

Cloud Load Balancer

Memulai

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

Memulai

[Memulai CLB](#)

[Memulai CLB IPv6](#)

[Memulai CLB Klasik](#)

[Men-deploy Nginx di CentOS](#)

[Men-deploy Java Web di CentOS](#)

Memulai

Memulai CLB

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

Tencent Cloud CLB menyediakan berbagai protokol seperti TCP, UDP, TCP SSL, HTTP, dan HTTPS sehingga melengkapi bisnis dengan nama domain dan layanan penerusan berbasis URL. Dokumen ini memandu Anda untuk membuat instance CLB dengan cepat dan meneruskan permintaan klien ke dua instance CVM.

Prasyarat

1. Anda telah membuat dua instance CVM (dokumen ini mengambil **rs-1** dan **rs-2** sebagai dua contoh instance). Untuk informasi tentang cara membuat instance CVM, lihat [Membuat Instance lewat Halaman Pembelian CVM](#).
2. Anda telah men-deploy layanan backend di dua instance CVM. Dokumen ini mengambil penerusan HTTP sebagai contoh. Server Nginx telah di-deploy di instance **rs-1** dan **rs-2** CVM, dan kedua instance tersebut mengembalikan dua halaman statis HTML dengan mengucapkan "Halo nginx! Ini adalah rs-1!" dan "Halo nginx! Ini adalah rs-2!" Untuk informasi selengkapnya, lihat [Men-deploy Nginx di CentOS](#).

Perhatian :

Dokumen ini menjelaskan langkah-langkah untuk akun tagihan-berdasarkan-IP. Untuk akun tagihan-berdasarkan-CVM, terlebih dahulu silakan membeli bandwidth jaringan publik untuk instance CVM. Jika Anda tidak tahu pasti jenis akun Anda, silakan lihat [Memeriksa Jenis Akun](#).

Dalam contoh ini, layanan berbeda yang di-deploy di server asli akan mengembalikan nilai yang berbeda. Dalam praktiknya, layanan yang di-deploy di server asli itu mirip untuk memberikan pengalaman yang konsisten bagi semua pengguna.

Langkah 1: Membeli Instance CLB

Setelah pembelian berhasil, sistem akan otomatis menetapkan VIP ke instance CLB. VIP akan digunakan sebagai alamat IP untuk menyediakan layanan kepada klien.

1. Masuk ke konsol Tencent Cloud dan buka [halaman pembelian CLB](#).
2. Pertama, pilih wilayah yang sama dengan instance CVM Anda. Selanjutnya, pilih **Cloud Load Balancer** (Cloud Load Balancer) sebagai jenis instance, **Public Network** (Jaringan Publik) sebagai jenis jaringan. Untuk detail selengkapnya, silakan lihat [Pilihan Atribut Produk](#).

Keterangan :

Pengujian beta IP jalur tunggal statis hanya tersedia di Jinan, Hangzhou, Fuzhou, Shijiazhuang, Wuhan, dan Changsha. Anda dapat mengirimkan aplikasi untuk menggunakannya. Setelah diizinkan, Anda dapat memilih ISP (China Mobile, China Unicom, atau China Telecom) di halaman pembelian. Jika Anda ingin mencobanya di Guangzhou, Shanghai, Nanjing, Beijing, Chengdu, dan Chongqing, hubungi perwakilan penjualan Anda.

3. Klik **Buy Now** (Beli Sekarang) dan lakukan pembayaran.

4. Kembali ke halaman **Instance Management** (Manajemen Instance), pilih wilayah untuk melihat instance baru.

<input type="checkbox"/>	ID/Name ↑	Monitor...	Status	VIP	Network... ▼	Network	Health Status	Creation Time ↕
<input type="checkbox"/>	lb- clb-test		Normal	1	Public Network		Health check not enabled (Configuration)	2019-07-05 17:06:4

Langkah 2: Mengonfigurasi Pendengar CLB

Pendengar CLB digunakan untuk meneruskan melalui protokol dan port yang ditentukan. Dokumen ini menjelaskan cara mengonfigurasi instance CLB untuk meneruskan permintaan HTTP klien.

Konfigurasi protokol dan port pendengar HTTP

Ketika seorang klien memulai permintaan, instance CLB akan menerima permintaan menurut protokol dan port pendengar, lalu meneruskan permintaan tersebut ke server asli.

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

2. Di halaman **Instance Management** (Manajemen Instance), klik **Configure Listener** (Konfigurasi Pendengar) di kolom **Operation** (Pengoperasian) dari instance CLB target.

3. Di halaman **Listener Management** (Manajemen Pendengar), klik **Create** (Buat) di bagian **HTTP/HTTPS Listener** (Pendengar HTTP/HTTPS).

← lb- [redacted]

Basic Info **Listener Management** Redirection Configurations Monitoring Se

Note: When custom redirection policies are configured, the original forwarding rules are modified, the redirection polici

HTTP/HTTPS Listener

Create

4. Di jendela **Create Listener** (Buat Pendengar), silakan konfigurasi item berikut dan klik **Submit** (Kirim).

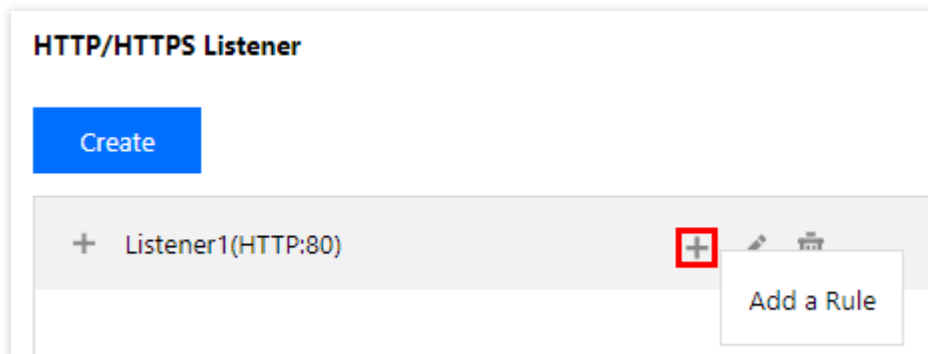
Nama pendengar.

Dengar port protokol (misalnya, **HTTP:80**).

Konfigurasi aturan penerusan pendengar

Jika seorang klien memulai permintaan, instance CLB akan meneruskan permintaan tersebut sesuai aturan penerusan pendengar yang sudah dikonfigurasi.

1. Di tab **Listener Management** (Manajemen Pendengar), klik **+** di sisi kanan pendengar baru.



2. Di jendela **Create Forwarding Rules** (Buat Aturan Penerusan), konfigurasi nama domain, URL, metode penyeimbangan, lalu klik **Next** (Selanjutnya).

Nama domain: nama domain server asli Anda (misalnya, `www.example.com`).

Nama domain default: jika permintaan seorang klien tidak cocok dengan nama domain pendengar, instance CLB akan meneruskan permintaan tersebut ke nama domain default (server default). Setiap pendengar dapat dikonfigurasi hanya dengan satu nama domain default. Jika pendengar tidak memiliki nama domain default, instance CLB akan meneruskan permintaan ke nama domain pertama. Contoh ini akan melewati langkah konfigurasi.

URL: jalur akses ke server asli Anda (misalnya, `/image/`).

Pilih **Weighted Round Robin** (Round Robin Tertimbang) sebagai metode penyeimbangan lalu klik **Next** (Berikutnya). Untuk informasi selengkapnya, lihat [Metode Penyeimbangan Muatan](#).

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](#)

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

Gzip compression

3. Aktifkan pemeriksaan kesehatan. Gunakan nilai default untuk domain pemeriksaan dan bidang jalur, lalu klik **Next** (Berikutnya).

Create Forwarding rules

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

Health Check

Check Domain

Path

[Show advanced options](#)

4. Nonaktifkan persistensi sesi lalu klik **Submit** (Kirim).

Untuk informasi selengkapnya tentang pendengar CLB, lihat [Ikhtisar Pendengar CLB](#).

Keterangan :

Aturan penerus: setiap pendengar dapat dikonfigurasi dengan beberapa nama domain, dan setiap nama domain dapat dikonfigurasi dengan beberapa URL. Anda dapat memilih nama pendengar atau domain, lalu klik ikon + untuk membuat aturan baru.

Persistensi sesi: jika persistensi sesi dinonaktifkan dan metode round-robin dipilih, permintaan dari klien yang sama akan ditetapkan ke berbagai server asli secara berurutan; jika persistensi sesi diaktifkan, atau dinonaktifkan tetapi metode penyeimbangan `ip_hash` digunakan, permintaan dari klien yang sama akan selalu ditetapkan ke server asli yang sama.

Ikut server asli dengan pendengar

Jika seorang klien memulai permintaan, instance CLB akan meneruskan permintaan tersebut ke instance CVM yang terikat dengan pendengarnya untuk pemrosesan.

1. Di tab **Listener Management** (Manajemen Pendengar), klik + untuk memperluas pendengar baru. Klik URL, dan klik **Bind** (Ikut) di bagian **Forwarding Rules** (Aturan Penerusan) di sisi kanan.

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

Note: When custom redirection policies are configured, the original forwarding rules are modified, the redirection policies will be removed automatically to configure it again. See details

HTTP/HTTPS Listener

Create

Listener1(HTTP:80)

- www.example.com
 - /image/

Forwarding Rules Expand

Bound Real Server

Bind Modify Port Modify Weight Unbind

2. Di jendela pop-up, pilih **CVM** sebagai jenis instance, pilih dua instance CVM **rs-1** dan **rs-2** (yang berada di wilayah yang sama dengan instance CLB), atur port keduanya ke **80** dan bobot ke **10** (nilai default), lalu klik **Confirm** (Konfirmasikan).

Bind with backend service

Select an instance

CVM ENI Please enter the domain name

IP address Search by IP address

Instance ID/name

- rs-2
- rs-1
- [redacted]
- [redacted]

10 / page 1 / 1 page

Press Shift key to select more

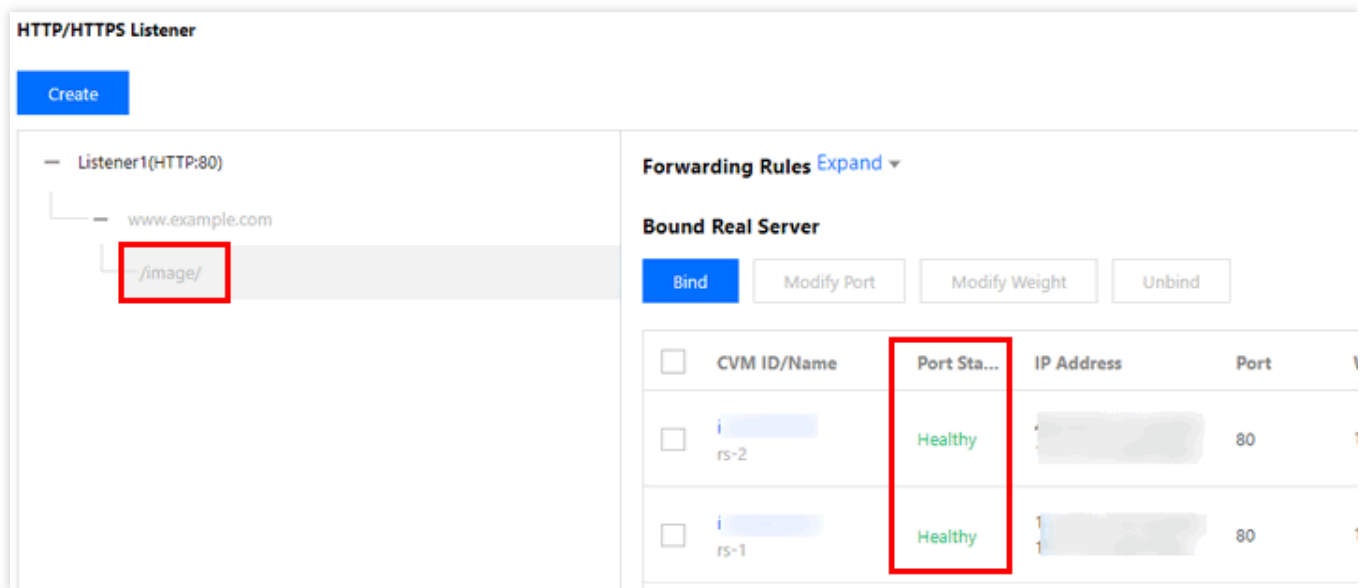
Selected (2)

Instance ID/name	Port	Weight
rs-2	80	10
rs-1	80	10

Confirm Cancel

3. Sekarang Anda dapat melihat instance CVM terikat dan status pemeriksaan kesehatannya di bagian **Forwarding Rules** (Aturan Penerusan). Jika status kesehatan port adalah **Healthy** (Sehat), instance CVM biasanya dapat

memproses permintaan yang diteruskan oleh instance CLB.



The screenshot shows the configuration of an HTTP/HTTPS Listener. The listener is named "Listener1(HTTP:80)" and is configured for the domain "www.example.com". A path "/image/" is highlighted with a red box. The "Forwarding Rules" section is expanded, showing a "Bound Real Server" table with two entries, both marked as "Healthy". The "Port Sta..." column in the table is also highlighted with a red box.

<input type="checkbox"/>	CVM ID/Name	Port Sta...	IP Address	Port	1
<input type="checkbox"/>	rs-2	Healthy		80	1
<input type="checkbox"/>	rs-1	Healthy		80	1

Perhatian :

Satu aturan penerusan (protokol pendengar, port, nama domain, dan URL) dapat diikat dengan beberapa port dari instance CVM yang sama. Jika seorang pengguna men-deploy layanan yang sama di port **80** dan **81** dari **rs-1**, kedua port dapat diikat dengan aturan penerusan contoh dan keduanya akan menerima permintaan yang diteruskan oleh instance CLB.

Langkah 3: Mengonfigurasi Grup Keamanan

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

Setelah mengonfigurasi grup keamanan, Anda dapat mengaktifkan atau menonaktifkan fitur **Allow Traffic by Default** (Izinkan Lalu Lintas secara Default):

Metode 1: Aktifkan "Allow Traffic by Default in Security Group" (Izinkan Lalu Lintas secara Default di Grup Keamanan)

Untuk informasi selengkapnya, silakan lihat [Konfigurasi Grup Keamanan CLB](#).

Metode 2: Izinkan IP klien khusus di grup keamanan CVM

Untuk informasi selengkapnya, silakan lihat [Konfigurasi Grup Keamanan CLB](#).

Langkah 4: Memverifikasi Layanan CLB

Setelah mengonfigurasi instance CLB, Anda dapat memverifikasinya dengan mengakses berbagai server asli melalui **domain names and URLs** (nama domain dan URL) yang berbeda di instance CLB yang sama, atau memverifikasi fitur **Content-based Routing** (Perutean berbasis Konten).

Metode 1: Konfigurasi `hosts` dan petakan nama domain ke instance CLB

1. Di perangkat Windows, modifikasi file **hosts** (host) di direktori `C:\Windows\System32\drivers\etc`, dan petakan nama domain ke VIP dari instance CLB.

```
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
[redacted] www.example.com
```

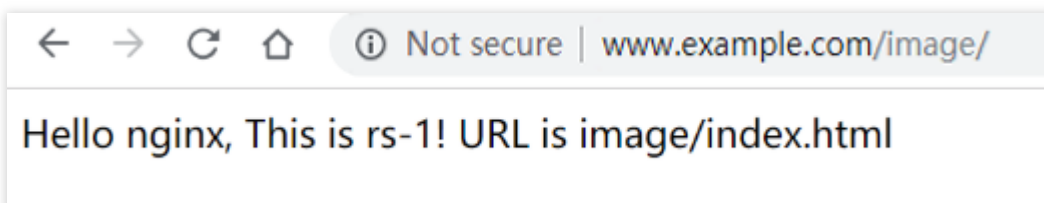
2. Untuk memverifikasi berhasil tidaknya konfigurasi **hosts** (host), Anda dapat menjalankan perintah **ping** di **cmd.exe** untuk menguji apakah nama domain berhasil diikat dengan VIP. Jika ada yang dikembalikan, paket data berhasil diikat.

```
C:\Users\Administrator>ping www.example.com

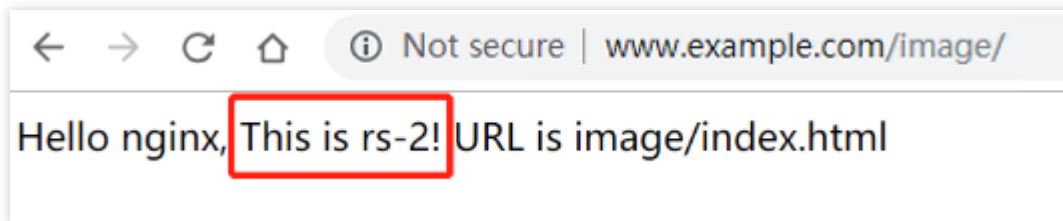
Pinging www.example.com [redacted] with 32 bytes of data:
Reply from [redacted]: bytes=32 time=159ms TTL=48
Reply from [redacted]: bytes=32 time=149ms TTL=48
Reply from [redacted]: bytes=32 time=158ms TTL=48
Reply from [redacted]: bytes=32 time=150ms TTL=48

Ping statistics for [redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 149ms, Maximum = 159ms, Average = 154ms
```

3. Uji layanan CLB dengan mengakses `http://www.example.com/image/` melalui peramban. Jika halaman Anda mengembalikan gambar berikut, berarti permintaan telah diteruskan oleh instance CLB ke CVM rs-1, dan CVM biasanya telah memproses permintaan tersebut dan mengembalikan halaman layanan.



4. Karena metode penyeimbangan pendengar berupa round robin tertimbang, dan bobot kedua instance CVM adalah 10, maka Anda dapat memuat ulang peramban untuk memulai permintaan lagi. Jika halaman Anda mengembalikan gambar berikut, berarti permintaan telah diteruskan oleh instance CLB ke CVM rs-2.



Perhatian :

/ di **image/** tidak dapat dihilangkan. / menunjukkan bahwa **image** (gambar) adalah direktori default, bukan nama file.

Mengonfigurasi Pengalihan (opsional)

CLB mendukung pengalihan otomatis dan pengalihan manual. Untuk informasi selengkapnya, silakan baca

[Mengonfigurasi Pengalihan Lapisan-7](#).

Pengalihan otomatis (HTTPS paksa): ketika PC atau peramban seluler mengakses layanan web dengan permintaan HTTP, respons HTTPS dikembalikan ke peramban setelah permintaan melewati proksi CLB sehingga memaksa peramban untuk mengakses halaman web menggunakan HTTPS.

Pengalihan manual: jika Anda ingin menonaktifkan bisnis web sementara waktu untuk kasus-kasus seperti penjualan produk, pemeliharaan halaman, atau pembaruan dan peningkatan, Anda perlu mengalihkan halaman asal ke halaman baru. Jika tidak, alamat lama di database favorit dan mesin pencarian pengunjung akan mengembalikan halaman pesan kesalahan 404 atau 503 sehingga mengganggu pengalaman pengguna dan mengakibatkan pemborosan lalu lintas serta bahkan membatalkan akumulasi skor pada mesin pencarian.

Operasi yang Relevan

[Men-deploy Web Java di CentOS](#)

[Menginstal dan Mengonfigurasi PHP](#)

Memulai CLB IPv6

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

CLB mendukung tiga versi IP:IPv4, IPv6, dan IPv6 NAT64. CLB IPv6 mendukung protokol TCP, UDP, TCP SSL, HTTP, dan HTTPS serta memberikan kemampuan meneruskan yang fleksibel berdasarkan nama domain dan jalur URL. Dokumen ini menjelaskan kepada Anda cara memulai IPv6 CLB.

Keterangan :

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

Prasyarat

1. CLB hanya meneruskan lalu lintas tetapi tidak dapat memproses permintaan; oleh karena itu, Anda harus membuat instance CVM yang memproses permintaan pengguna terlebih dahulu lalu menyelesaikan konfigurasi IPv6 untuknya.
2. Dokumen ini mengambil penerusan HTTP sebagai contoh. Server web yang sesuai (seperti Apache, Nginx, atau IIS) harus di-deploy pada instance CVM, dan port yang digunakan server harus mendengarkan IPv6.

Petunjuk

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.

