ALIBABA CLOUD

# Alibaba Cloud

## 负载均衡
## 教程專區

Document Version: 20210226

Alibaba Cloud

# 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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
| Danger | A danger notice 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. |
| Warning | A warning notice 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 restart an instance. |
| Notice | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. | **Notice:** If the weight is set to 0, the server no longer receives new requests. |
| Note | A note indicates supplemental instructions, best practices, tips, and other content. | **Note:** You can use Ctrl + A to select all files. |
| > | Closing angle brackets are used to indicate a multi-level menu cascade. | Click **Settings**> **Network**> **Set network type**. |
| **Bold** | Bold formatting is used for buttons , menus, page names, and other UI elements. | Click **OK**. |
| `Courier font` | Courier font is used for commands | Run the `cd /d C:/window` command to enter the Windows system folder. |
| *Italic* | Italic formatting is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | `switch {active\|stand}` |

# Table of Contents

# 1.CLB

# 2.負載平衡快速入門

本教程介紹什麼是負載平衡以及配置和使用負載平衡的操作步驟，通過視頻的方式直觀的指導您如何通過阿里雲負載平衡將流量分發給後端伺服器。

## 相關文檔

- 什麼是負載平衡
- 教程概述

# 3.使用SLB部署HTTPS業務（單向認證）

要配置HTTPS單向認證的監聽，您僅需要在配置監聽時上傳伺服器憑證。

## 步驟一 上傳伺服器憑證

在配置HTTPS監聽（單向認證）前，您需要購買伺服器憑證，並將伺服器憑證上傳到負載平衡的認證管理系統。上傳後，無需在後端ECS上進行其它認證配置。

1. 登入負載平衡管理主控台。
2. 在左側導覽列，選擇**認證管理**，單擊**建立認證**。
3. 單擊**上傳第三方簽發認證**。
4. 按照以下資訊，配置認證：
   - 認證名稱：長度限制為1-80個字元，只允許包含字母、數字、"-"、"/"、"."、"_"，"*"。
   - 認證部署地區：選擇*華東1*。

     > **說明** 認證的地區和負載平衡執行個體的地區要相同。

   - 認證類型：選擇**伺服器憑證**。
   - 認證內容和私密金鑰：複製伺服器憑證的內容和私密金鑰。單擊**匯入範例**查看合法的認證格式。上傳的認證必須是PEM格式，詳情查看證書要求。
5. 單擊**確定**，完成上傳。

## 步驟二 配置負載平衡執行個體

1. 登入負載平衡管理主控台。
2. 在**執行個體管理**頁面，單擊**建立負載平衡**。
3. 配置負載平衡執行個體，單擊**立即購買**完成支付。

   > **說明** 網路類型選擇**公網**，地區選擇**華東1**。詳細配置資訊參考建立Server Load Balancer執行個體。

4. 建立成功後，返回**執行個體管理**頁面，選擇**華東1**地區。
5. 單擊已建立的負載平衡執行個體ID連結，或者直接單擊**監聽設定嚮導**。
6. 在**監聽**頁簽下，單擊**添加監聽**。
7. 在**協議&監聽**頁簽下，完成如下配置。
   - **選擇負載平衡協議**：HTTPS
   - **監聽連接埠**：443
   - **調度演算法**：輪詢（RR）
8. 單擊**下一步**，在**SSL認證**頁簽下，選擇已經上傳的伺服器憑證和TLS安全性原則。
9. 單擊**下一步**，選擇**預設伺服器組**，單擊**繼續添加**，添加ECS伺服器，後端協議監聽連接埠設定為80。
10. 其他參數保持預設值，單擊**下一步**至**確定**，完成負載平衡執行個體配置。

## 步驟三 測試負載平衡服務

1. 負載平衡執行個體配置完成後，在**執行個體管理**頁面，查看健全狀態檢查狀態。

   當狀態為**正常**時，表示後端伺服器可以正常接收處理負載平衡監聽轉寄的請求。

2. 在瀏覽器中輸入負載平衡的公網服務地址。

# 4.使用SLB部署HTTPS業務（雙向認證）

要配置HTTPS雙向認證的監聽，您需要在配置監聽時上傳伺服器憑證和CA認證。

本指南中使用自簽名的CA認證為用戶端認證簽名，完成以下操作配置HTTPS監聽（雙向認證）：

1. 準備伺服器憑證
2. 使用OpenSSL產生CA認證
3. 產生用戶端認證
4. 上傳伺服器憑證和CA認證
5. 安裝用戶端認證
6. 配置負載平衡雙向認證監聽
7. 測試負載平衡服務

## 步驟一 準備伺服器憑證

伺服器憑證用於使用者瀏覽器檢查伺服器發送的認證是否是由自己信賴的中心簽發的，伺服器憑證可以到阿里雲Apsara Stack Security認證服務購買，也可以到其他服務位址購買。

## 步驟二: 使用OpenSSL產生CA認證

1. 運行以下命令在*/root*目錄下建立一個*ca*檔案夾，並在*ca*檔案夾下建立四個子檔案夾。

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

   其中:

   - *newcerts*目錄將用於存放CA簽署過的數位憑證(認證備份目錄)。
   - *private*目錄用於存放CA的私密金鑰。
   - *conf*目錄用於存放一些簡化參數用的設定檔。
   - *server*目錄存放伺服器憑證檔案。
2. 在*conf*目錄下建立一個包含如下資訊的*openssl.conf*檔案。

```
[ 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. 運行以下命令產生私密金鑰key檔案。

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

運行結果如下圖所示。

4. 運行以下命令並按命令後的樣本提供需要輸入的資訊，然後斷行符號，產生認證請求*csr*檔案。

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

> 說明　Common Name請輸入您的負載平衡服務的網域名稱。

5. 運行以下命令產生憑證*crt*檔案。

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

6. 運行以下命令為CA的key設定起始序號，可以是任意四個字元。

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

7. 運行以下命令建立CA鍵庫。

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

8. 運行以下命令為移除用戶端認證建立一個認證撤銷列表。

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

輸出為：

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

## 步驟三 產生用戶端認證

1. 運行以下命令在*ca*目錄內建立一個存放用戶端key的目錄*users*。

```
$ sudo mkdir users
```

2. 運行以下命令為用戶端建立一個key：

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

> **說明** 建立key時要求輸入pass phrase，這個是當前key的口令，以防止本密鑰泄漏後被人盜用。兩次輸入同一個密碼。

3. 運行以下命令為用戶端key建立一個認證簽章要求*csr*檔案。

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

輸入該命令後，根據提示輸入上一步輸入的pass phrase，然後根據提示，提供對應的資訊。

> **說明** `A challenge password` 是用戶端認證口令（請注意將它和 `client.key` 的口令區分開，本教程設定密碼為test），可以與伺服器端認證或者根憑證口令一致。

4. 運行以下命令使用步驟二中的CA Key為剛才的用戶端key簽名。

```
$ 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"
```

當出現確認是否簽名的提示時，兩次都輸入*y*。

5. 運行以下命令將認證轉換為大多數瀏覽器都能識別的*PKCS12*檔案。

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

按照提示輸入用戶端client.key的pass phrase。

再輸入用於匯出認證的密碼。這個是用戶端認證的保護密碼，在安裝用戶端認證時需要輸入這個密碼。

6. 運行以下命令查看產生的用戶端認證。

