

vRealize Log Insight の使用

2018 年 9 月 20 日

vRealize Log Insight 4.7



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴァイエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2014-2018 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

vRealize Log Insight 5

1 vRealize Log Insight の機能の利用 6

vRealize Log Insight Web ユーザー インターフェイスの概要 8

ログ イベントの検索とフィルタリング 9

イベント タイプのグループ化 9

ログ イベントの情報 10

ログ イベントを時間範囲でフィルタリングする 11

完全なキーワードを含むログ イベントを検索する 11

フィールド操作でログ イベントを検索する 12

イベントの前後に発生したイベントを検索する 13

コンテキストでのイベントの表示 14

イベント傾向の分析 14

すべてのフィルタリング ルールをクリアする 15

検索クエリの例 15

正規表現の例 17

対話形式の分析チャートを使用したログ分析 19

チャート タイプ 20

マルチファンクション チャート 20

集約関数 20

チャートの操作 21

インタラクティブ分析チャートのタイプを変更する 22

動的なフィールドの抽出 23

ワンクリック抽出を使ってフィールドを抽出する 23

抽出されたフィールドを変更する 24

抽出されたフィールドのコンテンツ バックのフィルタリング 25

抽出したフィールドの複製 25

抽出されたフィールドを削除する 26

管理クエリの管理 27

vRealize Log Insight でクエリを保存する 27

vRealize Log Insight でクエリの名前を変更する 28

vRealize Log Insight でクエリをロードする 28

vRealize Log Insight からクエリを削除する 28

現在のクエリを共有する 29

現在のクエリをエクスポートする 29

クエリのスナップショットの作成 30

vRealize Log Insight クエリ結果のトラブルシューティング 30

ダッシュボードの操作 31

ダッシュボードの管理	32
ダッシュボードにクエリ リスト ウィジェットを追加する	34
ダッシュボードのクエリ リスト ウィジェットにクエリを追加する	34
ダッシュボードにフィールドテーブル ウィジェットを追加する	35
ダッシュボードにイベントタイプ ウィジェットを追加する	36
ダッシュボードにイベントトレンド ウィジェットを追加する	36
チャートのフィールド値を使用してフィルタリングする	36
コンテンツ パックの操作	37
コンテンツ パック マーケットプレイスからのコンテンツ パックのインストール	38
コンテンツ パック マーケットプレイスからインストールしたコンテンツ パックのアップグレード	39
コンテンツ パックをインポートする	39
コンテンツ パックをエクスポートする	41
コンテンツ パック要素に関する詳細を表示する	42
コンテンツ パックをアンインストールする	43
コンテンツ パックの作成	43
コンテンツ パックの用語	44
クエリ	45
ダッシュボードのベスト プラクティス	51
コンテンツ パックのインポート エラー	53
コンテンツ パックの公開要件	54
コンテンツ パックを送信する	55
vRealize Log Insight のアラート クエリ	56
E メール通知を送信するためのアラート クエリの追加	58
Webhook を使用したサードパーティ製品へのアラート送信について	59
アラート クエリの表示	64
アラート クエリの変更	65
アラート クエリの有効化	67
アラート クエリの削除	68

vRealize Log Insight

vRealize Log Insight の使用トピックでは、Web ユーザー インターフェイスの使用に関する情報を提供します。これには、ログ メッセージのフィルタリングと検索、分析の実行と検索結果の可視化、アラート クエリの処理、カスタマイズされたクエリに基づくログ メッセージからの動的なフィールド抽出などの手順が含まれます。

この情報は、vRealize Log Insight を使用する方を対象としています。

vRealize Log Insight の機能の利用

vRealize Log Insight は、vCloud Suite (vSphere のすべてのエディションを含む) に対してスケーラブルなログ集約とインデックス作成を提供し、ほぼリアルタイムでの検索および分析機能を備えています。

vRealize Log Insight は、ログを収集、インポート、分析することによって、システム、サービス、アプリケーションに関する問題に回答を提供し、重要な洞察を導きます。

高性能な取り込み

vRealize Log Insight は、あらゆるタイプのログ、または機械的に生成されたデータを処理できます。スループットは高く、遅延は低く、Syslog と取り込み API を介してデータを受け取ることができます。

スケーラビリティ

vRealize Log Insight は複数の仮想アプライアンス インスタンスを使用してスケールアウトできます。これにより、取り込み時のスループットを線形的にスケールアップし、クエリのパフォーマンスを高めて、取り込み時に高可用性を実現することができます。クラスター モードの場合、vRealize Log Insight はマスター ノードとワーカー ノードを提供します。マスター ノードとワーカー ノードはいずれもデータのサブセットを処理します。マスター ノードとクエリ ノードはデータのあらゆるサブセットにクエリを実行して、結果を集計します。

ほぼリアルタイムの検索

vRealize Log Insight によって取り込まれたデータは、数秒以内に検索可能になります。また、履歴データも同じインターフェイスから同等に低い遅延で検索できます。

vRealize Log Insight は完全キーワード クエリをサポートしています。キーワードは、任意の英数字、ハイフン、またはアンダースコア文字として定義されます。完全キーワード クエリに加え、vRealize Log Insight は glob クエリ (たとえば、erro?、vm* など) およびフィールド ベースのフィルタリング (たとえば、test* に一致しないホスト名、「10.64」を含む IP アドレスなど) もサポートしています。さらに、数値を含むログ メッセージ フィールドを使用して、選択フィルタを定義することもできます (たとえば、CPU>80、10<threads<100 など)。

検索結果は、個別イベントとして表示されます。各イベントは単一のソースからのものですが、検索結果は複数のソースからのものである場合があります。vRealize Log Insight を使用してデータを 1 つまたは複数の次元 (たとえば、時間と要求識別子など) で関連付けることができるため、スタック全体で一貫した表示を得られます。そのため、原因分析が大幅に容易になります。

Windows および Linux 用のエージェント

vRealize Log Insight には、Linux および Windows マシンでイベントとファイルを収集するエージェントが含まれます。

インテリジェント グループینگ

vRealize Log Insight は、新しいマシン学習テクノロジーを採用しています。インテリジェント グループینگでは、受信した構造化されていないデータをスキャンし、メッセージを問題タイプでグループ化することにより、物理的、仮想的、およびハイブリッドなクラウド環境に広がる問題をすばやく理解することができます。

集約

ログ データから抽出されたフィールドを使用して集約することができます。これは、関係データベースや Microsoft Excel のピボット テーブルでの GROUP-BY クエリの機能に似ています。違いは、抽出、変換、読み込み（ETL）処理の必要がなく、vRealize Log Insight はあらゆるサイズのデータにスケーリングできるということです。

データの集約ビューを生成することで、複数のシステムやアプリケーションにアクセスすることなく、特定のイベントまたはエラーを特定できます。たとえば、重要なシステム メトリック（たとえば、1 分間あたりのエラー数など）を表示している間に、特定の時間範囲のイベントにドリルダウンし、環境内で発生したエラーを調べることができます。

ランタイムのフィールド抽出

生ログデータは常に理解しやすいとは限らないため、検索および集約のためにデータを処理して重要なフィールドを識別する必要がある場合があります。vRealize Log Insight では、この問題に対処するために、ランタイムのフィールド抽出機能を提供します。正規表現を指定することで、どのフィールドでもデータから動的に抽出することができます。抽出されたフィールドは、選択、予測、集約に使用することができます。これは、解析時に抽出されたフィールドの使用法と似ています。

ダッシュボード

詳しく監視したい有用なメトリックのダッシュボードを作成できます。任意のクエリをダッシュボード ウィジェットに変換して、任意の時間範囲で要約することができます。システムのパフォーマンスを過去 5 分間、1 時間、あるいは 1 日にわたって選択できます。時間ごとにエラーの内訳を表示し、ログ イベントの傾向を観察できます。

セキュリティの考慮事項

IT 上の意思決定者、設計者、管理者など、vRealize Log Insight のセキュリティ コンポーネントに精通する必要があるユーザーは、vRealize Log Insight の管理 のセキュリティに関するトピックをお読みください。

これらのトピックは、vRealize Log Insight のセキュリティ機能についての簡潔な参考情報を提供します。トピックの内容は、製品の外部インターフェイス、ポート、認証のメカニズム、セキュリティ機能を構成および管理するためのオプションなどです。

この章には、次のトピックが含まれています。

- [vRealize Log Insight Web ユーザー インターフェイスの概要](#)
- [ログ イベントの検索とフィルタリング](#)
- [対話形式の分析チャートを使用したログ分析](#)
- [動的なフィールドの抽出](#)
- [管理クエリの管理](#)
- [ダッシュボードの操作](#)
- [コンテンツ パックの操作](#)
- [コンテンツ パックの作成](#)
- [vRealize Log Insight のアラート クエリ](#)

vRealize Log Insight Web ユーザー インターフェイスの概要

ユーザーがアクセスできる機能は、vRealize Log Insight Web ユーザー インターフェイスのログインで使用するユーザー アカウントによって異なります。

[ダッシュボード] タブ

[ダッシュボード] タブには、カスタム ダッシュボードとコンテンツ パック ダッシュボードが含まれています。[ダッシュボード] タブでは、お使いの環境のログ イベントのグラフを表示したり、最も重要な情報にアクセスする一連のカスタム ウィジェットを作成したりすることができます。

[インタラクティブ分析] タブ

[インタラクティブ分析] タブでは、ログ イベントを検索してフィルタリングしたり、ログ イベントのタイムスタンプ、テキスト、ソース、フィールドを基にイベントを抽出するためのクエリを作成したりすることができます。vRealize Log Insight はクエリ結果のチャートを提供します。これらのチャートを保存して、後で [ダッシュボード] タブで検索することができます。

コンテンツ パック

コンテンツ パックには、特定の製品やログのセットに関連するダッシュボード、抽出されたフィールド、保存されたクエリ、アラートが含まれています。コンテンツ パックには、vRealize Log Insight Web ユーザー インターフェイスの右上にあるドロップダウン メニューからアクセスできます。

vRealize Log Insight ユーザーは、コンテンツ パックをインポートしたり、作成したりすることができます。 [コンテンツ パックの操作](#) を参照してください。

管理ユーザー インターフェイス

vRealize Log Insight 管理者はユーザー アカウントを管理し、ストレージの場所とアーカイブを構成し、電子メール通知用の発信 SMTP サーバを構成し、他の複数のパラメータを変更できます。管理 UI の URL 形式は `https://log_insight-host/admin/` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

ログ イベントの検索とフィルタリング

[インタラクティブ分析] タブでログ イベントを検索し、フィルタリングすることができます。

検索テキスト ボックスに任意の完全なキーワード、glob、または句を入力して、[検索] をクリックすると、指定のキーワードを含むイベントのみを検索することができます。

時間範囲は、Web ユーザー インターフェイスの [ダッシュボード] ページまたは [インタラクティブ分析] ページのいずれかで指定できます。時間範囲は、始まりと終わりも含めてフィルタ処理されます。

特定のフィールドの特定の値に一致するログ イベントを検索できます。メイン検索フィールドに引用符で囲んだテキストを入力すると、完全に一致する句が返されます。メイン検索フィールドにスペースを入力すると、論理 AND 演算子になります。検索ではフル トークンのみが使用されます。「err」を検索しても、「error」を一致として検出しません。

ログ イベントのリストの上にあるドロップダウン メニューやテキスト ボックスを使用すると、フィールドの検索条件またはフィルタを指定できます。

単一行のフィルタ内では、カンマで区切った値を使用して OR フィルタを指定できます。たとえば、[hostname] [contains] を選択して、**127.0.0.1, 127.0.0.2** と入力します。検索により、ホスト名が 127.0.0.1 または 127.0.0.2 のイベントが返されます。

注: [text contains] フィルタは、カンマ区切りの各値を完全なキーワードとして処理します。

内部クエリ言語の構文名（たとえば from または in）を使用するフィールドを持つクエリは処理できないため、使用しないでください。

フィールドごとに新しいフィルタ行を作成することで、複数のフィールド フィルタを結合できます。複数行フィルタに適用する演算子は切り替えることができます。

- [all] を選択すると、AND 演算子が適用されます。
- [any] を選択すると、OR 演算子が適用されます。

注: 切り替える値に関係なく、単一フィルタ行内にあるカンマ区切りの値の演算子は常に OR になります。

検索語に glob を使用できます。たとえば、vm* や vmw?re にすることができます。

- 0 個以上の文字には * を使用します。
- 1 個の文字には ? を使用します。

注: glob を検索語の最初の文字として使用することはできません。たとえば、フィルタリング クエリで 192.168.0* と指定できても、*.168.0.0 とすることはできません。

イベント タイプのグループ化

Log Insight は機械学習を使用して、類似のイベントをグループ化します。イベント タイプのグループ化により、トラブルシューティングと原因分析が容易になります。

Log Insight でクエリを実行する場合、結果の数はクエリと時間範囲によって異なります。ほとんどの場合、クエリによって大量の結果が返されます。機械学習は、Light Insight に送られるイベントから動的にパターンを学習して調整します。

[イベント タイプ] タブは、検索バーの下に [インタラクティブ分析] ページにあります。[イベント タイプ] タブをクリックすると、グループ化された類似イベントのリストが表示されます。

機械学習はイベントを分析して、類似のログ メッセージに含まれるフィールドのタイプを検出します。たとえば、タイプにはタイムスタンプ、文字列、整数、16 進数などがあります。検出されたタイプはハイパーリンクとして [イベント タイプ] リスト内に表示されます。

機械学習によって検出される各タイプは、スマート フィールドという新しいタイプのフィールドを表します。スマート フィールドのデフォルト名は、スマート フィールド形式 - `typenumber[event_type]` に従っています。スマート フィールドのデフォルト名は変更することができます。スマート フィールドに名前を付けると、他のフィールドとまったく同じように、[フィールド] セクションに表示されます。スマート フィールドは名前を変更したり削除したりできますが、その定義を変更することはできません。

機械学習では、`event_type` という新しい固定フィールドが導入されています。`event_type` をフィルタとして使用して、特定のイベント タイプをクエリに含めたり、クエリから除外したりすることができます。

ログ イベントの情報

vRealize Log Insight は、アプリケーション ログ、ネットワーク トレース、構成ファイル、メッセージ、パフォーマンス データおよびシステム状態のダンプなどの、マシンで生成されるすべての種類のログ データを収集して分析します。

オペレーティング システム、アプリケーション、ストレージ、ファイアウォール、ネットワーク デバイスなど、環境内に含まれるものすべてに vRealize Log Insight を接続してログを分析することで、企業全体の状態を把握できるようにします。

vRealize Log Insight を構成してログを収集できるようになったら、次のような方法でログ データを取り込むことができます。

- vSphere 統合 – vRealize Log Insight と vSphere を統合すると、vCenter Server のイベントや ESXi ホストのログを自動的に取り込むことができます。
- vRealize Operations Manager 統合 – vRealize Log Insight と vRealize Operations Manager を統合すると、さまざまなアラートを使用して vRealize Operations Manager で通知イベントを送信し、管理者に E メールを送信することができます。
- エージェント – vRealize Log Insight では、Linux または Windows から vRealize Log Insight にファイルやイベント ログを送信するための収集エージェントを使用できます。
- Syslog – vRealize Log Insight では、Syslog を介して任意のソースからデータを取り込むことができます。vRealize Log Insight サーバを Syslog の送信先として設定すれば実行できます。
- Syslogd –
- CFAPI – cfapi を使用して、イベントが元の形式を維持したまま vRealize Log Insight に送信されます。cfapi を介して送信されるイベントは、Syslog イベントのガイドラインに従う必要はなく、Syslog RFC に準拠するようには変更されません。

各イベントには、次の情報が含まれています。

タイプ	説明
タイムスタンプ	イベントが発生した時間
ソース	イベントの発生元です。ESXi ホストなどの Syslog メッセージの発生元、または Syslog 集約などのフォワーダがソースになることがあります。
テキスト	イベントの Raw テキストです。
フィールド	イベントから抽出された名前と値ペアです。エージェントで CFAPI プロトコルが使用されている場合にのみ、フィールドは固定フィールドとしてサーバに送られます。

注: vRealize Log Insight は、他の VMware 製品からのログ メッセージの内容に関与しません。ログの内容について質問がある場合は、そのログ メッセージを生成した製品のチームに問い合わせてください。

ログ イベントを時間範囲でフィルタリングする

ログ イベントをフィルタリングして、特定の期間のイベントのみを表示することができます。

時間範囲は、Web ユーザー インターフェイスの [ダッシュボード] ページまたは [インタラクティブ分析] ページのいずれかで指定できます。時間範囲は、始まりと終わりも含めてフィルタ処理されます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [検索] ボタンの左にあるドロップダウン メニューで、定義済み期間の 1 つを選択します。
- 2 (オプション) 時間範囲の開始点と終了点を設定するには、[カスタム時間範囲] を選択します。

完全なキーワードを含むログ イベントを検索する

完全なキーワードを含むログ イベントを検索できます。キーワードには、英数字、ハイフン、下線の文字が含まれます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 検索テキスト ボックスで、ログ イベント内で検索する完全なキーワードを入力して、[検索] ボタンをクリックします。

指定した完全なキーワードを含むログ イベントがリストに表示されます。

検索した文字列は黄色でハイライト表示されます。

次のステップ

現在のクエリを保存して、後の段階でロードすることができます。

フィールド操作でログ イベントを検索する

既存のフィールドのリストを使って、フィールドの特定の値でログ イベントを検索できます。

重要: vRealize Log Insight は、完全な英数字、ハイフン、アンダースコアの文字をインデックス化します。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [フィルタの追加] をクリックします。
- 3 検索テキスト ボックスの下フィルタ行で、最初のドロップダウン メニューを使用して、vRealize Log Insight 内で定義された任意のフィールドを選択します。

