Alibaba Cloud Elasticsearch

Monitoring Alarms

Issue: 20190723

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 ES CloudMonitor alarm

Alibaba Cloud Elasticsearch supports instance monitoring and allows text message alerting. You can set the alerting thresholds according to your needs.

Important

It is strongly recommended to configure monitoring alerts.

- Cluster status (whether the cluster status indicator is green or red)
- Node disk usage (%) (alerting threshold must be lower than 75%, and cannot exceed 80%)
- Node HeapMemory usage (%) (alerting threshold must be lower than 85%, and cannot exceed 90%)

Other requirements

- Node CPU usage (%) (alerting threshold cannot exceed 95%)
- Node load_1m (reference value: 80% of the number of CPU cores)
- Cluster query QPS (Count/Second) (reference value: practical test result)
- Cluster write QPS (Count/Second) (reference value: practical test result)

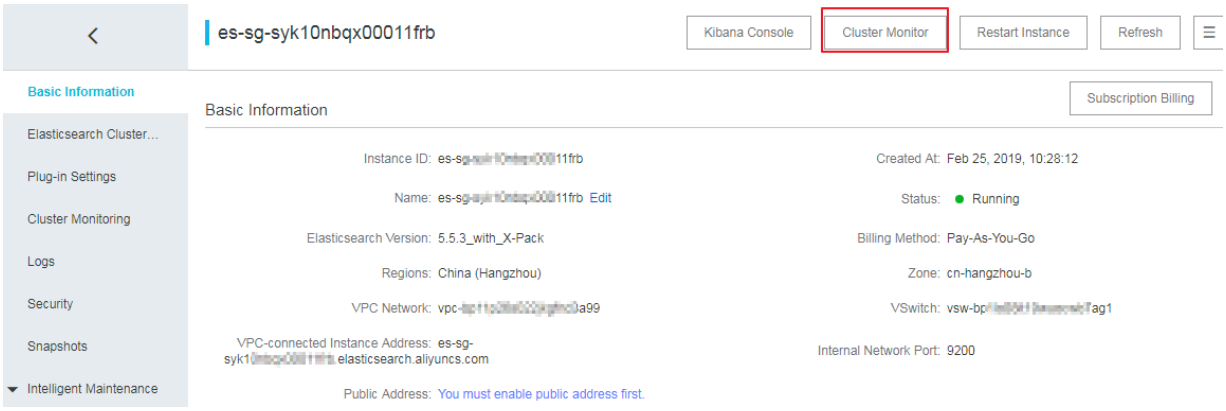
Instructions for use

Enter mode

- Elasticsearch console
- CloudMonitor Elasticsearch tab page

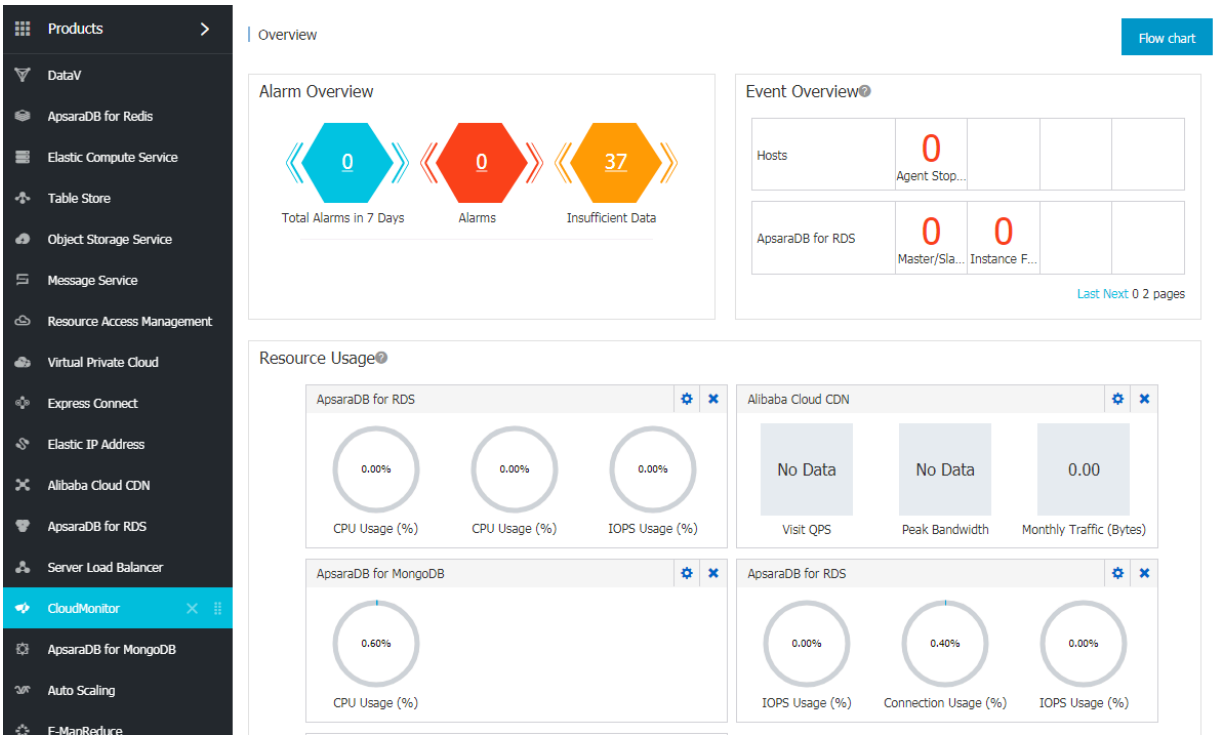
Elasticsearch console

Log on to the ES console and go to the ES instance basic information page. Click Cluster Monitor to go to the ES Cloud Monitor module.



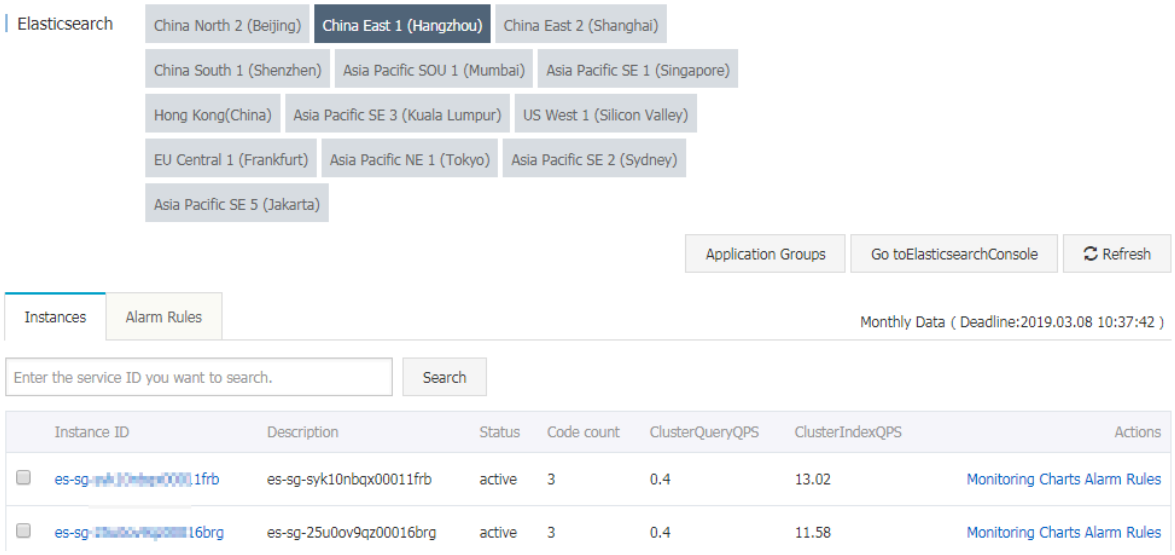
Cloud Monitor Elasticsearch tab

Log on to the Alibaba Cloud console using your account, select Cloud Monitor in the product navigator, and choose Elasticsearch from the cloud service monitor menu.