```
cd users
ls
```

## 步驟四 上傳伺服器憑證和CA認證

1. 登入負載平衡管理主控台。
2. 在**執行個體管理**頁面，單擊**建立負載平衡**。
3. 配置負載平衡執行個體，單擊**立即購買**完成支付。

   本操作中網路類型選擇**公網**，地區選擇**華東1（杭州）**，詳細配置資訊參考建立Server Load Balancer執行個體。
4. 建立成功後，在**執行個體管理**頁面，將滑鼠移至執行個體名稱地區，單擊出現的鉛筆表徵圖，修改負載平衡執行個體名稱。
5. 在選左側導覽列，單擊**認證管理**頁簽。
6. 單擊**建立認證**。
7. 在**建立認證**頁面，完成如下配置後，單擊**確定**。
   - **認證部署地區**：本教程中選擇**華東1**。

     > **說明** 認證的地區和負載平衡執行個體的地區要相同。

   - **認證類型**：選擇**伺服器憑證**。
   - **認證內容和私密金鑰**：複製您的伺服器憑證內容和私密金鑰。

     > **說明** 在複製內容前，您可以單擊**匯入樣式**，查看正確的認證和私密金鑰格式。更多詳細資料查看證書要求。
8. 在負載平衡左側導覽列，單擊**認證管理**，然後單擊**建立認證**，上傳CA認證。
9. 在**建立認證**頁面，完成如下配置後，單擊**確定**。
   - **認證部署地區**：本教程中選擇**華東1（杭州）**。

     > **說明** 認證的地區和負載平衡執行個體的地區要相同。

   - **認證類型**：選擇**CA認證**。
   - **認證內容**：複製您的CA認證內容。

     > **說明** 在複製內容前，您可以單擊**匯入樣式**，查看正確的認證和私密金鑰格式。更多詳細資料查看證書要求。

## 步驟五 安裝用戶端認證

將產生的用戶端認證安裝到用戶端。本教程以Windows用戶端，IE瀏覽器為例。

1. 開啟Git Bash命令列視窗，運行以下命令匯出步驟三中產生的用戶端認證。

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

   > **說明** IPaddress是產生用戶端認證的伺服器的IP地址。

2. 在IE瀏覽器中匯入下載的用戶端認證。
   i. 開啟IE瀏覽器，單擊**設定** > **Internet選項**。
   ii. 單擊**內容**頁簽，然後單擊**認證**，匯入下載的用戶端認證。在匯入認證時需要輸入在步驟三時產生*PKCS12*檔案的密碼。

## 步驟六 配置HTTPS雙向認證監聽

1. 登入負載平衡管理主控台。
2. 選擇**華東1（杭州）**地區，單擊已建立的負載平衡執行個體ID連結，或者單擊**監聽設定精靈**。
3. 選擇**監聽**頁簽，單擊**添加監聽**。
4. 在**協議&監聽**頁簽下，配置監聽。
   - **選擇負載平衡協議**：HTTPS
   - **監聽連接埠**：443
   - **調度演算法**：輪詢（RR）
5. 單擊**下一步**，在**SSL認證**頁簽下，配置SSL認證資訊，啟用雙向認證。
   - **伺服器憑證**：選擇已上傳的伺服器憑證。
   - **CA認證**： 選擇已上傳的CA認證。
6. 單擊**下一步**，選擇**預設伺服器組**頁簽，單擊**添加**，添加ECS伺服器，並將後端協議連接埠設定為80。
7. 單擊**下一步**，開啟健全狀態檢查。
8. 單擊**下一步**，查看監聽配置資訊。
9. 單擊**提交**，提交審核。
10. 單擊**確定**。

## 步驟七 測試HTTPS雙向認證

1. 在**執行個體管理**頁面，查看健全狀態檢查狀態。當狀態為**正常**時，表示後端伺服器可以正常接收處理負載平衡監聽轉寄的請求。
2. 在瀏覽器中，輸入負載平衡的公網服務地址，當提示是否信任用戶端認證時，選擇信任。
3. 重新整理瀏覽器，您可以觀察到請求在兩台ECS伺服器之間轉換。

# 5.HTTP重新導向至HTTPS

HTTPS是加密資料傳輸協議，安全性高。負載平衡支援將HTTP訪問重新導向至HTTPS，方便您進行全站HTTPS部署。負載平衡已經在全部地區開放了HTTP重新導向功能。

## 前提條件

已建立了HTTPS監聽，詳情參見添加HTTPS監聽。

## 背景信息

> **說明** 僅負載平衡新版控制台支援監聽轉寄功能。

本教程以將HTTP 80訪問重新導向轉寄至HTTPS 443為例。

## 操作步驟

1. 登入負載平衡管理主控台。
2. 在頂部功能表列選擇負載平衡執行個體的所屬地區。
3. 在**執行個體管理**頁面，單擊目標執行個體的ID連結。
4. 在**監聽**頁簽下，單擊**添加監聽**。
5. 在**添加監聽**對話方塊，負載平衡協議選擇**HTTP**， 監聽連接埠輸入**80**。
6. 開啟**監聽轉寄**，選擇目的監聽為**HTTPS:443**。
7. 單擊**下一步**。
8. 確認後，單擊**提交**。

   轉寄開啟後，所有來自HTTP的訪問都會轉寄至HTTPS，並根據HTTPS的監聽配置進行轉寄。

# 6.單SLB執行個體配置多網域名稱HTTPS網站

本教程介紹配置擴充網域名稱的詳細操作步驟。

## 情境描述

本教程以華東1（杭州）地區的效能保障型負載平衡執行個體SLB1為例。在本教程中您會建立一個七層HTTPS監聽，認證方式為單向認證，您需要將來自網域名稱為*.example1.com的前端請求轉寄至虛擬伺服器組test1上，將來自網域名稱為www.example2.com的前端請求轉寄至虛擬伺服器組test2上。

您需要完成以下操作：

1. 添加HTTPS監聽。
2. 配置轉寄規則。
3. 添加擴充網域名稱。

## 前提條件

- 在華東1（杭州）地區建立效能保障型執行個體SLB1，具體操作請參見建立Server Load Balancer執行個體。
