Server Load Balancer

User Guide

MORE THAN JUST CLOUD | Alibaba Cloud

User Guide

Preparation

Registration

A registered Alibaba Cloud account is required. If you do not have an Alibaba Cloud account, register in Account Registration.

Prepare backend ECS servers

Before using the Server Load Balancer service, ensure that you have created the backend ECS servers.

If you are a new user to Alibaba Cloud ECS, refer to Quick Start (Applicable to Linux Instances) or Quick Start (Applicable to Windows Instances) to purchase the service based on your operating needs.

Instance management

Create Server Load Balancer instances

A Server Load Balancer instance can:

- Flexibly distribute traffic, which is suitable for businesses with high access volumes.
- Horizontally scale application system service capabilities, which is suitable for a variety of web servers and apps with elastic traffic needs.
- Eliminate application system SPOF. Even if some ECS instances malfunction, the application

system will continue to function normally.

- Improve application systems disaster tolerance capabilities through multi-zone deployment. If a machine room malfunctions, the system will continue to function normally.
- Prevent attacks on the application system, which is suitable for businesses that often suffer WAF and CC related problems.

Procedure

Log on to the Server Load Balancer console.

On the **Instance Management** page, click **Create Server Load Balancer**.

Select a region, primary and backup zones, instance type, public bandwidth, and quantity, and then click **Buy Now**.

Check the configuration information and then click **Activate**.

Edit the Server Load Balancer instance name

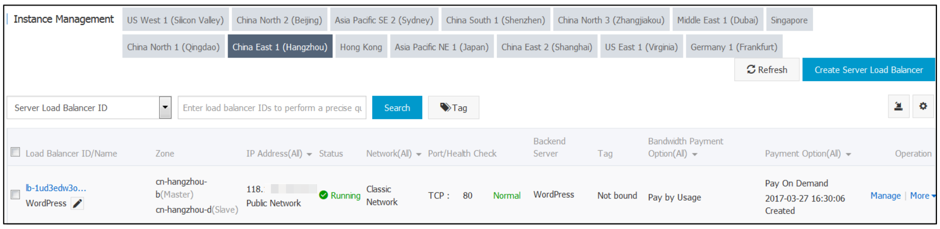
After a Server Load Balancer instance is created, an instance ID is automatically generated. You can add a name for the instance for easy management.

Procedure

Log on to the Server Load Balancer console.

On the **Instance Management** page, click the region where the Server Load Balancer instance is created.

Move the mouser pointer over the instance ID and click the pencil icon to enter an instance name.



□	Load Balancer ID/Name	Zone	IP Address(All)	Status	Network(All)	Port/Health Check	Backend Server	Tag	Bandwidth Payment Option(All)	Payment Option(All)	Operation

□	lb-1ud3edw3o...
	WordPress
		cn-hangzhou-b(Master)
		cn-hangzhou-d(Slave)
			118.[redacted]
			Public Network
				✓ Running	Classic Network	TCP : 80 Normal	WordPress	Not bound	Pay by Usage	Pay On Demand
										2017-03-27 16:30:06 Created
											Manage | More

Listener configurations

Listener configuration is mainly applicable to Layer-4 (TCP/UDP) Server Load Balancer and Layer-7 (HTTP/HTTPS) Server Load Balancer. An instance can be configured with up to 50 listeners.

TCP listener configurations

Application scenarios

TCP is a connection-oriented protocol requiring a reliable connection with the other peer end before data can be sent and received. It is applicable in scenarios with high reliability and data accuracy requirements, but with lower requirements for speed, such as scenarios involving file transfer, email and remote logon.

Recommended configurations

To facilitate the rapid convergence of user services and application status, the recommended parameter settings are as follows:

- Response timeout: 5 seconds
- Health check interval: 2 seconds
- Unhealthy threshold value: 3
- Healthy threshold value: 3

Lower the health check response timeout value for faster response, but ensure that the service is processed within a timeframe less than the value. The recommended ECS health check failure and success response times are as follows:

- ECS health check failure response time in case of a network exception: (2 + 5) × 3 = 21 seconds
- ECS health check success response time: 2×3=6 seconds

UDP listener configurations

Application scenarios

UDP is a non-connection-oriented protocol. Before sending data, it performs packet transmission directly instead of handshaking with the other party. It is mainly applicable in scenarios with preference to real-time information over reliability, such as video chats, push of real-time financial quotations, DNS and IoT.

Recommended configurations

To facilitate the rapid convergence of user services and application status, the recommended parameter settings are as follows:

- Response timeout time: 10 seconds
- Health check interval: 5 seconds
- Unhealthy threshold value: 3
- Healthy threshold value: 3

Lower the response timeout value for faster response, but ensure that the service is processed within a timeframe less than the value. The recommended ECS health check failure and success response times are as follows:

- ECS health check failure response time in the case of a network exception: (10 + 5) × 3 = 45 seconds
- ECS health check success response time: 5 × 3 = 15 seconds

HTTP listener configurations

Application scenario

HTTP is an application layer protocol mainly used to package data and is applicable to applications needing to identify data content, such as web applications and small-size mobile games.

Recommended configurations

To facilitate the rapid convergence of user services and application status, the recommended parameter settings are as follows:

- Response timeout: 5 seconds
- Health check interval: 2 seconds
- Unhealthy threshold value: 3
- Healthy threshold value: 3

Lower the response timeout value for faster response, but ensure that the service is processed within a timeframe less than the value. The recommended ECS health check failure and success response times are as follows:

- ECS health check failure response time (in case of a network exception): (2 + 5) × 3 = 21 seconds
- ECS health check success response time: 2×3=6 seconds

HTTPS listener configurations

Application scenarios

The HTTPS protocol is applicable to the scenario where sensitive information is transmitted between clients and servers. HTTPS ensures data transmission security by blocking unauthorized access requests.