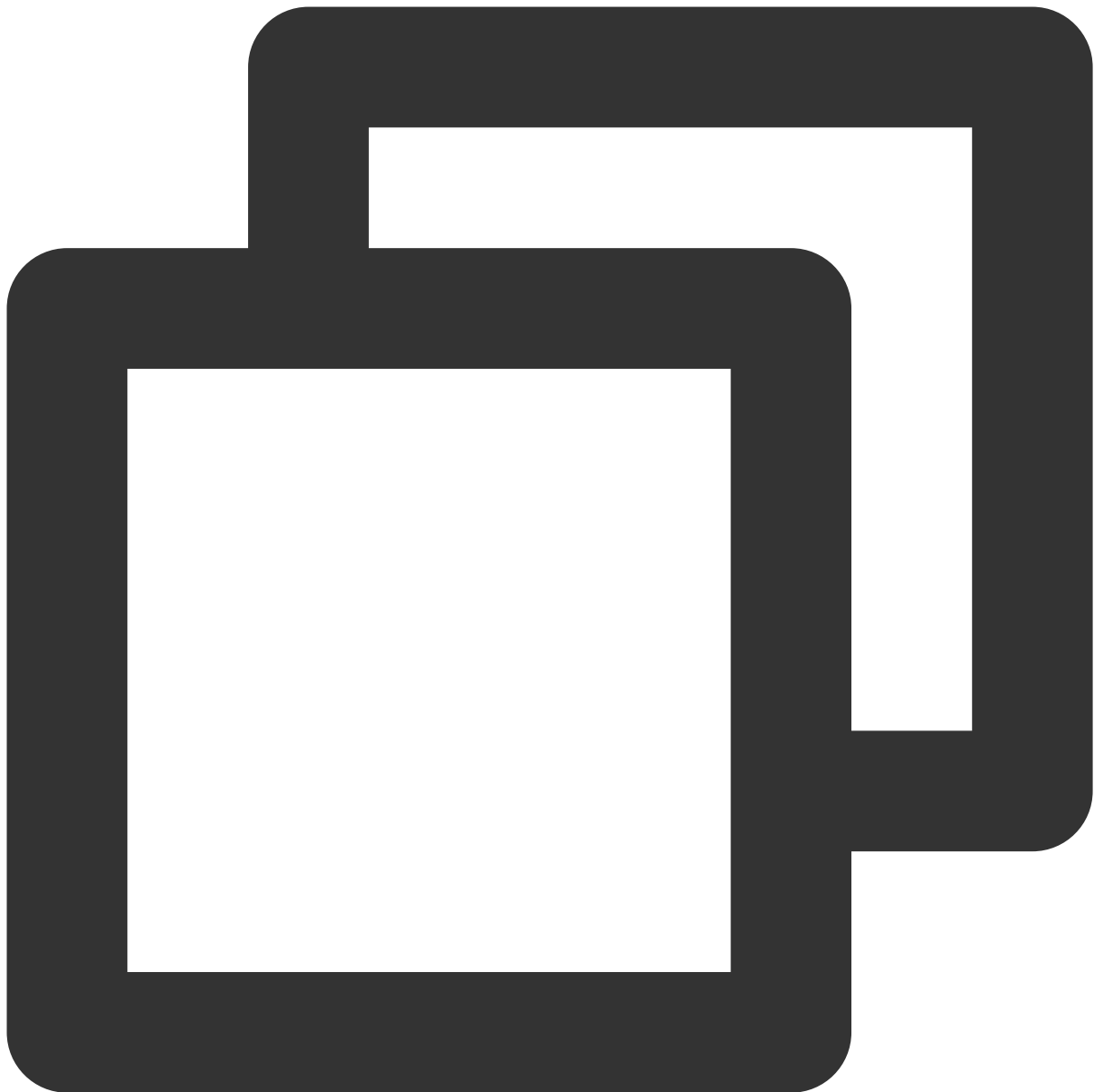
CLB IPv6 mendukung upaya mendapatkan alamat sumber IPv6 klien, yang dapat langsung diperoleh dengan lapisan-4 CLB IPv6 atau melalui header `X-Forwarded-For` dari HTTP lapisan-7 IPv6 CLB.

Saat ini, CLB IPv6 menyeimbangkan muatan sepenuhnya lewat jaringan publik. Klien di VPC yang sama tidak dapat mengakses CLB IPv6 lewat jaringan privat.

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

Langkah 1. Buat instance CVM dan konfigurasi IPv6

1. Masuk ke [Konsol CVM](#), masuk ke instance CVM, lalu selesaikan konfigurasi IPv6 dasar.
2. Pada instance CVM, jalankan perintah berikut secara berurutan untuk men-deploy dan memulai ulang layanan Nginx.



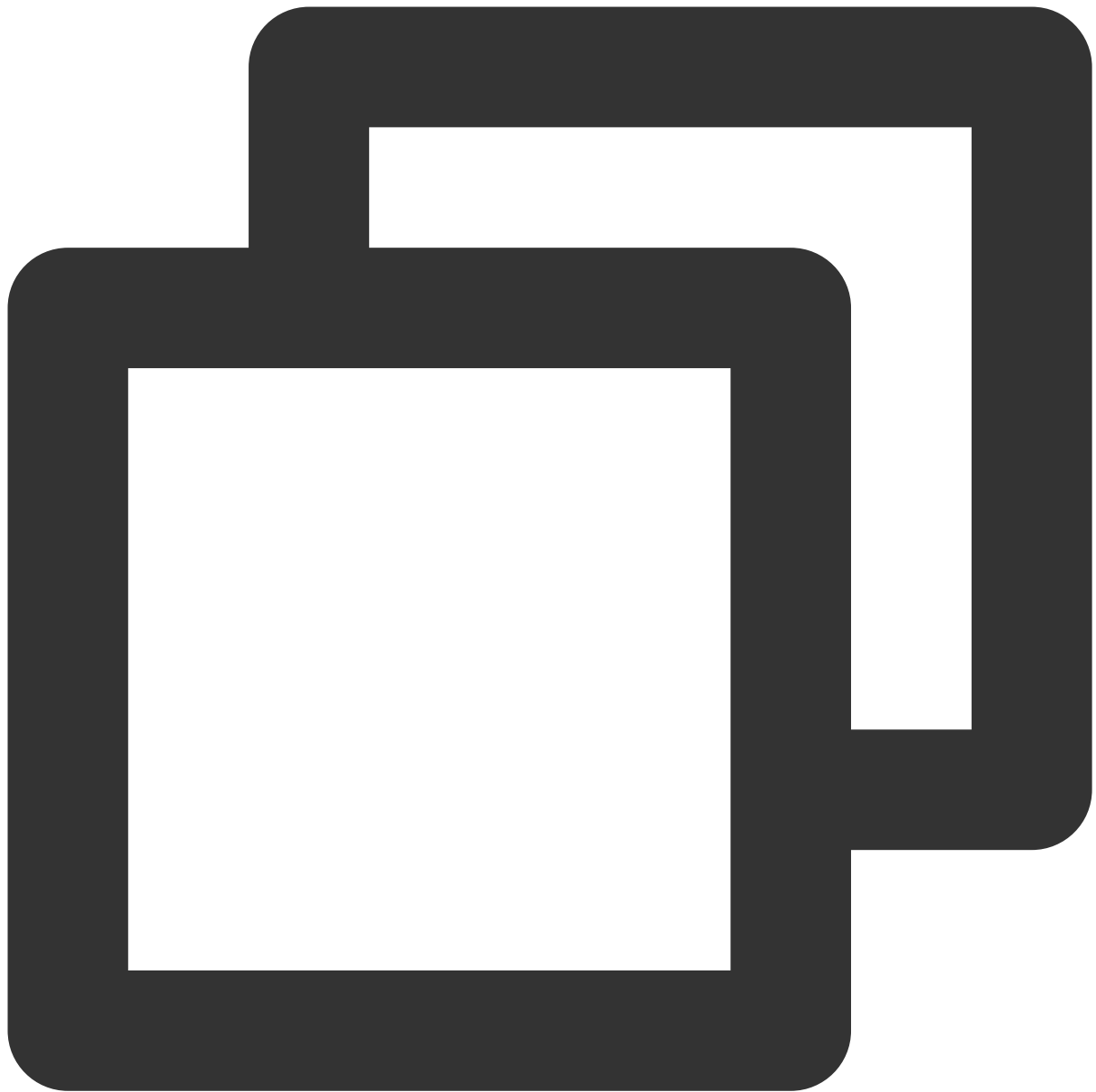
```
yum instal nginx  
mulai ulang layanan nginx
```

3. Peris

ksa apaka

h layanan Nginx yang di-deploy pada instance CVM mendengarkan IPv6.

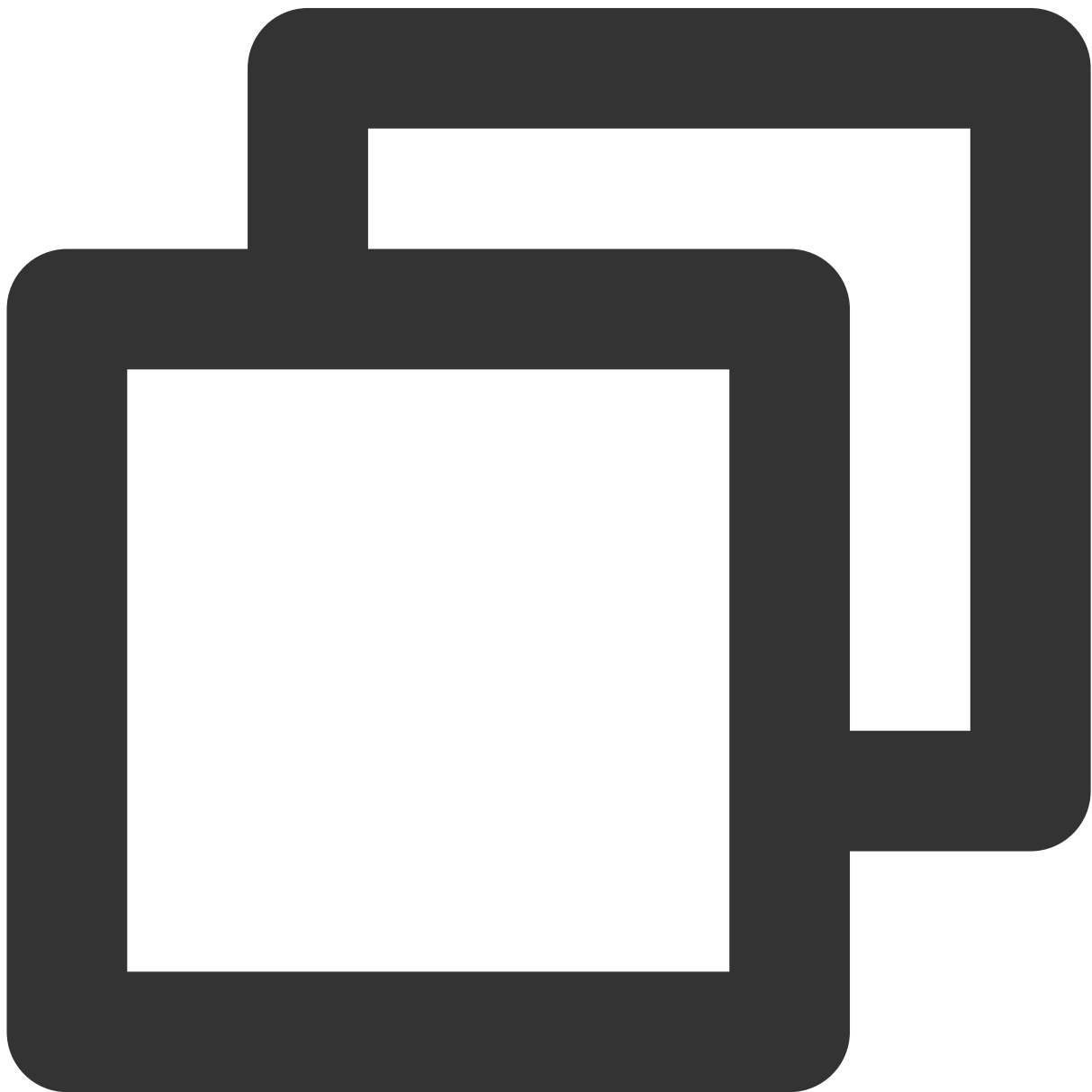
3.1 Jalankan perintah berikut untuk pemeriksaan.



```
netstat -tupln
```

```
[root@VM_0_14_centos ~]# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State                   PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN                  4314/nginx: master
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN                  3175/sshd
tcp6       0      0 :::80                  :::*                    LISTEN                  4314/nginx: master
udp        0      0 0.0.0.0:68             0.0.0.0:*               *                       2890/ncclient
udp        0      0 10.24.0.14:123         0.0.0.0:*               *                       3369/ntpd
udp        0      0 127.0.0.1:123          0.0.0.0:*               *                       3369/ntpd
udp        0      0 0.0.0.0:56713          0.0.0.0:*               *                       4333/ntpd
udp6       0      0 fe80::5054:ff:fe3d::546 :::*                    *                       4119/dhclient
udp6       0      0 2402:4e00:1400:1217:123 :::*                    *                       3369/ntpd
udp6       0      0 fe80::5054:ff:fe3d::123 :::*                    *                       3369/ntpd
udp6       0      0 :::1:123               :::*                    *                       3369/ntpd
```

3.2 Jalankan perintah berikut untuk membuka file konfigurasi Nginx untuk pemeriksaan.




```
vim /etc/nginx/nginx.conf
```

```
# Load modular configuration files from the /etc/nginx/conf.d directory.
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;

server {
    listen      80 default server;
    listen      [::]:80 default_server;
    server_name _;
    root        /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
    }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }
}

# Settings for a TLS enabled server.
#
#
server {
#
    listen      443 ssl http2 default server;
#
    listen      [::]:443 ssl http2 default_server;
#
    server_name _;
#
    root        /usr/share/nginx/html;
#
#
    ssl_certificate "/etc/pki/nginx/server.crt";
#
    ssl_certificate_key "/etc/pki/nginx/private/server.key";
#
    ssl_session_cache shared:SSL:1m;
#
}
```

Langkah 2. 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. Pilih item konfigurasi masing-masing di halaman pembelian dan klik **Buy Now** (Beli Sekarang).

4. Di halaman "CLB Instance List" (Daftar Instance CLB), pilih wilayah yang sesuai untuk melihat instance yang baru saja dibuat.

ID/Name	Monitoring	Status	VIP	Availability Zone	Network	ISP	Health Status	Billing Mode	Bandwidth	Project	Tag	Bind
		Normal		Qingyuan Zone 1	Public Network	BGP	Health check not enabled (Configuration)	Pay-as-you-go - bandwidth Created at 2020-08-06 11:32	1Mbps	Default Project	-	-

Langkah 3. Buat pendengar CLB IPv6

Mengonfigurasi protokol pendengar dan port HTTP

1. Masuk ke [Konsol CLB](#).
2. Di "CLB Instance List" (Daftar Instance CLB), cari instance CLB yang dibuat dan klik ID-nya untuk masuk ke halaman detail.
3. Di modul "Basic Information" (Informasi Dasar), Anda dapat mengklik ikon modifikasi di samping nama instance untuk mengganti namanya.
4. Di **HTTP/HTTPS Listeners** (Pendengar HTTP/HTTPS) di "Manajemen Pendengar", klik **Create** (Buat) untuk membuat pendengar CLB.

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

Note: When custom redirection policies are configured, the original forwarding rules are modified, the redirection policies will be removed automatically. Please re-configure it again. [See details](#)

HTTP/HTTPS Listener

Create

You've not created any listeners. [Create Now](#) Click to display details

TCP/UDP/TCP SSL Listener

Create

You've not created any listeners. [Create Now](#) Click to display details

5. Di jendela pop-up, konfigurasi berikut ini:

Atur nama ke "IPv6test", misalnya.

Atur protokol dan port pendengar ke `HTTP:80` .

6. Klik **Submit** (Kirim) untuk membuat pendengar CLB.

Mengonfigurasi aturan meneruskan pendengar

1. Di "Manajemen Pendengar", pilih pendengar baru IPv6test dan klik **+** untuk menambahkan aturan.
2. Di jendela pop-up, konfigurasi nama domain, jalur URL, dan metode penyeimbangan, lalu klik **Next** (Selanjutnya).

Nama Domain: nama domain yang digunakan oleh server asli Anda, yang bisa berisi kartubebas. Dalam contoh ini,

`www.qcloudipv6test.com` digunakan. Untuk informasi selengkapnya, silakan lihat [Lapisan-7 Meneruskan Aturan Nama Domain dan URL](#).

Jalur URL: jalur akses server asli Anda. `/` digunakan dalam contoh ini.

Pilih "WRR" untuk mode penyeimbang muatan.

Create Forwarding rules ✕

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

Domain Name ⓘ

Default Domain Name **Enable**
If a client request does not match any domain names of this listener, the CLB instance will forward the request to the default domain name (Default Server). Each listener only can configure one listener and must configure one. [Details](#)

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.

Get client IP **Enabled**

Gzip compression **Enabled** ⓘ

Target Group ⓘ

3. Konfigurasi pemeriksaan kesehatan: aktifkan pemeriksaan kesehatan, periksa nama domain dan jalur meneruskan default yang digunakan oleh nama domain, lalu klik **Next** (Selanjutnya).

Create Forwarding rules

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

Health Check 

Check Domain  It defaults to the forwarded domain

Path  Root Directory of CVM  /

[Show advanced options](#) 

Back

Next

4. Konfigurasi persistensi sesi: aktifkan persistensi sesi, konfigurasi periode persistensi, lalu klik **Submit** (Kirim).

Create Listener

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

Session Persistence 

Hold Time   30 Seconds 3600 Seconds  54  Seconds

Session persistence based on the source IP

Back

Submit

Untuk informasi selengkapnya tentang pendengar CLB, lihat [Ikhtisar Pendengar CLB](#).

Keterangan :

Pendengar (yaitu protokol:port yang mendengarkan) dapat dikonfigurasi dengan beberapa nama domain, dan nama domain dapat dikonfigurasi dengan beberapa jalur URL. Pilih nama pendengar atau domain dan klik + untuk membuat aturan baru.

Persistensi sesi: jika persistensi sesi dinonaktifkan dan metode round-robin digunakan untuk menyusun jadwal, permintaan akan ditetapkan ke berbagai server asli secara berurutan; jika persistensi sesi diaktifkan, atau dinonaktifkan tetapi penjadwalan ip_hash digunakan, permintaan akan selalu ditetapkan ke server asli yang sama.

Mengikat instance CVM

Keterangan :

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

1. Di halaman "Listener Management" (Manajemen Pendengar), pilih dan perluas pendengar yang barusan dibuat lalu pilih nama domain dan jalur URL, sedangkan informasi IPv6 dari instance CVM yang terikat ke jalur URL akan ditampilkan di sisi kanan. Klik **Bind** (Ikut).
2. Di jendela pop-up, pilih instance CVM, atur port layanan Nginx default ke 80, atur bobot (10 secara default), dan klik **OK** (Oke).

Bind with backend service

Select an instance

IP address

Instance ID/name

<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	

10 / page 1 / 1 page

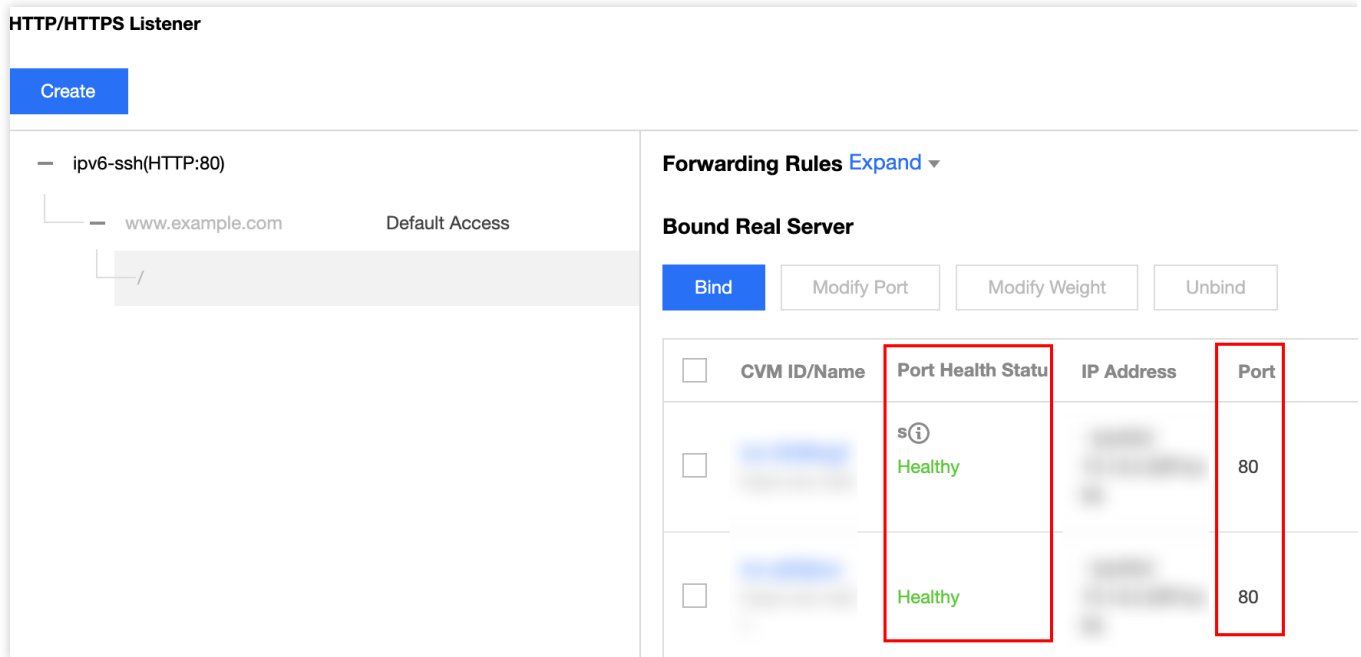
Press Shift key to select more

Selected (2)

Instance ID/name	Port	Weight <input type="button" value="i"/>
	<input type="text" value="80"/>	<input type="button" value="-"/> 10 <input type="button" value="+"/> <input type="button" value="↔"/>
	<input type="text" value="80"/>	<input type="button" value="-"/> 10 <input type="button" value="+"/> <input type="button" value="↔"/>

3. Setelah instance CVM berhasil diikat, lakukan berikut ini:

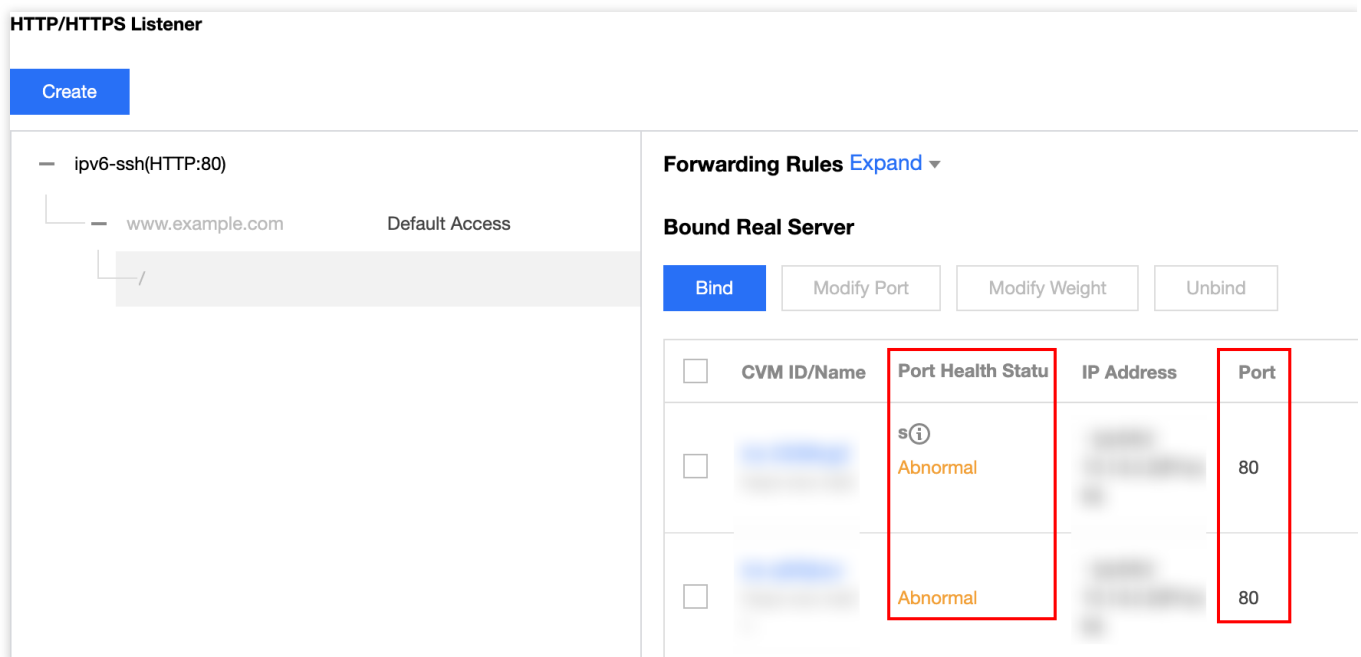
Periksa apakah status port "healthy" (sehat) atau tidak; dan jika sehat, silakan lanjut ke [Langkah 4.Uji IPv6 CLB](#).



