Alibaba Cloud
Elasticsearch
Instances

Issue: 20191231
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, consequent
ial, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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.
# Document conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Danger: Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td>⚠️</td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td>⚠️</td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td>Notice: If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td>💡</td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td>Note: You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Closing angle brackets are used to indicate a multi-level menu cascade.</td>
<td>Click Settings &gt; Network &gt; Set network type.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Bold formatting is used for buttons, menus, page names, and other UI elements.</td>
<td>Click OK.</td>
</tr>
<tr>
<td><code>Courier font</code></td>
<td>Courier font is used for commands.</td>
<td>Run the <code>cd /d C:/window</code> command to enter the Windows system folder.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic formatting is used for parameters and variables.</td>
<td><code>bae log list --instanceid Instance_ID</code></td>
</tr>
<tr>
<td>[ ] or [a</td>
<td>b]</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
</tr>
<tr>
<td>Style</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>{} or {a</td>
<td>b}</td>
<td>This format is used for a required value, where only one item can be selected.</td>
</tr>
</tbody>
</table>
11.1.2 Basic configuration (6.7.0) .......................................................129
11.1.3 Network access configuration ..................................................132
11.1.4 Plug-ins ...................................................................................133
11.1.5 BSearch-QueryBuilder plug-in .................................................136
11.1.6 BSearch-Label plug-in .............................................................147
The Instances list of Alibaba Cloud Elasticsearch (ES) displays basic instance information. You can create instances, configure alerting, update instance status, and manage instances on this page.

After you create an Elasticsearch instance, you are navigated to the Instances page. The Instances page shows all Elasticsearch instances in the current region under your account. You can perform the following tasks on this page:

- View the instance list.

  The instance list includes these columns: Instance ID/Name, Status, Version, Data Nodes, Instance Specification, Zone, Billing Method, Network Type, and Creation Time.

- View basic instance information.

  Click an instance ID in the Instance ID/Name column to open the Basic Information page. For more information, see Overview.

- Create an instance.

  Click Create to open the buy page and then create an instance. For more information, see #unique_5.

- Configure alerting.

  Click Alarms to navigate to the CloudMonitor console and enable the alerting feature for Alibaba Cloud Elasticsearch. By default, this feature is disabled for Alibaba Cloud Elasticsearch. After alerting is enabled for Elasticsearch, rules are created to detect errors such as cluster status errors, disk usage errors (>75%), and JVM heap memory errors (>85%). These rules are applied to all Elasticsearch instances under your Alibaba Cloud account. For more information, see #unique_6.

- Update instance status.

  Click Refresh to update the status of the Elasticsearch instances. After an Elasticsearch instance is created, it is in the Initializing state. Click Refresh to update the status of the instance. After the Status of the instance changes to Active, you can use the instance.
· Manage instances.

Click Manage in the Actions column to open the instance management page. On this page, you can perform tasks such as upgrade the cluster, view logs, configure security settings, and configure plug-ins. For more information, see Manage instances.

· Switch to subscription.

Click More > Switch to Subscription in the Actions column to open the Confirm Order page, and then change the billing method.

· Update configuration.

Click More > Update Configuration in the Actions column to open the Update page, and then modify the cluster configuration. For more information, see Cluster upgrade.

· Release an instance.

⚠️ Warning:
After an instance is released, all the data on the instance is lost and cannot be recovered. Exercise caution when you release instances.

Click More > Release in the Actions column to open the Release message, and click OK to release the instance.
2 Manage instances

The instance management module of Alibaba Cloud Elasticsearch supports features including cluster monitoring, instance restart, instance status refresh, and task list.

Go to the instance management page

After you create an Elasticsearch instance, click the ID of your instance in the Instance ID/Name column on the Instances page to open the Instance Management page.

Restart an instance

After you modify the configuration of an Elasticsearch instance or perform other operations, you may need to manually restart the instance for the changes to take effect.

Prerequisites

Before you restart an instance, make sure that the status of the Elasticsearch instance is Active (green color), the instance has at least one index replica, and the resource usage is not high. You can go to the Cluster alerting page to check the resource usage. Ensure that the NodeCPUUtilization(%) is around 80% or lower, the NodeHeapMemoryUtilization(%) is around 50%, and the NodeLoad_1m does not exceed the number of CPU cores of the current data node.

1. Go to the instance management page, and click Restart Instance in the upper-right corner of the page.
2. In the Restart Instance dialog box, select a restart method.

The supported restart methods are restart and force restart.

- **Restart**

  The Elasticsearch instance can continuously provide services during the restart process. However, you must first make sure that the instance meets the prerequisites. This restart method is time-consuming.

  **Notice:**
  - Before you restart the instance, make sure that the status of the instance is Active (green color). Otherwise, you have to use the *force restart* method to restart the instance.
  - The CPU and memory usage of the Elasticsearch instance will spike during the restart process. This may adversely affect the stability of your workloads for a short period of time.
  - The amount of time that the restart process takes depends on the amount of data stored on the instance and the numbers of nodes, indexes, and shards. Elasticsearch cannot estimate the total amount of time required to restart an instance. You can check the progress of the restart task on the Tasks page.

- **Force restart**

  If an Elasticsearch instance is restarted by this method, your workloads 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 display yellow or red color. In this situation, you cannot use the restart method to restart the instance. You can only forcibly restart the instance.

  - When the status of the instance displays yellow or red color, we recommend that you do not perform these operations on the instance: upgrade nodes, expand disk space, restart the instance, reset the password, or other operations that may change the configuration of the instance.
instance. Perform these operations only after the status of the instance displays green color.

- If you update the configuration of an Elasticsearch instance that contains two or more nodes in the preceding situation, the instance will be constantly in the Initializing state. You can submit a ticket to contact Alibaba Cloud Elasticsearch technical support to resolve this issue.

3. Click OK to restart the instance.

During the restart process, the status of the instance displays Initializing (yellow color). You can view the details on the Tasks page. After the instance is restarted, the Status field displays Active (green color).

Refresh an instance

If the instance information in the console is not updated promptly, you can use this feature to manually update the instance information. For example, after you create an Elasticsearch instance, the status of the instance still displays Failed. You can use this feature to update the instance status.

Go to the instance management page, and click Refresh in the upper-right corner of the page. After the instance status is updated, it displays Active. If the instance still displays an error, contact Alibaba Cloud Elasticsearch technical support to resolve this issue.
View task progress

You can click the Tasks icon to view the progress of a running task, such as an instance creation or restart task.

1. Go to the instance management page, and click the (Tasks) icon in the upper-right corner of the page.
2. On the Tasks page, check the progress under Updating Instance.
3. Click Show Details to view detailed information about the tasks.

Pause a task

1. Go to the instance management page, and click the (Tasks) icon in the upper-right corner of the page.
2. On the Tasks page, check the progress under Updating Instance.
3. Click Pause.

4. In the Pause Updates message, select the I Have Read and Understand the Risks check box after you read the agreement, and click OK.

Note:
It takes a short period of time for Elasticsearch to pause the task.

5. After you pause a task, you can click Resume on the Tasks page to resume the task.

Notice:
- An Elasticsearch instance is in the Paused state if it has a task paused. If your workloads running on the instance are adversely affected, resume the task or
run the task again to resolve the issue. You can resume a cluster upgrade task or plug-in management task.

- After you click Resume, Elasticsearch will restart all the nodes in the instance, which may take a short period of time.

Cluster monitoring

Alibaba Cloud Elasticsearch supports cluster monitoring. When Alibaba Cloud Elasticsearch detects any errors, it sends alerts to you through SMS messages.

Go to the instance management page, and click Cluster Monitoring in the upper-right corner of the page to log on to CloudMonitor. In the CloudMonitor console, you can customize alert thresholds. For more information, see Elasticsearch alerts.
3 Basic Information

3.1 Overview

This topic describes the content displayed on the Basic Information page of an Alibaba Cloud Elasticsearch (ES) instance.

Log on to the Alibaba Cloud Elasticsearch console, click the ID of your instance in the Instance ID/Name column on the Instances page to open the Basic Information page.

On the Basic Information page, you can view basic information of an Elasticsearch instance.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance ID</td>
<td>The unique ID of the Alibaba Cloud Elasticsearch instance.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the Elasticsearch instance. By default, the name of an Elasticsearch instance is the same as its ID. Instance names are user configurable. You can search instances by name.</td>
</tr>
<tr>
<td>Version</td>
<td>Elasticsearch V5.5.3, V6.3.2, and V6.7.0 are supported. You cannot switch between these Elasticsearch versions without data migration. To switch to another version, you must create a new Elasticsearch instance and then migrate the data on the existing instance to the new one. For more information, see #unique_14.</td>
</tr>
<tr>
<td>Region</td>
<td>The region where the Elasticsearch instance is deployed.</td>
</tr>
<tr>
<td>VPC</td>
<td>The VPC network to which the Elasticsearch instance is connected.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internal Network Address</td>
<td>In a VPC network, you can use an Elastic Compute Service (ECS) instance to connect to the internal network address of an Elasticsearch instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Notice:</strong></td>
</tr>
<tr>
<td></td>
<td>Data security is not guaranteed when you connect to an Alibaba Cloud Elasticsearch instance from the Internet. 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 the ECS instance to connect to the internal network address of the Elasticsearch instance.</td>
</tr>
<tr>
<td>Public Network Access</td>
<td>You can connect to the public network address of an Alibaba Cloud Elasticsearch instance from the Internet. To use this method, you must first enable public network access on the <code>Security</code> page.</td>
</tr>
<tr>
<td>Public Network Port</td>
<td>The public network port is shown only after you enable Public Network Access. Elasticsearch supports the following ports:</td>
</tr>
<tr>
<td></td>
<td>- Port 9200 for HTTP and HTTPS.</td>
</tr>
<tr>
<td></td>
<td>- Port 9300 for TCP. Only Alibaba Cloud Elasticsearch V5.5.3 with Commercial Feature supports this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>- Alibaba Cloud Elasticsearch V6.3.2 and V6.7.0 do not support using the transport client to connect to port 9300.</td>
</tr>
<tr>
<td></td>
<td>- To use these ports, you must first configure <code>Public network whitelist</code>. By default, Elasticsearch forbids all public network addresses.</td>
</tr>
<tr>
<td>Protocol</td>
<td>By default, HTTP is selected. You can click Edit to change the protocol. Currently, you can choose between HTTP and HTTPS. For more information, see <code>Enable HTTPS</code>.</td>
</tr>
<tr>
<td>Created At</td>
<td>The time when the Elasticsearch instance was created.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The status of the Elasticsearch instance. An Elasticsearch instance has these states: Active (green color), Initializing (yellow color), and Expired (gray color).</td>
</tr>
<tr>
<td><strong>Billing Method</strong></td>
<td>The supported billing methods are subscription and pay-as-you-go.</td>
</tr>
<tr>
<td><strong>Zone</strong></td>
<td>The zone where the Elasticsearch instance is deployed.</td>
</tr>
<tr>
<td><strong>VSwitch</strong></td>
<td>The VSwitch to which the Elasticsearch instance is connected.</td>
</tr>
<tr>
<td><strong>Internal Network Port</strong></td>
<td>The following internal network ports are supported:</td>
</tr>
<tr>
<td></td>
<td>• Port 9200 for HTTP and HTTPS.</td>
</tr>
<tr>
<td></td>
<td>• Port 9300 for TCP. Only Alibaba Cloud Elasticsearch V5.5.3 supports this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>Alibaba Cloud Elasticsearch V6.3.2 and V6.7.0 do not support using the transport client to connect to port 9300.</td>
</tr>
<tr>
<td><strong>Renew</strong></td>
<td>This option is shown only when the billing method is set to subscription.</td>
</tr>
<tr>
<td></td>
<td>You can click Renew on the right side of Basic Information to renew the instance. You can renew your subscription with one or more months. The minimum renewal period is one month.</td>
</tr>
</tbody>
</table>
### 3 Basic Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch to Subscription</td>
<td>This option is shown only when the billing method is set to pay-as-you-go.</td>
</tr>
<tr>
<td></td>
<td>You can click Switch to Subscription on the right side of Basic Information to open the page and then follow the instructions to change the billing method. With the switch to subscription feature, you can change the billing method of your Elasticsearch instance from pay-as-you-go to subscription. However, no discount is offered on subscription when you change the billing method.</td>
</tr>
</tbody>
</table>

#### 3.2 Node visualization

You can view visualized information about the nodes in an Alibaba Cloud Elasticsearch instance on the Data Visualization tab of the instance.