Recommended configurations

To facilitate the rapid convergence of user services and application status, the recommended parameter settings are as follows:

- Response timeout: 5 seconds
- Health check interval: 2 seconds
- Unhealthy threshold value: 3
- Healthy threshold value: 3

Lower the response timeout value for faster response, but ensure that the service is processed within a timeframe less than the value. The recommended ECS health check failure and success response times are as follows:

- ECS health check failure response time in case of a network exception: (2 + 5) × 3 = 21 seconds
- ECS health check success response time: 2×3=6 seconds

There is no specification for the HTTPS monitoring port selection, however, port 443 is recommended.

Add backend servers

Application scenarios

You can add, delete and configure the weights of backend servers to control traffic forwarding under the listeners of a Server Load Balancer instance.

Considerations

- By default, the ECS instance weight is set to 100 based on the average forwarding rule.
- Only ECS instances in **Running** status can be added.
- A Server Load Balancer instance with of the type Virtual Private Cloud (VPC) or classic public network can be added to backend private network ECS instances located in the same private network.

Procedure

Log on to the Server Load Balancer console.

On the **Instance Management** page, click the region where the Server Load Balancer instance is created and then click the instance ID to go to the **Details** page.

From the Server Load Balancer menu, click **Server** > **Backend server**.

Click the **Servers Not Added** tab.

Click **Add** next to the ECS instance that you want to add to the Server Load Balancer instance.

Set the weight in the pop-up window and then click **Confirm**.

The default value **100** indicates that the average forwarding rule is used.

Set whitelist access control

Overview

The whitelist is an access control mode that enables you to configure the IP addresses allowed for accessing the Server Load Balancer listener. It applies to scenarios where the application only allows the access from some specific IP addresses.

Note:

- There is certain business risk for setting a whitelist. Once a whitelist is configured, only the IP addresses in the whitelist can access the Server Load Balancer listener.
- If you enable the access control without setting a whitelist, no one will be able to access this Server Load Balancer listener.
- Setting up a whitelist might cause a short interrupt of access to the Server Load Balancer instance.

Prerequisites

You have enabled the whitelist access control feature through submitting a ticket.

Operating procedure

Log on to the Server Load Balancer console.

Select the desired region.

Click the ID link of the Server Load Balancer instance you want to set for access control.

Click **Listeners** in the left navigation bar.

In the Operation column of the desired listener, click **More > Set Access Controls**.

Click the **Turn on Access Control** switch which is in the Off status to enable the feature.

Enter the IP addresses allowed to access this listener in the **Whitelist Settings** box.

You can input single IP addresses or IP network segments. Multiple IP addresses should be separated by commas and duplicate IP addresses are not allowed. You can enter up to 300 IP addresses.

Click **OK** and confirm the settings in the pop-up box.

Related information

After you set up the whitelist access control, you can modify or disable the access control at any time:

- Modify the access control: Follow the operation steps 1-5 above to call out the **Access Control Settings** dialog box, modify the IP addresses in the **Whitelist Settings** box, and then click **OK**.
- Disable the access control: Follow the operation steps 1-5 above to call out the **Access Control Settings** dialog box. Click the **Turn on Access Control** switch which is in the On status to disable the feature, and then click **OK**.

Add a VServer group

By default, a backend server group in the instance dimension is created and maintained by the system. All listeners in a Server Load Balancer instance use the same backend server group. A VServer group allows you to personalize the server group in the listener dimension, that is, instances under different listeners can use a different set of backend servers, domain names, and URL forwarding to meet individual needs.

Considerations

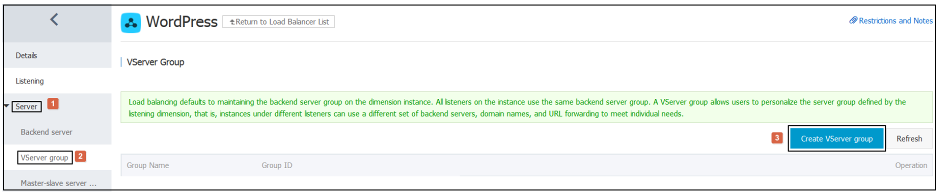
- The backend servers added to a VServer group must be in the same region of the listener.
- A backend server can be added to multiple VServer groups.
- A VServer group can be added to multiple listeners in a Server Load Balancer instance.
- A VServer group is group of ECS server instances with specified port numbers.

Procedure

Log on to the Server Load Balancer console.

On the **Instance Management** page, select a region and then click the instance ID of the Server Load Balancer that you want to add a VServer group for.

Click **Server** > **VServer Group**, and then click **Create VServer group**.



Load balancing defaults to maintaining the backend server group on the dimension instance. All listeners on the instance use the same backend server group. A VServer group allows users to personalize the server group defined by the listening dimension, that is, instances under different listeners can use a different set of backend servers, domain names, and URL forwarding to meet individual needs.

In the **Create VServer Group** window, complete the following information:

Enter a group name.

Select the network type.

Click the ECS server that you want to add.

In the **Selected Server Lists** panel, enter the port number and weight for each added server.

Click **Confirm**.

The added VServer group is displayed on the **VServer Group** page, you can :

- Click **View** to view the configurations of the VServer group.
- Click **Edit** to change the configurations of the VServer group.
- Click **Delete** to delete the VServer group.