The screenshot displays the 'HTTP/HTTPS Listener' configuration page. On the left, there is a tree view showing the listener configuration for 'ipv6-ssh(HTTP:80)' with a 'Default Access' rule for 'www.example.com'. On the right, the 'Forwarding Rules' section is expanded to show 'Bound Real Server'. A table lists two real servers, both with a 'Healthy' status, which is highlighted by a red box. The 'Port' column for both servers is also highlighted by a red box.

<input type="checkbox"/>	CVM ID/Name	Port Health Statu	IP Address	Port
<input type="checkbox"/>	[blurred]	Healthy	[blurred]	80
<input type="checkbox"/>	[blurred]	Healthy	[blurred]	80

Jika status port "exceptional" (luar biasa), periksa apakah pendengar terikat ke port layanan Nginx yang benar dari instance CVM, dan masuk ke instance CVM untuk memeriksa apakah port mendengar IPv6 secara normal atau tidak. Anda dapat melakukan pemeriksaan sesuai petunjuk di [sublangkah 3 di langkah 1](#) untuk melakukan pemeriksaan.



The screenshot displays the 'HTTP/HTTPS Listener' configuration page, similar to the previous one. However, the 'Bound Real Server' table shows two servers with an 'Abnormal' status, which is highlighted by a red box. The 'Port' column for both servers is also highlighted by a red box.

<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

Langkah 4.Uji IPv6 CLB

Setelah mengonfigurasi instance IPv6 CLB, Anda dapat memverifikasi aktif tidaknya arsitektur dengan memeriksa apakah nama domain dan URL yang berbeda-beda di dalam instance CLB dapat mengakses server asli yang berlainan, yaitu memeriksa apakah fitur perutean berbasis konten sudah tersedia atau belum.

Gunakan klien dengan kemampuan akses jaringan publik IPv6 untuk mengakses nama domain atau alamat IPv6 dari instance CLB. Jika dapat mengakses layanan web instance CVM sebagaimana mestinya, instance CLB IPv6 sudah bekerja normal.

Memulai CLB Klasik

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

Dokumen ini menjelaskan cara membuat instance CLB Klasik jaringan publik bernama `clb-test` dan meneruskan permintaan dari klien ke dua server asli.

Prasyarat

1. CLB hanya meneruskan lalu lintas tetapi tidak dapat memproses permintaan; oleh karena itu, Anda harus memiliki instance CVM yang memproses permintaan pengguna.

Dalam contoh ini, dua instance CVM sudah cukup, tetapi Anda juga dapat mengonfigurasi instance lebih banyak lagi. Instance CVM `rs-1` dan `rs-2` telah dibuat di wilayah Guangzhou dalam contoh ini. Untuk informasi selengkapnya tentang cara membuat instance CVM, lihat [Membeli dan Meluncurkan Instance CVM](#).

2. Dokumen ini mengambil penerusan HTTP sebagai contoh. Server web yang sesuai (seperti Apache, Nginx, atau IIS) harus di-deploy pada instance CVM.

Untuk memverifikasi hasil, dalam contoh ini, Apache di-deploy di `rs-1` dan juga `rs-2`. Apache mengembalikan "Halo Tomcat!Ini adalah rs-1!" di `rs-1` dan "Halo Tomcat!Ini adalah rs-2!" di `rs-2`. Untuk informasi selengkapnya tentang cara men-deploy komponen pada instance CVM, lihat [Men-deploy Web Java di Linux \(CentOS\)](#) dan [Menginstal dan Mengonfigurasi PHP di Windows](#).

3. Akses IP publik dan jalur instance CVM Anda. Jika halaman yang di-deploy ditampilkan, layanan telah berhasil di-deploy.

Perhatian :

Untuk akun tambahan, bandwidth jaringan publik harus dibeli untuk instance CVM karena bandwidth ditagih oleh CVM, bukan CLB. Anda dapat menentukan jenis akun sesuai petunjuk di [Ikhtisar Penagihan](#).

Dalam contoh, nilai yang dikembalikan oleh layanan yang di-deploy di dua server asli adalah berbeda. Dalam skenario aktual, layanan yang sama biasanya harus di-deploy di semua server asli untuk memastikan agar semua pengguna memiliki pengalaman yang seragam.

Membeli Instance CLB Klasik

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

2. Dalam contoh ini, pilih **Guangzhou** sebagai wilayah yang sama dengan wilayah di instance CVM. Pilih **Classic** (Klasik) sebagai jenis instance, **Public Network** (Jaringan Publik) sebagai atribut jaringan, dan **Default-VPC (Default)** sebagai jaringan dan masukkan "clb-test" sebagai nama instance.

3. Klik **Buy Now** (Beli Sekarang) dan lakukan pembayaran. Untuk informasi selengkapnya tentang instance CLB,

silakan lihat [Pilihan Atribut Produk](#).

4. Di halaman "CLB Instance List" (Daftar Instance CLB), pilih wilayah yang sesuai untuk melihat instance yang baru saja dibuat.

ID/Name	Monitor...	Status	Domain Name	VIP	Network...	Network	Health Status	Creatio
clb-test		Normal		1	Public Network		Health check not enabled (Configuration)	2019-01-0

Membuat Pendengar CLB

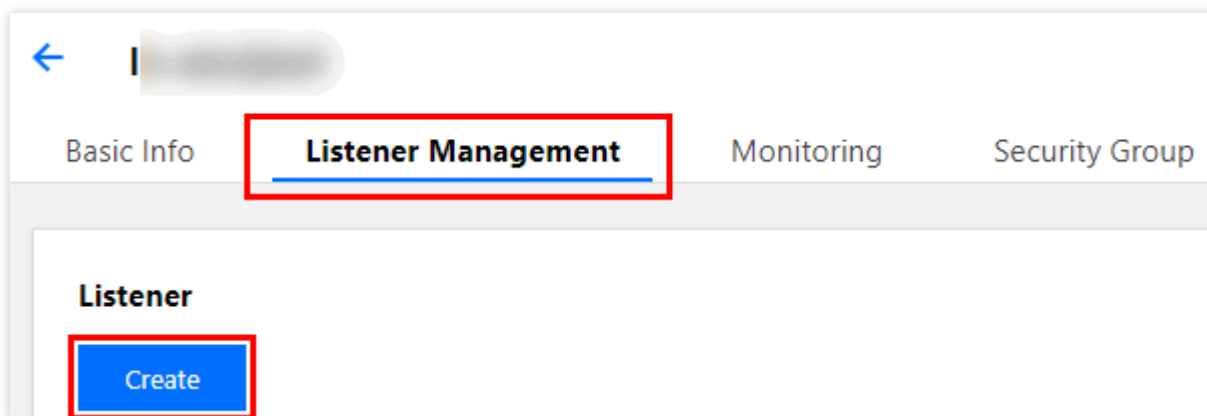
Pendengar CLB meneruskan permintaan dengan menetapkan protokol dan port. Dokumen ini mengambil konfigurasi meneruskan permintaan klien HTTP menggunakan CLB sebagai contoh.

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

2. Di "CLB Instance List" (Daftar Instance CLB), cari instance CLB Klasik `clb-test` yang dibuat dan klik ID-nya untuk masuk ke halaman detail.

3. Di bagian "Basic Info" (Info Dasar), Anda dapat mengklik "Edit" (Edit) di samping nama instance untuk mengganti namanya.

4. Di **Listeners** (Pendengar) di "Manajemen Pendengar", klik **Create** (Buat) untuk membuat pendengar CLB.



5. Di jendela pop-up, konfigurasi berikut ini:

Atur nama ke "Listener1" (Pendengar1).

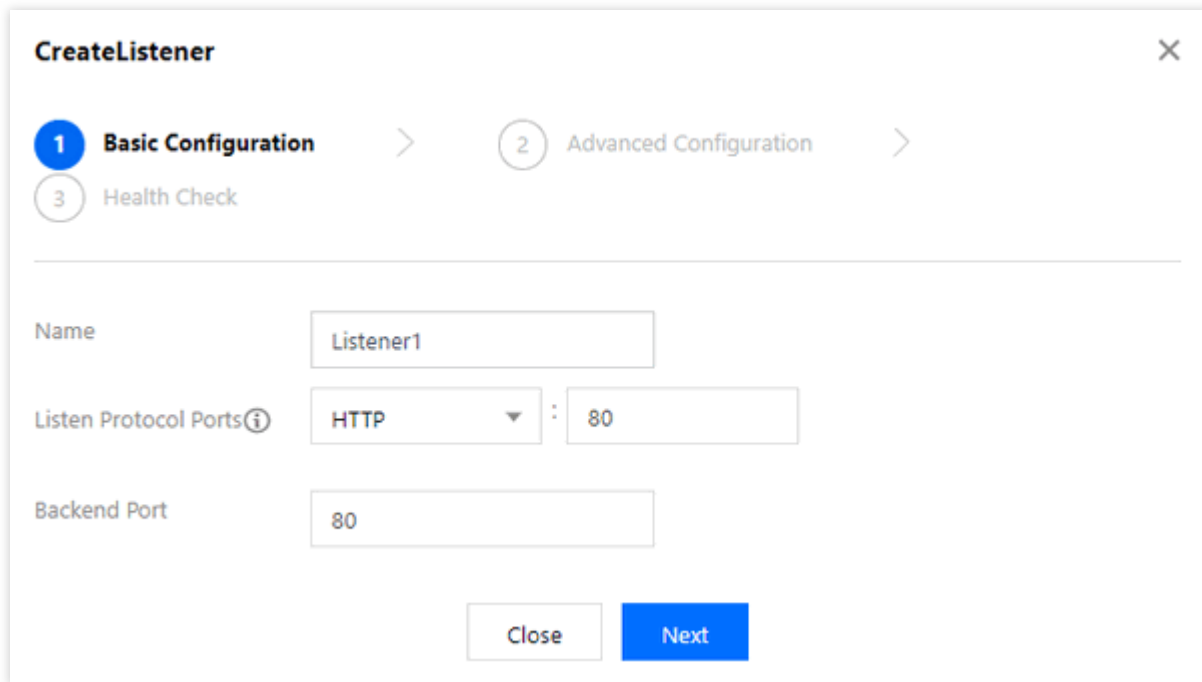
Atur protokol dan port pendengar ke `HTTP : 80` .

Atur port backend ke `80` .

Pilih "WRR" sebagai mode penyeimbang muatan.

Jangan periksa persistensi sesi.

Aktifkan pemeriksaan kesehatan.



CreateListener [Close]

1 **Basic Configuration** > 2 Advanced Configuration >
3 Health Check

Name: Listener1

Listen Protocol Ports ⓘ: HTTP : 80

Backend Port: 80

[Close] [Next]

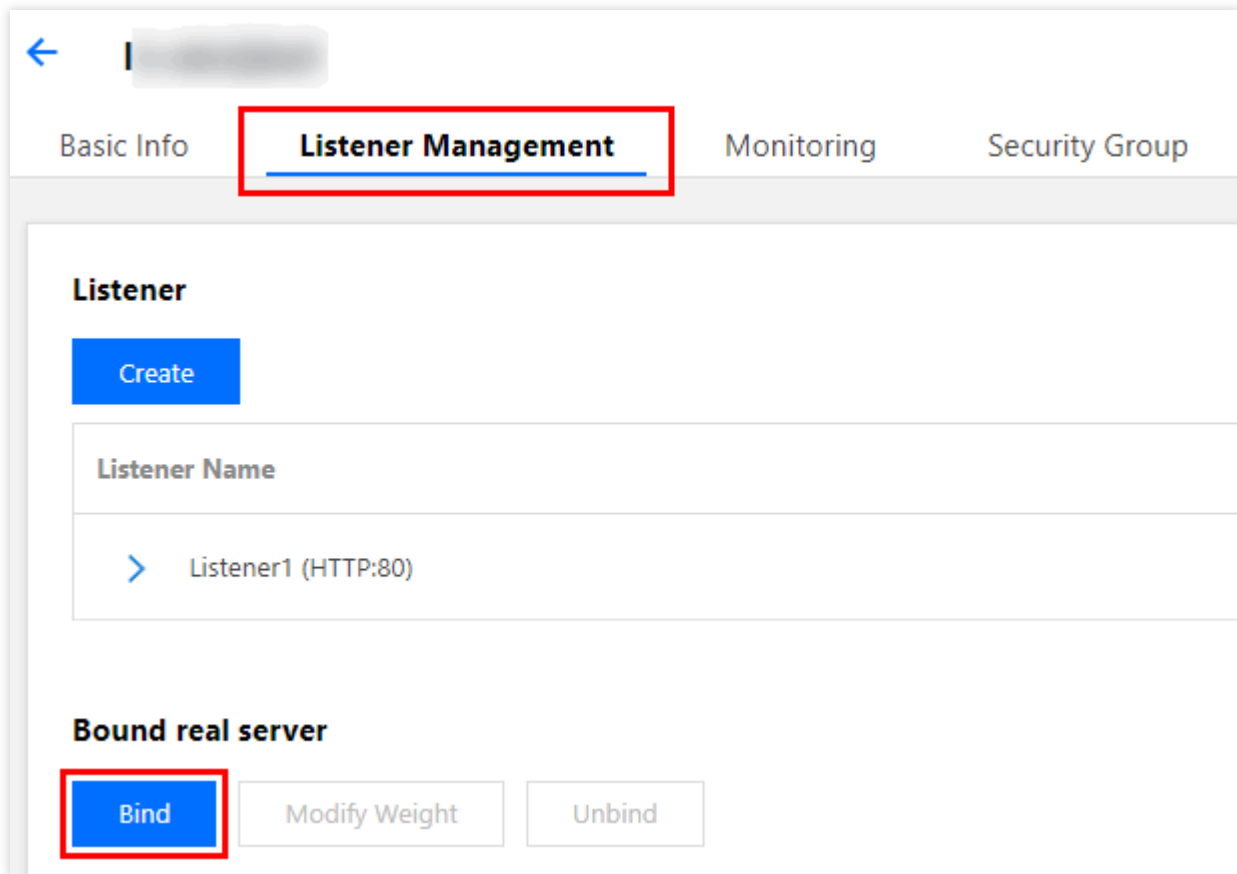
6. Klik **Complete** (Selesaikan) untuk membuat pendengar CLB.

Untuk informasi selengkapnya tentang pendengar CLB, lihat [Ikhtisar Pendengar CLB](#).

Mengikat Server Asli

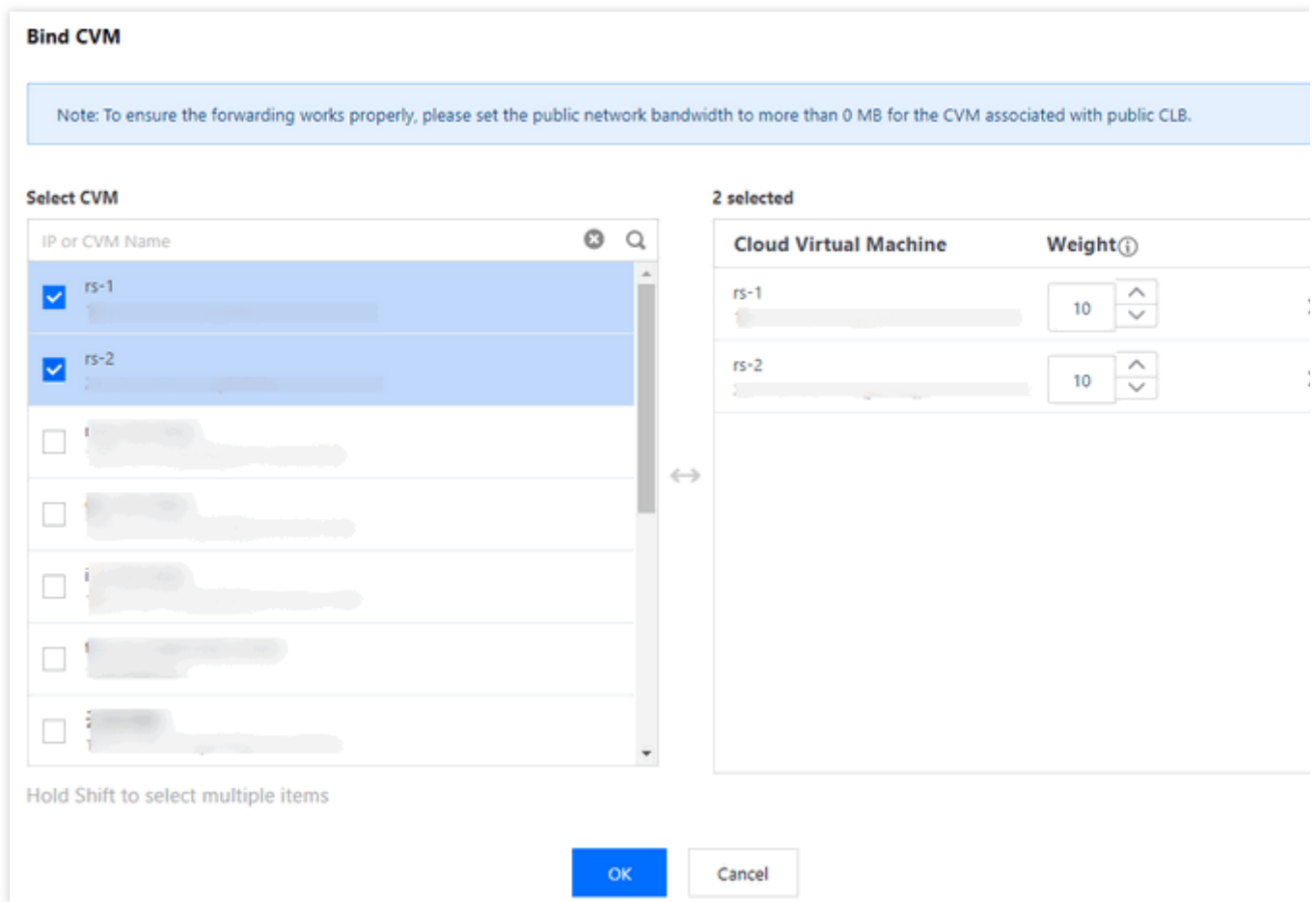
1. Di "CLB Instance List" (Daftar Instance CLB), cari `clb-test` yang dibuat dan klik ID-nya untuk masuk ke halaman detail.

2. Di modul "Bind Real Server" (Ikat Server Asli) di "Manajemen Pendengar", klik **Bind** (Ikat).



3. Di jendela pop-up, pilih instance CVM `rs-1` dan `rs-2` di wilayah yang sama dengan instance CLB dan pertahankan bobot default "10" untuk instance tersebut.

