# Alibaba Cloud Cloud Monitor

ユーザガイド

Document Version20190514

# 目次

1 ダッシュボード1
1.1 ダッシュボードの使用1
1.1.1 ダッシュボードの概要1
1.1.2 ダッシュボードの管理2
1.1.3 グラフの追加
2 ホストモニタリング10
2.1 ホストモニタリングの概要10
2.2 プロセスモニタリング11
<b>2.3 ホストモニタリングのメトリクス15</b>
2.4 アラームルールサービス21
2.5 Cloud Monitor Java エージェントの紹介22
2.6 Cloud Monitor Java エージェントのインストール
2.7 エージェントのリリースノート
3 アラームサービス
3.1 アラームサービスの概要
3.2 アラームテンプレートの使用
3.3 アラームルール
<b>3.3.1 アラームルールの管理37</b>
3.4 アラーム連絡先
341アラーム送信先おとびアラーム送信先グループの管理 30
5.7.1 / / 4.2.6月14360/ / 4.2.6月12/10 / 9.6座
4 可用性モニタリング
4 可用性モニタリング       42         4.1 可用性モニタリングの管理       42         4.2 ローカルサービス可用性モニタリング       45         4.3 ステータスコード       46         5 クラウドサービスモニタリング       48         5.1 AsparaDB for RDS のモニタリング       48         5.2 SLB モニタリング       52
4 可用性モニタリング

5.16 VPN ゲートウェイ	96
5.17 API ゲートウェイ	
5.18 DDoS 高セキュリティ IP	
5.19 ダイレクトメールモニタリング	
5.20 Elasticsearch モニタリング	104
5.21 Auto Scaling	
5.22 E-MapReduce モニタリング	
5.23 Express Connect のモニタリング	117
5.24 Function Compute モニタリング	120
5.25 StreamCompute	
5.26 ApsaraDB for HybridDB	
5.27 NAT ゲートウェイ	
5.28 Open Ad	
5.29 ApsaraDB for PetaData	
6 CloudMonitor 用の RAM	
7 アプリケーショングループ	
7.1 アプリケーショングループの概要	137
7.2 アプリケーショングループの作成	137
7.3 アプリケーショングループの詳細の確認	140
7.4 アプリケーショングループの変更	
7.5 アラームルールの管理	
8 イベントモニタリング	
8.1 イベントモニタリングの概要	
8.2 クラウド製品イベント	
8.2.1 クラウドプロダクトのシステムイベントモニタリング	
8.2.2 システムイベントアラームの使用	
8.3 カスタムイベント	
8.3.1 イベントデータのレポート	
8.3.2 イベントモニタリングのベストプラクティス	171
8.4 リクエストのヘッダー定義	
9 カスタムモニタリング	
9.1 カスタマイズモニタリングの概要	
9.2 モニタリングデータのレポート	
9.3 ダッシュボードの設定	198

# 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。
- 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**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。
- 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。

Dashboards : ECS-global-dashboard	•	Create Dashboard Delete Dashboard
1h         3h         6h         12h         1days         3days         7days	14days 🗮 Auto Refresh : Chart relevan	ice :
		Add View Full Screen C Refresh
11.68 10.00 4.24 20:25:00 20:40:00 21:23:00	113.16K 7.79K 20:25:00 20:40:00 21:23:00	192.37K 12.83K 20:25:00 20:40:00 21:23:00 • (ECS) Public Network Outboun • (ECS) Intranet Outbound Traf

4. ダッシュボードの名前を入力します。

Create Dashboard		×
Enter the dashboard name.		
	Create	Close

- 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。
- 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。
- 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、ダッシュボードヘ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。
- 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。

ld View			
Chart Type			
Line Area	Table Heat Map Pie Chart		
2 Select Metrics			
Dashboards Log Monitorin	g Custom		
ECS	ECS	Heat Map Gra	adient Range : 0 auto
		No Data	
		no buu	
Metrics : (Agent) Host.cpu.	total(Recommend)	alue 💌	
Resource :			
q20/i-bp140l3jmjqi5stmu	sq8	•	
+AddMetrics			

- 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、 cloudmonit or / 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 \ cloudmonit or \ 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。



・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。
- 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。
- [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。

Set Alarm Rules		
Alarm Type:	Threshold Value Alarm Event Alarm	6.00
Alarm Rule:	ØWhere is the alarm template?	
Rule Describe:	(Agent) Host.process.number   Imins  Average  Imins  Count/Min	4.00
processName:	Anyprocess java	2.00
Alarm Rule:	Delete	15:47:15 16:10:00 16:26:40 16:47:
Rule Describe:	(Agent) Host.process.number	gent) Host.process.number—Average—emr_C-7AF9E7BFD87B0EDF_2_RWjW—dfa aming Line (Value: 6) ▲ 1/2 ▼
processName:	Anyprocess dfasdf   Custom	
+Add Alarm F	ule	

# 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。	9%	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" cloudmonit or / 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 \ cloudmonit or \ 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.errorpacka ges	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。
- 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。
- [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 / cloudmonit or
- Windows: C : \ Program Files \ Alibaba \ cloudmonit or

#### 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 / cloudmonit or / jre / bin / java
- / usr / local / cloudmonit or / 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 / cloudmonit or / 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 / cloudmonit or / wrapper / logs にあります。
- ・ログレベルは、/ usr / local / cloudmonit or / 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2KB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。
- 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 / cloudmonit or / wrapper / bin / cloudmonit or . sh
status
# Start
/ usr / local / cloudmonit or / wrapper / bin / cloudmonit or . sh
start
# Stop
/ usr / local / cloudmonit or / wrapper / bin / cloudmonit or . sh
stop
# Restart
/ usr / local / cloudmonit or / wrapper / bin / cloudmonit or . sh
restart
# Uninstall
/ usr / local / cloudmonit or / wrapper / bin / cloudmonit or . sh
remove && \
rm - rf / usr / local / cloudmonit or
```

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_instal
l_for_linu x . 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_instal
l_for_linu x . sh )"
```