Certificate management

Certificate formats

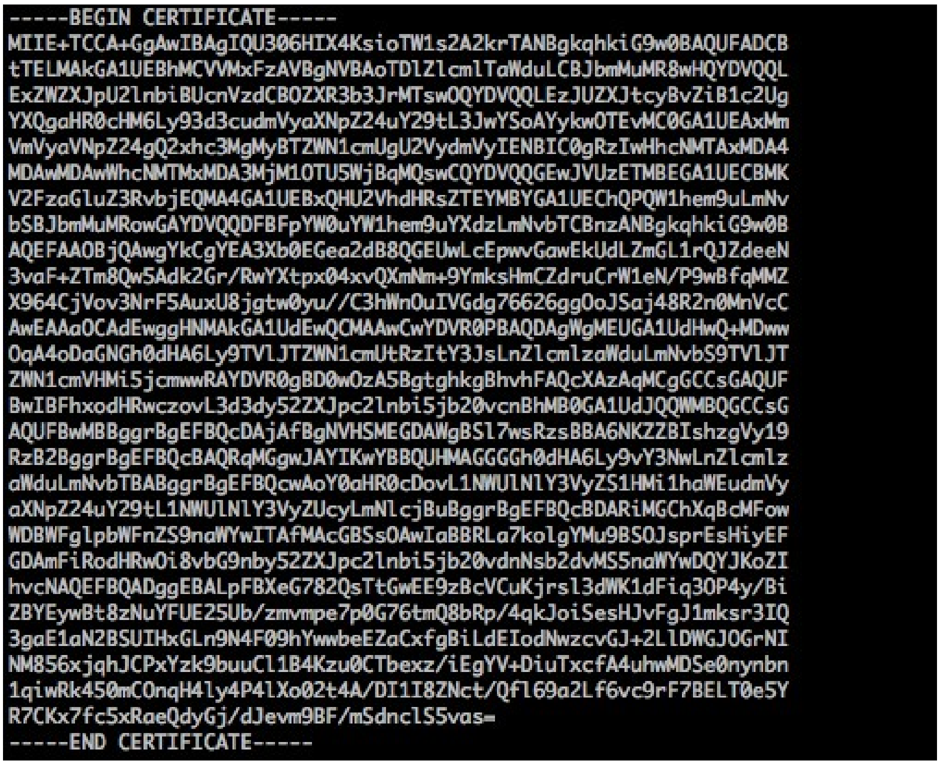
A certificate in the REM format is required in a Linux environment. The Server Load Balancer does not support other certificate formats.

If a certificate from the root CA has been obtained, only this is required for access devices, such as browsers, to trust your website. If a certificate file consisting of multiple certificates has been obtained from an intermediate CA, the server and intermediate certificate must be combined manually before uploading. The server certificate must be followed by the intermediate certificate without any blank lines. The CA will provide relevant descriptions when issuing a certificate, pay attention to the rule descriptions.

This document shows samples of the certificate and certificate link format, check the certificate format before uploading it.

