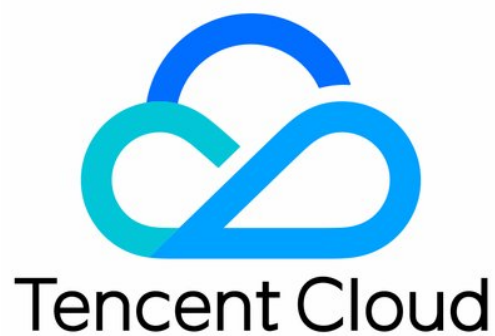


Cloud Load Balancer

Panduan Pengoperasian

Dokumen produk



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Direktori dokumen

Panduan Pengoperasian

Instance CLB

- Membuat Instance CLB
- Membuat Instance CLB IPv6
- Membuat Instance CLB IPv6 NAT64
- Membuat Instance Anycast
- Mengonfigurasi Grup Keamanan CLB
- Mengekspor Instance CLB
- Menghapus Instance CLB
- Menyesuaikan Konfigurasi Jaringan Publik Instance

Pendengar CLB

- Ikhtisar Pendengar CLB
- Mengonfigurasi Pendengar TCP
- Mengonfigurasi Pendengar UDP
- Mengonfigurasi Pendengar TCP SSL
- Mengonfigurasi Pendengar HTTP
- Mengonfigurasi Pendengar HTTPS
- Metode Penyeimbangan Beban
- Persistensi Sesi
- Mengonfigurasi Pengalihan Lapisan 7
- Konfigurasi Khusus Lapisan 7
- Aturan Penerusan dan URL Nama Domain Lapisan 7
- Menggunakan Protokol QUIC di CLB
- Dukungan SNI untuk Mengikat Beberapa Sertifikat ke Instance CLB

Server Asli

- Ikhtisar Server Asli
- Mengelola Server Asli
- Mengikat ENI
- Mengikat dengan SCF
- Pengikatan Lintas Wilayah 2.0 (Baru)
- Deployment Cloud Hibrida
- Konfigurasi Grup Keamanan pada Server Asli

Pemeriksaan Kesehatan

- Ikhtisar Pemeriksaan kesehatan
- Konfigurasi Pemeriksaan Kesehatan

Pengelolaan Sertifikat

Mengelola Sertifikat

Persyaratan Sertifikat dan Konversi Format Sertifikat

Autentikasi Satu Arah dan Autentikasi Bersama SSL

Pengelolaan Log

Ikhtisar Log Akses

Melihat Log Operasi

Mengonfigurasi Log Akses

Pemantauan dan Peringatan

Mendapatkan Data Pemantauan

Metrik Pemantauan

Mengonfigurasi Peringatan

Deskripsi Metrik Peringatan

Cloud Access Management

Ikhtisar

Definisi Otorisasi

Contoh Kebijakan

CLB Klasik

Ikhtisar CLB Klasik

Mengonfigurasi CLB Klasik

Mengelola Server Asli dari Instance CLB Klasik

Panduan Pengoperasian Instance CLB

Membuat Instance CLB

Waktu update terbaru : 2024-01-04 20:53:33

Tencent Cloud memungkinkan Anda membuat instance CLB di halaman pembelian resmi atau melalui API. Di bawah ini adalah perincian kedua metode tersebut:

Membuat instance CLB di halaman pembelian resmi

Anda bisa membeli satu instance CLB pada [Situs web resmi Tencent Cloud](#). Instance CLB jaringan pribadi tidak dikenai biaya, sementara instance CLB jaringan publik dikenai biaya instance per jam sesuai pemakaian. Anda bisa membeli jaringan publik pada [CVM](#). Untuk informasi selengkapnya tentang cara penagihan jaringan, silakan lihat [Penagihan Jaringan Publik](#).

Untuk metode pembelian akun tagihan per CVM, silakan lihat [Metode Pembelian](#). Bagi pengguna akun tagihan per IP, langkah pembeliannya adalah sebagai berikut:

1. Masuk ke konsol Tencent Cloud dan buka [halaman pembelian CLB](#).
2. **Cloud Load Balancer** (Penyeimbang Beban Cloud) direkomendasikan untuk **Instance type** (Jenis instance).
3. Pilih atribut sesuai kebutuhan, termasuk jenis jaringan dan proyek. Untuk detail atribut, silakan lihat [Pilihan Atribut Produk](#).

Keterangan :

Pengujian beta IP jalur tunggal statis hanya tersedia di Jinan, Hangzhou, Fuzhou, Shijiazhuang, Wuhan, dan Changsha. Silakan hubungi perwakilan penjualan jika Anda perlu bergabung dalam beta.

4. Konfirmasi dan bayar untuk instance CLB yang dipilih.
5. Layanan CLB akan diaktifkan setelah pembayaran selesai. Anda kini bisa mengonfigurasi dan menggunakan instance CLB.

Membuat instance CLB melalui API

Untuk membeli instance CLB melalui API, silakan lihat [CreateLoadBalancer](#) di [Pengantar](#).

Membuat Instance CLB IPv6

Waktu update terbaru : 2024-01-04 20:53:33

Keterangan :

CLB IPv6 saat ini dalam pengujian beta. Jika Anda ingin menggunakannya, silakan [kirim tiket](#) untuk mendaftar.

Saat ini, instance CLB IPv6 dapat dibuat di wilayah Guangzhou, Shanghai, Nanjing, Beijing, Chengdu, Hong Kong (Tiongkok), Singapura, dan Virginia.

CLB IPv6 tidak mendukung CLB klasik.

CLB IPv6 mendukung upaya mendapatkan alamat sumber IPv6 klien, yang dapat langsung diperoleh dengan CLB IPv6 lapisan 4 atau melalui header `X-Forwarded-For` dari HTTP CLB IPv6 lapisan 7.

Saat ini, CLB IPv6 sepenuhnya diimplementasikan pada jaringan publik, jadi klien di VPC yang sama tidak bisa mengakses CLB IPv6 melalui jaringan pribadi.

Implementasi IPv6 masih berada di tahap dasar di seluruh internet. Jika terjadi kegagalan akses, silakan [kirimkan tiket](#). SLA tidak dijamin selama periode pengujian beta.

Ikhtisar

CLB IPv6 adalah penyeimbangan beban yang diimplementasikan berdasarkan teknologi tumpukan tunggal IPv6. Itu bisa berkolaborasi dengan CLB IPv4 untuk mengimplementasikan komunikasi dua tumpukan IPv6/IPv4. Instance CLB IPv6 terikat ke alamat IPv6 dari instance CVM dan memberikan alamat VIP IPv6.

Keunggulan CLB IPv6

CLB IPv6 memiliki keunggulan sebagai berikut saat membantu bisnis Anda terhubung dengan cepat ke IPv6:

Koneksi cepat: CLB mengaktifkan koneksi ke IPv6 dalam hitungan detik dan tersedia pada saat pembelian.

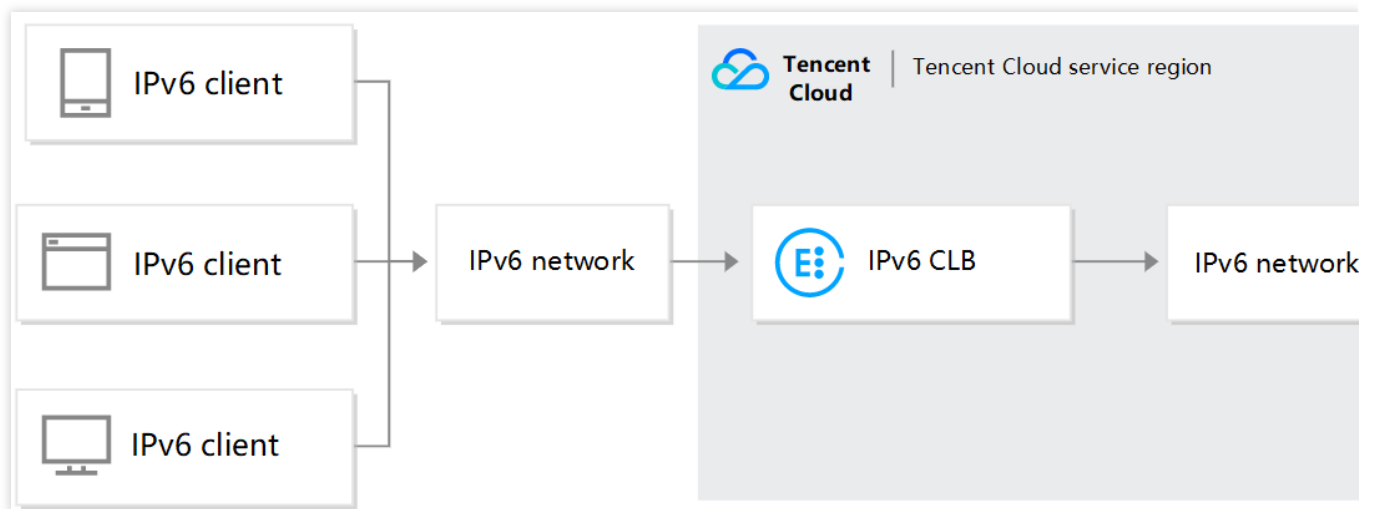
Kemudahan penggunaan: CLB IPv6 kompatibel dengan proses operasi CLB IPv4 dan mudah digunakan tanpa memerlukan biaya pembelajaran tambahan.

Komunikasi IPv6 menyeluruh: CLB IPv6 berkomunikasi dengan instance CVM melalui IPv6, yang membantu aplikasi yang di-deploy di instance CVM ditingkatkan dengan cepat ke IPv6 dan mengimplementasikan komunikasi IPv6 menyeluruh.

Arsitektur CLB IPv6

CLB mendukung pembuatan instance CLB IPv6. Tencent Cloud akan memberikan alamat IP publik IPv6, yaitu, VIP edisi IPv6, ke instance CLB IPv6, dan VIP akan meneruskan permintaan dari klien IPv6 ke instance CVM IPv6 nyata. Instance CLB IPv6 bisa mendukung akses cepat pengguna jaringan publik IPv6 dan berkomunikasi dengan server asli melalui IPv6, yang membantu aplikasi in-cloud ditingkatkan dengan cepat ke IPv6 dan mengimplementasikan komunikasi IPv6 menyeluruh.

Arsitektur CLB IPv6 seperti yang ditunjukkan di bawah ini.



Panduan Pengoperasian

Langkah 1. Buat instance CLB IPv6

1. Masuk ke situs web resmi Tencent Cloud dan masuk ke [halaman pembelian CLB](#).
2. Pilih opsi untuk parameter berikut dengan benar:
Cara Penagihan: hanya mendukung penagihan bayar sesuai pemakaian.
Wilayah: pilih wilayah.
Versi IP: IPv6.
Jenis ISP: BGP.
Jaringan: silakan pilih VPC dan subnet yang sudah mendapatkan CIDR IPv6.
3. Setelah mengatur item-item konfigurasi di halaman pembelian, klik **Buy Now** (Beli Sekarang) untuk kembali ke [halaman daftar instance CLB](#), tempat Anda bisa melihat instance CLB IPv6 yang baru saja Anda beli.

Langkah 2. Buat pendengar CLB IPv6

1. Masuk ke [Konsol CLB](#) dan klik ID instance CLB IPv6 untuk masuk ke halaman detail.
2. Pilih tab **Listener Management** (Manajemen Pendengar) dan klik **Create** (Buat) untuk membuat pendengar, misalnya, pendengar TCP.
Keterangan :
CLB mendukung pembuatan pendengar CLB IPv6 (TCP/UDP/TCP SSL) lapisan 4 dan (HTTP/HTTPS) lapisan 7.
7. Untuk informasi selengkapnya, silakan lihat [Ikhtisar Pendengar CLB](#).
3. Di "Konfigurasi Dasar", konfigurasi nama, port protokol pendengaran, dan metode penyeimbangan, dan klik **Next** (Berikutnya).

Create Listener

1 Basic Configuration > 2 Health Check >

Name

Listen Protocol Ports :

Balance Method

If you set a same weighted value for all CVMs, request pooling policy.

Close

Next

4. Konfigurasi pemeriksaan kesehatan dan klik **Next** (Berikutnya).

Create Listener



Basic Configuration



Health Check



Health Check 



Show advanced options ▼

Back

Next

5. Konfigurasi persistensi sesi dan klik **Submit** (Kirim).

Create Listener



Basic Configuration



Health Check



Session Persistence ⓘ



Hold Time ⓘ



30 Seconds

3600 Secon

Session persistence based on the source IP

Back

Submit

6. Setelah pendengar dibuat, pilih dan klik **Bind** (Ikat) di sebelah kanan.

Keterangan :

Sebelum mengikat pendengar ke instance CVM, silakan periksa apakah instance sudah memperoleh alamat IPv6.

TCP/UDP/TCP SSL Listener

[Create](#)

ipv6-ssh(TCP:22)

Listener Details [Expand](#) ▾

Bound Real Server

[Bind](#) [Modify Port](#) [Modify Weight](#) [Unbind](#)

| <input type="checkbox"/> | CVM ID/Name | Port Health Status | IP Address |
|--------------------------|-------------|--------------------|------------|
| <input type="checkbox"/> | ... | Healthy | ... |
| <input type="checkbox"/> | ... | Healthy | ... |

7. Di kotak pop-up, pilih instance CVM IPv6 nyata untuk berkomunikasi, konfigurasi port dan bobot layanannya, dan klik **OK**.

TCP/UDP/TCP SSL Listener

[Create](#)

ipv6-ssh(TCP:22)

Listener Details [Expand](#) ▾

Bound Real Server

[Bind](#) [Modify Port](#) [Modify Weight](#) [Unbind](#)

| <input type="checkbox"/> | CVM ID/Name | Port Health Status | IP Address |
|--------------------------|-------------|--------------------|------------|
| <input type="checkbox"/> | ... | Healthy | ... |
| <input type="checkbox"/> | ... | Healthy | ... |

Membuat Instance CLB IPv6 NAT64

Waktu update terbaru : 2024-01-04 20:53:33

Keterangan :

CLB IPv6 NAT64 hanya bisa dibuat di tiga wilayah:Beijing, Shanghai, dan Guangzhou.

CLB IPv6 NAT64 tidak mendukung CLB klasik.

CLB IPv6 NAT64 tidak mendukung pengambilan IP klien.

Implementasi IPv6 masih berada di tahap awal di seluruh internet, dan SLA tidak dijamin.Jika terjadi kegagalan akses, silakan [kirimkan tiket](#) untuk memperoleh bantuan.

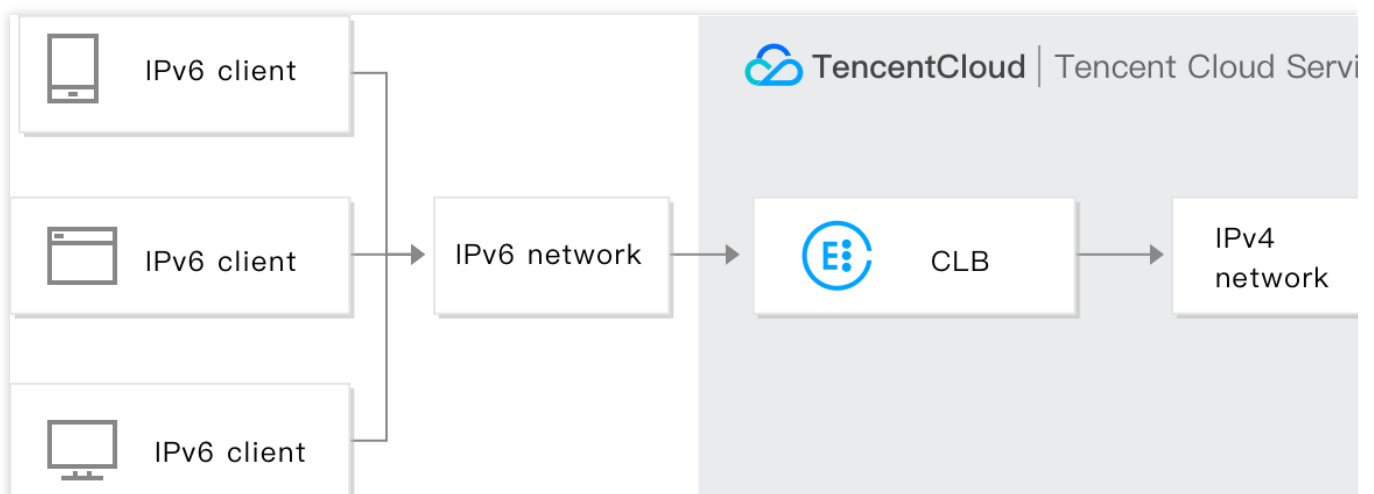
CLB mendukung pembuatan instance CLB IPv6 NAT64.Tencent Cloud akan memberikan alamat IP publik IPv6, yaitu, VIP edisi IPv6, ke suatu instance, dan VIP akan meneruskan permintaan dari klien IPv6 ke instance CVM IPv4 nyata.

Ikhtisar Instance CLB IPv6 NAT64

Instance CLB IPv6 NAT64 adalah penyeimbang beban yang diimplementasikan berdasarkan teknologi jembatan IPv6 NAT64.Melalui instance CLB IPv6 NAT64, server asli bisa diakses dengan cepat oleh pengguna IPv6 tanpa memerlukan modifikasi IPv6.

Arsitektur CLB IPv6 NAT64

Arsitektur CLB IPv6 NAT64 seperti yang ditunjukkan di bawah ini.



Jika CLB IPv6 NAT64 diakses dari jaringan IPv6, CLB dapat dengan lancar mengonversi alamat IPv6 ke alamat IPv4 untuk beradaptasi dengan layanan yang ada dan mengimplementasikan transformasi IPv6 dengan cepat.

Keunggulan CLB IPv6 NAT64

CLB IPv6 NAT64 Tencent Cloud memiliki keunggulan sebagai berikut saat membantu bisnis Anda terhubung dengan cepat ke IPv6:

Koneksi cepat: CLB mengaktifkan koneksi ke IPv6 dalam hitungan detik dan tersedia pada saat pembelian.

Transisi bisnis lancar: untuk mentransmisikan bisnis Anda ke IPv6 dengan lancar, Anda hanya perlu mentransformasikan klien tanpa perlu modifikasi untuk server asli. CLB IPv6 NAT64 mendukung akses dari klien IPv6 dan mengonversi pesan IPv6 menjadi pesan IPv4. Transisi IPv6 tidak terlihat oleh aplikasi di server asli, yang tetap bekerja dengan cara aslinya.

Kemudahan penggunaan: CLB IPv6 NAT64 kompatibel dengan proses operasi CLB IPv4 dan mudah digunakan tanpa memerlukan biaya pembelajaran tambahan.

Panduan Pengoperasian

Membuat instance CLB IPv6 NAT64

1. Masuk di situs resmi Tencent Cloud dan buka [halaman pembelian CLB](#).

2. Pilih opsi untuk parameter berikut dengan benar:

Wilayah: hanya Beijing, Shanghai, dan Guangzhou yang didukung.

Jenis Instance: CLB.

Jenis Jaringan: jaringan publik.

Versi IP: IPv6 NAT64.

Jaringan: VPC.

Konfigurasi lainnya sama seperti konfigurasi instance umum.

3. Setelah mengatur item-item konfigurasi di halaman pembelian, klik **Buy Now** (Beli Sekarang) untuk kembali ke [halaman daftar instance CLB](#), tempat Anda bisa melihat instance CLB IPv6 NAT64 yang baru saja Anda beli.

Memakai CLB IPv6 NAT64

Masuk ke [Konsol CLB](#) dan klik ID instance untuk masuk ke halaman detail. Di tab “Manajemen Pendengar”, Anda bisa mengonfigurasi pendengar dan meneruskan aturan dan mengikat instance CVM. Untuk informasi selengkapnya, silakan lihat [Memulai CLB](#).

Instance Management

Guangzhou(8) Shanghai Nanjing Beijing Chengdu Chongqing Taipei, China Hong Kong, China Singapore Bangkok Mumbai Seoul Tokyo Silicon Valley Virginia Toronto Frankfurt

Cloud Load Balancer(7) Classic Cloud Load Balancer(1)

Create Delete Change Project Edit Tags

| ID/Name | Monito... | Status | VIP | Networ... | Network | Health Status | Project |
|---------|-----------|--------|-----------------|----------------|---------|--|---------|
| | | Normal | 72 (IPv6 NAT64) | Public Network | 6) | Health check not enabled (Configuration) | DEFAUI |

Membuat Instance Anycast

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung pembuatan instance CLB Anycast. CLB Anycast adalah layanan penyeimbangan beban yang mendukung akselerasi dinamis lintas wilayah. VIP CLB dipublikasikan di beberapa wilayah. Klien menghubungkan ke POP terdekat dan meneruskan lalu lintas ke instance CVM melalui internet kecepatan tinggi IDC Tencent Cloud. CLB Anycast bisa mencapai pengoptimalan transfer jaringan dan akses multi-entri terdekat dan mengurangi jitter jaringan dan kehilangan paket, yang pada akhirnya bisa meningkatkan kualitas layanan aplikasi dalam cloud, memperluas cakupan layanan, dan mempersingkat deployment backend.

Keterangan :

Fitur ini sedang dalam pengujian beta. Untuk menerapkan uji coba, kirimkan tiket untuk kelayakan pengujian beta.

Apa itu Anycast?

Anycast artinya, saat IP yang sama dipublikasikan di beberapa lokasi secara bersamaan, algoritme perutean akan mengirimkan lalu lintas pengguna ke router terdekat.

Keunggulan CLB Anycast:

Low latency (Latensi rendah)

CLB Anycast memublikasikan VIP ke beberapa wilayah sekaligus melalui Anycast. Berdasarkan protokol transfer, paket permintaan akan tiba di wilayah publikasi VIP yang optimal untuk memperoleh akses khusus ke Tencent Cloud dan kemudian mencapai instance CVM melalui jaringan pribadi Tencent Cloud, menghindari kemacetan jaringan publik dan mengurangi latensi.

Reduced jitter and packet loss (Mengurangi jitter dan kehilangan paket)

Ketidakstabilan transmisi jaringan publik lintas batas atau lintas pembawa bisa menyebabkan jitter jaringan dan kehilangan paket, dan merusak pengalaman layanan. Sebaliknya, CLB Anycast menawarkan kestabilan transmisi tinggi. Hal ini memberikan permintaan klien terdekat akses ke Tencent Cloud dan mengaktifkan transmisi lintas wilayah melalui koneksi jaringan pribadi khusus Tencent Cloud, membantu menghilangkan jitter dan kehilangan paket.

High reliability (Keandalan tinggi)

Transmisi melalui jaringan publik mungkin tidak bisa diandalkan. Saat masalah baris khusus ISP membuat layanan tidak bisa diakses, pengguna biasanya harus menunggu hingga layanan kembali. Dengan bantuan CLB Anycast, jaringan pribadi Tencent Cloud, jaringan ISP, dan Tencent Cloud POP bisa mencapai beberapa jalur dan entri jaringan untuk menghilangkan kegagalan yang disebabkan oleh satu wilayah atau jalur dan meningkatkan kestabilan jaringan.

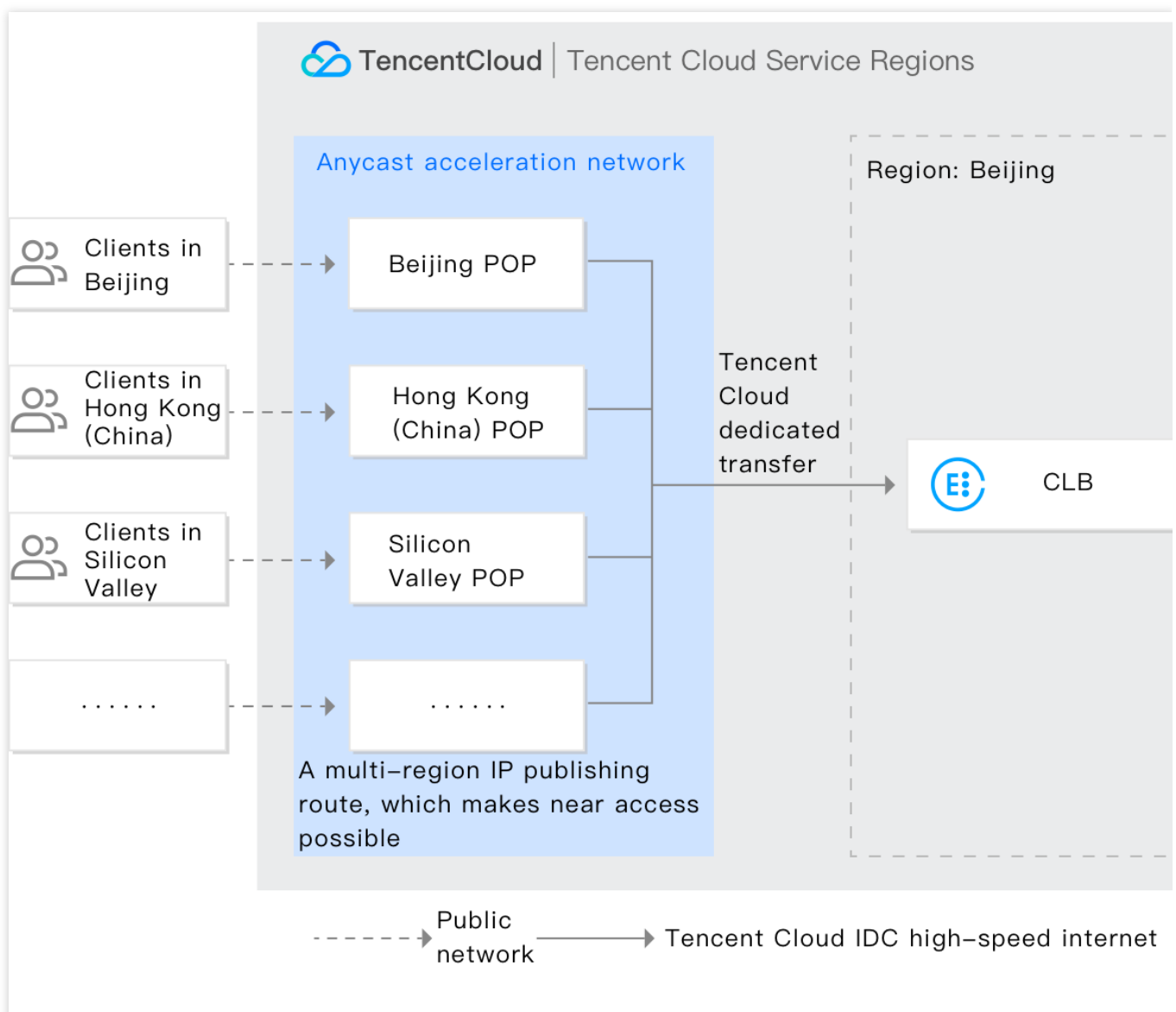
Simplified deployment (Deployment disederhanakan)

Saat klien Anda tersebar di seluruh wilayah dan membutuhkan akses terdekat, Anda harus men-deploy server di

semua wilayah itu dan mengonfigurasi DNS untuk mencapai penyeimbangan beban, dan IP yang bervariasi per wilayah membuat deployment jadi lebih rumit. Melalui CLB Anycast, atribut wilayah dipusatkan di level IP sehingga tidak membutuhkan konfigurasi IP untuk setiap wilayah. Selain itu, Anda hanya perlu mempertahankan satu set logika bisnis di backend, dan permintaan dari berbagai wilayah diarahkan langsung ke server-server asli melalui akselerasi jaringan pribadi.

Arsitektur CLB Anycast

Arsitektur CLB Anycast seperti yang ditunjukkan di bawah ini:



VIP CLB Anycast dipublikasikan ke berbagai wilayah di seluruh dunia. Klien terhubung ke POP terdekat dan meneruskan lalu lintas akses secara ultra cepat ke instance CVM melalui jaringan pribadi Tencent Cloud.

Wilayah publikasi Anycast

Wilayah publikasi Anycast adalah tempat alamat IP yang dipercepat dipublikasikan, yaitu, POP tempat VIP CLB Anycast dipublikasikan. Klien mengakses POP terdekat. Saat ini, CLB Anycast mendukung publikasi serentak di wilayah-wilayah berikut ini: Beijing, Shanghai, Guangzhou, Hong Kong (Tiongkok), Toronto, Silicon Valley, Frankfurt, Virginia, Moscow, Singapore, Seoul, Mumbai, Bangkok, dan Tokyo.

Wilayah CLB Anycast

Seperti wilayah instance CLB generik, wilayah CLB Anycast adalah wilayah yang Anda pilih saat membeli instance CLB Anycast atau wilayah tempat server asli Anda berada. Saat ini, CLB Anycast tersedia di sebagian besar wilayah. Tiongkok: Beijing, Shanghai, Guangzhou, dan Hong Kong SAR.

Eropa dan Amerika Utara: Toronto, Silicon Valley, Frankfurt, Virginia, dan Moscow.

Asia Tenggara: Singapore, Seoul, Mumbai, Bangkok, dan Tokyo.

Keterangan :

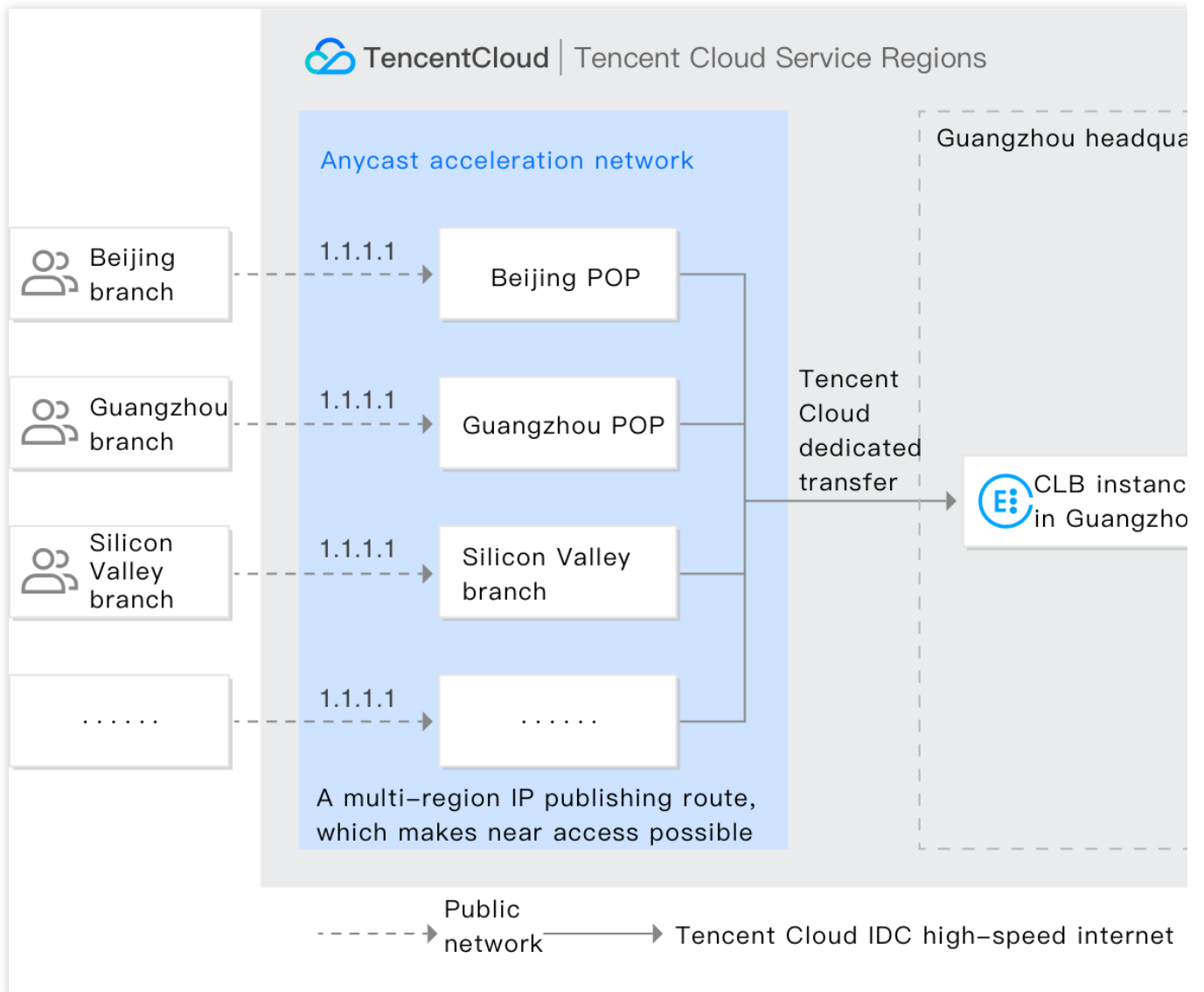
Kemampuan anycast dari CLB Anycast diimplementasikan dengan mengikat EIP Anycast ke instance CLB jaringan pribadi.

EIP Anycast bisa diikat ke instance CLB jaringan pribadi, tetapi tidak ke instance CLB jaringan pribadi klasik atau instance CLB jaringan klasik.

Kasus Penggunaan CLB Anycast

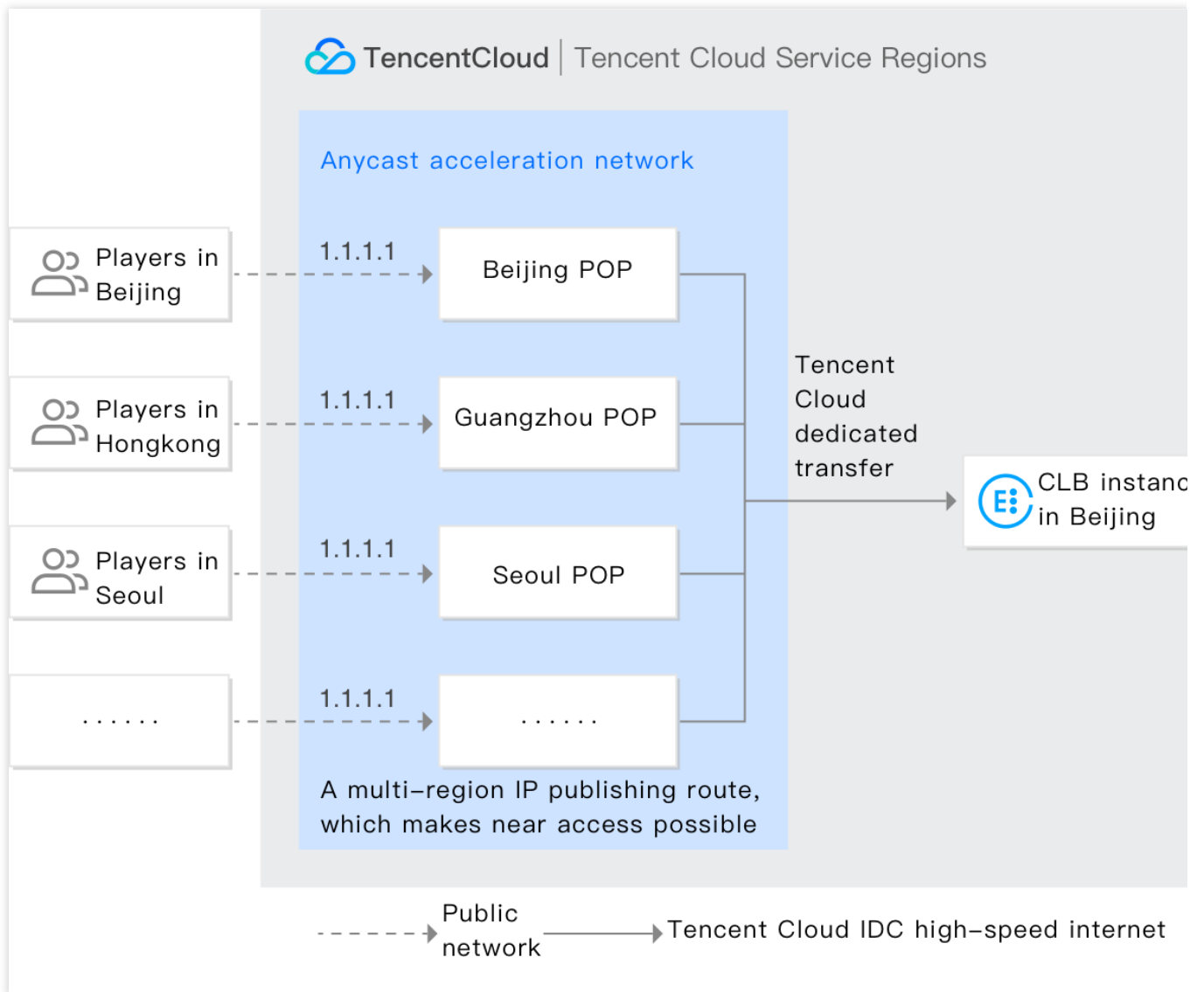
Server terpadu untuk akses lintas wilayah

Jika Anda dalam industri game, Anda bisa berharap para pemain dari berbagai tempat ada di satu wilayah server atau bahwa cabang-cabang Anda di seluruh dunia bisa berbagi IDC yang sama. Anda bisa menggunakan CLB Anycast untuk men-deploy server-server asli di satu wilayah (seperti Guangzhou), membeli instance CLB Anycast di wilayah tersebut dan memilih wilayah publikasi sesuai kebutuhan. Dengan cara ini, pemain atau karyawan bisa memperoleh akses terdekat ke server asli yang sama.



Akselerasi game

CLB Anycast telah digunakan secara luas dalam akselerasi game. Melalui CLB Anycast CLB, permintaan game bisa mendapat akses terdekat ke Tencent Cloud dan mencapai server game melalui jaringan pribadi Tencent Cloud, mempersingkat jalur jaringan publik dan mengurangi masalah seperti penundaan, jitter, dan kehilangan paket. Dibandingkan akselerasi tradisional, CLB Anycast tidak membutuhkan deployment penerima lalu lintas ekstra pada entri dan menghapus kebutuhan zoning sehingga menyederhanakan deployment DNS.



Panduan Pengoperasian

Prasyarat

Fitur ini saat ini dalam versi beta. Pastikan aplikasi Anda untuk kelayakan pengujian beta sudah disetujui sebelum memakainya.

Petunjuk

1. Masuk ke [Konsol CVM](#).
2. Pada bilah sisi kiri, klik **EIP** untuk masuk ke halaman manajemen EIP.
3. Klik **Apply** (Terapkan). Di jendela pop-up, pilih **Accelerated IP** (IP Dipercepat) sebagai jenis alamat IP dan klik **OK**.

Apply for EIP ✕

IP address type Normal IP
Ordinary BGP IP, balancing network quality and costs



Acceleration IP **Recommended**
Adopts Anycast acceleration, providing stable, reliable the low-latency internet access

Region South China(Guangzhou)









Accelerated Region Global

Amount 4/20

Advanced

Fee 
(Preview price)
Billed by the total bandwidth usage in all regions. An idle EIP will incur an idle fee of  No charges incur if it's bound with an instance.

4. Masuk ke [Konsol CLB](#), pilih instance CLB jaringan pribadi (instance CLB klasik tidak didukung), dan klik **More** (Lainnya) > **Bind Accelerated IP** (Ikat IP Dipercepat) di kolom "Operasi".

| <input type="checkbox"/> | ID/Name ↕ | Monitor... | Status | VIP | Network... ⌵ | Network | Health Status | Creatio |
|--------------------------|---|---|--------|---|-----------------|---|---|---------|
| <input type="checkbox"/> |  |  | Normal |  | Private Network |  | Health check not enable d(Configuration) | 2019-12 |
| <input type="checkbox"/> |  |  | Normal |  | Public Network |  | Abnormal(Abnormal po rts: 1) | 2019-12 |

5. Setelah instance CLB jaringan pribadi terikat ke IP yang dipercepat, layanan CLB Anycast bisa diberikan. Untuk informasi selengkapnya tentang konfigurasi CLB, silakan lihat [Ikhtisar Pendengar CLB](#).

| <input type="checkbox"/> | ID/Name ↕ | Monitor... | Status | VIP | Network... ▼ | Network | Health Status | Creati |
|--------------------------|-----------|------------|--------|-------------------------------------|-----------------|---------|---|--------|
| <input type="checkbox"/> | | | Normal | 1 (Accelerated IP) 1 (Private) | Private Network | | Health check not enabled Configuration | 2019- |

Mengonfigurasi Grup Keamanan CLB

Waktu update terbaru : 2024-01-04 20:53:33

Setelah instance CLB dibuat, Anda bisa mengonfigurasi satu grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Dokumen ini menjelaskan cara mengonfigurasi grup keamanan CLB di mode-mode berbeda.

Batasan Penggunaan

Satu instance CLB bisa diikat ke maksimum lima grup keamanan.

Hingga 512 aturan diizinkan untuk grup keamanan.

Grup keamanan tidak bisa diikat ke instance CLB pribadi berbasis jaringan klasik dan instance CLB pribadi klasik. Jika satu instance CLB terikat ke [Anycast EIP](#), grup keamanan yang terikat ke instance tersebut tidak akan aktif.

Allow by Default (Izinkan secara Default) tidak tersedia untuk CLB pribadi klasik dan CLB berbasis jaringan klasik.

Latar belakang

Grup keamanan adalah firewall virtual yang bisa memfilter paket data stateful dan mengendalikan lalu lintas keluar dan masuk pada level instance. Untuk informasi selengkapnya, lihat [Grup Keamanan](#).

Grup keamanan CLB terikat dengan instance CLB, sementara grup keamanan CVM terikat dengan instance CVM. Target mereka adalah objek yang berbeda. Untuk grup keamanan CLB, Anda bisa memilih untuk:

[Mengaktifkan **Allow by Default** \(Izinkan secara Default\)](#)

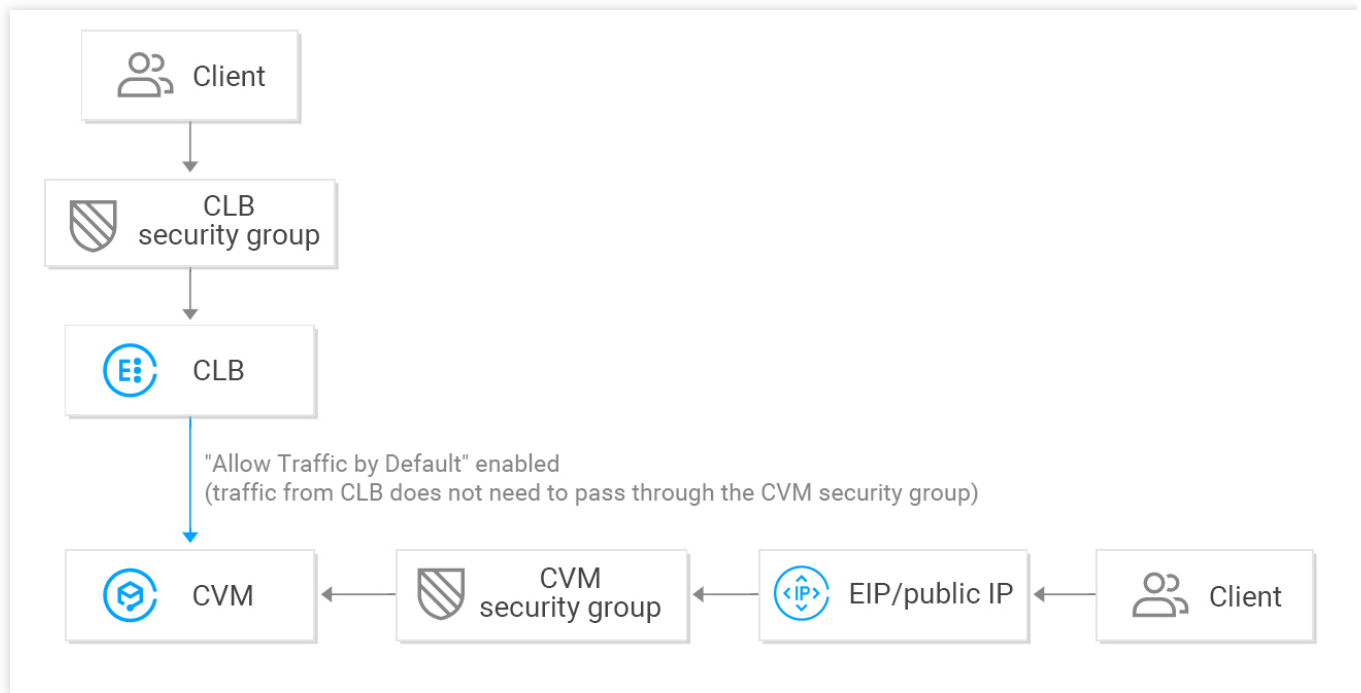
[Menonaktifkan **Allow by Default** \(Izinkan secara Default\)](#)

Keterangan :

Untuk grup keamanan CLB IPv4, **Allow by Default** (Izinkan secara Default) dinonaktifkan secara default, Anda bisa mengaktifkannya di konsol.

Untuk grup keamanan CLB IPv6, **Allow by Default** (Izinkan secara Default) diaktifkan secara default, Anda tidak bisa menonaktifkannya.

Mengaktifkan Allow by Default (Izinkan secara Default)



Saat **Allow by Default** (Izinkan secara Default) diaktifkan:

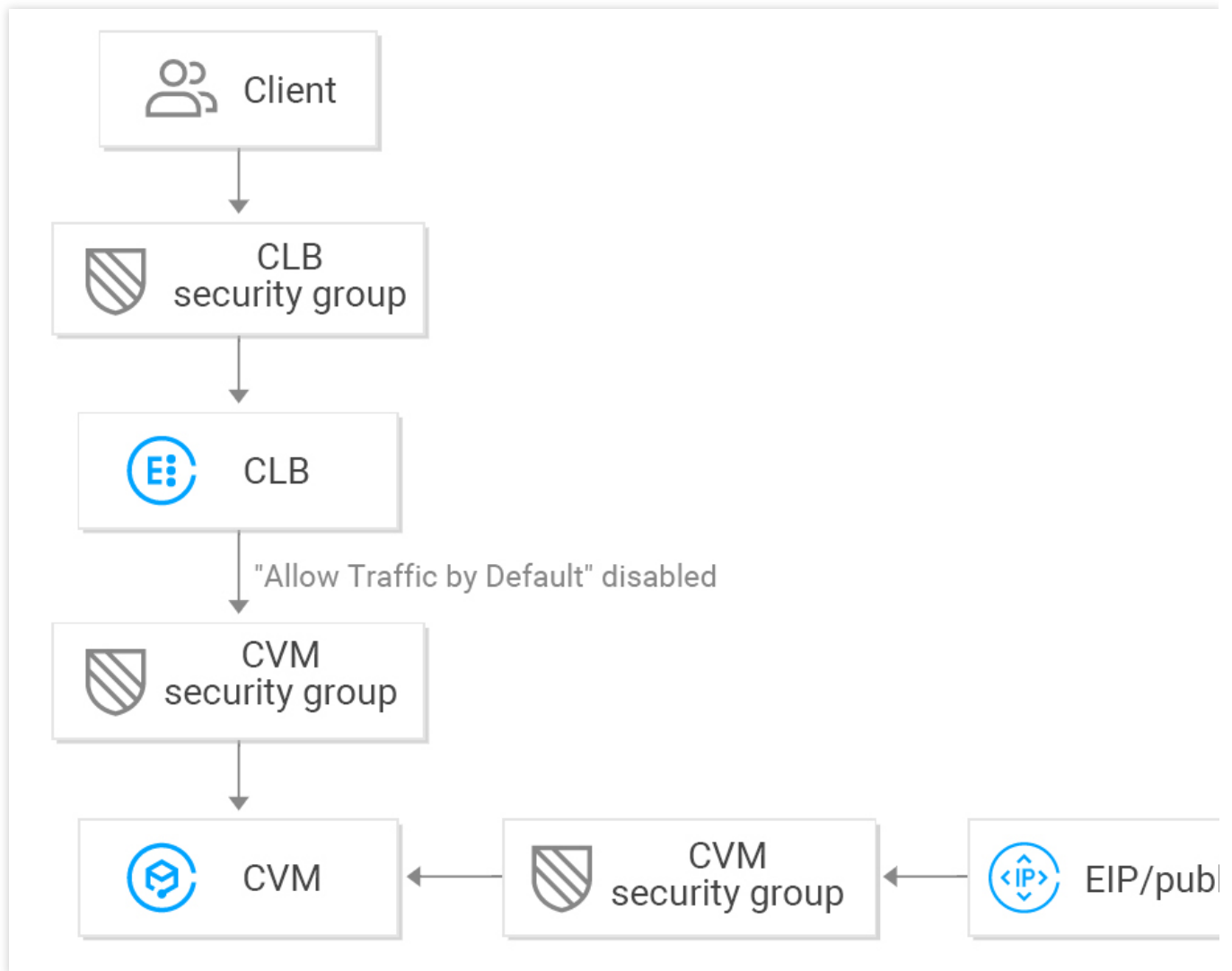
Jika Anda ingin memberi izin akses dari IP klien tertentu saja, Anda harus mengizinkannya dan port pendengaran di grup keamanan CLB, tetapi Anda tidak perlu mengizinkan IP klien dan port layanan di grup keamanan CVM backend. Lalu lintas akses dari CLB hanya melewati grup keamanan CLB, karena server asli mengizinkan lalu lintas dari CLB secara default.

Lalu lintas dari IP publik (termasuk IP dan EIP publik umum) masih harus melewati grup keamanan CVM.

Jika satu instance CLB belum mengonfigurasi grup keamanan, semua lalu lintas akan diizinkan, dan hanya port yang dikonfigurasi dengan pendengar di VIP instance CLB yang bisa diakses; oleh karena itu, port pendengaran akan mengizinkan lalu lintas dari semua IP.

Untuk menolak lalu lintas dari IP klien tertentu, Anda harus mengonfigurasi di grup keamanan CLB. Menolak IP klien di grup keamanan CVM hanya berlaku untuk lalu lintas dari IP publik (termasuk IP dan EIP publik umum) tetapi tidak untuk lalu lintas dari CLB.

Menonaktifkan Allow by Default (Izinkan secara Default)



Jika **Allow by Default** (Izinkan secara Default) dinonaktifkan:

Jika Anda hanya ingin mengizinkan akses dari IP klien tertentu, Anda harus mengizinkan IP klien dan port pendengaran di grup keamanan CLB dan juga mengizinkan IP klien dan port layanan di grup keamanan CVM; oleh karena itu, lalu lintas bisnis yang melewati CLB akan diperiksa dua kali oleh baik grup keamanan CLB dan grup keamanan CVM.

Lalu lintas dari IP publik (termasuk IP dan EIP publik umum) masih harus melewati grup keamanan CVM.

Jika instance CLB belum mengonfigurasi grup keamanan, hanya lalu lintas yang melewati grup keamanan CVM yang diizinkan.

Anda bisa menolak akses baik untuk grup keamanan CLB maupun grup keamanan CVM untuk menolak lalu lintas dari IP klien tertentu.

Jika Izinkan secara Default dinonaktifkan, grup keamanan CVM harus dikonfigurasi seperti berikut ini untuk memastikan pemeriksaan kesehatan yang efektif:

1. Konfigurasi jaringan publik

Anda harus mengizinkan VIP CLB di grup keamanan CVM backend, agar CLB bisa menggunakan VIP untuk mendeteksi status kesehatan CVM backend.

2. Konfigurasi jaringan pribadi

Untuk CLB jaringan pribadi (sebelumnya “CLB aplikasi pribadi”), jika instance CLB Anda dalam VPC, VIP CLB perlu diizinkan di grup keamanan CVM backend untuk pemeriksaan kesehatan; jika instance CLB Anda dalam jaringan klasik, konfigurasi tambahan tidak diperlukan karena IP pemeriksaan kesehatan sudah diizinkan secara default.

Untuk CLB klasik jaringan pribadi, jika instance CLB Anda dibuat sebelum 5 Desember 2016 dan ada di VPC, VIP CLB perlu diizinkan (untuk pemeriksaan kesehatan) di grup keamanan CVM backend; jika tidak, konfigurasi tambahan tidak diperlukan karena IP pemeriksaan kesehatan sudah diizinkan secara default.

Petunjuk

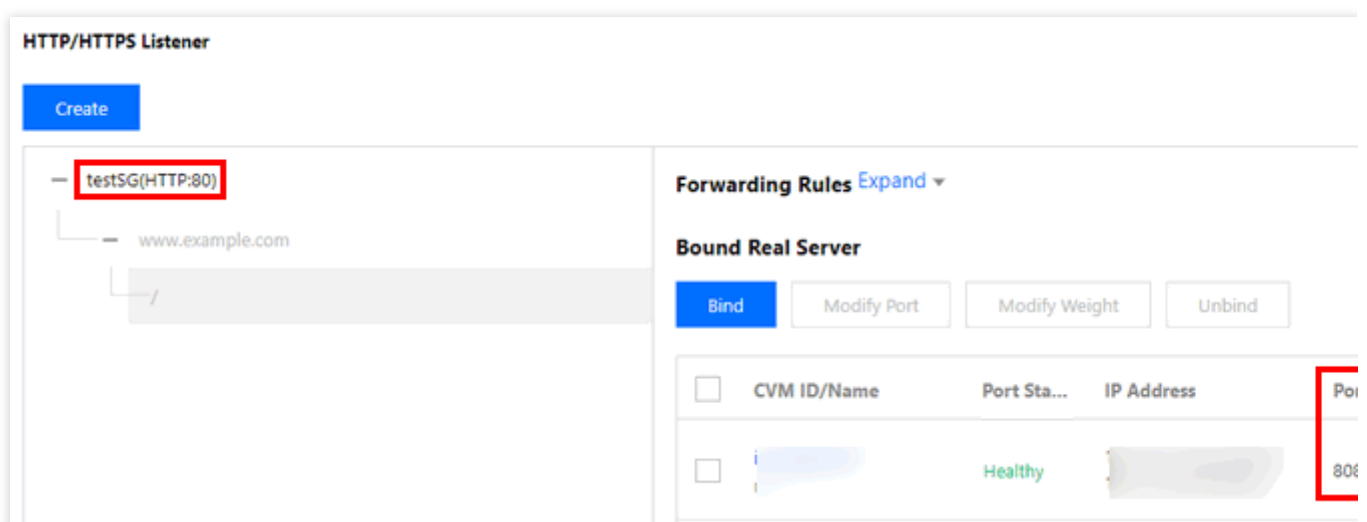
Pada contoh berikut ini, grup keamanan dikonfigurasi agar hanya mengizinkan lalu lintas masuk ke CLB dari port 80, dan layanan tersedia melalui CVM port 8080. Tidak ada batasan pada IP klien.

Perhatian :

Untuk instance CLB jaringan publik yang digunakan pada contoh ini, VIP CLB perlu diizinkan di grup keamanan CVM backend untuk pemeriksaan kesehatan. IP saat ini diatur ke `0.0.0.0/0`, yang artinya semua IP diizinkan.

Langkah 1. Buat satu instance dan pendengar CLB, dan ikat mereka ke CVM

Untuk informasi selengkapnya, silakan lihat [Memulai CLB](#). Satu pendengar HTTP:80 dibuat dan diikat ke instance CVM backend dengan port layanan 8080 pada contoh ini.



| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | | Healthy | | 8080 |

Langkah 2. Konfigurasi grup keamanan CLB

1. Konfigurasi aturan grup keamanan CLB

Masuk ke [Konsol Grup Keamanan](#) untuk mengonfigurasi aturan grup keamanan. Di aturan masuk, izinkan permintaan dari port 80 dari semua IP (misalnya, `0.0.0.0/0`) dan tolak lalu lintas dari port lainnya.

Keterangan :

Aturan grup keamanan disaring agar berlaku dari atas ke bawah. Jika aturan yang baru diberlakukan, aturan lainnya akan ditolak secara default; oleh karena itu, perhatikan urutannya. Untuk informasi selengkapnya, lihat [Ikhtisar Grup Keamanan](#).

Satu grup keamanan memiliki aturan masuk dan keluar. Konfigurasi di atas dimaksudkan untuk membatasi lalu lintas masuk dan karenanya merupakan **aturan masuk**, sementara aturan keluar tidak perlu dikonfigurasi secara khusus.

| Type | Source ⓘ | Protocol port ⓘ | Policy | Notes |
|----------|-----------|-----------------|---------|-------|
| Custom ▼ | 0.0.0.0/0 | TCP:80 | Allow ▼ | |

+ New Line

[Completed](#) [Cancel](#)

2. Ikat grup keamanan ke instance CLB

1. Masuk ke [Konsol CLB](#).

2. Di halaman "Manajemen Instance", klik ID instance CLB target.

3. Di halaman detail instance, klik tab **Security Group** (Grup Keamanan) dan klik **Bind** (Ikat) pada modul **Bound Security Groups** (Grup Keamanan Terikat).

4. Di jendela **Configure Security Group** (Konfigurasi Grup Keamanan) yang muncul, pilih grup keamanan yang terikat ke instance CLB dan klik **OK**.

Security Groups

Projects

Select a security group

Enter the security group name or ID

| <input type="checkbox"/> | ID/Name | Notes |
|-------------------------------------|---------------------|-------|
| <input checked="" type="checkbox"/> | sg- open port 80 | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |

Selected (1)

| | ID/Name | Notes |
|-------------------------------------|---------------------|-------|
| <input checked="" type="checkbox"/> | sg- open port 80 | |

OK Cancel

Konfigurasi grup keamanan CLB sudah selesai, yang hanya mengizinkan akses pada CLB dari port 80.

Note: from Dec 17, 2019, Tencent Cloud adds limits on the max number of security groups bound with an instance, instances bound to a security group, and rules refer details, please see [Details of Limit](#).

Bound to security group [Sort](#) [Bind](#)

| Priority | Security Group | Operation |
|----------|---------------------|-----------|
| 1 | sg- open port 80 | Unbind |

Rule preview [Inbound rule](#) [Outbound rule](#)

sg- | open port 80

| Source | Port Protocol | Policy |
|-----------|---------------|--------|
| 0.0.0.0/0 | TCP:80 | Allow |
| ALL | ALL | Refuse |

Langkah 3. Konfigurasi Allow by Default (Izinkan secara Default)

Anda bisa memilih untuk mengaktifkan atau menonaktifkan **Allow by Default** (Izinkan secara Default) dengan konfigurasi berbeda seperti berikut ini:

Metode 1. Aktifkan **Allow by Default** (Izinkan secara Default), agar server asli tidak perlu mengizinkan port.

Keterangan :

Fitur ini tidak didukung untuk CLB jaringan privat klasik dan CLB di jaringan klasik.

Metode 2. Nonaktifkan **Allow by Default** (Izinkan secara Default), dan Anda juga perlu mengizinkan IP klien (0.0.0.0/0 pada contoh ini) di grup keamanan CVM.

Metode 1. Aktifkan Allow by Default (Izinkan secara Default)

- Masuk ke [Konsol CLB](#).
- Di halaman **Instance Management** (Manajemen Instance), klik ID instance CLB target.
- Di halaman detail instance, klik tab **Security Group** (Grup Keamanan).
- Pada tab **Security Group** (Grup Keamanan), klik



untuk mengaktifkan **Allow by Default** (Izinkan secara Default).

3. Jika **Allow by Default** (Izinkan secara Default) diaktifkan, hanya aturan grup keamanan di **ikhtisar aturan** seperti yang ditunjukkan di bawah ini yang perlu diverifikasi.

Allow by Default

When it's enabled, the access between CLB and CVM is allowed by default. Requests from CLB only need to be verified by the CLB security group. When it's disabled, request verified by both security groups of CLB and CVM. If the CLB is not bound with a security group, all it's listening ports allow requests from all IPs.

Bound to security group Sort Bind

| Priority① | Security Grou... | Operation |
|-----------|------------------|-----------|
| 1 | xx-allow80 | Unbind |

Rule preview ①

Inbound rule Outbound rule

| Source | Port Protocol | Policy | N |
|--------|---------------|--------|-------------------|
| | TCP:80 | Allow | - |
| ALL | ALL | Refuse | If t s r ad |

Metode 2.Nonaktifkan Allow by Default (Izinkan secara Default)

Jika **Allow by Default** (Izinkan secara Default) dinonaktifkan, Anda perlu mengizinkan IP klien di grup keamanan CVM.Lalu lintas bisnis hanya diizinkan mengakses CVM dari port 80 CLB dan menggunakan layanan yang disediakan melalui port 8080 CVM.

Keterangan :

Untuk mengizinkan lalu lintas dari IP klien tertentu, Anda perlu mengizinkan IP tersebut di grup keamanan CLB dan grup keamanan CVM.Jika CLB tidak memiliki grup keamanan, silakan izinkan IP di grup keamanan CVM.

1.Konfigurasi aturan grup keamanan CVM

Grup keamanan CVM bisa dikonfigurasi agar hanya mengizinkan akses dari port layanan untuk lalu lintas yang mengakses instance CVM backend.

Buka [Konsol Grup Keamanan](#) untuk mengonfigurasi kebijakan grup keamanan.Di aturan masuk, semua port 8080 dari semua IP.Untuk memastikan kelancaran layanan masuk dan ping CVM jarak jauh, buka 22, 3389, dan layanan ICMP di grup keamanan.

2.Ikat grup keamanan ke instance CVM

1.Di [Konsol CVM](#), klik ID instance CVM yang terikat ke instance CLB untuk masuk ke halaman detail.

2.Pilih tab **Security Group** (Grup Keamanan) dan klik **Bind** (Ikat) di modul **Bound Security Groups** (Grup Keamanan Terikat).

3.Pada jendela **Configure Security Group** (Konfigurasi Grup Keamanan) yang muncul, pilih grup keamanan yang terikat ke instance CVM dan klik **OK**.

← **ii** [blurred]

Basic Information ENI Public IP Monitoring **Security Groups** Operation Logs

Note: from Dec 17, 2019, Tencent Cloud adds limits on the max number of security groups bound with an instance, instances bound to a security group, and rules. For details, please see [Details of Limit](#).

Bound to security group

Sort Bind

| Priority① | Security Group... | Operation |
|-----------|----------------------------------|-----------|
| 1 | sg- [blurred] TCP port 22,... | Unbind |

Rule preview

Inbound rule Outbound rule

sg- [blurred] | TCP port 22, 8 [blurred]

| Source | Port Protocol | Policy |
|-----------|---------------|--------|
| 0.0.0.0/0 | TCP:8080 | Allow |
| 0.0.0.0/0 | TCP:3389 | Allow |

Mengekspor Instance CLB

Waktu update terbaru : 2024-01-04 20:53:33

Anda bisa mengekspor daftar instance CLB yang berisi konfigurasi dan detail penggunaan sumber daya dengan menentukan wilayah atau kondisi lainnya.

Petunjuk

1. Masuk ke [Konsol CLB](#) dan pilih satu wilayah di sudut kiri atas halaman **Instance Management** (Manajemen Instance).

2. Di daftar instance, pilih satu instance dan klik



di sudut kanan atas.

3. Di jendela pop-up, pilih bidang dan lingkup untuk diekspor dan klik **Confirm** (Konfirmasi) untuk mengunduh daftar instance secara lokal.

Export instances ✕

Exported files:

Export All

Instance field:

| | | | |
|--|--|---|--|
| <input checked="" type="checkbox"/> ID | <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Status | <input checked="" type="checkbox"/> VIP |
| <input checked="" type="checkbox"/> Network type | <input checked="" type="checkbox"/> Network | <input checked="" type="checkbox"/> ISP | <input checked="" type="checkbox"/> Instance Specification |
| <input checked="" type="checkbox"/> Billing Mode | <input checked="" type="checkbox"/> Bandwidth Cap | <input checked="" type="checkbox"/> Project | <input checked="" type="checkbox"/> Tags |
| <input checked="" type="checkbox"/> VIP features | <input checked="" type="checkbox"/> Bind with Custom | <input checked="" type="checkbox"/> Creation Time | |

Rule filed:

Listener ID, listener protocol, listener port, forwarding rule ID, forwarding domain, forwarding URL, CVM ID, RS IP, RS port, RS weight

Backend service type:

Non-target group Target Group

In case some of the CLB's listeners are bound with the target group and the rest listeners don't, you need you export them separately.

Exported range:

All Instances Only search results Only selected instances

Confirm
Cancel

| Parameter | Deskripsi |
|-----------|---|
| Bidang | Bidang-bidang berikut ini dapat diekspor: Bidang instance Bidang aturan Jenis server asli "Status kesehatan RS" di bidang aturan hanya ditampilkan jika bidang aturan sudah diperiksa dan lingkup ekspornya "Instance terpilih saja". |
| Lingkup | Lingkup-lingkup berikut ini dapat diekspor: Semua instance Hasil pencarian saja Instance terpilih saja Bidang "Instance terpilih saja" akan berwarna abu-abu jika tidak ada instance yang dipilih. |

Menghapus Instance CLB

Waktu update terbaru : 2024-01-04 20:53:33

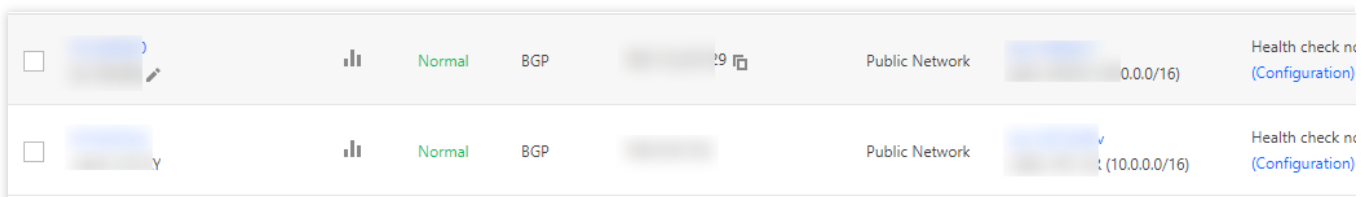
Keterangan :

Instance berlangganan bulanan tidak bisa dihapus, tetapi Anda bisa berhenti memperbaruinya saat kedaluwarsa. Setelah Anda mengonfirmasi bahwa instance CLB tidak memiliki lalu lintas dan tidak lagi dibutuhkan, Anda bisa menghapusnya melalui konsol CLB atau API.

Setelah dihapus, instance CLB akan benar-benar dihentikan dan tidak bisa dipulihkan. Kami sangat menyarankan untuk memutus semua server asli dan mengamati untuk sementara sebelum menghapus instance apa pun.

Menghapus instance CLB melalui konsol

1. Masuk ke [Konsol CLB](#).
2. Carilah instance CLB yang ingin Anda hapus dan klik **More** -> **Delete** (Lainnya -> Hapus) pada kolom **Operation** (Operasi) di sebelah kanan.



| | | | | | | | |
|--------------------------|-----------------|--------|-----|--------------|----------------|--------------|------------------------------------|
| <input type="checkbox"/> | [Instance Name] | Normal | BGP | [IP Address] | Public Network | [IP Address] | Health check no (Configuration) |
| <input type="checkbox"/> | [Instance Name] | Normal | BGP | [IP Address] | Public Network | [IP Address] | Health check no (Configuration) |

3. Kotak dialog konfirmasi akan muncul. Setelah Anda membaca prompt keamanan operasi, klik **Submit** (Kirim) untuk mengonfirmasi penghapusan.

Kotak dialog seperti yang ditunjukkan di bawah ini. Kami menyarankan untuk mengonfirmasi penghapusan saat terdapat **0** aturan pengikatan, **none** (tidak ada) instance terikat CVM, dan tanda hijau di bawah kolom **Notes About Operation Security** (Catatan Mengenai Keamanan Operasi).

Confirm to delete the following load balancers? ✕

| ID/Name | Bound rules | Bound CVM | Notes About Oper... |
|--------------------------|-------------|-----------|---------------------|
| lb-2jrl6dv0 lb-162309 | 0 | None | ✓ |

Menghapus instance CLB melalui API

Untuk informasi selengkapnya, buka [DeleteLoadBalancers](#).

Menyesuaikan Konfigurasi Jaringan Publik Instance

Waktu update terbaru : 2024-01-04 20:53:33

Anda bisa menyesuaikan bandwidth atau cara penagihan jaringan publik instance CLB sesuai kebutuhan secara real-time.

Batasan

Instance CLB IPv4: penyesuaian konfigurasi jaringan hanya didukung untuk akun tagihan per IP, tetapi tidak untuk akun tagihan per CVM.

Instance CLB IPv6: penyesuaian konfigurasi jaringan didukung untuk akun tagihan per IP dan tagihan per CVM.

Untuk informasi lebih jauh tentang cara memeriksa jenis akun Anda, silakan buka [Memeriksa Jenis Akun](#).

Batas Bandwidth

| Mode Tagihan Instance | Mode Tagihan Jaringan | Rentang Batas Bandwidth (dalam Mbps) |
|------------------------|---------------------------------|--------------------------------------|
| Bayar sesuai pemakaian | Tagihan per bandwidth (per jam) | 0 - 2048 (inklusif) |
| | Tagihan per lalu lintas | |
| | Paket bandwidth | |

Keterangan :

Jika Anda perlu mengatur batas bandwidth yang lebih tinggi, silakan [kirimkan tiket](#) atau hubungi perwakilan penjualan Tencent Cloud Anda.

Menyesuaikan Bandwidth

- Masuk ke [Konsol CLB](#).
- Pada halaman **Instance Management** (Manajemen Instance), pilih satu wilayah, dan klik **More** -> **Adjust Bandwidth** (Selengkapnya -> Sesuaikan Bandwidth) di sebelah kanan instance CLB jaringan publik.
- Di kotak dialog, atur batas bandwidth dan klik **Submit** (Kirim).

Mengubah Cara Penagihan

1. Masuk ke [Konsol CLB](#).

2. Pada halaman **Instance Management** (Manajemen Instance), pilih satu wilayah, klik **More** (Lainnya) di sebelah kanan instance CLB jaringan publik dan terus menyesuaikan cara penagihan jaringan.

| Cara Penagihan Instance | Cara Penagihan Jaringan | Penyesuaian |
|-------------------------|---------------------------------|---|
| Bayar sesuai pemakaian | Tagihan per bandwidth (per jam) | Tambahkan IP ke paket bandwidth: cara penagihan instance tetap sama; cara penagihan jaringan dialihkan ke menggunakan paket bandwidth; setiap instance hanya bisa dialihkan cara penagihannya satu kali. |
| | Tagihan per lalu lintas | Alihkan ke langganan bulanan: cara penagihan instance dialihkan ke langganan bulanan; cara penagihan jaringan dialihkan ke tagihan per bandwidth (bulanan); setiap instance hanya bisa dialihkan cara penagihannya satu kali. Tambahkan IP ke paket bandwidth: cara penagihan instance tetap sama; cara penagihan jaringan dialihkan ke menggunakan paket bandwidth; setiap instance bisa dialihkan cara penagihannya berulang kali. |
| | Paket bandwidth | Hapus IP dari paket bandwidth: cara penagihan instance tetap sama; cara penagihan jaringan dialihkan ke tagihan per lalu lintas; setiap instance bisa dialihkan cara penagihannya berulang kali. |

3. Klik **Submit** (Kirim) di kotak dialog pop-up.

Pendengar CLB

Ikhtisar Pendengar CLB

Waktu update terbaru : 2024-01-04 20:53:33

Setelah membuat instance CLB, Anda harus mengonfigurasi pendengar untuknya. Pendengar mendengarkan permintaan di instance dan mengarahkan lalu lintas ke server asli sesuai kebijakan penyeimbangan beban.

Anda harus mengonfigurasi pendengar CLB dengan item-item berikut:

1. Protokol dan port pendengaran. Port pendengaran, atau port frontend, digunakan untuk menerima dan meneruskan permintaan ke server asli.
2. Kebijakan pendengaran, seperti kebijakan penyeimbangan beban dan [persistensi sesi](#).
3. Kebijakan [pemeriksaan kesehatan](#).
4. Server asli. Ikat server asli dengan memilih IP dan port-nya. Port layanan, atau port backend, digunakan oleh server asli untuk menerima permintaan.

Jenis Protokol Yang Didukung

Satu pendengar CLB bisa mendengar permintaan lapisan 4 dan lapisan 7 di instance CLB dan mengarahkannya ke server asli untuk pemrosesan. Perbedaan utama antara CLB lapisan 4 dan CLB lapisan 7 adalah apakah protokol lapisan 4 atau lapisan 7 digunakan untuk meneruskan lalu lintas untuk penyeimbangan beban permintaan pengguna.

Protokol lapisan 4: membawa protokol layer yang menerima permintaan dan meneruskan lalu lintas ke server asli terutama melalui VIP dan port.

Protokol lapisan 7: protokol layer aplikasi yang mendistribusikan lalu lintas berdasarkan informasi layer aplikasi seperti URL dan header HTTP.

Jika Anda menggunakan pendengar lapisan 4 (misalnya, penerusan protokol lapisan 4), instance CLB akan menyambungkan koneksi TCP dengan server asli di port pendengaran, dan langsung meneruskan permintaan ke server asli. Proses ini tidak mengubah paket data apa pun (dalam mode pass-through) dan memiliki efisiensi penerusan tinggi.

