アラート
Alerts

本文の内容は、Alertsのドキュメント(https://docs.sysdig.com/en/alerts.html)を元に日本語に翻訳・再構成した内容となっております。

アラート

AlertはSysdig モニターの応答コンポーネントです。注意が必要なイベント/問題が発生すると、アラートによって通知されます。イベントと問題は、Sysdigモニターによって収集されたメトリクス値の変化に基づいて識別されます。アラートモジュールには、すぐに使用できるアラートと、必要に応じてアラートを作成および編集するためのウィザードが表示されます。

Sysdig Alertについて

Sysdig モニターは、設定した特定の条件またはイベントに基づいて通知を生成できます。アラート機能を使用すると、インフラストラクチャーを監視し、問題が発生したとき、または定義したアラート条件で問題が発生する前であっても、問題を見つけることができます。 Sysdigモニターでは、メトリクスはアラートの中心的な設定アーティファクトとして機能します。メトリクスは、1つ以上の条件またはイベントを、条件が満たされたとき、またはイベントが発生したときに実行する測定に結び付けます。アラートは、エクスプローラー、ダッシュボード、イベント、OverviewなどのSysdigモジュール全体で機能します。

アラートのタイプ

Sysdigモニターで使用可能なアラートのタイプ：

- ダウンタイム：ホスト、コンテナ、プロセスなどの任意のタイプのエンティティを監視し、エンティティがダウンしたときにアラートを出します。
- メトリクス：時系列のメトリクスを監視し、ユーザー定義のしきい値に違反していないか警告します。
- イベント：特定のイベントの発生を監視し、発生の総数がしきい値に違反した場合に警告します。コンテナ、オーケストレーション、および再起動や不正アクセスなどのサービスイベントに関するアラートに役立ちます。
- 異常検出：過去の動作に基づいてホストを監視し、予想されるパターンから逸脱した場合に警告します。
- グループ外れ値：ホストのグループを監視し、他のホストとは異なる動作をするときに通知されます。グループ外れ値アラートはホストでのみサポートされています。
- アウトオブボックス：Sysdig モニターは、デフォルトで一連のアラートを提供します。そのまま使用するか、テンプレートとして使用して独自のテンプレートを作成します。
- Sysdig API：SysdigのPythonクライアントを使用して、アラートを作成、リスト、削除、更新、および復元します。例を参照してください。

アラート作成のガイドライン

ステップ	説明
監視対象を決定する	アラートする問題のタイプを決定します。 問題のタイプを選択するには、アラートタイプを参照してください。
監視方法を定義する	違反をトリガーする動作を正確に指定します。 たとえば、Marathonアプリは、Productionという名前のKubernetesクラスターで10分間ダウンしています。
監視する場所を決定する	環境を絞り込み、微調整された結果を受け取ります。 スコープを使用して、注意して監視するエンティティを選択します。 問題にコンテキストを与えるために追加のセグメント（エンティティ）を指定します。 たとえば、Kubernetesクラスタを指定することに加えて、ネームスペースとデプロイメントを追加してスコープを調整します。
通知するタイミングを定義する	アラート条件を評価するためのしきい値と時間枠を定義します。 Single Alertはスコープ全体に対してアラートを発しますが、複数のアラートは、いずれかまたはすべてのセグメントが一度にしきい値に違反すると発動します。 Multiple Alertsには、場所を一意に識別するために指定したすべてのセグメントが含まれているため、問題が発生した場所を完全に把握できます。 セグメントの数が多いほど、影響を受けるエンティティを一意に識別しやすくなります。 複数のアラートの良い例は、都市へのアラートです。 たとえば、サンフランシスコで複数のアラートを作成すると、その一部である国が米国であり、大陸が北米であるなどの情報を含むアラートがトリガーされます。 Triggerを使用すると、通知の作成方法をコントロールできます。たとえば、すべての違反について通知を受け取りたい場合や、一連の連続した違反について1つの通知のみを受け取りたい場合があります。
通知の送信方法を決定する	Alertは、電子メール、モバイルプッシュ通知、OpsGenie、Slackなど、カスタマイズ可能な通知チャネルをサポートしています。サポートされているサービスを確認するには、通知チャネルの設定を参照してください。

アラートを作成するには、次の手順に従います。

1. アラートタイプを選択します。
2. アラートパラメータを設定します。

3. アラート通知に使用する通知チャネルを構成します。

注意

Sysdigは古いメトリクスを廃止する場合があります。 これらのメトリクスを使用するアラートは変更または無効化されませんが、更新されなくなります。 ヒューリスティックおよび非推奨のメトリクスを参照してください。

アラートを設定する

アラートウィザードを使用して、アラートを作成または編集します。

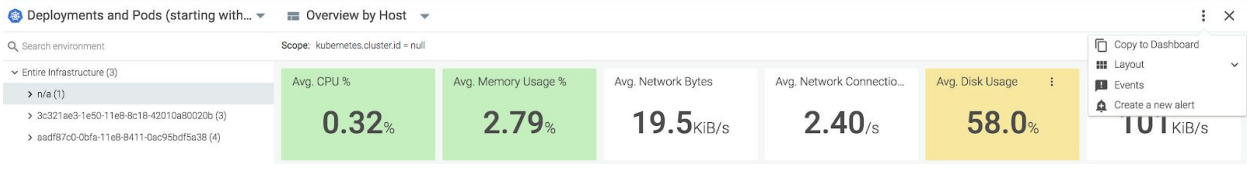
アラートウィザードを開く

アラートウィザードにアクセスするには、いくつかの方法があります。

エクスプローラーテーブルから

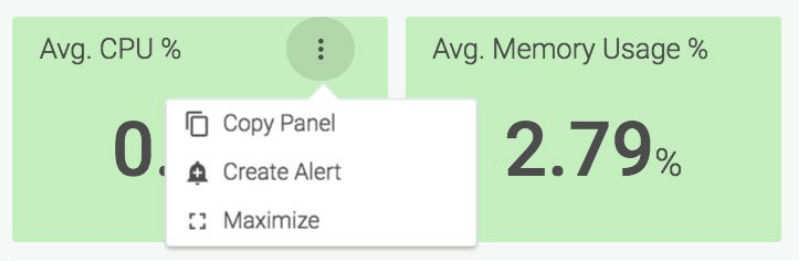
- エンティティの横にある`Alert`（ベル）アイコンを選択します。

- テーブルの[`More Options`]（3つのドット）アイコンをクリックし、[`Create a New Alert:`]を選択します。



ダッシュボードパネルから

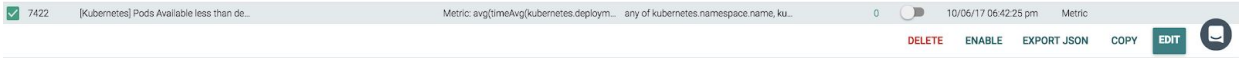
- パネルの[`More Options`]（3つのドット）アイコンをクリックし、[`Create Alert`]を選択します。



アラートモジュールから

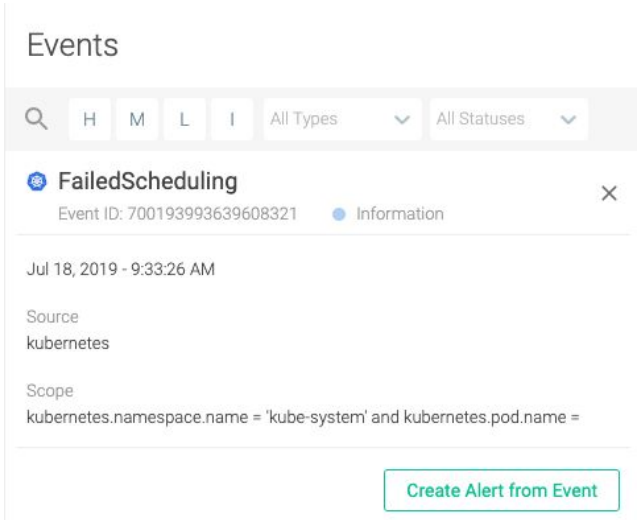
- [`Add Alert`]ボタンをクリックします。

- 既存のアラートを選択し（直接クリックするか、アラートの横にあるチェックボックスを選択）、[**`Edit`**]ボタンをクリックします。



Overviewから（ベータ版）

[Overview]画面の[イベント]パネルからカスタムイベントまたはインフラストラクチャタイプのイベントを選択します。イベントの説明画面で、[`Create Alert from Event`]をクリックします。



