Alibaba Cloud
云#控

ユーザガイド

Document Version20200122

目次

1 ダッシュボード

1.1 ダッシュボードの使用

1.1.1 ダッシュボードの概要

Cloud Monitor ダッシュボードは、測定値をリアルタイムに可視化することでアプリケーションとサービスの包括的な概要を提供し、問題のトラブルシューティングとリソース配分状況のモニターを可能にします。

複数インスタンスの測定傾向を表示

ダッシュボードには、複数のインスタンスに関する詳細な測定値と傾向が表示されます。 たとえば、アプリケーションが デプロイされた全ての **ECS** インスタンスを **1** つの測定グラフ上に表示できます。 これにより複数のインスタンスのトレンドを **1** つのエリアに表示できます。 同様に、複数の **ECS** インスタンスの 時間経過 に伴う **CPU** 使用率 を **1** つのグラフに表示できます。

インスタンスごとに複数の測定値を表示

また、ダッシュボードでは **1** つの **ECS** インスタンスの **CPU** 使用率、メモリ使用率、ディスク使用率等の複数の測定値を **1** つの測定 グラフ上に表示できます。 この可視化ソリューションは、例外を見つけてリソース使用量を効率的に監視するために利用できます。

インスタンスリソース配分状況をソートして表示

インスタンスをリソース配分状況レベルでソートすることでインスタンスごとの配分状況とインスタンス間の使用率の違いを迅速に確認できます。 この情報により十分な情報を得たうえでの決定を可能にし、不要なコストを削減します。

複数のインスタンスの測定値分布を表示

ECS インスタンスグループの **CPU** 使用率分布をヒートマップ として可視化して 迅速かつ正確に複数のマシンのリアルタイムの使用率を比較、確認することが可能です。 ヒートマップは強力な可視化ツールであるだけでなく、インタラクティブです。ヒートマップ上の カラーブロックをクリックすると指定された期間内の該当するマシンのメトリクスと傾向を表示します。

複数のインスタンスの集計メトリクスの表示

ダッシュボードを使用して特定のメトリクスの複数の **ECS** インスタンスの **CPU** 使用率等の平均集計値を **1** つのグラフ内に表示できます。 この機能により全般的な **CPU** 使用率キャパシティを迅速に見積もり、複数インスタンスのリソース配分のバランスが取れているかを確認できます。

フルスクリーン の可視化ソリューションを提供

ダッシュボードは自動的に最新の情報に更新するフルスクリーンモードをサポートします。 このモードでは簡単に複数のアプリケーションとプロダクト測定値をフルスクリーンディスプレイに追加でき、全てのモニタリングデータの概要を視覚的に表示します。

1.1.2 ダッシュボードの管理

ダッシュボードは簡単に表示、作成、削除できます。 これらのアクションを行う手順は以下のとおりです。

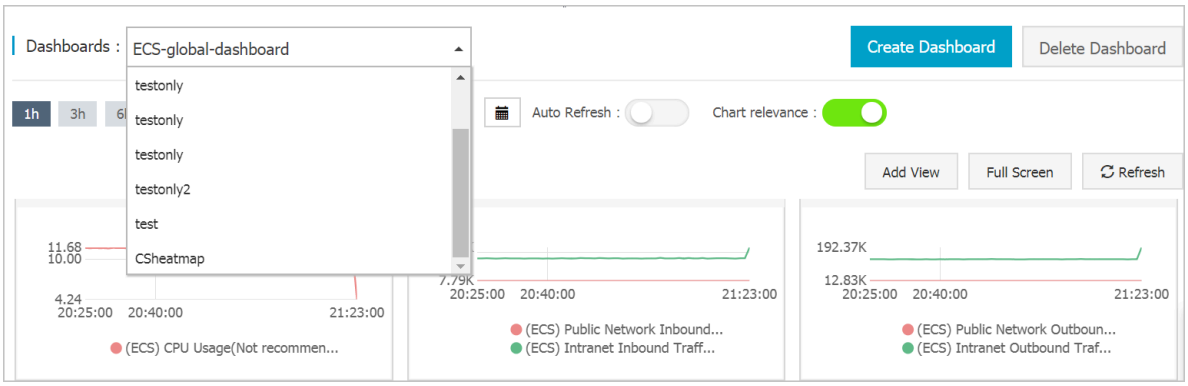
ダッシュボードの表示

ダッシュボードを表示し、1 つの領域内にある複数の異なるプロダクトおよびインスタンスからの測定値を表示およびモニターすることができます。

> 注：
>
> - **Cloud Monitor** は **ECS** ダッシュボードを自動的に初期化し、**ECS** 測定値を表示します。
> - **Cloud Monitor** は、**1** 時間、**3** 時間、および **6** 時間で測定されたデータを自動的に更新します。 ただし、**6** 時間を超えて測定されたデータを自動的に更新することはできません。

手順

1. *Cloud Monitor コンソール*にログインします。
2. 左のナビゲーションウインドウで [ダッシュボード] > [カスタマイズダッシュボード]をクリックします。
3. デフォルトでは、 [ECS グローバルダッシュボード] が表示されています。 ドロップダウンリストから別のダッシュボードを選択できます。



4. ダッシュボードをフルスクリーンで表示するには、ページの右上隅にある [フルスクリーン] をクリックします。

5. 時間範囲を選択します。 ページ上部の時間範囲ボタンをクリックします。 ここからダッシュボードのグラフに表示される時間範囲を選択できます。 選択した時間範囲はダッシュボードのすべてのグラフに適用されます。
6. [自動更新] をオンにした後、1 時間、3 時間、または 6 時間の照会期間を切り替えてると、自動更新が毎分実行されます。
7. 測定された測定値の単位は、グラフ名のかっこ内に表示されます。
8. グラフ上のある点にポインターを合わせると、その時点の値がすべてのグラフに表示されます。

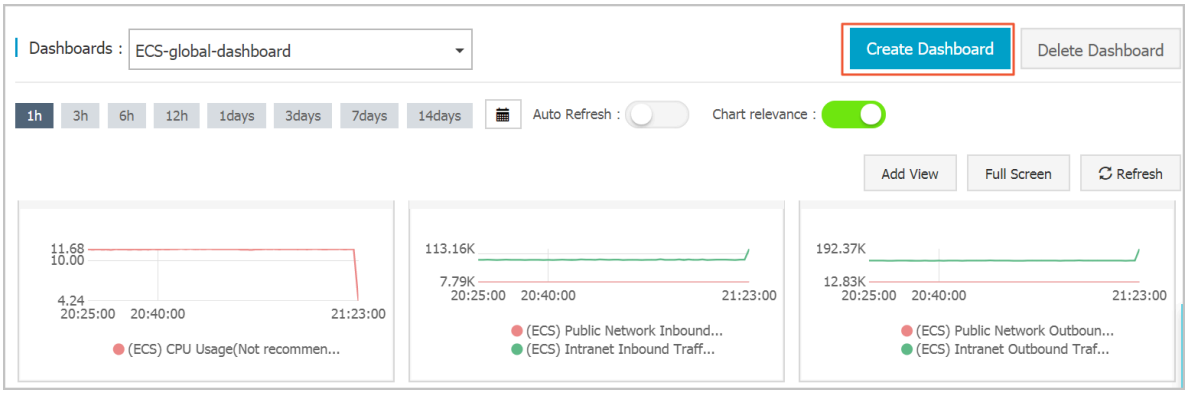
ダッシュボードの作成

デフォルトの ECS ダッシュボードが複雑な業務のモニタリングニーズを満たしていない場合、ダッシュボードを作成しグラフをカスタマイズできます。

> 注：
> 1 つのダッシュボードに最大 20 個のグラフを作成できます。

手順

1. *Cloud Monitor コンソール* にログインします。
2. 左のナビゲーションウィンドウから[ダッシュボード] > [カスタマイズダッシュボード]をクリックします。
3. ページの右上隅にある [ダッシュボードの作成] をクリックします。



4. ダッシュボードの名前を入力します。

5. [作成] をクリックします。 新しいダッシュボードページに自動的にリダイレクトされます。必要に応じてさまざまな測定グラフを追加できます。
6. ダッシュボード名の上にポインターを配置すると、 [編集] オプションが右側に表示されます。ダッシュボード名を変更するには、 [編集] をクリックします。

ダッシュボードの削除

事業運営上の変更等でダッシュボードが必要でなくなった場合は、削除ができます。

：
ダッシュボードを削除すると、そのダッシュボードに追加されているすべてのグラフも削除されます。

手順

1. *Cloud Monitor コンソール*にログインします。
2. 左のナビゲーションウインドウで[ダッシュボード] > [カスタマイズダッシュボード]をクリックします。
3. [ダッシュボード] ドロップダウンリストから該当するダッシュボードを選択します。
4. ページの右上隅にある [ダッシュボードの削除] をクリックしてダッシュボードを削除します。

1.1.3 グラフの追加

デフォルトでは、**Cloud Monitor** は初期化された **ECS** ダッシュボードを作成します。 **ECS** インスタンスの追加データを表示するには、ダッシュボードへグラフまたはテーブルを追加できます。 ここでは、**Cloud Monitor** のダッシュボードで利用可能ないくつかの一般的な種類のグラフについて説明します。

注：

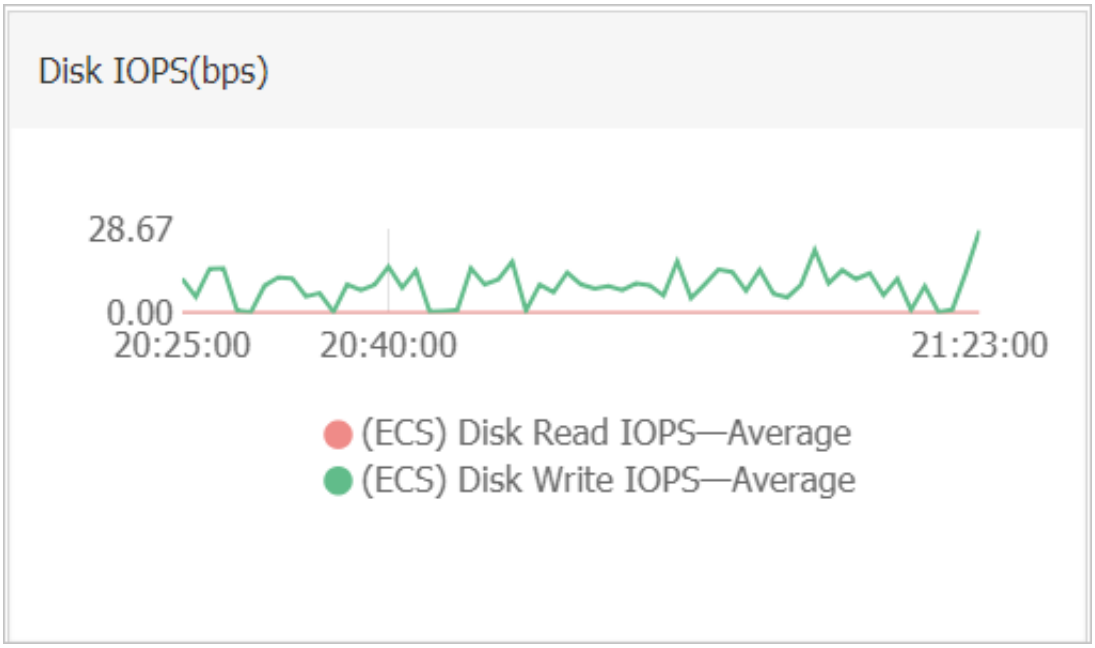
- デフォルトの **ECS** ダッシュボードは、次の **7** 種類のグラフを提供します。 **CPU** 使用率、ネットワークインバウンド帯域幅、 ネットワークアウトバウンド帯域幅、 ディスク **BPS**

ディスク **IOPS** 、 ネットワークインバウンドトラフィック、 ネットワークアウトバウンドトラフィックがあります。

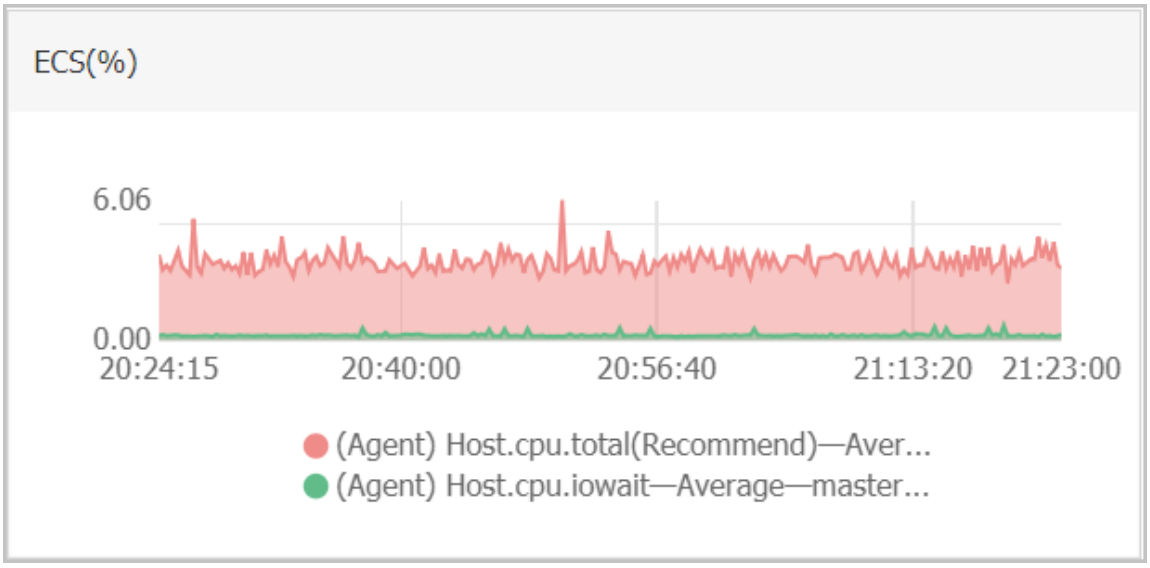
- 各折れ線グラフは、最大 **10** 本の折れ線を表示できます。
- 各エリアグラフには、最大 **10** 個のエリアを表示できます。
- 各テーブルには、最大 **1000** 個のソート済みデータレコードを表示できます。
- ヒートマップは、最大 **1000** のカラーブロックを表示できます。

グラフパラメータ

- グラフの種類
  - 折れ線グラフ: モニタリングデータの時系列表示。 複数のメトリクスを追加することができます。



  - エリアグラフ: モニタリングデータの時系列表示。 複数のメトリクスを追加することができます。

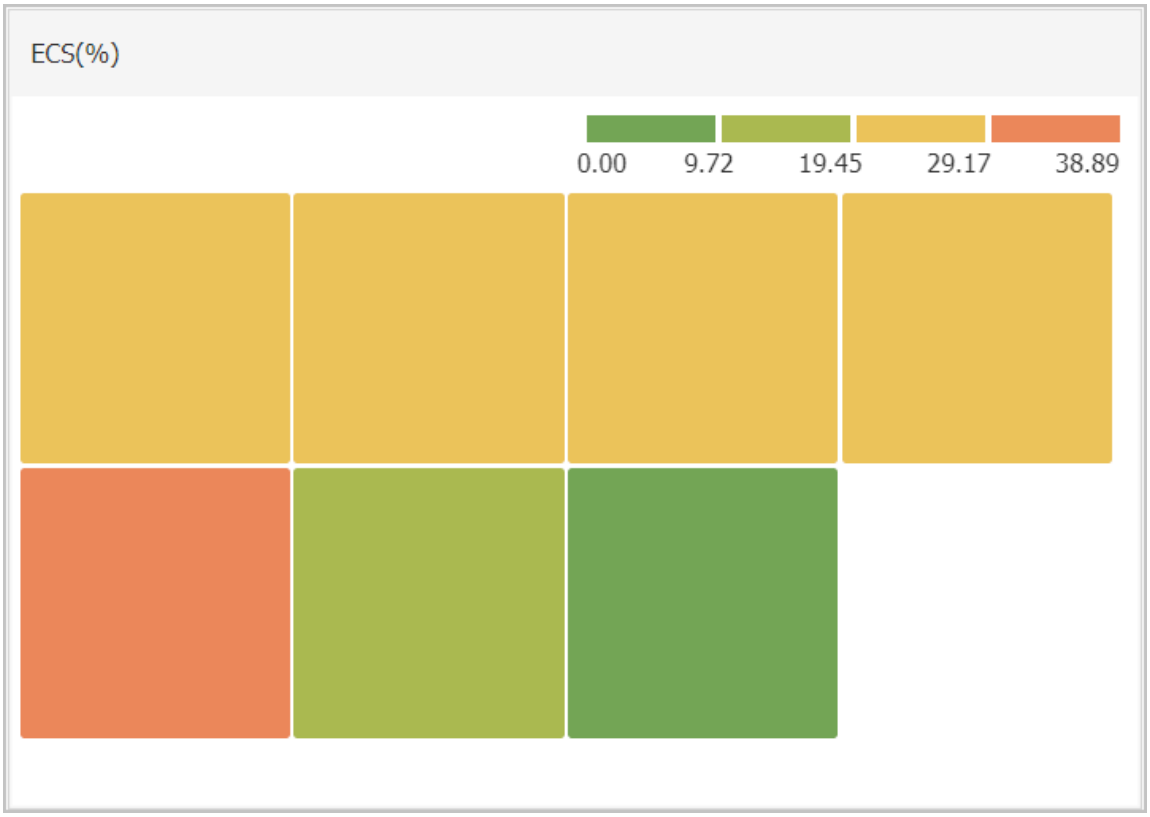


  - テーブル: リアルタイム測定データを降順で表示。 各テーブルは最大 1000 のデータレコードを表示でき、 最初の 1000 もしくは、最後から 1000 のデータレコードを表示します。 追加できる測定値は 1 つだけです。

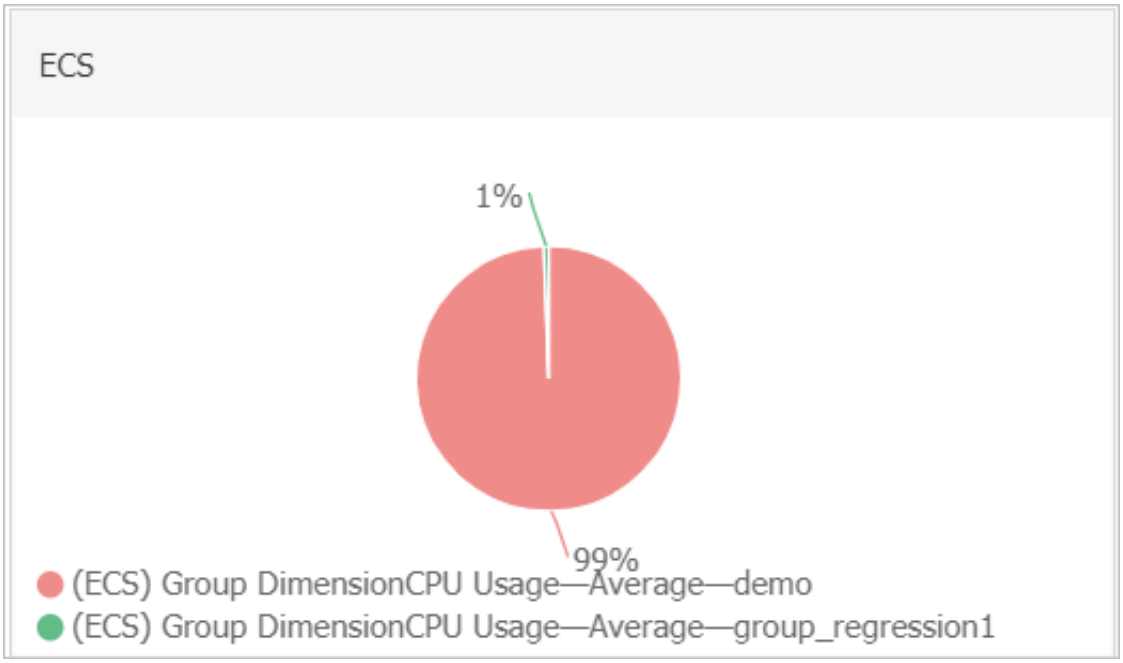
ECS(%)

Time	Dimensions	Maximum Value
2018-12-06 21:25:00	ESS-asg-yinna_test	100
2018-12-06 21:20:00	node-0003-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	55.56
2018-12-06 21:25:00	master-02-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.89
2018-12-06 21:25:00	master-03-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.1
2018-12-06 21:00:00	master-01-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	37.5
2018-12-06 21:00:00	node-0001-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	35.29
2018-12-06 21:20:00	node-0002-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	29.41

- ヒートマップ: リアルタイム測定データを表示。 ヒートマップは、複数のインスタンスに対する特定の測定値のリアルタイムデータの分布と比較を示します。 追加できる測定値は 1 つだけです。



- 円グラフ: リアルタイム測定データを表示。データ比較に使用できます。 追加できる測定値は 1 つだけです。

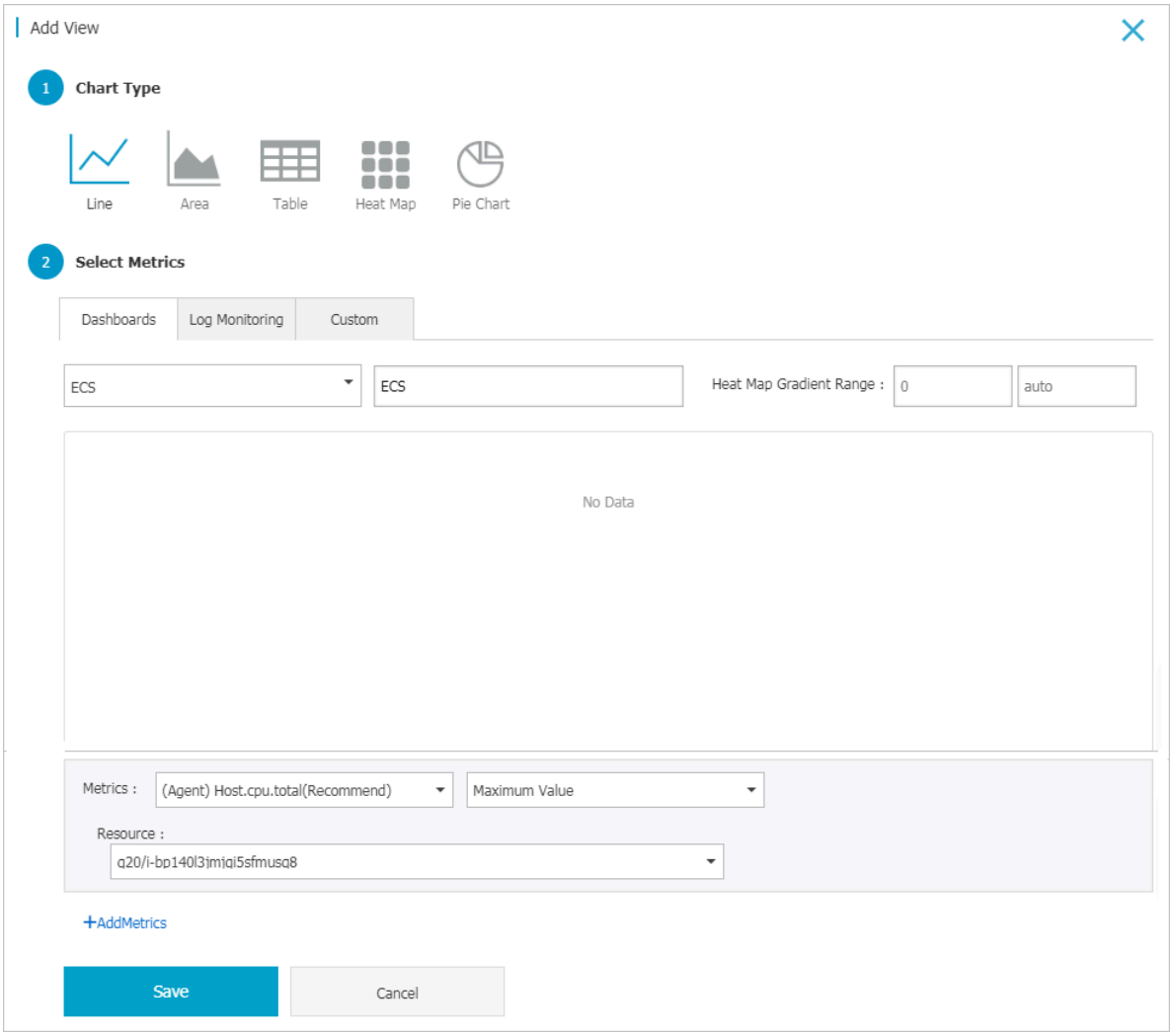


- ダッシュボード: **Alibaba Cloud** プロダクトをモニターします。
- ログモニタリング: ログモニタリングによって追加された測定値。
- カスタマイズ: カスタマイズモニタリングによって追加された測定値。
- メトリクス: **CPU** 使用率やメモリ使用率などのモニタリング測定値。
- 統計方法: 統計期間中に測定値を集計する方法。 一般的な統計的方法には、最大値、最小値、および平均値があります。
- リソース: アプリケーショングループまたはインスタンスを使用し、リソースをフィルタリングし、それらのリソースのモニタリングデータを表示できます。

手順

1. *Cloud Monitor コンソール*にログインします。
2. 左のナビゲーションウインドウで [ダッシュボード] > [カスタマイズダッシュボード]をクリックします。

3. ダッシュボードページの右上隅にある [ビューを追加] をクリックします。



4. グラフの種類を選択します。
5. [ダッシュボード] 、 [ログモニタリング] 、 [カスタマイズ] のタブの中から選択します。 この例では、 [ダッシュボード] タブをクリックします。
6. 該当する **Alibaba Cloud** プロダクトを選択して、グラフの名前を入力してください。
7. 測定値と統計方法を選択します。
   - 表示したい測定値を選択します。
   - 最大、最小、平均などから測定値データを集計する統計方法を選択します。
8. 測定値を追加するには、 [測定値の追加] をクリックして上記の手順を繰り返します。
9. [保存] をクリックします。 グラフがダッシュボードに表示されます。
10. グラフのサイズを変更する場合は、グラフの右罫線、下罫線、または右下隅をドラッグします。

2 ホストモニタリング

2.1 ホストモニタリングの概要

Cloud Monitor のホストモニタリングサービスを使用してサーバーにエージェントをインストールし、サーバーを体系的にモニターできます。ホストモニタリングは現在、**Linux** および **Windows OS** をサポートしています。

シナリオ

ホストモニタリングは、**Alibaba Cloud ECS** サーバーと他のベンダーが提供する仮想および物理マシンの両方で利用できます。

ホストモニタリングは、エージェントを使用してさまざまな **OS** 関連の測定値の統計を収集します。これにより、サーバーリソースの使用状況を収集し、トラブルシューティングのための測定値を取得できます。

ハイブリッドクラウドモニタリングのソリューション

ホストモニタリングはエージェントを使用してサーバー測定値を収集します。 エージェントをクラウド上やそれ以外の **ECS** サーバーまたは非 **ECS** サーバーにインストールし、クラウドの作動と停止をモニターできます。

エンタープライズレベルモニタリングのソリューション

ホストモニタリングは、他リージョンのサーバーをビジネスごとのサーバー管理のために同じグループに割り当てるアプリケーショングループ機能を提供します。これにより、**Alibaba Cloud** の異なるリージョンのサーバーを同じグループに割り当て、ビジネス運用の観点からより効率的なサーバー管理を行うことができます。 さらに、ホストモニタリングはグループベースのアラーム管理を提供します。 **1** つのアラームをグループ全体に設定することで運用及び **O&M** 効率と管理エクスペリエンス全般を大きく向上します。

注：

- ホストモニタリングは、**Linux** および **Windows** をサポートしていますが、**Unix** はサポートされていません。
- **Linux OS** へのエージェントのインストールには **root** 権限が必要であり、**Windows OS** へのエージェントのインストールには管理者権限が必要です。

- **TCP** ステータス統計機能は **Linux** の`netstat -anp` コマンドに類似した機能です。 **TCP** 接続が多数存在する場合、**CPU** 時間の大部分が消費されるため、この機能はデフォルトでは無効です。
  - **Linux** でこの機能を有効にするには、*cloudmonitor / config / conf.properties* 設定ファイルの `netstat.tcp.disable` を `false` に設定します。設定を変更した後、エージェントを再起動します。
  - **Windows** でこの機能を有効にするには、*C:\Program Files\Alibaba\cloudmonitor\config* 設定ファイルの `netstat.tcp.disable` を `false` に設定します。設定を変更した後、エージェントを再起動します。

モニタリング機能

ホストモニタリングでは、モニタリングリクエストと **O&M** ニーズを満たすため、**CPU**、メモリー、ディスク、ネットワークをカバーする **30** を超える測定基準が提供されます。 測定値の全リストは、ここ をクリックし表示します。

アラーム機能

ホストモニタリングは、すべての測定値に対してアラームサービスを提供し、インスタンス、アプリケーショングループ、およびすべてのリソースに対してアラームルールを設定できます。 ビジネスニーズに沿ったアラームサービスを使用できます。

グループにサーバーを追加後、ホストモニタリングリストから直接アラームサービスを使用、またはアプリケーショングループにアラームルールを適用することができます。

2.2 プロセスモニタリング

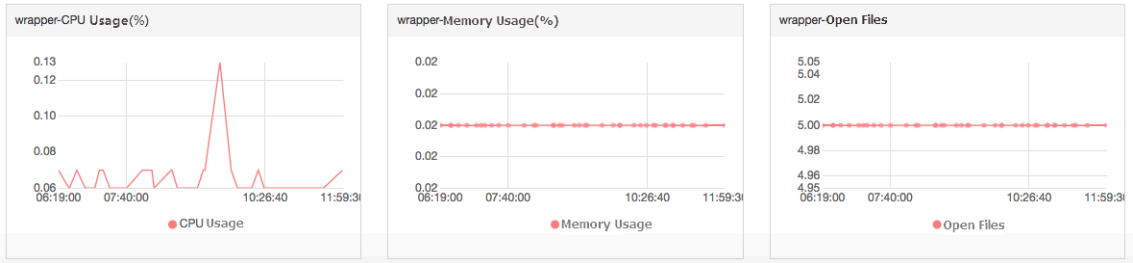
デフォルトでは、プロセスモニタリングを使用すると、**CPU** 使用率、メモリ使用量、およびアクティブなプロセスによって最近一定期間開かれたファイルの数に関する情報を収集できます。 プロセスキーワードを追加すると、そのキーワードを含むプロセス数が収集されます。

アクティブなプロセスのリソース消費量の表示

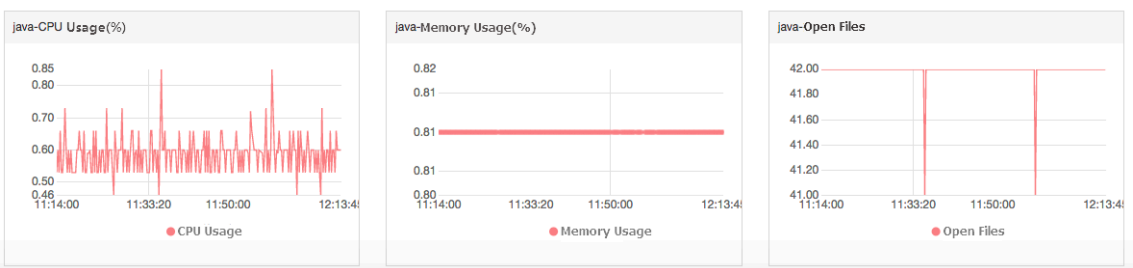
- **Cloud Monitor** エージェントは、毎分 **CPU** 使用率が最も高い上位 **5** つのプロセスを選別し、それぞれの **CPU** 使用率、メモリ使用量、およびこれらのプロセスによって開かれたファイルの数を記録します。
- プロセスの **CPU** およびメモリ使用量については、**Linux** の `top` コマンドを使用します。
- アクティブなプロセスによって開かれたファイルの数については、**Linux** の `lsof` コマンドを使用します。

注：

- プロセスが複数の CPU コアを占有している場合、収集された結果が複数の CPU コアの合計使用率を示しているため、CPU 使用率に表示される割合が 100 % を超える場合があります。
- 照会に指定された期間中に上位 5 つのプロセスが変更された場合、プロセスリストには、指定された期間中に上位 5 つとしてランク付けされたすべてのプロセスが表示されます。 リスト内の時間は、プロセスが最後にトップ 5 にランクインした日時を示します。
- CPU 使用率とメモリ使用率、および開かれているファイルの数は、上位 5 つのプロセスについてのみ収集されます。 そのため、照会に対して指定された期間にわたってプロセスが連続して上位 5 位にランク付けされていない場合、そのデータポイントはグラフで不連続に表示されます。 プロセスのデータポイントの密度は、サーバー上でのアクティビティの程度を示します。
  - 次の図に示すように、ラッパープロセスは、測定されるたびに上位 5 つのプロセスに連続的にランク付けされていません。 したがって、グラフ内のデータポイントはまばらで不連続です。 以下のグラフのデータポイントは、測定された特定の時間でプロセスが上位 5 位にランクされたことを意味します。



  - 次の図は、Java プロセスのグラフを示しています。 グラフ内のデータポイントは密集していて連続的です。 これは、プロセスが CPU 使用率の最も高い上位 5 つのプロセスに連続してランク付けされることを意味します。



指定したプロセスの数のモニタリング

プロセス数をモニタリングすることで、主要プロセスの数と実行可能性のステータスがわかります。 具体的には、関連プロセス数をモニターするための [プロセス数 (カウント)] グラフにプロセスキーワードを追加できます。

・ モニタリングするプロセスの追加

たとえば、次のプロセスがサーバーで実行されているとします。 `/ usr / bin / java -Xmx2300m -Xms2300m org.apache.catalina.startup.Bootstrap`、`/ usr / bin / ruby`、および `nginx -c /ect/nginx/nginx.conf`。 次に、以下の **6** つのキーワードを追加し (キーワードは、プロセス名、ファイルパス、パラメーター名 などの関連語にすることができます)、各ターゲットキーワードに対応するプロセス数が次のように出力されます。

- キーワード: `ruby`、収集されたプロセス数: **1**
- キーワード: `nginx`、収集されたプロセス数: **1**
- キーワード: `/usr/bin`、収集されたプロセス数: **2**
- キーワード: `apache catalina`、収集されたプロセス数: **1**
- キーワード: `nginx .conf`、収集されたプロセス数: **1**
- キーワード: `-c`、収集されたプロセス数: **1**

手順

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、 [ホストモニタリング] をクリックします。
3. ホストモニタリングの詳細ページにアクセスするために、対象ホストの名前をクリックするか、 [アクション] 内の [モニタリンググラフ] をクリックします。
4. 表示されたページで [プロセスモニタリング] タブをクリックします。
5. [プロセス数 (カウント)] グラフ上にポインターを置いて [プロセスの追加] をクリックします。
6. 表示された [プロセスモニターの追加] ページで、モニター対象とするプロセスの名前またはキーワードを追加して [追加] をクリックします。

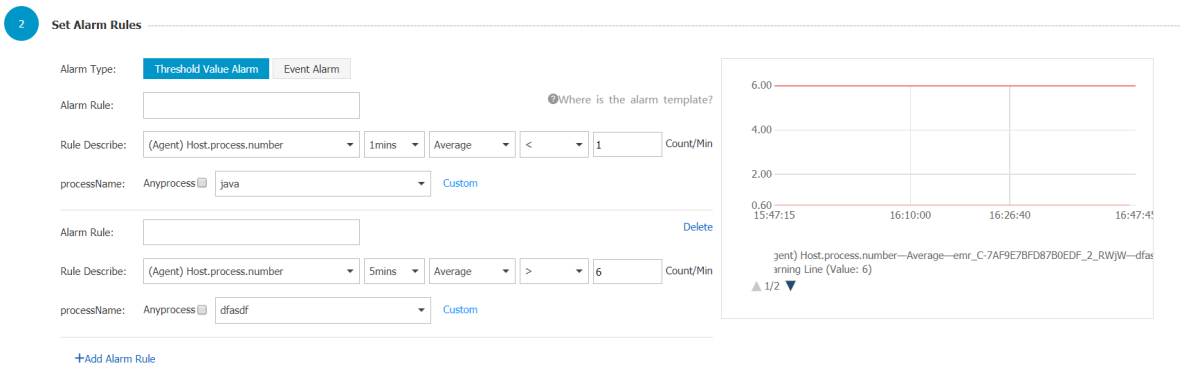
- モニタリング対象プロセスの削除

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[ホストモニタリング] をクリックします。
  3. ホストモニタリングの詳細ページにアクセスするために、対象ホストの名前をクリックするか、 [アクション] 内の [モニタリンググラフ] をクリックします。
  4. 表示されたページで [プロセスモニタリング] タブをクリックします。
  5. [プロセス数 (カウント)] グラフ上にポインターを置いて [プロセスの追加] をクリックします。
  6. 表示されたページで対象となるプロセスもしくはキーワードを探して[削除]をクリックします。

