Elasticsearch

Cloud Monitor

Cloud Monitor

ES Cloud Monitor alarm

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

Key requirements

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

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

CloudMonitor Elasticsearch tab

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

Monitor index configuration

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

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.

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.

Select the alert contact group.

To create a contact group, click **Quickly Create a Contact Group**.

Click **OK** to save the alert settings.

> **Note**:
>
> Elasticsearch monitoring data is collected 5 minutes after the instance runs properly. Then the monitoring statistics are displayed.

XPack Watcher

Overview

You can add Watcher to Elasticsearch as a monitoring and alarm service to trigger actions when certain conditions are met. For example, when log indexes contain ERROR, a watch automatically sends an alarm by email or DingTalk.

Features

Watcher supports multiple features, including **Triggers**, **Inputs**, **Conditions**, and **Actions**.

Triggers

Triggers determine the date and time to execute watches. Triggers are required to configure watches. Watcher provides multiple types of schedule triggers. For more information, see Schedule Trigger.

Inputs

You can use inputs to filter indexes monitored by Watcher. For more information, see Inputs.

Conditions

A condition determines whether or not to execute actions.

Actions

Actions are executed when certain conditions are met.

Procedure

Watches in Alibaba Cloud Elasticsearch cannot communicate through the public network. You can only access the internal endpoint of the instance over a VPC network. To use Watcher, you must create an Alibaba Cloud ECS instance that can access both the public network and Alibaba Cloud Elasticsearch instance. The ECS instance runs as a proxy to execute actions.

The following example shows how to configure Webhook actions. This example uses the DingTalk Chatbot.

1. Purchase an Alibaba Cloud ECS instance

Purchase an Alibaba Cloud ECS instance. Make sure that the ECS instance can access the public network.

Note:

- The Alibaba Cloud ECS instance and Elasticsearch instance must share the same VPC network.
- The Alibaba Cloud ECS instance must have access to the public network.

2. Configure a security group

Go to the instances page in the Alibaba Cloud ECS console, click **More** on the right side of the target instance, select Security Group Configuration, and then add a security group rule on the security group list page.

- Set the direction of the rule to Inbound.
- Use the default action of the authorization policy: Allow.
- Set the custom protocol to Custom TCP.
- Use the default priority setting.
- Configure the port range as needed. This example uses port 8080 for Nginx.
- Set the authorization type to CIDR.
- Add IP addresses of all nodes for your Alibaba Cloud Elasticsearch instance as authorization objects.

Obtain an Alibaba Cloud Elasticsearch instance IP address list:

Log on to the Kibana console of the Elasticsearch instance that you have purchased, click Monitoring, and click Nodes to view IP addresses of all nodes for your Elasticsearch instance.

3. Configure a Nginx proxy

1. Modify the Nginx configuration file. The following example shows how to configure the server settings in the Nginx configuration file:

```
server
{
listen 8080;#Listening port
server_name localhost;#Domain name
index index.html index.htm index.php;
root /usr/local/webserver/nginx/html;#Website directory
location ~ . *\.(php|php5)? $
{
#fastcgi_pass unix:/tmp/php-cgi.sock;
fastcgi_pass 127.0.0.1:9000;
fastcgi_index index.php;
include fastcgi.conf;
}
location ~ . *\.(gif|jpg|jpeg|png|bmp|swf|ico)$
{
expires 30d;
# access_log off;
}
location / {
proxy_pass Paste the Webhook address of the DingTalk Chatbot here.
}
location ~ . *\.(js|css)? $
{
expires 15d;
# access_log off;
}
access_log off;
}

}
```

2. After you have configured the Nginx configuration file, reload the configuration file and restart Nginx.

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

> **Obtain the Webhook address of the DingTalk Chatbot:**
>
> Create a DingTalk alarm reception group. Click Group Settings in the upper-right corner, select ChatBot, add a Webhook robot, and then obtain the Webhook address of the robot.