アラートを作成する

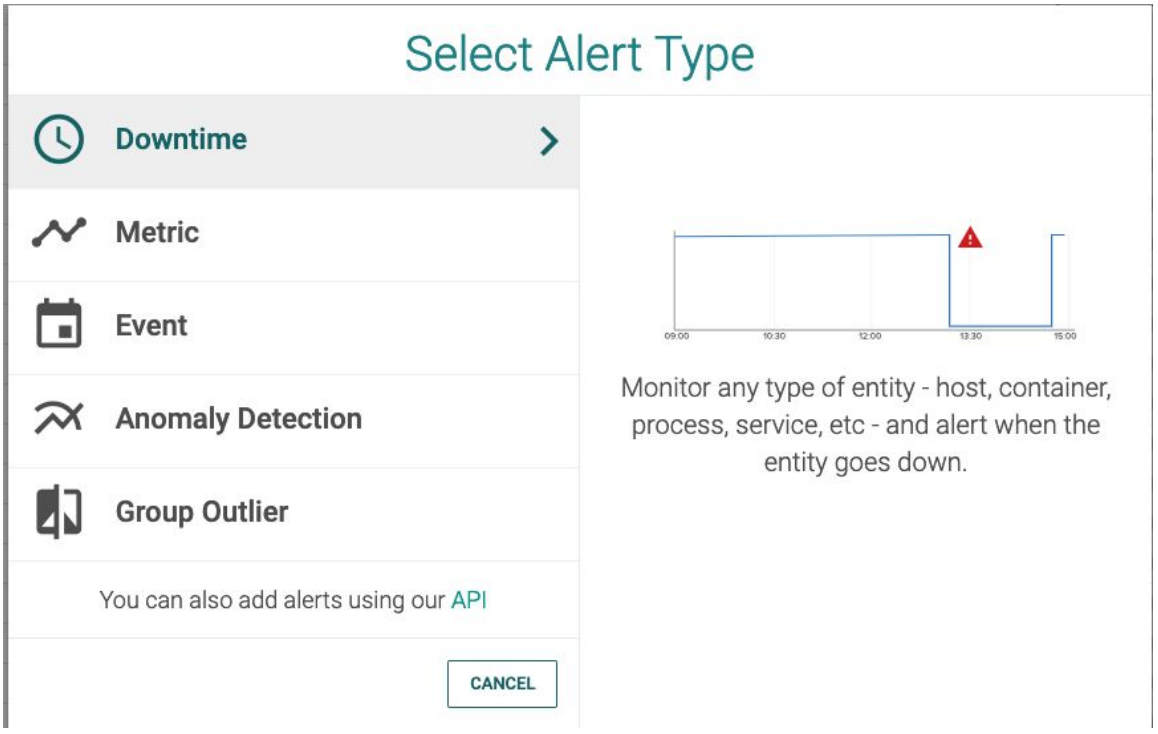
開始する前に通知チャネルを設定します。これにより、チャネルをアラートに割り当てることができます。必要に応じて、カスタムの件名と本文の情報を個々のアラート通知に追加できます。

基本的なアラート情報を入力

設定は、アラートタイプごとに少し異なります。詳細については、それぞれのページを参照してください。このセクションでは、アラートのユーザーインターフェイスを理解してナビゲートするための一般的な手順について説明します。

アラートを構成するには、アラートウィザードを開き、次のパラメーターを設定します。

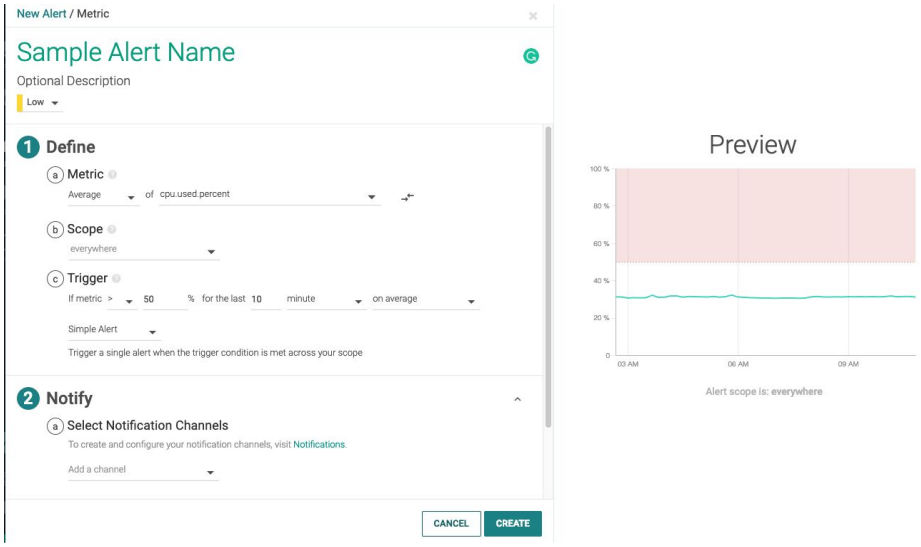
- （セットアップ）：
    - タイプ：目的のアラートタイプを選択します。



各タイプには異なるパラメーターがありますが、同じパターンに従います。

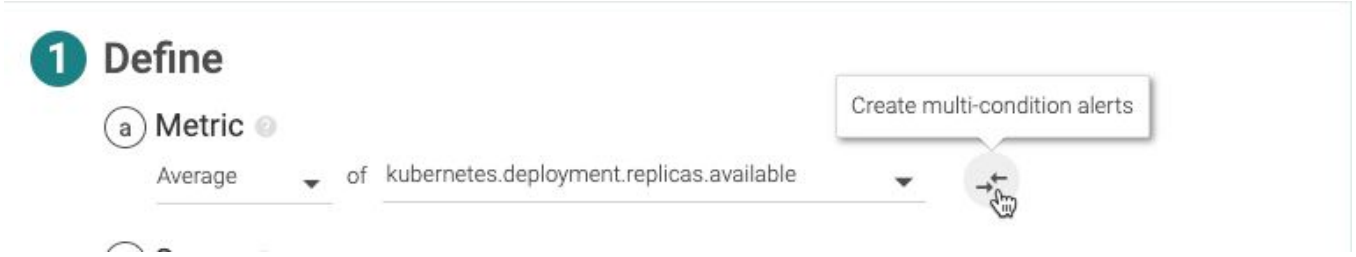
- `Name`：作成しているアラートを一意に表すことができる意味のある名前を指定します。たとえば、Production Cluster Failed Scheduling podsなどのターゲットにアラートを送信するエンティティ。

- `Description`（オプション）：アラート名またはアラート条件を簡単に展開して、受信者に追加のコンテキストを提供します。
- `Priority: High, Medium, Low,`および`Info`がイベントリストに反映され、イベント/アラートの重大度でソートできます。
- `Define`、`Notify`、および`Act`セクションのパラメータ



- （1）Define：
    - メトリクス：このアラートが監視するメトリクスまたはエンティティを選択します。また、avg、max、min、sumなど、データの集計方法も定義します。メトリクスはアイテムのグループに適用されます（グループ集約）。

ブールロジックを使用して複数のメトリクスでアラートを送信するには、[`Create multi-condition alerts`]をクリックします。複数条件アラートを参照してください。



- `Scope`：すべての場所、またはKubernetesデプロイメント、Sysdigエージェント、特定のサービスなど、監視対象のインフラストラクチャーの特定のコンポーネントをフィルタリングするためのより限定的なスコープ。
- `Trigger`：アラート条件を評価するための境界、およびシングルアラートを送信するかマルチプルアラートを送信するか。サポートされる時間スケールは、分、時間、または日です。
    - `Single alert`：シングルアラートは、スコープ全体に対してアラートを発生させます。
    - `Multiple alerts`：セグメントの一部またはすべてが一度にしきい値に違反すると、複数のアラートが発生します。

      指定したセグメントごとに複数のアラートがトリガーされます。指定したセグメントはアラートに表示されます。セグメントの数が多いほど、影響を受けるエンティティを一意に識別しやすくなります。

詳細については、アラートタイプの各セクションを参照してください。

- （2）Notify

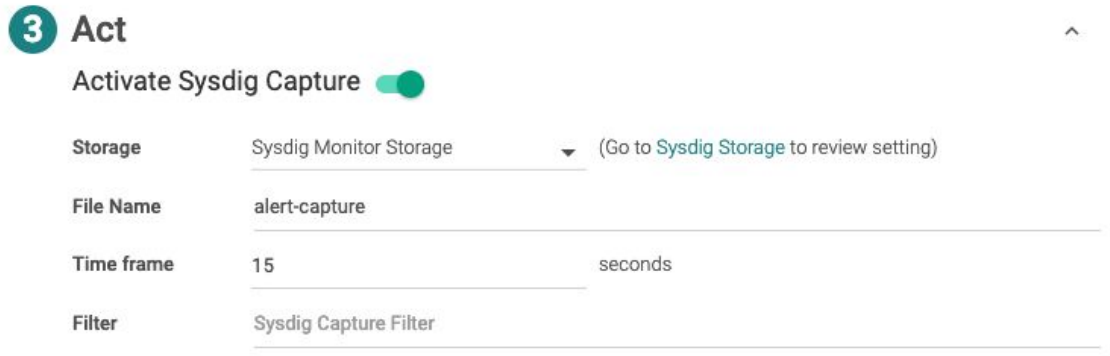
    - `Notification Channel`：リスト内の設定済み通知チャネルから選択します。サポートされるチャネルは次のとおりです。