On the Basic Information page, click the Data Visualization tab. On the Data Visualization tab, you can perform the following tasks:

- Move your mouse pointer to the Cluster icon, a message is popped up displaying the Status of the cluster. Click Intelligent Maintenance to navigate to the Intelligent Maintenance module. You can follow the instructions to activate Intelligent Maintenance or diagnose the cluster.
• You can verify the status of a cluster node based on its color.

Note:
The color of a cluster node is determined by the resource usage of the node. The resource usage thresholds are the same as those in CloudMonitor.

- Red: Warning.
- Yellow: Alert.
- Green: Normal.
- Grey: Unknown. This status indicates that the system has failed to retrieve the node information for a long period of time.
The node information includes Node IP, Node Status, CPU Usage | CPU Type, Disk Usage | Disk Capacity, Load Balancing, and JVM Memory.

If a node is in red, yellow, or gray color, the system displays the The node is disconnected or the node status is unhealthy, we recommend that you use Intelligent Maintenance message. Click Intelligent Maintenance to navigate to the Intelligent Maintenance > Cluster Diagnosis page, and then diagnose the cluster.

The nodes are not running in the Normal state. We recommend that you use Intelligent Maintenance to check your instance.
3.3 Configuration info

You can view the configuration of an Alibaba Cloud Elasticsearch instance on its Configuration Info tab. The instance configuration includes the number and specification of data nodes and the number and specification of Kibana nodes.

On the Basic Information page, click the Configuration Info tab to view the configuration of your Elasticsearch instance.

For more information about parameter descriptions, see #unique_18.

3.4 Downgrade data nodes

Alibaba Cloud Elasticsearch allows you to downgrade data nodes by removing data nodes from an Elasticsearch instance.

Notice:

- You can scale in both pay-as-you-go and subscription-based Elasticsearch instances deployed in one zone or across zones.
- After you remove data nodes from an instance, the system must restart the instance. Make sure that it does not adversely affect your workloads, and then confirm the operation to restart the instance.
- Before you remove data nodes, you must migrate the data on the data nodes to other nodes.

Procedure

1. Log on to the Alibaba Cloud Elasticsearch console.
2. On the Instances page, click the ID of your instance in the Instance ID/Name column.
3. In the Basic Information section, click Remove Data Nodes.

4. After you click Remove Data Nodes, specify the Node Type on the Remove Data Nodes page, and select the data nodes that you want to remove from the node list.

5. Migrate the data to other nodes.
   
   To ensure data security, you must make sure that no data is stored on the removed data nodes. If data is stored on these data nodes, the system prompts a message asking you to migrate the data. After the data migration process is
complete, no index data is stored on the data nodes and no index data will be written into these data nodes.

a. Click Data Migration Tool in the popped up message.

b. On the Migrate Data page, select a data migration method.

- **Smart migration**
  
The system automatically selects the data nodes to be downgraded for you. You must select the check box to accept the terms of data migration, and then click OK.

- **Custom data migration**
  
You must select the data nodes that you want to downgrade.
c. Select the check box to accept the terms of data migration, and then click OK.

6. After the data is migrated, click OK.

After you confirm to remove the data nodes, the instance is restarted. During the restart process, you can check the progress on the **Tasks** page. After the instance is restarted, the data nodes are removed from the instance.
During the data migration process, you can click Stop on the Tasks page to stop a migration task.

Roll back a migration

Data migration is time-consuming. Any cluster status or data changes may result in data migration failures. To view detailed information, you can open the Tasks page in the upper-right corner of the Elasticsearch console. You can use one of the following methods to roll back a migration when the migration task fails or completes.

1. Query the IP addresses of the removed data nodes.

   You can check the IP addresses of the removed data nodes on the Tasks page, or log on to the Kibana console and call the following API operation.

   // Query the configuration of the cluster.
   GET _cluster/settings

   The following result is returned.

   ```
   {
     "transient": {
       "cluster": {
         "routing": {
           "allocation": {
             "exclude": {
             }
           }
         }
       }
     }
   }
   ```

2. Roll back data.

   Log on to the Kibana console, and run the following command on the Console tab to roll back the data.

   - Roll back the data on some data nodes. Use the exclude parameter to exclude the data nodes that you do not want to roll back.

   ```
   PUT _cluster/settings
   {
     "transient": {
       "cluster": {
         "routing": {
           "allocation": {
             "exclude": {
             }
           }
         }
       }
     }
   }
   ```
**Roll back the data on all data nodes.**

```
PUT _cluster/settings
{
  "transient": {
    "cluster": {
      "routing": {
        "allocation": {
          "exclude": {
            "_ip": null
          }
        }
      }
    }
  }
}
```

3. Check whether the data is rolled back.

Log on to the *Kibana console*, run the `GET _cluster/settings` command to check the progress of the rollback task based on the returned data node IP addresses. You can also check the rollback progress based on whether the shards are reallocated to the corresponding data nodes.

**Note:**

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

**Error messages**

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

**Cause:** 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 workloads.

**Solution:** You can run the `GET _cat/indices? v` command to check whether the number of index replicas in the cluster exceeds the number of data nodes after the cluster is scaled in. You also need to check whether the resource usage, such as the disk usage, is below the threshold so that the cluster has sufficient resources.
resources to store data or process requests. If these requirements are not met, perform a *Cluster upgrade*.

- The cluster is running tasks or in an error status. Try again later.

  **Solution:** You can run the `GET _cluster/health` command to check the 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.

  **Solution:** For more information about data migration, see step 6 in *Procedure*.

- The number of nodes that you reserve must be greater than two and greater than half of the existing nodes.

  **Cause:** 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 to be rolled back or removed each time must be no greater than half of the existing data nodes.

  **Solution:** If these requirements are not met, reselect the data nodes that you need to roll back or perform a *Cluster upgrade*.

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

  **Solution:** You can run the `GET _cluster/settings` command to query the cluster configuration and check whether the cluster configuration contains settings that forbid data allocation.

- **auto_expand_replicas**

  **Cause:** Some users may use the permission management function supported by X-Pack. In earlier Elasticsearch versions, this function applies the "index .auto_expand_replicas" : "0-all" setting to the .security and .security-6 indexes by default. This causes errors when you migrate data or scale in nodes.

  **Solution:** We recommend that you modify the index setting *auto_expansd_replicas* as follows:

  1. Query the index settings.

     ```
     GET .security/_settings
     ```

     The following result is returned.

     ```
     {}
2. Use one of the following methods to modify the settings.

//Method 1:
PUT .security/_settings
{
   "index" : {
      "auto_expand_replicas" : "0-1"
   }
}

//Method 2:
PUT .security/_settings
{
   "index" : {
      "auto_expand_replicas" : "false",
      "number_of_replicas" : "1"
   }
}

⚠️ Notice:
Set the number of replicas based on the actual needs. You must guarantee a minimum of one replica per index and make sure that the number of replicas is no greater than the number of available data nodes.

3.5 Cluster upgrade

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

⚠️ Notice:
You cannot switch between Alibaba Cloud Elasticsearch V5.5.3, V6.3.2, and V6.7.0 without data migration. You must first create an instance and then migrate data to the instance. For more information, see #unique_14.

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, choose Instance ID > Basic Information > Upgrade to open the Update page.

The Update page includes the Current Config and Configuration Upgrade sections. 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.

Considerations

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

- If you need to upgrade the instance due to workload requirements, make an evaluation before you upgrade the cluster.
- For each upgrade operation, you can change only 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 only change the number of nodes, the instance is not restarted.
· If the status of your Elasticsearch instance is unhealthy (showing yellow or red color), you have to select Force Update when you upgrade the instance. Force update may adversely affect your workloads.
· 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-based instances currently do not support downgrading. For example, you cannot remove nodes from a cluster, scale in the disk space, or downgrade the node specification.
· You can downgrade Alibaba Cloud Elasticsearch pay-as-you-go instances by removing data nodes. The number of data nodes that you can remove 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 is 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 Considerations.

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.

Some of the parameters are described as follows.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Family/Instance Type</td>
<td>The Instance Family cannot be changed. If the Instance Family is set to a local disk type, the Instance Type cannot be changed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dedicated Master Node</td>
<td>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 GB. After you upgrade the dedicated master nodes, the Elasticsearch instance is billed based on the new configuration.</td>
</tr>
<tr>
<td>Client Node</td>
<td>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 GB. After you upgrade the client nodes, the Elasticsearch instance is billed based on the new configuration.</td>
</tr>
<tr>
<td>Warm Node</td>
<td>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 GB. After you upgrade the warm nodes, the Elasticsearch instance is billed based on the new configuration.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Kibana Node</td>
<td><em>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 2 cores and 4 GB of memory.</em></td>
</tr>
<tr>
<td><strong>Notice:</strong></td>
<td><em>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 is billed based on the new configuration.</em></td>
</tr>
<tr>
<td>Force update</td>
<td><em>If the status of your Elasticsearch instance is unhealthy (displaying red or yellow color), your workloads are 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.</em></td>
</tr>
</tbody>
</table>
| **Notice:**     | *
<p>|                 | • The Elasticsearch instance must restart to complete the force update process.                                                                                                                            |
|                 | • During the force update process, your workloads on the Elasticsearch instance may become unstable.                                                                                                      |
|                 | • If you do not select Force Update, the restart method is used to upgrade the instance. For more information, see <em>Manage instances</em>.                                                                           |
|                 | • If the status of your Alibaba Cloud Elasticsearch instance is not healthy (displaying red or yellow color), the system automatically selects Force Update for you. You cannot select the restart method to upgrade the instance.* |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>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 expand a purchased ultra disk to up to 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.</td>
</tr>
</tbody>
</table>
4 Elasticsearch cluster configuration

4.1 Elasticsearch cluster configuration

Word splitting

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

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.

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 Configuration

Auto Indexing: ○ Disable
○ Enable
○ Custom +, *

Index Deletion: ○ Index Names Only
○ Allow Wildcard Characters

Audit Log Indexing: ○ Disable
○ Enable

Watcher: ○ Disable
○ Enable

Other Configurations:

This operation will restart the instance. Continue?
Elasticsearch Instances / 4 Elasticsearch cluster configuration

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 *YML configuration*.

**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

### 4.2 Configure synonyms

Alibaba Cloud Elasticsearch (ES) allows you to configure synonyms. You can update the synonym dictionary of Elasticsearch by uploading a customized synonym dictionary file. After the synonym dictionary is updated, new indexes are searched using the updated synonym dictionary.

**Considerations**

- After you upload a synonym dictionary file, Alibaba Cloud Elasticsearch does not need to restart the nodes. The dictionary file is deployed to the nodes in the background. The time that it takes for the updated dictionary to take effect depends on the number of nodes.

- For example, the 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, the index index-aliyun cannot automatically
load the new dictionary file. Therefore, we recommend that you recreate the
indexes after you update the synonym dictionary. Otherwise, only new indexes
use the updated synonym dictionary.

- The synonym dictionary file must be a .txt file encoded by using UTF-8. Each
  line contains only one synonym expression. Example:

  ipod, i-pod, i pod => ipod, i-pod, i pod
  foo => foo bar

Synonym settings

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

```json
PUT /test_index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "synonym": {
            "tokenizer": "whitespace",
            "filter": ["synonym"]
          }
        },
        "filter": {
          "synonym": {
            "type": "synonym",
            "synonyms_path": "analysis/synonym.txt",
            "tokenizer": "whitespace"
          }
        }
      }
    }
  }
}
```

- filter: configure a synonym filter that contains the analysis/synonym.txt path.
  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_case: The default value is false.
  - expand: The default value is true.