- 上傳本教程中需要使用的認證，具體操作請參見生成CA證書。
  - 監聽使用的預設認證為default。
  - 網域名稱*.example1.com使用的認證為example1。
  - 網域名稱www.example2.com使用的認證為example2。

## 步驟一 添加HTTPS監聽

完成以下操作，添加七層HTTPS監聽：

1. 在左側導覽列，選擇**執行個體 > 執行個體管理**。
2. 在**執行個體管理**頁面，單擊效能保障型執行個體SLB1**操作**列的**監聽設定精靈**。

   首次配置監聽，也可以單擊**連接埠/健全狀態檢查/後端伺服器**列的**點我開始配置**。
3. 配置監聽。

   本操作的主要配置如下，其他配置參考添加HTTPS監聽。
   - 雙向認證：關閉。
   - SSL認證：選擇伺服器憑證default。
   - 後端伺服器：需要建立test1和test2兩個虛擬伺服器組。

## 步驟二 配置轉寄規則

完成以下操作，配置轉寄規則：

1. 單擊SLB1執行個體ID，進入**執行個體詳情**頁面。
2. 在**監聽**頁簽下，找到已建立的HTTPS監聽，單擊**添加轉寄策略**。
3. 在**轉寄策略**頁面，配置轉寄策略，詳情請參見基於網域名稱/URL路徑進行轉寄。

   本教程中佈建網域名轉寄規則，URL不進行設定。

- 設定規則名稱，在**網域名稱**操作列輸入*.example1.com，選擇test1虛擬伺服器組，單擊**添加轉寄策略 +**。
- 設定規則名稱，在**網域名稱**操作列輸入www.example2.com，選擇test2虛擬伺服器組，單擊**確認**。

> **說明** 轉寄規則中設定的網域名稱，必須與認證中和步驟三 添加擴充網域名稱中添加的擴充網域名稱保持一致。

## 步驟三 添加擴充網域名稱

完成以下操作，添加擴充網域名稱：

1. 單擊SLB1執行個體ID，進入**執行個體詳情**頁面。
2. 在**監聽**頁簽下，找到已建立的HTTPS監聽，選擇**更多 > 擴充網域名稱管理**。
3. 在**擴充網域名稱管理**頁面，單擊**添加擴充網域名稱**，配置擴充網域名稱。
   - 輸入欄位名。網域名稱只能使用字母、數字、連字號（-）、點（.）。

     網域名稱轉寄策略支援精確匹配和萬用字元匹配兩種模式：
     - 精確網域名稱：www.aliyun.com
     - 萬用字元網域名稱（泛網域名稱）：*.aliyun.com, *.market.aliyun.com

       當前端請求同時匹配多條網域名稱策略時，策略的匹配優先順序為：精確匹配高於小範圍萬用字元匹配， 小範圍萬用字元匹配高於大範圍萬用字元匹配，如下表所示。

| 模式 | 請求測試URL | 配置的轉寄網域名稱策略 | | |
|---|---|---|---|---|
| | | www.aliyun.com | *.aliyun.com | *.market.aliyun.com |
| 精確匹配 | www.aliyun.com | ✓ | × | × |
| 泛網域名稱匹配 | market.aliyun.com | × | ✓ | × |
| 泛網域名稱匹配 | info.market.aliyun.com | × | × | ✓ |

   - 選擇該網域名稱關聯的認證。

     > **說明** 認證中的網域名稱和您添加的擴充網域名稱必須一致。

> **注意** 配置完成後，如果出現問題，請嘗試重啟瀏覽器後再測試，避免緩衝對結果的影響。

# 7.基於網域名稱/URL路徑進行轉寄

負載平衡支援配置基於網域名稱和路徑的轉寄策略。您可以將來自不同網域名稱或路徑的請求轉寄給不同的後端伺服器組，合理分配伺服器資源。

> **說明** 只有7層監聽（HTTPS/HTTP協議）支援配置轉寄策略。

## 網域名稱和路徑轉寄介紹

七層負載平衡服務支援佈建網域名或者URL轉寄策略，將來自不同網域名稱或者URL的請求轉寄給不同的ECS處理。

URL轉寄支援字串匹配，按照首碼最長相符原則，比如有/abc和/abcd兩個規則，訪問/abcde，優先匹配/abcd規則。

網域名稱轉寄策略支援精確匹配和萬用字元匹配兩種模式：

- 精確網域名稱：www.aliyun.com
- 萬用字元網域名稱（泛網域名稱）：*.aliyun.com, *.market.aliyun.com

  當前端請求同時匹配多條網域名稱策略時，策略的匹配優先順序為：精確匹配高於小範圍萬用字元匹配，小範圍萬用字元匹配高於大範圍萬用字元匹配，如下表所示。

| 模式 | 請求測試URL | 配置的轉寄網域名稱策略 | | |
|---|---|---|---|---|
| | | www.aliyun.com | *.aliyun.com | *.market.aliyun.com |
| 精確匹配 | www.aliyun.com | ✓ | × | × |
| 泛網域名稱匹配 | market.aliyun.com | × | ✓ | × |
| 泛網域名稱匹配 | info.market.aliyun.com | × | × | ✓ |

您可以在一個監聽下添加多條轉寄策略，每條轉寄策略關聯不同的虛擬伺服器組（一個虛擬伺服器組由一組ECS執行個體組成）。比如您可以將所有讀請求轉寄到一組後端伺服器上而將寫請求轉寄到另一組後端伺服器上，這樣可以更靈活地適配業務需求，合理分配資源。

如下圖所示，在配置了轉寄策略後，負載平衡系統將按照以下策略轉寄前端請求：

- 如果能匹配到相應監聽關聯的轉寄策略，則按轉寄策略，將請求轉寄到對應的虛擬伺服器組。
- 如果未匹配，而對應監聽啟用並配置了虛擬伺服器組，則將請求轉寄到對應的虛擬伺服器組。
- 如果均未匹配，則轉寄到負載平衡執行個體預設伺服器組中的ECS。