- アラームルールの設定

  指定したプロセスのモニタリングを設定したら、そのプロセスのアラームルールを設定できます。 その後、プロセス数が変わるとアラーム通知を受け取ることができます。

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで [ホストモニタリング] をクリックします。
  3. プロセスモニタリングのアラームルールの設定先とするホストを探して、[アクション] 列の [アラームルール] をクリックします。
  4. ページの右上隅にある [アラームルールの作成] をクリックします。
  5. [アラームルールの設定] エリアで、[ルールの説明] ドロップダウンリストから **[(Agent)Host.process.number]** を選択し、適切なアラームしきい値を設定し、モニター対象プロセスを [プロセス名] ドロップダウンリストからを選択します。 ホストに複数のプロセスが設定されている場合は、プロセス数が異なります。 [アラームルールの追加] をクリックして、一度に複数のアラームルールを設定できます。



2.3 ホストモニタリングのメトリクス

ホストモニタリングのメトリクスは、エージェント収集メトリクスと ECS ネイティブメトリクスに分けられます。 エージェント収集メトリクスは 15 秒ごとに収集され、ECS 基本メトリクスは 1 分ごとに収集されます。

 注 :

ECS 基本メトリックデータは、主に次の理由により、OS (オペレーティングシステム) メトリックデータと矛盾する可能性があります。

- 異なる統計頻度メトリックグラフデータには、測定期間中に収集された平均値があります。基本モニタリングの統計頻度は 1 分ですが、OS モニタリングの統計頻度は 15 秒です。 メトリックデータの変動が大きい場合、基本メトリックデータは OS メトリックデータよりも小さくなります。これは、前者のデータがピークを外れているためです。
- さまざまな統計観点基本モニタリングのネットワークトラフィック請求データには、ECS と Server Load Balancer 間の未請求ネットワークトラフィックは含まれません。 一方、OS モニタリングのネットワークトラフィック統計は、各ネットワークアダプターの実際のネットワークトラフィックを記録します。 したがって、OS モニタリングのネットワークデータは基本モニタリングのネットワークデータよりも大きくなります (つまり、エージェントが収集したデータは、実際に購入した帯域幅またはトラフィッククォータよりも大きくなります)。

エージェントで収集されるメトリクス

- CPU のメトリクス

  メトリクスの意味を理解するには、Linux の top コマンドをご参照ください。

メトリック	定義	単位	備考
Host.cpu.idle	現在アイドル状態の CPU の割合	%	現在の CPU のアイドル割合
Host.cpu.system	CPU として使用されている現在のカーネル空間の割合	%	このメトリックは、システムコンテキストの切り替えによる消費量を測定します。 値が大きい場合は、多くのプロセスまたはスレッドがサーバー上で実行されていることを示します。

メトリック	定義	単位	備考
Host.cpu.user	このメトリックは、ユーザープロセスの **CPU** 消費量を測定します。	**%**	ユーザプロセスによる **CPU** 消費
Host. CPU iowait	現在 **IO** 操作を待機している **CPU** の割合	**%**	これは比較的高い値であり、これは頻繁に **IO** 操作が行われることを意味します。
Host.cpu.other	その他の **CPU** 使用率	**%**	その他の消費量、**(Nice + sofpratt q + IRQ +stolen)** の形式で計算されます。
Host.cpu. totalUsed	現在消費されている合計 **CPU** の割合	**%**	上記の **CPU** 使用量の合計。通常はアラーム用に使用されます。

・ メモリ関連モニター

インジケーターの意味を理解するには、**free** コマンドをご参照ください。

メトリクス	定義	単位	説明
Host.mem.total	総メモリ	バイト	サーバーメモリ合計
Host.mem.used	使用メモリ量	バイト	ユーザプログラムが使用するメモリ+バッファ+ キャッシュ、バッファに使用されるメモリ量、およびキャッシュによって使用されるシステムキャッシュに使用されるメモリ量
Host.mem. actualused	ユーザーが実際に使用しているメモリ	バイト	計算式**: (**使用済み - バッファー - キャッシュ済み**)**
Host.mem.free	メモリ残量	バイト	**(**合計メモリ - 使用されているメモリの量**)** として計算

メトリクス	定義	単位	説明
Host.mem. freeutilization	メモリ残量の割合	**%**	**(**メモリ残量 **/** メモリ総量 **×** 100**)** として計算
Host.mem. usedutilization	メモリ使用量	**%**	**(**実際の使用量**/**合計 **×** 100**)** として計算

・ 平均システム負荷のメトリクス

メトリクスの意味を理解するには、**Linux** の **top** コマンドをご参照ください。 モニタリング項目の値が大きいほど、システムがよりビジーであることを示します。

メトリクス	定義	単位
Host.load1	過去 **1** 分間の平均システム負荷で、**Windows** オペレーティングシステムにはこのメトリックはありません	なし
Host. load5	過去 **5** 分間の平均システム負荷で、**Windows** オペレーティングシステムにはこのメトリックはありません	なし
Host. load15	過去 **15** 分間の平均システム負荷で、**Windows** オペレーティングシステムにはこのメトリックはありません	なし

・ ディスク関連のメトリクス

- ディスク使用量と **i** ノード使用量は、**Linux** の **DF** コマンドをご参照ください。
- ディスク読み取り**/**書き込みメトリクスは、**Linux** の **iostat** コマンドをご参照ください。
-

メトリック	定義	単位
Host.diskusage.used	ディスク上の使用済み記憶域	バイト
Host.disk.utilization	ディスクの使用状況	**%**
Host.diskusage.free	ディスク上の残りの記憶域	バイト
Host.diskussage.total	総ディスク容量	バイト
Host.disk.readbytes	**1** 秒間にディスクによって読み取られたバイト数	バイト**/**秒
Host.disk.writebytes	**1** 秒間にディスクに書き込まれたバイト数	バイト**/**秒

メトリック	定義	単位
Host.disk.readiops	**1** 秒当たりのディスクへの読み取り要求数	回/秒
Host.disk.writeiops	**1** 秒当たりのディスクへの書き込み要求数	回/秒

・ ファイルシステムモニター

メトリクス	定義	単位	説明:
Host.fs.inode	**i** ノード 使用率、**Unix / Linux** システムでは、ファイルを識別するために **i** ノード 番号が使用され、ディスクには空きがあります。 ただし、**i** ノード が割り当てられると新しいファイルをディスクに作成できなくなります。 **Windows** オペレーティングシステムにはこのメトリックはありません。	**%**	**i** ノード 番号はファイルシステムファイルの数を表し、小さなファイルが多数あると **i** ノード の使用量が高くなりすぎることがあります。

・ ネットワーク関連のメトリクス

- **TCP** 接続の収集については、**Linux** の **iftop** コマンドと **SS** コマンドをご参照ください。
- **TCP** 接続数はデフォルトで収集されます。 デフォルトでは、**TCP_TOTAL** (総接続数)、**ESTABLISHED** (通常は確立された接続数)、および **NON_ESTABLISHED** (確立された状態にない接続数) ごとに、**TCP** 接続数に関する統計が収集されます。 各状態の接続数を取得する場合は、次の手順を実行します。

  ■ Linux

  設定ファイル "*cloudmonitor/config/conf.properties*" の `netstat.tcp.disable` を `false` に設定して、データ収集を有効にします。 設定を変更したら、

エージェントを再起動してください。 設定を変更したら、エージェントを再起動してください。

■ **Windows**

設定ファイル "*C:\"Program\Alibaba\cloudmonitor\config*" の `netstat.tcp.disable` を `false` に設定して、データ収集を有効にします。 設定を変更したら、エージェントを再起動してください。

メトリック	定義	単位
Host.netin.rate	**1** 秒間にネットワークアダプターのアップリンク帯域幅によって受信されたビット数	ビット/秒
Host.netout.rate	**1** 秒間にネットワークアダプターのダウンリンク帯域幅によって送信されたビット数	ビット/秒
Host.netin.packages	**1** 秒間にネットワークアダプターが受信したパケット数	パケット/秒
Host.netout.packages	ドライブによって検出された着信エラーパケットの数	パケット/秒
Host.netin.errorpackage	ドライブによって検出された発信エラーパケットの数	パケット/秒
Host.netout.errorpackages	ドライブによって検出された発信エラーパケットの数	パケット/秒
Host.tcpconnection	**LISTEN**、**SYN_SENT**、**ESTABLISHED**、**SYN_RECV**、**FIN_WAIT1**、**CLOSE_WAIT**、**FIN_WAIT2**、**LAST_ACK**、**TIME_WAIT**、**CLOSING**、**CLOSED** など、さまざまな状態の **TCP** 接続の数	

・ プロセスのメトリクス

- プロセス固有の **CPU** 使用率とメモリ使用率の詳細については、**Linux** の **top** コマンドをご参照ください。 **CPU** 使用率は、複数のカーネルの **CPU** 消費量を示します。
- **Host.process.openfile** については、**Linux** の **lsof** コマンドをご参照ください。
- **Host.process.number** については、**Linux** の **ps aux | grep 'keyword'** コマンドをご参照ください。

メトリック	定義	単位
Host.process.cpu	プロセスの **CPU** 使用率	**%**
Host.process.memory	プロセスのメモリ使用量	**%**
Host.process.openfile	プロセスによって開かれたファイルの数	ファイル
Host.process.number	指定されたキーワードに一致するプロセスの数	プロセス

ECS のメトリクス

ホストが **ECS** サーバーの場合、**ECS** インスタンスを購入すると、エージェントをインストールしなくても以下のメトリクスが提供されます。 収集粒度は **1** 分です。

メトリック	定義	単位
ECS.CPUUtilization	**CPU** 使用率	**%**
ECS.InternetInRate	インターネットインバウンドトラフィックの平均レート	ビット/秒
ECS.IntranetInRate	イントラネットインバウンドトラフィックの平均レート	ビット/秒
ECS.InternetOutRate	インターネットアウトバウンドトラフィックの平均レート	ビット/秒
ECS.IntranetOutRate	イントラネットアウトバウンドトラフィックの平均レート	ビット/秒
ECS.SystemDiskReadbps	**1** 秒間にシステムディスクから読み取られたバイト数	バイト/秒
ECS.SystemDiskWritebps	**1** 秒間にシステムディスクに書き込まれたバイト数	バイト/秒
ECS.SystemDiskReadOps	**1** 秒間にシステムディスクからデータが読み取られた回数	回/秒

メトリック	定義	単位
ECS.SystemDiskWriteOps	**1** 秒間にデータがシステムディスクに書き込まれた回数	回/秒
ECS. internetin	インターネットインバウンドトラフィック	バイト
ECS.InternetOut	インターネットアウトバウンドトラフィック	バイト
ECS.IntranetIn	イントラネットインバウンドトラフィック	バイト
ECS.IntranetOut	イントラネットアウトバウンドトラフィック	バイト

2.4 アラームルールサービス

ホストモニタリングには、アラームルールサービスオプションがあります。 このアラームサービスを使用して、ホストモニタリングで単一のサーバーにアラームルールを設定、または指定したグループにサーバーを追加後にグループ単位でアラームポリシーを設定できます。 詳しくは、「アラームルールの管理」をご参照ください。

アラームルールの作成

1. *Cloud Monitor* コンソールにログインします。
2. ホストモニタリングページのアラームルールに移動します。
3. 右上隅の[アラームルールの作成]をクリックします。
4. アラームルールの作成ページでアラームパラメーターを設定します。 必要な情報をすべてのフィールドに入力します。 詳しくは、「アラームルールの管理」をご参照ください。
5. **[確認]** をクリックし、アラームルール設定を保存します。

アラームルールの削除

1. **Cloud Monitor** のホストモニタリング ページを表示します。
2. **[アラームルール]** タブをクリックします。
3. アラームルールに対応した削除アクションをクリックし、**1** つのアラームルールを削除します。 複数のルールを選択した場合、一覧の下にある削除ボタンをクリックし複数のルールを一括で削除します。

アラームルールの変更

1. **Cloud Monitor** のホストモニタリング ページを表示します。

2. [アラームルール] タブをクリックします。
3. [変更] をクリックし、アラームルールを変更します。

アラームルールの表示

1. **Cloud Monitor** のホストモニタリングページを表示します。
2. [アクション] タブの [アラームルール] をクリックし、一つのサーバーのアラームルールを表示します。
3. アラームルールの ページに移動し、すべてのアラームルールを表示します。

2.5 Cloud Monitor Java エージェントの紹介

Cloud Monitor は、サーバーを体系的にモニタリングすることを可能にする強力なホストモニタリングエージェントを提供します。 以下はインストールとリソースの使用法を含む、このサービスの簡単な紹介です。

インストールパス

- **Linux:** */usr/local/cloudmonitor*
- **Windows:** *C:\Program Files\Alibaba\cloudmonitor*

プロセス情報

エージェントのインストール後、サーバー上で次の **2** つのプロセスが実行されます。

- */usr/local/cloudmonitor/jre/bin/java*
- */usr/local/cloudmonitor/wrapper/bin/wrapper*

ポートの説明

- ローカルホストの **TCP** ポート **32000** にアクセスし、デーモンを待ち受けます。
- リモートサーバーの **TCP** ポート **3128**、**8080**、または **443** が、ハートビートモニタリングおよびモニタリングデータレポートのためにアクセスされます。 ポート **3128** または **8080** は **Alibaba Cloud** ホストに使用され、ポート **443** は他のホストに使用されます。
- **Cloud Monitor** エージェントのアップグレードのためにリモートサーバーの **HTTP** ポート **80** にアクセスします。

エージェントログ

- モニタリングデータのログは、*/usr/local/cloudmonitor/logs* にあります。
- 起動、シャットダウン、およびデーモンのログは、*/usr/local/cloudmonitor/wrapper/logs* にあります。

- ログレベルは、*/usr/local/cloudmonitor/config/log4j.properties* を編集することで変更できます。

リソース使用量

- **/usr/local/cloudmonitor/wrapper/bin/wrapper** プロセスは、**CPU** 使用量がほとんどない状態で、約 **1 MB**のメモリーを占有します。
- **/usr/local/cloudmonitor/jre/bin/java** プロセスは、約 **70 MB**のメモリーと **1** コアの **CPU** 使用量の **1%** から **2%** を占めます。
- インストールパッケージは **70 MB**で、インストール完了後に約 **200 MB** のディスク容量を占有します。
- ログは最大 **40 MB** のスペースを使用し、**40 MB** を超えて使用すると消去されます。
- モニタリングデータは **15** 秒ごとに送信され、約 **10 KB** のイントラネット帯域幅を占有します。
- ハートビートデータは **3** 分ごとに送信され、約 **2 KB** のイントラネット帯域幅を占有します。

外部依存関係

- **Cloud Monitor** の **Java** エージェントは **JRE 1.8** に組み込まれています。
- **Java** サービスラッパーは、デーモン、起動時の起動、および **Windows** サービスの登録に使用されます。
- `ss -s` コマンドは **TCP** 接続をキャプチャするために使用されます。現在のシステムにこのコマンドがない場合は、**ip route** をインストールする必要があります。

インストール

「*Cloud Monitor Java エージェントのインストール*」をご参照ください。

Alibaba Cloud が提供していないホストへのエージェントのインストール方法

1. *Cloud Monitor コンソール*にログインします。
2. 左のナビゲーションウィンドウで、 **[ホストモニタリング]** をクリックします。
3. 表示されたページの上部にある **[Aliyun ecs** 未インストール**]** をクリックします。 表示される **[**モニターインストールガイド **]** ダイアログボックスで、エージェントおよびホストの種類を選択し、対応するインストール方法を表示します。

2.6 Cloud Monitor Java エージェントのインストール

Linux へ Cloud Monitor Java エージェントのインストール

頻繁に使用されているコマンド

```
# Running status
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status

# Start
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh start

# Stop
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh stop

# Restart
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh restart

# Uninstall
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh remove && \
rm -rf /usr/local/cloudmonitor
```

インストールコマンド

コマンドはリージョンによって異なります。 対応するコマンドをコピーし、サーバー上で **root** ユーザーとして実行します。

中国 (青島) **cn-qingdao**

```
REGION_ID=cn-qingdao VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-qingdao.oss-cn-qingdao-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (北京) **cn-beijing**

```
REGION_ID=cn-beijing VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-beijing.oss-cn-beijing-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (張家口) **cn-zhangjiakou**

```
REGION_ID=cn-zhangjiakou VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-zhangjiakou.oss-cn-zhangjiakou-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (フフホト) **cn-huhehaote**

```
REGION_ID=cn-huhehaote VERSION=1.3.7 \
```

```
bash -c "$(curl https://cms-agent-cn-huhehaote.oss-cn-huhehaote-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (杭州) **cn-hangzhou**

```
REGION_ID=cn-hangzhou VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (上海) **cn-shanghai**

```
REGION_ID=cn-shanghai VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-shanghai.oss-cn-shanghai-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (深セン) **cn-shenzhen**

```
REGION_ID=cn-shenzhen VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-shenzhen.oss-cn-shenzhen-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国 (香港) **cn-hongkong**

```
REGION_ID=cn-hongkong VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-hongkong.oss-cn-hongkong-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

米国 (シリコンバレー) **us-west-1**

```
REGION_ID=us-west-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-us-west-1.oss-us-west-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

米国 (バージニア) **us-east-1**

```
REGION_ID=us-east-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-us-east-1.oss-us-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

シンガポール **ap-southeast-1**

```
REGION_ID=ap-southeast-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-1.oss-ap-southeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

オーストラリア (シドニー) **ap-southeast-2**

```
REGION_ID=ap-southeast-2 VERSION=1.3.7 \
```

```
bash -c "$(curl https://cms-agent-ap-southeast-2.oss-ap-southeast-2-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

マレーシア (クアラルンプール) **ap-southeast-3**

```
REGION_ID=ap-southeast-3 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-3.oss-ap-southeast-3-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

インドネシア (ジャカルタ) **ap-southeast-5**

```
REGION_ID=ap-southeast-5 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-5.oss-ap-southeast-5-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

日本 (東京) **ap-northeast-1**

```
REGION_ID=ap-northeast-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-northeast-1.oss-ap-northeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

インド (ムンバイ) **ap-south-1**

```
REGION_ID=ap-south-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-south-1.oss-ap-south-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

ドイツ (フランクフルト) **eu-central-1**

```
REGION_ID=eu-central-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-eu-central-1.oss-eu-central-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

イギリス (ロンドン) **eu-west-1**

```
REGION_ID=eu-west-1 VERSION=1.3.7 \ bash -c "$(curl https://cms-agent
-eu-west-1.oss-eu-west-1-internal.aliyuncs.com/release/cms_instal
l_for_linux.sh)"
```

UAE (ドバイ) me-east-1

```
REGION_ID=me-east-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-me-east-1.oss-me-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国ファイナンスクラウド (杭州) **cn-hangzhou**

```
REGION_ID=cn-hangzhou VERSION=1.3.7 \
```

```
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

中国ファイナンスクラウド (上海) **cn-shanghai-finance-1**

```
REGION_ID=cn-shanghai-finance-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-shanghai-finance-1.oss-cn-
shanghai-finance-1-pub-internal.aliyuncs.com/release/cms_instal
l_for_linux.sh)"
```

中国ファイナンスクラウド (深セン) **cn-shenzen-finance-1**

```
REGION_ID=cn-shenzhen-finance-1 VERSION=1.3.7 \
bash -c "$(curl http://cms-agent-cn-shenzhen-finance-1.oss-cn-shenzhen
-finance-1-internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Windows へ Cloud Monitor Java エージェントのインストール

インストール手順

1. オペレーティングシステムのバージョンに合わせて *64 bit バージョン*または *32 bit バージョン*のエージェントをダウンロードします。
2. *C:/Program Files/Alibaba* に *cloudmonitor* というフォルダを作成します。
3. インストールパッケージを *C:/Program Files/Alibaba/cloudmonitor* に解凍します。
4. *C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/InstallApp-NT.bat* をダブルクリックし、管理者として **Cloud Monitor** をインストールします。
5. *C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/StartApp-NT.bat* をダブルクリックし、管理者として **Cloud Monitor** を起動します。
6. インストールの完了後、**Windows** のサービスパネルから **Cloud Monitor** を表示、起動、および停止できます。

アンインストール手順

1. **Windows** のサービスパネルから **Cloud Monitor** を停止します。
2. 管理者として*C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/UninstallApp-NT.bat* を実行して **Cloud Monitor** を削除します。
3. インストールディレクトリで、 *C:/Program Files/Alibaba/cloudmonitor* ディレクトリ全体を削除します。

インターネットに接続していない状態でエージェントをダウンロードする

インターネットに接続していない場合は、イントラネットからインストールパッケージをダウンロードできます。 たとえば、ホストのリージョンが青島で、ホストが **64** ビットシステムを使用

している場合、イントラネットのダウンロードアドレスは次のようになります。*http://cms-agent-cn-qingdao.oss-cn-qingdao.aliyuncs.com/release/1.3.7/windows64/agent-windows64-1.3.7-package.zip*

- 他のリージョンのホストの場合には `cn-qingdao` を該当するリージョン **ID** に変更します。
- **32** ビットシステムを使用するホストの場合は、 `windows64` を `windows32` に変更します。
- 別のバージョンでは、 `1.3.7`を対応するバージョン番号に変更します。

セキュリティ設定手順

次の表は、**Cloud Monitor** エージェントがサーバーとの対話に使用するポートの一覧です。 セキュリティソフトウェアがこれらのポートを無効にすると、モニタリングデータの収集に失敗することがあります。 **ECS** サーバーに高度なセキュリティが必要な場合は、次のいずれかの **IP** アドレスをホワイトリストに追加できます。

注：

Cloud Monitor の将来のバージョンアップデートおよびメンテナンスにより、以下の **IP** アドレスが変更される可能性があります。 ファイアウォールルールの設定を簡単にするために、**100.100** ネットワークセグメントを出力方向に直接許可することを推奨します。 このネットワークセグメントは **Alibaba Cloud** のイントラネット用に予約されており、セキュリティ上の問題はありません。

リージョン	IP	方向	説明
中国 (杭州) **cn-hangzhou**	**100.100.19.43:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.45.73:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (北京) **cn-beijing**	**100.100.18.22:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.18.50:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (青島) **cn-qingdao**	**100.100.36.102:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用

リージョン	IP	方向	説明
	100.100.15.23:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (深セン) **cn-shenzhen**	**100.100.0.13:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.0.31:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (香港) **cn-hongkong**	**100.103.0.47:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.103.0.45:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (フフホト) **cn-huhehaote**	**100.100.80.135:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.12:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (張家口) **cn-zhangjiakou**	**100.100.80.92:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.0.19:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (上海) **cn-shanghai**	**100.100.36.11:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.36.6:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
中国 (成都) **cn-chengdu**	**100.100.80.229:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用

リージョン	IP	方向	説明
	100.100.80.14:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
米国 (バージニア)	**100.103.0.95:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.103.0.94:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
米国 (シリコンバレー) **us-west-1**	**100.103.0.95:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.29.7:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
ドイツ (フランクフルト) **eu-central-1**	**100.100.80.241:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.72:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
イギリス (ロンドン) **eu-west-1**	**100.100.0.3:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.0.2:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
シンガポール **ap-southeast-1**	**100.100.30.20:3128**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.103.7:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
オーストラリア (シドニー) **ap-southeast-2**	**100.100.80.92:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用

リージョン	IP	方向	説明
	100.100.80.13:80 **[47.91.39.6:443]**	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
マレーシア (クアラルンプール) **ap-southeast-3**	**100.100.80.153:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.140:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
インドネシア (ジャカルタ) **ap-southeast-5**	**100.100.80.160:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.180:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
UAE (ドバイ) **me-east-1**	**100.100.80.142:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.151:80 **[47.91.99.5:443]**	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
日本 (東京) **ap-northeast-1**	**100.100.80.184:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.137:80 **[47.91.8.7:443]**	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用
インド (ムンバイ) **ap-south-1**	**100.100.80.152:8080**	**Egress**	構成管理、その他の管理および制御操作のモニタリングに使用
	100.100.80.66:80	**Egress**	**Cloud Monitor** にモニタリングデータを収集するために使用

リソース消費

- インストールパッケージのサイズ**: 75 MB**

- インストール後に占有されていたスペース: **200 MB**
- メモリ: **64 MB**
- **CPU: 1%** 未満
- ネットワーク: イントラネット、インターネット帯域幅の使用なし

よくある質問

- **Cloud Monitor** ログはどこに保存されますか？
  - **Linux:** */usr/local/cloudmonitor/logs*
  - **Windows:** *C:/Program Files/Alibaba/cloudmonitor/logs*
- エージェントによって占有されているポートと私のサービスによって使用されているポートが競合する場合はどのようにすればよいですか？
  1. **Cloud Monitor** 設定ファイル */usr/local/cloudmonitor/wrapper/conf/wrapper.conf* でポートの範囲を変更します。
  2. **Cloud Monitor** を再起動します。

```
wrapper.port.min=40000
wrapper.port.max=41000
wrapper.jvm.port.min=41001
wrapper.jvm.port.max=42000
```

2.7 エージェントのリリースノート

1.2.11

機能の最適化とバグ修正。ローカルヘルスチェック機能を使用している場合には、このエージェントバージョンにアップグレードする必要があります。

新機能

- **Telnet** および **HTTP** プロトコルをサポートするローカルおよびリモートプロトコル検出を追加

機能

- インストールスクリプトの一時的なダウンロードディレクトリとして **"tmp"** ディレクトリを使用した場合に、特権昇格ループホールが発生する場合がありましたが、これを修正しました。
- 同じディスクが複数回アタッチされた際に、同じデバイスデータを送信するバグがありましたが、これを修正しました。

- いくつかのプロセスがパスを取得できず、名前が固定されるというバグがありましたが、これを修正しました。
- ファイルのダウンロード方法を最適化しました。また、ダウンロードプロセスの結果として、モニタリングプロセスがブロックされることのないようにしました。

1.1.64

機能の最適化グ修正。 **CentOS 7.2** より後のエージェントバージョンを使用している場合には、このバージョンにアップグレードすることを推奨します。

- **CentOS 7.2** より後のエージェントバージョンで、**MemAvailable** フィールドを使用してメモリ使用量取得ロジックを調整し、正確なメモリ使用量を計算できるように最適化しました。

1.1.63

機能の最適化とバグ修正

- デフォルトの **wrapper** ログを **info** レベルに調整しました。
- エラーレベルログ情報を追加して、障害検知を最適化しました。
- デバッグレベルのログからメモリリークが発生するリスクがありましたが、それを修正しました。

1.1.62

機能の最適化とバグ修正

- エージェントインストールの成功率を上げるために、**HTTP** プロキシ選択ロジックを最適化しました。
- 障害検知の向上のためにキーログを追加しました。

1.1.61

機能の最適化とバグ修正

- いくつかのシステムにおいて、異常なプロセスユーザー名収集により発生していた間違った **topN** プロセス収集を修正しました。

1.1.59

機能の最適化とバグ修正

- プロセスカウント収集方法を最適化して、パフォーマンスを向上させました。
- プロセスモニタリングを調整して、**CloudMonitor** エージェントプロセスが、プロセスカウント収集から除外されるようにしました。

3 サイトモニタリング

3.1 サイトモニタリングの作成

ここでは、サイトモニタリングタスクを作成する方法について説明します。 サイトモニタリングタスクを使用して、ネットワークの品質とサービスのパフォーマンスを分析することが可能です。

背景情報

サイトモニタリングは、ユーザーアクセスのリクエストをシミュレートして、サービスに対するユーザーの挙動をよりよく分析するのに役立つ機能です。 この機能は、すべての **Alibaba Cloud** リージョンで使用できます。 サイトモニタリングを使用すると、次のアクションを実行できます。

- データ (ドメインネームサーバー **(DNS)** がドメイン名を解決する時間、接続が確立される時間、エンドポイントからリクエストを送信してから最初のパケットを受信するまでの時間、パケットのダウンロードが開始される時間など) を取得するサイトモニタリングタスクを作成します。 これらのデータは、サービスにおける問題の検出や、パフォーマンスの向上に役立ちます。
- **CloudMonitor** コンソールでモニタリングするサイトとピアのサイトをモニタリング項目として追加し、モニタリングするサイトとピアのサイトでネットワーク品質とサービスパフォーマンスを検出するプローブポイントを指定します。
- ユーザーの挙動をシミュレートし、すべての **Alibaba Cloud** リージョンからアクセスリクエストを送信します。

利用開始前に

- サイトモニタリングタスクを作成時にアラームルールを設定する場合は、先に連絡先と連絡先グループを作成することを推奨します。 アラームルールの設定時に連絡先グループを選択できます。アラームが報告されると連絡先グループが通知を受け取ります。 連絡先と連絡先グループの作成方法の詳細については、「アラート連絡先とアラート連絡先グループの作成」をご参照ください。
- アラームルールを設定時にアラームコールバック機能を有効化する場合は、インターネット経由でアクセス可能なコールバック **URL** を提供する必要があります。 **O&M** システムまたはメッセージシステムで **URL** コールバック機能を有効化します。

手順

> 注：
> サイトモニタリングタスクを作成時に、必要に応じてアラームルールの設定有無を選択できます。

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[新しいサイトモニター] > [サイト管理] を選択します。
3. サイトモニタリングページで、 [新しいモニタリングタスク] をクリックします。
4. 新しいタスクページで、サイトモニタリングタスクの基本情報を設定します。
   - [モニタリングタイプ] ：モニタリングプロトコルを選択します。 有効値： **HTTP | PING | TCP | UDP | DNS | SMTP | POP3 | FTP .**
   - [タスク名] ：タスクの名前。 タスク名には、**4 ～ 100** 文字 (文字、数字、アンダースコア (_) を含む) が含まれます。
   - [モニタリングアドレス] ：モニタリングする対象アドレス。 複数のアドレスがある場合は改行して分割します。 タスク設定を保存すると、各アドレスがジョブとして保存されます。
   - [モニタリング頻度]：対象アドレスが定期的にモニタリングされる間隔。 有効値：**1** 分 | **5** 分 | **15** 分 | **30** 分 | **60** 分。 たとえば、[モニタリング頻度] を [1 分] に設定した場合、各プローブポイントは **1** 分間隔で対象アドレスをモニタリングします。
   - [詳細設定] ：利用可能な詳細設定は、**Monitor Type** パラメーターで指定されたプロトコルに応じて変わります。 詳細については、「モニタリングタイプの詳細設定」をご参照ください。
5. プローブポイントを選択またはカスタマイズします。
   - [ECS プローブポイント] ：プローブポイントを選択します。
   - [プローブポイントの詳細オプション]：プローブポイントをカスタマイズします。
6. オプション。 アラームルールの設定
   - 次の **4** つの[可用性] オプションがあります： [利用可能なプローブポイントの割合] 、[利用可能なプローブポイントの数] 、[任意のステータスコード (独立したアラーム)] 、 [すべ

てのステータスコード (独立したアラーム)]。 検出結果の対象アドレスのステータスコードが 399 より大きい場合、対象アドレスはアクセス不可となります。 利用可能なプローブポイントの数は、モニタリング期間内にステータスコードが 400 未満の検出結果件数に等しくなります。 利用可能なプローブポイントの割合は、次のように算出されます。

利用可能なプローブポイントの割合 = (モニタリング期間内のステータスコードが 400 未満の検出結果件数/同じモニタリング期間内の検出結果の総数) × 100

- [平均レスポンス時間] ：モニタリング期間内で、選択したすべてのプローブポイントがレスポンスに要する平均時間。
- [アラーム再試行回数] : メトリックがしきい値を連続して超えるとアラームが報告される連続回数。 このパラメーターは、モニタリングデータの不定期な変動を検出するために使用されます。
- [連絡先グループ] ：アラーム通知を受信する連絡先グループ。
- [通知方法] ：アラーム通知の受信方法。
- [詳細設定] ： [チャンネルサイレント時間]、[有効時間]、[アラームコールバック]の 3 つのオプションがあります。
  - [チャンネルサイレント時間]：報告されたアラームが解除されるまで、定期的に通知が送信される間隔。
  - [有効時間] ：アラームルールの有効期間。 CloudMonitor が指定された期間内の間のみアラーム通知を送信します。 指定された期間を過ぎると、CloudMonitor では報告されたアラームの記録のみを行い、通知は送信されません。
  - [アラームコールバック] ：インターネット経由でアクセス可能な URL を入力します。 CloudMonitor がこの URL にアラーム情報を含む POST リクエストを送信します。 HTTP プロトコルに基づいて URL を入力する必要があります。

7. [作成] をクリックします。

モニタリングタイプの詳細設定

- **HTTP** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Address	**URL**	必須	入力したすべてのアドレスにスキーマを含めることを推奨します。例：**https://www.alibabacloud.com** スキーマを含まないアドレスが入力された場合、**CloudMonitor** がアドレスに **http** をスキーマとして追加します。
Request content	フォームデータまたは **JSON** オブジェクト	省略可能	リクエストコンテンツが **JSON** 形式の場合、入力した **JSON** オブジェクトが必ず中括弧 ({} で囲われているようにしてください。 **JSON** オブジェクトを中括弧 ({}) に含めない場合、**CloudMonitor** はそれらをフォームデータとみなします。
Request method	選択されたオプション	必須	有効値： **GET** | **POST** | **HEAD** 既定値 **: GET** 。
Match response method	選択されたオプション	必須	マッチレスポンスコンテンツが指定されている場合、**CloudMonitor** は **HTTP** サーバーから送信されるレスポンスのメッセージ本文の最初の **64 KB** を読み取って指定されたコンテンツを検索します。結果は次のいずれかになります。 1. レスポンスに指定されたコンテンツが含まれている。 2. レスポンスに指定されたコンテンツが含まれていない。 **CloudMonitor** は、指定されたマッチレスポンス方法に基づいてアラームをトリガーするかを判断します。 **Alibaba Cloud** プローブポイントのマッチレスポンスコンテンツは英語に対応しています。
Match response content	テキスト	省略可能	

パラメーター	値	必須/省略可能	説明
HTTP request header	テキストライン	省略可能	**HTTP** リクエストヘッダー情報の形式は次のとおりです。`key1:value1 carriage return linefeed key2:value2` **CloudMonitor** は、リクエストヘッダーに次の項目を事前設定します。 **Host: $ {Domain name specified in Monitor Address}** **Pragma: no-cache** **Cache-Control: no-cache** **User-Agent: Chrome/57** **Accept: */*** リクエストコンテンツがフォームの場合、リクエストヘッダーには次の項目が含まれる場合があります。 **Content-Type: application/x-www-form-urlencoded;charset=UTF-8** **HTTP** リクエストヘッダーに前述の項目が **1** つ以上含まれている場合、これらの項目は設定によって上書きされます。 **HTTP** プロトコルに従って、**CloudMonitor** はリクエストヘッダーのキーを標準形式の **MIME** ヘッダーに変換します。 **1.** キーの最初の文字とハイフン (-) に続く文字は大文字になります。 例えば、 `accept-encoding` は `Accept-Encoding` に変換されます。 **2.** キーにスペースまたはその他の無効な文字が含まれている場合、キーは変更されません。
Cookie	該当なし	省略可能	**HTTP** プロトコルに基づいて **cookie** テキストを入力します。

パラメーター	値	必須/省略可能	説明
HTTP Authentication Username	**Username**	省略可能	この認証は、**HTTP** プロトコルによる基本認証を指します。
HTTP Authentication Password	**Password**	省略可能	

- **PING** の詳細設定

パラメーター	値	必須/省略可能
Monitor Address	ドメイン名または **IP** アドレス	必須
Number of ping packets	正の整数	必須

注：

Number of ping packets パラメーターは `ping` コマンドが開始される回数を示します。

値の範囲：`1` ～ `40`。 既定値: `20` 。

- **TCP** および **UDP** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Address	ドメイン名または **IP** アドレス	必須	なし
Request content format	選択されたオプション	必須	リクエストコンテンツが指定されている場合に有効です。 有効値： **Hexadecimal Format** | **Text**

パラメーター	値	必須/省略可能	説明
Request content	テキストまたは **16** 進数テキスト	省略可能	テキスト：表示されるテキスト文字の文字列。 テキスト形式はエスケープ文字に対応していません。つまり、 `\n` は新しい行の入力として変換されず、システムはこれを **2** つの文字 **(**円記号 **(\)** と *n* 字**)** とみなします。 16 進数形式：リクエストのコンテンツがテキスト文字列で表現できない **byte** 型の文字列である場合、この文字列を **16** 進文字列に変換することができます。 変換ルールとして、各 **byte** は **2-byte** の **16** 進文字列に変換されます。 たとえば、**(byte)1** は **16** 進文字列 **01** に変換され、**(byte)27** は **16** 進文字列 **1B** に変換されます。 変換ルールに従って、**Java** 形式のバイナリ配列 **"{(byte)1, (byte)27}"** は、**16** 進数文字列 **011b** または **011B** に変換されます。 **CloudMonitor** では、**16** 進文字列の大文字と小文字が区別されません。 **Request content** フィールドに文字列 **011B** を入力し、**Request content format** を **16** 進数形式に設定します。
match response content format	選択されたオプション	必須	マッチレスポンスコンテンツが指定されている場合に有効です。 有効値：**Hexadecimal Format | Text**
Match response content	テキストまたは **16** 進数テキスト	省略可能	詳細については、 **Request content** パラメーターをご参照ください。