4. Set alarms

1. Log on to the Kibana console of the Elasticsearch instance, and click the left-side Dev Tools tab. The following example shows how to create a watcher named log_error_watch to check whether the log indexes contain ERROR every 10 seconds. Once an error log entry is detected, the watcher triggers an alarm.

```
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:// The private IP address of your ECS instance:8080",
"body" : "{\"msgtype\": \"text\", \"text\": { \"content\": \"An error log entry has been detected. Handle the issue immediately.\"}}"
}
}
}
}
```

Note:

The **URL** in the **actions** must be the internal IP address of your ECS instance that shares the same region and VPC with your Elasticsearch instance. The ECS instance must have been added to a security group that is created by following the steps in this example. Otherwise, the ECS instance cannot communicate with the Elasticsearch instance.

2. You can run the following command to delete a watcher.

DELETE _xpack/watcher/watch/log_error_watch

FAQ

1. No handler has been found for URI

The following error message indicates that the watcher feature has not been enabled for your Elasticsearch instance. You must go to the instance management page in the Alibaba Cloud Elasticsearch console, choose **Advanced Settings** > **YML File**, and then add xpack.watcher.enabled: true.

No handler found for uri [/_xpack/watcher/watch/log_error_watch_2] and method [PUT]

Note:

Currently, Alibaba Cloud Elasticsearch cannot periodically clear .watcher-history indexes. You must manually clear the .watcher-history indexes that you no longer need. You can schedule a task on your ECS instance to call the corresponding API operations to delete indexes.

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

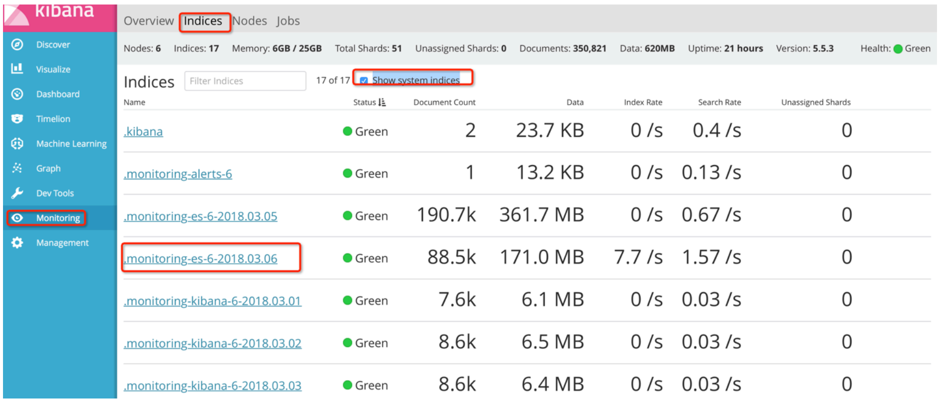
By default, X-Pack monitors clients and sends the collected cluster information every 10 seconds to the index prefixed with .monitoring-* of the instance you bought.

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.



Nodes: 6 Indices: 17 Memory: 6GB / 25GB Total Shards: 51 Unassigned Shards: 0 Documents: 350,821 Data: 620MB Uptime: 21 hours Version: 5.5.3 Health: ● Green

Indices Filter Indices 17 of 17 ☑ Show system indices

Name	Status	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
.kibana	● Green	2	23.7 KB	0 /s	0.4 /s	0
.monitoring-alerts-6	● Green	1	13.2 KB	0 /s	0.13 /s	0
.monitoring-es-6-2018.03.05	● Green	190.7k	361.7 MB	0 /s	0.67 /s	0
.monitoring-es-6-2018.03.06	● Green	88.5k	171.0 MB	7.7 /s	1.57 /s	0
.monitoring-kibana-6-2018.03.01	● Green	7.6k	6.1 MB	0 /s	0.03 /s	0
.monitoring-kibana-6-2018.03.02	● Green	8.6k	6.5 MB	0 /s	0.03 /s	0
.monitoring-kibana-6-2018.03.03	● Green	8.6k	6.4 MB	0 /s	0.03 /s	0

Log retention

By default, the monitored indexes of the past 7 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:

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 requirements. The indexes shall be retained at least one day.
```

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 information is not displayed in the Monitoring module of Kibana. For example, you cannot see the disabled index information 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.