CLB Tencent Cloud mendukung penerusan permintaan melalui protokol-protokol berikut ini:

TCP (layer transportasi)

UDP (layer transportasi)

TCP SSL (layer transportasi)

HTTP (layer aplikasi)

HTTPS (layer aplikasi)

Keterangan :

Pendengar TCP SSL saat ini mendukung instance CLB jaringan publik, tetapi tidak mendukung jaringan pribadi atau instance CLB klasik.

| Jenis Protokol | Protokol | Deskripsi | Kasus Penggunaan |
|--------------------|----------|---|--|
| Protokol lapisan 4 | TCP | <p>Protokol dan layer transportasi andal dan berorientasi koneksi: Ujung sumber dan tujuan harus melakukan jabat tangan tiga arah untuk membuat koneksi sebelum transfer data. Mendukung persistensi sesi berbasis IP Klien (IP sumber). IP klien bisa ditemukan di layer jaringan. Server bisa memperoleh IP klien secara langsung.</p> | <p>Itu cocok untuk skenario yang sangat membutuhkan keandalan dan akurasi data, tetapi tidak terlalu membutuhkan kecepatan transfer, seperti transfer file, menerima dan mengirim email, dan masuk jarak jauh. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi Pendengar TCP.</p> |
| | UDP | <p>Protokol layer transportasi tanpa koneksi: Ujung sumber dan tujuan tidak membuat koneksi atau mempertahankan status koneksi. Setiap koneksi UDP adalah point-to-point. Mendukung komunikasi satu-ke-satu, satu-ke-semuanya, semuanya-ke-satu, dan semuanya-ke-semuanya. Mendukung persistensi sesi berbasis IP Klien (IP sumber). Server bisa memperoleh IP klien secara langsung.</p> | <p>Itu cocok untuk skenario yang sangat membutuhkan efisiensi transfer, tetapi tidak terlalu membutuhkan akurasi, seperti pesan singkat dan video online. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi Pendengar UDP.</p> |
| | TCP SSL | <p>TCP Aman: Pendengar TCP SSL mendukung sertifikat konfigurasi untuk mencegah permintaan akses tidak resmi. Manajemen sertifikat terpadu disediakan bagi CLB untuk mengimplementasi dekripsi. Mendukung autentikasi bersama dan satu arah. Server bisa memperoleh IP klien secara langsung.</p> | <p>Ini cocok untuk skenario yang sangat membutuhkan keamanan saat TCP digunakan dan mendukung protokol khusus berbasis TCP. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi Pendengar TCP SSL.</p> |
| Protokol lapisan 7 | HTTP | <p>Protokol layer aplikasi: Mendukung penerusan berdasarkan nama domain dan URL yang diminta. Mendukung persistensi sesi berbasis cookie.</p> | <p>Ini cocok untuk aplikasi tempat konten permintaan perlu diidentifikasi, seperti aplikasi web, aplikasi seluler, dan</p> |

| | | | |
|--|-------|--|--|
| | | | sebagainya. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi Pendengar HTTP . |
| | HTTPS | <p>Protokol layer aplikasi terenkripsi:</p> <p>Mendukung penerusan berdasarkan nama domain dan URL yang diminta.</p> <p>Mendukung persistensi sesi berbasis cookie.</p> <p>Manajemen sertifikat terpadu disediakan bagi CLB untuk mengimplementasi dekripsi.</p> <p>Mendukung autentikasi bersama dan satu arah.</p> | Ini cocok untuk aplikasi HTTP yang membutuhkan transmisi terenkripsi. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi Pendengar HTTPS . |

Konfigurasi Port

| Jenis Port | Catatan | Pembatasan |
|----------------------------------|---|--|
| Port pendengaran (port frontend) | Port pendengaran digunakan oleh instance CLB untuk menerima dan meneruskan permintaan ke server asli. Anda bisa mengonfigurasi instance CLB untuk port 1 sampai 65535, seperti port 21 (FTP), 25 (SMTP), 80 (HTTP), dan 443 (HTTPS), dll. | <p>Pada satu instance CLB:</p> <p>Port pendengaran UDP bisa digunakan untuk TCP; misalnya, pendengar `TCP:80` bisa berdampingan dengan pendengar `UDP:80`.</p> <p>Port pendengaran harus unik untuk jenis protokol yang sama. TCP, TCP SSL, HTTP, dan HTTPS adalah dari TCP, jadi misalnya, pendengar `TCP:80` tidak bisa berdampingan dengan pendengar `HTTP:80`.</p> |
| Port layanan (port backend) | Port layanan digunakan oleh instance CVM untuk memberikan layanan, menerima dan memproses lalu lintas dari instance CLB. Pada satu instance CLB, satu port pendengaran bisa meneruskan lalu lintas ke port-port beberapa instance CVM. | <p>Pada satu instance CLB:</p> <p>Port layanan dari protokol pendengaran berbeda tidak harus unik; misalnya, pendengar `HTTP:80` dan `HTTPS:443` bisa ditemukan di port instance CVM yang sama. Saat menggunakan protokol pendengaran yang sama, setiap port layanan backend hanya bisa diikat ke satu pendengar, artinya, lipat empat (VIP, protokol pendengaran, IP pribadi server asli, dan port layanan backend) harus unik.</p> |

Mengonfigurasi Pendengar TCP

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Pendengar TCP

Anda bisa membuat pendengar TCP ke instance CLB untuk meneruskan permintaan TCP dari klien. TCP cocok untuk skenario yang sangat membutuhkan keandalan dan akurasi data, tetapi tidak terlalu membutuhkan kecepatan transfer, seperti transfer file, pesan email, dan masuk jarak jauh. Untuk pendengar TCP, server asli bisa memperoleh IP klien asli secara langsung.

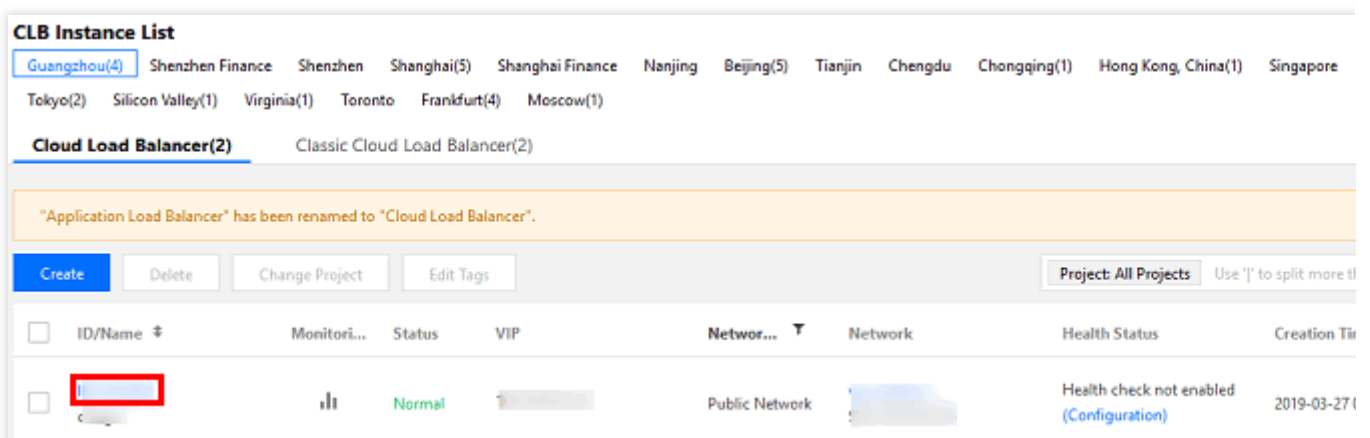
Prasyarat

Anda harus [membuat instance CLB](#) dahulu.

Mengonfigurasi Pendengar TCP

Langkah 1. Buka halaman "Manajemen Pendengar"

1. Masuk ke [Konsol CLB](#).
2. Pilih **Instance Management** (Manajemen Instance) di bilah sisi kiri.
3. Di daftar instance, klik ID instance yang akan dikonfigurasi untuk masuk ke halaman detail instance.
4. Klik tab **Listener Management** (Manajemen Pendengar) atau klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operation" (Operasi).



CLB Instance List

Guangzhou(4) Shenzhen Finance Shenzhen Shanghai(5) Shanghai Finance Nanjing Beijing(5) Tianjin Chengdu Chongqing(1) Hong Kong, China(1) Singapore Tokyo(2) Silicon Valley(1) Virginia(1) Toronto Frankfurt(4) Moscow(1)

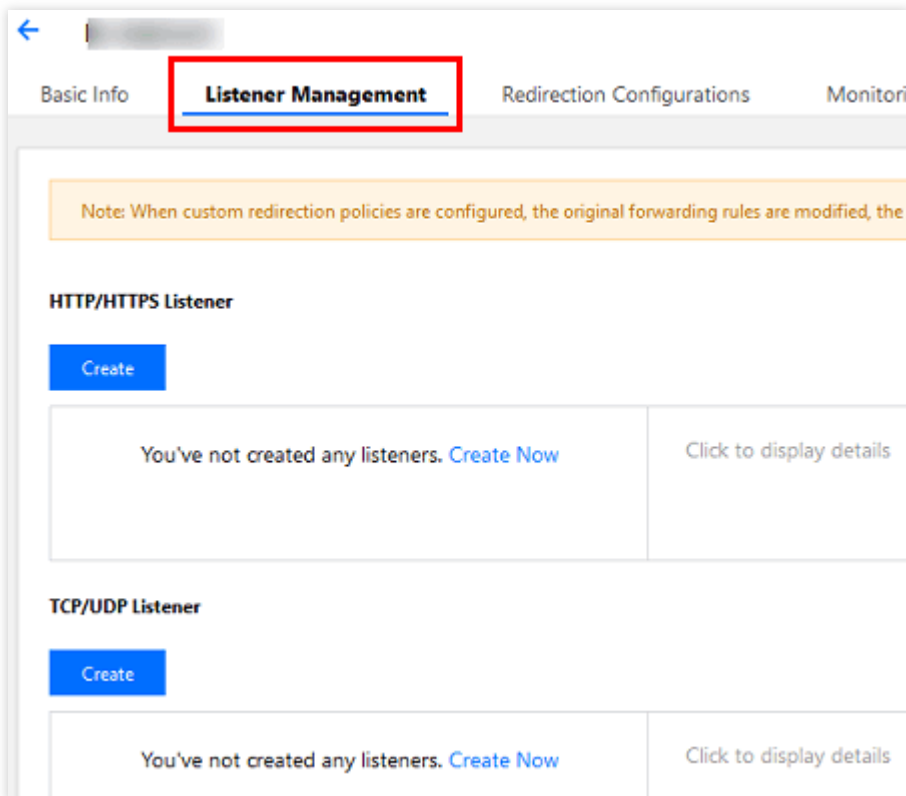
Cloud Load Balancer(2) Classic Cloud Load Balancer(2)

"Application Load Balancer" has been renamed to "Cloud Load Balancer".

Create Delete Change Project Edit Tags Project: All Projects Use ']' to split more tl

| <input type="checkbox"/> | ID/Name | Monitori... | Status | VIP | Networ... | Network | Health Status | Creation Ti |
|--------------------------|--|-------------|--------|------------|----------------|------------|--|--------------|
| <input type="checkbox"/> | [Redacted] | | Normal | [Redacted] | Public Network | [Redacted] | Health check not enabled (Configuration) | 2019-03-27 t |

5. Halaman "Listener Management" (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini:



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di **TCP/UDP/TCP SSL Listener** (Pendengar TCP/UDP/TCP SSL) dan konfigurasi pendengar TCP di jendela pop-up.

1. Konfigurasi dasar

| Item Konfigurasi | Deskripsi | Contoh |
|---|---|-------------|
| Nama | Nama pendengar | test-tcp-80 |
| Protokol pendengar dan port pendengaran | Protokol pendengar dan port pendengaran. Protokol pendengar: CLB mendukung berbagai protokol, termasuk TCP, UDP, HTTP, dan HTTPS. TCP digunakan dalam contoh ini. Port pendengaran: Port digunakan untuk menerima permintaan dan meneruskannya ke server asli. Rentang port: 1-65535. Port pendengar harus unik di instance CLB yang sama. | TCP:80 |
| Metode penyeimbangan | Untuk pendengar TCP, CLB mendukung dua algoritme penjadwalan: round robin tertimbang (WRR) dan koneksi terkecil tertimbang (WLC). WRR: Permintaan dikirimkan secara berurutan ke server-server asli berbeda sesuai bobotnya. Penjadwalan dilakukan berdasarkan jumlah koneksi baru, tempat server dengan bobot lebih tinggi akan melalui lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi), sementara server dengan bobot yang sama memproses jumlah koneksi yang sama. | WRR |

WLC: Beban server dinilai sesuai dengan jumlah koneksi aktif ke server-server. Penjadwalan dilakukan berdasarkan beban dan bobot server. Jika bobotnya sama, server dengan koneksi aktif yang lebih sedikit akan menjalani lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).

Konfigurasi tertentu pendengar TCP yang dibuat adalah seperti yang ditunjukkan di bawah ini:

Create Listener ✕

1 **Basic Configuration** > 2 Health Check > 3 Session Persistence

Name

Listen Protocol Ports :

Balance Method

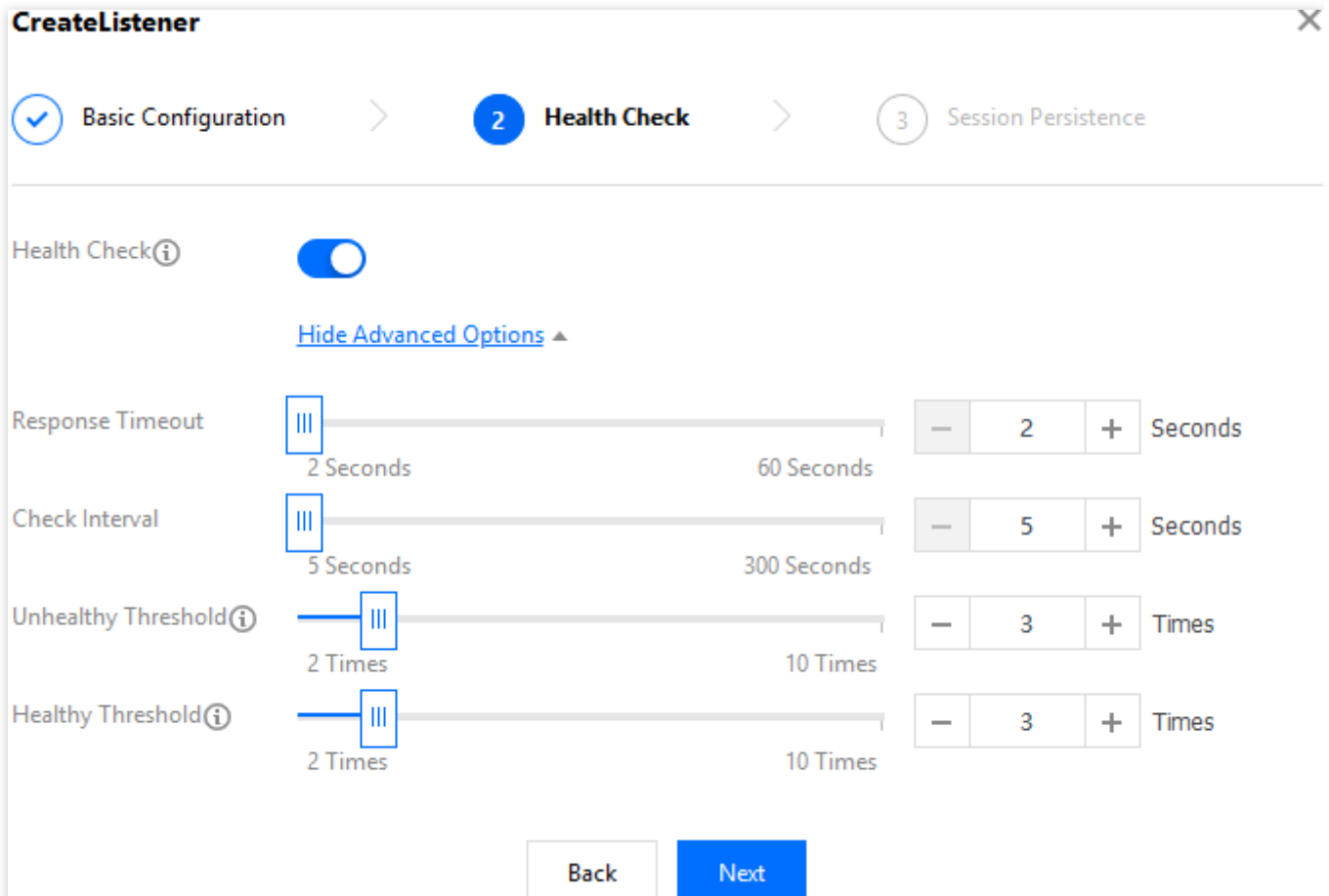
If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

2. Pemeriksaan kesehatan

| Item Konfigurasi | Deskripsi | Contoh |
|------------------------------|--|------------|
| Status pemeriksaan kesehatan | Pemeriksaan kesehatan bisa diaktifkan atau dinonaktifkan. Di pendengar TCP, instance CLB mengirimkan paket SYN ke port server tertentu untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Periode waktu habis respons | Periode waktu habis respons maksimum untuk pemeriksaan kesehatan. Jika satu server asli gagal merespons dengan tepat dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal. Rentang nilai: 2-60s. Nilai default: 2s. | 2s |
| Interval pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300s. Nilai default: 5s. | 5s |
| Ambang batas tidak sehat | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) gagal berturut-turut, instance akan dianggap tidak sehat, dan status yang ditampilkan di konsol akan menjadi Abnormal . Rentang nilai: 2-10. Nilai default: 3. | 3 kali |

| | | |
|--------------------|--|--------|
| Ambang batas sehat | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) berhasil berturut-turut, instance akan dianggap sehat, dan status yang ditampilkan di konsol akan menjadi Healthy (Sehat). Rentang nilai:2-10.Nilai default: 3. | 3 kali |
|--------------------|--|--------|

Konfigurasi khusus pemeriksaan kesehatannya seperti yang ditunjukkan di bawah ini:



3.Persistensi sesi

| Item Konfigurasi | Deskripsi | Contoh |
|-------------------------|---|------------|
| Status persistensi sesi | Persistensi sesi bisa diaktifkan atau dinonaktifkan. Jika persistensi sesi diaktifkan, pendengar CLB akan mengirimkan permintaan akses dari klien yang sama ke server asli yang sama. Persistensi sesi TCP diimplementasikan berdasarkan alamat IP klien, misalnya, permintaan akses dari alamat IP yang sama diteruskan ke server asli yang sama. Persistensi sesi bisa diaktifkan untuk penjadwalan WRR, tetapi tidak untuk penjadwalan WLC. | Diaktifkan |
| Waktu persistensi sesi | Waktu persistensi sesi. Jika tidak ada permintaan baru di koneksi dalam waktu persistensi sesi, persistensi sesi akan diputus secara otomatis. | 30s |

Rentang nilai: 30-3,600s.

Konfigurasi khusus persistensi sesi seperti yang ditunjukkan di bawah ini:

Create Listener

Basic Configuration > Health Check > **3 Session Persistence**

Session Persistence

Hold Time Seconds

30 Seconds 3600 Seconds

Session persistence based on the source IP

[Back](#) [Submit](#)

Langkah 3. Mengikat server asli

1. Di halaman "Manajemen Pendengar", klik pendengar `TCP : 80` yang dibuat untuk melihat server asli yang diikat di sebelah kanan pendengar.

TCP/UDP Listener

[Create](#)

test-tcp-80(TCP:80)

Listener Details [Expand](#)

Bound Real Server

[Bind](#) [Modify Port](#) [Modify Weight](#) [Unbind](#)

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--|-------------|-------------|------------|------|
| Listener created. Please Bound real server | | | | |

2. Klik **Bind** (Ikut), pilih server asli yang akan diikat dan konfigurasi port server dan bobot di jendela pop-up.

1. Tambahkan Port: Di kotak "Terpilih" di sebelah kanan, klik **Add Port** (Tambahkan Port) untuk menambahkan beberapa port untuk instance CVM yang sama, seperti port 80, 81, dan 82.

2. Port Default: Masukkan "Port Default" dahulu, kemudian pilih instance CVM. Port dari setiap instance CVM adalah port default.

Bound real server

IP Enter IP Address Q

| <input checked="" type="checkbox"/> | ID/Name |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |

Selected (3)

| ID/Name | Port | Weight |
|------------|------|--------|
| [Redacted] | 80 | - 10 |
| [Redacted] | 81 | - 10 |
| [Redacted] | 82 | - 10 |

↔

Note: When the private CLB is bound with one CVM, please DO NOT use this CVM as the client to access CLB.

OK
Cancel

Setelah tiga langkah ini selesai, aturan pendengar TCP sudah dikonfigurasi seperti yang ditunjukkan di bawah ini:

The screenshot shows the 'TCP/UDP Listener' management interface. On the left, there is a 'Create' button and a list of listeners. The selected listener is 'test-tcp-80(TCP:80)'. On the right, the 'Listener Details' section is expanded, showing 'Bound Real Server' options: 'Bind', 'Modify Port', 'Modify Weight', and 'Unbind'. Below these are three real servers, each with a checkbox, a CVM ID/Name, a 'Port Sta...' status (all 'Healthy'), an IP Address, and a Port (80, 81, and 82).

Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Mengonfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi/hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang dibuat, klik pendengar di halaman "Manajemen Pendengar" dan pilih **Modify** (Modifikasi) atau **Delete** (Hapus).

This screenshot is similar to the previous one, but the 'test-tcp-80(TCP:80)' listener entry in the list on the left is highlighted with a red box. A 'Modify' button is visible next to the listener name, indicating the modification step.

Mengonfigurasi Pendengar UDP

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Pendengar UDP

Anda bisa membuat pendengar UDP ke instance CLB untuk meneruskan permintaan UDP dari klien.UDP cocok untuk skenario yang sangat membutuhkan kecepatan transfer tetapi tidak terlalu membutuhkan akurasi, seperti pesan singkat dan video online.Untuk pendengar UDP, server asli bisa memperoleh IP klien asli secara langsung.

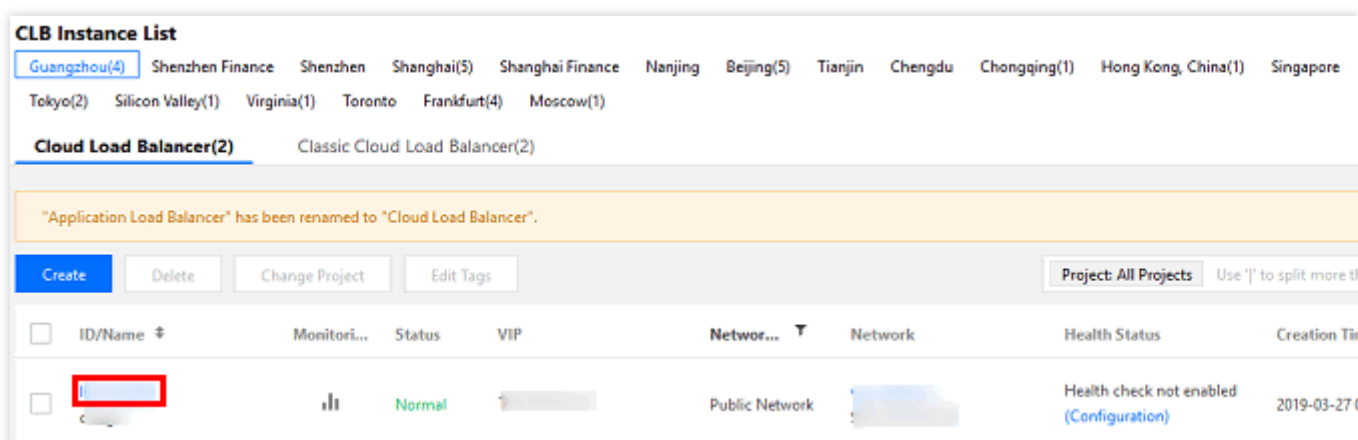
Prasyarat

Anda harus [membuat instance CLB](#) dahulu.

Mengonfigurasi Pendengar UDP

Langkah 1.Buka halaman "Manajemen Pendengar"

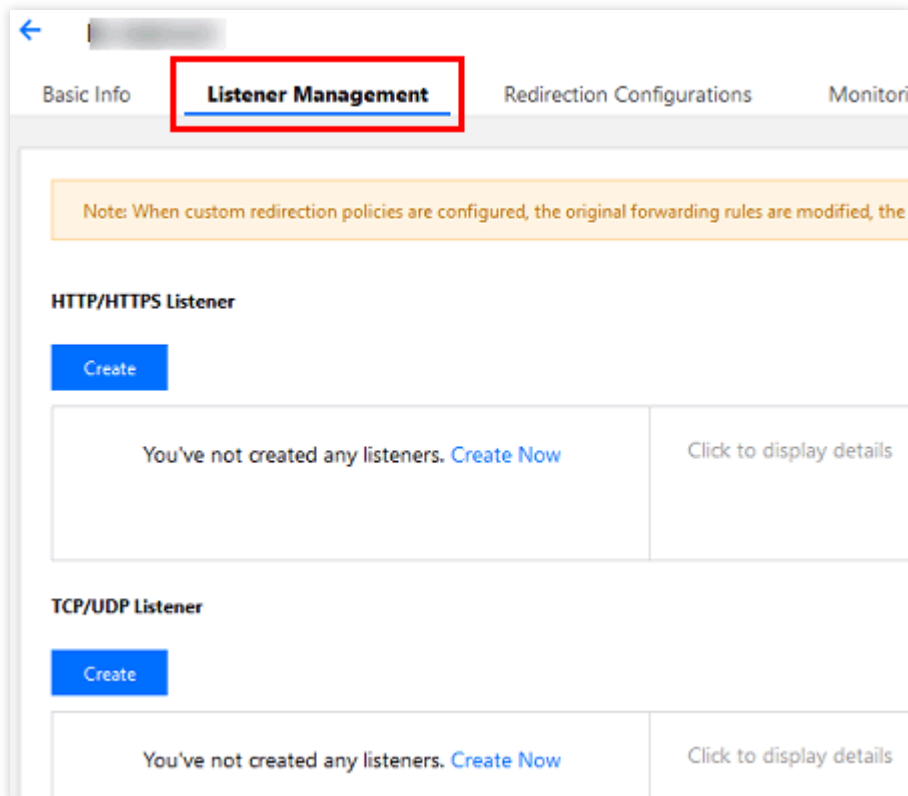
- 1.Masuk ke [Konsol CLB](#).
- 2.Pilih **Instance Management** (Manajemen Instance) di bilah sisi kiri.
- 3.Di daftar instance, klik ID instance yang akan dikonfigurasi untuk masuk ke halaman detail instance.
- 4.Klik tab **Listener Management** (Manajemen Pendengar) atau klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operation" (Operasi).



The screenshot displays the 'CLB Instance List' interface. At the top, there are tabs for various regions: Guangzhou(4), Shenzhen Finance, Shenzhen, Shanghai(5), Shanghai Finance, Nanjing, Beijing(5), Tianjin, Chengdu, Chongqing(1), Hong Kong, China(1), Singapore, Tokyo(2), Silicon Valley(1), Virginia(1), Toronto, Frankfurt(4), and Moscow(1). Below these, there are tabs for 'Cloud Load Balancer(2)' and 'Classic Cloud Load Balancer(2)'. A message states: '"Application Load Balancer" has been renamed to "Cloud Load Balancer".' Below the message are buttons for 'Create', 'Delete', 'Change Project', and 'Edit Tags'. On the right, there is a 'Project: All Projects' dropdown and a note 'Use '[' to split more tl'. The main table has columns: ID/Name, Monitoring, Status, VIP, Network, and Health Status. The first row shows a red box around the ID/Name field, which contains a partially visible ID.

| ID/Name | Monitori... | Status | VIP | Networ... | Network | Health Status | Creation Ti |
|-----------|-------------|--------|------------|----------------|------------|--|-------------|
| [Red Box] | [Bar Chart] | Normal | [Grey Box] | Public Network | [Blue Box] | Health check not enabled (Configuration) | 2019-03-27 |

- 5.Halaman "Listener Management" (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini:



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di **TCP/UDP/TCP SSL Listener** (Pendengar TCP/UDP/TCP SSL) dan konfigurasi pendengar UDP di jendela pop-up.

1. Konfigurasi dasar

| Item Konfigurasi | Deskripsi | Contoh |
|---------------------------------------|---|---------------|
| Nama | Nama pendengar | test-udp-8000 |
| Protokol pendengar dan port pendengar | Protokol pendengar dan port pendengaran. Protokol pendengar: CLB mendukung berbagai protokol, termasuk TCP, UDP, HTTP, dan HTTPS. UDP digunakan dalam contoh ini. Port pendengaran: Port digunakan untuk menerima permintaan dan meneruskannya ke server asli. Rentang port: 1-65535. Port pendengar harus unik di instance CLB yang sama. | UDP:8000 |
| Metode penyeimbangan | Untuk pendengar UDP, CLB mendukung dua algoritme penjadwalan: round robin tertimbang (WRR) dan koneksi terkecil tertimbang (WLC). WRR: Permintaan dikirimkan secara berurutan ke server-server asli berbeda sesuai bobotnya. Penjadwalan dilakukan berdasarkan jumlah koneksi baru, tempat server dengan bobot lebih tinggi akan melalui lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi), sementara server dengan bobot yang sama memproses jumlah koneksi yang sama. | WRR |

WLC: Beban server dinilai sesuai dengan jumlah koneksi aktif ke server-server. Penjadwalan dilakukan berdasarkan beban dan bobot server. Jika bobotnya sama, server dengan koneksi aktif yang lebih sedikit akan menjalani lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).

Konfigurasi tertentu pendengar UDP yang dibuat adalah seperti yang ditunjukkan di bawah ini:

Create Listener ✕

1 **Basic Configuration** > 2 Health Check > 3 Session Persistence

Name

Listen Protocol Ports :

Balance Method

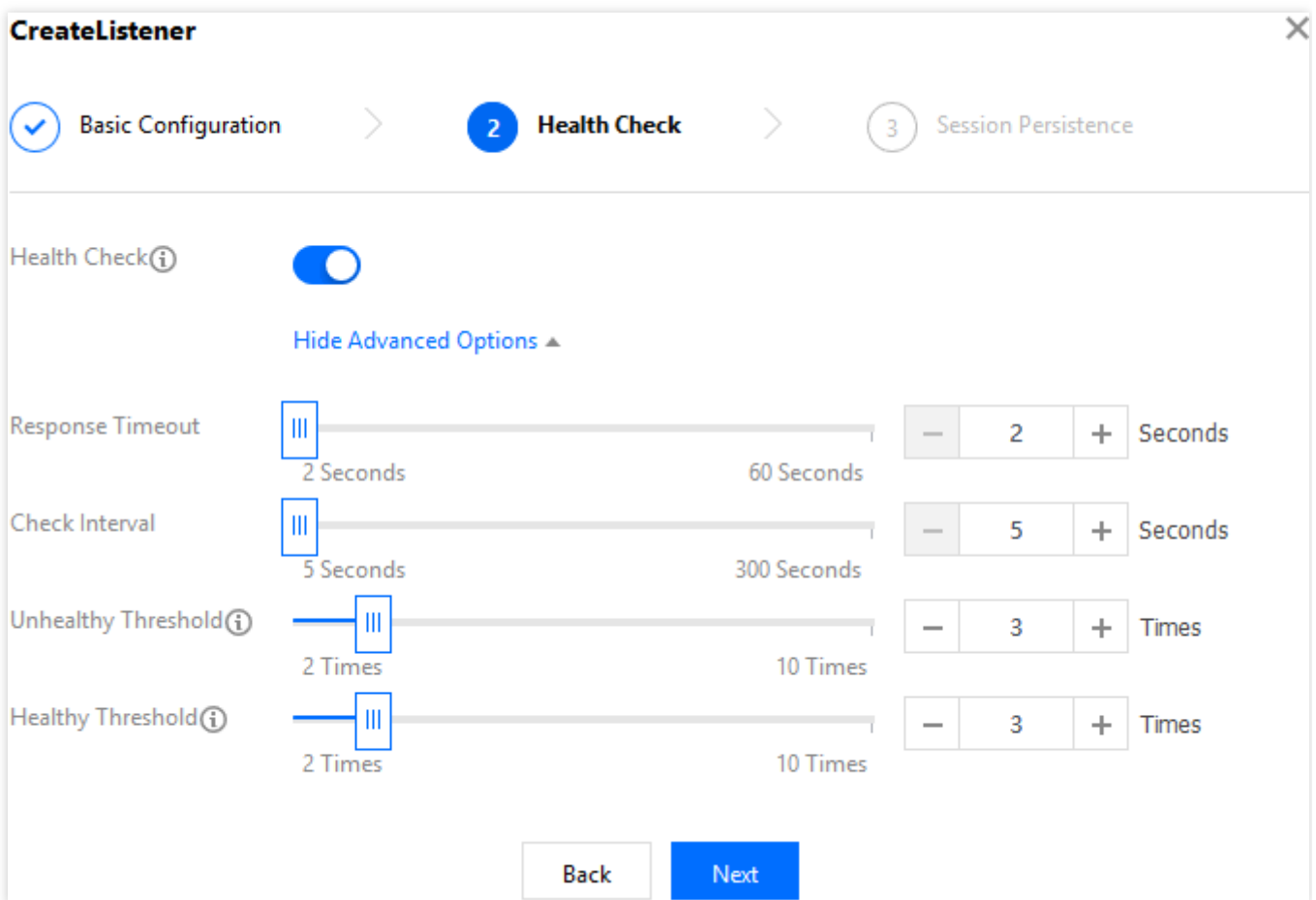
If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

2. Pemeriksaan kesehatan

| Item Konfigurasi | Deskripsi | Contoh |
|------------------------------|---|------------|
| Status pemeriksaan kesehatan | Pemeriksaan kesehatan bisa diaktifkan atau dinonaktifkan. Di pendengar UDP, instance CLB mengirimkan perintah ping ke server untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Periode waktu habis respons | Periode waktu habis respons maksimum untuk pemeriksaan kesehatan. Jika satu server asli gagal merespons dengan tepat dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal. Rentang nilai: 2-60s. Nilai default: 2s. | 2s |
| Interval pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300s. Nilai default: 5s. | 5s |
| Ambang batas tidak | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) gagal berturut-turut, instance akan dianggap tidak sehat, dan | 3 kali |

| | | |
|--------------------|--|--------|
| sehat | status yang ditampilkan di konsol akan menjadi Abnormal . Rentang nilai:2-10.Nilai default: 3. | |
| Ambang batas sehat | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) berhasil berturut-turut, instance akan dianggap sehat, dan status yang ditampilkan di konsol akan menjadi Healthy (Sehat). Rentang nilai:2-10.Nilai default: 3. | 3 kali |

Konfigurasi khusus pemeriksaan kesehatannya seperti yang ditunjukkan di bawah ini:

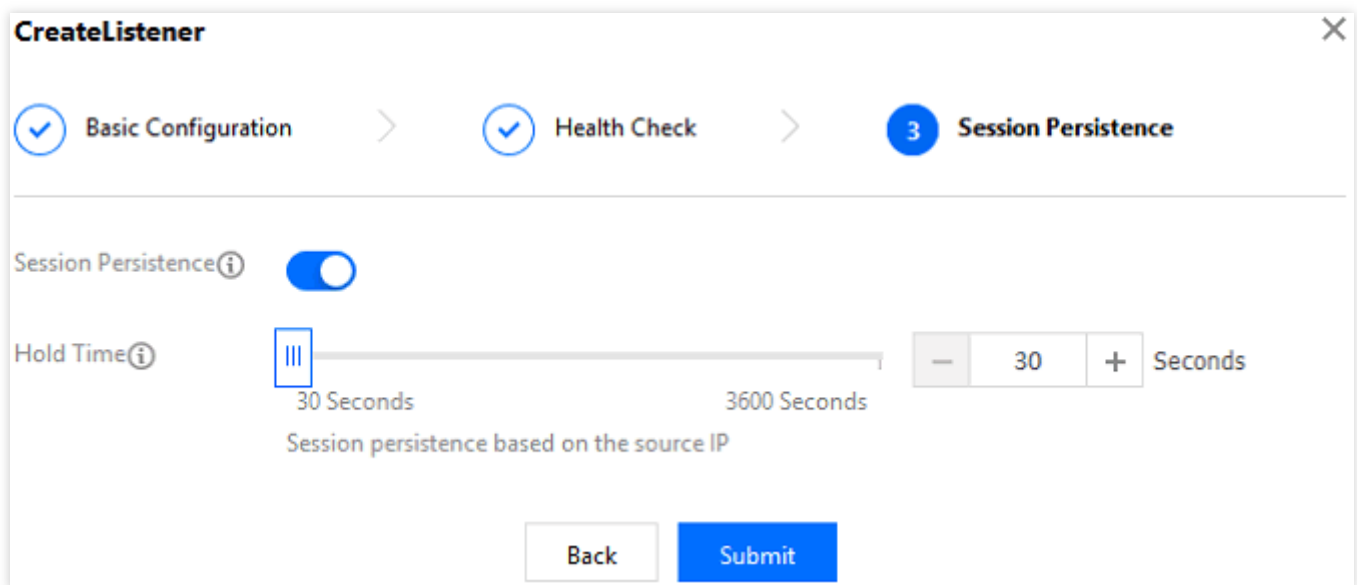


3.Persistensi sesi

| Item Konfigurasi | Deskripsi | Contoh |
|-------------------------|--|------------|
| Status persistensi sesi | Persistensi sesi bisa diaktifkan atau dinonaktifkan. Jika persistensi sesi diaktifkan, pendengar CLB akan mengirimkan permintaan akses dari klien yang sama ke server asli yang sama. Persistensi sesi UDP diimplementasikan berdasarkan alamat IP klien, misalnya, permintaan akses dari alamat IP yang sama diteruskan ke server asli yang sama. | Diaktifkan |

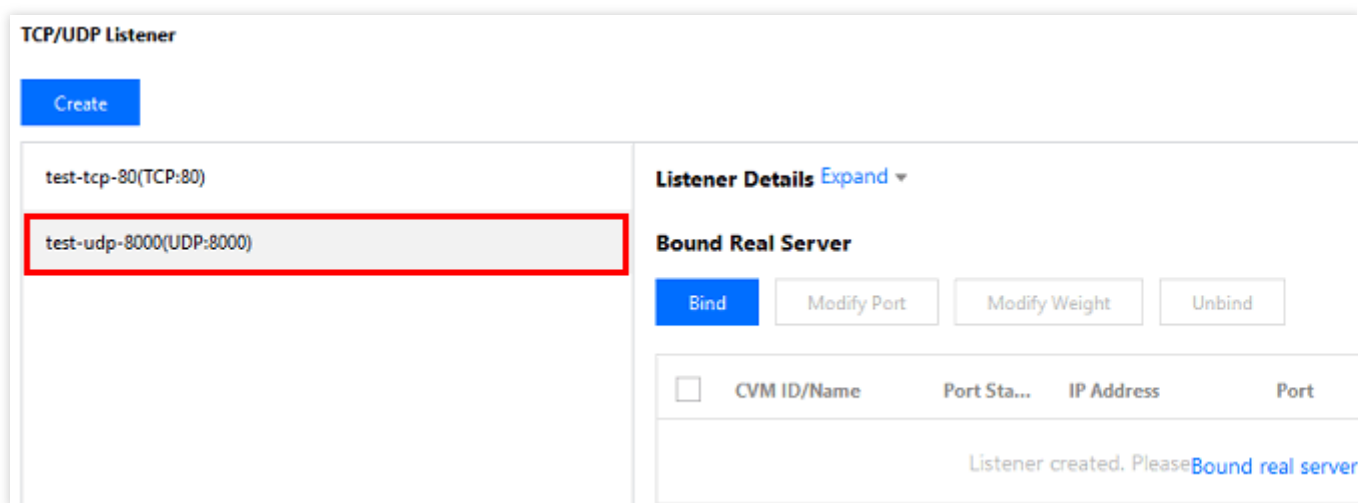
| | | |
|------------------------|--|-----|
| | Persistensi sesi bisa diaktifkan untuk penjadwalan WRR, tetapi tidak untuk penjadwalan WLC. | |
| Waktu persistensi sesi | Waktu persistensi sesi. Jika tidak ada permintaan baru di koneksi dalam waktu persistensi sesi, persistensi sesi akan diputus secara otomatis. Rentang nilai: 30-3,600s. | 30s |

Konfigurasi khusus persistensi sesi seperti yang ditunjukkan di bawah ini:



Langkah 3. Mengikat server asli

1. Di halaman "Manajemen Pendengar", klik pendengar `UDP : 8000` yang dibuat untuk melihat server asli yang diikat di sebelah kanan pendengar.



2. Klik **Bind** (Ikat), pilih server asli yang akan diikat dan konfigurasi port server dan bobot di jendela pop-up.

1. Tambahkan Port: Di kotak "Terpilih" di sebelah kanan, klik **Add Port** (Tambahkan Port) untuk menambahkan beberapa port untuk instance CVM yang sama, seperti port 80, 81, dan 82.

2. Port Default: Masukkan "Port Default" dahulu, kemudian pilih instance CVM. Port dari setiap instance CVM adalah port default.

Bound real server

IP

| ID/Name | Port | Weight |
|--|------|--------|
| <input checked="" type="checkbox"/> [Redacted] | 80 | 10 |
| <input checked="" type="checkbox"/> [Redacted] | 81 | 10 |
| <input checked="" type="checkbox"/> [Redacted] | 82 | 10 |

Note: When the private CLB is bound with one CVM, please DO NOT use this CVM as the client to access CLB.

Setelah tiga langkah ini selesai, aturan pendengar UDP sudah dikonfigurasi seperti yang ditunjukkan di bawah ini:

TCP/UDP Listener

Create

- test-tcp-80(TCP:80)
- test-udp-8000(UDP:8000)

Listener Details Expand ▾

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 80 |
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 81 |
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 82 |

Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Mengonfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi/hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang dibuat, klik pendengar di halaman "Manajemen Pendengar" dan pilih **Modify** (Modifikasi) atau **Delete** (Hapus).

TCP/UDP Listener

Create

- test-tcp-80(TCP:80)
- test-udp-8000(UDP:8000) Modify

Listener Details Expand ▾

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 80 |

Mengonfigurasi Pendengar TCP SSL

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Pendengar TCP SSL

Anda bisa menambahkan pendengar TCP SSL ke instance CLB untuk meneruskan permintaan TCP terenkripsi dari klien. Protokol TCP SSL cocok untuk skenario yang menuntut performa offloading TLS sangat tinggi dan skala besar. Dengan pendengar TCP SSL, server backend bisa memperoleh IP nyata klien secara langsung.

Keterangan :

Pendengar TCP SSL saat ini hanya mendukung CLB, tetapi tidak mendukung CLB klasik.

Prasyarat

Anda harus [membuat instance CLB](#) dahulu.

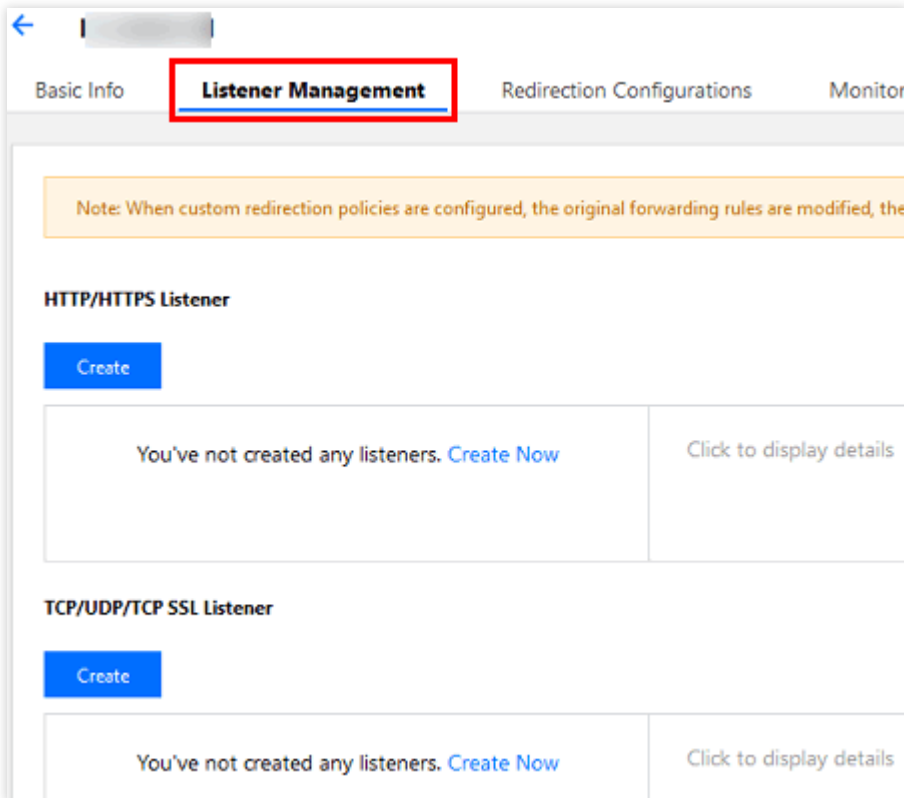
Mengonfigurasi Pendengar TCP SSL

Langkah 1. Buka halaman "Manajemen Pendengar"

1. Masuk ke [Konsol CLB](#).
2. Pilih **Instance Management** (Manajemen Instance) di bilah sisi kiri.
3. Di daftar instance, klik ID instance yang akan dikonfigurasi untuk masuk ke halaman detail instance.
4. Klik tab **Listener Management** (Manajemen Pendengar) atau klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operation" (Operasi).

The screenshot displays the 'CLB Instance List' interface. At the top, there are filters for various regions: Guangzhou(4), Shenzhen Finance, Shenzhen, Shanghai(5), Shanghai Finance, Nanjing, Beijing(5), Tianjin, Chengdu, Chongqing(1), Hong Kong, China(1), Singapore, Tokyo(2), Silicon Valley(1), Virginia(1), Toronto, Frankfurt(4), and Moscow(1). Below the filters, there are tabs for 'Cloud Load Balancer(2)' and 'Classic Cloud Load Balancer(2)'. A yellow notification banner reads: '"Application Load Balancer" has been renamed to "Cloud Load Balancer".' Below the banner are buttons for 'Create', 'Delete', 'Change Project', and 'Edit Tags'. On the right, there is a 'Project: All Projects' dropdown and a 'Use |' to split more tl' link. The main table has columns: ID/Name, Monitoring, Status, VIP, Network, and Health Status. The first row shows a red box around the ID/Name field, a monitoring icon, 'Normal' status, a greyed-out VIP field, 'Public Network', and 'Health check not enabled (Configuration)'. The creation time is '2019-03-27'.

5. Halaman "Listener Management" (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini:



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di **TCP/UDP/TCP SSL Listener** (Pendengar TCP/UDP/TCP SSL) dan konfigurasi pendengar TCP SSL di jendela pop-up.

1. Konfigurasi dasar

| Item Konfigurasi | Deskripsi | Contoh |
|---|--|--|
| Nama | Nama pendengar | test-tcpsl-9000 |
| Protokol pendengar dan port pendengaran | Protokol pendengar dan port pendengaran. Protokol pendengar: CLB mendukung berbagai protokol, termasuk TCP, UDP, TCP SSL, HTTP, dan HTTPS. TCP SSL digunakan dalam contoh ini. Port pendengaran: Port digunakan untuk menerima permintaan dan meneruskannya ke server asli. Rentang port: 1-65535. Port pendengar harus unik di instance CLB yang sama. | TCP SSL:9000 |
| Mertode parsing SSL | Mendukung autentikasi satu arah dan autentikasi bersama | Autentikasi satu arah |
| Sertifikat server | Anda bisa memilih sertifikat yang ada di layanan sertifikat SSL atau mengunggah sertifikat | Pilih sertifikat yang ada cc/UzxFoXsE |
| | | |

| | | |
|-----------------------------|---|------------|
| <p>Metode penyeimbangan</p> | <p>Untuk pendengar TCP SSL, CLB mendukung dua algoritme penjadwalan: round robin tertimbang (WRR) dan koneksi terkecil tertimbang (WLC). WRR:Permintaan dikirimkan secara berurutan ke server-server asli berbeda sesuai bobotnya.Penjadwalan dilakukan berdasarkan jumlah koneksi baru, tempat server dengan bobot lebih tinggi akan melalui lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi), sementara server dengan bobot yang sama memproses jumlah koneksi yang sama. WLC:Beban server dinilai sesuai dengan jumlah koneksi aktif ke server-server.Penjadwalan dilakukan berdasarkan beban dan bobot server.Jika bobotnya sama, server dengan koneksi aktif yang lebih sedikit akan menjalani lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).</p> | <p>WRR</p> |
|-----------------------------|---|------------|

Konfigurasi tertentu pendengar TCP SSL yang dibuat adalah seperti yang ditunjukkan di bawah ini:

2.Pemeriksaan kesehatan

| Item | Deskripsi | Contoh |
|------|-----------|--------|
|------|-----------|--------|

| Konfigurasi | | |
|------------------------------|---|------------|
| Status pemeriksaan kesehatan | Pemeriksaan kesehatan bisa diaktifkan atau dinonaktifkan. Di pendengar TCP SSL, instance CLB mengirimkan paket SYN ke port server tertentu untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Periode waktu habis respons | Periode waktu habis respons maksimum untuk pemeriksaan kesehatan. Jika satu server asli gagal merespons dengan tepat dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal. Rentang nilai: 2-60s. Nilai default: 2s. | 2s |
| Interval pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300s. Nilai default: 5s. | 5s |
| Ambang batas tidak sehat | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) gagal berturut-turut, instance akan dianggap tidak sehat, dan status yang ditampilkan di konsol akan menjadi Abnormal . Rentang nilai: 2-10. Nilai default: 3. | 3 kali |
| Ambang batas sehat | Jika hasil pemeriksaan kesehatan menerima n kali (n adalah jumlah yang dimasukkan) berhasil berturut-turut, instance akan dianggap sehat, dan status yang ditampilkan di konsol akan menjadi Healthy (Sehat). Rentang nilai: 2-10. Nilai default: 3. | 3 kali |

Konfigurasi khusus pemeriksaan kesehatannya seperti yang ditunjukkan di bawah ini:

CreateListener

Basic Configuration > **2 Health Check** > 3 Session Persistence

Health Check [Hide Advanced Options ▲](#)

Response Timeout Seconds Seconds

Check Interval Seconds Seconds

Unhealthy Threshold Times Times

Healthy Threshold Times Times

3.Persistensi sesi (saat ini tidak didukung)

CreateListener

Basic Configuration > Health Check > **3 Session Persistence**

Session Persistence [Not supported ⓘ](#)

Langkah 3.Mengikat server asli

1.Di halaman "Manajemen Pendengar", klik pendengar `TCP SSL : 9000` yang dibuat untuk melihat server asli yang diikat di sebelah kanan pendengar.

TCP/UDP/TCP SSL Listener

Create

- test-tcp-80(TCP:80)
- test-udp-8000(UDP:8000)
- test-tcpsl-9000(TCP SSL:9000)**

Listener Details Expand ▾

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--|-------------|-------------|------------|------|
| Listener created. Please Bound real server | | | | |

2. Klik **Bind** (Ikut), pilih server asli yang akan diikat dan konfigurasi port server dan bobot di jendela pop-up.

1. Tambahkan Port: Di kotak "Terpilih" di sebelah kanan, klik **Add Port** (Tambahkan Port) untuk menambahkan beberapa port untuk instance CVM yang sama, seperti port 80, 81, dan 82.

2. Port Default: Masukkan "Port Default" dahulu, kemudian pilih instance CVM. Port dari setiap instance CVM adalah port default.

Bound real server

IP ▾ Enter IP Address 🔍

| <input checked="" type="checkbox"/> | ID/Name |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |

Selected (3)

| ID/Name | Port | Weight |
|------------|------|--------|
| [Redacted] | 80 | 10 |
| [Redacted] | 81 | 10 |
| [Redacted] | 82 | 10 |

Note: When the private CLB is bound with one CVM, please DO NOT use this CVM as the client to access CLB.

OK Cancel

Setelah tiga langkah ini selesai, aturan pendengar TCP SSL sudah dikonfigurasi seperti yang ditunjukkan di bawah ini:

The screenshot displays the 'TCP/UDP/TCP SSL Listener' configuration page. On the left, a list of listeners is shown, with 'test-tcpsl-9000(TCP SSL:9000)' selected. On the right, the 'Listener Details' section is expanded, showing the 'Bound Real Server' configuration. A table lists three real servers, all with a 'Healthy' status and ports 80, 81, and 82.

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [Redacted] | Healthy | [Redacted] | 80 |
| <input type="checkbox"/> | [Redacted] | Healthy | [Redacted] | 81 |
| <input type="checkbox"/> | [Redacted] | Healthy | [Redacted] | 82 |

Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Mengonfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi/hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang dibuat, klik pendengar di halaman "Manajemen Pendengar" dan pilih **Modify** (Modifikasi) atau **Delete** (Hapus).

TCP/UDP/TCP SSL Listener

Create

test-tcp-80(TCP:80)

test-udp-8000(UDP:8000)

test-tcpsl-9000(TCP SSL:9000) Modify

Listener Details [Expand](#)

Bound Real Server

[Bind](#) [Modify Port](#) [Modify Weight](#) [Unbind](#)

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | | Healthy | | 80 |

Mengonfigurasi Pendengar HTTP

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Pendengar HTTP

Anda bisa membuat pendengar HTTP ke instance CLB untuk meneruskan permintaan HTTP dari klien. HTTP cocok untuk aplikasi tempat konten permintaan perlu diidentifikasi, seperti aplikasi web dan aplikasi seluler.

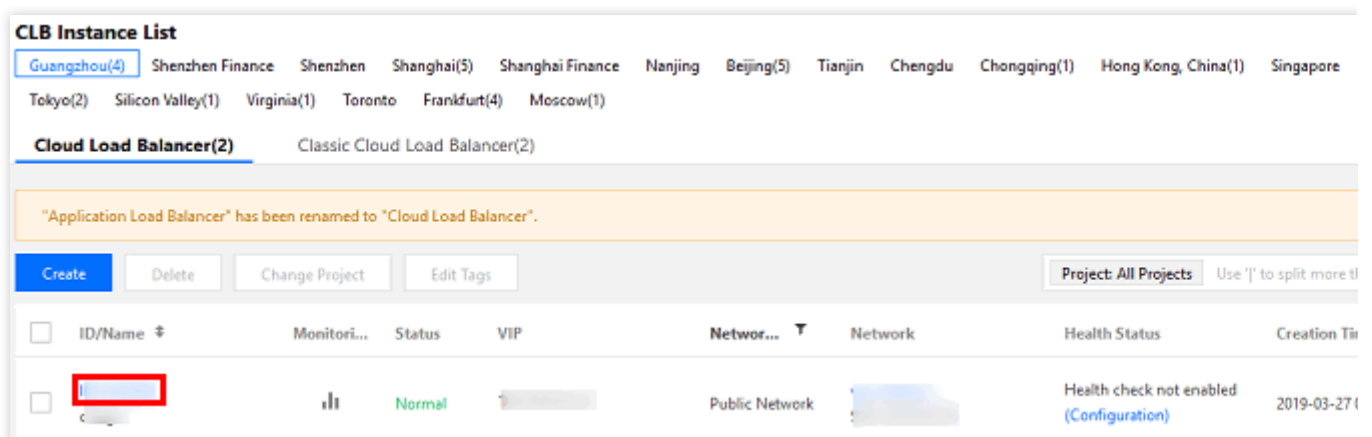
Prasyarat

Anda harus [membuat instance CLB](#) dahulu.

Mengonfigurasi Pendengar HTTP

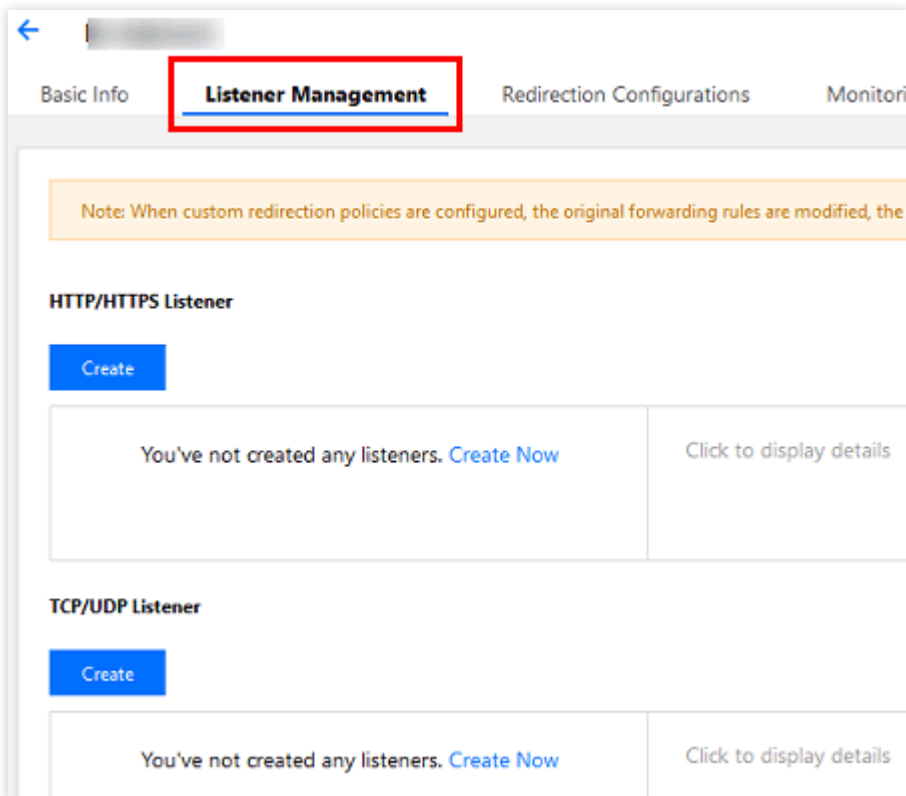
Langkah 1. Buka tab Listener Management (Manajemen Pendengar)

1. Masuk ke [Konsol CLB](#).
2. Pilih **CLB Instance List** (Daftar Instance CLB) di bilah sisi kiri.
3. Di daftar instance, klik ID instance untuk masuk ke halaman detail.
4. Buka tab **Listener Management** (Manajemen Pendengar). Anda juga bisa masuk ke halaman dengan mengklik **Configure Listener** (Konfigurasi Pendengar) di bawah kolom **Operation** (Operasi) instance.



The screenshot displays the 'CLB Instance List' interface. At the top, there are tabs for various regions: Guangzhou(4), Shenzhen Finance, Shenzhen, Shanghai(5), Shanghai Finance, Nanjing, Beijing(5), Tianjin, Chengdu, Chongqing(1), Hong Kong, China(1), Singapore, Tokyo(2), Silicon Valley(1), Virginia(1), Toronto, Frankfurt(4), and Moscow(1). Below these, there are sub-tabs for 'Cloud Load Balancer(2)' and 'Classic Cloud Load Balancer(2)'. A yellow notification banner reads: "Application Load Balancer" has been renamed to "Cloud Load Balancer". Below the notification, there are buttons for 'Create', 'Delete', 'Change Project', and 'Edit Tags'. On the right, there is a 'Project: All Projects' dropdown and a 'Use |' to split more tabs' option. The main table has columns: ID/Name, Monitoring, Status, VIP, Network, Health Status, and Creation Time. The first row shows a red box around the ID/Name 'Guangzhou(4)', a monitoring icon, a 'Normal' status, a greyed-out VIP, 'Public Network', and 'Health check not enabled (Configuration)'. The creation time is '2019-03-27'.

5. Tab **Listener Management** (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini:



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di bagian **HTTP/HTTPS Listener** (Pendengar HTTP/HTTPS) dan konfigurasi pendengar HTTP di jendela pop-up.

1. Buat pendengar

| Item Konfigurasi | Deskripsi | Contoh |
|-----------------------------|---|--------------|
| Nama | Nama pendengar | test-http-80 |
| Protokol dan port pendengar | <p>Protokol dan port pendengaran dari satu pendengar:</p> <p>Protokol pendengaran: CLB mendukung berbagai protokol, termasuk TCP, UDP, TCP SSL, HTTP, dan HTTPS. HTTP digunakan dalam contoh ini.</p> <p>Port pendengaran: Port digunakan untuk menerima permintaan dan meneruskannya ke server asli. Rentang port: 1 - 65535. Port-port ini sudah dicadangkan dan saat ini tidak tersedia bagi pengguna: 843, 1020, 1433, 1434, 3306, 3389, 6006, 20000, 36000, 42222, 48369, 56000, dan 65010.</p> <p>Port pendengaran dari setiap instance CLB harus unik.</p> | HTTP:80 |

Konfigurasi tertentu pendengar HTTP yang dibuat adalah seperti yang ditunjukkan di bawah ini:

CreateListener

Name

Listen Protocol Ports HTTP : 80

2. Buat aturan penerusan

| Item Konfigurasi | Deskripsi | Contoh |
|----------------------|---|-----------------|
| Nama domain | <p>Nama domain penerusan: Panjang: 1 - 80 karakter. Garis bawah (_) tidak bisa menjadi karakter pertama. Mendukung nama domain persis dan kartubebas. Mendukung ekspresi reguler. Untuk aturan konfigurasi selengkapnya, silakan lihat Aturan Penerusan Nama Domain dan URL Lapisan 7.</p> | www.example.com |
| Nama domain default | <p>Jika semua nama domain pendengar tidak cocok, sistem akan mengarahkan permintaan ke nama domain default sehingga akses default terkendali. Setiap pendengar hanya bisa dikonfigurasi dengan satu nama domain default.</p> | Diaktifkan |
| Jalur URL | <p>Jalur URL penerusan: Panjang: 1 - 200 karakter. Mendukung ekspresi reguler. Untuk aturan konfigurasi selengkapnya, silakan lihat Aturan Penerusan Nama Domain dan URL Lapisan 7.</p> | /index |
| Metode penyeimbangan | <p>Untuk pendengar HTTP, CLB mendukung tiga algoritme penjadwalan: round robin tertimbang (WRR), koneksi terkecil tertimbang (WLC), dan hash IP. WRR:Permintaan dikirimkan secara berurutan ke server-server asli berbeda sesuai bobotnya.Penjadwalan dilakukan berdasarkan number of new connections (jumlah koneksi baru), tempat server dengan bobot lebih tinggi akan melalui lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi), sementara server dengan bobot yang sama memproses jumlah koneksi yang sama.</p> | WRR |

| | | |
|----------------------|--|------------|
| | <p>WLC: Beban server dinilai sesuai dengan jumlah koneksi aktif ke server-server. Penjadwalan dilakukan berdasarkan beban dan bobot server. Jika bobotnya sama, server dengan koneksi aktif yang lebih sedikit akan menjalani lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).</p> <p>Hash IP: Kunci hash digunakan untuk menemukan server terkait di tabel hash statis berdasarkan IP sumber permintaan-permintaan. Jika server tersedia dan tidak kelebihan beban, permintaan akan dikirimkan ke sana; jika tidak, nilai nol akan dikembalikan.</p> | |
| Mendapatkan IP klien | Diaktifkan secara default | Diaktifkan |
| Kompresi Gzip | Diaktifkan secara default | Diaktifkan |

Pilih pendengar HTTP yang akan dibuatkan aturan penerusan dan klik + di sebelah kanan. Konfigurasi khususnya seperti yang ditunjukkan di bawah ini:

Create Forwarding rules ✕

1 **Basic Configuration** > 2 Health Check > 3 Session Persistence

Domain Name ⓘ

URL ⓘ

Balance Method ▼

If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Get client IP Enabled

Gzip compression Enabled ⓘ

3. Pemeriksaan kesehatan

| Item Konfigurasi | Deskripsi | Contoh |
|------------------|-----------|--------|
| | | |

| | | |
|------------------------------|--|---|
| Status pemeriksaan kesehatan | Pemeriksaan kesehatan bisa diaktifkan atau dinonaktifkan. Di pendengar HTTP, instance CLB mengirimkan permintaan HTTP ke port server tertentu untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Nama domain pemeriksaan | Nama domain pemeriksaan kesehatan: Panjang: 1 - 80 karakter. Ini diatur secara default ke nama domain penerusan. Tidak mendukung ekspresi reguler. Jika nama domain penerusan Anda adalah kartubebas, Anda harus menentukan nama tetap (non-ekspresi reguler) sebagai nama domain pemeriksaan kesehatan. Karakter yang didukung: <code>a-z0-9.-</code> . | <code>www.example.com</code> (nilai default) |
| Jalur pemeriksaan | Jalur pemeriksaan kesehatan: Panjang: 1 - 200 karakter. Ini diatur secara default ke <code>/</code> dan harus dimulai dengan <code>/</code> . Tidak mendukung ekspresi reguler. Kami menyarankan untuk menentukan jalur URL tetap (halaman statis) untuk pemeriksaan kesehatan. Karakter yang didukung: <code>a-zA-Z0-9.-_/?</code> . | <code>/</code> (nilai default) |
| Waktu habis respons | Waktu habis respons maksimum untuk pemeriksaan kesehatan. Jika satu server asli gagal merespons dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal. Rentang nilai: 2 - 60 detik. Nilai default: 2 detik. | 2 detik |
| Interval pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5 - 300 detik. Nilai default: 5 detik. | 5 detik |
| Ambang batas tidak sehat | Jika hasil pemeriksaan kesehatan gagal <code>n</code> (nilai khusus) kali berturut-turut, server asli itu tidak sehat dan Abnormal ditampilkan di konsol. Rentang nilai: 2 - 10 kali. Nilai default: 3 kali | 3 kali |
| Ambang batas sehat | Jika hasil pemeriksaan kesehatan berhasil <code>n</code> (nilai khusus) kali berturut-turut, server asli itu sehat dan Healthy (Sehat) ditampilkan di konsol. Rentang nilai: 2 - 10 kali. Nilai default: 3 kali | 3 kali |
| Metode permintaan HTTP | Metode permintaan HTTP untuk pemeriksaan kesehatan. Nilai yang valid: GET (nilai default) dan HEAD: Jika HEAD digunakan, server hanya akan mengembalikan header HTTP, yang bisa mengurangi overhead backend dan meningkatkan efisiensi permintaan. Server asli harus mendukung HEAD. Jika GET digunakan, server asli harus mendukung GET. | GET |
| Pemeriksaan kode status HTTP | Jika kode status termasuk yang terpilih, server asli dianggap hidup (sehat). Rentang nilai: <code>http_1xx</code> , <code>http_2xx</code> , <code>http_3xx</code> , <code>http_4xx</code> , dan <code>http_5xx</code> . | Beberapa nilai dipilih: <code>http_1xx</code> , <code>http_2xx</code> , |

http_3xx, dan
http_4xx.

Konfigurasi khusus pemeriksaan kesehatannya seperti yang ditunjukkan di bawah ini:

Create Forwarding rules

Basic Configuration > **2 Health Check** > 3 Session Persistence

Health Check

Check Domain

Path

Hide Advanced Options ▲

Check Interval 5 Seconds 300 Seconds 5 Seconds

Unhealthy Threshold 2 Times 10 Times 3 Times

Healthy Threshold 2 Times 10 Times 3 Times

HTTP Request Method

HTTP Status Code Detection http_1xx http_2xx http_3xx http_4xx http_5xx

When the status code is http_1xx, http_2xx, http_3xx, http_4xx, the back-end server is considered active

4.Persistensi sesi

| Item Konfigurasi | Deskripsi | Contoh |
|-------------------------|--|------------|
| Status persistensi sesi | Jika persistensi sesi diaktifkan, pendengar CLB akan mengirimkan permintaan akses dari klien yang sama ke server asli yang sama. Persistensi sesi HTTP diimplementasikan berdasarkan cookies, yang ditanamkan pada klien dengan instance CLB. | Diaktifkan |

| | | |
|--------------------------|---|----------|
| | Persistensi sesi bisa diaktifkan untuk penjadwalan WRR tetapi tidak untuk penjadwalan WLC atau hash IP. | |
| Periode persistensi sesi | Periode persistensi sesi: Jika tidak ada permintaan baru di koneksi dalam periode persistensi sesi, sesi akan terputus secara otomatis. Rentang nilai: 30 - 3600 detik. | 30 detik |

Konfigurasi khusus persistensi sesi seperti yang ditunjukkan di bawah ini:

Create Forwarding rules

Basic Configuration > Health Check > **3 Session Persistence**

Session Persistence

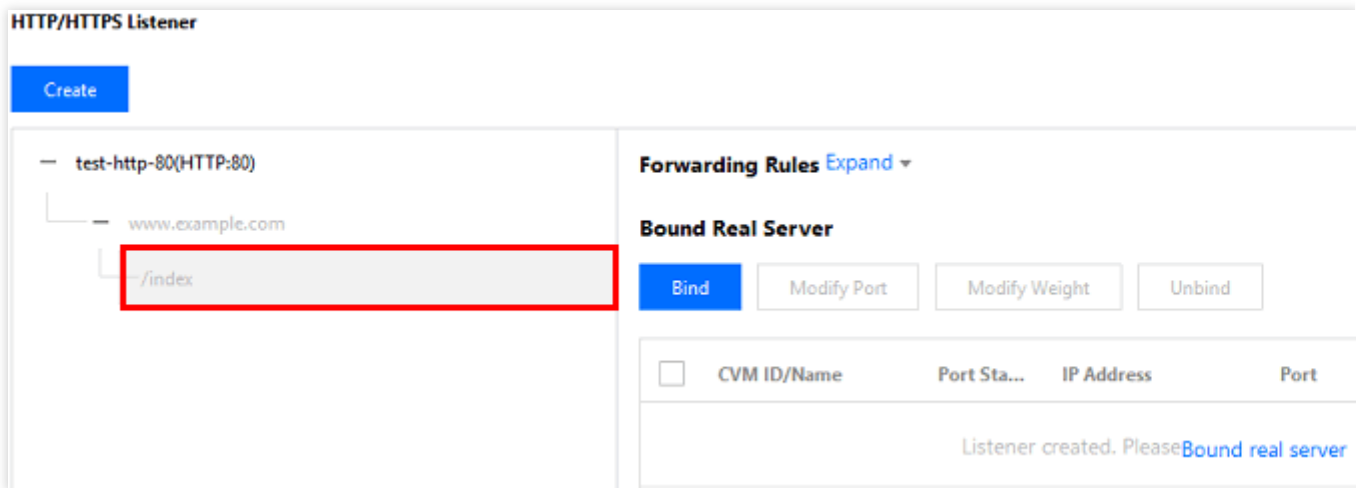
Hold Time 30 Seconds 3600 Seconds Seconds

Session persistence with cookies

Back Submit

Langkah 3. Mengikat server asli

1. Di halaman **Listener Management** (Manajemen Pendengar) pilih pendengar `HTTP : 80` yang dibuat. Klik **+** di sebelah kiri untuk memperluas nama domain dan jalur URL, pilih jalur URL yang diinginkan, dan lihat server asli yang terikat pada jalur itu di sebelah kanan pendengar.



2. Klik **Bind** (Ikat), pilih server asli target, konfigurasi port server dan beban di jendela pop-up.

① Tambahkan port: Di kotak **Selected** (Terpilih) di sebelah kanan, klik **Add Port** (Tambahkan Port) untuk menambahkan beberapa port untuk instance CVM yang sama, seperti port 80, 81, dan 82.

② Port default: Masukkan **Default Port** (Port Default) dahulu, kemudian pilih instance CVM. Port dari setiap instance CVM adalah port default.

Bound real server

IP

| <input checked="" type="checkbox"/> ID/Name | Selected (3) | | |
|--|--------------|---------------------------------|--|
| <input checked="" type="checkbox"/> [Redacted] | ID/Name | Port | Weight |
| <input checked="" type="checkbox"/> [Redacted] | [Redacted] | <input type="text" value="80"/> | <input type="button" value="-"/> <input type="text" value="10"/> |
| <input checked="" type="checkbox"/> [Redacted] | [Redacted] | <input type="text" value="81"/> | <input type="button" value="-"/> <input type="text" value="10"/> |
| <input checked="" type="checkbox"/> [Redacted] | [Redacted] | <input type="text" value="82"/> | <input type="button" value="-"/> <input type="text" value="10"/> |

Note: When the private CLB is bound with one CVM, please DO NOT use this CVM as the client to access CLB.

Setelah tiga langkah ini selesai, aturan pendengar HTTP sudah dikonfigurasi seperti yang ditunjukkan di bawah ini:

HTTP/HTTPS Listener

Create

test-http-80(HTTP:80)

- www.example.com
 - /index

Forwarding Rules Expand ▾

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [Redacted] | Abnormal | [Redacted] | 80 |
| <input type="checkbox"/> | [Redacted] | Abnormal | [Redacted] | 81 |
| <input type="checkbox"/> | [Redacted] | Abnormal | [Redacted] | 82 |

Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Konfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi dan hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang dibuat, klik pendengar/nama domain/jalur URL pada tab **Listener Management** (Manajemen Pendengar) dan pilih **Modify** (Modifikasi) atau **Delete** (Hapus).

HTTP/HTTPS Listener

Create

test-http-80(HTTP:80)

- www.example.com
 - /index

Forwarding Rules Expand ▾

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [Redacted] | Abnormal | [Redacted] | 80 |

Mengonfigurasi Pendengar HTTPS

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Pendengar HTTPS

Anda bisa membuat pendengar HTTPS ke instance CLB untuk meneruskan permintaan HTTPS dari klien. HTTPS cocok untuk aplikasi HTTP, tempat transfer data perlu dienkripsi.

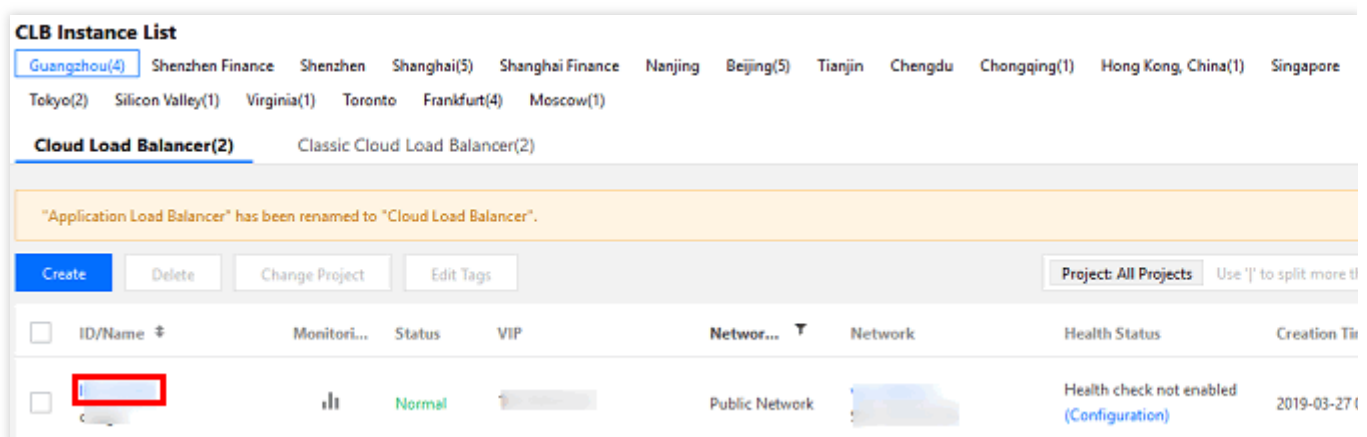
Prasyarat

Anda harus [membuat instance CLB](#) dahulu.

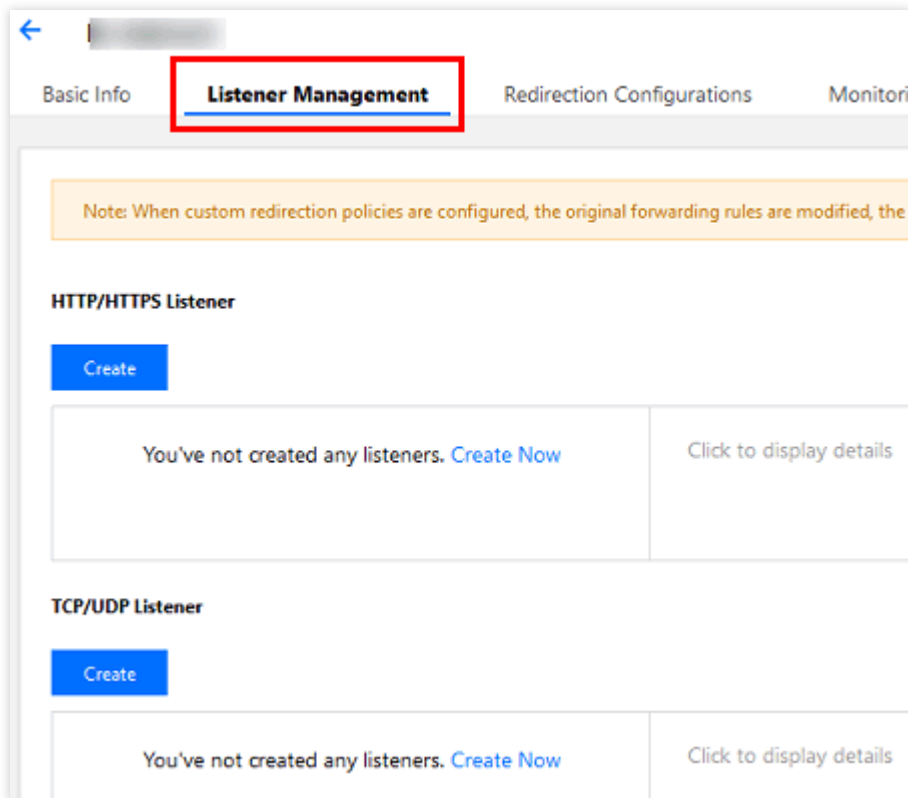
Mengonfigurasi Pendengar HTTPS

Langkah 1. Buka tab Listener Management (Manajemen Pendengar)

1. Masuk ke [Konsol CLB](#).
2. Pilih **CLB Instance List** (Daftar Instance CLB) di bilah sisi kiri.
3. Di daftar instance, klik ID instance untuk masuk ke halaman detail.
4. Buka tab **Listener Management** (Manajemen Pendengar). Anda juga bisa masuk ke halaman dengan mengklik **Configure Listener** (Konfigurasi Pendengar) di bawah kolom **Operation** (Operasi) instance.