中国 (張家口) cn-zhangjiakou

REGION\_ID = cn - zhangjiako u VERSION = 1 . 3 . 7 \

```
bash - c "$( curl https :// cms - agent - cn - zhangjiako u
. oss - cn - zhangjiako u - internal . aliyuncs . com / release /
cms_instal l_for_linu x . 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_instal
l_for_linu x . 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_instal
l_for_linu x . 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_instal
l_for_linu x . 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\_instal
l\_for\_linu x . 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_instal
l_for_linu x . 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_instal
l_for_linu x . 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_instal
l_for_linu x . 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_instal l_for_linu x . 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_instal l_for_linu x . 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_instal l_for_linu x . 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_instal l_for_linu x . 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_instal l_for_linu x . 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_instal
l_for_linu x . 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_instal l_for_linu x . 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_linu x . 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\_instal
l\_for\_linu x . 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\_instal
l\_for\_linu x . 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\_linu x . 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\_instal l\_for\_linu x . 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

- 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 cloudmonit or 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 / cloudmonit or に解凍します。
- 4. C:/ Program Files / Alibaba / cloudmonit or / 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 / cloudmonit or / 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 / cloudmonit or / wrapper / bin / UninstallA pp 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 / cloudmonit or 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://cmsagent-cn-qingdao.oss-cn-qingdao.aliyuncs.com/release/1.3.7/windows64/agent-windows64-1.3.7package.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。



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
	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

リージョン	IP	方向	説明
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
	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

リージョン	IP	方向	説明
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
	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

リージョン	IP	方向	説明
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 / cloudmonit or / logs
  - Windows: C :/ Program Files / Alibaba / cloudmonit or / 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?
  - Cloud Monitor 設定ファイル / usr / local / cloudmonit or / 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 アラームサービス

## 3.1 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。

## 3.2 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。

Aları	m Templates			${\cal C}$ Refresh	Create Alarm Template
	Template Name/ID	Description	Modified At		Actions
	100,0000		2018-04-26 01:19:30 View	Modify D	elete Apply to Group
	1000 000		2017-09-15 12:09:57 View	Modify   D	elete Apply to Group

## 3.3 アラームルール

## 3.3.1 アラームルールの管理

アラームサービスは、測定値の例外を簡単に検出して障害を迅速にトラブルシューティングでき るように、アラームをモニターするための強力な機能を提供します。

#### パラメーターの説明

- ・プロダクト: ECS、 RDS、 OSS などが含まれます。
- ・リソース範囲: アラームルール適用の範囲です。使用できるアラームルールの範囲には、[すべてのリソース]、[アプリケーショングループ]、[インスタンス] の3つがあります。[リソース
   範囲] を [すべてのリソース] に設定すると、最大 1000 のリソースに対してアラームを報告できます。 リソースの数が 1000 を超える場合、リソースの中には、アラームに設定されたしきい値を超えても、アラームの報告ができないものがあります。したがって、この問題を回避するために、アラームルールを設定する前に、アプリケーショングループを使用してリソースをサービス別に分割することを推奨します。
  - すべてのリソース:指定されたアラームルールがユーザーのすべてのインスタンスに適用 されます。たとえば、リソース範囲をすべてのリソースに設定し、MongoDB CPU 稼働

率のアラームしきい値を 80% に設定した場合、MongoDB インスタンスの CPU 稼働率が 80% を超えるとアラームがトリガーされます。

- アプリケーショングループ:指定されたルールがアプリケーショングループのすべてのインスタンスに適用されます。たとえば、リソース範囲をアプリケーショングループに設定し、ホスト CPU 稼働率のアラームしきい値を 80% に設定した場合、ホストインスタンスの CPU 稼働率が 80% を超えるとアラームがトリガーされます。
- インスタンス:指定されたルールは特定のインスタンスにのみ適用されます。たとえば、リ ソース範囲をインスタンスに設定し、ホスト CPU 稼働率のアラームしきい値を 80% に設 定した場合、指定したインスタンスの CPU 稼働率が 80% を超えるとアラームがトリガー されます。
- ・アラームルール:アラームルール名です。
- ・ルールの内容: 関連する測定値のアラーム発生条件または値のしきい値を定義するアラーム
   ルールの主な内容です。たとえば、ルールを [1 分間の平均 CPU 稼働率が 90%以上] と記述した場合、アラームサービスは毎分、1 分以内の平均測定値が 90% 以上になるかどうかを確認します。

次の例をご検討ください。 ホストモニタリングのアラームサービスの場合、1 つのサーバー測 定項目により、15 秒に 1 データポイント、5 分に 20 データポイントが報告されます。 これは 以下のアラームルールに関連しています。

- 5 分間の平均 CPU 稼働率 が 90%以上: 5 分間 20 データポイントで平均 CPU 稼働率が 90% を超えることを示します。
- 5分間の CPU 稼働率が常に 90%を超える: 5 分間 20 データポイントですべての CPU 稼働率が 90% を超えることを示します。
- 5分間の CPU 稼働率 が一度 90%を超える: 5分間 20 データポイントで少なくとも 1 回は CPU 稼働率が 90% を超えることを示します。
- 5-分間のインターネット送信トラフィックの合計が 50 MB を超える: 5 分間 20 データポイントの送信トラフィック値の合計が 50 MB を超えることを示します。
- ・しきい値を超過したらトリガー:検出された値がアラームルールのしきい値に連続して複数回 達すると、アラーム通知が送信されます。
- ・有効期間: アラームルールが有効である期間。アラームサービスは測定値をチェックし、この 期間中にのみアラームを生成するかどうかを決定します。
- ・アラーム 送信先: アラーム通知を受け取る送信先のグループ。

- ・通知方法: アラームレベルごとに別々の通知方法を利用できます。 [重大]、[警告]、[通知] と いう 3 つのアラームレベルが利用可能です。
  - 重大: 音声通話、SMS メッセージ、メール、および DingTalk チャットボット
  - 警告: SMS メッセージ、メール、および DingTalk チャットボット
  - 通知: メールおよび DingTalk チャットボット
- ・Email Remark: アラームメール用にカスタマイズされた補足情報 備考はアラーム通知メール の一部として送信されます。

#### アラームルールの管理

CloudMonitor には、アラームサービスのアプリケーショングループページ、測定値リストページ、アラームルールリストページという、3つのアラームルール管理ポータルがあります。

- アプリケーショングループでのアラームルールの管理については、「アラームルールの管理」
   をご参照ください。
- ・ホストモニタリングでのアラームルールの管理については、「アラームルールの管理」をご 参照ください。
- カスタムモニタリングでのアラームルールの設定については、「アラームルールの設定」をご 参照ください。
- 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することもできます。

## 3.4 アラーム連絡先

## 3.4.1 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。
  - 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。
  - 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。
  - 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。

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。
  - 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。
  - 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。
  - 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。
  - 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 可用性モニタリング

## 4.1 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。
- 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。

- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。

- 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。
- 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。
- 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。

## 4.2 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。

## 4.3 **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
НТТР	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。
НТТР	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。

# 5 クラウドサービスモニタリング

## 5.1 AsparaDB for RDS のモニタリング

ディスク使用量、IOPS 使用量、接続使用量、CPU 使用量など、リレーショナルデータベース サービス (RDS) 用の ApsaraDB の複数の測定値を監視することで、CloudMonitor は RDS の 実行状態をモニターするのに役立ちます。 CloudMonitor は、RDS サービスを購入すると自動 的に RDS の測定データを収集します。



- RDS は、マスターおよび読み取り専用インスタンスに対してのみモニタリングおよびアラー ムサービスを提供します。
- RDS サービスを購入すると、CloudMonitor は各マスターインスタンスと読み取り専用インスタンスに対して次の4つのアラームルールを自動的に作成します。CPU 使用率 > 80%、 接続使用率 > 80%、IOPS 使用率 > 80%、ディスク使用率 > 80% アラーム通知は、アラームルールのしきい値を超えたときに SMS メッセージや電子メールを通じてアラーム送信先に送信されます。



•	測定値
---	-----

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Disk Usage	RDS インスタン ス内のディスク 使用量のパーセ ンテージです。	インスタンス	%	5分
IOPS Usage	RDS インスタン ス内の IOPS 使 用率です。	インスタンス	%	5分

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Connections Usage	全接続のうちプ ログラムが RDS インスタンスと のアクティブな 接続を行なった パーセンテージ です。	インスタンス	%	5 分
CPU Usage	RDS インスタ ンス (CPU パ フォーマンスは データベースメ モリのサイズで 決定します) が消 費した CPU の キャパシティの パーセンテージ です。	インスタンス	%	5分
Memory Usage	RDS インスタ ンス内で使用さ れているメモリ のパーセンテー ジです。現状 では、メモリ使 用率測定値は MySQL データ ベースでのみ サポートされま す。	インスタンス	%	5分
Read-only Instance Delay	MySQL 読み取 り専用インスタ ンスのレイテン シです。	インスタンス	秒	5分
Network Inbound Traffic	毎秒のインスタ ンスへのイン バウンドトラッ フィックです。	インスタンス	bit/s	5分

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Network Outbound Traffic	毎秒のインスタ ンスからのアウ トバウンドトラ フィックです。	インスタンス	bit/s	5分
RDS Fault	アラームルール が設定できるイ ベントタイプの 測定値です。	N/A	N/A	N/A
RDS Master/ Slave Instance Switch	アラームルール が設定できるイ ベントタイプの 測定値です。	N/A	N/A	N/A

インバウンドとアウトバウンドのトラフィック測定は MySQL と SQLServer データベースで のみサポートされます。

- ・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。
  - 左側のナビゲーションウィンドウで、[Cloud Service モニタリング] > [ApsaraDB for RDS] を選択します。
  - 3. 対象となる RDS インスタンスのあるリージョンを選択し、対象のインスタンスを選びま す。
  - インスタンス名をクリックするか、 [アクション] 列から [グラフのモニタリング] を選択して [グラフのモニタリング] ページにアクセスします。
  - 5. 他のグラフビューに変更するには、ページの左上の [グラフ表示] ボタンをクリックしま す。

#### アラームサービス

- ・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。
  - 左側のナビゲーションウィンドウで、[Cloud Service モニタリング] > [ApsaraDB for RDS] を選択します。
  - 3. 対象となる RDS インスタンスのあるリージョンを選択し、対象のインスタンスを選びま す。
  - インスタンス名をクリックするか、 [アクション] 列から [アラームルール] をクリックして、[アラームルール] ページにアクセスします。
  - 5. 表示された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。
  - 6. 次の説明に従ってパラメーターを設定し、[確認] をクリックします。

・パラメーター

- プロダクト: ECS、 RDS、 OSS、 その他
- リソース範囲: アラームルールが適用される範囲 [すべてのリソース] と [インスタンス] が 利用可能です。
  - すべてのリソース: アラームルールはユーザーのすべての RDS インスタンスに適用され ることを意味します。たとえば、リソース範囲を [すべてのリソース] に設定し、CPU 使用率 80% をアラームしきい値に設定した場合、RDS インスタンスのどれかの CPU 使用率が 80% を超えるとアラームがトリガーされます。 [すべてのリソース] を選択し た場合、1000 個までのリソースのアラームをレポートできます。 リソースの数が 1000 を超えるとアラームルールでしきい値を設定していてもいくつかのリソースのアラーム はレポートされません。そのため、この問題を避けるためにアラームルールを設定する 前にアプリケーショングループを使用してサービスごとのリソースの分割を行うことを 推奨します。
  - インスタンス:指定されたルールが特定のインスタンスにのみ適用されることを意味 します。たとえば、リソース範囲を [インスタンス] に設定し、CPU 使用率 80% をア ラームしきい値に設定した場合、特定の RDS インスタンスの CPU 使用率が 80% を超 えるとアラームがトリガーされます。
- アラームルール:アラームルール名
- ルールの説明: 関連測定値のアラームをトリガーする条件、しきい値を設定する主なアラー ムルールの内容 たとえば、アラームルールを [5 分間の平均 CPU 使用率 >=90%] と記述し

た場合、アラームサービスは5分ごとに CPU 使用率の5分間の平均値が 90% に達するか 超えるかを確認します。

次の例をご参照ください。 ホストモニタリングのアラームサービスでは1つのデータポイントは単一のサーバー測定値に対して 15 秒で報告され、5 分で 20 データポイントとなります。 これは次のアラームルールに関連します。

- 5 分間の平均 CPU 使用率 > 90%: 5 分間の 20 データポイントで平均 CPU 使用率が 90% を超えることを示します。
- 5 分間の常時 CPU 使用率 > 90%: 5 分間の 20 データポイントで CPU 使用率が常に 90% を超えることを示します。
- 5 分間の一度の CPU 使用率 > 90%: 5 分間の 20 データポイントで CPU 使用率が少な くとも 1 回は 90% を超えることを示します。
- 5 分間の合計インターネット送信トラフィック > 50 MB: 5 分間の 20 データポイントに おける合計送信トラフィックが 50MB を超えることを示します。
- ミュート期間: アラームがミュートされ、アラーム送信先がアラーム通知を受け取らない期間
   問 アラームルールは 24 時間 (1日) ミュートすることができます。
- しきい値が超えられたときにトリガー:連続して一定の回数以上アラームルールのしきい値
   を超えた場合にアラーム通知を送信
- 有効期間: アラームルールが有効な期間 この期間はアラームサービスは測定値を確認して アラームを生成するかを決定します。
- 通知連絡先: アラーム通知を受け取るグループ
- 通知方法:

■ メール、DingTalk チャットボット

- メールの件名: デフォルトでは、メールの件名はプロダクト名、測定値、関連するインスタンス ID
- メールの備考:カスタマイズされたアラームメール用の追加情報 アラーム通知メールの本 文の一部として送信されます。
- HTTP コールバック: CloudMonitor がインターネット経由で POST 要求にてアラーム情報をプッシュできる URL を入力 現時点では HTTP にのみ対応しています。

## 5.2 SLB モニタリング

Server Load Balancer (SLB) からのインバウンドやアウトバウンドのトラフィック、データパ ケットや接続数などの複数の測定値をモニタリングすることで CloudMonitor は起動中のイン スタンスのステータスをモニターしたり、アラームルールの設定を適宜行うことができます。 CloudMonitor は、SLB インスタンスを作成した後から自動的に SLB からデータを収集します。

### モニタリングサービス

- ・測定値
  - レイヤ 4 測定値

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Port inbound traffic	インターネット から特定の SLB ポートにアクセ スするためのト ラフィック消費	ポート	ビット / 秒	1分
Port outbound traffic	指定された SLB ポートからイン ターネットにア クセスするため のトラフィック 消費	ポート	ビット / 秒	1分
Number of inbound data packets by port	指定された SLB ポートが受信す る要求パケット の数 (毎 1 秒)	ポート	回数 / 秒	1分
Number of outbound data packets by port	指定された SLB ポートが送信す る要求パケット の数 (毎 1 秒)	ポート	回数 / 秒	1分
Number of new port connections	統計期間中に TCP 3 方向 ハンドシェイ クで最初の SYN_SENT ス テータスが発生 した平均回数 (毎 1 秒)	ポート	回数 / 秒	1分
Number of active port connections	統計期間中に ESTABLISHED ステータスにあ る接続の数	ポート	回数	1分

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Number of inactive port connections	統計期間中に ESTABLISHED ステータスにあ る接続を除くす べての TCP 接 続の数	ポート	回数	1分
Number of concurrent port connections	接続の総数	ポート	回数	1分
Number of backend healthy ECS instances by port	ヘルスチェック によって報告さ れた正常なイン スタンスの数	ポート	回数	1分
Number of backend unhealthy ECS instances by port	ヘルスチェック によって報告さ れた異常なイン スタンスの数	ポート	回数	1分
Number of discarded port connections	1 秒間にドロッ プされた平均 TCP 接続数	ポート	回数 / 秒	1分
Number of discarded inbound data packets by port	1 秒間に破棄さ れたインバウン ドパケットの平 均数	ポート	回数 / 秒	1分
Number of discarded outbound data packets by port	1 秒間に破棄さ れたアウトバウ ンドパケットの 平均数	ポー <b>ト</b>	回数 / 秒	1分
Number of discarded inbound bandwidth by port	1 秒あたりに廃 棄された平均イ ンバウンドトラ フィック	ポート	ビット / 秒	1分

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Number of discarded outbound bandwidth by port	1 秒あたりに廃 棄された平均ア ウトバウンドト ラフィック	ポート	ビット / 秒	1分
Number of active instance connections	統計期間中に ESTABLISHED ステータスにあ る接続の数	インスタンス	回数 / 秒	1分
Number of inactive instance connections	統計期間中に ESTABLISHED ステータスにあ る接続を除くす べての接続の数	インスタンス	回数 / 秒	1分
Number of discarded instance connections	1 秒間にドロッ プされた接続数	インスタンス	回数 / 秒	1分
Number of discarded inbound data packets by instance	インスタンスに より1秒間にド ロップされたイ ンバウンドデー タパケット数	インスタンス	回数 / 秒	1分
Number of discarded outbound data packets by instance	1 秒間に破棄さ れたアウトバウ ンドパケットの 数	インスタンス	回数 / 秒	1分
Discarded inbound bandwidth by instance	1 秒間に破棄さ れたインバウン ドトラフィック の量	インスタンス	ビット / 秒	1分
Discarded outbound bandwidth by instance	1 秒間に破棄さ れたアウトバウ ンドトラフィッ クの量	インスタンス	ビット / 秒	1分

測定值	説明	ディメンション	単位	最小モニタリン
				グ頻度
Number of concurrent instance connections	インスタンスの 接続総数 (アク ティブ接続と非 アクティブ接続 の合計)	インスタンス	回数 / 秒	1分
Number of new instance connections	統計期間中に TCP 3 方向 ハンドシェイ クで最初の SYN_SENT ス テータスが発生 した平均回数 (毎 1 秒)	インスタンス	回数 / 秒	1分
Number of inbound data packets by instance	1 秒あたりに受 信された要求パ ケットの数	インスタンス	回数 / 秒	1分
Number of outbound data packets by instance	1 秒あたりに送 信されたパケッ ト数	インスタンス	回数 / 秒	1分
Number of inbound bandwidth by instance	インターネット から SLB インス タンスにアクセ スするためのト ラフィック消費	インスタンス	ビット / 秒	1分
Number of outbound bandwidth by instance	SLB インスタン スからインター ネットにアクセ スするためのト ラフィック消費	インスタンス	ビット / 秒	1分

- レイヤ7測定値

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Port QPS	指定されたポー トの QPS	ポート	回数 / 秒	1分

測定値	説明	ディメンション	単位	最小モニタリン グ頻度
Port RT	指定されたポー トの平均要求待 ち時間	ポート	ミリ秒	1分
Status codes of the format 2xx	SLB がクライア ントに返す形式 2xx のステータ スコードの数	ポート	回数 / 秒	1分
Status codes of the format 3xx	SLB がクライア ントに返す形式 3xx のステータ スコードの数	ポート	回数 / 秒	1分
Status codes of the format 4xx	SLB がクライア ントに返す形式 4xx のステータ スコードの数	ポート	回数 / 秒	1分
Status codes of the format 5xx	SLB がクライア ントに返す形式 5xx のステータ スコードの数	ポート	回数 / 秒	1分
Other status codes	SLB がクライア ントに返す他の ステータスコー ドの数	ポート	回数 / 秒	1分
Upstream status codes of the format 4xx	RS が SLB に返 す形式 4xx のス テータスコード の数	ポート	回数 / 秒	1分
Upstream status codes of the format 5xx	RS がクライア ントに返す 5xx 形式のステータ スコードの数	ポート	回数 / 秒	1分
Upstream RT	RS からプロキ シへの平均リク エスト遅延	ポート	ミリ秒	1分
Instance QPS	インスタンスの QPS	インスタンス	回数 / 秒	1分

測定値	説明	ディメンション	単位 	最小モニタリン グ頻度
Instance RT	インスタンスの 平均リクエスト レイテンシ	インスタンス	回数 / 秒	1分
Status codes of the format 2xx	SLB がクライア ントに返す形式 2xx のステータ スコードの数	インスタンス	回数 / 秒	1分
Status codes of the format 3xx	SLB がクライア ントに返す形式 3xx のステータ スコードの数	インスタンス	回数 / 秒	1分
Status codes of the format 4xx	SLB がクライア ントに返す形式 4xx のステータ スコードの数	インスタンス	回数 / 秒	1分
Status codes of the format 5xx	SLB がクライア ントに返す形式 5xx のステータ スコードの数	インスタンス	回数 / 秒	1分
Other status codes	SLB がクライア ントに返す他の 形式のステータ スコードの数	インスタンス	回数 / 秒	1分
Upstream status codes of the format 4xx	RS が SLB に返 す形式 4xx のス テータスコード の数	インスタンス	回数 / 秒	1分
Upstream status codes of the format 5xx	RS が SLB に返 す形式 5xx のス テータスコード の数	インスタンス	回数 / 秒	1分
Upstream RT	RS からプロキ シへの平均リク エスト遅延	インスタンス	ミリ秒	1分



新規接続、アクティブ接続、および非アクティブ接続の数はすべて、クライアントから SLB への TCP 接続要求に基づいています。

- ・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] > [Server Load Balancer] を選択して SLB インスタンスリストページを表示します。
  - 3. 対象となるインスタンスの属するリージョンを選択します。
  - 対象となるインスタンス名をクリックするか、 [アクション] 列の[モニタリンググラフ] を クリックします。
  - 5. [モニタリンググラフ] ページでモニタリングデータを参照できます。
  - 6. 他のグラフビューに変更するには、ページの左上隅にある [グラフ表示] ボタンをクリック します。

#### アラームサービス

- ・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. 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] を選択して SLB インスタンスリストページを表示します。
  - 3. Global Acceleration インスタンスの属するリージョンを選択します。
  - 対象となるインスタンスを見つけて、 [アクション] 列の[アラームルール] をクリックします。
  - 5. [アラームルール] 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。
  - 6. 次の説明に従ってパラーメータを設定し、[確認] をクリックします。
- ・パラメーター
  - プロダクト: ECS、RDS、OSS、その他
  - リソース範囲: アラームルールが適用される範囲 [すべてのリソース] と [インスタンス] が
     利用可能です。
    - すべてのリソース: アラームルールはユーザーのすべての RDS インスタンスに適用され ることを意味します。たとえば、リソース範囲を [すべてのリソース] に設定し、CPU 使用率 80% をアラームしきい値に設定した場合、RDS インスタンスのどれかの CPU 使用率が 80% を超えるとアラームがトリガーされます。 [すべてのリソース] を選択し た場合、1000 個までのリソースのアラームをレポートできます。 リソースの数が 1000 を超えるとアラームルールでしきい値を設定していてもいくつかのリソースのアラーム

はレポートされません。 そのため、この問題を避けるためにアラームルールを設定する 前にアプリケーショングループを使用してサービスごとのリソースの分割を行うことを 推奨します。

- インスタンス:指定されたルールが特定のインスタンスにのみ適用されることを意味 します。たとえば、リソース範囲を [インスタンス] に設定し、CPU 使用率 80% をア ラームしきい値に設定した場合、特定のRDS インスタンスの CPU 使用率が 80% を超 えるとアラームがトリガーされます。
- アラームルール:アラームルール名
- ルールの説明: 関連測定値のアラームをトリガーする条件、しきい値を設定する主なアラー ムルールの内容 たとえば、アラームルールを [5 分間の平均 CPU 使用率 >=90%] と設定し

た場合、アラームサービスは5分ごとに CPU 使用率の5分間の平均値が 90% に達するか 超えるかを確認します。

次の例をご参照ください。 ホストモニタリングのアラームサービスでは1つのデータポイントは単一のサーバー測定値に対して 15 秒で報告され、5 分で 20 データポイントとなります。 これは次のアラームルールに関連します。

- 5 分間の平均 CPU 使用率 > 90%: 5 分間の 20 データポイントにおける平均 CPU 使用 率が 90% を超えることを示します。
- 5 分間の常時 CPU 使用率 > 90%: 5 分間の 20 データポイントにおける CPU 使用率が 常に 90% を超えることを示します。
- 5 分間の一度の CPU 使用率 > 90%: 5 分間の 20 データポイントにおける CPU 使用率 が少なくとも 1 回は 90% を超えることを示します。
