Alibaba Cloud Elasticsearch

User Guide

Issue: 20190830

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 informatio n, 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 Instance management

1.1 Instance management

This topic describes the instance management feature of Alibaba Cloud Elasticsearch, including cluster monitoring, instance restart, refresh, and task list.

Manage instances

Alibaba Cloud Elasticsearch supports the Cluster monitoring, Restart instances, Refresh, and Tasks features for you to manage instances.

es-cn-0pp0wpgz400116mt2
Kibana Console
Cluster Monitor
Restart Instance
Refresh

Cluster monitoring

Alibaba Cloud Elasticsearch supports cluster monitoring and sending alerts to users through SMS messages. You can customize the threshold for triggering alerts. For more information, see CloudMonitor alerts for Elasticsearch.

Restart instances

Alibaba Cloud Elasticsearch allows you to use the restart and force restart methods to restart instances. Follow these guidelines to select an appropriate restart method:

- `Prerequisites` : Before you restart an instance, make sure that the status of the Elasticsearch instance is Active (green flag), the instance has at least one index replica, and the resource usage is not high. You can go to the #unique_6 page to check the resource usage. Ensure that the Node CPU Usage (%) is 80% or lower, the Node Heep Memory Usage (%) is around 50%, and the Node Workload Within One Minute does not exceed the number of cores of the current data node.

  Restart: If the Elasticsearch instance is restarted by this method, it can continuously provide services during the restart process. However, the instance must meet the requirements in Prerequisites. The restart process is time-consuming.

  Notice:

  - Before you restart the instance, make sure that the status of the instance is Active (green flag). Otherwise, you have to use the force restart method to restart the instance.
  - The CPU and memory usage of the Elasticsearch instance will experience a usage spike during the restart process. This may affect the stability of your service for a short period of time.
  - The time that the restart process takes depends on the amount of data stored on the instance, the number of nodes, and the number of indexes and replicas. Elasticsearch cannot estimate the total amount of time required to restart an instance. However, you can check the progress of the restart process in Tasks.

- Force restart: If an Elasticsearch instance is restarted by this method, the services running on the instance may become unstable during the restart process. The restart process takes only a short period of time.

  ! Notice:

  When the disk usage exceeds 85%, the status of the Elasticsearch instance may change to a yellow or red flag. If a yellow or red flag is displayed, you cannot use the restart method to restart the instance. You can only forcibly restart the instance.

  - When a yellow or red flag is displayed, we recommend that you do not perform these operations on the instance: upgrade nodes, upgrade disk space, restart, reset password, and other operations that may change the configuration of the instance. Perform these operations only after the status of the instance changes to a green flag.
  - If you update the configuration of an Elasticsearch instance with a yellow or red flag and the instance contains two or more nodes, the instance will be constantly in the Initializing state. You can submit a ticket to contact the Alibaba Cloud Elasticsearch Technical Support to resolve this issue.

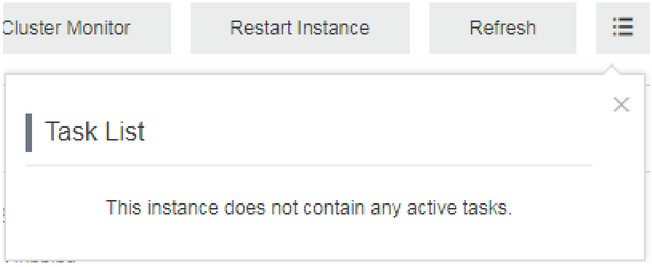
Refresh

You can use this feature to manually refresh the information displayed in the console . For example, if the console fails to display the status of the Elasticsearch instance that you have just created, use the refresh feature to update the status.

Tasks

You can click the Tasks icon to view the progress of tasks, such as the instance creation or restart progress.

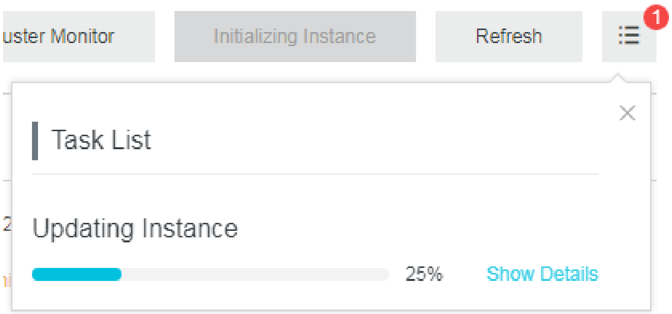
- No task is running on the current instance.



Task List

This instance does not contain any active tasks.

- Tasks that are running on the current instance.

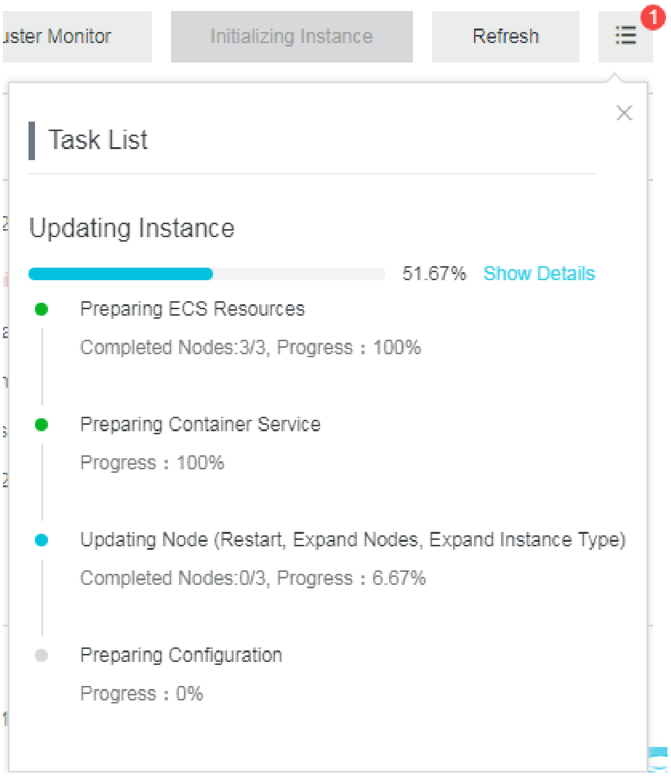


Task List

Updating Instance

25% Show Details

- Show detailed information about a running task.



Task List

Updating Instance

51.67% Show Details

Preparing ECS Resources

Completed Nodes:3/3, Progress：100%

Preparing Container Service

Progress：100%

Updating Node (Restart, Expand Nodes, Expand Instance Type)

Completed Nodes:0/3, Progress：6.67%

Preparing Configuration

Progress：0%

1.2 Basic information

Elasticsearch subscription instances

The following figure shows the information of an Alibaba Cloud Elasticsearch instance that uses the subscription billing method. For parameter descriptions, see the following sections and #unique_10.

- Name: By default, the name of an Alibaba Cloud Elasticsearch instance is the same as its ID. You can edit the name of the instance. You can also search instances by name.
- Internal Network Address: You can use the IP address of a VPC-connected ECS instance to access an Alibaba Cloud Elasticsearch instance.

  > Notice:
  > If you access an Alibaba Cloud Elasticsearch instance through the Internet, data security is not guaranteed. To protect your data, we recommend that you purchase an ECS instance that is connected to the same VPC network as your Elasticsearch instance. You can then use an internal network address to access the Elasticsearch instance.

- Internal Network Port: The following ports are supported:
  - Port `9200` for HTTP and HTTPS.
  - Port `9300` for TCP. Only Alibaba Cloud Elasticsearch 5.5.3 with Commercial Feature supports this port.

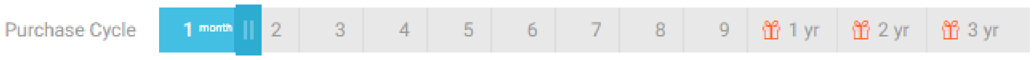
    > Note:
    > You cannot use the transport client to access Alibaba Cloud Elasticsearch 6.3.2 with Commercial Feature and Alibaba Cloud Elasticsearch 6.7.0 with Commercial Feature through port `9300`.

- Public Network Access: You can use public network addresses to access Alibaba Cloud Elasticsearch instances.

- Public Network Port: The following ports are supported:
  - Port `9200` for HTTP and HTTPS.
  - Port `9300` for TCP. Only Alibaba Cloud Elasticsearch 5.5.3 with Commercial Feature supports this port.

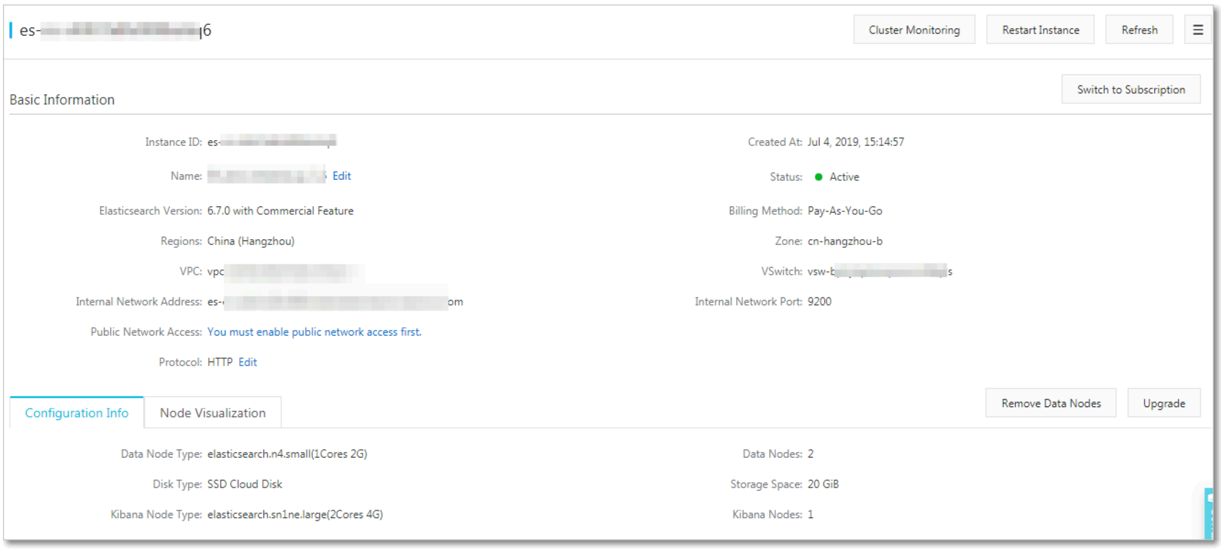
    Note:

    - You cannot use the transport client to access Alibaba Cloud Elasticsearch 6.3.2 with Commercial Feature and Alibaba Cloud Elasticsearch 6.7.0 with Commercial Feature through port `9300`.
    - To access an Elasticsearch instance through the Internet, you must configure the #unique_11/unique_11_Connect_42_section_ux5_yct_zgb. By default, the public network access feature forbids all IP addresses.
- Protocol: By default, HTTP is selected. You can click Edit to change the protocol. Currently, you can choose HTTP or HTTPS. For more information, see #unique_12/unique_12_Connect_42_section_i7x_sqt_enx.
- Renew: You can click Renew on the right side of Basic Information to renew the instance. You can renew your subscription one or more months. The minimum renewal period is one month.



Elasticsearch pay-as-you-go instances

The following figure shows the basic information of an Alibaba Cloud Elasticsearch instance that uses the pay-as-you-go billing method. For parameter descriptions, see Elasticsearch subscription instances and #unique_10.



Basic Information

Instance ID: es-[redacted]
Name: [redacted] Edit
Elasticsearch Version: 6.7.0 with Commercial Feature
Regions: China (Hangzhou)
VPC: vpc[redacted]
Internal Network Address: es-[redacted]om
Public Network Access: You must enable public network access first.
Protocol: HTTP Edit

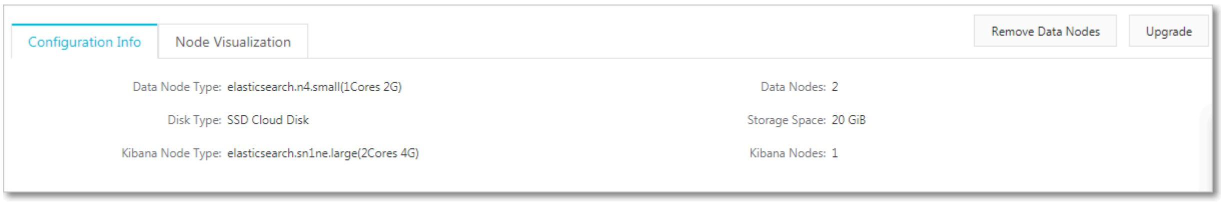
Created At: Jul 4, 2019, 15:14:57
Status: ● Active
Billing Method: Pay-As-You-Go
Zone: cn-hangzhou-b
VSwitch: vsw-b[redacted]s
Internal Network Port: 9200

Data Node Type: elasticsearch.n4.small(1Cores 2G)
Disk Type: SSD Cloud Disk
Kibana Node Type: elasticsearch.sn1ne.large(2Cores 4G)

Data Nodes: 2
Storage Space: 20 GiB
Kibana Nodes: 1

You can switch an Alibaba Cloud Elasticsearch instance from pay-as-you-go to subscription. To perform this task, click Switch to Subscription on the right side of Basic Information, and follow the instructions to switch the billing method.

Configuration information

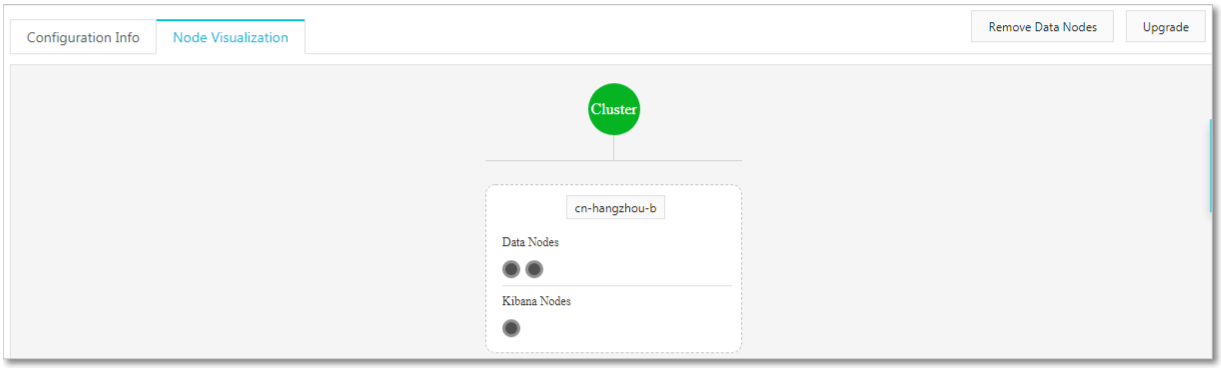


Data Node Type: elasticsearch.n4.small(1Cores 2G)
Disk Type: SSD Cloud Disk
Kibana Node Type: elasticsearch.sn1ne.large(2Cores 4G)

Data Nodes: 2
Storage Space: 20 GiB
Kibana Nodes: 1

For more information about parameter descriptions, see #unique_13.

Node visualization



Remove data nodes

Currently, you can downgrade data nodes for Elasticsearch pay-as-you-go instances and Elasticsearch instances deployed in one zone. Elasticsearch subscription instances and instances deployed across zones are not supported. This function only allows you to remove data nodes from an Alibaba Cloud Elasticsearch instance. You cannot downgrade the specification or disk space of dedicated master nodes, client nodes, and Kibaba nodes. For more information, see #unique_14.

Upgrade

You can upgrade the instance specification, number of nodes, dedicated master node specification, and storage space per data node for an Elasticsearch instance. For more information, see #unique_15.

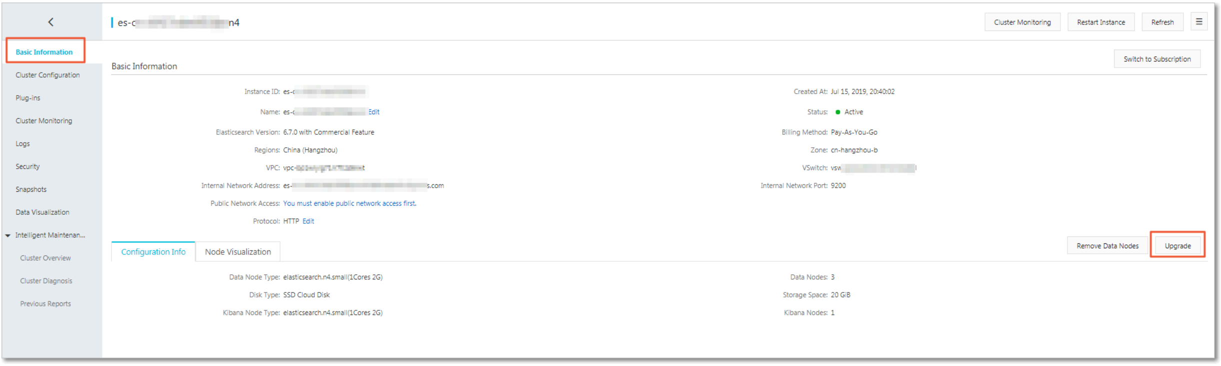
1.3 Cluster upgrade

This topic describes the procedure, guidelines, and restrictions of upgrading an Alibaba Cloud Elasticsearch instance.

Alibaba Cloud Elasticsearch allows you to upgrade the instance specification, number of nodes, dedicated master node specification, number of client nodes, client node specification, number of warm nodes, warm node specification, warm node storage space, and storage space per data node of an Elasticsearch instance.

Note:
You may not be able to upgrade some of the cluster properties due to certain restrictions. For more information, see Configuration upgrade.

Log on to the Alibaba Cloud Elasticsearch console, select Instance ID > Basic Information, and then click Upgrade to navigate to the Update page.



Basic Information

Instance ID: es-c[redacted]
Name: es-c[redacted] Edit
Elasticsearch Version: 6.7.0 with Commercial Feature
Regions: China (Hangzhou)
VPC: vpc-[redacted]
Internal Network Address: es-[redacted]s.com
Public Network Access: You must enable public network access first.
Protocol: HTTP Edit

Created At: Jul 15, 2019, 20:40:02
Status: ● Active
Billing Method: Pay-As-You-Go
Zone: cn-hangzhou-b
VSwitch: vsw[redacted]
Internal Network Port: 9200

Data Node Type: elasticsearch.n4.small(1Cores 2G)
Disk Type: SSD Cloud Disk
Kibana Node Type: elasticsearch.n4.small(1Cores 2G)

Data Nodes: 3
Storage Space: 20 GiB
Kibana Nodes: 1

The Update page includes the Current Config and Configuration Upgrade information. For more information, see Current configuration and Configuration upgrade.

Current configuration

The Current Config section shows the configuration of the current Alibaba Cloud Elasticsearch instance. You can reference the information when you upgrade the instance.

Precautions

Before you upgrade an Elasticsearch instance, pay close attention to the following precautions:

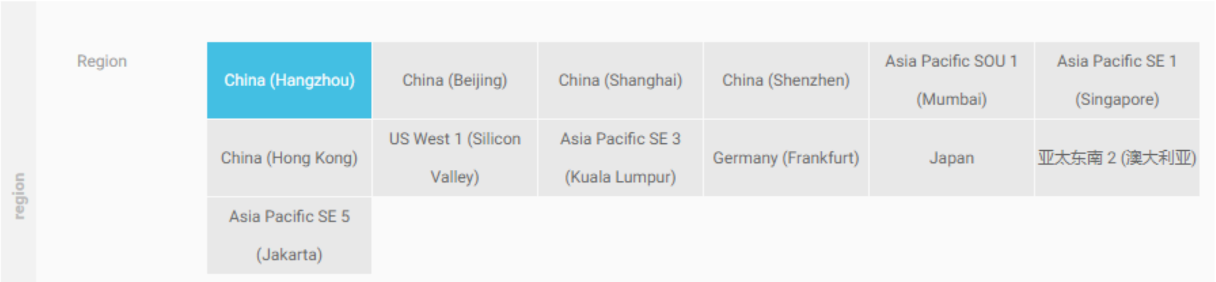
- If you need to upgrade the instance due to business requirements, make an assessment before you upgrade the cluster.
- For each upgrade operation, you can only change one of the upgradable cluster properties.
- Typically, Elasticsearch needs to restart your Elasticsearch instance for the upgrade to take effect. For an Elasticsearch instance with dedicated master nodes, if you change the number of nodes, the instance will not be restarted.
- If the status of your Elasticsearch instance is unhealthy (showing a yellow or red flag), then you must select Force Update to upgrade the instance. Force update may affect your businesses.
- You cannot change the disk type of nodes by upgrading the instance. You can only change the storage space per node.
- Alibaba Cloud Elasticsearch allows you to upgrade the specification of the Kibana node. Fees are charged for upgrading the Kibana node.
- Alibaba Cloud Elasticsearch subscription instances currently do not support downgrading. For example, you cannot remove nodes from clusters, scale in the disk space, or downgrade the node specifications.
- You can downgrade Alibaba Cloud Elasticsearch pay-as-you-go instances by scaling in the number of data nodes. The number of data nodes that you can scale in is restricted. Currently, you cannot perform other downgrade operations. For example, you cannot scale in the disk space or downgrade the node specification.
- After you change the configuration of the instance, you can check the amount of your order on the Update page.
- After you submit the order, your Elasticsearch instance will be billed based on the new configuration.

Configuration upgrade

Notice:

Before you upgrade the configuration of an Elasticsearch instance, make sure that you have read the precautions in Precautions.

You can follow the instructions on the configuration upgrade page to change the configuration of the instance to meet your business requirements. For more information about the parameters, see #unique_18.



region

Region	China (Hangzhou)	China (Beijing)	China (Shanghai)	China (Shenzhen)	Asia Pacific SOU 1 (Mumbai)	Asia Pacific SE 1 (Singapore)
	China (Hong Kong)	US West 1 (Silicon Valley)	Asia Pacific SE 3 (Kuala Lumpur)	Germany (Frankfurt)	Japan	亚太东南 2 (澳大利亚)
	Asia Pacific SE 5 (Jakarta)					

Some of the parameters are described as follows:

- Specification family and instance type

  The Specification Family cannot be changed. If the Specification Family is set to a local disk type, then the Instance Type cannot be changed.
- Dedicated master nodes

  On the Update page, click Yes on the right side of Dedicated Master Node to purchase dedicated master nodes. You can upgrade the specification of the purchased dedicated master nodes. By default, three dedicated master nodes are purchased. Each dedicated master node has 2 cores, 8 GB of memory, and a cloud disk of 20 GiB. After you upgrade the dedicated master nodes, the Elasticsearch instance will be billed based on the new configuration.

  Note:

  If you have purchased 1-core 2 GB dedicated master nodes, then you can repurchase dedicated master nodes of higher specifications on the Update page. The Elasticsearch instance will be billed based on the new configuration. If your dedicated master nodes are free nodes provided by Elasticsearch, then after you upgrade these nodes, we will start charging these nodes.

- Client nodes

  On the Update page, click Yes on the right side of Client Node to purchase client nodes. You can upgrade the specification of the purchased client nodes. By default, two client nodes are purchased. Each client node has 2 cores, 8 GB of memory, and a cloud disk of 20 GiB. After you upgrade the client nodes, the Elasticsearch instance will be billed based on the new configuration.
- Warm nodes

  On the Update page, click Yes on the right side of Warm Node to purchase warm nodes. You can upgrade the specification of the purchased warm nodes. By default, two warm nodes are purchased. Each warm node has 2 cores, 8 GB of memory, and a cloud disk of 500 GiB. After you upgrade the warm nodes, the Elasticsearch instance will be billed based on the new configuration.
- Kibana node

  On the Update page, click Yes on the right side of Kibana Node to purchase a Kibana node. You can upgrade the specification of the purchased Kibana node. By default, the Kibana node has two cores and 4 GB of memory.

  > ❗ Notice:
  > After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch provides you a free Kibana node with 1 core and 2 GB of memory. After you upgrade the Kibana node, the Elasticsearch instance will be billed based on the new configuration.
- Force update

  If the status of your Elasticsearch instance is unhealthy (showing a red or yellow flag), then your businesses have been severely affected. You must upgrade the instance immediately. You can select Force Update to ignore the status of the Elasticsearch instance and forcibly upgrade the instance. The upgrade process only takes a short period of time.

  > ❗ Notice:
  >
  > - The Elasticsearch instance needs to restart to complete the force update process.
  > - During the force update process, the services running on the Elasticsearch instance may become unstable.

- If you do not select Force Update, the restart method is used to upgrade the instance by default. For more information, see #unique_19/unique_19_Connect_42_section_p5n_ccm_zgb.
- If the status of your Alibaba Cloud Elasticsearch instance is not healthy (a red or yellow flag), then the system will automatically select Force Update for you. Elasticsearch will not use the restart method to upgrade the instance.

- Node storage

  The storage space of nodes is measured in GiB. A standard SSD disk can provide up to 2,048 GiB (2 TiB) of storage space.

  You can scale out an ultra disk to up 2 TiB. When you purchase an ultra disk, you can set the storage space to up to 5,120 GiB (5 TiB). Ultra disks larger than 2,048 GiB include 2,560 GiB, 3,072 GiB, 3,584 GiB, 4,096 GiB, 4,608 GiB, and 5,120 GiB.

1.4 Elasticsearch cluster configuration

Word splitting

This feature uses the synonym dictionary. New indexes will use the updated synonym dictionary. For more information, see #unique_21.

Word Splitting

Upload Synonym Dictionary: None

Note:

- After you upload and submit a synonym dictionary file, the Alibaba Cloud Elasticsearch instance will not restart immediately. It takes some time for the new configuration to take effect.
- If an index that is created before the uploaded synonym dictionary file takes effect needs to use synonyms, you must recreate the indexes and configure synonyms.

Write one synonym expression in each row and save the code as a `UTF - 8` encoded `. txt` file. Examples:

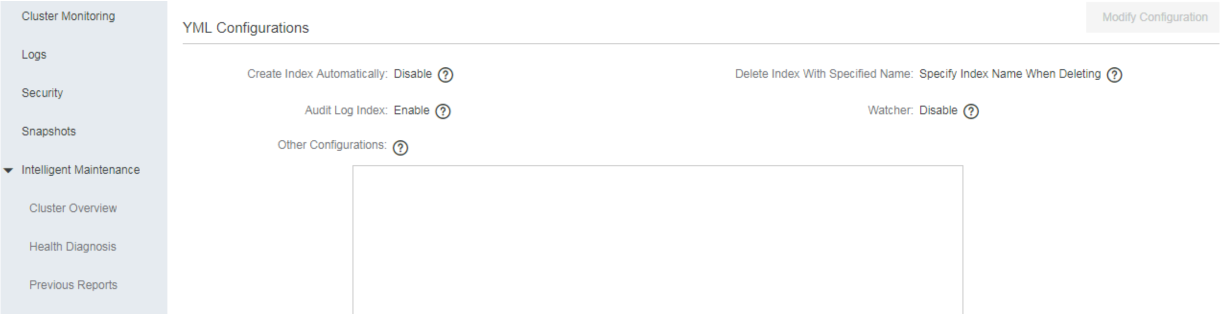
```
corn , maize => maize , corn
begin , start => start , begin
```

Configuration procedure:

1. Upload and save a synonym dictionary file in the Alibaba Cloud Elasticsearch console. Make sure that the uploaded file takes effect.
2. When you create an index and configure the `settings`, you need to specify the `"synonyms_path":"analysis/your_dict_name.txt"` path. Add a `mapping` for this index to configure synonyms for the specified field.
3. Confirm the synonyms and upload a file for testing.

YML configurations

The YML Configurations page displays the settings of the current Alibaba Cloud Elasticsearch instance.



YML Configurations

Create Index Automatically: Disable

Delete Index With Specified Name: Specify Index Name When Deleting

Audit Log Index: Enable

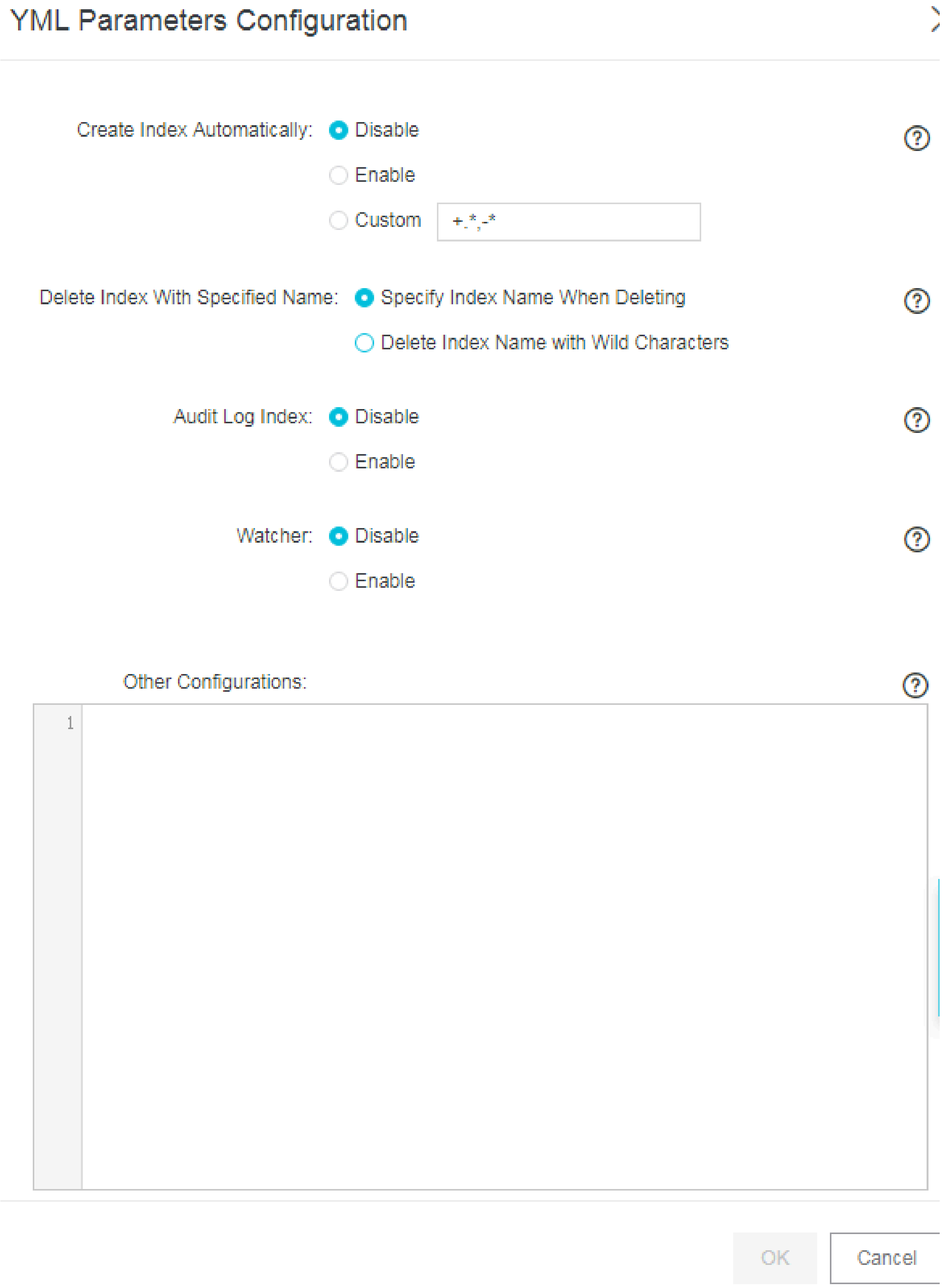
Watcher: Disable

Other Configurations:

Modify YML configurations

After you modify the YML Configurations, you must restart the Alibaba Cloud Elasticsearch instance for the new configuration to take effect.

> Note:
> After you modify the YML Configurations, select This operation requires a restart of the instance. Exercise with caution. at the bottom of the page and click OK. The Alibaba Cloud Elasticsearch instance automatically restarts.



YML Parameters Configuration

Create Index Automatically: ● Disable ○ Enable ○ Custom +.*,-*

Delete Index With Specified Name: ● Specify Index Name When Deleting ○ Delete Index Name with Wild Characters

Audit Log Index: ● Disable ○ Enable

Watcher: ● Disable ○ Enable

Other Configurations:

- Create Index Automatically: if you enable this feature, it allows the system to automatically create new indexes if a new file is uploaded to the Alibaba Cloud Elasticsearch instance and no indexes have been created on the file. We recommend that you disable this feature. Indexes created by this feature may not meet your requirements.

- Delete Index With Specified Name: this feature indicates whether you are required to specify the name of the index that you need to delete. If you select Delete Index Name with Wild Characters, you can delete multiple indexes by using a wildcard character. Indexes that are deleted cannot be restored. Proceed with caution.
- Audit Log Index: if you enable this feature, index logs are created and stored when you create, delete, modify, or view an Alibaba Cloud Elasticsearch instance. These logs consume disk space and affect the performance. We recommend that you disable this feature. Proceed with caution.
- Watcher: if you enable this feature, it allows you to use the X-Pack Watcher feature. Make sure that you regularly clear the `. watcher - history *` index. This index consumes large amounts of disk space.
- Other Configurations: the following parameters are supported. For more information, see #unique_22.

> Note:
> Excluding the parameters that have an Alibaba Cloud Elasticsearch version specified, the remaining parameters can only be applied to Elasticsearch V5.5.3 and V6.3.2.

- http.cors.enabled
- http.cors.allow-origin
- http.cors.max-age
- http.cors.allow-methods
- http.cors.allow-headers
- http.cors.allow-credentials
- reindex.remote.whitelist
- action.auto_create_index
- action.destructive_requires_name
- thread_pool.bulk.queue_size (Elasticsearch V5.5.3 with X-Pack)
- thread_pool.write.queue_size (Elasticsearch V6.3.2 with X-Pack)
- thread_pool.search.queue_size

1.5 YML configuration

Customize CORS requests

For more configurations, visit the Elasticsearch official website and view the HTTP information.

Configuration information

- Configurations in the table below are custom HTTP-based configurations provided by Alibaba Cloud Elasticsearch.
- For the following configurations, only static configuration is supported. Dynamic configuration is not supported. Note that for the following configurations to take effect, you must add the configurations to the `elasticsearch.yml` file.
- Cluster network settings are used for the following configurations. (Network settings)

Configuration item	Description
`http . cors . enabled`	A CORS (Cross-Origin Resource Sharing) configuration item, which can be used to enable or disable CORS resource accesses. In other words, this setting is used to determine whether to allow Elasticsearch to receive requests sent by browsers to access resources in different domains. If the parameter is set to `true`, Elasticsearch can process `OPTIONS` CORS requests. If the domain information in the sent request is already declared in `http . cors . allow - origin`, Elasticsearch adds `Access - Control - Allow - Origin` in the header to respond to the CORS request. If the parameter is set to `false` (which is the default value), Elasticsearch ignores the domain information in the request header, not adding the `Access - Control - Allow - Origin` to the header, disabling CORS access. If the client neither supports `pre - flight` requests that add the domain information header, nor checks `Access - Control - Allow - Origin` in the header of the packet returned from the server, then the secured CORS access will be affected. If Elasticsearch disables CORS access, then the client can only check whether a response is returned by sending the `OPTIONS` request.

Configuration item	Description
`http . cors . allow - origin`	A CORS resource configuration item, which can be used to specify requests from which domains are accepted. The parameter is left blank, by default, with no domain is allowed. If `/` is added before the parameter value, then the configuration is identified as a regular expression, which means that `HTTP` and `HTTPS` domain requests that follow the regular expression are supported. For example`/ Https ? : \/ Localhost  (: [ 0 - 9 ] + )? /` means requests follow the regular expression can be responded to. `*` means that a configuration is valid and can be identified as enabling the cluster to support CORS requests from any domain, resulting in security risks to the Elasticsearch cluster.
`http . cors . max - age`	The browser can send an `OPTIONS` request to get the CORS configuration. `max - age` can be used to set how long the browser can retain the output result cache. The default value is `1728000` seconds (20 days).
`http . cors . allow - methods`	A request method configuration item. The optional values are `OPTIONS` , `HEAD` , `GET` , `POST` , `PUT` , and `DELETE` .
`http . cors . allow - headers`	A request header configuration item. The default value is `X - Requested - With ,  Content - Type ,  Content - Length` .
`http . cors . allow - credential s`	A credential configuration item, which is used to specify whether to return `Access - Control - Allow - Credential  s` in the response header. If the parameter is set to `true` , Access-Control-Allow-Credentials is returned. The default value is `false` .

An example of custom cross-origin access configuration is as follows:

```
http . cors . enabled :  true
http . cors . allow - origin : "*"
http . cors . allow - headers : " X - Requested - With ,  Content -
Type ,  Content - Length ,  Authorizat  ion "
```

Customize remote re-indexing (whitelist)

The re-indexing component allows you to reconstruct the data index on the target remote Elasticsearch cluster. This function can work for all of the remote Elasticsearch versions available, allowing you to index the data of earlier versions to the current version.

```
 POST   _   reindex
{
  " source ": {
    " remote ": {
      " Host ": " http : //  otherhost :  9200  ",
      " username ": " username ",
      " password ": " password ",
    },
    " index ": " source ",
    " query ": {
      " match ": {
        " test ": " data "
      }
    }
  },
  " dest ": {
    " index ": " test - 1 ",
  }
}
```

- `host` must contain the protocol supported, domain name, port, for example, `Https : //  otherhost :  9200` .
- `username` and `password` are optional. If the remote Elasticsearch server requires Basic Authorization, enter the username and password in the request. When use `Basic   Authorizat  ion` , also use the `https` protocol, otherwise the password will be transmitted as a text.
- The remote host address must be declared in `elasticsea  rch . yml` by using the `reindex . remote . whitelist` attribute for the API to be called remotely. The combination of host and port is allowed. The combination of `host` and `port` is allowed. However, note that multiple host configurations must be separated by commas (,), for example,

  ```
   otherhost :  9200 ,  another :  9200 , 127 . 0  . 10 . **:  9200 ,
  ```

```
            localhost :**
```

). The whitelist does not identify the protocol and only uses the host and port information for the security policy configuration.