Two synonym formats are supported: Solr and WordNet.
Solr synonyms

The following example shows the format of the Solr synonym file:

```
# Blank lines and lines starting with pound are comments.
# Explicit mappings match any token sequence on the LHS of "=>"
# and replace with all alternatives 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 filter in the configuration file, but you must use synonyms instead of synonyms_path. The sample code is as follows:

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

Note:
We recommend that you use `synonyms_path` to define large synonym sets in the file. Using `synonyms` to define large synonym sets increases the size of your cluster.

- **WordNet synonyms**

The following example shows the format of the WordNet synonym file:

```json
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)."
            ]
          }
        }
      }
    }
  }
}
```

This example uses `synonyms` to define WordNet synonyms. You can also use `synonyms_path` to define WordNet synonyms.

**Procedure**

1. Log on to the Alibaba Cloud Elasticsearch console, upload a synonym file, and save. Make sure that the uploaded file takes effect.
2. When you configure `settings` to create an index, set 
   `"synonyms_path": "analysis/your_dict_name.txt"`, add a mapping to the index, and configure synonyms for the specified fields.
3. Verify the synonyms and upload a file to run a search test.

**Example 1**

The following example shows how to use a filter to configure synonyms.

1. On the **Cluster Configuration** page, click Synonym Dictionary Configuration on the right side of Word Splitting.
2. On the Synonym Dictionary Configuration page, click Upload, select the synonym dictionary file, and then click Save. In this example, the TXT file created as described in the Synonym settings section is uploaded.

3. After the Elasticsearch instance is activated and its status changes to Active, you can then use the synonym dictionary.

In this example, file aliyun_synonyms.txt is uploaded for testing. The file contains: begin, start.

4. Configure and test the synonym dictionary.
   a. Log on to the Kibana console.
   b. On the Console tab, send the following request to create an index:

```
PUT aliyun-index-test
{
    "index": {
        "analyzer": {
            "by_smart": {
                "type": "custom",
                "tokenizer": "ik_smart",
                "filter": ["by_tfr","by_sfr"],
                "char_filter": ["by_cfr"]
            },
            "by_max_word": {
                "type": "custom",
                "tokenizer": "ik_max_word",
                "filter": ["by_tfr","by_sfr"],
                "char_filter": ["by_cfr"]
            }
        },
        "filter": {
            "by_tfr": {
```

```
c. Send the following request to configure the synonym field title:

```plaintext
PUT /aliyun-index-test/_mapping/doc
{
  "properties": {
    "title": {
      "type": "text",
      "analyzer": "by_max_word",
      "search_analyzer": "by_smart"
    }
  }
}
```

d. Send the following request to verify the synonyms:

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

If the request is successful, the following result is returned:

```json
{
  "tokens": [
    {
      "token": "begin",
      "start_offset": 0,
      "end_offset": 5,
      "type": "ENGLISH",
      "position": 0
    },
    {
      "token": "start",
      "start_offset": 0,
      "end_offset": 5,
      "type": "SYNONYM",
      "position": 0
    }
  ]
}
```
e. Send the following request to add data for further testing:

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

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

f. Send the following request to run a search test:

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

If the request is successful, the following result is returned:

```json
{
"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": {}
}
]```
"_source": {
"_title": "Shall I begin?"
},
"highlight": {
"title": [
"Shall I <red>begin</red>?"
]
}
]
}
]

Example 2

The following example shows how to directly reference the synonym dictionary and use the IK filter.

1. Log on to the Kibana console, and send the following request on the Console tab.

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

This request is sent to complete the following tasks:

a. Configure the synonym filter `my_synonym_filter` and a synonym dictionary.

b. Create the `my_synonyms` analyzer, and use the IK tokenizer `ik_smart` to tokenize the query string.

c. The `ik_smart` tokenizer changes all tokens to lowercase and then matches the tokens against the synonym dictionary.

2. Send the following request to configure the synonym field `title`:

```
PUT /my_index/_mapping/doc
```

3. Send the following request to verify the synonyms:

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

If the request is successful, the following result is returned:

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

4. Send the following request to add data for further testing:

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

PUT /my_index/doc/2
{
```
5. Send the following request to run a search test:

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

If the request is successful, the following result is returned:

```json
{
"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>?"
]
}
}
]
}
Some of the content in this topic is referenced from the official Elasticsearch documentation. For more information, see Synonym Token Filter and Using Synonyms.

4.3 Advanced settings

For instances of Alibaba Cloud Elasticsearch (ES) V6.7.0 and later versions, you can change the garbage collector type if the memory size per data node is larger than 32 GB. Supported garbage collectors are: CMS and G1.

Considerations

• After you configure a garbage collector, Elasticsearch must restart the cluster for the garbage collector to take effect. Please confirm the operation and wait for the system to restart the cluster.

• Only Alibaba Cloud Elasticsearch V6.7.0 and later versions support changing the garbage collector type. Alibaba Cloud Elasticsearch V5.5.3 and V6.3.x do not support this feature.

• For instances of Alibaba Cloud Elasticsearch V6.7.0 and later versions, you can change the garbage collector type only if the memory size per data node is equal to or larger than 32 GB. If the memory size is smaller than 32 GB, only the CMS garbage collector is supported.

Procedure

1. Go to the Cluster Configuration page of your Alibaba Cloud Elasticsearch instance, click Edit Configuration on the right side of Advanced Configuration.

Warning:
After you change the garbage collector type, the system will restart the cluster. Make sure that this does not adversely affect your businesses and then confirm the operation.
2. In the Edit Configuration dialog box, select G1, and click OK to switch to the G1 garbage collector.

After you confirm the operation, the cluster is restarted. After the cluster is restarted, the garbage collector is switched to G1.

4.4 YML configuration

You can modify the YML configuration of Alibaba Cloud Elasticsearch (ES) to customize the configuration of your Alibaba Cloud Elasticsearch instance.

Procedure

⚠️ Warning:

After you modify the YML configuration, the system must restart the instance for the changes to take effect. Make sure that it does not adversely affect your workloads before you confirm to restart the instance.

1. On the Cluster Configuration page, click Modify Configuration on the right side of YML Configuration.
2. In the YML Configuration dialog box, set the parameters as follows:

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

- **Index Deletion**: indicates whether you need to specify the name of an index when you delete the index. If you select Allow Wildcard Characters, you can use wildcard characters to delete all matching indexes. You cannot restore the indexes that have been deleted. Proceed with caution.

- **Audit Log Index**: if you enable this feature, index log entries are created when you create, delete, modify, or search an index on an Alibaba Cloud Elasticsearch instance. These log entries consume disk space and affect the performance of your instance. We recommend that you disable this feature. Use caution when you configure this feature.

- **Watcher**: if you enable this feature, you can 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 supported configuration items are as follows. For more information, see Customize CORS (across regions), Recreate indexes from a remote Elasticsearch cluster in the whitelist, Customize audit log indexing, Customize queue size, and Parameters.

Note:
Unless otherwise specified, the following configuration items are only compatible with 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 (only compatible with Elasticsearch V5.5.3 with X-Pack)
- thread_pool.write.queue_size (only compatible with Elasticsearch V6.3.2 with X-Pack)
- thread_pool.search.queue_size

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

After you click Save, the instance is restarted. You can check the progress on the Tasks page. After the instance is restarted, the YML configuration is updated.

Customize CORS (across regions)

Notice:

- The configurations in the following table are custom configurations provided by Alibaba Cloud Elasticsearch to support HTTP.
- The configurations in the following table only support static configuration. This means that if you want the configurations to take effect, you must add the configurations to the elasticsearch.yml file.
- The following configurations are reliant on the network settings of the cluster.
<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.cors.enabled</td>
<td>The cross-origin resource sharing (CORS) setting. This setting indicates whether Elasticsearch allows a browser on another origin to send requests to it. Valid values: true and false.</td>
</tr>
<tr>
<td></td>
<td>• Set this value to true to enable CORS. After CORS is enabled, Elasticsearch can process pre-flight (OPTIONS) CORS requests. If the origin in a request is declared in the http.cors.allow-origin list, Elasticsearch responds to the request with the Access-Control-Allow-Origin header included in the response.</td>
</tr>
<tr>
<td></td>
<td>• Set this value to false (default value) to disable CORS. After CORS is disabled, Elasticsearch ignores the origin information in the request header. This effectively disables CORS because responses returned by Elasticsearch will never contain the Access-Control-Allow-Origin header. If a client does not support sending pre-flight requests with an origin header, or it does not validate the Access-Control-Allow-Origin header in the responses, the cross-origin security is compromised. If CORS is disabled for Elasticsearch, the only way for the client to know this is to send an OPTIONS request and check whether the required header is missing.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>http.cors.allow-origin</td>
<td>The origin setting. This setting specifies the origins to allow. By default, no origin is allowed. If you prepend and append a forward slash (/) to the value, the value is treated as a regular expression. This enables you to use regular expressions to support HTTP and HTTPS requests. For example, you can use /https?://localhost(:[0-9]+)? / to respond to any requests that match the regular expression.</td>
</tr>
<tr>
<td>http.cors.max-age</td>
<td>Browsers can send OPTIONS requests to query the CORS configuration. This setting specifies the caching time of the retrieved CORS configuration. The default is 1728000 seconds (20 days).</td>
</tr>
<tr>
<td>http.cors.allow-methods</td>
<td>The request method setting. This setting specifies the allowed methods. The default is OPTIONS, HEAD, GET, POST, PUT, DELETE.</td>
</tr>
<tr>
<td>http.cors.allow-headers</td>
<td>The request header setting. This setting specifies the headers to allow. The default is X-Requested-With, Content-Type, Content-Length.</td>
</tr>
</tbody>
</table>
Elasticsearch

Instances / 4 Elasticsearch cluster configuration

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http.cors.allow-credentials</code></td>
<td>The credential setting. This setting indicates whether Elasticsearch is allowed to return the <code>Access-Control-Allow-Credentials</code> header. The default is <code>false</code>, which means that Elasticsearch is not allowed to return the header. Set the value to <code>true</code> to allow Elasticsearch to return the header.</td>
</tr>
</tbody>
</table>

The following is an example of the custom CORS configurations.

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

For more information, see [HTTP](http://elasticsearch.org) in the official Elasticsearch documentation.

Recreate indexes from a remote Elasticsearch cluster in the whitelist

The reindex component allows you to recreate indexes from a remote Elasticsearch cluster. This feature is supported by all Elasticsearch versions.

With the reindex feature, you can copy data in indexes of an earlier Elasticsearch version to the indexes of a newly released Elasticsearch version. The following is an example. For more information, see [Reindex API](http://elasticsearch.org).

```plaintext
POST _reindex
{
  "source": {
    "remote": {
      "host": "http://otherhost:9200",
      "username": "user",
      "password": "pass"
    },
    "index": "source",
    "query": {
      "match": {
        "test": "data"
      }
    }
  },
  "dest": {
    "index": "dest"
  }
}
• host: the address of the remote host. The address must include the protocol, domain, and port information. Example: https://otherhost:9200.

⚠️ Notice:
The remote host must be declared by using the `reindex.remote.whitelist` property in the `elasticsearch.yml` file so that the host can call this API operation. The host can be declared by using a combination of the `host` and `port`. You can declare multiple hosts and separate them with commas (,). Example: otherhost:9200, another:9200, 127.0.10.*:9200,localhost:*. Only `host` and `port` are used because the whitelist ignores the protocol information.

• `username` and `password` are optional. If the requested Elasticsearch service uses basic authentication, include the information in the request. Basic authentication must be implemented over HTTPS. Otherwise, the password will be sent in plain text.

🔍 Note:
• If the host is already added to the whitelist, the `query` is directly sent to the Elasticsearch service without validation or modification.
• Reindexing from a remote cluster does not support manual slicing or automatic slicing. For more information, see Manual slicing and Automatic slicing.

**Batch size**

Reindexing from a remote cluster uses on-heap buffer. By default, the maximum batch size is 100 MB. If the index on the source cluster contains large documents, you must adjust the batch size to a smaller value.

In the following example, the batch size is set to 10.

```json
POST _reindex
{
    "source": {
        "remote": {
            "host": "http://otherhost:9200"
        },
        "index": "source",
        "size": 10,
        "query": {
            "match": {
                "test": "data"
            }
        }
    }
}
```
Elasticsearch

Instances / 4 Elasticsearch cluster configuration

Timeouts

- Use `socket_timeout` to set the socket read timeout. The default timeout is 30 seconds.
- Use `connect_timeout` to set the connection timeout. The default timeout is 1 second.

In the following example, the socket read timeout is set to 1 minute and the connection timeout is set to 10 seconds.

```json
POST _reindex
{
    "source": {
        "remote": {
            "host": "http://otherhost:9200",
            "socket_timeout": "1m",
            "connect_timeout": "10s"
        },
        "index": "source",
        "query": {
            "match": {
                "test": "data"
            }
        }
    },
    "dest": {
        "index": "dest"
    }
}
```

Customize audit log indexing

Enable audit log indexing

Alibaba Cloud Elasticsearch does not allow you to view the audit log. If you want to keep track of audit events on your Elasticsearch instance, you must log on to the Elasticsearch console and enable the audit log indexing feature for the instance.

