Alibaba Cloud
Cloud Monitor

Quick Start

Issue: 20190904

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Function overview

CloudMonitor provides you with an overview of your cloud services, cloud resource usage, alarms, and important events, allowing you to understand the utilization and maintenance of your resources and the alarms for your cloud services in real time.

Cloud service overview

The cloud service overview provides a summary of the resources that you use, helping you quickly and easily understand the assets you have. The cloud service overview displays the following services:

- Hosts, including ECS hosts and the non-ECS hosts that are installed with the CloudMonitor agent
- Server Load Balancer
- Elastic IP Address
- ApsaraDB for RDS, MongoDB, Memcache, and Redis
- OSS
- CDN
- Message Service
- Container Service
- Log Service
- StreamCompute
- Analytic DB
- API Gateway
- E-MapReduce
- HybridDB for MySQL
- HybridDB for PostgreSQL
- Express Connect

By clicking the number of resources, you can view the list page for the corresponding services under cloud service monitoring.

 Note:

To monitor and view ECS data (such as CPU, memory, and disk usage), you need to install the CloudMonitor agent. For more information about how to install the CloudMonitor agent, see #unique_4.

Alarm overview

The alarm overview provides alarm statistics, including the total number of alarms for the past seven days, the number of currently triggered alarm rules, the number of alarm rules with insufficient data, and the alarm SMS usage for the current month.

You can view more information by clicking the number of alarms or alarm rules.

Event overview

Event overview summarizes all the exceptions and O&M events that occur during a span of 24 hours. The following are important events that are supported.

Product	Event
Host	Agent stops working.
ApsaraDB for RDS	Master/Backup switchover
ApsaraDB for RDS	Instance failure
ApsaraDB for MongoDB	Instance failure
ApsaraDB for Redis	Master/Backup switchover
ApsaraDB for Redis	Instance failure

Resource usage overview

Resource usage shows the overall resource usage of each service under your account. The cumulative usage in the current month is monitored and measured for OSS, CDN, and Log Service. The metrics for all other services are monitored in real time by using the 95th percentile method. For example, if the 95th percentile for the CPU usage of ECS instances is 34%, 95% of the ECS instances have a CPU usage of less than 34%. The value that is determined by this method varies by product.

Resource indicator descriptions

Product	Indicator	Statistical method	Statistical period	Statistical range
Host	CPU usage	95th percentile	Real-time	All instances
Host	Memory usage	95th percentile	Real-time	All instances

Product	Indicator	Statistical method	Statistical period	Statistical range
Host	Disk usage	95th percentile	Real-time	All instances
Host	Outbound Internet bandwidth	95th percentile	Real-time	All instances
ApsaraDB for RDS	CPU usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	Connection usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	Disk usage	95th percentile	Real-time	All instances
OSS	Total outbound Internet traffic this month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total number of PUT requests this month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total number of GET requests this month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Storage size	Sum	The sum of the storage currently occupied by all OSS buckets	All buckets

Product	Indicator	Statistical method	Statistical period	Statistical range
CDN	Total traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All domain names
CDN	Peak network bandwidth	95th percentile	Real-time	All domain names
CDN	Access QPS	95th percentile	Real-time	All domain names
ApsaraDB for MongoDB	CPU usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Memory usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Connection usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Disk usage	95th percentile	Real-time	All instances
ApsaraDB for Memcache	Cache hit ratio	95th percentile	Real-time	All instances
ApsaraDB for Memcache	Cache usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	Memory usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	Connection usage	95th percentile	Real-time	All instances
EIP	Inbound network bandwidth	95th percentile	Real-time	All instances

