

# Alibaba Cloud Elasticsearch Monitoring Alarms

Issue: 20190326

## 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 ES CloudMonitor alarm.....	1
2 XPack Watcher.....	7
3 Log monitoring.....	12

# 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.

<
es-sg-syk10nbqx00011frb
Kibana Console
Cluster Monitor
Restart Instance
Refresh

Basic Information
Subscription Billing

Elasticsearch Cluster...
Plug-in Settings
Cluster Monitoring
Logs
Security
Snapshots
Intelligent Maintenance

Basic Information

Instance ID: es-sg-syk10nbqx00011frb Created At: Feb 25, 2019, 10:28:12

Name: es-sg-syk10nbqx00011frb Edit Status: ● Running

Elasticsearch Version: 5.5.3\_with\_X-Pack Billing Method: Pay-As-You-Go

Regions: China (Hangzhou) Zone: cn-hangzhou-b

VPC Network: vpc-l2t1t2b2a99 VSwitch: vsw-bp1t2b2a99

VPC-connected Instance Address: es-sg-syk10nbqx00011frb.elasticsearch.aliyuncs.com Internal Network Port: 9200

Public Address: You must enable public address first.

## 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.

Products
>

DataV
ApsaraDB for Redis
Elastic Compute Service
Table Store
Object Storage Service
Message Service
Resource Access Management
Virtual Private Cloud
Express Connect
Elastic IP Address
Alibaba Cloud CDN
ApsaraDB for RDS
Server Load Balancer
CloudMonitor
ApsaraDB for MongoDB
Auto Scaling
E-MapReduce

Overview
Flow chart

Alarm Overview

0 0 37

Total Alarms in 7 Days Alarms Insufficient Data

Event Overview

Hosts	0	Agent Stop...		
ApsaraDB for RDS	0	Master/Sl...	0	Instance F...

Last Next 0 2 pages

Resource Usage

ApsaraDB for RDS
CPU Usage (%) 0.00%
CPU Usage (%) 0.00%
IOPS Usage (%) 0.00%

Alibaba Cloud CDN
Visit QPS No Data
Peak Bandwidth No Data
Monthly Traffic (Bytes) 0.00

ApsaraDB for MongoDB
CPU Usage (%) 0.60%

ApsaraDB for RDS
IOPS Usage (%) 0.00%
Connection Usage (%) 0.40%
IOPS Usage (%) 0.00%

## Monitor index configuration

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

Elasticsearch

China North 2 (Beijing)

**China East 1 (Hangzhou)**

China East 2 (Shanghai)

China South 1 (Shenzhen)

Asia Pacific SOU 1 (Mumbai)

Asia Pacific SE 1 (Singapore)

Hong Kong(China)

Asia Pacific SE 3 (Kuala Lumpur)

US West 1 (Silicon Valley)

EU Central 1 (Frankfurt)

Asia Pacific NE 1 (Tokyo)

Asia Pacific SE 2 (Sydney)

Asia Pacific SE 5 (Jakarta)

Application Groups

Go toElasticsearchConsole

Refresh

Instances

Alarm Rules

Monthly Data ( Deadline:2019.03.08 10:37:42 )

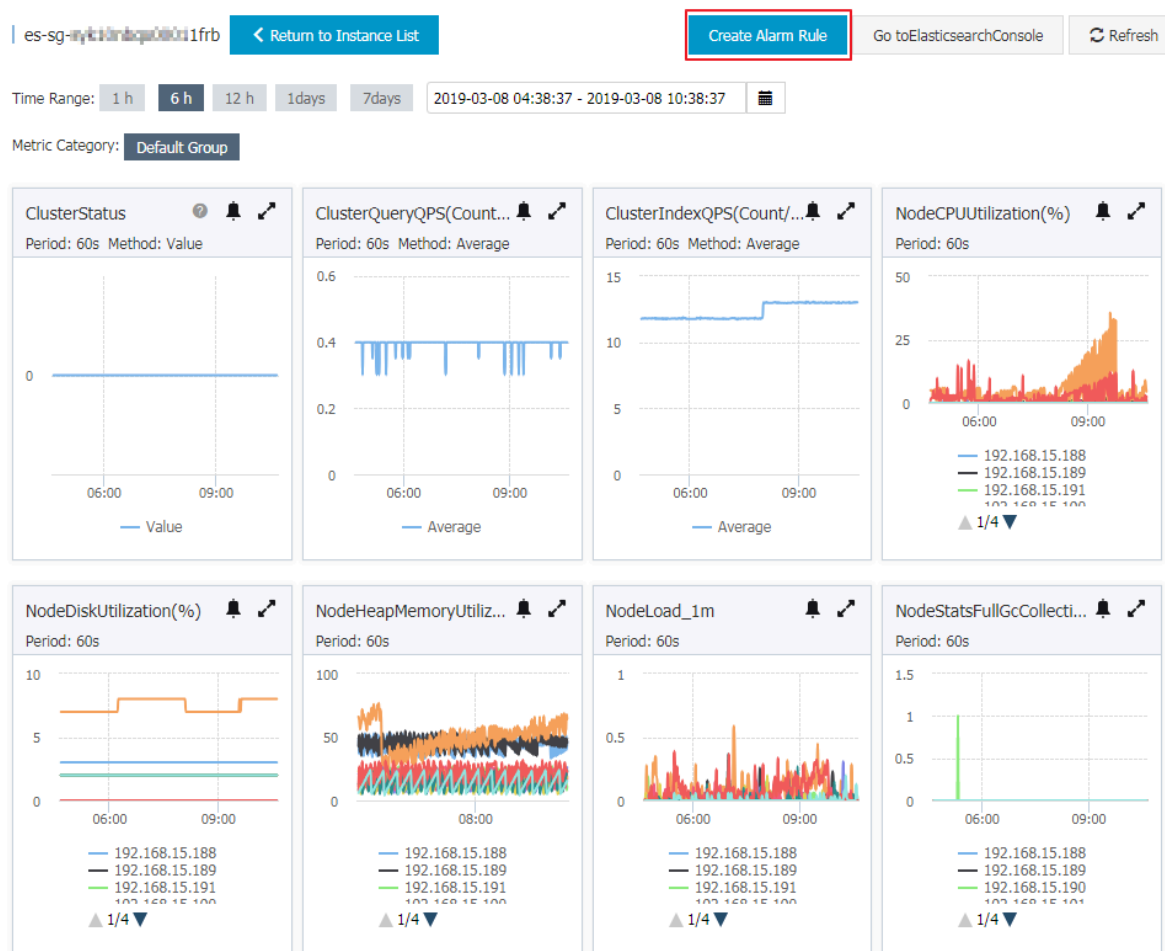
Enter the service ID you want to search.