        - Eメール
        - Slack
        - Amazon SNSトピック
        - Opsgenie
        - Pagerduty
        - VictorOps
        - Webhook
    - `Notification Options`：複数のアラートを送信する時間間隔を設定します。
    - `Format Message`：必要に応じて、メッセージフォーマットの詳細を追加します。通知のカスタマイズを参照してください。

- （3）Act

- （オプション）：Sysdigキャプチャーを構成します。キャプチャーも参照してください。

  Sysdigキャプチャファイルは、`Event Alerts`では使用できません。



- [`Create`]または[`Save`]をクリックします。

オプション：通知をカスタマイズする

オプションで、個別の通知をカスタマイズして、アラートをトリガーしたエラーのコンテキストを提供できます。すべての通知チャネルは、この追加されたコンテキスト情報とカスタマイズの柔軟性をサポートします。

次のように、アラート通知の件名、本文、またはその両方を変更します。

- 平文：問題を説明するカスタムメッセージ。たとえば、展開の停止。
- ハイパーリンク：たとえば、ダッシュボードへのURL。
- 動的変数：たとえば、ホスト名。規則に注意してください：
  - 挿入するすべての変数は、{{file_mount}}のように二重中括弧で囲む必要があります。
  - 変数では大文字と小文字が区別されます。
  - 変数は、アラートを作成したセグメント値に対応している必要があります。たとえば、アラートがhost.hostNameとcontainer.nameによってセグメント化されている場合、対応する変数はそれぞれ{{host.hostName}}と{{container.name}}になり、通知の件名と本文で他のセグメント変数を使用することはできません。
  - 通知の件名はイベントフィードに表示されません。
  - セグメントの一部ではない変数を使用すると、エラーが発生します。

- アラートで使用されるセグメント変数は、アラートの送信時に現在のシステム値に変換されます。

通知メッセージの本文には、デフォルトのアラートテンプレートが含まれています。これは、Sysdigモニターによって生成されるデフォルトのアラート通知です。テンプレートの前後にフリーテキスト、変数、またはハイパーリンクを追加できます。

カスタマイズしたアラート通知を次のチャネルに送信できます。

- Email
- Slack
- Amazon SNS Topic
- Opsgenie
- Pagerduty
- VictorOps
- Webhook

アラートを管理する

アラートは、アラートUIの左側のチェックボックスと下部のカスタマイズバーを使用して、個別に、またはグループとして管理できます。テーブルの列を構成して、ユースケースに必要なデータを提供することもできます。アラートのグループを選択し、削除、有効化、無効化、JSONオブジェクトへのエクスポートなど、いくつかのバッチ操作を実行します。個別のアラートを選択して、別のチームのコピーの作成などのタスクを実行します。

アラートを有効/無効にする

アラートは、カスタマイズバーを使用して有効または無効にできます。これらの操作は、シングルアラートまたはマルチプルアラートに対してバッチ操作として実行できます。

1. アラートモジュールで、関連するアラートの横にあるチェックボックスをオンにします。
2. 必要に応じて、[`Enable`]または[`Disable`]をクリックします。

`Enable`/`Disable`ボタンは、関連するアラートが選択されている場合にのみ表示されます。たとえば、下の画像では、選択したアラートが現在有効になっているため、[`Disable`]ボタンのみが表示されて

います。

以下の画像では、有効なアラートと無効なアラートが表示されているため、両方のボタンが表示されています。

アラートJSONのエクスポート

選択した各アラートのJSONスニペットを含むJSONファイルをローカルマシンにエクスポートできます。

1. エクスポートする関連アラートの横にあるチェックボックスをクリックします。
2. カスタマイズバーの[`Export JSON`]ボタンをクリックします。

アラートをコピーする

アラートを現在のチーム内にコピーして、同様のアラートをすばやく作成したり、別のチームにコピーしてアラートを共有したりできます。

同じチームにアラートをコピーする

現在のチーム内でアラートをコピーするには：

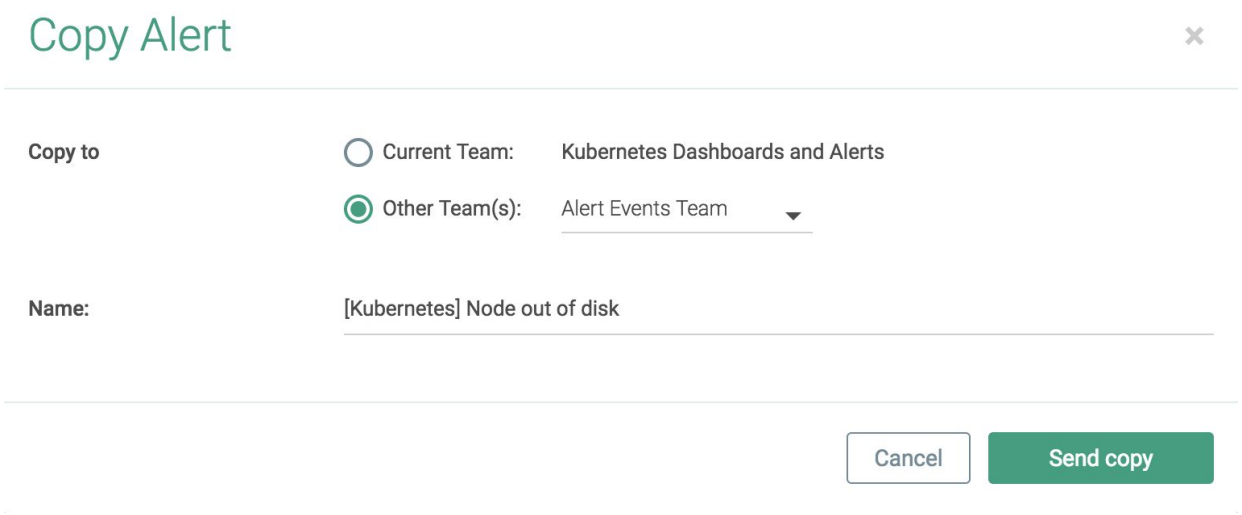
1. コピーするアラートの横のチェックボックスをクリックします。
2. カスタマイズバーの[`Copy`]ボタンをクリックします。

3. [`Current Team`]オプションが選択されていることを確認します。
4. アラートの名前を変更し、[`Copy and Open`]ボタンをクリックして変更を保存します。

アラートを別のチームにコピーする

現在のチーム内でアラートをコピーするには：

1. コピーするアラートの横のチェックボックスをクリックします。
2. カスタマイズバーの[`Copy`]ボタンをクリックします。
3. [`Other Team(s)`]オプションを選択します。
4. [`Select Team`]ドロップダウンメニューを開き、アラートのコピー先となるチームを選択します。



5. アラートの名前を変更し、[`Send Copy`]ボタンをクリックして変更を保存します。

アラートを削除

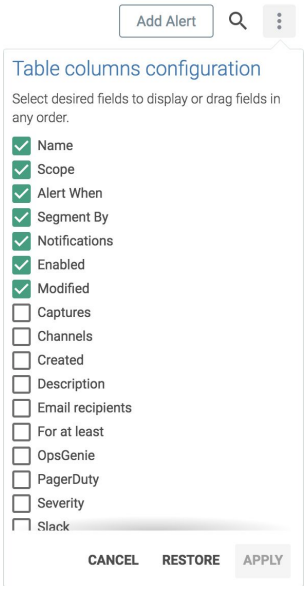
1つ以上のアラートを削除するには：

1. 削除するアラートの横にあるチェックボックスをクリックします。
2. カスタマイズバーの[`Delete`]ボタンをクリックします。
3. [`Yes, Delete Alerts`]ボタンをクリックして、変更を確認します。

アラートテーブル列の設定

表示される列を設定するには：

1. アラートモジュールから、`Table Columns Configuration`（3つのドット）アイコンをクリックします。



2. 目的の各列の横にあるボックスをオンにします。
3. [`Apply`]ボタンをクリックして変更を保存し、[`Restore`]ボタンをクリックしてテーブルを元の設定に戻すか、[`Cancel`]ボタンをクリックして以前の設定に戻します。