- 5 分間の合計インターネット送信トラフィック > 50 MB: 5 分間の 20 データポイントに おける合計送信トラフィックが 50MB を超えることを示します。
- ミュート期間: アラームがミュートされ、アラーム送信先がアラーム通知を受け取らない期間
   問 アラームルールは 24 時間 (1日) ミュートすることができます。
- しきい値が超えられたときにトリガー:連続して一定の回数以上アラームルールのしきい値
   を超えた場合にアラーム通知を送信
- 有効期間: アラームルールが有効な期間 この期間はアラームサービスは測定値を確認して アラームを生成するかを決定します。
- 通知連絡先: アラーム通知を受け取るグループ
- 通知方法:

■ メール、DingTalk チャットボット

- メールの件名: デフォルトでは、メールの件名はプロダクト名、測定値、関連するインスタンス ID
- メールの備考:カスタマイズされたアラームメール用の追加情報 アラーム通知メールの本 文の一部として送信されます。
- HTTP コールバック: CloudMonitor がインターネット経由で POST 要求にてアラーム情報をプッシュできる URL を入力 現時点では HTTP にのみ対応しています。

## 5.3 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

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。

## 5.4 CDN モニタリング

CDN の QPS、BPS、バイトヒット率などをモニタリングすることによるクラウドモニタリング は、ドメイン名の使用状況を把握するのに役立ちます。 高速ドメイン名を追加すると、クラウド モニタリングが自動的にそれをモニターし始め、クラウドモニタリングの CDN にログインが完 了します。 このページでモニタリングの詳細を表示できます。 モニタリング項目にアラームルー ルを設定して、データが異常なときにアラーム情報を受け取ることもできます。

#### モニタリングサービス

モニタリング項 目	意味	ディメンション	単位	最小モニター粒 度
1 秒あたりの訪 問数	時間グレイン内 の総訪問数/時間 粒度	ドメイン名	Ш	1分
ネットワーク帯 域幅 BPS	単位時間あた りの最大ネッ トワークトラ フィック	ドメイン名	BPS	1分
ヒット率	時間グレインで 要求されたバ イト数に対す るヒットキャッ シュの確率。バ イト = 要求数 x トラフィック"、 より直接トラフィック のバイトヒット 率に注意しま す。	ドメイン名	割合	1分

・モニタリング項目の説明

モニタリング項	意味	ディメンション	単位	最小モニター粒
目				度
パブリックネッ トワークのトラ フィック不足	つまり、CDN のパブリック ネットワークの ダウンストリー ムトラフィック です。	ドメイン名	バイト	5分
戻りコード 4xx	タイムグレイン 内のすべてのリ ターンコードと しての HTTP リ ターンコード 4xx の割合	ドメイン名	割合	1分
リターンコード 5xx share	タイムグレイン 内のすべてのリ ターンコードと しての HTTP リ ターンコード 5xx の割合	ドメイン名	割合	1分

・モニタリングデータの表示

- 1. Cloud Monitor コンソールにログインします。
- 2. クラウドサービスがモニターする CDN インスタンスのリストを入力します。
- 3. 操作内のインスタンス名またはモニターチャートをクリックして、モニターの詳細ページ に移動します。
- サイズチャートの切り替えボタンをクリックして、大きい画像表示を切り替えます (オプション)。

#### アラームサービス

- ・パラメーターの説明
  - モニター: CDN が提供するモニタリングメトリックス
  - 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい
     値を超えているかどうかを確認します。たとえば、メモリ使用量アラームルールを設定す

る場合、統計サイクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかど うかを確認します。

- 統計方法: 統計方法は、しきい値範囲を超える設定を指します。 統計的方法で平均、最大、 最小、カウント、および値を設定できます。
  - 平均:統計サイクル中にモニターされたデータの平均。統計結果は、15分以内に収集されたすべてのメトリックデータの平均です。80%を超える平均値は、しきい値を超えると見なされます。
  - 最大:統計サイクル中のモニターデータの最大値。統計サイクル中に収集されたモニタ リングデータの最大値がしきい値 80 を超えています。
  - 最小: 統計サイクル中のモニタリング対象データの最小値。統計サイクル中に収集され たデータをモニターするための最小値がしきい値 80 を超えています。
  - ■値:統計サイクル中のモニタリングデータの合計期間内に収集されたメトリックデータの合計が80%を超えると、しきい値を超えます。このような統計的方法はトラフィッククラスメトリクスに必要です。
- 複数回連続してしきい値を超えた場合のアラーム: アラームをトリガーするために値がしき
   い値を超え続けているいくつかの連続した統計的サイクルモニタリング項目を指します。

例: CPU 使用率を 80% を超えるように設定する 5 分の統計的周期で、しきい値を超えた後 に 3 回連続してアラームを発します。検出 CPU 使用率が 80% を初めて超えたときは、ア ラーム通知は発行されません。 セカンドプローブ 5 分間で CPU 使用率は 80% を超え、ア ラームは発行されません。 3 番目のプローブが 80% を超えたときのみ、 アラーム通知が 発行されます。 つまり、実際のデータが最初にしきい値を超えてから最後のアラームルー ルまでに必要な最小時間は、統計サイクル (連続プローブ数-1) = 5 (3-1) = 10 分です。

- ・アラームルールを設定します。
- ・1. Cloud Monitor コンソール にログインします。
  - 2. クラウドサービスがモニターする CDN インスタンスのリストを入力します。
  - インスタンスの "リスト" から [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 ルールページへ移動します。
  - アラームルールページの右上隅にある [新しいアラームルール] をクリックして、パラメー ターに基づいてアラームルールを作成します。

## 5.5 Elastic IP モニタリング

CloudMonitor は 4 つの Elastic IP Address (EIP) メトリクス (送信トラフィック、受信トラ フィック、送信パケット数、および受信パケット数) を提供し、サービスのステータスをモニター するのに役立ちます。 これらのメトリックに対してアラームルールを設定できます。 EIP サービ スを購入すると、 CloudMonitor は次の 4 つのメトリクスに関する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

メトリクス	意味	分析コード	ユニット	最小モニタリン グ粒度
Inbound bandwidth	EIP を通過して ECS インスタン スに到達する 1 秒あたりのトラ フィック量	インスタンス	ビット/秒	1分
Outbound bandwidth	ECS インスタン スから EIP を通 過する 1 秒あた りのトラフィッ ク量	インスタンス	ビット/秒	1分
Number of incoming packets	EIP を通過して ECS インスタン スに到達する 1 秒あたりのパ ケット数	インスタンス	パッケージ/秒	1分
Number of outgoing packets	ECS インスタン スから EIP を 通過する 1 秒あ たりのパケット 数。	インスタンス	パッケージ/秒	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. [クラウドサービスモニタリング] の [Elastic IP アドレス] へ移動します。
- プロダクトインスタンスリストからインスタンス名をクリックする、または [アクション]
   内から [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
   アクセスします。
- チャートサイズボタンをクリックすると、大きなチャート表示に切り替わります(オプション)。

#### アラームサービス

- ・パラメーターの説明
  - メトリクス: EIP が提供するモニタリングインジケーター
  - 統計サイクル: アラームルールシステムは、統計サイクルに基づいて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確認します。たとえば、メモリ使用量に関するア ラームルールの統計周期が1分に設定されている場合、システムはメモリ使用量が毎分しき い値を超えたかどうかを確認します。
  - 統計: データがしきい値を超えているかどうかを判断するための方法を設定します。 "統計"
     では、"平均"、"最大"、"最小"、"合計" を設定できます。
    - 平均: 統計サイクル内のメトリックデータの平均値 統計結果は、15 分以内に収集された すべてのメトリックデータの平均です。 80% 以上の平均値 がしきい値を超えていると 見なされます。
    - 最大: 統計サイクル内のメトリックデータの最大値 統計サイクル内に収集されたメト リックデータの最大値が 80% を超えると、値がしきい値を超えます。
    - 最小: 統計サイクル内のメトリックデータの最小値 統計周期内に収集されたモニタリン グデータの最小値が 80% を超えると、しきい値を超えます。
    - 合計:統計期間内のメトリックデータの合計期間内に収集されたメトリックデータの合計が 80% を超えると、しきい値を超えています。この方法はトラフィックメトリックに必要です。
  - しきい値を数回超過した後のアラーム:メトリック項目の値が連続した複数の統計サイクル
     でしきい値を継続的に超えたときにトリガーされるアラームを指します。

CPU使用率が統計的な5分周期で 80% 以上のアラームであり、3回連続してしきい値を超 えるアラームが発生し、CPU が初めて検出された場合 使用率が 80% を超えても、アラー ムは発生しません。 CPU使用率が 80% を 2 回続けて超えても、アラームは報告されませ ん。アラームは、CPU 使用率が 3 回目に 80% を超えた場合にのみ報告されます。 つま り、実際のデータが最初にしきい値を超えてからアラートポリシーがトリガーされるまで の間に消費される最小時間は次のとおりです。期間 \* (連続検出回数-1) = 5 \ \* (3-1) = 10 分 ・アラームルールを設定します。

- 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 [Elastic IP アドレス] インスタンスリストへ移動しま す。
- プロダクトインスタンスリストのインスタンス名をクリックする、または [アクション] 内 から [アラームルール] 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 ます。
- アラートポリシー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、入力した パラメーターに基づいたアラートポリシーを作成します。

## 5.6 ApsaraDB for Memcache

CloudMonitor は、サービスインスタンスのステータスをモニターするのに役立つ、ApsaraDB for Memcache の7つのモニタリングメトリクス (使用キャッシュや読み取りヒット率など) を 提供します。 これらのモニタリングメトリクスのためのアラームルールを設定することもできま す。 Memcache サービスを購入すると、CloudMonitor は以前のモニタリングメトリクスの データを自動的に収集します。

#### モニタリングサービス

モニタリングメ トリクス	意味	分析コード	単位	最小モニタリン グ細分性
Cache used	使用された キャッシュ量	インスタンス	バイト	1分
Read hit rate	Key-Value (KV ) を正常に読み取 る可能性	インスタンス	割合	1分
QPS	1 秒あたりの KV 読み取りの合計 時間	インスタンス	Ш	1分
Number of records	現在の測定期間 内の合計 KV 数	インスタンス	KV	1分
Cache inbound bandwidth	キャッシュへの アクセスによっ て生成されたト ラフィック	インスタンス	ビット/秒	1分

・ モニタリングメトリクスの説明
モニタリングメ トリクス	意味	分析コード	単位	最小モニタリン グ細分性
Cache outbound bandwidth	キャッシュの読 み取りによって 生成されたトラ フィック	インスタンス	ビット/秒	1分
Eviction	<b>1 秒間に削除さ</b> れたKVの数	インスタンス	1 秒あたりのKV	1分

🗎 注:

- モニタリングデータは最大 31 日間保存されます。
- メトリクスデータは最大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. [クラウドサービスモニタリング] ドロップダウンリストから、[ApsaraDB for Memcache] を選択します。
  - インスタンス名をクリックするか、または [アクション] 内から [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。
  - ページ上部にある [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。
  - 5. モニタリングチャートの右上隅にある [ ズームイン] ボタンをクリックして、チャートを拡 大表示します。

### アラームサービス

CloudMonitor は、すべての Memcache モニタリングメトリクスに対しアラームサービスを提供します。 重要なモニタリングメトリクスにアラームルールを設定した後は、モニタリングデー タが設定されたしきい値を超えるとアラーム通知を受け取ることができるため、問題を迅速に処 理して誤動作を回避できます。

- ・パラメーターの説明
  - モニタリングメトリクス: ECS for Redis によって提供されるモニタリングメトリクス
  - 統計サイクル: アラームシステムは、サイクルに基づいて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確認します。たとえば、メモリ使用量に関するアラームルール

の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。

- 統計方法: データがしきい値を超えているかどうかを決定するために使用される方法 平均 値、最大値、最小値、合計値を統計的方法に設定できます。
  - 平均値: 統計サイクル内のモニタリングデータの平均値 統計結果は、15 分以内に収集されたすべてのモニタリングデータの平均です。80% を超える平均値はしきい値を超えていると見なされます。
  - 最大値: 統計周期内のモニタリングデータの最大値 統計周期内に収集されたモニタリン グデータの最大値が 80% を超えると、しきい値を超えます。
  - 最小値: 統計サイクル内のモニタリングデータの最小値 統計周期内に収集されたモニタ リングデータの最小値が 80% を超えると、しきい値を超えます。
  - 合計値:統計サイクル内のモニタリングデータの合計統計サイクル内に収集されたモニ タリングデータの合計が80%を超えると、それはしきい値を超えます。この方法はト ラフィックメトリクスに必要です。
- 連続時間:モニタリングメトリクスの値が設定された連続サイクルの間、しきい値を継続的
  に超えたときにアラームがトリガーされます。

たとえば、CPU 使用率が 3 分間の連続した 5 分間の統計サイクルでしきい値の 80% を 超えるとアラームが発生するように設定したとします。 つまり、CPU 使用率が初めて 80 % を超えたことが判明してもアラームは発生しません。 CPU 使用率が 5 分後 2 回目の検 出で 80% を超えても、アラームは発生しません。 CPU 使用率が、 3回目の検出で 80% を超えた場合にアラームが発生します。 したがって、実際のデータが最初にしきい値を超 えてからアラームルールがトリガーされるまでの間に消費される最小時間は次のとおりで す。統計サイクルx (連続検出数-1) この場合、1) = 10 分

- ・アラームルールを設定する
  - 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] ドロップダウンリストから、[ApsaraDB for Memcache] を選択します。
  - インスタンス名をクリックするか、または [アクション] 内から [モニタリングチャート] を クリックし、インスタンスモニタリング詳細ページへアクセスします。
  - 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して、このインスタンスの対応するモニタリングメトリクスにアラームルールを設定します。

・バッチアラームルールを設定する

- 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] ドロップダウンリストから、[ApsaraDB for Memcache] を選択します。
- 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。 ページ下部にある [アラー ムルールの設定] をクリックし、アラームルールを一括で追加します。

# 5.7 ApsaraDB for Redis モニタリング

Cloud Monitor では、容量や接続の使用情報を含む ApsaraDB for Redis のステータスと使用 状況をさまざまなメトリクスに基づいて表示します。 Redis インスタンスを購入すると、Cloud Monitor は自動的にインスタンスのモニタリングを開始します。

Redis インスタンスを購入すると、Cloud Monitor は自動的にインスタンスのモニタリングを 開始します。 Cloud Monitor ページへアクセスしメトリックデータを表示します。 データの例 外が発生した場合にアラームが生成されるように、アラームルールを設定することができます。

### モニタリングサービス

•	X	ト	IJ	ク	ス
---	---	---	----	---	---

メトリック	定義	分析コード	単位	最小モニター細 分性
使用容量	現在使用中の Redis 容量	インスタンス	バイト	1分
使用されている 接続数	クライアント接 続の現在の総数	インスタンス	回	1分
書き込み速度	1 秒あたりの現 在の書き込み ネットワークト ラフィック	インスタンス	BPS	1分
読み取り速度	ネットワークト ラフィックは現 在 1 秒あたりに 読み取られます	インスタンス	BPS	1分
操作失敗数	現在の操作 kvstore が失敗 した回数	インスタンス	Ш	1分

メトリック	定義	分析コード	単位	最小モニター細 分性
使用済み容量の パーセント	総容量に対する 現在の使用容量 の割合	インスタンス	割合	1分
使用接続率	合計接続数に対 する確立された 現在の接続数	インスタンス	割合	1分
書き込み帯域幅 使用量	現在の書き込み 帯域幅 (総帯域幅 に対する割合)	インスタンス	割合	1分
読み取り帯域幅 使用量	現在の読み取り 帯域幅の合計帯 域幅に対する割 合	インスタンス	割合	1分
インスタンス障 害	イベントタイプ メトリクス、ア ラームルールを 設定可能	-	-	-
インスタンスマ スタスタンバイ スイッチ	イベントタイプ メトリクス、ア ラームルールを 設定可能	-	-	-

・モニタリングデータの表示

- 1. Cloud Monitor 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] にある ApsaraDB for Redis] インスタンスリストへ移動 します。
- プロダクトインスタンス一覧でインスタンス名をクリックするか、または [アクション] 列 から [モニタリングチャート] をクリックし、インスタンスモニタリング詳細ページへアク セスします。
- 4. [チャートサイズ] ボタンをクリックして、チャートの表示を拡大します (オプション)。

- ・パラメーターの説明
  - メトリクス: ECS for Redis によって提供されるモニタリングインジケーター
  - "統計サイクル":アラームルールシステムは、統計データに基づいてモニタリングデータが アラームルールのしきい値を超えたかどうかをチェックします。たとえば、メモリ使用量
     に関するアラームルールの統計サイクルが1分に設定されている場合、システムは、メモ リ使用量が1分おきにしきい値を超えたかどうかを確認します。
  - 統計: データがしきい値を超えているかどうかを判断するための方法を設定します。"統計"
    で "平均"、"最大"、"最小"、"合計" を設定できます。
    - 平均: 統計サイクル内のメトリックデータの平均値 統計結果は、15 分以内に収集された すべてのメトリックデータの平均です。80% を超える平均値は、しきい値を超えたと 見なされます。
    - 最大:統計サイクル内のメトリックデータの最大値統計サイクル内に収集されたメト リックデータの最大値が80%を超えると、その値はしきい値を超えます。
    - 最小: 統計サイクル内のメトリックデータの最小値 統計サイクル内に収集されたメト リックデータの最小値が 80% を超えると、その値はしきい値を超えます。
    - 合計:統計サイクル内のメトリックデータの合計統計サイクル内に収集されたメトリッ クデータの合計が80%を超えると、その値はしきい値を超えます。トラフィックベー スインジケーターには、前述の統計方法が必要です。
  - "しきい値が数回超えた後にアラームをトリガーする": これは、メトリクスの値が連続した
    統計的サイクルでしきい値を超えたときにトリガーされるアラームを表します。

たとえば、しきい値が3 回超えた後、5 分間の統計サイクルで CPU 使用率が80% を超え ると アラームが発生するようにに設定できます。 CPU 使用率が初めて 80% を超えたこと が判明した場合、警告通知は送信されません。5 分に 2 回目の CPU の検証の場合 CPU 使 用率が 2 回連続で 80% を超えてもアラームは発生しません。3 回目に CPU 使用率が 80 % を超えた場合のみに、アラームが発生します。 つまり、実際のデータが最初にしきい 値を超えてからアラームルールがトリガーされるまでの間に消費される最小時間は、統計 サイクル\*(連続検出回数 -1) = 5\*(3-1) = 10 分です。

### ・アラームルールの設定

- 1. Cloud Monitor 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] から[ApsaraDB for Redis] インスタンスリストへ移動します。
- [アクション] のインスタンスリストで [アラームルール] をクリックし、インスタンスア ラームルールページにアクセスします。
- 4. 必要なフィールドヘすべての関連情報を入力し、[確認] をクリックして新しいアラーム ルールを作成します。

## 5.8 ApsaraDB for MongoDB

クラウドデータベースアイテムの MongoDB サービスインスタンスの CPU 使用率、メモリ使用 率などの複数のモニターをモニタリングすることによるクラウドモニタリングは、ユーザーがイ ンスタンスの実行ステータスをモニタリングするのに役立ち、ユーザーがモニタリングアイテム にアラームルールを設定できるようにします。 MongoDB サービスを購入した後、 クラウドモ ニタリングは、上記のモニタリング項目のデータを自動的に収集します。

### モニタリングサービス

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
CPU 使用率	インスタンスの CPU 使用率	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	割合	5分
メモリ使用量	インスタンスの メモリ使用量	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	割合	5分

・モニタリング項目

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
ディスクの使用 状況	インスタンスの ディスク使用量	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	割合	5分
IOPS の使用量	インスタンスの 使用量	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	割合	5分
接続使用量	接続数は、アプ リケーションが MongoDB に 接続できるイン スタンスの数で す。接続使用数 は、使用された 接続数の割合で す。	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	割合	5分
1 秒あたりの平 均 SQL クエリ数	MongoDB イン スタンスの 1 秒 あたりの SQL ク エリの平均数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	Ш	5分
接続使用数	現在のアプリ ケーションが 接続している MongoDB のイ ンスタンス数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	回	5分
インスタンス が使用している ディスク容量	インスタンスに よって実際に 使用されている ディスク容量の 合計	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
データが占有し ているディスク 容量	データによって 使用されている ディスク容量	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分
ディスク容量の 使用ログ	ログが占有して いるディスク容 量	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分
イントラネット トラフィック	インスタンスの ネットワークフ ロートラフィッ ク	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分
アウトバウンド イントラネット トラフィック	インスタンスの ネットワークフ ロートラフィッ ク	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分
リクエスト数	サーバーに送信 された要求の総 数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	П	5分
挿入操作数	[INSERT] コマンドが MongoDB イン スタンスが最後 に開始されてか ら現在の累積受 領までの回数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	回	5分

マークリンドの	李叶	八七 N	))) []	目上エンクが
モニタリンク項	<b>息</b> 咻 	分析コート	単位	最小モニター細
B				分性
クエリ操作数	[query] コマン ドが MongoDB インスタンスが 最近開始されて から現在累積さ れている [query ] コマンドまでの 回数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	バイト	5分
更新操作数	[update] コマン ドが MongoDB インスタンス が最近開始さ れてから現在累 積されている [ update] コマン ドまでの回数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	回	5分
削除操作数	MongoDB イン スタンスが最後 に起動されてか ら[Delete] の累 積実行までの操 作数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	回	5分
[getmore] から の操作数	MongoDB イ ンスタンスが 最後に起動され てから現在の[ getmore] の累 積実行までの操 作数	ユーザーディメ ンション、イン スタンスディ メンション、マ スターディメン ション	Ш	5分
コマンド操作数	MongoDB 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、およ びマスター/バッ クアップ	Ш	5分

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
インスタンス障 害	アラームルール を設定できるイ ベントタイプメ トリック	-	-	-

- メトリックデータは最大 31 日間保存できます。
- メトリックデータは最大14日間連続して表示できます。
- ・メトリックデータの表示
  - 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] にある、 [ApsaraDB for MongoDB] インスタンスリス トへ移動します。
  - プロダクトインスタンスリストでインスタンス名をクリックするか、または[アクション]
    列から [メトリックチャート] をクリックし、インスタンスモニタリング詳細ページのメト リックを表示します。
  - ページ上部にある、[時間範囲] ショートカットをクリックする、または特定の選択機能を 使用します。データは、最大連続14日間分を閲覧することができます。
  - 5. メトリックチャートの右上隅にある [ズームイン] ボタンをクリックしてグラフを拡大しま す。

### アラームサービス

・パラメーターの説明

- メトリクス項目: MongoDB 用に ApsaraDB によって提供されるモニタリングインジケー ター
- 統計サイクル: アラームシステムは、統計サイクルに基づいて、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確認します。たとえば、メモリ使用量に関するアラー

ムルールの統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきに しきい値を超えたかどうかを確認します。

- 統計方法: データがしきい値を超えているかどうかを判断するための方法を設定します。
  計方法で "平均"、"最大"、"最小"、"合計" を設定できます。
  - 平均: 統計サイクル内のメトリックデータの平均値 統計結果は、15 分以内に収集された すべてのメトリックデータの平均です。 80% を超える平均値は、しきい値を超えたと 見なされます。
  - 最大: 統計サイクル内のメトリックデータの最大値 統計サイクル内に収集されたメト リックデータの最大値が 80% を超えると、値がしきい値を超えます。
  - 最小: 統計サイクル内のメトリックデータの最小値 統計サイクル内に収集されたメト リックデータの最小値が 80% を超えると、その値はしきい値を超えます。
  - 合計:統計サイクル内のメトリックデータの合計統計サイクル内に収集されたメトリッ クデータの合計が80%を超えると、それはしきい値を超えます。トラフィックベース インジケーターには、前述の統計方法が必要です。
- 連続時間:メトリック項目の値が連続した数回の統計サイクルでしきい値を継続的に超えた
  ときにトリガーされるアラームを指します。

たとえば、しきい値を3回超えた後、5分の統計サイクル内に CPU 使用率が 80% を超え るとアラームが発生するように設定できます。 CPU 使用率が初めて 80% を超えたことが 判明した場合、警告通知は送信されません。 CPU 使用率が 80% を 2 回続けて超えても、 アラームは発生しません。 アラームは、CPU 使用率が 3 回目に 80% を超えた場合にのみ 発生します。 つまり、実際のデータが最初にしきい値を超えてからアラームルールがトリ ガーされるまでの間に消費される最小時間は、統計サイクル\* (連続検出回数-1) = 5\*(3-1) = 10分です。

- ・単一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] > [ApsaraDB for MongoDB] を選択します。
  - 3. インスタンス名または稼働中のモニターチャートをクリックして、インスタンスのモニ ター詳細ページへ移動します。
  - 4. モニタリングチャートの右上隅にあるベルボタンをクリックして、インスタンスに対応す るモニタリング項目にアラームルールを設定します。

### 一括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. MongoDB (バージョンインスタンスのクラウドサービス一覧でモニターされているクラウ ドデータベース) へ移動します。
- 3. インスタンスリストページで目的のインスタンスを選択したら、ページの下にある [アラー ムルールの設定] をクリックして、アラームルールをまとめて追加できます。

# 5.9 メッセージサービスのモニタリング

メッセージサービスのモニタリングによるクラウドモニタリング、メッセージの遅延、無効 なメッセージ、アクティブなメッセージ、3つのモニタリング項目は、メッセージサービスの キュー使用量の取得を支援します。

ユーザーがメッセージサービス用のメッセージキューを作成すると、クラウドモニタリングが自 動的にそれらをモニターし始め、クラウドモニタリングメッセージサービスにログインします。 このページでモニタリングの詳細を表示できます。モニタリング項目にアラームルールを設定し て、データが異常なときにアラーム情報を受け取ることもできます。

### モニタリングサービス

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
Activemess ages	このキューでア クティブなメッ セージの総数	ユーザー ID、 リージョン、 ビッド、キュー	П	5分
Inactiveme ssages	このキューで 非アクティブな メッセージの総 数	ユーザー ID、 リージョン、 ビッド、キュー	E	5分
Delaymessage	このキュー内の 遅延状態にある メッセージの総 数	ユーザー ID、 リージョン、 ビッド、キュー	回	5分
Sendmessag eecount	メッセージ要求 を送信する	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600

・モニタリング項目の説明

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
Batchsendm essagecount	一括メッセージ 送信要求数	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600
Receivemes sagecount	メッセージ受信 要求数	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600
Batchrecei vemessagec ount	一括受信メッ セージ要求数	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600
Batchdelet emessageco unt	一括削除メッ セージ要求数	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600
Changemess agevisibil itycount	メッセージの表 示数を変更する	ユーザー ID、 リージョン、 ビッド、キュー	項目	3600

- ・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. クラウドサービスがモニターするメッセージサービスインスタンスの一覧へ移動します。
  - 3. 稼働中のインスタンス名またはモニターチャートをクリックして、モニターの詳細ページ に移動します。
  - サイズチャートの切り替えボタンをクリックして、大きい画像表示を切り替えます (オプション)。

- ・パラメーターの説明
  - モニター: メッセージサービスによって提供されるモニタリングメトリック
  - 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい
    値を超えているかどうかを確認します。たとえば、メモリ使用量アラームルールを設定す

る場合、統計サイクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかど うかを確認します。

- 統計方法: 統計方法は、しきい値範囲を超える設定を指します。 統計方法で "平均"、"最 大"、"最小"、"カウント"、および "値" を設定できます。
  - 平均: 統計サイクル中にモニターされたデータの平均 結果は、15 分以内に収集されたす べてのモニタリングデータの平均です (この平均が80を超える場合)。 しきい値を超え た場合のみ
  - 最大: 統計サイクル中のモニターデータの最大値 統計サイクル中に収集されたモニタリングデータの最大値がしきい値 80 を超えています。
  - 最小:統計サイクル中のモニター対象データの最小値統計サイクル中に収集されたデー タをモニターするための最小値がしきい値 80 を超えています。
  - ■値:統計サイクル中のモニタリングデータの合計統計期間中に収集されたモニタリング データを合計した値が80%を超える結果となります。つまり、しきい値を超えます。 このような統計方法はトラフィッククラスメトリクスに必要です。