- If the host address is already listed in the whitelist, the `query` request will not be verified or modified. Rather, the request will be directly sent to the remote server.

Note:

- Indexing data from a remote cluster is not supportedManual SlicingOrAutomatic Slicing. For more information, see Manual slicing or Automatic slicing.

Multiple indexes settings

The remote service uses a stack to cache indexed data. The default maximum size is `100 MB`. If the remote index contains a large document, set the size of batch settings to a small value.

In the example below, the size of multiple index settings is 10, which is the minimum value:

```
 POST   _   reindex
{
  " source ": {
    " remote ": {
      " host ": " http :// otherhost : 9200 "
    },
    " index ": " source ",
    " size ":  10 ,
    " query ": {
      " match ": {
        " test ": " data "
      }
    }
  },
  " dest ": {
    " index ": " test - 1 ",
  }
}
```

Timeout period

- Use `socket_timeout` to set the read timeout period of `socket`. The default value is `30s`.
- Use `connect_timeout` to set the connection timeout period. The default value is `1s`.

In the example below, the read timeout period of `socket` is one minute, and the connection timeout period is 10 seconds.

```
 POST   _   reindex
{
  " source ": {
    " remote ": {
      " host ": " http :// otherhost : 9200 ",
      " socket_tim  eout ": " 1m ",
      " connect_ti  meout ": " 10s "
    },
    " index ": " source ",
    " query ": {
      " match ": {
        " test ": " data "
      }
    }
  },
  " dest ": {
    " index ": " test - 1 ",
  }
}
```

Customize the access log

Enable auditing

The index auditing configuration is as follows.

```
xpack . security . audit . index . bulk_size :  5000
xpack . security . audit . index . events . emit_reque  st_body :
false
xpack . security . audit . index . events . exclude :  run_as_den
ied , anonymous_  access_den  ied , realm_auth  entication  _failed ,
access_den  ied , connection  _denied
xpack . security . audit . index . events . include :  authentica
tion_faile  d , access_gra  nted , tampered_r  equest , connection
_granted , run_as_gra  nted
xpack . security . audit . index . flush_inte  rval :  180s
xpack . security . audit . index . rollover :  hourly
xpack . security . audit . index . settings . index . number_of_
replicas :  1
xpack . security . audit . index . settings . index . number_of_
shards :  10
```

Index auditing output

Alibaba Cloud Elasticsearch instances do not support displaying request-related log files. Therefore, to view information about the Elasticsearch instance requests, such as the access_log, you must log in to the Elasticsearch console and enable the access log index function.

After this function is enabled, the access log is output to indexes on the Elasticsearch instance. The name of indexes starts with `. security_a  udit_log -*`.

Audit Log Index: ● Disable ○ Enable

Audit log indexing configuration

Note:

- Filtering is not supported during audits because sensitive data may be audited in plain text when the `request body` is included in audit events.
- Audit log indexing occupies Alibaba Cloud Elasticsearch instance storage space. You must manually clear old audit log indexes because no policy is available for clearing expired indexes.

Feature	Default value	[DO NOT TRANSLATE]
`xpack.security.audit.index.bulk_size`	`1,000`	Indicates how many audit events are batched into a single write file.
`xpack.security.audit.index.flush_interval`	`1s`	Indicates how often buffered events are flushed to the index.
`xpack.security.audit.index.rollover`	`daily`	Indicates how often to roll over to a new index. Options include `hourly`, `daily`, `weekly`, or `monthly`.
`Xpack.security.audit.index.events.include`	`anonymous_access_denied`, `authentication_failed`, `realm_authentication_failed`, `access_granted`, `access_denied`, `tampered_request`, `connection_granted`, `connection_denied`, `run_as_granted`, `run_as_denied`	Specifies the audit events to be indexed. For more information about audit event types, see Audit event types.

Feature	Default value	[DO NOT TRANSLATE]
`xpack.security.audit.index.events.exclude`		Excludes the specified auditing events from indexing.
`xpack.security.audit.index.events.emit_request_body`	`false`	Indicates whether to include the request body in REST requests in certain event types, such as `authentication_failed`.

Audit indexing settings

The configuration item `xpack.security.audit.index.settings` in the `elasticsearch.yml` file specifies the settings for the indexes in which the events are stored.

The following example sets both the number of shards and the number of replicas to `1` for the audit indexes.

```
xpack.security.audit.index.settings:
  index:
    number_of_shards: 1
    number_of_replicas: 1
```

Note:

You can pass custom settings to xpack.security.audit.index.settings when enabling audit indexing. Once you apply the change to the Elasticsearch instance, audit indexes will be available on the Elasticsearch instance. Otherwise, the elasticsearch instance audit log is set to the default `Number_of_shards: 5`, and `Number_of_replicas: 1`.

Remote audit log indexing settings

Indexing settings for remote audit logs are currently unavailable.

Customize thread pool queue size

You can set `Thread_pool.bulk.queue_size`, `Thread_pool.write.queue_size`, and `Thread_pool.search.queue_size` to customize the queue size of the write and search thread pools, respectively..

In the following example, both the write and search queue size are set to `500`.

Note:

The following parameters are not specifically identified for an ES version and by default are compatible with ES version 5.5.3 and 6.3.2.

```
thread_pool.bulk.queue_size: 500 (Only applicable to
the Elasticsearch 5.5.3 with X-Pack version)
thread_pool.write.queue_size: 500 (Only applicable to
the Elasticsearch 6.3.2 with X-Pack version)
thread_pool.search.queue_size: 500
```

Parameter optimization

Configuration Item	Description
Index. codec	The ES data compression algorithm defaults to LZ4. Usually, by setting LZ4 to best_compression in a warm or cold cluster using a high-speed cloud disk, a higher compression ratio DEFLATE algorithm can be used. After the algorithm is changed, segment merges will use the newest version of the algorithm. Note that using best_compr ession will result in reduced write performance.

REST API settings

You can set the `index.codec` parameter by using REST API.

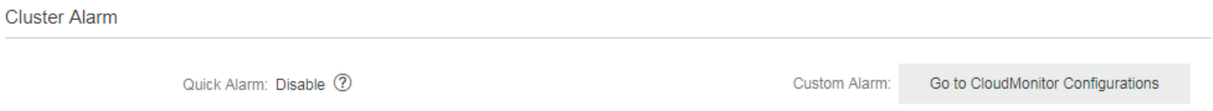
Note:

- `close` the corresponding index before running the command.
- $index_name: Replace with the index name you need to set.

```
 PUT $index_name/_settings
{
  "index": {
    "codec": "best_compression"
  }
}
```

1.6 Cluster monitoring

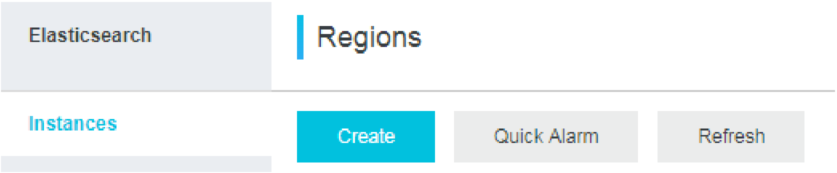
Cluster alarm


Cluster Alarm

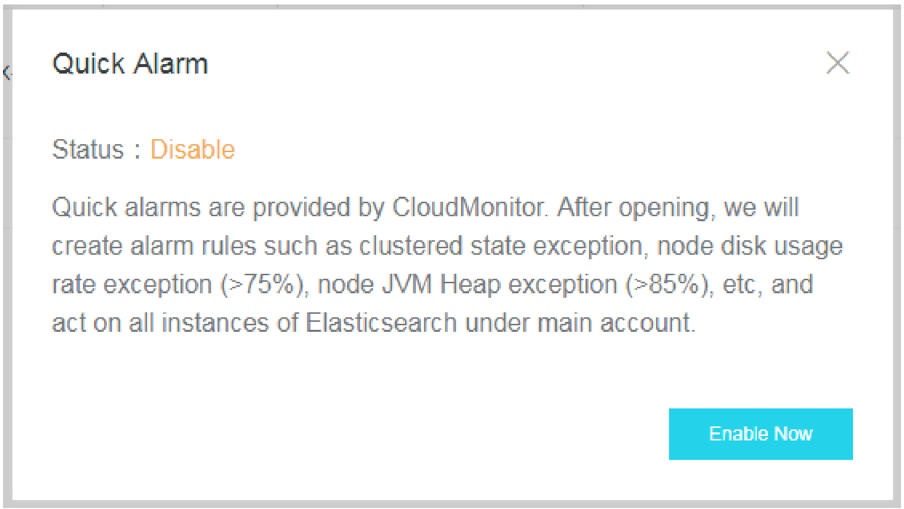
Quick Alarm: Disable

Quick alarm

1. Elasticsearch supports quick alarm. This feature is disabled by default. You can go to the clusters list page and click Quick Alarm to enable or disable this feature.



2. If this feature is disabled, click Quick Alarm, and then click Enable Now in the dialog box to manually enable it.


Quick Alarm

Status：Disable

Quick alarms are provided by CloudMonitor. After opening, we will create alarm rules such as clustered state exception, node disk usage rate exception (>75%), node JVM Heap exception (>85%), etc, and act on all instances of Elasticsearch under main account.

Custom alarms

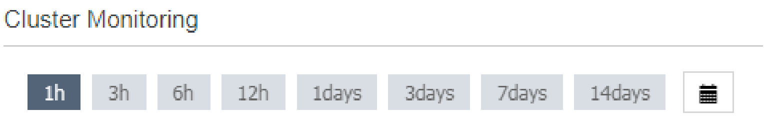
You can click Cluster Monitor to create custom alarm rules. For more information about creating alarm rules, see #unique_25.

Cluster monitor

You can view Elasticsearch instance parameters and workloads.

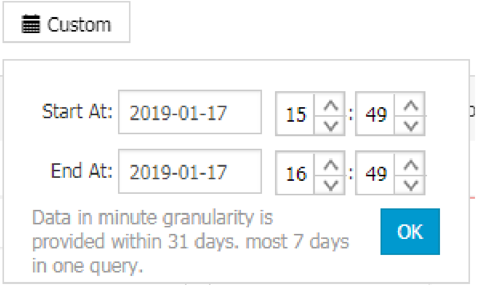
Preset time

You can click a time option to view cluster metrics that are collected in the specified time period.


Cluster Monitoring

Custom cluster monitoring time

You can click Custom to specify the start time and end time to define a time window and view cluster monitoring data collected within the time window.



Start At: 2019-01-17 15 : 49

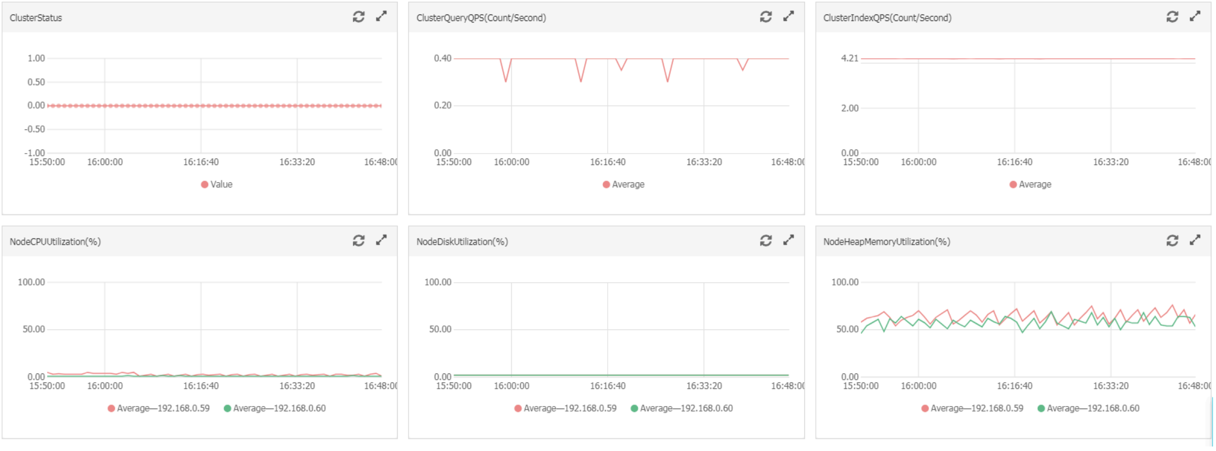
End At: 2019-01-17 16 : 49

Data in minute granularity is provided within 31 days. most 7 days in one query.

Note:

You can query up to 7 continuous days of data in the last 31 days by the minute.

Cluster monitoring metrics



1.7 Query logs

Alibaba Cloud Elasticsearch allows you to search and view multiple types of logs, including the Elasticsearch instance log, search slow log, indexing slow log, and GC log.

You can search for specific log entries by entering keywords and setting a time range . All Alibaba Cloud Elasticsearch log entries are sorted in time descending order. You can search for log entries that are stored within the last seven days.

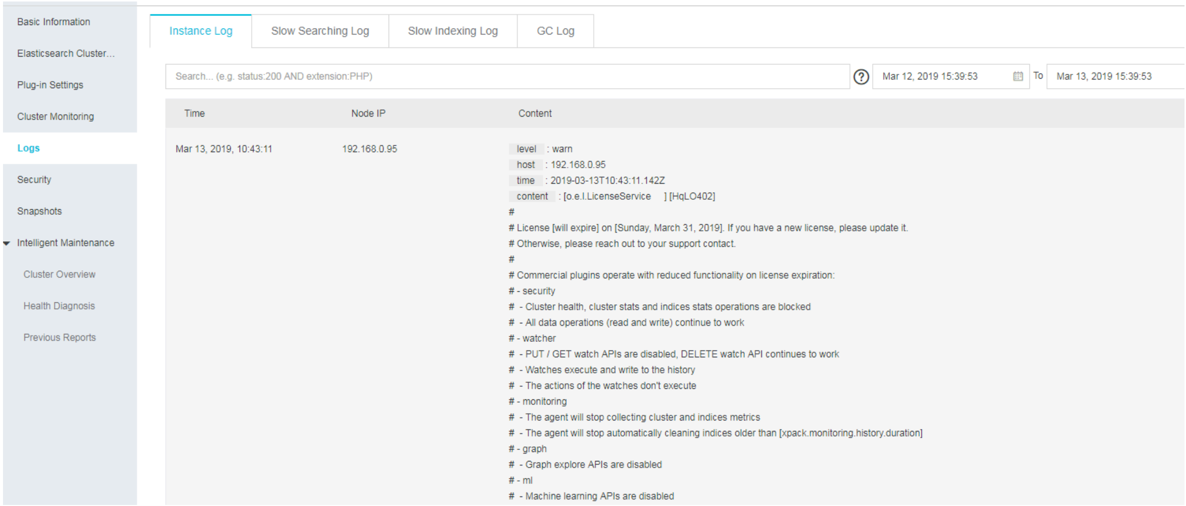
Alibaba Cloud Elasticsearch allows you to use Lucene to query logs. For more information, see Query String Query.

> Note:
>
> Due to the restrictions Elasticsearch puts on query conditions, a maximum of 10,000 log entries can be returned. If the log entries that you have queried are not contained in the returned 10,000 log entries, set a more specific time range to narrow down the search results.

Example

The following example shows how to search for Elasticsearch instance logs whose content contains the keyword `health` , level is set to `info` , and host is set to `192 . 168 . 1 . 123 .`

1. Log on to the Alibaba Cloud Elasticsearch console, select the target instance, and click Manage in the Actions column to go to the Basic Information page. On the Basic Information page, click Logs in the left-side navigation pane and then click the Instance Log tab.
2. Enter `host : 192 . 168 . 1 . 123  AND  content : health  AND  level : info` in the search box.
3. Specify a time range and click Search.



Time	Node IP	Content
Mar 13, 2019, 10:43:11	192.168.0.95	see below

```
level   : warn
host    : 192.168.0.95
time    : 2019-03-13T10:43:11.142Z
content : [o.e.l.LicenseService    ] [HqLO402]
#
# License [will expire] on [Sunday, March 31, 2019]. If you have a new license, please update it.
# Otherwise, please reach out to your support contact.
#
# Commercial plugins operate with reduced functionality on license expiration:
# - security
#  - Cluster health, cluster stats and indices stats operations are blocked
#  - All data operations (read and write) continue to work
# - watcher
#  - PUT / GET watch APIs are disabled, DELETE watch API continues to work
#  - Watches execute and write to the history
#  - The actions of the watches don't execute
# - monitoring
#  - The agent will stop collecting cluster and indices metrics
#  - The agent will stop automatically cleaning indices older than [xpack.monitoring.history.duration]
# - graph
#  - Graph explore APIs are disabled
# - ml
#  - Machine learning APIs are disabled
```

Note:

- If you do not specify the end time, it defaults to the current system time.
- If you do not specify the start time, it defaults to one hour later than the end time.
- The word `AND` connecting search conditions that you enter in the search box must be capitalized.

Log description

You can view log entries that are retrieved based on specified search conditions on the log search page. Each log entry contains the following parts: Time, Node IP, and Content.

Time

The time when the log entry was created.

Node IP

The IP address of the Alibaba Cloud Elasticsearch node.

Content

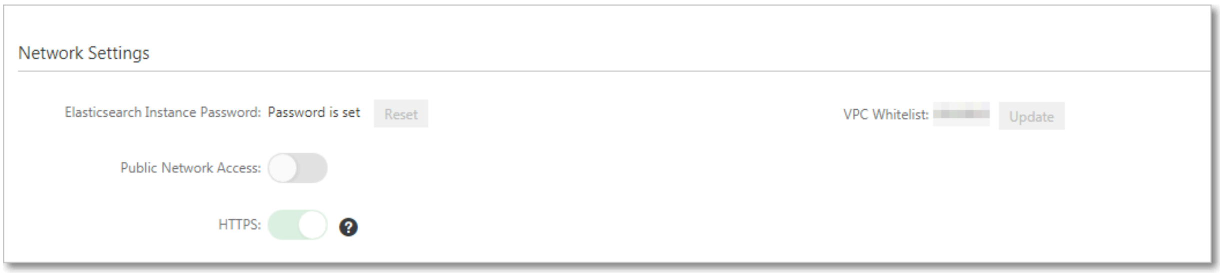
The information about the level, host, time, and content.

- level: the level of the log entry. Log levels include trace, debug, info, warn, and error. GC log entries do not have levels.
- host: indicates the IP address of the Elasticsearch node. You can view the IP address on the Nodes tab in the Kibana console.
- time: indicates the time when the log entry was created.
- content: displays major information about the log entry.

1.8 Security configuration

This topic describes the security configuration of Alibaba Cloud Elasticsearch, including the Elasticsearch instance password, public network whitelist, VPC whitelist, and HTTPS protocol.

Network settings



Network Settings

Elasticsearch Instance Password: Password is set

VPC Whitelist: [redacted]

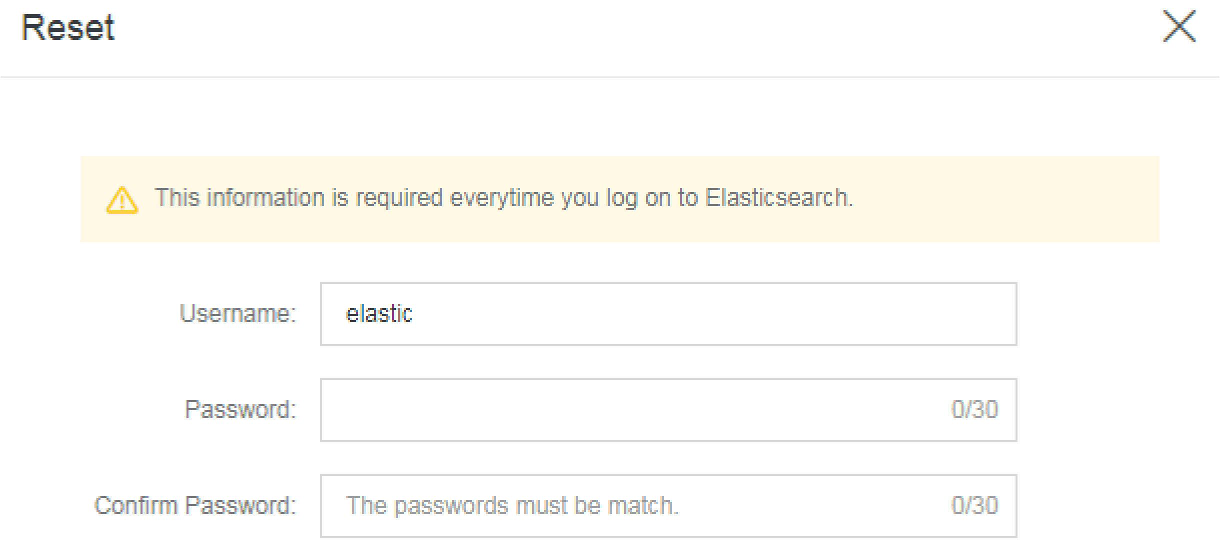
Public Network Access:

HTTPS:

You can reset the Elasticsearch instance password, configure the VPC whitelist, enable Public network access, and configure the Public network whitelist and Enable HTTPS in network settings.

Elasticsearch instance password

To reset the Elasticsearch instance password, click Reset, and enter a new password for the administrator account elastic. After you reset the password, it takes up to 5 minutes for the new password to take effect.



Reset

This information is required everytime you log on to Elasticsearch.

Username: elastic

Password: 0/30

Confirm Password: The passwords must be match. 0/30

If you use the elastic account to log on to the Alibaba Cloud Elasticsearch instance or Kibana console, then you must use the new password.

Note:

- The reset operation only resets the password of the elastic account. The operation does not reset the password of other accounts that are used to log on to the instance. We recommend that you do not use the elastic account to log on to your Alibaba Cloud Elasticsearch instance.
- The Reset operation does not restart the Alibaba Cloud Elasticsearch instance.

VPC whitelist

When you need to access an Alibaba Cloud Elasticsearch instance from an ECS instance in a VPC network, you must add the IP address of the ECS instance to the VPC whitelist.

Click Update, enter the IP address in the VPC whitelist dialog box, and click OK.

You can add IP addresses and CIDR blocks to the whitelist in the format of `192 . 168 . 0 . 1` and `192 . 168 . 0 . 0 / 24`, respectively. Separate these IP addresses and CIDR blocks with commas (,). Enter `127 . 0 . 0 . 1` to forbid all IPv4 addresses or enter `0 . 0 . 0 . 0 / 0` to allow all IPv4 addresses.

Note:

- By default, all private IPv4 addresses are allowed to access Elasticsearch.
- The VPC whitelist is used to control access from internal network addresses in VPC networks.

Public network access

Click the Public Network Access switch to enable public network access. After this feature is enabled, the switch is in green. By default, the switch is in gray, which means that public network access is disabled. To access your Alibaba Cloud Elasticsearch instance through the Internet, you must enable public network access.

Public network whitelist

Before you configure the public network whitelist, you must toggle on the Public Network Access switch. By default, the public network access feature forbids all public network addresses.

To access your Alibaba Cloud Elasticsearch instance through the Internet, you must add the IP address of your client to the public network whitelist.

You can add IP addresses and CIDR blocks in the format of `192 . 168 . 0 . 1` and `192 . 168 . 0 . 0 / 24`, respectively. Separate these IP addresses and CIDR blocks with commas (,). Enter `127 . 0 . 0 . 1` to forbid all IPv4 addresses or enter `0 . 0 . 0 . 0 / 0` to allow all IPv4 addresses.

If your Elasticsearch instance is deployed in the China (Hangzhou) region, then you can add IPv6 addresses and CIRD blocks to the whitelist in the format of `2401 : b180 : 1000 : 24 :: 5` and `2401 : b180 : 1000 ::/ 48`, respectively. Enter `:: 1` to forbid all IPv6 addresses or enter `::/ 0` to allow all IPv6 addresses.

Enable HTTPS

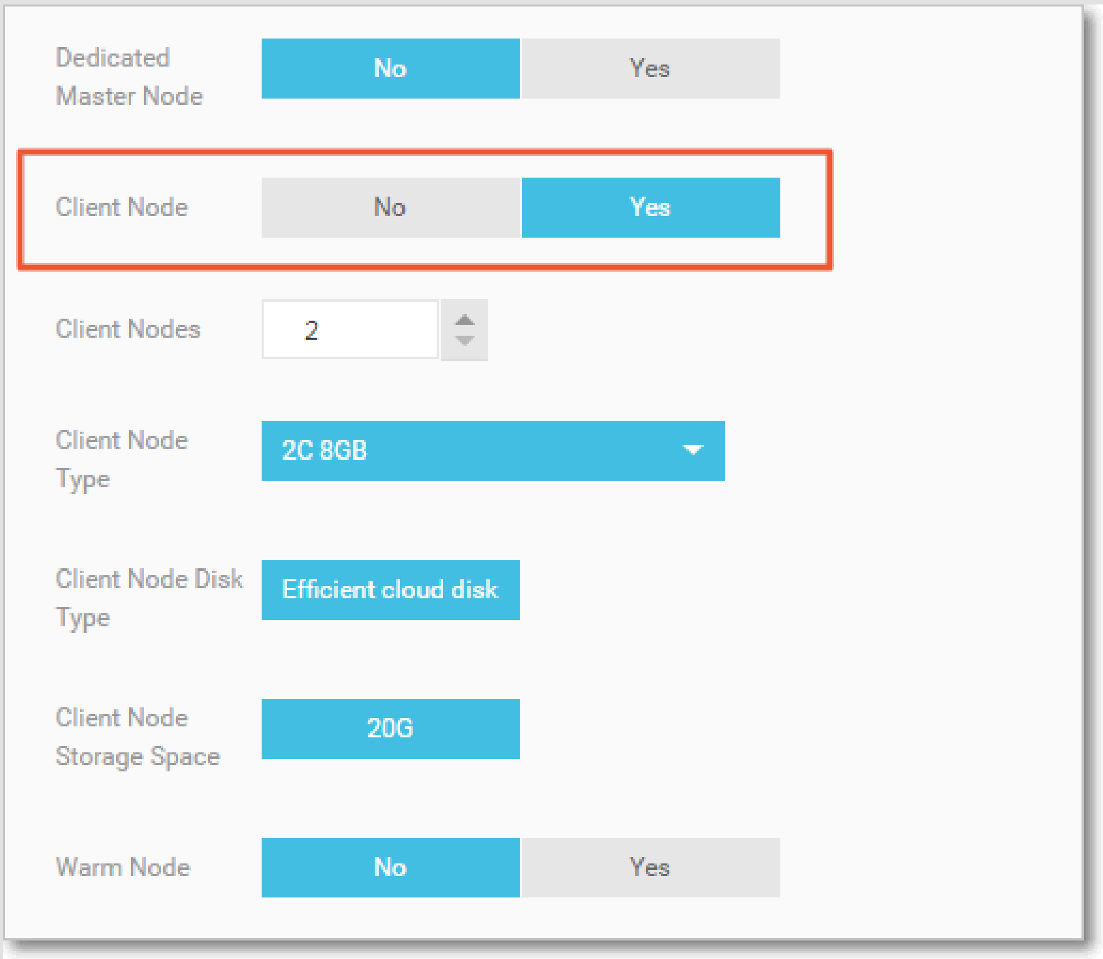
Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP. HTTPS uses Secure Socket Layer (SSL) for secure data transmission. This means that HTTPS still uses HTTP for communications. SSL is used to encrypt the data.

`Procedure`

Notice:

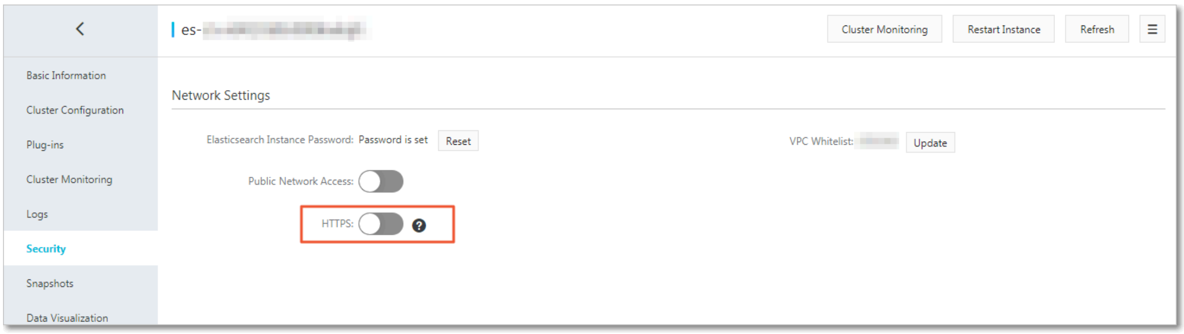
- Alibaba Cloud Elasticsearch allows you to enable and disable HTTPS. To protect your data, we recommend that you enable HTTPS.

- Before you enable HTTPS, you must purchase client nodes.



Dedicated Master Node	[✓ No] Yes
Client Node	No [✓ Yes]
Client Nodes	2
Client Node Type	2C 8GB
Client Node Disk Type	Efficient cloud disk
Client Node Storage Space	20G
Warm Node	[✓ No] Yes

1. Log on to the Alibaba Cloud Elasticsearch console, click Instance ID/Name > Security, and click the HTTPS switch to enable HTTPS.



es-[redacted]

Network Settings

Elasticsearch Instance Password: Password is set Reset

VPC Whitelist: [redacted] Update

Public Network Access: ○

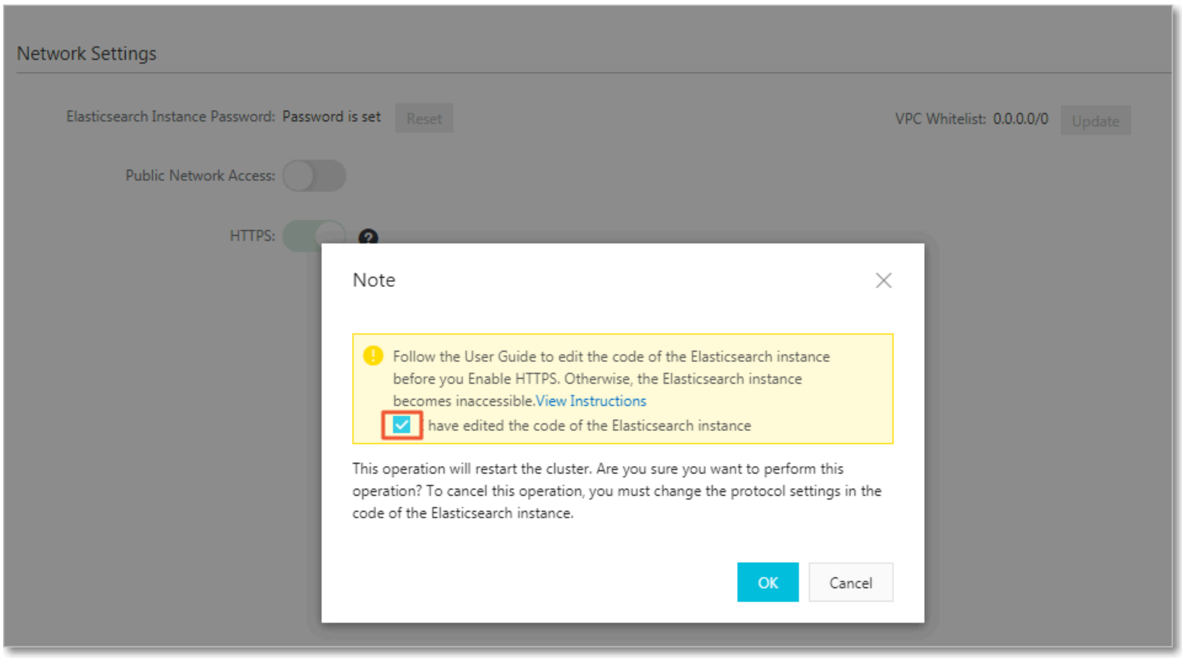
HTTPS: ○

Notice:

- Before you enable HTTPS, you must update the code of the client that is used to access the Elasticsearch instance. Otherwise, you may fail to access the instance. For more information, see Sample client code for enabling or disabling HTTPS.

- During the process of enabling or disabling HTTPS, the services running on the instance will be interrupted and the instance will be restarted. Before you enable or disable HTTPS, make sure that your businesses will not be adversely affected.

2. In the Confirm Operation dialog box, select I have edited the code of the Elasticsearch instance, and then click OK.



Network Settings

Elasticsearch Instance Password: Password is set

VPC Whitelist: 0.0.0.0/0

Note

Follow the User Guide to edit the code of the Elasticsearch instance before you Enable HTTPS. Otherwise, the Elasticsearch instance becomes inaccessible.View Instructions

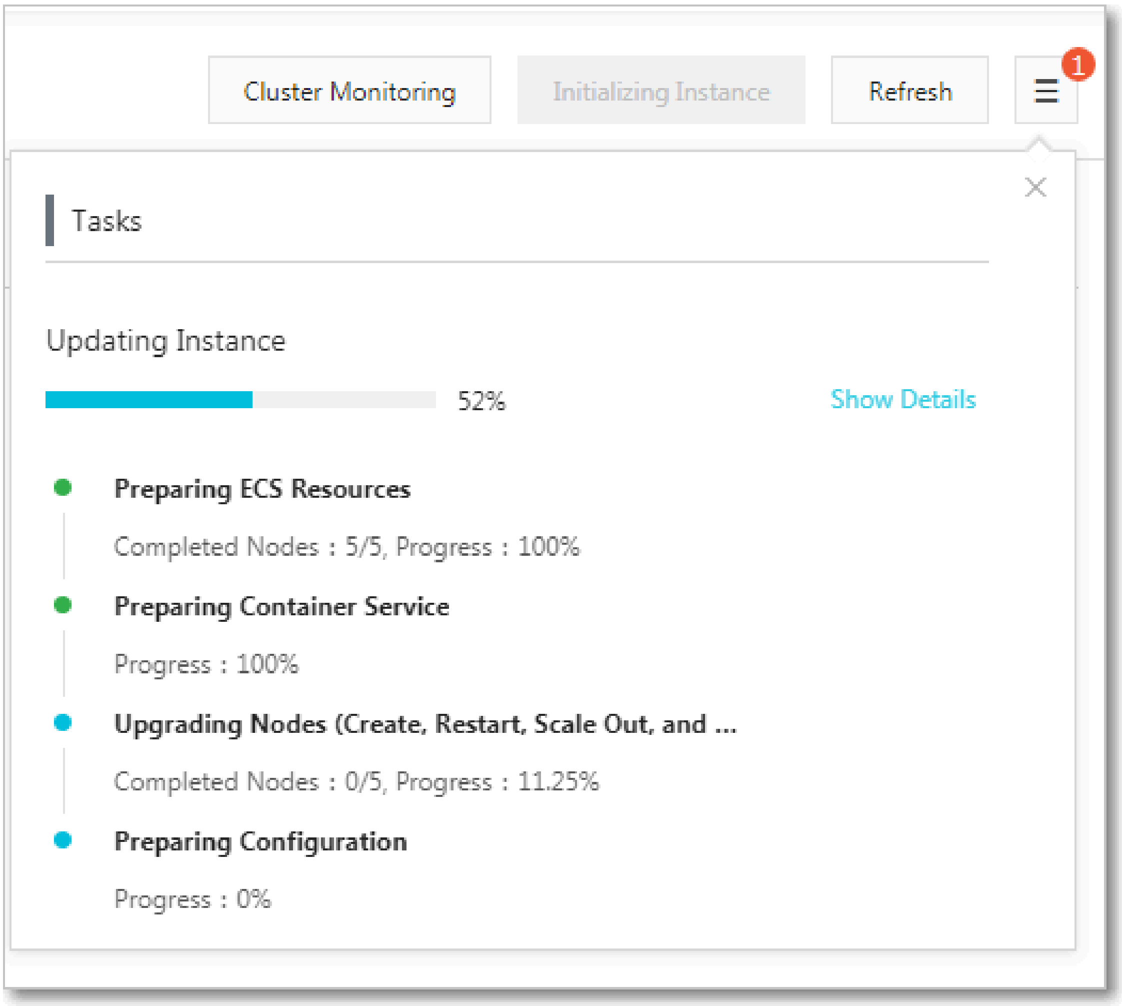
☑ have edited the code of the Elasticsearch instance

This operation will restart the cluster. Are you sure you want to perform this operation? To cancel this operation, you must change the protocol settings in the code of the Elasticsearch instance.

Note:

If you have not purchased client nodes, after you enable HTTPS, the system prompts a notification requiring you to purchase client nodes. You can follow the instructions to purchase client nodes.

After you confirm to enable or disable HTTPS, the instance will restart. You can click the Tasks icon in the upper-right corner to check the progress. After the instance is restarted, you can then access the instance through HTTPS.



Tasks

Updating Instance

52%

Show Details

Preparing ECS Resources

Completed Nodes : 5/5, Progress : 100%

Preparing Container Service

Progress : 100%

Upgrading Nodes (Create, Restart, Scale Out, and ...

Completed Nodes : 0/5, Progress : 11.25%

Preparing Configuration

Progress : 0%

Sample client code for enabling or disabling HTTPS

The following example shows the changes that need to be made to the code of the Elasticsearch REST client after you enable HTTPS.