たとえば、[hostname] を選択します。

リストには、コンテンツ パックとカスタム パック内で静的に使用できるすべての定義済みフィールドがあります。[text] フィールド以外のフィールドは名前ですべて置換されます。[text] はメッセージ テキストを参照する特別なフィールドなので、[text] はリストの最上部に表示され、デフォルトで選択されています。

注: 数値フィールドには、文字列フィールドにはないその他の演算子が含まれています：[=]、[>]、[<]、[>=]、[<=]。これらの演算子は数値比較を実行し、文字列演算子を使うよりも多様な結果を生成します。たとえば、フィルタ `[response_time][=]02` は、値が 2 の [response_time] フィールドを持つイベントに一致します。フィルタ `[response_time][contains]02` は、上記と同じ一致にはなりません。

- 4 検索テキスト ボックスの下フィルタ行で、2 番目のドロップダウン メニューを使用して、最初のドロップダウン メニューで選択したフィールドに適用する操作を選択します。

たとえば、[contains] を選択します。[contains] フィルタは、フル トークンに一致します。「err」は「error」を一致として検出しません。

- 5 フィルタ ドロップダウン メニューの右にあるテキスト ボックスに、フィルタとして使用する値を入力します。複数の値をカンマで区切って挙げることができます。これらの値の演算子は OR です。

注: 2 番目のドロップダウン メニューで [exists] 演算子を選択した場合、テキスト ボックスは使用できません。

- 6 (オプション) さらにフィルタを追加する場合は、[フィルタの追加] をクリックします。

フィルタ行の上にトグル ボタンが表示されます。

- 7 (オプション) 複数のフィルタ行の場合は、フィルタ間の演算子を選択します。

オプション	説明
すべて	フィルタ行の間に AND 操作を適用する場合に選択します。
任意	フィルタ行の間に OR 操作を適用する場合に選択します。

デフォルトでは、[all] が選択されています。

- 8 [検索] ボタンをクリックします。

例：名前に共通の文字列があるホスト グループを検索する

複数のホストの中に、w1-stvc-205-prod3 という名前のホストと w1-stvc-206-prod5 という名前の別のホストがあるとします。

両方のホストのログをすべて検索するには、次のクエリを作成します。

1. [検索] テキスト ボックスを空のままにします。
- 2 フィルタを定義します。
 - a 最初のドロップダウン メニューで [hostname] を選択します。
 - b 演算子ドロップダウン メニューで [starts with] を選択します。
 - c 値のテキスト ボックスに **w1-stvc** と入力します。

または、[contains] 演算子を使用できます。ただし、検索値に glob を使用する必要があります。この例では、値のテキスト ボックスに **w1-stvc-*** と入力する必要があります。

- 3 [検索] ボタンをクリックします。

次のステップ

現在のクエリを保存して、後の段階でロードすることができます。

イベントの前後に発生したイベントを検索する

リスト内のイベントの前後に発生したイベントについて、ログ イベントのリストを検索できます。


イベントの前後の環境のステータスに関する詳細を知りたい場合は、その前後のイベントを確認できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。 `log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、リスト内のイベントを見つけます。

- 2 イベント行の左にある  をクリックして、[このイベントから時間範囲を設定] を選択します。
- 3 [イベントから時間範囲を設定] ダイアログ ボックスでドロップダウン メニューを使用して、時間範囲の期間と方向を選択します。

定義済みの期間のリストで 1 秒から 10 分の期間を選択できます。

- 4 [範囲の設定] をクリックします。

選択したイベントの前後のイベントがリストに表示されます。

注: この操作により、以前指定した検索パラメータとフィルタがすべてクリアされます。

コンテキストでのイベントの表示



ログ イベントのコンテキストを表示し、その前後に受信したログ イベントを参照できます。

イベントの前後の環境のステータスに関する詳細を知りたい場合は、その前後のイベントを確認できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、リスト内のイベントを見つけます。
- 2 イベント行の左にある  をクリックし、[コンテキストにイベントを表示] をクリックします。
- 3 (オプション) 追加のイベントを読み込むには、ウィンドウの端を上方または下方スクロールします。
- 4 (オプション) 強調表示されたメッセージにスクロールして戻るには、紫色のタイムスタンプをクリックします。
- 5 (オプション) フィルタを追加するには、最上にある [フィルタの追加] をクリックするか、強調表示されたイベント内部のフィールドをクリックします。
- 6 (オプション) イベントをポイントして  をクリックすると、特定のイベント タイプを追加または削除できます。

イベント傾向の分析

傾向および異常についてログ イベントを分析できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。

- 2 検索テキスト ボックスを使用し、フィルタを適用して、クエリを作成して実行します。
- 3 [イベントから時間範囲を設定] ダイアログ ボックスでドロップダウン メニューを使用して、時間範囲の期間と方向を選択します。
- 4 [イベント傾向] タブをクリックします。

vRealize Log Insight は、直前の同期間とクエリを比較し、結果を表示します。

すべてのフィルタリング ルールをクリアする

フィルタリングと検索結果をクリアして、すべてのログ イベントのリストを表示できます。

イベント リストで検索を実行すると、すべてのクエリをクエリするまで検索結果は画面に残ります。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。 `log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、すべてのフィルタを削除します。
- 2 検索テキスト ボックスにテキストが表示されたら、削除します。
- 3 [検索] ボタンをクリックします。

検索クエリの例

vRealize Log Insight の [インタラクティブ分析] タブでクエリを作成するときには、これらの例を使用できます。

重要: vRealize Log Insight は、完全な英数字、ハイフン、アンダースコアの文字をインデックス化します。

例: 昨日の 9 ~ 10 AM に ESX/ESXi hostd プロセスによって報告されたすべてのハートビート イベントのクエリを実行する

ESX/ESXi hostd プロセスによって報告されたすべてのハートビート イベントのクエリを実行するには、次の手順を実行します。

- 1 検索テキスト ボックスに **heartbeat*** と入力します。
- 2 フィルタを定義します。
 - a 最初のドロップダウン メニューから [appname] を選択します。
 - b 2 番目のドロップダウン メニューから [contains] を選択します。
 - c 値のテキスト ボックスに **hostd** と入力します。
- 3 時間範囲を定義します。
 - a [時間範囲] ドロップダウン メニューで、[カスタム] を選択します。
 - b 最初のテキストボックスに昨日の日付と 9am を入力します。

- c 2 番目のテキストボックスに昨日の日付と 10am を入力します。

4 [検索] ボタンをクリックします。

例：名前に共通の文字列があるホスト グループを検索する

複数のホストの中に、w1-stvc-205-prod3 という名前のホストと w1-stvc-206-prod5 という名前の別のホストがあるとします。

両方のホストのログをすべて検索するには、次のクエリを作成します。

- 1 1. [検索] テキスト ボックスを空のままにします。
- 2 フィルタを定義します。
 - a 最初のドロップダウン メニューで [hostname] を選択します。
 - b 演算子ドロップダウン メニューで [starts with] を選択します。
 - c 値のテキスト ボックスに **w1-stvc** と入力します。

または、[contains] 演算子を使用できます。ただし、検索値に glob を使用する必要があります。この例では、値のテキスト ボックスに **w1-stvc-*** と入力する必要があります。

3 [検索] ボタンをクリックします。

例：vCenter Server のタスク、イベント、アラームによって報告されたすべてのエラーのクエリを実行します。

vCenter Server のタスク、イベント、アラームによって報告されたすべてのエラーのクエリを実行するには、次の手順を実行します。

- 1 検索テキスト ボックスに **error** と入力します。
- 2 フィルタを定義します。
 - a 最初のドロップダウン メニューから [vc_event_type] を選択します。
 - b 2 番目のドロップダウン メニューから [exists] 演算子を選択します。
- 3 [検索] ボタンをクリックします。

例：ESX/ESXi によって報告された、1 秒以上の SCSI 遅延のクエリを実行します。

ESX/ESXi によって報告された、1 秒以上の SCSI 遅延のクエリを実行するには、次の手順を実行します。

- 1 検索テキスト ボックスに **scsi latency "performance has"** と入力します。
- 2 フィルタを定義します。
 - a 最初のドロップダウン メニューから [vmw_vob_component] を選択します。
 - b 2 番目のドロップダウン メニューから [contains] 演算子を選択します。
 - c テキスト ボックスに **scsiCorrelator** と入力します。
- 3 2 番目のフィルタを定義します。
 - a 最初のドロップダウン メニューから [vmw_latency_in_micros] を選択します。

- b 2 番目のドロップダウン メニューから [>] 演算子を選択します。
- c テキスト ボックスに **1000000** と入力します。

4 [検索] ボタンをクリックします。

正規表現の例

フィールド値のテキスト ボックスに正規表現を入力して、ログ イベントからフィールドを抽出できます。

入力する正規表現には、Java の正規表現構文を使用する必要があります。

表 1-1. 文字演算子

正規表現	説明
\	特殊文字をエスケープ
\b	語境界
\B	非語境界
\d	1 つの数字
\D	1 つの非数字
\n	改行
\r	改行文字
\s	1 つのスペース
\S	空白以外の任意の文字
\t	タブ
\w	1 つの英数字またはアンダースコア文字
\W	1 つの非英数字または非アンダースコア文字

たとえば、文字列 1234-5678 があり、次の正規表現を適用するとします

正規表現	結果
\d	1
\d+	1234
\w+	1234
\S	1234-5678

表 1-2. 数量演算子

正規表現	説明
.	改行以外の文字
*	0 個以上の文字（最長一致）
?	0 または 1 個の文字または最短一致
+	1 個以上

正規表現	説明
{<n>}	正確に <n> 回
{<n>,<m>}	<n> ~ <m> 回

たとえば、文字列 aaaaaa があり、次の正規表現を適用するとします

正規表現	結果
.	a
*	aaaaa
.*?	aaaaa
{1}	a
{1,2}	aa

表 1-3. 結合演算子

正規表現	説明
*	すべて
.*?	すべて（直前の最短一致）

たとえば、文字列 a b 3 hi d hi があり、次の正規表現を適用するとします

正規表現	結果
a.* hi	b 3 hi d
a.*?hi	b 3

表 1-4. 論理演算子

正規表現	説明
^	行頭、またはカッコ内がない文字
\$	行の最後
()	カプセル化
[]	カッコ内の 1 文字
	OR
-	範囲
\A	文字列の最初
\Z	文字列の最後

たとえば、次の正規表現を適用するとします

正規表現	結果
(hello)?	hello を含んでいるか、または含んでいない
(a b c)	a または b または c

正規表現	結果
[a-cp]	a または b または c または p
world\$	world で終わり、後に何も続かない

表 1-5. 先読み演算子

正規表現	説明
?=	正の先読み（含む）
?!=	負の先読み（含まない）

たとえば、次の正規表現を適用するとします

正規表現	結果
is (?=\w+)\w{2} primary	is FT primary? 偽
opid=(?!Wfu-1fecf8f9)\S+	Wfu-3c9bb994

表 1-6. 正規表現のその他の例

正規表現	説明
[xyz]	x、y、または z
(info warn error)	info、warn、または error
[a-z]	1 個の小文字
[^a-z]	1 個の非小文字
[a-z]+	1 個以上の小文字
[a-z]*	0 個以上の小文字
[a-z]?	0 または 1 個の小文字
[a-z]{3}	3 個だけの小文字
[d]	数字
\d+\$	1 個以上の数字の後にメッセージ終了が続く
[0-5]	0 ～ 5 の数字
\w	文字（英字、数字、またはアンダースコア）
\s	空白
\S	空白以外の任意の文字
[a-zA-Z0-9]+	1 個以上の英数字
([a-z]{2,} [0-9]{3,5})	2 個以上の文字の後に 3 ～ 5 個の数字が続く

対話形式の分析チャートを使用したログ分析

[インタラクティブ分析] ページ上部のチャートを使用すると、クエリの結果に対して視覚的な分析を実行できます。

チャートは、ログ検索クエリのグラフィカルなスナップショットを表します。チャートの下のドロップダウン メニューを使用すると、チャート タイプを変更できます。

左側の最初のドロップダウン メニューを使用すると、チャートの集約レベルを制御できます。[カウント] 関数がデフォルトで選択されています。

チャート タイプ

[インタラクティブ分析] ページでさまざまなチャート タイプを選択して、データを視覚化する方法を変更することができます。

各種チャート タイプには、異なる集約関数、時系列の使用方法、グループ別フィールドが必要です。グラフには、最新の結果が 2,000 件まで表示されます。

チャート タイプ	集約関数	時系列の要件	グループ別フィールドの要件
列	任意	時系列	該当なし
行	任意	時系列	該当なし
エリア	任意	時系列	該当なし
棒	任意	非時系列	少なくとも 1 つのフィールド
円	Count または Unique Count	非時系列	少なくとも 1 つのフィールド
バブル	任意	非時系列	2 つのフィールド
ゲージ	数	非時系列	該当なし
スカラー	数	非時系列	該当なし
表	任意	任意	該当なし

マルチファンクション チャート

マルチファンクション チャートを使用して、尺度の異なる変数を比較できます。

マルチファンクション チャートを使用すると、カテゴリの異なるデータ セットを比較したい場合に、各シリーズに対して 1 つの Y 軸または X 軸を割り当てることができます。各軸は、チャートの右側または左側に配置できます。関数を入れ替えると、Y 軸を入れ替えることができます。各関数は、Y 軸上で右から左に配置されます。

たとえば、チャネルおよびレベル別にグループ化されたタスクの平均値に、チャネルおよびレベル別にグループ化されたイベント数を追加したチャートを作成できます。

集約関数

vRealize Log Insight では、複数の集約関数を提供しています。

タイプ	フィールド	説明
カウント	イベントのみ	特定のクエリのイベント数のチャートを作成します。
Unique Count	任意のフィールド	フィールドの一意の値の数に関するチャートを作成します。
最小値	数値フィールドのみ	フィールドの最小値のチャートを作成します。
最大値	数値フィールドのみ	フィールドの最大値のチャートを作成します。



タイプ	フィールド	説明
Average	数値フィールドのみ	フィールドの平均値のチャートを作成します。
Std dev	数値フィールドのみ	フィールド値の標準偏差のチャートを作成します。
合計	数値フィールドのみ	フィールド値の合計のチャートを作成します。
Variance	数値フィールドのみ	フィールド値の差異のチャートを作成します。

クエリ結果を表示する方法を変更できます。

表示	説明
特定のフィールド値でクエリ結果をグループ化する場合	チャートの下の 2 番目のドロップダウン メニューを使用すると、時系列以外の特定のフィールドで、または時系列と特定のフィールドを併用して、クエリ結果をグループ化することができます。
1 つのフィールドに対するイベント数を表示する場合	たとえば、ホストあたりのイベント数を表示する場合は、[時系列] チェック ボックスを選択解除して、目的のフィールドのチェック ボックスを選択します。
1 つのフィールドに対する積み重ね棒チャートに、時間ごとのグループを付加して表示する場合	[時系列] チェック ボックスと目的のフィールドのチェック ボックスの両方を選択します。

チャートの操作

[インタラクティブ分析] タブではチャートの表示方法を変更することができ、カスタム ダッシュボードにチャートを追加したり、ダッシュボードチャートを変更したりすることができます。

タスク	Procedure
チャートの時間範囲を変更する	[インタラクティブ分析] タブの [検索] ボタンの左にあるドロップダウン メニューを使用して、チャートに表示されている期間を切り替えます。
チャートの粒度を変更する	[インタラクティブ分析] タブの右上にあるボタンを使用して、チャートに表示されている各点のさまざまな時間範囲を切り替えます。使用可能な範囲は、クエリで指定された時間範囲によって異なります。
[インタラクティブ分析] タブでダッシュボードチャートをロードする	[ダッシュボード] タブでチャートを見つけて [インタラクティブ分析で開く] アイコン  をクリックします。時間範囲は、ダッシュボードの現在の時間範囲に設定されます。時間範囲は必要に応じて変更することができます。
チャートをカスタム ダッシュボードに保存する	<ol style="list-style-type: none"> [インタラクティブ分析] タブの左上にある [ダッシュボードに追加] をクリックします。あるいは、[検索] ボタンの右にあるメニューで [現在のクエリをダッシュボードに追加] を選択します。 名前を入力し、ドロップダウン メニューからターゲット ダッシュボードを選択し、ウィジェット タイプを選択し、そのウィジェットの情報を追加して、[追加] をクリックします。
クエリをチャートとしてカスタム ダッシュボードに保存します。	<ol style="list-style-type: none"> [検索] ボタンの横にある [現在のクエリをダッシュボードに追加] をクリックします。 名前を入力して、ドロップダウン メニューからターゲット ダッシュボードを選択し、ウィジェット タイプが [チャート] に設定されていることを確認して、ウィジェットに関する情報を追加したら、[追加] をクリックします。
クエリをフィールド テーブルとしてカスタム ダッシュボードに保存します。	<ol style="list-style-type: none"> [検索] ボタンの横にある [現在のクエリをダッシュボードに追加] をクリックします。 名前を入力して、ドロップダウン メニューからターゲット ダッシュボードを選択し、ウィジェット タイプが [フィールド テーブル] に設定されていることを確認して、ウィジェットに関する情報を追加したら、[追加] をクリックします。
カスタム ダッシュボードからウィジェットを削除する	<ol style="list-style-type: none"> [ダッシュボード] タブで、削除するウィジェットを含むカスタム ダッシュボードを選択します。 ウィジェットの右上隅で、[他の操作] アイコン  をクリックして、[削除] を選択します。 [ウィジェットの削除] ダイアログ ボックスで、[削除] をクリックして確定します。