After audit log indexing is enabled, auditing events are saved to your instance and added to indexes starting with `.security_audit_log-*`. 
Configure audit log indexing

⚠️ Notice:

- No filtering is performed during the auditing process. Therefore, if an auditing event contains the request body, sensitive data in plain text may be compromised.
- When auditing events are indexed, the storage space of your Elasticsearch instance is consumed. Alibaba Cloud Elasticsearch does not automatically clear expired indexes. You must manually clear old auditing event indexes.

The audit log indexing configuration is as follows:

```plaintext
xpack.security.audit.index.bulk_size: 5000
xpack.security.audit.index.events.emit_request_body: false
xpack.security.audit.index.events.exclude: run_as_denied,anonymous_access_denied,realm_authentication_failed,access_denied,connection_denied
xpack.security.audit.index.events.include: authentication_failed,access_granted,tampered_request,connection_granted,run_as_granted
xpack.security.audit.index.flush_interval: 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
```

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xpack.security.audit.index.bulk_size</td>
<td>1000</td>
<td>Specifies the number of auditing events that are batched in a single write.</td>
</tr>
<tr>
<td>xpack.security.audit.index.flush_interval</td>
<td>1s</td>
<td>Specifies the frequency of flushing buffered auditing events to the index.</td>
</tr>
<tr>
<td>xpack.security.audit.index.rollover</td>
<td>daily</td>
<td>Specifies the frequency of rolling over to a new index. Valid values: hourly, daily, weekly, and monthly.</td>
</tr>
</tbody>
</table>
You can also configure the indexes where the auditing events are stored. Use `xpack.security.audit.index.settings` as the namespace and add the setting to the `elasticsearch.yml` file.

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

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

### Note:

If you want to configure auditing event indexes by passing parameters, add the preceding setting to the YML configuration when enable audit log indexing. After the configuration takes effect, auditing event indexes are created on your Elasticsearch instance. If you do not customize the auditing event indexes, your Elasticsearch uses the default settings to create the indexes: `number_of_shards: 5` and `number_of_replicas: 1`.

For more information, see [Auditing Security Settings](#).
Customize queue size

You can customize the thread_pool.bulk.queue_size, thread_pool.write.queue_size, and thread_pool.search.queue_size settings to set the size of the document write queue and document search queue.

The following examples set the size of the document write and search queues to 500. You can adjust the values as needed.

Note:
Unless otherwise specified, the following examples are only compatible with Alibaba Cloud Elasticsearch V5.5.3 and V6.3.2.

| thread_pool.bulk.queue_size: 500 (only compatible with Elasticsearch V5.5.3 with X-Pack) |
| thread_pool.write.queue_size: 500 (only compatible with Elasticsearch V6.3.2 with X-Pack) |
| thread_pool.search.queue_size: 500 |

Parameters

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index.codec</td>
<td>By default, Elasticsearch compresses data with LZ4 compression. If your Elasticsearch cluster is a hot-warm cluster that uses ultra disks, set the parameter to best_compression to use DEFLATE for a higher compression ratio. After you change the compression type, data is compressed using the new compression type when segments are merged.</td>
</tr>
</tbody>
</table>

Notice:
The best_compression type degrades the read and write performance.
You can call the RESTful API to set the `index.codec` parameter. The example is as follows:

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

**Note:**
- You must close the relevant index before you send the request. Otherwise, an error occurs.
- `$index_name`: replace it with the name of the index.

### 4.5 Add Elasticsearch Head to Google Chrome

This topic describes how to add Elasticsearch Head to Google Chrome. With Elasticsearch Head, you can connect to the public network address of an Alibaba Cloud Elasticsearch instance and perform operations.

**Prerequisites**

Before you add Elasticsearch Head to Google Chrome, make sure that you can access the domain chrome.google.com.

**Context**

- Elasticsearch Head is a third-party extension.
- In a public network, you cannot use the internal network address and port of an Alibaba Cloud Elasticsearch instance to connect to the instance with Elasticsearch Head.

**Procedure**
1. Enter the Elasticsearch Head link [https://chrome.google.com/webstore/detail/elasticsearch-head/ffmkiejjmecolpfloofpjologoblkegm](https://chrome.google.com/webstore/detail/elasticsearch-head/ffmkiejjmecolpfloofpjologoblkegm) into the address bar of Google Chrome, and then click Add to Chrome.

![ElasticSearch Head](chrome web store)

2. Click Add extension in the dialog box.

![Add "ElasticSearch Head"?](Add extension)

The system then downloads and installs Elasticsearch Head. After the installation is complete, the system prompts a message indicating that Elasticsearch Head has been installed.

![ElasticSearch Head has been added to Chrome](ElasticSearch Head has been added to Chrome)
3. **Log on to the Alibaba Cloud Elasticsearch console, enable Public network access for your Elasticsearch instance, and add the public network IP address of your host to Public network whitelist.**

![Elasticsearch Configuration](image)

**Note:**

- To query the public network IP address of your host, open Google Chrome, enter "IP", and click What Is My IP Address.
- By default, the public network access function forbids all IPv4 addresses. You can add your host IP address to the public network whitelist to allow the host to access Elasticsearch.

4. **Click the Elasticsearch Head icon on the right side of the Google Chrome address bar to open the Elasticsearch cluster connection page.**

![Elasticsearch Connection](image)
5. Enter `http://<Elasticsearch instance public network address>:<Port number>/` into the address bar, and then click Connect.

You can log on to the Elasticsearch console and view the public network address and port number of the Elasticsearch instance on the basic information page. The default port number is 9200. The following is a sample connection address:

`http://es-cn-45xxxxxxxxx0lw6w.public.elasticsearch.aliyuncs.com:9200/`

6. In the Sign in dialog box, enter the username and password that are used to log on to the Kibana console of the Elasticsearch instance, and then click Sign in.

```
Sign in

http://es-cn-xxxxxx0lw6w.public.elasticsearch.aliyuncs.com:9200
Your connection to this site is not private

Username

Password

Sign in  Cancel
```

Note:
The Alibaba Cloud Elasticsearch with Commercial Feature is integrated with X-Pack for security purposes. Therefore, you must enter the username and password for authentication before you can log on to the instance. If the Sign in dialog box is not displayed, verify that the public network whitelist of Alibaba Cloud Elasticsearch contains the public network IP address of your host, or clear the cache of your Web browser and then try again.
7. After you log on to the Elasticsearch instance, you can then perform other operations.
5 Plug-ins

5.1 Overview

Based on plug-ins in open source communities, Alibaba Cloud Elasticsearch provides a variety of plug-ins and extensions. This 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 workload demands.

Use plug-ins

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

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 update IK dictionaries by uploading custom dictionary files. For more information, see Install and remove a built-in plug-in.

- Custom plug-ins

  You can upload, install, and remove custom plug-ins to meet your workload demands. For more information, see Custom plug-ins.
5.2 List of Built-in Plug-ins

5.2.1 Install and remove a built-in plug-in

This topic describes how to install and remove a built-in Alibaba Cloud Elasticsearch (ES) plug-in.

After you purchase an Alibaba Cloud Elasticsearch instance, the system automatically installs 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 the open source plug-in, a new function is added to this plug-in to support dynamically loading dictionary files stored on Object Storage Service (OSS). You can use the standard update or rolling update method to update dictionary files for the plug-in.

- elasticsearch-repository-oss: based on the open source plug-in, a new function is added to the plug-in for you to use OSS for storage when creating and restoring index snapshots.

Procedure

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 Confirm Operation message carefully and then click OK.

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.

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

Elasticsearch then restarts 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.

Additional information

Alibaba Cloud Elasticsearch supports the following built-in plug-ins:

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Default status</th>
<th>Description</th>
<th>Supported operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>analysis-aliws</td>
<td>Not Installed</td>
<td>Aliws analysis plug-in for Elasticsearch.</td>
<td>You can install or remove the plug-in, or configure dictionaries.</td>
</tr>
<tr>
<td>Plug-in</td>
<td>Default status</td>
<td>Description</td>
<td>Supported operation</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>analysis-icu</td>
<td>Installed</td>
<td>ICU analysis plug-in for Elasticsearch. It integrates the Lucene ICU module into Elasticsearch and adds ICU analysis components.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>analysis-ik</td>
<td>Installed</td>
<td>IK analysis plug-in for Elasticsearch. This plug-in cannot be removed.</td>
<td>You can use the standard update or rolling update method to upgrade the plug-in.</td>
</tr>
<tr>
<td>analysis-kuromoji</td>
<td>Installed</td>
<td>Japanese (Kuromoji) analysis plug-in for Elasticsearch. It integrates the Lucene Kuromoji analysis module into Elasticsearch.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>analysis-phonetic</td>
<td>Installed</td>
<td>Phonetic analysis plug-in for Elasticsearch. It integrates the phonetic token filter into Elasticsearch.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>analysis-pinyin</td>
<td>Installed</td>
<td>Pinyin analysis plug-in for Elasticsearch.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>analysis-smartcn</td>
<td>Installed</td>
<td>Smart Chinese analysis plug-in for Elasticsearch. It integrates the Lucene smart Chinese analysis module into Elasticsearch.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>analysis-stconvert</td>
<td>Not Installed</td>
<td>An analysis plug-in that allows you to convert text between simple Chinese and traditional Chinese.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>elasticsearch-repository-oss</td>
<td>Installed</td>
<td>The plug-in allows you to use Alibaba Cloud Object Storage Service (OSS) to store Elasticsearch snapshots. This plug-in cannot be removed.</td>
<td>N/A</td>
</tr>
<tr>
<td>Plug-in</td>
<td>Default status</td>
<td>Description</td>
<td>Supported operation</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>ingest-attachment</td>
<td>Installed</td>
<td>An ingest processor for Elasticsearch. It uses Apache Tika to extract content.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>mapper-murmur3</td>
<td>Installed</td>
<td>The Mapper Murmur3 plug-in allows you to compute the hashes of values of a field at index time and store them in the index.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>mapper-size</td>
<td>Installed</td>
<td>The Mapper Size plug-in allows documents to record their uncompressed size at index time.</td>
<td>You can install or remove the plug-in.</td>
</tr>
<tr>
<td>repository-hdfs</td>
<td>Installed</td>
<td>The HDFS repository plug-in enables support for Hadoop Distributed File System (HDFS) repositories.</td>
<td>You can install or remove the plug-in.</td>
</tr>
</tbody>
</table>

5.2.2 Update IK dictionaries

This topic describes how to use the standard or rolling update method to update the built-in IK analyzer plug-in of Alibaba Cloud Elasticsearch.

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

- *Standard update.*
- *Rolling update.*

Notice:

- For indexes that already have the IK analyzer configured, the updated dictionaries are only applied to new data added to these indexes. If you want to apply the updated dictionaries to both the existing data and new data, you must recreate the indexes.
- The Alibaba Cloud Elasticsearch IK analyzer plug-in is designed based on the open-source IK analyzer, with hot reload added as an addition. Hot reload allows an Elasticsearch instance to load a new version of a dictionary file.
without the need to restart all nodes. The current and new dictionary files must use the same name. The standard update method does not support hot reload.

Standard update

The standard update method updates the dictionaries on all nodes in an Elasticsearch instance. If you choose the standard update method, Elasticsearch will send the uploaded dictionary file to all nodes in the instance, 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 built-in 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 SYSTEM_MAIN.dic. The new dictionary file will automatically overwrite the current one. For more information about the main dictionary, see *IK Analysis for Elasticsearch*.

- If you want to update the built-in stopword list, upload a dictionary file named SYSTEM_STOPWORD.dic. The new dictionary file will automatically overwrite the current one. For more information about the stopword list, see *IK Analysis for Elasticsearch* and *How to configure the stopword list*.

Standard update example

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

2. In the left-side navigation pane, click Plug-ins, find the plug-in that you want to update, click Standard Update in the Actions column.
3. In the Plug-in Configuration dialog box, click Configure.

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

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 one of the above methods to manually upload the dictionary file again.

⚠️ **Warning:**
This operation will restart the Elasticsearch instance. Make sure that your workloads are not adversely affected before you confirm the operation.

