

Alibaba Cloud Server Load Balancer

Tutorials

Issue: 20190816

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.








1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

| Style | Description | Example |
|---|--|--|
|  | This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  Danger: Resetting will result in the loss of user configuration data. |
|  | This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  Warning: Restarting will cause business interruption. About 10 minutes are required to restore business. |
|  | This indicates warning information, supplementary instructions, and other content that the user must understand. |  Notice: Take the necessary precautions to save exported data containing sensitive information. |
| | This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user. |  Note: You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | It is used for buttons, menus, page names, and other UI elements. | Click OK. |
| Courier font | It is used for commands. | Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder. |
| <i>Italics</i> | It is used for parameters and variables. | <code>bae log list --instanceid Instance_ID</code> |
| [] or [a b] | It indicates that it is an optional value, and only one item can be selected. | <code>ipconfig [-all -t]</code> |

| Style | Description | Example |
|---------------------------------------|--|------------------------------------|
| <code>{}</code> or <code>{a b}</code> | It indicates that it is a required value, and only one item can be selected. | <code>swich {stand slave}</code> |

Contents

| | |
|--|----|
| Legal disclaimer..... | I |
| Generic conventions..... | I |
| 1 Add an HTTPS listener (one-way authentication)..... | 1 |
| 2 Add an HTTPS listener (mutual authentication)..... | 4 |
| 3 Redirect HTTP to HTTPS..... | 14 |
| 4 Configure a multi-domain-name HTTPS website on an SLB instance..... | 16 |
| 5 Traffic forwarding based on domain names or URLs..... | 21 |
| 6 Use access logs to rapidly locate abnormal backend servers..... | 34 |
| 7 Specify an IP address for an SLB instance with OpenAPI Explorer..... | 38 |
| 8 View traffic usage..... | 41 |

1 Add an HTTPS listener (one-way authentication)

To add an HTTPS listener with one-way authentication, you only need to upload a server certificate to SLB when configuring the listener.

Step 1 Upload the server certificate

Before configuring the HTTPS listener (one-way authentication), you must buy a server certificate and upload the server certificate to the certificate management system of SLB. You no longer need to maintain the certificate on the backend server after uploading it to SLB.

1. Log on to the [SLB console](#).
2. In the left-side navigation pane, click Certificates, and then click Create Certificate.
3. Configure the server certificate as follows:

- **Regions:** Select China (Hangzhou).



Note:

The region of the certificate must be the same as that of the SLB instance to use the certificate.

- **Certificate Type:** Select Server Certificate.
- **Certificate Content and Private Key:** Copy the content and private key of the server certificate. Click Import Sample to view the valid certificate format. The certificate to be uploaded must be in the PEM format. For more information, see [Certificate formats](#).



4. Click OK.

Step 2 Configure the SLB instance

1. Log on to the [SLB console](#).
2. On the Server Load Balancer page, click Create SLB Instance.
3. Configure the instance and then click Buy Now.



Note:

In this tutorial, the instance type is Internet and the region is China (Hangzhou). For more information, see [Create an SLB instance](#).

4. Go back to the Server Load Balancer page and select the China (Hangzhou) region.
5. Click the ID of the created SLB instance or click Configure Listener.
6. Click the Listeners tab and then click Add Listener.
7. In the Protocol and Listener tab, configure the listener.
 - Select Listener Protocol: HTTPS
 - Listening Port: 443
 - Scheduling Algorithm: Round Robin (RR)

← Configure Server Load Balancer

1 Protocol and Listener 2 SSL Certificates 3 Backend Servers 4 Health Check 5 Submit

Select Listener Protocol

TCP UDP HTTP **HTTPS**

Backend Protocol

HTTP

* Listening Port 443

Advanced Modify

Scheduling Algorithm Round-Robin

Session Persistence Disabled

HTTP/2 Access Control

Next Cancel

8. Click Next. Under the SSL Certificates tab, select the uploaded server certificate.

← Configure Server Load Balancer

1 Protocol and Listener 2 SSL Certificates 3 Backend Servers 4 Health Check 5 Submit

Configure SSL Certificates

1 Configure SSL certificates to ensure that your business is protected by encryptions and authenticated by a trusted certificate authority.

Select Server Certificate

.example1.com

Create Server Certificate Buy Certificate

Advanced Modify

Enable Mutual Authentication Disabled

CA Certificate None Selected

Previous Next Cancel

9. Click Next. On the displayed page, click Default Server Group and then click Add. Add ECS instances and set the backend port to 80.
10. In the left-side navigation pane, click Servers > Backend Servers, and then click Add Backend Servers to add ECS instances.

Step 3 Test the SLB service

1. Go back to the Server Load Balancer page to view the health check status.

When the status is Normal, the backend servers can receive requests forwarded by SLB listeners.

2. Enter the public IP of the Server Load Balancer instance in the web browser.

2 Add an HTTPS listener (mutual authentication)

To add an HTTPS listener with mutual authentication, you have to upload a server certificate and a CA certificate to SLB when configuring the listener.

A self-signed CA certificate is used to sign the client certificate in this tutorial. To add an HTTPS listener with mutual authentication, complete these steps:

1. [Prepare a server certificate](#)
2. [Generate a CA certificate using Open SSL](#)
3. [Generate a client certificate](#)
4. [Upload the server certificate and the CA certificate](#)
5. [Install the client certificate](#)
6. [Configure an HTTPS listener \(mutual authentication\)](#)
7. [Test the SLB service](#)

Step 1 Prepare a server certificate

A server certificate is used by the client browser to check whether the certificate sent by the server is signed and issued by a trusted center. You can purchase a server certificate from Alibaba Cloud Security [Certificate Service](#), or from other service providers.

Step 2 Generate a CA certificate by using Open SSL

1. Run the following commands to create a `ca` folder under the `/root` directory and then create four sub folders under the `ca` folder.

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

Where:

- `newcerts` is used to store the digit certificate signed by a CA certificate.
- `private` is used to hold the private key of the CA.
- `conf` is used to store the configuration files used for simplifying parameters.
- `server` is used to store the server certificate.

2. Create an `openssl . conf` file that contains the following information in the `conf` directory.

```
[ ca ]
default_ca = foo
[ foo ]
dir = / root / ca
database = / root / ca / index . txt
new_certs_dir = / root / ca / newcerts
certificate = / root / ca / private / ca . crt
serial = / root / ca / serial
private_key = / root / ca / private / ca . key
RANDFILE = / root / ca / private /. rand
default_days = 365
default_crl_days = 30
default_md = md5
unique_subject = no
policy = policy_any
[ policy_any ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = match
localityName = optional
commonName = supplied
emailAddress = optional
```

3. Run the following command to generate a private key.

```
$ CD / root / CA
$ sudo openssl genrsa - out private / ca . key
```

The following figure is an example of the key generation.

```
root@izbp1hfvicqx1jbwap3liZ:~/ca/conf# cd /root/ca
root@izbp1hfvicqx1jbwap3liZ:~/ca# sudo openssl genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
.....+++
..+++
e is 65537 (0x10001)
```

4. Run the following command and input the required information according to the prompts. Press Enter to generate the `csr` file used to generate the certificate.

```
$ Sudo OpenSSL req - New - key private / CA . Key - out
private / CA . CSR
```



Note:

Common Name is the domain name of the SLB instance.

```
root@iZbp1hfvivcqx1jbbwap31iZ:~/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) [AU]:CN
State or Province Name (full name) [Some-State]:ZheJiang
Locality Name (eg, city) []:HangZhou
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alibaba
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:mydomain
Email Address []:a@alibaba.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@iZbp1hfvivcqx1jbbwap31iZ:~/ca#
```

5. Run the following command to generate the `ca` file.

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

6. Run the following command to set the start sequence number for the private key, which can be any four characters.

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

7. Run the following command to create a CA key library.

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

8. Run the following command to create a certificate revocation list for removing the client certificate.

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

Output is:

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

Step 3 Generate a client certificate

1. Run the following command to generate a `users` directory under the `ca` directory to store the client key.

```
$ Sudo mkdir users
```

2. Run the following command to create a key for the client.

```
$ Sudo OpenSSL FIG / root / CA / users / client . Key 1024
```



Note:

Enter a pass phrase when creating the key. It is the password to protect the private key from unauthorized access. Enter the same password twice.