## 添加網域名稱和路徑轉寄策略

完成以下步驟，配置基於網域名稱和路徑的轉寄策略：

1. 登入負載平衡管理主控台。
2. 選擇地區，查看該地區的所有負載平衡執行個體。
3. 單擊負載平衡執行個體的ID。
4. 選擇**監聽**頁簽。

5. 單擊目標七層監聽的**添加轉寄策略**選項。
6. 在**添加轉寄策略**頁簽，根據以下資訊配置轉寄策略：
   i. **網域名稱**：輸入要轉寄的請求網域名稱。網域名稱只能使用字母、數字、連字號（-）、點（.）。
   ii. **URL**：輸入請求路徑。路徑必須以/開頭，只能包含字母、數字和特殊字元（-./%?#&）。

   > **說明** 如果您只想佈建網域名轉寄策略，則不需要配置URL。

   iii. **虛擬伺服器組**：選擇關聯的虛擬伺服器組。
   iv. **備忘**：輸入描述。
   v. 單擊**添加轉寄策略**。
7. 單擊**添加網域名稱**或**添加規則**再添加一個網域名稱或URL策略。

   一個HTTP或HTTPS監聽最多可添加轉寄策略個數請參見使用限制。

## 編輯轉寄策略

您可以修改轉寄策略關聯的後端伺服器。

完成以下操作，編輯轉寄策略：

1. 登入負載平衡管理主控台。
2. 選擇地區，查看該地區的所有負載平衡執行個體。
3. 單擊負載平衡執行個體的ID。
4. 選擇**監聽**頁簽。
5. 單擊目標七層監聽的**添加轉寄策略**選項。
6. 在**轉寄策略列表**地區，單擊目標轉寄策略的**編輯**選項。
7. 編輯轉寄策略，根據以下資訊自訂轉寄策略的調度演算法、會話保持和健全狀態檢查等配置。

   > **說明** 當前僅支援在以下地區自訂已有轉寄策略的進階配置：
   > - 華北2（北京）
   > - 華東1（杭州）
   > - 華東2（上海）
   > - 華北3（張家口）
   > - 華北5（呼和浩特）
   > - 香港
   > - 新加坡
   > - 日本

| 進階配置 | 說明 |
| --- | --- |

| 進階配置 | 說明 |
| --- | --- |
| **調度演算法** | 負載平衡支援輪詢、加權輪詢（WRR）、加權最小串連數（WLC）三種調度演算法。<br>○ **加權輪詢**：權重值越高的後端伺服器，被輪詢到的次數（機率）也越高。<br>○ **輪詢**：按照訪問順序依次將外部請求依序分發到後端伺服器。<br>○ **加權最小串連數**：除了根據每台後端伺服器設定的權重值來進行輪詢，同時還考慮後端伺服器的實際負載（即串連數）。當權重值相同時，當前串連數越小的後端伺服器被輪詢到的次數（機率）也越高。 |
| **開啟會話保持** | 選擇是否開啟會話保持。<br>開啟會話保持功能後，負載平衡會把來自同一用戶端的訪問請求分發到同一台後端伺服器上進行處理。<br>HTTP協議會話保持基於Cookie。負載平衡提供了兩種Cookie處理方式：<br>○ **植入Cookie**：您只需要指定Cookie的到期時間。<br>用戶端第一次訪問時，負載平衡會在返回請求中植入Cookie（即在HTTP/HTTPS響應報文中插入SERVERID），下次用戶端攜帶此Cookie訪問，負載平衡服務會將請求定向轉寄給之前記錄到的後端伺服器上。<br>○ **重寫Cookie**：可以根據需要指定HTTPS/HTTP響應中插入的Cookie。您需要在後端伺服器上維護該Cookie的到期時間和存留時間。<br>負載平衡服務發現使用者自訂了Cookie，將會對原來的Cookie進行重寫，下次用戶端攜帶新的Cookie訪問，負載平衡服務會將請求定向轉寄給之前記錄到的後端伺服器。詳情參考會話保持規則配置。 |
| **開啟健全狀態檢查** | ○ **健全狀態檢查連接埠**：健全狀態檢查服務訪問後端時的探測連接埠。<br>預設值為配置監聽時指定的後端連接埠。<br>○ **健全狀態檢查路徑**：用於健全狀態檢查分頁檔的URI，建議對靜態頁面進行檢查。<br>○ **健全狀態檢查網域名稱（可選）**：預設使用各後端伺服器的內網IP為網域名稱。<br>○ **正常狀態代碼**：選擇健全狀態檢查正常的HTTP狀態代碼。<br>預設值為http_2xx和http_3xx。<br>○ **健全狀態檢查響應逾時時間**：接收來自健全狀態檢查的響應需要等待的時間。如果後端ECS在指定的時間內沒有正確響應，則判定為健全狀態檢查失敗。<br>○ **健全狀態檢查間隔時間**：進行健全狀態檢查的時間間隔。<br>預設為2秒。<br>○ **健康不檢查健康閾值**：同一LVS節點伺服器針對同一ECS伺服器，從成功到失敗的連續健全狀態檢查失敗次數。<br>可選值2-10，預設為3次。<br>○ **健全狀態檢查健康閾值**：同一LVS節點伺服器針對同一ECS伺服器，從失敗到成功的連續健全狀態檢查成功次數。<br>可選值2-10，預設為3次。 |

8. 單擊**確定**。

## 刪除轉寄策略

完成以下操作，刪除轉寄策略：

1. 登入負載平衡管理主控台。
2. 選擇地區，查看該地區的所有負載平衡執行個體。
3. 單擊負載平衡執行個體的ID。
4. 選擇**監聽**頁簽。
5. 單擊目標七層監聽的**添加轉寄策略**選項。
6. 在**轉寄策略列表**地區，單擊目標轉寄策略的**刪除**選項。

# 8.獲取用戶端真實IP

## 負載平衡服務獲取真實IP說明

負載平衡提供獲取用戶端真實IP地址的功能，該功能預設是開啟的。

- 四層負載平衡（TCP協議）服務可以直接在後端ECS上獲取用戶端的真實IP地址，無需進行額外的配置。
- 七層負載平衡（HTTP/HTTPS協議）服務需要對應用伺服器進行配置，然後使用 `X-Forwarded-For` 的方式獲取用戶端的真實IP地址。

  真實的用戶端IP會被負載平衡放在HTTP頭部的X-Forwareded-For欄位，格式如下：

