Elasticsearch

Operation and Maintenance

MORE THAN JUST CLOUD | Alibaba Cloud

Operation and Maintenance

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

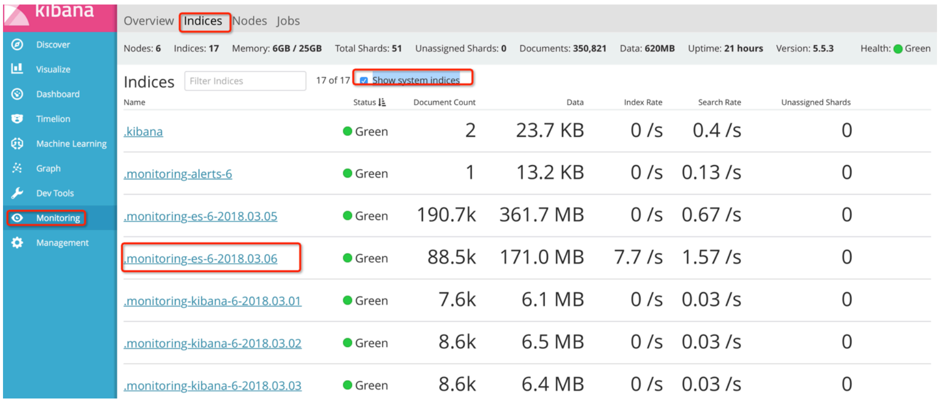
By default, X-Pack monitors clients and sends the collected cluster information every 10 seconds to the index prefixed with .monitoring-* of the instance you bought.

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 17 of 17

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.

Online operation and maintenance

Elasticsearch cluster provides many statistics, in which the cluster health is the most important index. Cluster health has three statuses: Red, Yellow, and Green.

Cluster health can be checked using the following command:

curl -u user name:password http://domain:9200/_cluster/health

Cluster health

Color	Status	Remarks
Red	Some major fragments are unavailable	The cluster contains unavailable major fragments, meaning that one or more indexes have major fragments unassigned.
Yellow	All major fragments are available, but some replicated fragments cannot be used	One or more replicated indexes have major fragments unassigned.
Green	All major and replicated fragments are available	All indexes of the cluster are healthy and all fragments are assigned.

Note:

To ensure that your Elasticsearch cluster status is Green, all major and replicated fragments must be always available.

Therefore, it is recommended that the number_of_replicas be not smaller than amount_Node – 1. Alibaba Cloud Elasticsearch ensures that the restarted cluster status is Green when you use dedicated master.

Troubleshooting

Cluster status is yellow

If the cluster is in the Yellow state, the password change or upgrade operation will take a long time.

You are suggested to perform the operation when the cluster health is in the Green state. The reason why the cluster health status is Yellow is that some replicated fragments of indexes are unassigned.

You need to check the problematic indexes in the cluster.

Index status query command

```
curl -u user name:password http://domain:9200/_cat/indices

# Find out the problematic index name. If the reason is that the number_of_replicas is larger than amount_Node – 1,
# change the number_of_replicas of the problematic index.
```

Index status recovery command

```
curl -XPUT -u user name:password http://domain:9200/problematic index name/_settings -H 'Content-Type:
application/json' -d '{"index":{"number_of_replicas":(amount_Node – 1)}'

# For example, if the number of requested instance nodes is 3 but the number_of_replicas of an index is also 3, the
cluster health status is yellow.
# Change the number_of_replicas of the problematic index to 2.
```

Note:

After finishing the operations (restart/scale-up/custom setting) on the instance, set the number_of_replicas according to the number of instance nodes. This improves the reliability and stability of the Elasticsearch service.