- ・ いくつかの連続したしきい値を超えた後のアラーム: アラームをトリガーするために値がし
  きい値を超え続けているいくつかの連続した統計サイクルモニタリング項目を指します。

例: しきい値を3回超えた後、5分の統計サイクル内に CPU 使用率が 80% を超えるとア ラームが発生するように設定できます。 CPU 使用率が初めて 80 を超えた場合、アラーム 通知は発生しません。 CPU 使用率が2回目の5分間で 80% を超えた場合、アラーム通知 は発生しません。3回目の検証でもまだ 80% を超える場合にアラーム通知が発生します。 つまり、実際のデータが最初にしきい値を超えてから最後のアラームルールまでに必要な 最小時間は、統計サイクル (連続プローブ数-1) = 5 (3-1) = 10分です。

- ・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. クラウドサービスがモニターするメッセージサービスインスタンスの一覧へ移動します。
  - インスタンスリストアクションでアラームルールをクリックし、インスタンスのアラート ルールページへ移動します。
  - アラームルールページの右上隅にある新しいアラームルールをクリックし、パラメーター に基づいたアラームルールを作成します。

# 5.10 AnalyticDB ELSU

Analytic dB ディスク定格容量、ディスク使用容量、ディスク使用量 3 メッセージの提供による クラウドモニタリングは、 Analytic DB サービスの利用に役立ちます。

Analytic dB の利用を開始すると、クラウドモニタリングは、クラウドモニタリングの Analytic dB のモニタリングを自動的に開始します。 このページでモニタリングの詳細を表示で きます。 モニタリング項目にアラームルールを設定して、データが異常なときにアラーム情報を 受け取ることもできます。

### モニタリングサービス

モニタリング項 目	意味	分析コード	単位	最小モニター細 分性
Disksize	ディスク定格容 量	インスタンス ID、テーブル スキーマ、ワー カー ID	МВ	1分
DiskUsed	ディスク使用容 量	インスタンス ID、テーブル スキーマ、ワー カー ID	МВ	1分
Diskusedpe rcent	ディスクの使用 状況	インスタンス ID、テーブル スキーマ、ワー カー ID	割合	1分

・モニタリング項目の説明

- ・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. クラウドサービスがモニターする Analytic データベースの一覧へ移動します。
  - 稼働中のインスタンス名またはモニターチャートをクリックし、モニター詳細ページへ移 動します。
  - サイズチャートの切り替えボタンをクリックして、大きい画像表示を切り替えます (オプション)。

- ・パラメーターの説明
  - モニタリング: 分析データベースによって提供されるモニタリングメトリックス
  - 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい 値を超えているかどうかを確認します。たとえば、メモリ使用量アラームルールを設定す る場合、統計サイクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかど うかを確認します。
  - 統計方法: 統計方法は、しきい値範囲を超える設定を指します。 統計方法で "平均"、"最 大"、"最小"、"カウント"、および "値" を設定できます。
    - 平均: 統計サイクル中にモニターされたデータの平均 結果は 15 分以内に収集されたす べてのモニタリングデータの平均です。この平均が 80% を超えると、しきい値を超え ます。
    - 最大:統計サイクル中のモニターデータの最大値統計サイクル中に収集されたモニター データの最大値がしきい値 80 を超えています。
    - 最小: 統計サイクル中のモニター対象データの最小値 統計サイクル中に収集されたデー タをモニターするための最小値がしきい値 80 を超えています。
    - 値: 統計サイクル中のモニタリングデータの合計 統計期間中に収集されたモニタリング データを合計すると、合計後に、結果の 80% 以上がしきい値を超えます。 このような 統計的方法はトラフィッククラスメトリクスに必要です。
  - ・いくつかの連続したしきい値を超えた後のアラーム:アラームをトリガーするために値が しきい値を超え続けているいくつかの連続した統計サイクルモニタリング項目を指します。

例: しきい値を 3 回超えた後、5 分の統計サイクル内に CPU 使用率が 80% を超えるとア ラームが発生するように設定できます。 CPU 使用率が初めて 80 を超えた場合、アラー ム通知は発生しません。 2 回目の5 分間でCPU 使用率が 80% を超えた場合、アラーム通 知は発生しません。 3 回目の検証でもまだ 80% を超える場合に アラーム通知が発生しま す。 つまり、実際のデータが最初にしきい値を超えてから最後のアラームルールまでに必 要な最小時間は、統計サイクルX (連続プローブ数-1) = 5 x (3-1) = 10 分です。

- ・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. クラウドサービスがモニターする分析データベースインスタンスの一覧へ移動します。
  - 3. インスタンスリストアクションでアラームルールをクリックし、インスタンスのアラート ルールページへ移動します。
  - 4. アラームルールページの右上隅にある新しいアラームルールをクリックして、パラメー ターに基づいてアラームルールを作成します。

# 5.11 ログサービスモニタリング

CloudMonitor では、11 種類のメトリックス (アウトバウンドトラフィック、インバウンドト ラフィック、全体 QPS、ログ統計メソッドを含む) に基づいたログサービスの使用量を表示しま す。ログサービスインスタンスを作成すると、CloudMonitor は自動的にサービスのモニター を開始します。 CloudMonitor Log Service ページにアクセスしてメトリクスデータを表示で きます。データ例外が発生したときにアラームがトリガーされるように、メトリックのアラーム ルールを設定できます。

### モニタリングサービス

メトリック	定義	分析コード	単位	最小モニター細 分性
Inflow	1 分あたりのロ グストアの送受 信フロー	userId、 Project、 Logstore	バイト	1分
Outflow	1 分あたりのロ グストアフロー	userId、 Project、 Logstore	バイト	1分
SumQPS	ログストア内の 1 分あたりの合 計書き込み数	userId、 Project、 Logstore	カウント	1分
LogMethodQ PS	ログストアへの 1 分あたりの合 計書き込み数。	userId、 Project、 Logstore、 Method	カウント	1分

・メトリックス

メトリック	定義	分析コード	単位	最小モニター細 分性
LogCodeQPS	ログストア内の 特定のステータ スコードにマッ ピングされた1 分あたりの書き 込み数。	userId、 Project、 Logstore、 Status	カウント	1分
SuccessdByte	ログストア内の 正常に解決され たバイト数	userId、 Project、 Logstore	バイト	10分
SuccessdLines	ログストア内の 解決されたログ の行数	userId、 Project、 Logstore	カウント	10分
Failedlines	ログストアで解 決できなかった ログ内の行数	userId、 Project、 Logstore	カウント	10分
AlarmPV	logStore 内の ECS 設定エラー の総数	userId、 Project、 Logstore	カウント	5分
AlarmUv	ログストア内の 構成が正しくな い ECS インスタ ンスの総数	userId、 Project、 Logstore	カウント	5分
AlarmIPCount	ログストア内の 特定のIPアドレ スによって発生 したエラーの数	userId、 Project、 Logstore、 alarm_type、 source_ip	カウント	5分

- ・メトリックデータの表示
  - 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] で、[ログサービス] インスタンスリストへ移動します。
  - プロダクトインスタンスリストからインスタント名をクリックするか、または [アクション] 列から [モニタリングチャート] をクリックし、インスタンスモニタリング詳細ページへ アクセスします。
  - 4. チャートサイズボタンをクリックすると、大きなチャート表示に切り替わります (オプション)。

- ・パラメーターの説明
  - メトリクス: ログサービスによって提供されるモニタリングインジケーター
  - 統計サイクル: アラームシステムは、統計サイクルに基づいて、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確認します。たとえば、メモリ使用量に関するアラー ムルールの統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきに しきい値を超えたかどうかを確認します。
  - 統計方法: この方法は、データがしきい値を超えているかどうかを判断するために使用されます。統計方法で "平均"、"最大"、"最小"、および "合計" を設定できます。
    - 平均: 統計サイクル内のメトリックデータの平均値 統計結果は、15 分以内に収集された メトリックデータの平均です。80% を超える平均値は、しきい値を超えたと見なされ ます。
    - 最大: 統計サイクル内のメトリックデータの最大値統計サイクル内に収集されたメト リックデータの最大値が 80% を超えると、値がしきい値を超えます。
    - 最小:統計サイクル内のメトリックデータの最小値統計サイクル内に収集されたメト リックデータの最小値が80%を超えると、その値はしきい値を超えます。
    - 合計:統計サイクル内のメトリックデータの合計統計サイクル内に収集されたメトリッ クデータの合計が80%を超えると、それはしきい値を超えます。トラフィックベース インジケーターには、前述の統計方法が必要です。
  - しきい値が数回超過した後にアラームをトリガーする:これは、メトリック項目の値が連続
    したいくつかの統計サイクルでしきい値を継続的に超えたときにトリガーされるアラーム
    を表します。

たとえば、しきい値を3回超えた後、5分の統計サイクル内で CPU 使用率が80% を超え るとアラームが発生ように設定できます。 CPU 使用率が初めて80% を超えたことが判明 した場合、警告通知は送信されません。 CPU 使用率が80% を2回続けて超えても、ア ラームは発生しません。アラームは、CPU 使用率が3回目に80% を超えた場合にのみ送 信されます。 つまり、実際のデータが最初にしきい値を超えてからアラームルールがトリ ガーされるまでの間に消費される最小時間は、統計サイクル\* (連続検出回数-1) = 5\*(3-1) = 10分です。



- アラームルールを設定するときに、QPS のログ方法とステータスコードを選択できます。 選択しない場合、QPS はすべてのログ方法とステータスコードの統計データを収集しま す。
- メソッドフィールドはPostLogStoreLogs、GetLogtailConfig、PutData、GetCursorO rData、GetData、GetLogStoreHistogram、GetLogStoreLogs、ListLogStores、 ListLogStoreTopicsを含みます。
- ステータスフィールドには、200、400、401、403、405、500、および 502 が含まれます。
- ・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] で、[ログサービス] インスタンスリストへ移動します。
  - 3. [アクション] 列から [アラームルール] をクリックし、インスタンスのアラームルールペー ジへアクセスします。
  - 4. 必要なフィールドにすべての関連情報を入力し、[確認] をクリックし、新しいアラーム ルールを作成します。

# 5.12 コンテナーサービスモニタリング

CPU 使用率、メモリ使用量などコンテナサービスの7つのモニタリング項目使ったクラウドモ ニタリングでは コンテナーサービスを利用できるように助けます。 コンテナーサービスを作成し た後、クラウドモニタリングは自動的にコンテナーサービスのモニターを開始します。クラウド モニタリング用のコンテナサービスページにログインしてモニタリングの詳細を表示できます。 データが異常なときにアラーム通知を受け取るように、モニターにアラームルールを設定するこ ともできます。

### モニタリングサービス

モニタリング項 目	意味	ディメンション	単位	最小モニター粒 度
containerC puUtilization	コンテナーの CPU 使用率	ユーザーディメ ンション、コン テナーディメン ション	割合	30 秒

・モニタリング項目の説明

モニタリング項 目	意味	ディメンション	単位	最小モニター粒 度
Containerm emoryutili zation	コンテナーメモ リ使用量	ユーザーディメ ンション、コン テナーディメン ション	割合	30 秒
Containerm emoryamount	コンテナーメモ リ使用量	ユーザーディメ ンション、コン テナーディメン ション	バイト	30 秒
Containeri nternetin	ネットワークへ のコンテナート ラフィック	ユーザーディメ ンション、コン テナーディメン ション	バイト	30 秒
containerI nternetOut	ネットワークか らのコンテナー トラフィック	ユーザーディメ ンション、コン テナーディメン ション	バイト	30 秒
containerI ORead	コンテナーの I/ O 読み取り	ユーザーディメ ンション、コン テナーディメン ション	バイト	30 秒
containerI OWrite	コンテナーの I/ O 書き込み	ユーザーディメ ンション、コン テナーディメン ション	バイト	30 秒



- モニターデータは最大 31 日間保存されます。
- ユーザーはモニタリングデータを最大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. クラウドモニタリングコンソールにログインします。
- クラウドサービスがモニタリングするコンテナサービスインスタンスのリストを入力します。
- 3. 操作内のインスタンス名または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 タリングの詳細ページに移動し、メトリックを表示します。
- ページ上部の[時間範囲] クイック選択ボタン、またはページの最上部にある完全選択機能 をクリックします。最大モニタリングデータでは連続14日分のモニタリングデータを表示 します。
- 5. モニター MAP の右上隅にあるズームインボタンをクリックして、モニターの大きい画像を 表示します。

アラームサービス

- ・単一のアラームルールを設定する:モニタリングチャートの右上隅にあるベルボタンをクリックします。このインスタンスに対応するモニタリング項目にアラームルールを設定できます。
- ・一括アラームルールを設定します。インスタンスのリストページで目的のインスタンスを選択します。ページの下にある [アラームルールの設定] をクリックして、アラームルールをまとめて追加できます。

### 5.13 共有帯域幅

CloudMonitor は、共有帯域幅をモニターすることによってネットワークアクセス、帯域幅な どをモニターし、ユーザーが共有帯域幅のネットワーク使用量をモニターするのに役立ち、ユー ザーがモニタリング項目にアラームルールを設定できるようにします。 自動スケーリングサービ スを購入すると、CloudMonitor は自動的に上記のメトリクスに関するデータを収集します。

### モニタリングサービス

モニタリング項目	分析コード	単位	最小モニター細分性
帯域幅パケットネッ トワークの受信帯域 幅	ユーザーディメン ション、インスタン スディメンション	ビット/秒	1分
帯域幅パケットネッ トワークの送信帯域 幅	ユーザーディメン ション、インスタン スディメンション	ビット/秒	1分

・モニタリング項目

モニタリング項目	分析コード	単位	最小モニター細分性
帯域幅パケットネッ トワークの受信パ ケット	ユーザーディメン ション、インスタン スディメンション	パッケージ/秒	1分
帯域幅パケットネッ トワークフローパ ケット	ユーザーディメン ション、インスタン スディメンション	パッケージ/秒	1分
帯域幅パケットネッ トワークの発信帯域 幅使用量	ユーザーディメン ション、インスタン スディメンション	%	1分

# 🗎 注:

- モニタデータは最大 31 日間保存されます。
- 最大7日間連続してモニタリングデータを表示できます。

・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. クラウドサービスがモニターする共有帯域幅のインスタンスのリストを入力します。
- 稼働中のインスタンス名または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 タリングの詳細ページに移動し、メトリックを表示します。
- ページ上部の時間範囲をクリックしてボタンを選択する、または正確な機能を選択する
  と、連続7日間分のモニタリングデータを表示できます。
- 5. モニタの拡大画像を表示するには、モニタ MAP の右上隅にあるズームボタンをクリック します。

### アラームサービス

- ・パラメーターの説明
  - モニター:帯域幅を共有するサービスによって提供されるモニタリングメトリック。
  - 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい 値を超えているかどうかを確認します。たとえば、メモリ使用量アラームルールを設定す る場合、統計サイクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかど うかを確認します。
  - 連続回数: アラームを発生させるためにしきい値を超え続けている統計サイクルモニタリン グ項目の連続回数を指します。

- ・単一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. クラウドサービスがモニターする共有帯域幅のインスタンスのリストを入力します。
  - 3. 稼働中のインスタンス名または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移動します。
  - モニターチャートの右上隅にあるベルボタンまたはページの右上隅にある新しいアラーム ルールをクリックすると、このインスタンスに対応するモニタリング項目にアラームルー ルを設定できます。
- 一括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. クラウドサービスがモニターする共有帯域幅インスタンスのリストを入力します。
  - 3. インスタンスリストページで目的のインスタンスを選択したら、ページの下にある [アラー ムルールの設定] をクリックして、アラームルールをまとめて追加できます。

# 5.14 Global Acceleration モニタリング

Cloud Monitor は、Global Acceleration のインバウンドおよびアウトバウンドネットワーク 帯域幅など、複数のモニタリングメトリクスをモニターします。 これは、Global Acceleration のネットワーク使用状況をモニターするのに役立ち、モニタリングメトリックにアラームルール を設定するのに役立ちます。 Global Acceleration サービスを購入した後、Cloud Monitor は 自動的に上記のモニタリングメトリクスに関するデータを収集します。

### モニタリングサービス

・メトリクス

測定値	ディメンション	単位	最小モニター細分性
インバウンド帯域幅	ユーザーとインスタ ンス	Bits/s	1分
アウトバウンド帯域 幅	ユーザーとインスタ ンス	Bits/s	1分
インバウンドパッ ケージ	ユーザーとインスタ ンス	pps	1分

測定値	ディメンション	単位	最小モニター細分性
アウトバウンドパッ ケージ	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 日間保存されます。
- 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. Cloud Monitor コンソールにログインします。
  - [クラウドサービスモニタリング]の [Global Acceleration] インスタンスリストへ移動します。
  - インスタンス名をクリックするか、または [アクション] の [モニタリングチャート] をク リックし、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。
  - ページ上部のメニューから [時間範囲] をクリックするか、または特定の選択機能を使用し 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. モニタリングチャートの右上隅にある [ズームイン] をクリックしてチャートを拡大しま す。

### アラームサービス

- ・パラメーターの説明
  - モニタリングメトリクス: Global Acceleration Service によって提供されるモニタリング メトリクス
  - 統計サイクル: アラームシステムは、サイクルに基づいて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確認します。たとえば、メモリ使用量に関するアラームルール の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。
  - 連続時間:モニタリングメトリクスの値が、設定された連続サイクルの間、しきい値を継続
    的に超えると、アラームがトリガーされます。

- ・アラームルールの設定
  - 1. Cloud Monitor 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 [Global Acceleration] インスタンスリストへ移動し ます。
  - インスタンス名をクリックするか、または [アクション] の [モニタリングチャート] をク リックし、インスタンスモニタリング詳細ページへアクセスします。
  - モニタリングチャートの右上隅にあるベルのアイコン、またはページの右上隅にある [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モニタリングメトリックの 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. Cloud Monitor 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 [Global Acceleration] インスタンスリストへ移動し ます。
  - 3. インスタンスの一覧ページで適切なインスタンスを選択します。 [アラームルールの設定] をクリックし、複数のアラームルールを追加します。

## 5.15 高性能時系列データベース hitsdb

CloudMonitor は、HiTSDB ディスク使用量、タイムライン数、タイムポイント数など、複数の モニタリングメトリックスをモニターします。 NAT ゲートウェイのネットワーク使用をモニター するのに役立ち、モニタリングメトリックスのアラームルールを設定できます。 hitsdb を購入 すると、クラウドモニタリングは hitsdb モニターのデータを自動的に収集します。

### モニタリングサービス

・モニタリング項目

モニタリング項目	分析コード	ユニット	最小モニター細分性
ディスク使用量	ユーザーとインスタ ンス	%	20 秒
タイムライン数量	ユーザーとインスタ ンス	カウント	20 秒
ポイントインタイム 成長率	ユーザーとインスタ ンス	カウント/秒	20 秒

🗎 注

- モニタリングデータは最大 31 日間保存されます。
- 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。
- ・メトリックデータの表示
  - 1. CloudMonitor コンソールにログインします。
  - 2. 2. [クラウドサービスモニタリング] の HiTSDB インスタンスリストに移動します。
  - 3. 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の詳細ページにアクセスし、さまざまなメト リックを表示します。
  - ページ上部の [時間範囲] ショートカットをクリックするか、特定の選択機能を使用します。
    最大 14 日間連続したメトリックデータを表示できます。
  - 5. モニタの拡大画像を表示するには、モニタ MAP の右上隅にあるズームボタンをクリック します。

・説明

- モニター: hitsdb のサービスによって提供されるモニタリングインジケーター
- 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい 値を超えているかどうかを確認します。たとえば、メモリ使用量に関するアラームルール の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。
- 連続時間:モニタリングメトリックの値が設定された連続サイクルの間、しきい値を継続的
  に超えたときにアラームがトリガーされます。
- ・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 HiTSDB インスタンスリストに移動します。
  - 操作中のインスタンス名またはモニタリングチャートをクリックすると、インスタンスモニタリングの詳細ページへ移動します。
  - 4. モニタリングチャートの右上隅にあるベルボタンまたはページの右上隅にある [New Alarm Rule]をクリックして、このインスタンスの対応するモニタリングメトリックにア ラームルールを設定します。

### ・バッチ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 HiTSDB 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目的のインスタンスを選択したら、ページの下にある [アラー ムルールの設定] をクリックして、アラームルールをまとめて追加できます。

## 5.16 VPN ゲートウェイ

Cloud Monitor は、VPN ゲートウェイのインバウンドおよびアウトバウンドのネットワーク帯 域幅など、複数のモニタリングメトリクスをモニターします。 VPN ゲートウェイのネットワー ク使用量をモニターするのに役立ち、モニタリングメトリクスのためにアラームルールを設定で きます。 VPN ゲートウェイサービスを購入した後、Cloud Monitor は自動的に上記のモニタリ ングメトリクスに関するデータを収集します。

### モニタリングサービス

・ モニタリングメトリクス

Cloud Monitor は以下のモニタリングメトリクスを提供します。

モニタリングメトリ クス	ディメンション	ユニット	最小モニター細分性
帯域幅パッケージの 受信ネットワーク帯 域幅	ユーザーとインスタ ンス	Bit/s	1分
帯域幅パッケージの 送信ネットワーク帯 域幅	ユーザーとインスタ ンス	Bit/s	1分
帯域幅パッケージの 着信パケット	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 日間保存されます。
- 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. Cloud Monitor 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 [VPN ゲートウェイ] インスタンスリストヘアクセスします。
- インスタンス名をクリックするか、または [アクション] の [モニタリングチャート] をク リックして、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。
- ページ上部にある [時間範囲] のクイック選択ボタンをクリック、または特定の選択機能を 使用します。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. モニタリングチャートの右上隅にある[ズームイン] ボタンをクリックし、グラフを拡大します。

### アラームサービス

- ・パラメーターの説明
  - モニタリングメトリクス: VPN ゲートウェイサービスによって提供されるモニタリングメ
    トリクス
  - 統計サイクル: アラームシステムは、サイクルに基づいて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確認します。たとえば、メモリ使用量に関するアラームルール の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。
  - 連続時間: モニタリングメトリクスの値が設定された連続したサイクルの間、しきい値を継 続的に超えたときにアラームがトリガーされます。
- ・アラームルールの設定
  - 1. Cloud Monitor コンソールにログインします。
  - [クラウドサービスモニタリング] の [VPN ゲートウェイ] インスタンスリストヘアクセスします。
  - インスタンス名をクリックするか、または [アクション] の [モニタリングチャート] をク リックして、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。
  - モニタリングチャートの右上にあるベルのアイコン、または、ページの右上隅にある [新し いアラームルール] をクリックし、インスタンスの対応するモニタリングメトリクスのア ラームルールを設定します。

### 一括アラームルールの設定

- 1. Cloud Monitor 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 [VPN ゲートウェイ] インスタンスリストヘアクセスします。
- 3. インスタンスの一覧ページから適切なインスタンスを選択します。 ページの下部にある [ア ラームルールを設定] をクリックし、アラームルールを一括で追加します。

# 5.17 API ゲートウェイ

Cloud Monitor は、API ゲートウェイで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、およびその他の測定データを提供し、API ゲートウェイサービスの使用情報を 取得するのに役立ちます。API ゲートウェイインスタンスをアクティブ化後、Cloud Monitor は自動的にインスタンスのモニタリングを開始します。API ゲートウェイインスタンスをアク ティブ化後、Cloud Monitor は自動的にインスタンスのモニタリングを開始します。Cloud Monitor API ゲートウェイページにアクセスして測定データを表示できます。データ例外が発 生したときにアラートが報告されるように、メトリックのアラートポリシーを設定できます。

### モニタリングサービス

測定値	定義	ディメンション	単位	最小モニター細 分性
エラー分布	1 つのモニタリ ング期間内に API に対して返 された 2XX、 4XX、および 5XX ステータス コードの回数	ユーザーと API	カウント	1分
インバウンドト ラフィック	1 つのモニタリ ング期間内の API からのリ 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

・メトリクス

測定值	定義	ディメンション	単位	最小モニター細
				分性
アウトバウンド トラフィック	1 つのモニタリ ング期間内の API からのリ 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
応答時間	ゲートウェイ が API を使っ てバックエンド サービスを呼び 出す時モニタリン グ期間と、1 つの間内にバッ クエンドサービ スが返却結果を 受け取る時刻と の差	ユーザーと API	秒	1分
1 モニタリング 期間中にAPI に よって受信され た	リクエストの合 計	ユーザーと API	時間あたり	1分

- ・測定データの表示
  - 1. Cloud Monitor コンソールにログインします。
  - [クラウドサービスモニタリング] の [API ゲートウェイ] インスタンスリストへ移動します。
  - プロダクトインスタンスリストのインスタンス名をクリックするか、または [アクション]
    の [測定チャート] をクリックし、インスタンスモニタリング詳細ページへアクセスします。
  - 4. チャートサイズボタンをクリックして、大きなチャート表示に切り替えます (オプション)。

- ・パラメーターの説明
  - メトリクス: API ゲートウェイによって提供されるモニタリングインジケーター
  - 期間: アラートシステムは、期間に基づいてモニタリングデータがアラートしきい値を超え
    たかどうかを確認します。たとえば、メモリ使用量に関するアラートポリシーの期間が1

分に設定されているとします。 システムはメモリ使用量が1分おきにしきい値を超えたか どうかを確認します。

- 統計: データがしきい値を超えているかどうかを判断するための方法を設定します。 統計で
  は、平均値、最大値、最小値、合計値を設定できます。
  - 平均: 統計期間内の測定データの平均値統計結果は、15 分以内に収集されたすべての測 定データの平均です。80%以上の平均値は、しきい値が超えたと見なされます。
  - 最大:統計期間内の測定データの最大値期間内に収集された測定データの最大値が80% を超えると、その値はしきい値を超えます。
  - 最小: 統計期間内の測定データの最小値 期間内に収集された測定データの最小値が 80% を超えると、その値はしきい値を超えます。
  - 合計:統計期間内の測定データの合計期間内に収集された測定データの合計が80%を超えると、しきい値を超えています。上記の統計はトラフィックベースインジケーターに必要です。
- しきい値を数回超えた後にアラートをトリガー: これは、測定値が連続した期間にしきい値 を超えたときにトリガーされるアラートを指します。

たとえば、5分以内に CPU 使用率が80% を超え しきい値を3回超えるとアラートが発生 するようにに設定できます。 CPU 使用率が初めて 80% を超えたことが判明した場合、ア ラートは発生しません。 次の 5 分間でCPU 使用率が再び 80% を超えた場合 それでもア ラートは発生しません。 n アラートは、CPU 使用率が 3 回目に 80% を超えた場合にのみ 報告されます。 つまり、実際のデータが最初にしきい値を超えてからアラートポリシーが トリガーされるまでの間に消費される最小時間は、次のとおりです。期間\* (連続検出回数-1) = 5 \* = 10 分

- ・アラームルールの設定
  - 1. Cloud Monitor コンソールにログインします。
  - [クラウドサービスモニタリング] の [API ゲートウェイ] インスタンスリストへ移動します。
  - プロダクトインスタンスリストのインスタンス名をクリックするか、または [アクションの [アラームルール] をクリックし、インスタンスモニタリング詳細ページへアクセスします。
  - アラートポリシーページの右上にある [アラームルールを作成] をクリックし、入力したパ ラメーターに基づいてアラートポリシーを作成します。

# 5.18 DDoS 高セキュリティ IP

DDoS の高いアンチ IP 発信帯域幅モニタを提供することによるクラウドモニタリングは、DDoS の高いセキュリティ IP 使用状況のモニタリングを助け、モニタリング項目にアラームルールを設 定することを可能にします。 DDoS 高セキュリティ IP を購入した後、クラウドモニタリングは 上記のモニタリング項目のデータを自動的に収集します。

### モニタリングサービス

・モニタリング項目

モニタリング項目	ディメンション	単位	最小モニター粒度
ネットワーク帯域幅	インスタンスディメ ンション、IP ディメ ンション	ビット/秒	30 秒

- モニターデータは最大 31 日間保存されます。
- モニタリングデータは最大14日間分連続して表示できます。
- ・モニタリングデータの表示
  - 1. クラウドモニタリングコンソールにログインします。
  - 2. クラウドサービスがモニターする DDoS 高セキュリティ IP のインスタンスの一覧へアクセ スします。
  - 操作内のインスタンス名または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 タリングの詳細ページに移動し、メトリックを表示します。
  - ページ上部の時間範囲をクリックしてボタンを選択する、または正確な機能を選択する
    と、最大モニタリングデータを使用して14日間連続してモニタリングデータを表示できます。
  - 5. モニターの拡大画像を表示するには、モニター MAP の右上隅にあるズームボタンをク リックします。

- ・パラメーターの説明
  - モニタリング: DDos 高セキュリティ IP サービスによって提供されるモニタリングメト リック