  ```
  X-Forwarded-For: 使用者真實IP, Proxy 伺服器1-IP， Proxy 伺服器2-IP，...
  ```

  當使用此方式獲取用戶端真實IP時，獲取的第一個地址就是用戶端真實IP。

  > **說明** 負載平衡的HTTPS監聽是在負載平衡服務上的加密控制，後端仍舊使用HTTP協議，因此，在Web應用伺服器配置上HTTPS和HTTP監聽沒有區別。

## 配置IIS7/IIS8伺服器

1. 下載並解壓 *F5XForwardedFor*檔案。
2. 根據自己的伺服器作業系統版本將*x86\Release*或者 *x64\Release*目錄下的 *F5XFFHttpModule.dll*和 *F5XFFHttpModule.in*拷貝到某個目錄，比如 *C:\F5XForwardedFor*\。確保IIS進程對該目錄有讀取許可權。
3. 開啟**IIS管理器**，雙擊**模組**功能。
4. 單擊**配置本機模組**，然後在彈出的對話方塊中，單擊**註冊**。
5. 添加下載的*.dll*檔案。
6. 為添加的兩個檔案授權允許運行ISAPI和CGI擴充。

   > **說明** 確保您已經安裝了ISAPI和CGI應用程式。

7. 重啟IIS伺服器，等待配置生效。

## 配置Apache伺服器

1. 運行以下命令安裝Apache的一個第三方模組mod_rpaf。

   ```
   wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
   tar zxvf mod_rpaf-0.6.tar.gz
   cd mod_rpaf-0.6
   /alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
   ```

2. 修改Apache的設定檔*/alidata/server/httpd/conf/httpd.conf*，在最末尾添加以下配置資訊。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips <IP_address>
RPAFheader X-Forwarded-For
```