- **DNS** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Domain Name	ドメイン名	必須	
DNS query type	選択されたオプション	必須	有効値：**A** | **MX** | **NS** | **CNAME** | **TXT** | **ANY** 既定値 **: A**
DNS server	**DNS IP** アドレス	省略可能	このパラメーターが指定されていない場合、**CloudMonitor** は既定の **DNS IP** アドレスを使用します。 ドメイン名または **IP** アドレスを入力できます。
Expected to resolve IP	テキストライン	省略可能	解決するドメイン名または **IP** アドレスのリストを入力します。 各行は、ドメイン名または **IP** アドレスを表します。 指定したリストが **DNS** リストのサブセットである場合のみ、検出が成功します。

- **POP3** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Address	**URL**	必須	**POP3(s)** プロトコルを選択した場合、入力するすべてのアドレスがスキーマを含んでいる必要があります。例： **pop3s://pop3.aliyun.com** スキーマを含まないアドレスを入力すると、**CloudMonitor** がアドレスに**pop3** をスキーマとして追加します。 **POP3 (s)** は、**TLS** を使用してデータを暗号化します。

パラメーター	値	必須/省略可能	説明
username	テキスト	必須	アカウントは USER および PASS コマンドを使用して認証されます。 必ず有効なユーザー名とパスワードを入力してください。 **CloudMonitor** は、 **Monitoring frequency** パラメーターで指定された時間間隔でインターネットを検出します。 当事者による無効なユーザー名とパスワードの入力が頻繁に検出された場合、アカウントがブロックされる可能性があります。
Password	テキスト	必須	

- **SMTP** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Address	**URL**	必須	入力するすべてのアドレスにはスキーマが含まれている必要があります。例： **smtp://smtp.aliyun.com** スキーマが含まれていないアドレスを入力すると、**CloudMonitor** がアドレスに**smtp** をスキーマとして追加します。 **SMTP** は STARTTLS コマンドで暗号化に関するサーバーとの交渉を行います。 セキュリティで保護された接続を使用すると、認証情報も暗号化されます。

パラメーター	値	必須/省略可能	説明
username	テキスト	必須	アカウントは、PLAIN コマンドで認証されます。 必ず有効なユーザー名とパスワードを入力してください。 **CloudMonitor** は、 **Monitoring frequency** パラメーターで指定された時間間隔でインターネットを検出します。 当事者による無効なユーザー名とパスワードの入力が頻繁に検出された場合、アカウントがブロックされる可能性があります。
Password	テキスト	必須	

- **FTP** の詳細設定

パラメーター	値	必須/省略可能	説明
Monitor Address	**URL**	必須	例： **ftp://smtp.aliyun.com**
Are you anonymous login	選択されたオプション	必須	有効値：**Anonymous Logon** | **Authentication Required** 既定値：**Anonymous Logon** **Authentication Required** を選択した場合、有効なユーザー名とパスワードを入力する必要があります。
username	テキスト		**FTP** 認証に使用されるユーザー名とパスワード。 **Anonymous Logon** を選択した場合、ユーザー名は anonymous 、パスワードは ftp@example.com になります。
Password	テキスト		

4 アラームサービス

4.1 アラームサービスの概要

ホストモニタリングの測定値、、クラウドサービスモニタリングのインスタンス、カスタマイズモニタリングの測定値にアラームルールを設定できます。 アラームルールは、すべてのリソース、アプリケーショングループ、または単一のインスタンスに適用できます。

アラームサービスは、電話、**SMS** メッセージ、メール、**TradeManager**、および **DingTalk** チャットボットなどのさまざまなチャネルを通じてアラーム通知をサポートします。 **TradeManager** は、 **PC** クライアントのアラーム通知のみサポートします。 **Alibaba Cloud** アプリをインストールし、アラーム通知を受け取ることもできます。

ホストモニタリングのアラームルール

ホストモニタリングのすべての測定値にアラームルールを設定できます。 アラーム検出頻度は最小で **1** 分ごとです。

クラウドサービスのアラームルール

Cloud Monitor を使用すると、クラウドリソースの消費量をモニターするためのしきい値アラームを設定し、インスタンスとサービスのステータスを監視するためのイベントアラームを設定できます。

カスタマイズモニタリングアラームルール

カスタマイズモニタリング **API** を介してモニタリングデータをレポートした後、対応する測定値にアラームルールを設定できます。 測定値が指定されたしきい値を超えるとアラームがトリガーされ、指定された通知方法でアラーム通知が送信されます。

カスタムイベントのアラームルール

カスタムイベント **API** を介してイベント例外を報告した後、イベントのアラームルールを設定できます。 アラームルールが満たされると、アラームがトリガーされ、指定された通知方法でアラーム通知が送信されます。

4.2 アラームテンプレートの使用

アラームテンプレート機能を使用してアラームルールをテンプレートに保存することで、アラームルール作成時にアラームルールを個別に定義する必要がなくなります。 この機能を使用すると、特に大規模で複雑な事業運営において、運用と全体的な効率を向上させることができます。

アラームテンプレートはアプリケーショングループと一緒に使用されます。 複数のクラウドリソース (ECS インスタンス、RDS サービス、SLB インスタンス、OSS バケットなど) がある場合は、ビジネスニーズに応じてこれらのリソース用のアプリケーショングループを作成することを推奨します。 その後、アラームテンプレートを作成すると、必要なアプリケーショングループにそのテンプレートを適用できます。 このプロセスにより、すべてのビジネスモジュールに対するアラームルールを迅速に作成できます。

デフォルトでは、CloudMonitor は、ECS、RDS、SLB、CDN、Redis、MongoDB、OSS などのプロダクトに共通の測定値を含む、初期化されたアラームテンプレートを提供します。

注:

- アラームテンプレートはアプリケーショングループ にのみ適用されます。つまり、アラームルールのリソース範囲として、アプリケーショングループを選択した場合にのみアラームテンプレートを使用できます。
- 各 Alibaba Cloud アカウントには、最大 100 個のアラームテンプレートを含めることができます。
- 各アラームテンプレートには、最大 30 個の測定値を含めることができます。
- アラームテンプレート機能は、複数のアラームルールを作成するための近道にすぎません。アラームルールはアラームテンプレートにバインドされていません。 アラームテンプレートを変更した後、このテンプレートを使用して生成されたアラームルールは変更されません。異なるアプリケーショングループのアラームルールをまとめて変更するには、変更したテンプレートを各アプリケーショングループに適用する必要があります。

テンプレートの作成

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、 [アラーム] > [アラームテンプレート] を選択します。
3. [アラームテンプレートの作成] をクリックします。
4. [基本情報] の下の [テンプレート名] と [説明] に入力します。
5. アラームルールを設定します。 [ルールの追加] をクリックして、アラームルールを追加します。

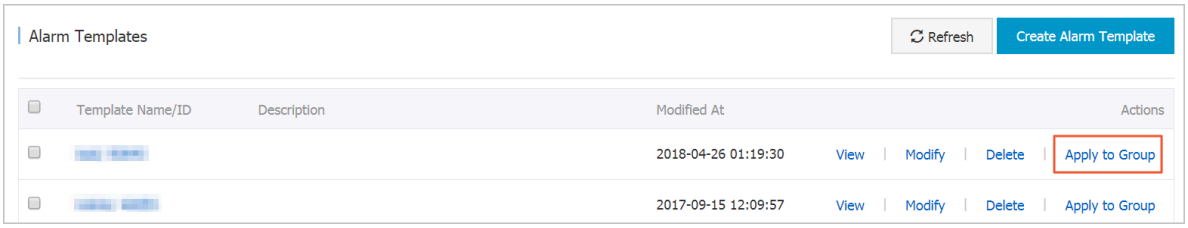
6. [追加] をクリックします。

テンプレートの使用

- アプリケーショングループの作成時にアラームテンプレートを使用

  リソース用のアプリケーショングループを作成するときに、**[MonitorAlarm]** エリアで既存のアラームテンプレートを選択できます。 アプリケーショングループが正常に作成されると、**CloudMonitor** は選択されたアラームテンプレートに基づいてこのグループのアラームルールを生成します。
- アラームテンプレートをアプリケーショングループに直接適用

  アプリケーショングループは作成したが、グループのアラームルールは作成していない場合は、アラームテンプレートを作成してからテンプレートをグループに迅速に適用できます。



4.3 アラームルール

4.3.1 アラームルールのパラメーター

ここでは、しきい値アラームルールのパラメーターについて説明します。

パラメーター

- **Product** ：モニタリングサービス (ECS、ApsaraDB for RDS、Object Storage Service (OSS) など) 。
- **Resource Range**：アラームルールの範囲。 有効値：**All Resources** 、**Instances**

> 注：
> **Resource Range** をAll Resources に設定した場合、アラームルールは 1,000 以下のインスタンスに適用されます。 モニタリング対象リソースの数が 1,000 を超える場合、指定されたメトリックがしきい値に達した際にアラームを受信しない場合があります。 アラームルールを作成する前に、サービス固有のアプリケーショングループにリソースを追加するこ

とを推奨します。 グループのしきい値アラームルールを作成するには、 グループインスタンスページに移動し、 [しきい値アラーム] をクリックします。

- **All Resources** ：指定したサービスのすべてのインスタンスをアラームルールの適用対象として指定します。 これらのインスタンスのメトリックが指定されたしきい値に達すると、システムはアラーム通知を送信します。
- **Instances** ：指定されたインスタンスをアラームルールの適用対象として指定します。 インスタンスのメトリックが指定されたしきい値に達すると、システムはアラーム通知を送信します。

・ **Alarm Rule**：アラームルールの名前。

・ **Rule Description**：アラームルールの内容。 このパラメーターは、アラームを引き起こすメトリック条件を定義します。

アラームルールの例 ：ホストモニタリングでは、単一のホストのメトリック上のデータポイントが **15** 秒間隔で報告されます。 したがって、**5** 分間で **20** 件のデータポイントが報告されます。

- **5** 分間サイクルの平均 **CPU** 使用率が連続した **3** サイクルで **90%** を超える：**5** 分間サイクルで報告される **CPU** 使用率の **20** 件のデータポイントの平均値が 連続した **3** サイクルで **90%** を超える状態を指定します。 指定されたメトリックがしきい値に達すると、システムがアラーム通知を送信します。
- **5** 分間サイクルの **CPU** 使用率が連続した **3** サイクルで必ず **90%** を超える：**5** 分間サイクルで報告される **CPU** 使用率の **20** 件のデータポイントの値が 連続した **3** サイクルで **90%** を超える状態を指定します。 指定されたメトリックがしきい値に達すると、システムがアラーム通知を送信します。
- **5** 分間サイクルの **CPU** 使用率が連続した **3** サイクルで一度 **90%** を超える：**5** 分間サイクルで報告される **CPU** 使用率の **20** 件のデータポイントの少なくとも **1** 件の値が 連続した **3** サイクルで **90%** を超える状態を指定します。 指定されたメトリックがしきい値に達すると、システムはアラーム通知を送信します。
- **5** 分間サイクルのパブリックネットワークアウトバウンドトラフィックの合計が連続した **3** サイクルで **50 MB/s**を超える：**5** 分間サイクルで報告されるパブリックネットワークアウトバウンドトラフィックの **20** 件のデータポイントの合計値が **50 MB/s** を超える状態を指定します。 指定されたメトリックがしきい値に達すると、システムはアラーム通知を送信します。

・ **Mute For** ：**CloudMonitor** は、指定された例外が指定回数連続して検出された場合にのみ、アラーム通知を送信します。 最小値は **5** 分で、最大値は **24** 時間です。

- **Effective Period**：アラームルールの有効期間です。 システムは、アラームルールに従って、有効期間内にのみアラーム通知を送信します。 有効期間外にアラームが発生した場合、システムではアラームの記録のみを行います。
- **Notification Contact**：**CloudMonitor** がアラーム通知を送信する連絡先グループ。
- **Alarm Levels**：指定された通知方法に対応するアラームの重大度レベルを指定します。 有効値 **: CRITICAL**、**WARN**、**INFO**。
  - **INFO**：メール、**DingTalk ChatBot** を使用してアラーム通知を送信します。
- **Auto Scaling**：**Auto Scaling** を選択してルールを設定すると、アラームが対応するスケーリングルールをトリガーします。
- **Email Remark**：アラームメールのカスタム補足情報。 **CloudMonitor** は、アラームメールとともにコメントを送信します。
- **HTTP CallBack**：**CloudMonitor** は **POST** リクエストを使用して、指定したパブリック **URL** アドレスにアラームをプッシュします。 このコールバックは、**HTTP**ベースのリクエストに対応しています。

4.3.2 アラームルールの管理

CloudMonitor は、クラウドサービスのモニタリングとアラームを提供します。例外のメトリックをタイムリーに特定し、トラブルシューティングを効率的に実行します。

CloudMonitor コンソールでアラームルールの管理を始める方法は **3** つあります。左側のナビゲーションウィンドウで [アプリケーショングループ] を選択し、[アプリケーショングループ] ページに移動する方法、必要なモニタリングタイプを選択して、対応するモニタリングメトリックページに移動する方法、[アラーム] > [アラームルール] を選択し、[アラームルール] ページに移動する方法です。

- アプリケーショングループのページでアラームルールを管理
- ホストモニタリングページでアラームルールを管理
- クラウドサービスモニタリングでアラームルールを設定
- カスタムモニタリングページでアラームルールを設定

4.3.3 MNS へのアラームの書き込み

ここでは、しきい値アラームをメッセージサービス (MNS) に書き込む方法について説明します。

手順

1. CloudMonitor による MNS へのアラームの書き込みを許可するには、ここをクリックします。

2. OpenAPI Explorer サービスを開始し、 *PutResourceMetricRule* 操作を呼び出して、アラームルールを作成します。
3. *PutMetricRuleTargets* 操作を呼び出して、指定のアラームルールのアラームを作成し、対応する MNS パラメーターを設定します。

   ARN：`"acs:mns:{$RegionId}:{$UserId}:/queues/{$queueName}/messages"`の形式で対象の MNS キューを指定します。または、`"acs:mns:{$RegionId}:{$UserId}:/topics/{$queueName}/messages"`の形式で対象の MNS トピックを指定します。

次の例では、PutMetricRuleTargets のパラメーターを示します。

```
RuleId:"db17-4afc-b11a-568512d5a1f9",
Targets:[{
    Id: 1,
    Arn:"acs:mns:{$RegionId}:{$UserId}:/queues/{$queueName}/messages",
    Level: ["INFO", "WARN", "CRITICAL"],
}]
```

MNS に書き込むメッセージ本文

CloudMonitor は、メッセージ本文を JSON 文字列形式で MNS に書き込みます。 MNS がメッセージ本文を読み込むと、クライアントは次のようにメッセージ構造をJSON 文字列として解析します。

```
{
  "ruleId": "putNewAlarm_group_778af9ba-a291-46ab-ac53-3983bcee****",
  "ruleName": "test",
  //Current level.
  "curLevel": "WARN",
  //Previous level.
  "preLevel": "OK",
  //The instance that triggers the alarm.
  "resources": "{\"instanceId\": \"i-uf61rfofjd2iku7e****\"}",
  //The condition that triggers the alarm.
  "escalation": {
    "comparisonOperator": "GreaterThanYesterday",
    "level": 3,
    "statistics": "Average",
    "tag": "WARN",
```

```
    "threshold": "0",
    "times": 1
  },
  "metricData": {
    "timestamp": 1534736160000,
    "userId": "127067667954****",
    "instanceId": "i-uf61rfofjd2iku7e****",
    "Average": 470687744,
    "Maximum": 470794240,
    "Minimum": 470556672,
    //Compare some metrics with those in the previous month and those
in the same period of the previous year.--Start.
    "AliyunCmsPrevValues": { //Compared values.
      "timestamp": 1534649760000,
      "userId": "127067667954****",
      "instanceId": "i-uf61rfofjd2iku7e****",
      "Average": 468463616,
      "Maximum": 468549632,
      "Minimum": 468258816
    },
    //Comparison formula.
    "AliyunCmsComplexExpression": "100.0 * ($Average-$$prevAverage)/$$
prevAverage",
    //Conversion formula.
    "AliyunCmsComplexMath": "100.0 * (470687744-468463616)/468463616",
    //Calculation result.
    "AliyunCmsComplexValue": 0.47477070236336133
    //Compare some metrics with those in the previous month and those
in the same period last year.--End.
  },
  //Metric parameters.
  "metricName": "memory_actualusedspace#60",
  "namespace": "acs_ecs_dashboard",
  "period": "60",

  //Application group parameters.
  "groupBy": "group",
  "productGroupName": "RDS instance group",
  "groupId":"44958",

  //Alarm time
  "lastTime": 327362743, //The duration of the alarm.
  "time": 1534736160000, //The time when the data occurred.

  "userId": "173651113438****",
  "eventName": "AlertOk",
  "eventType": "Alert",
  //Use the following parameters to trace the alarm.
  "batchId": "4272653-152082****-0",
  "version": "1.0"
}
```

4.4 アラーム連絡先

4.4.1 アラーム送信先およびアラーム送信先グループの管理

アラーム通知は、アラーム送信先およびアラーム送信先グループに送信されます。 アラームルール作成の際に、アラーム通知を受け取るためのアラーム送信先とアラーム送信先グループを作成する必要があります。

アラーム送信先の管理

メールアドレスなど、送信先の情報を作成、編集、削除できます。

- アラーム送信先の作成

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. ページ右上隅の [アラーム送信先の作成] をクリックします。 表示されたダイアログボックスで、送信先のメールアドレスなどの情報を入力します。

     指定されたメールアドレスが正しくないとアラーム通知が届かないため、指定内容が正しいことを確認する必要があります。

- アラーム送信先の編集

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. [アクション] 列の [編集] をクリックして、送信先の情報を編集します。

- アラーム送信先の削除

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. [アクション] 列の [削除] をクリックします。

 注 :
アラーム送信先を削除すると、**CloudMonitor** アラーム通知はその送信先に送信されなくなります。

アラーム送信先グループの管理

アラーム送信先グループには、**1** 人以上のアラーム送信先を含めることができます。 同じアラーム送信先は、複数のアラーム送信先グループに追加できます。アラームルール設定時に、すべてのアラーム通知はアラーム送信先グループを通じて送信する必要があります。

- アラーム送信先グループの作成

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. ページの最上部にある [アラーム送信先グループ] タブをクリックして、アラーム送信先グループリストに切り替えます。
  4. 右上隅の [アラーム送信先グループの作成] をクリックして 、[アラーム送信先の作成] ダイアログボックスを表示します。
  5. グループ名を入力し、グループに追加する送信先を選択します。

- アラーム送信先グループの編集

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. ページの最上部にある [アラーム送信先グループ] タブをクリックして、アラーム送信先グループリストに切り替えます。
  4. [アクション] 列の [編集] をクリックして、送信先グループを編集します。

- アラーム送信先グループの削除

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで、[アラーム] の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. ページの最上部にある [アラーム送信先グループ] タブをクリックして、アラーム送信先グループリストに切り替えます。
  4. [アクション] 列の [削除] をクリックして、送信先グループを削除します。

- 送信先グループへの送信先の一括追加

  1. *CloudMonitor コンソール*にログインします。
  2. 左のナビゲーションウィンドウで **[Alarms]** の下の [アラーム送信先] をクリックします。 [アラーム送信先管理] ページが表示されます。
  3. アラーム送信先リストから、追加する送信先を選択します。
  4. ページの最下部にある [送信先グループに追加] をクリックします。
  5. 表示されたダイアログボックスで、対象の送信先グループを選択して **[OK]** をクリックします。

4.5 アラームログの表示

ここでは、アラームログを表示する方法について説明します。

CloudMonitor コンソールで、ルール名またはグループ名でアラームログを検索できます。

手順

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、 [アラーム] > [アラームログ] を選択して、アラームログページを開きます。

3. ドロップダウンリストから検索条件 ([アラームルール] または [グループ名]) を選択し、検索バーにキーワードを入力します。 [検索] をクリックします。
4. 表示するレコードを特定し、 [アクション] コラムの [グラフ] をクリックします。

5. アラームログを表示する時間範囲を選択します。 直近 **31** 日間に生成されたアラームログを表示できます。

5 可用性モニタリング

5.1 可用性モニタリングの管理

可用性モニタリングは定期的な検出タスクを実行して、指定されたローカルまたはリモートのパスまたはポートが正しく応答するかどうかを確認し、応答タイムアウトが発生した場合、またはステータスコードがアラームルールで指定された条件に基づいてエラーを示します。 この機能を使用すると、ローカルまたはリモートのサービスが応答していないのか異常なのかをすばやく確認でき、全体的な運用と管理の効率が向上します。

注：

- 可用性モニタリング機能を使用する前に、**CloudMonitor** エージェントをインストールする必要があります。 この機能を使用する前に、指定したインスタンスに **CloudMonitor** エージェントをインストールしたことを確認してください。
- 作業が開始されると、モニタリングタスクが **1** 分間に **1** 回実行されます。

可用性モニタリングタスクの作成

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[アプリケーショングループ]** をクリックします。
3. 対象アプリケーショングループを見つけて、グループ名をクリックします。
4. 左側のナビゲーションウィンドウで、 **[可用性モニタリング]** を選択します。
5. ページの右上隅で、**[設定の作成]** をクリックして **[可用性モニタリングの作成]** ページを開きます。
6. タスク名を入力して対象サーバーを選択します。 アプリケーショングループ内のすべてのサーバーを選択して、それらに同じ可用性モニタリングルールを設定することも、アプリケーショングループ内の一部のサーバーを選択することもできます。
7. 検出タイプと検出対象の選択: **[URL または IP アドレス]**、**[ApsaraDB for RDS]**、および **[ApsaraDB for Redis]** がサポートされています。
   - **[ApsaraDB for RDS]** または **[ApsaraDB for Redis]** を選択する場合は、アプリケーショングループ内の関連インスタンスとアクセスアドレスが表示されます。
   - **[検出対象]** に **[HTTP(S)]** を選択した場合は、**HEAD**、**GET**、**POST** の各リクエストと戻り値に一致するコンテンツを設定できます。

8. アラームルールを設定します。 ステータスコードと応答時間ルールは、アラームに対してサポートされています。 アラームルールで指定された条件を満たす設定があれば、すべてアラームをトリガーします。 トリガーされたアラームは通知としてアプリケーショングループに関連づけられたアラーム送信先グループに送信されます。

   - ステータスコードアラーム**:** プローブのステータスコードが、指定されたアラームルールに適合した場合にトリガーされるアラーム。
   - 通知方法**:** メールや **SMS** メッセージなどのアラーム通知が送信される方法 。
   - 詳細設定**:** 有効期間とミュート期間両方の設定がサポートされます。有効期間は、アラームルールで指定された条件を満たすとき、アラームがトリガーされる可能性がある期間を指します。ミュート期間は、アラームルールで指定された条件を満たしても、アラーム通知がトリガーされないようにアラームルールがミュートされた期間を指します。

可用性モニタリングタスクの表示

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで **[**アプリケーショングループ**]** をクリックして、アプリケーショングループページに移動します。
3. 可用性モニタリングを表示するアプリケーショングループを選択し、アプリケーショングループ名をクリックして、アプリケーショングループの詳細ページに移動します。
4. 左側のナビゲーションウィンドウから **[**可用性モニタリング**]** を選択して、**[**可用性モニタリング**]** ページに移動します。グループ内のすべての可用性モニタリングに適用されるタスクのリストが表示されます。

モニタリング結果の表示

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで **[**アプリケーショングループ**]** をクリックして、**[**アプリケーショングループ**]** ページに移動します。
3. 可用性モニタリングを表示するアプリケーショングループを選択し、アプリケーショングループ名をクリックして、アプリケーショングループの詳細ページに移動します。
4. 左側のナビゲーションウィンドウから **[**可用性モニタリング**]** を選択して **[**可用性モニタリング**]** ページに移動します。

5. リストの中でモニタリング結果を確認できます。
   - タスクプローブがアラームをトリガーしない場合は、リストの中の問題のあるインスタンスの数は 0 です。
   - アラームがプローブの例外によりトリガーされると、アラームをトリガーしたインスタンスの数がリストに表示されます。例外番号をクリックすると、問題のあるインスタンスの詳細が表示されます。
   - 例外の詳細。

可用性モニタリングタスクの変更

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで [アプリケーショングループ] をクリックして、[アプリケーショングループ] ページに移動します。
3. 可用性モニタリングを変更するアプリケーショングループを選択し、アプリケーショングループ名をクリックして、アプリケーショングループの詳細ページに移動します。
4. 左側のナビゲーションウィンドウから可用性モニタリングを選択して、可用性モニタリングの管理ページに移動します。
5. 変更が必要なタスクを選択し、アクションの中から [変更] をクリックして 、アプリケーショングループの変更ページに移動します。
6. アプリケーショングループの変更ページで内容を編集し、設定を保存します。

アラームログの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで [アプリケーショングループ] をクリックして、[アプリケーショングループ] ページに移動します。
3. アラームログを表示するアプリケーショングループを選択し、アプリケーショングループ名をクリックして、アプリケーショングループの詳細ページに移動します。
4. 左側のナビゲーションウィンドウから [アラームログ] を選択して、[アラームログ] ページに移動してアラームログの詳細を表示します。

モニタリングタスクの有効化または無効化

ローカルの正常性確認のために、モニタリングタスクの有効化または無効化をサポートします。タスクが無効化されると、正常性確認は行われず、アラームはタスクに対してトリガーされなくなります。 しかし、タスクが有効化されるとプロービングが再起動し、アラームルール設定で指定された要件が満たされるとアラームがトリガーされます。

1. *CloudMonitor コンソール*にログインします。

2. 左側のナビゲーションウィンドウで [アプリケーショングループ] をクリックして、「アプリケーショングループ] ページに移動します。
3. 可用性モニタリングを有効化または無効化する必要のあるアプリケーショングループを選択し、アプリケーショングループ名をクリックして、アプリケーショングループの詳細ページに移動します。
4. ページの左側のメニューで [可用性モニタリング] を選択して、可用性モニタリングのタスク管理ページに移動します。
5. 有効または無効にするタスクを選択し、アクションで [有効] または [無効] をクリックしてタスクのステータスを変更します。

5.2 ローカルサービス可用性モニタリング

本ページでは、応答タイムアウトが発生した場合やステータスコードがエラーを示した場合に、ローカルサービスプロセスの可用性をモニターし、アラーム通知を送信する方法について説明します。

注：

- 可用性モニタリング機能を使用する前に、**CloudMonitor** エージェントをインストールする必要があります。 この機能を使用する前に、指定したインスタンスに **CloudMonitor** エージェントをインストールしたことを確認してください。
- モニタリングタスクは **1** 分に **1** 回実行されます。
- 可用性モニタリング機能を使用する前に、アプリケーショングループを作成する必要があります。 詳しくは、アプリケーショングループの作成をご参照ください。

手順

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで [アプリケーショングループ] をクリックします。
3. 対象アプリケーショングループを見つけて、グループ名をクリックします。
4. 左側のナビゲーションウィンドウで、[可用性モニタリング] をクリックします。

5. 右上隅にある [設定の作成] をクリックして、[可用性モニタリングの作成] ページに移動します。

   モニタリング設定:

   - 対象サーバー: 検出を開始するマシン。 ローカルサービスの可用性モニタリングでは、検出元と検出対象は同じマシンです。
   - 検出タイプ: [URL または IP アドレス] を選択します。
   - 検出対象: [HTTP(S)] を選択した場合、構文は「`localhost:port/path`」です。 [TELNET] を選択した場合、構文は「`127.0.0.1:port`」です。 どちらもさまざまなアプリケーションに役立ちます。 **Tomcat** が正しく応答しているかどうかを確認するには、[HTTP(S)] を選択し、「`localhost:8080/monitor`」と入力します。 **MySQL** の接続性を検出する場合は、[TELNET] を選択し、「`127.0.0.1:3306`」と入力します。

   アラーム設定:

   [ステータスコード] と [応答時間] が、可用性モニタリングの測定値として使われます。 いずれかの測定値が、指定されたしきい値に達すると、アラームがトリガーされます。 アラーム通知は、対応するアプリケーショングループのアラーム送信先グループに送信されます。 ローカル可用性モニタリングの場合は、ステータスコードを 400 より大きく設定してください。

   - ステータスコード: 返されたステータスコードがアラームルールに適合すると、アラームがトリガーされます。
   - 通知方法: アラーム通知が送信される方法。
   - 詳細設定:
     - ミュート期間: アラームルールで指定された条件を満たしても、アラーム通知がトリガーされないようにアラームルールがミュートされた期間。
     - 有効期間の開始日: アラームルールで指定された条件を満たすときアラームがトリガーされる可能性がある期間。
6. [OK] をクリックして設定を保存します。 サービスが応答しない場合は、SMSメッセージやメールなど、指定した方法でアラーム通知が送信されます。
7. 異常なホストの詳細を表示するには、 可用性モニタリングタスクリスト内の [異常なホスト]の数をクリックします。

5.3 ステータスコード

以下は、可用性の確認が完了した後で例外が検出されたときに返される、カスタムステータスコードの一覧です。

プロトコルの種類	ステータスコード	定義
HTTP	**610**	**HTTP** 要求が発行されてから **5** 秒以内に応答がないためタイムアウトしました。
HTTP	**611**	検出は失敗しました。
Telnet	**630**	**5** 秒以内に応答がないためタイムアウトしました。
Telnet	**631**	検出は失敗しました。

6 クラウドサービスモニタリング

6.1 ApsaraDB for RDS

CloudMonitor は、ディスク使用率、**IOPS (1** 秒あたりの入出力操作) の使用率、接続使用率、**CPU** 使用率など、**ApsaraDB for RDS** (リレーショナルデータベースサービス) のステータスのモニタリングに役立つ複数のメトリックを提供します。 **RDS** を購入すると、**CloudMonitor** はこれらのメトリックに基づいてデータを自動的に収集します。

注:

- **RDS** のプライマリインスタンスおよび読み取り専用インスタンスのみが、モニタリングおよびアラートサービスに対応しています。
- **CloudMonitor** は、既定で各プライマリインスタンスと読み取り専用インスタンスのアラートルールを作成します。 **CPU** 使用率、接続使用率、**IOPS** 使用率、ディスク使用率のアラートのしきい値は **80**%です。 リソースの使用率が **80**% を超えると、指定された連絡先に **SMS** メッセージとメールが送信されます。

モニタリングサービス

- メトリック

メトリック	説明	ディメンション	単位	最小頻度
ディスクの使用率	インスタンスによるディスク容量の使用率。	インスタンス	%	5 分
IOPS の使用	インスタンスによる IOPS の使用率。	インスタンス	%	5 分

メトリック	説明	ディメンション	単位	最小頻度
接続の使用率	現在のアプリケーションが接続するインスタンスの割合。 アプリケーションが接続できるインスタンスの数は制限されています。 このメトリックは、接続されたインスタンスの割合を示します。	インスタンス	%	5 分
CPU 使用率	インスタンスによる CPU 容量の使用率。 CPU 使用率は、データベースのメモリサイズに応じて決まります。	インスタンス	%	5 分
メモリ使用率	インスタンスによるメモリの使用率。 現在、MySQL データベースのみがこのメトリックに対応しています。	インスタンス	%	5 分
読み取り専用インスタンスのレイテンシ	MySQL 読み取り専用インスタンスのレイテンシ。	インスタンス	秒	5 分
インバウンドトラフィック	インスタンスへの 1 秒あたりのインバウンドトラフィック。	インスタンス	バイト/秒	5 分
アウトバウンドトラフィック	インスタンスからの 1 秒あたりのアウトバウンドトラフィック。	インスタンス	バイト/秒	5 分

メトリック	説明	ディメンション	単位	最小頻度
インスタンスエラー	イベントタイプのメトリック。このメトリックのアラートルールを設定できます。	-	-	-
インスタンスのフェールオーバー	イベントタイプのメトリック。このメトリックのアラートルールを設定できます。	-	-	-

インバウンドトラフィックおよびアウトバウンドトラフィックのメトリックは、**MySQL** および **SQLServer** データベースのみに対応しています。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[ApsaraDB for RDS]** を選択します。 **ApsaraDB for RDS** ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、インスタンスのモニタリングチャートを表示します。
  4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[ApsaraDB for RDS]** を選択します。 **ApsaraDB for RDS** ページが表示されます。
  3. **[アクション]** 列の **[アラームルール]** をクリックしてインスタンスのアラートルールを表示します。
  4. ページ右上隅の **[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

・ パラメーター

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.2 Server Load Balancer

CloudMonitor は、インバウンドトラフィックやアウトバウンドトラフィックなど、**SLB (Server Load Balancer)** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。 **SLB** インスタンスを作成すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

- レイヤー**4** プロトコルメトリック

メトリック	説明	ディメンション	単位	最小頻度
ポートのインバウンドトラフィック	インターネットからポートにアクセス時に消費されるトラフィック。	ポート	ビット/秒	**1** 分
ポートのアウトバウンドトラフィック	ポートからインターネットにアクセス時に消費されるトラフィック。	ポート	ビット/秒	**1** 分
ポートの受信パケット	**1** 秒間にポートで受信するパケット数。	ポート	カウント/秒	**1** 分
ポートの送信パケット	**1** 秒間にポートで送信するパケット数。	ポート	カウント/秒	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
ポートの新しい接続	モニタリング期間中の **TCP 3** ウェイハンドシェイクの最初のステータスが **SYN_SENT** である回数の平均値。	ポート	カウント	**1** 分
ポートのアクティブな接続	モニタリング期間中のポートの **ESTABLISHED** ステータスの接続の数。	ポート	カウント	**1** 分
ポートの非アクティブな接続	モニタリング期間中にポートでステータスが **ESTABLISHED** 以外の接続の数。	ポート	カウント	**1** 分
ポート上の同時接続	モニタリング期間中のポート上の総接続数 **(**アクティブ接続と非アクティブ接続の両方を含む**)**。	ポート	カウント	**1** 分
健全なバックエンド **ECS (Elastic Compute Service)** のインスタンス	正常性テストに合格したインスタンス数。	ポート	カウント	**1** 分
エラーのあるバックエンド **ECS** インスタンス	正常性テストで合格しなかったインスタンス数。	ポート	カウント	**1** 分
ポートで破棄された接続	**1** 秒間にポートで破棄された接続数の平均値。	ポート	カウント/秒	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
ポートで破棄された受信パケット	1 秒間にポートで破棄された受信パケットの平均数。	ポート	カウント/秒	1 分
ポートで破棄された送信パケット	1 秒間にポートで破棄された送信パケットの平均数。	ポート	カウント/秒	1 分
ポートで破棄されたインバウンドトラフィック	1 秒間にポートで破棄されたインバウンドトラフィックの平均値。	ポート	ビット/秒	1 分
ポートで破棄されたアウトバウンドトラフィック	1 秒間にポートで破棄されたアウトバウンドトラフィックの平均値。	ポート	ビット/秒	1 分
インスタンス上のアクティブな接続	モニタリング期間中のインスタンスの **ESTABLISHED** ステータスの接続の数。	インスタンス	カウント/秒	1 分
インスタンス上の非アクティブな接続	モニタリング期間中のインスタンスの **ESTABLISHED** 以外のステータスの接続の数。	インスタンス	カウント/秒	1 分
インスタンスで破棄された接続	1 秒間にインスタンスで破棄された接続の数。	インスタンス	カウント/秒	1 分
インスタンスで破棄された受信パケット	1 秒間にインスタンスで破棄された受信パケット数。	インスタンス	カウント/秒	1 分

メトリック	説明	ディメンション	単位	最小頻度
インスタンスで破棄された送信パケット	1 秒間にインスタンスで破棄された送信パケット数。	インスタンス	カウント/秒	1 分
インスタンスで破棄されたインバウンドトラフィック	インスタンスで破棄された 1 秒あたりのインバウンドトラフィック量。	インスタンス	ビット/秒	1 分
インスタンスで破棄されたアウトバウンドトラフィック	インスタンスで破棄された 1 秒あたりのアウトバウンドトラフィック量。	インスタンス	ビット/秒	1 分
インスタンスの同時接続	モニタリング期間中のインスタンス上の総接続数 (アクティブな接続と非アクティブな接続の両方を含む) 。	インスタンス	カウント/秒	1 分
インスタンスの新しい接続	モニタリング期間中の TCP 3 ウェイハンドシェイクの最初のステータスが SYN_SENT である回数の平均値。	インスタンス	カウント/秒	1 分
インスタンスで受信するパケット	インスタンスで 1 秒あたりに受信する パケット数。	インスタンス	カウント/秒	1 分
インスタンスで送信するパケット	インスタンスで 1 秒あたりに送信するパケット数。	インスタンス	カウント/秒	1 分

メトリック	説明	ディメンション	単位	最小頻度
インスタンスのインバウンドトラフィック	インターネットからインスタンスにアクセスするために消費されるトラフィック。	インスタンス	ビット/秒	1 分
インスタンスのアウトバウンドトラフィック	インスタンスからインターネットにアクセス時に消費されるトラフィック。	インスタンス	ビット/秒	1 分

- レイヤー7 プロトコルメトリック

メトリック	説明	ディメンション	単位	最小頻度
ポート上の QPS	ポートの QPS。	ポート	カウント/秒	1 分
ポートの応答時間 (RT)	ポートのリクエストに対する応答時間の平均。	ポート	ミリ秒	1 分
ポートのステータスコード 2xx	SLB からポートのクライアントに返すステータスコード 2xx の数。	ポート	カウント/秒	1 分
ポートのステータスコード 3xx	SLB からポートのクライアントに返すステータスコード 3xx の数。	ポート	カウント/秒	1 分
ポートのステータスコード 4xx	SLB からポートのクライアントに返すステータスコード 4xx の数。	ポート	カウント/秒	1 分
ポートのステータスコード 5xx	SLB からポートのクライアントに返すステータスコード 5xx の数。	ポート	カウント/秒	1 分