  - 統計サイクル: アラームシステムではこのサイクルでアラームしきい値を超えるモニタリン グデータを確認します。たとえば、メモリ使用量アラームルールを設定する場合、統計サ イクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかどうかを確認しま す。
  - 連続回数: アラームを発生させるためにしきい値を超え続けている統計サイクルモニタリン グ項目の連続回数を指します。
- ・単一アラームルールの設定
  - 1. クラウドモニタリングコンソールにログインします。
  - 2. クラウドサービスがモニターする DDoS 高セキュリティ IP のインスタンスの一覧へアクセ スします。
  - インスタンス名、または稼働中のモニターチャートをクリックして、インスタンスモニタ リングの詳細ページへアクセスします。モニターチャートの右上隅にあるベルボタンまた はページの右上隅にある新しいアラームルールをクリックすると、このインスタンスに対 応するモニタリング項目にアラームルールを設定できます。

## 5.19ダイレクトメールモニタリング

CloudMonitor は、ダイレクトメールのサービスステータスをリアルタイムでモニターし、モ ニタリングメトリックにアラームルールを設定するために、WEB/API メッセージング、SMTP メッセージング、アカウント例外を含むダイレクトメールのモニタリングメトリックを提供しま す。ダイレクトメールサービスを購入して使用した後、CloudMonitor は自動的に上記のモニ タリングメトリクスに関する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	単位	最小モニター粒度
Web/API エラー - QPS 遅延	カウント/分	1分
Web/API の割り当て超過 QPS	カウント/分	1分
Web/API エラースパム QPS	カウント/分	1分

Document Version20190514

メトリック	単位	最小モニター粒度
Web/API メッセージ成功 QPS	カウント/分	1分
SMTP 認証に失敗した QPS	カウント/分	1分
SMTP 認証が成功した QPS	カウント/分	1分
QPS を超えた SMTP エラー 長	カウント/分	1分
SMTP 割り当て超過 QPS	カウント/分	1分
SMTP エラースパム QPS	カウント/分	1分

# 🗎 注:

- モニターデータは最大 31 日間保存されます。
- モニタリングデータを最大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. [Cloud Service モニタリング] の [ダイレクトメールのモニタリング] ヘアクセスし、ダイ レクトメールサービスのモニタリング情報を表示します。

### アラームサービス

CloudMonitor はダイレクトメールモニタリングメトリックスのためのアラーム機能を提供しま す。

- アラームルールを設定します。
- 1. CloudMonitor コンソールにログインします。
- 2. [Cloud Service モニタリング] の [ダイレクトメールのモニタリング] ヘアクセスします。
- 3. [アラームルール] リストページに移動するには、[アラームルール] をクリックします。右上の [アラームルールの作成] をクリックして、アラームルールを作成します。

または、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の右上隅にある新 しいアラームルールをクリックして、このインスタンスの対応するモニタリングメトリックに アラームルールを設定します。

# 5.20 Elasticsearch モニタリング

CloudMonitor を使用すると、Elasticsearch のクラスターステータス、クラスタークエリQPS 、クラスター書き込みQPSなどのモニタリングメトリックを収集することによって Elasticsea rch サービスの使用状況をモニターできます。メトリックをモニターするためのアラームルール を設定することもできます。Elasticsearch を購入した後、CloudMonitor は自動的に上記の モニタリングメトリックスに関するデータを収集します。

### モニタリングサービス

モニタリングメト リックス	分析コード	ユニット	最小モニタリング細 分性
クラスタステータス	クラスター		1分
クラスタクエリ 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 CPU 使用率	ノード	%	1分
ノードディスク使用 量	ノード	%	1分
ノードヒープメモリ 使用量	ノード	%	1分
ノード: load_1m	ノード		1分
ノードフル GC 時間	ノード	カウント	1分
ノード例外時間	ノード	カウント	1分
クラスタスナップ ショットのステータ ス	クラスター	[-1] はスナップショッ トがないことを示し ます。[0] は成功を示 します。[1] は進行中 を示します。[2] は失 敗を示します。	1分

・モニタリングメトリックス



- モニタリングデータは最大 31 日間保存されます。

- 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. [クラウドサービスモニタリング] の [Elasticsearch] インスタンスリストへ移動します。
- 3. インスタンス名、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、インス タンスモニタリング詳細ページへアクセスし、さまざまなメトリックスを表示します。
- ページ上部にある [時間範囲] ショートカットをクリックする、または特定の選択機能を使用します。 最大 14 日間連続したメトリック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] をクリックしてチャートを拡大しま す。

#### アラームサービス

- ・パラメーターの説明
  - "モニタリングメトリックス": Elasticsearch サービスによって提供されるモニタリングメ トリックス
  - "統計サイクル": アラームシステムは、サイクルに基づいて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確認します。たとえば、メモリ使用量に関するアラームルールの統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値を超えたかどうかを確認します。
  - "連続時間": モニタリングメトリックの値が設定された連続サイクルの間、しきい値を継続 的に超えたときにアラームがトリガーされます。
- ・アラームルールの設定
  - 1. クラウドモニタリング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 [Elasticsearch] インスタンスリストへ移動します。
  - 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、インスタンスモニタリング詳細ージへアクセスします。
  - モニタリングチャートの右上にあるベルアイコン、または、ページの右上隅にある [新しい アラームルール] をクリックして、インスタンスの対応するモニタリングメトリックのア ラームルールを設定します。

# 5.21 Auto Scaling

CloudMonitor は、Auto Scaling グループ内のインスタンスの最小数と最大数など、複数のメ トリックスをモニターします。 これは、Auto Scaling グループ内のインスタンスのステータス をモニターし、メトリックに対するアラートポリシーを設定するのに役立ちます。 Auto Scaling サービスを購入すると、CloudMonitor は自動的に上記のメトリクスに関するデータを収集します。

## モニタリングサービス

・モニタリング項目

モニタリング項目	分析コード	ユニット	最小モニター細分性
最小インスタンス数	ユーザーディメン ション、elastic scaling グループ	項目	5分
最大インスタンス数	ユーザーディメン ション、elastic scaling グループ	項目	5分
インスタンスの合計 数	ユーザーディメン ション、elastic scaling グループ	項目	5分
実行中のインスタン ス数	ユーザーディメン ション、elastic scaling グループ	項目	5分
ジョイニングインス タンス番号	ユーザーディメン ション、elastic scaling グループ	項目	5分
インスタンス数の削 除	ユーザーディメン ション、elastic scaling グループ	項目	5分

🧾 注:

- モニターデータは最大 31 日間保存されます。
- モニタリングデータを最大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. クラウドモニタリング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] にある[自動スケーリング]の [Auto sclaing] グループリ ストに移動します。
- 稼働中のインスタンス名または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 タリングの詳細ページに移動し、メトリックを表示します。
- 4. ページ上部の時間範囲クイック選択ボタンまたは完全選択機能をクリックすると、最大モ ニタリングデータでは14日間連続してモニタリングデータを確認できます。
- 5. モニター MAP の右上隅にあるズームインボタンをクリックすると、拡大表示します。

#### アラームサービス

・パラメーターの説明

- メトリクス: Auto scaling サービスによって提供されるモニタリングインデックス
- 統計サイクル: アラームシステムは、モニタリングデータがこのサイクルのアラームしきい 値を超えているかどうかを確認します。たとえば、メモリ使用量アラームルールを設定す る場合、統計サイクルは1分です。1分間隔でメモリ使用量がしきい値を超えているかど うかを確認します。
- 統計方法:統計方法は、しきい値範囲を超える設定を指します。統計方法で平均、最大、最小、カウント、および値を設定できます。
  - 平均: 統計サイクル中に監視されたデータの平均 たとえば、統計方法では、15 分以内に 収集されたすべてのモニタリングデータの平均が 80% を超える場合、その平均を選択 し、しきい値を超えたと見なされます。
  - 最大: 統計サイクル中のモニターデータの最大値 たとえば、統計結果が 15 分以内に収 集されたすべてのメトリックデータの最大値である場合、80% を超える平均値がしきい 値を超えたと見なされます。 しきい値を超えたと見なされます。
  - 最小:統計サイクル中のモニター対象データの最小値 たとえば、統計結果が 15 分以内 に収集されたすべてのメトリックデータの最小値である場合、80% を超える平均値がし きい値を超えたと見なされます。しきい値を超えたと見なされます。
  - 値: 統計サイクル中のモニタリングデータの合計 たとえば、統計方法では、値が 80% を超える場合、15 分以内に収集されたすべてのモニタリングデータの要件と値が選択さ

れます。 しきい値を超えたと見なされます。 このような統計的方法はトラフィッククラ スメトリクスに必要です。

- 連続回数: アラームを発生させるためにしきい値を超え続けている統計サイクルモニタリン グ項目の連続回数を指します。

例: CPU 使用率を 80% 以上、統計サイクルを 5 分に設定し、3回連続 しきい値を超えた ときに発生するアラームに設定し、検出 CPU 使用率が初めて 80% を超えたとき、アラー ム通知は発行されません。 5 分以内に 2 回目に CPU 使用率が 80% を超えた場合、アラー ム通知は発行されません。 3 回目に 80% を超えた場合のみ、 アラーム通知が発行されま す。 つまり、実際のデータが最初にしきい値を超えてから最後のアラームルールまでに必 要な最小時間は、統計サイクルX (連続プローブ数-1) = 5 x (3-1) = 10 分です。

- ・単一アラームルールの設定
  - 1. クラウドモニタリングコンソールにログインします。
  - [クラウドサービスモニタリング] にある [自動スケーリング] の自動スケーリンググループ リストに移動します。
  - 3. 稼働中のインスタンス名または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 タリングの詳細ページに移動します。
  - モニターチャートの右上隅にあるベルボタンまたはページの右上隅にある新しいアラーム ルールをクリックすると、このインスタンスに対応するモニタリング項目にアラームルー ルを設定できます。
- 一括アラームルールの設定
  - 1. クラウドモニタリングコンソールにログインします。
  - 2. クラウドサービスによってモニターされている Elastic Scale モニタリングインスタンスの リストを入力します。
  - 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。次に、ページ下部の[ア ラートポリシー]をクリックして、複数のアラートポリシーを追加します。

## 5.22 E-MapReduce モニタリング

CloudMonitor は、クラスターの動作をモニターしやすくするために、CPU のアイドル状態、 メモリ容量、ディスク容量など、E-MapReduce クラスターの複数のモニタリングメトリック を提供します。 これらのモニタリングメトリックのためのアラームルールを設定できます。 E-MapReduce サービスを購入後 CloudMonitor は、前述のモニタリングメトリックスのデータ を自動収集します。

### モニタリングサービス

### ・メトリックス

メトリック	ディメンション	単位	最小モニタリング細 分性
受信トラフィック レート	ユーザー、クラス ター、およびロール	ビット/秒	30 秒
発信ネットワーク レートネットワーク ドレインレート	ユーザー、クラス ター、およびロール	ビット/秒	30 秒
CPU のアイドル状態	ユーザー、クラス ター、およびロール	%	1分
ユーザーモードの CPU 使用率	ユーザー、クラス ター、およびロール	%	30 秒
システムモードの CPU 使用率	ユーザー、クラス ター、およびロール	%	30 秒
アイドルディスク容 量	ユーザー、クラス ター、およびロール	バイト	30 秒
総ディスク容量	ユーザー、クラス ター、およびロール	バイト	30 秒
15 分以内の平均負荷	ユーザー、クラス ター、およびロール	-	30 秒
5 分以内の平均負荷	ユーザー、クラス ター、およびロール	-	30 秒
1 分以内の平均負荷	ユーザー、クラス ター、およびロール	-	30 秒
アイドルメモリ容量	ユーザー、クラス ター、およびロール	バイト	30 秒
総メモリ容量	ユーザー、クラス ター、およびロール	バイト	30 秒
受信データパケット レート	ユーザー、クラス ター、およびロール	パケット	30 秒
送信データパケット レート	ユーザー、クラス ター、およびロール	パケット/秒	30 秒
実行中プロセス数	ユーザー、クラス ター、およびロール	プロセス	30 秒

メトリック	ディメンション	単位	最小モニタリング細 分性	
総プロセス数	ユーザー、クラス ター、およびロール	プロセス	30 秒	
ブロックされたプロ セス数	ユーザー、クラス ター、およびロール	プロセス	30 秒	
作成したプロセス/ス レッド数	ユーザー、クラス ター、およびロール	プロセス/スレッド	30 秒	
MemNonHeap UsedM	ユーザー、クラス ター、およびロール	バイト	30秒	
MemNonHeap CommittedM	ユーザー、クラス ター、およびロール	バイト	30秒	
Memnonheap maxm	ユーザー、クラス ター、およびロール	バイト	30 秒	
MemHeapUsedM	ユーザー、クラス ター、およびロール	バイト	30 秒	
MemHeapCom mittedM	ユーザー、クラス ター、およびロール	バイト	30 秒	
МетНеарМахМ	ユーザー、クラス ター、およびロール	バイト	30秒	
MemMaxM	ユーザー、クラス ター、およびロール	バイト	30 秒	
Threadsnew	ユーザー、クラス ター、およびロール	-	30 秒	
ThreadsRunnable	ユーザー、クラス ター、およびロール	-	30 秒	
ThreadsBlocked	ユーザー、クラス ター、およびロール	-	30 秒	
ThreadsWaiting	ユーザー、クラス ター、およびロール	-	30 秒	
ThreadsTim edWaiting	ユーザー、クラス ター、およびロール	-	30 秒	
ThreadsTer minated	ユーザー、クラス ター、およびロール	-	30 秒	
GcCount	ユーザー、クラス ター、およびロール	-	30 秒	

メトリック	ディメンション	単位	最小モニタリング細
	, , , , , , , , , , , , , , , , , , , ,		分性
GcTimeMillis	ユーザー、クラス ター、およびロール	-	30 秒
CallQueueLength	ユーザー、クラス ター、およびロール	-	30 秒
NumOpenCon nections	ユーザー、クラス ター、およびロール	-	30 秒
ReceivedBytes	ユーザー、クラス ター、およびロール	-	30 秒
SentBytes	ユーザー、クラス ター、およびロール	-	30 秒
BlockCapacity	ユーザー、クラス ター、およびロール	-	30 秒
BlocksTotal	ユーザー、クラス ター、およびロール	-	30 秒
CapacityRe maining	ユーザー、クラス ター、およびロール	-	30 秒
CapacityTotal	ユーザー、クラス ター、およびロール	-	30 秒
CapacityUsed	ユーザー、クラス ター、およびロール	-	30 秒
CapacityUs edNonDFS	ユーザー、クラス ター、およびロール	-	30 秒
CorruptBlocks	ユーザー、クラス ター、およびロール	-	30 秒
ExcessBlocks	ユーザー、クラス ター、およびロール	-	30 秒
ExpiredHeartbeats	ユーザー、クラス ター、およびロール	-	30 秒
MissingBlocks	ユーザー、クラス ター、およびロール	-	30 秒
PendingDat aNodeMessa geCount	ユーザー、クラス ター、およびロール	-	30 秒

メトリック	ディメンション	単位	最小モニタリング細 分性
PendingDel etionBlocks	ユーザー、クラス ター、およびロール	-	30秒
PendingRep licationBlocks	ユーザー、クラス ター、およびロール	-	30 秒
PostponedM isreplicatedBlocks	ユーザー、クラス ター、およびロール	-	30 秒
ScheduledR eplicationBlocks	ユーザー、クラス ター、およびロール	-	30 秒
TotalFiles	ユーザー、クラス ター、およびロール	-	30 秒
TotalLoad	ユーザー、クラス ター、およびロール	-	30 秒
UnderRepli catedBlocks	ユーザー、クラス ター、およびロール	-	30 秒
BlocksRead	ユーザー、クラス ター、およびロール	-	30 秒
BlocksRemoved	ユーザー、クラス ター、およびロール	-	30 秒
BlocksReplicated	ユーザー、クラス ター、およびロール	-	30 秒
BlocksUncached	ユーザー、クラス ター、およびロール	-	30 秒
BlocksVerified	ユーザー、クラス ター、およびロール	-	30 秒
BlockVerif icationFailures	ユーザー、クラス ター、およびロール	-	30 秒
BlocksWritten	ユーザー、クラス ター、およびロール	-	30 秒
BytesRead	ユーザー、クラス ター、およびロール	-	30 秒
BytesWritten	ユーザー、クラス ター、およびロール	-	30 秒
FlushNanos AvgTime	ユーザー、クラス ター、およびロール	-	30 秒

メトリック	ディメンション	単位	最小モニタリング細 分性
FlushNanos NumOps	ユーザー、クラス ター、およびロール	-	30 秒
FsyncCount	ユーザー、クラス ター、およびロール	-	30 秒
VolumeFailures	ユーザー、クラス ター、およびロール	-	30 秒
ReadBlockO pNumOps	ユーザー、クラス ター、およびロール	-	30 秒
ReadBlockO pAvgTime	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
WriteBlock OpNumOps	ユーザー、クラス ター、およびロール	-	30 秒
WriteBlock OpAvgTime	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
BlockCheck sumOpNumOps	ユーザー、クラス ター、およびロール	-	30 秒
BlockCheck sumOpAvgTime	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
CopyBlockO pNumOps	ユーザー、クラス ター、およびロール	-	30 秒
CopyBlockO pAvgTime	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
ReplaceBlo ckOpNumOps	ユーザー、クラス ター、およびロール	-	30 秒
ReplaceBlo ckOpNumOps	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
BlockRepor tsNumOps	ユーザー、クラス ター、およびロール	-	30 秒
BlockRepor tsAvgTime	ユーザー、クラス ター、およびロール	ミリ秒	30 秒
NodeManage r_Allocate dContainers	ユーザー、クラス ター、およびロール	-	30 秒

メトリック	ディメンション	単位	最小モニタリング細 分性
Containers Completed	ユーザー、クラス ター、およびロール	-	30 秒
ContainersFailed	ユーザー、クラス ター、およびロール	-	30 秒
ContainersIniting	ユーザー、クラス ター、およびロール	-	30 秒
ContainersKilled	ユーザー、クラス ター、およびロール	-	30 秒
Containers Launched	ユーザー、クラス ター、およびロール	-	30 秒
Containers Running	ユーザー、クラス ター、およびロール	-	30 秒
ActiveApplications	ユーザー、クラス ター、およびロール	-	30 秒
ActiveUsers	ユーザー、クラス ター、およびロール	-	30 秒
AggregateC ontainersAllocated	ユーザー、クラス ター、およびロール	-	30 秒
AggregateC ontainersReleased	ユーザー、クラス ター、およびロール	-	30 秒
AllocatedC ontainers	ユーザー、クラス ター、およびロール	-	30 秒
AppsCompleted	ユーザー、クラス ター、およびロール	-	30 秒
AppsFailed	ユーザー、クラス ター、およびロール	-	30 秒
AppsKilled	ユーザー、クラス ター、およびロール	-	30 秒
AppsPending	ユーザー、クラス ター、およびロール	-	30 秒
AppsRunning	ユーザー、クラス ター、およびロール	-	30 秒
AppsSubmitted	ユーザー、クラス ター、およびロール	-	30 秒

メトリック	ディメンション	単位	最小モニタリング細 分性
AvailableMB	ユーザー、クラス ター、およびロール	-	30 秒
AvailableVCores	ユーザー、クラス ター、およびロール	-	30 秒
PendingContainers	ユーザー、クラス ター、およびロール	-	30 秒
ReservedCo ntainers	ユーザー、クラス ター、およびロール	-	30 秒

# 📃 注:

- モニタリングデータは最大 31 日間保存されます。
- 最大14日間連続してモニタリングデータを表示できます。
- ・モニタリングデータの表示
  - 1. クラウドモニタリングコンソール にログインします。
  - 2. [クラウドサービスモニタリング] の[E-MapReduce] インスタンスリストへ移動します。
  - 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の詳細ページにアクセスし、さまざまなメトリッ クを表示します。
  - ページ上部の [時間範囲] クイック選択ボタンをクリックするか、特定の選択機能を使用し 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. モニタリングチャートの右上隅にある [ズームイン] ボタンをクリックしてチャートを拡大 します。

#### アラームサービス

- ・パラメーターの説明
  - モニタリングメトリック: E-MapReduce サービスによって提供されるモニタリングメト リックス
  - 統計サイクル: アラームシステムは、サイクルに基づいて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確認します。たとえば、メモリ使用量に関するアラームルール

の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。

- 統計方法: データがしきい値を超えているかどうかを決定するために使用される方法を指し
   ます。統計方法としては、平均値、最大値、最小値、合計値を設定できます。
  - 平均: 統計期間内のメトリックデータの平均値 たとえば、15 分以内に収集されたすべてのモニタリングデータの平均値が統計方法として採用されている場合、80% を超える平均値がしきい値を超えていると見なされます。
  - 2. 最大: 統計期間内のメトリックデータの最大値 たとえば、15 分以内に収集されたすべてのモニタリングデータの最大値が統計方法として採用されている場合、80% を超える最大値がしきい値を超えると見なされます。
  - 3. 最小: 統計期間内のメトリックデータの最小値 たとえば、15 分以内に収集されたすべてのモニタリングデータの最小値が統計方法として採用されている場合、80% を超える最小値がしきい値を超えていると見なされます。
  - 4. 合計: 統計期間内のメトリックデータの合計 たとえば、15 分以内に収集されたすべての モニタリングデータの合計値が統計的方法として採用されている場合、80% を超える合 計値がしきい値を超えていると見なされます。上記の統計方法は、トラフィックベース のインデックスに必要です。
- 連続時間: 監視メトリックの値が設定された連続サイクルの間、しきい値を継続的に超えた
   ときにアラームがトリガーされます。

例: CPU 使用率が 80 %以上、統計サイクルを 5 分に設定し、3 回連続で しきい値を超え た場合、アラームが発生するように設定します。検出 CPU 使用率が初めて 80% を超えた 場合、アラーム通知は発行されません。 5 分以内に 2 回目の CPU 使用率が 80% を超えた ことが検出された場合、アラーム通知は発行されません。 3 回目に 80% を超えた場合の み、アラーム通知が発行されます。 したがって、実際のデータが初めてしきい値を超えて からアラームルールがトリガーされるまでの間に消費される最小時間は次のとおりです。 統計サイクル\*(連続検出数 - 1) = 5\*(3-1) = 10 分です。 ・アラームルールの設定

- 1. クラウドモニタリング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 [E-MapReduce] インスタンスリストへ移動します。
- 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の詳細ページにアクセスします。
- モニタリングチャートの右上隅にあるベルボタンまたはページの右上隅にある [新しいア ラームルール] をクリックして、このインスタンスの対応するモニタリングメトリックにア ラームルールを設定します。

# 5.23 Express Connect のモニタリング

CloudMonitorは、Express Connect インスタンスのインバウンドおよびアウトバウンドネッ トワークトラフィックなど、複数のメトリックスをモニターします。 インスタンスのネット ワーク使用率をモニターし、さまざまなメトリクスに対してアラームルールを設定できます。 Express Connect サービスを購入すると、CloudMonitor は自動的に次のメトリクスのデータ を収集します。

### モニタリングサービス

モニタリング項目	ディメンション	単位	最小モニタリング細 分性
受信ネットワークト ラフィック	ユーザーとインスタ ンス	バイト	1分
送信ネットワークト ラフィック	ユーザーとインスタ ンス	バイト	1分
受信ネットワーク帯 域幅	ユーザーとインスタ ンス	ビット/秒	1分
送信ネットワーク帯 域幅	ユーザーとインスタ ンス	ビット/秒	1分
レイテンシ	ユーザーとインスタ ンス	ミリ秒	1分
パケット損失率	ユーザーとインスタ ンス	%	1分

・モニタリング項目



- モニタリングデータは最大 31 日間保存されます。
- 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. [クラウドサービスモニタリング] にある [Express Connect] の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、メトリックスを表示し ます。
  - 4. ページ上部にある [時間範囲] ショートカットをクリックする、または特定の選択機能を使用します。 最大 14 日間連続したメトリックデータを表示できます。
  - 5. 拡大表示するには、モニタリングチャートの右上隅にある [ズームイン] ボタンをクリック します。

アラームサービス

- ・パラメーターの説明
  - メトリック: Express Connect サービスによって提供されるメトリック項目
  - 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ているか
     どうかをチェックする頻度を示します。たとえば、メモリ使用量に関するアラームルール

の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。

- 統計方法: データがしきい値を超えているかどうかを判断します。統計方法では、平均、最
   大、最小、合計を設定できます。
  - 平均値: 統計サイクル内のモニタリングデータの平均値 たとえば、15分以内に収集されたすべてのモニタリングデータの平均値が統計方法として使用される場合、80%を超える平均値は、しきい値を超えたと見なされます。
  - ■最大値:統計周期内の監視データの最大値たとえば、15分以内に収集されたすべてのモニタリングデータの最大値が統計方法として使用されている場合、80%を超える最大値は、しきい値を超えたと見なされます。
  - 最小値: 統計サイクル内のモニタリングデータの最小値 たとえば、15 分以内に収集されたすべてのモニタリングデータの最小値が統計方法として使用される場合、80%を超える最小値は、しきい値を超えたと見なされます。
  - 合計値:統計サイクル内のモニタリングデータの合計 たとえば、15分以内に収集された すべてのモニタリングデータの合計値が統計方法として使用されている場合、80%を超 える合計値は、しきい値を超えたと見なされます。この方法はトラフィックメトリック に必要です。
- 連続回数: モニタリングメトリックの値が、設定された連続サイクルの間、しきい値を継続 的に超えると、アラームがトリガーされます。

たとえば、3 回連続して 5分間の統計サイクル内で CPU 使用率が しきい値の 80% を超え るとアラームが発生するように設定したとします。 つまり、CPU 使用率が初めて80% を 超えたことが判明してもアラームは発生しません。 5 分後に再度 CPU使用率が 80% を超 過してもアラームは発生しません。 3 回目の検出で、CPU 使用率が 80% を超えると ア ラームがトリガーされます。 したがって、実際のデータが最初にしきい値を超えてからア ラームルールがトリガーされるまでの間に消費される最小時間は次のとおりです。統計サ イクルx (連続検出数 - 1)、つまり 5 x (3 - この場合、1) = 10 分。

- ・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] にある [Express Connect] の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、メトリックスを表示し ます。
  - モニタリングチャートの右上隅にある [ベル] ボタン、またはページの右上隅にある [新しい アラームルール] をクリックして、このインスタンスに対応するモニタリングメトリックス 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] にある [Express Connect] のインスタンスリストへ移動 します。
  - 3. インスタンスリストページでインスタンスを選択します。 [アラームルールの設定] をク リックして複数のアラームルールを追加します。

# 5.24 Function Compute モニタリング

CloudMonitor では、TotalInvocations、平均 期間、要求ステータス分散を含む、サービス および機能レベルでの Function Compute のモニタリングメトリックスを提供し、 Function Compute のサービススタータスをリアルタイムでモニターし、モニタリングメトリックスの アラームルールを設定することができます。 Function Compute サービスを購入して使用した 後、CloudMonitor は自動的に上記のメトリックスを収集します。

### モニタリングサービス

・メトリックス

メトリック	ディメンション	単位	最小モニター粒度
Billableinvocation	ユーザー、サービ ス、および機能	集計	1分
BillableIn vocationsRate	ユーザー、サービ ス、および機能	パーセント	1分
ClientErrors	ユーザー、サービ ス、および機能	集計	1分

メトリック	ディメンション	単位	最小モニター粒度
ClientErrorsRate	ユーザー、サービ ス、および機能	パーセント	1分
ServerErrors	ユーザー、サービ ス、および機能	集計	1分
ServerErrorsRate	ユーザー、サービ ス、および機能	パーセント	1分
Throttles	ユーザー、サービ ス、および機能	集計	1分
ThrottlesRate	ユーザー、サービ ス、および機能	パーセント	1分
Totalinvocations	ユーザー、サービ ス、および機能	集計	1分
平均期間	ユーザー、サービ ス、および機能	ミリ秒	1分

\_\_\_\_\_注:

- モニタリングデータは最大 31 日間保存されます。
- 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。
  - [クラウドサービスモニタリング] の Function Compute モニタリングページへ移動
     し、[Function Compute] サービスの全体的なモニタリングデータを表示します。
  - 3. [サービス一覧] をクリックして、サービスまたは Function レベルでモニタリング情報を 表示します。

### アラームサービス

CloudMonitor は Function Compute モニタリングメトリックス用のアラーム機能を提供して いるため、メトリックス例外が発生した場合には直ちに通知されます。

アラームルールを設定します。

### ・ 方法 1

- 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 [Function Compute モニタリング] ページへ移動します。
- 3. [サービスまたは機能] リストで、[アクション] 列の [モニタリングチャート] をクリックして、モニタリングの詳細ページにアクセスします。
- モニタリングチャートの右上にあるベルのアイコンまたは、ページの右上隅にある [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モニタリングメトリックのア ラームルールを設定します。

・ 方法 2

- 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 [Function Compute モニタリング] ページへ移動します。
- 3. [アラームのルール] をクリックし、[アラームルール] の一覧ページへ移動します。右上隅 にある [作成] をクリックしアラームルールを作成します。

# 5.25 StreamCompute

サービスレイテンシ、フェイルオーバーレート、読み書き RPS メトリックスなどをモニターする ことで、CloudMonitor はご利用中の StreamCompute サービスの全体的なパフォーマンスの 把握に役立ち、それに応じたアラームルールを設定できます。CloudMonitor は本プロダクト の利用を開始した時から、StreamCompute から自動的にデータを収集します。