5. Halaman "Listener Management" (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini:



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di **HTTP/HTTPS Listener** (Pendengar HTTP/HTTPS) dan konfigurasi pendengar HTTPS di jendela pop-up.

1. Buat pendengar

| Item Konfigurasi | Deskripsi | Contoh |
|-----------------------------|---|----------------|
| Nama | Nama pendengar | test-https-443 |
| Protokol dan port pendengar | Protokol dan port pendengaran dari satu pendengar: Protokol pendengaran: CLB mendukung berbagai protokol, termasuk TCP, UDP, TCP SSL, HTTP, dan HTTPS. HTTPS digunakan dalam contoh ini. Port pendengaran: Port digunakan untuk menerima permintaan dan meneruskannya ke server asli. Rentang port: 1 - 65535. Port-port ini sudah dicadangkan dan saat ini tidak tersedia bagi pengguna: 843, 1020, 1433, 1434, 3306, 3389, 6006, 20000, 36000, 42222, 48369, 56000, dan 65010. Port pendengaran dari setiap instance CLB harus unik. | HTTPS:443 |
| Aktifkan SNI | Jika SNI diaktifkan, beberapa nama domain dari satu pendengar bisa dikonfigurasi dengan sertifikat berbeda; jika dinonaktifkan, beberapa | Dinonaktifkan |

| | | |
|--------------------|--|---------------------------------------|
| | nama domain dari satu pendengar hanya bisa dikonfigurasi dengan satu sertifikat. | |
| Metode parsing SSL | Mendukung autentikasi satu arah dan autentikasi bersama | Autentikasi satu arah |
| Sertifikat server | Anda bisa memilih sertifikat yang ada di layanan sertifikat SSL atau mengunggah sertifikat | Pilih sertifikat yang ada cc/UzxFoXsE |

Konfigurasi tertentu pendengar HTTPS yang dibuat adalah seperti yang ditunjukkan di bawah ini:

Create Listener ✕

Name

Listen Protocol Ports :

SSL Phrasing [Detailed Comparison](#) 🔗

Note: Choose SSL two-way authentication if you also need a certificate from the client.

Server Certificate Select existing Create

1. If you select HTTPS protocol for forwarding, the accesses from client to load balancer is encrypted with HTTPS protocol. HTTP protocol is adopted to forward requests from load balancers to backend CVM.

2. The load balancer serves as an agent for the overhead of SSL encryption and decryption, and ensures Web access security.

3. You can go to [SSL Certificate Management Platform](#) to apply for an SSL certificate for free.

2. Buat aturan penerusan

| Item Konfigurasi | Deskripsi | Contoh |
|------------------|---|-----------------|
| Nama domain | Nama domain penerusan: Panjang: 1 - 80 karakter. | www.example.com |

| | | |
|----------------------|--|------------|
| | <p>Garis bawah (_) tidak bisa menjadi karakter pertama.</p> <p>Mendukung nama domain persis dan kartubebas.</p> <p>Mendukung ekspresi reguler.</p> <p>Untuk aturan konfigurasi selengkapnya, silakan lihat Aturan Penerusan Nama Domain dan URL Lapisan 7.</p> | |
| Nama domain default | <p>Jika semua nama domain pendengar tidak cocok, sistem akan mengarahkan permintaan ke nama domain default sehingga akses default terkendali.</p> <p>Setiap pendengar hanya bisa dikonfigurasi dengan satu nama domain default.</p> | Diaktifkan |
| HTTP 2.0 | <p>Setelah HTTP 2.0 diaktifkan, instance CLB bisa menerima permintaan HTTP 2.0. Instance CLB mengakses server asli melalui HTTP 1.1 apa pun versi HTTP yang digunakan klien untuk mengakses instance CLB.</p> | Diaktifkan |
| Jalur URL | <p>Jalur URL penerusan:</p> <p>Panjang: 1 - 200 karakter.</p> <p>Mendukung ekspresi reguler.</p> <p>Untuk aturan konfigurasi selengkapnya, silakan lihat Aturan Penerusan Nama Domain dan URL Lapisan 7.</p> | /index |
| Metode penyeimbangan | <p>Untuk pendengar HTTPS, CLB mendukung tiga algoritme penjadwalan: round robin tertimbang (WRR), koneksi terkecil tertimbang (WLC), dan hash IP.</p> <p>WRR:Permintaan dikirimkan secara berurutan ke server-server asli berbeda sesuai bobotnya. Penjadwalan dilakukan berdasarkan number of new connections (jumlah koneksi baru), tempat server dengan bobot lebih tinggi akan melalui lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi), sementara server dengan bobot yang sama memproses jumlah koneksi yang sama.</p> <p>WLC: Beban server dinilai sesuai dengan jumlah koneksi aktif ke server-server. Penjadwalan dilakukan berdasarkan beban dan bobot server. Jika bobotnya sama, server dengan koneksi aktif yang lebih sedikit akan menjalani lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).</p> <p>Hash IP: Kunci hash digunakan untuk menemukan server terkait di tabel hash statis berdasarkan IP sumber permintaan-permintaan. Jika server tersedia dan tidak kelebihan beban, permintaan akan dikirimkan ke sana; jika tidak, nilai nol akan dikembalikan.</p> | WRR |
| Protokol backend | <p>Protokol backend di-deploy antara instance CLB dan server asli:</p> <p>Jika HTTP dipilih sebagai protokol backend, layanan HTTP harus di-deploy di server asli.</p> | HTTP |

| | | |
|----------------------|---|------------|
| | Jika HTTPS dipilih sebagai protokol backend, layanan HTTPS harus di-deploy di server asli, dan enkripsi dan deskripsi layanan HTTPS akan mengonsumsi lebih banyak sumber daya di server asli. | |
| Mendapatkan IP klien | Diaktifkan secara default | Diaktifkan |
| Kompresi Gzip | Diaktifkan secara default | Diaktifkan |

Pilih pendengar HTTPS yang akan dibuatkan aturan penerusan dan klik + di sebelah kanan. Konfigurasi khususnya seperti yang ditunjukkan di bawah ini:

Create Forwarding rules

1 Basic Configuration >
2 Health Check >
3 Session Persistence

Domain Name ⓘ

URL ⓘ

Balance Method

If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Get client IP Enabled

Gzip compression Enabled ⓘ

3. Pemeriksaan kesehatan

| Item Konfigurasi | Deskripsi | Contoh |
|------------------------------|--|------------------------------------|
| Status pemeriksaan kesehatan | Pemeriksaan kesehatan bisa diaktifkan atau dinonaktifkan. Di pendengar HTTPS, instance CLB mengirimkan permintaan HTTPS ke port server tertentu untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Nama domain pemeriksaan | Nama domain pemeriksaan kesehatan: Panjang: 1 - 80 karakter. Ini diatur secara default ke nama domain penerusan. | www.example.com (nilai default) |

| | | |
|------------------------------|--|---|
| | <p>Tidak mendukung ekspresi reguler. Jika nama domain penerusan Anda adalah kartubebas, Anda harus menentukan nama tetap (non-ekspresi reguler) sebagai nama domain pemeriksaan kesehatan.</p> <p>Karakter yang didukung: <code>a-z0-9.-</code> .</p> | |
| Jalur pemeriksaan | <p>Jalur pemeriksaan kesehatan: Panjang: 1 - 200 karakter. Ini diatur secara default ke <code>/</code> dan harus dimulai dengan <code>/</code> . Tidak mendukung ekspresi reguler. Kami menyarankan untuk menentukan jalur URL tetap (halaman statis) untuk pemeriksaan kesehatan. Karakter yang didukung: <code>a-zA-Z0-9.-_/?</code> .</p> | <code>/</code> (nilai default) |
| Waktu habis respons | <p>Waktu habis respons maksimum untuk pemeriksaan kesehatan. Jika satu server asli gagal merespons dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal. Rentang nilai: 2 - 60 detik. Nilai default: 2 detik.</p> | 2 detik |
| Interval pemeriksaan | <p>Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5 - 300 detik. Nilai default: 5 detik.</p> | 5 detik |
| Ambang batas tidak sehat | <p>Jika hasil pemeriksaan kesehatan gagal n (nilai khusus) kali berturut-turut, server asli itu tidak sehat dan Abnormal ditampilkan di konsol. Rentang nilai: 2 - 10 kali. Nilai default: 3 kali</p> | 3 kali |
| Ambang batas sehat | <p>Jika hasil pemeriksaan kesehatan berhasil n (nilai khusus) kali berturut-turut, server asli itu sehat dan Healthy (Sehat) ditampilkan di konsol. Rentang nilai: 2 - 10 kali. Nilai default: 3 kali</p> | 3 kali |
| Metode permintaan HTTP | <p>Metode permintaan HTTP untuk pemeriksaan kesehatan. Nilai yang valid: GET (nilai default) dan HEAD: Jika HEAD digunakan, server hanya akan mengembalikan informasi header HTTP, yang bisa mengurangi overhead backend dan meningkatkan efisiensi permintaan. Server asli harus mendukung HEAD. Jika GET digunakan, server asli harus mendukung GET.</p> | GET |
| Pemeriksaan kode status HTTP | <p>Jika kode status termasuk yang terpilih, server asli dianggap hidup (sehat). Rentang nilai: <code>http_1xx</code>, <code>http_2xx</code>, <code>http_3xx</code>, <code>http_4xx</code>, dan <code>http_5xx</code>.</p> | Beberapa nilai dipilih: <code>http_1xx</code> , <code>http_2xx</code> , <code>http_3xx</code> , dan <code>http_4xx</code> . |

Konfigurasi khusus pemeriksaan kesehatannya seperti yang ditunjukkan di bawah ini:

Create Forwarding rules

1 Basic Configuration >
2 Health Check >
3 Session Persistence

Health Check (i)

Check Domain (i)

Path (i)

Hide Advanced Options ▲

Check Interval 5 Seconds 300 Seconds Seconds

Unhealthy Threshold (i) 2 Times 10 Times Times

Healthy Threshold (i) 2 Times 10 Times Times

HTTP Request Method (i)

HTTP Status Code Detection http_1xx http_2xx http_3xx http_4xx http_5xx

When the status code is http_1xx, http_2xx, http_3xx, http_4xx, the back-end server is considered active

4. Persistensi sesi

| Item Konfigurasi | Deskripsi | Contoh |
|-------------------------|---|------------|
| Status persistensi sesi | <p>Persistensi sesi bisa diaktifkan atau dinonaktifkan:</p> <p>Jika persistensi sesi diaktifkan, pendengar CLB akan mengirimkan permintaan akses dari klien yang sama ke server asli yang sama.</p> <p>Persistensi sesi HTTPS diimplementasikan berdasarkan cookies, yang ditanamkan pada klien dengan instance CLB.</p> <p>Persistensi sesi bisa diaktifkan untuk penjadwalan WRR tetapi tidak untuk penjadwalan WLC atau hash IP.</p> | Diaktifkan |

| | | |
|--------------------------|---|----------|
| Periode persistensi sesi | Periode persistensi sesi: Jika tidak ada permintaan baru di koneksi dalam periode persistensi sesi, sesi akan terputus secara otomatis. Rentang nilai: 30 - 3600 detik. | 30 detik |
|--------------------------|---|----------|

Konfigurasi khusus persistensi sesi seperti yang ditunjukkan di bawah ini:

Create Forwarding rules

Basic Configuration > Health Check > **3 Session Persistence**

Session Persistence

Hold Time 30 Seconds 3600 Seconds Seconds

Session persistence with cookies

Back Submit

Langkah 3. Mengikat server asli

1. Di halaman "Manajemen Pendengar", pilih pendengar `HTTPS : 443` yang dibuat. Klik **+** di sebelah kiri untuk memperluas nama domain dan jalur URL, pilih jalur URL yang diinginkan, dan lihat server asli yang terikat pada jalur itu di sebelah kanan pendengar.

HTTP/HTTPS Listener

Create

+ test-http-80(HTTP:80)

- test-https-443(HTTPS:443)

www.example.com

/index

Forwarding Rules Expand

Bound Real Server

Bind Modify Port Modify Weight Unbind

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--|-------------|-------------|------------|------|
| Listener created. Please Bound real server | | | | |

2. Klik **Bind** (Ikat), pilih server asli target, konfigurasi port server dan beban di jendela pop-up.

① Tambahkan port: Di kotak "Terpilih" di sebelah kanan, klik **Add Port** (Tambahkan Port) untuk menambahkan

beberapa port untuk instance CVM yang sama, seperti port 80, 81, dan 82.

② Port default: Masukkan **Default Port** (Port Default) dahulu, kemudian pilih instance CVM. Port dari setiap instance CVM adalah port default.

Bound real server

IP

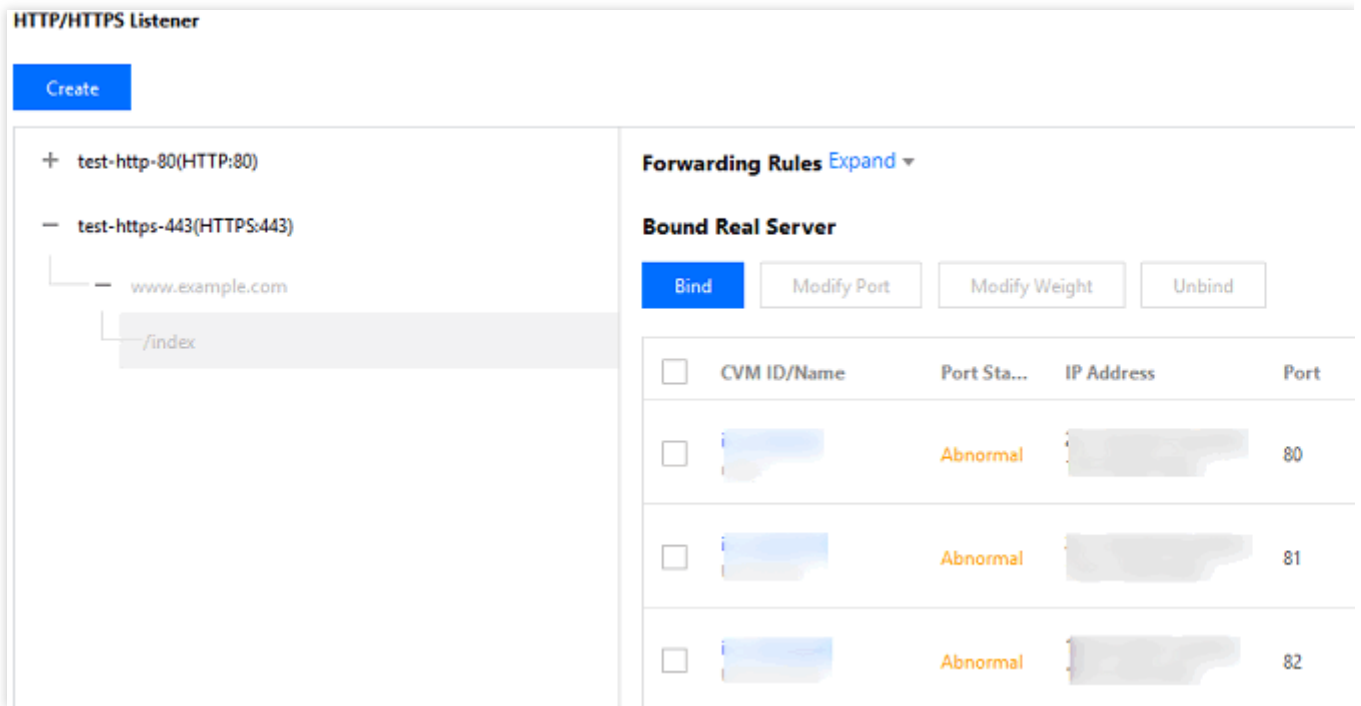
| <input checked="" type="checkbox"/> | ID/Name |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |
| <input checked="" type="checkbox"/> | [Redacted] |

Selected (3)

| ID/Name | Port | Weight |
|------------|---------------------------------|---------------------------------|
| [Redacted] | <input type="text" value="80"/> | <input type="text" value="10"/> |
| [Redacted] | <input type="text" value="81"/> | <input type="text" value="10"/> |
| [Redacted] | <input type="text" value="82"/> | <input type="text" value="10"/> |

Note: When the private CLB is bound with one CVM, please DO NOT use this CVM as the client to access CLB.

Setelah tiga langkah ini selesai, aturan pendengar HTTPS sudah dikonfigurasi seperti yang ditunjukkan di bawah ini:

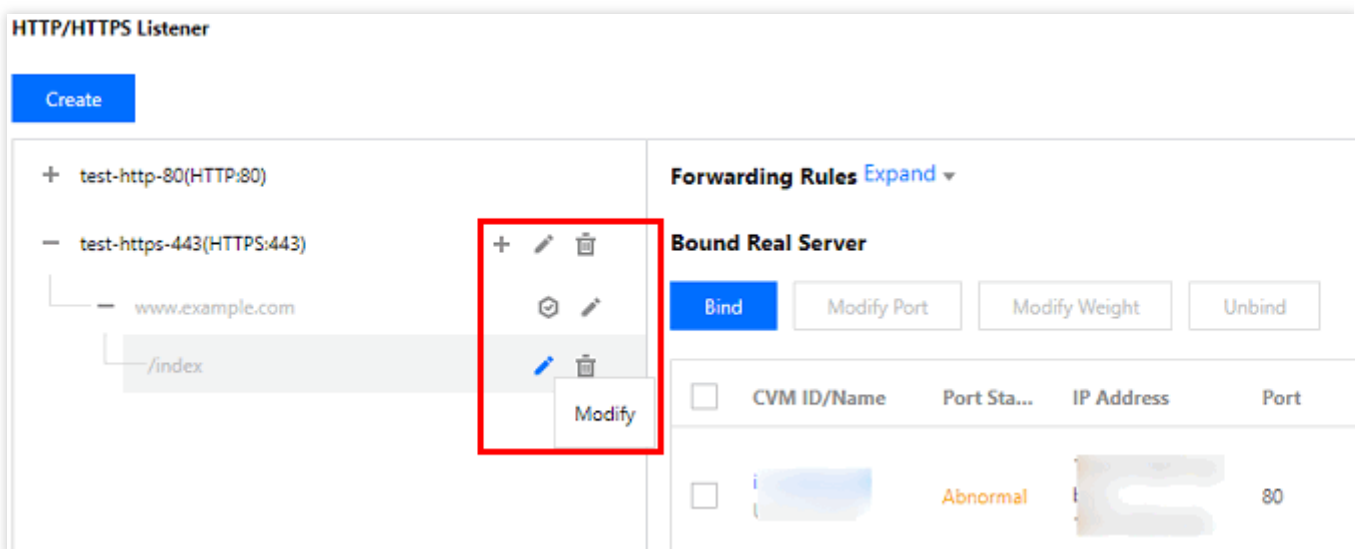


Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Konfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi dan hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang dibuat, klik pendengar/nama domain/jalur URL pada tab **Listener Management** (Manajemen Pendengar) dan pilih **Modify** (Modifikasi) atau **Delete** (Hapus).



Metode Penyeimbangan Beban

Waktu update terbaru : 2024-01-04 20:53:33

Metode penyeimbangan beban adalah algoritme yang mengalokasikan lalu lintas ke [server asli](#). Setiap metode menghasilkan efek penyeimbangan beban yang berbeda.

Penjadwalan Round-Robin Tertimbang

Algoritme penjadwalan round-robin tertimbang adalah untuk menjadwalkan permintaan ke server berbeda berdasarkan polling. Algoritme ini bisa menyelesaikan masalah performa tidak seimbang di server berbeda. Algoritme ini memakai bobot untuk mewakili performa pemrosesan server dan menjadwalkan permintaan ke server berbeda berdasarkan bobot dengan cara polling. Algoritme ini menjadwalkan server berdasarkan jumlah koneksi baru, tempat server dengan bobot lebih tinggi menerima koneksi lebih awal dan berpeluang lebih tinggi untuk dipilih. Server dengan bobot yang sama akan memproses jumlah koneksi yang sama.

Advantage (Keunggulan): algoritme ini memberikan kemudahan dan kepraktisan tinggi. Algoritme ini tidak perlu mencatat status semua koneksi dan oleh karena itu merupakan algoritme penjadwalan stateless.

Disadvantage (Kekurangan): algoritme ini cukup sederhana sehingga tidak cocok untuk situasi saat waktu layanan permintaan berubah secara signifikan, atau setiap permintaan membutuhkan jumlah waktu yang berbeda. Dalam kasus-kasus ini, algoritme itu akan menyebabkan distribusi beban yang tidak seimbang di antara server.

Applicable scenario (Skenario yang berlaku): Algoritme ini cocok untuk skenario saat setiap permintaan pada dasarnya membutuhkan jumlah waktu yang sama di backend dengan performa pemuatan terbaik. Algoritme ini biasanya digunakan di layanan koneksi non-persisten seperti layanan HTTP.

Recommendation (Rekomendasi): jika Anda tahu bahwa setiap permintaan pada dasarnya membutuhkan jumlah waktu yang sama di backend (contohnya, permintaan yang diproses server asli berjenis sama atau mirip), Anda sebaiknya menggunakan penjadwalan round-robin. Jika perbedaan waktu antara setiap permintaan kecil, sebaiknya menggunakan algoritme ini juga, karena tingkat konsumsi rendah dan efisiensi tinggi, tanpa membutuhkan traversal.

Penjadwalan Koneksi Terkecil Tertimbang

Pada situasi sebenarnya, waktu yang dihabiskan permintaan-permintaan klien di server bisa sangat bervariasi. Makin panjang waktu pengerjaannya, jika round-robin sederhana atau algoritme penyeimbangan beban acak digunakan, jumlah proses koneksi di setiap server bisa sangat bervariasi sehingga tidak bisa mencapai efek penyeimbangan beban.

Berbeda dengan penjadwalan round-robin, penjadwalan koneksi terkecil adalah algoritme penjadwalan dinamis yang memperkirakan beban server berdasarkan kuantitas koneksi aktifnya. Penjadwal harus merekam jumlah koneksi di

setiap server yang saat ini tersambung. Jika ada permintaan yang dijadwalkan ke satu server, jumlah koneksinya akan bertambah 1. Jika koneksi terhenti atau habis waktu, jumlah koneksinya akan berkurang 1.

Pada algoritme penjadwalan koneksi terkecil tertimbang yang didasarkan pada penjadwalan koneksi terkecil, bobot berbeda dialokasikan ke server-server sesuai kemampuan pemrosesannya. Dengan cara ini, satu server bisa mencapai jumlah permintaan terkait yang sesuai dengan bobotnya, yang merupakan peningkatan di penjadwalan koneksi terkecil.

Keterangan :

Misalkan bobot satu server asli adalah w_i , dan jumlah koneksi saat ini adalah c_i . Nilai c_i/w_i setiap server dihitung secara berurutan. Server asli dengan nilai c_i/w_i terkecil akan menjadi server yang menerima permintaan baru berikutnya. Jika ada server asli dengan nilai c_i/w_i yang sama, mereka akan dijadwalkan sesuai penjadwalan round-robin tertimbang.

Advantage (Keunggulan): algoritme ini cocok untuk permintaan yang pemrosesannya butuh waktu lama, seperti FTP.

Disadvantage (Kekurangan): karena batasan API, koneksi terkecil dan persistensi sesi tidak bisa diaktifkan di waktu yang sama.

Applicable scenario (Skenario yang berlaku): algoritme ini cocok untuk skenario saat waktu yang dihabiskan setiap permintaan di backend sangat bervariasi. Algoritme ini biasanya digunakan pada layanan koneksi persisten.

Recommendation (Rekomendasi): jika Anda harus memproses permintaan-permintaan berbeda dan waktu layanan yang dibutuhkan di backend sangat bervariasi (seperti 3 milidetik dan 3 detik), Anda sebaiknya menggunakan penjadwalan koneksi terkecil tertimbang untuk mencapai penyeimbangan beban.

Penjadwalan Hashing Sumber

Algoritme penjadwalan hashing sumber (`ip_hash`) menggunakan alamat IP sumber dari permintaan sebagai kunci hash dan mencari server yang sesuai dari tabel hash yang ditetapkan secara statis. Permintaan akan dikirimkan ke server ini jika tersedia dan tidak kelebihan beban; jika tidak, nol akan dikembalikan.

Advantage (Keunggulan): `ip_hash` bisa memetakan permintaan dari satu klien ke server asli yang sama melalui tabel hash. Oleh karena itu, dalam skenario saat persistensi sesi tidak didukung, algoritme ini bisa digunakan untuk mencapai efek persistensi sesi sederhana.

Recommendation (Rekomendasi): Algoritme menghitung nilai hash dari alamat sumber satu permintaan dan mendistribusikan permintaan itu ke server asli berdasarkan bobotnya. Dengan cara ini, semua permintaan dari IP klien yang sama bisa didistribusikan ke server yang sama. Algoritme ini cocok untuk protokol yang tidak mendukung cookie.

Memilih Algoritme Penyeimbangan Beban dan Mengonfigurasi Bobot

Agar kluster server asli bisa menjalankan bisnis dengan stabil dalam berbagai skenario, beberapa kasus mengenai cara memilih algoritme penyeimbangan beban dan mengonfigurasi bobot tersedia di bawah ini untuk referensi Anda.

Skenario 1:

1. Misalkan ada 3 server asli dengan konfigurasi yang sama (CPU dan memori) dan Anda mengatur semua bobotnya ke 10 karena performanya sama.
2. 100 koneksi TCP telah dibuat antara setiap server asli dan klien, dan satu server asli baru ditambahkan.
3. Dalam skenario ini, Anda sebaiknya menggunakan algoritme penjadwalan koneksi terkecil, yang bisa dengan cepat menambah beban server asli ke-4 dan mengurangi tekanan pada 3 server lainnya.

Skenario 2:

1. Misalkan Anda menggunakan layanan Tencent Cloud untuk pertama kalinya dan situs web Anda baru saja dibuat dengan beban rendah. Anda sebaiknya membeli server asli dengan konfigurasi yang sama, karena semuanya merupakan server layer akses setara.
2. Di skenario ini, Anda bisa mengatur bobot semua server asli ke nilai default 10 dan menggunakan algoritme penjadwalan round-robin tertimbang untuk mendistribusikan lalu lintas.

Skenario 3:

1. Misalkan kamu memiliki 5 server asli yang menjalankan permintaan akses ke halaman statis sederhana, dan rasio daya komputasi (dihitung berdasarkan CPU dan memori) server-server ini adalah 9:3:3:3:1.
2. Pada skenario ini, Anda bisa mengatur bobot server asli itu masing-masing ke 90, 30, 30, 30, dan 10. Karena kebanyakan permintaan akses ke halaman statis adalah jenis koneksi non-persisten, Anda bisa menggunakan algoritme penjadwalan round-robin, agar instance CLB bisa mengalokasikan permintaan sesuai rasio performa servernya.

Skenario 4:

1. Misalkan Anda memiliki 10 server asli untuk menjalankan sejumlah besar permintaan akses web dan tidak ingin membeli server lagi, karena bisa menambah pengeluaran, dan salah satu server itu sering mulai ulang karena kelebihan beban.
2. Dalam skenario ini, Anda sebaiknya mengatur bobot server itu sesuai performanya dan mengatur bobot yang cukup kecil untuk server dengan beban tinggi. Selain itu, Anda bisa menggunakan algoritme penjadwalan koneksi terkecil untuk mengalokasikan permintaan ke server asli dengan koneksi aktif yang lebih sedikit agar server tidak kelebihan beban.

Skenario 5:

1. Misalkan Anda memiliki 3 server asli untuk memproses beberapa koneksi persisten, rasio daya komputasi (dihitung dari CPU dan memori) server-server ini adalah 3:1:1.
2. Server dengan performa terbaik memproses lebih banyak permintaan, tetapi Anda tidak ingin sampai kelebihan beban dan ingin mengalokasikan permintaan baru ke server diam,.
3. Dalam skenario ini, Anda bisa menggunakan algoritme penjadwalan koneksi terkecil dan dengan tepat mengurangi bobot server yang sibuk, agar instance CLB bisa mengalokasikan permintaan ke server asli dengan koneksi aktif yang lebih sedikit sehingga mencapai penyeimbangan beban.

Skenario 6:

1. Misalkan Anda ingin permintaan dari klien berikutnya dialokasikan ke server yang sama. Karena penjadwalan round-robin tertimbang atau koneksi terkecil tertimbang tidak bisa memastikan bahwa permintaan dari klien yang sama dialokasikan ke server yang sama,

2. Untuk memenuhi persyaratan server aplikasi tertentu Anda dan mempertahankan "kelengketan" (atau "kelanjutan") sesi klien tersebut, Anda bisa menggunakan ip_hash untuk mendistribusikan lalu lintasnya. Algoritme ini bisa memastikan semua permintaan dari klien yang sama akan didistribusikan ke server asli yang sama, kecuali jika jumlah server berubah atau server menjadi tidak tersedia.

Persistensi Sesi

Waktu update terbaru : 2024-01-04 20:53:33

Persistensi sesi bisa meneruskan permintaan dari IP yang sama ke server asli yang sama. Secara default, instance CLB akan mengarahkan permintaan ke server asli berbeda untuk penyeimbangan beban; tetapi Anda bisa menggunakan persistensi sesi untuk mengarahkan permintaan dari pengguna tertentu ke server asli yang sama sehingga beberapa aplikasi yang harus menyimpan sesinya (seperti keranjang belanja) bisa berjalan lancar.

Persistensi Sesi Lapisan 4

Protokol lapisan 4 (TCP/UDP) mendukung persistensi sesi berbasis IP sumber. Durasi persistensi sesi bisa diatur ke integer berapa pun antara 30 dan 3600 detik. Jika ambang batas waktu terlampaui dan tidak ada permintaan baru di sesi, persistensi sesi akan berakhir. Persistensi sesi bergantung pada mode penyeimbangan beban:

Dalam mode "round-robin tertimbang" tempat permintaan didistribusikan sesuai bobot server asli, persistensi sesi berdasarkan IP source didukung.

Dalam mode "koneksi terkecil tertimbang" tempat penjadwalan keseluruhan bergantung pada beban dan bobot server, persistensi sesi tidak didukung.

Persistensi Sesi Lapisan 7

Protokol lapisan 7 (HTTP/HTTPS) mendukung persistensi sesi berdasarkan penyisipan cookies (CLB menyisipkan cookie ke klien). Durasi persistensi sesi bisa diatur ke nilai berapa pun antara 30 dan 3600 detik. Persistensi sesi bergantung pada mode penyeimbangan beban:

Dalam mode "round-robin tertimbang" tempat permintaan didistribusikan sesuai bobot server asli, persistensi sesi berdasarkan penyisipan cookies didukung.

Dalam mode "koneksi terkecil tertimbang" tempat penjadwalan keseluruhan bergantung pada beban dan bobot server, persistensi sesi tidak didukung.

Mode "IP Hash" mendukung persistensi sesi berdasarkan pada IP sumber, tetapi tidak pada penyisipan cookie.

Periode Waktu Habis Koneksi

Saat ini, periode waktu habis koneksi HTTP (`keepalive_timeout`) adalah 75s secara default. Jika Anda ingin mengubahnya, silakan aktifkan [konfigurasi khusus](#). Jika ambang batas terlampaui dan tidak ada transmisi data di sesi, koneksi akan diputus.

Saat ini, periode waktu habis koneksi TCP adalah 900s secara default dan tidak bisa diubah. Jika ambang batas terlampaui dan tidak ada transmisi data di sesi, koneksi akan diputus.

Mengonfigurasi Persistensi Sesi

1. Masuk ke [Konsol CLB](#) dan klik ID instance CLB yang akan dikonfigurasi dengan persistensi sesi untuk masuk ke halaman detailnya.
2. Pilih tab **Listener Management** (Manajemen Pendengar).
3. Klik **Modify** (Modifikasi) setelah pendengar CLB untuk dikonfigurasi dengan persistensi sesi.
4. Pilih apakah akan mengaktifkan fitur persistensi sesi. Klik tombol untuk mengaktifkannya, masukkan durasi persistensinya, dan klik **OK**.

Hubungan Antara Koneksi Persisten dan Persistensi Sesi

Skenario 1. Bisnis lapisan 7 HTTP

Dengan asumsi klien mengakses protokol HTTP/1.1 dan `Connection:keep-alive` dikonfigurasi di informasi header. Klien mengakses CVM melalui instance CLB tanpa mengaktifkan persistensi sesi. Apakah klien bisa mengakses CVM yang sama kali berikutnya?

J: tidak.

Pertama, keep-alive HTTP menandakan koneksi TCP tetap tersambung setelah permintaan dikirimkan sehingga peramban bisa mengirimkan permintaan melalui koneksi yang sama. Koneksi persisten mengurangi waktu yang dibutuhkan untuk membuat koneksi baru untuk setiap permintaan dan mengurangi konsumsi bandwidth. Periode waktu habis default kluster CLB adalah 75s (jika tidak ada permintaan baru dalam 75s, sambungan TCP akan diputuskan secara default).

Keep-alive HTTP dibuat antara klien dan instance CLB. Jika persistensi sesi cookie dinonaktifkan, instance CLB akan memilih acak instance CVM sesuai kebijakan polling. Koneksi persisten sebelumnya sudah tidak berlaku.

Oleh karena itu, kami menyarankan Anda untuk mengaktifkan persistensi sesi.

Jika periode persistensi sesi cookie dikonfigurasi pada 1000s, klien akan memulai permintaan lagi. Karena periode antara dua permintaan melebihi 75s, koneksi TCP harus dibuat lagi. Layer aplikasi mengidentifikasi cookie dan menemukan instance yang diakses klien terakhir kali, jadi akan diakses lagi kali ini.

Skenario 2. Bisnis lapisan 4 TCP

Dengan asumsi klien memulai akses, TCP adalah protokol layar transportasi, koneksi persisten diaktifkan, tetapi persistensi sesi berdasarkan IP sumber dinonaktifkan. Apakah klien yang sama bisa mengakses server yang sama dengan permintaan akses berikutnya?

J: belum tentu.

Pertama, menurut mekanisme implementasi lapisan 4, saat koneksi persisten diaktifkan untuk TCP dan tidak ditutup, dan koneksi yang sama diakses dalam dua permintaan, maka klien yang sama bisa mengakses server yang sama. Jika koneksi ditutup karena suatu alasan (seperti mulai ulang jaringan atau waktu koneksi habis) dalam permintaan akses kedua, permintaan itu bisa dijadwalkan ke server asli lainnya. Periode waktu habis global default untuk koneksi persisten adalah 900s, artinya, koneksi persisten akan dilepaskan jika tidak ada permintaan baru dalam 900s.

Mengonfigurasi Pengalihan Lapisan 7

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung pengalihan lapisan 7, agar Anda bisa mengonfigurasi pengalihan pada pendengar HTTP/HTTPS lapisan 7.

Keterangan :

Persistensi sesi: jika klien mengakses `example.com/bbs/test/123.html` dan persistensi sesi sudah diaktifkan di CVM backend, setelah pengalihan diaktifkan untuk meneruskan lalu lintas ke

`example.com/bbs/test/456.html` , mekanisme persistensi sesi awalnya tidak akan berlaku.

Pengalihan TCP/UDP: saat ini tidak mendukung pengalihan pada level IP + port, tetapi akan tersedia di versi berikutnya. Pengalihan TCP/UDP: saat ini tidak mendukung pengalihan pada level IP + port, tetapi akan tersedia di versi berikutnya.

Ikhtisar Pengalihan

Pengalihan otomatis

Ikhtisar

Untuk pendengar `HTTPS : 443` yang ada, pendengar HTTP (port 80) akan dibuat secara otomatis oleh sistem untuk penerusan. Permintaan yang dikirimkan ke `HTTP : 80` akan dialihkan secara otomatis ke `HTTPS : 443` .

Kasus penggunaan

Pengalihan paksa HTTPS, misalnya, mengalihkan permintaan HTTP ke HTTPS. Saat pengguna mengakses layanan web di PC atau peramban seluler melalui HTTP, CLB akan mengalihkan semua permintaan yang dikirimkan ke `HTTP : 80` ke `HTTPS : 443` untuk penerusan.

Keunggulan skema

Konfigurasi atur-dan-lupakan: pengalihan paksa HTTPS bisa diimplementasikan untuk nama domain, yang hanya membutuhkan satu operasi konfigurasi.

Pembaruan layanan: jika jumlah URL layanan HTTPS berubah, Anda hanya perlu menggunakan fitur ini lagi di konsol untuk menyegarkan.

Pengalihan manual

Ikhtisar

Anda bisa mengonfigurasi pengalihan 1-ke1. Contohnya, di instance CLB, Anda bisa mengonfigurasi pengalihan `listener 1 / domain name 1 / URL 1` ke `listener 2 / domain name 2 / URL 2` .

Kasus penggunaan

Pengalihan jalur tunggal. Contohnya, jika Anda ingin menonaktifkan bisnis web sementara waktu pada kasus seperti produk habis, pemeliharaan halaman, atau pembaruan dan peningkatan, halaman asal perlu dialihkan ke halaman baru. Jika tidak ada pengalihan yang dilakukan, alamat lama di favorit pengguna dan database mesin pencari akan

menampilkan halaman pesan kesalahan `404/503` , menurunkan pengalaman pengguna dan mengakibatkan hilangnya lalu lintas.

Pengalihan Otomatis

CLB mendukung pengalihan paksa satu klik dari HTTP ke HTTPS.

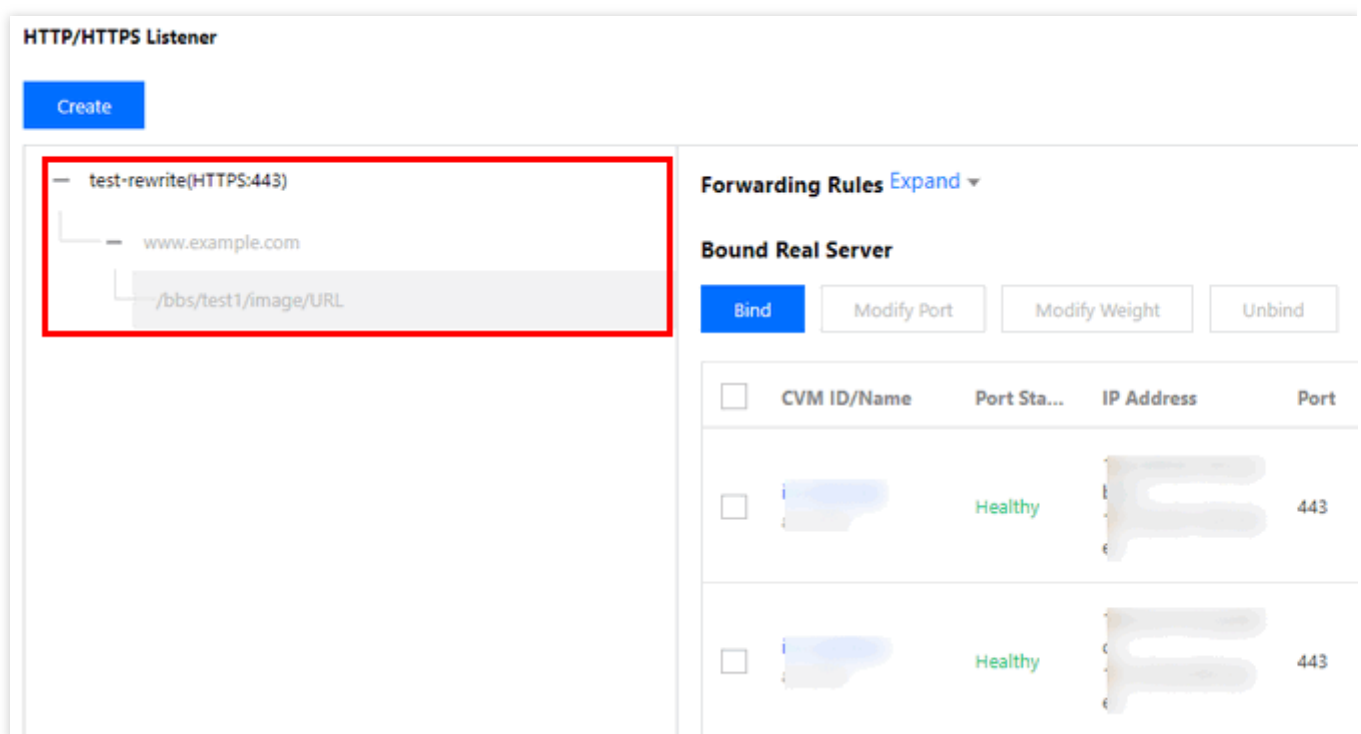
Dengan asumsi Anda perlu mengonfigurasi situs web `https://www.example.com` , agar pengguna akhir bisa mengunjunginya dengan aman melalui HTTPS terlepas dari apakah mereka mengirim permintaan HTTP (`http://www.example.com`) atau permintaan HTTPS (`https://www.example.com`) di peramban.

Prasyarat

Pendengar `HTTPS:443` telah dikonfigurasi.

Petunjuk

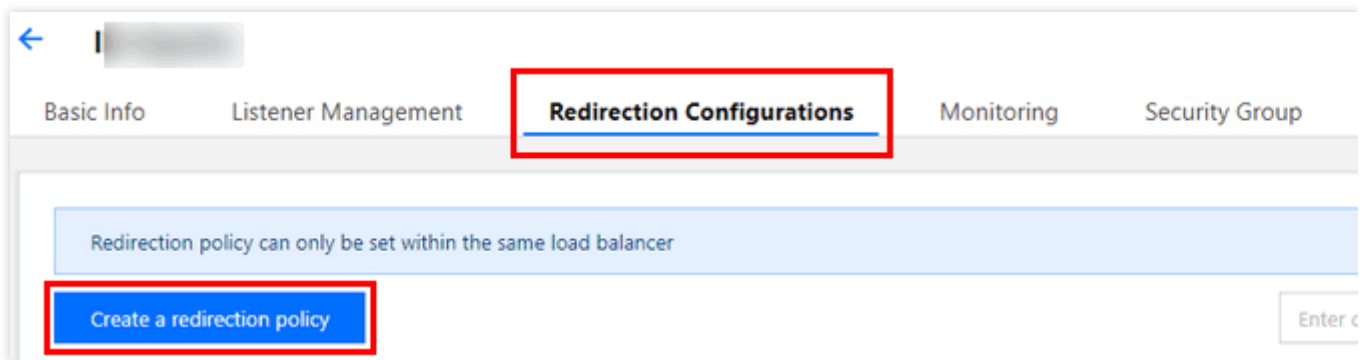
- 1.Konfigurasi pendengar HTTPS CLB di [Konsol CLB](#) dan atur lingkungan web dari `https://example.com` .Untuk informasi selengkapnya, silakan lihat [Mengonfigurasi Pendengar HTTPS](#).
- 2.Hasil konfigurasi pendengar HTTPS adalah seperti yang ditunjukkan di bawah ini:



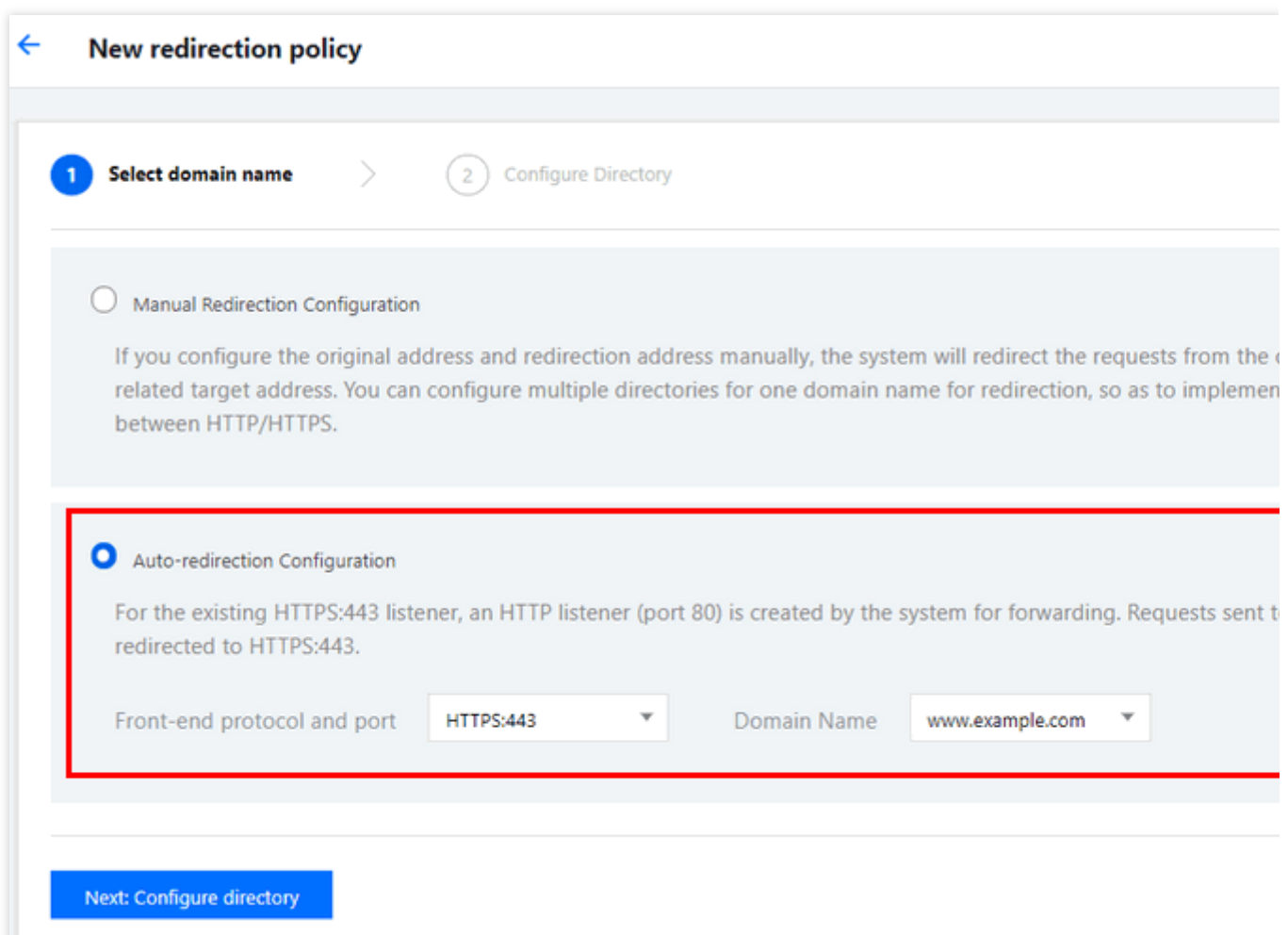
The screenshot displays the configuration for an HTTP/HTTPS Listener. The listener is named "test-rewrite(HTTPS:443)". The configuration shows a forwarding rule for "www.example.com" with a path "/bbs/test1/image/URL". The listener is bound to two real servers, both of which are healthy and listening on port 443.

| | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 443 |
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 443 |

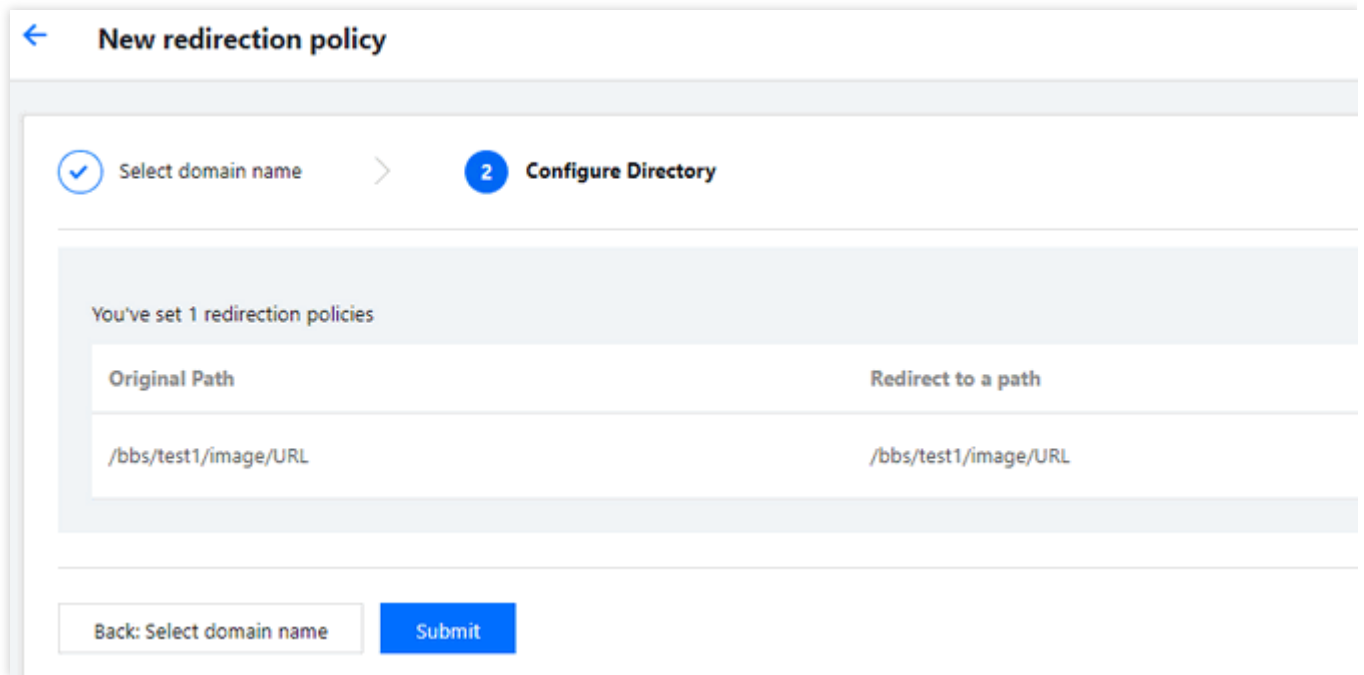
- 3.Pada tab "Redirection Configuration" (Konfigurasi Pengalihan) di detail instance CLB, klik **Create Redirection Configuration** (Buat Konfigurasi Pengalihan).



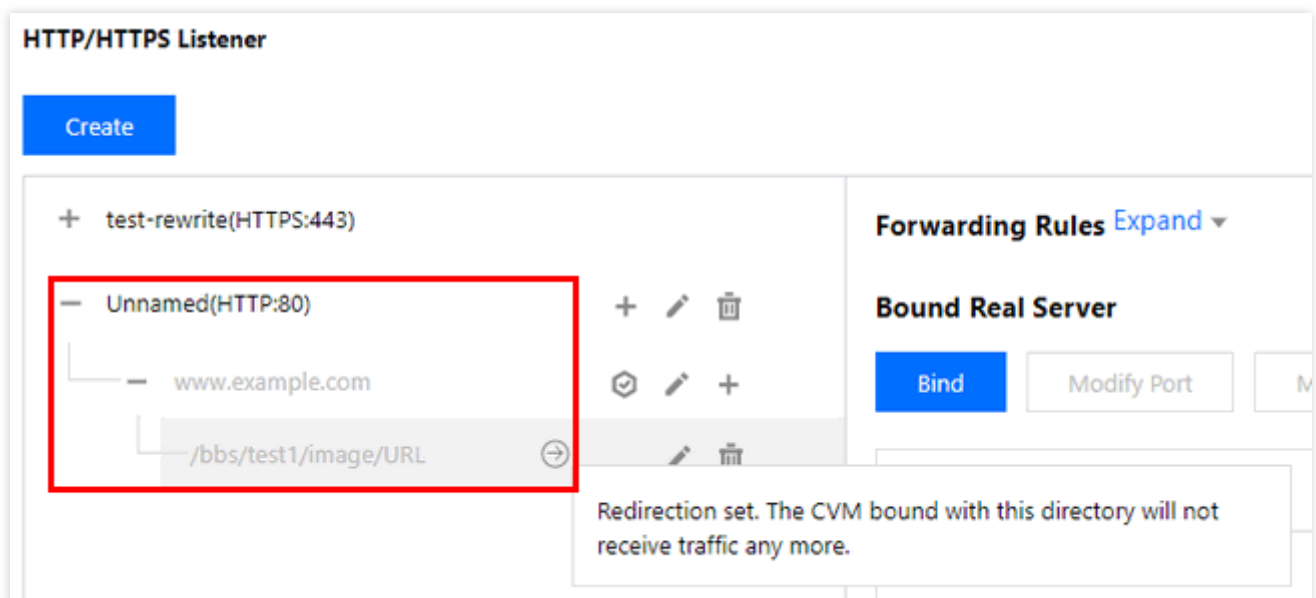
4. Pilih **Automatic Redirection Configuration** (Konfigurasi Pengalihan Otomatis), pilih pendengar dan nama domain HTTPS yang sudah dikonfigurasi, dan klik **Next:Configure Path** (Berikutnya: Konfigurasi Jalur).



5. Klik **Submit** (Kirim) untuk menyelesaikan konfigurasi.



6. Hasil setelah pengalihan dikonfigurasi adalah seperti yang ditunjukkan di bawah ini. Seperti yang bisa Anda lihat, pendengar `HTTP : 80` telah dikonfigurasi untuk pendengar `HTTPS : 443` secara otomatis, dan semua lalu lintas HTTP akan dialihkan ke HTTPS secara otomatis.



Pengalihan Manual

CLB mendukung konfigurasi pengalihan 1-ke-1.

Contohnya, bisnis Anda menggunakan halaman `forsale` untuk kampanye promosi dan harus mengalihkan

halaman kampanye `https://www.example.com/forsale` ke beranda baru `https://www.new.com/index` setelah kampanye berakhir.

Prasyarat

Pendengar HTTPS telah dikonfigurasi.

Nama domain yang diteruskan `https://www.example.com/forsale` telah dikonfigurasi.

Nama domain dan jalur yang diteruskan `https://www.new.com/index` telah dikonfigurasi.

Petunjuk

1. Konfigurasi pendengar HTTPS CLB di [Konsol CLB](#) dan atur lingkungan web dari

`https://example.com`. Untuk informasi selengkapnya, silakan lihat [Mengonfigurasi Pendengar HTTPS](#).

2. Hasil konfigurasi HTTPS adalah seperti yang ditunjukkan di bawah ini:

The screenshot shows the configuration for an HTTP/HTTPS Listener named 'test-sni(HTTPS:443)'. A red box highlights the domain and path configuration:

- Domain: `www.example.com`
- Path: `/forsale`
- Domain: `www.new.com`
- Path: `/index`

The 'Forwarding Rules' section is expanded, and the 'Bound Real Server' section shows a table of servers with 'Healthy' status.

| <input type="checkbox"/> | CVM ID/Name | Port Sta... | IP Address | Port |
|--------------------------|-------------|-------------|------------|------|
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 443 |
| <input type="checkbox"/> | [blurred] | Healthy | [blurred] | 443 |

3. Pada tab "Redirection Configuration" (Konfigurasi Pengalihan) di detail instance CLB, klik **Create Redirection Configuration** (Buat Konfigurasi Pengalihan).

The screenshot shows the 'Redirection Configurations' tab in the console. The 'Create a redirection policy' button is highlighted with a red box.

Redirection policy can only be set within the same load balancer

[Create a redirection policy](#)

4. Pilih **Manual Redirection Configuration** (Konfigurasi Pengalihan Manual), pilih port protokol frontend yang pertama diakses, `HTTPS:443` dan nama domain `https://www.example.com/forsale` , pilih port protokol frontend `HTTPS:443` dan nama domain `https://www.new.com/index` setelah pengalihan, dan klik **Next:Configure Path** (Berikutnya: Konfigurasi Jalur).

New redirection policy

1 Select domain name > 2 Configure Directory

Manual Redirection Configuration

If you configure the original address and redirection address manually, the system will redirect the requests from the original address to the can configure multiple directories for one domain name for redirection, so as to implement auto-redirection between HTTP/HTTPS.

Original Access

Front-end protocol and port `HTTPS:443` Domain Name `www.example.com`

Redirect to

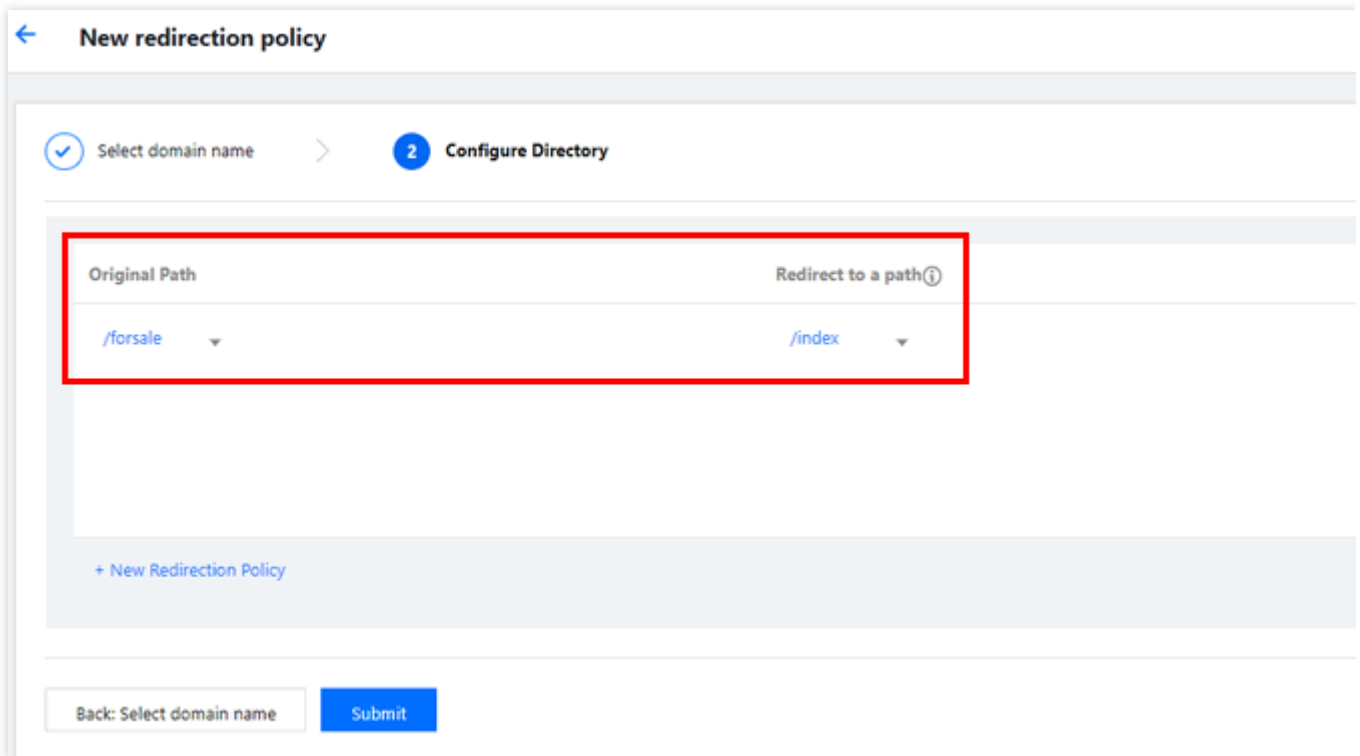
Front-end protocol and port `HTTPS:443` Domain Name `www.new.com`

Auto-redirection Configuration

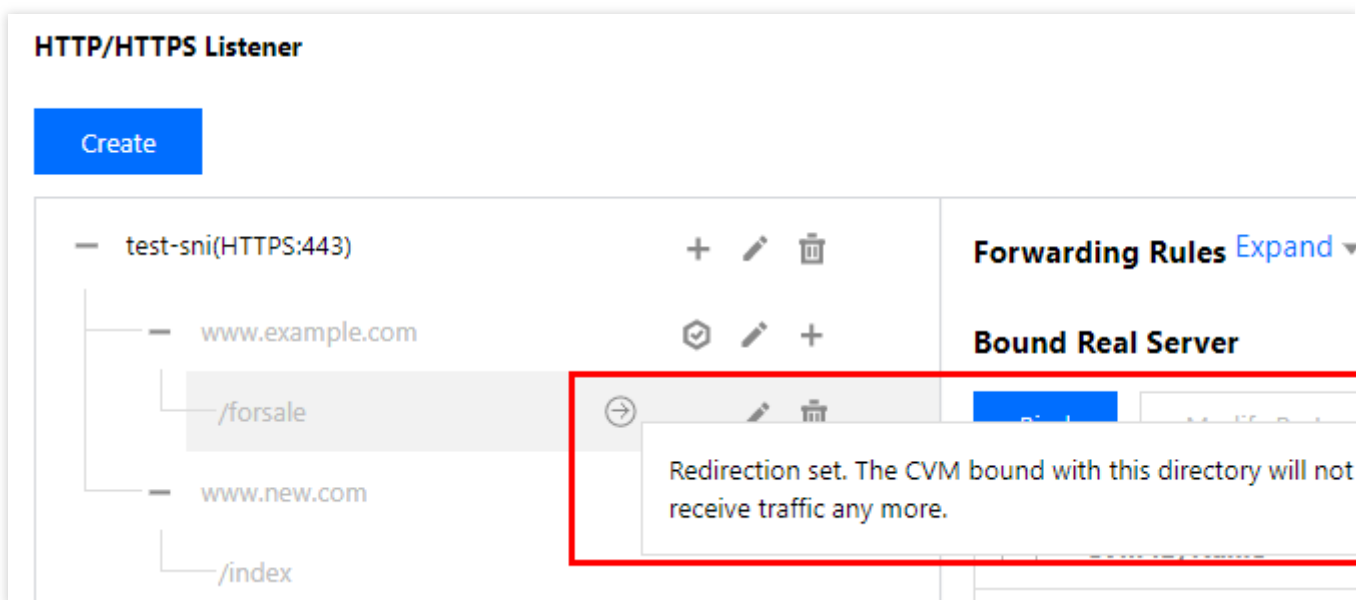
For the existing HTTPS:443 listener, an HTTP listener (port 80) is created by the system for forwarding. Requests sent to HTTP:80 will be redir

Next: Configure directory

5. Pilih `/forsale` untuk jalur akses pertama dan `/index` untuk jalur akses setelah pengalihan, dan klik **Submit** (Kirim) untuk menyelesaikan konfigurasi.



6. Hasil setelah konfigurasi pengalihan adalah seperti yang ditunjukkan di bawah ini. Seperti yang bisa Anda lihat, di pendengar `HTTPS:443`, `https://www.example.com/forsale` telah dialihkan ke `https://www.new.com/index`.



Konfigurasi Khusus Lapisan 7

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung konfigurasi khusus, membuat Anda bisa mengatur parameter konfigurasi untuk instance CLB tunggal, seperti `client_max_body_size` dan `ssl_protocols`, agar sesuai kebutuhan unik Anda.

Keterangan :

Setiap wilayah bisa memiliki hingga 200 entri konfigurasi khusus.

Konfigurasi khusus dibatasi pada 64K byte.

Saat ini, setiap instance hanya bisa diikat pada satu entri konfigurasi khusus.

Konfigurasi khusus hanya valid untuk pendengar CLB HTTP/HTTPS CLB (sebelumnya CLB Aplikasi) lapisan 7.

Parameter Konfigurasi Khusus CLB

Saat ini, konfigurasi khusus CLB mendukung bidang-bidang berikut ini:

| Bidang Konfigurasi | Nilai Default/Nilai yang Direkomendasikan | Rentang Parameter | Deskripsi |
|--|---|----------------------------------|---|
| <code>ssl_protocols</code> | TLSv1 TLSv1.1 TLSv1.2 | TLSv1 TLSv1.1 TLSv1.2 TLSv1.3 | Versi protokol TLS yang digunakan |
| <code>ssl_ciphers</code> | Lihat lebih lanjut di bawah ini. | Lihat lebih lanjut di bawah ini. | Rangkaian enkripsi |
| <code>client_header_timeout</code> | 60s | [30-120]s | Periode waktu habis untuk memperoleh |
| <code>client_header_buffer_size</code> | 4k | [1-256]k | Ukuran buffer default tempat header pe |
| <code>client_body_timeout</code> | 60s | [30-120]s | Periode waktu habis untuk memperoleh tetapi merujuk pada periode diam tanpa |
| <code>client_max_body_size</code> | 60M | [1-10240]M | Rentang konfigurasi default:1 MB – 256 Ukuran maksimum:2,048 MB; jika <code>cli</code> |
| <code>keepalive_timeout</code> | 75s | [0-900]s | Waktu tunggu koneksi persisten <code>Clie</code> hingga lebih dari 900, silakan kirim aplik level1_id=6&level2_id=163&source=08 maksimum yang bisa Anda atur adalah |
| <code>add_header</code> | Khusus | - | Bidang header khusus yang dikembalik |
| <code>more_set_headers</code> | Khusus | - | Bidang header khusus yang dikembalik |

| | | | |
|-----------------------------|------------------------------|---|--|
| proxy_connect_timeout | 4s | [4-120]s | Periode waktu habis koneksi backend u |
| proxy_read_timeout | 60s | [30-3600]s | Periode waktu habis pembacaan respon |
| proxy_send_timeout | 60s | [30-3600]s | Periode waktu habis pengiriman permin |
| server_tokens | on | on, off | <code>on</code> : menampilkan informasi versi; <code>off</code> : menyembunyikan informasi ver |
| keepalive_requests | 100 | [1-10000] | Jumlah permintaan maksimum yang bis |
| proxy_buffer_size | 4k | [1-64]k | Ukuran header respons server, yang me menggunakan <code>proxy_buffer_size</code> |
| proxy_buffers | 8 4k | [3-8] [4-8]k | Kuantitas dan ukuran buffer. |
| proxy_reques t_buffering | on | on, off | <code>on</code> : menyimpan bodi permintaan klie dalam beberapa bagian setelah perminti <code>off</code> : tidak menyimpan bodi perminta instance CVM backend, yang menamba |
| proxy_set_header | X-Real-Port \$remote_port | X-Real-Port \$remote_port X-clb-stgw-vip \$server_addr Stgw-request-id \$stgw_request_id X-Forwarded- Port \$vport X-Method \$request_method X-Uri \$uri X-Forwarded- Proto | <code>X-Real-Port \$remote_port :pc</code> <code>X-clb-stgw-vip \$server_addr</code> <code>Stgw-request-id \$stgw_reques</code> <code>X-Forwarded-Port :Port pendeng</code> <code>X-Method</code> : metode permintaan klien <code>X-Uri</code> : URI permintaan klien. <code>X-Forwarded-Proto</code> : protokol unt |
| send_timeout | 60s | [1-3600]s | Periode waktu habis transfer data dari s berurutan, bukan seluruh periode transf |
| ssl_verify_depth | 1 | [1, 10] | Kedalaman verifikasi rantai sertifikat klie |
| proxy_redirect | http:// https:// | http:// https:// | Jika server upstream mengembalikan p <code>proxy_redirect</code> akan mereset htt aman. |
| ssl_early_data | off | on, off | Mengaktifkan atau menonaktifkan TLS <code>ssl_early_data</code> bisa berlaku.You |

| | | | |
|----------------------|----|--|---|
| | | | (Anda harus mempertimbangkan risiko |
| http2_max_field_size | 4k | [1-256]k | Membatasi ukuran maksimum header p |
| error_page | - | error_page code [= [respons]] uri | URL yang telah ditentukan akan ditamp harus diawali dengan / . |

Keterangan :

Persyaratan pada nilai `proxy_buffer_size` dan `proxy_buffers` : $2 * \text{maks}(\text{proxy_buffer_size}, \text{proxy_buffers.size}) \leq (\text{proxy_buffers.num} - 1) * \text{proxy_buffers.size}$; Contohnya, jika `proxy_buffer_size` adalah "24k", `proxy_buffers` adalah "8 8k"; $2 * 24k = 48k$, $(8 - 1) * 8k = 56k$; dan $48k \leq 56k$, jadi tidak akan ada kesalahan konfigurasi.

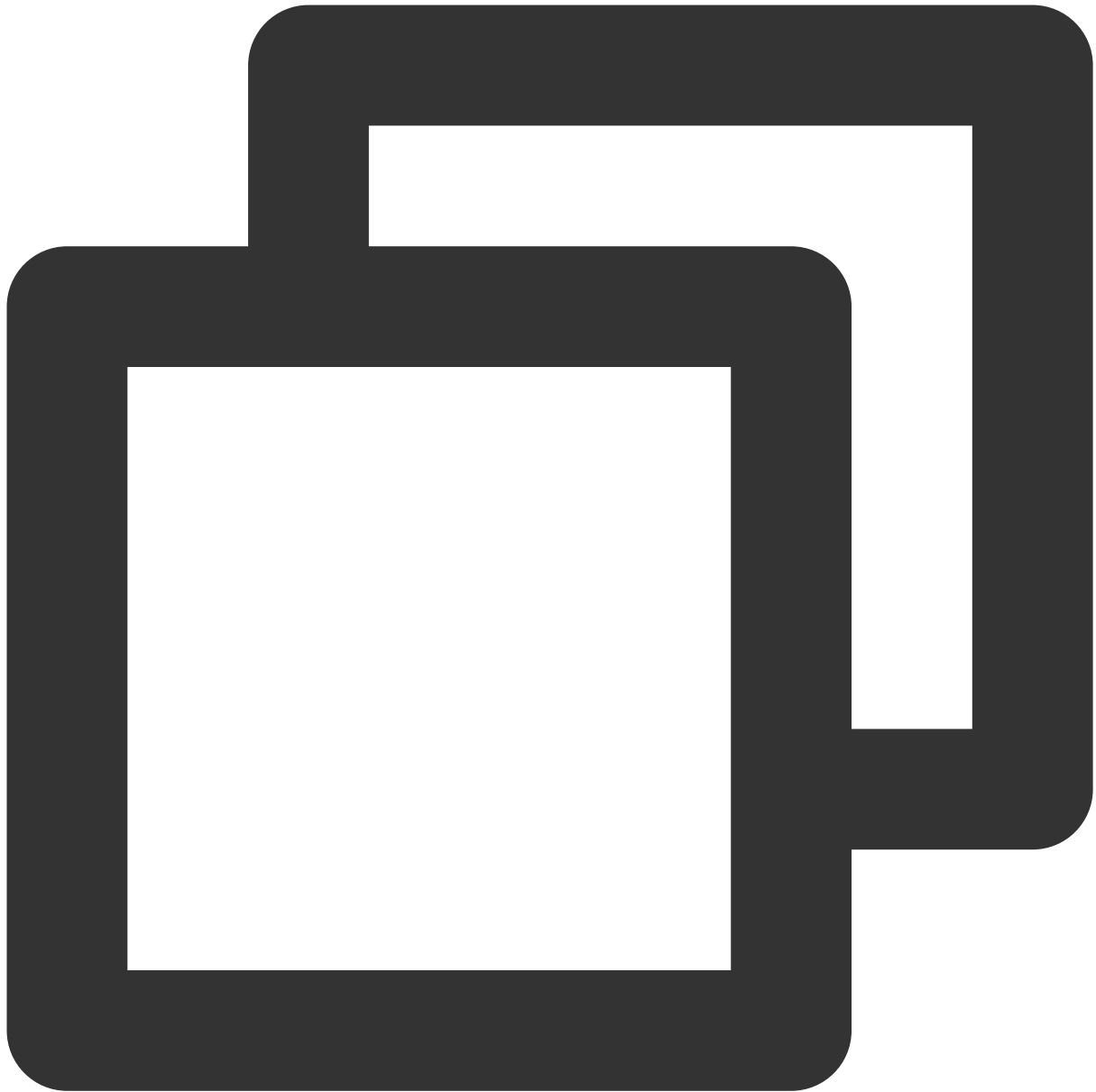
Instruksi Konfigurasi ssl_ciphers

Rangkaian enkripsi ssl_ciphers yang dikonfigurasi harus dalam format yang sama dengan yang digunakan OpenSSL. Daftar algoritme adalah satu `<cipher strings>` atau lebih; beberapa algoritme harus dipisah dengan ":"; ALL mewakili semua algoritme, "!" menandakan agar tidak mengaktifkan algoritme, dan "+" menandakan agar memindahkan algoritme ke tempat terakhir.