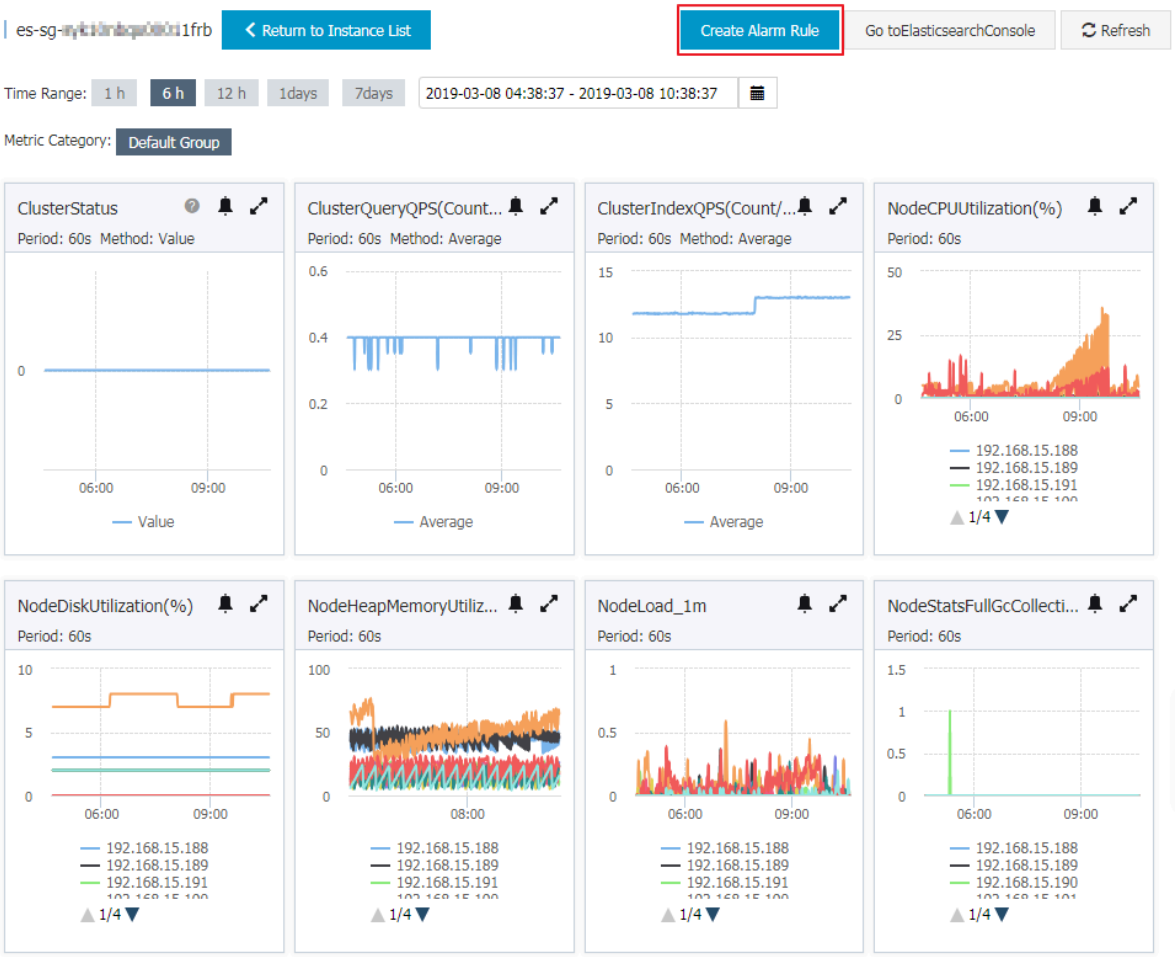
Monitor index configuration

1. Choose the area you want to check and click the ES instance ID.



2. Create alert policies on the index details page.

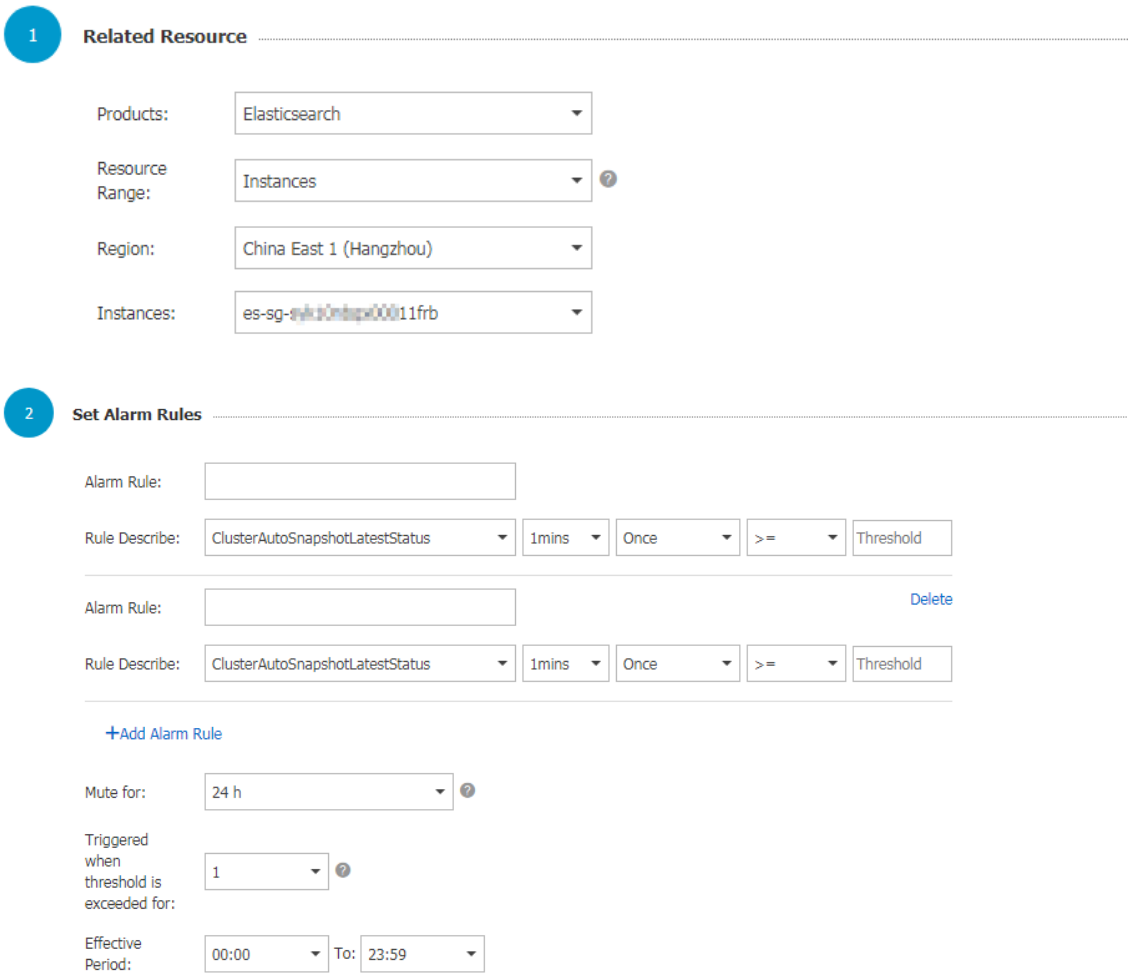
   On this page, you can check the historical cluster monitoring statistics. The monitoring