インタラクティブ分析チャートのタイプを変更する

チャートに表示されたクエリ結果の集約とグループを変更することで、ログ イベントをグラフィカルに分析できます。

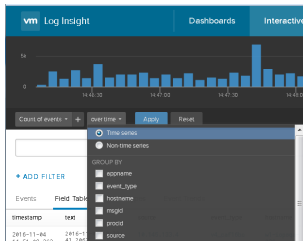
チャートの下に表示されるドロップダウン メニューの数は、選択した集約関数によって異なります。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 集約関数とグループ タイプを変更する場合は、インタラクティブ分析チャートの下のドロップダウン メニューを使用します。



- イベントを時系列で表示するには、[時系列] ボタンを選択します。
- イベントの値のみを表示する場合は、[非時系列] ボタンを選択して、少なくとも 1 つのフィールドを選択します。

- 2 [更新] をクリックします。

例：インタラクティブ分析チャートの集約とグループ

次の表では、vRealize Log Insight のチャートの集約とグループを例示します。

表 1-7. インタラクティブ分析チャートの集約とグループの例

最初のドロップダウン メニューの選択項目	2 番目のドロップダウン メニュー の選択項目	時系列の選択項目	画面に表示されるテキスト	結果
[数]	[時系列]	[時系列]	[時系列]で示すイベントの[数]	チャートには、現在のクエリのイベント数を時系列で示す棒グラフが表示されます。
[平均]	[vmw_op_latency (VMware - vSphere)]	[時系列]	[時系列]で示す [vmw_op_latency (VMware - vSphere)] の[平均]	チャートには、操作の遅延時間の平均値を時系列で示す折れ線グラフが表示されます。

最初のドロップダウンメニューの選択項目	2 番目のドロップダウンメニューの選択項目	時系列の選択項目	画面に表示されるテキスト	結果
[数]	[vmw_esx_problem] 注: vmw_esx_problem フィールドはデフォルトでは、表示されません。vmw_esx_problem をドロップダウンメニューに表示する場合は、vmw_esx_problem フィールドを抽出し、このクエリを保存する必要があります。	[非時系列]	[vmw_esx_problem] でグループ化されたイベントの[数]	チャートには、vmw_esx_problem フィールドを含んだイベント数を示す棒グラフが表示されます。
[数]	[時系列]、[vmw_esx_problem]	[時系列]	[vmw_esx_problem] でグループ化された、時系列で示すイベントの[数]	チャートには、vmw_esx_problem でグループ化された、時系列での積み重ね棒グラフが表示されます。

動的なフィールドの抽出

大量のログ イベントがある大規模環境の場合、重要なデータ フィールドを特定できないことがあります。

vRealize Log Insight では、この問題に対処するために、ランタイムのフィールド抽出機能を提供します。正規表現を指定することで、どのフィールドでもデータから動的に抽出することができます。 [正規表現の例](#)を参照してください。

注: 汎用クエリは非常に低速になることがあります。たとえば、`\(\d+\)` 正規表現を使用してフィールドを抽出しようすると、カッコ内に数値のあるすべてのログ イベントが返されます。できるだけ多くのテキスト内容がクエリに含まれていることを確認してください。たとえば、`Event for vm\(\d+\)` のように、フィールド抽出クエリを作成することをお勧めします。

抽出したフィールドを使用して、ログ イベントのリストを検索、フィルタリングしたり、[対話方式の分析] チャートでイベントを集約したりすることができます。

ワンクリック抽出を使ってフィールドを抽出する

フィールドを動的に抽出する場合、コンテキスト値を入力する代わりに、ワンクリック抽出機能を使用できます。


ワンクリック抽出を使用すると、ログ イベントで選択するフィールドに対応するすべてのコンテキスト値が入力されます。

注: ワンクリック抽出オプションは、[イベント] タブのみで使用できます。


前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。 `log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 ログ イベントのリストで、抽出するフィールドを表すテキストをハイライト表示します。
そのイベントにある一連のフィールド名の上にアクション メニューが表示されます。
- 3 [フィールドの抽出] をクリックします。
[フィールド] ペインの実行前および実行後のコンテキスト値が、ハイライト表示されたフィールドの抽出に必要なコンテキストで自動的に入力されます。
- 4 (オプション) [フィールド] ペインで、抽出された値の正規表現を変更します。
- 5 (オプション) [フィールド] ペインで、前後のコンテキストの正規表現を変更します。
- 6 (オプション)  [追加コンテキストを追加] をクリックして、その他のキーワードやフィルタを追加します。
1 つ以上のキーワードを追加し、1 つの固定フィールドをフィルタとして使用できます。
- 7 管理者ユーザーである場合、ドロップダウン メニューからフィールドにアクセスできるユーザーを選択します。

オプション	説明
すべてのユーザー	すべてのユーザーのイベントおよびフィルタ ドロップダウン メニュー内にフィールドが表示されます。
自分のみ	フィールドの作成者のイベントおよびフィルタ ドロップダウン メニュー内のみフィールドが表示されます。

- 8 (オプション) [フィールド] ペインの上部で、 に続いて [編集] をクリックして、このフィールドにメモを追加します。[メモの編集] ウィンドウでメモを追加して [OK] をクリックします。
- 9 [保存] をクリックします。

次のステップ

抽出したフィールドを使用して、ログ イベントのリストを検索、フィルタリングしたり、[インタラクティブ分析] チャートでイベントを集約したりすることができます。

保存したフィールドの定義は変更することができ、不要になった場合は削除できます。

抽出されたフィールドを変更する

抽出されたフィールドの定義を変更することができます。

チャート、クエリ、またはアラートの作成時に使用するフィールドのコピーが vRealize Log Insight によって作成されます。フィールドの定義を変更すると、その変更されたフィールドを使用するすべてのチャート、クエリ、およびアラートが更新されて新しい定義が反映されます。


通常のユーザーは自身のコンテンツのみを変更できます。管理者ユーザーは自身のコンテンツと共有コンテンツを変更できます。

コンテンツ バックのフィールドは読み取り専用です。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [フィールド] ペインの上部で、[抽出されたフィールドを管理]  をクリックし、リストから抽出されたフィールドを選択します。
- 3 値を変更して、[更新] をクリックします。

ダイアログ ボックスに、更新されたフィールドの影響を受けるコンテンツのリストが表示されます。フィールドが複数のユーザー間で共有されている場合は、影響を受けるユーザーのリストもダイアログ ボックスに表示されます。
- 4 (オプション) [フィールド] ペインの上部で、**i** に続いて [編集] をクリックして、このフィールドにメモを追加します。[メモの編集] ウィンドウでメモを追加して [OK] をクリックします。
- 5 [更新] をクリックして、変更内容を確定します。

vRealize Log Insight により、変更されたフィールドを使用するすべてのクエリ、アラート、チャートが更新されます。

抽出されたフィールドのコンテンツ パックのフィルタリング

どのコンテンツ パックからフィールドを抽出するかを指定できます。これにより不要なフィールドの抽出を回避し、より効率的に作業できます。

コンテンツ パックは、[インタラクティブ分析] ページの [コンテンツ パック] ドロップダウン メニューから選択できます。

抽出したフィールドの複製

抽出したフィールドは複製することができます。



イベントから複数のフィールドを抽出する場合は [複製] オプションを使用します。両方のフィールドが類似のコンテキストで表示されます。フィールドを抽出して保存したら、抽出したフィールドの定義を開いて、[複製] オプションを使用します。抽出したフィールドの定義は、元の抽出済みフィールドの定義と全く同じです。複製したフィールドの定義を、関心のあるイベントの別の値に一致するように変更することができます。

通常のユーザーは自身のコンテンツのみを複製できます。管理者ユーザーは自身のコンテンツと共有コンテンツを変更できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [フィールド] ペインの上部で、[抽出されたフィールドを管理]  をクリックし、リストから抽出されたフィールドを選択します。
- 3 [複製] をクリックして、フィールドのコピーを作成します。
- 4 (オプション) [フィールド] ペインで、抽出された値の正規表現を変更します。
- 5 (オプション) [フィールド] ペインで、前後のコンテキストの正規表現を変更します。
- 6 (オプション)  [追加コンテキストを追加] をクリックして、その他のキーワードやフィルタを追加します。
1 つ以上のキーワードを追加し、1 つの固定フィールドをフィルタとして使用できます。
- 7 管理者ユーザーである場合、ドロップダウン メニューからフィールドにアクセスできるユーザーを選択します。

オプション	説明
すべてのユーザー	すべてのユーザーのイベントおよびフィルタ ドロップダウン メニュー内にフィールドが表示されます。
自分のみ	フィールドの作成者のイベントおよびフィルタ ドロップダウン メニュー内のみフィールドが表示されます。

- 8 [保存] をクリックします。

次のステップ


抽出したフィールドを使用して、ログ イベントのリストを検索、フィルタリングしたり、[インタラクティブ分析] チャートでイベントを集約したりすることができます。

保存したフィールドの定義は変更することができ、不要になった場合は削除できます。

抽出されたフィールドを削除する

不要になった抽出済みフィールドを削除することができます。

ウィジェット、クエリ、またはアラートの作成時に使用するフィールドのコピーが vRealize Log Insight によって作成されます。ウィジェット、クエリ、またはアラートで使用されるフィールドを削除すると、そのフィールドを使用する各ウィジェット、クエリ、またはアラートの削除済みフィールドの一時コピーが vRealize Log Insight によって作成されます。


名前の横に [このフィールドを編集] アイコン  があるフィールドのみを削除できます。通常のユーザーは自身のコンテンツのみを削除できます。管理者ユーザーは自身のコンテンツと共有コンテンツを削除できます。

コンテンツ バックのフィールドは読み取り専用です。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [フィールド] ペインの最上部にある [抽出されたフィールドの管理]  をクリックし、リストから抽出されたフィールドにカーソルを合わせます。

- 3  をクリックします。

ダイアログボックスに、削除対象のフィールドを使用するコンテンツのリストが表示されます。管理者ユーザーの場合、フィールドが複数のユーザーによって共有されているときには、影響を受けるユーザーのリストも表示されます。

- 4 [削除] をクリックして確定します。

削除したフィールドが既存のクエリで使用されている場合は、vRealize Log Insight によってフィールドの一時コピーが作成され、削除済みフィールドを使用するクエリをロードする際にその一時コピーが表示されます。

一時フィールドを含むコンテンツをエクスポートすると、一時フィールドを避けるために、エクスポートされたコンテンツバック内にフィールドが vRealize Log Insight によって作成されます。

管理クエリの管理

クエリ結果のエクスポート、他のユーザーとのクエリの共有、既存のクエリの保存、削除、名前変更、ロードを行うことができます。クエリのスナップショットを作成し、ダッシュボードに保存できます。


vRealize Log Insight でクエリを保存する

現在のクエリと時間範囲を vRealize Log Insight で保存して後で表示することができます。保存したクエリは、[インタラクティブ分析] ページからのみロードできます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、保存するクエリを実行します。
- 2 [現在のクエリをお気に入りに追加] アイコン  をクリックします。
- 3 名前を入力して、[保存] をクリックします。

注: 保存したクエリには固定時間範囲が含まれており、更新はされません。クエリを保存することで、保存時の時間範囲内で使用可能なログメッセージのスナップショットが取得されます。

クエリは [お気に入りのクエリ] リストに追加されます。

管理者を含めたすべてのユーザーに、保存済みクエリの個別リストがあります。



vRealize Log Insight でクエリの名前を変更する

vRealize Log Insight で保存したクエリの名前を変更することができます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。 `log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [お気に入りのクエリ] アイコン  をクリックします。
- 3 名前を変更するクエリをポイントして、[この保存済みクエリを編集] アイコン  をクリックします。
- 4 新しい名前を入力して、[保存] をクリックします。

vRealize Log Insight でクエリをロードする

コンテンツ バックのクエリまたは保存したクエリをロードして、[インタラクティブ分析] タブで表示できます。


保存したクエリは、ダッシュボードの項目から分離されます。カスタム ダッシュボードには表示されません。保存したクエリを表示する場合は、ロードする必要があります。

管理者を含めたすべてのユーザーに、保存済みクエリの個別リストがあります。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。 `log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [お気に入りのクエリ] アイコン  をクリックします。
- 3 [お気に入りのクエリ] リストで、[インタラクティブ分析] タブに表示するクエリをクリックします。
[インタラクティブ分析] タブにクエリがロードされます。 クエリの時間範囲は、イベントのリストの上に表示されます。

次のステップ

クエリをダッシュボードに追加したり、チャートの粒度を変更したり、追加のフィルタリングをクエリ結果に適用したりすることができます。



vRealize Log Insight からクエリを削除する

保存したクエリを vRealize Log Insight から削除することができます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [検索] ボタンの右側にあるドロップダウン メニューで、[クエリのロード] を選択します。
- 3 [お気に入りのクエリ] アイコン  をクリックします。
- 4 [お気に入りのクエリ] リストで、削除するクエリの横にある  をクリックします。
- 5 [削除] をクリックして確定します。


現在のクエリを共有する

現在のクエリへのリンクを他のユーザーに送信できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、共有するクエリを実行します。
- 2  をクリックして、[クエリの共有] を選択します。

vRealize Log Insight は、クエリの短縮 URL を作成して表示します。URL は前回の使用から 93 日間保存され、その後削除されます。
- 3 URL をコピーして、共有先のユーザーに送信します。

現在のクエリをエクスポートする


ログ クエリの結果をエクスポートして、他のシステムと共有したり、サポート担当者に転送したりすることができます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、エクスポートするクエリを実行します。

- 2  をクリックして、[イベントの結果のエクスポート] を選択します。
- 3 クエリの保存形式を選択して、[エクスポート] をクリックします。

メニュー項目	説明
RAW イベント	結果を TXT 形式で保存する場合に選択します。
JSON	結果を JSON 形式で保存する場合に選択します。
CSV	結果を CSV 形式で保存する場合に選択します。

クエリのスナップショットの作成



現在のクエリと時間範囲のスナップショットを vRealize Log Insight で作成して、簡単に確認したり、ダッシュボードに保存したりできます。スナップショットは、[インタラクティブ分析] ページから作成できます。

スナップショットには、そのスナップショットの作成時の時間範囲内に使用可能なログ メッセージが保存されます。作成されたスナップショットをクリックすると、スナップショットを作成したときのクエリに戻ります。1 つまたは複数のスナップショットを保存する場合は、既存のダッシュボードに追加するか、新しいダッシュボードを作成します。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、スナップショットとして保存するクエリを実行します。
- 2 [スナップショット] アイコンをクリックします。
画面下部にスナップショットが表示されます。
- 3 (オプション) クエリを変更し、追加のスナップショットを作成します。
追加したスナップショットが画面下部に表示されます。
- 4 (オプション) 画面下部で  をクリックし、[すべてダッシュボードに保存] を選択します。
 - a 既存のダッシュボードを選択するか、新しいダッシュボードを作成します。
 - b [追加] をクリックします。
選択したダッシュボードまたは新しいダッシュボードにスナップショットが追加されます。
- 5 (オプション) スナップショットの [X] をクリックすると、スナップショットが削除されます。
- 6 (オプション)  をクリックして [すべて削除] を選択して、スナップショットを削除します。

vRealize Log Insight クエリ結果のトラブルシューティング

ダッシュボード ウィジェットの横または [インタラクティブ分析] ページの警告アイコンは、表示データに問題がある可能性があることを示します。

正確な結果を導き出すには vRealize Log Insight が非常に多数のログ イベントを処理する必要がある場合に、この問題が発生する可能性があります。収集されたログのごく一部が処理されず、最終結果に含まれないことがあります。処理されたログの数とクエリ結果は、クエリを処理する時点での vRealize Log Insight のロードと対象ログの数によって異なります。

group by 句を含むクエリ、非常に大量のログをカバーするクエリ、または比較的多数の結果を返すクエリはこの問題が発生する可能性があります。

ひとつの値でなく時系列の結果を生成するクエリを代わりに使用することで、この問題に対処することができます。このタイプのクエリは、クエリ処理がログの量に影響されないため、より正確な結果を生成します。

ダッシュボードの操作

vRealize Log Insight のダッシュボードは、チャート、フィールド テーブル、クエリ リスト ウィジェットの集まりです。

カスタム ダッシュボード

カスタム ダッシュボードは、vRealize Log Insight の現在のインスタンスのユーザーによって作成されます。カスタム ダッシュボードは、[マイ ダッシュボード] と [共有ダッシュボード] の 2 つのカテゴリで編成されます。[共有ダッシュボード] は、vRealize Log Insight インスタンスの全ユーザーに表示されます。