Algoritme enkripsi untuk penonaktifan paksa default adalah:

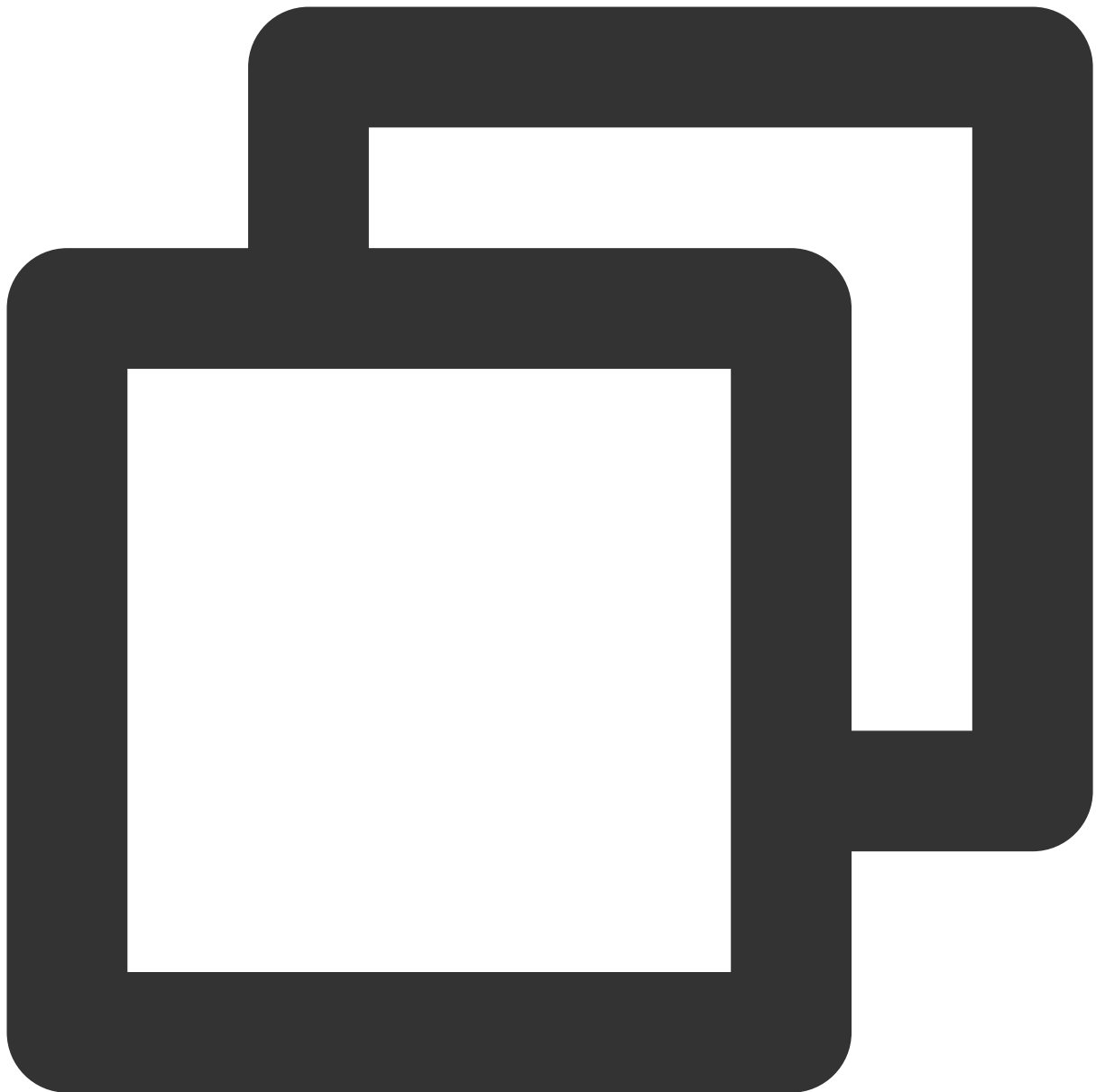
```
!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE .
```

Nilai default:



```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA3
```

Rentang parameter:



```
ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:SRP-DSS-AES-256-
```

Contoh Konfigurasi Khusus CLB

1. Masuk ke [Konsol CLB](#) dan klik **Custom Configuration** (Konfigurasi Khusus) di bilah sisi kiri.
2. Klik **Create** (Buat), isi item-item konfigurasinya dan akhiri dengan ";".

← **Create custom configuration**

Specifications

Configuration Name

Region **Guangzhou**

Code Configuration

```
1 client_max_body_size 2048M;  
2 proxy_request_buffering off;
```

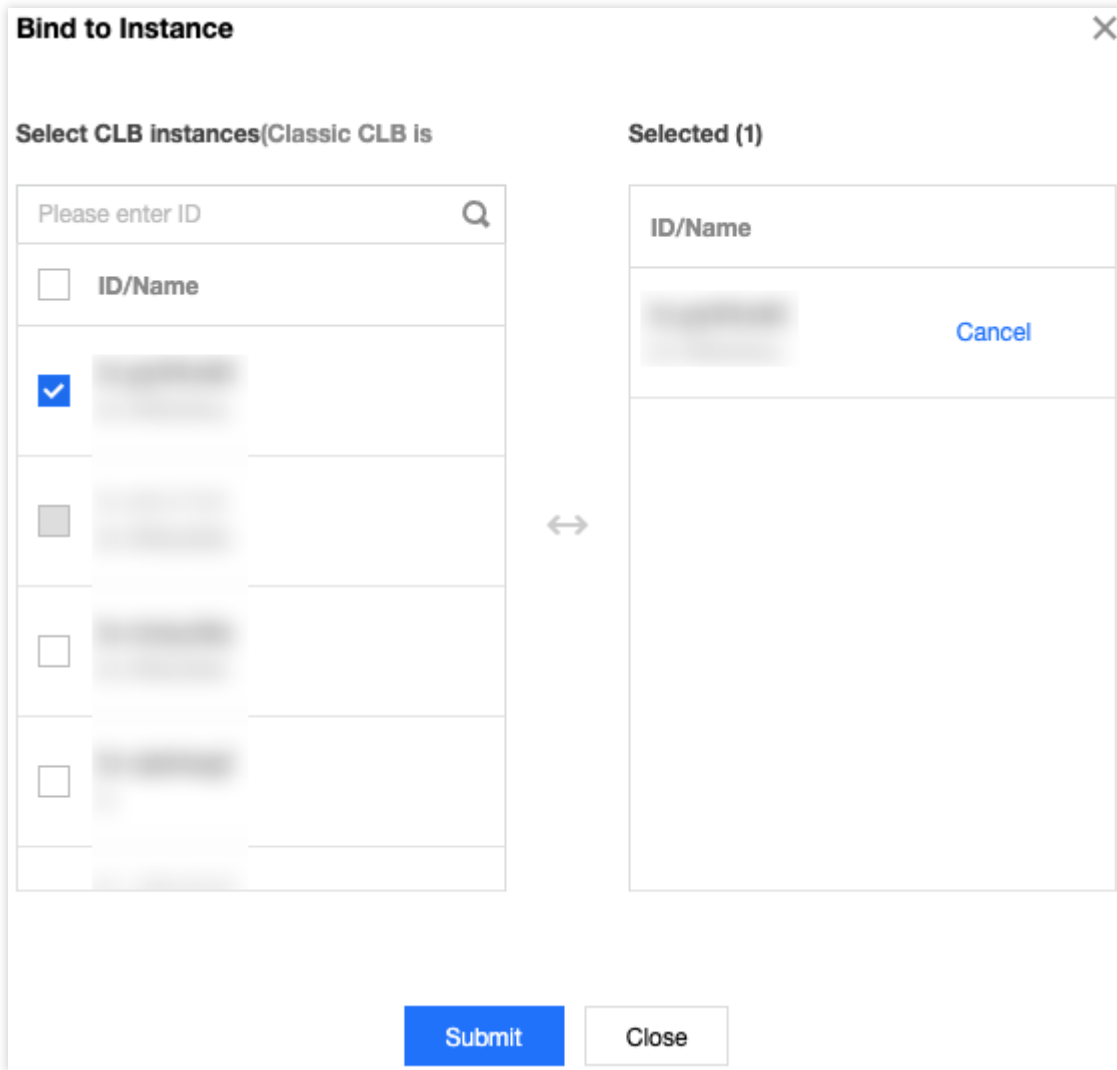
Parameters should accord with the supported configuration items and requirements, [Parameter De](#)

Completed

3. Klik **Completed** (Selesai).

4. Klik **Bind to Instance** (Ikat ke Instance).

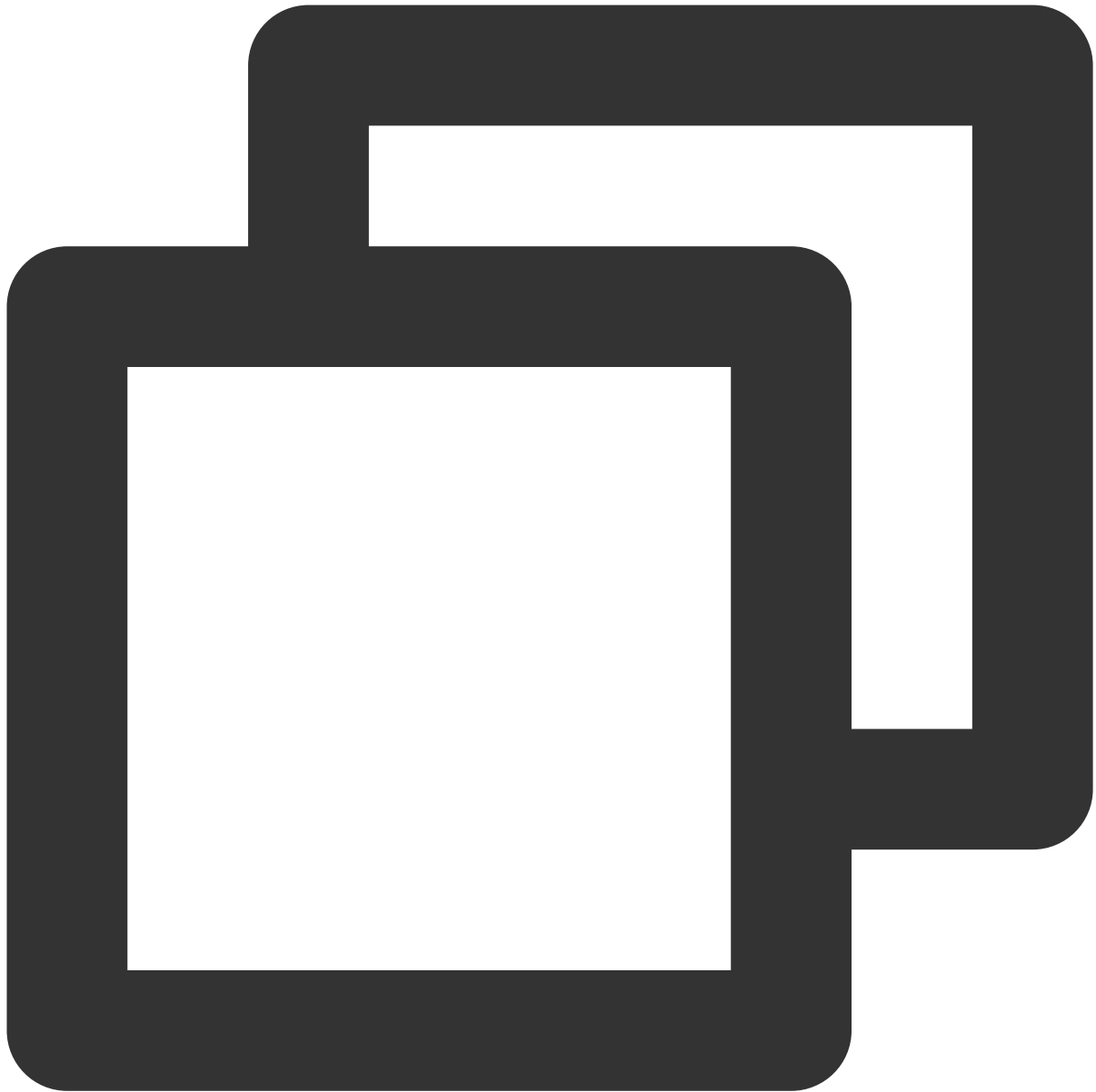
5. Di jendela pop-up, pilih instance CLB dari wilayah yang sama, dan klik **Submit** (Kirim).



6. Anda kini bisa melihat informasi konfigurasi khusus terkait di halaman daftar instance.

| <input type="checkbox"/> ID/Name ↕ | Mon... | Status | VIP | Availability Z... | Network ... ▾ | Network | Health Status |
|------------------------------------|-----------|--------|-----------|-------------------|----------------|---------------|---|
| <input type="checkbox"/> [blurred] | [blurred] | Normal | [blurred] | Guangzhou Zone 4 | Public Network | Basic Network | Health check not enabled (Configuration) |

Kode sampel konfigurasi default:



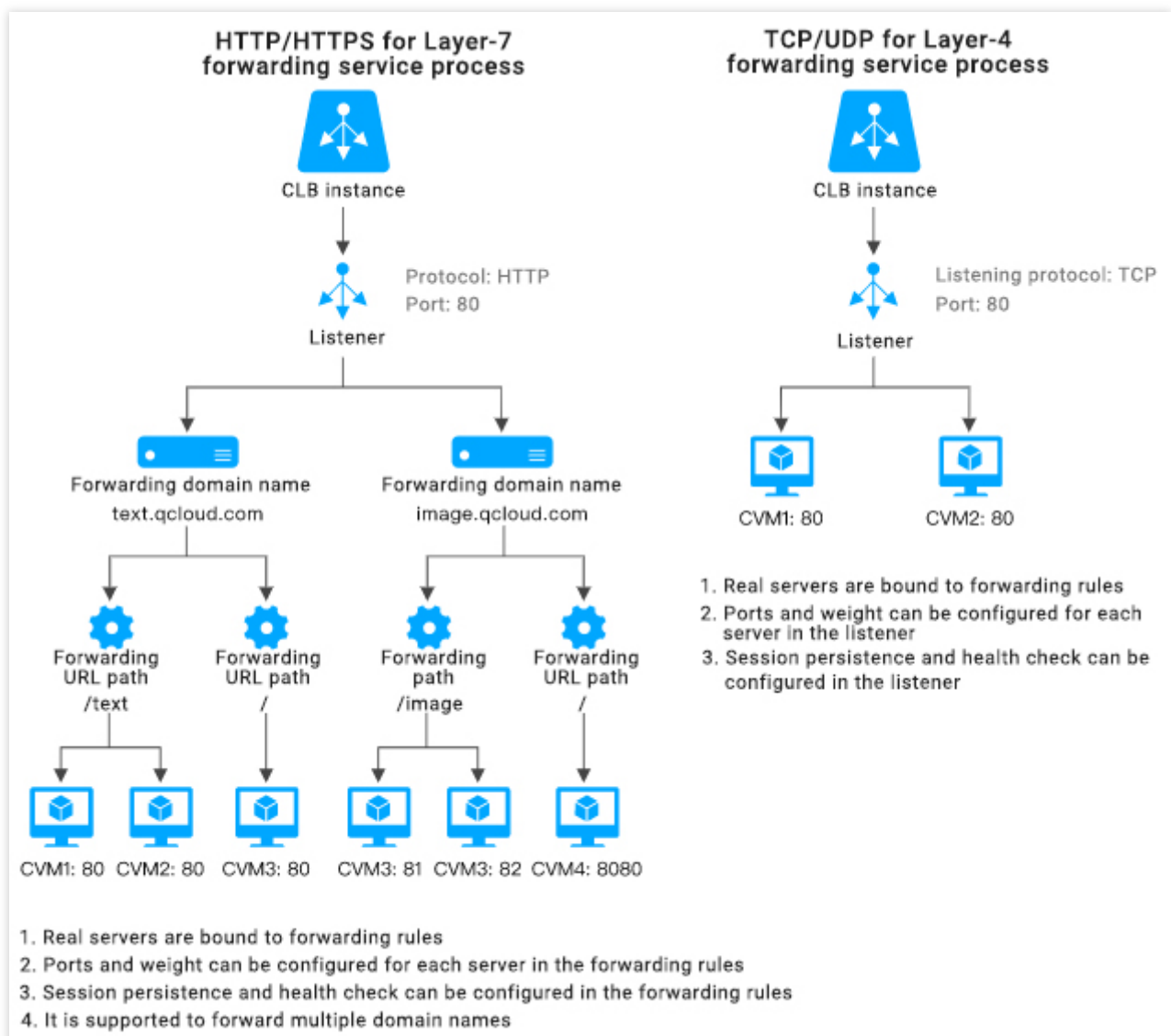
```
ssl_protocols    TLSv1 TLSv1.1 TLSv1.2;  
client_header_timeout    60s;  
client_header_buffer_size    4k;  
client_body_timeout    60s;  
client_max_body_size    60M;  
keepalive_timeout    75s;  
add_header    xxx yyy;  
more_set_headers    "A:B";  
proxy_connect_timeout    4s;  
proxy_read_timeout    60s;  
proxy_send_timeout    60s;
```


Aturan Penerusan dan URL Nama Domain Lapisan 7

Waktu update terbaru : 2024-01-04 20:53:33

Aliran Proses

Aliran proses CLB lapisan 7 dan lapisan 4 (sebelumnya aplikasi CLB) ditunjukkan di bawah ini:



Jika CLB lapisan 7 digunakan untuk meneruskan protokol HTTP/HTTPS, Anda bisa menambahkan nama domain yang sesuai saat membuat aturan penerusan di pendengar CLB.

Jika hanya ada satu aturan penerusan yang dibuat, Anda bisa mengakses aturan penerusan dan layanan yang sesuai melalui VIP+URL.

Jika ada beberapa aturan penerusan yang dibuat, penggunaan VIP+URL tidak menjamin akses ke name+URL domain tertentu. Anda harus mengakses name+URL domain secara langsung untuk memastikan aturan penerusan sudah aktif. Dengan kata lain, saat Anda mengonfigurasi beberapa aturan penerusan, satu VIP mungkin sesuai dengan beberapa nama domain. Dalam hal ini, kami sarankan Anda mengakses layanan melalui name+URL domain tertentu alih-alih VIP+URL.

Konfigurasi Penerusan Lapisan 7

Konfigurasi penerusan domain

CLB lapisan 7 bisa meneruskan permintaan dari nama dan URL domain berbeda ke server-server berbeda. Pendengar lapisan 7 bisa dikonfigurasi dengan beberapa nama domain, yang masing-masing bisa dikonfigurasi dengan beberapa jalur penerusan.

Batas panjang nama domain yang diteruskan: 1 hingga 80 karakter.

Tidak bisa diawali dengan `_`.

Mendukung satu domain pasti, seperti `www.example.com`.

Mendukung nama domain kartubebas, tetapi saat ini, hanya yang berupa `*.example.com` atau `www.example.*`, yaitu, nama domain kartubebas yang diawali atau diakhiri dengan `*`, yang hanya muncul satu kali.

Untuk nama domain non-ekspresi reguler yang diteruskan, set karakter yang valid mencakup `a-z`, `0-9`, `.`, `-`, `_`, `-` dan `_`.

Nama domain yang diteruskan mendukung ekspresi reguler. Nama domain ekspresi reguler:

Set karakter yang didukung mencakup `a-z`, `0-9`, `.`, `-`, `?`, `=`, `~`, `_`, `-`, `+`, `<code>\\`

Harus diawali dengan `~`, yang hanya bisa muncul satu kali.

Satu contoh nama domain yang didukung oleh CLB mungkin `~^www\\d+\\.example\\.com$`.

Pencocokan nama domain yang diteruskan

Kebijakan pencocokan umum

1. Jika Anda memasukkan alamat IP alih-alih nama domain di aturan penerusan dan mengonfigurasi beberapa URL di kelompok penerusan, VIP+URL akan digunakan untuk mengakses layanan.
2. Jika Anda mengonfigurasi satu nama domain lengkap di aturan penerusan dan beberapa URL di kelompok penerusan, name+URL domain akan digunakan untuk mengakses layanan.
3. Jika Anda mengonfigurasi satu nama domain kartubebas di aturan penerusan dan beberapa URL di kelompok penerusan, Anda akan mengakses layanan melalui pencocokan nama domain dan URL yang diminta. Agar nama domain yang berbeda mengarah ke URL yang sama, Anda bisa menggunakan metode ini untuk konfigurasi. Dengan menggunakan `example.qcloud.com` sebagai contoh, formatnya adalah sebagai berikut:

Pencocokan persis: mencocokkan nama domain yang benar-benar cocok dengan domain yang dimasukkan

Kartubebas awalan: mencocokkan semua nama domain dengan domain level dua dan teratas tertentu, seperti

```
*.qcloud.com .
```

Kartubebas akhiran: mencocokkan semua nama domain dengan domain level tiga dan dua tertentu, seperti

```
example.qcloud.* .
```

Pencocokan ekspresi reguler: `~^www\d+\\.example\com$`

Prioritas:**Exact match** (Pencocokan persis) > **Prefix wildcard** (Kartubebas awalan) > **Suffix wildcard** (Kartubebas akhiran) > **Regex match** (Pencocokan ekspresi reguler).Anda sebaiknya menggunakan nama domain yang lebih tepat untuk mencegah aktivasi beberapa aturan pencocokan.Jika tidak, Anda mungkin mendapat hasil pencocokan yang tidak akurat saat beberapa nama domain pada level yang sama dimasukkan sekaligus.

4.Jika Anda mengonfigurasi satu nama domain di aturan penerusan dan satu URL untuk pencocokan fuzzy di kelompok penerusan, Anda bisa memulai pencocokan lengkap dengan menggunakan pencocokan awalan dan menambahkan satu kartubebas akhiran `$` .

Contohnya, jika Anda memasukkan `URL ~*(gif|jpg|bmp)$` , hasilnya akan mencocokkan file .gif, .jpg, dan .bmp.

Kebijakan nama domain default

Jika nama domain yang diminta tidak cocok dengan aturan mana pun, CLB akan meneruskan permintaan itu ke nama domain default (Server Default).Satu pendengar hanya bisa memiliki satu nama domain default.

Contohnya, pendengar `HTTP:80` dari instance CLB 1 dikonfigurasi dengan dua nama domain:

`www.test1.com` dan `www.test2.com` , dan `www.test1.com` adalah nama domain defaultnya.Saat pengguna membuka `www.example.com` , karena tidak ada nama domain yang cocok, CLB akan meneruskan permintaan ke nama domain default `www.test1.com` .

Keterangan :

Jika pendengar lapisan 7 Anda sudah mengonfigurasi nama domain default, permintaan klien yang tidak cocok dengan aturan lainnya akan diteruskan padanya.

Jika pendengar lapisan 7 Anda belum mengonfigurasi nama domain default, permintaan klien yang tidak cocok dengan aturan lainnya akan diteruskan ke nama domain pertama yang dimuat oleh CLB (urutan pemuatannya bisa berbeda dengan yang dikonfigurasi di konsol, karenanya, ini mungkin bukan yang pertama dikonfigurasi di konsol).

Dimulai dari 18 Mei 2020:

Semua pendengar lapisan 7 baru harus memiliki nama domain default: aturan pertama pendengar lapisan 7 akan diatur sebagai nama domain default.Saat Anda membuat satu aturan lapisan 7 melalui API, bidang

```
DefaultServer diatur ke true .
```

Untuk semua pendengar yang sudah mengonfigurasi nama domain default, Anda harus menentukan nama domain default baru saat memodifikasi atau menghapus nama domain default yang ada: saat Anda melakukan operasi di konsol, Anda harus menentukan nama domain default baru; saat Anda melakukan operasi dengan

memanggil API, jika Anda tidak mengatur nama domain default baru, CLB akan mengatur nama yang paling awal dibuat di antara nama-nama domain tersisa sebagai nama domain default baru.

Untuk aturan tanpa nama domain default yang ada, Anda bisa mengonfigurasi nama domain default secara langsung sesuai kebutuhan bisnis Anda seperti yang diinstruksikan di [operasi 4](#) di bawah ini. Jika Anda tidak melakukannya, Tencent Cloud akan mengatur nama domain pertama yang dimuat oleh CLB sebagai nama domain default. Semua pendengar yang ada akan diproses sebelum 19 Juni 2020.

Kebijakan di atas akan diimplementasikan secara bertahap mulai dari 18 Mei 2020, dan tanggal berlaku untuk setiap instance mungkin sedikit berbeda. Mulai 20 Juni 2020, semua pendengar lapisan 7 yang telah meneruskan nama domain akan memiliki nama domain default.

Empat operasi berikut ini bisa dilakukan dengan nama domain default:

Operation 1 (Operasi 1): saat mengonfigurasi aturan penerusan yang pertama untuk pendengar lapisan 7, nama domain default harus berstatus “aktif”.

Operation 2 (Operasi 2): menonaktifkan nama domain default saat ini.

Jika di bawah satu pendengar ada beberapa nama domain, saat menonaktifkan nama domain saat ini, Anda harus menentukan nama domain default baru.

Jika satu pendengar hanya memiliki satu nama domain dan nama domainnya adalah nama domain default, nama domain itu tidak bisa dinonaktifkan.

Operation 3 (Operasi 3): menghapus nama domain default.

Jika di bawah satu pendengar ada beberapa nama domain, saat Anda menghapus satu aturan di bawah nama domain default:

Jika aturan itu bukan aturan terakhir pada nama domain default, Anda bisa langsung menghapusnya.

Jika aturan itu adalah aturan terakhir pada nama domain default, Anda harus mengatur nama domain default baru.

Jika di bawah satu pendengar hanya ada satu nama domain default, Anda bisa langsung menghapus semua aturan tanpa mengatur nama domain default baru.

O

Operation 4

(Operasi 4): Anda bisa dengan cepat memodifikasi nama domain default di daftar pendengar..

Aturan konfigurasi jalur URL yang diteruskan

CLB lapisan 7 bisa meneruskan permintaan dari URL berbeda ke server-server berbeda untuk pemrosesan, dan beberapa jalur URL yang diteruskan bisa dikonfigurasi untuk satu nama domain tunggal.

Batas panjang URL yang diteruskan: 1–200 karakter.

URL non-ekspresi reguler yang diteruskan harus dimulai dengan `/`, dengan set karakter yang valid termasuk `a-z`, `A-Z`, `0-9`, `.`, `-`, `_`, `/`, `=`, `?`, dan `:`.

URL yang diteruskan mendukung ekspresi reguler:

URL ekspresi reguler harus diawali dengan `~`, yang hanya bisa muncul satu kali.

Untuk URL ekspresi reguler, set karakter yang valid mencakup `a-z`, `A-Z`, `0-9`, `.`, `-`, `_`, `/`, `=`, `?`, `~`, `^`, `*`, `$`, `:`, `(`, `)`, `[`, `]`, `+`, dan `|`.

Satu contoh URL ekspresi reguler mungkin `~* .png$` .

Aturan pencocokan untuk URL yang diteruskan adalah sebagai berikut:

Diawali dengan `=` menunjukkan pencocokan persis.

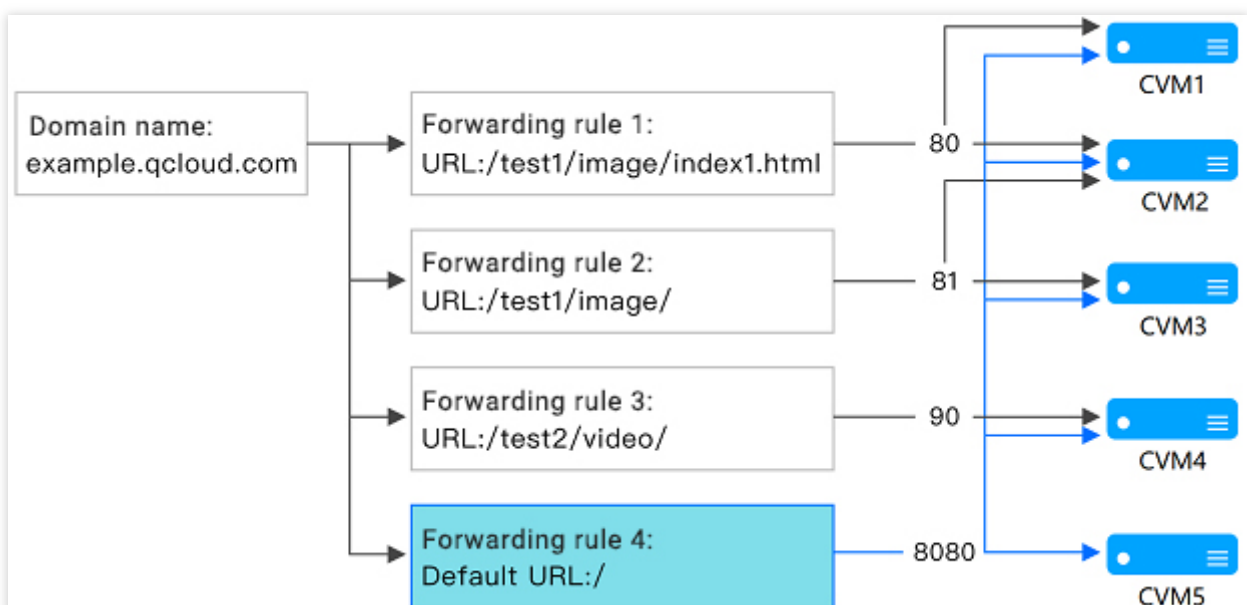
Diawali dengan `^~` menunjukkan URL dimulai dengan string reguler dan tidak untuk pencocokan ekspresi reguler.

Diawali dengan `~` menunjukkan pencocokan ekspresi reguler yang peka huruf besar/kecil.

Diawali dengan `~*` menunjukkan pencocokan ekspresi reguler yang tidak peka huruf besar/kecil.

`/` menunjukkan pencocokan generik, artinya permintaan apa pun akan dicocokkan jika tidak ada yang cocok lainnya.

Deskripsi pencocokan jalur ULR yang diteruskan



1. Aturan pencocokan: berdasarkan pencocokan awalan, pencocokan persis dilakukan dahulu, diikuti dengan pencocokan fuzzy.

Contohnya, setelah Anda mengonfigurasi aturan penerusan dan kelompok penerusan seperti yang ditunjukkan di atas, permintaan-permintaan berikut ini akan dicocokkan dalam aturan penerusan berbeda secara berurutan.

1. Karena `example.qcloud.com/test1/image/index1.html` benar-benar cocok dengan aturan URL yang dikonfigurasi dengan kelompok penerusan 1, permintaannya akan diteruskan ke server asli yang terkait dengan kelompok penerusan 1, yaitu, port 80 dari CVM1 dan CVM2 dalam gambar.

2. Karena tidak ada pencocokan persis untuk `example.qcloud.com/test1/image/hello.html` , ini akan dicocokkan dengan aturan penerusan 2 berdasarkan pencocokan awalan terpanjang; karenanya, permintaan itu akan diteruskan ke server asli yang terkait dengan aturan penerusan 2, yaitu, port 81 dari CVM2 dan CVM3 dalam gambar.

3. Karena tidak ada pencocokan persis untuk `example.qcloud.com/test2/video/mp4/` , ini akan dicocokkan dengan aturan penerusan 3 berdasarkan pencocokan awalan terpanjang; karenanya, permintaan itu akan diteruskan ke server asli yang terkait dengan aturan penerusan 3, yaitu, port 90 dari CVM4 dalam gambar.

4. Karena tidak ada pencocokan persis untuk `example.qcloud.com/test3/hello/index.html` , ini akan dicocokkan dengan URL default direktori root `example.qcloud.com/` dengan pencocokan awalan

terpanjang. Dalam hal ini, Nginx akan meneruskan permintaan ke server asli seperti FastCGI (php) atau Tomcat (jsp), sementara Nginx akan berperan sebagai server proksi terbalik.

5. Karena tidak ada pencocokan persis untuk `example.qcloud.com/test2/`, ini akan dicocokkan dengan URL default direktori root `example.qcloud.com/` dengan pencocokan awalan terpanjang.

2. Jika layanan tidak berfungsi dengan baik dalam aturan URL yang ditetapkan, ini tidak akan dialihkan ke halaman lain setelah pencocokan berhasil.

Contohnya, klien meminta `example.qcloud.com/test1/image/index1.html` dan mencocokkannya dengan kelompok penerusan 1. Namun, ada satu pengecualian di server asli kelompok penerusan 1 dan halaman kesalahan 404 muncul. Anda akan melihat halaman kesalahan 404, tetapi tidak dialihkan ke halaman lain.

3. Anda sebaiknya mengarahkan URL default ini ke halaman stabil (seperti halaman statis atau beranda) dan mengikatnya ke semua server asli. Jika tidak ada aturan yang cocok, sistem akan mengarahkan permintaan ke halaman URL default; jika tidak, mungkin muncul kesalahan 404.

4. Jika Anda tidak mengatur URL default, dan tidak ada aturan penerusan yang cocok, kesalahan 404 akan dikembalikan saat Anda mengakses layanan.

5. Perhatikan garis miring di akhir jalur URL lapisan 7: URL yang Anda atur diakhiri `/`, tetapi permintaan akses dari klien tidak mengandung `/`, permintaan akan dialihkan ke aturan yang diakhiri `/` (pengalihan 301).

Contohnya, di bawah pendengar `HTTP : 80`, nama domain yang dikonfigurasi adalah `www.test.com`:

1. Jika URL yang diatur di bawah nama domain ini adalah `/abc/`:

Saat klien mengakses `www.test.com/abc`, ini akan dialihkan ke `www.test.com/abc/`.

Saat klien mengakses `www.test.com/abc/`, ini akan cocok dengan `www.test.com/abc/`.

2. Jika URL yang diatur di bawah nama domain ini adalah `/abc`:

Saat klien mengakses `www.test.com/abc`, ini akan cocok dengan `www.test.com/abc`.

Saat klien mengakses `www.test.com/abc/`, ini juga akan cocok dengan `www.test.com/abc`.

Deskripsi Konfigurasi Pemeriksaan Kesehatan Lapisan 7

Aturan konfigurasi nama domain pemeriksaan kesehatan

Nama domain pemeriksaan kesehatan adalah nama domain yang digunakan oleh CLB lapisan 7 untuk mendeteksi status kesehatan server asli.

Batas panjang: 1-80 karakter.

Default: nama domain yang diteruskan.

Ekspresi reguler tidak didukung. Jika nama domain yang Anda teruskan adalah nama domain kartubebas, Anda harus menentukan nama yang tetap (non-ekspresi reguler).

Set karakter yang valid mencakup `a-z`, `0-9`, `.`, `-`, dan `_`. Contohnya, `www.example.qcloud.com`.

Aturan konfigurasi jalur pemeriksaan kesehatan

Jalur pemeriksaan kesehatan adalah jalur URL yang digunakan oleh CLB lapisan 7 untuk mendeteksi status kesehatan server asli.

Batas panjang: 1-200 karakter.

Default: `/`. Anda bisa memasuki jalur khusus berawalan `/`.

Ekspresi reguler tidak didukung. Anda sebaiknya menentukan URL tetap (halaman statis) untuk pemeriksaan kesehatan.

Set karakter yang valid mencakup `a-z`, `A-Z`, `0-9`, `.`, `-`, `_`, `/`, `=`, `?`, dan `:`. Contohnya, `/index`.

Menggunakan Protokol QUIC di CLB

Waktu update terbaru : 2024-01-04 20:53:33

Protokol QUIC membantu Anda mengakses aplikasi lebih cepat dan mencapai multiplexing tanpa membutuhkan koneksi ulang pada skenario seperti jaringan lemah atau sering beralih antara Wi-Fi dan 4G. Dokumen ini memperkenalkan cara mengonfigurasi protokol QUIC di Konsol CLB.

Ikhtisar QUIC

Quick UDP Internet Connection [QUIC](#) adalah protokol jaringan lapisan transportasi yang didesain oleh Google, aliran data bersamaan multiplexing menggunakan UDP. Dibandingkan dengan protokol TCP+TLS+HTTP2 yang populer, QUIC memiliki keunggulan sebagai berikut:

Mengurangi waktu untuk membuat koneksi.

Meningkatkan kontrol kemacetan.

Multiplex tanpa pemblokiran head-of-line (HOL).

Migrasi koneksi.

Setelah QUIC diaktifkan, klien bisa membuat koneksi QUIC dengan instance CLB. Jika koneksi QUIC gagal karena negosiasi antara klien dan instance CLB, HTTPS atau HTTP/2 akan digunakan. Namun, instance CLB dan server asli masih menggunakan protokol HTTP1.x.

Keterangan :

Saat ini, CLB mendukung QUIC Q044 dan versi lebih awal.

Batasan Penggunaan

Protokol QUIC di CLB saat ini ada di pengujian beta. Untuk menggunakannya, harap ajukan permohonan.

Protokol QUIC kini tersedia di Beijing, Shanghai, dan Mumbai.

Saat ini, hanya CLB jaringan publik dengan pendengar HTTPS lapisan 7 yang mendukung protokol QUIC.

Protokol QUIC saat ini hanya mendukung instance CLB AZ tunggal.

Petunjuk

1. Buat instance CLB sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Membuat Instance CLB](#).

Keterangan :

Saat membuat instance CLB, pilih “Beijing”, “Shanghai” atau “Mumbai” untuk **Region** (Wilayah), dan “Public Network” (Jaringan Publik) untuk **Network Type** (Jenis Jaringan).

2. Masuk ke [Konsol CLB](#), dan klik **Instance Management** (Manajemen Instance) di bilah sisi kiri.
3. Di halaman **Instance Management** (Manajemen Instance), pilih tab **Cloud Load Balancer** (Penyeimbang Beban Cloud).
4. Temukan instance CLB jaringan publik yang dibuat di wilayah Beijing, Shanghai atau Mumbai, dan klik **Configure Listener** (Konfigurasi Pendengar) di bawah kolom **Operation** (Operasi).
5. Di halaman **Listener Management** (Manajemen Pendengar), klik **Create** (Buat) di bawah **HTTP/HTTPS Listener** (Pendengar HTTP/HTTPS).
6. Di halaman **Create Listener** (Buat Pendengar), pilih "HTTPS" sebagai protokol port pendengaran. Selesaikan konfigurasi lainnya, lalu klik **Submit** (Kirim).
7. Di halaman **Listener Management** (Manajemen Pendengar), klik simbol **+** di samping pendengar yang baru Anda buat.
8. Di halaman **Create Forwarding rules** (Buat aturan Penerusan), aktifkan **QUIC** dan buat aturan lapisan 7. Isi bidang yang relevan dan klik **Next** (Berikutnya) untuk menyelesaikan konfigurasi dasar.

Keterangan :

Jika Anda mengaktifkan protokol QUIC saat membuat aturan penerusan HTTPS, Anda bisa mengaktifkan atau menonaktifkan protokol QUIC nanti sesuai kebutuhan. Jika Anda tidak mengaktifkan protokol QUIC saat membuat aturan penerusan HTTPS, Anda tidak bisa mengaktifkannya nanti.

Berdasarkan protokol UDP, QUIC akan menggunakan port UDP dari instance CLB. Jika Anda mengaktifkan QUIC untuk pendengar HTTPS, port UDP dan TCP akan digunakan. Contohnya, Anda mengaktifkan QUIC untuk pendengar HTTPS:443, baik port TCP:443 dan UDP:443 digunakan, dan Anda tidak bisa membuat pendengar TCP:443 atau UDP:443.

Operasi Selanjutnya

Setelah konfigurasi dasar diselesaikan, Anda bisa mengonfigurasi [pemeriksaan kesehatan](#) dan [persistensi sesi](#).

Dukungan SNI untuk Mengikat Beberapa Sertifikat ke Instance CLB

Waktu update terbaru : 2024-01-04 20:53:33

Indikasi Nama Server (SNI) didesain untuk menyelesaikan masalah bahwa satu server hanya bisa menggunakan satu sertifikat untuk meningkatkan perpanjangan SSL/TLS dari server dan klien. Jika suatu server mendukung SNI, artinya server tersebut bisa diikat ke beberapa sertifikat. Untuk menggunakan SNI untuk klien, nama domain yang akan disambungkan harus ditentukan sebelum koneksi SSL/TLS ke server tersambung, dan kemudian server akan mengembalikan sertifikat yang sesuai berdasarkan nama domain.

Kasus Penggunaan

Pendengar CLB HTTPS lapisan 7 mendukung SNI, yaitu, mengikat beberapa sertifikat, yang bisa digunakan oleh nama-nama domain berbeda di aturan pendengaran. Contohnya, di pendengar `HTTPS:443` yang sama dari suatu instance CLB, Anda bisa menggunakan sertifikat 1 dan sertifikat 2 untuk `*.test.com` dan `*.example.com` masing-masing untuk meneruskan permintaan dari nama-nama domain ini ke dua set server yang berbeda.

Prasyarat

Anda telah [membeli satu instance CLB](#).

Keterangan :

CLB klasik tidak mendukung penerusan berdasarkan nama domain dan URL; jadi, tidak mendukung SNI.

Petunjuk

1. Masuk ke [Konsol CLB](#).
2. [Konfigurasi pendengar HTTPS](#) dan aktifkan SNI.

CreateListener

Name

Listen Protocol Ports :

Enable SNI

1. If you select HTTPS protocol for forwarding, the accesses from client to load balancer is encrypted with HTTPS protocol. HTTP protocol is adopted to forward requests from load balancers to backend CVM.

2. The load balancer serves as an agent for the overhead of SSL encryption and decryption, and ensures Web access security.

3. You can go to [SSL Certificate Management Platform](#) to apply for an SSL certificate for free.

4. To enable SNI, you do not need to configure the certificate here. Please configure it on the domain configuration page.

3. Saat menambahkan aturan penerusan pada pendengar, konfigurasi sertifikat server berbeda untuk nama-nama domain berbeda. Kemudian, klik **Next** (Berikutnya) dan konfigurasi pemeriksaan kesehatan dan persistensi sesi.

Create Forwarding rules ✕

1 Basic Configuration >
2 Health Check >
3 Session Persistence

Domain Name ⓘ

Default Domain Name
If the client request does not match any domain name of this listener, CLB will forward the request to the default domain name. Each listener can only be configured with one default domain name, [Details](#)

HTTP2.0

URL ⓘ

Balance Method Weighted Round Robin ▾
If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Backend Protocol ⓘ HTTP ▾

SSL Phrasing One-way Authentication(Recommended) ▾ [Detailed Comparison](#)

Note: Choose SSL two-way authentication if you also need a certificate from the client.

Server Certificate Select existing Create

Please select ▾

Get client IP Enabled

Gzip compression Enabled ⓘ

Close
Next

Server Asli

Ikhtisar Server Asli

Waktu update terbaru : 2024-01-04 20:53:33

Apa itu server asli?

Server asli adalah [instance CVM](#) yang terikat ke instance CLB yang dibuat untuk memproses permintaan. Saat mengonfigurasi [pendengar CLB](#), Anda harus mengikat instance CVM sebagai server asli. Melalui berbagai [metode polling](#), CLB meneruskan permintaan ke server asli untuk pemrosesan untuk memastikan kestabilan dan keandalan aplikasi. Anda bisa mengikat instance CVM menjadi satu zona ketersediaan atau lebih, di wilayah tempat instance CLB berada untuk meningkatkan ketahanan aplikasi dan memblokir satu titik kegagalan.

Tindakan pencegahan

Saat menambahkan satu server asli, Anda sebaiknya:

Menginstal server web (misalnya, Apache atau IIS) pada semua instance CVM untuk diikat ke instance CLB dan memastikan konsistensi aplikasi.

Anda disarankan untuk mengaktifkan [persistensi sesi](#), agar CLB bisa mempertahankan koneksi TCP yang lebih panjang untuk digunakan ulang oleh beberapa permintaan sehingga mengurangi beban server web dan meningkatkan throughput CLB.

Pastikan grup keamanan instance nyata memiliki aturan masuk untuk port pendengar CLB dan port pemeriksaan kesehatan. Untuk informasi selengkapnya, silakan lihat [Konfigurasi Grup Keamanan pada Server Asli](#).

Mengelola Server Asli

Waktu update terbaru : 2024-01-04 20:53:19

CLB mengarahkan permintaan ke instance server asli yang berjalan dengan normal. Dokumen ini menjelaskan cara menambah atau menghapus server asli sesuai kebutuhan atau saat Anda menggunakan CLB untuk pertama kalinya.

Prasyarat

Anda telah membuat instance CLB dan mengonfigurasi satu pendengar. Untuk informasi selengkapnya, silakan lihat [Memulai CLB](#).

Petunjuk

Menambahkan server asli ke instance CLB

Keterangan :

Jika instance CLB diasosiasikan dengan grup penskalaan otomatis, instance CVM di grup itu akan ditambahkan secara otomatis ke server asli instance CLB. Jika instance CVM dihapus dari grup penskalaan otomatis, instance itu akan dihapus secara otomatis dari server asli instance CLB.

Jika Anda perlu menggunakan API untuk menambahkan server asli, silakan lihat [RegisterInstancesWithLoadBalancer](#) API.

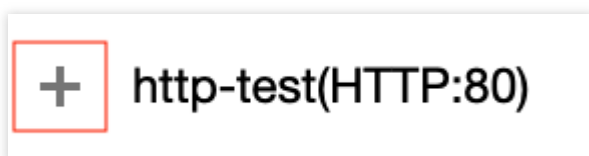
1. Masuk ke [Konsol CLB](#).
2. Pada tab "Penyeimbang Beban Cloud" di halaman "Manajemen Instance", klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB target.
3. Pada modul konfigurasi pendengar, pilih pendengar yang akan diikat pada server asli.

HTTP/HTTPS

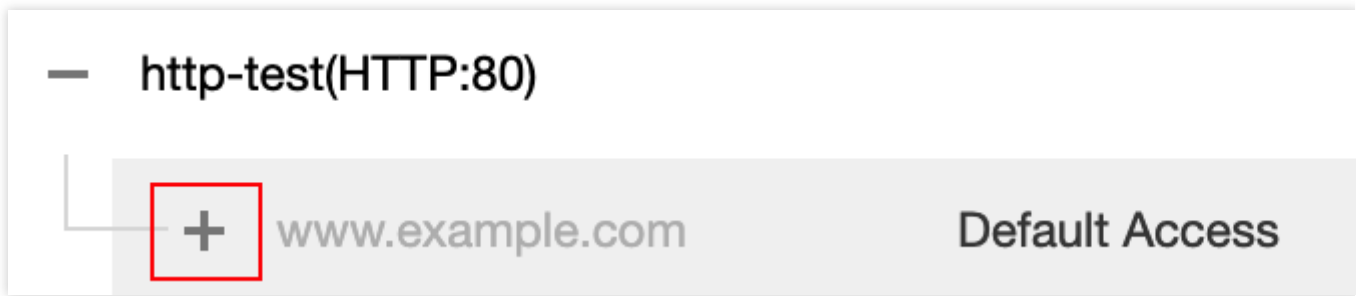
Listener

(Pendengar HTTP/HTTPS)

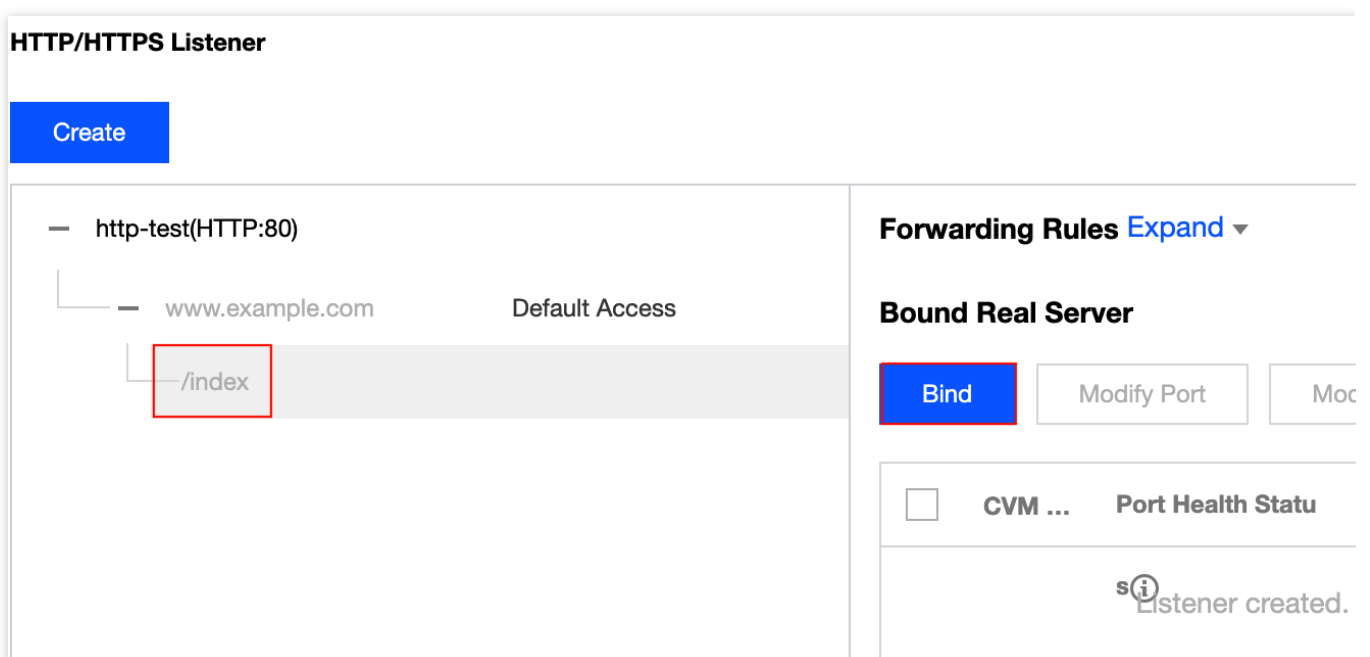
1. Di area pendengar HTTP/HTTPS, klik "+" di sebelah kiri pendengar target.



2. Klik "+" di sebelah kiri nama domain yang diperluas.



3. Pilih jalur URL yang diperluas dan klik **Bind** (Ikat).



TCP/UDP/TCP SSL listener (Pendengar TCP/UDP/TCP SSL)

Pada daftar di sebelah kiri modul pendengar TCP/UDP/TCP SSL, pilih pendengar yang akan diikat ke server asli dan klik **Bind** (Ikat).

TCP/UDP/TCP SSL Listener

Create

ipv6-ssh(TCP:22)

Listener Details Expand ▾

Bound Real Server

Bind Modify Port Moc

CVM ... Port Health Statu

Listener created.

4. Ikat server asli ke instance CLB

Method 1 (Metode 1). Di jendela pop-up "Ikat Server Asli", klik **CVM**, pilih satu atau beberapa instance CVM untuk berasosiasi, masukkan port dan beban, dan klik **OK**. Untuk informasi selengkapnya, silakan lihat [Port Server Umum](#).

Keterangan :

Jendela pop-up "Ikat Server Asli" hanya menampilkan instance CVM yang tersedia di satu wilayah dan satu lingkungan jaringan yang tidak terisolasi dan belum kedaluwarsa dengan batas bandwidth lebih dari 0.

Jika beberapa server asli terikat, CLB akan meneruskan lalu lintas sesuai dengan algoritme hash untuk menyeimbangkan beban.

Makin besar bobot server, makin banyak permintaan yang diteruskan ke sana. Nilai defaultnya 10, dan rentang nilai yang bisa dikonfigurasi adalah 0-100. Jika bobot diatur ke 0, server tidak akan menerima permintaan baru. Jika persistensi sesi diaktifkan, distribusi permintaan yang tidak merata di antara server asli bisa terjadi. Untuk informasi selengkapnya, silakan lihat [Konfigurasi Algoritme dan Bobot](#).

Bind with backend service

Select an instance

CVM
ENI
Please enter the d

IP address ▾
Search by IP address, Q

Instance ID/name

[blurred instance ID]

[blurred instance ID]

10 ▾ / page
◀ 1 ▶ / 1 page

Selected (2)

| Instance ID/name | Port |
|-----------------------|------|
| [blurred instance ID] | 80 |
| [blurred instance ID] | 80 |

Press Shift key to select more

Confirm
Cancel

Method 2 (Metode 2). Jika Anda perlu mengikat server dalam beberapa batch dengan nilai port praatur yang sama, Anda bisa mengklik **CVM** di jendela pop-up "Ikat Server Asli", masukkan nilai port default (untuk informasi selengkapnya mengenai pemilihan port, silakan lihat [Port Server Biasa](#)), periksa server target, atur nilai bobot, dan klik **OK**.

Bind with backend service

Select an instance

CVM
ENI
80

IP address Search by IP address, Q

Instance ID/name

| | |
|-------------------------------------|------------------|
| <input checked="" type="checkbox"/> | Instance ID/name |
| <input checked="" type="checkbox"/> | Instance ID/name |
| <input checked="" type="checkbox"/> | Instance ID/name |

10 / page ◀ 1 / 1 page ▶

Press Shift key to select more

Selected (2)

| Instance ID/name | Port | Weight ⓘ | |
|------------------|------|--|--------------|
| Instance ID/name | 80 | - 10 + | Add a Delete |
| Instance ID/name | 80 | - 10 + | Add a Delete |

Confirm
Cancel

Memodifikasi bobot server asli untuk instance CLB

Bobot server asli menentukan jumlah permintaan CVM yang akan diteruskan. Saat mengikat server asli, Anda harus mengatur bobotnya terlebih dahulu. Berikut ini adalah penjelasan cara memodifikasi bobot server asli dengan "pendengar HTTP/HTTPS" sebagai contoh (yang bisa dimodifikasi untuk pendengar TCP/UDP/TCP SSL dengan cara yang sama).

Keterangan :

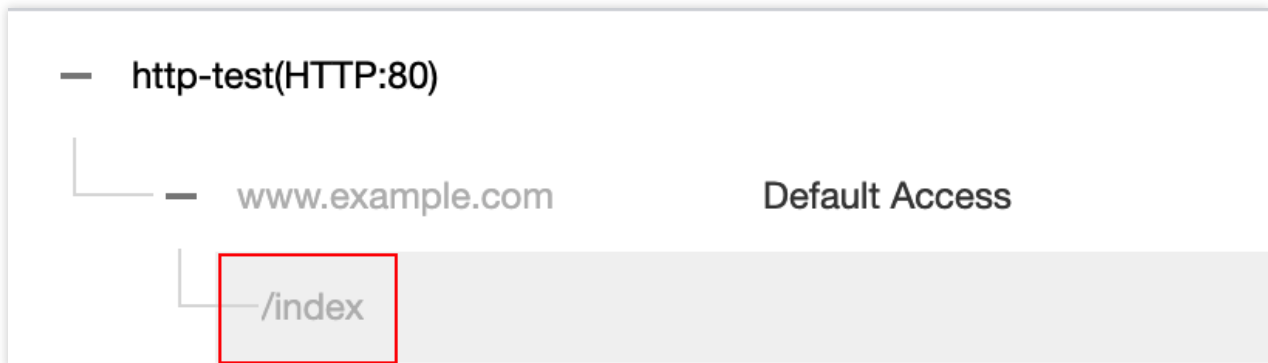
Jika Anda perlu menggunakan API untuk memodifikasi bobot server asli, silakan lihat [ModifyLoadBalancerBackends](#) API.

Untuk informasi selengkapnya mengenai bobot server asli CLB, silakan lihat [Metode Polling CLB](#).

1. Masuk ke [Konsol CLB](#).

2. Pada tab "Penyeimbang Beban Cloud" di halaman "Manajemen Instance", klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB target.

3. Pada daftar di sebelah kiri modul pendengar HTTP/HTTPS, perluas instance dan aturan pendengar, dan pilih jalur URL.



4. Pada daftar server di sebelah kanan modul pendengar HTTP/HTTPS, modifikasi bobot server yang relevan.

Keterangan :

Makin besar bobot server, makin banyak permintaan yang diteruskan ke sana. Nilai defaultnya 10, dan rentang nilai yang bisa dikonfigurasi adalah 0-100. Jika bobot diatur ke 0, server tidak akan menerima permintaan baru. Jika persistensi sesi diaktifkan, distribusi permintaan yang tidak merata di antara server asli bisa terjadi. Untuk informasi selengkapnya, silakan lihat [Konfigurasi Algoritme dan Bobot](#).

Method 1 (Metode 1). Modifikasi bobot satu server tunggal.

1. Temukan server yang bobotnya perlu dimodifikasi, arahkan kursor di bobot yang sesuai, dan klik



| <input type="button" value="Bind"/> <input type="button" value="Modify Port"/> <input type="button" value="Modify Weight"/> <input type="button" value="Unbind"/> | | | | |
|---|-------------|-------------------|------------|------|
| <input type="checkbox"/> | CVM ID/Name | Port Health Statu | IP Address | Port |
| <input type="checkbox"/> | [blurred] | Abnormal | [blurred] | 80 |
| <input type="checkbox"/> | [blurred] | Abnormal | [blurred] | 80 |

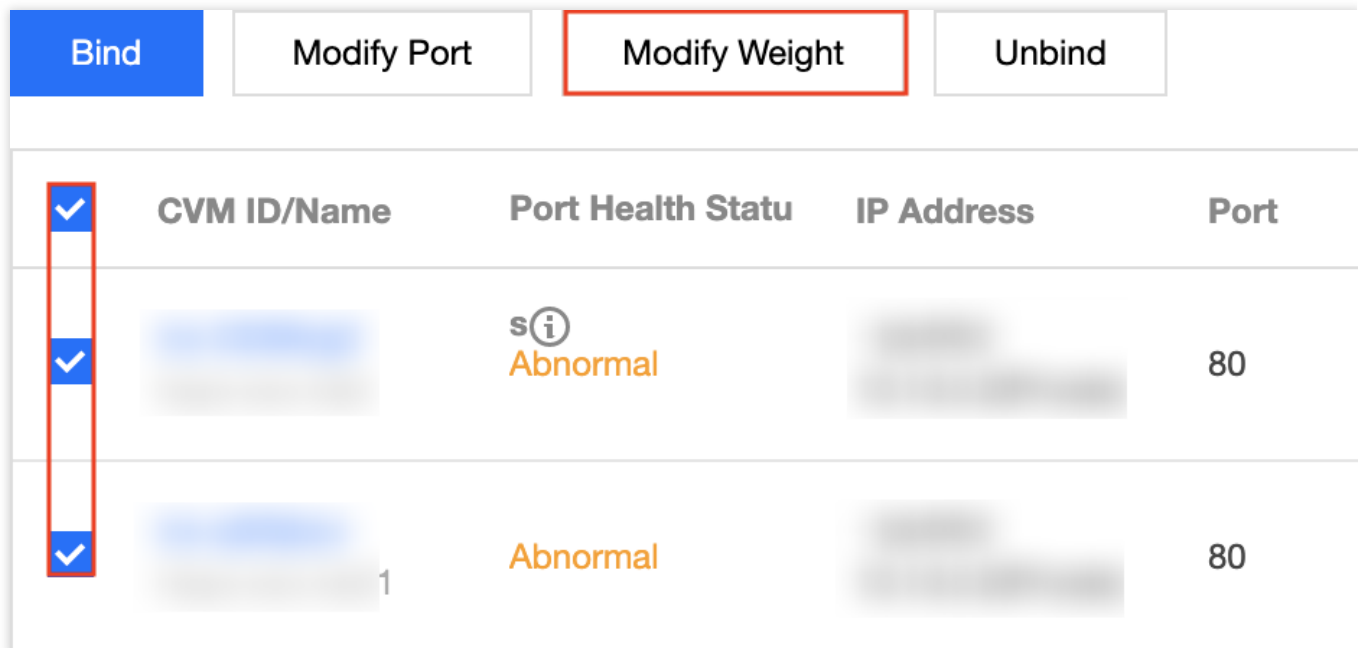
2. Di jendela pop-up "Modifikasi Bobot", masukkan nilai bobot yang baru dan klik **Submit** (Kirim).

Method 2 (Metode 2). Modifikasi bobot beberapa server dalam beberapa batch.

Keterangan :

Setelah modifikasi batch, server akan memiliki bobot yang sama.

1. Klik kotak di depan server, pilih beberapa server, dan klik **Modify Weight** (Modifikasi Bobot) di bagian atas daftar.



| | Bind | Modify Port | Modify Weight | Unbind |
|-------------------------------------|--------------------|------------------|---------------|--------|
| <input checked="" type="checkbox"/> | | | | |
| CVM ID/Name | Port Health Status | IP Address | Port | |
| <input checked="" type="checkbox"/> | | s(i) Abnormal | | 80 |
| <input checked="" type="checkbox"/> | | Abnormal | | 80 |

2. Di jendela pop-up "Modifikasi Bobot", masukkan nilai bobot yang baru dan klik **Submit** (Kirim).

Memodifikasi port server asli untuk instance CLB

Anda bisa memodifikasi port server asli di Konsol CLB. Berikut ini adalah penjelasan cara memodifikasi bobot server asli dengan "pendengar HTTP/HTTPS" sebagai contoh (yang bisa dimodifikasi untuk pendengar TCP/UDP/TCP SSL dengan cara yang sama).

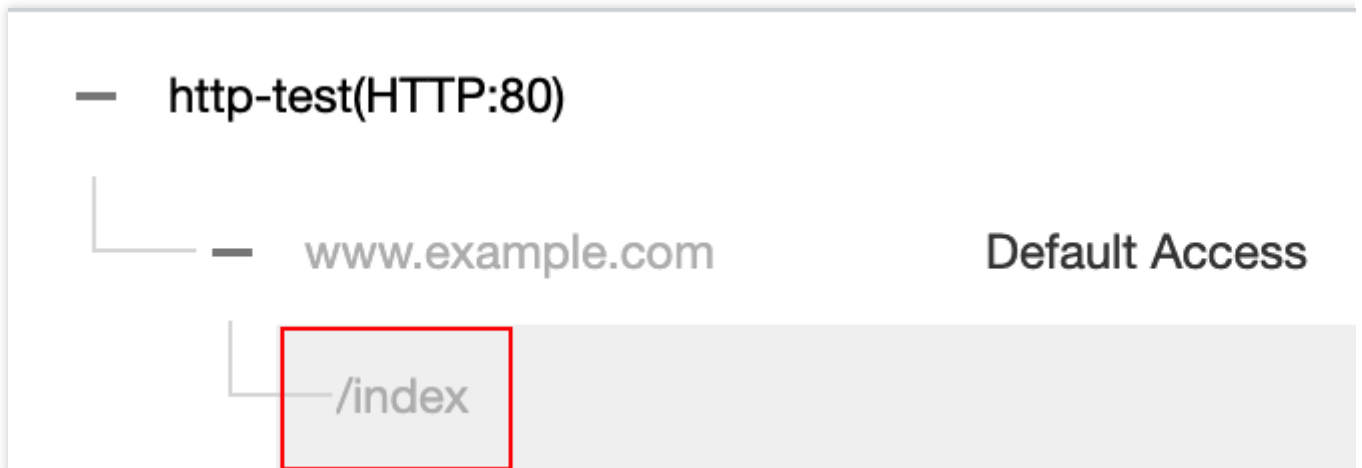
Keterangan :

Jika Anda perlu menggunakan API untuk memodifikasi port server asli, silakan lihat [ModifyTargetPort](#) API.

1. Masuk ke [Konsol CLB](#).

2. Pada tab "Penyeimbang Beban Cloud" di halaman "Manajemen Instance", klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB target.

3. Pada daftar di sebelah kiri modul pendengar HTTP/HTTPS, perluas instance dan aturan pendengar, dan pilih jalur URL.



4. Pada daftar server di sebelah kanan modul pendengar HTTP/HTTPS, modifikasi port server yang relevan. Untuk informasi selengkapnya mengenai pemilihan port, silakan lihat [Port Server Umum](#).

Method 1 (Metode 1). Modifikasi port satu server tunggal.

1. Temukan server yang portnya perlu dimodifikasi, arahkan kursor di port yang sesuai, dan klik



| Bind Modify Port Modify Weight Unbind | | | | | | |
|--|-------------|-------------------|------------|------|--------|----|
| <input type="checkbox"/> | CVM ID/Name | Port Health Statu | IP Address | Port | Weight | Op |
| <input type="checkbox"/> | [blurred] | Abnormal | [blurred] | 80 | 10 | Un |
| <input type="checkbox"/> | [blurred] | Abnormal | [blurred] | 80 | 10 | Un |







2. Di jendela pop-up "Modifikasi Port", masukkan nilai port yang baru dan klik **Submit** (Kirim).

Method 2 (Metode 2). Modifikasi port beberapa server dalam beberapa batch.

Keterangan :

Setelah modifikasi batch, server akan memiliki port yang sama.

1. Klik kotak di depan server, pilih beberapa server, dan klik **Modify Port** (Modifikasi Port) di bagian atas daftar.

| Bind | Modify Port | Modify Weight | Unbind | | |
|-------------------------------------|---|--|--------------------------|--------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| CVM ID/Name | Port Health Statu | IP Address | Port | Weight | C |
| <input checked="" type="checkbox"/> |  Abnormal |  | 80 | 10 |  |
| <input checked="" type="checkbox"/> |  Abnormal |  | 80 | 10 |  |

2. Di jendela pop-up "Modifikasi Port", masukkan nilai port yang baru dan klik **Submit** (Kirim).

Melepas ikatan server asli dari instance CLB

Anda bisa melepas ikatan server asli di Konsol CLB. Berikut ini adalah penjelasan cara melepas ikatan server asli dengan "pendengar HTTP/HTTPS" sebagai contoh (yang bisa dilepas dari pendengar TCP/UDP/TCP SSL dengan cara yang sama).

Keterangan :

Melepas ikatan server asli akan melepas ikatan instance CLB dari instance CVM, dan CLB akan langsung berhenti meneruskan permintaan ke sana.

Melepas ikatan server asli tidak akan memengaruhi siklus pemakaian instance CVM Anda, yang bisa ditambahkan lagi ke kluster server asli saat dibutuhkan.

Jika Anda perlu menggunakan API untuk melepas ikatan server asli, silakan lihat [DeregisterTargets](#) API.

1. Masuk ke [Konsol CLB](#).

2. Pada tab "Penyeimbang Beban Cloud" di halaman "Manajemen Instance", klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB target.

3. Pada daftar di sebelah kiri modul pendengar HTTP/HTTPS, perluas instance dan aturan pendengar, dan pilih jalur URL.



4. Pada server di sebelah kanan modul pendengar HTTP/HTTPS, lepas ikatan server asli.

Method 1 (Metode 1). Lepas ikatan satu server tunggal.

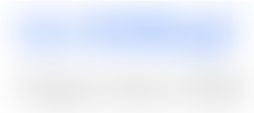

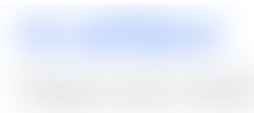

1. Temukan server yang perlu dilepas ikatannya dan klik **Unbind** (Lepas Ikatan) di kolom **Operation** (Operasi) di sebelah kanan.

| | Bind | Modify Port | Modify Weight | Unbind | |
|--------------------------|-------------|-------------|-----------------|------------|------|
| <input type="checkbox"/> | CVM ID/Name | Port | Health Status | IP Address | Port |
| <input type="checkbox"/> | | | s ⓘ Abnormal | | 80 |
| <input type="checkbox"/> | | 1 | Abnormal | | 80 |

2. Di jendela pop-up "Lepas Ikatan", konfirmasi server yang akan dilepas ikatannya dan klik **Submit** (Kirim).

Method 2 (Metode 2). Lepas ikatan beberapa server dalam beberapa batch.

1. Klik kotak di depan server, pilih beberapa server, dan klik **Unbind** (Lepas Ikatan) di bagian atas daftar.

| <input checked="" type="checkbox"/> | CVM ID/Name | Port Health Statu | IP Address | Port |
|-------------------------------------|---|----------------------------------|---|------|
| <input checked="" type="checkbox"/> |  | s i Abnormal |  | 80 |
| <input checked="" type="checkbox"/> |  1 | Abnormal |  | 80 |

2. Di jendela pop-up "Lepas Ikatan", konfirmasi server-server yang akan dilepas ikatannya dan klik **Submit** (Kirim).

Mengikat ENI

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar ENI

[Antarmuka Jaringan Elastis \(ENI\)](#) merujuk pada tipe antarmuka jaringan virtual yang bisa diikat ke instance CVM di VPC. ENI bisa bebas dimigrasi antara instance CVM dalam VPC dan AZ yang sama, membantu Anda membangun kluster ketersediaan tinggi dengan mudah, mengimplementasikan failover berbiaya rendah, dan mengelola jaringan dengan cara yang lebih baik.

Server asli CLB bisa diikat ke CVM dan ENI. Khususnya, instance CLB berkomunikasi dengan server asli melalui jaringan pribadi, dan jika beberapa instance CVM dan ENI diikat ke instance CLB, lalu lintas akses akan diteruskan ke IP pribadi instance CVM dan ENI.

Keterangan :

Fitur pengikatan ENI CLB sedang dalam pengujian beta. Jika Anda ingin menggunakannya, silakan [kirim tiket](#) untuk mendaftar.

Prasyarat

ENI harus diikat ke instance CVM terlebih dahulu sebelum bisa diikat ke instance CLB. Karena instance CLB hanya meneruskan lalu lintas sebagai penyeimbang beban, tetapi tidak memproses logika bisnis, instance CVM sebagai sumber daya komputasi diperlukan untuk memproses permintaan pengguna. Silakan masuk ke [Konsol ENI](#) untuk mengikat ENI yang dibutuhkan ke instance CVM terlebih dahulu.

ENI South China (Guangzhou) All VPCs

+ New Use ']' to split more than one keywords, and pre

| ID/Name | ENI Parameters | Network | Subnet | Bind CVM | Private I |
|---------|----------------|---------|--------|----------|-----------|
| | Secondary ENI | | | - | 1 |
| | Secondary ENI | | | - | 1 |
| | Secondary ENI | | | - | 1 |
| | Secondary ENI | | | | 1 |

Petunjuk

1. Anda harus mengonfigurasi pendengar CLB terlebih dahulu. Untuk informasi selengkapnya, silakan lihat [Ikhtisar Pendengar CLB](#).
2. Klik + di sebelah kiri pendengar yang dibuat untuk memperluas nama domain dan jalur URL, pilih jalur URL yang diinginkan, dan tampilkan server asli terikat yang ada di sebelah kanan pendengar.

HTTP/HTTPS Listener

Create

test(HTTP:80)

- www.example.com
 - /index**
 - /image

Forwarding Rules Expand

Bound Real Server

Bind Modify Port Modify Weight

| <input type="checkbox"/> | CVM ... | Port Sta... | IP Ad... | Port |
|---|---------|-------------|----------|------|
| Listener created. Please Bound real | | | | |

3. Klik **Bind** (Ikat), pilih server asli yang akan diikat dan konfigurasi port server dan bobot di jendela pop-up. Anda bisa memilih "CVM" atau "ENI" sebagai server asli.

CVM: Anda bisa mengikat IP pribadi primer dari ENI primer dari semua instance CVM di VPC yang sama sebagai instance CLB.

ENI: Anda bisa mengikat semua IP ENI di VPC yang sama sebagai instance CLB kecuali IP pribadi primer dari ENI primer dari instance CVM, seperti IP pribadi sekunder dari ENI primer dan IP pribadi dari ENI sekunder. Untuk informasi selengkapnya mengenai tipe-tipe IP ENI, silakan lihat [ENI - Konsep Utama](#).

Bound real server

IP

ID/Name

- [redacted] named
[redacted](Public)/10.20...
- [redacted] tke_cls-9cj31525_worker
[redacted](Public)/[redacted]
- [redacted] d/as-Demo
[redacted]13(Public)/[redacted]

Selected (3)

| ID/Name | Port | Weight |
|---|------|--------|
| ins-hq0utoivUnnamed 162.62.14.209(Public)/10.20... | 8000 | - 10 + |
| ins-bjei94w7tke_cls-9cj315... 162.62.17.174(Public)/10.20... | 8000 | - 10 + |
| ins-fdzhu1qdas-Demo 162.62.19.113(Public)/10.20... | 8000 | - 10 + |

Note: To ensure the forwarding works properly, please set the public network bandwidth to more than 0 MB for the CVM with public CLB.

OK
Cancel

4. Konfigurasi khusus setelah pengikatannya seperti yang ditunjukkan di bawah ini:

HTTP/HTTPS Listener







Create

- Demo(HTTP:80)
 - www.example.com
 - /index
 - /image

Forwarding Rules [Expand](#)

Bound Real Server

[Bind](#) [Modify Port](#) [Modify Weight](#) [Unbind](#)

| <input type="checkbox"/> | CVM ID/Name | Port S... | IP Address |
|--------------------------|--|-----------|--|
| <input type="checkbox"/> |  | Healthy |  9 (public Private) |
| <input type="checkbox"/> |  525_worker | Healthy |  4 (public Private) |
| <input type="checkbox"/> |  | Healthy |  3 (public Private) |

Selected 0 items, total 3 items

Mengikat dengan SCF

Waktu update terbaru : 2024-01-04 20:53:33

Anda bisa mengimplementasikan layanan web backend dengan menulis fungsi SCF dan mengikatnya dengan instance CLB untuk menyediakan layanan.

Keterangan :

Pengikatan instance CLB dengan fungsi SCF sedang dalam pengujian beta. Jika ingin menggunakannya, silakan hubungi perwakilan penjualan Anda.

Latar belakang

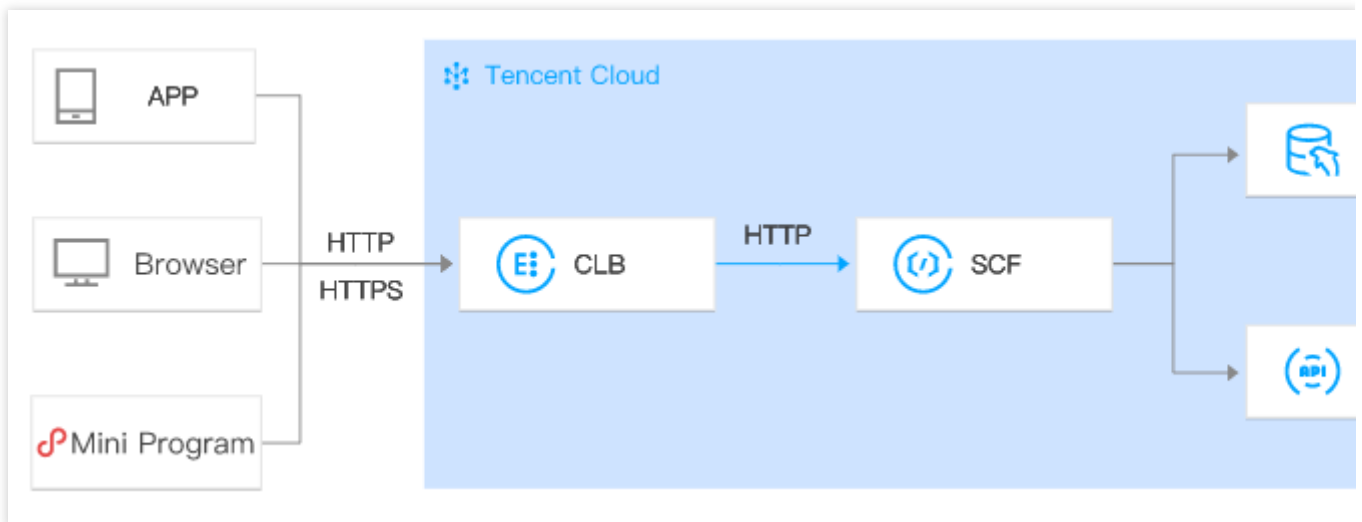
Tencent Cloud [Fungsi Cloud Tanpa Server \(SCF\)](#) adalah lingkungan eksekusi tanpa server yang membuat Anda bisa membangun dan menjalankan aplikasi tanpa harus membeli dan mengelola server. Setelah membuat fungsi, Anda bisa membuat pemicu CLB untuk mengikat fungsi dan event. Pemicu CLB akan meneruskan konten permintaan sebagai parameter fungsi dan mengembalikan hasil dari fungsi tersebut ke pemohon sebagai respons.