Certificate issued by the root CA

The following is a sample certificate issued in a Linux environment.



```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

Certificate rules

- [———-BEGIN CERTIFICATE———-, ———-END CERTIFICATE———-] indicates the content at the beginning and end of the certificate, which must be uploaded together.
- There are 64 characters in each line and the last line cannot exceed 64 characters.

Certificate link issued by the intermediate CA

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

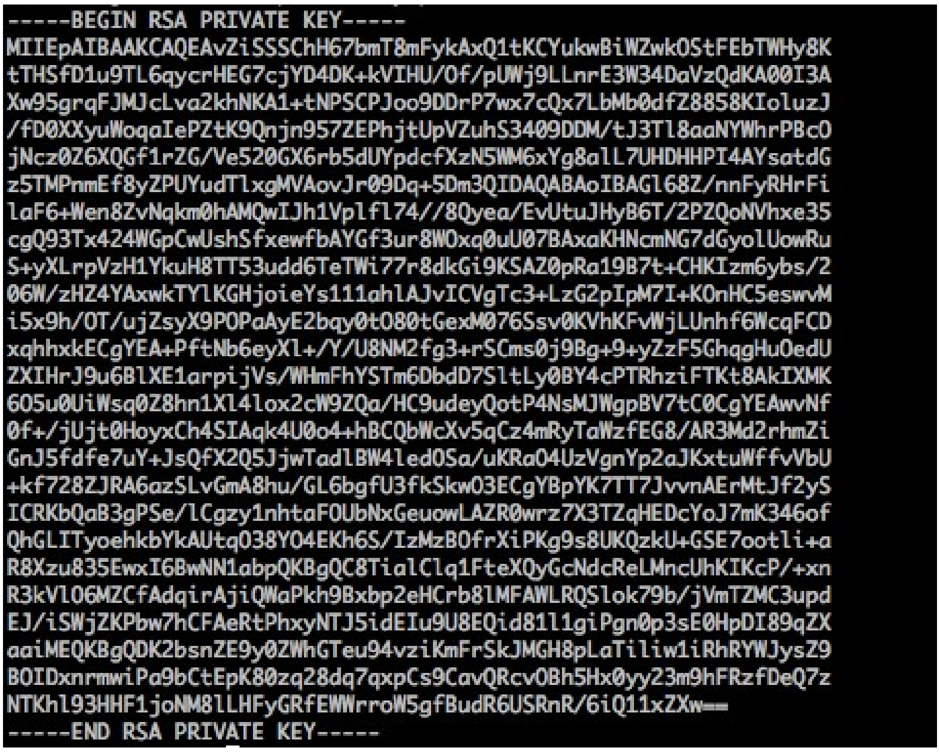
———-END CERTIFICATE———-

Certificate link rules

- Blank lines cannot be inserted between certificates.
- Each certificate must comply with the certificate rules.

RSA private key format

The following is a sample RSA private key.



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K
tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudTlxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHrFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8WOxq0uU07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM
i5x9h/OT/ujZsyX9POPaAyE2bqy0tO80tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHuOedU
ZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK
6O5u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkwO3ECgYBpYK7TT7JvvnAErMtJf2yS
ICRKbQaB3gPSe/lCgzy1nhtaFOUbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVlO6MZCfAdqirAjiQWaPkh9Bxbp2eHCrb8lMFAWLRQSlok79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcvOBh5Hx0yy23m9hFRzfDeQ7z
NTKhl93HHF1joNM8lLHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

RSA private key rules

[——-BEGIN RSA PRIVATE KEY——-, ——-END RSA PRIVATE KEY——-] indicates the content at the beginning and end of the RSA private key, which must be uploaded together.

There are 64 characters in each line and the last line cannot exceed 64 characters.

Note: If your private key is not generated in the format of [——-BEGIN PRIVATE KEY——-, ——-END PRIVATE KEY——-] based on the preceding rules, run the following command to convert the private key, and then upload the content of new_server_key.pem together with the certificate.

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Generate certificates

You have to generate the corresponding certificate, including the server, CA and client certificates, and upload them to the certificate management system of the Server Load Balancer service.

- Server certificate: used by the user browser to check whether the certificate sent by the server is signed by a trusted center. The server certificate must be uploaded to the certificate management system of the Server Load Balancer.
- Client certificate: used to prove the identity of the client user for communication with the server end.
- CA certificate: used to verify the client certificate. The server requires the client browser to send the client certificate and, once the certificate is received, a verification occurs. If the verification fails, the connection is denied. After two-way authentication is enabled, you must upload both the CA certificate and server certificate to the certificate management system of the Server Load Balancer service.

Generate a server certificate

You can buy and generate the server certificate from Alibaba Cloud Security Certificate Service, or from other providers.

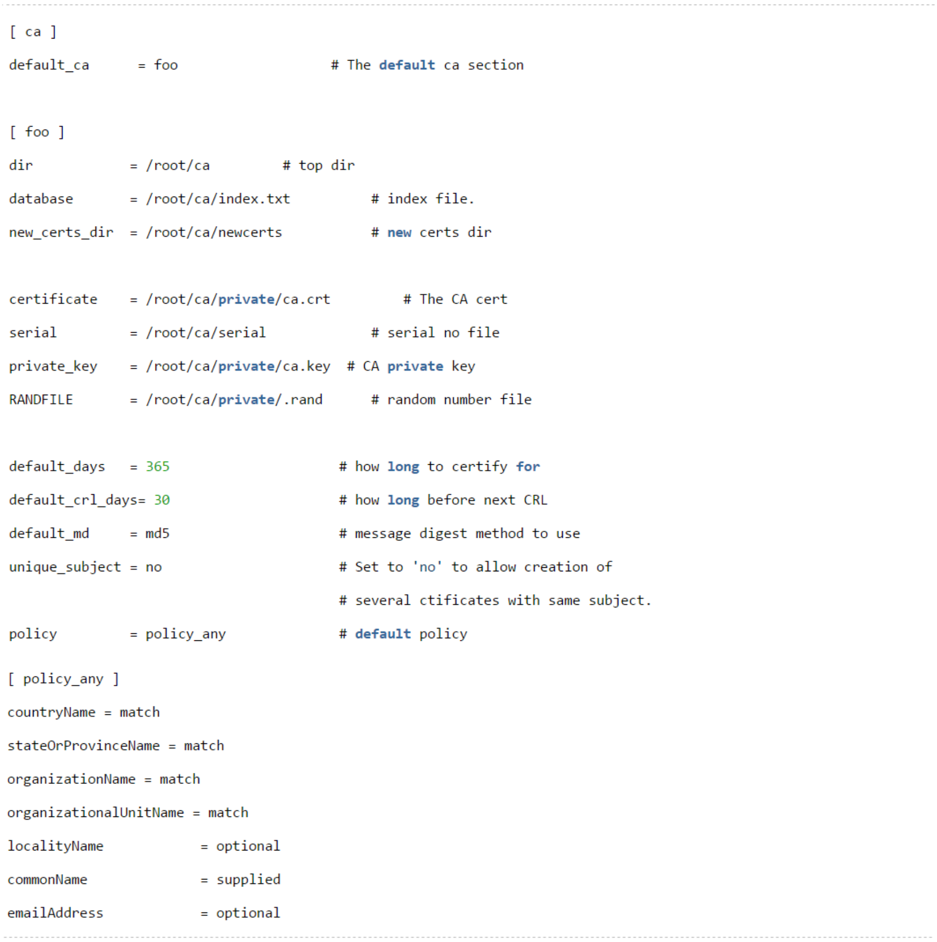
Generate a self-signed CA certificate using OpenSSL

Create a ca folder in the /root directory and create four subfolders under the ca folder:

```
$ sudo mkdir ca
$ cd ca
$ sudo mkdir newcerts private conf server
```

- The newcerts folder stores CA signed digital certificates (certificate backup directory);
- The private folder stores the CA private key;
- The conf folder stores some configuration files to simplify parameters;
- The server folder stores the server certificate file.

Create an openssl.conf file under the conf directory and edit the content as follows.



```
[ ca ]
default_ca      = foo                   # The default ca section

[ foo ]
dir            = /root/ca         # top dir
database       = /root/ca/index.txt          # index file.
new_certs_dir  = /root/ca/newcerts           # new certs dir

certificate    = /root/ca/private/ca.crt         # The CA cert
serial         = /root/ca/serial             # serial no file
private_key    = /root/ca/private/ca.key  # CA private key
RANDFILE       = /root/ca/private/.rand      # random number file

default_days   = 365                     # how long to certify for
default_crl_days= 30                     # how long before next CRL
default_md     = md5                     # message digest method to use
unique_subject = no                      # Set to 'no' to allow creation of
                                         # several ctificates with same subject.
policy         = policy_any              # default policy

[ policy_any ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = match
localityName            = optional
commonName              = supplied
emailAddress            = optional
```

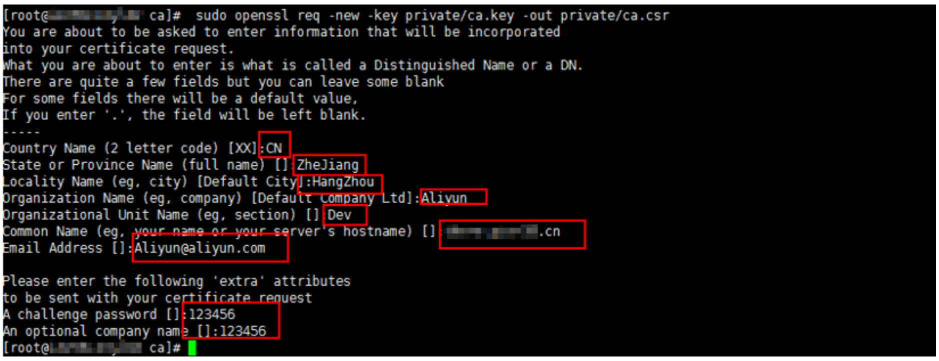
Run the following command to generate the private key file.