[マイ ダッシュボード] はユーザー固有です。

通常のユーザーは、[マイ ダッシュボード] セクションのダッシュボードのみを変更できます。

管理ユーザーは [マイ ダッシュボード] セクションのダッシュボード、および [共有ダッシュボード] セクションで作成したダッシュボードを変更できます。

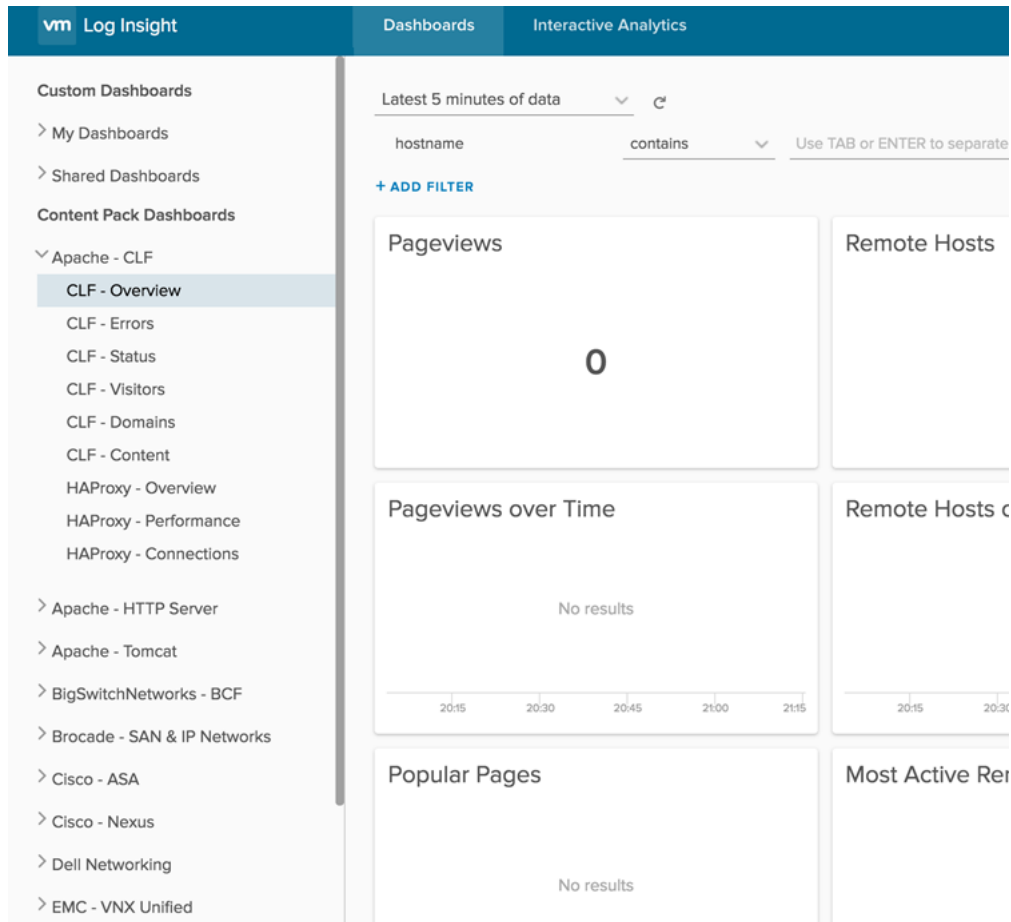
コンテンツ パックのダッシュボード

コンテンツ パックのダッシュボードは、コンテンツ パックと共にインポートされ、vRealize Log Insight インスタンスの全ユーザーに表示されます。

注: コンテンツ パック ダッシュボードは読み取り専用です。これらを削除したり、名前を変更したりすることはできません。ただし、コンテンツ パック ダッシュボードのクローンをカスタム ダッシュボードに作成することはできます。ダッシュボード全体のクローンを作成することも、各ウィジェットのクローンを作成することもできます。

vRealize Log Insight の自分のインスタンスで使用可能なダッシュボードを表示するには、vRealize Log Insight ユーザー インターフェイスの左上にある [ダッシュボード] をクリックします左側にペインが表示され、アクセスできるすべてのダッシュボードが表示されます。ダッシュボードは、カスタム ダッシュボードとコンテンツ パック ダッシュボードにグループ分けされます。各サブグループの横にある [>] をクリックすると、関連するダッシュボードを表示できます。グループ名の横の [>] をクリックすると、一度に 1 つのダッシュボード グループを開くことができます。別のグループ名の横の [>] をクリックすると、新しいグループが開かれて、前に開いていたグループが閉じられます。同時に開けるグループは 1 つだけです。

ダッシュボードの内容を表示するには、左側のリスト内のダッシュボード名をクリックします。



ダッシュボードの管理

[カスタム ダッシュボード] 領域でダッシュボードを追加、変更、削除することができます。

ダウンロードするビルド済みのコンテンツ バック ダッシュボードは変更できません。変更する場合は、ダッシュボードを [カスタム ダッシュボード] 領域にクローン作成し、クローンを変更してください。

重要: vRealize Log Insight では、ユーザーが保存またはクローン作成したダッシュボード、クエリ、アラートの名前が重複しているかどうかのチェックは実行されません。vRealize Log Insight がクエリを保存する際、表示名は一意の識別子にはなりません。したがって、複数のチャート、アラート、ダッシュボードを同じ名前で保存できます。データの取得を容易にするために、チャート、アラート、ダッシュボードを保存するときには、同じ名前を付けないでください。

カスタム ダッシュボードの操作

次の表は、カスタム ダッシュボードを作成または変更する際に使用できる製品機能を示します。

タスク	手順
カスタム ダッシュボードを作成する	[ダッシュボード] タブで [マイ ダッシュボード] を選択して、左下の [新規ダッシュボード] をクリックします。
カスタム ダッシュボードの名前を編集する	[ダッシュボード] タブでダッシュボード名をポイントしてメニュー アイコン  をクリックし、[名前の変更] を選択します。新しい名前を入力して、[保存] をクリックします。
カスタム ダッシュボードを削除する	[ダッシュボード] タブでダッシュボード名をポイントしてメニュー アイコン  をクリックし、[削除] を選択します。確認のダイアログボックスで、[削除] を選択します。
ダッシュボードをコンテンツ バックからカスタム ダッシュボードにクローン作成する	<ol style="list-style-type: none"> [ダッシュボード] タブでコンテンツバックを選択し、クローン作成するダッシュボードをポイントします。 メニュー アイコン  をクリックし、ドロップダウン メニューで [クローン作成] を選択します。 名前を入力して、[保存] をクリックします。 <p>管理者ユーザーの場合は、ダッシュボードを他のユーザーと共有するかどうかを選択できます。</p>
ダッシュボードにチャート ウィジェットを追加する	<ol style="list-style-type: none"> [インタラクティブ分析] タブの左上にある [ダッシュボードに追加] をクリックします。あるいは、[検索] ボタンの右にあるメニューで [現在のクエリをダッシュボードに追加] を選択します。 名前を入力し、ドロップダウン メニューからターゲット ダッシュボードを選択し、ウィジェット タイプを選択し、そのウィジェットの情報を追加して、[追加] をクリックします。
ダッシュボードにクエリ リスト ウィジェットを追加する	ダッシュボードにクエリ リスト ウィジェットを追加する を参照してください。
ダッシュボードのクエリ リスト ウィジェットにクエリを追加する	ダッシュボードのクエリ リスト ウィジェットにクエリを追加する を参照してください。
ダッシュボードのフィールド テーブル ウィジェットにクエリを追加する	ダッシュボードにフィールド テーブル ウィジェットを追加する を参照してください。
ダッシュボードにイベント タイプ ウィジェットを追加する	ダッシュボードにイベント タイプ ウィジェットを追加する
ダッシュボードにイベント トレンド ウィジェットを追加する	ダッシュボードにイベント トレンド ウィジェットを追加する
ダッシュボードからウィジェットを削除する	<ol style="list-style-type: none"> [ダッシュボード] タブで、削除するウィジェットを含むカスタム ダッシュボードを選択します。 ウィジェットの右上隅で、[他の操作] アイコン  をクリックして、[削除] を選択します。 [ウィジェットの削除] ダイアログ ボックスで、[削除] をクリックして確定します。

タスク	手順
すべてのウィジェットの時刻同期されているデータを表示します。	<p>デフォルトで、ウィジェット上の特定のデータ ポイントにカーソルを置くと、そのデータ ポイントの凡例ラベルを表示できます。また、すべてのダッシュボードに適用される [すべてのウィジェットの凡例を表示] 設定を有効にすると、同時刻のすべてのウィジェットの凡例ラベルを表示できます。この設定は Cookie ベースで、ブラウザ セッション間で維持されます。</p> <ol style="list-style-type: none"> 1 [ダッシュボード] タブで、ダッシュボードを選択します。 2 ダッシュボードの左上隅で、[すべてのウィジェットの凡例を表示] トグルを有効にします。
警告アイコンを表示するウィジェットのトラブルシューティングを行います。	vRealize Log Insight クエリ結果のトラブルシューティング を参照してください。


ダッシュボードにクエリ リスト ウィジェットを追加する

クエリ リスト ウィジェットを作成することで、検索クエリのリストをカスタム ダッシュボードに保存できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、ダッシュボードに追加するクエリを実行します。
- 2 [現在のクエリをダッシュボードに追加] アイコン  をクリックします。
- 3 [ダッシュボード] ドロップダウン メニューで、クエリの追加先にするダッシュボードを選択します。
- 4 [ウィジェットのタイプ] ドロップダウン メニューで、[クエリ リスト] を選択します。
- 5 [クエリ リスト] ドロップダウン メニューで、[新規クエリ リスト] を選択してリストの名前を入力し、[保存] をクリックします。
- 6 [追加] をクリックします。

クエリ リスト ウィジェットが指定のダッシュボードに表示されます。

次のステップ

作成したクエリ リスト ウィジェットにクエリを追加できます。[ダッシュボードのクエリ リスト ウィジェットにクエリを追加する](#)を参照してください。

ダッシュボードのクエリ リスト ウィジェットにクエリを追加する


クエリ リスト ウィジェットを使用すると、1 つ以上の保存済みクエリにダッシュボードから素早くアクセスできます。

カスタム クエリ リスト ウィジェットを変更して新しいクエリを追加できます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、クエリ リスト ウィジェットに追加するクエリを実行します。
- 2 [現在のクエリをダッシュボードに追加] アイコン  をクリックします。
- 3 [ダッシュボード] ドロップダウン メニューで、クエリ リスト ウィジェットを含んだダッシュボードを選択します。
- 4 [ウィジェットのタイプ] ドロップダウン メニューで、[クエリ リスト] を選択します。
- 5 [クエリ リスト] ドロップダウン メニューで、クエリを追加するウィジェットの名前を選択して、[保存] をクリックします。
- 6 [追加] をクリックします。

vRealize Log Insight により、選択したウィジェットにクエリが追加されます。

注: クエリ リスト ウィジェットでは、メッセージ クエリが使用されます。チャート ウィジェットで同じメッセージ クエリを使用していて、いずれのメッセージにも存在しないグループ別フィールドを選択すると、チャートには何の結果も表示されません。


ダッシュボードにフィールド テーブル ウィジェットを追加する

フィールド テーブル ウィジェットを使用すると、1 つ以上の保存済みフィールドにダッシュボードから素早くアクセスできます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、フィールド テーブル ウィジェットに追加するクエリを実行します。
- 2 [現在のクエリをダッシュボードに追加] アイコン  をクリックします。
- 3 [ダッシュボード] ドロップダウン メニューで、フィールド テーブルの追加先にするダッシュボードを選択します。
- 4 [ウィジェットのタイプ] ドロップダウン メニューで、[フィールド テーブル] を選択します。
- 5 フィールド テーブルに含めるフィールドを選択します。
- 6 [追加] をクリックします。

フィールド テーブル ウィジェットが指定のダッシュボードに表示されます。


ダッシュボードにイベント タイプ ウィジェットを追加する

イベント タイプ ウィジェットでは、類似したイベントと一緒にグループ化するためにマシン学習によって作成されるイベント タイプ グループへのアクセスが提供されています。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、ウィジェットに追加するクエリを実行します。
- 2 [現在のクエリをダッシュボードに追加] アイコン  をクリックします。
- 3 [ダッシュボード] ドロップダウン メニューで、ウィジェットの追加先にするダッシュボードを選択します。
- 4 [ウィジェット タイプ] ドロップダウンメニューで、[イベント タイプ] を選択します。
- 5 [追加] をクリックします。

ウィジェットが指定のダッシュボードに表示されます。


ダッシュボードにイベント トレンド ウィジェットを追加する

イベント トレンド ウィジェットでは、特定期間におけるトレンドを分析する、イベント トレンド に関する情報へのアクセスを提供しています。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブで、ウィジェットに追加するクエリを実行します。
- 2 [現在のクエリをダッシュボードに追加] アイコン  をクリックします。
- 3 [ダッシュボード] ドロップダウン メニューで、ウィジェットの追加先にするダッシュボードを選択します。
- 4 [ウィジェット タイプ] ドロップダウン メニューで、[イベント トレンド] を選択します。
- 5 [追加] をクリックします。

ウィジェットが指定のダッシュボードに表示されます。

チャートのフィールド値を使用してフィルタリングする

チャート内のフィールド値をフィルタとして、チャートを含むダッシュボード、フィールドを使用する別のダッシュボード、および [インタラクティブ分析] で使用することができます。

チャート内のフィールド値に問題がある場合は、フィールド値を入力として使用して、そのフィールドを使用する別のダッシュボードに素早くジャンプできます。他のダッシュボードでこのフィールドが使用されていない場合は、フィールド値をフィルタとして同じダッシュボード上で使用したり、[インタラクティブ分析] で実行したりすることができます。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [ダッシュボード] ドロップダウン メニューで、チャート ウィジェットを含むダッシュボードを選択します。
- 2 チャート ウィジェットで、チャート データにマウスを置き、ツールチップとして現れるフィールド値を表示します。
- 3 フィルタとして使用するフィールド値をクリックします。
[フィルタとして値を追加] メニューが表示されます。
- 4 フィールド値をフィルタとして使用する箇所を選択します。

オプション	操作
インタラクティブ分析	[インタラクティブ分析] ページが開いて、チャート クエリの結果が表示されます。ステップ 3 で選択したフィールド値がフィルタとして使用されます。
このダッシュボード	ステップ 3 で選択したフィールド値が同じダッシュボード上でフィルタとして使用されます。
他のダッシュボード	ステップ 3 で選択したフィールド値が、フィールドを含む別のダッシュボード上でフィルタとして使用されます。

コンテンツ パックの操作

コンテンツ パックには、特定の製品やログのセットに関連するダッシュボード、抽出されたフィールド、保存されたクエリ、アラートが含まれています。

システムにロードされたコンテンツ パックを表示するには、vRealize Log Insight ユーザー インターフェイスに右上にあるドロップダウン メニューから [コンテンツ パック] を選択します。

コンテンツ パックの内容を表示するには、左側のリスト内のコンテンツ パックをクリックします。

コンテンツ パック

[コンテンツ パック] カテゴリには、インポートされた一連のダッシュボード、抽出済みフィールド、クエリ、およびアラートがあります。General and VMware - vSphere コンテンツ パックはデフォルトでインポートされます。

注: コンテンツ パック ダッシュボードは読み取り専用です。これらを削除したり、名前を変更したりすることはできません。ただし、コンテンツ パック ダッシュボードのクローンをカスタム ダッシュボードに作成することはできます。ダッシュボード全体のクローンを作成することも、各ウィジェットのクローンを作成することもできます。

カスタム コンテンツ

[カスタム コンテンツ] カテゴリには、vRealize Log Insight の現在のインスタンス内に作成されたダッシュボード、抽出済みフィールド、およびクエリがあります。[マイ コンテンツ] セクションには、現在ログイン中のユーザーのカスタム コンテンツがあります。[共有コンテンツ] セクションには、vRealize Log Insight の全ユーザーが共有しているコンテンツがあります。

管理ユーザーのみが他のユーザーとコンテンツを共有できます。管理ユーザーのみが共有コンテンツを管理できます。

注: [カスタム コンテンツ] セクションからコンテンツをアンインストールすることはできません。[カスタム コンテンツ] セクションから保存済み情報を削除する場合は、ダッシュボード、クエリ、アラート、フィールドなどの個別の要素を削除する必要があります。

コンテンツ パック マーケットプレイスからのコンテンツ パックのインストール

コンテンツ パックは、vRealize Log Insight の UI から離れずに コンテンツ パック マーケットプレイスからインストールできます。

前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log-insight-host` です。`log-insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 左側の [コンテンツ パック マーケットプレイス] で、[マーケットプレイス] をクリックします。
- 3 インストールするコンテンツ パックをクリックします。
- 4 チェック ボックスをオンにして、使用許諾契約条件に同意します。
- 5 [インストール] をクリックします。

インストールが完了すると、左側の [インストール済みのコンテンツ パック] リストにコンテンツ パックが表示されます。

コンテンツ パック マーケットプレイスからインストールしたコンテンツ パックのアップグレード

コンテンツ パック マーケットプレイスからすでにインストールしているコンテンツ パックは、そのまま vRealize Log Insight でアップデートすることができます。

注: コンテンツ パックに含まれるアラートが有効な場合は、アラートがユーザー プロファイルにコピーされます。ユーザーはアラートのコピーの説明や条件を変更できます。4.0 でインスタンス化するアラートの定義、コンテンツ パックのアップデート、およびそのアラートの定義の拡張によって、改善されたコンテンツ パックと一致するようにコピーをアップデートまたは削除します。ユーザーが行った変更を保持するには、コンテンツ パックとして変更をエクスポートしてから、アップデート後にユーザー プロファイルにインポートして戻します。

前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log-insight-host` です。 *log-insight-host* は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 左側のメニューから [更新] を選択すると、アップデート可能なコンテンツ パックのリストが表示されます。
 - 1 つのコンテンツ パックをアップデートするには、そのアイコンをクリックして情報が記載されたウィンドウを開きます。[更新] をクリックするとインポートが開始されます。選択したコンテンツ パックによっては、インポートの完了後に、さらに手順を示すポップアップが表示される場合があります。表示された場合は、構成の手順に従ってアップグレードを正常に完了します。
 - アップデートを保留にしているすべてのコンテンツ パックのサイレント アップデートを行うには、[すべてを更新] をクリックします。情報が記載されたポップアップで手順を確認し、[更新] をクリックして続行します。アップグレード後、各コンテンツ パックをクリックして必要な設定を行い、インポート後のアップグレードが正しく完了していることを確認します。ユーザーが行った変更を保持するためにコンテンツ パックをエクスポートした場合は、ユーザー プロファイルにインポートして戻します。