3. Run the following command to create a `csr` file for requesting certificate sign.

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

As prompted, input the pass phrase used in the previous step and provide required information.



Note:

A challenge password is the client certificate password (Separate it from the password of `client.key`. In this tutorial, the password is test). It can be same as that of the root certificate or server certificate.

```
root@izbp1hfivcqxljwap3liZ:~/ca# 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) [AU]:CN
State or Province Name (full name) [Some-State]:ZheJiang
Locality Name (eg, city) []:HangZhou
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alibaba
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:mydomain
Email Address []:a@alibaba.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:test
An optional company name []:Alibaba
root@izbp1hfivcqxljwap3liZ:~/ca#
```

4. Run the following command to sign the client key by using the CA key in step 2.

```
$ 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 "
```

Enter y twice when prompted to confirm the operation.

```
root@izbp1hfivvcqx1jwap31iz:~/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/us  
ers/client.crt -config "/root/ca/conf/openssl.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:'Alibaba'  
organizationalUnitName:ASN.1 12:'Test'  
commonName :ASN.1 12:'mydomain'  
emailAddress :IA5STRING:'a@alibaba.com'  
Certificate is to be certified until Jun 4 15:28:55 2018 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  
root@izbp1hfivvcqx1jwap31iz:~/ca#
```

5. Run the following command to convert the certificate to the *PKCS12* file that can be recognized 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
```

Follow the prompts to enter the pass phrase of client. key.

Then enter the password used for exporting the client certificate. This password is used to protect the client certificate, which is required when installing the client certificate.

```
root@izbp1hfivvcqx1jwap31iz:~/ca# sudo openssl pkcs12 -export -clcerts -in /roo  
t/ca/users/client.crt -inkey /root/ca/users/client.key -out /root/ca/users/clien  
t.p12  
Enter pass phrase for /root/ca/users/client.key:  
Enter Export Password:  
Verifying - Enter Export Password:  
root@izbp1hfivvcqx1jwap31iz:~/ca#
```

6. Run the following command to view the generated client certificate.

```
cd users
```

```
ls
```

```
root@izbplhfvivcqx1jbwap31iZ:~/ca# cd users
root@izbplhfvivcqx1jbwap31iZ:~/ca/users# ls
client.crt client.csr client.key client.p12
root@izbplhfvivcqx1jbwap31iZ:~/ca/users#
```

Step 4 Upload the server certificate and the CA certificate

1. Log on to the [SLB console](#).
2. On the Server Load Balancer page, click Create SLB Instance.
3. Configure the instance and then click Buy Now.

In this tutorial, the instance type is Internet and the region is China (Hangzhou).
For more information, see [Create an SLB instance](#).

4. Go back to the Server Load Balancer page, hover the mouse to the instance name area, click the displayed pencil icon and modify the name of the SLB instance.
5. In the left-side navigation pane, click the Certificates tab.
6. Click Upload Certificate.
7. On the Create Certificate page, complete the following configurations and click OK.
 - Regions: In this tutorial, select China (Hangzhou).



Note:

The region of the certificate must be the same as that of the Server Load Balancer instance.

- Certificate Type: Select Server Certificate.
- Certificate Content and Private Key: Copy the content and private key of the server certificate.



Note:

Before copying the content, click Import Sample to view the valid certificate format and private key format. For more information, see [Certificate formats](#).

8. In the left-side navigation pane, click Certificates, and then click Create Certificate to upload a CA certificate.
9. On the Create Certificate page, complete the following configurations and click OK.
 - Regions: In this tutorial, select China (Hangzhou).



Note:

The region of the certificate must be the same as that of the Server Load Balancer instance.

- **Certificate Type:** Select CA Certificate.
- **Certificate Content:** Copy the content of the CA certificate.



Note:

Before copying the content, click Import Sample to view the valid certificate format and private key format. For more information, see [Certificate formats](#).

Step 5 Install client certificates

Install the generated client certificates. The Windows operating system and IE web browser are used as examples in this tutorial.

1. Open the Git Bash command line window, run the following command to export the client certificate generated in step 3.