## モニタリングサービス

・メトリックス

メトリック	ディメンション	単位	説明	最小モニタリン グ頻度
サービスレイテ ンシ	プロジェクト、 ジョブ	秒	現在のジョブの データプロセス レイテンシ	1分
読み取り RPS	プロジェクト、 ジョブ	読み取り/秒	タスクで1秒あ たりに読み取る データラインの 平均数	1分

メトリック	ディメンション	単位	説明	最小モニタリン グ頻度
書き込み RPS	プロジェクト、 ジョブ	書き込み/秒	タスクで1秒あ たりに書き込む データラインの 平均数	1分
フェイルオー バーレート	プロジェクト、 ジョブ	%	現在のジョブ のフェイルオー バー頻度の合計	1分

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] にある [StreamCompute] インスタンスリストへ移動します。
  - 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、さまざまなメトリック スを表示します。
  - ページの上部メニューにある [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います。 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。
  - 5. モニタリングチャートの右上隅にある [ズームイン] 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

- メトリックス: StreamCompute から取得されるモニタリングメトリックス
- 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ているか どうかをチェックする頻度を示します。たとえば、メモリ使用量に関するアラームルール の統計周期が1分に設定されている場合、システムはメモリ使用量が1分おきにしきい値 を超えたかどうかを確認します。
- 統計方法:計算方法とその結果値を使ってデータがアラームルールで指定されたしきい値を 超えたかどうかを判断します。統計方法では、平均、最大、最小、合計を設定できます。

たとえば、15分間の統計期間中に、メモリ使用量などのメトリックの 80% の平均を、ア ラームがトリガーされるしきい値として指定できます。

- 平均値: 統計サイクル内のモニタリングデータの平均値 たとえば、15分以内に収集されたすべてのモニタリングデータの平均値が統計方法として採用されている場合、80%を超える平均値がしきい値を超えていると見なされます。
- 最大値: 統計サイクル内のモニタリングデータの最大値 たとえば、15 分以内に収集されたすべてのモニタリングデータの最大値が統計方法として採用されている場合、80%を超える最大値がしきい値を超えると見なされます。
- 最小値: 統計サイクル内のモニタリングデータの最小値 たとえば、15 分以内に収集されたすべてのモニタリングデータの最小値が統計方法として採用されている場合、80%を超える最小値がしきい値を超えていると見なされます。
- 合計値:統計サイクル内のモニタリングデータの合計 たとえば、15 分以内に収集された すべてのモニタリングデータの合計値が統計方法として採用されている場合、80% を超 える合計値がしきい値を超えていると見なされます。この方法はトラフィックメトリッ クに必要です。
- 連続回数:メトリック値が、設定された連続サイクルの間、しきい値を継続的に超えると、 アラームがトリガーされます。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。

たとえば、CPU 使用率が 3 回連続して 5 分間の統計サイクルでしきい値の 80% を超える とアラームが発生するように設定したとします。 つまり、CPU 使用率が初めて 80% を超 えたことが判明してもアラームは発生しません。 5 分後の2 回目の検出で CPU 使用率が再 び 80% を超えた場合も、アラームは発生しません。 3 回目の検出で CPU 使用率が再び 80% を超えると、アラームがトリガーされます。 したがって、実際のデータが最初にしき い値を超えてからアラームルールがトリガーされるまでの間に消費される最小時間は次の とおりです。統計的サイクル (連続検出数-1)、つまり 5 (3 - 1) = 10 分です。

- ・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] にある [StreamCompute] 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。
  - モニタリングチャートの右上隅にある [ベル] 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、このインスタンスに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] にある [StreamCompute] インスタンスリストへ移動します。
  - 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。 [アラームルールの設定] をクリックして複数のアラームルールを追加します。

# 5.26 ApsaraDB for HybridDB

クラウドモニタリングは、HybridDBの CPU 使用量、メモリー使用量などをモニターすること により、ユーザーが hybriddb インスタンスの使用量をモニターするのを助け、モニタリング項 目にアラームルールを設定することを可能にします。 hybriddb を購入後、クラウドモニタリン グは上記のモニタリング項目のデータを自動的に収集します。

#### モニター

モニタリング項目	ディメンション	単位	最小モニター粒度
ディスクの使用状況	ユーザーとインスタ ンス	%	5分
接続の使い方	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
メモリ使用量	ユーザーとインスタ ンス	%	5分

・モニタリング項目

モニタリング項目	ディメンション	単位	最小モニター粒度
I/O スループット使用 量	ユーザーとインスタ ンス	%	5分

# 🗎 注:

- モニターデータは最大 31 日間保存されます。

- ユーザーはモニタリングデータを最大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. クラウドモニタリングコンソール ヘログインします。
  - 2. Cloud Service Monitoring の HybridDB インスタンスリストに移動します。
  - 3. インスタンス名またはアクションの [モニタリングチャート] をクリックし、インスタンス モニタリング情報ページへアクセスし、さまざまなメトリックを表示します。
  - ページ上部の [時間範囲クイック選択] ボタンまたは完全選択機能をクリックします。最大 モニタリングデータサポートビューは連続 14 日間のモニタリングデータです。
  - 5. モニター MAP の右上角にあるズームインボタンをクリックして、モニターの大きい画像を 表示します。

### アラームサービス

# 5.27 NAT ゲートウェイ

SNAT 接続や帯域幅パッケージデータを含む NAT ゲートウェイからの複数のメトリックスをモ ニターすることで、CloudMonitor は、ご利用中の NAT ゲートウェイサービスの全体的なネッ トワーク使用量やパフォーマンスを理解することに役立ち、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、NAT ゲートウェイか ら自動的にデータを収集します。

### モニタリングサービス

・メトリックス

メトリック	ディメンション	単位	最小モニター頻度
SNAT 接続	ユーザーとインスタ ンス	カウント/分	1分
帯域幅 パケット (受信 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	最小モニター頻度
帯域幅 パケット (送信 帯域幅)	ユーザーとインスタ ンス	ビット/秒	1分
帯域幅 パケット (受信 パケット)	ユーザーとインスタ ンス	パケット/秒	1分
帯域幅 パケット (送信 パケット)	ユーザーとインスタ ンス	パケット/秒	1分
帯域幅 パケット数 (ア ウトバウンド帯域幅 使用量)	ユーザーとインスタ ンス	%	1分



- 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。
  - [クラウドサービスモニタリング] にある [NAT ゲートウェイ] インスタンスリストへ移動します。
  - 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、さまざまなメトリック スを表示します。
  - 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

- メトリックス: NAT ゲートウェイ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。
  - [クラウドサービスモニタリング] にある [NAT ゲートウェイ] インスタンスリストへ移動します。
  - 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ます。
  - 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。
  - [クラウドサービスモニタリング] にある [NAT ゲートウェイ] インスタンスリストへ移動します。
  - 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。 [アラームルールの設定] をクリックして複数のアラームルールを追加します。

## 5.28 Open Ad

Open Ad で取得した 12 個以上のメトリック (RTB PV、QPS など) と ad クリック PV をモニタ リングすることで、CloudMonitor では、Open Ad サービスのリアルタイム状態を管理したり 解釈したりすることができます。それにあわせてアラームルールを設定できます。このプロダク トの使用を開始した時点から、CloudMonitor は自動的に Open Ad からデータを取得します。

### 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	最小モニタリング頻 度
RTB PV	ユーザー	カウント	1分
RTB QPS	ユーザー	時間/秒	1分
Ad クリック PV	ユーザー	カウント	1分
Ad クリック QPS	ユーザー	時間/秒	1分
Ad クリック遅延	ユーザー	ミリ秒	1分
Ad 露出 PV	ユーザー	カウント	1分
Ad 露出 QPS	ユーザー	時間/秒	1分
Ad 露出遅延	ユーザー	ミリ秒	1分
DMP のアクティブク ラウドカウント	ユーザー	カウント/日	1時間
DMP有効なクラウド リクエスト	ユーザー	時間/日	1時間
DMP が利用する記憶 領域	ユーザー	バイト/日	1時間
Umeng と DIP の有 効クラウドカウント	ユーザー	カウント/日	1時間
Umeng と DIP の有 効なオーディエンス 数	ユーザー	時間/日	1時間

# 🧾 注:

- モニタリングデータは、31日間保存されます。
- 最大連続14日間分のモニタリングデータを表示できます。

・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. [クラウドサービスモニタリング] で、[Open Ad モニタリングページ] を開き、Open Ad サービスのモニタリングデータを表示します。

### アラームサービス

CloudMonitor では、Open Ad モニタリングメトリックのアラーム機能を提供します。メト リックの有効期限が切れた場合すぐに通知を行います。

アラームルールを設定します。

・ 方法 1

- 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]で、[Open Ad モニタリングページ]ヘアクセスします。
- 3. モニタリングチャートの右上隅にあるベルアイコン、またはページの右上隅にある[新しい アラームルール] をクリックし、このインスタンスに対応したメトリックのアラームルール を設定します。

・ 方法 2

- 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] で、[Open Ad モニタリングページ] ヘアクセスします。
- 3. [アラームルール] をクリックしてアラームルールの一覧ページへアクセスします。右上隅 にある [アラームルールの作成] をクリックし、アラームルールを作成します。

# 5.29 ApsaraDB for PetaData

ディスク使用量、受信および送信帯域幅、QPS といったいくつかのメトリックスをモニター することで、CloudMonitor は ApsaraDB for PetaData スケーリンググループにあるイン スタンスのステータスを理解し、それにあわせたアラームルールを設定するのに役立ちます。 CloudMonitor は 本プロダクトの利用を開始したときから、ApsaraDB for PetaData から自動 的にデータを収集します。

モニタリングサービス

・メトリックス

メトリック	ディメンション	単位	最小モニタリング頻 度
ディスクの使用状況	ユーザーとインスタ ンス	バイト	5分
受信带域幅	ユーザーとインスタ ンス	バイト/秒	5分

メトリック	ディメンション	単位	最小モニタリング頻 度
発信帯域幅	ユーザーとインスタ ンス	バイト/秒	5分
QPS	ユーザーとインスタ ンス	カウント/秒	5分

# 🧾 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] にある [ApsaraDB for PetaData] インスタンスリストへ 移動します。
  - 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、さまざまなメトリック スを表示します。
  - 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、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

- メトリックス: ApsaraDB for PetaData 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。
- 統計方法: データがアラームルールで指定されたしきい値を超えたかどうかを判断するための計算方法と結果の値です。統計方法では、平均、最大値、最小値および合計を設定で

きます。たとえば、統計的な15分の期間に、メモリ使用量などのメトリックの平均80% を、アラームをトリガーするしきい値として指定できます。

- 均値: 統計サイクル内のモニタリングデータの平均値 たとえば、15分以内に収集された すべてのモニタリングデータの平均値が統計方法として採用されている場合、80%を超 える平均値がしきい値を超えていると見なされます。
- 最大値:統計周期内の監視データの最大値 たとえば、15分以内に収集されたすべてのモニタリングデータの最大値が統計方法として採用されている場合、80%を超える最大値がしきい値を超えると見なされます。
- 最小値:統計サイクル内のモニタリングデータの最小値たとえば、15分以内に収集されたすべてのモニタリングデータの最小値が統計方法として採用されている場合、80%を超える最小値がしきい値を超えていると見なされます。
- 合計値:統計サイクル内のモニタリングデータの合計 たとえば、15 分以内に収集された すべてのモニタリングデータの合計値が統計方法として採用されている場合、80% を超 える合計値がしきい値を超えていると見なされます。この方法はトラフィックメトリッ クに必要です。
- 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。

たとえば、CPU 使用率が3回連続して5分間の統計サイクルでしきい値の80%を超える とアラームが発生するように設定したとします。5分後の2回目の検出でCPU 使用率が再 び80%を超えた場合も、アラームは発生しません。3回目の検出でCPU 使用率が再び 80%を超えると、アラームがトリガーされます。つまり、実際のデータが最初にしきい値 を超えてから最後のアラームルールまでに必要な最小時間は、統計サイクルX (連続プロー ブ数-1)=5x (3-1)=10分です。

- ・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] にある [ApsaraDB for PetaData] インスタンスリストへ 移動します。
  - 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、インスタンスモニタリング詳細ページへアクセスします。
  - モニタリングチャートの右上隅にある [ベル] 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、このインスタンスに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] にある [ApsaraDB for PetaData] インスタンスリストへ 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。 [アラームルールの設定] をクリックして複数のアラームルールを設定します。

# 6 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。

- $\cdot$  ECS
- · RDS
- · Server Load Balancer
- $\cdot$  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

# 7 アプリケーショングループ

# 7.1 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。



・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。

# 7.2 アプリケーショングループの作成

シナリオ

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、複数の Alibaba Cloud 製品からのリソースは、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できま す。アプリケーショングループを使用すると、アラームルールを簡単に管理し、これらのグルー プ化されたリソースのモニタリングデータを表示できます。



- ・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。
- 動的モードまたは静的モードを使用して、インスタンスを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ときに、自身の名前規則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に、インスタンスの名前規則を設定できます。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インスタンスを削除する場合は、これらの設定を完了するためにインスタンス名を変更するだけで済

- みます。現在、動的モードは ECS、ApsaraDB for RDS、および SLB インスタンスでサ ポートされています。
- 静的モード:静的モードでは、手動でアプリケーショングループにインスタンスを追加す る必要があります。

#### 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から、[アプリケーショングループ] をクリックします。

3. 右上隅の [グループの作成]をクリックしま

	Basic Infomation		
	<ul> <li>Product Group Name</li> </ul>		
	Enter		
	Contact Group		
	Select   Quickly of  Quickly of	create	а
	MonitorAlarm		
	Select Template		
	Please select   Go to Create	e Alarm	1
	Initialize Agent Installation ⊘		
	Event Monitor		
	Subscribe Event notification		
	After subscription event notification, alarm notification will be sent when within the group. Introduction to Cloud Products Events	seriou	5
	Add Instance dynamically		
	Dynamic rules for ECS instances		
	• Dynamic rules		
	All rules O Any rule		
	Instance created in future according with this rule would be added to	group	
	Instance Name   Contain	•	E
	+Add Rules		
rsion20	90514 139		

Add Product

- (基本情報)を入力します。グループ名を入力し、アラーム通知を受け取る連絡先グループを1 つ以上選択します。
- [モニターアラーム] を設定します。1つ以上のテンプレートを選択し、グループ内 (オプション) にあるインスタンスのアラームルールを初期化し、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、CloudMonitor エージェントはグループ内すべてのサーバーヘインストールされ、データが収集されます。
- [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、重大および警告レベルのイベントがグループ内の関連リソースで発生した場合、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] を設定します。
  - ・名前規則を設定して、名前規則に一致する 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、将来のインスタンスを含め、指定した単語を含む、先頭で終わる、または末尾で終わるインスタンスが自動的にグループに追加されます。最大3の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。
  - ・他の Alibaba Cloud 製品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。

# 7.3 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。

**兰**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。

# **ゴ**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。

プロダクト	メトリック	グラフの種類	説明
UStry align-left colsep-1 rowsep-1"> ApsaraDB for RDS <br 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。
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。

# 7.4 アプリケーショングループの変更

シナリオ

アプリケーションが、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、より多くのクラウドプロダクトを使用するときは、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運用と保守 (O&M) および開発担当者が変更となったときは、アプリケー ショングループのアラーム通知オブジェクトを変更する必要があります。



・アプリケーションの運用と保守 (O&M) および開発担当者が変更となったときは、グループ のアラームルール通知連絡先を修正する必要があります。 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グループディメンション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。

#### 手順

- 1. Cloud Monitor コンソール にログインします。
- 2. ナビゲーションウィンドウから [アプリケーショングループ] を選択します。
- 3. グループの一覧から編集するグループを選択し、グループ詳細ページに移動します。
- 4. ページの右上隅にある [グループの変更] をクリックします。
- 5. グループコンテンツを編集します。
- 6. [OK] をクリックして、変更を保存します。

# 7.5 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。
- 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。
  - 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。
  - 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。

# 8 イベントモニタリング

# 8.1 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、「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。





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。

reate / modify event alerts		×
Basic Infomation		
• Alarm Rule Name		
Combination of alphabets, numbers and underscore, in 30 characte		
Event alert		
Event Type		
System Event O Custom Event		
Product Type		
Redis -		
Event Level		
CRITICAL 🗙		
Event Name		
Select -		
Resource Range		
All Resources      Application Groups		
Alarm type		
ОК	Cancel	

# 8.2 クラウド製品イベント

# 8.2.1 クラウドプロダクトのシステムイベントモニタリング

システムイベントモニタリングでは、さまざまな種類のクラウドプロダクトによって生成された システムイベントの統一された統計情報とクエリエントリポイントがユーザーに提供され、ユー ザーはクラウドプロダクトの使用状況を明確に把握でき、クラウドがより透明性の高いものにな ります。 グループ化を適用してリソースを分類した後、プロダクトによって生成されたシステムイベント は自動的にグループ内のリソースに関連付けられることで、あらゆる種類のモニタリング情報を 統合しやすくなり、ビジネス上の問題を容易に見つけ、迅速に問題の分析および特定が行えるよ うになります。

イベントのアラーム機能も併せて提供され、ユーザーはイベントのレベルに応じたアラームの設 定や、SMS、メール、DingTalk などによる通知の受信、またはアラームコールバックを設定す ることもできます。 初めての深刻なイベントとタイムリーな処理、そしてオンライン自動操作お よびクローズドループ操作の形成がユーザーに通知されます。

#### システムイベントの表示

・ 方法 1

- 1. クラウドモニタリングコンソールにログインし、イベントモニタリングページにアクセス します。
- 2. フィルターボックスはシステムイベントを選択し、指定した期間に発生したイベントを表示します。
- 3. アクションの [詳細の表示] をクリックし、関連するイベントの詳細を表示します。
- ・ 方法 2

インスタンスがグループ化を適用して分類および管理されている場合、特定のアプリケーショ ングループを入力して、グループ内の関連インスタンスのシステムイベントを表示することも できます。

- クラウドモニタリングコンソールにログインして、アプリケーションのグループ化ページ に入ります。
- 2. グループ化詳細ページへ移動し、メニューから [イベントモニタリング] をクリックしま す。
- 3. ページに表示されているシステムイベントは、グループ内のインスタンスに関連するシス テムイベントです。

#### 警告ポリシーの設定

すべてのシステムイベントで、イベントが発生したときに警告するようにを設定できます。 この 機能を以下のように設定できます。

1. [システムイベント] ページに入り、該当するイベントに対する [アラームルールアクションの 作成] をクリックして、[アラームルールの作成] ページに入ります。 2. 受信したいイベント情報と連絡先を選択します。連絡先を選択すると、その連絡先はクラウドアカウントのすべてのインスタンスからイベントを受信します。グループ化を適用することを選択すると、グループ化アソシエーションを適用する連絡先は、グループ内のインスタンスによって生成されたイベントを受け取ります。

create / modify event alerts		
Alarm type		
Alarm notification		
Contact Group	Delete	
Terminal Context Transport	-	
Notification Method		
Info (Email ID+Ali WangWang+DingTalk Robot )	•	
+Add		
MNS queue		
Function service (Best Practises)		
URL callback		
	ОК	Cancel

# サポートされているクラウドプロダクトシステムイベント

・ ECS システムイベント

イベント名	ステータス	イベントの意味	イベントレベル
Instance: InstanceFailure. Reboot	実行中	インスタンスエラー によりインスタンス の再起動を開始	クリティカル
Instance: InstanceFailure. Reboot	実行済	インスタンスエラー によるインスタンス の再起動終了	クリティカル

イベント名	ステータス	イベントの意味	イベントレベル
Instance: SystemFailure. Reboot	実行中	システムエラーイン スタンスのため再起 動を開始	クリティカル
Instance: SystemFailure. Reboot	実行済	システムエラーイン スタンスによる再起 動終了	クリティカル
Instance: SystemMain tenance.Reboot	スケジュール済	システムメンテナン スインスタンスによ るスケジュールされ た再起動	クリティカル
Instance: SystemMain tenance.Reboot	回避済	システムメンテナ ンスのため、スケ ジュールされたイン スタンスの再起動を 回避	クリティカル
Instance: SystemMain tenance.Reboot	実行中	システムメンテナン スのため、計画され たインスタンスの再 起動実行	クリティカル
Instance: SystemMain tenance.Reboot	実行済	システムメンテナ ンスのため、スケ ジュールされたイン スタンスの再起動完 了	クリティカル
Instance: SystemMain tenance.Reboot	キャンセル	システムメンテナ ンスのため、スケ ジュールされたイン スタンスの再起動 キャンセル	クリティカル
Instance: SystemMain tenance.Reboot	失敗	システムメンテナン スインスタンスのス ケジュールが原因で 再起動に失敗	クリティカル
Disk:Stalled	実行中	ディスクパフォーマン スへの深刻な影響を 受けて開始	クリティカル
Disk:Stalled	実行済	ディスクパフォーマン スへの深刻な影響を 受けて終了	クリティカル

# ・SLB システムイベント

イベント名	イベントの意味	イベントレベル
CertKeyExpired_1	証明書は1日で期限切れにな ります	警告
CertKeyExpired_3	証明書は3日で期限切れにな ります	警告
CertKeyExpired_7	証明書は7日で期限切れにな ります	警告
CertKeyExpired_15	証明書は 15 日で期限切れに なります	警告
CertKeyExpired_30	証明書は 30 日で期限切れに なります	警告
CertKeyExpired_60	証明書は 60 日で期限切れに なります	警告

# ・ OSS システムイベント

イベント名	イベントの意味	イベントレベル
BucketEgressBandwidth	バケットのダウンストリーム 帯域幅がレポートしきい値を 超過	情報
BucketEgressBandwidt hThresholdExceeded	バケットのダウンストリーム 帯域幅がストリーミングしき い値を超過	警告
BucketIngressBandwidth	バケットアップストリーム帯 域幅がレポートしきい値を超 過	情報
BucketIngressBandwid thThresholdExceeded	バケットアップストリーム帯 域幅がフロー制御しきい値を 超過	警告
UserEgressBandwidth	ユーザーダウンストリーム帯 域幅がレポートしきい値を超 過	情報
UserEgressBandwidthT hresholdExceeded	ユーザーのダウンストリーム 帯域幅がストリーミングしき い値を超過	警告
UserIngressBandwidth	ユーザアップストリーム帯域 幅がレポートしきい値を超過	情報

イベント名	イベントの意味	イベントレベル
UserIngressBandwidth ThresholdExceeded	ユーザアップストリーム帯域 幅がフロー制御しきい値を超 過	警告

# 8.2.2 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。
- [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

Alarm type	
Alarm notification	
Contact Group	Dele
Default Contact Group	
Notification Method	
Warning (Message+Email ID+ Ali WangWang+DingTalk Robot	
+Add	
MNS queue	
Function service	
URL callback	

# 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。	Event Monitoring				
	Query Event	Alarm Rules			
	System Event	Custom Even	t		
	Enter the name o	f alarm rule to s	earch		Search
	Rule Name	:	Enable	Rule Desc	ription
			Enabled	ECS   CRI	TICAL   Insta

- 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。
   Create event test
      Product Type ECS
      Event Level :CRITICAL
      Event Name
         Content(JSON)
       {
          "product": "ECS",
          "content": {
            "executeFinishTime": "2018-06-08T01:25:37Z",
            "executeStartTime": "2018-06-08T01:23:37Z",
            "ecsInstanceName": "timewarp",
            "eventId": "e-t4nhcpgcu8fgushpn3mm",
            "eventType": "InstanceFailure.Reboot",
            "ecsInstanceId":
                                          },
          "resourceId": "acs:ecs:cn-hangzhou:1270676679546704:instan
          "level": "CRITICAL",
          "instanceName": "instanceName",
          "status": "Executing",
          "name": "Instance:InstanceFailure.Reboot:Executing",
          "regionId": "cn-hangzhou"
```