```
$ cd /root/ca
$ sudo openssl genrsa -out private/ca.key
Output
Generating RSA private key, 512 bit long modulus
..++++++++++++
.++++++++++++
e is 65537 (0x10001)
```

A ca.key file is generated under the private folder. The OpenSSL is 512 bits by default, but usually 2048 bits is used.

Run the following command and provide the required information according to the figure after the command. Press **Enter** to generate the certificate request csr file.

```
$ sudo openssl req -new -key private/ca.key -out private/ca.csr
```



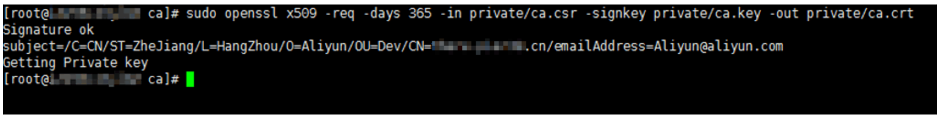
```
[root@[redacted] ca]#  sudo openssl req -new -key private/ca.key -out private/ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:ZheJiang
Locality Name (eg, city) [Default City]:HangZhou
Organization Name (eg, company) [Default Company Ltd]:Aliyun
Organizational Unit Name (eg, section) []:Dev
Common Name (eg, your name or your server's hostname) []:[redacted].cn
Email Address []:Aliyun@aliyun.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:123456
[root@[redacted] ca]#
```

Note: Enter xxx.xxx.cn as the common name if you do not have a domain name ready.

Run the following command to generate the crt file.

```
$ sudo openssl x509 -req -days 365 -in private/ca.csr -signkey private/ca.key -out private/ca.crt
```

The following is an output example on the console. A ca.crt file is generated under the private directory.



```
[root@[redacted] ca]# sudo openssl x509 -req -days 365 -in private/ca.csr -signkey private/ca.key -out private/ca.crt
Signature ok
subject=/C=CN/ST=ZheJiang/L=HangZhou/O=Aliyun/OU=Dev/CN=[redacted].cn/emailAddress=Aliyun@aliyun.com
Getting Private key
[root@[redacted] ca]#
```

Run the following command to set a starting serial number for the key. The serial number can be any four characters.

```
$ sudo echo FACE > serial
```

Run the following command to create a CA key library.

```
$ sudo touch index.txt
```

Run the following command to create a certificate revocation list for removing User Certificates.

```
$ sudo openssl ca -gencrl -out /root/ca/private/ca.crl -crldays 7 -config "/root/ca/conf/openssl.conf"
```

Output:

```
Using configuration from /root/ca/conf/openssl.conf
```

A ca.crl file is generated under the private directory.

Generate a client certificate

1. Run the following command to create a users directory for storing the key.

```
$ sudo mkdir users
```

Run the following command to create a key for the user.

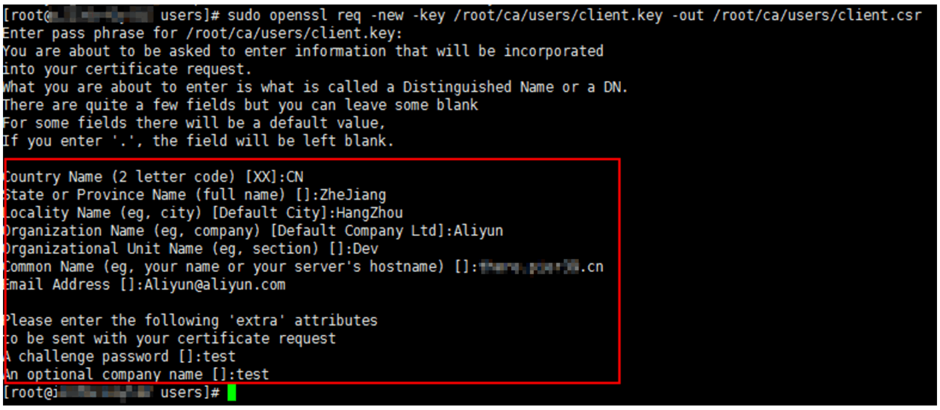
```
$ sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

The pass phrase is required. This is the password of the current key and acts to prevent the key from being stolen and used by others. Enter the same password for the two prompts. A client.key file is generated under the users directory.

Run the following command to create a certificate signature request csr file for the key.

```
$ sudo openssl req -new -key /root/ca/users/client.key -out /root/ca/users/client.csr
```

The pass phrase is required, and is the current key password. It prevents the key from being stolen and used by others. Enter the same password for the two prompts. A client.key file is generated under the users directory.

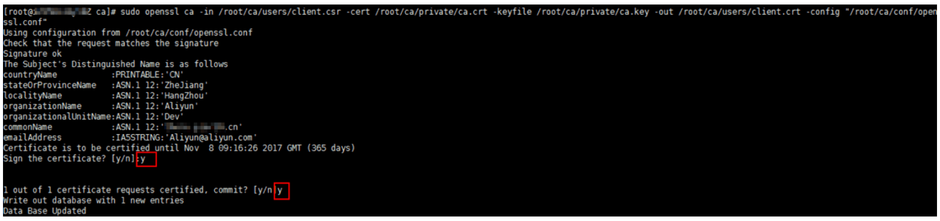


```
[root@[redacted] users]# sudo openssl req -new -key /root/ca/users/client.key -out /root/ca/users/client.csr
Enter pass phrase for /root/ca/users/client.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:ZheJiang
Locality Name (eg, city) [Default City]:HangZhou
Organization Name (eg, company) [Default Company Ltd]:Aliyun
Organizational Unit Name (eg, section) []:Dev
Common Name (eg, your name or your server's hostname) []:[redacted].cn
Email Address []:Aliyun@aliyun.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:test
An optional company name []:test
[root@i[redacted] users]#
```

Run the following command to sign the key with your private CA key.