アラートを検索

Alertsテーブルは、部分的または完全な文字列を使用して検索できます。たとえば、以下の検索では、kubernetesを含むイベントのみが表示されます。

Alerts

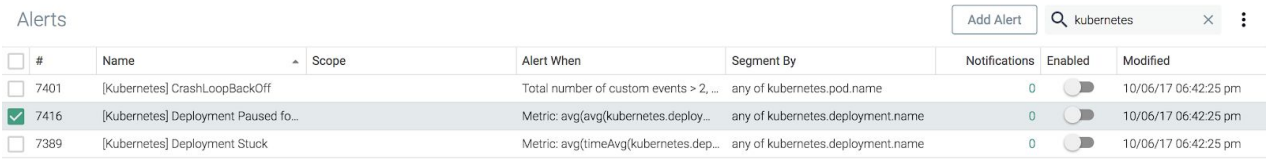
Add Alert | kubernetes

#	Name	Scope	Alert When	Segment By	Notifications	Enabled	Modified
7401	[Kubernetes] CrashLoopBackOff		Total number of custom events > 2, ...	any of kubernetes.pod.name	0		10/06/17 06:42:25 pm
7416	[Kubernetes] Deployment Paused fo...		Metric: avg(avg(kubernetes.deploy...	any of kubernetes.deployment.name	0		10/06/17 06:42:25 pm
7389	[Kubernetes] Deployment Stuck		Metric: avg(timeAvg(kubernetes.dep...	any of kubernetes.deployment.name	0		10/06/17 06:42:25 pm
7387	[Kubernetes] Deployments with no a...		Metric: avg(max(kubernetes.deploy...	any of kubernetes.namespace.nam...	0		07/04/18 06:28:50 pm
7405	[Kubernetes] Failed to pull image		Total number of custom events > 0, ...	any of kubernetes.pod.name	0		07/04/18 06:28:50 pm
7426	[Kubernetes] Node memory under p...		Metric: avg(avg(kubernetes.node.m...	any of kubernetes.node.name	0		07/04/18 06:28:50 pm
7403	[Kubernetes] Node network unavaila...		Metric: avg(avg(kubernetes.node.ne...	any of kubernetes.node.name	0		10/06/17 06:42:25 pm
7420	[Kubernetes] Node out of disk		Metric: avg(avg(kubernetes.node.ou...	any of kubernetes.node.name	0		07/04/18 06:28:50 pm
7411	[Kubernetes] Node under disk press...		Metric: avg(avg(kubernetes.node.dis...	any of kubernetes.node.name	0		10/06/17 06:42:25 pm
7424	[Kubernetes] Nodes unschedulable		Metric: avg(avg(kubernetes.node.un...	any of kubernetes.node.name	0		10/06/17 06:42:25 pm
7422	[Kubernetes] Pods Available less tha...		Metric: avg(timeAvg(kubernetes.dep...	any of kubernetes.namespace.nam...	0		10/06/17 06:42:25 pm
7390	[Kubernetes] Readiness probe failed		Total number of custom events > 0, ...	any of kubernetes.pod.name	0		10/06/17 06:42:25 pm
7391	[Kubernetes] Service generating HT...		Metric: sum(avg(net.http.error.count...	any of kubernetes.namespace.nam...	0		10/06/17 06:42:25 pm
7395	[Kubernetes] Service response time		Metric: avg(avg(net.request.time)) > ...	any of kubernetes.namespace.nam...	0		10/06/17 06:42:25 pm
7406	[Kubernetes]: Liveness probe failed		Total number of custom events > 1, ...	any of kubernetes.pod.name	0		10/06/17 06:42:25 pm
33633	TestTEst		Metric: avg(sum(kubernetes.pod.res...	any of kubernetes.pod.name	1325		03/23/18 09:05:06 am

既存のアラートを編集する

既存のアラートを編集するには：

1. アラートの横にあるチェックボックスをクリックします。

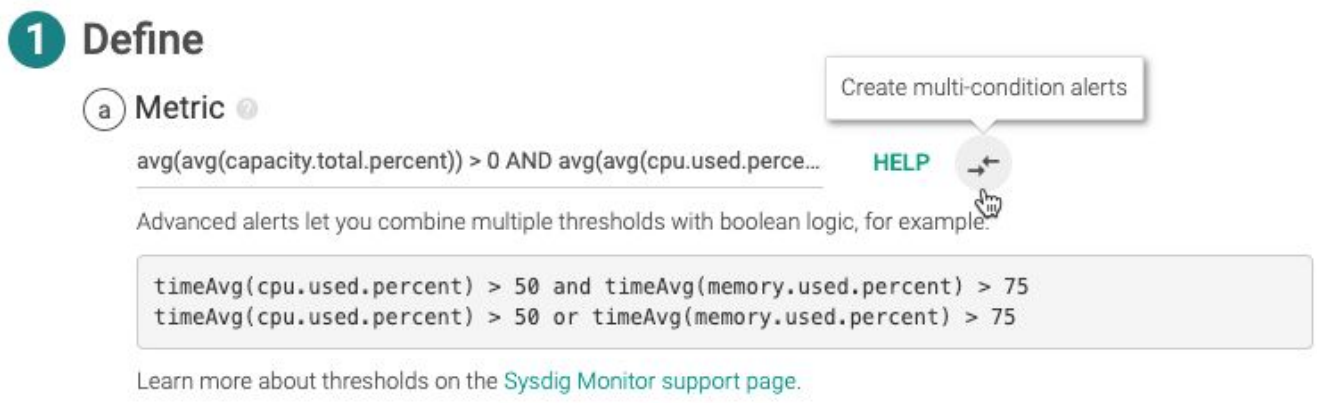


2. カスタマイズバーの[`Edit`]ボタンをクリックします。

3. アラートを編集し、[`Save`]ボタンをクリックして変更を確認します。

複数条件アラート

複数条件アラートは、複雑な条件で作成される高度なアラートしきい値です。そのためには、アラートのしきい値を、複数の条件を伴う可能性のあるカスタムのブール式として定義します。[`Create multi-condition alerts`]をクリックして、ブール式として条件を追加できるようにします。



以下の例で説明するように、これらの高度なアラートには特定の構文が必要です。

フォーマットと操作

各条件には5つの部分があります。

- メトリクス名：正確なメトリクス名を使用します。タイプミスを回避するには、HELPリンクをクリックして、使用可能なメトリクスのドロップダウンリストにアクセスします。リストからメトリクスを選択すると、編集中のしきい値式に名前が自動的に追加されます。
- グループ集約（オプション）：グループ集約タイプが選択されていない場合、メトリクスの適切なデフォルト（合計または平均）が適用されます。グループ集計関数は、時間集計関数の外で適用する必要があります。
- 時間の集計：選択した期間にロールアップされた履歴データです。
- 演算子：論理演算子と関係演算子の両方がサポートされています。
- 値：条件が評価される静的な数値。

次の表は、サポートされている時間集計関数、グループ集計関数、および関係演算子を示しています。

時間集計機能	グループ集約機能	演算子r
timeAvg()	avg()	=
min()	min()	<
max()	max()	>
sum()	sum()	<=
		>=
		!=

フォーマットは：

```
condition1 AND condition2
condition1 OR condition2
NOT condition1
```

操作の順序は括弧で変更することもできます：

```
NOT (condition1 AND (condition2 OR condition3))
```

条件は次の形式を取ります。

```
groupAggregation(timeAggregation(metric.name)) operator value
```