Kasus Penggunaan

HTTP/HTTPS general access

Berlaku pada aplikasi untuk ecommerce, media sosial dan layanan lainnya, dan aplikasi web untuk blog pribadi, halaman event dan lainnya. Alur kerjanya adalah sebagai berikut:

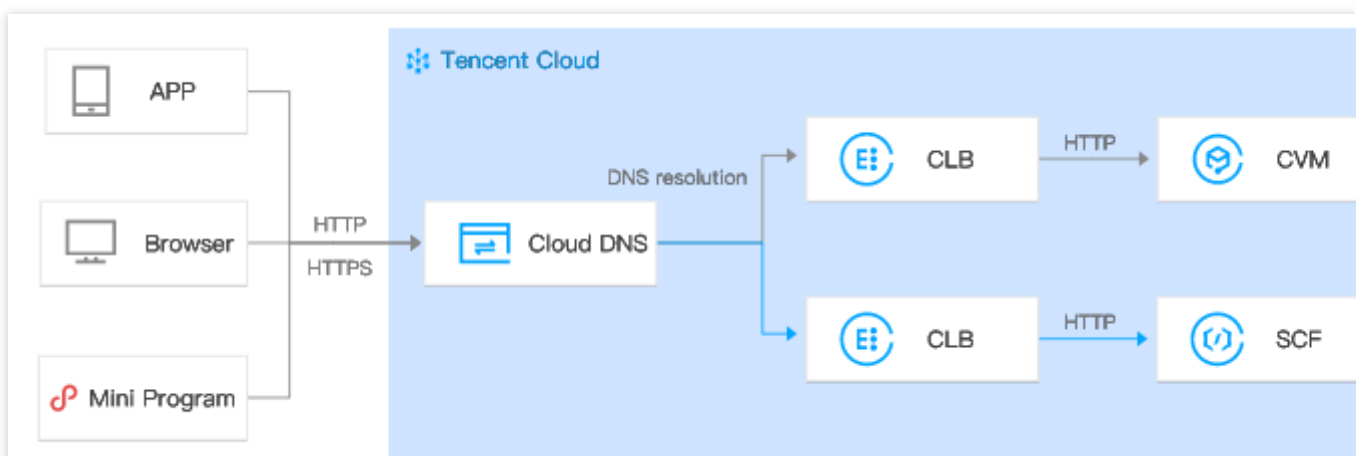
1. Permintaan HTTP/HTTPS yang dimulai oleh aplikasi, peramban, halaman H5, atau Program Mini mengakses fungsi SCF melalui instance CLB.
2. Setelah instance CLB menyelesaikan pelepasan instalasi sertifikat, SCF hanya perlu menyediakan layanan HTTP.
3. Permintaan kemudian ditransfer ke fungsi SCF untuk pemrosesan berikutnya, seperti penulisan ke database cloud dan memanggil API lainnya.



Switching between CVM and SCF

Berlaku untuk memigrasikan layanan HTTP/HTTPS dari CVM ke SCF, terutama jika terjadi failover. Alur kerjanya adalah sebagai berikut:

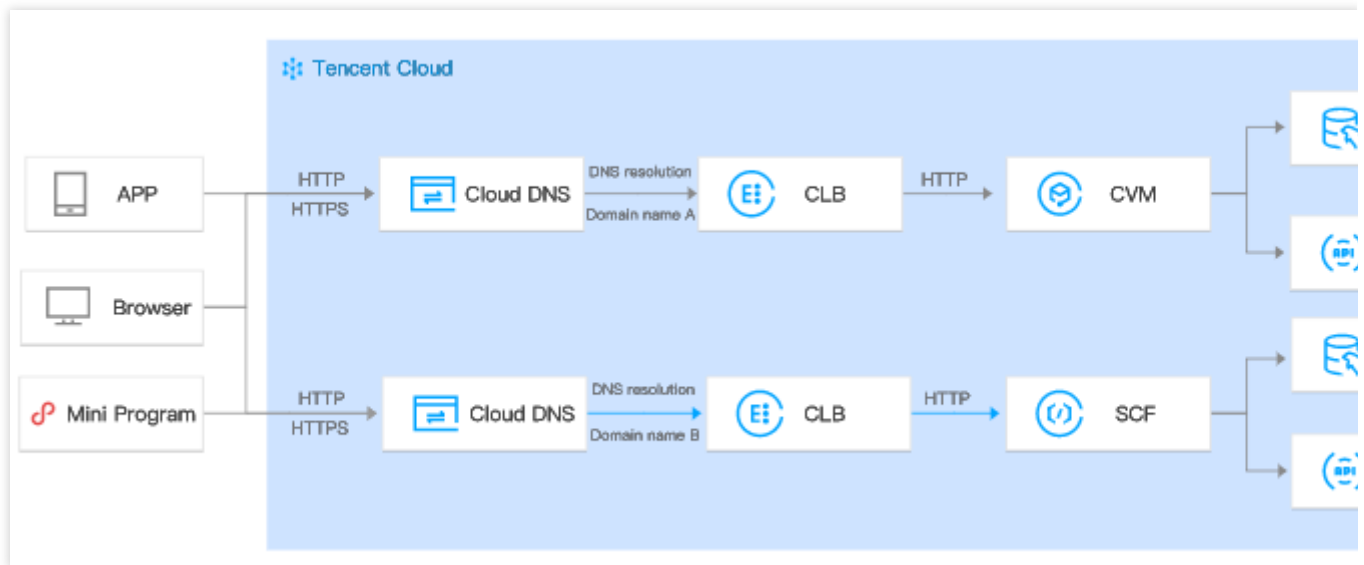
1. Aplikasi, peramban, H5, atau Program Mini Wechat memulai permintaan HTTP/HTTPS.
2. Permintaan itu kemudian diselesaikan ke dua VIP instance CLB oleh DNS.
3. Satu instance CLB meneruskan permintaan ke CVM dan yang lainnya meneruskannya ke SCF.
4. Peralihan dari CVM ke SCF di backend telah selesai tanpa memengaruhi pihak klien.



CVM/SCF business diversion

Berlaku saat pemakaian SCF untuk menangani layanan yang sangat elastis dan CVM untuk menangani bisnis harian dalam skenario seperti penjualan kilat dan pembelian snap-up.

1. Melalui resolusi DNS, nama domain A diselesaikan ke satu VIP instance CLB dan nama domain B diselesaikan ke VIP instance CLB lainnya.
2. Satu instance CLB meneruskan permintaan ke CVM dan yang lainnya meneruskannya ke SCF.



Batasan

Pengikatan dengan SCF hanya tersedia di Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (Tiongkok), Singapore, Mumbai, Tokyo, dan Silicon Valley.

Fungsi SCF hanya bisa diikat dengan instance CLB dari akun tagihan per IP, tetapi tidak dengan akun tagihan per CVM. Jika Anda menggunakan akun tagihan per CVM, kami menyarankan untuk meng-upgrade-nya ke akun tagihan per IP. Untuk informasi selengkapnya, silakan lihat [Memeriksa Tipe Akun](#).

Fungsi SCF tidak bisa diikat dengan instance CLB klasik.

Fungsi SCF tidak bisa diikat dengan instance CLB jaringan klasik.

Fungsi SCF hanya bisa diikat lintas VPC, tetapi tidak lintas wilayah.

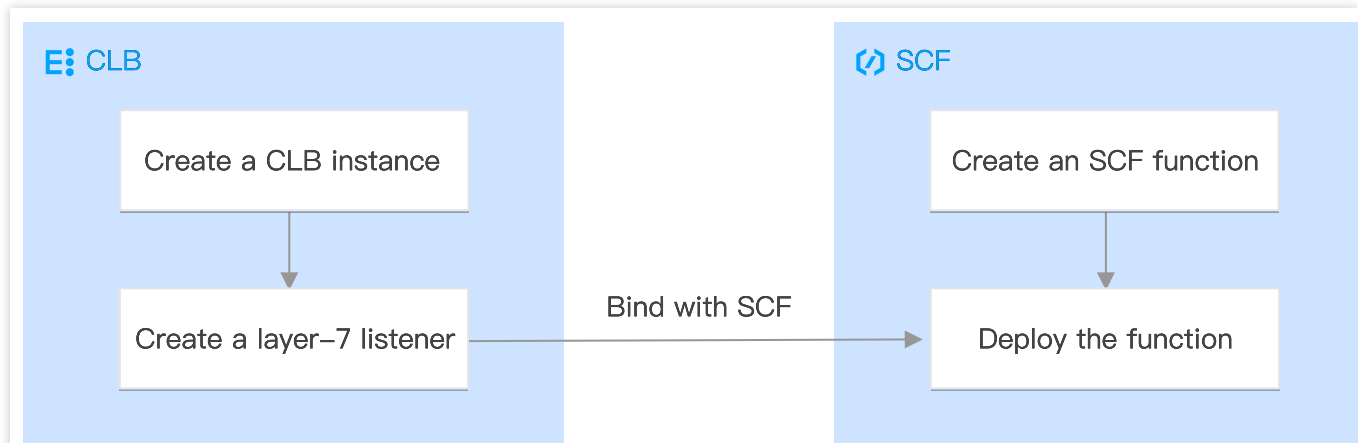
Fungsi SCF hanya bisa diikat dengan instance CLB IPv4 dan IPv6 NAT64, tetapi saat ini tidak dengan instance CLB IPv6.

Fungsi SCF hanya bisa diikat dengan pendengar HTTP dan HTTPS lapisan 7, tetapi tidak dengan pendengar QUIC lapisan 7 atau pendengar (TCP, UDP, dan TCP SSL) lapisan 4.

Prasyarat

1. Anda telah membuat [Instance CLB](#).
2. Anda telah mengonfigurasi pendengar [HTTP](#) atau [HTTPS](#).

Petunjuk

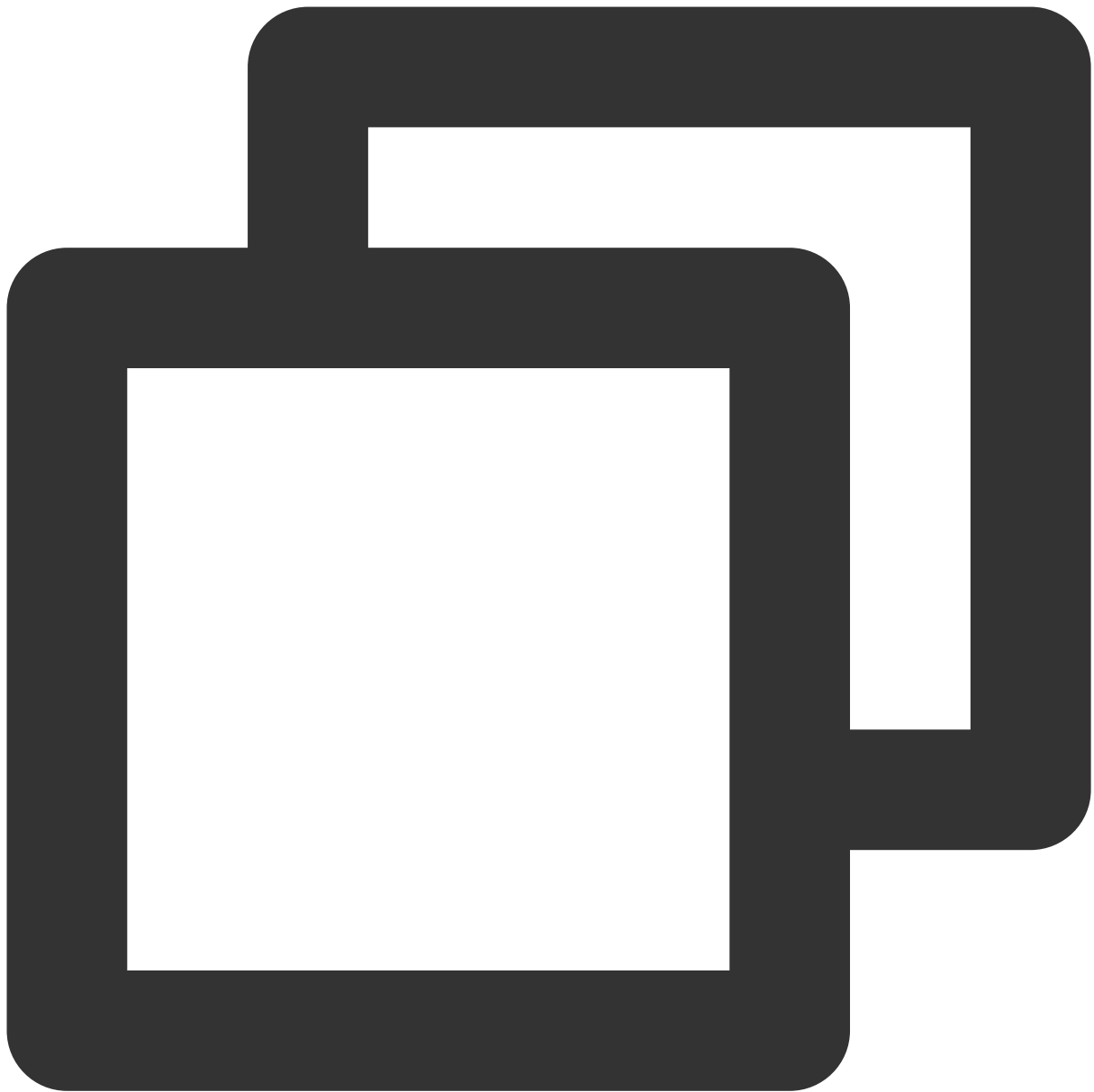


Langkah 1. Buat fungsi

1. Masuk ke [Konsol SCF](#) dan klik **Function Service** (Layanan Fungsi) di bilah sisi kiri.
2. Di halaman **Function Service** (Layanan Fungsi), klik **Create** (Buat).
3. Di halaman **Create** (Buat), pilih **Custom** (Khusus) untuk mode kreasinya, dan masukkan nama fungsi. Lalu pilih wilayah yang sama yang Anda pilih untuk instance CLB Anda dan **Python3.6** untuk lingkungan runtime, masukkan kode berikut ke kotak input (Hello CLB digunakan untuk ilustrasi), dan klik **Complete** (Selesai).

Perhatian :

Saat Anda mengikat instance CLB ke fungsi SCF, konten harus dikembalikan dalam format integrasi respons tertentu. Untuk informasi selengkapnya, lihat [Pemicu CLB](#).



```
# -*- coding: utf8 -*-
import json
def main_handler(event, context):

    return {
        "isBase64Encoded":False,
        "statusCode":200,
        "headers":{"Content-Type":"text/html"},
        "body": "<html><body><h1>Hello CLB</h1></body></html>"
    }
```

Langkah 2. Deploy fungsi

1. Di halaman daftar "Fungsi", klik nama fungsi yang Anda buat.
2. Di halaman **Function Management** (Manajemen Fungsi), pilih tab **Function Codes** (Kode Fungsi) dan klik **Deploy** di bagian bawah.

Langkah 3. Ikat fungsinya

1. Masuk ke [Konsol CLB](#) dan klik **Instance Management** (Manajemen Instance) di bilah sisi kiri.
2. Di halaman **Instance Management** (Manajemen Instance), klik **Configure Listener** (Konfigurasi Pendengar) di sebelah kanan instance.
3. Di bagian **HTTP/HTTPS Listener** (Pendengar HTTP/HTTPS), pilih pendengar yang akan diikat dengan fungsi SCF. Klik ikon **+** di sebelah kiri pendengar dan nama domain di bawahnya, pilih jalur URL yang ditampilkan, dan klik **Bind** (Ikat).
4. Di jendela pop-up, pilih SCF sebagai tipe target, atur item konfigurasi, dan klik **Confirm** (Konfirmasi).
5. Pada tab **Listener Management** (Manajemen Pendengar), Anda seharusnya melihat fungsi yang terikat pada instance CLB di bagian **Forwarding Rules** (Aturan Penerusan), yang menunjukkan pemicu CLB sudah dibuat.

Keterangan :

Anda juga bisa membuat pemicu CLB di konsol SCF untuk mengikat instance CLB dengan fungsi SCF. Untuk informasi selengkapnya, silakan lihat [Membuat Pemicu](#).

Validasi Hasil

1. Masuk ke [Konsol SCF](#) dan klik **Function Service** (Layanan Fungsi) di bilah sisi kiri.
2. Pada halaman **Function Service** (Layanan Fungsi), klik fungsi yang baru saja Anda buat.
3. Klik **Trigger Management** (Manajemen Pemicu) di sebelah kiri.
4. Di halaman **Trigger Management** (Manajemen Pemicu), klik **Access Path** (Jalur Akses).
5. Buka jalur akses di peramban. Jika "Hello CLB" ditampilkan, fungsi sudah berhasil di-deploy.

Referensi

[Membuat fungsi dengan konsol](#)

Pengikatan Lintas Wilayah 2.0 (Baru)

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung pengikatan instance CVM lintas wilayah melalui CCN, membuat Anda bisa memilih server asli dari wilayah berbeda dan mengikat instance CLB pada mereka di seluruh VPC atau wilayah.

Fitur ini saat ini dalam versi beta. Jika Anda ingin menggunakannya, untuk pengikatan lintas wilayah di luar Tiongkok daratan, silakan [hubungi perwakilan Tencent Cloud Anda](#).

Keterangan :

Saat ini tidak mendukung pengikatan CVM lintas wilayah untuk instance CLB klasik.

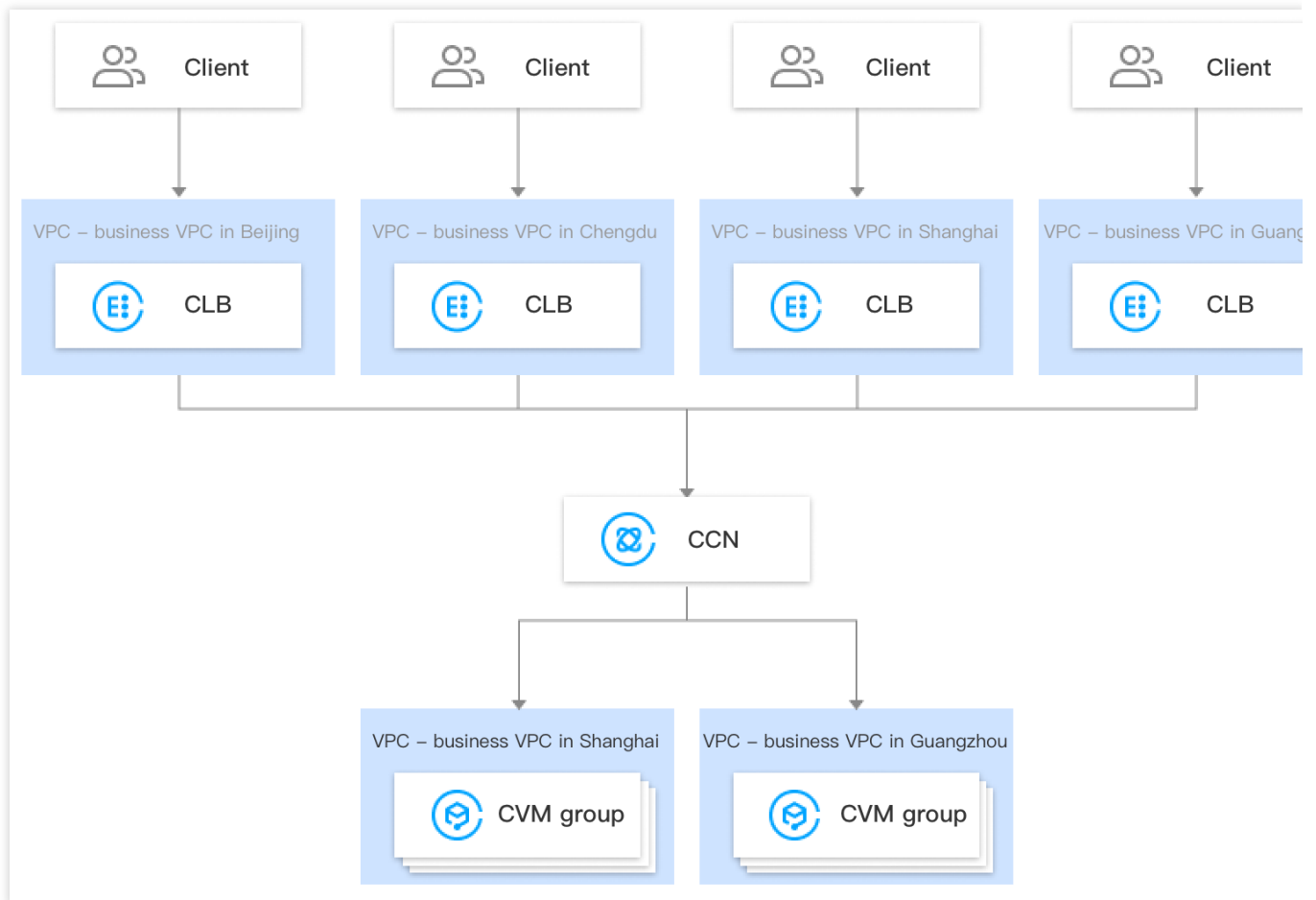
Fitur ini hanya tersedia untuk akun tagihan per IP. Untuk memeriksa tipe akun Anda, silakan lihat [Memeriksa Tipe Akun](#).

Pengikatan lintas wilayah 2.0 dan deployment cloud hibrida tidak mendukung [Izinkan Lalu Lintas secara Default di grup keamanan](#), yang mengharuskan Anda mengizinkan IP klien dan port layanan di server asli.

Kasus Penggunaan

1. Fitur pengikatan lintas wilayah dapat memenuhi kebutuhan skenario game P2P tempat server yang sama digunakan bersama oleh pemain-pemain dari wilayah berbeda. Contohnya, jika kluster server asli Anda di-deploy di Guangzhou, Anda bisa membuat instance CLB di Shanghai dan Beijing dan mengikatnya ke kluster server asli yang sama di Guangzhou untuk mencapai akselerasi dan konvergensi lalu lintas game, memastikan kualitas transfer data dan mengurangi latensinya.

2. Fitur ini bisa memastikan kualitas transfer dan konsistensi data dalam transaksi bisnis penting, memenuhi persyaratan ketat industri keuangan dan skenario pembayaran.



Prasyarat

1. Kirim permohonan untuk kelayakan pengujian beta. Untuk pengikatan lintas wilayah di Tiongkok daratan, silakan kirimkan tiket untuk mendaftar. Untuk pengikatan lintas wilayah di luar Tiongkok daratan, silakan [hubungi perwakilan Tencent Cloud Anda](#).
2. Buat instance CLB. Untuk informasi selengkapnya, silakan lihat [Membuat Instance CLB](#).
3. Buat instance CCN. Untuk informasi selengkapnya, silakan lihat [Membuat Instance CCN](#).
4. Asosiasikan VPC target dengan instance CCN yang dibuat. Untuk informasi selengkapnya, silakan lihat [Mengasosiasikan Instance Jaringan](#).

Petunjuk Operasi

1. Masuk ke [Konsol CLB](#).
2. Di halaman **Instance Management** (Manajemen Instance), klik ID instance CLB target.
3. Pada bagian **Real Server** (Server Asli) di tab **Basic Info** (Info Dasar), klik **Configure** (Konfigurasi) untuk mengikat IP pribadi VPC lainnya.

lb-kyqjxnhg

Basic Info | Listener Management | Redirection Configurations | Monitoring | Security Group

Basic Info

| | |
|-------------------|------------------|
| Name | |
| ID | |
| Status | Normal |
| VIP | |
| Instance Type | Public Network |
| Region | Guangzhou |
| Availability Zone | Guangzhou Zone 4 |
| ISP | BGP |
| Network | |

Access Log

The "Store Logs in COS" feature will be deactivated in all regions. For more information, please see [Deactivation](#).

Cloud Log Service ⓘ Not Enabled

Store Logs in COS ⓘ The "Store Logs in COS" feature will be deactivated in all regions. For more information, please see [Deactivation](#).

Real Server

Tencent Cloud CLB help you achieve cross-region connection. Only one policy can be selected:

- Cross-region Binding: A CLB instance can be bound with CVMs of a VPC across regions. [Configure](#)
- Binding IPs of other VPCs: A CLB instance can be bound with IPs of multiple VPCs and IDCs. [Configure](#)

4. Klik **Submit** (Kirim) di kotak pop-up.

Enable Binding IP of Other VPCs ✕

After enabling it, a CLB instance can be bound with private IPs of other VPCs.

Submit **Close**

5. Pada bagian **Real Server** (Server Nyata) di tab **Basic Info** (Info Dasar), Anda bisa melihat bahwa **Binding IP of Other VPCs** (Mengikat IP VPC Lain) diaktifkan, yang menunjukkan bahwa IP in-cloud bisa diikat padanya.

Real Server

Tencent Cloud CLB help you achieve cross-region connection. Only one policy can be selected:

- Cross-region Binding: A CLB instance can be bound with CVMs of a VPC across regions. [Configure](#)
- Binding IPs of other VPCs: A CLB instance can be bound with IPs of multiple VPCs and IDCs. [Configure](#)

Binding IP of Other VPCs

[Add SNAT IP](#)

6. Di halaman detail instance, buka tab **Listener Management** (Manajemen Pendengar), dan ikat server asli ke instance CLB di bagian konfigurasi pendengar. Untuk informasi selengkapnya, silakan lihat [Mengelola Server Asli](#).
7. Di kotak pop-up, pilih **Other VPC** (VPC Lain), klik **CVM**, pilih satu atau beberapa instance CVM target, masukkan port dan bobot penerusan, dan klik **Confirm** (Konfirmasi). Untuk informasi selengkapnya mengenai port, silakan lihat [Port Umum Server](#).
8. Kini di bagian **Bound Real Servers** (Server Asli Terikat), Anda bisa melihat instance CVM terikat dari wilayah lain.

Deployment Cloud Hibrida

Waktu update terbaru : 2024-01-04 20:53:33

Dalam skenario deployment cloud hibrida, Anda bisa langsung mengikat instance CLB ke IP di IDC lokal luar cloud untuk mengikatnya ke server asli di seluruh VPC dan IDC.

Fitur ini saat ini dalam versi beta. Jika Anda ingin menggunakannya, untuk pengikatan lintas wilayah di luar Tiongkok daratan, silakan [hubungi perwakilan Tencent Cloud Anda](#).

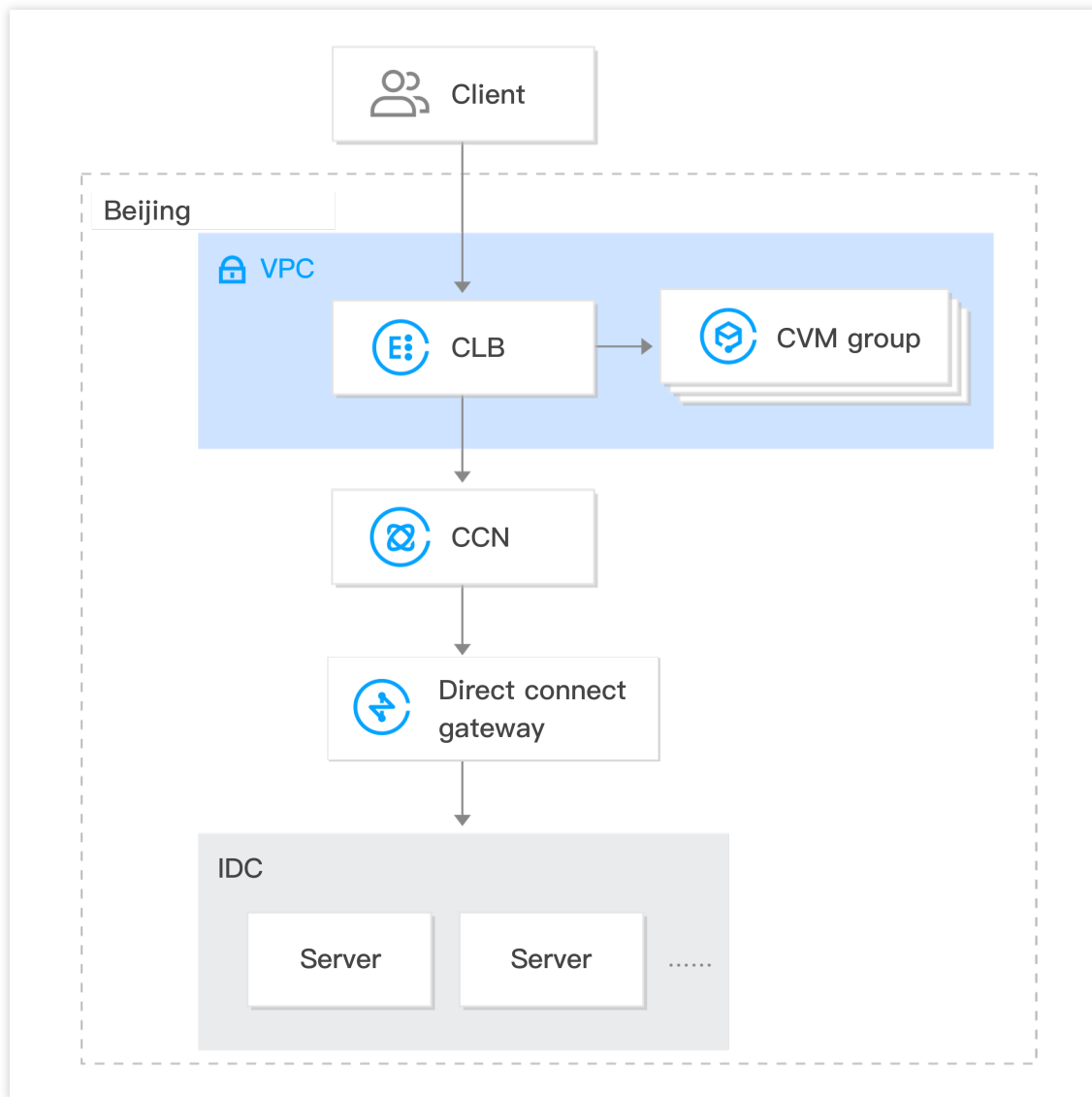
Keunggulan Solusi

Cloud hibrida bisa dibangun dengan cepat untuk menghubungkan lingkungan di dalam dan luar cloud dengan lancar. CLB bisa meneruskan permintaan ke instance CVM di VPC in-cloud dan IDC off-cloud sekaligus.

Kemampuan akses jaringan publik kualitas tinggi Tencent Cloud bisa digunakan kembali.

Fitur CLB yang kaya seperti akses lapisan 4/7, pemeriksaan kesehatan, dan persistensi sesi bisa digunakan kembali.

Jaringan pribadi bisa saling terhubung melalui [CCN](#), mendukung perutean mendetail untuk menjamin kualitas, dan mendukung diversifikasi harga bertingkat untuk mengurangi biaya.



Batas

Saat ini tidak mendukung pengikatan instance CVM lintas jaringan untuk instance CLB klasik.

Fitur ini hanya tersedia untuk akun tagihan per IP. Untuk memeriksa tipe akun Anda, silakan lihat [Memeriksa Tipe Akun](#).

Pengikatan lintas wilayah 2.0 dan deployment cloud hibrida tidak mendukung [Izinkan Lalu Lintas secara Default di grup keamanan](#), yang mengharuskan Anda mengizinkan IP klien dan port layanan di server asli.

Saat ini, fitur ini hanya didukung di Guangzhou, Shenzhen, Shanghai, Jinan, Hangzhou, Beijing, Tianjin, Chengdu, Chongqing, Hong Kong (Tiongkok), Singapore, dan Silicon Vally.

Pendengar TCP dan TCP SSL harus menggunakan TOA di server asli untuk memperoleh IP sumber. Untuk informasi selengkapnya, silakan lihat [Metode Pemuatan Modul TOA](#).

Pendengar HTTP dan HTTPS harus menggunakan `X-Forwarded-For` (XFF) untuk memperoleh IP sumber.

Pendengar UDP tidak bisa memperoleh IP sumber.

Prasyarat

- 1.Kirim permohonan untuk kelayakan pengujian beta.Untuk pengikatan lintas wilayah di Tiongkok daratan, silakan kirimkan tiket untuk mendaftar.Untuk pengikatan lintas wilayah di luar Tiongkok daratan, silakan [hubungi perwakilan Tencent Cloud Anda](#).
- 2.Buat instance CLB.Untuk informasi selengkapnya, silakan lihat [Membuat Instance CLB](#).
- 3.Buat instance CCN.Untuk informasi selengkapnya, silakan lihat [Membuat Instance CCN](#).
- 4.Asosiasikan Direct Connect gateway yang diasosiasikan dengan IDC dan VPC target dengan instance CCN yang dibuat.Untuk informasi selengkapnya, silakan lihat [Mengasosiasikan Instance Jaringan](#).

Petunjuk Operasi

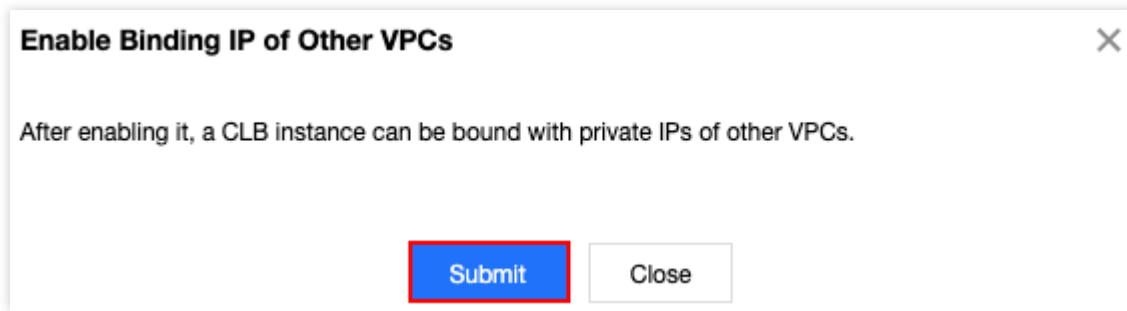
- 1.Masuk ke [Konsol CLB](#).
- 2.Di halaman **Instance Management** (Manajemen Instance), klik ID instance CLB target.
- 3.Pada bagian **Real Server** (Server Asli) di tab **Basic Info** (Info Dasar), klik **Configure** (Konfigurasi) untuk mengikat IP pribadi VPC lainnya.

The screenshot shows the Tencent Cloud console interface for a Cloud Load Balancer (CLB) instance. The instance name is 'lb-kyqjxnhg'. The 'Basic Info' tab is selected, displaying the following details:

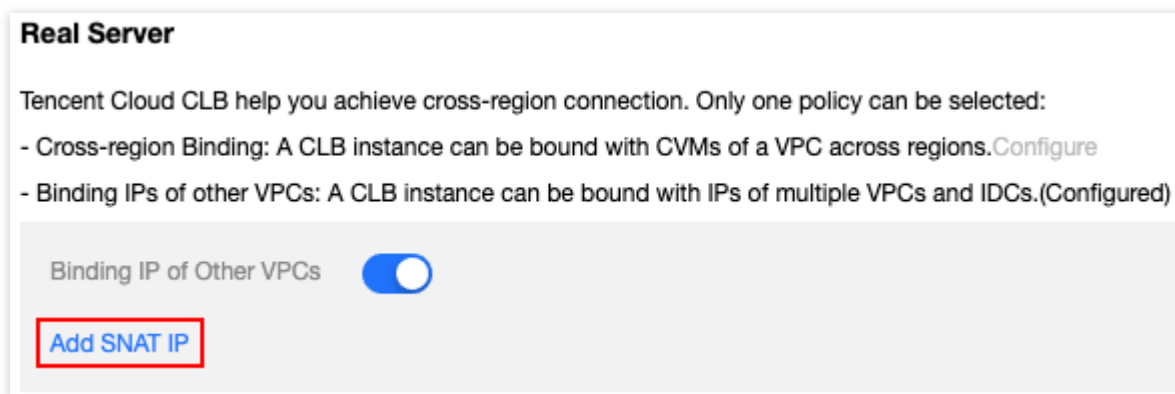
| Field | Value |
|-------------------|------------------|
| Name | [Redacted] |
| ID | [Redacted] |
| Status | Normal |
| VIP | [Redacted] |
| Instance Type | Public Network |
| Region | Guangzhou |
| Availability Zone | Guangzhou Zone 4 |
| ISP | BGP |
| Network | [Redacted] |

On the right side, the 'Access Log' section shows that 'Cloud Log Service' is 'Not Enabled' and 'Store Logs in COS' is also 'Not Enabled'. Below this, the 'Real Server' section provides information about cross-region binding and binding other VPCs.

- 4.Klik **Submit** (Kirim) di kotak pop-up.



5. Pada bagian **Real Server** (Server Asli) di tab **Basic Info** (Info Dasar), klik **Add SNAT IP** (Tambahkan IP SNAT).



6. Pada kotak pop-up, pilih **Subnet**, klik **Add** (Tambahkan) untuk menetapkan IP, dan klik **Save** (Simpan).

Konfigurasi Grup Keamanan pada Server Asli

Waktu update terbaru : 2024-01-04 20:53:33

Ikhtisar Grup Keamanan CVM

[Grup keamanan](#) bisa digunakan untuk mengakses kendali untuk server asli instance CLB, yang berperan sebagai firewall.

Anda bisa mengasosiasikan satu grup keamanan atau lebih dengan satu server asli dan kemudian menambahkan satu aturan atau lebih pada setiap grup keamanan untuk mengendalikan izin akses lalu lintas dari berbagai server. Anda bisa memodifikasi aturan grup keamanan kapan pun, dan aturan baru akan berlaku secara otomatis pada semua instance yang berkaitan dengan grup keamanan. Untuk informasi selengkapnya, silakan lihat [Panduan Pengoperasian Grup Keamanan](#). Di lingkungan [VPC](#), Anda juga bisa menggunakan [ACL Jaringan](#) untuk mengakses kendali.

Deskripsi Konfigurasi Grup Keamanan CVM

IP klien dan port keamanan harus dibuka ke internet di grup keamanan CVM.

Jika Anda ingin menggunakan CLB untuk meneruskan lalu lintas bisnis ke CVM, untuk memastikan pemeriksaan kesehatan yang efektif, grup keamanan CVM harus dikonfigurasi sebagai berikut:

1. CLB jaringan publik: Anda harus membuka VIP CLB ke internet di grup keamanan CVM backend, agar CLB bisa menggunakan VIP untuk mendeteksi status kesehatan CVM backend.

2. CLB jaringan pribadi:

Untuk CLB jaringan pribadi (sebelumnya "CLB Aplikasi jaringan pribadi"), jika instance CLB Anda dalam VPC, VIP CLB harus dibuka ke internet di grup keamanan CVM backend untuk pemeriksaan kesehatan; jika instance CLB Anda dalam jaringan dasar, konfigurasi tambahan tidak dibutuhkan karena IP pemeriksaan kesehatan dibuka ke internet secara default.

Untuk CLB klasik jaringan pribadi, jika instance CLB Anda dibuat sebelum 5 Desember 2016 dan dalam VPC, VIP CLB harus dibuka ke internet (untuk pemeriksaan kesehatan) di grup keamanan CVM backend; jika tidak, konfigurasi tidak dibutuhkan.

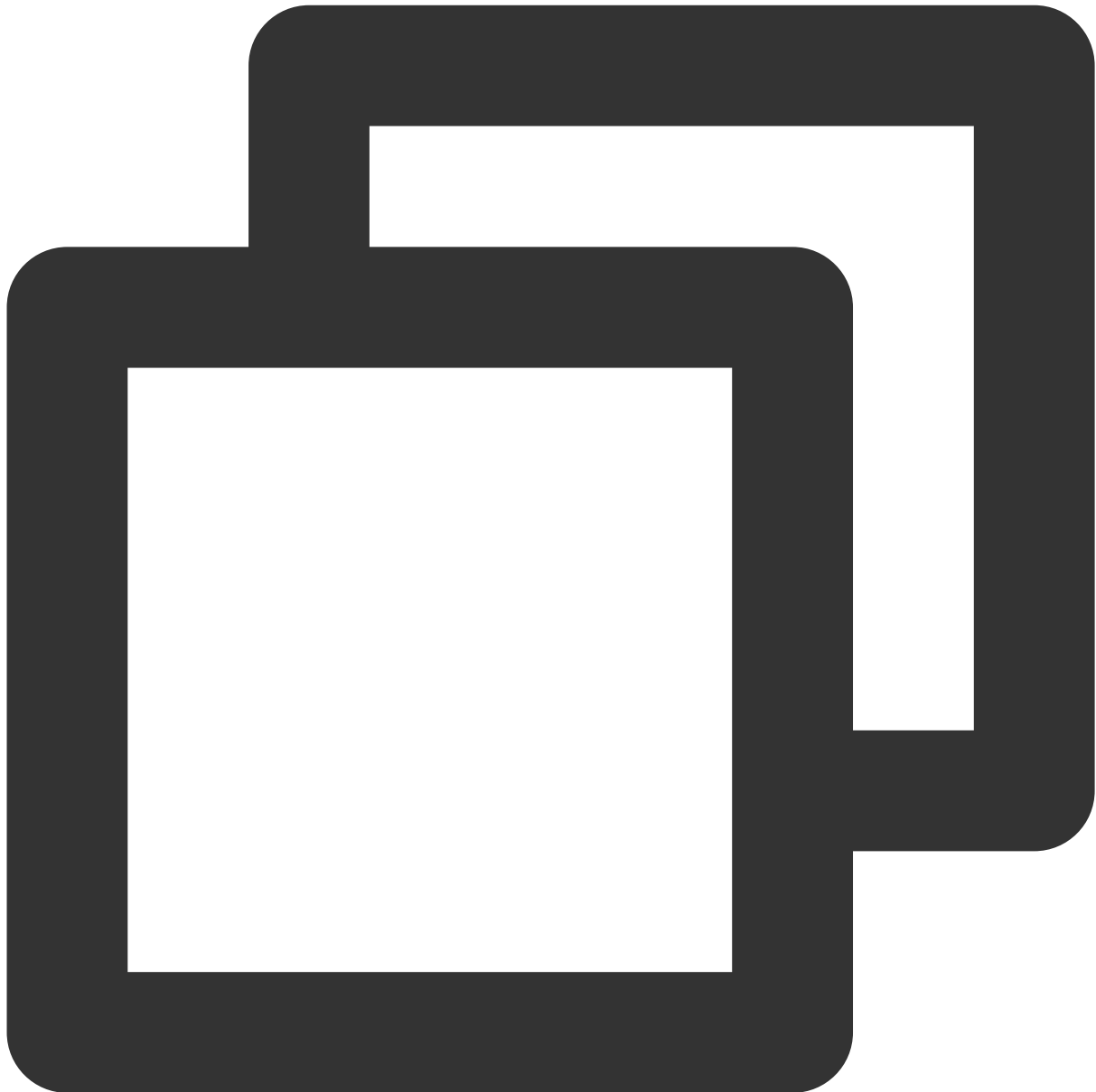
Sampel Konfigurasi Grup Keamanan CVM

Sampel berikut ini menunjukkan cara mengonfigurasi grup keamanan CVM saat mengakses CVM melalui CLB. Jika Anda juga sudah mengonfigurasi grup keamanan di CLB, silakan lihat [Mengonfigurasi Grup Keamanan CLB](#)

untuk informasi selengkapnya tentang cara mengonfigurasi aturan grup keamanan CLB.

Skenario aplikasi 1:

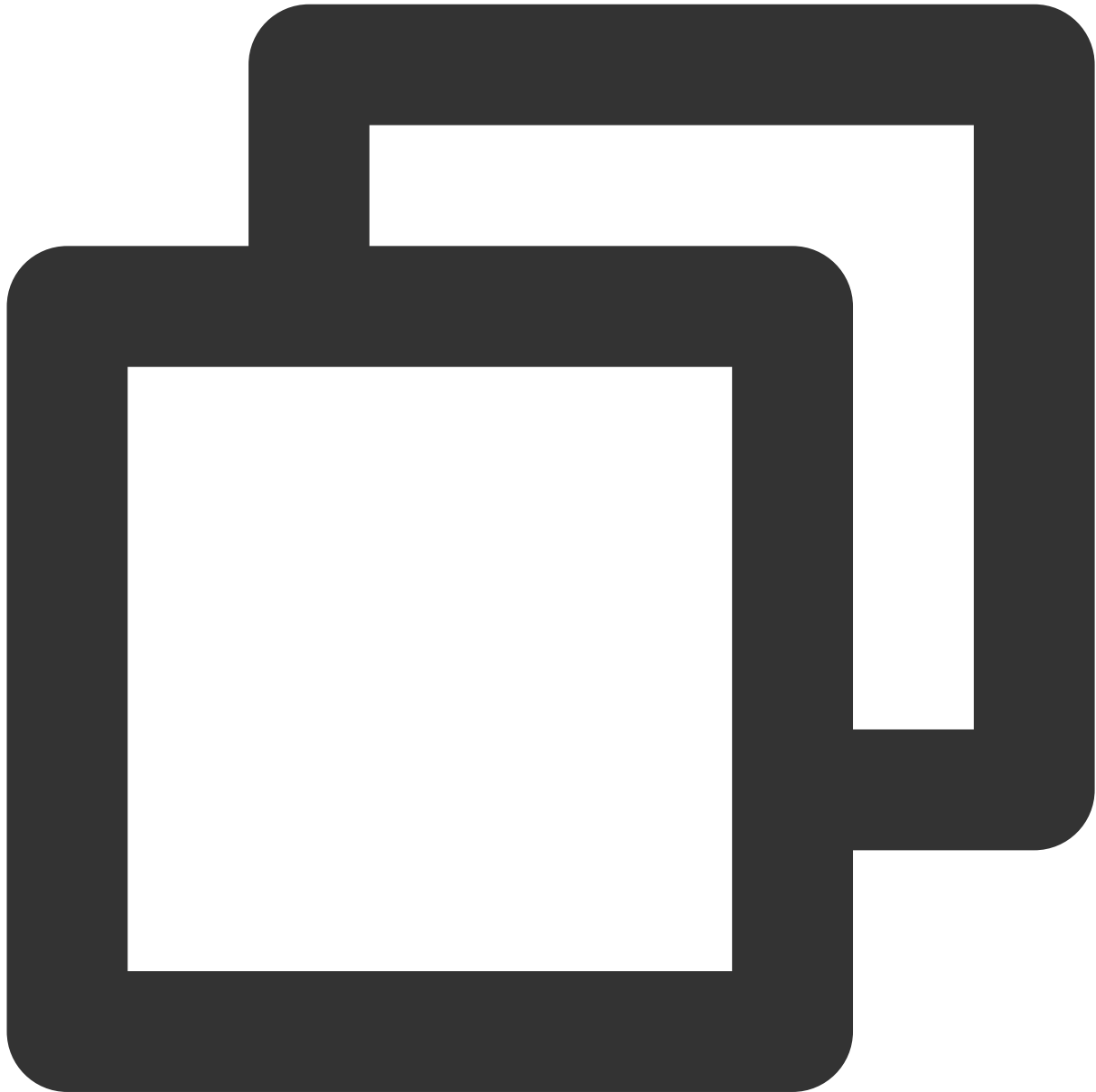
Jika instance CLB jaringan publik dikonfigurasi dengan pendengar TCP:80, port server aslinya adalah 8080, dan Anda hanya ingin IP Klien tertentu (IP ClientA dan IP ClientB) yang bisa mengakses instance CLB, konfigurasi aturan masuk grup keamanan server asli seperti yang berikut ini:



```
IP ClientA + 8080 izinkan
IP ClientB + 8080 izinkan
VIP CLB    + 8080 izinkan
0.0.0.0/0  + 8080 turunkan
```

Skenario aplikasi 2:

Jika instance CLB jaringan publik dikonfigurasi dengan pendengar HTTP:80, port server aslinya adalah 8080, dan Anda ingin semua IP Klien bisa mengakses instance CLB, konfigurasi aturan masuk grup keamanan server asli seperti yang berikut ini:



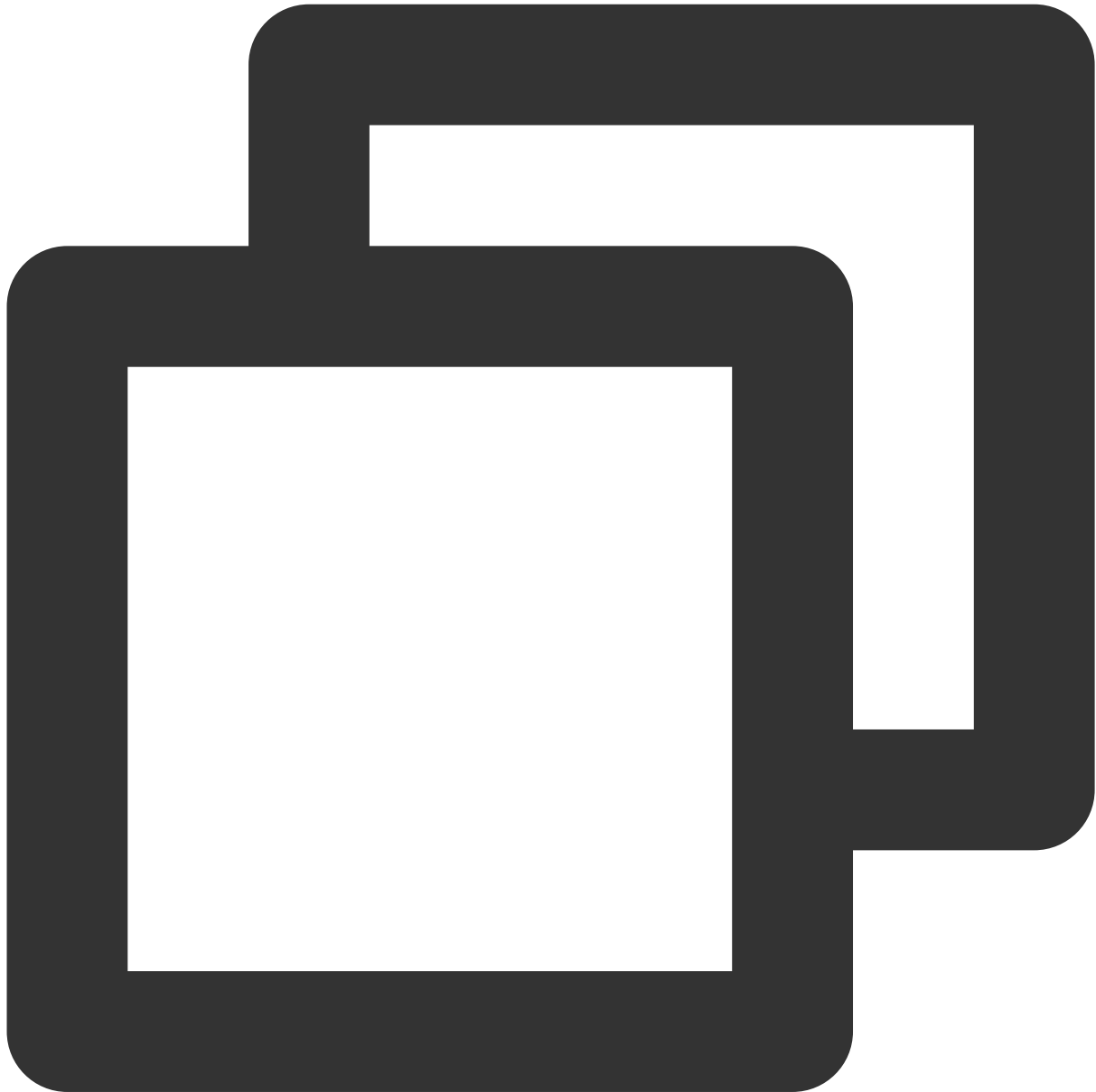
```
0.0.0.0/0 + 8080 izinkan
```

Skenario aplikasi 3:

Untuk instance CLB jaringan pribadi (sebelumnya "CLB Aplikasi jaringan pribadi"), tipe jaringannya VPC, grup keamanan CVM perlu membuka IP VIP CLB ke internet untuk pemeriksaan kesehatan, instance CLB ini

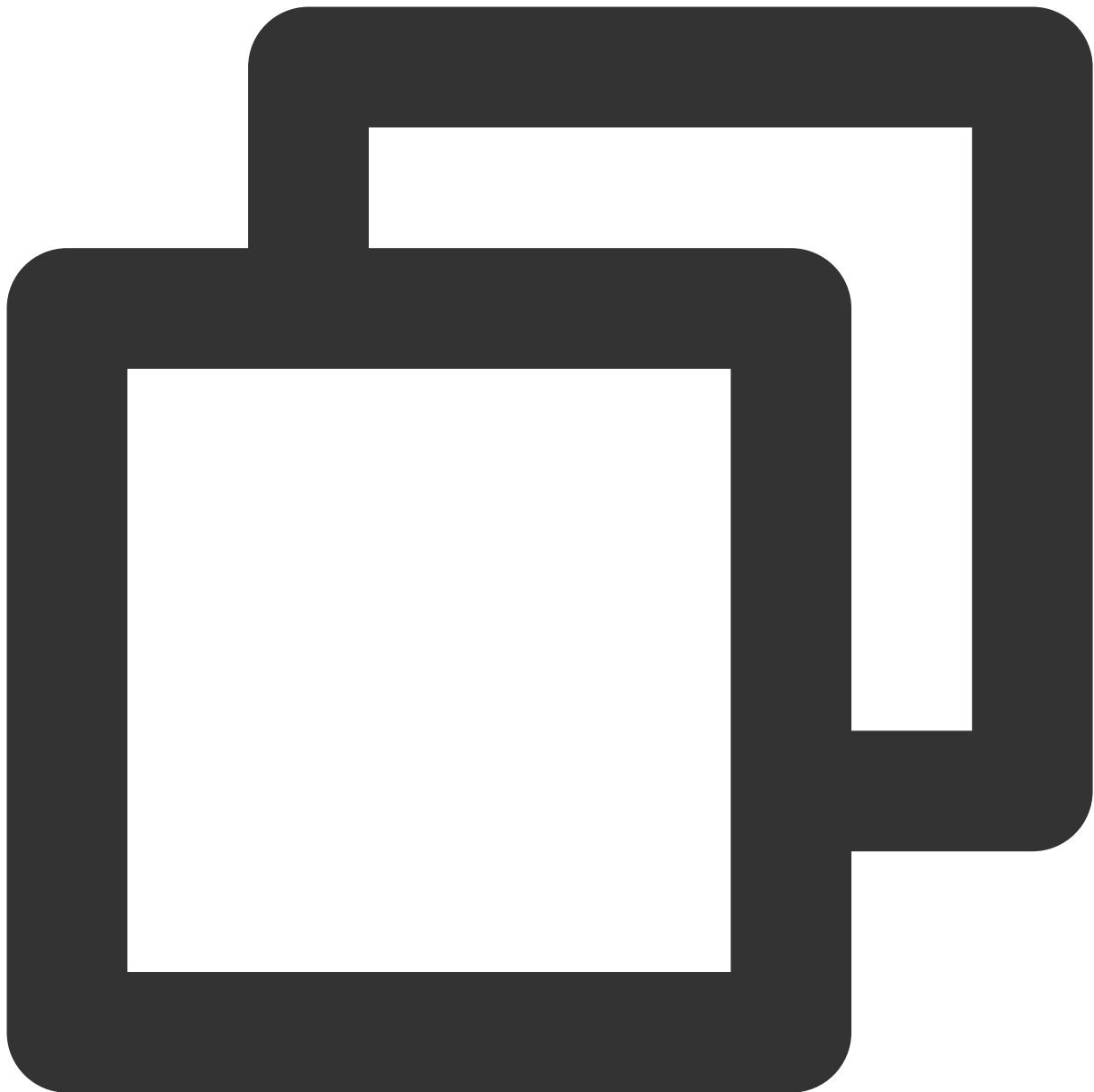
dikonfigurasi dengan pendengar TCP:80, port server aslinya adalah 8080, dan Anda ingin IP Klien tertentu (IP ClientA dan IP ClientB) untuk mengakses VIP CLB dan ingin IP Klien untuk mengakses server asli yang terikat ke instance CLB saja, maka:

a. Konfigurasi aturan masuk untuk grup keamanan server asli seperti yang berikut ini:



```
IP ClientA + 8080 izinkan  
IP ClientB + 8080 izinkan  
VIP CLB + 8080 izinkan  
0.0.0.0/0 + 8080 turunkan
```

b. Konfigurasi aturan keluar untuk grup keamanan server klien seperti yang berikut ini:



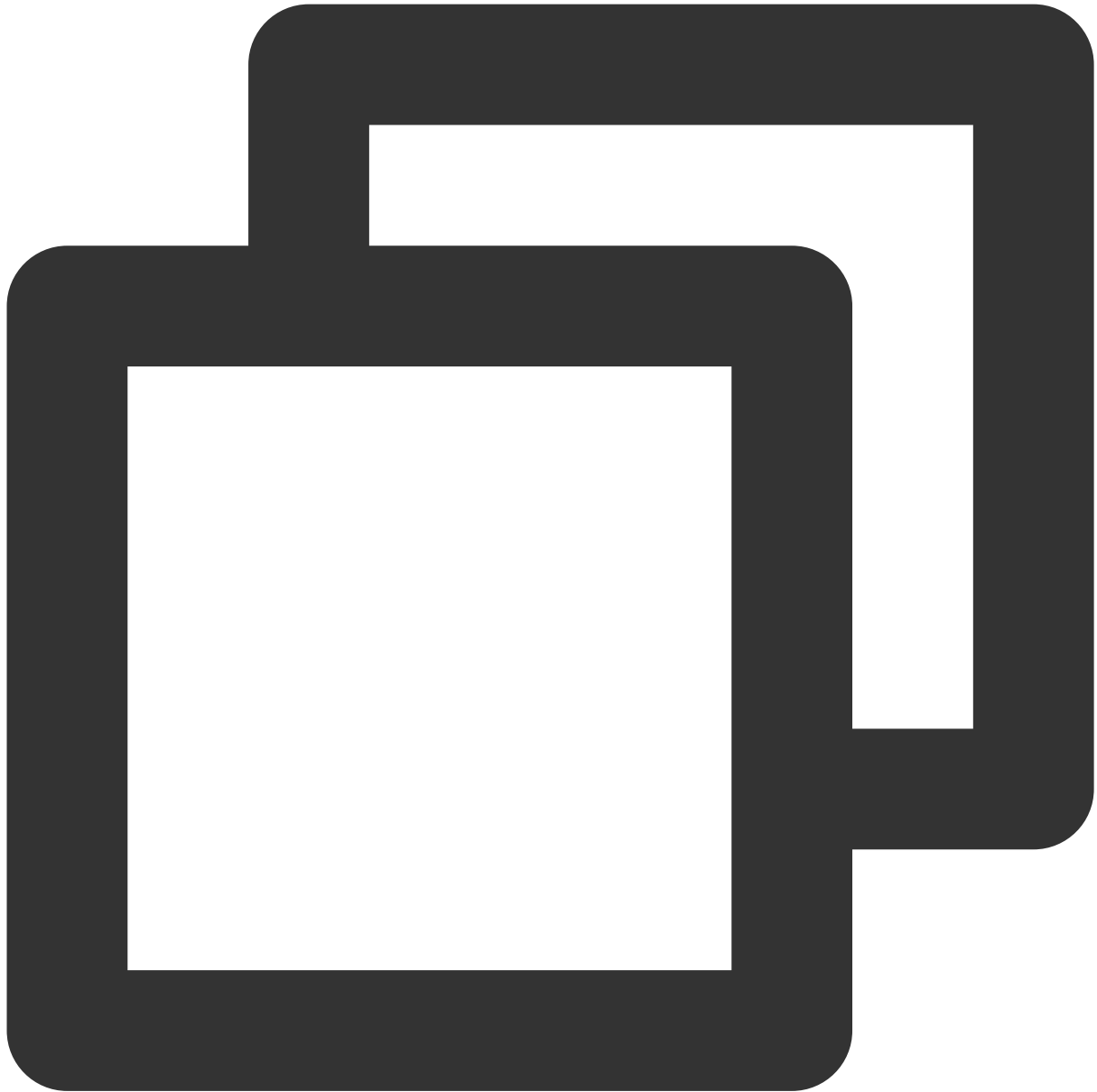
```
VIP CLB      + 8080 izinkan  
0.0.0.0/0    + 8080 turunkan
```

Skenario aplikasi 4:

Untuk instance CLB jaringan pribadi (misalnya, instance CLB VPC yang dibeli setelah 5 Desember 2016), grup keamanan CVM hanya perlu membuka IP Klien ke internet (tidak perlu membuka VIP CLB, dan IP pemeriksaan kesehatan terbuka secara default), instance CLB ini dikonfigurasi dengan pendengar TCP:80, port server aslinya adalah 8080, dan Anda ingin IP Klien tertentu (IP ClientA dan IP ClientB) untuk mengakses VIP CLB dan ingin IP

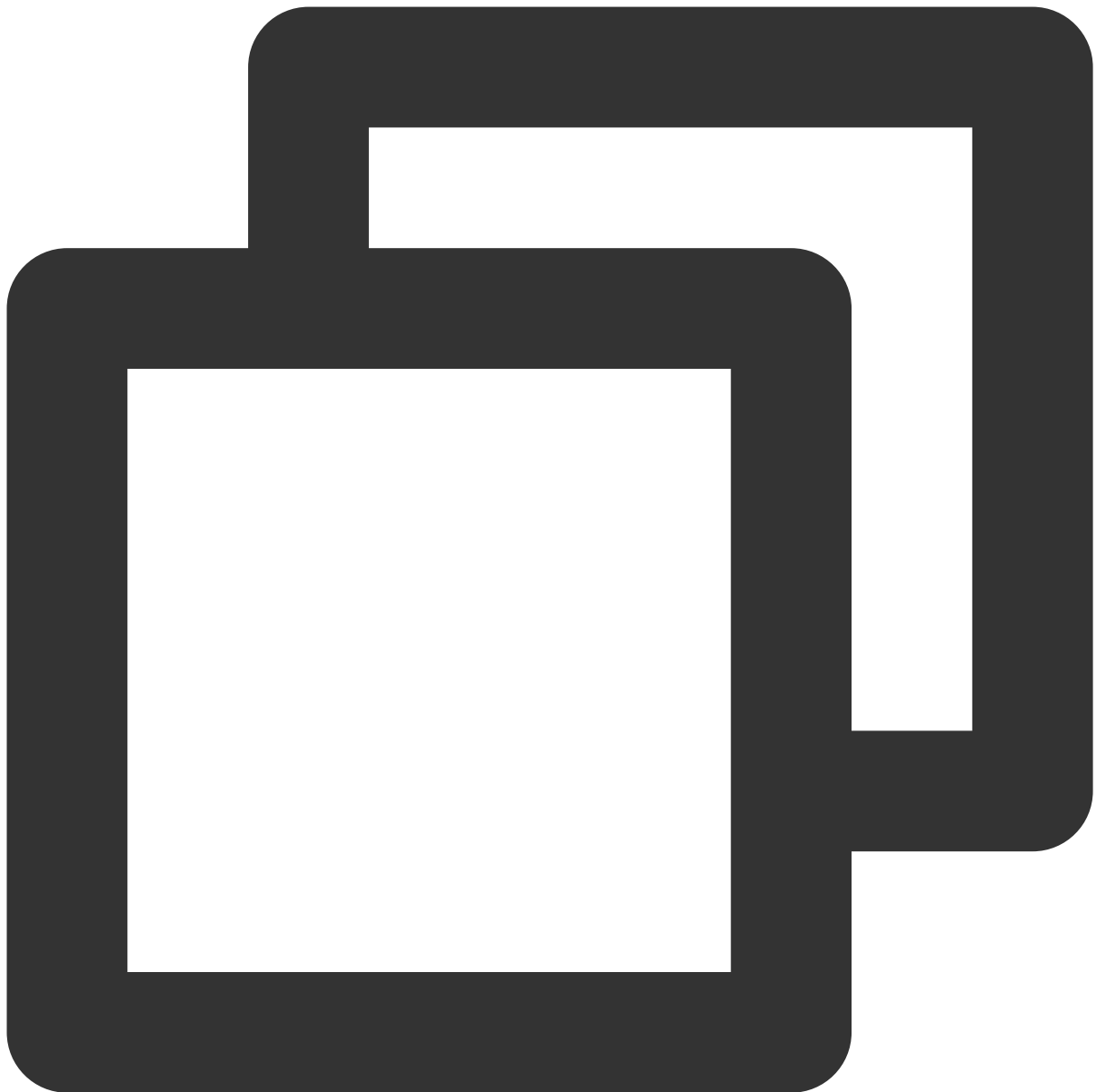
Klien untuk mengakses server asli yang terikat ke instance CLB saja, maka:

a. Konfigurasi aturan masuk untuk grup keamanan server asli seperti yang berikut ini:



```
IP ClientA + 8080 izinkan  
IP ClientB + 8080 izinkan  
0.0.0.0/0 + 8080 turunkan
```

b. Konfigurasi aturan keluar untuk grup keamanan server klien seperti yang berikut ini:



```
VIP CLB      + 8080 izinkan  
0.0.0.0/0    + 8080 turunkan
```

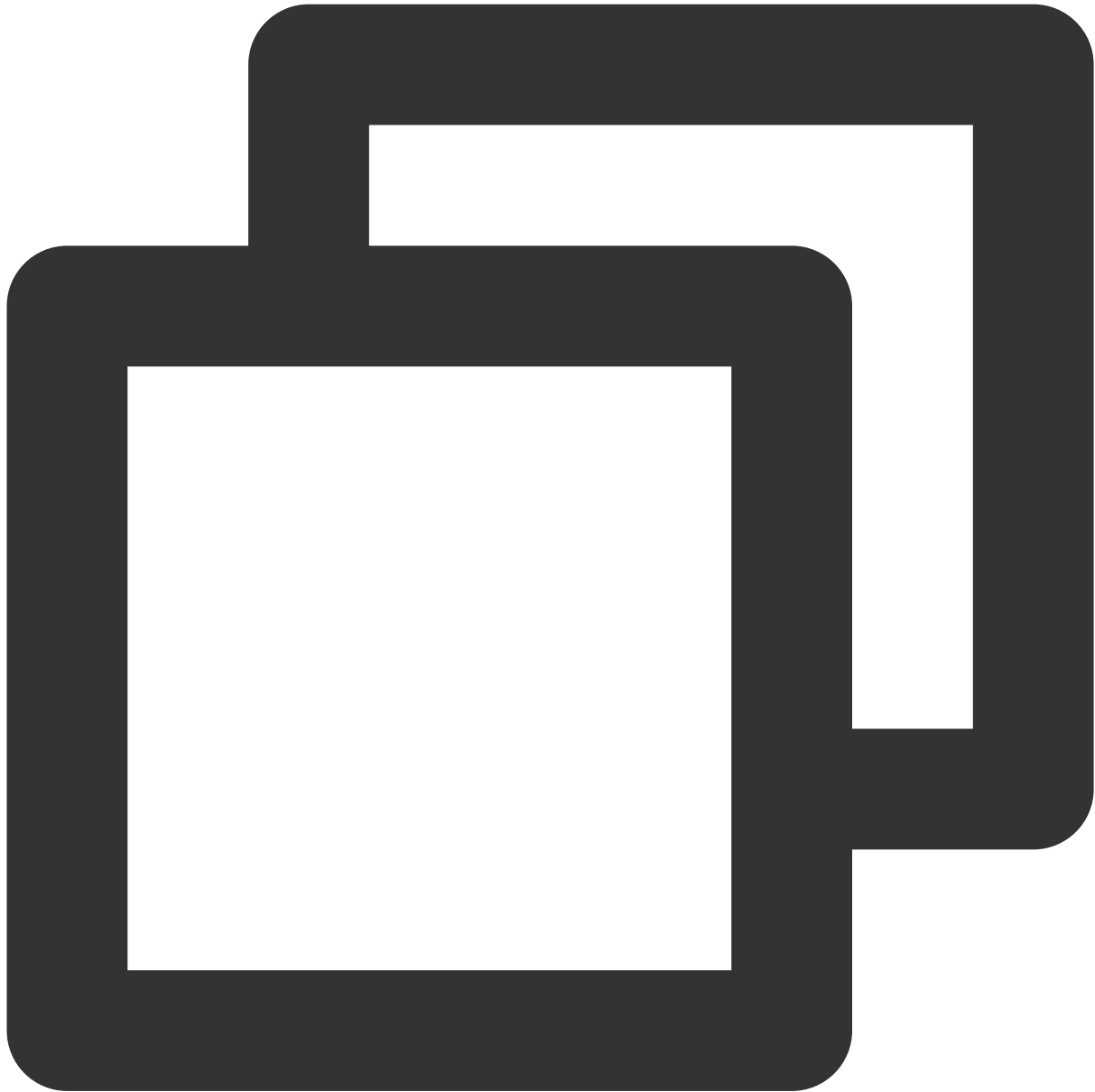
Skenario aplikasi 5: daftar hitam

Jika Anda perlu mengonfigurasi daftar hitam untuk beberapa IP klien untuk menolak permintaan akses mereka, Anda bisa mengonfigurasi grup keamanan yang berkaitan dengan layanan Tencent Cloud. Aturan grup keamanan perlu dikonfigurasi seperti yang berikut ini:

Tambahkan IP klien dan port yang akan ditolak ke grup keamanan dan pilih opsi tersebut di kolom "Kebijakan" untuk menolak akses dari IP ini.

Tambahkan aturan grup keamanan lainnya setelah menyelesaikan konfigurasi di atas untuk mengizinkan permintaan akses ke port dari semua IP secara default.

Setelah konfigurasi selesai, aturan grup keamanan adalah sebagai berikut:



```
IP clientA + port turunkan  
IP clientB + port turunkan  
0.0.0.0/0 + port terima
```

Keterangan :

Langkah-langkah konfigurasi di atas harus dilakukan **in a correct order** (sesuai urutan); jika tidak, konfigurasi daftar hitam tidak bisa berlaku.

Grup keamanan bersifat stateful; oleh karena itu, konfigurasi di atas digunakan untuk **inbound rules** (aturan masuk), sementara aturan keluar tidak membutuhkan konfigurasi khusus.

Panduan Pengoperasian Grup Keamanan CVM

Mengelola grup keamanan server asli di konsol

1. Masuk ke [Konsol CLB](#) dan klik ID instance CLB terkait untuk masuk ke halaman detail CLB.
2. Di halaman CVM, klik ID server asli terkait untuk masuk ke halaman detail instance CVM.
3. Klik tab **Security Group** (Grup Keamanan) untuk mengikat/melepas ikatan grup keamanan.

Mengelola grup keamanan server asli melalui API TencentCloud

Untuk informasi selengkapnya, silakan lihat [AssociateSecurityGroups](#) dan [DisassociateSecurityGroups](#).

Pemeriksaan Kesehatan

Ikhtisar Pemeriksaan kesehatan

Waktu update terbaru : 2024-01-04 20:53:33

Instance CLB menentukan ketersediaan server asli melalui pemeriksaan kesehatan sehingga bisnis frontend tidak akan terkena dampak pengecualian server asli dan meningkatkan ketersediaan bisnis secara umum.

Jika pemeriksaan kesehatan diaktifkan, instance CLB akan selalu melakukan pemeriksaan kesehatan di instance CVM backend berapa pun beratnya (termasuk 0).

Jika instance CVM backend abnormal, instance CLB secara otomatis akan meneruskan permintaan baru ke instance CVM normal lainnya, dan bukan ke instance yang tidak sehat.

Setelah instance CVM abnormal pulih, instance akan digunakan dalam layanan CLB kembali dan menerima permintaan baru.

Jika semua server asli terdeteksi abnormal, permintaan akan diteruskan ke semua instance CVM backend.

Jika pemeriksaan kesehatan dinonaktifkan, instance CLB akan meneruskan lalu lintas ke semua server asli termasuk abnormal. Oleh karena itu, sebaiknya Anda mengaktifkan pemeriksaan kesehatan pada instance CLB untuk memeriksa server asli secara otomatis dan menghapus yang abnormal.

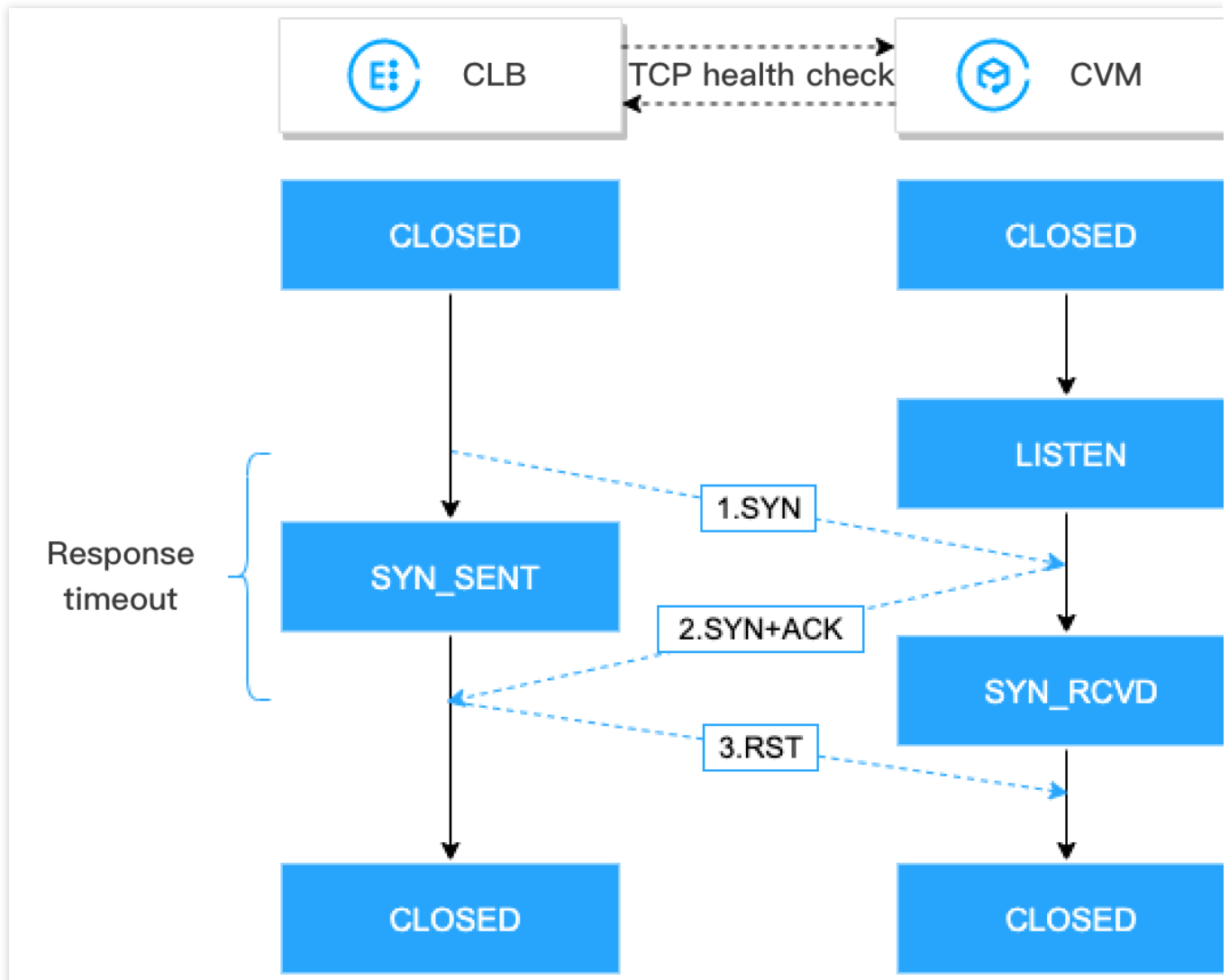
Status Pemeriksaan Kesehatan

Deskripsi status pemeriksaan kesehatan instance CVM backend yaitu sebagai berikut:

| Status | Deskripsi | Teruskan Lalu Lintas |
|---------------|---|--|
| Mendeteksi | Status instance CVM backend baru selama interval periode pemeriksaan \times batas sehat. Misalnya, anggap interval pemeriksaan 2 detik dan ambang batas sehat adalah 3 kali, instance CVM backend bertahan dalam status ini selama 6 detik. | Tidak. |
| Sehat | Kondisi server asli normal. | Ya. |
| Abnormal | Kondisi server asli abnormal. | Tidak. Menurut aturan pendengar lapisan 4 atau URL lapisan 7, jika instance CLB mendeteksi bahwa kondisi semua server asli abnormal, permintaan akan diteruskan ke semua server asli. |
| Dinonaktifkan | Pemeriksaan kesehatan dinonaktifkan. | Ya. |

Pemeriksaan Kesehatan TCP

Untuk pendengar TCP lapisan 4, Anda dapat mengonfigurasi pemeriksaan kesehatan TCP untuk melihat status instance CVM backend melalui paket SYN, misalnya, handshake tiga arah TCP. Selain itu, untuk mengatasinya, Anda dapat menyesuaikan permintaan dan mengembalikan konten protokol.