> 說明 如果您要獲取Proxy 伺服器的地址，可以將Proxy 伺服器的網段添加到 RPAFproxy_ips <IP_address> ，如負載平衡的IP地址段和高防IP地址段。多個IP地址段用逗號分隔。

3. 添加完成後重啟Apache。

```
/alidata/server/httpd/bin/apachectl restart
```

## 配置Nginx伺服器

1. 運行以下命令安裝http_realip_module。

```
wget http://nginx.org/download/nginx-1.0.12.tar.gz
tar zxvf nginx-1.0.12.tar.gz
cd nginx-1.0.12
./configure --user=www --group=www --prefix=/alidata/server/nginx --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. 開啟*nginx.conf*檔案。

```
vi /alidata/server/nginx/conf/nginx.conf
```

3. 在以下配置資訊後添加新的配置欄位和資訊。

```
fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;
```

需要添加的配置欄位和資訊為：

```
set_real_ip_from IP_address
real_ip_header X-Forwarded-For;
```

> **說明** 如果您要獲取Proxy 伺服器的地址，可以將Proxy 伺服器的網段添加到 `set_real_ip_from <IP_address>`，如負載平衡的IP地址段和高防IP地址段。多個IP地址段用逗號分隔。

4. 重啟Nginx。

```
/alidata/server/nginx/sbin/nginx -s reload
```

# 9.如何進行壓力測試

## 壓力測試效能概述

四層負載平衡採用開源軟體LVS（Linux Virtual Server）+ Keepalived的方式實現負載平衡，七層負載平衡由Tengine實現。其中四層監聽經過LVS後直接到達後端伺服器，而七層監聽經過LVS後，還需要再經過Tengine，最後達到後端伺服器。七層比四層多了一個處理環節，因此，七層效能沒有四層效能好。

如果您使用七層監聽進行壓來測試，發現根本跑不上去，掛了兩台ECS的七層負載平衡監聽效能還不如一台ECS的效能，除了七層本身的效能比四層低外，以下情況也可能會造成七層測壓效能低：

- 用戶端通信埠不足

  尤其容易發生在壓測的時候，用戶端通信埠不足會導致建立串連失敗，負載平衡預設會抹除TCP串連的timestamp屬性，Linux協議棧的tw_reuse(time_wait 狀態串連複用)無法生效，time_wait狀態串連堆積導致用戶端通信埠不足。

  解決方法：用戶端端使用長串連代替短串連。使用RST報文中斷連線（socket設定SO_LINGER屬性），而不是發FIN包這種方式斷開。

- 後端伺服器accept隊列滿

  後端伺服器accept隊列滿，導致後端伺服器不回複syn_ack報文，用戶端逾時

  解決方法：預設的net.core.somaxconn的值為128，執行 `sysctl -w net.core.somaxconn=1024` 更改它的值，並重啟後端伺服器上的應用。

- 後端伺服器串連過多

  由於架構設計的原因，使用七層負載平衡時，使用者長串連經過Tengine後變成短串連，可能造成後端伺服器串連過多，從而表現為壓測效能上不去。

- 後端伺服器依賴的應用成為瓶頸

  請求經過負載平衡達到後端伺服器後，後端伺服器本身負載都正常，但由於所有的後端伺服器上的應用又依賴其它應用，比如資料庫，資料庫成為瓶頸，也會引起效能低。

- 後端伺服器的健康檢查狀態異常

  尤其在壓測的時候容易忽略後端伺服器的健康檢查狀態，如果有後端伺服器健康檢查失敗或者健康檢查狀態經常跳躍（好到壞，又從壞到好，反覆變化）也會導致效能跑不上去。

## 壓力測試建議

在進行壓力測試，注意如下配置：

- 壓測負載平衡轉寄能力建議使用短連結

  一般來說壓測除了驗證會話保持，均衡性等功能外，主要想驗證的是負載平衡的轉寄能力，因此使用短連結比較合適，用於測試負載平衡和後端伺服器處理能力。但使用短串連測試時注意上述的用戶端通信埠不足問題。

- 壓測負載平衡輸送量建議使用長串連，用於測試頻寬上限或特殊業務

  壓測工具的逾時時間建議設定為一個較小值（5秒）。逾時時間太大的話，測試結果會體現在平均RT加長，不利於判斷壓測水位是否已到達。逾時時間調小，測試結果會體現在成功率上，便於快速判斷壓測水位。

- 後端伺服器提供一個靜態網頁用於壓測，以避免應用邏輯帶來的損耗
- 壓測時，監聽配置建議如下：

- 不開啟會話保持功能，否則壓力會集中在個別的後端伺服器。
- 監聽關閉健康檢查功能，減少健康檢查請求對後端伺服器的訪問請求。
- 用多個用戶端進行進行壓測最好多於5個，源IP分散，能夠更好的類比線上實際情況。

## 壓力測試工具建議

不建議您使用Apache ab作為壓力測試工具。

Apache ab在大量並發場景下存在3s，6s，9s階梯式停頓的現象。Apache ab會通過判斷content length來確定請求是否成功，而負載平衡掛載多台後端伺服器時，返回的content length會不一致，導致測試結果有誤。

建議使用阿里雲PTS。

可以選擇多個用戶端作為壓力測試源，測試結果清晰，並且可以通過配置監控，獲取壓力測試時後端伺服器的效能資料。

## 使用PTS簡單壓測樣本

建立一個負載均執行個體，添加兩台ECS執行個體作為後端伺服器，分別建立一個TCP監聽和HTTP監聽，後端通信埠設定為80。ECS伺服器的配置為CPU 1核，記憶體512M使用CentOS 6.3 64位的作業系統。

1. 安裝Apache Web Server提供Web服務。

   ```
   yum install -y httpd
   ```

2. 初始化預設首頁index.html。

   ```
   echo "testvm" > /var/www/html/index.html
   ```

3. 啟動HTTP服務。

   ```
   service httpd start
   ```

4. 訪問本地的80通信埠，確認Web服務可用。

   ```
   curl localhost
   ```

5. 在PTS中建立測試指令碼，開始壓力測試。

   注意關閉長串連和設定逾時時間：

   - 設定逾時時間為5秒： PTS.HttpUtilities.setTimeout(5000)
   - 關閉長串連： PTS.HttpUtilities.setKeepAlive(False)

# 10.使用訪問日誌快速定位異常後端伺服器

某段時間用戶端訪問延遲時，您可以結合阿里雲Log Service，通過儀錶盤巡檢，分析負載平衡的回應時間，快速定位異常後端伺服器。

本教程介紹如何使用訪問日誌快速定位異常後端伺服器，更多訪問日誌詳情請參見配置訪問日誌。

## 配置負載平衡訪問日誌

在配置訪問日誌前，確保：

1. 您已經建立了七層負載平衡。
2. 您已經開通了Log Service。

完成以下操作，配置訪問日誌：

1. 登入負載平衡管理主控台。
2. 在左側導覽列，選擇 **日誌管理 > 訪問日誌** 。
3. 選擇執行個體的所屬地區。
4. 單擊**立即授權**，然後在彈出的對話方塊，單擊**同意授權**授權SLB訪問Log Service。

   如果您使用的是子帳號，需要主帳號進行授權。

   > **說明** 該操作只有首次配置時需要。

5. 在**訪問日誌**頁面，找到目標SLB執行個體，然後單擊**設定**。
6. 選擇Log Service（LogProject）和日誌庫（LogStore），然後單擊**確認**。

   如果沒有可用的LogStore，單擊**前往SLS建立Store**。

   > **說明** 確保Project的名稱全域唯一，且Project的地區和負載平衡執行個體的地區相同。

## 查詢訪問日誌

完成以下操作，查詢訪問日誌：

1. 進入日誌查詢頁面。您可以通過負載平衡控制台和Log Service控制台進入日誌查詢頁面。
   - 負載平衡控制台

     在**訪問日誌**頁面，單擊**查看日誌**。
   - Log Service控制台

     在**日誌庫**頁面，單擊SLB日誌庫的**查詢**選項。
2. 單擊目標日誌欄位，查看對應的日誌資訊。
3. 輸入SQL語句查詢特定的訪問日誌。

   比如輸入如下SQL語句查詢Top20的用戶端，用於分析請求訪問來源，輔助商業決策。