- The code of the REST client before HTTPS is enabled:

```
final   Credential  sProvider   credential  sProvider  =  new
BasicCrede  ntialsProv  ider ();
        credential  sProvider . setCredent  ials ( AuthScope . ANY
,
            new   UsernamePa  sswordCred  entials (" elastic ", "
Your    password "));
RestClient  Builder   restClient  Builder  =  RestClient . builder
(
            new   HttpHost (" es - cn - xxxxx . elasticsea  rch .
aliyuncs . com ",  9200 ));
        RestClient   restClient  =  restClient  Builder .
setHttpCli  entConfigC  allback (
            new   RestClient  Builder . HttpClient  ConfigCall
back () {
               @ Override
                public   HttpAsyncC  lientBuild  er   customizeH
ttpClient ( HttpAsyncC  lientBuild  er   httpClient  Builder ) {
                    return   httpClient  Builder . setDefault
Credential  sProvider ( credential  sProvider );
               }
           }). build ();
```

- The code of the REST client after HTTPS is enabled:

```
final   Credential  sProvider   credential  sProvider   =   new
BasicCrede  ntialsProv  ider ();
        credential  sProvider . setCredent  ials ( AuthScope . ANY
,
            new   UsernamePa  sswordCred  entials (" elastic ", "
Your   password "));
RestClient  Builder   restClient  Builder   =  RestClient . builder
(
            new   HttpHost (" es - cn - xxxxx . elasticsea  rch .
aliyuncs . com ",  9200 , " https "));
        RestClient   restClient  =  restClient  Builder .
setHttpCli  entConfigC  allback (
            new   RestClient  Builder . HttpClient  ConfigCall
back () {
               @ Override
                public   HttpAsyncC  lientBuild  er   customizeH
ttpClient ( HttpAsyncC  lientBuild  er   httpClient  Builder ) {
                    return   httpClient  Builder . setDefault
Credential  sProvider ( credential  sProvider );
               }
           }). build ();
```

As shown in the preceding example, after you enable HTTPS, you must include the `https` parameter in `HttpHost`: `new   HttpHost (" es - cn - xxxxx . elasticsea  rch . aliyuncs . com ",  9200 , " https "));`

1.9 Configure synonyms

Description

Note:

- After you upload a synonym dictionary file to an Alibaba Cloud Elasticsearch instance, you do not need to restart the nodes in the instance. The system will update the synonym dictionary file to all nodes. Depending on the number of nodes, this process may be time-consuming.

- For example, index ‘index-aliyun’ is using the synonym dictionary file ‘aliyun .txt’. You have uploaded a new synonym dictionary file to overwrite the existing dictionary file. However, index ‘index-aliyun’ cannot automatically load the updated dictionary file. If you want the index to load the updated dictionary file, disable the index and then re-enable the index. We recommend that you rebuild the index after you update the dictionary file as a best practice. Otherwise , this may cause an issue that only the newly created data is using the updated dictionary file.

You can use a filter to configure synonyms. The sample code is as follows:

```
 PUT  / test_index
{
    " settings ": {
        " index " : {
            " analysis " : {
                " analyzer " : {
                    " synonym " : {
                        " tokenizer " : " whitespace ",

                        " filter " : [" synonym "]
                        }
                   },
                   " filter " : {
                        " synonym " : {
                             " type " : " synonym ",

                              " synonyms_p  ath " : " analysis /
 synonym . txt ",
                              " tokenizer " : " whitespace "

                          }
                       }
                    }
                  }
          }
}
```

- `filter` : configure a `synonym` token filter that contains the path `analysis / synonym . txt` . This path is relative to the location of config.
- `tokenizer` : the tokenizer that tokenizes synonyms. It is set to `whitespace` by default. Additional settings:
  - `ignore_cas  e` : the default value is false.
  - `expand` : the default value is true.

Two synonym formats are supported: Solr and WordNet.

- Solr synonyms

  The following is a sample format of the file:

```
#  Blank   lines   and   lines   starting   with   pound   are
 comments .
#  Explicit   mappings   match   any   token   sequence   on   the
 LHS   of  "=>"
#  and   replace   with   all   alternativ  es   on   the   RHS .
 These   types   of   mappings
#  ignore   the   expand   parameter   in   the   schema .
#  Examples :
 i - pod ,  i   pod  =>  ipod ,
 sea   biscuit ,  sea   biscit  =>  seabiscuit
#  Equivalent   synonyms   may   be   separated   with   commas
 and   give
#  no   explicit   mapping .   In   this   case   the   mapping
 behavior   will
#  be   taken   from   the   expand   parameter   in   the   schema
 .   This   allows
#  the   same   synonym   file   to   be   used   in   different
 synonym   handling   strategies .
#  Examples :
 ipod ,  i - pod ,  i   pod
 foozball  ,  foosball
 universe  ,  cosmos
 lol ,  laughing   out   loud
#  If   expand == true , " ipod ,  i - pod ,  i   pod "  is
 equivalent
#  to   the   explicit   mapping :
 ipod ,  i - pod ,  i   pod  =>  ipod ,  i - pod ,  i   pod
#  If   expand == false , " ipod ,  i - pod ,  i   pod "  is
 equivalent
#  to   the   explicit   mapping :
 ipod ,  i - pod ,  i   pod  =>  ipod
#  Multiple   synonym   mapping   entries   are   merged .
 foo  =>  foo   bar
 foo  =>  baz
#  is   equivalent   to
 foo  =>  foo   bar ,  baz
```

  You can also directly define synonyms for the token filter in the configuration file. You must use `synonyms` instead of `synonyms_p  ath`. Example:

```
 PUT  / test_index
{
    " settings ": {
        " index " : {
            " analysis " : {
                " filter " : {
                    " synonym " : {
                        " type " : " synonym ",
                        " synonyms " : [
                            " i - pod ,  i   pod  =>  ipod ",
                            " begin ,  start "
                        ]
                    }
                }
            }
        }
    }
}
```

We recommend that you use `synonyms_p ath` to define large synonym sets in the file. Using `synonyms` to define large synonym sets will increase the size of your cluster.

- WordNet synonyms

  Synonyms based on the WordNet format can be declared by using the following format:

```
 PUT  / test_index
{
    " settings ": {
        " index " : {
            " analysis " : {
                " filter " : {
                    " synonym " : {
                        " type " : " synonym ",
                        " format " : " wordnet ",
                        " synonyms " : [
                            " s ( 100000001 , 1 ,' abstain ', v , 1
 , 0 ).",
                            " s ( 100000001 , 2 ,' refrain ', v , 1
 , 0 ).",
                            " s ( 100000001 , 3 ,' desist ', v , 1 ,
 0 )."
                        ]
                    }
                }
            }
        }
    }
}
```

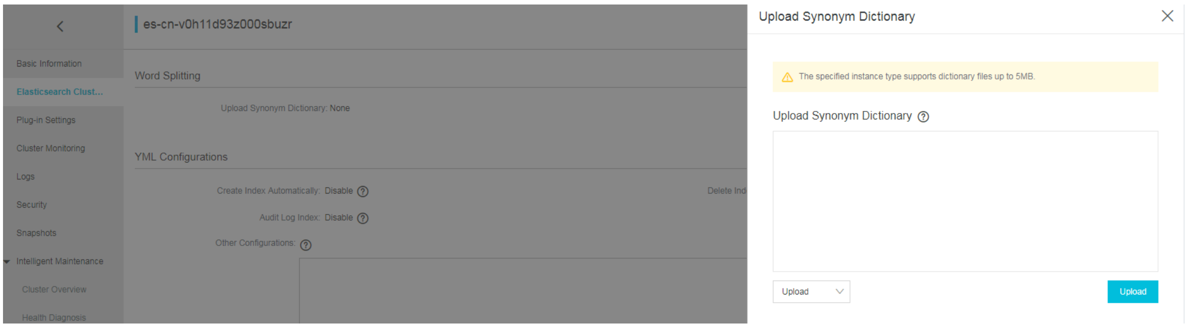
  You can also use `synonyms_p ath` to define WordNet synonyms in a file.

Example 1:

Upload a synonym dictionary file

1. Log on to the Alibaba Cloud Elasticsearch console.
2. Click Create in the upper-left corner to create an Alibaba Cloud Elasticsearch instance.
3. Click the instance to go to the configuration page.

4. In the left-side navigation pane, select Cluster Configuration, and then click Synonym Dictionary Configuration.



es-cn-v0h11d93z000sbuzr

Word Splitting

Upload Synonym Dictionary: None

YML Configurations

Create Index Automatically: Disable

Audit Log Index: Disable

Other Configurations:

Upload Synonym Dictionary

The specified instance type supports dictionary files up to 5MB.

Upload Synonym Dictionary

5. Click Upload, select the synonym dictionary file that you want to upload, and click Save . In this example, the TXT file that is generated in the format described in the preceding sections is uploaded.

   After the Alibaba Cloud Elasticsearch instance is activated and its status changes to Active, you can then use the synonym dictionary. In this example, file `aliyun_syn onyms . txt` is uploaded for testing. The file contains: `begin , start`

Configure and test the synonym dictionary

1. Click Kinana Console in the upper-right corner to go to the Kibana console.
2. In the left-side navigation pane, click Dev Tool.
3. Run the following command in the Console to create indexes:

```
 PUT   aliyun - index - test
{
" index ": {
 " analysis ": {
   " analyzer ": {
     " by_smart ": {
       " type ": " custom ",
       " tokenizer ": " ik_smart ",
       " filter ": [" by_tfr "," by_sfr "],
       " char_filte  r ": [" by_cfr "]
     },
     " by_max_wor  d ": {
       " type ": " custom ",
       " tokenizer ": " ik_max_wor  d ",
       " filter ": [" by_tfr "," by_sfr "],
       " char_filte  r ": [" by_cfr "]
     }
   },
   " filter ": {
     " by_tfr ": {
       " type ": " stop ",
       " stopwords ": [" "]
     },
     " by_sfr ": {
       " type ": " synonym ",
       " synonyms_p  ath ": " analysis / aliyun_syn  onyms . txt "
     }
   },
   " char_filte  r ": {
     " by_cfr ": {
       " type ": " mapping ",
       " mappings ": ["| => |"]
     }
   }
 }
}
}
```

4. Run the following command to configure the title field:

```
 PUT   aliyun - index - test / _mapping / doc
{
" properties ": {
 " title ": {
   " type ": " text ",
   " index ": " analyzed ",
   " analyzer ": " by_max_wor  d ",
   " search_ana  lyzer ": " by_smart "
 }
}
}
```

5. Run the following command to verify the synonyms:

```
 GET   aliyun - index - test / _analyze
{
" analyzer ": " by_smart ",
" text ":" begin "
}
```

The following results are returned if the configuration takes effect:

```
{
" tokens ": [
 {
   " token ": " begin ",
   " start_offs  et ":  0 ,
   " end_offset ":  5 ,
   " type ": " ENGLISH ",
   " position ":  0
 },
 {
   " token ": " start ",
   " start_offs  et ":  0 ,
   " end_offset ":  5 ,
   " type ": " SYNONYM ",
   " position ":  0
 }
]
}
```

6. Run the following command to add data for further testing:

```
 PUT   aliyun - index - test / doc / 1
{
" title ": " Shall   I   begin ?"
}
```

```
 PUT   aliyun - index - test / doc / 2
{
" title ": " I   start   work   at   nine ."
}
```

7. **Run the following command to perform a query test:**

```
 GET   aliyun - index - test / _search
{
 " query " : { " match " : { " title " : " begin " }},
 " highlight " : {
     " pre_tags " : ["< red >", "< bule >"],
     " post_tags " : ["</ red >", "</ bule >"],
     " fields " : {
         " title " : {}
     }
 }
}
```

If the query is successful, the following results are returned:

```
{
" took ":  11 ,
" timed_out ":  false ,
" _shards ": {
 " total ":  5 ,
 " successful ":  5 ,
 " failed ":  0 ,
},
" hits ": {
 " total ":  2 ,
 " max_score ":  0 . 41048482 ,
 " hits ": [
   {
     " _index ": " aliyun - index - test ",
     " _type ": " doc ",
     " _id ": " 2 ",
     " _score ":  0 . 41048482 ,
     " _source ": {
       " title ": " I   start   work   at   nine ."
     },
     " highlight ": {
       " title ": [
         " I  < red > start </ red >  work   at   nine ."
       ]
     }
   },
   {
     " _index ": " aliyun - index - test ",
     " _type ": " doc ",
     " _id ": " 1 ",
     " _score ":  0 . 39556286 ,
     " _source ": {
       " title ": " Shall   I   begin ?"
     },
     " highlight ": {
       " title ": [
         " Shall   I  < red > begin </ red >?"
       ]
     }
```

```
    }
  ]
 }
}
```

Example 2

Follow these steps to directly import the synonyms and use the IK analyzer to filter the synonyms:

1. Configure synonym filter `my_synonym _filter` and a synonym dictionary.
2. Configure analyzer `my_synonym s`, and use IK analyzer `ik_smart` to split words.

   The IK analyzer `ik_smart` splits the words and then changes all letters to lowercase.

   ```
    PUT  / my_index
   {
    " settings ": {
        " analysis ": {
            " analyzer ": {
                " my_synonym  s ": {
                    " filter ": [
                        " lowercase ",
                        " my_synonym  _filter "
                    ],
                    " tokenizer ": " ik_smart "
                }
            },
            " filter ": {
                " my_synonym  _filter ": {
                    " synonyms ": [
                        " begin , start "
                    ],
                    " type ": " synonym "
                }
            }
        }
    }
   }
   ```

3. Run the following command to configure the title field:

   ```
    PUT  / my_index / _mapping / doc
   {
   " properties ": {
    " title ": {
      " type ": " text ",
      " index ": " analyzed ",
      " analyzer ": " my_synonym  s "
    }
   }
   ```

```
}
```

4. Run the following command to verify the synonyms:

```
 GET  / my_index / _analyze
{
 " analyzer ":" my_synonym  s ",
 " text ":" Shall   I   begin ?"
}
```

If the synonyms are verified, the following results are returned:

```
{
" tokens ": [
 {
   " token ": " shall ",
   " start_offs  et ":  0 ,
   " end_offset ":  5 ,
   " type ": " ENGLISH ",
   " position ":  0
 },
 {
   " token ": " i ",
   " start_offs  et ":  6 ,
   " end_offset ":  7 ,
   " type ": " ENGLISH ",
   " position ":  1
 },
 {
   " token ": " begin ",
   " start_offs  et ":  8 ,
   " end_offset ":  13 ,
   " type ": " ENGLISH ",
   " position ":  2
 },
 {
   " token ": " start ",
   " start_offs  et ":  8 ,
   " end_offset ":  13 ,
   " type ": " SYNONYM ",
   " position ":  2
 }
]
}
```

5. Run the following command to add data for further testing:

```
 PUT  / my_index / doc / 1
{
" title ": " Shall   I   begin ?"
}
```

```
 PUT  / my_index / doc / 2
{
" title ": " I   start   work   at   nine ."
}
```

6. Run the following command to perform a query test:

```
 GET  / my_index / _search
```

```
{
" query " : { " match " : { " title " : " begin " }},
" highlight " : {
  " pre_tags " : ["< red >", "< bule >"],
  " post_tags " : ["</ red >", "</ bule >"],
  " fields " : {
      " title " : {}
  }
}
}
```

7. **If the query is successful, the following results are returned:**

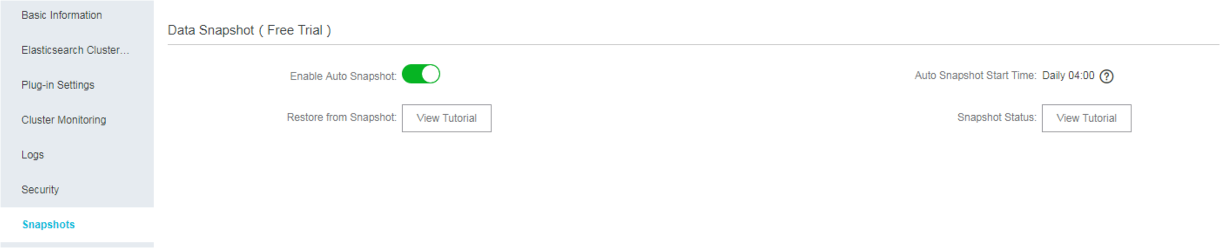
```
{
" took ":  11 ,
" timed_out ":  false ,
" _shards ": {
 " total ":  5 ,
 " successful ":  5 ,
 " failed ":  0 ,
},
" hits ": {
 " total ":  2 ,
 " max_score ":  0 . 41913947 ,
 " hits ": [
   {
     " _index ": " my_index ",
     " _type ": " doc ",
     " _id ": " 2 ",
     " _score ":  0 . 41913947 ,
     " _source ": {
       " title ": " I   start   work   at   nine ."
     },
     " highlight ": {
       " title ": [
         " I  < red > start </ red >  work   at   nine ."
       ]
     }
   },
   {
     " _index ": " my_index ",
     " _type ": " doc ",
     " _id ": " 1 ",
     " _score ":  0 . 39556286 ,
     " _source ": {
       " title ": " Shall   I   begin ?"
     },
     " highlight ": {
       " title ": [
         " Shall   I  < red > begin </ red >?"
       ]
     }
   }
 ]
}
}
```

1.10 Data backup

1.10.1 Snapshots

This topic describes the snapshot feature of Alibaba Cloud Elasticsearch.

Log on to the Alibaba Cloud Elasticsearch console, click Instance Name > Snapshots to navigate to the Snapshots (Free Trial) page.



Data Snapshot (Free Trial)

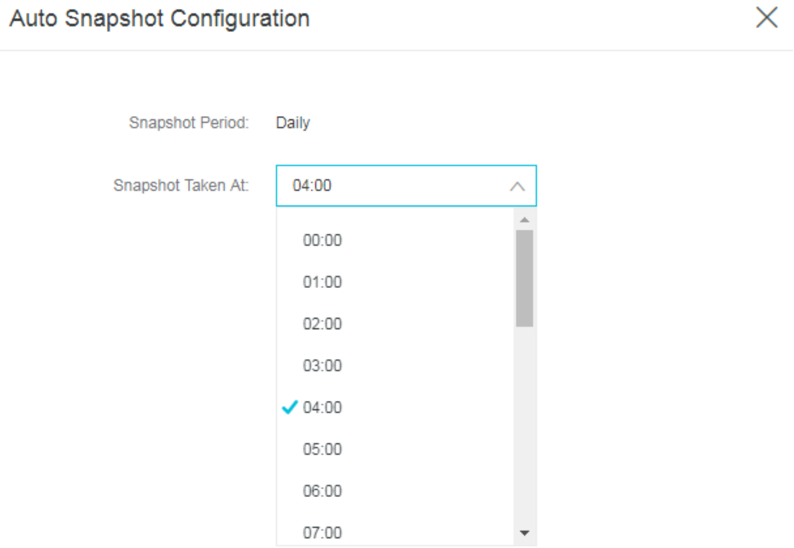
Enable Auto Snapshot:

Auto Snapshot Start Time: Daily 04:00

Restore from Snapshot:

Snapshot Status:

Parameter	Description
Auto Snapshot	When the Auto Snapshot switch is in the green color, auto snapshot is enabled. By default, auto snapshot is disabled.
Auto Snapshot Period	If auto snapshot is disabled, the You must enable auto snapshot first message is displayed. Notice: Auto snapshot uses the system time of the region where the Elasticsearch instance is created. Do not perform any snapshot operations when the system is creating snapshots.

Parameter	Description
Edit Configuration	If auto snapshot is enabled, you can click Edit Configuration in the upper-right corner to open the Auto Snapshot Configuration dialog box and then set the time for creating snapshots.  Auto Snapshot Configuration Snapshot Period: Daily Snapshot Taken At: 04:00 00:00 01:00 02:00 03:00 ✓ 04:00 05:00 06:00 07:00 Notice: · The Frequency parameter is set to Daily. · The Create Snapshot At parameter specifies the specific time for creating a snapshot daily. Valid values are from 0 to 23 hours. · Alibaba Cloud Elasticsearch only stores snapshots that are created in the last three days.
Restore from Snapshot	Click View Tutorial to learn how to restore data from a snapshot.
Snapshot Status	Click View Tutorial to learn more information about snapshot status.

1.10.2 View backup information

View automatic backup information

After enabling automatic backup, you can log on to the Kibana console that has been integrated into Alibaba Cloud Elasticsearch and run the Elasticsearch `snapshot` command in Dev Tools to view snapshots.

View all snapshots

Run the following command to view all the snapshots that are located in the aliyun_auto_snapshot repository.

```
GET   _   snapshot / aliyun_aut  o_snapshot / _   all
```

Response:

```
{
  " snapshots ": [
    {
      " snapshot ": " es - cn - abcdefghij  klmn_20180  628092236 ",
      " uuid ": " n7YIayyZTm  2hwg8BeWby  dA ",
      " version_id ":  5050399 ,
      " version ": " 2 . 0 . 0 ",
      " indices ": [
        ". kibana "
      ],
      " state ": " SUCCESS ",
      " start_time ": " 2018 - 06 - 28T01 : 22 : 39 . 609Z ",
      " start_time  _in_millis ":  1530148959  609 ,
      " end_time ": " 2018 - 06 - 28T01 : 22 : 39 . 923Z ",
      " end_time_i  n_millis ":  1530148959  923 ,
      " duration_i  n_millis ":  314 ,
      " failures ": [],
      " _shards " : {
        " total ": 1
        " failed " :  0
        " successful ":  1 ,
      }
    },
    {
      " snapshot ": " es - cn - abcdefghij  klmn_20180  628092500 ",
      " uuid ": " frdl1YFzQ5  Cn5xN9ZWuK  LA ",
      " version_id ":  5050399 ,
      " version ": " 2 . 0 . 0 ",
      " indices ": [
        ". kibana "
      ],
      " state ": " SUCCESS ",
      " start_time ": " 2018 - 06 - 28T01 : 25 : 00 . 764Z ",
      " start_time  _in_millis ":  1530149100  764 ,
      " end_time ": " 2018 - 06 - 28T01 : 25 : 01 . 482Z ",
      " end_time_i  n_millis ":  1530149101  482 ,
      " duration_i  n_millis ":  718 ,
      " failures ": [],
      " _shards " : {
        " total ": 1
        " failed " :  0
        " successful ":  1 ,
      }
    }
  ]
}
```

- state: Specifies the status of a snapshot. The snapshot status includes the following:
  - `IN_PROGRESS` : The snapshot is being restored.
  - `SUCCESS` : The snapshot has been restored and all shards have been successfully stored.
  - `FAILED` : The snapshot has been restored with an error. Some data cannot be stored.
  - `PARTIAL` : The snapshot has been successfully restored to an instance. However, one or more shards cannot be stored.
  - `INCOMPATIBLE` : The snapshot version is incompatible with the current instance version.

View specified snapshot

Run the following command to view detailed information about the specified snapshot in the aliyun_auto_snapshot repository.

```
GET _snapshot / aliyun_auto_snapshot /< snapshot >/ _status
```

- `< Snapshot >`: Specifies the name of the snapshot, for example, `Es - cn - abcdefghijklmn_20180628092236` .

Response:

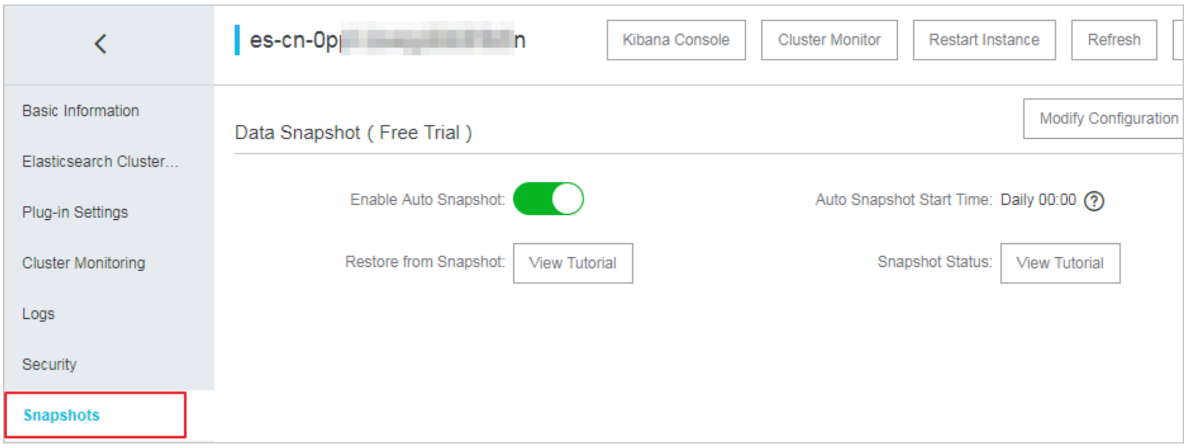
```
{
  " Snapshots ": {
    {
      " snapshot ": " es - cn - abcdefghijklmn_20180628092236 ",
      " repository ": " aliyun_auto_snapshot ",
      " uuid ": " n7YIayyZTm2hwg8BeWbydA ",
      " state ": " SUCCESS ",
      " shards_stats ": {
        " initializing ": 0 ,
        " started ": 0 ,
        " finalizing ": 0 ,
        " done ": 1 ,
        " failed " : 0
        " total ": 2
      },
      " stats ": {
        " number_of_files ": 4 ,
        " processed_files ": 4 ,
        " total_size_in_bytes ": 3296 ,
        " processed_size_in_bytes ": 3296 ,
        " start_time_in_millis ": 1530148959688 ,
        " time_in_millis ": 77
      },
      " indices ": {
        ". kibana ": {
          " shards_sta  ts ": {
            " initializi  ng ":  0 ,
            " started ":  0 ,
            " finalizing ":  0 ,
            " done ":  1 ,
            " failed " :  0
            " total ":  2
          },
          " stats ": {
            " number_of_  files ":  4 ,
            " processed_  files ":  4 ,
            " total_size  _in_bytes ":  3296 ,
            " processed_  size_in_by  tes ":  3296 ,
            " start_time  _in_millis ":  1530148959  688 ,
            " time_in_mi  llis ":  77
          },
          " shards ": {
            " 0 ": {
              " stage ": " DONE ",
              " stats ": {
                " number_of_  files ":  4 ,
                " processed_  files ":  4 ,
                " total_size  _in_bytes ":  3296 ,
                " processed_  size_in_by  tes ":  3296 ,
                " start_time  _in_millis ":  1530148959  688 ,
                " time_in_mi  llis ":  77
              }
            }
          }
        }
      }
    }
  ]
}
```

1.10.3 Auto snapshot guide

Enable auto snapshot

1. Log on to the Alibaba Cloud Elasticsearch console.
2. On the Instances page, click the target instance ID. You will be directed to the Basic Information page.
3. In the left-side navigation pane, click Snapshots.

4. On the Snapshots page, switch on Enable Auto Snapshot.



es-cn-0p[redacted]n

Data Snapshot (Free Trial)

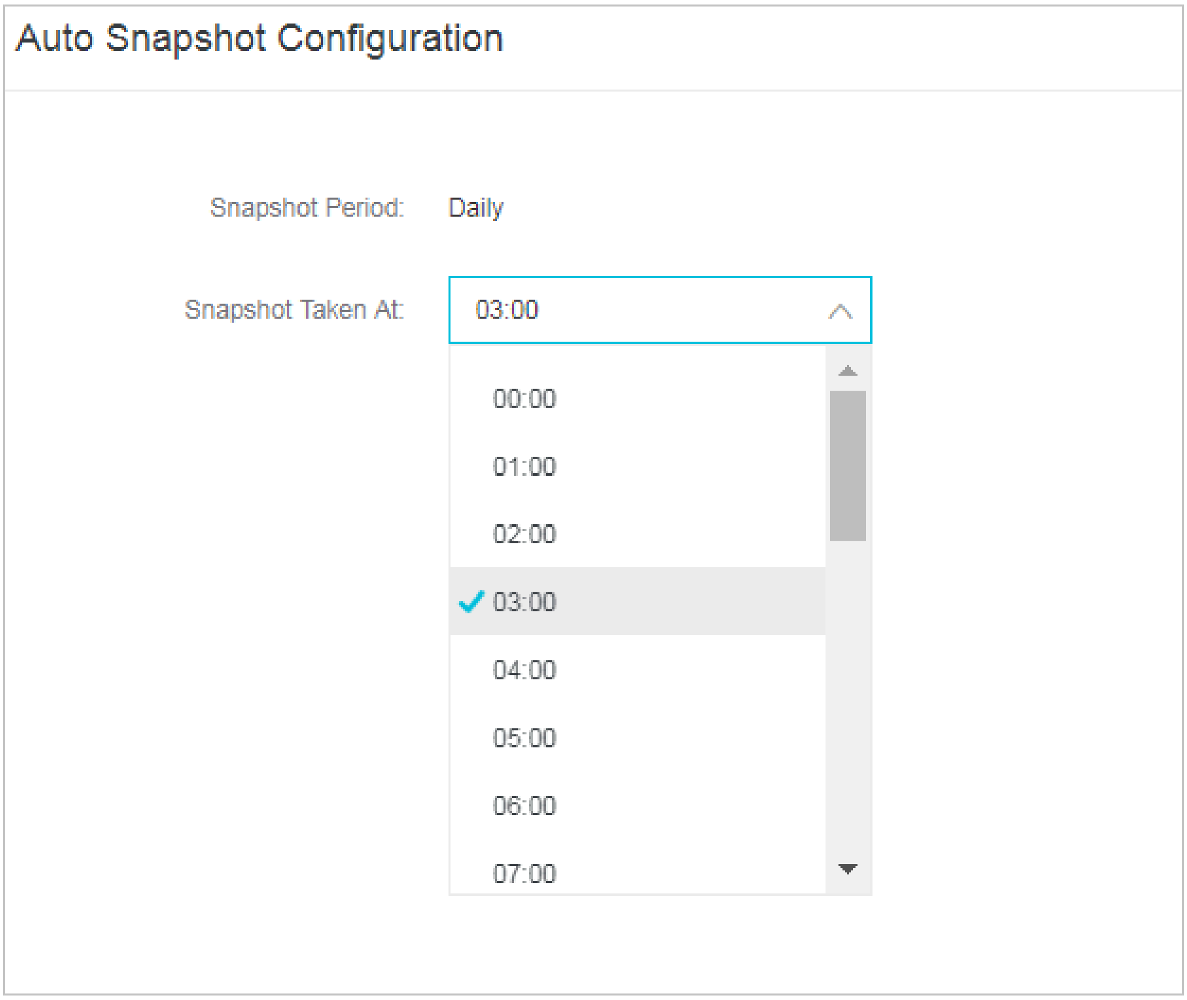
Enable Auto Snapshot: on

Auto Snapshot Start Time: Daily 00:00

Restore from Snapshot: View Tutorial

Snapshot Status: View Tutorial

5. Click Modify Configuration in the upper-right corner to set the time when the daily snapshot is created.



Auto Snapshot Configuration

Snapshot Period: Daily

Snapshot Taken At: 03:00

Restore snapshots into instances

If you have enabled auto snapshot for a specified Alibaba Cloud Elasticsearch instance, snapshots will be automatically created on a daily basis. You can call the corresponding `snapshot` operation to restore a snapshot into the Alibaba Cloud Elasticsearch instance where the snapshot is created.

Note:

- The first snapshot is a complete backup created on a running Alibaba Cloud Elasticsearch instance. The following snapshots are created based on the incremental data of the Elasticsearch instance. Therefore, it takes a longer time to create the first snapshot, but a shorter time to create subsequent snapshots.
- A snapshot does not store monitoring data generated by an Alibaba Cloud Elasticsearch instance, such as the `. monitoring` and `. security_a udit` files.
- An auto snapshot can only be restored into the Alibaba Cloud Elasticsearch instance where the snapshot is created.
- An auto snapshot repository is created when the first snapshot is created.

View all snapshot repositories

You can run the `GET _snapshot` command to view all snapshot repositories.

The following response is returned:

```
{
  " aliyun_aut  o_snapshot ": {
    " type ": " oss ",
    " settings ": {
      " compress ": " true ",
      " base_path ": " xxxx ",
      " endpoint ": " xxxx "
    }
  }
}
```

- `aliyun_aut  o_snapshot` : the name of the repository.
- `type` : the storage medium where snapshots are stored. This example uses Alibaba Cloud Object Storage Service (OSS).
- `compress : true` : enables compression of an index's metadata files.
- `base_path` : the location of the snapshots.
- `endpoint` : the region of the OSS instance.

View all snapshots

You can run the `GET _snapshot / aliyun_aut o_snapshot / _all` command to view all snapshots stored in the repository `aliyun_aut o_snapshot`

The following response is returned:

```
{
  " snapshots ": [
    {
      " snapshot ": " es - cn - abcdefghij  klmn_20180  627091600 ",
      " uuid ": " MMRniVLPRA  iawSCm8D8D  ug ",
      " version_id ":  5050399 ,
      " version ": " 5 . 5 . 3 ",
      " indices ": [
        " index_1 ",
        ". security ",
        ". kibana "
      ],
      " state ": " SUCCESS ",
      " start_time ": " 2018 - 06 - 27T01 : 16 : 01 . 009Z ",
      " start_time  _in_millis ":  1530062161  009 ,
      " end_time ": " 2018 - 06 - 27T01 : 16 : 05 . 632Z ",
      " end_time_i  n_millis ":  1530062165  632 ,
      " duration_i  n_millis ":  4623 ,
      " failures ": [],
      " shards ": {
        " total ":  12 ,
        " failed ":  0 ,
        " successful ":  12
      }
    }
  ]
}
```

Default parameters

Auto snapshots also support the following parameters that are not displayed:

- `max_snapsh ot_bytes_p er_sec : 40mb` : throttles per node snapshot rate. The default snapshot rate is 40 MB per second.
- `max_restor e_bytes_pe r_sec : 40mb` : throttles per node restore rate. The default restore rate is 40 MB per second.
- `chunk_size : Max 1Gb` : large files can be broken into smaller chunks during the snapshot process if needed. The maximum size of a chunk is 1 GB.

Restore a snapshot into an instance

You can run the `_restore` command to restore a snapshot into an instance:

- Restore all indexes in a specified snapshot that is stored in the `aliyun_auto_snapshot` repository. The restore tasks are executed in the background.

  ```
   POST   _snapshot / aliyun_auto_snapshot /< snapshot >/ _restore
  ```

  `< snapshot >`: replace it with the name of the specified snapshot. Example: `es - cn - abcdefghijklmn_20180627091600`

- Restore all indexes in the specified snapshot that is stored in the `aliyun_auto_snapshot` repository, and receive a response after all restore tasks are completed:

  The `_restore` command runs restore tasks asynchronously. The Alibaba Cloud Elasticsearch instance will return a response immediately if the restore command is executable. Restore tasks are executed in the background. You can add the `wait_for_completion` parameter to the command. This parameter requires the Alibaba Cloud Elasticsearch instance to return the response only after the restore tasks are completed.

  ```
   POST   _snapshot / aliyun_auto_snapshot /< snapshot >/ _restore
   ?  wait_for_completion = true
  ```

  `< snapshot >`: replace it with the name of the specified snapshot. Example: `es - cn - abcdefghijklmn_20180627091600`.

- Restore indexes in the specified snapshot that is stored in the `aliyun_auto_snapshot` repository, and rename the restored indexes. The restore tasks are executed in the background.

  ```
   POST   _snapshot / aliyun_auto_snapshot /< snapshot >/ _restore
  {
  " indices ": " index_1 ",
  " rename_pattern ": " index_ (.+)",
  " rename_replacement ": " restored_index_ $ 1 "
  }
  ```

  - `< snapshot >`: replace it with the name of the specified snapshot. Example: `es - cn - abcdefghijklmn_20180627091600`.
  - `indices`: specifies names of the indexes that you need to restore.
  - `rename_pattern`: uses a regular expression to match the restored indexes. This parameter is optional.
  - `rename_replacement`: renames the index that matches the regular expression. This parameter is optional.

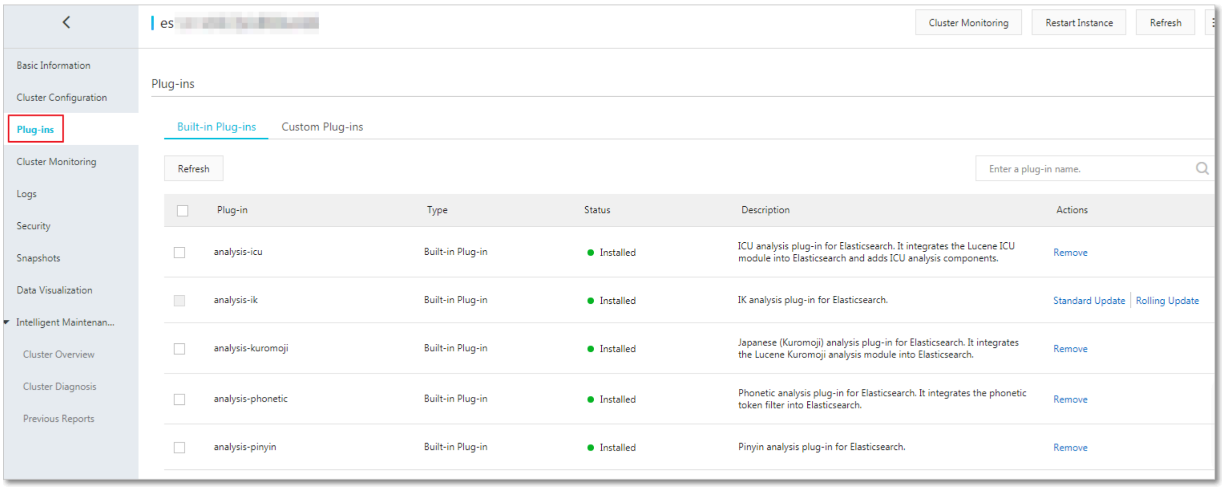
1.11 Plug-ins

1.11.1 Overview

Based on open-source community plug-ins, Alibaba Cloud Elasticsearch provides a variety of plug-ins and other extensions. The topic describes the plug-ins feature of Alibaba Cloud Elasticsearch. This feature allows you to use plug-ins provided by Alibaba Cloud Elasticsearch to meet business demands.