statistics of the past month are stored. After creating alert policies, you can configure alert monitoring for this instance.



3. Enter the policy name and description.

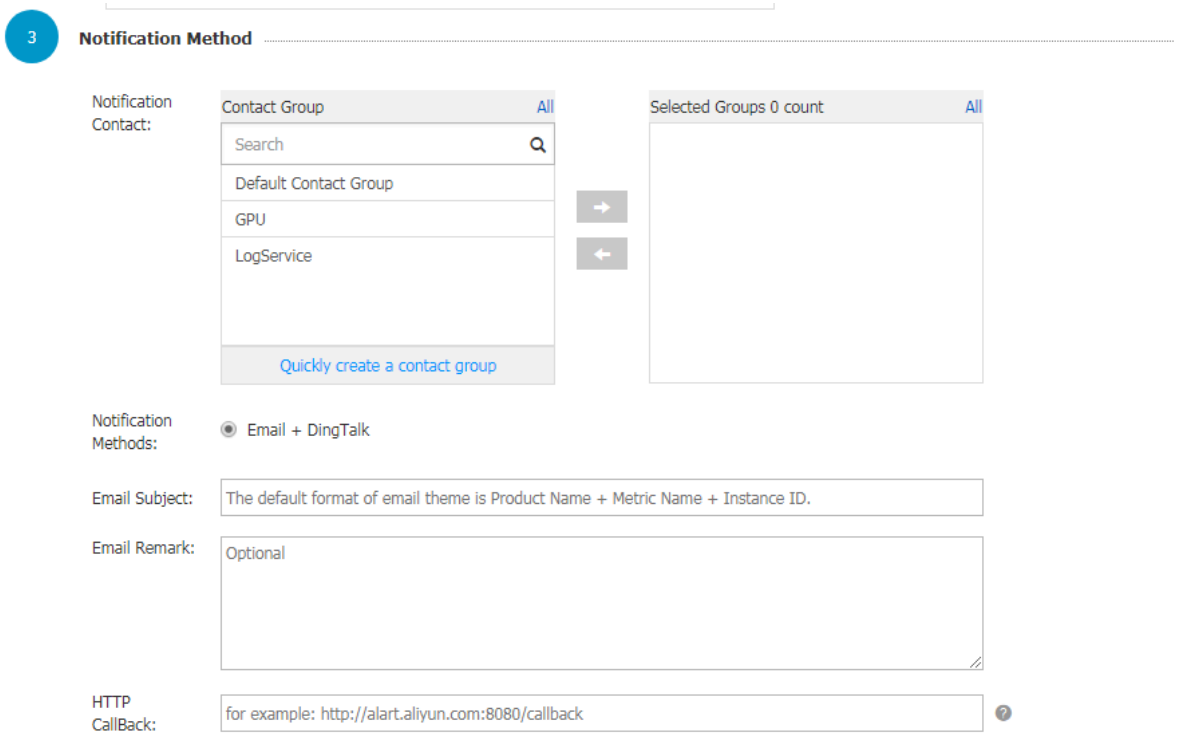
   In the following example, the monitoring on disk usage, cluster status, and node HeapMemory usage is configured.

