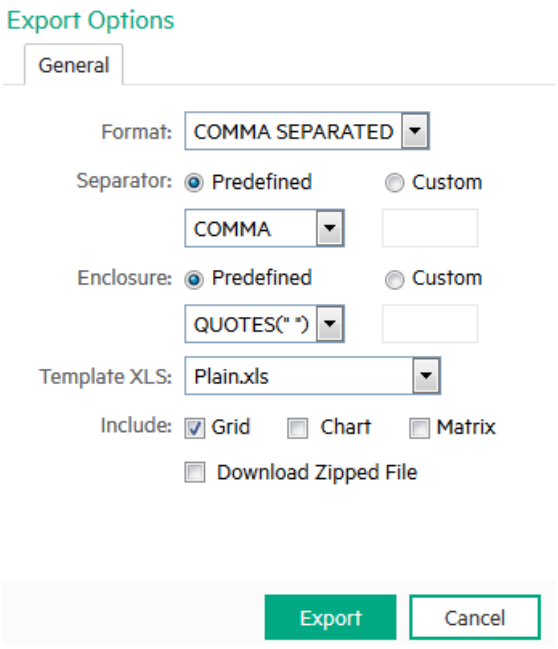
レポートの形式	オプション	設定
iHTML	ページ数	1つのページ
スマート	使用できるオプションはなし	基本的なページ分割表示

ヒント: 各ユーザーが使用できるレポート形式は、そのユーザーのユーザーアカウントに関連付けられているアクセス権によって異なります。「アクセス権限の割り当て」(163ページ)を参照してください。

エクスポート オプション

レポートをエクスポートするときには、レポートを表示する前に、レポート形式のエクスポートオプションを選択しておく必要があります。

ヒント: 一部のレポート形式では、表示オプションの数がエクスポートオプションの数を上回ります。「表示オプション」(208ページ) を参照してください。



以下の表に、各レポート形式の表示オプションを示します。**太字**はデフォルトです。

エクスポートオプション - 全レポート

レポートの形式	オプション	設定
マイクロソフトエクセル	圧縮済ファイルをダウンロード	有効/**無効**
PDF	圧縮済ファイルをダウンロード	有効/**無効**
	ページ設定	ページの向き、サイズ、余白を設定

エクスポートオプション - 全レポート (続き)

レポートの形式	オプション	設定
コンマ区切り(COMMA SEPARATED)	一般	• セパレータ (Separator): 事前定義 (Predefined) [**コンマ (COMMA)** | タブ] | カスタム (Custom) [文字を入力] • エンクロージャ (Enclosure): 事前定義 [**引用符 (" ") (QUOTES(" "))**] | カスタム [文字を入力] • テンプレートXLS (Template .xls): .XLSテンプレートを適用 **プレーン** • Include: グリッド (Grid) **はい**/いいえ | グラフ (Chart) はい/**いいえ** | 行列 (Matrix) はい/**いいえ** • 圧縮済ファイルをダウンロード 有効/**無効**
テキスト	圧縮済ファイルをダウンロード	有効/**無効**
マイクロソフトワード	圧縮済ファイルをダウンロード	有効/**無効**
	ページ設定	ページの向き、サイズ、余白を設定

以下の表に、スマートレポート専用のエクスポートオプションを示します。**太字** はデフォルトです。

エクスポートオプション - スマートレポート

レポートの形式	オプション	設定
iHTML	なし	使用できるオプションはなし
スマート	なし	使用できるオプションはなし

ヒント: MS Excel、Acrobat PDF、MS Wordの各形式を使用するスケジュール済みレポートでは、**[スマートエクスポート]** オプションを使用できます。レポートはそのネイティブ形式でエクスポートされるため、ユーザーは各ツールの機能を利用することができます。「スマートエクスポートとは」(188ページ) を参照してください。

レポートの発行

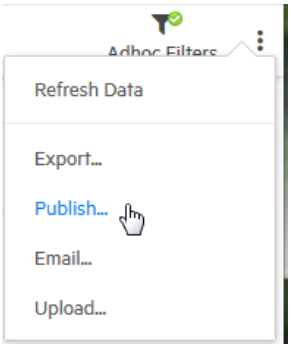
実行したレポートを公開すると、そのレポート実行の出力結果を後で使用するために保存することができます。また、スケジュールに基づいて実行されたレポートが公開されるように、スケジュールを設定することができます。スケジュールレポートの詳細については、「スケジュールレポート」(185ページ)を参照してください。

レポートの発行

レポートを公開すると、生成された出力を特定の形式と有効期限で保存することができます。プロセスはすべてのレポートで共通ですが、[公開する] メニューの表示にアイコンとメニューのどちらを使用するかはビューアーによって異なります。

スマートレポートを公開するには

1. レポートをスマート形式で実行します。「既存のレポートからの新しいレポートの作成」(224ページ)を参照してください。
2. スマートレポートビューアーの⋮をクリックして、オプションメニューを開きます。



3. メニューの **[公開する (Publish)...]** を選択します。[公開する] メニューが表示されます。
4. レポート公開の設定を指定します。「レポート公開オプション」(214ページ)を参照してください。
5. 必要に応じてレポートにコメントを追加します。「レポートへのコメントの追加」(204ページ)を参照してください。
6. **[公開する]** をクリックします。

アドホックレポートを公開するには

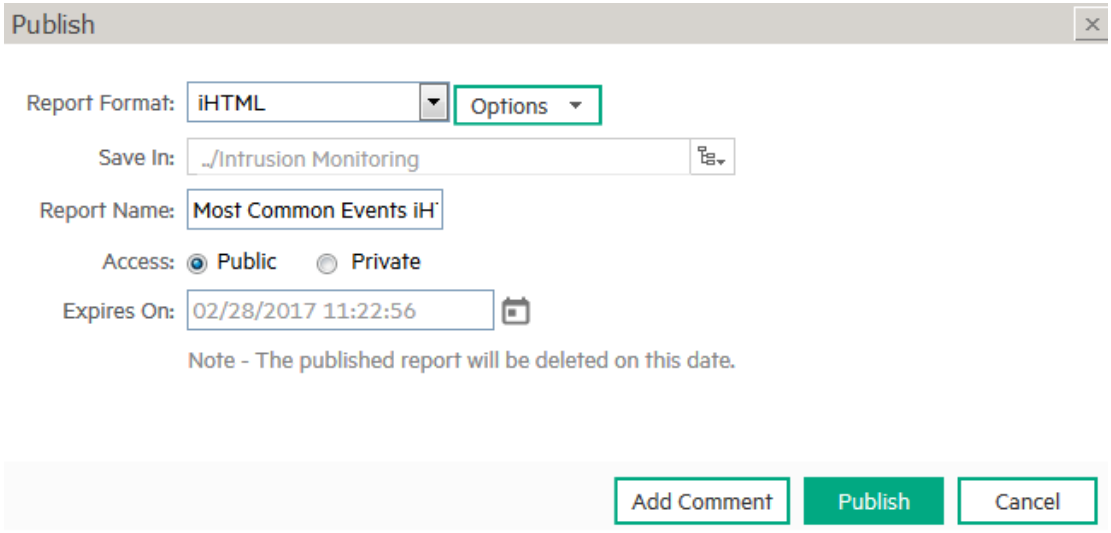
1. エクスプローラーからレポートをアドホック形式で実行します。
2. アドホックレポートビューアーの **[レポートを公開]** アイコンをクリックします。[公開する] メニューが表示されます。
3. レポート公開の設定を指定します。「レポート公開オプション」(214ページ) を参照してください。
4. 公開済みレポートにコメントを追加する場合は、**[コメントを追加]** をクリックします。「レポートへのコメントの追加」(204ページ) を参照してください。
5. **[公開する]** をクリックします。レポートが生成されると、[最近のレポート] ページの [公開済みレポート] リストにレポート名が表示されます。

公開済みレポートを削除するには

1. [最近のレポート] タブをクリックします。
2. アイコンをクリックして [公開済みレポート] ウィジェットを表示します。
3. ボタンをクリックして公開済みレポートを選択します。
4. をクリックして選択したレポートを削除します。アクションを確認します。

レポート公開オプション

レポートの公開には、以下の設定が必要です。必要に応じて、公開済みレポートにコメントを追加することができます。「レポートへのコメントの追加」(204ページ) を参照してください。



レポート公開オプション

設定	説明
レポートの形式 (Report Format)	レポートの出力形式。デフォルトの形式は、[HTML] です。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
保存場所 (Save In)	レポートを保存するカテゴリ (フォルダー) を指定します。カテゴリが指定されていない場合、公開されたレポートは、元のレポートが存在するカテゴリに保存されます。「レポートエクスプローラー」(171ページ) を参照してください。 **注:** レポートを最上位カテゴリの **[ルート]** に保存することはできません。アクセス権限がある場合は、新しいカテゴリを作成するか、既存のカテゴリに保存できます。
レポート名 (Report Name)	[公開済みレポート] リストに表示する名前を入力します。「公開済みレポート」(180ページ) を参照してください。
アクセス (Access)	アクセスの値を選択します。 • **[パブリック (Public)]** を選択すると、誰でもこのレポートを使用できるようになります。 • **[プライベート (Private)]** を選択すると、自分だけがこのレポートを使用できるようになります。
期限 (Expires on)	レポート出力を破棄する (そのため、表示できなくなる) 日時。レポートの結果を無期限に保持する場合は (つまり、期限切れがない場合)、このフィールドを空白にします。 **注:** 公開済みレポートは、Loggerのレポートサーバーに格納されます。サーバー領域を空けるために、有効期限を設定することをお勧めします。

公開済みレポートの操作

[公開済みレポート] ウィジェットでは、レポートの表示、保存、削除のほか、レポートに付加されたコメントも表示することができます。ウィジェット内でのレポートの表示方法や生成方法は、選択したファイル形式によって異なります。

- ブラウザーに表示可能なレポート形式は、新しいタブに表示されます。
- 別のアプリケーションで表示する必要のあるレポート形式は、新しいウィンドウに表示され、そこでレポートの保存、エクスポート、アップロードを行うことができます。

[公開済みレポート] のリストが長い場合は、公開名、日付、ソースレポート、その他のオプションを使用してリストをフィルタリングできます。

公開済みレポートを表示するには

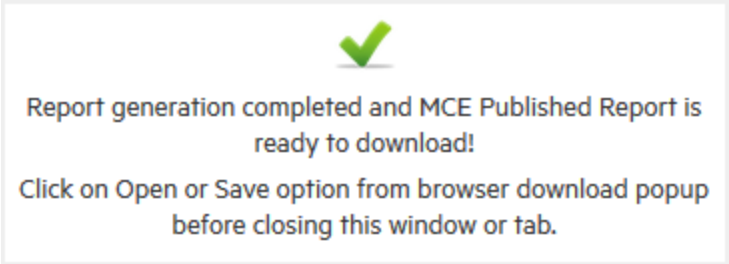
1. [最近のレポート] タブの ▶ をクリックして **[公開済みレポート (Published Reports)]** を開きます。

2. 公開済みレポートを選択します。
3. アイコンメニューから表示形式を選択してクリックします。「表示オプション」(208ページ) を参照してください。レポートは適切なビューワで表示されます。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
4. **[適用]** をクリックします。
5. 右上の  をクリックして [公開済みレポート] のリストに戻ります。

公開済みレポートをダウンロードするには

1. [最近のレポート] タブの  をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 公開済みレポートを選択します。
3. アイコンメニューから、PDF、CSV、Excel、Word、テキストなどのファイル形式を選択してクリックします。「表示オプション」(208ページ) を参照してください。

   新しいタブが開き、以下のようなメッセージが表示されます。



4. ブラウザーのポップアップウィンドウからダウンロードオプションを選択し、**[OK]** をクリックします。
5. 必要な情報を入力し、**[OK]** をクリックします。

公開済みレポートのコメントを表示するには

1. [最近のレポート] タブの  をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. 公開済みレポートを選択します。
3. アイコンメニューの  をクリックします。**[コメントを表示]** ウィンドウが開き、該当レポートに追加されたコメントが表示されます。
4. 確認を終えたら、**[完了]** をクリックします。「レポートへのコメントの追加」(204ページ) を参照してください。

公開済みレポートを削除するには

1. [最近のレポート] タブの  をクリックして **[公開済みレポート (Published Reports)]** を開きます。

2. 公開済みレポートを選択します。
3. をクリックし、アクションを確認します。[公開済みレポート] のリストからレポートのインスタンスが削除されます。

[公開済みレポート] のリストをフィルタリングするには

1. [最近のレポート] タブの をクリックして **[公開済みレポート (Published Reports)]** を開きます。
2. **[フィルター]** をクリックしてフィルターメニューを開きます。
3. フィルター条件を入力します。

注: これらのフィルター条件へのアクセスは、使用中のLoggerレポートのアクセス権限ポリシー、役割、自分自身のアクセス権限に基づきます。他の権限が必要になることもあります。「アクセス権限の割り当て」(163ページ) を参照してください。

フィルター条件	説明
次を含む公開済みの名前	公開済みレポートの名前の一部または全部を示すテキスト文字列を入力します。
更新の間に	レポートを更新時刻で絞り込むために、日付の範囲を入力します。日付を`MM/dd/yyyy`形式で手入力するか、をクリックして日付選択カレンダーを開きます。
レポートの選択	をクリックして [オブジェクト選択] ウィンドウを開きます。レポートまたはフォルダーを選択します。
孤立行	レイアウト (親レポート) が存在しない (見つからない、または削除された) 公開済みレポートを検索する場合にのみ、**[孤立行]** をオンにします。
オーナーの選択	ユーザーがアクセス権限を持つレポートオーナーから選択します。
Private Owned By	ユーザーがアクセス権限を持つプライベートレポートから選択します。
Public Owned By	ユーザーがアクセス権限を持つオーナーリストからパブリックレポートオーナーを選択します。

4. 必要に応じて **[(ルート)]** をクリックしてカテゴリフィルターを開き、目的の公開済みレポートまで移動します。
5. **[更新]** をクリックします。フィルタリングされたリストが表示されます。

レポートのエクスポートとアップロード

生成したレポートは、他の形式で使用するためにエクスポートしたり、FTPサイトや共有フォルダーにアップロードしたりすることができます。

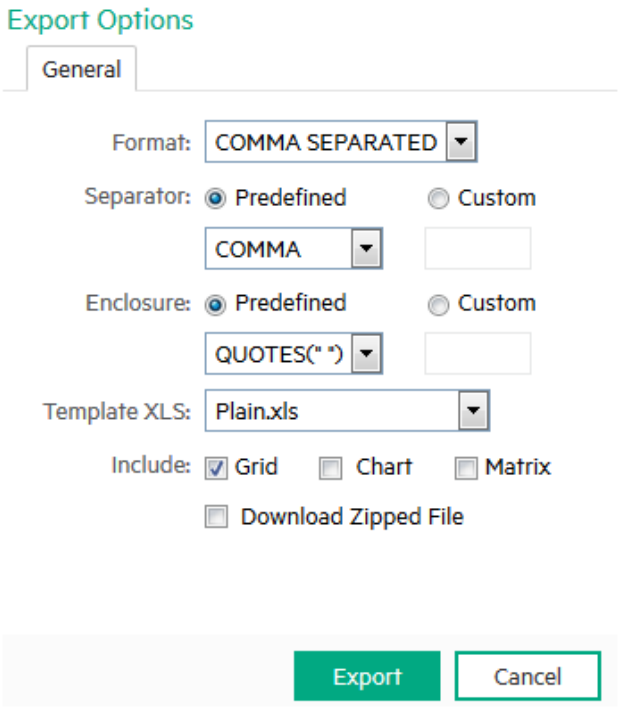
レポートのエクスポートと保存

レポートは、選択したファイルフォーマットでエクスポートして保存できます。

レポートをエクスポートし保存するには

1. レポートの表示中に以下のいずれかのアクションを行います。
   - スマートレポートビューアーの右上にあるをクリックしてビューアーのメニューを開き、**[エクスポート]** をクリックします。「スマートレポートビューアー」(203ページ) を参照してください。
   - アドホックレポートビューアーの [エクスポート] アイコンをクリックして [エクスポート] ダイアログを開きます。「アドホックレポートビューアー」(201ページ) を参照してください。
2. **[エクスポート関連オプション (Export Options)]** ダイアログで、[フォーマット (エクスポート用) (Export Format)] および関連する設定を指定します。「エクスポートオプション」(211ページ) を参照してください。

選択したエクスポートフォーマットに応じて、他の設定が表示されます。



3. **[エクスポート (Export)]** をクリックします。

生成されたレポートは、ローカルなファイルか、他のファイルと同様に任意の場所に保存できます。

サーバーまたはFTPサイトへのレポートのアップロード

サーバーまたはファイル転送プロトコル (FTP) サイトにレポートをアップロードすることができます。

レポートをアップロードするには

1. レポートの表示中に以下のいずれかのアクションを行います。
   - スマートレポートビューアーの右上にあるをクリックしてビューアーのメニューを開き、**[アップロード]** をクリックします。「スマートレポートビューアー」(203ページ) を参照してください。
   - アドホックレポートビューアーの [アップロード] をクリックするか、別の出力フォーマットを直接クリックします。「アドホックレポートビューアー」(201ページ) を参照してください。

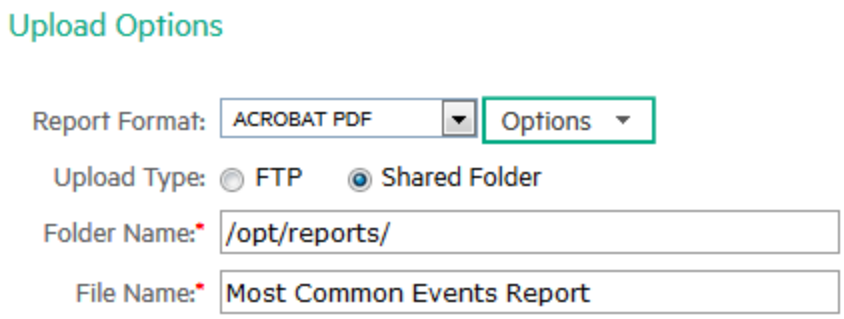
   [アップロード・オプション] メニューが表示されます。
2. レポート形式とアップロードオプションを選択します。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。

ヒント: アップロードオプションはエクスポートオプションに似ていますが、アップロードでは、圧縮済みファイルのデフォルトは **[はい]** です。

3. アップロードの種類を **[FTP]** と **[共有フォルダ]** から選択します。
   - [FTP] を選択する場合、「FTPのアップロードオプション」(221ページ) を参照してください。
   - [共有フォルダ] を選択する場合、「共有フォルダーのアップロードオプション」(220ページ) を参照してください。
4. アップロードの種類に該当する必須フィールドとオプションフィールドに入力します。
5. **[アップロード]** をクリックします。確認メッセージが表示されます。
   指定したフォルダーまたはサーバーにレポートがアップロードされます。

共有フォルダーのアップロードオプション

Loggerレポートを共有フォルダーにアップロードする場合は、以下のフィールドに入力します。

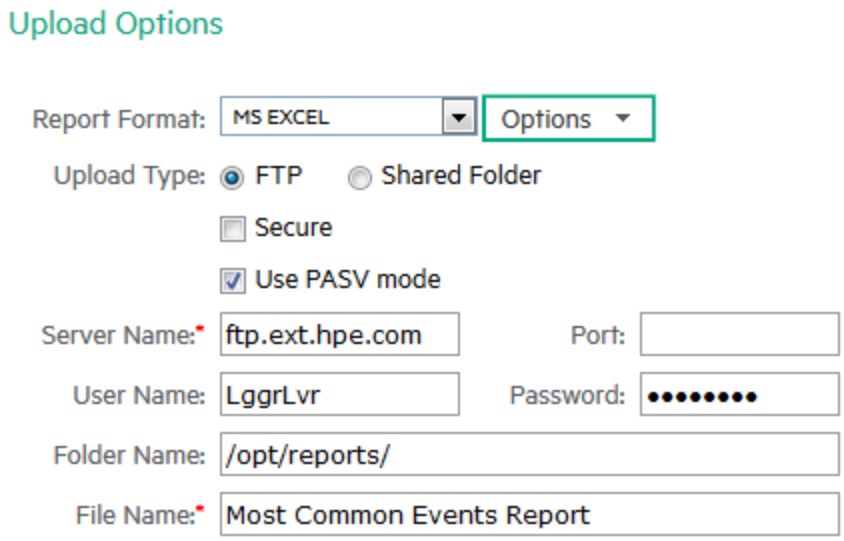


共有フォルダーにアップロードする場合のメニューフィールド

フィールド	説明
フォルダ名 (Folder Name)	(必須) レポートのアップロード先となる共有フォルダーのフォルダーパスを入力します。
ファイル名 (File Name)	(必須) レポートのファイル名を入力します。

FTPのアップロードオプション

Loggerレポートをファイル転送プロトコル(FTP)サイトにアップロードする場合は、以下のフィールドに入力します。



FTPにアップロードする場合のメニューフィールド

フィールド	説明
Secure	ファイルをアップロードするためにSecure Shell (SSH) FTPプロトコルを使用します。
PASVモードを使用 (Use PASV mode)	ファイルをアップロードするためにPassive FTPプロトコルを使用します。
サーバー名 (Server Name)	(必須) ターゲットサーバーのホスト名またはIPアドレスを入力します。
ポート (Port)	必要な場合、ポート番号を入力します。
ユーザ名 (User Name)	ターゲットサーバーにログインするときのサーバーのユーザー名を入力します。
フォルダ名 (Folder Name)	レポートのアップロード先となるターゲットサーバー上のフォルダーパスを入力します。
ファイル名 (File Name)	(必須) レポートのファイル名を入力します。

レポートのメール送信

レポートを、Webリンクまたは添付ファイルとしてメールで送信できます。

前提条件

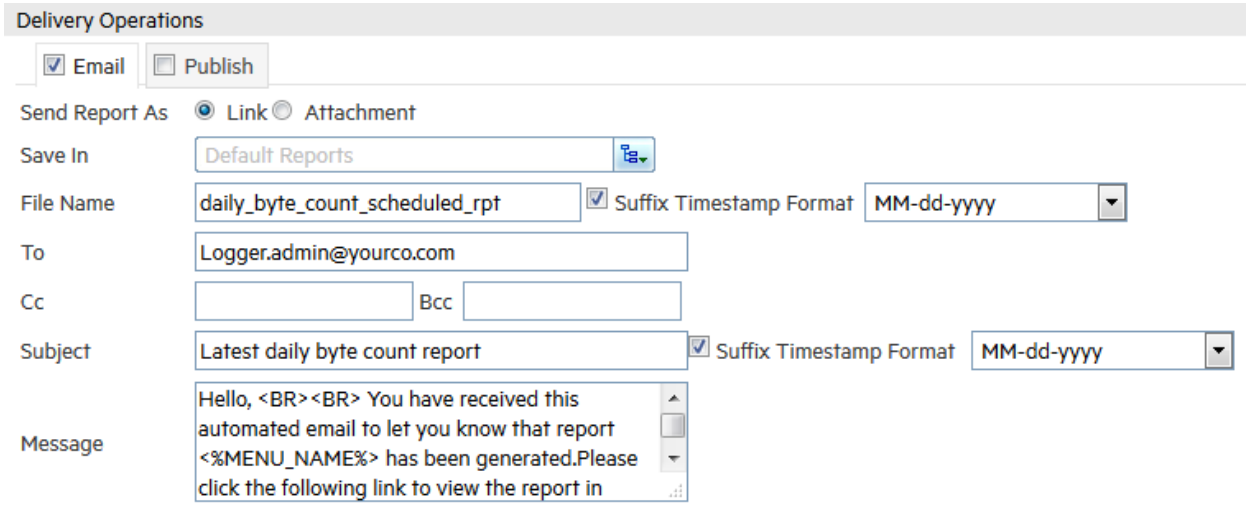
レポートをメールで送信する前に、まずレポート用のSMTPを設定する必要があります。**[レポート] > [レポート管理]** に移動し、SMTPの設定を行います。「レポートの設定」(305ページ)を参照してください。

レポートをメールで送信するには

1. アドホックレポートビューアーのメニューバーにある [電子メールレポート] アイコン ( ) をクリックします。
2. 電子メールの配布設定を指定します。「電子メールの配布設定」(222ページ)を参照してください。
3. **[電子メール]** をクリックしてレポートを送信します。

電子メールの配布設定

スケジュール済みのレポートまたは他のレポートの電子メールを生成するには、以下の設定を入力する必要があります。形式、配布オプション、パラメーターなどの他の設定も指定しなければならない場合があります。



電子メールの配布設定

設定	説明
名前を付けてレポートを送信 (Send Report As)	以下のいずれかを選択します。 • **リンク (Link)**: メールの本文にレポートのリンクを挿入します。 • **エンクロージャ (Attachment)**: レポートを電子メールの添付ファイルとして送信します。
ファイル名 (File	レポートのファイル名を入力します。

電子メールの配布設定 (続き)

設定	説明
Name)	
接尾辞タイムスタンプ形式 (Suffix Timestamp Format)	(オプション) ファイル名にタイムスタンプを追加するかどうかを指定します。ドロップダウンメニューからタイムスタンプの形式を選択します。
[宛先]、[CC]、[BCC]	**宛先**: (必須) 有効な電子メールアドレスを1つ以上入力します。アドレスのセパレータとして、コンマまたはセミコロンを使用します。**[CC]** と **[BCC]** はオプションです。
件名 (Subject)	電子メールの件名を入力します。
メッセージ (Message)	用意されている電子メールの本文を変更するか、デフォルトをそのまま使用します。 メッセージテキストには、システムパラメーターだけでなく、ユーザーパラメーターも追加できます。たとえば、電子メールで送信するレポートに`ReportDate`というパラメーターがある場合、このパラメーターを `<%ReportDate%>` としてメッセージテキストに挿入できます。この部分には、レポート実行の日付が代入されます。

カスタムレポートのデザイン

カスタムクエリ、テンプレート、検索パラメーターなどのレポートオブジェクトを使用して、新しいレポートやカスタマイズしたレポートを作成することができます。このセクションでは、レポートの設計ツールを使用して、これらのオブジェクトを組み合わせて新しいレポートを作成する方法について説明します。レポートオブジェクト自体を作成する方法については、「クエリ、パラメーター、テンプレートのデザイン」(262ページ)を参照してください。ロゴやグラフの追加、表示オプションの変更など、レポート結果の変更については、「スマートレポートデザイナー」(227ページ)および「アドホックパワービューワデザイナー」(232ページ)を参照してください。

既存のレポートからの新しいレポートの作成

Loggerには、一般的なセキュリティシナリオ向けに、あらかじめ作成された各種の有用なレポートが付属しているため、それをそのまま使用することも、新しいレポートを作成するためのテンプレートとして使用することもできます。レポート作成に慣れるには、まず、必要な機能を含む既存のレポートを新しい名前で保存し、そのレポートを変更することをお勧めします。「スマートレポートとアドホックおよびスタジオレポートとの違いは?」(168ページ)を参照してください。

注意: レポートとArcSightで定義されたコンテンツに対する変更は、コンテンツをアップグレードすると警告なく上書きされます。ArcSightで定義されたコンテンツを直接変更しないでください。

通常の手順として、ArcSightで定義されたコンテンツのコピーを変更してください。そうすれば、以降のアップグレードで変更内容が影響を受けなくなります。

既存のレポートを基に新しいLoggerレポートを作成するには

1. **エクスプローラー**で、新しいレポートの原案として使用するレポートを参照します。
2. このレポートを選択し、コンテキストメニューから **[このレポートをカスタマイズ]** をクリックします。

   ヒント: レポートをカスタマイズするオプションがない場合 (かつ、正しいアクセス権限がある場合)、まずレポートを実行し、[最近のレポート] リストからレポートを開きます。「カスタムレポートのデザイン」(223ページ)および「最近のレポート」(178ページ)を参照してください。

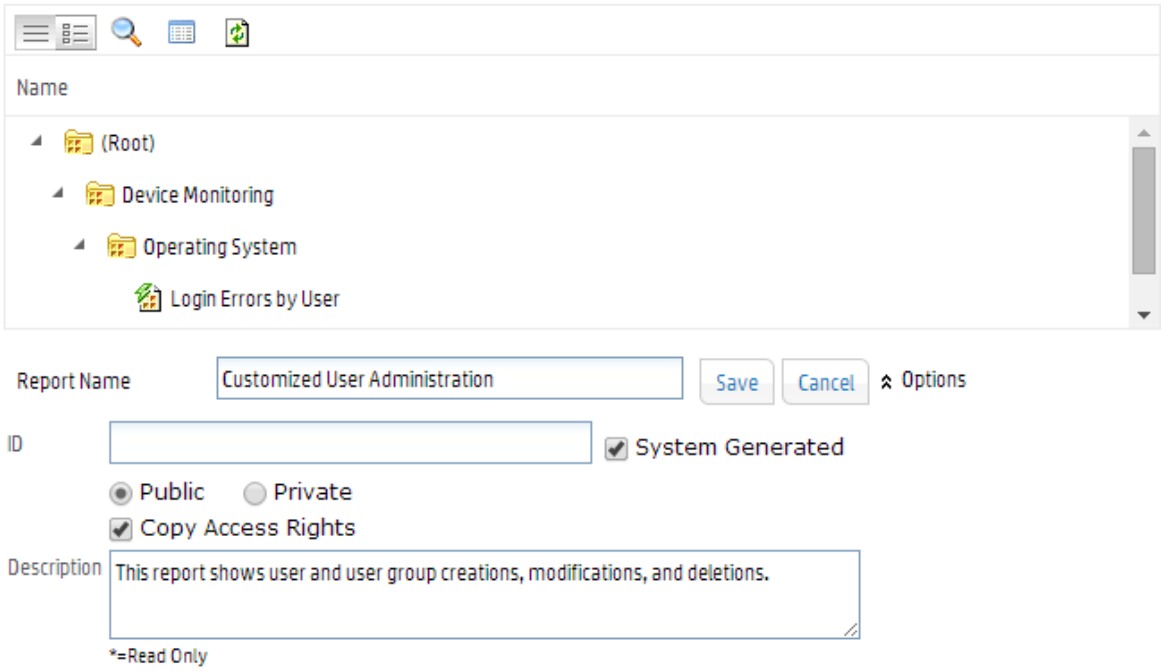
3. フィルターデータがあれば入力します。「追加フィルター」(196ページ)を参照してください。**[適用]** をクリックします。

   レポートが実行され、適切なデザイナーでレポートが開きます。ここでレポートをカスタマイズし、データを表示するグラフ、表、マップを作成できます。「カスタムレポートのデザイン」(223ページ)を参照してください。

   注: ArcSightまたは他のカスタム開発者ソースから入手したレポートなど、一部のレポートは、編集できない可能性があります。そのようなレポートでは、[このレポートをカスタマイズ] リンクは無効になっています。

4. 右下の **[保存]** の横にある▼をクリックしてメニューを開きます。
5. **[名前を付けて保存]** をクリックします。これにより、選択したレポートの **[レポート・レイアウトを名前を付けて保存]** ダイアログが表示されます (また、選択したレポートと同じカテゴリに含まれるすべてのレポートが表示されます)。

6. **[レポート名 (Report Name)]** にレポートの名前を入力します。



7. **[オプション (Options)]** をクリックし、以下の項目の値を入力します。

オプション	説明
ID	必要に応じてレポートのカスタムIDを入力します。または、**[生成済みシステム (System Generated)]** を選択して、IDを自動的に生成します (デフォルトで選択されています)。
パブリック/プライベート (Public/Private)	どちらかを選択します。[パブリック (Public)] を選択した場合、誰でもこのレポートにアクセスできます。[プライベート (Private)] の場合は自分だけがアクセスできます。
説明 (Description)	必要に応じてレポートの説明を入力します。

8. **[保存 (Save)]** をクリックします。
9. **[OK]** をクリックして保存を確認します。新しいレポートが、レポートを保存したカテゴリの下に表示されます。

Loggerレポートデザイナーの操作

どのレポートをどのデザイナーで扱うべきかわからない場合は、以下の手順に従ってください。

アドホックパワービューワでのアドホックレポートまたはスタジオレポートのカスタマイズ

1. [レポート] メニューから **[エクスプローラー]** をクリックしてエクスプローラーを開きます。
2. カスタマイズするレポートを右クリックしてコンテキストメニューを開きます。「エクスプローラーのオプションとコンテキストメニュー」(175ページ) を参照してください。
3. [スマート形式で実行] 以外の実行オプションを選択します。「レポート実行オプションについて」(191ページ) を参照してください。
4. レポートを実行すると、レポートがアドホックパワービューワに表示されます。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
5. 元のレポートを保存する場合は、表形式の結果の中を右クリックしてコンテキストメニューを開き、**[名前を付けてレイアウトを保存]** をクリックします。

スマートデザイナーでのアドホックレポートまたはスマートレポートのカスタマイズ

1. [レポート] メニューの [デザイン] セクションから **[新しいレポート]** をクリックして [スマートビュー] ページを開きます。
2. **[既存のレポートを開く...]** をクリックして [レポートのレイアウトを開く] メニューを開きます。
3. カスタマイズするレポートに移動し、選択します。
4. **[開く]** をクリックします。レポートが実行され、スマートデザイナーで表示されます。「スマートレポートデザイナー」(227ページ) を参照してください。
5. 元のレポートを保存する場合は、右下のメニューの **[名前を付けて保存]** をクリックします。

アドホックデザイナーでのアドホックレポートまたはスタジオレポートのカスタマイズ

エクスプローラーから

1. [レポート] メニューから **[エクスプローラー]** をクリックしてエクスプローラーを開きます。
2. カスタマイズするレポートを右クリックしてコンテキストメニューを開きます。「エクスプローラーのオプションとコンテキストメニュー」(175ページ) を参照してください。
3. **[カスタマイズ]** をクリックしてアドホックデザイナーでレポートを開きます。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
4. 元のレポートを保存する場合は、右上のメニューの **[名前を付けて保存]** をクリックします。

アドホックデザイナーから

1. [レポート] メニューの [クラシック] セクションから **[新しいレポート]** をクリックしてアドホックデザイナーを開きます。「新しいクラシックレポートの作成」(235ページ) を参照してください。
2. 右上のメニューの **[開く]** をクリックして [レポートのレイアウトを開く] メニューを開きます。
3. カスタマイズするレポートに移動し、選択します。

4. **[開く]** をクリックしてアドホックデザイナーでレポートを開きます。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
5. 元のレポートを保存する場合は、右上のメニューの **[名前を付けて保存]** をクリックします。

スマートレポートデザイナー

スマートレポートデザイナーは、スマートレポートの取得、表示、正確なレイアウト指定のために使用します。

エクスプローラーからのスマートレポートデザイナーの表示

1. [レポート] メニューから **[エクスプローラー]** をクリックします。
2. スマートレポートを選択し、コンテキストメニューから **[カスタマイズ]** をクリックします。レポートが実行され、スマートデザイナーで表示されます。
3. 必要に応じて、アドホックレポートを選択します。
   - **[スマート形式で実行]** をクリックします。レポートが実行され、スマートビューアーで表示されます。
   - レポートを**公開**します。
   - レポートを実行し、公開したら、エクスプローラーに戻ります。
   - レポートを選択し、コンテキストメニューから **[カスタマイズ]** をクリックします。レポートが実行され、スマートデザイナーで表示されます。

[最近のレポート] からのスマートレポートの表示

1. [最近のレポート] リストからスマートレポートを選択します。
2. レポートを実行または再実行します。レポートが実行され、スマートデザイナーで表示されます。

[レポート] メニューからのスマートレポートデザイナーの表示

1. [レポート] メニューの [デザイン] セクションから **[新しいレポート]** をクリックします。[新しいレポート] タブで **[Smart View]** ページが開きます。
   - **[クエリオブジェクトの選択]** リストにあるレポートをダブルクリックすると、Loggerはそのレポートを実行し、スマートデザイナーで編集用に開きます。ここでは、レポートの保存と変更を実行できます。ロゴやグラフの追加、表示オプションの変更など、レポート結果の変更については、「スマートレポートデザイナー」(227ページ) および「アドホックパワービューワデザイナー」(232ページ) を参照してください。

- 右下隅にある **[既存のレポートを開く...]** をクリックすると、保存したレポートの公開済みのコピーを選択できます。Loggerはレポートを実行し、スマートデザイナーで表示します。ここでは、レポートの保存と変更を実行できます。
- 新しいクエリを最初から作成するには、右下隅にある **[クエリオブジェクトの作成...]** をクリックします。Smart Viewでクエリページが開きます。「クエリ」(262ページ) を参照してください。

新しいスマートレポートの作成

新しいスマートレポートを作成するには

1. [レポート] メニューの [デザイン] セクションから **[新しいレポート]** をクリックします。[新しいレポート] タブで **[Smart View]** ページが開きます。
   - **[クエリオブジェクトの選択]** リストにあるレポートをダブルクリックすると、Loggerはそのレポートを実行し、スマートデザイナーで編集用に開きます。ここでは、レポートの保存と変更を実行できます。ロゴやグラフの追加、表示オプションの変更など、レポート結果の変更については、「スマートレポートデザイナー」(227ページ) および「アドホックパワービューワデザイナー」(232ページ) を参照してください。
   - 右下隅にある **[既存のレポートを開く...]** をクリックすると、保存したレポートの公開済みのコピーを選択できます。Loggerはレポートを実行し、スマートデザイナーで表示します。ここでは、レポートの保存と変更を実行できます。
   - 新しいクエリを最初から作成するには、右下隅にある **[クエリオブジェクトの作成...]** をクリックします。Smart Viewでクエリページが開きます。「クエリ」(262ページ) を参照してください。

スマートレポートのグラフへの注釈の付加

[グラフのプロパティ] メニューの [説明] フィールドを使用して、レポートのグラフに注釈 (説明またはコメント) を付加することができます。グラフのプロパティの詳細については、「グラフ」(246ページ) を参照してください。

ヒント: このリリースでは、スマートレポートのグラフのみ、この方法で注釈を付加できます。

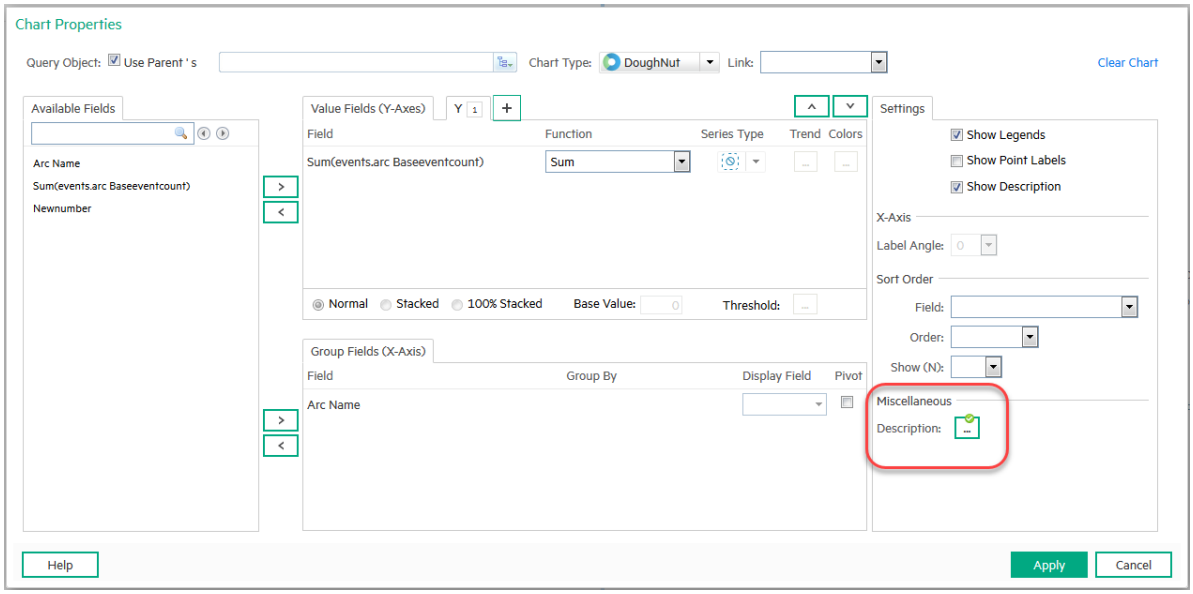
スマートレポートに注釈を付加するには

1. エクスプローラーから、グラフを含むスマートレポートを実行します。
2. レポートが [編集モード (Edit Mode)] であることを確認します。

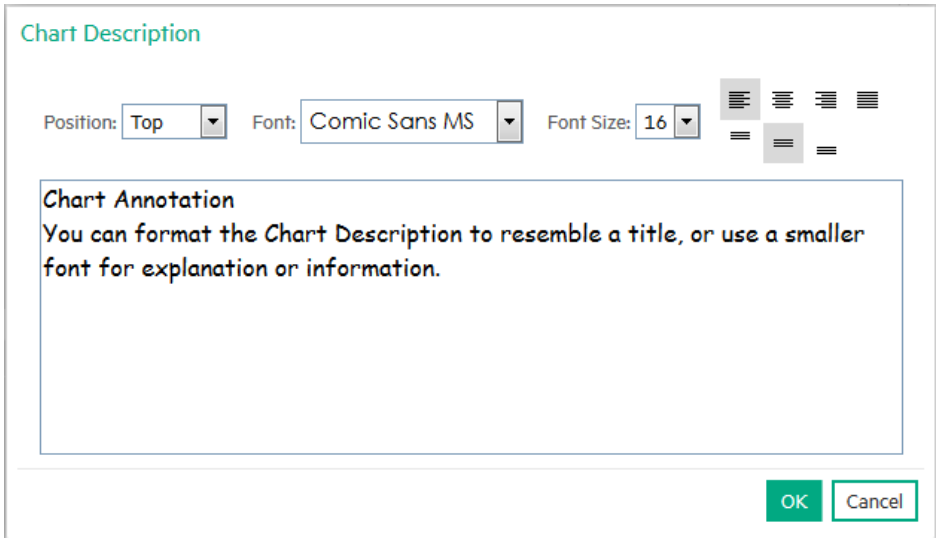
グラフの編集ツールが表示されます。

3. をクリックして [グラフのプロパティ (Chart Properties)] ウィンドウを開きます。「グラフ」(246ページ) を参照してください。

4. [設定 (Settings)] タブの [雑 (Miscellaneous)] セクションにある をクリックして、[説明 (Description)] メニューを開きます。



5. [説明 (Description)] メニューで注釈を作成し、**[OK]** をクリックします。



ヒント: 説明の配置先と大きさによって、グラフの表示サイズが変わることがあります。グラフがダッシュボードの一部の場合、レイアウトにリッチテキストウィジェットを追加す

ると、グラフを圧縮せずに情報を表示することができます。

6. グラフの変更が終了したら、**[適用 (Apply)]** をクリックします。グラフに注釈が表示されます。
7. グラフが目的どおりの形で表示されたら、必ず **[保存]** または **[名前を付けて保存]** (右下) をクリックしてレポートを保存してください。

プライベートレポート

すべてのレポートを表示、実行、スケジュールするためのアクセス権を持っている場合は、**プライベート**レポートを作成できます。変更したい**パブリック**レポートを編集するアクセス権がなく、プライベートレポートを作成するためのアクセス権がある場合は、パブリックレポートをプライベートレポートとして保存し、プライベートレポートを編集することができます。

レポートをパブリックまたはプライベートとして発行する方法の詳細については、「レポート公開オプション」(214ページ)を参照してください。レポートのアクセス権の詳細については、「アクセス権限の割り当て」(163ページ)を参照してください。

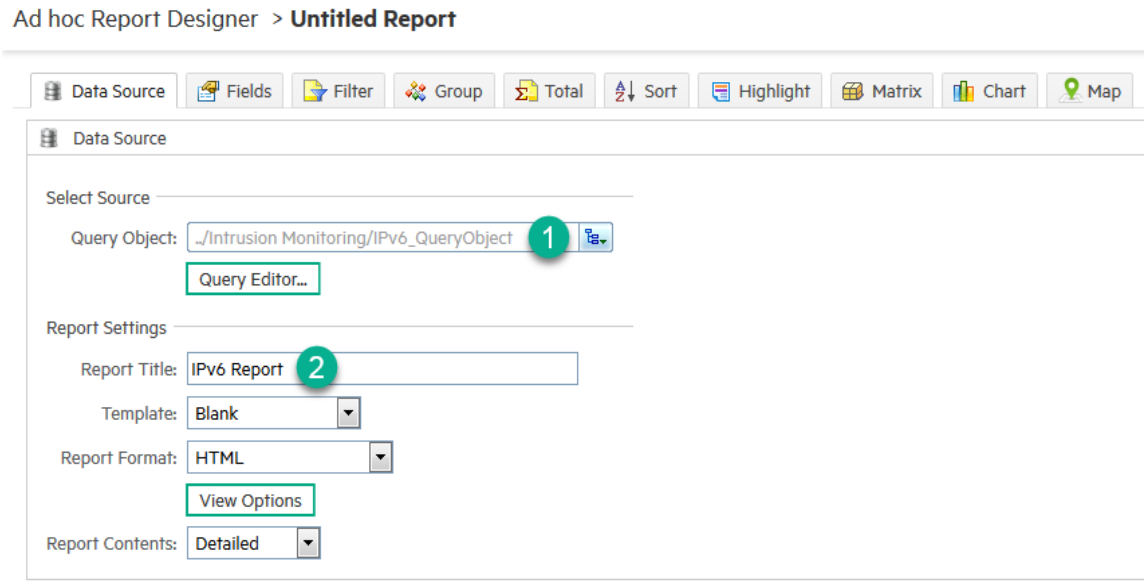
IPv6レポートの作成

前提条件

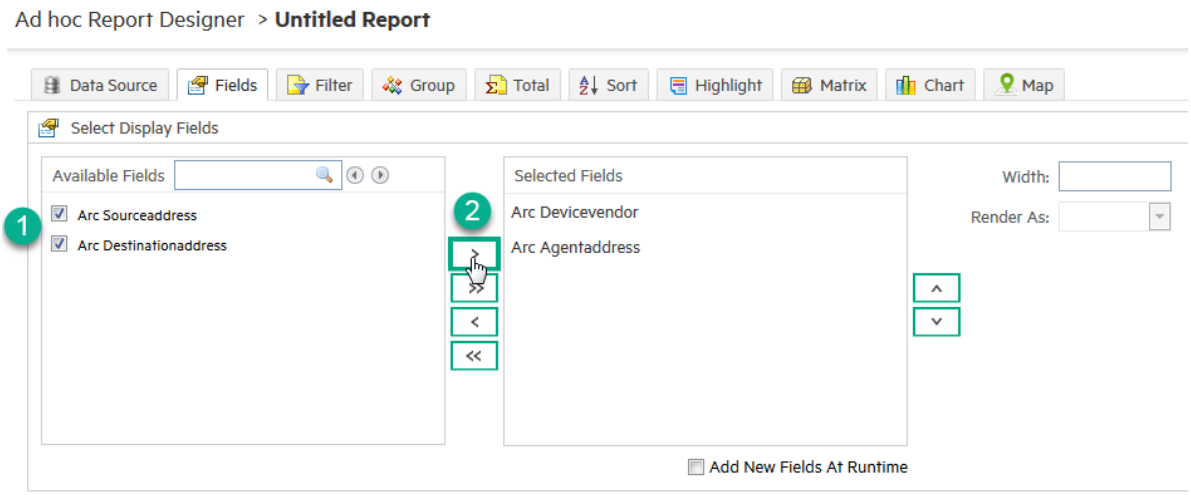
IPv6イベントを表示するレポートを作成する前に、まず、IPv6情報を取得するクエリを作成する必要があります。「レポートに使用するIPv6検索クエリの作成」(265ページ)を参照してください。

IPv6クエリを組み込んだレポートを作成するには

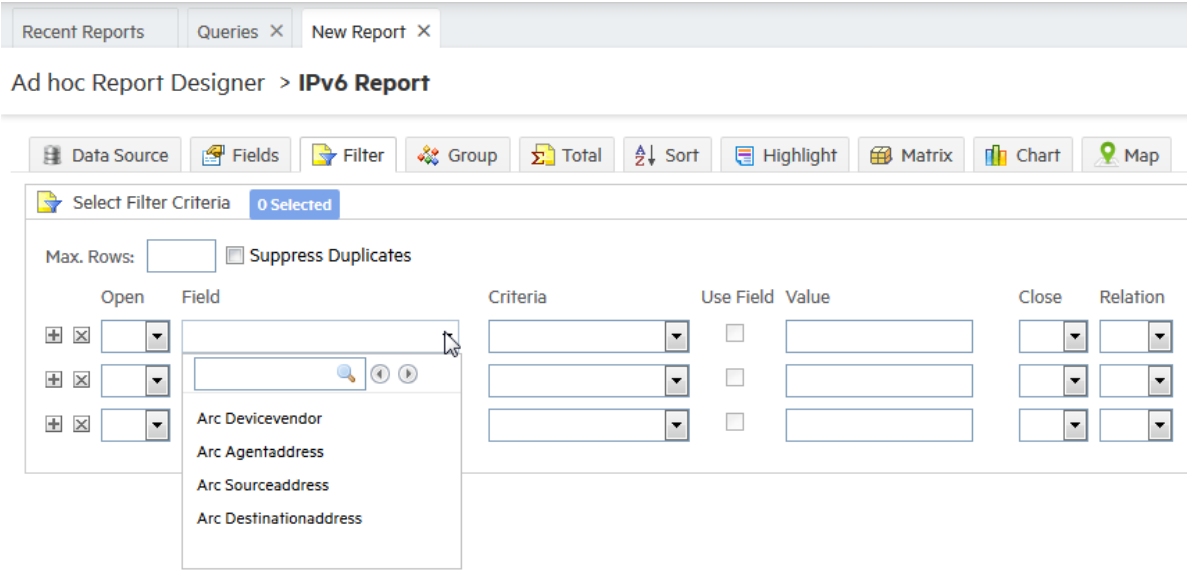
1. **[レポート]** > **[クラシック]** > **[新しいレポート]** の順に移動します。



2. **[フィールド (Fields)]** タブを開きます。**[選択したフィールド (Selected Fields)]** カラムから、レポートに表示するフィールドを選択します。IPv6アドレスフィールドをすべて選択します。



3. レポートを保存します。このレポートは、エクスプローラーから使用できるようになります。



ヒント: [フィルター (Filter)] タブを確認すると、フィールドのリストが表示されます。デフォルトでは、フィルターは実行時の前に設定できますが、実行時にも使用することができます。

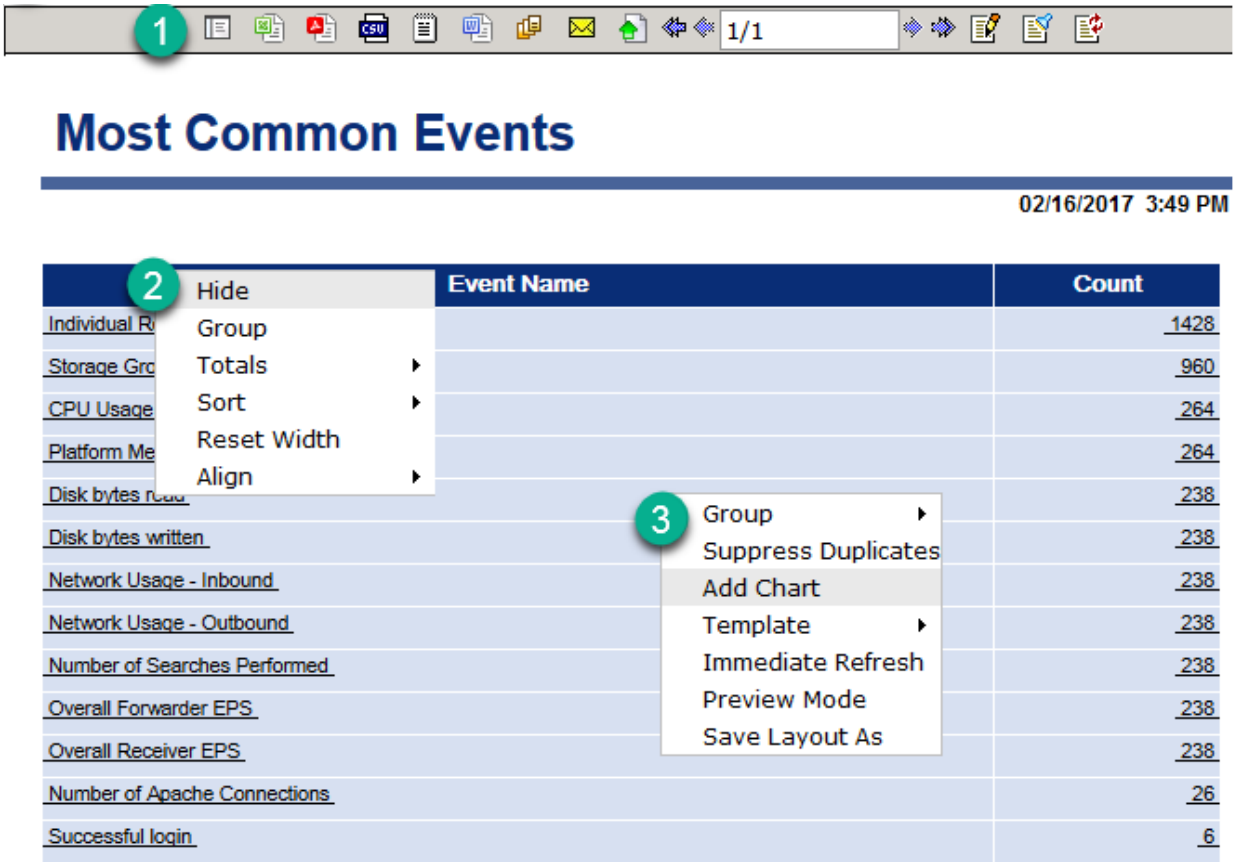
アドホックパワービューワとクラシックレポートデザイナー

どのレポートも、アドホックパワービューワか、[クラシック] > [新しいレポート] で表示されるアドホックレポートデザイナーで変更することができます。どちらのツールの機能も同じです。

- **アドホックパワービューワ**: レポートビューワから直接使用でき、変更内容をリアルタイムに確認することができます。レポート内を右クリックすると、オプションメニューが表示されます。「アドホックパワービューワデザイナー」(232ページ) を参照してください。
- **アドホックレポートデザイナー**: ツールキット環境で使用でき、ツール内のタブからさまざまなレポート要素を使用できます。「クラシック: アドホックレポートデザイナー」(233ページ) を参照してください。

アドホックパワービューワデザイナー

エクスプローラーまたは [最近のレポート] からアドホックレポートを実行すると、アドホックレポートはアドホックパワービューワデザイナーに表示されます。[表示] メニューツールバーだけでなく、データ表示内の右クリックでも、レポートの変更や、他の表示オブジェクトの追加を行うことができます。



ヒント: レポートのヘッダーやデータを右クリックすると、アドホックビューアーのコンテキストメニューが表示されます。

アドホックパワービューワには、次のメニューまたは作業領域があります。

ID	エリア	オプション	参照項目
1	メニューバー	レポートの公開、エクスポート、閲覧、コメントの追加と表示	「アドホックビューアーのメニューオプション」(202ページ)。
2	ヘッディングコンテキストメニュー	カラムヘッダーを右クリックして、オプションメニューを表示	
3	データコンテキストメニュー	データ内で右クリックして、オプションメニューを表示	

クラシック: アドホックレポートデザイナー

アドホックパワービューワよりクラシックレポートデザイナー(別称「アドホックレポートデザイナー」)の方が好みの場合、このクラシックツールを使用してレポートの作成と編集を行うことができます。「スマートデザインツールとアドホックデザインツールの違いは?」(170ページ)を参照してください。

レポートコンポーネント

レポートはさまざまなコンポーネントで構成されています。コンポーネントを使用して、レポートでのデータ表示方法を変更できます。[デザイナー] ページの上にある各コンポーネントのタブをクリックすると、コンポーネントの設定ページが開きます。

タブ	説明
データソース (Data Source)	詳細については、「データソース」(236ページ) を参照してください。
フィールド (Fields)	詳細については、「フィールド」(237ページ) を参照してください。
フィルタ (Filter)	詳細については、「フィルター」(238ページ) を参照してください。
グループ (Group)	詳細については、「グループ」(241ページ) を参照してください。
合計 (Totals)	詳細については、「合計」(243ページ) を参照してください。
ソート (Sort)	詳細については、「ソート」(243ページ) を参照してください。
ハイライト (Highlight)	詳細については、「強調表示」(244ページ) を参照してください。
マトリックス (Matrix)	詳細については、「マトリックス」(245ページ) を参照してください。
グラフ (Chart)	詳細については、「グラフ」(246ページ) を参照してください。
マップ (Map)	詳細については、「マップ」(248ページ) を参照してください。
すべて展開 (Expand All)/ すべてリセット (Collapse All) Expand All	詳細ビューの表示と非表示を切り替えます。 展開すると、デザイナーでコンポーネントのタイトルバーをクリックすることで、個別のコンポーネントの表示と非表示を切り替えることもできます。たとえば、**[ハイライト (Highlighting)]** コンポーネントの表示と非表示を切り替えるには、**[ハイライト (Highlighting)]** タイトルバーをクリックします (**[マトリックスを作成 (Create Matrix)]** タイトルバーの上)。

ツールバーボタン

ツールバーには以下のボタンがあります。

- 現在のバージョンのレポートをテストするには、**[実行 (Run)]** をクリックします。
- 保存前にレポートをプレビューするには、**[プレビュー (Preview)]** をクリックします。
- レポートデザイナで別のレポートを開くには、**[開く (Open)]** をクリックします。

- レポートを保存するには、**[保存 (Save)]** をクリックします。
- 別の名前で保存するには **[名前を付けて保存 (Save As)]** をクリックします。

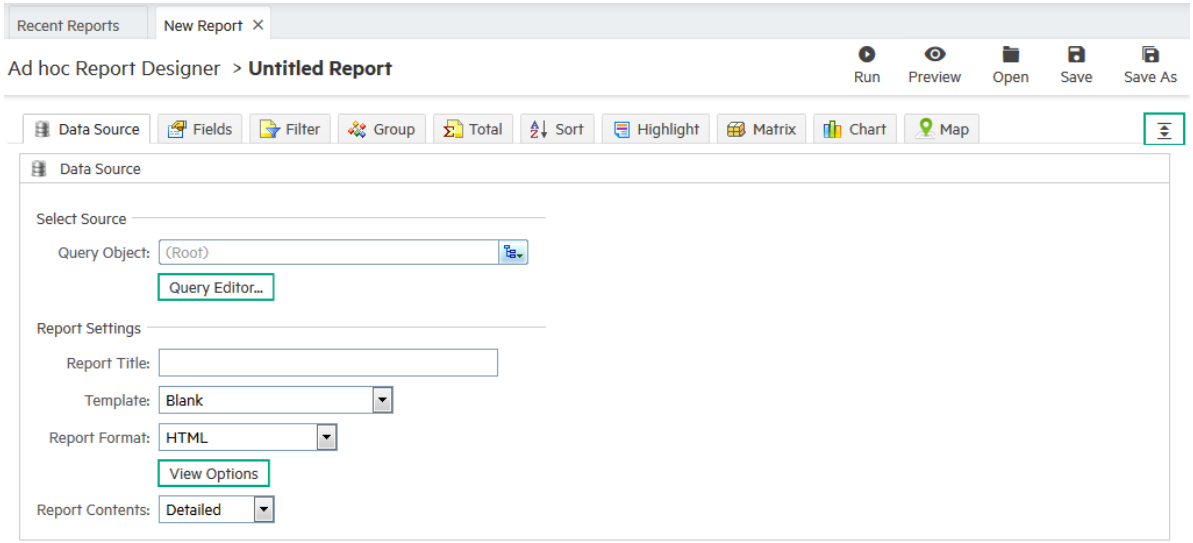
アドホックレポートデザイナーを開くには

1. [レポート] の [クラシック] メニューから **[新しいレポート]** を選択します。新しいタブにアドホックレポートデザイナーが開きます。

新しいクラシックレポートの作成

新しいクラシックレポートを作成するには

1. 左パネルの **[クラシック]** の下にある **[新しいレポート]** リンクをクリックします。[アドホックレポートデザイナー (Ad hoc Report Designer)] > [無題レポート (Untitled Report)] ページが表示されます。「クラシック: アドホックレポートデザイナー」(233ページ) を参照してください。



2. **[データソース (Data Source)]** タブで、リポジトリメニューからクエリを選択するか、**[クエリの編集画面 (Query Editor)...]** をクリックしてクエリを自分で作成します。「クエリ」(262ページ) を参照してください。

   タイトル、テンプレート、形式などのレポートデザインの基本情報を [レポート設定 (Report Settings)] セクションに入力します。「データソースのデザイン設定」(236ページ) を参照してください。

3. **[フィールド (Fields)]** タブでレポートの表示フィールドを設定します。「フィールド」(237ページ) を参照してください。
4. [フィルター (Filter)] タブにフィルター条件を入力します。「フィルター」(238ページ) を参照してください。

5. [グループ (Group)] タブにグループ化条件を入力します。「グループ」(241ページ) を参照してください。
6. [合計 (Total)] タブにカラムの合計の条件を入力します。「合計」(243ページ) を参照してください。
7. [ソート (Sort)] タブにソート条件を入力します。「ソート」(243ページ) を参照してください。
8. [ハイライト (Highlight)] タブにハイライト条件を入力します。「強調表示」(244ページ) を参照してください。
9. [行列 (Matrix)] タブに行列条件を入力します。「マトリックス」(245ページ) を参照してください。
10. [グラフ (Chart)] タブにグラフ作成条件を入力します。「グラフ」(246ページ) を参照してください。
11. 新しいレポートを保存するには、**[保存 (Save)]** をクリックします。

レポート要素のカスタマイズ

選択するレポートデザイナーに関係なく、主なレポート設定要素は同じです。

デザイナーからレポート設定ページにアクセスするには

- スマートデザイナーのスマートオプションメニューを使用します。
- アドホックパワービューワで、レポートを右クリックします。
- アドホックレポートデザイナーで、変更する設定要素のタブをクリックします。

データソース

すべてのレポートはベースクエリに基づいて構築されます。レポート用にベースクエリを選択するには、**[ソースの選択]** の下の **[クエリオブジェクト]** で、使用するクエリを参照します。

デフォルトの検索フィールドの一覧を表示する方法については、「デフォルトのフィールド」(354ページ) を参照してください。デフォルトスキーマに追加するカスタムスキーマフィールドについては、「スキーマへのフィールドの追加」(461ページ) を参照してください。

選択したクエリを編集するには、**[クエリの編集画面]** をクリックします(新しいクエリの作成については、「クエリ」(262ページ) を参照してください)。

データソースのデザイン設定

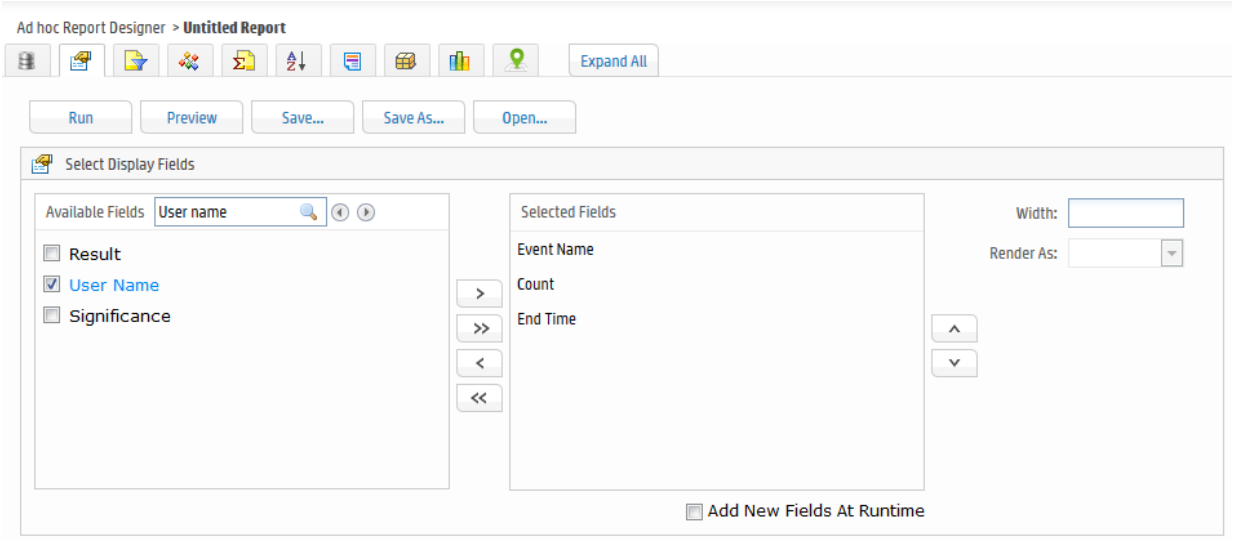
オプション	説明
クエリオブジェクト	クエリに移動するか、**[クエリの編集画面...]** をクリックして新しいクエリを作成します。「クエリ」(262ページ) を参照してください。

データソースのデザイン設定 (続き)

オプション	説明
レポートのタイトル	このレポートにタイトルを付けます。
テンプレート	このレポートに適用するテンプレートを選択します。[テンプレート (Template)] プルダウンメニューに、提供されているテンプレートと、追加したすべてのカスタムテンプレートが表示されます。レポートを実行するために使用する開始時刻、終了時刻、スキャン制限、デバイスグループ、ストレージグループ、デバイス情報をレポートに含めるには、「BlankWithHeader」テンプレートを選択します。「テンプレートスタイル」(302ページ) を参照してください。
レポートの形式	レポートのデフォルトフォーマットを選択します。「レポートの表示形式とエクスポート形式」(206ページ) を参照してください。
レポートの内容	詳細なレポートまたは要約されたレポートのどちらかを選択します。デフォルトは **[詳細]** です。

フィールド

レポートで使用するクエリを選択したら、それに含まれている表示フィールドが **[利用可能なフィールド]** リストに表示されます。これらの表示フィールドのうち、レポートで使用するフィールドを選択できます。選択したクエリを編集するには、**[クエリの編集画面]** リンクをクリックします。(新しいクエリの作成については、「クエリ」(262ページ) を参照してください)。



注: レポートの生成を高速化するには、クエリのWHERE句のフィールドに加えて、SELECT句のフィールドにもインデックスを作成する必要があります。フィールドのインデックス作成の詳細については、「インデックス作成」(152ページ) を参照してください。

レポートのタイトルを **[レポートのタイトル]** フィールドに入力し、**[レポートの内容]** フィールドで、レポート内容として [詳細] または [サマリー] を選択します。レポートのタイトルがレポートの上部に表示されます。

レポートで使用するクエリを、[フィールドを選択して表示する (Select Display Fields)] セクションの上部にあるドロップダウンリストから選択します。[利用可能なフィールド (Available Fields)] リストには、選択したクエリで定義されているフィールドが表示されます。

レポートで使用するフィールドを選択するには、**[利用可能なフィールド (Available Fields)]** から **[選択したフィールド (Selected Fields)]** リストにフィールドを移動します。

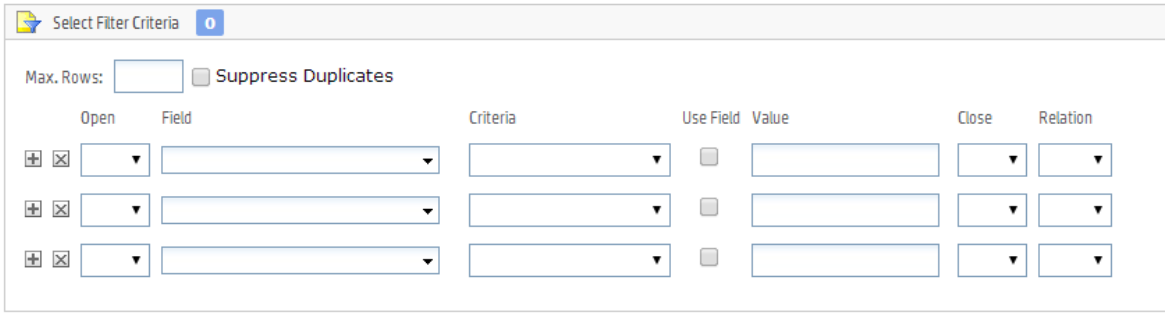
注: 少なくともいくつかの使用可能なフィールドを **[選択したフィールド (Selected Fields)]** リストに移動する必要があります。そうしないと、レポートが正しく実行されません。

- **[利用可能なフィールド (Available Fields)]** でフィールドを選択し、>をクリックして **[選択したフィールド (Selected Fields)]** リストに移動するか、»をクリックしてすべてのフィールドを追加します。
- レポートに含めないフィールドを選択解除するには、**[選択したフィールド (Selected Fields)]** リストでフィールドを選択し、<をクリックして **[利用可能なフィールド (Available Fields)]** リストに移動するか、«をクリックしてすべてのフィールドを選択解除します。
- [選択したフィールド (Selected Fields)] の順序を変更するには、上移動^および下移動v矢印を使用します。

ヒント: レポートで使用するクエリオブジェクトの作成方法については、「クエリ」(262ページ)を参照してください。ユーザーが作成した新しいクエリを含む使用可能なすべてのクエリが、アドホックレポートデザイナの [フィールドを選択して表示する] セクションのプルダウンメニューに表示されます。

フィルター

フィルター条件は、レポート設計の一部として定義されます。他のユーザーがレポートを実行するとき、デフォルトでは組み込みフィルターを使用できます。レポートを実行する際に、一度だけ使用するフィルター条件と行制限を設定することもできます。ただし、実行時に設定された値は、設計時に設定された値と違い、レポートに組み込まれません。実行時パラメーターは、特定のレポート実行のみに適用され、永続化はされません。



レポートにデフォルトフィルター条件が含まれている場合、ユーザーはデフォルトを使用してレポートを実行するか、組み込みフィルターを実行時に変更または削除できます。詳細については、「実行時フィルター、条件、パラメーター」(196ページ)を参照してください。

論理式を使用してベースクエリの結果に対してフィルターを設定し、レポート結果を絞り込むことができます。たとえば、[Top Password Changes] に対するレポートについて、指定したユーザー名や指定したIPアドレスに関係するパスワード変更についてのみレポートするように、フィルター条件を設定できます。

[最大記録 (Max. Rows)] の値を定義して、レポートの行数を定義することができます。また、**[必須]** オプションを使用すると、選択した1つ以上のフィールドに基づいてフィルター処理を要求することができます。

フィルター条件オプションの選択

オプション	説明
最大記録 (Max. Rows)	レポート出力の最大行数を指定します。行数が定義した最大行を超える結果は、レポートに含まれません。 • [最大記録 (Max. Rows)] を設定し、**[グループ設定 (Set Grouping)]** (「グループ」(241ページ) を参照) でグループ化も指定すると、[最大記録 (Max. Rows)] だけを指定してグループ化を行わなかった場合とは異なる結果になります。 • このフィールドに0を設定すると、無制限の数の行が返されます。 • レポートの最大行数を増やしても、レポートによって返される行数が必ずしも増えるとは限りません。レポートによって実行されるクエリにより、返される行数が制限されている場合は、レポートの [最大記録 (Max. Rows)] 設定を増やしても影響はありません。たとえば、NIST IR Top 10 High Risk Eventsレポートを編集し、[最大記録 (Max. Rows)] 列の値を10から20に増やしても、レポートを実行すると10行しか返されません。これは、レポートによって実行されるクエリが10行を返すためです。しかし、レポートによって返される行数を、デフォルト値よりも少ない数に制限することができます。たとえば、NIST IR Top 10 High Risk Eventsレポートで [最大記録 (Max. Rows)] フィールドの値を10から5に変更した場合、実行時に5行が返されます。 • クエリを編集し、クエリから返される行数を変更して、返される行数を増やし、レポートの [最大記録 (Max. Rows)] フィールドで指定される数を変更することができます。
フィールド (Field)	[フィールド (Field)] には、ベースクエリで指定されたイベントデータフィールドが設定されます(フィールドは、一般にレポートの列に等しくなります)。 1. フィルター処理するフィールドを選択します。 2. フィルター処理する別のフィールドを追加するには、⊞ ([フィルタを追加]) をクリックします。 3. フィルターを削除するには、⊠ ([フィルタを削除]) をクリックします。 デフォルトの検索フィールドの一覧を表示する方法については、「デフォルトのフィールド」(354ページ) を参照してください。デフォルトスキーマに追加するカスタムスキーマフィールドについては、「スキーマへのフィールドの追加」(461ページ) を参照してください。 異なるフィールドに対して条件が設定された複数のフィルターを指定すると、論理積演算が行われます。同じフィールドに対して条件が設定された複数のフィルターを指定すると、論理和演算が行われます。 たとえば、イベントをフィルター処理して、90～100の間の値/カウント (行など) に基づいてデータを返すには、**[間]** 条件を使用します (たとえば、<フィールド> 間 90と100)。 同じフィールドに対して、条件「90より**大きい**」と、「90より小さい」という2つのフィルターを設定すると、探しているデータが得られません。これらのフィルターのうち1つだけが起動されます。 このレポートに対して選択したクエリのフィルタリングが必須の場合、パネルタイトル [フィルタ条件の選択] と1つ以上のフィールドに赤いアスタリスクが付きます。詳細を参照してください。

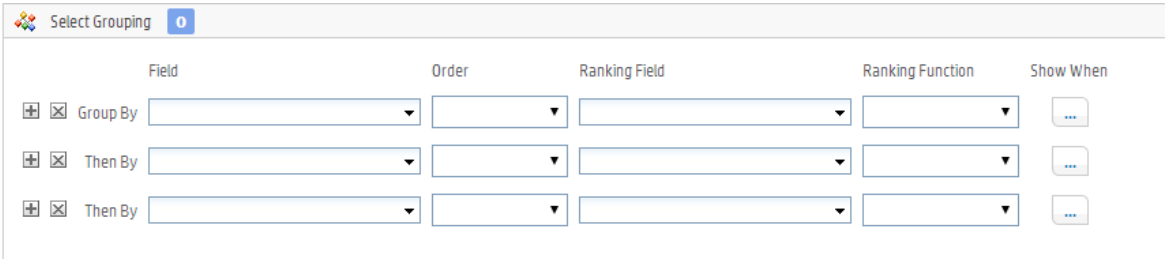
フィルター条件オプションの選択 (続き)

オプション	説明
条件 (Criteria)	論理演算子を選択します(たとえば、Is、Is Not、Starts With、Ends With、Containsなど)。 **ヒント:** クエリで大文字と小文字を区別するには、演算子に対する[大文字と小文字を区別]オプションを選択します。
値 (Value)	条件フィルター式を完成させる値を選択します。

グループ

グループ化とは、特定のフィールドに基づいて、関連するレポートデータを論理的なグループにまとめることです。データを昇順または降順に並べたり、選択したフィールドの値や集計値を表示したりすることができます。さまざまなグループを作成し、さまざまな方法で情報を表示することができます。

レポートグループを設定するには、**[レポート] > [新しいレポート]** を選択し、[デザイン] メニューから **[新しいレポート]** をクリックします。**[アドホックレポートデザイナー]** ページが表示されます。[グループ] タブ ( ) をクリックすると、**[グループ分けの基準の選択 (Select Grouping)]** メニューが表示されます。



注: グループが定義されたレポートは、最大で100,000行までしか表示できません。

例1:「総売上」を降順 (ZからAへ) に表示するグループを作成します。「東地区」の総売上は1000ユニット、「西地区」の総売上は1900ユニットです。このレポートでは、「西地区」グループ詳細は「東地区」グループ詳細より前に表示されます。

例2: レポートが日付フィールドを含むクエリを使用している場合、結果を日付でグループ化できます。レポートクエリで使用できる他のフィールドに応じて、「ユーザ名」、「ソースアドレス」、「通知先アドレス」などによりグループ化するための条件を追加できます。

注: [フィルタ条件の選択] で [最大記録] を選択し (「フィルター」(238ページ) を参照)、グループ化も指定した場合、[最大記録] だけを指定してグループ化を行わなかった場合とは異なる結果になります。

レポート設定の詳細については、「実行時フィルター、条件、パラメーター」(196ページ)を参照してください。

グループを定義するには

1. グループ化するイベント情報、グループ化の順序、グループ化の条件を指定するために、**[グループ分け (Group By)]** メニューの次のメニューから該当するオプションを選択します。

   [グループ分け (Group By)] フィールドはデータグループのプライマリフィールドです。これをランキングフィールドに基づいて昇順または降順に並べます。

   [グループ分け (Group By)] のフィールドの選択

オプション	説明
フィールド (Field)	レポートグループでプライマリフィールドにするオプションをこのメニューから選択します。**[フィールド (Field)]** メニューには、ベースクエリで指定されたイベントデータフィールドが設定されます。 • グループ化するフィールドを追加するには、⊞ ([フィールドの追加]) をクリックします。 • グループ化するフィールドを削除するには、☒ ([フィールドの削除]) をクリックします。
順番 (Order)	情報の表示順を選択します。 • 昇順 (0、1、2...またはA～Z) • 降順 (2、1、0...またはZ～A)
Ranking Field Ranking Function	順番の基準となるフィールド ([ランキングフィールド (Ranking Field)]) とレポートで表示する情報のタイプ ([ランキング関数 (Ranking Function)]) を選択します。Loggerでは、データを日付、数値、文字でグループ化できます。 たとえば、クエリオブジェクトとして "Login Errors by User" を選択する場合、データを「ユーザ名」別にグループ化し、ランキングフィールドとして「エラー」を、ランキング関数として "Count" を使用して、データを「昇順」に並べることができます。 そのため、レポートのデータグループセクションの先頭に、エラーの最も多いユーザーを表示することができます。
タイミングを表示 (Show When)	より詳細な条件を満たしたときに情報を表示する場合は、このメニューを使用します。

2. セカンダリグループを追加する場合は、**[次の基準 (Then By)]** のフィールドを指定します。たとえば、レポートにパスワード変更をレポートするクエリが使用されており、「User Name」フィールドが含まれている場合、結果を日ごとに「User Name」でサブグループ化することができます。

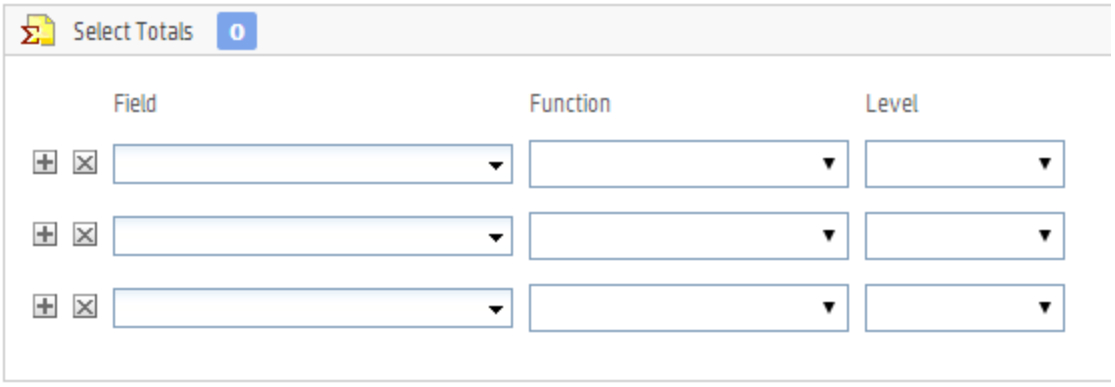
   サブグループの **[次の基準 (Then By)]** のフィールドを追加または削除するには、⊞ ([フィールドの追加] ボタン) または☒ ([フィールドの削除] ボタン) を使用します。

レポートでは、選択した順序で配置およびグループ化されたレコードが生成されます。

ヒント: または、グループの代わりにソート順序のみを指定することもできます。「ソート」

(243ページ) も参照してください。

合計



集計 (合計) フィールドを指定できます。以下のどのレベルにも集計を適用できます。

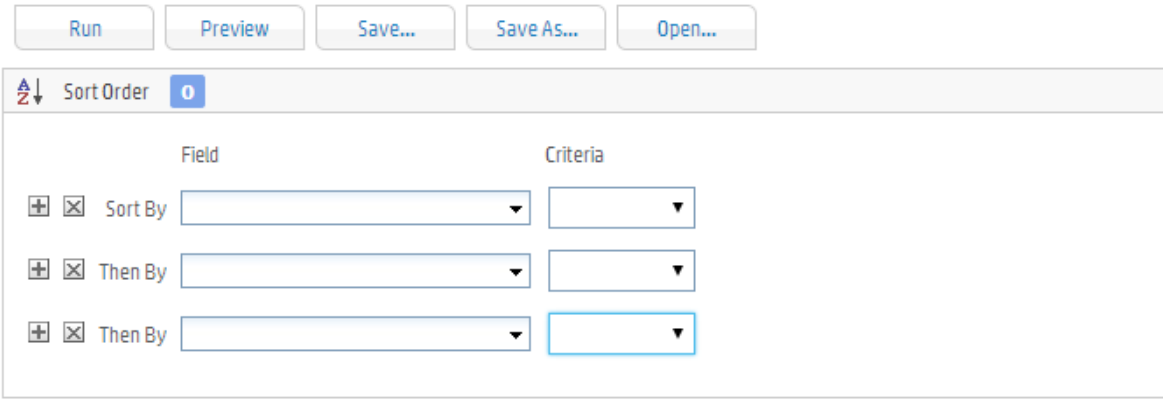
- レポート
- ページ
- グループ

集計の詳細を指定するには

1. **[フィールド (Field)]** で、集計情報を計算するために処理するフィールドを選択します。
2. 同じ行の **[関数 (Function)]** で、集計関数を選択します。
3. 同じ行の **[レベル (Level)]** で、集計するレベルを選択します。

注: [選択したフィールド (Selected Fields)] リストにないフィールドに合計を適用する場合、そのフィールドは [選択したフィールド (Selected Fields)] フィールドに自動的に追加されます。

ソート



レポート結果をグループ化 (「グループ」(241ページ)を参照) しないで、ソートを行う場合は、グループ化の代わりにソートを指定します。

注: ソート順序が定義されたレポートは、最大で100,000行までしか表示できません。

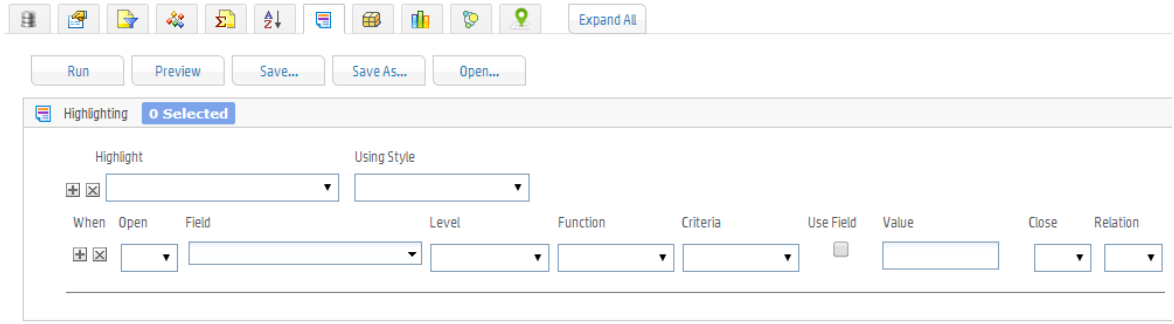
ソートレベルは3つまで指定できます。

ソート順序を指定するには

1. **[フィールド (Field)]** で、レポートをソートするフィールドを選択します。
2. **[条件 (Criteria)]** (同じ行) で、ソート条件を選択します。
3. 必要な場合は、ソート条件を追加指定するために [次の基準 (Then By)] 行に値を指定します。

強調表示

レポートには、指定したフィールドに対する複数レベルの強調表示を含めることができます。強調表示された項目は、生成されたレポート上で、指定された設定条件が満たされた場合に、視覚的なアラートとしての役割を果たすことができます。



強調表示を設定するには

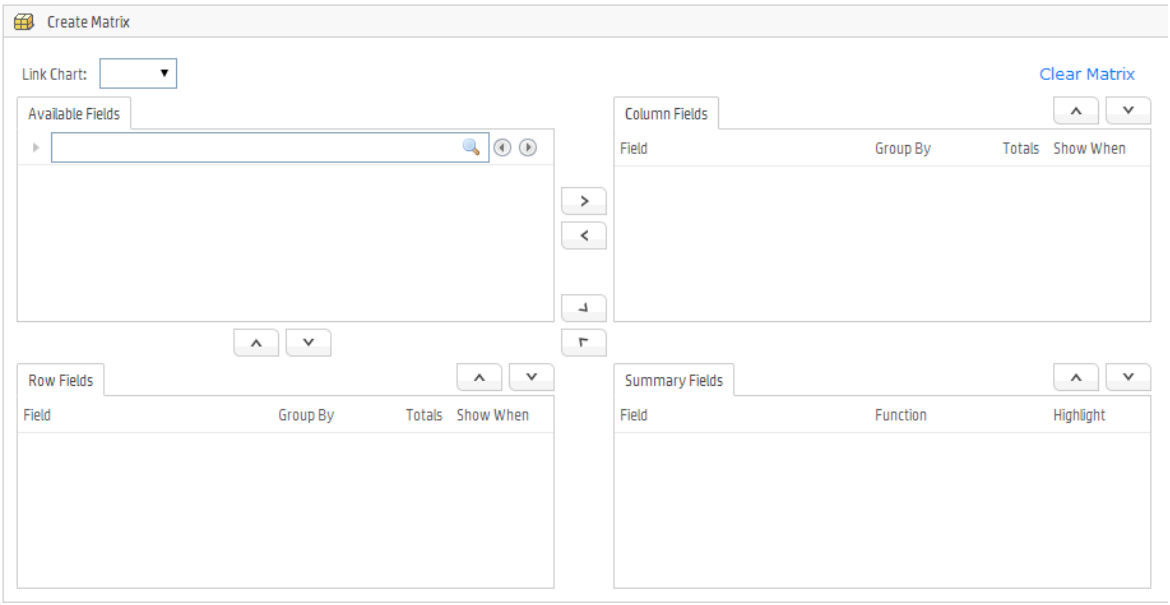
1. **[ハイライト (Highlight)]** で、強調表示するフィールドを選択します。レコード全体を強調表示するには、**[全ての行]** を選択します。
2. **[スタイルに使用する色 (Using Style)]** で、ハイライトのために適用するスタイルを選択します。
3. レポートビューアー上で視覚的なアラートを受け取るには、**[アラート]** チェックボックスをオンにします。
4. **[フィールド (Field)]** で、強調表示 (アラート) のために評価するフィールドを選択します。
5. **[レベル (Level)]** で、選択したフィールドを評価するレベルを選択します。
   - [詳細] は各行 (レコード) を評価します。
   - [レポート] はレポートの終わりで評価します。

- それぞれのグループは、各グループの終わりで評価されます。
- [ページ] はページの終わりで評価します。

6. [レベル (Level)] で [レポート] または [ページ] を選択した場合、適用する関数を選択します。
7. **[条件 (Criteria)]** を選択し、その **[値 (Value)]** を指定します。
   エントリを削除するには、条件エントリの左にある☒ ([条件を削除]) をクリックします。別のエントリを追加するには⊞ ([条件を追加]) をクリックします。

マトリックス

マトリックスはデータの集計を表すため、レポートにマトリックスを含めることを選択できます。**[フィールドを選択して表示する]** で適切なクエリオブジェクトが選択されていることを確認してください。



マトリックスを作成するには

1. 行または列にフィールドを配置するには、フィールドをクリックし、**[行フィールド (Row Fields)]** または **[列フィールド (Row Fields)]** ボックスにドラッグします。
2. フィールドをセル (集計) として配置するには、フィールドをクリックし、**[サマリー・フィールド (Summary Fields)]** ボックスにドラッグします。
3. **[サマリー・フィールド (Summary Fields)]** に配置されたフィールドのプルダウンメニューから **[関数 (Function)]** を選択します。
4. 必要に応じて、列または行内の数値または日付フィールドに対し、プルダウンメニュー内で **[グループ分け (Group By)]** 機能を指定します。
5. 必要に応じて、列または行内のフィールドに対し、**[総数 (Totals)]** チェックボックスをオン

にして行または列を表示します。

フィールドをマトリックスに **[列フィールド (Column Fields)]** の1つとして追加するには、フィールドを選択してpadding-right:0px;をクリックします。フィールドをマトリックスから削除するには、[列フィールド (Column Fields)] でフィールドを選択し、をクリックします。

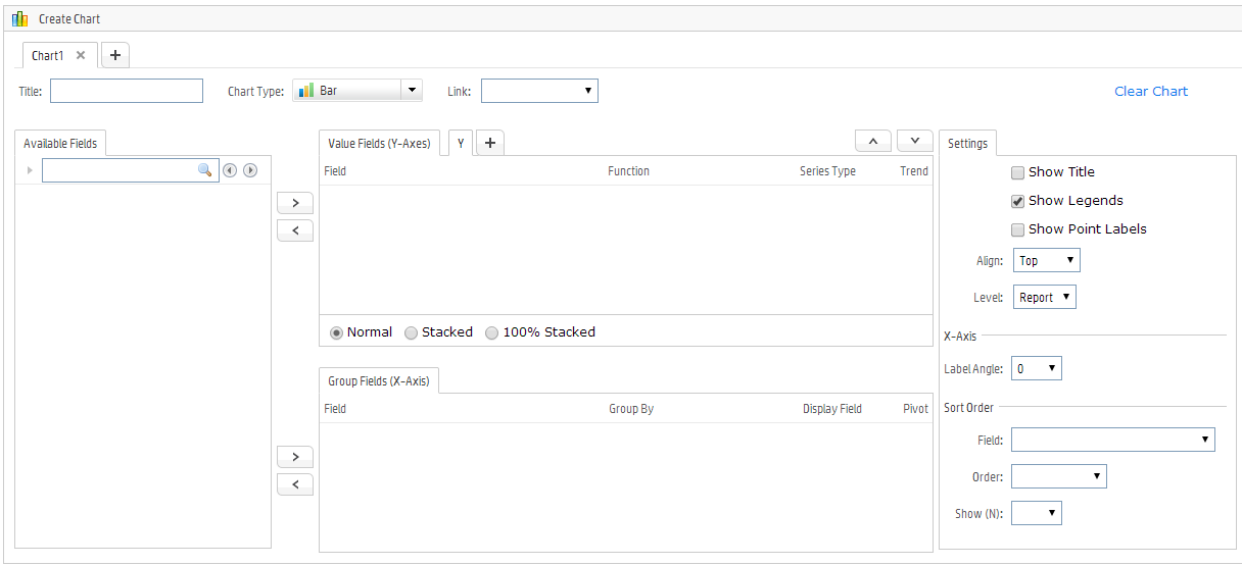
フィールドをマトリックスに **[行フィールド (Row Fields)]** の1つとして追加するには、フィールドを選択してをクリックします。フィールドをマトリックスから削除するには、[行フィールド (Row Fields)] でフィールドを選択し、をクリックします。

フィールドをマトリックスに **[サマリー・フィールド (Summary Fields)]** の1つとして追加するには、フィールドを選択してをクリックします。フィールドをマトリックスから削除するには、[サマリー・フィールド (Summary Fields)] でフィールドを選択し、をクリックします。

フィールドを上下に移動するには、フィールドを選択して ([上に移動 (Move up)]) または ([下に移動 (Move down)]) をクリックし、それぞれの方向にフィールドを移動します。

現在のマトリックスのすべての設定と内容を削除するには、**[マトリックスのクリア (Clear Matrix)]** をクリックします。

グラフ



集計データを図的に表現するために、グラフをレポートに追加できます。**[フィールドを選択して表示する]** で適切なクエリオブジェクトが選択されていることを確認してください。

グラフを作成するには、以下の値を指定します。

設定	説明
タイトル (Title)	グラフのタイトル
グラフの種類 (Chart Type)	ドロップダウンリストからグラフの種類を選択します。
リンク (Link)	レポートフィールドまたはマトリックスにグラフをリンクすることを選択します。
利用可能なフィールド (Available Fields)	利用可能なフィールドは、レポートクエリから取得されます。**[>]** ボタンを使用して、これらのフィールドを値フィールド (グラフ上のY軸) またはグループフィールドに割り当てます。「フィールドの割り当て」(247ページ) を参照してください。
設定 (Settings)	• **[タイトルを表示 (Show Title)]:** オンにすると、グラフのタイトルが表示されます。 • **[凡例を表示 (Show Legends)]**: オンにすると、グラフに各フィールドの凡例が表示されます。 • **[ポイント・ラベルを表示 (Show Point Labels)]** オンにすると、グラフ内にフィールドの値に対する一致数のラベルが表示されます。 • **[揃え (Align)]:** グラフ配置の整列方法を選択します。 • **[レベル (Level)]:** グラフに描画するデータのレベルを選択します。 ◦ **レポート (Report)**: レポート全体のデータをプロットします。 ◦ **ページ (Page)**: グラフの配置先ページのデータをプロットします。
ソート順序 (Sort Order)	グラフのソート順序を選択します。

フィールドの割り当て

グラフの値とソートフィールドを設定できます。

値フィールド (Y軸) を設定するには

1. **[値フィールド (Y軸)]** ボックスの中のフィールドをクリックしてドラッグするか、ボタン ([フィールドの追加]) を使用して選択したフィールドを追加します。
2. フィールドの集計関数を選択します。
3. 異なるグラフの種類を選択するには、右側のボタンをクリックして、グラフの種類を示すボックスを開きます。必要な種類を選択します。シリーズとして配置する各属性について、上記ステップ1から3を実行します。フィールドの位置を変更するには、フィールドを選択し、必要に応じて ([上に移動]) または ([下に移動]) をクリックします。

グループフィールド (X軸) を設定するには

1. **[グループのフィールド (X軸)]** ボックスの中のフィールドをクリックしてドラッグするか、ボタン ([フィールドの追加]) を使用して選択したフィールドを追加します。

2. グループ化する方法を選択します (数値または日付)。

   数値フィールドでグループを指定できます。たとえば、10個ずつのグループにするには、[グループ] ボックスに10を指定します。

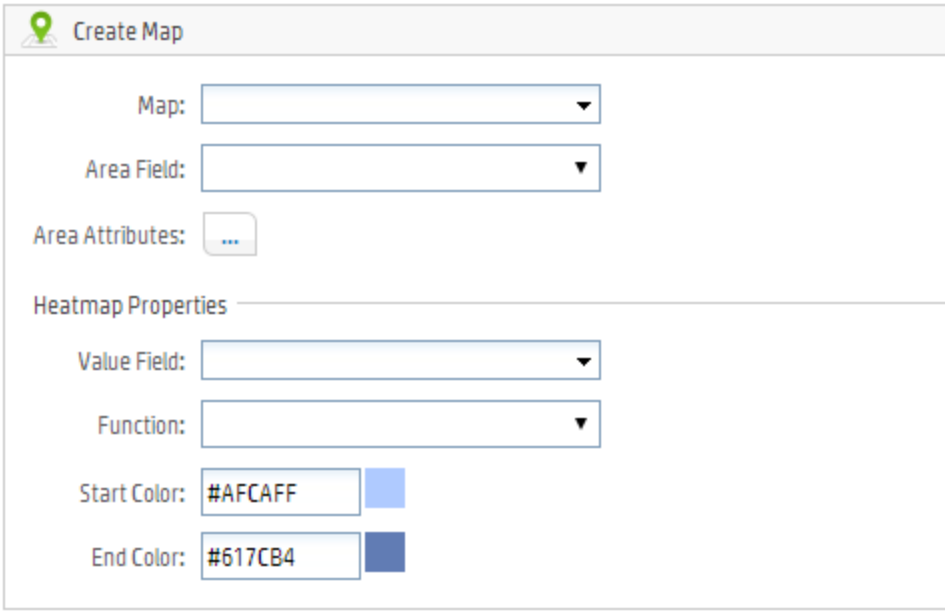
   日付フィールドでグループを指定できます。ドロップダウンボックスから、[Day]、[Week (Sunday to Saturday)]、[Month]、[Quarter (Jan-Mar, Apr - Jun, Jul - Sep, Oct - Dec)]、[Year] のいずれかを選択します。

   ヒント: 値フィールド (Y軸) またはグループフィールド (X軸) からフィールドを削除するには、それぞれのボックスから外にドラッグするか、選択したフィールドの ボタン ([フィールドを削除]) を使用します。

現在のグラフのすべての設定と内容を削除するには、**[グラフのクリア]** をクリックします。

マップ

レポートには、データに基づいてGIS (Geographic Information System) マップを含めることができます。これらのフィールドの説明については、「マップパラメーター」(251ページ) を参照してください。



GISマップにはヒートマップを含めることができます。ヒートマップは、指定した活動が最も多い領域を色で強調表示するものです。

注: GISヒートマップでのヒートとは、活動レベルを意味します。

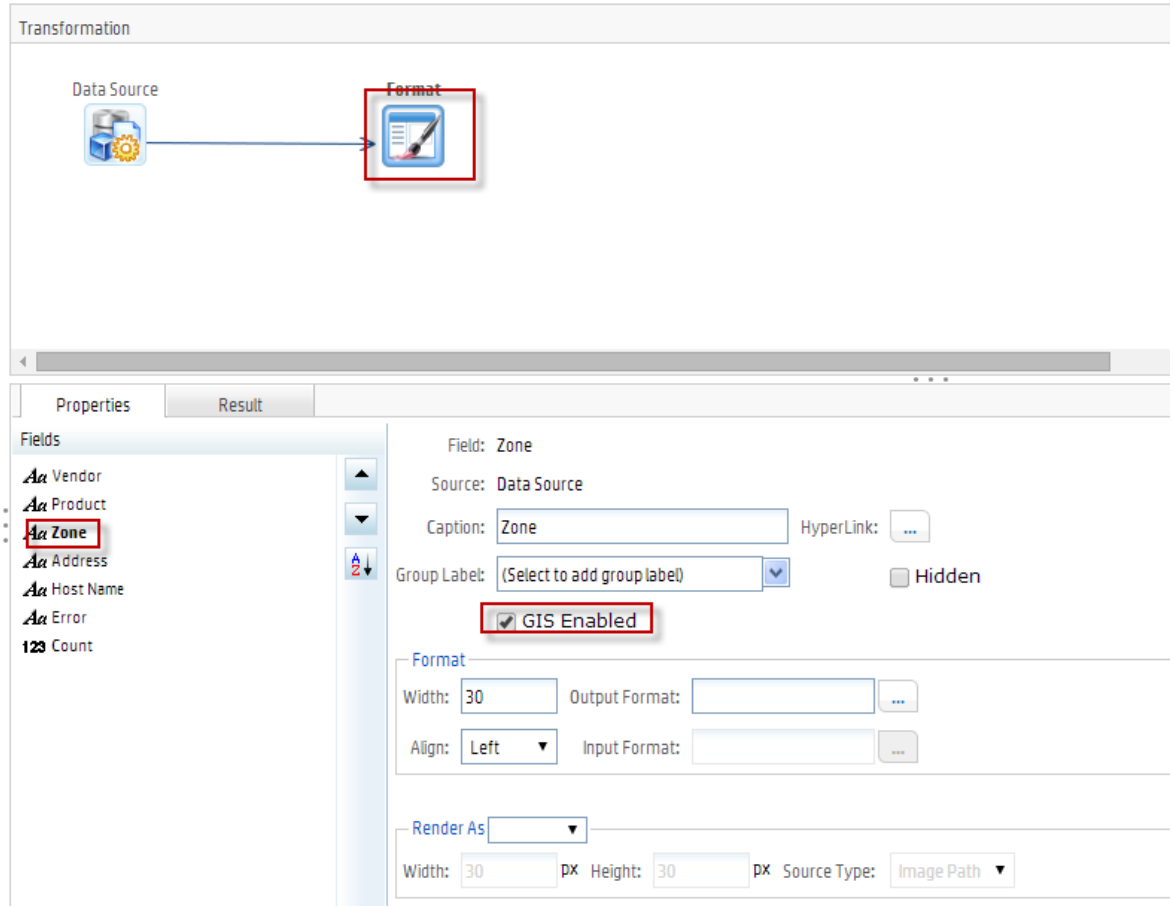
マップのレポートへの追加

クエリ内のフィールドの値を反映したGISマップを作成できます。このマップはレポートに含めることができます。レポートにマップを追加するには、以下の手順に従って、GISが有効なフィールドをマップタイプとして選択する必要があります。マップは、Interactive HTML (iHTML) 形式で表示されます。

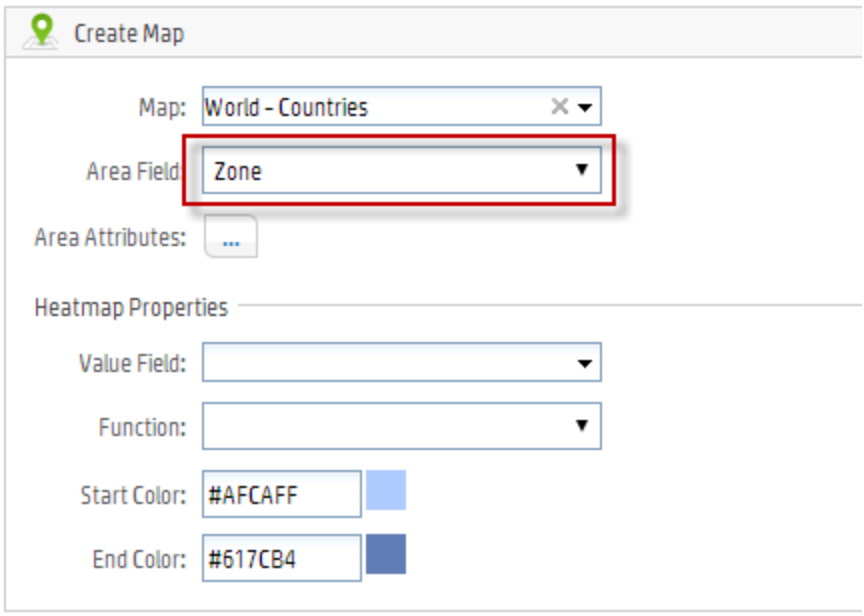
マップをレポートに追加するには

1. レポートペインの **[デザイン]** で、**[クエリ]** をクリックしてクエリオブジェクトエディターを開きます。
2. **[開く]** をクリックし、既存のクエリを参照して開くか、レポートで使用する新しいクエリを作成します(新しいクエリを作成する場合は、「クエリの操作」(264ページ) に従ってクエリを指定します)。
3. **[変換 (Transformation)]** ワークスペースで、**[形式 (Format)]** ステップをクリックします。
4. **[プロパティ (Properties)]** タブで、マップに追加するフィールドを選択します。

5. フィールドの詳細で、**[GISが有効になっています (GIS Enabled)]** を選択します。選択したフィールドには、国名、州名、都市名など、GIS分類データが含まれている必要があります。



6. ツールバーで **[保存]** をクリックし、変更したクエリオブジェクトを保存します。
7. [クラシック] の下の [レポート] メニューで、**[新しいレポート]** をクリックします。アドホックレポートデザイナーが開きます。
8. **[データソース (Data Source)]** で、前にフィールドでGISを有効にしたクエリオブジェクトを参照して選択します。
9. **[レポート設定]** の **[形式]** で、ドロップダウンリストからiHTMLを選択します。
10. **[マップ]** タブをクリックします。
11. **[マップ (Map)]** で、ドロップダウンリストからマップタイプを選択します。
12. **[面フィールド (Area Field)]** で、上記でGISを有効にしたフィールドを選択します。



13. **[面属性 (Area Attributes)]** をクリックします。**[属性 (Attributes)]** ダイアログで、「マップパラメーター」(251ページ) の説明に従い、情報バルーンに表示するフィールドを選択します。
14. **[ヒートマップ・プロパティ (Heatmap Properties)]** の **[値フィールド (Value Field)]** で、マップで使用する値を取得するフィールドを選択し、マップに設定します。
15. **[スタート・カラー (Start Color)]** と **[エンド・カラー (End Color)]** で、マップ上に値の範囲を表示する2つの色をパレットから選択します。たとえば、マップ上の明るい色は小さな値を示し、暗い色は大きな値を示すようにします。
16. 必要に応じてレポートに追加変更を行い、レポートを実行します。

マップパラメーター

マップには以下のパラメーターが含まれます。

マップパラメーター

パラメーター	説明と値
マップ (Map)	データの初期ロードのためのマップ名を選択します。 たとえば、米国の州のマップを描画する場合は、「米国 - 地域」を選択します。
面フィールド (Area Field)	これは、マップデータをグループ化するために使用する値です。マップの値の初期選択に基づいて領域を選択します。

マップパラメーター (続き)

パラメーター	説明と値
面属性 (Area Attributes)	情報バルーンを表示するマップの領域をクリックします。バルーン表示内の以下の属性について値を設定します。 • **[プレフィックス]:** フィールドのプレフィックスキャプション値 • **[フィールド]:** フィールドの値 • **[関数]:** フィールドのアグリゲーションサマリー • **[サフィックス]:** フィールドのサフィックスキャプション • **[タイトルとして使用]:** オンにした場合、この行をバルーンのタイトルバーとして表示
ヒートマッププロパティ (Heatmap Properties) - 値フィールド (Value Field)	ヒートマップが計算される値フィールドを選択します。
関数 (Function)	ヒートマップが計算されるフィールドのアグリゲーションサマリーを選択します。
スタート・カラー (Start Color)	値フィールドの最も小さい値を表す色を選択します。
エンド・カラー (End Color)	値フィールドの最も大きい値を表す色を選択します。中間のすべての色には、均等分布により自動的に値が割り当てられます。

ダッシュボードの作成

ダッシュボードでは、複数の情報が1つの画面に配置されるため、情報を一目で確認できます。ダッシュボードにはレポートだけでなく、Webコンテンツも表示できます。ビジネスアナリストやアプリケーション管理者は、総合的かつカスタマイズされた形でシステムを分析することができます。

ダッシュボードではウィジェットを使用します。これは、サポート対象オブジェクトを表示できる表示モジュールです。まずウィジェットを作成し、ダッシュボード内に配置して、表示します。

例:

- 1つ以上のレポートをダッシュボードに追加し、指定した間隔 (たとえば1時間に1回) で自動更新するようにレポートを設定できます。ダッシュボードは、最新の発行済みレポート結果にアクセスします (この場合は1時間に1回)。
- 1時間に1回レポートを実行して発行するようにスケジュールすれば、ダッシュボードに最新の結果が表示されます。これにより、各レポートを1時間ごとに手動で実行して表示しなくても、同じ更新情報を取得することができます。

スマートダッシュボードとアドホックダッシュボードとの違い

アドホックダッシュボードは、1つのレポートクエリを複数の形式で(たとえば、別々のグラフタイプを使用して)表示できますが、1つのダッシュボードで扱えるクエリは1つだけです。

スマートダッシュボードは、複数の異なるレポートクエリを同じダッシュボードに表示できます。

例

- スマートダッシュボードには、Most Common Eventsを示すグラフとLeast Common Eventsを示すグラフの2つのグラフを表示できます。各グラフは別々のクエリに基づきます。
- アドホックダッシュボードには、棒グラフと散布図グラフの2種類のグラフを表示できますが、どちらのグラフもMost Common Eventsクエリの情報に基づきます。

ダッシュボードに含めることができる項目

以下の情報をダッシュボードに配置できます。ただし、各レポートまたはWebリンクをウィジェットの中に配置して、ウィジェットをダッシュボードに配置する必要があります。「ウィジェット」(258ページ)を参照してください。

1つのダッシュボードには、以下のいずれかを含む1つ以上のウィジェットを格納できます。

- **公開済みレポート**: ダッシュボードには、最新の発行済みレポートが表示されます。「レポートの発行」(213ページ)を参照してください。

  注: ユーザーがダッシュボードビューでレポートデータにアクセスするには、レポートが発行されている必要があります。ダッシュボード上のレポートに発行済みの結果がない場合、ダッシュボードビューにはその旨を示すメッセージが表示されます。レポートが発行されると、ダッシュボードビューを更新することでレポートが表示されます。

- **外部のURL**: ダッシュボードには、リンク可能な外部URLが表示されます。アクセス許可は、HTTPヘッダーフィールドのX-Frame-Optionsの設定に基づいて行います。たとえば、URLとして`www.bing.com`を追加することはできますが、`www.google.com`を追加することはできません。
- **リッチテキスト**: リッチテキストボックスを使用してダッシュボードに説明または注釈を加えることができます。リッチテキストボックスでは、書式設定したテキスト、グラフィック、その他のオブジェクトを使用できます。

ダッシュボードの必須条件

ダッシュボードは、公開済みレポートから作成したウィジェットを使って作成します。このレポートは、既存レポートの実行またはレポートの新規作成によって作成します。ダッシュボードに

格納するオブジェクトを作成するための手順の概要は以下のとおりです。

ダッシュボード作成手順の概要

ダッシュボードの設定プロセスは、以下のタスクで構成されています。

1. レポートを実行します (既存レポートの変更またはレポートの新規作成)。
2. レポートにグラフの追加や、その他の変更を加えます。
3. レポートを公開します。
4. 公開したレポートから新しいウィジェットを作成します。
5. 新しいダッシュボードを作成します。

スマートダッシュボードデザイナーを使用する場合 ([デザイン] > [ダッシュボード])

a. 必要に応じて手順1～4 (上記) を繰り返し、ダッシュボードウィジェットを追加作成します。
b. **[デザイン] > [ダッシュボード]** をクリックします。空白のダッシュボードが表示されます。
c. [要素] メニューを使用して、ウィジェットやその他のダッシュボードオブジェクトをダッシュボードにドラッグアンドドロップします。

アドホックダッシュボードデザイナーを使用する場合 ([クラシック] > [ダッシュボード])

a. **[クラシック] > [ダッシュボード]** をクリックします。アドホックダッシュボードデザイナーが表示されます。
b. ダッシュボードに表示するすべてのレポートまたはWebリンクについて1つのウィジェットを作成します。詳細については、「新しいウィジェットの作成」(258ページ) を参照してください。
c. ウィジェットをダッシュボードに追加します。詳細については、「ウィジェットのダッシュボードへの配置」(262ページ) を参照してください。
d. 必要に応じて、ダッシュボードがダッシュボードビューア内でタブとして表示されるように、ダッシュボードを設定できます。詳細については、「ダッシュボードビューアでのダッシュボードの表示」(256ページ) を参照してください。

クラシックダッシュボード

ダッシュボードには、レポートデータが表示され、ネットワークイベントに関する最新情報を素早く参照できます。ダッシュボードには、各種のレポートと外部リンクを組み込むことができます。ただし、各レポートまたはリンクを独自のウィジェットに配置してから、ウィジェットをダッシュボードに配置する必要があります。ダッシュボードには、複数のウィジェットを配置できます。

ダッシュボードにレポートを配置することで、それらのレポートについて発行された最新の結果にアクセスできます。ダッシュボードビューアで結果にアクセスするには、レポートを実行して発

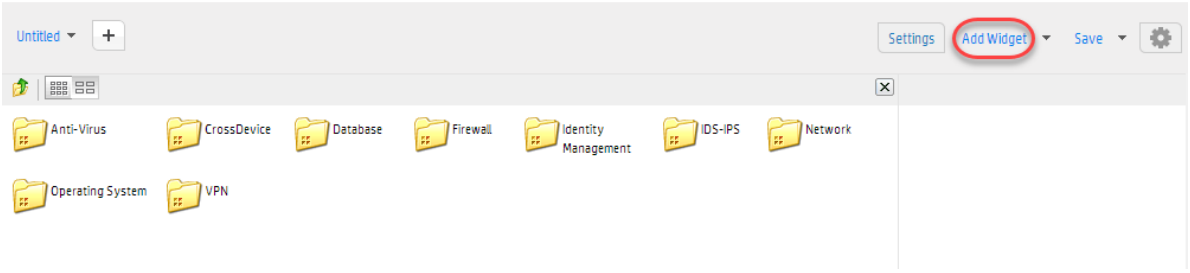
行する必要があることに注意してください。レポートを実行、発行し、妥当な保有期間 (たとえば1か月) にわたって保存するようスケジュールすれば、それらの結果をダッシュボードビューで常に使用できます。

新しいクラシックダッシュボードの作成

ここでは、ダッシュボードを作成するための手順の概要を示します。各ステップの詳しい説明は、以降のトピックを参照してください。

新しいダッシュボードを追加するには

1. [レポート] メニューの [クラシック] セクションにある **[ダッシュボード]** をクリックします。これにより「無題 (Untitled)」という名前の新しい空のダッシュボードタブが開きます。
2. **[ダッシュボードオプション (Dashboard Options)]** をクリックし、**[編集モードに切り替え (Switch to Edit Mode)]** を選択します。
3. ダッシュボードに項目を配置するには、右隅にある **[ウィジェットを追加 (Add Widget)]** をクリックします。「ウィジェット」(258ページ) を参照してください。



4. ウィジェットを選択し、クリックしてダッシュボードにドラッグします。
5. 配置したウィジェットごとに、必要に応じてウィジェットプロパティを指定します。

   注: デフォルトでは、外部リンク用のダッシュボードではスクロールバーを使用できません。スクロールバーを追加するには、[ダッシュボードのアイテム] の下の [外部リンク] の [ウィジェットのプロパティ] セクションで、「スクロールバーを表示」プロパティに「はい」を設定します。

6. **[保存 (Save)]** をクリックしてダッシュボードを保存します。

保存した新しいダッシュボードは、**[ダッシュボードのプロパティ]** の「利用可能なダッシュボード」のリストで使用できるようになります。

作成した新しいダッシュボードを表示する方法や、デフォルトの表示を別のダッシュボードに設定する方法については、「ダッシュボードビューアでのダッシュボードの表示」(256ページ) を参照してください。

ダッシュボードビューアでのダッシュボードの表示

ダッシュボードビューアで1つ以上のダッシュボードをタブとして開くには

1. [ダッシュボードビューア] ページの上部にある **[ダッシュボードのプロパティ]** リンクをクリックします。
2. [利用可能なダッシュボード] ボックスで、タブに表示するダッシュボードに移動します。
3. [+] をクリックします。ダッシュボード名が **[選択したダッシュボード]** ボックスに表示されます。
4. **[保存]** をクリックします。
5. 左パネルの **[ダッシュボード]** リンクをクリックしてダッシュボードビューアを表示します。選択したダッシュボードが表示されます。

> **注: [利用可能なダッシュボード]** の下に表示されるダッシュボードのセットまたはサブセットは、ユーザーグループのステータスと、[全ての所有者のダッシュボードを表示] チェックボックスの選択状態によって変わります。管理権限を持つユーザーは、権限の低いユーザーよりも多くのダッシュボードまたはすべてのダッシュボードを参照できます。自分のダッシュボードのみに表示を制限すると、他のユーザーが設計したダッシュボードはリストに表示されません。
>
> すべてのユーザー (設計者) のダッシュボードにアクセスするには、**[全ての所有者のダッシュボードを表示]** チェックボックスをオンにします。
>
> 自分のダッシュボードのみを表示するには、このチェックボックスをオフにします。

既存のダッシュボードの変更

既存のダッシュボードを変更するには

1. **[設定]** をクリックして **[編集モードに切り替え]** を選択します。現在の設定が表示され、必要に応じて設定を変更し、保存することができます。
2. **[プロパティ]** エリアには、基本的なダッシュボード設定が表示されます。ダッシュボードを定期的に更新するには、**[自動リフレッシュ]** チェックボックスをオンにし、自動更新時間を **[分]** に分単位で指定します。**[入力パラメータ形式]** を表示するには、**[最初の実行でプロンプト]** チェックボックスをオンにします。ここには、レポートがダッシュボードに表示された後で、レポートを初めてダッシュボードから実行する前のダッシュボードパラメーターの値が表示されます。
3. **[レイアウト]** エリアでは、ダッシュボード用にペインを選択できます。
4. **[情報]** エリアには、説明、範囲、ダッシュボードが保存される場所が表示されます。
5. **[ダッシュボードのパラメータ]** エリアには、書式設定パラメーター ([最大列数] と [カラム幅]) が表示されます。

ダッシュボードビューアからの既存のタブの削除

ダッシュボードをその保存場所から削除せずにダッシュボードビューアから既存のタブを削除するには

1. ダッシュボードのタイトルをクリックし、**[削除]** をクリックします。
2. **[OK]** をクリックして削除を確定します。

ダッシュボードの削除

既存のダッシュボードをダッシュボードビューアから削除することができます。

ダッシュボードをダッシュボードビューアから削除するには

1. ダッシュボードを選択し、**[設定]** をクリックします。
2. **[編集モードに切り替え]** を選択します。
3. 編集モードで、ダッシュボードのタイトルの横にある下矢印を選択し、**[削除]** をクリックします。
4. [Remove Tab] ダイアログで、**[Remove this dashboard from saved location]** チェックボックスをオンにし、**[OK]** をクリックします。

[レポート] ホームページのデフォルトダッシュボードビューの選択

ダッシュボードビューアのタブで複数のダッシュボードを開いている場合、いずれかのダッシュボードを、**[レポート]** ホームページのデフォルトダッシュボードとして表示するよう設定できます。

デフォルトダッシュボードを設定するには

1. [ダッシュボードビューア] ページの上部にある **[ダッシュボードのプロパティ]** リンクをクリックします。
2. **[選択したダッシュボード]** ボックスで、**[レポート]** ホームページにデフォルトダッシュボードとして表示するダッシュボードに対応するラジオボタンをクリックします。上矢印をクリックして、そのダッシュボードをリストの一番上に移動します。
3. **[保存]** ボタンをクリックします。
4. 左ペインの [ダッシュボード] リンクをクリックすると、選択したダッシュボードがデフォルトタブ (最初のタブ) として表示されます。

[ダッシュボードのプロパティ] ページには以下のフィールドがあります。

フィールド	説明
全ての所有者のダッシュボードを表示	すべてのユーザーが作成したすべてのダッシュボードを [利用可能なダッシュボード] ボックスに表示するには、[全ての所有者のダッシュボードを表示] チェックボックスをオンにします。
利用可能なダッシュボード	このボックスには、ダッシュボードビューアに表示できるすべてのダッシュボードの一覧が表示されます。
選択したダッシュボード	ダッシュボードビューアに表示するダッシュボードを [利用可能なダッシュボード] リストから [選択したダッシュボード] ボックスに移動します。このボックスに表示されているダッシュボードは、ダッシュボードビューアでタブとして表示されます。

ウィジェット

ウィジェットは、データを表示するためのメカニズムです。新しいダッシュボードを作成した後、レポートまたはWebリンクを表示するには、1つ以上のウィジェットを追加する必要があります。ウィジェットは、Widget Designerで設計します。ダッシュボードに表示する各ダッシュボード項目は、独自のウィジェットに格納する必要があります。ウィジェットは、複数のダッシュボードに配置できます。

ウィジェット デザイナー

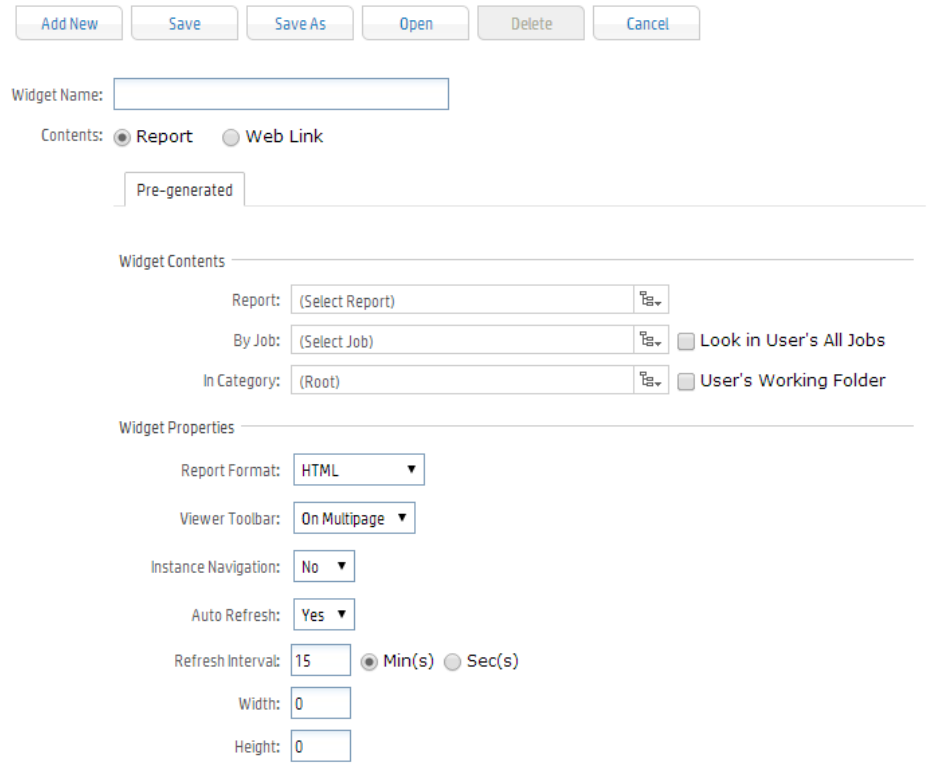
ウィジェット デザイナーを使用すると、新しいウィジェットの作成、ウィジェットの保存、ウィジェットの編集、ウィジェットの削除を行うことができます。レポートまたはWebリンク (外部リンク) をウィジェットに格納できます。各ウィジェットには、1つのオブジェクトのみを格納できます。

新しいウィジェットの作成

[ウィジェット・デザイナ] ページを開いて新しいウィジェットを作成するには、ダッシュボードビューアの上の **[ウィジェット・デザイナ]** をクリックします。

[ウィジェット・デザイナ] ページでは、ウィジェット、レポート、Webリンクに配置する内容を選択できます。

ダッシュボードビューからレポートを実行することはできません。以前保存し発行されたレポートの結果の表示だけを行うことができます。ダッシュボードを更新または自動更新すると、ダッシュボードの表示が、最後に発行された結果で更新されますが、レポートは実行されません。そのため、ダッシュボードビューでレポートデータを表示できるようにするには、ダッシュボード上のレポートを実行、保存、発行する必要があります。ダッシュボード上のレポートが保存または発行されていない場合、ダッシュボードビュー上のそのウィジェットにはエラーメッセージが表示され、ダッシュボードでレポートデータを利用できないことが示されます。



レポートウィジェットを作成するには

ウィジェットにレポートを格納するには、[ウィジェット・デザイナ] ページの **[レポート]** ラジオボタンをクリックします。

注: 実行および発行済みのレポートのみを追加できます。

ウィジェットには、次の項目の最後に発行したインスタンスを含めることができます。

- レポート: [レポート (Report)] フィールド、[ジョブ別 (By Job)]、または [カテゴリ内 (In Category)] では何も選択する必要がありません。
- 特定のレポート: [レポート (Report)] フィールドでレポートを参照します。[ジョブ別 (By Job)] および [カテゴリ内 (In Category)] フィールドは空白のままでかまいません。
- 特定のスケジュールレポートジョブで実行されたレポート: [ジョブ別 (By Job)] フィールドでジョブを参照します。[レポート (Report)] および [カテゴリ内 (In Category)] フィールドは空白のままでかまいません。
- 特定のカテゴリに展開され、特定のジョブで実行されたレポート: [カテゴリ内 (In Category)] フィールドでカテゴリを参照し、[ジョブ別 (By Job)] フィールドでジョブを参照します。
- 自分が所有しているジョブで出力された任意のレポート: ユーザーは、自分が作成したジョブか、自分の代わりに作成してもらったジョブを所有しています。**[ユーザーのすべてのジョブを検索 (Look in User's All Jobs)]** チェックボックスをオンにします。

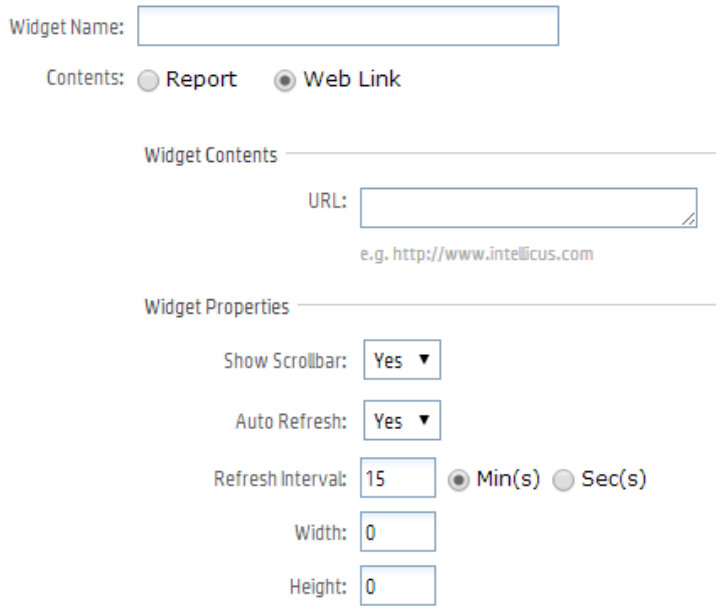
- デフォルトカテゴリに展開された任意のレポート: **[ユーザーの作業フォルダ (User's Working Folder)]** チェックボックスをオンにします。

以下のウィジェットプロパティを指定します。

ラベル	説明
ウィジェット名 (Widget Name)	作成する新しいウィジェットの名前を入力します。
レポートの形式 (Report Format)	レポートを表示する形式を選択します。
ツールバー (Toolbar)	ツールバーを表示するかどうかと、複数ページレポートの場合にすべてのページに表示するかどうかを選択します。
インスタンス・ナビゲーション (Instance Navigation)	レポートナビゲーション機能をダッシュボードに含めるかどうかを設定します。 • ダッシュボードのユーザーが保存したレポートを選択し表示できるように、プルダウンメニューを提供するには、**[はい (Yes)]** を選択します。 • この機能をダッシュボードで提供しない場合は **[いいえ (No)]** を選択します。
自動リフレッシュ (Auto Refresh)	一定の間隔でレポートを自動的に更新するには **[はい (Yes)]** を設定し、**[リフレッシュ間隔 (Refresh Interval)]** パラメーターを設定します。
リフレッシュ間隔 (Refresh Interval)	分単位の時間です。更新は、指定した時間 (分) の経過後に実行されます。たとえば、レポート結果を15分ごとに更新する場合、[リフレッシュ間隔 (Refresh Interval)] に15を設定します。
幅 (Width)	ウィジェットの幅をピクセル単位で選択します。整数のみを選択できます (小数は使用できません)。
高さ (Height)	ウィジェットの高さをピクセル単位で選択します (小数は使用できません)。

Webリンクウィジェットを作成するには

ウィジェットにWebリンクを格納するには、**[ウィジェット・デザイナ (Widget Designer)]** ページの **[Webリンク (Web Link)]** ラジオボタンをクリックします。



以下のプロパティを指定します。

ラベル	説明
URL	ウィジェットに表示するページの外部リンクのURLを指定します。
スクロールバーを表示 (Show Scrollbar)	ウィジェットにスクロールバーを表示するかどうかを選択します。デフォルトでは、スクロールバーが表示されます。
自動リフレッシュ (Auto Refresh)	デフォルトでは、Webページは自動的に更新されます。この機能をオフにするには [いいえ (No)] を選択します。
リフレッシュ間隔 (Refresh Interval)	分単位の時間です。更新は、指定した時間 (分) の経過後に実行されます。たとえば、Webページを15分ごとに更新する場合、[リフレッシュ間隔 (Refresh Interval)] に15を設定します。
幅 (Width)	ウィジェットの幅をピクセル単位で選択します。整数のみを選択できます (小数は使用できません)。
高さ (Height)	ウィジェットの高さをピクセル単位で選択します。整数のみを選択できます (小数は使用できません)。

ウィジェットの作成

ダッシュボードに表示する各ダッシュボード項目は、独自のウィジェットに格納する必要があります。新しいウィジェットは、**[ウィジェットデザイナ]** リンクを使用して作成します。

新しいウィジェットを追加するには

新しいウィジェットを追加するには、2つのウィジェットに分割するウィジェット上の  ([ウィジェットを水平方向に分割]) または  ([垂直方向に分割]) をクリックします。元のウィジェットはそのままとなり、新しい空のウィジェットがダッシュボードレイアウトに配置されます。

ウィジェットを削除するには

ウィジェットを削除するには、削除するウィジェットの右上隅にある **[ウィジェットを削除]** ボタンをクリックします。

ウィジェットのダッシュボードへの配置

レポートとWebリンク (外部リンク) オブジェクトを、ダッシュボードに配置できます。ただし、これらのオブジェクトをまずウィジェットに配置する必要があります。その後ウィジェットをダッシュボードに追加できます。

1. レポートが編集モードになっている状態で、空のダッシュボードページの右上隅にある **[ウィジェットを追加]** ボタンをクリックします。
2. ダッシュボードに配置するウィジェットを参照し、クリックしてダッシュボードにドラッグします。
3. ウィジェットをさらに追加するには、手順1と2を繰り返します。

ダッシュボード内での既存のウィジェットの移動

ダッシュボード上の既存のウィジェットを移動するには、ウィジェットの上部境界の上にマウスを移動します。ウィジェット名のバーがドロップダウンします。ウィジェット名のバーをクリックし、ドラッグしてウィジェットをダッシュボード上の目的の位置に移動します。

クエリ、パラメーター、テンプレートのデザイン

使い慣れたLoggerデザインツールを使用して、クエリ、パラメーター、パラメーター値グループ、テンプレートなどのレポートオブジェクトを作成または変更することができます。

クエリ

クエリオブジェクト (追加のメタデータが付属するクエリを構成します) は、レポートを設計するための基礎として使用されます。Loggerのレポート機能には、あらかじめ作成されたクエリが付

属しており、一般的なセキュリティユースケースを扱うシステム定義レポートとソリューションレポートの基礎として使用されます。

クエリオブジェクトは、エクスプローラーで参照または選択することができます。「レポートエクスプローラー」(171ページ) を参照してください。付属のクエリオブジェクトをそのまま使用するか、独自のレポートの基礎として使用するか、[クエリのリスト] ページで新しいクエリオブジェクトを設計することができます。既存のクエリオブジェクトを新しいクエリオブジェクトの出発点として使用できます。

注: 一部のクエリにはパラメーターが必要な場合があります。まず必要なパラメーターオブジェクトをすべて作成してから、それらのパラメーターオブジェクトを使用するクエリオブジェクトを作成することをお勧めします

パラメーターオブジェクトの作成については、「パラメーター」(292ページ) を参照してください。

デフォルトの検索フィールドの一覧を表示する方法については、「デフォルトのフィールド」(354ページ) を参照してください。デフォルトスキーマに追加するカスタムスキーマフィールドについては、「スキーマへのフィールドの追加」(461ページ) を参照してください。

SQLクエリを直接呼び出すレポートでは、SQLの標準的なinsubnet関数を以下のように使用することができます。`insubnet( "subnet string", address_column )`

注意: レポートとArcSightで定義されたコンテンツに対する変更は、コンテンツをアップグレードすると警告なく上書きされます。ArcSightで定義されているコンテンツを直接変更することはお勧めしません。

通常の手順として、ArcSightで定義されたコンテンツのコピーを変更してください。そうすれば、以降のアップグレードで変更内容が影響を受けなくなります。

このトピックでは、新しいクエリオブジェクトを設計する方法について説明します (最初から設計するか、既存のクエリオブジェクトを基にします)。

検索クエリとレポートクエリの違い

検索クエリとレポートクエリはどちらも同じ機能 (特定の条件に一致するイベントを見つける) を実行しますが、2つのクエリは以下のように違います。

- レポートクエリを作成するには、Loggerのクエリオブジェクトエディターを使用します。「クエリ」(262ページ) を参照してください。

  ヒント: レポートクエリとフィールド名クエリでは、インデックスフィールドを使用して、ベースとなる検索を高速化できます。

- 検索クエリを作成するには、LoggerのSearch UIを使用します。クエリは、通常の英語のキーワード、フィールド名、または正規表現を使用できます。「イベントの検索」(106ページ)を参照してください。

クエリ設計要素の概要

新しいクエリオブジェクトを作成するには、クエリ名を指定し、データ変換を定義し、クエリオブジェクトを保存する必要があります。Loggerレポートクエリのデータソースは、常にLoggerデータベースであるため、クエリオブジェクトの一部としてデータソースを指定する必要はありません。

必要に応じて、式の指定、フィールドプロパティの設定、変換の定義、書式設定の定義、フィールドグループの定義、ハイパーリンクの指定、ルックアップ値の定義、クエリへの必須のフィルタリングの構築を行うことができます。