Use plug-ins

Log on to the Alibaba Cloud Elasticsearch console, and select Instance ID > Plug-ins.



☐	Plug-in	Type	Status	Description	Actions
☐	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.	Remove
☐	analysis-ik	Built-in Plug-in	● Installed	IK analysis plug-in for Elasticsearch.	Standard Update | Rolling Update
☐	analysis-kuromoji	Built-in Plug-in	● Installed	Japanese (Kuromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis module into Elasticsearch.	Remove
☐	analysis-phonetic	Built-in Plug-in	● Installed	Phonetic analysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.	Remove
☐	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.	Remove

On the Plug-ins page, you can check Built-in Plug-ins and Custom Plug-ins.

- Built-in plug-ins

  You cannot remove the analysis-ik and elasticsearch-repository-oss plug-ins in the Built-in Plug-ins list. With the analysis-ik plug-in, you can use the standard update or rolling update method to upload and update IK dictionaries. This allows you to update customized dictionaries. For more information, see #unique_36.

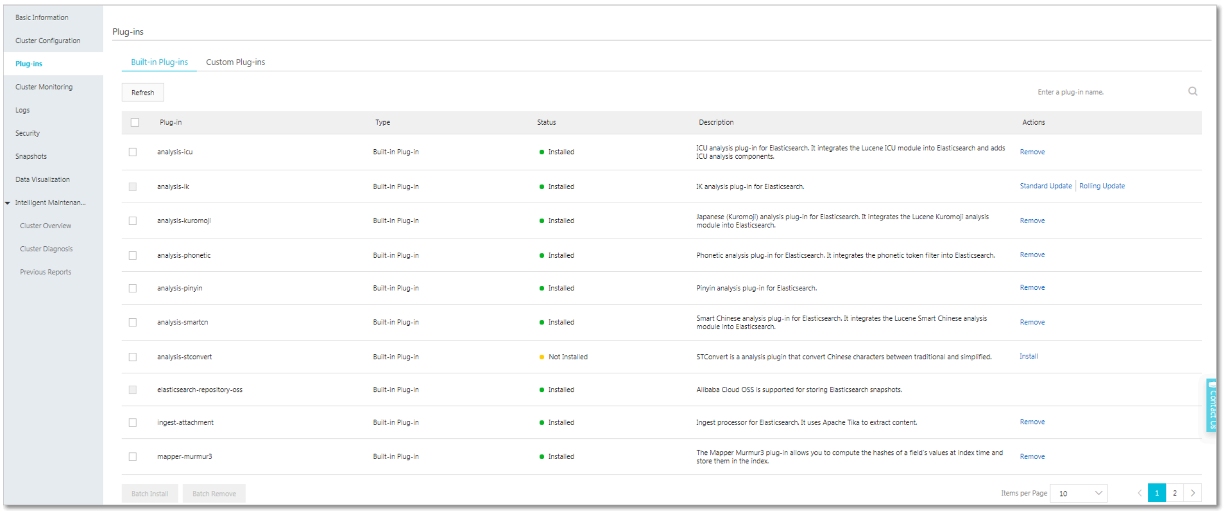
- Custom plug-ins

  You can upload, install, and remove custom plug-ins to meet your business demands. For more information, see #unique_37.

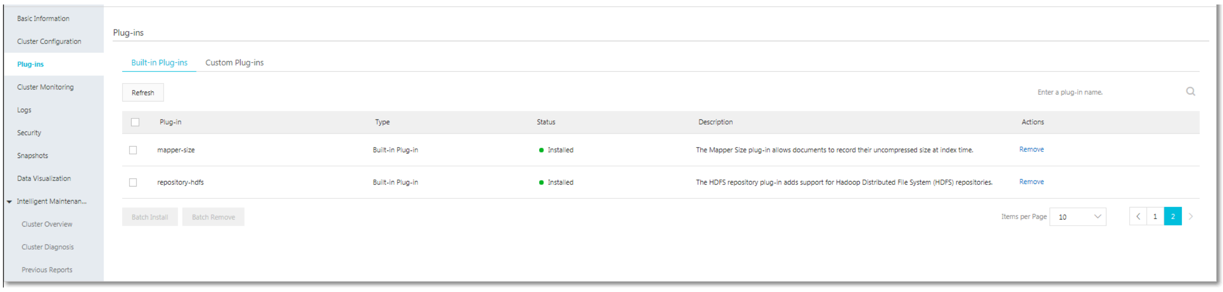
1.11.2 Built-in plug-ins

This topic describes the built-in plug-ins supported by Alibaba Cloud Elasticsearch, and introduces the standard update and rolling update methods for updating IK analyzer plug-ins.

The following figure shows the built-in plug-ins supported by Alibaba Cloud Elasticsearch:



☐	Plug-in	Type	Status	Description	Actions
☐	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.	Remove
☐	analysis-ik	Built-in Plug-in	● Installed	IK analysis plug-in for Elasticsearch.	Standard Update | Rolling Update
☐	analysis-kuromoji	Built-in Plug-in	● Installed	Japanese (Kuromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis module into Elasticsearch.	Remove
☐	analysis-phonetic	Built-in Plug-in	● Installed	Phonetic analysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.	Remove
☐	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.	Remove
☐	analysis-smartcn	Built-in Plug-in	● Installed	Smart Chinese analysis plug-in for Elasticsearch. It integrates the Lucene Smart Chinese analysis module into Elasticsearch.	Remove
☐	analysis-stconvert	Built-in Plug-in	● Not Installed	STConvert is a analysis plugin that convert Chinese characters between traditional and simplified.	Install
☐	elasticsearch-repository-oss	Built-in Plug-in	● Installed	Alibaba Cloud OSS is supported for storing Elasticsearch snapshots.	
☐	ingest-attachment	Built-in Plug-in	● Installed	Ingest processor for Elasticsearch. It uses Apache Tika to extract content.	Remove
☐	mapper-murmur3	Built-in Plug-in	● Installed	The Mapper Murmur3 plug-in allows you to compute the hashes of a field's values at index time and store them in the index.	Remove



☐	Plug-in	Type	Status	Description	Actions
☐	mapper-size	Built-in Plug-in	● Installed	The Mapper Size plug-in allows documents to record their uncompressed size at index time.	Remove
☐	repository-hdfs	Built-in Plug-in	● Installed	The HDFS repository plug-in adds support for Hadoop Distributed File System (HDFS) repositories.	Remove

After you purchase an Alibaba Cloud Elasticsearch instance, the system will automatically install the plug-ins in the Built-in Plug-ins list. You can also manually install or remove these plug-ins as needed. The analysis-ik and elasticsearch-repository-oss plug-ins are extensions of Alibaba Cloud Elasticsearch. You cannot remove these plug-ins.

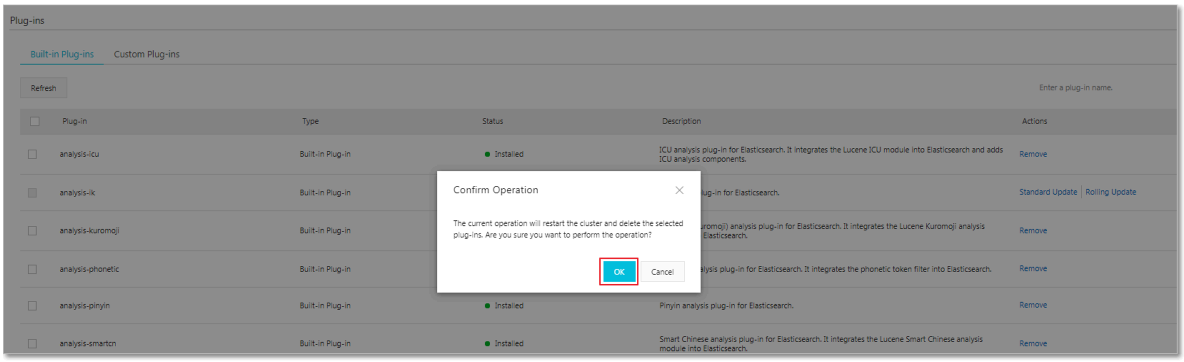
- analysis-ik: an IK analyzer plug-in. Based on open-source plug-ins, this plug-in supports dynamically loading dictionary files stored on Object Storage Service (OSS). You can use the standard update or rolling update method to update dictionary files.
- elasticsearch-repository-oss: based on open-source plug-ins, this plug-in allows you to use OSS for storage when creating and restoring index snapshots.

Install or remove built-in plug-ins

Notice:
To install or remove a built-in plug-in, Elasticsearch must restart the cluster. If you remove a built-in plug-in, Elasticsearch will delete the plug-in. You must confirm the operation before you can proceed.

The following example shows how to remove the analysis-kuromoji plug-in.

1. Click Remove in the Actions column on the right side of the analysis-kuromoji plug-in.
2. Read the note in the Confirm Operation dialog box carefully and then click OK.

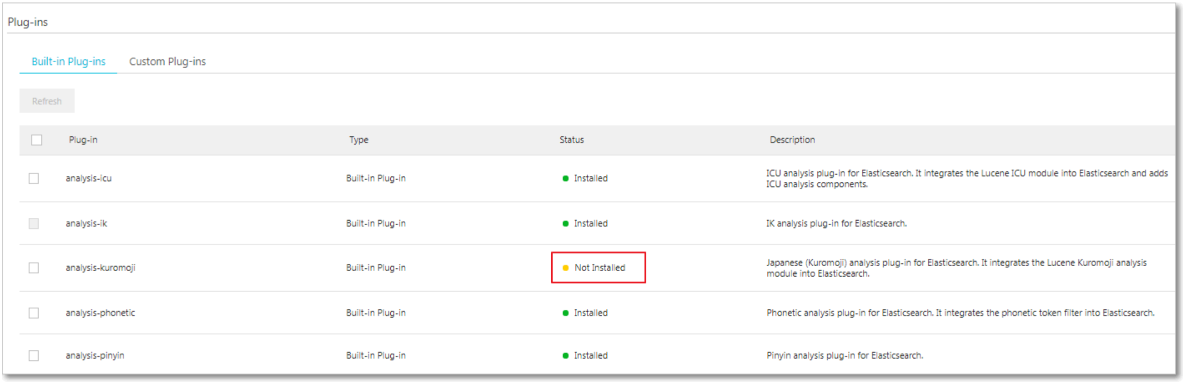


☐	Plug-in	Type	Status	Description	Actions
☐	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.	Remove
☐	analysis-ik	Built-in Plug-in		lug-in for Elasticsearch.	Standard Update | Rolling Update
☐	analysis-kuromoji	Built-in Plug-in		uromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis Elasticsearch.	Remove
☐	analysis-phonetic	Built-in Plug-in		lysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.	Remove
☐	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.	Remove
☐	analysis-smartcn	Built-in Plug-in	● Installed	Smart Chinese analysis plug-in for Elasticsearch. It integrates the Lucene Smart Chinese analysis module into Elasticsearch.	Remove

Confirm Operation

The current operation will restart the cluster and delete the selected plug-ins. Are you sure you want to perform the operation?

After you confirm the operation, the cluster is restarted. After the cluster is restarted, the status of the analysis-kuromoji plug-in changes to Not Installed. This indicates that the plug-in has been removed.



☐	Plug-in	Type	Status	Description
☐	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.
☐	analysis-ik	Built-in Plug-in	● Installed	IK analysis plug-in for Elasticsearch.
☐	analysis-kuromoji	Built-in Plug-in	● Not Installed	Japanese (Kuromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis module into Elasticsearch.
☐	analysis-phonetic	Built-in Plug-in	● Installed	Phonetic analysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.
☐	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.

If you want to use this plug-in again, follow these steps to re-install the plug-in.

3. Click Install on the right side of the plug-in to install the plug-in.

   Elasticsearch will restart the cluster to install the plug-in. After the cluster is restarted, the status of the plug-in displays Installed. This indicates that the plug-in has been installed.

Update IK dictionaries

The IK analyzer plug-in of Alibaba Cloud Elasticsearch allows you to use the following methods to update IK dictionaries:

- Standard update
- Rolling update

Note:

For indexes that are already configured with IK analyzers, the updated dictionary is only applied to new data in these indexes. If you want to apply the updated dictionary to both the existing data and new data, you must recreate these indexes.

Standard update

The standard update method updates the dictionary on all nodes in an Elasticsearch cluster. If you choose the standard update method, Elasticsearch will send the uploaded dictionary file to all nodes in the cluster, modify the *`IKAnalyzer.cfg.xml`* file, and then restart the nodes to load the uploaded dictionary file.

You can use the standard update method to update the IK main dictionary and stopword list. On the standard update page, you can check the built-in main dictionary `SYSTEM_MAIN.dic` and stopword list `SYSTEM_STOPWORD.dic`.

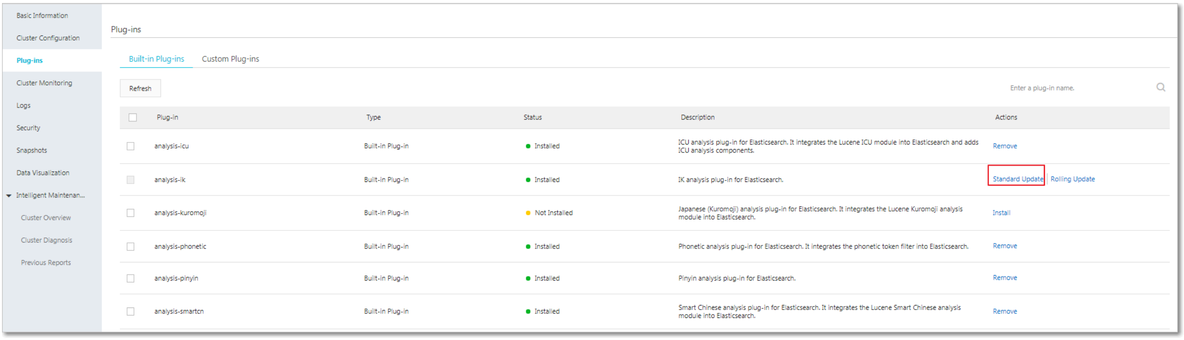
Note:

- If you want to update the built-in main dictionary, upload a dictionary file named as SYSTEM_MAIN.dic.
- If you want to update the built-in stopword list, upload a dictionary file named as SYSTEM_STOPWORD.dic.

Standard update example

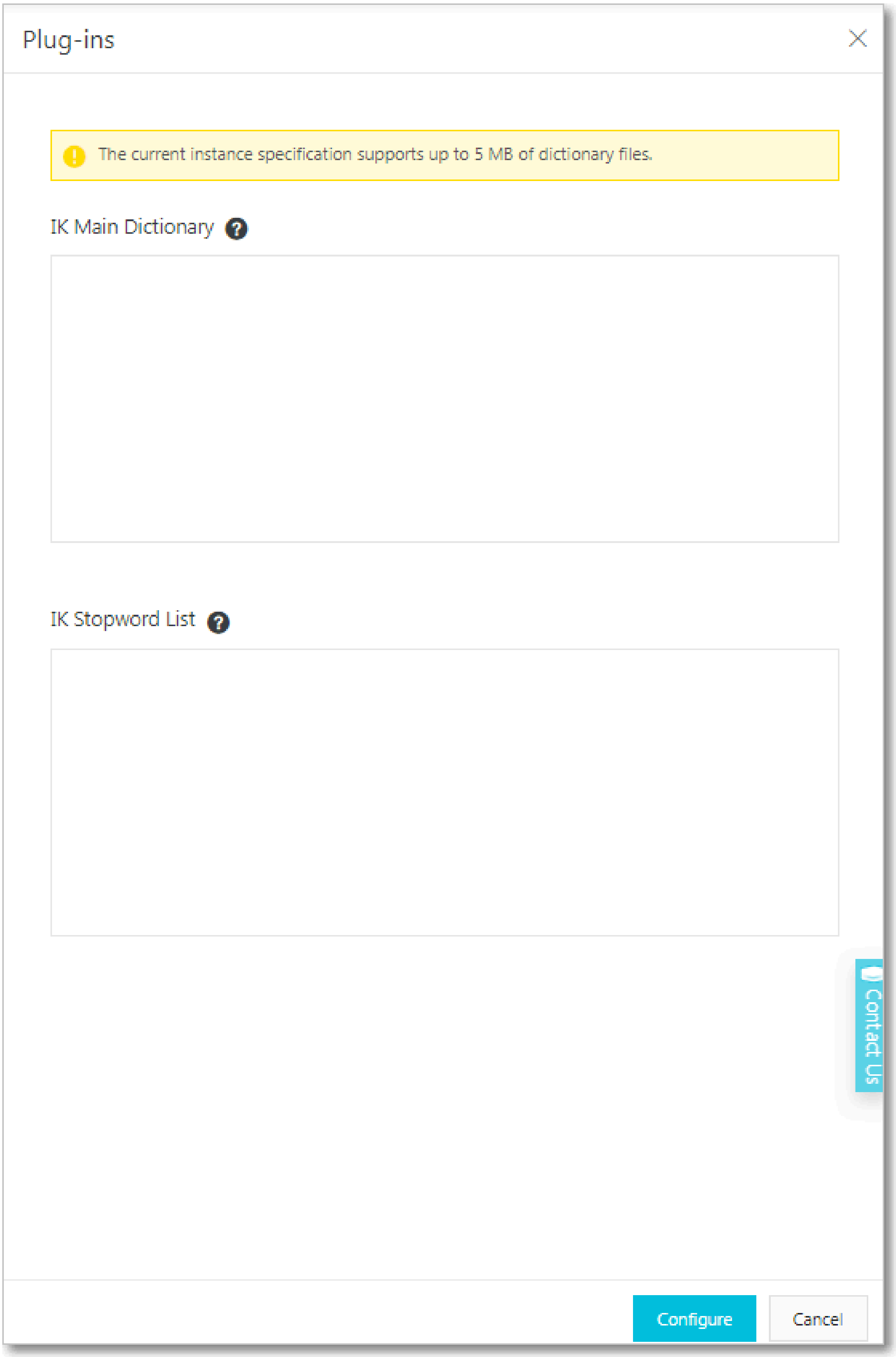
1. Log on to the Alibaba Cloud Elasticsearch console, and click the ID of the Elasticsearch instance that you want to update IK dictionaries for.

2. In the left-side navigation pane, click Plug-ins, locate the plug-in that you want to update, click Standard Update in the Actions column.



□	Plug-in	Type	Status	Description	Actions
□	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.	Remove
□	analysis-ik	Built-in Plug-in	● Installed	IK analysis plug-in for Elasticsearch.	Standard Update | Rolling Update
□	analysis-kuromoji	Built-in Plug-in	● Not Installed	Japanese (Kuromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis module into Elasticsearch.	Install
□	analysis-phonetic	Built-in Plug-in	● Installed	Phonetic analysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.	Remove
□	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.	Remove
□	analysis-smartcn	Built-in Plug-in	● Installed	Smart Chinese analysis plug-in for Elasticsearch. It integrates the Lucene Smart Chinese analysis module into Elasticsearch.	Remove

3. In the Plug-in Configuration dialog box, click Configure.



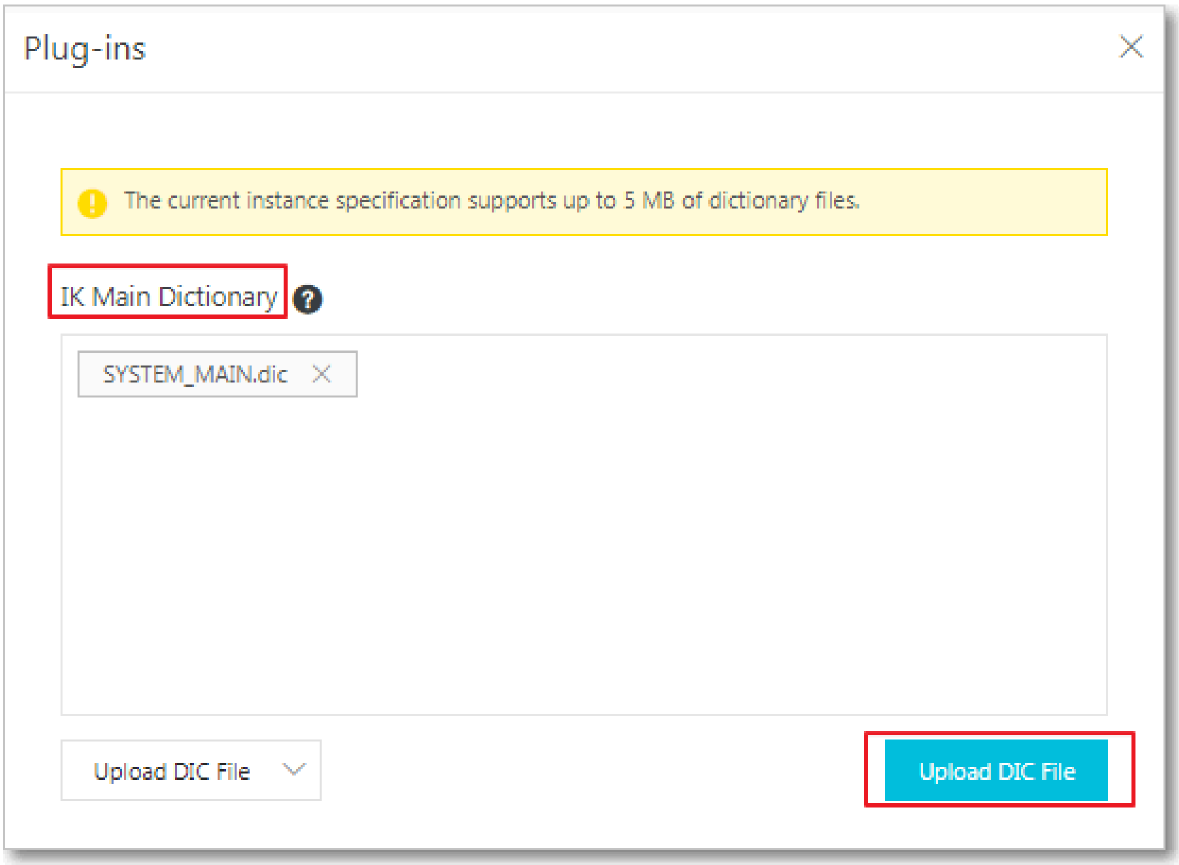
Plug-ins

The current instance specification supports up to 5 MB of dictionary files.

IK Main Dictionary

IK Stopword List

4. Click Upload DIC File under IK Main Dictionary, and upload a custom main dictionary file.



The current instance specification supports up to 5 MB of dictionary files.

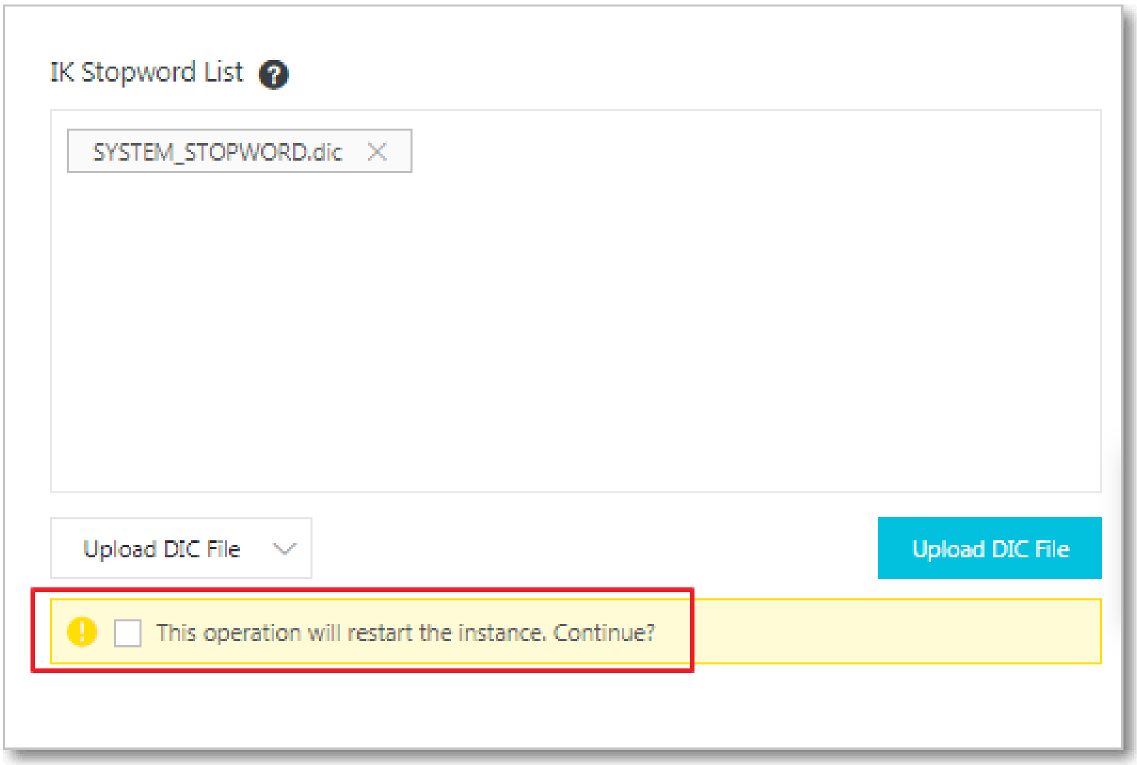
Note:

You can upload a dic file or add an OSS file. If the content of the dictionary file stored in the cloud or on your local host changes, you must use these methods to manually upload the dictionary file to update the dictionary.

5. Notice:

This operation will restart the Elasticsearch instance. Make sure that your businesses are not affected before you confirm the operation.

Scroll down to the bottom, select This operation will restart the instance. Continue? to confirm the operation, and click Save.



6. After the cluster is restarted, log on to the Kibana console, and then run the following command to verify the update is effective:

```
 GET   _analyze
{
" analyzer ": " ik_smart ",
" text ": [" tokens   in   your   updated   dictionary "]
}
```

Notice:

- You cannot delete the built-in main dictionary and stopword list.
- Whether you upload a new dictionary file, remove a dictionary file, or update the dictionary content, the standard update operation always requires Elasticsearch to restart the cluster.
- You can perform the standard update operation only when the status of the cluster is healthy.

Rolling update

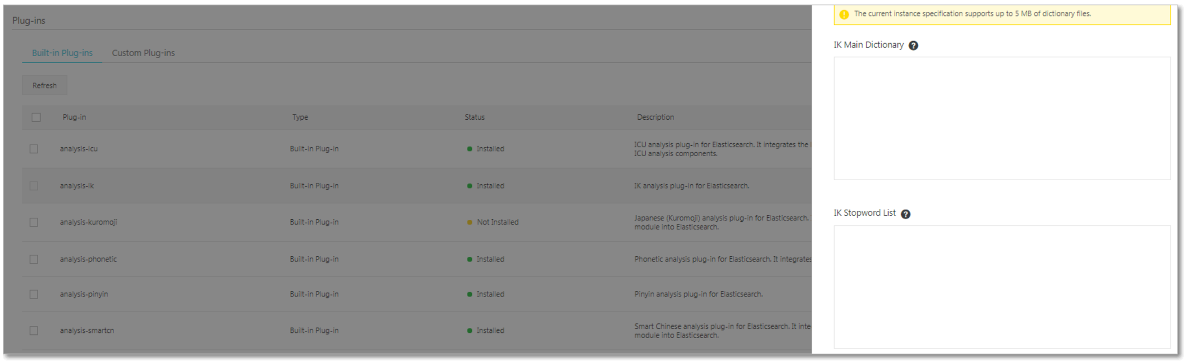
When the content of your dictionary file changes, you can use the rolling update method to update the dictionary. After you upload the latest dictionary file, the Elasticsearch nodes will automatically load the file.

When you perform a rolling update, if the dictionary file list changes, all nodes in the cluster need to reload the dictionary configuration. For example, when you upload a new dictionary file or delete an existing dictionary file, the changes will be updated to the `IKAnalyzer.cfg.xml` file.

The procedure of rolling update is similar to standard update. If this is the first time that you have uploaded a dictionary file, you must edit the `IKAnalyzer.cfg.xml` configuration file. This means that Elasticsearch needs to restart the cluster to reload the configuration file.

Rolling update example

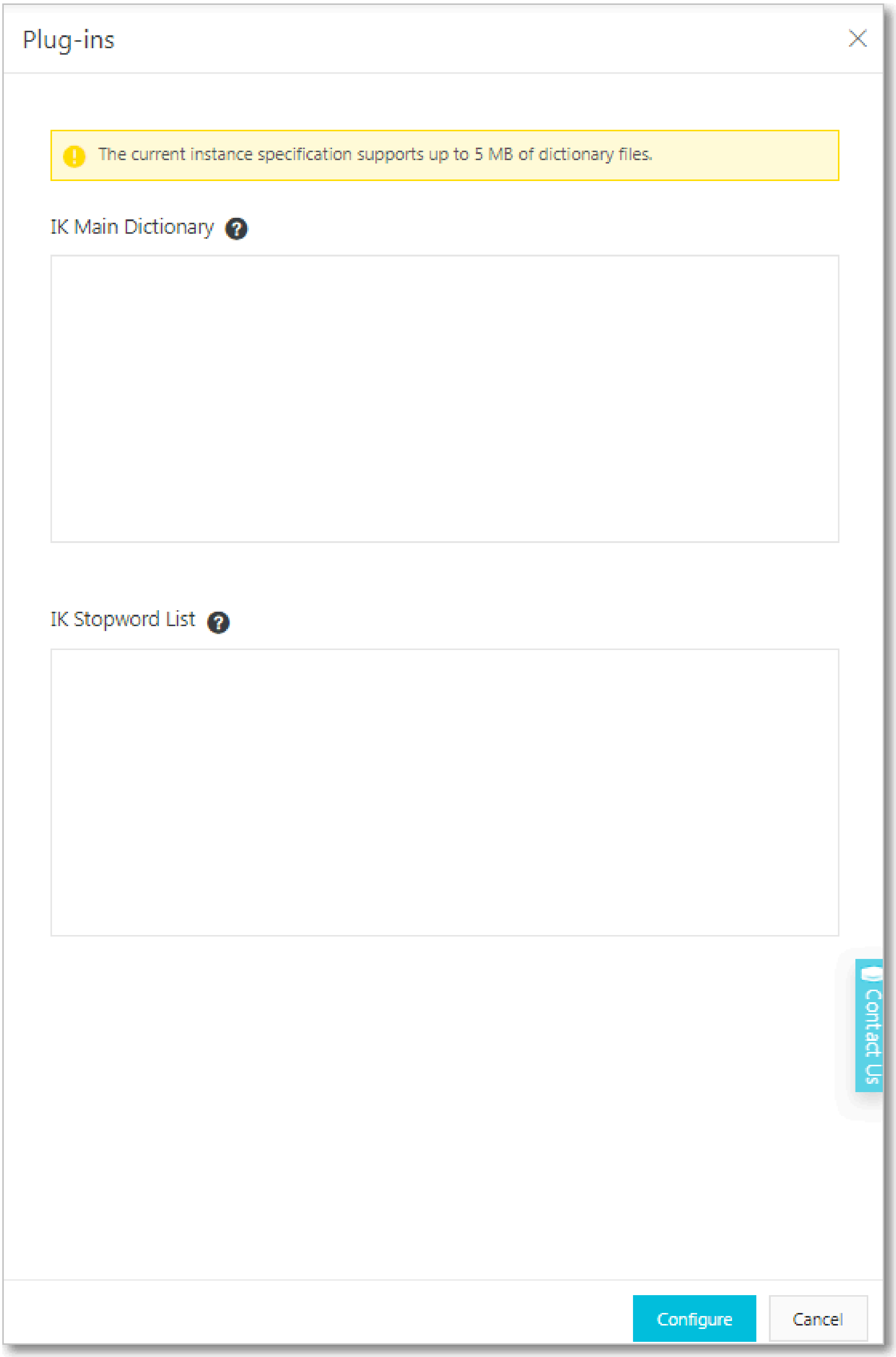
1. Log on to the Alibaba Cloud Elasticsearch console and click the ID of the Elasticsearch instance that you want to update the dictionaries for.
2. In the left-side navigation pane, click Plug-ins, locate the plug-in that you need to update, and click Rolling Update in the Actions column.



□	Plug-in	Type	Status	Description
□	analysis-icu	Built-in Plug-in	● Installed	ICU analysis plug-in for Elasticsearch. It integrates the ICU analysis components.
□	analysis-ik	Built-in Plug-in	● Installed	IK analysis plug-in for Elasticsearch.
□	analysis-kuromoji	Built-in Plug-in	● Not Installed	Japanese (Kuromoji) analysis plug-in for Elasticsearch. module into Elasticsearch.
□	analysis-phonetic	Built-in Plug-in	● Installed	Phonetic analysis plug-in for Elasticsearch. It integrates
□	analysis-pinyin	Built-in Plug-in	● Installed	Pinyin analysis plug-in for Elasticsearch.
□	analysis-smartcn	Built-in Plug-in	● Installed	Smart Chinese analysis plug-in for Elasticsearch. It inte module into Elasticsearch.

The current instance specification supports up to 5 MB of dictionary files.

3. In the Plug-in Configuration dialog box, click Configure.



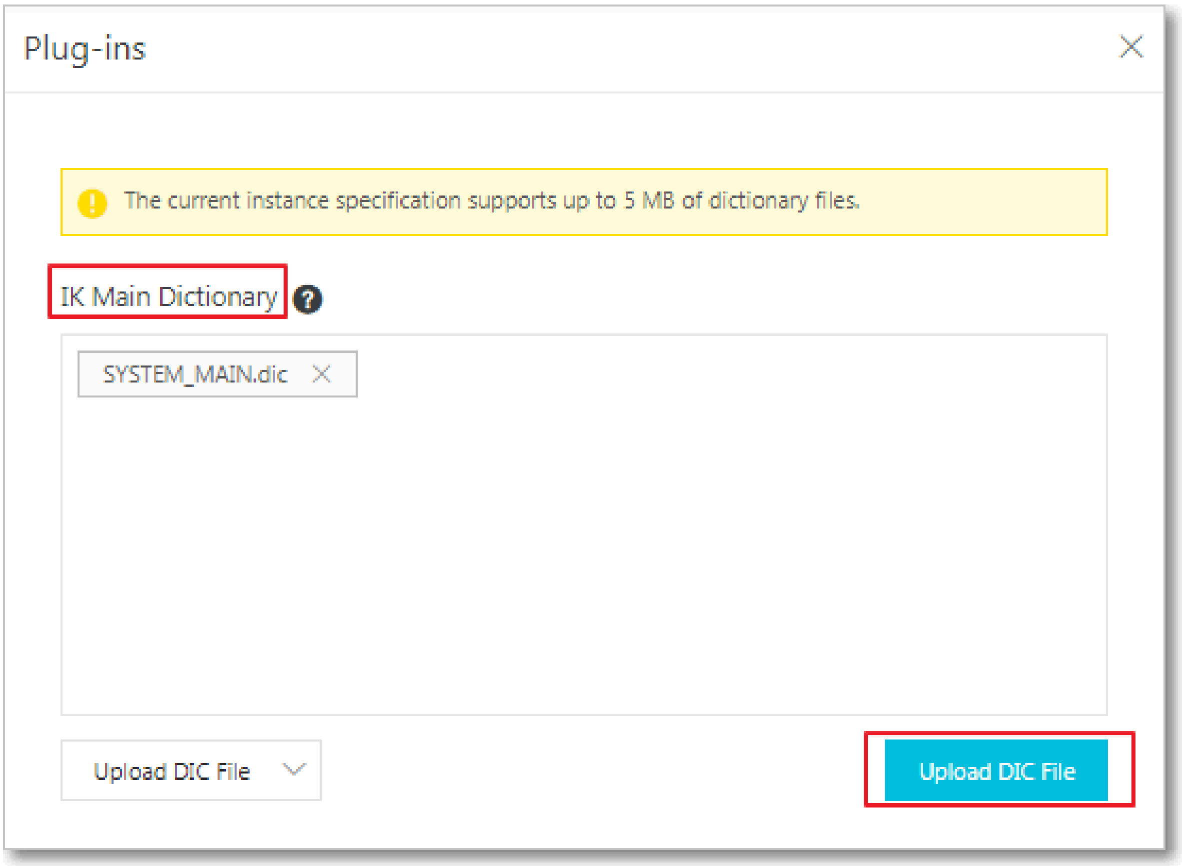
Plug-ins

The current instance specification supports up to 5 MB of dictionary files.