   - The cluster status green, yellow, and red match `0.0`, `1.0`, and `2.0`, respectively. Set the values to configure the cluster status alert indexes.
   - Within the channel silence time, one index can trigger alerting only once.

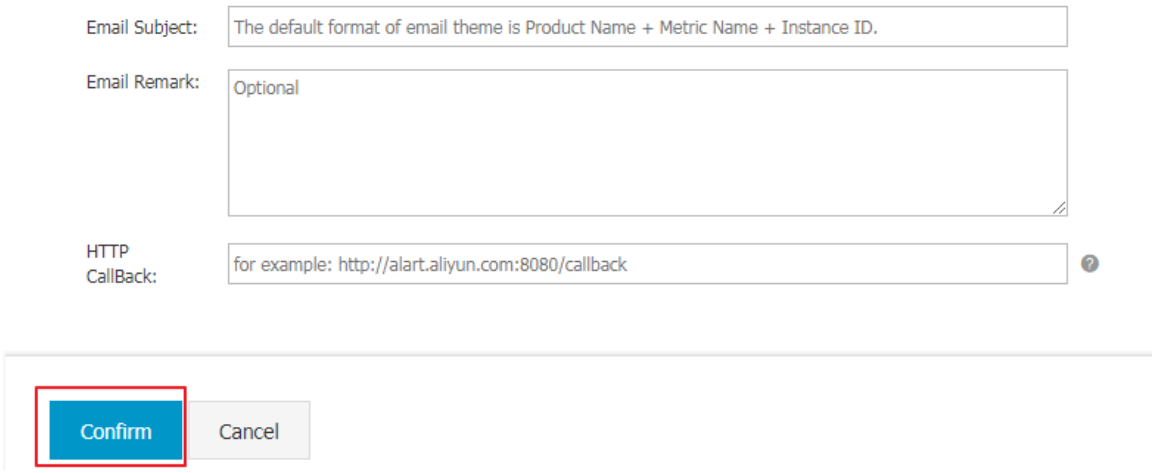


4. Select the alert contact group.

   To create a contact group, click Quickly create a contact group.



5. Click Confirm to save the alert settings.



Note:

Elasticsearch monitoring data is collected five minutes after the instance runs properly. Then the monitoring statistics are displayed.

2 X-Pack Watcher

This topic describes how to configure X-Pack Watcher. With X-Pack Watcher, you can use a watch to trigger specific actions. For example, you can create a watch to search the `logs` index for `errors` and then send alerts through emails or DingTalk messages. X-Pack Watcher is a monitoring and alerting service based on Elasticsearch.

 **Notice:**
X-Pack Watcher can be applied to Alibaba Cloud Elasticsearch instances deployed in only one zone. It does not support Elasticsearch instances deployed across multiple zones.

Features

X-Pack Watcher allows you to create watches. A watch consists of a `Trigger` , `Input` , `Condition` , and `Actions` .

- `Trigger`

  Determines when the watch is executed. All watches must have a trigger. X-Pack Watcher allows you to create various types of triggers. For more information, see Schedule Trigger.

- `Input`

  Loads data into the payload of a watch. Inputs are used as filters to match the specified type of index data. For more information, see Inputs.

- `Condition`

  Controls whether the actions of a watch are executed.

- `Actions`

  Determines the actions to be executed when the specified conditions are met.

Procedure

X-Pack Watcher of Alibaba Cloud Elasticsearch cannot directly access the Internet. To use this feature, you must purchase an Alibaba Cloud ECS instance that can access the Internet and Alibaba Cloud Elasticsearch. The ECS instance is used as a proxy

to perform actions. X-Pack Watcher uses the private network address of the ECS instance to communicate in a VPC network.

The following example shows how to use a Webhook action to connect the DingTalk Chatbot to your service.