Product	Indicator	Statistical method	Statistical period	Statistical range
EIP	Outbound network bandwidth	95th percentile	Real-time	All instances
Container Service	CPU usage	95th percentile	Real-time	All instances
Container Service	Memory usage	95th percentile	Real-time	All instances
Container Service	Outbound Internet traffic	95th percentile	Real-time	All instances
Log Service	Total inbound network traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All Projects
Log Service	Total outbound network traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All Projects
Log Service	Total requests for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All Projects
ApsaraDB for HybridDB	CPU usage	95th percentile	Real-time	All instances
ApsaraDB for HybridDB	Memory usage	95th percentile	Real-time	All instances
ApsaraDB for HybridDB	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for HybridDB	Connection usage	95th percentile	Real-time	All instances
ApsaraDB for HybridDB	Disk usage	95th percentile	Real-time	All instances

2 Dashboard

CloudMonitor dashboards are customizable pages that can be used to monitor data from multiple products and instances in all one area.

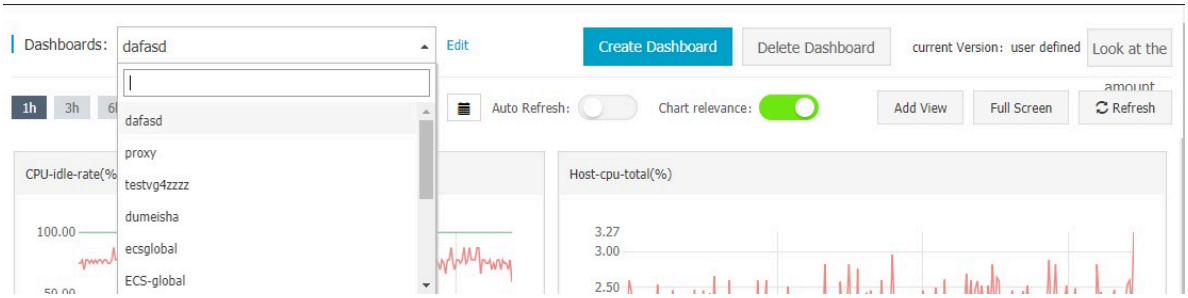
View a dashboard

You can quickly view the resources used by each cloud product on its corresponding dashboard.

> Note:
>
> - By default, CloudMonitor displays the ECS global dashboard and part of your ECS monitoring data.
> - You can add the monitoring data of other cloud products as needed.

Procedure

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select Dashboard and click Custom Dashboard. The Dashboards page is displayed.
3. Select the target dashboard from the Dashboards drop-down list. You can switch the dashboard view by selecting different dashboards.



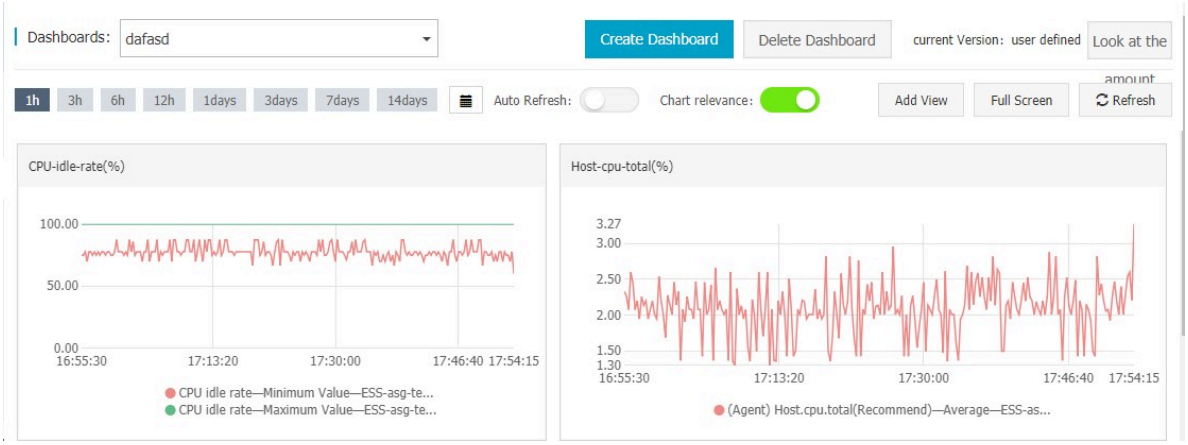
Create a dashboard

You can create a dashboard and customize the view to meet your specific requiremen ts in complex service scenarios.