# 8.3 カスタムイベント

# 8.3.1 イベントデータのレポート

イベントモニタリングは、イベント関連の例外を迅速かつ正確に収集し Cloud Monitor にレ ポートすることに役立つ、イベントレポートの API を提供します。 レポートされるイベントにア ラームルールを設定することで、イベント関連の例外が発生したらすぐにアラーム通知を受け取 ることができます。

Cloud Monitor では、OpenAPI、Java SDK、および Alibaba Cloud CLI を使用したイベント データのレポートをサポートします。

#### 制限

- 各 Alibaba Cloud アカウントは最大 20 QPS を送信できます。
- ・ 一度に最大 100 件のイベントをレポートできます。
- ・一度に最大 500 KB のデータをレポートできます。

## OpenAPI を使用したデータのレポート

・サービスアドレス

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

・リクエスト構文

```
POST / event / custom / upload HTTP / 1 . 1
Authorizat ion : < authorizat ionstring >
Content - Length :< Content Length >
Content - MD5 :< Content MD5 >
Content - Type : applicatio n / json
Date : < GMT date >
HOST : maid
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 ":" EventConte nt "," groupId ": GroupId ," name ":"
EventName "," time ":" 20171023T1 44439 . 948 + 0800 "}]
```

・パラメーター

名前	型	必須	説明
Name	文字列	はい	イベント名
GroupId	数値	はい	イベントが属する アプリケーショング ループ ID

名前	型	必須	説明
Time	文字列	はい	イベントが発生した 時刻
Content	文字列	はい	イベント詳細

リクエストのヘッダー定義

API リクエストの署名

・応答要素

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

```
POST / event / custom / upload HTTP / 1 . 1
Host : metrichub - cms - cn - hangzhou . aliyuncs . com
x - cms - api - version : 1 . 0
Authorizat ion : YourAccKey : YourAccSec ret
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 : E9EF574D1A EAAA370860 FE37856995 CD
x - cms - ip : 30 . 27 . 84 . 196
User - Agent : cms - java - sdk - v - 1 . 0
Content - Type : applicatio n / json
[{" Content ": " 123 , ABC ", " groupid ": 100 , " name ": "
event_0 ", " Time ": " loud . 948 + 0800 "}]
```

- 応答

```
{
    " Code ": 200 ",
    " msg ": "// return MSG is empty for reports that
    are normal
}
```

Java SDK を使用したデータのレポート

Maven 依存関係

・サンプルコード

```
public void uploadEven t () throws CMSExcepti on ,
Interrupte dException {
```

// Initialize Client CMSClient cmsClient = new CMSClient ( endpoint , accKey , secret ); Build event // 2 reports CustomEven tuptoauxeq tUploadReq uest . builder () . append ( CustomEven t . builder () . setContent (" abc , 123 ") . setGroupId ( 1011 ) . setName (" Event001 "). build ()) . setName (" Event002 "). build ()) . build (); CustomEven tUploadRes ponse response = cmsClient . putCustomE vent ( request ); List < CustomEven t > eventList = new ArrayList < t >(); CustomEven eventList . add ( CustomEven t . builder () . setName (" Event002 "). build ()); }

# Alibaba Cloud CLI を使用したデータのレポート

プライマリアカウントを使用して、クラウドモニタリング権限を持つ RAM アカウントの AccessKey を生成します(RAM アカウントはプライマリアカウントより、より安全であるこ とを前提としています)。

· RAM アカウントを作成します。

RAM	User Management		Create User Create User
Dashboard	User Name   Search by User Name  Search		
Groups	User Name/Display Name Description	Created At	Actions
Policies	Application_group Application_group	2018-11-01 11:27:10	Manage   Authorize   Delete Join Group
Roles	cs-group-test cs-group-test	2018-10-19 16:32:39	Manage   Authorize   Delete Join Group
ActionTrail	grafana-test grafana-test	2018-10-10 19:22:49	Manage   Authorize   Delete Join Group

•	RAM アカウントの	AccessKeyId と	AccessKeySecret を生成します。
---	------------	---------------	-------------------------

<	Application_group						
User Details	Pagia Information					Fult Daris Teferentian	
User Authorization P	User Name Applica	n ation_group	UID 260773841042830953		Created At 2018-11-01 11:27:10	Edit Basic Information	^
User Groups	Display Name Application_group		Mobile Phone		Email		
	Description -						
	Web Console Log	gon Management 🔞			Disable Console Logor	Reset Password	^
	You must activate !	MFA	Last Logon Time: 2018-11-01 11:37:3	35	On your next logon you must reset the	password.	
	MFA Device						^
	Туре	Introduction			Enabling Status		Actions
	VMFA Device	Application calculates a 6-digit verification code usin	ng the TOTP standard algorithm.		Not Enabled	Enable VMFA De	evice
	Liser Access Key					Croate Access Key	•
	AccessKey ID		Status	Created At		create Actess Rey	Actions

· RAM アカウントに Cloud Monitor アクセス権限を割り当てます。

(-)					s	earch Q M	1essage <sup>99+</sup> Billing Ma	nagement	Enterprise	More	🔄 Englis	h 🙆
	<	pop_test	Edit User-Level Authorization				×				Edit Authorizatio	on Policy
	User Details		Members added to this group have all th once.	e permissions	of this group. A	nember cannot be added to the same g	group more than			_		
	User Authorization P	User-Level Authorization	Available Authorization Policy Names	Туре		Selected Authorization Policy Name	Туре					
	User Groups	Authorization Policy Name	Search Keywords	۹		AliyunCloudMonitorFullAccess	System					Actions
		AliyunCloudMonitorFullAc	AdministratorAccess Provides full acce	System		AliyunCloudMonitorReadOnlyAcce	System		View Pe	rmissions	Revoke Autho	orization
		AliyunCloudMonitorReadC	AliyunOSSFullAccess Provides full acce	System	<	Provides read-only			View Pe	rmissions	Revoke Autho	orization
			AliyunOSSReadOnlyAccess Provides read-only	System								
	-		AliyunECSFullAccess Provides full acce	System								
							OK Close					Contact

## 手順

1. aliyuncli ツールをインストールします。

システム要件:Linux、UNIX、またはMac OS。 環境要件:Python 2.7.x インストール がされている必要があります。

a. Python のインストール

- ・ Python 2.7.x がデバイスにインストールがされている場合、この手順をスキップできます。
- Python 2.7.x がデバイスにインストールされていない場合、コマンドラインウィンド ウで次のコマンドを実行して Python をインストールします。 wget がデバイスにイン ストールされていることをご確認ください。

```
wget https://www.python.org/ftp/python/2.7.8
/ Python - 2.7.8.tgz (or download it in other
ways and put it in a certain path)
tar - zxvf Python - 2.7.8.tgz
cd Python - 2.7.8
./ configure
```

make		
sudo	make	install

b. pip のインストール

- ・ pip がデバイスにインストールされている場合、この手順をスキップできます。
- pip がデバイスにインストールされていない場合、コマンドラインウィンドウで次のコマンドを実行して pip をインストールします。

```
curl " https :// bootstrap . pypa . io / get - pip . py " - o
" pip - install . py "
sudo python pip - install . py
```

・インストールが成功すると、次のような情報が表示されます。

Successful ly installed pip - 7 . 1 . 2 setuptools - 18 . 7 wheel - 0 . 26 . 0

c. コマンドラインツールのインストール

インストールされている pip のバージョンがサポートされていない場合、Alibaba Cloud CLI のインストール中にエラーが発生します。 他の操作を実行する前に、次のコマンドを 使用して pip のバージョンをアップグレードできます。 pip 7.x 以降を使用することを推 奨します。 pip がサポートされているバージョンの場合、この手順をスキップできます。

A. コマンドラインウィンドウで次のコマンドを実行して、pip のバージョンをアップグ レードします。

sudo pip install - U pip

インストールが成功すると、次のような情報が表示されます。

```
Successful ly uninstalle d pip - 7 . 1 . 2
Successful ly installed pip - 8 . 1 . 2
```

B. 次のコマンドを実行して Alibaba Cloud コマンドラインツールをインストールします。

sudo pip install aliyuncli

インストールが成功すると、次のような情報が表示されます。

Successful ly installed aliyuncli - 2 . 1 . 2 colorama - 0 . 3 . 3 jmespath - 0 . 7 . 1

d. コマンドラインツールの設定

Default Region Id [ cn - hangzhou ]: cn - hangzhou Default output format [ json ]: json

- 2. CMS SDK のインストール
  - ·Windowsの場合は、コマンドラインウィンドウで次のコマンドを実行します。

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

· SDK を更新するには、次のコマンドを実行します。

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

· Linux の場合は、コマンドラインウィンドウで次のコマンドを実行します。

sudo pip install aliyun - python - sdk - cms

· SDK を更新するには、次のコマンドを実行します。

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 を使用します。

・Windows のレポート例

aliyuncli . exe cms PutEvent -- EventInfo "[{' content ':' helloworld ',' time ':' 20171013T1 70923 . 456 + 0800 ',' name ':' ErrorEvent ',' groupId ':' 27147 '}]"

・Linux のレポート例

aliyuncli cms PutEvent -- EventInfo "[{' content ':' helloworld ',' time ':' 20171023T1 80923 . 456 + 0800 ',' name ':' ErrorEvent ',' groupId ':' 27147 '}]"

・データが正常にレポートされると、システムはステータスコード 200 を返します。

```
'' code ": " 200 ",
}
```

### ステータスコード

ステータスコード	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、または認証エラー
500	内部サーバーエラー

## RAM アカウント許可

RAM ユーザーアカウントの AccessKey を使用してイベントをレポートするとき、そのRAMア カウントには Cloud Monitor の管理権限が必要です。 RAM アカウントに Cloud Monitor の 管理権限がない場合、RAM ユーザーアカウントに、この操作が許可されていないためイベント をアップロードできないことを示すプロンプトが表示されます。

- 1. アクセス制御 RAM コンソールにログインします。
- 2. ユーザー管理メニューに移動します。
- 3. データをレポートするために使われる RAM ユーザーアカウントの横にある [権限付与] をク リックします。

RAM	User Management		Create User 🗘 Refresh
Dashboard Users	User Name    Search by User Name  Search		
Groups	User Name/Display Name Description	Created At	Actions
Policies	STS-Test	2018-02-02 13:41:57	Manage   Authorize   Delete Join Group
Roles	acs_ram_account_c7e5896eb18544 aliyun container service use this account to provide enhance acs_ram_account	2018-01-23 10:20:13	Manage   Authorize   Delete Join Group
ActionTrail	xaozhen xiaozhen	2017-11-27 12:08:11	Manage   Authorize   Delete Join Group
	cms_readwrite readwrite	2017-09-12 10:07:06	Manage   Authorize   Delete

4. 権限付与ページで、[クラウドモニタリングの権限を管理] を選択し、[OK] をクリックし、権 限情報を保存します。

Members added to this group have all the once.	e permissions o	f this group. A r	nember cannot be added to the same grou	p more than
Available Authorization Policy Names	Туре		Selected Authorization Policy Name	Туре
CloudMonitor Q			AliyunSLBFullAccess Provides full acce	System
AliyunCloudMonitorReadOnlyAcce System Provides read-only AliyunCloudmonitorInstallRole 安装云监控Agent Custom	>	AliyunSTSAssumeRoleAccess Provides access to	System	
	Custom	<	AliyunKvstoreFullAccess Provides full acce	System
			AliyunCloudMonitorFullAccess Provides full acce	System
			ок	Close

# 8.3.2 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

## b. SDK の初期化

// Here , is applicatio n ID 118 the grouping of CloudMonit or. Events can be categorize d applicatio ns . You can view group bγ IDs in CloudMonit or applicatio n grouping list . CMSClientI nit . groupId = 118L ; // The address is the reporting entry
event system, which is currently the of 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、ScheduledExecutorSer vice 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 LinkedBloc kingQueue < EventEntry > eventQueue =
new
     LinkedBloc kingQueue < EventEntry >( 10000 );
private ScheduledE xecutorSer vice schedule = Executors.
newSingleT hreadSched uledExecut or ();
// Report event :
// Every
          event contains
                          its
                               name and
                                           content .
                                                       The
            for identifica tion and the content
  name
         is
contains details of the event, in which
                                                        full
                                                  the