1. Purchase an Alibaba Cloud ECS instance.

   The purchased ECS instance must meet the following requirements:

   Notice:

   - The ECS instance must be in the same region and VPC network as your Alibaba Cloud Elasticsearch instance.
   - The ECS instances must have access to the Internet.

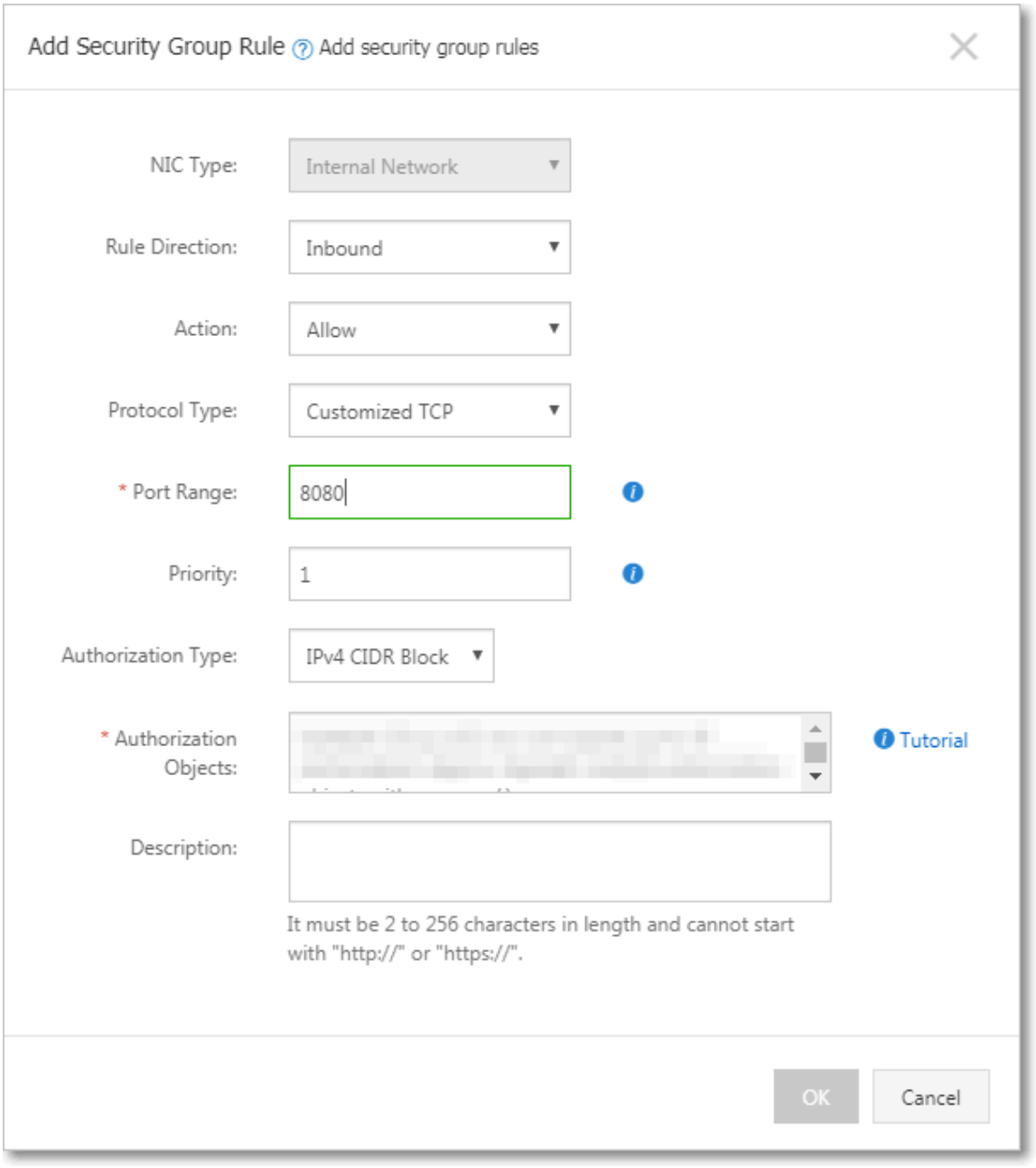
2. Configure a security group

   a. On the Instances page of the Alibaba Cloud ECS console, click More on the right side of the ECS instance, and then select Network and Security Group > Configure Security Group.

   b. In the Security Groups list, click Add Rules in the Actions column.

   c. On the Security Group Rules page, click Add Security Group Rule.

   d. Set the parameters, and click OK to complete the configuration.