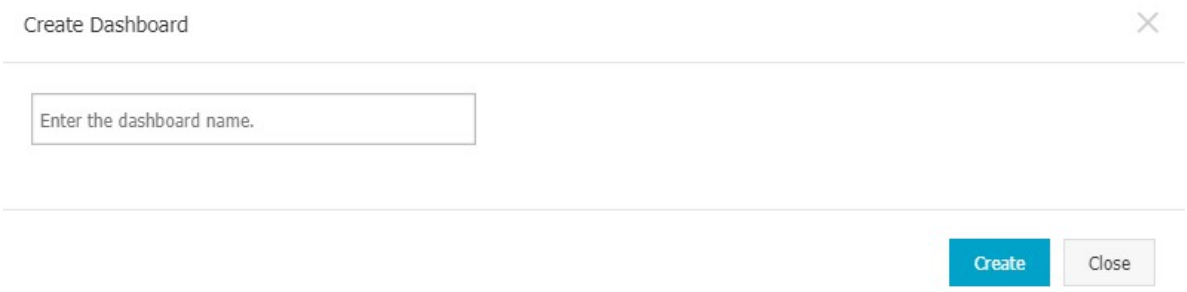
Procedure

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select Dashboard and click Custom Dashboard. The Dashboards page is displayed.

3. In the upper-right corner of the page, click Create Dashboard.



4. Enter the dashboard name and click Create.



5. On the displayed page, add charts as needed.

Add a monitoring chart

You can add major cloud product metrics and your service metrics to the dashboard.

If you use multiple cloud products for your application, you can add the cloud product metrics to the same dashboard by adding a chart, so that you can view the global cloud product monitoring data.

When you report your service monitoring data by using the CloudMonitor API, you can add a chart to display the monitoring data.

Procedure

For details, see #unique_6.

Delete a dashboard

Note:

- When you delete a dashboard, all charts added to it are deleted.
- Monitoring data cannot be restored after you delete it.

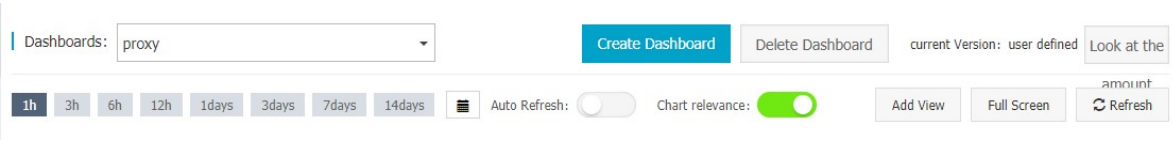
- We recommend that you not delete a dashboard unless necessary.

Procedure

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select Dashboard and click Custom Dashboard. The Dashboards page is displayed.
3. In the upper-right corner of the page, click Delete Dashboard.

Modify a dashboard

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select Dashboard and click Custom Dashboard. The Dashboards page is displayed.
3. Rest the pointer on a dashboard until the Edit button is displayed. Click Edit, enter the new dashboard name, and click OK.



3 Application groups

Application scenarios

- Service-based resource management

  Application groups allow enterprise-level users to categorize resources under their accounts and query monitoring and alarm information by service.
- Inspection and fault detection

  Application groups provide features such as group health measurements, fault lists, and resource dashboards, which allow you to inspect resource usage and quickly locate any faulty resources and determine alarm causes.
- Improved resource usage efficiency

  Application groups can aggregate and display multidimensional monitoring data, helping you query monitoring data from single instances or groups, so that you can quickly locate abnormally high resource usage.