更新したコンテンツ パックが左側の [インストール済みのコンテンツ パック] リストに表示されます。

コンテンツ パックをインポートする

コンテンツ パックをインポートして、他の vRealize Log Insight インスタンスとユーザー定義の情報を交換するか、古いコンテンツ パックを新しいバージョンでアップグレードできます。

vRealize vRealize Log Insight コンテンツ パック (VLCP) ファイルのみをインポートできます。

注: すでに存在するコンテンツパックの新しいバージョンをインポートする場合に新しいバージョンに変更済みのフィールド定義が含まれていると、そのフィールドを使用するすべてのクエリ、アラートおよびチャートが更新され、新しい定義が反映されます。

コンテンツ パックに含まれるアラートが有効な場合は、アラートがユーザー プロファイルにコピーされます。ユーザーはアラートのコピーの説明や条件を変更できます。4.0 でインスタンス化するアラートの定義、コンテンツ パックのアップデート、およびそのアラートの定義の拡張によって、改善されたコンテンツ パックと一致するようにコピーをアップデートまたは削除します。ユーザーが行った変更を保持するには、コンテンツ パックとして変更をエクスポートしてから、アップデート後にユーザー プロファイルにインポートして戻します。

<https://marketplace.vmware.com> の VMware Solutions Exchange からコンテンツ パックをダウンロードすることもできます。[コンテンツ タイプ] リストから vRealize Log Insight のコンテンツ パックを探し、コンテンツ パックとしてインストールします。

前提条件

- インストール方法として、コンテンツ パックとしてのインストールを使用する場合には、管理者の編集権限を持つユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は <https://log-insight-host> です。log-insight-host は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。
- マイ コンテンツへのインポートを使用する場合には、任意の権限レベルで vRealize Log Insight Web ユーザー インターフェイスにログインできます。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 左下隅にある [コンテンツ パックのインポート] をクリックします。
- 3 インポート方法を選択します。

オプション	説明
コンテンツ パックとしてインストール	<p>コンテンツは、vRealize Log Insight インスタンスのすべてのユーザーに対して表示される読み取り専用コンテンツ パックとしてインポートされます。</p> <p>注: コンテンツ パック ダッシュボードは読み取り専用です。これらを削除したり、名前を変更したりすることはできません。ただし、コンテンツ パック ダッシュボードのクローンをカスタム ダッシュボードに作成することはできます。ダッシュボード全体のクローンを作成することも、各ウィジェットのクローンを作成することもできます。</p>
マイ コンテンツにインポート	<p>コンテンツは、カスタム コンテンツとしてユーザー スペースにインポートされ、この操作を行っているユーザーのみに表示されます。インポートしたコンテンツは、クローン作成せずに編集できます。</p> <p>注: このモードでは、名前、作成者、アイコンといったコンテンツ パックのメタデータは表示されません。</p> <p>マイ コンテンツにインポートしたコンテンツ パックはパックとしてアンインストールできません。マイ コンテンツからコンテンツ パックを削除するには、ダッシュボード、クエリ、アラート、フィールドといった各要素を個別に削除する必要があります。</p>

通常のユーザーは、各自のユーザー スペースにのみコンテンツ パックをインポートできます。

- 4 インポートするコンテンツ パックを参照し、[開く] をクリックします。

- 5 [インポート] をクリックします。

カスタム コンテンツとしてインポートするオプションを選択した場合は、インポートするコンテンツを選択するためのダイアログ ボックスが表示されます。

- 6 (オプション) カスタム コンテンツをインポートするように選択した場合、チェックボックスを使用してインポートする項目を選択し、[インポート] を再びクリックします。

注: インポートしたクエリ、チャートおよびアラートで使用するフィールドもインポートされます。

- 7 (オプション) 一部のコンテンツ パックでは、コンテンツ パックを初めてインポートすると、インポートが完了した後にセットアップの手順を示すポップアップが表示される場合があります。それらの手順に従ってコンテンツ パックのセットアップを完了します。

- 8 (オプション) 一部のコンテンツ パックでは、コンテンツ パックをアップグレードとしてインポートすると、インポートが完了した後にアップグレードの手順を示すポップアップが表示される場合があります。それらの手順に従ってコンテンツ パックのセットアップを完了します。

インポートされたコンテンツ パックが使用できる状態になり、左側のコンテンツ パックまたはカスタム コンテンツ リストに表示されます。

注: インポートされたアラートは、デフォルトで無効になっています。[アラート クエリの有効化](#)を参照してください。

コンテンツ パックをエクスポートする


カスタム ダッシュボード、保存済みクエリ、アラート、および抽出したフィールドは、コンテンツ パックとしてエクスポートし、vRealize Log Insight インスタンス間またはコミュニティの vRealize Log Insight ユーザー間でコンテンツを共有できます。

コンテンツ パックは、vCenter Server vRealize Log Insight Content Pack (VLCP) ファイルとして保存されます。

エクスポートした、クエリ、チャート、およびアラートで使用するすべてのフィールドは、エクスポート済みのコンテンツ パックに格納されます。

一時フィールドを含むコンテンツをエクスポートすると、エクスポート中に、vRealize Log Insight によって、これらのフィールドがコンテンツ パック内に作成されます。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 エクスポートするコンテンツ パックをクリックし、コンテンツ パックの名前の横にあるドロップダウン メニュー  から [エクスポート] を選択します。

3 (オプション) コンテンツ パックに含めるコンテンツを選択します。

注: エクスポート対象として選択したダッシュボード、クエリ、またはアラートで使用されるフィールドを選択解除することはできません。

4 右のテキスト フィールドに、コンテンツ パックのメタデータを入力します。

オプション	説明
名前	コンテンツ パックを vRealize Log Insight インスタンスにインポートしたときに表示される名前を入力します。コンテンツ パックのファイル名は、[名前] テキスト ボックスの内容に由来します。推奨される形式は、 <i>Vendor- Product</i> です。たとえば、「VMware - vSphere」のようにします。
バージョン	このコンテンツ パックをアップグレードする予定がある場合は、バージョンを入力します。vRealize Log Insight では、コンテンツ パック リストにすでにあるコンテンツ パックをインストールしようすると、バージョンが表示されます。
名前空間	名前空間は、コンテンツ パックの一意な識別子です。 com.companyname.contentpackname のような、逆引き DNS 名を使用します。
作成者	オプションとして、自分の名前または会社名を入力することもできます。
Web サイト	オプションとして、コンテンツ パックと関連付けられた Web サイトへのリンクを指定することもできます。コンテンツ パックを表示できるすべてのユーザーは、この Web サイト リンクも表示できます。
説明	オプションとして、パックのコンテンツと目的に関する情報を指定することもできます。
アイコン	オプションとして、コンテンツ パック名の横に表示するアイコンを参照して指定することもできます。 注: アイコン ファイルの形式は、PNG または JPG でなければならず、サイズは 144 x 144 ピクセルに調整されます。

注: このデータは、[コンテンツ パックとしてインストール] オプションを使用してコンテンツ パックをインポートする場合にのみ表示できます。コンテンツ パックをカスタム コンテンツとしてインポートする場合はこの情報を表示できません。

5 [エクスポート] をクリックしてファイルの保存先とする場所を参照し、[保存] をクリックします。

エクスポートされた VLCP ファイルが、選択した場所にダウンロードされます。

コンテンツ パック要素に関する詳細を表示する

[コンテンツ パック] ビューから直接、ダッシュボードを構成するクエリを開いたり、フィールド、クエリ、アラートの定義を開いたりすることができます。

コンテンツ パック要素の定義をテンプレートとして、カスタム定義用に使用することができます。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 確認する要素を含んだコンテンツ パックを選択します。

3 確認する要素タイプに対応するボタンをクリックします。

たとえば、[アラート] をクリックして、コンテンツ パックに含まれるすべてのアラートを表示します。

4 要素のリストで、確認する要素の名前をクリックします。

[対話形式の] ページが開き、選択した要素に対応するクエリが表示されます。

次のステップ

コンテンツ パック要素のクエリまたは定義を変更して、カスタム コンテンツに保存できます。

コンテンツ パックをアンインストールする

コンテンツ パックをアンインストールすることができます。コンテンツ パックをアンインストールすると、カスタム ダッシュボード、保存されたクエリ、アラート、および抽出されたフィールドが削除されます。


コンテンツ パックは、vCenter Server vRealize Log InsightContent Pack (VLCP) ファイルとして保存されます。

コンテンツ パックをアンインストールすると、すべてのユーザーがそのコンテンツ パックを永久に使用できなくなります。最初にコンテンツ パックを VLCP ファイルとしてエクスポートして、バックアップを作成してください。[コンテンツ パックをエクスポートする](#)を参照してください。

前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log-insight-host` です。*log-insight-host* は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 右上のドロップダウン メニューで、[コンテンツ パック] を選択します。
- 2 アンインストールするコンテンツ パックをクリックし、コンテンツ パックの名前の横にあるドロップダウン メニュー  から [アンインストール] を選択します。
- 3 [アンインストール] をクリックします。

コンテンツ パックが [インストールしたコンテンツ パック] リストから削除されます。

コンテンツ パックの作成

Log Insight ユーザーは誰でも、私的または公的な用途のために、コンテンツ パックを作成できます。

コンテンツ パックは、vRealize Log Insight への変更できないまたは読み取り専用のプラグインで、ログ メッセージなど、特定のタイプのイベントに関する定義済みの知識を提供します。コンテンツ パックの目的は、管理者、エンジニア、監視チーム、エグゼクティブが容易に理解できる形式で、一連の特定のイベントに関する知識を提供することです。

コンテンツ パックには、製品やアプリケーションの健全性ステータスに関する情報があります。また、製品やアプリケーションがどのように機能するのか理解できるように支援します。

vRealize Log Insight のダッシュボードまたは [インタラクティブ分析] ページのいずれかを使用して、コンテンツ パックの情報を保存することができます。コンテンツ パックには以下の情報が含まれます。

- クエリ - 通常、コンテンツ パックには、ダッシュボードごとに少なくとも 3 つのクエリと 3 つのチャート ウィジェットが含まれています。したがって、全部で 9 つ以上のクエリが存在することになります
- フィールド - コンテンツ パックには、抽出されたフィールドが少なくとも 20 含まれている必要があります
- 集約
- アラート - 各コンテンツ パックには少なくとも 5 つのアラートがあります
- ダッシュボード - 各コンテンツ パックには少なくとも 3 つのダッシュボードがあります
- ダッシュボード フィルタ - [ログ イベントの検索とフィルタリング](#) を参照
- 視覚化 - [対話形式の分析チャートを使用したログ分析](#) を参照

vRealize Log Insight には、VMware - vSphere コンテンツ パックがデフォルトで付属しています。必要に応じて追加のコンテンツ パックをインポートできます。

コンテンツ パックの用語

コンテンツ パック作成ワークフローは、複数の概念と用語が基になっています。コンテンツ パックを効果的に作成して維持するには、これらの概念と用語についてよく理解する必要があります。

インスタンス

vRealize Log Insight 管理者のみがコンテンツ パック ファイルをコンテンツ パックとしてインポートできます。コンテンツ パックをコンテンツ パックとしてインポートすると、編集することはできません。

すべてのユーザーがコンテンツ パック ファイルをユーザー領域にインポートできます。コンテンツ パック ファイルをユーザー領域にインポートすると、オブジェクトが選択的に [マイ コンテンツ] にインポートされます。ユーザー領域にコンテンツ パックをインポートすると、vRealize Log Insight インスタンスでそのコンテンツ パックを編集できます。コンテンツ パックを公開または変更する場合は、エクスポートしたコンテンツ パックが必要です。

ユーザー

コンテンツ パックは、[カスタム ダッシュボード] で保存したコンテンツから部分的に作成されます。[カスタム ダッシュボード] は、ユーザー領域とも呼ばれ、より具体的には [ダッシュボード] ページの [マイ ダッシュボード] または [共有ダッシュボード] のいずれかになります。カスタム ダッシュボードのオブジェクトは選択的にエクスポートできますが、コンテンツ パックごとにクリーンなユーザー領域を確保するために、個別のユーザー エンティティが個別の各コンテンツ パックを vRealize Log Insight で作成することをお勧めします。

vRealize Log Insight でユーザーを作成する方法については、『VMware vRealize Log Insight 管理ガイド』を参照してください。

作成するコンテンツ パックごとに、vRealize Log Insight で個別のコンテンツ パック作成ユーザーを使用してください。

イベント

コンテンツ バックで製品やアプリケーションのすべての関連イベントが確実に網羅されるように、コンテンツ バックを作成する前に関連イベントを収集することが必要不可欠です。関連イベントを収集する一般的な方法の 1 つに、品質保証チームとサポート チームに問い合わせる方法があります。このようなチームは通常、共通のイベントにアクセスでき、これらのイベントに関する知識があります。

コンテンツ バックを作成しながらイベントを生成しようとする、時間がかかり、重要なイベントが抜ける結果となります。QA チームとサポート チームからイベントを入手できないときには、製品またはアプリケーション イベントが既知のもので文書化されている場合は、イベントをシミュレートして使うことが可能です。

適切なログを収集したら、vRealize Log Insight に取り込む必要があります。

作成者

コンテンツ バックの作成者は次の条件を満たす必要があります。

- VMware vRealize Log Insight の使用経験がある。
- 製品またはアプリケーションについて実用的な操作の知識がある。
- 最適化した正規表現を理解し、使用することができる。
- ログを使用して、製品またはアプリケーションの複数の問題をデバッグした経験がある。
- 多数の問題を扱うサポートのバックグラウンドがある。
- システム管理者のバックグラウンドがあり、これまでに syslog を扱ったことがある。

ワークフロー

コンテンツ バックを作成するときには、[インタラクティブ分析] ページからスタートして、エラーや警告など、特定のタイプのイベントのクエリを実行することから開始する方法をお勧めします。クエリの結果を確認し、潜在的なフィールド候補を適宜分析して抽出します。イベントのタイプ、およびイベントから入手できる有用な情報がある程度把握しながら、関連するクエリを適宜作成して保存します。迅速な対応が必要な問題があることを強く示すクエリについては、アラートを作成して保存します。クエリを保存する際、フィルタを使って結果リストから当該クエリを削除して、新たに保存したクエリの潜在的な候補になる可能性のある他のイベントを表示します。関連クエリをすべて保存したら、[ダッシュボード] ページで論理的に編成して表示します。

クエリ

vRealize Log Insight のクエリを使用すると、イベントを取得して、要約することができます。

[インタラクティブ分析] ページからクエリを作成し、保存することができます。クエリは以下のもの 1 つ以上で構成されます。

キーワード	完全、またはフルテキスト、英数字、ハイフン、または下線の一致。
glob	完全、またはフルテキスト、英数字、ハイフン、または下線の一致。
正規表現	Java 正規表現に基づく、高度な文字列パターンの一致。

フィールド操作 抽出済みのフィールドに適用されるキーワード、正規表現、およびパターン的一致。

集約 結果の 1 つ以上のサブグループに適用される関数。

vRealize Log Insight は、次のタイプのクエリをサポートしています。

- メッセージ。クエリは、キーワード、正規表現、またはフィールド操作で構成されます。
- 正規表現またはフィールド。クエリは、キーワードまたは正規表現で構成されます。
- 集約。クエリは、1 つの関数、1 つ以上のグループ、および任意の数のフィールドで構成されます。

vRealize Log Insight でカスタム アラートを定義して、どのタイプのスケジュール済みクエリからでもトリガーできます。

メッセージ クエリを作成する場合のベスト プラクティス

メッセージ クエリの作成に関する基本概念。

メッセージ クエリを入力するには、検索バーを使用するか、フィルタを入力します。

検索バーを使用して、vRealize Log Insight インスタンスのイベントに対する結果を絞り込みます。検索バーの代わりにフィルタを使用することはできますが、ほとんどの場合、同等のフィルタを使うよりも検索バーを使った方がわかりやすいクエリになります。同等のフィルタの代わりに、できるだけ検索バーを使用することをお勧めします。

フィルタでは、正規表現、フィールド、論理 OR 操作、または検索バーとフィルタ クエリの組み合わせを使用してクエリを作成できます。

検索バーとフィルタを使用してクエリを作成する場合は、次のベスト プラクティスを適用します。

- クエリが環境固有でないようにします。公開コンテンツ バックはどの環境にも対応できる必要があるため、環境固有の情報に依存しないようにする必要があります。環境固有の情報の例には、ソース、ホスト名があり、機能（機能で *local** が使用されている場合）も含まれることがあります。
- クエリを作成する場合はできるだけキーワードを使用し、キーワードが不十分な場合は glob を使用し、glob が不十分な場合は正規表現を使用します。キーワードは、リソースの使用量が最も少ないタイプのクエリです。glob は正規表現の簡易版であり、リソースの使用量が次に少ないタイプのクエリです。正規表現は、リソースを最も多く消費するタイプのクエリです。
- 正規表現またはフィールドを使用する際には、できるだけ多くキーワードを指定してください。 *this/that* など、正規表現に論理 OR が含まれている場合は、キーワードを含めないでください。vRealize Log Insight は、正規表現のオーバーヘッドを最小限に抑えるために、正規表現の前にキーワード クエリを実行するように最適化されています。