$ sudo openssl ca -in /root/ca/users/client.csr -cert /root/ca/private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/users/client.crt -config "/root/ca/conf/openssl.conf"

Output on the console:



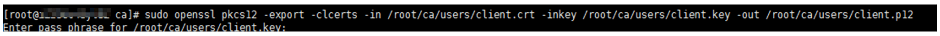
```
[root@[redacted]Z ca]# sudo openssl ca -in /root/ca/users/client.csr -cert /root/ca/private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/users/client.crt -config "/root/ca/conf/open
ssl.conf"
Using configuration from /root/ca/conf/openssl.conf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :ASN.1 12:'ZheJiang'
localityName          :ASN.1 12:'HangZhou'
organizationName      :ASN.1 12:'Aliyun'
organizationalUnitName:ASN.1 12:'Dev'
commonName            :ASN.1 12:'[redacted].cn'
emailAddress          :IA5STRING:'Aliyun@aliyun.com'
Certificate is to be certified until Nov  8 09:16:26 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Enter **y** for both confirmation prompts. A client.crt file is generated under the users directory.

Run the following command to concert the certificate into the PKCS12 file that is recognizable by most browsers.

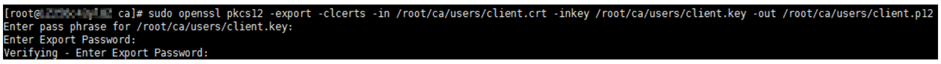
$ sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt -inkey /root/ca/users/client.key -out /root/ca/users/client.p12

Enter the pass phrase of theclient.key file when the following prompt is displayed.



```
[root@[redacted] ca]# sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt -inkey /root/ca/users/client.key -out /root/ca/users/client.p12
Enter pass phrase for /root/ca/users/client.key:
```

Enter Export Password when the following prompt is displayed. This is the protection password of the client certificate. The password is required when the client installs a certificate.