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

6. After the instance is restarted, Log on to the Kibana console, and send the following request to check whether the dictionary takes effect.

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

⚠️ **Notice:**
- You cannot delete the built-in main dictionary or stopword list.
- Whether you upload a new dictionary file, remove a dictionary file, or update the dictionary content, if you choose the standard update method, Elasticsearch must restart the instance.
You can use the standard update method only when the instance is in the Normal state.

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, the changes will be updated to the `IKAnalyzer.cfg.xml` file. Consequently, all the nodes in the instance must reload the dictionary configuration. For example, after you upload a new dictionary file or delete an existing dictionary file, all the nodes must reload the dictionary configuration.

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 modify the `IKAnalyzer.cfg.xml` file. After the dictionary is updated, Elasticsearch must restart the instance for the new dictionary to take effect.

Rolling update example

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

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

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 one of the above methods to manually upload the dictionary file again.

**Warning:**
This operation will restart the Elasticsearch instance. Make sure that your workloads are not adversely affected before you confirm the operation.

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

After you click Save, the instance performs 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 `a_1@words.dic`.

This task changes the content of an existing dictionary file on the instance. Therefore, Elasticsearch does not need to restart the instance for the update to take effect.

7. Click Save.

The plug-in on the nodes of the Elasticsearch instance will automatically load the dictionary file. The amount of 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 load the dictionary file. You can log on to the Kibana console and send the following request to verify that the new dictionary takes effect.

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

**Note:**
You cannot 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`.

### How to configure the stopword list

Alibaba Cloud Elasticsearch provides a built-in stopword list. The stopword list contains predefined tokens: an, and, are, as, at, be, but, by, for, if, in, into, is, it, no, not, of, on, or, such, that, the, their, then, there, these, they, this, to, was, will, with.

You can follow these steps to delete tokens from the stopword list:

1. Download the built-in stopword list package from Stopword list.
2. Extract the package and open the `stopword.dic` dictionary file in the config folder.
3. Delete the tokens and save the dictionary file.
4. Change the name of the `stopword.dic` dictionary file to `SYSTEM_STOPWORD.dic`.
5. Upload the `SYSTEM_STOPWORD.dic` file to your Elasticsearch instance. The file automatically overwrites the current stopword list.
6. After the instance is restarted, the new stopword list takes effect.

5.3 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

Note:

- After you upload a custom plug-in, Elasticsearch must 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.
- Plug-ins are not upgraded with the cluster. To upgrade a 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 plug-ins in open source communities.

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.

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 is added.

Note:
You can add more custom plug-in files in the same way.

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

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

If you no longer need the plug-in, click Remove on the right side to remove the plug-in. For more information about how to install and remove a plug-in, see *Install and remove a built-in plug-in.*
6 Cluster monitoring

6.1 Cluster alerting

This topic describes the cluster alerting feature of Alibaba Cloud Elasticsearch. You can enable the alerting feature and customize alerts.

Enable alerting

1. Log on to the Alibaba Cloud Elasticsearch console.
2. On the Instances page, click Alarms.
3. In the Alarms message box, click Enable Now. By default, the alerting feature is disabled.

4. In the CloudMonitor console, click the Initiative Alarm switch for Elasticsearch.
5. After you enable alerting, click Refresh, and click Instance ID/Name > Cluster Monitoring. The Alarms feature in the Cluster Alarms section displays Enabled.

Customize alerts

On the Cluster Monitoring page, click Go to CloudMonitor in the Cluster Alarms section. You can then create alert rules in the CloudMonitor console. For more information, see #unique_6.

6.2 Cluster monitoring

This topic describes how to view the monitoring data of an Alibaba Cloud Elasticsearch cluster, and also describes the relevant monitor metrics in details.

View cluster monitoring data

1. Log on to the Alibaba Cloud Elasticsearch console.
2. Choose Instance ID/Name > Cluster Monitoring.
3. On the Cluster Monitoring page, select a time period under Cluster Monitoring to view detailed monitoring data generated within the specified time period.
4. Click the Custom icon, select a start date and end date, and then click OK to view the detailed monitoring data generated within the customized time period.

Notice:
You can query monitoring data generated in the last 30 days with a per minute granularity, or query monitoring data generated in seven days in a row.

For more information about the monitor metrics, see Monitor metrics.

Monitor metrics

Alibaba Cloud Elasticsearch cluster monitoring supports the following metrics: ClusterStatus, ClusterQueryQPS(Count/Second), ClusterIndexQPS(Count/Second).
Elasticsearch Instances / 6 Cluster monitoring

Second), NodeCPUUtilization(%, NodeHeapMemoryUtilization(%), NodeDiskUtilization(%), NodeLoad_1m, NodeStatsFullGcCollectionCount(unit), NodeStatsExceptionLogCount(unit), and ClusterAutoSnapshotLatestStatus.

ClusterStatus

The ClusterStatus metric indicates the status of an Elasticsearch cluster. The value 0.00 indicates that the cluster is in the Normal state. You must create an alert rule for this metric. For more information, see #unique_6/unique_6_Connect_42_section_fll_q1m_zgb.

If the value of the metric is not 0 (the color is not green), the cluster is not in the Normal state. The common causes are as follows:

- The CPU usage or heap memory usage of the nodes in the cluster is too high or reaches 100%.
- The disk usage of the nodes in the cluster is too high (such as a usage higher than 85%) or reaches 100%.
- The node workload within one minute (load_1m) is too high.
- The status of the indexes in the cluster is abnormal (the color is not green).

The metric values and their definitions are as follows.

<table>
<thead>
<tr>
<th>Value</th>
<th>Color</th>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.00</td>
<td>Red</td>
<td>Not all of the primary shards are available.</td>
<td>Some primary shards in the cluster are unavailable. This means that one or more indexes have unassigned primary shards.</td>
</tr>
<tr>
<td>1.00</td>
<td>Yellow</td>
<td>All primary shards are available. Not all of the replica shards are available.</td>
<td>This means that one or more indexes have unassigned replica shards.</td>
</tr>
<tr>
<td>0.00</td>
<td>Green</td>
<td>All primary and replica shards are available.</td>
<td>This means that all indexes in the cluster are healthy. No unassigned shard exists.</td>
</tr>
</tbody>
</table>

ClusterQueryQPS(Count/Second)

Notice:
When the cluster QPS spikes, the CPU usage, heap memory usage, or node workload within one minute may reach a high level. This may adversely affect your businesses running in the cluster. You must avoid this issue.

The ClusterQueryQPS(Count/Second) metric indicates the number of queries processed by the cluster per second.

The number of queries processed per second is affected by the number of primary shards of the index that is queried. For example, if an index has five primary shards, the cluster can process five queries addressed to this index per second.

ClusterIndexQPS(Count/Second)

Notice:
When the write QPS spikes, the CPU usage, heap memory usage, or node workload within one minute may reach a high level. This may adversely affect your businesses running in the cluster. You must avoid this issue.

The value of the ClusterIndexQPS(Count/Second) metric is calculated based on the number of write requests that a cluster receives per second and the number of documents that these requests write.

If a cluster receives only one write request in one second and the request only writes one document, the write QPS is 1. The value of the metric increases with the number of write requests received per second.

If the cluster receives a _bulk request that writes more than one document in one second, the value of the write QPS metric equals the number of the documents to be written. The value of the metric also increases with the number of _bulk requests received per second.

NodeCPUUtilization(%)

The NodeCPUUtilization(%) metric indicates the CPU usage of the nodes in a cluster. When the CPU usage is high or close to 100%, your businesses running in the cluster are adversely affected.

If the CPU usage spikes or vastly fluctuates and your businesses are affected, check for the following causes:

- The cluster QPS or write QPS spikes or vastly fluctuates.
- The cluster receives a few slow queries or slow write requests.

  In this case, you may not be able to find spikes or fluctuations in cluster QPS and write QPS. You can log on to the Elasticsearch console and go to the Logs page, and then click the Search Slow Log tab to analyze the log data.

- The cluster has a large amount of indexes or shards.

  Elasticsearch monitors indexes in the cluster and records index changes in the log. If the cluster has too many indexes or shards, the CPU usage, heap memory usage, or node workload within one minute may reach a high level.

- Merge operations are performed on the cluster.

  Merge operations consume CPU resources. Consequently, the number of segments on the corresponding node vastly drops down. You can check the number of segments on the Overview page of the node in the Kibana console.

- Garbage collection operations are performed on the cluster.

  Garbage collection operations, such as full garbage collection, will try to release memory resources. CPU resources are consumed during a garbage collection. Consequently, the CPU usage may spike.

- Schedule tasks, such as backup tasks or other customized tasks, are performed on the cluster.

NodeHeapMemoryUtilization(%)  

The NodeHeapMemoryUtilization(%) metric indicates the heap memory usage of the nodes in a cluster. If the heap memory usage is high or a large object is stored in the memory, your businesses running in the cluster are adversely affected. This also triggers a garbage collection.

If the heap memory usage spikes or vastly fluctuates and your businesses are affected, check for the following causes:

- The cluster QPS or write QPS spikes or vastly fluctuates.
- The cluster receives a few slow queries or slow write requests.

  In this case, you may not be able to find spikes or fluctuations in cluster QPS and write QPS. You can log on to the Elasticsearch console and go to the Logs page, and then click the Search Slow Log tab to analyze the log data.
• The cluster receives a large amount of slow queries or slow write requests.

In this case, you may find spikes or fluctuations in cluster QPS and write QPS. You can log on to the Elasticsearch console and go to the Logs page, and then click the Indexing Slow Log tab to analyze the log data.

• The cluster has a large amount of indexes or shards.

Elasticsearch monitors indexes in the cluster and records index changes in the log. If the cluster has too many indexes or shards, the CPU usage, heap memory usage, or node workload within one minute may reach a high level.

• Merge operations are performed on the cluster.

Merge operations consume CPU resources. Consequently, the number of segments on the corresponding node vastly drops down. You can check the number of segments on the Overview page of the node in the Kibana console.

• Garbage collection operations are performed on the cluster.

Garbage collection operations, such as full garbage collection, will try to release memory resources. CPU resources are consumed during a garbage collection. Consequently, the heap memory usage vastly drops down.

Garbage collection operations, such as full garbage collection, will try to release memory resources. CPU resources are consumed during a garbage collection. Consequently, the heap memory usage vastly drops down.

• Schedule tasks, such as backup tasks or other customized tasks, are performed on the cluster.

NodeDiskUtilization(%) metric indicates the disk usage of the nodes in a cluster. The disk usage must be controlled under 85%. We recommend that you configure an alert rule for this metric. Otherwise, your businesses running in the cluster may be adversely affected in the following situations:

• By default, if the disk usage of a data node exceeds 85%, new shards cannot be allocated to the data node. This may adversely affect your businesses.

• By default, if the disk usage of a data node exceeds 90%, Elasticsearch attempts to move the shards on this node to data nodes with low disk usage. This may adversely affect your businesses.
• By default, if the disk usage of a data node exceeds 95%, Elasticsearch adds the `read-only-allow-delete` attribute to all indexes in the cluster. This means that the indexes cannot be written. They can only be read or deleted. This may adversely affect your businesses.

Notice:
Do not set the alert threshold of the disk usage to a value higher than 80%. We recommend that you set the threshold to a value lower than 75%. In this way, when alerts are triggered, you can expand disks, add nodes, or clear index data to avoid your businesses being affected.

**NodeLoad_1m**

The `NodeLoad_1m` metric indicates the workload of a node within one minute. You can reference this metric to determine whether the node is busy. You must keep this value lower than the number of CPU cores of the node to guarantee that your businesses are running normally.

If this value exceeds the number of CPU cores of the node, your businesses are adversely affected. The common causes are as follows:

• The CPU usage or heap memory usage is high or reaches 100%.
• The cluster QPS or write QPS spikes or vastly fluctuates.
• Slow queries that need a large amount of time to process are received.

A few or a large amount of slow queries are received. Log on to the Elasticsearch console, go to the Logs page, and click the corresponding log tab to analyze the log data.

Taking a single-core node as an example, the values of this metric and their definitions are described as follows:

• Load < 1: No pending process exists.
• Load = 1: The system does not have additional resources to run more processes.
• Load > 1: Processes are queued up waiting for resources.

**NodeStatsFullGcCollectionCount(unit)**

Warning:
If full garbage collection is frequently triggered, your businesses running in the cluster are adversely affected.
The **NodeStatsFullGcCollectionCount(unit)** metric indicates the number of full garbage collection times triggered within one minute.