クエリの操作

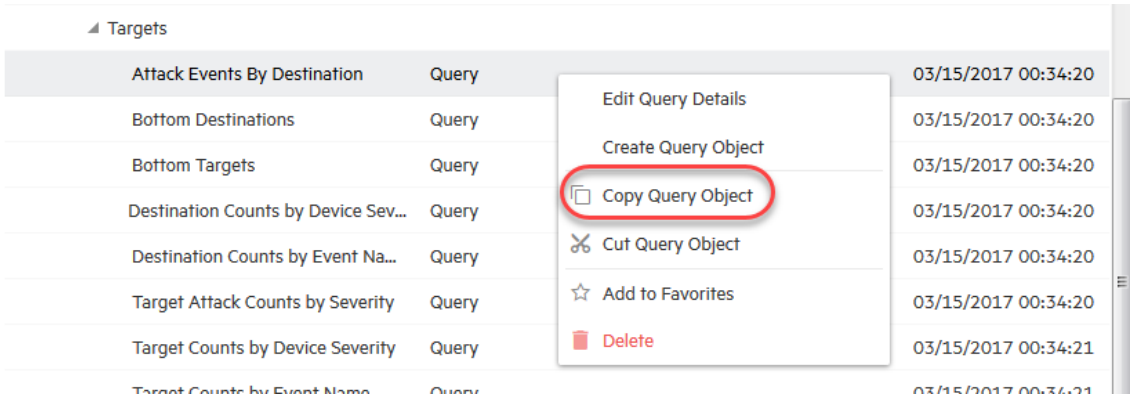
名前などの条件で既存のクエリを検索するには

1. レポートメニューの [デザイン] の下で、**[クエリ]** をクリックします。
2. ツールバーの **[開く]** をクリックします。
3. **[検索]**  をクリックします。
4. 条件ダイアログで、検索の条件を選択します。
5. **[検索]** をクリックします。条件に一致するすべてのクエリが返されます。

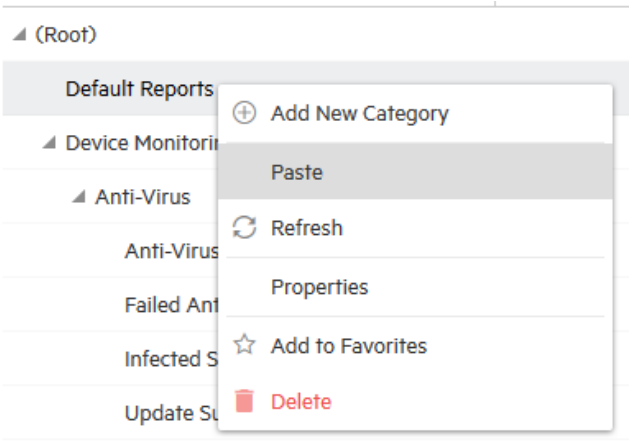
既存のクエリのコピーを作成する

既存のクエリオブジェクトを新しいクエリオブジェクトの基礎として使用するには

1. **エクスプローラー**から、カテゴリをクリックし、コピーするクエリの名前をクエリリストから選択します。
2. 右クリックしてコンテキストメニューを開きます。「エクスプローラーのオプションとコンテキストメニュー」(175ページ)を参照してください。
3. **[クエリオブジェクトをコピー (Copy Query Object)]** をクリックします。



4. カテゴリのリストで、コピーしたオブジェクトを配置するカテゴリ名を右クリックし、**[ペースト (Paste)]** を選択します。



新しいクエリオブジェクトの一時的なバージョンが、元のクエリオブジェクトと同じ内容で、同じ名前に「Copy of」というプレフィックスが追加されて作成されます。

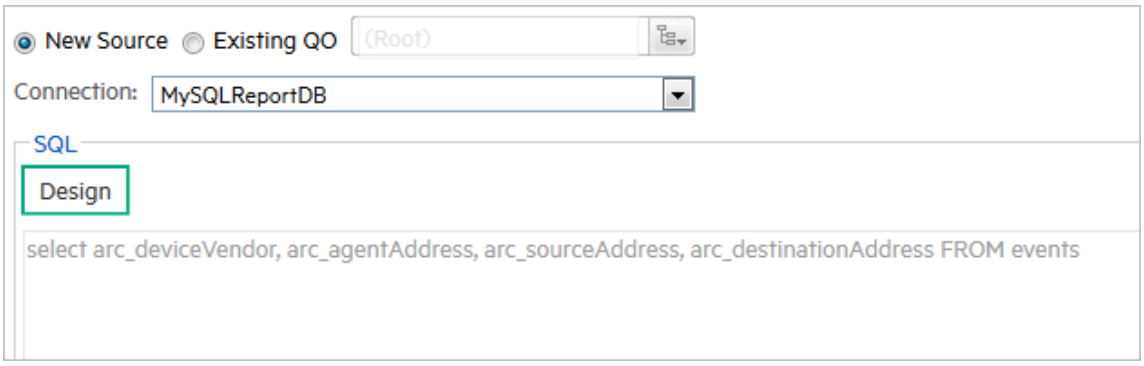
レポートに使用するIPv6検索クエリの作成

IPv6アドレスの検索クエリを作成するには

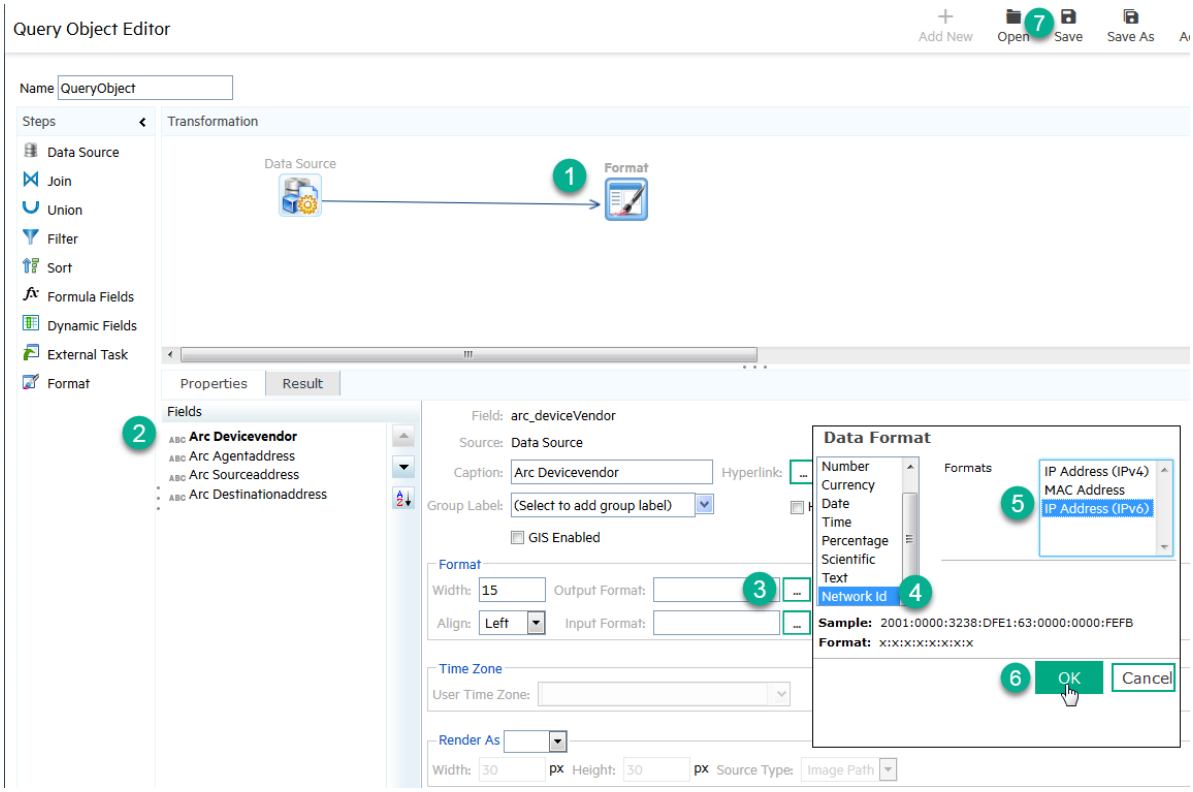
1. クエリオブジェクトを作成します。
   a. [レポート] の [デザイン] メニューの **[クエリ]** をクリックします。クエリオブジェクトエディターが表示されます。
   b. [プロパティ] タブの [SQL] セクションにある **[デザイン (Design)]** をクリックします。SQL Designerが表示されます。
   c. **[編集]** タブに、フィールドのリストを含むクエリを入力します。
   たとえば、以下のようなクエリを入力できます。

```
select arc_deviceVendor, arc_agentAddress, arc_sourceAddress, arc_
destinationAddress FROM events
```

d. **[OK]** をクリックします。クエリオブジェクトエディターの [SQL] セクションにフィールドが表示されます。



2. 各フィールドをIPv6フィールドとして定義します。以下の図を参照してください。



a. **[形式 (Format)]** アイコン (1) をクリックします。[プロパティ (Properties)] タブにクエリフィールドが表示されます。

b. **[フィールド (Fields)]** リスト (2) からフィールドを選択します。

c. **[出力フォーマット (Output Format)]** の横にある3つの点のアイコン ... (3) をクリックします。

d. [データ形式 (Data Format)] ポップアップ (4) から **[ネットワークID (Network Id)]**、**[IP**

アドレス(IPv6) (IP Address (IPv6))] (5) の順に選択します。

e. **[OK]** (6) をクリックしてポップアップを閉じます。

3. 各IPv6フィールドの定義が終了したら、クエリオブジェクトの名前を入力し、クエリを保存します。

クエリオブジェクトの変更

既存のクエリを変更するには、クエリオブジェクトエディターを使用します。

ヒント: Loggerやアドオンソリューションパックに用意されているクエリの変更はお勧めできません。用意されているクエリを土台にして固有のクエリを作成する場合は、「既存のクエリのコピーを作成する」(264ページ)に示すようにコピーを作成し、コピーを編集してください。

既存のクエリを変更するには

1. **[クエリエクスプローラ]** で、クエリが格納されている [クエリオブジェクト] カラムのカテゴリをクリックし、**[クエリ詳細を編集]** ボタンをクリックします。
2. クエリに必要な変更を加え (「クエリの操作」(264ページ)を参照)、**[保存]** をクリックします。

クエリオブジェクトの削除

カスタムクエリは削除できますが、Loggerやアドオンソリューションパックで用意されているクエリは削除できません。

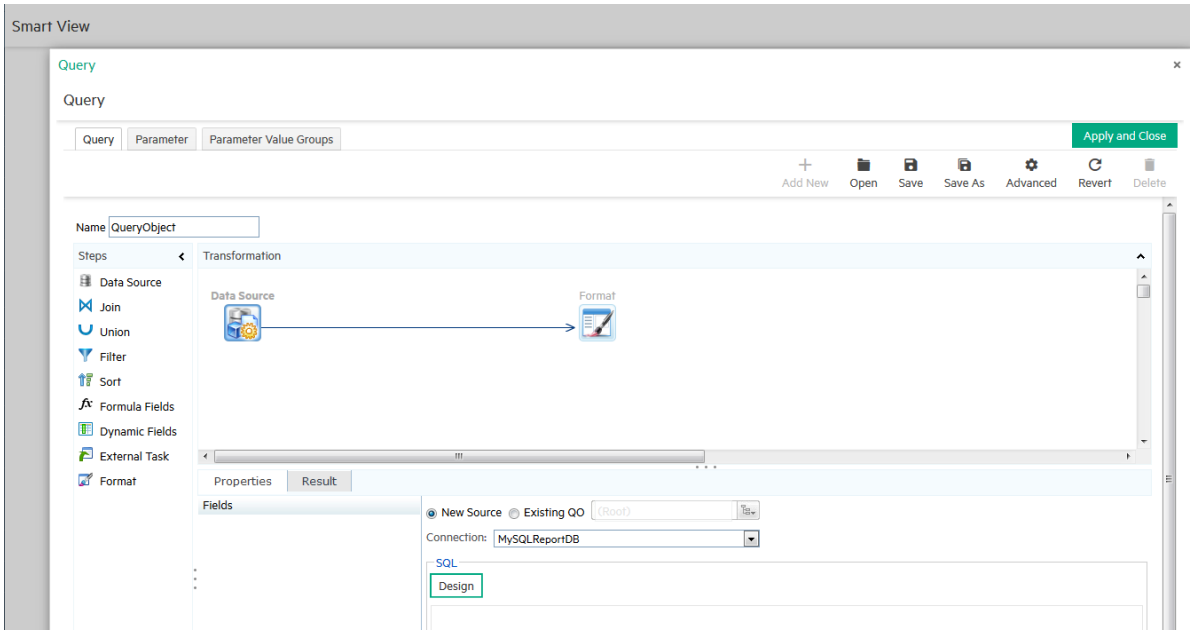
クエリを削除するには

[クエリエクスプローラ] で、クエリが格納されている [クエリオブジェクト] カラムのカテゴリをクリックし、**[削除]** ボタンをクリックします。

スマートデザイナーでの新しいクエリの作成

スマートレポートデザイナーによる新しいクエリの作成

1. [レポート] メニューの [デザイン] セクションから **[新しいレポート]** をクリックします。新しいタブに [スマートビュー (Smart View)] デザインページが開きます。
2. 右下の **[Create Query Object...]** をクリックします。
   クエリオブジェクトデザインエディターが開きます (スマートビュー内)。



3. クエリオブジェクトを選択するか、クエリを最初から作成する旨を選択します。デフォルト名は**QueryObject**です。「クエリ」(262ページ)を参照してください。
4. クエリオブジェクトのステップ情報を設定します。「ステップ」(273ページ)を参照してください。
   a. をクリックしてデータソーススステップを設定します。「データソーススステップ」(274ページ)を参照してください。
   b. をクリックして結合ステップを設定します。「結合ステップ」(277ページ)を参照してください。
   c. をクリックしてユニオンステップを設定します。「ユニオンステップ」(277ページ)を参照してください。
   d. をクリックしてフィルターステップを設定します。「フィルターステップ」(278ページ)を参照してください。
   e. をクリックしてソートステップを設定します。「ソートステップ」(278ページ)を参照してください。
   f. をクリックしてフォーミュラフィールドステップを設定します。「フォーミュラフィールドステップ」(278ページ)を参照してください。
   g. をクリックしてダイナミックフィールドステップを設定します。「動的フィールドステップ」(279ページ)を参照してください。
   h. をクリックして外部タスクステップを設定します。「外部タスクステップ」(280ページ)を参照してください。
   i. をクリックして形式ステップを設定します。「形式ステップ」(280ページ)を参照してください。

5. **[パラメータ (Parameter)]** タブをクリックして、クエリのパラメーターを設定します。「パラメーター」(292ページ) を参照してください。
6. 必要に応じて **[パラメータ値グループ (Parameter Value Groups)]** タブをクリックして、クエリのパラメーター値を設定します。「パラメーター値グループ」(300ページ) を参照してください。
7. 必要に応じてクエリを**保存**します。
8. 新しいクエリに問題がなければ、右上の **[Apply and Close]** をクリックします。

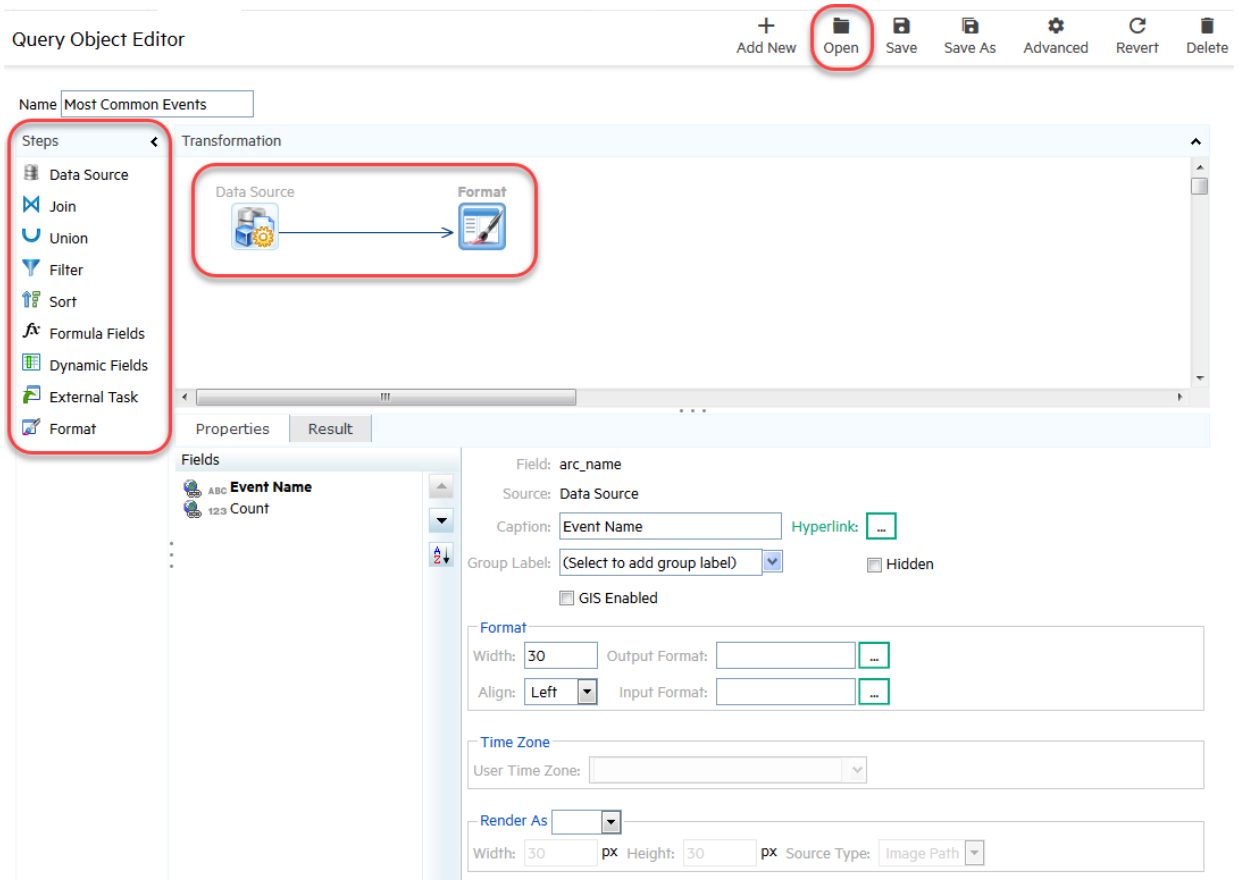
新しいクエリの設計

クエリオブジェクトは、データ変換を表し、最終的な出力を生成するための一連のステップ (要素) で構成されます。ステップは、データソース、ソート、フィルター、出力などの要素です。クエリは、クエリオブジェクトエディターを使用して対話的に設計します。

クエリオブジェクトエディターで新しいクエリを開くには

1. [レポート] メニューの [デザイン] セクションにある **[クエリ]** をクリックします。クエリオブジェクトエディターが開きます。

クエリオブジェクトエディターを以下に示します。**[ステップ (Steps)]** リストと **[変換 (Transformation)]** ワークスペースが強調表示されています。



変換を作成するには、クエリ要素 (ステップ) を **[ステップ (Steps)]** リストから **[変換 (Transformation)]** ワークスペースにドラッグし、要素を評価するシーケンスにリンクします。次に、各ステップのプロパティを指定します。

ステップの操作

ステップの使用方法を示します。

クエリへのステップの追加

1. リストから **[変換 (Transformation)]** ワークスペースにステップをドラッグします。

ステップのプロパティの指定

1. ステップを選択します。
2. **[プロパティ (Properties)]** タブをクリックします。
3. ステップの値を入力します。「ステップ」(273ページ) を参照してください。

追加したステップの結果表示

1. **[結果 (Results)]** タブをクリックします。

ステップから他のステップへのリンク

1. **[変換 (Transformation)]** ワークスペースで、ステップを選択します。
2. マウスボタンを押したままドラッグし、リンク先のステップに矢印 (リンク) を引き込みます。

3. リンクされた2つのステップの間にステップを追加するには、ステップをリンクにドラッグアンドドロップします。

ステップの名前変更

1. ステップを右クリックして、コンテキストメニューから **[ステップの名前を変更]** を選択します。
2. ステップの新しい名前を入力します。

ステップへのリンクの削除

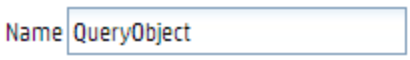
1. 項目を右クリックし、**[リンクを削除]** または **[ステップを削除]** を選択します。

クエリ設計手順

クエリは、**[変換 (Transformation)]** ワークスペースで視覚的に設計します。

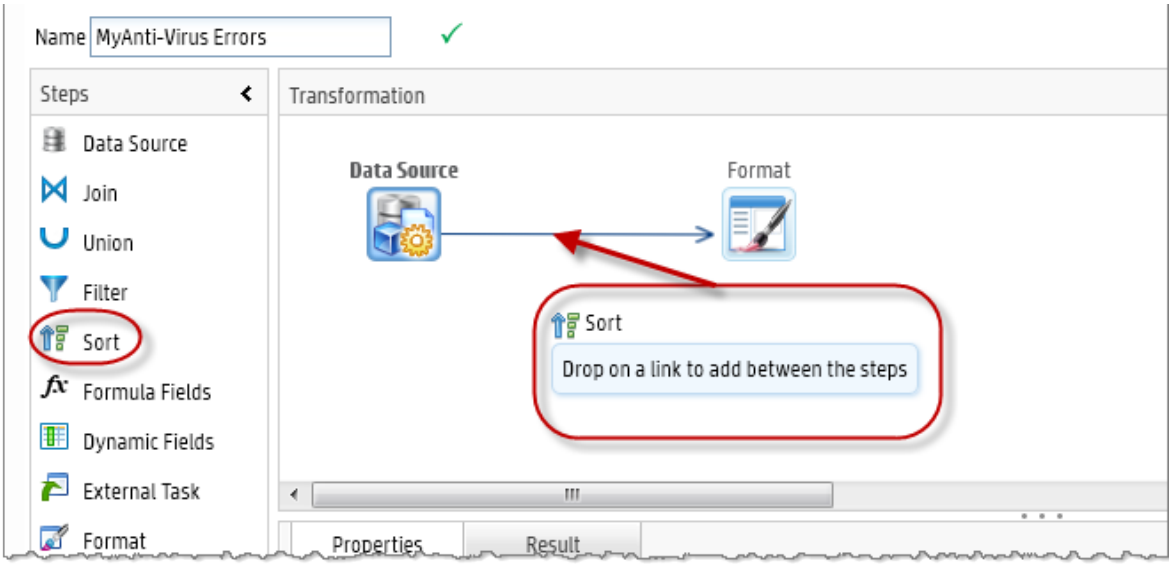
クエリを設計するには

1. ナビゲーションメニューの **[デザイン]** の下で、**[クエリ]** をクリックします。クエリオブジェクトエディターが開きます。
2. **[名前 (Name)]** フィールドに、このクエリオブジェクトの一意の名前を指定します。

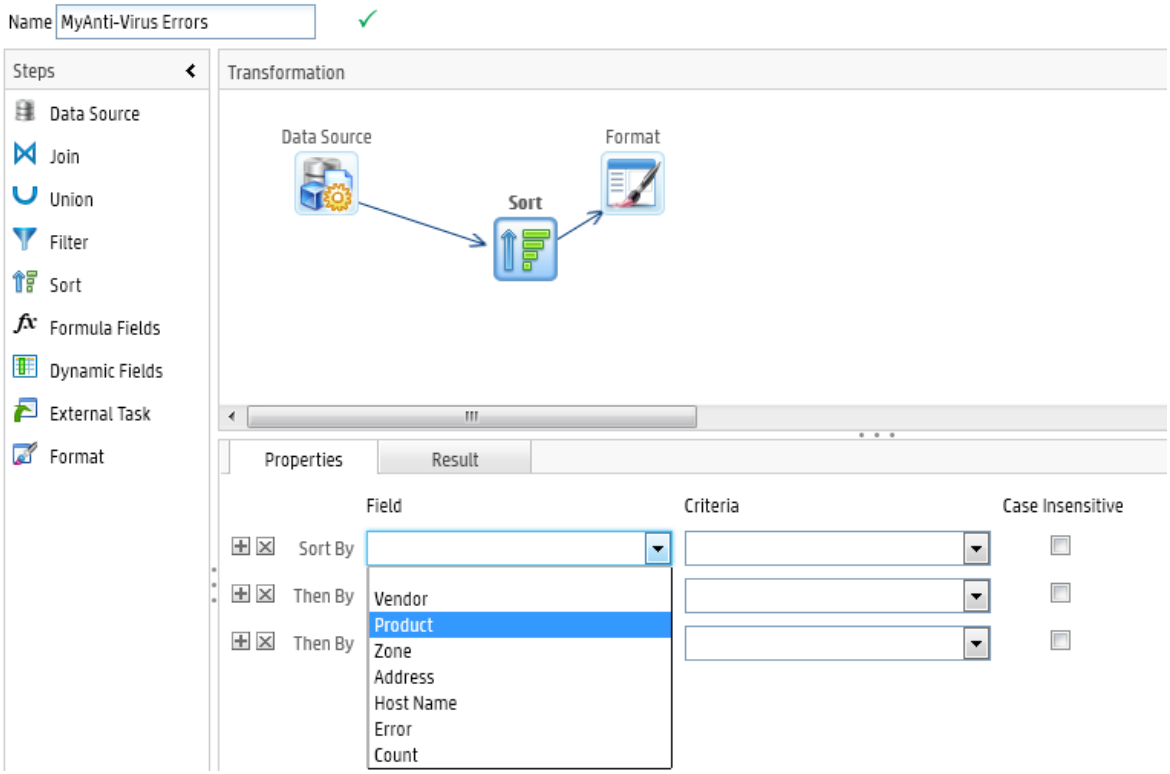


3. **[変換 (Transformation)]** ワークスペースで、クエリに必要なステップを **[ステップ (Steps)]** メニューから目的のシーケンスにドラッグアンドドロップします(デフォルトでは、**[変換 (Transformation)]** ウィンドウにData SourceおよびFormatステップが含まれています)。

   たとえば、変換にソートを追加するには、ソート要素を **[ステップ (Steps)]** リストから [変換 (Transformation)] フィールドにドラッグし、リンク上にドロップします。



その後、**[プロパティ (Properties)]** タブで、ソートに使用するフィールドを選択します。

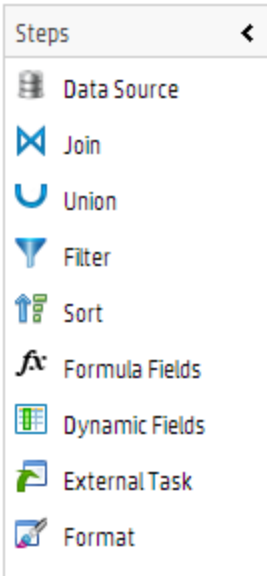


4. 必要に応じて、ツールバーの **[詳細 (Advanced)]** をクリックし、クエリオブジェクトの詳細なプロパティを設定します。
5. **[保存]** をクリックします。

注: このページを開いたとき、空のクエリオブジェクトが表示され、ツールバーの **[新規作成]** ボタンは、空のクエリオブジェクトを保存するまで無効になります。保存後、**[新規作成]** をクリックして新しいクエリオブジェクトを追加できます。

ステップ

ステップは、クエリオブジェクトの構築に使用される変換の要素です。ステップを使用するには、**[ステップ (Steps)]** メニューから **[変換 (Transformation)]** ウィンドウにドラッグします。ステップの動作は、**[プロパティ (Properties)]** タブでステップに割り当てたプロパティによって変わります。データに対するステップの結果は、ステップの **[結果 (Result)]** タブで確認できます。



クエリオブジェクトエディターでは以下のステップを使用できます。

ステップ

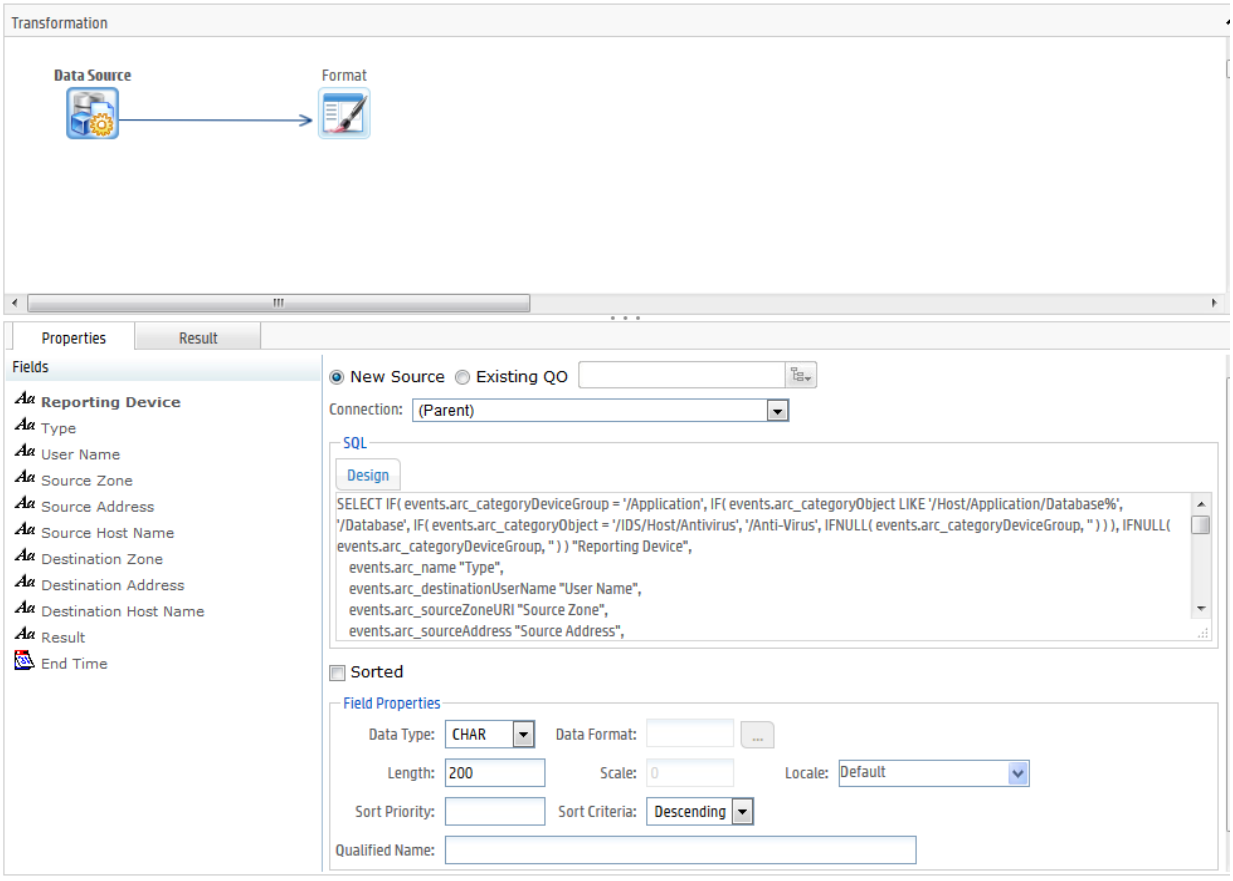
ステップ	説明
データソース (Data Source)	クエリオブジェクトにデータを取り込みます。少なくとも1つのデータソースが必要です。詳細については、「データソースステップ」(274ページ) を参照してください。
結合 (Join)	2つの入力を結合します。詳細については、「結合ステップ」(277ページ) を参照してください。
ユニオン (Union)	ある入力を別の入力に追加します。詳細については、「ユニオンステップ」(277ページ) を参照してください。
フィルタ (Filter)	定義済みのフィルターを適用し、ルックアップ値を設定します。詳細については、「フィルターステップ」(278ページ) を参照してください。
ソート (Sort)	ソート条件を設定します。詳細については、「ソートステップ」(278ページ) を参照してください。
フォーミュラフィールド (Formula Fields)	実行時に設定される計算フィールドの追加を可能にします。詳細については、「フォーミュラフィールドステップ」(278ページ) を参照してください。

ステップ (続き)

ステップ	説明
ダイナミックフィールド (Dynamic Fields)	実行時にクエリオブジェクトのフィールドを追加または削除します。詳細については、「動的フィールドステップ」(279ページ)を参照してください。
外部タスク (External Task)	標準およびカスタムサードパーティプロシージャーを呼び出します。詳細については、「外部タスクステップ」(280ページ)を参照してください。
形式 (Format)	クエリオブジェクトによって提供されるすべてのフィールドの一覧を表示します。一般に、フォーマットステップは、変換ワークフローの最後のステップになります。詳細については、「形式ステップ」(280ページ)を参照してください。

データソースステップ

データソースステップは、Loggerデータベースまたは既存のクエリオブジェクトからクエリオブジェクトにデータを取り込みます。1つのクエリは複数のデータソースステップを持つことができます。



データソースステップには以下のプロパティがあります。

データソースステップのプロパティ

プロパティ	説明
新規ソース/ 既存のQO	Loggerデータベースと既存のクエリオブジェクトのどちらを使用するかを選択します。
接続	親または接続の名前を選択します。 • 親: データは、クエリオブジェクトレベルで指定された接続から取得されるか、ユーザーに設定されているデフォルト接続に戻ります。 • 接続名: データは指定された接続からのみフェッチされます。
SQL	SQL Designerで設計された完全なSQL文。データソースがLoggerデータベースの場合にのみ表示されます。 SQL Designerを使用すると、テーブルをドラッグアンドドロップするか([デザイン]タブ)、完全なSQLを入力して([編集]タブ)SQL文を設計できます。 クエリエディターを使用する場合は、必ずデータ型に適したSQL構文を使用してください。たとえば、文字列データ型を呼び出すには、次のクエリのように、文字列を単一引用符で囲む必要があります。 `select arc_deviceVendor from events where lower(arc_deviceVendor) = 'arcsight'`
並べ替え済み	選択するとデータがソートされます。
フィールドプロパティ	[フィールド特性]のサブメニュー(有効な場合)では、選択したフィールドのプロパティを設定できます。これらのプロパティの説明については、「[フィールド特性]のサブメニュー」(275ページ)を参照してください。

[フィールド特性]のサブメニュー

プロパティ	値	コメント
データ型	CHAR、NUMBER、DATE、BINARY	取得するデータのデータ型を選択します。
データ形式	形式を示す文字列	取得するデータの形式を選択します。このプロパティが有効なのは、日付またはIPアドレスタイプのデータをCHAR型のフィールドに取得し、そのデータを今後の使用のために日付または数値タイプに変換しなければならない場合に限られます。

プロパティ	値	コメント
データベースタイムゾーン	リストからタイムゾーンを選択	取得した日付データを格納するときのタイムゾーンを指定します。このプロパティが有効なのは、レポートの要件に基づいて日時データを他のタイムゾーンデータに変換しなければならない場合に限られます。 たとえば、取得したGMTデータをレポート内で別のタイムゾーンに変換する必要がある場合、取得するデータを**GMT**と指定します。出力フォーマットは、一般に形式ステップまたはユーザー設定で指定します。
長さ/精度	値を入力	文字データ型の場合はフィールドの長さを、数値データ型の場合はフィールドの精度または長さを入力します。
目盛り	値を入力	スケールまたは小数点以下の桁数を入力します。
ロケール	メニューから選択	取得した日付データを格納するときの言語/国を指定します。
Sort Priority	数値0～*N*	データを複数のフィールドでソートする場合に、このフィールドのソート優先順位を指定します。プライマリソートフィールドには、最小の数値を指定する必要があります。
ソート条件	昇順/降順	昇順または降順のどちらでソートするかを指定します。
修飾名	値を入力	この名前は、WHEREやORDER BYなどのSQL句でフィールド名を指定するときに役立ちます。 また、別々のテーブルまたは式にある同名のフィールドを扱うとき、フィールド名の曖昧さを解決する際にも役立ちます。

結合ステップ

結合ステップは、2つの入力を結合します。結合ステップには以下のプロパティがあります。

結合ステップのプロパティ

プロパティ	説明
すべてのフィールドを選択	有効にすると、両方のソースのすべてのフィールドをこのステップの出力で使用できます。選択解除すると、出力で使用可能にするフィールドを選択できます。
結合タイプ	以下の結合タイプのいずれかから選択します。 • 内部結合 • Left Outer • Right Outer • Full Outer
結合条件	結合キーを形成します。

ユニオンステップ

ユニオンステップは、ある入力を別の入力に追加します。ユニオンステップには以下のプロパティがあります。

ユニオンステップのプロパティ

プロパティ	説明
ユニオンタイプ	[並べ替え済み] または [並べ替えなし] を選択します。
重複行を削除	選択した場合、結果の各行が別個のものになります。
横棒	列の名前を入力します。 列の名前を変更するにはクリックします。 列を追加するにはクリックします。 列を削除するにはクリックします。

フィルターステップ

フィルターステップは、定義済みのフィルターを適用し、ルックアップ値を設定します。フィルターステップには以下のプロパティがあります。

フィルターステップのプロパティ

プロパティ	説明
アドホックフィルター	1つ以上のアドホックフィルターを適用するには、**[フィルタ条件の選択]** で、**[フィールド名]**、**[条件]**、および **[値]** 入力します。**[+]** をクリックしてフィルターを追加するか、**[X]** をクリックして削除します。
ルックアップ値	有効な場合、ルックアップ値のリストがエンドユーザーに表示され、フィルターに適用する値を簡単に選択できるようになります。
必須	有効にすると、このクエリオブジェクトを使用するすべてのレポートで、選択したフィールドにフィルターを適用する必要があります。
非表示	有効にすると、フィールドは、エンドユーザーに対して、フィルター処理対象のフィールドのリストに表示されなくなります。

ソートステップ

ソートステップはソート条件を設定します。ソートステップには以下のプロパティがあります。

ソートステップのプロパティ

プロパティ	説明
フィールド	ソートで使用するフィールドをリストから選択します。**[並べ替え順]** 行と **[次の基準]** 行を使用して、ソートのための複数のフィールドを追加できます。
条件	昇順または降順のソート条件。
大文字小文字の区別なし	有効にすると、ソート時に大文字と小文字が無視されます (ABCは、abcと同じレベルになります)。
非表示	有効にすると、フィールドは、エンドユーザーに対して、フィルター処理対象のフィールドのリストに表示されなくなります。

フォーミュラフィールドステップ

フォーミュラフィールドステップを使用すると、実行時に設定される計算フィールドを追加できます。これらの計算フィールドは、一般に既存のフィールドに基づきます。

式フィールドを追加するには、**[+]** をクリックします。次に、以下のようにフィールドの値を指定します。

フォーミュラフィールドのプロパティ

プロパティ	説明
名前	フィールドの名前とキャプション。
戻り型	式フィールドのデータ型 (数、文字、または日付)。
長さ/ 精度	• 文字データ型の場合はフィールドの長さ。 • 数データ型の場合はフィールドの精度または長さ。
目盛り	スケールまたは小数点以下の桁数。

フォーミュラ	JavaScriptの構文を使用した式。式を作成するために、フィールド名を使用して変数を定義できます。
	• 式には、if文やネストしたifと論理演算子を含めることができます。
	• 式に複数の文を含めるには、セミコロン (;) を使用して文を区切ります。
	例 TotalAmountという名前の式フィールド
	`var total ;`
	`if (unitprice < 10 )`
	`{total = unitprice*quantity;}`
	`else`
	`{total = unitprice;}`
	`TotalAmount = total;`

動的フィールドステップ

動的フィールドステップは、実行時にクエリオブジェクトにフィールドを追加または削除できます。動的フィールドは、単一のデータソースからデータをピボットするか、フィールドプロパティのメタデータを動的にフェッチすることで追加できます。

- **動的マッピング**は、メタデータ結果セットから各フィールドを取得し、クエリオブジェクトのフィールドプロパティにマッピングします。プライマリマッピングは**フィールドID**、**フィールド名**、**キャプション**、および**データ型**です。
- **ピボット**は、正規化され名前と値がペアになったデータを、フラットな表形式データに変換します。[ピボット] タブには以下のフィールドがあります。
  - **[列をピボット]:** フィールドIDが格納されている列と、値が格納されている列を指定します。
  - **[グループ分けの基準の選択]:** グループ化フィールドを指定します。グループ化すると、正規化されたデータがフラットな表に変換されます。

外部タスクステップ

外部タスクステップを使用すると、標準のプロセスとカスタムサードパーティプロセスを呼び出すことができます。Loggerには、あらかじめ設定された以下の外部タスクがあります。

- **Java Rowプロセッサー**: Java行の処理用
- **Rジョブ**: R Analytics Serverスクリプト用 (プロパティについては「Rジョブのパラメーター」(280ページ) を参照)
- **ハイブジョブ**: Hiveスクリプト用
- **Pigジョブ**: Pigスクリプト用
- **カスタムMap Reduceジョブ**: カスタムマップ削減スクリプト用

Rジョブのパラメーター

プロパティ	説明
サーバIP	RサーバーのIPアドレス
プロットタイプ	フォーマットタイプが画像形式の場合、ドロップダウンリストからプロットタイプを選択します
フォーマットタイプ	フォーマットタイプを選択します
モデルファイル	Rモデルファイルの場所
イメージの数	フォーマットタイプが画像形式の場合は、出力中の画像の数を入力します
スクリプト	Rスクリプトファイル名
検証	クリックしてRジョブを検証します

形式ステップ

形式ステップは、ワークフローの最後のステップであり、クエリオブジェクトによって提供されたすべてのフィールドを一覧表示します。形式ステップには以下のパラメーターが含まれています。

形式ステップのパラメーター

プロパティ	説明
フィールド	フィールドの元の名前。
ソース	このフィールドの元となったステップ。
キャプション	このフィールドがエンドユーザーに表示される名前。
ハイパーリンク	ドリルダウンの詳細またはハイパーリンクURL。
グループ・ラベル	このフィールドを既存のグループに割り当てるには、ドロップダウンリストからグループ名を選択します。新しいグループを作成するには、新しいグループ名を入力します。

形式ステップのパラメーター (続き)

プロパティ	説明
非表示	選択した場合、レポートプロセスでフィールドがユーザーに表示されなくなります。
GISが有効になっています	選択した場合、フィールドには国名、州、都市名など、GIS分類データを格納する必要があります。[GISが有効になっています] フィールドは、**[GIS Mapping]** ダイアログのグループ化オプションの選択リストと、**[マップを作成]** ダイアログの **[面フィールド]** および **[ヒートマップ・プロパティ]** > **[値フィールド]** に表示されます。詳細については、「マップ」(248ページ) を参照してください。
書式設定プロパティ	
幅	レポートにドラッグしたときのこのフィールドのデフォルトの幅。有効な値は1～100です。
出力フォーマット	フォーマット文字列を入力します。フィールド値は、フォーマット文字列を使用してフォーマットされます。日付と数のフォーマットに便利です(フォーマット文字列を実行時に決める必要がある場合は、**[Apply Locale Default]** を選択します)。
揃え	レポートに割り当てるときのフィールドの位置揃え (左、中央、右)。
入力フォーマット	フォーマット文字列を入力します。この文字列は、アドホックフィルターでこのフィールドの値の入力を指示するフォーマットを決定します。日付またはIP値を目的の形式で入力指示する際に便利です。
User Time Zone	レポートデータの表示のためのタイムゾーン。レポートサーバーは、データベースタイムゾーンとユーザータイムゾーンの差を計算して変換を実行します。実行時にタイムゾーンを決定するには、[SYS_USER_TZ] を選択します。

形式ステップを定義するには

1. **[フィールド]** リストから、入力フォーマットを定義するフィールドを選択します (選択したフィールドは太字で表示されます)。
2. 適切な形式を選択し、その形式に必要な値を指定します。

必須のフィルタリングフィールドとして指定するには

[フィールド] リストから、必須のフィルタリングフィールドとして指定するフィールドを選択します。

[フィールド] リストの右側にある **[必須]** チェックボックスをオンにします。

[必須] チェックボックスを使用して、他のフィールドを選択または選択解除できます。

クエリオブジェクトの詳細プロパティ

クエリオブジェクトレベルの詳細プロパティは、クエリオブジェクトの動作と、クエリオブジェクトを使用して生成されるレポートを制御します。

[詳細プロパティ] タブで指定する値

プロパティ	値	コメント
監査ログ	(デフォルト) 有効にする 無効にする	クエリオブジェクトを使用して生成されるレポートの監査ログのオン/オフを、グローバルな監査ログ設定とは関係なく切り替えることができます。
実行の優先順位	(デフォルト) 低 中間 高い	レポートサーバーのリクエストキューの優先順位を決定します。
データベース接続タイムアウト	ユーザー指定	接続レベルまたはグローバルレベルの同名プロパティの値に優先します。
データソースフェッチサイズ	ユーザー指定	接続レベルまたはグローバルレベルの同名プロパティの値に優先します。
Max Rows	ユーザー指定	このクエリオブジェクトの最大行数制限。レポートレベルの [Max Rows] の値は、この値を下回ることはできますが、上回ることはできません。
クエリー実行	(デフォルト) 同期 非同期	同期: データベースリクエストを送信した後、データが戻るまで、スレッドは待機します。 非同期: データベースでのデータ処理に時間がかかる場合、データの返信開始までの間、表示スレッドを解放します。例: データベースで大量のソート処理を行う場合や、データの返信の前に複雑なデータ処理が必要な場合。
バックグラウンドに限定	(なし) 有効にする 無効にする	有効にする: このクエリオブジェクトを使用するレポートには、バックグラウンドでの実行のみが許可されます。クエリに長い時間がかかる場合に便利です。 無効にする: [実行] と [バックグラウンドで実行] の両方を選択できます。
次の形式に限定	(なし) 選択可能な形式のリスト	なし: このクエリオブジェクトを使用するレポートは、サポート対象のすべての形式で実行できます。 選択した値: このクエリオブジェクトを使用するレポートは、選択した形式でのみ実行できます。たとえば、数百万行が出力されるレポートは、XLS形式とRAWテキスト形式でのみ扱うことができます。
実行ごとのデフォルトのメモリ使用量	ユーザー指定	接続レベルまたはグローバルレベルの同名プロパティに優先します。
レポート・サーバー・チャンク・タイム・アウト	ユーザー指定	接続レベルまたはグローバルレベルの同名プロパティに優先します。
実行ごとにエリア・サイズを並べ替えます	ユーザー指定	行のメモリ内ソートのメモリ制限を決定します。接続レベルまたはグローバルレベルの同名プロパティに優先します。

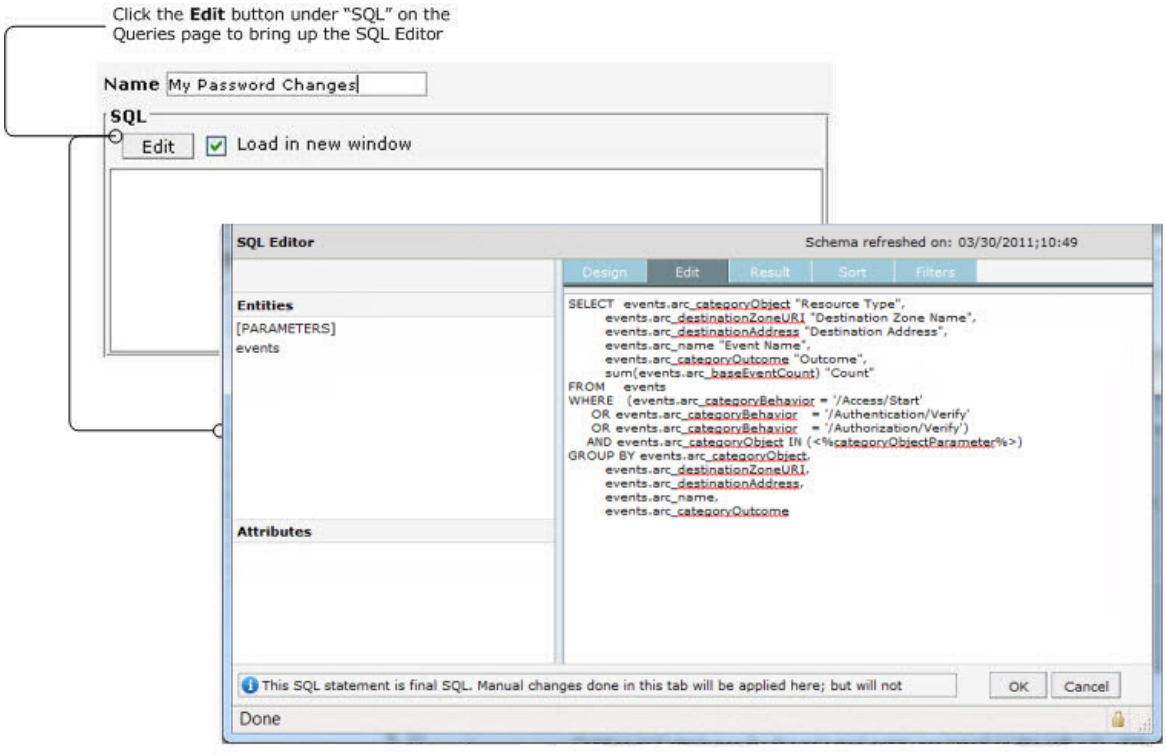
[詳細プロパティ] タブで指定する値 (続き)

実行ごとにスレッドを並べ替えます	ユーザー指定	スレッドのメモリ内ソートのメモリ制限を決定します。接続レベルまたはグローバルレベルの同名プロパティに優先します。
データのキャッシング	(なし) 有効にする 無効にする	有効にする: このクエリオブジェクトの結果セットのキャッシュを作成し、特定の時間までレポートの表示中および表示後の操作に再利用できるようにします。
Update Fields at Runtime	(なし) 有効にする 無効にする	有効にする: データベースクエリが実行時に新しいフィールドを返す場合、このクエリオブジェクトはそれらすべてのフィールドをアドホックウィザードまたはパワービューワでユーザーに表示します。

エディターでのSQLの定義

各レポートは、LoggerデータベースのSQLクエリに基づいて作成されます。SQL (Structured Query Language) とは、データベースの情報の取得と更新を目的としたISO規格のプログラミング言語です。LoggerはSQLクエリをサポートし、SQL文を定義できるインタラクティブなSQLエディタを提供しています。

[レポート] > [クエリ] ページでのSQLエディタへのアクセス



エンティティと、選択したエンティティの属性は、SQLエディタの左側にリスト表示されます。SQLエディタの右側には、選択した文に関連する情報を示すタブが表示されます。

注: [属性] リストには、Logger内部の属性がいくつか表示されます。これらの属性をクエリ

に使用すると、予想どおりの結果が結果レポートに出力されないため、これらの属性は使用しないでください。arc_sourceZoneResourceより後の属性、つまり、arc_eventTime、arc_deviceName、arc_rowId、arc_othersなどはすべて内部属性です。

SQLエディタのタブ

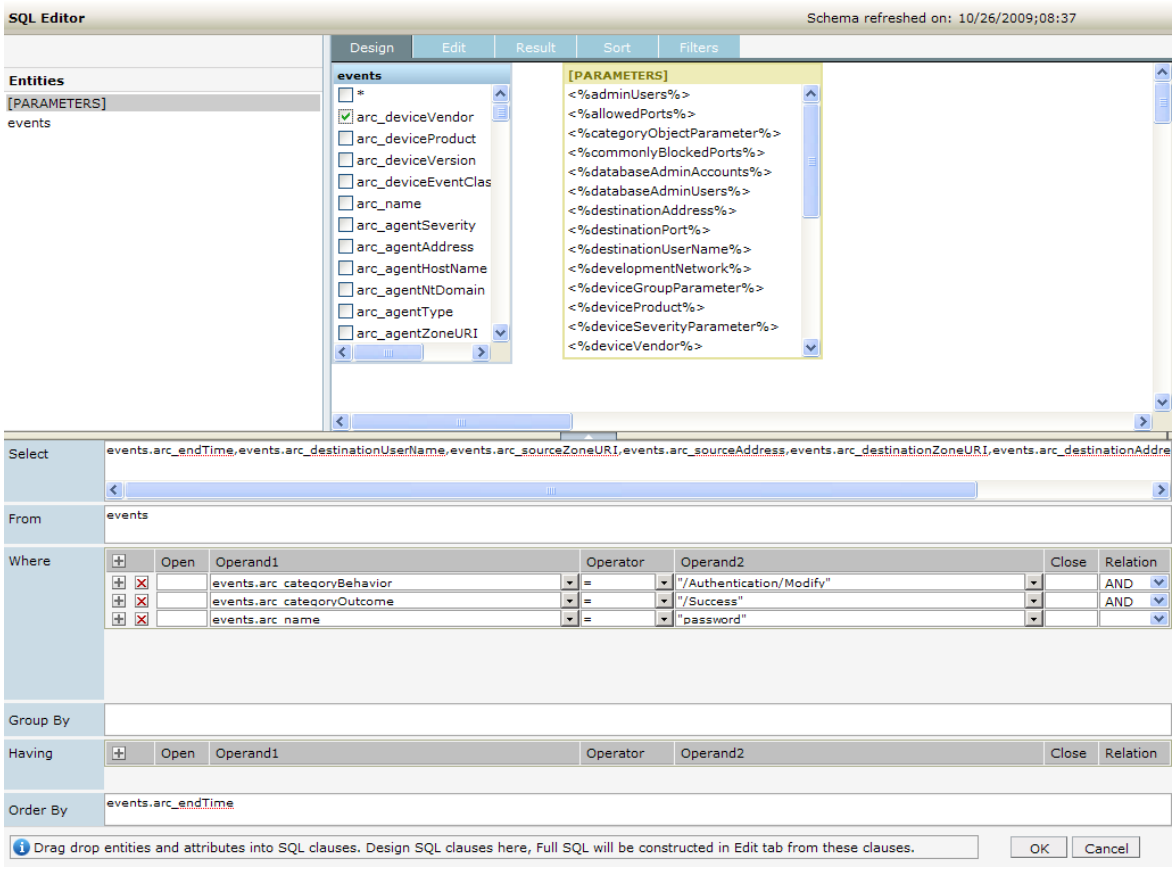
オプション	説明
デザイン (Design)	グラフィカルなSQLクエリデザイナーです。このタブのオプションを使用すれば、比較的簡単なクエリをドラッグアンドドロップ方式で設計できます。
編集 (Edit)	SQL文を表示します。[デザイン (Design)] タブで作成したクエリは、このタブにSQL文として表示されます。ここでSQLを直接記述したり、貼り付けたりすることもできます。
結果 (Results)	SQLの実行結果として受信した行が表示されます。
ソート (Sort)	ソートの設定を行います。
フィルタ (Filters)	フィルターを追加して、クエリに含める実行時フィルターの条件を設定します。

データベースオブジェクトのリスト

SQLエディタは、データベースオブジェクトのリストを提供するデータベースへの**デフォルトの接続**を示します。Loggerレポートは、1つのタイプのオブジェクトまたはエンティティを1つのeventsテーブルとして提供します。**[events]** ([エンティティ] の下) をクリックすると、イベントフィールド (属性) が **[属性]** の下に表示されます。

[デザイン] タブ

簡単なSQLクエリであれば、**[デザイン (Design)]** タブを使用して、「ドラッグアンドドロップ」方式で設計できます。



[デザイン (Design)] タブでSQLクエリ文を作成するには

1. エディターの左側の **[エンティティ (Entities)]** の下にある **[events]** をクリックして “events” エンティティを選択します。

   イベント属性のリストが [属性] の下に表示されます。
2. エディターの左側にある **[属性]** リストのイベント属性をクリックし、右側の **[選択 (Select)]** ボックスにドラッグします。**[から (From)]** 句に、関連する値が自動的に表示されます。

> **注:** [属性] リストには、Logger内部の属性がいくつか表示されます。これらの属性をクエリに使用すると、予想どおりの結果が結果レポートに出力されないため、これらの属性は使用しないでください。`arc_sourceZoneResource`より後の属性、つまり、`arc_eventTime`、`arc_deviceName`、`arc_rowId`、`arc_others`などはすべて内部属性です。

3. 別のエンティティから他の属性を選択するには、以上の手順を繰り返します。

ヒント: イベント属性を **[属性]** の下に表示するには、**[events]** エンティティ (左上の [エンティティ (Entities)] の下) を選択する必要があります。属性が表示されない場合、SQLエディタの左側の [エンティティ (Entities)] リストで [events] が選択されているかどうかを確認してください。

選択

[選択 (Select)] ボックスは、特定のエンティティのために選択された属性を示します。

場所

[どこ (Where)] 領域は、クエリの “where” 句を示します。

- 先頭に行を追加するには、カラムヘッダーの左端にあるセルの ([最初の条件を挿入]) をクリックします。
- 現在行の下に行を追加するには、条件行の追加先となる上の行の ([作成条件]) をクリックします。該当行の下に行が挿入されます。
- 条件を削除するには、条件を削除する行の ([この条件を削除]) をクリックします。
- where句を指定するには、[オペランド- 1 (Operand1)]、[オペランド- 2 (Operand2)]、[演算子 (Operator)] を選択して条件を作成します。
- 条件を結合するには、条件を2つ作成し、(結合する2つの条件のうちの) 最初の条件の右端にあるカラムから関係を選択します。
- 条件をグループ化するには、開きの波カッコと閉じの波カッコを適切な行に指定します。

グループ分け (Group By)

Group By句では、SQL文のグループ化条件を指定できます。[グループ分け (Group By)] にエンティティを配置するには、[エンティティ (Entity)] リストでエンティティをクリックし、[グループ分け (Group By)] の下のボックスにドラッグします。

所有 (Having)

“Having” 句を作成するには、“Where” 句の説明と同じ設定を使用します。「場所」(286ページ) を参照してください。

注: “Having” 句で使用できるように、“Select” 句には必ず適切な集計関数を追加してください。

順番の基準 (Order By)

Order By句では、SQL文のソート (昇順/降順) 条件を指定できます。グループ化を行うレポートでは、“Order By” 句のカラムの順序は、レイアウトエディターの各セクションと同じ順序であることが必要です。

注意: Order Byを使用するレポートクエリに数百万のイベントが含まれる場合、このクエリは失敗し、以下のエラーメッセージが表示されます。“`The server is too busy, try again later`”

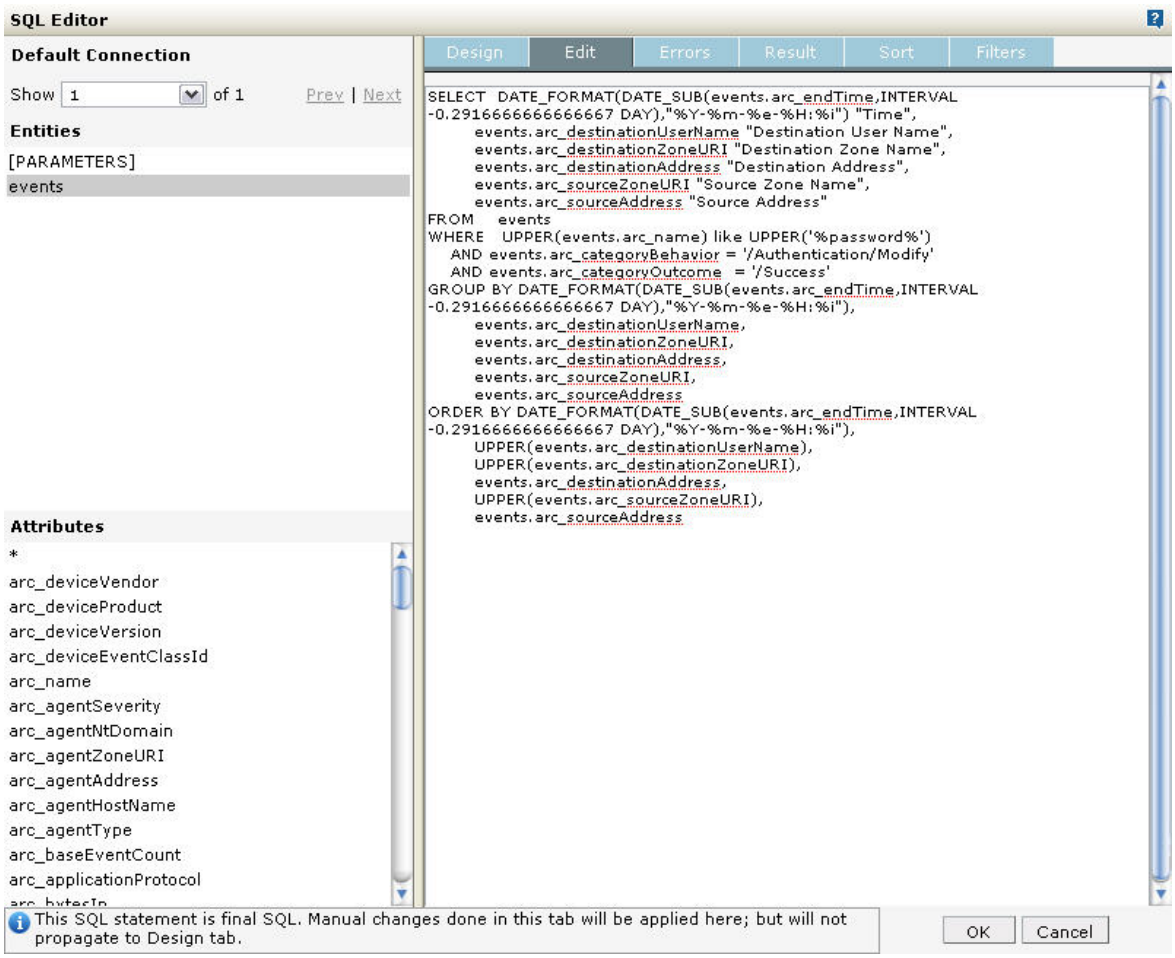
そのため、以下のベストプラクティスに従うことをお勧めします。

- スキャンするイベントの数を制限するために、[検索数の制限値] パラメーターを使用する。
- 名前または時間でグループ化するようにレポートクエリを書き直し、スキャンするイベントの粒度を下げる。

[編集] タブ

[デザイン (Design)] タブから **[編集 (Edit)]** タブに切り替えると、[デザイン (Design)] タブ内のSQLが構築され、完全なSQL文として [編集 (Edit)] タブに表示されます。[編集 (Edit)] タブを使用すると、[デザイン (Design)] タブでは定義できない複雑なSQL文を表示または記述することができます。

SQLエディタ: [編集] タブ



[編集 (Edit)] タブと [デザイン (Design)] タブの関係

[編集 (Edit)] タブで定義した複雑なクエリがその後の [デザイン (Design)] タブでの変更によって誤って上書きされないように、SQLエディタは作成中のSQL文を管理します。

まず [編集 (Edit)] タブに複雑なクエリを入力し、次に [デザイン (Design)] タブをクリックしてそこで変更を加えた後、再度 [編集 (Edit)] タブをクリックすると仮定します。その場合、[編集 (Edit)] タブの元の文に [デザイン (Design)] タブの変更内容を上書きするかどうかを確認するメッセージが表示されます。

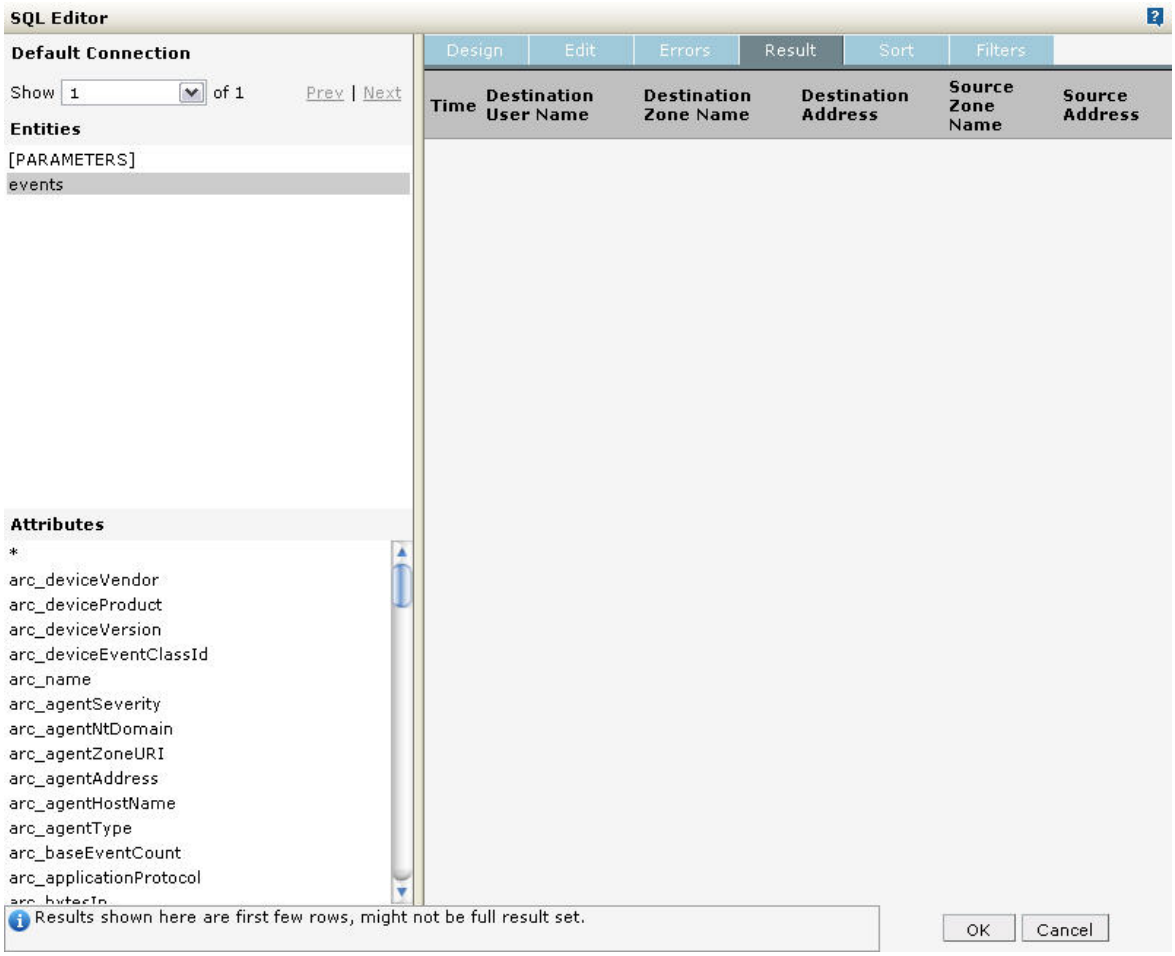
- **[OK]** をクリックすると、**[編集 (Edit)]** タブに変更内容が上書きされます。これは、[デザイン (Design)] タブのSQLが再構築されるためです。
- **[キャンセル (Cancel)]** をクリックすると、**[編集 (Edit)]** タブのSQLは影響を受けず、最終的なSQLとして使用されます。

[編集 (Edit)] タブに反映されたSQL文は、最終的なSQLとしてコンパイルに使用されます。

[結果 (Result)] タブ

[結果 (Result)] タブには、現在指定されているSQL文 ([編集 (Edit)] タブに表示) に基づくクエリの結果が表示されます。SQLでパラメーターを使用する場合、クエリの結果を表示するために値の指定を要求されます。

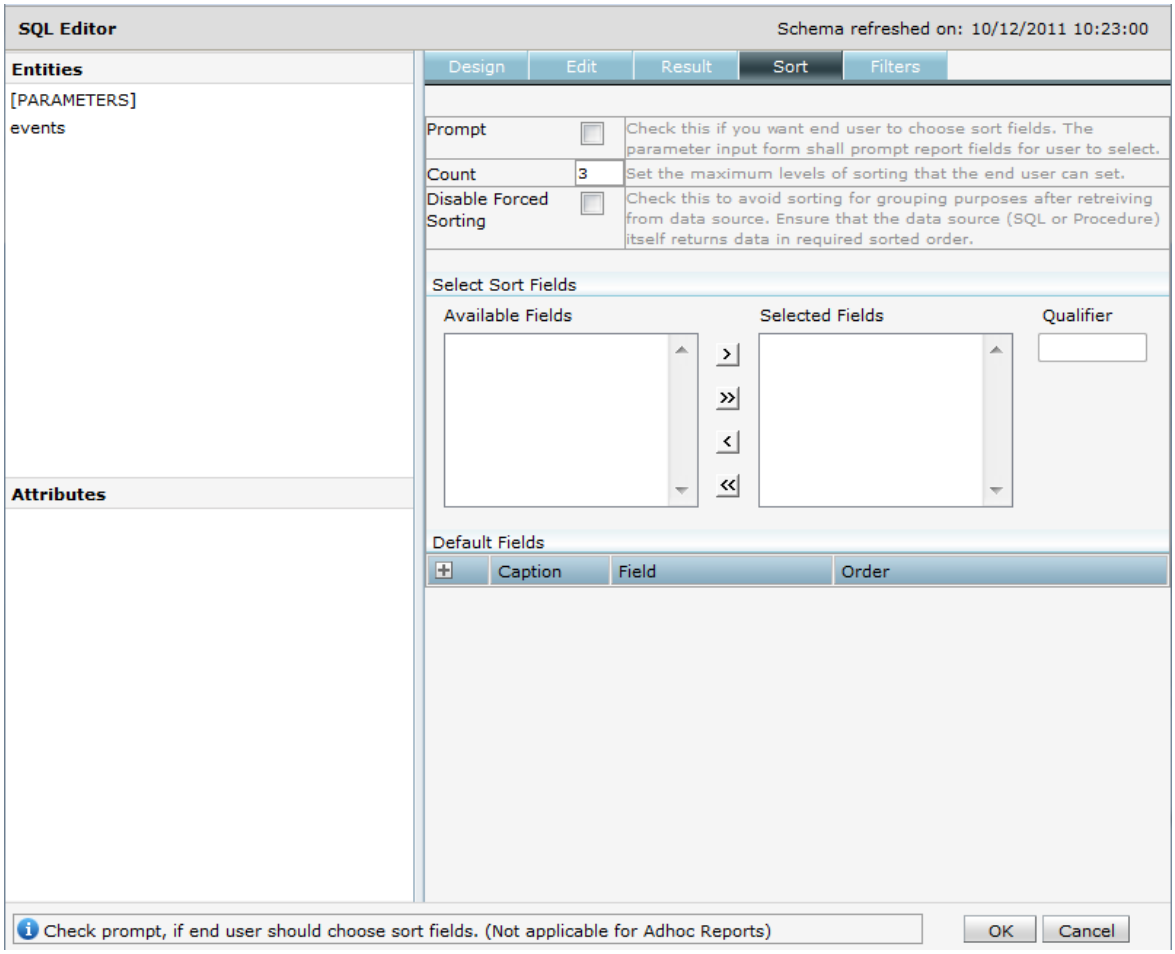
SQLエディタ: [結果 (Result)] タブ



[ソート (Sort)] タブ

レポート実行時のソートレベルを指定するには、**[ソート (Sort)]** タブをクリックします。

SQLエディタ: [ソート (Sort)] タブ



[ソート (Sort)] タブの設定について、以下の表で説明します。

[ソート (Sort)] タブのオプション

フィールド	説明
Prompt	レポートの実行時にソート順序に関する確認メッセージを表示する場合、このボックスをオンにします。**[プロンプト (Prompt)]** が有効な (チェックされている) 場合、レポートの実行時にソート順序の指定を求めるダイアログが表示されます。
カウント (Count)	ソートのレベル数を指定します。 たとえば、国でソートした後、都道府県、市区町村でソートする場合は、3を選択します。

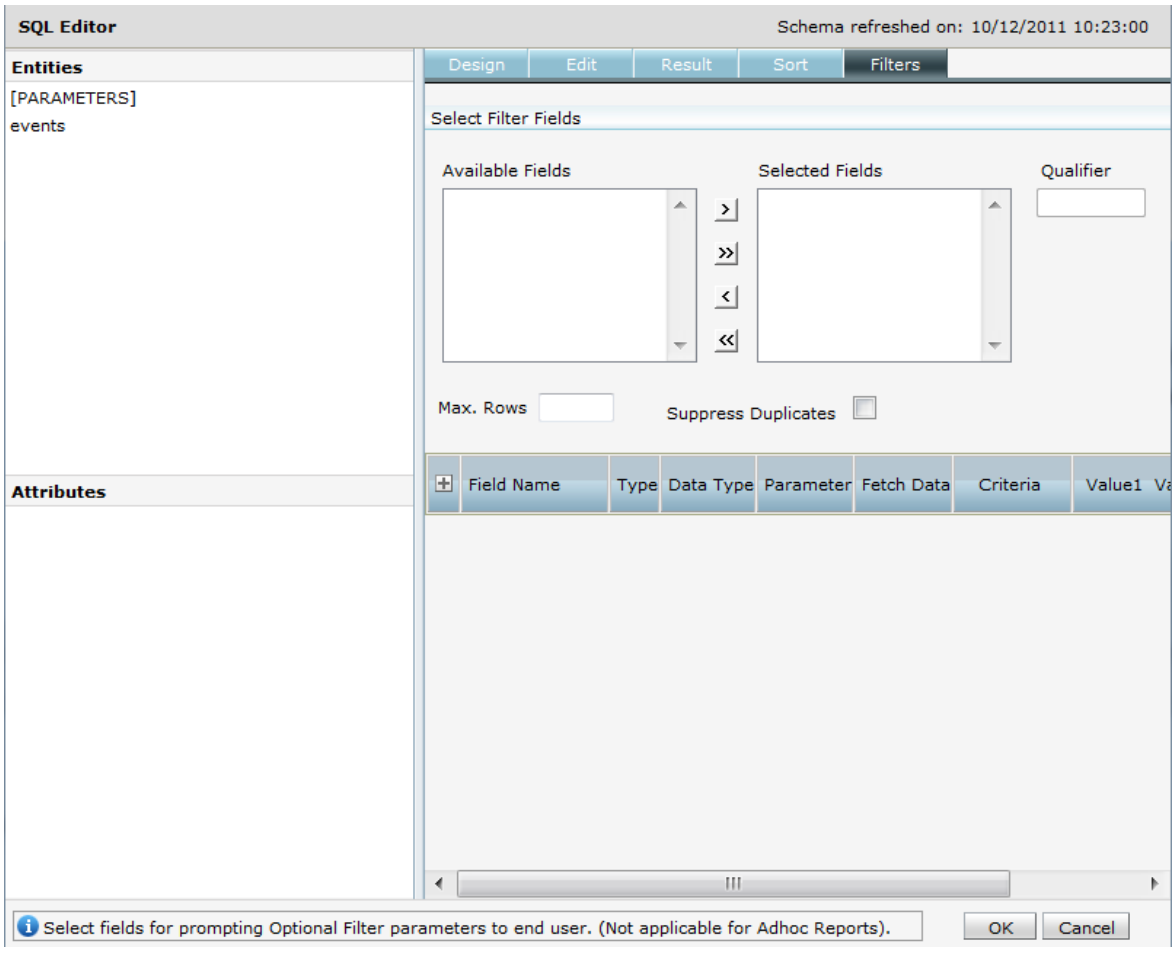
[ソート (Sort)] タブのオプション (続き)

フィールド	説明
強制並べ替えをオフ (Disable Forced Sorting)	データベースサーバーから送信されたデータをユーザーが並べ替えられないようにする場合、このボックスをオンにします。

[フィルター (Filter)] タブ

クエリにフィルターを追加するには、**[フィルター (Filter)]** タブをクリックします。レポートの実行時に1つ以上のオプションパラメーターを表示する必要があり、複数選択のコンボボックスを使用してユーザーまたはレポートデザイナーにパラメーターを選択させる場合、このタブは便利です。

SQLエディタ: [フィルター (Filter)] タブ



先頭に行を追加するには

カラムヘッダーの左端の ⊞ ([フィルタを作成する]) をクリックします。先頭に行が挿入されます。

現在行の下に行を追加するには

条件行の追加先となる上の行の ([フィルタを作成する]) をクリックします。現在行の下に行が挿入されます。

条件を削除するには

フィルターを削除する条件の横の ([このフィルタを削除]) をクリックします。

フィルターを指定するには

フィールド名と関連パラメーターを以下の説明に従って指定します。

フィールド	説明
フィールド	フィルター処理するフィールド。
タイプ	フィルタータイプを設定します。 • ユーザーが実行時に指定するパラメーター値と(等しいかどうかを)比較する場合、**[使用するパラメータ]** を選択します。 • 実行時にユーザーが条件タイプを選択できるようする場合、**[ad hoc]** を選択します。
データ型	パラメーターのデータ型を設定します。 • CHAR • NUMBER • DATE
パラメータ (Parameter)	[パラメータ (Parameter)] ドロップダウンボックスで、このフィルターに使用するパラメーターを選択します。
データを取得	**[データを取得 (Fetch Data)]** が選択 (チェック) されている場合、実行時にパラメーターフォームがユーザーに表示される前に、レポートサーバーがデータをあらかじめ取得します。

パラメーター

レポートは、あらかじめ作成されたクエリオブジェクトを実行してデータを取得します。レポートの実行時に値が必要なクエリは、組み込みの実行時パラメーターを使用します。レポートの実行時に、レポートを実行するための前提条件として、ユーザーは実行時パラメーターの値を入力するよう求められます。その後、ユーザーがそれらのパラメーターに対して入力した値に基づいて、レポートが生成されます。

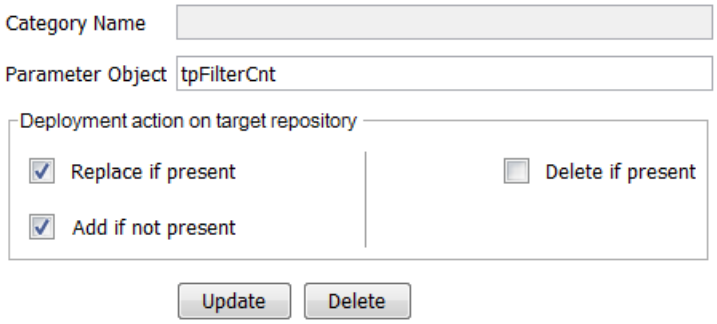
パラメーターはサーバーに格納されるため、1つ以上のレポートとクエリオブジェクトで使用できます。

注: まず必要なパラメーターオブジェクトをすべて作成してから、それらのパラメーターオブ

ジェクトを使用するクエリオブジェクトを作成することをお勧めします(クエリの作成については、「クエリ」(262ページ)を参照してください)。

パラメータープロパティ

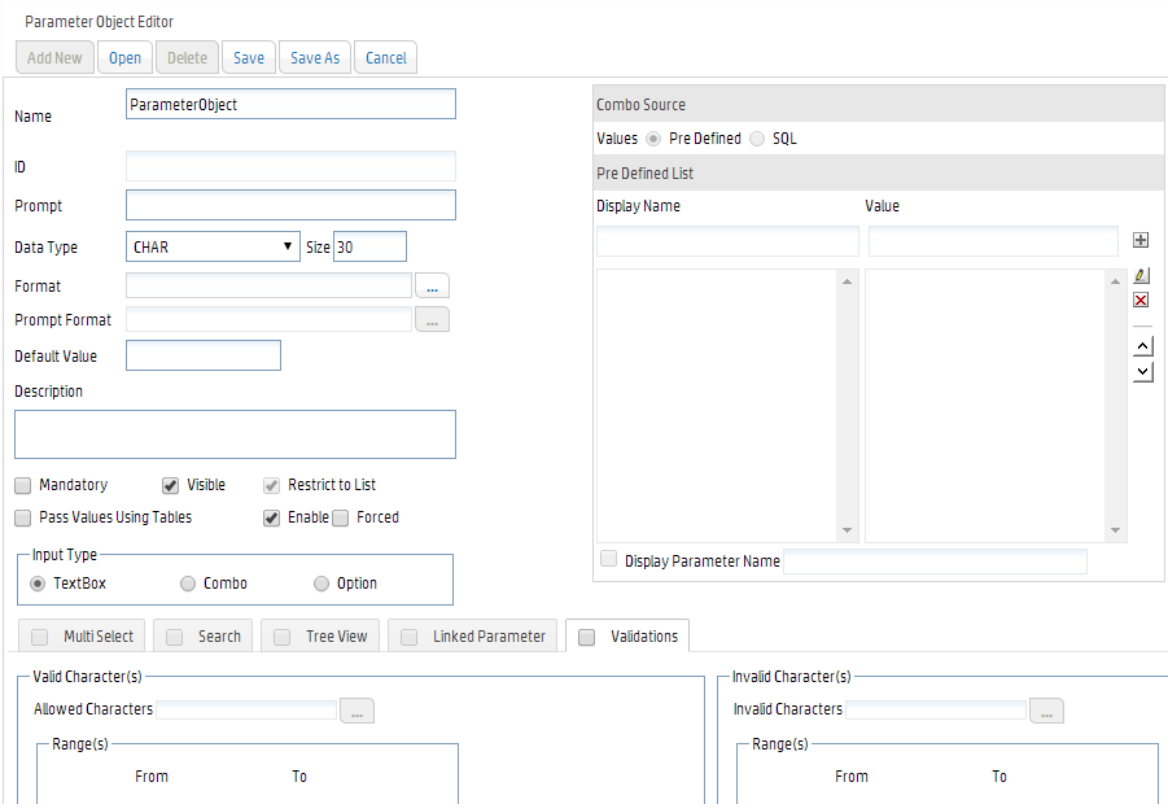
[iPackager] ページのナビゲーションツリーでパラメーターをクリックすると、以下のプロパティページが表示されます。



[Parameter Object] ボックスには、レポートサーバーにあるパラメーターオブジェクトの名前があらかじめ設定されます。パラメーターオブジェクト名は変更できます。ここで名前を変更すると、パラメーターオブジェクトは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

パラメーターオブジェクトエディター

Loggerレポートパラメーターを表示および操作するには、レポートの左ペインで **[デザイン]** の下の **[パラメータ]** をクリックするか、**[エクスプローラー]** をクリックしてカテゴリをクリックし、パラメーターを選択し、**[パラメータの詳細を編集]** ボタンをクリックしてパラメーターオブジェクトエディター(Parameter Object Editor)を開きます。



パラメーターの新規作成

新しいパラメーターを作成するには

1. [パラメータオブジェクトエディタ (Parameter Object Editor)] で、左上にある **[新規作成 (Add New)]** ボタンをクリックします。
2. 新しいパラメーターの値を指定します(詳細は以降のトピックで説明します)。

   注意: パラメーター名は、システム内のすべてのパラメーター中で一意である必要があります。

3. 必要なすべての値を入力した後、**[保存 (Save)]** をクリックします。
4. パラメーターが [パラメータ] リストに追加されます。

   注: このページを開いたとき、空のパラメーターオブジェクトが表示され、ツールバーの **[新規作成 (Add New)]** ボタンは、空のパラメーターオブジェクトを保存するまで無効になります。保存後、**[新規作成 (Add New)]** をクリックして新しいパラメーターオブジェクトを追加できます。

パラメーター名、データ型、デフォルト値の設定

以下の表に示すように、パラメーターの一意のID、表示名、データ型、サイズ、フォーマット、デフォルト値を指定します。

パラメーター名、データ型、デフォルト値

オプション	説明
名前	このパラメーターを一意に識別する名前を指定します。この名前は、システム内のすべてのパラメーター中で一意である必要があります。
プロンプト	レポートの実行時にユーザーに表示されるパラメーター名。
データ型	レポートの実行時にユーザーが指定する必要がある値の種類を指定します。 • CHAR - 値には、アルファベット、数字、特殊文字を使用できます。 • NUMBER - 値には、数字と小数点を使用できます。 • DATE - 日付または日付の一部 (日、月、年など) • BOOLEAN (詳細については、「ブールパラメーターの設定」(297ページ)を参照してください)。
サイズ	このパラメーターに指定できる文字数または桁数を指定します。 **注:** これは、データ型CHARおよびNUMBERのみに適用され、BOOLEANまたはDATE型のパラメーターには適用されません。
形式	ユーザーがこのパラメーターの値を指定する際の適切なフォーマットを選択します。...をクリックして**[データ形式]**ダイアログボックスを開きます。選択したフォーマットに基づいて、フォーマット文字列が入力ボックスに表示されます。
デフォルト値	レポートの実行時にこのパラメーターで使用する、ほとんどの場合に適切なデフォルト値を指定します。 デフォルト値は、レポートの実行時に自動的に選択されます。ユーザーは、必要に応じてデフォルト値を変更できます。ユーザーがデフォルト値を変更しなかった場合、レポートはこのパラメーターに対してここで指定したデフォルト値を使用して実行されます。

日付型パラメーターのデフォルト値

日付型のパラメーターでは、**[デフォルト値]**フィールドにプルダウンメニューとカレンダーが表示されます。カレンダーアイコン をクリックして明示的な日付を指定するか、以下の動的な変数値をプルダウンメニューから選択します。

- CURRENT_DATE
- MONTH_START_DATE
- YEAR_START_DATE

上記3つの動的可変日付のいずれかからの相対的なデフォルト日付を設定することもできます。

たとえば、CURRENT_DATEの3日後としてデフォルト値を設定するには、
CURRENT_DATE + 3を指定します。

MONTH_START_DATEの5日前としてデフォルト値を設定するには、
MONTH_START_DATE - 5を指定します。

動的変数に相対的な値を指定するには、いずれかの動的変数を選択し、相対的な値を計算する式として「+」または「-」と数値を[デフォルト値]フィールドに入力します。

レポートの実行時に、「Date」フォーマットのパラメーターには、ここで設定したデフォルト日付が表示されます。

入力タイプの定義

パラメーターの入力タイプは、レポートの実行時にユーザーに表示される、このパラメーターの値を入力するインターフェイスのスタイルを記述します。後述するように、**[テキストボックス]**、**[ドロップダウン形式]**、または **[オプション]** から選択します。

注: レポートデザイナで、パラメータータイプTextBoxを別のタイプに変更すると、エラーが発生します。パラメータータイプをTextBoxに変更する必要がある場合は、既存のパラメーターを編集せずに、そのパラメーターを削除して新しいパラメーターを追加してください。

入力タイプ

オプション	説明
テキストボックス	ユーザーにパラメーターの値を入力させる場合は、**テキストボックス**入力タイプを選択します。
ドロップダウン形式	ユーザーに、プルダウンから1つまたは複数の値を選択させるには、**[テキストボックス]** を選択します。 ユーザーがボックスから複数の値を選択できるようにするには、**[複数選択]** チェックボックスをオンにします。 このオプションの他の項目の設定については、「複数のデフォルト値の設定」(299ページ)を参照してください。
オプション	ユーザーに、オプションとして表現された値を選択させるには、**[オプション]** を選択します。 値オプションをチェックボックスの形で表示するには、**[複数選択]** チェックボックスをオンにします。 オプションをラジオボタンの形で表示するには、**[複数選択]** チェックボックスをオフのままにします。

複数のデフォルト値の設定

ドロップダウン形式入力タイプを選択した場合 (「入力タイプの定義」(296ページ)を参照)、パラメーターエディターで以下の設定を定義する必要があります。

- 選択可能最大値: パラメーターで選択または指定できる値の最大数を指定します。
- 囲い文字: 値のセットを囲むために使用する文字を指定します。これはデータベースによって変わります。
- セパレータ: 2つの値を区切るために使用する文字を指定します。これはデータベースによって変わります。
- デフォルト値の選択: レポートの実行時に表示するデフォルト値の数を指定します。以下のいずれかを選択できます。
  a. 選択済み: 選択したパラメーターの値のみが表示されます。
  b. すべて: すべてのパラメーターの値が表示されます。
  c. なし: デフォルト値は定義されません。

ブールパラメーターの設定

ブールデータ型のパラメーターは、ユーザーにチェックボックス (入力タイプ) として表示され、次の2つの状態のみを持ちます。

- Checked (実行時に選択)
- Unchecked (実行時に選択解除)

ブールパラメーターを設定するには

1. **[データ型]** で [ブール] を選択します。
2. **[値]** 領域で以下のオプションを選択します。
   a. **Checked**: ユーザーが実行時にこのオプションを選択する場合に渡す値を指定します。
   b. **Unchecked**: ユーザーが実行時にこのオプションを選択しない場合に渡す値を指定します。

実行時の各種動作の設定

レポート実行時のパラメーターの表示と動作方法についての、各種のオプションを指定できます。これらのオプションは一般に入力タイプに関係し、入力可能なユーザー入力値や、パラメーターの表示/非表示、検索可能な値などを定義します。

パラメーターオプション

オプション	説明
必須	レポート実行時にこのパラメーターに値を指定することをユーザーに義務付ける場合はこのチェックボックスをオンにします。
表示	レポート実行時にこの入力フォームにパラメーターを表示する場合はこのチェックボックスをオンにします。 このパラメーターの値が別のレポートから設定される場合や、あらゆる場合にパラメーターのデフォルト値を使用するときは、選択解除されたままにします。
リストに限定	この設定は、[入力タイプ] が **[ドロップダウン形式]** のパラメーターに適用されます。**[リストに限定]** チェックボックスは、選択可能な実行時オプションのみにパラメーター値のユーザー入力を制限する場合にオンにします。 ここで作成するパラメーター定義で **[リストに限定]** がオフの場合、ユーザーは値を指定できるか、選択可能なオプションから値を選択できます。
テーブルを使用しているパス値	この設定は **[複数選択]** に適用されます。このチェックボックスは、テーブルを通じてパラメーター値を渡す場合にオンにします。この方法は、特にSQLで渡すことができる値の数 (選択された値の合計バイト数) が許容範囲を超えている場合に使用します。
有効にする	
強制	パラメーター値を、あらかじめ指定された値のリストに制限する場合は、このチェックボックスをオンにします。

データソースリストの設定

チェックボックス、**ドロップダウン形式**、および**オプション**入力タイプの値を指定します。値は必ずあらかじめ定義します。

定義済みの値を設定するには

1. **[ディスプレイの名前]** フィールドで、実行時にユーザーに表示する値を指定します。
2. **[値]** フィールドで、フィルターとして渡す値を指定します。
3. ⊞ (**[追加する]**) をクリックして、表示名をリストに追加します

   (リストからオプションを削除するには、値を選択して ✕ をクリックします)。
4. それぞれのオプションについて上記の手順を繰り返します。
5. ユーザーが、レポート上のコントロールとしてパラメーターを追加できるようにする場合は、**[パラメータ名を表示]** チェックボックスをオンにします。

   [パラメータ名を表示] フィールドを選択すると、レポートで使用するために選択できるパラメーター表示名が自動的に設定されます。レポート上に表示される名前は、**[プロンプト]** フィールドで指定されたものになります。

> **ヒント: [パラメータ名を表示]** の設定は、パラメーターオブジェクトがアドホックレポートで使用される場合は無効です。

複数のデフォルト値の設定

ドロップダウン形式入力タイプを選択した場合 (「入力タイプの定義」(296ページ)を参照)、パラメーターエディターで以下の設定を定義する必要があります。

- 選択可能最大値: パラメーターで選択または指定できる値の最大数を指定します。
- 囲い文字: 値のセットを囲むために使用する文字を指定します。これはデータベースによって変わります。
- セパレータ: 2つの値を区切るために使用する文字を指定します。これはデータベースによって変わります。
- デフォルト値の選択: レポートの実行時に表示するデフォルト値の数を指定します。以下のいずれかを選択できます。
  a. 選択済み: 選択したパラメーターの値のみが表示されます。
  b. すべて: すべてのパラメーターの値が表示されます。
  c. なし: デフォルト値は定義されません。

パラメーターの変更

パラメーターを変更するには

1. **レポート**の右パネルメニューで、**[パラメータ エクスプローラ]**をクリックして [パラメータオブジェクト] リストを表示します。
2. 変更するパラメーターを参照します。
3. **[アクション]**メニューで、**[パラメータの詳細を編集]**をクリックします。
4. パラメーターに必要な編集を行い (「パラメーターの新規作成」(294ページ)で説明している設定を使用します)、**[保存]**をクリックします。

注: 変更できるのはカスタムパラメーターのみであり、提供されているパラメーターは変更できません。提供されているパラメーターは、システムのReports and Solutionパックアドオンで使用するうえで必要なためです。

パラメーターの削除

パラメーターを削除するには

1. **[レポート]**の左パネルで、**[パラメータ エクスプローラ]**をクリックして [パラメータ・オブジェクト・リスト] を表示します。
2. 変更するパラメーターを参照します。
3. **[アクション]**メニューで、**[削除]**をクリックします。
4. **[はい]**をクリックして削除を確定します。

注: 削除できるのはカスタムパラメーターのみであり、提供されているパラメーターは変更できません。提供されているパラメーターは、基盤となるReports and Solutionパックアドオンで使用するうえで必要なためです。

パラメーター値グループ

一部のレポートでは、国リストのように、実行時の値を複数指定する必要があります。長いリストから多くの国名を選択することは困難です。この問題に対処するために、パラメーター値グループを作成して、複数のパラメーターを含むグループをユーザーに選択させることができます。

パラメーター値グループの例

- 南北アメリカ (北アメリカ亜大陸の国々)
- ヨーロッパ (ヨーロッパの国々)
- アジア (アジアの国々)
- アフリカ (アフリカの国々)

実行時にユーザーがグループを選択すると、そのグループに属する複数の値が選択された状態で表示されます。ユーザーは、レポートの実行のたびに各国を手動で選択する必要はありません。時間の節約とともに、エラーの削減にもつながります。

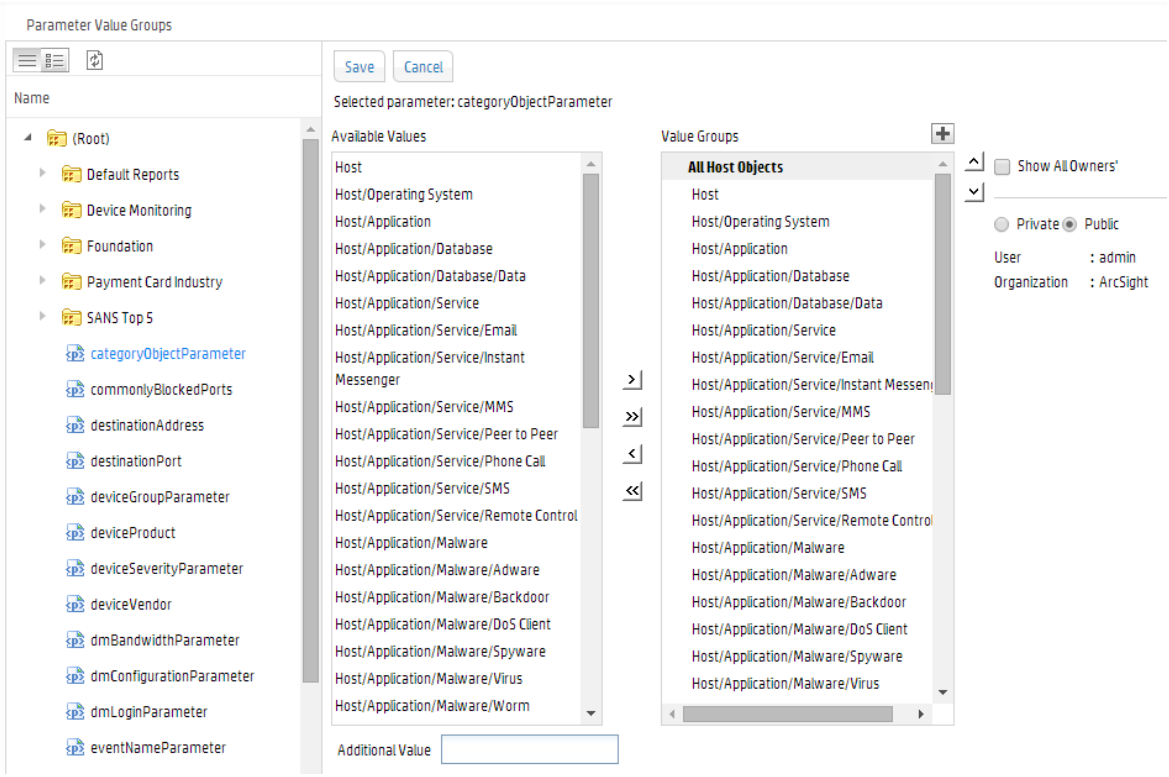
パラメーター値グループの設定

一部のレポートでは、ユーザーが実行時の値を複数指定する必要があり、グループ化することで選択が容易になる場合があります。たとえば、ユーザーが複数の国名を選択する必要があるレポートは、パラメーター値グループの適切な候補となります。1つの長い国名リストから複数の国名を選択するのは難しい可能性があります。

代わりに、クエリの設計者は、南北アメリカ、ヨーロッパ、アジア、アフリカなどのパラメーター値グループを作成することが考えられます。各パラメーター値グループには、それらの大陸または地域に属する国のリストを含めます。レポートの実行時に、ユーザーがグループを選択すると、そのグループに属する複数の値が事前に選択されています。レポートを実行するたびにパラメーターグループで手動で国を選択する必要はありません。選択内容は、あるレポート実行と次のレポート実行の間で保存されます。

クエリ設計戦略の一部としてパラメーター値グループを使用することで、レポート実行時の時間が節約され、間違いが減ります。

Loggerレポートパラメーター値グループを表示および操作するには、Reportsの左パネルで、**[デザイン]** の下の **[パラメータ値グループ]** をクリックします。



次の表で、**[パラメータ値グループ (Parameter Value Groups)]** ページのオプションについて説明します。

パラメーター値グループ

オプション	説明
名前 (Name)	すべてのパラメーターオブジェクトを一覧表示します。
利用可能な値 (Available Values)	選択したパラメーターで使用できる値を一覧表示します。
値グループ (Value Groups)	作成したグループと、グループ内で選択された値を一覧表示します。プライベートグループの左にはアイコンが表示されます。
全ての所有者のダッシュボードを表示 (Show All Owners)	オンにした場合、すべてのユーザーが作成したグループが表示されます。
オプションボタン: プライベート (Private) パブリック (Public)	自分専用に設定したグループを一覧表示するには **[プライベート (Private)]** を選択します。 全員に対して設定したグループを一覧表示するには **[パブリック (Public)]** を選択します。

グループを作成するには

1. **[値グループ (Value Groups)]** ボックスの横にある ([グループの挿入]) をクリックします。グループが作成され、[値グループ (Value Groups)] の下にデフォルトの名前 (パラメーター

リストで現在選択されているパラメーターが基になります) で表示されます。

2. [値グループ (Value Groups)] リストで、必要に応じて新しいグループ名を編集します(すでに編集モードになっていなければ、編集するには名前をダブルクリックします)。設定するには再度名前をダブルクリックするか、ボックスの外側をクリックします。
3. グループの値を追加するには、**[利用可能な値 (Available Values)]** リストで値を選択し、  ([選択されたグループに値を追加]) ボタンをクリックします。選択した値が [値グループ (Value Groups)] リストで選択されているグループに追加されます。
4. グループに追加する各値に対して、以上の手順を繰り返します。

   グループに追加する値が [利用可能な値 (Available Values)] リストに表示されていない場合は、**[追加の値 (Additional Value)]** フィールド ([利用可能な値 (Available Values)] の下) で値を指定し、Returnキーを押します。カスタム値が現在選択されているグループに追加されます。

   [値グループ (Value Groups)] 内で選択されているグループにすべての値を追加するには、[利用可能な値 (Available Values)] を選択して  をクリックします。選択した値を [値グループ (Value Groups)] から削除するには  をクリックします。すべての値を [値グループ (Value Groups)] ボックスから削除するには  をクリックします。

   選択したグループを上下に移動するには、グループを選択し、上  および下  矢印をクリックします。選択した値を上下 (グループ内) に移動するには、値を選択し、上  および下  矢印をクリックします。
5. **[保存 (Save)]** をクリックします。

   注: グループの名前をユーザーが変更した場合、そのグループに属する値はそのユーザーの設定の **[選択した値 Selected Values]** グループから削除されます。

ツリービューパラメーターを作成するには

1. リーフノードをクリックし、右矢印  ボタンをクリックします。
   - 分岐内のすべての値を選択するには (複数選択パラメーターのみ)、分岐をクリックし、  ボタンをクリックします。
   - グループ名を変更するには、グループ名をダブルクリックして編集可能にします。新しい名前を指定し、ボックスの外側をクリックします。
   - グループを削除するには、削除するグループのタイトルの  をクリックした後、**[保存 (Save)]** ボタンをクリックして変更内容を保存します。

テンプレートスタイル

Loggerレポートは、スタイルファイル (.sty) を使用して、指定した形式でレポート出力を生成します。スタイルファイルは、レポート出力のルックアンドフィール、配置、向きを定義します。

Loggerのレポートの [テンプレートのスタイル] ページから任意のスタイルファイルを変更できます。また、ニーズに合わせて新しいスタイルを定義することができます。

注: レポートレイアウトファイル (`.irl`) は、用紙サイズ、静的コントロール、レポートに含めるヘッダーとフッターなどの要素を定義します。独自のレイアウトファイルを定義できます。詳細については、「新しいテンプレートの定義」(304ページ) を参照してください。

Loggerレポートテンプレートの操作

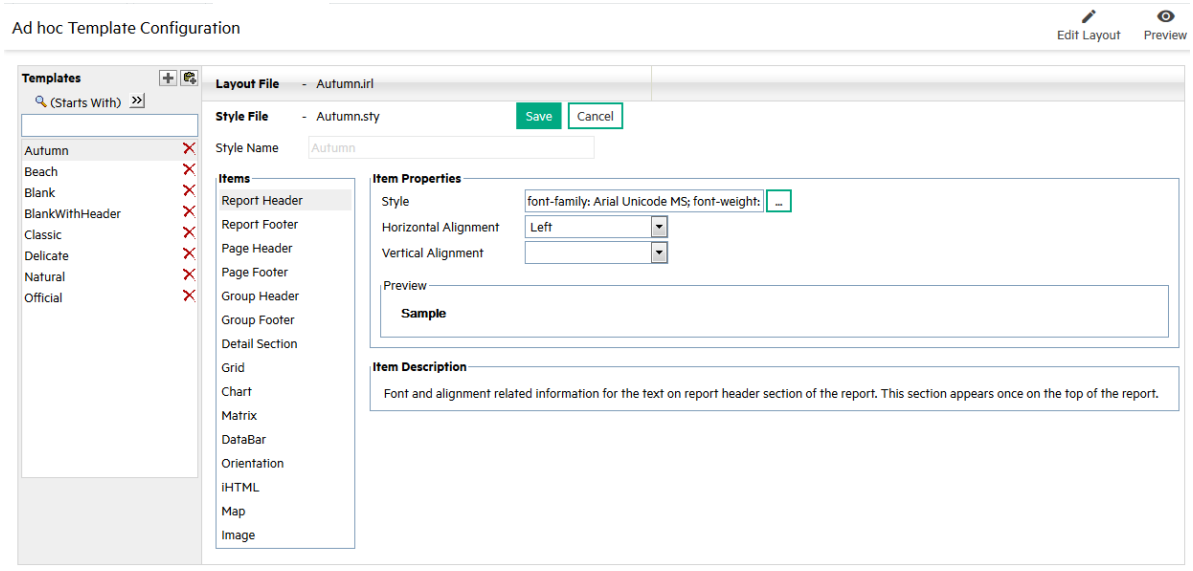
新しいテンプレートを作成する前に、ニーズを満たす既存のテンプレートがあるかどうかを確認することをお勧めします。

既存のテンプレートを検索するには

1. 以下のいずれかを実行します。
   - **[開始]** を選択: テンプレート名の最初の数文字を既存のテンプレートのリストの上にあるテキストボックスに入力します。
   - **[次の内容を含む]** を選択: テンプレート名に含まれる単語またはその一部を既存のテンプレートのリストの上にあるテキストボックスに入力します。

Loggerレポートのテンプレートスタイルを表示し、操作するには

1. [レポート] メニューの **[テンプレートのスタイル]** をクリックします。



2. 既存のテンプレートを選択するか、または新しいレイアウトを作成します。「新しいテンプレートの定義」(304ページ) を参照してください。
3. 必要な変更を加えます。
4. サンプルデータでテンプレートを表示するには、**[プレビュー (Preview)]** をクリックします。

5. **[保存 (Save)]** をクリックしてレイアウトを保存します。テンプレートが [テンプレート (Templates)] リストに表示されます。

新しいテンプレートの定義

新しいテンプレートを定義するには

1. デザイナーで、レポートの左メニューバーの **[テンプレートのスタイル]** をクリックします。
2. 右側のパネルで ⊞ アイコンをクリックします。
3. テンプレートの項目とそのプロパティを定義します。
4. レポートレイアウトファイルを定義または変更する場合は、**[レイアウトを編集]** をクリックします。「レポートにヘッダーまたはフッターを追加するには」(304ページ) を参照してください。
5. **[保存 (Save)]** をクリックします。

レポートにヘッダーまたはフッターを追加するには

1. テンプレートページ上部の **[レイアウトを編集]** をクリックします。
2. ヘッダーを追加する場合は **[レポートのヘッダー]** を、フッターを追加する場合は **[ページ・フッター]** をクリックします。
3. **[挿入] > [レイアウト・コントロール]** をクリックします。
4. サブメニューからオプションを選択し、必要な情報を入力します。

レポート管理

このセクションでは、Loggerレポートの設定と管理に関する管理プロセスについて説明します。

レポートユーザーグループの作成

複数のユーザーが類似のレポートアクセス権を必要とする場合、ユーザーグループを使用すると権限の管理が簡単になります。権限セットごとにユーザーグループを作成し、該当するグループにユーザーを追加するだけです。詳細については、「ユーザ/グループ」(530ページ) を参照してください。

新しいユーザーグループを作成し、Loggerのレポート権限を付与するには

1. メニューバーの **[システム管理]** をクリックします。
2. 左パネルの [ユーザ/グループ] セクションにある **[ユーザ管理]** をクリックします。
3. **[グループ]** タブを開き、**[追加]** をクリックします。
4. グループの名前を入力し、説明を追加します。
5. [グループタイプ]ドロップダウンメニューから **[Loggerレポート]** を選択します。
6. 矢印をクリックしてLoggerレポート権限の一覧を表示します。
7. **[すべてをクリア]** をクリックしてすべての許可を削除します。
8. ユーザーグループに付与する各許可の横のボックスをクリックします。

   たとえば、[Foundation] > [侵入モニタリング] > [Attackers] のレポートに対する表示、実行、スケジュール権限を付与する場合、以下の各アクセス権限の横にあるボックスをオンにします。

   ```
   Report folder [Attackers]: view, run, and schedule reports
   Report folder [Foundation]: view, run, and schedule reports
   Report folder [Intrusion Monitoring]: view, run, and schedule reports
   ```

9. **[メンバーシップの保存および編集]** をクリックします。
10. **[グループ メンバーシップの編集]** ダイアログで **[追加]** をクリックします。
11. グループに追加するユーザーのボックスをマークし、**[OK]** をクリックします。
12. 作成したグループのメンバーとしてログインし、目的の機能を実行できるかどうかをテストします。たとえば、ユーザーは、Attackersレポートのみを表示、実行、スケジュールできる必要があります。

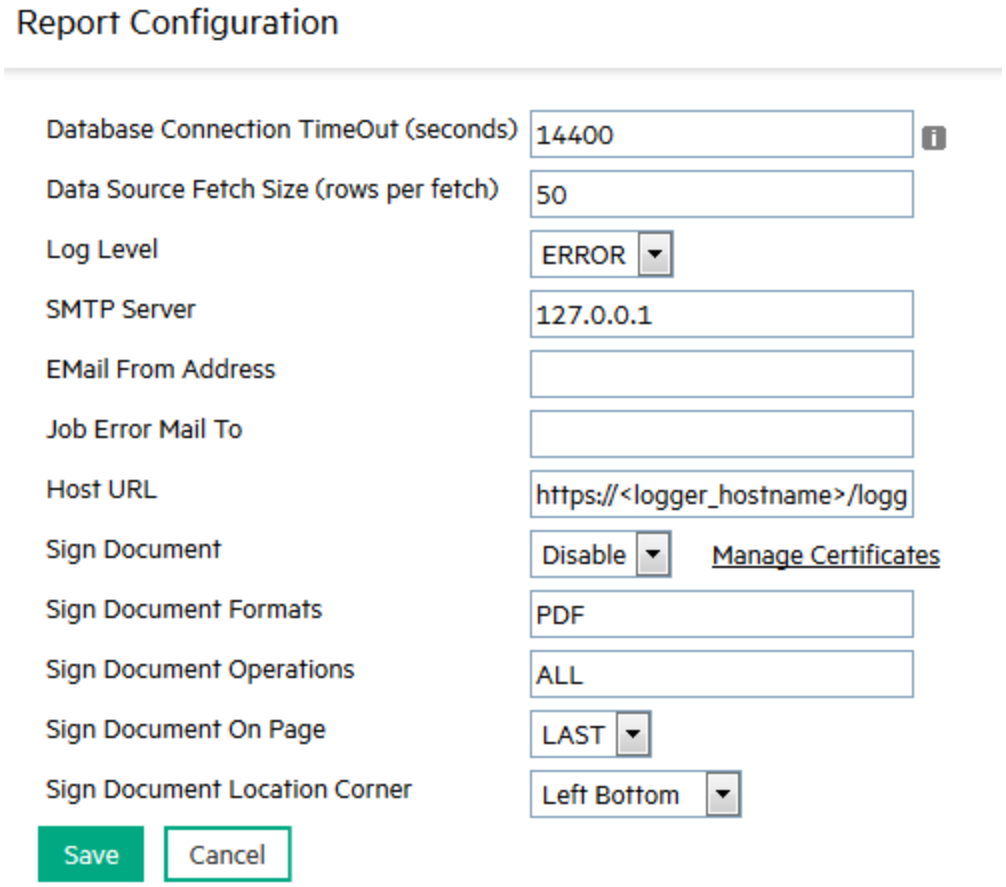
レポートサーバーの設定

Loggerレポートには、レポートサーバーのデフォルト設定が用意されています。レポートサーバーを変更しない場合、レポートはデフォルトの設定で実行されます。

レポートの設定

レポートサーバーの設定を表示または変更するには

1. ナビゲーションバーの **[レポート]** をクリックします。
2. [レポート] メニューの [管理] セクションで **[レポートの設定]** をクリックします。**[レポートの設定 (Report Configuration)]** ダイアログが表示されます。



3. レポート設定の入力が完了したら、**[保存 (Save)]** をクリックします。

次の表では、レポートの設定について説明します。

レポートの設定

オプション	説明
データベース接続タイムアウト (秒)	データベース接続が使用されていない状態が続いたときに接続を閉じるまでの時間 (秒単位)。 有効な値は、ゼロよりも大きな任意の整数です。 デフォルト値: **14400** 例: `DATABASE_CONNECTION_TIMEOUT`に50を設定すると、レポートサーバーとデータベースサーバーの間で50秒間通信が行われないと、レポートサーバーはデータベースへの接続を閉じます。
Data Source Fetch Size (rows per fetch)	データソースから一度に (1回の「読み取り」で) フェッチするレコード数を指定します。 有効な値は任意の正の整数です。 デフォルト値: **50** 例: `DATA_SOURCE_FETCH_SIZE=50`

レポートの設定 (続き)

オプション	説明
ログレベル	ログ記録の対象とする緊急度を設定します。 有効な値は、DEBUG、INFO、WARN、ERROR、FATALです。 デフォルト値: **ERROR** 例: LOG_LEVEL=ERROR
SMTPサーバー	スケジュールレポートをメール送信するために使用されるサーバーのIPアドレスまたはドメイン名 (IPまたはURL)。通知やレポート配信など、すべてのメール通信は、Loggerのレポート機能により、このメールサーバーを使用して送信されます。 例: SMTP_SERVER=127.0.0.1 LoggerのSMTP設定については、「SMTP」(500ページ)を参照してください。
電子メール-受信アドレス	Loggerレポートシステムから送信する電子メールの送信元アドレスを設定します。 例: loggeradmin@companyxyz.com
ジョブ・エラー・メール送信先	ジョブエラーメッセージが生成された場合に、それを受信するメールアドレス。複数のアドレスを指定するには、カンマで区切ります。
ホストのURL	Loggerレポートメールの一部として送信されるホストURL (Loggerアプリケーションの URL)。 構文: HOST_URL=[ホストURL](文字列) デフォルト値: **https://<logger_hostname>/logger/report** 例: HOST_URL=https://loggerA.xyz.com/logger/report
Sign Document	レポートのデジタル署名を有効または無効にします。オプションは [有効にする] と [無効にする] です。 デフォルトは、**[無効にする]** です。 適切な権限を持つ管理者は、シグネチャファイルのブラウズとアップロードが可能です。これは、グローバル、組織、またはユーザーレベルで行うことができます。[Sign Document] プロパティが有効な場合、これらのシグネチャがドキュメントに適用されます。「証明書」(423ページ)を参照してください。
Sign Document Formats	現在、シグネチャをサポートする形式は **[PDF]** のみです。

レポートの設定 (続き)

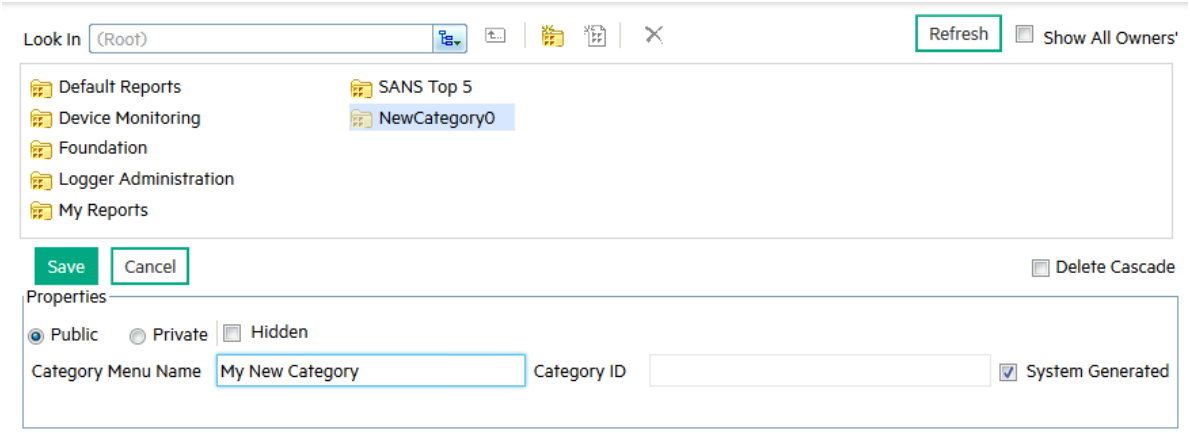
オプション	説明
Sign Document Operations	シグネチャを適用するレポートオペレーションのタイプを入力します。オプションは、[表示]、[電子メール]、[公開する]、[アップロード]、[印刷]、または [すべて (ALL)] です。 デフォルトは **[すべて (ALL)]** です。
Sign Document on Page	シグネチャを表示するページを選択します。オプションは [First] と [Last] です。 デフォルトは **[Last]** です。
Sign Document Location Corner	シグネチャを表示するページコーナーを選択します。オプションは [Right Top]、[Right Bottom]、[Left Top]、[Left Bottom] です。 デフォルトは **[Left Bottom]** です。

レポート カテゴリ

レポート、クエリ、パラメーターをカテゴリの下に整理して保存し、簡単にアクセスすることができます。カテゴリを自分で作成することも、既存のカテゴリのプロパティを編集することもできます。

[レポート カテゴリ] ページを開くには

1. [レポート] メニューの [管理] セクションから **[レポート カテゴリ]** をクリックします。



各カテゴリのオブジェクトには、レポートのエクスプローラーからアクセスすることができます。「レポート エクスプローラー」(171ページ) および「長いレポートをバックグラウンドでの実行に限定する方法」(194ページ) を参照してください。

システム定義のカテゴリ

共通の利用分野に基づき、システムにはいくつかのカテゴリがあらかじめ定義されています。**[Default Reports]** カテゴリは、ユーザー作成レポート用です。その他のカテゴリにはあらかじめレポートが定義されており、すぐに使用できます。各カテゴリのレポートの完全な一覧については、レポート エクスプローラでカテゴリにアクセスしてください。

Default Reports

ユーザー生成レポートは、このカテゴリに配置されます。

Device Monitoring

このカテゴリには、以下のサブカテゴリが含まれています。

- Anti-Virus: このカテゴリは、ウイルス対策の更新ステータス、時間ごとのウイルス活動、感染している上位のシステムなど、ウイルス対策処理に関する情報を提供するレポート、クエリ、パラメーター、ダッシュボード、ダッシュボード ウィジェットを格納するために使用します。
- CrossDevice: これらのレポートは、複数の種類のデバイスに適用される機能に関する情報を提供します。たとえば、失敗したログイン試行、ホストごとの帯域幅使用量、ユーザーが作成したアカウントなどです。
- Database: このカテゴリのレポートは、データベースのエラーと警告に関する情報を提供します。
- Firewall: これらのレポートは、ファイアウォールの活動に関する情報を提供します。たとえば、ポート、アドレス、時間ごとの拒否された接続などです。
- Identity Management: このレポートは、ネットワーク内のアイデンティティマネジメント デバイスによって報告された、ユーザーごとの接続数に関する情報を提供します。
- IDS-IPS: これらのレポートは、侵入検知システム (IDS) と侵入防止システム (IPS) に関する活動についての情報を提供します。たとえば、デバイス、ポート、重大度ごとのアラート数、上位のアラート通知先、ワームに感染したシステム、関連する測定値などです。
- Network: これらのレポートは、ネットワークインフラストラクチャーに関する活動についての情報を提供します。たとえば、インターフェイスステータス、デバイスエラー、SNMP認証失敗などです。
- OS: これらのレポートは、オペレーティングシステムに関する活動についての情報を提供します。たとえば、ユーザーごとのログインエラー、ユーザーとユーザーグループの作成、変更イベントなどです。
- VPN: これらのレポートは、VPN接続に関する活動についての情報を提供します。たとえば、認証エラーや、接続数、アドレスごとの許可および拒否、関連測定値などの接続情報です。

ヒント: これ以外にも、HPEカスタマーサポート サイト (SSO)からレポート パッケージとしてレポートをダウンロードできます(レポート パッケージの展開については、「レポート バンドル

の展開」(325ページ) を参照してください)。

Foundation

このカテゴリには、以下のサブカテゴリが含まれています。

- Configuration Monitoring: Loggerには、設定監視を行うためのレポートが用意されています。
- Intrusion Monitoring Reports: Loggerには、侵入監視を行うためのレポートが用意されています。

  たとえば、パスワード変更、ファイアウォール設定イベント、ファイアウォールトラフィック、ファイアウォールを突破した上位の攻撃者などのレポートが提供されます。
- Intrusion Monitoring Reports: Loggerには、侵入監視を行うためのレポートが用意されています。

  たとえば、パスワード変更、ファイアウォール設定イベント、ファイアウォールトラフィック、ファイアウォールを突破した上位の攻撃者などのレポートが提供されます。
- NetFlow Monitoring: ネットフロー監視レポートは、IPトラフィック情報を報告します。
- Network Monitoring Reports: ネットワーク監視レポートは、仮想プライベートネットワークに関する活動を示します。

Logger Administration

このカテゴリには、[Daily Byte Count] などのLogger管理タスクが含まれています。

SANSトップ5レポート

Loggerには、SANSトップ5ログレポートシナリオに対処するレポートが用意されています。すべてあらかじめ構築され、オンデマンドで実行したり、指定した頻度でスケジュールできます。

SANS Instituteは、共同のトレーニング、認定、研究組織であり、さまざまな潜在的脅威に対して情報セキュリティを高めるためのソリューションを開発することに注力しています。SANSは、世界中のさまざまな業界および分野の多数のセキュリティ実践者の共同作業を促進および支援し、情報セキュリティに関連する経験、ソリューション、リソースを共有します。

注: SANSは、SysAdmin、Audit、Network、Securityの略です。詳細については、Webサイトhttp://www.sans.org/を参照してください。

SANSトップ5は、セキュリティコミュニティの幅広い側面に対し、最新の最も重大なログレポートのセットを表しており、定期的に確認することをお勧めします。SANSのWebサイトからの次の引用は、SANSトップ5基本ログレポートの戦略と焦点を説明しています。

「目標は、疑わしい活動を最も高い確率で識別できるレポートを含める一方で、最も少ない数の擬陽性のレポートエントリを生成することです。ログレポートは、侵入の程度を必ずしも

明確に示していない場合がありますが、適切な管理者に対し、少なくとも疑わしい活動が検出され、さらなる調査が必要であるという十分な情報を提供します」。

SANSトップ5ログレポートは、以下の5つのシナリオを網羅しています。

- 1 - 既存のアカウントを通じたアクセスの試み
- 2 - ファイルまたはリソースアクセスの失敗した試み
- 3 - ユーザー、グループ、およびサービスの許可されない変更
- 4 - 攻撃に対して最も脆弱なシステム
- 5 - 疑わしいか許可されていないネットワークトラフィックパターン

SANSトップ5ログレポートの完全な説明については、www.sans.org/resources/top5_logreports.pdfを参照するか、SANSのWebサイトにあるリソースで関連するトピックを探してください。

これらの脅威シナリオに対処するために提供されるLogger SANSトップ5レポートは以下のとおりです。

- SANS Top 5 - 1 Number of Failed Logins
- SANS Top 5 - 1 Top Users with Failed Logins
- SANS Top 5 - 2 Failed Resource Access by Users and Drilldown
- SANS Top 5 - 2 Failed Resource Access Events and Drilldown
- SANS Top 5 - 3 Password Changes
- SANS Top 5 - 3 User Account Creations, Deletions, and Modifications
- SANS Top 5 - 4 Vulnerability Scanner Logs by Host or by Vulnerability
- SANS Top 5 - 5 Alerts from IDS
- SANS Top 5 - 5 IDS Signature Destinations and Source
- SANS Top 5 - 5 Top 10 Talkers
- SANS Top 5 - 5 Top 10 Types of Traffic
- SANS Top 5 - 5 Top Destination and Target IPs
- SANS Top 5 - 1 Number of Failed Logins
- SANS Top 5 - 1 Top Users with Failed Logins
- SANS Top 5 - 2 Failed Resource Access by Users and Drilldown
- SANS Top 5 - 2 Failed Resource Access Events and Drilldown
- SANS Top 5 - 3 Password Changes
- SANS Top 5 - 3 User Account Creations, Deletions, and Modifications
- SANS Top 5 - 4 Vulnerability Scanner Logs by Host or by Vulnerability
- SANS Top 5 - 5 Alerts from IDS
- SANS Top 5 - 5 IDS Signature Destinations and Source

- SANS Top 5 - 5 Top 10 Talkers
- SANS Top 5 - 5 Top 10 Types of Traffic
- SANS Top 5 - 5 Top Destination and Target IPs

ソリューションレポート

Loggerにインストールされたすべてのソリューションパッケージは、特定のレポートグループに表示されます。ソリューションパッケージは、特定のコンプライアンス要件またはシナリオに対応しており、個別にインストールされます。ソリューションレポートは、特定のコンプライアンス要件やシナリオ向けに、Loggerに対するアドオンパッケージとして利用できます。

注: ソリューションパッケージをインストールする前に、Loggerにログインし、[レポート] ページを少なくとも1回は開く必要があります。

使用可能なソリューションパッケージには以下のものがあります。

- ITGov (ISO 27002 & NIST 800-53ベースのレポート)
- Payment Card Industry (PCIベースのレポート)
- SOX (Sarbanes-Oxleyコンプライアンスレポート)

ソリューションパッケージの展開については、「レポートバンドルの展開」(325ページ)を参照してください。展開したソリューションレポートは、[ソリューション レポート] レポートグループの下のカテゴリに表示されます。これらのレポートにアクセスするには (展開後)、左側のメニューの **[レポート] > [ソリューション レポート] > [<レポートカテゴリ名 >]** をクリックします。ここで、<レポートカテゴリ名 >は、`Payment Card Industry`などです。

レポートカテゴリの編集方法など、その詳細については、「レポートカテゴリ」(308ページ)を参照してください。

システム定義クエリまたはパラメーターのカテゴリへの配置

あらかじめ定義されたクエリまたはパラメーターをカテゴリに配置できます。そのためにはカットアンドペースト機能を使用します。カットアンドペーストでは、そのIDが保持されるためです。

クエリ/パラメーターをカットアンドペーストするには

1. [レポート] メニューの **[エクスプローラー]** をクリックします。エクスプローラーが表示されます。
2. 移動する定義済みのクエリ/パラメーターを選択します。
3. 右クリックし、コンテキストメニューから **[クエリオブジェクトを切り取り]** または **[パラメータオブジェクトを切り取り]** を選択します。
4. このクエリまたはパラメーターを配置するカテゴリ名をクリックします。

注: レポートをルートカテゴリに保存することはできません。既存のいずれかのサブカテゴリに保存するか、新たなカテゴリを作成してください。

5. 再度右クリックし、**[貼り付け]** をクリックします。

> **ヒント:** クエリまたはパラメーターをコピーしてカテゴリに配置することはしないでください。これを行うと、クエリまたはパラメーターに新しいIDが付与され、それを使用しているレポートまたは他の既存のオブジェクトで使用できなくなります。代わりに、カットアンドペーストを使用してください。

現在よりも後の日付に一度、または指定した頻度で(毎日または毎週)、レポートの実行をスケジュールできます。現時点では月次レポートをスケジュールすることはできません。詳細については、「スケジュールレポート」(185ページ)を参照してください。

あらゆる種類のレポートを実行、発行、結果を保存できます。すべてのレポートで使用できる、一般的なレポートタスクについては、「レポートの実行」(190ページ)および「公開済みレポート」(180ページ)を参照してください。

新しいカテゴリの追加

既存のレポートカテゴリを使用するのに加えて、ビジネスニーズを満たす追加のカテゴリを作成できます。

カスタムカテゴリを追加するには

1. 左ペインの **[管理]** セクションにある **[レポート カテゴリ]** をクリックします。
   [レポートとカテゴリを配布] に使用可能なカテゴリが表示されます。ページ上部のツールバーに、使用可能なアクションのボタンが表示されます。
2. **[新しいカテゴリを追加]**  をクリックします。
3. 新しいカテゴリのプロパティを定義し、**[保存]** ボタンをクリックします。

プロパティ	使用目的
パブリック	このプロパティに **[パブリック]** を設定すると、誰でもカテゴリを使用できるようになります。
プライベート	このプロパティに **[プライベート]** を設定すると、自分だけがカテゴリを使用できるようになります。
非表示	レポートエクスプローラーでこのカテゴリを非表示にするには、**[非表示]** チェックボックスをオンにします。他のエクスプローラーには表示されます。
カテゴリメニュー名	カテゴリの名前。

プロパティ	使用目的
カテゴリID	**[カテゴリID]** は、すべてのカテゴリで一意であることが必要です。デフォルトでは、カテゴリIDはシステムによって自動的に生成されます。カテゴリIDを手動で指定するには、**[生成済みシステム]** チェックボックスをオフにして、カテゴリIDを指定します。
生成済みシステム	カテゴリIDを手動で指定するには、**[生成済みシステム]** チェックボックスをオフにして、カテゴリIDを指定します。
カスケード表示を削除します	カテゴリは、空の場合のみ削除できます。カテゴリとその内容を削除するには、**[カスケード表示を削除します]** チェックボックスをオンにします。

注: いったん設定したカテゴリIDとスコープ ([パブリック]/[プライベート] オプション) は変更できません。

4. 必要に応じて、カテゴリにレポートを追加できます。そのためには、カテゴリをダブルクリックして開き、**[新しいレポートを追加]** ボタンをクリックします。[プロパティ] ボックスで以下のプロパティを定義します。

プロパティ	使用目的
パブリック	このプロパティに **[パブリック]** を設定すると、誰でもレポートを使用できるようになります。
プライベート	このプロパティに **[プライベート]** を設定すると、自分だけがレポートを使用できるようになります。
非表示	このレポートをどのダイアログとページにも表示しない場合は (レポートエクスプローラーを除く)、**[非表示]** チェックボックスをオンにします。ユーザーがレポートに直接アクセスできないようにするには、レポートを非表示にします。
レポートファイル	レポートの生成元となる既存のデータファイル。
レポート名	**[レポート名]** は、カテゴリ内で一意であることが必要です。
レポートID	レポートを実行および発行したときに、デフォルトでシステムによって自動生成される、レポートの一意のID。任意のIDを手動で入力するには、**[生成済みシステム]** チェックボックスをオフにし、**[レポートID]** フィールドにIDを入力します。
デザインモード	**[デザインモード]** 内のテキストは、レポートが、スタジオ (Webスタジオまたはデスクトップスタジオ) を使用して設計されたか、アドホックレポートウィザードを使用して設計されたかを示します。
配布タイプ	読み取り専用として展開されたレポートは、変更したり、同じ名前でアップロードすることはできません。カスタムとして展開されたレポートは、変更したり、同じ名前でアップロードすることができます。
出力フォーマット	このレポートを生成する際の**出力フォーマット**。ここで選択されなかったフォーマットは、このレポートで使用できません。
生成済みシステム	レポートIDを手動で指定するには、**[生成済みシステム]** チェックボックスをオフにして、レポートIDを指定します。

レポートカテゴリフィルター

各レポートグループには、オプションで検索グループフィルターを割り当てることができます。レポートカテゴリに検索グループフィルターを割り当てると、そのカテゴリ内のすべてのレポートが、このフィルターで返されたイベントのみを処理するようになります。

検索グループフィルターをレポートカテゴリに割り当てるには

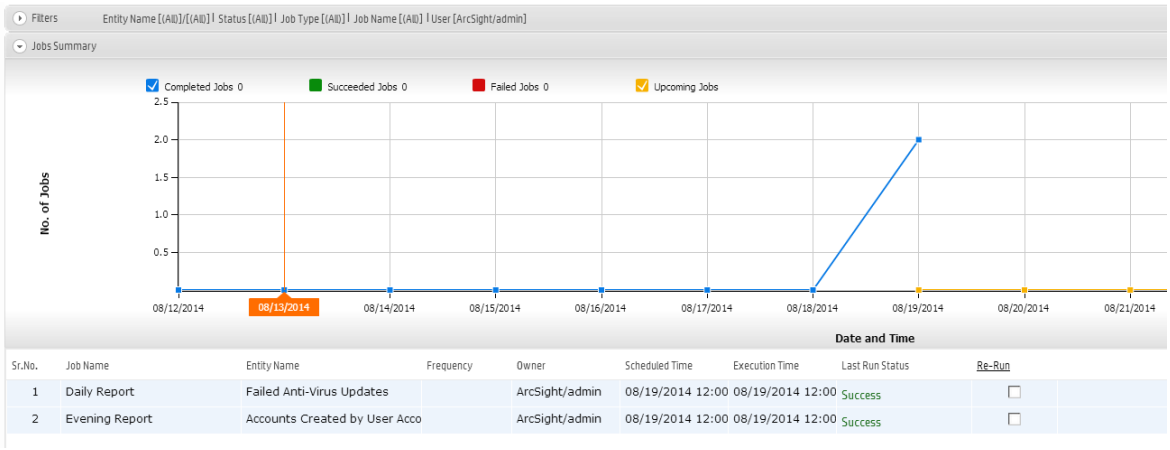
1. 特定のカテゴリ内のすべてのレポートに適用するフィルターを作成します。検索グループタイプのフィルターの作成については、「フィルター」(329ページ) を参照してください。
2. **[レポート]** ページを開きます。
3. メニューの **[管理]** の下で、**[レポート カテゴリフィルタ]** をクリックします。
4. 各カテゴリに関連付けられたプルダウンメニューに、新しい検索グループフィルターが表示されます。カテゴリごとに目的のフィルターを選択します。
5. **[保存]** をクリックします。

検索グループフィルターをレポートカテゴリから削除するには

1. **[レポート]** ページを開きます。メニューの [管理] の下で、**[レポート カテゴリフィルタ]** をクリックします。
2. フィルターを削除するレポートカテゴリに関連付けられたプルダウンメニューで、**[なし]** を選択します。
3. **[保存]** をクリックします。

ジョブ実行ステータス

[ジョブ実行ステータス] ページを表示するには、**[レポート]** ページの上部にある **[ジョブ実行ステータス]** リンクをクリックします。このページには、実行されたすべてのジョブのステータスのグラフィック表現が表示されます。このページには、**[ジョブ概要]** パネルと **[フィルター]** パネルの2つのパネルがあります。



[ジョブ概要] には、日ごとの実行ジョブ数を示すグラフが表示されます。ジョブには以下のステータスが割り当てられます。

- **完了**: 実行が完了したジョブ。
- **成功**: 完了し、成功したジョブ。
- **失敗**: 完了し、失敗したジョブ。
- **Upcoming**: このステータスは、今回のリリースでは無効です。