4. Klik **OK** (Oke) untuk menyelesaikan pengikatan.



5. Perluas pendengar **Listener1** (Pendengar1). Anda dapat melihat status pemeriksaan kesehatan dari instance CVM backend. Status "Healthy" (Sehat) menunjukkan bahwa instance CVM dapat memproses dengan semestinya permintaan yang diteruskan oleh CLB.

Mengonfigurasi Grup Keamanan

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

Setelah mengonfigurasi grup keamanan, Anda dapat memilih mengaktifkan atau menonaktifkan "Allow Traffic by Default in Security Group" (Izinkan Lalu Lintas secara Default di Grup Keamanan) dengan konfigurasi yang berbeda sebagai berikut:

Metode 1. Aktifkan "Allow Traffic by Default in Security Group" (Izinkan Lalu Lintas secara Default di Grup Keamanan)

Keterangan :

Fitur ini sedang dalam pengujian beta. Untuk mencobanya, silakan kirim tiket permohonan. Fitur ini tidak didukung untuk CLB jaringan privat klasik.

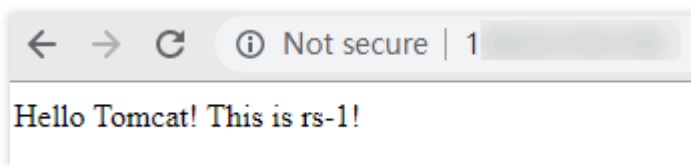
Untuk mendapatkan petunjuk lengkap, silakan lihat [Mengonfigurasi Grup Keamanan CLB](#).

Metode 2. Izinkan IP klien di dalam grup keamanan CVM

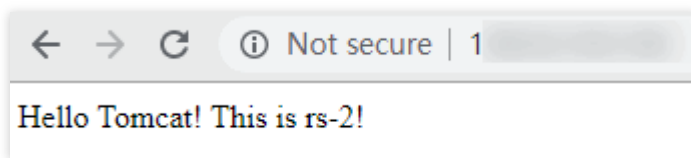
Untuk mendapatkan petunjuk lengkap, silakan lihat [Mengonfigurasi Grup Keamanan CLB](#).

Memverifikasi Layanan CLB

1. Masukkan alamat layanan dan port CLB `http://vip:80` ke peramban untuk menguji layanan CLB. Jika pesan ditampilkan seperti di bawah ini, permintaan telah diteruskan ke instance CVM `rs-1` oleh CLB, dan instance CVM telah memproses permintaan dengan semestinya dan mengembalikan hasilnya.



2. Algoritme round robin dari pendengar berupa "round robin tertimbang", dan bobot kedua instance CVM sama-sama "10". Jika Anda memuat ulang halaman web di peramban untuk mengirim permintaan baru, Anda dapat melihat bahwa permintaan tersebut diteruskan ke instance CVM `rs-2` oleh CLB.



Perhatian :

Jika persistensi sesi dinonaktifkan dan metode round-robin digunakan untuk penjadwalan, permintaan akan ditetapkan ke server asli yang berbeda secara berurutan.

Jika persistensi sesi diaktifkan, atau dinonaktifkan tetapi penjadwalan ip_hash digunakan, permintaan akan selalu ditetapkan ke server asli yang sama.

Men-deploy Nginx di CentOS

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

Dokumen ini menjelaskan cara men-deploy proyek-proyek Nginx di CentOS dan cocok untuk setiap pengguna baru Tencent Cloud.

Versi Perangkat Lunak

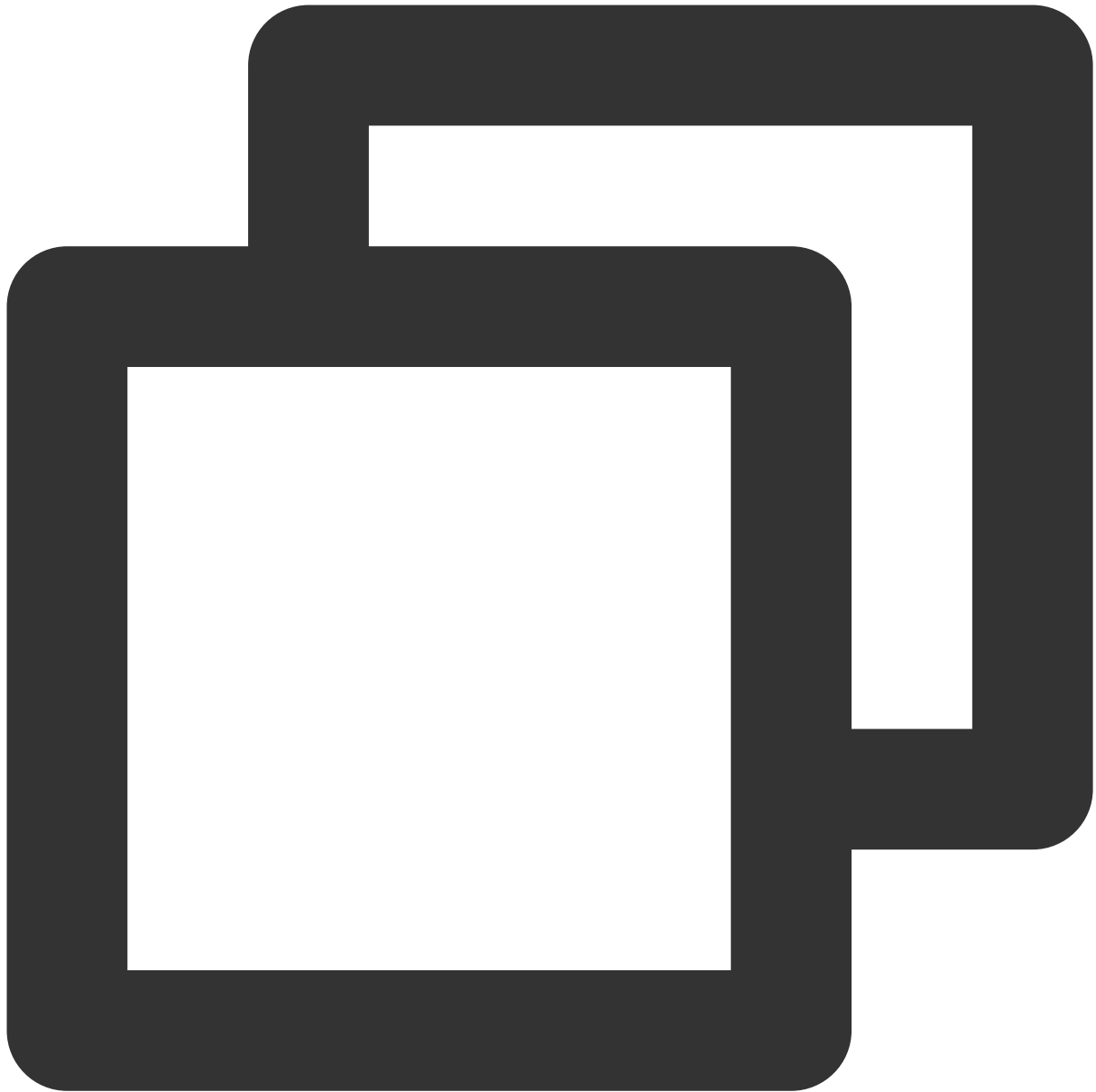
Versi alat perangkat lunak yang digunakan dalam dokumen ini adalah sebagai berikut, yang mungkin berbeda dengan versi perangkat lunak Anda selama operasi aktual.

Sistem operasi:CentOS 7.5

Nginx:Nginx 1.16.1

Menginstal Nginx

1.Setelah menyelesaikan pembelian, klik **Masuk** (Masuk) di halaman detail CVM untuk masuk ke instance CVM Anda lalu masukkan nama pengguna dan kata sandi guna menyiapkan lingkungan Nginx.Untuk informasi selengkapnya tentang cara membuat instance CVM, lihat [Membuat Instance CVM](#).



```
# Instal Nginx
yum -y instal nginx
# Lihat versi Nginx
nginx -v
# Lihat direktori penginstalan Nginx
rpm -ql nginx
# Mulai Nginx
mulai layanan nginx
```

2. Akses alamat IP publik dari instance CVM dan jika muncul halaman berikut, Nginx berhasil di-deploy:

Welcome to **nginx** on Fedora!

This page is used to test the proper operation of the **nginx** HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

Website Administrator

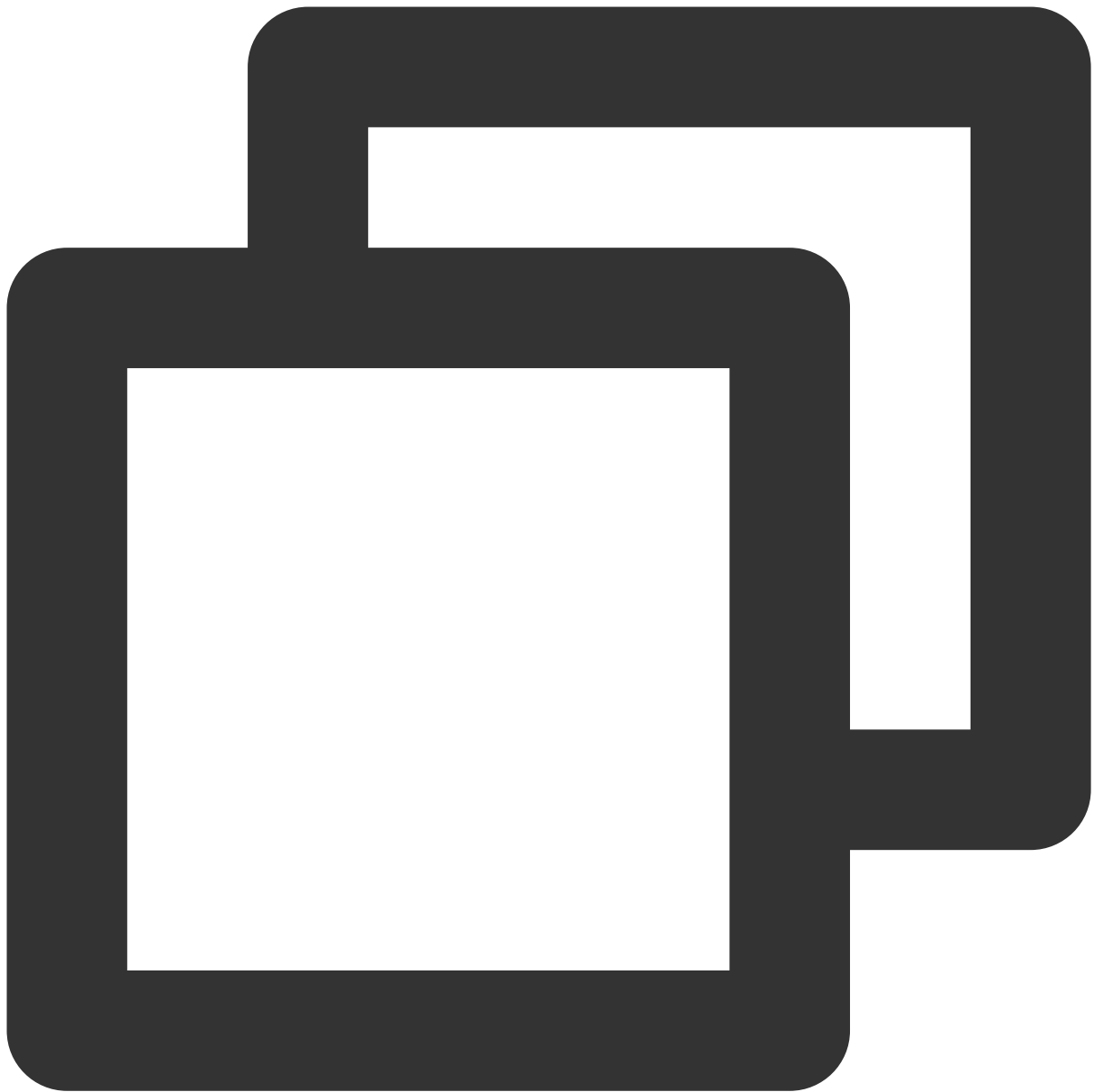
This is the default `index.html` page that is distributed with **nginx** on Fedora. It is located in `/usr/share/nginx/html`.

You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.



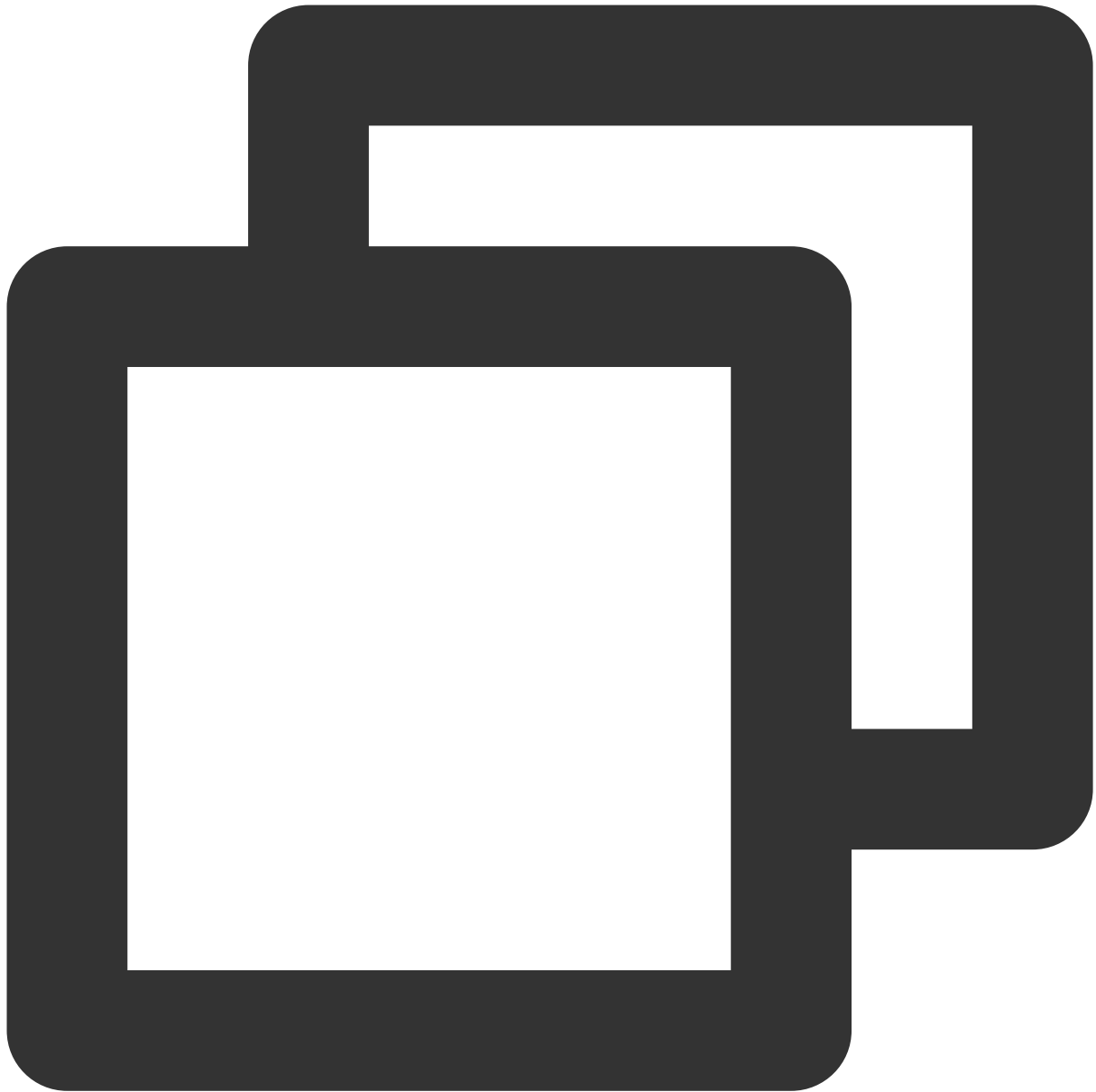
3. Direktori root default dari Nginx adalah `/usr/share/nginx/html`. Modifikasi halaman statis `index.html` dalam direktori `html` untuk menandai kekhususan halaman ini. Operasi yang relevan adalah sebagai berikut:

1. Jalankan perintah berikut untuk masuk ke halaman statis `index.html` di `html` :



```
vim /usr/share/nginx/html/index.html
```

2. Tekan "i" untuk masuk ke mode pengeditan dan tambahkan berikut ini ke dalam tag `<body></body>` :



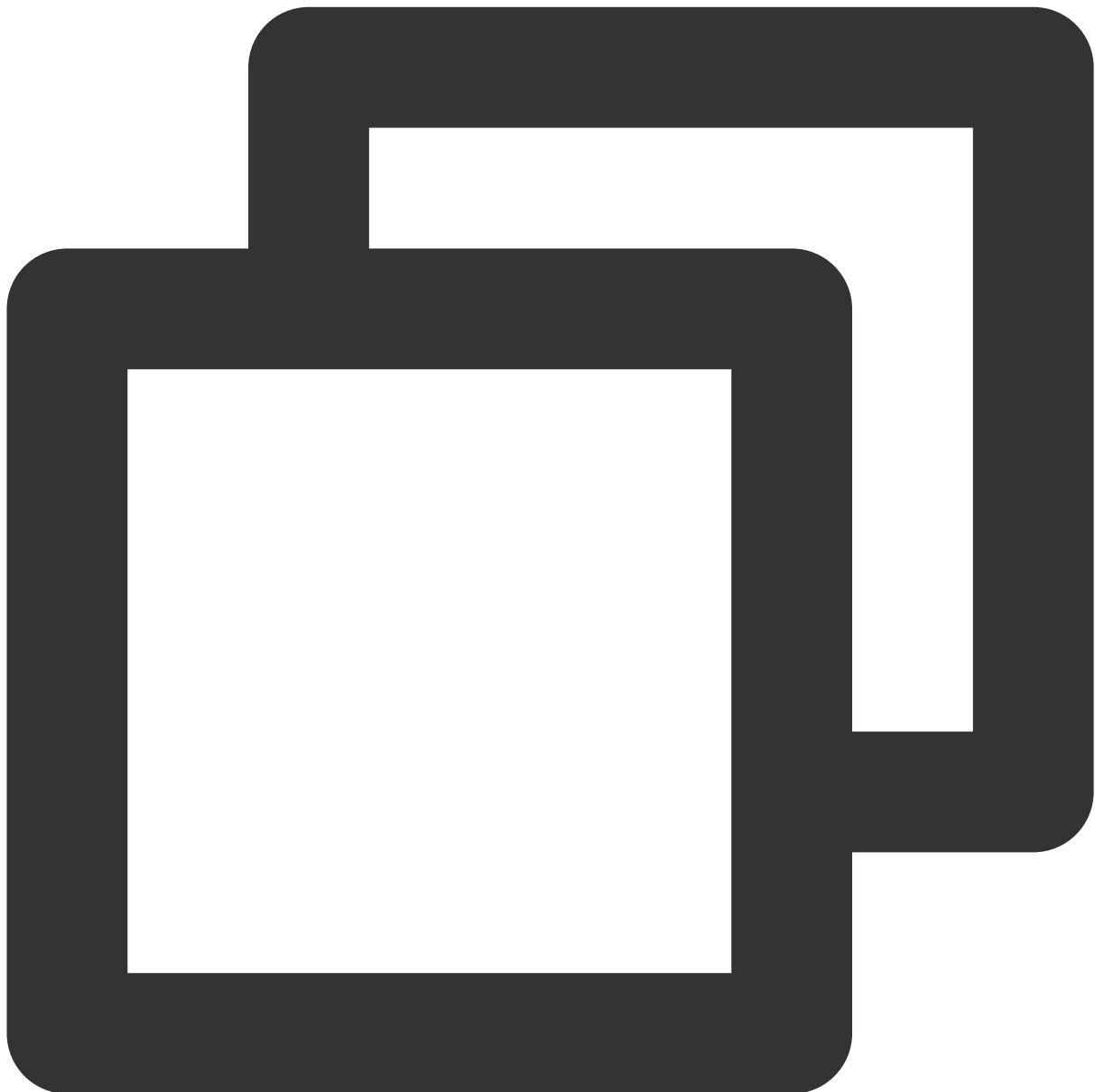
```
# Anda sebaiknya langsung masuk ke bagian `<body>`  
Halo nginx , Ini adalah rs-1!  
URL adalah index.html
```

```
<body>  
Hello nginx , This is rs-1!  
URL is index.html
```