   - Set the Rule Direction to Ingress.
   - Use the default Action setting: Allow.
   - Set the Protocol Type to Customized TCP.

- Use the default Priority setting.
- Set the Port Range to your frequently used port. This port is required for NGINX configuration. In this example, port 8080 is specified.
- Set the Authorization Type to IPv4 CIDR Block.
- In the Authorization Objects field, enter the IP addresses of all nodes in your Alibaba Cloud Elasticsearch instance.

> **Note:**
> You can use the following method to query the IP addresses of the nodes.
>
> Log on to the Kibana console of the Alibaba Cloud Elasticsearch instance, click Monitoring in the left-side navigation pane, and then click Nodes.

3. Configure an NGINX proxy.

   a. Modify the NGINX configuration file. Reference the following configuration and then replace the `server` configuration in Install and configure NGINX with this configuration.

```
server
 {
    listen   8080 ;# Listening   port
    server_nam  e   localhost ;# Domain   name
    index   index . html   index . htm   index . php ;
    root  / usr / local / webserver / nginx / html ;# Website
directory
      location  ~ . *\.( php | php5 )? $
   {
     # fastcgi_pa  ss   unix :/ tmp / php - cgi . sock ;
      fastcgi_pa  ss   127 . 0 . 0 . 1 : 9000 ;
      fastcgi_in  dex   index . php ;
      include   fastcgi . conf ;
   }
    location  ~ . *\.( gif | jpg | jpeg | png | bmp | swf | ico
)$
   {
      expires   30d ;
 #  access_log   off ;
   }
    location  / {
      proxy_pass   Enter   the   Webhook   address   of   the
DingTalk   Chatbot   here
   }
    location  ~ . *\.( js | css )? $
   {
      expires   15d ;
  #  access_log   off ;
    }
    access_log   off ;
 }
```

```
}
```

b. After you complete the replacement, reload the NGINX configuration file and then restart NGINX.

```
/ usr / local / webserver / nginx / sbin / nginx  - s   reload
         #  Reload   the   NGINX   configurat  ion   file
/ usr / local / webserver / nginx / sbin / nginx  - s   reopen
         #  Restart   Nginx
```

Note:

You can use the following method to query the Webhook address of the DingTalk Chatbot.

Create an alert contact group in DingTalk. Click the DingTalk group, click the More icon in the upper-right corner, click ChatBot, and select Custom to add a Webhook ChatBot. You can then view the Webhook address of the ChatBot.

4. Create a watch.

Log on to the Kibana console of your Alibaba Cloud Elasticsearch instance. In the left-side navigation pane, click Dev Tools, and then call the corresponding API operation to create a watch in the Console.

The following example shows how to create a watch named `log_error_ watch` to search the `logs` index for `errors` at an interval of `10s`. If more than `0` errors are found, an alert is triggered.

```
 PUT   _xpack / watcher / watch / log_error_  watch
{
  " trigger ": {
    " schedule ": {
      " interval ": " 10s "
    }
  },
  " inputs ": [
    " search ": {
      " request ": {
        " indices ": [" logs "],
        " body ": {
          " query ": {
            " match ": {
              " message ": " error "
            }
          }
        }
      }
    }
  },
  " condition ": {
    " compare ": {
      " ctx . payload . hits . total ": {
        " gt ":  0
```

```
      }
    }
  },
  " actions " : {
  " test_issue " : {
    " webhook " : {
      " method " : " POST ",
      " url " : " http :// Private IP address of your ECS
   instance : 8080 ",
      " body " : "{\" msgtype \": \" text \", \" text \": { \"
 content \": \" An error has been found . Handle the
 issue immediatel y .\"}}"
    }
  }
}
}
```

Note:

The `url` specified in the `actions` must be the private IP address of the purchased Alibaba Cloud ECS instance that is deployed in the same region and VPC network as your Elasticsearch instance. You must also make sure that you have followed the preceding procedure to create a security group for the ECS instance. Otherwise, Watcher cannot send alerts.

If you no longer need this watch, run the following command to delete the watch.

```
DELETE _xpack / watcher / watch / log_error_ watch
```

FAQ

Issue: An exception occurred while configuring a watch: `No handler found for uri [/ _xpack / watcher / watch / log_error_ watch_2 ] and method [ PUT ]`

Solution: You have not enabled the Watcher feature for your Alibaba Cloud Elasticsearch instance. Follow these steps to enable the Watcher feature.

1. Log on to the Alibaba Cloud Elasticsearch console, and select Instance ID > Cluster Configuration.
2. On the Cluster Configuration page, click Modify Configuration on the right side of YML Configuration.
3. On the YML Configuration page, select Enable for Watcher.