メトリック	説明	ディメンション	単位	最小頻度
ポートのその他のステータスコード	**SLB** からポートのクライアントに返すその他のステータスコードの数。	ポート	カウント/秒	**1** 分
ポートのアップストリームステータスコード **4xx**	**RS** からポートの **SLB** に返すステータスコード **4xx** の数。	ポート	カウント/秒	**1** 分
ポートのアップストリームステータスコード **5xx**	**RS** からポートのクライアントに返すステータスコード **5xx** の数。	ポート	カウント/秒	**1** 分
ポートのアップストリーム **RT**	**RS** からポートのプロキシへのリクエストに対する応答時間の平均。	ポート	ミリ秒	**1** 分
インスタンスの **QPS**	インスタンスの **QPS** 。	インスタンス	カウント/秒	**1** 分
インスタンスの **RT**	インスタンスのリクエストに対する応答時間の平均。	インスタンス	カウント/秒	**1** 分
インスタンスのステータスコード **2xx**	**SLB** からインスタンスのクライアントに 返すステータスコード **2xx** の数。	インスタンス	カウント/秒	**1** 分
インスタンスのステータスコード **3xx**	**SLB** からインスタンスのクライアントに 返すステータスコード **3xx** の数。	インスタンス	カウント/秒	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
インスタンスのステータスコード **4xx**	**SLB** からインスタンスのクライアントに 返すステータスコード **4xx** の数。	インスタンス	カウント/秒	**1** 分
インスタンスのステータスコード **5xx**	**SLB** からインスタンスのクライアントに 返すステータスコード **5xx** の数。	インスタンス	カウント/秒	**1** 分
インスタンスのその他のステータスコード	**SLB** からインスタンスのクライアントに返すその他のステータスコードの数。	インスタンス	カウント/秒	**1** 分
インスタンスのアップストリームステータスコード **4xx**	**RS** から インスタンスの **SLB** に返すステータスコード **4xx** の数。	インスタンス	カウント/秒	**1** 分
インスタンスのアップストリームステータスコード **5xx**	**RS** から インスタンスの **SLB** に返すステータスコード **5xx** の数。	インスタンス	カウント/秒	**1** 分
インスタンスのアップストリーム **RT**	**RS** からインスタンスのプロキシへのリクエストに対する応答時間の平均。	インスタンス	ミリ秒	**1** 分

注：

上表の、新しい接続およびアクティブ/非アクティブな接続は、クライアントから **SLB** に送信される **TCP** 接続リクエストを指します。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Server Load Balancer]** を選択します。 **Server Load Balancer** ページが表示されます。
  3. リージョンをクリックします。 リージョン内のすべてのインスタンスがインスタンスリストに表示されます。
  4. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Server Load Balancer]** を選択します。 **Server Load Balancer** ページが表示されます。
  3. リージョンをクリックします。 リージョン内のすべてのインスタンスがインスタンスリストに表示されます。
  4. [アクション] 列の [アラームルール] をクリックして、インスタンスのアラートルールを表示します。
  5. ページの右上にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.3 OSS モニタリング

OSS (Object Service Storage) サービスは、基本的なシステム稼働状況、パフォーマンス、およびメータリングのモニタリングデータを提供します。 また、リクエストの追跡、使用状況の分析、ビジネストレンドに関する統計の収集、システムの問題の迅速な発見と診断に役立つカスタムアラームサービスも提供されています。

モニタリングサービス

・ メトリックス

OSS モニタリングの測定基準には、主に基本サービス指標、パフォーマンス指標、およびメータリング指標が含まれます。 詳細については、「」をご参照ください。

 注：

課金ポリシーとの一貫性を維持するために、 メータリング指標の収集と表示には次の特別な機能があります。

- 測定指標データは時間ごとに収集されます。 つまり、各時間のリソースメータリングデータは、その時間の全体的な指標条件を表す単一の値に集約されます。
- 測定指標の出力遅延は 30 分近くです。
- メータリング指標データ時間は、関連統計期間の開始時間を指す。
- メータリングデータのカットオフ時間は、当月の最後の統計期間の終了時間です。 当月にメータリングデータが生成されない場合、メータリングデータのカットオフ時間は当月の初日の 00:00 です。
- 最大量のメータリング市ヒュおデータがプッシュされます。 メータリングデータの詳細については、「利用記録」をご参照ください。

  たとえば、PutObject 要求のみを使用してデータをアップロードし、この操作を1分間に平均 10 回実行するとします。 それから、2016 年 5 月 10 日の 08:00:00 から 09:00:00 までの時間では、PUT 要求の計測結果は600 回 (10 x 60 分)、計測データの時刻は 08:00 です。 2016 年 5 月 10 日の 00 から、結果は 2016 年 5 月 10 日の 9 時 30 分ごろに生成されます。 結果が 2016 年 5 月 1 日の 00:00:00 以降の最後のデータレコードである場合、当月のメータリングデータのカットオフ時間は 2016 年 5 月 10 日の 09:00:00 です。 2016 年 5 月にメータリングデータを作成していない場合、指標データのカットオフ時間は 2016 年 5 月 1 日の 00:00:00 になります。

アラームサービス

 注：

OSS バケットはグローバル的に特有です。 バケットを削除した後、同じ名前で別のバケットを作成すると、削除したバケットに設定されているモニタリングとアラームのルールが新しいバケットに適用されます。

メータリング指標と統計指標の他に、他のメトリクスのアラームルールを設定してそれらをモニタリングリストに追加できます。 さらに、単一のメトリックに対して複数のアラームルールを設定することができます。

説明

- アラームサービスの詳細については、「アラームサービスの概要」を参照してください。
- **OSS** アラームサービスのユーザーガイドの詳細については、「」をご参照ください。

6.4 Alibaba Cloud CDN

CloudMonitor は、**QPS (1** 秒あたりのクエリ)、帯域幅、バイトヒット率など、**CDN (**コンテンツ配信ネットワーク) のステータスのモニタリングに役立つ複数のメトリックを提供します。 **CDN** ドメイン名を追加すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 **CloudMonitor** コンソールにログインし、**CDN** モニタリングページでモニタリングの詳細を表示できます。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

- メトリック

メトリック	説明	ディメンション	単位	最小頻度
訪問数/秒	モニタリング期間中の訪問者数をモニタリング期間で割った値。	ドメイン名	**QPS**	**1** 分
帯域幅	単位時間あたりの最大トラフィック。	ドメイン名	ビット/秒	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
ヒット率	モニタリング期間中にリクエストバイトがキャッシュ内で見つかる確率。リクエストバイトの数は、リクエスト数 **x** トラフィックです。バイトヒット率は、**back-to-origin** トラフィックを示します。	ドメイン名	%	**1** 分
インターネットへのアウトバウンドトラフィック	**CDN** からインターネットへのトラフィック。	ドメイン名	バイト	**5** 分
ステータスコード **4xx** の割合	モニタリング期間中に返されたすべての **HTTP** ステータスコードに対する **HTTP** ステータスコード **4xx** の割合。	ドメイン名	%	**1** 分
ステータスコード **5xx** の割合	モニタリング期間中に返されたすべての **HTTP** ステータスコードに対する **HTTP** テータスコード **5xx** の割合。	ドメイン名	%	**1** 分

- モニタリングデータの表示

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Alibaba Cloud CDN]** を選択します。 **CDN** ページが表示されます。
  3. ドメイン名リストタブをクリックします。
  4. ドメイン名をクリックするか、 または、[アクション] 列の [モニタリングチャート] をクリックして、モニタリングチャートを表示します。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Alibaba Cloud CDN]** を選択します。 **CDN** ページが表示されます。
  3. ドメイン名リストタブをクリックします。
  4. [アクション] 列の [アラームルール] をクリックして、ドメイン名のアラートルールを表示します。
  5. ページの右上隅の [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.5 Elastic IP Address

CloudMonitor は、インバウンドトラフィック、アウトバウンドトラフィック、受信パケット、送信パケットなど、**EIP (Elastic IP Address)** のステータスのモニタリングに役立つ複数のメトリックを提供しています。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。 **EIP** を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	説明	ディメンション	単位	最小頻度
着信帯域幅	**EIP** を通過して **ECS (Elastic Compute Service)** に送信される **1** 秒あたりのトラフィック。	インスタンス	ビット/秒	**1** 分
発信帯域幅	**ECS** から **EIP** を通過する **1** 秒あたりのトラフィック。	インスタンス	ビット/秒	**1** 分
受信パケット	**EIP** から **ECS** を通過する **1** 秒あたりのパケット数。	インスタンス	**PPS**	**1** 分
送信パケット	**ECS** から **EIP** を通過する **1** 秒あたりのパケット数。	インスタンス	**PPS**	**1** 分
スロットルによるパケット損失率	実際に使用される帯域幅が設定された上限を超えたときのパケット損失率。	インスタンス	**PPS**	**1** 分

・ モニタリングデータの表示

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[Elastic IP Address]** を選択します。 **Elastic IP Address** ページが表示されます。
3. インスタンスの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、インスタンスのモニタリングチャートを表示します。
4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Elastic IP Address]** を選択します。 **Elastic IP Address** ページが表示されます。
  3. [アクション] 列の [アラームルール] をクリックして、アラートルールを表示します。
  4. ページの右上隅の [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.6 ApsaraDB for Redis

CloudMonitor は、使用中の容量や使用中の接続など、**AdisaraDB for Redis** のステータスのモニタリングに役立つ複数のメトリックを提供します。 **ApsaraDB for Redis** インスタンスを作成すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

- メトリック

メトリック	説明	ディメンション	単位	最小頻度
使用中の容量	インスタンスの残容量。	インスタンス	バイト	**1** 分
使用中の接続	クライアント接続の数。	インスタンス	カウント	**1** 分
書き込み帯域幅	**1** 秒あたりの書き込みトラフィック。	インスタンス	ビット/秒	**1** 分
読み取り帯域幅	**1** 秒あたりの読み取りトラフィック。	インスタンス	ビット/秒	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
失敗した操作	失敗した **KVStore** 操作の数。	インスタンス	カウント	**1** 分
容量の使用率	総容量に対する使用中容量の割合。	インスタンス	%	**1** 分
使用中の接続の割合	合計接続に対する使用中の接続の割合。	インスタンス	%	**1** 分
書き込み帯域幅の使用率	総帯域幅に対する書き込み帯域幅の割合。	インスタンス	%	**1** 分
読み取り帯域幅の使用率	総帯域幅に対する読み取り帯域幅の割合。	インスタンス	%	**1** 分
インスタンスエラー	イベントタイプのメトリック。このメトリックのアラートルールを設定できます。	-	-	-
インスタンスのフェイルオーバー	イベントタイプのメトリック。このメトリックのアラートルールを設定できます。	-	-	-

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[ApsaraDB for Redis]** を選択します。 **Redis** モニタリングリストページが表示されます。
  3. インスタンスの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、インスタンスのモニタリングチャートを表示します。
  4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[ApsaraDB for Redis]** を選択します。 **Redis** モニタリングリストページが表示されます。
  3. [アクション] 列の [アラームルール] をクリックし、インスタンスのアラートルールを表示します。
  4. ページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.7 Container Service

CloudMonitor は、**CPU** 使用率やメモリ使用率などの、**Container Service** のステータスのモニタリングに役立つ複数のメトリックを提供しています。 **Container Service** クラスターを作成すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

- メトリック

メトリック	説明	ディメンション	単位	最小頻度
containerCpuUtilization	コンテナーの CPU 使用率。	ユーザーとコンテナー	%	30 秒
containerMemoryUtilization	コンテナーのメモリ使用率。	ユーザーとコンテナー	%	30 秒
containerMemoryAmount	コンテナーが使用するメモリの量。	ユーザーとコンテナー	バイト	30 秒
containerInternetIn	コンテナーのインバウンドトラフィック。	ユーザーとコンテナー	バイト	30 秒

メトリック	説明	ディメンション	単位	最小頻度
containerInternetOut	コンテナーのアウトバウンドトラフィック。	ユーザーとコンテナー	バイト	**30** 秒
containerIORead	コンテナーの **I/O** 読み取りトラフィック。	ユーザーとコンテナー	バイト	**30** 秒
containerIOWrite	コンテナーの **I/O** 書き込みトラフィック。	ユーザーとコンテナー	バイト	**30** 秒

注：

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

- モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Container Service]** を選択します。 クラスターページが表示されます。
3. **[**アクション**]** 列の **[**モニタリングチャート**]** をクリックして、モニタリングチャートを表示します。
4. **[**時間範囲**]** で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一クラスターのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [**Container Service**]を選択します。 クラスターページが表示されます。
  3. [アクション] 列の [モニタリングチャート] をクリックして、モニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- 複数のクラスターのアラートルールの同時設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [**Container Service**] を選択します。 クラスターページが表示されます。
  3. 対象のクラスターを選択し、リストの下にある[アラームルールの設定] をクリックして、選択したクラスターのアラートルール設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.8 Log Service

CloudMonitor は、インバウンドトラフィックとアウトバウンドトラフィック、**QPS** (クエリ総数/秒) 、ログ統計など、**Log Service** のステータスのモニタリングに役立つ複数のメトリックを提供します。 **Log Service** プロジェクトを作成すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

・ メトリック

メトリック	説明	ディメンション	単位	最小頻度
Inflow	**Logstore** の **1** 分あたりのインバウンドトラフィック。	ユーザー、プロジェクト、**Logstore**	バイト	**1** 分
Outflow	**Logstore** の **1** 分あたりのアウトバウンドトラフィック。	ユーザー、プロジェクト、**Logstore**	バイト	**1** 分
SumQPS	**Logstore** 内の **1** 分あたりの書き込み数。	ユーザー、プロジェクト、**Logstore**	カウント	**1** 分
LogMethodQPS	**Logstore** 内の各メソッドの **1** 分あたりの書き込み数。	ユーザー、プロジェクト、**Logstore**、メソッド	カウント	**1** 分
LogCodeQPS	**Logstore** 内の各ステータスコードの **1** 分あたりの書き込み数。	ユーザー、プロジェクト、**Logstore**、ステータス	カウント	**1** 分
SuccessdByte	**Logstore** 内で解決されたバイト数。	ユーザー、プロジェクト、**Logstore**	バイト	**10** 分
SuccessdLines	**Logstore** の解決されたログの行数。	ユーザー、プロジェクト、**Logstore**	カウント	**10** 分
FailedLines	**Logstore** の解決に失敗したログの行数。	ユーザー、プロジェクト、**Logstore**	カウント	**10** 分
AlarmPV	**Logstore** 内の **(ECS) Elastic Compute Service** 設定エラーの総数。	ユーザー、プロジェクト、**Logstore**	カウント	**5** 分

メトリック	説明	ディメンション	単位	最小頻度
AlarmUv	**Logstore** 内の設定が不正確な **ECS** インスタンスの総数。	ユーザー、プロジェクト、**Logstore**	カウント	**5** 分
AlarmIPCount	**Logstore** 内の各 **IP** アドレスで発生したエラー数。	ユーザー、プロジェクト、**Logstore**、アラートタイプ、ソース **IP** アドレス	カウント	**5** 分

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Log Service]** を選択します。 **Log Service** ページが表示されます。
  3. [アクション] 列の [モニタリングチャート] をクリックして、モニタリングチャートを表示します。
  4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Log Service]** を選択します。 **Log Service** ページが表示されます。
  3. [アクション] 列の [アラームルール] をクリックして、アラートルールを表示します。
  4. ページの右上にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  注：

  - アラートルールを設定する際、ステータス関連のメトリックのステータスを指定可能です。 ステータスフィールドの有効値は、**200**、**400**、**401**、**403**、**405**、**500**、**502** です。
  - 操作回数に関連するメトリックのメソッドを指定できます。 メソッドフィールドの有効値は、**PostLogStoreLogs**、**GetLogtailConfig**、**PutData**、**GetCursorOrData**

、**GetData**、**GetLogStoreHistogram**、**GetLogStoreLogs**、**ListLogStores**、**ListLogStoreTopics** です。

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.9 API Gateway

CloudMonitor は、インバウンドトラフィック、アウトバウンドトラフィック、応答時間など、**API Gateway** のステータスのモニタリングに役立つ複数のメトリックを提供します。

API Gateway を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 **CloudMonitor** コンソールにログインし、**API Gateway** モニタリングページで詳細を閲覧できます。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

・ メトリック

メトリック	説明	ディメンション	単位	最小頻度
エラー分布	モニタリング期間に **API** に対して返された **2XX**、**4XX**、**5XX** ステータスコードの数。	ユーザーと **API**	カウント	**1** 分
インバウンドトラフィック	モニタリング期間に **API** が受信したリクエストのトラフィックの合計。	ユーザーと **API**	バイト	**1** 分
アウトバウンドトラフィック	モニタリング期間に **API** によって送信された応答のトラフィックの合計。	ユーザーと **API**	バイト	**1** 分

メトリック	説明	ディメンション	単位	最小頻度
反応時間	**API Gateway** が **API** のバックエンドサービスを呼び出してから、モニタリング期間にバックエンドサービスから結果を受信するまでの待ち時間。	ユーザーと **API**	秒	**1** 分
リクエストの合計	モニタリング期間中に **API** が受信したリクエストの総数。	ユーザーと **API**	カウント	**1** 分

- モニタリングデータの表示

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[API Gateway]** を選択します。 **API Gateway** モニタリングリスト ページが表示されます。
  3. **API** の名前をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックしてモニタリングチャートを表示します。
  4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[API Gateway]** を選択します。 **API Gateway** モニタリングリストページが表示されます。
  3. **[アクション]** 列の **[アラームルール]** をクリックし、**API** のアラームルールを表示します。
  4. ページの右上隅にある **[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.10 ApsaraDB for MongoDB

CloudMonitor は、**CPU** 使用率やメモリ使用率などの、**ApsaraDB for MongoDB** のステータスのモニタリングに役立つ複数のメトリックを提供しています。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。 **ApsaraDB for MongoDB** を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	説明	ディメンション	単位	最小頻度
CPU 使用率	インスタンスのステータスを示します。	ユーザー、インスタンス、プライマリ/セカンダリノード	%	**5** 分
メモリ使用率	インスタンスのメモリ使用率を示します。	ユーザー、インスタンス、プライマリ/セカンダリノード	%	**5** 分
ディスク使用率	インスタンスのディスク使用率。	ユーザー、インスタンス、プライマリ/セカンダリノード	%	**5** 分
入出力操作/秒 (**IOPS)** 使用率	インスタンスの **IOPS** 使用率。	ユーザー、インスタンス、プライマリ/セカンダリノード	%	**5** 分
接続の使用率	現在のアプリケーションが接続しているインスタンスの割合。 アプリケーションが接続できるインスタンスの数は限られています。 このメトリックは、接続済みのインスタンスの割合を示します。	ユーザー、インスタンス、プライマリ/セカンダリノード	%	**5** 分

メトリック	説明	ディメンション	単位	最小頻度
1 秒あたりの SQL クエリの平均	インスタンスの 1 秒あたりの SQL クエリの平均。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
使用中の接続	現在のアプリケーションが接続するインスタンスの数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
インスタンスによるディスク占有量	インスタンスが占有する総ディスク容量。	ユーザー、インスタンス、プライマリ/セカンダリノード	バイト	5 分
データによるディスク占有量	データが占めるディスク占有量。	ユーザー、インスタンス、プライマリ/セカンダリノード	バイト	5 分
ログによるディスク占有量	ログが占めるディスク容量。	ユーザー、インスタンス、プライマリ/セカンダリノード	バイト	5 分
インバウンド内部ネットワークトラフィック	インスタンスのインバウンドトラフィック。	ユーザー、インスタンス、プライマリ/セカンダリノード	バイト	5 分
アウトバウンド内部ネットワークトラフィック	インスタンスのアウトバウンドトラフィック。	ユーザー、インスタンス、プライマリ/セカンダリノード	バイト	5 分
リクエスト数	サーバーに送信されたリクエストの総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
挿入操作	インスタンスが最後に起動されてから受信した挿入コマンドの総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分

メトリック	説明	ディメンション	単位	最小頻度
クエリ操作	インスタンスが最後に起動されてから受信したクエリコマンドの総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
更新操作	インスタンスが最後に起動されてから受信した更新コマンドの総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
削除操作	インスタンスが最後に起動されてから実行された削除操作の総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
Getmore 操作	インスタンスが最後に起動されてから実行された getmore 操作の総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
コマンド操作	インスタンスが最後に起動されてからデータベースに送信されたコマンドの総数。	ユーザー、インスタンス、プライマリ/セカンダリノード	カウント	5 分
インスタンスエラー	イベントタイプのメトリック。このメトリックのアラートルールを設定できます。	-	-	-

注：

- モニタリングデータは最大 31 日間保持されます。
- モニタリングデータは最大 14 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[ApsaraDB for MongoDB]** を選択します。 **MongoDB** ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. [時間範囲] で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一のインスタンスのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[ApsaraDB for MongoDB]** を選択します。 **MongoDB** ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルアイコンをクリックして、このインスタンスの対応するメトリックのアラートルールを設定します。

- 複数のクラスターのアラートルールの同時設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[ApsaraDB for MongoDB]** を選択します。 **MongoDB** ページが表示されます。
  3. 対象のインスタンスを選択し、リストの下にある [アラームルールの設定] をクリックし、選択したインスタンスの設定をします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.11 Message Service

CloudMonitor は、遅延したメッセージ数、無効メッセージ数、アクティブなメッセージ数など、**Message Service (MNS)** のステータスのモニタリングに役立つ複数のメトリックを提供し

ます。 **MNS** キューを作成すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

モニタリングサービス

・ メトリック

メトリック	説明	ディメンション	単位	最小頻度
ActiveMessages	キュー内のアクティブなメッセージの総数。	ユーザー、リージョン、バケット、キュー	カウント	**5** 分
InactiveMessages	キュー内の非アクティブなメッセージの総数。	ユーザー、リージョン、バケット、キュー	カウント	**5** 分
DelayMessage	キュー内の遅延メッセージの総数。	ユーザー、リージョン、バケット、キュー	カウント	**5** 分
SendMessageCount	メッセージ送信リクエストの数。	ユーザー、リージョン、キュー	カウント	**60** 分
BatchSendMessageCount	複数のメッセージ同時送信のリクエスト数。	ユーザー、リージョン、キュー	カウント	**60** 分
ReceiveMessageCount	メッセージ受信リクエスト数。	ユーザー、リージョン、キュー	カウント	**60** 分
BatchReceiveMessageCount	複数のメッセージ同時受信のリクエスト数。	ユーザー、リージョン、キュー	カウント	**60** 分
BatchDeleteMessageCount	複数のメッセージ同時削除のリクエスト数。	ユーザー、リージョン、キュー	カウント	**60** 分
ChangeMessageVisibilityCount	表示されるメッセージの数を変更します。	ユーザー、リージョン、キュー	カウント	**60** 分

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Message Service]** を選択します。 **MNS**リストページが表示されます。
  3. キューの名前をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、キューのモニタリングチャートを表示します。
  4. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Message Service]** を選択します。 **MNS**リストページが表示されます。
  3. [アクション] 列の [アラームルール] をクリックして、キューのアラートルールを表示します。
  4. ページの右上隅の [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.12 E-MapReduce

CloudMonitor は、**CPU** アイドルレート、メモリ容量、ディスク容量など、**Elastic MapReduce (E-MapReduce)** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

E-MapReduce を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
インバウンドトラフィックレート	ユーザー、クラスター、ロール	ビット/秒	30 秒
アウトバウンドトラフィックレート	ユーザー、クラスター、ロール	ビット/秒	30 秒
CPU アイドルレート	ユーザー、クラスター、ロール	%	1 分
ユーザーモードの CPU 使用率	ユーザー、クラスター、ロール	%	30 秒
システムモードの CPU 使用率	ユーザー、クラスター、ロール	%	30 秒
アイドルディスク容量	ユーザー、クラスター、ロール	バイト	30 秒
総ディスク容量	ユーザー、クラスター、ロール	バイト	30 秒
15 分間の平均負荷	ユーザー、クラスター、ロール	-	30 秒
5 分間の負荷平均	ユーザー、クラスター、ロール	-	30 秒
1 分間の平均負荷	ユーザー、クラスター、ロール	-	30 秒
アイドルメモリ容量	ユーザー、クラスター、ロール	バイト	30 秒
総メモリ容量	ユーザー、クラスター、ロール	バイト	30 秒
受信パケット/秒	ユーザー、クラスター、ロール	PPS	30 秒
送信パケット/秒	ユーザー、クラスター、ロール	PPS	30 秒
実行中のプロセス	ユーザー、クラスター、ロール	カウント	30 秒
総プロセス数	ユーザー、クラスター、ロール	カウント	30 秒

メトリック	ディメンション	単位	最小頻度
ブロックされたプロセス数	ユーザー、クラスター、ロール	カウント	30 秒
作成したプロセスまたはスレッド数	ユーザー、クラスター、ロール	カウント	30 秒
MemNonHeapUsedM	ユーザー、クラスター、ロール	バイト	30 秒
MemNonHeapCommittedM	ユーザー、クラスター、ロール	バイト	30 秒
MemNonHeapMaxM	ユーザー、クラスター、ロール	バイト	30 秒
MemHeapUsedM	ユーザー、クラスター、ロール	バイト	30 秒
MemHeapCommittedM	ユーザー、クラスター、ロール	バイト	30 秒
MemHeapMaxM	ユーザー、クラスター、ロール	バイト	30 秒
MemMaxM	ユーザー、クラスター、ロール	バイト	30 秒
ThreadsNew	ユーザー、クラスター、ロール	-	30 秒
ThreadsRunnable	ユーザー、クラスター、ロール	-	30 秒
ThreadsBlocked	ユーザー、クラスター、ロール	-	30 秒
ThreadsWaiting	ユーザー、クラスター、ロール	-	30 秒
ThreadsTimedWaiting	ユーザー、クラスター、ロール	-	30 秒
ThreadsTerminated	ユーザー、クラスター、ロール	-	30 秒
GcCount	ユーザー、クラスター、ロール	-	30 秒
GcTimeMillis	ユーザー、クラスター、ロール	-	30 秒

メトリック	ディメンション	単位	最小頻度
CallQueueLength	ユーザー、クラスター、ロール	-	**30** 秒
NumOpenConnections	ユーザー、クラスター、ロール	-	**30** 秒
ReceivedByte	ユーザー、クラスター、ロール	-	**30** 秒
SentByte	ユーザー、クラスター、ロール	-	**30** 秒
BlockCapacity	ユーザー、クラスター、ロール	-	**30** 秒
BlocksTotal	ユーザー、クラスター、ロール	-	**30** 秒
CapacityRemaining	ユーザー、クラスター、ロール	-	**30** 秒
CapacityTotal	ユーザー、クラスター、ロール	-	**30** 秒
CapacityUsed	ユーザー、クラスター、ロール	-	**30** 秒
CapacityUsedNonDFS	ユーザー、クラスター、ロール	-	**30** 秒
CorruptBlocks	ユーザー、クラスター、ロール	-	**30** 秒
ExcessBlocks	ユーザー、クラスター、ロール	-	**30** 秒
ExpiredHeartbeats	ユーザー、クラスター、ロール	-	**30** 秒
MissingBlocks	ユーザー、クラスター、ロール	-	**30** 秒
PendingDataNodeMessageCount	ユーザー、クラスター、ロール	-	**30** 秒
PendingDeletionBlocks	ユーザー、クラスター、ロール	-	**30** 秒
PendingReplicationBlocks	ユーザー、クラスター、ロール	-	**30** 秒

メトリック	ディメンション	単位	最小頻度
PostponedMisreplicatedBlocks	ユーザー、クラスター、ロール	-	**30** 秒
ScheduledReplicationBlocks	ユーザー、クラスター、ロール	-	**30** 秒
TotalFiles	ユーザー、クラスター、ロール	-	**30** 秒
TotalLoad	ユーザー、クラスター、ロール	-	**30** 秒
UnderReplicatedBlocks	ユーザー、クラスター、ロール	-	**30** 秒
BlocksRead	ユーザー、クラスター、ロール	-	**30** 秒
BlocksRemoved	ユーザー、クラスター、ロール	-	**30** 秒
BlocksReplicated	ユーザー、クラスター、ロール	-	**30** 秒
BlocksUncached	ユーザー、クラスター、ロール	-	**30** 秒
BlocksVerified	ユーザー、クラスター、ロール	-	**30** 秒
BlockVerificationFailures	ユーザー、クラスター、ロール	-	**30** 秒
BlocksWritten	ユーザー、クラスター、ロール	-	**30** 秒
ByteRead	ユーザー、クラスター、ロール	-	**30** 秒
ByteWritten	ユーザー、クラスター、ロール	-	**30** 秒
FlushNanosAvgTime	ユーザー、クラスター、ロール	-	**30** 秒
FlushNanosNumOps	ユーザー、クラスター、ロール	-	**30** 秒
FsyncCount	ユーザー、クラスター、ロール	-	**30** 秒

メトリック	ディメンション	単位	最小頻度
VolumeFailures	ユーザー、クラスター、ロール	-	**30** 秒
ReadBlockOpNumOps	ユーザー、クラスター、ロール	-	**30** 秒
ReadBlockOpAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
WriteBlockOpNumOps	ユーザー、クラスター、ロール	-	**30** 秒
WriteBlockOpAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
BlockChecksumOpNumOps	ユーザー、クラスター、ロール	-	**30** 秒
BlockChecksumOpAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
CopyBlockOpNumOps	ユーザー、クラスター、ロール	-	**30** 秒
CopyBlockOpAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
ReplaceBlockOpNumOps	ユーザー、クラスター、ロール	-	**30** 秒
ReplaceBlockOpAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
BlockReportsNumOps	ユーザー、クラスター、ロール	-	**30** 秒
BlockReportsAvgTime	ユーザー、クラスター、ロール	ミリ秒	**30** 秒
NodeManager_AllocatedContainers	ユーザー、クラスター、ロール	-	**30** 秒
Containers Completed	ユーザー、クラスター、ロール	-	**30** 秒
ContainersFailed	ユーザー、クラスター、ロール	-	**30** 秒
ContainersIniting	ユーザー、クラスター、ロール	-	**30** 秒

メトリック	ディメンション	単位	最小頻度
ContainersKilled	ユーザー、クラスター、ロール	-	**30** 秒
Containers Launched	ユーザー、クラスター、ロール	-	**30** 秒
Containers Running	ユーザー、クラスター、ロール	-	**30** 秒
ActiveApplications	ユーザー、クラスター、ロール	-	**30** 秒
ActiveUsers	ユーザー、クラスター、ロール	-	**30** 秒
AggregateContainersAllocated	ユーザー、クラスター、ロール	-	**30** 秒
AggregateContainersReleased	ユーザー、クラスター、ロール	-	**30** 秒
AllocatedContainers	ユーザー、クラスター、ロール	-	**30** 秒
AppsCompleted	ユーザー、クラスター、ロール	-	**30** 秒
AppsFailed	ユーザー、クラスター、ロール	-	**30** 秒
AppsKilled	ユーザー、クラスター、ロール	-	**30** 秒
AppsPending	ユーザー、クラスター、ロール	-	**30** 秒
AppsRunning	ユーザー、クラスター、ロール	-	**30** 秒
AppsSubmitted	ユーザー、クラスター、ロール	-	**30** 秒
AvailableMB	ユーザー、クラスター、ロール	-	**30** 秒
AvailableVCores	ユーザー、クラスター、ロール	-	**30** 秒
PendingContainers	ユーザー、クラスター、ロール	-	**30** 秒

メトリック	ディメンション	単位	最小頻度
ReservedContainers	ユーザー、クラスター、ロール	-	**30** 秒

注：

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[E-MapReduce]** を選択します。 **E-MapReduce** モニタリングリストページが表示されます。
  3. クラスターの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、クラスターのモニタリングチャートを表示します。
  4. **[時間範囲]** で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、グラフを拡大します。

アラートサービス

- アラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[E-MapReduce]** を選択します。 **E-MapReduce** モニタリングリストページが表示されます。
  3. クラスターの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、クラスターのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある **[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.13 Auto Scaling

CloudMonitor は、インスタンスの最小数・最大数など、**Auto Scaling** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

Auto Scaling を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
インスタンスの最小数	ユーザーとスケーリンググループ	カウント	**5** 分
インスタンスの最大数	ユーザーとスケーリンググループ	カウント	**5** 分
合計インスタンス	ユーザーとスケーリンググループ	カウント	**5** 分
使用中のインスタンス	ユーザーとスケーリンググループ	カウント	**5** 分
追加するインスタンス	ユーザーとスケーリンググループ	カウント	**5** 分
削除するインスタンス	ユーザーとスケーリンググループ	カウント	**5** 分

注 :

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Auto Scaling]** を選択します。 **Alibaba Cloud Auto Scaling** ページが表示されます。
  3. スケーリンググループの名前をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、スケーリンググループのモニタリングチャートを表示します。
  4. [時間範囲] で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一のスケーリンググループのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Auto Scaling]** を選択します。 **Alibaba Cloud Auto Scaling** ページが表示されます。
  3. スケーリンググループの名前をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、スケーリンググループのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- 複数のスケーリンググループのアラートルールの同時設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Auto Scaling]** を選択します。 **Alibaba Cloud Auto Scaling** ページが表示されます。
  3. 対象のスケーリンググループを選択し、リストの下にある [アラームルールの設定] をクリックして、選択したスケーリンググループのアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.14 HybridDB for MySQL

CloudMonitor は、ディスク使用率、着信帯域幅、発信帯域幅など、**HybridDB for MySQL** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

HybridDB for MySQL を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
ディスクの使用率	ユーザーとインスタンス	ギガバイト	**60** 分
着信帯域幅	ユーザーとインスタンス	キロバイト/秒	**5** 分
発信帯域幅	ユーザーとインスタンス	キロバイト/秒	**5** 分
リクエスト/秒	ユーザーとインスタンス	カウント/秒	**5** 分
子ノードの **CPU** 使用率	ユーザーとインスタンス	%	**8** 分
子ノードのディスク使用量	ユーザーとインスタンス	ギガバイト	**8** 分
子ノードの **1** 秒あたりの入出力操作 **(IOPS)**	ユーザーとインスタンス	カウント/秒	**8** 分

注 **:**

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[HybridDB for MySQL]** を選択します。 **HybridDB for MySQL**ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. **[時間範囲]** で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一のインスタンスのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[HybridDB for MySQL]** を選択します。 **HybridDB for MySQL**ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- 複数のインスタンスのアラートルールの同時設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[HybridDB for MySQL]** を選択します。 **HybridDB for MySQL**ページが表示されます。
  3. 対象のインスタンスを選択し、リストの下にある [アラームルールの設定] をクリックして、選択したインスタンスのアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.15 AnalyticDB for PostgreSQL

CloudMonitor は、**CPU** 使用率やメモリ使用率など、**AnalyticDB for PostgreSQL** のステータスのモニタリングに役立つ複数のメトリックを提供しています。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

AnalyticDB for PostgreSQL を購入すると、**CloudMonitor** は当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
ディスク使用率	ユーザーとインスタンス	%	5 分
接続の使用率	ユーザーとインスタンス	%	5 分
CPU 使用率	ユーザーとインスタンス	%	5 分
メモリ使用率	ユーザーとインスタンス	%	5 分
I/O スループットの使用率	ユーザーとインスタンス	%	5 分

 注：

- モニタリングデータは最大 31 日間保持されます。
- モニタリングデータは最大 14 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[AnalyticDB for PostgreSQL]** を選択します。 **AnalyticDB for PostgreSQL** モニタリングリストページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. [時間範囲] で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一のインスタンスのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[AnalyticDB for PostgreSQL]** を選択します。 **AnalyticDB for PostgreSQL** モニタリングリストページが表示されます。
  3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- 複数のインスタンスのアラートルールの同時設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[AnalyticDB for PostgreSQL]** を選択します。 **AnalyticDB for PostgreSQL** モニタリングリストページが表示されます。
  3. 対象のインスタンスを選択し、リストの下にある [アラームルールの設定] をクリックし、選択したインスタンスのアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.16 Function Compute

CloudMonitor では、合計起動、平均期間、リクエストステータス分散のなど、**Function Compute** のステータスのモニタリングに役立つサービスレベルおよび関数レベルのメトリックを複数提供しています。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

Function Compute サービスを購入すると、**CloudMonitor** が自動的に当該メトリックスに基づいてデータを収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
BillableInvocations	ユーザー、サービス、関数	カウント	**1** 分
BillableInvocationsRate	ユーザー、サービス、関数	**%**	**1** 分
ClientErrors	ユーザー、サービス、関数	カウント	**1** 分
ClientErrorsRate	ユーザー、サービス、関数	**%**	**1** 分
ServerErrors	ユーザー、サービス、関数	カウント	**1** 分
ServerErrorsRate	ユーザー、サービス、関数	**%**	**1** 分
Throttles	ユーザー、サービス、関数	カウント	**1** 分
ThrottlesRate	ユーザー、サービス、関数	**%**	**1** 分
TotalInvocations	ユーザー、サービス、関数	カウント	**1** 分
Average duration	ユーザー、サービス、関数	ミリ秒	**1** 分