If this value is not 0, your businesses are affected. The common causes are as follows:

- The heap memory usage is high.
- Large objects are stored in memory.

**NodeStatsExceptionLogCount(unit)**

The **NodeStatsExceptionLogCount(unit)** metric indicates the number of warning-level entries generated in the instance log within one minute.

If this value is not 0, your businesses are affected. The common causes are as follows:

- Abnormal cluster queries are received.
- Abnormal write requests are received.
- Errors occur when the cluster runs tasks.
- A garbage collection is triggered.

**Note:**

- Log on to the Elasticsearch console, go to the Logs page, and click the Instance Log tab. On the Instance Log tab, look for exceptions occurred in the specific time and analyze the causes.
- The **NodeStatsExceptionLogCount(unit)** metric also counts the garbage collection times recorded in the Instance Log.

**ClusterAutoSnapshotLatestStatus**

The **ClusterAutoSnapshotLatestStatus** metric indicates the status of the auto snapshot feature of the cluster. If the value is -1 or 0, auto snapshot is running normally.

If the value is 2, an error has occurred to auto snapshot. The common causes are as follows:

- The disk usage of the nodes is high or close to 100%.
- The cluster is not in the Normal state.

The values of this metric and their definitions are as follows:
• 0: Snapshots are created.
• -1: No snapshot is created.
• 1: The system is creating a snapshot.
• 2: The system failed to create snapshots.
Elasticsearch

7 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.

You can query log entries generated in seven days in a row. By default, the log entries are displayed by time in descending order. The Lucene query syntax is supported. For more information, see Query string syntax.

Note:
Alibaba Cloud Elasticsearch can return up to 10,000 log entries upon each query. If the returned log entries do not contain the expected log data, you can specify a time range when you query the log data.

Examples

This example searches the Elasticsearch instance log. Log entries are returned if they meet all of these conditions: the content contains the health keyword, the level is info, and the host is 172.16.xx.xx.

1. Log on to the Alibaba Cloud Elasticsearch console and open the instance management page.
2. Choose Logs > Instance Log.
3. Enter the query string into the search box.

In this example, the query string is host:10.8.xx.xx AND content:health AND level:info.

Notice:
AND in the query string must be uppercase.

4. Select a start date and end date, and then click Search.

Notice:

- If you do not select an end date, the current system time is specified as the end date.
- If you do not select a start date, the start date is the time 1 hour earlier than the end time.

After you click Search, Elasticsearch returns the log entries that match your query string and displays them on the current page. The returned log data contains the following information: Time, Node IP, and Content.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time when the log entry was generated.</td>
</tr>
<tr>
<td>Node IP</td>
<td>The IP address of the node.</td>
</tr>
<tr>
<td>Content</td>
<td>The content of the log entry.</td>
</tr>
<tr>
<td>level</td>
<td>The level of the log entry. Log levels include trace, debug, info, warn, and error. The GC log does not contain the level field.</td>
</tr>
<tr>
<td>host</td>
<td>The IP address of the node.</td>
</tr>
</tbody>
</table>

Note:

To query the IP addresses of the nodes, log on to the Kibana console, open the Monitoring page, and click Nodes under Elasticsearch.
8 Security

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

*Go to the instance management page of your Elasticsearch instance, choose Security in the left-side navigation pane. You can perform the following tasks in the Network Settings section.*

- **Reset** Elasticsearch Instance Password.
- **Configure** VPC whitelist.
- **Enable** Public network access.
- **Configure** Public network whitelist.
- **Enable** HTTPS.

Reset the Elasticsearch instance password

**Notice:**

- If you are using the elastic account, after you reset the password, you must use the new password to log on to the Alibaba Cloud Elasticsearch instance or Kibana console.
- The password reset operation does not reset the passwords of the accounts other than the elastic account. We recommend that you do not use the elastic account to log on to your Elasticsearch instance.
- Click Reset, enter the new password, and confirm the operation. The system does not need to restart the instance for the new password to take effect.
On the Security page, click Reset on the right side of Elasticsearch Instance Password. Enter a new password for the elastic account, and click OK to reset the password.

Reset

⚠️ This information is required everytime you log on to Elasticsearch.

<table>
<thead>
<tr>
<th>Username:</th>
<th>elastic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
<td></td>
</tr>
<tr>
<td>0/30</td>
<td></td>
</tr>
<tr>
<td>Confirm Password:</td>
<td>The passwords must be match.</td>
</tr>
<tr>
<td>0/30</td>
<td></td>
</tr>
</tbody>
</table>

After you reset the password, it takes about five minutes for the new password to take effect.

VPC whitelist

When you need to connect to an Alibaba Cloud Elasticsearch instance through a VPC network, you must add the IP address of the client to the VPC whitelist of the Elasticsearch instance.

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

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.

Note:

- By default, all internal network IPv4 addresses are allowed to access Elasticsearch.
- The VPC whitelist is used to control access from internal network addresses in VPC networks.
- You can add up to 300 IP addresses or CIDR blocks to the VPC whitelist.
Public network access

Turn on the Public Network Access switch to enable public network access. After this feature is enabled, the switch displays green color. By default, the switch displays gray color, which means that public network access is disabled. To connect to your Alibaba Cloud Elasticsearch instance from the Internet, you must enable public network access for the instance.

Public network whitelist

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

To connect to your Alibaba Cloud Elasticsearch instance from 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, you can add IPv6 addresses and CIDR 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.

Note:
You can add up to 300 IP addresses or CIDR blocks to the public network whitelist.

Enable HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP. HTTPS uses Secure Socket Layer (SSL) to guarantee the security of 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.
1. Log on to the Alibaba Cloud Elasticsearch console, click Instance ID/Name > Security, and turn on the HTTPS switch.

Notice:

- After you enable HTTPS, you must use an HTTPS client to connect to the Elasticsearch instance. You cannot use an HTTP client to connect to the instance. For more information, see HTTP and HTTPS client sample code.
- To enable or disable HTTPS, the system must restart the instance. During the restart process, your workloads on the instance will be interrupted. Before you enable or disable HTTPS, make sure that your workloads are not adversely affected.
2. On the Confirm Operation message, select the I have created an HTTPS client check box, and then click OK.

Note:
If you have not purchased client nodes, after you turn on the HTTPS switch, the system prompts a message asking you to purchase client nodes. You can follow the instructions to purchase client nodes.

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

HTTP and HTTPS client sample code

Taking the official Elasticsearch REST client as an example, the sample code for creating an HTTP client and an HTTPS client is as follows. If HTTPS is disabled for your Elasticsearch instance, use an HTTP client. If HTTPS is enabled for your Elasticsearch instance, use an HTTPS client.

- Sample code for creating an HTTP client:

```java
final CredentialsProvider credentialsProvider = new BasicCredentialsProvider();
credentialsProvider.setCredentials(AuthScope.ANY, new UsernamePasswordCredentials("elastic", "Your password");
RestClientBuilder restClientBuilder = RestClient.builder(
    new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com", 9200));
RestClient restClient = restClientBuilder.setHttpClientConfigCallback(
    new RestClientBuilder.HttpClientConfigCallback() {
      @Override
      public HttpAsyncClientConfig build(HttpAsyncClientConfigBuilder configuredClient) {
        return configuredClient.setDefaultProxy(ServiceUtil.getProxy());
      }
    });
```
public HttpAsyncClientBuilder customizeHttpClient(HttpAsyncClientBuilder httpClientBuilder) {
    return httpClientBuilder.setDefaultCredentialsProvider(credentialsProvider);
}
}

Sample code for creating an HTTPS client:

```java
final CredentialsProvider credentialsProvider = new BasicCredentialsProvider();
credentialsProvider.setCredentials(AuthScope.ANY, new UsernamePasswordCredentials("elastic", "Your password"));
RestClientBuilder restClientBuilder = RestClient.builder(new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com", 9200, "https"));
RestClient restClient = restClientBuilder.setHttpClientConfigCallback(
    new RestClientBuilder.HttpClientConfigCallback() {
        @Override
        public HttpAsyncClientBuilder customizeHttpClient(HttpAsyncClientBuilder httpClientBuilder) {
            return httpClientBuilder.setDefaultCredentialsProvider(credentialsProvider);
        }
    }).build();
```

As shown in the preceding example, after you enable HTTPS, you must include the `https` parameter in `HttpHost`:

```java
new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com", 9200, "https"));
```

Interconnect Elasticsearch instances

You can interconnect Elasticsearch instances to support cross-cluster search. For more information, see Interconnect two Elasticsearch instances.
9 Interconnect two Elasticsearch instances

To guarantee data security, Alibaba Cloud Elasticsearch instances are isolated from each other by default. If you want to search data across two Elasticsearch instances, you must interconnect the Elasticsearch instances.

Prerequisites
Before you interconnect two Elasticsearch instances, make sure that the following requirements are met:

- Both instances are using the same Elasticsearch version.
- Both instances are created by the same user account.
- Both instances are deployed in the same VPC network.
- Both instances are deployed in one zone or deployed across multiple zones.

Context
After the preceding requirements are met, log on to the Elasticsearch console and go to the Instance Interconnection page to configure the corresponding settings.

For more information, see Configure instance interconnection.

Configure instance interconnection

2. Click Edit on the right side of Instance Interconnection.
3. In the Edit Configuration dialog box, click Add Instance.
4. In the Add Instance dialog box, select the ID of the instance to which you need to connect the current instance, and click OK.

Notice:

- If you are using a RAM user account, the RAM user account must have the List permission to obtain all instances under the corresponding Alibaba Cloud account.
- After the prerequisites are met, you can select one or more instances in the Add Instance dialog box.
After you connect Instance A to Instance B, you can find the ID of Instance A on the Instance Interconnection page of Instance B. This means that the communication between Instance A and Instance B is bidirectional.

After you add an instance, you can find the added instance in the Interconnected Instances list in the Edit Configuration dialog box.

Remove an interconnected instance

2. Click Edit on the right side of Instance Interconnection.
3. In the Edit Configuration dialog box, click Remove in the Actions column of the Interconnected Instances list.

![Edit Configuration dialog box](image)

4. In the Remove Instance message, click OK to disconnect the instance.
   After you click OK, the instance is removed from the Interconnected Instances list in the Edit Configuration dialog box.

Query interconnected instances

2. Click Edit on the right side of Instance Interconnection.
3. You can view the interconnected instances in the Interconnected Instances list in the Edit Configuration dialog box.

Notice:
When you delete an instance that is interconnected to another instance, the
The instance is already connected to an instance. If you delete the instance,
the interconnection is removed. Are you sure you want to delete the instance?
message is displayed for you to confirm the operation.

Configure cross-cluster search

1. Log on to the Kibana console of the Elasticsearch instance that is interconnected to the current instance.

2. Send the following request to create an index and add a document to the index.

```
PUT /twitter
{
  "settings": {
    "index": {
      "number_of_shards": 3,
      "number_of_replicas": 2
    }
  }
}

POST twitter/doc/
{
  "user": "kimchy",
```
3. **Log on to the Kibana console of the current Elasticsearch instance.**

4. Use one of the following methods to configure cross-cluster search on the current Elasticsearch instance.

In the following methods, Elasticsearch V6.7 is used. The methods used to configure cross-cluster search in other Elasticsearch versions are similar. For more information, see [Configure cross-cluster search in Elasticsearch V6.7](#), [Configure cross-cluster search in Elasticsearch V6.3](#), and [Configure cross-cluster search in Elasticsearch V5.5](#).

- **Method 1:** configure cross-cluster search by using the internal network endpoint of the remote Elasticsearch instance.

```json
PUT _cluster/settings
{
  "persistent": {
    "cluster": {
      "remote": {
        "cluster_one": {
          "seeds": [
            "es-cn-o4xxxxxxxxxxxx4f1.elasticsearch.aliyuncs.com:9300"
          ]
        }
      }
    }
  }
}
```

- **Method 2:** configure cross-cluster search by using the IP addresses of the nodes in the remote Elasticsearch instance.

```json
PUT _cluster/settings
{
  "persistent": {
    "cluster": {
      "remote": {
        "cluster_one": {
          "seeds": [
            "10.8.xx.xx:9300",
            "10.8.xx.xx:9300",
            "10.8.xx.xx:9300"
          ]
        }
      }
    }
  }
}
```
Notice:

- If the current instance is deployed in one zone, you can use method 1 or method 2 to configure cross-cluster search. More than one instance can be connected to the current instance.