Mekanisme pemeriksaan kesehatan TCP yaitu sebagai berikut:

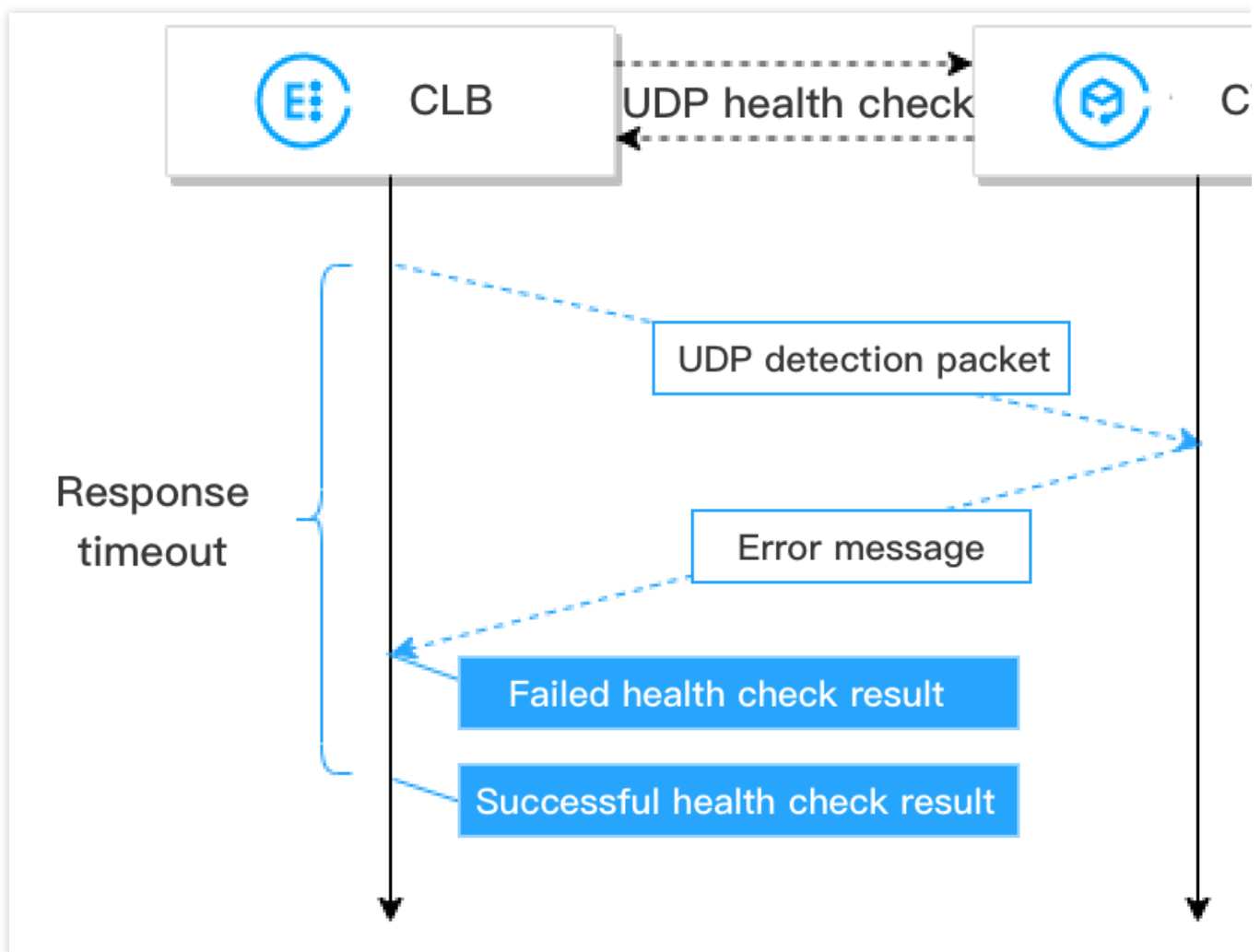
- 1.Instance CLB mengirimkan paket permintaan koneksi SYN ke (IP privat dan port pemeriksaan kesehatan dari) instance CVM backend.
- 2.Setelah menerima paket permintaan SYN, instance CVM backend akan mengembalikan paket respons SYN-ACK jika port mendengarkan secara normal.
- 3.Jika instance CLB menerima paket respons SYN-ACK yang dikembalikan dalam waktu habis respons, hal tersebut menunjukkan bahwa kondisi server asli normal dan hasil pemeriksaan kesehatan telah berhasil.Instance CLB akan

mengirimkan paket TCP Reset (RST) ke instance CVM backend untuk memutus koneksi TCP.

4. Jika instance CLB tidak menerima paket respons SYN-ACK yang dikembalikan dalam waktu habis respons, hal tersebut menunjukkan bahwa kondisi server asli abnormal dan hasil pemeriksaan kesehatan gagal. Instance CLB akan mengirimkan paket TCP Reset (RST) ke instance CVM backend untuk memutus koneksi TCP.

Pemeriksaan Kesehatan UDP

Untuk pendengar UDP lapisan 4, Anda dapat mengonfigurasi pemeriksaan kesehatan UDP untuk melihat status instance CVM backend dengan menjalankan perintah Ping dan mengirimkan paket deteksi UDP ke port pemeriksaan kesehatan. Selain itu, untuk mengatasinya, Anda dapat menyesuaikan permintaan dan mengembalikan konten protokol.



Mekanisme pemeriksaan kesehatan UDP yaitu sebagai berikut:

1. Instance CLB akan mengirimkan perintah Ping ke IP privat instance CVM backend.
2. Setelah itu, instance CLB akan mengirimkan paket deteksi UDP ke (IP privat dan port pemeriksaan kesehatan dari)

instance CVM backend.

3. Jika perintah Ping berhasil dan instance CVM backend tidak mengembalikan kesalahan `port XX tidak dapat dijangkau` dalam waktu habis respons, hal tersebut menunjukkan bahwa kondisi server asli normal dan hasil pemeriksaan kesehatan berhasil.

4. Jika perintah Ping gagal dan instance CVM backend mengembalikan kesalahan `port XX tidak dapat dijangkau` dalam waktu habis respons, hal tersebut menunjukkan bahwa kondisi server asli abnormal dan hasil pemeriksaan kesehatan gagal.

Perhatian :

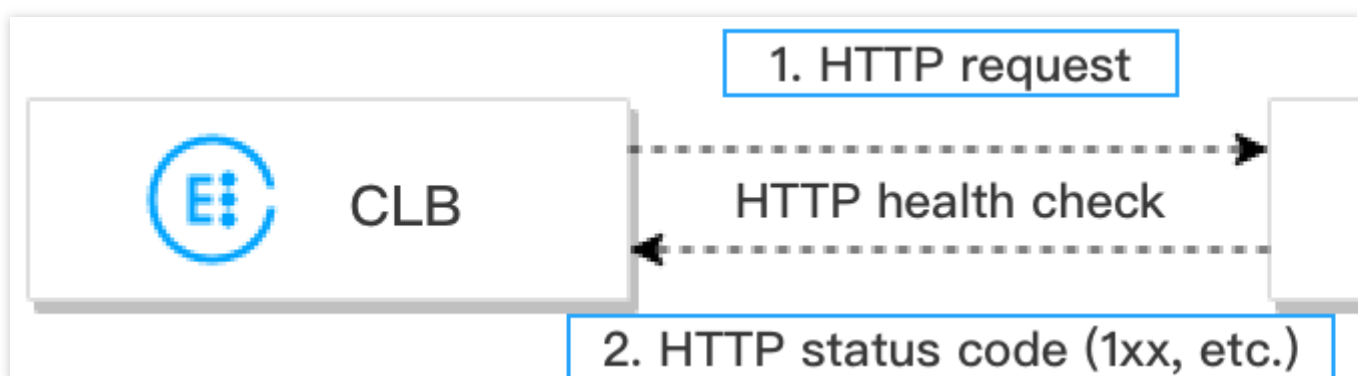
1. Pemeriksaan kesehatan UDP dilakukan berdasarkan ICMP sehingga instance CVM backend memerlukan izin agar dapat membalas paket ICMP (yaitu: perintah Ping didukung) dan paket "port tidak dapat dijangkau" ICMP (yaitu: port dapat dideteksi).

2. Jika server Linux digunakan sebagai instance CVM backend, kecepatan server untuk mengirimkan paket ICMP akan dibatasi selama konkurensi tinggi karena server Linux memiliki mekanisme pertahanan diri dari serangan ICMP. Dalam kasus ini, meskipun kondisi server asli abnormal, server tidak dapat mengembalikan kesalahan `port XX tidak dapat dijangkau` ke instance CLB. Kemudian, Instance CLB akan menentukan bahwa hasil pemeriksaan kesehatan berhasil sehingga status aktual server asli tidak dapat dikembalikan.

Solusi: Anda dapat mengonfigurasi pemeriksaan kesehatan UDP dengan input khusus dan string output. Dalam pemeriksaan kesehatan, string input khusus akan dikirimkan ke server asli, dan hasilnya akan ditetapkan sebagai berhasil hanya setelah instance CLB menerima string respons khusus. Metode ini dilakukan berdasarkan server asli, yang perlu memproses string input pemeriksaan kesehatan dan mengembalikan string output khusus.

Pemeriksaan Kesehatan HTTP

Untuk pendengar TCP lapisan 4 dan pendengar HTTP/HTTPS lapisan 7, Anda dapat mengonfigurasi pemeriksaan kesehatan HTTP untuk melihat status instance CVM backend dengan mengirimkan permintaan HTTP.



Mekanisme pemeriksaan kesehatan HTTP yaitu sebagai berikut:

1. Menurut konfigurasi pemeriksaan kesehatan, instance CLB dapat mengirimkan permintaan HTTP (nama domain

target telah ditentukan) ke (IP privat, port pemeriksaan kesehatan, dan jalur pemeriksaan dari) instance CVM backend.

2. Setelah menerima permintaan, instance CVM backend akan mengembalikan kode status HTTP yang sesuai.

3. Jika instance CLB menerima kode status HTTP yang dikembalikan dalam waktu habis respons dan kode status HTTP sesuai dengan yang ditetapkan, hal tersebut menunjukkan bahwa hasil pemeriksaan kesehatan berhasil, jika tidak, artinya gagal.

4. Jika instance CLB tidak menerima paket respons dari instance CVM backend dalam waktu habis respons, hal tersebut menunjukkan bahwa hasil pemeriksaan kesehatan gagal.

说明

Untuk pendengar HTTPS lapisan 7, jika HTTP dipilih sebagai protokol backend aturan penerusan pendengar HTTPS, pemeriksaan kesehatan HTTP akan dijalankan; jika HTTPS dipilih, pemeriksaan kesehatan HTTPS akan dijalankan.

Pemeriksaan kesehatan HTTPS pada dasarnya sama seperti [pemeriksaan kesehatan HTTP](#). Perbedaannya yaitu dalam pemeriksaan kesehatan HTTPS, permintaan HTTPS dikirimkan dan status instance CVM backend ditentukan oleh kode status HTTPS yang dikembalikan.

Periode Pemeriksaan Kesehatan

Mekanisme pemeriksaan kesehatan CLB meningkatkan ketersediaan bisnis, tetapi kegagalan pemeriksaan kesehatan yang berulang kali dapat menyebabkan penggantian server yang tidak diperlukan sehingga menurunkan ketersediaan sistem. Oleh karena itu, status pemeriksaan kesehatan hanya dapat diubah antara sehat dan abnormal jika diperoleh hasil yang sama dalam satu periode pemeriksaan kesehatan selama beberapa kali. Periode pemeriksaan kesehatan ditentukan berdasarkan faktor berikut:

| Konfigurasi Pemeriksaan Kesehatan | Catatan | Nilai Default |
|-----------------------------------|---|---------------|
| Waktu Habis Respons | Waktu habis respons maksimum pemeriksaan kesehatan. Jika server asli tidak dapat merespons dalam waktu habis, server akan dianggap dalam kondisi abnormal. Rentang nilai: 2-60 detik. | 2 detik |
| Interval pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300 detik. | 5 detik |
| Ambang batas tidak sehat | Jika hasil pemeriksaan kesehatan gagal sebanyak n (nilai dapat dikustomisasi) kali, instance CVM backend akan dianggap tidak sehat, dan konsol akan menampilkan status Abnormal. Rentang nilai: 2-10 kali. | 3 kali |
| | | |

| | | |
|--------------------|---|--------|
| Ambang batas sehat | Jika hasil pemeriksaan kesehatan berhasil sebanyak n (nilai dapat dikustomisasi) kali, instance CVM backend akan dianggap sehat, dan konsol akan menampilkan status Sehat. Rentang nilai: 2-10 kali. | 3 kali |
|--------------------|---|--------|

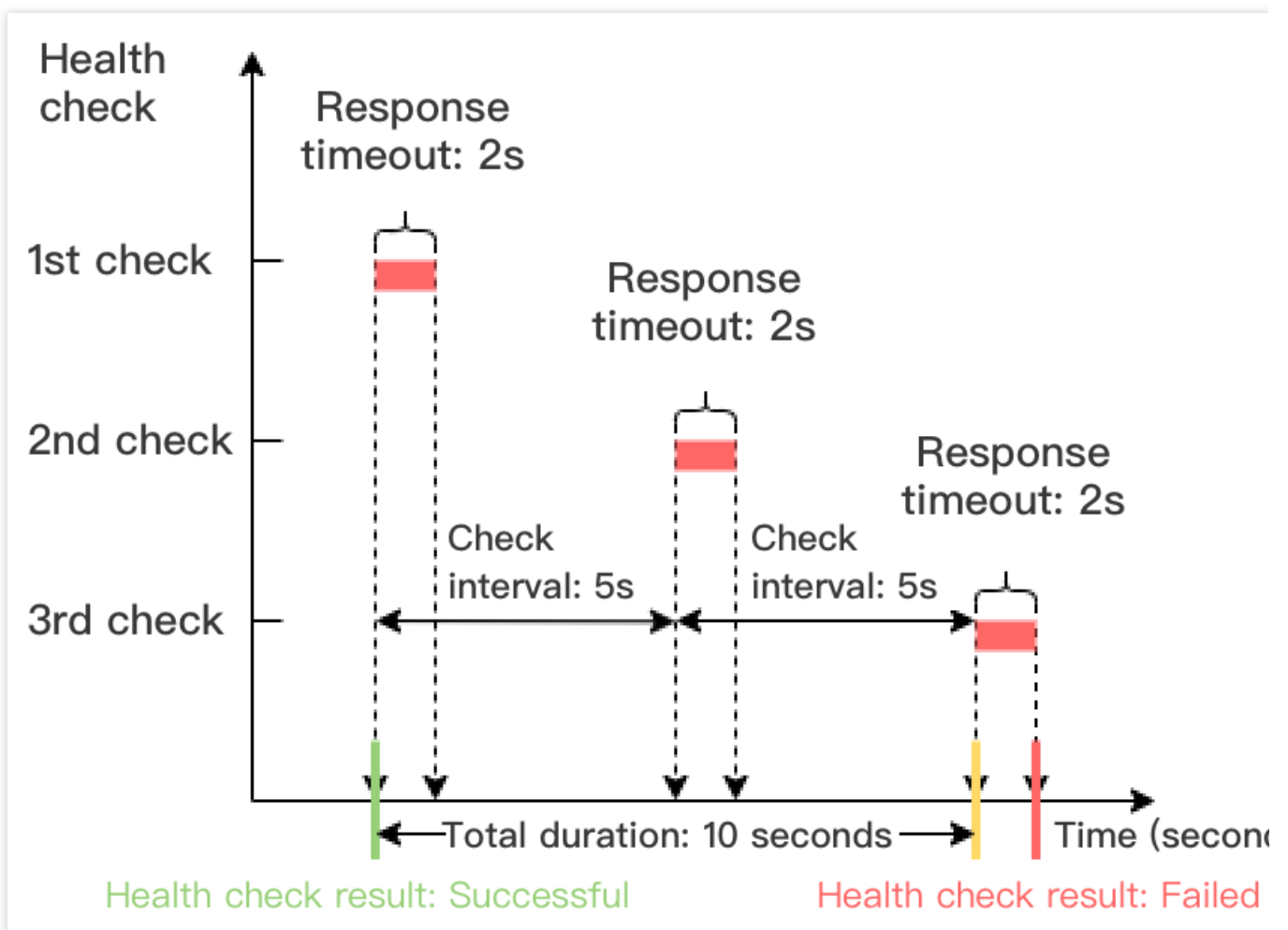
Penghitungan **lapisan 4 health check time window** (periode pemeriksaan kesehatan lapisan 4) yaitu sebagai berikut:

Keterangan :

Pemeriksaan kesehatan lapisan 4, terutama pemeriksaan kesehatan TCP atau UDP, interval waktu antara kedua pemeriksaan merupakan nilai tetap, apa pun hasilnya atau meskipun waktu respons habis.

Periode pemeriksaan kesehatan dengan hasil gagal = Interval pemeriksaan × (Ambang batas tidak sehat - 1)

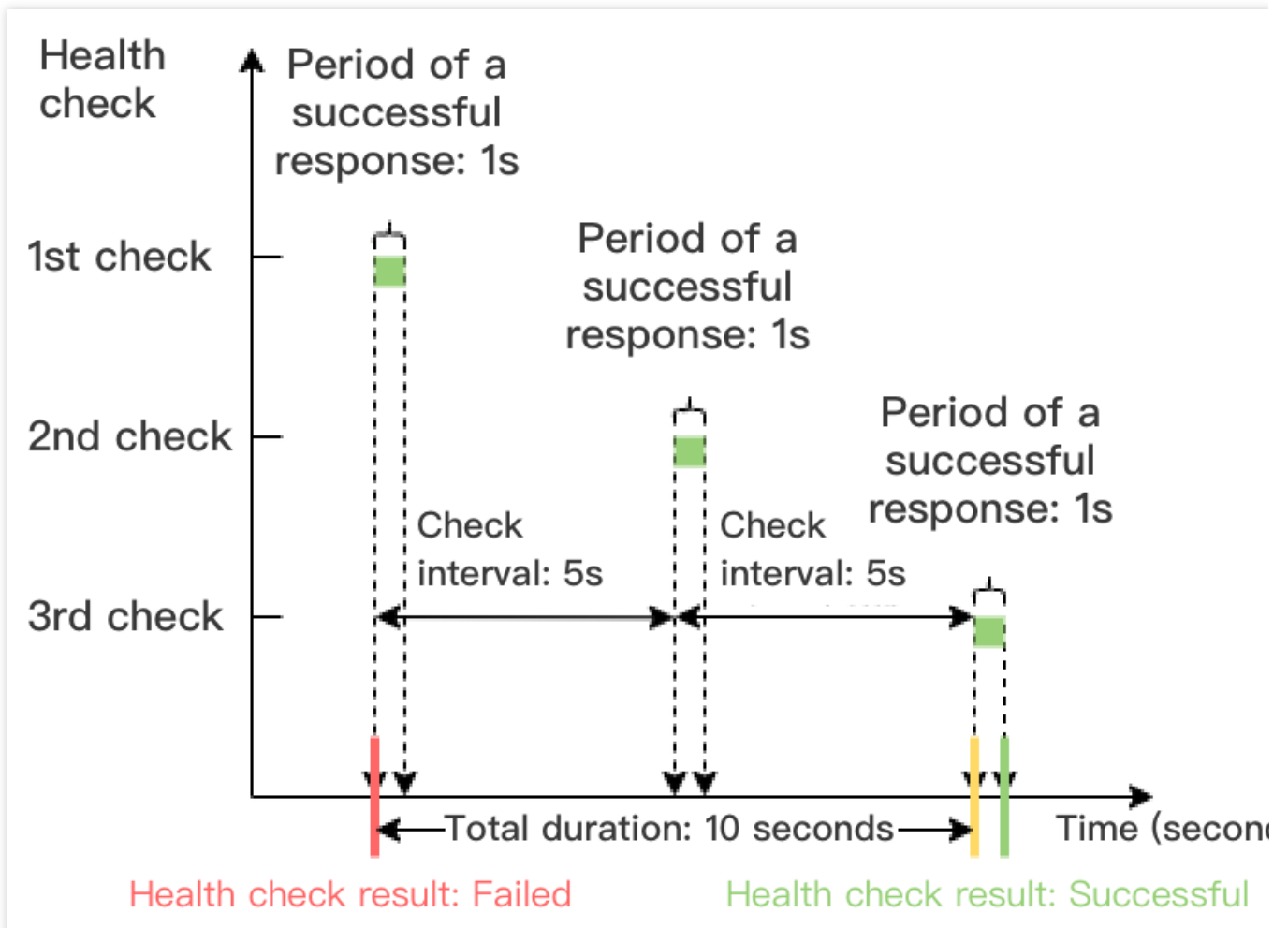
Dalam contoh di bawah ini, waktu habis respons pemeriksaan kesehatan yaitu 2 detik, interval pemeriksaan 5 detik, dan ambang batas tidak sehat 3 kali sehingga periode pemeriksaan kesehatan dengan hasil gagal = 5 × (3-1) = 10 detik.



Periode pemeriksaan kesehatan dengan hasil berhasil = Interval pemeriksaan × (Ambang batas sehat - 1)

Dalam contoh di bawah ini, periode respons pemeriksaan kesehatan yang berhasil yaitu 1 detik, interval pemeriksaan

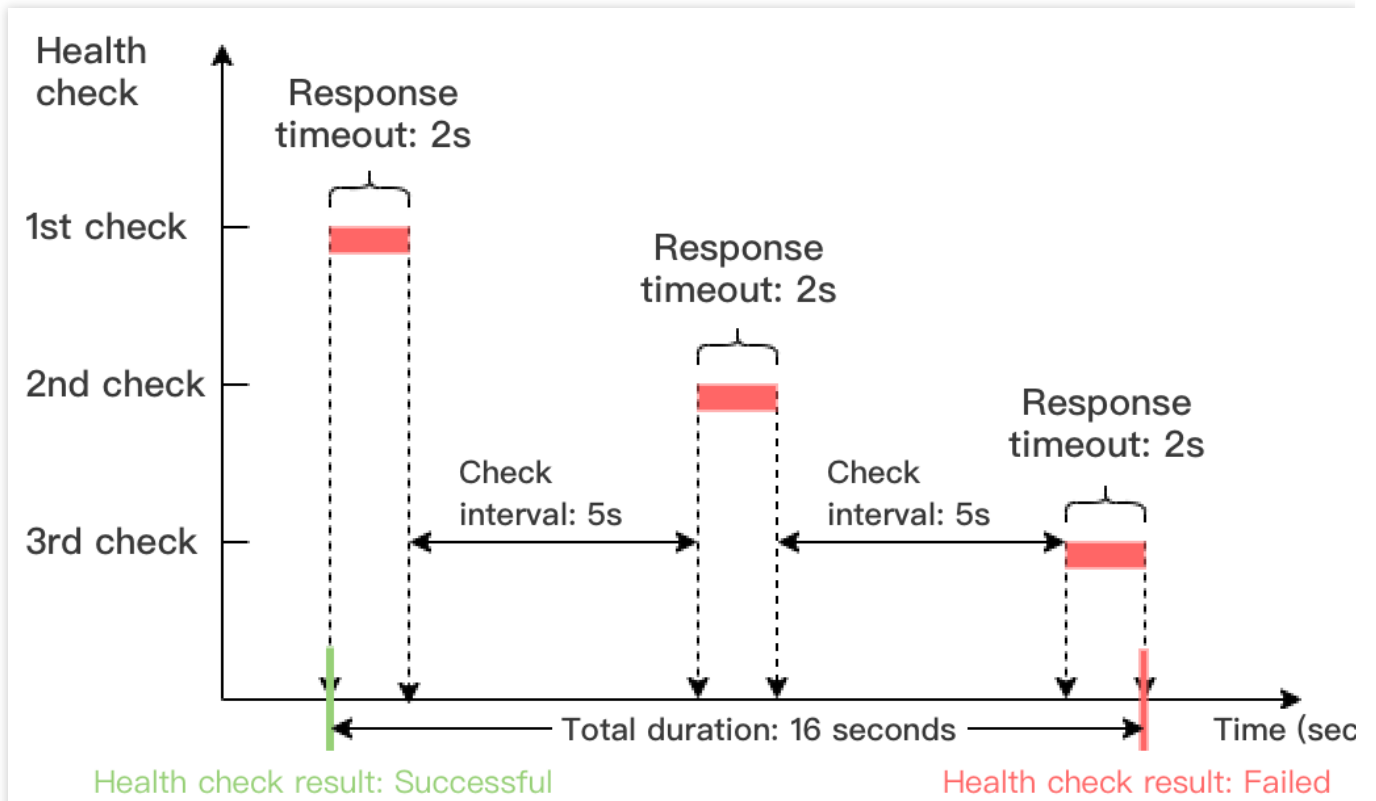
5 detik, dan ambang batas sehat 3 kali sehingga periode pemeriksaan kesehatan dengan hasil yang berhasil = $5 \times (3 - 1) = 10$ detik.



Penghitungan **lapisan 7 health check time window** (periode pemeriksaan kesehatan lapisan 7) yaitu sebagai berikut:

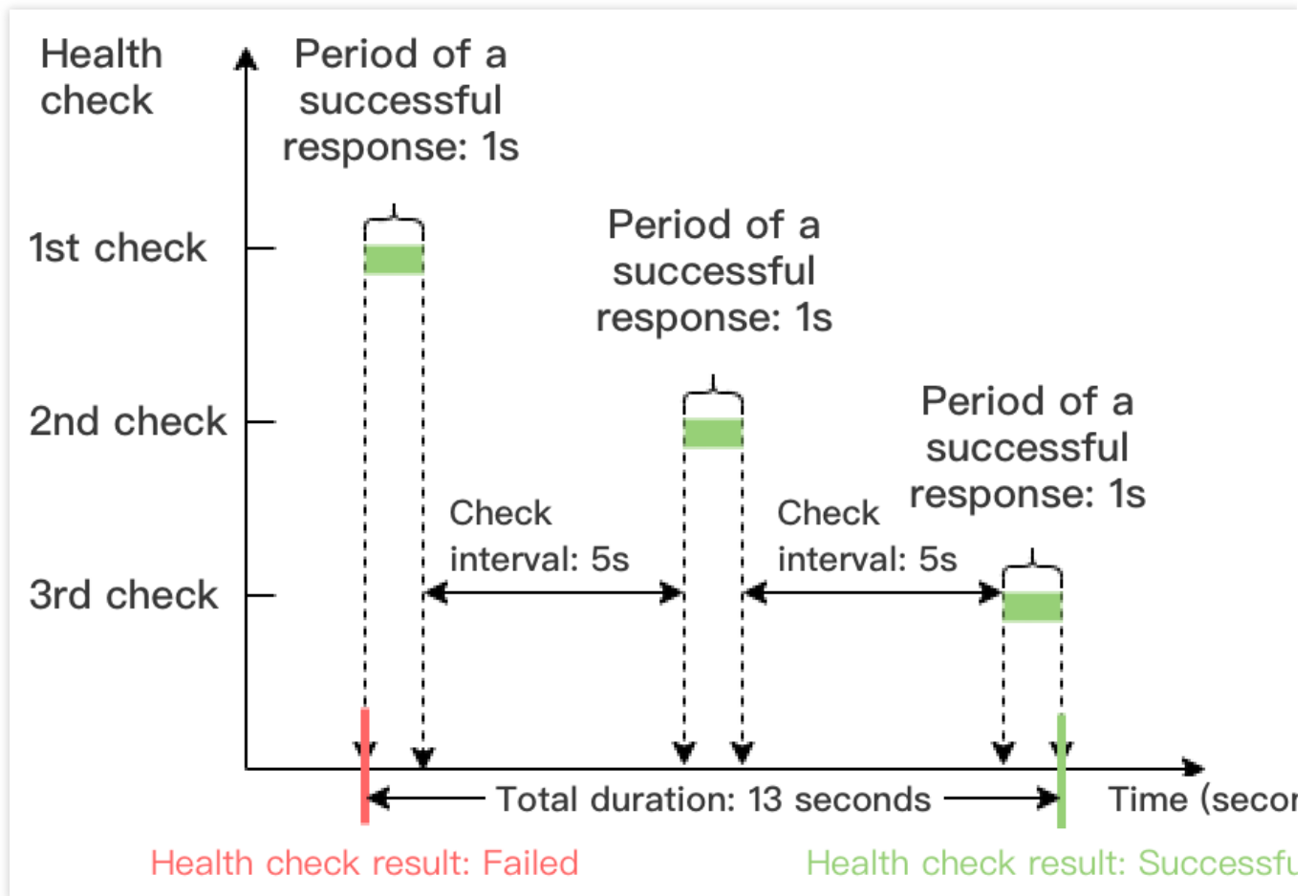
Periode pemeriksaan kesehatan dengan hasil gagal = Waktu habis respons \times Ambang batas tidak sehat + Interval pemeriksaan \times (Ambang batas tidak sehat - 1)

Dalam contoh di bawah ini, waktu habis respons pemeriksaan kesehatan yaitu 2 detik, interval pemeriksaan 5 detik, dan ambang batas tidak sehat 3 kali sehingga periode pemeriksaan kesehatan dengan hasil gagal = $2 \times 3 + 5 \times (3 - 1) = 16$ detik.



Periode pemeriksaan kesehatan dengan hasil berhasil = Periode respons pemeriksaan kesehatan berhasil × Ambang batas sehat + Interval pemeriksaan × (Ambang batas sehat - 1)

Dalam contoh di bawah ini, periode respons pemeriksaan kesehatan yang berhasil yaitu 1 detik, interval pemeriksaan 5 detik, dan ambang batas sehat 3 kali sehingga periode pemeriksaan kesehatan dengan hasil yang berhasil = $1 \times 3 + 5 \times (3-1) = 13$ detik.



Pengidentifikasi Pemeriksaan Kesehatan

Setelah pemeriksaan kesehatan CLB dimulai, server asli akan menerima permintaan pemeriksaan kesehatan selain permintaan bisnis biasa. Permintaan pemeriksaan kesehatan mungkin memiliki properti berikut:

IP sumber pemeriksaan kesehatan yaitu CLB VIP.

Permintaan pemeriksaan kesehatan dari pendengar lapisan 4 (TCP, UDP, dan TCP SSL) akan ditandai dengan "HEALTH CHECK" (PEMERIKSAAN KESEHATAN).

Untuk permintaan pemeriksaan kesehatan dari pendengar lapisan 7 (HTTP dan HTTPS), `user-agent` dalam header yaitu `clb-healthcheck`.

Keterangan :

Untuk permintaan pemeriksaan kesehatan dari instance CLB klasik jaringan privat, IP sumber pemeriksaan kesehatannya yaitu `169.254.128.0/17`.

Untuk permintaan pemeriksaan kesehatan dari instance CLB jaringan klasik, IP sumber pemeriksaan kesehatannya menggunakan IP fisik.

Referensi

Mengonfigurasi Pemeriksaan Kesehatan

Konfigurasi Pemeriksaan Kesehatan

Waktu update terbaru : 2022-01-14 10:13:44

Ketika mengonfigurasi pendengar, Anda dapat mengaktifkan pemeriksaan kesehatan untuk mendapatkan informasi ketersediaan tentang server asli. Untuk informasi selengkapnya tentang pemeriksaan kesehatan, lihat [Gambaran Umum Pemeriksaan Kesehatan](#).

Prasyarat

1. Buat instance CLB. Untuk informasi selengkapnya, silakan lihat [Membuat Instance CLB](#).

2. Buat pendengar CLB

- Untuk membuat pendengar TCP, lihat informasi selengkapnya di [Mengonfigurasi Pendengar TCP](#).
- Untuk membuat pendengar UDP, lihat informasi selengkapnya di [Mengonfigurasi Pendengar UDP](#).
- Untuk membuat pendengar TCP SSL, lihat informasi selengkapnya di [Mengonfigurasi Pendengar TCP SSL](#).
- Untuk membuat pendengar HTTP, lihat informasi selengkapnya di [Mengonfigurasi Pendengar HTTP](#).
- Untuk membuat pendengar HTTPS, lihat informasi selengkapnya di [Mengonfigurasi Pendengar HTTPS](#).

Pendengar TCP

Pendengar TCP lapisan 4 mendukung tiga tipe pemeriksaan kesehatan, antara lain pemeriksaan kesehatan TCP lapisan 4, pemeriksaan kesehatan HTTP lapisan 7, dan pemeriksaan protokol khusus.

- Pemeriksaan kesehatan TCP dilakukan dengan paket SYN, yaitu handshake tiga arah TCP yang dilakukan untuk mendapatkan informasi status instance CVM backend.
- Pemeriksaan kesehatan HTTP dilakukan dengan mengirimkan permintaan HTTP untuk mendapatkan informasi status instance CVM backend.
- Pemeriksaan kesehatan protokol khusus dilakukan dengan menyesuaikan konten input dan output protokol lapisan aplikasi untuk mendapatkan informasi status instance CVM backend.

Mengonfigurasi pemeriksaan kesehatan TCP

1. Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).

2. Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **TCP** sebagai protokol.

| Parameter | Deskripsi |
|-----------|-----------|
| | |

| | |
|-------------------------|--|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan. Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Pemeriksaan kesehatan TCP akan dilakukan jika TCP dipilih. |
| Port | Bersifat opsional. Sebaiknya jangan tentukan port, kecuali Anda perlu memeriksa port tertentu. Port server asli akan diperiksa jika port tidak ditentukan di sini. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Mengonfigurasi pemeriksaan kesehatan HTTP

1. Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).

2. Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **HTTP** sebagai protokol.

| Parameter | Deskripsi |
|-----------------------|--|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan. Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Pemeriksaan kesehatan HTTP akan dilakukan jika HTTP dipilih. |
| Port | Bersifat opsional. Sebaiknya jangan tentukan port, kecuali Anda perlu memeriksa port tertentu. Port server asli akan diperiksa jika port tidak ditentukan di sini. |
| Domain pemeriksaan | <p>Persyaratan terkait nama domain untuk pemeriksaan kesehatan:</p> <ul style="list-style-type: none"> Panjang: 1 hingga 80 karakter. Merupakan nama domain penerusan secara default. Tidak mendukung ekspresi reguler. Jika nama domain penerusan Anda menggunakan kartubebas, Anda perlu menetapkan nama domain tetap (non-reguler) sebagai nama domain pemeriksaan kesehatan. Karakter yang didukung: huruf kecil (a hingga z), digit (0 hingga 9), poin desimal (.), dan tanda hubung (-). |
| Jalur | <p>Persyaratan terkait jalur pemeriksaan kesehatan:</p> <ul style="list-style-type: none"> Panjang: 1 hingga 200 karakter. `/` adalah nilai default dan harus digunakan sebagai karakter pertama. Tidak mendukung ekspresi reguler. Sebaiknya tentukan URL tetap (halaman web statis) untuk pemeriksaan kesehatan. Karakter yang didukung: huruf kecil (a hingga z), huruf kapital (A hingga Z), digit (0 hingga 9), poin desimal (.), tanda hubung (-), garis bawah (_), garis miring (/), tanda sama dengan (=). |

| | |
|-------------------------|--|
| | (=), dan tanda tanya (?). |
| Metode permintaan HTTP | <p>Metode permintaan HTTP pada pemeriksaan kesehatan.Opsi:GET (metode default) dan HEAD.</p> <ul style="list-style-type: none"> Jika HEAD dipilih, server hanya akan mengembalikan informasi header HTTP, yang dapat mengurangi overhead backend dan meningkatkan efisiensi permintaan.Server asli harus mendukung HEAD. Jika GET dipilih, server asli harus mendukung GET. |
| Versi HTTP | <p>Versi HTTP server asli.</p> <ul style="list-style-type: none"> Jika server asli mendukung versi HTTP 1.0, bidang host permintaan tidak akan memerlukan autentikasi, artinya, domain pemeriksaan tidak perlu dikonfigurasi. Jika server asli mendukung versi HTTP 1.1, bidang host permintaan memerlukan autentikasi, artinya, domain pemeriksaan perlu dikonfigurasi atau Anda akan mendapatkan kode kesalahan 404. |
| Kode status normal | <p>Jika kode status merupakan kode yang telah dipilih, server asli akan dianggap aktif (sehat).Opsi: http_1xx, http_2xx, http_3xx, http_4xx, dan http_5xx.Anda dapat memilih beberapa opsi.</p> |
| Tampilkan opsi lanjutan | <p>Untuk informasi selengkapnya, lihat Opsi Lanjutan.</p> |

Mengonfigurasi pemeriksaan kesehatan protokol khusus

- Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).
- Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **HTTP** sebagai protokol.

| Parameter | Deskripsi |
|-----------------------|---|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan.Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Pemeriksaan kesehatan protokol khusus akan dilakukan jika Custom Protocol (Protokol Khusus) dipilih. |
| Port | Bersifat opsional.Sebaiknya jangan tentukan port, kecuali Anda perlu memeriksa port tertentu.Port server asli akan diperiksa jika port tidak ditentukan di sini. |
| Format input | Mendukung teks dan string heksadesimal. |

| | |
|-------------------------|--|
| | <ul style="list-style-type: none"> • Jika Teks dipilih, teks tersebut akan dikonversi menjadi string biner untuk mengirimkan permintaan dan membandingkan hasil yang dikembalikan. • Jika Heksadesimal dipilih, string heksadesimal akan dikonversi menjadi string biner untuk mengirimkan permintaan dan membandingkan hasil yang dikembalikan. |
| Permintaan | Konten permintaan pemeriksaan kesehatan khusus. |
| Hasil pengembalian | Ketika menyesuaikan permintaan pemeriksaan kesehatan, Anda perlu memasukkan hasil pemeriksaan kesehatan yang dikembalikan. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Pendengar UDP

Pendengar UDP mendukung pemeriksaan kesehatan UDP, yang dapat dilakukan dengan memeriksa port dan menjalankan perintah Ping.

Mengonfigurasi pemeriksaan kesehatan UDP - pemeriksaan port

1. Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).
2. Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **Port** sebagai protokol.

| Parameter | Deskripsi |
|-----------------------|---|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan. Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Jika Port dipilih, paket deteksi UDP akan dikirimkan ke instance CVM backend melalui VIP (yaitu alamat IP yang digunakan oleh instance CLB untuk menyediakan layanan kepada klien), dan ping akan dikirimkan ke IP instance CVM backend untuk mendapatkan status instance CVM backend. |
| Port | Bersifat opsional. Sebaiknya jangan tentukan port, kecuali Anda perlu memeriksa port tertentu. Port server asli akan diperiksa jika port tidak ditentukan di sini. |
| Format input | <p>Mendukung teks dan string heksadesimal.</p> <ul style="list-style-type: none"> • Jika Teks dipilih, teks tersebut akan dikonversi menjadi string biner untuk mengirimkan permintaan dan membandingkan hasil yang dikembalikan. • Jika Heksadesimal dipilih, string heksadesimal akan dikonversi menjadi string biner untuk mengirimkan permintaan dan membandingkan hasil yang dikembalikan. |

| | |
|-------------------------|--|
| Permintaan | Bersifat opsional.Konten permintaan pemeriksaan kesehatan khusus. |
| Hasil pengembalian | Bersifat opsional.Ketika menyesuaikan permintaan pemeriksaan kesehatan, Anda perlu memasukkan hasil pemeriksaan kesehatan yang dikembalikan. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Mengonfigurasi pemeriksaan kesehatan UDP - Perintah ping

- 1.Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).
- 2.Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **PING** sebagai protokol.

| Parameter | Deskripsi |
|-------------------------|---|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan.Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Jika PING dipilih, ping akan dikirimkan ke IP instance CVM backend untuk mendapatkan status instance CVM backend. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Pendengar TCP SSL

Mengonfigurasi pemeriksaan kesehatan TCP

- 1.Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).
- 2.Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **TCP** sebagai protokol.

| Parameter | Deskripsi |
|-----------------------|---|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan.Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Pemeriksaan kesehatan TCP akan dilakukan jika TCP dipilih. |
| Port | Port pemeriksaan kesehatan dan port pendengar untuk pendengar TCP SSL menggunakan |

| | |
|-------------------------|---|
| | port yang sama. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Mengonfigurasi pemeriksaan kesehatan HTTP

1.Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).

2.Dalam langkah **Health Check** (Pemeriksaan Kesehatan), pilih **HTTP** sebagai protokol.

| Parameter | Deskripsi |
|------------------------|---|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan.Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Protokol | Pemeriksaan kesehatan HTTP akan dilakukan jika HTTP dipilih. |
| Port | Port pemeriksaan kesehatan dan port pendengar untuk pendengar TCP SSL menggunakan port yang sama. |
| Domain pemeriksaan | Persyaratan terkait nama domain untuk pemeriksaan kesehatan: <ul style="list-style-type: none"> • Panjang: 1 hingga 80 karakter. • Merupakan nama domain penerusan secara default. • Tidak mendukung ekspresi reguler.Jika nama domain penerusan Anda menggunakan kartubebas, Anda perlu menetapkan nama domain tetap (non-reguler) sebagai nama domain pemeriksaan kesehatan. • Karakter yang didukung: huruf kecil (a hingga z), digit (0 hingga 9), poin desimal (.), dan tanda hubung (-). |
| Jalur | Persyaratan terkait jalur pemeriksaan kesehatan: <ul style="list-style-type: none"> • Panjang: 1 hingga 200 karakter. • ` ` adalah nilai default dan harus digunakan sebagai karakter pertama. • Tidak mendukung ekspresi reguler.Sebaiknya tentukan URL tetap (halaman web statis) untuk pemeriksaan kesehatan. • Karakter yang didukung: huruf kecil (a hingga z), huruf kapital (A hingga Z), digit (0 hingga 9), poin desimal (.), tanda hubung (-), garis bawah (_), garis miring (/), tanda sama dengan (=), dan tanda tanya (?). |
| Metode permintaan HTTP | Metode permintaan HTTP pada pemeriksaan kesehatan.Opsi:GET (metode default) dan HEAD. <ul style="list-style-type: none"> • Jika HEAD dipilih, server hanya akan mengembalikan informasi header HTTP, yang dapat mengurangi overhead backend dan meningkatkan efisiensi permintaan.Server asli harus |

| | |
|-------------------------|---|
| | <p>mendukung HEAD.</p> <ul style="list-style-type: none"> • Jika GET dipilih, server asli harus mendukung GET. |
| Versi HTTP | Versi HTTP server asli. Hanya mendukung HTTP 1.1. Jika server asli perlu mengautentikasi bidang host permintaan, artinya, domain pemeriksaan perlu dikonfigurasi atau Anda akan mendapatkan kode kesalahan 404. |
| Kode status normal | Jika kode status merupakan kode yang telah dipilih, server asli akan dianggap aktif (sehat). Opsi: http_1xx, http_2xx, http_3xx, http_4xx, dan http_5xx. Anda dapat memilih beberapa opsi. |
| Tampilkan opsi lanjutan | Untuk informasi selengkapnya, lihat Opsi Lanjutan . |

Pendengar HTTP

Mengonfigurasi pemeriksaan kesehatan HTTP

1. Konfigurasi pendengar menggunakan langkah **Health Check** (Pemeriksaan Kesehatan) sesuai petunjuk dalam [Prasyarat](#).

| Parameter | Deskripsi |
|-----------------------|--|
| Pemeriksaan kesehatan | Dapat diaktifkan atau dinonaktifkan. Sebaiknya aktifkan pemeriksaan kesehatan agar dapat melakukan pemeriksaan otomatis terhadap instance CVM backend dan menghapus port abnormal. |
| Domain pemeriksaan | <p>Persyaratan terkait nama domain untuk pemeriksaan kesehatan:</p> <ul style="list-style-type: none"> • Panjang: 1 hingga 80 karakter. • Merupakan nama domain penerusan secara default. • Tidak mendukung ekspresi reguler. Jika nama domain penerusan Anda menggunakan kartubebas, Anda perlu menetapkan nama domain tetap (non-reguler) sebagai nama domain pemeriksaan kesehatan. • Karakter yang didukung: huruf kecil (a hingga z), digit (0 hingga 9), poin desimal (.), dan tanda hubung (-). |
| Jalur | <p>Jalur pemeriksaan kesehatan dapat diatur ke direktori root server asli atau URL tertentu. Persyaratannya adalah sebagai berikut:</p> <ul style="list-style-type: none"> • Panjang: 1 hingga 200 karakter. • `^` adalah nilai default dan harus digunakan sebagai karakter pertama. • Tidak mendukung ekspresi reguler. Sebaiknya tentukan URL tetap (halaman web statis) untuk pemeriksaan kesehatan. |

| | |
|--------------------------|---|
| | <ul style="list-style-type: none"> Karakter yang didukung: huruf kecil (a hingga z), huruf kapital (A hingga Z), digit (0 hingga 9), poin desimal (.), tanda hubung (-), garis bawah (_), garis miring (/), tanda sama dengan (=), dan tanda tanya (?). |
| Waktu habis respons | <ul style="list-style-type: none"> Waktu habis respons maksimum untuk pemeriksaan kesehatan Jika server asli tidak merespons dalam periode waktu habis, server akan dianggap abnormal. Rentang nilai: 2-60 detik. |
| Interval pemeriksaan | <ul style="list-style-type: none"> Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300 detik. |
| Ambang batas tidak sehat | <ul style="list-style-type: none"> Jika hasil pemeriksaan kesehatan gagal sebanyak n (nilai dapat disesuaikan) kali, instance CVM backend akan dianggap tidak sehat, dan konsol akan menampilkan status Abnormal. Rentang nilai: 2-10 kali. |
| Ambang batas sehat | <ul style="list-style-type: none"> Jika hasil pemeriksaan kesehatan berhasil sebanyak n (nilai dapat disesuaikan) kali, instance CVM backend akan dianggap sehat, dan konsol akan menampilkan status Healthy (Sehat). Rentang nilai: 2-10 kali. |
| Metode permintaan HTTP | <p>Metode permintaan HTTP pada pemeriksaan kesehatan.Opsi:GET (metode default) dan HEAD.</p> <ul style="list-style-type: none"> Jika HEAD dipilih, server hanya akan mengembalikan informasi header HTTP, yang dapat mengurangi overhead backend dan meningkatkan efisiensi permintaan.Server asli harus mendukung HEAD. Jika GET dipilih, server asli harus mendukung GET. |
| Kode status normal | <p>Jika kode status merupakan kode yang telah dipilih, server asli akan dianggap aktif (sehat).Opsi: http_1xx, http_2xx, http_3xx, http_4xx, dan http_5xx.Anda dapat memilih beberapa opsi.</p> |

Pendengar HTTPS

undefined :

Jika HTTP dipilih sebagai protokol backend aturan penerusan pendengar HTTPS, pemeriksaan kesehatan HTTP akan dilakukan; jika HTTPS dipilih, pemeriksaan kesehatan HTTPS akan dilakukan.

Untuk konfigurasi pemeriksaan kesehatan pada pendengar HTTPS, lihat [Pendengar HTTP](#).

Opsi Lanjutan

| Konfigurasi Pemeriksaan Kesehatan | Deskripsi | Nilai Default |
|-----------------------------------|---|---------------|
| Waktu habis respons | <ul style="list-style-type: none">Waktu habis respons maksimum untuk pemeriksaan kesehatan.Jika server asli tidak merespons dalam periode waktu habis, pemeriksaan kesehatan dianggap abnormal.Rentang nilai: 2 - 60 detik. | 2 detik |
| Interval pemeriksaan | <ul style="list-style-type: none">Interval antara dua pemeriksaan kesehatan.Rentang nilai: 5 - 300 detik. | 5 detik |
| Ambang batas tidak sehat | <ul style="list-style-type: none">Jika hasil pemeriksaan kesehatan gagal sebanyak n (nilai dapat disesuaikan) kali, instance CVM backend akan dianggap tidak sehat, dan konsol akan menampilkan status Abnormal.Rentang nilai: 2-10 kali. | 3 kali |
| Ambang batas sehat | <ul style="list-style-type: none">Jika hasil pemeriksaan kesehatan berhasil sebanyak n (nilai dapat disesuaikan) kali, instance CVM backend akan dianggap sehat, dan konsol akan menampilkan status Healthy (Sehat).Rentang nilai: 2-10 kali. | 3 kali |

Pengelolaan Sertifikat

Mengelola Sertifikat

Waktu update terbaru : 2024-01-04 20:53:33

Ketika mengonfigurasi listener HTTPS pada instance CLB, Anda dapat langsung menggunakan sertifikat di SSL Certificate Service atau mengunggah sertifikat server dan [sertifikat SSL](#) yang diterbitkan oleh pihak ketiga CA untuk CLB.

Persyaratan Sertifikat

CLB hanya mendukung sertifikat dalam format PEM. Sebelum mengunggah sertifikat, pastikan sertifikat, rantai sertifikat, dan kunci privat Anda memenuhi persyaratan format. Untuk persyaratan sertifikat, lihat [Format Sertifikat SSL](#).

Mengonfigurasi Sertifikat

Konfigurasi sertifikat untuk listener HTTPS dibagi menjadi dua tipe berikut:

Jika SNI tidak diaktifkan, sertifikat dapat dikonfigurasi pada tingkat listener, selama semua nama domain menggunakan sertifikat yang sama. Untuk informasi selengkapnya, lihat [Mengonfigurasi Listener HTTPS](#).

Jika SNI diaktifkan, sertifikat dapat dikonfigurasi pada tingkat nama domain, dan sertifikat lainnya dapat dikonfigurasi untuk nama domain lain dalam listener. Untuk informasi selengkapnya, lihat [Dukungan SNI untuk Mengikat Beberapa Sertifikat ke Satu Instance CLB](#).

Memperbarui Sertifikat dalam Batch

Agar sertifikat yang kedaluwarsa tidak menghambat layanan Anda, silakan perbarui sertifikat sebelum sertifikat kedaluwarsa.

Keterangan :

Setelah sertifikat diperbarui, sistem tidak akan menghapus sertifikat lama; tetapi akan membuat sertifikat baru. Sertifikat secara otomatis akan diperbarui untuk semua instance CLB yang menggunakannya.

1. Masuk ke [Konsol CLB](#).
2. Klik **Certificate Management** (Manajemen Sertifikat) di bilah sisi kiri.
3. Dalam daftar sertifikat di halaman **Certificate Management** (Manajemen Sertifikat), klik **Update** (Perbarui) pada kolom "Operation" (Operasi) di sebelah kanan sertifikat target.
4. Dalam kotak dialog "Create Certificate" (Buat Sertifikat) yang muncul, masukkan isi sertifikat dan isi kunci sertifikat baru, lalu klik **Submit** (Kirim).

Create a new certificate ✕

Certificate Name

Cannot exceed 80 characters, only English letters, numbers, underscores, and hyphens are supported "-", ".".

Certificate Type Server Certificate Client CA Certificate

Certificate Content

```
-----BEGIN CERTIFICATE-----  
[Blurred content]  
-----END CERTIFICATE-----
```

[View Examples](#)

Key Content

```
-----BEGIN RSA PRIVATE KEY-----  
[Blurred content]  
-----END RSA PRIVATE KEY-----
```

[View Examples](#)

Menampilkan Instance CLB yang Terkait dengan Sertifikat

1. Masuk ke [Konsol CLB](#).
2. Klik **Certificate Management** (Manajemen Sertifikat) di bilah sisi kiri.
3. Dalam daftar sertifikat pada halaman **Certificate Management** (Manajemen Sertifikat), klik ID sertifikat target.
4. Di halaman "Basic Info" (Info Dasar), tampilkan instance CLB yang terkait dengan sertifikat.

Basic Info

Name manuel-test

ID ha2qQzkD

Certificate Type Server Certificate

Certificate Content

```
-----BEGIN CERTIFICATE-----  
[Blurred Certificate Content]  
-----END CERTIFICATE-----
```

[Copy](#)

Load Balancer Bound

[Blurred Load Balancer Bound Information]

Primary Domain Name

[Blurred]

Alternate Domain

-

Upload Time 2020-10-29 12:06:20

Start Time 2020-07-03 18:05:58

Expiry Time 2021-07-03 18:05:58

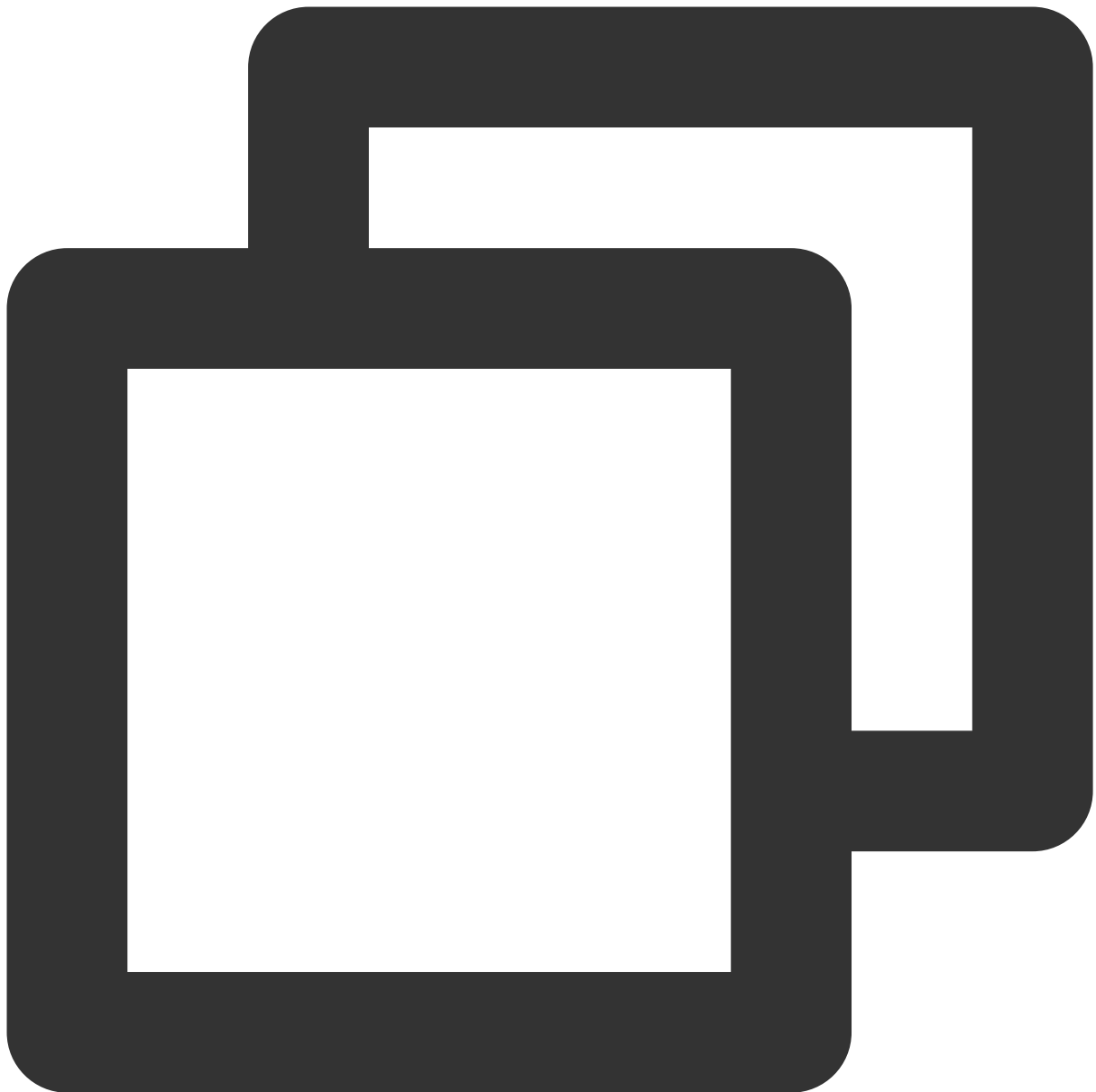
Persyaratan Sertifikat dan Konversi Format Sertifikat

Waktu update terbaru : 2024-01-04 20:53:33

Dokumen ini berisi persyaratan terkait sertifikat SSL dan menjelaskan tentang cara mengonversi format sertifikat.

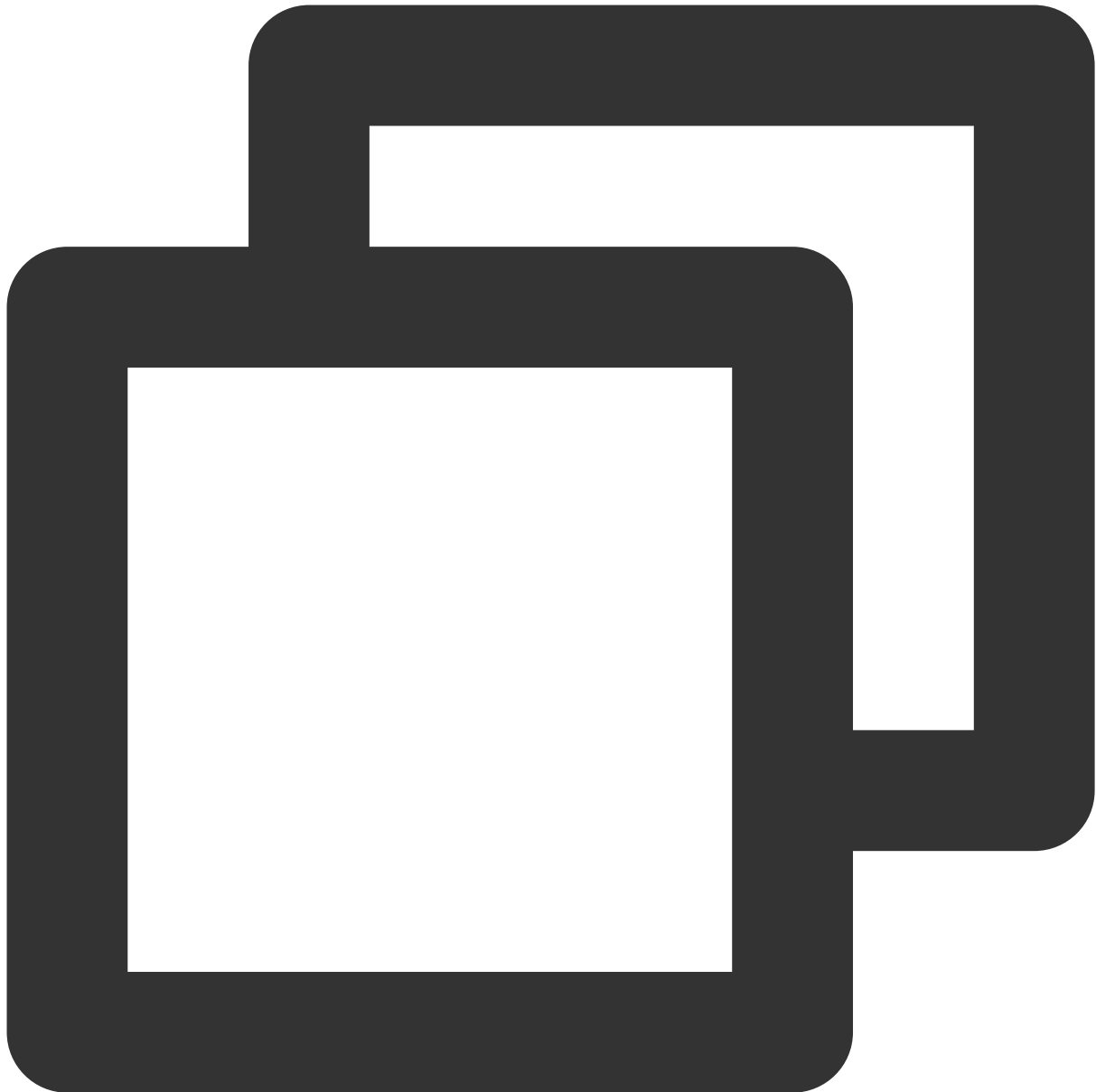
Proses Permohonan Sertifikat

1. Gunakan OpenSSL untuk membuat file kunci private secara lokal, misalnya: `privateKey.pem`. Harap rahasiakan kunci ini.



```
openssl genrsa -out privateKey.pem 2048
```

2. Gunakan OpenSSL untuk membuat file permintaan sertifikat, misalnya: `server.csr`. File ini dapat digunakan untuk permohonan sertifikat.



```
openssl req -new -key privateKey.pem -out server.csr
```

3. Simpan isi file permintaan sertifikat, lalu kunjungi situs CA untuk memohon sertifikat.

Persyaratan Format Sertifikat

Sertifikat yang perlu diminta harus menggunakan format PEM di Linux. CLB tidak mendukung sertifikat dalam format lain. Untuk informasi selengkapnya, lihat [Mengonversi Sertifikat ke format PEM](#).

Jika sertifikat Anda dikeluarkan oleh CA root, sertifikat akan bersifat unik, dan situs web yang dikonfigurasi akan dianggap tepercaya oleh peramban dan perangkat lain yang mengakses tanpa memerlukan sertifikat tambahan. Jika sertifikat Anda dikeluarkan oleh CA perantara, file sertifikat Anda akan terdiri dari beberapa sertifikat. Dalam kasus ini, Anda harus mengombinasikan secara manual sertifikat server dan sertifikat perantara untuk diunggah. Jika sertifikat Anda memiliki rantai sertifikat, silakan konversi sertifikat ke format PEM dan gabungkan dengan konten sertifikat untuk diunggah.

Aturan urutannya sebagai berikut: terapkan sertifikat server sebelum sertifikat perantara tanpa baris kosong di antaranya.

Keterangan :

Anda dapat memeriksa aturan yang berlaku atau instruksi yang disediakan oleh CA ketika mengeluarkan sertifikat.

Format sertifikat dan format rantai sertifikat

Berikut adalah contoh format sertifikat dan rantai sertifikat. Pastikan format sudah benar sebelum diunggah:

1. Sertifikat dikeluarkan oleh CA root: Format PEM di Linux, seperti yang ditunjukkan di bawah ini:

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMakGA1UEBhMCVVMxZzAVBgNVBAs0TD1Z1cm1TdWduLmNvbS99YDQVQQL
ExZWZxJpU2lubiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLZSJUZXRJcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYS0AYykw0TEvMC0GA1UEAxMm
VmVyaVNoZ24gQ2xhc3MgMyBTZW51cmUgU2VydGVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWHhcNMTAxMDA4MjMzMjU0U2VjBjBQswCQYDVQQGEwJVUzETMBEGA1UECBMk
V2FzaGluz3RvbjEQAQA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBjbmMuMR0wGAYDVQQDFBpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAA0BjQAwYkCgYEA3Xb0EGea2d88QGEUwLcEppwGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCzdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwgGHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVLJTZW51cmUgU2RzITtY3JslLnZ1cm1zaWduLmNvbS99YDQV
ZWN1cmVHMisjcmwwRAYDVR0gBD0wOzA5BgtghkgBhvFAQCXAzAqMCGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lubi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBgggrBgEFBQcDAjAFBgNVHSMEGDAWgBS17wsRzsBBA6NKZZBIshzgVy19
RzB2BgggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAAGGGGh0dHA6Ly9vY3NwLnZ1cm1z
aWduLmNvbTBABgggrBgEFBQcAwAoY0aHR0cDovL1NWU1N1Y3VyZS1HM1haWEudmVyaXNp
Z24uY29tL1NWU1N1Y3VyZUcyLmNlcm1uLmNvbS99YDQVQQLZSJUZXRJcyBvZiB1c2Ug
WDBWFglpbWFnZS9naWYwITAFMAcGBSs0AwIaBBRLa7kolgYMu9BS0JsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lubi5jb20vdnNsb2dvMSSnaWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeg782QstGwEE9zBcVCuKjrs13dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmp7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1a2BSUIHxGLn9N4F09hYwwbeEzaCxfGbiLdEiodNwzcvGJ+2L1DWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwrk450mC0nqH4ly4P41Xo02t4A/DI1I8ZNct/QfL69a2L f6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdncL5Svas=
-----END CERTIFICATE-----
```

Aturan sertifikat antara lain:

Sertifikat Anda harus diawali dengan "-----BEGIN CERTIFICATE-----" dan diakhiri dengan "-----END CERTIFICATE-----", yang harus diunggah bersama-sama.

Setiap baris harus berisi 64 karakter, sedangkan baris terakhir boleh berisi kurang dari 64 karakter.

2. Rantai sertifikat dari CA perantara:

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Aturan rantai sertifikat:

Tidak boleh ada baris kosong antar sertifikat.

Semua sertifikat harus memenuhi persyaratan yang disebutkan di atas.

Persyaratan Format Kunci Privat RSA

Berikut contohnya:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzVSSChH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMjclVa2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XyYuoqaIePZtK9Qnjn957ZEPHjtUpVZuhS3409DDM/tJ3T18aaNYWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5MM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGL68Z/nnFyRHRFi
LaF6+Wen8ZvNqkm0hAMQwIjH1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WgpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHnCMNG7dGyo1UowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoiEys111ah1AJvICVgTc3+LzG2pIpM7I+K0nHCSeswM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyX1+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhagHu0edU
ZXIHRJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTad1BW4led0Sa/uKRa04UzVgnYp2aJKxtuWfFvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgFU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS
ICRkQaB3gPSe/LCgzy1nhtafOUbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kV106MZCFAdqirAjiQWapkh9Bxpb2eHCrB81MFAWLQSLok79b/jVmTZMC3upd
EJ/iSwjZKpbw7hCFARtPhxyNTJ5idEiu9U8EQid8111giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
B0IDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFrzfDeQ7z
NTKh193HHF1joNM81LHFyGRFEWwrr0W5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

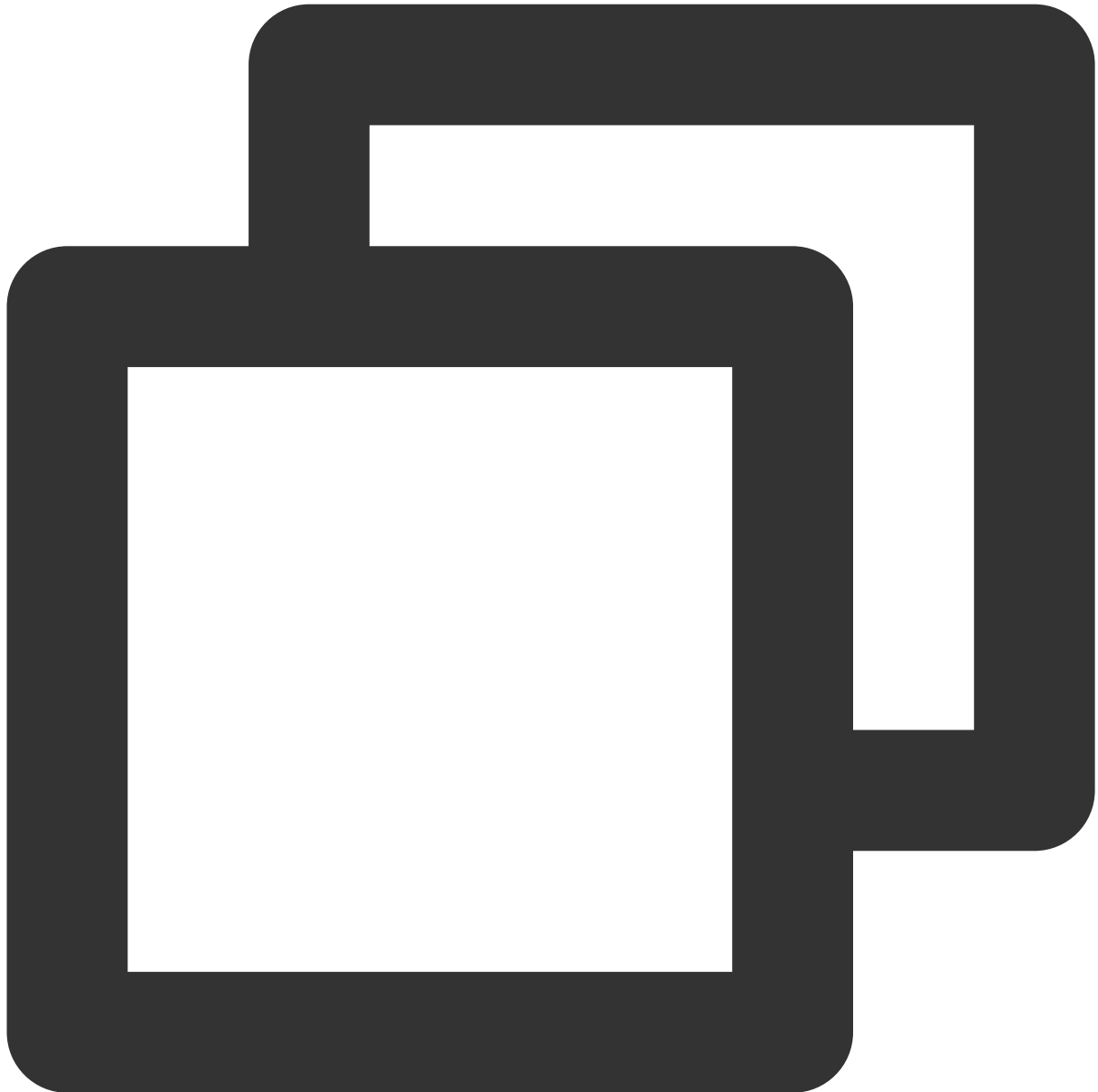
Kunci privat RSA dapat mencakup semua kunci privat (RSA dan DSA), kunci publik (RSA dan DSA), serta sertifikat (X.509). Kunci ini menyimpan data dalam format DER dalam kode Base64 dan dibungkus oleh header ASCII sehingga sesuai untuk ditransmisikan dalam mode teks antar sistem.

Aturan kunci privat RSA:

Sertifikat Anda harus diawali dengan "-----BEGIN RSA PRIVATE KEY-----" dan diakhiri dengan "-----END RSA PRIVATE KEY-----", yang harus diunggah bersama-sama.

Setiap baris harus berisi 64 karakter, sedangkan baris terakhir boleh berisi kurang dari 64 karakter.

Jika kunci privat Anda tidak diawali dengan "-----BEGIN PRIVATE KEY-----" dan diakhiri dengan "-----END PRIVATE KEY-----", Anda dapat mengonversinya dengan cara berikut:



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

Setelah itu, Anda dapat mengunggah konten `new_server_key.pem` bersama sertifikat.

Mengonversi Sertifikat ke Format PEM

Saat ini, CLB hanya mendukung sertifikat dalam format PEM. Sertifikat dalam format lain perlu dikonversi ke format PEM terlebih dahulu sebelum diunggah ke CLB. Kami menyarankan Anda menggunakan OpenSSL. Berikut adalah cara mengonversi beberapa format umum ke PEM.

DER to PEM

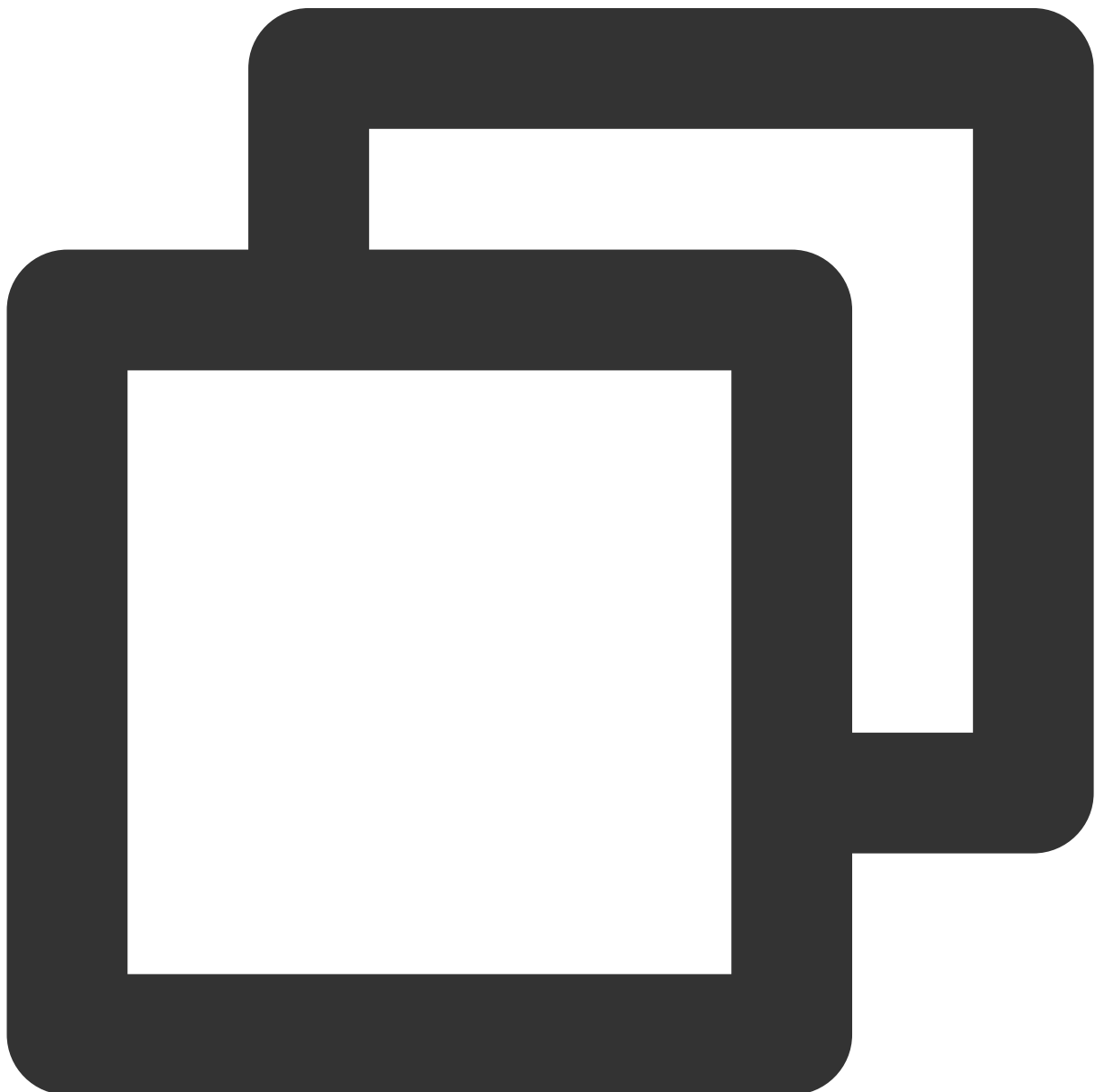
P7B to PEM

PFX to PEM

CER/CRT to PEM

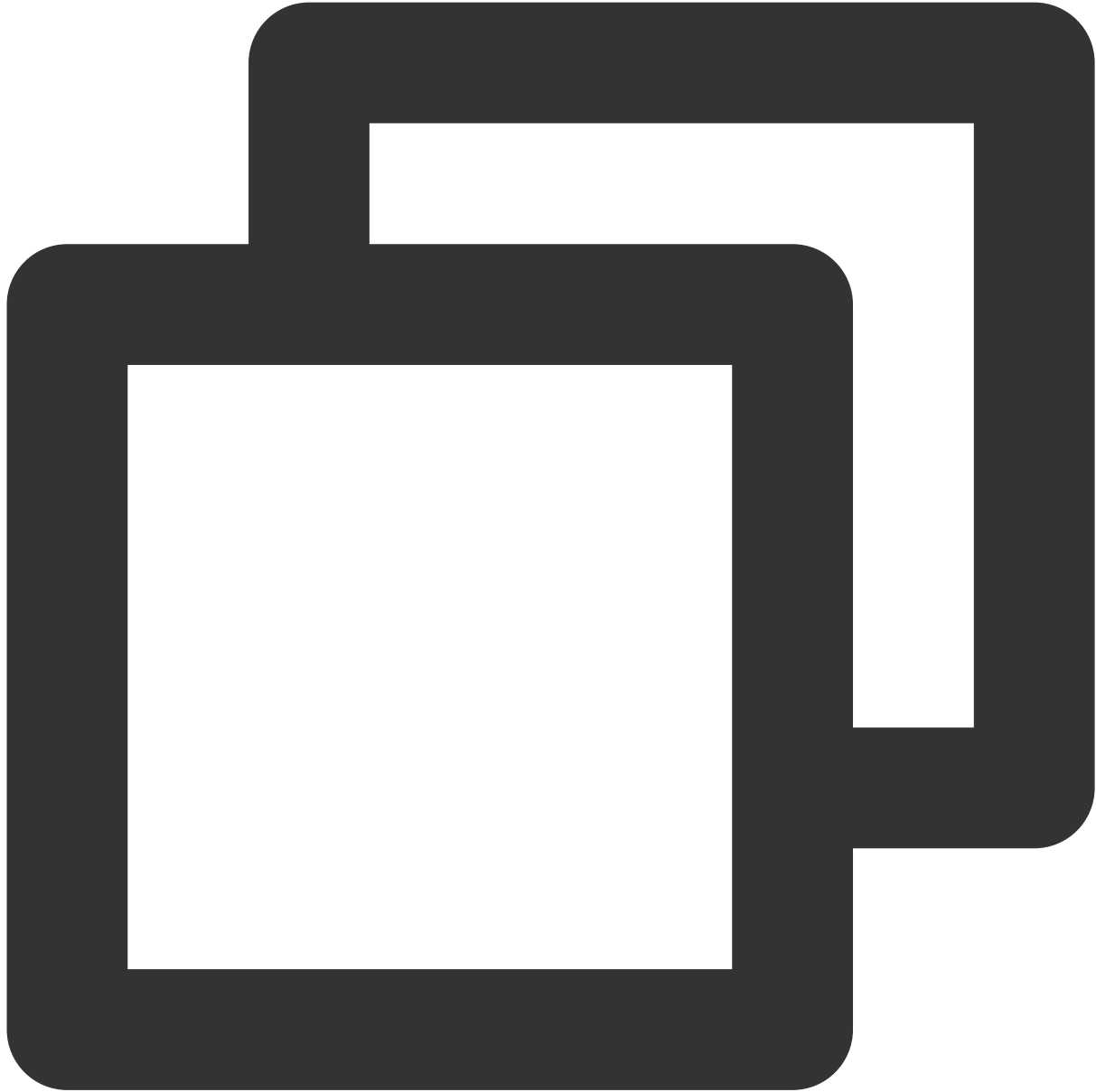
Format DER umumnya digunakan pada platform Java.

Konversi sertifikat:



```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

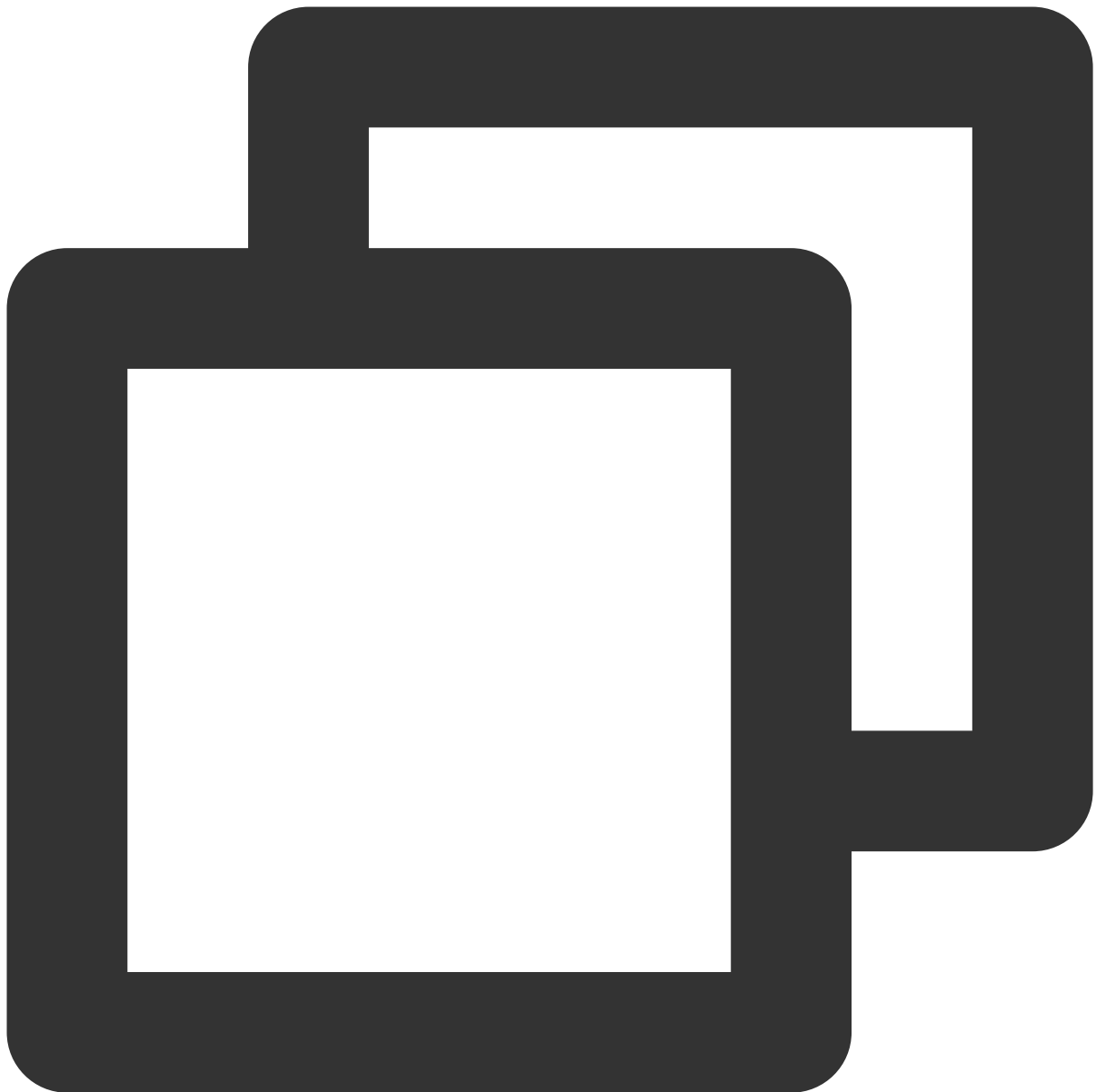
Konversi kunci privat:



```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

Format P7B umumnya digunakan pada Windows Server dan Tomcat.

Konversi sertifikat:



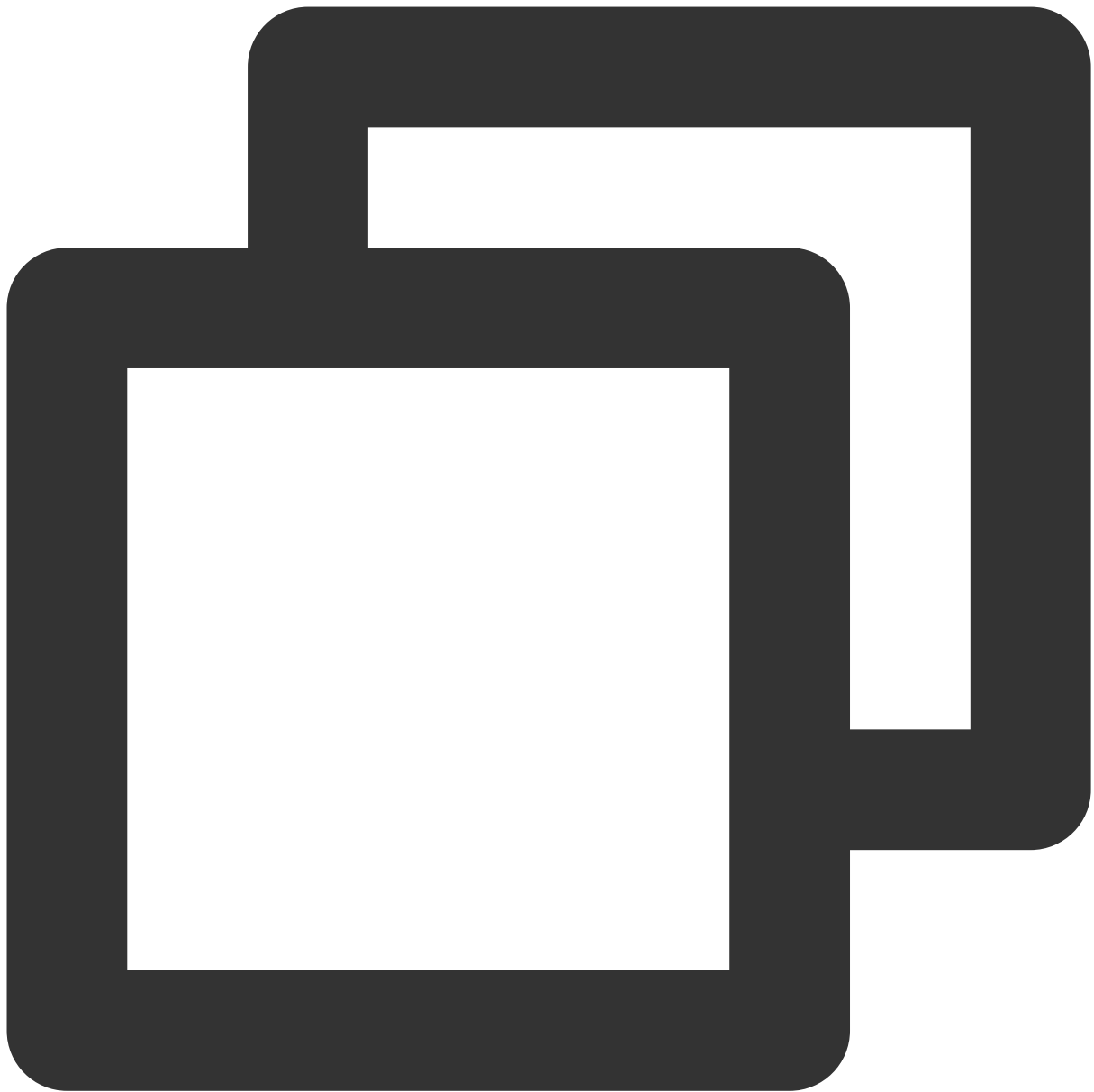
```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

Anda harus menyimpan konten antara "-----BEGIN CERTIFICATE-----" dan "-----END CERTIFICATE-----" dalam `outcertificat.cer` untuk diunggah sebagai sertifikat.

Konversi kunci privat: kunci privat umumnya dapat diekspor ke server IIS.

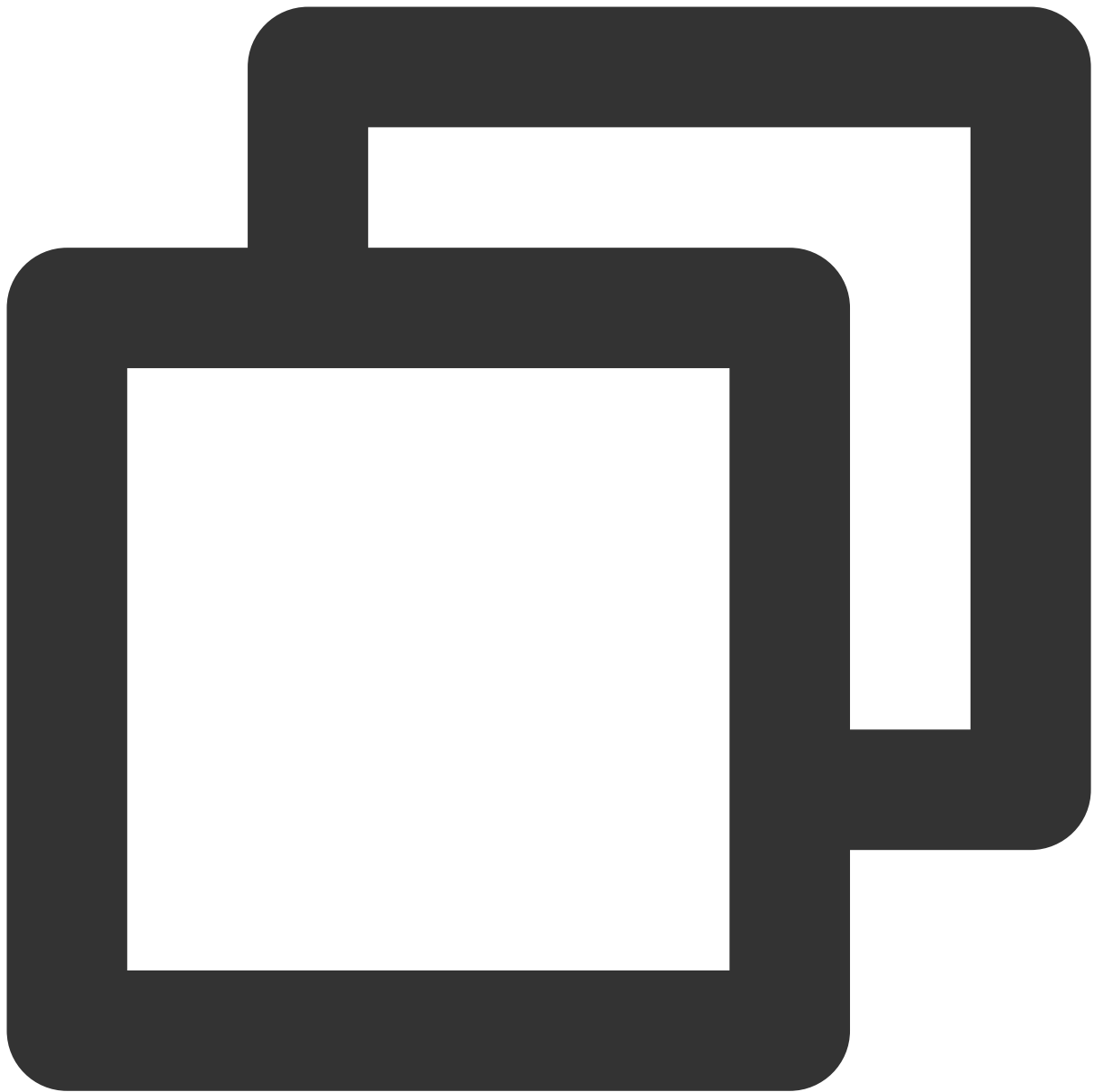
Format PFX umumnya digunakan pada Windows Server.

Konversi sertifikat:



```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

Konversi kunci privat:



```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes  
^^^
```

Anda dapat mengonversi sertifikat dalam format CER/CRT ke PEM dengan langsung memodifikasi nama ekstensi file. Misalnya, Anda dapat langsung mengganti nama file sertifikat `servertest.crt` sebagai `servertest.pem` .

Autentikasi Satu Arah dan Autentikasi Bersama SSL

Waktu update terbaru : 2024-01-04 20:53:33

Secure Sockets Layer (SSL) adalah protokol keamanan yang dirancang untuk memastikan keamanan dan integritas data dalam komunikasi Internet. Dokumen ini memperkenalkan autentikasi satu arah dan autentikasi bersama SSL.

Keterangan :

Ketika membuat pendengar SSL TCP atau pendengar HTTPS untuk instance CLB, Anda dapat memilih autentikasi satu arah atau autentikasi bersama sebagai metode parsing SSL. Untuk informasi selengkapnya, lihat [Mengonfigurasi Pendengar SSL TCP](#) dan [Mengonfigurasi Pendengar HTTPS](#).

Perbedaan Antara Autentikasi Satu Arah dengan Autentikasi Bersama SSL

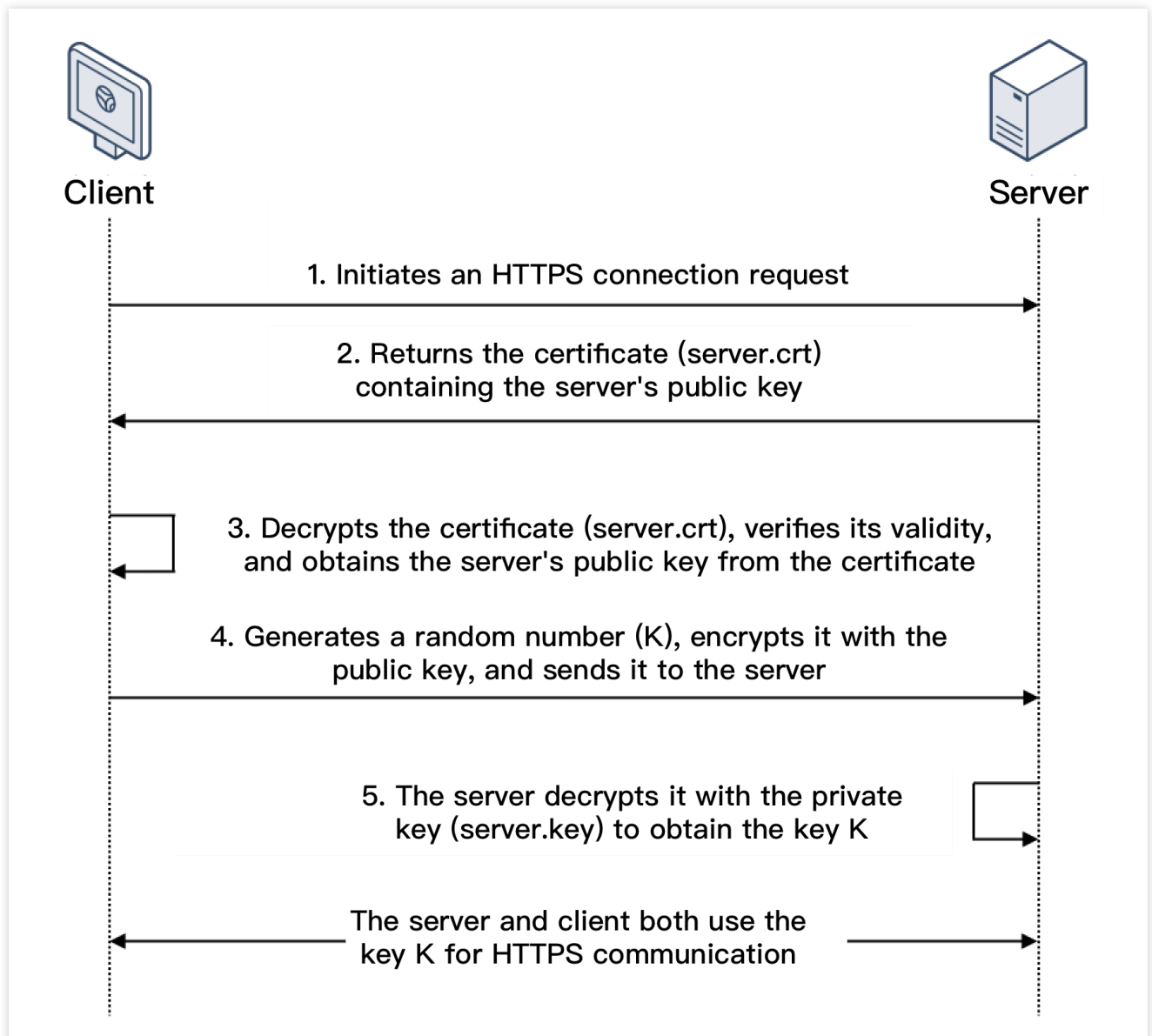
Untuk [autentikasi satu arah SSL](#), sertifikat hanya diperlukan di server tetapi klien tidak memerlukannya; sedangkan [autentikasi bersama SSL](#), sertifikat diperlukan baik di server maupun klien.

Dibandingkan autentikasi bersama SSL, autentikasi satu arah tidak memerlukan verifikasi sertifikat klien dan negosiasi skema enkripsi di server. Meskipun skema enkripsi yang dikirimkan oleh server ke klien tidak dienkripsi, keamanan autentikasi SSL akan tetap terjaga.

Aplikasi web umumnya memiliki banyak pengguna dan verifikasi identitas pengguna tidak diperlukan pada lapisan komunikasi sehingga autentikasi satu arah SSL dapat digunakan. Namun, klien yang ingin terhubung ke aplikasi keuangan mungkin memerlukan verifikasi identitas sehingga mereka harus menggunakan autentikasi bersama SSL

Autentikasi Satu Arah SSL

Dalam autentikasi satu arah SSL, hanya identitas server yang perlu diverifikasi, identitas klien tidak perlu. Proses autentikasi satu arah SSL diperlihatkan dalam gambar di bawah ini:



1. Klien membuat permintaan koneksi HTTPS ke server beserta versi protokol SSL yang didukung, algoritme enkripsi, nomor acak yang dihasilkan, dan informasi lainnya.

2. Server akan mengembalikan versi protokol SSL, algoritme enkripsi, nomor acak yang dihasilkan, sertifikat server (server.crt), dan informasi lainnya kepada klien.

3. Klien akan memverifikasi validitas sertifikat (server.crt) terkait faktor di bawah ini dan mengambil kunci publik server dari sertifikat.

Apakah sertifikat telah kedaluwarsa.

Apakah sertifikat dibatalkan.

Apakah sertifikat tepercaya

Apakah nama domain yang diminta sama dengan nama domain dalam sertifikat yang diterima.

4. Setelah sertifikat diverifikasi, klien akan membuat nomor acak (K kunci; yang digunakan sebagai kunci enkripsi simetri untuk komunikasi), mengenkripsinya menggunakan kunci publik yang diperoleh dari sertifikat server, lalu mengirimkannya ke server.

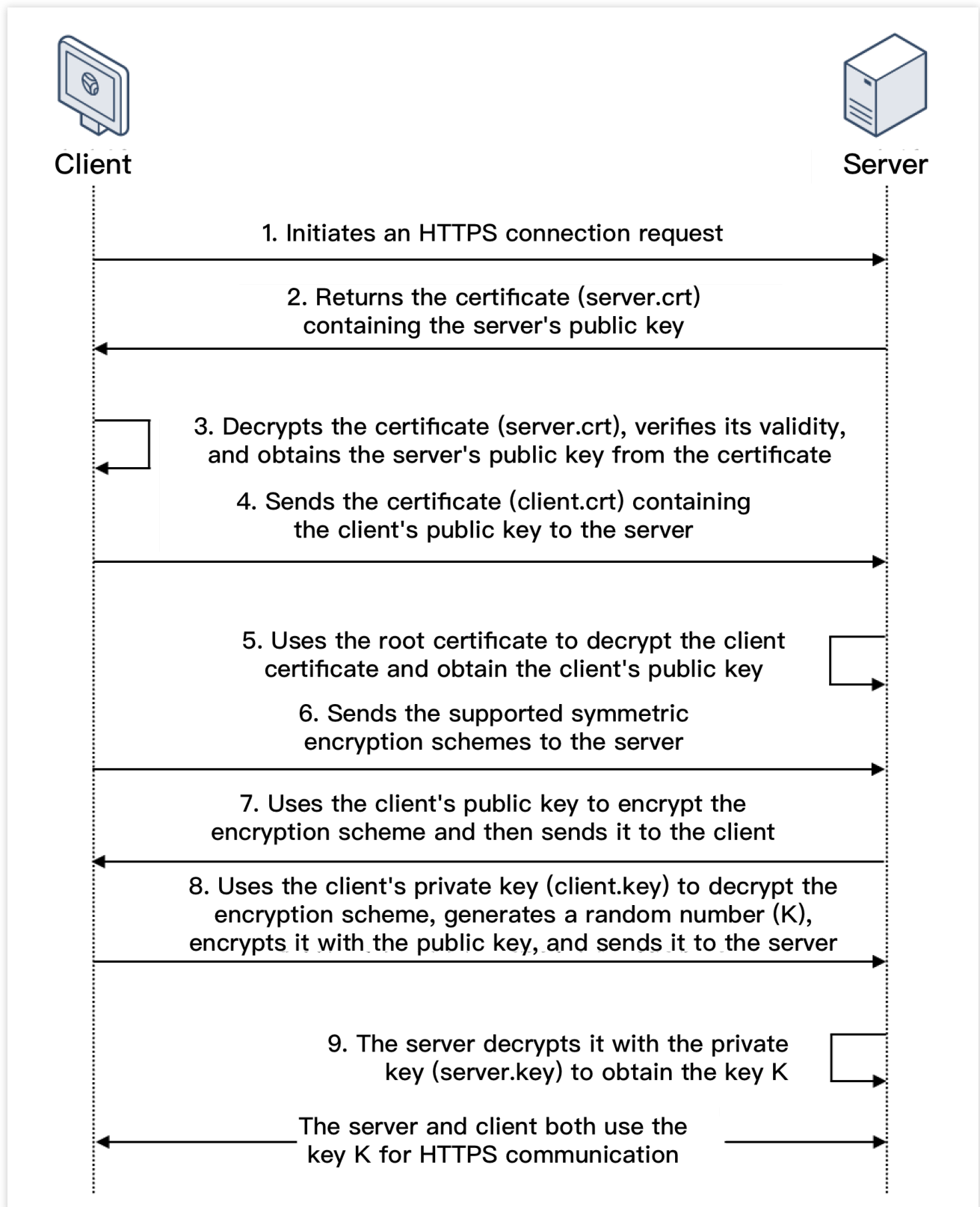
5. Setelah menerima informasi yang dienkripsi, server akan menggunakan kunci privatnya (server.key) untuk mendekripsi guna mendapatkan kunci enkripsi simetri (K kunci).

Kunci enkripsi simetri (K kunci) akan digunakan oleh server dan klien untuk berkomunikasi guna menjamin keamanan informasi.

i.

Autentikasi Bersama SSL

Dalam autentikasi bersama SSL, identitas server maupun identitas klien perlu diverifikasi. Proses autentikasi bersama SSL diperlihatkan dalam gambar di bawah ini:



1. Klien membuat permintaan koneksi HTTPS ke server beserta versi protokol SSL yang didukung, algoritme enkripsi, nomor acak yang dihasilkan, dan informasi lainnya.

2. Server akan mengembalikan versi protokol SSL, algoritme enkripsi, nomor acak yang dihasilkan, sertifikat server (server.crt), dan informasi lainnya kepada klien.

3.Klien akan memverifikasi validitas sertifikat (server.crt) terkait faktor di bawah ini dan mengambil kunci publik server dari sertifikat.

Apakah sertifikat telah kedaluwarsa.

Apakah sertifikat dibatalkan.

Apakah sertifikat tepercaya

Apakah nama domain yang diminta sama dengan nama domain dalam sertifikat yang diterima.

4.Server akan meminta klien untuk mengirimkan sertifikat klien (client.crt), dan klien akan melakukan permintaan tersebut.

5.Server memverifikasi sertifikat klien (client.crt).Setelah diverifikasi, server akan menggunakan sertifikat root untuk mendekripsi sertifikat klien dan mendapatkan kunci publik klien.

6.Klien akan mengirimkan skema enkripsi simetri yang didukung ke server.

7.Server akan memilih skema enkripsi dengan tingkat enkripsi tertinggi dari skema yang dikirimkan oleh klien, menggunakan kunci publik klien untuk mengenkripsi, lalu mengembalikannya kepada klien.

8.Klien akan menggunakan kunci privatnya (client.key) untuk mendekripsi skema enkripsi dan membuat nomor acak (K kunci; yang digunakan sebagai kunci enkripsi simetri untuk komunikasi), mengenkripsinya menggunakan kunci publik yang diperoleh dari sertifikat server, lalu mengirimkannya ke server.

9.Setelah menerima informasi yang dienkripsi, server akan menggunakan kunci privatnya (server.key) untuk mendekripsi guna mendapatkan kunci enkripsi simetri (K kunci).

Kunci enkripsi simetri (K kunci) akan digunakan oleh server dan klien untuk berkomunikasi guna menjamin keamanan informasi.

Dokumen yang Relevan

[Persyaratan Sertifikat dan Konversi Format Sertifikat](#)

Pengelolaan Log

Ikhtisar Log Akses

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung konfigurasi log akses untuk mengumpulkan dan mencatat detail setiap permintaan klien, seperti waktu permintaan, jalur permintaan, IP dan port klien, kode pengembalian, dan waktu respons. Fitur ini dapat membantu Anda lebih memahami permintaan klien, memecahkan masalah, dan menganalisis perilaku pengguna.

Keterangan :

Hanya CLB Lapisan 7 yang mendukung konfigurasi log akses.

Fitur ini hanya tersedia di wilayah yang tercantum di bawah ini.

Metode Penyimpanan

Log akses CLB dapat disimpan di [Cloud Log Service \(CLS\)](#): CLS adalah platform layanan log lengkap yang menyediakan beragam layanan log termasuk kumpulan log, penyimpanan, pencarian, analisis, ekspor real-time, dan pengiriman. Layanan ini akan membantu Anda menerapkan operasi bisnis, pemantauan keamanan, audit log, dan analisis log.

| Item | Menyimpan Log Akses di CLS |
|------------------------------------|--|
| Detail waktu untuk menampilkan log | Menit |
| Pencarian online | Didukung |
| Sintaks pencarian | Pencarian khusus teks, pencarian nilai kunci, pencarian kata kunci fuzzy, dll. Untuk informasi selengkapnya, lihat Sintaks Pencarian CLS Warisan . |
| Wilayah yang didukung | Guangzhou, Shanghai, Nanjing, Beijing, Chengdu, Chongqing, Hong Kong (Tiongkok), Singapura, Mumbai, Seoul, Tokyo, Silicon Valley, Virginia, Toronto, Frankfurt. |
| Tipe CLB yang didukung | CLB jaringan publik/jaringan privat |
| Tautan upstream dan downstream | Log CLS dapat dikirimkan ke COS, dan diekspor ke CKafka untuk diproses lebih lanjut. |
| Retensi log | Tencent Cloud tidak menyimpan log akses secara default. Fitur penyimpanan dapat dikonfigurasi sesuai kebutuhan. |

Operasi yang Relevan

[Menyimpan Log Akses di CLS](#)

Melihat Log Operasi

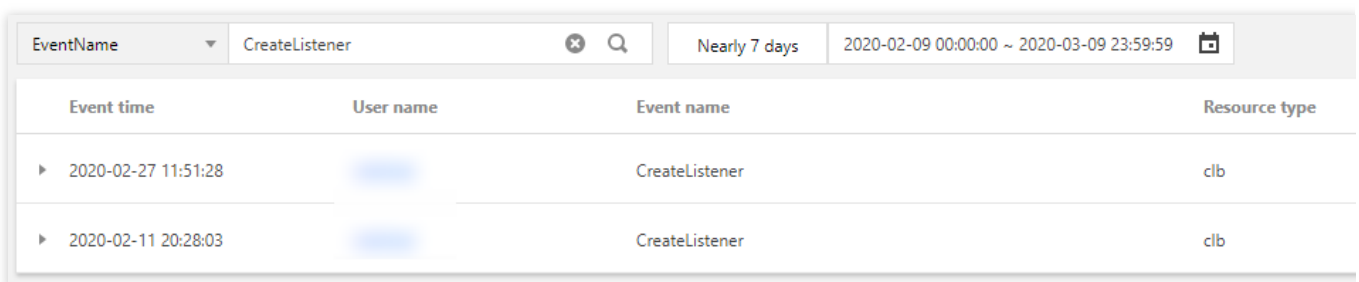
Waktu update terbaru : 2024-01-04 20:53:33

Anda dapat membuat kueri dan mengunduh riwayat operasi CLB di [Konsol CloudAudit](#).

[CloudAudit](#) memungkinkan Anda memantau, memeriksa kepatuhan, meninjau operasional, dan meninjau risiko akun Tencent Cloud Anda. Anda dapat melihat riwayat kejadian di aktivitas akun Tencent Cloud, termasuk operasi yang dijalankan melalui Tencent Cloud Console, API, alat baris perintah, dan layanan Tencent Cloud lainnya, yang memudahkan analisis keamanan, pelacakan perubahan sumber daya, dan penanggulangan masalah.

Petunjuk

1. Masuk ke [Konsol CloudAudit](#).
2. Pada bilah sisi kiri, klik **Event History** (Riwayat Kejadian) untuk membuka halaman riwayat kejadian.
3. Di halaman riwayat kejadian, Anda dapat membuat kueri operasi menurut nama pengguna, tipe sumber daya, nama sumber daya, sumber kejadian, ID kejadian, dll. Secara default, hanya sebagian data yang akan ditampilkan, dan Anda dapat mengklik **View More** (Tampilkan Lainnya) di bagian bawah halaman untuk melihat hasil lainnya.



| EventName | CreateListener | Nearly 7 days | 2020-02-09 00:00:00 ~ 2020-03-09 23:59:59 |
|-----------------------|----------------|----------------|---|
| Event time | User name | Event name | Resource type |
| ▶ 2020-02-27 11:51:28 | | CreateListener | clb |
| ▶ 2020-02-11 20:28:03 | | CreateListener | clb |

4. Klik

▶ di samping kiri operasi untuk menampilkan detail seperti kunci akses, kode kesalahan, dan ID kejadian. Anda juga dapat mengklik **View Event** (Tampilkan Kejadian) untuk melihat detail kejadian.

| Event time | User name | Event name | Resource type |
|----------------------------|---------------------|----------------|---------------|
| 2020-02-27 11:51:28 | roleUser | CreateListener | clb |
| access key | | CAM Error Code | 0 |
| Event ID | f | Event Region | ap-guangzhou |
| Event name | CreateListener | Event source | c |
| Event time | 2020-02-27 11:51:28 | Request ID | |
| Source IP address | | User name | |
| Resource Region | gz | | |
| View event | | | |

Mengonfigurasi Log Akses

Waktu update terbaru : 2024-01-04 20:53:33

CLB mendukung konfigurasi log akses lapisan 7 (HTTP/HTTPS) yang dapat membantu Anda lebih memahami permintaan klien, memecahkan masalah, dan menganalisis perilaku pengguna. Saat ini, log akses dapat disimpan di CLS, dilaporkan dengan interval setiap menit, dan dicari secara online dengan beberapa aturan.

Log akses CLB umumnya digunakan untuk dengan cepat menemukan dan memecahkan masalah. Fitur pencatatan akses mencakup pelaporan log, penyimpanan, dan pencarian:

Pelaporan log memberikan layanan terbaik, yaitu memprioritaskan penerusan layanan dibandingkan pelaporan log.

Pencarian dan penyimpanan log memberikan SLA berdasarkan layanan penyimpanan yang saat ini digunakan.

Keterangan :

Saat ini, log akses dapat disimpan di CLS hanya untuk protokol lapisan 7 (HTTP/HTTPS) tetapi tidak untuk protokol lapisan 4 (TCP/UDP/TCP SSL).

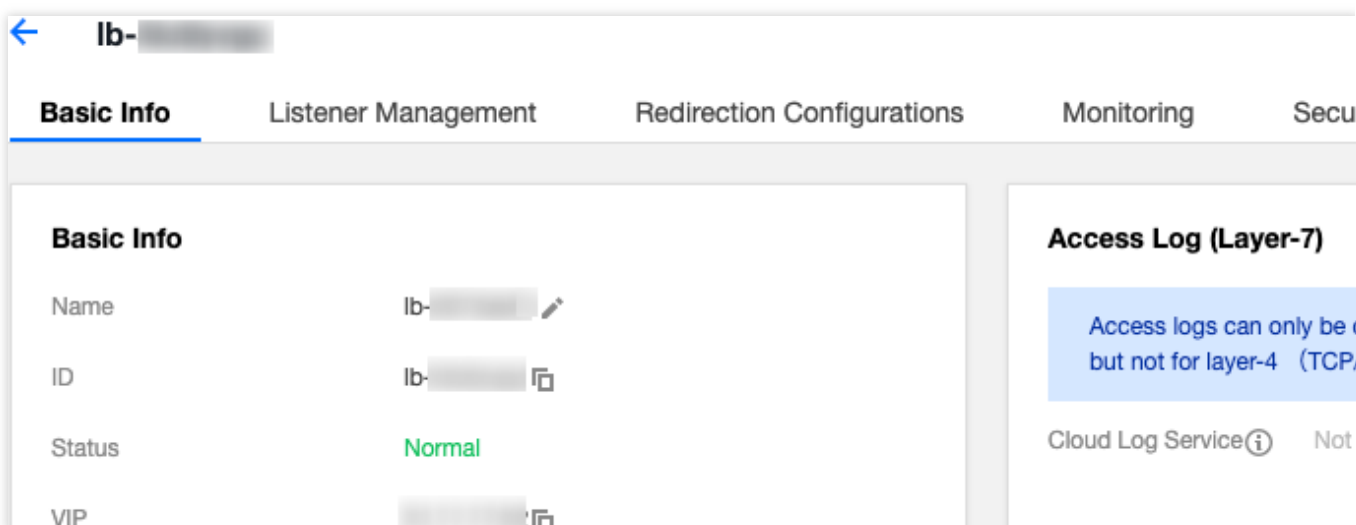
Menyimpan log akses CLB ke CLS kini bebas biaya. Anda hanya perlu membayar layanan CLS.

Fitur ini hanya didukung di wilayah yang menyediakan CLS. Lihat [Wilayah Ketersediaan](#).

Metode 1: Pencatatan Akses Instance Tunggal

Langkah 1. Mengaktifkan penyimpanan log akses di CLS

1. Masuk konsol CLB, lalu klik **Instance Management** (Manajemen Instance) di bilah sisi kiri.
2. Klik ID instance CLB untuk membuka halaman **Instance Management** (Manajemen Instance).
3. Klik ikon pensil pada modul **Access Log (Layer-7)** (Log Akses (Lapisan 7)) di halaman **Basic Information** (Informasi Dasar).



4. Di jendela pop-up **Modify CLS Log Storage Location** (Modifikasi Lokasi Penyimpanan Log CLS), aktifkan pencatatan dan pilih logset tujuan serta topik log untuk penyimpanan log akses, lalu klik **Submit** (Kirim). Jika Anda

belum membuat logset atau topik log, silakan buat sumber daya yang relevan, lalu pilih sumber daya tersebut sebagai lokasi penyimpanan.

Keterangan :

Sebaiknya Anda menggunakan topik log yang ditandai dengan "CLB" dalam logset clb_logset. Perbedaan antara topik log yang bertanda "CLB" dengan topik log umum yaitu:

Topik log CLB secara otomatis dapat membuat indeks, sedangkan topik log umum harus membuat indeks secara manual.

Dasbor untuk topik log CLB disediakan secara default, tetapi untuk topik log umum harus dikonfigurasi secara manual.

5. Klik logset atau topik log untuk mengalihkan ke halaman pencarian log di CLS.

6. (Opsional) Untuk menonaktifkan pencatatan, klik ikon pensil untuk membuka jendela **Modify CLS Log Storage Location** (Modifikasi Lokasi Penyimpanan Log CLS), lalu nonaktifkan.

Langkah 2. Mengonfigurasi indeks topik log

Keterangan :

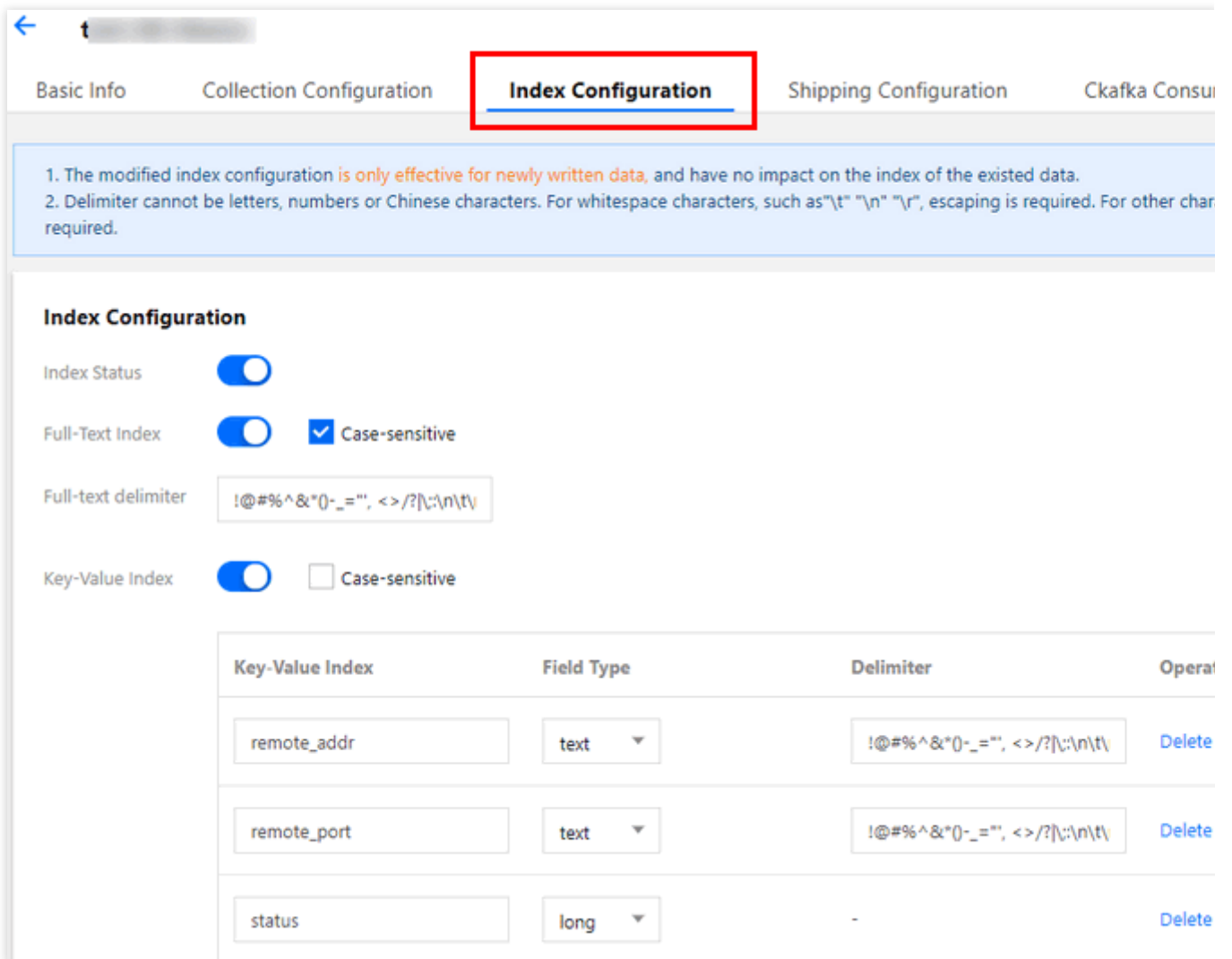
Jika log akses dikonfigurasi untuk satu instance, Anda harus mengonfigurasi indeks untuk topik log; jika tidak, log tidak akan dapat ditemukan.

Indeks yang direkomendasikan yaitu sebagai berikut:

| Indeks Nilai Utama | Tipe Bidang | Pemisah |
|--------------------|-------------|--------------------------|
| server_addr | teks | Tidak memerlukan pemisah |
| server_nama | teks | Tidak memerlukan pemisah |
| http_host | teks | Tidak memerlukan pemisah |
| status | panjang | - |
| vip_vpcid | panjang | - |

Langkah-langkah adalah sebagai berikut:

1. Masuk ke [Konsol CLS](#), lalu klik **Log Topic** (Topik Log) di bilah sisi kiri.
2. Klik ID topik log target di halaman "Log Topic" (Topik Log).
3. Di halaman detail topik log, pilih tab **Index Configuration** (Konfigurasi Indeks), lalu klik **Edit** (Edit) untuk menambahkan indeks. Lihat [Mengonfigurasi Indeks](#) untuk informasi selengkapnya tentang konfigurasi indeks.



Basic Info Collection Configuration **Index Configuration** Shipping Configuration Ckafka Consum

1. The modified index configuration is only effective for newly written data, and have no impact on the index of the existed data.
2. Delimiter cannot be letters, numbers or Chinese characters. For whitespace characters, such as "\t" "\n" "\r", escaping is required. For other char required.

Index Configuration

Index Status

Full-Text Index Case-sensitive

Full-text delimiter

Key-Value Index Case-sensitive

| Key-Value Index | Field Type | Delimiter | Operat |
|--|------------|---|--------|
| <input type="text" value="remote_addr"/> | text | <input <>="" '="" ,="" ?[\;:\n\t\"="" type="text" value="!@#%^&*()-_=\"/> | Delete |
| <input type="text" value="remote_port"/> | text | <input <>="" '="" ,="" ?[\;:\n\t\"="" type="text" value="!@#%^&*()-_=\"/> | Delete |
| <input type="text" value="status"/> | long | - | Delete |

4. Hasil konfigurasi indeks seperti yang ditunjukkan di bawah ini:

Index Configuration Edit

Index Status **Enabled**

Full-Text Index **Enabled** Case-sensitive

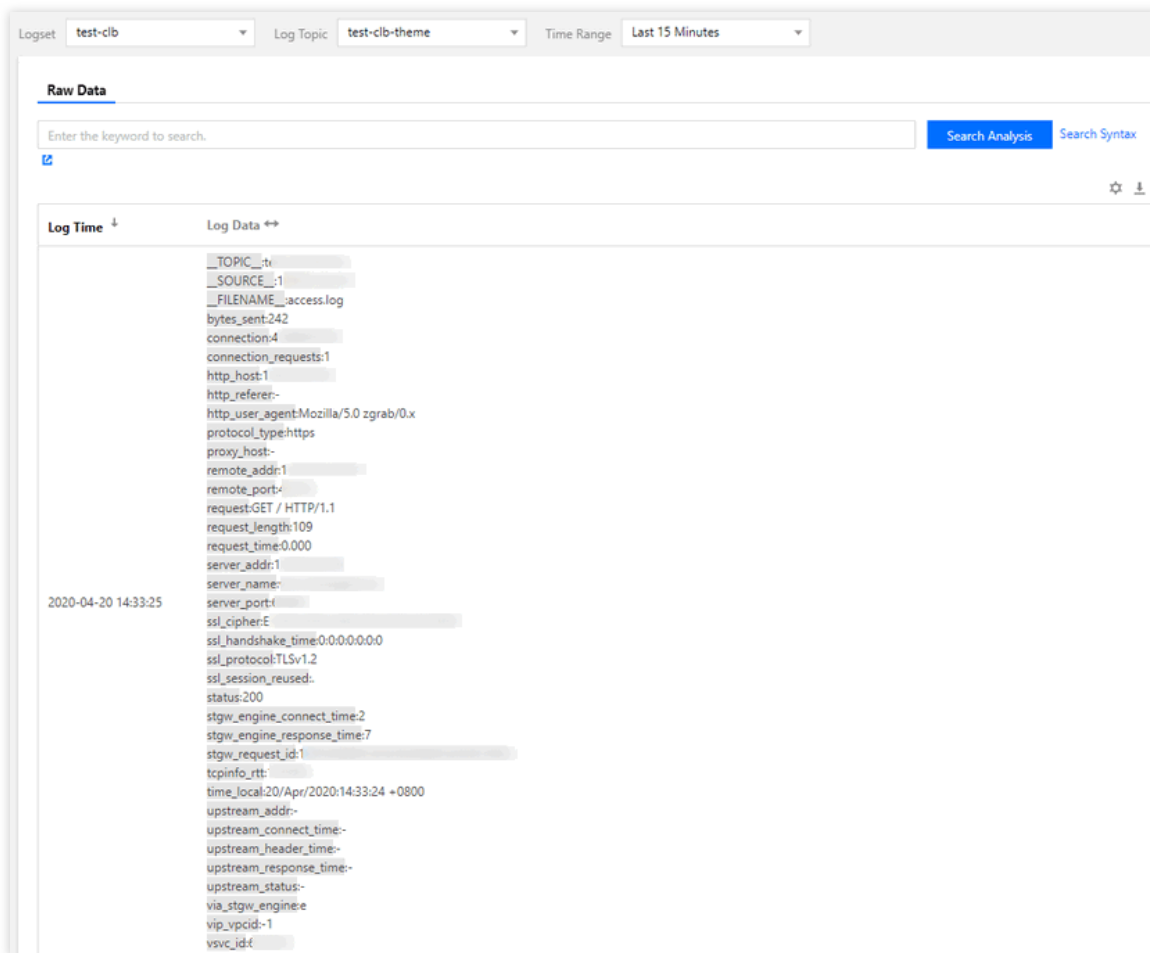
Full-text delimiter `!@#%^&*()-_=", <>/?\|:~\n\t\r{}[]`

Key-Value Index **Enabled**

| Key-Value Index | Field Type | Delimiter |
|-----------------|------------|-----------------------------------|
| remote_addr | text | !@#%^&*()-_=", <>/?\ :~\n\t\r{}[] |
| remote_port | text | !@#%^&*()-_=", <>/?\ :~\n\t\r{}[] |
| status | long | None |
| server_addr | text | !@#%^&*()-_=", <>/?\ :~\n\t\r{}[] |
| server_name | text | !@#%^&*()-_=", <>/?\ :~\n\t\r{}[] |
| http_host | text | !@#%^&*()-_=", <>/?\ :~\n\t\r{}[] |
| request_time | double | None |

Langkah 3.Melihat log akses

1. Masuk ke [Konsol CLS](#), lalu klik **Search and Analysis** (Pencarian dan Analisis) di bilah sisi kiri.
2. Di halaman **Search Analysis** (Cari Analisis), pilih logset, topik log, dan rentang waktu, lalu klik **Search Analysis** (Cari Analisis) untuk mencari log akses yang dilaporkan oleh CLB ke CLS.Lihat [Sintaks Pencarian CLS Lama](#) untuk informasi selengkapnya tentang sintaks pencarian.



Metode 2: Konfigurasi pencatatan akses secara batch

Keterangan :

Fitur ini hanya tersedia untuk pengguna beta saat ini. Untuk menggunakan fitur ini, Anda perlu mengirimkan permohonan.

Langkah 1. Membuat logset dan topik log

Untuk mengonfigurasi log akses di CLS, Anda perlu membuat logset dan topik log terlebih dahulu.

Anda dapat langsung beralih ke [Langkah 2](#) jika sudah membuat logset dan topik log.

1. Masuk ke [Konsol CLB](#) dan pilih **Access Logs** (Log Akses) di bilah sisi kiri.
2. Di halaman **Access Logs** (Log Akses), pilih wilayah untuk logset, lalu klik **Create Logset** (Buat Logset) di bagian "Logset Information" (Informasi Logset).
3. Dalam kotak dialog pop-up **"Create Logset"** (Buat Logset), atur periode retensi dan klik **Save** (Simpan).

Keterangan :

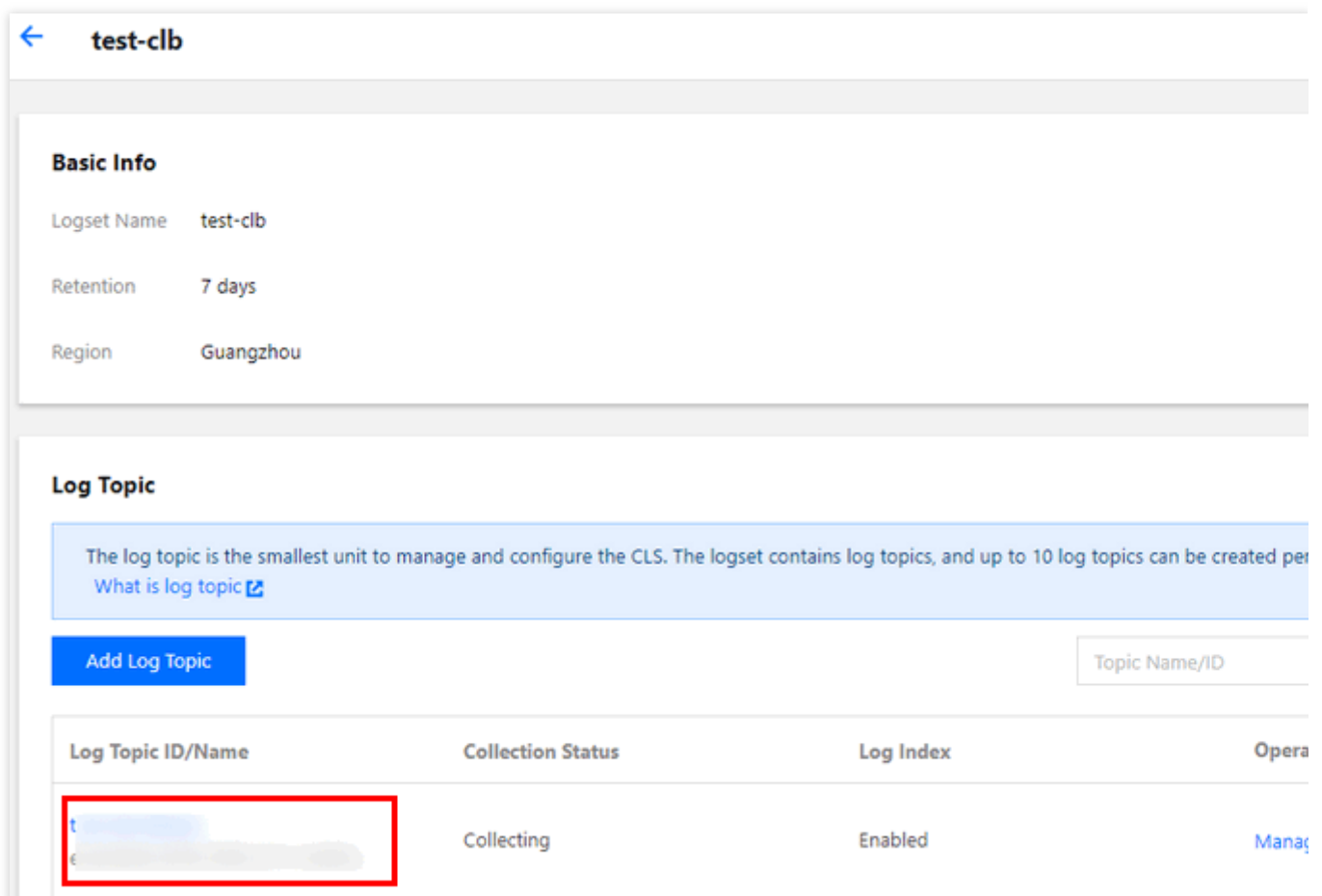
Anda hanya dapat membuat satu logset bernama "clb_logset" di setiap wilayah.

4. Klik **Create Log Topic** (Buat Topik Log) di bagian **Log Topic** (Topik Log) di halaman "Access Logs" (Log Akses).
5. Di jendela pop-up, pilih instance CLB yang ingin ditambahkan ke daftar di sebelah kanan, lalu klik **Save** (Simpan).

Keterangan :

Ketika membuat topik log, Anda dapat menambahkan instance CLB sesuai kebutuhan. Untuk menambahkan instance, pilih topik log dalam daftar, lalu klik **Manage** (Kelola) di kolom operasi. Setiap instance CLB hanya dapat ditambahkan ke satu topik log.

Satu logset dapat berisi beberapa topik log. Anda dapat mengelompokkan log CLB dalam berbagai topik log yang akan ditandai dengan "CLB".



The screenshot shows the 'test-club' logset configuration page. Under the 'Log Topic' section, there is a table with the following data:

| Log Topic ID/Name | Collection Status | Log Index | Opera |
|-------------------|-------------------|-----------|-------|
| t e | Collecting | Enabled | Manag |

6. (Opsional) Untuk menonaktifkan pencatatan, cukup klik **Disable** (Nonaktifkan).

Langkah 2. Melihat log akses

Tanpa perlu konfigurasi manual apa pun, CLB telah dikonfigurasi otomatis dengan pencarian indeks menurut log akses penting. Anda dapat langsung membuat kueri log akses melalui pencarian dan analisis.

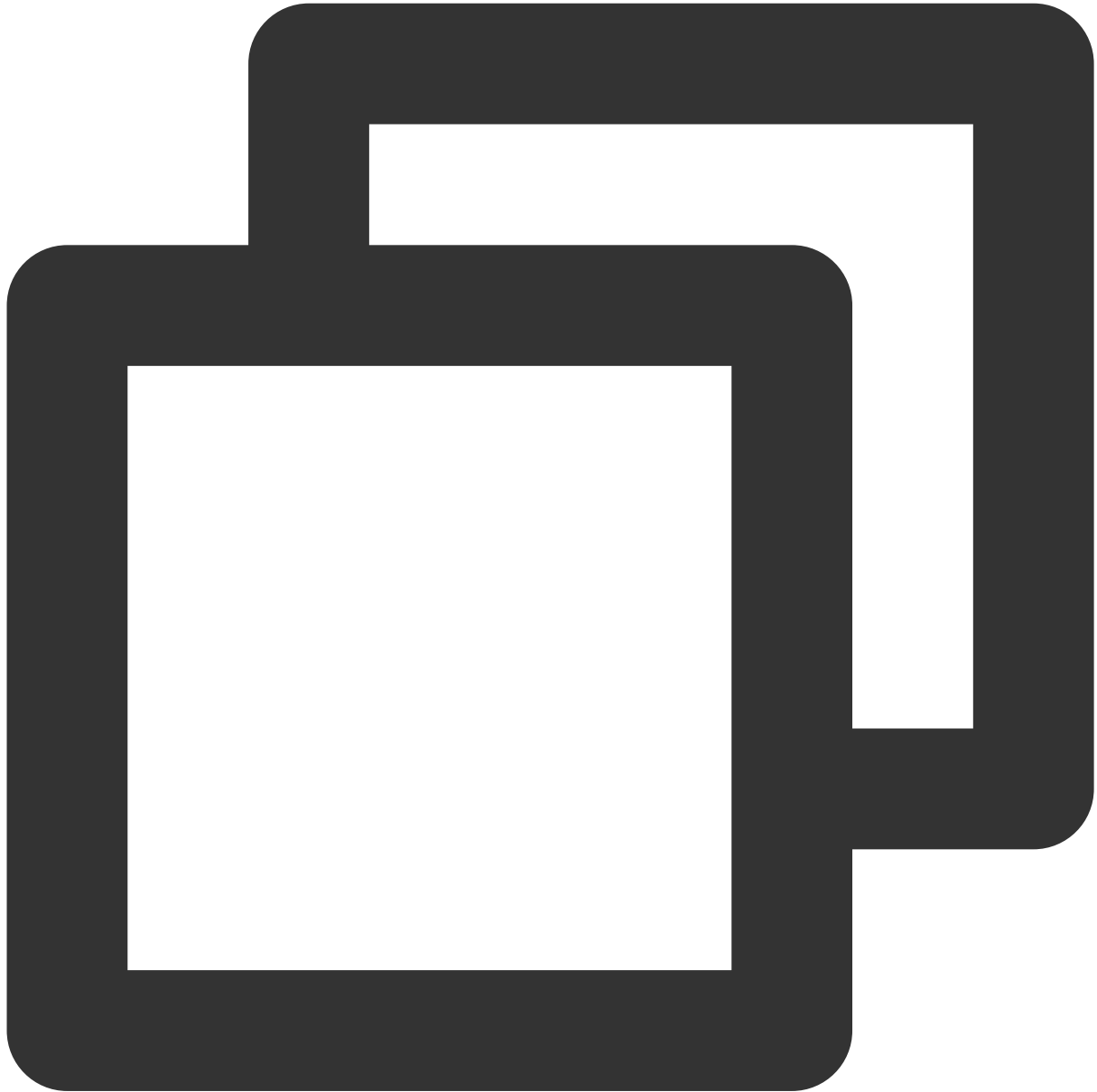
1. Masuk ke [Konsol CLB](#) dan pilih **Access Logs** (Log Akses) di bilah sisi kiri.
2. Pilih topik log, lalu klik **Search** (Pencarian) di kolom operasi untuk beralih ke halaman **Search Analysis** (Cari Analisis) di [Konsol CLS](#).
3. Di halaman **Search Analysis** (Cari Analisis), masukkan sintaks pencarian dalam kotak input, pilih rentang waktu, lalu klik **Search Analysis** (Cari Analisis) untuk mencari log akses yang dilaporkan oleh CLB ke CLS.

Keterangan :

Lihat [Sintaks dan Aturan](#) untuk informasi selengkapnya tentang sintaks pencarian.

Format Log dan Deskripsi Variabel

Format log