IK Main Dictionary

IK Stopword List

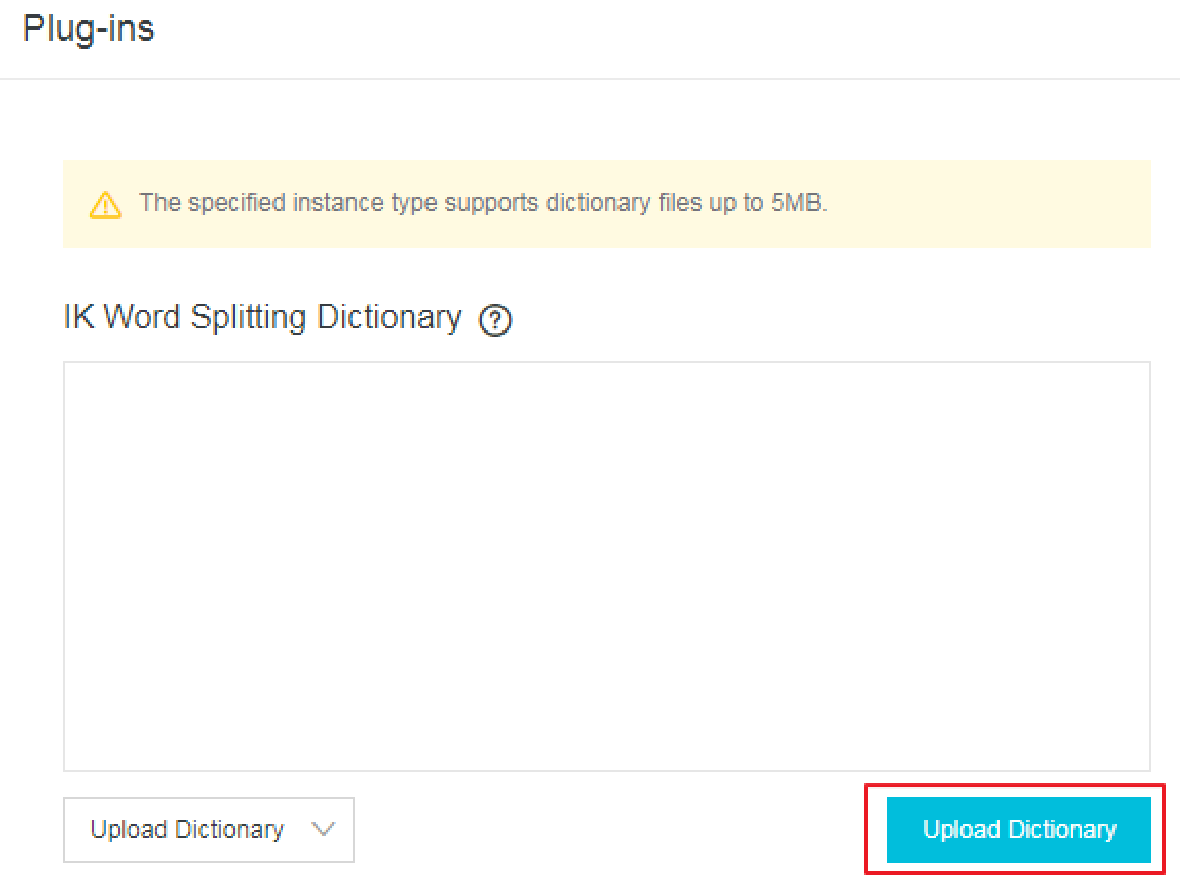
4. Click Upload DIC File under IK Main Dictionary, and upload a custom main dictionary file.



Plug-ins

The current instance specification supports up to 5 MB of dictionary files.

IK Main Dictionary



Plug-ins

The specified instance type supports dictionary files up to 5MB.

IK Word Splitting Dictionary

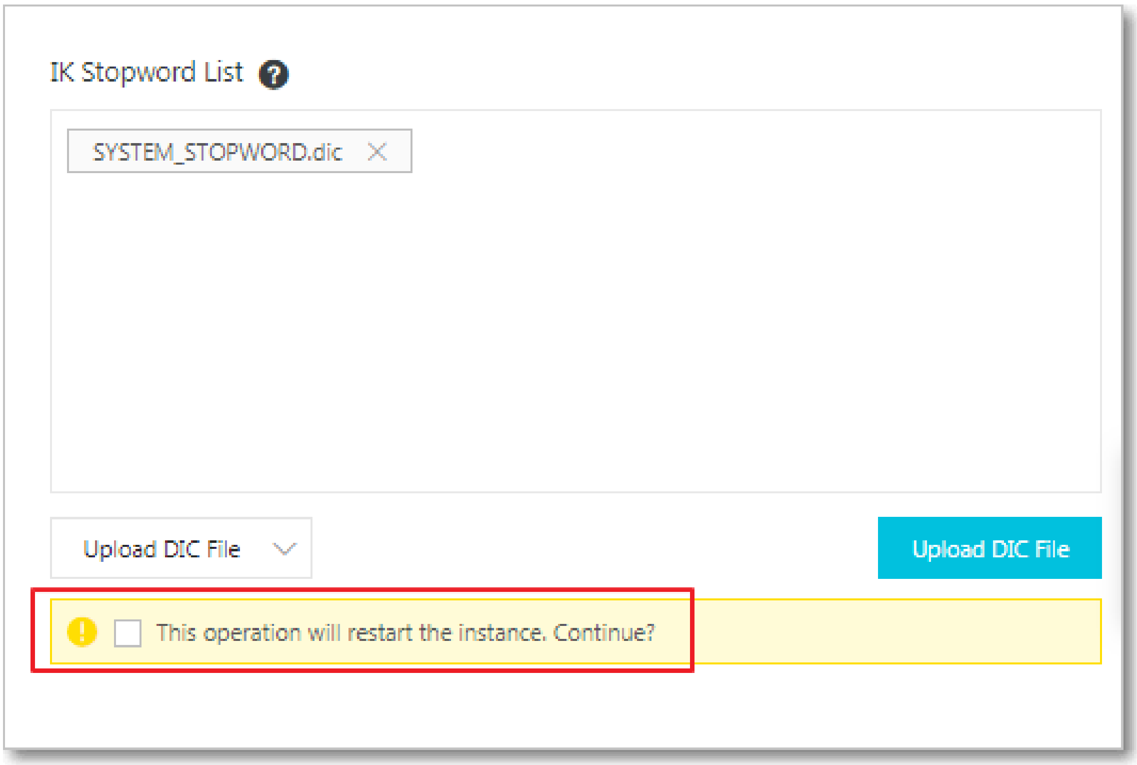
Note:

You can upload a dic file or add an OSS file. If the content of the dictionary file stored in the cloud or on your local host changes, you must use these methods to manually upload the dictionary file to update the dictionary.

5. Notice:

This operation will restart the Elasticsearch instance. Make sure that your businesses are not affected before you confirm the operation.

Scroll down to the bottom, select the This operation will restart the instance. Continue? check box to confirm the operation, and click Save. Elasticsearch needs to restart the cluster only if this is the first time that you have uploaded a dictionary file.


IK Stopword List

SYSTEM_STOPWORD.dic

□ This operation will restart the instance. Continue?

After you click Save, the cluster will perform a rolling update. After the rolling update is complete, the updated dictionary takes effect.

If you need to add tokens to or remove tokens from the updated dictionary, follow these steps to replace the `a_10words . dic` dictionary file.

6. In the rolling update dialog box, delete the existing dictionary file, and then upload a new dictionary file named as `a_10words . dic` .

   This task changes the content of an existing dictionary file on the cluster. Therefore, Elasticsearch does not need to restart the cluster for the update to take effect, as shown in the following figure.

7. Click Save.

   The plug-in on the nodes of the Elasticsearch cluster will automatically load the dictionary file. The time that each node takes to load the dictionary file varies. Please wait for the new dictionary to take effect. It may take about two minutes for all nodes to upload the dictionary file. You can log on to the Kibana console and run the following command to verify that the new dictionary is effective.

```
 GET   _analyze
{
" analyzer ": " ik_smart ",
" text ": [" tokens   in   your   updated   dictionary "]
}
```

Note:

You can not use the rolling update method to edit the built-in main dictionary. If you want to modify the built-in main dictionary, use the standard update method.

For more information, see elasticsearch-analysis-ik.

1.11.3 Custom plug-ins

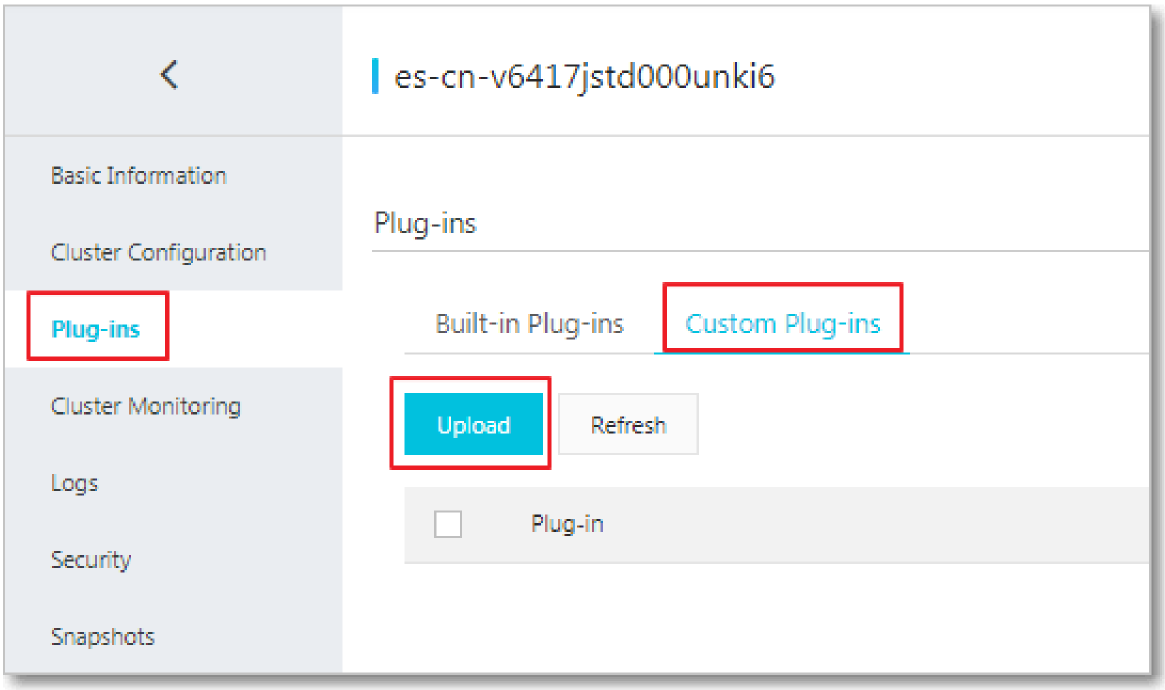
This topic describes how to upload, install, and remove custom plug-ins for Alibaba Cloud Elasticsearch.

Upload and install a custom plug-in

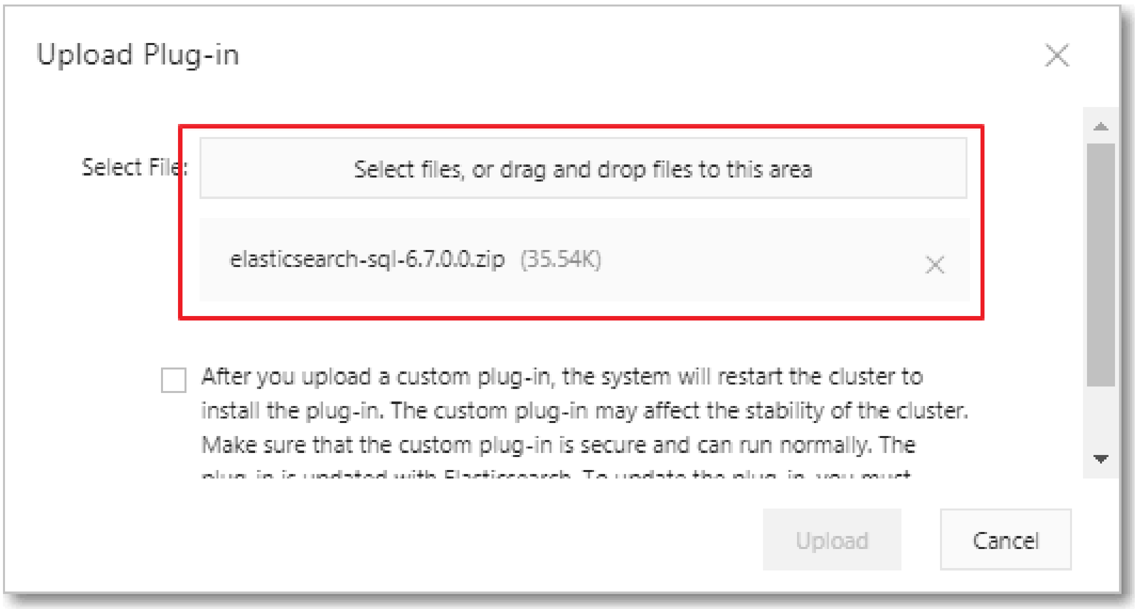
Notice:

- After you upload a custom plug-in, Elasticsearch needs to restart the cluster to install the plug-in. The custom plug-in may adversely affect the stability of the cluster. Make sure that the uploaded custom plug-in is secure and can run normally on the cluster.
- When the Elasticsearch cluster is upgraded, it will not upgrade the custom plug-in at the same time. To upgrade the plug-in, you have to upload the new version of the plug-in to the cluster.
- If your plug-in is not included in any privacy policies, we hope that you can make it open-source to help us develop our open-source community plug-ins.

1. On the Plug-ins page, select Custom Plug-ins > Upload.



2. In the Upload Plug-in dialog box, click Select files, or drag and drop files to this area, and select the custom plug-in that you want to upload.


Upload Plug-in
Select File:
Select files, or drag and drop files to this area
elasticsearch-sql-6.7.0.0.zip (35.54K)
Upload
Cancel

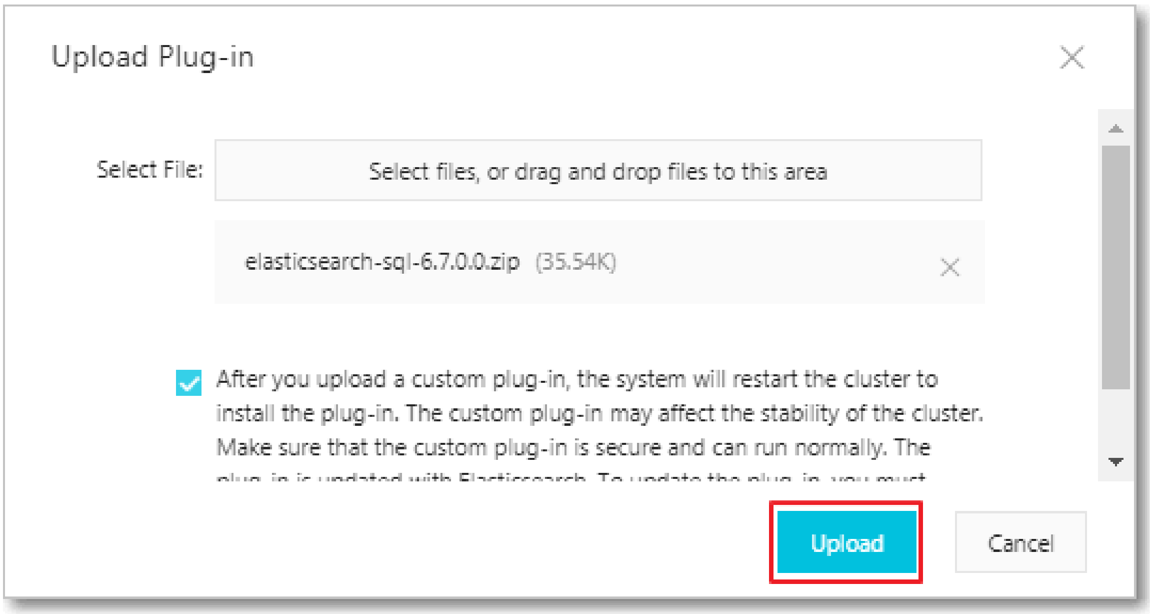
□ After you upload a custom plug-in, the system will restart the cluster to install the plug-in. The custom plug-in may affect the stability of the cluster. Make sure that the custom plug-in is secure and can run normally. The plug-in is updated with Elasticsearch. To update the plug-in, you must

You can also drag and drop a custom plug-in file to this area to upload the plug-in. As shown in the preceding figure, the plug-in file Elasticsearch-sql-6.7.0.0 has been added.

Note:

You can add multiple custom plug-ins in the same way.

3. Read the agreement carefully, select the check box, and click Upload.



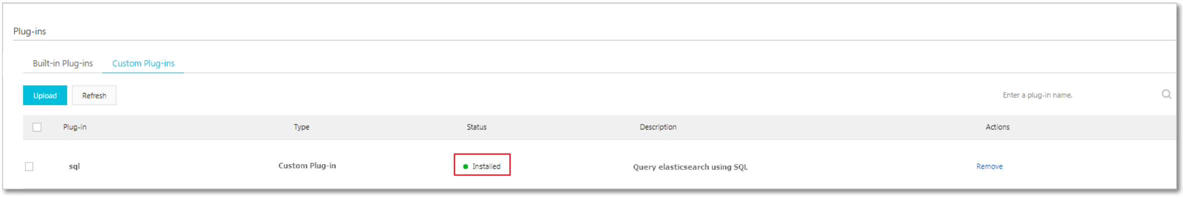
Upload Plug-in

Select File: Select files, or drag and drop files to this area

elasticsearch-sql-6.7.0.0.zip (35.54K)

☑ After you upload a custom plug-in, the system will restart the cluster to install the plug-in. The custom plug-in may affect the stability of the cluster. Make sure that the custom plug-in is secure and can run normally. The plug-in is updated with Elasticsearch. To update the plug-in, you must

After you upload the plug-in, Elasticsearch will restart the cluster to install the plug-in. After the cluster is restarted, you can check the plug-in in the Custom Plug-ins list. The status of the plug-in that you upload will display Installed. This indicates that the plug-in has been uploaded and installed successfully.



Plug-ins

□	Plug-in	Type	Status	Description	Actions
□	sql	Custom Plug-in	● Installed	Query elasticsearch using SQL	Remove

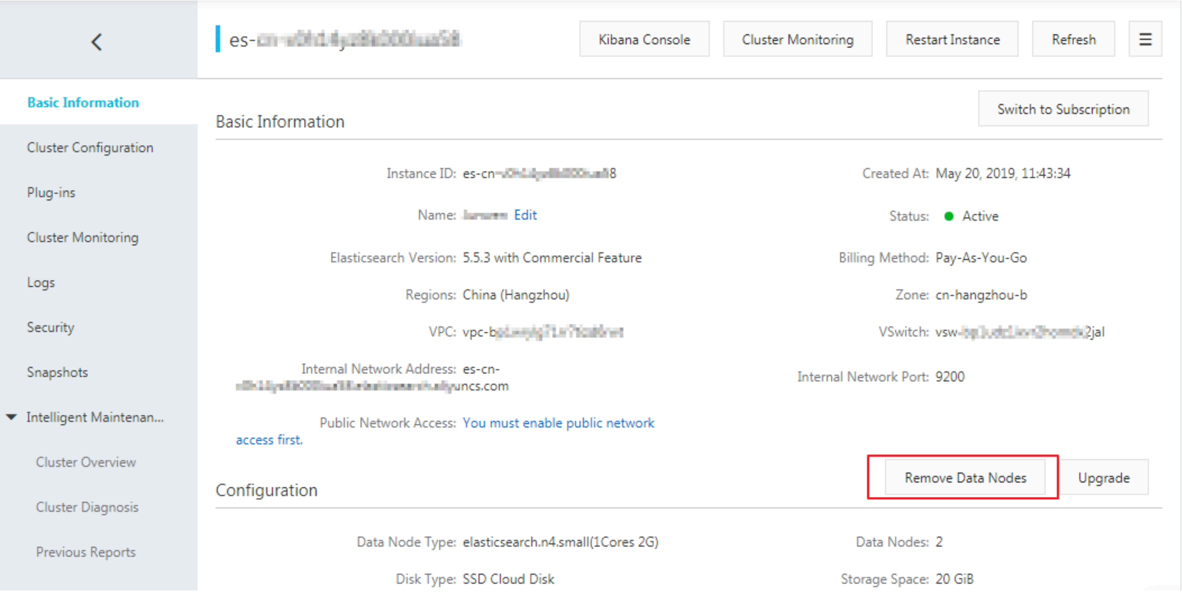
If you no longer need the plug-in, click Remove on the right side to remove the plug-in. For more information, see #unique_36/unique_36_Connect_42_section_d0y_kyx_fu0.

1.12 Downgrade data nodes

You can only downgrade data nodes in an Alibaba Cloud Elasticsearch instance that uses the Pay-As-You-Go billing method and is deployed in one zone. You cannot downgrade data nodes in an instance that uses the Subscription billing method or that is deployed across zones. Currently, Alibaba Cloud Elasicsearch only supports removing data nodes from an Alibaba Cloud Elasticsearch instance. The specification and disk capacity of dedicated master nodes, client nodes, and Kibana nodes cannot be downgraded.

Procedure

1. Log on to the Alibaba Cloud Elasticsearch console, locate the Elasticsearch instance that you need to downgrade data nodes for, and click the instance ID.
2. On the Basic Information tab page, click Downgrade Data Nodes.



Basic Information

Instance ID: es-cn- [illegible] Created At: May 20, 2019, 11:43:34

Name: [illegible] Edit Status: ● Active

Elasticsearch Version: 5.5.3 with Commercial Feature Billing Method: Pay-As-You-Go

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

VPC: vpc-b [illegible] VSwitch: vsw- [illegible] 2jal

Internal Network Address: es-cn- [illegible] uncs.com Internal Network Port: 9200

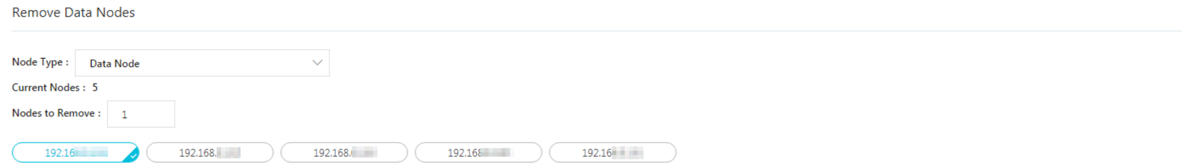
Public Network Access: You must enable public network access first.

Configuration

Data Node Type: elasticsearch.n4.small(1Cores 2G) Data Nodes: 2

Disk Type: SSD Cloud Disk Storage Space: 20 GiB

3. On the Downgrade Data Nodes page, select Data Node, and then specify the data nodes to be downgraded.


Remove Data Nodes

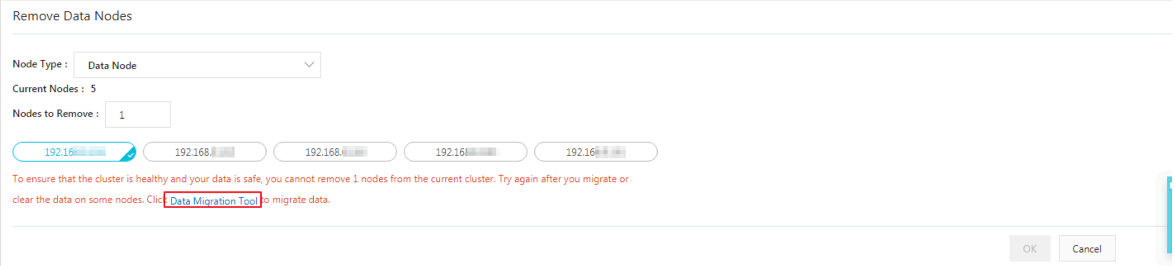
Node Type : Data Node

Current Nodes : 5

Nodes to Remove : 1

Note:

For data security, make sure that no data is stored on these data nodes. If the data nodes still contain data, click Data Migration Tool to migrate the data. After the data migration process is complete, no index data is stored on the data nodes. New index data is not written into these data nodes.


Remove Data Nodes

Node Type : Data Node

Current Nodes : 5

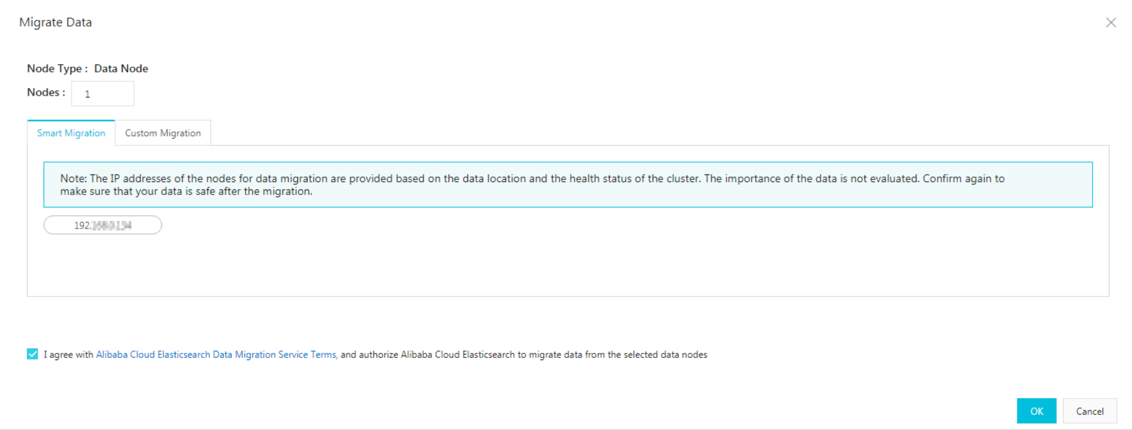
Nodes to Remove : 1

To ensure that the cluster is healthy and your data is safe, you cannot remove 1 nodes from the current cluster. Try again after you migrate or clear the data on some nodes. Click Data Migration Tool to migrate data.

You can choose the smart migration or custom migration method to migrate the data:

- Smart migration

  The system will automatically select the data nodes to be downgraded for you. You must select the check box to agree to the terms of data migration, and then click OK.



Migrate Data

Node Type : Data Node

Nodes : 1

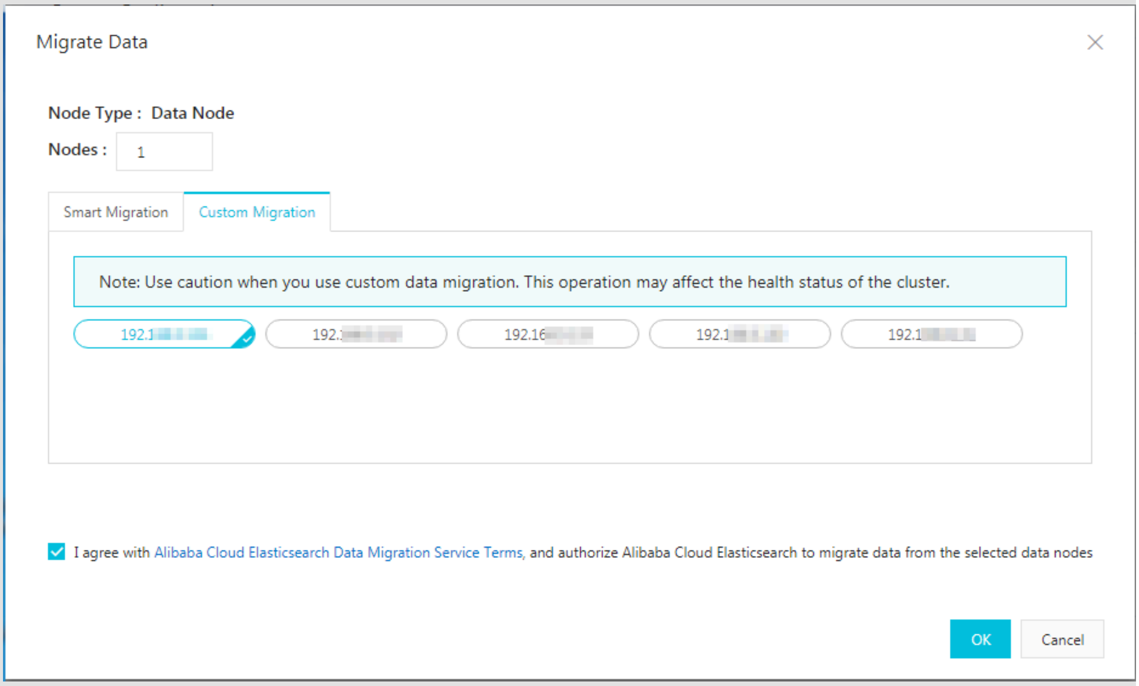
Note: The IP addresses of the nodes for data migration are provided based on the data location and the health status of the cluster. The importance of the data is not evaluated. Confirm again to make sure that your data is safe after the migration.

192.[redacted]

☑ I agree with Alibaba Cloud Elasticsearch Data Migration Service Terms, and authorize Alibaba Cloud Elasticsearch to migrate data from the selected data nodes

- Custom migration

  You need to manually specify the data nodes to be downgraded on the Custom Migration page, select the check box to agree to the terms of data migration, and click OK.



Migrate Data

Node Type : Data Node

Nodes : 1

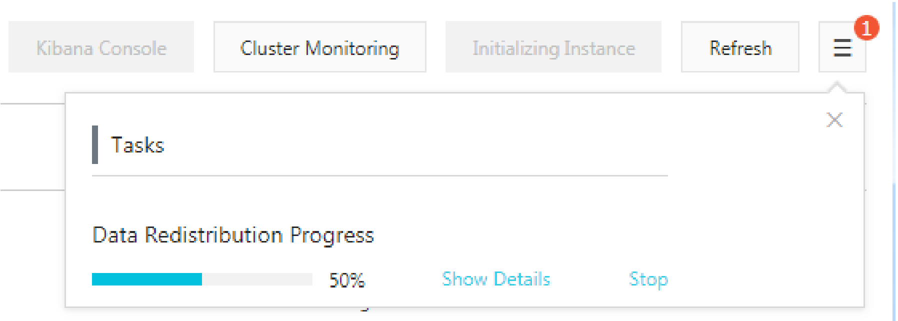
Note: Use caution when you use custom data migration. This operation may affect the health status of the cluster.

192.1[redacted] 192.[redacted] 192.16[redacted] 192.1[redacted] 192.1[redacted]

☑ I agree with Alibaba Cloud Elasticsearch Data Migration Service Terms, and authorize Alibaba Cloud Elasticsearch to migrate data from the selected data nodes

View the downgrade or data migration progress

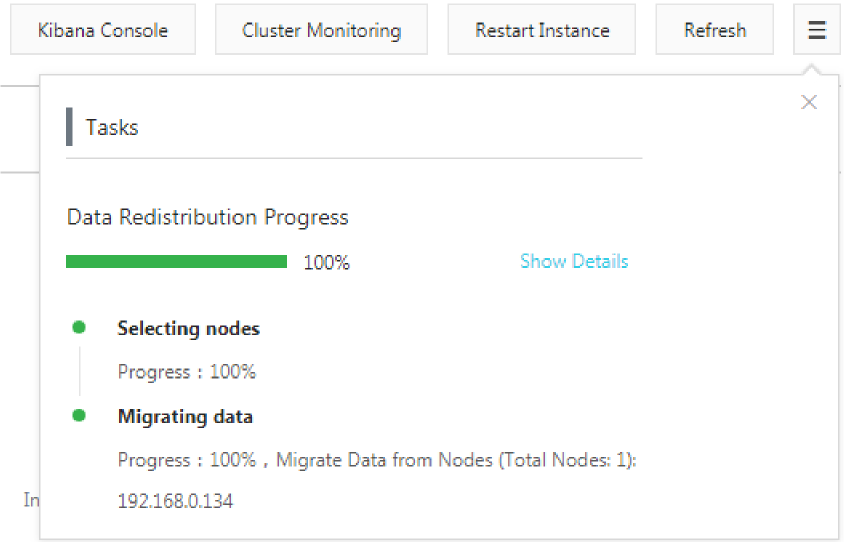
You can click the tasks list icon in the upper-right corner of the page to view the progress of the downgrade or data migration process.



Tasks

Data Redistribution Progress

50% Show Details Stop



Tasks

Data Redistribution Progress

100% Show Details

● **Selecting nodes**

Progress：100%

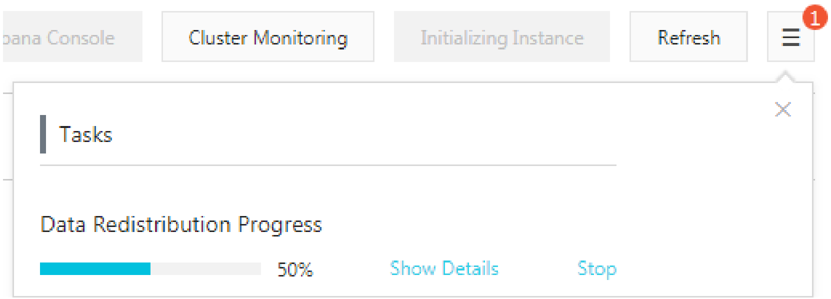
● **Migrating data**

Progress：100%，Migrate Data from Nodes (Total Nodes: 1):

192.168.0.134

Migration rollback

During the migration process, you can stop the migration task to roll back the migration.



Tasks

Data Redistribution Progress

50% Show Details Stop

Handle data migration failures

The data migration process is time-consuming. Any cluster status or data changes may result in data migration failures. You can check the Tasks list in the upper-right corner to locate the cause. You can perform the following operations when the data migration task fails or after the task is complete:

1. Query the IP addresses of the data nodes

   You can go to the tasks list or call the Elasticsearch API to query the IP addresses of the data nodes where the data is migrated:

```
//  Call   the   following   operation   to   query   the   cluster
   configurat  ion
 PUT   _cluster / settings

//  Sample   response
{
  " transient ": {
    " cluster ": {
      " routing ": {
        " allocation ": {
          " exclude ": {
            " _ip ": " 192 . 168 . ***. ***, 192 . 168 . ***. ***,
 192 . 168 . ***. ***"
          }
        }
      }
    }
  }
}
```

2. Roll back data nodes

   You can call the following operation to roll back data nodes:

```
//  To   roll   back   the   required   data   nodes ,  specify
 the   IP   addresses   of   the   data   nodes   that   you   do
 not   want   to   roll   back   in   the   API   request .
 PUT   _cluster / settings
{
  " transient ": {
    " cluster ": {
      " routing ": {
        " allocation ": {
          " exclude ": {
            " _ip ": " 192 . 168 . ***. ***, 192 . 168 . ***. ***"
          }
        }
      }
    }
  }
}

//  Roll   back   all   data   nodes
 PUT   _cluster / settings
{
  " transient ": {
    " cluster ": {
      " routing ": {
        " allocation ": {
          " exclude ": {
            " _ip ":  null
          }
        }
      }
    }
    }
 }
```

3. Verify the rollback result

   You can call the `GET _cluster / settings` operation to confirm the IP addresses of the data nodes. At the same time, you can check whether shards are reallocated to the data nodes to determine the progress of the rollback task.

   To check the status of the data migration or rollback task, call the `GET _cat / shards ? v` operation.

Error messages

Error messages and solutions

During the data migration or downgrade process, the system may prompt the following error messages:

- This operation may cause a shard distribution error or insufficient storage, CPU, or memory resources.

  Cause and solution: after the data migration or downgrade task is complete, the cluster does not have sufficient storage, memory, or CPU resources to store the system data or handle the workload. Call the `GET _cat / indices ? v` operation to check whether the number of index replicas in the cluster exceeds the number of data nodes after the cluster is scaled. You also need to check whether the storage, memory, or CPU resources are sufficient to store the existing data or handle the requests.
- The cluster is running tasks or in an error status. Try again later.

  Cause and solution: call the `GET _cluster / health` operation to check the health status of the cluster or go to the Intelligent Maintenance page to verify the cause.
- The nodes in the cluster contain data. You must migrate the data first.
- The number of nodes that you reserve must be greater than two and greater than half of the existing nodes.

  Cause and solution: to ensure the reliability of the cluster, the number of reserved nodes must be greater than 2. To ensure the stability of the cluster, the number of data nodes specified for data migration or downgrading must be no greater than half of the existing data nodes.

- The current Elasticsearch cluster configuration does not support this operation. Check the Elasticsearch cluster configuration first.

  Cause and solution: call the `GET _cluster / settings` operation to query the cluster configuration and check whether the cluster configuration contains settings that forbid data allocation.

auto_expand_replicas

Some users may use the permission management function supported by X-Pack. In former Elasticsearch versions, this function applies the `" index . auto_expan d_replicas " : " 0 - all "` setting to indexes .security and .security-6 by default. This causes data migration or downgrading failures. We recommend that you modify the auto_expand_replicas option as follows:

```
//  Query   the   index   configurat  ion
 GET  . security / _settings

//  Returned   results
{
  ". security - 6 " : {
    " settings " : {
      " index " : {
        " number_of_  shards " : " 1 ",
        " auto_expan  d_replicas " : " 0 - all ",
        " provided_n  ame " : ". security - 6 ",
        " format " : " 6 ",
        " creation_d  ate " : " 1555142250  367 ",
        " priority " : " 1000 ",
        " number_of_  replicas " : " 9 ",
        " uuid " : " 9t2hotc7S5  OpPuKEIJ ****",
        " version " : {
          " created " : " 6070099 "
        }
      }
    }
  }
}

//  Use   one   of   the   following   methods   to   modify   the
 auto_expan  d_replicas   setting
 PUT  . security / _settings
{
  " index " : {
    " auto_expan  d_replicas " : " 0 - 1 "
  }
}

 PUT  . security / _settings
{
  " index " : {
    " auto_expan  d_replicas " : " false ",
    " number_of_  replicas " :  1 ,
  }
}
```

```
// Set the number of replicas based on the actual
 needs . The number of replicas must be greater than
 1 and less than or equal to the number of the
 available data nodes .
```

2 Data visualization

2.1 Kibana

2.1.1 Log on to the Kibana console

This topic describes how to log on to the Kibana console. After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch provides you a free Kibana node with one core and 2 GB of memory. The Kibana console supports data query, data visualization, and other features.

Prerequisites

To log on to the Kibana console, you must first purchase an Elasticsearch instance. Make sure that #unique_47/unique_47_Connect_42_section_bbj_euc_ly7 is Active.