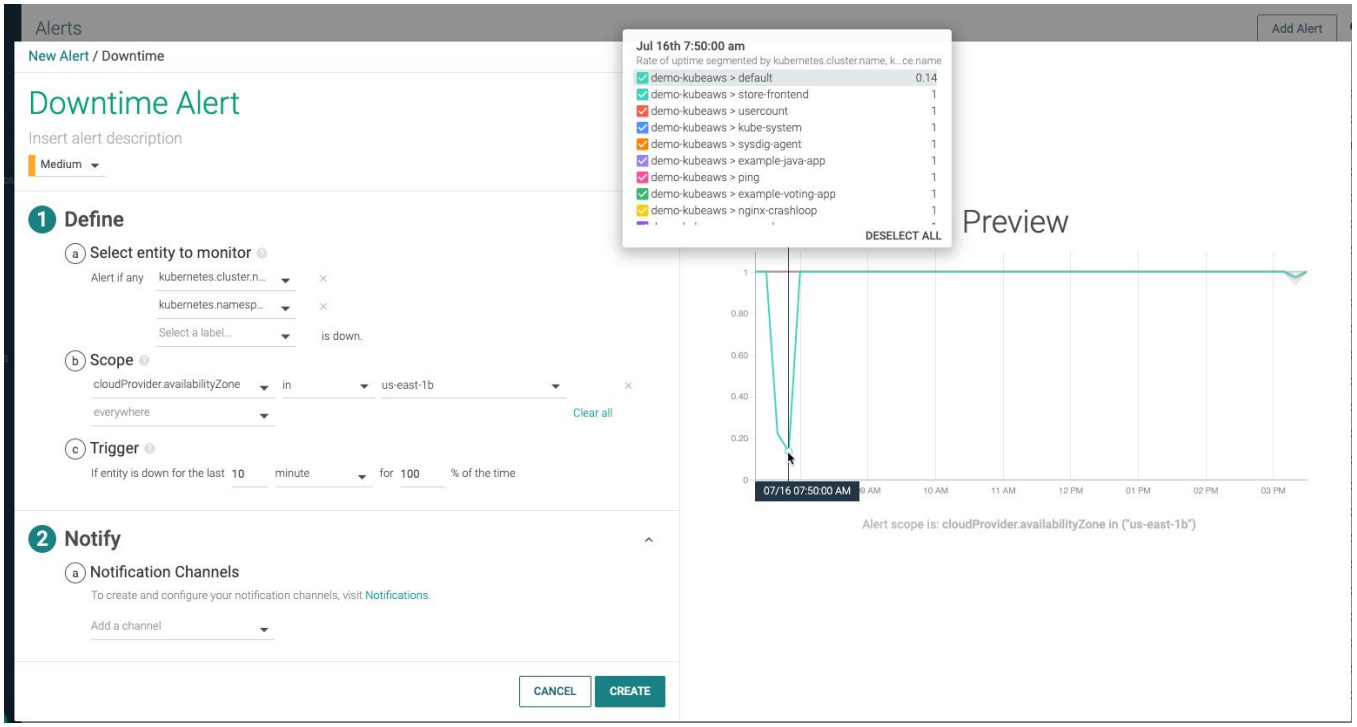
式の例

高度なアラートのいくつかの例を以下に示します。

```
timeAvg(cpu.used.percent) > 50 AND timeAvg(memory.used.percent) > 75
timeAvg(cpu.used.percent) > 50 OR timeAvg(memory.used.percent) > 75
timeAvg(container.count) != 10
min(min(cpu.used.percent)) <= 30 OR max(max(cpu.used.percent)) >= 60
sum(file.bytes.total) > 0 OR sum(net.bytes.total) > 0
timeAvg(cpu.used.percent) > 50 AND (timeAvg(mysql.net.connections) > 20 OR
timeAvg(memory.used.percent) > 75)
```

ダウンタイムアラート

Sysdigモニターは、ホスト、コンテナ、プロセス、サービスなど、インフラストラクチャー内のあらゆるタイプのエンティティーを継続的に監視し、モニター対象のエンティティーが使用できないか応答しない場合に通知します。ダウンタイムアラートは、インフラストラクチャーの予定外のダウンタイムに主に焦点を当てています。



この例では、Kubernetesクラスターが監視され、アラートはクラスターとネームスペースの両方でセグメント化されます。選択したアベイラビリティーゾーンのKubernetesクラスターがダウンすると、クラスターと影響を受けるネームスペースの両方に関する必要な情報を含む通知が送信されます。プレビューチャートに表示される線は、監視対象として選択されたセグメントの値を表します。ポップアップは、色分けされた凡例であり、線が表すセグメント（または複数ある場合はセグメントの組み合わせ）を示します。一部の線分を選択解除して、チャートに表示されないようにすることもできます。Sysdig モニターがプレビューチャートに表示する行は10行に制限されていることに注意してください。ダウンタイムアラートの場合、セグメントは「**Select entity to monitor**」オプションで実際に選択するものです。

ダウンタイムアラートの定義

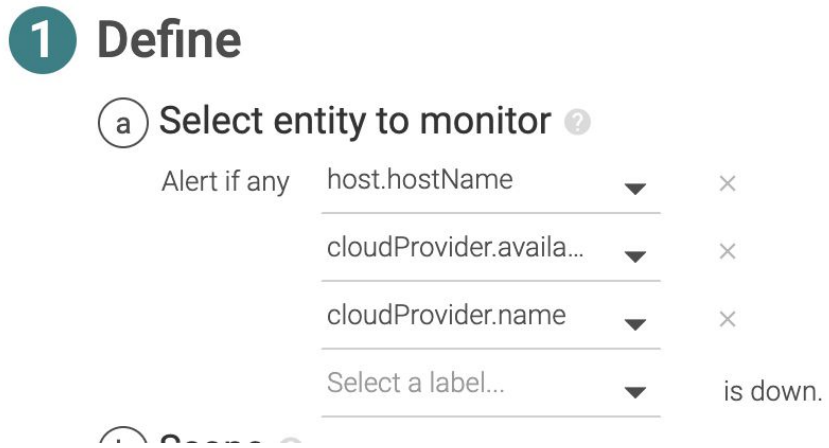
ガイドライン

- **ユニーク名と説明を設定する**：受信者がアラートを簡単に識別できるように、わかりやすい名前と説明を設定します。
- **重大度**：アラートの重大度レベルを設定します。ダッシュボードでイベントを表示およびソートしたり、UIを探索したりすることもできます。優先度：`High`, `Medium`, `Low`、および`Info`がイベントリストに反映され、イベント/アラートの重大度で並べ替えることができます。イベントとアラートを作成するときに、重大度を基準として使用できます。たとえば、重大度の高いイベントが10個以上ある場合は通知します。
- **複数のセグメントを指定する**：単一のセグメントを選択しても、トラブルシューティングに十分な情報が常に提供されるとは限りません。関連するセグメントを追加して、選択したエンティティに関連情報を追加します。階層エンティティを入力して、何がどこで何が問題だったかをボトムダウンで把握します。たとえば、Kubernetesクラスタのみを指定しても、トラブルシューティングに必要なコンテキストが提供されません。問題を絞り込むために、Kubernetesネームスペース、Kubernetesデプロイメントなどのコンテキスト情報をさらに追加します。

エンティティを指定

1. ダウンタイムを監視するエンティティを選択します。
   この例では、ホストの予定外のダウンタイムを監視しています。

2. 追加のセグメントを指定します。



指定したエンティティはセグメント化され、デフォルトの通知テンプレートとプレビューで通知されます。この例では、データはホスト名、クラウドプロバイダーのアベイラビリティーゾーン、およびクラウドプロバイダー名でセグメント化されています。ホストがダウンした場合、通知には影響を受けるホスト名だけでなく、関連するクラウドプロバイダーと、それが含まれるアベイラビリティーゾーンも含まれます。

スコープを構成する

このアラートが適用される環境をフィルタリングします。ホストがアベイラビリティーゾーンus-east-1bでダウンすると、アラートが発生します。

演算子を使用または含むことで、スコープを適用するために複数の異なる可能な値と一致します。
包含演算子と非包含演算子は、値の一部がわかっている場合に値を取得するのに役立ちます。たとえば、「us-east-1b」、「us-west-2b」など、「us」で始まる文字列を含む値を取得します。
in演算子とnot in演算子は、複数の値をフィルタリングするのに役立ちます。
また、エクスプローラーとダッシュボードから直接アラートを作成して、このスコープに自動的に入力することもできます。

トリガーの構成

アラート条件を評価するためのしきい値と時間枠を定義します。サポートされる時間スケールは、分、時間、または日です。

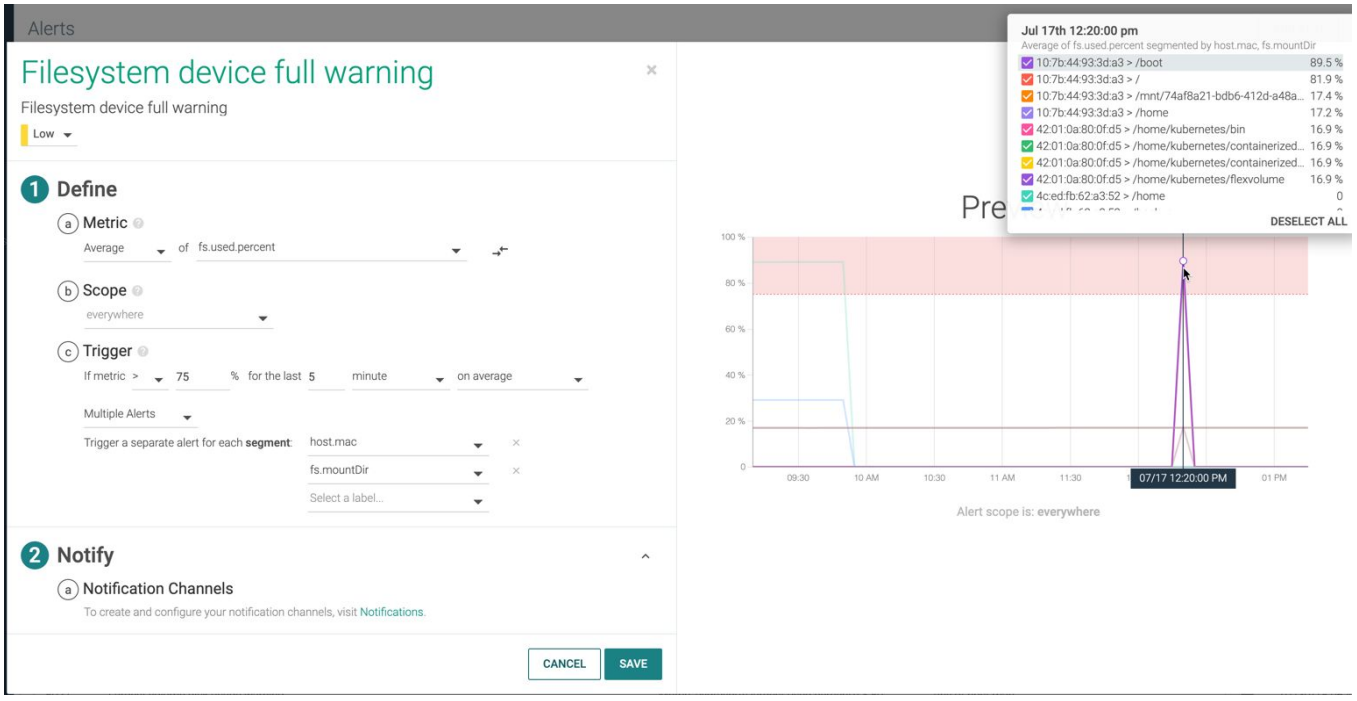
監視対象のホストまたはKubernetesクラスタが使用できないか、過去5分間応答がない場合、受信者に通知されます。
%には任意の値を設定でき、時間枠には1より大きい値を設定できます。たとえば、100%ではなく50%を選択した場合、選択した5分の時間枠でエンティティが2.5分間ダウンすると、通知がトリガーされます。