```
[${stgw_request_id}] [${time_local}] [${protocol_type}] [${server_addr}:${server_port}] [${se
```

Tipe bidang

Saat ini, CLS mendukung tiga tipe bidang berikut:

| | |
|--|--|
| | |
|--|--|

| Nama | Deskripsi Tipe |
|--------|-----------------------------|
| teks | Tipe teks |
| long | Tipe integer (Int 64) |
| double | Tipe poin floating (64 bit) |

Deskripsi variabel log

| Variabel | Deskripsi | Tipe Bidangtext |
|-----------------|---|-----------------|
| stgw_request_id | ID Permintaan. | text |
| time_local | Waktu akses dan zona waktu, misalnya "01/Jul/2019:11:11:00 +0800" dengan "+0800" mewakili UTC+8, yaitu waktu Beijing. | text |
| protocol_type | Tipe protokol (HTTP/HTTPS/SPDY/HTTP2/WS/WSS). | teks |
| server_addr | CLB VIP. | teks |
| server_port | CLB VPort, yaitu port pendengar. | long |
| server_name | `server_name` aturan, yaitu nama domain yang dikonfigurasi di pendengar CLB. | teks |
| remote_addr | IP Klien. | teks |
| remote_port | Port klien. | long |
| status | Kode status yang dikembalikan kepada klien. | long |
| upstream_addr | Alamat RS. | teks |
| upstream_status | Kode status yang dikembalikan oleh RS ke CLB. | teks |
| proxy_host | ID Stream. | teks |
| request | Baris permintaan. | teks |
| request_length | Jumlah byte permintaan yang diterima dari klien. | long |
| bytes_sent | Jumlah byte yang dikirimkan kepada klien. | long |
| http_host | Nama domain permintaan, yaitu host header HTTP. | teks |

| | | |
|------------------------|--|--------|
| http_user_agent | Bidang `user_agent` header HTTP. | teks |
| http_referer | Sumber permintaan HTTP. | teks |
| request_time | Waktu pemrosesan permintaan. Penghitungan waktu dimulai ketika byte pertama diterima dari klien dan berhenti ketika byte terakhir dikirimkan kepada klien, yaitu total waktu yang diperlukan untuk menyelesaikan seluruh proses, ketika permintaan klien mencapai instance CLB, instance CLB akan meneruskan permintaan ke RS, RS akan merespons dan mengirimkan data ke instance CLB, dan akhirnya instance CLB meneruskan data kepada klien. | double |
| upstream_response_time | Waktu yang diperlukan untuk menyelesaikan seluruh proses permintaan backend. Penghitungan waktu dimulai ketika instance CLB terhubung dengan RS dan berhenti ketika RS menerima permintaan dan merespons. | double |
| upstream_connect_time | Waktu yang diperlukan untuk membuat koneksi TCP dengan RS. Penghitungan waktu dimulai ketika instance CLB terhubung dengan RS dan berhenti ketika mengirimkan permintaan HTTP. | double |
| upstream_header_time | Waktu yang diperlukan untuk menerima header HTTP dari RS. Penghitungan waktu dimulai ketika instance CLB terhubung dengan RS dan berhenti ketika header respons HTTP diterima dari RS. | double |
| tcpinfo_rtt | RTT koneksi TCP. | long |
| connection | ID Koneksi. | long |
| connection_requests | Jumlah permintaan dalam koneksi. | long |
| ssl_handshake_time | Waktu yang diperlukan untuk menyelesaikan handshake SSL. | double |
| ssl_cipher | Rangkaian cipher SSL. | teks |
| ssl_protocol | Versi protokol SSL. | teks |
| vip_vpcid | ID VPC dari CLB VIP; `vip_vpcid` instance CLB jaringan publik yaitu `-1`. | long |
| request | Metode permintaan. Hanya mendukung permintaan POST dan GET. | teks |
| uri | Pengidentifikasi Sumber Daya. | teks |
| server_protocol | Protokol yang digunakan untuk CLB. | teks |

Item log pencarian default

Bidang berikut dapat ditemukan dalam logset dengan "CLB" secara default:

| Bidang Indeks | Deskripsi | Tipe Bidang |
|------------------------|--|-------------|
| time_local | Waktu akses dan zona waktu, misalnya "01/Jul/2019:11:11:00 +0800" dengan "+0800" mewakili UTC+8, yaitu waktu Beijing. | text |
| protocol_type | Tipe protokol (HTTP/HTTPS/SPDY/HTTP2/WS/WSS). | teks |
| server_addr | CLB VIP. | teks |
| server_name | `server_name` aturan, yaitu nama domain yang dikonfigurasi di pendengar CLB. | teks |
| remote_addr | IP Klien. | teks |
| status | Kode status yang dikembalikan kepada klien. | long |
| upstream_addr | Alamat RS. | teks |
| upstream_status | Kode status yang dikembalikan oleh RS ke CLB. | teks |
| request_length | Jumlah byte permintaan yang diterima dari klien. | long |
| bytes_sent | Jumlah byte yang dikirimkan kepada klien. | long |
| http_host | Nama domain permintaan, yaitu host header HTTP. | teks |
| request_time | Waktu pemrosesan permintaan. Penghitungan waktu dimulai ketika byte pertama diterima dari klien dan berhenti ketika byte terakhir dikirimkan kepada klien, yaitu total waktu yang diperlukan untuk menyelesaikan seluruh proses, ketika permintaan klien mencapai instance CLB, instance CLB akan meneruskan permintaan ke RS, RS akan merespons dan mengirimkan data ke instance CLB, dan akhirnya instance CLB meneruskan data kepada klien. | double |
| upstream_response_time | Waktu yang diperlukan untuk menyelesaikan seluruh proses permintaan backend. Penghitungan waktu dimulai ketika instance CLB terhubung dengan RS dan berhenti ketika RS menerima permintaan dan merespons. | double |

Pemantauan dan Peringatan

Mendapatkan Data Pemantauan

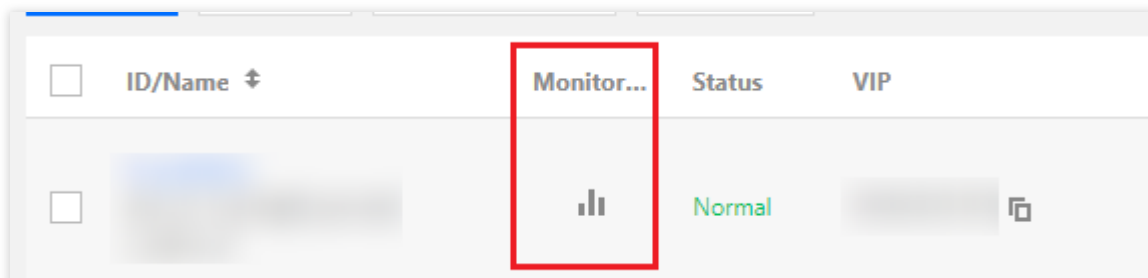
Waktu update terbaru : 2024-01-04 20:53:33

Tencent Cloud Monitor mengumpulkan dan menampilkan data dari instance CLB dan server asli, membantu Anda memperoleh statistik CLB, memverifikasi apakah sistem berjalan normal dan membuat alarm. Untuk informasi selengkapnya mengenai Tencent Cloud Monitor, lihat dokumentasi [Cloud Monitor Dasar](#).

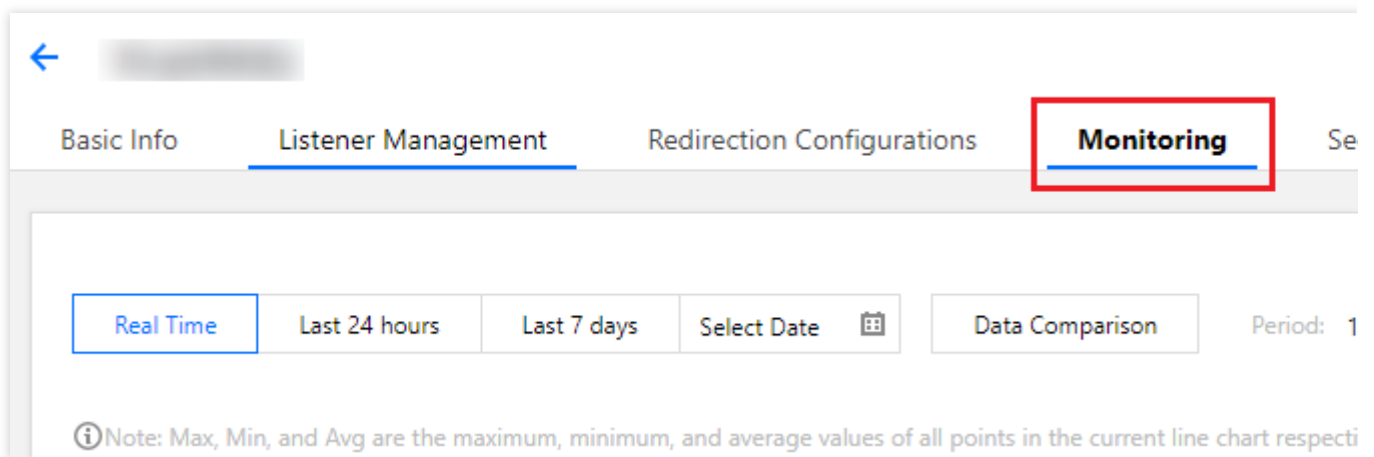
Tencent Cloud menyediakan fitur Cloud Monitor untuk semua pengguna secara default dan tidak membutuhkan aktivasi manual. Anda bisa menggunakan Cloud Monitor untuk mengumpulkan data pemantauan instance CLB Anda dan menampilkan data dengan metode berikut.

Metode Konsol CLB

1. Masuk ke [Konsol CLB](#), klik ikon bilah pemantauan di samping ID instance CLB, dan kemudian jelajahi data performa instance tersebut di jendela floating.



2. Klik ID/Nama instance CLB untuk mengakses halaman detailnya. Klik **Monitoring** (Pemantauan) untuk melihat data pemantauannya.



Metode Konsol Cloud Monitor

Masuk ke [Konsol Cloud Monitor](#) untuk melihat data pemantauan CLB. Klik [Cloud Load Balancer](#) (Penyeimbang Beban Cloud) di bilah sisi kiri, dan klik ID/nama instance CLB untuk mengakses halaman detail pemantauannya. Anda bisa melihat data pemantauan instance CLB dan memperluas daftar drop-down untuk melihat informasi pemantauan pendengar dan server asli.

Metode API

Gunakan `GetMonitorData` API untuk mendapatkan data pemantauan semua produk. Untuk informasi selengkapnya, lihat [GetMonitorData](#), [Metrik Pemantauan CLB Jaringan Publik](#), [Protokol Lapisan 4 CLB Jaringan Pribadi](#).

Metrik Pemantauan

Waktu update terbaru : 2024-01-04 20:53:33

Cloud Monitor mengumpulkan data mentah dari instance CLB yang sedang berjalan dan menampilkan entri data dalam grafik intuitif. Statistik akan disimpan selama satu bulan secara default. Anda bisa mengamati operasi instance dalam satu bulan untuk terus mengetahui status layanan aplikasi.

Anda bisa membuka [Konsol Cloud Monitor](#) untuk melihat data pemantauan CLB. Klik **Cloud Product Monitoring** (Pemantauan Produk Cloud) -> **Cloud Load Balancer (Penyeimbang Beban Cloud)** dan kemudian klik ID instance CLB untuk masuk ke halaman detail pemantauan. Anda bisa melihat data pemantauan instance CLB, dan memperluasnya untuk melihat informasi pemantauan pendengar dan server asli.

Level Instance CLB

Keterangan :

Pemanfaatan bandwidth masuk dan pemanfaatan bandwidth keluar berlaku untuk semua wilayah layanan kecuali Tokyo dan Bangkok. Kedua metrik ini hanya untuk akun tagihan per IP. Untuk memeriksa tipe akun Anda, silakan lihat [Memeriksa Tipe Akun](#).

| Metrik | Unit | Deskripsi |
|----------------------------------|---------|---|
| Bandwidth masuk | Mbps | Bandwidth yang digunakan klien untuk mengakses CLB melalui jaringan publik dalam periode referensi. |
| Bandwidth keluar | Mbps | Bandwidth yang digunakan CLB untuk mengakses jaringan publik dalam periode referensi. |
| Paket masuk | Paket | Jumlah paket data permintaan yang diterima oleh CLB per detik dalam periode referensi. |
| Paket keluar | Paket | Jumlah paket data yang dikirim oleh CLB per detik dalam periode referensi. |
| Koneksi yang diturunkan | Koneksi | Jumlah koneksi yang diturunkan oleh CLB per detik dalam periode referensi. |
| Bandwidth masuk yang diturunkan | bps | Bandwidth masuk yang diturunkan oleh CLB per detik dalam periode referensi. |
| Bandwidth keluar yang diturunkan | bps | Bandwidth keluar yang diturunkan oleh CLB per detik dalam periode referensi. |
| Paket data masuk | Paket | Jumlah paket data masuk yang diturunkan oleh CLB per detik dalam |

| | | |
|-----------------------------------|-------|---|
| yang diturunkan | | periode referensi. |
| Paket data keluar yang diturunkan | Paket | Jumlah paket data masuk yang diturunkan oleh CLB per detik dalam periode referensi. |
| Pemanfaatan bandwidth masuk | % | Pemanfaatan bandwidth masuk CLB dalam periode referensi. |
| Pemanfaatan bandwidth keluar | % | Pemanfaatan bandwidth keluar CLB dalam periode referensi. |

Level (TCP/UDP) Pendengar Lapisan 4

Pendengar lapisan 4 memungkinkan Anda melihat metrik pemantauan dalam tiga level:

Level pendengar

Level server asli

Level port server asli

| Metrik | Unit | Deskripsi |
|------------------|--------|---|
| Koneksi | Jumlah | Jumlah koneksi pada pendengar dalam periode referensi. |
| Koneksi baru | Jumlah | Jumlah koneksi baru pada pendengar dalam periode referensi. |
| Bandwidth masuk | Mbps | Bandwidth yang digunakan klien untuk mengakses CLB melalui jaringan publik dalam periode referensi. |
| Bandwidth keluar | Mbps | Bandwidth yang digunakan CLB untuk mengakses jaringan publik dalam periode referensi. |
| Paket masuk | Paket | Jumlah paket data permintaan yang diterima oleh CLB per detik dalam periode referensi. |
| Paket keluar | Paket | Jumlah paket data yang dikirim oleh CLB per detik dalam periode referensi. |

Level (HTTP/HTTPS) Pendengar Lapisan 7

Pendengar lapisan 7 memungkinkan Anda melihat metrik pemantauan dalam lima level:

Level pendengar

Level nama domain

Level jalur penerusan URL

Level server asli

Level port server asli

| Metrik | Unit | Deskripsi |
|-------------------------------|------------------|---|
| Koneksi | - | Jumlah koneksi pada pendengar dalam periode referensi. |
| Koneksi baru | - | Jumlah koneksi baru pada pendengar dalam periode referensi. |
| Bandwidth masuk | Mbps | Bandwidth yang digunakan klien untuk mengakses CLB melalui jaringan publik dalam periode referensi. |
| Bandwidth keluar | Mbps | Bandwidth yang digunakan CLB untuk mengakses jaringan publik dalam periode referensi. |
| Paket masuk | Paket | Jumlah paket data permintaan yang diterima oleh CLB per detik dalam periode referensi. |
| Paket keluar | Paket | Jumlah paket data yang dikirim oleh CLB per detik dalam periode referensi. |
| Durasi permintaan rata-rata | ms | Durasi permintaan rata-rata CLB dalam periode referensi. Durasi dimulai dari titik saat instance CLB menerima byte pertama dari klien dan berakhir saat instance CLB mengirim byte terakhir kepada klien. |
| Durasi permintaan maksimum | ms | Durasi permintaan maksimum CLB dalam periode referensi. Durasi dimulai dari titik saat instance CLB menerima byte pertama dari klien dan berakhir saat instance CLB mengirim byte terakhir kepada klien. |
| Durasi respons rata-rata | ms | Durasi respons rata-rata server asli dalam periode referensi. Durasi mengacu pada seluruh durasi permintaan, mulai dari titik saat instance CLB tersambung ke server asli dan berakhir saat server asli menerima byte respons terakhir. |
| Durasi respons maksimum | ms | Durasi respons maksimum server asli dalam periode referensi. Durasi mengacu pada seluruh durasi permintaan, mulai dari titik saat instance CLB tersambung ke server asli dan berakhir saat server asli menerima byte respons terakhir. |
| Permintaan habis waktu | Permintaan/menit | Jumlah permintaan yang habis waktu dalam periode referensi. |
| Permintaan berhasil per menit | Permintaan/menit | Jumlah permintaan CLB berhasil per menit dalam periode referensi. |
| Permintaan per detik | - | Jumlah permintaan CLB per detik dalam periode referensi, yaitu, QPS. |
| | | |

| | | |
|--|---|--|
| Kode status 2xx | - | Jumlah kode status 2xx yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 3xx | - | Jumlah kode status 3xx yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 4xx | - | Jumlah kode status 4xx yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 5xx | - | Jumlah kode status 5xx yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 404 | - | Jumlah kode status 404 yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 502 | - | Jumlah kode status 502 yang dikembalikan oleh server asli dalam periode referensi. |
| Kode status 3xx yang dikembalikan oleh CLB | - | Jumlah kode status 3xx yang dikembalikan oleh CLB dalam periode referensi (jumlah kode kembali CLB dan server asli). |
| Kode status 4xx yang dikembalikan oleh CLB | - | Jumlah kode status 4xx yang dikembalikan oleh CLB dalam periode referensi (jumlah kode kembali CLB dan server asli). |
| Kode status 5xx yang dikembalikan oleh CLB | - | Jumlah kode status 5xx yang dikembalikan oleh CLB dalam periode referensi (jumlah kode kembali CLB dan server asli). |
| Kode status 404 yang dikembalikan oleh CLB | - | Jumlah kode status 404 yang dikembalikan oleh CLB dalam periode referensi (jumlah kode kembali CLB dan server asli). |
| Kode status 502 yang dikembalikan oleh CLB | - | Jumlah kode status 502 yang dikembalikan oleh CLB dalam periode referensi (jumlah kode kembali CLB dan server asli). |

Perhatian :

Jika Anda ingin melihat data pemantauan instance CVM di bawah pendengar, silakan masuk ke [Konsol CLB](#), klik ikon bilah pemantauan di dekat ID instance CLB, dan kemudian jelajahi data performa setiap instance di jendela floating.

Mengonfigurasi Peringatan

Waktu update terbaru : 2024-01-04 20:53:33

Anda bisa membuat alarm untuk memicu alarm dan mengirim pesan alarm ke grup pengguna tertentu jika produk Tencent Cloud memenuhi syarat yang dikonfigurasi. Alarm yang dibuat bisa secara berkala menentukan apakah notifikasi alarm harus dikirimkan berdasarkan perbedaan di antara metrik yang dipantau dan ambang batas yang diberikan.

Pengguna tertentu bisa melakukan tindakan pencegahan atau perbaikan tepat waktu saat alarm terpicu. Oleh karena itu, alarm yang dibuat dengan tepat bisa membantu meningkatkan ketahanan dan keandalan aplikasi Anda. Untuk informasi selengkapnya mengenai alarm, silakan lihat [Membuat Kebijakan Alarm](#).

Anda bisa membuat kebijakan alarm dengan langkah berikut:

1. Masuk ke Konsol Monitor Cloud.
2. Klik Alarm Configuration (Konfigurasi Alarm) > Alarm Policy (Kebijakan Alarm) di bilah sisi kiri untuk masuk ke halaman konfigurasi kebijakan alarm.
3. Klik Add (Tambahkan) untuk mengonfigurasi kebijakan alarm.
4. Konfigurasi item dasar seperti yang ditunjukkan di bawah ini:

Nama Kebijakan: masukkan nama kebijakan.

Keterangan: tambahkan keterangan pada kebijakan.

Tipe Kebijakan: pilih metrik pemantauannya.

Proyek: pilih proyek sesuai kebutuhan.

5. Konfigurasi objek alarm.

Jika Anda memilih "semua objek", kebijakan alarm akan diasosiasikan dengan semua instance di bawah akun saat ini.

Jika Anda memilih "beberapa objek", kebijakan alarm akan diasosiasikan dengan instance terpilih.

Jika Anda memilih "grup Instance", kebijakan alarm akan diasosiasikan dengan grup instance terpilih.

6. Atur pemicu alarmnya. Anda bisa memilih satu templat syarat pemicu atau mengonfigurasi syarat-syarat pemicu.

Templat syarat pemicu

Aktifkan "Templat Syarat Pemicu" dan pilih templat yang dikonfigurasi dari daftar drop-down. Untuk konfigurasi selengkapnya, silakan lihat [Mengonfigurasi Templat Syarat Pemicu](#). Jika templat yang baru saja dibuat tidak ditampilkan, klik **Refresh** di sebelah kanan.

Konfigurasi syarat pemicu

Pemicu alarm adalah syarat semantik yang terdiri dari metrik, periode statistik, hubungan perbandingan, ambang batas, durasi, dan frekuensi notifikasi.

Contohnya, metrik yang ditentukan adalah `paket masuk`, periode statistik `1 menit`, hubungan perbandingannya `>`, ambang batasnya `100 paket/dtk`, durasinya `2 periode`, dan frekuensi notifikasinya `satu kali per hari`, maka jumlah paket masuk akan dikumpulkan satu kali setiap menit, dan alarm akan terpicu satu kali per hari jika jumlah paket masuk pendengar CLB melebihi 100 paket/dtk dua kali berturut-turut.

7. Konfigurasi saluran alarm. Konfigurasi grup penerima, periode valid, dan saluran penerima (email dan objek) sesuai kebutuhan.
8. Konfigurasi callback API opsional sesuai kebutuhan. Masukkan URL yang bisa diakses melalui jaringan publik sebagai alamat API callback (nama domain atau IP[:port][/jalur]), dan Cloud Monitor akan segera mendorong pesan alarm ke alamat ini.
9. Setelah menyelesaikan konfigurasi, klik **Complete** (Selesai).

Deskripsi Metrik Peringatan

Waktu update terbaru : 2024-01-04 20:53:33

Deskripsi Alarm

Anda bisa membuat alarm untuk metrik instance tertentu agar instance CLB Anda akan mengirimkan informasi alarm ke grup pengguna target saat status berjalannya memenuhi syarat tertentu. Dengan melakukannya, Anda bisa mendeteksi pengecualian apa pun tepat waktu dan mengambil langkah tepat untuk memastikan kestabilan dan keandalan sistem. Untuk informasi selengkapnya, silakan lihat [Ikhtisar Alarm](#).

Kebijakan alarm CLB mencakup yang berikut ini:

Pendengar jaringan publik

Pendengar jaringan pribadi

Port server (lainnya)

Level pendengar

Level port server

Port server (tipe Klasik jaringan pribadi)

Pemantauan protokol lapisan 7

Pendengar Jaringan Publik/Pribadi

Saat ini, baik CLB jaringan publik dan CLB jaringan pribadi mendukung alarm di level pendengar dengan metrik berikut ini:

| Metrik | Unit | Deskripsi |
|---------------------|-------|--|
| Bandwidth masuk | Mbps | Bandwidth yang digunakan klien untuk mengakses CLB melalui jaringan publik dalam satu periode referensi. |
| Bandwidth keluar | Mbps | Bandwidth yang digunakan CLB untuk mengakses jaringan publik dalam satu periode referensi. |
| Jumlah paket masuk | Paket | Jumlah paket data permintaan yang diterima oleh CLB per detik dalam satu periode referensi. |
| Jumlah paket keluar | Paket | Jumlah paket data yang dikirim oleh CLB per detik dalam satu periode referensi. |

Port Server (Lainnya)

Semua instance CLB kecuali Klasik jaringan pribadi mendukung alarm di dua level berikut:

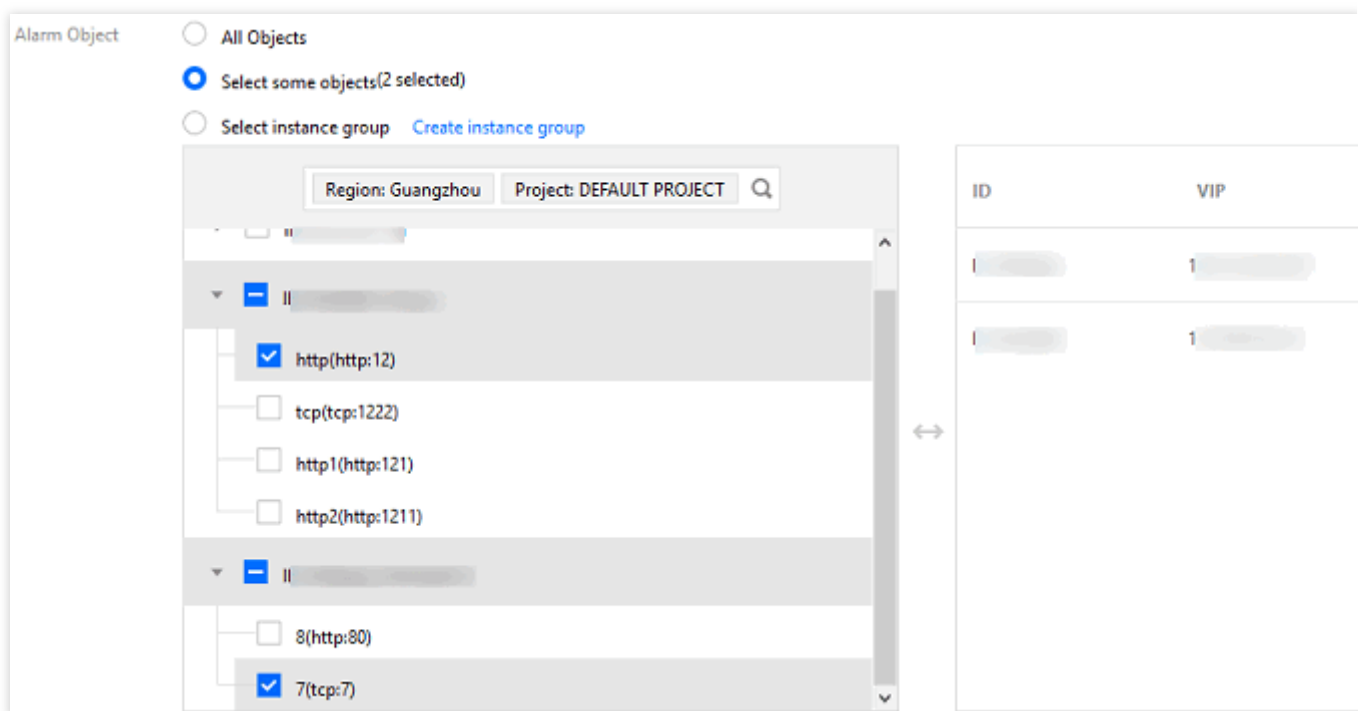
1.Level pendengar

Anda bisa mengonfigurasi jumlah port server asli luar biasa dari pendengar untuk statistik pengecualian dari semua port server terikat di bawah pendengar, yang akan memicu alarm sesuai ambang batas yang dikonfigurasi.Seperti yang ditunjukkan di bawah ini, jumlah port pengecualian dari semua server asli di bawah pendengar terpilih dikumpulkan satu kali setiap menit; jika jumlahnya lebih dari 10 per detik dalam dua periode referensi berturut-turut, dia akan memicu alarm satu kali per hari.

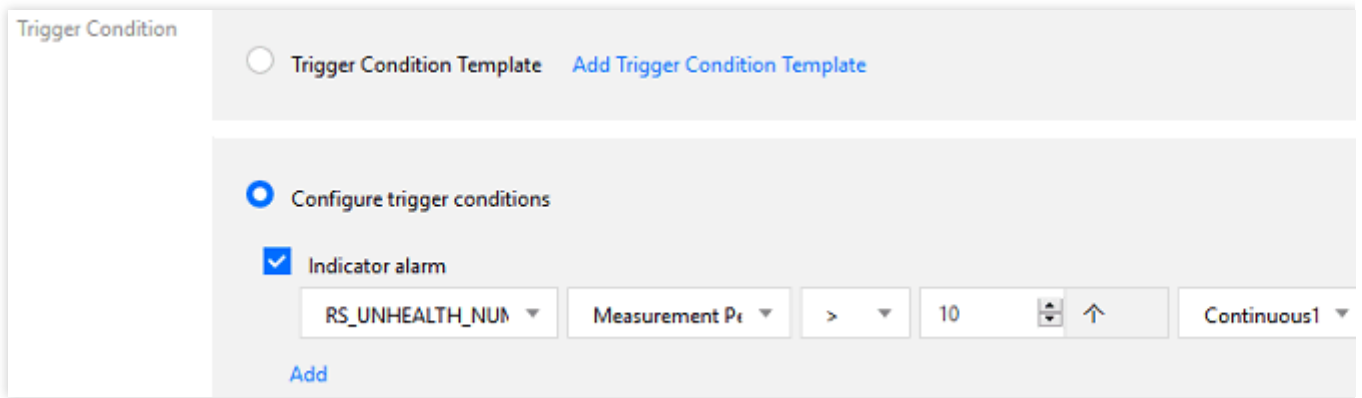
Keterangan :

Untuk mengaktifkan alarm level pendengar, silakan [kirimkan tiket](#) untuk mendaftar.

Konfigurasi objek alarm:



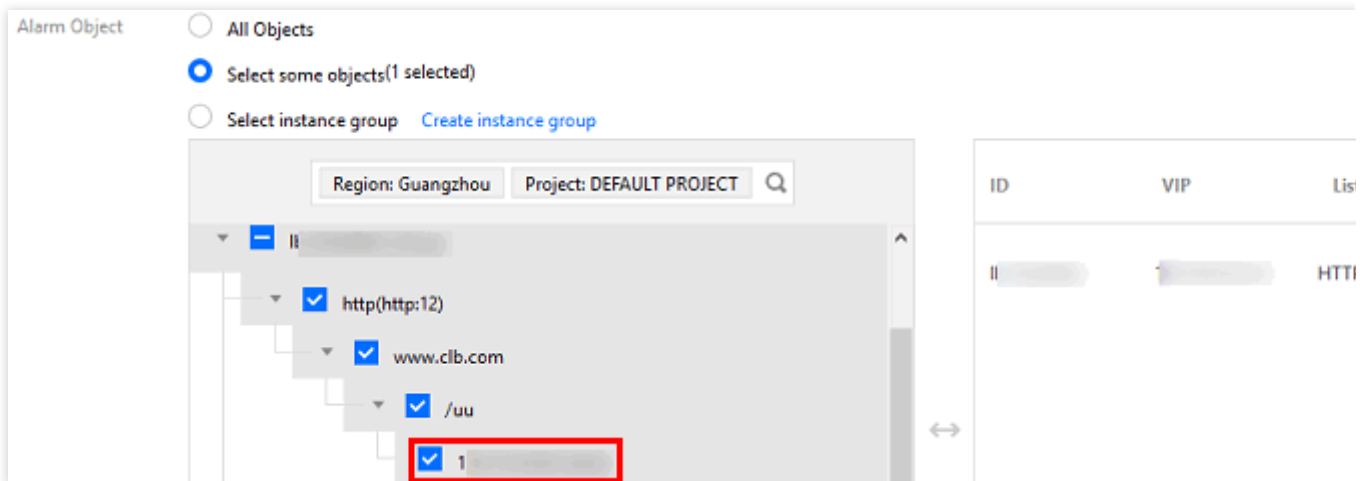
Konfigurasi syarat pemicu:



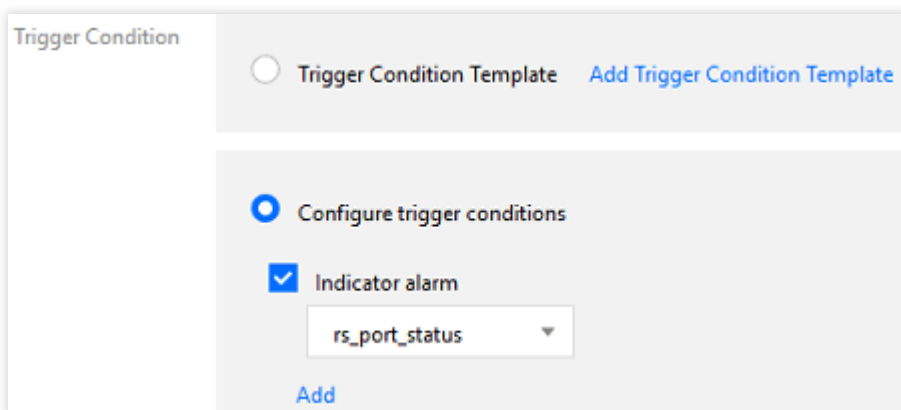
2.Level port server

Anda bisa mengonfigurasi alarm pengecualian untuk port tertentu dari server asli yang terikat pada satu pendengar sehingga alarm akan dikirim kapan pun port menjadi pengecualian.

Konfigurasi objek alarm:



Konfigurasi syarat pemicu:



Perhatian :

Pengecualian port server asli: artinya port server asli dianggap tidak tersedia oleh CLB; pada beberapa kasus, jitter jaringan juga bisa memicu pengecualian port.

Statistik pada level pendengar mencakup status port dari semua server di bawah pendengar, dari konvergensi alarm tunggal ke alarm ambang batas. Untuk menghindari dampak jitter jaringan, Anda sebaiknya menggunakan alarm level pendengar.

Port Server (Tipe Klasik Jaringan Pribadi)

Anda bisa mengonfigurasi alarm pengecualian port server untuk CLB Klasik jaringan pribadi sesuai yang diinstruksikan di "Port Server (lainnya) > Level port server".

Anda bisa mengonfigurasi alarm pengecualian untuk port tertentu dari server asli yang terikat pada satu pendengar sehingga alarm akan dikirim kapan pun port menjadi pengecualian.

Pemantauan Protokol Lapisan 7

Anda bisa mengonfigurasi kebijakan alarm metrik pemantauan unik untuk semua pendengar lapisan 7 (HTTP/HTTPS). Metrik tertentu adalah sebagai berikut:

| Metrik | Unit | Deskripsi |
|-------------------------|-------|--|
| Bandwidth masuk | Mbps | Bandwidth yang digunakan klien untuk mengakses CLB melalui jaringan publik dalam satu periode referensi. |
| Bandwidth keluar | Mbps | Bandwidth yang digunakan CLB untuk mengakses jaringan publik dalam satu periode referensi. |
| Jumlah paket masuk | Paket | Jumlah paket data permintaan yang diterima oleh CLB per detik dalam satu periode referensi. |
| Jumlah paket keluar | Paket | Jumlah paket data yang dikirim oleh CLB per detik dalam satu periode referensi. |
| Jumlah koneksi baru | - | Jumlah koneksi baru yang dibuat per menit dalam satu periode referensi. |
| Jumlah koneksi aktif | - | Jumlah koneksi aktif per menit dalam satu periode referensi. |
| Waktu respons rata-rata | ms | Waktu respons rata-rata CLB dalam satu periode referensi. |
| Waktu respons maksimum | ms | Waktu respons maksimum CLB dalam satu periode referensi. |
| Kode status 2xx | - | Jumlah kode status 2xx yang dikembalikan oleh server asli dalam |

| | | |
|---------------------------------------|---|---|
| | | satu periode referensi. |
| Kode status 3xx | - | Jumlah kode status 3xx yang dikembalikan oleh server asli dalam satu periode referensi. |
| Kode status 4xx | - | Jumlah kode status 4xx yang dikembalikan oleh server asli dalam satu periode referensi. |
| Kode status 5xx | - | Jumlah kode status 5xx yang dikembalikan oleh server asli dalam satu periode referensi. |
| Kode status 404 | - | Jumlah kode status 404 yang dikembalikan oleh server asli dalam satu periode referensi. |
| Kode status 502 | - | Jumlah kode status 502 yang dikembalikan oleh server asli dalam satu periode referensi. |
| Kode status 3xx yang dikembalikan CLB | - | Jumlah kode status 3xx yang dikembalikan oleh CLB dalam satu periode referensi. |
| Kode status 4xx yang dikembalikan CLB | - | Jumlah kode status 4xx yang dikembalikan oleh CLB dalam satu periode referensi. |
| Kode status 5xx yang dikembalikan CLB | - | Jumlah kode status 5xx yang dikembalikan oleh CLB dalam satu periode referensi. |
| Kode status 404 yang dikembalikan CLB | - | Jumlah kode status 404 yang dikembalikan oleh CLB dalam satu periode referensi. |
| Kode status 502 yang dikembalikan CLB | - | Jumlah kode status 502 yang dikembalikan oleh CLB dalam satu periode referensi. |

Cloud Access Management

Ikhtisar

Waktu update terbaru : 2024-01-04 20:53:33

Jika Anda menggunakan beberapa layanan Tencent Cloud seperti CLB, CVM, dan TencentDB yang dikelola oleh beberapa pengguna yang berbagi kunci akun Tencent Cloud Anda, mungkin Anda akan mengalami masalah berikut: Kunci Anda dibagikan oleh beberapa pengguna sehingga berisiko tinggi untuk disusupi.

Anda tidak dapat membatasi izin akses pengguna lain, yang menimbulkan risiko keamanan karena potensi kesalahan operasi.

[Cloud Access Management \(CAM\)](#) digunakan untuk mengelola izin akses ke sumber daya Tencent Cloud. Dengan CAM, Anda dapat menggunakan fitur manajemen identitas dan manajemen kebijakan untuk mengontrol sumber daya Tencent Cloud yang dapat diakses oleh subakun.

Misalnya, jika memiliki beberapa instance CLB dalam akun yang diterapkan di beberapa proyek, untuk mengelola izin akses dan memberi izin sumber daya, Anda dapat mengikat admin proyek A dengan kebijakan otorisasi, yang mengatur bahwa hanya admin ini yang dapat menggunakan sumber daya CLB dalam proyek A.

Jika Anda tidak perlu mengelola izin akses ke sumber daya CLB untuk subakun, silakan lewati bagian ini. Tindakan ini tidak akan memengaruhi pemahaman Anda dan penggunaan bagian lain dalam dokumentasi.

Konsep Dasar di CAM

Akun root mengotorisasi subakun dengan mengikat kebijakan. Pengaturan kebijakan dapat ditetapkan khusus ke tingkat **API, Resource, User/User Group, Allow/Deny, and Condition** (API, Sumber Daya, Pengguna/Grup Pengguna, Izinkan/Tolak, dan Kondisi).

1. Akun

Root account (Akun root)

Sebagai pemilik utama sumber daya Tencent Cloud, akun root berfungsi sebagai dasar bagi penagihan dan penghitungan biaya penggunaan sumber daya, serta dapat digunakan untuk masuk ke layanan Tencent Cloud.

Sub-account (Subakun)

subakun dibuat oleh akun root, serta memiliki ID khusus dan kredensial identitas yang dapat digunakan untuk masuk ke Tencent Cloud Console. Akun root dapat membuat beberapa subakun (pengguna). **Subakun tidak memiliki sumber daya apa pun secara default; sebagai gantinya, sumber daya tersebut akan diotorisasi oleh akun root subakun.**

Identity credential (Kredensial identitas)

Mencakup kredensial masuk dan sertifikat akses. **Login credential** (Kredensial masuk) merujuk pada nama

pengguna dan kata sandi. **Access certificate** (Sertifikat akses) merujuk pada kunci API TencentCloud (SecretId dan SecretKey).

2. Sumber daya dan izin

Resource (Sumber daya)

Sumber daya merupakan objek yang dioperasikan di layanan Tencent Cloud, seperti instance CVM dan instance VPC.

Permission (Izin)

Izin adalah otorisasi untuk mengizinkan atau melarang pengguna tertentu ketika menjalankan operasi tertentu. Secara default, **akun root memiliki akses penuh ke sumber daya yang dimilikinya**, sedangkan **subakun tidak memiliki akses ke sumber daya apa pun yang dimiliki akun root**.

Policy (Kebijakan)

Kebijakan adalah aturan sintaks yang digunakan untuk menetapkan dan menjelaskan satu atau beberapa izin. **Akun root** menjalankan otorisasi dengan **mengaitkan kebijakan** dengan pengguna/grup pengguna.

Untuk informasi selengkapnya, lihat [Ringkasan CAM](#).

Dokumen Terkait

| Deskripsi Dokumen | Tautan |
|--|---|
| Hubungan antara kebijakan dan pengguna | Kebijakan |
| Struktur dasar kebijakan | Referensi Elemen |
| Produk lain yang mendukung CAM | Layanan Cloud yang Didukung CAM |

Definisi Otorisasi

Waktu update terbaru : 2024-01-04 20:53:33

Tipe Sumber Daya CLB yang Dapat Diotorisasi di CAM

| Tipe Sumber Daya | Deskripsi Sumber Daya dalam Kebijakan Otorisasi |
|------------------|---|
| Instance CLB | <code>qcs::clb:\$region::clb/\$loadbalancerid</code> |
| Server asli CLB | <code>qcs::cvm:\$region:\$account:instance/\$cvminstanceid</code> |

Berikut:

`$region` harus selalu berisi ID wilayah dan boleh dikosongi.

`$account` harus selalu berisi `AccountId` pemilik sumber daya atau `*`.

`$loadbalancerid` harus selalu berisi ID instance CLB atau `*`.

Dan seterusnya...

API yang Dapat Diotorisasi untuk CLB di CAM

Anda dapat mengotorisasi tindakan berikut untuk sumber daya CLB di CAM.

Instance

| Operasi API | Deskripsi Sumber Daya | Deskripsi API |
|-----------------------|-----------------------------------|---|
| DescribeLoadBalancers | Membuat kueri daftar instance CLB | <code>*</code> menunjukkan agar hanya mengautentikasi API |
| CreateLoadBalancer | Membeli instance CLB | <code>qcs:\$projectid:clb:\$region:\$account:clb/*</code> |
| DeleteLoadBalancers | Menghapus instance CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |

| | | |
|------------------------------|-----------------------------------|--|
| ModifyLoadBalancerAttributes | Memodifikasi atribut instance CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalanceri</code> |
| ModifyForwardLBName | Mengganti nama instance CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalanceri</code> |

Pendengar

| Operasi API | Deskripsi Sumber Daya | Deskripsi API |
|--------------------------------|---|--|
| DeleteLoadBalancerListeners | Menghapus pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| DescribeLoadBalancerListeners | Menampilkan daftar pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| ModifyLoadBalancerListener | Memodifikasi atribut pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| CreateLoadBalancerListeners | Membuat pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| DeleteForwardLBListener | Menghapus pendengar CLB (lapisan 4 dan lapisan 7) | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| ModifyForwardLBSeventhListener | Memodifikasi atribut pendengar lapisan 7 CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |

| | | |
|--------------------------------------|--|--|
| ModifyForwardLBFourthListener | Memodifikasi atribut pendengar lapisan 4 CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| DescribeForwardLBListeners | Membuat kueri daftar pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| CreateForwardLBSeventhLayerListeners | Membuat pendengar lapisan 7 CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |
| CreateForwardLBFourthLayerListeners | Membuat pendengar lapisan 4 CLB | <code>qcs::clb:\$region:\$account:clb/\$loadb</code> |

URL dan nama domain CLB

| Operasi API | Deskripsi Sumber Daya | Deskripsi API |
|------------------------------|---|--|
| ModifyForwardLBRulesDomain | Memodifikasi nama domain aturan penerusan pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |
| CreateForwardLBListenerRules | Membuat aturan penerusan pendengar CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |
| DeleteForwardLBListenerRules | Menghapus aturan pendengar CLB lapisan 7 | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |
| DeleteRewrite | Menghapus hubungan | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |

| | | |
|---------------|---|--|
| | pengalihan aturan penerusan instance CLB | |
| ManualRewrite | Secara manual menambahkan hubungan pengalihan aturan penerusan instance CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |
| AutoRewrite | Secara otomatis membuat hubungan pengalihan aturan penerusan instance CLB | <code>qcs::clb:\$region:\$account:clb/\$loadbalance</code> |

Server asli

| Operasi API | Deskripsi Sumber Daya | Deskripsi API |
|-------------------------------------|---|--|
| ModifyLoadBalancerBackends | Memodifikasi berat server asli instance CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| DescribeLoadBalancerBackends | Menampilkan daftar server asli yang terikat dengan instance CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| DeregisterInstancesFromLoadBalancer | Melepaskan server asli | <code>qcs::clb:\$region:\$account:clb</code> |
| RegisterInstancesWithLoadBalancer | Mengikat server asli ke | <code>qcs::clb:\$region:\$account:clb</code> |

| | | |
|--|--|--|
| | instance CLB | |
| DescribeLBHealthStatus | Membuat kueri status kondisi CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| ModifyForwardFourthBackendsPort | Memodifikasi port instance CVM dalam aturan penerusan pendengar lapisan 4 | <code>qcs::clb:\$region:\$account:clb</code> |
| ModifyForwardFourthBackendsWeight | Memodifikasi berat instance CVM dalam aturan penerusan pendengar lapisan 4 | <code>qcs::clb:\$region:\$account:clb</code> |
| RegisterInstancesWithForwardLBSeventhListener | Mengikat instance CVM ke aturan penerusan pendengar lapisan 7 CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| RegisterInstancesWithForwardLBFourthListener | Mengikat instance CVM ke aturan penerusan pendengar lapisan 4 CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| DeregisterInstancesFromForwardLBFourthListener | Melepaskan instance CVM dari aturan penerusan | <code>qcs::clb:\$region:\$account:clb</code> |

| | | |
|----------------------------------|--|--|
| | pendengar lapisan 4 CLB | |
| DeregisterInstancesFromForwardLB | Melepaskan instance CVM dari aturan penerusan pendengar lapisan 7 CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| ModifyForwardSeventhBackends | Memodifikasi berat instance CVM dalam aturan penerusan pendengar lapisan 7 | <code>qcs::clb:\$region:\$account:clb</code> |
| ModifyForwardSeventhBackendsPort | Memodifikasi port instance CVM dalam aturan penerusan pendengar lapisan 7 | <code>qcs::clb:\$region:\$account:clb</code> |
| DescribeForwardLBBackends | Membuat kueri daftar instance CVM dari instance CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| DescribeForwardLBHealthStatus | Membuat kueri status pemeriksaan kondisi CLB | <code>qcs::clb:\$region:\$account:clb</code> |
| ModifyLoadBalancerRulesProbe | Memodifikasi jalur penerusan dan pemeriksaan | <code>qcs::clb:\$region:\$account:clb</code> |

| | | |
|--|--|--|
| | kondisi aturan penerusan pendengar CLB | |
|--|--|--|

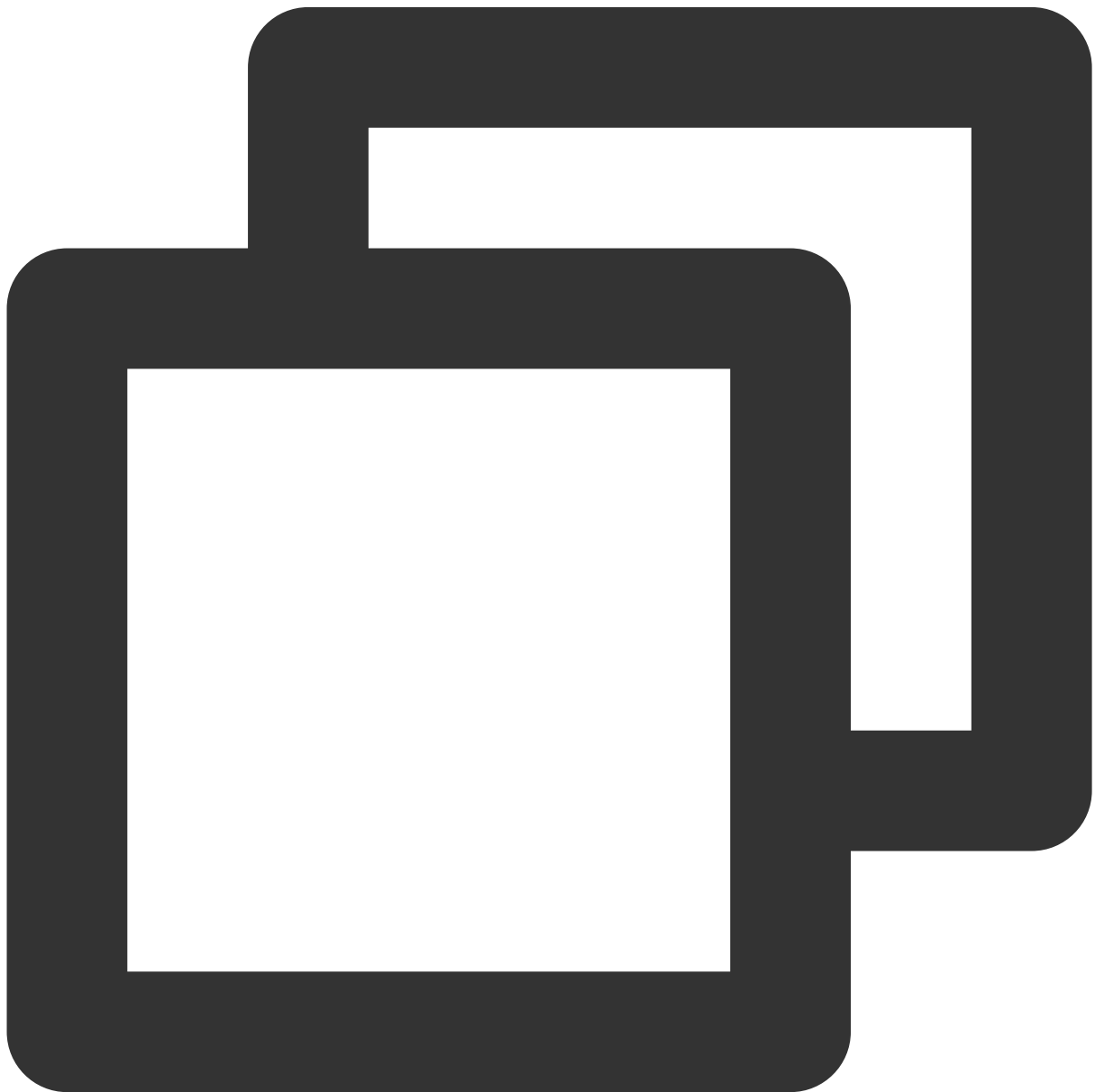
Contoh Kebijakan

Waktu update terbaru : 2024-01-04 20:53:33

Kebijakan Akses Penuh untuk Seluruh Instance CLB

Beri subakun akses penuh ke layanan CLB (membuat, mengelola, dll.).

Nama kebijakan:CLBResourceFullAccess



```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "name/clb:*"
    ],
    "resource": "*",
    "effect": "allow"
  }]
}
```

Kebijakan Baca-Saja untuk Seluruh Instance CLB

Beri subakun akses baca-saja ke CLB (contoh: izin untuk menampilkan tetapi tidak dapat membuat, memperbarui, atau menghapus semua sumber daya CLB). Di konsol, prasyarat untuk memanipulasi sumber daya adalah kemampuan untuk menampilkan sumber daya sehingga sebaiknya Anda memberi subakun izin akses baca penuh ke CLB.

Nama kebijakan: CLBResourceReadOnlyAccess

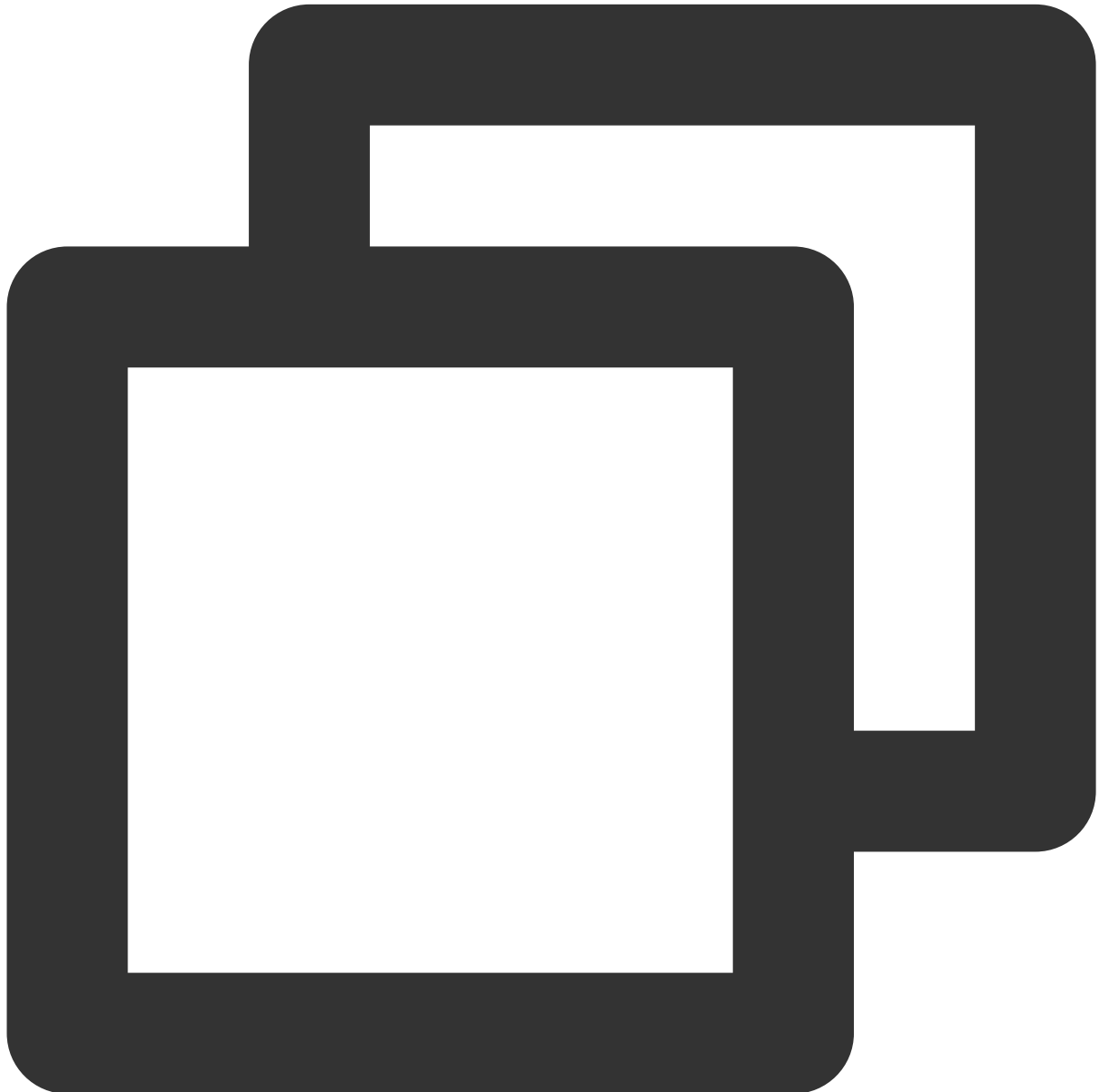


```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "name/clb:Describe*"
    ],
    "resource": "*",
    "effect": "allow"
  }]
}
```

Kebijakan Akses Penuh untuk Layanan CLB Dengan Tag Tertentu

Beri subakun akses penuh ke layanan CLB (membuat instance, mengelola pendengar, dll.) dengan tag tertentu (kunci tag: tagkey; nilai tag: tagvalue).

Instance CLB mendukung konfigurasi tag dan menggunakan tag untuk autentikasi.



```
{  
  "version": "2.0",  
  "statement": [  
    {
```



```
"effect": "allow",
"action": "*",
"resource": "*",
"condition": {
  "for_any_value:string_equal": {
    "qcs:tag": [
      "tagkey&tagvalue"
    ]
  }
}
]
```

CLB Klasik

Ikhtisar CLB Klasik

Waktu update terbaru : 2024-01-04 20:56:41

Ikhtisar

CLB Klasik mudah dikonfigurasi dan mendukung skenario penyeimbangan beban sederhana:

CLB klasik **Public network** (Jaringan publik): mendukung protokol TCP/UDP/HTTP/HTTPS.

CLB klasik **Private network** (Jaringan pribadi): mendukung protokol TCP/UDP.

Instance CLB bisa diklasifikasikan menjadi dua tipe: CLB (sebelumnya "CLB aplikasi") dan CLB klasik.

CLB mencakup semua fitur CLB klasik. Berdasarkan fitur dan performa mereka, Anda sebaiknya menggunakan CLB. Untuk perbandingan mendetail, lihat [Tipe Instance](#).

Perhatian :

Saat ini, ada dua jenis akun Tencent Cloud: tagihan per EIP/CLB dan tagihan per CVM. Semua akun Tencent Cloud yang terdaftar setelah 17 Juni 2020 00.00.00 adalah akun tagihan per EIP/CLB. Untuk akun Tencent Cloud yang terdaftar sebelum 17 Juni 2020, [periksa tipe akun Anda](#) di konsol. Akun tagihan per EIP/CLB tidak lagi mendukung CLB klasik. Anda kini hanya bisa membeli instance CLB.

Dokumen ini memperkenalkan instance CLB klasik. Setelah membuat instance, Anda perlu mengonfigurasi pendengar untuknya. Pendengar mendengar permintaan di instance CLB dan mendistribusikan lalu lintas ke server asli sesuai kebijakan penyeimbangan beban.

Konfigurasi Pendengar

Anda harus mengonfigurasi pendengar CLB seperti di bawah ini:

1. Protokol pendengar dan port pendengaran. Port pendengaran, atau port frontend, digunakan untuk menerima dan meneruskan permintaan ke server asli.
2. Port backend. Ini adalah port tempat instance CVM menyediakan layanan, menerima dan memproses lalu lintas dari instance CLB.
3. Kebijakan pendengaran, seperti kebijakan penyeimbangan beban dan persistensi sesi.
4. Kebijakan pemeriksaan kesehatan.
5. Server asli bisa diikat dengan memilih IP-nya.

Keterangan :

Jika Anda mengonfigurasi beberapa pendengar ke instance CLB klasik dan mengikat beberapa server asli, setiap pendengar akan meneruskan permintaan ke semua server asli sesuai konfigurasinya.

Jenis protokol yang didukung

Satu pendengar CLB bisa mendengar permintaan Lapisan 4 dan Lapisan 7 di instance CLB dan mendistribusikannya ke server asli untuk pemrosesan. Perbedaan utama antara CLB Lapisan 4 dan CLB Lapisan 7 adalah protokol mana yang digunakan untuk meneruskan lalu lintas saat menyeimbangkan beban permintaan pengguna.

Protokol Lapisan 4: protokol layer transportasi, termasuk TCP dan UDP.

Protokol Lapisan 7: protokol layer aplikasi, termasuk HTTP dan HTTPS.

Keterangan :

- 1.Instance CLB klasik menerima permintaan dan meneruskan lalu lintas ke server asli melalui VIP dan port. Protokol Lapisan 7 tidak mendukung penerusan berdasarkan nama domain dan URL.
- 2.Instance CLB klasik jaringan pribadi hanya mendukung protokol Lapisan 4, bukan protokol Lapisan 7.
- 3.Jika Anda membutuhkan fitur-fitur lanjutan yang disebutkan di atas, kami menyarankan untuk memilih CLB daripada CLB klasik. Untuk informasi selengkapnya, lihat [Jenis Instance](#).

Konfigurasi Port

| Port Pendengaran (port frontend) | Port Layanan (port backend) | Deskripsi |
|---|---|--|
| Port pendengaran digunakan oleh instance CLB untuk menerima dan meneruskan permintaan ke server asli untuk penyeimbangan beban. Anda bisa mengonfigurasi CLB untuk rentang port 1-65535, seperti 21 (FTP), 25 (SMTP), 80 (HTTP), dan 443 (HTTPS). | Port layanan digunakan oleh CVM untuk memberikan layanan, menerima dan memproses lalu lintas dari instance CLB. Pada satu instance CLB, satu port pendengaran bisa meneruskan lalu lintas ke port-port beberapa instance CVM. | <p>Pada instance CLB, port pendengaran harus unik. Contohnya, pendengar TCP:80 dan HTTP:80 tidak bisa dibuat di waktu yang sama. Hanya port TCP dan UDP yang boleh sama. Contohnya, Anda bisa membuat baik pendengar TCP:80 dan UDP:80.</p> <p>Port layanan yang sama bisa digunakan pada instance CLB. Contohnya, pendengar</p> |

| | | |
|--|--|---|
| | | HTTP:80 dan HTTPS:443 bisa diikat ke port instance CVM yang sama. |
|--|--|---|

Mengonfigurasi CLB Klasik

Waktu update terbaru : 2024-01-04 20:56:41

Setelah membuat instance CLB klasik, Anda perlu mengonfigurasi pendengar untuknya. Pendengar mendengar permintaan di instance dan mendistribusikan lalu lintas ke server-server asli sesuai kebijakan penyeimbangan beban.

Prasyarat

Anda harus [membuat instance CLB](#) dahulu dan memilih "CLB Klasik" untuk **Instance type** (Tipe instance).

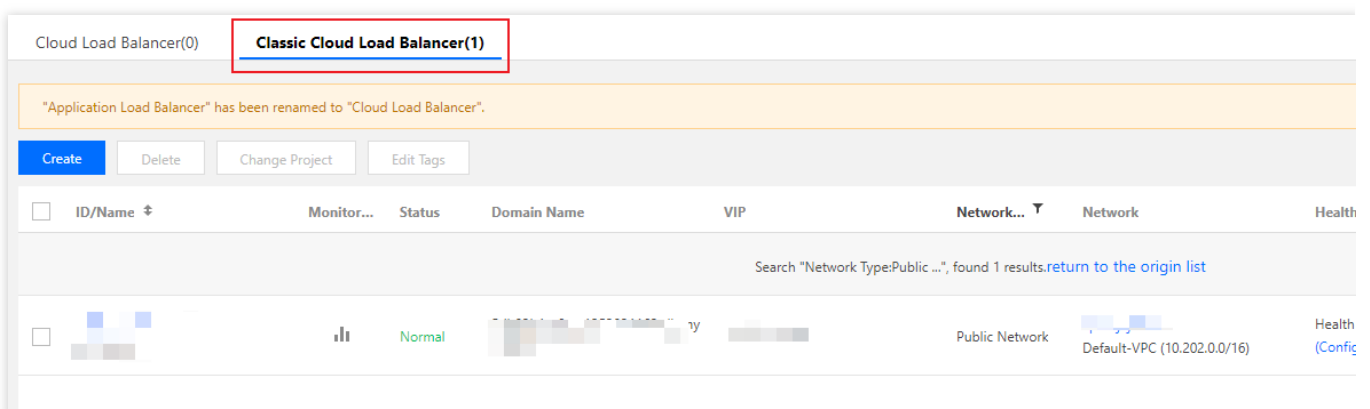
Keterangan :

Saat ini, ada dua jenis akun Tencent Cloud: tagihan per EIP/CLB dan tagihan per CVM. Semua akun Tencent Cloud yang terdaftar setelah 17 Juni 2020 00.00.00 adalah akun tagihan per EIP/CLB. Untuk akun Tencent Cloud yang terdaftar sebelum 17 Juni 2020, [periksa tipe akun Anda](#) di konsol. Akun tagihan per EIP/CLB tidak lagi mendukung CLB klasik. Anda kini hanya bisa membeli instance CLB.

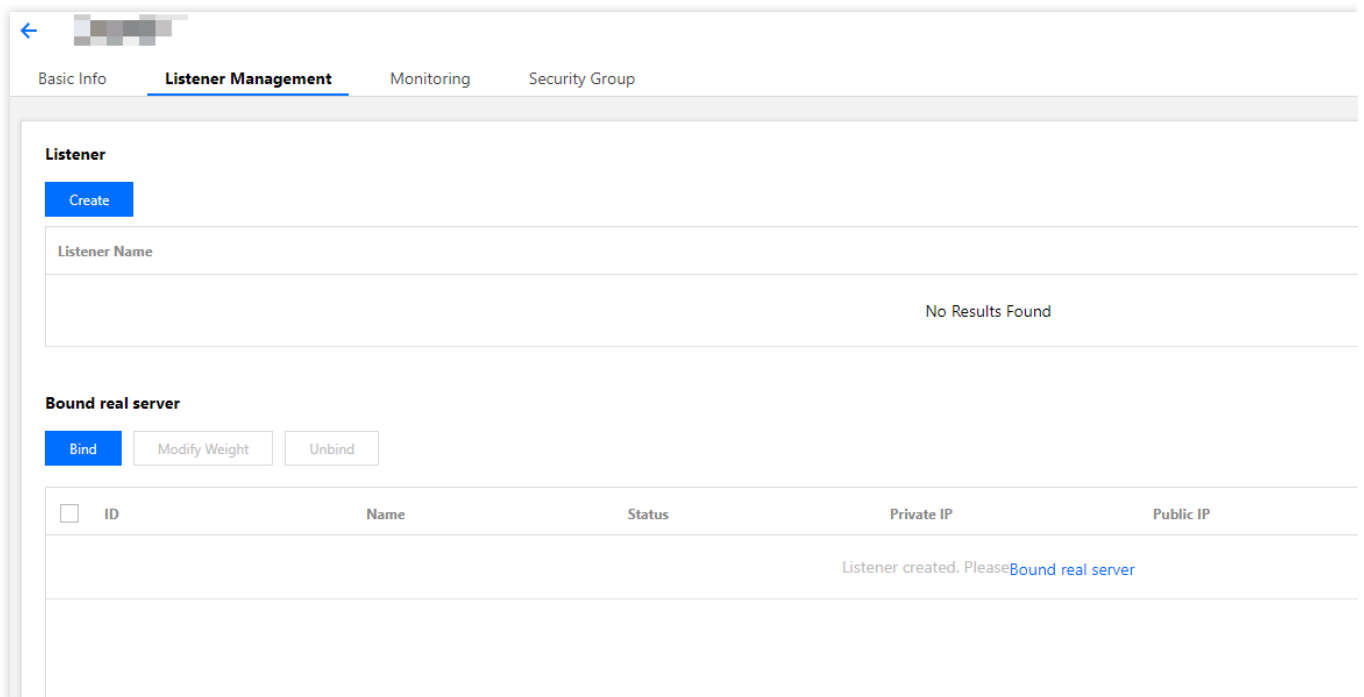
Mengonfigurasi Pendengar

Langkah 1. Buka halaman Listener Management (Manajemen Pendengar)

1. Masuk ke [Konsol CLB](#).
2. Pilih **CLB Instance List** (Daftar Instance CLB) di bilah sisi kiri.
3. Di halaman **Instance Management** (Manajemen Instance), klik ID/Nama instance yang akan dikonfigurasi untuk masuk ke halaman detail instance.
4. Pilih tab **Listener Management** (Manajemen Pendengar), atau klik **Configure listener** (Konfigurasi pendengar) di bawah kolom **Operation** (Operasi) di halaman **Instance Management** (Manajemen Instance).



5. Halaman **Listener Management** (Manajemen Pendengar) adalah seperti yang ditunjukkan di bawah ini.



Langkah 2. Konfigurasi pendengar

Klik **Create** (Buat) di bawah **Listener Management** (Manajemen Pendengar) dan konfigurasi pendengar TCP pada jendela pop-up.

1. Konfigurasi dasar

| Item Konfigurasi | Deskripsi | Contoh |
|-------------------------|---|-------------|
| Nama | Nama pendengar. | test-tcp-80 |
| Port Protokol Pendengar | Protokol pendengar dan port pendengaran Protokol pendengar: CLB mendukung protokol seperti TCP, UDP, HTTP, dan HTTPS. Contoh ini menggunakan TCP. Port pendengaran: digunakan untuk menerima dan meneruskan permintaan ke server asli. Rentang port adalah 1-65535. Port pendengaran harus unik di instance CLB yang sama. | TCP:80 |
| Port Backend | Port tempat instance CVM menyediakan layanan, menerima dan memproses lalu lintas dari instance CLB. | 80 |

Untuk membuat pendengar TCP, selesaikan konfigurasi dasar seperti yang ditunjukkan di bawah ini:

Create Listener

1 **Basic Configuration** >
 2 **Advanced Configuration** >
 3 **Health Check**

Name

Listen Protocol Ports ⓘ TCP :

Backend Port

Close
Next

2. Konfigurasi lanjutan

| Item Konfigurasi | Deskripsi | Contoh |
|---------------------|--|------------|
| Metode Keseimbangan | <p>Untuk pendengar TCP, CLB mendukung dua algoritme penjadwalan: round robin tertimbang (WRR) dan koneksi terkecil tertimbang (WLC).</p> <p>WRR: permintaan diteruskan ke server-server berbeda secara berurutan sesuai bobotnya. Penjadwalan disesuaikan dengan jumlah koneksi baru, tempat server dengan bobot lebih tinggi menerima lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi) dan server dengan bobot yang sama memproses jumlah koneksi yang sama.</p> <p>WLC: beban pada server dihitung berdasarkan jumlah koneksi aktifnya. Penjadwalan disesuaikan beban dan bobot server. Jika bobotnya sama, server asli dengan koneksi aktif yang lebih sedikit akan menerima lebih banyak polling (dengan kata lain, kemungkinan yang lebih tinggi).</p> | WRR |
| Persistensi Sesi | <p>Mengaktifkan atau menonaktifkan sesi.</p> <p>Setelah persistensi sesi diaktifkan, pendengar CLB akan mendistribusikan permintaan akses dari klien yang sama ke server asli yang sama.</p> <p>Persistensi sesi TCP diimplementasikan sesuai alamat IP klien. Permintaan akses dari alamat IP yang sama diteruskan ke server asli yang sama.</p> <p>Persistensi sesi bisa diaktifkan untuk penjadwalan WRR tetapi tidak untuk penjadwalan WLC.</p> | Diaktifkan |
| Waktu Tunggu | Waktu persistensi sesi. | 30s |

Jika tidak ada permintaan baru di koneksi dalam waktu persistensi sesi, persistensi sesi akan diputus secara otomatis.
Rentang nilai: 30-3600 detik.

Selesaikan konfigurasi seperti yang ditunjukkan di bawah ini:

CreateListener

Basic Configuration > **2 Advanced Configuration** > Health Check

Balance Method: **Weighted Round Robin**

If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Session Persistence

Hold Time Seconds

Session persistence based on the source IP

3.Pemeriksaan kesehatan

| Item Konfigurasi | Deskripsi | Contoh |
|-----------------------|---|-----------------------|
| Pemeriksaan Kesehatan | Mengaktifkan atau menonaktifkan pemeriksaan kesehatan.Di pendengar TCP, instance CLB mengirimkan paket SYN ke port server tertentu untuk melakukan pemeriksaan kesehatan. | Diaktifkan |
| Protokol Pemeriksaan | Yang akan ditambahkan. | Yang akan ditambahkan |
| Port Pemeriksaan | Yang akan ditambahkan. | Yang akan ditambahkan |
| Waktu Habis Respons | Periode waktu habis respons maksimum untuk pemeriksaan kesehatan. | 2s |

| | | |
|--------------------------|---|--------|
| | Jika satu server asli gagal merespons dalam periode waktu habis, server dianggap tidak sehat. Rentang nilai: 2-60 detik.Nilai default: 2s. | |
| Interval Pemeriksaan | Interval antara dua pemeriksaan kesehatan. Rentang nilai: 5-300 detik.Nilai default: 5s. | 5s |
| Ambang Batas Tidak Sehat | Jika pemeriksaan kesehatan mengembalikan <code>gagal</code> n kali berturut-turut (n ditentukan pengguna), server asli itu tidak sehat dan status unhealthy (tidak sehat) ditampilkan di konsol. Rentang nilai: 2-10 kali.Nilai default: 3 kali | 3 kali |
| Ambang Batas Sehat | Jika pemeriksaan kesehatan mengembalikan <code>berhasil</code> n kali berturut-turut (n ditentukan pengguna), server asli itu sehat dan status healthy (sehat) ditampilkan di konsol. Rentang nilai: 2-10 kali.Nilai default: 3 kali. | 3 kali |

Selesaikan konfigurasi pemeriksaan kesehatan seperti yang ditunjukkan di bawah ini:

Create Listener

✓ Basic Configuration >
 ✓ Advanced Configuration >
 3 Health Check

Health Check ⓘ

[Hide Advanced Options](#) ▲

Response Timeout ⓘ 2 Seconds 60 Seconds − 2 + Seconds

Check Interval ⓘ 5 Seconds 300 Seconds − 5 + Seconds

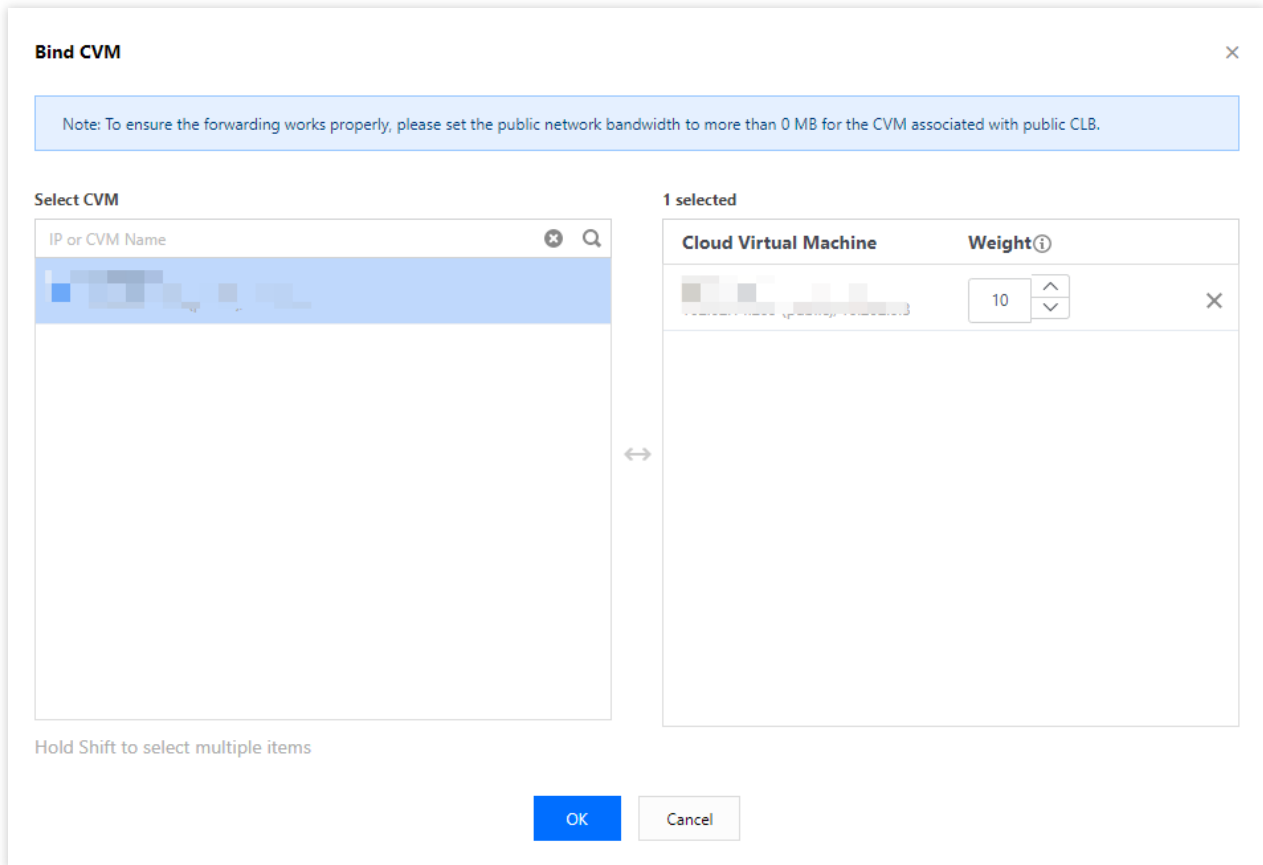
Unhealthy Threshold ⓘ 2 Times 10 Times − 3 + Times

Healthy Threshold ⓘ 2 Times 10 Times − 3 + Times

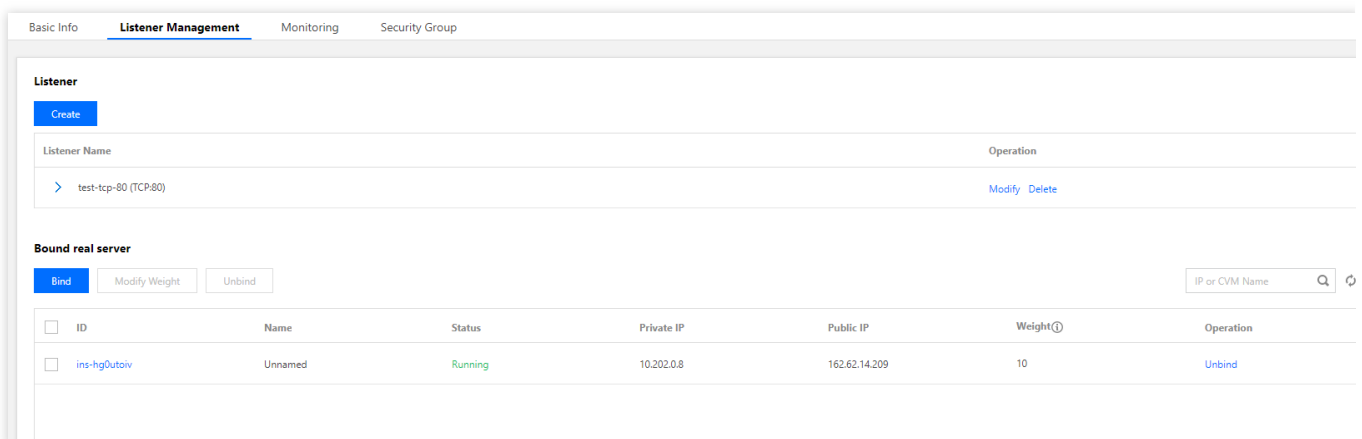
Back Submit

Langkah 3. Mengikat server asli

Klik **Bind** (Ikat) di halaman **Listener Management** (Manajemen Pendengar) dan pilih server asli yang akan diikat di jendela pop-up, seperti yang ditunjukkan di bawah ini:



Konfigurasi seperti yang ditunjukkan di bawah ini:



Keterangan :

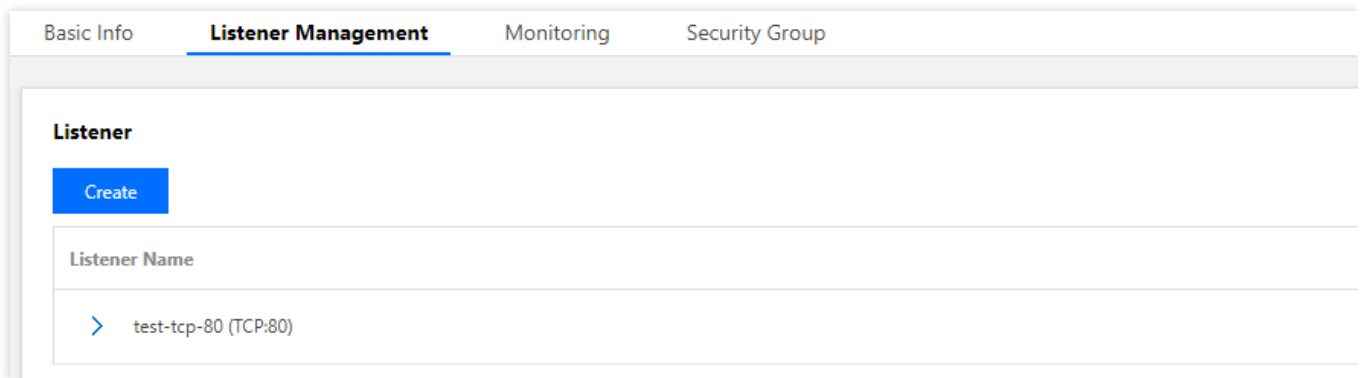
Jika Anda mengonfigurasi beberapa pendengar ke instance CLB klasik dan mengikat beberapa server asli, setiap pendengar akan meneruskan permintaan ke semua server asli sesuai konfigurasinya.

Langkah 4. Grup keamanan (opsional)

Anda dapat mengonfigurasi grup keamanan CLB untuk mengisolasi lalu lintas jaringan publik. Untuk informasi selengkapnya, lihat [Mengonfigurasi Grup Keamanan CLB](#).

Langkah 5. Modifikasi atau hapus satu pendengar (opsional)

Jika Anda perlu memodifikasi atau menghapus pendengar yang ada, pilih pendengar di halaman **Listener Management** (Manajemen Pendengar) dan klik **Modify** (Modifikasi) atau **Delete** (Hapus).



Mengelola Server Asli dari Instance CLB Klasik

Waktu update terbaru : 2024-01-04 20:56:41

CLB klasik mengarahkan permintaan ke instance server asli yang berjalan dengan normal. Dokumen ini menjelaskan cara menambah atau menghapus server asli sesuai kebutuhan atau saat Anda menggunakan CLB Klasik untuk pertama kalinya.

Prasyarat

Anda telah membuat instance CLB Klasik dan mengonfigurasi pendengar. Untuk informasi selengkapnya, silakan lihat [Memulai CLB Klasik](#).

Petunjuk

Menambahkan server asli ke instance CLB Klasik

Keterangan :

Jika instance CLB Klasik diasosiasikan dengan grup penskalaan otomatis, instance CVM di grup itu akan ditambahkan secara otomatis ke server asli instance CLB Klasik tersebut. Jika instance CVM dihapus dari grup penskalaan otomatis, dia akan dihapus secara otomatis dari server-server asli instance CLB Klasik.

Jika Anda perlu menggunakan API untuk menambah server asli, silakan lihat [RegisterTargetsWithClassicalLB](#) API.

1. Masuk ke [Konsol CLB](#).
2. Di halaman "Manajemen Instance", pilih tab **Classic Cloud Load Balancer** (Penyeimbang Beban Cloud Klasik).
3. Klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB Klasik target.
4. Pada modul konfigurasi pendengar, klik **Create** (Buat).
5. Pada jendela pop-up "Buat Pendengar", masukkan "port backend" (untuk informasi selengkapnya mengenai pemilihan port, silakan lihat [Port Server Biasa](#)) dan bidang terkait lainnya dan klik **Next** (Berikutnya) untuk menyelesaikan konfigurasi. Untuk informasi selengkapnya, silakan lihat [Mengonfigurasi CLB Klasik](#).

Keterangan :

Anda perlu menentukan port server asli untuk CLB Klasik selama **listener creation** (pembuatan pendengar).

CreateListener

1 Basic Configuration > 2 Advanced Configuration > 3 Health Check

Name

Listen Protocol Ports ⓘ :

Backend Port

6. Setelah pendengar dibuat, klik **Bind** (Ikat) pada modul pengikatan server asli.

7. Pada jendela pop-up **Bind CVM** (Ikat CVM), pilih instance CVM yang akan diikat, masukkan bobotnya, dan klik **OK**.

Keterangan :

Jendela pop-up hanya menampilkan instance CVM yang tersedia di satu wilayah dan satu lingkungan jaringan yang tidak terisolasi dan belum kedaluwarsa dengan bandwidth puncak lebih dari 0.

Jika beberapa server asli terikat, CLB akan meneruskan lalu lintas sesuai dengan algoritme hash untuk menyeimbangkan beban.

Makin besar bobot server, makin banyak permintaan yang diteruskan ke sana. Nilai defaultnya 10, dan rentang nilai yang bisa dikonfigurasi adalah 0-100. Jika bobot diatur ke 0, server tidak akan menerima permintaan baru. Jika persistensi sesi diaktifkan, distribusi permintaan yang tidak merata di antara server asli bisa terjadi. Untuk informasi selengkapnya, silakan lihat [Konfigurasi Algoritme dan Bobot](#).

Bind CVM

Note: The communication between CLB and CVM is based on private network, so no traffic fee is incurred.

Select CVM

IP or CVM Name ✕ 🔍

| | |
|-------------------------------------|-----|
| <input checked="" type="checkbox"/> | ... |
| <input checked="" type="checkbox"/> | ... |

2 selected

Cloud Virtual Machine

| |
|-----|
| ... |
| ... |

Hold Shift to select multiple items

OK

Cancel

Memodifikasi bobot server asli untuk instance CLB Klasik

Keterangan :

Saat ini, bobot server asli tidak bisa dimodifikasi melalui API untuk CLB Klasik.

1. Masuk ke [Konsol CLB](#).
2. Di halaman "Manajemen Instance", pilih tab **Classic Cloud Load Balancer** (Penyeimbang Beban Cloud Klasik).
3. Klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB Klasik target.
4. Pada modul pengikatan server asli, modifikasi bobot server yang relevan.

Keterangan :

Makin besar bobot server, makin banyak permintaan yang diteruskan ke sana. Nilai defaultnya 10, dan rentang nilai yang bisa dikonfigurasi adalah 0-100. Jika bobot diatur ke 0, server tidak akan menerima permintaan baru. Jika

persistensi sesi diaktifkan, distribusi permintaan yang tidak merata di antara server asli bisa terjadi. Untuk informasi selengkapnya, silakan lihat [Konfigurasi Algoritme dan Bobot](#).

Method 1 (Metode 1). Modifikasi bobot satu server tunggal.

1. Temukan server yang bobotnya perlu dimodifikasi, arahkan kursor di bobot yang sesuai, dan klik



| Bind | | Modify Weight | Unbind | | | |
|--------------------------|-----|---------------|---------|------------|-----------|--|
| <input type="checkbox"/> | ID | Name | Status | Private IP | Public IP | |
| <input type="checkbox"/> | ... | ... | Running | ... | ... | |
| <input type="checkbox"/> | ... | ... | Running | ... | ... | |

2. Di jendela pop-up "Modifikasi Bobot", masukkan nilai bobot yang baru dan klik **Submit** (Kirim).

Method 2 (Metode 2). Modifikasi bobot beberapa server dalam beberapa batch.

Keterangan :

Setelah modifikasi batch, server akan memiliki bobot yang sama.

1. Klik kotak di depan server, pilih beberapa server, dan klik **Modify Weight** (Modifikasi Bobot) di bagian atas daftar.

| Bind | | Modify Weight | Unbind | | | |
|-------------------------------------|-----|---------------|---------|------------|-----------|----|
| <input checked="" type="checkbox"/> | ID | Name | Status | Private IP | Public IP | W |
| <input checked="" type="checkbox"/> | ... | ... | Running | ... | ... | 10 |
| <input checked="" type="checkbox"/> | ... | ... | Running | ... | ... | 10 |

2. Di jendela pop-up "Modifikasi Bobot", masukkan nilai bobot yang baru dan klik **Submit** (Kirim).

Melepas ikatan server asli dari instance CLB Klasik

Keterangan :

Melepas ikatan server asli akan melepas ikatan instance CLB Klasik dari instance CVM, dan CLB Klasik akan segera berhenti meneruskan permintaan ke sana.

Melepas ikatan server asli tidak akan memengaruhi siklus pemakaian instance CVM Anda, yang bisa ditambahkan lagi ke kluster server asli saat dibutuhkan.

Jika Anda perlu menggunakan API untuk melepas ikatan server asli, silakan lihat [DeregisterTargetsFromClassicalLB](#) API.

1. Masuk ke [Konsol CLB](#).
2. Di halaman "Manajemen Instance", pilih tab **Classic Cloud Load Balancer** (Penyeimbang Beban Cloud Klasik).
3. Klik **Configure Listener** (Konfigurasi Pendengar) di kolom "Operasi" di sebelah kanan instance CLB Klasik target.
4. Pada modul pengikatan server asli, lepas ikatan server yang terikat.

Method 1 (Metode 1).Lepas ikatan satu server tunggal.

1. Temukan server yang perlu dilepas ikatannya dan klik **Unbind** (Lepas Ikatan) di kolom **Operation** (Operasi) di sebelah kanan.

| <input type="checkbox"/> | ID | Name | Status | Private IP | Public IP |
|--------------------------|-----|------|---------|------------|-----------|
| <input type="checkbox"/> | ... | ... | Running | ... | ... |
| <input type="checkbox"/> | ... | ... | Running | ... | ... |

2. Pada jendela pop-up "Lepas Ikatan Server Asli", konfirmasi server yang akan dilepas dan klik **Submit** (Kirim).

Method 2 (Metode 2).Lepas ikatan beberapa server dalam beberapa batch.

1. Klik kotak di depan server, pilih beberapa server, dan klik **Unbind** (Lepas Ikatan) di bagian atas daftar.

| <input checked="" type="checkbox"/> | ID | Name | Status | Private IP | Public IP |
|-------------------------------------|-----|------|---------|------------|-----------|
| <input checked="" type="checkbox"/> | ... | ... | Running | ... | ... |
| <input checked="" type="checkbox"/> | ... | ... | Running | ... | ... |

2. Pada jendela pop-up "Lepas Ikatan Server Asli", konfirmasi server-server yang akan dilepas dan klik **Submit** (Kirim).