Features

With application groups, you can:

- Manage your cloud resources across products and regions by service.
- Manage all resources in a group by configuring only one alarm rule, helping to improve O&M efficiency.
- Identify faulty instances immediately by checking the fault list.
- Display the charts in a group as required on the application group details page.

Procedure

To create an application group, perform the following steps:

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select Application Groups. The Application Groups page is displayed.
3. In the upper-right corner of the page, click Create Group. The Create Group page is displayed.
4. Enter the product group name and select a contact group.
5. Select an alarm template.

6. Add an instance dynamically. For example, you can add an ECS instance according to the dynamic rule you have created. All instances that are created according to the rule are automatically added to the application group.
7. Add products. The ECS products are initialized by default. You can click Add Product and Delete to specify the product scope.
8. Click Create Application Group.

4 Host monitoring

Application scenarios

- Hybrid cloud monitoring solution

  CloudMonitor uses an agent to collect server monitoring data. You can install the agent on a non-ECS server to perform basic monitoring check both locally and on the cloud.
- Enterprise-level monitoring solution

  Host monitoring provides an application grouping feature with which you can allocate servers in different regions to the same group for business-based server management. In addition, host monitoring provides group-based alarm management. You can configure one alarm rule for the entire group greatly improving O&M efficiency and your overall management experience.

Features

- Diverse metrics

  Once a CloudMonitor agent is installed, you can use more than 30 metrics. For details, see #unique_9.
- Refined collection frequency

  Key metrics are collected every second. All the metrics are reported at a 15-second interval, which is the minimum interval between the data points in a chart.
- Business-level process monitoring

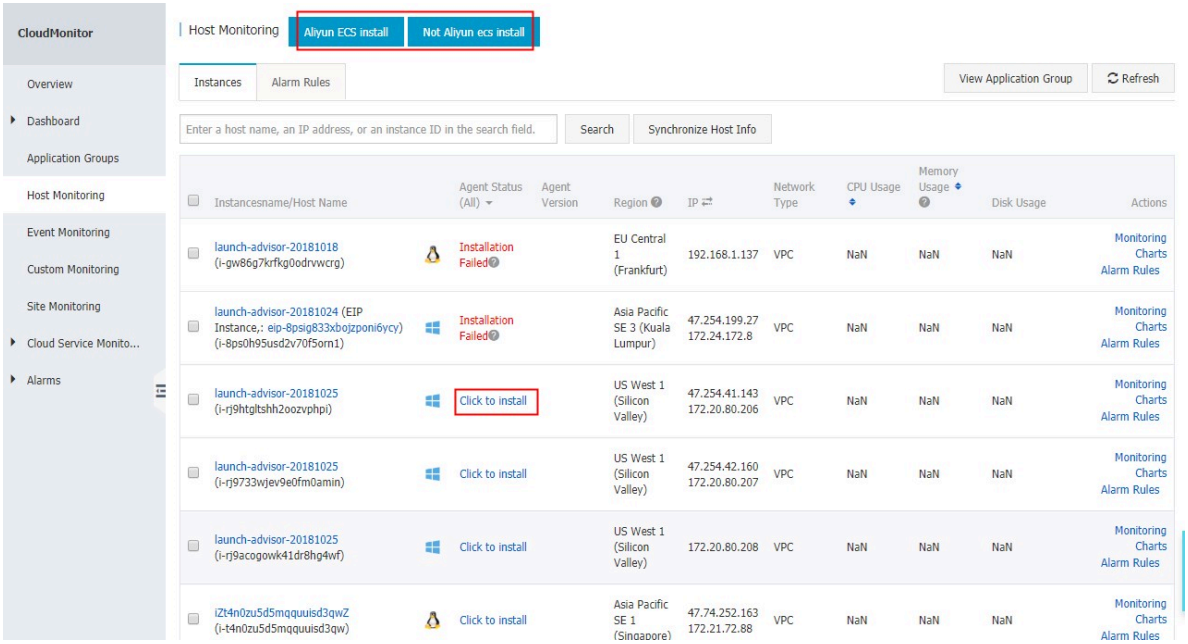
  The host monitoring service collects statistical data from the CPU and memory usage of active processes and the number of opened files, helping you gain insight into server resource allocation. For details, see #unique_10.
- Application groups