```
scp root @ IPaddress :/ root / ca / users / client . p12 . /
```



Note:

IPaddress is the IP of the server where the client certificate is generated.

2. Import the certificate to the IE web browser:
 - a. Open the IE web browser, click Settings > Internet Options.
 - b. Click the Content tab, and then click Certificates to import the downloaded client certificate. When importing the certificate, enter the password of the *PKCS12* file.

Step 6 Configure an HTTPS listener (mutual authentication)

1. Log on to the [SLB console](#).
2. Select the China (Hangzhou) region, click the ID of the created SLB instance or click Configure Listener.
3. Select the Listeners tab and click Add Listener.

4. Under the Protocol and Listener tab, configure the listener.

- **Select Listener Protocol: HTTPS**
- **Listening Port: 443**
- **Scheduling Algorithm: Round Robin (RR)**

← Configure Server Load Balancer

1 Protocol and Listener 2 SSL Certificates 3 Backend Servers 4 Health Check 5 Submit

Select Listener Protocol

TCP UDP HTTP **HTTPS**

Backend Protocol

HTTP

* Listening Port ?

443

Advanced Modify

Scheduling Algorithm Session Persistence

Next Cancel

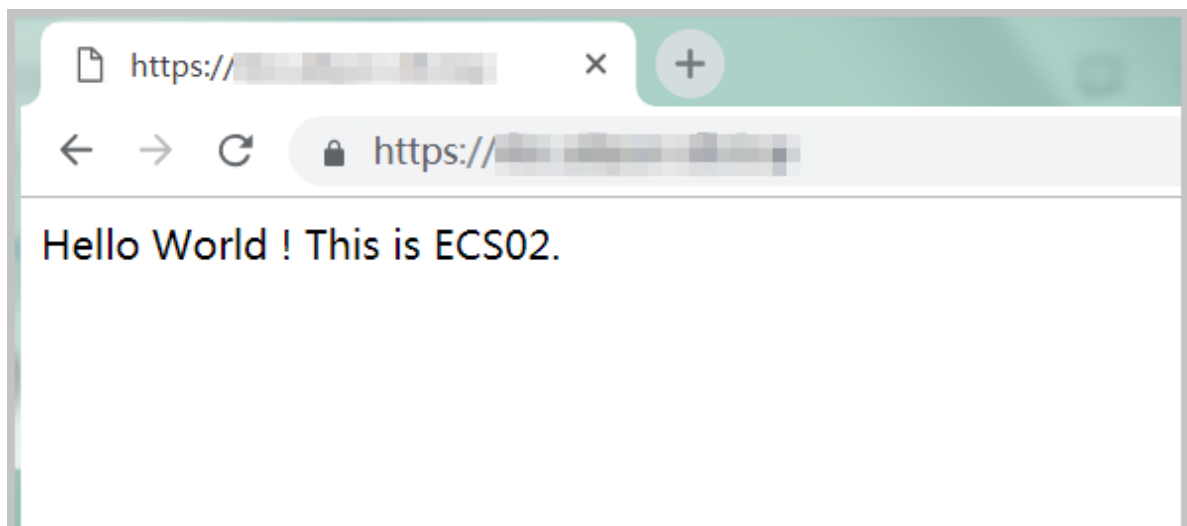
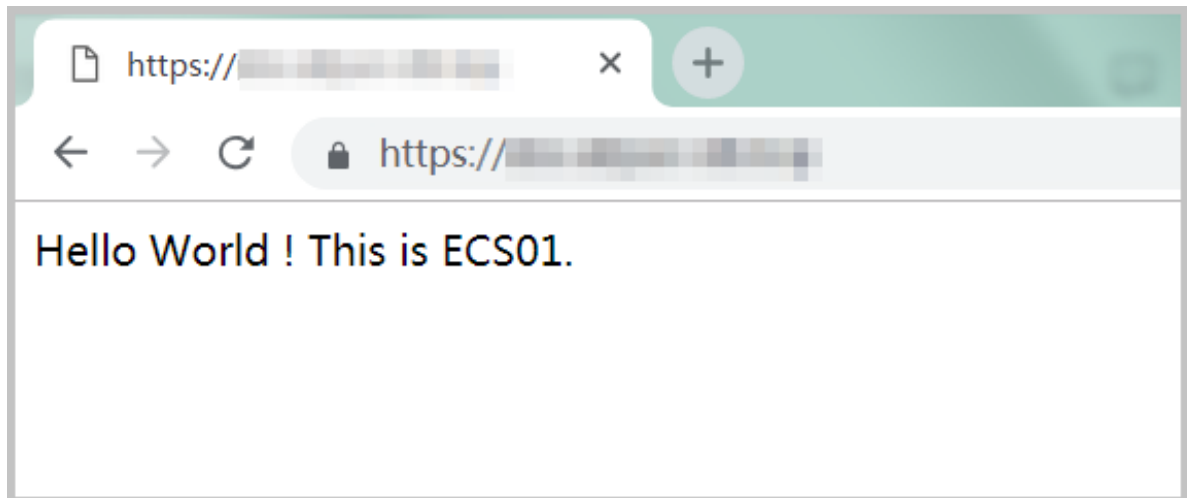
5. Click Next. Under the SSL Certificates tab, configure the SSL certificate and enable mutual authentication.

- **Server Certificate:** Select the uploaded server certificate.
- **CA Certificate:** Select the uploaded CA certificate.

6. Click Next. On the displayed page, click Default Server Group and then click Add. Add ECS instances and set the backend port to 80.**7. Click Next and enable health check.****8. Click Next to view the listener configurations.****9. Click Submit.****10. Click OK.****Step 7 Test the SLB service**

1. Go back to the Server Load Balancer page to view the health check status. When the status is Normal, the backend servers can receive requests forwarded by SLB listeners.
2. Enter the public IP address of the Server Load Balancer instance in the web browser, and select Trust when prompted whether to trust the client certificate.

3. Refresh web page, and then you can find that the requests are evenly distributed to the backend servers.



3 Redirect HTTP to HTTPS

HTTPS is the secure version of HTTP. With HTTPS, the data sent between the browser and the server is encrypted. Server Load Balancer supports redirecting HTTP requests to HTTPS to facilitate whole-site HTTPS deployment. Redirecting HTTP requests to HTTPS is supported in all regions.

Prerequisites

You have created an HTTPS listener. For more information, see [#unique_8](#).

Context

In this tutorial, redirecting HTTP 80 requests to HTTPS 443 is taken as an example.

Procedure

1. Log on to the [SLB console](#).
2. In the top menu, select the region where the SLB instance is located.
3. On the Server Load Balancer page, click the ID of the target SLB instance.
4. Click the Listeners tab and then click Add Listener.
5. In the Configure Server Load Balancer dialog box, select HTTP as the listener protocol and set the listening port to 80.
6. Enable Redirection and select HTTPS:443 as the target port.

← Configure Server Load Balancer

1 Protocol and Listener 2 Submit

Select Listener Protocol

TCP UDP **HTTP** HTTPS

Backend Protocol

HTTP

* Listening Port 80

Advanced Hide

Redirection ☒

Target Port HTTPS:443

Next Cancel

7. Click Next.

8. Confirm and click Submit.

After the redirection function is enabled, all the HTTP requests will be redirected to the HTTPS listener and distributed according to the listener configurations of the HTTPS listener.

| <input type="checkbox"/> | Frontend Protocol/Port | Backend Protocol/Port | Name | Status | Health Status | Monitoring | Forwarding Rule | Session Persistence | Peak Bandwidth | Server Group | Access Control List | Actions |
|--------------------------|------------------------|---|----------|-----------|---------------|----------------------|-----------------|---------------------|----------------|--------------|---------------------|------------------------|
| <input type="checkbox"/> | HTTP:80 | <div> Redirect To HTTPS: 443</div> | http_800 | ✓ Running | - | View | -- | -- | -- | -- | -- | More ✓ |

4 Configure a multi-domain-name HTTPS website on an SLB instance

This tutorial introduces how to configure a domain name extension.

Scenario

This tutorial uses a guaranteed-performance SLB instance (SLB1) in the China (Hangzhou) region as an example. An HTTPS listener with one-way authentication is added to the SLB instance. You want to forward requests from the domain name *.example1.com to the VServer group test1 and forward requests from the domain name www.example2.com to the VServer group test2.

To achieve this, follow these steps:

1. Add an HTTPS listener.
2. Configure forwarding rules.
3. Add a domain name extension.

Prerequisites

- Create a guaranteed-performance SLB instance (SLB1) in China (Hangzhou). For more information, see [#unique_10](#).
- Upload the certificate required in this tutorial. For more information, see [#unique_11](#).
 - By default, the listener uses the certificate named as default.
 - Upload a certificate (example1) for domain name *.example1.com to use.
 - Upload a certificate (example2) for domain name www.example2.com to use.

| Certificates | | | | | | | |
|----------------------------------|----------------|---------------------------------|---------------------|----------------------------|--------------------|-------------------|---------|
| Create Certificate | | Remove All Expired Certificates | | | | | |
| Certificate Name/Certificate ID | Domain Name | Expire At | Associated Listener | Associated Extended Domain | Certificate Type | Source | Actions |