3. Tekan "Esc" (Esc) dan masukkan `:wq` untuk menyimpan perubahan.

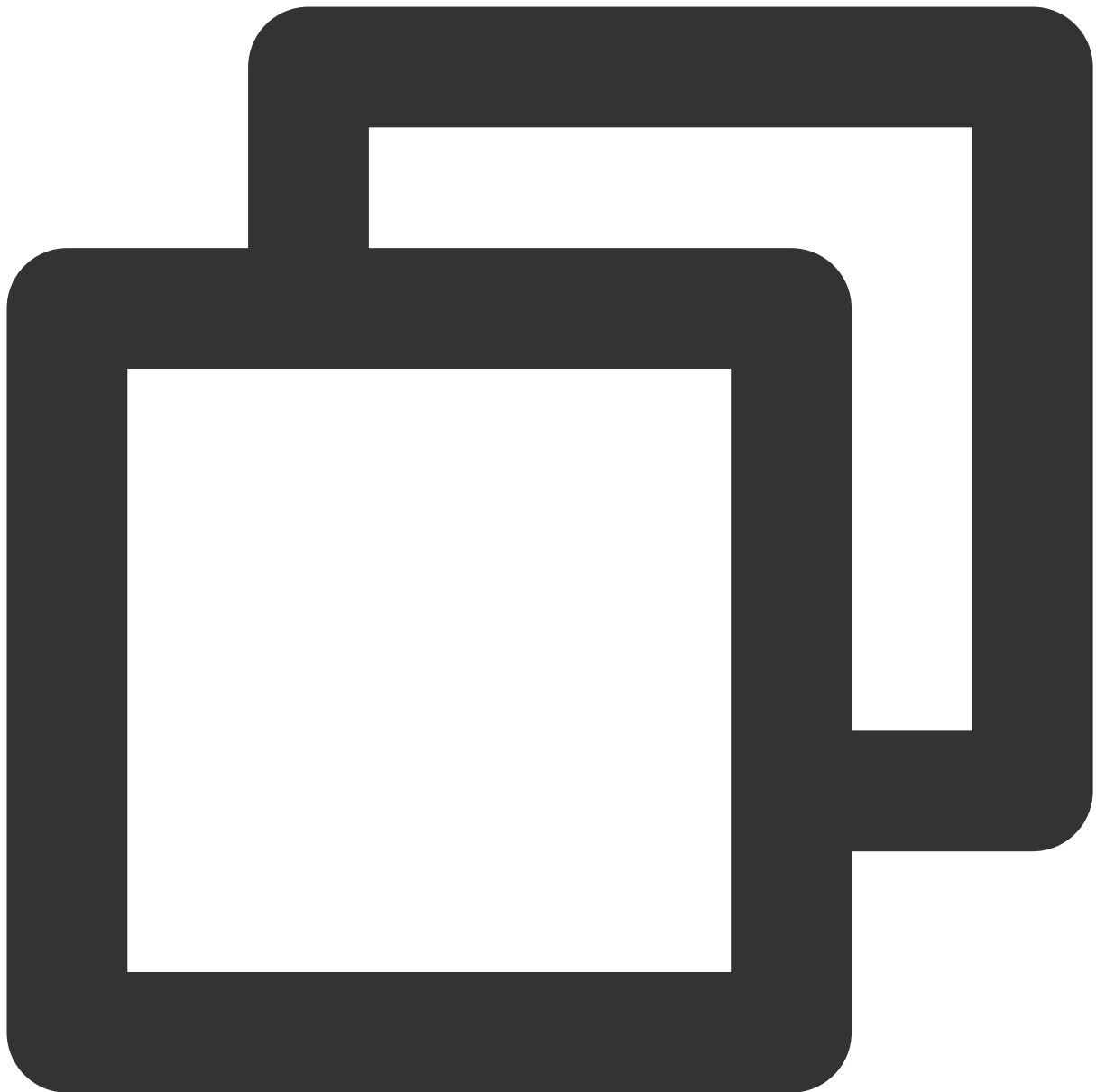
4. CLB (sebelumnya "Aplikasi CLB") dapat meneruskan permintaan menurut jalur server asli dan men-deploy halaman statis di jalur `/image`. Operasi yang relevan adalah sebagai berikut:

1. Jalankan perintah-perintah berikut untuk membuat dan masuk ke direktori `image` :



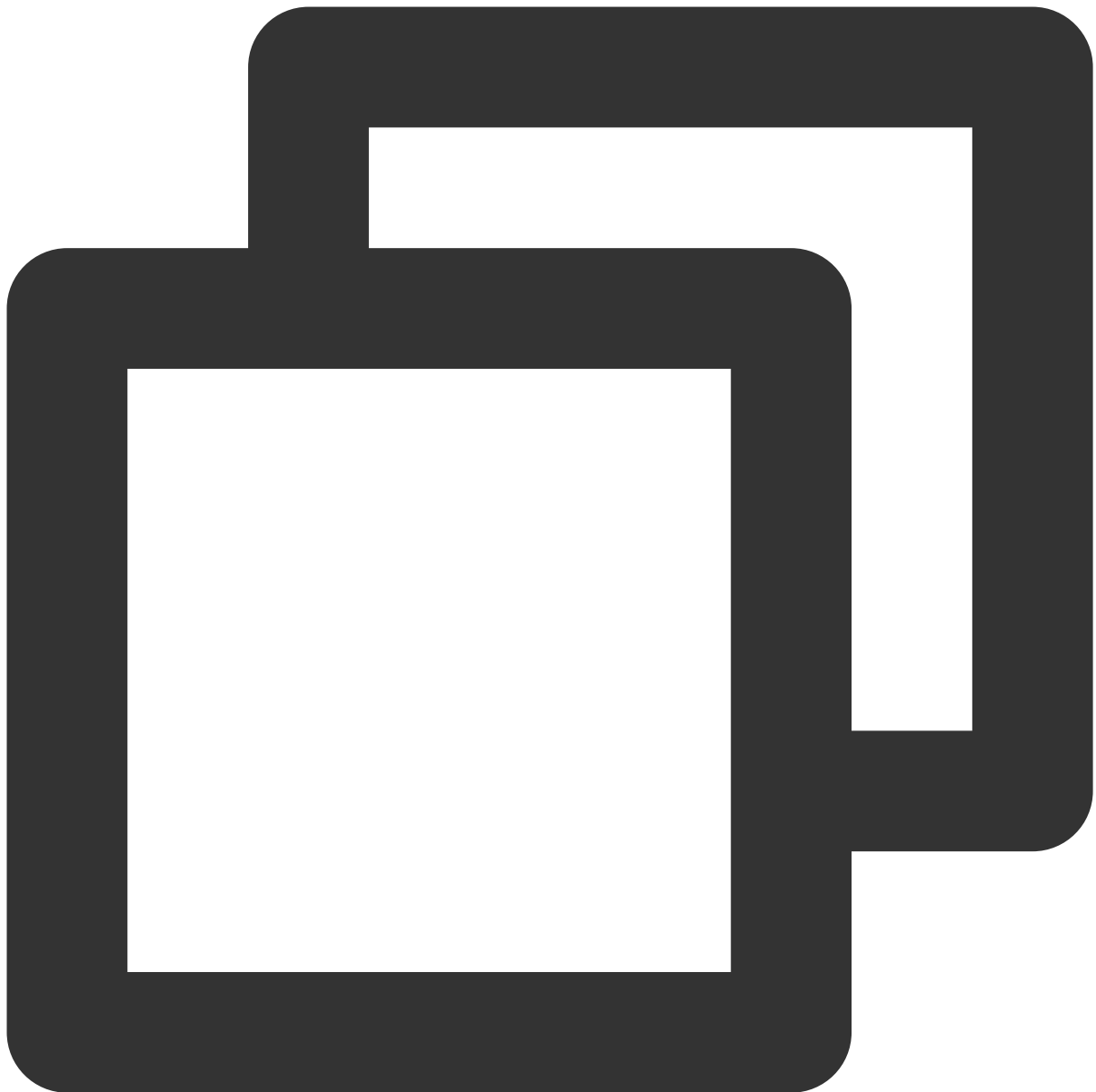
```
mkdir /usr/share/nginx/html/image  
cd /usr/share/nginx/html/image
```

2. Jalankan perintah berikut untuk membuat halaman statis `index.html` di dalam direktori `image` :



```
vim index.html
```

3. Tekan "i" untuk masuk ke mode pengeditan dan tambahkan berikut ini ke halaman:



```
Halo nginx , Ini adalah rs-1!  
URL adalah image/index.html
```

4. Tekan "Esc" (Esc) dan masukkan `:wq` untuk menyimpan perubahan.

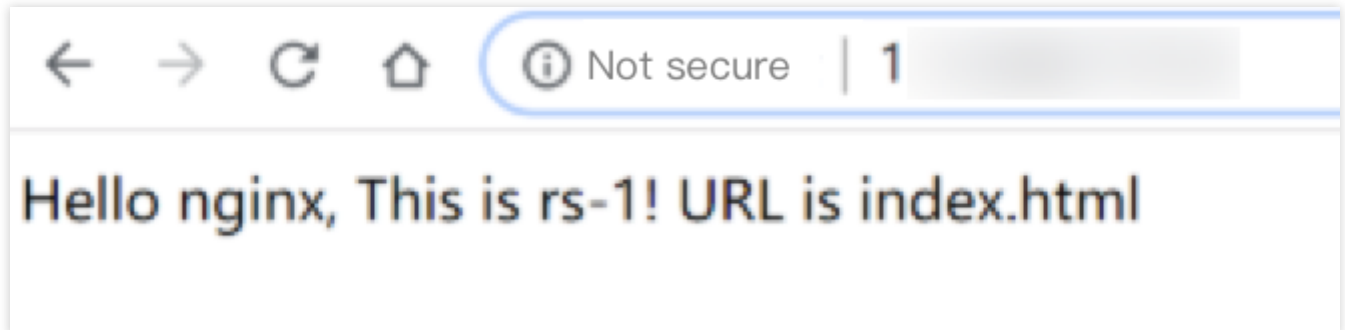
Perhatian :

Port default Nginx adalah `80` . Untuk mengubah port, silakan modifikasi file konfigurasi dan mulai ulang Nginx.

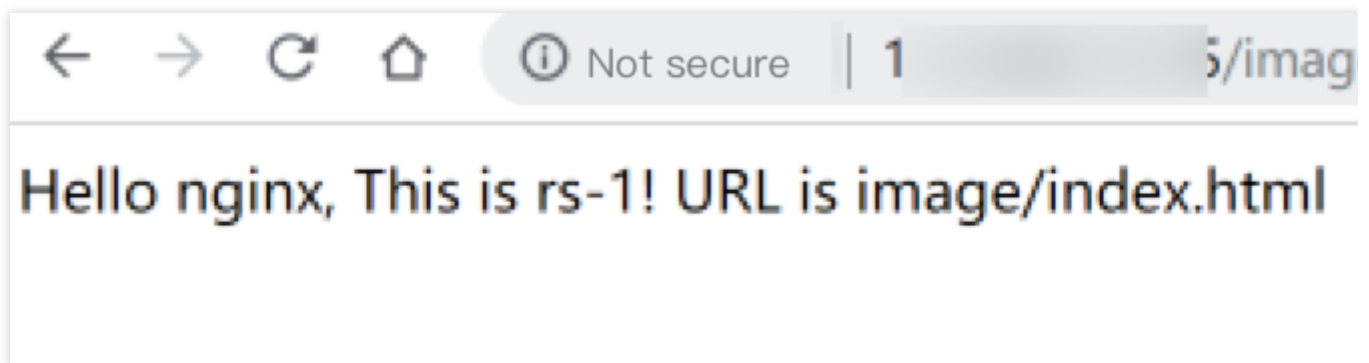
Memverifikasi Layanan Nginx

Akses IP publik dan jalur instance CVM Anda. Jika halaman statis yang di-deploy ditampilkan, Nginx telah berhasil di-deploy.

halaman `index.html` dari `rs-1` :



halaman `/image/index.html` dari `rs-1` :



Men-deploy Java Web di CentOS

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

Dokumen ini menjelaskan cara men-deploy proyek-proyek Web Java di CentOS dan cocok untuk setiap pengguna baru Tencent Cloud.

Versi Perangkat Lunak

Versi alat perangkat lunak yang digunakan dalam dokumen ini adalah sebagai berikut, yang mungkin berbeda dengan versi perangkat lunak Anda selama operasi aktual.

Sistem operasi:CentOS 7.5

Tomcat: apache-tomcat-8.5.39

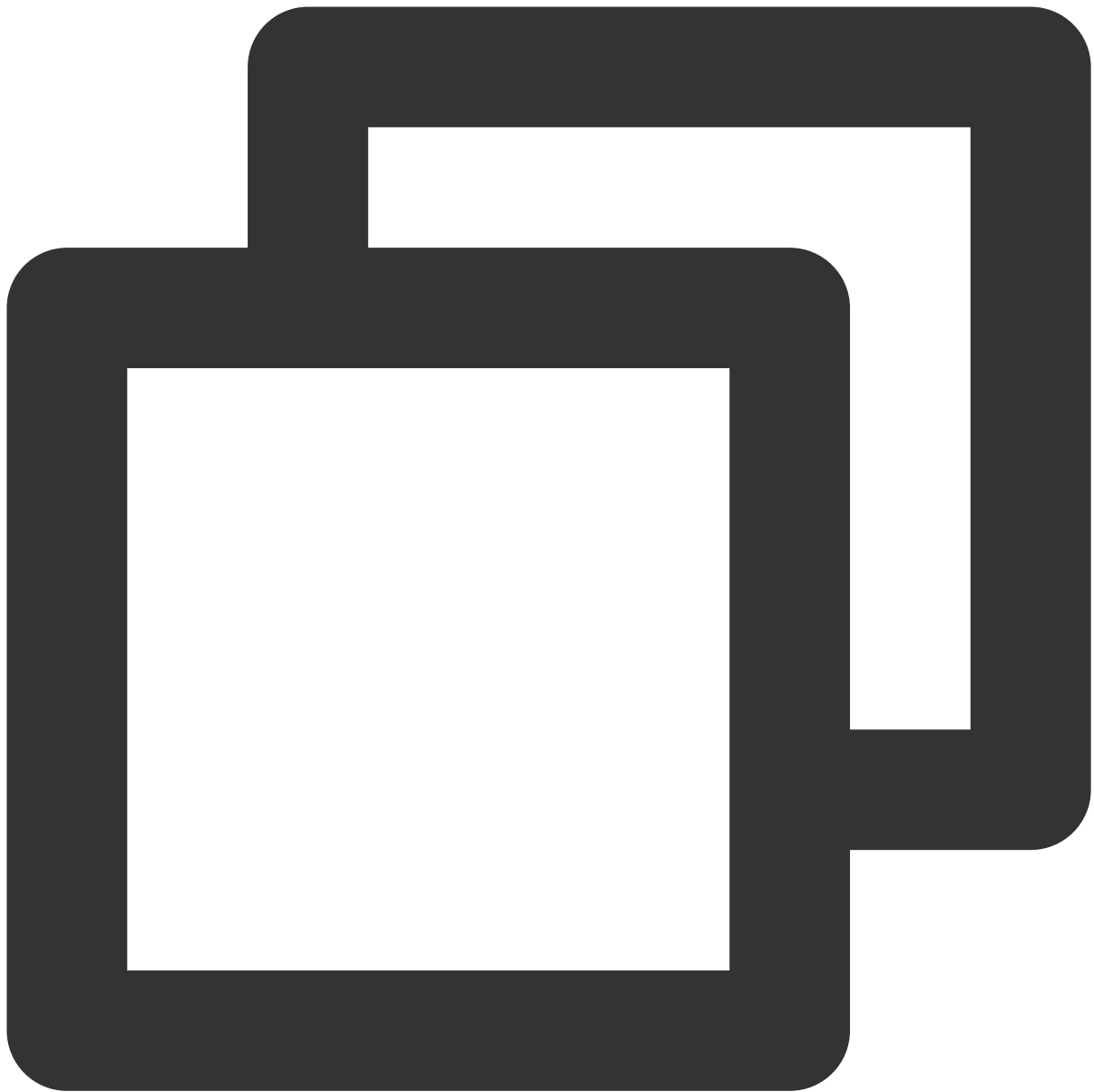
JDK:JDK 1.8.0_201

Menginstal JDK

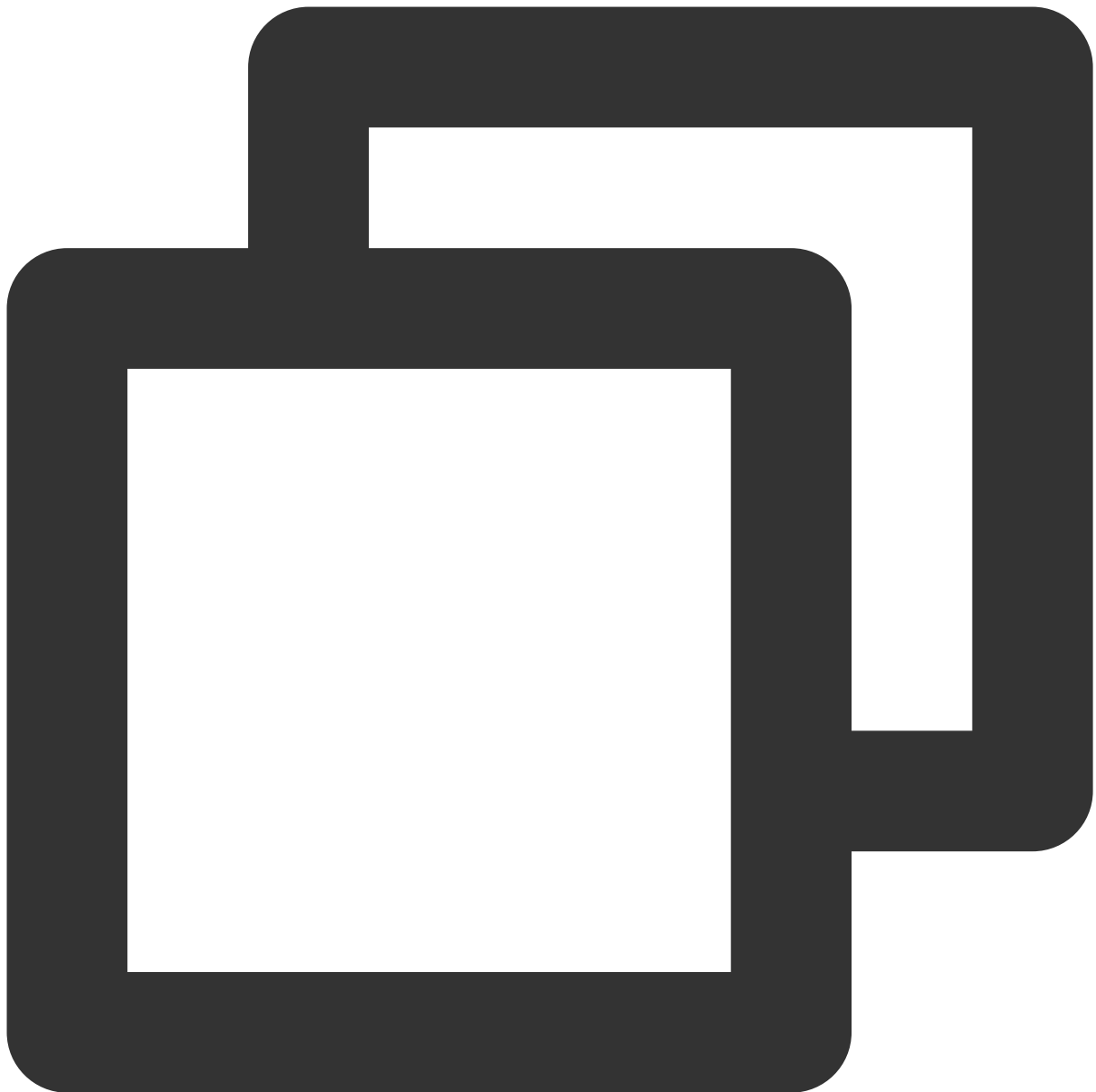
Setelah membeli CVM, Anda dapat mengklik **Login** (Masuk) di halaman detail CVM untuk masuk ke instance CVM Anda agar dapat memasukkan nama pengguna dan kata sandi guna menyiapkan lingkungan web Java.Untuk informasi selengkapnya tentang cara membuat instance CVM, lihat [CVM - Membuat Instance](#).