  You can manage servers by group across regions and set alarm rules according to group, greatly reducing monitoring management costs.
- Alarm service

  You can set alarm rules for the metrics. The following alarm notification methods are supported: telephone alarms, messages, email IDs, TradeManager, and DingTalk Robot.

Procedure

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, click Host Monitoring. The Host Monitoring page is displayed.
3. Click Click to install in the instance list. Alternatively, click Aliyun ECS install or Not Aliyun ecs install and install the agent manually as prompted.



4. Wait 1 to 3 minutes and click Monitoring Charts to view the monitoring data.

5 Custom monitoring

Application scenarios

Custom monitoring allows you to customize metrics and alarm rules.

You can monitor service metrics as needed and report monitoring data to CloudMonit or. CloudMonitor then processes the data and, if the metric thresholds are met or exceeded, generates alarms according to the results.

The difference between event monitoring and custom monitoring is as follows:

- Event monitoring is used to report and query singular event monitoring data and generate alarms if needed.
- Custom monitoring is used to report and query time series monitoring data collected periodically and generate alarms if needed.

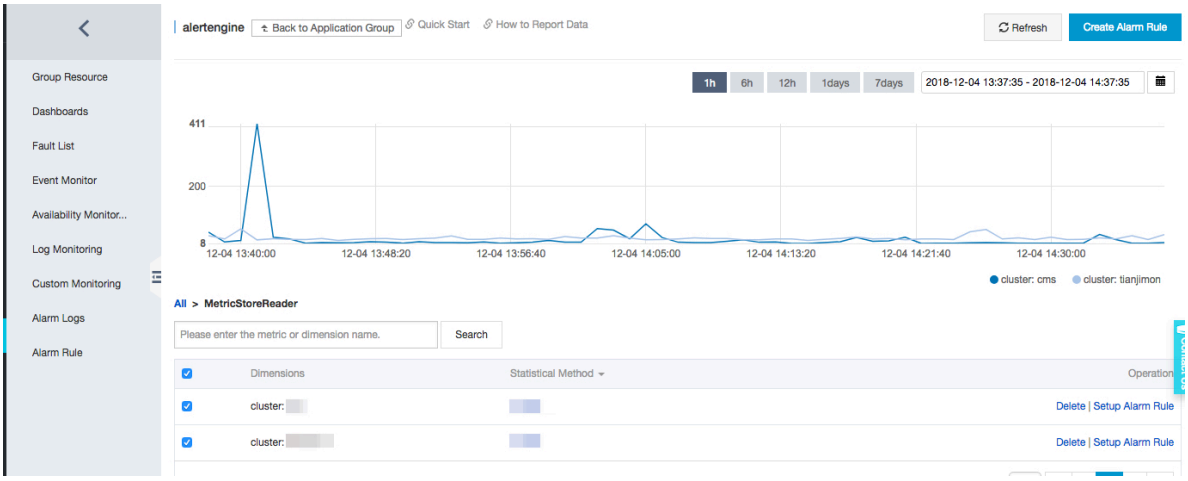
Report monitoring data

For more information, see Report monitoring data.

Query monitoring data

To view custom monitoring data, follow these steps:

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click Application Groups.
3. Find the target application group and click the group name.
4. In the left-side navigation pane, click Custom Monitoring.
5. On the displayed page, click the target metric name.
6. Select the time series you want to view.