いずれかのジョブステータスボタン (たとえば **[失敗ジョブ]** ボタン) を選択して、そのステータスに対応するジョブをグラフに表示します。

ポップアップに表示するジョブの日付をクリックします。

[ジョブ概要] の下には、各ジョブとその詳細を表示する表があります。

[フィルター] では、ジョブ概要の結果をフィルター処理して、さまざまな条件に一致する結果を表示することができます。

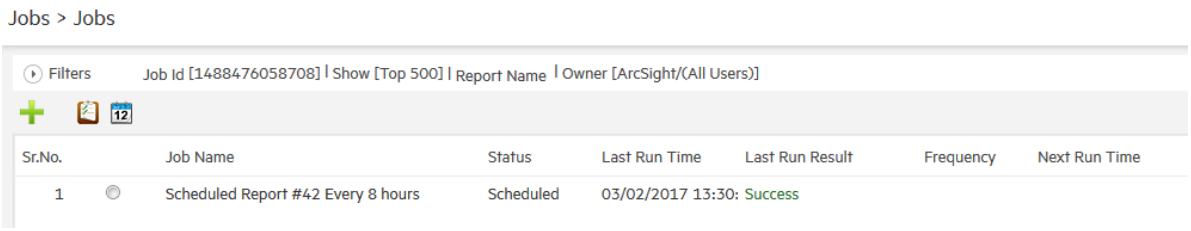
[ジョブ (Jobs)] ページ

レポートジョブ名をクリックすると、**[ジョブ (Jobs)]** ページが開き、選択したジョブに近いジョブが表示されます。このページでは以下の操作を実行できます。

- 既存のタスクとスケジュールのリスト表示
- 新しいジョブとスケジュールの作成

新しいレポートジョブまたはスケジュールの作成

1. [ジョブ実行ステータス] ページでジョブ名をクリックして、**[ジョブ (Jobs)] > [ジョブ (Jobs)]** ページを開きます。



2. ジョブとスケジュールの間で切り替えを行うには、クリップボードまたはカレンダーをクリックします。
3. をクリックして、**[ジョブ (Jobs)]** ページまたは **[スケジュール]** ページを開きます。
4. 必要なジョブの値を設定します。
5. **[保存]** をクリックします。

レポート内容のバックアップとリストア

レポートの内容と設定情報のバックアップ、復元、展開を行うことができます。CABファイルの作成にはiPackagerを、CABファイルの導入には [Deploy Report Bundler] を使用します。詳細については、「iPackagerユーティリティ」(317ページ) および「レポートバンドルの展開」(325ページ) を参照してください。

iPackagerユーティリティ

iPackagerユーティリティを使用すると、Loggerの中に存在するレポートとレポートオブジェクトをパッケージ化できます。このパッケージは、別のLoggerシステムにインポートできます。複数のLoggerがある場合、パッケージを使用してそれらのレポート機能を設定できます。この方法を使用すると、各Loggerでのレポート機能の設定は不要になります。

注: iPackagerユーティリティには管理者特権が必要です。

iPackagerユーティリティにアクセスするには

1. 上部のナビゲーションバーの **[レポート]** をクリックします。[レポート] ホームページが表示されます。
2. [レポート] メニューから **[管理]** をクリックします。[管理] メニューが表示されます。
3. メニューの下部にある **[iPackager]** をクリックします。[iPackager] ページが表示されます。

iPackagerの仕組み

まず、設定 (.conf) ファイルを作成します。このファイルには、パッケージに収容するすべてのエンティティオブジェクトの参照を収集 (インポート) できます。設定ファイルはいつでも保存し、編集することができます。.confファイルの内容が完成したら、パッケージをCABファイルにビルドで

きます。複数のレポートサーバーからデータがインポートされ、1つのCABにパッケージ化されます。

注: iPackagerで同時に開くことができる.confファイルは1つだけです。

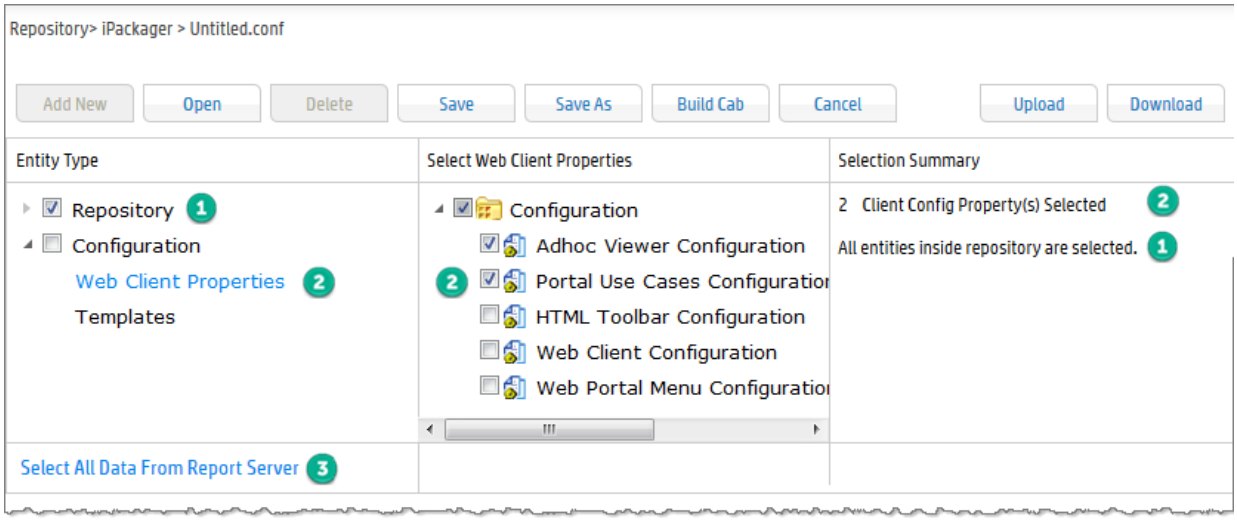
ヒント: iPackagerは、.confファイルを開くときに、.confファイルにすでにインポートされているオブジェクトの使用可否を確認します。インポート済みのオブジェクトのいずれかがレポートサーバーにない場合は、ツリービューでそのことが示されます。見つからないオブジェクトが置き換えられるまで、またはそのオブジェクトが.confファイルから削除されるまで、CABファイルはビルドできません。

iPackagerのアクション

iPackagerでは、以下のアクションを行うことができます。

アクション	説明
新規作成	新しい設定 (.conf) ファイルを作成します。
開く	既存の.confファイルをiPackagerで開きます。
削除	選択した.confファイルを削除します。
保存	現在開かれている.confファイルを保存します。
名前を付けて保存	現在開かれている.confファイルを新しい名前で保存します。
CABの作成	CABファイルの作成処理を開始します。
キャンセル	オペレーションをキャンセルします。
アップロード	.confファイルをWebサーバーにアップロードします。
ダウンロード	.confファイルをWebサーバーからブラウザーのデフォルトのダウンロードフォルダーにダウンロードします。

エンティティの選択



エンティティオブジェクトは、様々な粒度で選択できます。

1 リポジトリ内の全エンティティを選択するには、該当するエンティティタイプのチェックボックスをオンにします。[Selection Summary] ペインに [All entities inside <リポジトリ名 > are selected.] と表示されます。

2 リポジトリのサブセットを選択するには、エンティティタイプを ▸ で開き、表示されたリストからエンティティのサブタイプを選択します。[Select Entities] ペインに、選択可能なエンティティオブジェクトが表示されます。選択を終えると、[Selection Summary] ページに選択したエンティティの数とタイプが表示されます。

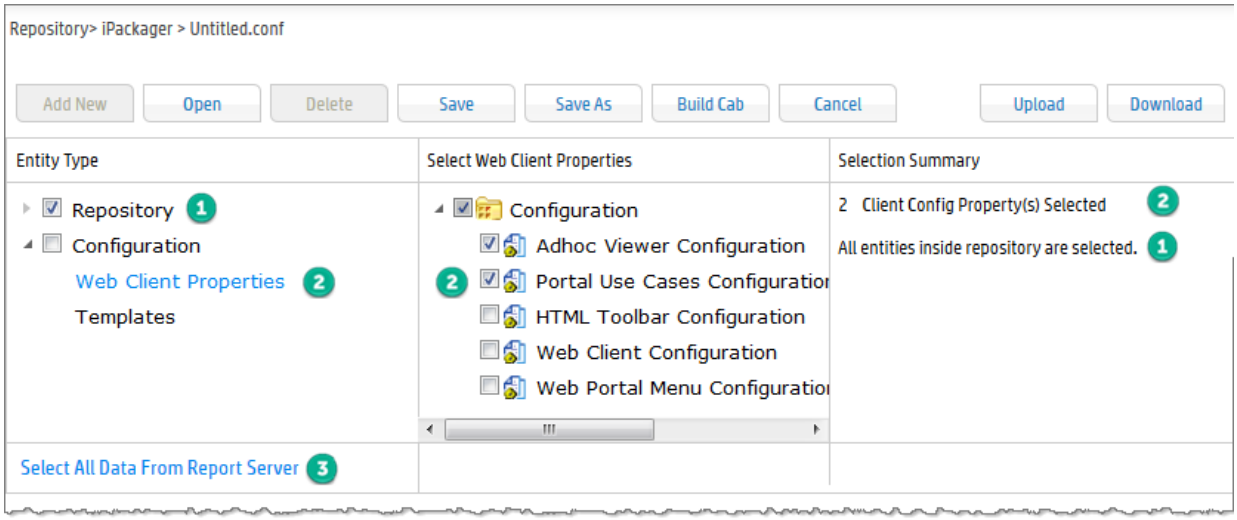
3 レポートサーバーの全エンティティを選択するには、[Entity Type] ペインの下にある [Select All Data From Report Server] をクリックします。[Selection Summary] ペインに [All data from report server is selected.] と表示されます。選択を元に戻すには、[Deselect Complete Data] をクリックします。

設定ファイルを開く

既存の.confファイルをiPackagerで開くには

1. iPackagerツールバーの **[Open]** をクリックします。[Open Configuration File] ダイアログが表示されます。
2. 使用可能な設定ファイルを選択します。
3. **[Open]** をクリックします。

エンティティオブジェクトの選択



エンティティオブジェクトは、様々な粒度で選択できます。

1 リポジトリ内の全エンティティを選択するには、該当するエンティティタイプのチェックボックスをオンにします。[Selection Summary] ペインに [All entities inside <リポジトリ名 > are selected.] と表示されます。

2 リポジトリのサブセットを選択するには、エンティティタイプを ▸ で開き、表示されたリストからエンティティのサブタイプを選択します。[Select Entities] ペインに、選択可能なエンティティオブジェクトが表示されます。選択を終えると、[Selection Summary] ページに選択したエンティティの数とタイプが表示されます。

3 レポートサーバーの全エンティティを選択するには、[Entity Type] ペインの下にある [Select All Data From Report Server] をクリックします。[Selection Summary] ペインに [All data from report server is selected.] と表示されます。選択を元に戻すには、[Deselect Complete Data] をクリックします。

設定ファイルへのエンティティオブジェクトの追加

エンティティオブジェクトの参照をレポートサーバーから.confファイルにインポートできます。

注: エンティティの参照のみがインポートされます。実際のコンポーネントは、CABファイルの作成時にインポートされます。

.confファイルにエンティティオブジェクトの参照を追加するには

1. インポートするエンティティオブジェクトを選択します。「エンティティオブジェクトの選択」(320 ページ) を参照してください。

2. **[Save]** または **[Save As]** をクリックすると、[Save Configuration File] ダイアログボックスが表示されます。
3. 設定ファイルの名前を入力します。
4. **[Save]** をクリックします。成功すると、ページ上部に確認メッセージが表示されます。

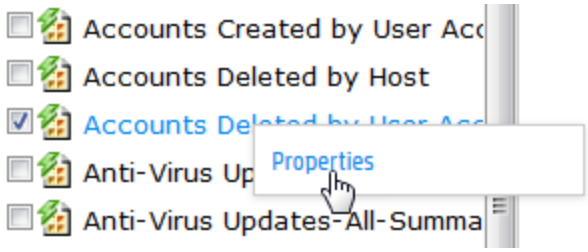
注: [Add New] ボタンが使用可能になります。このボタンをクリックすると、新しい設定ファイルの作成のために、エンティティ選択ペインがクリアされます。

エンティティオブジェクトのプロパティの変更

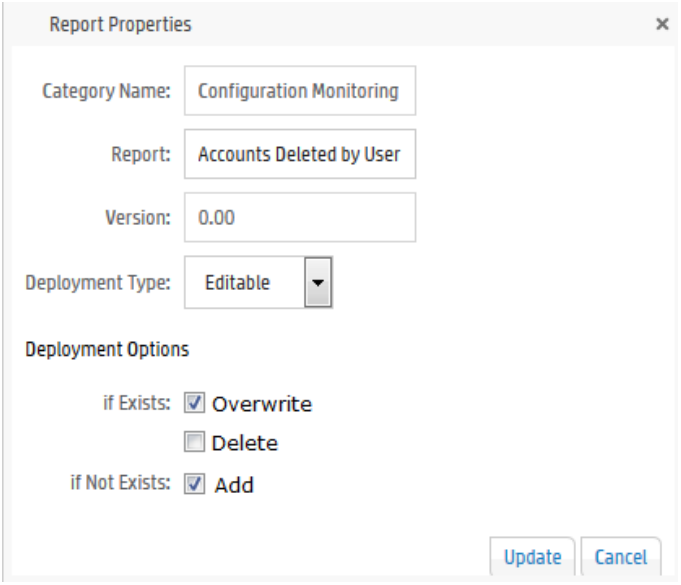
.confファイルを開き、エンティティオブジェクトのプロパティを変更することができます。

エンティティオブジェクトのプロパティを変更するには

1. **[Open]** をクリックして既存の.confファイルを開きます。
2. エンティティタイプを選択し、変更するオブジェクトを開きます。
3. [Select Entity] ペインでオブジェクトを右クリックし、ポップアップメニューの **[Properties]** をクリックします。



そのオブジェクトのプロパティダイアログボックスが開き、各オブジェクトのデフォルトプロパティが表示されます。



オブジェクト名として、レポートサーバーで使用されているオブジェクト名があらかじめ設定されています。オブジェクト名は変更できます。ここで名前を変更すると、オブジェクトは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

さらに、どのオブジェクトにも以下のような [Deployment Options] があります。

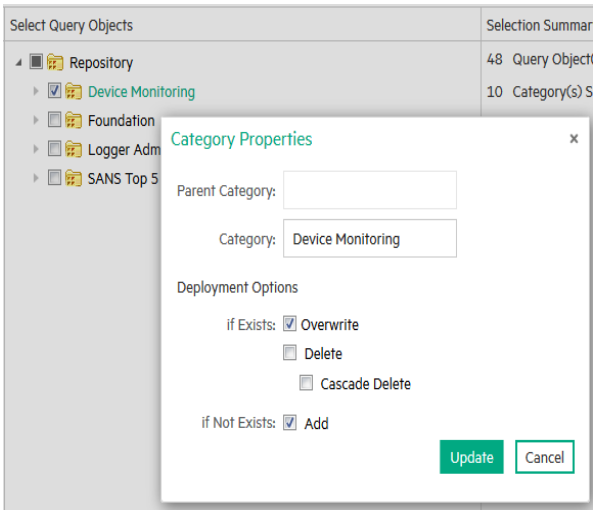
- If Exists:
  - Overwrite: インポートの際、コンポーネントがパッケージ中に見つかった場合、パッケージ内のコンポーネントをレポートサーバー上のコンポーネントで置き換えます。
  - Delete: インポートの際、コンポーネントがパッケージ中に見つかった場合、コンポーネントを削除します。
  - Cascade Delete (カテゴリフォルダーのみ): レポートが含まれている場合でもカテゴリフォルダーを削除します。
- If Not Exists:
  - Add: インポートの際、コンポーネントがパッケージ中に見つからなかった場合、コンポーネントをパッケージに追加します。

カテゴリのプロパティ

iPackagerでCABファイルを作成するとき、選択したカテゴリの名前を変更できます。ここで名前を変更すると、カテゴリは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

iPackagerでのカテゴリ名の変更

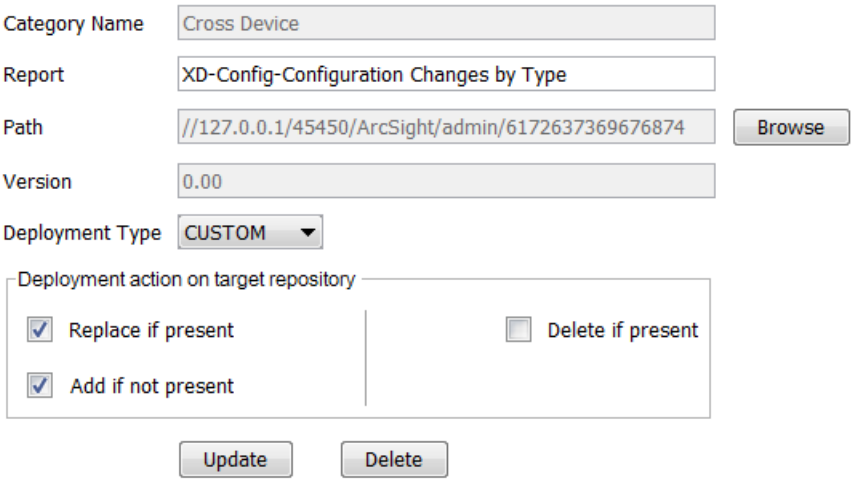
1. iPackagerのナビゲーションツリーから、名前を変更するカテゴリを選択します。
2. 右クリックして、**[Properties]** を選択します。[Category Properties] ダイアログが開きます。



3. 必要に応じてプロパティを変更します。
4. **[Update]** をクリックします。新しいカテゴリ名がiPackagerに表示されます。

レポートプロパティ

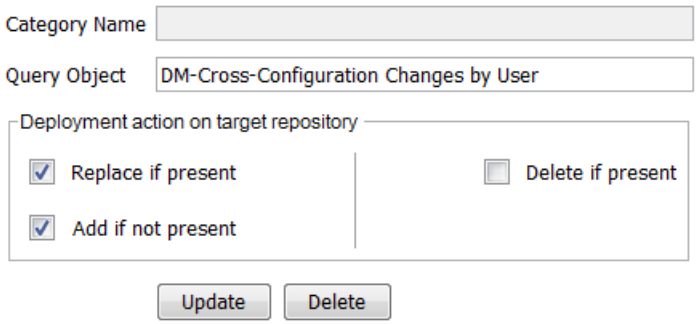
[iPackager] ページのナビゲーションツリーでレポートをクリックすると、以下のプロパティページが表示されます。



[Report] ボックスには、レポートサーバーにあるレポートの名前があらかじめ設定されます。レポート名は変更できます。ここで名前を変更すると、レポートは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

クエリプロパティ

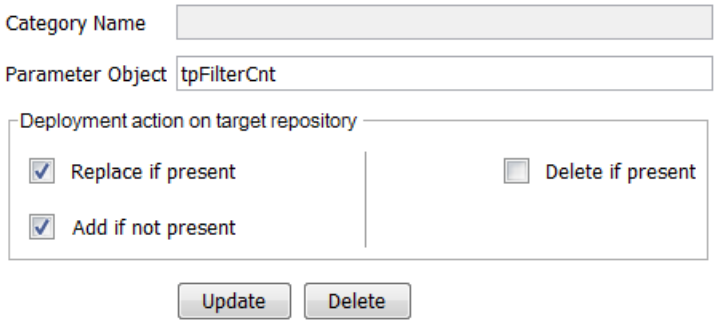
[iPackager] ページのナビゲーションツリーでクエリをクリックすると、以下のプロパティページが表示されます。



[Query Object] ボックスには、レポートサーバーにあるクエリオブジェクトの名前があらかじめ設定されます。クエリオブジェクト名は変更できます。ここで名前を変更すると、クエリオブジェクトは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

パラメータープロパティ

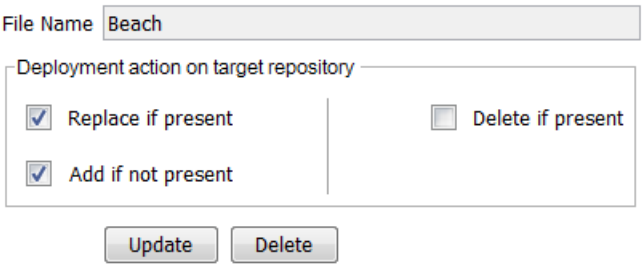
[iPackager] ページのナビゲーションツリーでパラメーターをクリックすると、以下のプロパティページが表示されます。



[Parameter Object] ボックスには、レポートサーバーにあるパラメーターオブジェクトの名前があらかじめ設定されます。パラメーターオブジェクト名は変更できます。ここで名前を変更すると、パラメーターオブジェクトは新しい名前でパッケージ化されますが、レポートサーバー上の元の名前は変更されません。

テンプレートプロパティ

[iPackager] ページのナビゲーションツリーでテンプレートをクリックすると、以下のプロパティページが表示されます。



CABファイルの作成

CABファイルを作成するためのコマンドを実行すると、開かれている.confファイル内の参照で指定された実際のオブジェクトが、それぞれの場所から実際に取得され、CABファイルが作成されます。このCABファイルには、すべてのオブジェクトが格納されます。

CABファイルの作成時に、.confファイルに保存されているいずれかの情報が正しいソースにない場合、エラーメッセージが表示され、CABの作成処理が停止します。CABファイルを再度作成する前に、すべてのエラーを修正する必要があります。

CABファイルを作成するには

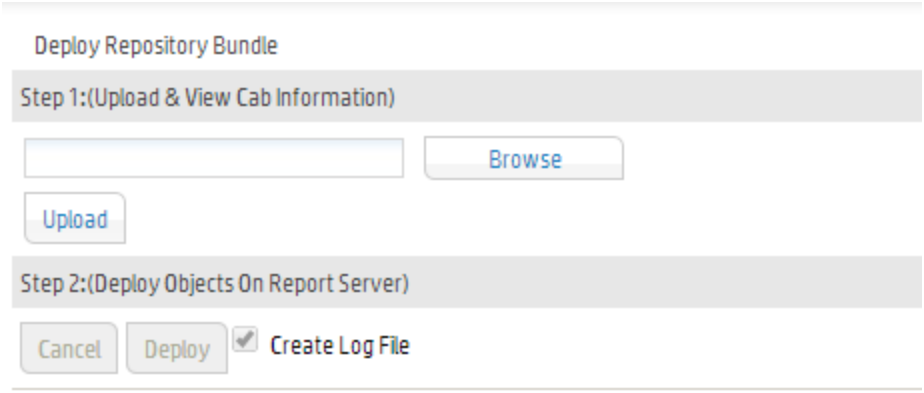
1. **[Build CAB]** をクリックします。
2. **[Build Properties]** ダイアログで、ファイルの名前を入力します。
3. 必要に応じて、**[Author]**、**[Company]**、**[Version]**、**[Comment]** の各フィールドに情報を入力します。
4. **[Build and Download]** をクリックします。[Build Status] ウィンドウにステータスが表示されます。プロセスを停止するには、**[Cancel Build]** をクリックします。
5. CABファイルが完成したら、ファイルに含まれるオブジェクトをメッセージで確認します。

レポートバンドルの展開

新しいセキュリティシナリオへの対処、パッケージ化されたソリューションの追加、更新されたレポートによる現在のカバー範囲の拡大のために、ArcSightから追加のレポートセットを入手することがあります。**[Deploy Report Bundle]** ページを使用すると、新しいレポートのパッケージをLoggerシステムにロードおよび展開することができます。

レポートのCABファイルを展開するには

[Report] ページの左パネルメニューで、**[Deploy Report Bundle]** リンクをクリックして開始します。



レポートパッケージ (CABファイル) には、以下のものを含め、多くの種類のレポート作成リソースが含まれています。

- カテゴリとレポート
- 組織情報
- ポータルプロパティとサーバープロパティ
- パラメーターオブジェクト
- クエリオブジェクト
- アドホックレポートテンプレート
- プリンター設定
- データベース接続

レポートパッケージをアップロードおよび展開するには

1. [Step 1] 下に表示される入力ボックスに、レポートパッケージファイル名とそのフルパスを指定します。**[Browse]** をクリックしてファイルを探します。
2. **[Upload]** をクリックします。

   内容がアップロードされ、含まれているカテゴリとレポートオブジェクトに関する情報が表示されます
3. 展開処理のログを作成する場合は、**[Create Log File]** オプションをオンにします。
4. **[Deploy]** をクリックして展開処理を続行するか、**[Cancel]** をクリックして中断します。

   展開中のパッケージ内のオブジェクトに関するステータス情報が表示されます。

   [Deploy] ボタンのすぐ下に凡例が表示されます。パッケージ内の各コンポーネントに関する情報がそれぞれのタブに表示されます。

   注: 上書き動作は、パッケージが作成されたときに決定されています。

   たとえば、展開したパッケージ内のオブジェクトがシステム上の既存のオブジェクトを上書きするかどうかの指示や、上書きする条件は、パッケージの作成時に決定されます。そのため、パッケージの展開についてのこれらの設定は、展開時には指定できま

せん。「iPackagerユーティリティ」(317ページ) を参照してください。

[Create Log File] チェックボックスをオンにした場合はログファイルが作成されます。

展開されたレポートパッケージの内容は、Loggerのレポートの各ページで使用できます。ソリューションレポートは、左パネルメニューの **[Solution Reports]** の下に表示されます。これらの種類のレポートの詳細については、「ソリューションレポート」(312ページ) を参照してください。

ヒント: CABファイルをソースLoggerからターゲットLoggerに展開するとき、インポートされるカテゴリの名前とIDが両方のLoggerで同じでないと、展開に失敗します。

この問題に遭遇した場合は、ターゲットLoggerまたはソースLoggerで、カテゴリの名前またはIDが一意になるように、競合するカテゴリ名を変更します (ソースLoggerで変更した場合は、CABファイルの再作成が必要になります)。その後、CABファイルを再度展開します。

iPackager設定ファイルの削除

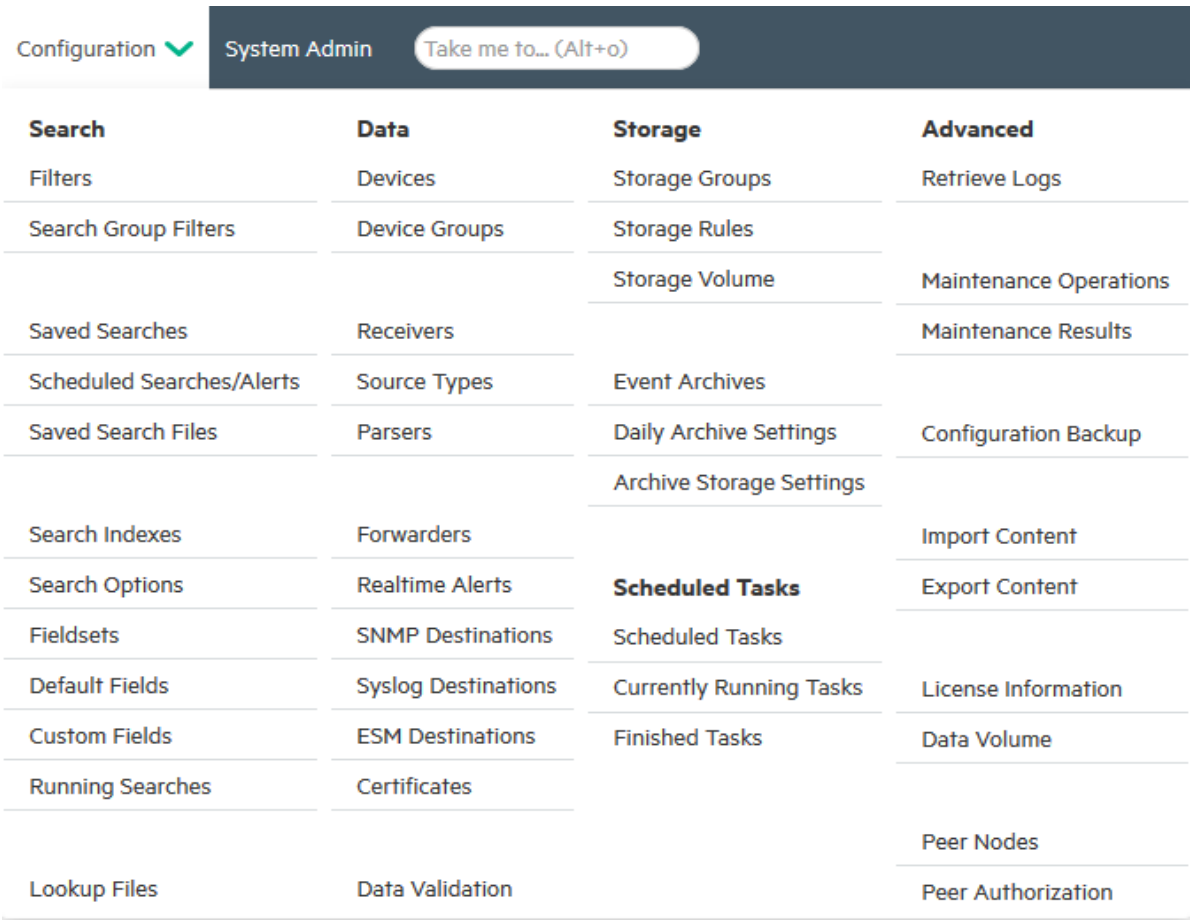
.confファイルを削除するには

1. iPackagerで.confファイルを開きます。
2. **[Delete]** をクリックします。
3. 警告ダイアログで **[Yes]** をクリックし、削除を確定します。

第5章: 設定

以下の各トピックでは、受信者、転送者、デバイス、デバイスグループ、SmartConnector、フィルターを作成および管理する方法について説明します。あるユーザーが作成した受信者やデバイスなどのリソースは、他のすべてのユーザーが参照できますが、ユーザーグループの権限が適用されます。リソースはすべてのセッションで共有されます。

これらの設定オプションには、Logger UIの[設定 (Configuration)]ドロップダウンメニューを使用するか、[移動... (Take Me To...)]テキストボックスに機能名を入力しながらドロップダウンメニューで該当する機能をクリックすることによってアクセスできます。



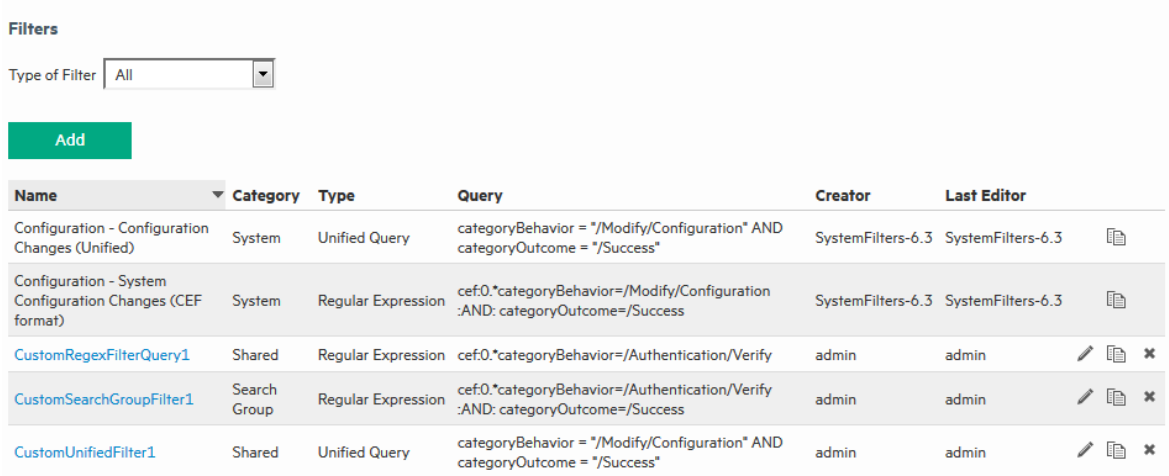
検索

[**設定 | ストレージ**] カテゴリのオプションを使用すると、Loggerで検索が機能する方法を管理できます。

フィルター

検索フィルターを作成して特定のクエリを保存すれば、簡単に再利用することができます。フィルターは保存された検索に似ています。しかし、フィルターにはクエリのみが保存されるのに対して、保存された検索には、クエリに加えて、時間範囲の情報も保存されます。

システムには、定義済みの検索フィルターのセットが用意されています。これらのフィルターの詳細については、「システムフィルター/事前定義フィルター」(145ページ)を参照してください。[フィルタ (Filters)] ページでは、新しいフィルターを追加したり、既存のフィルターを編集したりできます。



[フィルタ (Filters)] ページには、以下のフィルターカテゴリが表示されます。

- 共有 (Shared): 共有検索フィルターはユーザーが作成したフィルターであり、すべてのユーザーが参照できます。作成した共有検索フィルターは、すべてのユーザーがイベントの検索に使用できます。
- 検索グループ (Search Group): 検索グループフィルターは、特定のユーザーグループに属するユーザーが参照できるイベントを制限するための、アクセス制御メカニズムを提供します。検索グループフィルターは、あるレポートカテゴリによって処理されるイベントを制限するためにも使用できます (「レポートカテゴリフィルター」(315ページ) を参照)。検索グループフィルターのクエリには、正規表現のみを含めることができます。詳細については、「検索グループフィルター」(332ページ) を参照してください。

  検索グループフィルターを作成または編集するには、管理者レベルの特権が必要です。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。
- システム (System): システムフィルターと呼ばれる、システム付属の定義済みのフィルターセットです。システムフィルターの詳細については、「システムフィルター/事前定義フィルター」(145ページ) を参照してください。

検索フィルターには、以下の2種類のクエリのいずれかを設定できます。

- 統合クエリ (Unified Query): 統合クエリ ([Unified]) 検索クエリは、キーワードとフィールドを指定します。
- 正規表現 (Regular Expression): 正規表現 ([Regex Query]) 検索クエリは、正規表現を指定します。正規表現に基づく検索フィルターは、正規表現クエリのみを受け付けるリアルタイムアラートを作成する際に便利です。

フィルターを作成するには

1. ナビゲーションバーの [設定] メニューから [**フィルタ**] を選択して、[フィルタ] ページを開きます。
2. [**追加 (Add)**] をクリックします。[フィルタを追加] ページが表示されます。

3. 新しいフィルターの名前を、[名前] フィールドに入力します。フィルター名では大文字と小文字が区別されます。
4. 以下のいずれかのオプションを選択します。
   - 共有フィルターを作成する場合は、[**統合**] または [**正規表現クエリ**] を選択します。
   - 検索グループフィルターを作成する場合は、[**検索グループ**] を選択します。

     注: 検索グループフィルターを作成できるのは、管理者ユーザーだけです。Logger のユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。
5. [**次へ**] をクリックします。
6. 前の手順で、クエリタイプ [統合] または [正規表現クエリ] を選択した場合は、新しいフィルターのクエリを入力します。
   - [統合] クエリの場合

     クエリの入力時は、Loggerの検索ヘルパーによって、提案、考えられる一致、適用可能な演算子が自動的に提供されるため、クエリ式を素早く構築できます。詳細については、「検索ヘルパー」(102ページ) を参照してください。

     または

     [**検索の詳細設定**] をクリックし、検索ビルダーツールを使用してクエリを作成します。検索ビルダーツールの使用方法の詳細については、「検索の詳細設定ビルダーの使用」(94ページ) を参照してください。
   - [正規表現] クエリの場合 [クエリ] テキストボックスに正規表現を入力します。
7. [**保存**] をクリックします。

   注: 検索グループフィルターを作成した場合は、ユーザーグループに関連付けます (「検索グループフィルター」(332ページ) を参照)。

既存のフィルターをコピーしてフィルターを作成するには

1. ナビゲーションバーの [設定] メニューから [**フィルタ**] を選択して、[フィルタ] ページを開きます。
2. フィルターのリストから、コピーするフィルターを探します。[コピー] アイコン () をクリックします。

   「コピー <フィルター名>」という名前の新しいフィルターが作成されます。
3. フィルター名を変更し、必要に応じて新しいフィルターのクエリを編集します。
4. [**保存**] をクリックします。

フィルターを編集するには

1. ナビゲーションバーの [設定] メニューから [**フィルタ**] を選択して、[フィルタ] ページを開きます。
2. 編集するフィルターを探し、その行の [編集] アイコン ( ) をクリックします。
3. フォームの情報を変更し、[**保存**] をクリックします。

フィルターを削除するには

1. ナビゲーションバーの [設定] メニューから [**フィルタ**] を選択して、[フィルタ] ページを開きます。
2. 削除するフィルターを探し、その行の [削除] アイコン ( ) をクリックします。
3. 削除を確定します。

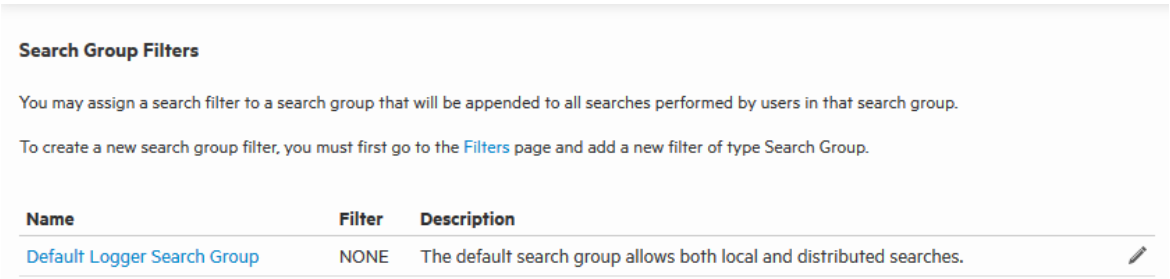
検索グループフィルター

検索グループフィルターは、ユーザーグループと検索グループフィルターの関連付けを管理します。検索グループフィルターは、以下の2つの方法でイベントを制限するために使用できます。

- **あるレポートカテゴリで処理されるイベントを制限する**: 検索グループフィルターは、レポートカテゴリに直接関連付けることができます。この関連付けにより、レポートカテゴリ内のすべてのレポートによって処理されるイベントを制限できます。

  検索グループフィルターを使用して、レポートカテゴリによって処理されるイベントを制限する場合は、以下で説明するように [検索グループフィルタ] ページで検索グループを設定する必要はありません。タイプが「検索グループ」のフィルターを追加した後、[レポート] メニューの [レポートカテゴリフィルタ] ページに直接移動し、レポートカテゴリ用のフィルターを選択できます。詳細については、「レポートカテゴリフィルター」(315ページ) を参照してください。
- **ユーザーグループのメンバーが参照できるイベントを制限する**: 検索グループフィルターは、ユーザーグループ (タイプがLogger検索のもの) に関連付けることができます。この関連付けは、そのユーザーグループのすべてのメンバーが、検索グループフィルターに一致するイベントのみを参照できることを意味します。ユーザーグループ (後でこの章で詳しく説明します) は、指定したユーザーに特権を割り当てるための手段を提供します。

  [検索グループフィルタ (Search Group Filters)] ページ



> **ヒント:** タイプがデフォルトLogger検索グループのユーザーグループが [名前] 列に表示され、関連フィルターが中央の列に表示されます。
>
> 検索グループフィルターが関連付けられていないユーザーグループに属するユーザーは、すべてのイベントを参照できます。

検索グループフィルターを追加、編集、削除するには、「フィルター」(329ページ)を参照してください。ユーザーグループを追加、編集、削除するには、「ユーザ/グループ」(530ページ)で、Loggerのユーザー権限とその管理方法の詳細を参照してください。システム管理グループに属しているユーザーのみが、検索グループフィルターを割り当てることができます。

検索グループフィルターをユーザーグループに関連付けるには

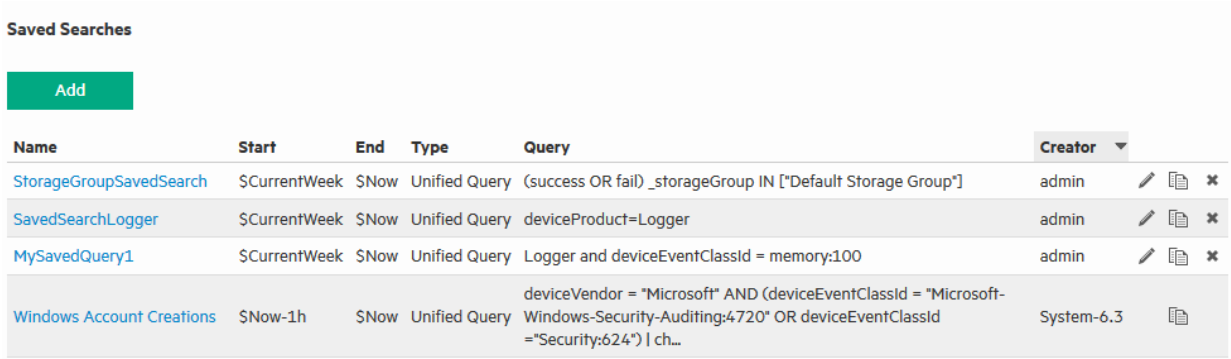
1. 検索グループフィルターに関連付けるユーザーグループが存在しない場合は、タイプが検索グループの新しいユーザーグループを作成します。「ユーザ/グループ」(530ページ)の説明を参照してください。
2. ユーザーグループに関連付ける検索グループフィルターが存在しない場合は、タイプが検索グループのフィルターを作成します。「フィルターを作成するには」(330ページ)の説明を参照してください。フィルターを作成する際、[**タイプ**] プルダウンメニューから [**検索グループ**] オプションを選択します。
3. ナビゲーションバーの [設定] メニューから、[**検索グループフィルタ**] を選択します。
4. [検索グループフィルタ] テーブルでユーザーグループを見つけます。[編集] アイコン (✎) をクリックします。
5. プルダウンリストからフィルターを選択します。(タイプが検索グループのフィルターのみが表示されます)。
6. [**保存**] をクリックします。

保存された検索

保存された検索には、検索フィルターと同様に、特定のクエリが記憶されます。ただし、保存された検索には、クエリに加えて、時間範囲と、検索結果に表示するフィールドセットが保存されます。時間範囲を保存することで、スケジュールされた検索とレポートがサポートされます。保存された検索は、一定の間隔で実行するようにスケジュールできます。スケジュールされた保存された検索は、アラートを生成するように設定することもできます。詳細については、「スケジュールされた検索/アラート」(335ページ)を参照してください。

[保存された検索] ページには、保存された検索がすべて表示され、保存された検索の追加、編集、削除が可能です。ここで保存された検索を追加するか、[検索] ページから直接追加できます。

[保存された検索 (Saved Search)] ページ



[検索] ページから検索を保存する方法については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) を参照してください。

このページで作成した保存された検索を使用する方法については、「保存済みクエリでの検索」(149ページ) を参照してください。

保存された検索を追加するには

1. [**設定 | 検索**] メニューを開き、[**保存された検索**] をクリックします。
2. [**追加**] をクリックし、以下のパラメーターを入力します。

パラメーター	説明
名前	この保存された検索の名前。この名前は、エクスポートされる出力ファイルに使用され、保存された検索の日付と時刻が追加されます。
開始時刻	最も早いイベントの絶対日付と時刻。また、[**動的**] をオンにして、保存された検索ジョブの実行時刻からの相対的な開始時刻を指定することもできます。
終了時刻	上記と同様に、最後のイベントの絶対的または動的な日付と時刻。
クエリ	テキストフィールドにクエリを入力するか、テキストフィールドの下のリストから1つ以上のフィルターを選択します。 クエリの入力時は、Loggerの検索ヘルパーによって、提案、考えられる一致、適用可能な演算子が自動的に提供されるため、クエリ式を素早く構築できます。詳細については、「検索ヘルパー」(102ページ) を参照してください。
ローカル検索	このチェックボックスをオンにすると、保存された検索がローカルなLoggerボックスに制限されます。[ローカル検索] チェックボックスをオフのままにすると、保存された検索には、ローカルなLoggerに加えて、すべてのピアLoggerが含まれます。

3. [**保存**] をクリックして新たな保存された検索を追加するか、[**キャンセル**] をクリックして終了します。

保存された検索を編集するには

1. [**設定 | 検索**] メニューを開き、[**保存された検索**] をクリックします。
2. 編集する保存された検索を探し、その行の [編集] アイコン(✎)をクリックします。

3. フォームの情報を変更し、[**保存**] をクリックします。

保存された検索を削除するには

1. [**設定 | 検索**] メニューを開き、[**保存された検索**] をクリックします。
2. 削除する保存された検索を探し、その行の [削除] アイコン (✖) をクリックします。
3. 削除を確定します。

スケジュールされた検索/アラート

保存された検索は、一定の間隔で実行するようにスケジュールできます。スケジュールされ保存された検索は、アラートを生成するように設定することができます。スケジュールされた検索の結果はファイルに書き込まれます (「保存された検索ファイル」(346ページ) を参照)。スケジュールされたアラートの結果は、指定された通知先に送信されます。

[スケジュールされた検索/アラート] ページには、現在スケジュールされている保存された検索およびアラートのリストが表示されます。ここから、新しいスケジュールされた検索またはアラートを追加したり、既存のスケジュールされた検索またはアラートを編集したりすることができます。スケジュールされ保存された検索アラートの詳細については、「保存された検索アラート」(343ページ) を参照してください。

注: 保存された検索アラートをスケジュールする前に、保存された検索を1つ以上作成しておく必要があります。アラートに使用される保存された検索には、chartやtopなどのアグリゲーション演算子を含めることはできません。

新しいスケジュールされた検索またはアラートを追加するには

スケジュールされた検索またはアラートを新しく追加するには、[設定] メニューを使用するか、[検索結果] ページから直接追加します。

- 検索結果ページ (**[分析] > [検索]**) からスケジュールされた検索/アラートをセットアップする手順については、「保存された検索アラート (スケジュールされたアラート) の作成」(343ページ) を参照してください。
- 検索結果ページ (**[分析] > [検索]**) から、スケジュールされた検索をセットアップするには、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) の手順を実行し、タイプを **[スケジュールされた検索]** に設定して、**[スケジュールに入れる]** オプションを選択します。
- 設定メニュー (**[設定 | 検索]** > **[スケジュール済み検索/アラート]**) からスケジュールされた検索またはアラートをセットアップする方法については、「スケジュールされた検索またはスケジュールされたアラートの追加」(336ページ) を参照してください。

既存のスケジュールされた検索およびアラートのリストを表示するには

[**設定 | 検索**] メニューを開き、[**スケジュールされた検索/アラート**] をクリックします。

現在のスケジュールされた検索およびアラートのリストが表示されます。

既存のスケジュールされた検索またはアラートを編集するには

1. [**設定 | 検索**] メニューを開き、[**スケジュールされた検索/アラート**] をクリックします。
2. 編集するスケジュールされた検索/アラートを探し、その行の [編集] アイコン (✎) をクリックします。
3. [編集] アイコン(✎)をクリックして、必要に応じてパラメーターを更新します。設定の詳細については、「スケジュールされた検索またはアラートを [スケジュールされた検索/アラート] ページから設定するには」(337ページ) を参照してください。
4. [**保存**] をクリックして、スケジュールされた検索/アラートを更新するか、[**キャンセル**] をクリックして変更内容を破棄します。

スケジュールされた検索またはアラートを削除するには

1. [**設定 | 検索**] メニューを開き、[**スケジュールされた検索/アラート**] をクリックします。
2. 削除するスケジュールされた検索/アラートを特定し、その行の [編集] アイコン(✖)をクリックします。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてスケジュールされた検索/アラートを保持します。

スケジュールされた検索またはアラートを有効または無効にするには

1. [**設定 | 検索**] メニューを開き、[**スケジュールされた検索/アラート**] をクリックします。
2. 有効にするスケジュールされた検索/アラートを探します。
3. 対応するアイコン (✔または⊘) をクリックして、アラートを有効または無効にします。

トリガーされたアラートを表示するには

「アラートの表示」(156ページ) を参照してください。

スケジュールされた検索またはスケジュールされたアラートの追加

保存された検索またはアラートは、いつでもスケジュールを設定して任意の時刻に実行できます。保存された検索またはアラートのスケジュールを設定する前に、保存された検索を1つ以上作成するか、保存しておく必要があります。「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) を参照してください。

スケジュールされた検索またはアラートを新しく追加するには、[設定] メニューを使用するか、[検索結果] ページから直接追加します。

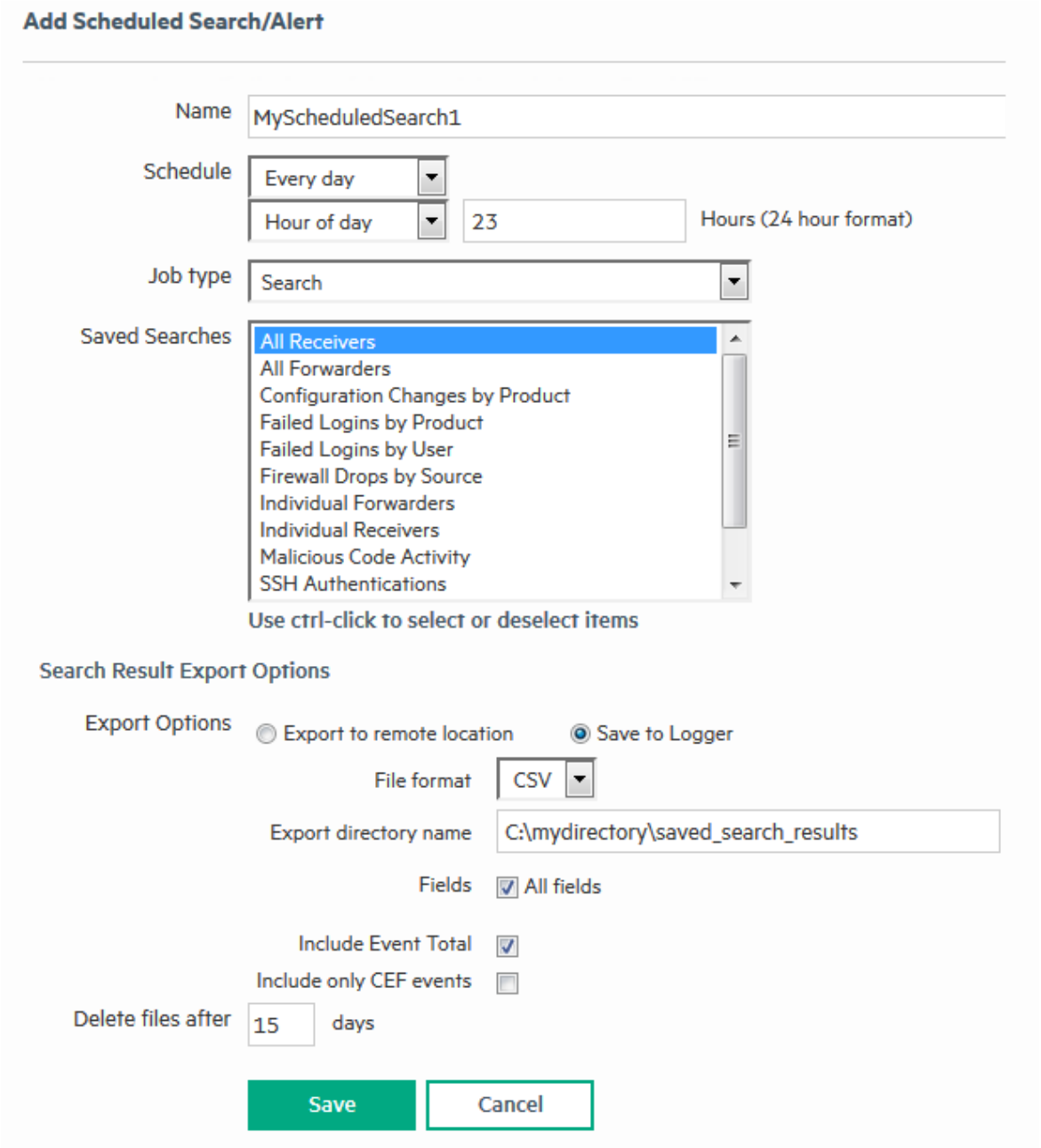
- スケジュールされた検索またはアラートを [検索結果] ページ ([分析] > [検索]) から設定する方法については、「保存された検索アラート (スケジュールされたアラート) の作成」(343

ページ) を参照してください。

- スケジュールされた検索を [検索結果] ページ ([分析] > [検索]) から設定するには、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) の手順を実行し、[タイプ] を **[スケジュールされた検索]** に設定して、**[スケジュールに入れる]** オプションを選択します。

スケジュールされた検索またはアラートを [スケジュールされた検索/アラート] ページから設定するには

1. [設定 | 検索] メニューを開き、**[スケジュールされた検索/アラート]** をクリックします。
2. **[追加]** をクリックします。以下のような画面が表示されます。



3. 以下のパラメーターを入力します。

パラメーター	説明
名前 (Name)	このスケジュールされた検索の名前。
スケジュール (Schedule)	レポートを実行するタイミングと頻度を設定します。これらのオプションの詳細については、「日付と時刻のスケジュールのオプション」(150ページ)を参照してください。

パラメーター	説明
ジョブタイプ (Job Type)	保存された検索をスケジュールする場合は、**[検索 (Search)]** を選択します。 保存された検索アラートをスケジュールする場合は、**[アラート]** を選択します。
保存された検索 (Saved Searches)	保存された検索のリストから選択します。保存された検索の中に目的に合うものがない場合は、**[保存された検索 (Saved Searches)]** ページをクリックして新しい検索を定義します。その後、このページに戻って保存された検索をスケジュールします。保存された検索クエリの定義の詳細については、「保存された検索」(333ページ) を参照してください。 Ctrlを押しながらクリックすると、リスト内の複数の項目を選択または選択解除できます。 **注:** 1つのスケジュールされた検索ジョブで複数の保存された検索が指定されている場合、生成されるファイルには、実際のイベントの数ではなく、それぞれの保存された検索のヒット数が格納されます。 **注:** 設定する各アラートに対して、選択できる保存された検索は1つだけです。 **注:** chartやtopなどのアグリゲーション演算子を、スケジュールされたアラートの検索クエリに含めることはできません。保存された検索アラートの場合、作成した検索を指定した後、アグリゲーション演算子を含む保存された検索は選択リストに表示されません。

4. [ジョブタイプ (Job Type)] で [検索 (Search)] を選択した場合、[検索結果エクスポート オプション (Search Result Export Options)] を指定します。

検索ジョブのオプション

パラメーター	説明
エクスポート オプション (Export Options)	Loggerアプライアンスの場合 以下のいずれかのオプションを選択します。 • [リモート ロケーションへエクスポート (Export to remote location)]: ファイルは、NFSマウント、CIFSマウント、またはSANシステムの指定した場所に書き込まれます。 • [Loggerへ保存 (Save to Logger)]: ファイルはLoggerのオンボードディスクに保存されます。ファイルがローカルに保存されている場合は、保存された検索ファイル (「保存された検索ファイル」(346ページ)) 機能を使用してそれらのファイルにアクセスできます。 ソフトウェアLoggerの場合、該当する唯一のオプションは、あらかじめ選択されている [Logger へ保存 (Save to Logger)] です。 **ヒント:** Loggerアプライアンスは、ユーザーインターフェイスを通じたマウントをサポートしています。ソフトウェアLoggerは、そのファイルシステムを使用します。これには、オペレーティングシステムを通じてマウントされたリモートロケーションが含まれていてもかまいません。
ファイル形式 (File Format)	エクスポートされる検索結果のフォーマットを選択します。 • [CSV]: CSVファイルです。 • [PDF]: 検索結果がグラフと表として含まれる、レポートスタイルのファイルです。[タイトル (Title)] フィールドにレポートのタイトルを指定する必要があります。検索クエリに、chart、topなど、グラフを作成する演算子が含まれている場合、PDFにグラフが含まれます。その場合、[グラフタイプ (Chart Type)] フィールドと[グラフ結果リミット (Chart Result Limit)] フィールドも設定できます。これらのフィールドについては、この表の中で後述します。
リモートロケーション	このフィールドは、Loggerアプライアンスでのみ使用可能です。既存のリモートファイルシステムの場所をドロップダウンから選択します。既存のリモートファイルシステムがない場合、リモートファイルシステムの場所を指定するページのリンクが表示されます。

検索ジョブのオプション (続き)

パラメーター	説明
ディレクトリ名をエクスポート (Export Directory Name)	Loggerアプライアンスの場合は、検索結果のエクスポート先のディレクトリを、プルダウンメニューから選択します。 ソフトウェアLoggerの場合は、このフィールドにディレクトリパスを入力します。ここに指定できるのは、ソフトウェアLoggerがインストールされているマシン上のローカルディレクトリまたはマウントポイントのパスです。 デフォルトでは、保存された検索はすべて`/opt/arcsight/logger/userdata/logger/user/logger/data/savedsearch`に格納されます。 **ヒント:** 検索をフォルダーにグループ化するには、検索を保存するサブディレクトリを指定します。 指定された名前のディレクトリが存在しない場合は、ディレクトリが作成されます。指定した名前のディレクトリが存在し、[上書きしますか?] チェックボックスがオフになっている場合、エラーが生成されます。[上書きしますか?] チェックボックスがオンになっている場合、ディレクトリの現在の内容が上書きされます。
タイトル	(オプション) PDFファイルの最上部に表示されるタイトルを入力します。タイトルを指定しないと、デフォルトの「Untitled」が使用されます。 **ヒント:** このフィールドは、PDF出力形式を選択したときに使用可能になります。
フィールド	エクスポートされたファイルに含まれるイベントフィールドのリスト。デフォルトでは、表示されているすべてのフィールドが含まれます。 フィールドのリストを表示および編集するには、[すべてのフィールド] をオフにします。表示されているフィールドを削除するには、[クリア] をクリックします。
グラフタイプ (PDFのみ)	PDFファイルに含めるグラフの種類。選択できるのは、 カラム、棒、円グラフ、エリア、ライン、積み上げカラム、積み上げ棒グラフです。 **注:** このオプションは、[検索結果] 画面に表示される [グラフタイプ] を上書きします (このフィールドは、検索クエリにグラフを生成する演算子が含まれている場合に意味があります。そうでない場合は無視されます)。
グラフ結果リミット (PDFのみ)	グラフに含める一意の値の最大数。デフォルト値は10です。 (このフィールドは、検索クエリにグラフを生成する演算子が含まれている場合に意味があります。そうでない場合は無視されます)。 設定された [グラフ結果リミット] の値が、クエリの一意の値数未満の場合、上位から [グラフ結果リミット] の値に等しい数の値がプロットされます。つまり、グラフ結果リミットが5で、一意の値が7個見つかった場合、上位5個の値がプロットされます。

検索ジョブのオプション (続き)

パラメーター	説明
イベント合計を含む (Include Event Total)	このチェックボックスをオンにすると、保存された検索のイベント数か、複数の保存された検索が指定されている場合は合計が含まれます。
CEF イベントのみを含む (Include Only CEF events)	このチェックボックスをオンにすると、共通イベントフォーマット (CEF) イベントのみが含まれます。チェックボックスをオフにすると、すべてのイベントが出力に含まれます。 CEFの詳細については、『ArcSight CEF』を参照してください。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品マニュアルのコミュニティから "ArcSight Common Event Format (CEF) Guide" を検索してください。
ファイルを <日数> 日後に削除する (Delete files After)	保存された検索の結果を保持する日数を指定します。

5. [ジョブタイプ (Job Type)] で [アラート] を選択した場合、[アラート オプション] を指定します。

アラートジョブのオプション

パラメーター	説明
マッチ数	[閾値] で指定した秒数の間に何個のイベントが一致したらアラートを起動するか。
閾値 (秒)	[マッチ数] で指定した個数のイベントが、何秒の間に一致したらアラートを起動するか。
通知先はオプションです。指定しなかった場合、通知は送信されません。	
メールアドレス	(オプション) アラートの送信先の電子メールアドレスを、カンマで区切ったリスト。
SNMP 通知先	(オプション) アラートの送信先となるSNMP通知先。詳細については、「SNMP通知先」(417ページ) を参照してください。
Syslog 通知先	(オプション) アラートの送信先となるsyslogサーバーのアドレス。 詳細については、「syslog通知先」(417ページ) を参照してください。
ESM通知先	(オプション) アラートの送信先となるArcSightマネージャーのアドレス。詳細については、「ESM通知先への通知の送信」(419ページ) を参照してください。

6. **[保存]** をクリックして、新しいスケジュールされた検索/アラートを追加するか、[キャンセル] をクリックして終了します。
7. スケジュールされた検索を作成した後、「スケジュールされた検索またはアラートを有効または無効にするには」(336ページ) の説明に従って検索を有効にします。

保存された検索アラート

このセクションでは、保存された検索アラートについて説明します。保存された検索アラートは、Logger上で保存した検索クエリに基づきます。保存された検索クエリの詳細については、「保存された検索」(333ページ)を参照してください。

注: リアルタイムアラートについては、「リアルタイムアラート」(408ページ)を参照してください。アラート全般については、「Loggerアラートの種類」(412ページ)を参照してください。

保存された検索アラートごとに、一致数、しきい値、通知先、アラートを起動するスケジュールを設定します (指定したしきい値内で指定した一致数が発生した場合に起動されます)。新しいアラートが、電子メール、SNMP、またはSyslog通知先に通知を送信する場合は、アラートを作成する前に通知先を設定してください。

詳細は、「静的ルート」(496ページ)、「アラート通知の受信」(414ページ)および「アラート通知の設定」(416ページ)を参照してください。アラートの監査イベントは、デフォルトでは内部ストレージグループのみに書き込まれ、ESM通知先に転送されません。これらの監査イベントをESMに転送する必要がある場合は、カスタマーサポートにお問い合わせください。

注: この変更は、アラート用に生成された監査イベントのみに適用され、他の監査イベントはESM通知先に送信することができます。

注: システムのパフォーマンスを確保するため、保存された検索アラートジョブあたり最大200件のアラートが許可されます。そのため、保存された検索アラートジョブによって200件を超えるアラートが起動されると、その回のジョブ実行では最初の200件のアラートが送信され、残りは送信されません。また、ジョブが中断されるため、その回の実行に対してそれ以上アラートは起動されず、[完了したタスク] ページ (**[設定 | 実行中のタスク] > [完了したタスク]**) でそのジョブのステータスが「Failed」になります。ジョブは、次のスケジュール間隔でスケジュールどおりに実行され、上限に達するまでアラートが送信されます。

この制限は、リアルタイムアラートにはありません。

保存された検索アラート (スケジュールされたアラート) の作成

このセクションでは、保存された検索をスケジュールされたアラートとして実行するようにスケジュールする方法について説明します。リアルタイムアラートの作成方法については、「リアルタイムアラートの作成」(410ページ)を参照してください。アラートのタイプの説明については、「Loggerアラートの種類」(412ページ)を参照してください。

保存された検索は、任意の時間に実行されるようにスケジュールできます。保存された検索アラートをスケジュールする前に、保存された検索を1つ以上作成しておく必要があります。

注: アラートに使用される保存された検索には、chartやtopなどのアグリゲーション演算子を含めることはできません。詳細については、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) を参照してください。

スケジュールされた検索またはアラートを新しく追加するには、[設定] メニューを使用するか、[検索結果] ページから直接追加します。

- 検索結果ページ (**[分析] > [検索]**) からスケジュールされた検索/アラートをセットアップする手順については、「保存された検索アラート (スケジュールされたアラート) の作成」(343ページ) を参照してください。
- 検索結果ページ (**[分析] > [検索]**) から、スケジュールされた検索をセットアップするには、「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ) の手順を実行し、タイプを **[スケジュールされた検索]** に設定して、**[スケジュールに入れる]** オプションを選択します。
- 設定メニュー (**[設定 | 検索] > [スケジュール済み検索/アラート]**) からスケジュールされた検索またはアラートをセットアップする方法については、「スケジュールされた検索またはスケジュールされたアラートの追加」(336ページ) を参照してください。

検索結果ページから保存された検索アラートをセットアップするには

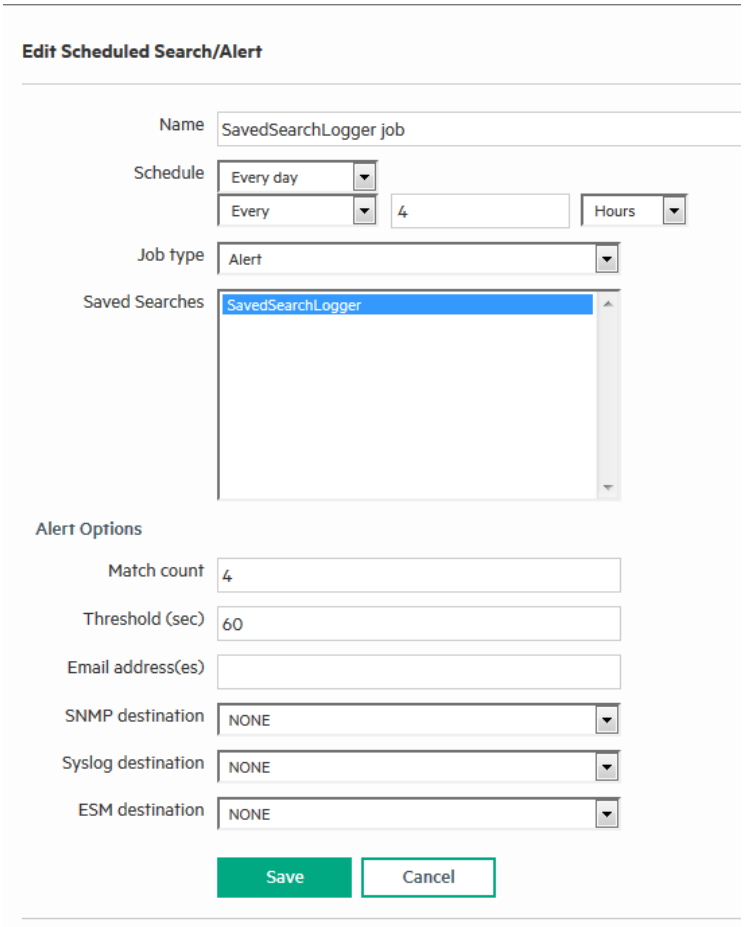
1. 検索を実行します (「イベントの検索」(106ページ) を参照)。
2. [保存] アイコン ( ) をクリックし、以下の設定を入力します。

パラメーター	説明
名前	保存しようとしているクエリの名前。
名前を付けて保存	スケジュールオプションを有効にするには、[保存された検索] を選択します。
スケジュールに入れる	今すぐスケジュールする場合はクリックし、後でスケジュールする場合は空白のままにします。
タイプ	検索またはアラートのどちらをスケジュールするのかを選択します。 スケジュールされた検索は、あらかじめ決められたスケジュールに従って実行され、あらかじめ指定された場所に結果がエクスポートされます。 スケジュールされたアラートでは、あらかじめ決められたスケジュールに従って検索が実行されますが、指定されたしきい値内の指定された数のイベントが見つかった場合にのみアラートが生成されます。 アラートを作成するには、[スケジュールされた警告] を選択します。

3. **[保存 (Save)]** をクリックします。

   前のステップで [スケジュールに入れる] 設定をオンにした場合は、スケジュールを編集するかどうかを選択するよう求められます。**[OK]** をクリックすると、次のステップに示す [スケジュールされた検索の編集] ページが表示されます。**[キャンセル (Cancel)]** をクリックすると、検索が保存されますが、実行はスケジュールされません。

4. [スケジュールされた検索/警告の編集 (Edit Scheduled Search/Alert)] ページでは、保存した検索ジョブのスケジュールとアラートオプションを定義できます。必要なオプションを選択し、**[保存 (Save)]** をクリックします。パラメーターの詳細については、「アラートジョブのオプション」(342ページ) を参照してください。

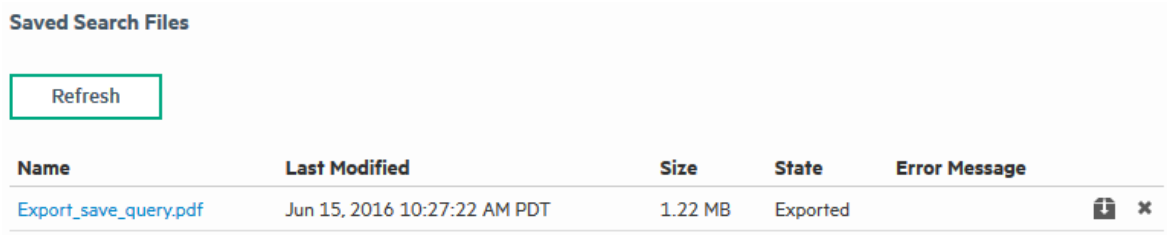


5. スケジュールされたアラートの作成後は、「スケジュールされた検索またはアラートを有効または無効にするには」(336ページ) の説明に従って、そのアラートを有効にしてください。

保存された検索ファイル

Loggerに保存された、保存された検索結果にアクセスするには、[保存された検索ファイル] コマンドを使用します。保存された検索ファイルを取得 (ブラウザーにストリーミング) または削除できます。ファイルの一覧を更新するには、[更新 (Refresh)] をクリックします。

[保存された検索ファイル (Saved Search Files)] ページ



以下のようにして、保存された検索結果にアクセスします。

1. [**設定 | 検索**] メニューを開き、[**保存された検索ファイル**] をクリックします。検索結果が格納されたファイルが表示されます。
2. ファイルをダウンロードして開くには、[名前] 列のリンクをクリックするか、その行の [**取得**] アイコンをクリックします。

検索インデックス

フィールドベースのインデックスにはいつでもフィールドを追加できます。ただし、**フィールドをインデックスに追加した後に、インデックスからフィールドを削除することはできません。**

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

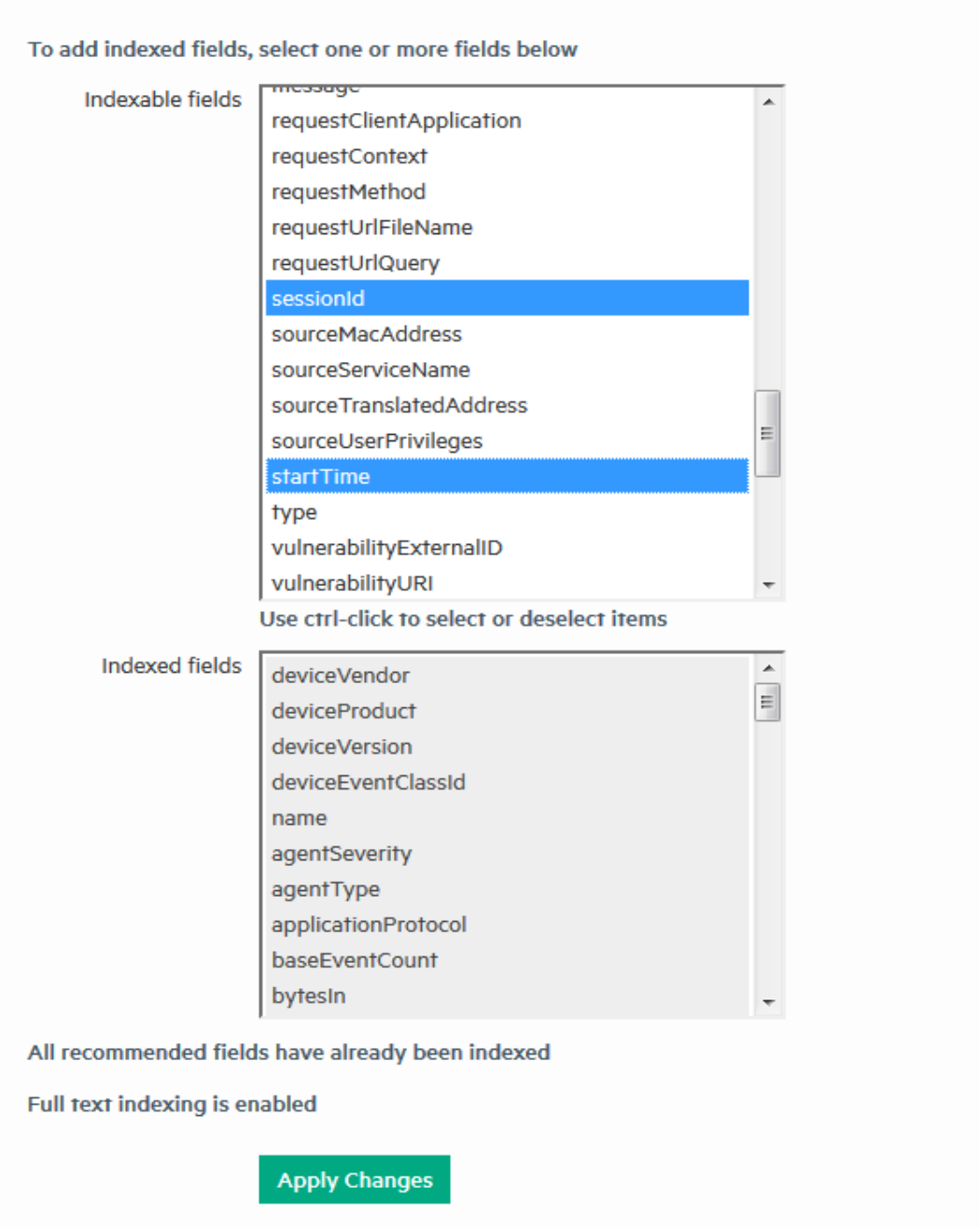
- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ) を参照してください。

注意: インデックスにフィールドを追加する前に、「フィールドベースのインデックス付けのガイドライン」(348ページ) に記載されている内容をよくお読みください。

フィールドベースのインデックスにフィールドを追加するには

1. [**設定 | 検索**] メニューを開き、[**検索インデックス**] をクリックします。
2. [インデックスを追加できるフィールド (Indexable fields)] リストからフィールドを選択します。



3. 複数のフィールドを選択するには、Ctrlキーを押しながらフィールドをクリックします。
4. [**変更を適用 (Apply Changes)**] をクリックします。

フィールドベースのインデックス付けのガイドライン

フィールドのインデックスを作成する前に、以下のガイドラインをよくお読みください。

- イベントは、[インデックスフィールド (Indexed fields)] リスト ([検索インデックス] ページ) のフィールドとデフォルトイベントメタデータフィールド (イベント時刻、Loggerイベント、デバイスアドレス) ごとにインデックス作成されます。
- Logger上でインデックス作成できるフィールドは123個までです。この数には、Loggerに追加したカスタムスキーマフィールドが含まれます。
- フィールドをインデックスに追加した後に、インデックスからフィールドを削除することはできません。
- システム管理グループに属するユーザーのみがフィールドをインデックスに追加できます。
- フィールドをインデックスに追加した後、Loggerによりそのフィールドに対するインデックス作成がすぐに開始されない可能性があります。そのため、フィールドを追加してから検索クエリでフィールドを使用するまで少し待ちます。Loggerでフィールドに対するインデックス作成を実行している最中に、そのフィールドを使用して検索クエリを実行すると、その操作の検索パフォーマンスが予想よりも低速になります。
- イベントフィールドに、予期せぬ型のデータが含まれている場合 (たとえば、整数が期待される場合に文字列)、データは無視されます。そのため、そのデータ値の検索では結果が生成されません。たとえば、ポートフィールドに8080 (英数字) ではなく値8080A (英数字) が含まれている場合、英数字の値は無視されます。
- レポート生成を高速化するためには、レポートのすべてのフィールド (レポートに表示されるフィールドを含む) にインデックスが作成されている必要があります。つまり、クエリのWHERE句のフィールドに加えて、SELECT句のフィールドにもインデックスを作成する必要があります。
- 最適な検索パフォーマンスのためには、クエリで指定した時間範囲について、すべてのピアのイベントフィールドにインデックスが作成されていることを確認してください。指定した時間範囲について、あるLoggerではイベントフィールドのインデックスが作成されていても、そのピアでインデックスが作成されていない場合、そのLoggerでの分散検索の実行が低速になります。ただし、ローカルLoggerでは最適な速度で実行されます。そのため、そのような設定での検索パフォーマンスは低下します。
- Logger 6.4 (ADP 2.6) 以降のリリースは、`requestUrl`フィールドのインデックス付けをサポートします。このフィールドは、World Wide WebからWebサイトアドレスを返します。`requestUrl`をインデックス付けすると、結果を返すまでにかかる時間を短縮できますが、検索結果のサイズが大幅に増加するので、検索ストレージ容量に影響を及ぼす可能性があります。

グローバル検索オプション

[検索オプションを編集] ページでは、管理者が、フィールド、フルテキスト、正規表現、および同時検索オプションのためのグローバル検索設定や、検索ディスプレイおよびフィールドサマリーオプションを設定できます。

これらのオプションを調整するには、[**設定 | 検索**] メニューを開き、[**検索オプション**] をクリックします。

ヒント: このページの検索オプションは、国際化 (i18n) された選択肢をサポートしています。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ) を参照してください。

グローバル検索オプションの設定

[検索オプションを編集] ページでは、Loggerのグローバル検索設定を設定できます。

Loggerグローバル検索設定を表示または変更するには

1. ナビゲーションバーで、[**設定 | 検索**] メニューから [**検索オプション**] をクリックします。[検索オプションを編集] ページが開きます。
2. 「検索オプションのパラメーター」(349ページ) の説明に従って、設定を表示または変更します。
3. [**保存**] をクリックして変更内容を保存します。

注: これらのオプションの一部では、Loggerアプライアンスのリブートか、ソフトウェアLoggerの再起動が必要です。

検索オプションのパラメーター

これらのパラメーターは、[検索オプションの詳細設定] ページで詳細なグローバル検索オプションを設定します。これらのオプションを調整するには、[**設定 | 検索**] メニューから [**検索オプション**] をクリックします。

フィールド検索オプション

オプション	説明
大文字と小文字を区別	デフォルト値: **はい** 検索時に大文字と小文字を区別するかどうかを制御します。このオプションが[いいえ]に設定されている場合、「login」を検索すると、「login」、「Login」、および「LOGIN」が見つかります。 このオプションを「**いいえ**」に設定すると、クエリパフォーマンスが影響を受ける可能性があります。 大文字と小文字の区別に対する変更は、ローカルなLoggerのみに適用されます。ピアLoggerでは、それ自身の設定が引き続き使用されます。 フルテキスト検索 (キーワード検索) では、大文字と小文字が区別されません。この大文字と小文字の区別の設定は変更できません。 **注:** この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。
NOT演算子の結果にNULLフィールド値を含める	デフォルト値: **いいえ** このオプションを[**はい**]に設定すると、NOT演算子を使用するクエリは、フィールド値がフィルター条件と一致するイベント、またはNULLのイベントを返すようになります。 デフォルトの[いいえ]を設定すると、NOT演算子を使用するクエリは、フィールド値がフィルター条件と一致するイベントのみを返すようになります。 **注:** この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。

フィールド検索の詳細については、「フィールドベースの検索」(73ページ)を参照してください。

フルテキスト検索オプション

プライマリ区切り文字を使用	デフォルト値: **はい** プライマリ区切り文字をイベントに適用して、インデックス作成用にトークン化するかどうかを制御します。 プライマリ区切り文字は、イベントをインデックス作成用にトークン化します。たとえば、イベント「john doe the first」は、プライマリ区切り文字「スペース」を使用して、「john」「doe」「the」「first」にトークン化されます。 プライマリ区切り文字は、次のとおりです。 スペース、タブ、改行、コンマ、セミコロン、( ) [ ] { } “ | *
セカンダリ区切り文字を使用	デフォルト値: **いいえ** セカンダリ区切り文字をイベントに適用して、プライマリ区切り文字によって作成されたトークンをさらにトークン化するかどうかを制御します。これにより、プライマリトークンの一部を照合する検索が可能になります。 たとえば、http://www.hpe.comの中の「hpe.com」を検索できます。 セカンダリ区切り文字は、次のとおりです。 ピリオド、= : / \ @ - ? # & _ > <

フルテキスト検索の詳細については、「キーワード検索 (フルテキスト検索)」(72ページ)を参照してください。

正規表現検索オプション

大文字と小文字を区別	デフォルト値: **いいえ** 「大文字と小文字を区別」(350ページ)を参照してください。 **注:** この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。
大文字と小文字を区別するUnicode	デフォルト値: **いいえ** 英語以外の言語のイベントを、大文字と小文字を区別して比較するかどうかを制御します。 **注意:** このオプションは変更しないことを強くお勧めします。 **注:** この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。

基準の同等性をチェック	デフォルト値: **いいえ** 英語以外の言語のイベントを、ロケール固有のアルゴリズムを使用して比較するかどうかを制御します。 **注意:** このオプションは変更しないことを強くお勧めします。 **注:** この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。

正規表現検索の詳細については、「正規表現ヘルパーツール」(100ページ)を参照してください。

検索表示オプション

syslog イベントの rawEvent フィールドを生成	デフォルト値: **いいえ** Raw Eventフィールドセットを使用して、rawEventという名前の書式設定された列に、rawイベントを表示するかどうかを制御します。このオプションは、syslogイベントのみに適用されます。CEFイベントに関連付けられたrawイベントを表示するには、この設定を行う必要はありません。その代わり、イベントをLoggerに送信しているコネクターが、rawEventフィールドにrawイベントを設定するように設定します。 **注:** rawEvent列にrawイベントが表示される場合でも、この列はLoggerデータベースに追加されず、インデックスが作成されません。そのため、このイベントに対しては、キーワード (フルテキスト) 検索または正規表現検索のみを実行できます。
ソースフィールドとソースタイプフィールドを表示	デフォルト値: **いいえ** [ソース] フィールドと [ソースタイプ] フィールドをフィールドサマリーとクエリ結果に含めるかどうかを制御します。 この変更を有効にするには、Loggerアプライアンスまたはソフトウェアの再起動が必要です。 **注:** このオプションを **[はい]** に設定すると、クエリパフォーマンスが影響を受ける可能性があります。

RAWイベントの詳細については、「[rawイベント] フィールドセット」(83ページ)を参照してください。フィールドサマリーおよびクエリ検索の詳細については、「ソースタイプ」(388ページ)を参照してください。

同時検索オプション

終了時間 (分)	デフォルト値: **10** 範囲: **1-60** 完了した検索が期限切れになる前に、Loggerメモリ内で使用可能な状態になっている時間を制御します。 • このオプションは、単一検索と同時検索の両方の有効期限を制御します。 • セッションIDをクリックすると、新しいタブに検索結果が表示され、有効期限がリセットされます。検索のためにページ番号リンクを使用する (表示ページ間を移動する) 場合にも、有効期限がリセットされます。
最大同時検索数	デフォルト値: **0** (検索数は無制限) 範囲: **1-1000** このLoggerが実行できる同時検索の数を制御します(ダッシュボードと保存された検索を含む)。

同時検索の詳細については、「同時検索」(111ページ) を参照してください。

フィールドサマリーオプション

フィールドサマリーの使用	デフォルト値: **はい** [フィールド サマリ] パネルを検索結果にデフォルトで含めるかどうかを制御します。デフォルトにかかわらず、[検索] 画面の [フィールド サマリ] チェックボックスを使用して、その場で設定を変更できます。
フィールドを検出	デフォルト値: **いいえ** フィールドサマリー機能で、rawイベント内の非CEFフィールドを自動的に検出するかどうかを制御します。デフォルトにかかわらず、[検索] 画面の [フィールドを検出] チェックボックスを使用して、その場で設定を変更できます。 このフィールドは、[フィールドサマリーの使用] に「No」が設定されていると表示されません。

[フィールド サマリ] パネルの詳細については、「フィールドサマリーパネル」(132ページ) を参照してください。フィールド検出の詳細については、「rawイベントデータでのフィールドの検出」(136ページ) を参照してください。

フィールドセットの管理

あらかじめ定義されたフィールドセットと、[フィールドセット (Fieldsets)] ページ (**[設定 | 検索] > [フィールドセット]**) で作成したフィールドセットを表示できます。

Fieldsets

Name	Type	Fields
Network, Routers, and Switches	System	Event Time, deviceVendor, deviceProduct, name, deviceEventClassId, sourceAddress, sourceHostName, sourcePort, destinationAddress, destinationHostName, destinationPort, transportProtocol, deviceAction, deviceSeverity, deviceAddress, deviceHostName, deviceCustomNumber2Label, deviceCustomNumber2, deviceCustomString2Label, deviceCustomString2, deviceCustomString3Label, deviceCustomString3, deviceCustomString5Label, deviceCustomString5, deviceCustomString6Label, deviceCustomString6, categoryDeviceGroup, categoryBehavior, categoryObject, categoryOutcome, categorySignificance, *user, Raw Message
NIDS	System	Event Time, deviceVendor, deviceProduct, name, deviceEventClassId, sourceAddress, sourceHostName, sourcePort, destinationAddress, destinationHostName, destinationPort, fileName, deviceCustomString2Label, deviceCustomString2, deviceCustomString3Label, deviceCustomString3, deviceCustomString4Label, deviceCustomString4, deviceCustomString5Label, deviceCustomString5, deviceCustomNumber1Label, deviceCustomNumber1, deviceAddress, deviceHostName, deviceSeverity, categoryDeviceGroup, categoryBehavior, categoryObject, categoryOutcome, categorySignificance, *user, Raw Message
VPN	System	Event Time, deviceVendor, deviceProduct, name, deviceEventClassId, message, deviceAction, sourceAddress, sourceTranslatedAddress, sourceHostName, destinationAddress, destinationHostName, transportProtocol, deviceAddress, deviceHostName, deviceSeverity, sourceUserName, destinationUserName, deviceCustomNumber1Label, deviceCustomNumber1, deviceCustomNumber2Label, deviceCustomNumber2, deviceCustomNumber3Label, deviceCustomNumber3, deviceCustomString1Label, deviceCustomString1, deviceCustomString2Label, deviceCustomString2, deviceCustomString3Label, deviceCustomString3, deviceCustomString4Label, deviceCustomString4, deviceCustomString5Label, deviceCustomString5, deviceCustomString6Label, deviceCustomString6, bytesIn, bytesOut, deviceInboundInterface, deviceOutboundInterface, categoryDeviceGroup, categoryBehavior, categoryObject, categoryOutcome, categorySignificance, *user, Raw Message

このフィールドセットリストで、「*user」は、ユーザーが作成したフィールドを示します。フィールドリストの最後にあるアスタリスク (*) は、表示しきれないフィールドが含まれていることを示します。

[フィールドセットの編集、保存および削除] 特権がある場合は、この画面からカスタムフィールドセットを削除できます。

注: 削除できるのは自分が作成したフィールドセットのみであり、Loggerであらかじめ定義されているフィールドセットは削除できません。

カスタムフィールドセットを削除するには

1. **[設定 | 検索]** メニューを開き、**[フィールドセット]** をクリックします。
2. 削除するフィールドセットを探し、[削除] アイコン (✖) をクリックします。
3. 削除を確定します。

デフォルトのフィールド

Loggerスキーマには、あらかじめ定義されたフィールドセットが付属しています。これらのフィールドの一部は、検索速度と効率を高めるために、あらかじめインデックスが作成されています。カスタムフィールドをLoggerスキーマに追加し、フィールドベースの検索用にインデックス作成することができます。フィールドベースの検索では、このスキーマ内のフィールドのみを使用できます。

注: スキーマ内の各フィールドのサイズはあらかじめ決められています。検索対象の文字

列がフィールド長よりも長い場合は、=検索ではなくSTARTSWITHを使用し、フィールドサイズを超えない文字数を含めることをお勧めします。詳細については、「フィールドベースの検索」(1ページ)を参照してください。

[デフォルト フィールド] ページ (**[設定 | 検索] > [デフォルト フィールド]**) には、スキーマに含まれている定義済みのフィールドが表示されます。これには、各デフォルトフィールドの表示名、タイプ、長さ、およびフィールド名が含まれています。現在あるカスタムフィールドの情報を表示する方法については、「カスタムフィールド」(356ページ)を参照してください。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

デフォルトのスキーマフィールドを表示するには、次の操作を実行します。

1. [検索] の下の [設定] メニューで **[デフォルト フィールド]** をクリックします。

	sessionId	LONG	-	sessionId	-
■	sourceAddress	TEXT	16	src	Superindexed
■	sourceHostName	TEXT	100	shost	Superindexed
	sourceMacAddress	LONG	-	smac	-
■	sourceNtDomain	TEXT	100	sntdom	Indexed
■	sourcePort	LONG	-	spt	Superindexed
■	sourceProcessName	TEXT	30	sproc	Indexed
	sourceServiceName	TEXT	30	sourceServiceName	-
	sourceTranslatedAddress	TEXT	-	sourceTranslatedAddress	-
■	sourceUserId	TEXT	100	suid	Superindexed
■	sourceUserName	TEXT	100	suser	Superindexed

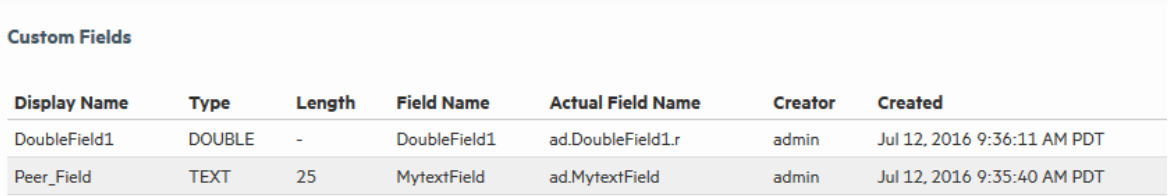
2. [デフォルト フィールド] ページにデフォルトのスキーマフィールドが表示されます。列見出しをクリックすると、フィールドをソートできます。

   Loggerは、各フィールドのインデックスステータスを次の2つの方法で表示します。

   - **[インデックス付き (Indexed)]** 列には、インデックス付きフィールドとスーパーインデックス付きフィールドが表示されます。
   - **[表示名]** フィールドには、インデックス付きフィールド用の薄い緑色のアイコン(■)と、スーパーインデックス付きフィールド用の深緑色のアイコン(■)があります。インデックスが作成されていないフィールドにはアイコンはありません。

カスタムフィールド

Loggerスキーマに追加されたカスタムフィールドは、[設定 | 検索] > **[カスタム フィールド]** で確認できます。



Custom Fields

Display Name	Type	Length	Field Name	Actual Field Name	Creator	Created
DoubleField1	DOUBLE	-	DoubleField1	ad.DoubleField1.r	admin	Jul 12, 2016 9:36:11 AM PDT
Peer_Field	TEXT	25	MytextField	ad.MytextField	admin	Jul 12, 2016 9:35:40 AM PDT

このページには、保存されているすべてのカスタムフィールドが一覧表示されます。フィールドのアルファベット順のリストを表示できますが、編集や削除はできません。カスタムフィールドの詳細については、「スキーマへのフィールドの追加」(461ページ)を参照してください。

実行中の検索

検索の実行中、または検索が期限切れになっていないか削除されていない間は、[実行中の検索] ページで、検索クエリ(検索結果ではない)の詳細を確認できます。

[実行中の検索] ページには、以下の検索タイプが表示されます。

- ローカルまたはピアのLogger上の手動検索 (**[分析] > [検索]**)「検索の実行」(107ページ)を参照してください。
- スケジュールされた検索 (**[設定 | 検索] > [スケジュールされた検索/アラート]**)「スケジュールされた検索/アラート」(335ページ)を参照してください。
- 保存された検索アラート (**[設定 | 検索] > [保存された検索]**)「保存された検索」(333ページ)を参照してください。
- [クエリを再実行してください] オプションをオンにした状態での検索エクスポート (**[分析] > [検索] > [結果のエクスポート]**)

このページは、次のような問題が生じていないかどうかを確認するのに役立ちます。

- 検索が応答してない
- 検索の実行に時間がかかり過ぎている
- 検索によってLoggerの全体のパフォーマンスが低下している
- メモリ内の同時検索オプションが多すぎる

前提条件

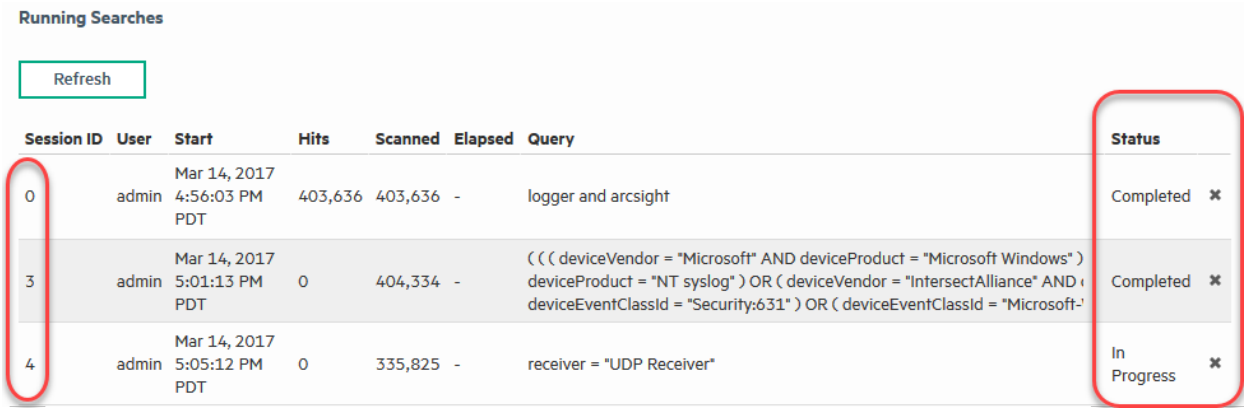
実行中の検索プロセスを終了するには、adminユーザー特権が必要です。Loggerのユーザー権限とその管理方法の詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

[実行中の検索] ページを表示するには

[設定 | 検索] > [実行中の検索] をクリックします。

実行中の検索のリスト

このリストには、セッションID、タスクを開始したユーザー、タスクが開始された日時、一致した検索数、スキャンされたイベント数、経過時間、クエリ、実行ステータス、および削除アイコン ✖ が表示されています。



現在実行中の検索を表示するには

[設定 | 検索] メニューを開き、**[実行中の検索]** をクリックします。
現在実行中の検索が表示されます。

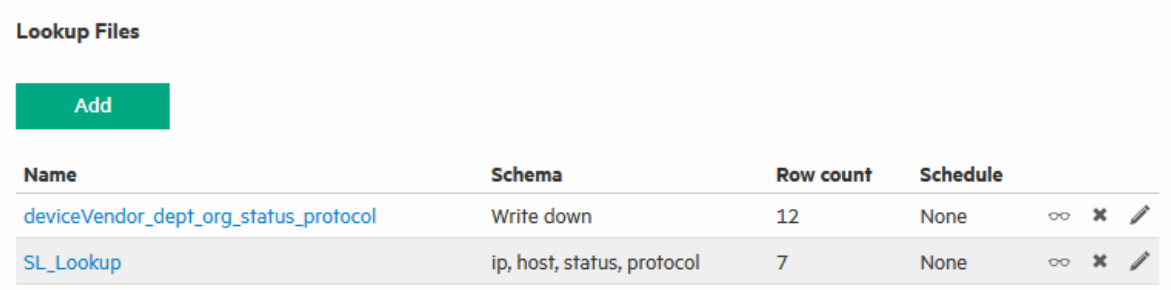
現在実行中の検索を終了するには

1. **[設定 | 検索]** メニューを開き、**[実行中の検索]** をクリックします。
2. 検索プロセスを停止するには、タスクの ✖ アイコンをクリックします。

ルックアップファイル

ルックアップファイルは、検索時のLoggerデータを補強するために、lookup検索演算子によって使用されます。有効なルックアップファイルをLoggerにアップロードした後、そのルックアップファイルを検索コマンドlookupで使用できます。

[ルックアップ ファイル (Lookup Files)] ページには、アップロードされたルックアップファイルが表示されています。



- lookup演算子を使用すべき場合については、「静的相関関係を通じたLoggerデータの強化」(152ページ)を参照してください。
- 検索時にlookup演算子を使用する方法については、「lookup」(580ページ)を参照してください。

ルックアップファイルの作成

ルックアップファイルは、CSV形式で、先頭行がルックアップフィールド名になっている必要があります(ルックアップフィールドは、ルックアップファイル内の独立した列です)。テーブルの各行は、順番に読み込まれ、最初の行が表内の列の定義として扱われます。行に含まれるカンマ区切り値の数が最初の行と同じではない場合、その行はlookup演算子による検索の際にスキップされます。lookup演算子を使用した検索で、1つ以上の行をスキップする必要がある場合、警告メッセージが検索ページに表示されます。この表をMicrosoft Excelなどのツールでチェックし、各行にヘッダー行と同じ数の列があることを確認してから、ルックアップファイルとしてアップロードすることをお勧めします。

ヒント: ルックアップファイルが従う必要のあるCSV形式の詳細については、RFC 4180を参照してください。

ルックアップファイルの命名

ルックアップファイルの名前に使用できる文字は、英数字とアンダースコアのみで、先頭には数字を使用できません。ファイル名に+、-、*を含めないでください。これらの文字はlookupコマンド用に予約されています。

ルックファップファイルの名前を短く分かりやくすると、出力の中でルックアップフィールドを識別しやすくなります。Loggerのフィールドと区別するために、ルックアップファイルから取得したフィールドには、検索結果に表示される際に、ルックアップファイル名の先頭の6文字が追加されます。

たとえば、以下の検索を見てください。

```
lookup _table_20160608 ip as src output hostname
```

この例では、「_table_」がルックアップフィールド「hostname」に追加されます。日付(20160608)は含まれません。ルックアップファイル名の先頭の6文字のみが追加されるため、検索結果に表示される名前は、「hostname_table_」になります。

ルックアップファイルのフィールドの命名

ルックアップフィールド名には、英数字とアンダースコアのみを使用でき、先頭には数字を使用できません。フィールド名に+、-、*を含めないでください。これらの文字はlookupコマンド用に予約されています。

ルックアップファイル内の重複する値

ルックアップ列の複数の行に同じ値が含まれる場合、ルックアップ操作では、一致する最初の行のみが使用され、以降の一致は無視されます。

Loggerのエクスポートされた検索結果をルックアップファイルとして使用する場合は、「dedup」演算子を使用して、ルックアップフィールドとして使用されるフィールド内の重複する値を削除できます。ルックアップフィールドの重複の詳細については、lookup演算子を参照してください(「lookup」(580ページ))。dedup演算子の詳細については、「dedup」(569ページ)を参照してください。

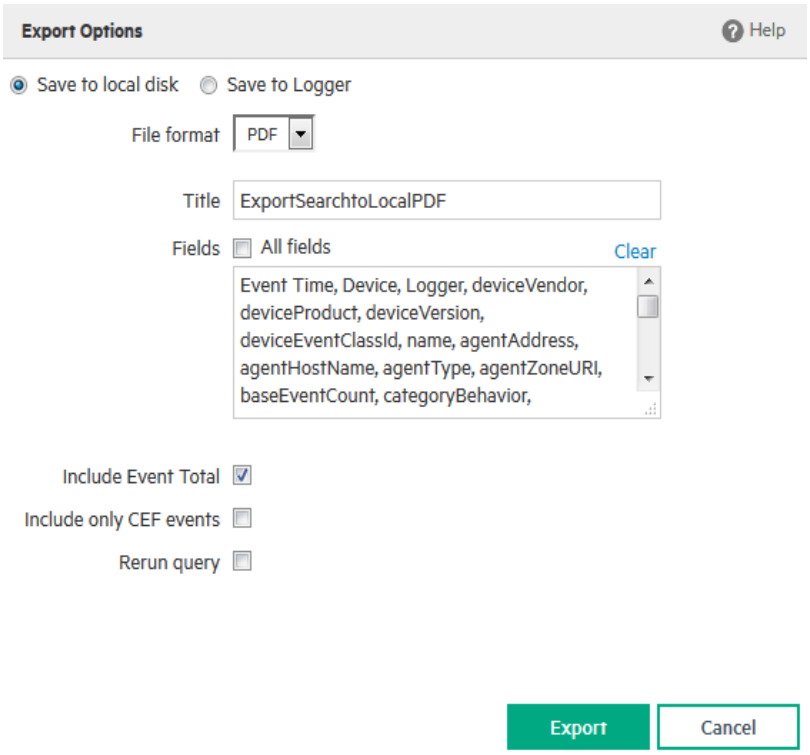
ルックアップの容量

- アップロードできるルックアップファイルの最大サイズは50MBです(非圧縮または圧縮)。
- ルックアップファイルを格納するために割り当てられる最大ディスク領域は1GBです。これは、すべてのルックアップファイルを格納するために許可されるディスク領域全体の上限です。
- ルックアップエントリの最大数は5,000,000です(ルックアップファイル内の1つのカンマ区切り値が、1個のルックアップエントリになります)。

  たとえば、ルックアップファイルの列数が4で、行数が10の場合、ルックアップエントリの総数は4x10=40です。そのようなルックアップファイルを検索で使用すると、そのすべてのエントリがメモリにロードされます。ルックアップ用にロードされる最大行数は、ルックアップファイルの列数によって異なります。

  たとえば、ルックアップファイルに含まれている列数が500の場合、ルックアップで許容される最大行数は、5,000,000/500 = 10,000行となり、以降の行は使用されません。これに対し、表の列数が4のみの場合、ルックアップで許容される最大行数は5,000,000/4 = 1,250,000行です。

  Loggerの検索結果をエクスポートしてルックアップファイルとして使用する場合は、[**すべてのフィールド (All Fields)**] チェックボックスをオフにし、必要なフィールドのみをエクスポートしてください。



全体のルックアップエントリ数は500万に制限されているため、必要なフィールドのみをエクスポートすることで、ルックアップ用にロードされる行数が減ります。

ルックアップファイルのアップロード

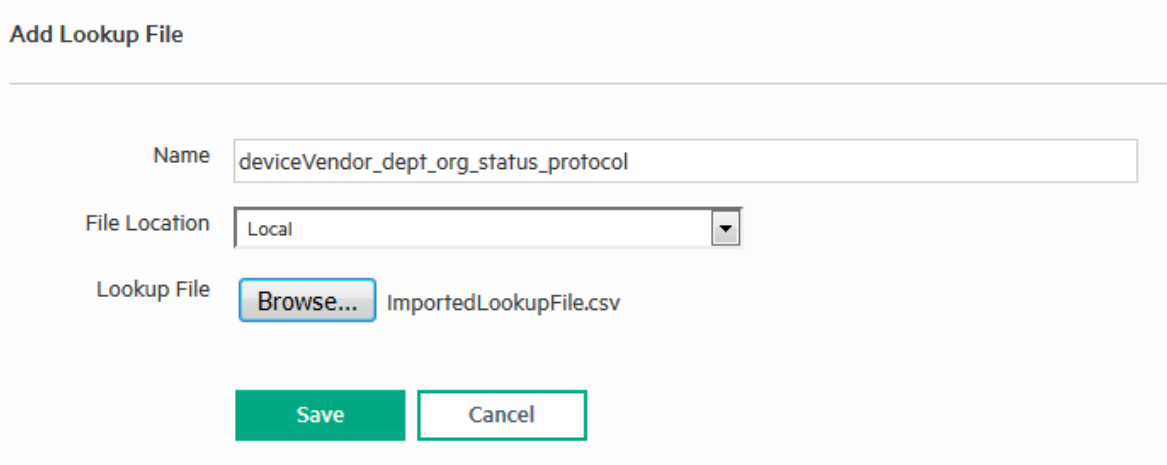
[ルックアップ ファイル] ページの [**追加**] をクリックして、.csv、.zip、または.gz形式のルックアップファイルをアップロードします。個別のルックアップファイルをローカルデスクトップからアップロードするか、Loggerがアクセス可能な場所からルックアップファイルを定期的にアップロードするようスケジュールすることができます。

非圧縮ファイル(.csv形式でアップロードされるファイル)は、.zip形式に圧縮されて、ユーザーが指定した名前 (<名前>.zip) で保存されます。圧縮ファイルは、元の圧縮形式で、指定した名前 (<名前>.zipまたは<名前>.gz) でアップロードおよび保存されます。できるだけ圧縮したルックアップファイル(.zipまたは.gz) をアップロードしてください。これにより、アップロード時間が短縮され、同じアップロードファイルサイズでより多くの情報がロードされるようになります。それぞれの.zipファイルまたは.gzファイルには、1つのルックアップファイルのみを.csvフォーマットで格納できます。

検索時にlookup演算子を使用する方法については、「lookup」(580ページ) を参照してください。

ルックアップファイルを追加するには

1. **[設定 | 検索]** メニューを開き、**[ルックアップ ファイル]** をクリックします。
2. **[追加]** をクリックします。[ルックアップ ファイルの追加 (Add Lookup File)] ページが開きます。



3. ルックアップファイルの意味のある名前を入力します。この名前には、英数字とアンダースコアのみを使用でき、先頭には数字を使用できません。名前に+、-、*を含めないでください。これらの文字はlookupコマンド用に予約されています。
4. ルックアップファイルにアクセスする場所を選択します。
   - ローカルマシン上の場所を参照して、ファイルを一度だけアップロードするには、**[ローカル (Local)]** を選択します。
   - Loggerのサーバー上のパスを入力するには、**[Logger上 (On Logger)]** を選択します。このオプションを選択すると、定期的な更新スケジュールを設定できます。

   使用可能なオプションは、選択によって異なります。
5. ルックアップファイルの場所を指定します。
   - **[ローカル]** を選択した場合は、**[参照... (Browse...)]** をクリックし、目的の.csv、.zip、または.gzファイルを参照して、**[開く]** をクリックします。
   - **[Logger上]** を選択した場合は、Loggerシステム上の絶対パスとファイル名を指定します。たとえば、ファイルがLogger上の/optフォルダーにある場合は、`/opt/lookup.csv`のように指定します。ルックアップファイルは、この場所にすでに存在している必要があります。Loggerをインストールしたユーザーは、ルックアップファイルと、ここで指定するディレクトリに対する読み取り権限を持っている必要があります。

     注: Loggerアプライアンスは、ユーザーインターフェイスによるマウントをサポートしています。ソフトウェアLoggerは、そのファイルシステムを使用します。これには、オペレーティングシステムによってマウントされたリモートフォルダーが含まれていてもかまいません。

6. [**Logger上**] を選択した場合は、ルックアップファイルをアップロードする頻度を指定します。
   - ルックアップファイルを一度だけアップロードする場合は、[**一度だけ (One time only)**] をオンにします。
   - ルックアップファイルを今すぐアップロードし、スケジュールされた間隔で定期的にアップロードするようにスケジュールするには、[**一度だけ**] をオフにして、スケジュールを選択します。その後、スケジュールオプションを使用して、ルックアップファイルを更新する頻度をしています。これらのオプションの詳細については、「日付と時刻のスケジュールのオプション」(150ページ) を参照してください。
7. **[保存 (Save)]** をクリックします。アップロードされたルックアップファイルは、ルックアップファイルのリストに表示されます。スケジュールを指定した場合は、ルックアップ処理によって、指定された時間に指定された場所が調べられ、新しいバージョンがあればアップロードされます。

アップロードされたルックアップファイルの管理

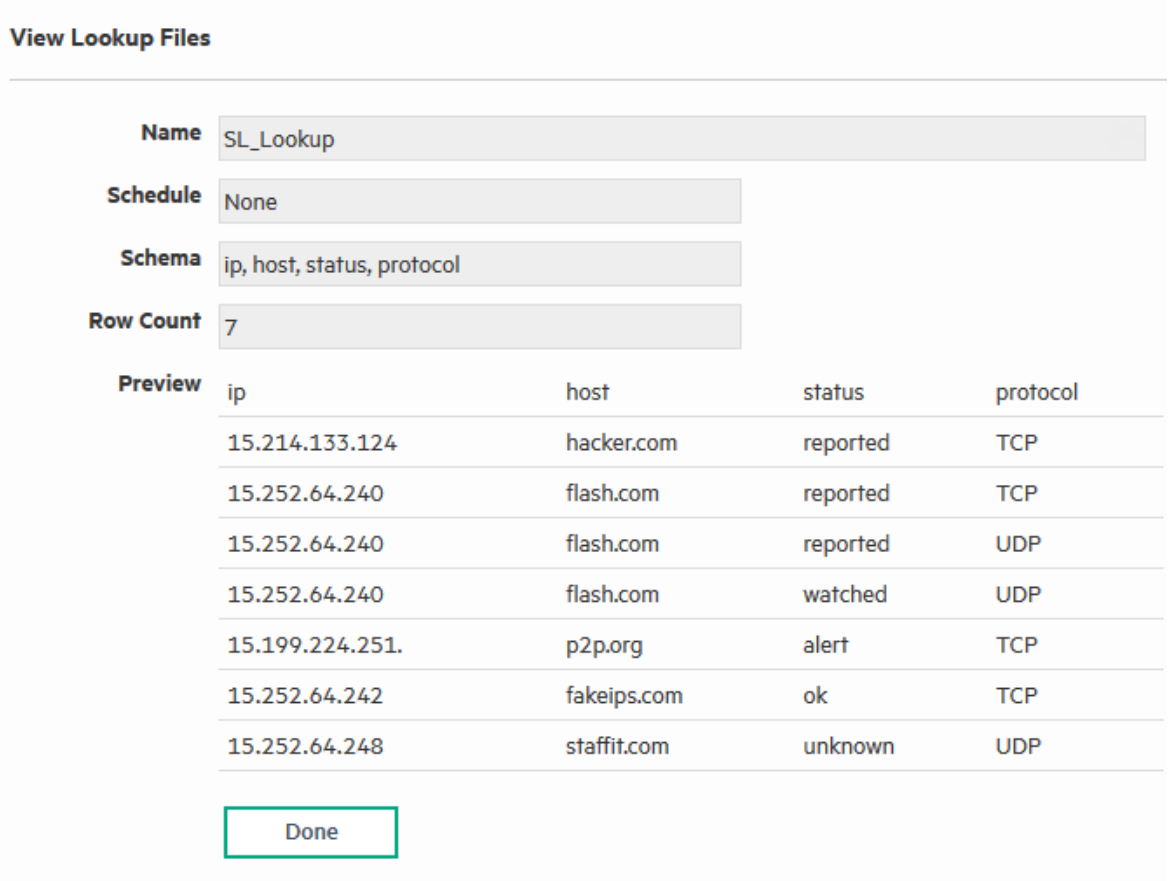
ルックアップファイルのアップロード後は、そのファイルに対応する行の最後にあるアイコンを使用して、ファイルを表示、編集、または削除することができます。

アップロードされたルックアップファイルを表示するには

1. **[設定 | 検索]** メニューを開き、**[ルックアップ ファイル]** をクリックします。
2. 表示するルックアップファイルを探して、表示アイコン (👓) またはルックアップファイルの名前をクリックします。

   このビューでは、数行のみが表示されます。ファイル全体は表示されません。

   注: [スケジュール (Schedule)] フィールドは、ルックアップフィールドが更新のためにスケジュールされている場合にのみ表示されます。



3. **[完了 (Done)]** をクリックし、[ルックアップ ファイル (Lookup files)] リストに戻ります。ここからファイルを編集することはできません。変更を加える必要がある場合は、「ルックアップファイルを編集するには」(363ページ) の手順に従ってください。

ルックアップファイルを削除するには

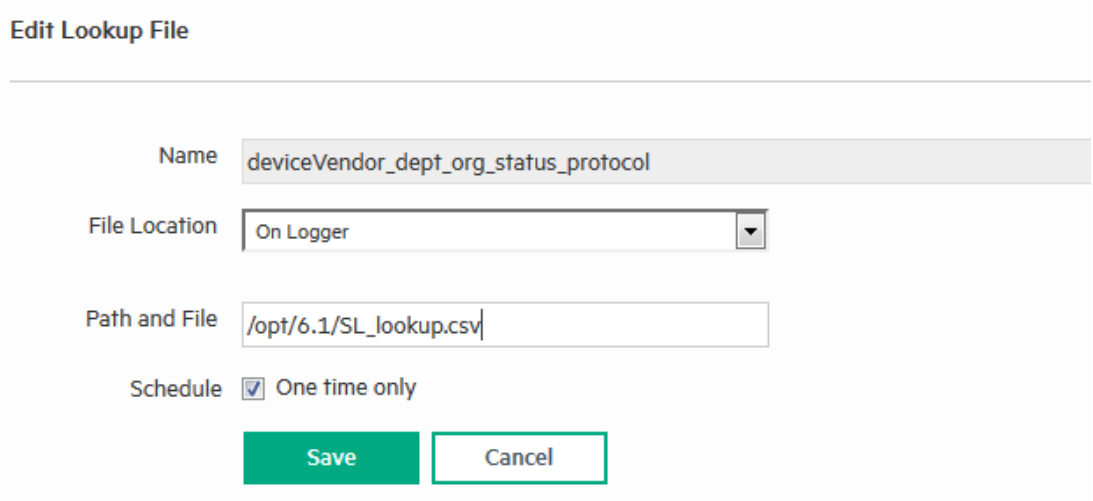
1. **[設定 | 検索]** メニューを開き、**[ルックアップ ファイル]** をクリックします。
2. 削除するルックアップファイルを探し、その行の [削除] アイコン (✖) をクリックして、**[OK]** をクリックします。

注: 現在の検索セッションでまだ使用されているルックアップファイルを削除しようとすると、エラーメッセージが表示されます。ファイルは削除されません。そのようなファイルを検索キャッシュから素早くクリアして、削除できるようにするには、lookup演算子を使用しない検索を実行します。これによりルックアップ検索セッションが終了し、ルックアップファイルは使用中でなくなります。セッションの終了後に、ルックアップファイルを削除できます。

ルックアップファイルを編集するには

1. **[設定 | 検索]** メニューを開き、**[ルックアップ ファイル]** をクリックします。

2. 編集するルックアップファイルを探し、その行の [編集] アイコン ( ) をクリックして、**[OK]** をクリックします。[ルックアップ ファイルを編集 (Edit Lookup File)] ページが開きます。



新しいバージョンのルックアップファイルのアップロード、ルックアップ更新のスケジュール、または既存の更新スケジュールの変更を行うことができます。

3. ルックアップファイルにアクセスする場所を選択します。
   - ローカルマシン上の場所を参照して、ファイルを一度だけアップロードするには、[**ローカル**] を選択します。
   - Loggerのサーバー上のパスを入力するには、[**Logger上**] を選択します。このオプションを選択すると、定期的な更新スケジュールを設定できます。

   使用可能なオプションは、選択によって異なります。
4. ルックアップファイルの場所を指定します。
   - [**ローカル**] を選択した場合は、[**ブラウズ**] をクリックして、目的の`.csv`、`.zip`または`.gz`ファイルに移動してから [**開く**] をクリックします。
   - [**Logger上**] を選択した場合は、Loggerシステム上の絶対パスとファイル名を指定します。たとえば、ファイルがLogger上の/optフォルダーにある場合は、`/opt/lookup.csv`を指定できます。ルックアップファイルは、この場所に既に存在している必要があります。

     注: Loggerアプライアンスは、ユーザーインターフェイスによるマウントをサポートしています。ソフトウェアLoggerは、ファイルシステムを使用します。これには、オペレーティングシステムによってマウントされたリモートフォルダーが含まれていてもかまいません。
5. [**Logger**] を選択した場合は、ルックアップファイルをアップロードする頻度を指定します。
   - ルックアップファイルを一度だけアップロードする場合は、[**一度だけ**] をオンにします。
   - ルックアップファイルを今すぐアップロードし、スケジュールされた間隔で定期的にアップロードするようにスケジュールするには、[**一度だけ**] をオフにして、スケジュールを選択し

ます。スケジューリングの詳細については、「日付と時刻のスケジュールのオプション」(150ページ)を参照してください。

6. **[保存 (Save)]** をクリックします。アップロードされたルックアップファイルは、ルックアップファイルのリストに表示されます。スケジュールを指定した場合は、ルックアップ処理によって、指定された時間に指定された場所が調べられ、新しいバージョンがあればアップロードされます。

データ

[設定 | データ] カテゴリのオプションを使用すると、Loggerとの間で入力または出力されるデータを制御できます。

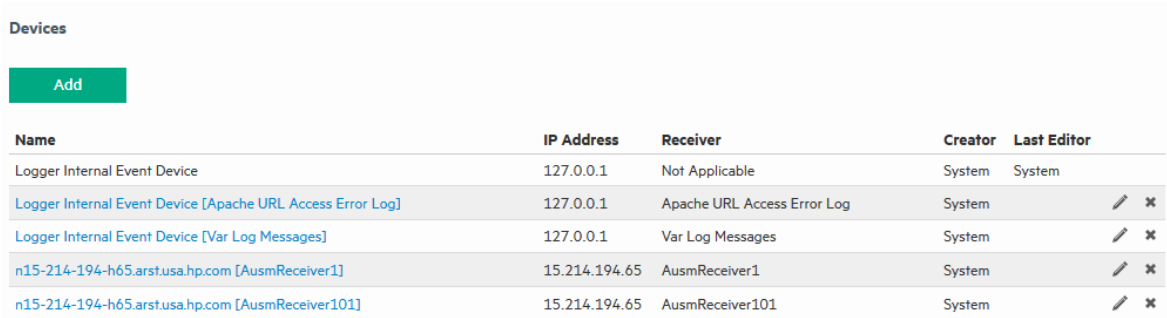
デバイス

デバイスは、名前が付けられたイベントソースであり、IPアドレス (またはホスト名) と受信者名からなります。2つの受信者が同じIPアドレスからのイベントを受信できるため、IPアドレスだけではデバイスを識別するのに不十分です。イベントソースは、イベントを直接Loggerに送信するデバイスです。イベントがSmartConnectorを介して送信されるときのイベントソースはSmartConnectorが動作しているシステムであり、SmartConnectorにイベントを送信したデバイスではありません。

デバイスをデバイスグループに追加することができ、デバイスグループをフィルターやクエリで参照できます。受信者は、各ソースIPアドレスに対してデバイスを自動的に作成することで、自動検出を実行します。自動検出によって作成されたデバイスの名前には、ホスト名か、ホスト名が特定できない場合はIPアドレスが使用されます。

[デバイス] ページには、定義済みのすべてのデバイスが表示され、デバイスを追加、編集、削除するためのコントロールが含まれています。

[デバイス (Devices)] ページ



Loggerで定義可能なデバイスの最大数: 制限なし。

自動検出によりデバイスが自動的に作成されますが、手動で定義することもできます。

デバイスを定義するには

1. **[設定 | データ]** メニューを開き、**[デバイス]** をクリックします。
   「[デバイス (Devices)] ページ」(366ページ) と似た画面が表示されます。
2. **[追加 (Add)]** をクリックします。
3. 新しいデバイスの名前とIPアドレスを入力し、受信者を選択します。
4. **[保存]** をクリックして新しいデバイスを追加するか、**[キャンセル]** をクリックして中止します。

デバイスを編集する理由の1つは、自動検出によって作成されるデフォルトの名前 (IPアドレスまたはホスト名) を、よりわかりやすい名前で置き換えることです。

デバイスを編集するには

1. **[設定 | データ]** メニューを開き、**[デバイス]** をクリックします。
   「[デバイス (Devices)] ページ」(366ページ) と似た画面が表示されます。
2. 編集するデバイスを探し、その行の [編集] アイコン ( ) をクリックします。
3. デバイスの名前またはIPアドレスを変更します。
4. **[保存]** をクリックしてデバイスグループを更新するか、**[キャンセル]** をクリックして変更内容を破棄します。

デバイスを削除するには

1. **[設定 | データ]** メニューを開き、**[デバイス]** をクリックします。
   「[デバイス (Devices)] ページ」(366ページ) と似た画面が表示されます。
2. 削除するデバイスを探し、その行の [削除] アイコン ( ) をクリックします。

デバイスを削除しても、ソースIPアドレスによるイベントの送信がブロックされるわけではありません。新しいイベントが受信されると、自動検出によってデバイスが再作成されます。

3. **[OK]** をクリックして削除を確定するか、**[キャンセル]** をクリックしてデバイスを保持します。

デバイスグループ

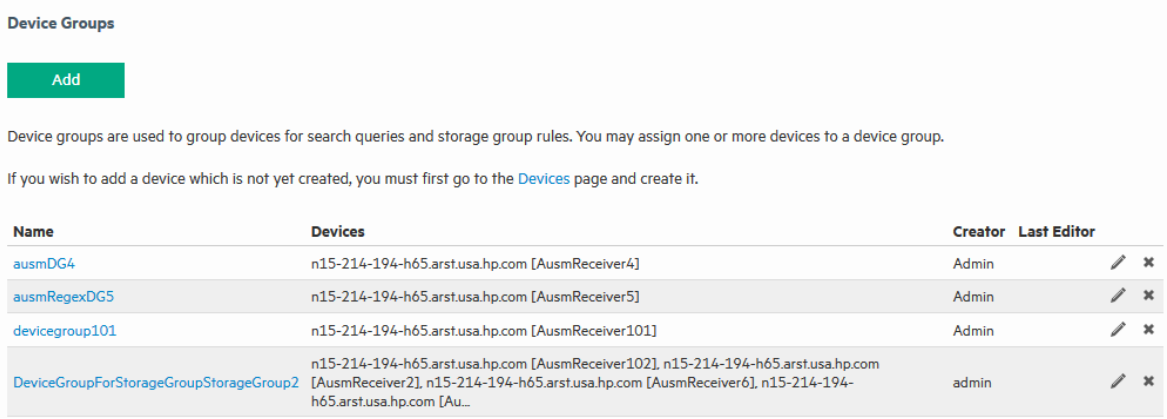
デバイスグループを使用すると、デバイスと呼ばれる、名前付きソースIPアドレスを分類できます。[デバイス グループ] ページには、すべてのデバイスグループのリストが編集および削除アイコンとともに表示されます。新しいデバイスグループを作成することもできます。

ヒント: デバイスグループは、特定のデバイスの格納先となるストレージグループを定義するストレージルールに関連付けることができます。そうすることで、さまざまなソースからのイベントデータをさまざまな期間にわたって保持できます (さまざまなストレージグループに対して、さまざまな保有ポリシーを定義できるため)。ストレージルールの詳細については、「ストレージルール」(430ページ) を参照してください。

ヒント: Loggerで作成可能なデバイスグループの最大数の制限はありません。

デバイスグループを作成するには

1. **[設定 | データ]** メニューを開き、**[デバイス グループ]** をクリックします。
2. **[追加 (Add)]** をクリックします。次に示すような画面が表示されます。



3. 新しいデバイスグループの名前を入力します。クリックしてリストからデバイスを選択します。デバイスを選択に追加するには、**Ctrl**キーを押したままクリックします。ある範囲のデバイスを選択するには、最初のデバイスをクリックして選択した後、**Shift**キーを押したまま最後のデバイスをクリックします。
4. **[保存]** をクリックして新しいデバイスグループを作成するか、**[キャンセル]** をクリックして中止します。

デバイスグループを編集するには

1. [**設定 | データ**] メニューを開き、[**デバイス グループ**] をクリックします。
2. 編集するデバイスグループを探し、その行の [編集] アイコン ( ) をクリックします。
3. 名前を変更するか、デバイスを選択に追加または削除します。選択されていないデバイスを選択したり、選択済みのデバイスを選択から削除するには、Ctrlを押したままクリックします。
4. [**保存**] をクリックしてデバイスグループを更新するか、[**キャンセル**] をクリックして変更内容を破棄します。

デバイスグループを削除するには

1. [**設定 | データ**] メニューを開き、[**デバイス グループ**] をクリックします。
2. 削除するデバイスグループを探し、その行の [削除] アイコン ( ) をクリックします。デバイスグループを削除しても、デバイスには影響がありません。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてデバイスグループを保持します。

受信者

Loggerは、ネットワークを通じて送信されるか、ファイルから読み込んだテキストイベントを受信できます。[受信者] ページからイベントデータをキャプチャーする受信者を設定し、各イベントにその送信元に関する情報を設定できます。一部の受信者は、デバイス、アプリケーション、サービスなどによってネットワークを介して送信されたストリーミングイベントをキャプチャーできます。他の種類の受信者は、指定されたパターンに基づいて、個別のファイルのイベントを監視するか、ディレクトリツリーから選択されたファイルを監視します。受信者は、単一のソースタイプのイベントのみを受信できるため、ログファイルの種類ごとに個別の受信者を設定する必要があります。

イベントの受信を開始するには、イベントソースをデフォルト受信者に送信します。デフォルト受信者の詳細については、『Loggerインストールガイド』を参照してください。

受信者のタイプには、UDP、TCP、SmartMessage、およびファイル転送、ファイル受信者、フォルダーフォロアー受信者の3種類のファイルベースの受信者があります。

受信者がデータを受信するには、リッスンしているポートが事前にファイアウォールによって開かれている必要があります。詳細については、「ファイアウォールルール」(558ページ) を参照してください。

以下の種類の受信者を設定できます。

- **UDP受信者**: UDP受信者は、指定したポート上でUDPメッセージをリッスンします。Loggerでは、UDP受信者がポート514または8514であらかじめ設定されていて、デフォルトで有効になっています。ソフトウェアLoggerの場合、このポートは、インストール時に利用で

きるポート番号に基づいて変わる可能性があります。

- **CEF UDP受信者**: 共通イベントフォーマットのイベントを受信するUDP受信者です。
- **TCP受信者**: TCP受信者は、指定したポート上でTCPメッセージをリッスンします。Loggerでは、TCP受信者がポート515または8515であらかじめ設定されていて、デフォルトで有効になっています。ソフトウェアLoggerの場合、このポートは、インストール時に利用できるポート番号に基づいて変わる可能性があります。
- **CEF TCP受信者**: 共通イベントフォーマットのイベントを受信するTCP受信者です。
- **Event Broker受信者**: Event Broker受信者は、Event Brokerのパブリッシュ-サブスクライブメッセージングシステムのコンシューマーです。これらはイベントトピックにサブスクライブしており、Event Brokerから共通イベントフォーマット(CEF)でイベントを受信します。
- **フォルダーフォロワー受信者**: フォルダーフォロワー受信者は、指定したディレクトリ内のログファイルが更新されると、継続的にそれを読み取ります。ソースディレクトリに異なる種類のログファイルが格納されている場合、監視するファイルの種類ごとに受信者を作成できます。Loggerには、LoggerのApacheアクセスエラーログ、システムメッセージログ、およびシステム監査ログ(監査が有効になっている場合)用のあらかじめ設定されたフォルダーフォロワー受信者があります。これらの受信者を使用するには、有効化する必要があります。
- **ファイル転送**: ファイル転送受信者は、SCP、SFTP、またはFTPプロトコルを使用してリモートログファイルを読み込みます。これらの受信者は、単一行または複数行のログファイルを読み込みます。1つまたは複数のファイルを定期的に読み込むように受信者をスケジュールできます。

  注: ファイル転送受信者の設定時は、以下の点に注意してください。

  - SCP、SFTP、およびFTPファイル転送受信者は、システムにインストールされているFTP (File Transfer Protocol)、SCP (Secure Copy Protocol)、およびSFTP (SSH File Transfer Protocol) クライアントを利用します。受信者を作成する前に、システムに適切なクライアントがインストールされていることを確認してください。
  - Loggerアプライアンス上のSCPおよびSFTPプロトコルは、FIPSに準拠していません。

- **SmartMessage受信者**: SmartMessage受信者は、ArcSight SmartConnectorからの暗号化されたメッセージをリッスンします。Loggerでは、SmartMessage受信者が「SmartMessage受信者」という名前であらかじめ設定されています。この受信者を使用してSmartConnectorからイベントを受信するには、SmartConnectorの通知先の設定時に、[**Receiver Name**] を「SmartMessage Receiver」に設定します。SmartConnectorの詳細については、「SmartConnectorを使用したイベントの収集」(599ページ)を参照してください。

Event Broker受信者

LoggerのEvent Broker受信者は、ArcSight Data Platform Event Brokerに接続して、サブスクライブ先のトピックについてのすべてのイベントを取得します。Event Brokerからイベントを

受信しているLoggerは、配布や冗長性のバランスを取るために、Loggerのプールの一部を構成することができます。イベントは、プール内のLogger間でラウンドロビン式に配布されます。プール内の1つのLoggerがダウンした場合、イベントは他のいずれかのLoggerに送信されます。

同一のイベントトピックリストにサブスクライブしていて、同一のコンシューマーグループに属しているEvent Broker受信者を持つ複数のLoggerを設定できます。グループ内の各LoggerEvent Broker受信者は、トピック内のパーティションのさまざまなサブセットからイベントを受信します。Event Brokerは、同一のコンシューマーグループ内で設定されているすべてのEvent Broker受信者間でパーティションのバランスを取ります。

イベントはArcSight SmartConnectorによってEvent Brokerへパブリッシュされます。データをEvent Broker受信者に送信するようにSmartConnectorを設定する場合は、[Event Broker]オプションを使用します。

Event Broker受信者を設定する前に、Loggerとイベントブローカー間で双方向認証をセットアップする必要があります。詳細と手順については、「イベントブローカー認証」(370ページ)を参照してください。

ArcSight Event Brokerについて詳しくは、『ArcSight Event Broker User's Guide』を参照してください (Protect 724のArcSight製品マニュアルのコミュニティからダウンロード可能)。

SmartConnectorについて詳しくは、『SmartConnectorユーザーガイド』を参照してください (Protect 724のArcSight製品マニュアルのコミュニティからダウンロード可能)。

イベントブローカー認証

Event Broker受信者を設定する前に、Loggerとイベントブローカー間で双方向認証をセットアップする必要があります。

双方向認証をセットアップするには、次のセクションの手順を実行します。

- 「ステップ1: Logger側でCSRを生成する」
- 「ステップ2: Event Broker上でLogger CSRに署名する」
- 「ステップ3: 署名付き証明書とプライベートキーをLoggerキーストアにインポートする」

これらの手順は、Event Brokerからデータを受信する必要があるそれぞれのLoggerで繰り返す必要があります。新しいLoggerについては、この手順をいつでも実行できます。

ステップ1: Logger側でCSRを生成する

1. オペレーティングシステムの資格情報を使用して、Loggerホストにログインします。
2. 次のように`eb_cert_tool`スクリプトを実行して、CSRを生成します。

   ```
   eb_cert_tool.sh --generate-csr --eb-host <EBホスト名またはIP>
   --key-length 2048
   ```

   Loggerアプライアンスの場合、このスクリプトは次の場所にあります。

   ```
   /opt/arcsight/logger/bin/scripts/eb_cert_tool.sh
   ```

ソフトウェアLoggerの場合、このスクリプトは次の場所にあります。
<インストールディレクトリ>/current/arcsight/logger/bin/scripts/eb_cert_tool.sh

3. 端末に出力されているCSRを(BEGIN行とEND行も含めて)テキストファイルにコピーします。たとえば、CSRのデータを切り取って/tmp/csr.csrファイルに貼り付けます。
4. ステップ3で生成したCSRテキストファイルをEvent Brokerホストにコピーします。例:

```
scp /tmp/csr.csr root@<eb_host_ip>:/tmp/
```

ステップ2: Event Broker上でLogger CSRに署名する

詳細については、『ArcSight Event Broker管理者ガイド』を参照してください。

1. Event Brokerホストにログインします。
2. securityフォルダーに移動します。たとえば、次のようにします。

```
cd /var/opt/arcsight/eventbroker/security
```

3. 次のコマンドを実行して、CSRに署名します。

```
openssl x509 -req -CA ca-cert.pem -CAkey ca-key.pem -in /tmp/csr.csr -out
/tmp/logger_cert.pem -days 3650 -CAcreateserial -passin pass:arcsight -
sha256
```

4. 署名付き証明書をLoggerホストにコピーします。たとえば、次のようにします。

```
scp /tmp/logger_cert.pem arcsight@<logger_host>:/tmp/
```

ステップ3: 署名付き証明書とプライベートキーをLoggerキーストアにインポートする

1. オペレーティングシステムの資格情報を使用して、Loggerホストにログインします。CSRの生成に使用したものと同じ証明書を使用します。
2. 次のようにeb_cert_toolを実行して、証明書をインポートします。

```
/opt/arcsight/logger/current/arcsight/logger/bin/scripts/eb_cert_tool.sh
--import-cert --eb-host <EBホスト名またはIP> --cert-path <location of cert
signed by EB>
```

3. 「受信者の使用」(374ページ)の説明に従って、Event Broker用にEvent Broker受信者を設定します。1つのEvent BrokerまたはEvent Brokerクラスターにつき、1つの署名付き証明書が必要です。
4. Loggerがイベントを受信する必要がある、同じCA証明書を持っていないすべてのEvent Brokerについて、このトピックの各セクションの手順を実行します。

これで、Logger上で、Event Broker受信者を設定できるようになりました。

ファイルベースの受信者

ファイルベースの受信者としては、ファイル受信者、ファイル転送受信者、フォルダーフォロアー受信者があります。これらを複数の受信者としてセットアップすることができ、取得したイベント

からデータを抽出するために、関連付けられているパーサーでソースタイプを使用するように設定することができます。

注: ファイルやフォルダーが削除または名称変更されている場合など、受信者がログファイルを読み込むことができない場合、Loggerは `current/arcsight/logger/logs/logger_receiver.log`にメッセージを記録します。