- If the current instance is deployed across multiple zones, you can only use method 2 to configure cross-cluster search. More than one instance can be connected to the current instance.

- If you log on to Instance A and specify Instance B as the remote instance, you can search indexes on Instance B from Instance A. However, you cannot search indexes on Instance A from Instance B. To search indexes on Instance A from Instance B, you must log on to Instance B and specify the endpoint or node IP addresses of Instance A.

5. Send the following request to verify that the cross-cluster search feature runs normally.

```
POST /cluster_one:twitter/doc/_search
{
  "query": {
    "match_all": {}
  }
}
```

If the cross-cluster search feature runs normally, the following result is returned.

```
{
  "took" : 78,
  "timed_out" : false,
  "_shards" : {
    "total" : 3,
    "successful" : 3,
    "skipped" : 0,
    "failed" : 0
  },
  "_clusters" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0
  },
  "hits" : {
    "total" : 1,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "cluster_one:twitter",
        "_type" : "doc",
        "id" : "5c0b5a07ac76b0528f251b03",
        "_score" : 1.0,
        "_source" : {
          "index" : "cluster_one:twitter",
          "docid" : "5c0b5a07ac76b0528f251b03",
          "name" : "Instance B"
        }
      }
    ]
  }
}
```
"_id" : "qudxxxxxxxxxx_7ie6J",
"_score" : 1.0,
"_source" : {
   "user" : "kimchy",
   "post_date" : "2009-11-15T14:12:12",
   "message" : "trying out Elasticsearch"
}
}
10 Data backup

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Snapshot</td>
<td>When the Auto Snapshot switch is in the green color, auto snapshot is enabled. By default, auto snapshot is disabled.</td>
</tr>
<tr>
<td>Auto Snapshot Period</td>
<td>If auto snapshot is disabled, the You must enable auto snapshot first message is displayed.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Configuration</td>
<td>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.</td>
</tr>
</tbody>
</table>

![Auto Snapshot Configuration](image)

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.

<table>
<thead>
<tr>
<th>Restore from Snapshot</th>
<th>Click View Tutorial to learn how to restore data from a snapshot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Status</td>
<td>Click View Tutorial to learn more information about snapshot status.</td>
</tr>
</tbody>
</table>

10.2 Auto snapshot guide

This topic describes the auto snapshot and auto restore features of Alibaba Cloud Elasticsearch. After you enable auto snapshot, you can specify the snapshot creation time. Snapshots are automatically created to ensure data security.

Enable auto snapshot

1. Go to the instance management page of your Elasticsearch instance.
2. In the left-side navigation pane, click Snapshots.

3. On the Snapshots page, click the Auto Snapshot switch to enable the feature.

4. Click Edit Configuration on the right side, select a time to create snapshots daily, and click Save. A snapshot is then created at the specified time.

Auto restore

If you have enabled auto snapshot for your Alibaba Cloud Elasticsearch instance, the system automatically creates a snapshot for the instance daily. You can call the snapshot operation to restore data in a snapshot to the Elasticsearch instance where the snapshot is created.

Note:

- The first snapshot is a complete backup created on the Alibaba Cloud Elasticsearch instance. The subsequent snapshots are created based on the incremental
data of the Elasticsearch instance. Therefore, it takes more time to create the first snapshot, but less time to create subsequent snapshots.

- A snapshot does not store monitoring data generated by an Alibaba Cloud Elasticsearch instance, such as the indexes starting with `.monitoring` and `.security_audit`.
- An automatically created snapshot can only be restored to the Alibaba Cloud Elasticsearch instance where the snapshot is created.
- A snapshot repository is created when the first snapshot is created.

Query all repositories

*Log on to the Kibana console, and call the GET _snapshot operation to query all repositories.*

The following result is returned:

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

- **aliyun_auto_snapshot**: the name of the repository.
- **type**: the storage where the snapshots are stored. In this example, Alibaba Cloud Object Storage Service (OSS) is used.
- **compress:true**: enables compression of the metadata files of the indexes during snapshot creation.
- **base_path**: the location of the snapshots.
- **endpoint**: the endpoint of the OSS bucket.

Query all snapshots

*The following example shows how to call the GET _snapshot/aliyun_auto_snapshot/_all operation to query all snapshots in the aliyun_auto_snapshot repository.*

The following result is returned:

```
{
   "snapshots": [
```

Default parameters

The auto snapshot feature also supports the following default parameters that are not displayed:

- **max_snapshot_bytes_per_sec**: throttles per node snapshot rate. The default snapshot rate is 40 MB per second.
- **max_restore_bytes_per_sec**: 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 index data from a snapshot

You can call the _restore operation to restore index data from a snapshot.

- Call the following operation to restore all indexes from a specified snapshot stored in the aliyun_auto_snapshot repository. The restore task is executed in the background.

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

  `<snapshot>`: replace it with the name of the specified snapshot, for example, `es-cn-abcd...`
• Call the following operation to restore all indexes from the specified snapshot stored in the aliyun_auto_snapshot repository, and receive a response after the restore task is completed.

The _restore operation runs restore tasks asynchronously. The Alibaba Cloud Elasticsearch instance will return a response immediately if the restore operation is executable. Restore tasks are executed in the background. You can set the wait_for_completion parameter. 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, for example, es-cn-abcdefghijklmn_20180627091600.

• Call the following operation to restore the specified indexes from a specific snapshot stored in the aliyun_auto_snapshot repository, and rename the restored indexes. The restore task is 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, for example, es-cn-abcdefghijklmn_20180627091600.
- `indices`: specifies the indexes that you want to restore.
- `rename_pattern`: specifies a regular expression to match the restored indexes by name. This parameter is optional.
- `rename_replacement`: specifies a regular expression to rename the matching indexes. This parameter is optional.
10.3 View snapshot status

This topic describes how to query the status of snapshots automatically created on your Alibaba Cloud Elasticsearch instance to help you check the snapshot creation progress.

*Enable auto snapshot, and log on to the Kibana console.* Choose Dev Tools in the left-side navigation pane. On the Console tab, call the snapshot operation to query the status of the automatically created snapshots.

Query all snapshots

You can send the following request to query information about all snapshots stored in the `aliyun_auto_snapshot` repository.

```
GET _snapshot/aliyun_auto_snapshot/_all
```

The following result is returned:

```
{
    "snapshots": [
        {
            "snapshot": "es-cn-abxxxxxxxxxlmn_20180628092236",
            "uuid": "n7YxxxxxxxxxxxxdA",
            "version_id": 5050399,
            "version": "5.5.3",
            "indices": [".kibana"],
            "state": "SUCCESS",
            "start_time_in_millis": 1530148959609,
            "end_time": "2018-06-28T01:22:39.923Z",
            "end_time_in_millis": 1530148959923,
            "duration_in_millis": 314,
            "failures": [],
            "shards": {
                "total": 1,
                "failed": 0,
                "successful": 1
            }
        },
        {
            "snapshot": "es-cn-abxxxxxxxxxmn_20180628092500",
            "uuid": "frdxxxxxxxxxxxxKLA",
            "version_id": 5050399,
            "version": "5.5.3",
            "indices": [".kibana"],
            "state": "SUCCESS",
            "start_time": "2018-06-28T01:25:00.764Z",
            "start_time_in_millis": 1530148950764,
            "end_time": "2018-06-28T01:25:01.482Z",
            "end_time_in_millis": 1530148951482,
        }
    ]
}
```


```
"duration_in_millis": 718,
"failures": [],
"shards": {
  "total": 1,
  "failed": 0,
  "successful": 1
}
]
```

**state:** indicates the status of the snapshot. A snapshot can be in one of the following states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN_PROGRESS</td>
<td>The snapshot is being restored.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>The snapshot has been restored and all shards have been successfully stored.</td>
</tr>
<tr>
<td>FAILED</td>
<td>The snapshot has been restored with an error. Some data cannot be stored.</td>
</tr>
<tr>
<td>PARTIAL</td>
<td>The cluster data is stored, but at least one shard fails to be stored.</td>
</tr>
<tr>
<td>INCOMPATIBLE</td>
<td>The snapshot version is incompatible with the current instance version.</td>
</tr>
</tbody>
</table>

**Query a specified snapshot**

You can send the following request to query information about a specified snapshot stored in the repository `aliyun_auto_snapshot`.

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

where `<snapshot>`: replace it with the name of the snapshot, for example, `es-cn-abxxxxxxxxxxxxlmn_20180628092236`. You can call the `Query all snapshots` operation to query the name of a snapshot.

The following result is returned:

```
{
  "snapshots": [
  {
    "snapshot": "es-cn-abxxxxxxxxxxxxlmn_20180628092236",
    "repository": "aliyun_auto_snapshot",
    "uuid": "n7YxxxxxxxxxxxxxydA",
    "state": "SUCCESS",
    "shards_stats": {
      "initializing": 0,
      "started": 0,
      "finalizing": 0,
      "total": 1,
      "failed": 0,
      "successful": 1
    }
  }
```

```
10.4 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 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 a repository

```
PUT _snapshot/my_backup
{
    "type": "oss",
    "settings": {
        "endpoint": "http://oss-cn-hangzhou-internal.aliyuncs.com",
        "access_key_id": "xxxx",
        "secret_access_key": "xxxxxx",
        "bucket": "xxxxxx"
    }
}
```
Elasticsearch
Instances / 10 Data backup

```

"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_47.
- <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_access_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_completion` parameter as follows:

```
PUT _snapshot/my_backup/snapshot_1? wait_for_completion=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_2014_28_10",
      "index1",
      "index2"
    ],
    "state": "SUCCESS",
    "start_time": "2014-09-02T13:01:43.115Z",
    "start_time_in_millis": 1409662903115,
    "end_time": "2014-09-02T13:01:43.439Z",
    "end_time_in_millis": 1409662903439,
    "duration_in_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
```
• 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_completion 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_PROGRESS",
         "shards_stats": {
            "initializing": 0,
            "started": 1,
            "finalizing": 0,
            "done": 4,
            "failed": 0,
            "total": 5
         }
      }
   ]
}
```
"stats": {
  "number_of_files": 5,
  "processed_files": 5,
  "total_size_in_bytes": 1792,
  "processed_size_in_bytes": 1792,
  "start_time_in_millis": 1409663054859,
  "time_in_millis": 64
},
"indices": {
  "index_3": {
    "shards_stats": {
      "initializing": 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_bytes": 1792,
      "start_time_in_millis": 1409663054859,
      "time_in_millis": 64
    },
    "shards": {
      "0": {
        "stage": "DONE",
        "stats": {
          "number_of_files": 1,
          "processed_files": 1,
          "total_size_in_bytes": 514,
          "processed_size_in_bytes": 514,
          "start_time_in_millis": 1409663054862,
          "time_in_millis": 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_pattern": "index_(.+)",  \<2\>
  "rename_replacement": "restored_index_$1"  \<3\>
}
```

In this example, the `index_1` index is restored to your Elasticsearch cluster and renamed as `restored_index_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_completion parameter as follows:**

```
POST /_snapshot/my_backup/snapshot_1/_restore? wait_for_completion=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_completion` 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_index_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:

```json
{
  "restored_index_3" : {
    "shards" : [ {
      "id" : 0,
      "type" : "snapshot", <1>
      "stage" : "index",
      "primary" : true,
      "stop_time" : 0,
      "total_time_in_millis" : 175576,
      "source" : { <2>
        "repository" : "my_backup",
        "snapshot" : "snapshot_3",
        "index" : "restored_index_3"
      },
      "target" : {
        "id" : "ryqJ5l05S4-lSFbGntkEkg",
        "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
      }
    }
  }
}
```
- <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.

10.5 Shared OSS repositories

Alibaba Cloud Elasticsearch (ES) provides shared OSS repositories to help you restore data across Elasticsearch instances.

Context

You can restore an automatically created snapshot in a shared OSS repository of an Elasticsearch instance to another Elasticsearch instance.
For example, you have created two Elasticsearch V6.7.0 instances. Their instance IDs are es-cn-a and es-cn-b. The instance es-cn-a has enabled auto snapshot and automatically created a snapshot. If you want to restore the snapshot of the instance es-cn-a to instance es-cn-b, you must use shared OSS repositories.

Compatibility

- To use shared OSS repositories to restore a snapshot created on an Elasticsearch instance to another Elasticsearch instance, you must make sure that both instances are created by the same user account and deployed in the same region.
- In the case of two Elasticsearch instances using two different Elasticsearch versions, the later version can use the repository of the earlier version. The earlier version cannot use the repository of the later version.

⚠️ Notice:
When the later version uses the repository of the earlier version, it may not support the data format of the earlier version. For example, you can restore indexes that contain only one document type from an Elasticsearch V5.5.3 instance to an Elasticsearch V6.7.0 instance. However, if you restore indexes that contain multiple document types from the Elasticsearch V5.5.3 instance to the Elasticsearch V6.7.0 instance, a restore error may occur. This is because Elasticsearch V6.7.0 does not support indexes that contain multiple document types. Therefore, we recommend that you run a test before you restore the data.

Add a shared OSS repository

1. Log on to the Alibaba Cloud Elasticsearch console, and select Instance ID/Name > Snapshots.
2. In the Shared OSS Repositories section, click Add Now.
3. In the Add Shared Repository dialog box, select an Elasticsearch instance. The system then creates a shared repository for the instance.

![Add Shared Repository](image)

**Notice:**

The selected instance version must be compatible with the current instance version. For more information, see [Compatibility](#).

4. Click OK.

After the shared repository is added, the current page shows the instance that owns the repository and the repository status.

![Repository Status](image)

**Notice:**

- A shared repository has two states: Active and Inactive. The Active state indicates that the repository is available. The Inactive state indicates that the specified instance or repository does not exist.
- The system uses your Elasticsearch instance to retrieve the repository list. If the instance is updating its configuration, the instance is not in the Normal state, or the workload of the instance is high, the system may fail to retrieve the repository list. If this error occurs, you can log on to the Kibana console, and send a `GET _snapshot` request to retrieve the endpoints of all repositories.
Restore an index

A shared OSS repository is only used to share data between two Elasticsearch instances. It cannot help you restore data. If you need to restore index data, send the corresponding API requests from the Kibana console.

For example, send the following request from the Kibana console to restore the index file-2019-08-25 from the instance es-cn-a.

1. Query information about all snapshots in the repository.

   GET /_cat/snapshots/aliyun_auto_snapshot_from_a? v

   The request returns information about all snapshots in the repository.

2. According to the returned snapshot information, restore indexes in the snapshot.

   Notice:
   Before you restore an index, you must make sure that the node to which the index is restored does not have an index with the same name. If the node has an index with the same name, make sure that the index status is close. If the status of the index is open, an error occurs when you restore the index to the node.

   POST _snapshot/aliyun_snapshot_from_es-cn-a/es-cn-a_20190705220000/_restore
   {"indices": "file-2019-08-25"}

   POST _snapshot/aliyun_snapshot_from_es-cn-a/es-cn-a_20190705220000/_restore
   {"indices": "kibana_sample_data_ecommerce,kibana_sample_data_logs"}
11 Data visualization

11.1 Kibana

11.1.1 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 1 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 Public network access is Enabled.

Context

Alibaba Cloud Elasticsearch provides the Kibana console for you to scale your workloads. 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 select Instance ID > Plug-ins.
2. On the Data Visualization page, click Console under Kibana.
3. Enter the username and password on the logon page, and then click Log in.

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

The following figure shows the Kibana console logged on from an Alibaba Cloud Elasticsearch V6.7 instance. If you use other Elasticsearch versions, the actual console may look slightly different from the one in the figure.
What's next

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

11.1.2 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 click *Instance ID/Name > Data Visualization*.

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

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.

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](image)

**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, *Log on to the Kibana console* and verify that the console is switched to the selected language.
11.1.3 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.

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.

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.

### 11.1.4 Plug-ins

Based on the plug-ins in open source communities, Alibaba Cloud Kibana provides a variety of plug-ins. This topic introduces Kibana custom plug-ins, and describes how to install and remove custom plug-ins, and the relevant considerations.

**Custom plug-ins**

**BSearch-QueryBuilder plug-in.**

BSearch-QueryBuilder is an advanced query plug-in developed by Alibaba Cloud, as well as a frontend plug-in. It supports the following features:

- **Easy to learn:** BSearch-QueryBuilder is a UI component, allowing you to create Elasticsearch DSL queries by clicking and selecting. You can customize search conditions without coding. This saves the costs of learning complicated 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 audited by Alibaba Cloud Security.

Note:
BSearch-QueryBuilder only supports Alibaba Cloud Elasticsearch V6.3 and V6.7. Alibaba Cloud Elasticsearch V5.5.3 is not supported.

Install the plug-in

Notice:
After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch provides you a free Kibana node with 1 core and 2 GB of memory. The plug-in consumes many resources. Before you install the plug-in, you must upgrade the Kibana node to 2 core 4 GB or higher. For more information, see Cluster upgrade.

1. Log on to the Alibaba Cloud Elasticsearch console, and purchase an Elasticsearch instance.
2. Click Instance ID/Name > Data Visualization.
3. In the Kibana section, click Edit Configuration.
4. In the Plug-ins section of the Kibana Configuration page, click Install in the Actions column.

Notice:

- After you confirm to install the plug-in, the Kibana node is restarted. During the restart process, Kibana cannot provide services normally. Make sure that the restart process does not affect your operations on Kibana before you confirm the operation.
- If the specification of your Kibana node is lower than 2 core 4 GB, the system prompts a message asking you to upgrade the node. Follow the instructions to upgrade your Kibana node to 2 core 4 GB or higher.

5. Confirm the operation and wait for the system to restart the Kibana node.

After the Kibana node is restarted, the plug-in is installed. The status of the plug-in displays Installed.

Note:
The restart process may be time-consuming.

Remove the plug-in

1. The procedure is similar as Install the plug-in. In the Plug-ins section of the Kibana Configuration page, click Remove in the Actions column.

Notice:
After you confirm to remove the plug-in, the Kibana node is restarted. During the restart process, Kibana cannot provide services normally. Make sure that the restart process does not affect your operations on Kibana before you confirm the operation.
2. Confirm the operation and wait for the system to restart the Kibana node.

After the Kibana node is restarted, the plug-in is removed. The status of the plug-in displays Not Installed.

11.1.5 BSearch-QueryBuilder plug-in

BSearch-QueryBuilder is an advanced query plug-in, as well as a frontend plug-in. With the BSearch-QueryBuilder plug-in, you no longer need to write complicated domain-specific language (DSL) statements for data query. It allows you to create complicated queries in a visualized manner. This topic describes how to use the BSearch-QueryBuilder plug-in to query data.

Features

BSearch-QueryBuilder supports the following features:

- Easy to learn: BSearch-QueryBuilder is a UI component, allowing you to create Elasticsearch DSL queries by clicking and selecting. You can customize search conditions without coding. This saves the costs of learning complicated 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 audited by Alibaba Cloud Security.

Background

Query DSL 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, Query DSL 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 combine any query expression
and filter supported by Elasticsearch to create a complicated query 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.

Preparations

Before you use the BSearch-QueryBuilder plug-in, you must purchase an Elasticsearch
instance. The version of the instance must be V6.3 or V6.7. Elasticsearch V5.5.3 is not
supported.
You can also use an existing instance. If the instance version does not meet the requirements, upgrade the instance.

Install BSearch-QueryBuilder

Notice:
After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch provides you a free Kibana node with 1 core and 2 GB of memory. The plug-in consumes many resources. Before you install the plug-in, you must upgrade the Kibana node to 2 core 4 GB or higher. For more information, see Cluster upgrade.

1. Log on to the Alibaba Cloud Elasticsearch console, and purchase an Elasticsearch instance.
2. Click Instance ID/Name > Data Visualization.
3. In the Kibana section, click Edit Configuration.

4. In the Plug-ins section of the Kibana Configuration page, click Install in the Actions column.

**Notice:**

- After you confirm to install the plug-in, the Kibana node is restarted. During the restart process, Kibana cannot provide services normally. Make sure that the restart process does not affect your operations on Kibana before you confirm the operation.

- If the specification of your Kibana node is lower than 2 core 4 GB, the system prompts a message asking you to upgrade the node. Follow the instructions to upgrade your Kibana node to 2 core 4 GB or higher.
5. Confirm the operation and wait for the system to restart the Kibana node.

After the Kibana node is restarted, the plug-in is installed. The status of the plug-in displays Installed.

![Kibana Configuration](image)

**Note:**
The restart process may be time-consuming.

Use BSearch-QueryBuilder

1. Return to the Data Visualization page of the Elasticsearch instance, click Console in the Kibana section.

2. Enter the username and password of the Kibana console, and click Log in.

   The default username is elastic. Enter the password specified when you create the instance.

3. In the Kibana console, choose Discover > Query.

**Notice:**
Before you create a query, make sure that you have created an index pattern. To create an index pattern in the Kibana console, click Management, choose Index Patterns > Create index pattern under Kibana, and follow the instructions to create the 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.

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

For more information about how to create a query, 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.

The following figure shows the returned result.

• 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. The
type filters are set to Undergraduate teaching materials, Math, Foreign language teaching, and Undergraduate textbooks.

The following figure shows the returned result.

- 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 within the specified time range are returned. The specified time
range is: [Current time - 240 days, Current time].

The following figure shows the returned result.

With all these search conditions and filters, you can define a complicated query as follows.
The actual DSL statement for the query is as follows.
As shown in the preceding examples, BSearch-QueryBuilder significantly simplifies the complexity of Elasticsearch queries.
11.1.6 BSearch-Label plug-in

BSearch-Label is a frontend data labeling plug-in. BSearch-Label supports visualized data labeling, saving you the need to write complicated domain-specific language (DSL) statements. This topic describes how to use the BSearch-Label plug-in to label data.

Background

In most cases, when you analyze data, you want to use query strings to filter the data rather than directly go through the data. You want to add tags to existing fields (or new fields) to classify them. This procedure is known as data labeling. After you add tags to the data, you can use the tags to aggregate and classify the data, and then perform statistical analysis. You can also filter data by tag. The labeled data can be consumed in subsequent procedures.

Install the BSearch-Label plug-in

Notice:
After you purchase an Alibaba Cloud Elasticsearch instance, Elasticsearch provides you a free Kibana node with 1 core and 2 GB of memory. The plug-in consumes many resources. Before you install the plug-in, you must upgrade the Kibana node to 2 core 4 GB or higher. For more information, see Cluster upgrade.

1. Log on to the Alibaba Cloud Elasticsearch console, and purchase an Elasticsearch instance.
2. Click Instance ID/Name > Data Visualization.
3. In the Kibana section, click Edit Configuration.

4. In the Plug-ins section of the Kibana Configuration page, click Install in the Actions column.

Notice:

- After you confirm to install the plug-in, the Kibana node is restarted. During the restart process, Kibana cannot provide services normally. Make sure that the restart process does not affect your operations on Kibana before you confirm the operation.

- If the specification of your Kibana node is lower than 2 core 4 GB, the system prompts a message asking you to upgrade the node. Follow the instructions to upgrade your Kibana node to 2 core 4 GB or higher.
5. Confirm the operation and wait for the system to restart the Kibana node.

After the Kibana node is restarted, the plug-in is installed. The status of the plug-in displays Installed.

![Kibana Configuration](image)

**Note:**
The restart process may be time-consuming.

Use the BSearch-Label plug-in

1. Return to the Data Visualization page of the Elasticsearch instance, click Console in the Kibana section.

2. Enter the username and password of the Kibana console, and click Log in.

   The default username is elastic. Enter the password specified when you create the instance.

3. Log on to the Kibana console, and choose Discover > Label.

**Notice:**
Before you create a query, make sure that you have created an index pattern. To create an index pattern in the Kibana console, click Management, choose Index Patterns > Create index pattern under Kibana, and follow the instructions to create the index pattern.
4. Select one of the following methods to label the data.

- Add a tag to an existing field.

As shown in the following example, find the record of user zhangsan, select the age field, add tag 18 to the field, and click make tag.

![Image of Kibana interface showing tagging a field](image1)

Click the History switch to view detailed labeling history.

![Image of Kibana interface showing tagging history](image2)

- Add a tag to a new field.

As shown in the following example, find the record of user zhangsan, select the custom marking field option, add field tag, add tag teenager to this field, and then click make tag.

![Image of Kibana interface showing tagging a new field](image3)

View the labeling result.