Set an alarm rule

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click Application Groups.
3. Find the target application group and click the group name.
4. In the left-side navigation pane, click Custom Monitoring.
5. Click the target metric name and then select the target time series.
6. Click Setup Alarm Rule in the Operation column.
7. On the displayed Create Alarm Rule page, enter a name for the alarm rule and select the corresponding metric, dimension, alarm policy, and notification method.

6 Site monitoring

Application scenarios

Site monitoring is used to simulate actual user access to test availability, connectivity , and DNS resolution.

With site monitoring, you can monitor domain names, IP addresses, port connectivity , and access response time, and set alarms based on results.

Create a monitoring site

1. Log on to the CloudMonitor console.
2. Click Site Management in the left-side navigation pane to enter the Site Monitoring page.
3. Click Create a Monitoring Site in the upper-right corner of the page.
4. Enter required information on the page for creating a monitoring site.

View data of a monitoring site

1. Log on to the CloudMonitor console.
2. Click Site Management in the left-side navigation pane to enter the Site Monitoring page.
3. Click the name of a monitoring site in the monitoring site list or click Monitoring Chart in the Actions column.
4. View site monitoring details.

Delete a monitoring site

1. Log on to the CloudMonitor console.
2. Click Site Management in the left-side navigation pane to enter the Site Monitoring page.
3. Select the monitoring site to be deleted in the monitoring site list.
4. Click the Batch Delete button under the list to delete the monitoring site.

Set alarm rules

1. Log on to the CloudMonitor console.
2. Click Site Management in the left-side navigation pane to enter the Site Monitoring page.

3. **Click Alarm Rules in the Actions column in the monitoring site list to enter the page for setting alarm rules.**

7 Cloud service monitoring

With cloud service monitoring, you can query the performance metrics of the purchased cloud service instances. This information can help you analyze the resource utilization and business trend statistics, allowing you to quickly detect and diagnose system problems.

CloudMonitor supports the following products:

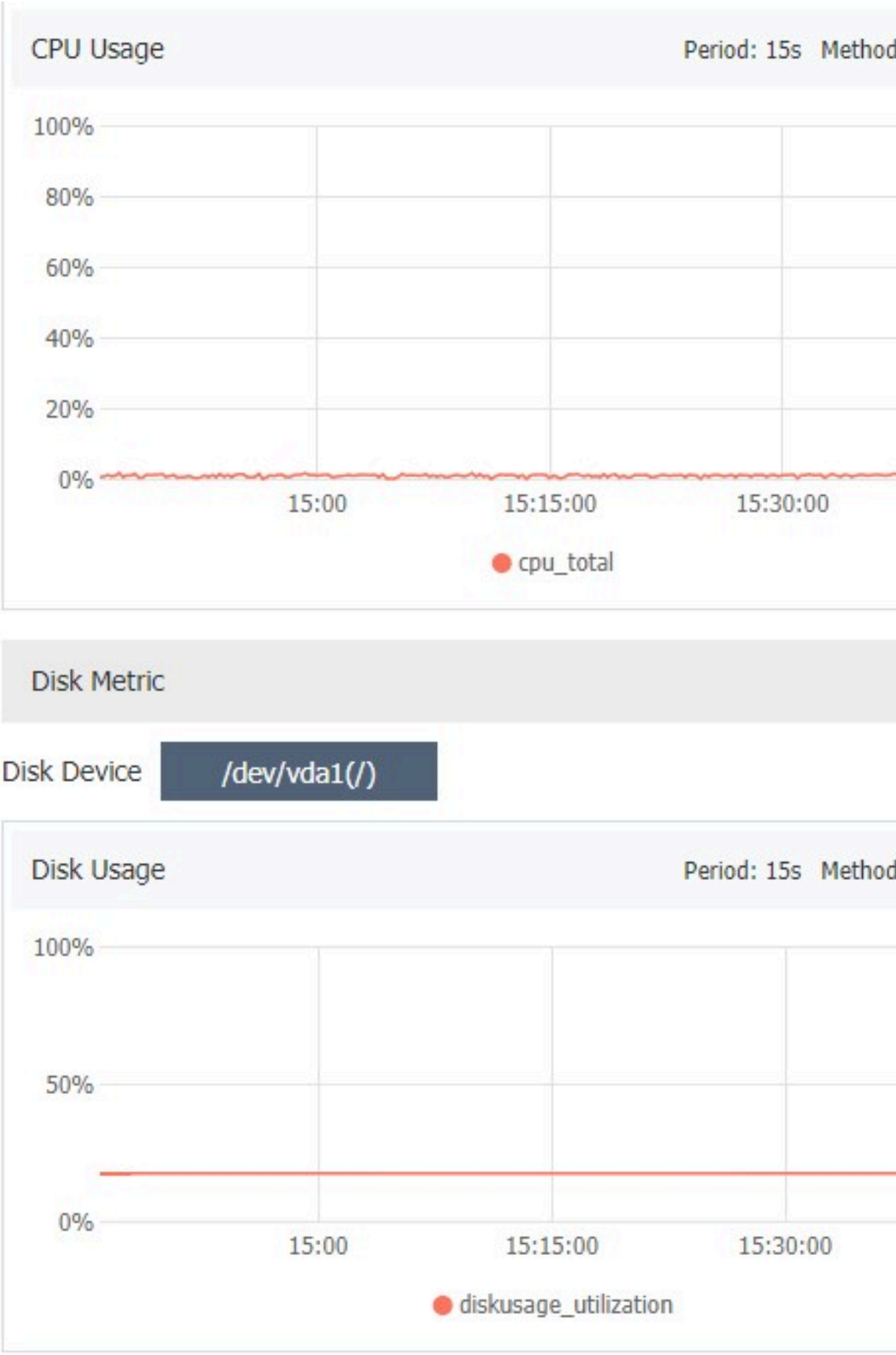
- Host Monitoring
- ApsaraDB for RDS
- Server Load Balancer
- Object Storage Service
- Alibaba Cloud CDN
- Elastic IP Address
- Express Connect
- NAT Gateway
- ApsaraDB for Memcache
- ApsaraDB for MongoDB
- ApsaraDB for Redis
- Analytic DB
- HiTSDB
- Message Service
- Log Service
- Container Service
- API Gateway
- E-MapReduce
- Auto Scaling
- ApsaraDB for PetaData
- ApsaraDB for HybridDB
- Openad
- Function Compute

Procedure

1. Log on to the CloudMonitor Console.

2. In the left-side navigation pane, select Cloud Service Monitoring, and click the product you want to view. To view the ECS instances, select Host Monitoring.
3. Click an instance name or click Monitoring Charts in the Actions column to access the instance monitoring details page.

4. **View the instance monitoring details.**



8 Alarm service

Application scenarios

The CloudMonitor alarm service generates alarms during data monitoring. You can set alarm rules to specify how the alarm system checks data and how it sends alarm notifications when alarms are triggered.

By setting alarm rules for important metrics, you can monitor for, and immediately handle, any system exceptions.

Note:

- Alarm rules have a default mute period of 24 hours, so that, if an exception occurs , only one alarm notification will be sent in the first 24 hours so to avoid sending unnecessary alarms.
- By default, CloudMonitor adds the contact name specified during account registration as the alarm contact and creates an alarm contact group for this alarm contact.

Features

With the CloudMonitor alarm service, you can:

- Set alarm rules for any of the metrics of CloudMonitor.
- Set alarm rules for instances, application groups, and all resources.
- Set the alarm rule effective period customizing the period of time where an alarm rule takes effect.
- Set the notification methods for different channels and customize the subject and remarks for an email notification.

Procedure

1. Log on to the CloudMonitor console.
2. Add one or more contacts and contact groups. For more information, see Manage alarm contacts and alarm contact groups.
3. Create one or more alarm rules as required. For more information, see #unique_39.