Mengunduh JDK

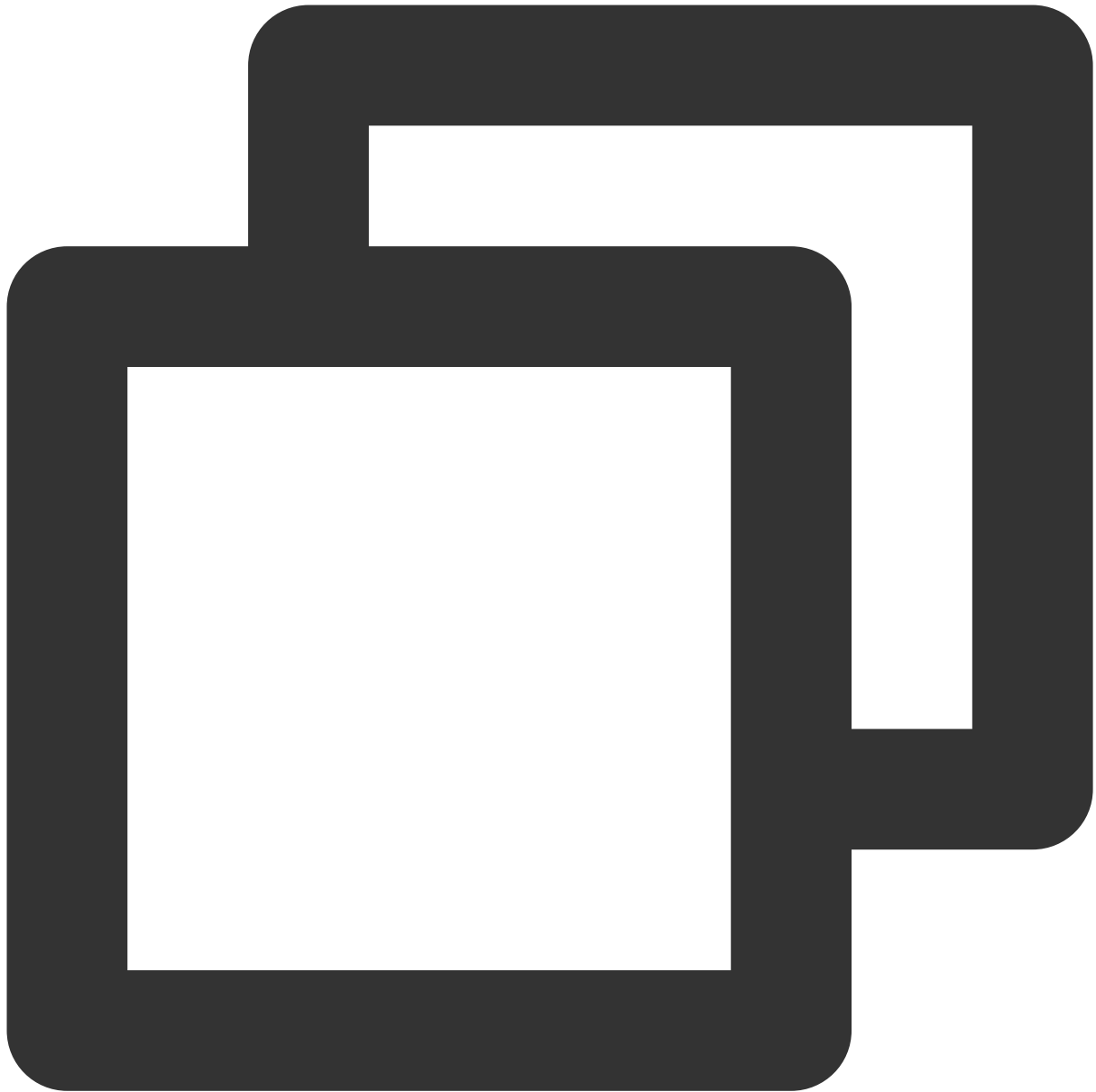
Masukkan perintah berikut:



```
mkdir /usr/java # Buat folder `java`  
cd /usr/java # Masukkan folder `java`
```



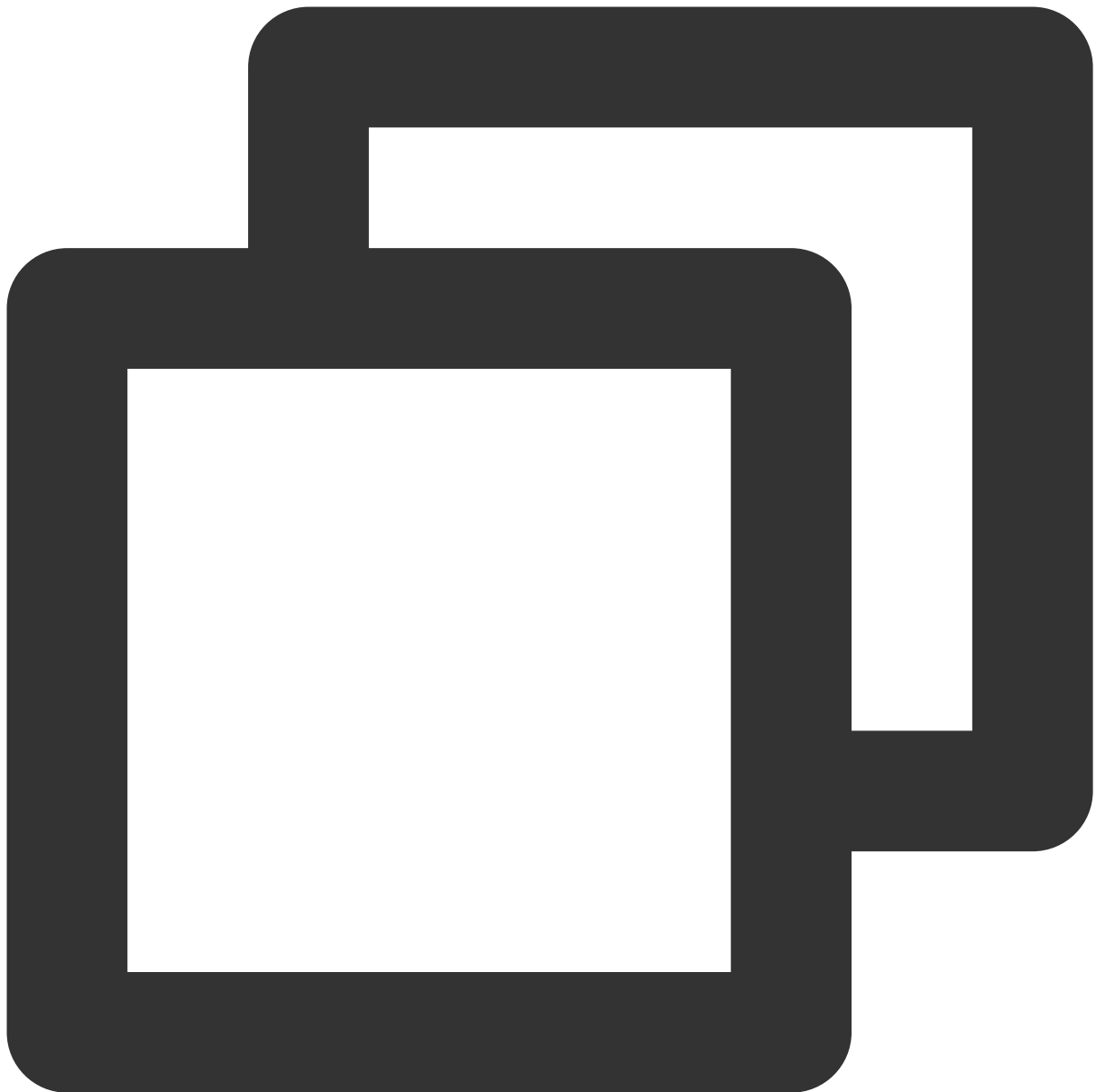
```
# Mengunggah paket penginstalan JDK (disarankan)
Anda sebaiknya menggunakan alat seperti WinSCP untuk mengunggah paket penginstalan
Atau
# Gunakan perintah (Anda sebaiknya mengunggah paket penginstalan): jalankan `wget`
wget --no-check-certificate --no-cookies --header "Cookie: oraclelicense=accept-sec
```



```
# Dekompresi
chmod +x jdk-8u201-linux-x64.tar.gz
tar -xzvf jdk-8u201-linux-x64.tar.gz
```

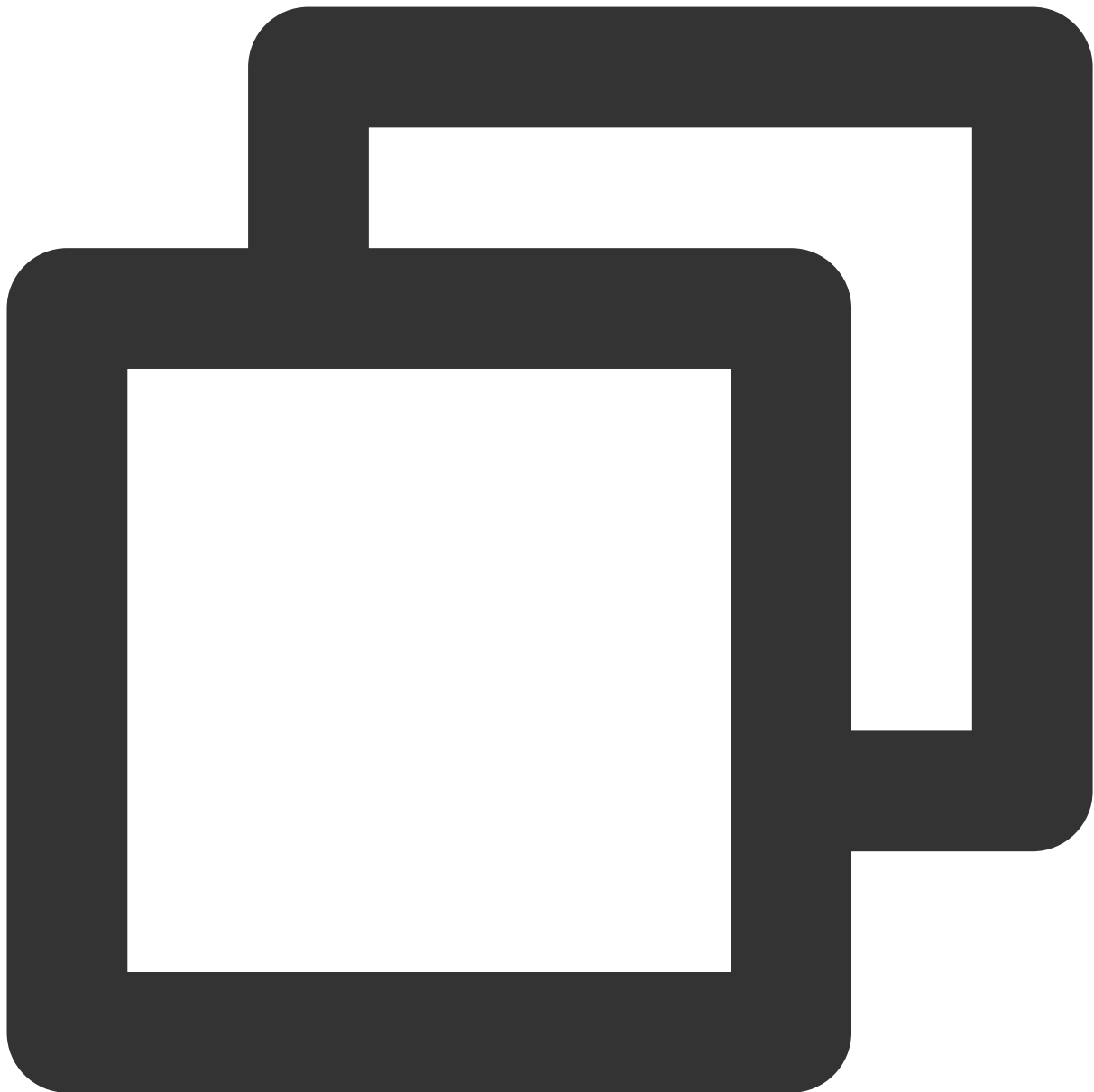
Mengatur variabel lingkungan

1. Buka file `/etc/profile` .



```
vi /etc/profile
```

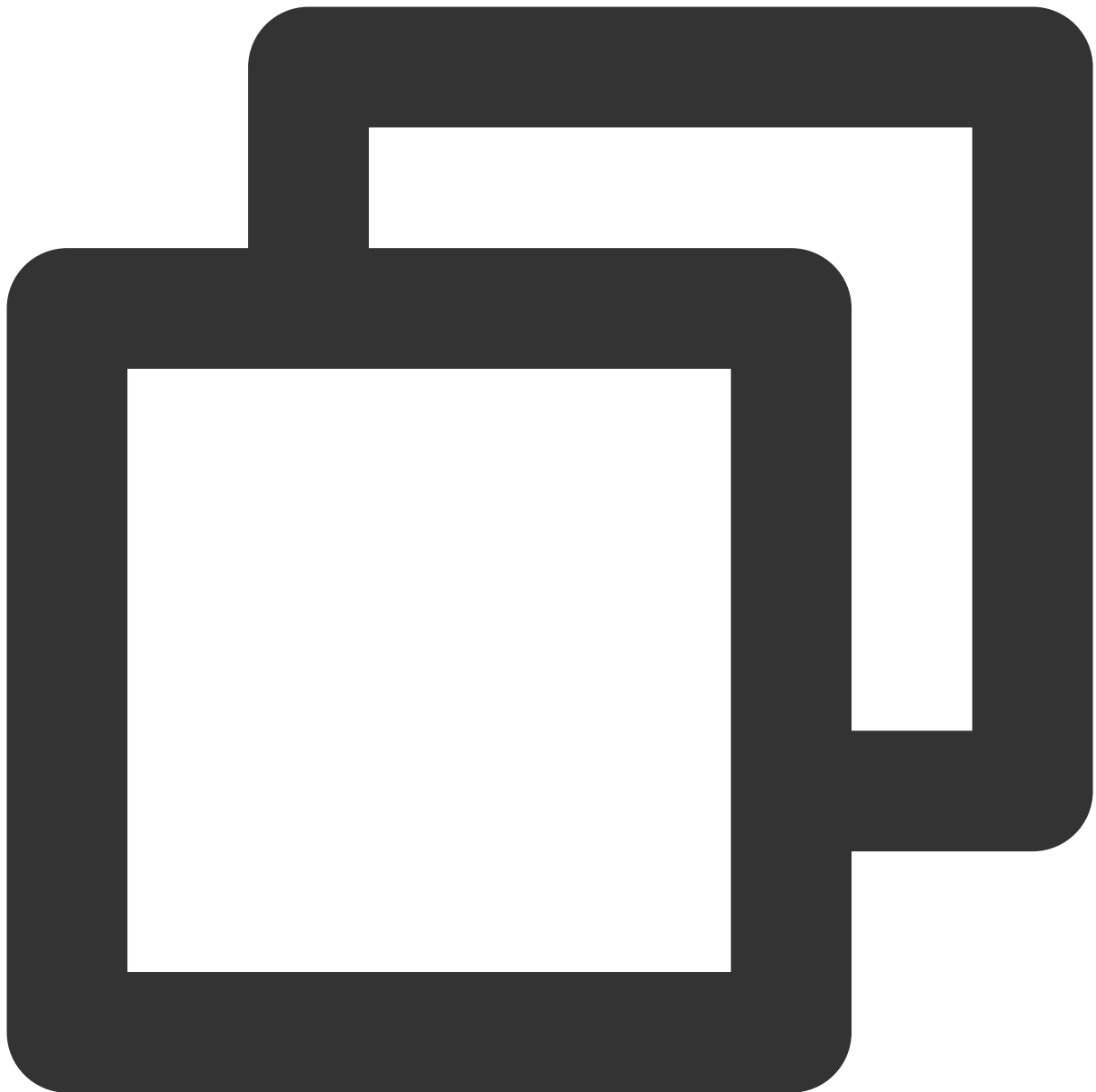
2. Tekan I untuk masuk ke mode pengeditan dan tambahkan informasi berikut ke dalam file.



```
# atur lingkungan java
ekspor JAVA_HOME=/usr/java/jdk1.8.0_201
ekspor CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
ekspor PATH=$JAVA_HOME/bin:$PATH
```

3. Tekan Esc untuk keluar dari mode pengeditan dan masukkan `:wq` untuk menyimpan dan menutup file.

4. Muat variabel lingkungan.



```
source /etc/profile
```

Melihat hasil penginstalan JDK

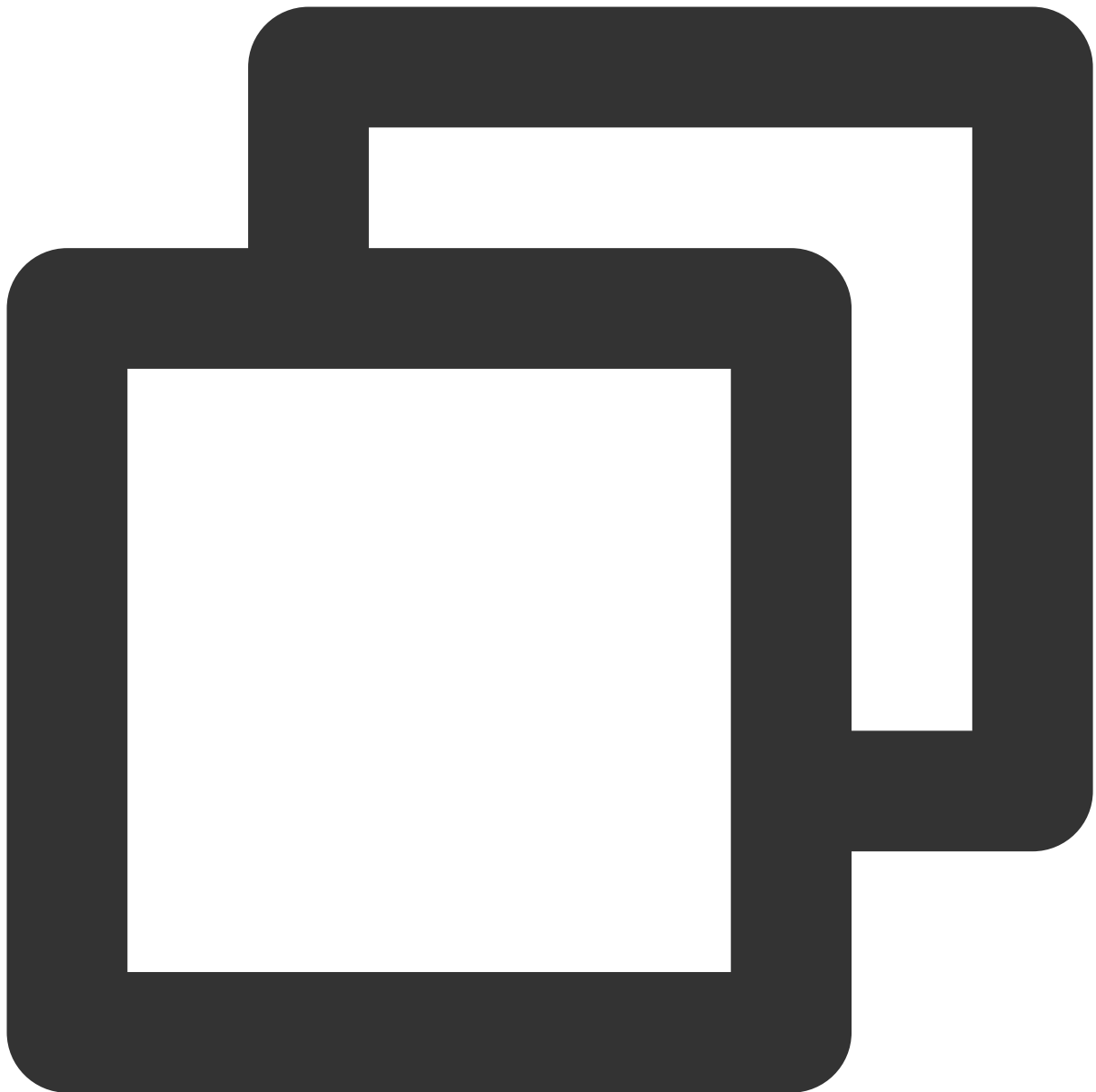
Jalankan perintah `java -version`. Jika informasi versi JDK ditampilkan, JDK telah berhasil diinstal.

```
[root@emma /]# java -version
java version "1.8.0_201"
Java(TM) SE Runtime Environment (build 1.8.0_201-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.201-b09, mixed mode)
```

Menginstal Tomcat

Mengunduh Tomcat

Masukkan perintah-perintah berikut:



```
# Alamat cermin dapat berubah dan versi Tomcat mungkin terus-menerus ditingkatkan.J
wget http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-8/v8.5.39/bin/apache-
tar -xzvf apache-tomcat-8.5.39.tar.gz
mv apache-tomcat-8.5.39 /usr/local/tomcat/
```

File-file berikut ada di dalam direktori `/usr/local/tomcat/` :

`bin`: file skrip, yang berisi skrip untuk memulai dan menghentikan layanan Tomcat.

`conf`: file-file konfigurasi global, dengan file-file terpenting berupa `server.xml` dan `web.xml` .

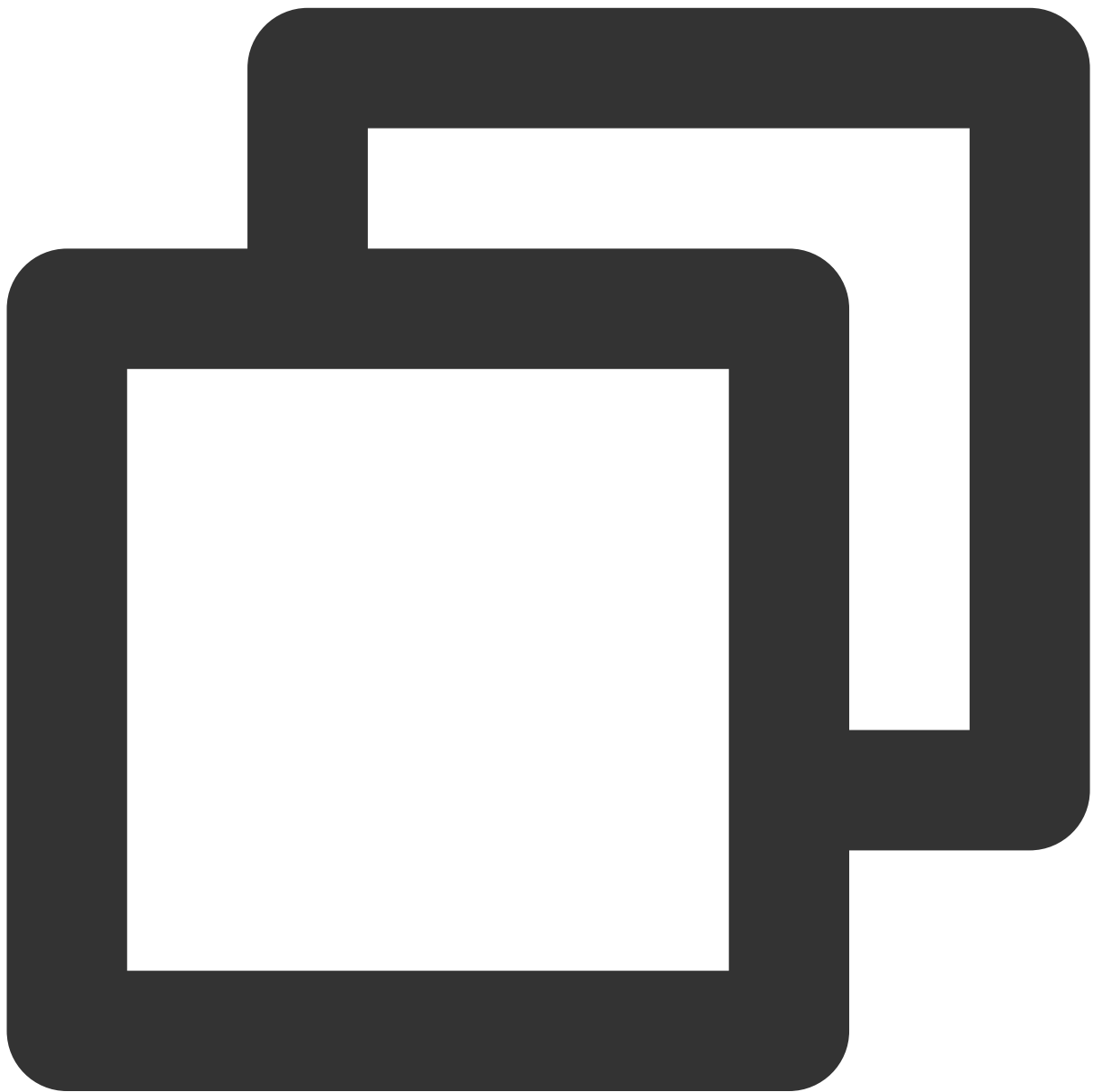
`webapps`: direktori rilis web utama di Tomcat, yang merupakan direktori default untuk menyimpan file-file aplikasi web.

logs:file log Tomcat.