```
[root@[redacted] ca]# sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt -inkey /root/ca/users/client.key -out /root/ca/users/client.p12
Enter pass phrase for /root/ca/users/client.key:
Enter Export Password:
Verifying - Enter Export Password:
```

A client.p12 file is generated under the users directory.

Convert the certificate format

Server Load Balancer only supports certificates in the PEM format. Certificates in other formats must be converted to PEM before uploading to the certificate management system of the Server Load Balancer service. OpenSSL is recommended for format conversion.

DER to PEM

The DER format is usually used on Java platforms.

- Certificate conversion: openssl x509 -inform der -in certificate.cer -out certificate.pem
- Private key conversion: openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem

P7B to PEM

The P7B format is usually used in Windows Server and Tomcat.

- Certificate conversion: openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer Obtain the content of [——-BEGIN CERTIFICATE——- ， ——-END CERTIFICATE——-] from outcertificat.cer and upload the content as a certificate.
- Private key conversion: no private key

PFX to PEM

The PFX format is usually used in Windows Server.

- Private key extraction: openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
- Certificate extraction: openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

Upload certificates

To support HTTPS，Server Load Balancer provides the certificate management function, enabling you to store certificates in the certificate management system without deploying certificates on backend servers. The private key uploaded to the certificate management system will be encrypted.

Considerations

- Each user can create up to 100 certificates.
- A certificate can be applied to one or more listeners.
- For security and performance considerations, if your certificate is used in multiple regions, it must be uploaded into all these regions.

Procedure

Log in to the Server Load Balancer console.

On the **Server Load Balancer** menu, click **Certificates**.

On the **Certificates** page, click **Create Certificate**.

On the **Create Certificate** page, enter a certificate name, select the regions where the certificate is used and then upload the certificate. Click **Confirm**.

Note: The certificate must be in the PEM formats. Refer to Certificate formats for more details.

Use certificates

After uploading a certificate, you can create a HTTPS listener and bind the required certificate to it.

Procedure

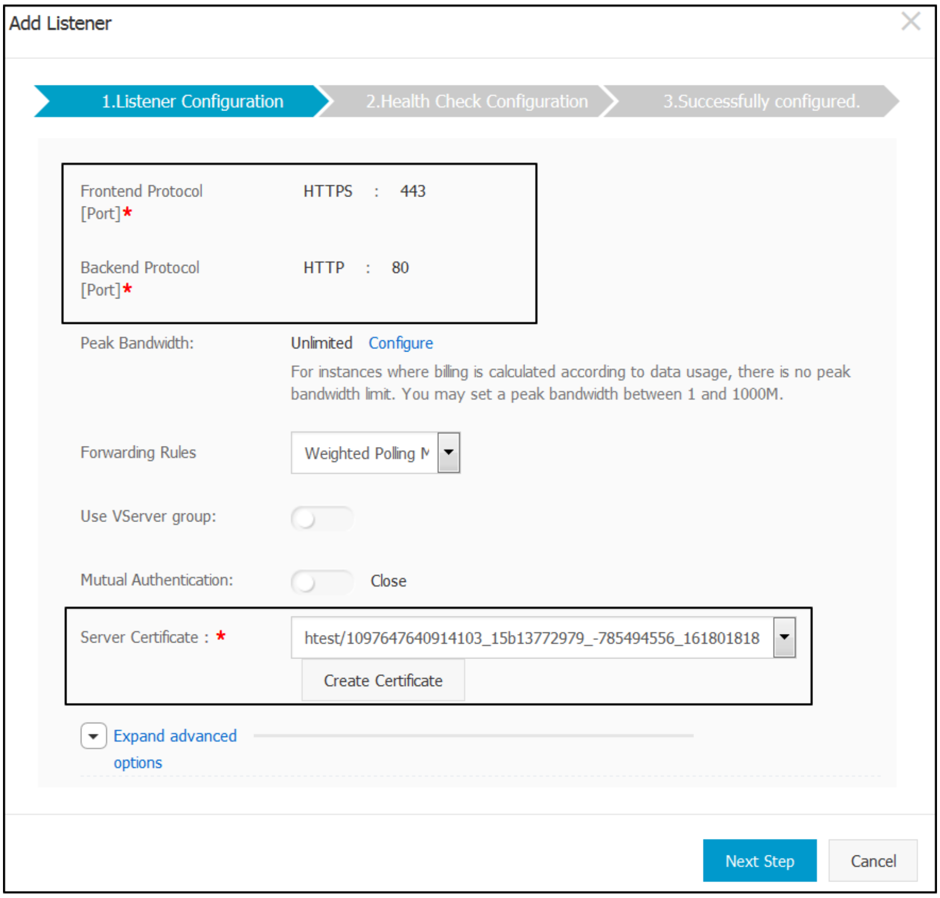
Log on to the Server Load Balancer console.

On the **Instance Management** page, select a region and then click the ID link of the Server Load Balancer instance.

Click **Listening** and then click **Create Listener**.

Configure the listener settings and click **Next Step**.

- For the frontend protocol, select HTTPS and port 443 is recommended.
- For the backend protocol, HTTP port 80 is recommended.
- Select the server certificate used for authorization.



Add Listener

Frontend Protocol [Port]*: HTTPS : 443

Backend Protocol [Port]*: HTTP : 80

Peak Bandwidth: Unlimited Configure

For instances where billing is calculated according to data usage, there is no peak bandwidth limit. You may set a peak bandwidth between 1 and 1000M.

Forwarding Rules: Weighted Polling M

Use VServer group:

Mutual Authentication: Close

Server Certificate : * htest/1097647640914103_15b13772979_-785494556_161801818

Configure the health check settings and click **Confirm**. For details, refer to **Listener configurations**.

Configure HTTPS mutual authentication

Server Load Balancer supports HTTPS mutual authentication to secure data transfer between the server and the client. Both the CA certificate and server certificate are required to enable HTTPS mutual authentication.

Procedure

Generate the certificate, including the server certificate, CA certificate and client certificate. Refer to **Generate certificates** for details.

Import the client certificate.

Download the client certificate.

Double click the import program to run it.

Enter the certificate password.

Select the storage location for the imported certificate to complete the import.

Configure HTTPS mutual authentication.

Upload the generated server certificate and CA certificate. For details, refer to Upload certificates.

When you create a new HTTPS listener or configure an existing HTTPS listener on the Server Load Balancer console, click the **Mutual Authentication** toggle to enable the function and select an uploaded server certificate and CA certificate.

For details about how to create and configure the listener, refer to Listener configurations.

Substitute certificates

- A new certificate must be created when the existing one expires.
- If an error occurs when you add a certificate of Server Load Balancer, the private key may be incorrect. In this case, you must replace the certificate with a correct one.

Procedure

Create and upload a certificate.

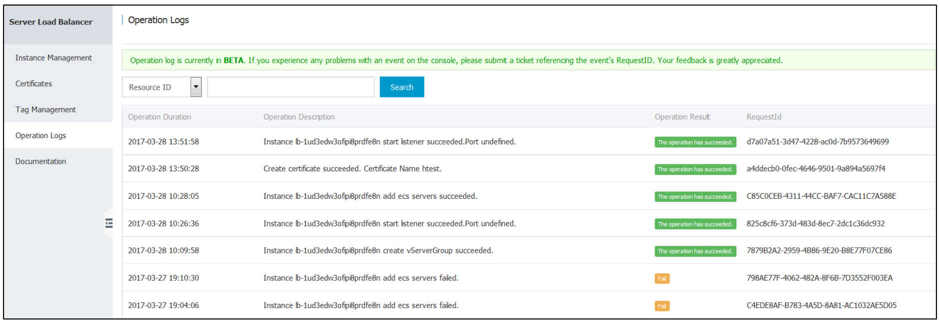
Update the HTTPS listener.

(Optional) Delete the old certificate.

Log management

Operation log information

The following is an example of operation logs.



Operation log is currently in **BETA**. If you experience any problems with an event on the console, please submit a ticket referencing the event's RequestID. Your feedback is greatly appreciated.

Operation Duration	Operation Description	Operation Result	RequestId
2017-03-28 13:51:58	Instance lb-1ud3edw3ofipi8prdfe8n start listener succeeded.Port undefined.	The operation has succeeded.	d7a07a51-3d47-4228-ac0d-7b9573649699
2017-03-28 13:50:28	Create certificate succeeded. Certificate Name htest.	The operation has succeeded.	a4ddecb0-0fec-4646-9501-9a894a5697f4
2017-03-28 10:28:05	Instance lb-1ud3edw3ofipi8prdfe8n add ecs servers succeeded.	The operation has succeeded.	C85C0CEB-4311-44CC-BAF7-CAC11C7A588E