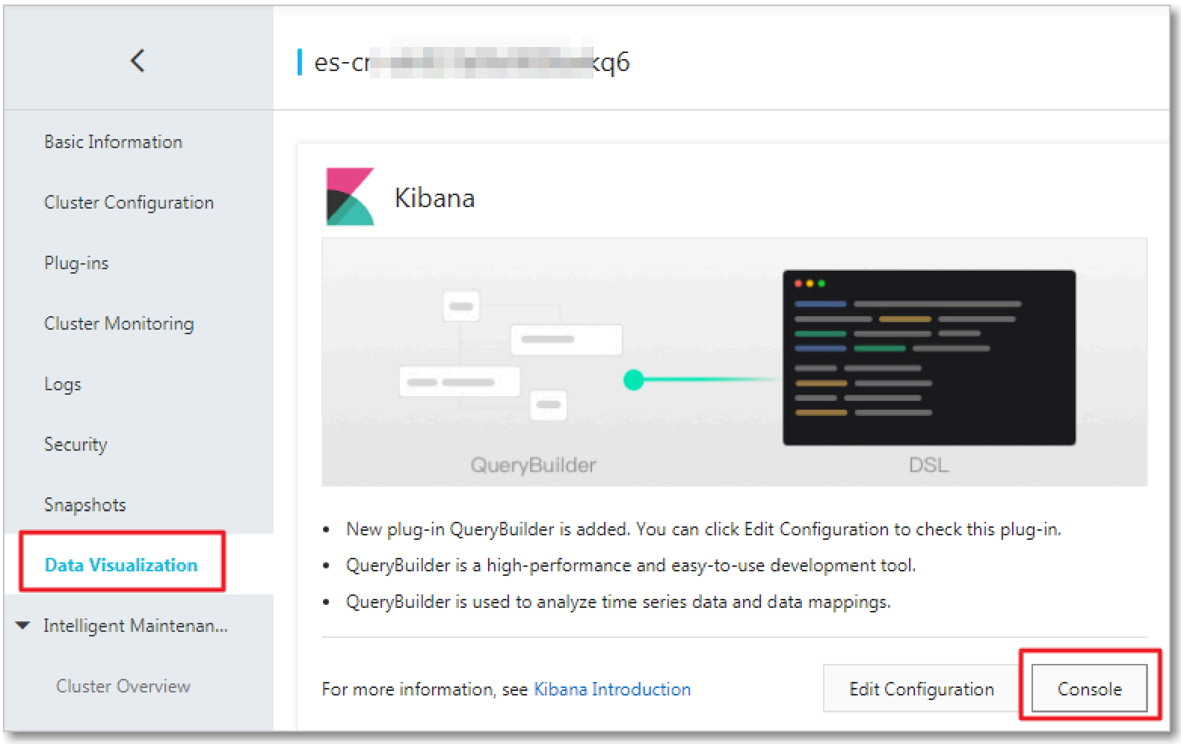
Context

Alibaba Cloud Elasticsearch provides the Kibana console for you to scale your business. The Kibana console is a part of the Elasticsearch ecosystem, which has been seamlessly integrated into Elasticsearch. The Kibana console enables you to monitor the status of your Elasticsearch instances and manage these instances.

Procedure

1. Log on to the Alibaba Cloud Elasticsearch console, and clickInstance ID/Name > Data Visualization.

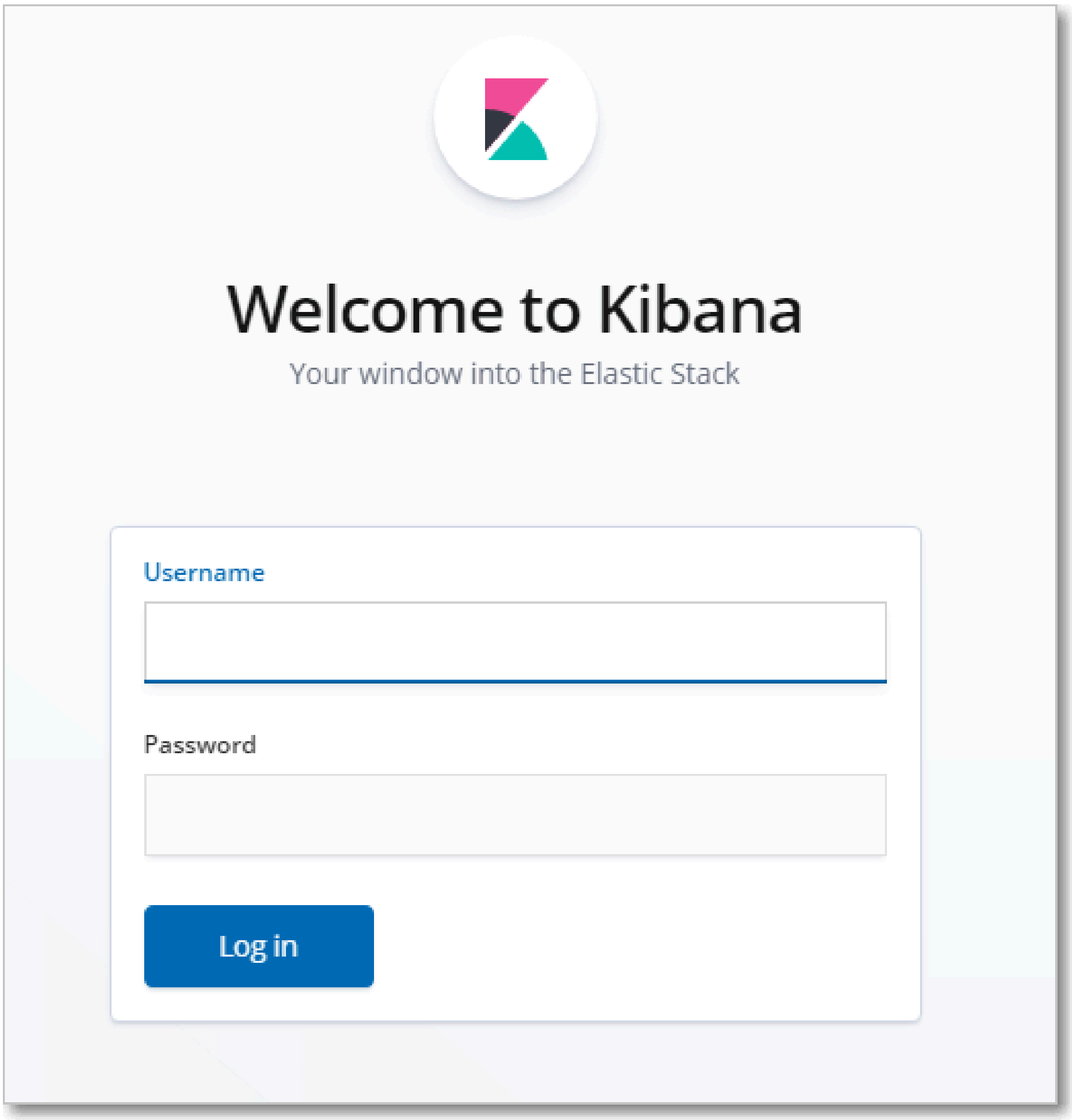
2. On the Data Visualization page, click Console under Kibana.



- New plug-in QueryBuilder is added. You can click Edit Configuration to check this plug-in.
- QueryBuilder is a high-performance and easy-to-use development tool.
- QueryBuilder is used to analyze time series data and data mappings.

For more information, see Kibana Introduction

3. Enter the username and password on the logon page, and then click LOG IN.

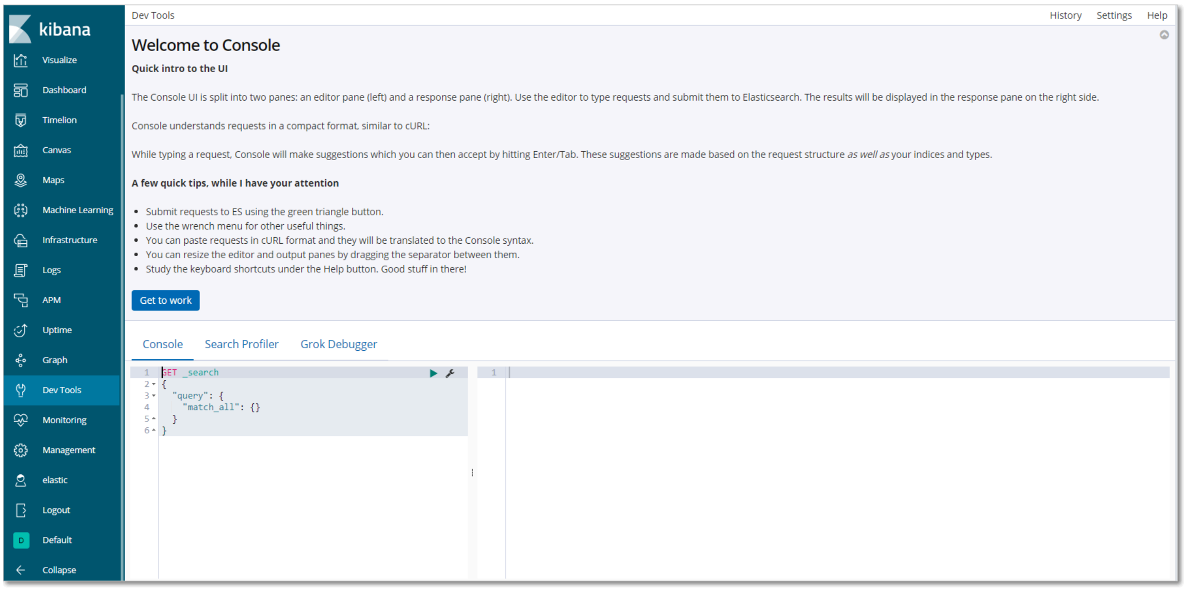


Welcome to Kibana

Your window into the Elastic Stack

- Username: the default username is elastic.
- Password: enter the password that you have set when you purchase the Elasticsearch instance.

The following figure shows the Kibana console logged on from an Alibaba Cloud Elasticsearch instance 6.7. If you use other Elasticsearch versions, the actual console may look slightly different from the one in the figure.



Welcome to Console

Quick intro to the UI

The Console UI is split into two panes: an editor pane (left) and a response pane (right). Use the editor to type requests and submit them to Elasticsearch. The results will be displayed in the response pane on the right side.

Console understands requests in a compact format, similar to cURL:

While typing a request, Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure *as well as* your indices and types.

A few quick tips, while I have your attention

- Submit requests to ES using the green triangle button.
- Use the wrench menu for other useful things.
- You can paste requests in cURL format and they will be translated to the Console syntax.
- You can resize the editor and output panes by dragging the separator between them.
- Study the keyboard shortcuts under the Help button. Good stuff in there!

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

What's next

After you log on to the Kibana console, you can then perform operations such as query data or create dashboards. For more information, see Kibana User Guide.

2.1.2 Basic configuration (6.7.0)

This topic introduces the basic configuration of the Kibana node. You can switch the language of the Kibana console in the basic configuration.

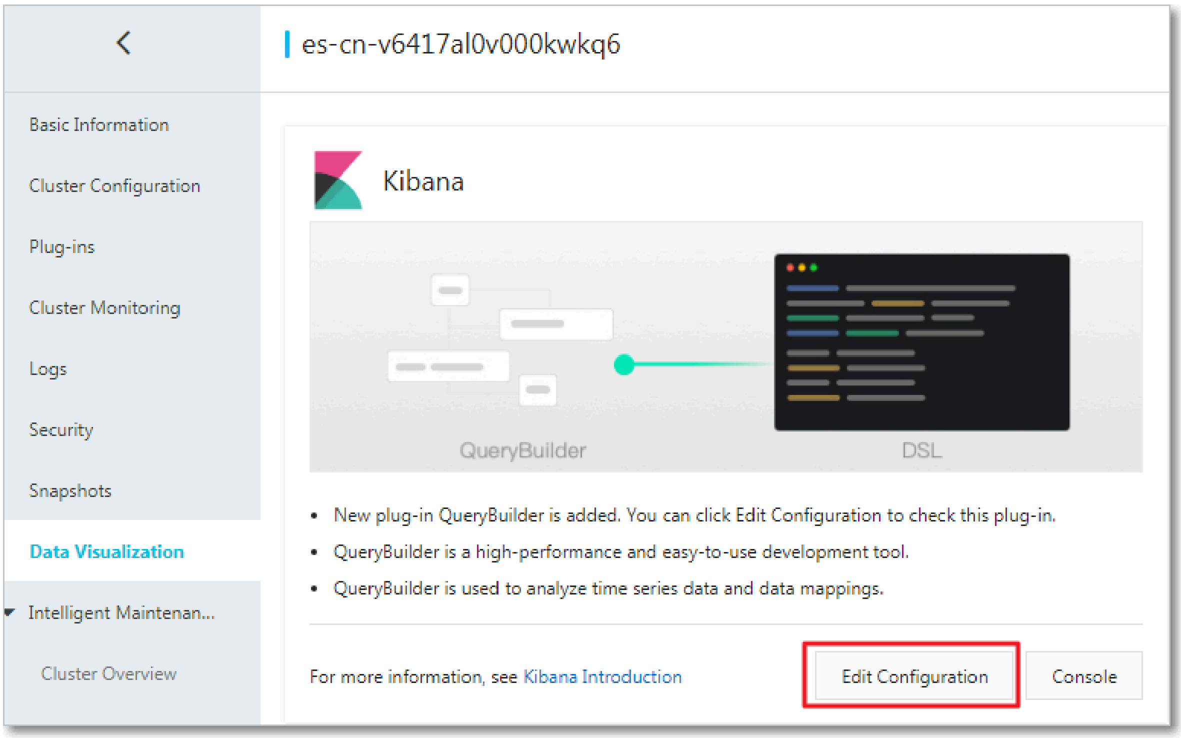
Notice:

The basic configuration of the Kibana node is only available in Alibaba Cloud Elasticsearch 6.7.0 with Commercial Feature.

Switch the language of the Kibana console

1. Log on to the Alibaba Cloud Elasticsearch console, and then clickInstance ID/Name > Data Visualization.

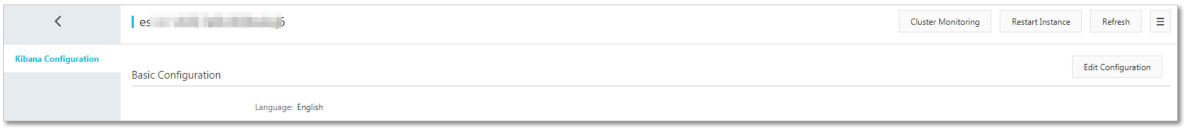
2. Click Edit Configuration under Kibana to go to the Kibana Configuration page.



- New plug-in QueryBuilder is added. You can click Edit Configuration to check this plug-in.
- QueryBuilder is a high-performance and easy-to-use development tool.
- QueryBuilder is used to analyze time series data and data mappings.

For more information, see Kibana Introduction

You can then view the Basic Configuration on the Kibana Configuration page. In the Basic Configuration area, follow these steps to switch the language of the Kibana console. By default, the language is set to English.



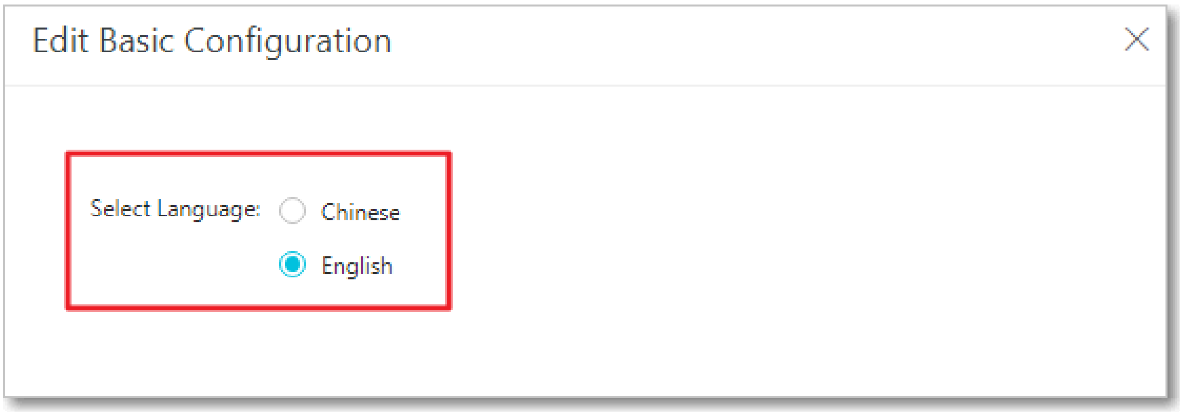
Language: English

3. Click Edit Configuration on the right side of Basic Configuration.

Notice:

The system must restart the Kibana node for the changes to take effect. Make sure that the restart process does not affect your operations on the Kibana console before you perform the following steps:

4. On the Edit Basic Configuration page, select a language from the Select Language list, and click OK.



Edit Basic Configuration

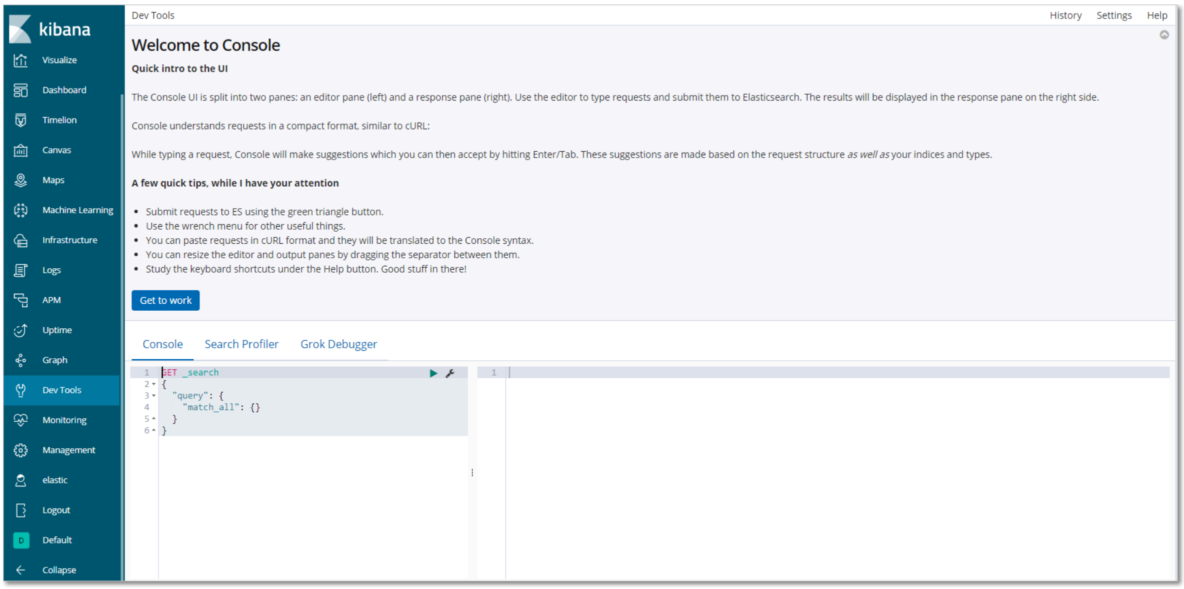
Select Language: ○ Chinese

● English

Note:

The Kibana console supports both English and Chinese. The default language is English.

After you click OK, the Kibana node will automatically restart. After the Kibana node is restarted, #unique_49 and verify that the console is switched to the selected language.



Welcome to Console

Quick intro to the UI

The Console UI is split into two panes: an editor pane (left) and a response pane (right). Use the editor to type requests and submit them to Elasticsearch. The results will be displayed in the response pane on the right side.

Console understands requests in a compact format, similar to cURL:

While typing a request, Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure *as well as* your indices and types.

A few quick tips, while I have your attention

- Submit requests to ES using the green triangle button.
- Use the wrench menu for other useful things.
- You can paste requests in cURL format and they will be translated to the Console syntax.
- You can resize the editor and output panes by dragging the separator between them.
- Study the keyboard shortcuts under the Help button. Good stuff in there!

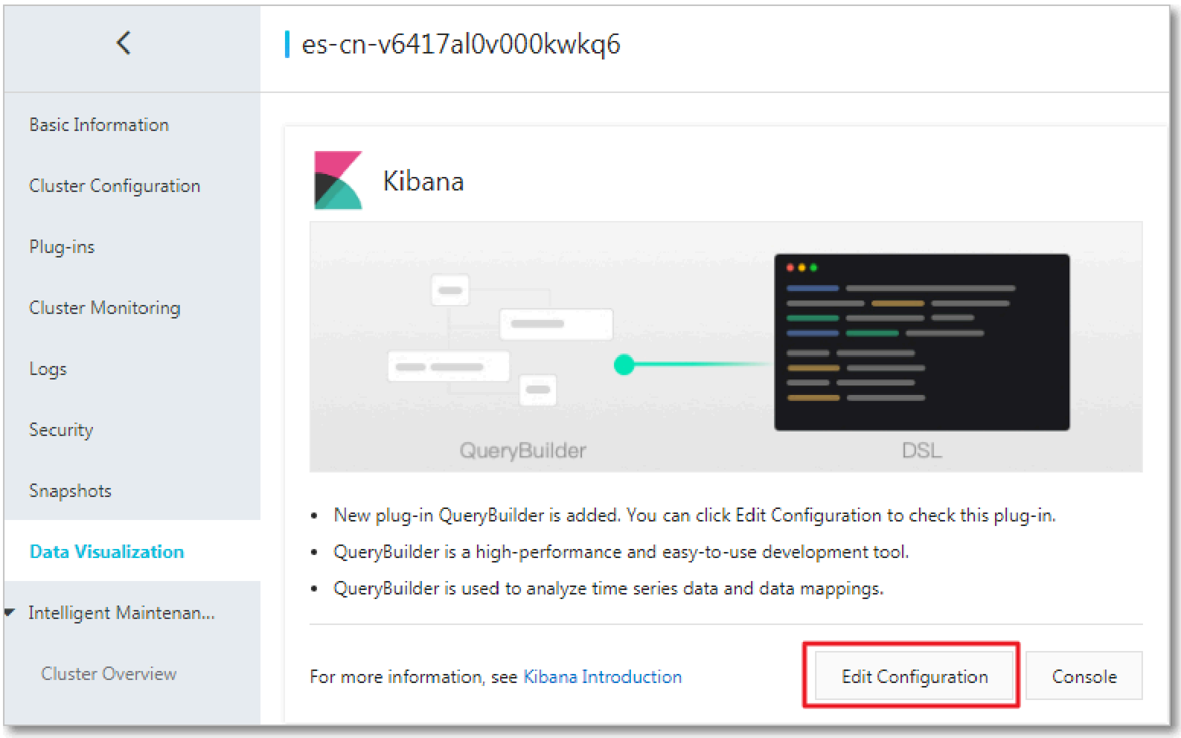
```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

2.1.3 Network access configuration

This topic describes the network access configuration of Kibana clusters. The network access configuration includes the public network access configuration and Kibana whitelist.

Go to the network access configuration page

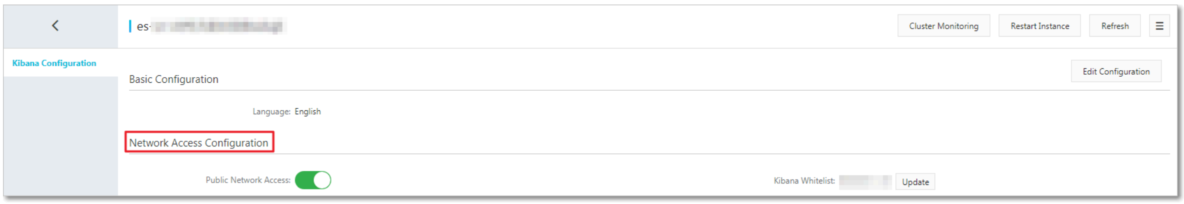
1. Log on to the Alibaba Cloud Elasticsearch console, and click Instance ID/Name > Data Visualization.
2. Click Edit Configuration under Kibana to go to the Kibana Configuration page.



- New plug-in QueryBuilder is added. You can click Edit Configuration to check this plug-in.
- QueryBuilder is a high-performance and easy-to-use development tool.
- QueryBuilder is used to analyze time series data and data mappings.

For more information, see Kibana Introduction

You can then view the Network Access Configuration on the Kibana Configuration page. In the Network Access Configuration area, you can enable or disable Public network access, and configure the Kibana whitelist. By default, the public network access feature is enabled.



Language: English

Public Network Access:

Kibana Whitelist: [redacted]

Public network access

By default, the Public Network Access switch is toggled on (green). You can click the Public Network Access switch to disable this feature. When this feature is disabled, the switch is gray. When the Public Network Access feature is disabled, you cannot log on to the Kibana console through the Internet.

Kibana whitelist

To configure the Kibana whitelist, click Update next to the Kibana whitelist, enter IP addresses into the dialog box, and click OK.

> Note:
> By default, all public network addresses are allowed to access the Kibana console.

The Kibana console supports both IP addresses and CIDR blocks. Enter IP addresses and CIDR blocks in the format of `192 . 168 . 0 . 1` and `192 . 168 . 0 . 0 / 24`, respectively. Separate these IP addresses and CIDR blocks with commas (,). You can enter `127 . 0 . 0 . 1` to forbid all IPv4 addresses or enter `0 . 0 . 0 . 0 / 0` to allow all IPv4 addresses.

If your Kibana node is deployed in the China (Hangzhou) region, then you can add IPv6 addresses to the Kibana whitelist. Enter IPv6 addresses and CIDR blocks in the format of `2401 : b180 : 1000 : 24 :: 5` and `2401 : b180 : 1000 ::/ 48`, respectively. Enter `:: 1` to forbid all IPv6 addresses and enter `::/ 0` to allow all IPv6 addresses.

2.1.4 Plug-in configuration

Alibaba Cloud Kibana provides multiple plug-ins based on open-source community plug-ins. This topic introduces Alibaba Cloud Kibana plug-ins and describes how to install and remove these plug-ins.

Plug-ins

BSearch-QueryBuilder

BSearch-QueryBuilder is an advanced query plug-in, as well as a UI component.

- Easy to learn: the BSearch-QueryBuilder plug-in is a UI component, allowing you to create Elasticsearch DSL queries in a visualized manner. You can customize search conditions without coding. This saves the costs on learning complex DSL statements. It also helps developers write and verify DSL statements.
- Easy to use: all queries that you have defined are saved in Kibana, which are ready for use at anytime.

- Compact: BSearch-QueryBuilder only consumes about 14 MB of disk space. BSearch-QueryBuilder does not stay resident in the memory. This means that it will not adversely affect the performance of Kibana and Elasticsearch.
- Secure and reliable: BSearch-QueryBuilder does not rewrite, store, or forward any user data. The source code of BSearch-QueryBuilder has been verified by Alibaba Cloud security auditing.

Note:

BSearch-QueryBuilder currently only supports Alibaba Cloud Elasticsearch instances V6.3 and V6.7. Version 5.5.3 is not supported.

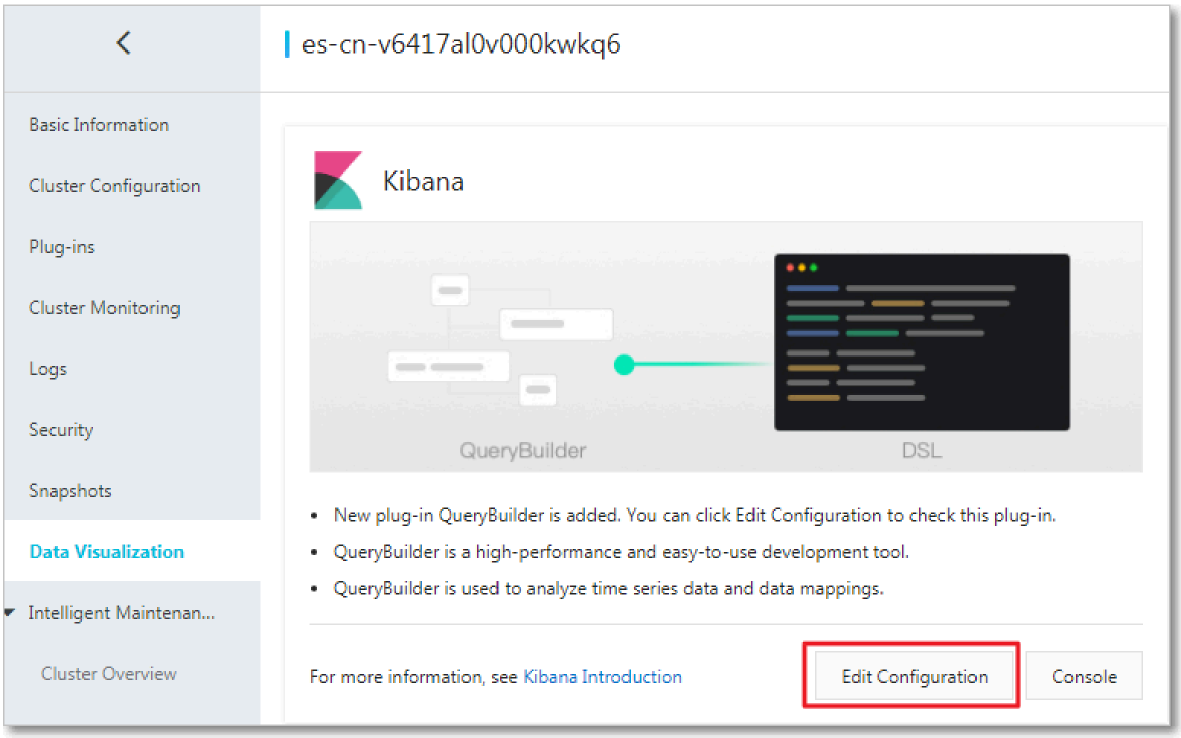
Install a plug-in

Notice:

After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch offers you a free Kibana node with one core and 2 GB of memory. A plug-in consumes resources. Before you install a plug-in, you must upgrade the Kibana node to 2-core, 4 GB or higher. For more information, see #unique_53.

1. Log on to the Alibaba Cloud Elasticsearch console, and purchase an Elasticsearch instance.
2. ClickInstance ID/Name > Data Visualization.

3. Click Edit Configuration under Kibana.



- New plug-in QueryBuilder is added. You can click Edit Configuration to check this plug-in.
- QueryBuilder is a high-performance and easy-to-use development tool.
- QueryBuilder is used to analyze time series data and data mappings.

For more information, see Kibana Introduction

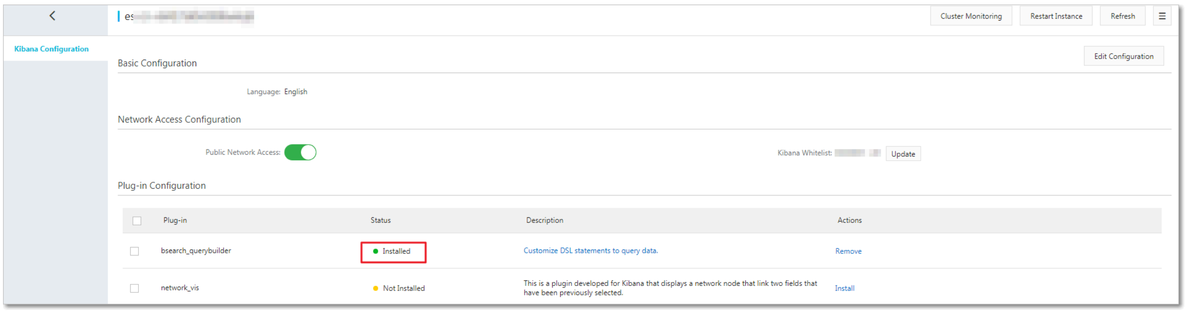
4. On the Kibana Configuration page, click Install in the Actions column in the Plug-in Configuration list.

Notice:

- After you confirm the install operation, the system will restart the Kibana node. During the restart process, Kibana cannot provide services normally. Therefore, before you confirm the operation, make sure that the restart process does not affect your operations on the Kibana console.
- If the specification of your Kibana node is lower than 2-core, 4 GB, the system prompts a notification requiring you to upgrade the instance. Follow the instructions to upgrade the Kibana node to 2-core, 4 GB or higher.

5. Confirm the operation and restart the Kibana node.

   After the Kibana node is restarted, the installation process is then completed. The plug-in will be in the Installed state.



Basic Configuration

Language: English

Network Access Configuration

Public Network Access: ●

Kibana Whitelist: [redacted]

Plug-in Configuration

□	Plug-in	Status	Description	Actions
□	bsearch_querybuilder	● Installed	Customize DSL statements to query data.	Remove
□	network_vis	● Not Installed	This is a plugin developed for Kibana that displays a network node that link two fields that have been previously selected.	Install

Note:

The installation process may be time-consuming.

Remove a plug-in

1. Follow the steps in Install a plug-in to go to the Kibana Configuration page, and then click Remove in the Actions column in the Plug-in Configuration list.

   Notice:

   After you confirm the remove operation, the system will restart the Kibana node. During the restart process, Kibana cannot provide services normally. Therefore, before you confirm the operation, make sure that the restart process does not affect your operations on the Kibana console.

2. Confirm the operation and restart the Kibana node.

   After the Kibana node is restarted, the remove process is then completed. The plug-in will be in the Not Installed state.

2.1.5 Use BSearch-QueryBuilder

BSearch-QueryBuilder is an advanced query plug-in, as well as a UI component. With the BSearch-QueryBuilder plug-in, you no longer need to write complex DSL statements for data query. It allows you to create complex queries in a visualized manner. This document describes how to use the BSearch-QueryBuilder plug-in to create a query.

Features

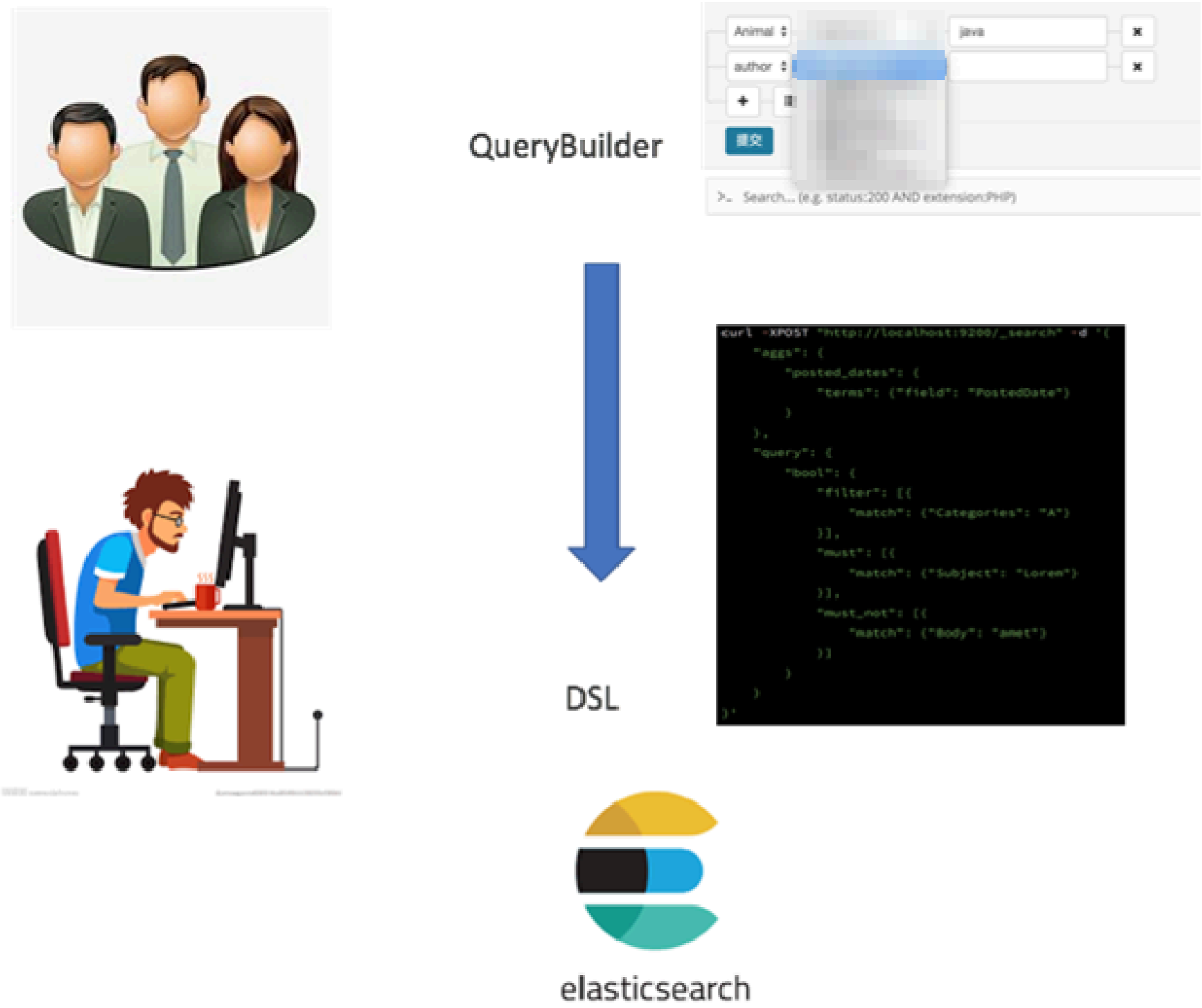
BSearch-QueryBuilder has the following features:

- Easy to learn: the BSearch-QueryBuilder plug-in is a UI component, allowing you to create Elasticsearch DSL queries in a visualized manner. You can customize search conditions without coding. This saves the costs of learning complex DSL statements. It also helps developers write and verify DSL statements.
- Easy to use: all queries that you have defined are saved in Kibana, which are ready for use at anytime.
- Compact: BSearch-QueryBuilder only consumes about 14 MB of disk space. BSearch-QueryBuilder does not stay resident in the memory. This means that it will not adversely affect the performance of Kibana and Elasticsearch.
- Secure and reliable: BSearch-QueryBuilder does not rewrite, store, or forward any user data. The source code of BSearch-QueryBuilder has been verified by Alibaba Cloud security auditing.

Background

QueryDSL is an open-source Java framework used to define SQL type-safe queries . It allows you to use API operations to send queries instead of writing statements . Currently, QueryDSL supports JPA, JDO, SQL, Java Collections, RDF, Lucene, and Hibernate Search.

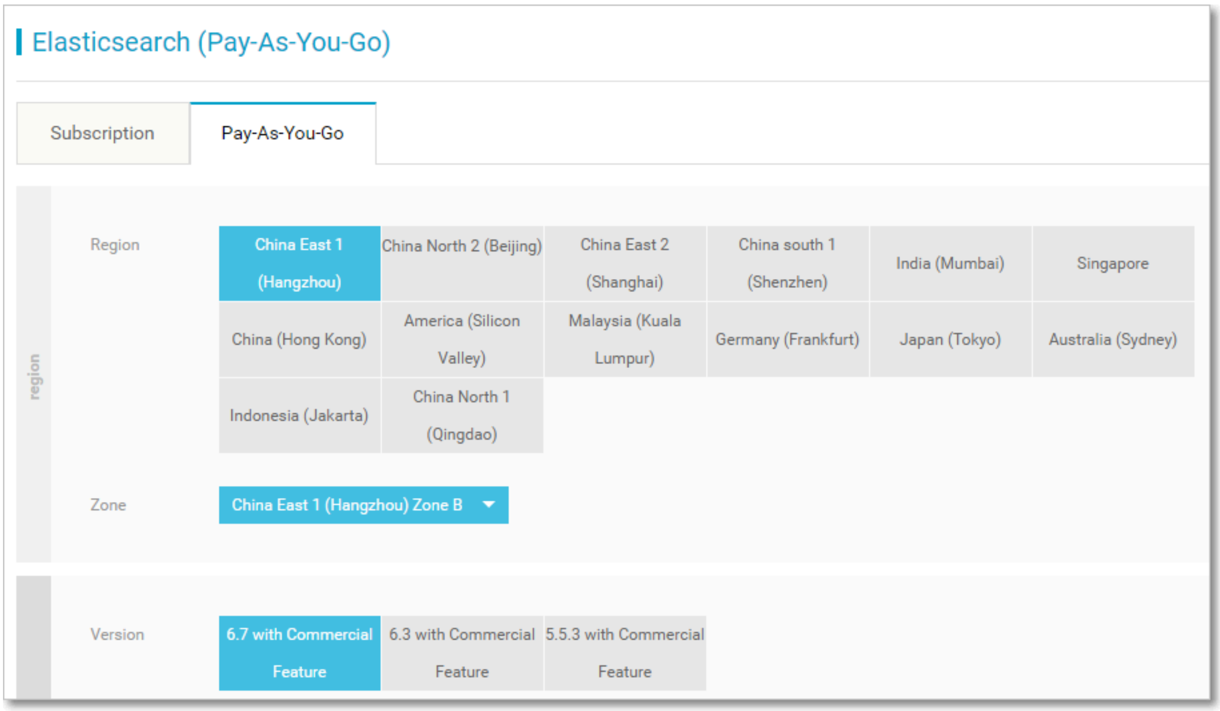
Elasticsearch provides a complete JSON query DSL for you to define queries. QueryDSL provides various query expressions. Some queries can wrap other queries, such as the boolean queries. Some queries can wrap filters, such as the constant score queries. Some queries can wrap other queries and filters at the same time, such as the filtered queries. You can use any query expressions and filters supported by Elasticsearch to create complex queries and filter the returned result. DSL is only mastered by a few programmers. You may make mistakes when writing DSL statements. QueryBuilder can help users that do not have much knowledge in Elasticsearch DSL or those that want to create DSL queries efficiently.