マルチライン受信者

TCP受信者およびUDP受信者は、`\r`や`\n`などの改行文字をイベントの終了として解釈します。入力イベントに文字`\r`または`\n`が含まれている場合、イベントは複数のイベントとして扱われます。イベントが複数行にわたっている場合は、マルチライン受信者を使用できます。マルチライン受信者としては、ファイル転送、ファイル受信者、フォルダフォロアー受信者があります。

マルチライン受信者は、サーバーログのような複数行にまたがるイベントを読み込むことができます。各行を個別に読み込むのではなく、スタックトレース全体を単一のイベントとして読み込むことで、ログに報告されたスタックトレースを処理するように、受信者を設定できます。

マルチライン受信者を作成する際には、ログファイル中の新しいイベントの開始を検出するために受信者が使用する正規表現を指定する必要があります。それぞれの新しいイベントは、ログファイル中の文字が正規表現に一致した場所で開始されます。

たとえば、次のログファイルで、各イベントは角括弧で囲まれたタイムスタンプ (`[yy-MM-dd HH:mm:ss.SSS]`) で始まります。そのため、次の正規表現を使用して各イベントを識別できます。

```
^\[\d+-\d+-\d+ \d+:\d+:\d+,\d+\].*
```

```
[2016-06-06 13:11:26,824][INFO][I18N]Locale has not been chosen by the user.
[2016-06-06 13:11:26,824][ERROR][DirectConnection$ReadChannel]
java.io.IOException: end of communication channel
    at com.arcsight.logger.distributed.DirectConnection.a(DirectConnection.java:39)
    at com.arcsight.logger.distributed.DirectConnection.access$200(DirectConnection.java:19)
    at com.arcsight.logger.distributed.DirectConnection$ReadChannel.run(DirectConnection.java:85)
    at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:886)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:908)
    at java.lang.Thread.run(Thread.java:619)
```

- マルチラインファイル受信者とファイル転送受信者では、新しいイベントの開始を識別する正規表現を、受信者の[複数行イベントの開始位置]フィールドで指定する必要があります。
- マルチラインフォルダーフォロアー受信者では、新しいイベントの開始を識別する正規表現を、受信者自身ではなく、その受信者に関連付けられている**ソースタイプ**の[複数行イベントの開始位置]フィールドで指定する必要があります。

受信者の作成と使用については、「受信者の使用」(374ページ)を参照してください。ソースタイプの作成と使用については、「ソースタイプ」(388ページ)を参照してください。

フォルダフォロアー受信者

アクティブなファイルの更新を監視するには、フォルダフォロアー受信者を使用します。フォルダフォロアー受信者は、設定して有効にすると、そのディレクトリの指定したファイルを監視し、絶えず新しいイベントをシステムにアップロードします。フォルダフォロアー受信者は、ファイルローテーションを認識します。

ディレクトリを監視するための手順の概要

1. 監視する必要があるログの種類を特定します。
2. デフォルトのソースタイプまたはソースタイプとパーサーのペアが要件を満たしているかどうかを判別します。詳細については、「ソースタイプ」(388ページ) および「パーサー」(392ページ) を参照してください。

   要件を満たしている場合は、次のステップに進みます。

   要件を満たしていない場合は、必要なパーサーとソースタイプを作成します。

   a. 追跡するディレクトリに格納されているログファイルに適したパーサーを1つ以上選択します。デフォルトのパーサーでは要件が満たされない場合は、適切なパーサーを作成します。

   b. 各パーサーにソースタイプを割り当てます。デフォルトのソースタイプでは要件が満たされない場合は、適切なソースタイプを作成します。
3. 上記で選択または作成したソースタイプを選択して、ディレクトリ内のログを監視するために必要なフォルダーフォロアー受信者を作成します。詳細については、「受信者の使用」(374ページ) を参照してください。
4. 受信者を有効にします。
5. オプションで、ログファイルイベントを転送するために、1つ以上の転送者を設定します。詳細については、「転送者」(398ページ) を参照してください。

ファイルフォロアー受信者でのソースタイプの使用

Loggerは、受信者に対して選択したソースタイプに関連付けられているパーサーを使用して、受信したイベントからフィールドとそれぞれの値を抽出します。これらのフィールドは、検索時に解析されます。ソースタイプとパーサーの使用の詳細については、「ソースタイプ」(388ページ) および「パーサー」(392ページ) を参照してください。

ファイルフォロアー受信者を作成する際には、特定の種類のログファイルを監視するのに適したソースタイプを選択する必要があります。ファイルフォロアー受信者のソースタイプを選択した後、それに関連付けられているパーサーがソースファイルを処理できることを確認します。

ソースタイプが同じでも、バージョンが異なるイベントは、形式が異なっている可能性があります。同様に、ベンダーが同じでも、ソースタイプが異なるイベントの形式は異なっている可能性があります。そのため、ソースファイルのソースタイプがソースタイプの指定と正確に一致しな

い場合、関連付けられているパーサーはイベントを正しく解析せず、検索結果に解析したフィールドが表示されません。

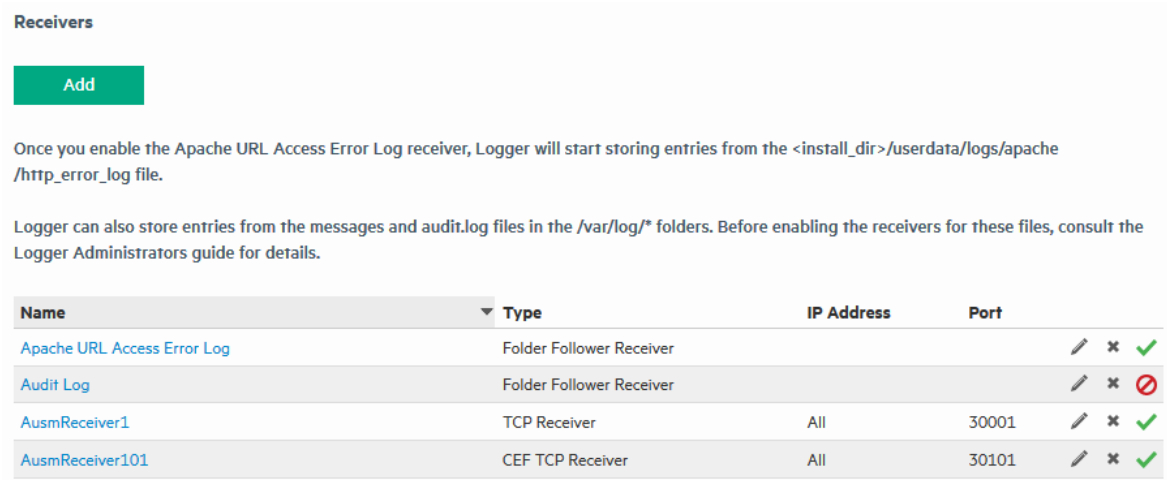
ソースタイプに有効なパーサーが関連付けられていることを確認するため、受信者を設定した後、受信イベントが解析されるかどうかを確認してください。これを判断するには、検索を実行し、検索結果の「パーサ」フィールドを確認します。検索に使用されたパーサーは、検索結果の[パーサ]列に表示されます。イベントが解析された場合、このフィールドにはパーサーの名前が表示されます。イベントが正常に解析されなかった場合、このフィールドには「Not parsed」と表示されます。ソースタイプにパーサーが定義されていない場合や、ソースタイプがない場合、このフィールドは空になります。

受信者の使用

システムにはいくつかの受信者が付属しています。必要に応じて他の受信者を追加できます。作成できる受信者の最大数は、システムリソース(メモリ、CPU、ディスクI/O、場合によりネットワーク帯域幅)によって制限されます。システムで使用できる受信者ポートは、示されている図とは違っている可能性があります。

受信者がデータを受信するには、リッスンしているポートが事前にファイアウォールによって開かれている必要があります。詳細については、「ファイアウォールルール」(558ページ)を参照してください。

[受信者 (Receivers)] ページ



ファイル受信者を作成する前に

- Loggerアプライアンスの場合は、ネットワークファイルシステムマウントを設定します。「ストレージ」(428ページ)を参照してください。
- ソフトウェアLoggerの場合は、ログファイルの読み込み元となるファイルシステムが、Loggerをインストールしたシステムにマウントされている必要があります。

注: ファイル転送受信者を作成する前に、適切なSCP、SFTP、およびFTPクライアントがシステムにインストールされていることを確認してください。

Loggerアプライアンスは、ユーザーインターフェイスを通じたマウントをサポートしています。ソフトウェアLoggerは、そのファイルシステムを使用します。これには、オペレーティングシステムを通じてマウントされたリモートフォルダーが含まれていてもかまいません。

受信者を作成するには

1. [**設定 | データ**] メニューを開き、[**受信者**] をクリックします。
   「[受信者 (Receivers)] ページ」(374ページ) には、現在の受信者とそのステータスが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. [**追加 (Add)**] をクリックします。
3. 新しい受信者の名前を入力します。SmartMessage受信者名は、関連付けられているArcSight SmartConnectorを設定するときに使用されます。
4. 受信者のタイプを選択します。[UDP 受信者]、[TCP 受信者]、[CEF UDP 受信者]、[CEF TCP 受信者]、[ファイル受信者]、[フォルダフォロア受信者]、[ファイル転送]、または [SmartMessage 受信者] を選択します。受信者を作成した後で受信者の種類を変更することはできません。

   注: Event Broker受信者を設定する前に、Loggerとイベントブローカー間で双方向認証をセットアップする必要があります。詳細と手順については、「イベントブローカー認証」(370ページ) を参照してください。

5. [**次へ**] をクリックして受信者パラメーターを編集します。
   [受信者を編集] ダイアログボックスに表示されるフィールドは、Loggerの種類と受信者のタイプによって変わります。
6. 適切なフィールドに入力します。フィールドの説明については、以下の表を参照してください。
   - 「UDP、TCP、CEF UDP、およびCEF TCP受信者のパラメーター」(377ページ)
   - 「Event Broker受信者のパラメーター」(379ページ)
   - 「ファイル受信者のパラメーター」(380ページ)
   - 「フォルダーフォロアー受信者のパラメーター」(382ページ)
   - 「ファイル転送受信者のパラメーター」(384ページ)
   - 「SmartMessage受信者のパラメーター」(386ページ)
7. [**有効にする**] チェックボックスはデフォルトでオンになっているため、受信者は、受信者の作成直後に有効になります。受信者を今すぐ有効にしない場合は、チェックボックスをクリックしてオフにします。後で有効にすることできます。
8. [**保存**] をクリックします。

受信者を有効または無効にするには

注: 以下のあらかじめ設定されているフォルダーフォロアー受信者をソフトウェアLoggerに対して有効にする前に、インストール時のユーザーかインストール時に指定した非rootユーザーがファイルを読み取ることができることを確認してください。

- `/var/log/messages`
- `/var/log/audit/audit.log`

1. **[設定 | データ]** メニューを開き、**[受信者]** をクリックします。
   「[受信者 (Receivers)] ページ」(374ページ) には、現在の受信者とそのステータスが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 有効または無効にする受信者を探します。
   - 受信者が現在無効になっている場合は、[無効] アイコン (⊘) をクリックして有効にします。
   - 受信者が現在有効になっている場合は、[有効] アイコン (✔) をクリックして無効にします。

     ヒント: 受信者を有効にした後は、無効する前に数分待ってください。同様に、無効にしたばかりの受信者を有効にする前にも待ってください。受信者を有効化または無効化することで開始されたバックグラウンドタスクが中断されると、予期しない結果が生じる可能性があります。

受信者を編集するには

1. **[設定 | データ]** メニューを開き、**[受信者]** をクリックします。
   「[受信者 (Receivers)] ページ」(374ページ) には、現在の受信者とそのステータスが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 更新する受信者を探し、その行の [編集] アイコン (✎) をクリックします。
   [受信者を編集] ダイアログボックスに表示されるフィールドは、Loggerの種類と受信者のタイプによって変わります。
3. 適切なフィールドを編集します。フィールドの説明については、以下の表を参照してください。
   - 「UDP、TCP、CEF UDP、およびCEF TCP受信者のパラメーター」(377ページ)
   - 「Event Broker受信者のパラメーター」(379ページ)
   - 「ファイル受信者のパラメーター」(380ページ)
   - 「フォルダーフォロアー受信者のパラメーター」(382ページ)
   - 「ファイル転送受信者のパラメーター」(384ページ)
   - 「SmartMessage受信者のパラメーター」(386ページ)

4. [**有効にする**] チェックボックスをオンにして受信者をすぐに有効にするか、チェックボックスをオフにして受信者を後で有効にします。
5. [**保存**] をクリックします。

受信者を削除するには

1. [**設定 | データ**] メニューを開き、[**受信者**] をクリックします。
   「[受信者 (Receivers)] ページ」(374ページ) には、現在の受信者とそのステータスが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 削除する受信者を探し、その行の [削除] アイコン (✖) をクリックします。
3. [**OK**] をクリックして削除を確認します。

UDP、TCP、CEF UDP、およびCEF TCP受信者のパラメーター

UDP受信者、TCP受信者、CEF UDP受信者、およびCEF TCP受信者を作成または編集する際には、以下のフィールドに入力します。

パラメーター	説明
名前	レポート作成とステータス監視で使用される受信者の名前を入力します。
IP/ホスト	受信者がリッスンする使用可能なネットワーク接続を1つ選択します。両方のネットワーク接続をリッスンする場合は [**すべて**] を選択します。 **注:** リストにlocalhost (`127.0.0.1`) が表示されている場合は、Loggerのホスト名が設定されていません。ホスト名を設定するには、「ネットワーク」(493ページ) を参照してください。

パラメーター	説明
ポート	Loggerアプライアンスの場合 • デフォルトのUDP受信者は、ポート514を使用するようにあらかじめ設定されています。 • SmartMessage受信者の場合は、SmartConnectorでポート443を設定します。 ソフトウェアLoggerの場合 • ソフトウェアLoggerをルートユーザーでインストールした場合は、空いている任意のポートを使用できます。そのポートが使用できない場合は、次に大きい空きポートが選択されます。 • ソフトウェアLoggerをルート以外のユーザーでインストールした場合は、1024よりも大きなポート番号のみを使用できます。デフォルトのUDP受信者は、ポート8514を使用するようにあらかじめ設定されています。そのポートが使用できない場合は、次に大きい空きポートが選択されます。
エンコーディング	文字エンコーディング(US-ASCII、Big5、EUC-KRなど)をプルダウンリストから選択します。CEF UDP、CEF TCP、およびSmartMessage受信者は、US-ASCIIまたはUTF-8エンコーディングを使用する必要があります。
ソースタイプ	プルダウンリストから、以下のものを含むログファイルの種類を選択します。 • Apache HTTP Server Access • Apache HTTP Server Error • Juniper Steel-Belted Radius • Microsoft DHCP Log • IBM DB2 Audit • 追加オプション... また、自社の要件に基づいて、独自のソースタイプを定義することもできます。「ソースタイプ」(388ページ)を参照してください。 1つの受信者は、1つのソースタイプのイベントのみを受信できます。ログファイルの種類ごとに個別の受信者を設定してください。 **注:** CEF TCPおよびCEF UDP受信者は、CEFソースタイプに設定されており、変更できません。現在、CEFソースタイプに関連付けられているパーサーはありません。 Logger 5.3 SP1以前のリリースで作成されたTCPおよびUDPは、[その他]のソースタイプを使用します。

Event Broker受信者のパラメーター

Event Broker受信者を作成または編集する際には、以下のフィールドに入力します。詳しくは、『Event Broker管理者ガイド』およびApache Kafkaの資料を参照してください。

パラメーター	説明
名前	Event Broker受信者の名前を入力します。 このフィールドは必須フィールドです。
Event Brokerホストおよびポート	Event Brokerクラスターへの初回接続を確立するために使用するホスト/ポートのペアのリストを入力します。 このフィールドは必須フィールドです。 有効な値: 次の形式のEvent Brokerのホストおよびポート: host1:port1, host2:port2, … **注:** ホスト名は解決可能でなければなりません。DNSを設定して、適切なホストを追加してください。詳細については、「ネットワーク」(493ページ)を参照してください。
イベントトピックリスト	受信者がサブスクライブするイベントトピックを入力します。 このフィールドは必須フィールドです。 有効な値: イベントトピックのコンマ区切りリスト。イベントトピック名では大文字と小文字が区別されます。
最初のオフセットからイベントを取得	このトピックについてEvent Brokerに送信されたイベントのうち、保有ポリシーの期間内にあるすべてのイベントを取得するには、trueに設定します。これらをスキップして最新のイベントで開始するには、falseに設定します。いずれの場合も、今後、このトピックについてEvent Brokerによって受信されたすべてのイベントが取得されます。 このオプションは、初期設定でのみ使用されます。 デフォルトはtrueです。
コンシューマーグループ	この受信者が属するコンシューマーグループを一意に識別する名前を入力します。 複数のLoggerに、同一のトピックをサブスクライブしていて、同一のコンシューマーグループに属しているEvent Broker受信者がある場合、グループ内の各Loggerは、トピック内のパーティションのさまざまなサブセットからイベントを受信します。Event Brokerは、同一のコンシューマーグループ内で設定されているすべてのLogger間でパーティションのバランスを取ります。 **注:** コンシューマーグループを実際に作成する必要はありません。コンシューマーグループは、このフィールドによって指定されるコンシューマーの論理的なグループに過ぎません。これはプール内のすべてのLogger上で同一でなければなりません。 Event Broker受信者がイベントを受信するために必要です。

パラメーター	説明
SSL/TLSの使用	SSL/TLS暗号化を有効にするには、trueを選択します。falseを選択すると、この受信者には、プレーンテキストで情報が送信されます。 **注意:** HPE Security ArcSightでは、このオプションをtrueに設定することを推奨しています。 デフォルトはfalseです。
クライアント認証の使用	Event BrokerとのTLS接続の確立時に、クライアント認証を有効にするには、このフィールドをtrueに設定します。 このフィールドは必須フィールドです。 デフォルトはfalesです。
有効にする	受信者を有効にするには、このボックスをオンにします。

ファイル受信者のパラメーター

ファイル受信者を作成または編集する際には、以下のフィールドに入力します。

パラメーター	説明
名前	レポート作成とステータス監視で使用される受信者の名前を入力します。
RFS名	NFSまたはCIFSのマウント名のプルダウンリストから選択します。リストには、SANをサポートしているLoggerモデル上で接続されているSANも含まれます。 NFSボリュームをマウントするには、「ストレージ」(509ページ)を参照してください。CIFS共有をマウントするには、「ストレージ」(509ページ)を参照してください。SANの詳細については、「SAN」(512ページ)を参照してください。
フォルダ	[ローカル]を選択し、リモートファイルシステムがマウントされているLogger上のディレクトリを、[フォルダ]フィールドに指定します。 Loggerをインストールしたシステムにリモートファイルシステムをマウントするには、そのオペレーティングシステムのマニュアルを参照してください。
ソースの種類	プルダウンリストから、以下のものを含むログファイルの種類を選択します。 • Apache HTTP Server Access • Apache HTTP Server Error • Juniper Steel-Belted Radius • Microsoft DHCP Log • IBM DB2 Audit • 追加オプション... また、自社の要件に基づいて、独自のソースタイプを定義することもできます。「ソースタイプ」(388ページ)を参照してください。 1つの受信者は、1つのソースタイプのイベントのみを受信できます。ログファイルの種類ごとに個別の受信者を設定してください。

パラメーター	説明
ワイルドカード (正規表現)	読み込むログファイルを記述した正規表現 (regex)。 これは、「*.*」のような一般的なファイルワイルドカードではなく、正規表現です。 デフォルトは、すべてのファイルを意味する「.*」です。 例 .processで終わるすべてのファイルを含めるには、次のようにします。 .*\.process *.propertiesファイルのみを監視するには、次のようにします。 .*\.properties ファイル名が8桁の数字になっている.logファイルのみを含めるには、次のようにします。 \d{8}.log **注:** .zipや.binのようなバイナリファイルなど、テキスト以外のデータの種類をアップロードすると、Loggerが正しく動作しない可能性があります。[正規表現] フィールドで「.*」を指定し、ディレクトリ内のすべての内容を取得する場合は、誤ってバイナリファイルを含めてしまう可能性があるため、注意してください。
モード	以下のいずれかを選択します。 • [Delete] - 処理済みのログファイルを削除します。 • [Rename] - 処理済みのログファイルの名称を変更します。ファイルには「Rename」拡張子を追加した名前が付けられます。 • [Persist] - Loggerは、処理済みのファイルを記憶し、ファイルを1回だけ処理します。
名前変更拡張子	処理済みのログファイルに追加されるサフィックス。
文字エンコーディング	文字エンコーディング (US-ASCII、Big5、EUC-KRなど) をプルダウンリストから選択します。CEF UDP、CEF TCP、およびSmartMessage受信者は、US-ASCIIまたはUTF-8エンコーディングを使用する必要があります。
検出後の遅延	ソースファイルが最初に認識されてから処理されるまでの待機時間 (秒)。これにより、処理が開始される前に、ファイル全体をLoggerにコピーしたり、リモートファイルシステムにコピーしたり (ファイル受信者の場合) することができます。 デフォルトは**10秒**です。 **注:** ファイル転送受信者では、大きなファイルが予想される場合、このパラメーターに大きな値を設定する必要があります。大きなファイル (1GBなど) の場合、デフォルトの10秒では十分ではありません。
イベント時刻ロケール	プルダウンリストから、[英語 (アメリカ合衆国)]、[中国語 (香港)]、[中国語 (台湾)] などのロケールを選択します。

パラメーター	説明
日付/時刻ゾーン	ログファイルのタイムスタンプでタイムゾーンが指定されていない場合に必要です。 ファイル転送およびファイル受信者では、日時の形式または日時と場所の正規表現が空白の場合、このパラメーターは無視されます。 アプライアンスLoggerでは、Loggerで設定されているタイムゾーンを **[システム管理 | システム | ネットワーク] > [時間/NTP]** タブで確認できます。ソフトウェアLoggerはシステム時刻を使用します。
イベント時刻ロケーション	ログファイル内のタイムスタンプを表す文字を記述する正規表現。例: `.*\[(.*?)\].*` この正規表現は、タイムスタンプが各行の最初の角括弧の内側にあることを指定します。最初のキャプチャーグループ(正規表現の括弧内の部分)が、日付/時間の形式を使用して解析される部分です。 デフォルトは、タイムスタンプなしです。
イベント時刻フォーマット	ログファイルに含まれているタイムスタンプが、それぞれのイベントで同じ形式である場合に必要です。指定しない場合(または日時と場所の正規表現が空白の場合)、ファイル内の各イベントは、ファイルのファイルシステムタイムスタンプではなく、ファイル自体がLoggerによって最初に認識された日付でタイムスタンプが設定されます 形式の一覧については、「日付と時刻の指定」(387ページ)を参照してください。 デフォルトは、タイムスタンプなしです。

複数行イベントの開始位置	ログファイル内の新しいイベントの開始位置を指定する正規表現。受信者が複数行のログファイルを読み取れるようにするには、この正規表現を指定します。正規表現がログファイル内の文字と一致する位置が、各イベントの先頭になります。例:
	`^\[\d+-\d+-\d+ \d+:\d+,\d+].*`
	この正規表現は、次のようなタイムスタンプに一致します。
	`[2010-12-06 13:09:46,818]`
	このフィールドを空白のままにした場合、ログファイル内の各行が1つのイベントとして扱われます。
	デフォルトでは、ログファイル内の各行が1つのイベントとして扱われます。

フォルダーフォロアー受信者のパラメーター

フォルダーフォロアー受信者を作成または編集する際には、以下のフィールドに入力します。

パラメーター	説明
名前	レポート作成とステータス監視で使用される受信者の名前を入力します。
ローカルフォルダー	処理するローカルフォルダーを指定します。Loggerアプライアンスでは、このフィールドを使用できるのは、[マウント名]で[ローカル]を選択した場合のみです。

パラメーター	説明
ソースの種類	プルダウンリストから、以下のものを含むログファイルの種類を選択します。 • Apache HTTP Server Access • Apache HTTP Server Error • Juniper Steel-Belted Radius • Microsoft DHCP Log • IBM DB2 Audit • 追加オプション... また、自社の要件に基づいて、独自のソースタイプを定義することもできます。「ソースタイプ」(388ページ)を参照してください。 1つの受信者は、1つのソースタイプのイベントのみを受信できます。ログファイルの種類ごとに個別の受信者を設定してください。

ワイルドカード (正規表現)	読み込むログファイルを記述した正規表現 (regex)。
	これは、「*.*」のような一般的なファイルワイルドカードではなく、正規表現です。
	デフォルトは、すべてのファイルを意味する「.*」です。
	例
	.processで終わるすべてのファイルを含めるには、次のようにします。
	`.*\.process`
	*.propertiesファイルのみを監視するには、次のようにします。
	`.*\.properties`
	ファイル名が8桁の数字になっている.logファイルのみを含めるには、次のようにします。
	`\d{8}.log`
	注: .zipや.binのようなバイナリファイルなど、テキスト以外のデータの種類をアップロードすると、Loggerが正しく動作しない可能性があります。[正規表現] フィールドで「.*」を指定し、ディレクトリ内のすべての内容を取得する場合は、誤ってバイナリファイルを含めてしまう可能性があるため、注意してください。

パラメーター	説明
ブラックリスト (正規表現)	無視するログファイルの名前を記述した正規表現 (regex)。この正規表現に一致するファイルは監視されません。 これは、「*.*」のような一般的なファイルワイルドカードではなく、正規表現です。 例: .txtで終わるファイルを除外するには、次のように指定します。 `.*\.txt` *.txt以外のすべてのファイルを監視するには、次のように指定します。 ワイルドカード: `.*` ブラックリスト: `.*\.txt`
文字エンコーディング	文字エンコーディング (US-ASCII、Big5、EUC-KRなど) をプルダウンリストから選択します。CEF UDP、CEF TCP、およびSmartMessage受信者は、US-ASCIIまたはUTF-8エンコーディングを使用する必要があります。
日付/時刻ゾーン	ログファイルのタイムスタンプでタイムゾーンが指定されていない場合に必要です。 ファイル転送およびファイル受信者では、日時の形式または日時と場所の正規表現が空白の場合、このパラメーターは無視されます。 Loggerで設定されているタイムゾーンを **[システム管理 | システム | ネットワーク] > [時間/NTP]** タブで確認できます。 ソフトウェアLoggerはシステム時刻を使用します。

ファイル転送受信者のパラメーター

ファイル転送受信者を作成または編集する際には、以下のフィールドに入力します。

パラメーター	説明
名前	レポート作成とステータス監視で使用される受信者の名前を入力します。
プロトコル	SCP、SFTP、またはFTPプロトコルを選択します。
ポート	受信者のポート番号。デフォルトのポートは22です。
IP/ホスト	受信者がリッスンするLoggerのネットワーク接続を1つ選択します。両方のネットワーク接続をリッスンする場合は [すべて] を選択します。 **注:** リストにlocalhost (127.0.0.1) が表示されている場合は、Loggerのホスト名が設定されていません。ホスト名を設定するには、「ネットワーク」(493ページ) を参照してください。
ユーザー	ソースログファイルの表示および読み取りの特権を持つ、ホスト上のユーザーを入力します。プロトコルがFTPの場合、特殊なユーザー「anonymous」を指定できます。
パスワード	指定したユーザーのパスワードを入力します。匿名FTPの場合であっても、パスワードを空にすることはできません(ただし、この場合、パスワードは無視されます)。

パラメーター	説明
ファイル パス	読み取る対象のログファイルのパスと名前を入力します。パス名とファイル名では、?や*などのワイルドカードを使用できます (たとえば、「*.log」または「Log-??.txt」)。ディレクトリはスラッシュ (/) で区切ります。 複数のファイルを指定するには、カンマで区切ります。 例: /tmp/SyslogData/syslog.log.gz, /security/logs/*/, /security/log?/admin/special/ **注:** .zipや.binのようなバイナリファイルなど、テキスト以外のデータをアップロードすると、Loggerが正しく動作しない可能性があります。指定するディレクトリにバイナリファイルが含まれないようにしてください。「*」を指定し、ディレクトリ内のすべての内容を取得する場合は、誤ってバイナリファイルを含めてしまう可能性があるため、注意してください。
スケジュール	ファイル転送を実行するタイミングと頻度を指定します。スケジュールが指定されていない場合、ファイル転送は1回だけ実行されます。スケジューリングの詳細については、「日付と時刻のスケジュールのオプション」(150ページ)を参照してください。
zip フォーマット	[gzip]、[zip]、または [なし] を選択します。
ソースの種類	プルダウンリストから、以下のものを含むログファイルの種類を選択します。 • Apache HTTP Server Access • Apache HTTP Server Error • Juniper Steel-Belted Radius • Microsoft DHCP Log • IBM DB2 Audit • 追加オプション... また、自社の要件に基づいて、独自のソースタイプを定義することもできます。「ソースタイプ」(388ページ)を参照してください。 1つの受信者は、1つのソースタイプのイベントのみを受信できます。ログファイルの種類ごとに個別の受信者を設定してください。
文字エンコーディング	文字エンコーディング (US-ASCII、Big5、EUC-KRなど) をプルダウンリストから選択します。CEF UDP、CEF TCP、およびSmartMessage受信者は、US-ASCIIまたはUTF-8エンコーディングを使用する必要があります。
検出後の遅延	ソースファイルが最初に認識されてから処理されるまでの待機時間 (秒) を入力します。これにより、処理が開始される前に、ファイル全体をLoggerにコピーしたり、リモートファイルシステムにコピーしたり (ファイル受信者の場合) することができます。 デフォルトは10秒です。 ファイル転送受信者では、大きなファイルが予想される場合、このパラメーターに大きな値を設定する必要があります。大きなファイル (1GBなど) の場合、デフォルトの10秒では十分ではありません。
イベント時刻ロケール	プルダウンリストから、[英語 (アメリカ合衆国)]、[中国語 (香港)]、[中国語 (台湾)] などのロケールを選択します。

パラメーター	説明
日付/時刻ゾーン	日付/時刻ゾーンを入力します。詳細については、「日付と時刻の指定」(387ページ)を参照してください。 ログファイルのタイムスタンプでタイムゾーンが指定されていない場合に必要です。 ファイル転送およびファイル受信者では、日時の形式または日時と場所の正規表現が空白の場合、このパラメーターは無視されます。 Loggerで設定されているタイムゾーンを[システム管理 | システム | ネットワーク] > [時間/NTP] タブで確認できます。 ソフトウェアLoggerはシステム時刻を使用します。
イベント時刻ロケーション	ログファイル内のタイムスタンプを表す文字を記述する正規表現。例: `.*\[(.*?)\].*` この正規表現は、タイムスタンプが各行の最初の角括弧の内側にあることを指定します。最初のキャプチャーグループ(正規表現の括弧内の部分)が、日付/時間の形式を使用して解析される部分です。 デフォルトは、タイムスタンプなしです。
イベント時刻フォーマット	ログファイルに含まれているタイムスタンプが、それぞれのイベントで同じ形式である場合に必要です。指定しない場合(または日時と場所の正規表現が空白の場合)、ファイル内の各イベントは、ファイルのファイルシステムタイムスタンプではなく、ファイル自体がLoggerによって最初に認識された日付でタイムスタンプが設定されます 形式指定の一覧については、「日付と時刻の指定」(387ページ)を参照してください。 デフォルトは、タイムスタンプなしです。

複数行イベントの開始位置	ログファイル内の新しいイベントの開始位置を指定する正規表現。受信者が複数行のログファイルを読み取れるようにするには、この正規表現を指定します。正規表現がログファイル内の文字と一致する位置が、各イベントの先頭になります。例:
	`^\[\d+-\d+-\d+ \d+:\d+,\d+].*`
	この正規表現は、次のようなタイムスタンプに一致します。
	`[2010-12-06 13:09:46,818]`
	このフィールドを空白のままにした場合、ログファイル内の各行が1つのイベントとして扱われます。
	デフォルトでは、ログファイル内の各行が1つのイベントとして扱われます。

SmartMessage受信者のパラメーター

SmartMessage受信者を作成または編集する際には、以下のフィールドに入力します。

パラメーター	説明
名前	関連付けられているArcSight SmartConnectorの設定時に使用される受信者の名前を入力します。
エンコーディング	文字エンコーディング(US-ASCII、Big5、EUC-KRなど)をプルダウンリストから選択します。CEF UDP、CEF TCP、およびSmartMessage受信者は、US-ASCIIまたはUTF-8エンコーディングを使用する必要があります。

日付と時刻の指定

日付と時刻の形式を指定して、ファイル受信者 (ファイル受信者、フォルダーフォロアー受信者、ファイル転送) で解析できるようにするには、「日付と時刻の形式の指定」(387ページ)という表を参照してください。Loggerは、内部的に、SimpleDateFormatという共通のJavaメソッドを使用しています。Javaソースに記述されているように、SimpleDateFormatの洗練された使用は、Loggerで機能します。通常、パターン文字は繰り返され、その数で正確な表現が決まります。

次の例は、U.S.ロケールで日付と時刻のパターンがどのように解釈されるかを示しています。指定された日付と時刻は、2013年7月4日、ローカル時刻は12時08分56秒、タイムゾーンは「U.S. Pacific Time」です。

日付と時刻の例

ソース	日付と時刻のパターン
2013.07.04 AD at 12:08:56 PDT	yyyy.MM.dd G 'at' HH:mm:ss z
Wed, Jul 4, '13	EEE, MMM d, ''yy
12:08 PM	h:mm a
12 o'clock PM, Pacific Daylight Time	hh 'o'clock' a, zzzz
0:08 PM, PDT	K:mm a, z
2013.July.04 AD 12:08 PM	yyyyy.MMMMM.dd GGG hh:mm aaa
Wed, 4 Jul 2013 12:08:56 -0700	EEE, d MMM yyyy HH:mm:ss Z
130704120856-0700	yyMMddHHmmssZ
2013-07-04T12:08:56.235-0700	yyyy-MM-dd'T'HH:mm:ss.SSSZ

日付と時刻の形式の指定

記号	意味	表現	例
G	年代指定	(テキスト)	AD
y	年	(数字)	2013または13
M	月 (1～12)	(月)	July、Jul、07
w	年の中の週 (1～52)	(数字)	39
W	月の中の週 (1～5)	(数字)	2
D	年の中の日 (1～366)	(数字)	129
d	月の中の日 (1～31)	(数字)	10
E	曜日	(テキスト)	TuesdayまたはTue
F	月の中の第何曜日か		

日付と時刻の形式の指定 (続き)

記号	意味	表現	例
a	am/pmマーカー	(テキスト)	AMまたはPM
H	時 (0～23)	(数字)	0
k	時 (1～24)	(数字)	24
K	am/pmの時 (0～11)	(数字)	0
h	am/pmの時 (1～12)	(数字)	12
m	分 (0～59)	(数字)	30
s	秒 (0～59)	(数字)	55
S	ミリ秒 (0～999)	(数字)	978
z	タイムゾーン	(テキスト)	Pacific Standard Time、PST、GMT-08:00
Z	タイムゾーン	(RFC 822)	-0800 (PSTを示す)

ソースタイプ

ソースタイプは、特定のデータソースから取得されるイベントの種類を識別します。たとえば、イベントは、Apacheアクセスログ、単純なsyslog、ユーザーが作成したアプリケーションのログから取得します。パーサーを使用して、指定したソースタイプからのイベントデータを解析できます。

イベントがソースタイプに関連付けられると、ソースタイプがパーサーに関連付けられている場合、それらのイベントを照合する検索を実行すると、イベントはそのパーサーによって解析されます。検索結果には、CEFイベントと同様に、一致する解析済みイベントのフィールドが列に表示されます(これらのイベントを表示するには、「ユーザ定義フィールド」フィールドセットを使用します)。詳細については、「パーサー」(392ページ)を参照してください。

いずれかの行がCEFではないソースタイプを含む検索から取得された場合、イベントのソース、ソースタイプ、パーサーが検索結果の列リストに表示されます。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

ソースタイプが使用されている場合、検索結果に以下の列が表示されます。

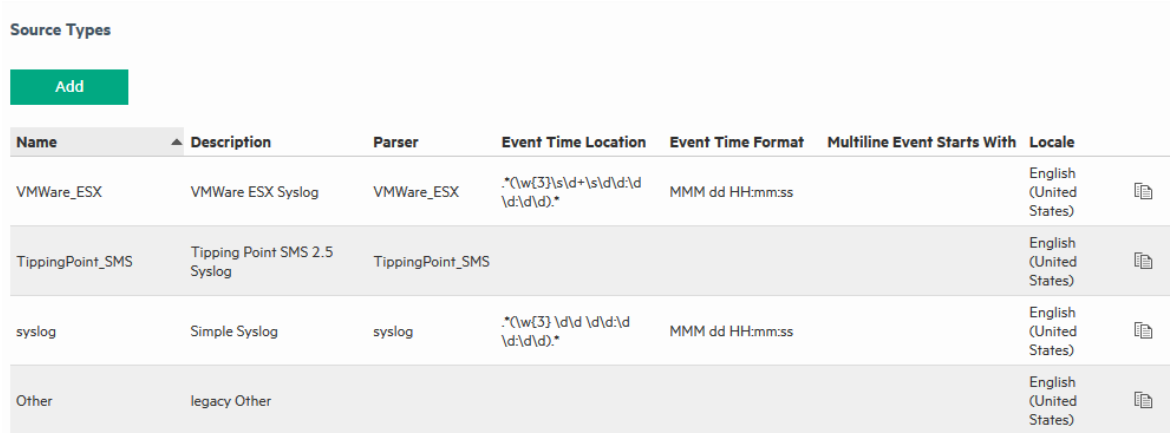
- **ソース:** イベントの受信元のログファイルの名前。

  たとえば`/opt/mnt/testsoft/web_server.out.log`と表示されます。イベントを受信したときにソースが適用されなかった場合、このフィールドは空になります。このフィールドを表示するかどうかを、[検索オプション] ページで制御できます。このオプションの設定方法については、「グローバル検索オプション」(349ページ)を参照してください。
- **ソースタイプ:** イベントの受信元のファイルの種類。[ソースタイプ] ページ (**[設定 | データ] > [ソースタイプ]**) で定義します。イベントを受信したときにソースタイプが適用されなかった場合、このフィールドは空になります。このフィールドを表示するかどうかを、[検索オプション] ページで制御できます。このオプションの設定方法については、「グローバル検索オプション」(349ページ)を参照してください。
- **パーサー:** イベントが解析された場合、このフィールドにはパーサーの名前が表示されます。イベントが正常に解析されなかった場合、このフィールドには「Not parsed」と表示されます。ソースタイプにパーサーが定義されていない場合や、ソースタイプがない場合、このフィールドは空になります。

ソースタイプの使用

Loggerでは、いくつものソースタイプと事前に設定されたパーサーが提供されています。また、新しいソースタイプを定義してパーサーを割り当てることができます。これにより、特定の種類のイベントで抽出するフィールドセットを選択できます。1つのソースタイプに関連付けることができるパーサーは1つだけですが、1つのパーサーに複数のソースタイプを関連付けることができます。デフォルトのソースタイプは編集または削除できませんが、ソースタイプをコピーして、要件を満たす類似のソースタイプを作成できます。カスタムソースタイプは、必要に応じて編集または削除できます。Loggerで使用できるソースタイプは、以下の図とは違っている可能性があります。

[ソースタイプ (Source Types)] ページ



以下のソースタイプにはパーサーが関連付けられています。

ソースタイプ	説明
Apache_access	Apacheアクセスログ
Apache_error	Apacheエラーログ
audit_log	監査ログファイル用のsyslog
Bluecoat_proxy	Bluecoat Proxy SG
Cisco_PIX	Cisco PIX
IBM_DB2	IBM DB2 9.x監査ログ
Juniper_NSM	Juniper NSM 2009 syslog
logger_syslog	Loggerアプライアンス上のsyslogファイル用のsyslog
Microsoft_DHCP	Microsoft DHCP for 2008 v6ログファイル
syslog	単純なsyslog
TippingPoint_SMS	Tipping Point SMS 2.5 syslog
VMware_ESX	VMware ESX syslog

Loggerは、Connector転送者を使用してイベントをESMに転送できます。ESMは、さらにStreaming Connectorにイベントを転送します。このコネクターは、イベントを正規化し、ESMに転送します。

Connector転送者を使用してイベントをESMに転送する必要がある場合は、以下のソースタイプのいずれかを選択する必要があります。

ソースタイプ	
Apache HTTP Server Access	Juniper Steel-Belted Radius
Apache HTTP Server Error	Microsoft DHCP Log
IBM DB2 Audit	Other

ソースタイプを追加するには

1. **[設定 | データ]** メニューを開き、**[ソースタイプ]** をクリックします。
   「[ソースタイプ (Source Types)] ページ」(389ページ) に、現在のソースタイプが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. **[追加]** をクリックします。

3. フィールドに入力してソースタイプを定義します。

ソースタイプのフィールド

フィールド	説明
名前	ソースタイプの名前。
説明	ソースタイプの説明。
パーサ	このソースタイプに関連付けるパーサー。必要なパーサーがドロップダウンリストに表示されない場合は、パーサーを追加できます。パーサーの追加方法については、「パーサー」(392ページ)を参照してください。
イベント時刻ロケーション	ログファイル中のタイムスタンプを記述した正規表現。例: `.*\[(.*?)\].*` この表現は、タイムスタンプが各行の最初の角括弧の内側にあることを指定します。最初のキャプチャーグループ(正規表現の括弧内の部分)が、日時の形式を使用して解析される部分になります。 ログファイルにタイムスタンプがないことは、‘’で指定できます。
イベント時刻フォーマット	ログファイル内の日付と時刻の形式を記述した正規表現。たとえば、`dd/MMM/yyyy:HH:mm:ss Z`のように指定します。 ログファイルにタイムスタンプがないことは、‘’で指定できます。 イベント時刻の詳細については、「時間範囲」(79ページ)および「日付と時刻の指定」(387ページ)を参照してください。
複数行イベントの開始位置	隣接する行が同じイベントであるか、新しいイベントの開始であるかを認識する方法を記述する正規表現。たとえば、各イベントが形式yy-MM-dd HH:mm:ss.SSSの日付で始まる場合、(`\d+-\d+-\d+ \d+:\d+:\d+.\d+`)を使用して、新しいイベントの開始を示すことができます。
ロケール	プルダウンリストから、[英語(アメリカ合衆国)]、[中国語(香港)]、[中国語(台湾)]などのロケールを選択します。これは、Loggerがファイル内で探すデータのロケールです。

4. [**保存**]をクリックします。

ソースタイプを編集するには

1. [**設定 | データ**]メニューを開き、[**ソースタイプ**]をクリックします。
   「[ソースタイプ(Source Types)]ページ」(389ページ)に、現在のソースタイプが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 更新するソースタイプを探し、その行の[編集]アイコン(✎)をクリックします。

> **注:** [編集]アイコン(✎)は、デフォルトのソースタイプでは使用できません。代わりに、ソースタイプをコピーして、類似のソースタイプを作成できます。

3. 必要に応じて、フィールドを編集します。

フィールドの詳細については、表「ソースタイプのフィールド」(391ページ) を参照してください。

4. [**保存**] をクリックします。
5. このソースタイプを使用している受信者を無効にしてから再度有効にします。

注: ソースタイプの変更は、再度有効にするまで、関連付けられている受信者に反映されません。

ソースタイプをコピーするには

1. [**設定 | データ**] メニューを開き、[**ソースタイプ**] をクリックします。
   「[ソースタイプ (Source Types)] ページ」(389ページ) に、現在のソースタイプが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. コピーするソースタイプを探し、その行の [コピー] アイコン ( ) をクリックします。
3. 新しいソースタイプの名前を入力し、必要に応じてフィールドを編集します。
   フィールドの詳細については、表「ソースタイプのフィールド」(391ページ) を参照してください。
4. [**保存**] をクリックします。

ソースタイプを削除するには

1. [**設定 | データ**] メニューを開き、[**ソースタイプ**] をクリックします。
   「[ソースタイプ (Source Types)] ページ」(389ページ) に、現在のソースタイプが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 削除するソースタイプを探し、その行の [削除] アイコン ( ) をクリックします。

注: [削除] アイコン ( ) は、デフォルトのソースタイプでは使用できません。削除できるのは、自分が追加したソースタイプのみです。

3. [**OK**] をクリックして削除を確定します。

パーサー

パーサーを使用すると、ネットワーク環境内のさまざまなソースからのrawイベント (非CEFデータ) を抽出して操作できます。イベントフィールドを解析した後、容易にデータの検索、グラフ化、その他の操作を実行できます。イベントについて深く理解している1人のユーザーがパーサーを作成すれば、それらのイベントを参照するすべてのユーザーがその作業の恩恵を受けることができます。

パーサーは、イベントを読み込むための単純な方法を提供します。rawイベントデータを見てその意味を理解しようとする代わりに、パーサーを使用して非CEFイベントの各部分をフィー

ルドに抽出できます。ただし、パーサーによって作成されたフィールドは検索操作のみで使用でき、Loggerスキーマには追加されません。

パーサーは、以下のいずれかの方法で使用できます。

- **パーサーをソースタイプとともに使用**: パーサーをソースタイプに関連付けて、任意の種類のイベントの任意のフィールドセットを抽出できます。詳細については、「ソースタイプ」(388ページ)を参照してください。
- **検索でparseコマンドを使用**: 検索時にparseコマンドを使用してイベントからフィールドを抽出し、他の検索演算子 (where、chart、topなど) を使用して検索をさらに調整するか、フィールド内のデータを操作することができます。これは、ITの運用や、rawイベントデータを抽出して操作する必要があるその他の顧客に有用です。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

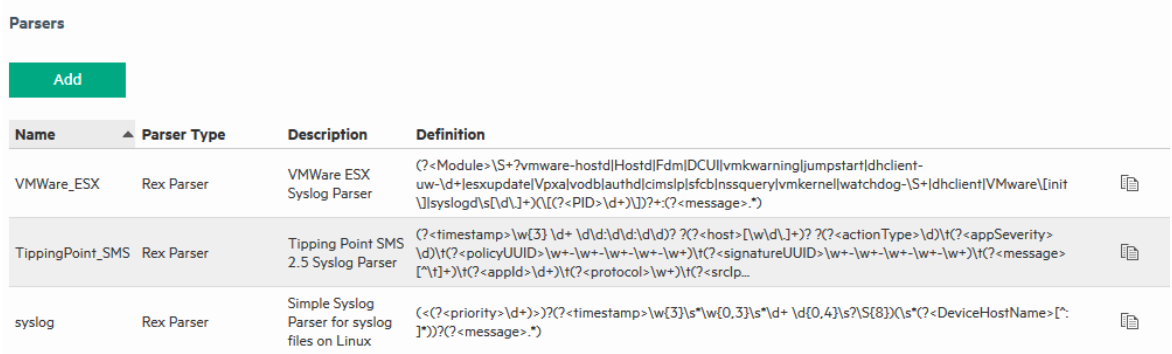
- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

パーサーをソースタイプとともに使用する

Loggerには、ソースタイプが関連付けられた設定済みのパーサーがいくつか用意されています。新しいパーサーを定義して、ソースタイプに関連付けることもできます。1つのソースタイプに関連付けることができるパーサーは1つだけですが、複数のソースタイプが同じパーサーを使用できます。デフォルトのパーサーは編集または削除できませんが、コピーして要件を満たす類似のパーサーを作成できます。カスタムパーサーは、必要に応じて編集または削除できます。

[パーサ (Parsers)] ページ



parseコマンドの使用

parseコマンドは、検索によって返された任意の非CEFイベントに対してパーサーを実行するために使用できます。これは、rexパーサーの正規表現など、パーサーの定義を各イベントに適用します。その後、その正規表現によって抽出されたフィールドを、渡されるフィールドに追加します。REXパーサーの場合、これは、パーサーの定義と同じ正規表現を使用したrexコマンドと機能的に同じであるため、REX parseコマンドは、保存されたrex式を実行するものと考えることができます。

parseコマンドの詳細については、「parse」(585ページ)を参照してください。検索全般については、「イベントの検索と分析」(67ページ)を参照してください。

パーサーの使用

パーサーとしては、Rexパーサーと抽出パーサーの2種類のパーサーを定義できます。パーサーを追加する前に、イベントを解析するために使用するクエリを定義する必要があります。

Rexパーサーでこれを行うための1つの方法は、rex検索演算子を使用して、処理するイベントから目的のフィールドが返されるまで、正規表現をテストして調整することです。その後、rex式をコピーし、パーサーの**[定義 (Definition)]**フィールドに貼り付けます。抽出パーサの場合は、extract演算子を使用します。検索演算子の詳細については、「parse」(585ページ)、「rex」(590ページ)、および「extract」(576ページ)を参照してください。

検索に使用されたパーサーは、検索結果の[パーサ]列に表示されます。イベントが解析された場合、このフィールドにはパーサーの名前が表示されます。イベントが正常に解析されなかった場合、このフィールドには「Not parsed」と表示されます。ソースタイプにパーサーが定義されていない場合や、ソースタイプがない場合、このフィールドは空になります。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

パーサーを追加するには

1. **[設定 | データ]**メニューを開き、**[パーサ]**をクリックします。
   「[パーサ (Parsers)] ページ」(393ページ)に示す[パーサ]ページに、現在のパーサーが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. **[追加]**をクリックします。

3. パーサーの名前を入力します
4. ドロップダウンリストからパーサーの種類を選択します。
5. [**保存**] をクリックします。
   [**パーサを編集**] ダイアログボックスに表示されるフィールドは、パーサーの種類によって変わります。
6. パーサーのフィールドに設定値を入力します。
   パーサーのフィールド

フィールド	説明
名前	パーサーの名前。既存の名前を変更する場合は、新しい名前を入力します。
説明	パーサーの目的を示すわかりやすい説明。
rexパーサのみ	
定義	イベントを解析するために使用するrex式。
抽出パーサのみ	
ペアの区切り文字	イベント内のキーと値のペアを区切る文字。次の例のように、区切り文字のみを入力します。 |,
キー/値の区切り文字	キーと値を区切る文字。次の例のように、区切り文字のみを入力します。 =
フィールド	イベントを解析する際に使用するフィールド名のリスト。 フィールド名をカンマ(,)で区切って入力します。たとえば、次のようなイベントを解析するとします。`foo=abc, bar=xyz, baz=def` その場合は、次のように入力します。`foo,bar,baz`

7. [**保存**] をクリックします。

パーサーを編集するには

1. [**設定 | データ**] メニューを開き、[**パーサ**] をクリックします。
   「[パーサ (Parsers)] ページ」(393ページ) に示す [パーサ] ページに、現在のパーサーが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 更新するパーサーを探し、その行の [編集] アイコン (✎) をクリックします。

   注: [編集] アイコン (✎) は、デフォルトのパーサーでは使用できません。代わりに、パーサーをコピーして、類似のパーサーを作成できます。

3. 適宜パーサーのフィールドを編集します。
   [パーサを編集] ダイアログボックスに表示されるフィールドは、パーサーの種類によって変わります。パーサーのフィールドについては、「パーサーのフィールド」(395ページ) の表を参照

してください。

4. [**保存**] をクリックします。

パーサーをコピーするには

1. [**設定 | データ**] メニューを開き、[**パーサ**] をクリックします。
   「[パーサ (Parsers)] ページ」(393ページ) に示す [パーサ] ページに、現在のパーサーが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. コピーするパーサーを探し、その行の [コピー] アイコン (⎘) をクリックします。
   [パーサを編集] ダイアログボックスに表示されるフィールドは、パーサーの種類によって変わります。
3. 新しいパーサーの名前を入力し、適宜フィールドを編集します。
   パーサーのフィールドについては、「パーサーのフィールド」(395ページ) の表を参照してください。
4. [**保存**] をクリックします。

パーサーを削除するには

1. [**設定 | データ**] メニューを開き、[**パーサ**] をクリックします。
   「[パーサ (Parsers)] ページ」(393ページ) に示す [パーサ] ページに、現在のパーサーが表示されます。列見出しをクリックすると、フィールドをソートできます。
2. 削除するパーサーを探し、その行の [削除] アイコン (✖) をクリックします。

   注: [削除] アイコン (✖) は、デフォルトのパーサーでは使用できません。削除できるのは、自分が追加したパーサーのみです。

3. [**OK**] をクリックして削除を確定します。

   ヒント: パーサーを削除する場合は注意してください。ソースの種類に関連付けられているパーサーを変更または削除するときに、Loggerに警告は表示されません。

例: 抽出パーサーの作成

以下のようなログの、INT、MAC、DST、およびSRCフィールドの内容を見つけるパーサーを作成するとします。

```
Jul 12 14:30:31 n15-214-128-h92 kernel: IN=eth2
MAC=00:24:e8:60:cb:82:00:50:56:92:2a:d5:08:00 SRC=192.0.2.9 | DST=192.0.2.2
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=21408 DF PROTO=TCP SPT=56978 DPT=443
WINDOW=8192 RES=0x00 SYN URGP=0
Jul 12 14:30:31 n15-214-128-h92 kernel: IN=eth2 |
MAC=00:24:e8:60:cb:82:00:50:56:92:2a:d5:08:00 | SRC=192.0.2.9 | DST=192.0.2.2
```

```
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=21408 DF PROTO=TCP SPT=56978 DPT=443
WINDOW=8192 RES=0x00 SYN URGP=0
Jul 12 14:30:31 n15-214-128-h92 kernel: IN=eth2 |
MAC=00:24:e8:60:cb:82:00:50:56:92:2a:d5:08:00 | SRC=192.0.2.9 | DST=192.0.2.2
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=21408 DF PROTO=TCP SPT=56978 DPT=443
WINDOW=8192 RES=0x00 SYN URGP=0
```

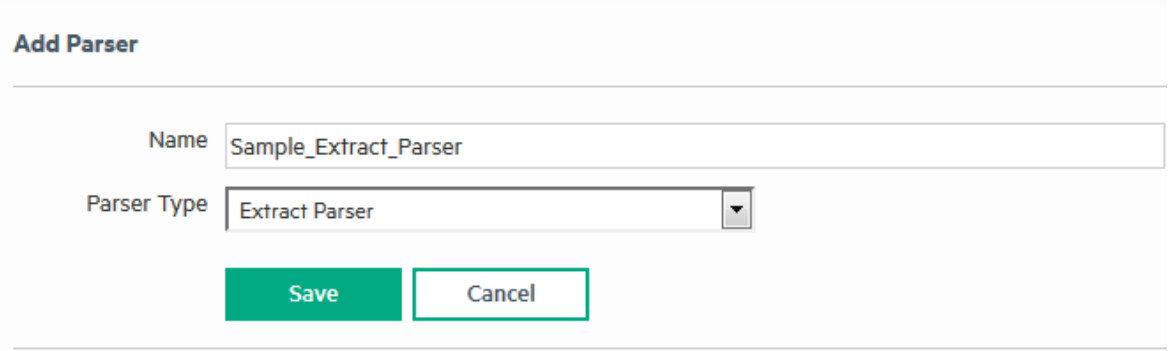
このログの例で、フィールドの値は等号記号 (=) で示され、フィールドはパイプ (|) とコロン (:) で区切られています。次のクエリを使用して、IN、MAC、DST、およびSRCフィールドの内容を検索できます。

```
extract pairdelim= “|:” kvdelim= “=” fields= “IN,MAC,DST,SRC”
```

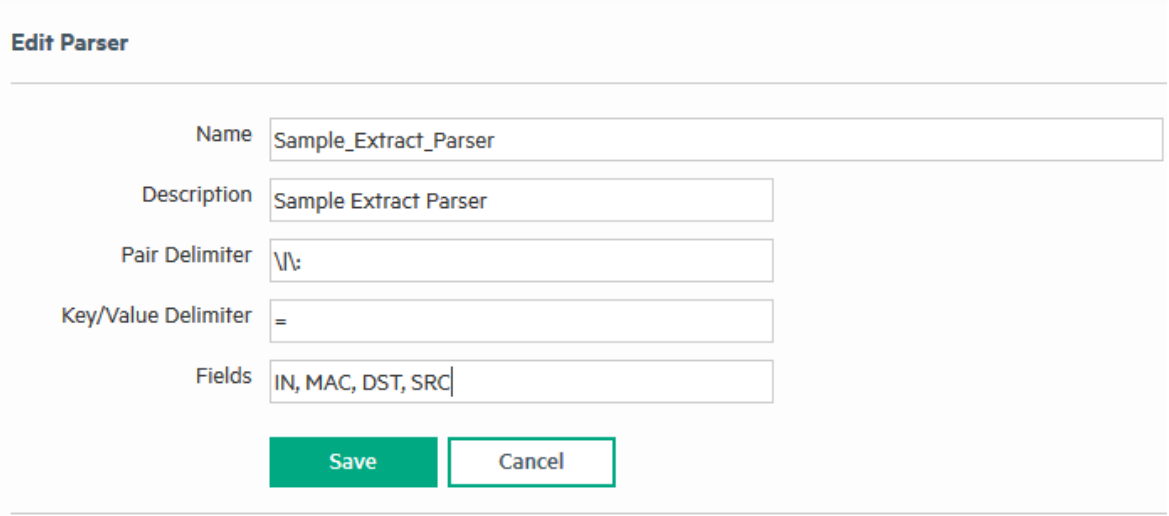
以下の手順では、そのクエリを使用して抽出パーサーを作成する方法について説明します。

サンプルの抽出パーサーを作成するには

1. [設定 | データ] メニューを開き、**[パーサ]** をクリックします。
2. **[追加]** をクリックします。[パーサを追加 (Add Parser)] ダイアログボックスが表示されます。



3. 名前を入力し、パーサーの種類を選択します。たとえば、以下のように入力します。
   [名前 (Name)]: `Sample_Extract_Parser`
   [パーサタイプ (Parser Type)]: `Extract Parser`
4. **[保存 (Save)]** をクリックします。[パーサを編集 (Edit parser)] ダイアログボックスが表示されます。



5. パーサーのペアの区切り、キー値、およびフィールドを入力します。たとえば、以下のように入力します。

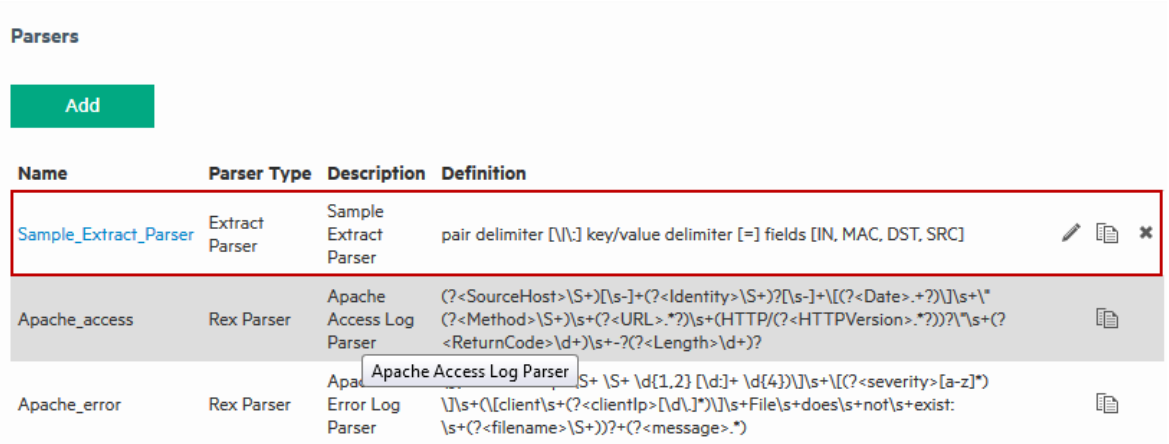
   [ペアの区切り文字 (Pair Delimiter)]: `\|\:`

   [キー/値の区切り文字 (Key/Value Delimiter)]: `=`

   [フィールド (Fields)]: `INT, MAC, DST, SRC`

   注: パイプ (|) とコロン (:) はバックスラッシュ (\) でエスケープする必要があります。

6. **[保存 (Save)]** をクリックします。[パーサ (Parsers)] ページに新しいパーサーが表示されます。



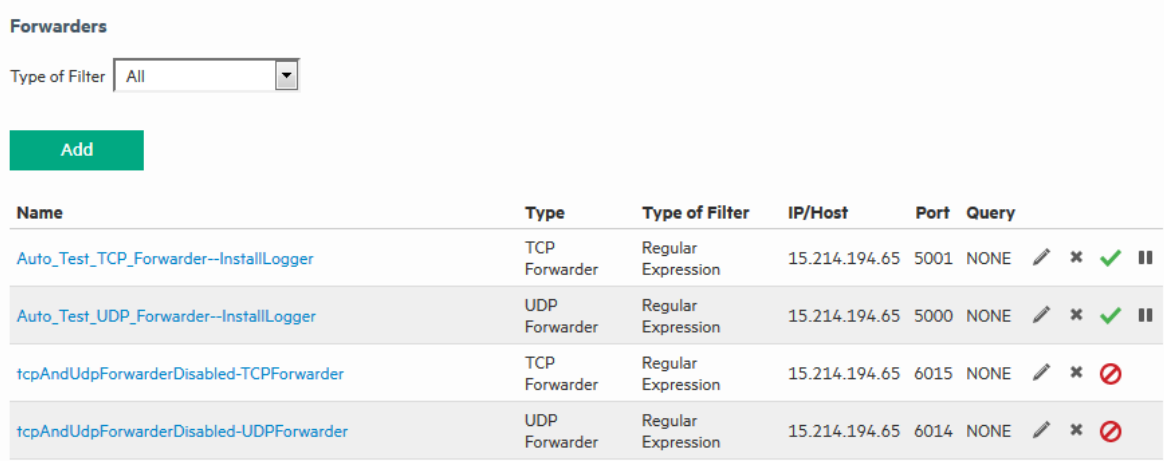
転送者

転送者は、すべてのイベントまたは特定のフィルターに一致するイベントを、特定のホストまたはArcSightマネージャーなどの通知先に送信します。

転送者ごとに異なるフィルターを定義できるため、Loggerは、トラフィックを複数の通知先に分割できます。たとえば、LoggerはArcSightマネージャーよりも高速にイベントを処理できるた

め、Loggerを使用して複数のArcSightマネージャーにイベントを転送できます。転送者フィルターを使用すると、マネージャーごとに1つの転送者を使用して、マネージャー間でフローを分割することが可能になります。また、転送により、一部のイベントを他の通知先に送信し、そこで処理する一方で、長期間保存するためにすべてのイベントをLogger上で保持できます。

[転送者 (Forwarders)] ページ



転送フィルターは一致するイベントを検索するクエリであり、オプションで期間を指定できます。**連続**フィルターと、**期間指定**フィルターの、2種類の転送者フィルターを作成できます。

- **連続**フィルターは、受信イベントを絶えず評価し、一致するイベントを指定された通知先に転送します。
- **期間指定**フィルターは、指定された条件に加えて期間を使用して、イベントを通知先に転送すべきかどうかを判定します。指定した期間に該当し、指定した条件に一致するイベントは転送されます。そうでないイベントは転送されません。転送者フィルターにイベントの転送を評価する期間が指定されている場合、Loggerによるイベントの受信時刻を使用して、イベントを通知先に転送するかどうかが判定されます。ある期間内のすべてのイベントを転送し終えた転送者は、それ以上イベントを転送しません。

転送者がイベントを転送できるのは、転送者が設定されているLoggerからだけで、ピアからイベントを転送することはできません。

転送者の動作は、任意の時点で一時停止および再開できます。転送者が動作を再開すると、転送処理を一時停止する前に確立された最後のチェックポイントから転送が再開されます。

また、転送者を無効にして再度有効にすることもできます。転送者を再度有効にすると、以前に確立したすべてのチェックポイントが削除され、転送者の設定に従って転送が再度開始されます。連続フィルターを持つ転送者は、現在の時刻から開始しますが、時間範囲が指定されたフィルターを持つ転送者は、設定された時間範囲の始めから開始します。

転送者の種類としては、UDP転送者、TCP転送者、Connector転送者、ArcSight ESM転送者があります。

- **UDP転送者**: UDP転送者は、UDP (User Datagram Protocol) を使用してイベントを転送します。
- **TCP転送者**: TCP転送者は、TCP (Transmission Control Protocol) を使用してイベントを転送します。
- **Connector転送者**: Connector転送者は、Logger Streaming Connectorにイベントを送信します。
- **ArcSight ESM CEF転送者**: ArcSight ESM CDF転送者は、共通イベントフォーマット (CEF)イベントをESM通知先に送信します。Loggerに内蔵されているコネクターを使用して、これらのイベントがESMに転送されます。

注: ArcSight ESM転送者を作成するには、まずESM通知先を作成する必要があります。詳細については、「ESM通知先」(419ページ) を参照してください。

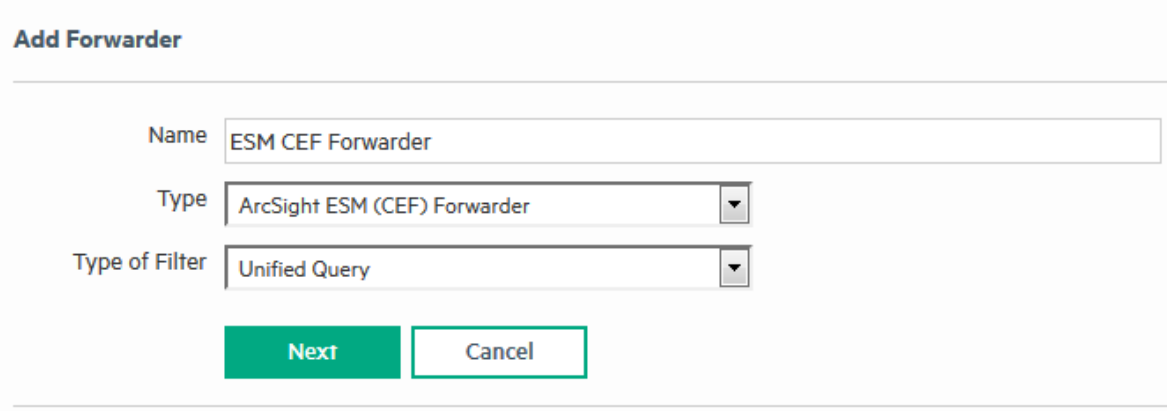
10個を超える正規表現転送者を追加しないことをお勧めします。転送者を追加するたびに転送速度は高まりますが、この関係は比例するわけではありません。EPS (秒あたりのイベント数) が高い状況や、リソースを大量に使用する他の機能が並列に動作しており (アラート、レポート、複数の検索処理)、転送フィルターが複雑な状況では、あまり多くの転送者を追加するとパフォーマンスが低下する可能性があります。これは、複数の転送者が同じLoggerリソースを使用し、同じ内蔵コネクターを使用して転送しようとして競合するからです。

フィルターに正規表現またはインデックス付き検索クエリ(統合クエリ)を指定できます。こうすることで、インデックス作成テクノロジーを利用して、転送するイベントを素早く効率的に検索できます。

注: 統合クエリに基づく転送者は、インデックス作成されたイベントを転送します。インデックス作成はLoggerでバッチ的に実行されるため、これらの転送者は、「爆発」的な動作を示します。EPS出力バーゲージ (Loggerのインターフェイス画面の上部にある) で爆発的な動作に気づくことがあります。バーゲージには、大量のデータが転送されると高いEPSレベルが表示され、その後通常のレベルに戻ります。

転送者を作成するには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. **[追加]** をクリックし、以下のフォームを表示します。



3. 新しい転送者の名前を入力し、要件に合った転送者の種類を選択します。選択できるのは、UDP転送者、TCP転送者、Connector転送者、またはArcSight ESM (CEF)転送者です。
4. この転送者で使用転送フィルターの種類として、**[統合クエリ(Unified Query)]** または **[正規表現]** を選択します。インデックス検索クエリを指定する場合は [統合クエリ(Unified Query)] を選択し、正規表現クエリを指定する場合は [正規表現] を選択します。
5. **[次へ(Next)]** をクリックします。
6. さらに、以下の表で説明する種類ごとの情報を入力します。

転送者パラメーター

パラメーター	転送者の種類	説明
名前	すべて	前の画面で入力した名前が自動的に表示されます。名前を変更する場合はこの画面で変更します。

転送者パラメーター(続き)

パラメーター	転送者の種類	説明

クエリ	すべて	転送者が転送するイベントをフィルターするために使用するクエリを入力するか、[フィルタ] リストからフィルターを選択します。
		転送者クエリは、デバイスグループとストレージグループで制限できますが、ピアで制限することはできません。
		前に画面で [統合クエリ] を選択した場合は、全文およびフィールドベースのインデックス付きフィールドを含むインデックス検索クエリを入力します。[検索の詳細設定] リンクをクリックして Search Builderツールにアクセスし、インデックスクエリを構築できます(詳細については、「検索の詳細設定ビルダーへのアクセス」(94ページ)を参照してください)。
		ヒント: 指定する統合クエリは、以下のガイドラインに従っている必要があります。そうしないとクエリまたは転送者を保存できなくなります。
		以下の形式のクエリが有効です。他の形式は許可されません。
		`(full-text terms | field search)* | regex`
		つまり、クエリにはフルテキスト (キーワード) クエリ要素とフィールドベースクエリ要素のみが含まれている必要があります。アグリゲーション検索演算子や、検索を詳細化するために検索したデータをさらに処理する演算子を含めることはできません。たとえば、chart、sort、eval、topなどです。
		そのため、次のクエリは有効なクエリです。
		`failed message CONTAINS “failed device”`
		しかし、次のクエリは無効なクエリです。
		`failed message CONTAINS “failed device” | sort deviceEventCategory`
		クエリには、パイプライン文字 (|) の後に`regex`演算子を含めることができます。そのため、次のクエリは転送者で有効なクエリです。
		`failed message CONTAINS “failed device” | regex deviceEventCategory = “fan”`
		ヒント: クエリのすべての検索条件 (「regex」部分を除く) は、インデックス付けされている必要があります。クエリにフルテキスト (キーワード) の語が含まれている場合は、フルテキストインデックス付けが有効になっている必要があります。同様に、クエリにフィールドが含まれている場合、フィールドベースのインデックス作成が有効になっており、指定されたフィールドにインデックスが作成されている必要があります。
		前の画面で [正規表現] を選択した場合は、このテキストボックスに正規表現を指定します。「イベントの検索」(106ページ)

転送者パラメーター(続き)

パラメーター	転送者の種類	説明
		を参照してください。
フィルター	すべて	統合クエリを指定する代わりに、[フィルタ] リストからフィルターを選択できます。[フィルター] リストには、保存されているすべてのフィルターと、Logger上であらかじめ定義されているシステムフィルターが含まれています。「クエリ」(403ページ) で説明されている妥当性ガイドラインを満たすフィルターを選択してください。そうしないと、転送者の定義を保存したときに、ユーザーインターフェイスにエラーが表示されます。 転送者ごとに選択できるのは、1つの統合クエリフィルターのみです。ただし、正規表現に基づく転送者には複数のフィルターを選択できます。 同様に、正規表現に基づくフィルターを作成する場合は、このリストからフィルターを選択します。
時間範囲でのフィルタリング	すべて	受信イベントを継続的に評価し、一致するイベントを転送する連続フィルターを作成する場合は、このパラメーターをスキップします。この場合、クエリは継続的に実行され、転送は一時停止するまで継続します。 期間指定フィルターを作成する場合は、このチェックボックスをオンにして、転送者が転送するイベントの期間を指定します。期間を入力した場合、転送者はその期間に含まれるイベントを送信して停止します。 このチェックボックスをオンにすると、[開始日]、[終了日]、[時刻] フィールドが表示されます。 開始は終了より前でなければなりません。将来の時刻を指定すると、そのフィールドが現在時刻に変化します。たとえば、当日の午前7時を開始、当日の午後7時を終了として指定すると、午前7時からフィルターが保存される時間(午後7時より前)までのタイムスタンプを持つイベントが生成されます。

転送者パラメーター(続き)

パラメーター	転送者の種類	説明
ソースの種類	コネクター	プルダウンリストから、以下のものを含むログファイルの種類を選択します。 • Apache HTTP Server Access • Apache HTTP Server Error • IBM DB2 Audit • Juniper Steel-Belted Radius • Microsoft DHCP Log • その他... **注:** [ソースの種類] は、受信者、転送者、SmartConnectorで同じであることが必要です。「ログファイルイベントのESMへの転送」(424ページ)を参照してください。 1つの受信者は、1つのソースタイプのイベントのみを受信できます。ログファイルの種類ごとに個別の受信者を設定してください。
Syslogタイムスタンプの保存	UDP、TCP	syslogタイムスタンプを保存する場合はtrueを設定します。デフォルトはtrueです。この場合、タイムスタンプはイベントの元の受信時刻になります。 falseを設定すると、元のタイムスタンプがLoggerの受信時刻で置き換えられます。
元のSyslog送信者の保存	UDP、TCP	LoggerのIPアドレスをsyslogイベントのホスト名 (またはそれに相当する) フィールドに挿入せずに、イベントをそのまま送信するにはtrueを設定します。デフォルトはtrueです。 falseを設定すると、Loggerの情報が、syslogイベントのホスト名 (またはそれに相当する) フィールドに挿入されます。
IP/ホスト	UDP、TCP、コネクター	転送されたイベントを受信する通知先のIPアドレスまたはホスト名。 **注:** Logger転送者は、それ自体が設定されているのと同じシステムにデータを転送するように設定することはできません。
ポート	UDP、TCP、コネクター	転送されたイベントを受信する通知先のポート。 デフォルトのポートは514です。
接続再試行タイムアウト	TCP、Connector、ESM	接続を再試行する前に待機する時間(秒単位)。デフォルトは5秒です。
ESM通知先	ESM	転送されたイベントを受信する既存のESM通知先。(詳細は、「ESM通知先」(419ページ)を参照してください)。

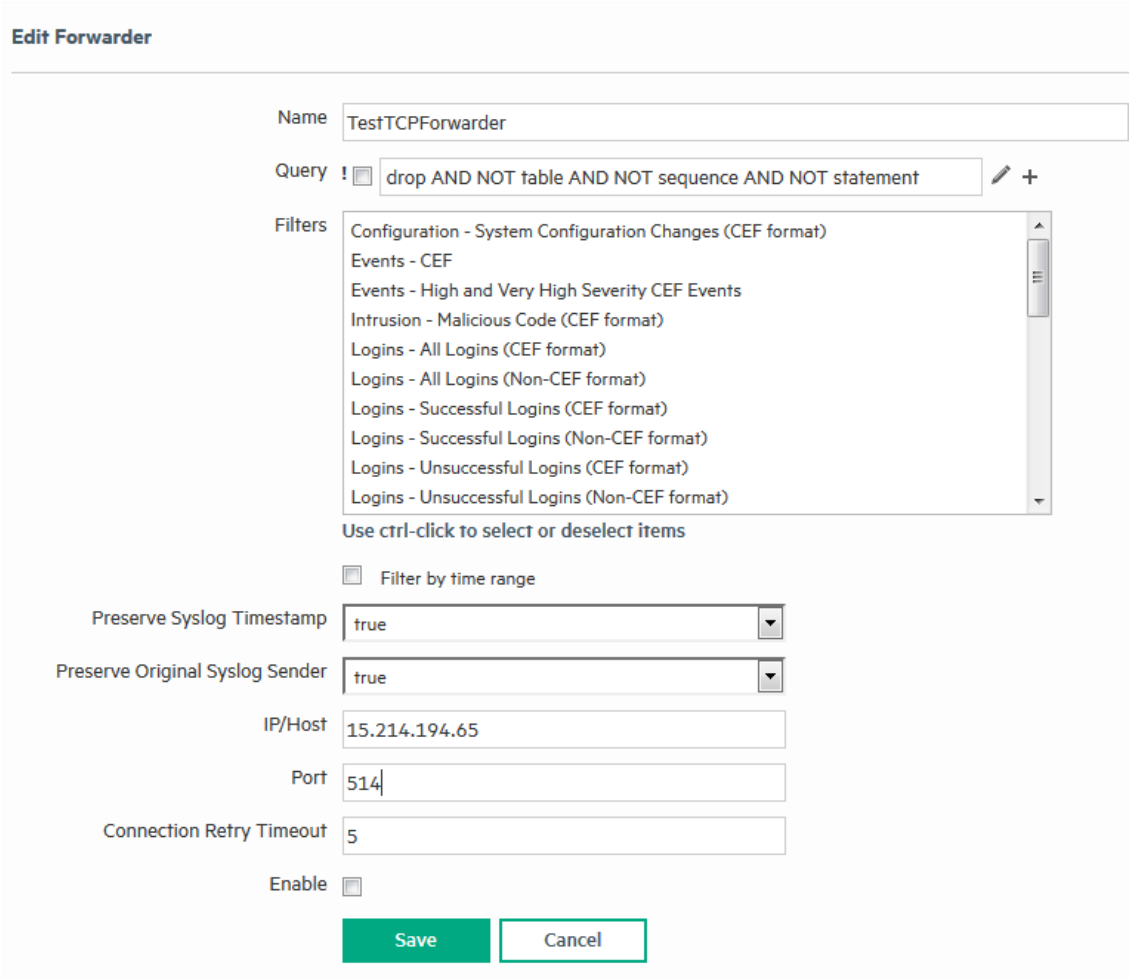
7. 転送者を今すぐ有効にするには、**[有効にする (Enable)]** チェックボックスをオンにします。転送者を今すぐ有効にしない場合は、後で有効にすることができます。
8. **[保存]** をクリックします。

転送者を編集するには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 編集する転送者を探します。
3. 転送者が有効になっている場合は、**[有効]** アイコン (✔) をクリックして無効にします。
4. **[編集 (Edit)]** アイコン (✎) をクリックします。

   以下に、正規表現に基づく転送者の [転送者を編集 (Edit Forwarder)] 画面を示します。統合クエリ転送者の [転送者を編集 (Edit Forwarder)] 画面には、統合クエリに基づくフィルターの一覧が表示され、[クエリ (Query)] テキストボックスでは1つのクエリのみを指定できます。

   クエリの項、フィルター、その他の転送者パラメーターの指定



5. 「転送者パラメーター」(402ページ) の表の説明に従って、フォームの情報を編集します。

6. 転送者を今すぐ有効にするには、**[有効にする (Enable)]** チェックボックスをオンにします。転送者を今すぐ有効にしない場合は、後で有効にすることができます。
7. **[保存 (Save)]** をクリックします。

転送者を削除するには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 削除する転送者を探します。
3. 転送者が有効になっている場合は、[有効] アイコン (✔) をクリックして無効にします。
4. [削除] アイコン (✖) をクリックします。
5. **[OK]** をクリックして削除を確認します。

転送者を一時停止するには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 一時停止する転送者を探します。
3. [実行中] アイコン (⏸) をクリックして転送者を一時停止します。

転送者を再開するには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 動作を再開する転送者を探します。
3. [一時停止] アイコン (▶) をクリックして転送者の操作を再開します。

転送者を無効にするには

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 左パネルで **[イベントの出力]** をクリックします。
3. 無効にする転送者を探します。
4. [有効] アイコン (✔) をクリックして無効にします。

転送者を有効化または再有効化するには

ヒント: 有効にしたばかりの転送者を無効にするには、数分待ってください。同様に、無効にしたばかりの転送者を有効にする前にも待ってください。転送者を有効化または無効化することで開始されたバックグラウンドタスクが中断されると、予期せぬ結果が生じる可能性があります。

1. **[設定 | データ]** メニューを開き、**[転送者]** をクリックします。
2. 有効または再度有効にする転送者を探します。
3. [無効] アイコン (⊘) をクリックします。

リアルタイムアラート

このセクションでは、リアルタイムアラートについて説明します。保存された検索アラートについては、「保存された検索アラート」(343ページ)を参照してください。アラートのタイプの説明については、「Loggerアラートの種類」(412ページ)を参照してください。

指定されたイベントまたはイベントパターンによってトリガーされるリアルタイムアラートを設定したり、オプションで、メールアドレスやSNMPサーバーなどの以前に設定されていた通知先に通知を送信したりすることができます。イベントパターンとは、特定の頻度 (指定した期間内のイベント数のしきい値) を超えて発生する指定のイベントです。たとえば、特定のデバイスから5分以内に受信した5つのイベントに、「unauthorized」という単語が含まれている場合に生成されるアラートを作成できます。また、ストレージ容量警告や、一部のLoggerアプライアンスモデルでのCPU温度警告など、内部イベントに対してアラートを生成することもできます。

アラートを作成するには、クエリまたはフィルター、イベントアグリゲーション値 (一致数としきい値)、1つ以上の通知先 (オプション) を指定する必要があります。新しいアラートが、電子メール、SNMP、またはSyslog通知先に通知を送信する場合は、アラートを作成する前に通知先を設定してください。詳細は、「静的ルート」(496ページ)、「アラート通知の受信」(414ページ)および「アラート通知の設定」(416ページ)を参照してください。

アラートの監査イベントは、デフォルトでは内部ストレージグループのみに書き込まれ、ESM通知先に転送されません。これらの監査イベントをESMに転送する必要がある場合は、カスタマーサポートにお問い合わせください。

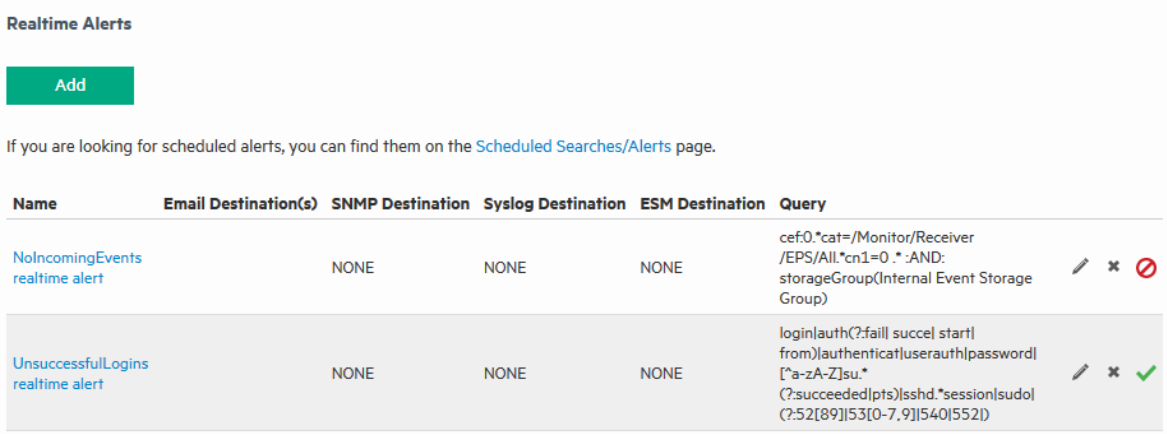
注: この変更は、アラート用に生成された監査イベントのみに適用され、他の監査イベントはESM通知先に送信することができます。

Loggerでは、一般的に必要とされるイベントパターンをもとにしたフィルターがあらかじめ定義されており、それを使用して必要なアラートを簡単に作成できるようになっています。関心のある特定のイベントパターンを見つけるための新しいフィルターを作成することもできます。

設定されたリアルタイムアラートのリストを確認するには

1. **[設定 | データ]** メニューを開き、**[アラート]** をクリックします。
   リアルタイムアラートのリストが表示されます。

リアルタイムアラート (Realtime Alerts)



リアルタイムアラートを追加するには

「リアルタイムアラートの作成」(410ページ) を参照してください。

リアルタイムアラートを有効または無効にするには

1. [**設定 | データ**] メニューを開き、[**アラート**] をクリックします。
2. 無効または有効にするアラートを探します。対応するアイコン (または) をクリックして、アラートを有効または無効にします。

> **注:** 同時に有効にできるアラートは25個までです。追加のアラートを有効にするには、現在有効なアラートを無効にする必要があります。
>
> 有効になっているアラートが最大数に達していて、受信者EPSが30kより多い場合は、検索時間が低下しないように受信者EPSの速度が少し低下します。

リアルタイムアラートを編集するには

1. [**設定 | データ**] メニューを開き、[**アラート**] をクリックします。
2. 編集するアラートを探し、その行の [編集] アイコン ( ) をクリックします。
   「[リアルタイム アラートを追加 (Add Realtime Alert)] ダイアログボックス」(410ページ) のような画面が表示されます。アラート名には英数字のみを使用できます。

リアルタイムアラートを削除するには

1. [**設定 | データ**] メニューを開き、[**アラート**] をクリックします。
2. 削除するアラートを探し、その行の [削除] アイコン ( ) をクリックします。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてアラートを保持します。

トリガーされたアラートを表示するには

「アラートの表示」(156ページ) を参照してください。

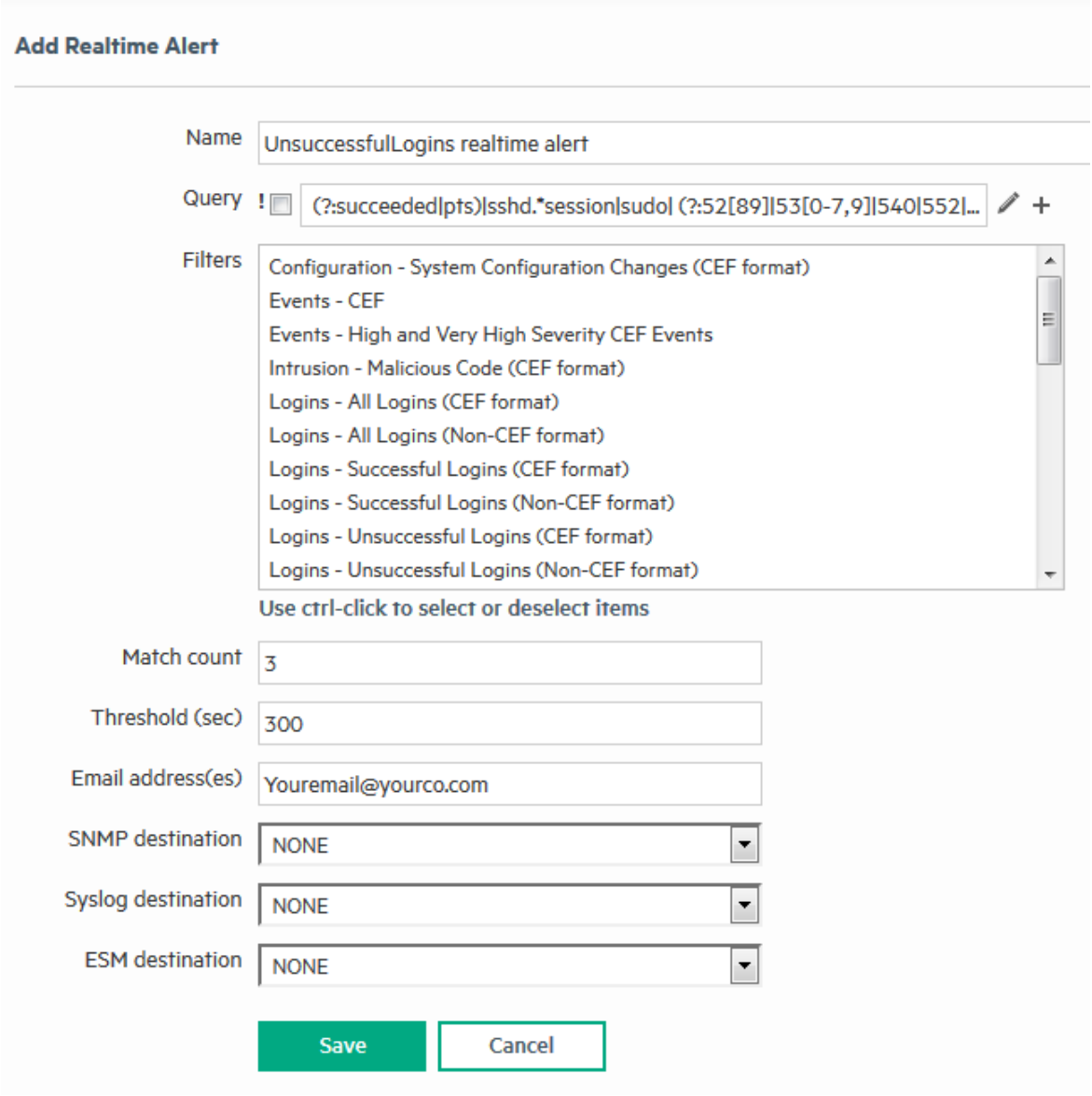
リアルタイムアラートの作成

このセクションでは、リアルタイムアラートを作成する方法について説明します。保存された検索アラートについては、「保存された検索アラート (スケジュールされたアラート) の作成」(343ページ) を参照してください。アラートのタイプの説明については、「Loggerアラートの種類」(412ページ) を参照してください。

リアルタイムアラートを作成するには

1. **[設定 | データ]** メニューを開き、**[アラート]** をクリックします。
2. **[追加]** をクリックします。[リアルタイム アラートを追加 (Add Realtime Alert)] ダイアログボックスが表示されます。

   [リアルタイム アラートを追加 (Add Realtime Alert)] ダイアログボックス



3. 新しいアラートの名前を入力して、クエリを指定するか、リストから使用可能なフィルターを選択します。このクエリに一致するイベントがアラートの候補となります。
4. 検索フィルタークエリは必要に応じて編集できます。英数字とスペースを使用できますが、%や&などの一部の特殊文字は使用できません。

   フィルターの詳細については、「フィルター」(329ページ)を参照してください。

ヒント: アラートクエリが正しいことをテストするには、**検索**ユーザーインターフェイスを使用します。[検索]テキストボックスに以下の形式でクエリを入力します。

リアルタイムアラート: `|regex “regex expression”`

スケジュールされ保存されたアラート: `_deviceGroup IN [“192.0.2.3 [TCPC]”] name=“*[4924TestAlert]*” AND (“192.0.*”OR categoryBehavior CONTAINS Stop)`

クエリが正しい場合は、正規表現の二重引用符(“ ”)で囲まれた正規表現を切り取って、[リアルタイム アラートを追加(Add Realtime Alert)] ページの [**クエリ(Query)**] テキストボックスに貼り付けます。

5. [**マッチ数 (Match count)**] と [**閾値 (Threshold)**] の値を入力します。候補イベントの数が [閾値 (Threshold)] で指定した時間 (秒) 内に [マッチ数 (Match count)] の値以上になると、アラートが起動されます。

   いずれかのイベントがフィルターに一致したときに通知を受け取るには (たとえば、High CPU Temperatureなどの内部イベント)、[マッチ数 (Match count)] に1、[閾値 (Threshold)] に1を入力します。

   注: マッチ数を101以上にした場合、アラートイベントの最適なサイズを維持するため、イベントにはすべての起動イベントのイベントIDが含まれません。その結果、イベントの`baseEventCount`フィールドには、そのようなアラートイベントの一致イベントの正確な数が反映されません。

   起動イベントは、100の倍数単位で切り捨てられます。そのため、[マッチ数 (Match count)] に101を指定すると、アラートイベントには1個のイベントのみが含まれ、`baseEventCount`フィールドの値は1になります。同様に、[マッチ数 (Match count)] に720を指定すると、アラートイベントには20個のイベントのみが含まれ、`baseEventCount`フィールドの値は20になります。

6. 通知先を入力します。以下の任意の組み合わせを入力します。
   - カンマで区切った1つ以上のメールアドレス
   - SNMP通知先—詳細については、「SNMP通知先」(417ページ)を参照してください。
   - syslog通知先—詳細については、「syslog通知先」(417ページ)を参照してください。
   - ArcSightマネージャー—詳細については、「ESM通知先への通知の送信」(419ページ)を参照してください。
7. [**保存 (Save)**] をクリックします。

   作成したアラートは無効になっています。「リアルタイムアラートを有効または無効にするには」(409ページ)の手順に従って、有効にしてください。

Loggerアラートの種類

Loggerには、以下の2種類のアラートがあります。

- リアルタイムアラートは、継続的に検索を行い、指定された条件が見つかった場合は自動的に通知を送信します。詳細については、「リアルタイムアラート」(408ページ)を参照してください。
- 保存された検索アラートは、スケジュールされた間隔で検索を行い、指定された条件が見つかった場合は自動的に通知を送信します。詳細については、「保存された検索アラート」(343ページ)を参照してください。

次の表では、2種類のアラートについて比較します。

リアルタイムアラート	保存された検索アラート
定義されるアラートの数に制限はありません。 任意の時点で有効にできるアラートの最大数は25です。	任意の数のアラートを定義できます。定義されたすべてのアラートを有効にできますが、同時に実行できるアラートの最大数は50です。
設定できるメール通知先の数に制限はありませんが、設定できるSNMP、Syslog、およびESM通知先はそれぞれ1つだけです。	設定できるメール通知先の数に制限はありませんが、設定できるSNMP、Syslog、およびESM通知先はそれぞれ1つだけです。
これらのアラートには、正規表現クエリのみを指定できます。	これらのアラートのクエリは、フローベースの検索言語を使用して定義されます。この言語では、正規表現を含む複数の検索コマンドをパイプライン形式で指定できます。 chartやtopなどのアグリゲーション演算子を検索クエリに含めることはできません。
アラートはリアルタイムで起動されます。つまり、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、すぐにアラートが起動されます。	これらのアラートは、スケジュールされた間隔で起動されます。つまり、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、スケジュールされた次の間隔でアラートが起動されます。
リアルタイムアラートを定義するには、クエリ、一致数、しきい値、1つ以上の通知先を指定します。 時間範囲は、これらのアラートに対して定義されたクエリに関連付けられません。そのため、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、アラートが起動されます。	保存された検索アラートを定義するには、保存された検索(時間範囲を含むクエリ)、一致数、しきい値、1つ以上の通知先を指定します。 イベントを検索する時間範囲は、これらのアラートに関連付けられたクエリに対して指定されます。そのため、指定された時間範囲内で、指定されたしきい値内に、クエリとの一致が指定した回数に達する必要があります。また、動的な時間範囲を使用することもできます (たとえば、`$Now-1d`、`$Now`など)。 たとえば、保存された検索クエリの開始および終了時刻が次のようになっているとします。 • 開始時刻: 2010年5月11日の午前10時38分04秒 • 終了時刻: 2010年5月12日の午前10時38分04秒 そして、一致数としきい値が以下のようになっているとします。 • 一致数: 5 • しきい値: 3600 その場合、このアラートが起動されるには、2016年5月11日の午前10時38分04秒から、2016年5月12日の10時38分04秒の間の1時間の間に5個のイベントが発生する必要があります。

アラートの起動と通知

アラートは、指定されたしきい値 (秒単位の期間) 内に指定された数の一致が発生した場合に起動されます。アラートが起動されると、Loggerはトリガーイベントまたはイベント IDを含むアラートイベントを作成し、設定済みの通知先 (メールアドレス、SNMPサーバー、Syslogサーバー、ArcSightマネージャー) に通知を送信します。

デフォルトでは、メール通知先に送信されるアラート通知のみに、アラートを起動したすべての一致イベントが含まれます。SNMP、Syslog、ESMへの通知にも一致イベントを含めるようにLoggerを設定することができます。ただし、この種の設定はLoggerのコマンドラインインターフェイスでしか行えないため、カスタマーサポートにお問い合わせください。

アラートイベントが起動されるタイミング

期間と一致イベントの数も指定します。その数の一致イベントがその期間内に検出されると、アラートイベントが起動されます。

Loggerは、100個の一致イベントを検出した後でカウントをリセットします。そのため、その期間内に発生するすべてのイベントが、必ずしもアラートに記録されるわけではありません。たとえば、2分間に一致イベントが20個発生するたびにアラートが送信されるように設定した場合、2分間に152個のイベントが発生すると、アラートは7回送信され、12個の一致イベントはどのアラートにも含まれません。この状況では、以下のアラートイベントが起動されます。

- アラート1の一致イベントは20個
- アラート2の一致イベントは40個
- アラート3の一致イベントは60個
- アラート4の一致イベントは80個
- アラート5の一致イベントは100個 (1～100)
- アラート6の一致イベントは20個 (101～120)
- アラート7の一致イベントは40個 (101～140)

残りの12個のイベントは残ったままとなり、2分間でさらに20個のイベントというしきい値に達するかどうかを判断するために使用されます。

アラート通知の受信

アラートからの通知を受信するには、メールアドレス、SNMPサーバ、syslogサーバー、ArcSightマネージャーなどの、あらかじめ設定された通知先に送信されるようにアラートを設定します。

デフォルトでは、メール通知先に送信されるアラートのみに、アラートを起動したすべての一致イベントが含まれます。SNMP、Syslog、およびESM通知先についても、一致イベントを含めるようにLoggerを設定できます。ただし、そのような設定は、Loggerのコマンド行インターフェイスによってのみ可能であるため、手順についてはカスタマーサポートにお問い合わせください。

通知先を設定する方法については、「ESM通知先」(419ページ)、「SNMP通知先」(417ページ)および「syslog通知先」(417ページ)を参照してください。メール通知先を設定するには、「静的ルート」(496ページ)も参照してください。

注: アラートの監査イベントは、デフォルトでは内部ストレージグループのみに書き込まれ、ESMに転送されません。これらの監査イベントをESM通知先に転送する必要がある場合は、カスタマーサポートにお問い合わせください。これは、アラート用に生成された監査イベントのみに適用され、他の監査イベントはESM通知先に送信することができます。

メール通知先への通知の送信

アラートの通知をメールで送信する場合、メールメッセージには、起動アラート情報と一致(ベース)イベントの両方が含まれます。

以下に起動アラート情報の例を示します。

```
Alert event match count [1], threshold [10] sec
```

一致イベントは以下のとおりです。

```
Event Time [Tue May 11 16:46:49 PST 2016]

Event Receipt Time [Tue May 11 16:46:50 PST 2016]

Event Device Address [192.0.2.1]

Event Content [May 11 10:31:20 localhost
CEF:0|NetScreen|Firewall/VPN||traffic:1|Permit|Low| eventId=590 msg=start_
time\= “2016-05-11 15:25:02” duration\=15 policy_id\=0 service\=SSH proto\=6
src zone\=Trust dst zone\=Untrust action\=Permit sent\=656 rcvd\=680
src\=192.0.2.4 dst\=192.0.2.5 src_port\=54759 dst_port\=22 translated
ip\=192.0.2.2 port\=54759 app=SSH proto=TCP in=680 out=656
categorySignificance=/Normal categoryBehavior=/Access
categoryDeviceGroup=/Firewall categoryOutcome=/Success
categoryObject=/Host/Application/Service art=1165861874880 cat=Traffic Log
deviceSeverity=notification act=Permit rt=1165861874880 shost=n111-
h046.qa.arcsight.com src=192.0.2.4 sourceZoneURI=/All Zones/System
Zones/Private Address Space/RFC1918: 192.0.2.0-192.255.255.255
sourceTranslatedAddress=192.0.2.2 sourceTranslatedZoneURI=/All Zones/System
Zones/Public Address Space/192.0.2.0-192.0.255.255 spt=54759
sourceTranslatedPort=54759 dst=192.0.2.10 destinationZoneURI=/All
Zones/System Zones/Private Address Space/RFC1918: 192.0.2.0-192.255.255.255
dp]
```

アラート通知の設定

アラート通知を設定するには

1. 目的のメールアドレス通知先によってLoggerのSMTPを設定する(「静的ルート」(496ページ)を参照)か、SNMP通知先(「SNMP通知先」(417ページ)を参照)またはSyslog通知先(「syslog通知先」(417ページ)を参照)を作成します。

   アラートごとの通知先の数:

   - メール: 複数。カンマで区切ります。
   - SNMP: 1
   - syslog: 1
2. 関心のあるイベントを探すためのクエリを作成し、クエリをフィルターとして保存します「クエリの保存 (保存された検索、保存されたフィルターの作成)」(142ページ)を参照してください。

   注: アラートに指定するクエリでは、正規表現のみを使用できます。
3. 新しいフィルターを使用するアラートを作成し、一致数としきい値を指定します(「保存された検索」(333ページ)を参照)。
4. 新しいアラートを有効にします。

syslogおよびSNMP通知先への通知の送信

SNMPおよびsyslog通知先にアラートを送信するようにLoggerを設定する場合は、以下の内容をよくお読みください。

- Loggerは、SNMP v2cおよびv3をサポートしています。
- メールアラートと違い、起動アラートは、アラートを起動した一致 (ベース) イベントを含むアラートとは別に送信されます。
- すべてのSNMPアラートはSNMPトラップとして送信されます。そのため、起動アラートとそれに関連する一致 (ベース) イベントは、SNMP通知先でSNMPトラップとして受信されます。SNMPトラップには起動イベントが含まれますが、アラートの起動原因となったイベント (一致イベント) は含まれません。起動イベントには、すべての一致イベントのイベントIDが含まれます。起動アラート内のイベントIDを使用して、関連する一致イベントを識別できます。

  注: 非CEFイベントにはイベントIDが含まれていません。そのようなベースイベントをその起動アラートと関連付ける必要がある場合は、そのようなイベントを、Loggerにコネクターを通じて送信してください。
- SNMPはUDPを使用してパケットを送信します。その結果、SNMP通知先にアラートが到着する順序は保証されません。

- syslogイベントがUDPを使用して送信されるとき、起動アラートと一致イベントが到着する順序は保証されません。

SNMP通知先

SNMP通知先は、SNMP (Simple Network Management Protocol) を使用してアラート通知を送信する方法を表します。SNMP通知先は、それを使用するアラートを作成する前に設定します。SNMP通知先を設定する前に、「syslogおよびSNMP通知先への通知の送信」(416ページ)の内容をよくお読みください。

SNMP通知先を追加するには

1. [**設定 | データ**] メニューを開き、[**SNMP 通知先**] をクリックします。
2. [**追加**] ボタンをクリックします。
3. 以下のパラメーターを入力します。

パラメーター	説明
SNMP 通知先名	この通知先の名前。
コネクタ名	SmartConnector名。
コネクタの場所	SmartConnectorマシンの物理的な場所。場所を指定しない場合は「None」と入力します。
Loggerの場所	Loggerの物理的な場所を示すオプションのコメント。
SNMPホスト	ホスト名またはIPアドレス。
SNMPポート	デフォルトでは162。
コミュニティ名	SNMPコミュニティ名。

4. [**保存**] をクリックして新しいSNMP通知先を作成します。

SNMP通知先を削除するには

1. [**設定 | データ**] メニューを開き、[**SNMP 通知先**] をクリックします。
2. 削除するSNMP通知先を探し、その行の [削除] アイコン (✖) をクリックします。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてSNMP通知先を保持します。

syslog通知先

syslog通知先は、比較的単純なsyslogプロトコルを使用してアラート通知を送信する方法を表します。Syslog通知先は、それを使用するアラートを作成する前に設定する必要があり

ます。Syslog通知先を設定する前に、「syslogおよびSNMP通知先への通知の送信」(416ページ)の内容をよくお読みください。

syslog通知先を追加するには

1. [**設定 | データ**] メニューを開き、[**Syslog 通知先**] をクリックします。
2. [**追加**] ボタンをクリックします。
3. 以下のパラメーターを入力します。

パラメーター	説明
名前	この通知先の名前。
タイプ	UDPまたはTCP Syslog。 **注:** この選択内容は後で編集できません。

4. [**次へ**] をクリックします。以下の二次パラメーターを入力します。

パラメーター	説明
名前	通知先の名前。
タイプ	これは、前の画面で入力した値です。この値は変更できません。
IP/ホスト	ホスト名またはIPアドレス。
ポート	ポート(デフォルトは514)。
接続再試行タイムアウト	(TCP Syslog通知先のみ)接続を再試行する前に待機する時間(秒単位)。デフォルトは5秒です。

5. [**保存**] をクリックして新しいsyslog通知先を作成します。

syslog通知先を編集するには

1. [**設定 | データ**] メニューを開き、[**Syslog 通知先**] をクリックします。
2. [編集] アイコン ( ) をクリックします。Syslog通知先の種類以外のパラメーターを編集できます。
3. [**保存**] をクリックして変更するか、[**キャンセル**] をクリックしてSyslog通知先の表に戻ります。

syslog通知先を削除するには

1. [**設定 | データ**] メニューを開き、[**Syslog 通知先**] をクリックします。
2. 削除するsyslog通知先を探し、その行の [削除] アイコン ( ) をクリックします。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてsyslog通知先を保持します。

ESM通知先への通知の送信

ESM通知先は、ArcSightマネージャーにアラート通知を送信する方法を表します。ESM通知先は、それを使用するアラートを作成する前に設定します。

ArcSightマネージャーが署名付きSSL証明書を使用する場合は、Loggerに証明書をロードする必要があります。

注: アラートの監査イベントは、デフォルトでは内部ストレージグループのみに書き込まれ、ESMに転送されません。アラート用に生成された監査イベントをESMに転送する必要がある場合は、カスタマーサポートに問い合わせて支援を受けてください。

ArcSightマネージャーにアラートを送信するようにLoggerを設定するには

1. ArcSightマネージャーが証明書を使用する場合は、サーバーSSL証明書ファイルを、ArcSightコンソールまたはターゲットのマネージャーとすでに通信している他のコンポーネントからコピーし、「証明書のLoggerへのアップロード」(423ページ)の説明に従って証明書ファイルをLoggerにアップロードします。

   注: 信頼済みの証明書のリポジトリであるcacertsファイルをLoggerにインポートすることはできません。代わりに、特定のSSL証明書ファイルをインポートする必要があります。

2. 「ESM通知先を作成するには」(421ページ)の説明に従って、ESM通知先を作成します。

ESM通知先

ESM通知先は、LoggerとArcSightマネージャーの間の信頼関係接続を確立し、Loggerの組み込みSmartConnectorを使用して、Loggerからマネージャーにイベントおよびアラートを共通イベントフォーマット (CEF) で転送できるようにします。

CEFイベントは、すでに正規化または分類されています。CEFの詳細については、『Implementing ArcSight CEF』を参照してください。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品マニュアルのコミュニティで「ArcSight Common Event Format (CEF) Guide」を検索してください。

Loggerは、以下の種類のイベントをArcSightマネージャーに転送できます。

- ArcSightマネージャーに接続されているArcSight Syslog SmartConnectorへのsyslogイベントの転送

- Logger ESM通知先を使用したArcSightマネージャーへの共通イベントフォーマット (CEF) イベントの直接転送。ESM通知先は、ArcSightコンソールにとってはSmartConnectorに見えます。
- 指定された種類が [その他] 以外の、ファイル受信者によって受信されたイベント。そのようなイベントは、ArcSight Streaming SmartConnectorを使用して転送されます。

ESM通知先の最大数: ご使用のSmartConnectorでは、許容される通知先の数に制限はありません。ただし、パフォーマンス上の理由で、HPE ArcSightでは、1つのArcSightマネージャーを指すESM通知先を3つ以上作成しないことを推奨しています (ほとんどの場合、1つで十分です)。

注: Loggerに組み込まれているSmartConnectorでは、リソースを大量に消費するため、基本アグリゲーションを使用しないでください(基本アグリゲーションは、ArcSightコンソールの [**アグリゲーションを有効にする (秒単位)**] フィールドを使用して設定します)。代わりに、ArcSightコンソールで次の手順を実行して、フィールドベースアグリゲーションを設定してください。

1. 基本アグリゲーションを無効にするために、[処理] > [アグリゲーションを有効にする (秒単位)] が [**無効**] に設定されていることを確認します。
2. コネクターを右クリックして、[**inspect/edit/**] を選択します。

フィールドベースアグリゲーションの設定方法の詳細については、ArcSight SmartConnectorの『ユーザーガイド』を参照してください。

ArcSightマネージャーにイベントを転送するようにLoggerを設定するには

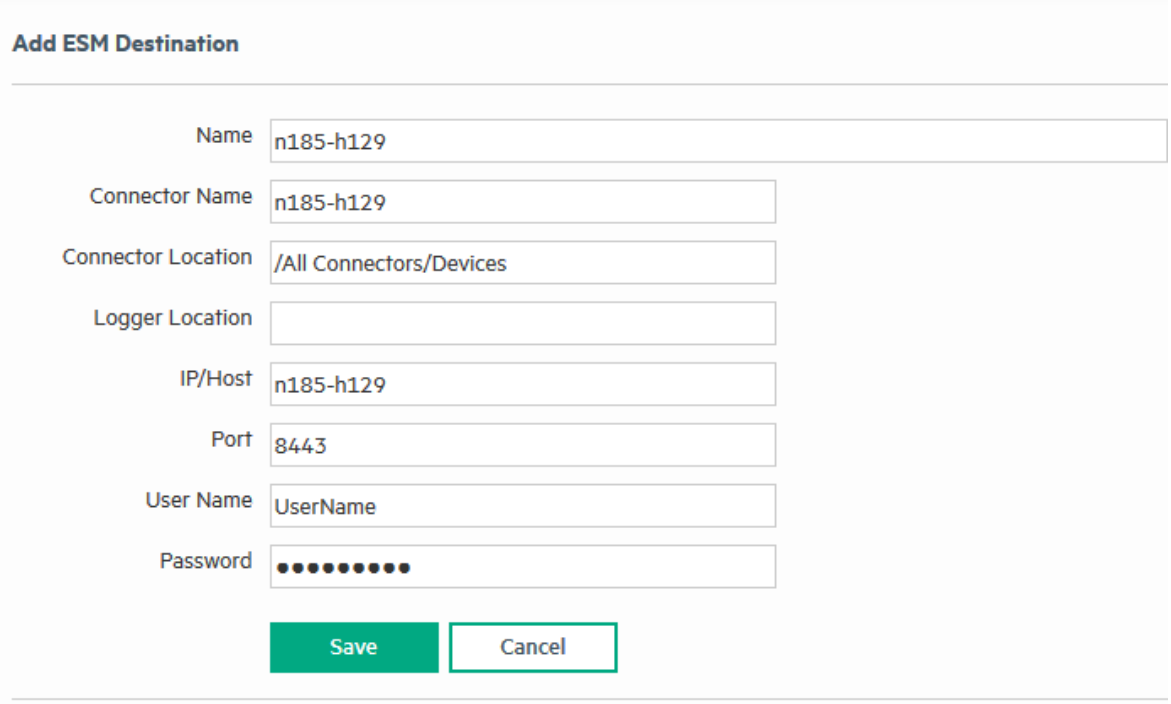
1. ArcSightコンソールまたはターゲットのマネージャーとすでに通信している他のコンポーネントからサーバーSSL証明書ファイルをコピーし、「証明書のLoggerへのアップロード」(423ページ) の説明に従って証明書ファイルをLoggerにアップロードします。

   LoggerがFIPSモードで動作している場合、ArcSightマネージャーの有効で最新の (期限が切れていない) サーバーSSL証明書ファイルがLogger上で必要です。これがないと、転送者はイベントを転送しません。

   注: 信頼済みの証明書のリポジトリである`cacerts`ファイルをLoggerにインポートすることはできません。代わりに、特定のSSL証明書ファイルをインポートする必要があります。

2. 「ESM通知先を作成するには」(421ページ) の説明に従って、ESM通知先を作成します。
3. このESM通知先を参照するESM転送者を作成します (「転送者」(398ページ) を参照)。

[ESM通知先 (ESM Destinations)] ページ



ESM通知先を作成するには

「証明書のLoggerへのアップロード」(423ページ) の説明に従ってArcSightマネージャーの証明書ファイルをロードしてからLoggerで通知先として追加してください。Logger上に証明書ファイルが存在しない場合は、ESM通知先を作成できません。

1. **[設定 | データ]** メニューを開き、**[ESM 通知先]** をクリックします。
2. **[追加]** をクリックします。[ESM通知先] ページが表示されます。
3. 以下のパラメーターを入力します。

パラメーター	説明
名前 (Name)	このESM通知先の名前。
コネクタ名 (Connector Name)	SmartConnector名。
コネクタの場所 (Connector Location)	SmartConnectorマシンの物理的な場所。場所を指定しない場合は「None」と入力します。
Loggerの場所 (Logger Location)	Loggerの物理的な場所。場所を指定しない場合は「None」と入力します。

パラメーター	説明
Ipまたはホスト (IP/Host)	この転送者がイベントを送信するArcSightマネージャー。 **注:** このフィールドに指定する名前またはIPアドレスが、ArcSightマネージャーで設定されている名前またはIPアドレスと正確に一致していることを確認してください。2つの名前またはIPアドレスが一致しない場合、ESM通知先を正常に設定できません。
ポート (Port)	通常は8443です。
ユーザ名 (User Name)	管理者権限を持つArcSightマネージャーの既存のユーザーの名前。
パスワード (Password)	ログインユーザーのパスワード。 このパスワードには、特殊文字のうち、パーセント (%)、等号 (=)、セミコロン (;)、二重引用符 (“)、単一引用符 (‘)、小なり不等号 (<)、大なり不等号 (>) を使用できません。 **注意:** ArcSightマネージャーではこれらの特殊文字をパスワードで使用できますが、Loggerでは使用できません。ArcSightマネージャーユーザーのパスワードにこれらの文字が含まれている場合は、このパスワードを設定する前に、ArcSightマネージャーでパスワードを変更する必要があります。

4. **[保存]** をクリックします。

ヒント: 新しいESM通知先を追加するときに次のエラーを受け取った場合は、[IPまたはホスト] フィールドに指定したホスト名が、ArcSightマネージャーで設定した名前と正確に一致していることを確認してください。

```
There was a problem: Failed to add destination
```

さらに、ArcSightマネージャーがIPアドレスではなく、ホスト名を使用して設定されている場合は、ArcSightマネージャーホスト名とIPアドレスをLoggerのホストファイル(**[システム管理] > [ネットワーク] > [ホスト]**)に必ず追加してください。

ESM通知先を削除するには

1. **[設定 | データ]** メニューを開き、**[ESM 通知先]** をクリックします (アラートを転送するためのESM通知先を削除する場合は、**[アラート]** をクリックし、**[ESM 通知先]** ページを開きます)。
2. 削除するESM通知先を探し、その行の [削除] アイコン (✖) をクリックします。
3. **[OK]** をクリックして削除を確定するか、**[キャンセル]** をクリックしてESM通知先を保持します。

証明書

証明書のLoggerへのアップロード

Loggerからイベントとアラートを転送するArcSightマネージャーの有効なサーバーSSL (Secure Sockets Layer) 証明書ファイルをアップロードします。

マネージャーでFIPS 140-2モードが有効になっていない場合は、マネージャー用の証明書ファイルを以下の方法で入手できます。

- マネージャーのキーストアから
- ArcSightコンソールのトラストストアから
- マネージャーと通信するいずれかのSmartConnectorのトラストストアから

『ArcSight ESM管理者ガイド』の「証明書のエクスポート」の手順に従い、keytoolguiユーティリティを使用してマネージャーの証明書をエクスポートします。キーストアおよびトラストストアと、マネージャー、ArcSightコンソール、およびSmartConnector上でのそれらの場所については、『ArcSight ESM管理者ガイド』を参照してください。

マネージャー用の証明書をエクスポートしたら、Loggerに接続するマシンにコピーします。

マネージャーでFIPS 140-2モードが有効になっている場合は、次のコマンドを実行して、マネージャーの証明書をマネージャーの<ARCSIGHT_HOME>/binディレクトリからエクスポートします。

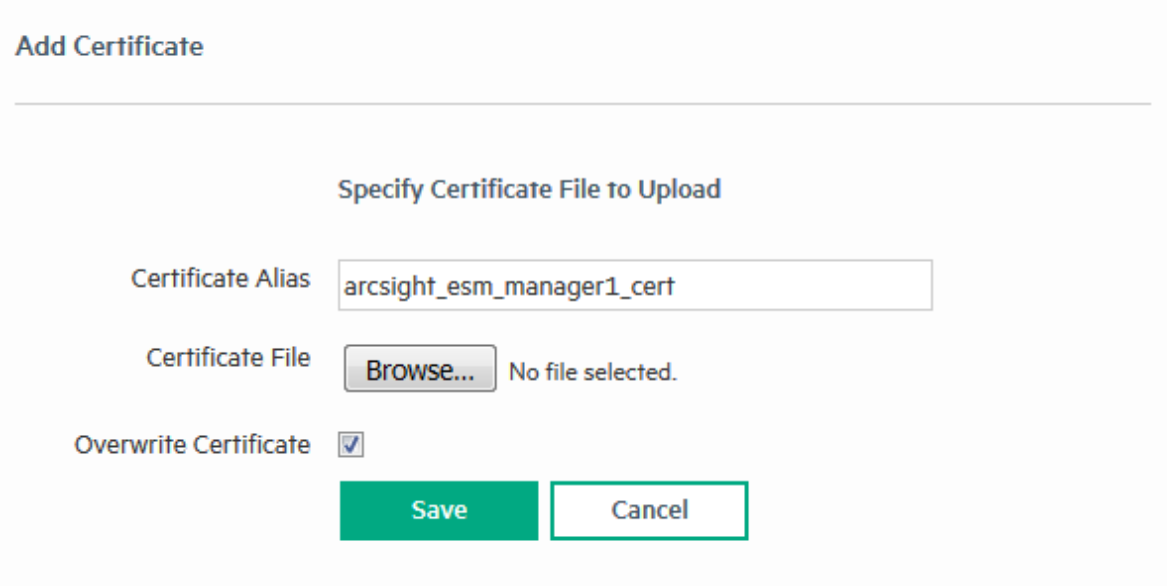
```
arcsight runcertutil -L -n managerkey -r -d <ARCSIGHT_
HOME>/config/jetty/nssdb -o <absolute_path_to_manager.cert>
```

このコマンドは、マネージャーの証明書であるmanager.certファイルを、上記のコマンドで指定した場所に生成します。

注: manager.certファイルの格納先の絶対パスを指定しなかった場合、デフォルトでは、manager.certファイルは<ARCSIGHT_HOME>ディレクトリにエクスポートされます。

ESM通知先のための証明書ファイルをアップロードするには

1. マネージャーの証明書を、Loggerに接続するマシンにコピーしてあることを確認します。
2. **[設定 | データ]** メニューを開き、**[証明書]** をクリックします。
3. **[追加]** をクリックし、以下の画面を表示します。



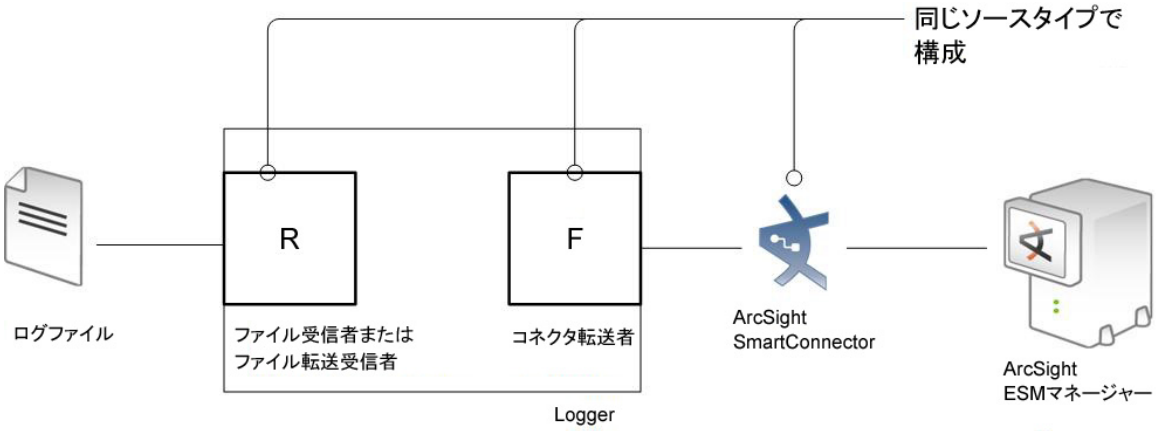
4. 証明書ファイルの別名を入力します。この名前は、証明書ファイルを容易に識別するために使用されます。たとえば`arcsight_esm_manager1_cert`とします。
5. **[ブラウズ (Browse)]** をクリックして、コピーしたマネージャー証明書ファイルの場所を参照します。
6. この証明書で、同じ別名の既存の証明書を上書きするには、[資格情報を上書き (Overwrite Certificate)] チェックボックスをオンにします。
7. **[保存 (Save)]** をクリックします。

ログファイルイベントのESMへの転送

Loggerは、ログファイルからイベントを読み込み、それらのイベントをLoggerストリーミングSmartConnectorに転送できます。イベントは、そこからArcSightマネージャーに送信されます。

ログファイルイベントをESMに転送するには、同じソースタイプを受け入れるように受信者、転送者、およびSmartConnectorを設定します(「ソースタイプの使用」(389ページ) を参照)。

注: LoggerからArcSight ESMにログファイルイベントを正常に転送するには、受信者、転送者、およびSmartConnectorはすべて**同じソースタイプ値**を使用して設定する必要があります。



syslog、SmartMessage、CEFなど、Loggerが受信するイベントと異なり、ログファイルイベントは、イベントのタイムスタンプを特定するために解析する必要があります。そのため、コネクター転送者を使用してイベントをESMに転送する必要がある場合は、受信者に以下のソースタイプのいずれかを選択する必要があります。

ソースタイプ	
Apache HTTP Server Access	Microsoft DHCP Log
Apache HTTP Server Error	Other
IBM DB2 9.x Audit Log	Tipping Point SMS 2.5 syslog
IBM DB2 Audit	VMware ESX syslog
Juniper Steel-Belted Radius	

データ検証

データ検証画面では、Loggerデータファイルに対して監査品質検証を実行できます。この画面から、指定した時間範囲内のすべてのデータファイルのハッシュ値を確認して、データを検証できます。この機能は、管理者のみが使用できます。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

データ検証処理では、SHA1ハッシュアルゴリズムを使用して、指定された時間範囲内のデータファイルのハッシュ値を計算し、事前に計算された値と比較して、データファイルの整合性を判定します。各データファイルには最大1GBのデータが格納されます。ハッシュ値は、データファイルが一杯になった後で計算されます。データファイルがまだ一杯になっていない場合は、その検証結果を算出できません。

前提条件

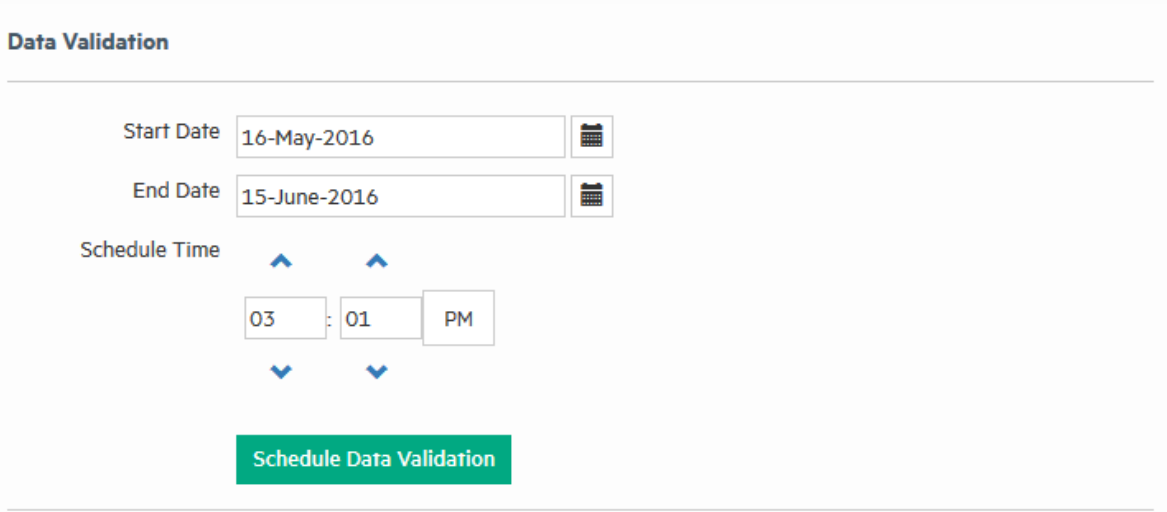
この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

詳細については、「Loggerのユーザー権限の設定」(546ページ)を参照してください。

Logger上のデータを検証するには

1. **[設定 | データ]** メニューを開き、**[データ検証]** をクリックします。



2. **[開始日 (Start Date)]** および **[終了日 (End Date)]** フィールドで、検証するデータの範囲を指定します。
3. **[スケジュール時刻 (Schedule Time)]** の各フィールドにある上下の矢印を使用して、検証を実行する時刻を指定します。
4. [**Email Me Validation Results**] チェックボックスをオンにして、検証プロセスが完了すると同時に検証結果を通知する電子メールをLoggerが送信するようにします。Loggerは、ログイン済みユーザーのために保存されているメールアドレスに、この通知を送信します。

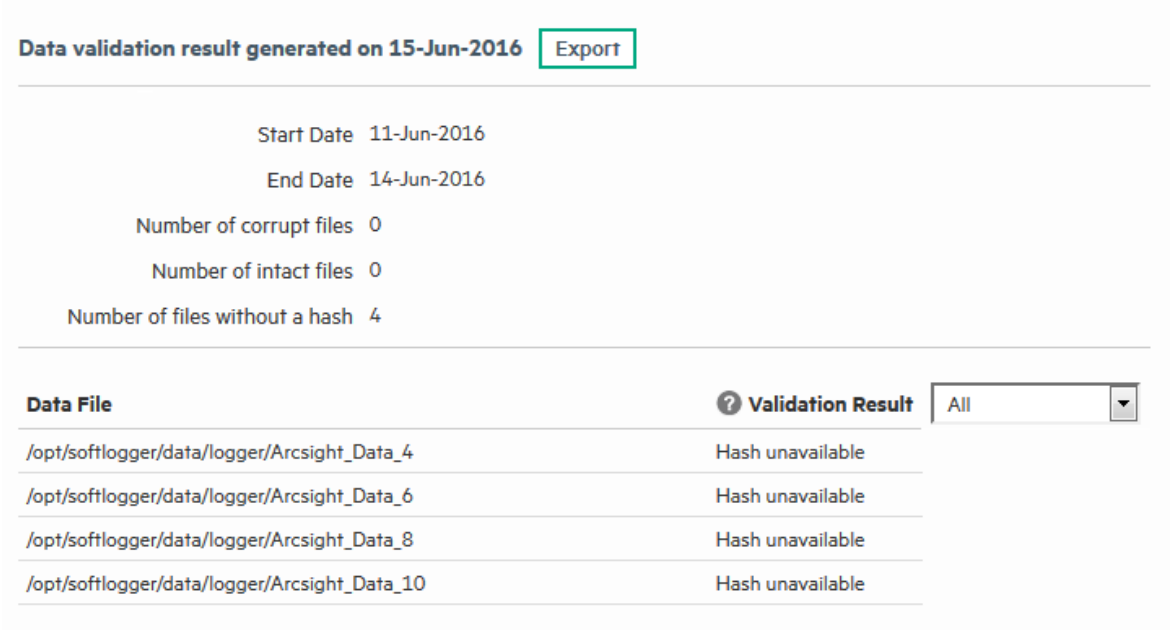
   注: [**Email Me**] オプション使用できない場合は、LoggerのSMTPサーバーが設定されていません。この機能は、Loggerのシステム管理者が有効にすることができます。詳細については、「SMTP」(500ページ)を参照してください。

5. **[データ検証のスケジュール (Schedule Data Validation)]** をクリックします。

   注: 実行中のデータ検証はキャンセルできません。 データ量が多いと、データ検証処理に長い時間がかかることがあります。そのため、ピーク時間外に処理を実行するようスケジュールし、時間範囲を狭めて関心のあるデータのみを含めるようにしてください。

データ検証処理が完了すると、指定された時間範囲内の各データファイルが、その検証結果とともに表示されます。[Email Me] チェックボックスを選択した場合は、「Data Validation

results from Logger <Loggerホスト名>」という件名の電子メールが、ログイン済みユーザーのために保存されているメールアドレスに送信されます。



検証結果を表示するには

- **[検証結果 (Validation Result)]**ドロップダウンの下矢印をクリックして、表示する結果の種類を選択します。[すべて]、[破損]、[正常]、[ハッシュなし] のいずれかを選択できます。

  または
- 検証データが格納されたスプレッドシートをダウンロードするには、**[エクスポート (Export)]** をクリックします。

次の表で、考えられる検証結果について説明します。

表示される値	エクスポートされたファイル内の値	説明
正常	True	ハッシュが一致。データは変更されていません。
破損	False	ハッシュが不一致。データが変更されたか壊れています。
ハッシュなし	N/A	ファイルにハッシュがありません。データを検証できませんでした。データファイルがまだ一杯になっていないか、データファイルが以前のバージョンのLoggerで作成されていることが考えられます。

注: Logger 6.0以前のバージョンからシステムをアップグレードした場合は、旧バージョンのデータのステータスはN/Aになっています。これは、データの作成時にデータ検証ハッシュ値が格納されていないためです。ただし、将来のアップグレードでは、ハッシュ検証データが保持され、アップグレード後にデータを検証できるようになります。

ストレージ

[設定 | ストレージ] カテゴリのオプションを使用すると、Loggerでデータを保存する方法を管理できます。さまざまなストレージグループによって、複数の保有ポリシーの実装がサポートされています。各グループのポリシーは違っていてもよく、また、ストレージルールによって、特定のデバイスグループからのイベントに使用するストレージグループが決まります。詳細については、『Loggerインストールガイド』を参照してください。

ストレージグループ

ストレージグループは、イベントを保持する最大サイズ (割り当て済み (GB)) と日数 (最大期間) を定義することで、複数の保有ポリシーをサポートしています。イベントが最大期間で指定された日数よりも古くなるか、ストレージグループに保持するイベント数 (最大サイズで指定) を超えると、最も古いイベントが次の保有サイクルで削除されます。保有プロセスはLogger上で定期的に起動されるため、イベントが最大期間よりも古くなるか、ストレージグループのサイズが最大サイズの上限を超えても、すぐには削除されない可能性があります。

Loggerには、最大で6つのストレージグループを作成できます。そのうちの2つはLoggerにあらかじめ存在し (内部ストレージ グループとデフォルトのストレージ グループ)、4つをユーザーが作成できます。ストレージグループはいつでも追加できます (最大6つ)。

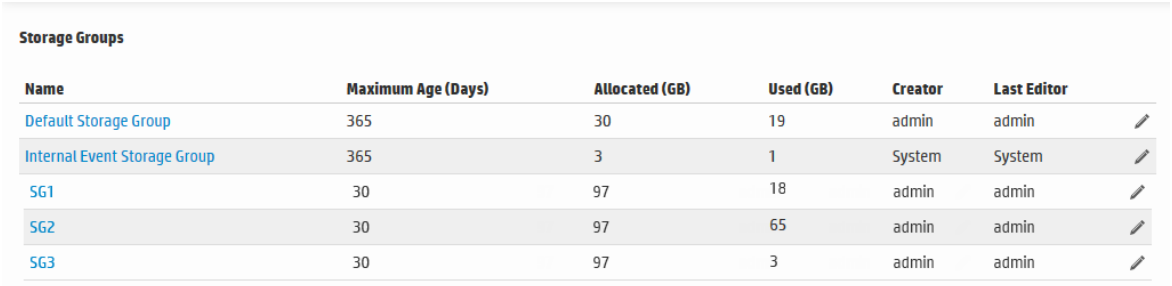
あらかじめ存在するストレージグループに加えて、4つのストレージグループを作成することをお勧めします。これにより、イベントの保存用に5つのストレージグループを使用でき、Loggerの内部イベント用に1つを使用できます。

ストレージグループを追加するには、「ストレージグループの追加」(459ページ) の手順に従ってください。

作成されたストレージグループは削除できませんが、そのサイズはいつでも増減できます。ストレージグループのサイズを小さくする場合で、新しいサイズがストレージグループ上で現在使用している領域よりも小さい場合、新しいサイズに合わせるためにデータを削除する必要があり

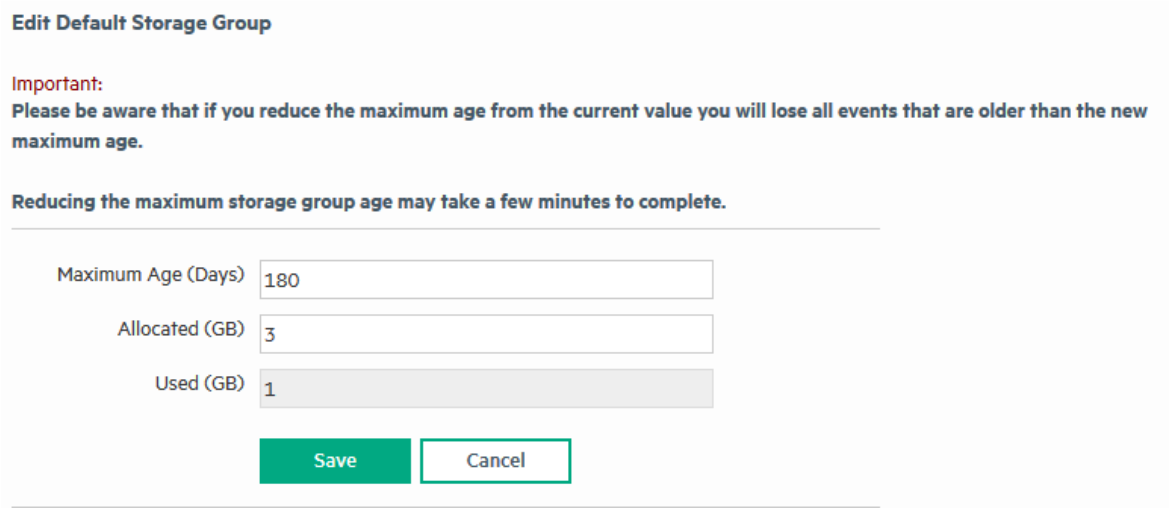
ます。このような状況では、LoggerのUIで、必要なデータを削除するためのガイドが提供されます。