2017-03-28 10:26:36	Instance lb-1ud3edw3ofipi8prdfe8n start listener succeeded.Port undefined.	The operation has succeeded.	825c8cf6-373d-483d-8ec7-2dc1c36dc932
2017-03-28 10:09:58	Instance lb-1ud3edw3ofipi8prdfe8n create vServerGroup succeeded.	The operation has succeeded.	7879B2A2-2959-4B86-9E20-B8E77F07CE86
2017-03-27 19:10:30	Instance lb-1ud3edw3ofipi8prdfe8n add ecs servers failed.	Fail	798AE77F-4062-482A-8F6B-7D3552F003EA
2017-03-27 19:04:06	Instance lb-1ud3edw3ofipi8prdfe8n add ecs servers failed.	Fail	C4EDE8AF-B783-4A5D-8A81-AC1032AE5D05

- Operation Duration: shows the time that the operation occurred. It is the local time.
- Operation Description: shows the operation that you performed.
- Operation result: shows whether the operation is successful or not.
- RequestedID: shows the operation ID and is unique.

View operation logs

You can check the operation log for troubleshooting. The system only displays operation logs generated in the most recent month. Operation logs can be searched on the console by resource IDs and operation results.

The operation log feature is currently under a public beta test.

Procedure

Log on to the Server Load Balancer console.

Click **Operation Logs**. You are then directed to the **Operation logs** page.

You can use the resource ID or the operation result to search specific operations. The resource ID is the ID of the current operation object, such as a Server Load Balancer instance ID, certificate ID, virtual server group ID, and forwarding policy ID.

Monitoring

View monitoring data

Server Load Balancer provides you with the function to view real-time metrics and historical metrics of the Server Load Balancer instances.

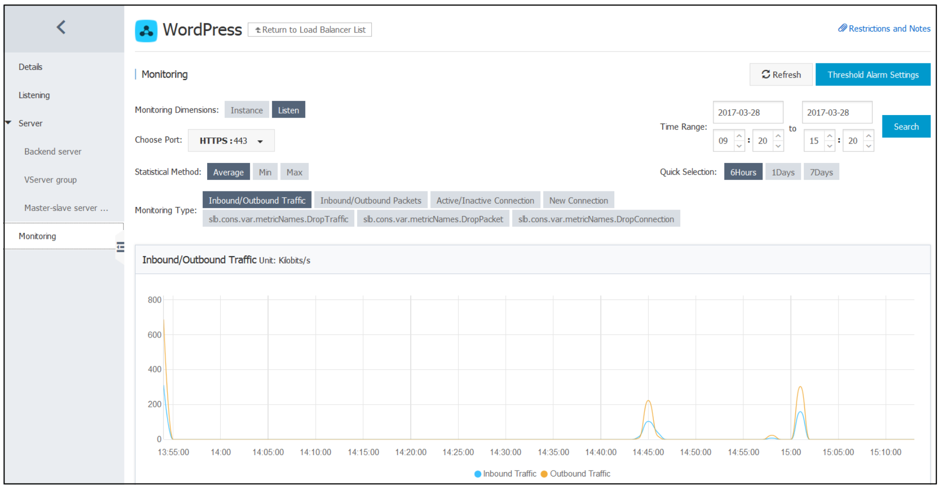
Note: The Server Load Balancer instances without backend ECS servers or with the abnormal status are unable to provide metric data. Ensure your Server Load Balancer instance is configured correctly and is running properly.

Procedure

Log on to the Server Load Balancer console.

Select a region and click the ID link of the instance that you want to view.

Click **Monitoring** and configure the monitoring settings to filter the result.



Monitoring Dimensions: Listen

Choose Port: HTTPS : 443

Statistical Method: Average

Monitoring Type: Inbound/Outbound Traffic

Time Range: 2017-03-28 09 : 20 to 2017-03-28 15 : 20

Quick Selection: 6Hours

Set alarm settings

You can use Cloud Monitor to configure a set of alarms based on the specified thresholds for the following items:

- Inbound traffic
- Outbound traffic
- Number of new connections
- Number of active connections
- Number of inactive connections
- Number of incoming packets
- Number of outgoing packets.

Alarms are raised by SMS as well as e-mail, or both.

Prerequisite

The Cloud Monitor service has been activated.

Procedure

Log on to the Server Load Balancer console.

Select a region and click the ID link of the instance that you want to view.

Click **Monitoring** and then click **Threshold Alarm Settings**. You are then directed to Cloud Monitor console.

Click **New alarm rule** to create an alarm.

Refer to Server Load Balancer monitoring for more information on how to configure the alarm rules.

Restrictions

Limitations

Limitation	Description	Ticket Submission Supports Exception

Number of ECS instances to be added	You must have one ECS instance at least to add to the Server Load Balancer instance, and the region of the ECS instance and the Server Load Balancer instance must be the same.	Not supported
Billing method	Pay-As-You-Go	Not supported
Peak public bandwidth range for a single listener (Pay-As-You-Go)	1 – 1,000 Mbps or unlimited	Not supported
System limit on the peak private bandwidth for a single listener	1 Gbps	Not supported
Default quota of Pay-As-You-Go instances	- Common users: 30 - Ant Financial Cloud users: 30	Supported
Restrictions on Server Load Balancer instance name	Length range is 1–80 characters, including letters, digits, hyphen (-), backslash （/）, period （.） and underscore （_）.	Not supported
Number of Server Load Balancer instance listeners	50 instance listeners	Not supported
Protocol types available for Server Load Balancer monitoring	HTTP/HTTPS/TCP	Not supported
Frontend/Backend port range for Server Load Balancer monitoring	1 – 65535	Not supported
Forwarding rules of Server Load Balancer monitoring	wrr and wlc	Not supported
HTTP protocol-session persistence-cookie processing method	insert and server	Not supported
HTTP-session persistence-cookie timeout time	1 – 86,400 (default is 3,600)	Not supported
HTTP-session persistence-cookie name	No more than 200 characters and cookies must comply with RFC 2965. This means that they can only contain ASCII English letters and digits, and cannot contain commas, semicolons, spaces, or begin with a dollar symbol “$”.	Not supported
HTTP-health check-port	1 – 65,535 (default is the	Not supported

	backend server port)	
HTTP-health check-timeout time	1 – 50 (default is 5. If HCTimeout < Interval, HCTimeout is invalid and the timeout time will be Interval.)	Not supported
HTTP-health check-check interval	1 - 5 (default is 2)	Not supported
HTTP-health check-healthy threshold value	1 - 10 (default is 3)	Not supported
HTTP-health check-unhealthy threshold value	1 - 10 (default is 3)	Not supported
Number of backend ECS instances that can be batch added or deleted	20	Not supported
ECS instance status to be added	Running	Not supported
Weight input range for backend ECS instances	1 - 100 (default is 100)	Not supported
API access frequency limit for a single key	5,000 times/day	No automatic process is available now. Contact customer service or Business Development for help.
Maximum number of certificates uploaded by a single user	100	No automatic process is available now. Contact customer service or Business Development for help.