ユースケース

- ブラックフライデー、クリスマス、または新年のシーズンのピーク時にeコマースWebサイトがダウンしています。
- データセンターの本番サーバーで重大な機能停止が発生
- MySQLデータベースに接続ができません
- ファイルのアップロードがマーケティングWebサイトでは機能していません

メトリクスアラート

Sysdig モニターは時系列のメトリクスを監視し、それらがユーザー定義のしきい値に違反した場合にアラートを出します。



プレビューチャートに表示される線は、監視対象として選択されたセグメントの値を表します。ポップアップは、色分けされた凡例であり、線が表すセグメント（または複数ある場合はセグメントの組み合わせ）を示します。一部の線分を選択解除して、チャートに表示されないようにすることもできます。 Sysdig モニターがプレビューチャートに表示する行は10行に制限されていることに注意してください。

メトリクスアラートの定義

ガイドライン

- **ユニーク名と説明を設定する**：受信者がアラートを簡単に識別できるように、意味のある名前と説明を設定します
- **複数のセグメントを指定する**：単一のセグメントを選択しても、トラブルシューティングに十分な情報が常に提供されるとは限りません。関連するセグメントを追加して、選択したエンティティに関連情報を追加します。階層エンティティを入力して、何がどこで何が問題だったかを下から見下ろすようにします。たとえば、Kubernetesクラスタのみを指定しても、トラブルシューティングに必要なコンテキストが提供されません。問題を絞り込むために、

Kubernetes名前空間、Kubernetesデプロイメントなどのコンテキスト情報をさらに追加します。

エンティティを指定

1. ダウンタイムを監視するエンティティを選択します。
   この例では、ホストの予定外のダウンタイムを監視しています。
2. 追加のセグメントを指定します。
   この例では、ホストのMACアドレスとファイルシステムのマウントディレクトリを監視しています。

メトリクスを指定する

このアラートが監視するメトリクスを選択します。また、avg、max、min、sumなど、データの集計方法を定義することもできます。ブールロジックを使用して複数のメトリクスでアラートを送信するには、複数条件アラートに切り替えます。

スコープを構成する

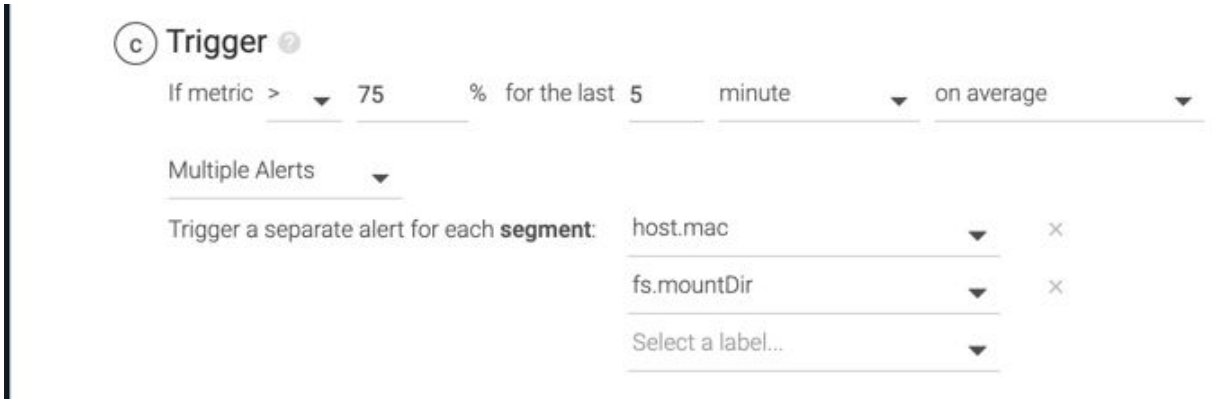
このアラートが適用される環境をフィルタリングします。
このアラートが適用される環境をフィルタリングします。ホストがアベイラビリティーゾーンus-east-1bでダウンすると、アラートが発生します。

高度な演算子を使用して、グループ、タグ、エンティティを含めたり、除外したり、パターンマッチしたりします。複数条件アラートを参照してください。
また、エクスプローラとダッシュボードから直接アラートを作成して、このスコープに自動的に入力することもできます。

トリガーの設定

アラート条件を評価するためのしきい値と時間枠を定義します。単一のアラートはスコープ全体に対してアラートを発しますが、複数のアラートは、いずれかまたはすべてのセグメントが一度にしきい

値に違反すると発動します。



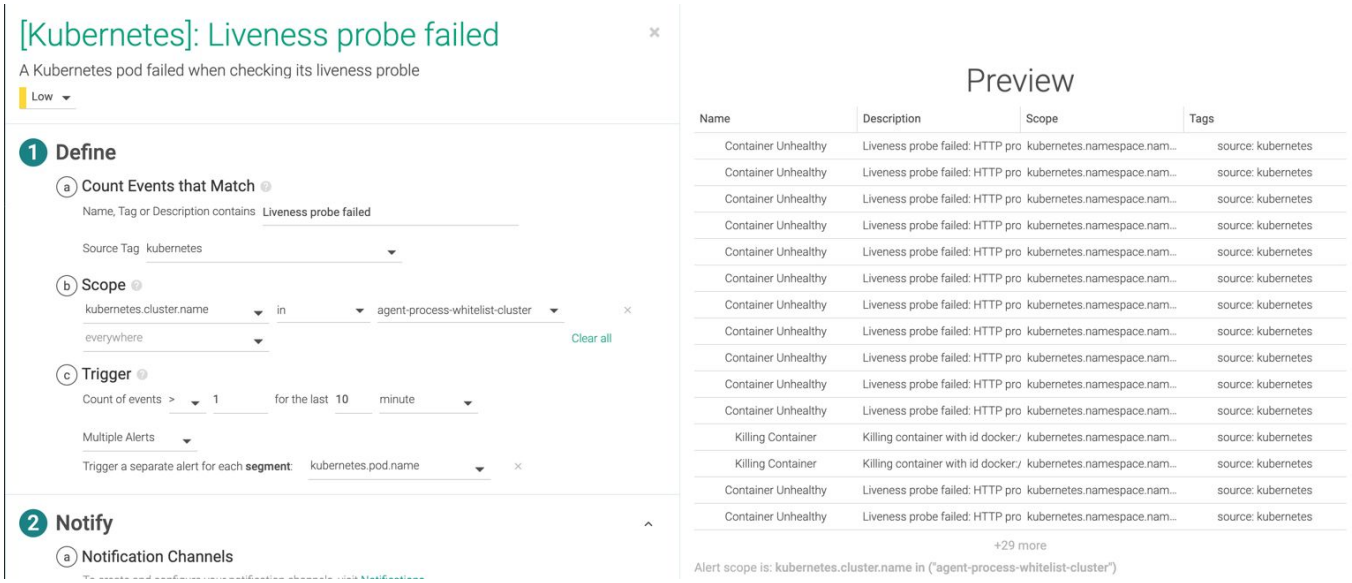
この例では、ファイルシステムの使用率が過去5分間の平均で75を超えると、複数のアラートがトリガーされます。ホストのMACアドレスとファイルシステムのマウントディレクトリがアラート通知に表示されます。