```
curl -XPOST "http://localhost:9200/_search" -d '{
    "aggs": {
        "posted_dates": {
            "terms": {"field": "PostedDate"}
        }
    },
    "query": {
        "bool": {
            "filter": [{
                "match": {"Categories": "A"}
            }],
            "must": [{
                "match": {"Subject": "Lorem"}
            }],
            "must_not": [{
                "match": {"Body": "amet"}
            }]
        }
    }
}'
```

Preparations

To use the BSearch-QueryBuilder plug-in, you must first purchase an Elasticsearch instance. The version of the instance must be 6.3 or 6.7. Version 5.5.3 is not supported.



Elasticsearch (Pay-As-You-Go)

Subscription | Pay-As-You-Go

region						
Region	China East 1 (Hangzhou)	China North 2 (Beijing)	China East 2 (Shanghai)	China south 1 (Shenzhen)	India (Mumbai)	Singapore
	China (Hong Kong)	America (Silicon Valley)	Malaysia (Kuala Lumpur)	Germany (Frankfurt)	Japan (Tokyo)	Australia (Sydney)
	Indonesia (Jakarta)	China North 1 (Qingdao)				
Zone	China East 1 (Hangzhou) Zone B					
Version	6.7 with Commercial Feature	6.3 with Commercial Feature	5.5.3 with Commercial Feature			

Note:

You can also use an existing instance. If the instance version does not meet the requirements, upgrade the instance.

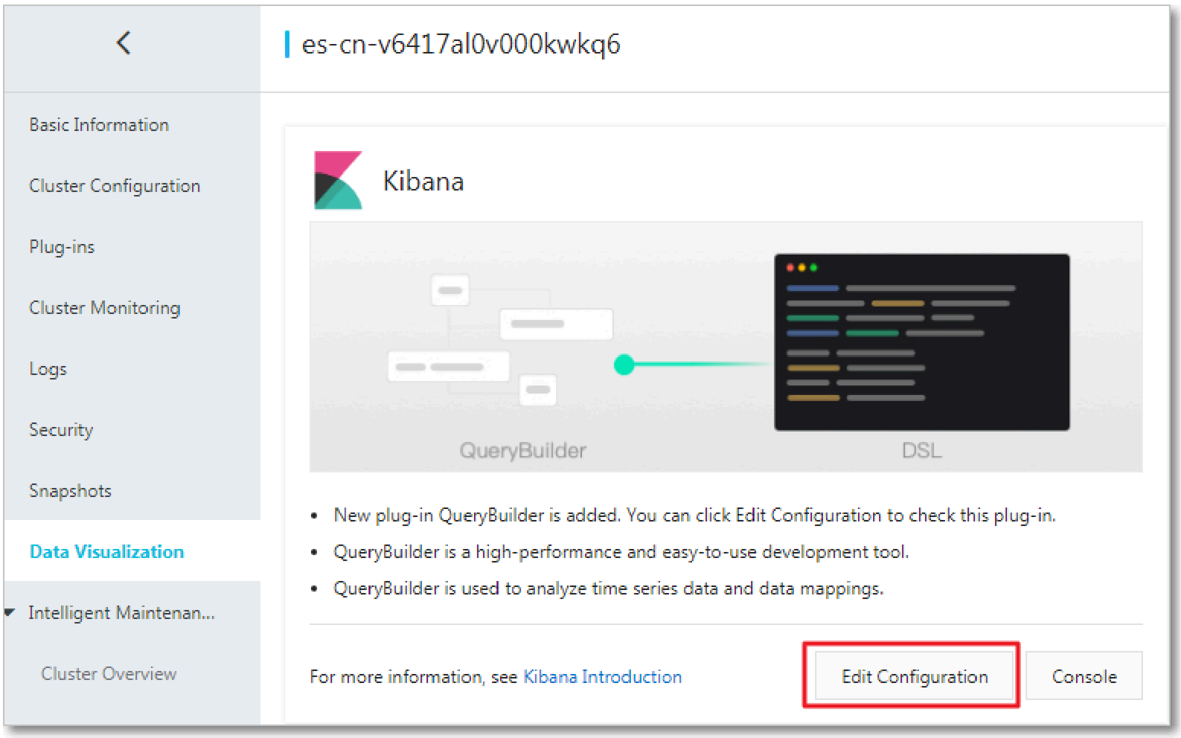
Install the BSearch-QueryBuilder plug-in

Notice:

Before you install the BSearch-QueryBuilder plug-in, make sure that the specification of your Kibana node is 2-core, 4 GB or higher. Otherwise, #unique_53.

1. Log on to the Alibaba Cloud Elasticsearch console.
2. Click the name of the Elasticsearch instance, and then click Data Visualization in the left-side navigation pane.

3. On the Data Visualization page, click Edit Configuration under Kibana.



- New plug-in QueryBuilder is added. You can click Edit Configuration to check this plug-in.
- QueryBuilder is a high-performance and easy-to-use development tool.
- QueryBuilder is used to analyze time series data and data mappings.

For more information, see Kibana Introduction

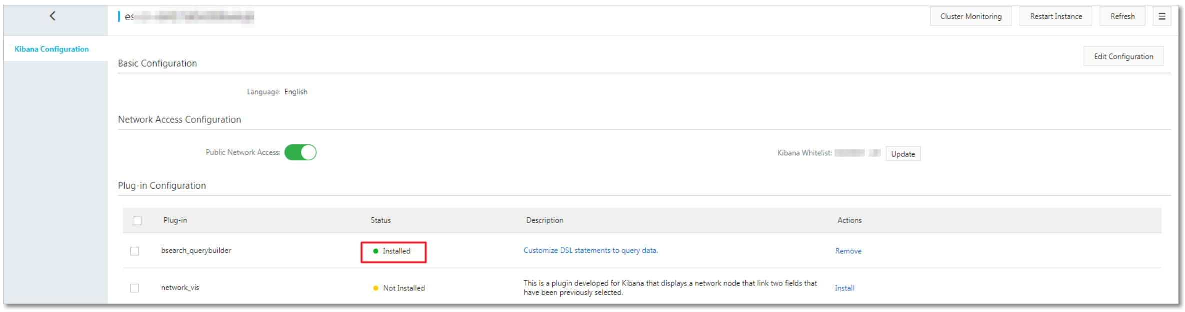
4. On the Kibana Configuration page, click Install on the right side of Bsearch_querybuilder in the Plug-in Configuration list.

Notice:

After you confirm the install operation, the system will restart the Kibana node. Therefore, before you confirm the operation, you must make sure that the restart process does not affect your operations on the Kibana console.

5. Confirm the operation and restart the Kibana node.

After the Kibana node is restarted, the installation process is then completed. The plug-in will be in the Installed state.



Basic Configuration

Language: English

Network Access Configuration

Public Network Access: ●

Kibana Whitelist: [redacted]

Plug-in Configuration

□	Plug-in	Status	Description	Actions
□	bsearch_querybuilder	● Installed	Customize DSL statements to query data.	Remove
□	network_vis	● Not Installed	This is a plugin developed for Kibana that displays a network node that link two fields that have been previously selected.	Install

Note:

The installation process may be time-consuming.

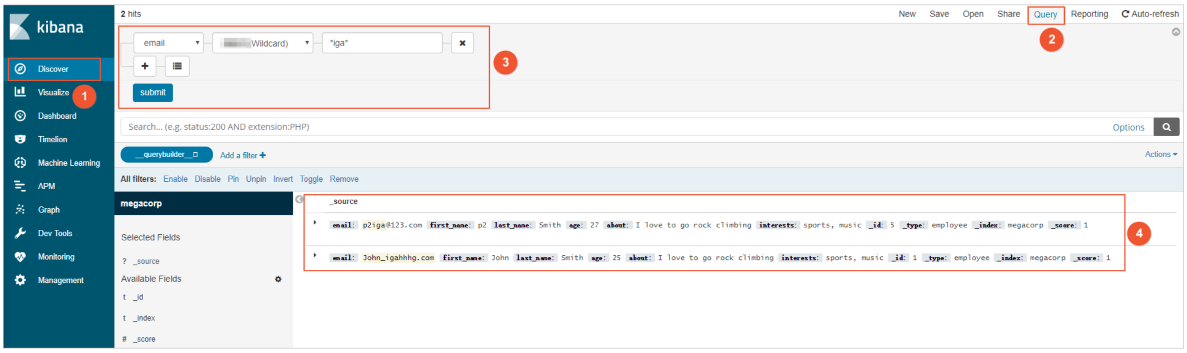
Use the BSearch-QueryBuilder plug-in

1. Go back to the Data Visualization page, click Console under Kibana.
2. Enter the username and password, and then click LOG IN to log on to the Kibana console.

   The default username is elastic. Enter the password that you have set when purchasing the Elasticsearch instance.
3. In the Kibana console, select Discover > Query.

   > **Notice:**
   > Before querying, make sure that you have created an index pattern. To create an index pattern, in the Kibana console, click Management, find the Kibanaarea, and click Index Patterns > Create index pattern.
4. In the query area, select a search condition and filter, and click Submit.

   After you submit the query, the system shows the query result.



email ▾ Wildcard) ▾ *iga*

Search... (e.g. status:200 AND extension:PHP)

```
_source
email: p2iga@123.com first_name: p2 last_name: Smith age: 27 about: I love to go rock climbing interests: sports, music _id: 5 _type: employee _index: megacorp _score: 1
email: John_igahhhg.com first_name: John last_name: Smith age: 25 about: I love to go rock climbing interests: sports, music _id: 1 _type: employee _index: megacorp _score: 1
```

In the query area, click the ✚ icon to add a search condition, click the ☰ icon to add a filter for the condition, or click the ✖ icon to delete a search condition or filter.

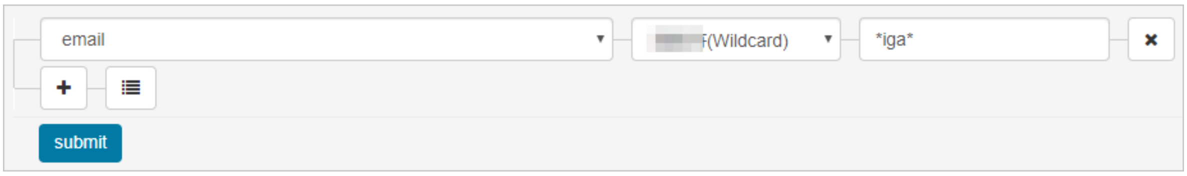
For more information, see Examples.

Examples

The BSearch-QueryBuilder plug-in allows you to create a variety of queries, such as regexp queries, boolean queries, and range queries.

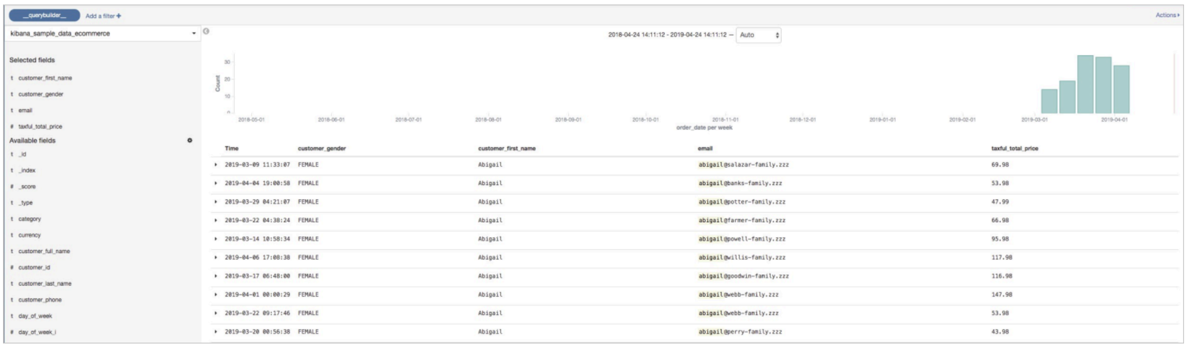
- Regexp queries

  As shown in the following figure, the email condition is added for fuzzy match. The email condition matches all email addresses that contain the iga keyword.



email ▾ [redacted](Wildcard) ▾ *iga*

  The following figure shows the returned result:



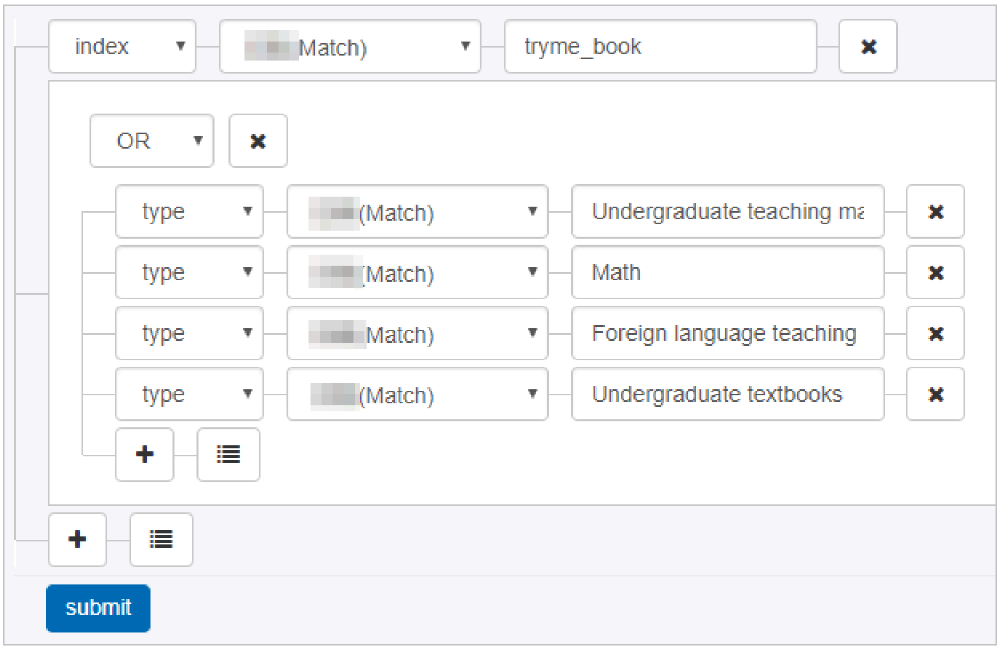
kibana_sample_data_ecommerce

2018-04-24 14:11:12 - 2019-04-24 14:11:12 — Auto

Time	customer_gender	customer_first_name	email	taxful_total_price
▸ 2019-03-09 11:33:07	FEMALE	Abigail	abigail@salazar-family.zzz	69.98
▸ 2019-04-04 19:00:58	FEMALE	Abigail	abigail@banks-family.zzz	53.98
▸ 2019-03-29 04:21:07	FEMALE	Abigail	abigail@potter-family.zzz	47.99
▸ 2019-03-22 04:38:24	FEMALE	Abigail	abigail@farmer-family.zzz	66.98
▸ 2019-03-14 10:58:34	FEMALE	Abigail	abigail@powell-family.zzz	95.98
▸ 2019-04-06 17:08:38	FEMALE	Abigail	abigail@willis-family.zzz	117.98
▸ 2019-03-17 06:48:00	FEMALE	Abigail	abigail@goodwin-family.zzz	116.98
▸ 2019-04-01 00:00:29	FEMALE	Abigail	abigail@webb-family.zzz	147.98
▸ 2019-03-22 09:17:46	FEMALE	Abigail	abigail@webb-family.zzz	53.98
▸ 2019-03-20 00:56:38	FEMALE	Abigail	abigail@perry-family.zzz	43.98

- Boolean queries

  As shown in the following figure, the index condition is set to tryme_book. An OR condition containing multiple filters is also added to filter data by type. These type filters are set to Undergraduate teaching materials, Math, Foreign language teaching, and Undergraduate textbooks.



index Match) tryme_book

OR

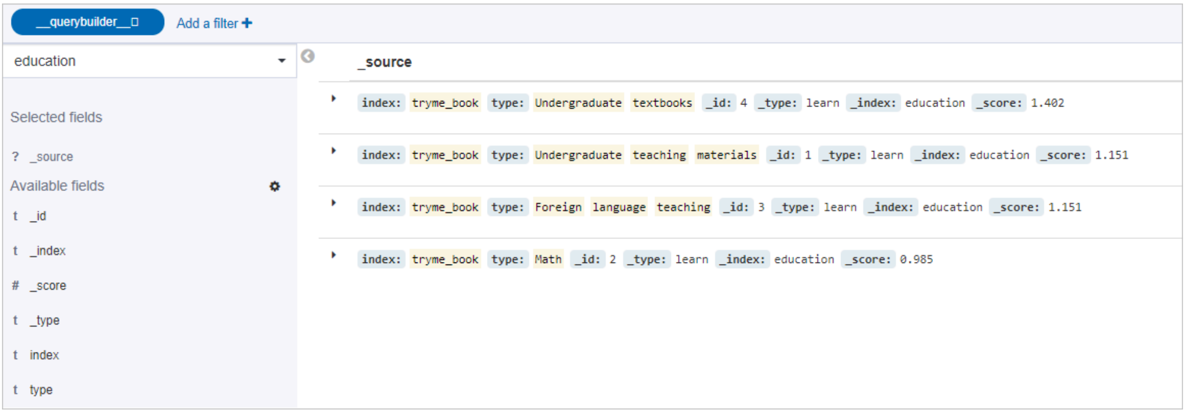
type (Match) Undergraduate teaching ma

type Match) Math

type Match) Foreign language teaching

type (Match) Undergraduate textbooks

The following figure shows the returned result.



education

Selected fields

? _source

Available fields

t _id

t _index

_score

t _type

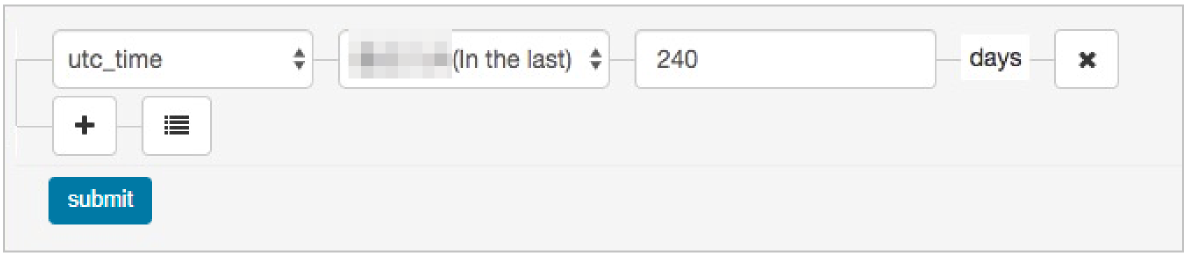
t index

t type

```
_source
index: tryme_book type: Undergraduate textbooks _id: 4 _type: learn _index: education _score: 1.402
index: tryme_book type: Undergraduate teaching materials _id: 1 _type: learn _index: education _score: 1.151
index: tryme_book type: Foreign language teaching _id: 3 _type: learn _index: education _score: 1.151
index: tryme_book type: Math _id: 2 _type: learn _index: education _score: 0.985
```

- Range queries

  Range queries allow you to search data by date. As shown in the following figure, the range condition is used to filter data based on the utc_time field. Only data entries created `in the last 240 days` are returned.



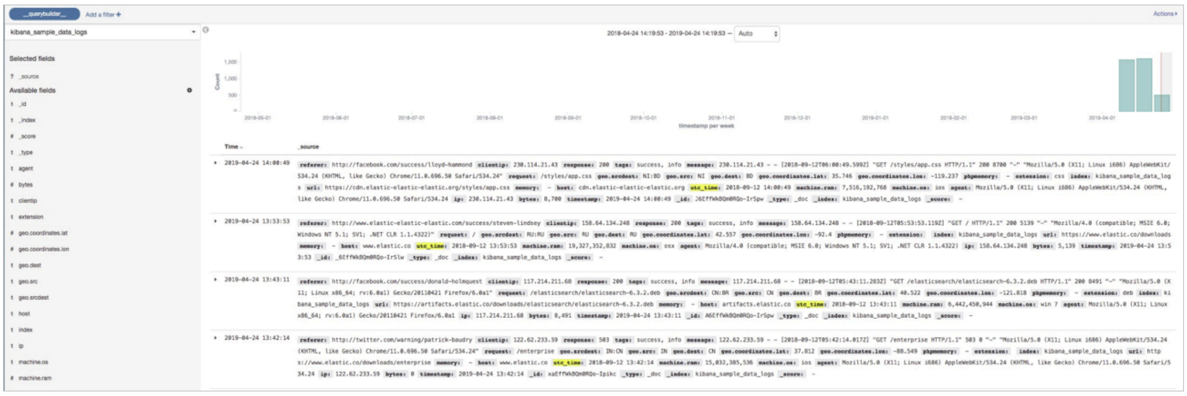
utc_time

(In the last)

240

days

  The following figure shows the returned result.



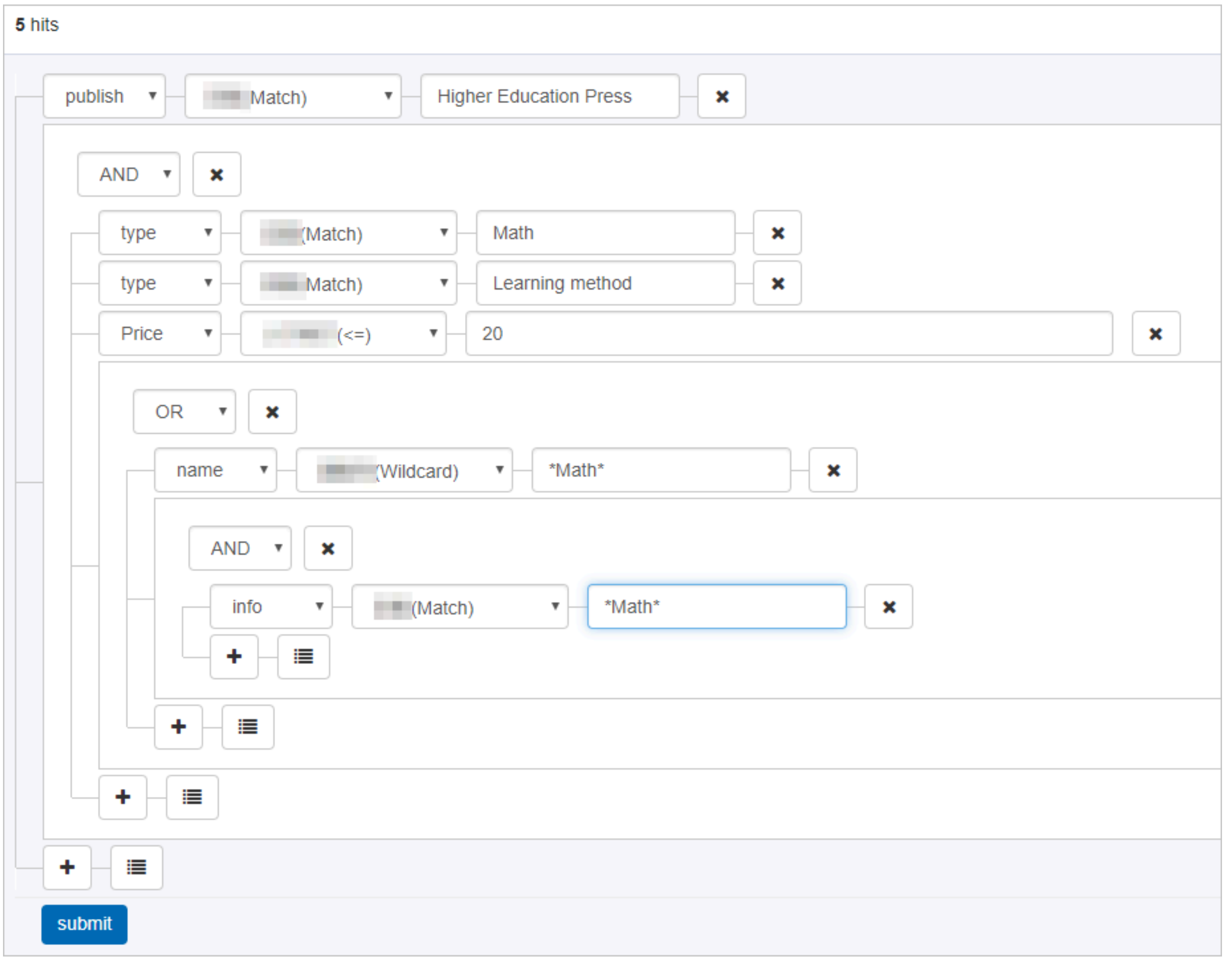
```
▸ 2019-04-24 14:00:49   referer: http://facebook.com/success/lloyd-hammond clientip: 230.114.21.43 response: 200 tags: success, info message: 230.114.21.43 - - [2018-09-12T06:00:49.599Z] "GET /styles/app.css HTTP/1.1" 200 8700 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/
                        534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24" request: /styles/app.css geo.srcdest: NI:BD geo.src: NI geo.dest: BD geo.coordinates.lat: 35.746 geo.coordinates.lon: -119.237 phpmemory: - extension: css index: kibana_sample_data_log
                        s url: https://cdn.elastic-elastic-elastic.org/styles/app.css memory: - host: cdn.elastic-elastic-elastic.org utc_time: 2018-09-12 14:00:49 machine.ram: 7,516,192,768 machine.os: ios agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML,
                        like Gecko) Chrome/11.0.696.50 Safari/534.24 ip: 230.114.21.43 bytes: 8,700 timestamp: 2019-04-24 14:00:49 _id: J6EffWkBQm0RQo-IrSpw _type: _doc _index: kibana_sample_data_logs _score: -

▸ 2019-04-24 13:53:53   referer: http://www.elastic-elastic-elastic.com/success/steven-lindsey clientip: 158.64.134.248 response: 200 tags: success, info message: 158.64.134.248 - - [2018-09-12T05:53:53.119Z] "GET / HTTP/1.1" 200 5139 "-" "Mozilla/4.0 (compatible; MSIE 6.0;
                        Windows NT 5.1; SV1; .NET CLR 1.1.4322)" request: / geo.srcdest: RU:RU geo.src: RU geo.dest: RU geo.coordinates.lat: 42.557 geo.coordinates.lon: -92.4 phpmemory: - extension:  index: kibana_sample_data_logs url: https://www.elastic.co/downloads
                        memory: - host: www.elastic.co utc_time: 2018-09-12 13:53:53 machine.ram: 19,327,352,832 machine.os: osx agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) ip: 158.64.134.248 bytes: 5,139 timestamp: 2019-04-24 13:5
                        3:53 _id: _6EffWkBQm0RQo-IrSlw _type: _doc _index: kibana_sample_data_logs _score: -

▸ 2019-04-24 13:43:11   referer: http://facebook.com/success/donald-holmquest clientip: 117.214.211.68 response: 200 tags: success, info message: 117.214.211.68 - - [2018-09-12T05:43:11.283Z] "GET /elasticsearch/elasticsearch-6.3.2.deb HTTP/1.1" 200 8491 "-" "Mozilla/5.0 (X
                        11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1" request: /elasticsearch/elasticsearch-6.3.2.deb geo.srcdest: CN:BR geo.src: CN geo.dest: BR geo.coordinates.lat: 40.522 geo.coordinates.lon: -121.818 phpmemory: - extension: deb index: ki
                        bana_sample_data_logs url: https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.3.2.deb memory: - host: artifacts.elastic.co utc_time: 2018-09-12 13:43:11 machine.ram: 6,442,450,944 machine.os: win 7 agent: Mozilla/5.0 (X11; Linux
                        x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 ip: 117.214.211.68 bytes: 8,491 timestamp: 2019-04-24 13:43:11 _id: A6EffWkBQm0RQo-IrSpw _type: _doc _index: kibana_sample_data_logs _score: -

▸ 2019-04-24 13:42:14   referer: http://twitter.com/warning/patrick-baudry clientip: 122.62.233.59 response: 503 tags: success, info message: 122.62.233.59 - - [2018-09-12T05:42:14.017Z] "GET /enterprise HTTP/1.1" 503 0 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24
                        (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24" request: /enterprise geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coordinates.lat: 37.812 geo.coordinates.lon: -88.549 phpmemory: - extension:  index: kibana_sample_data_logs url: http
                        s://www.elastic.co/downloads/enterprise memory: - host: www.elastic.co utc_time: 2018-09-12 13:42:14 machine.ram: 15,032,385,536 machine.os: ios agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/5
                        34.24 ip: 122.62.233.59 bytes: 0 timestamp: 2019-04-24 13:42:14 _id: xaEffWkBQm0RQo-Ipikc _type: _doc _index: kibana_sample_data_logs _score: -
```

With all these search conditions and filters, you can define a complex query as follows:



5 hits

publish ▾ [redacted]Match) ▾ Higher Education Press ✖

AND ▾ ✖

type ▾ [redacted](Match) ▾ Math ✖

type ▾ [redacted]Match) ▾ Learning method ✖

Price ▾ [redacted](<=) ▾ 20 ✖

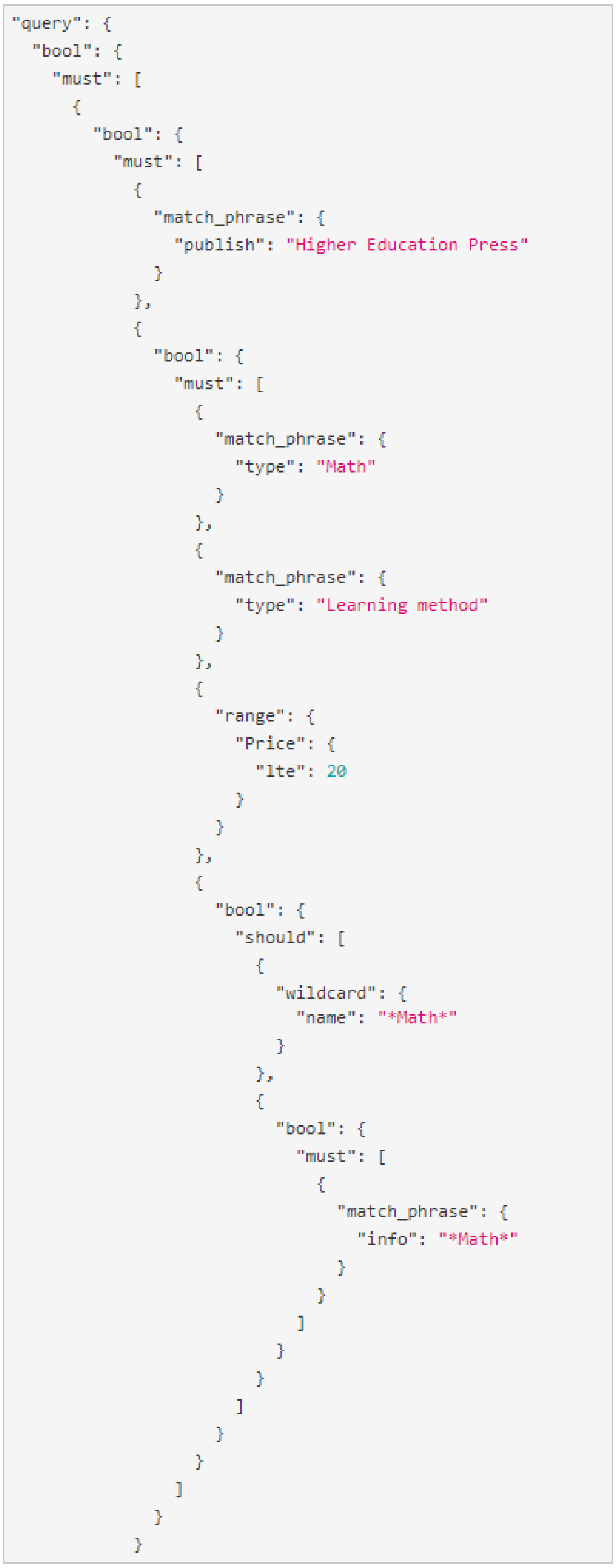
OR ▾ ✖

name ▾ [redacted](Wildcard) ▾ *Math* ✖

AND ▾ ✖

info ▾ [redacted](Match) ▾ *Math* ✖

The actual DSL statement for the query is as follows:



```
"query": {
  "bool": {
    "must": [
      {
        "bool": {
          "must": [
            {
              "match_phrase": {
                "publish": "Higher Education Press"
              }
            },
            {
              "bool": {
                "must": [
                  {
                    "match_phrase": {
                      "type": "Math"
                    }
                  },
                  {
                    "match_phrase": {
                      "type": "Learning method"
                    }
                  },
                  {
                    "range": {
                      "Price": {
                        "lte": 20
                      }
                    }
                  },
                  {
                    "bool": {
                      "should": [
                        {
                          "wildcard": {
                            "name": "*Math*"
                          }
                        },
                        {
                          "bool": {
                            "must": [
                              {
                                "match_phrase": {
                                  "info": "*Math*"
                                }
                              }
                            ]
                          }
                        }
                      ]
                    }
                  }
                ]
              }
            }
          ]
        }
      }
```

As shown in the preceding examples, BSearch-QueryBuilder significantly simplifies the complexity of Elasticsearch queries.

3 ES self-built functions

Elasticsearch official documentation

Alibaba Cloud Elasticsearch is built based on open-source Elasticsearch 5.5.3. For more information, see Elasticsearch Reference 5.5.

SDK Client

The SDK client only supports HTTP requests. You can use Java REST Client, which is provided by Elasticsearch.

Elasticsearch Clients

- Java REST Client [6.4] — other versions
- Java API [6.4] — other versions
- JavaScript API
- Groovy API [2.4] — other versions
- . NET API [6.x] — other versions
- PHP API [6.0] — other versions
- Perl API
- Python API
- Ruby API
- Community Contributed Clients

4 Snapshots and restore

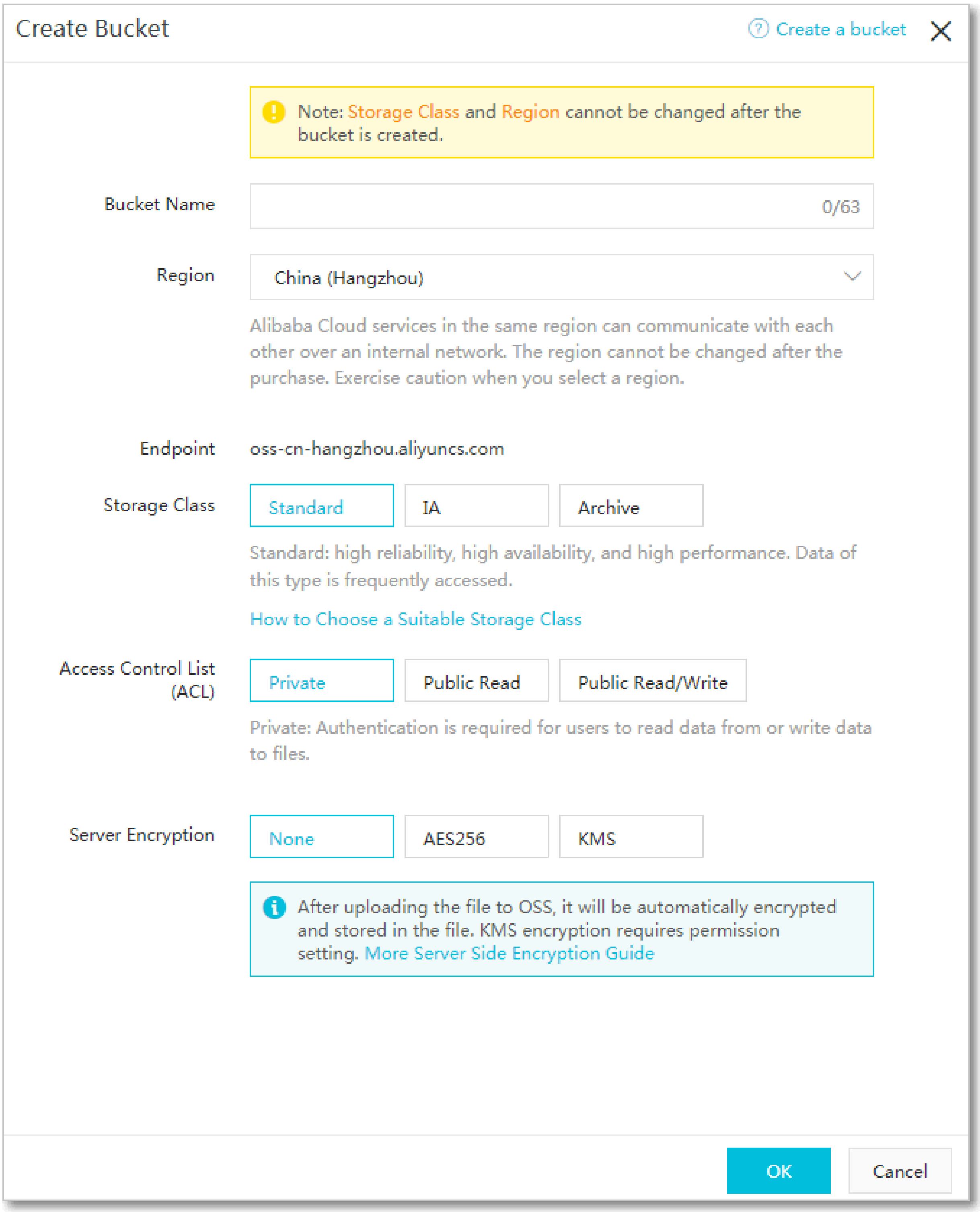
You can call the `snapshot` operation to back up your Alibaba Cloud Elasticsearch cluster. The `snapshot` operation retrieves the current status and data of the cluster, and then saves them to a shared repository. The backup process is intelligent.

The first snapshot is a full copy of the cluster. Subsequent snapshots only save the difference between the existing snapshots and the new data. Therefore, when you create new snapshots, Elasticsearch only needs to add data to or delete data from the backups. This means that it will be much faster to create subsequent snapshots than creating the first snapshot.

> Notice:
> The <1>, <2>, and <3> tags in this topic are markers used for code description purposes. Remove these tags when you run the code.

Prerequisites

Before you create a snapshot for an Alibaba Cloud Elasticsearch cluster, you must first #unique_57 and create an OSS bucket. The OSS bucket must be Standard because Archive type OSS buckets are not supported. You must create the OSS bucket and Elasticsearch instance in the same region.



Create Bucket

Note: Storage Class and Region cannot be changed after the bucket is created.

Bucket Name: 0/63

Region: China (Hangzhou)

Alibaba Cloud services in the same region can communicate with each other over an internal network. The region cannot be changed after the purchase. Exercise caution when you select a region.

Endpoint: oss-cn-hangzhou.aliyuncs.com

Storage Class: Standard | IA | Archive

Standard: high reliability, high availability, and high performance. Data of this type is frequently accessed.

How to Choose a Suitable Storage Class

Access Control List (ACL): Private | Public Read | Public Read/Write

Private: Authentication is required for users to read data from or write data to files.

Server Encryption: None | AES256 | KMS

After uploading the file to OSS, it will be automatically encrypted and stored in the file. KMS encryption requires permission setting. More Server Side Encryption Guide

Create a repository

```
 PUT   _snapshot / my_backup
{
   " type ": " oss ",
    " settings ": {
        " endpoint ": " http :// oss - cn - hangzhou - internal .
 aliyuncs . com ", < 1 >
        " access_key  _id ": " xxxx ",
        " secret_acc  ess_key ": " xxxxxx ",
        " bucket ": " xxxxxx ", < 2 >
```

```
         " compress ": " true ",
         " base_path ": " snapshot /" < 3 >
     }
 }
```

- <1>: `endpoint` specifies the intranet endpoint of the OSS bucket. For more information, see Intranet endpoint for ECS access in #unique_59.
- <2>: the name of the OSS bucket. The OSS bucket must exist.
- <3>: the base_path field specifies the path of the repository. The default is the root directory.

Set the shard size

When you need to upload a large amount of data to an OSS bucket, you can set the shard size to divide the data into multiple shards and then upload them to the OSS bucket.

```
 POST   _snapshot / my_backup / < 1 >
 {
     " type ": " oss ",
     " settings ": {
         " endpoint ": " http :// oss - cn - hangzhou - internal .
 aliyuncs . com ",
         " access_key  _id ": " xxxx ",
         " secret_acc  ess_key ": " xxxxxx ",
         " bucket ": " xxxxxx ",
         " chunk_size ": " 500mb ",
         " base_path ": " snapshot /" < 2 >
     }
 }
```

- <1>: call the `POST` method instead of the `PUT` method. The POST method updates the repository settings.
- <2>: the *`base_path`* field specifies the path of the repository. The default is the root directory.

Query repository information

```
 GET   _snapshot
```

You can call `GET   _snapshot / my_backup` to query information of a specified repository.

Migrate a snapshot to an Elasticsearch cluster

Follow these steps to migrate a snapshot to an Elasticsearch cluster.

1. Back up a snapshot to OSS.

2. Create a snapshot repository on the target cluster. The repository must use the OSS bucket that stores the snapshot.
3. Set the `base_path` field to the path of the snapshot.
4. Call the restore operation.

Create a snapshot for all open indexes

A repository stores multiple snapshots. Each snapshot is a copy of the indexes on the cluster. You can create a snapshot for one or more specified indexes, or all indexes. When you create a snapshot, make sure that the snapshot name is unique.

Snapshot operations

The following is a basic snapshot operation:

```
 PUT   _snapshot / my_backup / snapshot_1
```

This operation creates the `snapshot_1` snapshot for all open indexes. The snapshot is saved to the `my_backup` repository. After you call this operation, the result is returned immediately. The snapshot creation process is running in the background.

If you want Elasticsearch to return the result after it creates the snapshot, add the `wait_for_c ompletion` parameter as follows:

```
 PUT   _snapshot / my_backup / snapshot_1 ?  wait_for_c  ompletion =
 true
```

This operation does not return the result until the snapshot is created. This process can be time-consuming when you create a snapshot for large indexes.

Create a snapshot for the specified indexes

By default, a snapshot contains all open indexes. For Kibana, due to the disk space limit, you may want to ignore all diagnosis indexes (the `. kibana` indexes) when you create a snapshot. To perform this task, create a snapshot for the specified indexes as follows:

```
 PUT   _snapshot / my_backup / snapshot_2
{
    " indices ": " index_1 , index_2 "
}
```

In this example, only the `index1` and `index2` indexes are backed up.

Query snapshot information

In some cases, you may need to query the snapshot information. For example, a snapshot name containing a date is hard to remember, such as `backup_2014_10_28`.

To query the information of a snapshot, send a `GET` request that contains the repository name and snapshot ID.

```
GET   _snapshot / my_backup / snapshot_2
```

The response contains detailed information of the snapshot:

```
{
" snapshots ": [
   {
      " snapshot ": " snapshot_2 ",
      " indices ": [
         ". marvel_201  4_28_10 ",
         " index1 ",
         " index2 "
      ],
      " state ": " SUCCESS ",
      " start_time ": " 2014 - 09 - 02T13 : 01 : 43 . 115Z ",
      " start_time  _in_millis ":  1409662903  115 ,
      " end_time ": " 2014 - 09 - 02T13 : 01 : 43 . 439Z ",
      " end_time_i  n_millis ":  1409662903  439 ,
      " duration_i  n_millis ":  324 ,
      " failures ": [],
      " shards ": {
         " total ":  10 ,
         " failed ":  0 ,
         " successful ":  10
      }
   }
]
}
```

You can replace the snapshot ID in the operation with `_all` to query all snapshots in the repository:

```
GET   _snapshot / my_backup / _all
```

Delete a snapshot

You can specify a repository name and snapshot ID, and send a `DELETE` request to delete the specified snapshot as follows:

```
DELETE   _snapshot / my_backup / snapshot_2
```

Notice:

- You must use only the `delete` operation to delete snapshots. Do not manually or use other methods to delete snapshots. A snapshot is associated with other backup files. Some of the files are also used by other snapshots. The `delete` operation does not delete files that are still used by other snapshots. It only deletes files that are associated with the deleted snapshot and are not used by other snapshots.
- If you choose to manually delete a snapshot, you may delete all files that are associated with the snapshot by mistake. This may cause data loss.

Monitor snapshot progress

The `wait_for_c  ompletion` parameter provides the simplest method for you to monitor the progress of a snapshot process. However, this parameter is not suitable for snapshot processes running for medium-size Elasticsearch clusters. You can call the following operations to query detailed information about a snapshot:

- Specify a snapshot ID and send a `GET` request.

```
GET   _snapshot / my_backup / snapshot_3
```

  If Elasticsearch is still creating the snapshot when you call this operation, the operation returns the progress information, such as the time when the snapshot creation process started and the duration.

  Notice:

  The monitor snapshot progress operation shares the same thread pool with the snapshot creation operation. Therefore, if a snapshot is being created on large shards, the monitor snapshot progress operation has to wait until the snapshot creation operation releases the resources in the thread pool.

- Call the `_status` operation to query the snapshot status.

```
{
" snapshots ": [
   {
      " snapshot ": " snapshot_3 ",
      " repository ": " my_backup ",
      " state ": " IN_PROGRES  S ", < 1 >
      " shards_sta  ts ": {
         " initializi  ng ":  0 ,
         " started ":  1 , < 2 >
         " finalizing ":  0 ,
         " done ":  4 ,
         " failed ":  0 ,
         " total ":  5
      },
      " stats ": {
         " number_of_  files ":  5 ,
         " processed_  files ":  5 ,
         " total_size  _in_bytes ":  1792 ,
         " processed_  size_in_by  tes ":  1792 ,
         " start_time  _in_millis ":  1409663054  859 ,
         " time_in_mi  llis ":  64
      },
      " indices ": {
         " index_3 ": {
            " shards_sta  ts ": {
               " initializi  ng ":  0 ,
               " started ":  0 ,
               " finalizing ":  0 ,
               " done ":  5 ,
               " failed ":  0 ,
               " total ":  5
            },
            " stats ": {
               " number_of_  files ":  5 ,
               " processed_  files ":  5 ,
               " total_size  _in_bytes ":  1792 ,
               " processed_  size_in_by  tes ":  1792 ,
               " start_time  _in_millis ":  1409663054  859 ,
               " time_in_mi  llis ":  64
            },
            " shards ": {
               " 0 ": {
                  " stage ": " DONE ",
                  " stats ": {
                     " number_of_  files ":  1 ,
                     " processed_  files ":  1 ,
                     " total_size  _in_bytes ":  514 ,
                     " processed_  size_in_by  tes ":  514 ,
                     " start_time  _in_millis ":  1409663054  862 ,
                     " time_in_mi  llis ":  22
                  }
               },
                    ...
```

- <1>: the status of the snapshot. If a snapshot is in progress, the field shows `IN_PROGRESS`.
- <2>: indicates the number of shards that are being transmitted. When value 1 is returned, this indicates that a shard of the snapshot is being transmitted. The other four shards have been transmitted.

The `shards_stats` list contains the status of the snapshot and statistics about each index and shard. This allows you to learn detailed information about the snapshot progress. A shard can be in one of the following states:

- `INITIALIZING`: the shard is verifying the status of the cluster to confirm whether the shard can be snapshotted. Typically, this process is fast.
- `STARTED`: data is being transmitted to the repository.
- `FINALIZING`: the data transmission process is completed. The shard is sending snapshot metadata.
- `DONE`: the snapshot is created.
- `FAILED`: an error occurred during the snapshot process. The shard, index, or snapshot cannot be completed. You can check the log for more information.

Cancel a snapshot

To cancel a snapshot, you can call the following operation when the snapshot is in progress:

```
DELETE   _snapshot / my_backup / snapshot_3
```

This operation stops the snapshot process and then deletes the snapshot in progress from the repository.

Restore from a snapshot

To restore indexes from a snapshot, call the Create a repository operation on the Elasticsearch instance that you want to restore the indexes to. You can choose one of the following methods to restore indexes from a snapshot:

- To restore indexes from a specified snapshot, append the `_restore` parameter to the snapshot ID and call the operation as follows:

  ```
  POST   _snapshot / my_backup / snapshot_1 / _restore
  ```

  By default, the operation restores all indexes in the snapshot. For example, if the `snapshot_1` snapshot contains five indexes, all these indexes will be restored to the Elasticsearch cluster. You can also reference Create a snapshot for the specified indexes and specify the indexes that you want to restore.
- Restore the specified indexes and rename the indexes. Use this method when you want to restore the former data to verify or process its content without overwriting the existing data.

  ```
   POST  / _snapshot / my_backup / snapshot_1 / _restore
  {
   " indices ": " index_1 ", < 1 >
   " rename_pat  tern ": " index_ (.+)", < 2 >
   " rename_rep  lacement ": " restored_i  ndex_ $ 1 " < 3 >
  }
  ```

  In this example, the `index_1` index is restored to your Elasticsearch cluster and renamed as `restored_i  ndex_1` .

  - <1>: only restore the `Index_1` index in the snapshot.
  - <2>: search for indexes that are being restored and match the provided pattern.
  - <3>: rename the matching indexes.
- If you want the operation to return the result after the restore process is complete, add the `wait_for_c  ompletion` parameter as follows:

  ```
  POST   _snapshot / my_backup / snapshot_1 / _restore ?  wait_for_c
  ompletion = true
  ```

  The `_restore` operation returns the result immediately. The restoration process is running in the background. If you want the operation to return the result after the restore process is complete, add the `wait_for_c  ompletion` parameter.

Monitor restore operations

> Note:
> Restoring data from a repository applies the existing restoration mechanism in Elasticsearch. Restoring shards from a repository is the same as restoring data from a node.

You can call the `recovery` operation to monitor the restore operations.

- Monitor a specified index that is being restored.

  ```
  GET   restored_i  ndex_3 / _recovery
  ```

  The `recovery` operation is a general-purpose operation that shows the status of the shards that are being transmitted to your cluster.

- Monitor all indexes on the cluster. This may include shards that are irrelevant to the restore operation:

  ```
  GET  / _recovery /
  ```

  The returned result can be verbose depending on the activity of your cluster. The returned result is as follows:

  ```
  {
  " restored_i  ndex_3 " : {
   " shards " : [ {
     " id " :  0 ,
     " type " : " snapshot ", < 1 >
     " stage " : " index ",
     " primary " :  true ,
     " start_time " : " 2014 - 02 - 24T12 : 15 : 59 . 716 ",
     " stop_time " :  0 ,
     " total_time  _in_millis " :  175576 ,
     " source " : { < 2 >
       " repository " : " my_backup ",
       " snapshot " : " snapshot_3 ",
       " index " : " restored_i  ndex_3 "
     },
     " target " : {
       " id " : " ryqJ5lO5S4 - lSFbGntkEk  g ",
       " hostname " : " my . fqdn ",
       " ip " : " 10 . 0 . 1 . 7 ",
       " name " : " my_es_node "
     },
     " index " : {
       " files " : {
         " total " :  73 ,
         " reused " :  0 ,
         " recovered " :  69 ,
         " percent " : " 94 . 5 %" < 3 >
       },
       " bytes " : {
         " total " :  79063092 ,
         " reused " :  0 ,
         " recovered " :  68891939 ,
         " percent " : " 87 . 1 %"
       },
       " total_time  _in_millis " :  0
     },
     " translog " : {
       " recovered " :  0 ,
       " total_time  _in_millis " :  0
     },
     " start " : {
  ```

```
   "check_index_time": 0,
   "total_time_in_millis": 0
  }
 } ]
}
}
```

- <1>: the `type` field indicates the type of the restore operation. The value `snapshot` indicates that the shard is being restored from a snapshot.
- <2>: the `source` field indicates the source snapshot and repository.
- <3>: the `percent` field indicates the progress of the restore operation. The value `94.5%` indicates that 94.5% of the shard files have been restored.

The output lists all indexes that are being restored and the shards in these indexes . Each shard has statistics about the start or stop time, duration, restoration progress, and bytes transmitted.

Cancel a restore operation

To cancel a restore operation, you only need to delete the indexes that are being restored. A restore operation is a shard restore process. You can call the `DELETE` operation to modify the status of the cluster to cancel the restore process.

```
DELETE /restored_index_3
```

If the `restored_index_3` index is being restored, this operation stops the restore process and deletes the data that has been restored to the cluster.

For more information, see Snapshot And Restore.

5 RAM

5.1 Authorized resources

Resource types and descriptions

The following table lists the supported resource types and the corresponding Aliyun resource names (ARN).

Resource type	ARN
instances	acs:elasticsearch:$regionId:$accountId:instances/*
instances	acs:elasticsearch:$regionId:$accountId:instances/$instanceId
vpc	acs:elasticsearch:$regionId:$accountId:vpc/*
vswitch	acs:elasticsearch:$regionId:$accountId:vswitch/*

- $regionId: the ID of the specified region. You can also enter an asterisk `*`.
- $accountId: the ID of your Alibaba Cloud account. You can also enter an asterisk `*`.
- $instanceId: the ID of a specified Alibaba Cloud Elasticsearch instance. You can also enter an asterisk `*`.

Instance authorization

Note:
The following ARNs are shortened. For the complete name information, see the preceding table.

- Common actions on instances

Action	Description	ARN
elasticsearch:CreateInstance	You can perform this action to create an instance.	`instances /*`
elasticsearch:ListInstance	You can perform this action to view instances.	`instances /*`

Action	Description	ARN
elasticsearch:DescribeInstance	You can perform this action to view instance description.	`instances /*` or `instances /$ instanceId`
elasticsearch:DeleteInstance	You can perform this action to delete an instance.	`instances /*` or `instances /$ instanceId`
elasticsearch:RestartInstance	You can perform this action to restart an instance.	`instances /*` or `instances /$ instanceId`
elasticsearch:UpdateInstance	You can perform this action to update an instance.	`instances /*` or `instances /$ instanceId`

- Actions on plug-ins

Action	Description	ARN
elasticsearch:ListPlugin	You can perform this action to obtain the list of plug-ins.	`instances /$ instanceId`
elasticsearch:InstallSystemPlugin	You can perform this action to install system plug-ins.	`instances /$ instanceId`
elasticsearch:UninstallPlugin	You can perform this action to uninstall a plug-in.	`instances /$ instanceId`

- Actions on networks

Action	Description	ARN
elasticsearch:UpdatePublicNetwork	You can perform this action to check whether access through the public address is allowed.	`instances /$ instanceId`
elasticsearch:UpdatePublicIps	You can perform this action to modify the public network whitelist.	`instances /$ instanceId`
elasticsearch:UpdateWhiteIps	You can perform this action to modify the VPC whitelist.	`instances /$ instanceId`

Action	Description	ARN
elasticsearch:UpdateKibanaIps	You can perform this action to modify the Kibana whitelist.	`instances /$ instanceId`

- Actions on dictionaries

Action	Description	ARN
elasticsearch:UpdateDict	You can perform this action to modify the IK analyzer and synonym dictionary.	`instances /$ instanceId`

Authorized CloudMonitor actions (CloudMonitor console)

Note:

The following ARNs are shortened to a * wildcard form.

Action	Description	ARN format
cms:ListProductOfActiveAlert	You can perform this action to view services that have CloudMonitor enabled.	*
cms:ListAlarm	You can perform this action to query the specified or all alarm rule settings.	*
cms:QueryMetricList	You can perform this action to query the monitoring data of a specified instance.	*

VPC and VSwitch authorization

Note:

The following ARNs are shortened. For the complete name information, see the preceding table.

Action	Description	ARN
DescribeVpcs	You can perform this action to obtain a VPC list.	`vpc /*`

Action	Description	ARN
DescribeVswitches	You can perform this action to obtain a VSwitch list.	`vswitch /*`

Intelligent Maintenance authorization

Note:

The following ARNs are shortened. For the complete name information, see the preceding table.

Action	Description	ARN
elasticsearch:OpenDiagnosis	You can perform this action to enable health diagnosis.	`instances /*` or `instances /$ instanceId`
elasticsearch:CloseDiagnosis	You can perform this action to disable health diagnosis.	`instances /*` or `instances /$ instanceId`
elasticsearch:UpdateDiagnosisSettings	You can perform this action to update the health diagnosis settings.	`instances /*` or `instances /$ instanceId`
elasticsearch:DescribeDiagnosisSettings	You can perform this action to query the health diagnosis settings.	`instances /*` or `instances /$ instanceId`
elasticsearch:ListInstanceIndices	You can perform this action to query instance indexes.	`instances /*` or `instances /$ instanceId`
elasticsearch:DiagnoseInstance	You can perform this action to start health diagnosis.	`instances /*` or `instances /$ instanceId`
elasticsearch:ListDiagnoseReportIds	You can perform this action to query diagnosis report IDs.	`instances /*` or `instances /$ instanceId`
elasticsearch:DescribeDiagnoseReport	You can perform this action to view diagnosis report details.	`instances /*` or `instances /$ instanceId`

Action	Description	ARN
elasticsearch:ListDiagnoseReport	You can perform this action to list diagnosis reports.	`instances /*` or `instances /$ instanceId`

Supported regions

Elasticsearch region	RegionId
China (Hangzhou	cn-hangzhou-d
China (Beijing)	cn-beijing
China (Shanghai)	cn-shanghai
China (Shenzhen	cn-shenzhen
India (Mumbai)	ap-south-1
Singapore	ap-southeast-1
cn-hongkong	cn-hongkong
US (Silicon Valley)	us-west-1
Malaysia (Kuala Lumpur)	ap-southeast-3
Germany (Frankfurt)	eu-central-1
Japan (Tokyo	ap-northeast-1
Australia (Sydney	ap-southeast-2
Indonesia (Jakarta)	ap-southeast-5
China (Qingdao)	cn-qingdao
China (Zhangjiakou)	cn-zhangjiakou

5.2 Access authentication rules

General permission policies

The following two general permission policies are provided to meet the needs for common access, so that you can select a permission policy suitable for you. You can search for the policy name in the brackets from Optional Authorization Policy Names and select it.

- Read-only permissions for Elasticsearch instances, applicable for read-only users (AliyunElasticsearchReadOnlyAccess).

- Administrator permissions for Elasticsearch instances, applicable for the administrator (AliyunElasticsearchFullAccess).

  Note:
  If none of the above general permission policies can meet your needs, you can refer to the following description and customize a permission policy.

Permission to buy instances (post-payment & prepayment)

Permission to access the VPC of the primary account

- [“vpc:DescribeVSwitch*” , “vpc:DescribeVpc*”]

  Note:
  You can refer to the system template AliyunVPCReadOnlyAccess.

Subaccount order permission

- [“bss:PayOrder”]

  Note:
  You can refer to the system template AliyunBSSOrderAccess.

API permissions

Method	URI	Resource	Action
GET	/instances	instances/*	ListInstance
POST	/instances	instances/*	CreateInstance
GET	/instances/$ instanceId	instances/$ instanceId	DescribeInstance
DELETE	/instances/$ instanceId	instances/$ instanceId	DeleteInstance
POST	/instances/$ instanceId/actions/ restart	instances/$ instanceId	RestartInstance
PUT	/instances/$ instanceId	instances/$ instanceId	UpdateInstance

Authorization examples

- #unique_64 (for example, $regionid, $accountid, and $instanceId).
- Elasticsearch instances in the resource can be indicated by the wildcard `*`.

Authorization example 1

To a subaccount under the primary account (accountId “1234”), assign all operation permissions, except for CreateInstance, over all instances in China East 1 (Hangzhou) on the console, and set the instances to be accessible from only the specified IP address.

After this policy is created on the console of the primary account, you need to use your primary account on the RAM console or the RAM SDK to authorize the subaccount.

1. Create a policy

```
{
  " Statement  ":[
    {
      " Action ": [
        " imagesearc  h : ListInstan  ce ",
        " imagesearc  h : DescribeIn  stance ",
        " elasticsea  rch : DeleteInst  ance ",
        " elasticsea  rch : RestartIns  tance ",
        " elasticsea  rch : UpdateInst  ance "
      ],
      " Condition ": {
        " IpAddress ": {
          " acs : SourceIp ": " xxx . xx . xxx . x / xx "
        }
      },
      " Effect ": " Allow ",
      " Resource ": " acs : imagesearc  h : cn - shanghai : 1234 :
 instance /*"
    }
  ],
  " Version ": " 1 "
}
```

2. Authorize the current policy to your specified subaccount.

Authorization example 2

For a subaccount under the primary account (accountId “1234”), assign all operation permissions, except for CreateInstance, over the specified instances in China East 1 (Hangzhou) on the console, and set the instances to be accessible from only the specified IP address.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

1. Create a policy

```
{
  " Statement  ":[
    {
      " Action ": [
        " elasticsea  rch : ListInstan  ce "
      ],
      " Condition ": {
        " IpAddress ": {
          " acs : SourceIp ": " xxx . xx . xxx . x / xx "
        }
      },
      " Effect ": " Allow ",
      " Resource ": " acs : imagesearc  h : cn - shanghai : 1234 :
 instance /*"
    },
    {
      " Action ": [
        " elasticsea  rch : DescribeIn  stance ",
        " elasticsea  rch : DeleteInst  ance ",
        " elasticsea  rch : RestartIns  tance ",
        " elasticsea  rch : UpdateInst  ance "
      ],
      " Condition ": {
        " IpAddress ": {
          " acs : SourceIp ": " xxx . xx . xxx . x / xx "
        }
      },
      " Effect ": " Allow ",
      " Resource ": " acs : elasticsea  rch : cn - hangzhou : 1234 :
 instances /$ instanceId "
    }
  ],
  " Version ": " 1 "
}
```

2. Authorize the current policy to your specified subaccount.

Authorization example 3

To a subaccount under the primary account (accountId “1234”), assign all operation permissions over all instances in all regions supported by Alibaba Cloud Elasticsearch on the console.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

1. Create a policy

```
{
  " Statement  ":[
    {
      " Action ": [
          " elasticsea  rch :*"
          ],
      " Effect ": " Allow ",
      " Resource ": " acs : imagesearc  h :*: 1234 : instance /*"
    }
  ],
  " Version ": " 1 "
}
```

2. Authorize the current policy to your specified subaccount.

Authorization example 4

To a subaccount under the primary account (accountId “1234”), assign all operation permissions, except for CreateInstance and ListInstance, over specified instances in all regions supported by Alibaba Cloud Elasticsearch on the console.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

1. Create a policy

```
{
  " Statement  ":[
    {
      " Action ": [
          " elasticsea  rch : DescribeIn  stance ",
          " elasticsea  rch : DeleteInst  ance ",
          " elasticsea  rch : UpdateInst  ance ",
          " elasticsea  rch : RestartIns  tance "
            ],
      " Effect ": " Allow ",
      " Resource ": " acs : elasticsea  rch :*: 1234 : instances /$
 instanceId "
    }
  ],
  " Version ": " 1 "
}
```

2. Authorize the current policy to your specified subaccount.

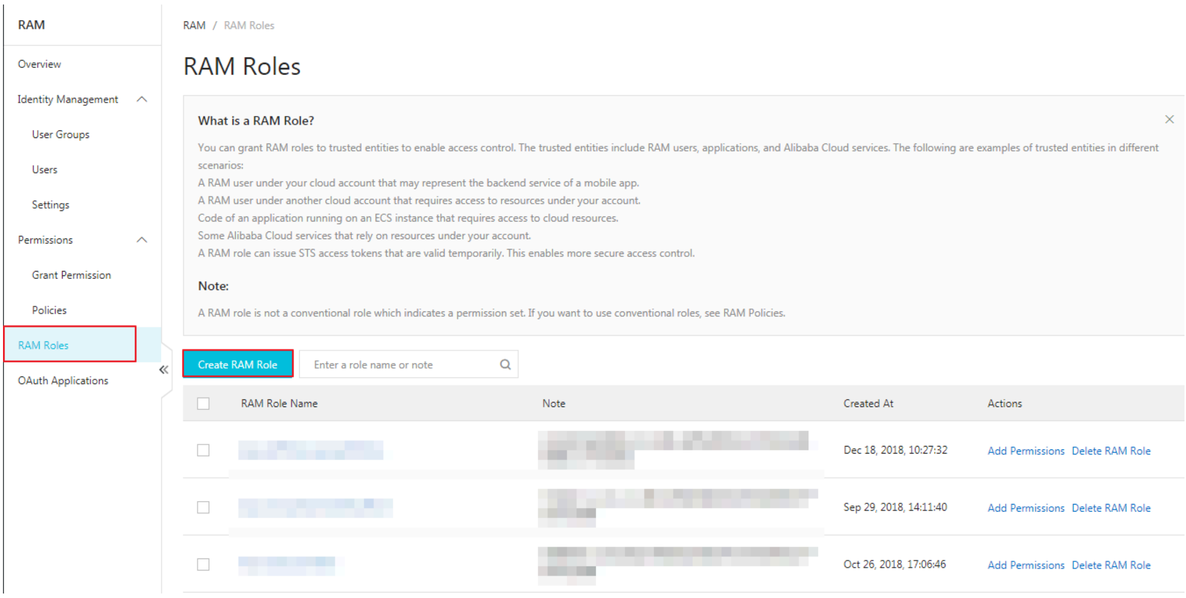
5.3 Temporary access token

Users (people or applications) that only access your cloud resources occasionally are called temporary users. You can use Security Token Service (STS, an extended authorization service of RAM) to issue an access token to these users (subaccounts). The permission and automatic expiration time of the token can be defined as required upon issuing.

The advantage of using the STS access token to authorize temporary users is making the authorization more controllable. You do not need to create a RAM user account and key for the temporary users. The RAM user account and key are valid in the long term but the temporary users do not need to access the resources for long. For use cases, see #unique_66 and #unique_67.

Create a role

1. On the RAM console, choose RAM Roles > Create RAM Role



RAM Roles

What is a RAM Role?

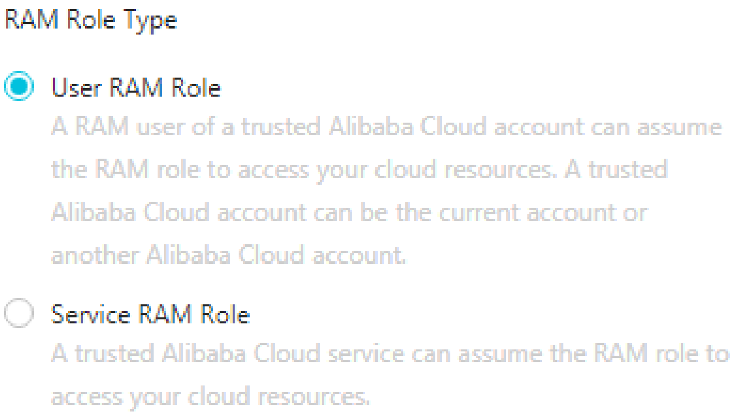
You can grant RAM roles to trusted entities to enable access control. The trusted entities include RAM users, applications, and Alibaba Cloud services. The following are examples of trusted entities in different scenarios:
A RAM user under your cloud account that may represent the backend service of a mobile app.
A RAM user under another cloud account that requires access to resources under your account.
Code of an application running on an ECS instance that requires access to cloud resources.
Some Alibaba Cloud services that rely on resources under your account.
A RAM role can issue STS access tokens that are valid temporarily. This enables more secure access control.

Note:

A RAM role is not a conventional role which indicates a permission set. If you want to use conventional roles, see RAM Policies.

□	RAM Role Name	Note	Created At	Actions
□	[redacted]	[redacted]	Dec 18, 2018, 10:27:32	Add Permissions Delete RAM Role
□	[redacted]	[redacted]	Sep 29, 2018, 14:11:40	Add Permissions Delete RAM Role
□	[redacted]	[redacted]	Oct 26, 2018, 17:06:46	Add Permissions Delete RAM Role

2. Select the role type. Here, the role User is selected.

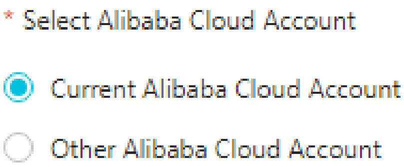


RAM Role Type

● User RAM Role
A RAM user of a trusted Alibaba Cloud account can assume the RAM role to access your cloud resources. A trusted Alibaba Cloud account can be the current account or another Alibaba Cloud account.

○ Service RAM Role
A trusted Alibaba Cloud service can assume the RAM role to access your cloud resources.

3. Enter the type information. A subaccount of a trusted account can play the created role.

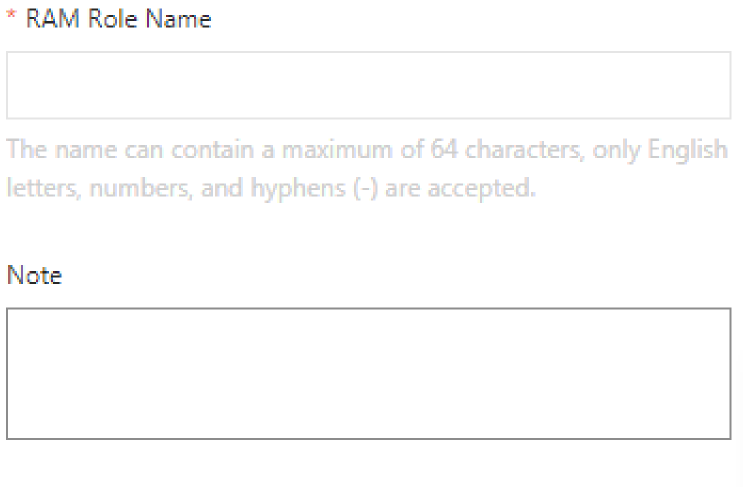


* Select Alibaba Cloud Account

● Current Alibaba Cloud Account

○ Other Alibaba Cloud Account

4. Enter the role name.



* RAM Role Name

The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

5. After a role is created, authorize the role. For details, see #unique_68 and #unique_64.

Temporary access authorization

Before using STS for access authorization, authorize the role to be assumed by the subaccount of the trusted cloud account created in Step 3. If any subaccount could assume these roles, unpredictable risks may occur. Therefore, in order to assume the corresponding role, a subaccount has to have explicitly configured permissions.

Authorization of the trusted cloud account

1. Click Policy Management on the left side of the page to go to the Policy Management page.
2. Click Create Authorization Policy on the right side of the page to go to the Create Authorization Policy page.
3. Select a blank template to go to the Create Custom Authorization Policy page.
4. Enter the authorization policy name and fill the following content to the policy content field.

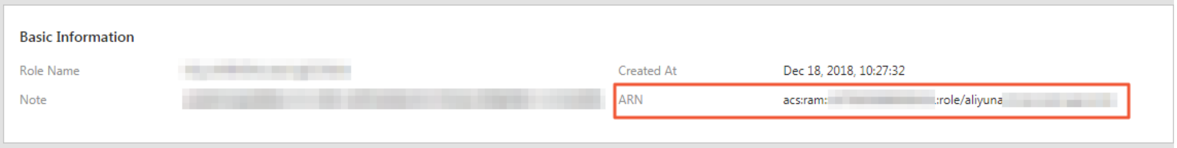
```
{
" Version ": " 1 ",
" Statement ": [
{
   " Effect ": " Allow ",
   " Action ": " sts : AssumeRole ",
   " Resource ": " acs : ram ::${ aliyunID }: role /${ roleName }"
}
]
}
```

${aliyunID} indicates the ID of the user that creates the role.

${roleName} indicates the role name in lowercase.

Note:

The resource details can be obtained from the Arn field in Role Details and Basic Information.



Basic Information

Role Name	[redacted]	Created At	Dec 18, 2018, 10:27:32
Note	[redacted]	ARN	acs:ram:[redacted]:role/aliyuna[redacted]

5. On the User Management page, authorize the permission of the role created for the subaccount. For details, see #unique_68.

Role assumed by a subaccount

After logging on to the console through the subaccount, the subaccount can switch to the authorized role assumed by the subaccount to practise permissions of the role. The steps are as follows:

1. Move the mouse to the profile picture on the upper-right corner of the navigation bar, and click Switch Role in the window.
2. Enter the enterprise alias of the account with which you intend to create a role. If the enterprise alias is not modified, the account ID is used by default. Enter the role name and then click Switch to switch to the specified role.