Perhatian :

Jika tautan unduh kedaluwarsa, silakan ganti dengan tautan terbaru di [situs web resmi Tomcat](#).

Menambahkan pengguna

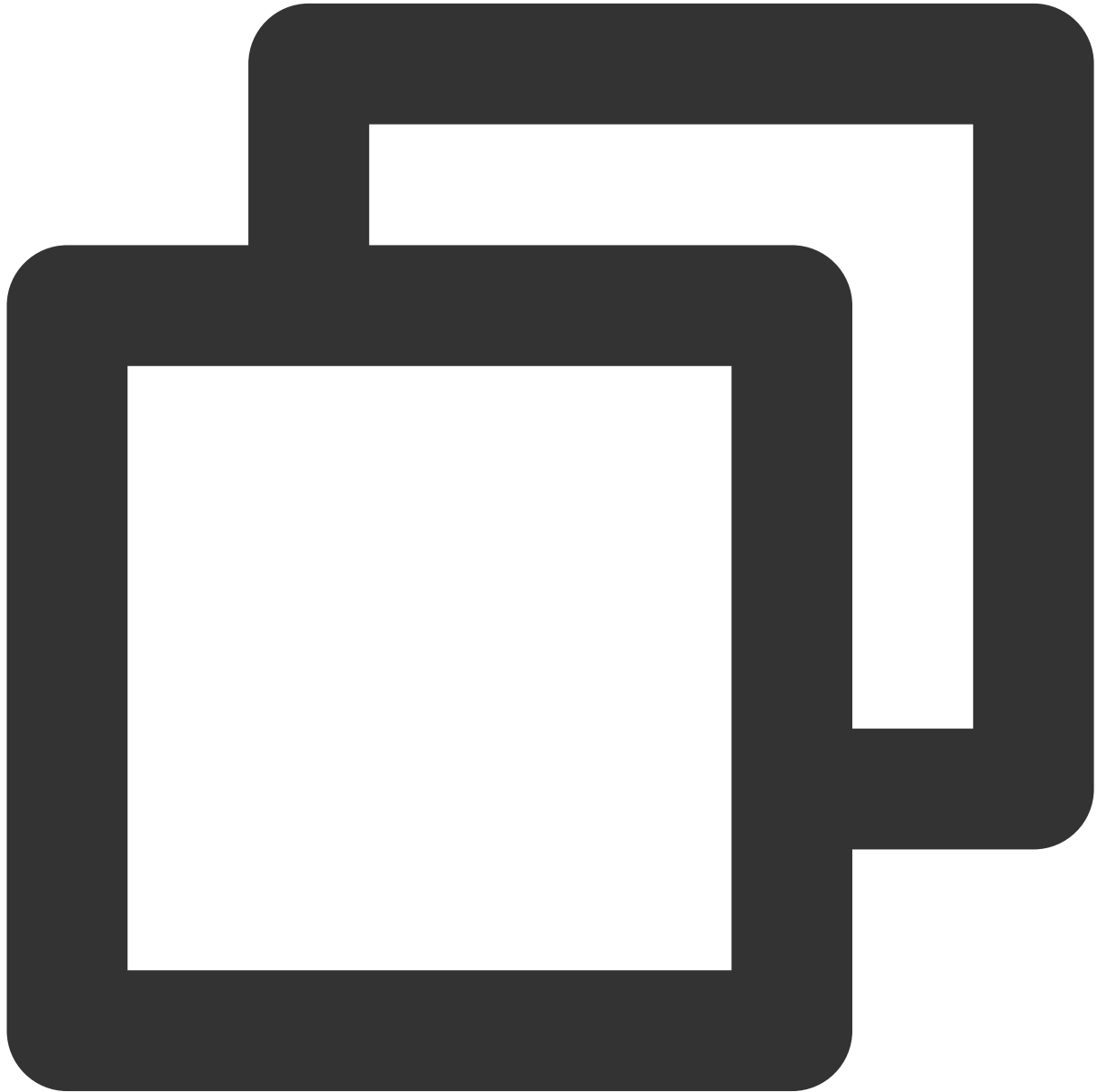


```
# Tambahkan `www` pengguna umum untuk menjalankan Tomcat
useradd www
# Buat direktori root situs web
mkdir -p /data/wwwroot/default
```

```
# Unggah file proyek web Java (paket WAR) ke direktori root situs web dan ubah izin  
echo Halo Tomcat! > /data/wwwroot/default/index.jsp  
chown -R www.www /data/wwwroot
```

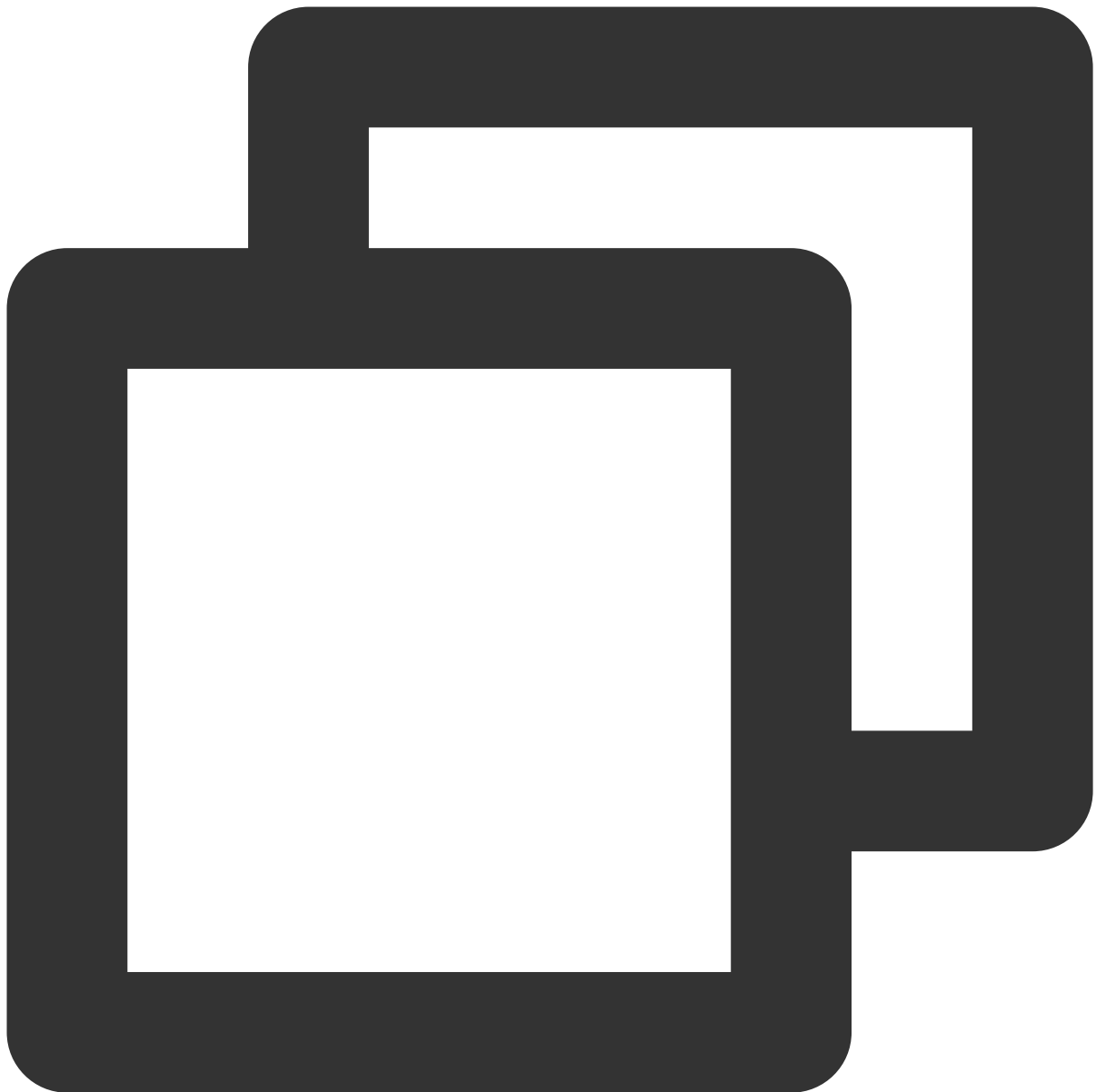
Mengatur parameter memori JVM

1. Buat file skrip `/usr/local/tomcat/bin/setenv.sh` .



```
vi /usr/local/tomcat/bin/setenv.sh
```

2. Tekan `I` untuk masuk ke mode pengeditan dan tambahkan berikut ini.

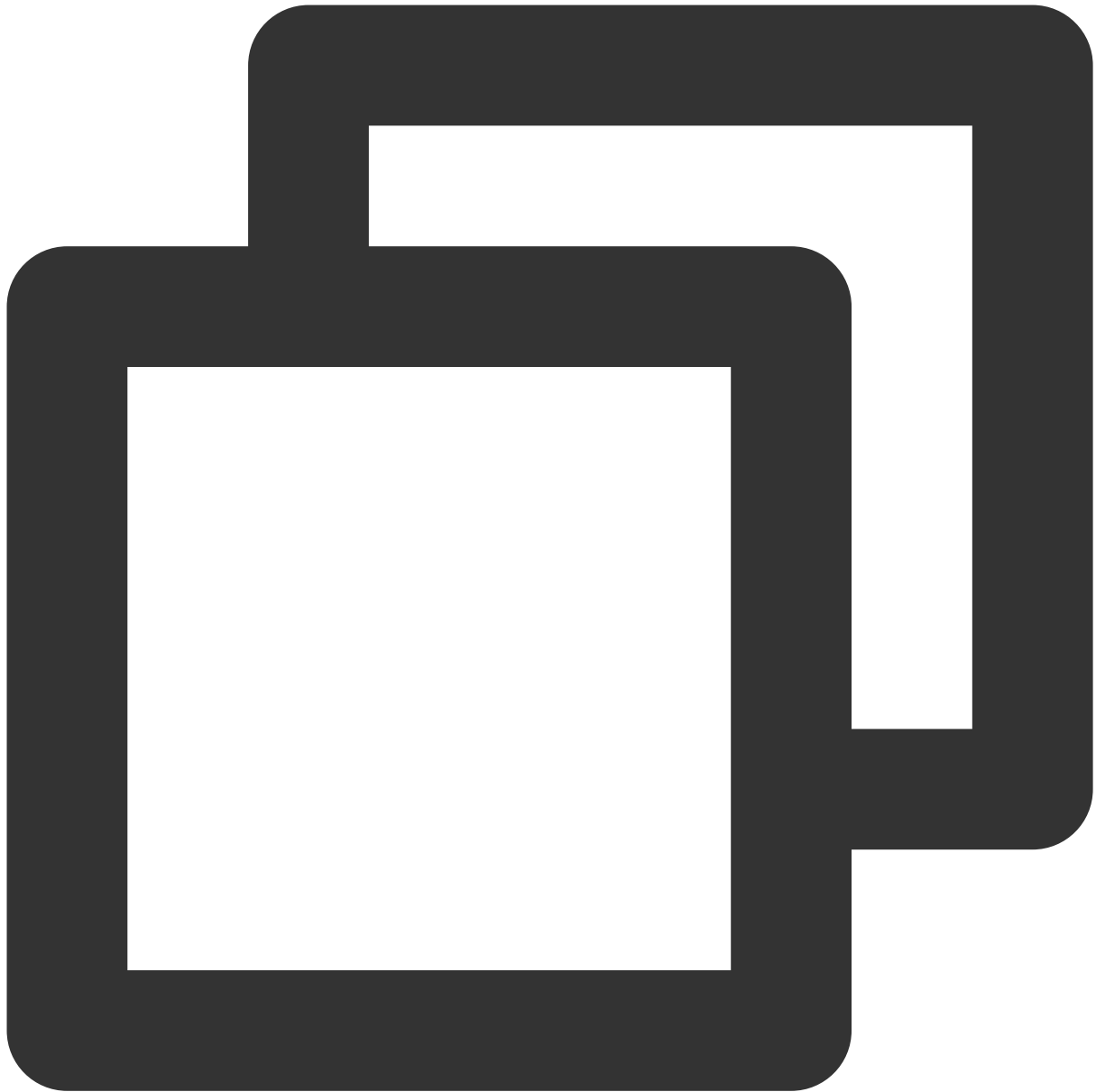


```
JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m -Dfile
```