Notice:

After you enable Watcher, the Elasticsearch instance will be restarted. Make sure that your businesses are not adversely affected by the restart process before you confirm the operation.

4. Select the This operation will restart the instance. Continue? check the box, and then click OK.

   It may take up to 30 minutes to restart the Elasticsearch instance. Please wait. After the Elasticsearch instance is restarted, Watcher is enabled.

3 Log monitoring

Alibaba Cloud Elasticsearch provides the open-source Elasticsearch v5.5.3 and the X-Pack Business Edition to the scenarios such as data analysis and data search. A range of features such as enterprise-level rights management, security monitoring alerts, and automatic report generation are built upon open-source Elasticsearch.

Monitoring log configuration

Log collection

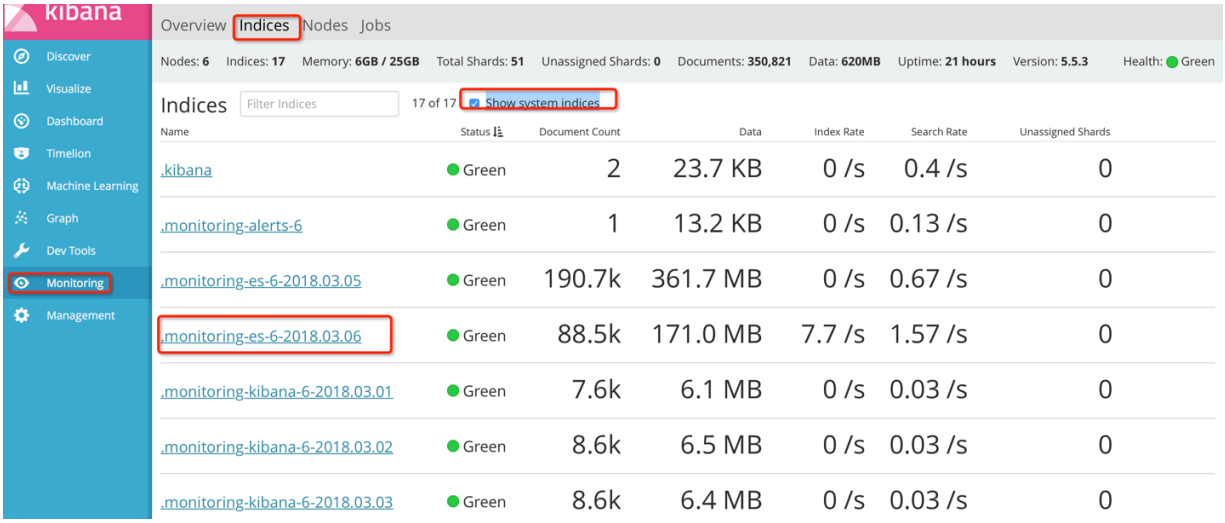
By default, X-Pack monitors clients and sends the collected cluster information every 10 seconds to the index prefixed with `.monitoring-*` of the instance you bought.

The indexes `.monitoring-es-6-*` and `.monitoring-kibana-6-*` are available and created on a daily basis. The collected information is saved in the index prefixed with `.monitoring-es-6-` and suffixed with the current date.

The `.monitoring-es-6-*` index occupies a relatively large disk space. It stores information such as cluster status, cluster statistics, node statistics, and index statistics.

System index display

Select `Show system indices` on the Kibana page to view the space occupied by the index.



Log retention

By default, the monitored indexes of the past seven days are stored. These `.monitoring-es-6-*` indexes occupy the ES instance space. The index size depends on the number of indexes (including system indexes) and the number of nodes in the cluster. To prevent the indexes from occupying most of instance space, use the following methods:

1. Set the index retention days through the following API:

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.history.duration":"1d
"}}
# The number of days shall be configured according
to your requiremen ts. The indexes shall be retained
at least one day.
```

2. Specify the indexes to be monitored.

   You can specify which indexes need to be monitored through the API to reduce the disk space occupied by the `.monitoring-es-6-*` indexes. In the following example, the system indexes are not monitored.

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.collection.indices":
"*,-.*"}}
# The disabled index informatio n is not displayed
in the Monitoring module of Kibana. For example,
you cannot see the disabled index informatio n in
the index list or on the index monitoring page.
In this situation, the index list obtained through
_cat/indices is different from the index list
displayed in the Monitoring module of Kibana.
```

Note:

In practice, you can use both methods to save disk space.