 注：

- モニタリングデータは最大 **31** 日間保持されます。

- モニタリングデータは最大 14 日間連続して表示できます。

・ モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [Function Compute] を選択します。 表示される Function Compute ページでは、Function Compute の全体的なステータスを閲覧できます。
3. [サービスリスト] のタブをクリックして、サービスレベルまたは関数レベルのモニタリング情報を表示します。

アラートサービス

また、CloudMonitor では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

・ 単一のサービスのアラートルールの設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [Function Compute] を選択します。 Function Compute ページが表示されます。
3. [アラームルール] のタブをクリックし、ページの右上の [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

・ 複数のサービスのアラートルールの同時設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [Function Compute] を選択します。 Function Compute ページが表示されます。
3. [サービスリスト] をクリックします。
4. 対象のサービスを選択して、リストの下にある [アラームルールの設定] をクリックして、選択されたサービスのアラートルールを設定します。

・ パラメーター

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.17 DirectMail

CloudMonitor は、Web や API メッセージング送信方法に関するメトリック、SMTP (簡易メール転送プロトコル) メッセージ送信方法に関するメトリック、異常なアカウントに関するメ

トリックなど、**DirectMail** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

DirectMail を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	単位	最小頻度
Web/API over-length-error QPS	カウント/分	**1** 分
Web/API over-quota-error QPS	カウント/分	**1** 分
Web/API スパム **QPS**	カウント/分	**1** 分
Web/API の成功 **QPS**	カウント/分	**1** 分
SMTP 認証エラー **QPS**	カウント/分	**1** 分
SMTP 認証成功 **QPS**	カウント/分	**1** 分
SMTP over-length-error QPS	カウント/分	**1** 分
SMTP over-quota-error QPS	カウント/分	**1** 分
SMTP スパム **QPS**	カウント/分	**1** 分

注：

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

・ モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[DirectMail]** を選択します。 表示された **DirectMail** ページで、**DirectMail** のメトリックを閲覧できます。

アラートサービス

また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう **DirectMail** のメトリックのアラートルールを設定することが可能です。

・ アラートルールの設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[DirectMail]** を選択します。 **DirectMail** ページが表示されます。
3. ページの右上隅にある **[アラームルール]** をクリックして、**[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

・ パラメーター

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.18 NAT Gateway

CloudMonitor は、送信元ネットワークアドレス変換 **(SNAT)** 接続の数など、ネットワークアドレス変換 **(NAT)** ゲートウェイのステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

NAT Gateway を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

・ メトリック

メトリック	ディメンション	単位	最小頻度
SNAT 接続	ユーザーとインスタンス	カウント/分	**1** 分
帯域幅パッケージの着信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの発信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの受信パケット	ユーザーとインスタンス	**PPS**	**1** 分

メトリック	ディメンション	単位	最小頻度
帯域幅パッケージの送信パケット	ユーザーとインスタンス	**PPS**	**1** 分
帯域幅パッケージの発信帯域幅の使用率	ユーザーとインスタンス	**%**	**1** 分

注：

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **14** 日間連続して表示できます。

- モニタリングデータの表示

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[NAT Gateway]** を選択します。 **NAT Gateway List** ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、インスタンスのモニタリングチャートを表示します。
  4. **[時間範囲]** で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
  5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一のインスタンスのアラートルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[NAT Gateway]** を選択します。 **NAT Gateway List** ページが表示されます。
  3. インスタンスの **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、インスタンスのモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある **[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

- 複数のインスタンスのアラートルールの同時設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[NAT Gateway]** を選択します。 **NAT Gateway List** ページが表示されます。
  3. 対象のインスタンスを選択し、リストの下にある [アラームルールの設定] をクリックして、選択したインスタンスのアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.19 Shared Bandwidth

CloudMonitor は、着信帯域幅や発信帯域幅など、**Shared Bandwidth** のステータスのモニタリングに役立つ複数のメトリックを提供します。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

Shared Bandwidth を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

- メトリック

メトリック	ディメンション	単位	最小頻度
帯域幅パッケージの着信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの発信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの受信パケット	ユーザーとインスタンス	**PPS**	**1** 分
帯域幅パッケージの送信パケット	ユーザーとインスタンス	**PPS**	**1** 分
帯域幅パッケージの発信帯域幅の使用率	ユーザーとインスタンス	%	**1** 分

注：

- モニタリングデータは最大 **31** 日間保持されます。

- モニタリングデータは最大 14 日間連続して表示できます。

・ モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Shared Bandwidth]** を選択します。 **Shared Bandwidth** ページが表示されます。
3. 帯域幅の **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、帯域幅パッケージのモニタリングチャートを表示します。
4. [時間範囲] で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 14 日間連続して表示できます。
5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

・ 単一の帯域幅パッケージのアラートルール設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Shared Bandwidth]** を選択します。 **Shared Bandwidth** ページが表示されます。
3. 帯域幅パッケージの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、帯域幅パッケージのモニタリングチャートを表示します。
4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

・ 複数の帯域幅パッケージのアラートルールの同時設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Shared Bandwidth]** を選択します。 **Shared Bandwidth** ページが表示されます。
3. 対象の帯域幅パッケージを選択し、リストの下にある [アラームルールの設定] をクリックして、帯域幅パッケージのアラートルールを設定します。

・ パラメーター

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.20 VPN Gateway

CloudMonitor は、着信帯域幅や発信帯域幅などの、仮想プライベートネットワーク **(VPN)** ゲートウェイのステータスのモニタリングに役立つ複数のメトリックを提供しています。 また、**CloudMonitor** では、例外が発生した際にアラートを受信するよう当該メトリックのアラートルールを設定することが可能です。

VPN Gateway を購入すると、**CloudMonitor** が当該メトリックに基づいて自動的にデータを収集します。

モニタリングサービス

- メトリック

メトリック	ディメンション	単位	最小頻度
帯域幅パッケージの着信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの発信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分
帯域幅パッケージの受信パケット	ユーザーとインスタンス	**PPS**	**1** 分
帯域幅パッケージの送信パケット	ユーザーとインスタンス	**PPS**	**1** 分

注：

- モニタリングデータは最大 **31** 日間保持されます。
- モニタリングデータは最大 **7** 日間連続して表示できます。

- モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[VPN]** を選択します。 **VPN** ページが表示されます。
3. **VPN** の **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、**VPN** のモニタリングチャートを表示します。
4. **[時間範囲]** で、事前設定されている期間を選択するか、または期間をカスタマイズします。 モニタリングデータは最大 **14** 日間連続して表示できます。
5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

- 単一の **VPN** のアラートルールの設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[VPN]** を選択します。 **VPN** ページが表示されます。
  3. **VPN** の **ID** をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックして、**VPN** のモニタリングチャートを表示します。
  4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある **[アラームルールの作成]** をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、**[確定]** をクリックします。

- 複数の **VPN** のアラートルールの同時設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、**[クラウドサービスモニタリング]** > **[VPN]** を選択します。 **VPN** ページが表示されます。
  3. 対象の **VPN** を選択し、リストの下にある **[アラームルールの設定]** をクリックして、選択した **VPN** のアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.21 Global Acceleration

CloudMonitor は、着信帯域幅や発信帯域幅など、**Global Acceleration** のステータスのモニタリングに役立つ複数のメトリックを提供します。 **CloudMonitor** では、例外が発生したときにアラートを受信するよう当該メトリックのアラートルールを設定することも可能です。

Global Acceleration を購入すると、**CloudMonitor** が当該メトリックに基づいてデータを自動的に収集します。

モニタリングサービス

- メトリック

メトリック	ディメンション	単位	最小頻度
着信帯域幅	ユーザーとインスタンス	ビット/秒	**1** 分

メトリック	ディメンション	単位	最小頻度
発信帯域幅	ユーザーとインスタンス	ビット/秒	1 分
受信したパケット	ユーザーとインスタンス	PPS	1 分
送信パケット	ユーザーとインスタンス	PPS	1 分

 注：

- モニタリングデータは最大 31 日間保持されます。
- モニタリングデータは最大 7 日間連続して表示できます。

・ モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Global Acceleration]** を選択します。 **Global Acceleration** ページが表示されます。
3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
4. [時間範囲] で、事前設定されている期間を選択するか、期間をカスタマイズします。 モニタリングデータは、最大 7 日間連続して表示できます。
5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

・ 単一のインスタンスのアラートルールの設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Global Acceleration]** を選択します。 **Global Acceleration**ページが表示されます。
3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

- 複数のインスタンスのアラートルールの同時設定

  1. *CloudMonitor* コンソールにログインします。
  2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > **[Global Acceleration]** を選択します。 **Global Acceleration** ページが表示されます。
  3. 対象のインスタンスを選択し、リストの下の [アラームルールの設定]をクリックして、選択したインスタンスのアラートルールを設定します。

- パラメーター

  アラートルールのパラメーターの詳細は、「アラームルールのパラメーター」をご参照ください。

6.22 Elasticsearch

CloudMonitor では、クラスターステータス、**QPS (1** 秒あたりのクラスタークエリ)、クラスター書き込み **QPS** など、**Elasticsearch** のステータスのモニタリングを支援する複数のメトリックを提供します。 **CloudMonitor** では、例外が発生したときにアラートを受信するよう当該メトリックのアラートルールを設定することも可能です。

Elasticsearch を購入すると、**CloudMonitor** はこれらのメトリックに基づいてデータを自動的に収集します。

モニタリングサービス

- メトリック

メトリック	ディメンション	単位	最小頻度
クラスターのステータス	クラスター		**1** 分
クラスター **QPS**	クラスター	カウント/秒	**1** 分
クラスター書き込み **QPS**	クラスター	カウント/秒	**1** 分
ノードの **CPU** 使用率	ノード	%	**1** 分
ノードのディスク使用率	ノード	%	**1** 分
ノードヒープメモリ使用率	ノード	%	**1** 分
1 分間のノードの負荷	ノード		**1** 分
ノードフル **GC** 時間	ノード	カウント	**1** 分

メトリック	ディメンション	単位	最小頻度
ノードの例外	ノード	カウント	1 分
クラススナップショットのステータス	クラスター	値が -1 の場合、スナップショットが存在しないことを示します。 値が 0 の場合、スナップショットが作成済みであることを示します。 値が 1 の場合、スナップショットが作成中であることを示します。 値が 2 の場合は、スナップショットの作成に失敗したことを示します。	1 分

注：

- モニタリングデータは最大 31 日間保持されます。
- モニタリングデータは最大 14 日間連続して表示できます。

・ モニタリングデータの表示

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [Elasticsearch] を選択します。 Elasticsearch ページが表示されます。
3. インスタンスの ID をクリックするか、または [アクション] 列の [モニタリングチャート] クリックして、インスタンスのモニタリングチャートを表示します。
4. [時間範囲]で、事前設定された期間を選択するか、または期間をカスタマイズします。 モニタリングデータは、最大 14 日間連続して表示できます。
5. 任意。 モニタリングチャートの右上隅にある拡大アイコンをクリックして、チャートを拡大します。

アラートサービス

・ アラートルールの設定

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[クラウドサービスモニタリング] > [Elasticsearch] を選択します。 **Elasticsearch** ページが表示されます。
3. インスタンスの **ID** をクリックするか、または [アクション] 列の [モニタリングチャート] をクリックして、インスタンスのモニタリングチャートを表示します。
4. モニタリングチャートの右上隅にあるベルのアイコンをクリックするか、またはページの右上隅にある [アラームルールの作成] をクリックします。 リソース範囲を指定し、アラートルールを設定し、通知方法を設定したら、[確定] をクリックします。

・ パラメーター

アラートルールのパラメーターの詳細については、「アラームルールのパラメーター」をご参照ください。

6.23 OpenSearch

open search のストレージ容量、ドキュメントの総数やその他いくつかのメトリクスをモニターすることで、**CloudMonitor** は **OpenSearch** サービスの全体的なパフォーマンスと使用状況を把握するのに役立ち、それにあわせたアラームルールを設定できます。**CloudMonitor** は、本プロダクトの利用を開始したときから、**OpenSearch** からデータを自動的に収集します。

モニタリングサービス

・ メトリクス

メトリック	ディメンション	単位	最小モニター細分性
Storagecapacity	**APP**	バイト	**10** 分
Storage capacity usage	**APP**	%	**10** 分
Total number of documents	**APP**	項目	**10** 分
QPS	**APP**	カウント/秒	**20** 秒
Maximum QPS	**APP**	カウント/秒	**20** 秒
Query time	**APP**	ミリ秒	**20** 秒
Compute resources	**APP**	**LCU**	**20** 秒

メトリック	ディメンション	単位	最小モニター細分性
Compute resource usage	**APP**	**%**	**20** 秒
Compute consumption by single query	**APP**	**LCU**	**20** 秒

注：

- モニタリングデータは、**31** 日間保存されます。
- 連続 **14** 日分のモニタリングデータを表示することができます。

- モニタリングデータの表示

1. *CloudMonitor* コンソールにログインします。
2. **[**クラウドサービスモニタリング**]** の **[OpenSearch]** インスタンスリストへ移動します。
3. インスタンス名をクリックするか、または **[**アクション**]** 列の **[**モニタリングチャート**]** をクリックして、インスタンスモニタリング詳細ページへアクセスし、さまざまなメトリクスを表示します。
4. 上部メニューから **[**時間範囲**]** クイック選択ボタンをクリックするか、または特定の選択機能を使用します。 連続 **14** 日分のモニタリングデータを表示できます。
5. モニタリングチャートの右上隅にある **[**ズームイン**]** アイコンをクリックして、チャートを拡大表示します。

アラームサービス

- パラメーター
  - メトリクス**: OpenSearch** から取得したモニタリングメトリック
  - 統計サイクル**:** アラームシステムがモニタリングデータがアラームしきい値を超えたかどうかをチェックする繰り返し期間 たとえば、メモリ使用量のアラームルールで統計サイクルが **1** 分に設定されている場合、システムはメモリ使用量がアラームルールで指定されたしきい値を **1** 分おきに超えているかどうかを確認します。
  - 連続回数**:** 一連のサイクルで、メトリック値がアラームルールで指定されたしきい値を継続的に超えた後に、アラームが発生します。 たとえば、連続回数が **3** に設定されている場合、アラームがトリガーされる前に、アラームルールに指定された条件が**3** 回連続した統計サイクルで満たされる必要があります。

- アラームルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. **[クラウドサービスモニタリング]** の **[OpenSearch]** インスタンスリストへ移動します。
  3. インスタンス名をクリックするか、または **[アクション]** 列の **[モニタリングチャート]** をクリックします。
  4. モニタリングチャートの右上隅にある **[ベル]** のアイコン、またはページ右上隅にある **[新しいアラームルール]** をクリックし、このインスタンスの対応する メトリックのアラームルールを設定します。

- 複数 のアラームルールの設定

  1. *CloudMonitor コンソール*にログインします。
  2. クラウドサービスモニタリング] の **[OpenSearch]** インスタンスリストに移動します。
  3. インスタンスリストページで適切なインスタンス を選択します。 **[アラートundefined** ルールの設定]をクリックして、複数のアラームルールを追加します。

7 CloudMonitor 用の RAM

CloudMonitor では、*RAM* 権限がサポートされています。モニタリングコンソールとアクセス制御機能を統合することで、クラウドサービス監視データ、アラームルール管理、アラーム連絡先とアラーム連絡先グループ、およびイベント購読と関連機能に対する権限を簡単かつ迅速に適用できます。

 注：

以下のクラウドプロダクトでは、**RAM**モニタリングデータ クエリがサポートされています。

- **ECS**
- **RDS**
- **Server Load Balancer**
- **OSS**
- **CDN**
- **ApsaraDB for Memcache**
- **EIP**
- **ApsaraDB for Redis**
- メッセージサービス **(Message Service)**
- **Log service**

権限

RAM で **CloudMonitor** の読み取り専用権限が許可されている場合、関連データ (モニタリングデータやアラームサービス)の閲覧のみが可能で、データを書き込むことはできません。

認証タイプ

標準的な **RAM** アカウント権限管理に追加して、時間ベース、マルチファクター、**IP** 認証がサポートされています。

リソース

細粒度リソースの概要は **RAM** ではサポートされていません。 リソースの認証にはワイルドカード **"*"** を使用します。

操作説明

・ データのモニタリング

データクエリアクションは **2** つのカテゴリに分かれます。プロダクトインスタンスリストと **CloudMonitor** メトリックデータクエリです。 **RAM** アカウントを許可し、**CloudMonitor** ポータルにログインしてメトリックデータを表示する際、対応するプロダクトのインスタンスリストとメトリックデータクエリへのアカウント権限も許可する必要があります。

対応するアクションは、以下の表にリストされています。

プロダクト	アクション
CMS	**QuerMetricList**
CMS	**QueryMetricLast**
ECS	**DescribeInstances**
RDS	**DescribeDBInstances**
SLB	**DescribeLoadBalancer***
OSS	**ListBuckets**
OCS	**DescribeInstances**
EIP	**DescribeEipAddresses**
Aliyun Redis 向けクラウド	**DescribeInstances**
メッセージサービス **(Message Service)**	**ListQueue**
CDN	**DescribeUserDomains**

・ アラームサービス

アラームサービスでは、アラームルールの管理、アラーム連絡先やアラーム連絡先グループの管理、イベントサブスクリプション、および関連機能の権限管理を行うことができます。

クエリ関連のアクションは、以下の表にリストされています。

アクション	説明
QueryAlarm	アラームルールの照会
QueryAlarmHistory	アラーム履歴の照会
QueryContactGroup	連絡先グループの照会
QueryContact	連絡先の照会
QuerySms	使用されている **SMS** の数を照会する

アクション	説明
QueryMns	イベントサブスクリプション設定の照会

次の表に、管理関連の操作を示します。

アクション	説明
UpdateAlarm	アラームルールの変更
CreateAlarm	アラームルールの作成
DeleteAlarm	アラームルールの削除
DisableAlarm	アラームルールの無効化
EnableAlarm	アラームルールの有効化
CreateContact	連絡先の作成
DeleteContact	連絡先の削除
UpdateContact	連絡先の変更
SendEmail	メール確認コードの送信
SendSms	**SMS** 確認コードの送信
CheckEmail	メール確認コードの確認
CheckSms	**SMS** 確認コードの確認
CreateGroup	連絡先グループの作成
DeleteGroup	連絡先グループの削除
UpdateGroup	連絡先グループの変更
CreateMns	イベントサブスクリプションの作成
DeleteMns	イベントサブスクリプションの削除
UpdateMns	イベントサブスクリプションの変更

8 アプリケーショングループ

8.1 アプリケーショングループの概要

Cloud Monitor のアプリケーショングループ機能を使用すると、関連リソースをグループ化し、これらのリソースを一元的にモニターできます。 アプリケーショングループを使用すると、サーバー、データベース、**SLB** インスタンス、ストレージなどのターゲットリソースのグループを簡単にモニターし、アプリケーショングループにアラームルールを適用することで全体的な **O&M** 効率を向上させることができます。

注：

- **1** つのアカウントで最大 **100** 個のアプリケーショングループを作成できます。
- **1** つのアプリケーショングループに最大 **1,000** 個のリソースインスタンスを追加できます。

8.2 アプリケーショングループの作成

ここでは、アプリケーショングループを作成してクラウドリソースをグループ化することでリソースとアラームルールをグループごとに管理する方法について説明します。

シナリオ

Alibaba Cloud で複数のプロダクトを購入済みの場合は、アプリケーショングループを作成することで一元的にグループ化することができます。 アプリケーショングループを使用すると、ビジネスモジュールに応じて、異なるリージョンのリソース (サーバー、データベース、オブジェクトストレージ、キャッシュなど) を管理することができます。 さらに、アラームルールの管理や、グループ化されたリソースのモニタリングデータの表示を容易に行うことができます。

アプリケーショングループモード

インスタンスは、動的モードまたは静的モードを使用してアプリケーショングループに追加できます。

- 動的モード：アプリケーショングループを作成する際、名前ルールを満たすインスタンスが自動的にアプリケーショングループに追加されるようインスタンスの名前ルールを設定することができます。 将来、グループにインスタンスを追加またはグループから削除する場合は、インスタンス名を変更するだけでこれらの設定を完了できます。 現在、**ECS**、**ApsaraDB for RDS**、**SLB** インスタンスのみが動的モードに対応しています。

- 静的モード：静的モードでは、アプリケーショングループに手動でインスタンスを追加する必要があります。

アプリケーショングループの作成

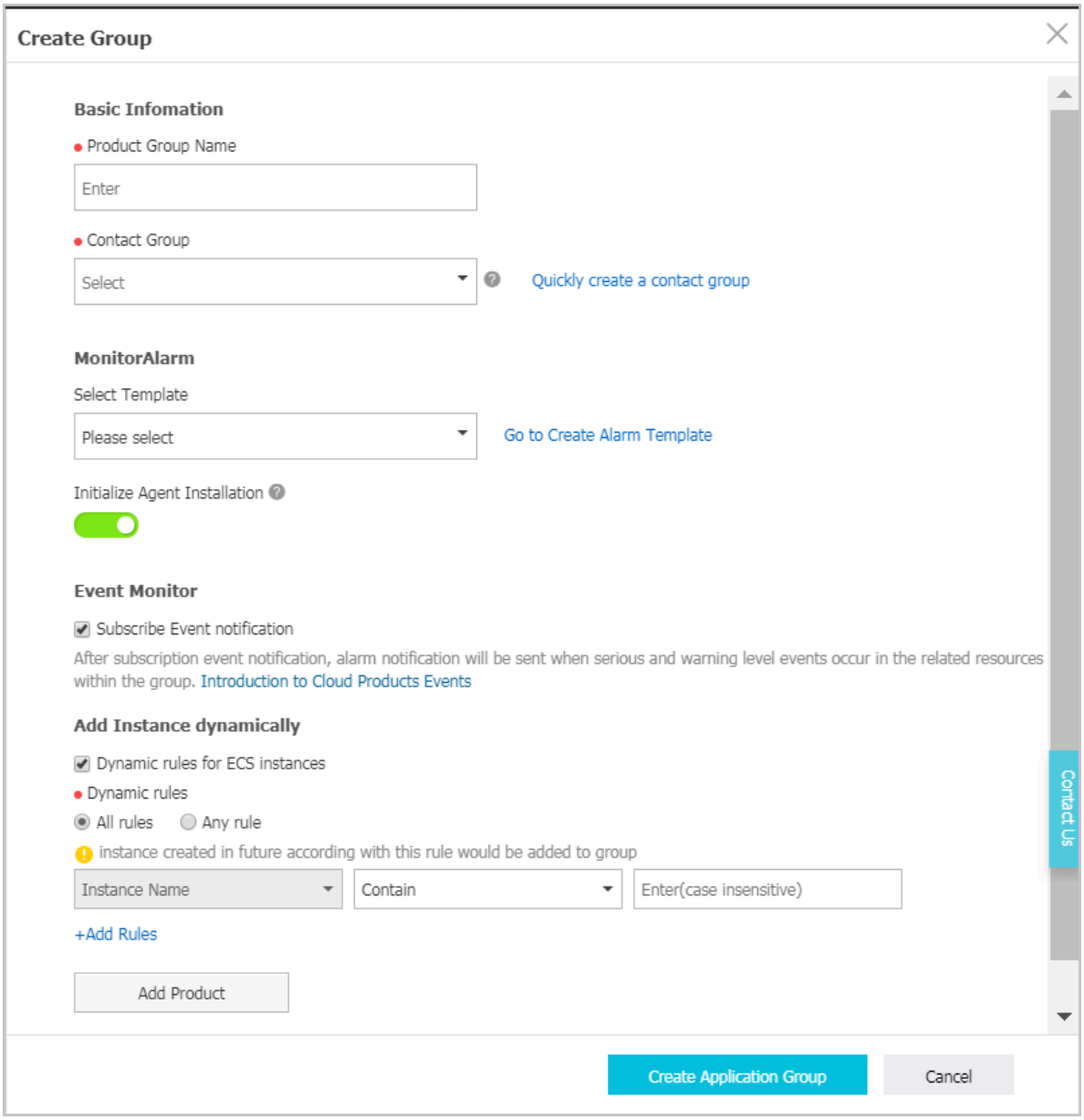
 注：

- 各アプリケーショングループに最大 1,000 個のリソースインスタンスを追加できます。
- 各アカウントで最大 5,000 個のアプリケーショングループを作成できます。

手順

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。

3. 表示されるページの右上隅にある [グループの作成] をクリックします。



4. [基本情報] の入力：グループ名を入力し、アラーム通知を受信する 1 つ以上の連絡先グループを選択します。
5. **MonitorAlarm** の設定 ：1 つ以上のテンプレートを選択して、グループ内のインスタンスのアラームルールを初期化し (任意)、通知方法を選択します。 [エージェントインストールの初期化] スイッチをオンにした場合、モニタリングデータを収集するために **CloudMonitor** エージェントがグループ内のすべてのサーバーにインストールされます。
6. [イベントモニター] の設定：[イベント通知の登録] チェックボックスを選択すると、グループ内の関連リソースでクリティカルレベルまたは警告レベルのイベントが発生した際、アラーム通知が送信されます。

7. [インスタンスを動的に追加] の設定
   - 名前ルールを設定して、名前ルールに一致する ECS インスタンスを自動的にグループに追加することができます。 具体的には、名前に指定の単語を含むインスタンス、指定の単語で始まるインスタンス、指定の単語で終わるインスタンス (将来作成されるインスタンスを含む) が自動的にグループに追加されます。 最大 3 つのルールを追加でき、ルール間の関係は AND または OR になります。
   - ApsaraDB for RDS または SLB インスタンスのルールを追加するには、 [プロダクトの追加] をクリックします。
   - その他の Alibaba Cloud プロダクトのインスタンスを追加するには、アプリケーショングループを作成した後にそれらを手動で追加する必要があります。
8. [アプリケーショングループの作成] をクリックします。

8.3 アプリケーショングループの詳細の確認

グループ詳細ページには、障害リスト、アラーム履歴、アラームルール、グループリソース、イベント、およびグループリソースメトリックデータが含まれています。 このページを使って、アプリケーショングループの上記詳細をモニターすることができます。

グループリスト

CloudMonitor 上のすべてのアプリケーショングループは、各グループのリソースとヘルスステータスと共に、グループ詳細ページに表示されます。

パラメーター

- グループ名（または ID): アプリケーショングループの名前または識別番号。
- ヘルスステータス: 任意のグループリソースのアラームステータス。 アプリケーショングループは、グループ内のどのリソースに対してもアクティブなアラームがトリガーされていない場合は正常ですが、グループ内のリソースのメトリックしきい値が満たされてアラームがトリガーされた場合は正常ではありません。
- インスタンス数: アプリケーショングループ内の、ECS インスタンスと非 ECS インスタンス両方を含む、インスタンスの総数。
- リソースタイプ: アプリケーショングループ内のリソースタイプの数。 たとえば、アプリケーショングループに ECS、ApsaraDB for RDS、および Server Load Balancer インスタンスが含まれている場合、この数は 3 です。

- 異常状態のインスタンス: アプリケーショングループ内でアクティブなアラームが発生しているインスタンスの総数。 たとえば、2 つの ECS インスタンスと1つの ApsaraDB for RDS インスタンスにアクティブなアラームがある場合、異常なインスタンスの数は 3 です。
- 作成時刻: アプリケーショングループが作成された時刻。
- アクション: アプリケーショングループに適用できるアクション。 サポートされているアクションタイプは、管理、通知の停止、すべてのアラームルールの有効化と無効化、およびグループの削除です。

障害リスト

グループ内でアクティブなアラームを持つリソースは障害リストに表示され、異常なインスタンスを簡単に見分けられ、原因をすばやくトラブルシューティングするのに役立ちます。

注:

- リソースの複数のメトリックに同時にアクティブなアラームがある場合、障害リストにはリソースが複数回表示されます。 リストの各行は、アクティブなアラームを含むメトリックを示しています。
- アクティブなアラームのあるアラームルールを無効にすると、そのルールに関連付けられているリソースとメトリックは、障害リストに表示されなくなります。

パラメーター

- 障害のあるリソース: アクティブなアラームがあるリソース。
- 開始時刻: リソースに対して最初のアラームが生成された時刻。
- ステータス: リソースにアクティブなアラームがあるかどうかを示します。
- 期間: 障害のリソースがアラーム状態にある期間。
- アラームルール名: 障害のあるリソースに適用されるアラームルールの名前。
- アクション: 障害のリソースに適用できるアクション。 [展開] をクリックすると、過去 6 時間にアクティブなアラームがある障害リソースのメトリック傾向が表示され、メトリックデータをアラームしきい値と比較できます。

アラーム履歴

アラーム履歴では、グループに適用されているすべてのアラームルールのアカウントが提供されます。

注:

過去3日間のアラーム履歴をリクエストできます。 クエリの開始時刻と終了時刻の間隔が3日を超えると、システムから時間範囲を再選択するように求められます。

パラメーター

- 障害のあるリソース: アクティブなアラームがあるリソース。
- 期間: 障害のリソースがアラーム状態にある時間。
- 発生時刻: アラームが発生した時刻。
- アラームルール名: : 障害のリソースに適用されたアラームルール名。
- 通知方法: SMS、Eメール、TradeManagerなど、アラーム通知を送信する方法。
- プロダクトタイプ: 障害のリソースが属するプロダクトタイプ。
- ステータス: アラームステータス、クリアステータス、ミュート状態など、アラームルールのステータス。
- 通知先: アラーム通知を受け取る連絡先のグループ。

アラームルール

グループに適用されているすべてのアラームルールのリストが、アラームルールリストに表示されます。 リストから目的にかなったアラームルールを選択し、要件に基づいてルールを有効化、無効化、または変更できます。

注 :
アラームルールリストには、特定のアプリケーショングループに適用されているアラームルールのみが表示されます。"リソース範囲" が "すべてのリソース" または "インスタンス" に設定されているアラームルールは表示されません。

パラメーター

- アラーム名: アラームルールを作成したときに指定したアラームルールの名前。
- ステータス: アラームルールに関連付けられているリソースにアクティブなアラームがあるかどうかを表示します。
  - 標準状態: アラームルールに関連付けられているすべてのリソースが正常なことを示します。
  - アラーム状態: アラームルールに関連付けられている少なくとも 1 つのインスタンスにアクティブなアラームがあります。
  - データが不十分: アラームルールに関連付けられている少なくとも 1 つのインスタンスにデータ不足があり、どのインスタンスにもアクティブなアラームがありません。
- 有効化: アラームルールが有効かどうかを示します。

- プロダクト名: グループリソースが属するプロダクトの名前。
- アラームの説明: アラームルール設定の簡単な説明。
- アクション: オプションの操作には、変更、有効化、無効化、削除、およびアラーム履歴があります。
  - 変更: クリックして、アラームルールを変更します。
  - 無効化: クリックして、アラームルールを無効にします。 アラームルールが無効になると、アラームサービスはメトリックデータがしきい値を超えているかどうかを確認しません。
  - 有効化: クリックして、アラームルールを有効にします。 以前に無効にしたアラームルールを有効にすると、アラームサービスはメトリックデータを確認し、アラームルールに基づいてアラームをトリガーするかどうかを決定します。
  - 削除: クリックして、アラームルールを削除します。
  - アラーム履歴: クリックして、アラームルールのアラーム履歴を表示します。

グループリソース

グループのすべてのリソースとこれらリソースの正常性条件を表示します。

パラメーター

- インスタンス名 (または ID): リソースのインスタンス名または ID。
- ヘルスステータス: 任意のグループリソースのアラーム状態。 アプリケーショングループは、グループ内のどのリソースに対してもアラームがトリガーされていない場合は正常ですが、グループ内のいずれかのリソースについてアラームがトリガーされている場合は異常です。

イベント

追加、変更、削除アクションなどのアラームルール操作イベントのアラーム履歴とレコードがサポートされているため、特定のアラームルールに対して実行された操作を追跡できます。

> 注:
> 過去 90 日間のイベント情報をクエリできます。

パラメーター

- 発生時刻: イベントが発生した時刻。
- イベント名: イベントの名前。発生したアラームやクリアされたアラームなどのアラームイベント、あるいはアラームルールの作成、アラームルールの変更、アラームルールの削除などのシステムイベントがあります。
- イベントタイプ: イベントのタイプ。システムイベントとアラームイベントに分けることができます。システムイベントの種類には、アラームルールの作成、アラームルールの削除、およ

びアラームルールの変更があります。 アラームイベントの種類には、発生したアラームとクリアされたアラームがあります。

・ イベントの詳細: イベントに関連した詳細情報。

グラフ

アプリケーショングループ詳細ページの下のエリアには、グループリソースのモニタリング詳細が表示されます。デフォルトでは、**CloudMonitor** は頻繁に使用されるメトリックデータを初期化します。 表示されるチャートタイプとメトリックデータを変更して、エリアをカスタマイズすることを選択できます。

注:

ECS の **OS** メトリックスを取得するには、**CloudMonitor** エージェントをインストールする必要があります。

初期化されたメトリックデータ

デフォルトでは、**CloudMonitor** は次のアプリケーショングループデータを開始し、これらはすべて折れ線グラフに表示されます。 さらにメトリックデータを表示する場合、**[Add Metric Chart]** をクリックして、データにメトリックを追加します。

プロダクト	メトリック	グラフの種類	説明
ECS	**CPU**使用率とアウトバウンド帯域幅 (インターネット)	折れ線グラフ	グループ内の全サーバの集計データを表示します。
<td class="en-UStry align-left colsep-1 rowsep-1">ApsaraDB for RDS</td>	**CPU**使用率、ディスク使用率、**IOPS**使用率、接続使用率	折れ線グラフ	単一のデータベースインスタンスのデータを表示します。
Server Load Balancer	オウトバウンド帯域幅とインバウンド帯域幅	折れ線グラフ	単一の **Server Load Balancer** インスタンスのデータを表示します。
OSS	ストレージサイズと **GET/PUT** リクエスト数	折れ線グラフ	単一のバケットのデータを表示します。
CDN	ダウンストリーム帯域幅とヒット率	折れ線グラフ	単一ドメイン名のデータを表示します。

プロダクト	メトリック	グラフの種類	説明
EIP	アウトバウンド帯域幅(インターネット)	折れ線グラフ	単一インスタンスのデータを表示します。
ApsaraDB for Redis	メモリ使用率、接続使用率、および**QPS**使用率	折れ線グラフ	単一インスタンスのデータを表示します。
ApsaraDB for MongoDB	**CPU**使用率、メモリ使用率、**IOPS**使用率、および接続使用率	折れ線グラフ	単一インスタンスのデータを表示します。

8.4 アプリケーショングループの変更

シナリオ

サービスのサイズ変更や技術的なアーキテクチャ改善の要件を満たすためにアプリケーションがより多くのクラウドプロダクトを使用する際は、アプリケーショングループ内のリソースを変更する必要があります。

アプリケーションの**O**&**M**および開発の担当者が変更された場合、アプリケーショングループのアラーム連絡先グループを変更する必要があります。

注:

- アプリケーショングループからリソースを削除されると、そのアプリケーショングループに設定されているアラームルールは、削除されたインスタンスに適用されません。
- インスタンスがグループに追加されると、そのインスタンスはそのアプリケーショングループに設定されたアラームルールに自動的に関連付けられます。 インスタンスのアラームルールを作成する必要はありません。

基本情報の変更

アプリケーショングループ名または連絡先グループを変更するには、対象のアプリケーショングループの詳細ページに移動します。 **[**基本情報**]** で、グループ名または連絡先グループ情報の横にある鉛筆のアイコンをクリックします。 名前または連絡先グループを変更して **[OK]** をクリックします。

インスタンスの追加または削除

1. インスタンスを削除するには、対象プロダウトのタブをクリックし、対象のインスタンスを特定し、[アクション] の列にある [削除] をクリックします。

2. インスタンスを追加するには、対象プロダクトのタブをクリックし、タブページの右上隅にある[インスタンスの追加] をクリックします。 表示された **AddResource** ページで、対象のインスタンスを選択して [確定] をクリックします。

新しいカテゴリの追加

対象のアプリケーショングループの詳細ページに移動します。 [カテゴリの追加] をクリックします。 表示された **AddResource** ページで、対象のプロダクトとインスタンスを選択し、 [確定] をクリックします。

8.5 アラームルールの管理

アプリケーショングループで、しきい値アラームルールの作成、表示、変更、有効化、無効化、および削除ができます。

> 注：
> アプリケーショングループのアラームルールを表示すると、このアプリケーショングループに適用されているアラームルールだけがシステムで表示されます。グループ内のインスタンスまたはリソースに適用されているアラームルールは表示されません。

アラームルールの作成

1. *Cloud Monitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
3. 対象のグループを見つけて、グループ名をクリックします。
4. 右上隅の [しきい値アラーム] をクリックします。
5. プロダクトの種類を選択し、1 つまたは複数のアラームルールを追加します。アラームメカニズムを設定し、連絡先グループを選択し、[追加] をクリックします。