    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 asynchrono usly . Initialize scheduled
tasks . Report events in
                              batch by run every second
    You can adjust the reporting interval
                                                       needed
                                                 as
schedule . scheduleAt FixedRate ( this , 1 , 1 , TimeUnit .
SECONDS );
public void run () {
    do
       {
        batchPut ();
   } while ( this . eventQueue . size () > 500 );
                batchPut () {
private void
   // Extract
                            from
                                   the
                                         queue for batch
                99 events
 reporting .
    List < CustomEven t > events = new ArrayList <
CustomEven t >();
    for ( int i = 0 ; i < 99 ; i ++) {
    EventEntry e = this . eventQueue . poll ();
    if ( e == null ) {</pre>
            break ;
```

events . add ( CustomEven t . builder (). setContent ( e . getContent ()). setName ( e . getName ()). build ()); if ( events . isEmpty ()) { return ; // Report events in batch to CloudMonit or . No retry or retry in SDK is added here. If you have high requirement for event reliability, add retry policies. { try CustomEven tUploadReq uestBuilde r builder = CustomEven tUploadReq uest . builder (); builder . setEventLi st ( events ); CustomEven tUploadRes ponse response = cmsClient . putCustomE vent ( builder . build ()); if (!" 200 ". equals ( response . getErrorCo de ())) { iogger . warn (" event reporting error : msg
; {}, rid : {}", response . getErrorMs g (), response .
getRequest Id ()); } 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 informativ e for searching and locating. Here, map is used for organizing events and converted to Json format as event content . Map < String , String > eventConte nt = new HashMap < String , String >(); eventConte nt . put (" method ", " GET "); // http request method eventConte nt . put (" path ", "/ users "); // http path eventConte nt . put (" exception ", e . getClass (). getName ()); // Exception class name for searching eventConte nt . put (" error ", e . getMessage ()); // Error message of exception eventConte nt . put (" stack\_trac e ", ExceptionU tils . getStackTr ace ( e )); // Exception stack for locating // Finally submit the events in the pre asynchrono us reporting method . Since no is performed in asynchrono us reporting , // Finally the preceding no retrv event loss of small probabilit y may happen. However

, it is sufficient for alarms of unknown http exceptions . put (" http\_error ", JsonUtils . toJson ( eventConte nt )); image . png ]( http :// ata2 - img . cn - hangzhou . img - pub . aliyun - inc . com / 864cf09597 7cf61bd340 dd1461a024 7c . 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 organizati on of the message queue : Map < String > eventConte nt = new HashMap <</pre> String , String >(); eventConte nt . put (" cid ", consumerId ); // Consumer TD eventConte nt . put (" mid ", msg . getMsgId ()); // Message ID eventConte nt . put (" topic ", msg . getTopic ()); // topic Message eventConte nt . put (" body ", body ); // Message body eventConte nt . put (" reconsume\_ times ", String . valueOf ( msg . getReconsu meTimes ())); // The number of retries after message failure eventConte nt . put (" exception ", e . getClass (). getName ()); // Exception class name in case of exception eventConte nt . put (" error ", e . getMessage ()); // Exception message eventConte nt . put (" stack\_trac e ", ExceptionU tils . getStackTr ace ( e )); // Exception stack // Finally , report the event

put (" metaq\_erro r ", JsonUtils . toJson ( eventConte nt
));

レポート後、イベントを確認します。

<	demo 😤 Back to Application
Group Resource	S Quick Start S How to Repo
<ul> <li>Dashboards</li> </ul>	
Fault List	System Event  CloudMonit
Event Monitor	
Availability Monitor	2
Log Monitoring Custom Monitoring	1
Alarm Logs	<b>16:18</b> 21:33
Alarm Rule	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
Souick Start Start Outco Repo
System Event  CloudMonit
2
1
0
<b>16:18</b> 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	Solutick Start Start Start
Dashboards	
Fault List	System Event V
Event Monitor	
Availability Monitor	1
Log Monitoring	0.5
Custom Monitoring	0
Alarm Logs	<b>16:18</b> 21:33
Alarm Rule	Product Time Name
	18-11-01 09:28:38 CloudMonito
	18-10-31 Document Version2019 09:32:34

## 8.4 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

## 9 カスタムモニタリング

## 9.1 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。
  - 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。
    - Custom Monitoring S Quick Start S How to Report Data Time Series Alarm Rules C Refresh 
       1h
       6h
       12h
       1days
       7days
       2018-12-04 13:31:57 - 2018-12-04 14:31:57
       ##
       43 12-04 13:40:00 12-04 13:48:20 12-04 13:56:40 12-04 14:30:00 12-04 14:05:00 12-04 14:13:20 12-04 14:21:40 env: public env: pre All > alertnotify > NetworkMonitorNameRT Please enter the metric or dimension name Search Statistical Method -Dimensions Operation ~ env: public SampleCount Delete | Setup Alarm Rule SampleCount Delete | Setup Alarm Rule ~ env: pre Total 3 10 \$ « < 1 > »
  - 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。
  - 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。
  - (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。

	<	alertengine t Back to Application Group I Guick Start I How to Report Data								
	Group Resource					1h	6h 12h	1days 7days	2018-12-04 13:37:35 - 20	18-12-04 14:37:35
L	Dashboards	411								
L	Fault List	Λ								
L	Event Monitor	200								
L	Availability Monitor					~			_	
L	Log Monitoring	8 12-04 13:40:0	0 12-04 13:4	48:20 12-04	13:56:40 12-04	14:05:00	12-04 14:13:2	0 12-04	14:21:40 12-04	14:30:00
L	Custom Monitoring								Cluster: cr	ns 🔹 cluster: tianjimon
	Alarm Logs	All > MetricStoreH	eader	Search						
	Alarm Rule	Piedoo enter uno me	une of dimension name.	Gearch						
L		Dime	ensions		Statistical Method -					Operation
		clus	ter:							Delete   Setup Alarm Rule
		clus	ter:							Delete   Setup Alarm Rule

・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。
  - 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。
  - 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。
- 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。
- 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。

### 9.2 モニタリングデータのレポート

カスタマイズモニタリングでは、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。 具体的には、API を使用すると、収集した時系列データを Cloud Monitor にレポートした り、アラーム通知を受信するようアラームルールの設定ができます。

Cloud Monitor では、OpenAPI、Java SDK、および Alibaba Cloud CLI の 3 つのデータレ ポート方法が提供されます。

制限

・ QPS は、北京、上海、杭州の各リージョンで 200、張家口、深センの各リージョンで 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。ボディサイズは 256 KB を超える ことはできません。
- metricName フィールドは、文字、数字、および下線のみをサポートします。フィールドは文字で始まる必要があります。文字以外で開始した場合、大文字の "A" に置き換えられ、その他のすべての無効な文字はアンダースコア (\_) に置き換えられます。
- dimensions フィールドでは、"="、"&" および "," はサポートされていません。 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 は 64 バイトを超えることはできません。それ以外の場合、Key-Value は切り詰められます。
- ・生データの報告には手数料がかかります。 無料版では、集計データレポートがサポート されています (つまり、データをレポートするときは、 type フィールドに "1" を入 れ、"request" パラメーターに渡す必要があります)。

#### OpenAPI を使ったレポートデータ

OpenAPI を使用して生データをレポートした後、Cloud Monitor では次の統計方法を使用して 1分間隔と5分間隔で統計が計算されます。

- · Average: 平均值
- ・ Maximum: 最大値
- ・ Minimum: 最小値
- ・Sum: 合計値
- · SampleCount: カウント
- ・ SumPerSecond: 対応する集約期間の合計/合計秒。 移動平均計算を使用することもできます。
- ・ CountPerSecond: 対応する集約期間のカウント/合計秒。 移動平均計算を使用することもで きます。
- ・LastValue: 集約期間内の最後のサンプリング値。これはゲージに似ています。
- · P10: 0.1 パーセンタイル、集約期間内の全サンプリングデータの 10% より大きい
- ・ P20: 0.2 パーセンタイル、集約期間内の全サンプリングデータの 20% より大きい
- ・ P30: 0.3 パーセンタイル、集約期間内の全サンプリングデータの 30% より大きい
- ・ P40: 0.4 パーセンタイル、集約期間内の全サンプリングデータの 40% より大きい
- ・ P50: 0.5 パーセンタイル、集約期間内の全サンプリングデータの 50% より大きい、中央値と も呼ばれる
- · P60: 0.6 パーセンタイル、集約期間内の全サンプリングデータの 60% より大きい
- ・ P70: 0.7 パーセンタイル、集約期間内の全サンプリングデータの 70% より大きい

- ・ P75: 0.75 パーセンタイル、集約期間内の全サンプリングデータの 75% より大きい
- ・ P80: 0.8 パーセンタイル、集約期間内の全サンプリングデータの 80% より大きい
- · P90: 0.9 パーセンタイル、集約期間内の全サンプリングデータの 90% より大きい
- · P95: 0.95 パーセンタイル、集約期間内の全サンプリングデータの 95% より大きい
- · P98: 0.98 パーセンタイル、集約期間内の全サンプリングデータの 98% より大きい
- · P99: 0.99 パーセンタイル、集約期間内の全サンプリングデータの 99% より大きい
- ・サービスアドレス

サービスのインターネットアドレス: https://metrichub-cms-cn-hangzhou.aliyuncs.com サービスのイントラネットアドレスは次のとおりです。

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
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

リージョン	リージョン ID	エンドポイント
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
Authorizat ion :< Authorizat ionString >
Content - Length :< Content Length >
Content - MD5 :< Content MD5 >
Content - Type : applicatio n / 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 ":{" sampleName
1 ":" value1 "," sampleName 2 ":" value2 "}," time ":""," type ":
0 ," period ": 60 ," values ":{" value ": 10 . 5 ," Sum ": 100 }}]
```

・ 署名アルゴリズム

詳しくは、「署名アルゴリズム」をご参照ください。

・リクエストパラメーター

名前	型	必須	説明
groupId	long	はい	アプリケーショング ループ ID。
metricName	文字列	はい	モニタリング測定 名。名前の長さは最 大 64 バイトで、文 字、数字、およびコ ネクタ "/\"を含む ことができます。制 限を超える文字は切 り詰められます。

名前	型	必須	説明
dimensions	オブジェクト	はい	デメンションマップ。 key-value は文字列 で、キーと値の長さ がそれぞれ最大 64 バイトで、文字、数 字、およびコネクタ" /\"を含むことがで きます。制限を超え る文字は切り詰めら れます。key-value のペアの最大数は 10 です。
time	文字列	はい	測定データの時刻。 "yyyyMMdd'T' HHmmss.SSSZ" と 長い形式のタイム スタンプをサポート します、たとえば、 20171012T132456. 888+0800、または 1508136760000。
type	int	はい	レポートされたデー タの型。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。そうでな ければ、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	文字列	いいえ	秒単位の集約期間。 type=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。

名前	型	必須	説明
values	オブジェクト	はい	測定値の集まり。 type=0 の場合、キー は "value" である 必要があり、生デー タがレポートされま す。 Cloud Monitor は、最大、カウン ト、合計などの集計 期間に基づいて、生 データを複数の種類 のデータに集計しま す。

#### Java SDK を使ったデータのレポート

・Java SDK のインストール

Maven を介して Java SDK をインストールするときは、次の依存関係を追加する必要があります。

・応答要素

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
Authorizat ion : yourAccess KeyId : yourAccess KeySecret
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 : E9EF574D1A EAAA370860 FE37856995 CD
x - cms - ip : 30 . 27 . 84 . 196
User - Agent : cms - java - sdk - v - 1 . 0
Content - Type : applicatio n / json
[{" groupId ": 101 ," metricName ":""," dimensions ":{"
sampleName 1 ":" value1 "," sampleName 2 ":" value2 "}," time
```

```
":""," type ": 0 ," period ": 60 ," values ":{" value ": 10 . 5 ," Sum ": 100 }}]
```

- 応答の例

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

- ・コード例
  - 生データのレポート

```
CMSClientI nit . groupId = 101L ;// Set a
                                                 common
                                                          group
ID .
CMSClient cmsClient = new accKey , secret );// Initialize the
                                        CMSClient ( endpoint ,
                                        client .
CustomMetr icUploadRe quest
icUploadRe quest builder ()
                                        request = CustomMetr
               Metric
         name
                       . setGroupId ( 102L )// Set a
                                                         custom
        ID .
group
                       . setTime ( new Date ())
                       . setType ( CustomMetr ic . TYPE_VALUE
)// The type
                 is
                      raw data
                       . appendValu e ( MetricAttr ibute .
VALUE , 1f )// The
                      key must be
                                        this
                                             when
                                                      the
                                                           type
      raw
  is
            data .
                       . appendDime nsion (" key ", " value ")//
        dimension .
Add
      а
                       . appendDime nsion (" ip ", " 127 . 0 . 0
. 1 ")// Add
                   dimension .
               а
                       . build ())
               . build ();
CustomMetr icUplóadRe sponse response = cmsClient.
putCustomM etric ( request );// Report data .
        System . out . println ( JSONObject . toJSONStri  ng (
response ));
```

- 複数の集計期間の集計データを自動的に報告

SDK ではローカル集計後のデータレポートがサポートされます。 集計期間は、1 分と 5 分です。

データ型	説明	集計值	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	標準値	LastValue 以外のす べてのプロパティ	約 4 KB

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)
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 、CountPerSe cond、Average , Maximum、 Minimum、PXX ( P10–P99)	約 4 KB
Histogram	ディストリビュー ション	SampleCoun t, Average, Maximum, Minimum, PXX( P10–P99)	約4KB

```
// Initialize
         CMSClientI nit . groupId = OL ;
         CMSClient cmsClient = new CMSClient ( accKey ,
 secret , endpoint );// Create a ctreate
CMSMetricR egistryBui lder builder = new
Dui lder ();
          endpoint );// Create a client .
 CMSMetricR egistryBui lder ();
         builder . setCmsClie nt ( cmsClient );
         final MetricRegi stry registry = builder .
 build ();// Create a registry which contains
                                                        two
 aggregatio n periods.
        // or final MetricRegi stry registry = builder .
 build ( RecordLeve l . _60S );// Create a registry which
 contains only the one-minute aggregatio n period.
// Use value .
                 value = registry . value ( MetricName . build
 ValueWrapp er
 (" value "));
 value . update ( 6 . 5 );
// Use meter .
                 meter = registry . meter ( MetricName . build
 MeterWrapp er
 (" meter "));
 meter . update ( 7 . 2 );
       counter .
// Use
 CounterWra pper counter = registry . counter ( MetricName .
build (" counter "));
counter . inc ( 20 );
counter . dec ( 5 );
// Use timer .
```

```
TimerWrapp er timer = registry . timer ( MetricName . build
 (" timer "));
timer . update ( 30 , TimeUnit . MILLISECON DS );
           histogram .
// Use
HistogramW rapper histogram = registry . histogram (
MetricName . build (" histogram "));
histogram . update ( 20 );
 / Use gauge .
final List list = new ArrayList ();
registry . gauge ( MetricName . build (" gauge "), new
// Use
                                                                           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 アカウントで RAM ユーザーを作成し、Cloud Monitor アクセス権限を持つ RAM ユーザー Access Key (AK) を生成したことをご確認ください。

· RAM ユーザーの作成

RAM	User Management		Create User Create User
Dashboard	User Name   Search by User Name  Search		
Groups	User Name/Display Name Description	Created At	Actions
Policies	Application_group Application_group	2018-11-01 11:27:10	Manage   Authorize   Delete Join Group
Roles	cs-group-test cs-group-test	2018-10-19 16:32:39	Manage   Authorize   Delete Join Group
ActionTrail	grafana-test grafana-test	2018-10-10 19:22:49	Manage   Authorize   Delete Join Group

· RAM ユーザーの AccessKeyID と AccessKeySecret の生成

<	Display Name test123			•
User Details	Description -			
User Authorization P	Web Console Logon Management 🞯		Disable Console Logon Reset Password	^
User Groups	You must activate MFA	Last Logon Time:	On your next logon you must reset the passwe	ord.
=	MFA Device			^
	Type Introduction		Enabling Status	Actions act
	VMFA Device Application calculates a 6-digit ver	ification code using the TOTP standard algorithm.	Not Enabled Enable VMF	A Device
	User Access Key		Create Access Key	^
	AccessKey ID Sta	rus Created At		New Version

#### · RAM ユーザーに対して、Cloud Monitor アクセス許可を付与

1	lt	Edit User-Level Authorization	Edit Authorization Policy
User Details		Members added to this group have all the permissions of this group. A member cannot be added to the same group more than once.	
User Authorization P		Available Authorization Policy Names Type Selected Authorization Policy Name Type	
User Groups	А	CloudMonitor Q	Actions
		AllyunCloudMonitorFullAccess Provides full acce	
	E	AllyunCloudMonitorReadOnlyAcce System	
			antact Us
		OK Close	New Version

Alibaba Cloud CLI のインストール

システム要件:Linux、UNIX、または Mac OS

環境要件: Python 2.7.x をインストール済

- 1. Python のインストール
  - · Python 2.7.x をインストール済の場合、この手順をスキップします。
  - ・それ以外の場合は、コマンドラインインターフェイスで次のコマンドを実行します。

注:

wget をインストール済であることをご確認ください。

```
wget https :// www . python . org / ftp / python / 2 . 7 . 8
/ Python - 2 . 7 . 8 . tgz ( or download it in some
other way and put it in a certain path )
tar - zxvf Python - 2 . 7 . 8 . tgz
cd Python - 2 . 7 . 8
./ configure
make
sudo make install
```

- 2. pip のインストール
  - ・コマンドラインインターフェイスで次のコマンドを実行します。

```
    注:
    pipをインストール済の場合、この手順をスキップしてください。
    curl "https://bootstrap.pypa.io/get-pip.py"-o
    pip - install.py "
```

"

7

```
pip - install . py
   sudo
         python

    システムに次のような、あるいは同様の情報が表示されれば、インストールは成功です。

   Successful ly installed
                           pip - 7 . 1 . 2 setuptools - 18 .
      wheel - 0 . 26 . 0
```

- 3. Alibaba Cloud CLI のインストール。
  - ・ 以前のバージョンの pip を使うと Alibaba Cloud CLI のインストールに失敗する可能性 があります。 必ず、pip 7.x 以降のバージョンをご使用ください。 コマンドラインイン ターフェイスで次のコマンドを実行して pip をアップグレードできます。

sudo install - U pip pip

システムに次のような、あるいは同様の情報が表示されれば、アップグレードは成功で す。

uninstalle d Successful ly pip - 7 . 1 . 2 installed pip - 8 . 1 . 2 Successful ly

· Alibaba Cloud CLI をインストールするには、次のコマンドを実行します。

sudo install pip aliyuncli

システムに次のような、あるいは同様の情報が表示されれば、インストールは成功です。

Successful ly installed aliyuncli - 2 . 1 . 2 colorama - 0 . 3 . 3 jmespath - 0 . 7 . 1

4. Alibaba Cloud CLI の設定 Alibaba Cloud CLI を設定するために、次のコマンドを実行しま

す。

~ sudo aliyuncli configure Aliyun Access Key keyid Aliyun Secret [\* b ]: Access Key youraccess keysecret Default Region Id [ cn - hangzhou ]: cn - hangzhou Default output format [ json ]: json

CMS SDK のインストール

·Windows システムのインストール方法は以下のとおりです。

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

・Windows システムで SDK を更新するには、次のコマンドを実行します。

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

· Linux システムのインストール方法は以下のとおりです。

sudo pip install aliyun - python - SDK - ecs

・ Linux システムで SDK を更新するには、次のコマンドを実行します。

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

モニタリングデータのレポート

モニタリングデータをレポートするには PutCustomM etric インターフェイスを使用します。

・Windows システムの例

aliyuncli . exe cms PutCustomM etric -- MetricList "[{'
groupId ': 1 ,' metricName ':' testMetric ',' dimensions ':{'
sampleName 1 ':' value1 ',' sampleName 2 ':' value2 '},' type ':
0 ,' values ':{' value ': 10 . 5 }}]"

・Linux システムの例

aliyuncli cms PutCustomM etric -- MetricList "[{' groupId
': 1 ,' metricName ':' testMetric ',' dimensions ':{' sampleName 1
':' value1 ',' sampleName 2 ':' value2 '},' type ': 0 ,' values ':
{' value ': 10 . 5 }}]"

・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。

{
" code ": " 200 ",
}

ステータスコード

ステータスコード	説明
200	正常

ステータスコード	説明
206	<ul> <li>一部は正常</li> <li>"reach max time series num" が返された場 合、時系列クォータが不足していることを示し 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。</li> <li>"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。</li> <li>"type is invalid" が返された場合は、"type" 値が無効であることを示しています。0または 1 以外の番号が渡されていないか、ご確認くだ さい。</li> </ul>
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、または未許可
500	内部サーバーエラー

RAM ユーザー認証

RAM ユーザー AK を使用してイベントデータをレポートする前に、Cloud Monitor アクセス権 限を対応する RAM ユーザーに付与する必要があります。 アクセス権限を付与しないと、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] をクリックします。
- 3. 対象ユーザーを見つけ、[許可] をクリックします。

RAM	User Management		Create User C Refresh
Dashboard	User Name v Search by User Name	Search	
Groups	User Name/Display Name Description	Created At	Actions
Policies		2018-12-03 10:18:32	Manage   Authorize   Delete Join Group
Roles	N	2018-11-22 11:24:03	Manage   Authorize   Delete Join Group

# 4. 権限付与ページで、Aliyun Cloud Monitor Full Access ポリシーを選択し、[OK] をクリックします。

once.	e permissions o	r this group. A r		more than
Available Authorization Policy Names	Туре		Selected Authorization Policy Name	Туре
CloudMonitor	्र System	>	AdministratorAccess Provides full acce	System
AliyunCloudMonitorReadOnlyAcce Provides read-only			AliyunCloudMonitorFullAccess Provides full acce	System

## 9.3 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。
  - 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。

Create Dashboard	×
test_dashboard	
	Create Close

・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。

Dasinboards	Log Montoning	Gustom					
Custom Monito	oring	▼ online-ap	plication	Heat	Map Gradient Range:	0	auto
127.24 100.00 50.00							
19:29:00	19:35:00	19:43:20	19:51:40 MetricStoreR	20:00:00 eader-Average-clust	20:08:20 er:cms	20:16:40	
Metrics:	MetricStoreReader		Average				
Dimension	s: cluster:cms				•		
	- ·						