| example1 1231579085529123_... | *.example1.com | May 18, 2019, 14:34:24 | -- | -- | Server Certificate | Uploaded by Users | Delete |
| example2 1231579085529123_... | *.example2.com | May 18, 2019, 14:34:58 | -- | -- | Server Certificate | Uploaded by Users | Delete |
| default 1231579085529123_... | - | Nov 21, 2024, 14:04:25 | | -- | Server Certificate | Uploaded by Users | Delete |

Step 1 Add an HTTPS listener

To add an HTTPS listener, follow these steps:

1. In the left-side navigation pane, click **Instances > Server Load Balancer**.
2. On the Server Load Balancer page, locate the target instance SLB1 and click **Configure Listener** in the Actions column.

If it is the first time you configure the listener, you can also click **Configure** in the **Port/Health Check/Backend Server** column.

3. Configure the listener.

The configurations used in this tutorial are as follows. For more information, see [#unique_8](#).

- **Mutual Authentication:** Disable.
- **SSL Certificate:** Select the uploaded server certificate.
- **Backend Servers:** Create VServer groups test1 and test2.

Step 2 Configure forwarding rules

To configure forwarding rules, follow these steps:

1. Click the ID of the instance SLB1.
2. On the **Listeners** tab, find the created HTTPS listener and click **Add Forwarding Rules**.
3. On the **Add Forwarding Rules** page, configure forwarding rules. For more information, see [#unique_12](#).

In this tutorial, three domain name-based forwarding rules are configured and URLs are left empty.

- Set a rule name, and then enter *.example1.com in the **Domain Name** column, select the VServer group test1 and click **Add Forwarding Rules**.
- Set a rule name, and then enter www.example2.com in the **Domain Name** column, select the VServer group test2 and click **OK**.



Note:

The domain names configured in the forwarding rules must be the same as the domain names added in the certificate and [#unique_13/unique_13_Connect_42_section_bk4_ypt_q2b](#).

Add Forwarding Rules

Domain Name Rule

- Wildcard Domain Name: For example, *.test.com. The asterisk (*) operator must be the initial character of the domain name. The domain name must be in the * or *aaa format.
- Standard domain name: www.test.com

* URL rule:

URLs must be 2-80 characters in length. Only letters a-z, numbers 0-9, and characters '-', '/', '?', '%', '#', and '&' are allowed. URLs must be started with the character '/', but cannot be '/' alone.

* At least one domain name rule or URL rule is required.

Add Forwarding Rules

| Domain Name | URL | VServer Group | Description | Actions |
|--|------------------------|--------------------------------------|--|------------------------|
| <input type="text" value="Example: test.com"/> | / <input type="text"/> | <input type="text" value="test1"/> ▼ | <input type="text" value="Enter a description"/> | Delete |
| + Add Domain | | + Add Rule | | |

Add Forwarding Rules

Forwarding Rules

| Domain Name | URL | VServer Group | Description | Actions |
|------------------|-----|---------------|-----------------|---|
| *.example1.com | / | test1 | auto_named_rule | Edit Delete ⓘ |
| www.example2.com | / | test2 | auto_named_rule | Edit Delete ⓘ |

OK

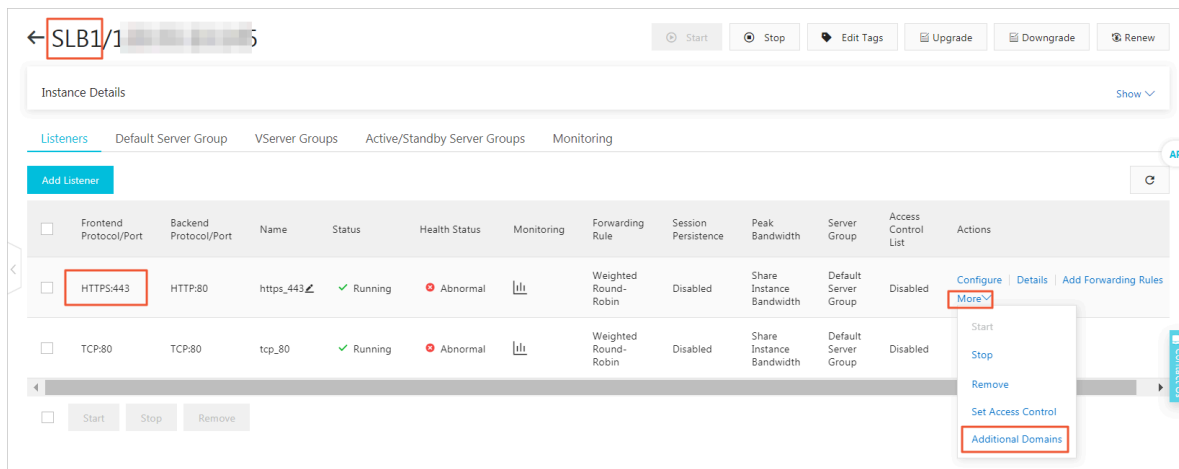
Cancel

Step 3 Add a domain name extension

To add a domain name extension, follow these steps:

1. Click the ID of the instance SLB1.

2. On the Listeners tab, find the created HTTPS listener, choose More > Additional Domains.



3. On the Additional Domains page, click Add Additional Domain to add a domain name extension.

- Enter a domain name. The domain name can only contain letters, numbers, hyphens (-), or periods (.).

Domain name-based forwarding rules support exact match and wildcard match.

- Exact domain name: `www.aliyun.com`
- Wildcard domain name (generic domain name): `*.aliyun.com`, `*.market.aliyun.com`

When a request matches multiple forwarding rules, exact match takes precedence over small-scale wildcard match and small-scale wildcard match takes precedence over large-scale wildcard match, as shown in the following table.

| Type | Request URL | Domain name based forwarding rule | | |
|----------------|--------------------------------|-----------------------------------|---------------------------|----------------------------------|
| | | <code>www.aliyun.com</code> | <code>*.aliyun.com</code> | <code>*.market.aliyun.com</code> |
| Exact match | <code>www.aliyun.com</code> | ✓ | × | × |
| Wildcard match | <code>market.aliyun.com</code> | × | ✓ | × |

| Type | Request URL | Domain name based forwarding rule | | |
|----------------|------------------------|-----------------------------------|--------------|---------------------|
| | | www.aliyun.com | *.aliyun.com | *.market.aliyun.com |
| Wildcard match | info.market.aliyun.com | × | × | √ |

- Select the certificate associated with the domain name.



Note:

The domain name in the certificate must be the same as the added domain name extension.

Additional Domains
×

Add Domain Extension

+ Add Additional Domain

Domain Extensions

| Domain Name | Certificate Name (Domain Name) | Actions |
|------------------|--------------------------------|---------------|
| | default() | |
| *.example1.com | .example1.com(*.example1.com) | Edit Delete |
| www.example2.com | example2(*.example2.com) | Edit Delete |

OK
Cancel



Notice:

After the configuration is complete, if there is a problem, restart the browser to avoid the impact of the cache on the results.

5 Traffic forwarding based on domain names or URLs

Server Load Balancer (SLB) supports domain name-based and URL-based forwarding rules. You can forward requests with different domain names or URLs to different backend servers so that you can optimize the utilization of your server resources.