アラームテンプレートを使ったアラームルールの作成

1. *Cloud Monitor コンソール* にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
3. 対象のグループを見つけて、グループ名 をクリックします。
4. 表示されたページの右上隅の [グループにテンプレートを適用] をクリックします。
5. 必要なアラームテンプレートを選択し、**[OK]** をクリックします。

アラームルールの削除

1. *Cloud Monitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
3. 対象のアプリケーショングループを見つけて、グループ名 をクリックします。
4. 左側のナビゲーションウィンドウで、[アラームルール] をクリックします。
5. 対象のアラームルールを見つけ、"アクション" の [削除] をクリックしてこのルールを削除します。 一度に複数のルールを削除するには、削除する複数のルールを選択して、アラームルールの一覧の下にある [削除] をクリックします。

アラームルールの変更

1. *Cloud Monitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
3. 対象のアプリケーショングループを見つけて、グループ名 をクリックします。
4. 左側のナビゲーションウィンドウで、[アラームルール] をクリックします。
5. 対象のアラームルールを見つけ、"アクション" の [変更] をクリックしてルールを変更します。

アラームルールの有効化または無効化

アプリケーションのメンテナンスまたはアップグレードのためにサービスを停止したい場合、不要なアラーム通知を避けるためにアプリケーショングループのすべてのアラームルールを無効化できます。 メンテナンスまたはアップグレード完了後、アラームルールを有効化できます。

・ アプリケーショングループのすべてのアラームルールの無効化

1. *Cloud Monitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
3. 対象のアプリケーショングループを見つけ、"アクション" の [詳細] をクリックします。
4. [すべてのアラームルールの無効化] をクリックします。

- アプリケーショングループのすべてのアラームルールの有効化

  1. *Cloud Monitor コンソール*ログインします。
  2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
  3. 対象のアプリケーショングループを見つけ、"アクション" の [詳細] をクリックします。
  4. [すべてのアラームルールの有効化] をクリックします。

- アプリケーショングループの一部のアラームルールの無効化

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
  3. 対象のアプリケーショングループを見つけて、グループ名 をクリックします。
  4. 左側のナビゲーションウィンドウで、[アラームルール] をクリックします。
  5. 対象のアラームルールを見つけ、"アクション" の [無効化] をクリックしてこのルールを無効にします。 この手順を繰り返して他のアラームルールを無効化するか、複数のルールを選択してアラーム一覧の下にある [無効化] をクリックします。

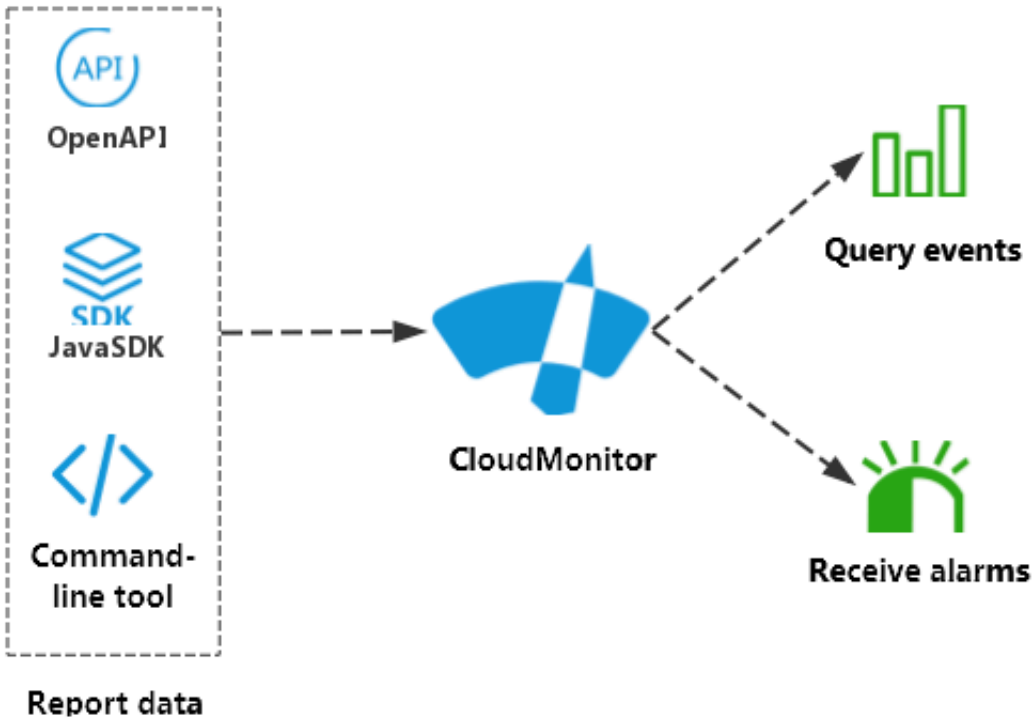
- アプリケーショングループの一部のアラームルールの有効化

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
  3. 対象のアプリケーショングループを見つけて、グループ名 をクリックします。
  4. 左側のナビゲーションウィンドウで、[アラームルール] をクリックします。
  5. 対象のアラームルールを見つけ、"アクション" の [有効化] をクリックしてこのルールを有効にします。 この手順を繰り返して他のアラームルールを有効化するか、複数のルールを選択してアラーム一覧の下にある [有効化] をクリックします。

9 イベントモニタリング

9.1 イベントモニタリングの概要

イベントモニタリングでは、イベント関連データのレポート、照会、およびアラームモニタリング機能が提供されるため、ビジネスオペレーションにおけるさまざまな例外や重要な変化がすばやく簡単にモニターおよびレポートされます。 イベントモニタリングによって、イベント関連の例外が発生するとすぐにアラーム通知の受信もできるようになります。



イベントモニタリングとカスタマイズモニタリングの違いは以下のとおりです。

- イベントモニタリングでは、不連続イベントモニタリングデータをレポートおよび照会し、アラームルールで指定された条件が満たされるとアラームが生成されます。
- カスタマイズモニタリングでは、定期的に収集された時系列モニタリングデータをレポートおよび照会し、アラームルールで指定された条件が満たされるとアラームが生成されます。

イベントモニタリング処理

- イベントデータのレポート

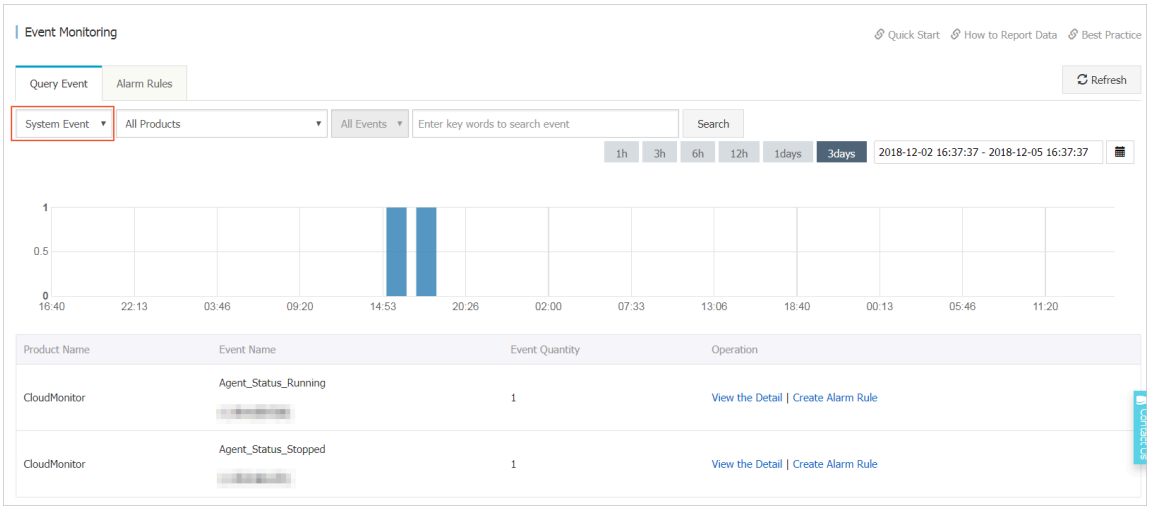
  詳細は、「カスタムイベントデータのレポート」をご参照ください。

- イベントデータの照会

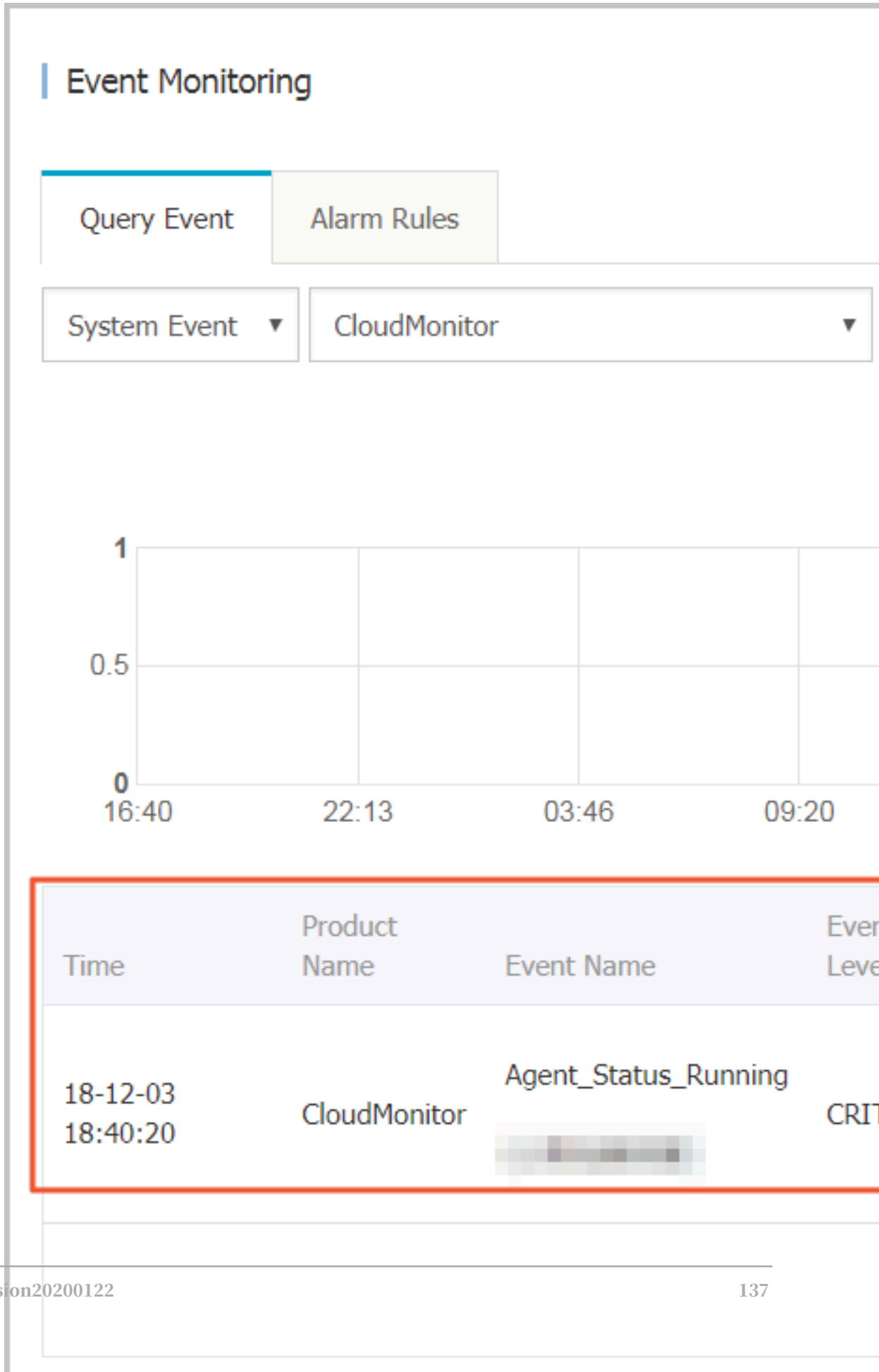
  Cloud Monitor コンソールで、報告されたイベントデータを照会できます。 イベントモニタリングページですべてのイベントを表示することも、特定のアプリケーショングループを入力してそのグループのイベントを表示することもできます。

  報告されたすべてのイベントを表示させるには、以下の手順に従います

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[イベントモニタリング] をクリックします。
  3. 次の図に示すように、イベントモニタリングページで、[システムイベント] または [カスタマイズイベント] にあるすべてのイベントを表示できます。



4. 特定のイベントの詳細を表示するには、対象のイベントの右側にある [詳細を表示] をクリックします。



特定のグループのイベントを照会するには、そのグループのイベントモニタリングページに移動します。

- アラームルールの設定

  イベントモニタリングでは、アラームレポート機能が提供されます。 アラームルールを設定するときは、対応するアプリケーショングループを選択する必要があります。 アラームが生成

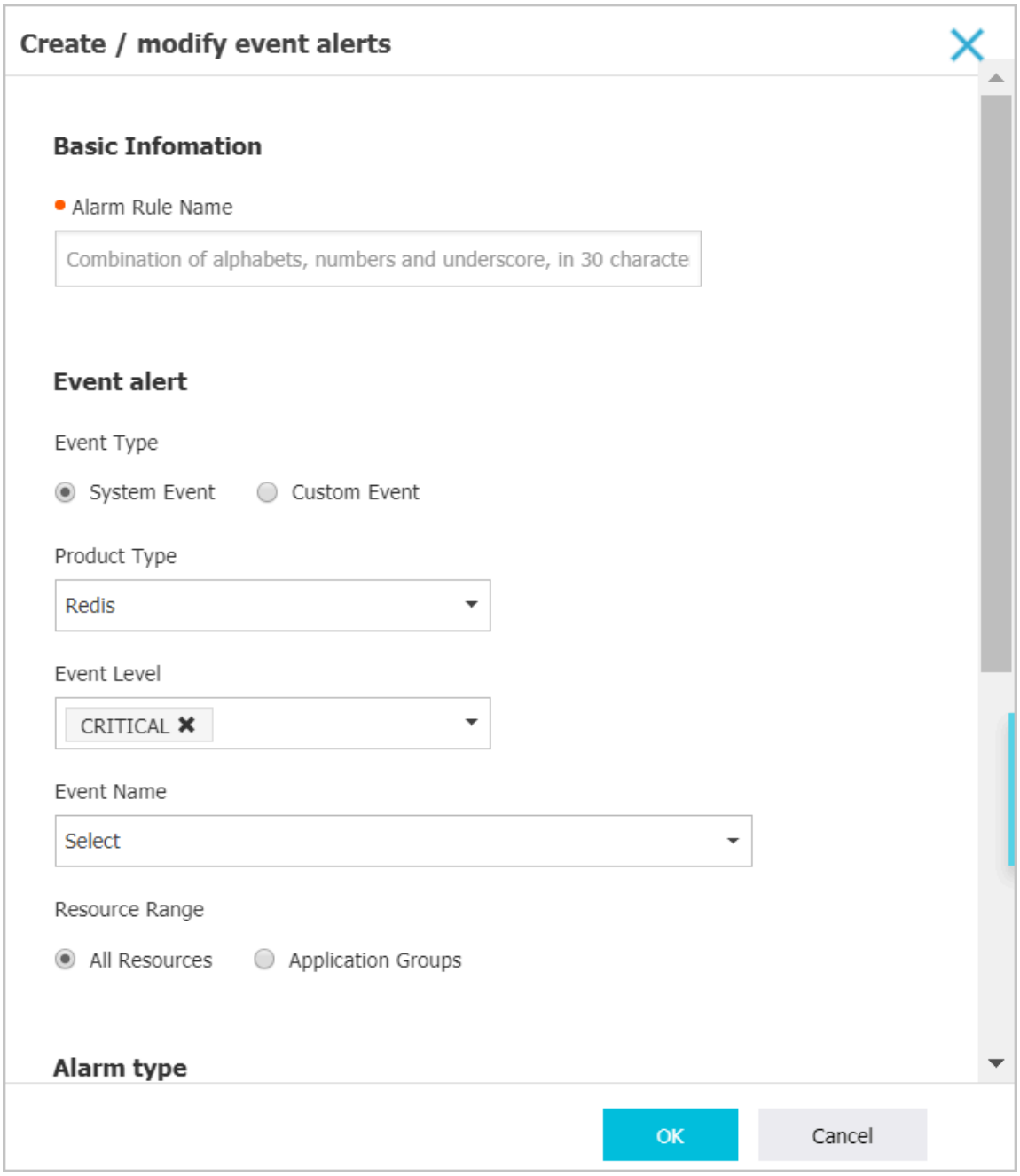
されると、通知がアラーム連絡先グループに送信されます。 イベントにアラームルールを設定するには、次の 2 つの方法のいずれかを使用します。

- 方法 1：

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[イベントモニタリング] をクリックします。
  3. ターゲットイベントの右側にある [アラームルールの作成] をクリックします。
  4. 表示される[イベントアラームの作成/変更]ダイアログボックスで、アラームルールの名前を入力し、対応するルールと通知方法を設定し、**[OK]** をクリックします。

- 方法 2：

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。
  3. 対象グループ名をクリックします。
  4. 左側のナビゲーションウィンドウで、[イベントモニタリング] をクリックします。
  5. ターゲットイベントの右側にある [アラームルールの作成] をクリックします。
  6. 表示される [イベントアラームの作成/変更] ダイアログボックスで、アラームルールの名前を入力し、対応するルールと通知方法を設定し、**[OK]** をクリックします。



9.2 クラウド製品イベント

9.2.1 クラウドサービスイベントの表示

イベントモニタリングでは、さまざまなクラウドサービスによって生成されたすべてのシステムイベントの統計の照会および表示ができます。 これらのサービスの運用状況の概要を取得できます。

アプリケーショングループを使用してリソースを分類すると、サービス関連のシステムイベントがさまざまなグループのリソースに自動的に関連付けられます。 これにより、あらゆる種類のモニタリング情報を統合し、すばやく問題を分析・特定します。

サービスごとのシステムイベントの表示

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで、[イベントモニタリング] をクリックします。 イベントモニタリングページが表示されます。 イベントタイプを [システムイベント] に設定します。 サービスのドロップダウンリストからサービスを選択し、イベントのドロップダウンリストからイベントを選択します。 時間範囲を選択します。 指定した時間範囲内に発生したイベントが表示されます。
3. イベントに対応する [アクション] 列で [詳細を表示] をクリックして、イベントの詳細を表示します。

グループごとのシステムイベントの表示

インスタンスをアプリケーショングループごとに管理する場合、特定のアプリケーショングループにアクセスして、グループ内のインスタンスに関連するシステムイベントを表示することも可能です。

1. *CloudMonitor* コンソールにログインします。
2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。 アプリケーショングループページが表示されます。
3. グループ名をクリックして、グループの詳細ページに移動します。
4. グループの詳細ページで、左側のナビゲーションウィンドウの [イベントモニタリング] をクリックします。 イベントモニタリングページには、グループ内のインスタンスに関連するシステムイベントが表示されます。

9.2.2 システムイベントアラームの使用

シナリオ

1 つ以上の **Alibaba Cloud** プロダクトにおいてシステムイベントが発生したとき、システムイベント例外を迅速に把握し、これらのイベント関連例外の処理を自動化するため、イベントモニタリングのアラーム機能は次の通知方法を提供します。

・ システムイベントのアラーム通知は、音声、テキスト、または電子メールメッセージとして送信されます。

- システムイベントは、**MNS** キュー、機能サービス、および **URL** コールバックに配信されます。

アラームルールの作成

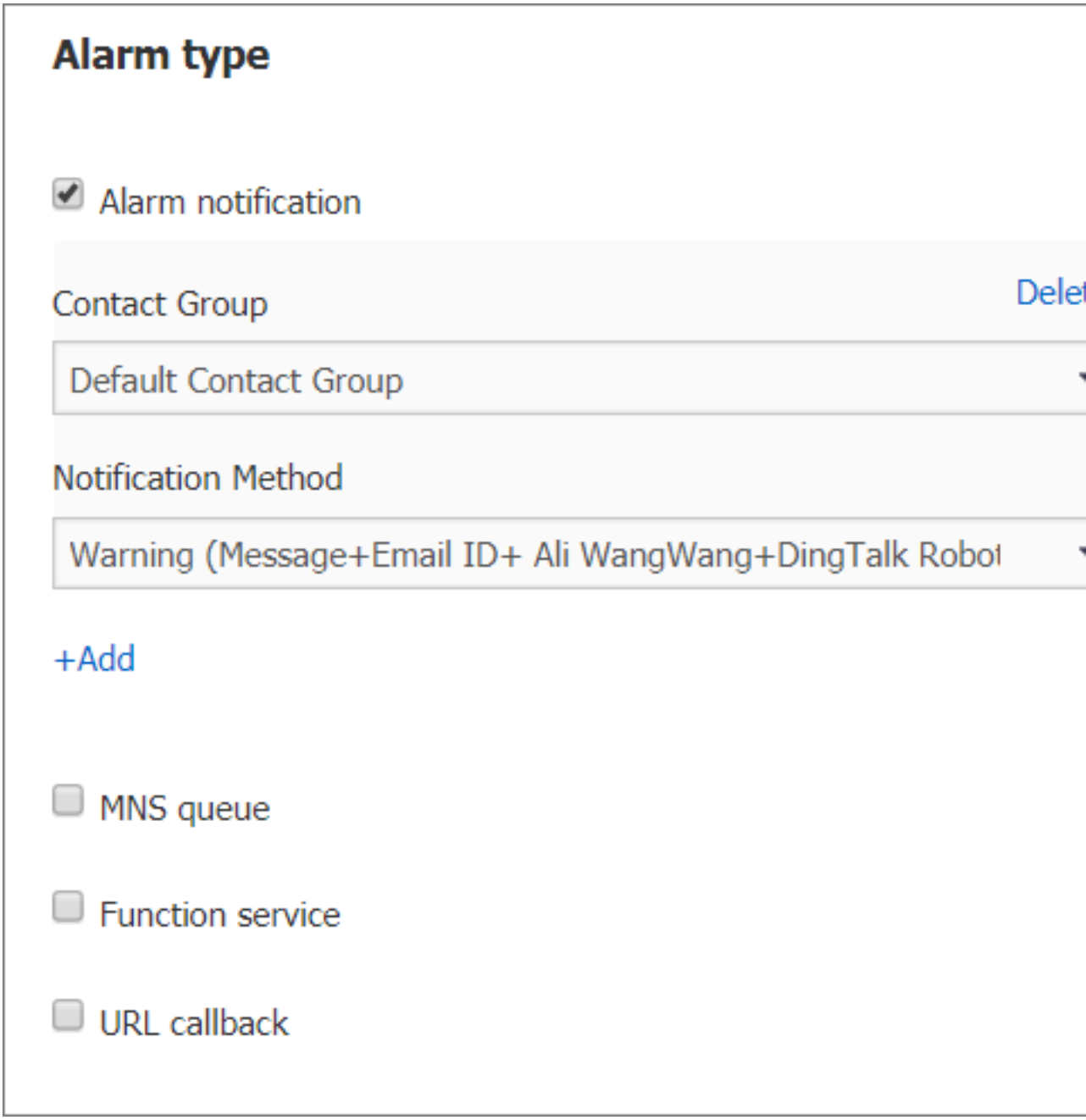
1. *Cloud Monitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[**イベントモニタリング**]** をクリックします。
3. **[**アラームルール**]** タブページで、右上隅にある **[** イベントアラームの作成**]** をクリックします。 **[**イベントアラームの作成/変更**]** ダイアログボックスが表示されます。
4. 基本情報エリアで、アラームルール名を入力します。
5. **[**イベントアラーム**]** エリアで、以下の情報を入力します。

   a. イベントの種類**:** システムイベントを選択します。

   b. プロダクトの種類、イベントレベル**,** イベント名**:** 要件に基づいて情報を入力してください。

   c. リソース範囲**: [**すべてのリソース**]** または **[**アプリケーショングループ**]** を選択します。 **[**すべてのリソース**]** を選択した場合、リソース関連の例外について通知が送信されます。 **[**アプリケーショングループ**]** をクリックした場合、指定した **1** つまたは複数のアプリケーショングループ内のリソースに例外が発生したときにのみ通知が送信されます。

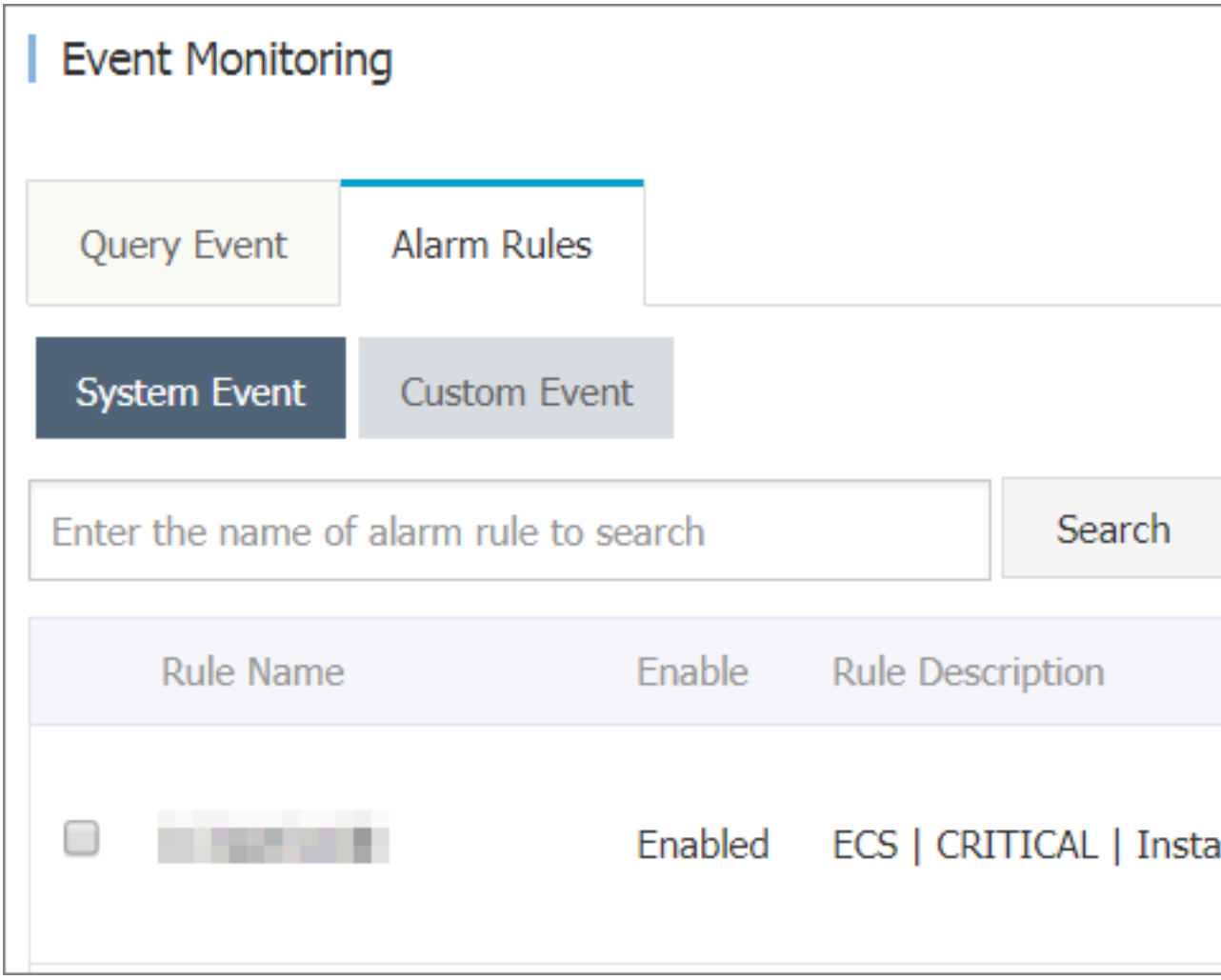
6. アラームの種類を選択します。 **Cloud Monitor** では、アラーム通知、**MNS** キュー、機能サービス、および **URL** コールバックの **4** 種類のアラームがサポートされます。



アラームルールのテスト

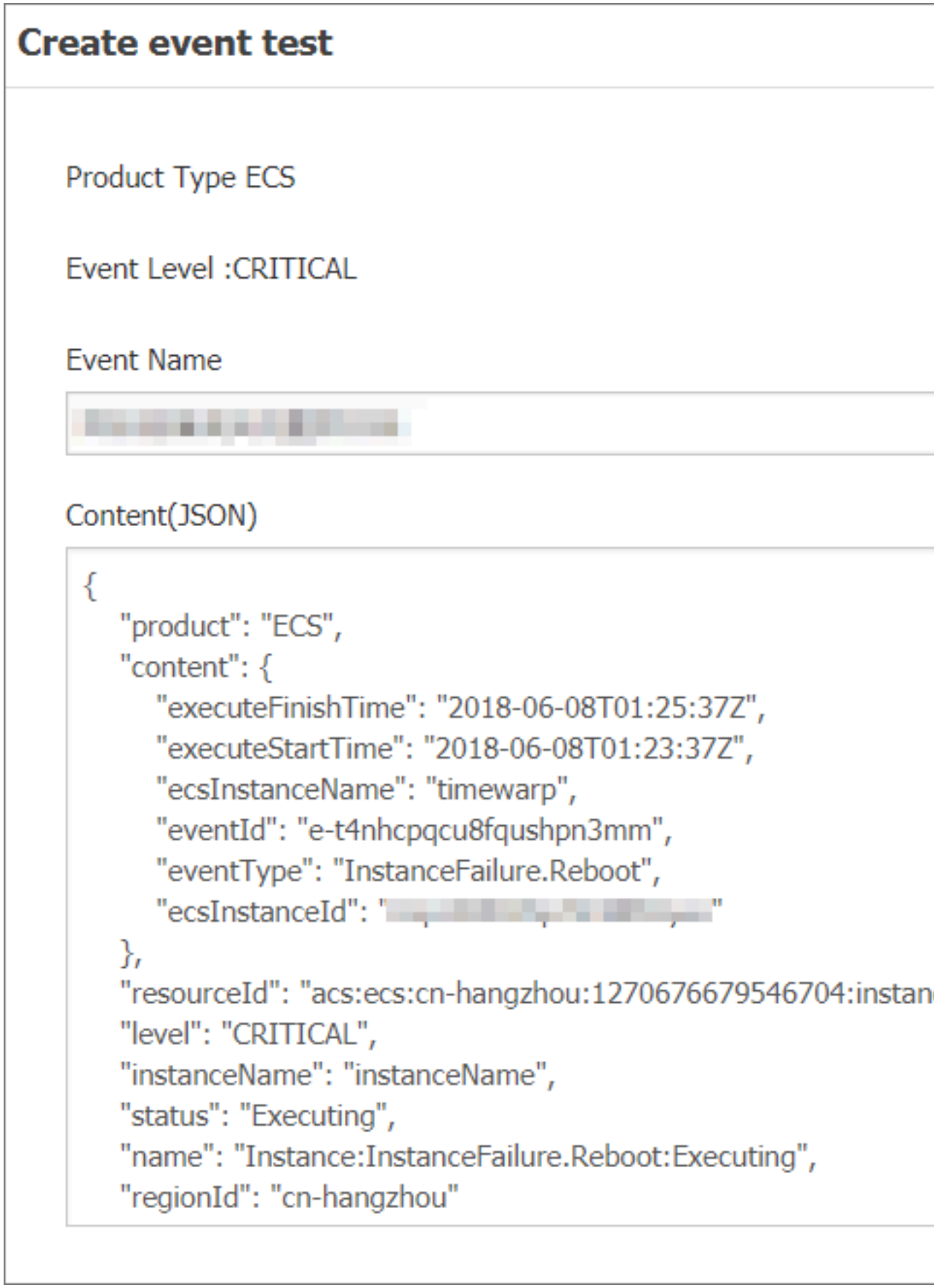
アラームルールに設定されている **MNS** キューおよび機能サービスが正しく機能していることを確認するために、システムイベントアラームテスト機能を使用してシステムイベントの発生をシミュレートできます。

1. イベントモニタリング用の [アラームルール] タブページに移動します。



2. "アクション" の [テスト] をクリックします。
3. テストするイベントをクリックします。 クリックしたイベントに対応するコンテンツが表示されます。 要件に基づいて、インスタンス **ID** などの表示されたフィールドを変更できます。
4. **[OK]** をクリックすると、システムはその内容に基づいてイベントを送信し、アラームルールで指定したアラーム通知、**MNS** キュー、

機能サービス、および **URL** コールバック設定をトリガーしま
す。



9.3 カスタムイベント

9.3.1 カスタムイベントデータのレポート

イベントモニタリングには、カスタムイベントをレポートするための **API** が複数用意されています。 これらの **API** を使用してイベント関連の例外を収集し、**CloudMonitor** にレポートできます。 イベント関連の例外発生時にアラート通知を受信できるようにアラートルールを構成することもできます。

CloudMonitor は、**API**、**Java SDK**、および **Alibaba Cloud CLI** を使用したデータのレポーティングに対応しています。

制限事項

- **1** 件の **Alibaba Cloud** アカウントから送信できるレポートリクエストの数は、**1** 秒あたり最大 **20** 件です。
- **1** 回のレポートで送信できるイベント数は、最大 **100** 件です。
- **1** 回のレポートで送信できるデータサイズは、最大 **500 KB** です。

API を使用したデータのレポート

- エンドポイント

  `https://metrichub-cms-cn-hangzhou.aliyuncs.com`

- リクエストの構文

```
POST /event/custom/upload HTTP/1.1
Authorization:<AuthorizationString>
Content-Length:<Content Length>
Content-MD5:<Content MD5>
Content-Type application/json
Date:<GMT Date>
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-signature:hmac-sha1
x-cms-api-version:1.0
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
[{"content":"EventContent","groupId":GroupId,"name":"EventName","
time":"20171023T144439.948+0800"}]
```

- リクエストパラメーター

名前	タイプ	必須/任意	説明
name	**String**	必須	イベント名

名前	タイプ	必須/任意	説明
groupId	**Numerical**	必須	イベントが属するアプリケーショングループの **ID**
time	**String**	必須	イベントの発生時刻
content	**String**	必須	イベントの詳細

・ リクエストヘッダーの定義

下表に、イベントモニタリング用 **API** のリクエストヘッダーを示します。

ヘッダー	型	説明
Authorization	文字列	認証文字列。 内容**: AccessKeyId:SignString**
User-Agent	文字列	クライアントの説明。
Content-MD5	文字列	リクエスト本文の値で **MD5** ハッシュを計算して取得した、すべて大文字の文字列。 リクエストに本文がない場合は不要。
Content-Length	数値	**RFC 2616** に定義された、**HTTP** リクエストの本文の長さ。 リクエストに本文がない場合は不要。
Content-Type	文字列	**HTTP** リクエストの本文のタイプ。 有効な値**: applicatio n** および **json**。
Date	文字列	**HTTP** リクエストの標準タイムスタンプヘッダー。 このヘッダーは、**RFC 1123** 形式に準拠し、**GMT** を使用 **(**例**: Mon, 3 Jan 2010 08:33:47 GMT)** 。
Host	文字列	**HTTP** リクエストの完全なホスト名。 **(https://** などのプロトコルヘッダーは含まれない。 例**: metrichub-cms -cn-hangzhou.aliyuncs. com)**

ヘッダー	型	説明
x-cms-api-version	文字列	**API** のバージョン。 現在のバージョンは **1.0**。
x-cms-signature	文字列	署名アルゴリズム。 現在サポートされている署名アルゴリズムは **HMAC-SHA1** のみ。
x-cms-ip	文字列	イベントをレポートするサーバーの **IP** アドレス (例: **10.1.1.1**)。

- 署名アルゴリズム

  現在サポートされている署名アルゴリズムは **HMAC-SHA1** のみです。

  1. **Alibaba Cloud AccessKey** のペアを準備します。

     API リクエストのデジタル署名を生成するには、**AccessKey ID** と **AccessKey Secret** で構成される**AccessKey** のペアを使用する必要があります。 既存の **AccessKey** のペアを使用することも、新しいペアを作成して使用することもできます。 **AccessKey** のペアは、アクティブである必要があります。

  2. リクエストの署名文字列を生成します。

     API 署名文字列は、**HTTP** リクエストのメソッド、ヘッダー、および 本文で構成されます。

     ```
     SignString = VERB + "\n"
                  + CONTENT-MD5 + "\n"
                  + CONTENT-TYPE + "\n"
                  + DATE + "\n"
                  + CanonicalizedHeaders + "\n"
                  + CanonicalizedResource
     ```

     上記の式で、`\n` は改行エスケープ文字を示し、プラス記号 (+) は文字列連結演算子を示します。 他の部分は次のように定義されます。

名前	定義	例
VERB	**HTTP** リクエストのメソッド名。	**PUT**、**GET**、および **POST**。
CONTENT-MD5	**HTTP**リクエストの本文の **MD5** の値。すべて大文字の文字列。	**875264590688CA6171F6228AF5BBB3D2**
CONTENT-TYPE	リクエストの本文のタイプ。	**application/json**

名前	定義	例
DATE	**HTTP** リクエストの標準タイムスタンプヘッダー。**RFC1123** 形式に従い、**GMT** を使用。	**Mon, 3 Jan 2010 08:33:47 GMT**
CanonicalizedHeaders	**HTTP** リクエストで **x-cms** および **x-acs** のプレフィックスが付加されたカスタムヘッダーによって構成された文字列。	**x-cms-api-version:0.1.0\nx-cms-signature**
CanonicalizedResource	**HTTP** リクエストのリソースで構成された文字列 (後述)。	**/event/custom/upload**