ユースケース

- ホストで実行されているプロセスの数が通常と異なる
- コンテナのルートボリュームのディスク使用率が高い

イベントアラート

特定のイベントの発生を監視し、発生の総数がしきい値に違反した場合に警告します。コンテナ、オーケストレーション、および再起動やデプロイメントなどのサービスイベントに関するアラートに役立ちます。



イベントアラートの定義

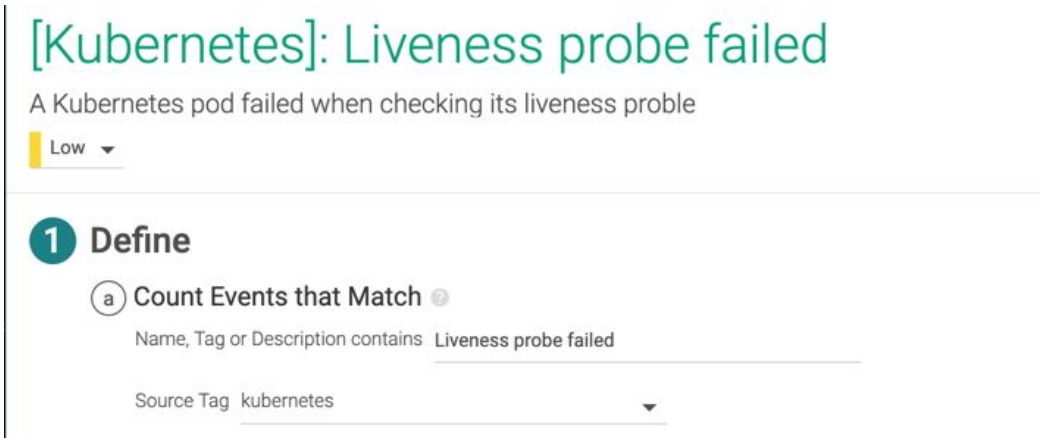
ガイドライン

- **ユニーク名と説明を設定する**：受信者がアラートを簡単に識別できるように、わかりやすい名前と説明を設定します。
- **重大度**：アラートの重大度レベルを設定します。ダッシュボードでイベントを表示およびソートしたり、UIを探索したりすることもできます。優先度：`High`, `Medium`, `Low`、および`Info`がイベントリストに反映され、イベント/アラートの重大度で並べ替えることができます。イベントとアラートを作成するときに、重大度を基準として使用できます。たとえば、重大度の高いイベントが10個以上ある場合は通知します。
- ソースタグ：サポートされているソースタグは、Kuberentes、Docker、およびContainerdです。
- 複数のセグメントを指定する：単一のセグメントを選択しても、トラブルシューティングに十分な情報が常に提供されるとは限りません。関連するセグメントを追加して、選択したエンティティに関連情報を追加します。階層エンティティを入力して、何がどこで何が問題だった

かをボトムダウンで把握します。たとえば、Kubernetesクラスタのみを指定しても、トラブルシューティングに必要なコンテキストが提供されません。問題を絞り込むために、Kubernetesネームスペース、Kubernetesデプロイメントなどのコンテキスト情報をさらに追加します。

イベントを指定

1. イベントの名前、タグ、または説明を指定します。



2. ソースタグを指定します。

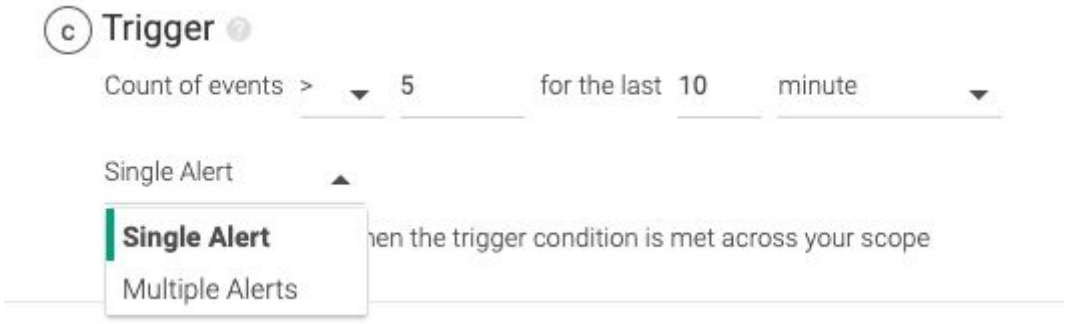
スコープを設定する

このアラートが適用される環境をフィルタリングします。高度な演算子を使用して、グループ、タグ、エンティティを含めたり、除外したり、パターンマッチしたりします。また、エクスプローラーとダッシュボードから直接アラートを作成して、このスコープに自動的に入力することもできます。

この例では、agent-process-whitelist-clusterクラスターでlivenessプローブが失敗すると、アラートがトリガーされます。

トリガーの設定

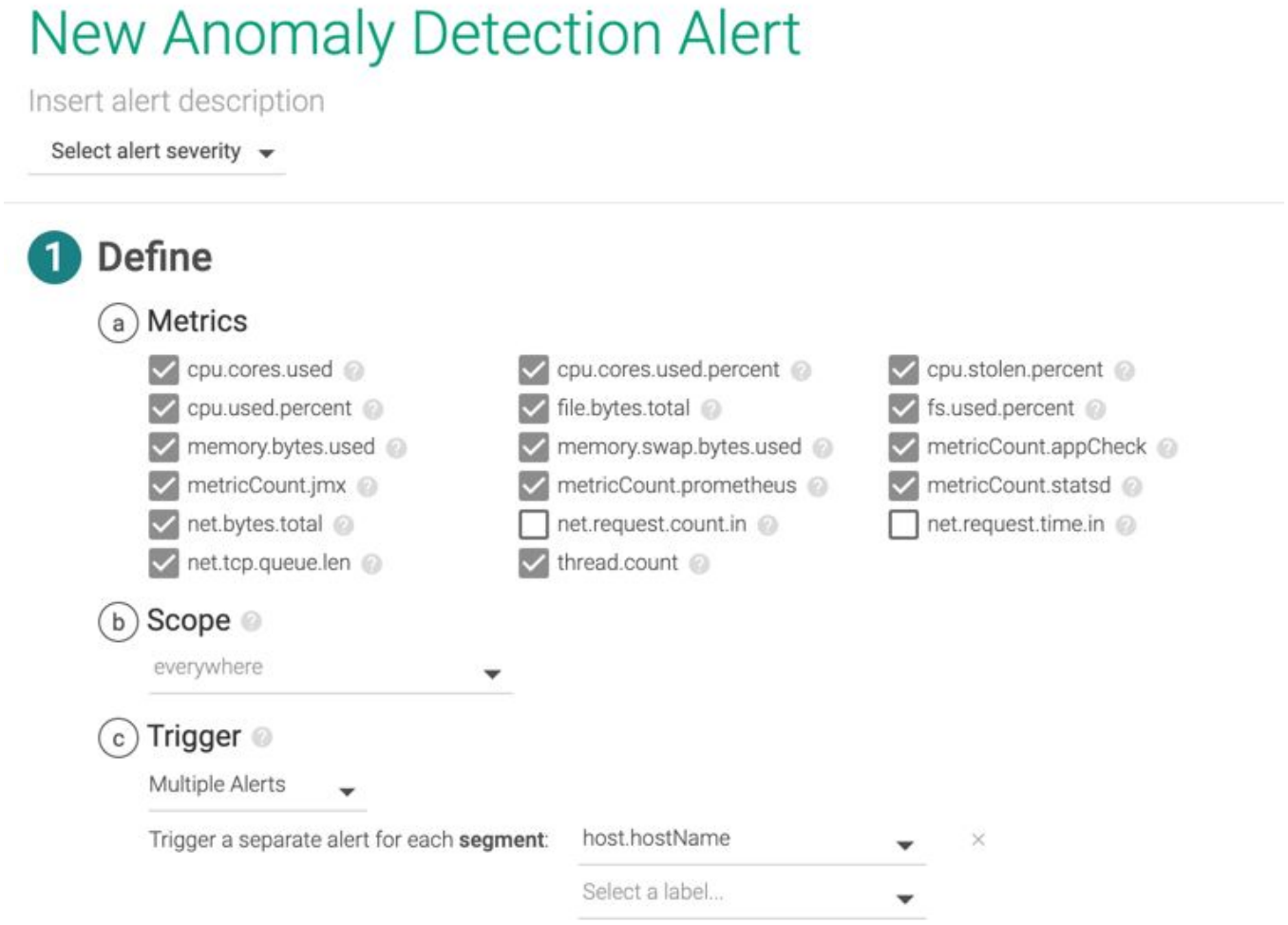
アラート条件を評価するためのしきい値と時間枠を定義します。シングルアラートはスコープ全体に対してアラートを発しますが、マルチプルアラートは、いずれかまたはすべてのセグメントが一度にしきい値に違反すると発動します。