Note:

Only Layer-7 listeners (HTTP/HTTPS protocol) support forwarding rules.

Introduction to domain name-based and URL-based forwarding rules

Layer-7 listeners support domain name-based and URL-based forwarding rules to distribute requests with different domain names or URLs to different ECS instances.

URL-based forwarding rules support string matching and the rule with the longest matched prefix is applied. For example, if the two forwarding rules /abc and /abcd are created and a request with the prefix of /abcde is received, the rule /abcd is applied.

Domain name-based forwarding rules support exact match and wildcard match.

- Exact domain name: `www.aliyun.com`
- Wildcard domain name (generic domain name): `*.aliyun.com`, `*.market.aliyun.com`

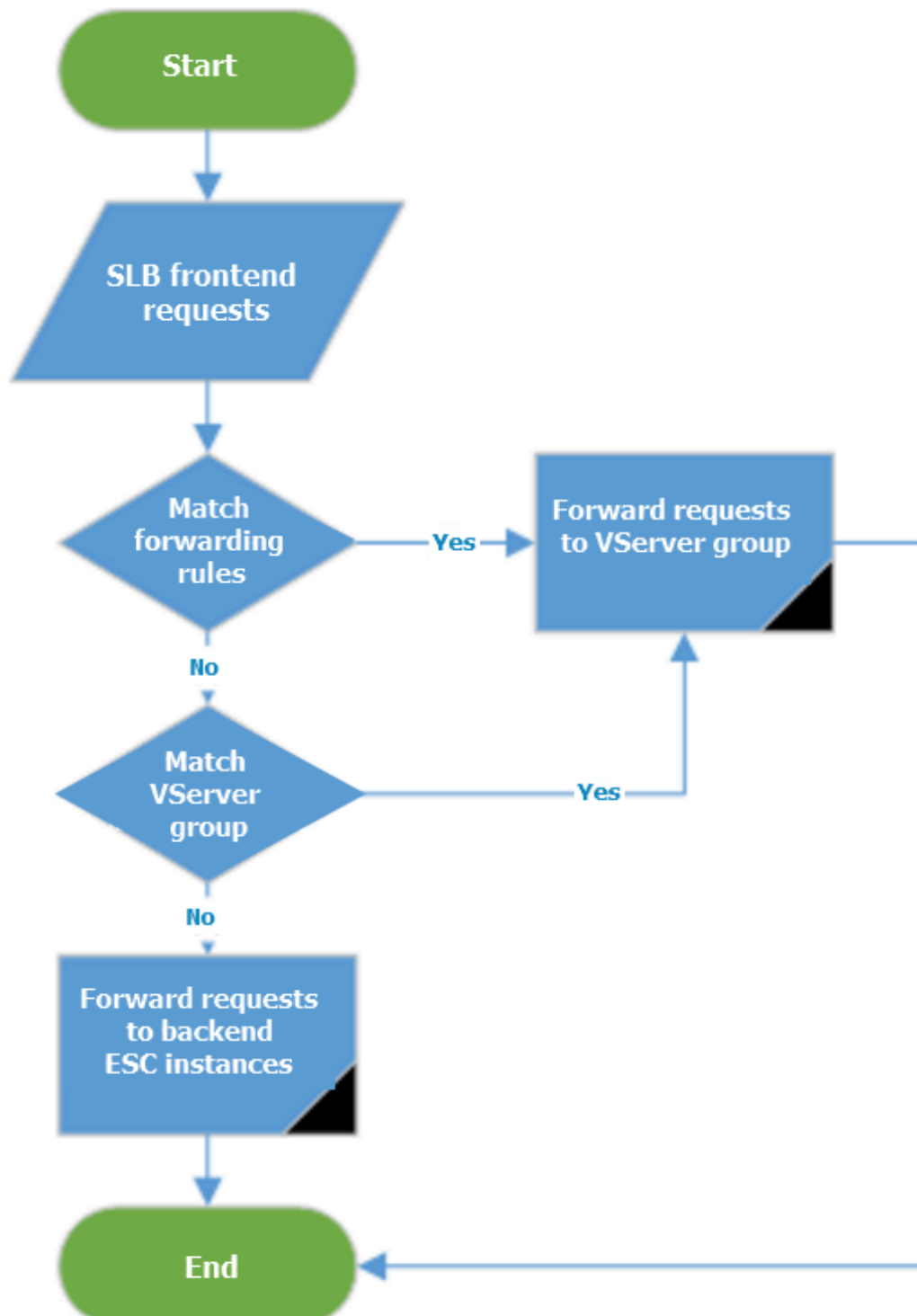
When a request matches multiple forwarding rules, exact match takes precedence over small-scale wildcard match and small-scale wildcard match takes precedence over large-scale wildcard match, as shown in the following table.

| Type | Request URL | Domain name-based forwarding rule | | |
|----------------|-------------------------------------|-----------------------------------|---------------------------|----------------------------------|
| | | <code>www.aliyun.com</code> | <code>*.aliyun.com</code> | <code>*.market.aliyun.com</code> |
| Exact match | <code>www.aliyun.com</code> | ✓ | × | × |
| Wildcard match | <code>market.aliyun.com</code> | × | ✓ | × |
| Wildcard match | <code>info.market.aliyun.com</code> | × | × | ✓ |

You can add different forwarding rules associated with different VServer groups to a Layer-7 listener (a VServer group consists of multiple ECS instances). For example, you can forward all read requests to a VServer group and forward all write requests to another VServer group to optimize resource usage.

After forwarding rules are configured, the sequence of request forwarding is as follows:

- If the requests match a forwarding rule, the requests are distributed to the VServer group associated with the rule.
- If not, but the listener is associated with a VServer group, the requests are distributed to the VServer group configured in the listener.
- If none of the above conditions are met, the requests are forwarded to ECS instances in the default server group.



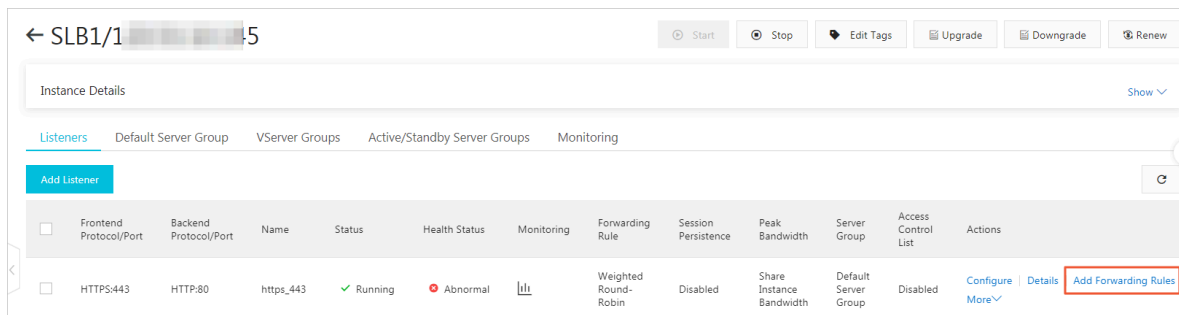
Add a domain name-based or URL-based forwarding rule

Before you add a forwarding rule, make sure that the following conditions are met:

- [#unique_15](#) or [#unique_8](#).
- [Create a VServer group](#).

To add a domain name-based or URL-based forwarding rule, follow these steps:

1. Log on to the [SLB console](#).
2. Select the region of the target SLB instance.
3. Click the ID of the target SLB instance.
4. Click the Listeners tab.
5. Find the target HTTP or HTTPS listener and then click Add Forwarding Rules.



6. On the Add Forwarding Rules page, configure the forwarding rule according to the following information and click Add Forwarding Rules.
 - a. **Domain Name:** Enter the domain name of the requests to be forwarded. The domain name can only contain letters, numbers, hyphens (-), or periods (.).
 - b. **URL:** Enter the path of the requests to be forwarded. The URL must start with a slash (/), and can only contain letters, numbers, and the following special characters: - . / % ? # &



Note:

If you only want to configure a domain name-based forwarding rule, leave the URL empty.

- c. **VServer Group:** Select the VServer group that you want to forward the requests to.
- d. **Description (optional):** Enter a description for the forwarding rule.

Add Forwarding Rules

Domain Name **URL** **VServer Group** **Description** **Actions**

| | | | | |
|------------------|---|-------|---------------------|--------|
| www.example2.com | / | test2 | Enter a description | Delete |
|------------------|---|-------|---------------------|--------|

+ Add Domain + Add Rule

Add Forwarding Rules

Forwarding Rules

| Domain Name | URL | VServer Group | Description | Actions |
|----------------|-----|---------------|-----------------|---------------|
| *.example1.com | / | test1 | auto_named_rule | Edit Delete |

OK Cancel

7. To add another domain name-based or URL-based forwarding rule, click **Add Domain** or **Add Rule**.

For more information, see [#unique_17](#).

8. Click **OK**.

Edit a forwarding rule

You can change the backend servers associated with the forwarding rule.

To edit a forwarding rule, follow these steps:

1. Log on to the [SLB console](#).
2. Select the region of the target SLB instance.
3. Click the ID of the target SLB instance.
4. Click the **Listeners** tab.

5. Find the target HTTP or HTTPS listener and then click **Add Forwarding Rules**.
6. In the Forwarding Rules section, find the target forwarding rule and then click **Edit**.

Add Forwarding Rules

* Domain name rule:

- Wildcard Domain Name: For example, *test.com. The asterisk (*) operator must be the initial character of the domain name. The domain name must be in the * or *aaa format.

- Standard domain name: www.test.com

* URL rule:

URLs must be 2-80 characters in length. Only letters a-z, numbers 0-9, and characters '-' '/' '?' '%' '#' and '&' are allowed. URLs must be started with the character '/', but cannot be '/' alone.

* At least one domain name rule or URL rule is required.

Add Forwarding Rules

| Domain Name | URL | VServer Group | Description | Actions |
|-------------------|------------|---------------|---------------------|---------|
| Example: test.com | / | Select | Enter a description | Delete |
| + Add Domain | + Add Rule | | | |

Add Forwarding Rules

Forwarding Rules

| Domain Name | URL | VServer Group | Description | Actions |
|----------------|-----|---------------|-----------------|-------------|