CanonicalizedHeaders の作成方法は次のとおりです。

a. プレフィックス `x-cms` および `x-acs` が付加されたすべての **HTTP** リクエストヘッダーの名前を小文字に変換します。

b. 上記の手順で取得した **CMS** カスタムリクエストヘッダーを昇順に並べ替えます。

c. リクエストヘッダーとコンテンツの間の区切り文字の両側のスペースを削除します。

d. すべてのヘッダーとコンテンツを区切り記号 (`\n`) で区切り、最終的な**CanonicalizedHeaders** を作成します。

CanonicalizedResource の作成方法は次のとおりです。

a. **CanonicalizedResource** を空の文字列 (""）として設定します。

b. アクセス先の **URI** (例: `/event/custom/upload`) を引用符の間に挿入します。

c. リクエストにクエリ文字列 (`QUERY_STRING`) が含まれている場合、疑問符 (`?`) を付加し、さらにクエリ文字列を **CanonicalizedResource** 文字列の最後に追加します。

`QUERY_STRING` は、**URL** に含まれるリクエストパラメーターの辞書式文字列です。 パラメーターの名前と値の間に等号 (`=`) を挿入した文字列を作成します。 パラメーターの

名前と値のペアは、辞書順に並べ替えられ、アンパサンド (&) で接続されて文字列を作成します。 式は次のとおりです。

```
QUERY_STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"
```

3. リクエストのデジタル署名を生成します。

現在サポートされている署名アルゴリズムは **HMAC-SHA1** のみです。 次の式を使用して署名を生成します。

```
Signature = base16(hmac-sha1(UTF8-Encoding-Of(SignString),
AccessKeySecret))
```

・ レスポンスの要素

HTTP ステータスコード **200** が返されます。

・ 例

- リクエストの例

```
POST /event/custom/upload HTTP/1.1
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version:1.0
Authorization:YourAccKey:YourAccSecret
Host:metrichub-cms-cn-hangzhou.aliyuncs.com"
Date:Mon, 23 Oct 2017 06:51:11 GMT
Content-Length:180
x-cms-signature:hmac-sha1
Content-MD5:E9EF574D1AEAAA370860FE37856995CD
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
Content-Type:application/json
[{"content":"123,abc","groupId":100,"name":"Event_0","time":"
20171023T144439.948+0800"}]
```

- レスポンスの例

```
{
  "code":"200",
  "msg":""//The returned msg is null when the reporting is normal.
}
```

Java SDK を使用したデータのレポート

・ **Maven**の依存関係

```
<dependency>
    <groupId>com.aliyun.openservices</groupId>
    <artifactId>aliyun-cms</artifactId>
    <version>0.1.2</version>
```

```
</dependency>
```

・サンプルコード

```
public void uploadEvent() throws CMSException, InterruptedException
 {
        // Initialize the client.
        CMSClient cmsClient = new CMSClient(endpoint, accKey, secret
);
       //Construct two events to be reported.
         CustomEventUploadRequest request = CustomEventUploadRequest
.builder()
                    .append(CustomEvent.builder()
                            .setContent("abc,123")
                            .setGroupId(101l)
                            .setName("Event001").build())
                    .append(CustomEvent.builder()
                            .setContent("abc,123")
                            .setGroupId(101l)
                            .setName("Event002").build())
                    .build();
            CustomEventUploadResponse response = cmsClient.
putCustomEvent(request);
            List<CustomEvent> eventList = new ArrayList<CustomEvent
>();
            eventList.add(CustomEvent.builder()
                    .setContent("abcd,1234")
                    .setGroupId(101l)
                    .setName("Event001").build());
            eventList.add(CustomEvent.builder()
                    .setContent("abcd,1234")
                    .setGroupId(101l)
                    .setName("Event002").build());
            request = CustomEventUploadRequest.builder()
                    .setEventList(eventList).build();
            response = cmsClient.putCustomEvent(request);
```

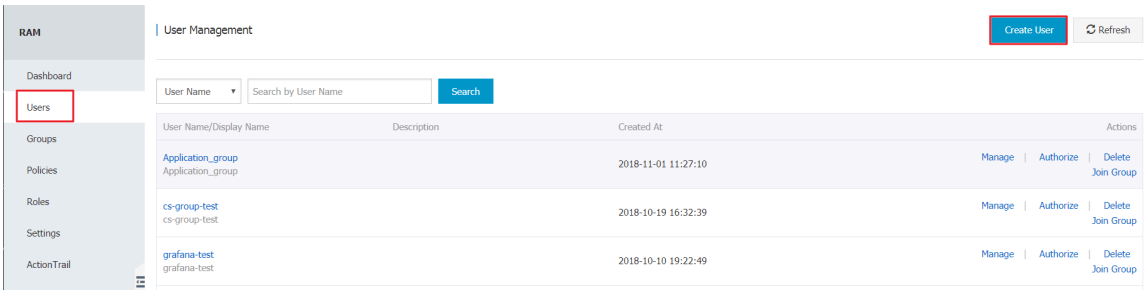
```
        }
```

Alibaba Cloud CLI を使用したデータのレポート

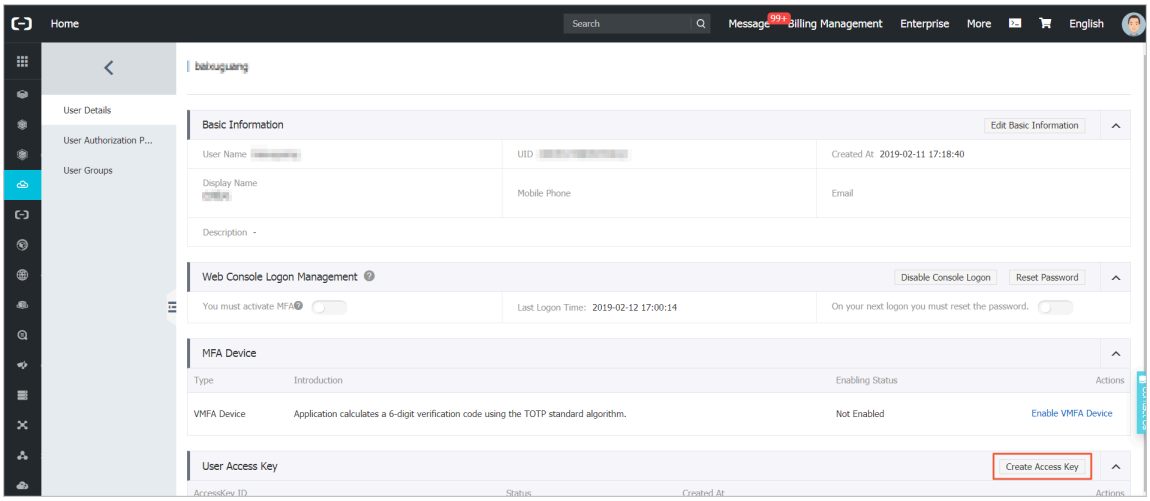
1. 前提条件

   Alibaba Cloud アカウントおよびアカウントで使用する **RAM** ユーザーを作成し、また **CloudMonitor** 権限が付与された **RAM** ユーザー用のアクセスキーを生成します。

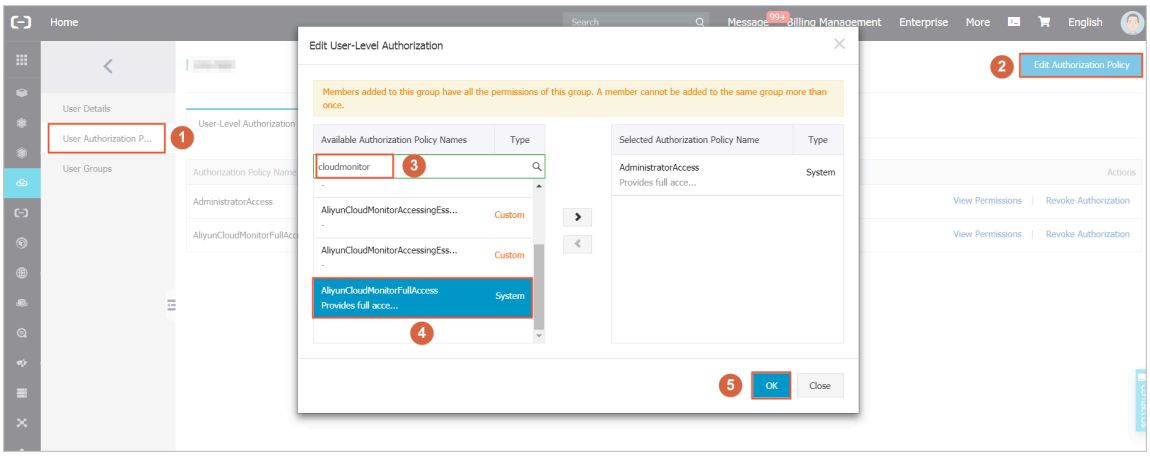
   a. **RAM** ユーザーを作成します。



   b. **RAM** ユーザーの **AccessKey ID** と **AccessKey Secret** を生成します。



   c. **RAM** ユーザーに **CloudMonitor** 権限を付与します。



2. CMS SDK のインストール

   - Windows でのインストール方法は次のとおりです。

     ```
     cd C:\Python27\Scripts
     pip install aliyun-python-sdk-cms
     ```

     次のコマンドを実行して Logtail をアップグレードします。

     ```
     pip install --upgrade aliyun-python-sdk-cms
     ```

   - Linux でのインストール方法は次のとおりです。

     ```
     sudo pip install aliyun-python-sdk-cms
     ```

     次のコマンドを実行して Logtail をアップグレードします。

     ```
     sudo pip install –upgrade aliyun-python-sdk-cms
     ```

3. モニタリングデータのレポート

   PutEvent API を使用して、モニタリングデータをレポートします。

   - Windows での例：

     ```
     aliyuncli.exe cms PutEvent --EventInfo "[{'content':'helloworld','
     time':'20171013T170923.456+0800','name':'ErrorEvent','groupId':'
     27147'}]"
     ```

   - Linux での例：

     ```
     aliyuncli cms PutEvent --EventInfo "[{'content':'helloworld','time
     ':'20171023T180923.456+0800','name':'ErrorEvent','groupId':'27147
     '}]"
     ```

   - データのレポートが正常に処理された場合、、ステータスコード 200 が返されます。

     ```
     {
     "Code": "200"
     }
     ```

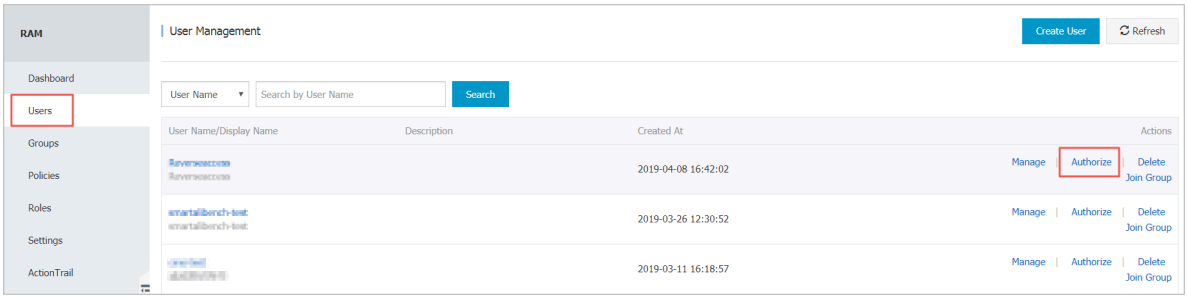
エラーコード

エラーコード	説明
200	正常
400	クライアントリクエストの構文エラー
403	検証失敗、制限速度、または権限不足
500	内部サーバーエラー

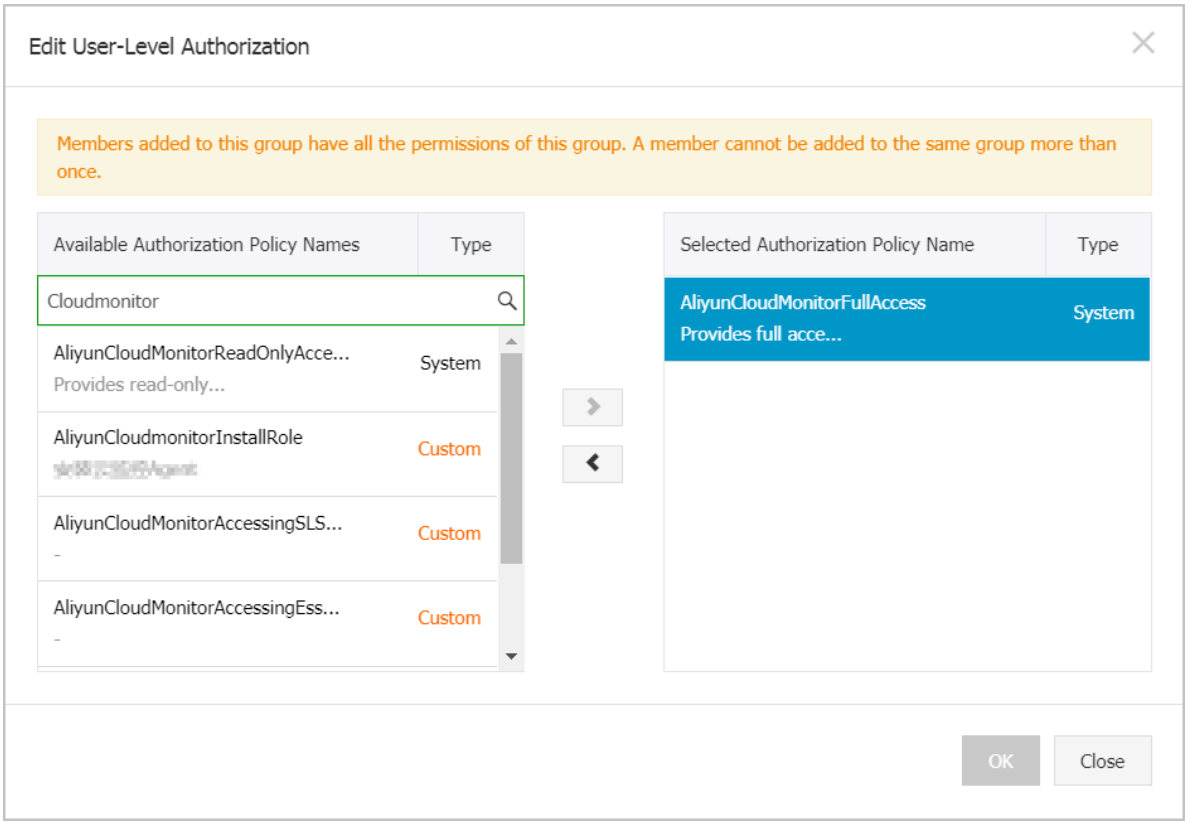
RAM ユーザーの認証

RAM ユーザーのアクセスキーでイベントデータをレポートするには、**RAM** ユーザーに **CloudMonitor** 権限を付与する必要があります。 権限を付与しなかった場合、データのレポート時に、「イベントをアップロードできません。認証に **RAM** を使用してください」というメッセージが表示されます。

1. *RAM コンソール* にログインします。
2. 左側のナビゲーションウィンドウで、**[ユーザー]** をクリックします。
3. **[ユーザー]** ページで、**RAM** ユーザーに対応する **[操作]** 列の **[許可]** をクリックします。



4. **[許可]** ページで **[AliyunCloudMonitorFullAccess]** を選択し、 **[OK]** を選択します。



9.3.2 イベントモニタリングのベストプラクティス

ユースケース

例外はサービス実行中に発生する可能性があります。 一部の例外は再試行などの方法で自動的に復元されますが、復元されない例外もあります。 重大な例外は、顧客の業務を中断することさえ

あります。 したがって、これらの例外を記録し、特定の条件が満たされたときにアラームをトリガーするシステムが必要です。 従来の方法では、ファイルログを印刷し、特定のシステム、たとえばオープンソースのELK (ElasticSearch、Logstash、Kibana) にログを収集します。これらのオープンソースシステムは、複数の複雑な分散システムから構成されます。 複雑な技術と高いコストのために、独自でメンテナンスするのが難しくなっています。CloudMonitor はイベントモニタリング機能を提供し、これらの問題を効果的に解決します。

次の例で、イベントモニタリング機能の使用方法について説明します。

ケーススタディ

1. 例外のレポート

   イベントモニタリングは、データレポートのための 2 つの方法、Java SDK と Open API を提供します。 以下は、Java SDK を使用してデータをレポートする方法について説明します。

   a. Maven に依存関係を追加する

   ```
   <dependency>
       <groupId>com.aliyun.openservices</groupId>
       <artifactId>aliyun-cms</artifactId>
       <version>0.1.2</version>
   </dependency>
   ```

   b. SDK の初期化

   ```
   // Here, 118 is the application grouping ID of CloudMonitor.
   Events can be categorized by applications. You can view group IDs
   in CloudMonitor application grouping list.
   CMSClientInit.groupId = 118L;
   // The address is the reporting entry of the event system, which
    is currently the public network address.  AccessKey と Secret /
   key は個人の身元確認に使用されます。
   CMSClient c = new CMSClient("https://metrichub-cms-cn-hangzhou.
   aliyuncs.com", accesskey, secretkey);
   ```

   c. データを非同期にレポートするかどうかを決定します。

   CloudMonitor イベントモニタリングでは、デフォルトで同期レポートポリシーが提供されます。 長所は、簡単にコードが書け、レポートされたイベントは信頼性があり、データが失われないことです。

   しかし、そのようなポリシーにはいくつか問題もあります。 イベントレポートコードはビジネスコードに埋め込まれており、ネットワークの変動が発生した場合にコードの実行が妨げられ、通常のビジネスに影響を与える可能性があります。 多くのビジネスシナリオでは、100% 信頼できるイベントを必要としないため、単純な非同期レポートのカ

プセル化で十分です。イベントを **LinkedBlockingQueue** に書き込み、**ScheduledExecutorService** を使用してバックエンドで非同期にバッチレポートを実行します。

```
//Initialize queue and Executors:
private LinkedBlockingQueue<EventEntry> eventQueue = new
LinkedBlockingQueue<EventEntry>(10000);
private ScheduledExecutorService schedule = Executors.newSingleT
hreadScheduledExecutor();
// Report event:
//Every event contains its name and content. The name is for
identification and the content contains details of the event, in
which the full-text search is supported.
public void put(String name, String content) {
    EventEntry event = new EventEntry(name, content);
     // When the event queue is full, additional events are
discarded directly. You can adjust this policy as needed.
    boolean b = eventQueue.offer(event);
    if (! b) {
        logger.warn("The event queue is full, discard: {}", event
);
    }

//Submit events asynchronously. Initialize scheduled tasks.
Report events in batch by run every second.  You can adjust the
reporting interval as needed.
schedule.scheduleAtFixedRate(this, 1, 1, TimeUnit.SECONDS);
public void run() {
    do {
        batchPut();
    } while (this.eventQueue.size() > 500);

private void batchPut() {
    // Extract 99 events from the queue for batch reporting.
    List<CustomEvent> events = new ArrayList<CustomEvent>();
    for (int i = 0; i < 99; i++) {
        EventEntry e = this.eventQueue.poll();
        if (e == null) {
            break;

        events.add(CustomEvent.builder().setContent(e.getContent
()).setName(e.getName()).build());

    if (events.isEmpty()) {
        return;

     // Report events in batch to CloudMonitor. No retry or retry
 in SDK is added here. If you have high requirement for event
reliability, add retry policies.
    try {
        CustomEventUploadRequestBuilder builder = CustomEven
tUploadRequest.builder();
        builder.setEventList(events);
        CustomEventUploadResponse response = cmsClient.putCustomE
vent(builder.build());
        if (!" 200".equals(response.getErrorCode())) {
            logger.warn("event reporting error: msg: {}, rid:
 {}", response.getErrorMsg(), response.getRequestId());

    } catch (Exception e1) {
         logger.error("event reporting exception", e1);
```

d. イベントレポートのデモ

- デモ **1: http** コントローラーの例外モニタリング

  主な目的は、**HTTP** リクエストに多数の例外が存在するかどうかをモニターすることです。 **1** 分あたりの例外数が一定の限度を超えると、アラームがトリガーされます。 実装の原則は、**Spring** インターセプター、サーブレットフィルタ、その他のテクノロジを使用して **HTTP** リクエストをインターセプトすることです。 例外が発生した場合はログが作成され、アラームルールを設定することでアラームがトリガーされます。

  以下は、イベントレポートのデモです。

```
// Each event should be informative for searching and locating
. Here, map is used for organizing events and converted to Json
 format as event content.
Map<String, String> eventContent = new HashMap<String, String
>();
eventContent.put("method", "GET"); // http request method
eventContent.put("path", "/users"); // http path
eventContent.put("exception", e.getClass().getName()); //
Exception class name for searching
eventContent.put("error", e.getMessage()); // Error message of
exception
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e
)); // Exception stack for locating
// Finally submit the events in the preceding asynchronous
reporting method. Since no retry is performed in asynchronous
reporting, event loss of small probability may happen. However
, it is sufficient for alarms of unknown http exceptions.
put("http_error", JsonUtils.toJson(eventContent));
image.png](http://ata2-img.cn-hangzhou.img-pub.aliyun-inc.com/
864cf095977cf61bd340dd1461a0247c.png)
```

- デモ **2:** バックエンドでスケジュールされたタスクのモニタリングとメッセージ処理

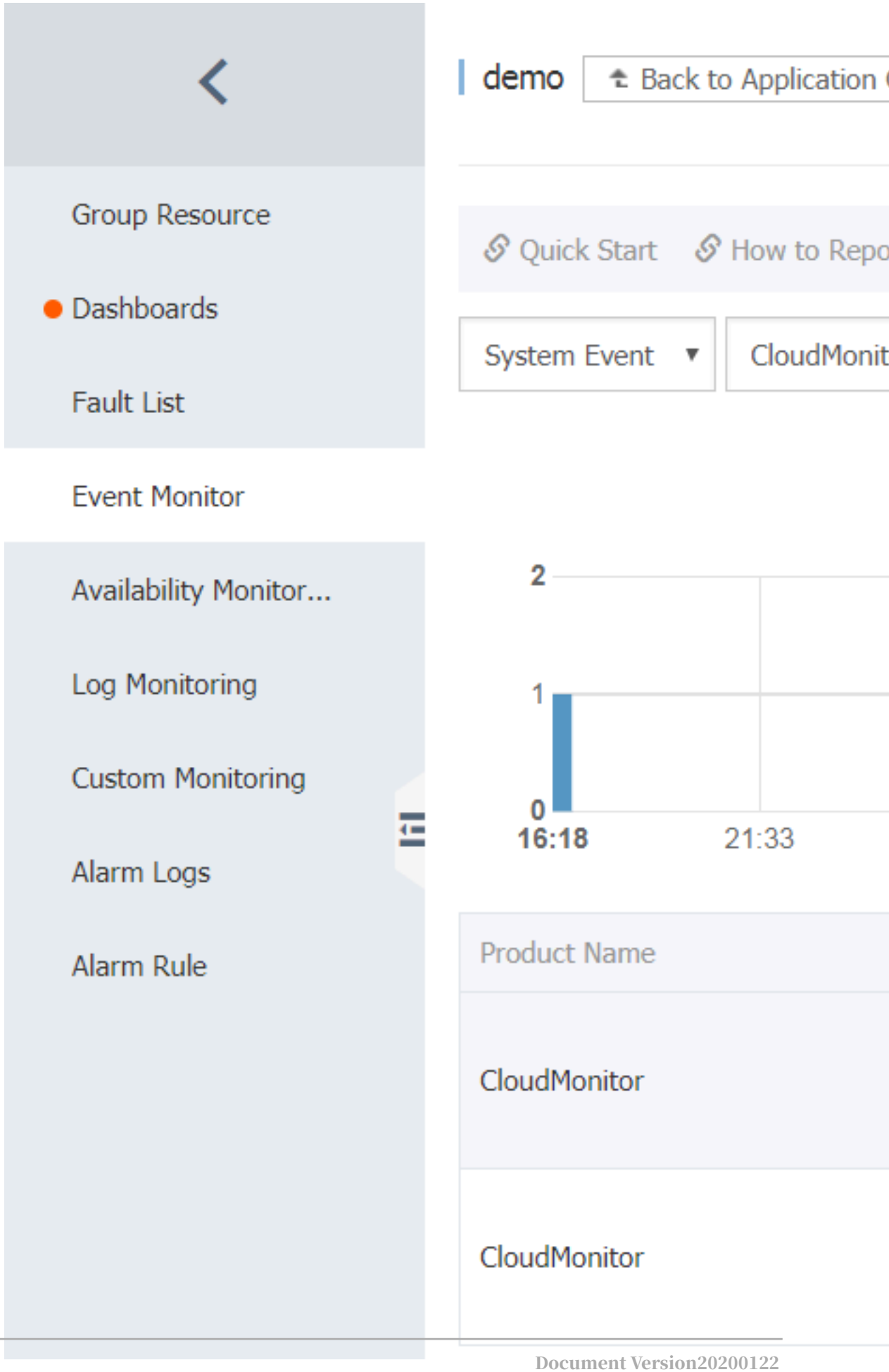
  前述の **http** イベントと同様に、多くの同様のビジネスシナリオではアラームが必要です。 バックエンドタスクやメッセージキュー処理などのビジネスシナリオでは、同様の方法でイベントがレポートされ、効果的なモニタリングが実現できます。 例外が発生したときは、直ちにアラームがトリガーされます。

```
//Event organization of the message queue:
Map<String, String> eventContent = new HashMap<String, String
>();
eventContent.put("cid", consumerId); // Consumer ID
eventContent.put("mid", msg.getMsgId()); // Message ID
eventContent.put("topic", msg.getTopic()); // Message topic
eventContent.put("body", body); // Message body
eventContent.put("reconsume_times", String.valueOf(msg.
getReconsumeTimes())); // The number of retries after message
failure
eventContent.put("exception", e.getClass().getName()); //
Exception class name in case of exception
eventContent.put("error", e.getMessage()); // Exception message
```

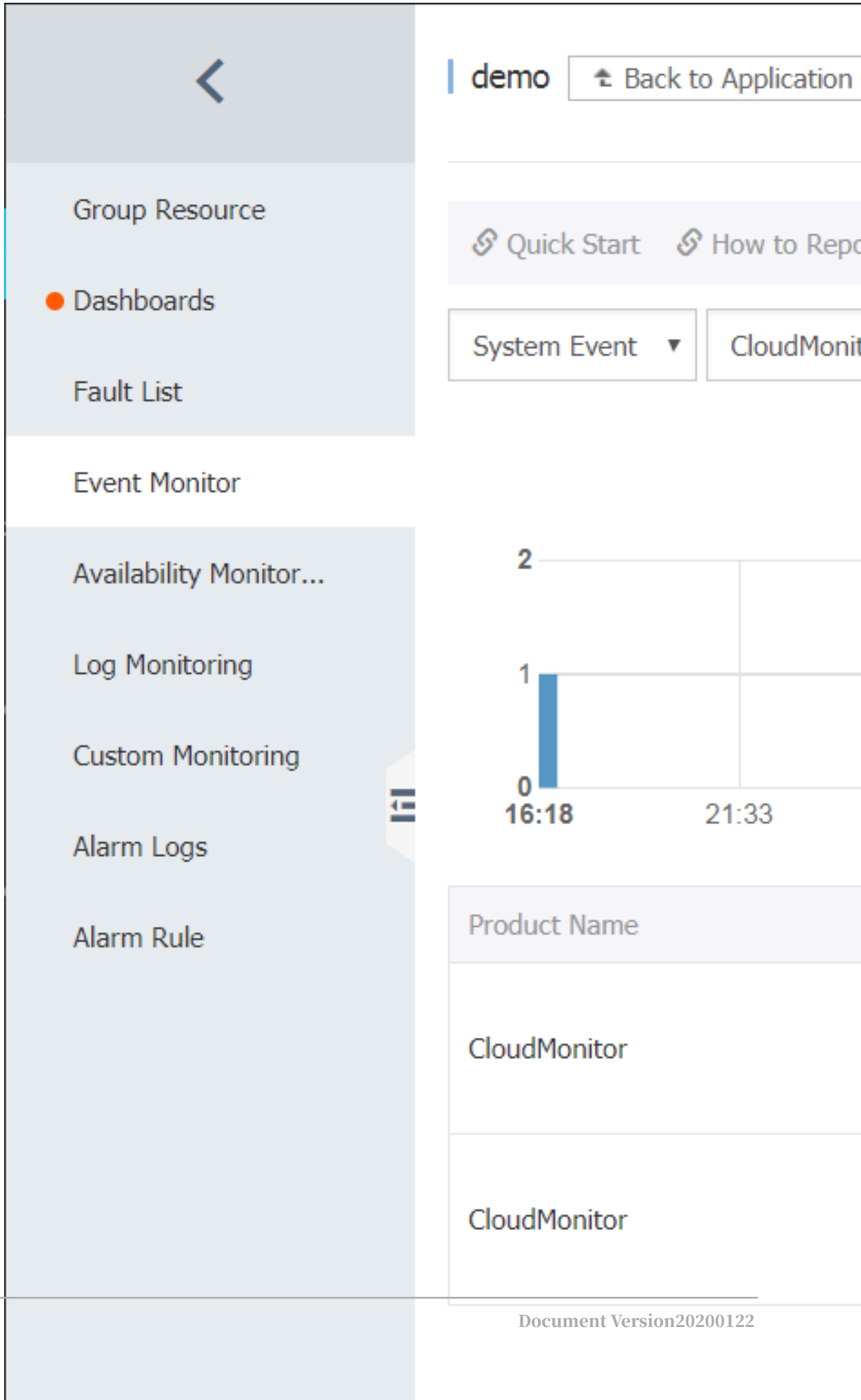
```
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e
)); // Exception stack
// Finally, report the event
```

```
put("metaq_error", JsonUtils.toJson(eventContent));
```

レポート後、イベントを確認します。

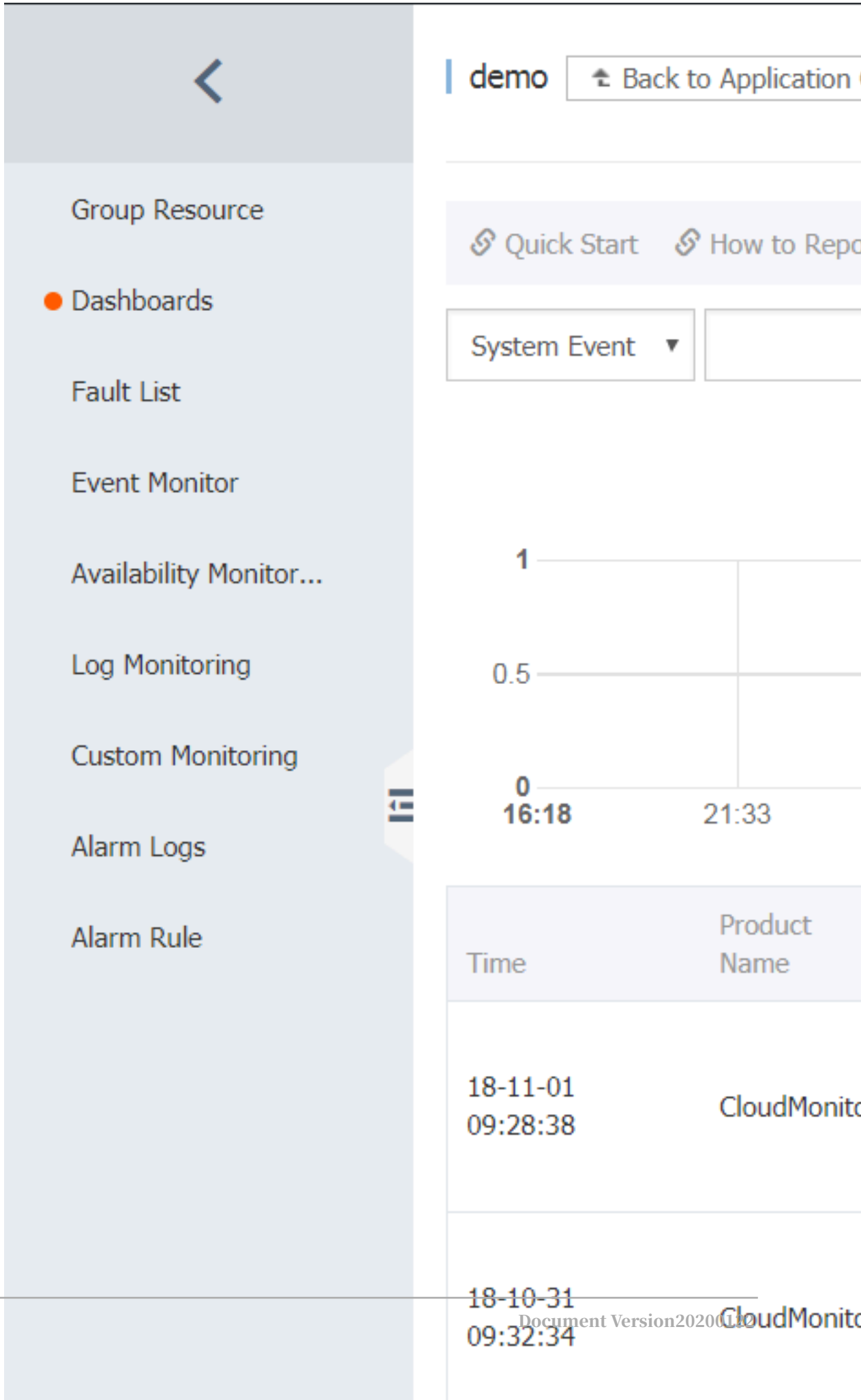

demo
Back to Application
Group Resource
Dashboards
Fault List
Event Monitor
Availability Monitor...
Log Monitoring
Custom Monitoring
Alarm Logs
Alarm Rule
Quick Start
How to Repo
System Event
CloudMonit
2
1
0
16:18
21:33
Product Name
CloudMonitor
CloudMonitor

・ キューメッセージ処理例外のアラームを設定します。


demo
Back to Application
Group Resource
Dashboards
Fault List
Event Monitor
Availability Monitor...
Log Monitoring
Custom Monitoring
Alarm Logs
Alarm Rule
Quick Start
How to Repo
System Event
CloudMonit
2
1
0
16:18
21:33
Product Name
CloudMonitor
CloudMonitor

- デモ 3: 重要なイベントを記録する

  イベントのもう1つのユースケースは、アラームを送信せずに後で確認するための重要なアクションを記録することです。 たとえば、重要な業務、パスワードの変更、注文の変更、リモートログインなどの操作ログなどです。


demo
Back to Application
Group Resource
Dashboards
Fault List
Event Monitor
Availability Monitor...
Log Monitoring
Custom Monitoring
Alarm Logs
Alarm Rule
Quick Start
How to Repo
System Event
1
0.5
0
16:18
21:33
Time
Product Name
18-11-01 09:28:38
CloudMonito
18-10-31 09:32:34
CloudMonito

9.4 リクエストのヘッダー定義

イベントモニタリングインターフェイスのリクエストのヘッダーは以下のように定義されます。

ヘッダー	型	説明
Authorization	**String**	コンテンツ：**AccessKeyId**：**SignString**
User-Agent	**String**	クライアントの説明
Content-MD5	**String**	リクエスト本文の **MD5** ハッシュとして生成された文字列。すべて大文字で表示されます。リクエストに本文がない場合、このリクエストのヘッダーは必要ありません。
Content-Length	**Value**	**RFC 2616** で定義されている **HTTP** リクエスト本文の長さ。 リクエストに本文がない場合、このリクエストのヘッダーは必要ありません。
Content-Type	**String**	**application/json** のみがサポートされています。
Date	**String**	**HTTP** リクエスト内の標準タイムスタンプヘッダー (**RFC 1123** 形式に従い、**GMT** 標準時を使用)：**Mon, 3 Jan 2010 08:33:47 GMT**。
Host	**String**	**HTTP** リクエストの完全なホスト名 (**https://** などのプロトコルヘッダーは含まれません)：**metrichub-cms-cn-hangzhou.aliyuncs.com**
x-cms-api-version	**String**	**API v1.0**
x-cms-signature	**String**	署名アルゴリズム：**HMAC-SHA1**。
x-cms-ip	**String**	イベントをレポートするための **IP**：**10.1.1.1**

10 カスタムモニタリング

10.1 カスタマイズモニタリングの概要

アプリケーションシナリオ

カスタマイズモニタリングでは、測定値とアラームルールのカスタマイズが可能なため、メトリクスをモニター、モニタリングデータをレポート、特定の要件を反映したアラームルールを設定することができます。

カスタマイズモニタリングは、定期的に収集されたタイムシリーズデータをレポートおよび照会するという点において、イベントモニタリングとは異なります。一方、イベントモニタリングは、単一のイベントに関連するデータのみをレポートおよび照会します。

このトピックでは、コンソールでのモニタリングデータのレポート、照会、表示などのカスタマイズモニタリングの操作手順、およびアラームルールの設定方法について説明します。