監視対象エンティティでトリガーされたイベントの数が過去10分間に5を超える場合、選択したチャネルを通じて受信者に通知されます。

異常検出アラート

異常とは、環境からポーリングされた特定のデータセットの外れ値を指します。これは、適合パターンからの逸脱を示します。異常検出とは、これらの異常な観測を識別することです。データポイントの集合、データの単一のインスタンス、またはコンテキスト固有の異常は、異常の検出に役立ちます。たとえば、コンテナからのディレクトリの不正コピー、CPUまたはメモリの大量消費などです。



異常検出アラートを定義する

ガイドライン

- **ユニーク名と説明を設定する**：受信者がアラートを簡単に識別できるように、意味のある名前と説明を設定します

- **重大度**：アラートの重大度レベルを設定します。ダッシュボードでイベントを表示およびソートしたり、UIを探索したりすることもできます。優先度：`High`, `Medium`, `Low`、および`Info`がイベントリストに反映され、イベント/アラートの重大度で並べ替えることができます。イベントとアラートを作成するときに、重大度を基準として使用できます。たとえば、重大度の高いイベントが10個以上ある場合は通知します。
- **複数のセグメントを指定する**：単一のセグメントを選択しても、トラブルシューティングに十分な情報が常に提供されるとは限りません。関連するセグメントを追加して、選択したエンティティに関連情報を追加します。階層エンティティを入力して、何がどこで何が問題だったかをボトムダウンで把握します。たとえば、Kubernetesクラスタのみを指定しても、トラブルシューティングに必要なコンテキストが提供されません。問題を絞り込むために、Kubernetesネームスペース、Kubernetesデプロイメントなどのコンテキスト情報をさらに追加します。

エンティティを指定

動作を監視するメトリクスを1つ以上選択します。

スコープを設定する

このアラートが適用される環境をフィルタリングします。選択したメトリクスの1つから返された値が、可用性ゾーンus-east-1bのパターンに従っていない場合にアラートが発生します。

また、エクスプローラーとダッシュボードから直接アラートを作成して、このスコープに自動的に入力することもできます。

トリガーの設定

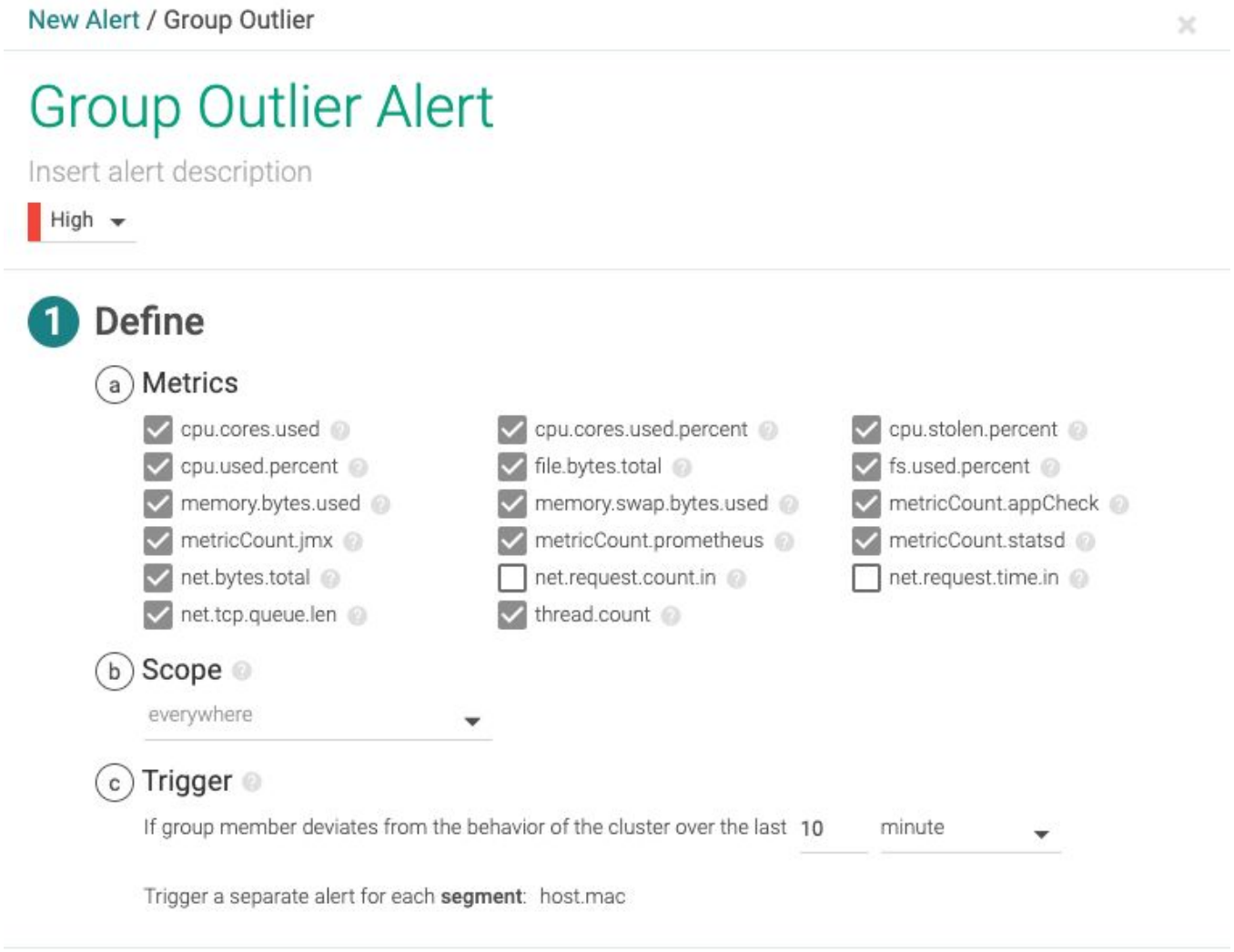
トリガーを使用すると、通知の作成方法を制御でき、通知チャネルが通知で溢れるのを防ぐことができます。たとえば、すべての違反について通知を受け取りたい場合や、一連の連続した違反について1つの通知のみを受け取りたい場合があります。

アラート条件を評価するためのしきい値と時間枠を定義します。サポートされる時間スケールは、分、時間、または日です。

監視対象のホストまたはKubernetesクラスタが使用できないか、過去5分間応答がない場合、受信者に通知されます。
%には任意の値を設定でき、時間枠には1より大きい値を設定できます。たとえば、100%ではなく50%を選択した場合、選択した5分の時間枠でエンティティが2.5分間ダウンすると、通知がトリガーされます。

グループ外れ値アラート

Sysdig モニターはホストのグループを監視し、他のホストとは異なる動作をする場合に通知します。



グループ外れ値アラートを定義する

ガイドライン

- **ユニーク名と説明を設定する**：受信者がアラートを簡単に識別できるように、意味のある名前と説明を設定します
- **重大度**：アラートの重大度レベルを設定します。ダッシュボードでイベントを表示およびソートしたり、UIを探索したりすることもできます。優先度：`High`, `Medium`, `Low`、および`Info`がイベ

ントリストに反映され、イベント/アラートの重大度で並べ替えることができます。イベントとアラートを作成するときに、重大度を基準として使用できます。たとえば、重大度の高いイベントが10個以上ある場合は通知します。

エンティティを指定

動作を監視するメトリクスを1つ以上選択します。

スコープを設定する

このアラートが適用される環境をフィルタリングします。選択したメトリクスの1つから返された値が、可用性ゾーンus-east-1bのパターンに従っていない場合にアラートが発生します。

また、エクスプローラーとダッシュボードから直接アラートを作成して、このスコープに自動的に入力することもできます。

トリガーの設定

トリガーを使用すると、通知の作成方法を制御でき、通知チャネルが通知で溢れるのを防ぐことができます。たとえば、すべての違反について通知を受け取りたい場合や、一連の連続した違反について1つの通知のみを受け取りたい場合があります。
アラート条件を評価するためのしきい値と時間枠を定義します。サポートされる時間スケールは、分、時間、または日です。

監視対象のホストまたはKubernetesクラスタが使用できないか、過去5分間応答がない場合、受信者に通知されます。

%には任意の値を設定でき、時間枠には1より大きい値を設定できます。たとえば、100%ではなく50%を選択した場合、選択した5分の時間枠でエンティティが2.5分間ダウンすると、通知がトリガーされます。

ユースケース

- ロードバランサーサーバーのワークロードが均一になっていない
- 異なるアベイラビリティーゾーンにデプロイされたアプリケーションまたはインスタンスの変更。
- クラスター内においてネットワーク負荷が高いホスト