[ストレージ グループ (Storage Group)] ページ



ストレージグループを編集するには (サイズ変更を含む)

1. [**設定 | ストレージ**] メニューを開き、[**ストレージ グループ**] をクリックします。
   [ストレージ グループ] ページに使用可能なストレージグループが表示されます。
2. 変更するストレージグループを特定し、関連付けられている [**編集**] アイコン( )をクリックします。[ストレージ グループ] ページに [<ストレージグループ名>ストレージ グループを編集 (Edit <ストレージグループ名> Strage Group)] ペインが表示されます。



3. ストレージグループ名を変更したり、[最大期間 (Maximum Age)] や [割り当て済み (Allocated)] を増減します。

   注: 内部ストレージ グループとデフォルトのストレージ グループの名前は変更できません。

   ストレージグループのサイズを小さくする場合 で、新しいサイズが [ストレージ グループを編集 (Edit Storage Group)] ページの [**使用済み (GB) (Used (GB))**] フィールドに示されている現在のサイズよりも小さい場合は、この状況でストレージグループのサイズを小さくす

るには、既存のデータを削除する必要があることを示すメッセージがLoggerで表示されます。

データを削除してストレージグループサイズを減らす場合は、以下の手順に従います。

a. [**最大期間 (Maximum Age)**] の値を、メッセージに示される数値に設定します。これにより、イベントの削除が起動されます。
b. [ストレージ グループを編集] 画面を更新します。[**使用済み (GB) (Used (GB))**] の値が、設定するストレージグループサイズ以下になっている場合は、次のステップに進みます。そうでない場合は、画面を定期的に更新し続けます。

   注: [使用済み (GB)] の値は、データが削除されることで変化しますが、時間がかかる場合があります。そのため、次のステップに進む前に待つ必要があります。

c. [**使用済み (GB) (Used (GB))**] を必要な値に設定します。
d. 必要であれば、[**最大期間 (Maximum Age)**] の設定 (ステップaで変更) を元の値に戻します。

   データを削除しない場合は、次のステップに進んで手順を終了します。

   注: ストレージグループのサイズを小さくするときに、十分な空き領域がある場合は、保有ポリシーを変更してデータを削除するために [最大期間] の値を変更することなくサイズを変更できます。

4. [**保存 (Save)**] をクリックして変更内容を保存するか、[**キャンセル (Cancel)**] をクリックして終了します。

ストレージルール

ストレージルールは、デバイスグループとストレージグループの間のマッピングを作成します。このマッピングにより、特定のソースからのイベントを特定のストレージグループに保存できます。これらのストレージグループは異なる保有ポリシーを使用して設定できるため、受信イベントのソースに基づいてイベントデータを保持できます。たとえば、ファイアウォールデバイスからのすべてのイベントの保有期間を短くすることができます。そのためには、ファイアウォールデバイスをデバイスグループに手動で割り当て、保有期間の短いストレージグループにデバイスグループをマッピングするようなストレージルールを作成します。

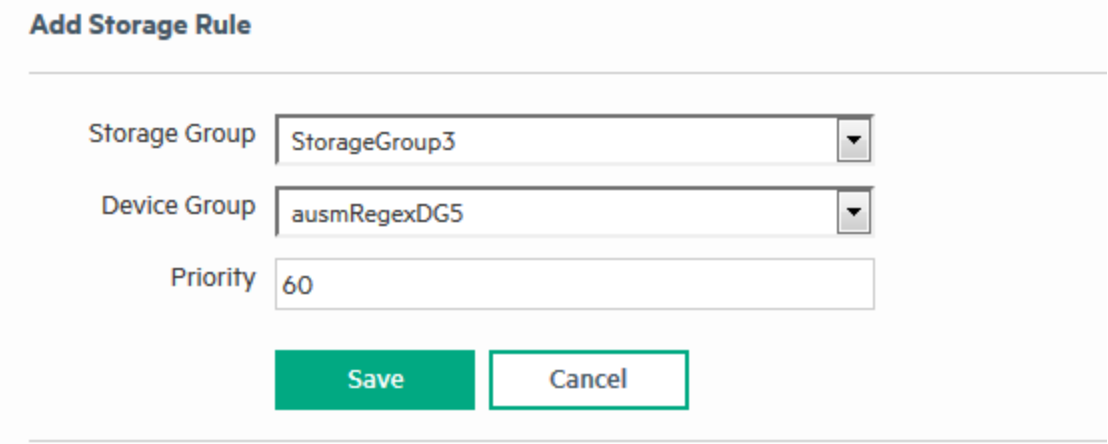
ヒント: どのストレージルールも適用されないイベントは、デフォルトのストレージグループに送られます。

ストレージルールを追加する前に、イベントを保存するストレージグループと、イベントの保存対象のデバイスを含むデバイスグループが存在することを確認してください。デバイスグループの作成方法については、「デバイスグループ」(367ページ) を参照してください。

Loggerでは、最大40個のストレージルールを作成できます。追加のルールを作成すると、エラーが生成される可能性があります。

ストレージルールを追加するには

1. [**設定 | ストレージ**] メニューを開き、[**ストレージ ルール**] をクリックします。
2. [**追加**] をクリックします。[ストレージ ルールを追加 (Add Storage Rule)] ページが表示されます。



3. 以下のパラメーターを入力します。

パラメーター	説明
ストレージ グループ	ドロップダウンリストからストレージグループを選択します。ストレージグループは、ストレージルールを追加する前に設定されている必要があります。
デバイスグループ	ストレージグループに関連付ける、デバイスを選択します。 **注:** ストレージグループ内の複数のデバイスからのイベントを含める場合は、必要なすべてのLoggerデバイスを含むデバイスグループを作成してから、ストレージルール用のデバイスグループを選択します。
優先順位	新しいルールの優先順位を示す整数。数値は、ストレージルールごとに一意であることが必要です。数値が小さいほどルールの優先順位が高くなります。

4. [**保存 (Save)**] をクリックして新しいストレージルールを追加するか、[**キャンセル (Cancel)**] をクリックして終了します。

ストレージルールを編集または順序変更するには

1. [**設定 | ストレージ**] メニューを開き、[**ストレージ ルール**] をクリックします。
2. 編集するストレージルールを探し、その行の [編集] アイコン (✎) をクリックします。
3. フォームの情報を変更します。たとえば、重要度の値を変更して、表内のストレージルールの位置を変更します。その後、[**保存**] をクリックします。

ストレージルールを削除するには

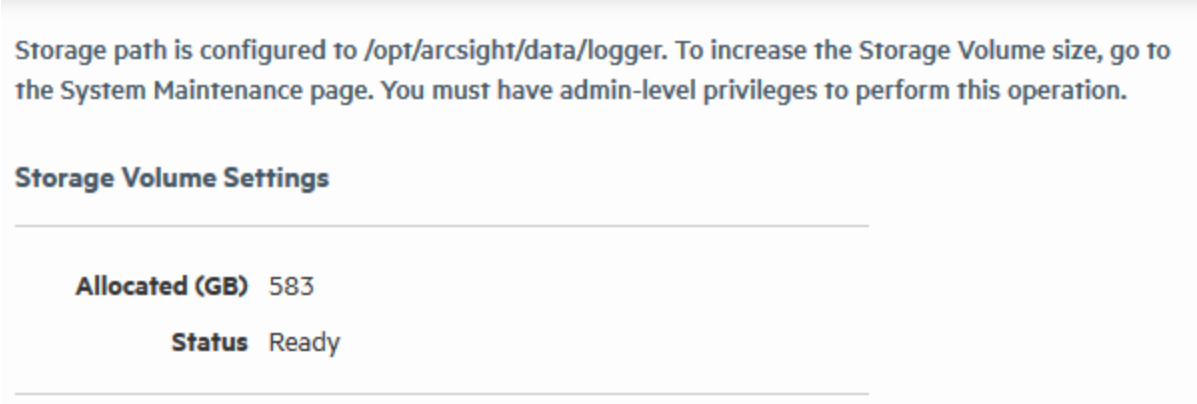
1. [**設定 | ストレージ**] メニューを開き、[**ストレージ ルール**] をクリックします。
2. 削除するストレージルールを探し、[削除] アイコン (✖) をクリックします。
3. **[OK]** をクリックして削除を確認します。

ストレージボリューム

[ストレージ ボリューム] ページには、マウント場所と現在のストレージボリューム設定が表示されます。

既存のストレージボリュームの設定を表示するには

1. ナビゲーションバーの [設定 | ストレージ] メニューから、[**ストレージ ボリュームの設定**] を選択します。



ストレージボリュームのサイズを増やすには

詳細については、「ストレージボリュームサイズの増加」(457ページ) を参照してください。この操作を行うには、管理者レベルの特権が必要です。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

イベントアーカイブ

イベントアーカイブを使用すると、現在の日を含まない過去の任意の日のイベントを保存できます。イベントアーカイブを作成する前に、アーカイブストレージの設定を行う必要があります。アーカイブストレージ設定は、イベントアーカイブを書き込む場所を指定します。

注意: 設定バックアップ (設定用) とイベントアーカイブ (データ用) の両方が定期的に実行され、リモートロケーションに保存されていることを確認してください。致命的な障害が発生した場合は、最新の設定バックアップとイベントアーカイブを復元する必要がありま

す。設定バックアップについては、「設定のバックアップとリストア」(468ページ)を参照してください。

- Loggerアプライアンスの場合、この場所はNFSマウント、CIFSマウント、またはSANでなければならず、これはLoggerユーザーインターフェイスを使用して設定されます。
- ソフトウェアLoggerの場合は、この場所はディレクトリです (ローカルディレクトリか、Loggerホスト上で確立済みのマウントポイント)。

各ストレージグループのイベントは、個別にアーカイブされます。つまり、ストレージグループごとに、毎日1つのアーカイブファイルが作成されます。さらに、イベントを一括してアーカイブできます。つまり、1回のアーカイブ操作でイベントをアーカイブする日にちの範囲を指定できます。

各ストレージグループのイベントを個別のアーカイブ場所にアーカイブすることで、特定のストレージグループのデータを他のストレージグループのデータよりも長く保持することができます。次の図に示されているように、イベントをアーカイブする前に、アーカイブストレージの設定を行う際に、これらの場所を指定する必要があります。これは、Loggerアプライアンスの図です。**[マウントポイント]** フィールドは、ソフトウェアLoggerでは使用できません。

- Loggerアプライアンスでは、[アーカイブ パス] フィールドに指定したパスが [マウントポイント] で指定したパスに追加されます。
- ソフトウェアLoggerでは、アーカイブファイルが書き込まれる完全なパスを [アーカイブ パス] フィールドに入力する必要があります。このパスには、Loggerソフトウェアがインストールされているマシン上のローカルディレクトリまたは確立済みのマウントポイントを指定できます。[**マウントポイント**] フィールドは、ソフトウェアLoggerでは使用できません。

Loggerは、イベントの受信時刻を使用してそのアーカイブ日を決定します。たとえば、タイムスタンプが12月7日午後11時55分00秒のイベントが、12月8日午前12時01分00秒にLoggerで受信されたとします。このイベントは、12月7日ではなく、12月8日用に作成されたアーカイブファイルにアーカイブされます。アーカイブ処理が実行されるとき、ストレージグループごとに1つのアーカイブファイルが、**アーカイブストレージ設定**で指定した場所に作成されます。各アーカイブファイルには、特定の日の1つのストレージグループに対する、午前12時00分00秒から、午後11時59分59秒までのイベントが格納されます。日付の範囲を指定した場合、ストレージグループあたり1つのアーカイブファイルが、指定された日ごとに作成されます。

イベントをアーカイブする方法には、**手動**と**スケジュール**の2つの方法があります。イベントを手動でアーカイブする場合、イベントアーカイブの開始日および終了日と、アーカイブするストレージグループを指定します。この処理は、指定された日付範囲に対して1回だけ実行されます。イベントアーカイブをスケジュールする場合は、アーカイブ操作を毎日実行する時刻を指定し、対象に含めるストレージグループを選択します。

注: スケジュールされたアーカイブでは、イベントアーカイブを午前1時に開始するように設定することはできません。この制限は、夏時間 (DST: Daylight Savings Time) の切り替えに対応するための設計上の制限です。

Loggerがアーカイブを開始すると、[**Daily Task Settings**] ページ (スケジュールされたアーカイブの場合) または [**イベントアーカイブを追加**] ページ (手動アーカイブの場合) にリストされているさまざまなストレージグループが順番に処理されます。

イベントがアーカイブされても、イベント (および関連するインデックス付け情報) は、設定されている保有ポリシーによって期限切れになるまで、ローカルストレージからは削除されません。これらのイベントは、期限切れで削除されるまで検索操作に含まれます。

アーカイブされたイベントがLoggerのローカルストレージから削除されると、検索操作の対象に含まれなくなります。そのようなイベントを検索操作の対象とするには、それらのイベントが格納されているアーカイブをLoggerにロードする必要があります。イベントアーカイブがロードされると、そのイベントは検索の対象となりますが、アーカイブ自体はリモートストレージに保持されたままになります。

ソースタイプ情報 (イベントに関連付けられている場合) は、イベントのアーカイブ時に保存されます。ソースタイプの作成と使用については、「ソースタイプ」(388ページ) を参照してください。

インデックスステータスのアーカイブ

イベントをアーカイブする際、それらのイベントのインデックス情報はアーカイブされません。そのため、イベントアーカイブをロードしてもインデックスは使用できません。その結果、Loggerにロードされたアーカイブ済みイベントに対して実行される検索クエリは、データがアーカイブされていない場合よりも低速になります。これは、アーカイブデータのインデックスデータを利用できないためです。アーカイブのイベントにインデックスを付けることができます。この処理には、しばらく時間がかかることがあります。このインデックス付け処理が完了したら、インデックス付けアーカイブ内のイベントに対して、検索が通常の速度で実行されるようになります。

注意: アーカイブではインデックスの作成に長い時間がかかり、インデックスの作成中は検索が低速になる場合があります。必要なアーカイブにのみインデックスを作成してください。

イベントをアーカイブするためのガイドライン

- 設定バックアップとイベントアーカイブは定期的に実行して、リモートロケーションに保管するようにしてください。致命的な障害が発生した場合は、最新の設定バックアップとイベントアーカイブを復元する必要があります。設定バックアップについては、「設定のバックアップとリストア」(468ページ) を参照してください。
- 大量のイベント (数十ギガバイト) をアーカイブする必要がある場合は、ピーク時間外にアーカイブし、Loggerのパフォーマンスに影響を与えないようにすることをお勧めします。
- アーカイブのロード、アンロード、アーカイブ、削除などの複数のアーカイブ操作を同時に実行できます。そのため、アーカイブ処理の進行中でも既存のアーカイブのロードを開始できます。

ヒント: 一度に実行できる手動アーカイブジョブは1つのみです。ただし、スケジュールされたアーカイブ操作は手動ジョブと並行して実行できます。

- アーカイブ済みのイベントを再度アーカイブすることはできません。これを行おうとすると、Loggerでエラーが報告されます。
- アーカイブファイルをアーカイブ場所から移動しないでください。最初にアーカイブされた場所から移動されたアーカイブは、Loggerにロードできません。アーカイブを削除する必要がある場合は、Loggerのユーザーインターフェイスを使用してください。
- アーカイブジョブが失敗した場合は、手動でジョブを開始する必要があります。そのためには、失敗したアーカイブを削除し、手動でアーカイブします。失敗したアーカイブの通知を受け取るには、監査イベント [**Event Archive Failed**] のアラートを設定します。このイベントの詳細については、「Logger監査イベント」(610ページ)を参照してください。アラートの設定の詳細については、「保存された検索」(333ページ)を参照してください。
- アーカイブ操作の実行中にLoggerアプライアンスが停止した場合、操作が失敗したときにアーカイブされていなかったストレージグループについてのみ、アーカイブ操作を再度開始する必要があります。そのようなストレージグループには、[イベント アーカイブ] ページの [ステータス] 欄に「失敗」と表示されます。

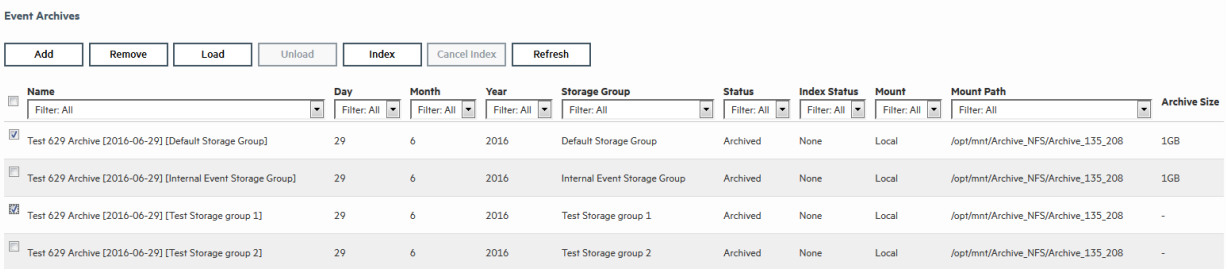
  たとえば、12/1/16のイベントデータをアーカイブし、このデータが「デフォルト」、「内部」、「Short-Term」、「Long-Term」の4つのストレージグループのイベントで構成されているとします。「デフォルト」および「内部」グループのイベントが正常にアーカイブされた後、「Short-Term」のイベントのアーカイブ中にアプライアンスが停止したとします。[イベント アーカイブ] ページ上の「Short-Term」ストレージグループのステータスは「失敗」と表示され、「デフォルト」および「内部」グループのステータスは「アーカイブ済み」と表示されます(「Long-Term」ストレージグループのステータスは表示されません)。この場合、「Short-Term」および「Long-Term」ストレージグループのアーカイブを手動で再度開始する必要があります。

  注: 上記の例で、「Long-Term」ストレージグループのステータスが障害発生後に [イベント アーカイブ] ページに表示されないのは、そのアーカイブ処理中にこのグループのアーカイブが開始されていなかったためです。

  アーカイブが失敗した場合は、アーカイブできなかったストレージグループを特定し、それらのグループすべてについて手動でアーカイブを再度開始してください。
- 手動で開始した進行中のアーカイブ操作は、[イベント アーカイブ] ページの上部に表示されている [**キャンセル**] リンクを使用して、いつでもキャンセルできます。

イベントのアーカイブ

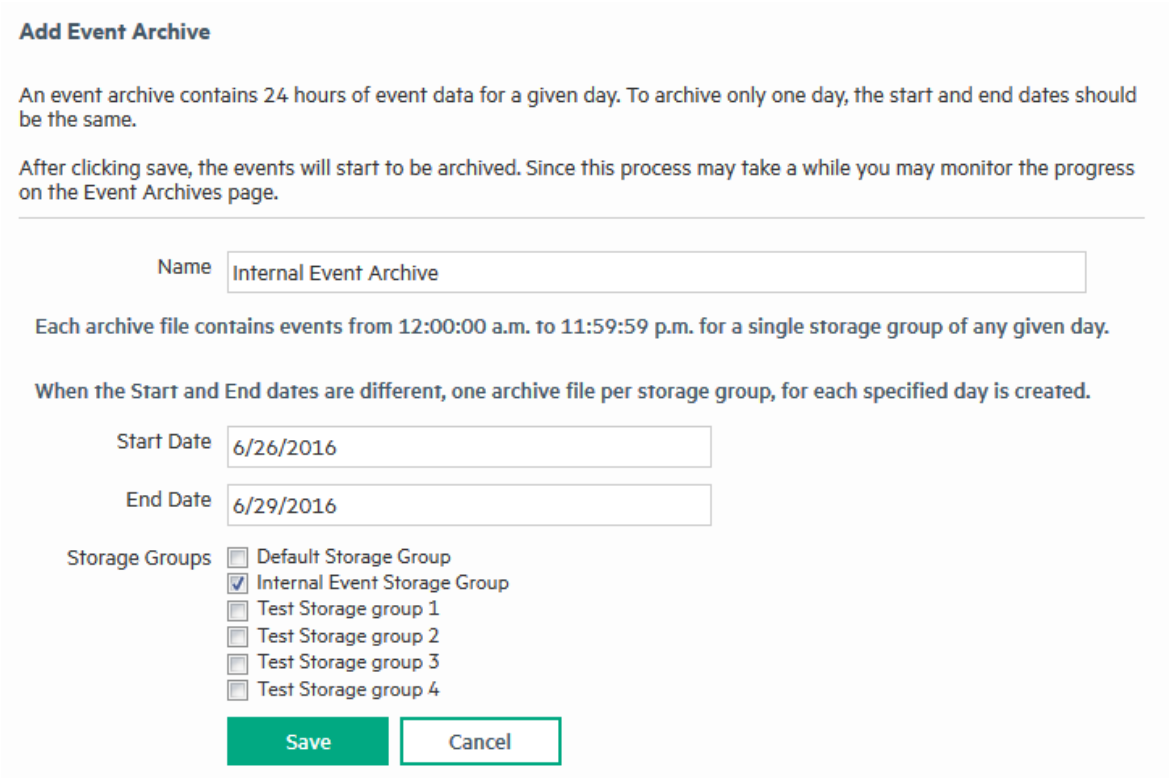
特定の日のイベントを保存するには、イベントアーカイブを追加する必要があります。[イベントアーカイブ (Event Archives)] ページの表は、現在のアーカイブとそのステータスを示しています。



アーカイブの保存場所をLoggerで確立してからそのイベントをアーカイブする必要があります。これは1回限りの設定です。アーカイブ保存場所を確立するには、「アーカイブ保存設定」(438ページ) を参照してください。

イベントアーカイブを追加するには

1. **[設定 | ストレージ]** メニューを開き、**[イベント アーカイブ]** をクリックします。
2. [イベント アーカイブ (Event Archives)] ページで **[追加 (Add)]** をクリックします。



3. 新しいイベントアーカイブの **[名前 (Name)]** フィールドに意味のある名前を入力し、**開始日**と**終了日**を`m/dd/yy`形式で指定します。ここで、`m`は月番号、`dd`は日 (必要に応じて先頭に0を追加)、`yy`は2桁の年番号です。

   開始日と終了日が異なる場合、ストレージグループあたり1つのアーカイブファイルが、指定された日ごとに作成されます。たとえば、次の開始日と終了日を指定したとします。

   開始日: 2015/08/12
   終了日: 2015/08/13

   > **注:** ある日のイベントをアーカイブ済みの場合、それらのイベントを再度アーカイブすることはできません。同じ日のイベントを2回アーカイブしようとすると、アーカイブ済みの曜日または日付を示すメッセージが表示されます。日にちの範囲をアーカイブする場合、その範囲内にすでにアーカイブされている日があると、アーカイブ済みの日を除いてアーカイブプロセスが行われ、アーカイブ済みの日付を示すメッセージが表示されます。

   両方のストレージグループ、つまり **[内部イベント ストレージ グループ (Internal Event Storage Group)]** と **[デフォルトのストレージ グループ (Default Storage Group)]** を設定する場合、このアーカイブオペレーションでは、指定した2日分のアーカイブファイルが各ストレージグループ分作成されます。つまり、4つのアーカイブファイルが作成されることになります。

   イベントアーカイブの表 ([イベント アーカイブ (Event Archives)] ページ) に、次の形式でエイリアスごとにアーカイブが一覧表示されます。<アーカイブ名> [<yyyy-m-dd>] [<ストレージグループ名>]。
4. アーカイブに含める必要があるストレージグループの名前を選択します。
5. **[保存 (Save)]** をクリックしてイベントのアーカイブを開始するか、**[キャンセル (Cancel)]** をクリックして終了します。

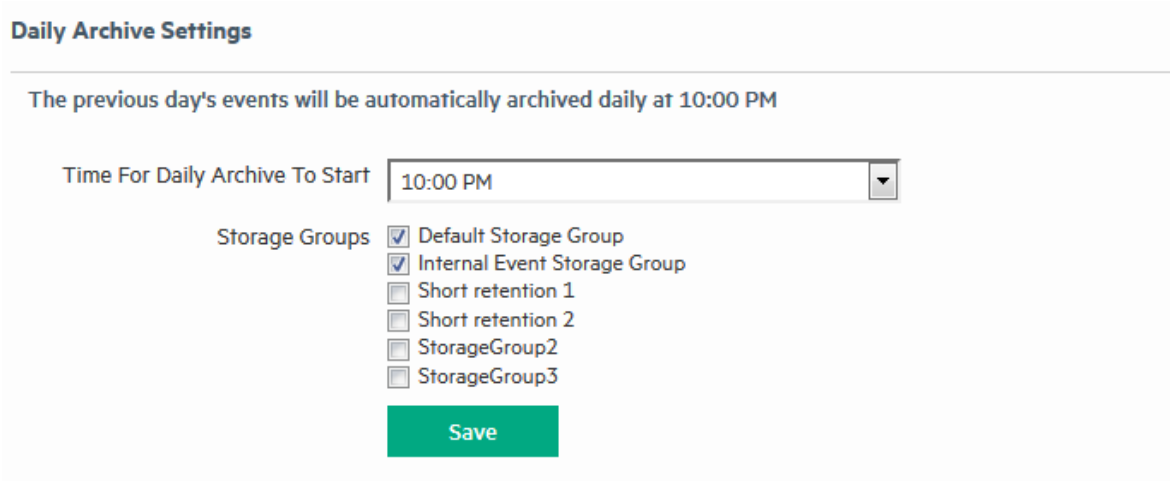
   > **注:** 処理中のアーカイブオペレーションは、[イベント アーカイブ (Event Archives)] ページの上部にある **[キャンセル (Cancel)]** リンクでいつでもキャンセルできます。

イベントアーカイブを削除するには

1. **[設定 | ストレージ]** メニューを開き、**[イベント アーカイブ]** をクリックします。
2. 一番左の列にあるチェックボックスをオンにし、削除するイベントアーカイブを選択します。
3. 画面上部の **[削除]** をクリックし、選択したアーカイブを削除します。
4. **[OK]** をクリックして削除を確定するか、**[キャンセル]** をクリックしてイベントアーカイブを保持します。

日次アーカイブの設定

日次イベントアーカイブをスケジュールし、それを実行する時刻を指定できます。実行が終了したスケジュールされたイベントアーカイブは、[イベント アーカイブ] ページのアーカイブリストに表示されます。一度に実行できるスケジュールされたイベントアーカイブは1つのみですが、手動でスケジュールされたアーカイブと同時に実行することはできます。



イベントアーカイブをスケジュールする前に、「時刻/NTP」(497ページ)に記載されている情報をよくお読みください。

日次イベントアーカイブをスケジュールするには

1. [**設定 | ストレージ**] メニューを開き、[**日次アーカイブの設定**]をクリックします。
2. [**日次アーカイブの開始時刻 (Time For Daily Archive to Start)**] リストから時刻を選択します。

   ヒント: スケジュールアーカイブは、正時に開始する必要があります。午前零時と午前1時00分はリストにありません。これは、Loggerが、前日のすべてのイベントを受信できるようにするためです。

3. スケジュールされたアーカイブに含めるイベントが属しているストレージグループを選択します。
4. [**保存 (Save)**] をクリックして日次イベントアーカイブをスケジュールするか、別のページをクリックしてキャンセルします。

アーカイブ保存設定

Loggerアプライアンスでは、イベントアーカイブは特定のNFSまたはCIFSのマントポイント、またはSANに保存されます。ソフトウェアLoggerの場合は、イベントアーカイブは指定したディレク

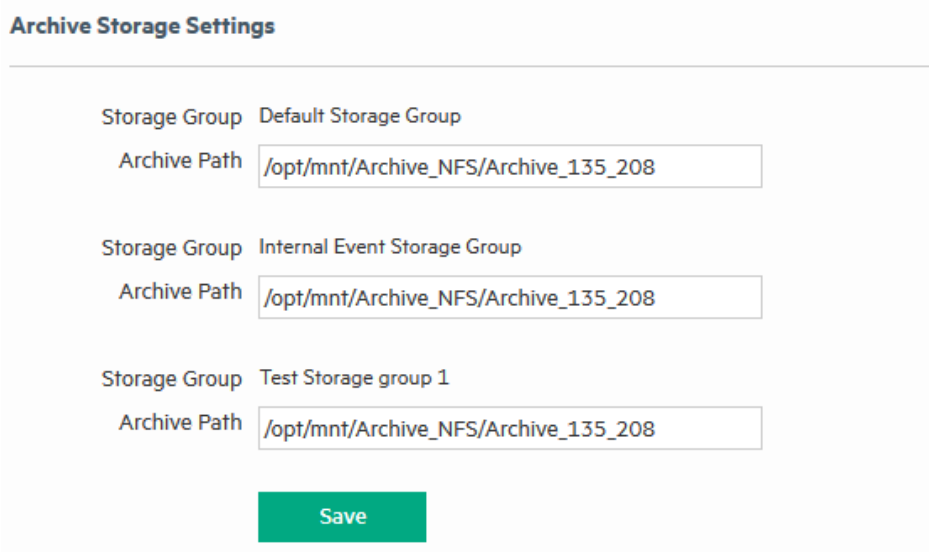
トリに保存されます。指定できるのは、ソフトウェアLoggerがインストールされているマシン上のローカルディレクトリまたはマウントポイントのパスです。マウントポイントを作成するには、使用しているシステムのオペレーティングシステムのマニュアルを参照してください。

アーカイブ保存設定を行うには

1. Loggerアプライアンスを使用している場合は、NFSまたはCIFSマウントポイントを作成します(「ストレージ」(509ページ) および「リモートファイルシステム」(509ページ) を参照)。

   ソフトウェアLoggerを使用しており、NFSまたはCIFSマウントポイントを使用する予定の場合は、外部の記憶場所が、Loggerがインストールされているマシンにマウントされていることを確認します。詳細については、使用しているシステムのオペレーティングシステムのマニュアルを参照してください。
2. **[設定 | ストレージ]** メニューを開き、**[アーカイブ ストレージの設定]** をクリックします。
3. 各ストレージグループのマウント場所とアーカイブパスを指定します。ストレージグループごとに異なるパスを指定できるため、Loggerは、ストレージグループごとに異なる場所にイベントをアーカイブできます。
   - Loggerアプライアンスの場合は、[**マウントポイント**] フィールドで、NFSマウント、CIFSマウント、またはSANマウントポイントの名前を選択します。このドロップダウンリストには、NFS、CIFS、またはSANマウントポイントを作成したときに指定した名前が含まれています (**[システム管理] > [ストレージ] > [リモート ファイル システム]**)。
     たとえば、選択したマウントポイントがパス`/opt/ARCHIVES`を指し、その場所のアーカイブディレクトリが`archivedir`の場合、[**アーカイブ パス**] フィールドには`archivedir`と指定します。
   - ソフトウェアLoggerの場合、[**マウントポイント**] フィールドは存在しません。アーカイブファイルが書き込まれる完全なパスを [**アーカイブ パス**] フィールドに入力する必要があります。このパスには、Loggerソフトウェアがインストールされているマシン上のローカルディレクトリまたは作成済みのマウントポイントを指定できます。
     たとえば、`/opt/ARCHIVES/archivedir`と指定します。

注: すべてのストレージグループをアーカイブする意図がない場合でも、[アーカイブ ストレージの設定] ページのすべてのストレージグループを設定する必要があります。



4. [**保存 (Save)**] をクリックします。

アーカイブのロードとアンロード

アーカイブされたイベントを検索操作に含めるには、その前にそれらのイベントをLoggerにロードする必要があります。イベントアーカイブがロードされると、そのイベントは検索の対象となりますが、アーカイブ自体はリモートストレージに保持されたままになります。アンロードされたイベントアーカイブはロードできますが、そのイベントは検索の対象にはなりません。ロードされたアーカイブを検索操作に含める必要がなくなった場合は、そのアーカイブをアンロードできます。

アーカイブインデックスは、アーカイブと一緒にロードおよびアンロードされます。詳細については、「アーカイブされたイベントのインデックス付け」(441ページ)を参照してください。

注: アーカイブが作成されているとしても、現在のストレージに存在しているデータのアーカイブをロードすることはできません。つまり、そのデータの保持期限がまだ過ぎておらず、現在のストレージからエージアウトされていない場合は、アーカイブのロードが失敗します。

イベントアーカイブをロードまたはアンロードするには

1. [**設定 | ストレージ**] メニューを開き、[**イベント アーカイブ**] をクリックします。
2. 一番左の列にあるチェックボックスをオンにし、ロードまたはアンロードするイベントアーカイブを選択します。
3. 画面上部の [**ロード**] または [**アンロード**] をクリックし、選択したアーカイブをロードまたはアンロードします。

注: ロードされているアーカイブのインデックスを作成すると、そのアーカイブはインデックスの作成後に自動的にリロードされます。

アーカイブされたイベントのインデックス付け

イベントをアーカイブするときにインデックスデータは保存されませんが、既存のアーカイブのインデックスを作成できます。作成されたインデックスは、現在のアーカイブと同じルートの新しく作成されたサブディレクトリ(名前に「Index」接尾部が付いている)に格納されます。

ロードされたアーカイブにインデックスが付いていない場合、そのアーカイブ内のイベントを検索すると、現在のストレージに存在しているイベントの検索よりも時間がかかります。インデックスを作成すると、アーカイブされたデータの検索時にパフォーマンスが向上します。アーカイブのインデックスを作成すると、そのアーカイブ内のイベントの検索は、ローカルストレージ内の検索と同じくらい速くなります。

既にロードされているアーカイブのインデックスを作成すると、そのアーカイブはインデックスの作成後に自動的にリロードされます。

ヒント: tmpディレクトリとアーカイブディレクトリは、両方とも書き込み可能でなければならず、インデックスを作成するための十分なスペースが存在する必要があります。

イベントアーカイブのインデックスを作成するには

1. [**設定** | **ストレージ**] メニューを開き、[**イベント アーカイブ**] をクリックします。
2. 一番左の列にあるチェックボックスをオンにし、インデックスを作成するイベントアーカイブを選択します。

   注意: アーカイブではインデックスの作成に長い時間がかかり、インデックスの作成中は検索が低速になる場合があります。必要なアーカイブにのみインデックスを作成してください。

3. 画面上部の [**インデックス**] をクリックし、選択したアーカイブのインデックスを作成します。

   ヒント: インデックスの作成が進行している間は作成をキャンセルすることはできませんが、保留キュー内のアーカイブのインデックス作成はキャンセルできます。インデックスの作成をキャンセルするには、一番左の列にあるチェックボックスをクリックして、インデックスの作成ステータスが [**保留**] のイベントアーカイブを選択します。次に [**インデックスのキャンセル**] をクリックします。

   注: インデックスの作成が失敗した場合は、ログを調べて失敗の原因を特定してください。問題を解決してから、インデックスの作成を再試行してください。

スケジュールされたタスク

スケジュールされたタスクは、自動的に実行されるようにプログラムされたジョブです。ジョブタイプには、設定バックアップ、ファイル転送、イベントアーカイブ、保存された検索があります。[**設定 | スケジュールされたタスク**] カテゴリのオプションを使用すると、スケジュールされたタスクを管理できます。

スケジュールされたタスクに影響を与える可能性がある、「時刻/NTP」(497ページ) に記載されている内容をよくお読みください。

スケジュールされたタスク

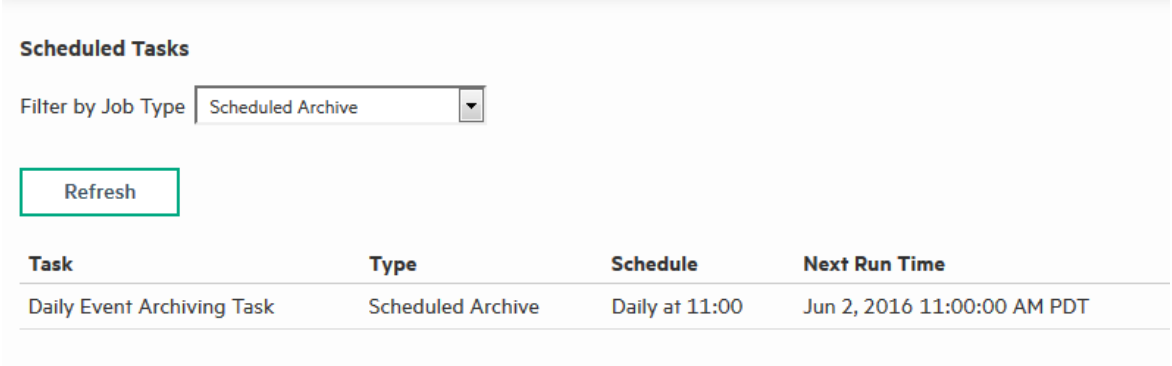
スケジュールされたタスクは、以下のアクティビティに対して作成できます。

- 保存された検索 (「スケジュールされた検索/アラート」(335ページ) を参照)
- ファイル受信者とファイル転送受信者 (「受信者」(368ページ) を参照)
- イベントアーカイブ (「イベントのアーカイブ」(436ページ) を参照)
- 設定バックアップ (「設定のバックアップとリストア」(468ページ) を参照)
- ルックアップファイルの更新 (「ルックアップファイル」(357ページ) を参照)

[スケジュールされたタスク (Scheduled Tasks)] ページには、スケジュールされたジョブの一覧が表示されます。一部のタスクは、この画面から管理できます。使用可能な管理オプション (編集、有効にする、無効にする、削除など) は、列の右端に表示されます。

ページ上部のドロップダウンリストでは、すべてのスケジュールされたタスク (**すべて**) か、特定の種類のタスクのみを表示できます。

[スケジュールされたタスク (Scheduled Tasks)] ページ



スケジュールされたタスクを表示するには

1. [スケジュールされたタスク] の下にある [設定] メニューから [**スケジュールされたタスク**] をクリックします。
2. ドロップダウンリストから特定のタイプのスケジュールされたタスクを選択してリストをフィルター処理するか、[**すべて**] を選択します。
3. タスクの一覧を更新するには、[**更新 (Refresh)**] をクリックします。

スケジュールされたタスクを削除するには

1. [スケジュールされたタスク] の下にある [設定] メニューから [**スケジュールされたタスク**] をクリックします。
2. 削除するスケジュールされたタスクを探し、その行の [削除] アイコン (✖) をクリックします。
3. [**OK**] をクリックして削除を確定するか、[**キャンセル**] をクリックしてスケジュールされたタスクを保持します。

現在実行中のタスク

[現在実行中のタスク] ページには、現在実行中のスケジュールされたタスクが表示されます。表には、タスク名、種類、タスクを開始した日時が表示されます。

前提条件

この機能にアクセスするには、ユーザーが以下のユーザーグループに割り当てられている必要があります。

- デフォルトLogger検索グループ
- デフォルトシステム管理グループ

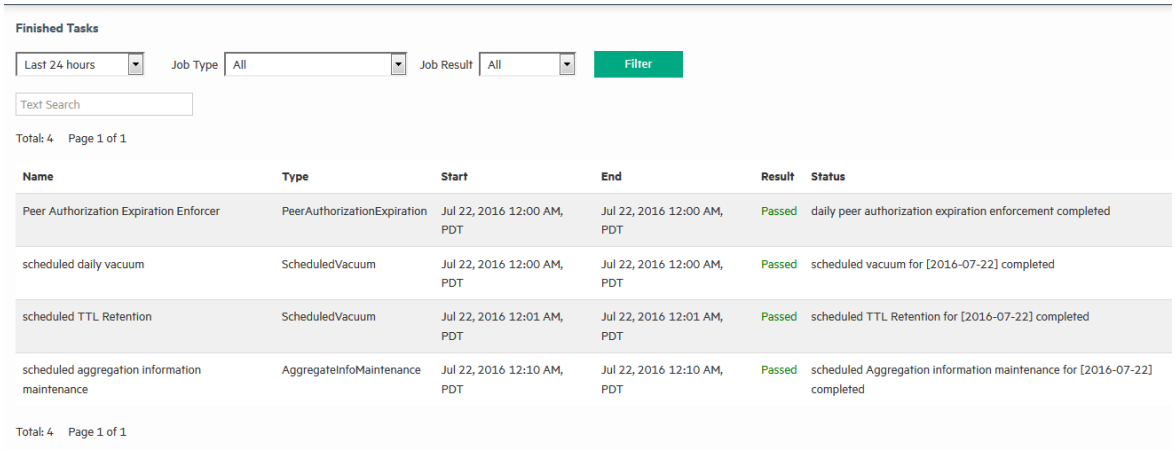
詳細については、「Loggerのユーザー権限の設定」(546ページ) を参照してください。

現在実行中のタスクを表示するには

1. [スケジュールされたタスク] の下にある [設定] メニューから [**現在実行中のタスク**] をクリックします。
2. タスクの一覧を更新するには、[**更新**] をクリックします。
3. ドロップダウンリストから特定のタイプのスケジュールされたタスクを選択してリストをフィルター処理するか、[**すべて**] を選択します。

完了したタスク

[完了したタスク] ページには、実行が完了したスケジュールされたタスクが表示されます。[完了したタスク (Finished Tasks)] ページは、すべてのスケジュールされたタスク実行の記録としての役割を果たし、最後に終了したタスクが一番上に表示されます。



完了したタスクを表示するには

[スケジュールされたタスク] の下にある [設定] メニューから [**完了したタスク**] をクリックします。

タスクリストのフィルタリング

タスクリストは、時間または期間、ジョブタイプ、あるいはテキスト検索によってフィルター処理できます。デフォルトで、タスクリストには、過去24時間の完了したタスクがページあたり20エントリ表示されます。

ヒント: [**フィルタ**] をクリックすると、いつでも [完了したタスク] リストを更新できます。

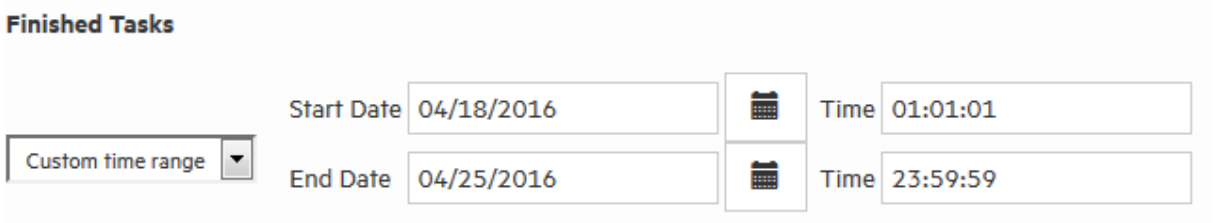
完了したタスクの時間によるフィルタリング

1. 最初のフィルターメニューから、以下のいずれかのオプションを選択するか、デフォルトを使用します。
   - **過去 24 時間** (デフォルト) — 過去24時間の完了したタスクを返します。
   - **過去 7 日間** — 過去7日間の完了したタスクを返します。
   - **30日** — 過去30日間の完了したタスクを返します。
   - **カスタム時間範囲** — 指定した日付および時間範囲の完了したタスクを返します。「特定の日時による完了したタスクのフィルタリング」(445ページ) を参照してください。

2. オプションで、[**フィルタ**] をクリックすると、結果を表示したり、フィルタリング基準をさらに追加したりすることができます。

特定の日時による完了したタスクのフィルタリング

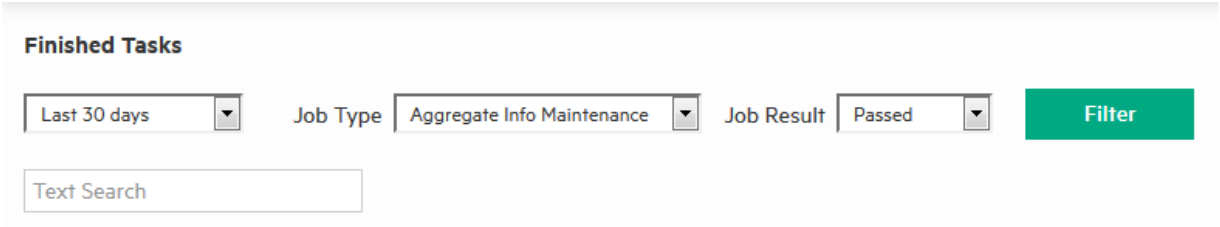
[カスタム時間範囲] を選択すると、[日付] フィールドと [時間] フィールドが表示されます。



1. [**開始日**] フィールドに日付を入力します。日付を`mm/dd/yyyy`形式で入力するか、カレンダーアイコン(📅)をクリックして日付を選択できます。[**終了日**] フィールドでも同じようにします。
2. オプションで、[**時間**] メニューから開始時間と終了時間を入力できます。時間を`hh:mm:ss`形式で入力するか、デフォルトの開始時間`00:00:00`と終了時間`23:59:59`を受け入れることができます。
3. オプションで、[**フィルタ**] をクリックすると、結果を表示したり、フィルタリング基準をさらに追加したりすることができます。

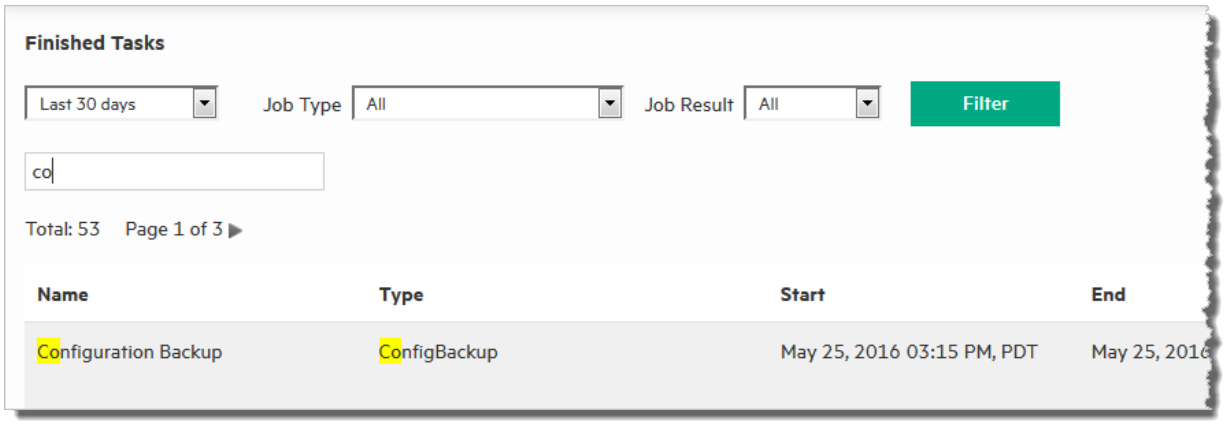
ジョブタイプまたはタスク結果による完了したタスクのフィルタリング

オプションで、ジョブタイプとジョブ結果のリストから値を選択すると、検索条件をさらに絞り込むことができます。[**フィルタ**] をクリックすると、結果を表示したり、フィルタリング基準をさらに追加したりすることができます。



テキスト検索による完了したタスクのフィルタリング

オプションで、[テキスト検索] フィールドに単語や語句のテキストを入力すると、そのテキストを含むタスクのリストが返されます。文字列を入力すると、その文字列に一致するテキストが強調表示されます。[**フィルタ**] をクリックして、結果を表示します。



詳細設定

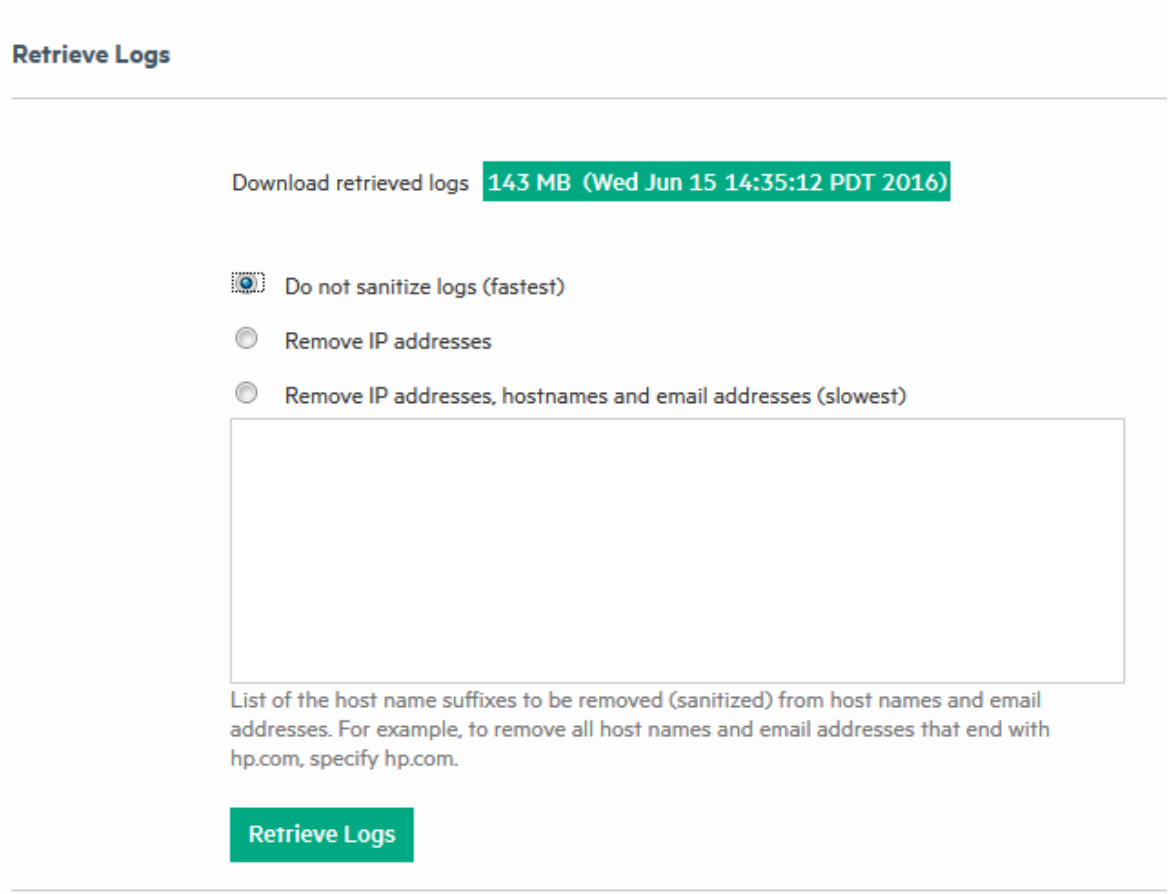
[設定 | 詳細] カテゴリのオプションを使用すると、詳細なタスクを管理できます。これらのタスクのほとんどで管理者権限が必要です。

ログの取得

Loggerでは、発生した問題の詳細など、いくつかの監査およびデバッグ情報を記録します。これらのシステムログ (イベントログと混同しないでください) は、旅客機の「フライトレコーダー」のようなものです。何か問題が発生した場合はログが役立ちます。カスタマーサポートから、インシデント調査の一環としてログを取得するよう求められる場合があります。その場合は、以下の手順に従って、得られた.zipファイルをカスタマーサポートに提出してください。

ログを取得する際、IPアドレス、ホスト名、メールアドレスの情報をわからなくすることで、ログファイルをサニタイズできます。ただし、サニタイズを行うと、ログの取得に余分な時間がかかります。サニタイズされた各IPアドレス、ホスト名、メールアドレスは、記号 `xxx.xxx.xxx.xxx` (IPアドレス)、`sanitized@email` (メール)、および`sanitized.host.name` (ホスト名) で置き換えられます。

[ログの取得 (Retrieve Logs)] ページ



Loggerのシステムログを取得するには

1. **[設定 | 詳細]** メニューを開き、**[ログの取得]** をクリックします。
2. ログファイルを作成するときに使用するログ取得オプションを選択します。
   - **[ログを削除しない (最速)]** を選択すると、すべてのIPアドレス、ホスト名、メールアドレスがログファイル内に保持されます。
   - **[IP アドレスを削除する]** を選択すると、ログの中のすべてのIPアドレスがわからなくなります。個別のIPアドレスを指定することはできません。
   - **[IP アドレス、ホスト名、およびメール アドレスを削除する (最遅)]** を選択する場合は、ホスト名とメールアドレスのサフィックスをテキストボックスで指定する必要があります。

     複数のサフィックスは、カンマ、スペースまたは改行で区切ります。たとえば、hp.comおよびgmail.comで終わるすべてのホスト名とメールアドレスをわからなくする場合は、次のように指定します。

     ```
     hp.com, gmail.com
     ```

指定されたサフィックスを持つすべてのIPアドレス、ホスト名、およびメールアドレスがわからなくなります。name@hp.comのように個別のメールアドレスを指定することはできません。個別のメールアドレスとそのサフィックスは無視されます。

3. [ログの取得] をクリックします。ログの取得中は、ページに進行状況バーが表示されます。
4. 収集が完了すると、システムログファイルが単一のzipファイルに圧縮されます。このファイルへのリンクが [ログの取得] ページに表示されます。ファイルをダウンロードするには、このリンクをクリックします。

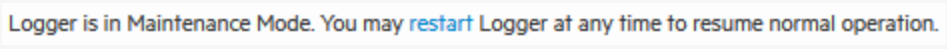
メンテナンス操作

データベースの最適化、ストレージボリュームサイズの拡大、ストレージグループの追加、スキーマフィールドの追加など、Logger上の特定の操作では、Loggerをメンテナンス状態にする必要があります。これは、Logger上のデータに関連した操作が実行されていない状態です。メンテナンスモードでは、Loggerをそのような状態にすることができます。Loggerがメンテナンスモードの場合、以下のようになります。

- イベントは処理されません。
- レポートは生成されません。
- 検索を実行できません。
- スケジュールされたジョブが実行されません。

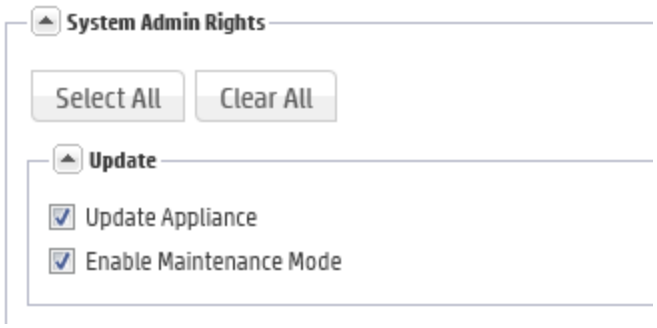
ヒント: Loggerを直接メンテナンスモードにすることはできません。Loggerをメンテナンスモードに移行できるのは、メンテナンスモードになっていることが必要な操作を実行する場合だけです。

注意: メンテナンスモードになっているLoggerを、コマンド行から再起動/リブートしないでください。[メンテナンス] ページの再起動リンクを使用してください。

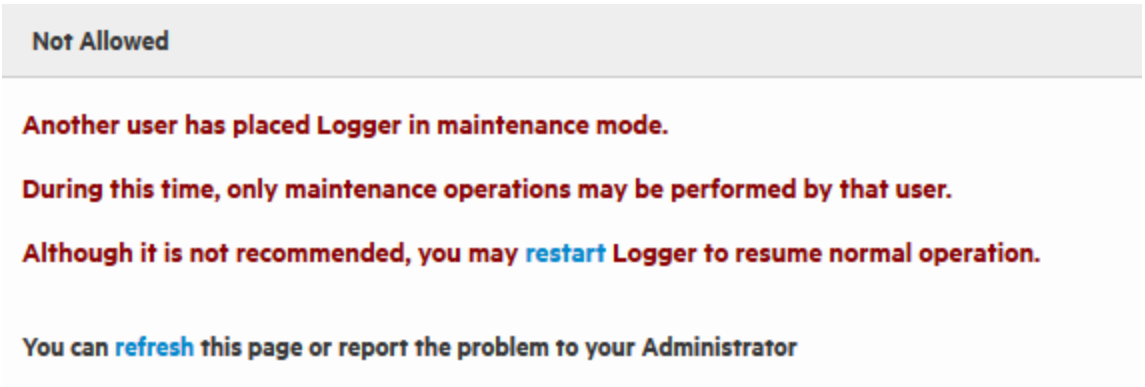


メンテンナンスモードで必要な権限

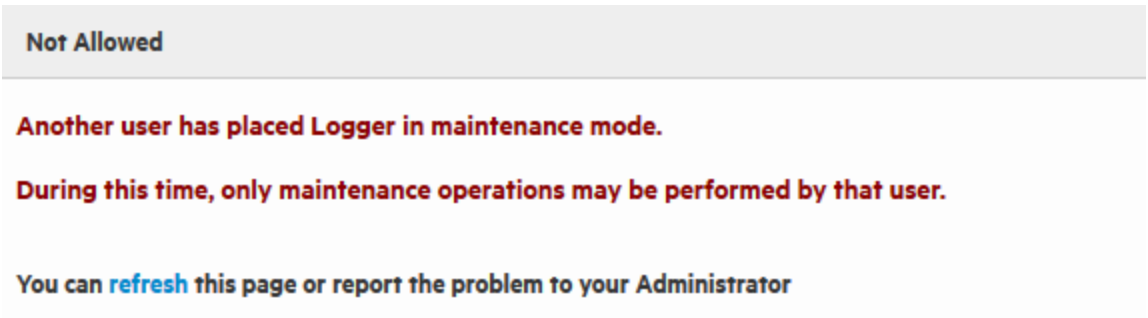
Loggerがメンテナンスモードになっている必要がある操作を実行するユーザーは、「メンテナンスモードを有効にする」権限がオンになっている必要があります (**[システム管理] > [ユーザ管理] > [グループ] タブ > [システム管理グループ]**)。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。



Loggerがメンテナンスモードになっている場合、「メンテナンスモードを有効にする」権限を持つユーザーに次のUIメッセージが表示されます。



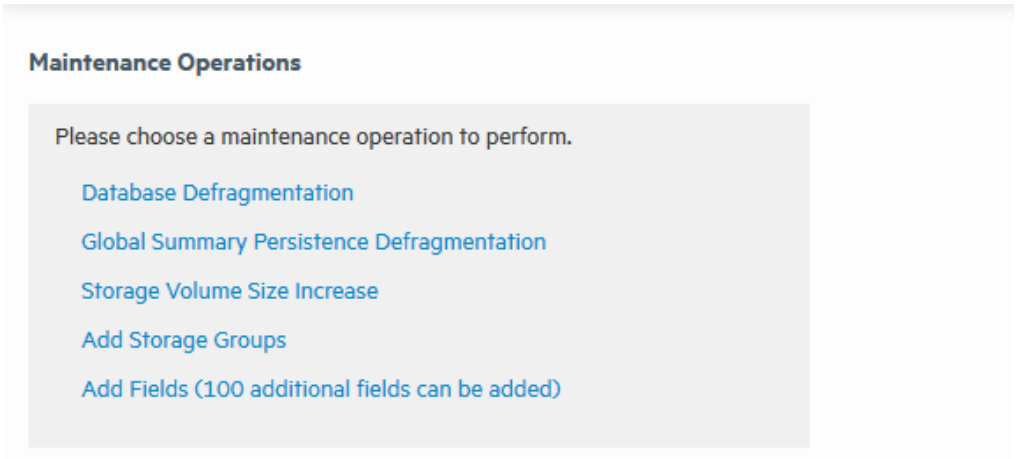
その他すべてのユーザーには、ログイン画面に次のメッセージが表示されます。



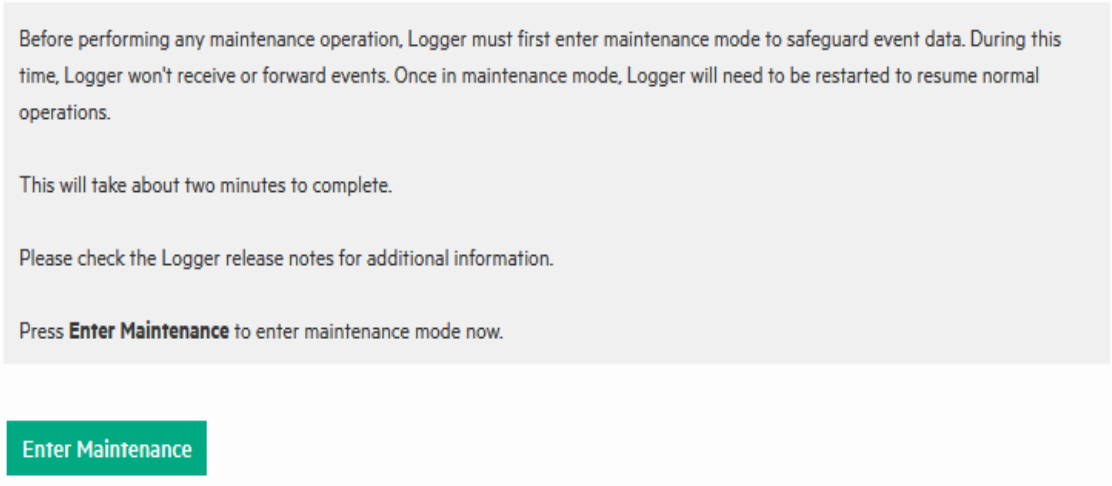
メンテナンスモードへの移行と終了

メンテナンスモードに移行するには

1. [**設定 | 詳細**] メニューから、[**メンテナンス操作**] をクリックします。[メンテナンス操作] パネルに使用可能なオプションが表示されます。



2. [メンテナンス操作] パネルのオプションをクリックします。このオプションのための確認ウィンドウが表示されます。

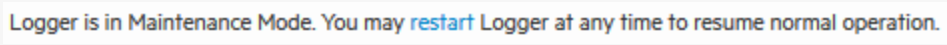


3. [**メンテナンスに移行**] をクリックして、選択したメンテナンス操作のための次の手順を実行します。
   - 「Loggerデータベースの最適化」(451ページ)
   - 「グローバルサマリーパーシステンスの最適化」(455ページ)
   - 「ストレージボリュームサイズの増加」(457ページ)
   - 「ストレージグループの追加」(459ページ)
   - 「スキーマへのフィールドの追加」(461ページ)

メンテナンスモードを終了するには

1. メンテナンス モードのページのリンクを使用して、Loggerアプライアンスをリブートするか、ソフトウェアLoggerを再起動します。

注意: メンテナンスモードになっているLoggerを、コマンド行から再起動/リブートしないでください。[メンテナンス] ページの再起動リンクを使用してください。



Loggerデータベースの最適化

Loggerのデータベースは、時間とともにフラグメント化される可能性があります。保有タスクを頻繁に実行すると、この問題が深刻になる場合があります。データベースの最適化が必要となる場合は、Loggerで以下の症状が現れます。

- 検索とレポート生成の速度低下
  たとえば、過去2分間のデータに対する検索操作でさえも低速になります。
- 受信者と転送者の操作の一時停止時間が長くなる

このような症状が見られる場合は、Loggerを最適化することができます。最適化処理を開始する前に、必ず以下のガイドラインをお読みください。

データベース最適化のためのガイドライン

Loggerの症状が、ネットワークレイテンシなどのネットワークインフラストラクチャーが関係する問題や、Logger上の予期しない負荷によるものでないことを確認します。

最適化を開始する前に、Loggerシステムをメンテナンスモードにする必要があります。その結果、Logger上のほとんどの処理が停止します。イベントは処理されず、スケジュールされたジョブは実行されず、ほとんどのユーザーインターフェイスの操作は使用できなくなります。メンテナンスモードの詳細については、「メンテナンス操作」(448ページ) を参照してください。

データベースの最適化を実行するには、システム上に最低限の量の空きディスク領域が必要です。ユーティリティにより、必要な空き領域が自動的にチェックされ、十分なディスク領域がないとメッセージが表示されます。

ヒント: 必要に応じて最適化を実行できますが、このユーティリティの使用頻度が高すぎる場合は (過去数日以内に最適化を実行したシステムなど)、カスタマーサポートに連絡して助言を求めてください。

最適化処理がいずれかの時点で失敗すると、Loggerは、最適化を開始する前と同じ状態に戻ります。

Loggerアプライアンスを再起動して、安全に最初から処理を再開することができます。ソフトウェアLoggerの場合は、「プロセスステータス」(502ページ) の説明に従ってLoggerプロセスを再起動します。

必要な権限

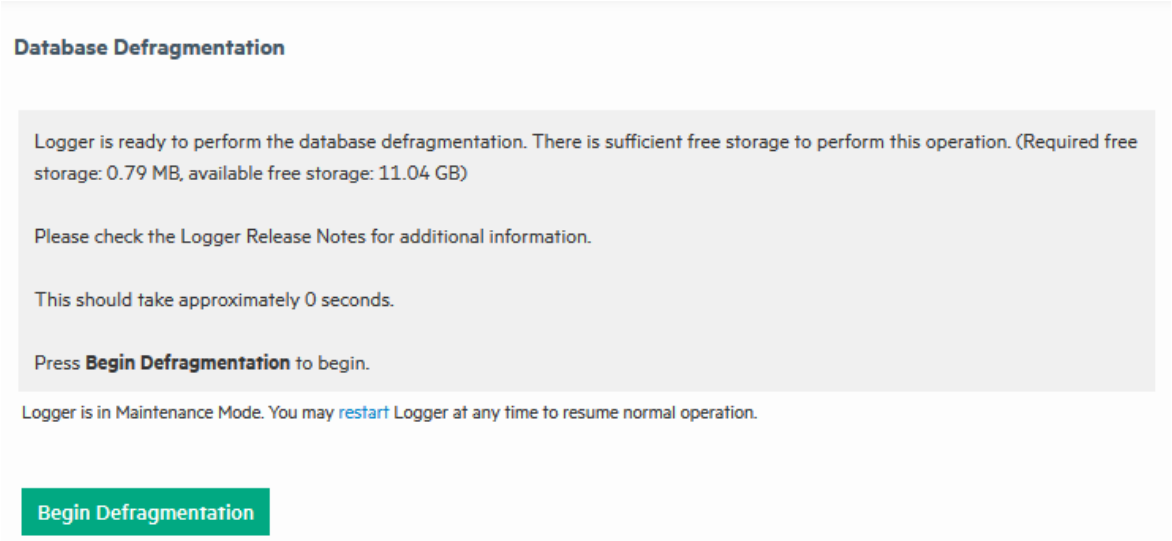
この処理を実行できるのは、割り当てられているシステム管理グループの [**システム管理権限**] リストで [**メンテナンス モードを有効にする**] 特権を [**はい**] に設定している場合だけです。これを設定するには、**[システム管理] > [ユーザー管理] > [グループ] タブ > [グループの管理]** ページに移動し、[システム管理グループ] を選択して [**追加**] または [**編集**] をクリックします。

Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

Loggerの最適化

Loggerを最適化するには

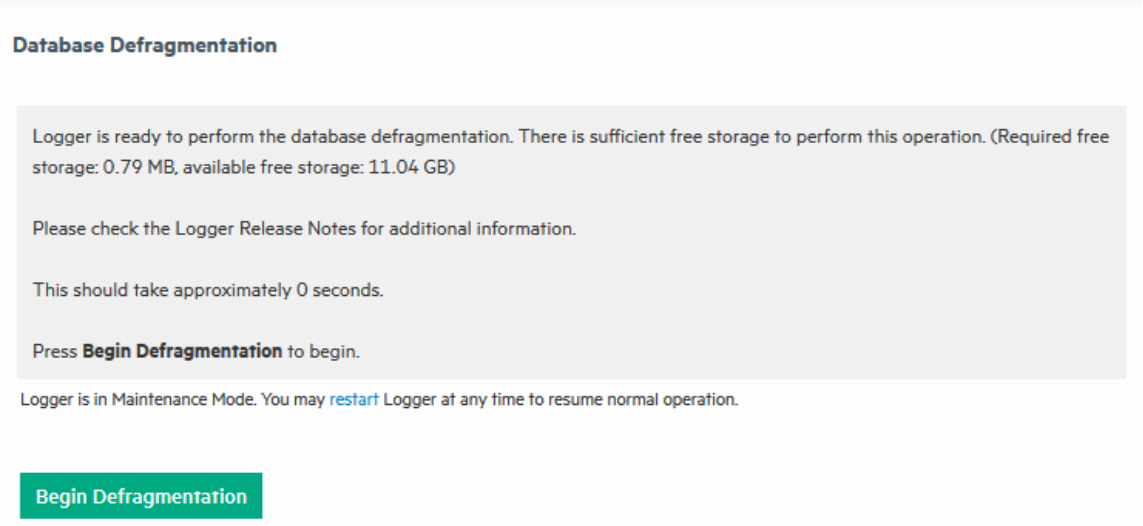
1. [**設定 | 詳細**] メニューを開き、[**メンテナンス操作**] をクリックします。
   [メンテナンス操作] パネル (「メンテナンス操作」(448ページ)) に使用可能なオプションが表示されています。
2. [**データベースの最適化**] をクリックします。
3. [**メンテナンスに移行**] をクリックして、Loggerがメンテナンスモードに移行できるようにします。
   データベースの最適化処理を実行するには、最低限の量の空き領域が必要です。そのため、Loggerは、メンテナンスモードに移行するときにチェックを実行して空き領域を確認します。



4. [**最適化を開始 (Begin Defragmentation)**] をクリックします。
   - 必要な領域がない場合は、「最適化ストレージスペースの解放」(454ページ) の指示に従ってください。
   - 必要な量の空き領域があり、Loggerが正常にメンテナンスモードに移行すると、次の

画面が表示されます。

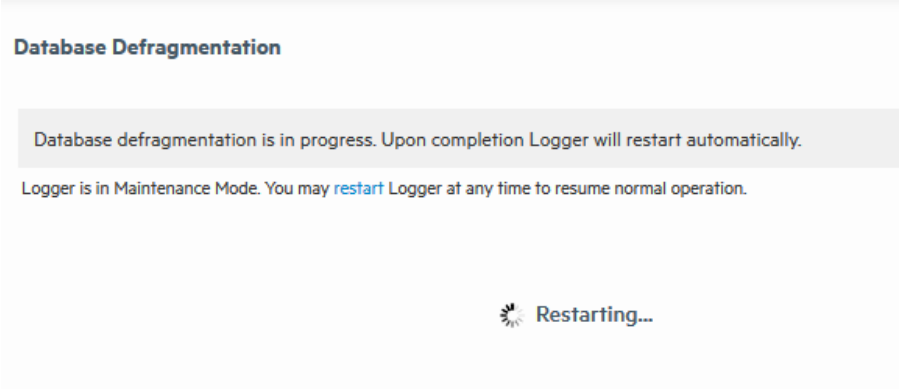
データベースの最適化の開始



注: ソフトウェアLoggerでは、以降の[データベースの最適化]画面で、Loggerがメンテナンスモードになっているときに通常動作を再開するには、[**再起動**]をクリックするように指示されます。[再起動]をクリックすると、Loggerサービスとその関連プロセスのみが、ソフトウェアLoggerがインストールされているマシン上で開始されます。

5. 最適化処理が開始されます。次に示すように、進行状況インジケーターに最適化のステータスが表示されます。最適化が完了するまでは、Logger上であらゆる操作を行わないことをお勧めします。

   最適化が完了すると、Loggerが自動的に再起動します。これによりメンテナンスモードが終了します。



最適化ストレージスペースの解放

必要な領域がない場合は、十分な領域を解放するよう、Loggerによって求められます。

以下のオプションのいずれかを選択できます。

- **手動で削除**

  注: [手動で削除] オプションは、L7x00 Loggerでは使用できません。

  Logger上で、削除しても安全なファイルをリストしたテキストファイルが自動的に作成されます。ソフトウェアLoggerアプライアンスでは、このファイルの保管場所は次のとおりです。
  `/opt/arcsight/logger/user/logger/defragmentation/filelist.txt`
  ソフトウェアLoggerでは、このファイルの保管場所は次のとおりです。<インストールディレクトリ>`/current/arcsight/logger/user/logger/defragmentation/filelist.txt`
  テキストファイル中で、各ファイルは、サイズの降順に列挙されます。十分な数のファイルを削除して領域を空けることができます。ただし、カスタマーサポートに連絡して説明を受けるまでは、ファイルを削除**しないでください**。

  以下の手順に従って続行します。

  a. 何もせずにメッセージ画面を終了します。
  b. カスタマーサポートに連絡して、テキストファイルに列挙されているファイルの削除についての説明を確認します。
  c. 十分な数のファイルを削除した後、メッセージ画面から、データベースの最適化処理を再開します。再開するには、[**再チェック**] をクリックして、最適化を続行するのに十分な領域が利用できるようになったかどうかを確認します。

     十分な領域がある場合は、「データベースの最適化の開始」(453ページ) が表示されます。[**最適化を開始**] をクリックして続行します。

     まだ十分な領域がない場合は、メッセージが表示されます。表示されるオプションから選択して、追加の領域を作成します。

     注: 十分な領域を作成せずに最適化処理を終了する必要がある場合は、[**リブート**] をクリックします。

- **データベースインデックスの削除**

  Loggerは、十分な数のデータベースインデックスを自動的に削除します。まず最も大きなインデックスが削除され、必要な量の領域が開放されます。データベースインデックスの削除後に十分な領域が利用可能になった場合、最適化処理が自動的に進みます。

  しかし、データベースインデックスを削除した後でも十分な領域が利用できない場合は、以下の手順に従って続行してください。

a. [**手動で削除**] をクリックします。

注: [手動で削除] オプションは、L7x00 Loggerでは使用できません。

Logger上で、削除しても安全なファイルの一覧が記載されたテキストファイルが作成されます。テキストファイル中で、各ファイルは、サイズの降順に列挙されます。

b. [**リブート**] をクリックします。

Loggerがメンテナンスモードを終了します。

c. カスタマーサポートに連絡し、ファイルの手動削除について指示を受けます。

十分な数のファイルを削除して領域を空けることができます。

d. ファイルを削除した後は、「Loggerを最適化するには」(452ページ) の説明に従って、最適化処理を再起動します。

注: 任意の時点で最適化処理が失敗するか中断した場合、Loggerはそれらのインデックスを復元する必要があります。復元処理は自動的に行われますが、完了するまでに少なくとも数時間かかる可能性があります。この処理の間にデータが失われることはありません。

- **リブート**

  データベース最適化処理が中断され、Loggerが最適化ユーティリティを開始する前の状態に戻ります。

グローバルサマリーパーシステンスの最適化

グローバルサマリーパーシステンス機能に既知の問題があります。この機能は、Loggerの [グローバルサマリー] セクションで報告された統計をリブート中に保持するために設計されたものです。一部の環境では、この機能によりディスク領域が影響を受ける可能性があります。

本リリースでは、グローバルサマリーパーシステンスは無効化されています。ほとんどの場合、アクションは不要です。ただし、Logger 5.3からアップグレードしたばかりの場合は、できるだけ早くグローバルサマリーテーブルを最適化する必要があります。最適化処理を開始する前に、必ず以下のガイドラインをお読みください。

グローバルサマリーパーシステンスの最適化のためのガイドライン

- グローバルサマリーパーシステンス最適化を開始する前に、Loggerシステムをメンテナンスモードにする必要があります。その結果、Logger上のほとんどの処理が停止します。イベントは処理されず、スケジュールされたジョブは実行されず、ほとんどのユーザーインターフェイスの操作は使用できなくなります。メンテナンスモードの詳細については、「メンテナンス操作」(448ページ) を参照してください。
- グローバルサマリーパーシステンスの最適化を実行するには、システム上に最低限の量の空きディスク領域が必要です。ユーティリティにより、必要な空き領域が自動的にチェックされ、十分なディスク領域が見つからないとメッセージが表示されます。

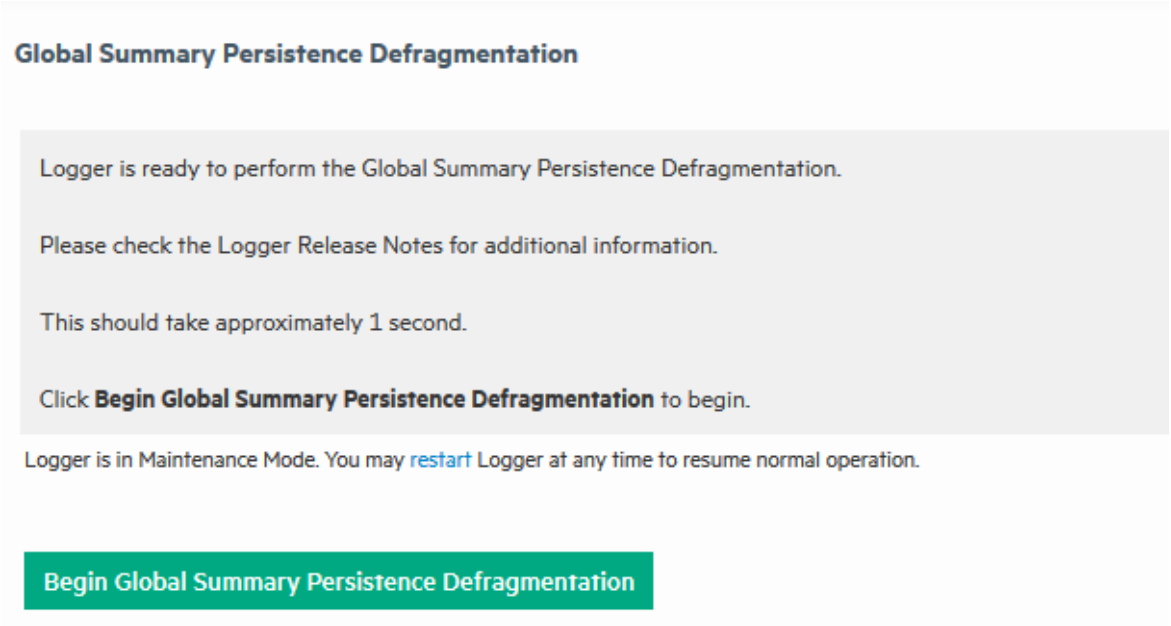
- 最適化処理がいずれかの時点で失敗すると、Loggerは、最適化を開始する前と同じ状態に戻ります。安全にアプライアンスを再起動したり、ソフトウェアLoggerプロセスを再起動したりすることができます。
  a. 「システムの再起動」(492ページ) に従ってLoggerアプライアンスを再起動します。
  b. ソフトウェアLoggerの場合は、「プロセスステータス」(502ページ) に従ってLoggerプロセスを再起動します。

必要な権限

この処理は、「メンテナンスモードを有効にする」権限が「はい」になっている場合のみ実行できます ([**システム管理**] > [**ユーザ/グループ**] > [**グループの管理**] > [**システム管理グループ**])。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

グローバルサマリーパーシステンスの問題を最適化するには

1. [**設定 | 詳細**] メニューを開き、[**メンテナンス操作**] をクリックします。
   [メンテナンス操作] パネル(「メンテナンス操作」(448ページ))に使用可能なオプションが表示されています。
2. [**グローバルサマリパーシステンスの最適化**] をクリックします。
3. [**メンテナンスに移行**] をクリックして、Loggerがメンテナンスモードを開始できるようにします。



4. [**グローバルサマリパーシステンスの最適化の開始**] をクリックして最適化処理を開始します。
5. 最適化処理が開始されます。進行状況インジケーターに、最適化のステータスが表示されます。最適化が完了するまでは、Logger上であらゆる操作を行わないことをお勧め

します。

最適化が完了すると、Loggerが再起動します。これによりメンテナンスモードが自動的に終了します。

注: ソフトウェアLoggerでは、Loggerサービスとその関連プロセスのみが再起動されます。

ストレージボリュームサイズの増加

初期設定時に設定したストレージボリュームサイズはいつでも拡張できます。一度拡張したボリュームサイズは縮小できません。Loggerインターフェイスに、現在の値と、サイズを拡張できる最大値が表示されます。

注: 「ストレージ ボリューム サイズの増加」操作がシステムメンテナンス操作の下にオプションとして表示されるには (**[設定 | 詳細] > [メンテナンス操作]**)、システム管理グループ (「メンテナンス モードを有効にする」権限が有効) とLogger権限グループに属している必要があります。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

SAN Logger上のストレージボリュームサイズの拡大について

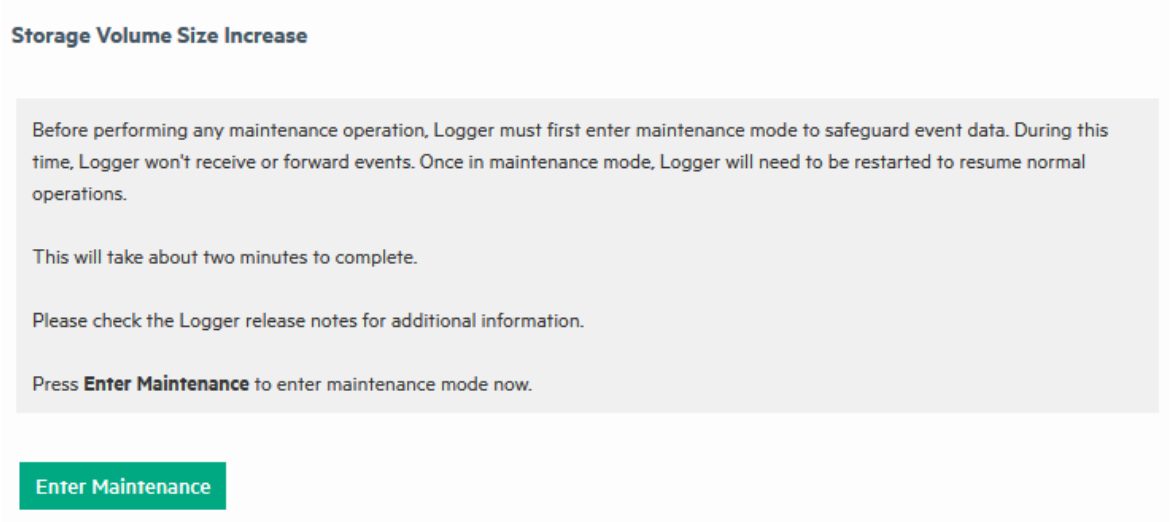
Loggerは、サイズ変更されたLUNを検出できません。そのため、Loggerにマウントした後でLUNのサイズを変更すると、新しいサイズはLoggerによって認識されません。その結果、ストレージボリュームのサイズは、Loggerに最初にマウントしたときのLUNサイズまでしか拡張できません。

LUNの初期サイズは、マウントする前に可能な限り大きくしておく必要があります。次の例は、SAN Loggerのストレージボリュームサイズの拡張を示しています。

初期 LUNサイズ	LUNの サイズ変更	現在のストレージ ボリュームサイズ	ストレージボリュームサイズの 拡張が可能か
4TB	なし	1TB	はい。最大4TB
4TB	なし	4TB	なし
8TB	なし	4TB	はい。最大8TB
2TB	8TB	1TB	はい。最大2TB
4TB	8TB	1TB	はい。最大4TB
8TB	8TB	4TB	はい。最大8TB

ストレージボリュームのサイズを拡張するには

1. ナビゲーションバーから、[**設定 | メンテナンス操作**] を選択します。
   [メンテナンス操作] ページに使用可能なオプションが表示されます。「メンテナンス操作」(448ページ) を参照してください。
2. [**ストレージ ボリューム サイズの増加**] をクリックします。
3. [**メンテナンスに移行**] をクリックして、Loggerがメンテナンスモードを開始できるようにします。

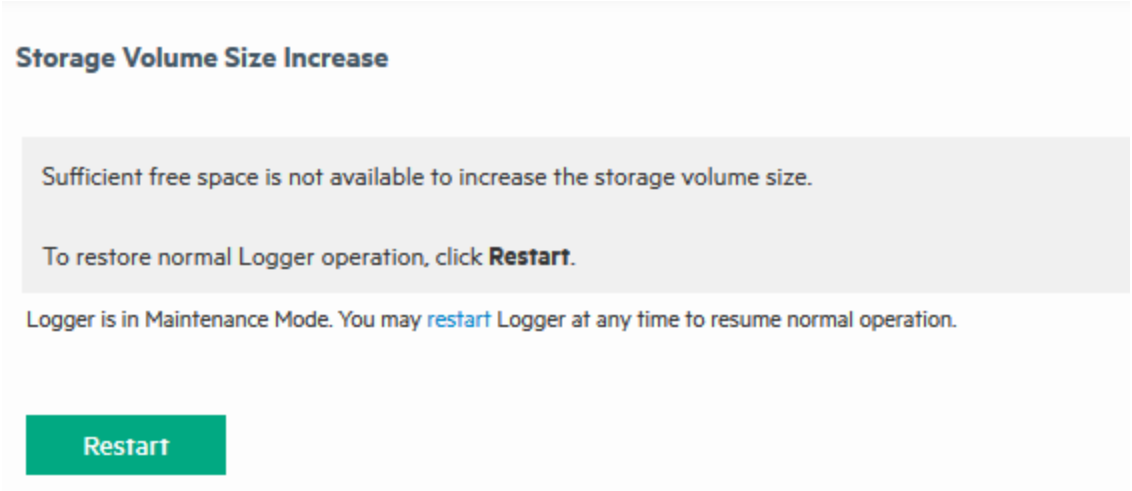


4. メンテナンスモードでは、ストレージボリュームサイズを拡張できるか、また、どれだけ拡張できるかを判断するためのチェックがLoggerで実行されます。ストレージボリュームが拡張可能な場合は、新しいサイズを入力して [**OK**] をクリックします。

   注: ソフトウェアLoggerでは、以降の [ストレージ ボリューム サイズの増加] 画面で、Loggerがメンテナンスモードになっているときに通常動作を再開するには、[**再起動**] をクリックするよう指示されます。[再起動] をクリックすると、Loggerサービスとその関連プロセスのみが再起動されます。

   ストレージボリュームを拡張するために十分な領域がない場合、以下のメッセージが表示されます。[**再起動**] をクリックしてLoggerを再起動し、メンテナンスモードを終了しま

す。



ストレージグループの追加

Logger上にデフォルトで存在する2つのストレージグループに加えて、最大4つのストレージグループを追加できます。以下の条件が満たされていれば、いつでもストレージグループを追加できます。

- 許可される最大数である6個のストレージグループがLogger上にすでに存在していないこと。
- ストレージボリュームに、追加するストレージグループに割り当てることができる余分のストレージ領域があること。

  ヒント: ストレージボリュームに、別のストレージグループを追加するための十分な領域がなく、既存のグループに空き領域がある場合は、既存のストレージグループのサイズを縮小し、追加するストレージグループのための領域を空けることを検討してください。または、「ストレージボリュームサイズの増加」(457ページ)に従って既存のストレージボリュームのサイズを拡大してください。

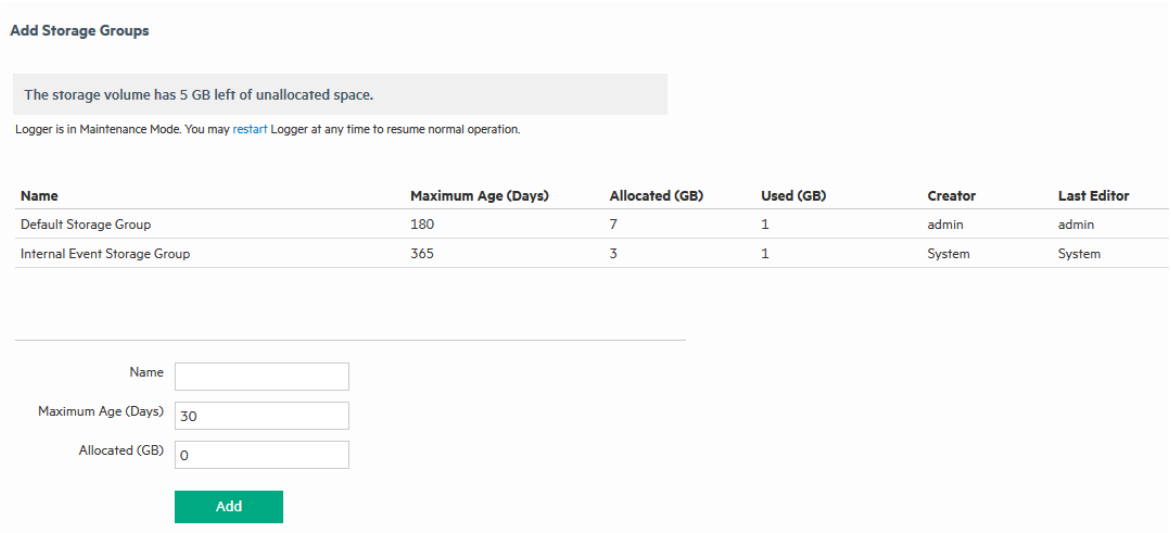
ストレージグループを追加する際、Loggerはメンテナンスモードになっている必要があります。ストレージグループを追加するとき、Loggerは、指定されたストレージグループのサイズが必要な最小サイズ (5 GB) よりも大きく、ストレージボリューム上の空き領域よりも小さいことを自動的に確認します。

ストレージグループを追加し、Loggerをリブートしてメンテナンスモードを終了した後には、グループにイベントアーカイブが作成されるように、追加したグループを [アーカイブ ストレージの設定] で必ず設定してください。

ストレージグループを追加するには

1. [**設定 | 詳細**] メニューを開き、[**メンテナンス操作**] をクリックします。
   [メンテナンス操作] パネル (「メンテナンス操作」(448ページ) を参照) に

   使用可能なオプションが表示されます。
2. [**ストレージ グループを追加**] をクリックします。
   最大6個のストレージグループがLogger上に存在できます。そのため、Logger上にデフォルトで存在する2個に加えて、4個までストレージグループを追加できます。
   Logger上に存在するストレージグループの数が許容される最大数**ではない**場合、画面が表示され、次のステップで説明するように、メンテナンスモードを開始します。
   6個すべてのストレージグループがLogger上に存在するか、ストレージボリューム上にグループを追加するための十分な領域がない場合、画面にメッセージが表示され、Loggerをメンテナンスモードにすることはできません。
3. [**メンテナンスに移行**] をクリックして、Loggerがメンテナンスモードを開始できるようにします。
   メンテナンスモードの詳細については、「メンテナンス操作」(448ページ) を参照してください。
4. Loggerがメンテナンスモードになると、次の [ストレージ グループを追加] ページが表示されます。



   この画面には、既存のストレージグループと、ストレージボリュームに残っている領域の量に関する情報も表示されます。
5. 以下の情報を入力します。

パラメーター	説明
名前 (Name)	ストレージグループの名前を選択します。
最大期間 (日) (Maximum Age (Days))	イベントを保持する日数を指定します。この日数よりも古いイベントは削除されます。
最大サイズ (GB) (Maximum Size (GB))	最大イベントデータサイズをギガバイト単位で入力します。

6. **[追加 (Add)]** をクリックします。
   ストレージグループがLoggerに追加されます。Logger上のストレージグループの数が、許容される最大数である6個に達していない場合は、**[追加 (Add)]** をクリックしてストレージグループを追加できます。最大数に達している場合が、[追加 (Add)] ボタンが表示されません。他のストレージグループを追加しない場合は、次のステップに進みます。
7. 変更を適用し、メンテナンスモードを終了するために、Loggerアプライアンスをリブートするか、ソフトウェアLoggerを再起動します。

スキーマへのフィールドの追加

Loggerのスキーマには、定義済みのフィールドが複数含まれています。フィールドベースのクエリには、これらのフィールドのみを含めることができます。また、高速な検索処理のために、これらのフィールドのみにインデックスを作成できます。デフォルトのLoggerスキーマフィールドを表示する方法については、「デフォルトのフィールド」(354ページ)を参照してください。

Logger 5.2よりも前のバージョンでは、ログ分析で現在Loggerスキーマにないフィールドの検索が必要な場合、自分でスキーマにフィールドを追加する方法はありませんでした。Logger 5.2より、Loggerスキーマにフィールドを追加できるようになりました。つまり、Loggerスキーマに、Logger上で収集するイベントに適したフィールドを挿入できるため、これらのフィールドを使用して検索およびレポート作成を行うことが可能です。また、追加するフィールドのインデックスを作成して、これらのフィールドを使用する検索およびレポートクエリを高速化できます。たとえば、金融機関であれば、クレジットカード番号や社会保障番号をスキーマに追加することが考えられます。

Loggerに追加できるカスタムスキーマフィールドは100個までです。また、ピアLoggerからカスタムフィールドをインポートすることもできます。ただし、追加およびインポートされるフィールドの総数が、最大数である100個を超えることはできません。

Logger上でインデックスを作成できるフィールドは123個までです。そのため、インデックスを作成できるカスタムスキーマフィールドの数は、Logger上で現在インデックスが作成されているデフォルトフィールドの数によって変わります。

カスタムフィールドを含むイベントをLoggerで処理するためには、イベントがCEF形式 (キーと値のペア) になっている必要があります。そのため、追加データを生成するSmartConnectorを使用するか、ArcSight FlexConnectorを定義して、イベントソースからのカスタムフィールドを含むイベントを収集および解析し、CEF形式に変換して、Loggerに転送する必要があります。

Loggerは、コネクタービルド5.0.0.5560以降を使用して作成されたFlexConnectorからのイベントのみを処理できます。FlexConnectorの設計の詳細については、『ArcSight FlexConnector Developer's Guide』を参照してください。

注: Loggerは、FlexConnectorからCEFバージョン0で受信した追加のフィールドデータを処理できず、そのようなフィールドがCEFバージョン0のイベントに存在する場合、値がNULLであると見なします。その結果、それらのフィールドを検索したり、インデックスを作成したりすることはできません。ただし、これらのフィールドは、フィールドセットで「*」を選択すればUIに表示されます。なぜなら、インターフェイスには、rawイベントに含まれている情報が表示されるためです。そのため、Loggerが「ad.callnumber=5678」を受信した場合、Logger UIには、列ad.callnumberが値5678で表示されます。ただし、「5678」を検索しても、検索結果ではこのイベントが返されません。

カスタムスキーマフィールドを追加またはインポートするには、メンテナンスモードになっていることが必要です。スキーマフィールドの追加やインポートの処理では、追加またはインポート操作の後で保存操作が必要です。追加またはインポート操作では、指定したフィールドが追加されますが、Loggerスキーマには書き込まれません。追加またはインポートしたフィールドは、この時点で編集または削除できます。これらのフィールドを保存すると、フィールドがスキーマに書き込まれます。これ以降、これらのフィールドは編集または削除できません。そのため、保存前に、スキーマに追加しようとしているフィールドを慎重に見直してください。

注: 「フィールドの追加」操作がシステムメンテナンス操作の下にオプションとして表示されるには (**[設定 | 詳細] > [メンテナンス操作]**)、システム管理グループ (「メンテナンスモードを有効にする」権限が有効) とLogger権限グループに属している必要があります。Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ)を参照してください。

カスタムスキーマフィールドを追加するには、以下の情報を指定する必要があります。

- **表示名** — フィールドの意味のある名前。この名前は、フィールドの列見出し名として表示され、検索クエリで指定する名前になります。たとえば、SocialSecurityNumberと指定します。
- **タイプ** — このフィールドに格納されるデータの型。選択肢はDouble、BigInt、DateTime、Textです。

  それぞれのデータ型について次の表で説明します。

型	説明
Double	10進数または小数を格納するために使用します。 範囲は －1.79769313486231570E＋308～－4.94065645841246544E－324 (負の値)と 4.94065645841246544E－324～1.79769313486231570E＋308 (正の値)です。
BigInt	整数を格納するために使用します。 範囲は －2^63～2^63－1、つまり －9,223,372,036,854,775,808～9,223,372,036,854,775,807です。
DateTime	日付と時刻の両方または日付のみを格納するために使用します。
Text	任意の文字を格納するために使用します。1つのフィールドに最大で255文字を格納できます。

- **長さ** — このフィールドは、[タイプ] に [**Text**] を指定した場合にのみ適用されます。このフィールドは、データ型がTextの場合にフィールドの値に設定できる最大文字数を指定します。このフィールドは、[タイプ] に [**Text**] を指定した場合にのみ適用されます。このフィールドは、データ型がTextの場合にフィールドの値に設定できる最大文字数を指定します。
- **フィールド名** — Loggerスキーマに追加するフィールド名です。一般には、**表示**名の省略名です。たとえばSSNと指定します。

ピアからのスキーマフィールドのインポート

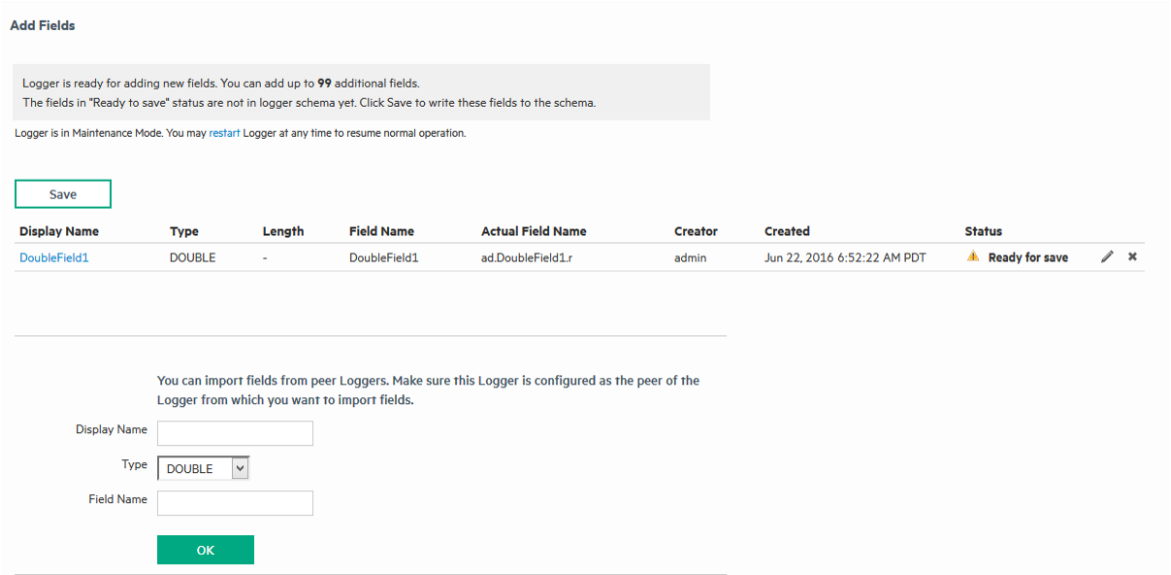
Loggerが別のLoggerのピアになっている場合は、ピアのスキーマに追加されたカスタムフィールドをインポートできます。フィールドのインポート元となるピアは、ユーザーインターフェイス画面で指定します。フィールドは、以下の条件が満たされている場合にインポートできます。

- 同じ表示名とフィールド名を持つフィールドが、スキーマフィールドのインポート先のLoggerに存在していないこと。競合するフィールドが存在してもインポートされますが、ユーザーインターフェイス画面で競合が通知されます。競合を解決するまでは、インポートしたフィールドをスキーマに保存できません。
- インポート先のLoggerで、カスタムフィールドが最大数である100個に達していないこと。インポートできる数よりも多くのフィールドがある場合、最大数に達するまで、最初のN個のみがインポートされます。

検索クエリに含まれているカスタムスキーマフィールドは、クエリが実行されるすべてのピアに存在している必要があります。そうなっていない場合、クエリは実行されず、エラーが返されます。

カスタムスキーマフィールドを追加またはインポートするには

1. [**設定 | 詳細**] メニューを開き、[**メンテナンス操作**] をクリックします。
   [メンテナンス操作] パネル(「メンテナンス操作」(448ページ))に使用可能なオプションが表示されています。
2. [**フィールドの追加 (フィールドをあと100個追加できます)**] をクリックします。
   最大で100個のカスタムフィールドをLoggerスキーマに追加できます。[フィールドの追加 (Add Fields)] リンクの数字は、追加できるカスタムフィールドの数を反映しています。この数値は、フィールドをLoggerスキーマに追加すると減っていきます。
3. [**メンテナンスに移行**] をクリックして、Loggerがメンテナンスモードを開始できるようにします。
4. Loggerがメンテナンスモードになると、[フィールドの追加 (Add Fields)] ページが表示されます。



フィールドは、手動で追加するか、ピアLoggerからインポートできます。

手動でフィールドを追加するには

1. メンテナンスモードを開始した後、[**新規フィールドを追加**] をクリックします (選択されていない場合)。
2. [**ディスプレイの名前 (Display Name)**] フィールドに意味のある名前を入力します。
   表示名は、検索クエリで指定する名前であり、検索結果でフィールドの列見出し名として表示されます。たとえば、SocialSecurityNumberと指定します。これは、Loggerスキーマに追加されません。
   表示名を指定する際には、以下のガイドラインに従ってください。
   - 表示名は一意でなければなりません。つまり、同じ表示名の別のフィールド (カスタムフィールドまたはLoggerスキーマフィールド) がLoggerにすでに存在していてはなりませ

ん。

- ASCII文字のみを使用できます。つまり、中国語や日本語のネイティブな文字をこのフィールドで使用することはできません。
- 表示名の長さは最大で100文字であり、英数字とアンダースコア文字を使用できます。

  注: 有効な表示名であるためには、先頭に「arc_」またはアンダースコアが含まれていてはなりません。

3. [**タイプ (Type)**] プルダウンメニューから、フィールドのデータ型を選択します。選択可能なオプションは、[Double]、[BigInt]、[DateTime]、[Text] です。詳細については、「スキーマへのフィールドの追加」(461ページ) を参照してください。
4. [**長さ (Length)**] フィールドに、データ型がTextの場合にフィールドの値に設定できる最大文字数を入力しますこのフィールドは、[長さ (Length)] に [テキスト (Text)] を指定した場合のみ使用できます。このフィールドには、1～255文字を指定できます。
5. [**フィールド名 (Field name)**] フィールドに名前を入力します。

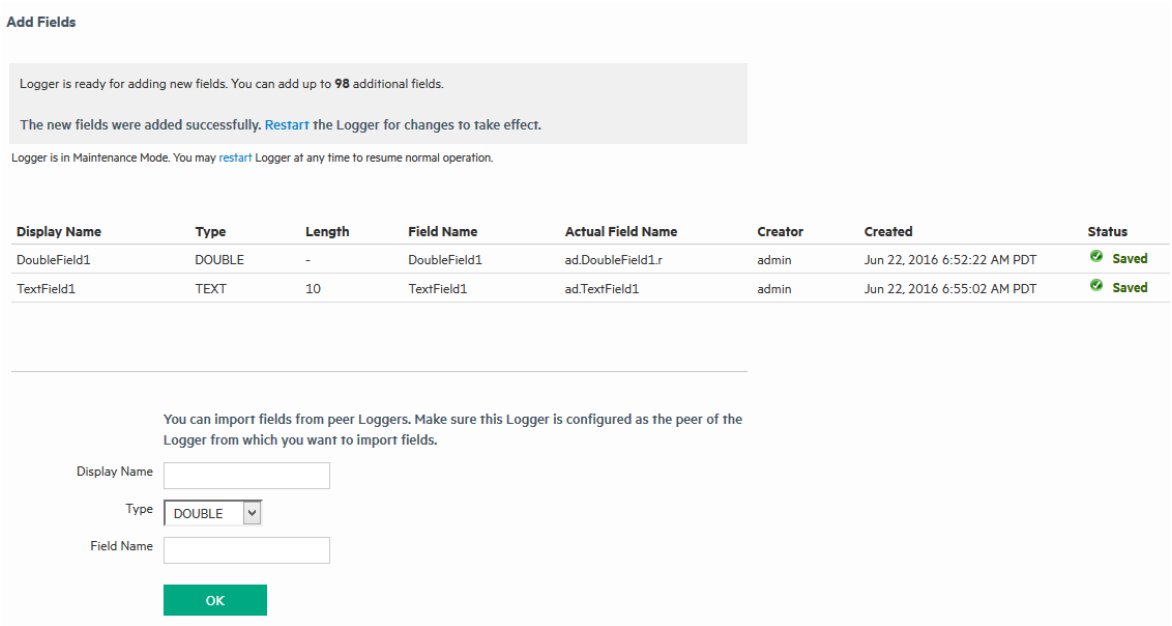
   この名前は、Loggerスキーマに追加される名前です。一般には、表示名の省略名です。たとえばSSNと指定します。

   フィールド名を指定する際には、以下のガイドラインに従ってください。

   - このフィールドは必須フィールドです。
   - フィールド名は一意でなければなりません。つまり、同じフィールド名のカスタムフィールドがLoggerにすでに存在していてはなりません。
   - ASCII文字のみを使用できます。つまり、中国語や日本語のネイティブな文字をこのフィールドで使用することはできません。
   - フィールド名の長さは最大で40文字であり、英数字、ハイフン、アンダースコア文字を使用できます。アンダースコアは、実際のフィールド名のエスケープ文字として使用されます。したがって、フィールド名にアンダースコアを含めると、実際のフィールド名にはアンダースコアが2つ(__)含まれることになります。

   このフィールドに名前を入力すると、プレフィックスとサフィックスが自動的に追加され、得られた名前が [実際のフィールド名] フィールドに表示されます (下図参照)。このフィールドには、入力したフィールド名がLoggerでどのように保存されたかが表示されます。プレフィックスは「ad」です。
6. [**OK**] をクリックします。

   追加したフィールドは、[フィールドの追加] フォームの上部に表示されます(下図参照)。このフィールドはまだ保存されていないため([保存の準備完了] ステータス)、編集または削除できます。[保存] をクリックすると、フィールドがスキーマに追加され、変更や削除ができなくなります。



7. 上記のステップを繰り返して、他のフィールドを追加します。
8. 追加したフィールドを確認し、必要に応じて編集( )または削除( )を行います。

   注意: 次のステップでは、追加したフィールドをLoggerのスキーマにコミットします。この処理は元に戻すことができません。つまり、いったんLoggerのスキーマに書き込んだフィールドは、編集または削除できなくなります。保存せずにこの処理を終了すると、追加途中のフィールドは記憶されず、変更内容が失われます。

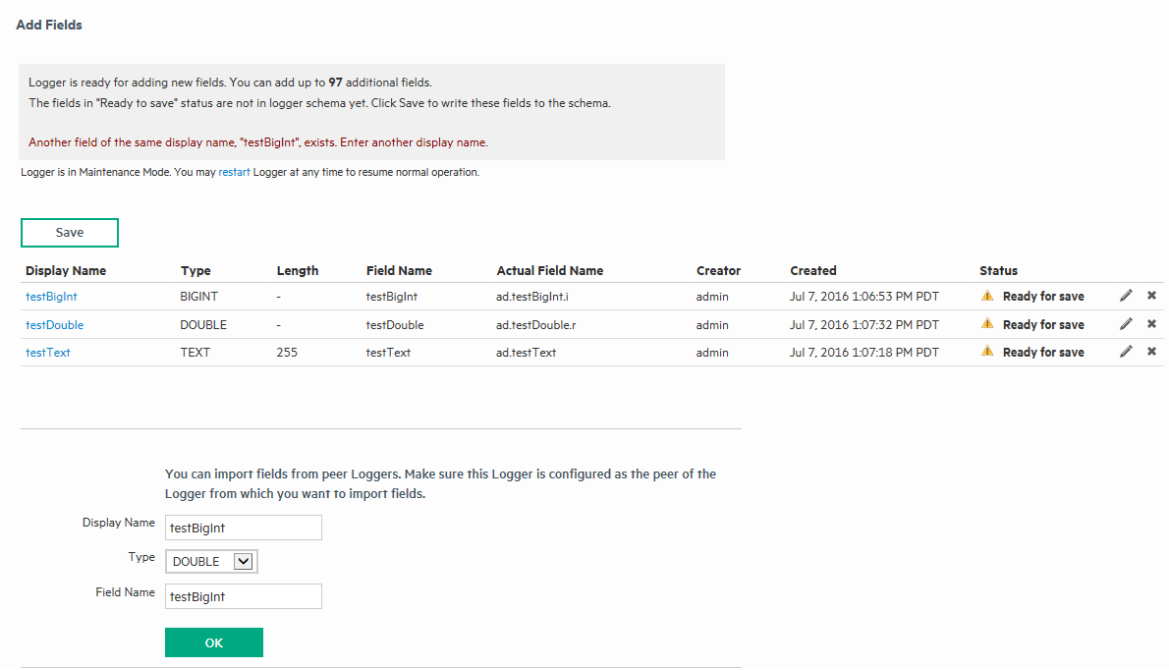
9. [**保存 (Save)**] をクリックして追加したフィールドをコミットし、Loggerのスキーマに書き込みます。

ピアからフィールドをインポートするには

1. メンテナンスモードを開始した後、[**ピアからのフィールドをインポート**] をクリックします (選択されていない場合)。
2. フィールドのインポート元となるピアを、[**ピアホスト名**] ドロップダウンリストから選択します。
3. 画面右下の [**OK**] をクリックします。

   競合するフィールドがない場合、ピアからのすべてのフィールドが正常にインポートされます。

   競合がある場合、競合するフィールドは正常にインポートされたフィールドの前に表示されます。[ステータス (Status)] 列には、衝突の理由が表示されます。これらのフィールドをスキーマに保存する前に、リストされている問題を解決する必要があります。追加したフィールドを変更または削除するには、行末にある編集 ( ) または削除 ( ) アイコンを使用します。



インポートできる数よりも多くのフィールドがある場合、最大数(100)に達するまで、最初のN個のみがインポートされます。

注意: インポートされたフィールドは、Loggerのスキーマにまだコミットされていません。次のステップでコミットします。この処理は元に戻すことができません。つまり、一度Loggerのスキーマに書き込んだフィールドは、編集または削除できなくなります。

保存せずにこの処理を終了すると、追加途中のフィールドは記憶されず、変更内容が失われます。

4. [**保存 (Save)**] をクリックして追加したフィールドをコミットし、Loggerのスキーマに書き込みます。Loggerを再起動して、変更内容を有効にします。

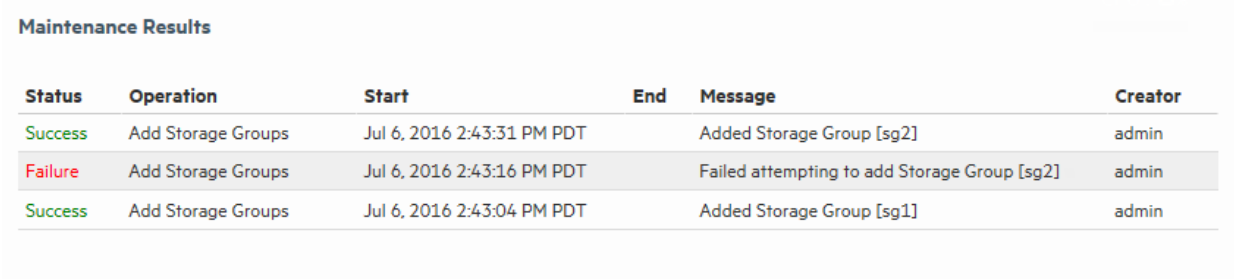
   ピアLoggerからフィールドを追加した場合は、必ず同じフィールドを他のピアにも追加してください。

カスタムスキーマフィールドを表示するには、「カスタムフィールド」(356ページ)を参照してください。

メンテナンス結果

メンテナンス操作のステータスは、[メンテナンス結果] ページで確認できます。

[メンテナンス結果] ページ (以下に例を示します) にアクセスするには、**[設定 | 詳細]** メニューを開き、**[メンテナンス結果]** をクリックします。



Maintenance Results

Status	Operation	Start	End	Message	Creator
Success	Add Storage Groups	Jul 6, 2016 2:43:31 PM PDT		Added Storage Group [sg2]	admin
Failure	Add Storage Groups	Jul 6, 2016 2:43:16 PM PDT		Failed attempting to add Storage Group [sg2]	admin
Success	Add Storage Groups	Jul 6, 2016 2:43:04 PM PDT		Added Storage Group [sg1]	admin

設定のバックアップとリストア

デフォルトでは、Loggerはどのデータもバックアップしません。ただし、以下のデータをリモートシステムにバックアップするように設定できます。

- イベント以外のすべてのデータ (ルックアップファイルを除く)
- レポートデータのみ

このデータは、一度だけバックアップしたり (アドホック)、定期的にバックアップするようスケジュールしたりすることができます。データはバックアップ場所に.tar.gz形式のファイルで保存されます。

注意: 設定バックアップ (設定用) とイベントアーカイブ (データ用) が定期的に実行され、離れた場所に保存されることを確認してください。また、ライセンスのコピーも保存する必要があります。致命的な障害が発生した場合は、最新の設定バックアップ、イベントアーカイブ、ライセンスを復元する必要があります。イベントアーカイブについては、「イベントアーカイブ」(432ページ) を参照してください。

バックアップデーターを使用して、以下のことが可能です。

- 期待どおりに機能していないか、工場出荷時のデフォルトにリセットされたLoggerを回復する。
- 複数のLoggerの間でデータをコピーする。

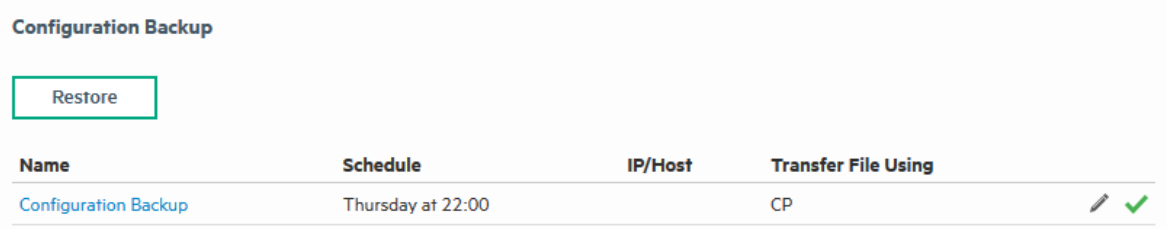
注意: Loggerにデータをリストアすると、現在の内容が削除または上書きされます。

次の表に、イベント以外のすべてのデータとレポートのみのデータをバックアップしたときにバックアップに含まれる情報の一覧を示します。

イベント以外の全データのバックアップの内容	レポートのみのバックアップの内容
システム情報 ライセンス* ログ グローバル設定 ユーザーおよびグループ情報 すべての設定 既存のフィルターと保存された検索 Logger Monitor設定 以下のレポートデータ • クエリ、レポート、パラメーター、パラメーター値グループ、ダッシュボード • テンプレート **注:** ルックアップファイルは、設定バックアップに含まれていません。	以下のレポートデータのみ • クエリ、レポート、パラメーター、パラメーター値グループ、ダッシュボード • テンプレート

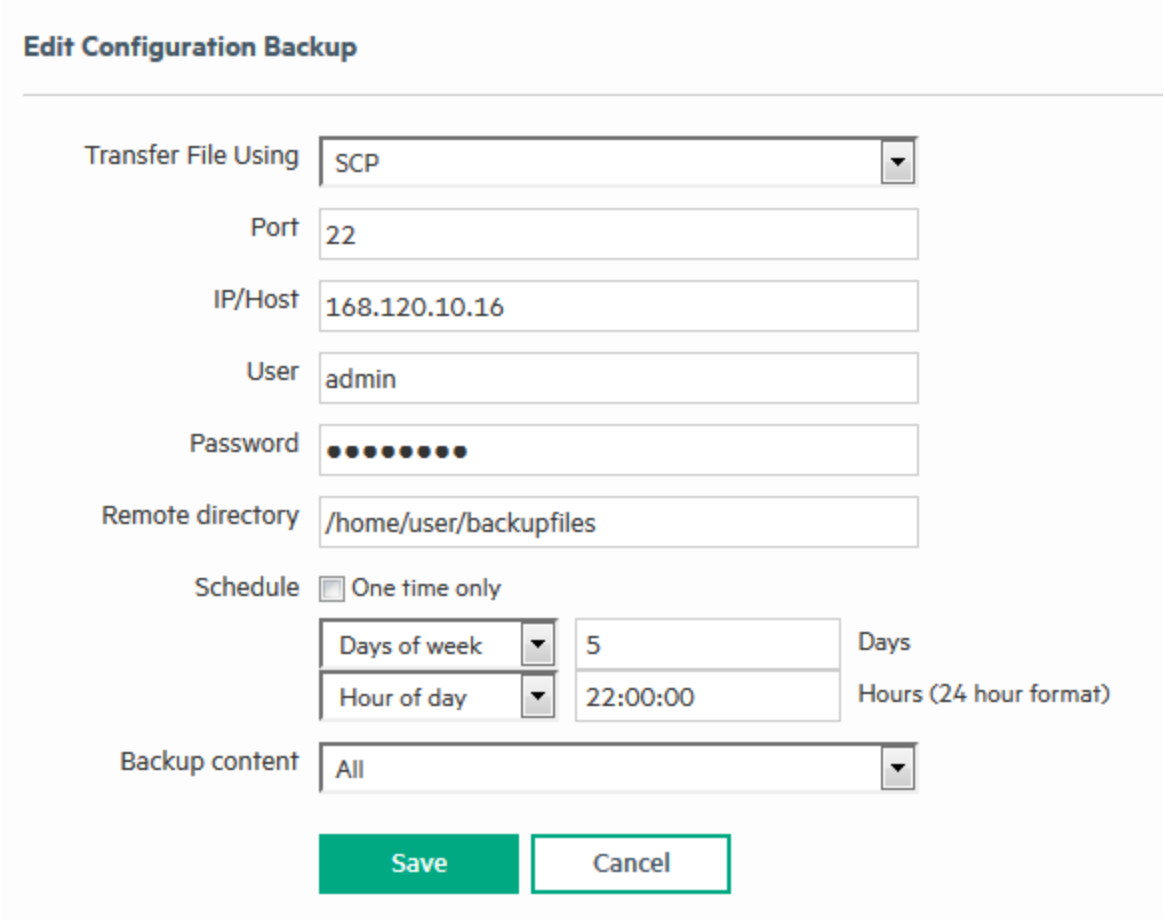
設定バックアップの実行

Logger設定情報のバックアップを作成して実行するには、次の手順を実行します。



設定バックアップの実行または設定バックアップの編集を行うには

1. **[設定 | 詳細]** メニューを開き、**[設定バックアップ]** をクリックします。
2. (✎) アイコンをクリックし、以下のパラメーターを入力します。



パラメーター	説明
使用するファイルの転送 (Transfer File Using)	• ファイルをリモートホストに転送する場合は、**SCP**を選択します。 • ファイルをLogger上の場所にコピーする場合は、**CP**を選択します。 使用可能なオプションは、選択内容によって異なります。
ポート (Port) (SCPのみ)	Loggerがリモートシステムに接続するために使用するポート。
Ip/ホスト (IP/Host) (SCPのみ)	リモートシステムのIPアドレスまたはホスト名。
ユーザー (User) (SCPのみ)	バックアップフォルダー (以下の [リモート ディレクトリ] で指定) に対する書き込み権限を持つリモートシステム上のユーザー。

パラメーター	説明
パスワード (Password) (SCPのみ)	ユーザーのパスワード。パスワードには次の文字を使用できません。% = ; " ' <>
マウントポイント (アプライアンスのみ)	アプライアンスに以前に追加されていたマウントポイントを選択します。
リモートディレクトリ (Remote Directory)	設定バックアップファイルを保存する場所。リモートディレクトリ名にスペースを含めることはできません。 **注:** Loggerアプライアンスは、ユーザーインターフェイスによるマウントをサポートしています。ソフトウェアLoggerは、ファイルシステムを使用します。これには、オペレーティングシステムによってマウントされたリモートフォルダーを含めることができます。
スケジュール (Schedule)	バックアップを実行するタイミングと頻度をスケジュールします。 • デフォルトの [**一度だけ**] チェックボックスを有効のままにすると、他のフィールドは非表示になり、[**保存**] をクリックしたときに、設定バックアップが一度だけ実行されます(アドホック)。 • [**一度だけ**] チェックボックスを無効にすると、設定バックアップを実行する頻度を指定するためのスケジュールオプションを使用できるようになります。「定期バックアップのスケジューリング」(472ページ) を参照してください。
バックアップ コンテンツ (Backup content)	イベント以外の全データをバックアップするか、レポートデータのみをバックアップするかを指定します。 • イベント以外のデータをバックアップする場合は、[**すべて**] を選択します。 • レポートコンテンツのみをバックアップする場合は、[**レポート コンテンツのみ**] を選択します。

3. **[保存 (Save)]** をクリックします。設定した構成バックアップは、[構成バックアップ] ページに表示されます。

   注: バックアップを**一度だけ**実行することを選択した場合は、設定バックアップがすぐに実行されます。そうでない場合は、指定した時刻に実行するようスケジュールされます。

4. 1つ以上の設定バックアップを作成すると、[設定バックアップ] ページから、以下のアクションを実行できます。
   a. [**復元**] をクリックして、設定バックアップのリストを開始します。「設定バックアップからの復元」(472ページ) を参照してください。
   b. 関連付けられている編集アイコン(✎)か、バックアップファイルの名前をクリックして、設定バックアップのパラメーターを変更します。
   c. 目的のバックアップファイルが無効になっている場合は、⊘アイコンをクリックして有効にします(✔)。

d. 目的のバックアップファイルが有効になっている場合は、✔アイコンをクリックして無効にします(⊘)。

定期バックアップのスケジューリング

定期バックアップをスケジュールする場合は、「日付と時刻のスケジュールのオプション」(150ページ)で説明されているように、スケジューリングオプションを設定します。

設定バックアップからの復元

Logger上にバックアップファイルを復元する前に、以下のガイドラインをよくお読みください。

- Loggerにデータを復元すると、現在の内容が削除または上書きされます。
  Loggerは、バックアップを取得した時点で最新だった、特定の環境設定を復元します。バックアップ時点と復元時点の間に更新された設定はすべて失われます。これにはライセンスファイルが含まれます。
- バックアップファイルを作成するために使用したのと同じバージョンのLoggerにデータを復元する必要があります。
- 同じ形式のLogger (ソフトウェア、アプライアンス、またはVMware) に復元する必要があります。
- アプライアンスLoggerの場合、Loggerアプライアンスのモデルは、バックアップファイルを作成するために使用したものと同じであることが必要です。
- ソフトウェアLoggerと、VMware上のLoggerの場合、Loggerで動作しているオペレーティングシステムは、バックアップファイルを作成するために使用したものと同じであることが必要です。
- 現在のライセンスはバックアップによって上書きされるため、必要に応じて、復元の完了後に再適用するために既存のライセンスのコピーを保持します。

設定バックアップから復元するには

1. **[設定 | 詳細]** メニューを開き、**[設定バックアップ]** をクリックします。
2. **[復元]** をクリックします。
   [設定バックアップをアップロード] オプションが、[設定バックアップ] ページに表示されます。設定の復元後に、Loggerを再起動する必要があるというメッセージが表示されます。
3. **[ブラウズ]** をクリックしてバックアップファイルを探します。
4. **[送信]** をクリックして復元処理を開始します。
5. 復元処理が完了すると、Loggerをリブートするよう求められます。
   a. Loggerアプライアンス—復元処理が完了すると、**[システム管理] > [システム] > [システムリブート]** ページにリダイレクトされます。[リブート] を選択して **[リブート]** をクリックします。「システムの再起動」(492ページ)を参照してください。

b. ソフトウェアLogger—復元処理が完了すると、システムをリブートするよう求められます。「ソフトウェアLoggerのコマンドラインオプション」(557ページ) を参照してください。

ヒント: 新しいライセンスをアップロードするか、バックアップ前のライセンスのコピーを再適用しなければならない場合があります。

コンテンツ管理

ユーザーは、その権限に応じて、アラート、ダッシュボード、フィールドセット、フィルター、パーサー、保存された検索、ソースタイプをLoggerからファイルにエクスポートして、そのデータを別のLoggerにインポートしたり、バックアップとして同じLoggerに再度インポートしたりすることができます。特定の種類のデータをインポートまたはエクスポートするために必要なユーザーの権限と、Loggerのデータをインポートおよびエクスポートするための手順およびガイドラインについては、「データをエクスポートするためのユーザー権限」(475ページ) および「データをインポートするためのユーザー権限」(473ページ) を参照してください。

データのインポートとエクスポートは、以下の状況で有用です。

- Loggerのデータのバックアップコピーを作成する必要がある場合。Loggerが使用不要になるか、工場出荷時のデフォルトにリセットされた場合は、保存したデータをインポートすることで、その内容を素早く復元できます。
- 同じデータを持つ複数のLoggerをネットワークにインストールする必要がある場合、設定する必要があるのは1つのLoggerのみです。それ以降のLoggerは、最初のLoggerのデータをインポートすることで展開できるため、展開時間を短縮できます。
- あるLoggerのデータを別のLoggerに追加する必要がある場合。

[**エクスポート**] 機能を使用すると、Loggerのデータは、ネットワーク上の格納場所か、Loggerへの接続に使用しているコンピューターのローカルディスクに保存されます。前述のいずれかの状況でそのデータを使用する必要がある場合は、保存したデータをインポートするだけで済みます。

データをインポートするためのユーザー権限

インポートできるデータは、ユーザーの権限によって変わります。以下のいずれかの権限を持っている場合、**[コンテンツのインポート]** ページを使用できます。

- [Logger 権限] > [**フィルター**]: 共有フィルターの編集、保存、削除。
- [Logger 権限] > [**転送者と警告**]: 転送者と警告の編集、保存および削除。

注: このLoggerの権限では、転送者と警告の両方を編集、保存、削除できますが、インポートできるのは警告のみで、転送者はインポートできません。

- [Logger 権限] > [**ダッシュボード**]: ダッシュボードの編集、保存および削除。

ユーザーがダッシュボードの保存権限を持っているものの、保存された検索の保存権限を持っていない場合、検索結果パネルを使用したダッシュボードはインポートされません(警告メッセージに、スキップされるダッシュボードが示されます)。

- [Logger 権限] > [**保存された検索**]: 保存された検索の編集、保存および削除。
- [**システム管理**]: パーサーとソースタイプについては、ユーザーをシステム管理グループに割り当てることができます。ユーザーが管理者でない場合、パーサータイプとソースタイプはインポートできません。

  Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ)を参照してください。

[インポート] ページが表示される場合でも、すべての種類のデータをインポートできるとは限りません。関連付けられたユーザー権限を持っていない場合、その種類のデータをインポートできず、代わりに警告メッセージが表示されます。

データのインポート

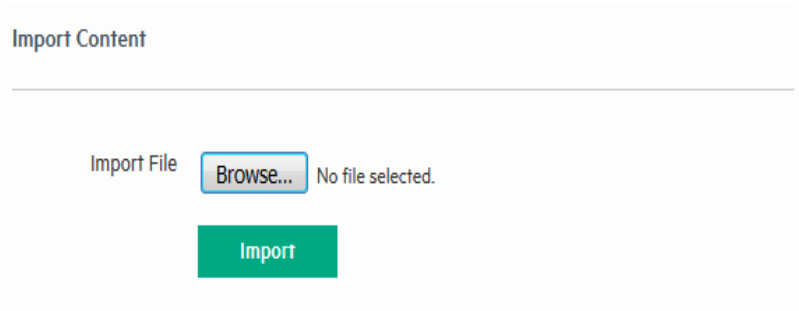
Loggerのデータをインポートする前に、以下のガイドラインをお読みください。

- 同じ名前のオブジェクトがインポート先のシステムに存在する場合、インポートされるオブジェクトの名前が `<ObjectName> [import]` になります。たとえば、インポートされるアラートの名前は`AlertName [import]` となり、インポートされるフィルターの名前は`FilterName [import]` となります。

  名前が `<ObjectName> [import]` のオブジェクトがインポート先のLoggerにすでに存在する場合 (前回のインポート処理の結果)、インポートされるオブジェクトの名前は `<ObjectName> [import] [import]` となります。
- インポートするアラートのアラート通知先 (SNMP、syslog、ESM通知先、およびSMTPサーバー) を必ず設定してください。この情報は、エクスポートされたデータには含まれていません。
- データのエクスポートおよびインポートでは、Loggerのインポートは、Loggerのエクスポートと同じ設定が使用されているものと想定されます。データのインポート先のLoggerの設定 (デバイス、デバイスグループ、ストレージグループ) は、Loggerのエクスポートと同じでなければなりません。信頼できるデータをインポートしなかった場合は、その設定を使用することはできません。

別のLoggerからデータをインポートするには

1. [**設定 | 詳細**] メニューを開き、[**コンテンツのインポート**] をクリックします。



2. [**ブラウズ (Browse)**] をクリックしてファイルを探します。
   このファイルは、Loggerのユーザーインターフェイスにアクセスするために使用しているブラウザーが動作するシステムからアクセス可能なローカルドライブまたはリモートドライブに存在している必要があります。
3. [**インポート (Import)**] をクリックします。

データをエクスポートするためのユーザー権限

エクスポートできるデータは、ユーザーの権限によって変わります。以下のいずれかの権限を持っている場合、「データのエクスポート」(476ページ) で説明されている [**エクスポート**] ページを使用できます。

- [Logger 権限] > [**フィルター**]: 共有フィルターの使用と表示。
- [Logger 権限] > [**転送者と警告**]: 転送者と警告の表示。

  注: このLoggerの権限では、転送者と警告の両方を表示できますが、エクスポートできるのは警告のみで、転送者はエクスポートできません。

- [Logger 権限] > [**ダッシュボード**]: ダッシュボードの使用と表示。
  ユーザーがダッシュボードの読み取り権限を持っているものの、保存された検索の読み取り権限を持っていない場合、検索結果パネルを含むダッシュボードは [エクスポートするコンテンツ] ダイアログボックスで選択できません。
- [Logger 権限] > [**フィールドセット**] : フィールドセットの表示。
- [Logger 権限] > [**保存された検索**] : 保存された検索の表示。
- [**システム管理**] : パーサーとソースタイプについては、ユーザーをシステム管理グループに割り当てることができます。ユーザーが管理者でない場合、パーサーとソースタイプはエクスポートできません。
  Loggerのユーザー権限とその管理方法の詳細については、「ユーザ/グループ」(530ページ) を参照してください。

[エクスポート] ページが表示される場合でも、すべての種類のデータをエクスポートできるとは限りません。上記のいずれかのユーザー権限を持っていない場合、対応する種類のデータを [**エクスポートするコンテンツ**] ダイアログボックスで使用できません。

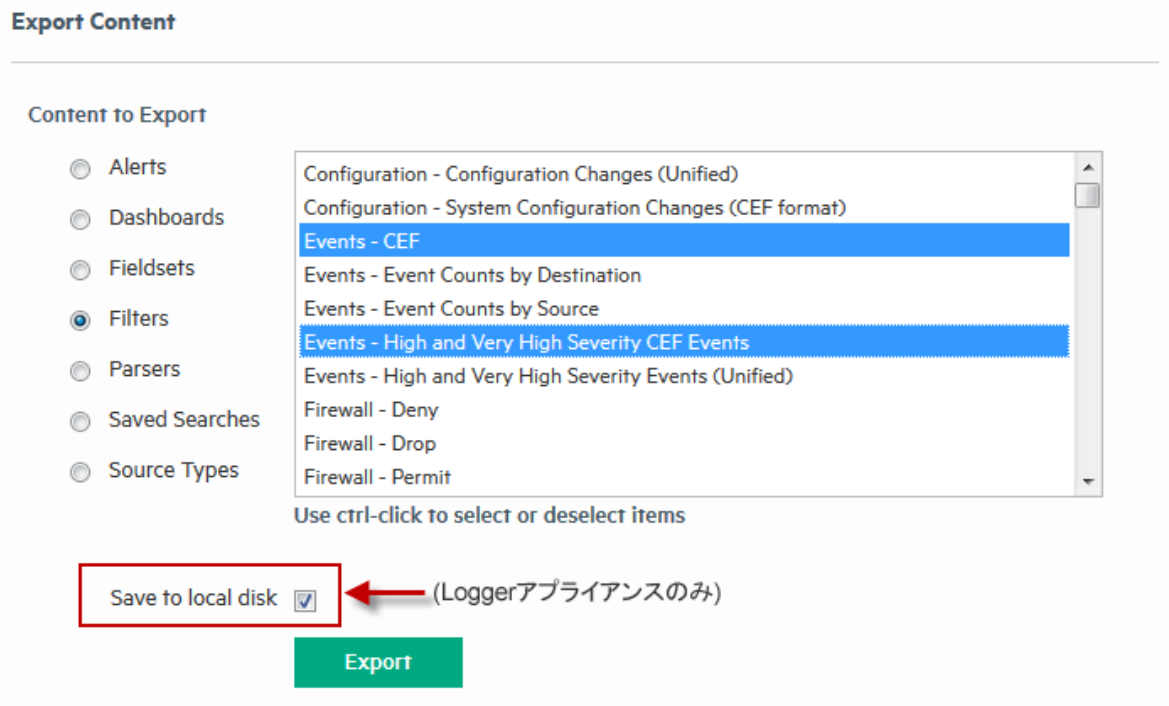
データのエクスポート

Loggerのデータをエクスポートする前に、以下のガイドラインをよくお読みください。

- エクスポートされたデータは、gzipファイル内にXML形式で格納されます。たとえば、`allfilters.xml.gz`となります。
- Loggerデータのエクスポート先となる、リモートファイルシステム上のフォルダーは、データをエクスポートする前に存在している必要があります。
- アラートをエクスポートする場合、アラートに関連付けられているクエリ、一致数、しきい値、ステータスがエクスポートに含められます。エクスポートには、メール、SNMP、ESM通知先の情報や、syslog通知先の情報は含まれません。アラート通知先 (SNMP、syslog、ESM通知先、およびSMTPサーバー) の情報はエクスポートされないため、アラートのインポート時にこの情報を設定する必要があります。
- ダッシュボードをエクスポートする場合、エクスポートされるダッシュボードで使用されている保存された検索のデータもエクスポートされます。
- ソースタイプをエクスポートする場合、エクスポートされるソースタイプで使用されているパーサーのデータもエクスポートされます。