フィールド クエリ

フィールドは、構造化されていないイベントを構造化し、データのテキストおよびビジュアル表示の両方の操作を可能にする有効な手段となります。

フィールドは、集約やフィルタなどさまざまな方法で使用できるため、コンテンツ バックの最も重要な項目の 1 つになります。集約を使用すると、関数とグループ化をフィールドに適用できます。フィルタを使用すると、複数のフィールドにわたって操作を実行できます。

クエリまたは集約に適用できる可能性のあるログ メッセージの部分をすべて抽出する必要があります。フィールドは正規表現クエリのタイプに属し、複雑なパターン マッチングで役立つため、ユーザーは複雑な正規表現を知り、記憶し、学習する必要がありません。

フィールドのコンテキスト値	定義
Regex before value	可能な限り多くのキーワードを含めます。このフィールドが空か、特殊文字のみを指定している場合、Regex after value にキーワードを含める必要があります。
Regex after value	可能な限り多くのキーワードを含めます。このフィールドが空か、特殊文字のみを指定している場合、Regex before value にキーワードを含める必要があります。
名前	英数字のみを使用します。すべての文字を小文字にし、スペースの代わりにアンダースコアを使用してください。アンダースコアを使用すると、フィールドが見やすくなります。コンテンツ バック フィールドとユーザー フィールドの名前は同じにすることができ、点に留意してください。ただし、コンテンツ バック フィールドの場合、フィールド名の右にカッコで囲んだ名前空間があります。コンテンツ バック フィールドには、vmw_ のようにプリフィックスを付けて混乱を防ぎます。
キーワード検索語句	フィールドを含むイベント内に表示される 1 つまたは複数のキーワードを、スペースで区切って指定します。
フィルタ	固定フィールドや演算子を指定したり、フィールドを含むイベント内に表示される可能性のある値を指定することができます。これは、キーワードを含まないイベントに対して、vRealize Log Insight エージェントおよびタグと組み合わせて使用することが一般的です。
情報 ([i] ボタン)	フィールドの意味や返される可能性のある値を示したり、人間が理解できる情報に値をわかりやすくマッピングするなど、フィールドに関する情報を提供するために使用されます。

ベスト プラクティス

フィールドを構成する各種要素に加えて、複数のベスト プラクティスを適用します。

- 正規表現パターン用のフィールドのみを作成します。キーワード クエリを使用してクエリを実行できることができれば、またはクエリから 1 つの値のみが返される場合は、定義済みのフィールドの代わりにキーワード クエリを使用します。フィールドから 2 つの値のみが返される場合は、フィールドを抽出する代わりに、個別のクエリを作成することを検討してください。フィールドは、構造化されていないデータを構造化し、イベントの特定の部分のクエリを実行するためのものです。
- 全イベントのごく一部を返す、正規表現パターン用のフィールドのみを作成します。フィールドがほとんどのイベントに一致する場合、または大量の結果を返す場合、それらはフィールド抽出に適した候補ではありません。正規表現は大量のイベントに適用する必要がありますが、リソースを大量に使用します。可能であれば、キーワードをさらに追加することで、返される結果の数を減らし、クエリを最適化してください。
- フィールドの正規表現構文内にキーワードが含まれる場合は、そのようなキーワードを、正規表現構文なしでフィルタとして追加します。たとえば、フィールドの値またはコンテキストの正規表現構文内にキーワード (*this*/*that* など) が含まれる場合、これらのキーワードをテキスト フィルタとして追加して、**text contains this, that** のようにクエリを最適化します。
- クエリの実行前または実行後のコンテキストで、複雑な正規表現に対して 1 つまたは複数のキーワードを持つ追加コンテキストを使用することをお勧めします。
- クエリのパフォーマンスを最適化するために、すべての抽出済みフィールドに追加コンテキストを追加します。

一時フィールド

一時フィールドは、クエリの一部として存在するフィールドですが、vRealize Log Insight インスタンス内にグローバルに保存されたり、インストール済みパックの一部として保存されたりすることはありません。

vRealize Log Insight は、変更対象のフィールドに依存するクエリを自動的に更新することで、一時フィールドが作成される可能性を減らします。

注: 保存済みクエリが依存するフィールドを削除すると、そのクエリには一時フィールドが作成されます。

[インタラクティブ分析] ページで保存済みクエリを実行すると一時フィールドが表示され、保存済みクエリで使用されているフィールドの名前の右に名前空間「Temporary」が付きます。

1 つ以上のフィールドを含むクエリ vRealize Log Insight 内に保存されたクエリの場合、クエリの保存時に使用されるフィールド定義は、フィールドが変更されると変更されます。フィールドの変更には次のものがあります。

- フィールド値の変更
- 値の前の正規表現、およびフィールド値の後の正規表現の変更
- フィールド名の変更
- フィールドの削除

コンテンツ パックをエクスポートすると、vRealize Log Insight によってすべての一時フィールドがコンテンツ パック フィールドに変換されます。コンテンツ パック内に一時フィールドが表示されている場合は、一時フィールドと共にエクスポートされた以前の製品バージョンのコンテンツ パックが表示されているか、コンテンツ パックが手動で編集された可能性があります。

既存の抽出済みフィールドと同じ名前の一時フィールドがある場合、この一時フィールドの末尾に {n} が表示されます。たとえば、`product_test_field` という名前のフィールドがあった場合は、エクスポート中に `product_test_field {2}` も表示される場合があります。この動作が見られる場合は、一時フィールドが存在します。この問題に対処するには、[選択しない] オプションをエクスポート ダイアログ ボックスの下部で選択し、末尾に {n} が表示される抽出フィールドが選択されるまで、各ダッシュボードとアラートまたはそのいずれかを選択します。ダッシュボードとアラート、またはそのいずれかに移動し、各クエリを編集します。抽出されたフィールドを使用するクエリを見つけたら、末尾の {n} がいないフィールドを使用するようにフィルタまたは集約を変更してクエリを保存します。末尾が {n} のフィールドを使用しているすべてのクエリに対してこの手順を完了すると、エクスポート中にこのフィールドは表示されなくなります。

集約クエリ

vRealize Log Insight では、集約クエリを使ってイベントのビジュアル表示を操作できます。

集約クエリは、次の 2 つの属性から構成されます。

- 機能
- グループ

集約クエリには 1 つの関数および少なくとも 1 つのグループが必要です。グループはコンテンツ パックの重要な部分です。関数とグループは、グラフの表示方法に影響します。

グラフには、最新の結果が 2,000 件まで表示されます。

棒グラフ

vRealize Log Insight の [インタラクティブ分析] ページの概要グラフには、デフォルトによりイベント数が時系列で表示されます。カウント関数を時系列のグループとともに使用すると、vRealize Log Insight によって棒グラフが作成されます。

カウント関数を時系列ではなく単一のフィールド グループとともに使用すると、vRealize Log Insight によって、最大から最小の順で数を示す棒グラフが作成されます。

折れ線グラフ

カウント関数以外の関数はすべて数学関数です。数学関数には、式を適用するフィールドが必要です。フィールドと時系列のグループに数学関数を実行すると、vRealize Log Insight によって折れ線グラフが作成されます。

積み重ねグラフ

vRealize Log Insight の [インタラクティブ分析] ページの概要グラフは、デフォルトで時系列でのイベント数になっています。1 つのフィールドを時系列グループに追加すると、vRealize Log Insight によって積み重ねグラフが作成されます。

時系列のグループとフィールドを使用する場合に、カウント以外の関数を使用すると、vRealize Log Insight によって積み重ね折れ線グラフが作成されます。積み重ねグラフは、オブジェクト上の異常を見つける場合に非常に役に立ちます。

集約クエリが返す可能性のあるオブジェクトの数を基に、使用する積み重ねグラフのタイプを決定する必要があります。オブジェクトをより多く表示するには、情報の解析と表示のために、より多くのリソースが必要になります。また、色の数は決まっており、返されたオブジェクトの数によっては、オブジェクト間の区別が難しくなります。一般に、次のベスト プラクティスが適用されます。

- 各棒で返されたオブジェクト数が 10 未満の場合は、積み重ねグラフが適しています。
- 各棒で返されたオブジェクト数が 10 ～ 20 になるか、その可能性がある場合、積み重ねグラフでも問題ありません。グラフをコンテンツ バックでどのようにビジュアル表示するのかを考慮する必要があります。
- 各棒で返されたオブジェクト数が 21 以上になるか、その可能性がある場合、積み重ねグラフは不適切です。

多色グラフ

複数のフィールドと時系列を使ってグループを作成する場合は、vRealize Log Insight によって多色グラフが作成されます。グラフは、入れ替わる 2 つの色で構成されます。入れ替わる各色は新しい時間範囲を表します。多色グラフは解釈が難しい場合があるため、こうしたグラフが、コンテンツ バックに含めるほど有益かどうかを考えてください。

複数のフィールドのグループを作成する場合は、非時系列の使用を検討してください。時系列をなくすと、棒グラフがわかりやすくなります。

特定の時間範囲内で複数のフィールドが重要な意味を持つ場合は、フィールドごとにその時間範囲でのグラフを個別に作成して、複数のグラフにすることができます。作成後、コンテンツ バックのダッシュボード グループの同じ列でグラフを表示できます。

その他のグラフ

円、バブル、表など、その他の種類のグラフを利用できます。これらのグラフを使用するには、特定のクエリ タイプが必要です。グラフ用のオプションが利用可能になっている場合は、適切なクエリがすでにあります。グラフ用のオプションが利用可能になっていない場合は、目的のグラフ名をマウスでポイントします。そのグラフ タイプに必要なクエリの種類を説明する、ポップアップ メッセージが表示されます。

メッセージ クエリ

集約クエリを作成する場合、メッセージ クエリからは集約クエリに関連する結果のみが返されるようにする必要があります。そうすることで、分析が容易になり、関連するフィールドだけが結果に確実に表示されます。メッセージ クエリから集約クエリと同じ結果が返されるようにするには、集約クエリで使用される各フィールドに対して *exists* 演算子を使ってフィルタを追加する必要があります。

チャート タイプの変更

ダッシュボード上のウィジェットのチャート タイプを変更する場合は、ウィジェットの歯車アイコンをクリックして、[チャート タイプの編集] を選択します。ウィジェット タイプを変更する場合は、新しいウィジェットを保存して、古いウィジェットを削除します。

アラート

アラートを使用すると、特定のタイプのイベントが発生したときに応答がトリガーされます。

vRealize Log Insight では、2 つのタイプのアラートがサポートされます。

- 電子メール
- vRealize Operations Manager

アラートはユーザーの領域のみに保存できます。デフォルトでは、すべてのコンテンツ パックのアラートが無効になっています。有効なアラートを作成して、コンテンツ パックの一部としてエクスポートした場合、そのアラートはコンテンツ パックで無効にされます。

コンテンツ パックには電子メールおよび vRealize Operations Manager の設定は含まれません。また、コンテンツ パックにこれらの設定を追加することはできません。

しきい値

しきい値は、トリガーされたアラート数の制限値を設定します。

しきい値を有効にしたときに、コンテンツ パックのアラートが誤ってユーザーに大量送信されることのないように、しきい値がどのように動作するのかを理解しておくことが重要です。しきい値の使用を検討するときには、常に 2 つの点に留意する必要があります。

- アラートをトリガーする頻度。Log Insight では、あらかじめ頻度が定義されています。アラートは、特定のしきい値の枠内で 1 回だけトリガーされます。
- アラートの状態が発生したかどうかを確認する頻度アラートはクエリによってトリガーされます。現バージョンのアラートはクエリと同様に、リアルタイムではありません。各しきい値の枠内には、あらかじめ決定されたクエリの頻度が割り当てられています。しきい値を変更すると、クエリの時間も変更されます。

グループ

電子メール アラートを作成する際は、アラートのソースを識別するフィールド別にグループ化することが重要です。

アラートから送信される電子メールには、特定の集約クエリの結果をまとめた表が含まれます。クエリの視覚的な表現は [インタラクティブ分析] ページで確認できます。

グループ化するための一意の識別子がないと、結果が、環境内の 1 つまたは複数のシステムに関連するかどうかかわかりません。グループ化は、ソース フィールド別ではなく、ホスト名フィールド別に行う必要があります。イベントのソースを一意に識別するフィールドを追加することもできます。

ダッシュボードのベスト プラクティス

ダッシュボードはコンテンツ パックの一部です。ダッシュボードを作成するときに適用するベスト プラクティスがいくつかあります。

ダッシュボードを作成するときには、次のベスト プラクティスを適用します。

- コンテンツ パックには通常、最小 3 つのダッシュボードが含まれています。概要ダッシュボードから始めて、特定の製品やアプリケーションのイベントを簡単にまとめた情報を提供することをお勧めします。概要ダッシュボードに加えて、イベントの論理グループに基づいたダッシュボードを作成する必要があります。論理グループは製品固有またはアプリケーション固有のいずれかですが、パフォーマンス、障害、監査といった一部共通のアプローチがあります。また、ディスクやコントローラなどのコンポーネント用にダッシュボードを作成することも一般的です。コンポーネント アプローチの場合、特定のコンポーネントから結果を返すようにクエリを作成できる場合のみ効果がある点に留意することが重要です。そのようなクエリを作成できない場合は、論理アプローチをお勧めします。
- ダッシュボードに名前を付けるときには一般的なタイトルにし、コンポーネント固有の方法で使用するのではない限り、製品固有またはアプリケーション固有の名前を加えることは避けてください。たとえば、VMware - vSphere コンテンツ パックには、VMware ESX/ESXi ではなく、ESX/ESXi というダッシュボード グループがあります。
- ダッシュボードには、最小 3 つ、最大 6 つのダッシュボード ウィジェットを含める必要があります。ダッシュボード ウィジェットが 3 つ未満の場合、ダッシュボードで得られる知識量は最小限になります。また、ダッシュボードが数多くあって、その中のダッシュボード ウィジェットの数が少なすぎる場合、ユーザーはさまざまなページを切り替えなくてはならず、情報がまとまって伝わりません。

その反対に、1 つのダッシュボードに 7 つ以上のダッシュボード ウィジェットがあると、マイナスの影響が出る可能性があります。情報の量が多すぎて、混乱するかもしれません。それぞれのウィジェットは、システムに対して実行する必要のあるクエリです。そのため、ウィジェットの数が多すぎると、システム リソースが大量に消費されます。

1 つのダッシュボードに 7 つ以上のダッシュボード ウィジェットを含める場合は、情報を分けて、複数のダッシュボードを作成する必要があります。ダッシュボード ウィジェットを 1 つ以上のダッシュボードに適用できる場合は、該当する各ダッシュボード内でそのウィジェットを作成します。

ダッシュボード フィルタ

ダッシュボード フィルタは、特定のイベントにドリル ダウンするために使用できます。このフィルタは、[インタラクティブ分析] ページのフィルタと同じように機能し、各フィールドを活用してドリル ダウンします。各ダッシュボードには、少なくとも 1 つのダッシュボード フィルタが必要ですが（通常はホスト名フィールドが含まれる）、追加できるフィールドは最大 5 つです。

追加するフィールドは、特定のダッシュボード上のウィジェットの大部分によって使用されるフィールドにする必要があります。これは、そのダッシュボード フィルタを使用した場合に、ほとんどのウィジェットから結果が返されるようにするためです。たとえば、ダッシュボード フィルタに、重要度のフィールド、ユーザー フィールド、またはコンポーネント フィールドなどを含めることが考えられます。

注: ダッシュボード フィルタで使用されるフィールドと演算子は、エクスポートしたコンテンツ パックに保存されます。ダッシュボード フィルタによって使用されるすべての値は、すべての環境で汎用的に用いられるものではなく、特定の環境に固有の場合があるため、エクスポートの際に保存されません。

ダッシュボード ウィジェット

ダッシュボード ウィジェットを使用すると、情報を可視化できます。

ダッシュボードに追加できる vRealize Log Insight のウィジェットには複数のタイプがあります。以下のとおりです。

- 保存済みクエリへのリンクを持つイベントのビジュアル表示を含むチャート ウィジェット
- 保存済みクエリへのタイトル リンクを含むクエリ リスト ウィジェット
- イベントが含まれるフィールド テーブル ウィジェットであり、イベント内の各フィールドは 1 つの列を表します。
- 1 つのグループに結合された類似したイベントを含む簡易イベント タイプ テーブル ウィジェット
- クエリで検出され、発生数によって並べ替えられたイベント タイプのリストを表示する簡易イベント トレンド テーブル。これにより、クエリで最も頻繁に発生しているイベントの種類を迅速に確認できます。

チャート

ダッシュボード チャート ウィジェットには、イベントがビジュアル表示されます。チャートは棒グラフまたは折れ線グラフとして表示でき、両方とも積み重ねた形で表示できます。

チャートの表示方法は複数あります。

- チャートには多くの情報を含めることができます。1 つの行に 3 つ以上のチャート ウィジェットを含めることは避けてください。ごくまれに、3 つのウィジェットを効果的に使用することはできますが、4 つ以上は使用しないことを強くお勧めします。チャート ウィジェットが見やすいかどうかを判断する場合は、必ず vRealize Log Insight でサポートされている最小解像度、1024 x 768 ピクセルを使用してください。
- 最後の行以外の行に単一のチャート ウィジェットがある場合は、そのウィジェットを全幅にします。
- チャート ウィジェットに名前を付けるときには、理解しやすいタイトルをつけ、わかりにくいフィールド名は避けてください。たとえば、抽出されたフィールドが、`vmw_error_message` という名前だとします。チャートを Count of `vmw_error_message` という名前にせずに、Count of error messages という名前にします。