Search

Instance ID	Description	Status	Code count	ClusterQueryQPS	ClusterIndexQPS	Actions
<input type="checkbox"/> <a href="#">es-sg-10nbnx00011frb</a>	es-sg-syk10nbqx00011frb	active	3	0.4	13.02	<a href="#">Monitoring Charts Alarm Rules</a>
<input type="checkbox"/> <a href="#">es-sg-25u0ov9qz00016brg</a>	es-sg-25u0ov9qz00016brg	active	3	0.4	11.58	<a href="#">Monitoring Charts Alarm Rules</a>

## 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.

1
**Related Resource**

Products: Elasticsearch
Resource Range: Instances
Region: China East 1 (Hangzhou)
Instances: es-sg-xxxxxx00011frb

2
**Set Alarm Rules**

Alarm Rule:
Rule Describe: ClusterAutoSnapshotLatestStatus 1mins Once >= Threshold
Delete
Alarm Rule:
Rule Describe: ClusterAutoSnapshotLatestStatus 1mins Once >= Threshold
+Add Alarm Rule
Mute for: 24 h
Triggered when threshold is exceeded for: 1
Effective Period: 00:00 To: 23:59

#### 4. Select the alert contact group.

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

3

Notification Method

Notification Contact:

Contact Group

All

Search

Default Contact Group

GPU

LogService

Quickly create a contact group

Selected Groups 0 count

All

Notification Methods:

☒ Email + DingTalk

Email Subject:

The default format of email theme is Product Name + Metric Name + Instance ID.

Email Remark:

Optional

HTTP CallBack:

for example: <http://alart.aliyun.com:8080/callback>

#### 5. Click Confirm to save the alert settings.

Email Subject:

The default format of email theme is Product Name + Metric Name + Instance ID.

Email Remark:

Optional

HTTP CallBack:

for example: <http://alart.aliyun.com:8080/callback>

**Confirm**

Cancel

**Note:**

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

## 2 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.

#### Trigger

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.

### Configuration

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.



Note:

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

- a. 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 ;
}
}

```

- b. 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

```



#### Note:

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

- a. 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 ": 2
  " 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\":\"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.

- b. You can run the following command to delete a watcher.

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

**FAQs**

- 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.

## 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

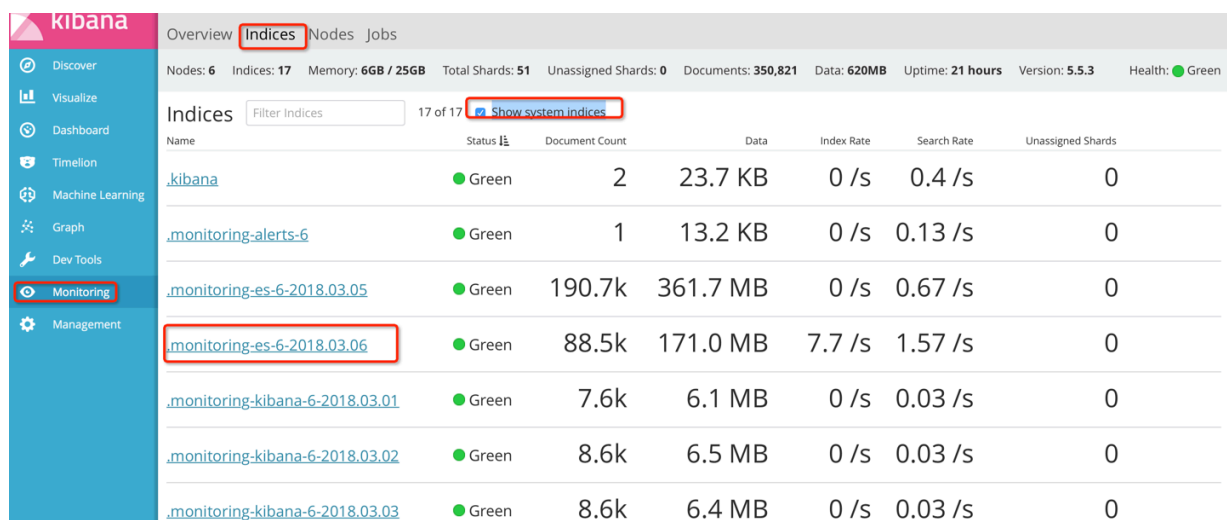
By default, X-Pack monitors clients and sends the collected cluster information every 10 seconds to the index prefixed with `.monitoring-*` of the instance you bought.

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.



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

#### 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 requirements . 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 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.