Loggerデータをエクスポートするには

1. [**設定 | 詳細**] メニューを開き、[**コンテンツのエクスポート**] をクリックします。



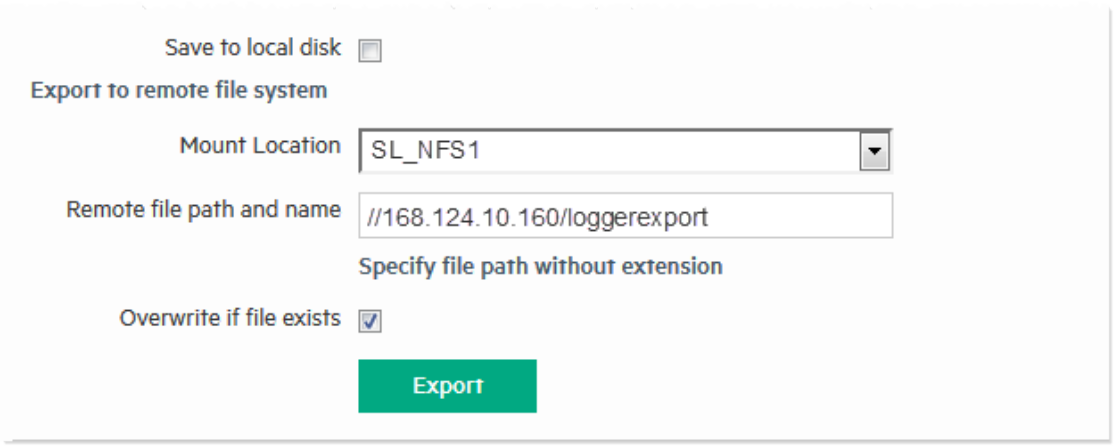
2. エクスポートするデータの種類に対応したラジオボタンを選択します。選択するデータの種類によって、使用可能なオブジェクトのメニューが変わります。
3. エクスポートするオブジェクトをメニューから選択します。

   1つのオブジェクトを選択するには、その名前をクリックします。複数のオブジェクトを選択するには、Ctrlキーを押しながら複数の名前をクリックします。
4. ソフトウェアLoggerの場合は、[**エクスポート (Export)**] をクリックします。ブラウザーの設定に従ってデータが保存されます。Loggerアプライアンスを使用している場合は、次のステップに進みます。
5. アプライアンスLoggerの場合は、エクスポートされるデータの保存場所を選択します。[**ローカル ディスクへ保存 (Save to local disk)**] がデフォルトのオプションです。

   Loggerへの接続に使用しているコンピューターのローカルディスクに保存するには、[**ローカル ディスクへ保存 (Save to local disk)**] をオンにしたままにします。

リモート ロケーションにエクスポートするには

a. [**ローカル ディスクへ保存 (Save to local disk)**] をオフにし、リモートファイルシステムにエクスポートするためのオプションを表示します。



b. データのエクスポート先の場所を、[**マウント ポイント (Mount Location)**] フィールドで選択します。目的の場所がドロップダウンリストにない場合は、それを追加する必要があります。ネットワークの格納場所の追加については、「ストレージ」(509ページ) を参照してください。

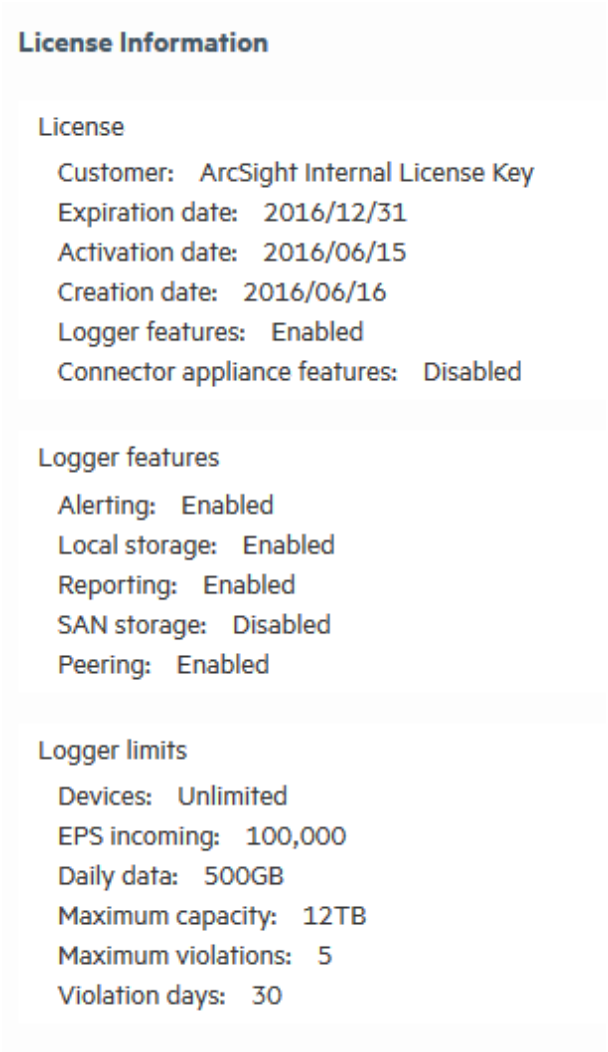
c. [**リモート ファイルのパスと名前 (Remote file path and name)**] フィールドに、前のステップで指定した、[マウント ポイント (Mount Location)] にある、エクスポートされたデータファイルを作成するためのフォルダーを入力します。このステップで指定するフォルダーは、[マウント ポイント (Mount Location)] で指定した場所にあらかじめ作成されている必要があります。これはLoggerによって作成されるわけではありません。

注: 拡張子を使用せずにファイル名を指定します。

6. 前のステップで指定したフォルダーの、エクスポートされるデータファイルと同じ名前のファイルを上書きする場合は、[**ファイルが存在する場合は上書き (Overwrite if file exists)**] をオンにします。
7. [**エクスポート (Export)**] をクリックします。

ライセンス情報

[ライセンス情報] ページ ([**設定 | 詳細] > [ライセンス情報**]) には、現在適用されているライセンスに関する情報が表示されます (次の例参照)。



試用版ライセンス

どちらのArcSight Loggerにも90日間の評価期間に使用できる試用版ライセンスが付属しています。評価期間が終了した後は、有効なライセンスを適用するまでLoggerのどの機能にもアクセスできなくなります。

試用版ライセンスでは、以下の機能にアクセスできます。

- レポートを除くLoggerのすべての機能。
- 1日あたり5 GBのデータ収集量(ソフトウェアLoggerのみ)。
- 90 GBのストレージ。(アップグレードされたシステムの場合、ライセンスでは90GBと表示されますが、Logger上のストレージボリュームは、この限度まで下がることはありません)

新しいライセンスをできるだけ早くアップロードしてください。新しいライセンスをアップロードするには、メニューバーの[**システム管理**]を開き、[**システム**]セクションの[**ライセンスおよび更新**]をクリックします。「Loggerライセンスの更新」(501ページ)の説明を参照してください。

使用するライセンスでArcMCによる管理が許可されているかどうかによって、試用版ライセンスをスタンドアロンArcSight Loggerライセンスまたは ADPライセンスのいずれかで更新できます。(ADP LoggerはArcMCによって管理されます)。いずれかのライセンスをアップロードすると、レポート機能が有効になり、使用可能な1日のデータ量とストレージ量がライセンスで許可された容量に増加します。

Loggerが収集する1日のデータ量は、[データボリューム] ページの **[構成 | 詳細] > [データボリューム]** の下に表示されます。1日のデータの制限やその他のライセンス情報は、Loggerの **[構成] > [詳細] > [ライセンス情報]** および **[システム管理] > [システム] > [ライセンスおよび更新]** の下で確認できます。

データボリューム

[データボリューム] ページ(**[設定 | 詳細] > [データボリューム]**)には、ソフトウェアLogger上に保存されている過去30日の各日のデータの量が表示されています。

データボリュームの制限機能は、00:00:00 UTCの時点で過去24時間のデータを測定し、その情報を [データボリューム] ページで通知します。この機能が使用する時間は、Loggerのローカル時間とは無関係です。

データボリュームの制限機能の動作方法と、[データボリューム] ページに表示される内容は、ご使用のライセンスのタイプによって異なります。

- 試用版Logger、スタンドアロンArcSight Logger、すべての新しくアップグレードされたLoggerの場合、データボリュームの制限機能は、特定の日に受信されたイベントのサイズを合計して、取得される1日のデータボリューム(Loggerに入ってくる1日あたりのデータ量)を計算します。Loggerは、その値とライセンスの1日のデータ制限を比較します。この制限値を超えても、Loggerはイベントを収集して保存するので、イベントが紛失することはありません。ただし、過去30日間のウィンドウ内で制限値を超えた日が6日以上ある場合、検索関連のすべての機能が無効になります。

  注意: 無効となる検索機能には、すべての検索およびレポート機能だけでなく、転送者も含まれます。

- ADP Loggerの場合は、ArcMCがライセンス制限を管理するため、データボリュームの制限機能で検索、転送、レポートが無効になることはありません。詳細については、『ArcSight Management Center管理者ガイド』を参照してください。

試用版およびスタンドアロンLoggerの [データボリューム] ページについては、「スタンドアロンのLoggerの [データボリューム] ページ」(481ページ)を参照してください。ADP Loggerの [データボリューム] ページについては、「ADP Loggerの [データボリューム] ページ」(482ページ)を参照してください。

新しくアップグレードされたソフトウェアLoggerの1日のデータ制限

Logger 6.3では、新しいタイプのライセンスファイルが実装されています。Logger 6.3へのアップグレード直後に、この新しいタイプのライセンスが有効になります。試用版Loggerライセンス(試用版ライセンス制限あり)は、6.3のスタンドアロンArcSight LoggerまたはArcSightデータプラットフォーム(ADP) Loggerライセンスをアップロードするまで使用されます。詳細については、「試用版ライセンス」(479ページ)を参照してください。

完全版ライセンスにアップグレードするまで、1日のデータ制限は5GBです。Loggerは、5GBのデータ容量制限を超過した日は、「ライセンスされたデータボリュームの制限を超過しました」という警告バナーを表示します。

注意: 30日間の間にデータ制限を6回超過した場合は、表示されている30日間のデータの中で違反が5回以下になるまで、一切の検索関連機能が使用できなくなります。無効になる検索関連機能には、すべての検索およびレポート機能だけでなく、転送者も含まれます。

「ライセンスと更新」(501ページ)の手順に従って、完全版ライセンスを適用します。

スタンドアロンのLoggerの[データボリューム]ページ

このトピックは、スタンドアロンArcSight Logger、新しくアップグレードされたLogger、および試用版Loggerに適用されます。

スタンドアロンおよび試用版のソフトウェアLoggerでは、[データボリューム]ページ(**[設定 | 詳細] > [データボリューム]**)に、1日のデータ収集量、1日あたりのライセンスサイズ(GB)、および発生したライセンス違反数が表示されます。データボリュームライセンス違反の制限は、30日間で5回までです。受信データボリュームがこの制限を超過すると、Loggerは「ライセンスされたデータボリュームの制限を超過しました」という警告バナーを表示します。

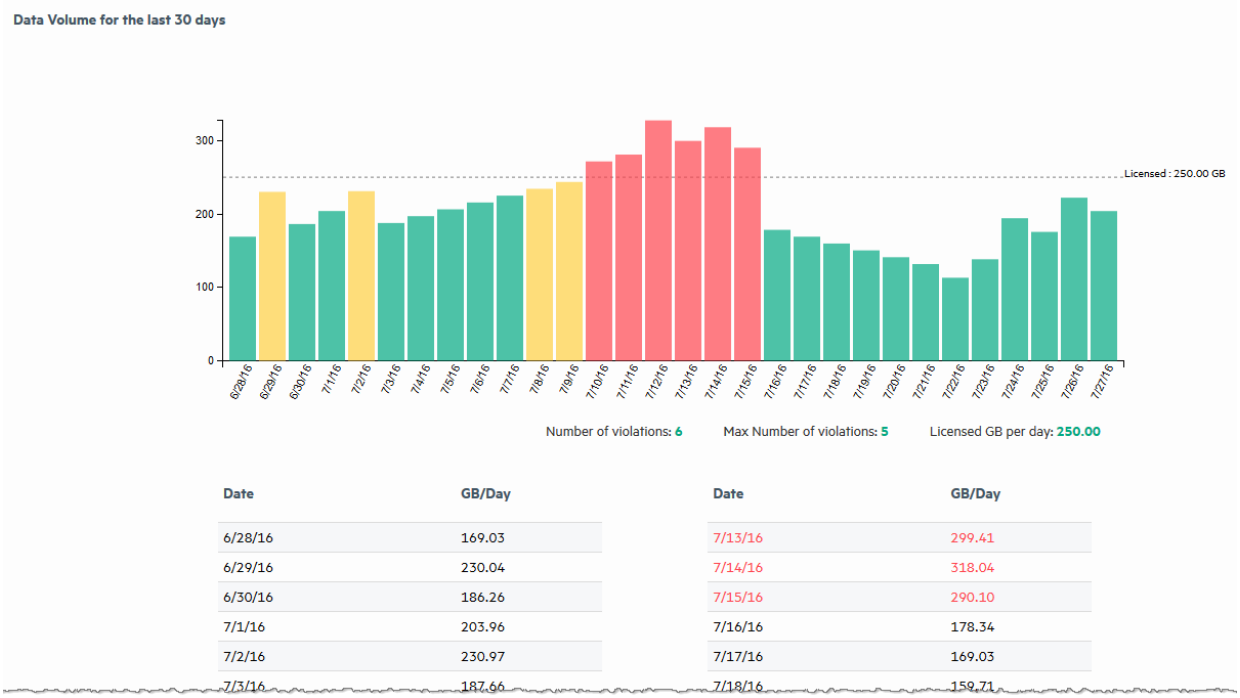
注: Loggerには、90日間の試用版ライセンスが付属しています。試用期間中に許可されているデータ収集の制限は、1日あたり5GBです。詳細は、「試用版ライセンス」(479ページ)を参照してください。この制限を緩和するには、「ライセンスと更新」(501ページ)の手順に従って、ライセンスを適用してください。

データボリュームグラフで、縦軸は許可されている1日のデータボリュームを示し、緑の棒はデータボリュームがその日のライセンス制限の90%未満であること、黄色の棒はその日のライセンス制限の90%に達していること、赤のバーはその日のライセンス制限を超過していることを示しています。グラフの下に、違反数、許容される最大違反数、1日あたりのライセンスサイズ(GB)の一覧が表示されています。また、表には、過去30日の各日に収集されたデータが表示されています。

注意: 30日間の間にデータ制限を6回超過した場合は、表示されている30日間のデー

タの中で違反が5回以下になるまで、一切の検索関連機能が使用できなくなります。無効になる検索関連機能には、すべての検索およびレポート機能だけでなく、転送者も含まれます。

1日のデータ制限およびその他のライセンス情報は、Loggerの **[設定 | 詳細] > [ライセンス情報]** と、**[システム管理] > [システム] > [ライセンスおよび更新]** で確認できます。



Date	GB/Day	Date	GB/Day
6/28/16	169.03	7/13/16	299.41
6/29/16	230.04	7/14/16	318.04
6/30/16	186.26	7/15/16	290.10
7/1/16	203.96	7/16/16	178.34
7/2/16	230.97	7/17/16	169.03
7/3/16	187.66	7/18/16	159.71

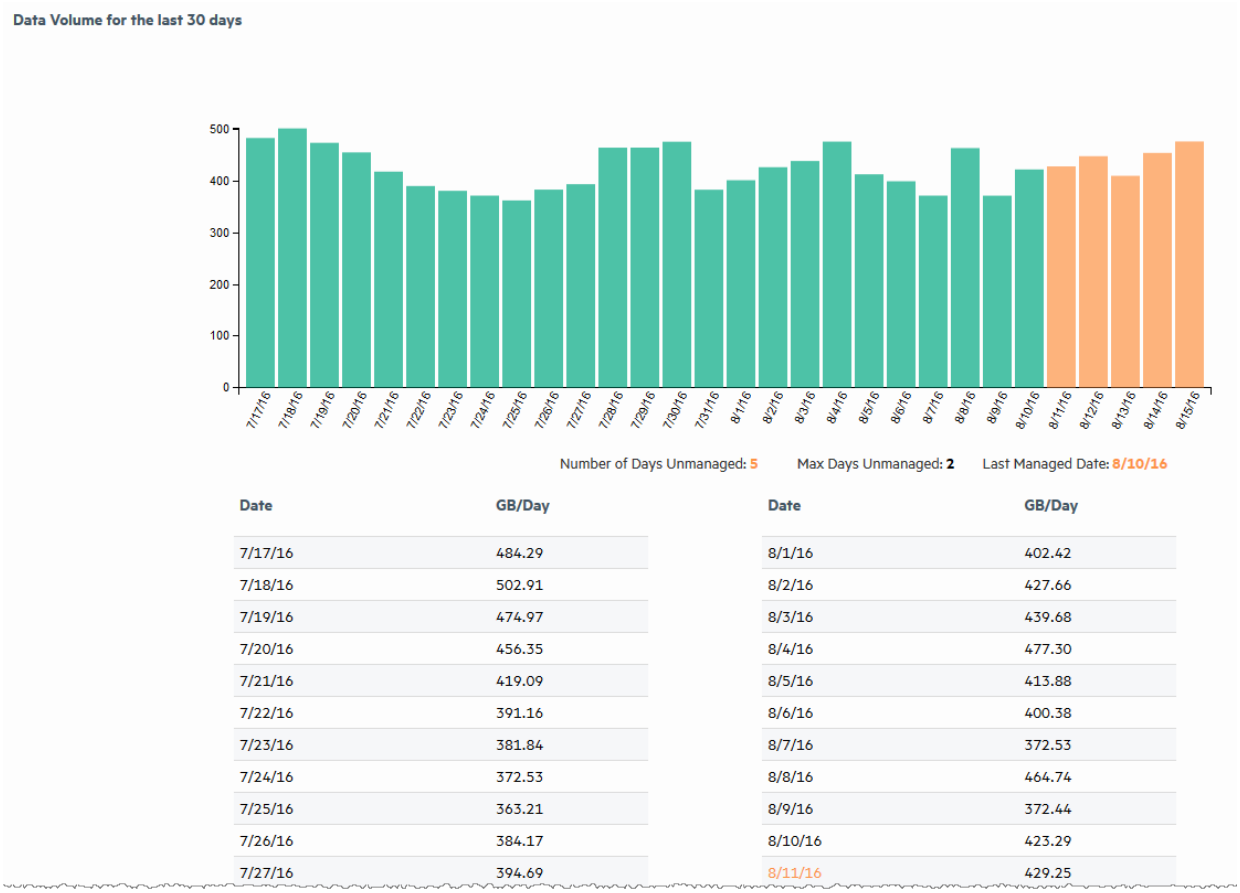
ADP Loggerの [データボリューム] ページ

このトピックは、ADP Loggerにのみ適用されます。

ADPソフトウェアLoggerの [データボリューム] ページ(**[設定 | 詳細] > [データボリューム]**)には、収集される1日のデータボリュームやLoggerの管理ステータスが表示されます。

注: ADP LoggerはArcMCによって管理されるため、スタンドアロンLoggerのデータボリュームの制限は適用されません。

[データボリューム] グラフでは、緑のバーは、その日にLoggerがArcMCに管理されていたことを示し、オレンジのバーは、その日にLoggerが管理されていなかったことを示しています。グラフの下に、管理されない日数、管理されない日数の最大許容数、最後の管理対象日がリストされています。また、表には、過去30日の各日に取得されたデータが表示されています。



Date	GB/Day	Date	GB/Day
7/17/16	484.29	8/1/16	402.42
7/18/16	502.91	8/2/16	427.66
7/19/16	474.97	8/3/16	439.68
7/20/16	456.35	8/4/16	477.30
7/21/16	419.09	8/5/16	413.88
7/22/16	391.16	8/6/16	400.38
7/23/16	381.84	8/7/16	372.53
7/24/16	372.53	8/8/16	464.74
7/25/16	363.21	8/9/16	372.44
7/26/16	384.17	8/10/16	423.29
7/27/16	394.69	8/11/16	429.25

ピアノード

Loggerは、1つ以上のLoggerまたはArcSightマネージャーとピア関係を確立し、分散された検索を有効にできます。他のLoggerまたはマネージャーを検索するには、1つ以上のピアを定義する必要があります。

2台のシステムが互いにピアになっている場合、一方が関係を開始します。イニシエーター(ピア関係の確立を開始する側)は、証明書を送信して、ターゲットシステムに自身の正当性を証明します。認証に成功すると、2台のシステムの間でピア関係が確立されます。

ピアを設定するための手順の概要

ピア関係を設定するには、次の手順を実行する必要があります。

1. ピア関係を開始するマネージャーまたはLoggerを決定します。この例では、マネージャーまたはLogger Aが開始側であり、Logger Bがターゲットです。
2. 「ピア認証メソッドの選択」(485ページ) の情報に基づいて、ピア認証メソッドを決定します。
   - ユーザー名とパスワードで認証するには、次の操作を実行します。
     「ユーザ/グループ」(530ページ) に説明されているように、マネージャーまたはLogger AがBとのピア接続またはユーザーの設定時に認証に使用するユーザー名とパスワードを特定します。
   - 認証IDとコードで認証するには、次の操作を実行します。
     マネージャーまたはLogger B上で、AがBとピア接続するときに、Aの認証に使用するAのための認証IDとコードを生成します。この手順については、「ピアの承認」(486ページ) を参照してください。
3. マネージャーまたはLogger A上で、「ピアの追加」(486ページ) に説明されているように、この認証情報をBから追加します。
   - ユーザー名とパスワードを使用して認証する場合、特定したユーザー名とパスワードを使用します。
   - 認証IDとコードを使用して認証する場合、生成した認証IDとコードを使用します。

ピア設定のガイドライン

ピアを設定する際は、次のガイドラインを考慮してください。

- Logger 6.4は、ESM 6.8c、ESM 6.5c、およびLogger 5.3以降とピアリングできます。
- 1つのLoggerで、最大で100のピアを設定できます。
- ピア関係にあるマネージャーまたはLoggerのシステム時間と日付が、タイムゾーンに合わせて正しく設定されている必要があります。HPEでは、NTPサーバーと定期的に同期するようシステムを設定することを推奨しています。
- リモートLoggerがSSLクライアント認証(SSL/CAC認証)用に設定されている場合は、イニシエーターLogger上で、認証IDとコードを設定する必要があります。
- FIPSを有効にしたLoggerでの特別な認証要件はありません。そのようなLoggerは、許可されているどの認証方式でも使用できます。
- ピアは編集できませんが、ピアを削除してから再度追加できます。
- 分散された検索 (複数のピアを対象とする検索) を実行している場合は、以下の追加のガイドラインに従ってください。

a. ユーザーは、「リモート ピアのイベント検索」権限が「**Yes**」に設定されたLogger検索ユーザーグループと、「登録されたピアを表示」権限が「**Yes**」に設定されたLogger権限グループに属している必要があります。「ピアの検索 (分散検索)」(115ページ) を参照してください。

b. ピア上で検索操作を実行するユーザーは、ログインしたLogger上でそれらのユーザーが持っている権限と同じ権限をピア上で持ちます。たとえば、ユーザーAは、検索グループフィルターによって、deviceVendorが「Cisco」に設定されているイベントのみを検索するように制限されています。ユーザーAがLogger Aの複数のピアにまたがって検索操作を実行すると、同じ制約 (deviceVendorが「Cisco」のイベントを検索) がすべてのピアに適用されます。

- 分散レポート (複数のピアにまたがるレポート) を実行する場合は、「グループ、デバイス、ピアの選択」(200ページ) を参照してください。
- リモートピアへの認証にユーザー名とパスワードを使用する場合、ピア関係の確立後にユーザー名とパスワードを変更しても、関係に影響はありません。しかし、ピア関係を削除したり、その他の理由によって関係が切断された場合、この関係を再確立するために、変更した資格情報を提供する必要があります。

ピアの認証

認証は、ピア関係の構築時に1回だけ実行されます。リモートシステムが、ピアとして以前に認証されているシステムからピア要求を受け取るときに、ピアサービスに使用される認証は、毎回暗黙の認証になります。

ピアは次の2つの方法のいずれかで認証できます。

- **ピア認証IDとコード**: これらの資格情報は、一方のマネージャーまたはLogger上で生成され、相互間のピア接続を設定するためにもう一方で使用されます。認証IDとコードを生成するときは、ピア接続の開始側マネージャーまたはLoggerのIPアドレスを接続相手の [ピア認証] ページに入力します。このIPアドレスは、固有のIDおよびコードを生成するために使用され、そのアドレスからのピア接続用にのみ使用できます。そのため、この方法は、ユーザー名とパスワードを使用する方法よりも安全です。

  注: HP ArcSightでは、認証にはピア認証IDとコードを使用することをお勧めします。

- **ユーザー名とパスワード**: 認証には、ターゲットシステム上ですでに設定されているユーザー名とパスワードが使用されます。

ピア認証メソッドの選択

- ピア接続を設定するためにユーザー名とパスワードを使用するときは、LDAPまたはRADIUS認証を使用するようにシステムを設定している場合でも、ローカル認証用のユーザーパスワードを使用する必要があります。

- ピアマネージャーまたはLoggerがSSL Client認証 (CAC) 用に設定されている場合、ターゲットのマネージャーまたはLogger上で、認証IDとコードを設定する必要があります。ユーザー名とパスワードを使用することはできません。
- FIPSが有効なシステムは、特定の認証方法に制限されません。

ピアの承認

ピア関係を確立するターゲットのマネージャーまたはLoggerで認証IDとコードを生成するには、以下の手順を使用します。「ピアノード」(483ページ)の例ではマネージャーまたはLogger Bです。その後、ピア関係の設定時に、関係の開始側のマネージャーまたはLogger (この例ではマネージャーLogger A) 上でこのIDとコードを使用します。

ピア関係の設定時に使用する認証IDとコードを生成するには

1. [**設定 | 詳細**] メニューを開き、[**ピア認証**] をクリックします。
2. [**追加**] をクリックします。
3. このシステムとピア接続するマネージャーまたはLoggerのホスト名またはIPアドレス、およびポートを入力します。
4. [**保存**] をクリックします。

   承認IDと承認コードが表示されます。この情報をコピーし、このシステムをピアとして追加するときに、もう一方のマネージャーまたはLoggerで使用します。
5. [**完了**] をクリックし、[ピア認証] リストに戻ります。

ピア関係の追加および削除

[**ピアノード**] ページに、現在のピア関係が表示されます。ここからピアを追加および削除できます。

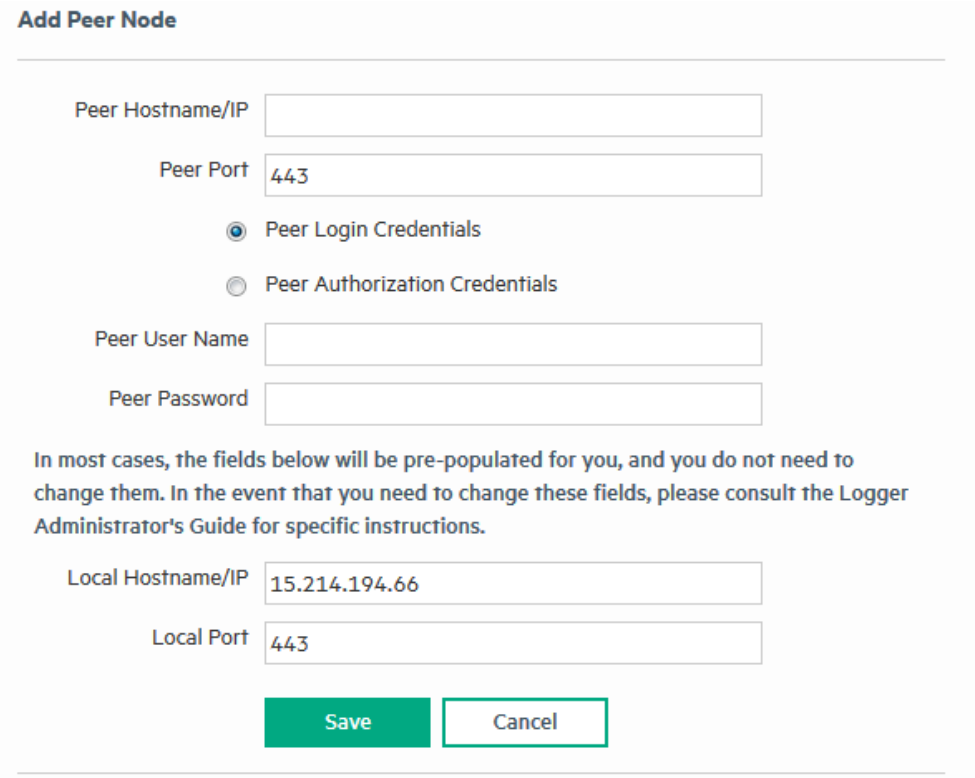
ピアの追加

ピアを追加すると、2つのLogger間、2つのArcSightマネージャー間、または1つのLoggerと1つのマネージャーとの間にピア関係が作成されます。ピアの追加後は、ピアを削除することはできますが、編集することはできません。詳細については、「ピア設定のガイドライン」(484ページ)を参照してください。

Loggerでのピアの追加は、双方向のプロセスです。つまり、Logger AがLogger Bに対するピアアクセスを追加すると、Logger BはLogger Aに対するピアアクセスを自動的に追加します。同様に、A上でBに対するピアアクセスを削除すると、B上でAに対するピアアクセスが自動的に削除されます。

ピアを追加するには

1. [**設定 | 詳細**] メニューを開き、[**ピアノード**] をクリックします。



2. [**追加**] をクリックし、以下のパラメーターを入力します。

パラメーター	説明
ピアホスト名/IP (Peer Hostname/IP)	ターゲットのマネージャーまたはLoggerのホスト名またはIPアドレスを入力します。
ピアポート (Peer Port)	ターゲットシステムのインストール時または初回設定時に設定されたポートを使用します。「ピア設定のガイドライン」(484ページ)を参照してください。 Loggerアプライアンスの場合、デフォルトはポート443です。

パラメーター	説明
ピアログインの資格情報 (Peer Login Credentials) ピア認証の資格情報 (Peer Authorization Credentials)	パスワードベース認証の場合は [**ピア ログインの資格情報 (Peer Login Credentials)**] を選択します。 または 認証IDとコードを使用する場合は [**ピア認証の資格情報 (Peer Authorization Credentials)**] を選択します。 • ローカルまたはRADIUS認証を使用するシステム上では、どちらの認証メソッドでも使用することもできます。ただし、ピア認証IDとコードが推奨されます。 • SSLクライアント認証 (CAC) を使用するシステム上では、ピアを認証するための方法は認証IDとコードのみです。ユーザー名とパスワードを使用することはできません。(「SSLクライアント認証」(523ページ) を参照)。 • FIPSが有効なシステムは、特定の認証方法に制限されません。
[ピア ログインの資格情報 (Peer Login Credentials)] を選択した場合	
ピア ユーザ名 (Peer User Name)	ターゲットシステム上ですでに設定されているユーザー名を入力します。
ピア パスワード (Peer Password)	[ピアユーザ名] フィールドに指定したユーザーのパスワードを入力します。
[ピア認証の資格情報 (Peer Authorization Credentials)] を選択した場合	
ピア認証 ID (Peer Authorization ID)	ターゲットのマネージャーまたはLogger上で生成された認証IDを入力します。(詳細については、「ピア関係の設定時に使用する認証IDとコードを生成するには」(486ページ) を参照してください)。
ピア認証コード (Peer Authorization Code)	ターゲットのマネージャーまたはLogger上で生成された認証コードを入力します。(詳細については、「ピア関係の設定時に使用する認証IDとコードを生成するには」(486ページ) を参照してください)。
その他のフィールド: 以下のフィールドの更新が必要になることは滅多にありません。	
ローカルホスト名/IP (Local Hostname/IP)	ほとんどの場合、このフィールドの値は、ブラウザーからこのLoggerに接続するために使用するIPアドレスまたはホスト名に一致し、何もする必要はありません。 ただし、IPアドレスまたはホスト名が一致しない場合は (たとえば、LoggerがVPNコンセントレーターの背後にある場合)、値を変更して、このLoggerに接続するための使用するIPアドレスに合わせます。
ローカルポート (Local Port)	ほとんどの場合、このフィールドの値は、このシステム (ピアを開始するマネージャーまたはLogger) にログインしたときのブラウザー内のポートと一致し、何か操作をする必要はありません。 ただし、ポートがIPアドレスのポートと一致しない場合は (たとえば、マネージャーまたはLoggerがVPNコンセントレーターの背後にある場合)、値を変更して、ブラウザーのIPアドレスのポートに合わせます。

3. [**保存 (Save)**] をクリックして新しいLoggerを追加するか、[**キャンセル (Cancel)**] をクリックして終了します。

ピアの削除

ピアを削除すると、2つのLoggerまたは2つのArcSightマネージャーの間、または1つのマネージャーと1つのLoggerとの間のピア関係も削除されます。この処理は、どちらのピア側からも実行できます。

ピアを削除するには

1. [**設定 | 詳細**] メニューを開き、[**ピアノード**] をクリックします。
2. ピア関係を削除するピアを探し、その行の [削除] アイコン (✖) をクリックします。
3. **[OK]** をクリックして削除を確認するか、**[キャンセル]** をクリックしてピアを保持します。

第6章: システム管理

システム管理ツールでは、ユーザーとユーザーグループの作成および管理、セキュリティ設定、SMTP、その他のシステム設定を実行できます。

注: システム管理トピックには、ソフトウェアLoggerに適用されるトピック、Loggerアプライアンスに適用されるトピック、両方のLoggerに適用されるトピックが含まれています。適用されるLoggerのタイプは、各システム管理トピックの最初に記載されています。

このセクションのトピックは次のとおりです。

システム

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[システム] タブから、システム固有の設定を設定できます。

システムロケール

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムロケール設定は、ユーザーインターフェイスに、日付、時刻、数値、メッセージなどの情報が、選択した国に適した形式と言語で表示されるようにします。

システムロケールは、Loggerのインストール手順の中で設定します。いったん設定したシステムロケールは変更できません。

システムロケールを表示するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[システム ロケール]** をクリックします。**[システム ロケール設定]** ダイアログボックスにロケールが表示されます。

システムの再起動

このトピックは、Loggerアプライアンスにのみ適用されます。

アプライアンスを再起動またはシャットダウンできます。ソフトウェアLoggerの関連情報については、「ソフトウェアLoggerのコマンドラインオプション」(557ページ)を参照してください。

システムを再起動またはシャットダウンするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[システム リブート]** をクリックします。
3. 以下のオプションから選択します。

ボタン	説明
リブート	システムは約60秒後に再起動します。 再起動処理には、一般に5～10分かかり、その間はシステムを使用できなくなります。
5分以内にリブート	システムは5分間の遅延後に再起動します。 再起動処理には、一般に5～10分かかり、その間はシステムを使用できなくなります。
シャットダウン	システムを自動的にシャットダウン(電源オフ)します。

上記の各アクションはキャンセルできます。[リブート]と[シャットダウン]では、**60秒**以内であればキャンセルできます。[5分以内にリブート]は、**300秒**以内であればキャンセルできます。

4. **[リブート]**、**[5分以内にリブート]**、または **[シャットダウン]** をクリックして選択したアクションを実行します。

注意: 再起動中は、Loggerがイベントを受信できなくなります。SmartConnectorを使用しない限り、Loggerの再起動中はイベントが失われます。SmartConnectorは、Loggerなどの通知先が一時的に使用不能な場合、イベントをキャッシュします。

ネットワーク

このトピックは、Loggerアプライアンスにのみ適用されます。

Loggerアプライアンスでは、**[ネットワーク]** メニューでDNS、ホスト、NIC、静的ルート、システム時刻を設定できます。ソフトウェアLoggerでは、この設定はオペレーティングシステムで行います。

システムDNS

このトピックは、Loggerアプライアンスにのみ適用されます。

[システムDNS] タブでは、DNS設定の編集や、DNS検索ドメインの追加を行うことができます。

DNS設定を変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックします。
3. **[システムDNS]** タブで、プライマリおよびセカンダリDNSサーバーのIPアドレスの新しい値を入力するか、検索ドメインのリストを編集します。

   新しいドメインを追加するには、⊞アイコンをクリックします。ドメインを削除するには、✖アイコンをクリックします。ドメインの検索順序を変更するには、ドメイン名を選択し、上下の矢印をクリックして、ドメインを目的の位置に移動します。
4. **[保存]** をクリックします。
5. **[ネットワークサービスを再起動]** をクリックして、変更内容を有効にします。

ホスト

このトピックは、Loggerアプライアンスにのみ適用されます。

[ホスト] タブでは、システムの/etc/hostsファイルを直接編集できます。**[システム ホスト]** テキストボックスにデータを入力するか、ローカルファイルからデータをインポートします。

ホスト情報を変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックし、**[ホスト]** タブをクリックします。
3. **[システム ホスト]** テキストボックスに、次の形式でホスト情報を入力します (1行に1ホスト)。

   <IPアドレス> <ホスト名1> <ホスト名2> <ホスト名3>

   ファイルから情報をインポートするには、**[ローカル ファイルからインポート]** をクリックし、システムへのアクセスに使用しているコンピューター上のテキストファイルを参照します。
4. **[保存]** をクリックします。

NIC

このトピックは、Loggerアプライアンスにのみ適用されます。

[NIC] タブでは、システム上のNIC (ネットワークインターフェイスカード) のIPアドレスを設定できます。また、システムのホスト名とデフォルトゲートウェイを設定できます。

NICを設定または設定変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックします。
3. **[NIC]** タブで、以下の設定を入力します。NICのIPアドレス、サブネットマスク、または速度/二重モードを編集するには、NICを選択し、[NIC 名] リストの上にある **[編集]** をクリックします。

設定	説明
デフォルトゲートウェイ	デフォルトゲートウェイのIPアドレス。
ホスト名	このシステムのネットワークホスト名。DNSが、指定したホスト名をシステムのIPアドレスに解決できることを確認してください。DNSがホスト名を解決できない場合、パフォーマンスに大きな影響があります。 この名前は、「CSR (証明書署名要求) の生成」(520ページ) で説明する証明書署名要求で指定したドメインと同じであることが必要です。 **注:** 以前自己署名証明書またはCA署名証明書をこのシステムで使用しており、ここでそのホスト名を変更しようとしている場合、新しい自己署名証明書またはCSRを生成し直す必要があります。新しい証明書によって、コネクターがFIPSモードでシステムと通信し、ホスト名を検証できるようになります。CSRの生成の詳細については、「CSR (証明書署名要求) の生成」(520ページ) を参照してください。
送信パケットを自動的にルーティングします (インターフェイス ホーミング)	このオプションを有効 (チェックボックスをオン) にすると、要求パケットが到着したのと同じシステムインターフェイス上で応答パケットが返送されます。このオプションを有効にすると、パフォーマンスが向上する可能性があります。システムからパケットを送出するために、デフォルトゲートウェイの情報と静的ルートを使用したルーティングの判断を行う必要がなくなるためです。静的ルートが設定されている場合、この機能を有効にすると静的ルートは無視されます。 この機能を無効 (チェックボックスをオフ) にすると、静的ルート (設定されている場合) を使用して、応答パケットを送信するために使用するインターフェイスが決定されます。 ネットワークインターフェイスを1つしか設定しない場合は、この設定を使用しても追加の利点はありません。

設定	説明
IPアドレス	システム内の各NIC (ネットワークインターフェイスカード) のIPアドレス。混乱を避け、受信者と転送者の間で負荷分散を可能にするには、これらのIPアドレスが個別のサブネット上にある必要があります。 **NICエイリアスの追加** 表示されているどのNICにもエイリアスを作成できます。そのためには、以下の手順を実行します。 a. エイリアスを作成するNICを強調表示します。 b. **[追加]** をクリックします。 c. エイリアス用に別のIPアドレスを作成します。 d. **[保存]** をクリックします。 オリジナルには、コロンと、特定のNICに対して作成したエイリアスの数を示す数字が追加されるので、エイリアスと区別できます。 **注:** IPエイリアスの速度を変更することはできません。 エイリアスは何個でも作成できます。
サブネット マスク	NICに入力したIPアドレスに対応するサブネットマスク。
速度/二重	速度と二重モードを選択するか、ネットワーク速度をシステムに自動判定させます。 • Auto (推奨) • 10 Mbps - 半二重 • 10 Mbps - 全二重 • 100 Mbps - 半二重 • 100 Mbps - 全二重 • 1 Gbps - 全二重

4. **[保存]** をクリックします。
5. **[ネットワーク サービスを再起動]** をクリックして、変更内容を有効にします。

静的ルート

このトピックは、Loggerアプライアンスにのみ適用されます。

システム上のNICに静的ルートを指定できます。

静的ルートを追加、編集、削除するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックします。
3. **[静的ルート]** タブで、以下の手順を実行します。

- 新しい静的ルートを追加するには、**[追加]** をクリックします。
- 既存のルートを編集または削除するには、まず経路を選択し、**[編集]** または **[削除]** をクリックします。

  静的ルートを追加または編集した場合は、以下の設定を設定する必要があります。

設定	説明
タイプ	静的ルートがネットワーク宛かホスト宛か
通知先	静的ルートの宛先のIPアドレス
サブネット マスク	宛先としてネットワークを指定した場合はサブネットマスク
ゲートウェイ	経路のゲートウェイのIPアドレス

4. **[保存]** をクリックします。

時刻/NTP

このトピックは、Loggerアプライアンスにのみ適用されます。

ソフトウェアLoggerでは、時刻、日付、タイムゾーンを設定する必要はありません。ソフトウェアLoggerは、オペレーティングシステムの時刻とタイムゾーンの設定を使用します。

[時間/NTP] タブでは、システム時刻、日付、ローカルタイムゾーン、NTPサーバーを設定できます。システム上の時刻と日付を手動で設定する代わりに、NTPサーバーを使用することを強くお勧めします。

正確で信頼できるログ管理には、イベントの正確なタイムスタンプもきわめて重要です。検索、レポート、スケジュールされたジョブなど、Loggerの操作に表示される時刻は、Loggerのローカルタイムゾーンの時刻です。

システム時刻、日付、タイムゾーンを手動で設定または変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックします。
3. [**時間/NTP**] タブで以下の設定を設定します。

設定	説明
現在のタイムゾーン	システムの場所に該当するタイムゾーン。この設定を変更するには、**[タイムゾーンの変更]** をクリックします。 ローカルタイムゾーンは、その地域のDST (サマータイム) 規則に従います。GMT (グリニッジ標準時刻) +および-タイムゾーンは、DSTに関知しません。 たとえば、米国/ロサンゼルスのタイムゾーンは、DSTが開始および終了する際に、GMTと比べて1時間違います。 • 太平洋標準時 (PST) = GMT-8 • 太平洋夏時間 (PDT) = GMT-7
現在の時刻	システムがある場所の現在の日付と時刻。この設定を変更するには、**[日付/時刻の変更...]** をクリックします。

4. タイムゾーンを変更すると、アプライアンスの再起動が必要になります。ただし、現在時刻の変更はすぐに有効になります。

> **注意:** 日付と時刻を手動で設定し、NTPサービスも使用している場合、手動で入力する日付と時刻は、NTPサーバーから渡される日付と時刻よりも16分以上進んでいたり遅れていたりしてはなりません。手動で入力した時刻がNTPサーバーの時刻と16分以上違う場合、NTPサービスが起動に失敗します。

システムをNTPサーバーとして設定するか、システムでNTPサーバーを使用するように設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[ネットワーク]** をクリックします。
3. **[時間/NTP]** タブをクリックします。
4. **[NTP サーバ]** で以下の設定を行います。

   新しいNTPサーバーを追加するには、⊞アイコンをクリックします。サーバーを削除するには、✖アイコンをクリックします。NTPサーバーを使用する順序を変更するには、サーバーを選択し、NTPサーバーが目的の位置にくるまで上下矢印をクリックします。

設定	説明
NTP サーバとして有効にする	このシステムをNTPサーバーとして使用する場合はこの設定をオンにします。
NTP サーバ	NTPサーバーのホスト名を入力します。たとえば、time.nist.govと入力します。 システムの時刻が正確になるように、2台以上のNTPサーバーを使用することをお勧めします。複数のNTPサーバーを入力するには、1行に1つのサーバー名を入力します。 このリストにサーバーを追加したら、**[Click to Test]** リンクをクリックして、追加したサーバーにシステムから到達できることを確認できます。 • ArcSightシステムは、他のArcSightシステムに対するNTPサーバーとしての役割を果たすことができます。 • システムAがシステムBに対するNTPサーバーとして機能する場合、システムBでは、システムAが [NTP サーバ] リストに記載されている必要があります。 • **[テスト サーバ]** ボタンを使用すると、**[NTP サーバ]** ボックスに入力したサーバーのステータスを確認できます。

5. **[保存]** をクリックします。

   ヒント: [保存] ボタンと **[NTP サービスを再起動]** ボタンを表示するには、下にスクロールすることが必要な場合があります。

6. **[NTP サービスを再起動]** をクリックして、変更内容を有効にします。

サマータイムの変更がLoggerの処理に与える影響

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

サマータイム (DST) は秋に終了しますが、DSTの終了に伴って時刻が変更される (1時間戻ります) 午前1時から2時の間に発生したイベントを検索する場合、開始時刻に12:59:59以前、または終了時刻に2:00:01以降を指定すると、必要なイベントをすべて取得できます。

DSTは春に開始しますが、DSTの開始に伴って時刻が変更される (1時間進みます) 午前1時から2時の間に発生したイベントを検索する場合、終了時刻に2:00:01以降を指定すると、必要なイベントをすべて取得できます。

レポート、イベントアーカイブ、ファイル転送などの、Logger上のスケジュールされた処理も、米国のDST (サマータイム) 期間の開始時と終了時にLogger上のシステム時刻が調整されると、影響を受けます。

DSTの開始時 (たとえば、2015年3月9日) に失われる時間にスケジュールされた処理は、時刻調整の日に実行されません。同様に、DSTの終了時 (たとえば、2015年11月2日) に増える時間にスケジュールされた処理は、DSTの時刻ではなく標準時刻に実行されます。

例

- 2015年11月2日の午前1時DSTに実行されるようにスケジュールされたレポートは、標準時の午前1時に実行されます。これは、その日のDST時刻よりも1時間遅い時刻です。
- 2015年11月2日の午前2時に実行するようにスケジュールされたレポートは午前2時に実行されますが、時刻調整のため、前日 (2015年11月1日) に実行された時刻よりも1時間遅くなります。
- 2015年3月9日の午前2時に実行されるようにスケジュールされたレポートは実行されません。

SMTP

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムは、SMTP (Simple Mail Transfer Protocol) 設定を使用して、アラートやパスワードリセットのメールなど、メール通知を送信します。

SMTPの設定を追加または変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[SMTP]** をクリックし、以下の設定の値を入力します。

設定	説明
プライマリSMTP サーバ	送信メールを処理するSMTPサーバーのIPアドレスまたはホスト名。
バックアップSMTP サーバ	プライマリSMTPサーバーが使用不能な場合に送信メールを処理するSMTPサーバーのIPアドレスまたはホスト名。
送信 メールアドレス	送信メールの「From:」フィールドに表示されるメールアドレス。

3. **[保存]** をクリックします。

注: 各レポートは、必ず同じSMTP設定を使用するように設定してください。「レポートサーバーの設定」(305ページ) の説明を参照してください。

ライセンスと更新

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

このページには、ライセンス情報、コンポーネントのバージョン、最後のLoggerのリブート (Loggerアプライアンス) または再起動 (ソフトウェアLogger) からの経過時間が表示されます。

このページでは、新しいライセンスをLoggerに適用することができます。また、Loggerアプライアンスの更新も実行できます。ただし、ソフトウェアLoggerのアップグレードにはアップグレードパッケージのインストールが必要です。アップグレードバージョンの手順については、リリースノートを参照してください。

現在のライセンスの詳細を表示するには、上部のメニューバーから **[設定]** を開き、**[ライセンス情報]** をクリックします。詳細については、「ライセンス情報」(478ページ) を参照してください。

Loggerライセンスの更新

Loggerライセンスを更新するには

1. HPEソフトウェア資格ポータルでライセンスを取得し、Loggerに接続可能なコンピューターにライセンスファイルをダウンロードします。詳細については、HPEから配信されるソフトウェア配布確認メールを参照してください。
2. 更新ファイルをダウンロードしたコンピューターから、管理者 (アップグレード) 権限を持っているアカウントを使用して、Loggerにログインします。
3. 上部のメニューバーから **[システム管理]** をクリックします。
4. **[システム]** セクションの **[ライセンスおよび更新]** をクリックします。
5. ダウンロードしたライセンスファイルを参照し、**[更新のアップロード]** をクリックします。[更新中] ページに更新の進行状況が表示されます。

更新が完了すると、**[更新結果]** ページに更新結果 (成功/失敗) が表示されます。リブートや再起動は必要ありません。

新しいライセンスを適用した後、ストレージボリュームの追加が必要になることがあります。手順については、「ストレージボリュームサイズの増加」(457ページ) を参照してください。

注: アップグレードの完了後や、試用版のLoggerをフル機能バージョンに切り替えた後は、ライセンス供与された機能をすべて活用できるように、ストレージボリュームを追加してください。

Loggerアプライアンスのアップグレード

Loggerアプライアンスをアップグレードするには

1. HPEソフトウェア資格ポータルから更新ファイルを取得し、Loggerに接続可能なコンピューターにダウンロードします。詳細については、HPEから配信されるソフトウェア配布確認メールを参照してください。
2. 更新ファイルをダウンロードしたコンピューターから、管理者 (アップグレード) 権限を持っているアカウントを使用して、Loggerにログインします。
3. 上部のメニューバーから **[システム管理]** をクリックします。
4. **[システム]** セクションの **[ライセンスおよび更新]** をクリックします。
5. **[ブラウズ]** をクリックしてファイルを探します。
6. **[更新のアップロード]** をクリックします。**[更新中]** ページに更新の進行状況が表示されます。
7. 更新が完了すると、[更新結果] ページに更新結果 (成功/失敗) と、再起動が必要かどうかが表示されます。必要に応じて、Loggerは自動的にリブートまたは再起動を実行します。

プロセスステータス

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[プロセス ステータス] ページには、システムに関連するすべてのプロセスの一覧が表示され、それらのプロセスの詳細を表示したり、プロセスを開始、停止、再起動できます。

重要: serversプロセスを停止しないことをお勧めします。

- ソフトウェアLoggerをシャットダウンするには、`loggerd stop`コマンドまたは`quit`コマンドを使用します。詳細については、「ソフトウェアLoggerのコマンドラインオプション」(557ページ)を参照してください。
- Loggerアプライアンスをシャットダウンするには、UIの [シャットダウン] を実行します。詳細については、「システムの再起動」(492ページ)を参照してください。

イベントの受信中、Logger **servers**プロセスを停止しないでください。データ損失の原因になります。**servers**プロセスの停止が必要な場合には、**receivers**プロセスを停止してから、**servers**プロセスを停止してください。

[プロセス ステータス] ページを表示するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションで **[プロセス ステータス]** をクリックしますLoggerプロセスのリストが表示

されます。

ヒント: [プロセス] テーブルの「processors」とは、転送者を意味します。

3. **[プロセス ステータス]** ダイアログで、プロセスの詳細表示を切り替えるには、プロセス名の左にあるアイコンをクリックします。

プロセスを開始、停止、再起動するには、プロセスを選択して、プロセスリストの上部にある **[開始]**、**[停止]**、または **[再起動]** をクリックします。

システム設定

このトピックは、ソフトウェアLoggerにのみ適用されます。

インストール手順の中で、Loggerをサービスとして起動することを選択しなかった場合は、**[システム設定]** ページを使用してこの設定を行うことができます。このオプションを選択すると、Loggerは、実行レベル2、3、4、5で実行される、`arcsight_logger`という名前のサービスを使用します。

サービスとして起動されるようにLoggerを設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルで **[システム設定]** をクリックします。
3. **[サービス設定]** の下で、以下の適切なオプションを選択します。
   - **サービスとして開始**
   - **サービスとして開始しないでください**
4. **[保存]** をクリックします。

SNMP

このトピックは、Loggerアプライアンスにのみ適用されます。

アプライアンスのヘルス監視には、SNMP (Simple Network Management Protocol) を使用できます。Loggerアプライアンスは、SNMP v2cとSNMP v3をサポートします。

SNMPポーリングと通知 (トラップ) を設定できます。

- SNMPポーリングを設定すると、マネージャーステーションから、Logger上のSNMPエージェントに対してクエリを実行できます。クエリでは、ハードウェアレベルとオペレーティングシステムレベルの詳細な情報が取得されます。
- SNMP通知先を設定すると、Loggerは以下に示すイベントに関する通知を送信できます。この通知は、アラートが送信する通知とは異なります(アラートを使用してイベント情報をSNMP通知として送信する方法については、「リアルタイムアラート」(408ページ) および 「SNMP通知先」(417ページ) を参照してください)。この新しい通知は、標準的なイベント

通知ではなく、単一のイベントに関する具体的な内容を通知するものであり、HP NMMiなどのネットワーク管理システム(NMS)によって簡単に解釈できます。

サポートされているSNMP指標

ハードウェア

Loggerは、次のハードウェアパラメーターのポーリングと通知をサポートします。

- CPU Usage
- Memory Usage
- Disk Almost Full
- Fan Failure
- Power Supply Failure
- Temperature Out of Range
- Ethernet Link Down

Loggerアプリケーション

次の通知は、`ARCSIGHT-EVENT-MIB`で定義されています。

- Login attempt failed
- Password change attempt failed
- User account locked
- Reboot command launched
- Manual backup failed
- Scheduled backup failed
- Enable FIPS mode successful
- Disable FIPS mode successful
- Enable FIPS mode failed
- Disable FIPS mode failed

Loggerアプライアンスでの設定

SNMPポーリングを設定するには

1. メインメニューバーで **[システム管理]** をクリックします。
2. ナビゲーションツリーの **[システム]** の下で、**[SNMP]** をクリックします。SNMPポーリングの設定タブが開きます。
3. **ステータス**: **[有効]** または **[無効]** を選択します。

4. **ポート**: ポート番号を入力します。デフォルトは161 (UDP) ですが、使用可能なポートを指定できます。
5. **SNMPバージョン**: **[V2c]** または **[V3]** を選択します。デフォルトは [V2c] です。
   - **V2c** - 次の値を入力します。
     コミュニティ文字列: 6～128個の英数字、下線 (_)、ダッシュ (-)。
   - **V3** - 次のフィールドに値を入力します。
     ユーザー名: 4～16個の英数字を小文字で指定します。ユーザー名の先頭にはアルファベットを指定してください。下線を含めることができます。
     認証プロトコル: **[MD5]** または **[SHA]** を選択します。
     認証パスフレーズ: 4～256文字のパスワードを入力します。
     プライバシープロトコル: **[DES]** または **[AES128]** を選択します。
     プライバシーパスフレーズ: 4～256文字のパスワードを入力します。

     注: 有効な設定を行うには、ポーリング設定とトラップ設定で同じ値を指定してください。
6. **システム名**: ポーリングを行うシステムの名前を入力します。
7. **接点**: 有効な通知先を入力します。
8. **ロケーション**: ポーリングを行うシステムの場所を入力します。
9. **[保存]** をクリックします。
10. SNMPポートを開く設定をファイアウォールで行います。詳細については、「ファイアウォールルール」(558ページ) を参照してください。

SNMP通知先が設定されている場合、Loggerは所定のイベントセットの通知を送信できます (「サポートされているSNMP指標」(504ページ) を参照してください)。

SNMP通知は、SmartConnectorが送信する標準的なArcSightイベント通知とは異なります。単一イベントに関する具体的な内容なので、HP NMMiなどのネットワーク管理システムが解釈しやすい通知となっています。

SNMP通知の送信先を設定するには

1. メインメニューバーで **[システム管理]** をクリックします。
2. ナビゲーションツリーの **[システム]** の下で、**[SNMP]** をクリックします。SNMPポーリングの設定タブが開きます。
3. **[SNMP 通知先]** タブを選択し、SNMPトラップ設定メニューを開きます。
4. **ステータス**: **[有効]** または **[無効]** を選択します。
5. **NMS IPアドレス**: ネットワーク管理システム (NMS) ホストのIPアドレスを入力します。
6. **ポート**: ポート番号を入力します。デフォルトは162 (UDP) ですが、使用可能なポートを指定できます。

7. **SNMPバージョン**: **[V2c]** または **[V3]** を選択します。デフォルトは [V2c] です。
   - **V2c** - 次の値を入力します。
     コミュニティ文字列: 6～128個の英数字、下線 (_)、ダッシュ (-)。
   - **V3** - 次のフィールドに値を入力します。
     ユーザー名: 4～16個の英数字を小文字で指定します。ユーザー名の先頭にはアルファベットを指定してください。下線を含めることができます。
     認証プロトコル: **[MD5]** または **[SHA]** を選択します。
     認証パスフレーズ: 4～256文字のパスワードを入力します。
     プライバシープロトコル: **[DES]** または **[AES128]** を選択します。
     プライバシーパスフレーズ: 4～256文字のパスワードを入力します。

     注: 有効な設定を行うには、ポーリング設定とトラップ設定で同じ値を指定してください。
8. **[保存]** をクリックします。

NMSでの設定

1. ArcSight MIBファイルとその他の標準Net-SNMP MIBファイルを、次のURLからダウンロードします。
   - `https://<system_name_or_ip>/platform-service/ARCSIGHT-EVENT-MIB.txt`
   - `https://<system_name_or_ip>/platform-service/DISMAN-EVENT-MIB.txt`
   - `https://<system_name_or_ip>/platform-service/HOST-RESOURCES-MIB.txt`
   - `https://<system_name_or_ip>/platform-service/IF-MIB.txt`
   - `https://<system_name_or_ip>/platform-service/UCD-SNMP-MIB.txt`
2. MIBをロードします。
3. 使用するプロトコル (v2cまたはv3) に基づいて、ノード (アプライアンス) をNMS (またはMIBブラウザー) で設定します。

MIBの内容

標準的なMIBファイルには、次のタイプの通知が含まれています。

モジュール	通知タイプ
DISMAN-EVENT-MIB	標準ネットワーク管理に適用されるイベントトリガーとアクション。
IF-MIB	ネットワークインターフェイスのオブジェクト。
IP-MIB	IPとICMPの実装。
HOST-RESOURCES-MIB	標準ハードウェアパラメーター。

アプライアンスへのSSHアクセス

このトピックは、Loggerアプライアンスにのみ適用されます。

注: ソフトウェアLoggerへのSSHアクセスは、オペレーティングシステムによって制御されます。

問題をカスタマーサポートに連絡し、カスタマーサポートがユーザーのアプライアンスにアクセスしてトラブルシューティングや診断を行う必要がある場合 (アップグレードの失敗、アプライアンスの無応答など)、アプライアンスへのSSHアクセスを有効にするよう指示されます。

デフォルトでは、アプライアンスへのSSHアクセス (以前のリリースではサポートログインと呼ばれていました) は無効になっています (これには、以前のバージョンからバージョン6.0にアップグレードしたLoggerも含まれます)。しかし、アプライアンスのユーザーインターフェイスで以下のオプションのいずれかを選択して、SSHを有効にすることができます。

- **有効:** SSHアクセスは常に有効です。
- **8時間のみ有効:** SSHアクセスは、有効にしてから8時間後に自動的に無効になります。
- **起動/リブート時のみ有効:** SSHアクセスは、アプライアンスが再起動している間だけ有効になります。アプライアンス上のすべてのプロセスが起動されると無効になります。このオプションは、アプライアンスが再起動後に正常に起動しないといった状況で、最低限の期間のSSHアクセスを可能にします。

  セキュリティを最適化するために、rootアカウントに強力なパスワードを設定することをお勧めします。また、SSHアクセスは無効のままにし、トラブルシューティング目的など、必要な場合にのみ有効にしてください。

  注: アプライアンスでSSHが無効になっている場合でも、HP ProLiant Integrated Lights-Out (iLO) Advancedリモート管理カードを使用してリモートアクセス用にコンソールが設定されていれば、コンソールにアクセスできます。詳細については、『Loggerインストールガイド』を参照してください。

SSHアクセスの有効化と無効化

SSHアクセスを有効または無効にするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[システム]** セクションの **[SSH]** をクリックします。
3. [SSH 設定] ダイアログボックスが開いたら、SSH設定を選択します。
4. 確認すると、新しいSSH設定が有効になります。

アプライアンスでSSHアクセスを有効にした後、SSHを使用してアプライアンスに接続するには、以下の手順に従います。

SSHを使用したアプライアンスへの接続

SSHを使用したアプライアンスに接続するには

1. SSHクライアントを使用し、「root」としてアプライアンスに接続します。
2. パスワードプロンプトでパスワードを入力し、**Enter**キーを押します。

ログ

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムは、アプリケーションレベルとプラットフォームレベルで監査ログを生成できます。監査ログを検索するには [ログ] サブメニューを使用します。

監査ログ

システムの監査ログを表示できます。監査ログは、CEF (共通イベントフォーマット) の監査イベントとしてArcSight ESMに直接送信し、分析と関連付けを行うことができます。監査イベントの転送については、「監査転送」(508ページ)を参照してください。

監査ログを表示するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ログ]** セクションの **[監査ログ]** をクリックします。
3. ログを取得する日付と時刻の範囲を選択します。
4. (オプション) 監査ログの検索を絞り込むには、**[説明]** フィールドに文字列を指定し、**[ユーザ]** フィールドにユーザー名を指定します。説明文字列を指定した場合、[説明] フィールドにその文字列が含まれるログのみが表示されます。同様に、ユーザーを指定した場合、[ユーザ] フィールドにそのユーザー名が含まれるログのみが表示されます。
5. **[検索]** をクリックします。

監査転送

監査イベントをArcSight ESMに転送して、関連付けと分析を行うことができます。転送可能な監査イベントの一覧については、「アプリケーションイベント」(619ページ)を参照してください。

監査イベントを特定のESM通知先に転送するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ログ]** セクションの **[監査の転送]** をクリックします。
3. **[利用可能な通知先]** リストから通知先を選択し、右矢印アイコン () をクリックして、選択した通知先を **[通知先を選択]** リストに移動します。

   一度に複数の通知先を選択して移動したり、  アイコンをクリックして使用可能なすべての通知先を移動できます。

   通知先は、[ESM 通知先] ページ (**[設定]** > **[データ]** > **[ESM 通知先]**) で設定するESM通知先です。
4. **[Save Settings]** をクリックします。

ストレージ

このトピックは、Loggerアプライアンスにのみ適用されます。

[ストレージ] サブメニューは、NFSマウントやCIFSマウント、またはSAN (該当する場合) を追加、およびハードディスクアレイ (RAID) コントローラーと特定のシステムプロセスのステータスを表示するために使用します。

リモートファイルシステム

このトピックは、Loggerアプライアンスにのみ適用されます。

システムは、NFS (Network File System) およびCIFS (Windows) 共有をマウントできます。これにより、UNIX、Linux、Windowsのリモートホストや、これらのオペレーティングシステムに基づく任意のNAS (Network Attached Storage) ソリューションからログファイルとイベントデータを読み込むことができます。また、NFSおよびCIFSマウントを、イベント、エクスポートされたフィルターとアラート、保存された検索などのデータをアーカイブするために使用できます。SAN (Storage Area Network) 機能を備えたLoggerは、SANと通信することもできます。

LoggerアプライアンスはNFSv4をサポートします。ただし、Loggerイベントのプライマリストレージに NFSを使用することはお勧めしません。CIFS共有をプライマリストレージとして使用することはサポートされていません。

リモートファイルシステムの管理

このトピックは、Loggerアプライアンスにのみ適用されます。

共有をマウントする前に、以下の要件が満たされていることを確認してください。

ファイルシステムタイプ	要件
CIFS (Windows)	• 共有ドライブにアクセス可能なユーザーアカウントがWindowsシステムに存在すること。 • マウントポイントを確立しようとしているフォルダーが共有用に設定されていること。
NFS	• NFSシステム上で、ArcSightシステムに読み書きが許可されていること。 • マウントに使用するアカウントが、uidとして数値ID 1500、gidとして750を使用していること。

リモートファイルシステムマウントを追加するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ストレージ]** セクションにある **[リモート ファイル システム]** をクリックします。 **[リモート ファイル システム]** 表が表示されます。
3. ページ左上の **[追加]** をクリックし、表示されるフォームの以下のフィールドに値を入力します。

パラメーター	説明
ファイルシステムタイプの選択	NFSとCIFSのどちらの共有をマウントするのか。
NFSの設定	
名前	マウントポイントの意味のある名前。この名前は、システム上でマウントポイントを参照するためにローカルに使用され、共有上に保存されるデータのアーカイブ設定を設定するときに指定する必要があります。 **ヒント:** マウント名にスペースを含めることはできません。
ホスト名/IPアドレス	マウントを作成するホストの名前またはIPアドレス。
リモートパス (NFS用)	ネットワークファイルシステムマウントのルートとなる、リモートホスト上のフォルダー。たとえば/public/system_logsを指定します。 このフィールドに指定する場所に書き込むことができるのがこのシステムのみであることを確認してください。複数のシステム (または他のシステム) がこの場所をマウントして書き込むと、この場所のデータが破壊されます。

パラメーター	説明
マウントオプション	AutoFSオプション。たとえば、リモートホストから読み取り専用である場合はro、読み書きの場合はrw、リモートホストが応答するまで再試行し続ける場合はhardを指定します。 **注:** マウントポイントでrw許可を設定しても、ホストが読み取り専用アクセスを許可するように設定されている場合は、リモートホストに読み書きアクセスは許可されません。
説明	マウントポイントの意味のある説明。
CIFSの設定	
名前	名前は、システム上でマウントポイントを参照するためにローカルに使用され、共有上に保存されるデータのアーカイブ設定を設定するときに指定する必要があります。 **注:** マウント名には、英数字、ダッシュ(-)、下線(_)を指定できます。先頭には、英数字を指定してください。
場所	以下のいずれかの方法で共有名を入力します。 • 次の形式の共有名: <IPアドレス>または<ホスト名>:<共有名> 例: 198.0.2.160:myshare このフォルダーは、共有用に設定されている必要があります(一般に、Windowsフォルダーで共有を設定するには、フォルダー名を右クリックし、**[プロパティ] > [共有]**を選択します)。 **注意:** クラスター内のWindows Server 2008からマウントする場合には、IPアドレス**ではなく**ホスト名を使用しないと正常にマウントできません。 • UNCパス: 例: //198.0.2.160/myshare
マウントオプション	AutoFSオプション。たとえば、リモートホストから読み取り専用である場合はro、読み書きの場合はrw、リモートホストが応答するまで再試行し続ける場合はhardを指定します。 **注:** マウントポイントでrw許可を設定しても、ホストが読み取り専用アクセスを許可するように設定されている場合は、リモートホストに読み書きアクセスは許可されません。
説明	マウントポイントの意味のある説明。

パラメーター	説明
CIFSの認証情報	
ユーザー名	Windows共有への読み書き権限を持つユーザーアカウントの名前。 ユーザー名の前には、必ずドメイン情報を追加してください。例: `tahoe\arcsight`
パスワード	上記で指定したユーザー名のパスワード。

4. **[追加]** をクリックします。
   すべてのマウントポイントは`/opt/mnt`の下に作成されます。

リモートファイルシステムマウントを編集するには

注: 使用中のマウントポイントは編集できません。**[編集]** リンクは、マウントポイントを編集できる場合のみ表示されます。

マウントポイントの名前を変更した場合、マウントポイント名を元の名前に戻すまで、元の名前を使用して作成されたアーカイブへのアクセスはできなくなります。

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ストレージ]** セクションにある **[リモート ファイル システム]** をクリックします。
3. 編集するマウントポイントを選択し、ページの左上から **[編集]** をクリックします。
4. フィールドの値を変更します。
5. **[保存]** をクリックします。

リモートファイルシステムマウントを削除するには

注: 使用中のマウントポイントは削除できません。**[削除]** リンクは、マウントポイントを削除できる場合のみ表示されます。

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ストレージ]** セクションにある **[リモート ファイル システム]** をクリックします。
3. 削除するマウントポイントを選択し、ページの左上にある **[削除]** をクリックします。

SAN

このトピックは、Loggerアプライアンスにのみ適用されます。

Loggerアプライアンスの一部のモデルには、SAN (Storage Area Network) に接続するための機能が搭載されています。SANには、ワールドワイド名で識別されるLUN (Logical Unit) が含まれています。

LUNの管理

このトピックは、Loggerアプライアンスにのみ適用されます。

LUNの状態は、「available」、「attached」、「detached」のいずれかです。状態に応じて、Loggerで実行可能なアクションが決まります。

次の表に、LUNの状態と実行可能なアクションの要約を示します。

接続ステータス	アクション	説明
available	添付	SAN上で検出されたLUNは、初期状態では接続可能です。
attached	切り離し	接続されているLUNは、Loggerによってアクセスできます。 **「切り離し」**アクションを実行できるのは、ストレージボリュームがLUNで設定されていない場合のみです。ストレージボリュームの設定後は、「工場出荷時設定の復元」(694ページ)の手順でファクトリーリセットを行わない限り、LUNの**「切り離し」**は実行できません。
detached	再添付 破棄	接続済みLUNが切断されても、そのデータは保持されますが、Loggerによってアクセスできなくなります。再度使用可能にするには、**「再添付」**アクションを使用します。**「破棄」**アクションはLUNを**「available」**状態に戻します。 切断した場合、すぐに使用できる唯一のアクションは**「再添付」**です。**「破棄」**状態が表示されるまでには数分かかります。LUNがシステム上で切断されるまでに数分かかるためです。 LUNを破棄すると、そのLUNは、以降の接続によってLUNに格納されているすべてのデータが消去される状態になります。LUNが誤って破棄された場合、それ以降LUNの接続を試みていなければ、カスタマーサポートがデータを復元できる可能性があります。

Loggerは、1次ストレージ用には、同時には1つのLUNのみに接続できます。イベントアーカイブ、設定バックアップ、エクスポート用に、追加のLUNを接続することができます。

L7500-SANには2つのHBAがあります。1つをマルチパス、もう1つをイベントアーカイブ、バックアップ設定、エクスポートに使用することができます。マルチパス機構については、「LUNへの複数のパスの作成」(515ページ)を参照してください。

LUNに接続するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの [**ストレージ**] セクションにある **[SAN]** をクリックします。
3. **[SAN 設定]** の中の [LUN 名リスト] の中からLUNを探して選択します。
4. [SAN 設定] ページの左上にある **[添付]** をクリックします。**[添付]** メニューオプションが表示されない場合は、現在Loggerに接続できるLUNがありません。

   注: LUNを接続できるのは、LUNが「Available」状態の場合のみです。

   LUNの接続状態は、LUNが使用可能な状態になると「Attached」に変わります。

LUNを切断するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの [ストレージ] セクションにある **[SAN]** をクリックします。
3. [LUN 名リスト] で、切断するLUNを探します。
4. [SAN 設定] ページの左上にある **[切り離し]** をクリックします。[切り離し] メニューオプションが表示されない場合は、現在Loggerから切断できるLUNがありません。

   注: LUNでストレージボリュームが設定されている場合、LUNを切り離すことはできません。

LUNに再接続するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの [ストレージ] セクションにある **[SAN]** をクリックします。
3. [LUN 名リスト] で、再接続するLUNを探します。LUNは**Detached**状態になっている必要があります。
4. [SAN 設定] ページの左上から **[再添付]** をクリックします。

   [再添付] メニューオプションが表示されない場合は、現在Loggerに再接続できるLUNがありません。

LUNを破棄するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの [ストレージ] セクションにある **[SAN]** をクリックします。
3. [LUN 名リスト] で、破棄するLUNを探します。LUNはdetached状態になっている必要があります。
4. [SAN 設定] ページの左上にある **[破棄]** をクリックします。

> **注意:** 切断されているLUN (Logical Unit) を破棄すると、そのLUNは、以降の接続によってLUNに格納されているすべてのデータが消去される状態になります。LUNが誤って破棄された場合、それ以降LUNの接続を試みていなければ、カスタマーサポートがデータを復元できる可能性があります。

SANのリストア

このトピックは、Loggerアプライアンスにのみ適用されます。

SANは、以前接続されていたLoggerか、新しいLoggerにリストアできます (ディザスターリカバリの場合)。

SANをリストアするには

1. Loggerの電源がオフになっている状態で、SANを物理的に接続します。
2. Loggerの電源をオンにします。
3. 設定をLoggerにリストアします。リストア目的でバックアップファイルが利用できるように、設定を定期的にバックアップすることをお勧めします。バックアップファイルが利用できない場合は、このステップをスキップし、SANをリストアした後で、手動で受信者、転送者、ユーザーなどを追加します。詳細については、「設定のバックアップとリストア」(468ページ) を参照してください。
4. LoggerへのSSHアクセスを有効にします (「アプライアンスへのSSHアクセス」(507ページ) を参照)。
5. カスタマーサポート (https://softwaresupport.hpe.com/) に連絡します。
6. カスタマーサポートは、リモートでログインし、すべてのLoggerプロセスを停止し、内部データベースをSANに移行します。
7. カスタマーサポートの作業が終了したら、Loggerを再起動します。

LUNへの複数のパスの作成

このトピックは、Loggerアプライアンスにのみ適用されます。

Logger上のHBAカードには2個のポートがあります。両方のポートを同じLUNに接続できます。それらのポートを使用して、LoggerとLUNの間に2つの異なるパスを作成することで (マル

チパス機構)、LUNが使用不能になる単一障害点をなくすことができます。

注: マルチパス機構をサポートしているどのSANベンダーの製品もLoggerで使用できますが、ArcSightは、特にHPE 3PAR SANでテストされています。

Loggerには、出発点としてデフォルトのマルチパス設定が用意されています。ただし、ユーザーの環境固有の情報については、必ず使用しているSANのマニュアルを参照してください。

マルチパスユーザーインターフェイス(UI)は、SANをサポートするLoggerモデルでデフォルトで使用できます。ただし、マルチパス機構を使用するには、LUNを両方のHBAポートに接続し、マルチパス設定をUIで設定する必要があります。Loggerでいったん有効にした**マルチパスは無効にできません**。

異なるSAN上の2つの異なるLUNに接続する場合は、重複するパスがないため、マルチパスを有効にする必要はありません。同じSAN上の2つの異なるLUNに接続する場合や、同じLUNに2つ接続する場合は、マルチパス機構を設定する必要があります。そうしないと、OSは同じLUNへの重複するパスを検出し、どちらのパスを使用すべきかを解決できません。

Loggerの新規インストールでマルチパスを有効にするには、LUNを接続する前にマルチパス機構を設定してください。

マルチパスの有効化

マルチパスを有効にするには

1. LUNがLoggerに接続されて**いない**ことを確認します(「SAN」(512ページ)を参照)。
2. 上部のメニューバーから **[システム管理]** をクリックします。
3. 左パネルの **[ストレージ]** セクションにある **[マルチパス]** をクリックします。
4. ドロップダウンメニューから [SAN マルチパス設定] を選択します。
5. **[カスタム]** を選択するか、表示されている設定が要件を満たしていない場合は、パラメーターをカスタマイズします。
6. **[テスト]** をクリックして、選択した設定または行った変更が正しいことを確認します。

   テストに失敗する場合は、さらに変更を加えるか、**[リセット]** をクリックして最初からやり直します。
7. **[保存]** をクリックします。

アプライアンスへのマルチパスSAN接続を設定したら、再起動時に`multipathd`サービスが起動される設定になっていることを確認する必要があります。

multipathdサービスがブート時に起動するよう設定されていることを確認するには

1. `chkconfig --list multipathd`を実行します。

   目的の実行レベルに「`#:on`」が表示されることを確認します。現在の実行レベルは、「`runlevel`」コマンドで表示できます。

2. サービスが有効になっていない場合は、次のようにして有効にします。
   `chkconfig multipathd on`
3. アプライアンスを再起動するか、次のようにしてマルチパスデーモンを起動します。
   `/sbin/service multipathd start`

   注: ベンダー固有のマルチパス設定も、`/etc/multipath.conf`ファイルで必ず適切に設定してください。

シングルパスLUNをマルチパスに変換するには

シングルパスLUNをマルチパスに変換するには

1. SSHを使用してLoggerに接続します (「アプライアンスへのSSHアクセス」(507ページ) を参照)。
2. 以下のコマンドを実行します。

   ```
   cd /opt/arcsight/aps/mpath

   ./mpath_prepare.sh
   ```

3. 第2ファイバーケーブルをHBAカードの第2ポートに接続します。
4. SAN向けの`multipath.conf`ファイルを作成します。

   このファイルの内容は、SANのベンダーおよび設定によって異なります。Loggerのユーザーインターフェイスには、EMC CLARiiON SANのマルチパス設定がデフォルトで含まれます。この設定は、`multipath.conf`ファイルに情報を入力するときに参照できます。ただし、お客様のセットアップおよび環境に固有の情報については、お使いのSANのマニュアルを参照してください。

   EMC CLARiiON SANのマルチパスのデフォルト設定を表示するには、Logger UIに接続して、[システム管理] > [マルチパス] にアクセスします。次に、UIから設定をコピーして、`/opt/arcsight/aps/mpath/multipath.conf`ファイルにコピーした設定を貼り付けます。
5. 次のテストコマンドを実行します。

   ```
   ./mpath_test.sh <path_to_your_multipath.conf >
   ```

   テストコマンドの出力を表示して、作成予定のマルチパスデバイスが出力の最後に表示されていることを確認します。
6. テスト出力の内容が正しくない場合は、マルチパスデバイスが正しく表示されるまで、手順「SAN向けのmultipath.confファイルを作成します。」(517ページ) と「次のテストコマンドを実行します。」(517ページ) を繰り返します。
7. 次のコマンドを実行します。

   ```
   ./mpath_enable.sh <path_to_your_multipath.conf >
   ```

8. アプライアンスをリブートします。

RAIDコントローラー/ハードディスクのSMARTデータ

このトピックは、Loggerアプライアンスにのみ適用されます。

RAIDコントローラーに関する情報またはハードディスクのSMARTデータを、[General Controller Information] 画面で確認できます。この情報は、通常のシステム運用では不要ですが、特定のハードウェアの問題を診断する際に役立つ可能性があります。RAIDストレージは、その性質上冗長であるため、単一のドライブ障害が起きてもシステムが使用不能になりません。代わりにパフォーマンスが低下します。このレポートを使用して、パフォーマンスの問題がディスク障害によって引き起こされているかどうかを判断してください。カスタマーサポートも問題を診断するためにこの情報を使用することがあります。

[General Controller Information] 画面を表示するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ストレージ]** セクションにある **[RAID コントローラ]** をクリックします。
3. 表示される情報は、システムのハードウェアモデルによって変わります。矢印をクリックして表示される情報を切り替えます。

セキュリティ

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

セキュリティ設定では、SSLサーバー証明書の設定、システム上のFIPS (Federal Information Processing Standards) モードの有効化と無効化、クライアント証明書とCAC (Common Access Card) サポートのためのSSLクライアント認証の設定を行うことができます。

ヒント: ユーザーDNを作成するための手順については、「ユーザーの作成とアクティブ化」(542ページ)と、パラメーター表の「クライアント DN を使用」を参照してください。

SSLサーバー証明書

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

SmartMessagingテクノロジーや他のArcSightシステムを使用する際、SmartConnectorなどのクライアントと暗号化されたチャネル上で安全に通信するために、SSL (Secure Sockets

Layer) テクノロジーが使用されます。システムには自己署名証明書が付属しており、アプライアンスを初めて使用するときにSSLセッションを確立できるようになっています。このオプションの詳細については、「自己署名証明書の生成」(519ページ)を参照してください。

自己署名証明書が付属してはいますが、CA (認証局) が署名した証明書を使用することを強くお勧めします。また、システムの証明書に署名したCAのルート証明書がSmartConnector上で信頼されていることを確認してください。CAのルート証明書がSmartConnector上で信頼済みになっていない場合は、「SmartConnectorをFIPS互換としてインストールまたはアップグレードする」(528ページ)の手順に従ってください。

CAが署名した証明書の入手を容易にするため、システムで証明書署名要求を生成できます。署名済みの証明書ファイルをCAから入手したら、システムにアップロードして以降の認証で使用できます。詳しい手順については、「CSR (証明書署名要求) の生成」(520ページ)を参照してください。

インストールされているSSL証明書が30日未満で失効する場合や、すでに失効している場合、監査イベントが生成されます。30日以内に失効しない証明書で証明書を置き換えるまで、デバイスイベントクラスIDが「`platform:407`」のイベントが定期的に生成されます。

自己署名証明書の生成

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

アプライアンスには自己署名証明書が付属しており、初めて接続するときにSSLセッションを確立できるようになっています。この種の証明書には、別の団体からの署名が不要で、すぐに使用できます。

自己署名証明書を生成するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[セキュリティ]** セクションにある **[SSL サーバ証明書]** をクリックし、**[証明書/証明書署名要求の生成]** ページを表示します。
3. **[証明書の生成]** タブをクリックします。
4. **[証明書設定の入力]** で、以下のフィールドに新しい値を入力します。

パラメーター	説明
国	2文字の国コード (たとえば米国の場合は「US」)。
都道府県	州または県名 (例:「California」)。

パラメーター	説明
市町村	都市名 (例:「Sunnyvale」)。
組織名	会社名、政府機関などの大きな組織。
組織単位	組織内の部門または部署。
ホスト名	このシステムのホスト名またはIPアドレス。 ホスト名を指定する場合には、この名前がシステムのDNS (Domain Name Service) サーバーに登録されている名前に一致することを確認してください。Loggerアプライアンスの場合、この名前は「NIC」(494ページ) で指定したホスト名と同じである必要があります。 **注:** このシステムのホスト名またはIPアドレスが将来変わった場合は、新しい自己署名証明書またはCSRを生成する必要があります。新しい証明書を入手したら、証明書をアップロードして、システムと通信するコネクター (FIPSモード) がホスト名を検証できるようにする必要があります。
メールアドレス	このCSRの管理者または窓口のメールアドレス。
プライベートキーの長さ	プライベートキーの長さ (ビット単位)。**1024**、**2048**、**4096**、**8192**のいずれかを選択します。

CSRまたは自己署名証明書を生成するには、最初の2個のボタンを使用します。**[資格情報を表示]** ボタンは、生成された証明書を表示するためだけに使用します。

ボタン	説明
CSRの生成	クリックすると、CSR (証明書署名要求) が生成されます。
証明書の生成	クリックすると自己署名証明書が生成されます。
資格情報を表示	クリックすると、生成された証明書が表示されます。

5. **[証明書の生成]** ボタンをクリックして自己署名証明書を生成します。

   注: 証明書の生成中にApacheサーバーが再起動します。その間Webサーバーへの通信がエラーになる可能性があります。これは予想される動作であり、Apacheが起動すれば通信は自動的に回復します。

6. **[Ok]** をクリックして生成を確定します。
7. **[資格情報を表示]** ボタンをクリックしてPEMエンコードされた自己署名証明書を表示します。

CSR (証明書署名要求) の生成

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

CSR (証明書署名要求) の生成は、VeriSignなどのサードパーティ証明機関 (CA) が署名した証明書を取得する際、最初に行う手順です。生成されたCSRをVeriSignなどのCAに

送信し、署名済み証明書ファイルを返送してもらう必要があります。CSRは、証明書を要求するシステム上で生成する必要があります。つまり、システムA用のCSRをシステムBで生成したり、サードパーティ製のユーティリティを使用して生成したりすることはできません。

証明書署名要求を生成するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[セキュリティ]** セクションにある **[SSL サーバ証明書]** をクリックし、**[証明書/証明書署名要求の生成]** ページを表示します。
3. **[証明書の生成]** タブをクリックします。
4. **[証明書設定の入力]** で、以下のフィールドに新しい値を入力します。

パラメーター	説明
国	2文字の国コード (たとえば米国の場合は「US」)。
都道府県	州または県名 (例:「California」)。
市町村	都市名 (例:「Sunnyvale」)。
組織名	会社名、政府機関などの大きな組織。
組織単位	組織内の部門または部署。
ホスト名	このシステムのホスト名またはIPアドレス。 ホスト名を指定する場合には、この名前がシステムのDNS (Domain Name Service) サーバーに登録されている名前に一致することを確認してください。Logger アプライアンスの場合、この名前は「NIC」(494ページ) で指定したホスト名と同じである必要があります。 **注:** このシステムのホスト名またはIPアドレスが将来変わった場合は、新しい自己署名証明書またはCSRを生成する必要があります。新しい証明書を入手したら、証明書をアップロードして、システムと通信するコネクター (FIPSモード) がホスト名を検証できるようにする必要があります。
メールアドレス	このCSRの管理者または窓口のメールアドレス。
プライベートキーの長さ	プライベートキーの長さ (ビット単位)。**1024**、**2048**、**4096**、**8192**のいずれかを選択します。

5. CSRまたは自己署名証明書を生成するには、最初の2個のボタンを使用します。**[資格情報を表示]** ボタンは、生成された証明書を表示するためだけに使用します。

ボタン	説明
CSRの生成	クリックすると、CSR (証明書署名要求) が生成されます。
証明書の生成	クリックすると自己署名証明書が生成されます。
資格情報を表示	クリックすると、生成された証明書が表示されます。

6. **[CSRの生成]** を選択して、証明書署名要求を生成します。
7. CSRが正常に生成されると、ポップアップウィンドウが表示され、CSRファイルをダウンロー

ドするか、その内容をコピー/貼り付けできるようになります。

コピー/貼り付けを行うには、 `-----BEGIN CERTIFICATE REQUEST-----` から`-----END CERTIFICATE REQUEST-----`までのすべての行 (これらを含む) をコピーします。

8. CSRファイルを認証局に送付し、CA署名証明書を入手します。
9. CA署名証明書ファイルを入手したら、次の「証明書のインポート」(522ページ)に進みます。

証明書のインポート

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

CA (認証局) から証明書を入手したら、以下の手順に従ってシステムにインポートします。

証明書をインポートするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[セキュリティ]** セクションにある **[SSL サーバ証明書]** をクリックします。
3. **[証明書のインポート]** タブをクリックします。
4. **[ブラウズ]** ボタンをクリックし、ローカルファイルシステム上の署名された証明書ファイルを探します。

   注: インポートする証明書は、PEM (Privacy Enhanced Mail) 形式になっている必要があります。

5. **[インポートしてインストール]** をクリックして指定した証明書をインポートします。
6. **HTTPS**を使用する場合、ブラウザーによっては、新しい証明書を有効にするために、ブラウザーを閉じてから再起動する必要があります。ブラウザーの要件が不明な場合は、ブラウザーを閉じてから再起動してください。

HTTP Strict Transport Securityの有効化

HTTP Strict Transport Security (HSTS) は、ブラウザーがHTTPSで確実にWebサイトに接続できるようにするシンプルな標準規格であり、幅広くサポートされています。これにより、ユーザーを`http://`から`https:///`URLへとリダイレクトする安全性の低いプラクティスが不要になります。

Logger Web UIへの接続には、次のHTTPS URLが必要です。

- `https://`<ホスト名またはIPアドレス>: Loggerアプライアンス。
- `https://`<ホスト名またはIPアドレス>`:`<設定ポート>: ソフトウェアLogger。

ただし、HTTPSではなくHTTPでLoggerに誤って接続する可能性があるので、中間者攻撃に対する脆弱性が存在します。LoggerのHSTSサポートを利用すれば、ブラウザーからのLogger接続に必ずHTTPSを使用することができます。

HSTSを有効化するには

1. Loggerで、CSR (証明書署名要求) を生成します。CSRを生成する手順については、「CSR (証明書署名要求) の生成」(520ページ) を参照してください。
   - 自己署名証明書は使用しないでください。
   - 完全修飾ドメイン名 (FQDN) (`n192-0-2-h24.server.yourco.com`など) を使用してください。
2. Verisignなどの証明機関 (CA) に署名を要求すると、CAによって署名された証明書が返されます。
3. CAによって署名された証明書をLoggerにインポートします。証明書をインポートする手順については、「証明書のインポート」(522ページ) を参照してください。
4. CAによって署名された証明書を、ブラウザーのトラストストアにインポートします。信頼証明書をインポートする手順については、ブラウザーのヘルプを参照してください。

   たとえばFirefox 47.xの場合、☰メニューで **[オプション]** を選択し、**[詳細]**、**[証明書]** タブ、**[証明書を表示]**、**[認証局証明書]**、**[インポート]** ボタンの順にクリックします。
5. ブラウザーを閉じ、再度開きます。次のHTTPアドレスで、Loggerにアクセスできるようになります。
   - `http://<Logger FQDN>`: Loggerアプライアンス。
   - `http://<Logger FQDN>:<設定ポート>`: ソフトウェアLogger。

注: URLには、IPアドレスやホスト名ではなく、Logger FQDNを使用してください。

SSLクライアント認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムでは、SSL証明書を使用したクライアント認証がサポートされています。SSLクライアント認証はTwo-Factor認証の1つの形であり、ローカルパスワード認証の代替手段または追加手段として使用できます。その結果、CAC (Common Access Card) ベースの認証など、SmartCards用にシステムを設定できます。CACは、軍人、選抜予備隊、DOD軍属、資格のある個人契約者の現役メンバーのための標準のIDカードです。

注: CACは、クライアント証明書認証の1つの形態です。クライアント証明書認証に関する情報は、CACに適用されます。

システムでは、LDAPS認証もサポートされています。LDAPSサーバー用のSSL証明書は、トラストストアにアップロードする必要があります。SSL証明書をアップロードした後、apsプロセスを再起動する必要があります (**[システム管理] > [プロセス ステータス] > [aps] > [再起動]**)。

SSLクライアント認証をサポートするためのLoggerの設定

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

SSLクライアント認証をサポートするようにLoggerを設定するには、次の手順を実行します。

SSLクライアントをサポートするためにLoggerを設定するには

Loggerでの作業

1. Loggerが、ArcSightから提供されている付属のデフォルト署名証明書を使用している場合は、FIPS準拠の署名されたSSLサーバー証明書で置き換えます。証明書をロードするには、「信頼済みの証明書のアップロード」(525ページ) の手順に従ってください。

   注意: 認証に使用するすべてのSSLクライアント証明書は、LoggerでFIPSが有効になっていない場合でも、FIPS互換である (つまり、FIPS互換のアルゴリズムでハッシュ作成されている) ことが必要です。

2. クライアント証明書認証を有効にします (「クライアント証明書認証」(536ページ) を参照)。
3. 以下のいずれかを選択します。
   - クライアント証明書が**CAによって署名されている場合は**、クライアントの認証に使用する証明書に署名したCAのルート証明書をアップロードします (「信頼済みの証明書のアップロード」(525ページ) を参照)。
   - Loggerで認証するために使用するクライアント証明書がさまざまなCAによって署名されている場合は、必ず**すべての**CAのルート証明書をアップロードしてください。
   - クライアント証明書が**自己署名**されている場合は、クライアント証明書の公開部分をアップロードします。
4. クライアント証明書を使用してLoggerに接続する各ユーザーのユーザー名を設定します (「ユーザー管理」(542ページ) を参照)。
5. (オプション) CRL (証明書失効リスト) をアップロードします (「証明書失効リストのアップロード」(525ページ) を参照)。
6. (オプション) このLoggerが、SSLクライアント認証**のみ**を使用するように設定されている場合は、このLoggerの認証IDとコードが、他のLoggerで適切に設定されていることを確認します。詳細については、「ピアノード」(483ページ) を参照してください。

クライアント (Webブラウザー) 上の作業

LoggerにアクセスするときにSSLクライアント証明書を渡すようにブラウザーを設定します(ブラウザーで、プライベートキーをPKCS 12形式でアップロードします)。

信頼済みの証明書のアップロード

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

信頼済みの証明書は、システムにログインするユーザーを認証するために使用されます。信頼済みの証明書のアップロードは、LDAPS認証を使用する場合に必要です。信頼済みの証明書は、リモートLDAPSサーバーを認証するために使用されます。証明書は、PEM (Privacy Enhanced Mail) 形式になっている必要があります。

信頼済みの証明書をアップロードするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[セキュリティ]** セクションにある **[SSL クライアント認証]** をクリックします。
3. **[信頼証明書]** タブで **[ブラウズ]** をクリックし、ローカルファイルシステム上の信頼済みの証明書を参照します。
4. **[アップロード]** をクリックします。信頼済みの証明書がアップロードされ、**[リポジトリの証明書]** リストに表示されます。

   信頼済みの証明書の詳細を表示するには、[証明書名] 欄に表示されるリンクをクリックします。

   信頼済みの証明書を削除するには、証明書を選択して **[削除]** をクリックします。

証明書失効リストのアップロード

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

CRL (証明書失効リスト) は、コンピューターによって生成された記録であり、有効期限の前に取り消されるか保留された証明書を識別します。CACをサポートするには、CRLファイルをArcSightシステムにアップロードする必要があります。CRLファイルはPEM形式になっている必要があります。

CRLファイルをアップロードするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[セキュリティ]** セクションにある **[SSL クライアント認証]** をクリックします。
3. **[証明書失効リスト]** タブで **[ブラウズ]** をクリックし、ローカルファイルシステム上のCRLファイルを参照します。
4. **[アップロード]** をクリックします。CRLがアップロードされ、**[証明書失効リスト]** リストに表示されます。

CRLの詳細を表示するには、**[発行者名]** 欄に表示されるリンクをクリックします。

CRLファイルを削除するには、ファイルを選択して **[削除]** ボタンをクリックします。

注: クライアント証明書認証を有効にするには、「クライアント証明書認証」(536ページ)を参照してください。

FIPS 140-2

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムでは、FIPS 140-2 (Federal Information Processing Standard 140-2) がサポートされています。FIPS 140-2は、NIST (National Institute of Standards and Technology) によって発行された規格であり、ソフトウェアコンポーネントの暗号化モジュールを認可するために使用されます。米国連邦政府は、SBU (取り扱い注意ではあるが機密扱いでない) 情報を扱うすべてのIT製品がこれらの規格に準拠していることを義務付けています。

FIPS準拠

システムをFIPS 140-2準拠にする必要がある場合は、FIPSを有効にできます。いったん有効にすると、NISTによりFIPS 140-2用に定義されている暗号化アルゴリズムが、内部コンポーネントと外部コンポーネントの間のすべての暗号化された通信に使用されます。

注: 完全にFIPS 140-2準拠にするには、展開しているLoggerのすべてのコンポーネントをFIPS 140-2モードにする必要があります。たとえば、Logger上でFIPS 140-2を有効にしても、Loggerにイベントを送信するSmartConnectorがFIPS 140-2モードで動作していない場合、完全にFIPS 140-2準拠になっていません。

一般的な展開では、Loggerは以下のコンポーネントと通信します。完全にFIPS準拠にするには、以下のすべてのコンポーネントでFIPSを有効にする必要があります。

- Loggerにイベントを送信するSmartConnector: コネクターをFIPS準拠にするには、「SmartConnectorをFIPS互換としてインストールまたはアップグレードする」(528ページ)の手順に従ってください。
- Loggerによるイベントとアラートの転送先となる、ArcSightマネージャーなどのLogger転送者: FIPS準拠のLoggerのイベント送信先のシステムもFIPS準拠であることが必要です。また、そのシステムのSSLサーバー証明書をLogger上にインポートして、LoggerがSSLサーバーと通信できるようにする必要があります。

  イベントとアラートをArcSightマネージャーに転送する場合は、FIPS 140-2を有効にするために、ESM 4.0 SP2以降が動作している必要があります。詳細については、使用しているバージョンのESMに対応する『ArcSight ESM インストールおよび構成ガイド』を参照してください。また、「ESM通知先」(419ページ)の手順に従って、このステップの設定を完了してください。

- Logger: Loggerでは、FIPS 140-2準拠のアルゴリズムが自動的に使用されます。そのため、Loggerでは、このセクションで説明するようにFIPSを有効にする以外のアクションは不要です。ソフトウェアLogger上でFIPSを有効にする場合には、Loggerがインストールされているマシンを必ずLogger専用に使用してください。

  注: ソフトウェアLogger上でFIPS 140-2を有効にしても、それがインストールされているシステムがFIPS 140-2準拠になるわけではありません。システム全体をFIPS 140-2準拠にするための要件を確認するには、システムのマニュアルを参照してください。

- LoggerがソフトウェアベースのSmartConnectorの通知先になっている場合は、CAによって署名された証明書を使用する必要があります。また、Loggerの証明書に署名したCAのルート証明書が、SmartConnector上で信頼されていることを確認してください。CAのルート証明書がSmartConnector上で信頼済みになっていない場合は、「SmartConnectorをFIPS互換としてインストールまたはアップグレードする」(528ページ)の手順に従ってください。

LoggerでのFIPSモードの有効化と無効化

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

FIPSモードは、必要に応じてLogger上で有効または無効にできますが、新しいモードを有効にするには、リブート (Loggerアプライアンス) または再起動 (ソフトウェアLogger) が必要です。

LoggerでFIPSモードを有効にする際の注意事項

- Loggerは、CAによって署名されたSSL証明書を使用してセットアップされている必要があります。詳細については、「SSLサーバー証明書」(518ページ)を参照してください。
- FIPSモードになっていないLoggerでも、ソフトウェアベースのSmartConnectorの通知先になっている場合は、CAによって署名された証明書を使用する必要があります。また、Loggerの証明書に署名したCAのルート証明書が、SmartConnector上で信頼されていることを確認してください。CAのルート証明書がSmartConnector上で信頼済みになっていない場合は、「SmartConnectorをFIPS互換としてインストールまたはアップグレードする」(528ページ)の手順に従ってください。

FIPSモードを有効または無効にするには

注: Loggerに対する設定要件をよくお読みください (「LoggerでFIPSモードを有効にする際の注意事項」(527ページ)を参照)。

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの [セキュリティ] セクションにある **[FIPS 140-2]** をクリックします。
3. [FIPS モードの選択] オプションで **[有効にする]** または **[無効にする]** をクリックします。
4. **[保存]** をクリックします。

5. 以下のいずれかを実行します。
   - 次のコマンドを使用してソフトウェアLoggerを再起動します。
     <インストールディレクトリ>/current/arcsight/logger/bin/loggerd restart
   - Loggerアプライアンスをリブートします。

FIPS状態を示す表に、Loggerのどのプロセスとコンポーネントでが有効になっているかが表示されます。

SmartConnectorをFIPS互換としてインストールまたはアップグレードする

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

このセクションの内容は、『ArcSight Installing FIPS-Compliant SmartConnectors』の内容とほぼ同じですが、同ドキュメントの内容は一般に適用されるのに対し、このセクションの内容はLogger固有です。

FIPSモードは、バージョン4.7.5.5372以降が動作するSmartConnectorでサポートされています。

目的	アクション
新しいSmartConnectorをインストールして、FIPS互換モードのLoggerにイベントを送信する	インストールで表示されるプロンプトに従います。追加の手順は必要ありません。
バージョン4.7.5.5372以降を実行して**いない**SmartConnectorを、FIPS互換となるようにアップデートする	1. SmartConnectorを、FIPSをサポートしているバージョンにアップグレードします。『SmartConnectorユーザーガイド』の指示に従って、SmartConnectorをアップグレードします。 2. `agent.properties`ファイルを作成します (以下のステップ2aを参照してください)。追加の手順は必要ありません。
バージョン4.7.5.5372以降を実行しているSmartConnectorを、FIPS互換となるようにアップデートする	`agent.properties`ファイルを作成します (以下のステップ2aを参照してください)。追加の手順は必要ありません。

SmartConnectorをFIPS準拠にするには

1. SmartConnectorの構成ガイド (HPEカスタマーサポートサイト (SSO) (https://softwaresupport.hp.com) から入手可能) に記載されているデバイス設定手順に従い、その後コアコネクターソフトウェアのインストールを通じてインストール手順に従います (SmartConnectorのインストールステップ2)。

   コネクターのセットアップのステップ3で、**[キャンセル]** をクリックしてセットアップを終了します。次にNSS DBを設定する必要があります。これは、FIPS互換モードでコネクターをインストールするために必要です。

NSS DBの設定が完了したら、次のステップに進みます。

2. SmartConnectorでFIPSモードを有効にするには
   a. 以下の場所にagent.propertiesを作成します (まだ存在していない場合)。

      ```
      $ARCSIGHT_HOME/current/user/agent
      ```

   b. 次のプロパティを入力し、ファイルを保存して閉じます。

      ```
      fips.enabled=true
      ```

3. SmartConnector上でLoggerの証明書をインポートします。
   a. SmartConnectorマシンのコマンドウィンドウで、$ARCSIGHT_HOME/current/binから次のコマンドを入力してFIPSモードを無効にします。

      ```
      ./arcsight runmodutil -fips false -dbdir $ARCSIGHT_
      HOME/current/user/agent/nssdb.client
      ```

   b. 以下のようにして、Logger証明書ファイルをエクスポートし、SmartConnectorのNSS DBにインポートします。
      - Loggerの証明書ファイルを、接続に使用するブラウザーからエクスポートします。手順については、ブラウザーのヘルプを参照してください。たとえば、Firefox v.44でLoggerの証明書ファイルをエクスポートするには、☰をクリックして **[オプション]** メニューを開き、**[詳細] > [証明書] > [証明書を表示] > [サーバ証明書] >** [使用しているLoggerアプライアンス] をクリックし、**[エクスポート...]** をクリックします。証明書ファイルを、拡張子 .crtまたは.cer付きで保存します。
      - 前の手順でエクスポートした証明書ファイル (この例では**loggercert.crt**) を、SmartConnector上の$ARCSIGHT_HOME/current/binディレクトリにコピーします。$ARCSIGHT_HOME/current/binから、次のコマンドを入力します。

        ```
        ./arcsight runcertutil -A -n mykey -t “CT,C,C” -d $ARCSIGHT_
        HOME/current/user/agent/nssdb.client -i bin/loggercert.crt
        ```

   c. 次のコマンドを入力して、ステップ1で無効にしたFIPSモードを再度有効にします。

      ```
      ./arcsight runmodutil -fips true -dbdir $ARCSIGHT_
      HOME/current/user/agent/nssdb.client
      ```

   d. SmartConnectorが、Logger証明書のSubject: フィールドのCN値で指定されている名前を解決できることを確認します。名前を解決できない場合は、SmartConnectorシステムの**Hosts**ファイルに名前を追加します。
   e. 新しいSmartConnectorをインストールしている場合は、次のステップを続行します。

      SmartConnectorをFIPS互換にアップデートする場合は、コネクターのLogger通知先ホスト名が、証明書のSubjectフィールドのCN値と同じであることを確認し、**この手順を終了します**。

4. SmartConnector設定ウィザードに戻るには、`$ARCSIGHT_HOME/current/bin`から次のコマンドを入力します。

   ```
   ./arcsight connectorsetup
   ```

5. ウィザードモードで開始するかどうか質問された場合は、**[はい]** をクリックします。

   通知先選択ウィンドウが再度表示されます。『**SmartConnector Configuration Guide**』の「**Installation Step 4**」に戻り、コネクター設定を続行します。

   注: コネクターを構成する際には、コネクターのLogger通知先ホスト名が、証明書の**Subject:**フィールドの`CN`値と同じであることを確認してください。

残りの設定手順については、インストール中のSmartConnectorの設定ガイドを参照してください。専用の構成ガイドには、イベント収集用にデバイスを設定する方法、設定手順の中で必要になる詳細なインストールパラメーター、ArcSightイベントへのベンダー固有のフィールドマッピングの表が記載されています。

ユーザ/グループ

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[ユーザ/グループ] サブメニューは、ユーザーとユーザーグループを設定し、認証オプションを設定するために使用します。

認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[認証設定] では、ユーザーログインセッションの設定とポリシー、パスワードルールとロックアウト、外部認証オプションを指定できます。

セッション

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[セッション] タブでは、単一のユーザーアカウントに対する最大同時セッション数と、ユーザーセッションが自動的にログアウトされるかユーザーアカウントが無効にされるまでの時間の長さを指定できます。デフォルトでは、1つのユーザーアカウントでアクティブなセッションを同時に15個まで使用でき、15分間操作しないとユーザーアカウントがログアウトされます。

セッションの設定を変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[セッション]** タブで、次の表で説明するパラメーターを更新します。

パラメーター	説明
最大同時ログイン数/ユーザ	1つのユーザーアカウントに許可される最大同時セッション数。デフォルトは**15セッション**です。
非アクティブセッションをログアウトするまでの時間	操作のないセッションを自動的に終了させるまでの時間 (分単位)。デフォルトは**15分**です。
非アクティブアカウントを無効にするまでの時間	アクティブでないユーザーアカウントを無効にするまでの日数。デフォルト値は**0**で、アカウントは無効にならないことを意味します。

4. **[保存]** をクリックして変更するか、別のタブをクリックしてキャンセルします。

ローカルパスワード

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[ローカルパスワード] タブを使用すると、最小および最大文字数や、その他のパスワード要件など、パスワードポリシーを設定できます。

ヒント: 認証方法を [ローカルパスワード] に設定した場合、セキュリティを強化するために、アカウントのロックアウトポリシーを有効にしてください。

パスワード設定を変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[ローカルパスワード]** タブを選択します。
   次の表で説明するパラメーターを使用して、パスワード設定をカスタマイズします。

パラメーター	説明
アカウントのロックアウト	
アカウントのロックアウトを有効にする	以降の設定の定義に従ってユーザーアカウントのロックアウトを有効にするには、チェックボックスをオンにします。デフォルトでは、ポリシーは**無効**になっています。 **注:** 認証方法を[ローカルパスワード]に設定する場合は、このパラメーターを有効にしてください。
アカウントをロックアウトするまでの回数	ユーザーアカウントをロックアウトするまでのログイン失敗回数。デフォルト値は**3**です。
次の試み失敗を記憶	失敗したログイン試行を記憶する時間 (分)。デフォルト値は**1**です。
アカウントをロックアウトする時間	ロックアウトされたアカウントのロックを解除できない時間 (分)。デフォルト値は**15**です。
パスワードの有効期限	
パスワードの有効期限を有効にする	以降の設定の定義に従ってユーザーパスワードの期限を有効にするには、チェックボックスをオンにします。デフォルトでは、ポリシーは**無効**になっています。
パスワードの有効期限	パスワードが期限切れになるまでの日数。デフォルト値は**90**です。
期限が切れる前にユーザに通知	期限切れの何日前にユーザーに通知するか。ユーザーが期限切れの前にパスワードを更新できるようにするには、このオプションを選択します。デフォルト値は**5**です。
パスワードの有効期限ポリシーから除外するユーザ	パスワードを期限切れにしないユーザーを設定するには、リンクをクリックします。 この機能の使用方法については、「パスワードの有効期限から除外するユーザー」(533ページ)を参照してください。
パスワード強度ルール	
パスワード強度の強化	以降の設定の定義に従ってパスワードポリシーを適用するには、チェックボックスをオンにします。デフォルトでは、ポリシーは**無効**になっています。
最小文字数	パスワードに含まれる必要がある最小文字数。デフォルト値は**10**です。
最大文字数	パスワードに含めることができる最大文字数。デフォルト値は**20**です。
パスワード文字ルール	
パスワード文字ルールは、パスワードの強度を確保するための追加の文字要件を定義します。	
数字	パスワード内の数字 (0～9) の最小文字数。デフォルト値は**2**です。
大文字	パスワード内の大文字 (A～Z) の最小文字数。デフォルト値は**0**です。
特殊文字	パスワードに必要な英数字以外の文字の最小文字数。デフォルト値は**2**です。

パラメーター	説明
小文字	パスワード内の小文字 (a～z) の最小文字数。デフォルト値は**0**です。
パスワードの必須文字N文字が現在のパスワードと異なります	新しいパスワードと以前のパスワードで違っている必要がある最小文字数。デフォルト値は**2**です。
ログイン画面に[パスワードを忘れた場合]リンクを含みます	• ユーザーがログインページ上の「パスワードを忘れた場合」リンクを使用してローカルパスワードをリセットできるようにするには、チェックボックスをオンにします。デフォルトでは、オプションは**無効**になっています。 • この機能が正常に動作するには、SMTPサーバーをシステム上で設定し、ユーザー名で正しいメールアドレスを指定する必要があります。 • SMTPサーバーが設定されていない場合は、一時的なパスワードを含むメールを送信できないため、パスワードをリセットできません。 • ユーザー名に対し、ユーザー設定でメールアドレスが指定されている必要があります。一時的なパスワードがそのメールアドレスに送信されます。メールアドレスが指定されていないか、メールアドレスが正しくない場合は、ユーザーにメールが送信されません。 この機能の使用方法については、「パスワードを忘れた場合」(534ページ)を参照してください。

4. **[保存]**をクリックして変更内容を保存するか、別のタブをクリックしてキャンセルします。

パスワードの有効期限から除外するユーザー

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ほとんどのユーザーに対してパスワードの有効期限ポリシーを設定した場合でも、パスワード有効期限が自動的に切れないユーザーを指定したい場合があります。

ユーザーをパスワードの有効期限ポリシーから除外するには

1. 上部のメニューバーから**[システム管理]**をクリックします。
2. **[ユーザ/グループ]**セクションの**[認証]**をクリックします。
3. **[ローカルパスワード]**タブを選択し、**[パスワードの有効期限ポリシーから除外するユーザ]**をクリックします。
4. **[パスワードの有効期限から除外するユーザ]**ページが表示されます。
5. **[非除外ユーザ]**リストからユーザーを選択し、右矢印アイコンをクリックして、選択したユーザーを**[除外ユーザ]**リストに移動します。除外するユーザーのリストからユーザーを削除するには、逆の操作を行います。

   一度に複数のユーザーを選択して移動できます。また、アイコンをクリックすれば、すべ

てのユーザーを移動できます。

6. **[保存]** をクリックしてポリシーを保存するか、**[キャンセル]** をクリックして終了します。

パスワードを忘れた場合

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ユーザーは、ログイン画面の **[パスワードを忘れた場合 (Forgot Password)]** リンクから、自分のパスワードをリセットできます。Loggerにより、ファイルで指定されたメールアドレスに一時パスワードが送信されます。

この設定はデフォルトでは選択されていません。有効化するには、**[システム管理] > [認証] > [ローカル パスワード]** タブをクリックし、ページの下までスクロールしてから、**[ログイン画面に [パスワードを忘れた場合] リンクを含みます]** をオンにして **[保存]** をクリックします。

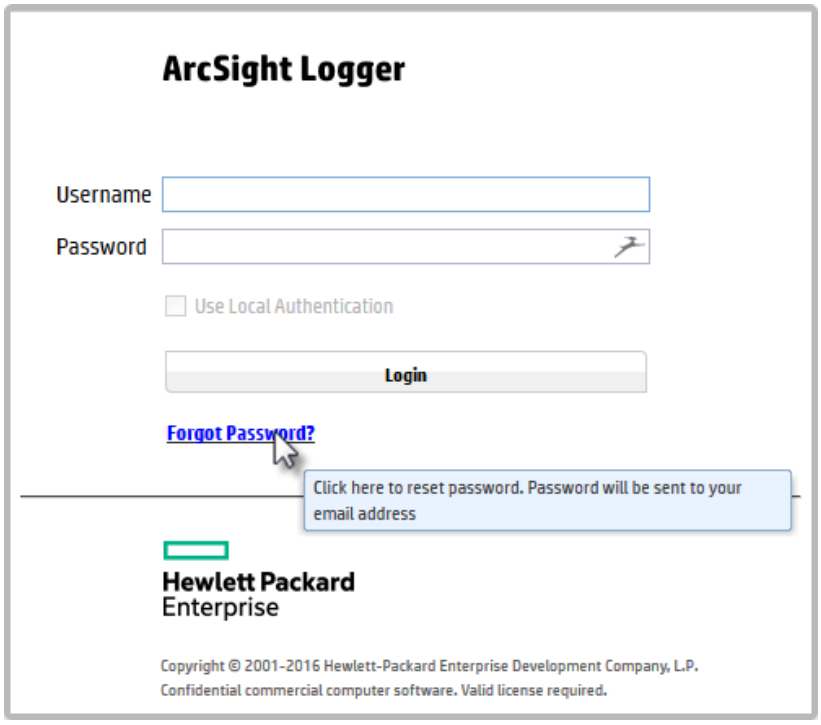
次回のログイン時には、このリンクが有効になります。

この機能を使用するには、SMTPサーバーが設定されている必要があります。この設定を有効にする方法の詳細については、「ローカルパスワード」(531ページ) を参照してください。

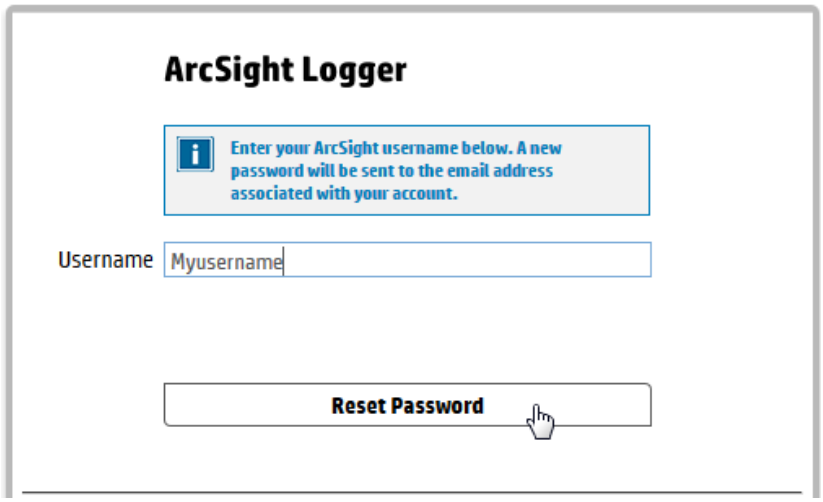
ヒント: 一時的なパスワードは、メールで指定された時刻まで有効です。デフォルトは5時間です。指定した時刻までにログインしなかった場合、管理者のみがパスワードをリセットして別の一時的なパスワードを生成できます。

パスワードをリセットするには

1. [ログイン] ダイアログボックスで **[パスワードを忘れた場合 (Forgot Password?)]** リンクをクリックします。



2. [パスワードのリセット] 画面が表示されます。



3. [パスワードのリセット] 画面でユーザー名を入力します。
4. **[パスワードのリセット (Reset Password)]** をクリックします。

   一時的なパスワードが記載された自動的なメールが、そのユーザーの指定されたメールアドレスに送信されます。一時パスワードでログインすると、Loggerは [パスワードの変更] ページへとリダイレクトします。このページで、パスワードをリセットできます。

外部認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムでは、ローカルパスワード認証方式が提供されるのに加えて、クライアント証明書/CAC、LDAP、およびRADIUS認証がサポートされています。すべての認証方式を同時に有効にすることはできません。

外部認証を有効にするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. [ユーザ/グループ] セクションの **[認証]** をクリックします。
3. **[外部認証]** タブを選択します。
4. メニューから認証方法を選択します。
5. **[保存]** をクリックします。

注: CACは、クライアント証明書認証の1つの形態です。クライアント証明書認証に関する情報は、CACに適用されます。

ローカルパスワード認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ローカルパスワード認証は、デフォルトの認証方法です。**[ローカルパスワード]** タブで設定されているローカルパスワードポリシーが実装されます。詳細については、「ローカルパスワード」(531ページ) を参照してください。

ローカルパスワード認証を設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[外部認証]** タブを選択します。
4. プルダウンメニューから **[ローカルパスワード認証]** を選択します。
5. **[保存]** をクリックします。

クライアント証明書認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

この認証方式では、クライアント証明書を使用してユーザーを認証する必要があります。クライアント証明書ごとに、クライアント証明書のDN (Distinguished Name) と一致するDNを持つユーザーアカウントがシステム上に存在する必要があります。

注意: 認証に使用するすべてのSSLクライアント証明書は、システムでFIPSが有効になっていない場合でも、FIPS互換である(FIPS互換のアルゴリズムでハッシュ作成されている)ことが必要です。

クライアント証明書認証を設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[外部認証]** タブを選択します。
4. ドロップダウンメニューから **[クライアント証明書]** を選択します。
5. **[ローカルパスワードのフォールバックを許可]** には以下の2つのオプションがあります。
   - **[デフォルト Admin に対してのみローカルパスワードのフォールバックを許可]**
     このオプションを選択すると、クライアント証明書が使用できないか無効な場合に、デフォルト管理者ユーザーは、ユーザー名とパスワードのみを使用してログインできるようになります。この権限は、デフォルト管理者ユーザーのみに制限されます。他のユーザーがシステムにアクセスするには、有効なクライアント証明書が必要です。このオプションは、デフォルトで有効になっています。
   - **[すべてのユーザに対してローカルパスワードのフォールバックを許可]**
     このオプションを選択すると、クライアント証明書が無効か使用できない場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。
     詳細については、「ローカルパスワードフォールバック」(541ページ)を参照してください。
6. **[保存]** をクリックします。

クライアント証明書とローカルパスワード認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

この認証方式では、SSLクライアント証明書と有効なローカルパスワードを使用してユーザーを認証する必要があります。ローカルパスワードとは、**[ユーザ/グループ]** セクションの **[ユーザ管理]** で作成したユーザー認証情報に関連付けられたパスワードを指します。詳細については、「ユーザーの作成とアクティブ化」(542ページ)を参照してください。

システム上のユーザーアカウントは、クライアント証明書のDN (Distinguished Name) と一致するDNを使用して定義されている必要があります。

ユーザーDNを作成するための手順については、「ユーザーの作成とアクティブ化」(542ページ)と、パラメーター表の「クライアントDNを使用」を参照してください。

注意: 認証に使用するすべてのSSLクライアント証明書は、システムでFIPSが有効になっていない場合でも、FIPS互換である(FIPS互換のアルゴリズムでハッシュ作成されている)ことが必要です。

クライアント証明書とパスワード認証を設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[外部認証]** タブを選択します。
4. ドロップダウンメニューから **[クライアント証明書とローカルパスワード]** を選択します。
5. **[ローカルパスワードのフォールバックを許可]** には以下の2つのオプションがあります。
   - **[デフォルト Admin に対してのみローカルパスワードのフォールバックを許可]**
     このオプションは常に有効であり、デフォルト管理者ユーザーは、ユーザー名とパスワードのみを使用してログインできます。
   - **[すべてのユーザに対してローカルパスワードのフォールバックを許可]**
     このオプションは常に無効になっています。認証方法として、**[クライアント証明書とローカルパスワード]** を使用している場合は、有効にできません。
     詳細については、「ローカルパスワードフォールバック」(541ページ) を参照してください。
6. **[保存]** をクリックします。

RADIUS認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

この認証方式では、RADIUSサーバーでユーザーを認証できます。RADIUS認証が有効になっていても、各ユーザーアカウントはシステム上にローカルに存在している必要があります。ユーザー名はRADIUSサーバー上のユーザー名と一致している必要がありますが、パスワードは違っていてもかまいません。ユーザーが正常に認証されるには、有効なユーザー名と(RADIUS) パスワードを入力する必要があります。

RADIUS認証設定を設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。
3. **[外部認証]** タブを選択します。
4. ドロップダウンメニューから **[RADIUS]** を選択します。
5. **[ローカルパスワードのフォールバックを許可]** には以下の2つのオプションがあります。
   - **[デフォルト Admin に対してのみローカルパスワードのフォールバックを許可]**
     このオプションを選択すると、RADIUS認証に失敗する場合に、デフォルト管理者ユーザーがユーザー名とパスワードのみを使用してログインできるようになります。この権限は、管理者ユーザーのみに制限されます。他のすべてのユーザーはRADIUSで認証される必要があります。このオプションは、デフォルトで有効になっています。
   - **[すべてのユーザに対してローカルパスワードのフォールバックを許可]**

このオプションを選択すると、RADIUS認証に失敗する場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。詳細については、「ローカルパスワードフォールバック」(541ページ)を参照してください。

6. 必要に応じて**RADIUSサーバー**のパラメーターを更新します。

パラメーター	説明
サーバーホスト名: [ポート]	RADIUSサーバーのホスト名とポートを入力します。
バックアップ サーバ ホスト名: [ポート] (オプション)	**(オプション)** プライマリサーバーが応答しない場合に使用する、バックアップRADIUSサーバーを入力します。サーバーが認証失敗 (不正なパスワード、不明なユーザー名など) を返した場合は、バックアップサーバーが試行されません。バックアップサーバーは、プライマリサーバーが通信障害になった場合にのみ試行されます。 プライマリサーバーと同じ形式を使用してホスト名とポートを指定します。
認証の秘密の共有	RADIUSパスフレーズを入力します。
NAS IP アドレス	NAS (Network Access Server) のIPアドレス。
要求のタイムアウト	RADIUSサーバーからの応答を待つ時間 (秒)。デフォルト値は**10**です。
要求の再試行	RADIUSリクエストを再試行する回数。デフォルト値は**1**です。
RADIUS プロトコル	ドロップダウンメニューを使用してプロトコルオプションを選択します。デフォルトは **なし**です。

7. **[保存]** をクリックします。

LDAP/ADおよびLDAPS認証

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

この認証方式は、LDAPサーバーでユーザーを認証します。LDAPが有効になっていても、各ユーザーアカウントはシステム上にローカルに存在している必要があります。ローカルに指定されたユーザー名は、LDAPサーバー上で指定されたユーザー名と違っていてもかまいませんが、各ユーザーアカウントに指定されたDN (Distinguished Name) は、LDAPサーバー上のものと一致している必要があります。

ヒント: ユーザーDNの作成手順については、「ユーザーの作成とアクティブ化」(542ページ)と、パラメーター表の「クライアント DN を使用」(544ページ)を参照してください。

LDAP認証

LDAP認証を設定するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[認証]** をクリックします。

3. **[外部認証]** タブを選択します。
4. ドロップダウンメニューから **[LDAP]** を選択します。
5. **[ローカル パスワード のフォールバックを許可]** には以下の2つのオプションがあります。
   - **[デフォルト Admin に対してのみローカル パスワード のフォールバックを許可]**
     このオプションを選択すると、LDAP認証に失敗する場合に、デフォルト管理者ユーザーがユーザー名とパスワードのみを使用してログインできるようになります。この権限は、デフォルト管理者ユーザーのみに制限されます。他のすべてのユーザーはLDAPで認証する必要があります。このオプションは、デフォルトで有効になっています。
   - **[すべてのユーザに対してローカル パスワード のフォールバックを許可]**
     このオプションを選択すると、LDAP認証に失敗する場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。詳細については、「ローカルパスワードフォールバック」(541ページ) を参照してください。

     LDAPサーバーには以下のパラメーターがあります。

パラメーター	説明

サーバーホスト名:[ポート] (オプション)	(オプション) LDAPサーバーのホスト名またはIPアドレスとポートを次の形式で入力します。
	`ldap://<hostname or IP address>:<port>`
	`ldaps://<hostname or IP address>:<port>`
	LDAPSを使用するには追加の手順が必要です。■を参照してください。

バックアップ サーバ ホスト名: [ポート] (オプション)	(オプション) プライマリサーバーが応答しない場合に使用する、バックアップLDAPサーバーを入力します。サーバーが認証失敗 (不正なパスワード、不明なユーザー名など) を返した場合は、バックアップサーバーが試行されません。バックアップサーバーは、プライマリサーバーが通信障害になった場合にのみ試行されます。 プライマリサーバーと同じ形式を使用してホスト名とポートを指定します。
要求のタイムアウト	LDAPサーバーからの応答を待つ時間 (秒)。デフォルト値は**10**です。

6. 完了したら **[保存]** をクリックします。

LDAPS認証

LDAP Over SSL認証を設定するには

1. LDAPSサーバー用のSSL証明書が、トラストストアにアップロードされていることを検証します。「信頼済みの証明書のアップロード」(525ページ) を参照してください。
2. 「LDAP認証を設定するには」(539ページ) の手順を実行します。
3. LDAPSサーバーのURLを入力します。先頭に、`ldaps://`を指定します。
4. システム管理の **[システム]** メニューで、**[プロセス ステータス]** をクリックします。

5. プロセステーブルで **[aps]** を選択します。
6. **[再起動]** をクリックします。

> **注意:** apsプロセスの再起動が必要です。再起動しないと、LDAPSによる認証は失敗します。

ローカルパスワードフォールバック

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

この機能を使用すると、外部認証 (証明書、LDAP、RADIUS) が失敗した場合や、認証サーバーのパスワードを忘れた場合、認証サーバーが利用できない場合に、ローカルユーザー名とパスワードを使用してログインできます。

[ローカル認証の使用] を使用すると、リモート認証サーバーが使用できない場合でも、**[ローカル認証の使用]** チェックボックスをログイン画面に追加することで、デフォルト管理者がログインできるようになります。初期状態では、デフォルト管理者のみに対してこのオプションが有効になっています。しかし、すべてのユーザーに対してローカルパスワードフォールバックを有効にすることができます。たとえば、RADIUS認証方法を設定することにより、設定済みの外部RADIUSサーバーへの認証に失敗した場合、RADIUS認証ではなくローカル認証を使用したログインをユーザーに許可できます。

すべてのユーザーに対してローカルパスワードフォールバックを許可する方法については、「クライアント証明書認証」(536ページ)、「LDAP/ADおよびLDAPS認証」(539ページ)、または「RADIUS認証」(538ページ)を参照してください。

認証失敗時にログインするには

1. **[ArcSight Logger ログイン]** ダイアログで、**[ローカル認証の使用]** チェックボックスをオンにします。

   > **注:** このオプションは、他のユーザーに対して有効にしていない限り、デフォルト管理者のみに対して使用できます。

2. ユーザー名とパスワードを入力し、**[ログイン]** をクリックします。

ログインバナー

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ログイン画面のメッセージは、ニーズに合わせてカスタマイズできます。[コンテンツ] フィールドに入力したテキストは、ログイン画面の [ユーザ名] および [パスワード] フィールドの上に表示されます。また、**[ユーザ名]** および **[パスワード]** フィールドを有効にするためにユーザーがクリックする必要がある確認メッセージも入力できます。

ログインバナーを編集するには、ユーザーアカウントに対する「ログイン設定の構成」許可が有効になっている必要があります。

ログインバナーをカスタマイズするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. **[ユーザ/グループ]** セクションの **[ログイン バナー]** をクリックします。
3. ログインバナーとして表示するテキストを、**[コンテンツ]** フィールドに入力します。

   このフィールドには、書式設定されていないテキストのみを入力できますが、標準のHTMLタグを適用して、書式設定されたテキストを表示できます。このフィールドに画像をロードすることはできません。
4. (オプション) **[確認]** フィールドにテキストを入力します。

   このフィールドにテキストを入力すると、テキストとともにチェックボックスが表示されます。[ユーザ名] および [パスワード] フィールドを有効にするには、このチェックボックスをクリックする必要があります。たとえば、このフィールドに「Are you sure?」、「Do you want to proceed」、または「I agree」と入力した場合、ユーザーがログインするためには、チェックボックスをクリックする必要があります。
5. **[保存]** をクリックします。

ユーザー管理

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

[ユーザ] および **[グループ]** タブでは、システム上のユーザーとユーザーグループを管理できます。ユーザーグループは、システムのさまざまな部分に対するアクセス制御を適用するための手段です。

ユーザーの作成とアクティブ化

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

システムにログインできるユーザーを管理するには、**[ユーザ]** タブを開きます。新しいユーザーの追加、ユーザー情報の編集、ユーザーの削除はいつでも行うことができます。これらの機能を実行するには、適切なシステム管理グループ権限を持っている必要があります。

ユーザーの追加

新しいユーザーを追加するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[ユーザ]** タブで、**[追加]** をクリックします。

4. 以下のパラメーターを入力します。

パラメーター	説明
資格情報	
ログイン	ユーザーのログイン名。
パスワード	ユーザーのパスワード。
パスワード確認	ユーザーのパスワードを再度入力します。
詳細情報	

クライアント DN を使用	SSLクライアント証明書またはLDAP認証を有効にした場合は、このリンクをクリックして、ユーザーのDN (Distinguished Name、証明書サブジェクト) 情報を入力します。DNは、次のような形式になっている必要があります。
	`CN=UserA,OU=Engg Team,O=ArcSight\, Inc.,`
	`L=Cupertino,C=US,ST=California`
	DNを判定するには、次のURLを使用して証明書を表示します。
	`https://<ホスト名またはIPアドレス>/platform-service/`
	`DisplayCertificate`
	または
	システムに接続するためにユーザーが開くブラウザーから、ユーザーのDN情報を入手します。たとえば、Firefoxの場合は、[ツール] > [オプション] > [詳細] > [証明書] > [証明書を表示] > [あなたの証明書] > 証明書を選択 > [表示] の順にクリックします。

名	ユーザーの名。
姓	ユーザーの姓。
電子メール	ユーザーのメールアドレス。
電話	(オプション) ユーザーの電話番号。
タイトル	(オプション) ユーザーの肩書き。
所属	(オプション) ユーザーの部署。
Fax	(オプション) ユーザーのFAX番号。
代替数字	(オプション) ユーザーの他の電話番号。
説明	(オプション) ユーザーに関するその他の情報。
グループに割り当て	
この設定は、ユーザーがこのLoggerに対して持つ権限を制御します。このユーザーが属するグループを選択します。「Loggerのユーザー権限の設定」(546ページ) を参照してください。	
システム管理	すべてのシステム管理の権限。

パラメーター	説明
Logger 権限	システム管理を除くすべてのLogger操作を読み取りおよび編集する権限。
Logger レポート	すべてのレポートを表示、実行、スケジュール設定、編集、削除する権限。
Logger 検索	ローカル検索と分散検索の両方を実行する権限。

5. **[保存および閉じる]** をクリックします。

ユーザーの編集と削除

ユーザーを編集するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[ユーザ]** タブで、編集するユーザーを選択します (複数可)。
4. **[編集]** をクリックします。
5. 必要に応じてユーザー情報を更新します。
6. **[ユーザを保存]** をクリックします。

ユーザーを削除するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[ユーザ]** タブで、削除するユーザーを選択します (複数可)。
4. ページの左上にある **[削除]** をクリックします。

> **注意:** ユーザーを削除すると、そのユーザーのすべてのレポートも削除されます。

ユーザーのアクティブ化

ユーザーをアクティブ化するには

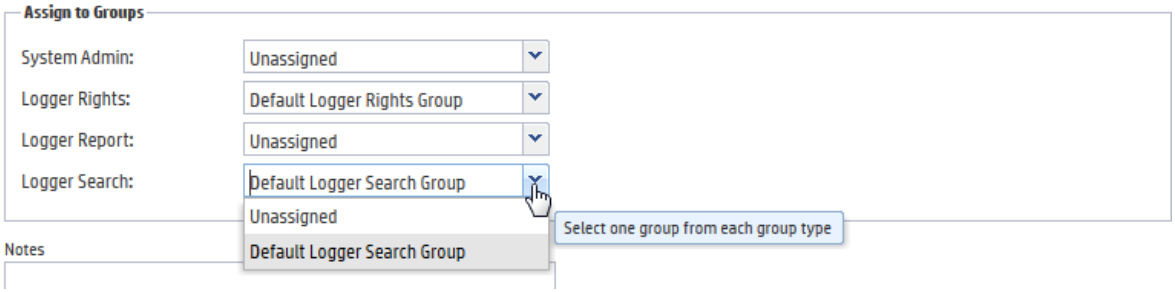
1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[ユーザー]** タブで、アクティブ化するユーザーを選択します (複数可)。
4. **[編集]** を選択します。
5. **[アクティブ]** チェックボックスをオンにします。
6. 変更内容を**保存**します。