- 類似するチャートを保存して、ダッシュボード グループの同じ列に積み重ねることで、視覚的に比較することができます。例：
 - 時系列で示すイベントの平均数 X + 時系列で示すイベントの最大数 X 。異なる関数を使用されていることを前提とすると、チャートの Y 軸には異なる目盛が付いていることがあります。
 - X でグループ化された、時系列で示すイベント数 + Y でグループ化された、時系列で示すイベント数。

クエリ リスト

ダッシュボードのクエリ リスト ウィジェットには、定義済みクエリへの 1 つ以上のリンクが含まれています。

クエリ リスト ウィジェットは次の場合に使用できます。

- チャート ウィジェットにではなく、基盤となるクエリに重要な価値がある場合。
- 正規表現を使用するような複雑なクエリを保存する場合。
- ダッシュボード グループ内で、基盤となる同じクエリに対してさまざまな集約を使用する場合。

フィールド テーブル

イベントが含まれるフィールド テーブルであり、イベント内の各フィールドは 1 つの列を表します。

ダッシュボードのフィールド テーブル ウィジェットには、特定のクエリに対する最新のイベントがテーブル形式で含まれます。このテーブルの各フィールドが 1 つの列を表します。

フィールド テーブル ウィジェットは、次の目的に使用できます。

- 特定のクエリに対する最新イベントを参照する。これは、変更管理やセキュリティの目的に役立つ場合があります。
- 特定のクエリに対する目的のフィールドのみを参照する。これは、イベント出力を制限するために役立つ場合があります。

コンテンツ パックのインポート エラー

コンテンツ パックのインポート時に、警告またはエラー メッセージが表示されることがあります。

アップグレード

アップグレード メッセージを受信することがあります。これは、同じ名前空間を持つシステムに別のコンテンツ パックがインストールされていることを意味します。この場合、アップグレードして既存のコンテンツ パックを置き換えるか、アップグレード プロセスをキャンセルして既存のコンテンツ パックを維持することができます。

無効な形式

形式が無効であることを伝えるメッセージを受信することがあります。これは、VLCP ファイルが手動で編集されたか、構文エラーを含んでいることを意味します。コンテンツ パックをインポートする前に、構文エラーを修正する必要があります。

より新しいバージョン

このタイプのメッセージは、コンテンツ パックが作成され、Log Insight のより新しいバージョンのみでサポートされていることを意味します。Log Insight 1.5 以降の製品バージョンでこのメッセージが表示された場合、VLCP ファイルが手動で編集されたことを意味します。

認識されないバージョン

VLCP ファイルが手動で編集され、構文エラーが含まれている場合、このタイプのメッセージが表示されることがあります。コンテンツ パックをインポートする前に、構文エラーを修正する必要があります。

注: VLCP ファイルは手動で編集しないでください。手動で編集すると、構文エラーが見つけて修復するのが難しくなります。

コンテンツ パックの公開要件

コンテンツ パックを作成して公開するときには、コンテンツ パックが基本的な公開要件を満たしていることを確認します。

コンテンツ パックの要件と公開要件の両方を確認する必要があります。

コンテンツ パックの要件

コンテンツ パックはコンテンツ、品質、標準に関するいくつかの要件を満たす必要があります。

コンテンツの要件は次のとおりです。

- 最小 3 つのダッシュボード
- ダッシュボードあたり、最小 1 つ、理想的には 3 つ、最大 5 つのダッシュボード フィルタ
- ダッシュボードあたり最小 3 つのダッシュボード ウィジェット
- ダッシュボードあたり最大 6 つのダッシュボード ウィジェット
- 行あたり最大 3 つのダッシュボード ウィジェット
- 最小 5 つのアラート
- 最小 20 の抽出済みフィールド

コンテンツ パックの品質要件は次のとおりです。

- どのクエリにもフルテキストのキーワードを少なくとも 1 つ含め、できるだけ 3 つ以上のキーワードを含めます
- クエリは、ソース、ホスト名、または *facility** などの環境固有の属性には基づきません
- どのフィールドにもフルテキストのキーワードを少なくとも 1 つ含め、できるだけ 3 つ以上のキーワードを含めます
- フィールドは製品/アプリケーション固有であり、他の製品/アプリケーション ログの結果を返しません
- どのダッシュボード ウィジェットにも、チャートで表示する内容、その重要性を示す情報/リンクを含める必要があります

コンテンツ パックの作成基準は、次のルールに従っています。

コンテンツ パックの部分	フォーマット
コンテンツ パック名の形式	<i>Company- Product</i>
コンテンツ パックの名前空間形式（コンテンツ パックは名前空間と共にエクスポートする必要があります）	<i>Ext.Domain.Product</i>
抽出されたファイル形式	<i>Prefix_Field_Name</i> 。Prefix は、会社名または会社の略語です。

公開要件

コンテンツ パックを公開する前に、公開要件を満たしていることを確認してください。Developer Center のコンテンツ パックの発行元で、コンテンツ パックの推奨事項を確認し、VMware のレビューのためにバージョンをアップロードします。<https://developercenter.vmware.com/web/loginsight>

公開要件	説明
コンテンツ パックのファイル形式	VLCP ファイル。
イベント	コンテンツ パックの検証に必要な、適切なイベント。
概要	1 ～ 2 パラグラフで構成される、コンテンツ パックに関する概要。
ハイライト	そのコンテンツ パックのポイントを示す、ハイライト 3 件。
説明	コンテンツ パックとその価値を表す、2 ～ 3 パラグラフの説明。
技術仕様	製品のバージョンおよび構成と、Log Insight のバージョンおよび構成を含む、システムの最小要件の説明。この他に、Log Insight にログを作成し、コンテンツ パックを配置するために製品を構成する際に必要となるすべての指示も提供します。
スクリーンショット	実際のデータを含んだコンテンツ パックを示す 3 つ以上のスクリーンショット。
ビデオ（オプション）	コンテンツ パックがどのように価値をもたらすのかを例示
ホワイト ペーパー（オプション）	ログを vRealize Log Insight に転送するために製品やアプリケーションを構成する方法。

コンテンツ パックを送信する

VMware Solutions Exchange で作成したコンテンツ パックを送信します。

前提条件

- コンテンツ パックが [コンテンツ パックの公開要件](#) を満たしていることを確認します。
- <http://solutionexchange.vmware.com> にアカウントがない場合は、[登録] をクリックして、[パートナー] を選択します。パートナー登録要請フォームを入力して送信します。ログイン要求が承認されると、通知メールが届きます。

手順

- 1 <http://solutionexchange.vmware.com> に移動して、ページの右上にある [今すぐログイン] をクリックします。
- 2 ユーザー名とパスワードを入力して、[今すぐログイン] をクリックします。

3 [管理] をクリックして [ソリューションの管理] を選択し、ソリューションを追加または編集します。

4 [ソリューションの追加] をクリックして、必要な情報を入力します。

作業が失われないように、[ドラフトの保存] ボタンを頻繁に使用します。

5 [承認を得るために送信] をクリックします。

ソリューションが検証と承認のために、VMware Solution Exchange Alliance Team に送信されます。

ソリューションの承認ステータスに関する電子メールが届きます。

次のステップ

ソリューションのリストを完成させる方法については、ページ上部の [パートナー コーナー] リンクをクリックしてください。必要な情報が見つからない場合は、どのようなことでも、VSXAlliance@vmware.com にお問い合わせください。

vRealize Log Insight のアラート クエリ

スケジュールした時間間隔で特定のクエリを実行するように、vRealize Log Insight を構成できます。

クエリに一致するイベント数が設定済みのしきい値を超えると、vRealize Log Insight は vRealize Operations Manager で電子メール通知または Webhook 通知を送信し、通知イベントをトリガーできます。

使用可能なアラートのリストを表示するには、[インタラクティブ分析] ページに移動して、[検索] フィールドの横にある [Create and manage alerts...(アラートの作成および管理)] ドロップダウン メニューから [アラートの管理] を選択します。各アラートのステータスはアラート名の下に表示されます。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

vRealize Log Insight で作成するアラートのタイプ

ユーザーはアラート クエリの実行間隔を制御でき、アラート タイプの 1 つを選択することで、vRealize Log Insight からアラート通知を送信する条件を制御できます。

どの一致でもトリガーされるアラート	アラート クエリは 5 分間隔で自動的に実行されます。5 分以内に少なくとも 1 つのイベントがクエリに一致すると、通知がトリガーされます。
イベント タイプに基づくアラート	アラート クエリは 5 分間隔で自動的に実行されます。指定したイベント タイプが発生すると、通知がトリガーされます。
カスタム期間内のイベント数に基づくアラート	アラート クエリの間隔はユーザーの設定によって異なります。通知はユーザーの設定 (X 以上または未満の一致するイベントが過去 Y 分で発生したとき) に従ってトリガーされます。

このタイプのアラートがトリガーされると、重複するアラートが同じ一連のイベントに対して生成されないように、当該アラートはその期間中スヌーズされます。スヌーズ中にアラートを有効にする場合は、無効にしてから再度有効にします。

集約クエリに基づくアラート

グループの関数の値が定義する値を超えると、集約クエリ アラートは通知をトリガーします。これはチャートに表示され、チャート内の少なくとも 1 つのバーが、指定の期間内に設定済みのしきい値を超えるか下回ります。

このアラート タイプは、イベントの[数]を[時系列]で視覚化しないチャートに対して設定できます。

コンテンツ パック アラート

コンテンツ パックにはアラート クエリを含めることができます。vRealize Log Insight にデフォルトで付属する vSphere コンテンツ パック内には、複数の定義済みアラート クエリがあります。これらのアラート クエリは、ESXi ホストが syslog データの送信を停止した場合、vRealize Log Insight がイベント、タスク、アラーム データを vCenter Server から収集できなくなった場合、またはアラーム ステータスが赤に変わった場合に、アラートをトリガーできます。これらのアラート クエリをテンプレートとして使用して、環境に固有のアラートを作成することができます。

コンテンツ パック アラートはすべて、デフォルトで無効になっています。

特定のバージョンの ESXi ホストは、vRealize Log Insight の再起動時に syslog データの送信を停止することがあるため、[vCenter Server: ESX/ESXi がログを停止しました] アラートを有効にしておくことをお勧めします。このアラートは、vCenter Server イベント `esx.problem.vmsyslogd.remote.failure` を監視し、syslog フィードの送信を停止した ESXi ホストがあるかどうかを検出します。syslog の問題および解決方法の詳細については、[\[VMware ESXi 5.x host stops sending syslogs to remote server \(VMware ESXi 5.x ホストからリモート サーバへの Syslog 送信が停止される\) \(2003127\)\]](#) を参照してください。

次のフィルタをアラート クエリに追加して、新しいアラートとして保存すると、vRealize Log Insight のインスタンスにフィードの送信を停止した ESXi ホストのみを検出することができます：`[vc_remote_host (VMware - vSphere)][contains]/log-insight-hostname`。

コンテンツ パックのアラート クエリは読み取り専用です。コンテンツ パックのアラートへの変更を保存するには、アラートをカスタム コンテンツに保存する必要があります。

■ E メール通知を送信するためのアラート クエリの追加

特定のデータがログに表示されたときに E メール通知が送信されるように、vRealize Log Insight でアラート クエリを構成できます。

■ Webhook を使用したサードパーティ製品へのアラート送信について

Webhook を使用してサードパーティ製品に vRealize Log Insight ユーザー アラートを送信することができます。

■ アラート クエリの表示

作成したアラート クエリを表示して、これらのクエリの通知が有効になっているかどうかを確認できます。

■ アラート クエリの変更

アラート クエリのトリガーの変更、クエリによって送信される通知の有効化/無効化、または通知方法の変更（電子メール、Webhook、または vRealize Operations Manager への送信）を行えます。

■ アラート クエリの有効化

アラート クエリを無効にすると、vRealize Log Insight によって E メール通知または Webhook 通知が送信されず、vRealize Operations Manager 通知イベントがトリガーされません。

■ アラート クエリの削除

不要になったアラート クエリは削除することができます。


E メール通知を送信するためのアラート クエリの追加

特定のデータがログに表示されたときに E メール通知が送信されるように、vRealize Log Insight でアラート クエリを構成できます。

前提条件

- vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。
- E メール通知が有効になるように SMTP が管理者によって構成されていることを確認します。「[SMTP サーバを Log Insight 用に構成する](#)」を参照してください。

手順

- 1 [インタラクティブ分析] タブで、通知を送信するクエリを実行します。
- 2 [検索] ボタンの右側の [アラートを作成または管理] メニューから、 をクリックして [クエリからアラートを作成] を選択します。
- 3 [アラートの追加] ダイアログ ボックスにアラート名を入力して、アラートをトリガーするイベントについて短くて分かりやすい説明を入力します。

アラート名と説明は、vRealize Log Insight が送信する E メールに含まれます。
- 4 [E メール] チェック ボックスを選択して、vRealize Log Insight から通知を送信するメール アドレスを入力します。

複数のアドレスを入力する場合は、コンマで区切ります。
- 5 アラートのしきい値を設定します。

アラート タイプ	選択
すべての一致	[すべての一致する項目] オプションを選択します。 クエリは 5 分おきに実行されます。
イベント タイプに基づくアラート	[新しいイベント タイプが以下の直近の期間に最初に発生したとき] <期間> オプションを選択して、ドロップ ダウン メニューから時間を選択します。 クエリは 5 分おきに実行されます。

アラート タイプ	選択
ある期間内のイベント数に基づくアラート	3 番目のオプションを選択し、ドロップダウン メニューを使用してパラメータを設定します。クエリはドロップダウン メニューの選択内容に基づいて実行されます。
チャートの値に基づくアラート	4 番目のオプションを選択し、ドロップダウン メニューを使用してパラメータを構成します。 注: このアラート タイプを使用できるのは、少なくとも 1 つのフィールドに従ってイベントをグループ化するように選択した場合のみです。時系列のみを視覚化するチャートの場合は、このアラート タイプを作成できません。 クエリは 2 番目のドロップダウン メニューの選択内容に基づいて実行されます。

プレビュー チャート内のオレンジ色の線は、現在のしきい値を示します。

6 [保存] をクリックします。

次のステップ

保存されたアラートを有効化、無効化、または削除できるようになります。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

Webhook を使用したサードパーティ製品へのアラート送信について

Webhook を使用してサードパーティ製品に vRealize Log Insight ユーザー アラートを送信することができます。

vRealize Log Insight は、Webhook を使用して HTTP POST 経由で他のアプリケーションにアラートを送信します。vRealize Log Insight は、Webhook を独自のフォーマットで送信しますが、サードパーティのソリューションは、受信する Webhook が専用のフォーマットであると想定しています。vRealize Log Insight Webhook で送信される情報を使用するには、サードパーティ アプリケーションが vRealize Log Insight のフォーマットをネイティブでサポートするか、vRealize Log Insight のフォーマットとサードパーティによって使用されるフォーマットの間に shim を使用してマッピングを作成する必要があります。shim は、vRealize Log Insight のフォーマットを別のフォーマットに変換またはマップします。

メッセージ クエリにより作成されるアラート、集約クエリにより作成されるアラート、およびシステム通知には、それぞれ専用の Webhook フォーマットがあります。

HTTP 基本認証がサポートされています。認証情報は、`{{https://username:password@hostname/path}}` の形式で URL に組み込みます。

vRealize Log Insight Webhook の実装により、リモート サーバに対して送信 HTTP 要求が実行されます。サーバは「成功」または「失敗」のいずれかを報告します。vRealize Log Insight は失敗した要求を再試行します。すべての HTTP/2xx ステータス コード応答は「成功」として扱われ、タイムアウトおよび接続拒否を含むその他のすべての応答は「失敗」として扱われて後で再試行されます。

システム通知を作成するには vRealize Log Insight 管理者である必要があります。

Webhook 通知を送信するためのアラート クエリの追加


特定のデータがログに表示されたときに Webhook 通知がリモート Web サーバに送信されるように、vRealize Log Insight でアラート クエリを構成できます。Webhook は、HTTP POST 経由でイベント通知を行います。

注: サーバは「成功」または「失敗」のいずれかを報告します。失敗の場合、vRealize Log Insight は再試行します。vRealize Log Insight はすべての HTTP/2xx ステータス コード応答を「成功」として扱います。タイムアウトおよび接続拒否を含むその他のすべての応答は「失敗」として扱われて後で再試行されます。

前提条件

- vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。
- Web サーバが、Webhook 通知を受け取るように構成されていることを確認します。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [検索] ボタンの右側の [アラートを作成または管理] メニューから、 をクリックして [クエリからアラートを作成] を選択します。
- 3 [アラートの追加] ダイアログ ボックスにアラート名を入力して、アラートをトリガーするイベントについて短くて分かりやすい説明を入力します。
アラート名と説明は、vRealize Log Insight が送信する通知に含まれます。
- 4 [Webhook] チェックボックスを選択して、vRealize Log Insight から通知を送信する URL を入力します。
- 5 アラートのしきい値を設定します。

アラート タイプ	選択
すべての一致	[すべての一致する項目] オプションを選択します。 クエリは 5 分おきに実行されます。
イベント タイプに基づくアラート	[新しいイベント タイプが以下の直近の期間に最初に発生したとき] <期間> オプションを選択して、ドロップダウン メニューから時間を選択します。 クエリは 5 分おきに実行されます。
ある期間内のイベント数に基づくアラート	3 番目のオプションを選択し、ドロップダウン メニューを使用してパラメータを設定します。 クエリはドロップダウン メニューの選択内容に基づいて実行されます。
チャートの値に基づくアラート	4 番目のオプションを選択し、ドロップダウン メニューを使用してパラメータを構成します。 注: このアラート タイプを使用できるのは、少なくとも 1 つのフィールドに従ってイベントをグループ化するように選択した場合のみです。時系列のみを視覚化するチャートの場合は、このアラート タイプを作成できません。 クエリは 2 番目のドロップダウン メニューの選択内容に基づいて実行されます。