3. Tekan Esc untuk keluar dari mode pengeditan dan masukkan `:wq` untuk menyimpan dan keluar.

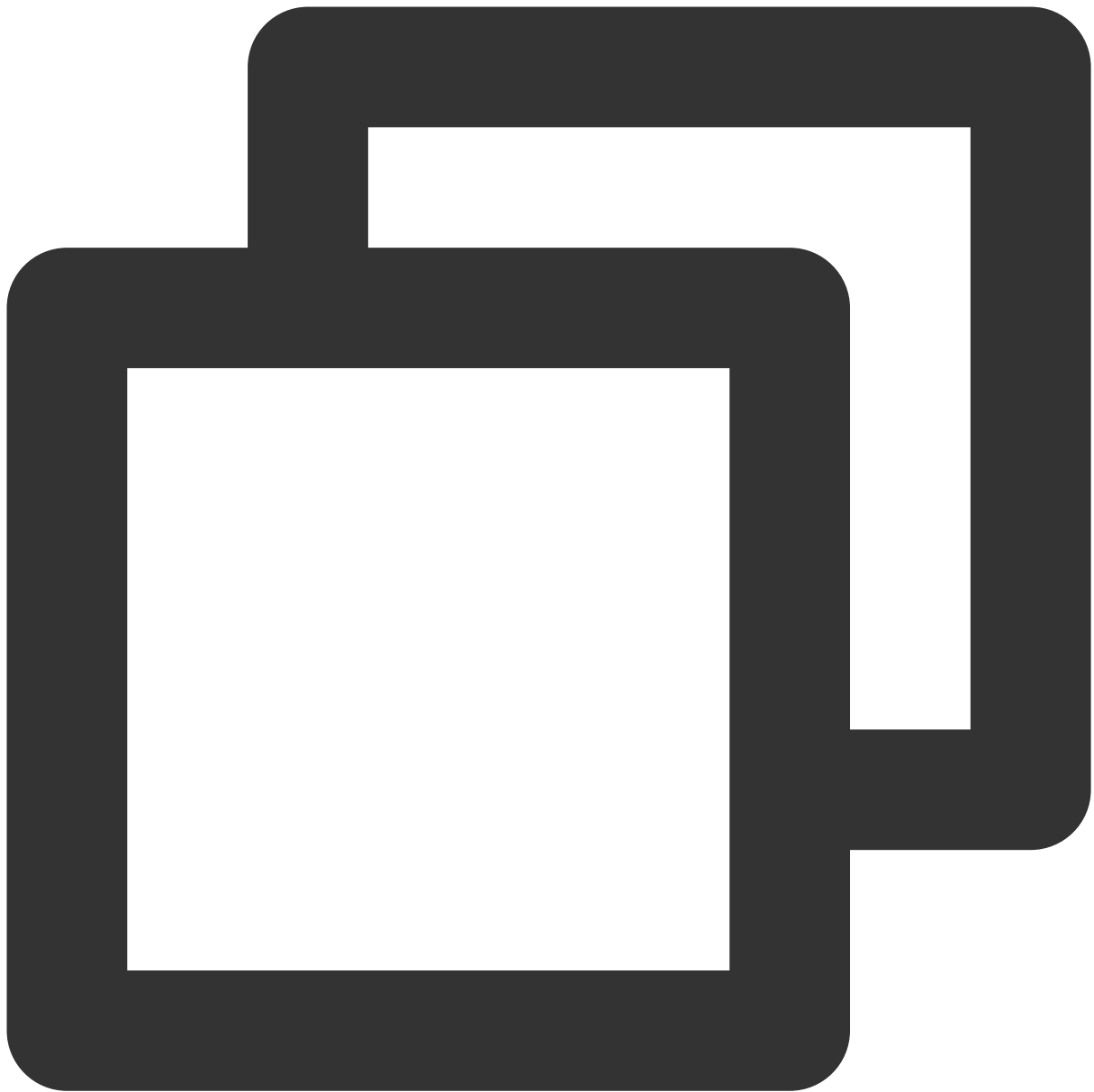
Mengonfigurasi server.xml

1. Beralihlah ke direktori `/usr/local/tomcat/conf/`.



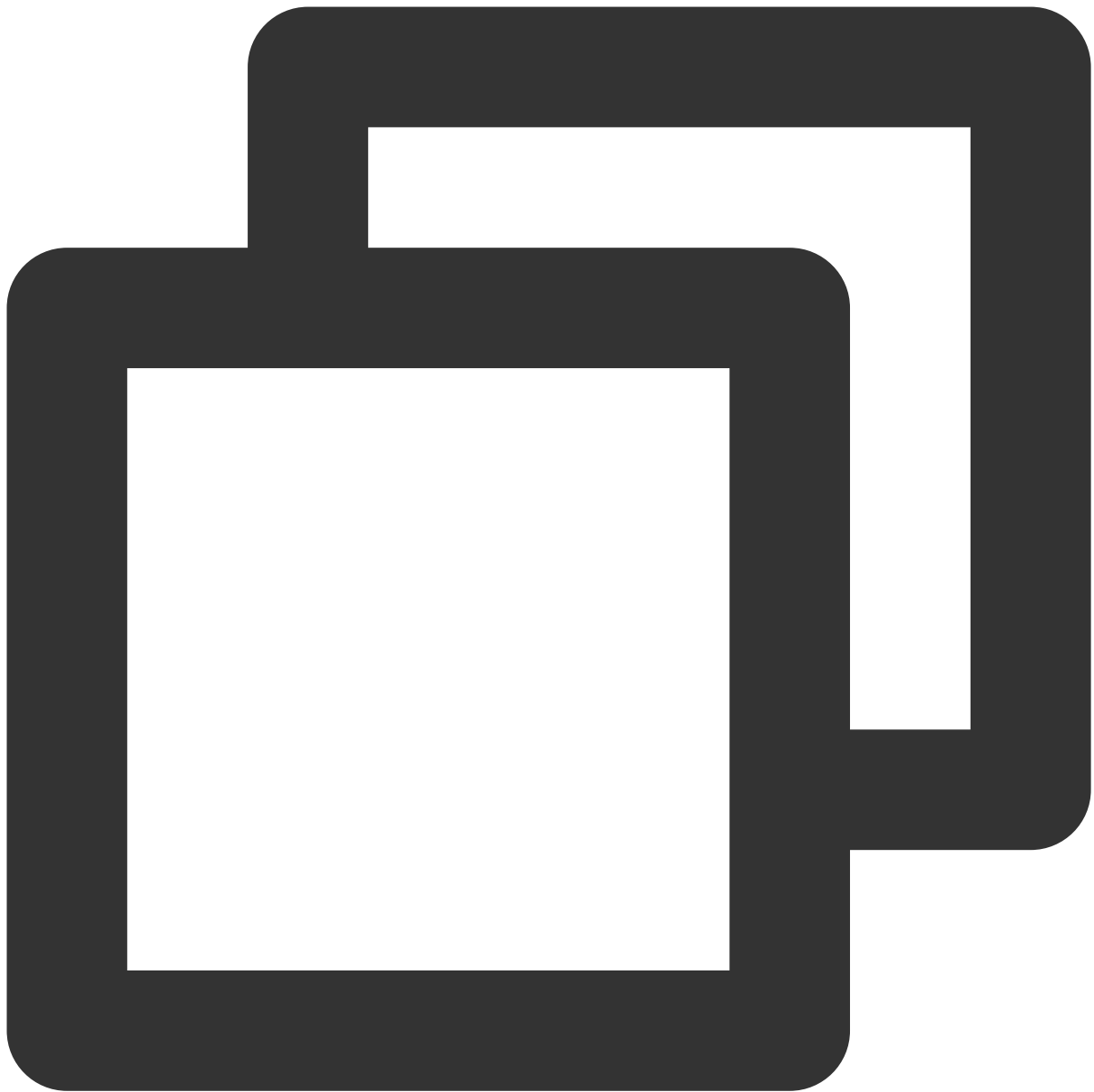
```
cd /usr/local/tomcat/conf/
```

2. Cadangkan file `server.xml` .



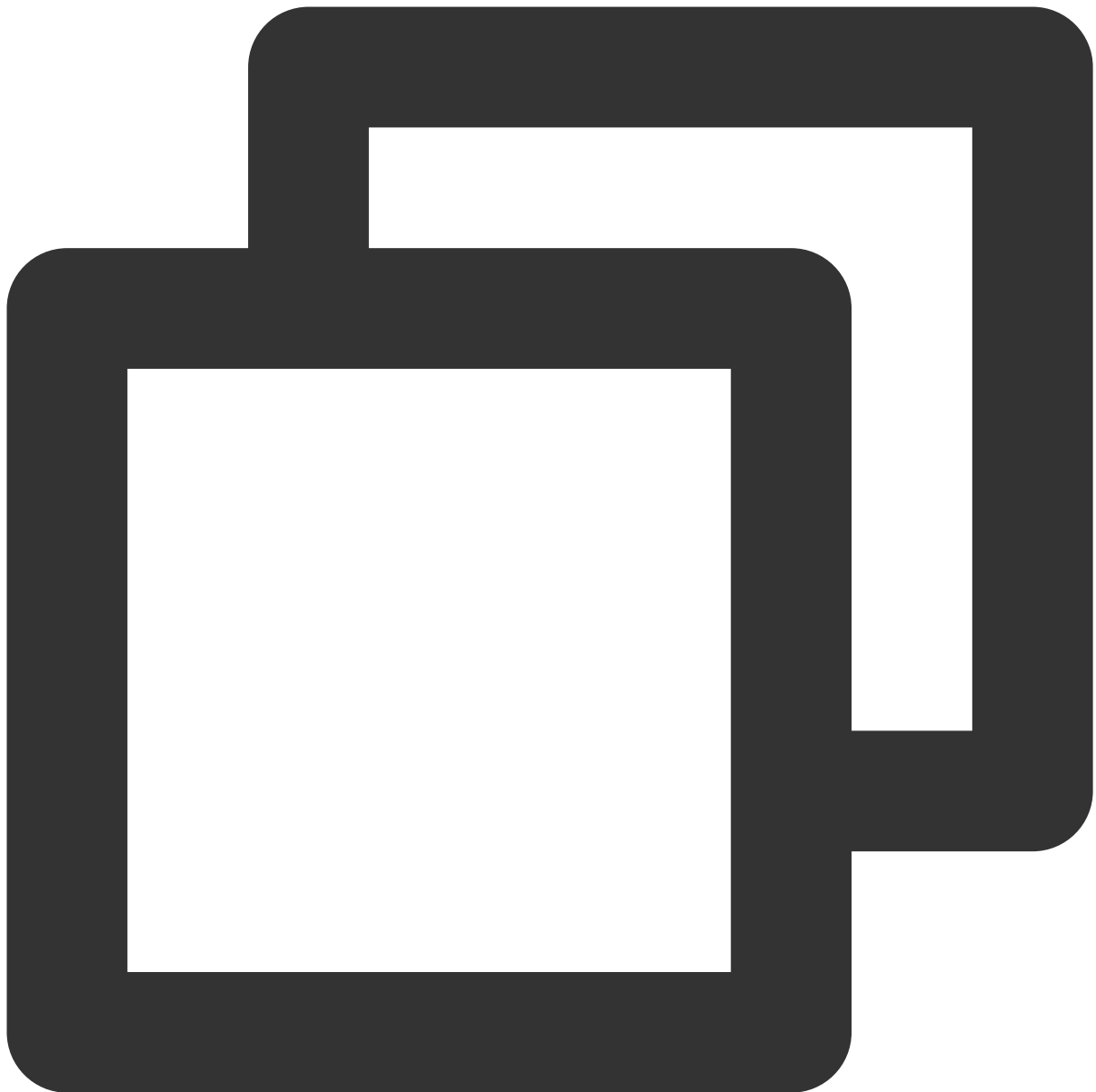
```
mv server.xml server_default.xml
```

3. Buat file `server.xml` yang baru.



```
vi server.xml
```

4. Tekan I untuk masuk ke mode pengeditan dan tambahkan berikut ini.



```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8006" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener"/>
  <Listener className="org.apache.catalina.core.AprLifecycleListener"/>
  <GlobalNamingResources>
    <Resource name="UserDatabase" auth="Container"
      type="org.apache.catalina.UserDatabase"
      deskripsi="User database that can be updated and saved" (Database pengguna yang dap
      factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
```

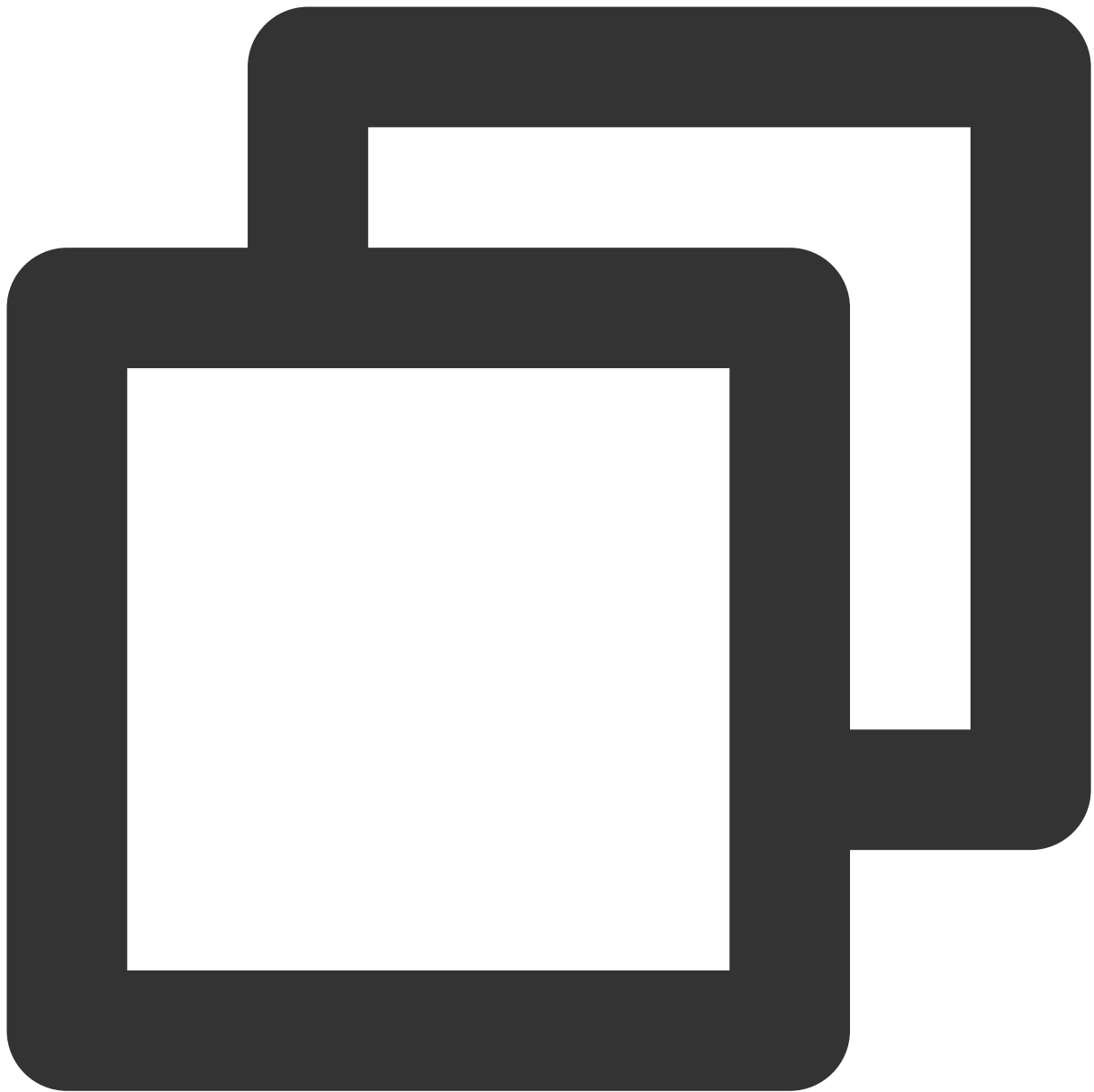
```
pathname="conf/tomcat-users.xml"/>
</GlobalNamingResources>
<Service name="Catalina">
<Connector port="8080"
protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443"
maxThreads="1000"
minSpareThreads="20"
acceptCount="1000"
maxHttpHeaderSize="65536"
debug="0"
disableUploadTimeout="true"
useBodyEncodingForURI="true"
enableLookups="false"
URIEncoding="UTF-8"/>
<Engine name="Catalina" defaultHost="localhost">
<Realm className="org.apache.catalina.realm.LockOutRealm">
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"/>
</Realm>
<Host name="localhost" appBase="/data/wwwroot/default" unpackWARs="true" autoDeploy
<Context path="" docBase="/data/wwwroot/default" debug="0" reloadable="false" cross
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log."suffix=".txt" pattern="%h %l %u %t &quot;%r&quot; %s
</Host>
</Engine>
</Service>
</Server>
```

5. Tekan Esc untuk keluar dari mode pengeditan dan masukkan `:wq` untuk menyimpan dan keluar.

Memulai Tomcat

Metode 1

Masukkan direktori `bin` dari server Tomcat lalu jalankan perintah `./startup.sh` untuk memulai server Tomcat.



```
cd /usr/local/tomcat/bin  
./startup.sh
```

Hasil eksekusi adalah sebagai berikut:

```
[root@emma bin]# ./startup.sh
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr/java/jdk1.8.0_201
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local
Tomcat started.
```

Metode 2

1. Siapkan mulai cepat agar server Tomcat dapat dimulai di mana saja melalui `service tomcat start` .



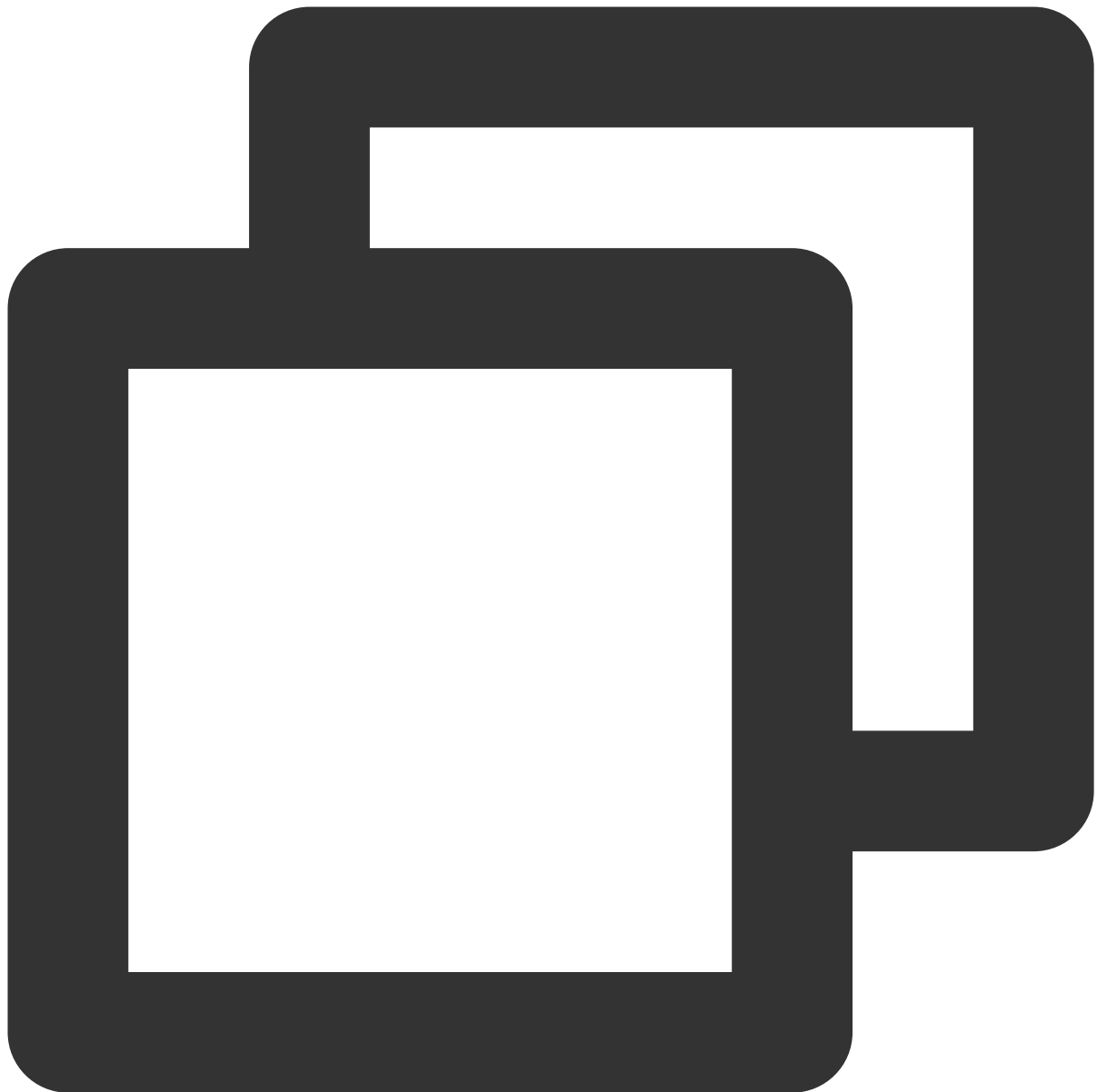
```
wget https://github.com/lj2007331/oneinstack/raw/master/init.d/Tomcat-init
mv Tomcat-init /etc/init.d/tomcat
chmod +x /etc/init.d/tomcat
```

2. Jalankan perintah berikut dan atur skrip startup `JAVA_HOME` .



```
sed -i 's@^export JAVA_HOME=.*@export JAVA_HOME=/usr/java/jdk1.8.0_201@' /etc/init.
```

3. Atur jalankan otomatis.



```
chkconfig --tambahkan tomcat  
chkconfig tomcat di
```

4. Mulai Tomcat.

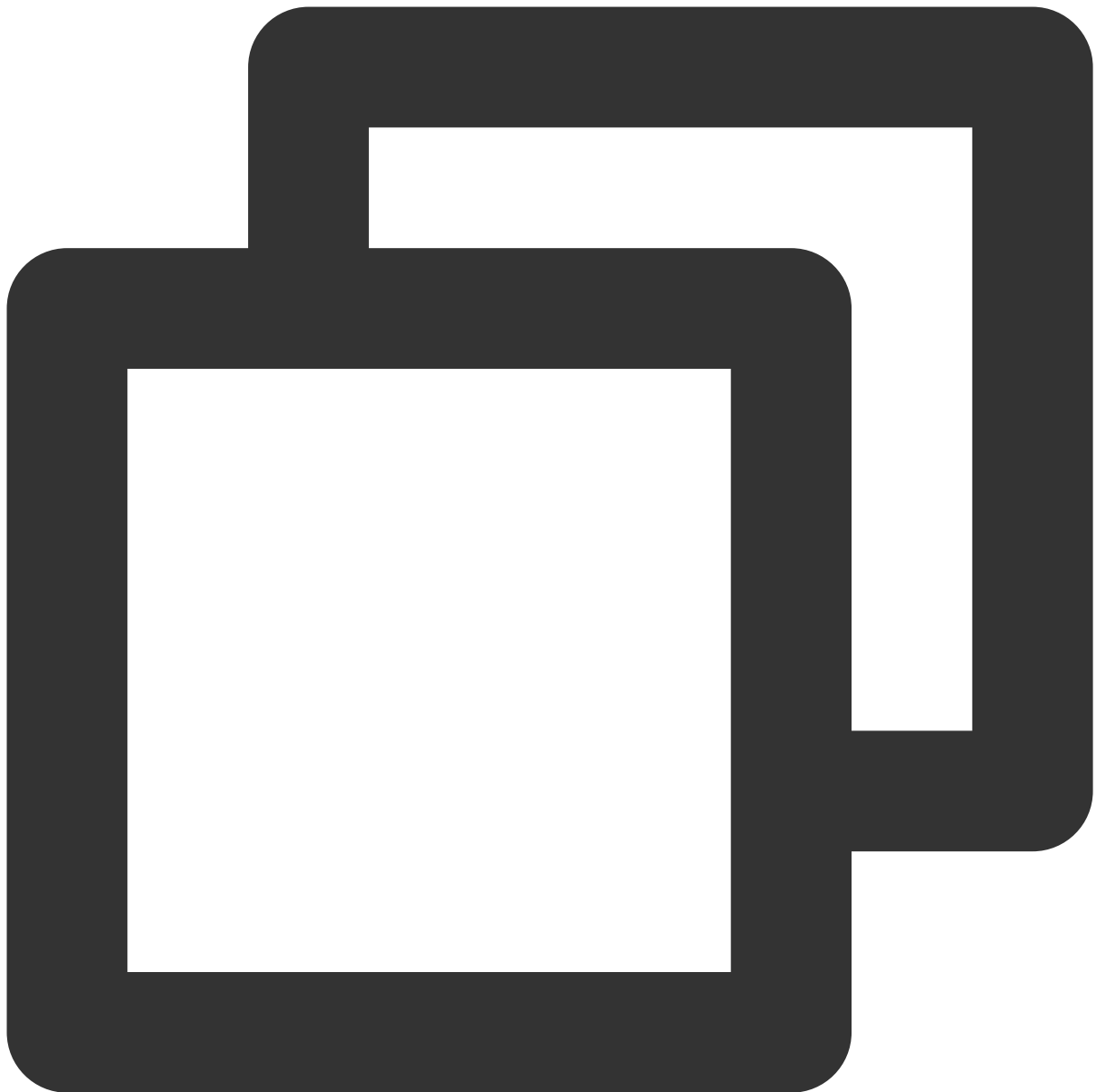


```
# Mulai Tomcat
mulai layanan tomcat
# Lihat status server Tomcat
status layanan tomcat
# Hentikan Tomcat
hentikan layanan tomcat
```

Hasil eksekusi adalah sebagai berikut:

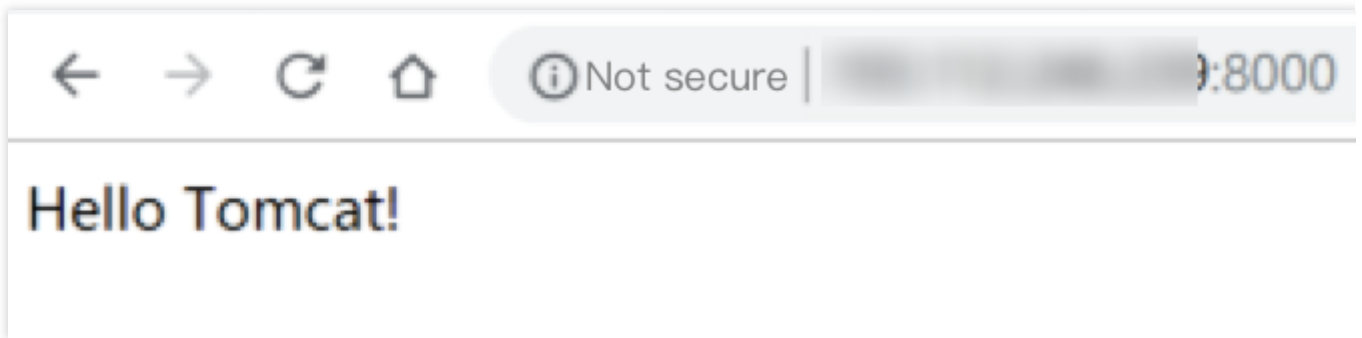
```
[root@emma bin]# service tomcat start
Tomcat is already running (pid: 27293)
[root@emma bin]# service tomcat status
Tomcat is running with pid: 27293
[root@emma bin]# service tomcat stop
Stopping Tomcat
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr/java/jdk1.8.0_201
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local
waiting for processes to exit
```

5. Jika sistem menampilkan prompt bahwa Anda tidak memiliki izin, beralihlah ke pengguna root dan ubah izinnya.



```
cd /usr/local  
chmod -R 777 tomcat
```

6. Masukkan `http://public IP:port` (di sini port adalah port konektor yang diatur dalam `server.xml`) di bilah alamat peramban. Jika muncul halaman berikut, penginstalan berhasil.



Mengonfigurasi grup keamanan

Jika terjadi kegagalan akses, periksa grup keamanan. Seperti yang terpampang pada contoh di atas, port konektor adalah 8080 di `server.xml` sehingga Anda harus membuka TCP:8080 ke internet di grup keamanan yang terikat dengan instance CVM yang sesuai.

Add Inbound rule

Type	Source ⓘ	Protocol port ⓘ	Policy	Notes
Custom ▼	0.0.0.0/0	TCP:8080	Allow ▼	Tomcat
+ New Line				
		<input type="button" value="Completed"/>	<input type="button" value="Cancel"/>	