Loggerのユーザー権限の設定

Loggerのインストールには、デフォルトの管理者ユーザーが付属します。このユーザーには、他のユーザーの作成とアクセス権限の割り当てに必要な権限がすべて割り当てられています。ユーザーに特定の権限セットが必要な場合、必要な権限を割り当てたカスタムユーザーグループを作成することができます。詳しい手順については、「ユーザーグループの新規作成」(549ページ)を参照してください。

Loggerの権限をユーザーに割り当てるには

1. Loggerナビゲーションバーの **[システム管理]** をクリックします。
2. [ユーザ/グループ] メニューの **[ユーザ管理]** をクリックします。[ユーザの管理] ページが開きます。
3. 権限を割り当てるユーザーのチェックボックスをオンにします。
4. **[編集]** をクリックします。[ユーザを編集] ページが開きます。
5. [グループに割り当て (Assign to Groups)] セクションで、各グループタイプからオプションを1つ選択します。新規ユーザーには、デフォルトで [未割り当て (Unassigned)] が選択されます。Loggerを使用するには、ユーザーは少なくとも1つのユーザーグループのメンバーである必要があります。



6. **[保存および閉じる]** をクリックします。

ユーザーのパスワードのリセット

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

パスワードのリセット機能を使用すると、パスワードを知らなくてもユーザーのパスワードをリセットできます。SMTPが設定されたサーバーを使用しており、ユーザーを作成および更新できる許可があれば、**[パスワードのリセット]** ボタンをクリックしてユーザーのパスワードをリセットできます。新しいパスワード文字列を含む自動的なメールがユーザーに送信されます。

一時的なパスワードが記載された自動的なメールを送信するには、SMTPサーバーが設定されている必要があります。SMTPサーバーが設定されていない場合は、メールを送信できないため、パスワードはリセットされません。

ユーザーのパスワードをリセットするには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[ユーザ]** タブで、パスワードをリセットするユーザーを選択します (複数可)。
4. ページの左上にある **[パスワードのリセット]** をクリックします。

ユーザーは、メールで指定された期間内に、一時的な文字列を使用してログインする必要があります。ユーザーが指定の期間内にログインしなかった場合、アカウントが非アクティブ化されます。アカウントが非アクティブ化された場合、管理者は、再度アカウントをアクティブ化してからパスワードをリセットする必要があります。

自分のパスワードの変更

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

パスワードを変更するには **[パスワードの変更]** メニューを使用します。この機能は、システム管理者がパスワードを知らなくてもユーザーのパスワードをリセットできるようにするためのパスワードリセット機能と異なり、すべてのユーザーがパスワードを変更するために使用できます。パスワードには、管理者ユーザーによって指定されたパスワードポリシーが適用されます。

パスワードを変更するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[パスワードの変更]** をクリックして、**[ユーザ < ユーザー名 > のパスワードの変更]** ページを表示します。
3. 以前のパスワード、新しいパスワードを入力し、確認用に新しいパスワードを再度入力します。
4. **[パスワードの変更]** をクリックします。

ユーザーグループ

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ユーザーグループは、システム上の特定の機能に対する権限を定義し、これらの機能に対するアクセス制御を適用するための役割を果たします。たとえば、ユーザーAに検索の実行を許可するもののレポートの実行を許可しない場合は、そのユーザーを検索グループに割り当てますが、レポートグループには割り当てません。

ユーザーグループは、以下のタイプに分類されます。システム管理、Logger権限、Logger検索、Loggerレポート。それぞれのタイプには、定義済みのデフォルトユーザーグループがあり、そのタイプのすべての権限が有効になっています。特定のグループタイプの権限の一部を許可するには、新しいユーザーグループを作成し、そのグループに許可する権限のみを有効にします。その後、制限するユーザーを新たに作成したグループに割り当てます。

システム管理グループ

システム管理グループは、システムに対するシステム管理操作を制御します。これには、ネットワーク情報の設定、ストレージマウントの設定、SSL証明書のインストール、ユーザー管理などがあります。

Read Only System Adminグループ

すべてのシステム管理権限を有効にするデフォルトのSystem Adminグループに加えて、システムではRead Only System Adminグループを使用できます。このグループに割り当てられたユーザーは、システム管理設定を表示できますが、変更はできません。

このグループに許可される権限の完全なリストについては、システムのユーザーインターフェイスを参照してください。

Logger権限グループ

Logger権限グループは、システムに対するLoggerアプリケーションの操作を制御します。これには、Loggerダッシュボードの表示と[設定]メニューのすべての設定 (イベントアーカイブ、ストレージグループ、アラート、フィルター、スケジューリングタスクなど) といった操作が含まれます。

このグループに許可される権限の完全なリストについては、システムのユーザーインターフェイスを参照してください。

Logger検索グループ

Logger検索グループは、次の権限を通じてローカルおよびピア検索を制御します。

- イベントの検索
- リモートピア上のイベントの検索

グループが、ユーザーにローカルおよびピア検索を許可するように設定されている場合、このグループに割り当てられているユーザーはそれらの操作を実行できます。逆に、グループが、ユーザーにローカルおよびピア検索を禁止するように設定されている場合、このグループに割り当てられているユーザーはそれらの操作を実行できません。

Loggerレポートグループ

Loggerレポートグループは、Logger上のすべてのレポート操作を制御します。これには、発行済みレポートの実行、編集、削除、スケジュール表示などがあります。

このグループに許可される権限の完全なリストについては、システムのユーザーインターフェイスを参照してください。

ユーザーグループの管理

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ユーザーグループの新規作成

新しいユーザーグループを作成するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[グループ]** タブをクリックします。
4. **[追加]** をクリックします。
5. 次のようにして新しいグループを定義します。
   a. **[グループ名]** フィールドにグループ名を入力します。
   b. **[説明]** フィールドにグループの説明を入力します。
   c. [グループ タイプ] ドロップダウンボックスで、グループタイプを選択します。
   d. グループタイプ名の横の下矢印アイコン ( ) をクリックし、このグループのユーザーに割り当てる権限を表示および選択します。
6. **[保存および閉じる]** をクリックしてグループの設定を保存するか、**[メンバーシップの保存および編集]** をクリックしてこのグループにユーザーを追加します。

ユーザーグループの編集と削除

ユーザーグループを編集するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[グループ]** タブをクリックします。
4. 編集するグループを選択し、**[編集]** をクリックします。
5. ユーザーグループ情報を更新します。

   グループのメンバーシップを編集する必要がある場合は、次のようにします。
   a. **[メンバーシップの保存および編集]** をクリックして [グループ メンバーシップの編集] ページを表示します。
   b. [グループ メンバーシップの編集] ページの左上から **[追加]** をクリックします。
   c. 追加するユーザーを選択します。デフォルトでは、編集中のタイプの他のグループに属していないユーザーのみを追加できます。他のグループに属しているユーザーを追加するには、**[他の <group_type> グループに属するユーザを表示]** をクリックします。

更新中のものとグループタイプが同じ別のグループに属しているユーザーを追加すると、そのユーザーは前のグループから自動的に削除されます。

d. **[OK]** をクリックします。
e. **[グループリストへ戻る]** をクリックします。

6. **[保存および閉じる]** をクリックします。

ユーザーグループを削除するには

1. 上部のメニューバーから **[システム管理]** をクリックします。
2. 左パネルの **[ユーザ/グループ]** セクションにある **[ユーザ管理]** をクリックします。
3. **[グループ]** タブをクリックします。
4. 削除するグループを選択します (複数可)。
5. ページの左上にある **[削除]** をクリックします。

その他のシステム管理情報

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

ここには、ソフトウェアLoggerの起動と停止、システムヘルスイベントやSNMPポーリングなど、Loggerを完全に管理するために必要な、システム管理に関する情報が含まれています。

システムの稼働状況の監視

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

以下の方法でLoggerの稼働状況を監視できます。

- 「システムフィルター/事前定義フィルター」(145ページ) に記載されている、定義済みのシステムフィルターを使用する。定義済みのシステムヘルスフィルターは、「システムヘルスイベント」(551ページ) に示すシステムヘルスイベントに基づいています。
- Loggerの内部ストレージグループで、「システムヘルスイベント」(551ページ) に示すシステムヘルスイベントを検索する。あらかじめ定義されているシステムヘルスフィルターが要件に合っていない場合は、システムヘルスイベントに基づいてアラートを作成できます。

- 「SNMP」(503ページ) の手順に従って、システムヘルスイベントをポーリングする (Loggerアプライアンスのみ)。SNMPバージョン2cまたは3を使用して、任意の標準的なネットワーク管理システムから、システムのシステムヘルス情報をポーリングできます。

システムヘルスイベントの通知を設定するには

1. LoggerのSMTPの設定 (「SMTP」(500ページ) を参照)、SNMP通知先の作成 (「SNMP通知先」(417ページ) を参照)、またはSyslog通知先の作成 (「syslog通知先」(417ページ) を参照) を行います。
2. 1つ以上のシステムアラートフィルターを使用するアラートを作成するか、Loggerの内部ストレージグループ内のシステムヘルスイベントを検索するクエリを定義し、一致数としきい値を指定します (「Loggerアラートの種類」(412ページ) を参照)。
3. 新しいアラートを有効にします。

システムヘルスイベント

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

次の表に、Loggerによって生成されるシステムヘルスイベントの一覧を示します。これらのイベントは、Loggerの内部ストレージグループに格納されるため、Logger内部イベントとも呼ばれます。これらのイベントの例については、「システムヘルスイベントの例」(639ページ) を参照してください。

システムの稼働状態を提供する、あらかじめ定義されているシステムフィルターは、これらのイベントの一部に基づいています。あらかじめ定義されているフィルターが要件に合っていない場合は、これらのイベントのいずれかを使用してアラートを作成します。

Logger 5.1より、システムヘルスイベントが生成される形式が変更され、より意味のある情報が提供されるようになりました。以下の変更が含まれています。

- 新しいイベントの追加 (たとえば、Current and Voltage)。
- `name`フィールドですべてのシステムヘルスイベントをLogger内部イベントとして参照する代わりに、意味のあるイベント名が使用されます (例: Fan OK、Temperature OK)。
- `agentSeverity`フィールドに、各イベントの3つの緊急度レベルとして、1 (OK)、5 (Degraded)、8 (Severe) が追加されました。
- `deviceCustomString`フィールドと`deviceCustomStringLabel`フィールドのマッピングが変更されました。変更内容については、各イベントを参照してください。
- イベントのデバイスイベントクラスID (`deviceEventClassId`) とデバイスイベントカテゴリ (`deviceEventCategory`) が変更されました。更新されたリストを次の表に示します。
- すべてのハードウェア関連のイベントは`hardware:nnn`イベントとして分類されます。ここで、nnnは、ハードウェアコンポーネントを示す3桁の数です (たとえば、`hardware:13x`はファンイベントを示します)。

システムヘルスイベントの操作では、次の点に注意してください。

- 各イベントのセンサー名はハードウェア固有であるため、各種Loggerプラットフォームで一貫していません。センサーのステータスを判定するには、イベント名 (Name) フィールドおよびステータス (CustomString3) フィールドを使用してください。rawステータス (CustomString4)、場所 (CustomString5)、およびセンサー名 (CustomString6) フィールドは、ハードウェアの問題を診断するための情報として使用するためのものであり、異なる種類のアプライアンス間での一貫性はありません。
- ユーザーに表示するアラートが頻繁になりすぎないように、特定のシステムヘルスイベントに対するカスタムアラートを作成することをお勧めします。システムがアラートを発行する一部の条件は、自動的に解消されるものであったり、特定の数の警告が生成されるまでアラートを表示したくない警告である可能性があります。

両方のタイプのLoggerで使用できるシステムヘルスイベント

グループ	デバイスイベントカテゴリ	デバイスイベントクラスID
CPU	/Monitor/CPU/Usage	cpu:100
Disk	/Monitor/Disk/Read	disk:102
	/Monitor/Disk/Write	disk:103
EPS	/Monitor/Receiver/EPS/All	eps:100
	/Monitor/Receiver/EPS/Individual	eps:102
	/Monitor/Forwarder/EPS/All	eps:101
	/Monitor/Forwarder/EPS/Individual	eps:103
Memory	/Monitor/Memory/Usage/Platform	memory:100
Network	/Monitor/Network/Usage/In	network:100
	/Monitor/Network/Usage/Out	network:101
Search	/Monitor/Search/Performed	search:100
Storage Group	/Monitor/StorageGroup/Space/Used **注:** ストレージグループのサイズ (「`fsize`」フィールドに表示) の単位はGBです。	storagegroup:100

Loggerアプライアンス専用のシステムヘルスイベント

グループ	デバイスイベントカテゴリ	デバイスイベントクラスID
Battery	/Monitor/Sensor/Battery/OK	hardware:121**
	/Monitor/Sensor/Battery/Degraded	hardware:122**

グループ	デバイスイベントカテゴリ	デバイスイベントクラスID
	/Monitor/Sensor/Battery/Failed	hardware:123**
Current (Electrical)	/Monitor/Sensor/Current/OK	hardware:101**
	/Monitor/Sensor/Current/Degraded	hardware:102**
	/Monitor/Sensor/Current/Failed	hardware:103**
Disk	/Monitor/Disk/Space/Remaining/Root	disk:101
Fan	/Monitor/Sensor/Fan/OK	hardware:131
	/Monitor/Sensor/Fan/Degraded	hardware:132
	/Monitor/Sensor/Fan/Failed	hardware:133
Power Supply	/Monitor/Sensor/PowerSupply/OK	hardware:141
	/Monitor/Sensor/PowerSupply/Degraded	hardware:142
	/Monitor/Sensor/PowerSupply/Failed	hardware:143
RAID	/Monitor/RAID/Controller/OK	raid:101
	/Monitor/RAID/Controller/Degraded	raid:102
	/Monitor/RAID/Controller/Failed	raid:103
	/Monitor/RAID/BBU/OK	raid:111
	/Monitor/RAID/BBU/Degraded	raid:112
	/Monitor/RAID/BBU/Failed	raid:113
	/Monitor/RAID/Disk/OK	raid:121
	/Monitor/RAID/Disk/Rebuilding	raid:122
	/Monitor/RAID/Disk/Failed	raid:123
Temperature	/Monitor/Temperature/OK	hardware:151
	/Monitor/Temperature/Degraded	hardware:152
	/Monitor/Temperature/Failed	hardware:153
Voltage	/Monitor/Sensor/Voltage/OK	hardware:111**
	/Monitor/Sensor/Voltage/Degraded	hardware:112**
	/Monitor/Sensor/Voltage/Failed	hardware:113**

注: この表で、表記**は、イベントがHP製ではない旧モデルのアプライアンスのみで生成されることを示しています。

アプライアンスのコマンドラインインターフェイスの使用

このトピックは、Loggerアプライアンスにのみ適用されます。

LoggerアプライアンスのCLIでは、アプライアンスの起動や停止、Loggerアプリケーションのコマンド発行を行うことができます。

アプライアンスのコマンドラインインターフェイス (CLI) に接続するには、以下のいずれかの方法を使用します。

- ProLiant Integrated Lights-Out (iLO) にログインし、リモートコンソール機能を起動します。詳細については、『Loggerインストールガイド』を参照してください。
- キーボードとモニターをアプライアンスのリアパネルにあるポートに接続します。
- DB-9コネクター付きヌルモデムケーブルを使用して、ターミナルをアプライアンスのシリアルポートに接続します。シリアルポートは、標準のVT100互換のターミナルを期待し、設定は**9600 bps**、**8ビット**、**パリティなし**、**1ストップビット** (**8N1**)、**フロー制御なし**とします。

CLIに接続すると、ログインプロンプトが表示されます。

CLIプロンプトでは以下のコマンドを使用できます。

カテゴリ	コマンド	説明
システムコマンド		
	exit	ログアウトします。
	halt	Loggerアプライアンスを停止し電源をオフにします。
	help	コマンド行インターフェイスのヘルプを開きます。
	reboot	Loggerアプライアンスを再起動します。
管理コマンド		
	show admin	デフォルト管理者ユーザーの名前を表示します。
認証コマンド		
	reset authentication	ローカル認証にリセットします。
設定コマンド		
	show config	Loggerのホスト名、IPアドレス、DNS、およびデフォルトゲートウェイを表示します。
日付コマンド		
	show date	Loggerで現在設定されている日付と時刻を表示します。

カテゴリ	コマンド	説明
	set date	Logger上の日付と時刻を設定します。日付と時刻の形式はyyyyMMddhhmmssです。日付の例: 20101219081533
デフォルトゲートウェイコマンド		
	set defaultgw <IP> [nic]	1つまたはすべてのネットワークインターフェイスのデフォルトゲートウェイを設定します。
	show defaultgw [nic]	すべてまたは指定したネットワークインターフェイスのデフォルトゲートウェイを表示します。
DNSコマンド		
	show dns	Logger上で現在設定されているDNSサーバーを表示します。
	set dns <sd> <ns> set dns <sd1>,<sd2> <ns1> <ns2>	DNSネームサーバーを設定します。 sd=検索ドメイン、ns = ネームサーバー 3台までのネームサーバーと6個までの検索ドメインを追加できます。 **注:** 複数の検索ドメインを使用する場合は、スペースではなくカンマで区切ります。複数のネームサーバーを使用する場合は、カンマではなくスペースで区切ります。
ホスト名コマンド		
	show hostname	Logger上で現在設定されているホスト名を表示します。
	set hostname <host>	Loggerのホスト名を設定します。
IPコマンド		
	show ip [nic]	すべてのネットワークインターフェイスまたは指定したネットワークインターフェイスのIPアドレスを表示します。
	set ip <nic> <IP> [/prefix] [netmask]	特定のネットワークインターフェイスについて、LoggerのIPアドレスを設定します。
NTPコマンド		

カテゴリ	コマンド	説明
	set ntp <ntp server> <ntp server> <ntp server> ...	NTPサーバーのアドレスを設定します。このエントリは、現在のNTPサーバー設定を上書きします。 NTPサーバーは必要に応じていくつでも指定できます。複数のNTPサーバーを指定した場合、サーバーは順番に確認されます。最初に応答したサーバーから取得した時刻が使用されます。 例 `logger> set ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
	show ntp	現在のNTPサーバーの設定を表示します。 例 `logger> show ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
パスワードコマンド		
	set password	現在のユーザーアカウントのパスワードを設定します。
プロセスコマンド **重要: servers**プロセスを停止しないことをお勧めします。Loggerアプライアンスをシャットダウンするには、`halt`コマンドまたは`reboot`コマンドを実行するか、UIからシステムリブートを実行します。詳細については、「システムの再起動」(492ページ)を参照してください。 イベントの受信中、Logger **servers**プロセスを停止しないでください。データ損失の原因になります。**servers**プロセスの停止が必要な場合には、**receivers**プロセスを停止してから、**servers**プロセスを停止してください。		
	restart process	プロセスを再起動します。
	start process	プロセスを起動します。
	status process	プロセスのステータスを表示します。
	stop process	プロセスを停止します。
SSL証明書コマンド		
	show sslcert	現在Loggerにロードされ**ている**SSL証明書を表示します。

カテゴリ	コマンド	説明
	reset sslcert	元のデフォルト情報に基づいて新しい自己署名証明書を作成およびインストールし、HTTPSサーバーを再起動します。
	diag sslcert	SSLセッション情報を表示します。
ステータスコマンド		
	show status	Loggerの設定を表示します。

ソフトウェアLoggerのコマンドラインオプション

このトピックは、ソフトウェアLoggerにのみ適用されます。

loggerdコマンドを使用すると、マシン上で動作しているLoggerソフトウェアを起動または停止できます。また、このコマンドには、Loggerソフトウェアの一部として動作する他のプロセスを制御するために使用可能ないくつかのサブコマンドが含まれています。

注: Loggerが、システムサービスとして動作するようにインストールされている場合は、オペレーティングシステムのserviceコマンドを使用して、Logger上のプロセスの起動、停止、ステータス確認を行うことができます。デフォルトのサービス名はarcsight_loggerです。

```
<インストールディレクトリ>/current/arcsight/logger/bin/loggerd
{start|stop|restart|status|quit}
```

```
<インストールディレクトリ>/current/arcsight/logger/bin/loggerd {start <プロセス名> |
stop <プロセス名> | restart <プロセス名>}
```

loggerdを使用して起動、停止、再起動できるプロセスを表示するには、最上位のメニューバーの **[システム管理]** をクリックします。次に、**[システム]** の中の **[プロセス ステータス]** をクリックします。プロセスは、右側の **[プロセス]** の下に一覧表示されます。

次の表では、loggerdで使用できるサブコマンドとその用途について説明します。

コマンド	用途
`loggerd start`	[システム] セクションと[プロセス] セクションに一覧表示されているすべてのプロセスを起動します。このコマンドは、Loggerを起動するために使用します。
`loggerd stop`	[プロセス] セクションに一覧表示されているプロセスのみを停止します。このコマンドは、loggerdを実行したまま他のすべてのプロセスを停止する場合に使用します。 **重要: servers**プロセスを停止しないことをお勧めします。Loggerをシャットダウンするには、`loggerd stop`コマンドまたは`quit`コマンドを使用します。 イベントの受信中、Logger **servers**プロセスを停止しないでください。データ損失の原因になります。**servers**プロセスの停止が必要な場合には、**receivers**プロセスを停止してから、**servers**プロセスを停止してください。

`loggerd restart`	このコマンドは、[プロセス] セクションに一覧表示されているプロセスのみを再起動します。
	
	注: `loggerd restart`コマンドを使用してLoggerを再起動する場合、「aps」プロセスのステータスメッセージに次のメッセージが表示されます。
	
	`Process 'aps' Execution failed.`
	
	メッセージは数秒後に次のように変わります。
	
	`Process 'aps' running.`

`loggerd status`	すべてのプロセスのステータスを表示します。
`loggerd quit`	[システム] セクションと[プロセス] セクションに一覧表示されているすべてのプロセスを停止します。このコマンドは、Loggerを停止するために使用します。
`loggerd start <プロセス名>`	指定したプロセスを起動します。例: `loggerd start apache`
`loggerd stop <プロセス名>`	指定したプロセスを停止します。例: `loggerd stop apache`
`loggerd restart <プロセス名>`	指定したプロセスを再起動します。例: `loggerd restart apache`

ファイアウォールルール

このトピックは、ソフトウェアLoggerとLoggerアプライアンス両方に適用されます。

Loggerがデータを受信できるようにするには、一部のポートをファイアウォールで開く必要があります。

- ソフトウェアLoggerの場合、ファイアウォールの設定はユーザーが行います。Logger 6.4の初回インストールまたはアップグレードが完了したら、「デフォルトの受信ポート」(559ページ)で指定されたポートのみを開く設定をファイアウォールで行い、さらに他に必要なポートがあれば設定を行います。

注意: HPE ArcSightは、必要なポートだけを開くようにファイアウォールを設定することを強くお勧めします。

- Loggerアプライアンスの場合、ファイアウォールは設定済みです。HPE ArcSightでは、ファイアウォールの更新に使用できるスクリプトが用意されています。詳細については、「Loggerアプライアンスでのファイアウォール設定」(559ページ)を参照してください。

ヒント: Logger受信者やSNMPポーリングなど、受信トラフィック用にオープンポートを必要とするサービスを追加または削除する場合には、必ずファイアウォールの設定を更新してください。

Loggerでは、他のサーバーと同じ方法でファイアウォールを設定できます。適切なポートのホワイトリストを`iptables` (CentOSおよびRHEL 6.X) または`firewalld` (CentOSおよびRHEL 7.X) で指定してください。

デフォルトの受信ポート

サービス	Loggerアプライアンス	ソフトウェアLogger rootインストール	ソフトウェアLogger root以外でのインストール
SSH	22/TCP	—	—
HTTPS	443/TCP	443/TCP	9000/TCP *
ArcMCエージェント	7913/TCP	7913/TCP	7913/TCP
NTP	123/UDP	—	—
UDP受信者	514/UDP *	514/UDP *	8514/UDP *
TCP受信者	515/TCP *	515/TCP *	8515/UDP *

* 設定ポートは上記と異なる場合があります。

Loggerアプライアンスでのファイアウォール設定

このトピックは、Loggerアプライアンスにのみ適用されます。

Loggerアプライアンスでは、ファイアウォールの設定に使用できるスクリプトが用意されています。このスクリプトは、現在のLogger設定をチェックし、オープンにしておく必要があるポートを判定します。または、Loggerでは、他のサーバーと同じ方法でファイアウォールを設定することができます。適切なポートのホワイトリストを`iptables` (CentOSおよびRHEL 6.X) または`firewalld` (CentOSおよびRHEL 7.X) で指定してください。

引数を指定しないで`/usr/sbin/arcfirewall`スクリプトを実行すると、オープンにしておく必要があるポートが表示されますが、ファイアウォール設定は変更されません。ファイアウォール設定を変更するには、`--set`オプションを指定します。

スクリプトによって開かれるポートを一覧表示するには

1. rootでアプライアンスにログインします。
2. 以下のコマンドを実行します。

```
/usr/sbin/arcfirewall
```

--setオプションを指定してスクリプトを実行した場合に開かれるポートが表示されます。

ファイアウォールを設定するには

1. rootでアプライアンスにログインします。
2. 以下のコマンドを実行します。

```
[root@myserver ~]# /usr/sbin/arcfirewall --set
```

スクリプトによってファイアウォールが設定され、オープンにしておく必要があるポートのみが開きます。

システム管理タスク

システム管理の章から、タスクを一覧表示します。

システムタスク

システムロケールを表示するには

システムを再起動またはシャットダウンするには

DNS設定を変更するには

ホスト情報を変更するには

NICを設定または設定変更するには

静的ルートを追加、編集、削除するには

システム時刻、日付、タイムゾーンを手動で設定または変更するには

システムをNTPサーバーとして設定するか、システムでNTPサーバーを使用するように設定するには

SMTPの設定を追加または変更するには

Loggerライセンスを更新するには

Loggerアプライアンスを更新するには

[プロセス ステータス] ページを表示するには

サービスとして起動されるようにLoggerを設定するには

SNMP通知の送信先を設定するには

SSHアクセスの有効化と無効化

SSHを使用したアプライアンスへの接続

ログタスク

監査ログを表示するには

監査イベントを特定のESM通知先に転送するには

ストレージタスク

リモートファイルシステムマウントを追加するには

リモートファイルシステムマウントを編集するには

リモートファイルシステムマウントを削除するには

LUNに接続するには

LUNを切断するには

LUNに再接続するには

LUNを破棄するには

SANをリストアするには

マルチパスを有効にするには

multipathdサービスがブート時に起動するよう設定されていることを確認するには

シングルパスLUNをマルチパスに変換するには

[General Controller Information] 画面を表示するには

セキュリティタスク

自己署名証明書を生成するには

証明書署名要求を生成するには

証明書をインポートするには

SSLクライアントをサポートするようにLoggerを設定するには

信頼済みの証明書をアップロードするには

CRLファイルをアップロードするには

FIPSモードを有効または無効にするには

SmartConnectorをFIPS準拠にするには

ユーザ/グループタスク

セッションの設定を変更するには

パスワード設定を変更するには

ユーザーをパスワードの有効期限ポリシーから除外するには

パスワードをリセットするには

外部認証を有効にするには

ローカルパスワード認証を設定するには

クライアント証明書認証を設定するには

クライアント証明書とパスワード認証を設定するには

LDAP Over SSL認証を設定するには

RADIUS認証設定を設定するには

認証失敗時にログインするには

ログインバナーをカスタマイズするには

新しいユーザーを追加するには

ユーザーを編集するには

ユーザーを削除するには

ユーザーをアクティブ化するには

Loggerの権限をユーザーに割り当てるには

ユーザーのパスワードをリセットするには

パスワードを変更するには

新しいユーザーグループを作成するには

ユーザーグループを編集するには

ユーザーグループを削除するには

その他のタスク

システムヘルスイベントの通知を設定するには

<<<text: コマンドラインインターフェイスに接続するには (3つのオプション)>>>

<<<text: loggerコマンドを使用して起動、停止、再起動できるプロセスを表示するには>>>

付録A: 検索演算子

以下のトピックでは、検索ボックス (**[分析] > [検索]**) で指定できる演算子について説明し、その使用方法の例を示します。

アグリゲーション演算子は複数フィールドの組み合わせ結果を返します。この演算子は「chart」(565ページ) 、「head」(578ページ) 、「keys」(579ページ) 、「rare」(586ページ) 、「sort」(593ページ) 、「tail」(594ページ) 、「top」(594ページ) を含みます。詳細については、「集計関数」(566ページ) を参照してください。

cef (非推奨)

5.2よりも前のLoggerでは、インデックス作成された検索フィルター (クエリ式の最初のパイプラインの前のクエリ部分) に一致したCEFイベントからCEFフィールドを抽出するには、演算子cefを使用してから、それらのフィールドを処理する他の検索演算子を使用する必要がありました。しかし、Logger 5.2から、明示的にCEFフィールドを抽出してから他の検索演算子をそれらのフィールドに適用する必要がなくなりました。イベントフィールドを直接クエリで指定できます。

一致するCEFイベントから指定したフィールドの値を抽出します。イベントが非CEFの場合、フィールド値にNULLが設定されます。

構文

```
...| cef <field1> <field2> <field3> ...
```

使用上の注意

複数のフィールドを指定する場合は、各フィールド名を空白またはカンマで区切ります。

CEFフィールドの名前を識別するには、検索ビルダーツールを使用して ([検索] テキストボックスの下の [検索の詳細設定] をクリックします)、すべてのフィールドの名前をアルファベット順に一覧表示します。

抽出したフィールドは、[システムフィールドセット] の [すべてのフィールド] ビューの追加の列として表示されます。抽出した列のみを表示するには、[システムフィールドセット] リストから **[ユーザ定義フィールド]** を選択します。

例

```
...| cef categorySignificance agentType
```

```
...| cef deviceEventCategory name
```

chart

検索結果を、指定したフィールドのグラフ形式で表示します。

構文

```
...| chart count by <field1> <field2> <field3> ...[span [<time_field>]=<time_bucket>]
```

```
...| chart {{sum | avg | min | max | stdev | perc<N>} (<field>)}+ by <field1>, <field2>, <field3> ...[span [<time_field>]= <time_bucket>]
```

```
...| chart {<function> (<field>)} as <new_column_name> by <field> [span [<time_field>]=<time_bucket>]
```

<field>、<field1>、<field2>は、グラフ化するフィールドの名前です。各フィールドには、Loggerスキーマで使用可能なイベントフィールドか、クエリの前半でrexまたはeval演算子を使用して作成したユーザー定義フィールドのいずれかを使用できます。

<time>は、イベントをグループ化するためのバケットサイズです。日にはd、時間にはh、分にはm、秒にはsを使用します。たとえば、2h、5d、1mのように指定します (詳細は、「使用上の注意」を参照してください)。

<function>には、count、sum、avg（またはmean)、min、max、stdev、percNのうちのいずれかを指定します。

<new_column_name>は、この機能の結果を表示する際に列に割り当てる名前です。たとえばTotalと指定します。

<N>はパーセンタイル値であるため、0～100の値 (0と100を含む) を使用できます。

廃止予定: 以下の非推奨の使用方法には「_count」が含まれています。前述のように、推奨される使用方法は「count」です。

```
...| chart _count by <field1> <field2> <field3> ...
```

使用上の注意

デフォルトでは、縦棒グラフが表示されます。他の種類のグラフとして選択できるのは、横棒グラフ、折れ線グラフ、ドーナツグラフ、面グラフ、積み上げ棒グラフ、積み上げ横棒グラフです。

グラフの設定 (その種類を含む) を変更するには、画面の [結果グラフ] フレームの右上隅にある  をクリックします。以下の設定を変更できます。

- **グラフタイトル:** グラフの意味のある名前を入力します。
- **タイプ:** カラム、棒、円グラフ、エリア、ライン、積み上げカラム、積み上げ棒グラフです。最後の2種類を選択すると、複数の値が積み上げられた、複数値の積み上げグラフが作成されます。これらのグラフは、以下で説明する多系列のグラフを表現するためのもう1つの方法です。
- **表示制限:** プロットする一意の値の数。デフォルト値: 10

  [表示制限] の設定値が、あるクエリに対する一意の値の数よりも小さい場合、上位の値が [表示制限] の設定値と等しい数だけプロットされます。つまり、表示制限が5で、一意の値が7個見つかった場合、上位5個の値のみがプロットされます。

「count by」を除くすべてのchartコマンドは、入力として1つのフィールドのみを受け付けます。指定したフィールドには、数値が含まれている必要があります。

複数のフィールドを指定する場合は、フィールド名を空白またはカンマで区切ります。

グラフに表示されている値をクリックして、指定したフィールド値を持つイベントを素早く絞り込むことができます。詳細については、「グラフのドリルダウン」(131ページ) を参照してください。

パーセンタイル関数

perc<N>関数は、<N>パーセンタイルを返します。<N>は、0～100の数値です (0と100を含む)。

...| chart perc by <field1> <field2> <field3> ... (<N>を指定しない) では、...| chart count by <field1> <field2> <field3> ...で生成されたすべての結果が返されます。

...| chart perc50 by <field1> <field2> <field3> ...では、...| chart count by <field1> <field2> <field3> ...で生成されたすべての結果の中央値が返されます。

...| chart perc90 by <field1> <field2> <field3> ...では、...| chart count by <field1> <field2> <field3> ...で生成されたすべての結果の90パーセンタイル値が返されます。

パーセンタイル値は、フィールド値の昇順に基づいて導き出されます。文字列フィールドの派生値では、アルファベット順 (ASCII値) が使用されます。

集計関数

注: 集計関数は、数値フィールドのみに使用できます。指定したフィールドには、数値が含まれている必要があります。指定したフィールドのデータ型が正しくない場合、次のようなエラーメッセージが表示されます。「java.lang.NumberFormatException」

count、sum、avgなどの集計関数が指定されている場合、集計結果のグラフが表示されるとともに、集計操作の表形式の結果が結果表に表示されます。たとえば、集計関数sum

(deviceCustomNumber1)では、結果表のsum_deviceCustomNumber1列に、deviceCustomNumber1フィールドの一意の値の合計が表示されます。

このフィールドに2つの一意の値1と20があり、それぞれ2回出現する場合、sum_deviceCustomNumber1列にはそれら2つの値の合計が表示されます。

注: グラフに表示されるイベントが多すぎると、見にくくなります。そのため、返されるイベントの数がデフォルトでは500個に制限されています。デフォルト値を変更する必要がある場合は、カスタマーサポートにお問い合わせください。

数値演算子avgとmeanは同じです。

複数の機能を同じchartコマンドに含めることができます。その場合、次の例のように各機能をカンマで区切ります。

```
...| chart count, sum(deviceCustomNumber3) by deviceEventClassId
```

複数の機能を含める場合は、機能ごとに1個の列が検索結果表に表示されます。しかし、結果グラフには、「by」句で指定したフィールドのグラフがプロットされます。

次の例のように、「as new_column_name」句を使用して、集計関数で得られた任意の列に名前を付けることができます。

```
...| chart sum(deviceCustomNumber3) as TotalStorage, avg(deviceCustomNumber3) as
AverageStorage by deviceCustomNumber3
```

新たに定義された列は、他のフィールドと同様にパイプラインで使用できます。例:

```
...| chart sum(deviceCustomNumber3) as TotalStorage, avg(deviceCustomNumber3) as
AverageStorage by deviceCustomNumber3 | eval UpdatedStorage = TotalStorage + 100
```

chart演算子の検索結果をエクスポートするとき、新たに定義した列名 (chart function as new_column_nameコマンドを使用) が保持されます。

多系列グラフ

多系列グラフでは、複数の集計関数の値を1つのグラフにプロットできます。複数の集計関数をchartコマンドに含めると、Loggerは、指定した集計関数の値をY軸に沿ってプロットする多系列グラフを生成します (「例2」(569ページ) を参照)。多系列グラフは、ドーナツグラフ以外のどの種類のグラフでも使用できます。たとえば、多系列グラフを積み上げグラフ (積み上げ棒グラフまたは積み上げ横棒グラフ) としてプロットすることを選択できます。この場合、複数の値が積み上げられた形でプロットされます。

span機能

イベントをグループ化する方法としては、Loggerのスキーマフィールド (または、rexまたはeval演算子で定義したフィールド) を使用する方法がありますが、これに加えて、span機能を使用すると、時間フィールド (EventTimeやdeviceReceiptTimeなど) や時間バケットでイベントをグループ化することができます。次の例で、deviceReceiptTimeは時間フィールドであり、5m (5分) は時間バケットです。

```
...| chart count by deviceEventCategory span (deviceReceiptTime) = 5m
```

span機能で時間フィールドが指定されていない場合、EventTimeがデフォルトとして使用されます。たとえば、次のクエリはデフォルトでEventTimeを使用します。

```
...| chart count by deviceEventCategory span = 5m
```

デフォルトでは、chartコマンドは最初の10個の一意の値を表示します。span機能によって、10個を超える一意のグループが作成される場合、その一部は表示されません。一意のグループすべてを表示するには、[グラフ設定] で [表示制限] の値を大きくする必要があります (画面の [結果グラフ] フレームの右上隅をクリックします)。

spanを使用したグループ化は、特定の時間範囲内の発生回数を見つける場合に便利です。

あるデバイスの合計受信バイト数を5分ごとに表示するには、次の例のように5mのspanを指定します。

```
...| chart sum(deviceCustomNumber1) span=5m
```

この例では、deviceCustomNumber1フィールドがこれらのイベントの受信バイト情報を提供するものと仮定しています。

spanフィールドを使用したグループ化は、rexまたはeval演算子を使用して、Loggerスキーマに存在するイベントフィールドまたはユーザー定義フィールドと組み合わせることも、組み合わせないこともできます。spanフィールドをイベントフィールドと組み合わせて指定した場合、それらすべてのフィールドの一意のセットを使用してグループ化されます。次の例では、deviceCustomNumber3とdeviceAddressをspanとともに使用し、特定のソース (deviceAddressを使用) からの1時間のイベント数 (deviceCustomNumber3 を使用) を見つけます。

```
...| chart sum(deviceCustomNumber3) by deviceAddress span=1h
```

クエリにspanが含まれている場合、検索結果は指定した時間バケットでグループ化されます。たとえば、span=5mの場合、検索結果には、5分ごとに1つの行が含まれます。特定の5分間の間にイベントがない場合、その行は空になります。

また、span機能では、1年を通じて1日が24時間であることが仮定されます。span=1dまたは24hの場合、サマータイムの変更日には、検索結果内のspan_eventTimeフィールドによって示されるイベント時刻は、前の日と1時間違います。1日に23時間しかない日 (3月) でも、ス

パンバケットには過去24時間のイベントが含まれます。同様に、1日に25時間ある日 (11月) でも、スパンバケットには過去24時間のイベントが含まれます。

例1

デフォルトのグラフ設定 (縦棒グラフ) を使用して複数のフィールドを指定します。この例では、deviceEventCategoryおよび名前フィールドの一意のグループの数が表示およびプロットされます。

```
...| chart count by deviceEventCategory name
```

例2

これらの機能の複数の値を単一のグラフのY軸に沿ってプロットする多系列グラフを生成するために、averageとsumをchartコマンドに含めます。多系列グラフを積み上げグラフ (積み上げ棒グラフまたは積み上げ横棒グラフ) としてプロット表示し、複数の値が積み上げられた形でプロットするには、**グラフ設定**を変更します。

dedup

検索結果から重複するイベントを削除します。つまり、指定したフィールド内に同じ値を含むイベントが削除されます。最初の一致イベントが保持され、指定したフィールドの値が同じ以降のイベントが削除されます。

構文

```
...| dedup [N] <field1>,<field2>, ...[keepevents=(true|false)] [keepempty=
(true|false)]
```

Nは、オプションで保持する重複イベントの数を指定する数値です。たとえば、「dedup 5 deviceEventClassId」は、それぞれのdeviceEventClassIdについて、deviceEventClassIdの値が同じ最初の5個のイベントを保持し、その後の一致イベントを削除します。デフォルト値: **1**。

field1、field2は、フィールドまたはカンマ区切りのフィールドリストであり、その値を比較して重複イベントを判定します。フィールドリストが指定されている場合、それらすべてのフィールドの一意のセットを使用してイベントが削除されます。たとえば、nameとdeviceCustomNumber1が指定され、2つのイベントに「Network Usage - Outbound」と「2347896」が含まれている場合、最初のイベントのみが検索結果で保持されます。

keepeventsは、フィールドリストで指定されたフィールドにNULLを設定するかどうかを指定します。このオプションにTrueが設定された場合、値はNULLに設定され、イベントは検索結果から削除されません。しかし、このオプションにFalseが設定されている場合、重複するイベントは検索結果から削除されます。デフォルト値: False。

keepemptyは、指定されたフィールドにNULL値が含まれているイベントを検索結果に保持するかどうかを指定します。このオプションにTrueが設定されている場合、NULL値を含むイベン

トが保持されますが、Falseが設定されている場合、NULL値を含むイベントは削除されます。デフォルト値: False。

例1

一意のデバイスからのイベントを表示するには

```
...| dedup deviceAddress
```

例2

一意のデバイスからの一意のdeviceEventClassIdを含むイベントを表示するには

```
...| dedup deviceEventClassId deviceAddress
```

例3

messageフィールドにJava例外を含むイベントのclassNameを表示するには

```
exception | <rex_expression> | dedup 5 className
```

上の例で、<rex_expression>は詳しく示されていませんが、この式はclassNameという名前のフィールド中のクラス名を抽出し、それをdedup演算子が処理します。

eval

指定した式の結果を評価した後でイベントを表示します。この式には、数式、文字列、論理演算を指定でき、クエリの実行時に評価されます。式の結果の値は、フィールド名 (式の中で指定) に割り当てられます。クエリ中のeval演算子によって新しいフィールドが定義されると、このフィールドをクエリで使用して、さらに検索結果を絞り込むことができます (以下の「例3」(575ページ)では、新しいフィールド「Plus」をeval演算子で定義し、このフィールドをsort演算子で使用しています)。

構文

```
...|eval <type> <newField>=function([<field>|<value>]*)
```

ここで、

<newField>は、検索結果に表示される派生フィールドです。

<type>は新しいフィールドのデータ型で、int、bigint、long、float、またはdoubleの値を取ります。データ型を含めない場合、デフォルトは文字列です。<type>を含めるかどうかは任意です。文字列以外のデータ型が必要な場合は、<type>を含めます。たとえば、<type>を含めない場合、ソートはアルファベット順になります。数値でソートする必要がある場合は、<type>をいずれかの数値データ型にします。指定するデータ型は、標準的なデータ型の定義に従って、<newField>に表示されるデータと一致している必要があります。一時的なフィール

ドはLoggerスキーマに含まれないため、そのデータ型が<field>のLoggerスキーマのデータ型と一致している必要はありません。

<function>は次のうちのいずれかです。abs(X)、case(X,"Y",...)、ceil(X)、ceiling(X)、exp(X)、floor(X)、if(X,Y,Z)、isfalse(X)、istrue(X)、len(X)、ln(X)、log(X)、lower(X)、tolower(X)、mod(x,y)、rand()、replace(X,Y,Z)、round(X)、sqrt(X)、substr(X,Y,Z)、sum(x,y,z,…)、trim(X)、ltrim(X)、rtrim(X)、upper(X)toupper(X)、urldecode(X)

注: これらの関数については、以下の「使用上の注意」で詳しく説明します。

<field>はユーザーが評価するフィールドの名前です。フィールドには、Loggerスキーマで使用可能なイベントフィールドか、クエリの前半でrexまたはeval演算子を使用して作成したユーザー定義フィールドのいずれかを使用できます。

<value>は文字列または数値です。

eval式でサポートされている演算子

オペレーション	記号
加算、減算	+, -
乗算、除算	*, /
ブールのAND、OR、NOT	&&, ||, !
等しい、等しくない	==, !=
小なり、大なり	<, >
以下、以上	<=, >=
剰余、べき乗	%, ^
単項プラス、単項マイナス	+x, -x

使用上の注意

一般的には、cefまたはrex演算子 (一致イベントからフィールドを抽出する) は、下の例のようにeval演算子よりも前に使用します。しかし、クエリ内の先行するeval演算子によって定義されたフィールドに対してeval演算子を使用することができます。

eval演算子を使用するときには、以下の点に注意してください。

- 関数では、文字列のリテラル値またはフィールドを使用できます。
- Xがリテラル文字列であることを示すには、Xを二重引用符で囲みます ("X")。二重引用符がない場合、関数はXがフィールドであるとみなします。
- 文字列フィールドの派生値では、アルファベット順 (ASCII値) が使用されます。

eval演算でサポートされる関数

関数	説明	例
abs(X)	数値 (X) を取り、その絶対値を返します。	この関数は、評価した値を新しいフィールドに割り当てます。Xの値が3または-3の場合、この関数は評価した値である3をフィールドabsnumに割り当てます。 `...| eval absnum=abs(number)`
case(X,"Y",...)	引数のペア (XとY) を取ります。 引数Xは、最初から最後の順に評価される複数のブール式です。条件を満たす最初のX式が見つかると、それに対応するYが返されます。その後の引数は無視されます。条件を満たすX式がない場合は、Nullを返します。	次の例では、deviceCustomNumber1が200かどうかに応じて、outcome =Successまたはoutcome =Failureが返されます。 `...| eval outcome=case (deviceCustomNumber1== 200, "Success", deviceCustomNumber1 != 200, "Failure")`
ceil(X)、ceiling(X)	数値 (X) を最も近い整数に切り上げます。	次の例ではn=2を返します。 `...| eval n=ceil(1.9)`
exp(X)	数値 (X) を取り、eXを返します。	次の例ではy=e3を返します。 `...| eval y=exp(3)`
floor(X)	数値 (X) を最も近い整数に切り下げます。	次の例では1を返します。 `...| eval n=floor(1.9)`
if(X,Y,Z)	3つの引数を取ります。最初の引数 (X) は、ブール式である必要があります。XがTRUEと評価されると、結果は2番目の引数 (Y) になります。XがFALSEと評価されると、結果は3番目の引数 (Z) になります。	次の例は、deviceCustomNumber1の値を参照し、outcome=200の場合は、outcome=Succeededを返します。それ以外の場合は、outcome=Failedを返します。 `...| eval outcome=if(deviceCustomNumber1 == 200, "Succeeded", "Failed")`
isfalse(X)	式XがFalseかどうかを確認します。式XがFalseの場合Trueを、そうでない場合はFalseを返します。 **注:** X > 0の場合、結果はFalseです。X <=0の場合、結果はTrueです。	次の例では、4+4は9と等しくないため、Trueが返されます。 `...| eval newField = isfalse(4+4==9)`

eval演算でサポートされる関数 (続き)

istrue(X)	式XがTrueかどうかを確認します。式XがTrueの場合Trueを、そうでない場合はFalseを返します。 **注:** X > 0の場合、結果はTrueです。X <=0の場合、結果はFalseです。	次の例では、8は0より大きいため、Trueが返されます。 `...| eval newField = istrue(8)`

len(X)	文字列 (X) の文字数を返します。	次の例では、(field) の文字数が返されます。このフィールドの文字数が256文字である場合、n=256が返されます。
		`...| eval n=len(field)`
		次の例ではn=3を返します。(abcは二重引用符で囲まれたリテラルな文字列です。)
		`...| eval n=len("abc")`

ln(X)	数値 (X) を取り、その自然対数を返します。	次の例では、「bytes」の値の自然対数が返されます。「bytes」に100が含まれる場合、4.605170186が返されます。 `...| eval lnBytes=ln(bytes)`
log(X)	数値Xの10を底とする対数を評価します。	次の例では4を返します。 `...| eval num=log(10000).`
lower(X) tolower(X)	文字列の引数 (X) を取り、その小文字バージョンを返します。	次の例では、フィールドusernameの値が小文字で返されます。usernameフィールドにFRED BROWNが含まれている場合、name=fred brownが返されます。 `...| eval name=lower("username")`
mod(X,Y)	XをYで割った後の余りを返します (X%Yは、XをYで割った余りです)。	次の例では5を返します。 `...| eval newField = mod(25,10)`
rand()	0〜1の間 (0と1を含む) のランダムな数値を返します。	次の例では、0.56789のような数値が返されます。 `...| eval newField = rand()`
replace(X,Y,Z)	文字列X内の正規表現文字列Yをすべて文字列Zに置き換えた文字列を返します。3番目の引数 (Z) は、正規表現で照合するグループを参照することもできます。	次の例では、deviceVendorフィールド内の値「ArcSight」が値「HP」に置き換えられます。 `...| eval n=replace(deviceVendor, "ArcSight", "HP")`

eval演算でサポートされる関数 (続き)

round(X)	Xを最も近い整数に丸めます。	次の例では1を返します。
		`...| eval n=round(1.4)`
		次の例では2を返します。
		`...| eval n=round(1.5)`

sqrt(X)	数値の引数 (X) を1つ取り、その平方根を返します。	次の例では3を返します。 `...| eval n=sqrt(9)`

substr(X,Y,Z)	この関数は、文字列Xの部分文字列である新しい文字列を返します。部分文字列はインデックスYの文字から始まり、インデックスZ-1の文字まで続きます。
	注: インデックスは文字列Xの文字の場所を示す数で、0から始まり、左から右に数えます。
		次の例では「g」を返します。
		`...| eval n=substr("ArcSight",5,6)`
		次の例では「cSig」を返します。
		`...| eval n=substr("ArcSight",2,6)`
		次の例では「ght」を返します。
		`...| eval n=substr("ArcSight",5,8)`
		次の例では「ArcSight」を返します。
		`...| eval n=substr("ArcSight",0,8)`
		次の例では「Sight」を返します。
		`...| eval n=substr("ArcSight",3,8)`
		次の例では「Arc」を返します。
		`...| eval n=substr("ArcSight",0,3)`

sum(X,Y,Z,…)	数値をすべて足します。	次の例では、baseEventCount、deviceCustomNumber1、およびdeviceCustomNumber2フィールドの値の合計が返されます。 `...| eval newnum = sum(baseEventCount, deviceCustomNumber1, deviceCustomNumber2)`

eval演算でサポートされる関数 (続き)

trim(X)
ltrim(X)
rtrim(X)
	trim(X) は、文字列Xの両側のスペースをすべて削除します。
	ltrim(X) は、文字列Xの左側のスペースをすべて削除します。
	rtrim(X) は、文字列Xの右側のスペースをすべて削除します。
		ここでは例のため、Xがリテラル文字列で、_が任意の数のスペース文字を表すものとします。
		次の例ではtrimmed="string_"を返します。
		`...| eval trimmed=ltrim("_string_")`
		次の例では trimmed="_string"を返します。
		`...| eval trimmed=rtrim("_string_")`
		次の例では"string"を返します。
		`...| eval trimmed=trim("_string_")`

upper(X) toupper(X)	文字列の引数を1つ取り、その大文字バージョンを返します。	次の例では、フィールドusernameの値が大文字で返されます。usernameにfred brownが含まれている場合、name=FRED BROWNが返されます。 `...| eval name=upper("username")`
urldecode(X)	URL文字列の引数Xを1つ取り、エスケープまたはデコードされていないURL文字列を返します。	次の例では「http://www.hp.com/download?r=header」を返します。 `...| eval n=urldecode ("http%3A%2F%2Fwww.hp.com%2Fdownload%3Fr%3Dheader")`

例1

カテゴリ動作が「Communicate」の場合、値「communicate」を新しいフィールド「cat」に割り当てます。そうでない場合は、値「notCommunicate」を割り当てます。

```
_storageGroup IN [“Default Storage Group”] | cef categoryBehavior | eval cat=if(categoryBehavior== “/Communicate”, “communicate”, “notCommunicate”)
```

例2

抽出したイベント名の末尾に単語「END」を追加します。たとえば、イベント名が「Logger Internal Event」の場合、eval演算の後は「Logger Internal EventEND」になり、新しいフィールド「fullname」に割り当てられます。

```
logger | cef msg name | eval fullname=name + “END”
```

例3

受信バイト数の値に100を加え、新しいフィールド「Plus」に割り当てます。次に、「Plus」に割り当てられた値を昇順にソートします。

```
_storageGroup IN [“Default Storage Group”] | cef bytesIn bytesOut name | eval Plus=bytesIn +100 | sort Plus
```

例4

ベンダーArcSightから最も長いURLを見つけます。

```
deviceVendor = ArcSight |eval (int)urllength=len(requestUrl) |sort urllength
```

extract

キーと値のペアをrawイベントから抽出します。

構文

```
...| extract [pairdelim="<delimiters>"] [kvdelim="<delimiters>"] [maxchars=<n>]
fields="key1,key2,key3..."
```

ここで、

- pairdelimは、イベント中の1つのキーと値のペアを、別のキーと値のペアから分離する区切り文字 (または区切り文のリスト) です。デフォルトでは、セミコロン、パイプ、カンマ (; | ,) が使用されます。
- kvdelimは、キーと値を分離する区切り文字 (または区切り文字のリスト) です。デフォルトでは「=」です。
- maxcharsは、キーと値のペアを抽出するためにスキャンするイベント内の最大文字数です。デフォルト値は10240です。
- fieldsは、検索結果に値を表示するキー (またはカンマ区切りのキーのリスト) です。

たとえば、次のイベントからName、Age、Locationの値を表示するとします。

```
Name:Jane | Age:30 | Location:LA
```

「Name」、「Age」、「Location」のキーを抽出し、fieldsリストに列挙します。

extract演算子の動作

キーはrawイベント中のフィールドを表しており、その値は、イベント中で、キーの後から次のキーまでに現れる文字からなります。この概念を説明するために次のrawイベントを使用します。

```
[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP Warning:
memcache_pconnect() [<a href='function.memcache-pconnect'>function.memcache-
pconnect</a>]: Can't connect to 10.4.31.4:11211
```

上のイベントからURLを抽出するには、イベント中のキーと値のペアを分離する、次のキーペア区切り文字を定義します。

- 大なり記号 (>)
- 角カッコ ([)

また、キーと値を分離する次のキー区切り文字を定義します。

- 等号 (=)

その結果、次のコマンドがURLを抽出します。

```
...| extract pairdelim= “>\[” kvdelim= “=" fields=“<a href”
```

イベント中のキーと値のペアは次のようになります。`[<a href='function.memcache-pconnect'>`

イベント中のキーは次のようになります。`<a href`

抽出されるURLは次のようになります。`'function.memcache-pconnect'`

使用上の注意

この演算子は、rawイベントのみに使用できます。つまり、キーと値のペアを、CEFイベントや`rex`演算子で定義されたフィールドから抽出することはできません。

extract演算子コマンドで区切り文字`pairdelim`と`kvdelim`を指定して、キーとその値を抽出できます。しかし、これらの区切り文字が生成するキー名を特定する必要がある場合は、`keys`演算子を使用します (「keys」(579ページ) を参照)。`keys`演算子は、キーを特定するためにのみ使用できます。これらのキーを`extract`演算子にパイプで渡すことはできません。つまり、...| `keys | extract fields=field1`は正しくありません。

フィールドリストで指定したキーを、さらにパイプライン演算子で使用できます。たとえば、...| `extract pairdelim= “|” kvdelim= “:” fields= “count” | top count`のようにします。

指定した`pairdelim`文字がイベント中に存在しない場合、イベントはキーと値のペアに解析されません。イベント全体がスキップされます。同様に、指定された`kvdelim`が存在しない場合、値はキーから分離されません。

区切り文字として二重引用符 (“) を指定するには、2つの二重引用符で囲み、バックスラッシュ (\) でエスケープします。たとえば、“=\”|”のようにします。同様に、バックスラッシュ文字を文字どおり扱うには、2個のバックスラッシュを使用します。たとえば、“\\”のようにします。

例

```
...| extract pairdelim= “|” kvdelim= “:” fields= “Name,Age,Location”
```

これは、次の形式のイベントから値を抽出します。

Name:Jane | Age:30 | Location:LA

fields

検索結果に指定したフィールドを含めるか除外します。

構文

```
...| fields ([(+ | -)] <field>)+
```

ここで、

+は、指定された1つ以上のフィールドを検索結果に含めます。これがデフォルトです。

-は、指定された1つ以上のフィールドを検索結果から除外します。

使用上の注意

一般に、<field>リストには、Loggerスキーマで使用できるイベントフィールドか、クエリの先行部分でrex演算子を使用して作成したユーザー定義フィールドが含まれます (次の例を参照)。しかし、eval演算子などの他の演算子でフィールドを定義することもできます。

複数のフィールドを指定する場合、+と-は同じ式で使用できます。例:
```
| fields + name - agentType
```

> **ヒント:** この演算子では、完全なフィールド名を指定する必要があります。フィールド名の中のワイルドカードはサポートされていません。

この演算子がクエリに含まれている場合、検索結果を表示するには、[システムフィールドセット] リストから **[ユーザ定義フィールド]** を選択します。

例1

```
...| fields - agentType + categorySignificance
```

例2

```
...| fields - name
```

head

検索結果の最初の<N>行を表示します。

構文

```
...| head [<N>]
```

<N>は表示する行数です。デフォルト値: <N>が指定されない場合は**10**。

使用上の注意

この演算子がクエリに含まれている場合、検索結果をプレビューできません。つまり、検索結果を表示する前にクエリの実行が完了している必要があります。

例

```
...| head
```

keys

指定した区切り文字に基づいて、rawイベント内のキーを識別します。

構文

```
...| keys [pairdelim= “<delimiters>”] [kvdelim= “<delimiters>”] [limit=<n>]
```

ここで、

- pairdelimは、イベント中の1つのキーと値のペアを、別のキーと値のペアから分離する区切り文字 (または区切り文のリスト) です。デフォルトでは、セミコロン、パイプ、カンマ (; | ,) が使用されます。
- kvdelimは、キーと値を分離する区切り文字 (または区切り文字のリスト) です。デフォルトでは「=」です。
- limitは、検索するキーと値のペアの最大数です。このパラメーターのデフォルトまたは最大値はありません。

使用上の注意

この演算子は、rawイベントのみに使用できます。つまり、キーと値のペアを、CEFイベントやrex演算子で定義されたフィールドから識別することはできません。

キーを特定するためにこの演算子は必要ありませんが、最初にこの演算子を使用し、extract演算子を使用して取得する必要がある値のキーを特定することをお勧めします。この演算子は集約された結果を返します。そのため、検索結果は、一致イベント内に見つかったキーとその数の一覧を表示します。

keys演算子は、キーを特定するためにのみ使用できます。これらのキーをextract演算子にパイプで渡すことはできません。つまり、| keys | extract fields=field1は正しくありません。

空白 (またはnull) のキー値は無視され、ヒット数にカウントされません。

たとえば、次のイベントデータを考えます。

```
Date=3/24/2011 | Drink=Lemonade
Date=3/23/2011 | Drink=
Date=3/22/2011 | Drink=Coffee
```

検索クエリ: `keys pairdelim= “|” kvdelim= “=”`

検索結果: Date, 3 hits and Drink, 2 hits

指定した`pairdelim`文字がイベント中に存在しない場合、イベントはキーと値のペアに解析されません。イベント全体がスキップされます。同様に、指定された`kvdelim`が存在しない場合、値はキーから分離されません。

区切り文字として二重引用符 (“) を指定するには、2つの二重引用符で囲み、バックスラッシュ (\) でエスケープします。たとえば、“=\”|”のようにします。同様に、バックスラッシュ文字を文字どおり扱うには、2個のバックスラッシュを使用します。たとえば、“\\”のようにします。

例1

```
...| keys pairdelim= “|” kvdelim= “=”
```

これは、次の形式のイベントのキー (DateとDrink) を識別します。
`Date=3/24/2011 | Drink=Lemonade.`

例2

```
...| keys pairdelim= “,” kvdelim= “>=”
```

これは、次の形式のイベントのキー (PathとIPAddress) を識別します。
`Path>c:\usr\log, IPAddress=1.1.1.1`

lookup

イベントのフィールドの値がアップロードしたルックアップファイル内の対応するフィールドの値と同じかどうかに基づいて、増やされたり絞り込まれたりしたイベントセットを返します。

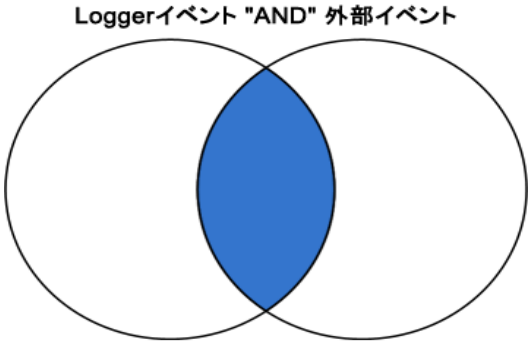
この演算子を使用する前に、ルックアップファイルをLoggerにアップロードする必要があります。ルックアップファイルを追加するには、[**リストルックアップ**] 設定ページからCSVファイルをアップロードします。

- `lookup`演算子を使用すべき場合については、「静的相関関係を通じたLoggerデータの強化」(152ページ) を参照してください。
- ルックアップファイルの作成とLoggerへのアップロードについては、「ルックアップファイル」(357ページ) を参照してください。

構文

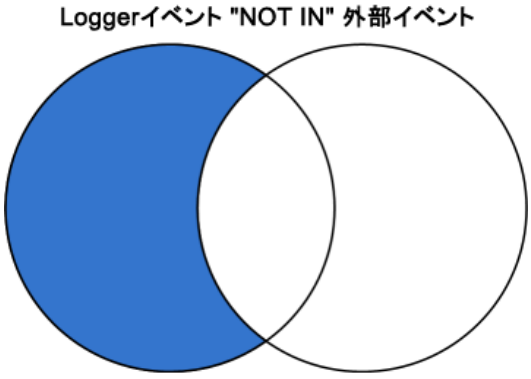
```
...| lookup [+/-/*] lookupTableName externalField1 [as loggerField1] [,
externalField2 [as loggerField2] ...][output [  *  | externalField1,
externalField2...] ]
```

プラス記号 (+) は、ルックアップフィールド (loggerField1、loggerField2) の値がアップロードしたルックアップファイルの値 (externalField1、externalField2) と同じイベントを選択します。output句が使用されている場合、アップロードされたルックアップファイル内の指定された出力列が検索結果に追加されます。+はデフォルトのlookup演算子です。+、-、*のどれも指定しないと、+が使用されます。



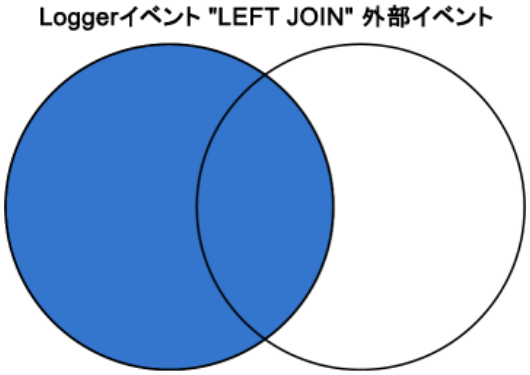
ルックアップフィールドの値が、アップロードされたルックアップファイルの複数の行に一致する場合、最初に一致した行のみが使用されます。Loggerは、ルックアップフィールドがルックアップファイルの複数の行に一致し、最初の一致のみが含まれることを示すアラートメッセージを表示します。

マイナス記号 (-) は、ルックアップフィールドの値がアップロードしたルックアップファイルに含まれないイベントを選択します。lookupをマイナス記号とともに実行した場合、結果のUIフィールドに外部フィールドが表示されません。output句は否定のlookupに適用されません。これは、否定のlookupがアップロードされたルックアップファイルからの一致を**除外**するためです。



アスタリスク (*) は、アップロードされたルックアップファイルにイベントが含まれるかどうかにかかわらず、すべてのイベントを含めます(Loggerイベントテーブルとルックアップファイルの間で左外部結合を実行します)。output句が使用された場合、ルックアップファイルのどの行にも一致しな

いLoggerイベントの出力フィールドは空 (null) になります。



+、-、*のどれも指定されなかった場合、デフォルトは+になります。

loggerField1とloggerField2は、Loggerの検索結果で有効なフィールド名です。

externalField1とexternalField2は、ルックアップファイルからの有効な列名です。

loggerField1 as externalField1は、Loggerの検索結果のloggerField1と、アップロードされたルックアップファイルのexternalField1の間の値を検索します。

検索パイプライン中の最初のlookup演算子では、loggerField1はLoggerイベント中の有効なフィールド名であることが必要です。そうでない場合、このフィールドはLoggerフィールドであるか、前のパイプライン演算子からの検索結果中の、検索で生成されたフィールドとなります。

loggerField1 as externalField1, loggerField2 as externalField2は、Loggerの検索結果とアップロードされたルックアップファイルの間で複数のフィールドに対して値の検索を実行します。

[output [* | externalField1, externalField2...]]1つ以上の外部フィールドを指定した場合、指定されたフィールドが検索結果に追加されます。output *を使用すると、アップロードされたルックアップファイルのすべてのフィールドが追加されます。output句を使用しない場合、アップロードされたルックアップファイルからのフィールドはどれも検索結果に追加されません。

使用上の注意

lookup演算子は、特定の日付/時刻形式をサポートしています。Loggerイベントフィールドは、文字列、整数、日付/時刻の3つの異なるデータ型のいずれかとなります。lookup演算子は、ルックアップフィールド内の値を対応するLoggerイベントフィールドの同じデータ型の値に変換します。

lookup演算子は、日付/時刻フィールドで以下の形式をサポートしています。

```
MM/dd/yyyy HH:mm:ss z
MM/dd/yyyy HH:mm:ss
yyyy/MM/dd HH:mm:ss z
```

```
dd/MMM/yyyy HH:mm:ss Z
dd MMM yyyy HH:mm:ss z
yyyy-M-d H:mm:ss
yyyy-MM-dd'T'HH:mm:ss
yyyy-MM-dd'T'HH:mm:ssZ
```

Loggerでは、すべてのlookup検索で約1GBのシステムメモリを使用できます。大規模なルックアップテーブルに対し、複数のlookup検索を同時に実行すると、最大で1GBのメモリを使用します。この制限に達すると、一部のlookup検索の動作が遅くなったり、タイムアウトしたりする可能性があります。他のlookup検索の実行中やメモリがフルの状態でlookup検索を開始すると、Loggerは、現在のlookup検索が終了しメモリが解放された後でlookup検索を実行することを推奨するメッセージを表示します。

ルックアップフィールドには、アップロードされたルックアップファイル中で値が一意のフィールドを選択してください。lookup処理では、一致する最初の行のみを使用し、以降の一致を無視します。そのため、ルックアップ列が一意の値を持つようにし、重複する一致が無視されないようにすることをお勧めします。

たとえば、次の検索を考えます。

```
| lookup testLU deviceVendor output status
```

ここで、ルックアップファイル「testLU」には、次のように、deviceVendorの値が同じ「ArcSight」である4つの行が含まれています。

testLU

deviceVendor	dept	org
ArcSight	sales	HPE
ArcSight	marketing	HPE
BlueCoat	sales	BlueCoatINC
ArcSight	engineering	HPE
ArcSight	marketing	ESP

lookup処理でルックアップフィールドに重複が見つかると(testLUの「deviceVendor=ArcSight」と、Loggerイベントテーブルの「deviceVendor=ArcSight」)、検索結果では最初のエントリ「status_testLU=ok」のみが一致するLoggerイベントに追加され、「status_testLU=alert」などの以降の一致は使用されません。

ヒント: まれにですが、[ルックアップ ファイルの追加] ページからルックアップファイルをアップロードした後で、空白のページが返される場合があります。この場合は、ページを手動で更新します。ページを更新すると、ローディングページに戻り、再度ルックアップファイルのロードが行われます。このファイルはすでにアップロードされているため、エラーメッセージが表示されます。このエラーは無視して問題ありません。

ルックアップファイルでのIPアドレスの使用

ルックアッププロセスでは、ルックアップファイルにIPアドレスが含まれているかどうかを自動的に判断し、IPアドレスが含まれている場合には、それらを文字列ではなくIPアドレスとして扱います。ルックアップファイルを使用して検索を行う場合、Loggerはルックアップの各列の最初の10行をチェックし、それぞれの列にIPアドレスのみが含まれているかどうかを判断します。

- 最初の10行にIPアドレスのみが含まれているルックアップ列が存在した場合、Loggerはその列の残りの行にもIPアドレスが含まれていると判断します。

  注: 同じ列の後の方にIPアドレス以外のデータが含まれていると、例外が発生することがあります。

- 最初の10行にIPアドレス以外の文字列が含まれている場合、Loggerは対応するLoggerイベント列のフィールドタイプを使用してデータ型を特定します。
- 上記のルールに基づいてルックアッププロセスがIPアドレスルックアップであると判断した場合、同じIPアドレス形式で一致するIPアドレスの検索が行われます。

たとえば、ルックアップ列の最初の10行にIPアドレス以外の内容が含まれている場合は、次のように検索が行われます。

- 文字列「2001:db8:250:0:0:fefe:0:1」の検索では、ターゲットフィールドが文字列「2001:db8:250:0:0:fefe:0:1」と完全に一致するイベントのみが検索されます。
- 文字列「192.168.10.100」の検索では、ターゲットフィールドが文字列「192.168.10.100」と完全に一致するイベントのみが検索されます。

ところが、ルックアップ列の最初の10行にIPアドレスのみが含まれている場合は、次のように検索が行われます。

- アドレス「192.0.2.010」を検索すると、「192.0.2.010」、「192.0.2.10」のようなアドレスを含むイベントが検出されます。
- アドレス「2001:db8:250:0:0:fefe:0:1」を検索すると、「2001:db8:250:0:0:fefe:0:1」、「2001:db8:250::fefe:0000:1」のようなアドレスを含むイベントが検出されます。

注: IPv6アドレスデータをLoggerに含めて検索する方法の詳細については、「IPv6データのLoggerへの送信」(31ページ)および「IPv6アドレスの検索」(121ページ)を参照してください。

例1

次の例は、ルックアップファイル「maliciousIP」の「ip」列に記されたIPアドレスとsourceAddressが等しいイベントを探します。

```
lookup maliciousIP ip as sourceAddress
```

例2

次の例は、sourcePortがday_xのsourcePortと異なるアクセスイベントを探します。day_xは、前日にエクスポートされたLoggerイベントから生成されたルックアップファイルです。

```
access | lookup - day_x sourcePort
```

parse

指定したパーサーを検索クエリの一致イベントに適用します。

構文

```
...| parse <parser_name>
```

ここで、<parser_name>は使用するパーサーの名前です。パーサーの作成方法については、「パーサーの使用」(394ページ)を参照してください。

ヒント: パーサーをクエリで使用する前に、パーサーが存在している必要があります。

parse演算子は、Logger上に格納された非CEF (構造化されていないテキスト) データを、パーサーの定義に従って解析し、特定のフィールドに分割する際に有用です。

解析してフィールドに分割すると、このデータをさらに検索操作で使用できます。たとえば、次のparse演算子は、ユーザー定義のパーサー「Web Server Access Logs」を使用してイベントを解析し、「username」、「login_status」、「num_attempts」フィールドを作成します。

これらの作成されたフィールドをさらにパイプラインクエリで使用して、ログインに失敗した回数の多い10人のユーザー名と、試行回数を表示できます。

```
...| parse Web Server Access Log | where login_status = “failed” | top
username num_attempts
```

パーサー定義はrexまたはextract式であるため、指定した式に一致する値を含めるために追加のフィールドを作成します。これらのフィールドは、rex式やextract式の結果と同様に検索結果に表示されます。そのため、上の例で、username、login_status、num_attemptの3つのフィールドが検索結果に追加されます。

parse演算子を検索クエリで使用すると、追加フィールド「parser」も検索結果に追加されます。

このフィールドには、パーサーが一致イベントの定義で指定された1つ以上のフィールドを解析できる場合、パーサーの名前が格納されます。イベントが正常に解析されなかった場合や、ソースタイプにパーサーが定義されていない場合、またはソースタイプがない場合は、このフィールドが表示され「Not parsed」が格納されます。同様に、パーサー定義が一致イベントのどのフィールドも解析できない場合、値「not parsed」が格納されます。

例

また、このフィールドを使用して、正常に解析されたか、解析されなかったイベントを探すこともできます。

```
...| parse Web Server Access Log | where parser = “not parsed”
```

使用上の注意

parse演算子を使用すべき場合: Logger上のTCPまたはUDP受信者を通じて受信した非CEFイベントは、ソースタイプに関連付けられないため、パーサー定義に関連付けられません。そのため、そのようなイベントは自動的に解析されません。同様に、Loggerバージョン5.2以前で保存された非CEFイベントも解析されません。それらのバージョンでは、パーサー機能が存在しなかったためです。そのようなイベントがクエリに一致した場合に解析する必要がある場合は、parse演算子を使用します。

定義されたソースタイプがLogger上に存在するイベントをparse演算子で解析すると、ソースタイプに関連付けられているパーサーと、parserパイプラインコマンドで指定したパーサーを通じて、複数のユーザー定義フィールドが作成される可能性があります。両方のパーサーが一意のフィールド名を作成する場合、イベントに一致するクエリが実行されるときに、それらのすべてのフィールドが作成されます。パーサーが同じ名前のフィールドを1つ以上指定した場合、parse演算子のパーサーが最初に適用されるため、このパーサーで指定したフィールド名が優先されます。

例

```
...| parse Web Server Access Log | where url CONTAINS “.org” | top url
```

rare

指定したフィールドで最も出現頻度が低い値を表形式で検索結果に表示します。つまり、値は出現数の小さいものから大きいものの順に表示されます。

複数のフィールドを指定した場合、それらすべてのフィールドの一意のセットの数が、小さいものから大きいものの順に表示されます。

構文

```
...| rare <field1> <field2> <field3> ...
```

```
Sorts the matching results from least to most common for the specified
fields.
```

使用上の注意

一般に、<field>リストには、Loggerスキーマで使用できるイベントフィールドか、クエリの先行部分でrexまたはeval演算子を使用して作成したユーザー定義フィールドが含まれます (次の例を参照)。しかし、eval演算子などの他の演算子でフィールドを定義することもできます。

この演算子がクエリに含まれていると、検索結果のグラフが自動的に生成されます。グラフに表示されている値をクリックして、指定したフィールド値を持つイベントを素早く絞り込むことができます。詳細については、「グラフのドリルダウン」(131ページ)を参照してください。

複数のフィールドを指定する場合は、フィールド名を空白またはカンマで区切ります。

例

```
...| rare deviceEventCategory
```

regex

指定した正規表現に一致するイベントを選択します。

構文

```
...| regex <regular_expression>
```

または

```
...| regex <field> (=|!=) <regular_expression>
```

使用上の注意

正規表現のパターンマッチングでは、大文字と小文字が区別されません。

最初の使用方法 (フィールド名なし) はrawイベントに適用されます。2番目の使用方法 (フィールド名あり) は指定したフィールドに適用されます。

2番目の使用方法を使用する場合は (上記および下記の例2)、Loggerスキーマで使用できるイベントフィールドか、rexまたはeval演算子を使用して作成されるユーザー定義のフィールドを指定します。

例

```
...| regex “failure”
```

```
...| regex deviceEventCategory != “fan”
```

rename

指定したフィールド名を変更します。

構文

```
...| rename <field> as <new_name>
```

ここで、

- <field>は、Loggerスキーマで使用できるイベントフィールドか、rexまたはeval演算子を使用して作成されるユーザー定義フィールドの名前です。
- <new_name>は、フィールドに割り当てる新しい名前です。

使用上の注意

名前を変更した各フィールドについて、検索結果に列が追加されます。名前を変更したフィールドに加えて、元の名前のフィールドも検索結果に引き続き表示されます。たとえば、deviceEventCategoryをCategoryに名称変更した場合、deviceEventCategoryとCategoryの2つの列が検索結果に表示されます。

ワイルドカード文字*をフィールド名に含めることができます。しかし、ワイルドカード文字を含むフィールドは二重引用符 (" ") で囲む必要があります。例:

```
...| rename “*IPAddress” as “*Address”
```

または

```
...| rename “*IPAddress” as Address
```

フィールド名に特殊文字 (_、スペース、#など) が含まれる場合は、rename演算子の式では二重引用符 (" ") で囲む必要があります。例:

```
...| rename src_ip as “Source IP Address”
```

rename操作で得られたフィールドに特殊文字が含まれる場合は、パイプライン演算子式で使用する場合に、必ず二重引用符 (" ") で囲む必要があります。例:

```
...| rename src_ip as “Source IP Address” | top “Source IP Address”
```

内部フィールド名 ("_raw"で始まります) の名前は変更できません。

名前を変更したフィールドは、クエリの間のみ有効です。

rename操作で得られたフィールドでは、大文字と小文字が区別されます。そのようなフィールドを検索操作で使用する場合は、フィールドを定義するために使用したのと同じ文字であることを確認してください。

rename式を含む検索クエリの検索結果をエクスポートする場合、結果ファイルには名称変更後のフィールドが含まれています。

例

```
...| rename src_ip as IPAddress

...| rename src_ip as “Source IP Address”
```

replace

指定したフィールドの指定した文字列を指定した新しい文字列で置換します。

構文

```
<orig_str> with <new_str> [in <field_list>]
```

ここで、

- <orig_str>は置換対象の元の文字列です。
- <new_str>は置換後の新しい文字列です。
- <field_list>はオプションですが、強く推奨されます。

使用上の注意

ヒント: このコマンドのフィールドリストはオプションですが、replace演算子がこのコマンドで操作するフィールドを指定することを強くお勧めします。

フィールドリストを省略すると、replace演算子は、replaceコマンドの前にcef、rex、およびeval演算子を使用して明示的に定義したフィールドか、replace演算子コマンドの前に指定された他の演算子コマンドで使用したフィールドを操作します。

たとえば、replaceコマンドは、以下のすべての場合にdeviceEventCategoryを操作し、「EPS」のすべてのインスタンスを「Events」で置き換えます。

```
...| replace *EPS* with *Events* in deviceEventCategory
...| cef deviceEventCategory | replace *EPS* with *Events*
...| top deviceEventCategory | replace *EPS* with *Events*
```

文字列が置換される各フィールドについて、同じ名前の列が検索結果に追加されます。値を置換した列に加えて、元の値の列も検索結果に引き続き表示されます。たとえば、「message」列で「err」を「Error」に置換した場合、変更された値が格納された「message」列が検索結果に追加されます。

文字列全体を置換する場合は、全体を指定します (イベントに表示されるとおり)。たとえば、「192.168.35.3」と指定します。

文字列の一部を置換する場合は、変更しない部分についてワイルドカード文字 (*) を使用します。

たとえば、元の文字列 (置換対象の文字列) が「192.168*」の場合、イベントの192.168の部分のみが置換されます。残りの文字列は保持されます。その結果、イベントに192.168.35.3が含まれている場合、最初の2バイトのみが置換されます。残り(35.3) は保持されます。同様に、イベントに192.168.DestIPが含まれている場合、DestIPは保持されます。ただし、イベントに文字列192.168が含まれている場合、この文字列は置換されません。

元の文字列と新しい文字列の両方にワイルドカード文字が含まれている場合、元の文字列の中のワイルドカード文字の数は、新しい文字列の中のワイルドカード文字の数に一致する必要があります。

```
...| replace “*.168.*” with “*.XXX.*
```

元の文字列または新しい文字列に/や?などの特殊文字が含まれている場合は、文字列を二重引用符 (" ") で囲みます。

```
...| replace “/Monitor” with Error
```

複数のフィールドの複数の値を1回の操作で置換するには、それぞれの式をカンマ (,) で区切ります。フィールドリストは、置換するすべての値の「with」式を指定した後に指定する必要があることに注意してください (次の例を参照)。

```
...| replace "Arc*" with HP, "cpu:100" with EPS in deviceVendor,
deviceEventClassId
```

元の文字列では、大文字と小文字は区別されません。そのため、文字列「err」は、「Err」を含むイベントを置換します。

例1

出現するすべての「a」を「b」で置換します。ただし、「a」の前後の文字は保持されます。

```
...| replace *a* with *b*
```

例2

出現するすべての「a」を「b」で置換し、「a」の前後の文字は保持しません。

```
...| replace *a* with b in name
```

rex

指定した正規表現に基づいて値を抽出 (キャプチャー) するか、指定した「sed」式に基づいて値を抽出して置換します。値は、クエリ中で以前指定したフィールドか、rawイベントメッセージです。

構文

```
...| rex <regular_expression containing a field name>
```

または

```
...| rex field = <field> mode=sed “s/<string to be substituted>/<substitution value>”
```

抽出動作の説明

正規表現に基づいて値が抽出されるとき、抽出された値は、正規表現の一部として指定されたフィールド名に割り当てられます。フィールド名を定義するための構文は?<fieldname>です。ここで、fieldnameは、英数字の文字列です。アンダースコア (_) の使用は推奨されません。

rexの強力な機能を説明するために、例えば次のイベントを使用します。

```
[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP Warning: Can't connect to 10.4.31.4:11211
```

上のイベントから任意のIPアドレスを抽出し、IP_Addressというフィールドに割り当てるには、次のrex式を指定します。

```
| rex “(?<IPAddress>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})”
```

しかし、イベントの単語「client」の後にあるIPアドレスを抽出し、SourceIPというフィールドに割り当てる場合は、IPアドレス抽出の開始場所と終了場所を指定して、イベント中の2つ目のIPアドレスがキャプチャーされないようにする必要があります。このイベントの開始場所は、[clientとなり、終了場所は] となります。そのため、rex式は次のようになります。

```
| rex “\[client (?<SourceIP>[^\]]*)”
```

このrex式で、?<SourceIP>は、IPアドレスをキャプチャーするために定義されたフィールド名であり、clientは、その後でデータを抽出する、イベント内のテキストまたは場所を指定します。[^\]]*式は、閉じ角括弧でないすべての文字に一致するため、前述のイベント例では、式は最初のIPアドレスの終わりまでと一致し、イベントメッセージの単語「to」の後に現れる2つ目のIPアドレスでは一致しません。

置換動作の説明

rex演算子をsedモードで使用する場合は、抽出したフィールドの値を指定した値で置き換えることができます。たとえば、クレジットカード番号を含むイベントのレポートを生成する場合は、クレジットカード番号を置換して、実際の番号をわからなくすることができます。

置換は、検索結果でのみ実行されます。実際のイベントは変更されません。

次の例で、CCNフィールドのクレジットカード番号は「xxxx」で置き換えられ、機密データが表示されなくなります。

```
| rex field=CCN mode=sed “s/*/xxxx/g”
```

コマンドの最後にある「/g」は、グローバル置換を示します。つまり、すべての一致イベント中に出現する指定したパターンがすべて置換されます。「/g」を省略すると、各イベント中に最初に現れる指定したパターンのみが置換されます。

1つのコマンドで複数の置換を実行できます (次の例を参照)。この例では、単語「Authentication」を「xxxx」ですべてグローバルに (すべての一致イベントについて) 置換し、「192」で始まるエージェントアドレスの最初のバイトを「xxxx」で置換し、「10」で始まるIPアドレスを「xxxx」で置換します。

```
| rex field=msg mode=sed “s/Authentication/xxxx/g” | rex field=agentAddress
mode=sed “s/192/xxxx/g” | rex field=dst mode=sed “s/10.*/xxxx/g”
```

使用上の注意

rex演算子についての詳細なチュートリアルが「rex演算子の使用」(604ページ)にあります。

正規表現ヘルパーツールを使用すると、関心のあるフィールドの正規表現を作成できます。正規表現ヘルパーは、イベントを分析してフィールドに割り当てます。その後、rex式に含めるフィールドを選択します。それらのフィールドの正規表現が [検索] ボックスに自動的に挿入されます。正規表現ヘルパーツールの詳細については、「正規表現ヘルパーツール」(100ページ)を参照してください。

抽出した値は、[システムフィールドセット] の [すべてのフィールド] ビューの追加の列として表示されます。抽出した列のみを表示するには、[システムフィールドセット] リストから **[ユーザ定義フィールド]** を選択します。上の例で、「SourceIP」という見出しの列が [すべてのフィールド] ビューに追加されます。イベントから抽出したIPアドレス値はこの列に表示されます。

fields、sort、chartなどの他の検索演算子を使用して検索結果を操作する場合は、まずこの演算子を使用してそれらのフィールドを抽出する必要があります。

例1

次の例は、name:John ssn:123-45-6789の形式のデータを含むイベントから名前と社会保障番号を抽出し、NameとSSNフィールドに割り当てます。

```
...| rex “name: (?<Name>.*) ssn: (?<SSN>.*)”
```

例2

次の例は、イベントからURLを抽出し、抽出したURLの上位10個を表示します。

```
...| rex “http://(?<URL>[^ ]*)” | top URL
```

例3

次の例は、最初のイベントから抽出した社会保障番号の最後の4桁をxxxxで置換します。

```
...| rex field=SSN mode=sed “s/-\d{4}/-xxxx/g”
```

sort

ソート条件の指定に従って検索結果をソートします。

構文

```
...| sort [<N>] ((+ | -) field)+
```

ここで、

- プラス記号 (+) は、指定したフィールドで昇順に結果をソートします。これがデフォルトです。
- マイナス記号 (-) は、指定したフィールドで降順に結果をソートします。
- <N>は上位N個の結果を保持します。Nは、1～10,000の間の数値です。デフォルト値: 10,000。

使用上の注意

一般に、<field>リストには、Loggerスキーマで使用できるイベントフィールドか、クエリの先行部分でrex演算子を使用して作成したユーザー定義フィールドが含まれます。しかし、eval演算子などの他の演算子でフィールドを定義することもできます。

ソートは、指定したフィールドのデータ型に基づいて行われます。

ソート処理で複数のフィールドが指定されている場合は、最初のフィールドを使用してデータがソートされます。最初のソート後に同じ値が複数ある場合、2番目のフィールドを使用して同じ値の中でソートされ、次に3番目のフィールドでソートされるといった具合になります。たとえば、次の例では、まず一致イベントが「cat」(デバイスイベントカテゴリ) でソートされます。複数のイベントの「cat」が同じ場合、それらのイベントはさらに「eventId」でソートされます。

複数のフィールドが指定されている場合、フィールドごとに異なるソート順を指定できます。たとえば、| sort + deviceEventCategory - eventIdと指定できます。

複数のフィールドを指定する場合は、フィールド名を空白またはカンマで区切ります。

ソートでは大文字と小文字が区別されます。そのため、「Error:105」は、ソートリスト中で「error:105」よりも前に表示されます (昇順でソートした場合)。

sort演算子がクエリに含まれている場合、上位10,000個の一致のみが表示されます。これは既知の制限であり、Loggerの将来のリリースで対処される予定です。

この演算子がクエリに含まれている場合、検索結果をプレビューできません。つまり、検索結果を表示する前にクエリの実行が完了している必要があります。

例

```
...| sort deviceEventCategory eventId
```

tail

検索結果の最後の<N>行を表示します。

構文

```
...| tail [<N>]
```

ここで、

<N>は表示する行数です。デフォルト値: <N>が指定されない場合は**10**。

使用上の注意

この演算子がクエリに含まれている場合、検索結果をプレビューできません。つまり、検索結果を表示する前にクエリの実行が完了している必要があります。

例

```
...| tail 5
```

top

指定したフィールドで最も出現頻度が高い値を表形式で検索結果に表示します。つまり、値は出現数の多いものから少ないものの順に表示されます。

構文

```
...| top [<N>] <field1> <field2> <field3> ...
```

<N>は、指定されたフィールドの上位n個の値に一致を制限します。デフォルト値: <N>が指定されない場合は500。

使用上の注意

各フィールドには、Loggerスキーマで使用可能なイベントフィールドか、クエリの前半でrexまたはeval演算子を使用して作成したユーザー定義フィールドのいずれかを使用できます。複数のフィールドを指定する場合は、フィールド名を空白またはカンマで区切ります。

複数のフィールドを指定した場合、それらすべてのフィールドの一意のセットの数が、大きいものから小さいものの順に表示されます。

この演算子がクエリに含まれていると、検索結果のグラフが自動的に生成されます。グラフに表示されている値をクリックして、指定したフィールド値を持つイベントを素早く絞り込むことができます。詳細については、「グラフのドリルダウン」(131ページ)を参照してください。

指定されたフィールドの上位n個の値に一致を制限するには、nの値を指定します。

指定した値でデフォルト値の500が上書きされます。たとえば、次のクエリを考えます。

```
...| top 1000 deviceEventCategory
```

このクエリは、deviceEventCategoryフィールドに最も頻繁に使用される1000個の値を使用してイベントをグラフ化します。

例

```
...| top deviceEventCategory
```

```
...| top 5 categories
```

transaction

指定したフィールドの値が同じイベントをグループ化します。

構文

```
...| transaction <field1> <field2>...[maxevents=<number>] [maxspan=<number>
[s|m|h|d]] [maxpause=<number>[s|m|h|d]] [startswith=<reg_exp>]
[endswith=<reg_exp>]
```

ここで、

`field1`、`field2`は、フィールドまたはカンマ区切りのフィールドリストであり、その値を比較してグループ化するイベントを判定します。フィールドリストが指定されている場合、それらすべてのフィールドの一意のセットを使用してグループ化するイベントが判定されます。たとえば、hostとportNumが指定され、2つのイベントに「hostA」と「8080」が含まれている場合、これらのイベントが1つのトランザクションにグループ化されます。

`maxevents`は、1つのトランザクションに属することができるイベントの最大数を指定します。たとえば、5を指定すると、一致するイベントが5個見つかった後、以降のイベントはトランザクションに含まれません。デフォルト値: 1000

`maxspan`は、トランザクションの期間に対する制限を指定します。つまり、1つのトランザクション中の最初のイベントと他のすべてのイベントの間の時間差は、指定した上限を超えることはありません。たとえば、maxspan=30sと指定した場合、トランザクション内のすべてのイベント

のイベント時刻は、トランザクション中の最初のイベントのイベント時刻から30秒以内になります。デフォルト値: 無制限

maxpauseは、1つのトランザクション中の連続するイベントの最大間隔を指定します。つまり、このオプションを使用すると、1つのトランザクションに含まれるイベントが、トランザクション内の前のイベントからmaxpauseの値を超えることはありません。デフォルト値: 無制限

startswithは、トランザクションの開始を認識するために使用する正規表現を指定します。たとえば、transaction演算子にstartswith= “user [L|l]ogin”が含まれている場合、すべてのイベントがこの正規表現に対してスキャンされます。イベントが正規表現に一致する場合、トランザクションが作成され、フィールドが一致する以降のイベントがトランザクションに追加されます。

注: 正規表現はrawイベントに適用され、イベント中のフィールドには適用されません。

endswithは、既存のトランザクションの終了を認識するための正規表現を指定します。つまり、現在のトランザクションは、イベントが「endswith」で指定した正規表現に一致したときに完了します。たとえば、transaction演算子にendswith= “[L|l]ogout”が含まれている場合、トランザクションに追加されるイベントが確認され、イベントが正規表現に一致するとトランザクションが完了します。

注: 正規表現はrawイベントに適用され、イベント中のフィールドには適用されません。

使用上の注意

上記のオプションのいくつかは、トランザクションを終了させる条件を指定します。そのため、複数の終了条件が1つのtransaction演算子で指定されている場合、他の条件がまだ満たされていない場合でも、発生した最初の終了条件によってトランザクションが終了します。たとえば、maxspanに達したものの、まだmaxeventsに達していない場合や、endswithの正規表現に一致したもののmaxeventsに達していない場合などです。

transaction演算子の動作

トランザクションとは、指定したフィールドに同じ値が格納された一連のイベントです。イベントは、前述のmaxspanやmaxpauseなどで説明したオプションに基づいてさらにフィルター処理できます。transaction演算子は、イベントをグループ化するのに加えて、フィールドtransactionid、duration、eventcountを各イベントに追加します。これらのフィールドは、検索結果中で個別の列として表示されます。

transactionidは、トランザクションが完了したときに各トランザクションに割り当てられます。トランザクションIDは整数であり、現在のクエリ中で見つかったトランザクション (イベントのセット) に対して、1から順に割り当てられます。同じトランザクション中のすべてのイベントのトランザクションIDが同じになります。

現在のクエリで見つかったどのトランザクションにも属していないイベントには、トランザクションIDとして0が割り当てられます。たとえば、startswith正規表現があるtransaction演算子で、

パイプライン中の最初のイベントが正規表現に一致しない場合、そのイベントはトランザクションに属さず、トランザクションIDとして0が割り当てられます。

durationは、トランザクションの期間をミリ秒単位で表したものであり、トランザクション中の最後のイベントのイベント時刻と、トランザクション中の最初のイベントのイベント時刻との差です。1つのトランザクション中のすべてのイベントのdurationフィールドには、トランザクションのduration値が設定されます。

eventcountには、トランザクション中のイベント数が表示されます。

例1

5分間の間にアクセスしたソースアドレスを表示します。

```
...| transaction sourceAddress maxspan=5m
```

例2

ソースアドレスをソースポートでグループ化し、1つのグループあたり5個のイベントを表示します。

```
...| transaction sourceAddress sourcePort maxevents=5
```

例3

ユーザーと10分間の間にユーザーがアクセスしたURLをグループ化します。

```
...| transaction username startswith= “http://” maxspan=10m
```

例4

1時間の間の、同じセッションIDとソースアドレスからのログイントランザクションを表示します。

```
...| transaction sessionID sourceAddress maxspan=1h startswith= “user
[L|l]ogin”
```

where

「where」式で指定した条件に一致するイベントを表示します。

構文

```
...| where <expression>
```

<expression>は、「クエリのインデックス検索部分」(72ページ)で説明されている、任意の有効なフィールドベースのクエリ式です。

使用上の注意

<expression>には、必ず有効なフィールドベースのクエリ式を指定します。算術式や関数はサポートされていません。

例

```
...| where eventId is NULL

...| where eventId=10006093313 OR deviceVersion CONTAINS “4.0.6.4924.1”

...| where eventId >=10005985569 OR categories= “/Agent/Started”
```

付録B: SmartConnectorを使用したイベントの収集

ArcSightマネージャーと同様に、LoggerもArcSight SmartConnectorを使用してイベントを収集します。SmartConnectorは、ネットワーク上の異なるタイプのデバイス (たとえば、ファイアウォールとサーバー) からセキュリティ上のイベントを読み出すことができ、対象となるイベントをフィルター処理 (オプションで集約) してLogger受信者に送信します。Loggerは、SmartConnectorから正規化された共通イベントフォーマット (CEF) の形式の構造化データを受信します。

注: IPv6データを含んだイベントを受信するには、バージョン7.5.0以降のSmartConnectorを使用する必要があります。

以下のトピックでは、基本的な情報について説明します。特定のコネクターの詳細については、当該コネクターの設定ガイドを参照してください。

SmartMessage

SmartMessageはArcSightのテクノロジーの1つであり、ArcSight SmartConnectorとLoggerの間のCEF (共通イベントフォーマット) イベントのための効率的でセキュアなチャネルを提供します。

SmartMessageは、SSL (Secure Sockets Layer) を使用し、暗号化された安全なエンドツーエンドのチャネルを提供します。一方の端はArcSight SmartConnectorであり、サポートされている多数のデバイスからのイベントを受信します。もう一方の端はLoggerのSmartMessage受信者です。

注: SmartMessageのセキュアチャネルは、SSLプロトコルを使用して暗号化されたイベントをLoggerに送信します。これは、SmartConnectorとArcSightマネージャーの間で使用されている暗号化バイナリプロトコルに似てはいますが、異なるものです。

SmartConnectorを設定してLoggerにイベントを送信する

Loggerは、SmartMessage受信者があらかじめ設定された状態で出荷されています。これを使用してSmartConnectorからイベントを受信するには、以下の説明に従ってSmartConnectorを設定する必要があります。また、新しいSmartMessage受信者を作成し、この新たに作成した受信者を使用してSmartConnectorを設定することもできます。SmartConnectorを設定する際には、必ず正しい受信者名を指定してください。

LoggerにイベントをSmartConnectorを設定するには

1. サポートされている参照用デバイスのSmartConnector設定ガイドを使用してSmartConnectorコンポーネントをインストールします。通知先としては、ArcSightマネージャーやCEFファイルではなく、Loggerを指定します。
2. 必要な通知先パラメーターを指定します。Loggerのホスト名またはIPアドレスと、SmartMessage受信者の名前を入力します。これらの設定は、このコネクターからのイベントを受信するLogger内の受信者に一致している必要があります。
   - 設定済みの受信者を使用するには、[Receiver Name] に「**SmartMessage受信者**」を指定します。
   - SmartMessageを使用して、ArcSight SmartConnectorとLoggerアプライアンスの間で通信するには、ポート443を使用するようにSmartConnectorを設定します。
   - ArcSight SmartConnectorとソフトウェアLoggerの間で通信するには、ソフトウェアLoggerで設定されているポートを使用するようにSmartConnectorを設定します。
   - 暗号化されていないCEF syslogの場合は、Loggerのホスト名またはIPアドレスと目的のポートを入力し、UDPまたはTCP出力を選択します。

SmartConnectorを設定してLoggerとArcSightマネージャーの両方にイベントを送信する

SmartConnectorを設定して、LoggerにCEF syslog出力を、ArcSightマネージャーにイベントを、同時に送信できます。

1. SmartConnectorを通常インストールします。実行中のArcSightマネージャーにSmartConnectorを登録し、SmartConnectorが正常に動作しているかテストします。
2. `$ARCSIGHT_HOME`が参照しているSmartConnectorのインストールディレクトリにある`$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプトを使用して、SmartConnector設定プログラムを再起動します。

3. **[Modify Connector]** を選択し、**[Next]** をクリックして、**[Add, modify, or remove destinations]** を選択します。**[Next]** をクリックします。**[Add destination]** を選択します。
4. **Logger**を選択し、要求されたパラメーターを指定します。SmartConnectorを再起動し、変更を有効にします。

フェイルオーバー先のSmartConnectorの設定

SmartConnectorを設定し、プライマリ接続が障害になったときにセカンダリ(フェイルオーバー先)にイベントを送信するようにします。

フェイルオーバー先を設定するには以下の手順を実行します。

1. 上述のように、プライマリLogger用にSmartConnectorを設定します。トランスポートは、フェイルオーバーの原因となる転送エラーを検出できるよう、raw TCPである必要があります。
2. `$ARCSIGHT_HOME/current/user/agent`ディレクトリのagent.propertiesファイルを編集します。ここで、`$ARCSIGHT_HOME`は、SmartConnectorコンポーネントをインストールしたルートディレクトリです。

   次のプロパティを追加します。`transport.types=http,file,cefsyslog`

   次のプロパティを削除します。`transport.default.type`
3. `$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプトを使用して、SmartConnector設定プログラムを再起動します。
4. **[Modify Connector]** を選択し、**[Next]** をクリックして、**[Add, modify, or remove destinations]** を選択します。Loggerの通知先が選択されていることを確認して、**[Next]** をクリックします。
5. セカンダリLogger用の情報を入力します。
6. SmartConnectorを再起動し、変更を有効にします。
7. ArcSight SmartConnectorのインストールと設定の詳細については、Protect 724のArcSight製品マニュアルのコミュニティから入手できる『ArcSight SmartConnectorユーザーガイド』、または特定の『SmartConnector Configuration Guides』を参照してください。

ArcSight ESMからLoggerにイベントを送信する

ArcSight Forwarding Connectorは、ArcSightマネージャーからイベントを読み取り、これをCEF形式のsyslogメッセージとしてLoggerに転送します。

注: Forwarding Connectorは下記のような名称を持つ、個別インストールが可能なファイルです。

```
ArcSight-4.x.x.<build>.x-SuperConnector-<platform>.exe
```

Loggerと互換性を取るために、ビルド4810以降を使用してください。

ArcSight Forwarding Connectorを設定してLoggerにイベントを送信するには

1. 『Forwarding Connector Configuration Guide』で説明されている「コアソフトウェアのインストール」を使用して、SmartConnectorコンポーネントを通常インストールします。ここでウィザードを終了します。
2. `$ARCSIGHT_HOME/current/user/agent`ディレクトリに**agent.properties**という名称のファイルを作成します。ここで、`$ARCSIGHT_HOME`は、SmartConnectorコンポーネントをインストールしたルートディレクトリです。このファイルは、以下の行のみを含むようにします。

   ```
   transport.default.type=cefsyslog
   ```

3. `$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプトを使用してSmartConnectorの設定プログラムを再起動します。
4. CEF出力に必要なパラメーターを指定します。UDPまたはTCP出力のための希望のポートを入力します。

   ヒント: これらの設定は、ArcSight ESMからのイベントを受信するためにLoggerで作成した受信者と合致する必要があります。

パラメーター	説明
Ip/Host	LoggerのIPアドレスまたはホスト名
Port	514または受信者に合致する他のポート
Protocol	UDPまたはRaw TCP
ArcSight Source Manager Host Name	ソースArcSightマネージャーのIPアドレスまたはホスト名
ArcSight Source Manager Port	8443 (デフォルト)
ArcSight Source Manager User Name	ソースマネージャー上でイベントを読み取るための十分な権限を持つユーザーアカウント

パラメーター	説明
ArcSight Source Manager Password	指定されたマネージャーのユーザーアカウントのパスワード
SmartConnector Name	ESMからLoggerへのコネクター (マネージャーで認識可能) の名前
SmartConnector Location	コネクターがインストールされた場所の通知
Device Location	ソースマネージャーがインストールされた場所の通知
Comment	コメント (オプション)

Forwarding ConnectorがLoggerにCEF出力を送り、同時に別のArcSightマネージャーにイベントを送信するように設定する方法については、「SmartConnectorを設定してLoggerとArcSightマネージャーの両方にイベントを送信する」(600ページ)を参照してください。

付録C: rex演算子の使用

rex演算子は、指定した正規表現に一致する情報を抽出し、指定した名前のフィールドに割り当てることができる、強力な演算子です。また、rex式の中で、正規表現に一致する情報を検索する際の開始場所と終了場所をオプションで指定することもできます。

rex式が検索クエリに含まれている場合、その前に、rex式が情報を抽出する元となるイベントを探す基本検索クエリが指定されている必要があります。例:

```
failed | rex “(?<srcip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})”
```

次のトピックでは、検索演算子rexについて詳しく説明します。

rex演算子の構文

```
| rex “text1(?<field1>text2regex)”
```

ここで、

- text1: イベント内の、その後から情報抽出を開始するテキストまたは場所。デフォルトはイベントの先頭です。
- text2: イベント内の、情報抽出を終了するテキストまたは場所。
- field1: 抽出した情報を割り当てるフィールドの名前。
- regex: text1とtext2の間で抽出する情報の照合に使用するパターン(正規表現)。

ヒント: 正規表現の使用経験が豊富なユーザーの場合は、次のセクションの「注」を参照すると、rexを使用して指定した入力を取得し、それを参照してさらに処理する方法を素早く理解できます。

rex演算子の構文の説明

text1の後からtext2までのすべての情報のうち、指定したregex(正規表現)に一致するものを抽出して、field1に割り当てます。

- text1と[text2]には、イベントの任意の場所を指定できます。指定できるのは、イベントの開始と終了、イベント中の特定の文字列(文字列がイベント内の単語の途中にあってもかまいません)、イベントの先頭または末尾からの特定の文字数、パターンです。
- イベント内の次のスペースをtext2として指定するには、[^]と入力します。

これは「スペース以外」と解釈されます。そのため、「否定」を入力すると、イベント内で指定した文字 (この例ではスペース) が見つかった場所で取得が停止します。

- [text2] に行末を指定するには、[^$] と入力します。

  これは「行末以外」と解釈されます。そのため、イベント内で行末に達すると、その時点で取得が停止します。[^$] を使用すると、行末文字でない1文字のみを取得します。しかし、rex式で [^$]*を指定することで、行末までのすべての文字が取得されます。

  また、[^$] の代わりに.*を指定して、すべての文字を取得することを指定することもできます。ただし、本書の例では [^$] を使用します。
- rex式内の二重引用符の中の任意のスペースは文字どおりに扱われます。
- rex式でエスケープする必要がある文字は、正規表現のものと同じです。そのような文字の完全な一覧については、任意の正規表現のドキュメントを参照してください。
- rex式によって取得された情報を使用して、次の例で示すように、以降のrex式でさらに処理することができます。この例では、最初のrex式でIPアドレスを取得し、取得したIPアドレスからIPアドレスが属するネットワークID (IPアドレスの最初の3バイトが表現していると仮定) を抽出しています。

  ```
  logger | rex "(?<srcip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | rex field=srcip "(?<netid>\d{1,3}\.\d{1,3}\.\d{1,3})"
  ```

  注: 使用経験の豊富な正規表現のユーザーであれば、rex式の構文を以下のように解釈できます。

  ```
  rex "(?<field1>regex)"
  ```

  ここで、括弧内の式全体が名前付きの取得を指定しています。つまり、取得したグループに名前が割り当てられ、後で参照してさらに処理できます。たとえば、次の式では、取得したデータに「srcip」という名前が割り当てられています。

  ```
  failed | rex "(?<srcip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
  ```

  名前を付ければ、次のように「srcip」を使用してさらに処理を行うことができます。

  ```
  failed | rex "(?<srcip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | top srcip
  ```

rex式を作成するための方法

rex式は、次の2つの方法で作成できます。

- 手動: この付録で説明する構文とガイドラインに従い、要件に合わせてrex式を作成します。

- 正規表現ヘルパー: 「正規表現ヘルパーツール」(100ページ) で説明している正規表現ヘルパーツールを使用します。このツールを使用すると、手順が単純になるだけでなく、誤りが発生しにくく、より効率的になります。

手動でのrex式の作成

まず、関心のある情報を含むイベントを探す単純な検索を作成します。イベントが表示されたら、それらのイベントの中で、情報の前にある共通の開始場所を特定します。

たとえば、クライアントのIPアドレスの抽出に関心があり、次のイベントのように、IPアドレスが常に単語「[client」の後に現れるとします。

```
[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP Warning:
memcache_pconnect() [<a href='function.memcache-pconnect'>function.memcache-
pconnect</a>]: Can't connect to 10.4.31.4:11211
```

そのため、「[client」が開始場所になります。適切な終了場所は、クライアントIPアドレスの最後のバイトの後の「]」です。ここで、IPアドレスを抽出する正規表現を定義する必要があります。この例では、「client」という単語の後にクライアントIPアドレスのみが現れるため、正規表現として「すべてを抽出する」を意味する「*」を使用します(より具体的には、IPアドレスに対して`\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`を使用することもできます)。IPアドレスをフィールド名「clientIP」に割り当てます。これでrex式を作成する準備はほぼ完了ですが、式の中で文字「[」と「]」をエスケープする必要があります。使用するエスケープ文字は「\」です。

これで、上記のイベントの中の「client」という単語の後に現れるIPアドレスを抽出するrex式を作成する準備ができました。

```
| rex "\[client(?<clientip>[^\]]*)"
```

rex式の例

ここでは、さまざまな種類の情報をイベントから抽出するためのいくつかのサンプルを示します。後の例になるほど、抽出する情報が具体的になります。これらの例を元に、ニーズに合ったrex式を作成してください。また、rex式の作成が簡単になる正規表現ヘルパーツールを使用してください。

以下のイベントの例では、異なるrex式による情報抽出の仕組みについて説明しています。

例1

次のrex例では、説明用に以下のイベントを使用しています。

- パイプラインの左側から一致するイベントを取得して、フィールドmessageに割り当てます。イベント全体が「message」フィールドに割り当てられます。

  ```
  | rex “(?<message>[^$]*)”
  ```

  この式は、「CEF:0」という単語で始まる上記のイベント全体を抽出します。
- 開始場所を、特定の文字や単語ではなく、イベントの先頭からの文字数として指定します。

  ```
  | rex “[a-zA-Z0-9:\.\s]{16}(?<message>[^$]*)”
  ```

  この式は、text1に指定された文字 (英数字、コロン、ピリオド、スペース) が16個**連続して**現れた後から抽出を開始します。1つ目のイベントの最初の16文字は「CEF:0|ArcSight|L」ですが、抽出は「Logger|4.5.0...」で始まりません。これは、このイベントの最初の16文字に含まれるパイプライン文字が、rex式で照合する文字に含まれていないためです。そのため、最初に16個連続して現れるのは「Logger Internal」です。その結果、単語「Event」で始まる情報がこのイベント例から抽出されます。
- 次のスペースや行末などの終了場所を指定する代わりに、指定した文字数を抽出します。

  ```
  | rex “[a-zA-Z0-9:\.\s]{16}(?<message>[^$]{5})”
  ```

  この式は、単語「Event」のみを抽出します。(抽出が単語「Event」で始まる理由の詳しい説明については、前のrex式の例を参照してください)。
- 「CEF:0|」の後のすべてをmessageフィールドに抽出します。その後、messageフィールドがnullでないイベントを別のrex式にパイプで渡し、一致するイベントに含まれているIPアドレスを抽出して、IPアドレスを別のフィールドmsgipに割り当てます。msgipがnullでないイベントのみを表示します。

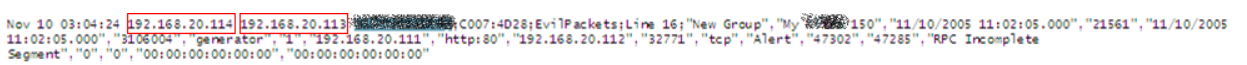
  ```
  | rex “CEF:0\|(?<message>[^$]*)” | where message is not null | rex “dvc=
  (?<msgip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | where msgip is not null
  ```

  注: 文字「:」と「=」をエスケープする必要はありませんが、「|」はエスケープする必要があります。rex式でエスケープする必要がある文字は、正規表現のものと同じです。そのような文字の完全な一覧については、任意の正規表現のドキュメントを参照してください。

  この式は、デバイスのIPアドレスをイベントから抽出します。

例2

次のrex例では、説明用に以下のイベントを使用しています。



- 最初の2つのIPアドレスをイベントから抽出し、2つの異なるフィールドIP1とIP2に割り当てます。

  ```
  | rex “(?<IP1>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | rex “\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}(?<IP2>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})”
  ```

  この式は、上のイベントの1つ目と2つ目のIPアドレスを抽出します。

  2つのIPアドレスは、このイベント中で連続しているため、2つのIPアドレスの抽出を1つのrex式で次のように指定することもできます。

  ```
  | rex “(?<IP1>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?<IP2>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})”
  ```

  注: 式中にスペースを入力しないでください。

- 前の例をベースにし、Ignoreという新しいフィールドを追加します。前の例で抽出した2つのIPアドレスが同じであればこのフィールドに値「Y」を割り当て、IPアドレスが違う場合は値「N」を割り当てます。次に、Ignoreフィールドが「N」のイベントに対し、上位のIP1とIP2の組み合わせを表示します。

  ```
  | rex (?<IP1>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | rex “\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}(?<IP2>[^$]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | eval Ignore=if(IP1==IP2,“Y”,“N”) | where Ignore=“N” | top IP1 IP2
  ```

  注: evalコマンドは、二重の等号である==を使用して2つのフィールドを照合しています。

- rex式で取得した情報を使用して、次の例に示すように、以降のrex式でさらに処理することができます。最初のrex式で1つ目のIPアドレスを取得し、取得したIPアドレスからIPアドレスが属するネットワークID (IPアドレスの最初の3バイトが表現していると仮定) を抽出しています。

  ```
  logger | rex “(?<srcip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | rex field=srcip “(?<netid>\d{1,3}\.\d{1,3}\.\d{1,3})
  ```

例3

次のrex例では、説明用に以下のイベントを使用しています。

```
127.0.0.1 - name [10/Oct/2010:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"
```

- イベントからすべてのURLを抽出し、空のURLを除くURL数のグラフを生成します(イベントには、「http://」形式のURL文字列が含まれています)。

```
| rex “http://(?<customURL>[^ ]*)” | where customURL is not null | chart
count by customURL | sort - customURL
```

注: メタ文字「/」を文字どおりに扱うには、角括弧 [] で囲む必要があります。

例4

次のrex例では、説明用に以下のイベントを使用しています。

1	2010/04/06 22:11:46 CDT 10.0.10.222 [Raw_Syslog]	Local	root
RAW	Feb 25 14:03:24 beach login(pam_unix)[123]: session closed for user root		
2	2010/04/06 22:11:46 CDT 10.0.10.222 [Raw_Syslog]	Local	sysadmin
RAW	Feb 25 14:03:24 beach sshd(pam_unix)[123]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=123.123.123.123 user=sysadmin		
3	2010/04/06 22:11:46 CDT 10.0.10.222 [Raw_Syslog]	Local	p4admin
RAW	Feb 25 14:03:24 beach sshd(pam_unix)[123]: session closed for user p4admin		
4	2010/04/06 22:11:46 CDT 10.0.10.222 [Raw_Syslog]	Local	sysadmin
RAW	Feb 25 14:03:24 beach sshd(pam_unix)[123]: session opened for user sysadmin by (uid=500)		

- 「user」の直後の単語 (単語の後に1個のスペース) または「user=」を抽出します。単語「user」は、この場合大文字と小文字が区別されず、前にスペース文字が必要です。つまり、「ruser」や「suser」などの単語は一致しません。

  ```
  | rex “\s[u|U][s|S][e|E][r|R][\s|=](?<CustomUser>[^ ]*)”
  ```

付録D: Logger監査イベント

共通イベントフォーマット (CEF) のLoggerの監査イベントを、直接ArcSight ESMに送信して分析し、関連付けることができます。イベントを転送するには、監査転送機能 (「監査転送」(508ページ) を参照) を使用します。

CEFの詳細については、『ArcSight CEF』を参照してください。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品マニュアルのコミュニティから "ArcSight Common Event Format (CEF) Guide" を検索してください。

次のトピックでは、Loggerの監査イベントについて説明します。

監査イベントの種類

Loggerでは2種類の監査イベントが生成され、ArcSight ESMへの監査転送に使用できます。

- 「プラットフォームイベント」(611ページ) (Loggerハードウェア/システムに関係)
- 「アプリケーションイベント」(619ページ) (Loggerの機能とその設定変更に関係)

両方の種類のイベントが、Loggerの内部ストレージグループに格納されます。その結果、これらのイベントは、Loggerの検索UIを使用して検索できます。たとえば、次のプラットフォームイベントを検索できます。

「/Platform/Authentication/Failure/Password」

監査イベント内の情報

Loggerの監査イベント (CEF形式) には、以下のプレフィックスフィールドに関する情報が含まれています。

- デバイスイベントクラスID
- デバイスの緊急度
- メッセージ
- デバイスイベントカテゴリ (このCEF拡張のkeyNameは「cat」です)

例:

```
Sep 19 08:26:10 zurich CEF:0|ArcSight|Logger|3.5.0.13412.0|logger:500|Filter
added|2|  cat=/Logger/Resource/Filter/Configuration/Add
msg=Filter [Regex Query Test] has been added
```

プラットフォームイベント

次の表では、Loggerプラットフォームに関連する監査イベントに含まれる情報を一覧に示します。すべてのイベントに以下のフィールドが含まれています。

- duser—ユーザー名
- duid—ユーザーID
- src—クライアントのIPアドレス
- dst—アプライアンスのIPアドレス
- cat—デバイスイベントカテゴリ
- cn1—セッション番号
- cn1label—セッション

追加のフィールド (該当する場合) を次の表に示します。

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:200	5	/Platform/Authentication/PasswordChange/Failure	Failed password change	
platform:201	7	/Platform/Authentication/Failure	Failed login attempt	
platform:202	5	/Platform/Authentication/PasswordChange	Password changed	cs1: 影響のあるユーザーID cs2: 影響のあるユーザーログイン cs3: 影響のあるユーザーのフルネーム
platform:203	7	/Platform/Authentication/InactiveUser/Failure	Login attempt by inactive user	
platform:213	7	/Platform/Configuration/Global/AuditEvents	Audit forwarding modified	cs1: 監査転送者
platform:220	5	/Platform/Certificate/Install	Installed certificate	cs1: ネットワークプロトコル

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:221	7	/Platform/Certificate/Mismatch	Certificate mismatch failure	cs1: ネットワークプロトコル
platform:222	1	/Platform/Certificate/Request	Created certificate signing request	cs1: 証明書署名要求 cs2: ネットワークプロトコル
platform:224	5	/Platform/Certificate/Regenerate	Re-generate self-signed certificate	cs1: 証明書署名要求 cs2: ネットワークプロトコル
platform:226	7	/Platform/Update/Failure/CorruptPackage	Uploaded update file damaged or corrupt	cs1: エラー cs2: fname cs3: fsize
platform:227	5	/Platform/Update/Applied	Update installation success	cs1: 更新名 cs2: 再起動が必要かどうか
platform:228	7	/Platform/Update/Failure/Installation	Update installation failure	cs1: エラー cs2: 更新名
platform:230	3	/Platform/Authentication Login	Successful login	
platform:234	7	/Platform/Authentication/Failure/LOCKED	Failed login attempt (LOCKED)	
platform:239	3	/Platform/Authentication/Logout	User logout	
platform:240	3	/Platform/Authorization/Groups/Add	Added user group	cn2: 現在のユーザー数 cn3: 現在のユーザー権限数 cs1: 影響のあるグループ名 cs2: 影響のあるグループID flexNumber1: 古いユーザー数 flexNumber2: 古いユーザー権限数

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:241	3	/Platform/Authorization /Groups/Update	Updated user group	cn2: 現在のユーザー数 cn3: 現在のユーザー権限数 cs1: 影響のあるグループ名 cs2: 影響のあるグループID flexNumber1: 古いユーザー数 flexNumber2: 古いユーザー権限数
platform:242	5	/Platform/Authorization /Groups/Membership /Update/Clear	Removed all members from group	
platform:243	3	/Platform/Authorization /Groups/Membership/Update	Modified user group membership	
platform:244	3	/Platform/Authorization /Groups/Delete	Deleted user group	cs1: 影響のあるグループ名 cs2: 影響のあるグループID
platform:245	3	/Platform/Authorization /Users/Add	Added user	cs1: 影響のあるユーザーID cs2: 影響のあるユーザーログイン cs3: 影響のあるユーザーのフルネーム
platform:246	3	/Platform/Authorization /Users/Update	Updated user	cs1: 影響のあるユーザーID cs2: 影響のあるユーザーログイン cs3: 影響のあるユーザーのフルネーム
platform:247	3	/Platform/Authorization/Users /Delete	Deleted user	cs1: 影響のあるユーザーID cs2: 影響のあるユーザーログイン cs3: 影響のあるユーザーのフルネーム
platform:248	3	/Platform/Authentication /Logout/SessionExpiration	Session expired	

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:249	7	/Platform/Authentication/AccountLocked	Account locked	
platform:250	5	/Platform/Storage/RFS/Add	Added remote mount point	cs1: RFSマウント名 cs2: RFSマウントホストとリモートパス
platform:251	5	/Platform/Storage/RFS/Edit	Edited remote mount point	cs1: RFSマウント名 cs2: RFSマウントホストとリモートパス
platform:252	7	/Platform/Storage/RFS/Failure	Failed to create remote mount point	cs1: サーバー cs2: リモートディレクトリ cs3: マウント名 cs4: マウントタイプ cs5: ユーザー名
platform:253	5	/Platform/Storage/RFS/Remove	Removed remote mount point	cs1: RFSマウント名 cs2: RFSマウントホストとリモートパス
platform:254	5	/Platform/Storage/SAN/Destroy	Destroyed SAN Logical Unit	cs1: ボリュームラベル
platform:255	5	/Platform/Storage/SAN/Attach	Attached SAN Logical Unit	cn2: ボリュームサイズ (MB単位) cs1: ボリュームラベル cs2: ワールドワイド名 cs3: ファイルシステムタイプ
platform:256	7	/Platform/Storage/SAN/Detach	Detached SAN Logical Unit	cs1: ストレージユニットの詳細
platform:259	5	/Platform/Storage/SAN/Reattach	Reattached SAN Logical Unit	cs1: ボリュームラベル cs2: ファイルシステムタイプ
platform:260	5	/Platform/Configuration/Network/Route/Update	Static route modified	cs1: 通知先 cs2: サブネット cs3: ゲートウェイ
platform:261	5	/Platform/Configuration/Network/Route/Remove	Static route removed	cs1: 通知先 cs2: サブネット cs3: ゲートウェイ

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:262	5	/Platform/Configuration/Time	Appliance time modified	cs1: 古い日付/時刻 cs2: 新しい日付/時刻 cs3: 古いタイムゾーン cs4: 新しいタイムゾーン
platform:263	5	/Platform/Configuration/Network	NIC settings modified	cs1: NIC cs2: IPアドレス cs3: ネットマスク cs4: 速度
platform:264	5	/Platform/Configuration/Network/NTP	NTP server settings modified	cs1: NTPサーバー cs2: アプライアンスがNTPサーバーかどうか
platform:265	5	/Platform/Configuration/Network/DNS	DNS settings modified	
platform:266	5	/Platform/Configuration/Network/Hosts	Hosts file modified	cs1: 以前のhostsファイルからの差分
platform:267	5	/Platform/Configuration/SMTP	SMTP settings modified	cs1: メールアドレス cs2: SMTPサーバー cs3: バックアップSMTPサーバー
platform:268	5	/Platform/Configuration/Network/Route/Add	Static route added	cs1: 通知先 cs2: サブネット cs3: ゲートウェイ
platform:270	5	/Platform/Authorization/Users/Inactive/Disable	Inactive user disabled	cs1: ユーザーログイン deviceCustomDate1: 最後にアクティブだった日付
platform:280	7	/Appliance/State/Reboot/Initiate	Appliance reboot initiated	
platform:281	3	/Appliance/State/Reboot/Cancel	Appliance reboot canceled	
platform:282	7	/Appliance/State/Shutdown	Appliance poweroff initiated	
platform:284	5	/Platform/Storage/Multipathing/Enable	Enabled SAN Multipathing	cs1: マルチパス構成
platform:285	5	/Platform/Storage/Multipathing/Disable	Disabled SAN Multipathing	

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:300	5	/Platform/Certificate /Install	Installed trusted certificate	cs1: 証明書の詳細
platform:301	5	/Platform/Certificate /Revocation/Install	Installed certificate revocation list	cs1: CRLの詳細
platform:302	5	/Platform/Certificate/Delete	Deleted trusted certificate	cs1: 証明書の詳細
platform:303	5	/Platform/Certificate/ Revocation/Delete	Deleted certificate revocation list	cs1: CRLの詳細
platform:304	7	/Platform/Certificate/ Install/Failure	Failed installing trusted certificate	cs1: エラー cs2: ファイルサイズ cs3: ファイル名
platform:305	7	/Platform/Certificate/ Revocation/Install/Failure	Failed installing certificate revocation list	cs1: エラー cs2: ファイルサイズ cs3: ファイル名
platform:306	5	/Platform/Process/Start	Start process	cs1: プロセス名
platform:307	5	/Platform/Process/Stop	Stop process	cs1: プロセス名
platform:308	5	/Platform/Process/Restart	Restart process	cs1: プロセス名
platform:310	5	/Platform/Configuration /FIPS/Enable	Enabled FIPS mode	
platform:311	7	/Platform/Configuration /FIPS/Disable	Disabled FIPS mode	
platform:312	7	/Platform/Configuration /WebServer/CipherStrength	Web server cipher strength changed	cs1: 新しい値 cs2: 古い値
platform:320	3	/Appliance/State /Shutdown/Cancel	Appliance poweroff canceled	
platform:371	5	/Platform/Service/Restart	Restarted OS service	cs1: サービス名
platform:400	2	/Platform/Diagnostics /Command	Ran diagnostic command	cs1: 診断コマンド

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:407	7	/Platform/Certificate /SSL/Expiration	SSL certificate expiration warning	cs1: 発行元 cs2: 件名 deviceCustomDate1: 期限日
platform:408	5	/Appliance/State/Startup	Appliance startup completed	deviceCustomDate1: 起動日
platform:409	3	/Platform/Configuration /LoginBanner	Configure login warning banner	cs1: 確認プロンプト cs2: バナーテキスト
platform:410	5	/Platform/Configuration /Network	Network settings modified	cs1: ゲートウェイ cs2: マルチホーミング cs3: ホスト名
platform:411	5	/Platform/Authentication /PasswordChange	Automated Password Reset	cn2: ユーザーID cs1: ユーザーログイン
platform:412	3	/Platform/Configuration /Locale	Set Locale	cs1: ロケール
platform:440	3	/Platform/Configuration/ SNMP	SNMP configuration modified	cn2: ポート番号 cn3: 更新間隔 cs1: SNMP有効 cs2: コミュニティストリング cs3: リッスンアドレス
platform:460	3	/Platform/Network/Alias/Add	NIC alias added	cs1: NIC cs2: IPアドレス cs3: ネットマスク
platform:462	3	/Platform/Network/Alias /Remove	NIC alias removed	cs1: NIC cs2: IPアドレス cs3: ネットマスク
platform:500	5	/Platform/Authorization /Groups/Membership /Remove	Remove member from group	cs1: 影響のあるグループ名 cs2: 影響のあるユーザーログイン cs3: 影響のあるグループID cs4: 影響のあるユーザーID

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:501	5	/Platform/Authorization /Groups/Membership/Add	Group member added	cs1: 影響のあるグループ名 cs2: 影響のあるユーザーログイン cs3: 影響のあるグループID cs4: 影響のあるユーザーID
platform:502	5	/Platform/Authorization /Users/Groups/Remove	User removed from group	cs1: 影響のあるグループ名 cs2: 影響のあるユーザーログイン cs3: 影響のあるグループID cs4: 影響のあるユーザーID
platform:503	5	/Platform/Authorization /Users/Groups/Add	User added to group	cs1: 影響のあるグループ名 cs2: 影響のあるユーザーログイン cs3: 影響のあるグループID cs4: 影響のあるユーザーID
platform:530	5	/Platform/Configuration /Authentication/Sessions /Success	Authentication Session settings successfully changed.	cn2: 新しい値 cn3: 古い値 cs1: 変更されたパラメーター
platform:540	5	/Platform/Configuration /Authentication/Password /Lockout/Success	Password Lockout settings successfully updated.	cn2: 新しい値 cn3: 古い値 cs1: 変更されたパラメーター
platform:550	5	/Platform/Configuration /Authentication/Password /Expiration/Success	Password Expiration settings successfully updated.	cn2: 新しい値 cn3: 古い値 cs1: 変更されたパラメーター
platform:560	5	/Platform/Configuration /Authentication/Password /Validation/Success	Password Validation settings successfully updated.	cn2: 新しい値 cn3: 古い値 cs1: 変更されたパラメーター

デバイスイベントクラスID	緊急度	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
platform:570	5	/Platform/Configuration /Authentication/Password /AutomatedPasswordReset /Success	Password Automated Password Reset setting successfully updated.	cs1: 変更されたパラメーター cs2: 新しい値 cs3: 古い値
platform:580	5	/Platform/Configuration /Authentication/Certificate /Success	Client Certificate authentication settings successfully changed.	cs1: 変更されたパラメーター cs2: 新しい値 cs3: 古い値
platform:590	5	/Platform/Configuration /Authentication/RADIUS /Success	RADIUS authentication settings successfully changed.	cs1: 変更されたパラメーター cs2: 新しい値 cs3: 古い値
platform:600	5	/Platform/Configuration /Authentication/LDAP/ [Success]	LDAP authentication settings successfully changed.	cs1: 変更されたパラメーター cs2: 新しい値 cs3: 古い値
platform:610	5	/Platform/Configuration /Authentication/Global /Success	Global Authentication settings successfully changed.	cs1: 変更されたパラメーター cs2: 新しい値 cs3: 古い値

アプリケーションイベント

次の表では、Loggerの各種機能とその設定変更に関連する監査イベントに含まれる情報を一覧に示します。すべてのLoggerアプリケーションイベントの緊急度は**2**です。

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
アラート			
logger:610	/Logger/Component/Alert/Configuration/Add	Alert [name] has been added	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmpHostName cn1Label=Syslog or SNMP Destination Port cn1=syslogOrSnmpPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses
logger:611	/Logger/Component/Alert/Configuration/Delete	Alert [name] has been deleted	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmHostName cn1Label=Syslog or SNMP Destination Port cn1=syslogOrSnmpPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:612	/Logger/Component /Alert/Configuration /Update	Alert [name] has been updated	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmpHostName cn1Label=Syslog or SNMP Destination Port cn1=syslogOrSnmpPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses
logger:613	/Logger/Component /Alert/Configuration /Enable	Alert [name] has been enabled	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmpHostName cn1Label=Syslog or SNMP Destination Port cn1=syslogOrSnmpPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses
logger:614	/Logger/Component /Alert/Configuration /Disable	Alert [name] has been disabled	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmpHostName cn1Label=Syslog or SNMP Destination Port cn1=syslogOrSnmpPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:615	/Logger/Alert /Configuration/Sent	Alert [name] has been sent	fname=AlertName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=syslogOrSnmpIpAddr dvchost=syslogOrSnmpOr EsmHostName cn1Label=Syslog Or SNMP Or ESM Destination Port cn1=syslogOrSnmpOrEsmPort cs1Label=Filter cs1=filter cs2Label=Email Destination(s) cs2=emailAddresses
証明書			
logger:643	/Logger/Component/ Certificate/Configuration /Add	Certificate [name] has been added	fname=alias duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Certificate
logger:650	/Logger/Component/ Certificate/Configuration /Delete	Certificate [name] has been deleted	fname=alias duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Certificate
logger:651	/Logger/Component/ Certificate/Configuration /Update	Certificate [name] has been updated	fname=alias duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Certificate
設定バックアップ			
logger:660	/Logger/Component/ ConfigBackup /Configuration/Update	Configuration backup has been updated	fname=Configuration Backup duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Configuration Backup

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:661	/Logger/Component/ConfigBackup/Configuration/Enable	Configuration backup has been enabled	fname=Configuration Backup duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Configuration Backup
logger:662	/Logger/Component/ConfigBackup/Configuration/Disable	Configuration backup has been disabled	fname=Configuration Backup duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Configuration Backup
logger:665	/Logger/Component/ConfigBackup/Configuration/Backup	Configuration backup succeeded.Transfer process finished.	fname=Configuration Backup fileType=Configuration Backup fpath=pathToBackupFile fsize=fileSizeInByte
ESM通知先			
logger:640	/Logger/Component/EsmDestination/Configuration/Add	ESM destination [name] has been added	fname=esmDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=ESM Destination fileId=esmDestinationId dvc=esmDestinationIp dvchost=esmDestinationHost cn1Label=ESM Destination Port cn1=esmDestinationPort cs1Label=Connector Name cs1=connectorName cs2Label=Connector Location cs2=connectorLocation cs3Label=Logger Location cs3=loggerLocation

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:641	/Logger/Component/EsmDestination/Configuration/Delete	ESM destination [name] has been deleted	fname=esmDestinationName duser=UserName duid=userId cs4=sessionId file cs4Label=Session ID fileType=ESM Destination fileId=esmDestinationId dvc=esmDestinationIp dvchost=esmDestinationHost cn1Label=ESM Destination Port cn1=esmDestinationPort cs1Label=Connector Name cs1=connectorName cs2Label=Connector Location cs2=connectorLocation cs3Label=Logger Location cs3=loggerLocation
転送者			
logger:605	/Logger/Component/Forwarder/Configuration/Add	Forwarder [name] has been added	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter
logger:606	/Logger/Component/Forwarder/Configuration/Delete	Forwarder [name] has been deleted	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:607	/Logger/Component/Forwarder/Configuration/Update	Forwarder [name] has been updated	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter
logger:608	/Logger/Component/Forwarder/Configuration/Enable	Forwarder [name] has been enabled	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter
logger:609	/Logger/Component/Forwarder/Configuration/Disable	Forwarder [name] has been disabled	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:663	/Logger/Component/Forwarder/Configuration/Pause	Forwarder [name] has been paused	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter
logger:664	/Logger/Component/Forwarder/Configuration/Resume	Forwarder [name] has been resumed	fname=forwarderName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=forwarderType dvc=forwarderIpAddr dvchost=forwarderHostName cn1Label=Forwarder Port cn1=forwarderPort cs1Label=Forwarder Filter cs1=forwarderFilter
受信者			
logger:600	/Logger/Component/Receiver/Configuration/Add	Receiver [name] has been added	fname=receiverName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=receiverType dvc=receiverIpAddr dvchost=receiverHostName cn1Label=Receiver Port cn1=receiverPort

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:601	/Logger/Component/Receiver/Configuration/Delete	Receiver [name] has been deleted	fname=receiverName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=receiverType dvc=receiverIpAddr dvchost=receiverHostName cn1Label=Receiver Port cn1=receiverPort
logger:602	/Logger/Component/Receiver/Configuration/Update	Receiver [name] has been updated	fname=receiverName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=receiverType dvc=receiverIpAddr dvchost=receiverHostName cn1Label=Receiver Port cn1=receiverPort
logger:603	/Logger/Component/Receiver/Configuration/Enable	Receiver [name] has been enabled	fname=receiverName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=receiverType dvc=receiverIpAddr dvchost=receiverHostName cn1Label=Receiver Port cn1=receiverPort
logger:604	/Logger/Component/Receiver/Configuration/Disable	Receiver [name] has been disabled	fname=receiverName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=receiverType dvc=receiverIpAddr dvchost=receiverHostName cn1Label=Receiver Port cn1=receiverPort
SNMP通知先			