| *.example1.com | / | test1 | auto_named_rule | Edit Delete |

OK Cancel

7. Edit the forwarding rule. Customize the advanced configurations such as scheduling algorithm, session persistence, and health checks according to the following information:

Note:

Currently, customizing the advanced configurations of a forwarding rule is only supported in the following regions:

- China (Beijing)
- China (Hangzhou)
- China (Shanghai)
- China (Zhangjiakou)
- China (Hohhot)
- China (Hong Kong)
- Singapore

26

Issue: 20190816

· Japan (Tokyo)

| Advanced configurations | Description |
|-------------------------|---|
| Scheduling Algorithm | <p>SLB supports three scheduling algorithms: round robin, weighted round robin (WRR), and weighted least connections (WLC).</p> <ul style="list-style-type: none">• Weighted Round-Robin (WRR): Backend servers with higher weights receive more requests.• Round-Robin (RR): Requests are evenly and sequentially distributed to backend servers.• Weighted Least Connections (WLC): A backend server with a higher weight will receive more requests. When the weight values of two backend servers are the same, the backend server with a smaller number of connections is more likely to be polled. |

| Advanced configurations | Description |
|----------------------------|---|
| Enable Session Persistence | <p>Select whether to enable session persistence.</p> <p>After you enable session persistence, all session requests from the same client are sent to the same backend server.</p> <p>HTTP session persistence is based on cookies. The following two methods are supported:</p> <ul style="list-style-type: none">· Insert cookie: You only need to specify the cookie timeout period. <p>SLB adds a cookie to the first response from the backend server (inserts SERVERID in the HTTP/HTTPS response packet). The next request will contain the cookie and the listener will distribute the request to the same backend server.</p> · Rewrite cookie: You can set the cookie to insert to the HTTP/HTTPS response according to your needs. You must maintain the timeout period and lifecycle of the cookie on the backend server. <p>SLB will overwrite the original cookie when it discovers that a new cookie is set. The next time the client carries the new cookie to access SLB, the listener will distribute the request to the recorded backend server. For more information, see Session persistence.</p> |

| Advanced configurations | Description |
|-------------------------|---|
| Enable Health Check | <ul style="list-style-type: none">• Health Check Port: the port used by health checks to access backend servers. By default, the backend port configured in the listener is used.• Health Check Path: the URI of the health check web page. We recommend that you check a static web page.• Health Check Domain Name (Optional): The intranet IP addresses of backend servers are used as health check domain names by default.• Normal Status Code: the HTTP status code that indicates a healthy server. The default values are http_2xx and http_2xx.• Response Timeout: the amount of time to wait for a response from a health check. If an ECS instance sends no response within the specified timeout period, the health check fails.• Health Check Interval: the amount of time between two consecutive health checks. The default value is 2 seconds.• Unhealthy Threshold: the number of consecutive health check failures performed by the same LVS node server on the same ECS instance (from success to failure) before the ECS instance is declared unhealthy. Value range: 2 to 10. Default value: 3.• Healthy Threshold: the number of consecutive health check successes performed by the same LVS node server on the same ECS instance (from failure to success) before the ECS instance is declared healthy. Value range: 2 to 10. Default value: 3. |

Edit Forwarding Rule

Domain Name

URL

Description

* Select VServer Group:

[Show Details](#)

Advanced Settings



* Scheduling Algorithm

☒ Weighted Round-Robin (WRR)☐ Weighted Least Connections (WLC)☐ Round-Robin (RR)

Enable Session Persistence



Enable Health Check



Health Check Method

HEAD

Health Check Port

Valid range: 1-65535.

Health Check Path

The URI path can be 1 to 80 characters in length and can contain letters, numbers and special characters, including the hyphen (-), underline(_), forward slash (/), period (.), percent sign (%), question mark (?), number sign (#), ampersand (&), and equals sign (=).

Health Check Domain Name (Optional)

Only letters, numbers, hyphens (-), and periods (.) are allowed. If no domains are specified, the internal IP address of each backend server is used as a domain name.

Normal Status Code

☒ http_2xx ☒ http_3xx ☐ http_4xx ☐ http_5xx

* Response Timeout

Seconds

Valid range: 1-300. The default is 5.

* Health Check Interval

Seconds

Valid range: 1-50. The default is 2.

* Healthy Threshold

8. Click OK.**Delete a forwarding rule**

To delete a forwarding rule, follow these steps:

1. Log on to the [SLB console](#).
2. Select the region of the target SLB instance.
3. Click the ID of the target SLB instance.
4. Click the Listeners tab.
5. Find the target HTTP or HTTPS listener, and then click Add Forwarding Rules.

6. In the Forwarding Rules section, find the target forwarding rule and then click Delete.

Add Forwarding Rules



* Domain name rule:

- Wildcard Domain Name: For example, *test.com. The asterisk (*) of the domain name must be in the * or *aaa format.

- Standard domain name: www.test.com

* URL rule:

URLs must be 2-80 characters in length. Only letters a-z, numbers 0-9, and hyphens (-) are allowed, with the character '/', but cannot be '/' alone.

* At least one domain name rule or URL rule is required.

Add Forwarding Rules