手順

- モニタリングデータのレポート

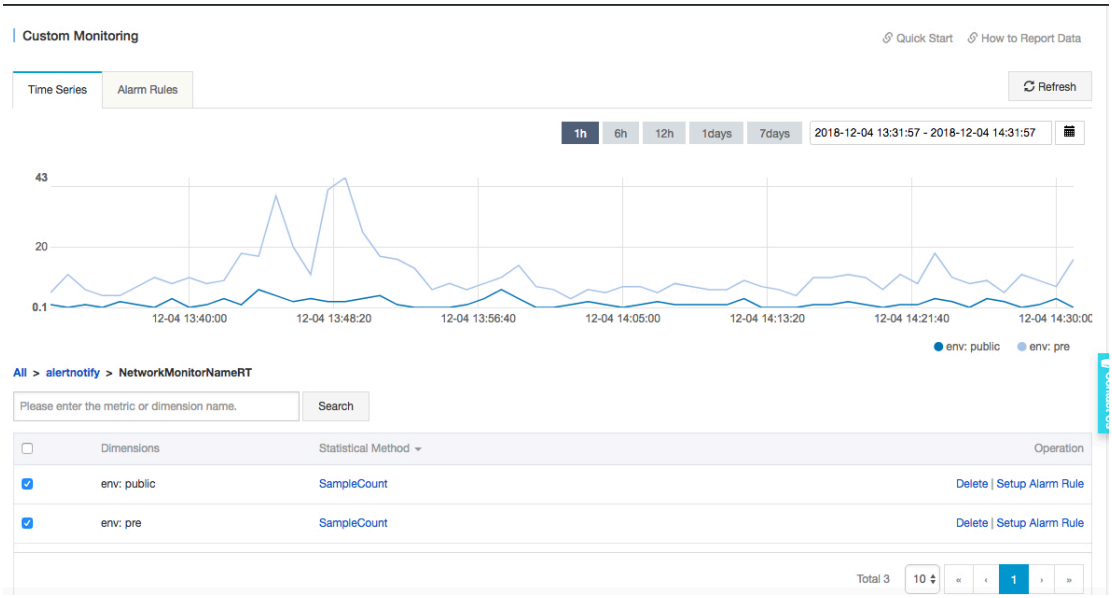
  詳細および使用される特定の手順については、「モニタリングデータのレポート」をご参照ください。

- モニタリングデータの照会

  モニタリングデータをレポートした後、レポートデータをコンソールへ表示できます。 カスタマイズモニタリングページにすべてのモニタリングデータを表示、または 1 つ以上のアプリケーショングループのカスタマイズモニタリングデータを表示するかを選択できます。

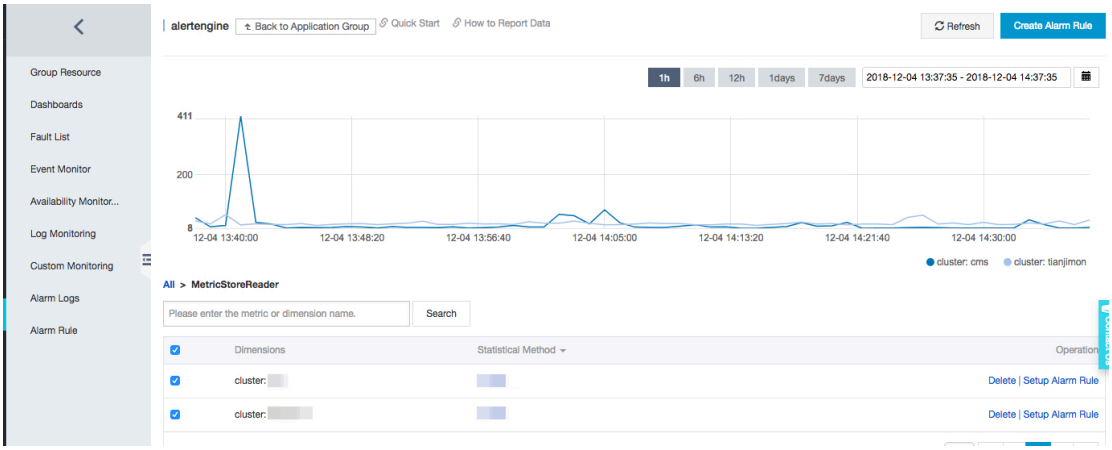
  - すべてのカスタマイズモニタリングデータを表示するには、次の手順を実行します。

    1. *Cloud Monitor コンソール*にログインします。
    2. 左側のナビゲーションウィンドウで、[カスタマイズモニタリング] をクリックします。 カスタマイズモニタリング ページが表示されます。
    3. 対応のアプリケーショングループと測定を順に選択し、タイムシリーズのページにアクセスします。
    4. タイムシリーズを選択し表示します。



  - アプリケーショングループ内のカスタマイズモニタリングデータを表示するには、次の手順を実行します。

    1. *Cloud Monitor コンソール*にログインします。
    2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。 アプリケーショングループ ページが表示されます。
    3. 目的のアプリケーショングループをクリックします。
    4. [カスタマイズモニタリング] をクリックします。 カスタマイズモニタリングページが表示されます。
    5. 対象の測定を選択します。 タイムシリーズページが表示されます。
    6. 表示したい時系列をクリックします。



・ アラームルールの設定

カスタマイズモニタリングでは、アラームレポート機能が提供されます。 アラームルールを設定するには、アプリケーショングループを選択する必要があります。 アラームがトリガーされると、アプリケーショングループのアラームの連絡先に通知が送信されます。 モニタリング

データに対してアラームを生成するには、次の 2 つの方法のいずれかを使用してアラームルールを設定します。

- 方法 1

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[カスタマイズモニタリング] をクリックします。カスタマイズモニタリング ページが表示されます。
  3. 対象するアプリケーショングループと測定を選択します。 タイムシリーズページが表示されます。
  4. アラームルールを作成したいタイムシリーズを選択し、次に "操作"の [アラームルールの設定] をクリックします。
  5. アラームルールの設定ページで、アラームルールの名前を入力し、対応するアラームポリシーと通知方法を設定します。

- 方法 2

  1. *Cloud Monitor コンソール*にログインします。
  2. 左側のナビゲーションウィンドウで、[アプリケーショングループ] をクリックします。アプリケーショングループ ページが表示されます。
  3. 目的のアプリケーショングループを選択します。 カスタマイズモニタリングのページが表示されます。 アラームルールを作成したいタイムシリーズを選択し、次に "操作"の [アラームルールの設定] をクリックします。
  4. アラームルールの設定ページで、アラームルールの名前を入力し、該当する測定値、ディメンション、アラームルール、および通知方法を選択します。

10.2 モニタリングデータのレポート

このトピックでは、カスタムモニタリングデータをレポートする方法について説明します。

カスタムモニタリングを使用すると、独自のビジネスニーズに合わせてメトリックとアラームルールをカスタマイズできます。 カスタムモニタリングでは、モニタリングデータのレポートに使用できる **API** を提供します。 **API** を使用して、収集した時系列データを **CloudMonitor** にレポートできます。 例外が発生したときに通知を受け取るようにアラームルールを設定することもできます。

CloudMonitor は、データをレポートするための **API**、**Java SDK**、および **Alibaba Cloud** コマンドラインインターフェース **(CLI)** を提供します。

制限事項

- 1 秒あたりの照会数 (QPS) は、中国 (北京)、中国 (上海)、中国 (杭州) では 200、中国 (張家口)、中国 (深圳) では 100、その他のリージョンでは 50 に制限されています。
- 最大 100 のデータエントリーが一度にレポートされます。 サイズは 256 KB を超えることはできません。
- `metricName` フィールドには、英数字、およびアンダースコア (_) を使用できます。 また、英字で始める必要があります。 開始文字が英字でない場合は、大文字の A に置き換えられます。無効な文字は、アンダースコア (_) に置き換えられます。
- `ディメンション` フィールドには、等号 (=)、アンパサンド (&)、またはコンマ (,) は使用できません。 無効な文字はアンダースコア (_) に置き換えられます。
- `metricName` と `dimensions` の Key-Value は、64 バイトを超えることはできません。 超えた場合、Key-Value 文字列は切り捨てられます。
- 生データのレポートは有料機能です。 無料版では、データ集計のレポートができます。 データをレポートするときは、リクエストパラメーターの type フィールドに「1」を入力する必要があります。

API を使用してデータをレポートする

API を使用して生データをレポートした後、CloudMonitor は次の統計方法を使用して、1 分間隔と 5 分間隔で統計を計算します。

- **Average:** 平均値
- **Maximum:** 最大値
- **Minimum:** 最小値
- **Sum:** 合計値
- **SampleCount**：カウント
- **SumPerSecond**：合計を対応する集計期間の合計秒数で割ったもの。 移動平均を使用して値を計算することもできます。
- **CountPerSecond**：カウントを対応する集計期間の合計秒数で割ったもの。 移動平均を使用して値を計算することもできます。
- **LastValue**：集計期間内の最後のサンプリング値。 gauge と同様です。
- **P10**：10 パーセンタイルの値。 集計期間内の全データの 10% を超える値です。
- **P20**：20 パーセンタイルの値。 集計期間内の全データの 20% を超える値です。
- **P30**：30 パーセンタイルの値。 集計期間内の全データの 30% を超える値です。
- **P40**：40 パーセンタイルの値。 集計期間内の全データの 40% を超える値です。
- **P50**：50 パーセンタイルの値。 中央値で、集計期間内の全データの 50% を超える値です。

- **P60**：**60** パーセンタイルの値。 集計期間内の全データの **60%** を超える値です。
- **P70**：**70** パーセンタイルの値。 集計期間内の全データの **70%** を超える値です。
- **P75**：**75** パーセンタイルの値。 集計期間内の全データの **75%** を超える値です。
- **P80**：**80** パーセンタイルの値。 集計期間内の全データの **80%** を超える値です。
- **P90**：**90** パーセンタイルの値。 集約期間内の全データの **90%** を超える値です。
- **P95**：**95** パーセンタイルの値。 集計期間内の全データの **95%** を超える値です。
- **P98**：**98** パーセンタイルの値。 集計期間内の全データの **98%** を超える値です。
- **P99**：**99** パーセンタイルの値。 集計期間内の全データの **99%** を超える値です。
- エンドポイント

  インターネットエンドポイント： `https://metrichub-cms-cn-hangzhou.aliyuncs.com`

  次の表に、イントラネットエンドポイントを示します。

リージョン	リージョン ID	エンドポイント
中国 (杭州)	**cn-hangzhou**	**http://metrichub-cn-hangzhou.aliyun.com**
中国 (張家口)	**cn-zhangjiakou**	**http://metrichub-cn-zhangjiakou.aliyun.com**
中国 (上海)	**cn-shanghai**	**http://metrichub-cn-shanghai.aliyun.com**
中国 (北京)	**cn-beijing**	**http://metrichub-cn-beijing.aliyun.com**
中国 (青島)	**cn-qingdao**	**http://metrichub-cn-qingdao.aliyun.com**
中国 (深セン)	**cn-shenzhen**	**http://metrichub-cn-shenzhen.aliyun.com**
中国 (香港)	**cn-hongkong**	**http://metrichub-cn-hongkong.aliyun.com**
中国 (フフホト)	**cn-huhehaote**	**http://metrichub-cn-huhehaote.aliyun.com**
UAE (ドバイ)	**me-east-1**	**http://metrichub-me-east-1.aliyun.com**
米国 (シリコンバレー)	**us-west-1**	**http://metrichub-us-west-1.aliyun.com**

リージョン	リージョン ID	エンドポイント
米国 (バージニア)	**us-east-1**	**http://metrichub-us-east-1.aliyun.com**
日本 (東京)	**ap-northeast-1**	**http://metrichub-ap-northeast-1.aliyun.com**
ドイツ (フランクフルト)	**eu-central-1**	**http://metrichub-eu-central-1.aliyun.com**
オーストラリア (シドニー)	**ap-southeast-2**	**http://metrichub-ap-southeast-2.aliyun.com**
シンガポール	**ap-southeast-1**	**http://metrichub-ap-southeast-1.aliyun.com**
マレーシア (クアラルンプール)	**ap-southeast-3**	**http://metrichub-ap-southeast-3.aliyun.com**
インド (ムンバイ)	**ap-south-1**	**http://metrichub-ap-south-1.aliyuncs.com**

- リクエスト構文

```
POST /metric/custom/upload HTTP/1.1
Authorization:<AuthorizationString>
Content-Length:<Content Length>
Content-MD5:<Content MD5>
Content-Type:application/json
Date:<GMT Date>
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-signature:hmac-sha1
x-cms-api-version:1.0
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
[{"groupId":101,"metricName":"","dimensions":{"sampleName1":"value1
","sampleName2":"value2"},"time":"","type":0,"period":60,"values":{"
value":10.5,"Sum":100}}]
```

- 署名アルゴリズム

  現在、**HMAC-SHA1** 署名アルゴリズムのみがサポートされています。

  1. **Alibaba Cloud AccessKey** ペアを準備します。

     API リクエストのデジタル署名を生成するには、**AccessKey ID** と**AccessKey Secret** で構成される **AccessKey** ペアを使用する必要があります。 既存の **AccessKey** ペアを使用

することも、新しいペアを作成することもできます。 **AccessKey** ペアは有効でなければなりません。

2. リクエストの署名文字列を生成します。

   API 署名文字列は、**HTTP** リクエストの Method、Header、および Body フィールドから構成されます。

```
SignString = VERB + "\n"
             + CONTENT-MD5 + "\n"
             + CONTENT-TYPE + "\n"
             + DATE + "\n"
             + CanonicalizedHeaders + "\n"
             + CanonicalizedResource
```

   上記の式で、\n は改行エスケープ文字を示し、プラス記号 (+) は、文字列連結演算子を示します。 その他の部分は次のように定義されています。

名前	定義	例
VERB	**HTTP** リクエストのメソッド名	**PUT**、**GET**、**POST**
CONTENT-MD5	**HTTP** リクエストの Body フィールドの **MD5** 値。 値は大文字の文字列でなければなりません。	**875264590688CA6171F6228AF5BBB3D2**
CONTENT-TYPE	リクエスト内の Bodyフィールドの型	**application/json**
DATE	**HTTP** リクエスト内の標準タイムスタンプヘッダー **(RFC 1123** 時刻形式に従い、**GMT** 標準時を使用)	**Mon, 3 Jan 2010 08:33:47 GMT**
CanonicalizedHeaders	**HTTP** リクエストで **x-cms** および **x-acs** という接頭辞が付いたカスタムヘッダーで構成された文字列	**x-cms-api-version:0.1.0\nx-cms-signature**

名前	定義	例
CanonicalizedResource	次のセクションで説明しているように、**HTTP** リクエストリソースによって構成された文字列。	**/event/custom/upload**

上記の表の **CanonicalizedHeaders** は、次のように構成されています。

a. `x-cms` と `x-acs` の接頭辞を持つすべての **HTTP** リクエストヘッダー名を小文字に変換します。

b. 前の手順で取得した **CMS** カスタムリクエストヘッダーを、辞書式順序の昇順でソートします。

c. リクエストヘッダーとコンテンツの間の、区切り文字の両側にあるスペースをすべて削除します。

d. すべてのヘッダーとコンテンツを `\n` セパレーターで区切り、最終的な**CanonicalizedHeaders** を作成します。

上記の表の **CanonicalizedResource** は、次のように構成されています。

a. **CanonicalizedResource** を空の文字列 **("")** に設定します。

b. `/event/custom/upload` などのアクセスしたい **URI** を引用符で囲みます。

c. リクエストにクエリ文字列 (`QUERY_STRING`) が含まれる場合、疑問符（ `?` ）とクエリ文字列を **CanonicalizedResource** 文字列の末尾に追加します。

`QUERY_STRING` は、**URL** に含まれるリクエストパラメーターの辞書式文字列です。等号 (`=`) がパラメーターの名前と値の間に配置され、文字列を形成します。 **key-value**

のペアは、辞書式順序の昇順でソートされ、アンパサンド (&) で接続され文字列を形成します。 式は次のとおりです。

```
QUERY_STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"
```

3. リクエストのデジタル署名を生成します。

現在、**HMAC-SHA1** 署名アルゴリズムのみがサポートされています。 次の式は署名を生成するために使用されます。

```
Signature = base16(hmac-sha1(UTF8-Encoding-Of(SignString),
AccessKeySecret))
```

・ リクエストパラメーター

パラメーター	データ型	必須/省略可能	説明
groupId	**long**	必須	アプリケーショングループ **ID**
metricName	**string**	必須	メトリックの名前。メトリック名には、英数字、およびアンダースコア (_)、ハイフン (-)、ピリオド (.)、スラッシュ (/)、バックスラッシュなどのコネクターを使用できます。 他の文字は無効です。 最大長は **64** バイトです。超過した文字は、文字列から切り捨てられます。

パラメーター	データ型	必須/省略可能	説明
dimensions	**object**	必須	ディメンションマップ。 **key-value** ペアは、すべて文字列です。 文字列には、英数字、およびアンダースコア (_)、ハイフン (-)、ピリオド (.)、スラッシュ (/)、バックスラッシュなどのコネクターを使用できます。 **key-value** ペアの最大数は **10** です。 **key** の最大長は **64** バイトです。 **value** の最大長は **64** バイトです。超過した文字は文字列から切り捨てられます。
time	**string**	必須	メトリック値が生成された時刻。 **20171012T132456.888+0800** や **1508136760000** など、 **"yyyyMMdd'T'HHmmss.SSSZ"** 形式、または **long** 形式のタイムスタンプをサポートしています。

パラメーター	データ型	必須/省略可能	説明
type	**int**	必須	レポートされた値のデータ型。 0 は生データを表し、1 は集計データを表します。 集計データをレポートするときは、**60** 秒と **300** 秒の両方の集計期間でデータをレポートすることを推奨します。 それ以外では、**7** 日以上経過したモニタリングデータを照会することはできません。
period	**string**	省略可能	集計サイクル (秒単位)。 type の値が 1 の場合、このフィールドは必須です。 値は、**60** または **300** です。
values	**object**	必須	メトリック値のコレクション。 type の値が 0 の場合、**key** は **"value"** のみとなり、生データがレポートされます。 **CloudMonitor** は、集計期間中の生データを最大、カウント、合計などのいくつかのデータタイプに集計します。

Java SDK を使用したデータのレポート

- **Java SDK** のインストール

  Maven を使用して **Java SDK** をインストールするときは、次の依存関係を追加してください。

```
<dependency>
            <groupId>com.aliyun.openservices</groupId>
            <artifactId>aliyun-cms</artifactId>
            <version>0.2.4</version>
</dependency>
```

- レスポンス要素

  システムは **HTTP** ステータスコード **200** を返します。

- 例

  - リクエストの例

```
POST /metric/custom/upload HTTP/1.1
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version:1.0
Authorization:yourAccessKeyId:yourAccessKeySecret
Host:metrichub-cms-cn-hangzhou.aliyuncs.com"
Date:Mon, 23 Oct 2017 06:51:11 GMT
Content-Length:180
x-cms-signature:hmac-sha1
Content-MD5:E9EF574D1AEAAA370860FE37856995CD
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
Content-Type:application/json
[{"groupId":101,"metricName":"","dimensions":{"sampleName1":"
value1","sampleName2":"value2"},"time":"","type":0,"period":60,"
values":{"value":10.5,"Sum":100}}]
```

  - レスポンスの例

```
{
   "code":"200",
   "msg":""//The returned msg is null when the reporting is normal
.
}
```

- コードの例

  - 生データのレポート

```
CMSClientInit.groupId = 101L;//Set the common group ID.
        CMSClient cmsClient = new CMSClient(endpoint, accKey, secret
);//Initialize the client.
        CustomMetricUploadRequest request = CustomMetricUploadRe
quest.builder()
                .append(CustomMetric.builder()
                        .setMetricName("testMetric")//The metric
name
                        .setGroupId(102L)//Set the custom group ID.
                        .setTime(new Date())
```

```
                        .setType(CustomMetric.TYPE_VALUE)//The type
is raw data.
                        .appendValue(MetricAttribute.VALUE, 1f)//The
 original value. Key must be an original value.
                        .appendDimension("key", "value")//Add a
dimension.
                        .appendDimension("ip", "127.0.0.1")//Add a
dimension.
                        .build())
                .build();
        CustomMetricUploadResponse response = cmsClient.putCustomM
etric(request);//Report data.
        System.out.println(JSONObject.toJSONString(response));
```

- 複数の集計期間の集計データを自動的にレポートします。

SDK ではローカル集計後のデータレポートをサポートしています。 データは **1** 分または **5** 分の期間で集計できます。

データ型	説明	集計値	メモリ使用量 (名前、ディメンション、個々の時系列、および個々の集計期間を除く)
value	代表的な値型	**LastValue** 以外のすべてのプロパティ	約 **4 KB**
gauge	サンプル値	**LastValue**	**4** バイト
meter	合計と速度	**Sum**、**SumPerSecond**	**50** バイト
counter	カウント	**SampleCount**	**10** バイト
timer	計算時間	**SampleCount, CountPerSecond, Average, Maximum, Minimum, PXX(P10-P99)**	約 **4 KB**
histogram	分布	**SampleCount, Average, Maximum, Minimum, PXX(P10-P99)**	約 **4 KB**

```
//Initialization
        CMSClientInit.groupId = 0L;
        CMSClient cmsClient = new CMSClient(accKey, secret, endpoint
);//Create a client.
```

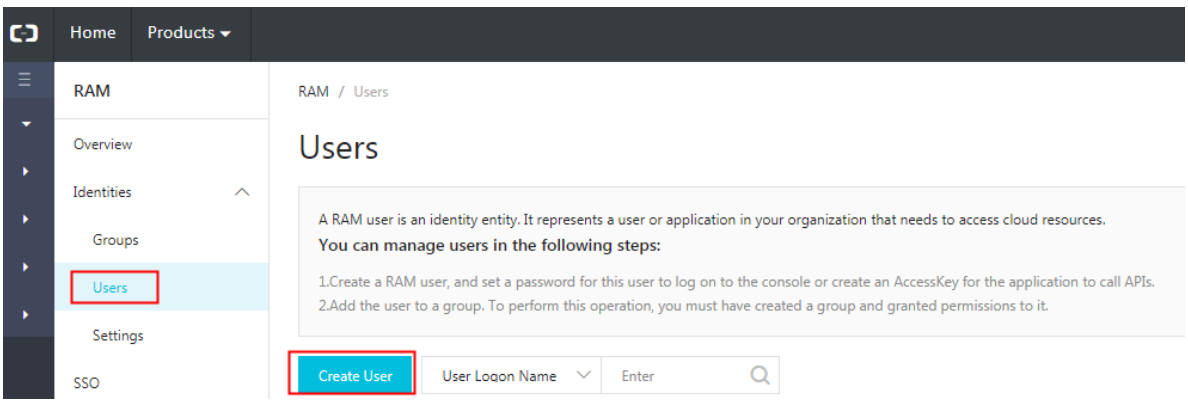
```
        CMSMetricRegistryBuilder builder = new CMSMetricRegistryBui
lder();
        builder.setCmsClient(cmsClient);
        final MetricRegistry registry = builder.build();//Create a
registry, which includes two aggregation periods.
        //Or final MetricRegistry registry = builder.build(
RecordLevel. _60S);//Create a registry that only includes aggregate
data with an aggregation period of 1 minute.
//Use value.
ValueWrapper value = registry.value(MetricName.build("value"));
value.update(6.5);
//Use meter.
MeterWrapper meter = registry.meter(MetricName.build("meter"));
meter.update(7.2);
//Use counter.
CounterWrapper counter = registry.counter(MetricName.build("counter
"));
counter.inc(20);
counter.dec(5);
//Use timer.
TimerWrapper timer = registry.timer(MetricName.build("timer"));
timer.update(30, TimeUnit.MILLISECONDS);
//Use histogram.
HistogramWrapper histogram = registry.histogram(MetricName.build("
histogram"));
histogram.update(20);
//Use gauge.
final List list = new ArrayList();
registry.gauge(MetricName.build("gauge"), new Gauge() {
                        @Override
                        public Number getValue() {
                            return list.size();
                        }
                    });
```

Alibaba Cloud CLI を使用したデータのレポート

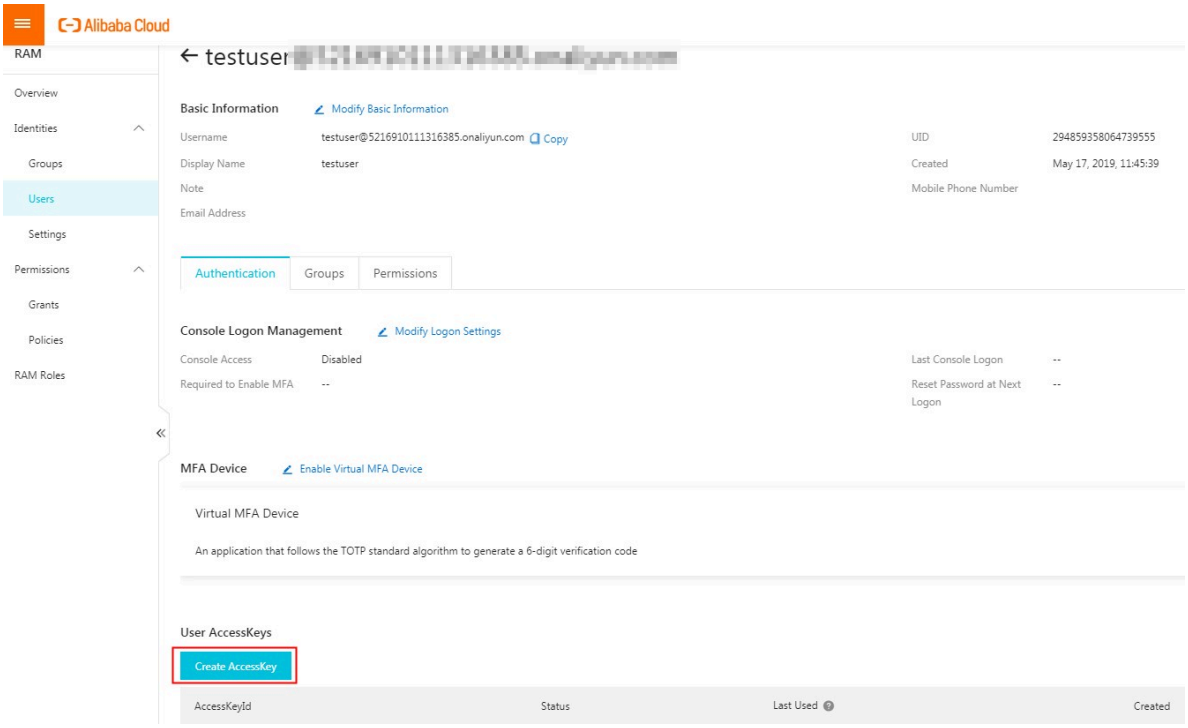
Alibaba Cloud アカウントの準備

Alibaba Cloud アカウントを作成します。次に、アカウント用の RAM ユーザーを作成し、CloudMonitor の権限を持つ RAM ユーザー AccessKey を生成したことを確認してください。

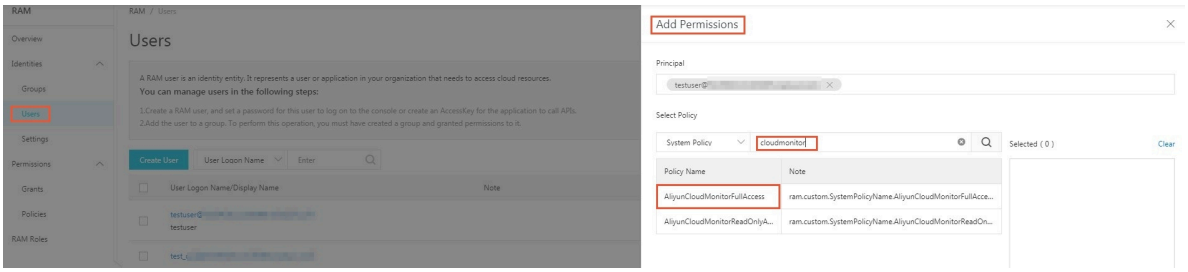
- RAM ユーザーの作成



- **RAM** ユーザーの **AccessKeyID** と **AccessKey Secret** を生成



- **RAM** ユーザーに対して、**Cloud Monitor** アクセス権限を付与



Alibaba Cloud CLI のインストール

システム要件：**Linux**、**UNIX**、または **Mac OS**

- 方法 **1.** インストールパッケージをダウンロードする

  最新の **CLI** は **Alibaba Cloud CLI GitHub** からダウンロードできます。 **CLI** は **MacOS**、**Linux**、および **Windows (x64)** で動作します。 パッケージを解凍したら、ファイルを **/usr/local/bin** ディレクトリに移動するか、 **$PATH** 環境変数に追加します。

- 方法 **2.** ソースコードをコンパイルする

  Golang 環境をインストールして設定し、手順に従ってソースコードをダウンロードしてコンパイルします。

```
...
$ mkdir -p $GOPATH/src/github.com/aliyun
$ cd $GOPATH/src/github.com/aliyun
$ git clone http://github.com/aliyun/aliyun-cli.git
$ git clone http://github.com/aliyun/aliyun-openapi-meta.git
```

```
$ cd aliyun-cli
$ make install
...
```

Alibaba Cloud CLI の設定

Alibaba Cloud CLI を使用する前に、**aliyun configure** コマンドを実行して、**Alibaba Cloud** リソースを呼び出すための **AccessKey**、リージョン、および言語を設定する必要があります。 **Alibaba Cloud** コンソールの **AccessKey** ページで、**AccessKey** を作成および表示するか、システム管理者から **AccessKey** を入手することができます。

```
$ aliyun configure
Configuring profile 'default' ...
Aliyun Access Key ID [None]: <Your AccessKey ID>
Aliyun Access Key Secret [None]: <Your AccessKey Secret>
Default Region Id [None]: cn-hangzhou
Default output format [json]: json
Default Language [zh]: zh
```

Alibaba Cloud CLI は、マルチユーザー設定をサポートしています。 **$ aliyun configure --profile user1** コマンドを実行して、**Alibaba Cloud API** を呼び出すことができる **RAM** ユーザーを指定できます。 次の表に示すように、`$ aliyun configure list` コマンドを実行して **RAM** ユーザー設定を表示できます。 **Profile** 列のアスタリスク (*) は、その設定が使用されていることを示します。

Profile	Credential	Valid	Region	Language
default *	AK:***f9b	Valid	cn-beijing	zh
aaa	AK:******	Invalid		
test	AK:***456	Valid		en
ecs	EcsRamRole: EcsTest	Valid	cn-beijing	en

Alibaba Cloud CLI では、**configure** コマンドの後に **--mode <authenticationMethod>**パラメーターを追加することで、さまざまな認証方法を使用できます。 現在、以下の **3** つの認証方法がサポートされています。

認証方法	説明
AK	**AccessKey ID** と **Access Key Secret** を含みます。
STS Token	**STS** トークンです。
RamRoleArn	**RAM** ユーザーの **AssumeRole** アクションを呼び出します。

認証方法	説明
EcsRamRole	**ECS** インスタンスの **EcsRamRole** アクションを呼び出します。

モニタリングデータのレポート

`PutCustomMetric` **API** を使用して、モニタリングデータをレポートします。

```
aliyun cms PutCustomMetric  --MetricList. 1.MetricName cpu_total --
MetricList. 1.Dimensions '{"sampleName1":"value1","sampleName2":"
value2"}' --MetricList. 1.Time 1555390981421 --MetricList. 1.Type 0
 --MetricList. 1.Period 60 --MetricList. 1.Values '{"value":10.5}' --
MetricList. 1.GroupId "0"
```

データが正常にレポートされた場合、ステータスコード **200** が返されます。

```
{
  "Message": "success",
  "RequestId": "F69F5623-DDD6-42AE-AE59-87A2B841620B",
  "Code": "200"
}
```

エラーコード

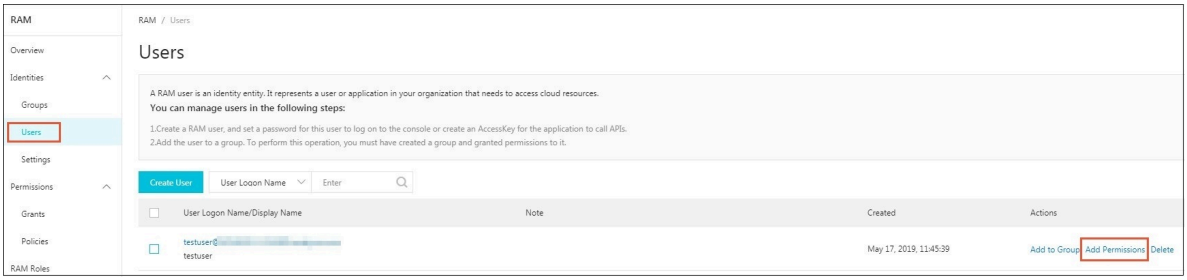
エラーコード	説明
200	正常
206	一部は正常 **"reach Max time series num"** が返された場合は、最大時系列数に達しています。クォータを増やすか、不要な時系列を削除することを推奨します。 **"not allowed original value, please upgrade service"** が返された場合、生データのレポートをサポートしていない無料バージョンを使用していることを示しています。 **"type is invalid"** が返された場合、**type** パラメーターの値は無効です。 このパラメーターの値が **0** または **1** であることを確認してください。
400	クライアントリクエストの構文エラー

エラーコード	説明
403	検証失敗、限界速度、または未許可
500	内部サーバーエラー

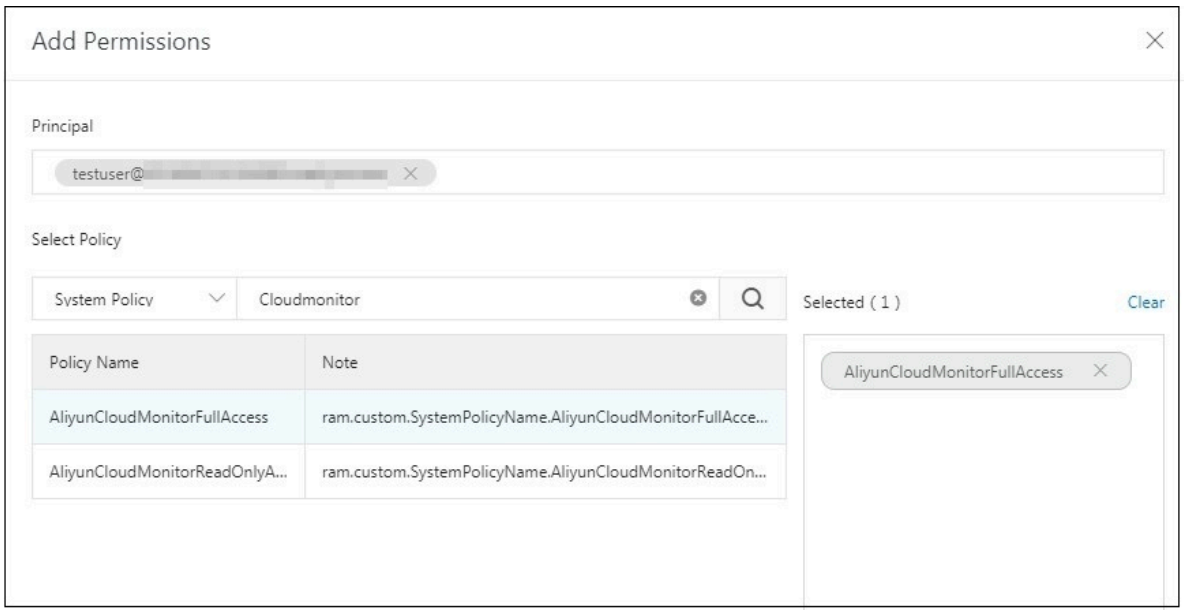
RAM ユーザー認証

イベントデータを **RAM** ユーザーの **AccessKe** でレポートする前に、対応する **RAM** ユーザーに **CloudMonitor** 権限を付与する必要があります。 これらのアクセス権限が付与されていない場合は、データをレポートするときに **"cannot upload, please use ram to auth"** というプロンプトが表示されます。

1. *RAM コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、**[ユーザー]** を選択します。 **[ユーザー]** ページが表示されます。
3. 該当する **RAM** ユーザーを選択し、**[権限の追加]** をクリックします。



4. 表示されたページで **[AliyunCloudMonitorFullAccess]** を選択し、**[OK]** をクリックします。



10.3 ダッシュボードの設定

モニタリングデータをカスタムモニタリングにレポートした後、簡単にモニタリングとデータクエリをするためのダッシュボードを作成できます。

・ ダッシュボードの作成

1. *CloudMonitor コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[ダッシュボード > [カスタマイズダッシュボード] をクリックします。
3. 右上隅にある [ダッシュボードの作成] をクリックし、ダッシュボード名を入力し、[作成] をクリックし、ダッシュボードを作成します。

- グラフの追加

  1. 右上隅の [グラフの追加] をクリックします。
  2. 測定値の選択 エリアから、[カスタマイズ] タブをクリックしグラフ名を入力します。
  3. 対象測定値、統計的方法、およびデメンションを選択します。
  4. [保存] をクリックし、設定を保存します。