プレビュー チャート内のオレンジ色の線は、現在のしきい値を示します。

- 6 [保存] をクリックします。

次のステップ

保存されたアラートを有効化、無効化、または削除できるようになります。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

vRealize Log Insight アラートの変換 shim の記述について

shim は、さまざまな Webhook フォーマットをマップするために使用されます。

vRealize Log Insight は Webhook を独自のフォーマットで送信し、サードパーティのソリューションは受信する Webhook が自分独自のフォーマットであると期待します。これは、サードパーティ ソリューションが vRealize Log Insight のフォーマットをネイティブでサポートするか、vRealize Log Insight とサードパーティ ソリューションの間に vRealize Log Insight のフォーマットをサードパーティのフォーマットに変換するための shim が必要になることを意味します。

以下の図は、ユーザー アラート クエリ、およびクエリに対して生成される Webhook を示します。この情報を使用して、サポート用の shim に必要なマッピングについてよりよく理解することができます。

図 1-1. ユーザー定義のアラート クエリ

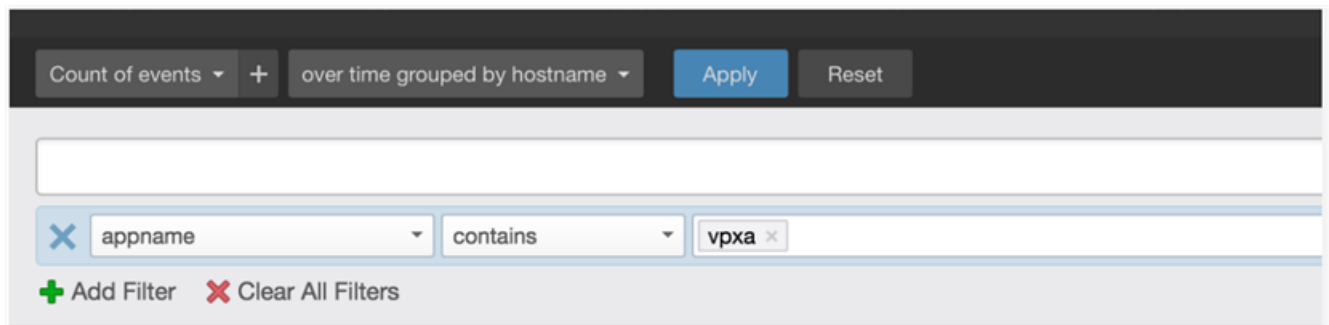


図 1-2. ユーザー アラート集約クエリのための Webhook 出力

```
{
  "AlertType":1,
  "AlertName":"ESXi Vpxa Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"2016-06-24T15:42:42.055Z esx01 Vpxa: [4845FB90 verbose 'VpxaHalCnxHostagent'
opID=WFU-dcfc2d3a] [WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"hostname",
          "content":"esx01"
        },
        {
```

```

        "name": "appname",
        "content": "vpxa"
    }
]
},
{
    "text": "2016-06-24T15:42:42.055Z esx02 Vpxa: [4845FB90 verbose 'vpxavpxaInvtVm' opID=WFU-
dcfc2d3a] [VpxaInvtVmChangeListener] Guest DiskInfo Changed",
    "timestamp": 1451940561008,
    "fields": [
        {
            "name": "hostname",
            "content": "esx02"
        },
        {
            "name": "appname",
            "content": "vpxa"
        }
    ]
}
],
"HasMoreResults": false,
"Url": "https://10.11.12.13/s/8pgzq6",
"EditUrl": "https://10.11.12.13/s/56monr",
"Info": "This is an alert for all the 'ESXi Vpxa' messages",
"NumHits": 2
}

```

ユーザー アラート メッセージ クエリのための Webhook フォーマット

vRealize Log Insight Webhook によって使用されるフォーマットは、作成されるクエリのタイプに依存します。システム通知、ユーザー アラート メッセージ クエリ、および集約ユーザー クエリから生成されたアラートにはそれぞれ異なる Webhook フォーマットがあります。

ユーザー アラート メッセージ クエリによって生成されたアラートをサードパーティ プログラムに送信する場合は、vRealize Log Insight 情報がサードパーティ プログラムのフォーマットによって理解できるように shim を記述する必要があります。

ユーザー アラート メッセージ クエリの Webhook フォーマット

次の例は、ユーザー アラート メッセージ クエリの vRealize Log Insight Webhook フォーマットを示します。

```

{
    "AlertType": 1,
    "AlertName": "Hello World Alert",
    "SearchPeriod": 300000,
    "HitCount": 0.0,
    "HitOperator": 2,
    "messages": [
        {
            "text": "hello world 1",
            "timestamp": 1451940578545,
            "fields": [
                {
                    "name": "Field_1",

```

```

        "content": "Content 1"
      },
      {
        "name": "Field_2",
        "content": "Content 2"
      }
    ]
  },
  {
    "text": "hello world 2",
    "timestamp": 1451940561008,
    "fields": [
      {
        "name": "Field_1",
        "content": "Content 1_2"
      },
      {
        "name": "Field_2",
        "content": "Content 2_2"
      }
    ]
  }
],
"HasMoreResults": false,
"Url": "https://10.11.12.13/s/8pgzq6",
"EditUrl": "https://10.11.12.13/s/56monr",
"Info": "This is an alert for all the 'Hello World' messages",
"NumHits": 2
}

```

ユーザー アラート集約クエリのための Webhook フォーマット

vRealize Log Insight Webhook によって使用されるフォーマットは、作成されるクエリのタイプに依存します。システム通知、ユーザー アラート メッセージ クエリ、および集約ユーザー クエリから生成されたアラートにはそれぞれ異なる Webhook フォーマットがあります。

サードパーティ プログラムにシステム通知を送信する場合は、vRealize Log Insight 情報がサードパーティ プログラムのフォーマットによって理解できるように shim を記述する必要があります。

ユーザー アラート集約クエリのための Webhook フォーマット

```

{
  "AlertType": 2,
  "AlertName": "field_1 aggregated alert",
  "SearchPeriod": 300000,
  "HitCount": 2.0,
  "HitOperator": 2,
  "messages": [
    {
      "fields": [
        {
          "name": "Field_1",
          "content": "Content 1"
        }
      ]
    }
  ]
}

```

```

    ]
  }
],
"HasMoreResults":false,
"Url":"https://10.11.12.13/s/r25g3s",
"EditUrl":"https://10.11.12.13/s/n3gsed",
"Info":null,
"NumHits":1
}

```

アラート クエリの表示

作成したアラート クエリを表示して、これらのクエリの通知が有効になっているかどうかを確認できます。

ユーザーとして作成したアラートを表示および管理するには、[ユーザー アラート] ウィンドウを開始点として使用します。このウィンドウから、アラートのアクティビティの監視、アラート履歴の表示、およびアラートの管理を実行できます。次のタスクを実行することができます。

- すべてのアラートまたは個別のアラートを有効または無効にする
- アラートをアラート名、所有者名、またはコンテンツ パックで並べ替える
- アラートのパラメータを変更する
- アラートを削除する

画面上の各アイコンの詳細については、ツールチップのヘルプを参照してください。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

図 1-3. ユーザー アラート


Name	Enabled	Owner	Avg Run	Frequency	Dally Run	Last Hit	Last Run
test_		admin	84ms	288/day	24s	1mo 11d ago	9d 6h ago

最初のヒットが発生するまで、[前回のヒット] 列の値は never のままです。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 左側のメニューの [管理] セクションで、[ユーザー アラート] をクリックします。

アラート クエリすべてのリストが表示されます。アラート通知のステータスがアラート名の下に表示されます。

次のステップ

リストのアラート クエリをクリックしてパラメータを変更したり、不要になったクエリを削除したりすることができます。

コンテンツ パックのアラート クエリは読み取り専用です。コンテンツ パックのアラートへの変更を保存するには、アラートをカスタム コンテンツに保存する必要があります。

アラート クエリの変更

アラート クエリのトリガーの変更、クエリによって送信される通知の有効化/無効化、または通知方法の変更（電子メール、Webhook、または vRealize Operations Manager への送信）を行えます。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。


コンテンツ パックのアラート クエリは読み取り専用です。コンテンツ パックのアラートへの変更を保存するには、アラートをカスタム コンテンツに保存する必要があります。

変更を 1 つまたは複数のアラートに同時に適用できます。

前提条件

- vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。
- E メール通知が有効になるように SMTP が管理者によって構成されていることを確認します。[「SMTP サーバを Log Insight 用に構成する」](#) を参照してください。
- アラートの統合が有効になるように vRealize Log Insight と vRealize Operations Manager 間の接続が管理者によって構成されていることを確認します。[「vRealize Operations Manager に通知イベントを送信する Log Insight の構成」](#) を参照してください。
- Webhook を使用している場合は、Web サーバが、Webhook 通知を受け取るように構成されていることを確認します。

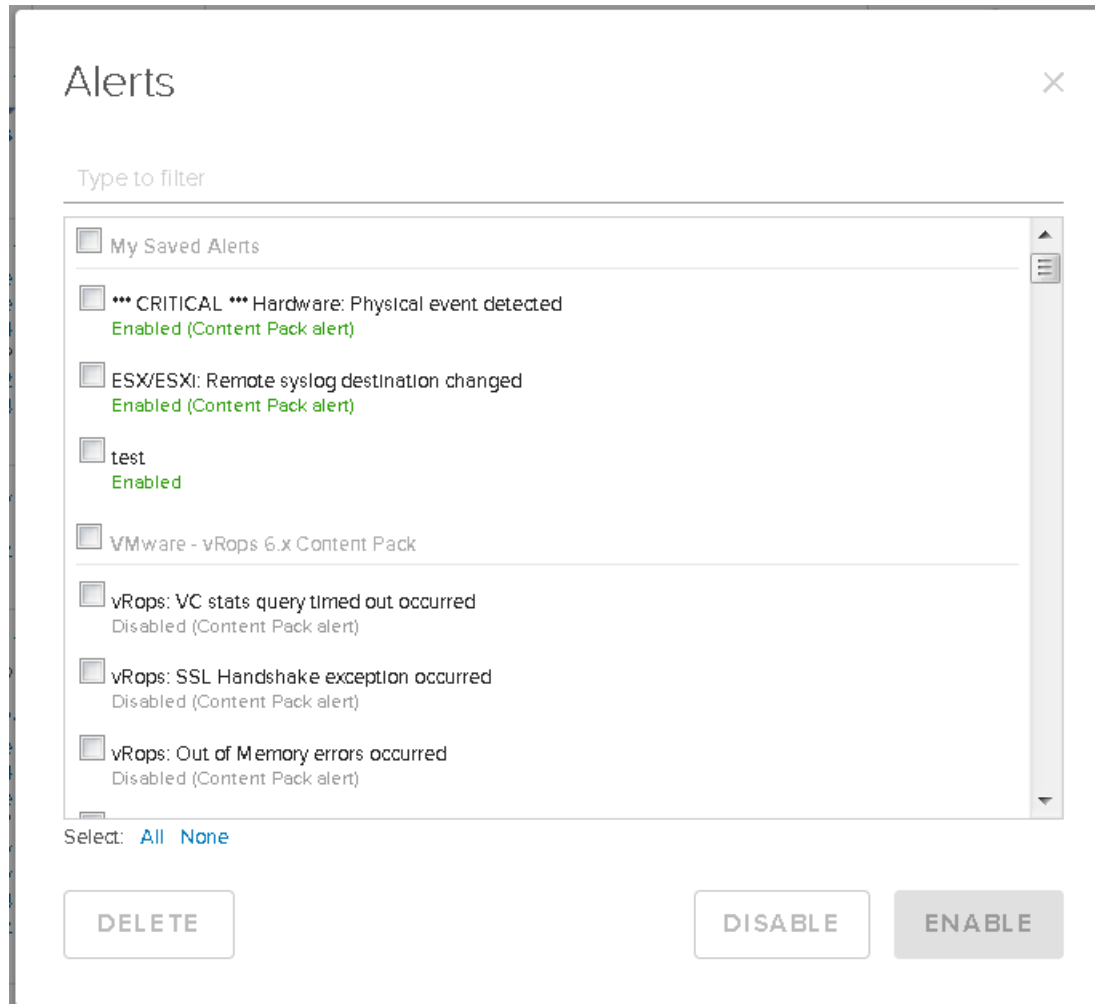
手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [検索] ボタンの右側の [アラートを作成または管理] メニューから、 をクリックして [アラートの管理] を選択します。

- 3 [アラート] リストで、変更するアラート クエリを 1 つまたは複数選択して、必要に応じてクエリのパラメータを変更します。

文字列をフィルタとして入力することで、クエリを検索できます。クエリには、有効か無効かを示すラベルと、コンテンツ パックのクエリかどうかを示すラベルが付いています。

注: すべての通知オプションを選択解除すると、アラート クエリは無効になります。



- 4 変更内容を保存します。

オプション	説明
保存	自分のアラートを変更するときにこのボタンが表示されます。
マイ アラートに保存	共有アラートまたはコンテンツ パックのアラートを変更するときに、このボタンが表示されます。元のアラートは変更されませんが、アラートのコピーをカスタム コンテンツに保存します。

アラート クエリの有効化

アラート クエリを無効にすると、vRealize Log Insight によって E メール通知または Webhook 通知が送信されず、vRealize Operations Manager 通知イベントがトリガーされません。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

次の条件下では、アラート クエリが無効になります。


- [アラートの編集] ダイアログ ボックスですべての通知オプションを無効にした場合
- アラートがコンテンツ パックの一部である場合

コンテンツ パックのアラート クエリは読み取り専用です。コンテンツ パックのアラートへの変更を保存するには、アラートをカスタム コンテンツに保存する必要があります。

前提条件

- vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。
- E メール通知が有効になるように SMTP が管理者によって構成されていることを確認します。「[SMTP サーバを Log Insight 用に構成する](#)」を参照してください。
- アラートの統合が有効になるように vRealize Log Insight と vRealize Operations Manager 間の接続が管理者によって構成されていることを確認します。「[vRealize Operations Manager に通知イベントを送信する Log Insight の構成](#)」を参照してください。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [検索] ボタンの右側の [アラートを作成または管理] メニューから、 をクリックして [アラートの管理] を選択します。
- 3 [アラート] リストで、有効にするアラート クエリを 1 つまたは複数クリックします。
- 4 有効にする通知オプションを選択して、必要なパラメータを入力します。

オプション	説明
E メール	少なくとも 1 つのメール アドレスをテキスト ボックスに入力します。複数のアドレスを入力する場合は、コンマで区切ります。
Webhook	vRealize Log Insight で通知を送信する URL を入力します。
vRealize Operations Manager に送信	通知イベントに関連付ける vRealize Operations Manager リソースを選択して、イベントの重大度レベルを選択します。

5 変更内容を保存します。

オプション	説明
保存	自分のアラートを変更するときにこのボタンが表示されます。
マイ アラートに保存	共有アラートまたはコンテンツ パックのアラートを変更するときに、このボタンが表示されます。元のアラートは変更されませんが、アラートのコピーをカスタム コンテンツに保存します。

アラート クエリによってアラート基準に一致する結果が返されると、vRealize Log Insight は構成に従って通知を送信します。

例：VMware - vSphere コンテンツ パックからのアラートを有効にする

VMware - vSphere コンテンツ パックには、[vCenter Server: ESX/ESXi がログを停止しました] アラートなど、複数の定義済みアラート クエリが含まれています。

特定のバージョンの ESXi ホストは、vRealize Log Insight の再起動時に syslog データの送信を停止することがあるため、[vCenter Server: ESX/ESXi がログを停止しました] アラートを有効にしておくことをお勧めします。このアラートは、vCenter Server イベント `esx.problem.vmsyslogd.remote.failure` を監視し、syslog フィードを停止した ESXi ホストがあれば検出します。

- 1 [インタラクティブ分析] タブの [検索] ボタンの右側にあるドロップダウン メニューを展開して、[アラートの管理] を選択します。
- 2 VMware - vSphere コンテンツ パックの下の [vCenter Server: ESX/ESXi がログを停止しました] をクリックします。
- 3 E メール通知、Webhook 通知、または vRealize Operations Manager の通知イベントを有効にします。
- 4 [マイ アラートに保存] をクリックします。

vRealize Log Insight の自分のインスタンスへのフィードの送信を停止した ESXi ホストのみを検出するには、フィルタ `[vc_remote_host (VMware - vSphere)][contains] <log-insight-hostname>` をアラート クエリに追加して、この新しいクエリを自分のアラートに保存します。

Syslog の問題および解決方法の詳細については、<https://kb.vmware.com/kb/2003127> でナレッジベースの記事「VMware ESXi 5.x host stops sending syslogs to remote server (KB2003127)」を参照してください。

アラート クエリの削除



不要になったアラート クエリは削除することができます。

注: アラート クエリはユーザー固有です。ユーザーは自分のアラートのみを管理できます。その他のユーザー アラートを管理するには、スーパー管理者ロールが割り当てられている必要があります。

前提条件

vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。URL 形式は `https://log_insight-host` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

手順

- 1 [インタラクティブ分析] タブに移動します。
- 2 [検索] ボタンの右側のメニューから、 をクリックして [アラートの管理] を選択します。
- 3 削除するアラートを 1 つまたは複数選択して、[削除] または削除アイコン  をクリックします。
- 4 [アラートの削除] ダイアログ ボックスで [削除] を選択して、アクションを確定します。