| Domain Name | URL |
|--|--------------------------------|
| <input type="text" value="Example: test.com"/> | <input type="text" value="/"/> |
| + Add Domain | + Add Rule |

Add Forwarding Rules

Forwarding Rules

| Domain Name | URL | VServer Group |
|----------------|-----|---------------|
| *.example1.com | / | test1 |

6 Use access logs to rapidly locate abnormal backend servers

When client access delay occurs, you can view the dashboard in Log Service to analyze the response time of the SLB instance to rapidly locate an abnormal backend server.

This tutorial introduces how to use access logs to rapidly locate an abnormal backend server. For more information, see [Configure access logs](#).

Configure access logs

Before you configure access logs, make sure that:

- A Layer-7 listener is added.
- Log Service is activated.

To configure access logs, complete these steps:

1. Log on to the [SLB console](#).
2. In the left-side navigation pane, choose Logs > Access Logs.
3. Select a region.
4. Click Authorize, and then click Confirm Authorization Policy to authorize SLB to write logs to Log Service.

If you are a RAM user, you must obtain permissions from the corresponding account. For more information, see [#unique_21](#).



Note:

This step is required only at the first time.

5. On the Access Logs page, find the target SLB instance and click Configure Logging.
6. Select the LogProject and LogStore and then click OK.

If there is no available LogStore, click Log Service console to create log projects.



Note:

Make sure that the name of the LogProject is globally unique and the region of the LogProject is the same as that of the SLB instance.

Configure Logging

Configure layer-7 access logging.

* LogProject

Select

* LogStore

Select

OK

Cancel

API

Contact Us

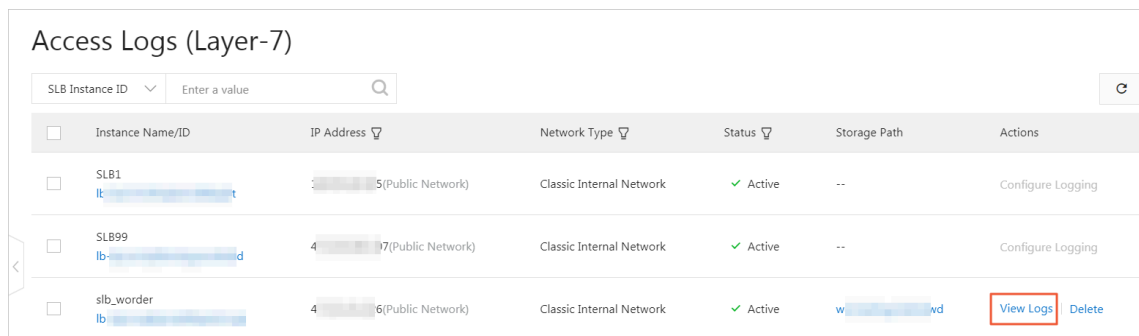
Search access logs

To search access logs, complete these steps:

1. Go to the log search page. You can navigate to the search page from the SLB console or the Log Service Console:

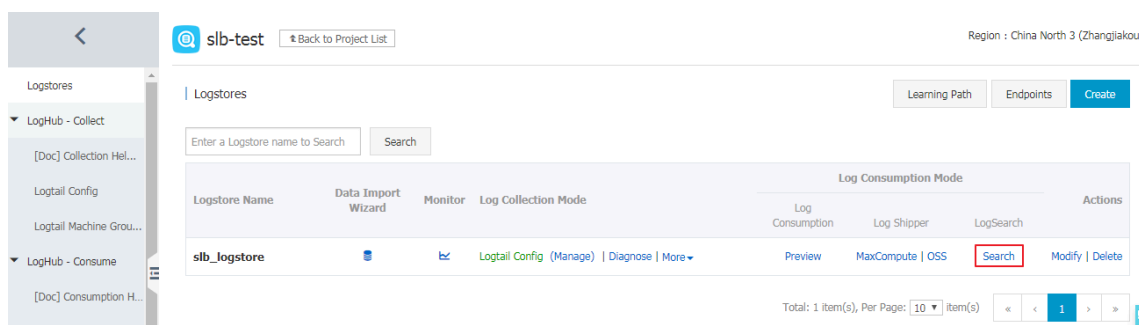
- From the SLB console:

On the Access Logs page, click View Logs.



- From the Log Service Console:

On the Logstores page, click Search of the target Logstore.

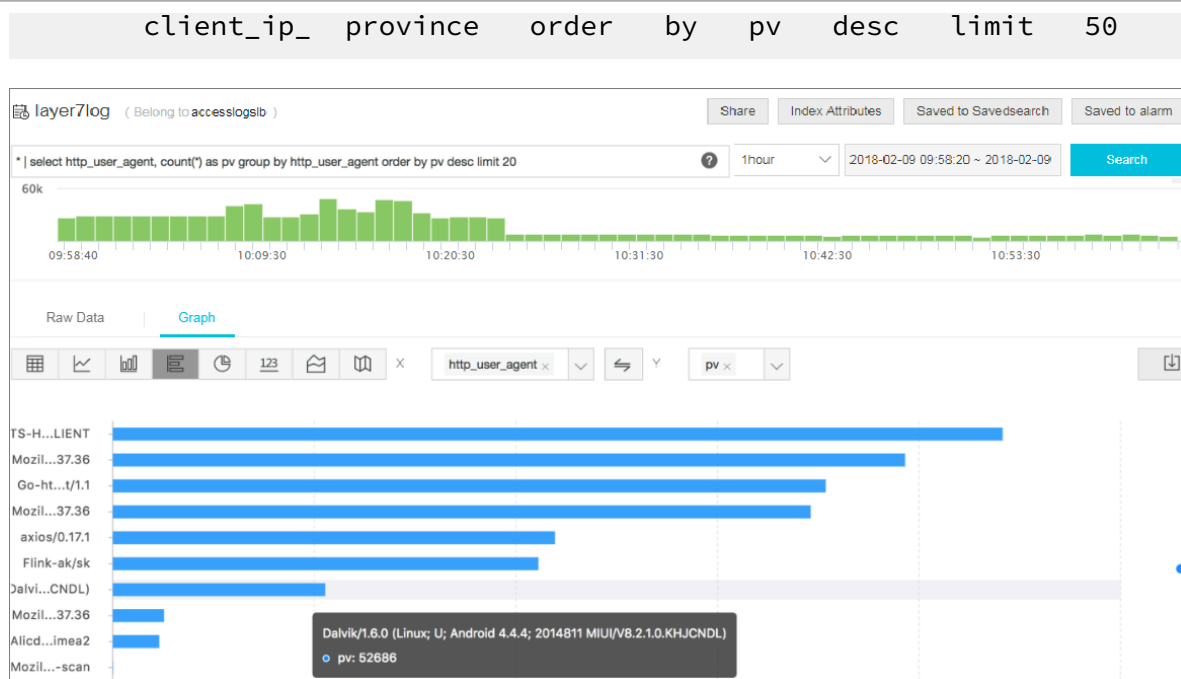


2. Click the target log field to view detailed information.

3. Enter an SQL statement to query access logs.

For example, enter the following SQL statement to query the Top20 clients, which is used for analyzing the request source to assist business decision-making.

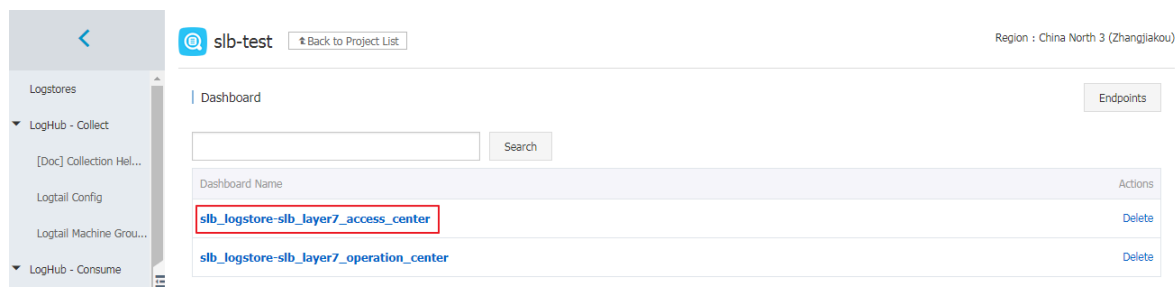
```
* | select ip_to_province ( client_ip ) as client_ip_province , count (*) as pv group by
```



Locate the abnormal backend server

You can locate the abnormal backend server by checking the dashboard of Log Service.

1. On the Log Service console, click the project link of the SLB instance.
2. In the left-side navigation pane, click Search/Analytics - Query > Dashboard.



3. Click the link of the SLB access log.
4. In the dashboard, view the value in the top upstream response time tab. You can select to display the Average upstream response time (s) in descending order to check if the response time of any backend server surpasses 1 second.

If so, run the `ssh` command to log on to the backend server. Check if the CPU has kept running at high levels and handle the high loads.

7 Specify an IP address for an SLB instance with OpenAPI Explorer

This topic describes how to specify an intranet IP address when you create a Server Load Balancer (SLB) instance using OpenAPI Explorer. Specifically, when you create an SLB instance in a VPC network using OpenAPI Explorer, you can specify the IP address used by the CIDR block of the VSwitch where the SLB instance to be created belongs as the intranet IP address of the SLB instance.

Procedure

1. Log on to the [OpenAPI Explorer](#).
2. Search for the `CreateLoadBalancer` API.

3. Configure required parameters.

Some parameters are listed here. For a full list, see [#unique_23](#).

- **RegionId** : the region to which the SLB instance belongs. In this example, select `cn - hangzhou`.
- **VpcId** : the ID of the VPC where the SLB instance belongs.

To view the VPC ID, follow these steps:

- Log on to the VPC console.
- In the upper-left corner, select the region to which the target VPC belongs. In this example, select China (Hangzhou).
- View the target VPC ID from the VPC list.

- **VSwitchId** : the ID of the VSwitch to which the SLB instance belongs. To specify the IP address of the SLB instance, this parameter is required.

To view the ID of the target VSwitch, follow these steps:

- Log on to the VPC console.
- In the upper-left corner, select the region to which the target VPC belongs. In this example, select China (Hangzhou).
- Click the target VPC ID.
- Click the number of VSwitch in the Network Resources area.
- View the VSwitch ID from the VSwitch list.
- To view the destination CIDR block of the VSwitch, click the VSwitch ID. In this example, the destination CIDR block is 192.168.0.0/24.

- **Address** : the intranet IP address of the SLB instance. This IP address must belong to the destination CIDR block of the VSwitch (for example, 192.168.0.3).

4. Click Submit Request.

The response parameters are as follows:

- XML format

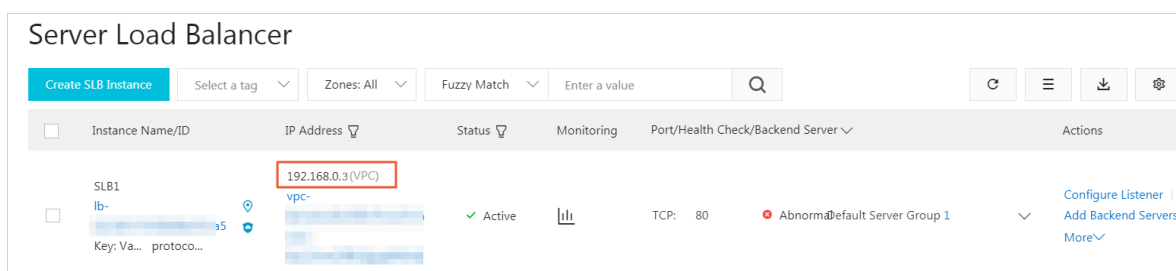
```
<? xml    version =" 1 . 0 "    encoding =" UTF - 8 " ?>
< NetworkType    e > vpc </ NetworkType    e >
< LoadBalanc    erName > auto_named    _slb </ LoadBalanc    erName >
< Address > 192 . 168 . 0 . 3 </ Address >
< ResourceGr    oupId > rg - acfmxazb4p    h6aiy </ ResourceGr    oupId
>
< RequestId > 09197EEB - 7013 - 4F56 - A5CE - A756FFE5B7    5D </
RequestId >
< AddressIPV    ersion > ipv4 </ AddressIPV    ersion >
```