```
* | select ip_to_province(client_ip) as client_ip_province, count(*) as pv group by
  client_ip_province order by pv desc limit 50
```

## 查詢訪問日誌

完成以下操作，查詢訪問日誌：

1. 進入日誌查詢頁面。您可以通過負載平衡控制台和Log Service控制台進入日誌查詢頁面。
   - 負載平衡控制台

     在**訪問日誌**頁面，單擊**查看日誌**。
   - Log Service控制台

     在**日誌庫**頁面，單擊SLB日誌庫的**查詢**選項。
2. 單擊目標日誌欄位，查看對應的日誌資訊。
3. 輸入SQL語句查詢特定的訪問日誌。

   比如輸入如下SQL語句查詢Top20的用戶端，用於分析請求訪問來源，輔助商業決策。

   ```
   * | select ip_to_province(client_ip) as client_ip_province, count(*) as pv group by
     client_ip_province order by pv desc limit 50
   ```

   \

## 定位異常後端伺服器

您可以通過Log Service的儀錶盤定位異常後端伺服器。

1. 在Log Service控制台，單擊負載平衡的Project連結。
2. 在左側導覽列，單擊**Search/Analytics - 查詢分析 > 儀錶盤**。
3. 單擊負載平衡訪問日誌的名稱連結。
4. 在儀錶盤中，查看**top upstream回應時間**頁簽下Server Load Balancer的回應時間，可以將參數**平均upstream回應時間(s)**設定降序排列，查看是否有後端伺服器的回應時間超過1s。

   如果有回應時間超過1s的後端伺服器，執行**ssh**命令，登入該後端伺服器，查看CPU是否持續高位運行，進行高負載處理。

# 11.配置存取控制

通過視頻模式介紹配置存取控制的詳細操作步驟，負載平衡提供監聽層級的存取控制，您可以為不同的監聽配置不同的存取控制策略。

# 12.通過OpenAPI Explorer建立VPC類型執行個體時指定IP

使用APIexplorer建立VPC類型負載平衡執行個體時，支援在負載平衡執行個體所屬交換器支援的網段中，指定其中一個地址作為負載平衡執行個體的私網IP地址。

## 操作步驟

1. 登入OpenAPI Explorer控制台。
2. 搜尋負載平衡產品的CreateLoadBalancer介面。
3. 設定建立負載平衡執行個體的參數。 此處設定部分參數作為樣本，詳細參數說明參見CreateLoadBalancer：
   - RegionId：表示負載平衡執行個體的地區，此處設定為*cn-hangzhou*。
   - VpcId：表示負載平衡執行個體所屬VPC的ID。

     此處可登入Virtual Private Cloud控制台，選擇華東1（杭州）地區，查看VPC的ID。
   - VSwitchId：表示負載平衡所屬交換器的ID，如果需要指定負載平衡IP地址，該參數必須要設定。

     此處可在Virtual Private Cloud控制台，單擊負載平衡執行個體所屬VPC的ID，在**網路資源**頁面下，單擊交換器的個數，查看交換器的ID。

     單擊交換器ID，查看交換器的目標網段，如192.168.0.0/24。
   - Address：指定負載平衡執行個體的私網IP地址，該地址必須包含在交換器的目標網段下，如192.168.0.3。
4. 單擊**發送請求**。 返回結果如下：
   - XML格式

     ```
     <?xml version="1.0" encoding="UTF-8" ?>
     <NetworkType>vpc</NetworkType>
     <LoadBalancerName>auto_named_slb</LoadBalancerName>
     <Address>192.168.0.3</Address>
     <ResourceGroupId>rg-acfmxazb4ph6aiy</ResourceGroupId>
     <RequestId>09197EEB-7013-4F56-A5CE-A756FFE5B75D</RequestId>
     <AddressIPVersion>ipv4</AddressIPVersion>
     <LoadBalancerId>lb-bp1h66tp5uat84khmqc9e</LoadBalancerId>
     <VSwitchId>vsw-bp14cagpfysr29feg5t97</VSwitchId>
     <VpcId>vpc-bp18sth14qii3pnvodkvt</VpcId>
     ```
   - JSON格式

```
{
  "NetworkType": "vpc",
  "LoadBalancerName": "auto_named_slb",
  "Address": "192.168.0.3",
  "ResourceGroupId": "rg-acfmxazb4ph6aiy",
  "RequestId": "09197EEB-7013-4F56-A5CE-A756FFE5B75D",
  "AddressIPVersion": "ipv4",
  "LoadBalancerId": "lb-bp1h66tp5uat84khmqc9e",
  "VSwitchId": "vsw-bp14cagpfysr29feg5t97",
  "VpcId": "vpc-bp18sth14qii3pnvodkvt"
}
```


5. 登入負載平衡管理主控台，選擇華東1（杭州）地區，查看IP為192.168.0.3的負載平衡執行個體是否建立成功。

# 13.查看流量使用方式

使用者需要查看某一時間段內雲帳號下負載平衡執行個體流量使用方式。

## 操作步驟

1. 登入負載平衡控制台。
2. 在功能表列右上方選擇 **費用 > 進入費用中心**。
3. 在**費用中心**頁面，選擇 **消費記錄 > 使用記錄**。
4. 在**使用記錄**頁面，選擇**負載平衡**產品，配置需要查看的負載平衡流量使用方式的使用期間和計量粒度。
5. 單擊**匯出CSV**，在本地產生 *.CSV*格式的流量使用表格。 該表格包含以下資訊，可根據執行個體、地區或者服務地址等查看具體流量使用方式。