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:644	/Logger/Component/SnmpDestination/Configuration/Add	SNMP destination [name] has been added	fname=snmpDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=SNMP Destination fileId=snmpDestinationId dvc=snmpDestinationIp dvchost=snmpDestinationHost cn1Label=SNMP Destination Port cn1=snmpDestinationPort cs1Label=Connector Name cs1=connectorName cs2Label=Connector Location cs2=connectorLocation cs3Label=Logger Location cs3=loggerLocation
logger:645	/Logger/Component/SnmpDestination/Configuration/Delete	SNMP destination [name] has been deleted	fname=snmpDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=SNMP Destination fileId=snmpDestinationId dvc=snmpDestinationIp dvchost=snmpDestinationHost cn1Label=SNMP Destination Port cn1=snmpDestinationPort cs1Label=Connector Name cs1=connectorName cs2Label=Connector Location cs2=connectorLocation cs3Label=Logger Location cs3=loggerLocation
syslog通知先			

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:647	/Logger/Resource/SyslogDestination/Configuration/Add	Syslog destination [name] has been added	fname=syslogDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Syslog Destination fileId=syslogDestinationId dvc=syslogDestinationIp dvchost=syslogDestinationHost cn1Label=Syslog Destination Port cn1=syslogDestinationPort
logger:648	/Logger/Component/SyslogDestination/Configuration/Delete	Syslog destination [name] has been deleted	fname=syslogDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Syslog Destination fileId=syslogDestinationId dvc=syslogDestinationIp dvchost=syslogDestinationHost cn1Label=Syslog Destination Port cn1=syslogDestinationPort
logger:649	/Logger/Component/SyslogDestination/Configuration/Update	Syslog destination [name] has been updated	fname=syslogDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Syslog Destination fileId=syslogDestinationId dvc=syslogDestinationIp dvchost=syslogDestinationHost cn1Label=Syslog Destination Port cn1=syslogDestinationPort
アーカイブ			
logger:520	/Logger/Resource/Archive/Configuration/Add	Archive [archiveName] has been added	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:521	/Logger/Resource/Archive/Configuration/Delete	Archive [archiveName] has been deleted	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
logger:523	/Logger/Resource/Archive/Configuration/Load	Archive [archiveName] has been loaded	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
logger:524	/Logger/Resource/Archive/Configuration/Unload	Archive [archiveName] has been unloaded	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
logger:525	/Logger/Resource/Archive/Configuration/Archive	Archive [archiveName] has been archived	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
logger:526	/Logger/Resource/Archive/Add	Event archive settings added	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
logger:527	/Logger/Resource/Archive/Update	Daily archive task settings updated	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:528	/Logger/Resource/Archive/Failed	Event archive failed	fname=archiveName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=EventArchive fileId=archiveId
ダッシュボード			
logger:580	/Logger/Resource/Dashboard/Configuration/Add	Dashboard [name] has been added	fname=dashboardName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Dashboard fileId=DashboardId rt=receiptTime
logger:581	/Logger/Resource/Dashboard/Configuration/Add	Dashboard [name] has been deleted	fname=dashboardName duser=UserName duid=userId cs4=sessionIdfile fileType=Dashboard fileId=DashboardId rt=receiptTime
logger:582	/Logger/Resource/Dashboard/Configuration/Update	Dashboard [name] has been updated	fname=dashboardName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Dashboard fileId=DashboardId rt=receiptTime
デバイス			
logger:510	/Logger/Resource/Device/Configuration/Add	Device [deviceName] has been added	fname=deviceName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Device fileId=deviceId

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:511	/Logger/Resource/Device/Configuration/Delete	Device [deviceName] has been deleted	fname=deviceName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Device fileId=deviceId
logger:512	/Logger/Resource/Device/Configuration/Update	Device [deviceName] has been updated	fname=deviceName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Device fileId=deviceId
フィルター			
logger:500	/Logger/Resource/Filter/Configuration/Add	Filter [filterName] has been added	fname=filterName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Filter fileId=filterId
logger:501	/Logger/Resource/Filter/Configuration/Delete	Filter [filterName] has been deleted	fname=filterName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Filter fileId=filterId
logger:502	/Logger/Resource/Filter/Configuration/Update	Filter [filterName] has been updated	fname=filterName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Filter fileId=filterId
グループ			

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:513	/Logger/Resource/Group/Configuration/Add	Group [groupName] has been added	fname=groupName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Group fileId=groupId
logger:514	/Logger/Resource/Group/Configuration/Delete	Group [groupName] has been deleted	fname=groupName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Group fileId=groupId
logger:515	/Logger/Resource/Group/Configuration/Update	Group [groupName] has been updated	fname=groupName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Group fileId=groupId
ピアLogger			
logger:550	/Logger/Resource/PeerLogger/Configuration/Add	Peer Logger [name] has been added	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger fileId=LoggerId
logger:551	/Logger/Resource/PeerLogger/Configuration/Delete	Peer Logger [name] has been deleted	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger fileId=LoggerId
logger:570	/Logger/Resource/Peer/Authorizations/Configuration/Add	Peer Logger authorization [name] has been added	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger Authorization

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:571	/Logger/Resource/PeerLogger/Authorizations/Configuration/Delete	Peer Logger authorization [name] has been deleted	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger Authorization fileId=LoggerId
パーサー			
logger:590	/Logger/Resource/ParserDescription/Configuration/Add	Parser Description [name] has been added	fileType=Parser Description duid=1 cs4=sessionIdfile cs4Label=Session ID duser=UserName rt=receiptTime fname=parserName
logger:591	/Logger/Resource/ParserDescription/Configuration/Delete	Parser Description [name] has been deleted	fileType=Parser Description cs4=sessionIdfile duser=UserName fileId=ParserID 710 duid=1 cs4Label=Session ID rt=receiptTime fname=parserName
logger:592	/Logger/Resource/ParserDescription/Configuration/Update	Parser Description [name] has been updated	fileType=Parser Description cs4=sessionIdfile duser=UserName fileId=ParserID duid=1 cs4Label=Session ID rt=receiptTime fname=parserName
保存された検索			
logger:540	/Logger/Resource/SavedSearch/Configuration/Add	Saved search [name] has been added	fname=savedSearchName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Saved Search fileId=savedSearchId

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:541	/Logger/Resource/SavedSearch/Configuration/Delete	Saved search [name] has been deleted	fname=savedSearchName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Saved Search fileId=savedSearchId
logger:542	/Logger/Resource/SavedSearch/Configuration/Update	Saved search [name] has been updated	fname=savedSearchName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Saved Search fileId=savedSearchId
ソースタイプ			
logger:596	/Logger/Resource/SourceType/Configuration/Add	Source Type [name] has been added	cs4=sessionIdfile fileType=Source Type duid=1 cs4Label=Session ID duser=UserName rt=receiptTime fname=SourceTypeName
logger:597	/Logger/Resource/SourceType/Configuration/Delete	Source Type [name] has been deleted	fileType=Source Type cs4=sessionIdfile duser=UserName fileId=SourceTypeID duid=1 cs4Label=Session ID rt=receiptTime fname=SourceTypeName
logger:598	/Logger/Resource/SourceType/Configuration/Update	Source Type [name] has been updated	fileType=Source Type cs4=sessionIdfile duser=UserName fileId=1SourceTypeID duid=1 cs4Label=Session ID rt=receiptTime fname=SourceTypeName
ストレージグループ			

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:530	/Logger/Resource/StorageGroup/Configuration/Add	Storage group [storageGroupName] has been added	fname=storageGroupName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Storage Group fileId=storageGroupId
logger:532	/Logger/Resource/StorageGroup/Configuration/Update	Storage group [storageGroupName] has been updated	fname=storageGroupName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Storage Group fileId=storageGroupId
ストレージルール			
logger:533	/Logger/Resource/StorageRule/Configuration/Add	Storage rule [name] has been added	fname=storageRuleName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Storage Rule
logger:535	/Logger/Resource/StorageRule/Configuration/Update	Storage rule [name] has been updated	fname=storageRuleName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Storage Rule
ストレージボリューム			
logger:536	/Logger/Resource/StorageVolume/Configuration/Add	Storage volume [name] has been added	fname=storageVolumeName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Storage Volume fileId=storageVolumeId
検索			

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:680	/Logger/Search/Index/Update	Search indices have been added または Search index has been added	cs4=sessionId fileType=Search Index Configuration duser=UserName msg=Search index has been added cn1=1 duid=1 cs4Label=Session ID rt=receiptTime cn1Label=No. of fields added
logger:690	/Logger/Search/Options/Update	Search options have been updated	cs6=false cs7=true cs4=sessionId cs5=false cs2=false cs3=false cs1=true cs8=false cs1Label=Field Search Case Sensitivity duid=1 cs7Label=Field Summary cs8Label=Field Summary Field Discovery cs6Label=Display options raw Event cs3Label=Regex Search Unicode Case Sensitivity fileType=Search Options duser=UserName cs5Label=Regex Search Canonical Equality Check cs4Label=Session ID rt=receiptTime cs2Label=Regex Search Case Sensitivity

デバイスイベントクラスID	デバイスイベントカテゴリ (cat)	メッセージ	追加フィールド
logger:710	/Logger/Search/Canceled	Search session [sessionID] has been canceled by [user]	cs1Label=Session ID duid=1 cs1=sessionIdfile duser=UserName rt=receiptTime
メンテナンスモード			
logger:700	/Logger/Server/MaintenanceMode/Enter	Maintenance mode entered	fname=Maintenance Mode duser=UserName duid=userId cs4=sessionId cs4Label=Session ID fileType=Maintenance Mode

付 録 E: システムヘルスイベントの例

次 の表 では、Loggerで生 成 されるシステムヘルスイベントの例 を示 します。これらの例 は、生 成 されるイベントの形 式 と各 種 フィールドについての理 解 を助 けることを目 的 としています。

注 : システムヘルスイベントが生 成 されたときに起 動 されるアラートを設 定 できます。詳 細 については、「保 存 された検 索 」(333ページ) を参 照 してください。

この表 には、以 下 のシステムヘルスイベントクラスについての情 報 が含 まれています。

デバイスイベントクラスID	例
cpu	
cpu:100	CEF:0|ArcSight|Logger|5.1.0.5780.0|cpu:100|CPU Usage|1| cat=/Monitor/CPU/Usage cn1=3 cn1Label=Percent Usage cs2=CurrentValue cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6 end=1302739080014 rt=1302739080014
ディスク	
disk:101	CEF:0|ArcSight|Logger|5.1.0.5803.0|disk:101|Root Disk Space Remaining|1| cat=/Monitor/Disk/Space/Remaining/Root cn1=99 cn1Label=Percent Available cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=Ok cs4Label=Raw Status cs5=Root cs5Label=Location cs6=Disk/Space/Remaining/Root cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1303927171790 rt=1303927171790
disk:102	CEF:0|ArcSight|Logger|5.1.0.5780.0|disk:102|Disk bytes read|1| cat=/Monitor/Disk/Read cn1=373524 cn1Label=Kb Read cs2=SinceStartup cs2Label=timeframe cs6=c0d0 cs6Label=Partition Name dst=192.0.2.6 dvc=192.0.2.6 end=1302743760036 rt=1302743760036
disk:103	CEF:0|ArcSight|Logger|5.1.0.5780.0|disk:103|Disk bytes written|1| cat=/Monitor/Disk/Write cn1=24474998 cn1Label=Kb Written cs2=SinceStartup cs2Label=timeframe cs6=c0d0 cs6Label=Partition Name dst=192.0.2.6 dvc=192.0.2.6 end=1302743760038 rt=1302743760038
eps	
eps:100	CEF:0|ArcSight|Logger|5.1.0.5780.0|eps:100|Overall Receiver EPS|1| cat=/Monitor/Receiver/All/EPS cn1=0 cn1Label=EPS cs2=SinceLastMonitorEvent cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6 end=1302733680034 rt=1302733680034

デバイスイベントクラスID	例
eps:101	CEF:0|ArcSight|Logger|5.1.0.5780.0|eps:101|Overall Forwarder EPS|1| cat=/Monitor/Forwarder/All/EPS cn1=0 cn1Label=EPS cs2=SinceLastMonitorEvent cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6
eps:102	CEF:0|ArcSight|Logger|6.1.0.0.1|eps:102|Individual Receiver EPS|1| cat=/Monitor/Receiver/EPS/Individual cn1=0 cn1Label=EPS cn2=0 cn2Label=EVENT COUNT cs1=TCP cs1Label=Receiver Type cs2=SinceLastMonitorEvent cs2Label=timeframe cs3=up cs3Label=STATUS cs6=TCP Receiver cs6Label=Receiver name dst=192.0.2.6 dvc=192.0.2.6 end=1420620420064 rt=1420620420064
eps:103	CEF:0|ArcSight|Logger|6.1.0.0.1|eps:103|Individual Forwarder EPS|1| cat=/Monitor/Forwarder/EPS/Individual cn1=0 cn1Label=EPS cn2=0 cn2Label=EVENT COUNT cs1=TCP cs1Label=Forwarder Type cs2=SinceLastMonitorEvent cs2Label=timeframe cs3=up cs3Label=STATUS cs6=TCP Forwarder cs6Label=Forwarder name dst=192.0.2.6 dvc=192.0.2.6 end=1420620420064 rt=1420620420064
ハードウェア	
hardware:101	CEF:0|ArcSight|Logger|5.1.0.5784.0|hardware:101|Electrical (Current) OK|1| cat=/Monitor/Sensor/Current/Ok cs1=0.80 Amps cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=ok cs4Label=Raw Status cs5=10.2 (Power Supply) cs5Label=Location cs6=Current 2 cs6Label=Sensor Name dst=192.0.2.5 dvc=192.0.2.5 end=1303937520837 rt=1303937520837
hardware:102	CEF:0|ArcSight|Logger|5.1.0.5776.0|hardware:102|Electrical (Current) Degraded|5| cat=/Monitor/Sensor/Current/Degraded cs1=126 Watts cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Degraded cs3Label=Status cs4=lnc cs4Label=Raw Status cs5Label=Location cs6=Power Meter cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302817019262 rt=1302817019262
hardware:103	CEF:0|ArcSight|Logger|5.1.0.5776.0|hardware:103|Electrical (Current) Failed|8| cat=/Monitor/Sensor/Current/Failed cs1=126 Watts cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=lcr cs4Label=Raw Status cs5Label=Location cs6=Power Meter cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302817019262 rt=1302817019262
hardware:111	CEF:0|ArcSight|Logger|5.1.0.5780.0|hardware:111|Electrical (Voltage) OK|1| cat=/Monitor/Sensor/Voltage/Ok cs1=State Deasserted cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=ok cs4Label=Raw Status cs5=3.1 (Processor) cs5Label=Location cs6=VCORE cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302819047959 rt=1302819047959

デバイスイベントクラスID	例
hardware:112	CEF:0|ArcSight|Logger|5.1.0.5780.0|hardware:112|Electrical (Voltage) Degraded|5| cat=/Monitor/Sensor/Voltage/Degraded cs1=State Deasserted cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Degraded cs3Label=Status cs4=Inc cs4Label=Raw Status cs5=3.1 (Processor) cs5Label=Location cs6=VCORE cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302819047959 rt=1302819047959
hardware:113	CEF:0|ArcSight|Logger|5.1.0.5780.0|hardware:113|Electrical (Voltage) Failed|8| cat=/Monitor/Sensor/Voltage/Failed cs1=State Deasserted cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=Icr cs4Label=Raw Status cs5=3.1 (Processor) cs5Label=Location cs6=VCORE cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302819047959 rt=1302819047959
hardware:121	CEF:0|ArcSight|Logger|5.1.0.5803.0|hardware:121|Battery OK|1| cat=/Monitor/Sensor/Battery/Ok cs1=cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=ok cs4Label=Raw Status cs5=7.1 (System Board) cs5Label=Location cs6=CMOS Battery cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1303937972008 rt=1303937972008
hardware:122	CEF:0|ArcSight|Logger|5.1.0.5803.0|hardware:122|Battery Degraded|5| cat=/Monitor/Sensor/Battery/Degraded cs1=cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Degraded cs3Label=Status cs4=Inc cs4Label=Raw Status cs5=7.1 (System Board) cs5Label=Location cs6=CMOS Battery cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1303937972008 rt=1303937972008
hardware:123	CEF:0|ArcSight|Logger|5.1.0.5803.0|hardware:123|Battery Failed|8| cat=/Monitor/Sensor/Battery/Degraded cs1=cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=Icr cs4Label=Raw Status cs5=7.1 (System Board) cs5Label=Location cs6=CMOS Battery cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1303937972008 rt=1303937972008
hardware:131	CEF:0|ArcSight|Logger|5.1.0.5780.0|hardware:131|Fan OK|1| cat=/Monitor/Sensor/Fan/Ok cs1=29.01 unspecified cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=Inc cs4Label=Raw Status cs5=7.1 (System Board) cs5Label=Location cs6=Fan Block 1 cs6Label=Sensor Name dst=192.0.2.1 dvc=192.0.2.1 end=1302823237825 rt=1302823237825
hardware:132	
hardware:133	CEF:0|ArcSight|Logger|5.1.0.5780.0|hardware:133|Fan Failure|8| cat=/Monitor/Sensor/Fan/Failed cs1=29.01 unspecified cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=Icr cs4Label=Raw Status cs5=7.1 (System Board) cs5Label=Location cs6=Fan Block 1 cs6Label=Sensor Name dst=192.0.2.1 dvc=192.0.2.1 end=1302823237825 rt=1302823237825

デバイスイベントクラスID	例
hardware:141	CEF:0|ArcSight|Logger|5.1.0.5803.0|hardware:141|Power Supply OK|1| cat=/Monitor/Sensor/PowerSupply/Ok cs1=cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=ok cs4Label=Raw Status cs5=10.1 (Power Supply) cs5Label=Location cs6=Status cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1303938572149 rt=1303938572149
hardware:142	
hardware:143	CEF:0|ArcSight|Logger|5.1.0.5776.0|hardware:143|Power Supply Failed|8| cat=/Monitor/Sensor/PowerSupply/Failed cs1=0 Watts cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=lcr cs4Label=Raw Status cs5=10.2 (Power Supply) cs5Label=Location cs6=Power Supply 2 cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302817019263 rt=1302817019263
hardware:151	CEF:0|ArcSight|Logger|5.1.0.5776.0|hardware:151|Temperature OK|1| cat=/Monitor/Sensor/Temperature/Ok cs1=17 degrees C cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=ok cs4Label=Raw Status cs5=64.1 (Unknown (0x40)) cs5Label=Location cs6=Temp 1 cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302823560051 rt=1302823560051
hardware:152	
hardware:153	
メモリ	
memory:100	CEF:0|ArcSight|Logger|5.1.0.5780.0|memory:100|Platform Memory Usage|1| cat=/Monitor/Memory/Usage/Platform cn1=2757 cn1Label=MB Used cs2=CurrentValue cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6 end=1302797940018 rt=1302797940018
ネットワーク	
network:100	CEF:0|ArcSight|Logger|5.1.0.5780.0|network:100|Network Usage - Inbound|1| cat=/Monitor/Network/Usage/In cn1=41837428 cn1Label=Bytes Received cs2=SinceStartup cs2Label=timeframe cs6=eth0 cs6Label=Interface Name dst=192.0.2.6 dvc=192.0.2.6 end=1302733620026 rt=1302733620026
network:101	CEF:0|ArcSight|Logger|5.1.0.5780.0|network:101|Network Usage - Outbound|1| cat=/Monitor/Network/Usage/Out cn1=158442791 cn1Label=Bytes Sent cs2=SinceStartup cs2Label=timeframe cs6=eth0 cs6Label=Interface Name dst=192.0.2.6 dvc=192.0.2.6 end=1302733620028 rt=1302733620028
raid	

デバイスイベントクラスID	例
raid:101	CEF:0|ArcSight|Logger|5.1.0.5780.0|raid:101|RAID Controller OK|1| cat=/Monitor/RAID/Controller/Ok cs1=Type: RAID-5 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=Optimal cs4Label=Raw Status cs5=RAIDController/Configuration cs5Label=Location cs6=RAIDController/Configuration cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302886250104 rt=1302886250104
raid:102	CEF:0|ArcSight|Logger|5.1.0.5780.0|raid:102|RAID Controller Degraded|5| cat=/Monitor/RAID/ControllerDegraded cs1=Type: RAID-5 Critical Disks: 0 Failed Disks: 0 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Degraded cs3Label=Status cs4=Degraded cs4Label=Raw Status cs5=RAIDController/Configuration cs5Label=Location cs6=RAIDController/Configuration cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302826128482 rt=1302826128482
raid:103	
raid:111	CEF:0|ArcSight|Logger|5.1.0.5776.0|raid:111|RAID BBU OK|1| cat=/Monitor/RAID/BBU/Ok cs1=Battery/Capacitor Count: 1 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=OK cs4Label=Raw Status cs5=RAIDController/Battery/bbu cs5Label=Location cs6=RAIDController/Battery/bbu cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302890169285 rt=1302890169285
raid:112	CEF:0|ArcSight|Logger|5.1.0.5780.0|raid:112|RAID BBU Degraded|5| cat=/Monitor/RAID/BBU/Degraded cs1=Fully Charged: false Remaining Time Alarm: false Remaining Capacity Alarm: false Over Charged: false isSOHGood: true cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Degraded cs3Label=Status cs4=Degraded cs4Label=Raw Status cs5=RAIDController/Battery/bbu cs5Label=Location cs6=RAIDController/Battery/bbu cs6Label=Sensor Name dst=192.0.2.6 dvc=192.0.2.6 end=1302820608015 rt=1302820608015
raid:113	
raid:121	CEF:0|ArcSight|Logger|5.1.0.5780.0|raid:121|RAID Disk OK|1| cat=/Monitor/RAID/DISK/Ok cs1=Port: 1I Box: 1 Bay: 1 Size: 500 GB Serial Number: 9SP24JD5 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Ok cs3Label=Status cs4=OK cs4Label=Raw Status cs5=Port: 1I Box: 1 Bay: 1 Serial Number: 9SP24JD5 cs5Label=Location cs6=RAIDController/Port/p0 cs6Label=Sensor Name dst=192.0.2.1 dvc=192.0.2.1 end=1302849041777 rt=1302849041777

デバイスイベントクラスID	例
raid:122	CEF:0|ArcSight|Logger|5.1.0.5776.0|raid:122|RAID Disk Rebuilding|5| cat=/Monitor/RAID/DISK/Rebuilding cs1=Port: 2I Box: 1 Bay: 1 Size: 1 TB Serial Number: WMATV6348517 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Rebuilding cs3Label=Status cs4=Rebuilding cs4Label=Raw Status cs5=Port: 2I Box: 1 Bay: 1 Serial Number: WMATV6348517 cs5Label=Location cs6=RAIDController/Port/p0 cs6Label=Sensor Name dst=192.0.2.4 dvc=192.0.2.4 end=1302826980530 rt=1302826980530
raid:123	CEF:0|ArcSight|Logger|5.1.0.5780.0|raid:123|RAID Disk Failed|8| cat=/Monitor/RAID/DISK/Failed cs1=Port: 1I Box: 1 Bay: 2 Size: 500 GB Serial Number: 9SP23M08 cs1Label=Raw Value cs2=CurrentValue cs2Label=timeframe cs3=Failed cs3Label=Status cs4=Failed cs4Label=Raw Status cs5=Port: 1I Box: 1 Bay: 2 Serial Number: 9SP23M08 cs5Label=Location cs6=RAIDController/Port/p1 cs6Label=Sensor Name dst=192.0.2.1 dvc=192.0.2.1 end=1302826358346 rt=1302826358346
検索	
search:100	CEF:0|ArcSight|Logger|5.1.0.5780.0|search:100|Number of Searches Performed|1| cat=/Monitor/Search cn1=0 cn1Label=Number of Searches cs2=SinceStartup cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6 end=1302741300026 rt=1302741300026
ストレージグループ	
storagegroup:100	CEF:0|ArcSight|Logger|5.1.0.5803.0|storagegroup:100|Storage Group Space Used|1| cat=/Monitor/StorageGroup/Space/Used cn1=1 cn1Label=Percent Used cn2=7 cn2Label=retention period (days) cn3=1024 cn3Label=used (MB) cs2=CurrentValue cs2Label=timeframe dst=192.0.2.6 dvc=192.0.2.6 end=1303928072008 fileType=storageGroup fname=Default Storage Group fsize=1534 rt=1303928072008

付録F: イベントフィールド名のマッピング

フィールド名の体系は、Loggerの機能領域に依存します。次の表に、これらの間のマッピングを示します。

- **データベース名:** このフィールドのインデックスを作成するときに、データベース内に作成されたフィールド名。インデックスが作成されていないフィールドのデータベース名はありません。このフィールド名は、レポートを生成するためのSQLクエリを作成するときに使用します。
- **検索結果:** 検索によりこのフィールドのデータが返される場合に、検索結果に表示されるフィールド名。
- **CEFフィールド名:** 『Implementing ArcSight CEF』で定義されたキーまたはフィールド名。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品マニュアルのコミュニティで「ArcSight Common Event Format (CEF) Guide」を検索してください。
- **レポート:** このフィールドから取得したデータを含むレポートに表示されるフィールド名。

データベース名	検索結果	CEFフィールド名	レポート
arc_agentAddress	agentAddress	agt	エージェントアドレス
arc_agentHostName	agentHostName	ahost	エージェントのホスト名
arc_agentNtDomain	agentNtDomain	agentNtDomain	エージェントのNTドメイン
arc_agentSeverity	agentSeverity	Severity	緊急度
arc_agentType	agentType	at	エージェントタイプ
arc_agentZone	agentZone	agentZone	エージェントゾーン
arc_agentZoneName	agentZoneName	agentZoneName	エージェントゾーン名
arc_agentZoneResource	agentZoneResource	agentZoneResource	エージェントゾーンリソース
arc_agentZoneURI	agentZoneURI	agentZoneURI	エージェントゾーンURI
arc_applicationProtocol	applicationProtocol	app	アプリケーションプロトコル

データベース名	検索結果	CEFフィールド名	レポート
arc_baseEventCount	baseEventCount	cnt	ベースイベント数
arc_bytesIn	bytesIn	in	受信バイト数
arc_bytesOut	bytesOut	out	送信バイト数
arc_categoryBehavior	categoryBehavior	categoryBehavior	カテゴリ動作
arc_categoryDeviceGroup	categoryDeviceGroup	categoryDeviceGroup	カテゴリデバイスグループ
arc_categoryObject	categoryObject	categoryObject	カテゴリオブジェクト
arc_categoryOutcome	categoryOutcome	categoryOutcome	カテゴリ結果
arc_categorySignificance	categorySignificance	categorySignificance	カテゴリ重要性
arc_categoryTechnique	categoryTechnique	categoryTechnique	カテゴリ技術
arc_customerName	customerName	customerName	顧客名
arc_destinationAddress	destinationAddress	dst	通知先アドレス
arc_destinationDnsDomain	destinationDnsDomain	destinationDnsDomain	通知先DNSドメイン
arc_destinationHostName	destinationHostName	dhost	通知先ホスト名
arc_ destinationMacAddress	destinationMacAddress	dmac	通知先MACアドレス
arc_destinationNtDomain	destinationNtDomain	dntdom	通知先NTドメイン
arc_destinationPort	destinationPort	dpt	通知先ポート
arc_ destinationProcessName	destinationProcessName	dproc	通知先プロセス名
arc_ destinationServiceName	destinationServiceName	destinationServiceName	通知先サービス名
arc_ destinationTranslatedAddress	destinationTranslatedAddress	destinationTranslatedAddress	通知先変換アドレス
arc_destinationUserId	destinationUserId	duid	通知先ユーザID
arc_destinationUserName	destinationUserName	duser	通知先ユーザ名

データベース名	検索結果	CEFフィールド名	レポート
arc_destinationUserPrivileges	destinationUserPrivileges	dpriv	通知先ユーザ権限
arc_destinationZone	destinationZone	destinationZone	通知先ゾーン
arc_destinationZoneName	destinationZoneName	destinationZoneName	通知先ゾーン名
arc_destinationZoneResource	destinationZoneResource	destinationZoneResource	通知先ゾーンのリソース
arc_destinationZoneURI	destinationZoneURI	destinationZoneURI	通知先ゾーンURI
arc_deviceAction	deviceAction	act	デバイスのアクション
arc_deviceAddress	deviceAddress	dvc	デバイスアドレス
arc_deviceCustomDate1	deviceCustomDate1	deviceCustomDate1	デバイスのカスタム日付1
arc_deviceCustomDate1Label	deviceCustomDate1Label	deviceCustomDate1Label	デバイスのカスタム日付1ラベル
arc_deviceCustomDate2	deviceCustomDate2	deviceCustomDate2	デバイスのカスタム日付2
arc_deviceCustomDate2Label	deviceCustomDate2Label	deviceCustomDate2Label	デバイスのカスタム日付2ラベル
arc_deviceCustomNumber1	deviceCustomNumber1	cn1	デバイスカスタム数1
arc_deviceCustomNumber1Label	deviceCustomNumber1Label	cn1Label	デバイスカスタム数1ラベル
arc_deviceCustomNumber2	deviceCustomNumber2	cn2	デバイスカスタム数2
arc_deviceCustomNumber2Label	deviceCustomNumber2Label	cn2Label	デバイスカスタム数2ラベル
arc_deviceCustomNumber3	deviceCustomNumber3	cn3	デバイスカスタム数3
arc_deviceCustomNumber3Label	deviceCustomNumber3Label	cn3Label	デバイスカスタム数3ラベル

データベース名	検索結果	CEFフィールド名	レポート
arc_deviceCustomString1	deviceCustomString1	cs1	デバイスカスタム文字列1
arc_deviceCustomString1Label	deviceCustomString1Label	cs1Label	デバイスカスタム文字列1ラベル
arc_deviceCustomString2	deviceCustomString2	cs2	デバイスカスタム文字列2
arc_deviceCustomString2Label	deviceCustomString2Label	cs2Label	デバイス カスタム文字列2ラベル
arc_deviceCustomString3	deviceCustomString3	cs3	デバイスカスタム文字列3
arc_deviceCustomString3Label	deviceCustomString3Label	cs3Label	デバイスカスタム文字列3ラベル
arc_deviceCustomString4	deviceCustomString4	cs4	デバイスカスタム文字列4
arc_deviceCustomString4Label	deviceCustomString4Label	cs4Label	デバイスカスタム文字列4ラベル
arc_deviceCustomString5	deviceCustomString5	cs5	デバイスカスタム文字列5
arc_deviceCustomString5Label	deviceCustomString5Label	cs5Label	デバイスカスタム文字列5ラベル
arc_deviceCustomString6	deviceCustomString6	cs6	デバイスカスタム文字列6
arc_deviceCustomString6Label	deviceCustomString6Label	cs6Label	デバイス カスタム文字列6ラベル
arc_deviceEventCategory	deviceEventCategory	cat	デバイスイベントカテゴリ
arc_deviceEventClassId	deviceEventClassId	Signature ID	署名ID
arc_deviceExternalId	deviceExternalId	deviceExternalId	デバイス外部ID
arc_deviceHostName	deviceHostName	dvchost	デバイスホスト名
arc_deviceInboundInterface	deviceInboundInterface	deviceInboundInterface	デバイスインバウンド インターフェイス
arc_deviceOutboundInterface	deviceOutboundInterface	deviceOutboundInterface	デバイスアウトバウンド インターフェイス

データベース名	検索結果	CEFフィールド名	レポート
arc_deviceProduct	deviceProduct	Device Product	デバイス製品
arc_deviceReceiptTime	deviceReceiptTime	rt	デバイス受信時刻
arc_deviceSeverity	deviceSeverity	deviceSeverity	デバイスの緊急度
arc_deviceVendor	deviceVendor	Device Vendor	デバイスベンダ
arc_deviceVersion	deviceVersion	Device Version	デバイスバージョン
arc_deviceZone	deviceZone	deviceZone	デバイスゾーン
arc_deviceZoneName	deviceZoneName	deviceZoneName	デバイスゾーン名
arc_deviceZoneResource	deviceZoneResource	deviceZoneResource	デバイスゾーンリソース
arc_deviceZoneURI	deviceZoneURI	deviceZoneURI	デバイスゾーンURI
arc_endTime	endTime	end	終了時刻
arc_eventId	eventId	eventId	イベントID
arc_externalId	externalId	externalId	外部ID
arc_fileName	fileName	fname	ファイル名
arc_filePath	filePath	filePath	ファイルパス
arc_flexDate1	flexDate1	flexDate1	フレックス日付1
arc_flexDate1Label	flexDate1Label	flexDate1Label	フレックス日付1ラベル
arc_flexNumber1	flexNumber1	flexNumber1	フレックス番号1
arc_flexNumber1Label	flexNumber1Label	flexNumber1Label	フレックス番号1ラベル
arc_flexNumber2	flexNumber2	flexNumber2	フレックス番号2
arc_flexNumber2Label	flexNumber2Label	flexNumber2Label	フレックス番号2ラベル
arc_flexString1	flexString1	flexString1	フレックス文字列1
arc_flexString1Label	flexString1Label	flexString1Label	フレックス文字列1ラベル

データベース名	検索結果	CEFフィールド名	レポート
arc_flexString2	flexString2	flexString2	フレックス文字列2
arc_flexString2Label	flexString2Label	flexString2Label	フレックス文字列2ラベル
arc_message	message	msg	メッセージ
arc_name	name	Name	名前
arc_priority	priority	priority	重要度
arc_requestClientApplication	requestClientApplication	requestClientApplication	リクエストクライアントアプリケーション
arc_requestContext	requestContext	requestContext	リクエストコンテクスト
arc_requestMethod	requestMethod	requestMethod	リクエストメソッド
arc_requestUrl	requestUrl	request	リクエストURL
arc_requestUrlFileName	requestUrlFileName	requestUrlFileName	リクエストURLのファイル名
arc_requestUrlQuery	requestUrlQuery	requestUrlQuery	リクエストURLクエリ
arc_sessionId	sessionId	sessionId	セッションID
arc_sourceAddress	sourceAddress	src	ソースアドレス
arc_sourceHostName	sourceHostName	shost	ソースのホスト名
arc_sourceMacAddress	sourceMacAddress	smac	ソースMACアドレス
arc_sourceNtDomain	sourceNtDomain	sntdom	ソースNTドメイン
arc_sourcePort	sourcePort	spt	ソースポート
arc_sourceProcessName	sourceProcessName	sproc	ソースプロセス名
arc_sourceServiceName	sourceServiceName	sourceServiceName	ソースサービス名
arc_sourceTranslatedAddress	sourceTranslatedAddress	sourceTranslatedAddress	ソース変換アドレス
arc_sourceUserId	sourceUserId	suid	ソースユーザID

データベース名	検索結果	CEFフィールド名	レポート
arc_sourceUserName	sourceUserName	suser	ソースユーザ名
arc_sourceUserPrivileges	sourceUserPrivileges	spriv	ソースのユーザ権限
arc_sourceZone	sourceZone	sourceZone	ソースゾーン
arc_sourceZoneName	sourceZoneName	sourceZoneName	ソースゾーン名
arc_sourceZoneResource	sourcezoneResource	sourceZoneResource	ソースゾーンのリソース
arc_sourceZoneURI	sourceZoneURI	sourceZoneURI	ソースゾーンURI
arc_startTime	startTime	start	開始時刻
arc_transportProtocol	transportProtocol	proto	転送プロトコル
arc_type	type	type	タイプ
arc_vulnerabilityExternalID	vulnerabilityExternalID	vulnerabilityExternalID	脆弱性の外部ID
arc_vulnerabilityURI	VulnerabilityURI	vulnerabilityURI	脆弱性URI

付 録 G: Loggerコンテンツ

以 下 のトピックでは、デフォルト のLoggerレポート について説 明します。

レポート

Loggerでは、以 下 の表 に示 すレポート が提 供 されています。Logger UIでは、これらのレポートはカテゴリに表 示 されており、カテゴリエクスプローラ (左 ペイン) を通 じてアクセスできます。たとえば、「Top Infected Systems」レポート はAnti-Virusカテゴリ内 に表 示 され、Anti-Virusカテゴリは「Device Monitoring」という名 前 の親 カテゴリ内 に表 示 されます。

レポート には、他 のレポート にドリルダウンするハイパーリンクが含 まれています。たとえば、レポート「Most Common Events」には、Countという名 前 のフィールド が表 示 されます。Count フィールド をクリックすると、レポート「Target Attack Counts by Severity」にドリルダウンします。このレポート は、下 図 に示 すような詳 細 な情 報 を提 供 します。レポート 間 のドリルダウン関 係 を以 降 の表 に示 します。

Severity	Name	Count
Very-High	SMB: WinLogon DoS	2089
Very-High	IRC: Trojan.IrcBounce Command Channel	70
Very-High	Snort Alarm [1:2404:5]	58
Very-High	Host is DOWN	41
Very-High	ids syn attack	26
Very-High	RCRS/POP3_INVALID_ARG_TO_QUIT	16
Very-High		11

Severity	Target Zone	Target Address	Count
Very-High	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.0.0.10	57
Very-High	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.156.106.101	25
Very-High	/All Zones/ArcNet Zones/sj2.west.arcnet.com - internal	10.0.112.187	10
Very-High	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.0.0.10	10
Very-High	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 172.16.0.0-172.31.255.255	172.16.5.157	8

Loggerには、以 下 の最 上 位 カテゴリがあります。

Device Monitoring

このカテゴリは、デバイスまたはアプリケーションに基づいたイベントのビューを提供します。

Device Monitoringカテゴリの下には以下のカテゴリがあります。

Anti-Virus

これはDevice Monitoringカテゴリのサブカテゴリであり、アンチウイルスシステムに関連するイベントを対象としています。

Anti-Virusカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Anti-Virus
```

Anti-Virusカテゴリのレポートを以下の表に示します。

Anti-Virus

レポート	説明	ドリルダウン	パラメーター
Errors Detected in Anti-Virus Deployment	このレポートには、アンチウイルス製品情報、ホストの詳細、エラー情報、エラー数など、アンチウイルスエラーに関する情報の要約が表示されます。	なし	なし
Failed Anti-Virus Updates	このレポートには、デバイス、ベンダー、デバイス製品ターゲットゾーン名、ターゲットホスト名、ターゲットアドレス、分(EndTime)を含む表が表示されます。	なし	なし

Anti-Virus (続き)

レポート	説明	ドリルダウン	パラメーター
Top Infected Systems	このレポートには、最も感染を報告したシステムの要約が表示されます。	なし	なし
Update Summary	このレポートには、アンチウイルス更新処理の要約と詳細が表示されます。	なし	なし
Virus Activity by Hour	このレポートには、時間ごとのマルウェア活動が表示されます。	なし	なし

CrossDevice

これはDevice Monitoringカテゴリのサブカテゴリです。ログイン、起動、シャットダウンなど、複数のデバイス間で同じイベントに関する情報が表示されます。

CrossDeviceカテゴリは、以下のパスの下にあります。

```
Device Monitoring\CrossDevice
```

CrossDeviceカテゴリのレポートを以下の表に示します。

CrossDevice

レポート	説明	ドリルダウン	パラメーター
Bandwidth Usage by Hour	このレポートには、デバイスの種類ごとに時間あたりのネットワーク帯域幅使用量が表示されます。帯域幅の値は、ネットワーク内のトラフィックに加えて、内部と外部のソースとの間のトラフィックを含む、報告されたすべてのトラフィックに基づいていることに注意してください。デバイスを、ファイアウォール、ネットワーク機器、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Bandwidth Usage by Hour」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Bandwidth Usage by Protocol	このレポートには、デバイスの種類ごとに、帯域幅使用量でソートされたすべてのプロトコルが表示されます。帯域幅の値は、ネットワーク内のトラフィックに加えて、内部と外部のソースとの間のトラフィックを含む、報告されたすべてのトラフィックに基づいていることに注意してください。デバイスを、ファイアウォール、ネットワーク機器、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Bandwidth Usage by Protocol」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
By User Account - Accounts Created	このレポートには、Loggerに報告された、新たに作成されたすべてのアカウントが表示されます。	なし	なし
Configuration Changes by Type	このレポートには、Loggerに報告された最近の設定変更が表示されます。	Reporting Deviceフィールドは、「Configuration Changes by Type」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Configuration Changes by User	このレポートには、Loggerに報告された最近の設定変更が表示されます。	Reporting Deviceフィールドは、「Configuration Changes by User」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

CrossDevice (続き)

レポート	説明	ドリルダウン	パラメーター
Failed Login Attempts	このレポートには、時間ごとにログイン試行での認証失敗が表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Failed Login Attempts」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Failed Logins by Destination Address	このレポートには、宛先アドレスごとにログイン試行での認証失敗が表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Failed Logins by Destination Address」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Failed Logins by Source Address	このレポートには、ソースアドレスごとにログイン試行での認証失敗が表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Failed Logins by Source Address」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Failed Logins by User	このレポートには、ユーザーごとにログイン試行での認証失敗が表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Failed Logins by User」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

CrossDevice (続き)

レポート	説明	ドリルダウン	パラメーター
Login Event Audit	このレポートには、すべての認証イベントが表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Login Event Audit」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Password Changes	このレポートには、Loggerに報告されたすべてのパスワード変更が表示されます。	Reporting Deviceフィールドは、「Password Changes」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Successful Logins by Destination Address	このレポートには、成功した認証イベントが宛先アドレスごとに表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Successful Logins by Destination Address」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Successful Logins by Source Address	このレポートには、成功した認証イベントがソースアドレスごとに表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Successful Logins by Source Address」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

CrossDevice (続き)

レポート	説明	ドリルダウン	パラメーター
Successful Logins by User	このレポートには、成功した認証イベントがユーザーごとに表示されます。デバイスを、データベース、ファイアウォール、アイデンティティマネジメントシステム、ネットワーク機器、オペレーティングシステム、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Successful Logins by User」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Top Bandwidth Hosts	このレポートには、帯域幅使用量でソートされた上位ホストが表示されます。帯域幅の値は、ネットワーク内のトラフィックに加えて、内部と外部のソースとの間のトラフィックを含む、報告されたすべてのトラフィックに基づいていることに注意してください。デバイスを、ファイアウォール、ネットワーク機器、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	なし	なし
Top Hosts by Number of Connections	このレポートには、上位ホストごとに接続数の要約が表示されます。デバイスを、ファイアウォール、ネットワーク機器、VPNのいずれかに制限するためのパラメーターがあります。デフォルトでは、パラメーターは、データを報告するすべてのデバイスとアプリケーションに設定されています。	Reporting Deviceフィールドは、「Top Hosts by Number of Connections」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

Database

これは、Cross Deviceカテゴリのサブカテゴリであり、データベースのイベントを対象としています。

Databaseカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Database
```

Databaseカテゴリのレポートを以下の表に示します。

Database

レポート	説明	ドリルダウン	パラメーター
Database Errors and Warnings	このレポートには、最近のデータベースエラーと警告が表示されます。	なし	なし

Firewall

これは、Device Monitoringカテゴリのサブカテゴリであり、ファイアウォールのイベントを対象としています。

Firewallカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Firewall
```

Firewallカテゴリのレポートを以下の表に示します。

Firewall

レポート	説明	ドリルダウン	パラメーター
Denied Connections by Address	このレポートには、ファイアウォールデバイスによって拒否された着信および発信接続の要約と詳細が表示されます。	なし	なし
Denied Connections by Port	このレポートには、ファイアウォールデバイスによって拒否された着信および発信ポートの要約と詳細が表示されます。	なし	なし
Denied Connections per Hour	このレポートには、ファイアウォールデバイスによって拒否された着信および発信接続の要約と詳細が、時間ごとに表示されます。	なし	なし

IDS-IPS

これはDevice Monitoringカテゴリのサブカテゴリであり、侵入検知システムと侵入防止システムのイベントを対象としています。

IDS-IPSカテゴリは、以下のパスの下にあります。

```
Device Monitoring\IDS-IPS
```

IDS-IPSカテゴリのレポートを以下の表に示します。

IDS-IPS

レポート	説明	ドリルダウン	パラメーター
Alert Counts by Device	このレポートには、IDSアラートとIPSアラートの数が表示されます。	なし	なし
Alert Counts by Port	このレポートには、IDSアラートとIPSアラートの数が宛先ポートごとに表示されます。	なし	なし
Alert Counts by Severity	このレポートには、IDSアラートとIPSアラートの数がエージェントの緊急度ごとに表示されます。	なし	なし
Alert Counts by Type	このレポートには、IDSアラートとIPSアラートの数が種類 (カテゴリテクニック) ごとに表示されます。	なし	なし
Alert Counts per Hour	このレポートには、時間ごとのIDSアラートとIPSアラートの数が表示されます。	なし	なし
Top Alert Destinations	このレポートには、IDSアラートとIPSアラートの数が上位の宛先が表示されます。	なし	なし
Top Alerts from IDS and IPS	このレポートには、IDS (侵入検知システム) とIPS (侵入防止システム) から受信した上位のアラートが表示されます。	なし	なし
Top Alert Sources	このレポートには、IDSアラートとIPSアラート数が上位のソースが表示されます。	なし	なし
Worm Infected Systems	このレポートには、ワームに感染したシステムの一覧が表示されます。	なし	なし

Identity Management

これは、Device Monitoringカテゴリのサブカテゴリであり、アイデンティティマネジメントシステムのイベントを対象としています。

Identity Managementカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Identity Management
```

Identity Managementカテゴリのレポートを以下の表に示します。

Identity Management

レポート	説明	ドリルダウン	パラメーター
Connection Counts by User	このレポートには、Identity Managementデバイスによって報告されたユーザーごとの接続に関する数の情報が表示されます。	なし	なし

Network

これはDevice Monitoringカテゴリのサブカテゴリであり、ルーターやスイッチなどのネットワークデバイスを対象としています。

Networkカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Network
```

Networkカテゴリのレポートを以下の表に示します。

Network

レポート	説明	ドリルダウン	パラメーター
Device Critical Events	このレポートには、ネットワークデバイス上の重大なイベントに関する情報が表示されます。重大なイベントとは、ハードウェア障害、リソース不足、設定の問題、攻撃などを示すことがあります。	なし	なし
Device Errors	このレポートには、ネットワークデバイス上のエラーイベントに関する情報が表示されます。重大なイベントとは、ハードウェア障害、リソース不足、設定の問題、攻撃などを示すことがあります。	なし	なし
Device Events	このレポートには、ネットワークデバイス上のイベントに関する情報が表示されます。重大なイベントとは、ハードウェア障害、リソース不足、設定の問題、攻撃などを示すことがあります。	なし	なし
Device Interface Down Notifications	このレポートには、ダウンリンクを報告したネットワークデバイスを示す表が表示されます。	なし	なし
Device Interface Status Messages	このレポートには、リンクステータスの変化を報告したネットワークデバイスが表示されます。	なし	なし
Device SNMP Authentication Failures	このレポートには、ネットワークデバイスのSNMP障害に関する情報が表示されます。	なし	なし

Operating System

これは、Device Monitoringカテゴリのサブカテゴリであり、オペレーティングシステムのイベントを対象としています。

Operating Systemカテゴリは、以下のパスの下にあります。

```
Device Monitoring\Operating System
```

Operating Systemカテゴリのレポートを以下の表に示します。

Operating System

レポート	説明	ドリルダウン	パラメーター
Login Errors by User	このレポートには、ユーザー名ごとの失敗したログインの詳細 (時刻、イベント名、ソース、宛先) が表示されます。	なし	なし
User Administration	このレポートには、ユーザーとユーザーグループの作成、変更、削除が表示されます。	なし	なし

VPN

これは、Device Monitoringカテゴリのサブカテゴリであり、仮想プライベートネットワークのイベントを対象としています。

VPNカテゴリは、以下のパスの下にあります。

```
Device Monitoring\VPN
```

VPNカテゴリのレポートを以下の表に示します。

VPN

レポート	説明	ドリルダウン	パラメーター
Authentication Errors	このレポートには、VPN接続の試行によって生成されたエラーが表示されます。アドレスは、VPN接続元のIPアドレスです。このレポートは、VPNクライアントをうまく使用または設定できないユーザーを確認するために使用できます。	なし	なし
Connection Counts by User	このレポートには、各ユーザーのVPN接続に関する数の情報が表示されます。接続数、アクセスしたシステムを含め、各ユーザーの接続数の詳細が提供されます。	なし	なし
Connections Accepted by Address	このレポートには、成功したVPN接続のデータが表示されます。	なし	なし
Connections Denied by Address	このレポートには、拒否されたVPN接続のデータが表示されます。	なし	なし
Connections Denied by Hour	このレポートには、拒否されたVPN接続のデータが時間ごとに表示されます。	なし	なし

Foundation

このカテゴリは、セキュリティや境界防衛から、ネットワーク帯域幅使用状況、設定イベントまで、幅広いイベントを対象としています。

Foundationカテゴリの下には以下のカテゴリがあります。

Configuration Monitoring

このカテゴリは、システムおよびアプリケーションの設定変更を対象としています。

Configuration Monitoringカテゴリは、以下のパスの下にあります。

```
Foundation\Configuration Monitoring
```

Configuration Monitoringカテゴリのレポートを以下の表に示します。パラメーターはありません。

Configuration Monitoring

レポート	説明	ドリルダウン
Accounts Created by User Account	このレポートには、ネットワークホスト上で正常に作成されたアカウントの詳細が表示されます。表には、アカウント作成時刻のタイムスタンプ、作成されたアカウント名 (Destination User Name)、アカウントを作成したユーザーの名前 (Source User Name)、アカウント作成イベント名、アカウントが作成されたデバイスのゾーンとホスト名が含まれています。	なし
Accounts Deleted by Host	このレポートには、ユーザー削除の一覧が、顧客、ゾーン、システムごとに並べて提供されます。	なし
Accounts Deleted by User Account	このレポートには、削除日付、削除されたユーザー名、アカウントを削除したユーザーの名前、アカウント削除イベント名、アカウントを削除したシステムのゾーンとホスト名を示す表が表示されます。	なし
Anti-Virus Updates-All-Failed	このレポートには、失敗したすべてのアンチウイルス更新イベントのデバイス、ベンダー、デバイス製品ターゲットゾーン名、ターゲットホスト名、ターゲットアドレス、分 (EndTime) を含む表が表示されます。	なし
Anti-Virus Updates-All-Summary	このレポートには、すべてのアンチウイルスイベントのターゲットゾーン名、ターゲットホスト名、ターゲットアドレス、デバイスベンダー、デバイス製品、カテゴリ、集約したイベント数の合計を示す表が表示されます。	なし

Configuration Monitoring (続き)

レポート	説明	ドリルダウン
Asset Startup and Shutdown Event Log	このレポートには、システムの起動およびシャットダウンイベントの一覧が表示されます。	なし
Device Configuration Changes	このレポートには、成功したデバイス設定変更イベントに関連するイベントが表で示されます。ここには、デバイスグループ、ゾーン、アドレスおよびホスト名、設定イベント名、変更を行ったユーザーIDおよび名前、変更を行った時間などが表示されます。[デバイスグループ] カラムのデバイスエントリをクリックすると、新しくDevice Configuration Changes Drilldownレポートが開きます。このレポートでは、特定のデバイスタイプの設定イベントのみが表示されます。	Device Group フィールドは、「Device Configuration Changes」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Device Configuration Events	このレポートには、イベントの成否を問わず、さまざまなデバイス設定変更イベントに関連するイベントが表で示されます。ここには、デバイスグループ、ゾーン、アドレスおよびホスト名、設定イベント名、変更を行ったユーザーIDおよび名前、変更を行った時間などが表示されます。[デバイスグループ] カラムのデバイスエントリをクリックすると、新しくDevice Configuration Events Drilldownレポートが開きます。このレポートでは、特定のデバイスタイプの設定イベントのみが表示されます。	Device Group フィールドは、「Device Configuration Events」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Device Misconfigurations	このレポートには、デバイス設定チェックに関連するイベントが表で示されます。ここには、デバイスグループ、ゾーン、アドレスおよびホスト名、設定ミスの名前、検出された設定ミスの数などが表示されます。Device Groupエントリをクリックすると、クリックしたデバイスタイプに焦点を当てたDevice Misconfigurations Drilldownレポートが実行されます。	Device Group フィールドは、「Device Misconfigurations」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Password Changes	このレポートには、パスワードを変更したユーザーアカウントの表が表示されます。表には、パスワードを変更した時刻、新たにパスワードを設定したアカウントのユーザー名、パスワードを変更したシステムのゾーンとアドレス、変更の開始元のゾーンとアドレスが表示されます。	なし
Vulnerability Scanner Logs by Host	このレポートには、脆弱性スキャナーのログが、ゾーンとホストIPアドレスごとにグループ化されて表示されます。	なし
Vulnerability Scanner Logs by Vulnerability	このレポートには、脆弱性スキャナーのログが、脆弱性のIDと名前でグループ化されて表示されます。	なし

Intrusion Monitoring

これは、Foundationカテゴリのサブカテゴリであり、セキュリティ、境界防御、リソースアクセス、ユーザー追跡イベントを対象にしています。

Intrusion Monitoringカテゴリは、以下のパスの下にあります。

```
Foundation\Intrusion Monitoring
```

Intrusion Monitoringカテゴリのレポートを以下の表に示します。パラメーターはありません。

Intrusion Monitoring

レポート	説明	ドリルダウン
Firewall Traffic by Service	このレポートには、ファイアウォールから報告されたポート、トランスポートプロトコル、アプリケーションプロトコル、イベント数を示す表が表示されます。	なし
Least Common Events	このレポートには、選択した期間内のすべてのイベントが表示されます。イベントは、集約されたイベントの総数の昇順に並べられます。利便性を高めるため、列はハイパーリンクになっています。Event Nameをクリックすると、同じ期間を使用したBottom Destinationsレポートが表示されます。Countをクリックすると、同じ期間を使用したBottom Sourcesレポートが表示されます。	Event Nameフィールドは、「Bottom Destinations」レポートにドリルダウンします。 Countフィールドは、「Bottom Sources」レポートにドリルダウンします。
Most Common Events	このレポートには、指定した時間範囲内に最も頻繁に発生した200個のイベントが表示されます。イベント名はハイパーリンクになっており、Destination Counts by Event Nameレポートにドリルダウンできるようになっており、選択したイベントの宛先情報が表示されます。Countフィールドは、宛先ポートごとのすべてのソースに関する情報を含むSource Counts by Destination Portレポートを表示します。	arc_nameフィールドは、「Destination Counts by Event Name」レポートにドリルダウンします。 SUM(events.arc_baseEventCount)フィールドは、「Source Counts by Destination Port」レポートにドリルダウンします。
Most Common Events by Severity	このレポートには、緊急度、イベント名、イベント数を降順に示す表が表示されます。	Severityフィールドは、「Source Counts by Device Severity」レポートにドリルダウンします。 Countフィールドは、「Destination Counts by Device Severity」レポートにドリルダウンします。

Intrusion Monitoring (続き)

レポート	説明	ドリルダウン
Probes on Blocked Ports by Source	このレポートには、宛先ポートが一般にブロックされるポートのリストに含まれているイベントのソースゾーン、アドレスとホスト名、トランスポートプロトコル、宛先ポート、イベント数を示すイベントの表が表示されます。クエリはcommonlyblockedPortsパラメーターを使用します。このパラメーターを編集して他のポートを追加することができます (Foundation Contentの更新によって変更内容が上書きされる可能性があるため、レポート、クエリ、パラメーターのコピーを作成し、各自のバージョンを更新として変更してください)。	なし
SecurityDash BoardRpt	このカスタムレポートには、ソースアドレス、カテゴリの動作、宛先アドレス、イベントIDを示す表が表示されます。	なし
SecurityDB Report	このカスタムSecurity Dashboardレポートには、2つのグラフと表が表示されます。最初のグラフには、イベント数がソースアドレスごとに表示されます。2番目のグラフには、イベント数が宛先アドレスごとに表示されます。表には、ソースと宛先ごとのイベント数が表示されます。	なし
Top IDS Attack Events	このレポートには、IDSシステムからの上位イベントに加えて、IDSイベント名、IDSの種類、カテゴリの重要性がCompromiseまたはHostileの各IDSイベント数が表示されます。	なし
Top IDS Events	このレポートには、IDSシステムからの上位イベントに加えて、IDSイベント名、IDSの種類、各IDSイベント数が表示されます。	なし
Top Machines Traversing Firewall	このレポートには、ファイアウォールから報告されたイベントのソースゾーン、アドレスとホスト名、イベント数が表示されます。	なし

Intrusion Monitoring (続き)

レポート	説明	ドリルダウン
Top Web Traffic	このレポートには、宛先ポートがwebPortsパラメーターに列挙されているイベントの時間、ソースゾーン、アドレスとホスト名、Webポートとイベント数を示す表が表示されます。	なし
Windows Events	このレポートには、Microsoftオペレーティングシステムによって報告される各種イベントのデバイスゾーン、アドレスとホスト名、デバイスイベントID、ソースのユーザーID、ユーザー名、NTドメイン、宛先のユーザーID、ユーザー名、NTドメイン、動作、結果、イベントタイプ、イベント数を示す表が表示されます。	なし
Worm Infected Systems	このレポートには、ワームによる感染の兆候を示すシステムのゾーン名、ホスト名、アドレスを示す表が表示されます。	なし

Intrusion Monitoringカテゴリの下には以下のカテゴリがあります。

Attackers

これはIntrusion Monitoringカテゴリのサブカテゴリであり、ソースまたは攻撃者情報に基づくイベントを対象としています。

Attackersカテゴリは、以下のパスの下にあります。

```
Foundation\Intrusion Monitoring\Attackers
```

Attackersカテゴリのレポートを以下の表に示します。パラメーターはありません。

Attackers

レポート	説明	ドリルダウン
Bottom Sources	このレポートには、ソースゾーン名、ソースアドレス、イベント数が、ベースイベント数の合計の昇順に表示されます。Count列のハイパーリンクをクリックすると、Bottom Targetsレポートが表示されます。このレポートは、Least Common EventsレポートのCount列のターゲットです。	Countフィールドは、「Bottom Targets」レポートにドリルダウンします。
Source Counts by Destination	このレポートには、特定の宛先ゾーンとアドレスのイベントのうち、カテゴリの重大度がCompromiseまたはHostileのものについて、宛先ゾーンとアドレス、ソースゾーン、イベント数を示す表が表示されます。	Destination Zoneフィールドは、「Source Counts by Destination」レポートにドリルダウンします。 Destination Addressフィールドは、「Source Counts by Destination」レポートにドリルダウンします。 Source Countフィールドは、「Attack Events by Destination」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Source Counts by Destination Port	このレポートには、各ポートの宛先ポート、ソースゾーンとアドレス、イベント数を示す表が表示されます。	なし
Source Counts by Device	このレポートには、カテゴリの重大度がCompromiseまたはHostileの各イベントの、デバイスゾーンとアドレス、ソースゾーンとアドレス、イベント数を示す表が表示されます。	なし
Source Counts by Device Severity	このレポートには、緊急度、ソースゾーンとアドレス、その緊急度のイベントの数を示す表が表示されます。	なし
Source Counts by Source Port	このレポートには、カテゴリの重大度がCompromiseまたはHostileの各イベントの、ソースポート、ソースゾーンとアドレス、イベント数を示す表が表示されます。	なし
Source Port Counts	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、ソースポート、イベント名、イベント数を示す表が表示されます。	なし
Top 10 Talkers	このレポートには、イベントの生成数が上位10台のシステムについて、ソースゾーンとアドレス、そのシステムからのイベント数の表が表示されます。	なし

Attackers (続き)

レポート	説明	ドリルダウン
Top Attacker Detail	このレポートには、指定したソースゾーンとアドレスのイベントのうち、カテゴリの重大度がCompromiseまたはHostileのものについて、緊急度、攻撃者のゾーンとアドレス、イベント数を示す表が表示されます。	なし
Top Attacker Details	このレポートには、カテゴリの重大度がCompromiseまたはHostileのものについて、緊急度、攻撃者のゾーン、攻撃者のアドレス、ターゲットゾーン、ターゲットアドレス、イベント数が、イベント数の降順に表示されます。このレポートは、Top Attackersレポートの Attacker Address列のターゲットです。	なし
Top Attacker Ports	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、攻撃者ポート、トランスポートプロトコル、イベント数を示す表が表示されます。	なし
Top Attackers	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、攻撃者のゾーン名、攻撃者のアドレス、イベント数が、ベースイベント数の合計の降順に表示されます。このレポートには、選択したフィールドに基づいて詳細情報を表示するレポートを実行するハイパーリンクがあります。Attacker Zone列は、Top Attack Sourcesレポートを実行します。Attacker Address列は、Top Attacker Detailsレポートを実行します。Count列は、Top Targetsレポートを実行します。	`Attacker Address`フィールドは、「Top Attacker Details」レポートにドリルダウンします。 `Count`フィールドは、「Top Targets」レポートにドリルダウンします。
Top Attack Sources	このレポートには、カテゴリの重大度がCompromiseまたはHostileのものについて、攻撃者のゾーンとイベント数が、イベント数の降順に表示されます。このレポートのAttacker Zone列はハイパーリンクになっており、Top Attackersレポートを実行します。	`Attacker Zone`フィールドは、「Top Attackers」レポートにドリルダウンします。
Top Sources Detected by Snort	このレポートには、Snortによって検出されたイベントのソースゾーン、アドレスとホスト名、イベント数を示す表が表示されます。	なし
Top Sources Traversing Firewalls	このレポートには、ファイアウォールデバイスによって報告されたイベントのソースゾーン、アドレスとホスト名、イベント数の表が表示されます。	なし

Resource Access

これは、Intrusion Monitoringカテゴリのサブカテゴリであり、保護されたリソースを対象としています。

Resource Accessカテゴリは、以下のパスの下にあります。

```
Foundation\Intrusion Monitoring\Resource Access
```

Resource Accessカテゴリのレポートを以下の表に示します。パラメーターはありません。

Resource Access

レポート	説明	ドリルダウン
Access Events by Resource	このレポートには、選択した期間中に発生したイベントのリソースタイプ、ゾーンとアドレス、アクセスイベント、結果と回数を示す表が表示されます。リソースタイプをクリックすると、Access Events by Resource Drilldownレポートが実行され、選択したリソースタイプのイベントが表示されます。	Resource Typeフィールドは「Access Events by Resource」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Least Common Accessed Ports	このレポートには、トランスポートプロトコルがTCPまたはUDPのポートの、宛先ポート、トランスポートプロトコル、イベント数を示す表が表示されます。	なし
Resource Access by Users - Failures	このレポートには、特定のリソースへのアクセス試行の失敗について、リソースタイプ、ユーザーIDと名前、宛先ゾーンとアドレス、アクセスイベントと回数を示す表が表示されます。Resource Type列のエントリをクリックすると、Resource Access by Users - Failures Drilldownレポートが開き、そのリソースタイプのすべての関連イベントが表示されます。	Resource Typeフィールドは「Resource Access by Users - Failures」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Resource Access by Users - Successes-Attempts	このレポートには、該当するイベントのリソースタイプ、結果、宛先ユーザーIDと名前、宛先ゾーンとアドレス、アクセスイベント名と回数を示す表が表示されます。Resource Type列はハイパーリンクになっており、リソースタイプをクリックするとResource Access by Users - Successes-Attempts Drilldownレポートが実行され、選択したリソースタイプのイベントのみが表示されます。	Resource Typeフィールドは「Resource Access by Users - Successes-Attempts」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Top Machines Accessing the Web	このレポートには、宛先ポートがwebPortsパラメーターに列挙されているイベントのソースゾーン、アドレスとホスト名、宛先ポートとイベント数を示す表が表示されます。	なし

Targets

これはIntrusion Monitoringカテゴリのサブカテゴリであり、宛先またはターゲット情報に基づくイベントを対象としています。

Targetsカテゴリは、以下のパスの下にあります。

```
Foundation\Intrusion Monitoring\Targets
```

Targetsカテゴリのレポートを以下の表に示します。パラメーターはありません。

Targets

レポート	説明	ドリルダウン
Attack Events by Destination	このレポートには、特定の宛先ゾーンとアドレスのイベントのうち、カテゴリの重大度がCompromiseまたはHostileのものについて、宛先ゾーンとアドレス、ソースゾーンとアドレス、イベント名、イベント数を示す表が表示されます。	`Destination Zone`フィールドは、「Attack Events by Destination」レポートにドリルダウンします。 `Destination Address`フィールドは、「Attack Events by Destination」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。
Bottom Destinations	このレポートには、宛先ゾーン名、宛先アドレス、イベント数が、ベースイベント数の合計の昇順に表示されます。このレポートは、Common EventsレポートのEvent Name列のターゲットです。	なし
Bottom Targets	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、ターゲットのゾーン名、ターゲットのアドレス、イベント数が、ベースイベント数の合計の昇順に表示されます。このレポートは、Bottom SourcesレポートのCount列のターゲットです。	なし
Destination Counts by Device Severity	このレポートには、緊急度、ターゲットゾーンとアドレス、各緊急度のイベントの数を示す表が表示されます。	なし
Destination Counts by Event Name	このレポートには、各宛先のイベント名、ターゲットゾーンとアドレス、イベント数を示す表が表示されます。	なし
Target Attack Counts by Severity	このレポートには、カテゴリの重大度がCompromise、Hostile、またはSuspiciousのイベントの、緊急度、ターゲットゾーン、イベント数を示す表が表示されます。	なし
Target Counts by Event Name	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、イベント名、ターゲットゾーンとアドレス、イベント数を示す表が表示されます。	なし
Target Counts by Severity	このレポートには、カテゴリの重大度がCompromise、Hostile、またはSuspiciousのイベントの、緊急度、ターゲットゾーンとアドレス、イベント数を示す表が表示されます。	なし
Target Counts by Source	このレポートには、カテゴリの重大度がCompromise、Hostile、またはSuspiciousのイベントの、ソースゾーンとアドレス、ターゲットゾーンとアドレス、イベント数を示す表が表示されます。	なし

Targets (続き)

レポート	説明	ドリルダウン
Target Counts by Source Port	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、ソースポート、そのポートのイベント数、宛先ゾーンとアドレスを示す表が表示されます。	なし
Target Counts by Target Port	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、宛先ポート、各ポートのイベント数、ターゲットゾーンとアドレスを示す表が表示されます。	なし
Target Port Counts	このレポートには、カテゴリの重大度がCompromiseまたはHostileのイベントの、ターゲットポート、そのポートのイベント数、ターゲットゾーンとアドレスを示す表が表示されます。	なし
Top Destination Ports	このレポートには、上位宛先ポートと各ポートのイベント数を示す表が表示されます。	なし
Top Destinations Across Firewalls	このレポートには、ファイアウォールデバイスによって報告されたイベントの宛先ゾーン、アドレスとホスト名、イベント数の表が表示されます。	なし
Top Destinations in IDS Events	このレポートには、IDSから送信されたすべてのイベントについて、宛先ゾーン、アドレスとホスト名、各ホスト宛のイベント数を示す表が表示されます。	なし
Top Targets	このレポートには、カテゴリの重大度がCompromiseまたはHostileのものについて、ターゲットゾーン、ターゲットアドレス、イベント数が、イベント数の降順に表示されます。このレポートは、Top AttackersレポートのCount列のターゲットです。	なし

User Tracking

これはIntrusion Monitoringカテゴリのサブカテゴリであり、ユーザー情報に基づくイベントを対象としています。

User Trackingカテゴリは、以下のパスの下にあります。

```
Foundation\Intrusion Monitoring\User Tracking
```

User Trackingカテゴリのレポートを以下の表に示します。パラメーターはありません。

User Tracking

レポート	説明	ドリルダウン
Common Account Login Failures by Source	このレポートには、リソースタイプ、アタッカーアドレス、アタッカーのアセット名、アタッカーNTドメイン、アタッカーのユーザーID、アタッカーのユーザー名、アタッカーゾーン名、アグリゲートされたイベント数の合計が表で示されます。	なし
Number of Failed Logins	このレポートには、レポート期間内で失敗したログインの時間ごとの数が表で示されます。	なし
Top User Logins	このレポートには、NTドメイン、ユーザーIDおよび名前、成功したログイン数が表で示されます。	なし
Top Users with Failed Logins	このレポートには、ユーザーIDおよび名前、時間 (分単位)、失敗したログイン試行数が表で示されます。	なし
User Activity	このレポートには、イベントのソースユーザーIDおよびユーザー名、通知先ユーザーIDおよびユーザー名、イベントの時刻、イベント名および結果 (成功、試行、失敗) が表で示されます。	なし

NetFlow Monitoring

これは、Foundationカテゴリのサブカテゴリであり、NetFlowデータを対象としています。

NetFlow Monitoringカテゴリは、以下のパスの下にあります。

```
Foundation\NetFlow Monitoring
```

NetFlow Monitoringカテゴリのレポートを以下の表に示します。

NetFlow Monitoring

レポート	説明	ドリルダウン
Daily Bandwidth Usage	このレポートには、日ごとの帯域幅使用量を示すグラフと表が表示されます。	なし
Hourly Bandwidth Usage	このレポートには、時間ごとの帯域幅使用量を示すグラフと表が表示されます。	なし
Top Bandwidth Usage by Destination	このレポートには、宛先アドレスごとの帯域幅使用量を示すグラフと表が表示されます。	なし
Top Bandwidth Usage by Destination Port	このレポートには、宛先ポートごとの帯域幅使用量を示すグラフと表が表示されます。	なし
Top Bandwidth Usage by Source	このレポートには、ソースアドレスごとの帯域幅使用量を示すグラフと表が表示されます。	なし

Network Monitoring

これは、Foundationカテゴリのサブカテゴリであり、ネットワーク帯域幅とステータスイベントを対象としています。

Network Monitoringカテゴリは、以下のパスの下にあります。

```
Foundation\Network Monitoring
```

Network Monitoringカテゴリのレポートを以下の表に示します。パラメーターはありません。

Network Monitoring

レポート	説明	ドリルダウン
Top VPN Accesses by User	このレポートには、VPNアクセス、認可、認証イベントのソースユーザーIDと名前、イベント数を示す表が表示されます。	なし
Top VPN Event Destinations	このレポートには、VPNデバイスから報告された、変更イベントを除くイベントのVPN宛先ゾーン、アドレスとホスト名、そのホストのイベント数を示す表が表示されます。	なし
Top VPN Events	このレポートには、VPNデバイスから報告された、変更イベントを除くイベントのVPNイベント名、ソースゾーンとアドレス、宛先ゾーンとアドレス、イベント数を示す表が表示されます。	なし
Top VPN Event Sources	このレポートには、VPNデバイスから報告された、変更イベントを除くイベントのVPNソースゾーン、アドレスとホスト名、そのソースのイベント数を示す表が表示されます。	なし
Traffic Statistics	このレポートには、2つのグラフと表が表示されます。最初のグラフは、時間ごとの入出力バイト数を示します。2番目のグラフは、デバイスごとの入出力バイト数を示します。表は、時間、ファイアウォールゾーンとアドレス、トランスポートプロトコル、入出力バイト数を示します。	なし
VPN Connection Attempts	このレポートには、失敗しなかったVPNアクセス、認可、認証イベントについて、ソースホスト名、ソースユーザー名、宛先のゾーン、アドレス、ホスト名、宛先ユーザーIDとユーザー名、イベント数を示す表が表示されます。	なし
VPN Connection Failures	このレポートには、VPNデバイスからアクセス、認可、認証失敗が報告されたイベントについて、VPNデバイスゾーン、アドレスとホスト名、VPNイベント、ソースユーザーID、ホスト名とユーザー名、宛先ゾーン、アドレス、ホスト名、ユーザー名、各イベントの数を示す表が表示されます。	なし

Logger Administration

このカテゴリは、Loggerの管理タスクを対象としています。Logger Administrationカテゴリのレポートを以下の表に示します。

Logger Administration

レポート	説明	ドリルダウン	パラメーター
Daily Byte Count	このレポートには、コネクターから受信したイベントの日次バイト数が表示されます。	なし	なし

SANS Top 5

このカテゴリは、SANS Top 5 Essential Log Reports (http://www.sans.org/security-resources/top5-logreports.pdf) を対象としています。それぞれのサブカテゴリは、5つの領域のいずれかを対象としています。

SANS Top 5カテゴリの下には以下のカテゴリがあります。

1 - Attempts to Gain Access through Existing Accounts

これは、SANS Top 5 Essential Log Reportsのサブカテゴリです。このカテゴリは、既存のアカウントを通じたアクセスの試みを対象としています。

1 - Attempts to Gain Access through Existing Accountsカテゴリは、以下のパスの下にあります。

```
SANS Top 5\1 - Attempts to Gain Access through Existing Accounts
```

1 - Attempts to Gain Access through Existing Accountsカテゴリのレポートを以下の表に示します。

1 - Attempts to Gain Access through Existing Accounts

レポート	説明	ドリルダウン	パラメーター
Number of Failed Logins	このレポートは、SANS Top 5 Essential Log Reportsのセクション「1 - Attempts to Gain Access Through Existing Accounts」に基づいており、レポート期間内で失敗したログインの時間ごとの数が表で示されます。	なし	なし
Top Users with Failed Logins	このレポートは、SANS Top 5 Essential Log Reportsのセクション「1 - Attempts to Gain Access Through Existing Accounts」に基づいており、その時間 (分) の間のシステムへのログインの試みについて、ユーザーIDと名前、時間と回数を示す表が表示されます。	なし	なし

2 - Failed File or Resource Access Attempts

これは、SANS Top 5 Essential Log Reportsのサブカテゴリです。このカテゴリは、失敗したファイルまたはリソースアクセスの試みを対象としています。

2 - Failed File or Resource Access Attemptsカテゴリは、以下のパスの下にあります。

```
SANS Top 5\2 - Failed File or Resource Access Attempts
```

2 - Failed File or Resource Access Attemptsカテゴリのレポートを以下の表に示します。

2 - Failed File or Resource Access Attempts

レポート	説明	ドリルダウン	パラメーター
Failed Resource Access by Users	このレポートは、SANS Top 5 Essential Log Reportsのセクション「2 - Failed File or Resource Access Attempts」に基づいており、特定のリソースへのアクセス試行について、リソースタイプ、ユーザーIDと名前、宛先ゾーンとアドレス、アクセスイベントと回数を示す表が表示されます。Resource Type列のエントリをクリックすると、SANS Top 5 -2- Failed Resource Access by Users Drilldownレポートが開き、そのリソースタイプのすべての関連イベントが表示されます。	`Resource Type`フィールドは「Failed Resource Access by Users」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Failed Resource Access Events	このレポートは、SANS Top 5 Essential Log Reportsのセクション「2 - Failed File or Resource Access Attempts」に基づいており、特定のリソースへのアクセス試行について、リソースタイプ、ユーザーIDと名前、宛先ゾーンとアドレス、アクセスイベントと回数を示す表が表示されます。Resource Type列のエントリをクリックすると、SANS Top 5 -2- Failed Resource Access Events Drilldownレポートが開き、そのリソースタイプのすべての関連イベントが表示されます。	`Resource Type`フィールドは「Failed Resource Access Events」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

3 - Unauthorized Changes to Users Groups and Services

これは、SANS Top 5 Essential Log Reportsのサブカテゴリです。このカテゴリは、ユーザー、グループ、およびサービスの許可されない変更を対象にしています。

3 - Unauthorized Changes to Users Groups and Servicesカテゴリは、以下のパスの下にあります。

```
SANS Top 5\3 - Unauthorized Changes to Users Groups and Services
```

3 - Unauthorized Changes to Users Groups and Servicesカテゴリのレポートを以下の表に示します。

3 - Unauthorized Changes to Users Groups and Services

レポート	説明	ドリルダウン	パラメーター
Account Modifications	このカスタムレポートは、SANS Top 5 Essential Log Reportsのセクション「3 - Unauthorized Changes to Users, Groups and Services」に基づいており、グラフと表を表示します。グラフは、上位のユーザーアカウント変更を示します。表は、ソースユーザー名、ソースゾーンとアドレス、宛先ユーザー名、宛先ゾーンとアドレス、変更イベント、変更日を示します。	なし	なし
Password Changes	このレポートは、SANS Top 5 Essential Log Reportsのセクション「3 - Unauthorized Changes to Users, Groups and Services」に基づいており、パスワード変更イベントのユーザー名、ソースゾーンとアドレス、宛先ゾーンとアドレス、日付を示す表が表示されます。	なし	なし
User Account Creations	このレポートは、SANS Top 5 Essential Log Reportsのセクション「3 - Unauthorized Changes to Users, Groups and Services」に基づいており、アカウント作成のソースユーザー名、ソースゾーンとアドレス、宛先ユーザー名、宛先ゾーンとアドレス、変更イベント名と日付を示す表が表示されます。	なし	なし
User Account Deletions	このレポートは、SANS Top 5 Essential Log Reportsのセクション「3 - Unauthorized Changes to Users, Groups and Services」に基づいており、ユーザーアカウントが削除されたときのソースユーザー名、ソースゾーンとアドレス、宛先ユーザー名、宛先ゾーンとアドレス、時刻を示す表が表示されます。	なし	なし
User Account Modifications	このレポートは、SANS Top 5 Essential Log Reportsのセクション「3 - Unauthorized Changes to Users, Groups and Services」に基づいており、アカウント変更のソースユーザー名、ソースゾーンとアドレス、宛先ユーザー名、宛先ゾーンとアドレス、変更イベント名と日付を示す表が表示されます。	なし	なし

4 - Systems Most Vulnerable to Attack

これは、SANS Top 5 Essential Log Reportsのサブカテゴリです。このカテゴリは、攻撃に最も脆弱なシステムを対象としています。

4 - Systems Most Vulnerable to Attackカテゴリは、以下のパスの下にあります。

```
SANS Top 5\4 - Systems  Most Vulnerable to Attack
```

4 - Systems Most Vulnerable to Attackカテゴリのレポートを以下の表に示します。

4 - Systems Most Vulnerable to Attack

レポート	説明	ドリルダウン	パラメーター
Vulnerability Scanner Logs by Host	このレポートは、SANS Top 5 Essential Log Reportsのセクション「4 - Systems Most Vulnerable to Attack」に基づいており、システムのゾーンとアドレス、脆弱性IDと名前、そのシステムに対してその脆弱性が報告された回数を示す表が表示されます。	`arc_destinationAddress` フィールドは、「Vulnerability Scanner Logs by Host」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし
Vulnerability Scanner Logs by Vulnerability	このレポートは、SANS Top 5 Essential Log Reportsのセクション「4 - Systems Most Vulnerable to Attack」に基づいており、脆弱性IDと名前、ゾーンとアドレス、そのシステムに対してその脆弱性が報告された回数を示す表が表示されます。	`arc_destinationAddress` フィールドは、「Vulnerability Scanner Logs by Host」レポートにドリルダウンします。 このレポートは自身にドリルダウンします。	なし

5 - Suspicious or Unauthorized Network Traffic Patterns

これは、SANS Top 5 Essential Log Reportsのサブカテゴリです。このカテゴリは、疑わしいネットワークトラフィックパターンや許可されていないネットワークトラフィックパターンを対象にしています。

5 - Suspicious or Unauthorized Network Traffic Patternsカテゴリは、以下のパスの下にあります。

```
SANS Top 5\5 - Suspicious or Unauthorized Network Traffic Patterns
```

5 - Suspicious or Unauthorized Network Traffic Patternsカテゴリのレポートを以下の表に示します。

5 - Suspicious or Unauthorized Network Traffic Patterns

レポート	説明	ドリルダウン	パラメーター
Alerts from IDS	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、デバイスのベンダーと製品、デバイスイベントID、IDSシグニチャ名、そのシグニチャが報告された回数を示す表が表示されます。	なし	なし
IDS Signature Destinations	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、宛先ゾーンとアドレス、デバイスのベンダーと製品、IDSによってそのアドレスに対し報告されたイベントの数を示す表が表示されます。	なし	なし
IDS Signature Sources	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、宛先ゾーンとアドレス、デバイスのベンダーと製品、各イベントの数を示す表が表示されます。	なし	なし
Top 10 Talkers	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、ソースゾーンとアドレス、各アドレスから受信したイベント数を示す表が表示されます。	なし	なし
Top 10 Types of Traffic	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、アプリケーションプロトコル、ポート番号、トランスポートプロトコルの少なくともいずれかがわかり、入力または出力のバイト数がわかる場合に、トラフィックの詳細を示します。これらの条件を満たす各イベントは、何らかの種類のパケットを表すものと想定して、ベースイベントの数に基づく数が表示されます。	なし	なし

5 - Suspicious or Unauthorized Network Traffic Patterns (続き)

レポート	説明	ドリルダウン	パラメーター
Top Alerts from IDS	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、グラフと表が表示されます。グラフは、IDSからの上位10個のアラートを示します。表は、シグニチャID、シグニチャ名、デバイスベンダー、そのシグニチャが報告された回数を示します。	なし	なし
Top Destination IPs	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、ターゲットゾーンとアドレス、宛先アドレスごとのイベント数を示す表が表示されます。	なし	なし
Top IDS Signature Destinations	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、グラフと表が表示されます。グラフは、アドレスごとの上位シグニチャ宛先を示します。表は、宛先ゾーンとアドレス、デバイスベンダーと製品、そのホストへのイベント数を示します。	なし	なし
Top IDS Signature Sources	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、グラフと表が表示されます。グラフは、アドレスごとの上位シグニチャソースを示します。表は、ソースゾーンとアドレス、デバイスベンダーと製品、そのホストによるイベント数を示します。	なし	なし
Top Target IPs	このレポートは、SANS Top 5 Essential Log Reportsのセクション「5 - Suspicious or Unauthorized Network Traffic Patterns」に基づいており、カテゴリの重大度がCompromiseまたはHostileのイベントの、ターゲットゾーンとアドレス、そのアドレスに対して報告されたIDSイベントの数を示す表が表示されます。	なし	なし

パラメーター

一部のレポートは、レポートの実行中にフィールド値の入力を求めるクエリを実行します。これらのフィールドに入力された値は、パラメーターを使用してクエリに渡されます。クエリに渡すパラメーターの値を変更するには、実行時にレポートによって入力を求められたときに新しい値を入力するか、パラメーターのデフォルト値を変更することができます。パラメーターの値では、SQLのワイルドカードがサポートされています。たとえば、ワイルドカード文字%は1つ以上の文字に一致します。パラメーターの詳細については、「パラメーター」(292ページ)を参照してください。

Loggerレポートは、以下のパラメーターを使用するクエリを実行します。

IPAddress

レポートが、`IPAddress`パラメーターを入力として期待するクエリを実行するとき、レポートの実行時にIP Addressプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、`192.168.35.5`などのIPアドレスを受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Attackers \\ Top Attacker Detailsを参照してください。

categoryObjectParameter

レポートが、categoryObjectParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にResource Typeプロンプトがデフォルト値'/Host/Application/Database','/Host/Application/Database/Data','/Host/Application/Service/Email','/Host/Resource/File'で表示されます。

これは複数値の文字型 (CHAR) パラメーターであり、Host/Application/Databaseのように1つ以上のカテゴリオブジェクトURIの選択を可能にします。

このパラメーターは、INキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Resource Access \\ Access Events by Resourceを参照してください。

commonlyBlockedPorts

レポートが、commonlyBlockedPortsパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にBlocked Portsプロンプトが表示され、すべてのデフォルト値が [Combo Source] パネルに表示されます。

これは複数値の数値型 (NUMBER) パラメーターであり、135,139のように1つ以上のポート番号のリストの選択を可能にします。

このパラメーターは、INキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Probes on Blocked Portsを参照してください。

destinationAddress

レポートが、destinationAddressパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDestination IP Addressプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、192.168.35.5などのIPアドレスを受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Attackers \\ Source Counts by Destinationを参照してください。

destinationPort

レポートが、destinationPortパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDestination Portプロンプトがデフォルト値80で表示されます。

これは単一値の数値型 (NUMBER) パラメーターであり、80のように1つのポート番号の入力を可能にします。

deviceGroupParameter

レポートが、deviceGroupParameterパラメーターを入力として期待するクエリを実行するとき、Category Device Groupプロンプトがレポートの実行時にデフォルト値 '/Firewall','/IDS','/IDS/Host','/IDS/Host/Antivirus','/IDS/Host/File Integrity','/IDS/Network','/IDS/Network/Traffic Analysis','/Network Equipment','/Network Equipment/Router','/Network Equipment/Switches','/VPN'で表示されます。

これは複数値の文字型 (CHAR) パラメーターであり、Host/Application/Databaseのように1つ以上のカテゴリオブジェクトURIの選択を可能にします。

このパラメーターは、INキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Configuration Monitoring \\ Device Configuration Changesを参照してください。

deviceProduct

レポートが、deviceProductパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Productプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Snortなどの文字列を受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Configuration Monitoring \\ Vulnerability Scanner Logs by Hostを参照してください。

deviceSeverityParameter

レポートが、deviceSeverityParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Severityプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Highなどの文字列を受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion

Monitoring \\ Attackers \\ Source Counts by Device Severityを参照してください。

deviceVendor

レポートが、deviceVendorパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Vendorプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Snortなどの文字列を受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Configuration Monitoring \\ Vulnerability Scanner Logs by Hostを参照してください。

dmBandwidthParameter

レポートが、dmBandwidthParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Typeプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Firewallのように定義済みの値の選択を可能にします。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Configuration Monitoring \\ Vulnerability Scanner Logs by Hostを参照してください。

dmConfigurationParameter

レポートが、dmConfigurationParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Typeプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Firewallのように定義済みの値の選択を可能にします。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。

dmLoginParameter

レポートが、dmLoginParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にDevice Typeプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Firewallのように定義済みの値の選択を可能にします。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトDevice Monitoring \\

CrossDevice \\ Failed Login Attemptsを参照してください。

eventNameParameter

レポートが、eventNameParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にEvent Nameプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、Connector Raw Event Statisticsなどの文字列を受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Targets \\ Destination Counts by Event Nameを参照してください。

resourceTypeParameter

レポートが、resourceTypeParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にResource Typeプロンプトがデフォルト値/Host/Application/Databaseで表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、/Host/Application/Databaseなどの文字列を受け取ります。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。

webPorts

レポートが、webPortsパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にWeb Portsプロンプトが表示され、すべてのデフォルト値が [Combo Source] パネルに表示されます。

これは複数値の数値型 (NUMBER) パラメーターであり、80,443のように1つ以上のポート番号のリストの選択を可能にします。

このパラメーターは、INキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Top Web Trafficを参照してください。

zoneParameter

レポートが、zoneParameterパラメーターを入力として期待するクエリを実行するとき、レポートの実行時にZoneプロンプトがデフォルト値%で表示されます。

これは単一値の文字型 (CHAR) パラメーターであり、`/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255`のように1つ以上のカテゴリオブジェクトURIの選択を可能にします。

このパラメーターは、LIKEキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Attackers \\ Top Attacker Detailsを参照してください。

zones

レポートが、`zones`パラメーターを入力として期待するクエリを実行するとき、レポートの実行時にZoneプロンプトがデフォルト値`%`で表示されます。

これは複数値の文字型 (CHAR) パラメーターであり、`/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255,/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255`のように1つ以上のカテゴリオブジェクトURIの選択を可能にします。

このパラメーターは、INキーワードとともに、SQLクエリのWHERE句で使用されます。このパラメーターを使用するクエリの例については、クエリオブジェクトFoundation \\ Intrusion Monitoring \\ Attackers \\ Source Counts by Destinationを参照してください。

システムフィルター

Loggerには、以下の表に示すシステムフィルターが用意されています。

フィルター

フィルター	種類	説明
設定 - 設定変更 (統合)	統合クエリ	このフィルターは、設定変更イベントとして分類されるイベントを探します。
設定 - システム設定変更 (CEF形式)	正規表現	このフィルターは、設定変更イベントとして分類されるイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
イベント - CEF	正規表現	このフィルターは、すべてのCEF形式のイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
イベント - 通知先単位のイベント数	統合クエリ	このフィルターは、宛先アドレスがあるすべてのCEFイベントを探しグラフを表示します。
イベント - ソース単位のイベント数	統合クエリ	このフィルターは、ソースアドレスがあるすべてのCEFイベントを探しグラフを表示します。

フィルター(続き)

フィルター	種類	説明
イベント - 高緊急度および最高緊急度CEFイベント	正規表現	このフィルターは、緊急度が高いか非常に高いCEFイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
イベント - 高緊急度および最高緊急度イベント(統合)	統合クエリ	このフィルターは、緊急度が高いか非常に高いCEFイベントを探します。
ファイアウォール - 拒否	統合クエリ	このフィルターは、denyまたはshunのイベントを探します。
ファイアウォール - ドロップ	統合クエリ	このフィルターは、データベースに関連しないドロップイベントを探します。
ファイアウォール - 許可	統合クエリ	このフィルターは、permitという単語が含まれるイベントを探します。
侵入 - 悪意のあるコード(CEF形式)	正規表現	このフィルターは、悪意のあるコードを示すものとして分類されるCEFイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
侵入 - 悪意のあるコード(統合)	統合クエリ	このフィルターは、悪意のあるコードを示すものとして分類されるCEFイベントを探します。
ログイン - すべてのログイン(CEF形式)	正規表現	このフィルターは、認証イベントに分類されるCEFイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
ログイン- すべてのログイン(非CEF形式)	正規表現	このフィルターは、認証イベントであることを示す単語を含む、非CEF形式のイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
ログイン - すべてのログインに成功 (統合)	統合クエリ	このフィルターは、認証イベントに分類されるCEFイベントを探します。
ログイン - ログインの失敗	統合クエリ	このフィルターは、ログイン、ユーザー認証、ユーザー認可に関する失敗イベントを探します。
ログイン- ログインに成功(非CEF形式)	正規表現	このフィルターは、成功したログインを示すキーワードを含むイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
ログイン - ログイン成功(CEF形式)	正規表現	このフィルターは、成功したログインイベントに分類されるCEFイベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
ログイン - ログインに成功(統合)	統合クエリ	このフィルターは、成功したログインイベントに分類されるCEFイベントを探します。
ログイン - ログインに失敗(非CEF形式)	正規表現	このフィルターは、ログイン、ユーザー認証、ユーザー認可に関する失敗イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。

フィルター(続き)

フィルター	種類	説明
ログイン - ログインに失敗 (CEF形式)	正規表現	このフィルターは、ログイン、ユーザー認証、ユーザー認可に関する失敗イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
ログイン - ログインに失敗 (統合)	統合クエリ	このフィルターは、ログインイベントに分類される失敗イベントを探します。
ネットワーク- DHCPリースイベント	統合クエリ	このフィルターは、DHCPリース関連のイベントを探します。
ネットワーク - ポートリンクのアップダウン	統合クエリ	このフィルターは、ポートまたはリンクステータスメッセージを探します。
ネットワーク - プロトコルリンクアップダウン	統合クエリ	このフィルターは、プロトコルステータスメッセージを探します。
システムアラート - CPU使用率が90%を超過 (CEF形式)	正規表現	このフィルターは、CPU使用率が90%を超えていることを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - CPU使用率が90%を超過 (統合)	統合クエリ	このフィルターは、CPU使用率が90%を超えていることを示す内部イベントを探します。
システムアラート - CPU使用率が95%を超過 (CEF形式)	正規表現	このフィルターは、CPU使用率が95%を超えていることを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - CPU使用率が95%を超過 (統合)	統合クエリ	このフィルターは、CPU使用率が95%を超えていることを示す内部イベントを探します。
システムアラート - デバイス設定変更 (CEF形式)	正規表現	このフィルターは、Loggerの設定変更を示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - デバイス設定変更 (統合)	統合クエリ	このフィルターは、Loggerの設定変更を示す内部イベントを探します。
システムアラート - フィルタ設定変更 (CEF形式)	正規表現	このフィルターは、Loggerフィルターの変更を示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - フィルタ設定変更 (統合)	統合クエリ	このフィルターは、Loggerフィルターの変更を示す内部イベントを探します。
システムアラート- CPUが過熱 (CEF形式)	正規表現	このフィルターは、CPUの過熱の可能性を示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - CPUが過熱 (統合)	統合クエリ	このフィルターは、CPUの過熱の可能性を示す内部イベントを探します。

フィルター(続き)

フィルター	種類	説明
SystemAlert - Bad Fan (CEF format)	正規表現	このフィルターは、ファン障害に関連するLoggerアプライアンスの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - 電源装置障害 (CEF形式)	正規表現	このフィルターは、電源が障害になったことを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - 電源装置障害 (統合)	統合クエリ	このフィルターは、電源が障害になったことを示す内部イベントを探します。
システムアラート - RAIDステータスバッテリ障害 (CEF形式)	正規表現	このフィルターは、RAID BBU (バッテリバックアップユニット) が障害になったことを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - RAIDステータスバッテリ障害 (統合)	統合クエリ	このフィルターは、RAID BBU (バッテリバックアップユニット) が障害になったことを示す内部イベントを探します。
SystemAlert - Disk Failure (CEF format)	正規表現	このフィルターは、ディスク障害を示すLoggerアプライアンスの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
SystemAlert - Disk Failure (Unified)	統合クエリ	このフィルターは、ディスク障害を示すLoggerアプライアンスの内部イベントを探します。
SystemAlert - RAID Controller Issue (CEF format)	正規表現	このフィルターは、RAIDディスクが障害になったことを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
SystemAlert - RAID Controller Issue (Unified)	統合クエリ	このフィルターは、RAIDディスクが障害になったことを示す内部イベントを探します。
SystemAlert - Root Partition Free Space Below 5% (Unified)	統合クエリ	このフィルターは、ルートディスクの空き領域が5%を下回ったことを示す内部イベントを探します。
SystemAlert - Root Partition Free Space Below 10% (Unified)	統合クエリ	このフィルターは、ルートディスクの空き領域が10%を下回ったことを示す内部イベントを探します。
SystemAlert - Root Partition Free Space Below 10% (CEF format)	正規表現	このフィルターは、ルートディスクの空き領域が10%を下回ったことを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
SystemAlert - Root Partition Free Space Below 5% (CEF format)	正規表現	このフィルターは、ルートディスクの空き領域が5%を下回ったことを示す内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。

フィルター(続き)

フィルター	種類	説明
システムアラート - ストレージ設定変更 (CEF形式)	正規表現	このフィルターは、ストレージ設定の変更に関連するLoggerの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - ストレージ設定変更 (統合)	統合クエリ	このフィルターは、ストレージ設定の変更に関連するLoggerの内部イベントを探します。
システムアラート - ストレージグループの使用率が90%を超過 (CEF形式)	正規表現	このフィルターは、ストレージグループの使用率が90%を超えていることを示すLoggerの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - ストレージグループの使用率が90%を超過 (統合)	統合クエリ	このフィルターは、ストレージグループの使用率が90%を超えていることを示すLoggerの内部イベントを探します。
システムアラート - ストレージグループの使用率が95%を超過 (CEF形式)	正規表現	このフィルターは、ストレージグループの使用率が95%を超えていることを示すLoggerの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - ストレージグループの使用率が95%を超過 (統合)	統合クエリ	このフィルターは、ストレージグループの使用率が95%を超えていることを示すLoggerの内部イベントを探します。
システムアラート - 着信イベントはゼロ (CEF形式)	正規表現	このフィルターは、Loggerがイベントを受信していないことを示すLoggerの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - 着信イベントはゼロ (統合)	統合クエリ	このフィルターは、Loggerがイベントを受信していないことを示すLoggerの内部イベントを探します。
システムアラート - 発信イベントはゼロ (CEF形式)	正規表現	このフィルターは、Loggerがイベントを転送していないことを示すLoggerの内部イベントを探します。これは、正規表現フィルターであり、アラートを作成するために使用できます。
システムアラート - 発信イベントはゼロ (統合)	統合クエリ	このフィルターは、Loggerがイベントを転送していないことを示すLoggerの内部イベントを探します。
システムステータス - コネクタホストによるCPU利用	統合クエリ	このフィルターは、SmartConnectorシステムのヘルスイベントを探し、ホストごとにCPU使用率をグラフ化します。
システムステータス - コネクタホストによるディスクの使用	統合クエリ	このフィルターは、SmartConnectorシステムのヘルスイベントを探し、ホストごとにディスク使用率をグラフ化します。
システムステータス - コネクタホストによるメモリ利用	統合クエリ	このフィルターは、SmartConnectorシステムのヘルスイベントを探し、ホストごとにメモリ使用率をグラフ化します。
Unix - CRON関連イベント	統合クエリ	このフィルターは、キーワードcronを含むイベントを探します。

フィルター(続き)

フィルター	種類	説明
Unix - IOエラーおよび警告	統合クエリ	このフィルターは、キーワードerrorまたはwarningを含むI/Oイベントを探します。
Unix - PAMおよびSudoメッセージ	統合クエリ	このフィルターは、キーワードPAMまたはsudoを含むイベントを探します。
Unix - パスワードの変更	統合クエリ	このフィルターは、パスワード変更に関連するイベントを探します。
Unix - SAMBAイベント	統合クエリ	このフィルターは、SAMBAに関連するイベントを探します。
Unix - SSH認証	統合クエリ	このフィルターは、SSH認証イベントを探します。
Unix - ユーザおよびグループの追加	統合クエリ	このフィルターは、ユーザーまたはグループの追加に関連するイベントを探します。
Unix - ユーザおよびグループの削除	統合クエリ	このフィルターは、ユーザーまたはグループの削除に関連するイベントを探します。
Windows - グローバルグループに追加されたアカウント	統合クエリ	このフィルターは、WindowsアカウントのGlobal Groupへの追加に関連する非CEFイベントを探します。
Windows - グローバルグループに追加されたアカウント (CEF)	統合クエリ	このフィルターは、Windowsアカウントのグローバルグループへの追加に関連するCEFイベントを探します。
Windows - 監査ポリシーの変更	統合クエリ	このフィルターは、Windows監査ポリシーに関連する非CEFイベントを探します。
Windows - 監査ポリシーの変更 (CEF)	統合クエリ	このフィルターは、Windows監査ポリシーに関連するCEFイベントを探します。
Windows - パスワードの試行を変更	統合クエリ	このフィルターは、Windowsパスワード変更に関連する非CEFイベントを探します。
Windows - パスワードの試行を変更 (CEF)	統合クエリ	このフィルターは、Windowsパスワード変更に関連するCEFイベントを探します。
Windows - 作成されたグローバルグループ	統合クエリ	このフィルターは、Windowsグローバルグループの作成に関連する非CEFイベントを探します。
Windows - 作成されたグローバルグループ (CEF)	統合クエリ	このフィルターは、Windowsグローバルグループの作成に関連するCEFイベントを探します。
Windows - ログオン不正なユーザ名またはパスワード	統合クエリ	このフィルターは、Windowsログオン失敗に関連する非CEFイベントを探します。
Windows - ログオン不正なユーザ名またはパスワード (CEF)	統合クエリ	このフィルターは、Windowsログオン失敗に関連するCEFイベントを探します。

フィルター(続き)

フィルター	種類	説明
Windows - ログオンローカルユーザ	統合クエリ	このフィルターは、ローカルシステムへのWindowsログオンに関連する非CEFイベントを探します。
Windows - ログオン ローカル ユーザ(CEF)	統合クエリ	このフィルターは、ローカルシステムへのWindowsログオンに関連するCEFイベントを探します。
Windows - ログオンリモートユーザ	統合クエリ	このフィルターは、リモートシステムへのWindowsログオンに関連する非CEFイベントを探します。
Windows - ログオンリモートユーザ(CEF)	統合クエリ	このフィルターは、リモートシステムへのWindowsログオンに関連するCEFイベントを探します。
Windows - ログオンの予期せぬ失敗	統合クエリ	このフィルターは、予期せず失敗したWindowsログオンに関連する非CEFイベントを探します。
Windows - ログオンの予期せぬ失敗 (CEF)	統合クエリ	このフィルターは、予期せず失敗したWindowsログオンに関連するCEFイベントを探します。
Windows - 新しいプロセスの作成	統合クエリ	このフィルターは、新しいWindowsプロセスの作成に関連する非CEFイベントを探します。
Windows - 新しいプロセスの作成 (CEF)	統合クエリ	このフィルターは、新しいWindowsプロセスの作成に関連するCEFイベントを探します。
Windows - 認証前処理の失敗	統合クエリ	このフィルターは、Windowsの事前認証に関連する非CEFイベントを探します。
Windows - 認証前処理の失敗 (CEF)	統合クエリ	このフィルターは、Windowsの事前認証に関連するCEFイベントを探します。
Windows - 新規のログオンに割り当てられた特別権限	統合クエリ	このフィルターは、特別な権限を持つアカウント (パワーユーザーまたは管理者などのアカウント) のログオンに関連する非CEFイベントを探します。
Windows - 新規のログオンに割り当てられた特別権限 (CEF)	統合クエリ	このフィルターは、特別な権限を持つアカウント (パワーユーザーまたは管理者などのアカウント) のログオンに関連するCEFイベントを探します。
Windows - ユーザアカウントの変更	統合クエリ	このフィルターは、ユーザーアカウントの変更に関連する非CEFイベントを探します。
Windows - ユーザアカウントの変更 (CEF)	統合クエリ	このフィルターは、ユーザーアカウントの変更に関連するCEFイベントを探します。
Windows - ユーザアカウントパスワードの設定	統合クエリ	このフィルターは、ユーザーアカウントのパスワード変更に関連する非CEFイベントを探します。
Windows - ユーザアカウントパスワードの設定 (CEF)	統合クエリ	このフィルターは、ユーザーアカウントのパスワード変更に関連するCEFイベントを探します。
Windows - Windowsイベント (CEF)	統合クエリ	このフィルターは、Microsoft Windowsによって生成されるすべてのCEFイベントを探します。

付録G: 工場出荷時設定の復元

以下のトピックでは、アプライアンスを元の工場出荷時設定に戻すために、現在のファイルを元のシステムのイメージで上書きする方法について説明します。

注意: アプライアンスを元の工場出荷時設定に戻すと、一部の設定と**すべてのイベントデータが削除されて復元不能になり**ます。

システムを復元する前に

工場出荷時設定を復元する前に、以下の注意事項とガイドラインに注意してください。

Loggerの設定をバックアップから復元するときは、最初にアプライアンスがバックアップから復元されていることを確認してから、目的のバージョンへのアップグレードを完了します。

復元後、データと設定のバックアップを復元できます。

マルチパスSANが有効になっているロガー

Loggerで5.1以降が実行され、マルチパスSANが有効になっている場合、以下のいずれかの状況になることがあります。

- システムをHPEに返却し、Logger 5.0 Patch 3以前が実行する新しいシステムを受け取った
- システムを工場出荷時のデフォルト設定に復元したため、Loggerのバージョンが5.0 Patch 3以前にリセットされた

Loggerでバージョン5.1が実行され、マルチパスが有効になっていた最後の稼動状態を復元するには、LUNを接続する前にシステムをLogger 5.1以降にアップグレードする必要があります。

システムの復元

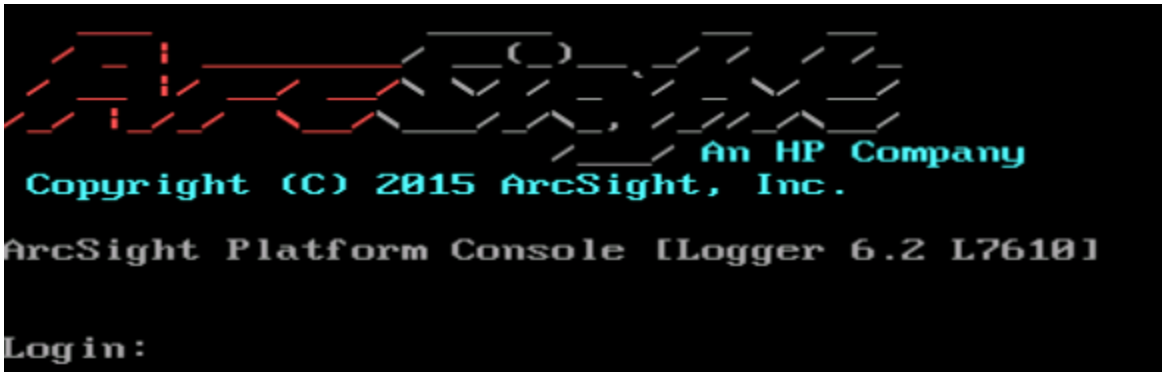
工場出荷時設定を復元するための手順は、アプライアンスモデルごとに異なります。使用しているアプライアンスに対応する適切なセクションを参照してください。

LX400以前のアプライアンスモデルの復元

LX400以前のアプライアンスモデルを元の工場出荷時設定に復元するには、組み込みのAcronis True Imageソフトウェアを使用します。

LX400以降のアプライアンスモデルを復元するには

1. キーボード、モニター、およびマウスをアプライアンスに直接接続します。またはアプライアンスにiLO経由のリモートアクセスが設定されている場合は、その機能を使用してアプライアンスのコンソールにアクセスできます(Loggerアプライアンスでリモートアクセスを設定する方法については、『Loggerインストールガイド』を参照してください)。下図のような画面が表示されます。



2. アプライアンスにログインし、コマンドプロンプトで「reboot」と入力し、Enterキーを押します。
3. システムが再起動すると、メッセージがスクロールします。下図のようなメッセージが画面に表示されたら、すぐにキーボードのいずれかのキーを押します。

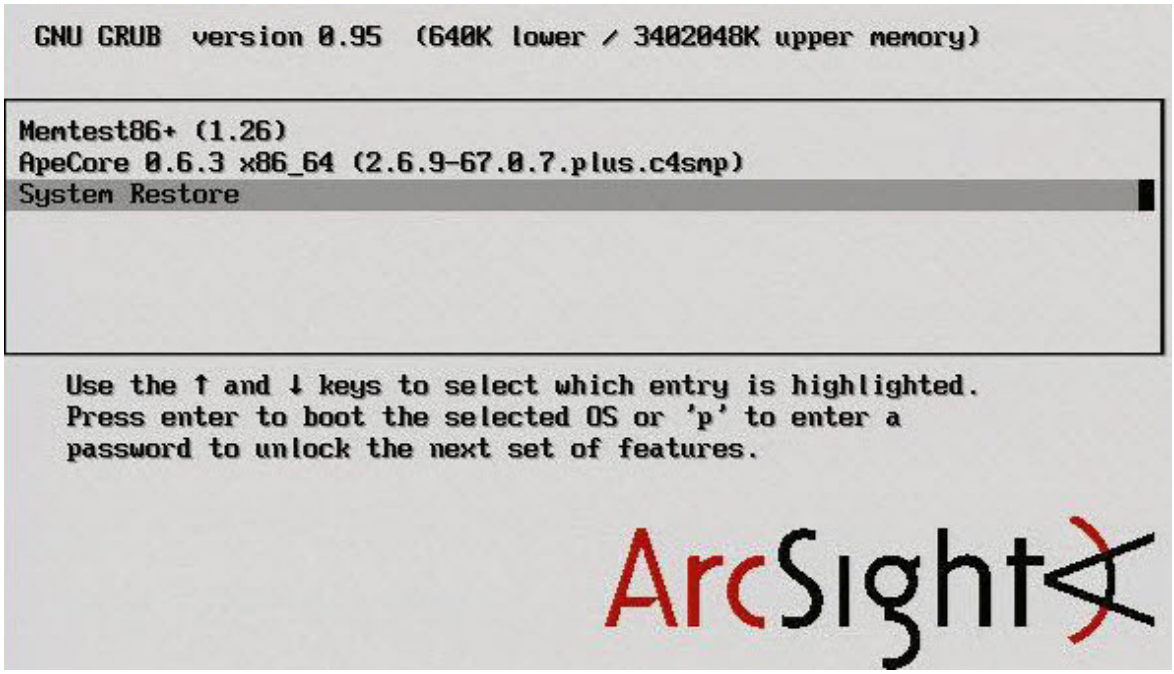
   ```
   Press any key to enter the menu

   Booting Red Hat Enterprise Linux <version> in N seconds...
   ```

   このメッセージは、非常に短時間しか表示されません。キーボードのキーを素早く押してください。そうしないと、アプライアンスは通常の起動を続行します。BIOSが起動したら、OSが起動する前にキーを押す必要があります。

   OSが起動すると、次のキャプチャー画像のような画面が表示されます。その場合はやり直す必要があります。

4. セッションビューアーが開きます。



マウスまたは矢印キーを使用して [**System Restore**] を選択し、**Enter**キーを押します。

5. [**Acronis True Image Echo Server**] ダイアログボックスで、[**Pick a Task**] リストから [**Recovery**] を選択し、Enterキーを押します。
6. Restore Data Wizardが起動したら、[**Next**] をクリックして続行します。
7. [Welcome to the Restore Data Wizard] ページで、[**Next**] をクリックして続行します。
8. [**Backup Archive Selection**] ページで [**Acronis Secure Zone**] を選択し、[**Next**] をクリックします。このページと以降のウィザードページで行う変更は、復元処理を開始する前に確認する機会があります。
9. [**Restoration Type Selection**] ページで [**Restore disks or partitions**] を選択し、[**Next**] をクリックします。カスタマーサポートから明確に指示があった場合のみ他のオプションを選択してください。
10. [**Partition or Disk to Restore**] ページで、**cciss/c0d0**または**sda** (アプライアンスモデルによって異なります) というラベルが付けられたドライブ全体を選択し、[**Next**] をクリックします。
11. [**NT Signature selection for image restoration**] ページで、復元したディスクからのNTシグネチャーを処理する方法を選択し、[**Next**] をクリックします。
12. [**Restored Hard disk Location**] ページで、復元するドライブ (**cciss/c0d0**または**sda**) を選択し、[**Next**] をクリックします。
13. [**Non-empty Destination Hard Disk Drive**] ページで、[**Yes, I want to delete all partitions on the destination hard disk drive before restoring**] を選択し、[**Next**] をクリックします。
14. [**Next Selection**] ページで [**No, I do not**] を選択し、[**Next**] をクリックします (復元する他のパーティションやディスクはありません)。

15. アプライアンスをリセットする前にアーカイブを検証する場合は、[**Restoration Options**] ページで、[**Validate backup archive for the data restoration process**] を選択します。アプライアンスを自動的に再起動するには [**Reboot the computer automatically after the restoration is finished**] を選択します。[**Next**] をクリックします。
16. 実行する操作のチェックリストを確認し、[**Proceed**] をクリックしてファクトリーリセットを開始します。前のページに戻るには [**Back**] をクリックします。

    注意: 復元処理の間は、中断したり、Loggerアプライアンスの電源をオフにしたりしないでください。復元処理を中断すると、システムが回復不能な状態に陥る可能性があります。

    進行状況バーに現在の処理のステータスと全体の進行状況が表示されます。
17. データが正常に復元されたことを示すメッセージが表示されたら、[**OK**] をクリックします。

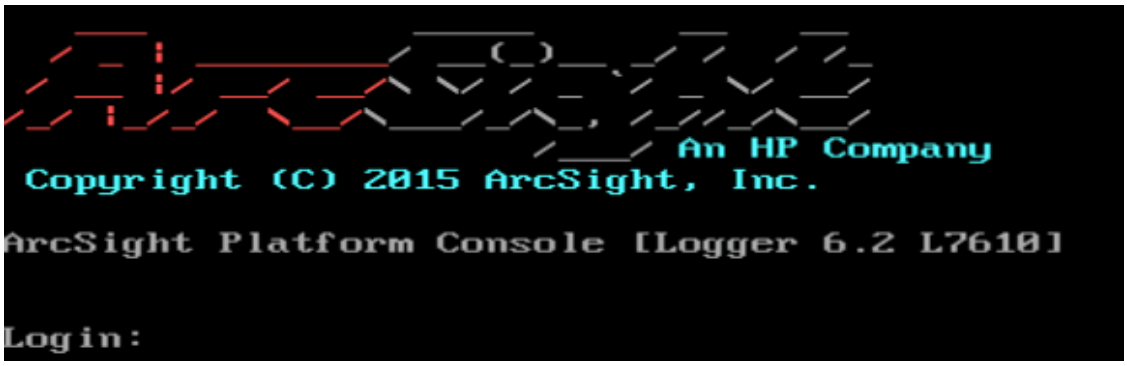
    自動的な再起動を指定した場合、復元が完了するとアプライアンスが再起動します。自動的な再起動を指定しなかった場合は、手動で再起動します。

LX500またはLX600アプライアンスモデルの復元

LX500またはLX600アプライアンスモデルを元の工場出荷時設定に復元するには、組み込みのSystem Restoreユーティリティを使用します。

LX500またはLX600アプライアンスを復元するには

1. キーボード、モニター、およびマウスをアプライアンスに直接接続します。またはアプライアンスにiLO経由のリモートアクセスが設定されている場合は、その機能を使用してアプライアンスのコンソールにアクセスできます(Loggerアプライアンスでリモートアクセスを設定する方法については、『Loggerインストールガイド』を参照してください)。下図のような画面が表示されます。



2. ユーザー名とパスワードを使用して、アプライアンスにログインします。
3. コマンドプロンプトで、「`reboot`」と入力し、Enterキーを押します。
4. システムが再起動すると、メッセージがスクロールします。下図のようなメッセージが画面に表示されたら、すぐにキーボードのいずれかのキーを押します。

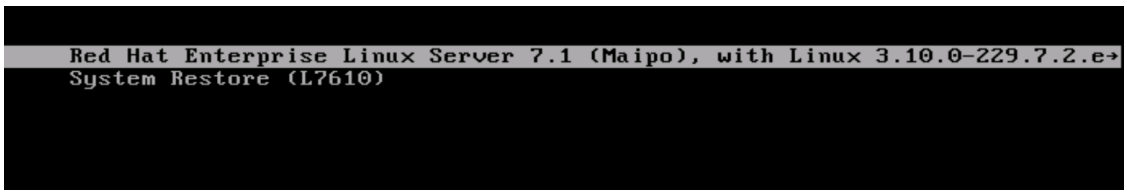
```
Press any key to enter the menu

Booting Red Hat Enterprise Linux <version> in N seconds...
```

このメッセージは、非常に短時間しか表示されません。キーボードのキーを素早く押してください。そうしないと、アプライアンスは通常の起動を続行します。BIOSが起動したら、OSが起動する前にキーを押す必要があります。

OSの起動が始まると、次のキャプチャー画像のような画面が表示されます。その場合はやり直す必要があります。

5. セッションビューアーウィンドウが開きます。



マウスまたは矢印キーを使用して、[**System Restore L<XXXX>**]を選択し、**Enter**キーを押します。

6. System Restoreによって自動的にアーカイブイメージが検出され、表示されます。イメージは、`YYYY-MM-DD_LXX00_L<XXXX>.ari`というパターンに従って名前が付けられます。`YYYY-MM-DD`は日付、`LXX00`はアプライアンスのバージョン、`L<XXXX>`はアプライアンスのビルド番号です。
7. **F1**キー(自動選択)を押して、上部のパネルに表示されるソースイメージを下部のパネルに表示されるターゲットディスクに自動的にマップします。リストアイメージ名が一番右の列に表示されます。
8. オプションで、**F10** (検証)を押して、復元を行う前にアーカイブが損傷していないことを確認します。アーカイブが確認されたら、Enterを押して続行します。
9. **F2** (復元)を押して復元処理を開始します。ダイアログボックスで、復元するかどうかが質問されます。**y**を押して復元を続けるか、**n**を押してキャンセルします。
10. 進行状況バーに、復元のステータスが表示されます。

> **注意:** 復元処理の間は、中断したり、アプライアンスの電源をオフにしたりしないでください。復元処理を中断すると、システムが回復不能な状態に陥る可能性があります。

11. 復元処理が完了したら、F12を押してアプライアンスを再起動します。ダイアログボックスで、再起動するかどうかを質問されます。**y**を押して再起動を続けます。

付録H: ArcSight ESMからのLogger検索

ArcSight LoggerとArcSight ESMがネットワークインフラストラクチャーに展開されている場合、Logger検索操作をArcSightコマンドセンターまたはArcSightコンソールから実行できます。

ESM 6.5c以降を実行している場合は、ArcSight Command Centerで提供されている検索機能を使用できます。この機能については、『ArcSightコマンドセンターユーザーズガイド』を参照してください。ESM 6.0c以前のバージョンでは、Logger検索をArcSightコンソールから実行できます。

ArcSightコンソールの統合された検索機能を使用する方法については、以下のトピックを参照してください。

統合検索機能について

ヒント: ESM 6.5c以上を使用している場合は、ここで説明するArcSightコンソールに加えて、ArcSightコマンドセンターから検索を行うこともできます。詳細は『ArcSightコマンドセンターUser's Guide』を参照してください。

ArcSightコンソールからLogger上の検索操作を実行するための方法としては、以下の方法があります。

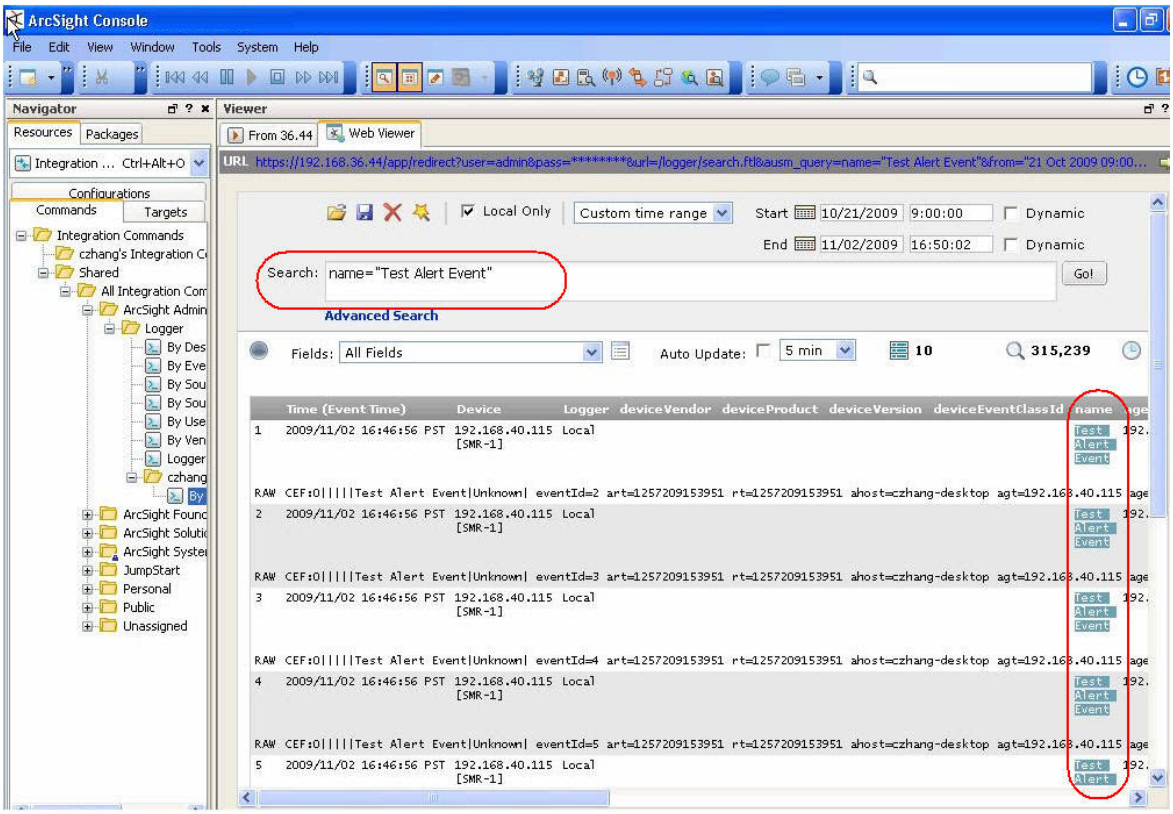
- 検索: 検索オプションを指定可能な通常の検索操作です。
- クイック検索: ArcSightコンソールの表示チャネルで選択したフィールドと値に基づく検索操作です。検索オプションの指定は求められません。

Logger検索を実行するには、ArcSightコンソールの表示チャネルのイベントを右クリックしてメニューを表示し、検索方法 (Logger検索またはLoggerクイック検索) を選択します。

Logger検索を選択した場合、イベント名、通知先、ソースなどの検索オプションと、検索を実行するLoggerアプライアンスを選択する必要があります (複数のLoggerアプライアンスがある場合)。Loggerクイック検索を選択した場合は、クリックしたフィールドに基づいて検索が実行されるため、検索オプションの指定を求められません。

検索結果がArcSightコンソールに表示されます (下図参照)。

注: この図は、ESM 5.xの場合です。ESM 6.xでは、結果が別のブラウザーウィンドウに表示されます。



ArcSightコンソールからLogger上の検索操作を実行する前に、検索を実行するユーザーを認証するために使用されるパラメーターをArcSightコンソールで設定する必要があります。認証は、基本認証 (ユーザー名とパスワード) またはOTP (ワンタイムパスワード) を通じて実行できます。このオプションを使用すると、LoggerとArcSightコンソールの間のユーザー認証のセキュリティが非常に高まります。

デフォルトでは、ArcSightコンソールからのLogger検索はOTP方式を使用して認証されます。ただし、LoggerまたはArcSightコンソールが、OTPオプションをサポートしているリリースを実行していない場合、エラーメッセージが表示され基本認証が使用されます。

セットアップと設定

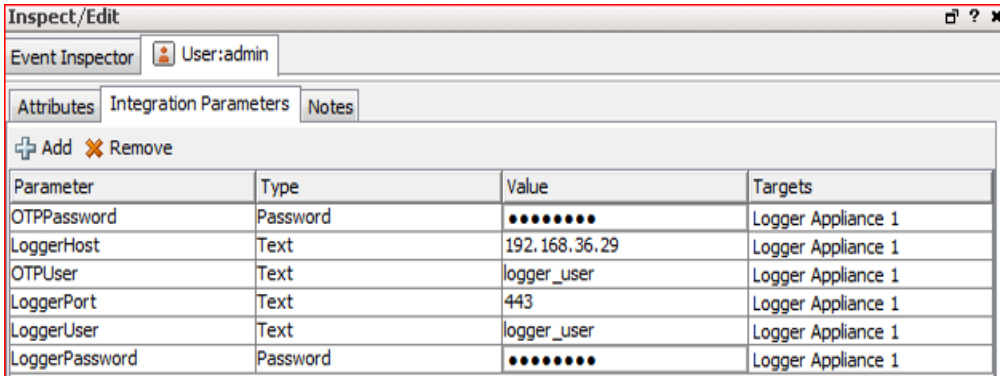
次の表に、LoggerおよびArcSightコンソールが実行している必要がある最小のバージョンと推奨されるバージョンを示します。

オプション	要件
推奨	Logger 6.2 ESM 6.8 **ヒント:** サポートされている最新のESMリリースを確認するには、HPE ArcSight Protect 724のArcSight製品ドキュメントを参照してください。
最低	Logger 5.1 ESM 5.0 SP1 Patch 2

ESMの場合

以下の手順に従って、統合された検索操作を実行するようにArcSightマネージャーのセットアップと設定を行います。

1. ArcSightマネージャーが推奨されるバージョンのいずれかを実行していることを確認します。
2. 『ArcSight ESMコンソールユーザーズガイド』の手順に従って、Logger上の統合検索用にArcSightコンソールを設定します。Loggerアクセス用のユーザーを設定する際 (ユーザーガイドの「Loggerへのユーザーアクセスのセットアップ」セクションを参照)、以下の統合パラメーターを指定します。



パラメーター	説明
Loggerアプライアンスターゲットの場合	
LoggerUser	Loggerアプライアンスターゲットのユーザーアカウント。
LoggerPassword	LoggerUserのパスワード。
LoggerHost	LoggerホストのIPアドレス。
LoggerPort	443
ソフトウェアLoggerターゲットの場合	
OTPUser	ワンタイムパスワード (OTP) 認証用のユーザーアカウント。このアカウントは、Logger上に存在している必要があります。
OTPPassword	OTPUserのパスワード。
LoggerHost	LoggerホストのIPアドレス。
LoggerPort	インストール時に割り当てたLoggerポート番号。

『ArcSight ESM User's Guide』は、Protect 724のArcSight製品マニュアルのコミュニティから入手できます。

Loggerの場合

確認すべき内容

1. Loggerが推奨されるバージョンのいずれかであること。
2. Loggerユーザー名が、ArcSightコンソールで統合パラメーター (`in`) の作成時に指定したユーザー名であること。

サポートされる検索オプション

ArcSightコンソールからLogger検索 (クイック検索ではない) を実行するとき、以下の検索オプションから選択できます。

- 通知先別
- イベント名別
- ソース別
- ソースと通知先別
- ユーザー別
- ベンダと製品別

また、ArcSightコンソールで複数のLoggerが設定されている場合は、統合検索を実行するLoggerを選択できます。

ガイドライン

ArcSightコンソールからLogger検索を実行する際には、以下のガイドラインに注意してください。

- Logger上で検索を実行するために、フィールドベースの検索クエリが使用されます。
- ArcSightコンソールの表示チャネルからの検索のみがサポートされています。他のESMリソースからの検索はサポートされていません。
- 1つの検索操作につき1つの検索オプションのみがサポートされます。つまり、1つの検索操作で[イベント名別]と[通知先別]の両方を選択することはできません。複数の検索オプションについては、「サポートされる検索オプション」(702ページ)を参照してください。
- 検索操作は、一度に1つのLoggerに対してのみ実行できます。つまり、複数のLoggerをArcSightコンソール上のメニューリストから選択することはできません。

  また、他のLoggerが他のLoggerとピアリングしていても、統合検索は、ArcSightコンソール上のメニューリストから選択したローカルLogger上でのみ実行されます。
- ワンタイムパスワード(OTP)認証が使用できるのは、Loggerが5.1以降を実行し、ArcSightコンソールが5.0 SP1 Patch 2以降を実行している場合のみです。パスワードポリシーについては、お使いのバージョンの『ESM管理者ガイド』を確認してください。

  OTPを使用できない場合、ArcSightコンソールから実行した検索に対し、1回だけ使用されるセッショントークンをネゴシエートできなかったために通常の認証が使用されることを示すメッセージが表示されます。[**OK**]をクリックします。続いて、LoggerUserとLoggerPasswordを使用して認証します。

ArcSightコンソールからのLogger上の検索

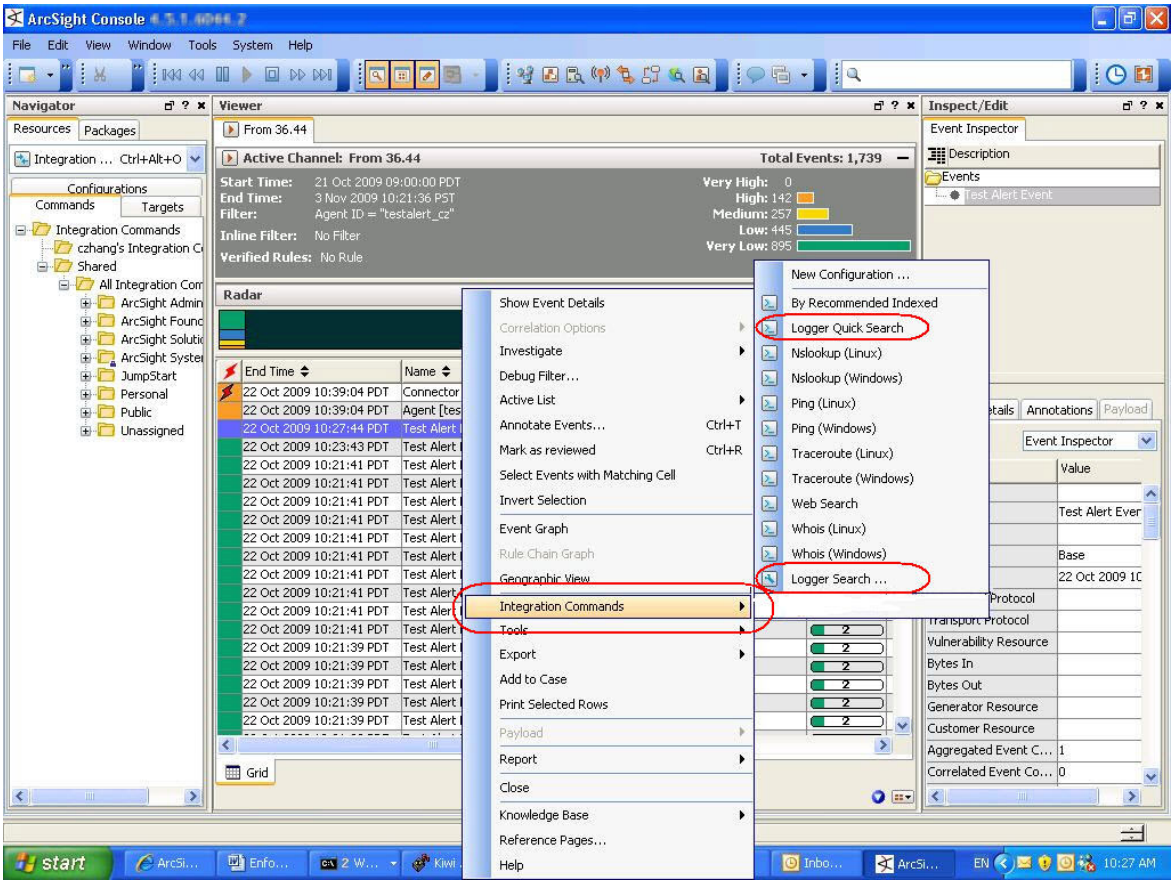
ArcSightコンソールからLogger上で2つのタイプの検索(クイック検索と通常の検索)を実行することができます。実行する検索のタイプの手順に従ってください。

クイック検索の実行:

Logger上でクイック検索を実行するには(「統合検索機能について」(699ページ)を参照)

1. ArcSightコンソールの表示チャネルのイベントフィールドを右クリックします。
2. メニューリストから、[**組み込みコマンド(Integration Commands)**] > [**Loggerクイック検**

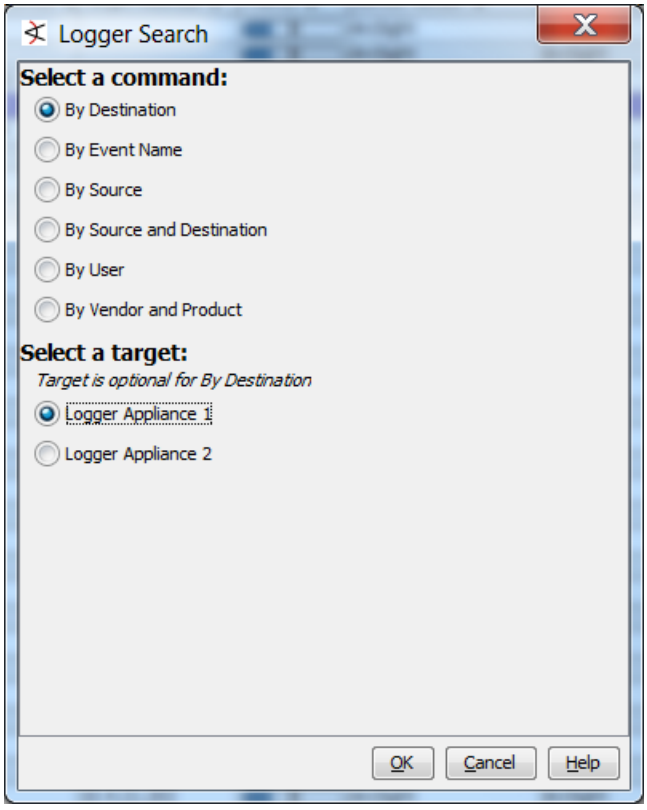
索 (Logger Quick Search)] をクリックします (下図参照)。



通常の検索の実行:

通常の**検索**を実行するには (検索オプションを指定)

1. ArcSightコンソールの表示チャネルのイベントフィールドを右クリックします。
2. メニューリストから、**[組み込みコマンド] > [Logger 検索] > [検索オプション]** を選択します (下図を参照)。



3. [**OK**] をクリックして検索を実行するか、[**キャンセル (Cancel)**] をクリックして中断します。
   a. LoggerまたはArcSightコンソールが、OTPオプションをサポートしているリリースを実行していない場合、1回だけ使用されるセッショントークンをネゴシエートできず、代わりに基本認証が使用されることを示すエラーメッセージが表示されます。
   b. 問題ない場合は、[**OK**] をクリックして続行します。

検索結果がArcSightコンソールWebビューアーに表示されます。

ドキュメントのフィードバックを送信

本ドキュメントについてのご意見、ご感想については、電子メールでドキュメント制作チームまでご連絡ください。このシステムで電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電子メールウィンドウが開きます。

管理者ガイド (Logger 6.4) に関するフィードバック

本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、arc-doc@hpe.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。