

Elasticsearch

FAQ

FAQ

Classic network errors

Access to a VPC from a classic network

To ensure network security, Alibaba Cloud Elasticsearch is deployed in virtual private clouds (VPCs) of users. If your business systems are deployed in a classic network, you can use ClassicLink provided in your VPC to access Elasticsearch from the classic network.

What is ClassicLink?

ClassicLink is a network channel provided by Alibaba Cloud VPCs to allow access from a classic network.

Note:

One classic network instance can be linked to only one VPC.

- A VPC on network segment 172.16.0.0/12 is accessible through ClassicLink by default.
- If the VPC is on network segment 10.0.0.0/8, the switches between ClassicLink and the ECS instance in the classic network must be on network segment 10.111.0.0/16.
- If the VPC is on network segment 192.168.0.0/16, you must submit a ticket to the ECS product line to activate the ClassicLink service. In addition, add a route from 192.168.0.0/16 to the private NIC in the classic network instance. Add the route using the official [script](#).

Create a ClassicLink connection to a VPC

In the VPC console, select the VPC you want to access using an ECS instance in the classic network, and enable ClassicLink for the VPC.

We recommend that you enable ClassicLink for a VPC on network segment 172.16.0.0/12.

Select a VPC from the VPC list and click **Manage** to open the VPC management page.

Click **Enable ClassicLink** on the upper right corner of the VPC management page to enable this function for the VPC.

In the ECS console, select the region where the ClassicLink-enabled VPC is located, for example, China East 1 (Hangzhou). Select a classic network instance in this region, and you can see the option of **Connect to VPC** in the **More** drop-down link box.

Select **the option of Connect to VPC**, and then select the ClassicLink-enabled VPC in the dialog box that is displayed.

After you select the VPC, the VPC name displayed in the dialog box is tagged by a ClassicLink icon. If this icon is green, ClassicLink is enabled for the selected VPC. If this icon is yellow, ClassicLink is not enabled for the VPC.

Click **OK**, A connection from the classic network instance to the VPC is created.

Click the link in the dialog box to set a ClassicLink security group rule.

On the security group setting page, click the button on the upper right corner to add a ClassicLink security group rule.

In the dialog box that is displayed, set the security group rule, which is the authorization mode used between a Classic network security group and a VPC security group. A classic network security group allows access to five VPC security groups. Three authorization modes are supported, among which bidirectional access between the classic network and VPC is recommended. Choose unidirectional or bidirectional access based on your business requirements.

After setting the security group rule, open the details page to check whether the setting is correct. If the security group rule is not set correctly, delete it and set a new one. If the security group is set correctly, verify the connectivity.

Verify connectivity between the classic network and VPC

The ECS console provides a custom item list. If the link status of the classic network instance is not displayed on the instance list on the console, select **Link Status** from the custom item list. Then, the link status of the classic network instance can be seen on the page.

Log on to the ECS instance connected through ClassicLink, and access the Alibaba Cloud Elasticsearch instance in the VPC using the curl command to verify the connectivity.

Kibana console password

What is the password of Alibaba Cloud Elasticsearch Kibana console used for?

- The elastic account is the root account that gives you access to the Alibaba Cloud Elasticsearch service. This account has the maximum permissions of cluster management, so keep the root account information safe.
- If you use an API or SDK to access the Alibaba Cloud Elasticsearch instance, verify your privilege using elastic/your_password. If no password is set, initialize the password in the console.
- If you use the Kibana service to access the Alibaba Cloud Elasticsearch instance, verify your privilege using elastic/your_password. If no password is set, initialize the password in the console.

Permission management in Kibana

How to effectively manage user permissions in Elasticsearch Kibana?

- We recommend that you create users and assign roles to them using the Kibana service of your Elasticsearch instance, instead of using the root account directly for instance operations. To create a user, see [Kibana User Guide](#).
- We recommend that you do not use the root account elastic for the search service, because exposure of its password may bring security risks to your service cluster.
- Exercise caution when changing the password of the root account elastic if this account is used to provide the search service. After the password of the Alibaba Cloud Elasticsearch instance is reset, the search service becomes unavailable due to authorization failure.