```
< LoadBalancerId > lb - bp1h66tp5u at84khamqc9 e </
LoadBalancerId >
< VSwitchId > vsw - bp14cagpfy sr29feg5t9 7 </ VSwitchId >
< VpcId > vpc - bp18sth14q ii3pnvodkv t </ VpcId >
```

- JSON format

```
{
  "NetworkType": "vpc",
  "LoadBalancerName": "auto_named_slb",
  "Address": "192.168.0.3",
  "ResourceGroupId": "rg-acfmxazb4p-h6aiy",
  "RequestId": "09197EEB-7013-4F56-A5CE-A756FFE5B75D",
  "AddressIPVersion": "ipv4",
  "LoadBalancerId": "lb-bp1h66tp5u-at84khamqc9-e",
  "VSwitchId": "vsw-bp14cagpfy-sr29feg5t9-7",
  "VpcId": "vpc-bp18sth14q-ii3pnvodkv-t"
}
```

5. Log on to the [SLB console](#) and select the China (Hangzhou) region to check whether the SLB instance with the intranet IP address 192.168.0.3 has been created.



8 View traffic usage

You can view the traffic usage of a Server Load Balancer (SLB) instance in a certain period through the SLB console.

Procedure

1. Log on to the [SLB console](#).
2. In the upper-right corner of the top navigation bar, choose Billing Management > Billing Management.
3. In the left-side navigation pane, select Usage Records.

4. On the Usage Records page, select Server Load Balancer (SLB) from the Product Name drop-down list, set a period and measurement cycle, and enter the verification code.

Usage Records

Note:

1. The exported file is in CSV format. You can use a tool like
2. If an error message is displayed during file export, perform
3. If the size of exported records is too large, the file may be
4. Beijing Time (UTC+8) is used when exporting the result.

Product Name :

Server Load Balancer (SLB)

Use Period ? :

2019-04-01

-

20

Unit :

Day

Verification :

HV2Y

 Export CSV

5. Click Export CSV to generate a traffic usage table in the . CSV format.

The table includes the following information. You can view the traffic usage by instance, region or endpoint.

| | A | B | C | D | E | F | G | H | I |
|----|-------------|--------------------|-----------------|-----------------|-----------|---------------------------|-----------------------------|---------------|---------------|
| 1 | Instance ID | Region | Service Address | Service Address | Bandwidth | Upstream traffic (Byte) | Downstream traffic (Byte) | Start Time | End Time |
| 2 | lb- k | cn-hangzhou-dg-a01 | 1 66 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 3 | lb- k | cn-hangzhou-dg-a01 | 1 66 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 4 | lb- 77 | cn-hangzhou-dg-a01 | 1 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 5 | lb- 77 | cn-hangzhou-dg-a01 | 1 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 6 | lb- 3gx | cn-hangzhou-dg-a01 | 1 42 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 7 | lb- 3gx | cn-hangzhou-dg-a01 | 1 42 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 8 | lb- o | cn-hangzhou-dg-a01 | 1 4 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 9 | lb- o | cn-hangzhou-dg-a01 | 1 4 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 10 | lb- 0 | cn-hangzhou-dg-a01 | 1 35 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 11 | lb- 0 | cn-hangzhou-dg-a01 | 1 35 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 12 | lb- 0 | cn-hangzhou-dg-a01 | 1 | internet | 0 | 262302 | 169494 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 13 | lb- 0 | cn-hangzhou-dg-a01 | 1 | internet | 0 | 231549 | 144793 | 2019/4/2 0:00 | 2019/4/3 0:00 |
| 14 | lb- m | cn-hangzhou-dg-a01 | 4 | internet | 0 | 0 | 0 | 2019/4/1 0:00 | 2019/4/2 0:00 |
| 15 | lb- m | cn-hangzhou-dg-a01 | 4 | internet | 0 | 0 | 0 | 2019/4/2 0:00 | 2019/4/3 0:00 |